



Verwenden Sie StorageGRID

StorageGRID 11.8

NetApp
March 19, 2024

Inhalt

- Nutzung von StorageGRID Mandanten und Clients 1
 - Verwenden Sie ein Mandantenkonto 1
 - S3-REST-API VERWENDEN 116
 - Swift REST API verwenden (veraltet) 252

Nutzung von StorageGRID Mandanten und Clients

Verwenden Sie ein Mandantenkonto

Verwenden Sie ein Mandantenkonto: Überblick

Ein Mandantenkonto ermöglicht Ihnen, entweder die Simple Storage Service (S3) REST-API oder die Swift REST-API zu verwenden, um Objekte in einem StorageGRID System zu speichern und abzurufen.

Was ist ein Mandantenkonto?

Jedes Mandantenkonto verfügt über eigene föderierte bzw. lokale Gruppen, Benutzer, S3 Buckets oder Swift Container und Objekte.

Mandantenkonten können verwendet werden, um gespeicherte Objekte durch verschiedene Einheiten zu trennen. Beispielsweise können für einen der folgenden Anwendungsfälle mehrere Mandantenkonten verwendet werden:

- **Anwendungsbeispiel für Unternehmen:** Wenn das StorageGRID-System innerhalb eines Unternehmens verwendet wird, kann der Objekt-Storage des Grid von den verschiedenen Abteilungen des Unternehmens getrennt werden. Beispielsweise können Mandantenkonten für die Marketingabteilung, die Kundenbetreuung, die Personalabteilung usw. vorhanden sein.



Wenn Sie das S3-Client-Protokoll verwenden, können Sie auch S3-Buckets und Bucket-Richtlinien verwenden, um Objekte zwischen den Abteilungen eines Unternehmens zu trennen. Sie müssen keine separaten Mandantenkonten erstellen. Siehe Anweisungen zur Implementierung "[S3-Buckets und Bucket-Richtlinien](#)" Finden Sie weitere Informationen.

- **Anwendungsfall des Service-Providers:** Wenn das StorageGRID-System von einem Service-Provider verwendet wird, kann der Objekt-Storage des Grid von den verschiedenen Einheiten getrennt werden, die den Storage leasen. Beispielsweise können Mandantenkonten für Unternehmen A, Unternehmen B, Unternehmen C usw. vorhanden sein.

Erstellen eines Mandantenkontos

Mandantenkonten werden von einem erstellt "[StorageGRID Grid-Administrator, der den Grid Manager verwendet](#)". Beim Erstellen eines Mandantenkontos gibt der Grid-Administrator Folgendes an:

- Grundlegende Informationen, einschließlich Mandantename, Client-Typ (S3 oder Swift) und optionalem Storage-Kontingent.
- Berechtigungen für das Mandantenkonto, z. B. ob das Mandantenkonto S3-Platformservices verwenden, seine eigene Identitätsquelle konfigurieren, S3 Select verwenden oder eine Grid-Verbundverbindung verwenden kann.
- Der erste Root-Zugriff für den Mandanten basiert darauf, ob das StorageGRID System lokale Gruppen und Benutzer, Identitätsföderation oder Single Sign On (SSO) verwendet.

Grid-Administratoren können zudem die S3-Objektsperreinstellung für das StorageGRID System aktivieren, wenn S3-Mandantenkonten die gesetzlichen Anforderungen erfüllen müssen. Wenn S3 Object Lock aktiviert

ist, können alle S3-Mandantenkonten konforme Buckets erstellen und managen.

S3-Mandanten konfigurieren

Nach einem ["S3-Mandantenkonto wird erstellt"](#), Sie können auf den Tenant Manager zugreifen, um Aufgaben wie die folgenden durchzuführen:

- Identitätsföderation einrichten (es sei denn, die Identitätsquelle wird mit dem Grid gemeinsam genutzt)
- Verwalten von Gruppen und Benutzern
- Grid-Verbund für Account-Klone und Grid-übergreifende Replizierung verwenden
- Managen von S3-Zugriffsschlüsseln
- S3 Buckets erstellen und managen
- Verwenden Sie S3-Plattformservices
- Verwenden Sie S3 Select
- Monitoring der Storage-Auslastung



Sie können S3-Buckets zwar mit dem Tenant Manager erstellen und managen, Sie müssen jedoch ein verwenden ["S3-Client"](#) Oder ["S3-Konsole"](#) Zum Einspielen und Verwalten von Objekten.

Konfigurieren Sie Swift Mandanten

Nach A ["Swift-Mandantenkonto wird erstellt"](#), Sie können auf den Tenant Manager zugreifen, um Aufgaben wie die folgenden durchzuführen:

- Identitätsföderation einrichten (es sei denn, die Identitätsquelle wird mit dem Grid gemeinsam genutzt)
- Verwalten von Gruppen und Benutzern
- Monitoring der Storage-Auslastung



Swift-Benutzer müssen über die Root-Zugriffsberechtigung für den Zugriff auf den Mandanten-Manager verfügen. Die Root-Zugriffsberechtigung erlaubt Benutzern jedoch nicht, sich beim zu authentifizieren ["Swift REST API"](#) Um Container zu erstellen und Objekte aufzunehmen. Benutzer müssen über die Swift-Administratorberechtigung verfügen, um sich bei der Swift-REST-API zu authentifizieren.

So melden Sie sich an und melden sich ab

Melden Sie sich bei Tenant Manager an

Sie greifen auf den Mandanten-Manager zu, indem Sie die URL für den Mandanten in die Adresszeile von A eingeben ["Unterstützter Webbrowser"](#).

Bevor Sie beginnen

- Sie haben Ihre Anmeldedaten.
- Sie verfügen über eine URL für den Zugriff auf den Mandanten-Manager, die vom Grid-Administrator bereitgestellt wird. Die URL sieht wie ein Beispiel aus:

```
https://FQDN_or_Admin_Node_IP/
```

`https://FQDN_or_Admin_Node_IP:port/`

`https://FQDN_or_Admin_Node_IP/?accountId=20-digit-account-id`

`https://FQDN_or_Admin_Node_IP:port/?accountId=20-digit-account-id`

Die URL enthält immer einen vollständig qualifizierten Domänennamen (FQDN), die IP-Adresse eines Admin-Knotens oder die virtuelle IP-Adresse einer HA-Gruppe von Admin-Knoten. Sie kann auch eine Portnummer, die 20-stellige Mandanten-Account-ID oder beides enthalten.

- Wenn die URL nicht die 20-stellige Konto-ID des Mandanten enthält, haben Sie diese Konto-ID.
- Sie verwenden ein ["Unterstützter Webbrowser"](#).
- Cookies sind in Ihrem Webbrowser aktiviert.
- Sie gehören einer Benutzergruppe an, die über verfügt ["Bestimmte Zugriffsberechtigungen"](#).

Schritte

1. Starten Sie A ["Unterstützter Webbrowser"](#).
2. Geben Sie in der Adressleiste des Browsers die URL für den Zugriff auf Tenant Manager ein.
3. Wenn Sie aufgefordert werden, eine Sicherheitswarnung zu erhalten, installieren Sie das Zertifikat mithilfe des Browser-Installationsassistenten.
4. Melden Sie sich beim Tenant Manager an.

Der angezeigte Anmeldebildschirm hängt von der eingegebenen URL und davon ab, ob Single Sign-On (SSO) für StorageGRID konfiguriert wurde.

SSO wird nicht verwendet

Wenn StorageGRID SSO nicht verwendet, wird einer der folgenden Bildschirme angezeigt:

- Die Anmeldeseite des Grid Manager. Wählen Sie den Link **Tenant Sign-in**.



NetApp StorageGRID®

Grid Manager

Username

Password

[Sign in](#)

[Tenant sign in](#) | [NetApp support](#) | [NetApp.com](#)

- Die Anmeldeseite von Tenant Manager. Das Feld **Account** ist möglicherweise bereits ausgefüllt, wie unten gezeigt.

NetApp StorageGRID®

Tenant Manager

Recent

-- Optional --

Account

64600207336181242061

Username

|

Password

Sign in

[NetApp support](#) | [NetApp.com](#)

- i. Wenn die 20-stellige Konto-ID des Mandanten nicht angezeigt wird, wählen Sie den Namen des Mandantenkontos aus, wenn er in der Liste der letzten Konten angezeigt wird, oder geben Sie die Konto-ID ein.
- ii. Geben Sie Ihren Benutzernamen und Ihr Kennwort ein.
- iii. Wählen Sie **Anmelden**.

Das Dashboard von Tenant Manager wird angezeigt.

- iv. Wenn Sie ein erstes Passwort von einer anderen Person erhalten haben, wählen Sie **username > Passwort ändern**, um Ihr Konto zu sichern.

SSO wird verwendet

Wenn StorageGRID SSO verwendet, wird einer der folgenden Bildschirme angezeigt:

- Die SSO-Seite Ihres Unternehmens. Beispiel:

Sign in with your organizational account

Geben Sie Ihre Standard-SSO-Anmeldeinformationen ein, und wählen Sie **Anmelden**.

- Die SSO-Anmeldeseite für den Tenant Manager.
 - i. Wenn die 20-stellige Konto-ID des Mandanten nicht angezeigt wird, wählen Sie den Namen des Mandantenkontos aus, wenn er in der Liste der letzten Konten angezeigt wird, oder geben Sie die Konto-ID ein.
 - ii. Wählen Sie **Anmelden**.
 - iii. Melden Sie sich mit Ihren Standard-SSO-Anmeldedaten auf der SSO-Anmeldeseite Ihres Unternehmens an.

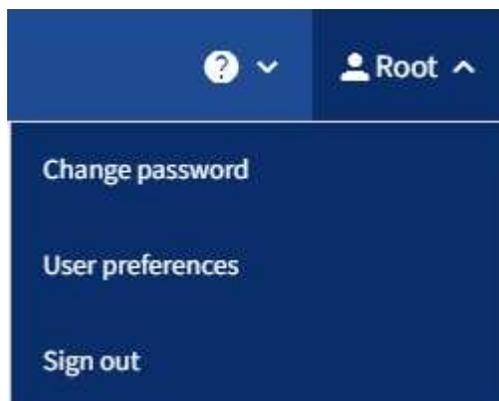
Das Dashboard von Tenant Manager wird angezeigt.

Melden Sie sich von Tenant Manager ab

Wenn Sie die Arbeit mit dem Mandantenmanager abgeschlossen haben, müssen Sie sich abmelden, um sicherzustellen, dass nicht autorisierte Benutzer nicht auf das StorageGRID-System zugreifen können. Wenn Sie Ihren Browser schließen, werden Sie möglicherweise aufgrund der Cookie-Einstellungen des Browsers nicht aus dem System abgesendet.

Schritte

1. Suchen Sie das Dropdown-Menü Benutzername in der oberen rechten Ecke der Benutzeroberfläche.



2. Wählen Sie den Benutzernamen und dann **Abmelden**.

- Wenn SSO nicht verwendet wird:

Sie sind vom Admin-Knoten abgemeldet. Die Anmeldeseite für den Mandanten-Manager wird angezeigt.



Wenn Sie sich bei mehr als einem Admin-Node angemeldet haben, müssen Sie sich von jedem Knoten abmelden.

- Wenn SSO aktiviert ist:

Sie sind von allen Admin-Knoten abgemeldet, auf die Sie zugreifen konnten. Die Seite StorageGRID-Anmeldung wird angezeigt. Der Name des Mietkontos, auf das Sie gerade zugegriffen haben, wird als Standard im Dropdown-Menü **Letzte Konten** angegeben, und die **Konto-ID** des Mieters wird angezeigt.



Wenn SSO aktiviert ist und Sie sich auch beim Grid Manager angemeldet haben, müssen Sie sich auch vom Grid Manager abmelden, um sich von SSO abzumelden.

Mandantenmanager-Dashboard verstehen

Das Tenant Manager-Dashboard bietet einen Überblick über die Konfiguration eines Mandantenkontos und die Menge an Speicherplatz, die von Objekten in den Buckets (S3) oder Containern (Swift) verwendet wird. Wenn der Mandant über ein Kontingent verfügt, wird im Dashboard angezeigt, wie viel des Kontingents verwendet wird und wie viel übrig bleibt. Wenn Fehler im Zusammenhang mit dem Mandantenkonto auftreten, werden die Fehler auf dem Dashboard angezeigt.



Die Werte für den genutzten Speicherplatz sind Schätzungen. Diese Schätzungen sind vom Zeitpunkt der Aufnahme, der Netzwerkverbindung und des Node-Status betroffen.

Wenn Objekte hochgeladen wurden, sieht das Dashboard wie das folgende Beispiel aus:

Dashboard

16 Buckets
View buckets

2 Platform services endpoints
View endpoints

0 Groups
View groups

1 User
View users

Storage usage [?](#)

6.5 TB of 7.2 TB used

0.7 TB (10.1%) remaining



Bucket name	Space used	Number of objects
Bucket-15	969.2 GB	913,425
Bucket-04	937.2 GB	576,806
Bucket-13	815.2 GB	957,389
Bucket-06	812.5 GB	193,843
Bucket-10	473.9 GB	583,245
Bucket-03	403.2 GB	981,226
Bucket-07	362.5 GB	420,726
Bucket-05	294.4 GB	785,190
8 other buckets	1.4 TB	3,007,036

Total objects

8,418,886
objects

Tenant details [?](#)

Name: Tenant02
ID: 3341 1240 0546 8283 2208
 Platform services enabled
 Can use own identity source
 S3 Select enabled

Zusammenfassung des Mandantenkontos

Oben im Dashboard sind die folgenden Informationen enthalten:

- Die Anzahl der konfigurierten Buckets oder Container, Gruppen und Benutzer
- Die Anzahl der Endpunkte von Plattformservices, falls vorhanden

Sie können die Links auswählen, um die Details anzuzeigen.

Auf der rechten Seite des Dashboards sind folgende Informationen enthalten:

- Die Gesamtzahl der Objekte für den Mandanten.

Wenn für ein S3-Konto keine Objekte aufgenommen wurden und Sie über den verfügen "[Root-Zugriffsberechtigung](#)", Erste Startrichtlinien werden anstelle der Gesamtanzahl der Objekte angezeigt.

- Mandantendetails, einschließlich des Mandantenkontonamens und der ID und der Frage, ob der Mandant verwendet werden kann "[Plattform-Services](#)", "[Seine eigene Identitätsquelle](#)", "[Grid-Verbund](#)", Oder "[S3 Select](#)" (Es werden nur die aktivierten Berechtigungen aufgelistet.)

Storage- und Kontingentnutzung

Das Fenster Speichernutzung enthält die folgenden Informationen:

- Die Menge der Objektdaten für den Mandanten.



Dieser Wert gibt die Gesamtanzahl der hochgeladenen Objektdaten an und stellt nicht den Speicherplatz dar, der zum Speichern der Kopien dieser Objekte und ihrer Metadaten verwendet wird.

- Wenn ein Kontingent festgelegt ist, ist die Gesamtmenge an Speicherplatz, der für Objektdaten verfügbar ist, sowie die Menge und der Prozentsatz des verbleibenden Speicherplatzes. Der Kontingentnutzer beschränkt die Menge der Objektdaten, die aufgenommen werden können.



Die Quotennutzung basiert auf internen Schätzungen und kann in einigen Fällen überschritten werden. StorageGRID überprüft beispielsweise das Kontingent, wenn ein Mandant beginnt, Objekte hochzuladen und neue Einlässe zurückweist, wenn der Mieter die Quote überschritten hat. StorageGRID berücksichtigt jedoch bei der Bestimmung, ob das Kontingent überschritten wurde, nicht die Größe des aktuellen Uploads. Wenn Objekte gelöscht werden, kann ein Mandant vorübergehend daran gehindert werden, neue Objekte hochzuladen, bis die Kontingentnutzung neu berechnet wird. Berechnungen der Kontingentnutzung können 10 Minuten oder länger dauern.

- Ein Balkendiagramm, das die relative Größe der größten Buckets oder Container darstellt.

Sie können den Mauszeiger über eines der Diagrammsegmente platzieren, um den gesamten Speicherplatz anzuzeigen, der von diesem Bucket oder Container verbraucht wird.



- Zur Übereinstimmung mit dem Balkendiagramm, eine Liste der größten Buckets oder Container, einschließlich der Gesamtzahl der Objektdaten und der Anzahl der Objekte für jeden Bucket oder Container.

Bucket name	Space used	Number of objects
Bucket-02	944.7 GB	7,575
Bucket-09	899.6 GB	589,677
Bucket-15	889.6 GB	623,542
Bucket-06	846.4 GB	648,619
Bucket-07	730.8 GB	808,655
Bucket-04	700.8 GB	420,493
Bucket-11	663.5 GB	993,729
Bucket-03	656.9 GB	379,329
9 other buckets	2.3 TB	5,171,588

Wenn ein Mandant mehr als neun Buckets oder Container enthält, werden alle anderen Buckets oder Container zu einem Eintrag im unteren Teil der Liste zusammengefasst.



Um die Einheiten für die im Tenant Manager angezeigten Speicherwerte zu ändern, wählen Sie oben rechts im Tenant Manager das Benutzer-Dropdown aus, und wählen Sie dann **Benutzereinstellungen** aus.

Warnmeldungen zur Kontingentnutzung

Wenn im Grid Manager Warnmeldungen zur Kontingentnutzung aktiviert wurden, werden diese im Mandanten-Manager angezeigt, wenn das Kontingent niedrig oder überschritten ist, wie folgt:

Wenn 90% oder mehr der Quote eines Mandanten verwendet wurden, wird die Meldung **Tenant Quotenverbrauch hoch** ausgelöst. Führen Sie die empfohlenen Aktionen für die Warnmeldung aus.

 Only 0.6% of the quota is remaining. If the quota is exceeded, you can no longer upload new objects.

Wenn Sie Ihre Quote überschreiten, können Sie keine neuen Objekte hochladen.

 The quota has been met. You cannot upload new objects.

Endpunktfehler

Wenn Sie mit Grid Manager einen oder mehrere Endpunkte für die Verwendung mit Plattformdiensten konfiguriert haben, zeigt das Tenant Manager-Dashboard eine Warnmeldung an, wenn in den letzten sieben Tagen Endpunktfehler aufgetreten sind.

 One or more endpoints have experienced an error and might not be functioning properly. Go to the [Endpoints](#) page to view the error details. The last error occurred 2 hours ago.

Um Details über anzuzeigen "[Fehler am Endpunkt der Plattformdienste](#)" Wählen Sie **Endpoints**, um die Seite Endpoints anzuzeigen.

Mandantenmanagement-API

Mandantenmanagement-API verstehen

Sie können Systemmanagementaufgaben mit der REST-API für das Mandantenmanagement anstelle der Mandantenmanager-Benutzeroberfläche ausführen. Möglicherweise möchten Sie beispielsweise die API zur Automatisierung von Vorgängen verwenden oder mehrere Einheiten, wie beispielsweise Benutzer, schneller erstellen.

Die Mandantenmanagement-API:

- Verwendet die Open Source API-Plattform von Swagger. Swagger bietet eine intuitive Benutzeroberfläche, über die Entwickler und nicht-Entwickler mit der API interagieren können. Die Swagger-Benutzeroberfläche bietet vollständige Details und Dokumentation für jeden API-Vorgang.
- Verwendet "[Versionierung zur Unterstützung unterbrechungsfreier Upgrades](#)".

So greifen Sie auf die Swagger-Dokumentation für die Mandantenmanagement-API zu:

1. Melden Sie sich beim Tenant Manager an.
2. Wählen Sie oben im Tenant Manager das Hilfesymbol aus und wählen Sie **API-Dokumentation**.

API-Betrieb

Die Mandantenmanagement-API organisiert die verfügbaren API-Vorgänge in die folgenden Abschnitte:

- **Account:** Operationen auf dem aktuellen Mandantenkonto, einschließlich der Speichernutzung Informationen.
- **Auth:** Operationen zur Authentifizierung der Benutzersitzung.

Die Mandantenmanagement-API unterstützt das Authentifizierungsschema für das Inhabertoken. Für eine Mandantenanmeldung geben Sie einen Benutzernamen, ein Passwort und eine Buchhaltungs-ID im JSON-Körper der Authentifizierungsanforderung (d. h. `POST /api/v3/authorize`). Wenn der Benutzer erfolgreich authentifiziert wurde, wird ein Sicherheitstoken zurückgegeben. Dieses Token muss im Header der nachfolgenden API-Anforderungen ("Authorization: Bearer Token") bereitgestellt werden.

Informationen zur Verbesserung der Authentifizierungssicherheit finden Sie unter "[Schützen Sie sich vor Cross-Site Request Forgery](#)".

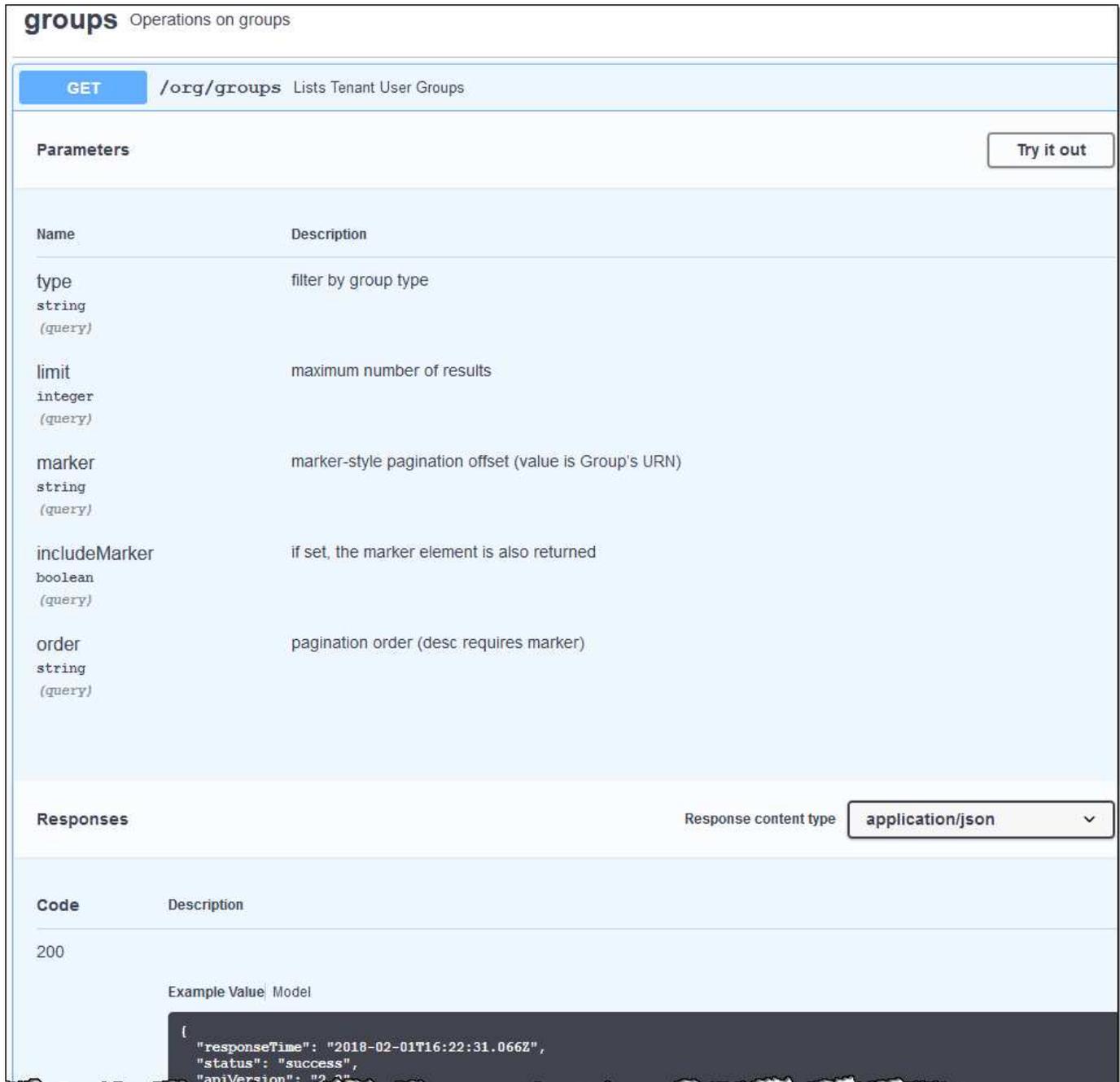


Wenn Single Sign-On (SSO) für das StorageGRID-System aktiviert ist, müssen Sie zur Authentifizierung verschiedene Schritte durchführen. Siehe "[Anweisungen zur Verwendung der Grid Management API](#)".

- **Config:** Operationen im Zusammenhang mit der Produktversion und den Versionen der Mandantenmanagement-API. Sie können die Produktversion und die Hauptversionen der von dieser Version unterstützten API auflisten.
- **Container:** Operationen auf S3 Buckets oder Swift Containern.
- **Deactivated-Features:** Operationen zum Anzeigen von Features, die möglicherweise deaktiviert wurden.
- **Endpunkte:** Operationen zur Verwaltung eines Endpunkts. Endpunkte ermöglichen es einem S3-Bucket, einen externen Service für die Replizierung, Benachrichtigungen oder Suchintegration von StorageGRID CloudMirror zu verwenden.
- **Grid-Federation-connections:** Operationen auf Grid Federation-Verbindungen und Cross-Grid-Replikation.
- **Groups:** Operationen zur Verwaltung lokaler Mandantengruppen und zum Abrufen verbundener Mandantengruppen aus einer externen Identitätsquelle.
- **Identity-source:** Operationen zum Konfigurieren einer externen Identitätsquelle und zum manuellen Synchronisieren von föderierten Gruppen- und Benutzerinformationen.
- **ilm:** Operationen zu Information Lifecycle Management (ILM) Einstellungen.
- **Regionen:** Operationen, um zu bestimmen, welche Regionen für das StorageGRID-System konfiguriert wurden.
- **s3:** Operationen zur Verwaltung von S3-Zugriffsschlüsseln für Mandantenbenutzer.
- **s3-Object-Lock:** Operationen auf globalen S3 Object Lock-Einstellungen, die zur Unterstützung der Einhaltung gesetzlicher Vorschriften verwendet werden.
- **Benutzer:** Operationen zum Anzeigen und Verwalten von Mandantenbenutzern.

Betriebsdetails

Wenn Sie die einzelnen API-Operationen erweitern, können Sie die HTTP-Aktion, die Endpunkt-URL, eine Liste aller erforderlichen oder optionalen Parameter, ein Beispiel des Anforderungskörpers (falls erforderlich) und die möglichen Antworten sehen.



groups Operations on groups

GET /org/groups Lists Tenant User Groups

Parameters Try it out

Name	Description
type string (query)	filter by group type
limit integer (query)	maximum number of results
marker string (query)	marker-style pagination offset (value is Group's URN)
includeMarker boolean (query)	if set, the marker element is also returned
order string (query)	pagination order (desc requires marker)

Responses Response content type: application/json

Code	Description
200	

Example Value | Model

```
{
  "responseTime": "2018-02-01T16:22:31.066Z",
  "status": "success",
  "apiVersion": "2.3"
}
```

API-Anforderungen ausgeben



Alle API-Operationen, die Sie mit der API Docs Webseite durchführen, sind Live-Operationen. Achten Sie darauf, dass Konfigurationsdaten oder andere Daten nicht versehentlich erstellt, aktualisiert oder gelöscht werden.

Schritte

1. Wählen Sie die HTTP-Aktion aus, um die Anfragedetails anzuzeigen.

2. Stellen Sie fest, ob für die Anforderung zusätzliche Parameter erforderlich sind, z. B. eine Gruppe oder eine Benutzer-ID. Dann erhalten Sie diese Werte. Sie müssen möglicherweise zuerst eine andere API-Anfrage stellen, um die Informationen zu erhalten, die Sie benötigen.
3. Bestimmen Sie, ob Sie den Text für die Beispielanforderung ändern müssen. In diesem Fall können Sie **Modell** wählen, um die Anforderungen für jedes Feld zu erfahren.
4. Wählen Sie **Probieren Sie es aus**.
5. Geben Sie alle erforderlichen Parameter ein, oder ändern Sie den Anforderungskörper nach Bedarf.
6. Wählen Sie **Ausführen**.
7. Überprüfen Sie den Antwortcode, um festzustellen, ob die Anfrage erfolgreich war.

Mandantenmanagement-API-Versionierung

Die Mandanten-Management-API verwendet Versionierung zur Unterstützung unterbrechungsfreier Upgrades.

Diese Anforderungs-URL gibt beispielsweise die Version 4 der API an.

`https://hostname_or_ip_address/api/v4/authorize`

Die Hauptversion der API wird bei Änderungen, die *nicht kompatibel* mit älteren Versionen sind, angestoßen. Die Minor-Version der API wird bei Änderungen, die *kompatibel* mit älteren Versionen gemacht werden, angestoßen. Zu den kompatiblen Änderungen gehört das Hinzufügen neuer Endpunkte oder neuer Eigenschaften.

Das folgende Beispiel zeigt, wie die API-Version basierend auf dem Typ der vorgenommenen Änderungen angestoßen wird.

Typ der Änderung in API	Alte Version	Neue Version
Kompatibel mit älteren Versionen	2.1	2.2
Nicht kompatibel mit älteren Versionen	2.1	3.0

Wenn Sie die StorageGRID-Software zum ersten Mal installieren, wird nur die neueste Version der API aktiviert. Wenn Sie jedoch ein Upgrade auf eine neue Funktionsversion von StorageGRID durchführen, haben Sie weiterhin Zugriff auf die ältere API-Version für mindestens eine StorageGRID-Funktionsversion.



Sie können die unterstützten Versionen konfigurieren. Siehe den Abschnitt **config** der Dokumentation zur Swagger API für das ["Grid Management API"](#). Finden Sie weitere Informationen. Sie sollten die Unterstützung für die ältere Version deaktivieren, nachdem Sie alle API-Clients aktualisiert haben, um die neuere Version zu verwenden.

Veraltete Anfragen werden wie folgt als veraltet markiert:

- Der Antwortkopf ist "Deprecated: True"
- Der JSON-Antwortkörper enthält „veraltet“: Wahr
- Eine veraltete Warnung wird nms.log hinzugefügt. Beispiel:

```
Received call to deprecated v2 API at POST "/api/v2/authorize"
```

Legen Sie fest, welche API-Versionen in der aktuellen Version unterstützt werden

Verwenden Sie die `GET /versions` API-Anforderung zur Rückgabe einer Liste der unterstützten API-Hauptversionen. Diese Anfrage befindet sich im Abschnitt **config** der Swagger API-Dokumentation.

```
GET https://{{IP-Address}}/api/versions
{
  "responseTime": "2023-06-27T22:13:50.750Z",
  "status": "success",
  "apiVersion": "4.0",
  "data": [
    2,
    3,
    4
  ]
}
```

Geben Sie eine API-Version für eine Anforderung an

Sie können die API-Version mithilfe eines Pfadparameters angeben (`/api/v4`) Oder eine Kopfzeile (`Api-Version: 4`). Wenn Sie beide Werte angeben, überschreibt der Kopfzeilenwert den Pfadwert.

```
curl https://[IP-Address]/api/v4/grid/accounts

curl -H "Api-Version: 4" https://[IP-Address]/api/grid/accounts
```

Schutz vor standortübergreifenden Anfrageschmieden (CSRF)

Sie können mithilfe von CSRF-Tokens die Authentifizierung verbessern, die Cookies verwendet, um Angriffe auf Cross-Site Request Forgery (CSRF) gegen StorageGRID zu schützen. Grid Manager und Tenant Manager aktivieren diese Sicherheitsfunktion automatisch; andere API-Clients können wählen, ob sie aktiviert werden sollen, wenn sie sich anmelden.

Ein Angreifer, der eine Anfrage an eine andere Website auslösen kann (z. B. mit einem HTTP-FORMULARPOST), kann dazu führen, dass bestimmte Anfragen mithilfe der Cookies des angemelden Benutzers erstellt werden.

StorageGRID schützt mit CSRF-Tokens vor CSRF-Angriffen. Wenn diese Option aktiviert ist, muss der Inhalt eines bestimmten Cookies mit dem Inhalt eines bestimmten Kopfes oder eines bestimmten POST-Body-Parameters übereinstimmen.

Um die Funktion zu aktivieren, stellen Sie die ein `csrfToken` Parameter an `true` Während der

Authentifizierung. Die Standardeinstellung lautet `false`.

```
curl -X POST --header "Content-Type: application/json" --header "Accept: application/json" -d "{
  \"username\": \"MyUserName\",
  \"password\": \"MyPassword\",
  \"cookie\": true,
  \"csrfToken\": true
}" "https://example.com/api/v3/authorize"
```

Wenn wahr, A `GridCsrfToken` Cookies werden mit einem zufälligen Wert für die Anmeldung bei Grid Manager und dem gesetzt `AccountCsrfToken` Cookie wird mit einem zufälligen Wert für die Anmeldung bei Tenant Manager gesetzt.

Wenn das Cookie vorhanden ist, müssen alle Anforderungen, die den Status des Systems (POST, PUT, PATCH, DELETE) ändern können, eine der folgenden Optionen enthalten:

- Der `X-Csrf-Token` Kopfzeile, wobei der Wert der Kopfzeile auf den Wert des CSRF-Token-Cookies gesetzt ist.
- Für Endpunkte, die einen formcodierten Körper annehmen: A `csrfToken` Formularkodierung für den Anforderungskörperparameter.

Verwenden Sie zum Konfigurieren des CSRF-Schutzes die ["Grid Management API"](#) Oder ["Mandantenmanagement-API"](#).



Anforderungen, die ein CSRF-Token-Cookie gesetzt haben, erzwingen auch den `"Content-Type: Application/json"`-Header für jede Anforderung, die einen JSON-Request-Body als zusätzlichen Schutz gegen CSRF-Angriffe erwartet.

Netzverbundverbindungen verwenden

Klonen von Mandantengruppen und Benutzern

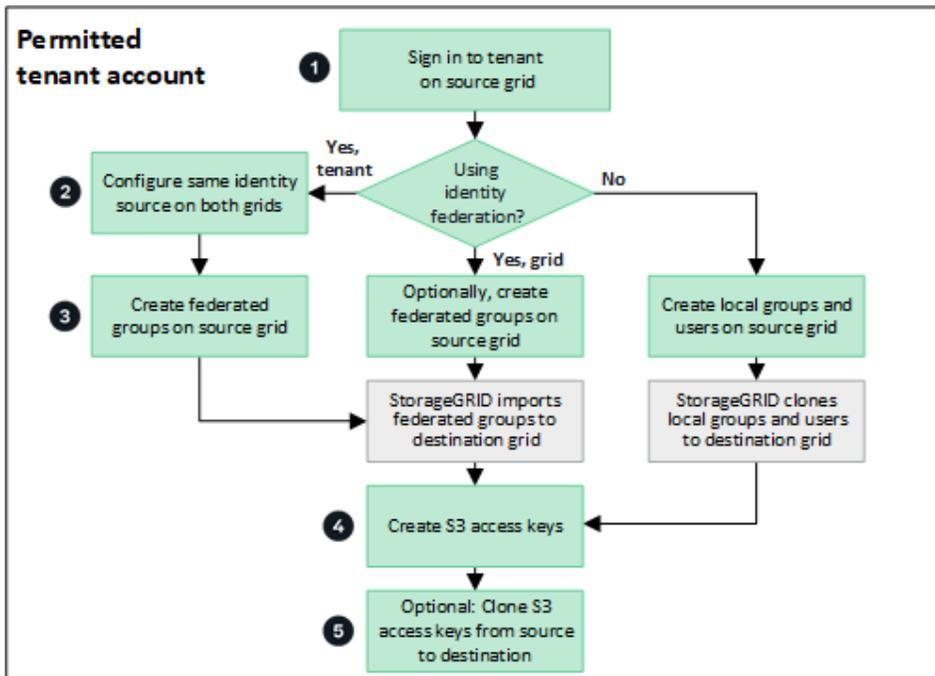
Wenn ein Mandant zur Verwendung einer Grid-Verbundverbindung erstellt oder bearbeitet wurde, wird dieser Mandant von einem StorageGRID System (dem Quellmandanten) auf ein anderes StorageGRID System (dem Replikatmandanten) repliziert. Nach der Replizierung des Mandanten werden alle Gruppen und Benutzer, die dem Quellmandanten hinzugefügt wurden, dem Replikatmandanten geklont.

Das StorageGRID-System, auf dem der Tenant ursprünglich erstellt wurde, ist das *source Grid* des Tenants. Das StorageGRID-System, auf dem der Mandant repliziert wird, ist das *Destination Grid* des Mandanten. Beide Mandantenkonten haben die gleiche Konto-ID, den gleichen Namen, eine Beschreibung, das gleiche Storage-Kontingent und die gleichen Berechtigungen, Der Zielmandant verfügt jedoch zunächst nicht über ein Root-Benutzerpasswort. Weitere Informationen finden Sie unter ["Was ist Account-Klon"](#) Und ["Management zulässiger Mandanten"](#).

Das Klonen von Mandantenkontoinformationen ist für erforderlich ["Grid-übergreifende Replizierung"](#) Von Bucket-Objekten. Durch die Verwendung derselben Mandantengruppen und Benutzer in beiden Grids können Sie auf die entsprechenden Buckets und Objekte in beiden Grids zugreifen.

Mandanten-Workflow für Account-Klon

Wenn Ihr Mandantenkonto über die Berechtigung **Grid Federation connection** verwenden verfügt, sehen Sie sich im Workflow-Diagramm die Schritte an, die Sie zum Klonen von Gruppen, Benutzern und S3-Zugriffsschlüsseln durchführen werden.



Das sind die primären Schritte im Workflow:

1

Melden Sie sich beim Mandanten an

Melden Sie sich beim Mandantenkonto im Quellraster an (dem Raster, in dem der Mandant ursprünglich erstellt wurde).

2

Optional können Sie die Identity Federation konfigurieren

Wenn Ihr Mandantenkonto über die Berechtigung **eigene Identitätsquelle verwenden** verfügt, um verbundene Gruppen und Benutzer zu verwenden, konfigurieren Sie die gleiche Identitätsquelle (mit den gleichen Einstellungen) für die Quell- und Zielmandanten-Konten. Föderierte Gruppen und Benutzer können nur geklont werden, wenn beide Grids dieselbe Identitätsquelle verwenden. Anweisungen hierzu finden Sie unter "[Verwenden Sie den Identitätsverbund](#)".

3

Erstellen Sie Gruppen und Benutzer

Wenn Sie Gruppen und Benutzer erstellen, beginnen Sie immer vom Quellraster des Mandanten. Wenn Sie eine neue Gruppe hinzufügen, klonst StorageGRID sie automatisch in das Zielraster.

- Wenn die Identity Federation für das gesamte StorageGRID System oder Ihr Mandantenkonto konfiguriert wurde, "[Erstellen neuer Mandantengruppen](#)" Durch Importieren föderierter Gruppen aus der Identitätsquelle.
- Wenn Sie keine Identitätsföderation verwenden, "[Erstellen Sie neue lokale Gruppen](#)" Und dann "[Erstellen](#)

Sie lokale Benutzer".

4

Erstellen von S3 Zugriffsschlüsseln

Das können Sie ["Erstellen Sie Ihre eigenen Zugriffsschlüssel"](#) Oder an ["Erstellen Sie die Zugriffsschlüssel eines anderen Benutzers"](#) Entweder im Quell- oder im Zielraster, um auf Buckets in diesem Grid zuzugreifen.

5

Optionales Klonen von S3-Zugriffsschlüsseln

Wenn Sie auf Buckets mit denselben Zugriffsschlüsseln in beiden Grids zugreifen müssen, erstellen Sie die Zugriffsschlüssel im Quellraster und klonen Sie sie dann manuell mit der Tenant Manager-API in das Zielraster. Anweisungen hierzu finden Sie unter ["Klonen von S3-Zugriffsschlüsseln mithilfe der API"](#).

Wie werden Gruppen, Benutzer und S3-Zugriffsschlüssel geklont?

Lesen Sie diesen Abschnitt, um zu erfahren, wie Gruppen, Benutzer und S3-Zugriffsschlüssel zwischen dem Mandanten-Quellraster und dem Mandanten-Zielraster geklont werden.

Lokale Gruppen, die im Quellraster erstellt wurden, werden geklont

Nachdem ein Mandantenkonto erstellt und in das Zielraster repliziert wurde, klonst StorageGRID automatisch alle lokalen Gruppen, die Sie dem Quell-Grid des Mandanten zum Zielraster des Mandanten hinzufügen.

Sowohl die ursprüngliche Gruppe als auch der zugehörige Klon weisen den gleichen Zugriffsmodus, die gleichen Gruppenberechtigungen und die S3-Gruppenrichtlinie auf. Anweisungen hierzu finden Sie unter ["Gruppen für S3 Mandanten erstellen"](#).



Alle Benutzer, die Sie beim Erstellen einer lokalen Gruppe im Quellraster auswählen, werden nicht berücksichtigt, wenn die Gruppe im Zielraster geklont wird. Wählen Sie aus diesem Grund keine Benutzer aus, wenn Sie die Gruppe erstellen. Wählen Sie stattdessen die Gruppe aus, wenn Sie die Benutzer erstellen.

Lokale Benutzer, die im Quellraster erstellt wurden, werden geklont

Wenn Sie einen neuen lokalen Benutzer im Quellraster erstellen, klonst StorageGRID diesen Benutzer automatisch in das Zielraster. Sowohl der ursprüngliche Benutzer als auch sein Klon haben den gleichen vollständigen Namen, Benutzernamen und die gleiche Einstellung für **Zugriff verweigern**. Beide Benutzer gehören ebenfalls zu den gleichen Gruppen. Anweisungen hierzu finden Sie unter ["Managen Sie lokale Benutzer"](#).

Aus Sicherheitsgründen werden lokale Benutzerpasswörter nicht im Zielraster geklont. Wenn ein lokaler Benutzer im Zielraster auf Tenant Manager zugreifen muss, muss der Root-Benutzer des Mandantenkontos ein Kennwort für diesen Benutzer im Zielraster hinzufügen. Anweisungen hierzu finden Sie unter ["Managen Sie lokale Benutzer"](#).

Im Quellraster erstellte Verbundgruppen werden geklont

Angenommen, die Anforderungen für die Verwendung von Account Clone mit werden angenommen ["Single Sign On"](#) Und ["Identitätsföderation"](#) Zusammengetragen wurden, werden gebündelte Gruppen, die Sie für den Mandanten im Quellraster erstellen (importieren), automatisch auf den Mandanten im Zielraster geklont.

Beide Gruppen verfügen über denselben Zugriffsmodus, dieselben Gruppenberechtigungen und dieselbe S3-Gruppenrichtlinie.

Nachdem für den Quellmandanten gebündelte Gruppen erstellt und für den Zielmandanten geklont wurden, können sich föderierte Benutzer in beiden Grids beim Mandanten anmelden.

S3-Zugriffsschlüssel können manuell geklont werden

StorageGRID klonet S3-Zugriffsschlüssel nicht automatisch, da die Sicherheit durch unterschiedliche Schlüssel auf jedem Grid verbessert wird.

Zum Verwalten der Zugriffsschlüssel in den beiden Grids haben Sie folgende Möglichkeiten:

- Wenn Sie nicht die gleichen Tasten für jedes Raster verwenden müssen, können Sie ["Erstellen Sie Ihre eigenen Zugriffsschlüssel"](#) Oder ["Erstellen Sie die Zugriffsschlüssel eines anderen Benutzers"](#) Auf jedem Raster.
- Wenn Sie dieselben Schlüssel auf beiden Rastern verwenden müssen, können Sie Schlüssel im Quellraster erstellen und dann die Tenant Manager-API manuell verwenden ["Schlüssel klonen"](#) Zum Zielraster.



Wenn Sie S3-Zugriffsschlüssel für einen föderierten Benutzer klonen, werden sowohl der Benutzer als auch die S3-Zugriffsschlüssel zum Zielmandanten geklont.

Gruppen und Benutzer, die dem Zielraster hinzugefügt wurden, sind nicht geklont

Das Klonen erfolgt nur vom Quell-Grid des Mandanten zum Ziel-Grid des Mandanten. Wenn Sie Gruppen und Benutzer im Zielraster des Mandanten erstellen oder importieren, werden diese Elemente von StorageGRID nicht im Quellraster des Mandanten geklont.

Bearbeitete oder gelöschte Gruppen, Benutzer und Zugriffsschlüssel werden nicht geklont

Das Klonen erfolgt nur, wenn Sie neue Gruppen und Benutzer erstellen.

Wenn Sie Gruppen, Benutzer oder Zugriffsschlüssel in einer der beiden Raster bearbeiten oder löschen, werden die Änderungen nicht in der anderen Tabelle geklont.

Klonen von S3-Zugriffsschlüsseln mithilfe der API

Wenn Ihr Mandantenkonto über die Berechtigung **Grid Federation connection** verwenden verfügt, können Sie die Tenant Management API verwenden, um S3-Zugriffsschlüssel vom Mandanten im Quellraster manuell auf den Mandanten im Zielraster zu klonen.

Bevor Sie beginnen

- Das Mandantenkonto hat die Berechtigung **Grid Federation connection** verwenden.
- Die Netzverbundverbindung hat einen **Verbindungsstatus** von **Verbunden**.
- Sie sind mit einem beim Tenant Manager im Quellraster des Mandanten angemeldet ["Unterstützter Webbrowser"](#).

- Sie gehören einer Benutzergruppe an, die über den verfügt "[Managen Sie Ihre eigenen S3-Anmeldedaten oder Root-Zugriffsberechtigungen](#)".
- Wenn Sie Zugriffsschlüssel für einen lokalen Benutzer klonen, ist der Benutzer bereits in beiden Grids vorhanden.



Wenn Sie S3-Zugriffsschlüssel für einen föderierten Benutzer klonen, werden sowohl der Benutzer als auch die S3-Zugriffsschlüssel zum Zielmandanten hinzugefügt.

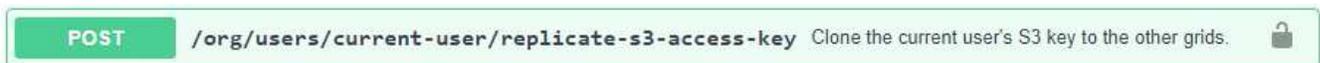
Eigene Zugriffsschlüssel klonen

Sie können Ihre eigenen Zugriffsschlüssel klonen, wenn Sie auf dieselben Buckets in beiden Rastern zugreifen müssen.

Schritte

1. Mithilfe des Tenant Manager im Quellraster "[Erstellen Sie Ihre eigenen Zugriffsschlüssel](#)" Und laden Sie die herunter .csv Datei:
2. Wählen Sie oben im Tenant Manager das Hilfesymbol aus und wählen Sie **API-Dokumentation**.
3. Wählen Sie im Abschnitt **s3** den folgenden Endpunkt aus:

POST /org/users/current-user/replicate-s3-access-key



4. Wählen Sie **Probieren Sie es aus**.
5. Ersetzen Sie im Textfeld **body** die Beispieleinträge für **accesskey** und **secretAccessKey** durch die Werte aus der heruntergeladenen .csv-Datei.

Achten Sie darauf, dass die doppelten Anführungszeichen um jede Zeichenfolge herum beibehalten werden.



6. Wenn der Schlüssel abläuft, ersetzen Sie den Beispieleintrag für **expires** durch das Ablaufdatum und die Zeit als String im ISO 8601-Datenzeitformat (z. B. 2024-02-28T22:46:33-08:00). Wenn der Schlüssel nicht abläuft, geben Sie **null** als Wert für den Eintrag **expires** ein (oder entfernen Sie die Zeile **expires** und das vorangegangene Komma).
7. Wählen Sie **Ausführen**.
8. Bestätigen Sie, dass der Server-Antwortcode **204** lautet, was darauf hinweist, dass der Schlüssel erfolgreich in das Zielraster geklont wurde.

Die Zugriffsschlüssel eines anderen Benutzers klonen

Sie können die Zugriffsschlüssel eines anderen Benutzers klonen, wenn er auf dieselben Buckets in beiden Rastern zugreifen muss.

Schritte

1. Mithilfe des Tenant Manager im Quellraster "[Erstellen Sie die S3-Zugriffsschlüssel des anderen Benutzers](#)" Und laden Sie die herunter `.csv` Datei:
2. Wählen Sie oben im Tenant Manager das Hilfesymbol aus und wählen Sie **API-Dokumentation**.
3. Die Benutzer-ID abrufen. Sie benötigen diesen Wert, um die Zugriffsschlüssel des anderen Benutzers zu klonen.
 - a. Wählen Sie im Abschnitt **Users** den folgenden Endpunkt aus:

```
GET /org/users
```

- b. Wählen Sie **Probieren Sie es aus**.
 - c. Geben Sie alle Parameter an, die beim Suchen von Benutzern verwendet werden sollen.
 - d. Wählen Sie **Ausführen**.
 - e. Suchen Sie den Benutzer, dessen Schlüssel Sie klonen möchten, und kopieren Sie die Nummer in das Feld **id**.
4. Wählen Sie im Abschnitt **s3** den folgenden Endpunkt aus:

```
POST /org/users/{userId}/replicate-s3-access-key
```



5. Wählen Sie **Probieren Sie es aus**.
6. Fügen Sie im Textfeld **userid** die von Ihnen kopierte Benutzer-ID ein.
7. Ersetzen Sie im Textfeld **body** die Beispieleinträge für **example Access key** und **secret Access key** durch die Werte aus der `.csv`-Datei für diesen Benutzer.

Achten Sie darauf, dass die doppelten Anführungszeichen um die Zeichenfolge herum beibehalten werden.

8. Wenn der Schlüssel abläuft, ersetzen Sie den Beispieleintrag für **expires** durch das Ablaufdatum und die Zeit als String im ISO 8601-Datenzeitformat (z. B. `2023-02-28T22:46:33-08:00`). Wenn der Schlüssel nicht abläuft, geben Sie **null** als Wert für den Eintrag **expires** ein (oder entfernen Sie die Zeile **expires** und das vorangegangene Komma).
9. Wählen Sie **Ausführen**.
10. Bestätigen Sie, dass der Server-Antwortcode **204** lautet, was darauf hinweist, dass der Schlüssel erfolgreich in das Zielraster geklont wurde.

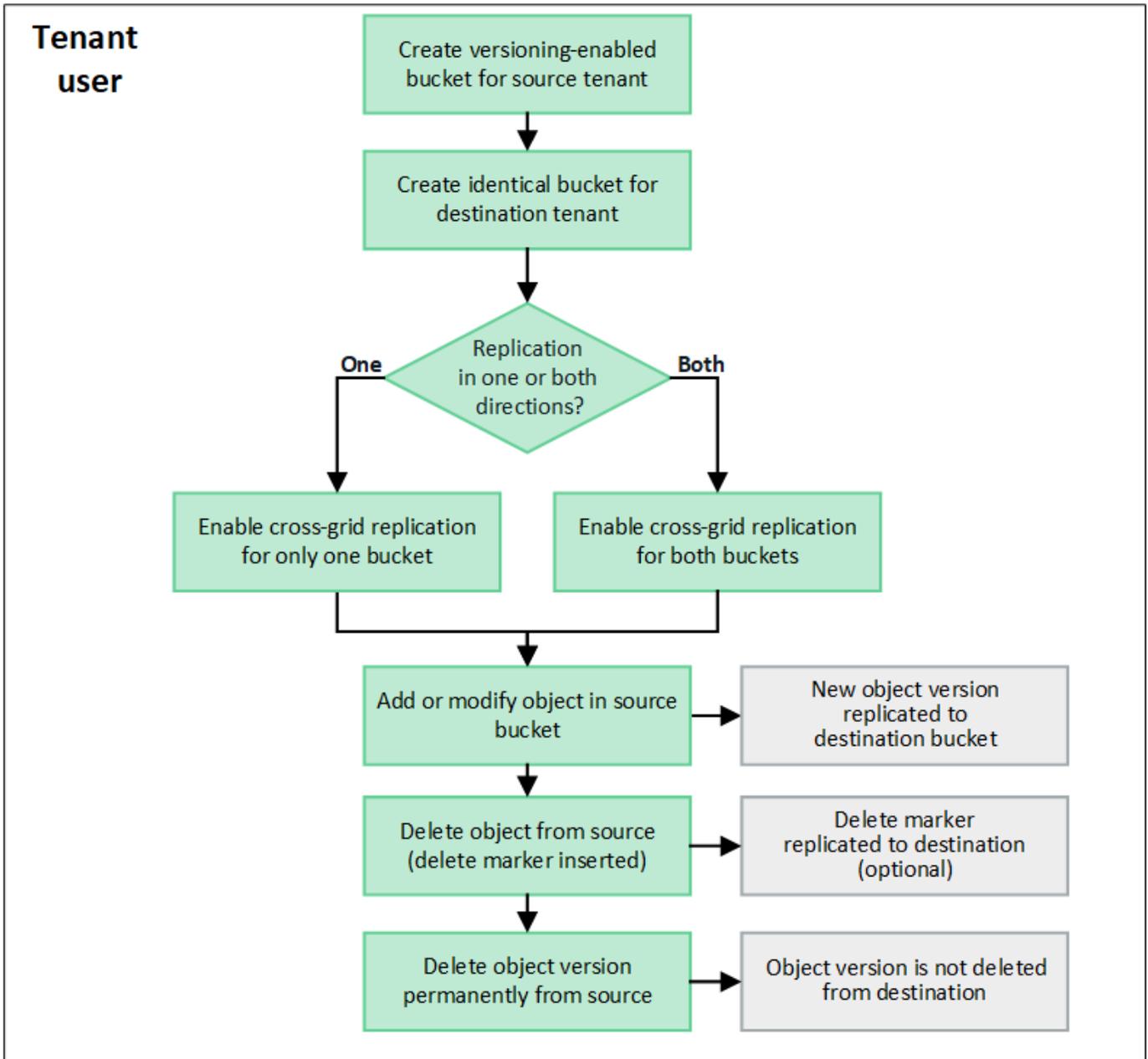
Grid-übergreifende Replizierung managen

Wenn Ihrem Mandantenkonto bei der Erstellung die Berechtigung **Grid Federation connection** zugewiesen wurde, können Sie mittels Grid-Replizierung automatisch Objekte zwischen Buckets im Quell-Grid des Mandanten und Buckets im

Zielraster des Mandanten replizieren. Die Grid-übergreifende Replizierung kann in eine oder beide Richtungen erfolgen.

Workflow für Grid-übergreifende Replizierung

Das Workflow-Diagramm fasst die Schritte zusammen, die Sie zur Konfiguration der Grid-übergreifenden Replikation zwischen Buckets in zwei Grids durchführen. Diese Schritte werden im Folgenden genauer beschrieben.



Konfiguration der Grid-übergreifenden Replizierung

Bevor Sie die Grid-übergreifende Replizierung verwenden können, müssen Sie sich bei den entsprechenden Mandantenkonten in jedem Grid anmelden und identische Buckets erstellen. Anschließend können Sie die Grid-übergreifende Replizierung für einen oder beide Buckets aktivieren.

Bevor Sie beginnen

- Sie haben die Anforderungen für die Grid-übergreifende Replizierung überprüft. Siehe "[Was ist Grid-übergreifende Replizierung](#)".
- Sie verwenden ein "[Unterstützter Webbrowser](#)".
- Das Mandantenkonto hat die Berechtigung **use Grid Federation connection**, und identische Mandantenkonten existieren auf beiden Grids. Siehe "[Verwalten Sie die zulässigen Mandanten für die Grid Federation-Verbindung](#)".
- Der Mandantenbenutzer, den Sie sich anmelden, da er bereits in beiden Rastern vorhanden ist, gehört zu einer Benutzergruppe, die über den verfügt "[Root-Zugriffsberechtigung](#)".
- Wenn Sie sich als lokaler Benutzer am Zielraster des Mandanten anmelden, hat der Stammbenutzer des Mandantenkontos ein Kennwort für Ihr Benutzerkonto in diesem Raster festgelegt.

Erstellen Sie zwei identische Buckets

Melden Sie sich als ersten Schritt bei den entsprechenden Mandantenkonten in jedem Grid an und erstellen Sie identische Buckets.

Schritte

1. Erstellen Sie ausgehend von einem der beiden Raster in der Grid Federation-Verbindung einen neuen Bucket:
 - a. Melden Sie sich mit den Anmeldeinformationen eines Mandantenbenutzers an, der in beiden Grids vorhanden ist.



Wenn Sie sich nicht als lokaler Benutzer am Zielraster des Mandanten anmelden können, bestätigen Sie, dass der Root-Benutzer für das Mandantenkonto ein Kennwort für Ihr Benutzerkonto festgelegt hat.

- b. Befolgen Sie die Anweisungen unter "[Erstellen eines S3-Buckets](#)".
 - c. Wählen Sie auf der Registerkarte **Objekteinstellungen verwalten Objektversionierung aktivieren**.
 - d. Wenn die S3-Objektsperre für Ihr StorageGRID-System aktiviert ist, aktivieren Sie nicht die S3-Objektsperre für den Bucket.
 - e. Wählen Sie **Eimer erstellen**.
 - f. Wählen Sie **Fertig**.
2. Wiederholen Sie diese Schritte, um einen identischen Bucket für dasselbe Mandantenkonto auf dem anderen Grid in der Grid-Federation-Verbindung zu erstellen.



Je nach Bedarf kann jeder Bucket einen anderen Bereich verwenden.

Grid-übergreifende Replizierung

Sie müssen diese Schritte ausführen, bevor Sie Objekte zu einem Bucket hinzufügen.

Schritte

1. Aktivieren Sie, beginnend mit einem Raster, dessen Objekte Sie replizieren möchten "[Grid-übergreifende Replizierung in eine Richtung](#)":
 - a. Melden Sie sich beim Mandantenkonto für den Bucket an.
 - b. Wählen Sie **View Buckets** aus dem Dashboard, oder wählen Sie **STORAGE (S3) > Buckets**.

- c. Wählen Sie den Bucket-Namen aus der Tabelle aus, um auf die Seite mit den Bucket-Details zuzugreifen.
- d. Wählen Sie die Registerkarte **Grid-Replikation** aus.
- e. Wählen Sie **enable**, und überprüfen Sie die Liste der Anforderungen.
- f. Wenn alle Anforderungen erfüllt sind, wählen Sie die zu verwendende Netzverbundverbindung aus.
- g. Optional können Sie die Einstellung **Replicate delete Markers** ändern, um festzustellen, was im Zielraster passiert, wenn ein S3-Client eine Löschanforderung an das Quellraster ausgibt, das keine Versions-ID enthält:
 - **Ja** (Standard): Ein Löschmarker wird zum Quell-Bucket hinzugefügt und in den Ziel-Bucket repliziert.
 - **Nein**: Eine Löschmarkierung wird dem Quell-Bucket hinzugefügt, wird aber nicht in den Ziel-Bucket repliziert.



Wenn die Löschanforderung eine Versions-ID enthält, wird diese Objektversion dauerhaft aus dem Quell-Bucket entfernt. StorageGRID repliziert Löschanforderungen, die eine Versions-ID enthalten, nicht, sodass dieselbe Objektversion nicht vom Ziel gelöscht wird.

Siehe "[Was ist Grid-übergreifende Replizierung](#)" Entsprechende Details.

- a. Ändern Sie optional die Einstellung der Audit-Kategorie **Grid-übergreifende Replikation**, um das Volumen der Audit-Nachrichten zu verwalten:
 - **Error** (Standard): Nur fehlgeschlagene Cross-Grid-Replikationsanforderungen sind in der Audit-Ausgabe enthalten.
 - **Normal**: Alle Grid-übergreifenden Replikationsanfragen sind enthalten, was das Volumen der Audit-Ausgabe erheblich erhöht.
- b. Überprüfen Sie Ihre Auswahl. Sie können diese Einstellungen nur ändern, wenn beide Buckets leer sind.
- c. Wählen Sie **Enable und Test**.

Nach einigen Augenblicken wird eine Erfolgsmeldung angezeigt. Objekte, die diesem Bucket hinzugefügt wurden, werden nun automatisch in das andere Grid repliziert. **Grid-übergreifende Replikation** wird als aktivierte Funktion auf der Bucket-Detailseite angezeigt.

2. Gehen Sie optional zum entsprechenden Bucket auf dem anderen Raster und "[Aktivieren Sie die Grid-übergreifende Replizierung in beide Richtungen](#)".

Testen Sie die Replikation zwischen Grids

Wenn die Grid-übergreifende Replizierung für einen Bucket aktiviert ist, müssen Sie möglicherweise überprüfen, ob die Verbindung und die Grid-übergreifende Replizierung ordnungsgemäß funktionieren und dass die Quell- und Ziel-Buckets nach wie vor alle Anforderungen erfüllen (beispielsweise ist die Versionierung weiterhin aktiviert).

Bevor Sie beginnen

- Sie verwenden ein "[Unterstützter Webbrowser](#)".
- Sie gehören einer Benutzergruppe an, die über den verfügt "[Root-Zugriffsberechtigung](#)".

Schritte

1. Melden Sie sich beim Mandantenkonto für den Bucket an.
2. Wählen Sie **View Buckets** aus dem Dashboard, oder wählen Sie **STORAGE (S3) > Buckets**.
3. Wählen Sie den Bucket-Namen aus der Tabelle aus, um auf die Seite mit den Bucket-Details zuzugreifen.
4. Wählen Sie die Registerkarte **Grid-Replikation** aus.
5. Wählen Sie **Verbindung testen**.

Wenn die Verbindung in einem ordnungsgemäßen Zustand ist, wird ein Erfolgsbanner angezeigt. Andernfalls wird eine Fehlermeldung angezeigt, die Sie und der Grid-Administrator zur Behebung des Problems verwenden können. Weitere Informationen finden Sie unter "[Fehler beim Grid-Verbund beheben](#)".

6. Wenn die Grid-übergreifende Replikation in beide Richtungen konfiguriert ist, gehen Sie zum entsprechenden Bucket auf dem anderen Grid und wählen Sie **Verbindung testen** aus, um zu überprüfen, ob die Grid-übergreifende Replikation in die andere Richtung funktioniert.

Deaktivieren Sie die Grid-übergreifende Replizierung

Sie können die Grid-übergreifende Replikation dauerhaft beenden, wenn Sie keine Objekte mehr in das andere Raster kopieren möchten.

Beachten Sie vor dem Deaktivieren der Grid-übergreifenden Replikation Folgendes:

- Durch die Deaktivierung der Grid-übergreifenden Replikation werden keine Objekte entfernt, die bereits zwischen den Rastern kopiert wurden. Beispiel: Objekte in `my-bucket` In Raster 1, die in `my-bucket` In Grid 2 kopiert wurden, werden nicht entfernt, wenn Sie die Grid-übergreifende Replizierung für diesen Bucket deaktivieren. Wenn Sie diese Objekte löschen möchten, müssen Sie sie manuell entfernen.
- Wenn die Grid-übergreifende Replizierung für jeden Bucket aktiviert wurde (d. h. wenn die Replikation in beide Richtungen erfolgt), können Sie die Grid-übergreifende Replizierung für einen oder beide Buckets deaktivieren. Sie können beispielsweise die Replikation von Objekten von `my-bucket` Auf Raster 1 bis `my-bucket` In Tabelle 2, während Sie weiterhin Objekte aus `my-bucket` Auf Raster 2 bis `my-bucket` In Raster 1.
- Sie müssen die Grid-übergreifende Replizierung deaktivieren, bevor Sie die Berechtigung eines Mandanten zur Verwendung der Grid-Federation-Verbindung entfernen können. Siehe "[Management zulässiger Mandanten](#)".
- Wenn Sie die Grid-übergreifende Replizierung für einen Bucket deaktivieren, der Objekte enthält, können Sie die Grid-übergreifende Replizierung nur wieder aktivieren, wenn Sie alle Objekte sowohl aus den Quell- als auch aus den Ziel-Buckets löschen.



Die Replikation kann nur dann wieder aktiviert werden, wenn beide Buckets leer sind.

Bevor Sie beginnen

- Sie verwenden ein "[Unterstützter Webbrowser](#)".
- Sie gehören einer Benutzergruppe an, die über den verfügt "[Root-Zugriffsberechtigung](#)".

Schritte

1. Beenden Sie die Grid-Replizierung für den Bucket, beginnend mit dem Grid, dessen Objekte Sie nicht mehr replizieren möchten:
 - a. Melden Sie sich beim Mandantenkonto für den Bucket an.

- b. Wählen Sie **View Buckets** aus dem Dashboard, oder wählen Sie **STORAGE (S3) > Buckets**.
- c. Wählen Sie den Bucket-Namen aus der Tabelle aus, um auf die Seite mit den Bucket-Details zuzugreifen.
- d. Wählen Sie die Registerkarte **Grid-Replikation** aus.
- e. Wählen Sie **Replikation deaktivieren**.
- f. Wenn Sie sicher sind, dass Sie die Grid-übergreifende Replikation für diesen Bucket deaktivieren möchten, geben Sie **Yes** in das Textfeld ein und wählen Sie **Disable** aus.

Nach einigen Augenblicken wird eine Erfolgsmeldung angezeigt. Neue Objekte, die diesem Bucket hinzugefügt wurden, können nicht mehr automatisch in das andere Grid repliziert werden. **Grid-übergreifende Replikation** wird nicht mehr als aktivierte Funktion auf der Buckets-Seite angezeigt.

2. Wenn die Grid-übergreifende Replizierung für beide Richtungen konfiguriert wurde, wechseln Sie zum entsprechenden Bucket auf dem anderen Grid und beenden Sie die Grid-übergreifende Replizierung in die andere Richtung.

Anzeigen von Verbindungen mit Grid Federation

Wenn Ihr Mandantenkonto die Berechtigung **Grid Federation connection** verwenden hat, können Sie die zulässigen Verbindungen anzeigen.

Bevor Sie beginnen

- Das Mandantenkonto hat die Berechtigung **Grid Federation connection** verwenden.
- Sie sind mit einem beim Mandantenmanager angemeldet "[Unterstützter Webbrowser](#)".
- Sie gehören einer Benutzergruppe an, die über den verfügt "[Root-Zugriffsberechtigung](#)".

Schritte

1. Wählen Sie **STORAGE (S3) > Grid Federation Connections**.

Die Seite Grid Federation Connection wird angezeigt und enthält eine Tabelle, in der die folgenden Informationen zusammengefasst werden:

Spalte	Beschreibung
Verbindungsname	Der Grid-Verbund stellt Verbindungen her, zu denen dieser Mandant berechtigt ist.
Buckets mit Grid-übergreifender Replizierung	Für jede Grid-Verbundverbindung die Mandanten-Buckets, für die die Grid-übergreifende Replizierung aktiviert ist Objekte, die diesen Buckets hinzugefügt werden, werden in das andere Raster der Verbindung repliziert.
Letzter Fehler	Bei jeder Grid-Federation-Verbindung tritt ggf. der letzte Fehler auf, wenn die Daten in das andere Grid repliziert wurden. Siehe Löschen Sie den letzten Fehler .

2. Wählen Sie optional einen Bucket-Namen aus "[Bucket-Details anzeigen](#)".

Leeren Sie den letzten Fehler

In der Spalte **Last error** kann aus einem der folgenden Gründe ein Fehler auftreten:

- Die Version des Quellobjekts wurde nicht gefunden.
- Der Quell-Bucket wurde nicht gefunden.
- Der Ziel-Bucket wurde gelöscht.
- Der Ziel-Bucket wurde von einem anderen Konto neu erstellt.
- Im Ziel-Bucket ist die Versionierung angehalten.
- Der Ziel-Bucket wurde vom selben Konto neu erstellt, ist aber jetzt nicht mehr versioniert.



In dieser Spalte wird nur der letzte gitterübergreifende Replikationsfehler angezeigt. Frühere Fehler, die möglicherweise aufgetreten sind, werden nicht angezeigt.

Schritte

1. Wenn in der Spalte **Last error** eine Meldung angezeigt wird, sehen Sie sich den Nachrichtentext an.

Dieser Fehler zeigt beispielsweise an, dass der Ziel-Bucket für die Grid-übergreifende Replizierung in einem ungültigen Status war, möglicherweise weil die Versionierung ausgesetzt oder S3 Object Lock aktiviert wurde.

Connection name	Buckets with cross-grid replication	Last error
Grid 1-Grid 2	my-cgr-bucket	2022-12-07 16:02:20 MST Cross-grid replication has encountered an error. Failed to send cross-grid replication request from source bucket 'my-cgr-bucket' to destination bucket 'my-cgr-bucket'. Error code: DestinationRequestError. Detail: InvalidBucketState. Confirm that the source and destination buckets have object versioning enabled and S3 Object Lock disabled. (logID 4791585492825418592)

2. Führen Sie alle empfohlenen Aktionen aus. Wenn beispielsweise die Versionierung auf dem Ziel-Bucket für die Grid-übergreifende Replizierung angehalten wurde, aktivieren Sie die Versionierung für diesen Bucket neu.
3. Wählen Sie die Verbindung aus der Tabelle aus.
4. Wählen Sie **Fehler löschen**.
5. Wählen Sie **Ja**, um die Meldung zu löschen und den Systemstatus zu aktualisieren.
6. Warten Sie 5-6 Minuten, und nehmen Sie dann ein neues Objekt in den Bucket auf. Bestätigen Sie, dass die Fehlermeldung nicht erneut angezeigt wird.



Um sicherzustellen, dass die Fehlermeldung gelöscht wird, warten Sie mindestens 5 Minuten nach dem Zeitstempel in der Nachricht, bevor Sie ein neues Objekt aufnehmen.

7. Informationen zum Bestimmen, ob Objekte aufgrund des Bucket-Fehlers nicht repliziert werden konnten, finden Sie unter "[Identifizieren Sie fehlgeschlagene Replikationsvorgänge und versuchen Sie es erneut](#)".

Verwalten von Gruppen und Benutzern

Verwenden Sie den Identitätsverbund

Durch die Verwendung eines Identitätsverbunds können Mandantengruppen und Benutzer schneller eingerichtet werden, und Mandantenbenutzer können sich dann mithilfe der vertrauten Anmeldedaten beim Mandantenkonto anmelden.

Konfigurieren Sie die Identitätsföderation für Mandanten-Manager

Sie können eine Identitätsföderation für den Mandanten-Manager konfigurieren, wenn Mandantengruppen und Benutzer in einem anderen System, z. B. Active Directory, Azure Active Directory (Azure AD), OpenLDAP oder Oracle Directory Server, gemanagt werden sollen.

Bevor Sie beginnen

- Sie sind mit einem beim Mandantenmanager angemeldet "[Unterstützter Webbrowser](#)".
- Sie gehören einer Benutzergruppe an, die über den verfügt "[Root-Zugriffsberechtigung](#)".
- Sie verwenden Active Directory, Azure AD, OpenLDAP oder Oracle Directory Server als Identitäts-Provider.



Wenn Sie einen nicht aufgeführten LDAP v3-Dienst verwenden möchten, wenden Sie sich an den technischen Support.

- Wenn Sie OpenLDAP verwenden möchten, müssen Sie den OpenLDAP-Server konfigurieren. Siehe [Richtlinien für die Konfiguration von OpenLDAP-Server](#).
- Wenn Sie Transport Layer Security (TLS) für die Kommunikation mit dem LDAP-Server verwenden möchten, muss der Identitäts-Provider TLS 1.2 oder 1.3 verwenden. Siehe "[Unterstützte Chiffren für ausgehende TLS-Verbindungen](#)".

Über diese Aufgabe

Ob Sie einen Identitätsföderationsdienst für Ihren Mandanten konfigurieren können, hängt davon ab, wie Ihr Mandantenkonto eingerichtet wurde. Der Mandant kann sich möglicherweise den für den Grid Manager konfigurierten Identitätsföderationsdienst teilen. Wenn diese Meldung angezeigt wird, wenn Sie auf die Seite Identity Federation zugreifen, können Sie keine separate föderierte Identitätsquelle für diesen Mandanten konfigurieren.



This tenant account uses the LDAP server that is configured for the Grid Manager. Contact the grid administrator for information or to change this setting.

Konfiguration eingeben

Wenn Sie Identifizieren Verbund konfigurieren, geben Sie die Werte an, die StorageGRID für die Verbindung mit einem LDAP-Dienst benötigt.

Schritte

1. Wählen Sie * ACCESS MANAGEMENT* > **Identity Federation**.
2. Wählen Sie **Identitätsföderation aktivieren**.
3. Wählen Sie im Abschnitt LDAP-Servicetyp den Typ des LDAP-Dienstes aus, den Sie konfigurieren möchten.

LDAP service type

Select the type of LDAP service you want to configure.

Active Directory	Azure	OpenLDAP	Other
------------------	-------	----------	-------

Wählen Sie **Other** aus, um Werte für einen LDAP-Server zu konfigurieren, der Oracle Directory Server verwendet.

4. Wenn Sie **Sonstige** ausgewählt haben, füllen Sie die Felder im Abschnitt LDAP-Attribute aus. Andernfalls fahren Sie mit dem nächsten Schritt fort.
 - **Eindeutiger Benutzername:** Der Name des Attributs, das die eindeutige Kennung eines LDAP-Benutzers enthält. Dieses Attribut ist äquivalent zu `sAMAccountName` Für Active Directory und `uid` Für OpenLDAP. Wenn Sie Oracle Directory Server konfigurieren, geben Sie ein `uid`.
 - **Benutzer-UUID:** Der Name des Attributs, das den permanenten eindeutigen Identifier eines LDAP-Benutzers enthält. Dieses Attribut ist äquivalent zu `objectGUID` Für Active Directory und `entryUUID` Für OpenLDAP. Wenn Sie Oracle Directory Server konfigurieren, geben Sie ein `nsuniqueid`. Der Wert jedes Benutzers für das angegebene Attribut muss eine 32-stellige Hexadezimalzahl im 16-Byte- oder String-Format sein, wobei Bindestriche ignoriert werden.
 - **Group Unique Name:** Der Name des Attributs, das den eindeutigen Identifier einer LDAP-Gruppe enthält. Dieses Attribut ist äquivalent zu `sAMAccountName` Für Active Directory und `cn` Für OpenLDAP. Wenn Sie Oracle Directory Server konfigurieren, geben Sie ein `cn`.
 - **Group UUID:** Der Name des Attributs, das den permanenten eindeutigen Identifier einer LDAP-Gruppe enthält. Dieses Attribut ist äquivalent zu `objectGUID` Für Active Directory und `entryUUID` Für OpenLDAP. Wenn Sie Oracle Directory Server konfigurieren, geben Sie ein `nsuniqueid`. Der Wert jeder Gruppe für das angegebene Attribut muss eine 32-stellige Hexadezimalzahl im 16-Byte- oder String-Format sein, wobei Bindestriche ignoriert werden.
5. Geben Sie für alle LDAP-Servicetypen die Informationen zum erforderlichen LDAP-Server und zur Netzwerkverbindung im Abschnitt LDAP-Server konfigurieren ein.
 - **Hostname:** Der vollständig qualifizierte Domainname (FQDN) oder die IP-Adresse des LDAP-Servers.
 - **Port:** Der Port, über den eine Verbindung zum LDAP-Server hergestellt wird.



Der Standardport für STARTTLS ist 389 und der Standardport für LDAPS ist 636. Sie können jedoch jeden beliebigen Port verwenden, solange Ihre Firewall korrekt konfiguriert ist.

- **Benutzername:** Der vollständige Pfad des Distinguished Name (DN) für den Benutzer, der eine Verbindung zum LDAP-Server herstellt.

Für Active Directory können Sie auch den unten angegebenen Anmeldenamen oder den Benutzerprinzipalnamen festlegen.

Der angegebene Benutzer muss über die Berechtigung zum Auflisten von Gruppen und Benutzern sowie zum Zugriff auf die folgenden Attribute verfügen:

- `sAMAccountName` Oder `uid`

- objectGUID, entryUUID, Oder nsuniqueid
 - cn
 - memberOf Oder isMemberOf
 - **Active Directory:** objectSid, primaryGroupID, userAccountControl, und userPrincipalName
 - **Azure:** accountEnabled Und userPrincipalName
- **Passwort:** Das mit dem Benutzernamen verknüpfte Passwort.



Wenn Sie das Passwort in Zukunft ändern, müssen Sie es auf dieser Seite aktualisieren.

- **Group Base DN:** Der vollständige Pfad des Distinguished Name (DN) für einen LDAP-Unterbaum, nach dem Sie nach Gruppen suchen möchten. Im Active Directory-Beispiel (unten) können alle Gruppen, deren Distinguished Name relativ zum Basis-DN (DC=storagegrid,DC=example,DC=com) ist, als föderierte Gruppen verwendet werden.



Die **Group Unique Name**-Werte müssen innerhalb des **Group Base DN**, zu dem sie gehören, eindeutig sein.

- **User Base DN:** Der vollständige Pfad des Distinguished Name (DN) eines LDAP-Unterbaums, nach dem Sie nach Benutzern suchen möchten.



Die **Benutzer-eindeutigen Namen**-Werte müssen innerhalb des **User Base DN**, zu dem sie gehören, eindeutig sein.

- **Bind username Format** (optional): Das Standard-Username Muster StorageGRID sollte verwendet werden, wenn das Muster nicht automatisch ermittelt werden kann.

Es wird empfohlen, **Bind username Format** bereitzustellen, da Benutzer sich anmelden können, wenn StorageGRID nicht mit dem Servicekonto verknüpft werden kann.

Geben Sie eines der folgenden Muster ein:

- **UserPrincipalName pattern (Active Directory und Azure):** [USERNAME]@example.com
- **Namensmuster für Anmeldung auf der Ebene nach unten (Active Directory und Azure):**
example\[USERNAME]
- *** Distinguished Name pattern*:** CN=[USERNAME],CN=Users,DC=example,DC=com

Fügen Sie **[USERNAME]** genau wie geschrieben ein.

6. Wählen Sie im Abschnitt Transport Layer Security (TLS) eine Sicherheitseinstellung aus.

- **Verwenden Sie STARTTLS:** Verwenden Sie STARTTLS, um die Kommunikation mit dem LDAP-Server zu sichern. Dies ist die empfohlene Option für Active Directory, OpenLDAP oder andere, diese Option wird jedoch für Azure nicht unterstützt.
- **LDAPS verwenden:** Die Option LDAPS (LDAP über SSL) verwendet TLS, um eine Verbindung zum LDAP-Server herzustellen. Sie müssen diese Option für Azure auswählen.
- **Verwenden Sie keine TLS:** Der Netzwerkverkehr zwischen dem StorageGRID-System und dem LDAP-Server wird nicht gesichert. Diese Option wird für Azure nicht unterstützt.



Die Verwendung der Option **keine TLS** verwenden wird nicht unterstützt, wenn Ihr Active Directory-Server die LDAP-Signatur erzwingt. Sie müssen STARTTLS oder LDAPS verwenden.

7. Wenn Sie STARTTLS oder LDAPS ausgewählt haben, wählen Sie das Zertifikat aus, mit dem die Verbindung gesichert werden soll.
 - **Verwenden Sie das Betriebssystem CA-Zertifikat:** Verwenden Sie das auf dem Betriebssystem installierte Standard-Grid-CA-Zertifikat, um Verbindungen zu sichern.
 - **Benutzerdefiniertes CA-Zertifikat verwenden:** Verwenden Sie ein benutzerdefiniertes Sicherheitszertifikat.

Wenn Sie diese Einstellung auswählen, kopieren Sie das benutzerdefinierte Sicherheitszertifikat in das Textfeld CA-Zertifikat und fügen Sie es ein.

Testen Sie die Verbindung und speichern Sie die Konfiguration

Nachdem Sie alle Werte eingegeben haben, müssen Sie die Verbindung testen, bevor Sie die Konfiguration speichern können. StorageGRID überprüft die Verbindungseinstellungen für den LDAP-Server und das BIND-Username-Format, wenn Sie es angegeben haben.

Schritte

1. Wählen Sie **Verbindung testen**.
2. Wenn Sie kein bind username Format angegeben haben:
 - Wenn die Verbindungseinstellungen gültig sind, wird die Meldung „Verbindung erfolgreich testen“ angezeigt. Wählen Sie **Speichern**, um die Konfiguration zu speichern.
 - Wenn die Verbindungseinstellungen ungültig sind, wird die Meldung „Testverbindung konnte nicht hergestellt werden“ angezeigt. Wählen Sie **Schließen**. Beheben Sie anschließend alle Probleme, und testen Sie die Verbindung erneut.
3. Wenn Sie ein bind username Format angegeben haben, geben Sie den Benutzernamen und das Kennwort eines gültigen föderierten Benutzers ein.

Geben Sie beispielsweise Ihren eigenen Benutzernamen und Ihr Kennwort ein. Geben Sie keine Sonderzeichen in den Benutzernamen ein, z. B. @ oder /.

Test Connection ✕

To test the connection and the bind username format, enter the username and password of a federated user. For example, enter your own federated username and password. The test values are not saved.

Test username

The username of a federated user.

Test password

 🗨

Cancel Test Connection

- Wenn die Verbindungseinstellungen gültig sind, wird die Meldung „Verbindung erfolgreich testen“ angezeigt. Wählen Sie **Speichern**, um die Konfiguration zu speichern.
- Es wird eine Fehlermeldung angezeigt, wenn die Verbindungseinstellungen, das Bind-Username-Format oder der Test-Benutzername und das Kennwort ungültig sind. Beheben Sie alle Probleme, und testen Sie die Verbindung erneut.

Synchronisierung mit Identitätsquelle erzwingen

Das StorageGRID-System synchronisiert regelmäßig föderierte Gruppen und Benutzer von der Identitätsquelle aus. Sie können die Synchronisierung erzwingen, wenn Sie Benutzerberechtigungen so schnell wie möglich aktivieren oder einschränken möchten.

Schritte

1. Rufen Sie die Seite Identity Federation auf.
2. Wählen Sie oben auf der Seite **Sync Server** aus.

Der Synchronisierungsprozess kann je nach Umgebung einige Zeit in Anspruch nehmen.



Die Warnmeldung * Identity Federation Failure* wird ausgelöst, wenn es ein Problem gibt, das die Synchronisierung von föderierten Gruppen und Benutzern aus der Identitätsquelle verursacht.

Deaktivieren Sie den Identitätsverbund

Sie können den Identitätsverbund für Gruppen und Benutzer vorübergehend oder dauerhaft deaktivieren. Wenn die Identitätsföderation deaktiviert ist, besteht keine Kommunikation zwischen StorageGRID und der Identitätsquelle. Allerdings bleiben alle von Ihnen konfigurierten Einstellungen erhalten, sodass Sie die Identitätsföderation zukünftig einfach wieder aktivieren können.

Über diese Aufgabe

Bevor Sie die Identitätsföderation deaktivieren, sollten Sie Folgendes beachten:

- Verbundene Benutzer können sich nicht anmelden.
- Föderierte Benutzer, die sich derzeit anmelden, erhalten bis zu ihrem Ablauf Zugriff auf das StorageGRID-System, können sich jedoch nach Ablauf der Sitzung nicht anmelden.
- Die Synchronisierung zwischen dem StorageGRID-System und der Identitätsquelle erfolgt nicht, und Warnmeldungen oder Alarmer werden nicht für Konten ausgelöst, die nicht synchronisiert wurden.
- Das Kontrollkästchen **Enable Identity Federation** ist deaktiviert, wenn Single Sign-On (SSO) auf **enabled** oder **Sandbox Mode** eingestellt ist. Der SSO-Status auf der Seite Single Sign-On muss **deaktiviert** sein, bevor Sie die Identitätsföderation deaktivieren können. Siehe "[Deaktivieren Sie Single Sign-On](#)".

Schritte

1. Rufen Sie die Seite Identity Federation auf.
2. Deaktivieren Sie das Kontrollkästchen **Enable Identity Federation**.

Richtlinien für die Konfiguration von OpenLDAP-Server

Wenn Sie einen OpenLDAP-Server für die Identitätsföderation verwenden möchten, müssen Sie bestimmte Einstellungen auf dem OpenLDAP-Server konfigurieren.



Bei Identitätsquellen, die nicht ActiveDirectory oder Azure sind, blockiert StorageGRID den S3-Zugriff nicht automatisch für Benutzer, die extern deaktiviert sind. Löschen Sie zum Blockieren des S3-Zugriffs alle S3-Schlüssel für den Benutzer oder entfernen Sie den Benutzer aus allen Gruppen.

Überlagerungen in Memberof und Refint

Die Überlagerungen Memberof und Refint sollten aktiviert sein. Weitere Informationen finden Sie in den Anweisungen zur Wartung der Umkehrgruppenmitgliedschaft im ["OpenLDAP-Dokumentation: Version 2.4 Administratorhandbuch"](#).

Indizierung

Sie müssen die folgenden OpenLDAP-Attribute mit den angegebenen Stichwörtern für den Index konfigurieren:

- `olcDbIndex: objectClass eq`
- `olcDbIndex: uid eq,pres,sub`
- `olcDbIndex: cn eq,pres,sub`
- `olcDbIndex: entryUUID eq`

Stellen Sie außerdem sicher, dass die in der Hilfe für den Benutzernamen genannten Felder für eine optimale Leistung indiziert sind.

Weitere Informationen zur Wartung von Gruppenmitgliedschaften finden Sie im ["OpenLDAP-Dokumentation: Version 2.4 Administratorhandbuch"](#).

Managen von Mandantengruppen

Erstellen von Gruppen für einen S3-Mandanten

Sie können Berechtigungen für S3-Benutzergruppen managen, indem Sie föderierte Gruppen importieren oder lokale Gruppen erstellen.

Bevor Sie beginnen

- Sie sind mit einem beim Mandantenmanager angemeldet ["Unterstützter Webbrowser"](#).
- Sie gehören einer Benutzergruppe an, die über den verfügt ["Root-Zugriffsberechtigung"](#).
- Wenn Sie planen, eine föderierte Gruppe zu importieren, haben Sie ["Konfigurierte Identitätsföderation"](#), Und die föderierte Gruppe ist bereits in der konfigurierten Identitätsquelle vorhanden.
- Wenn Ihr Mandantenkonto über die Berechtigung **Grid Federation connection** verwenden verfügt, haben Sie den Workflow und die Überlegungen für überprüft ["Klonen von Mandantengruppen und Benutzern"](#), Und Sie sind im Quellraster des Mandanten angemeldet.

Rufen Sie den Assistenten zum Erstellen von Gruppen auf

Rufen Sie als ersten Schritt den Assistenten zum Erstellen von Gruppen auf.

Schritte

1. Wählen Sie **ZUGRIFFSVERWALTUNG > Gruppen**.

2. Wenn Ihr Mandantenkonto über die Berechtigung **Grid Federation connection** verfügt, bestätigen Sie, dass ein blaues Banner erscheint, das anzeigt, dass neue Gruppen, die in diesem Raster erstellt werden, auf demselben Mandanten auf dem anderen Raster der Verbindung geklont werden. Wenn dieses Banner nicht angezeigt wird, werden Sie möglicherweise im Zielraster des Mandanten angemeldet.

Groups

Create and manage local and federated groups. Set group permissions to control access to specific pages and features.

0 groups Create group

Actions ▾

i This tenant has **Use grid federation connection** permission for connection Grid 1 to Grid 2. New local tenant groups will be automatically cloned to the same tenant on the other grid in the connection. If you edit or remove a group, your changes will not be synced to the other grid.

3. Wählen Sie **Gruppe erstellen**.

Wählen Sie einen Gruppentyp aus

Sie können eine lokale Gruppe erstellen oder eine föderierte Gruppe importieren.

Schritte

1. Wählen Sie die Registerkarte **Lokale Gruppe** aus, um eine lokale Gruppe zu erstellen, oder wählen Sie die Registerkarte **Federated Group** aus, um eine Gruppe aus der zuvor konfigurierten Identitätsquelle zu importieren.

Wenn Single Sign-On (SSO) für Ihr StorageGRID-System aktiviert ist, können sich Benutzer, die zu lokalen Gruppen gehören, nicht beim Mandanten-Manager anmelden, obwohl sie sich mithilfe von Client-Applikationen die Ressourcen des Mandanten basierend auf Gruppenberechtigungen managen können.

2. Geben Sie den Namen der Gruppe ein.
 - **Lokale Gruppe**: Geben Sie einen Anzeigenamen und einen eindeutigen Namen ein. Sie können den Anzeigenamen später bearbeiten.



Wenn Ihr Mandantenkonto über die Berechtigung **Grid Federation connection** verwenden verfügt, tritt ein Klonfehler auf, wenn der gleiche **eindeutige Name** bereits für den Mandanten im Zielraster vorhanden ist.

- **Federated Group**: Geben Sie den eindeutigen Namen ein. Bei Active Directory ist der eindeutige Name der dem zugeordneten Name `sAMAccountName` Attribut. Bei OpenLDAP ist der eindeutige Name der Name, der dem zugeordnet ist `uid` Attribut.
3. Wählen Sie **Weiter**.

Gruppenberechtigungen verwalten

Gruppenberechtigungen steuern, welche Aufgaben Benutzer in Tenant Manager und Tenant Management API durchführen können.

Schritte

1. Wählen Sie für **Access Mode** eine der folgenden Optionen aus:
 - **Lesen-Schreiben** (Standard): Benutzer können sich beim Tenant Manager anmelden und die Konfiguration des Mandanten verwalten.
 - **Schreibgeschützt**: Benutzer können nur Einstellungen und Funktionen anzeigen. Sie können keine Änderungen vornehmen oder keine Vorgänge in der Tenant Manager- oder Mandantenmanagement-API ausführen. Lokale schreibgeschützte Benutzer können ihre eigenen Passwörter ändern.



Wenn ein Benutzer zu mehreren Gruppen gehört und eine beliebige Gruppe auf schreibgeschützt eingestellt ist, hat der Benutzer schreibgeschützten Zugriff auf alle ausgewählten Einstellungen und Funktionen.

2. Wählen Sie eine oder mehrere Berechtigungen für diese Gruppe aus.

Siehe "[Mandantenmanagement-Berechtigungen](#)".

3. Wählen Sie **Weiter**.

Legen Sie die S3-Gruppenrichtlinie fest

Die Gruppenrichtlinie legt fest, über welche S3-Zugriffsberechtigungen Benutzer verfügen.

Schritte

1. Wählen Sie die Richtlinie aus, die Sie für diese Gruppe verwenden möchten.

Gruppenrichtlinie	Beschreibung
Kein S3-Zugriff	Standard. Benutzer in dieser Gruppe haben keinen Zugriff auf S3-Ressourcen, es sei denn, der Zugriff wird über eine Bucket-Richtlinie gewährt. Wenn Sie diese Option auswählen, hat nur der Root-Benutzer standardmäßig Zugriff auf S3-Ressourcen.
Schreibgeschützter Zugriff	Benutzer in dieser Gruppe haben schreibgeschützten Zugriff auf S3-Ressourcen. Benutzer in dieser Gruppe können beispielsweise Objekte auflisten und Objektdaten, Metadaten und Tags lesen. Wenn Sie diese Option auswählen, wird im Textfeld der JSON-String für eine schreibgeschützte Gruppenrichtlinie angezeigt. Diese Zeichenfolge kann nicht bearbeitet werden.
Voller Zugriff	Benutzer in dieser Gruppe haben vollständigen Zugriff auf S3-Ressourcen, einschließlich Buckets. Wenn Sie diese Option auswählen, wird im Textfeld der JSON-String für eine Richtlinie mit vollem Zugriff angezeigt. Diese Zeichenfolge kann nicht bearbeitet werden.

Gruppenrichtlinie	Beschreibung
Ransomware-Minimierung	<p>Diese Beispielrichtlinie gilt für alle Buckets für diesen Mandanten. Benutzer in dieser Gruppe können allgemeine Aktionen ausführen, aber Objekte aus Buckets, für die die Objektversionierung aktiviert ist, nicht dauerhaft löschen.</p> <p>Tenant Manager-Benutzer mit der Berechtigung Alle Buckets verwalten können diese Gruppenrichtlinie überschreiben. Beschränken Sie die Berechtigung zum Verwalten aller Buckets auf vertrauenswürdige Benutzer und verwenden Sie die Multi-Faktor-Authentifizierung (MFA), sofern verfügbar.</p>
Individuell	Benutzer in der Gruppe erhalten die Berechtigungen, die Sie im Textfeld angeben.

2. Wenn Sie **Benutzerdefiniert** ausgewählt haben, geben Sie die Gruppenrichtlinie ein. Jede Gruppenrichtlinie hat eine Größenbeschränkung von 5,120 Byte. Sie müssen einen gültigen JSON-formatierten String eingeben.

Ausführliche Informationen zu Gruppenrichtlinien, einschließlich Sprachsyntax und Beispiele, finden Sie unter "[Beispiel für Gruppenrichtlinien](#)".

3. Wenn Sie eine lokale Gruppe erstellen, wählen Sie **Weiter**. Wenn Sie eine Verbundgruppe erstellen, wählen Sie **Gruppe erstellen** und **Fertig stellen** aus.

Benutzer hinzufügen (nur lokale Gruppen)

Sie können die Gruppe speichern, ohne Benutzer hinzuzufügen, oder Sie können optional alle bereits vorhandenen lokalen Benutzer hinzufügen.



Wenn Ihr Mandantenkonto über die Berechtigung **Grid Federation connection** verfügt, werden alle Benutzer, die Sie beim Erstellen einer lokalen Gruppe im Quellraster auswählen, nicht berücksichtigt, wenn die Gruppe im Zielraster geklont wird. Wählen Sie aus diesem Grund keine Benutzer aus, wenn Sie die Gruppe erstellen. Wählen Sie stattdessen die Gruppe aus, wenn Sie die Benutzer erstellen.

Schritte

1. Wählen Sie optional einen oder mehrere lokale Benutzer für diese Gruppe aus.
2. Wählen Sie **Gruppe erstellen** und **Fertig stellen**.

Die von Ihnen erstellte Gruppe wird in der Gruppenliste angezeigt.

Wenn Ihr Mandantenkonto die Berechtigung **Grid Federation connection** verwenden hat und Sie sich im Quellraster des Mandanten befinden, wird die neue Gruppe im Zielraster des Mandanten geklont. **Success** erscheint als **Klonstatus** im Abschnitt Übersicht der Detailseite der Gruppe.

Erstellen von Gruppen für einen Swift Mandanten

Sie können Zugriffsberechtigungen für ein Swift-Mandantenkonto verwalten, indem Sie föderierte Gruppen importieren oder lokale Gruppen erstellen. Mindestens eine Gruppe

muss über die Swift-Administratorberechtigung verfügen, die zur Verwaltung der Container und Objekte für ein Swift-Mandantenkonto erforderlich ist.



Die Unterstützung für Swift-Client-Anwendungen wurde veraltet und wird in einer zukünftigen Version entfernt.

Bevor Sie beginnen

- Sie sind mit einem beim Mandantenmanager angemeldet "[Unterstützter Webbrowser](#)".
- Sie gehören einer Benutzergruppe an, die über den verfügt "[Root-Zugriffsberechtigung](#)".
- Wenn Sie planen, eine föderierte Gruppe zu importieren, haben Sie "[Konfigurierte Identitätsföderation](#)", Und die föderierte Gruppe ist bereits in der konfigurierten Identitätsquelle vorhanden.

Rufen Sie den Assistenten zum Erstellen von Gruppen auf

Schritte

Rufen Sie als ersten Schritt den Assistenten zum Erstellen von Gruppen auf.

1. Wählen Sie **ZUGRIFFSVERWALTUNG > Gruppen**.
2. Wählen Sie **Gruppe erstellen**.

Wählen Sie einen Gruppentyp aus

Sie können eine lokale Gruppe erstellen oder eine föderierte Gruppe importieren.

Schritte

1. Wählen Sie die Registerkarte **Lokale Gruppe** aus, um eine lokale Gruppe zu erstellen, oder wählen Sie die Registerkarte **Federated Group** aus, um eine Gruppe aus der zuvor konfigurierten Identitätsquelle zu importieren.

Wenn Single Sign-On (SSO) für Ihr StorageGRID-System aktiviert ist, können sich Benutzer, die zu lokalen Gruppen gehören, nicht beim Mandanten-Manager anmelden, obwohl sie sich mithilfe von Client-Applikationen die Ressourcen des Mandanten basierend auf Gruppenberechtigungen managen können.

2. Geben Sie den Namen der Gruppe ein.
 - **Lokale Gruppe**: Geben Sie einen Anzeigenamen und einen eindeutigen Namen ein. Sie können den Anzeigenamen später bearbeiten.
 - **Federated Group**: Geben Sie den eindeutigen Namen ein. Bei Active Directory ist der eindeutige Name der dem zugeordneten Name `sAMAccountName` Attribut. Bei OpenLDAP ist der eindeutige Name der Name, der dem zugeordnet ist `uid` Attribut.
3. Wählen Sie **Weiter**.

Gruppenberechtigungen verwalten

Gruppenberechtigungen steuern, welche Aufgaben Benutzer in Tenant Manager und Tenant Management API durchführen können.

Schritte

1. Wählen Sie für **Access Mode** eine der folgenden Optionen aus:
 - **Lesen-Schreiben** (Standard): Benutzer können sich beim Tenant Manager anmelden und die

Konfiguration des Mandanten verwalten.

- **Schreibgeschützt:** Benutzer können nur Einstellungen und Funktionen anzeigen. Sie können keine Änderungen vornehmen oder keine Vorgänge in der Tenant Manager- oder Mandantenmanagement-API ausführen. Lokale schreibgeschützte Benutzer können ihre eigenen Passwörter ändern.



Wenn ein Benutzer zu mehreren Gruppen gehört und eine beliebige Gruppe auf schreibgeschützt eingestellt ist, hat der Benutzer schreibgeschützten Zugriff auf alle ausgewählten Einstellungen und Funktionen.

2. Aktivieren Sie das Kontrollkästchen **Root Access**, wenn Gruppenbenutzer sich beim Tenant Manager oder der Tenant Management API anmelden müssen.
3. Wählen Sie **Weiter**.

Swift-Gruppenrichtlinie festlegen

Swift-Benutzer benötigen Administratorberechtigungen, um sich bei der Swift-REST-API zu authentifizieren, um Container zu erstellen und Objekte aufzunehmen.

1. Aktivieren Sie das Kontrollkästchen **Swift Administrator**, wenn Gruppenbenutzer die Swift REST API zum Verwalten von Containern und Objekten verwenden müssen.
2. Wenn Sie eine lokale Gruppe erstellen, wählen Sie **Weiter**. Wenn Sie eine Verbundgruppe erstellen, wählen Sie **Gruppe erstellen** und **Fertig stellen** aus.

Benutzer hinzufügen (nur lokale Gruppen)

Sie können die Gruppe speichern, ohne Benutzer hinzuzufügen, oder Sie können optional alle bereits vorhandenen lokalen Benutzer hinzufügen.

Schritte

1. Wählen Sie optional einen oder mehrere lokale Benutzer für diese Gruppe aus.

Wenn Sie noch keine lokalen Benutzer erstellt haben, können Sie diese Gruppe dem Benutzer auf der Seite Benutzer hinzufügen. Siehe "[Managen Sie lokale Benutzer](#)".

2. Wählen Sie **Gruppe erstellen** und **Fertig stellen**.

Die von Ihnen erstellte Gruppe wird in der Gruppenliste angezeigt.

Mandantenmanagement-Berechtigungen

Bevor Sie eine Mandantengruppe erstellen, überlegen Sie, welche Berechtigungen Sie dieser Gruppe zuweisen möchten. Über die Mandantenmanagement-Berechtigungen wird festgelegt, welche Aufgaben Benutzer mit dem Tenant Manager oder der Mandantenmanagement-API durchführen können. Ein Benutzer kann einer oder mehreren Gruppen angehören. Berechtigungen werden kumulativ, wenn ein Benutzer zu mehreren Gruppen gehört.

Um sich beim Tenant Manager anzumelden oder die Mandantenmanagement-API zu verwenden, müssen Benutzer einer Gruppe mit mindestens einer Berechtigung angehören. Alle Benutzer, die sich anmelden können, können die folgenden Aufgaben ausführen:

- Dashboard anzeigen
- Eigenes Kennwort ändern (für lokale Benutzer)

Für alle Berechtigungen legt die Einstellung Zugriffsmodus der Gruppe fest, ob Benutzer Einstellungen ändern und Vorgänge ausführen können oder ob sie nur die zugehörigen Einstellungen und Funktionen anzeigen können.



Wenn ein Benutzer zu mehreren Gruppen gehört und eine beliebige Gruppe auf schreibgeschützt eingestellt ist, hat der Benutzer schreibgeschützten Zugriff auf alle ausgewählten Einstellungen und Funktionen.

Sie können einer Gruppe die folgenden Berechtigungen zuweisen. Beachten Sie, dass S3-Mandanten und Swift-Mandanten unterschiedliche Gruppenberechtigungen haben.

Berechtigung	Beschreibung	Details
Root-Zugriff	Bietet vollständigen Zugriff auf den Tenant Manager und die Mandanten-Management-API.	Swift-Benutzer müssen über Root-Zugriffsberechtigungen verfügen, um sich beim Mandantenkonto anzumelden.
Verwalter	Nur Swift Mandanten. Bietet vollständigen Zugriff auf die Swift Container und Objekte für dieses Mandantenkonto	Swift-Benutzer müssen über die Swift-Administrator-Berechtigung verfügen, um alle Vorgänge mit der Swift-REST-API auszuführen.
Management Ihrer eigenen S3 Zugangsdaten	Benutzer können ihre eigenen S3-Zugriffsschlüssel erstellen und entfernen.	Benutzer, die diese Berechtigung nicht besitzen, sehen die Menüoption STORAGE (S3) > Meine S3-Zugriffstasten nicht.
Alle Buckets anzeigen	<p>S3 Tenants: Ermöglicht es Benutzern, alle Buckets und Bucket-Konfigurationen anzuzeigen.</p> <p>Swift Tenants: Ermöglicht Swift-Benutzern, alle Container und Container-Konfigurationen über die Tenant Management API anzuzeigen.</p>	<p>Benutzer, die weder die Berechtigung Alle Buckets anzeigen noch die Berechtigung Alle Buckets verwalten haben, sehen die Menüoption Buckets nicht.</p> <p>Diese Berechtigung wird durch die Berechtigung zum Verwalten aller Buckets ersetzt. Dies hat keine Auswirkungen auf S3-Bucket oder Gruppenrichtlinien, die von S3-Clients oder S3-Konsole verwendet werden.</p> <p>Diese Berechtigung können Sie Swift-Gruppen nur über die Mandanten-Management-API zuweisen. Diese Berechtigung können Swift-Gruppen nicht mit dem Tenant Manager zugewiesen werden.</p>

Berechtigung	Beschreibung	Details
Managen aller Buckets	<p>S3-Mandanten: Ermöglicht Benutzern die Verwendung des Tenant Manager und der Tenant Management API, um S3-Buckets zu erstellen und zu löschen sowie die Einstellungen für alle S3-Buckets im Mandantenkonto zu managen, unabhängig von S3-Bucket oder Gruppenrichtlinien.</p> <p>Swift Tenants: Ermöglicht Swift-Benutzern die Kontrolle der Konsistenz für Swift-Container mithilfe der Mandanten-Management-API.</p>	<p>Benutzer, die weder die Berechtigung Alle Buckets anzeigen noch die Berechtigung Alle Buckets verwalten haben, sehen die Menüoption Buckets nicht.</p> <p>Diese Berechtigung ersetzt die Berechtigung Alle Planungsperioden anzeigen. Dies hat keine Auswirkungen auf S3-Bucket oder Gruppenrichtlinien, die von S3-Clients oder S3-Konsole verwendet werden.</p> <p>Diese Berechtigung können Sie Swift-Gruppen nur über die Mandanten-Management-API zuweisen. Diese Berechtigung können Swift-Gruppen nicht mit dem Tenant Manager zugewiesen werden.</p>
Verwalten von Endpunkten	Ermöglicht Benutzern die Verwendung des Tenant Managers oder der Mandanten-Management-API zum Erstellen oder Bearbeiten von Plattformdienstendpunkten, die als Ziel für StorageGRID-Plattformdienste verwendet werden.	Benutzer, die diese Berechtigung nicht besitzen, sehen die Menüoption Plattform-Dienste-Endpunkte nicht.
Verwenden Sie die Registerkarte S3 Console	In Kombination mit der Berechtigung Alle Buckets anzeigen oder alle Buckets verwalten können Benutzer Objekte über die Registerkarte S3 Console auf der Detailseite für einen Bucket anzeigen und managen.	

Gruppen managen

Managen Sie die Mandantengruppen nach Bedarf, um eine Gruppe anzuzeigen, zu bearbeiten oder zu duplizieren und vieles mehr.

Bevor Sie beginnen

- Sie sind mit einem beim Mandantenmanager angemeldet "[Unterstützter Webbrowser](#)".
- Sie gehören einer Benutzergruppe an, die über den verfügt "[Root-Zugriffsberechtigung](#)".

Gruppe anzeigen oder bearbeiten

Sie können die grundlegenden Informationen und Details für jede Gruppe anzeigen und bearbeiten.

Schritte

1. Wählen Sie **ZUGRIFFSVERWALTUNG > Gruppen**.
2. Überprüfen Sie die Informationen auf der Seite Gruppen, auf der grundlegende Informationen für alle lokalen und föderierten Gruppen für dieses Mandantenkonto aufgeführt sind.

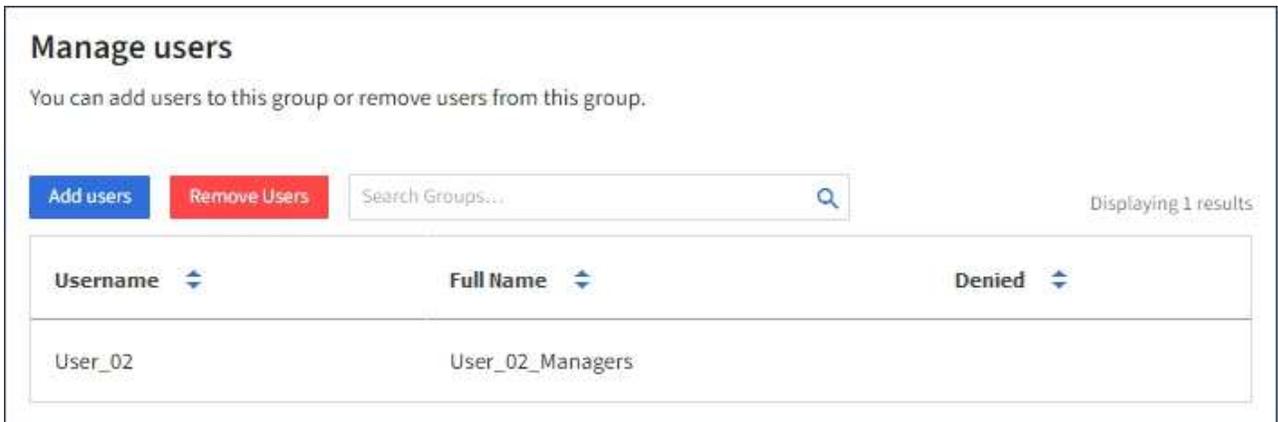
Wenn das Mandantenkonto über die Berechtigung **Grid Federation connection** verwenden verfügt und

Sie Gruppen im Quellraster des Mandanten anzeigen:

- Eine Banner-Meldung zeigt an, dass Ihre Änderungen nicht mit dem anderen Raster synchronisiert werden, wenn Sie eine Gruppe bearbeiten oder entfernen.
 - Bei Bedarf gibt eine Banner-Meldung an, ob Gruppen nicht für den Mandanten im Zielraster geklont wurden. Das können Sie [Wiederholen Sie einen Gruppenklon](#) Das ist gescheitert.
3. Wenn Sie den Namen der Gruppe ändern möchten:
- a. Aktivieren Sie das Kontrollkästchen für die Gruppe.
 - b. Wählen Sie **actions > Edit Group Name**.
 - c. Geben Sie den neuen Namen ein.
 - d. Wählen Sie **Änderungen speichern**.
4. Wenn Sie weitere Details anzeigen oder weitere Änderungen vornehmen möchten, führen Sie einen der folgenden Schritte aus:
- Wählen Sie den Gruppennamen aus.
 - Aktivieren Sie das Kontrollkästchen für die Gruppe und wählen Sie **actions > View Group Details**.
5. Lesen Sie den Abschnitt „Übersicht“, in dem die folgenden Informationen für jede Gruppe angezeigt werden:
- Anzeigename
 - Eindeutiger Name
 - Typ
 - Zugriffsmodus
 - Berechtigungen
 - S3-Richtlinie
 - Anzahl der Benutzer in dieser Gruppe
 - Zusätzliche Felder, wenn das Mandantenkonto die Berechtigung **Grid Federation connection** verwendet hat und Sie die Gruppe im Quellraster des Mandanten anzeigen:
 - Klonstatus, entweder **success** oder **failure**
 - Ein blaues Banner, das darauf hinweist, dass Ihre Änderungen nicht mit dem anderen Raster synchronisiert werden, wenn Sie diese Gruppe bearbeiten oder löschen.
6. Bearbeiten Sie die Gruppeneinstellungen nach Bedarf. Siehe "[Erstellen von Gruppen für einen S3-Mandanten](#)" Und "[Erstellen von Gruppen für einen Swift Mandanten](#)" Für Details, was eingegeben werden soll.
- a. Ändern Sie im Abschnitt Übersicht den Anzeigenamen, indem Sie den Namen oder das Bearbeitungssymbol auswählen .
 - b. Aktualisieren Sie auf der Registerkarte **Gruppenberechtigungen** die Berechtigungen und wählen Sie **Änderungen speichern**.
 - c. Nehmen Sie auf der Registerkarte **Gruppenrichtlinie** Änderungen vor und wählen Sie **Änderungen speichern**.
 - Wenn Sie eine S3-Gruppe bearbeiten, wählen Sie optional eine andere S3-Gruppenrichtlinie aus, oder geben Sie bei Bedarf den JSON-String für eine benutzerdefinierte Richtlinie ein.
 - Wenn Sie eine Swift-Gruppe bearbeiten, aktivieren oder deaktivieren Sie optional das Kontrollkästchen **Swift Administrator**.

7. So fügen Sie der Gruppe einen oder mehrere vorhandene lokale Benutzer hinzu:

a. Wählen Sie die Registerkarte Benutzer aus.



b. Wählen Sie **Benutzer hinzufügen**.

c. Wählen Sie die vorhandenen Benutzer aus, die Sie hinzufügen möchten, und wählen Sie **Benutzer hinzufügen**.

Oben rechts wird eine Erfolgsmeldung angezeigt.

8. So entfernen Sie lokale Benutzer aus der Gruppe:

a. Wählen Sie die Registerkarte Benutzer aus.

b. Wählen Sie **Benutzer entfernen**.

c. Wählen Sie die Benutzer aus, die Sie entfernen möchten, und wählen Sie **Benutzer entfernen**.

Oben rechts wird eine Erfolgsmeldung angezeigt.

9. Bestätigen Sie, dass Sie für jeden geänderten Abschnitt **Änderungen speichern** ausgewählt haben.

Gruppe duplizieren

Sie können eine vorhandene Gruppe duplizieren, um neue Gruppen schneller zu erstellen.



Wenn Ihr Mandantenkonto die Berechtigung **Grid Federation connection** verwenden hat und Sie eine Gruppe aus dem Quellraster des Mandanten duplizieren, wird die duplizierte Gruppe im Zielraster des Mandanten geklont.

Schritte

1. Wählen Sie **ZUGRIFFSVERWALTUNG > Gruppen**.

2. Aktivieren Sie das Kontrollkästchen für die Gruppe, die Sie duplizieren möchten.

3. Wählen Sie **Aktionen > Gruppe duplizieren**.

4. Siehe "[Erstellen von Gruppen für einen S3-Mandanten](#)" Oder "[Erstellen von Gruppen für einen Swift Mandanten](#)" Für Details, was eingegeben werden soll.

5. Wählen Sie **Gruppe erstellen**.

Gruppenklone erneut versuchen

So wiederholen Sie einen fehlgeschlagenen Klon:

1. Wählen Sie jede Gruppe aus, die (*Klonen fehlgeschlagen*) unter dem Gruppennamen anzeigt.
2. Wählen Sie **actions > Clone groups**.
3. Zeigen Sie den Status des Klonvorgangs auf der Detailseite jeder Gruppe an, die Sie klonen.

Weitere Informationen finden Sie unter "[Klonen von Mandantengruppen und Benutzern](#)".

Löschen Sie eine oder mehrere Gruppen

Sie können eine oder mehrere Gruppen löschen. Alle Benutzer, die nur zu einer Gruppe gehören, die gelöscht wurde, können sich nicht mehr beim Tenant Manager anmelden oder das Mandantenkonto verwenden.



Wenn Ihr Mandantenkonto über die Berechtigung **Grid Federation connection** verwenden verfügt und Sie eine Gruppe löschen, wird StorageGRID die entsprechende Gruppe im anderen Raster nicht löschen. Wenn Sie diese Informationen synchron halten müssen, müssen Sie dieselbe Gruppe aus beiden Rastern löschen.

Schritte

1. Wählen Sie **ZUGRIFFSVERWALTUNG > Gruppen**.
2. Aktivieren Sie das Kontrollkästchen für jede Gruppe, die Sie löschen möchten.
3. Wählen Sie **Aktionen > Gruppe löschen** oder **Aktionen > Gruppen löschen**.

Ein Bestätigungsdiaologfeld wird angezeigt.

4. Wählen Sie **Gruppe löschen** oder **Gruppen löschen**.

Managen Sie lokale Benutzer

Sie können lokale Benutzer erstellen und lokalen Gruppen zuweisen, um zu bestimmen, auf welche Funktionen diese Benutzer zugreifen können. Der Tenant Manager enthält einen vordefinierten lokalen Benutzer mit dem Namen „root“. Obwohl Sie lokale Benutzer hinzufügen und entfernen können, können Sie den Root-Benutzer nicht entfernen.



Wenn Single Sign-On (SSO) für Ihr StorageGRID-System aktiviert ist, können sich lokale Benutzer nicht beim Tenant Manager oder der Mandanten-Management-API anmelden, obwohl sie Clientanwendungen verwenden können, um basierend auf Gruppenberechtigungen auf die Ressourcen des Mandanten zuzugreifen.

Bevor Sie beginnen

- Sie sind mit einem beim Mandantenmanager angemeldet "[Unterstützter Webbrowser](#)".
- Sie gehören einer Benutzergruppe an, die über den verfügt "[Root-Zugriffsberechtigung](#)".
- Wenn Ihr Mandantenkonto über die Berechtigung **Grid Federation connection** verwenden verfügt, haben Sie den Workflow und die Überlegungen für überprüft "[Klonen von Mandantengruppen und Benutzern](#)", Und Sie sind im Quellraster des Mandanten angemeldet.

Erstellen Sie einen lokalen Benutzer

Sie können einen lokalen Benutzer erstellen und diesen einer oder mehreren lokalen Gruppen zuweisen, um ihre Zugriffsberechtigungen zu steuern.

S3-Benutzer, die keiner Gruppe angehören, haben keine Managementberechtigungen oder S3-Gruppenrichtlinien, die auf sie angewendet werden. Diese Benutzer haben möglicherweise S3-Bucket-Zugriff, der über eine Bucket-Richtlinie gewährt wird.

Swift-Benutzer, die keiner Gruppe angehören, haben keine Managementberechtigungen oder Swift-Container-Zugriff.

Rufen Sie den Assistenten zum Erstellen von Benutzern auf

Schritte

1. Wählen Sie **ZUGRIFFSVERWALTUNG > Benutzer**.

Wenn Ihr Mandantenkonto die Berechtigung **Grid Federation connection** verwenden hat, zeigt ein blaues Banner an, dass dies das Quellraster des Mandanten ist. Alle lokalen Benutzer, die Sie in diesem Raster erstellen, werden in das andere Raster der Verbindung geklont.

2. Wählen Sie **Benutzer erstellen**.

Geben Sie die Anmeldedaten ein

Schritte

1. Füllen Sie für den Schritt **Enter user credentials** die folgenden Felder aus.

Feld	Beschreibung
Vollständiger Name	Der vollständige Name für diesen Benutzer, z. B. der vor- und Nachname einer Person oder der Name einer Anwendung.
Benutzername	Der Name, den dieser Benutzer zur Anmeldung verwendet. Benutzernamen müssen eindeutig sein und können nicht geändert werden. Hinweis: Wenn Ihr Mieterkonto die Berechtigung Grid Federation connection verwenden hat, tritt ein Klonfehler auf, wenn der gleiche Benutzername bereits für den Mieter im Zielraster vorhanden ist.
Passwort und Passwort bestätigen	Das Passwort, das der Benutzer beim Anmelden verwendet.
Zugriff verweigern	Wählen Sie Ja , um zu verhindern, dass sich dieser Benutzer beim Mandantenkonto anmeldet, obwohl er noch zu einer oder mehreren Gruppen gehört. Wählen Sie zum Beispiel Ja , um die Anmelde-Fähigkeit eines Benutzers vorübergehend zu unterbrechen.

2. Wählen Sie **Weiter**.

Zu Gruppen zuweisen

Schritte

1. Weisen Sie den Benutzer einer oder mehreren lokalen Gruppen zu, um zu bestimmen, welche Aufgaben er ausführen kann.

Das Zuweisen eines Benutzers zu Gruppen ist optional. Wenn Sie möchten, können Sie Benutzer auswählen, wenn Sie Gruppen erstellen oder bearbeiten.

Benutzer, die keiner Gruppe angehören, haben keine Verwaltungsberechtigungen. Berechtigungen sind kumulativ. Benutzer haben alle Berechtigungen für alle Gruppen, denen sie angehören. Siehe "[Mandantenmanagement-Berechtigungen](#)".

2. Wählen Sie **Benutzer erstellen**.

Wenn Ihr Mandantenkonto die Berechtigung **Grid Federation connection** verwenden hat und Sie sich im Quellraster des Mandanten befinden, wird der neue lokale Benutzer im Zielraster des Mandanten geklont. **Success** erscheint als **Klonstatus** im Abschnitt Übersicht der Detailseite des Benutzers.

3. Wählen Sie **Fertig**, um zur Benutzerseite zurückzukehren.

Lokalen Benutzer anzeigen oder bearbeiten

Schritte

1. Wählen Sie **ZUGRIFFSVERWALTUNG > Benutzer**.
2. Überprüfen Sie die Informationen auf der Seite Benutzer, auf der grundlegende Informationen für alle lokalen und föderierten Benutzer dieses Mandantenkontos aufgeführt sind.

Wenn das Mandantenkonto über die Berechtigung **Grid Federation connection** verwenden verfügt und Sie den Benutzer im Quellraster des Mandanten anzeigen:

- Wenn Sie einen Benutzer bearbeiten oder entfernen, werden Ihre Änderungen nicht mit dem anderen Raster synchronisiert.
 - Bei Bedarf gibt eine Banner-Meldung an, ob Benutzer nicht für den Mandanten im Zielraster geklont wurden. Das können Sie [Wiederholen Sie einen fehlgeschlagenen Benutzerklon](#).
3. Wenn Sie den vollständigen Namen des Benutzers ändern möchten:
 - a. Aktivieren Sie das Kontrollkästchen für den Benutzer.
 - b. Wählen Sie **actions > vollständigen Namen bearbeiten**.
 - c. Geben Sie den neuen Namen ein.
 - d. Wählen Sie **Änderungen speichern**.
 4. Wenn Sie weitere Details anzeigen oder weitere Änderungen vornehmen möchten, führen Sie einen der folgenden Schritte aus:
 - Wählen Sie den Benutzernamen aus.
 - Aktivieren Sie das Kontrollkästchen für den Benutzer, und wählen Sie **Aktionen > Benutzerdetails anzeigen**.
 5. Lesen Sie den Abschnitt Übersicht, in dem die folgenden Informationen für jeden Benutzer angezeigt werden:
 - Vollständiger Name

- Benutzername
 - Benutzertyp
 - Zugriff verweigert
 - Zugriffsmodus
 - Gruppenmitgliedschaft
 - Zusätzliche Felder, wenn das Mandantenkonto die Berechtigung **Grid Federation connection** verwenden hat und Sie den Benutzer im Quellraster des Mandanten anzeigen:
 - Klonstatus, entweder **success** oder **failure**
 - Ein blaues Banner, das darauf hinweist, dass Ihre Änderungen nicht mit dem anderen Raster synchronisiert werden, wenn Sie diesen Benutzer bearbeiten.
6. Bearbeiten Sie die Benutzereinstellungen nach Bedarf. Siehe [Erstellen Sie einen lokalen Benutzer](#) Für Details, was eingegeben werden soll.
- a. Ändern Sie im Abschnitt Übersicht den vollständigen Namen, indem Sie den Namen oder das Bearbeiten-Symbol auswählen .

Sie können den Benutzernamen nicht ändern.

 - b. Ändern Sie auf der Registerkarte **Passwort** das Passwort des Benutzers und wählen Sie **Änderungen speichern**.
 - c. Wählen Sie auf der Registerkarte **Access No** aus, damit sich der Benutzer anmelden kann, oder wählen Sie **Yes**, um die Anmeldung des Benutzers zu verhindern. Wählen Sie dann **Änderungen speichern**.
 - d. Wählen Sie auf der Registerkarte **Zugriffstasten** die Option **Schlüssel erstellen** aus, und befolgen Sie die Anweisungen für "[Erstellen der S3-Zugriffsschlüssel eines anderen Benutzers](#)".
 - e. Wählen Sie auf der Registerkarte **Gruppen** die Option **Gruppen bearbeiten**, um den Benutzer zu Gruppen hinzuzufügen oder ihn aus Gruppen zu entfernen. Wählen Sie dann **Änderungen speichern**.
7. Bestätigen Sie, dass Sie für jeden geänderten Abschnitt **Änderungen speichern** ausgewählt haben.

Doppelter lokaler Benutzer

Sie können einen lokalen Benutzer duplizieren, um einen neuen Benutzer schneller zu erstellen.



Wenn Ihr Mandantenkonto über die Berechtigung **Grid Federation connection** verwenden verfügt und Sie einen Benutzer aus dem Quellraster des Mandanten duplizieren, wird der duplizierte Benutzer im Zielraster des Mandanten geklont.

Schritte

1. Wählen Sie **ZUGRIFFSVERWALTUNG > Benutzer**.
2. Aktivieren Sie das Kontrollkästchen für den Benutzer, den Sie duplizieren möchten.
3. Wählen Sie **Actions > Dupliziere Benutzer**.
4. Siehe [Erstellen Sie einen lokalen Benutzer](#) Für Details, was eingegeben werden soll.
5. Wählen Sie **Benutzer erstellen**.

Benutzerklon wiederholen

So wiederholen Sie einen fehlgeschlagenen Klon:

1. Wählen Sie jeden Benutzer aus, der (*Klonen fehlgeschlagen*) unter dem Benutzernamen anzeigt.
2. Wählen Sie **actions > Clone users**.
3. Den Status des Klonvorgangs können Sie auf der Detailseite jedes Benutzers, den Sie klonen, anzeigen.

Weitere Informationen finden Sie unter "[Klonen von Mandantengruppen und Benutzern](#)".

Löschen Sie einen oder mehrere lokale Benutzer

Sie können einen oder mehrere lokale Benutzer, die nicht mehr auf das StorageGRID-Mandantenkonto zugreifen müssen, dauerhaft löschen.



Wenn Ihr Mandantenkonto über die Berechtigung **Grid Federation connection** verwenden verfügt und Sie einen lokalen Benutzer löschen, wird StorageGRID den entsprechenden Benutzer im anderen Raster nicht löschen. Wenn Sie diese Informationen synchron halten müssen, müssen Sie denselben Benutzer aus beiden Rastern löschen.



Sie müssen die föderierte Identitätsquelle verwenden, um verbundene Benutzer zu löschen.

Schritte

1. Wählen Sie **ZUGRIFFSVERWALTUNG > Benutzer**.
2. Aktivieren Sie das Kontrollkästchen für jeden Benutzer, den Sie löschen möchten.
3. Wählen Sie **Aktionen > Benutzer löschen** oder **Aktionen > Benutzer löschen**.

Ein Bestätigungsdialogfeld wird angezeigt.

4. Wählen Sie **Benutzer löschen** oder **Benutzer löschen**.

Managen von S3-Zugriffsschlüsseln

Managen Sie S3 Zugriffsschlüssel: Übersicht

Jeder Benutzer eines S3-Mandantenkontos muss über einen Zugriffsschlüssel verfügen, um Objekte im StorageGRID System zu speichern und abzurufen. Ein Zugriffsschlüssel besteht aus einer Zugriffsschlüssel-ID und einem geheimen Zugriffsschlüssel.

S3-Zugriffsschlüssel können wie folgt gemanagt werden:

- Benutzer, die die Berechtigung **Manage your own S3 credentials** besitzen, können ihre eigenen S3-Zugriffsschlüssel erstellen oder entfernen.
- Benutzer mit der Berechtigung **Root-Zugriff** können die Zugriffsschlüssel für das S3-Root-Konto und alle anderen Benutzer verwalten. Root-Zugriffsschlüssel bieten vollständigen Zugriff auf alle Buckets und Objekte für Mandanten, sofern nicht ausdrücklich von einer Bucket-Richtlinie deaktiviert wurde.

StorageGRID unterstützt die Authentifizierung nach Signature Version 2 und Signature Version 4. Der Zugriff auf übergreifende Konten ist nur zulässig, wenn diese durch eine Bucket-Richtlinie ausdrücklich aktiviert wurde.

Erstellen Ihrer eigenen S3-Zugriffsschlüssel

Wenn Sie einen S3-Mandanten verwenden und über die entsprechenden Berechtigungen

verfügen, können Sie Ihre eigenen S3-Zugriffsschlüssel erstellen. Sie benötigen einen Zugriffsschlüssel für den Zugriff auf Ihre Buckets und Objekte.

Bevor Sie beginnen

- Sie sind mit einem beim Mandantenmanager angemeldet "[Unterstützter Webbrowser](#)".
- Sie gehören einer Benutzergruppe an, die über den verfügt "[Managen Sie Ihre eigenen S3-Anmeldedaten oder Root-Zugriffsberechtigungen](#)".

Über diese Aufgabe

Sie können einen oder mehrere S3-Zugriffsschlüssel erstellen und managen, mit denen Sie Buckets für Ihr Mandantenkonto erstellen und verwalten können. Nachdem Sie einen neuen Zugriffsschlüssel erstellt haben, aktualisieren Sie die Anwendung mit Ihrer neuen Zugriffsschlüssel-ID und dem geheimen Zugriffsschlüssel. Aus Sicherheitsgründen sollten Sie nicht mehr Schlüssel erstellen, als Sie benötigen, und die Schlüssel löschen, die Sie nicht verwenden. Wenn Sie nur einen Schlüssel haben und demnächst ablaufen, erstellen Sie einen neuen Schlüssel, bevor der alte Schlüssel abläuft, und löschen Sie dann den alten Schlüssel.

Jeder Schlüssel kann eine bestimmte Ablaufzeit haben oder keinen Ablauf haben. Beachten Sie die folgenden Richtlinien für die Ablaufzeit:

- Legen Sie eine Ablaufzeit für Ihre Schlüssel fest, um den Zugriff auf einen bestimmten Zeitraum zu beschränken. Durch die Einrichtung einer kurzen Ablaufzeit kann Ihr Risiko verringert werden, wenn Ihre Zugriffsschlüssel-ID und Ihr geheimer Zugriffsschlüssel versehentlich ausgesetzt sind. Abgelaufene Schlüssel werden automatisch entfernt.
- Wenn das Sicherheitsrisiko in Ihrer Umgebung gering ist und Sie nicht regelmäßig neue Schlüssel erstellen müssen, müssen Sie keine Ablaufzeit für Ihre Schlüssel festlegen. Wenn Sie sich zu einem späteren Zeitpunkt für die Erstellung neuer Schlüssel entscheiden, löschen Sie die alten Schlüssel manuell.



Sie können auf die S3-Buckets und Objekte aus Ihrem Konto zugreifen, indem Sie die Zugriffsschlüssel-ID und den geheimen Zugriffsschlüssel verwenden, die für Ihr Konto im Mandanten-Manager angezeigt werden. Aus diesem Grund schützen Sie Zugriffsschlüssel wie ein Passwort. Drehen Sie regelmäßig Zugriffsschlüssel, entfernen Sie alle nicht verwendeten Schlüssel aus Ihrem Konto und teilen Sie sie niemals mit anderen Benutzern.

Schritte

1. Wählen Sie **STORAGE (S3) > Meine Zugriffsschlüssel** aus.

Die Seite Meine Zugriffsschlüssel wird angezeigt und enthält alle vorhandenen Zugriffsschlüssel.

2. Wählen Sie **Schlüssel erstellen**.
3. Führen Sie einen der folgenden Schritte aus:
 - Wählen Sie **Verfallszeit nicht festlegen**, um einen Schlüssel zu erstellen, der nicht abläuft. (Standard)
 - Wählen Sie **Verfallszeit festlegen**, und legen Sie das Ablaufdatum und die Uhrzeit fest.



Das Ablaufdatum kann maximal fünf Jahre ab dem aktuellen Datum liegen. Die Verfallszeit kann mindestens eine Minute von der aktuellen Zeit entfernt sein.

4. Wählen Sie **Zugriffsschlüssel erstellen**.

Das Dialogfeld Zugriffsschlüssel herunterladen wird angezeigt, in dem Ihre Zugriffsschlüssel-ID und Ihr geheimer Zugriffsschlüssel aufgeführt sind.

5. Kopieren Sie die Zugriffsschlüssel-ID und den Schlüssel für den geheimen Zugriff an einen sicheren Ort, oder wählen Sie **.csv herunterladen**, um eine Tabellenkalkulationsdatei mit der Zugriffsschlüssel-ID und dem geheimen Zugriffsschlüssel zu speichern.



Schließen Sie dieses Dialogfeld erst, wenn Sie diese Informationen kopiert oder heruntergeladen haben. Sie können keine Schlüssel kopieren oder herunterladen, nachdem das Dialogfeld geschlossen wurde.

6. Wählen Sie **Fertig**.

Die neue Taste wird auf der Seite eigene Zugriffsschlüssel angezeigt.

7. Wenn Ihr Mandantenkonto über die Berechtigung **Grid Federation connection** verwenden verfügt, können Sie optional die Tenant Management API verwenden, um S3-Zugriffsschlüssel vom Mandanten im Quellraster manuell auf den Mandanten im Zielraster zu klonen. Siehe "[Klonen von S3-Zugriffsschlüsseln mithilfe der API](#)".

Die S3-Zugriffsschlüssel anzeigen

Wenn Sie einen S3-Mandanten verwenden und über die verfügen "[Entsprechende Berechtigung](#)", Sie können eine Liste Ihrer S3-Zugriffsschlüssel anzeigen. Sie können die Liste nach Ablauf der Zeit sortieren, sodass Sie feststellen können, welche Schlüssel bald ablaufen. Nach Bedarf können Sie "[Erstellen Sie neue Schlüssel](#)" Oder "[Schlüssel löschen](#)" Die Sie nicht mehr verwenden.



Sie können auf die S3-Buckets und Objekte aus Ihrem Konto zugreifen, indem Sie die Zugriffsschlüssel-ID und den geheimen Zugriffsschlüssel verwenden, die für Ihr Konto im Mandanten-Manager angezeigt werden. Aus diesem Grund schützen Sie Zugriffsschlüssel wie ein Passwort. Drehen Sie regelmäßig Zugriffsschlüssel, entfernen Sie alle nicht verwendeten Schlüssel aus Ihrem Konto und teilen Sie sie niemals mit anderen Benutzern.

Bevor Sie beginnen

- Sie sind mit einem beim Mandantenmanager angemeldet "[Unterstützter Webbrowser](#)".
- Sie gehören einer Benutzergruppe an, die über die eigenen S3-Anmeldeinformationen verwalten verfügt "[Berechtigung](#)".

Schritte

1. Wählen Sie **STORAGE (S3) > Meine Zugriffsschlüssel** aus.
2. Sortieren Sie auf der Seite Meine Zugriffsschlüssel alle vorhandenen Zugriffsschlüssel nach **Ablaufzeit** oder **Zugriffsschlüssel-ID**.
3. Erstellen Sie nach Bedarf neue Schlüssel oder löschen Sie alle Schlüssel, die Sie nicht mehr verwenden.

Wenn Sie neue Schlüssel erstellen, bevor die vorhandenen Schlüssel ablaufen, können Sie mit der Verwendung der neuen Schlüssel beginnen, ohne vorübergehend den Zugriff auf die Objekte im Konto zu verlieren.

Abgelaufene Schlüssel werden automatisch entfernt.

Löschen Ihrer eigenen S3-Zugriffsschlüssel

Wenn Sie einen S3-Mandanten verwenden und über die entsprechenden Berechtigungen verfügen, können Sie Ihre eigenen S3-Zugriffsschlüssel löschen. Nach dem Löschen eines Zugriffsschlüssels kann dieser nicht mehr für den Zugriff auf die Objekte und Buckets im Mandantenkonto verwendet werden.

Bevor Sie beginnen

- Sie sind mit einem beim Mandantenmanager angemeldet "[Unterstützter Webbrowser](#)".
- Sie haben die "[Management Ihrer eigenen S3-Berechtigungsnachweise](#)".



Sie können auf die S3-Buckets und Objekte aus Ihrem Konto zugreifen, indem Sie die Zugriffsschlüssel-ID und den geheimen Zugriffsschlüssel verwenden, die für Ihr Konto im Mandanten-Manager angezeigt werden. Aus diesem Grund schützen Sie Zugriffsschlüssel wie ein Passwort. Drehen Sie regelmäßig Zugriffsschlüssel, entfernen Sie alle nicht verwendeten Schlüssel aus Ihrem Konto und teilen Sie sie niemals mit anderen Benutzern.

Schritte

1. Wählen Sie **STORAGE (S3) > Meine Zugriffsschlüssel** aus.
2. Aktivieren Sie auf der Seite Meine Zugriffsschlüssel das Kontrollkästchen für jeden Zugriffsschlüssel, den Sie entfernen möchten.
3. Wählen Sie * Taste löschen*.
4. Wählen Sie im Bestätigungsdialogfeld **Delete key**.

In der oberen rechten Ecke der Seite wird eine Bestätigungsmeldung angezeigt.

Erstellen Sie die S3-Zugriffstasten eines anderen Benutzers

Wenn Sie einen S3-Mandanten verwenden und über die entsprechenden Berechtigungen verfügen, können Sie S3-Zugriffsschlüssel für andere Benutzer erstellen, beispielsweise Applikationen, die Zugriff auf Buckets und Objekte benötigen.

Bevor Sie beginnen

- Sie sind mit einem beim Mandantenmanager angemeldet "[Unterstützter Webbrowser](#)".
- Sie gehören einer Benutzergruppe an, die über den verfügt "[Root-Zugriffsberechtigung](#)".

Über diese Aufgabe

Sie können einen oder mehrere S3-Zugriffsschlüssel für andere Benutzer erstellen und managen, damit sie Buckets für ihr Mandantenkonto erstellen und verwalten können. Nachdem Sie einen neuen Zugriffsschlüssel erstellt haben, aktualisieren Sie die Anwendung mit der neuen Zugriffsschlüssel-ID und dem geheimen Zugriffsschlüssel. Erstellen Sie aus Sicherheitsgründen nicht mehr Schlüssel als der Benutzer benötigt, und löschen Sie die Schlüssel, die nicht verwendet werden. Wenn Sie nur einen Schlüssel haben und demnächst ablaufen, erstellen Sie einen neuen Schlüssel, bevor der alte Schlüssel abläuft, und löschen Sie dann den alten Schlüssel.

Jeder Schlüssel kann eine bestimmte Ablaufzeit haben oder keinen Ablauf haben. Beachten Sie die folgenden Richtlinien für die Ablaufzeit:

- Legen Sie eine Ablaufzeit für die Schlüssel fest, um den Zugriff des Benutzers auf einen bestimmten

Zeitraum zu beschränken. Durch das Festlegen einer kurzen Ablaufzeit kann das Risiko verringert werden, wenn die Zugriffsschlüssel-ID und der geheime Zugriffsschlüssel versehentlich ausgesetzt sind. Abgelaufene Schlüssel werden automatisch entfernt.

- Wenn das Sicherheitsrisiko in Ihrer Umgebung gering ist und Sie keine periodischen neuen Schlüssel erstellen müssen, müssen Sie keine Ablaufzeit für die Schlüssel festlegen. Wenn Sie sich zu einem späteren Zeitpunkt für die Erstellung neuer Schlüssel entscheiden, löschen Sie die alten Schlüssel manuell.



Auf die S3-Buckets und Objekte, die zu einem Benutzer gehören, kann über die Zugriffsschlüssel-ID und den geheimen Zugriffsschlüssel zugegriffen werden, die für diesen Benutzer im Mandanten-Manager angezeigt werden. Aus diesem Grund schützen Sie Zugriffsschlüssel wie ein Passwort. Drehen Sie die Zugriffstasten regelmäßig, entfernen Sie alle nicht verwendeten Schlüssel aus dem Konto und geben Sie sie niemals anderen Benutzern zur Verfügung.

Schritte

1. Wählen Sie **ZUGRIFFSVERWALTUNG > Benutzer**.
2. Wählen Sie den Benutzer aus, dessen S3-Zugriffsschlüssel Sie managen möchten.

Die Seite mit den Benutzerdetails wird angezeigt.

3. Wählen Sie **Zugriffstasten**, und wählen Sie dann **Schlüssel erstellen**.
4. Führen Sie einen der folgenden Schritte aus:
 - Wählen Sie **Keine Ablaufzeit einstellen**, um einen Schlüssel zu erstellen, der nicht abläuft. (Standard)
 - Wählen Sie **Verfallszeit festlegen**, und legen Sie das Ablaufdatum und die Uhrzeit fest.



Das Ablaufdatum kann maximal fünf Jahre ab dem aktuellen Datum liegen. Die Verfallszeit kann mindestens eine Minute von der aktuellen Zeit entfernt sein.

5. Wählen Sie **Zugriffsschlüssel erstellen**.

Das Dialogfeld Zugriffsschlüssel herunterladen wird angezeigt, in dem die Zugriffsschlüssel-ID und der geheime Zugriffsschlüssel aufgeführt sind.

6. Kopieren Sie die Zugriffsschlüssel-ID und den Schlüssel für den geheimen Zugriff an einen sicheren Ort, oder wählen Sie **.csv herunterladen**, um eine Tabellenkalkulationsdatei mit der Zugriffsschlüssel-ID und dem geheimen Zugriffsschlüssel zu speichern.



Schließen Sie dieses Dialogfeld erst, wenn Sie diese Informationen kopiert oder heruntergeladen haben. Sie können keine Schlüssel kopieren oder herunterladen, nachdem das Dialogfeld geschlossen wurde.

7. Wählen Sie **Fertig**.

Der neue Schlüssel wird auf der Registerkarte Zugriffsschlüssel der Seite mit den Benutzerdetails angezeigt.

8. Wenn Ihr Mandantenkonto über die Berechtigung **Grid Federation connection** verwenden verfügt, können Sie optional die Tenant Management API verwenden, um S3-Zugriffsschlüssel vom Mandanten im Quellraster manuell auf den Mandanten im Zielraster zu klonen. Siehe "[Klonen von S3-Zugriffsschlüsseln mithilfe der API](#)".

Zeigen Sie die S3-Zugriffstasten eines anderen Benutzers an

Wenn Sie einen S3-Mandanten verwenden und über die entsprechenden Berechtigungen verfügen, können Sie die S3-Zugriffsschlüssel eines anderen Benutzers anzeigen. Sie können die Liste nach Ablauf der Zeit sortieren, sodass Sie feststellen können, welche Schlüssel bald ablaufen. Nach Bedarf können Sie neue Schlüssel erstellen und Schlüssel löschen, die nicht mehr verwendet werden.

Bevor Sie beginnen

- Sie sind mit einem beim Mandantenmanager angemeldet "[Unterstützter Webbrowser](#)".
- Sie haben die "[Root-Zugriffsberechtigung](#)".



Auf die S3-Buckets und Objekte, die zu einem Benutzer gehören, kann über die Zugriffsschlüssel-ID und den geheimen Zugriffsschlüssel zugegriffen werden, die für diesen Benutzer im Mandanten-Manager angezeigt werden. Aus diesem Grund schützen Sie Zugriffsschlüssel wie ein Passwort. Drehen Sie die Zugriffstasten regelmäßig, entfernen Sie alle nicht verwendeten Schlüssel aus dem Konto und geben Sie sie niemals anderen Benutzern zur Verfügung.

Schritte

1. Wählen Sie **ZUGRIFFSVERWALTUNG > Benutzer**.
2. Wählen Sie auf der Seite Benutzer den Benutzer aus, dessen S3-Zugriffsschlüssel Sie anzeigen möchten.
3. Wählen Sie auf der Seite mit den Benutzerdetails **Zugriffstasten** aus.
4. Sortieren Sie die Tasten nach **Ablaufzeit** oder **Zugriffsschlüssel-ID**.
5. Erstellen Sie bei Bedarf neue Schlüssel und löschen Sie manuell die nicht mehr verwendeten Schlüssel.

Wenn Sie neue Schlüssel erstellen, bevor die vorhandenen Schlüssel ablaufen, kann der Benutzer mit der Verwendung der neuen Schlüssel beginnen, ohne vorübergehend den Zugriff auf die Objekte im Konto zu verlieren.

Abgelaufene Schlüssel werden automatisch entfernt.

Verwandte Informationen

["Erstellen von S3-Zugriffsschlüsseln eines anderen Benutzers"](#)

["Löschen Sie die S3-Zugriffsschlüssel eines anderen Benutzers"](#)

Löschen Sie die S3-Zugriffstasten eines anderen Benutzers

Wenn Sie einen S3-Mandanten verwenden und über die entsprechenden Berechtigungen verfügen, können Sie die S3-Zugriffsschlüssel eines anderen Benutzers löschen. Nach dem Löschen eines Zugriffsschlüssels kann dieser nicht mehr für den Zugriff auf die Objekte und Buckets im Mandantenkonto verwendet werden.

Bevor Sie beginnen

- Sie sind mit einem beim Mandantenmanager angemeldet "[Unterstützter Webbrowser](#)".
- Sie haben die "[Root-Zugriffsberechtigung](#)".



Auf die S3-Buckets und Objekte, die zu einem Benutzer gehören, kann über die Zugriffsschlüssel-ID und den geheimen Zugriffsschlüssel zugegriffen werden, die für diesen Benutzer im Mandanten-Manager angezeigt werden. Aus diesem Grund schützen Sie Zugriffsschlüssel wie ein Passwort. Drehen Sie die Zugriffstasten regelmäßig, entfernen Sie alle nicht verwendeten Schlüssel aus dem Konto und geben Sie sie niemals anderen Benutzern zur Verfügung.

Schritte

1. Wählen Sie **ZUGRIFFSVERWALTUNG > Benutzer**.
2. Wählen Sie auf der Seite Benutzer den Benutzer aus, dessen S3-Zugriffsschlüssel Sie verwalten möchten.
3. Wählen Sie auf der Seite mit den Benutzerdetails **Zugriffsschlüssel** aus, und aktivieren Sie dann das Kontrollkästchen für jeden Zugriffsschlüssel Sie möchten löschen.
4. Wählen Sie **Aktionen > Ausgewählte Taste löschen**.
5. Wählen Sie im Bestätigungsdiaologfeld **Delete key**.

In der oberen rechten Ecke der Seite wird eine Bestätigungsmeldung angezeigt.

Management von S3-Buckets

Erstellen eines S3-Buckets

Sie können im Mandanten-Manager S3-Buckets für Objektdaten erstellen.

Bevor Sie beginnen

- Sie sind mit einem beim Mandantenmanager angemeldet "[Unterstützter Webbrowser](#)".
- Sie gehören einer Benutzergruppe an, die über den Root-Zugriff oder Alle Buckets verwalten verfügt "[Berechtigung](#)". Diese Berechtigungen überschreiben die Berechtigungseinstellungen in Gruppen- oder Bucket-Richtlinien.



Berechtigungen zum Festlegen oder Ändern der S3-Objektsperrereigenschaften von Buckets oder Objekten können von erteilt werden "[Bucket-Richtlinie oder Gruppenrichtlinie](#)".

- Wenn Sie die S3-Objektsperrung für einen Bucket aktivieren möchten, hat ein Grid-Administrator die globale S3-Objektsperrung für das StorageGRID-System aktiviert, und Sie haben die Anforderungen für S3-Objektsperrbuckets und -Objekte geprüft. Siehe "[Verwenden Sie S3 Objektsperrung, um Objekte beizubehalten](#)".

Greifen Sie auf den Assistenten zu

Schritte

1. Wählen Sie **View Buckets** aus dem Dashboard, oder wählen Sie **STORAGE (S3) > Buckets**.
2. Wählen Sie **Eimer erstellen**.

Geben Sie Details ein

Schritte

1. Geben Sie Details für den Bucket ein.

Feld	Beschreibung
Bucket-Name	<p>Ein Name für den Bucket, der die folgenden Regeln erfüllt:</p> <ul style="list-style-type: none"> • Jedes StorageGRID System muss eindeutig sein (nicht nur innerhalb des Mandantenkontos). • Muss DNS-konform sein. • Darf mindestens 3 und nicht mehr als 63 Zeichen enthalten. • Jedes Etikett muss mit einem Kleinbuchstaben oder einer Zahl beginnen und enden. Es können nur Kleinbuchstaben, Ziffern und Bindestriche verwendet werden. • Perioden sollten nicht in Anforderungen im virtuellen gehosteten Stil verwendet werden. Perioden verursachen Probleme bei der Überprüfung des Server-Platzhalterzertifikats. <p>Weitere Informationen finden Sie im "Dokumentation der Amazon Web Services (AWS) zu den Bucket-Benennungsregeln".</p> <p>Hinweis: Sie können den Bucket-Namen nicht ändern, nachdem Sie den Bucket erstellt haben.</p>
Region	<p>Der Bereich des Eimers.</p> <p>Der StorageGRID-Administrator managt die verfügbaren Regionen. Die Regionen eines Buckets können die Datensicherungsrichtlinie, die auf Objekte angewendet wird, beeinflussen. Standardmäßig werden alle Buckets im erstellt <code>us-east-1</code> Werden.</p> <p>Hinweis: Sie können die Region nicht ändern, nachdem Sie den Bucket erstellt haben.</p>

2. Wählen Sie **Weiter**.

Verwalten von Objekteinstellungen

Schritte

1. Aktivieren Sie optional die Objektversionierung für den Bucket.

Aktivieren Sie die Objektversionierung, wenn Sie jede Version jedes Objekts in diesem Bucket speichern möchten. Sie können dann nach Bedarf frühere Versionen eines Objekts abrufen. Sie müssen die Objektversionierung aktivieren, wenn der Bucket für die Grid-übergreifende Replizierung verwendet wird.

2. Wenn die globale S3 Object Lock-Einstellung aktiviert ist, können Sie optional S3 Object Lock für den Bucket aktivieren, um Objekte mithilfe eines WORM-Modells (Write-Once-Read-Many) zu speichern.

Aktivieren Sie die S3-Objektsperre für einen Bucket nur, wenn Objekte z. B. für eine bestimmte Zeit aufbewahrt werden müssen, um bestimmte gesetzliche Vorgaben zu erfüllen. S3 Object Lock ist eine permanente Einstellung, mit der Sie verhindern können, dass Objekte für einen festgelegten Zeitraum oder für einen unbegrenzten Zeitraum gelöscht oder überschrieben werden.



Nachdem die S3-Objektsperrung für einen Bucket aktiviert ist, kann sie nicht deaktiviert werden. Jeder mit den richtigen Berechtigungen kann diesem Bucket Objekte hinzufügen, die nicht geändert werden können. Sie können diese Objekte oder den Bucket selbst möglicherweise nicht löschen.

Wenn Sie S3 Object Lock für einen Bucket aktivieren, wird die Bucket-Versionierung automatisch aktiviert.

3. Wenn Sie **S3 Object Lock aktivieren** ausgewählt haben, aktivieren Sie optional **Default Retention** für diesen Bucket.

Wenn **Default Retention** aktiviert ist, werden neue Objekte, die dem Bucket hinzugefügt werden, automatisch vor dem Löschen oder Überschreiben geschützt. Die Einstellung **Default Retention** gilt nicht für Objekte mit eigenen Aufbewahrungsfristen.

- a. Wenn **Default Retention** aktiviert ist, geben Sie einen **Default Retention Mode** für den Bucket an.

Standardaufbewahrungsmodus	Beschreibung
Compliance	<ul style="list-style-type: none">• Das Objekt kann erst gelöscht werden, wenn das Aufbewahrungsdatum erreicht ist.• Das Aufbewahrungsdatum des Objekts kann erhöht, aber nicht verringert werden.• Das Aufbewahrungsdatum des Objekts kann erst entfernt werden, wenn dieses Datum erreicht ist.
Governance	<ul style="list-style-type: none">• Benutzer mit <code>s3:BypassGovernanceRetention</code> Berechtigung kann den verwenden <code>x-amz-bypass-governance-retention: true</code> Kopfzeile anfordern, um Aufbewahrungseinstellungen zu umgehen.• Diese Benutzer können eine Objektversion löschen, bevor das Aufbewahrungsdatum erreicht ist.• Diese Benutzer können das Aufbewahrungsdatum eines Objekts erhöhen, verringern oder entfernen.

- b. Wenn **Default Retention** aktiviert ist, geben Sie die **Default Retention Period** für den Bucket an.

Die **Default Retention Period** gibt an, wie lange neue Objekte zu diesem Bucket hinzugefügt werden sollen, beginnend mit dem Zeitpunkt, zu dem sie aufgenommen werden. Geben Sie einen Wert zwischen 1 und 36,500 Tagen oder zwischen 1 und 100 Jahren an, einschließlich.

4. Wählen Sie **Eimer erstellen**.

Der Bucket wird erstellt und der Tabelle auf der Seite Buckets hinzugefügt.

5. Wählen Sie optional **Gehe zur Seite mit den Bucket-Details** zu "[Bucket-Details anzeigen](#)" Und zusätzliche Konfiguration durchführen.

Bucket-Details anzeigen

Sie können die Buckets in Ihrem Mandantenkonto anzeigen.

Bevor Sie beginnen

- Sie sind mit einem beim Mandantenmanager angemeldet ["Unterstützter Webbrowser"](#).
- Sie gehören einer Benutzergruppe an, die über den verfügt ["Root-Zugriff, Alle Buckets verwalten oder Alle Buckets anzeigen"](#). Diese Berechtigungen überschreiben die Berechtigungseinstellungen in Gruppen- oder Bucket-Richtlinien.

Schritte

1. Wählen Sie **View Buckets** aus dem Dashboard, oder wählen Sie **STORAGE (S3) > Buckets**.

Die Seite „Buckets“ wird angezeigt.

2. Überprüfen Sie die Zusammenfassungsinformationen für jeden Bucket.

Bei Bedarf können Sie die Informationen nach einer beliebigen Spalte sortieren oder Sie können die Seite vorwärts und zurück durch die Liste blättern.



Die angezeigten Werte für Objektanzahl und verwendeter Speicherplatz sind Schätzungen. Diese Schätzungen sind vom Zeitpunkt der Aufnahme, der Netzwerkverbindung und des Node-Status betroffen. Wenn Buckets die Versionierung aktiviert ist, sind gelöschte Objektversionen in der Objektanzahl enthalten.

Spalte	Beschreibung
Name	Der eindeutige Name des Buckets, der nicht geändert werden kann.
Aktivierte Funktionen	Die Liste der Funktionen, die für den Bucket aktiviert sind.
S3-Objektsperre	Gibt an, ob S3 Object Lock für den Bucket aktiviert ist. Diese Spalte wird nur angezeigt, wenn die S3-Objektsperre für das Raster aktiviert ist. In dieser Spalte werden außerdem Informationen für alle Buckets angezeigt, die für die Konformität mit älteren Daten verwendet wurden.
Region	Der Bereich des Eimers, der nicht geändert werden kann.
Objektanzahl	Die Anzahl der Objekte in diesem Bucket. Wenn Objekte hinzugefügt oder gelöscht werden, wird dieser Wert möglicherweise nicht sofort aktualisiert. Wenn für Buckets die Versionierung aktiviert ist, sind nicht aktuelle Objektversionen in diesem Wert enthalten.
Belegten Speicherplatz	Die logische Größe aller Objekte im Bucket Die logische Größe umfasst nicht den tatsächlich benötigten Speicherplatz für replizierte oder Erasure Coding-Kopien oder für Objekt-Metadaten.
Erstellungsdatum	Datum und Uhrzeit der Erstellung des Buckets.

3. Um Details für einen bestimmten Bucket anzuzeigen, wählen Sie den Bucket-Namen aus der Tabelle aus.

Die Seite mit den Bucket-Details wird angezeigt. Auf dieser Seite können Sie die folgenden Aufgaben ausführen, wenn Sie über die erforderlichen Berechtigungen verfügen:

- Konfiguration und Management von Bucket-Optionen:
 - "ILM-Richtlinien-Tags"
 - "Management der Bucket-Konsistenz"
 - "Aktualisierung der Uhrzeit des letzten Zugriffs"
 - "Objektversionierung"
 - "S3-Objektsperre"
 - "Standardmäßige Bucket-Aufbewahrung"
- Konfigurieren Sie den Bucket-Zugriff, z. B. "[Cross-Origin Resource Sharing \(CORS\)](#)"
- "[Management von Plattform-Services](#)" (Falls dem Mandanten gestattet), einschließlich CloudMirror-Replizierung, Ereignisbenachrichtigungen und Suchintegration
- Aktivieren Sie und "[Grid-übergreifende Replizierung managen](#)" (Falls dies für den Mandanten zulässig ist) zum Replizieren von Objekten, die in diesen Bucket aufgenommen wurden, auf ein anderes StorageGRID-System
- Auf das zugreifen "[S3-Konsole](#)" Zum Verwalten der Objekte im Bucket
- "[Löschen aller Objekte in einem Bucket](#)"
- "[Löschen eines Buckets](#)" Das ist bereits leer

Anwenden eines ILM-Richtlinien-Tags auf einen Bucket

Wählen Sie ein ILM-Richtlinien-Tag aus, das auf einen Bucket angewendet werden soll, basierend auf den Anforderungen des Objekt-Storage.

Die ILM-Richtlinie steuert, wo die Objektdaten gespeichert werden und ob sie nach einem bestimmten Zeitraum gelöscht werden. Der Grid-Administrator erstellt ILM-Richtlinien und weist sie ILM-Richtlinien-Tags zu, wenn mehrere aktive Richtlinien verwendet werden.



Vermeiden Sie die häufige Neuzuweisung des Policy-Tags eines Buckets. Anderenfalls kann es zu Performance-Problemen kommen.

Bevor Sie beginnen

- Sie sind mit einem beim Mandantenmanager angemeldet "[Unterstützter Webbrowser](#)".
- Sie gehören einer Benutzergruppe an, die über den verfügt "[Root-Zugriff, Alle Buckets verwalten oder Alle Buckets anzeigen](#)". Diese Berechtigungen überschreiben die Berechtigungseinstellungen in Gruppen- oder Bucket-Richtlinien.

Schritte

1. Wählen Sie **View Buckets** aus dem Dashboard, oder wählen Sie **STORAGE (S3) > Buckets**.

Die Seite „Buckets“ wird angezeigt. Bei Bedarf können Sie die Informationen nach einer beliebigen Spalte sortieren oder Sie können die Seite vorwärts und zurück durch die Liste blättern.

2. Wählen Sie den Namen des Buckets aus, dem Sie ein ILM-Richtlinien-Tag zuweisen möchten.

Sie können auch die ILM-Richtlinien-Tag-Zuweisung für einen Bucket ändern, dem bereits eine Tag zugewiesen ist.



Die angezeigten Werte für Objektanzahl und verwendeter Speicherplatz sind Schätzungen. Diese Schätzungen sind vom Zeitpunkt der Aufnahme, der Netzwerkverbindung und des Node-Status betroffen. Wenn Buckets die Versionierung aktiviert ist, sind gelöschte Objektversionen in der Objektanzahl enthalten.

- Erweitern Sie auf der Registerkarte Bucket-Optionen das ILM-Richtlinien-Tag Akkordeon. Dieses Akkordeon wird nur angezeigt, wenn Ihr Grid-Administrator die Verwendung von benutzerdefinierten Richtlinien-Tags aktiviert hat.
- Lesen Sie die Beschreibung der einzelnen Richtlinien-Tags, um festzulegen, welches Tag auf den Bucket angewendet werden soll.



Wenn Sie das ILM-Richtlinien-Tag für einen Bucket ändern, wird eine ILM-Neubewertung aller Objekte im Bucket ausgelöst. Wenn die neue Richtlinie Objekte für eine begrenzte Zeit aufbewahrt, werden ältere Objekte gelöscht.

- Aktivieren Sie das Optionsfeld für das Tag, das Sie dem Bucket zuweisen möchten.
- Wählen Sie **Änderungen speichern**. Auf dem Bucket wird ein neuer S3-Bucket-Tag mit dem Schlüssel festgelegt `NTAP-SG-ILM-BUCKET-TAG` Und den Wert des ILM-Richtlinien-Tag-Namens.



Stellen Sie sicher, dass Ihre S3-Anwendungen das neue Bucket-Tag nicht versehentlich überschreiben oder löschen. Wenn dieses Tag beim Anwenden eines neuen TagSet auf den Bucket nicht angegeben ist, werden Objekte in dem Bucket anhand der standardmäßigen ILM-Richtlinie wiederhergestellt.



ILM-Richtlinien-Tags können nur mit der Tenant Manager- oder Tenant Manager-API festgelegt und geändert werden, wobei das ILM-Richtlinien-Tag validiert wird. Ändern Sie nicht die `NTAP-SG-ILM-BUCKET-TAG` ILM-Richtlinien-Tag mithilfe der `S3-PutBucketTagging`-API oder der `S3-DeleteBucketTagging`-API.



Das Ändern der Richtlinie-Tag, die einem Bucket zugewiesen ist, wirkt sich vorübergehend auf die Performance aus, während Objekte mithilfe der neuen ILM-Richtlinie neu bewertet werden.

Management der Bucket-Konsistenz

Mithilfe von Konsistenzwerten können Änderungen an den Bucket-Einstellungen festgelegt und ein Gleichgewicht zwischen der Verfügbarkeit der Objekte in einem Bucket und der Konsistenz dieser Objekte in verschiedenen Storage-Nodes und Standorten sichergestellt werden. Sie können die Konsistenzwerte so ändern, dass sie sich von den Standardwerten unterscheiden, damit Client-Anwendungen ihre betrieblichen Anforderungen erfüllen können.

Bevor Sie beginnen

- Sie sind mit einem beim Mandantenmanager angemeldet "[Unterstützter Webbrowser](#)".
- Sie gehören einer Benutzergruppe an, die über den verfügt "[Managen aller Buckets oder Root-Zugriffsberechtigungen](#)". Diese Berechtigungen überschreiben die Berechtigungseinstellungen in Gruppen- oder Bucket-Richtlinien.

Bucket-Konsistenzrichtlinien

Die Bucket-Konsistenz wird verwendet, um die Konsistenz von Client-Applikationen zu bestimmen, die sich auf Objekte in diesem S3 Bucket auswirken. Im Allgemeinen sollten Sie die Konsistenz **Read-after-New-write** für Ihre Buckets verwenden.

Bucket-Konsistenz ändern

Wenn die Konsistenz von **Read-after-New-write** nicht den Anforderungen der Client-Anwendung entspricht, können Sie die Konsistenz ändern, indem Sie die Bucket-Konsistenz festlegen oder den verwenden `Consistency-Control` Kopfzeile. Der `Consistency-Control` Header überschreibt die Bucket-Konsistenz.



Wenn Sie die Konsistenz eines Buckets ändern, erfüllen nur die Objekte, die nach der Änderung aufgenommen werden, die überarbeitete Einstellung.

Schritte

1. Wählen Sie **View Buckets** aus dem Dashboard, oder wählen Sie **STORAGE (S3) > Buckets**.
2. Wählen Sie den Bucket-Namen aus der Tabelle aus.

Die Seite mit den Bucket-Details wird angezeigt.

3. Wählen Sie auf der Registerkarte **Bucket options** die Option **** accordion** aus.
4. Wählen Sie eine Konsistenz für Vorgänge aus, die an den Objekten in diesem Bucket ausgeführt werden.
 - **All**: Bietet die höchste Konsistenz. Alle Nodes erhalten die Daten sofort, sonst schlägt die Anfrage fehl.
 - **Strong-global**: Garantiert Lese-nach-Schreiben-Konsistenz für alle Client-Anfragen über alle Standorte hinweg.
 - **Strong-site**: Garantiert Lese-nach-Schreiben Konsistenz für alle Client-Anfragen innerhalb einer Site.
 - **Read-after-New-write** (default): Bietet Read-after-write-Konsistenz für neue Objekte und eventuelle Konsistenz für Objektaktualisierungen. Hochverfügbarkeit und garantierte Datensicherung Empfohlen für die meisten Fälle.
 - **Verfügbar**: Bietet eventuelle Konsistenz für neue Objekte und Objekt-Updates. Verwenden Sie für S3-Buckets nur nach Bedarf (z. B. für einen Bucket mit Protokollwerten, die nur selten gelesen werden, oder für HEAD- oder GET-Vorgänge für nicht vorhandene Schlüssel). Nicht unterstützt für S3 FabricPool-Buckets.
5. Wählen Sie **Änderungen speichern**.

Was passiert, wenn Sie Bucket-Einstellungen ändern

Buckets verfügen über mehrere Einstellungen, die sich auf das Verhalten der Buckets und der Objekte in diesen Buckets auswirken.

Die folgenden Bucket-Einstellungen verwenden standardmäßig **strong**-Konsistenz. Wenn zwei oder mehr Storage-Nodes innerhalb eines Standorts nicht verfügbar sind oder ein Standort nicht verfügbar ist, sind Änderungen an diesen Einstellungen möglicherweise nicht verfügbar.

- ["Löschen von leeren Buckets im Hintergrund"](#)
- ["Zeitpunkt Des Letzten Zugriffs"](#)
- ["Bucket-Lebenszyklus"](#)

- ["Bucket-Richtlinie"](#)
- ["Bucket-Tagging"](#)
- ["Bucket-Versionierung"](#)
- ["S3-Objektsperre"](#)
- ["Bucket-Verschlüsselung"](#)



Der Konsistenzwert für Bucket-Versionierung, S3 Object Lock- und Bucket-Verschlüsselung kann nicht auf einen Wert festgelegt werden, der nicht stark konsistent ist.

Die folgenden Bucket-Einstellungen verwenden keine starke Konsistenz und weisen eine höhere Verfügbarkeit für Änderungen auf. Änderungen an diesen Einstellungen können einige Zeit dauern, bevor sie wirksam werden.

- ["Konfiguration von Plattform-Services: Benachrichtigung, Replikation oder Suchintegration"](#)
- ["CORS-Konfiguration"](#)
- [Änderung der Bucket-Konsistenz](#)



Wenn die Standardkonsistenz, die beim Ändern von Bucket-Einstellungen verwendet wird, die Anforderungen der Client-Applikation nicht erfüllt, können Sie die Konsistenz mithilfe von ändern Consistency-Control Kopfzeile für den ["S3-REST-API"](#) Oder verwenden Sie die `reducedConsistency` Oder `force` Optionen in ["Mandantenmanagement-API"](#).

Aktiviert bzw. deaktiviert Updates der letzten Zugriffszeit

Wenn Grid-Administratoren die Regeln für das Information Lifecycle Management (ILM) für ein StorageGRID-System erstellen, können sie optional angeben, dass die letzte Zugriffszeit eines Objekts verwendet wird, um zu bestimmen, ob das Objekt auf einen anderen Storage-Standort verschoben werden soll. Wenn Sie einen S3-Mandanten verwenden, können Sie diese Regeln nutzen, indem Sie Updates der letzten Zugriffszeit für die Objekte in einem S3-Bucket aktivieren.

Diese Anweisungen gelten nur für StorageGRID-Systeme, die mindestens eine ILM-Regel enthalten, die die Option **Letzte Zugriffszeit** als erweiterten Filter oder als Referenzzeit verwendet. Sie können diese Anweisungen ignorieren, wenn Ihr StorageGRID System eine solche Regel nicht enthält. Siehe ["Verwenden Sie die letzte Zugriffszeit in ILM-Regeln"](#) Entsprechende Details.

Bevor Sie beginnen

- Sie sind mit einem beim Mandantenmanager angemeldet ["Unterstützter Webbrowser"](#).
- Sie gehören einer Benutzergruppe an, die über den verfügt ["Managen aller Buckets oder Root-Zugriffsberechtigungen"](#). Diese Berechtigungen überschreiben die Berechtigungseinstellungen in Gruppen- oder Bucket-Richtlinien.

Über diese Aufgabe

Letzte Zugriffszeit ist eine der Optionen für die **Referenzzeit**-Platzierungsanweisung für eine ILM-Regel. Durch Festlegen der Referenzzeit für eine Regel auf Letzte Zugriffszeit können Grid-Administratoren festlegen, dass Objekte an bestimmten Speicherorten platziert werden, basierend auf dem Zeitpunkt, zu dem diese Objekte zuletzt abgerufen (gelesen oder angezeigt) wurden.

Um z. B. sicherzustellen, dass kürzlich angezeigte Objekte im schnelleren Storage verbleiben, kann ein Grid-Administrator eine ILM-Regel erstellen, die Folgendes angibt:

- Objekte, die im letzten Monat abgerufen wurden, sollten auf lokalen Speicherknoten verbleiben.
- Objekte, die im letzten Monat nicht abgerufen wurden, sollten an einen externen Standort verschoben werden.

Standardmäßig werden Updates zur letzten Zugriffszeit deaktiviert. Wenn Ihr StorageGRID System eine ILM-Regel enthält, die die Option **Uhrzeit des letzten Zugriffs** verwendet, und Sie möchten, dass diese Option auf Objekte in diesem Bucket angewendet wird, müssen Sie für die in dieser Regel angegebenen S3-Buckets Updates für den letzten Zugriff aktivieren.



Durch das Aktualisieren der letzten Zugriffszeit, zu der ein Objekt abgerufen wird, kann sich die StorageGRID-Performance insbesondere für kleine Objekte reduzieren.

Eine Performance-Beeinträchtigung wird durch die letzten Updates der Zugriffszeit beeinflusst, da StorageGRID jedes Mal, wenn Objekte abgerufen werden, die folgenden zusätzlichen Schritte durchführen muss:

- Aktualisieren Sie die Objekte mit neuen Zeitstempel
- Fügen Sie die Objekte zur ILM-Warteschlange hinzu, damit sie anhand aktueller ILM-Regeln und Richtlinien neu bewertet werden können

Die Tabelle fasst das Verhalten zusammen, das auf alle Objekte im Bucket angewendet wird, wenn die letzte Zugriffszeit deaktiviert oder aktiviert ist.

Art der Anfrage	Verhalten, wenn die letzte Zugriffszeit deaktiviert ist (Standard)		Verhalten, wenn die letzte Zugriffszeit aktiviert ist	
	Zeitpunkt des letzten Zugriffs aktualisiert?	Das Objekt wurde zur ILM-Auswertungswarteschlange hinzugefügt?	Zeitpunkt des letzten Zugriffs aktualisiert?	Das Objekt wurde zur ILM-Auswertungswarteschlange hinzugefügt?
Anforderung zum Abrufen eines Objekts, seiner Zugriffssteuerungsliste oder seiner Metadaten	Nein	Nein	Ja.	Ja.
Anforderung zum Aktualisieren der Metadaten eines Objekts	Ja.	Ja.	Ja.	Ja.

Anforderung zum Kopieren eines Objekts von einem Bucket in einen anderen	<ul style="list-style-type: none"> • Nein, für die Quellkopie • Ja, für die Zielkopie 	<ul style="list-style-type: none"> • Nein, für die Quellkopie • Ja, für die Zielkopie 	<ul style="list-style-type: none"> • Ja, für die Quellkopie • Ja, für die Zielkopie 	<ul style="list-style-type: none"> • Ja, für die Quellkopie • Ja, für die Zielkopie
Anforderung zum Abschließen eines mehrteiligen Uploads	Ja, für das zusammengesetzte Objekt	Ja, für das zusammengesetzte Objekt	Ja, für das zusammengesetzte Objekt	Ja, für das zusammengesetzte Objekt

Schritte

1. Wählen Sie **View Buckets** aus dem Dashboard, oder wählen Sie **STORAGE (S3) > Buckets**.
2. Wählen Sie den Bucket-Namen aus der Tabelle aus.

Die Seite mit den Bucket-Details wird angezeigt.

3. Wählen Sie auf der Registerkarte **Bucket options** das Akkordeon **Letzte Zugriffszeit-Updates** aus.
4. Aktivieren oder deaktivieren Sie die Zeitaktualisierungen für den letzten Zugriff.
5. Wählen Sie **Änderungen speichern**.

Ändern Sie die Objektversionierung für einen Bucket

Wenn Sie einen S3-Mandanten verwenden, können Sie den Versionsstatus für S3-Buckets ändern.

Bevor Sie beginnen

- Sie sind mit einem beim Mandantenmanager angemeldet "[Unterstützter Webbrowser](#)".
- Sie gehören einer Benutzergruppe an, die über den verfügt "[Managen aller Buckets oder Root-Zugriffsberechtigungen](#)". Diese Berechtigungen überschreiben die Berechtigungseinstellungen in Gruppen- oder Bucket-Richtlinien.
- Alle Storage-Nodes sind verfügbar.

Über diese Aufgabe

Sie können die Objektversionierung für einen Bucket aktivieren oder aussetzen. Nachdem Sie die Versionierung für einen Bucket aktiviert haben, kann dieser nicht in den Status „unversioniert“ zurückkehren. Sie können die Versionierung für den Bucket jedoch unterbrechen.

- Deaktiviert: Versionierung wurde noch nie aktiviert
- Aktiviert: Versionierung ist aktiviert
- Suspendiert: Die Versionierung war zuvor aktiviert und wird ausgesetzt

Weitere Informationen finden Sie im Folgenden:

- "[Objektversionierung](#)"
- "[ILM-Regeln und Richtlinien für versionierte S3-Objekte \(Beispiel 4\)](#)"
- "[So werden Objekte gelöscht](#)"

Schritte

1. Wählen Sie **View Buckets** aus dem Dashboard, oder wählen Sie **STORAGE (S3) > Buckets**.
2. Wählen Sie den Bucket-Namen aus der Tabelle aus.

Die Seite mit den Bucket-Details wird angezeigt.

3. Wählen Sie auf der Registerkarte **Bucket options** das Akkordeon **Object Versioning** aus.
4. Wählen Sie einen Versionierungsstatus für die Objekte in diesem Bucket aus.

Die Objektversionierung muss für einen Bucket aktiviert bleiben, der für die Grid-übergreifende Replizierung verwendet wurde. Wenn die S3-Objektsperre oder die ältere Compliance aktiviert ist, sind die Optionen **Objektversionierung** deaktiviert.

Option	Beschreibung
Aktivieren Sie die Versionierung	<p>Aktivieren Sie die Objektversionierung, wenn Sie jede Version jedes Objekts in diesem Bucket speichern möchten. Sie können dann nach Bedarf frühere Versionen eines Objekts abrufen.</p> <p>Objekte, die sich bereits im Bucket befanden, werden versioniert, wenn sie von einem Benutzer geändert werden.</p>
Die Versionierung unterbrechen	<p>Unterbrechen Sie die Objektversionierung, wenn Sie keine neuen Objektversionen mehr erstellen möchten. Sie können weiterhin alle vorhandenen Objektversionen abrufen.</p>

5. Wählen Sie **Änderungen speichern**.

Verwenden Sie S3 Objektsperre, um Objekte beizubehalten

Sie können S3 Object Lock verwenden, wenn Buckets und Objekte die gesetzlichen Aufbewahrungsanforderungen erfüllen müssen.

Was ist S3 Object Lock?

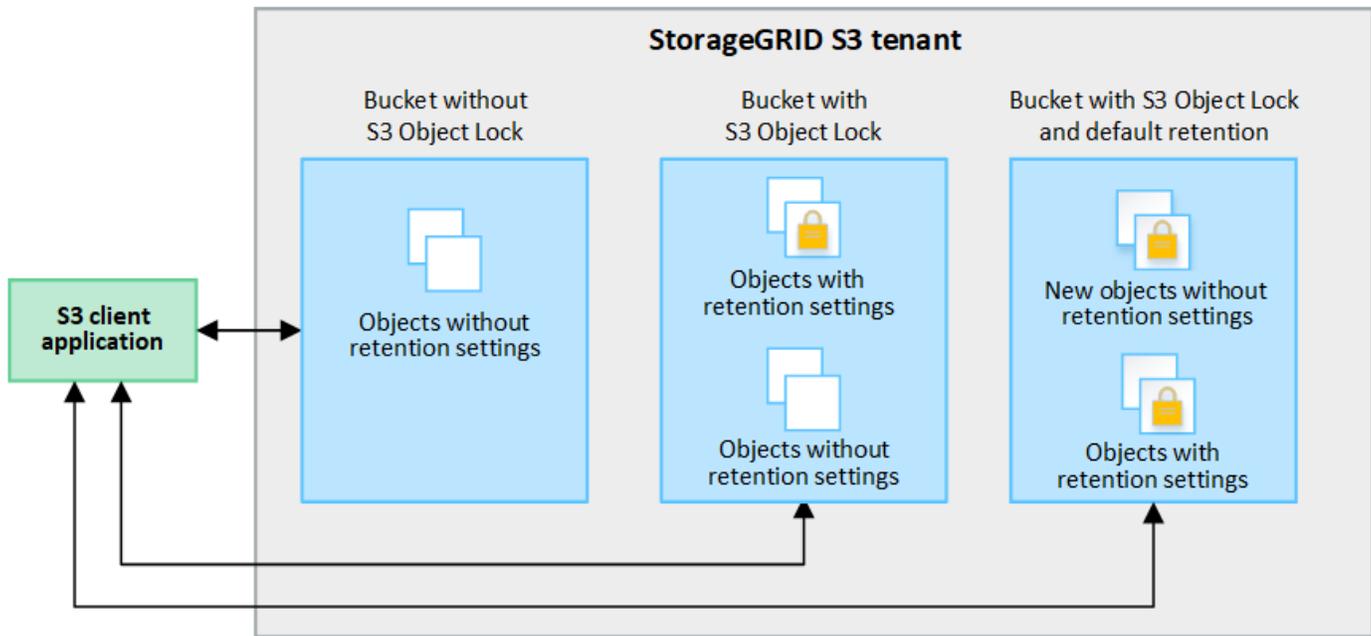
Die Funktion StorageGRID S3 Object Lock ist eine Objektschutzlösung, die der S3 Object Lock in Amazon Simple Storage Service (Amazon S3) entspricht.

Wenn die globale S3-Objektsperre für ein StorageGRID-System aktiviert ist, kann ein S3-Mandantenkonto Buckets mit oder ohne aktivierte S3-Objektsperre erstellen. Wenn für einen Bucket die S3 Object Lock aktiviert ist, ist die Bucket-Versionierung erforderlich und wird automatisch aktiviert.

Wenn für einen Bucket die S3 Object Lock aktiviert ist, können S3-Client-Applikationen optional Aufbewahrungseinstellungen für jede Objektversion angeben, die in diesem Bucket gespeichert ist.

Darüber hinaus kann für einen Bucket, auf dem die S3 Object Lock aktiviert ist, optional ein Standardaufbewahrungsmodus und ein Aufbewahrungszeitraum verwendet werden. Die Standardeinstellungen gelten nur für Objekte, die ohne eigene Aufbewahrungseinstellungen zum Bucket hinzugefügt werden.

StorageGRID with S3 Object Lock setting enabled



Aufbewahrungsmodi

Die Objektsperrefunktion StorageGRID S3 unterstützt zwei Aufbewahrungsmodi, um verschiedene Schutzstufen auf Objekte anzuwenden. Diese Modi entsprechen den Amazon S3 Aufbewahrungsmodi.

- Im Compliance-Modus:
 - Das Objekt kann erst gelöscht werden, wenn das Aufbewahrungsdatum erreicht ist.
 - Das Aufbewahrungsdatum des Objekts kann erhöht, aber nicht verringert werden.
 - Das Aufbewahrungsdatum des Objekts kann erst entfernt werden, wenn dieses Datum erreicht ist.
- Im Governance-Modus:
 - Benutzer mit besonderer Berechtigung können in Anfragen einen Überbrückungskopf verwenden, um bestimmte Aufbewahrungseinstellungen zu ändern.
 - Diese Benutzer können eine Objektversion löschen, bevor das Aufbewahrungsdatum erreicht ist.
 - Diese Benutzer können das Aufbewahrungsdatum eines Objekts erhöhen, verringern oder entfernen.

Aufbewahrungseinstellungen für Objektversionen

Wenn ein Bucket mit aktivierter S3-Objektsperre erstellt wird, können Benutzer mithilfe der S3-Client-Applikation optional die folgenden Aufbewahrungseinstellungen für jedes Objekt angeben, das dem Bucket hinzugefügt wird:

- **Retention Mode:** Entweder Compliance oder Governance.
- **Rebeat-until-date:** Wenn das Aufbewahrungsdatum einer Objektversion in der Zukunft liegt, kann das Objekt abgerufen, aber nicht gelöscht werden.
- **Legal Hold:** Die Anwendung eines gesetzlichen Hold auf eine Objektversion sperrt diesen Gegenstand sofort. Beispielsweise müssen Sie ein Objekt, das mit einer Untersuchung oder einem Rechtsstreit zusammenhängt, rechtlich festhalten. Eine gesetzliche Aufbewahrungspflicht hat kein Ablaufdatum, bleiben aber bis zur ausdrücklichen Entfernung erhalten. Die gesetzlichen Aufbewahrungspflichten sind unabhängig von der bisherigen Aufbewahrungsfrist.



Befindet sich ein Objekt unter einer Legal Hold-Funktion, kann das Objekt unabhängig vom Aufbewahrungsmodus nicht gelöscht werden.

Weitere Informationen zu den Objekteinstellungen finden Sie unter ["Konfigurieren Sie die S3-Objektsperre über die S3-REST-API"](#).

Standardeinstellung für die Aufbewahrung von Buckets

Wenn ein Bucket mit aktivierter S3-Objektsperre erstellt wurde, können Benutzer optional die folgenden Standardeinstellungen für den Bucket angeben:

- **Default Retention Mode:** Entweder Compliance oder Governance.
- **Default Retention Period:** Wie lange neue Objektversionen, die zu diesem Bucket hinzugefügt wurden, beibehalten werden sollen, beginnend mit dem Tag, an dem sie hinzugefügt werden.

Die Standard-Bucket-Einstellungen gelten nur für neue Objekte, die keine eigenen Aufbewahrungseinstellungen haben. Vorhandene Bucket-Objekte werden nicht beeinflusst, wenn Sie diese Standardeinstellungen hinzufügen oder ändern.

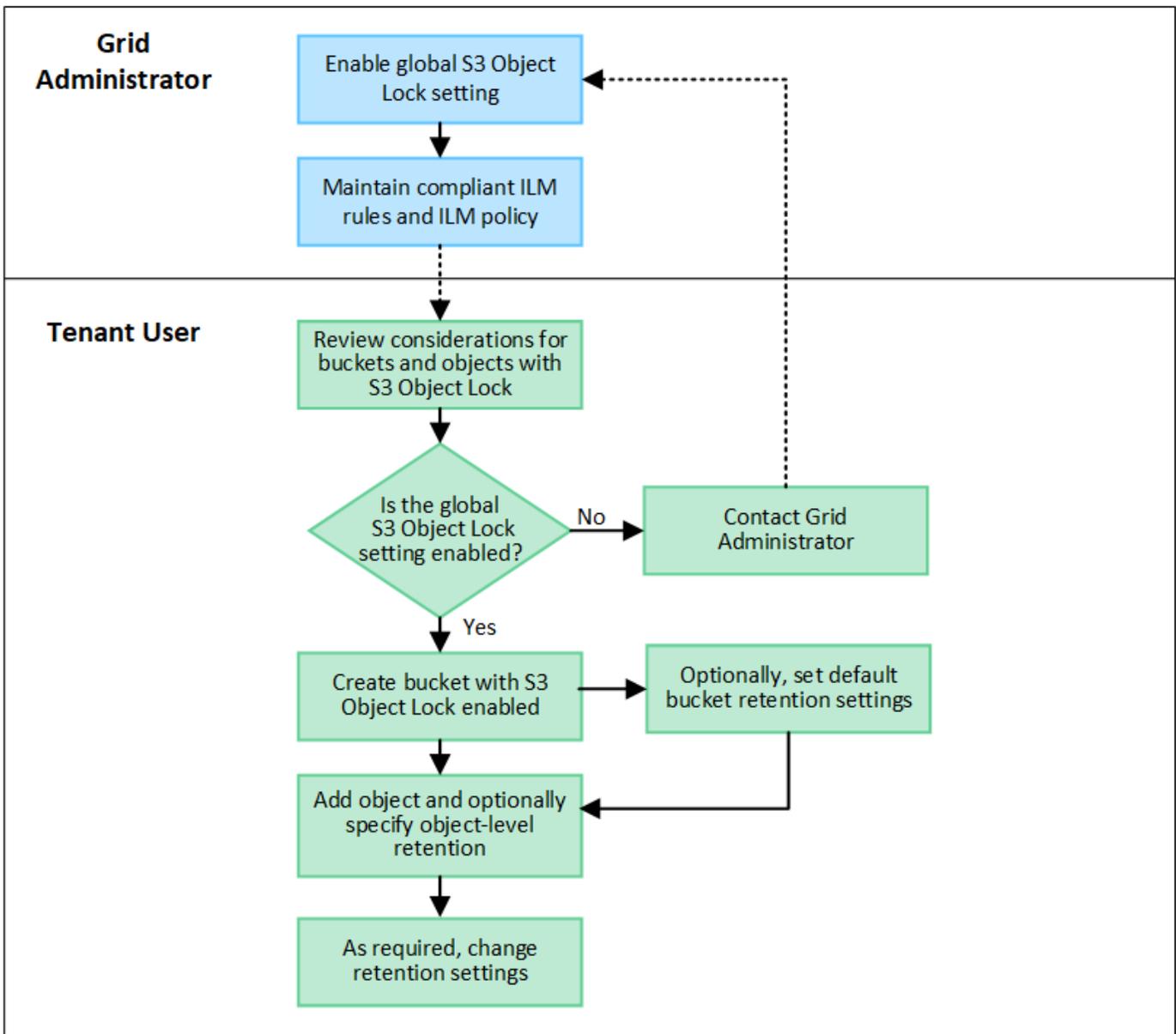
Siehe ["Erstellen eines S3-Buckets"](#) Und ["Aktualisieren Sie die S3 Object Lock-Standardaufbewahrung"](#).

S3-Objektsperre-Workflow

Das Workflow-Diagramm zeigt die grundlegenden Schritte zur Verwendung der S3-Objektsperre in StorageGRID.

Bevor Sie Buckets mit aktivierter S3-Objektsperre erstellen können, muss der Grid-Administrator die globale S3-Objektsperreinstellung für das gesamte StorageGRID-System aktivieren. Der Grid-Administrator muss außerdem sicherstellen, dass die Richtlinie für Information Lifecycle Management (ILM) „konform“ ist; er muss die Anforderungen von Buckets erfüllen, für die S3 Object Lock aktiviert ist. Weitere Informationen erhalten Sie von Ihrem Grid-Administrator oder in den Anweisungen für ["Managen von Objekten mit S3 Object Lock"](#).

Nachdem die globale S3 Object Lock-Einstellung aktiviert wurde, können Sie Buckets erstellen, für die S3 Object Lock aktiviert ist, und optional für jeden Bucket Standardaufbewahrungseinstellungen festlegen. Darüber hinaus können Sie mit der S3-Client-Anwendung optional Aufbewahrungseinstellungen für jede Objektversion angeben.



Anforderungen für Buckets, bei denen die S3-Objektsperre aktiviert ist

- Wenn die globale S3-Objektsperre für das StorageGRID System aktiviert ist, können Sie die Buckets mit aktivierter S3-Objektsperre über den Mandantenmanager, die Mandantenmanagement-API oder die S3-REST-API erstellen.
- Wenn Sie die S3-Objektsperre verwenden möchten, müssen Sie beim Erstellen des Buckets die S3-Objektsperre aktivieren. Sie können die S3-Objektsperre für einen vorhandenen Bucket nicht aktivieren.
- Wenn die S3-Objektsperre für einen Bucket aktiviert ist, ermöglicht StorageGRID automatisch die Versionierung für diesen Bucket. Sie können S3 Object Lock nicht deaktivieren oder die Versionierung für den Bucket nicht unterbrechen.
- Optional können Sie mithilfe von Tenant Manager, der Mandanten-Management-API oder der S3-REST-API für jeden Bucket einen Standardaufbewahrungsmodus und einen Aufbewahrungszeitraum angeben. Die Standardaufbewahrungseinstellungen des Buckets gelten nur für neue Objekte, die dem Bucket hinzugefügt wurden und keine eigenen Aufbewahrungseinstellungen haben. Sie können diese Standardeinstellungen außer Kraft setzen, indem Sie einen Aufbewahrungsmodus und das Aufbewahrungsdatum für jede Objektversion festlegen, wenn sie hochgeladen wird.

- Die Konfiguration des Bucket-Lebenszyklus wird für Buckets unterstützt, für die S3 Object Lock aktiviert ist.
- Die CloudMirror-Replizierung wird für Buckets nicht unterstützt, wenn S3-Objektsperre aktiviert ist.

Anforderungen für Objekte in Buckets, bei denen die S3-Objektsperre aktiviert ist

- Zum Schutz einer Objektversion können Sie Standardaufbewahrungseinstellungen für den Bucket angeben oder Aufbewahrungseinstellungen für jede Objektversion angeben. Aufbewahrungseinstellungen auf Objektebene können mit der S3-Client-Applikation oder der S3-REST-API angegeben werden.
- Aufbewahrungseinstellungen gelten für einzelne Objektversionen. Eine Objektversion kann sowohl eine Aufbewahrungsfrist als auch eine gesetzliche Haltungseinstellung haben, eine jedoch nicht die andere oder keine. Wenn Sie eine Aufbewahrungsfrist oder eine gesetzliche Aufbewahrungseinstellung für ein Objekt angeben, wird nur die in der Anforderung angegebene Version geschützt. Sie können neue Versionen des Objekts erstellen, während die vorherige Version des Objekts gesperrt bleibt.

Lebenszyklus von Objekten in Buckets, wobei S3 Objektsperre aktiviert ist

Jedes in einem Bucket gespeicherte Objekt mit aktivierter S3 Object Lock durchlaufen die folgenden Phasen:

1. Objektaufnahme

Wenn einem Bucket eine Objektversion hinzugefügt wird, für die S3 Object Lock aktiviert ist, werden die Aufbewahrungseinstellungen wie folgt angewendet:

- Wenn für das Objekt Aufbewahrungseinstellungen angegeben werden, werden die Einstellungen auf Objektebene angewendet. Alle standardmäßigen Bucket-Einstellungen werden ignoriert.
- Wenn für das Objekt keine Aufbewahrungseinstellungen angegeben sind, werden die Standard-Bucket-Einstellungen angewendet, sofern diese vorhanden sind.
- Wenn für das Objekt oder den Bucket keine Aufbewahrungseinstellungen angegeben wurden, ist das Objekt nicht durch S3 Object Lock geschützt.

Wenn Aufbewahrungseinstellungen angewendet werden, sind sowohl das Objekt als auch alle benutzerdefinierten S3-Metadaten geschützt.

2. Objektaufbewahrung und -Löschung

Von jedem geschützten Objekt werden innerhalb StorageGRID des angegebenen Aufbewahrungszeitraums mehrere Kopien gespeichert. Die genaue Anzahl und Art der Objektkopien sowie der Speicherort werden durch konforme Regeln in den aktiven ILM-Richtlinien bestimmt. Ob ein geschütztes Objekt gelöscht werden kann, bevor das Aufbewahrungsdatum erreicht ist, hängt vom Aufbewahrungsmodus ab.

- Befindet sich ein Objekt unter einer Legal Hold-Funktion, kann das Objekt unabhängig vom Aufbewahrungsmodus nicht gelöscht werden.

Kann ich auch ältere konforme Buckets verwalten?

Die S3-Objektsperre ersetzt die in früheren StorageGRID-Versionen verfügbare Compliance-Funktion. Wenn Sie mithilfe einer früheren Version von StorageGRID konforme Buckets erstellt haben, können Sie die Einstellungen dieser Buckets weiterhin verwalten. Sie können jedoch keine neuen, konformen Buckets mehr erstellen. Anweisungen hierzu finden Sie unter

["NetApp Knowledge Base: Management älterer, konformer Buckets für StorageGRID 11.5"](#).

Aktualisieren Sie die S3 Object Lock-Standardaufbewahrung

Wenn Sie beim Erstellen des Buckets die S3-Objektsperre aktiviert haben, können Sie den Bucket bearbeiten, um die Standardeinstellungen für die Aufbewahrung zu ändern. Sie können die Standardaufbewahrung aktivieren (oder deaktivieren) und einen Standardaufbewahrungsmodus und eine Standardaufbewahrungsdauer festlegen.

Bevor Sie beginnen

- Sie sind mit einem beim Mandantenmanager angemeldet "[Unterstützter Webbrowser](#)".
- Sie gehören einer Benutzergruppe an, die über den verfügt "[Managen aller Buckets oder Root-Zugriffsberechtigungen](#)". Diese Berechtigungen überschreiben die Berechtigungseinstellungen in Gruppen- oder Bucket-Richtlinien.
- S3 Objektsperre ist global für Ihr StorageGRID-System aktiviert; Sie haben S3 Objektsperre bei Erstellung des Buckets aktiviert. Siehe "[Verwenden Sie S3 Objektsperre, um Objekte beizubehalten](#)".

Schritte

1. Wählen Sie **View Buckets** aus dem Dashboard, oder wählen Sie **STORAGE (S3) > Buckets**.
2. Wählen Sie den Bucket-Namen aus der Tabelle aus.

Die Seite mit den Bucket-Details wird angezeigt.

3. Wählen Sie auf der Registerkarte **Bucket options** das Akkordeon **S3 Object Lock** aus.
4. Aktivieren oder deaktivieren Sie optional **Default Retention** für diesen Bucket.

Änderungen an dieser Einstellung gelten nicht für Objekte, die bereits im Bucket vorhanden sind, oder für Objekte, die möglicherweise eigene Aufbewahrungsfristen haben.

5. Wenn **Default Retention** aktiviert ist, geben Sie einen **Default Retention Mode** für den Bucket an.

Standardaufbewahrungsmodus	Beschreibung
Compliance	<ul style="list-style-type: none">• Das Objekt kann erst gelöscht werden, wenn das Aufbewahrungsdatum erreicht ist.• Das Aufbewahrungsdatum des Objekts kann erhöht, aber nicht verringert werden.• Das Aufbewahrungsdatum des Objekts kann erst entfernt werden, wenn dieses Datum erreicht ist.
Governance	<ul style="list-style-type: none">• Benutzer mit <code>s3:BypassGovernanceRetention</code> Berechtigung kann den verwenden <code>x-amz-bypass-governance-retention: true</code> Kopfzeile anfordern, um Aufbewahrungseinstellungen zu umgehen.• Diese Benutzer können eine Objektversion löschen, bevor das Aufbewahrungsdatum erreicht ist.• Diese Benutzer können das Aufbewahrungsdatum eines Objekts erhöhen, verringern oder entfernen.

6. Wenn **Default Retention** aktiviert ist, geben Sie die **Default Retention Period** für den Bucket an.

Die **Default Retention Period** gibt an, wie lange neue Objekte zu diesem Bucket hinzugefügt werden sollen, beginnend mit dem Zeitpunkt, zu dem sie aufgenommen werden. Geben Sie einen Wert zwischen 1 und 36,500 Tagen oder zwischen 1 und 100 Jahren an, einschließlich.

7. Wählen Sie **Änderungen speichern**.

Konfiguration der Cross-Origin Resource Sharing (CORS)

Sie können CORS (Cross-Origin Resource Sharing) für einen S3-Bucket konfigurieren, wenn Webapplikationen in anderen Domänen auf diesen Bucket und die Objekte in diesem Bucket zugreifen sollen.

Bevor Sie beginnen

- Sie sind mit einem beim Mandantenmanager angemeldet ["Unterstützter Webbrowser"](#).
- Sie gehören einer Benutzergruppe an, die über den verfügt ["Managen aller Buckets oder Root-Zugriffsberechtigungen"](#). Diese Berechtigungen überschreiben die Berechtigungseinstellungen in Gruppen- oder Bucket-Richtlinien.

Über diese Aufgabe

CORS (Cross-Origin Resource Sharing) ist ein Sicherheitsmechanismus, mit dem Client-Webanwendungen in einer Domäne auf Ressourcen in einer anderen Domäne zugreifen können. Angenommen, Sie verwenden einen S3-Bucket mit dem Namen `Images` Zum Speichern von Grafiken. Durch Konfigurieren von CORS für das `Images` Bucket: Sie können zulassen, dass die Bilder in diesem Bucket auf der Website angezeigt werden `http://www.example.com`.

CORS für einen Bucket aktivieren

Schritte

1. Verwenden Sie einen Texteditor, um die erforderliche XML zu erstellen.

Dieses Beispiel zeigt die XML, die zur Aktivierung von CORS für einen S3-Bucket verwendet wird. Mit dieser XML-Datei kann jede Domäne GET-Anforderungen an den Bucket senden, es erlaubt jedoch nur das `http://www.example.com` Domain zum Senden VON POST- und LÖSCHEN von Anfragen. Alle Anfragezeilen sind zulässig.

```

<CORSConfiguration
  xmlns="http://s3.amazonaws.com/doc/2020-10-22/">
  <CORSRule>
    <AllowedOrigin>*</AllowedOrigin>
    <AllowedMethod>GET</AllowedMethod>
    <AllowedHeader>*</AllowedHeader>
  </CORSRule>
  <CORSRule>
    <AllowedOrigin>http://www.example.com</AllowedOrigin>
    <AllowedMethod>GET</AllowedMethod>
    <AllowedMethod>POST</AllowedMethod>
    <AllowedMethod>DELETE</AllowedMethod>
    <AllowedHeader>*</AllowedHeader>
  </CORSRule>
</CORSConfiguration>

```

Weitere Informationen zur CORS-Konfigurations-XML finden Sie unter ["Amazon Web Services \(AWS\) Dokumentation: Amazon Simple Storage Service Developer Guide"](#).

2. Wählen Sie **View Buckets** aus dem Dashboard, oder wählen Sie **STORAGE (S3) > Buckets**.
3. Wählen Sie den Bucket-Namen aus der Tabelle aus.

Die Seite mit den Bucket-Details wird angezeigt.

4. Wählen Sie auf der Registerkarte **Bucket Access** das Akkordeon **Cross-Origin Resource Sharing (CORS)** aus.
5. Aktivieren Sie das Kontrollkästchen **CORS aktivieren**.
6. Fügen Sie die CORS-Konfigurations-XML in das Textfeld ein.
7. Wählen Sie **Änderungen speichern**.

CORS-Einstellung ändern

Schritte

1. Aktualisieren Sie die CORS-Konfigurations-XML im Textfeld, oder wählen Sie **Clear**, um von vorne zu beginnen.
2. Wählen Sie **Änderungen speichern**.

Deaktivieren Sie die CORS-Einstellung

Schritte

1. Deaktivieren Sie das Kontrollkästchen **CORS aktivieren**.
2. Wählen Sie **Änderungen speichern**.

Löschen von Objekten in Bucket

Sie können den Tenant Manager verwenden, um die Objekte in einem oder mehreren Buckets zu löschen.

Überlegungen und Anforderungen

Bevor Sie diese Schritte durchführen, beachten Sie Folgendes:

- Wenn Sie die Objekte in einem Bucket löschen, entfernt StorageGRID endgültig alle Objekte und alle Objektversionen in jedem ausgewählten Bucket von allen Nodes und Standorten im StorageGRID System. StorageGRID entfernt auch alle zugehörigen Objekt-Metadaten. Sie können diese Informationen nicht wiederherstellen.
- Das Löschen aller Objekte in einem Bucket kann je nach Anzahl der Objekte, Objektkopien und gleichzeitigen Vorgängen Minuten, Tage oder sogar Wochen dauern.
- Wenn ein Eimer hat "[S3-Objektsperre aktiviert](#)", Kann es im Zustand **delete objects: Read-only** für *years* bleiben.



Ein Bucket, der S3 Object Lock verwendet, bleibt im Zustand **delete Objects: Read-only**, bis das Aufbewahrungsdatum für alle Objekte erreicht ist und alle Legal Holds entfernt werden.

- Während Objekte gelöscht werden, ist der Zustand des Buckets **delete objects: Read-only**. In diesem Status können Sie dem Bucket keine neuen Objekte hinzufügen.
- Nachdem alle Objekte gelöscht wurden, verbleibt der Bucket im schreibgeschützten Status. Sie haben folgende Möglichkeiten:
 - Versetzen Sie den Bucket in den Schreibmodus und verwenden Sie ihn für neue Objekte wieder
 - Löschen Sie den Bucket
 - Belassen Sie den Bucket im schreibgeschützten Modus, um seinen Namen für eine zukünftige Verwendung zu reservieren
- Wenn für einen Bucket die Objektversionierung aktiviert ist, können Löschmarkierungen, die in StorageGRID 11.8 oder höher erstellt wurden, mithilfe der Option Objekte löschen in Bucket-Operationen entfernt werden.
- Wenn für einen Bucket die Objektversionierung aktiviert ist, entfernt der Vorgang „Objekte löschen“ keine Löschmarkierungen, die in StorageGRID 11.7 oder früher erstellt wurden. Weitere Informationen zum Löschen von Objekten in einem Bucket finden Sie unter "[Löschen von S3-versionierten Objekten](#)".
- Wenn Sie verwenden "[Grid-übergreifende Replizierung](#)", Beachten Sie Folgendes:
 - Mit dieser Option werden keine Objekte aus dem Bucket auf dem anderen Raster gelöscht.
 - Wenn Sie diese Option für den Quell-Bucket auswählen, wird die Warnung **gitterübergreifender Replikationsfehler** ausgelöst, wenn Sie dem Ziel-Bucket auf dem anderen Grid Objekte hinzufügen. Wenn Sie nicht garantieren können, dass niemand dem Bucket auf dem anderen Raster Objekte hinzufügen wird, "[Deaktivieren Sie die Grid-übergreifende Replizierung](#)" Für diesen Bucket, bevor alle Bucket-Objekte gelöscht werden.

Bevor Sie beginnen

- Sie sind mit einem beim Mandantenmanager angemeldet "[Unterstützter Webbrowser](#)".
- Sie gehören einer Benutzergruppe an, die über den verfügt "[Root-Zugriffsberechtigung](#)". Diese Berechtigung überschreibt die Berechtigungseinstellungen in Gruppen- oder Bucket-Richtlinien.

Schritte

1. Wählen Sie **View Buckets** aus dem Dashboard, oder wählen Sie **STORAGE (S3) > Buckets**.

Die Seite Buckets wird angezeigt und zeigt alle vorhandenen S3-Buckets an.

2. Verwenden Sie das Menü **Aktionen** oder die Detailseite für einen bestimmten Bucket.

Menü „Aktionen“

- a. Aktivieren Sie das Kontrollkästchen für jeden Bucket, aus dem Sie Objekte löschen möchten.
- b. Wählen Sie **actions > Delete objects in bucket**.

Detailseite

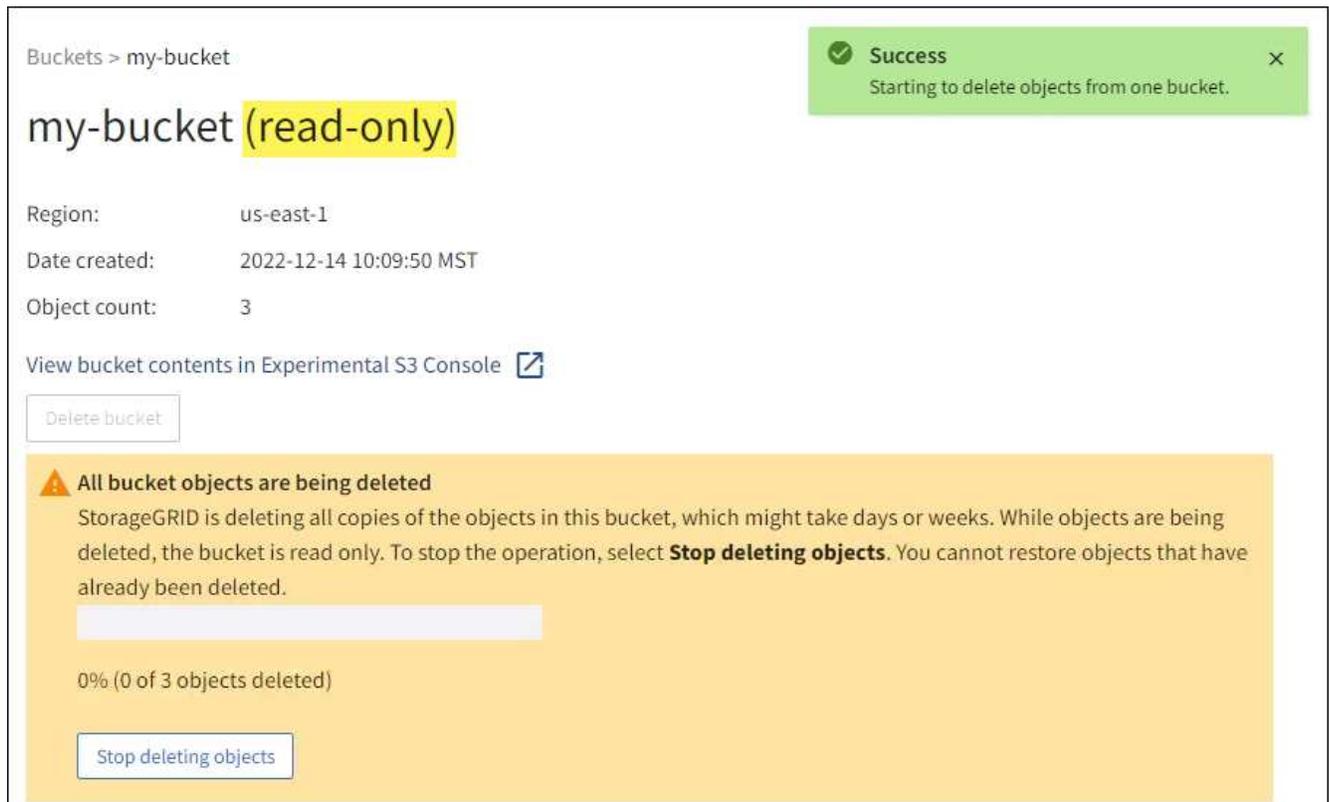
- a. Wählen Sie einen Bucket-Namen aus, um die Details anzuzeigen.
- b. Wählen Sie **Objekte im Bucket löschen**.

3. Wenn das Bestätigungsdiaologfeld angezeigt wird, überprüfen Sie die Details, geben Sie **Ja** ein und wählen Sie **OK**.

4. Warten Sie, bis der Löschvorgang beginnt.

Nach ein paar Minuten:

- Auf der Seite mit den Bucket-Details wird ein gelbes Statusbanner angezeigt. Der Fortschrittsbalken gibt an, wie viel Prozent der Objekte gelöscht wurden.
- **(read-only)** erscheint nach dem Namen des Buckets auf der Seite mit den Bucket-Details.
- **(Objekte löschen: Schreibgeschützt)** erscheint neben dem Namen des Buckets auf der Buckets-Seite.

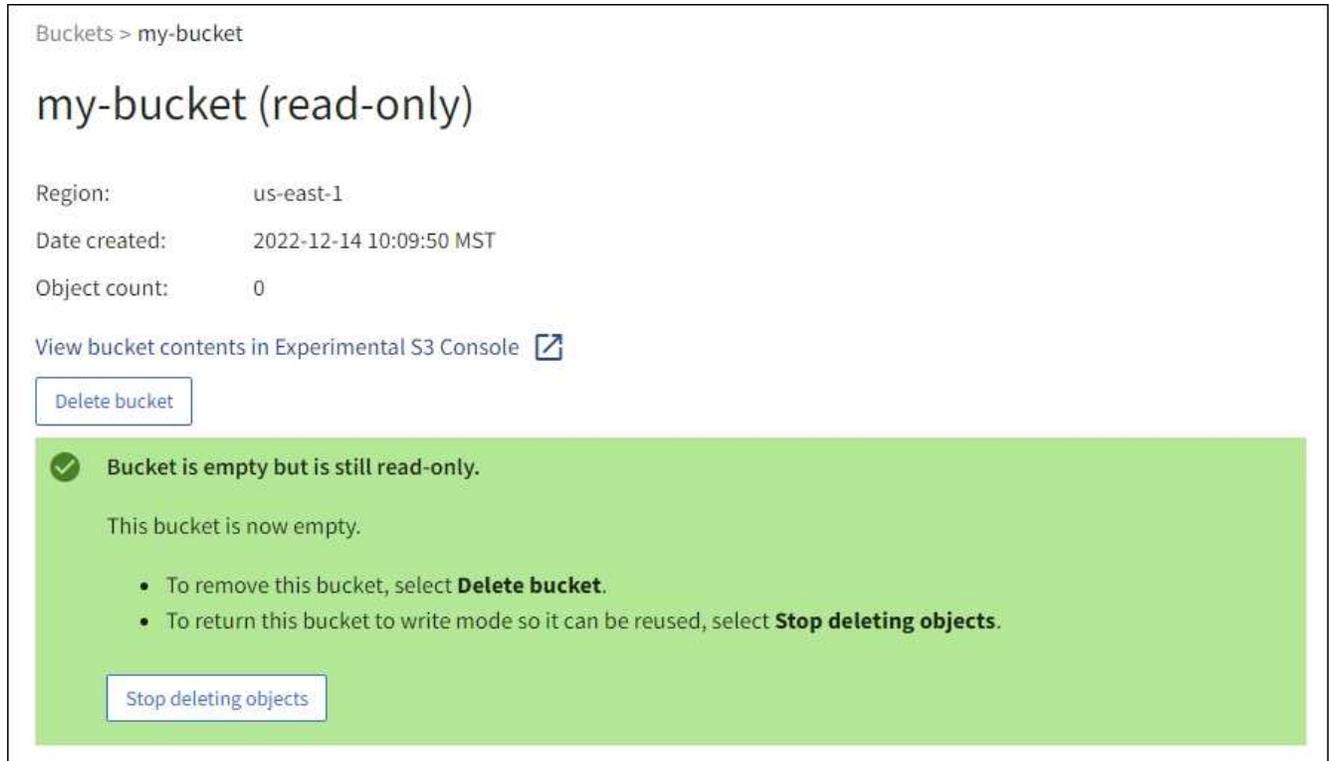


5. Wählen Sie, wie erforderlich, während der Vorgang ausgeführt wird, **Löschen von Objekten stoppen**, um den Prozess anzuhalten. Wählen Sie dann optional **Objekte im Bucket löschen** aus, um den Prozess fortzusetzen.

Wenn Sie **Löschen von Objekten stoppen** auswählen, wird der Bucket in den Schreibmodus zurückversetzt. Sie können jedoch nicht auf Objekte zugreifen oder diese wiederherstellen.

6. Warten Sie, bis der Vorgang abgeschlossen ist.

Wenn der Bucket leer ist, wird das Statusbanner aktualisiert, der Bucket bleibt jedoch weiterhin schreibgeschützt.



7. Führen Sie einen der folgenden Schritte aus:

- Schließen Sie die Seite, um den Bucket im schreibgeschützten Modus zu belassen. Beispielsweise können Sie einen leeren Bucket im schreibgeschützten Modus belassen, um den Bucket-Namen für die zukünftige Verwendung zu reservieren.
- Löschen Sie den Bucket. Sie können **Eimer löschen** auswählen, um einen einzelnen Eimer zu löschen, oder die Buckets-Seite zurücksenden und **Aktionen** > *Eimer löschen auswählen, um mehr als einen Eimer zu entfernen.



Wenn Sie einen versionierten Bucket nicht löschen können, nachdem alle Objekte gelöscht wurden, bleiben möglicherweise Löschkennzeichnungen erhalten. Um den Bucket zu löschen, müssen Sie alle verbleibenden Löschkennzeichnungen entfernen.

- Versetzen Sie den Bucket in den Schreibmodus und verwenden Sie ihn optional für neue Objekte wieder. Sie können für einen einzelnen Bucket **Stop delete objects** auswählen oder zur Buckets-Seite zurückkehren und für mehr als einen Bucket **Action** > **Stop delete objects** auswählen.

S3-Bucket löschen

Mit dem Tenant Manager können Sie eine oder mehrere leere S3-Buckets löschen.

Bevor Sie beginnen

- Sie sind mit einem beim Mandantenmanager angemeldet "[Unterstützter Webbrowser](#)".
- Sie gehören einer Benutzergruppe an, die über den verfügt "[Managen aller Buckets oder Root-Zugriffsberechtigungen](#)". Diese Berechtigungen überschreiben die Berechtigungseinstellungen in Gruppen- oder Bucket-Richtlinien.
- Die Buckets, die Sie löschen möchten, sind leer. Wenn Buckets, die Sie löschen möchten, *nicht* leer sind, "[Löschen von Objekten aus dem Bucket](#)".

Über diese Aufgabe

Diese Anweisungen beschreiben das Löschen eines S3-Buckets mithilfe von Tenant Manager. Sie können auch S3-Buckets über löschen "[Mandantenmanagement-API](#)" Oder im "[S3-REST-API](#)".

Sie können einen S3-Bucket nicht löschen, wenn er Objekte, nicht aktuelle Objektversionen enthält oder Markierungen löscht. Informationen zum Löschen von S3-versionierten Objekten finden Sie unter "[So werden Objekte gelöscht](#)".

Schritte

1. Wählen Sie **View Buckets** aus dem Dashboard, oder wählen Sie **STORAGE (S3) > Buckets**.

Die Seite Buckets wird angezeigt und zeigt alle vorhandenen S3-Buckets an.

2. Verwenden Sie das Menü **Aktionen** oder die Detailseite für einen bestimmten Bucket.

Menü „Aktionen“

- a. Aktivieren Sie das Kontrollkästchen für jeden Bucket, den Sie löschen möchten.
- b. Wählen Sie **Actions > Eimer löschen**.

Detailseite

- a. Wählen Sie einen Bucket-Namen aus, um die Details anzuzeigen.
- b. Wählen Sie **Eimer löschen**.

3. Wenn das Bestätigungsdiaologfeld angezeigt wird, wählen Sie **Ja**.

StorageGRID bestätigt, dass jeder Bucket leer ist und löscht dann jeden Bucket. Dieser Vorgang kann einige Minuten dauern.

Wenn ein Bucket nicht leer ist, wird eine Fehlermeldung angezeigt. Unbedingt "[Löschen Sie alle Objekte und alle Löschmarkierungen im Bucket](#)" Bevor Sie den Bucket löschen können.

Verwenden Sie die S3-Konsole

Mit der S3-Konsole können Sie die Objekte in einem S3-Bucket anzeigen und managen.

Mithilfe der S3-Konsole können Sie

- Hochladen, herunterladen, umbenennen, kopieren, verschieben, und Objekte löschen
- Objektversionen anzeigen, zurücksetzen, herunterladen und löschen
- Suchen Sie nach Objekten nach Präfix
- Verwalten von Objekt-Tags

- Zeigen Sie Objektmetadaten an
- Anzeigen, Erstellen, Umbenennen, Kopieren, Verschieben, und Ordner löschen

Die S3-Konsole bietet in den gängigsten Fällen eine höhere Benutzerfreundlichkeit. Es ist nicht dafür ausgelegt, CLI- oder API-Vorgänge in allen Situationen zu ersetzen.



Wenn Vorgänge durch die Verwendung von S3-Konsole zu lange dauern (z. B. Minuten oder Stunden), sollten Sie Folgendes berücksichtigen:

- Reduzieren der Anzahl ausgewählter Objekte
- Verwenden von nicht-grafischen (API oder CLI) Methoden für den Zugriff auf Ihre Daten

Bevor Sie beginnen

- Sie sind mit einem beim Mandantenmanager angemeldet "[Unterstützter Webbrowser](#)".
- Wenn Sie Objekte verwalten möchten, gehören Sie einer Benutzergruppe an, die über die Root-Zugriffsberechtigung verfügt. Alternativ gehören Sie zu einer Benutzergruppe, die über die Berechtigung zur Registerkarte „S3-Konsole verwenden“ und entweder die Berechtigung „Alle Buckets anzeigen“ oder „Alle Buckets verwalten“ verfügt. Siehe "[Mandantenmanagement-Berechtigungen](#)".
- Für den Benutzer wurde eine S3-Gruppen- oder Bucket-Richtlinie konfiguriert. Siehe "[Verwendung von Bucket- und Gruppenzugriffsrichtlinien](#)".
- Sie kennen die Zugriffsschlüssel-ID und den geheimen Zugriffsschlüssel des Benutzers. Optional haben Sie eine `.csv` Datei mit diesen Informationen. Siehe "[Anweisungen zum Erstellen von Zugriffsschlüsseln](#)".

Schritte

1. Wählen Sie **STORAGE** > **Buckets** > **bucket Name** aus.
2. Wählen Sie die Registerkarte S3-Konsole aus.
3. Fügen Sie die Zugriffsschlüssel-ID und den geheimen Zugriffsschlüssel in die Felder ein. Wählen Sie andernfalls * Zugriffsschlüssel hochladen* aus, und wählen Sie Ihr aus `.csv` Datei:
4. Wählen Sie **Anmelden**.
5. Die Tabelle der Bucket-Objekte wird angezeigt. Sie können Objekte nach Bedarf verwalten.

Weitere Informationen

- **Suche nach Präfix:** Die Präfix-Suche sucht nur nach Objekten, die mit einem bestimmten Wort relativ zum aktuellen Ordner beginnen. Die Suche umfasst keine Objekte, die das Wort an anderer Stelle enthalten. Diese Regel gilt auch für Objekte in Ordnern. Beispiel: Eine Suche nach `folder1/folder2/somefile-` Gibt Objekte zurück, die sich innerhalb des befinden `folder1/folder2/` Ordner und beginnen Sie mit dem Wort `somefile-`.
- **Drag & Drop:** Sie können Dateien aus dem Dateimanager Ihres Computers in die S3-Konsole ziehen und ablegen. Sie können jedoch keine Ordner hochladen.
- **Operationen für Ordner:** Wenn Sie einen Ordner verschieben, kopieren oder umbenennen, werden alle Objekte im Ordner einzeln aktualisiert, was Zeit in Anspruch nehmen kann.
- **Permanent Deletion wenn Bucket-Versionierung deaktiviert ist:** Wenn Sie ein Objekt in einem Bucket mit deaktivierter Versionierung überschreiben oder löschen, ist der Vorgang permanent. Siehe "[Ändern Sie die Objektversionierung für einen Bucket](#)".

Management von S3-Plattform-Services

Plattform-Services verwalten: Übersicht

Die StorageGRID Plattform-Services unterstützen Sie bei der Implementierung einer Hybrid-Cloud-Strategie, da Sie Ereignisbenachrichtigungen und Kopien von S3 Objekten und Objekt-Metadaten an externe Ziele senden können.

Falls die Verwendung von Plattform-Services für Ihr Mandantenkonto zulässig ist, können Sie die folgenden Services für jeden S3-Bucket konfigurieren:

Replizierung von CloudMirror

Nutzung "[StorageGRID CloudMirror Replikationsservice](#)" So spiegeln Sie bestimmte Objekte aus einem StorageGRID Bucket an ein angegebenes externes Ziel:

So können Sie beispielsweise CloudMirror Replizierung verwenden, um spezifische Kundendaten in Amazon S3 zu spiegeln und anschließend AWS Services für Analysen Ihrer Daten nutzen.



Die CloudMirror-Replizierung wird nicht unterstützt, wenn im Quell-Bucket S3-Objektsperre aktiviert ist.

Benachrichtigungen

Nutzung "[Bucket-spezifische Ereignisbenachrichtigungen](#)" So senden Sie Benachrichtigungen über bestimmte Aktionen, die an Objekten ausgeführt werden, an einen bestimmten externen Amazon Simple Notification Service (Amazon SNS).

Beispielsweise können Sie Warnmeldungen so konfigurieren, dass sie an Administratoren über jedes Objekt, das einem Bucket hinzugefügt wurde, gesendet werden, wo die Objekte Protokolldateien darstellen, die mit einem kritischen Systemereignis verbunden sind.



Obwohl die Ereignisbenachrichtigung für einen Bucket konfiguriert werden kann, bei dem S3 Object Lock aktiviert ist, werden die S3 Object Lock Metadaten (einschließlich „Aufbewahrung bis Datum“ und „Legal Hold“-Status) der Objekte in den Benachrichtigungsmeldungen nicht enthalten.

Suchintegrations-Service

Verwenden Sie die "[suchintegrations-Service](#)" Senden von S3-Objektmetadaten an einen angegebenen Elasticsearch-Index, bei dem die Metadaten über den externen Service durchsucht oder analysiert werden können.

Sie könnten beispielsweise die Buckets konfigurieren, um S3 Objekt-Metadaten an einen Remote-Elasticsearch-Service zu senden. Anschließend kann Elasticsearch verwendet werden, um nach Buckets zu suchen und um anspruchsvolle Analysen der Muster in den Objektmetadaten durchzuführen.



Die Elasticsearch-Integration kann auf einem Bucket konfiguriert werden, bei dem die S3-Objektsperre aktiviert ist, aber die S3-Objektsperremetadaten (einschließlich Aufbewahrung bis Datum und Status der Aufbewahrung) der Objekte werden nicht in die Benachrichtigungen einbezogen.

Da der Zielspeicherort für Plattformservices normalerweise außerhalb Ihrer StorageGRID-Implementierung liegt, erhalten Sie bei Plattform-Services die Leistung und Flexibilität, die sich aus der Nutzung externer Storage-Ressourcen, Benachrichtigungsservices und Such- oder Analyseservices für Ihre Daten ergibt.

Jede Kombination von Plattform-Services kann für einen einzelnen S3-Bucket konfiguriert werden. Beispielsweise könnten Sie sowohl den CloudMirror-Service als auch Benachrichtigungen über einen StorageGRID S3-Bucket konfigurieren, damit Sie bestimmte Objekte auf den Amazon Simple Storage Service spiegeln können, während Sie gleichzeitig eine Benachrichtigung über jedes einzelne Objekt an eine Monitoring-Applikation eines Drittanbieters senden können, um Ihre AWS-Ausgaben zu verfolgen.



Die Nutzung von Plattformdiensten muss für jedes Mandantenkonto durch einen StorageGRID-Administrator aktiviert werden, der den Grid Manager oder die Grid Management API verwendet.

Die Konfiguration von Plattform-Services

Plattform-Services kommunizieren mit externen Endpunkten, die Sie über das konfigurieren "[Mandanten-Manager](#)" Oder im "[Mandantenmanagement-API](#)". Jeder Endpunkt stellt ein externes Ziel dar, z. B. einen StorageGRID S3-Bucket, einen Amazon Web Services-Bucket, ein Amazon SNS-Thema oder ein lokal auf AWS oder anderswo gehostetes Elasticsearch-Cluster.

Nachdem Sie einen externen Endpunkt erstellt haben, können Sie einen Plattformdienst für einen Bucket aktivieren, indem Sie dem Bucket eine XML-Konfiguration hinzufügen. Die XML-Konfiguration identifiziert die Objekte, auf denen der Bucket handeln soll, die Aktion, die der Bucket durchführen sollte, und den Endpunkt, den der Bucket für den Service verwenden sollte.

Sie müssen für jeden Plattformdienst, den Sie konfigurieren möchten, separate XML-Konfigurationen hinzufügen. Beispiel:

- Wenn Sie alle Objekte wünschen, mit denen die Tasten beginnen /images Um in einen Amazon S3-Bucket repliziert werden zu können, müssen Sie dem Quell-Bucket eine Replizierungskonfiguration hinzufügen.
- Wenn Sie auch Benachrichtigungen senden möchten, wenn diese Objekte im Bucket gespeichert sind, müssen Sie eine Benachrichtigungskonfiguration hinzufügen.
- Wenn Sie die Metadaten für diese Objekte indizieren möchten, müssen Sie die Konfiguration für die Metadatenbenachrichtigung hinzufügen, die zur Implementierung der Suchintegration verwendet wird.

Das Format für die Konfigurations-XML wird durch die S3-REST-APIs geregelt, die zur Implementierung von StorageGRID Plattform-Services verwendet werden:

Plattform-Service	S3-REST-API	Siehe
Replizierung von CloudMirror	<ul style="list-style-type: none"> • GetBucketReplication • PutBucketReplication 	<ul style="list-style-type: none"> • "Replizierung von CloudMirror" • "Operationen auf Buckets"
Benachrichtigungen	<ul style="list-style-type: none"> • GetBucketNotificationConfiguration • PutBucketNotificationKonfiguration 	<ul style="list-style-type: none"> • "Benachrichtigungen" • "Operationen auf Buckets"

Plattform-Service	S3-REST-API	Siehe
Integration von Suchen	<ul style="list-style-type: none"> • Konfiguration der Bucket-Metadaten-Benachrichtigungen ABRUFEN • PUT Bucket-Metadaten-Benachrichtigungskonfiguration 	<ul style="list-style-type: none"> • "Integration von Suchen" • "Benutzerdefinierte Operationen von StorageGRID"

Verwandte Informationen

["Überlegungen zu Plattformservices"](#)

CloudMirror Replikationsservice

Sie können die CloudMirror-Replizierung für einen S3-Bucket aktivieren, wenn StorageGRID bestimmte Objekte replizieren soll, die dem Bucket zu einem oder mehreren Ziel-Buckets hinzugefügt wurden.

Die CloudMirror Replizierung wird unabhängig von den aktiven ILM-Richtlinien des Grids durchgeführt. Der CloudMirror-Service repliziert Objekte, sobald sie im Quell-Bucket gespeichert werden, und liefert sie so schnell wie möglich an den Ziel-Bucket. Die Bereitstellung replizierter Objekte wird ausgelöst, wenn die Objektaufnahme erfolgreich ist.



Die CloudMirror-Replizierung weist wichtige Ähnlichkeiten und Unterschiede zur Grid-übergreifenden Replizierungsfunktion auf. Weitere Informationen finden Sie unter ["Vergleichen Sie Grid-Replizierung und CloudMirror Replizierung"](#).

Wenn Sie die CloudMirror-Replizierung für einen vorhandenen Bucket aktivieren, werden nur die neuen, zu diesem Bucket hinzugefügten Objekte repliziert. Alle vorhandenen Objekte in dem Bucket werden nicht repliziert. Um die Replizierung von vorhandenen Objekten zu erzwingen, können Sie die Metadaten des vorhandenen Objekts durch eine Objektkopie aktualisieren.



Wenn Sie zum Kopieren von Objekten an ein Amazon S3 Ziel CloudMirror Replizierung verwenden, beachten Sie, dass Amazon S3 die Größe der benutzerdefinierten Metadaten innerhalb jedes PUT-Anforderungsheaders auf 2 KB beschränkt. Wenn in einem Objekt benutzerdefinierte Metadaten größer als 2 KB sind, wird dieses Objekt nicht repliziert.

In StorageGRID können Sie die Objekte in einem einzelnen Bucket auf mehrere Ziel-Buckets replizieren. Geben Sie dazu das Ziel für jede Regel in der Replikationskonfiguration-XML an. Ein Objekt kann nicht gleichzeitig in mehr als einen Bucket repliziert werden.

Darüber hinaus können Sie die CloudMirror-Replizierung für versionierte oder nicht versionierte Buckets konfigurieren und ein versioniertes oder unversioniertes Bucket als Ziel angeben. Es können beliebige Kombinationen aus versionierten und nichtversionierten Buckets verwendet werden. Beispielsweise können Sie einen versionierten Bucket als Ziel für einen Bucket ohne Versionsangabe angeben oder umgekehrt. Zudem ist eine Replizierung zwischen nicht versionierten Buckets möglich.

Das Löschverhalten für den CloudMirror-Replikationsservice entspricht dem Löschverhalten des CRR-Dienstes (Cross Region Replication) von Amazon S3 — beim Löschen eines Objekts in einem Quell-Bucket wird niemals ein repliziertes Objekt im Ziel gelöscht. Wenn sowohl Quell- als auch Ziel-Buckets versioniert sind, wird die Löschmarkierung repliziert. Wenn der Ziel-Bucket nicht versioniert ist, wird durch das Löschen eines Objekts im Quell-Bucket der Löschmarker nicht in den Ziel-Bucket repliziert oder das Zielobjekt gelöscht.

Wenn Objekte in den Ziel-Bucket repliziert werden, kennzeichnet StorageGRID sie als „Replikate“. Ein Ziel-StorageGRID-Bucket repliziert keine als Replikate markierten Objekte erneut, sodass Sie vor versehentlichen Replikations-Loops geschützt sind. Diese Replikatmarkierung ist intern in StorageGRID und verhindert nicht, dass Sie AWS CRR verwenden, wenn Sie einen Amazon S3-Bucket als Ziel verwenden.



Die benutzerdefinierte Kopfzeile, die zum Markieren eines Replikats verwendet wird, ist `x-ntap-sg-replica`. Diese Markierung verhindert einen kaskadierenden Spiegel. StorageGRID unterstützt auch einen bidirektionalen CloudMirror zwischen zwei Grids.

Die Einzigartigkeit und Reihenfolge von Ereignissen im Ziel-Bucket ist nicht garantiert. Als Folge von Betriebsabläufen wird möglicherweise mehr als eine identische Kopie eines Quellobjekts an das Ziel übergeben, um eine erfolgreiche Bereitstellung zu gewährleisten. In seltenen Fällen entspricht die Reihenfolge der Vorgänge auf dem Ziel-Bucket nicht der Reihenfolge der Ereignisse auf dem Quell-Bucket, wenn dasselbe Objekt gleichzeitig von zwei oder mehr verschiedenen StorageGRID-Standorten aktualisiert wird.

Die CloudMirror-Replizierung wird normalerweise so konfiguriert, dass sie einen externen S3-Bucket als Ziel verwendet. Die Replizierung kann jedoch auch für eine andere StorageGRID Implementierung oder einen beliebigen S3-kompatiblen Service konfiguriert werden.

Informieren Sie sich über Benachrichtigungen für Buckets

Sie können die Ereignisbenachrichtigung für einen S3-Bucket aktivieren, wenn StorageGRID Benachrichtigungen über angegebene Ereignisse an ein Kafka-Zielcluster oder Amazon Simple Notification Service senden soll.

Das können Sie "[Konfigurieren Sie Ereignisbenachrichtigungen](#)" Durch Verknüpfung von XML für die Benachrichtigungskonfiguration mit einem Quell-Bucket. Die XML-Benachrichtigungskonfiguration folgt S3-Konventionen für die Konfiguration von Bucket-Benachrichtigungen. Das Ziel-Kafka- oder Amazon SNS-Thema wird als URN eines Endpunkts angegeben.

Ereignisbenachrichtigungen werden auf dem Quell-Bucket erstellt, wie in der Benachrichtigungskonfiguration angegeben, und werden an das Ziel übergeben. Wenn ein Ereignis, das einem Objekt zugeordnet ist, erfolgreich ist, wird eine Benachrichtigung über dieses Ereignis erstellt und für die Bereitstellung in die Warteschlange verschoben.

Die Eindeutigkeit und Bestellung von Benachrichtigungen ist nicht garantiert. Möglicherweise werden mehrere Benachrichtigungen zu einem Ereignis an das Ziel übermittelt, da die Maßnahmen zur Sicherstellung des Liefererfolgs durchgeführt werden. Da die Bereitstellung asynchron ist, entspricht die Reihenfolge der Benachrichtigungen am Ziel nicht der Reihenfolge der Ereignisse auf dem Quell-Bucket. Dies gilt insbesondere für Vorgänge, die von unterschiedlichen StorageGRID-Standorten stammen. Sie können das verwenden `sequence` Schlüssel in der Ereignismeldung, um die Reihenfolge der Ereignisse für ein bestimmtes Objekt zu bestimmen, wie in der Amazon S3-Dokumentation beschrieben.

Unterstützte Benachrichtigungen und Meldungen

StorageGRID-Ereignisbenachrichtigungen folgen der Amazon S3-API mit einigen Einschränkungen:

- Die folgenden Ereignistypen werden unterstützt:
 - `s3:ObjectCreated:*`
 - `s3:ObjectCreated:Put`
 - `s3:ObjectCreated:Post`

- s3:ObjectCreated:Copy
 - s3:ObjectCreated:CompleteMultipartUpload
 - s3:ObjectRemoved:*
 - s3:ObjectRemoved:Löschen
 - s3:ObjectRemoved>DeleteMarkerCreated
 - s3:ObjectRestore:Post
- Aus StorageGRID gesendete Ereignisbenachrichtigungen verwenden das Standard-JSON-Format, enthalten aber keine Schlüssel und verwenden bestimmte Werte für andere, wie in der Tabelle gezeigt:

Schlüsselname	Wert von StorageGRID
EventSource	sgws:s3
AwsRegion	Nicht enthalten
X-amz-id-2	Nicht enthalten
arn	urn:sgws:s3:::bucket_name

Den Suchintegrations-Service verstehen

Sie können die Integration der Suche in einen S3-Bucket aktivieren, wenn Sie einen externen Such- und Analyseservice für Ihre Objektmetadaten verwenden möchten.

Der Suchintegrations-Service ist ein benutzerdefinierter StorageGRID Service, der automatisch und asynchron S3-Objektmetadaten an einen Ziel-Endpunkt sendet, wenn ein Objekt oder seine Metadaten aktualisiert werden. Anschließend können Sie mit den vom Ziel-Service bereitgestellten Tools für die Suche, Datenanalyse, Visualisierung und maschinelles Lernen Objektdaten suchen, analysieren und daraus Erkenntnisse gewinnen.

Sie können den Such-Integrationsservice für jeden versionierten oder nicht versionierten Bucket aktivieren. Die Suchintegration wird konfiguriert, indem eine XML-Verknüpfung für die Metadatenbenachrichtigung mit dem Bucket verknüpft wird, an dem Objekte ausgeführt werden sollen, und das Ziel für die Objektmetadaten.

Benachrichtigungen werden in Form eines JSON-Dokuments mit dem Bucket-Namen, Objektnamen und Versionsnummer generiert, falls vorhanden. Jede Metadatenbenachrichtigung enthält zusätzlich zu allen Tags und Benutzer-Metadaten des Objekts einen Standardsatz an Systemmetadaten für das Objekt.



Für Tags und Benutzer-Metadaten gibt StorageGRID Daten und Nummern an Elasticsearch als Strings oder als S3-Ereignisbenachrichtigungen weiter. Um Elasticsearch so zu konfigurieren, dass diese Strings als Daten oder Zahlen interpretiert werden, befolgen Sie die Elasticsearch-Anweisungen für die dynamische Feldzuordnung und die Zuordnung von Datumsformaten. Sie müssen die dynamischen Feldzuordnungen im Index aktivieren, bevor Sie den Suchintegrationsdienst konfigurieren. Nachdem ein Dokument indiziert wurde, können Sie die Feldtypen des Dokuments im Index nicht mehr bearbeiten.

Benachrichtigungen werden generiert und in die Warteschlange für die Zustellung gestellt, wann immer:

- Ein Objekt wird erstellt.
- Ein Objekt wird gelöscht, auch wenn Objekte aus dem Vorgang der ILM-Richtlinie des Grid gelöscht werden.
- Metadaten oder Tags von Objekten werden hinzugefügt, aktualisiert oder gelöscht. Der komplette Satz an Metadaten und Tags wird immer bei Update gesendet - nicht nur die geänderten Werte.

Nachdem Sie einem Bucket die XML-Benachrichtigungskonfiguration für Metadaten hinzugefügt haben, werden Benachrichtigungen für alle neuen Objekte gesendet, die Sie erstellen, und für alle Objekte, die Sie ändern, indem Sie deren Daten, Benutzer-Metadaten oder Tags aktualisieren. Es werden jedoch keine Benachrichtigungen für Objekte gesendet, die sich bereits im Bucket befinden. Um sicherzustellen, dass Objektmetadaten für alle Objekte im Bucket an das Ziel gesendet werden, sollten Sie eines der folgenden Aktionen durchführen:

- Konfigurieren Sie den Suchintegrationsdienst unmittelbar nach dem Erstellen des Buckets und vor dem Hinzufügen von Objekten.
- Führen Sie eine Aktion für alle Objekte aus, die sich bereits im Bucket befinden, und löst eine Metadaten-Benachrichtigung aus, die an das Ziel gesendet wird.

Der StorageGRID Such-Integrationsservice unterstützt ein Elasticsearch-Cluster als Ziel. Wie bei den anderen Plattformdiensten wird das Ziel im Endpunkt angegeben, dessen URN in der Konfigurations-XML für den Dienst verwendet wird. Verwenden Sie die ["NetApp Interoperabilitäts-Matrix-Tool"](#) Um die unterstützten Versionen von Elasticsearch zu ermitteln.

Verwandte Informationen

["Konfigurations-XML für die Integration der Suche"](#)

["Objektmetadaten sind in Metadaten-Benachrichtigungen enthalten"](#)

["JSON durch den Suchintegrations-Service generiert"](#)

["Konfigurieren Sie den Suchintegrationsdienst"](#)

Überlegungen zu Plattformservices

Vor der Implementierung von Plattform-Services sollten Sie die Empfehlungen und Überlegungen zu deren Verwendung überprüfen.

Informationen zu S3 finden Sie unter ["S3-REST-API VERWENDEN"](#).

Überlegungen bei der Verwendung von Plattform-Services

Überlegungen	Details
Ziel-Endpoint-Monitoring	Sie müssen die Verfügbarkeit jedes Zielendpunkts überwachen. Wenn die Verbindung zum Zielendpunkt über einen längeren Zeitraum unterbrochen wird und ein großer Rückstand von Anfragen besteht, schlagen zusätzliche Clientanforderungen (wie Z. B. PUT-Anforderungen) an StorageGRID fehl. Sie müssen diese fehlgeschlagenen Anforderungen erneut versuchen, wenn der Endpunkt erreichbar ist.

Überlegungen	Details
Drosselung des Zielendpunkts	<p>StorageGRID kann eingehende S3-Anfragen für einen Bucket drosseln, wenn die Rate, mit der die Anforderungen gesendet werden, die Rate übersteigt, mit der der Zielendpunkt die Anforderungen empfangen kann. Eine Drosselung tritt nur auf, wenn ein Rückstand von Anfragen besteht, die auf den Zielendpunkt warten.</p> <p>Der einzige sichtbare Effekt besteht darin, dass die eingehenden S3-Anforderungen länger in Anspruch nehmen. Wenn Sie die Performance deutlich schlechter erkennen, sollten Sie die Aufnahme rate reduzieren oder einen Endpunkt mit höherer Kapazität verwenden. Falls der Rückstand von Anforderungen weiterhin wächst, scheitern Client-S3-Vorgänge (wie Z. B. PUT-Anforderungen) letztendlich.</p> <p>CloudMirror-Anforderungen sind wahrscheinlicher von der Performance des Zielendpunkts betroffen, da diese Anfragen in der Regel mehr Datentransfer beinhalten als Anfragen zur Suchintegration oder Ereignisbenachrichtigung.</p>
Bestellgarantien	<p>StorageGRID garantiert die Bestellung von Vorgängen an einem Objekt innerhalb eines Standorts. Solange sich alle Vorgänge für ein Objekt innerhalb desselben Standorts befinden, entspricht der endgültige Objektstatus (für die Replizierung) immer dem Status in StorageGRID.</p> <p>StorageGRID unternimmt alle Anstrengungen, Anfragen zu bestellen, wenn die Vorgänge an verschiedenen StorageGRID Standorten durchgeführt werden. Wenn Sie beispielsweise ein Objekt zunächst an Standort A schreiben und später dasselbe Objekt an Standort B überschreiben, ist das von CloudMirror in den Ziel-Bucket replizierte Objekt nicht garantiert, dass es sich um das neuere Objekt handelt.</p>
ILM-gesteuerte Objektlöschungen	<p>Um dem Löschverhalten von AWS CRR und Amazon Simple Notification Service anzupassen, werden CloudMirror- und Ereignisbenachrichtigungsanforderungen nicht gesendet, wenn ein Objekt im Quell-Bucket aufgrund von StorageGRID-ILM-Regeln gelöscht wird. Beispiel: Es werden keine Anfragen für CloudMirror- oder Ereignisbenachrichtigungen gesendet, wenn eine ILM-Regel ein Objekt nach 14 Tagen löscht.</p> <p>Suchintegrationsanfragen werden dagegen gesendet, wenn Objekte aufgrund von ILM gelöscht werden.</p>

Überlegungen	Details
Kafka-Endpunkte werden verwendet	<p>Bei Kafka-Endpunkten wird gegenseitiges TLS nicht unterstützt. Als Ergebnis, wenn Sie haben <code>ssl.client.auth</code> auf <code>required</code> in Ihrer Kafka-Broker-Konfiguration kann dies Probleme mit der Konfiguration von Kafka-Endpunkten verursachen.</p> <p>Für die Authentifizierung von Kafka-Endpunkten werden die folgenden Authentifizierungstypen verwendet. Diese Typen unterscheiden sich von denen, die für die Authentifizierung anderer Endpunkte verwendet werden, z. B. Amazon SNS, und erfordern Benutzernamen und Kennwort-Anmeldeinformationen.</p> <ul style="list-style-type: none"> • SASL/PLAIN • SASL/SCRAM-SHA-256 • SASL/SCRAM-SHA-512 <p>Hinweis: konfigurierte Speicher-Proxy-Einstellungen gelten nicht für Kafka-Plattform-Services-Endpunkte.</p>

Überlegungen bei der Verwendung des CloudMirror Replikationsservice

Überlegungen	Details
Replikationsstatus	StorageGRID unterstützt das nicht <code>x-amz-replication-status</code> Kopfzeile.
Objektgröße	<p>Die maximale Größe für Objekte, die vom CloudMirror-Replikationsservice in einen Ziel-Bucket repliziert werden können, beträgt 5 tib. Dies ist die gleiche wie die maximal <i>unterstützte</i> Objektgröße.</p> <p>Hinweis: Die maximale <i>recommended</i> Größe für einen einzelnen PutObject-Vorgang beträgt 5 gib (5,368,709,120 Bytes). Wenn Sie über Objekte mit einer Größe von mehr als 5 gib verfügen, verwenden Sie stattdessen mehrteilige Uploads.</p>
Bucket-Versionierung und VersionIDs	<p>Wenn die Versionierung im S3-Quell-Bucket von StorageGRID aktiviert ist, sollten Sie auch die Versionierung für den Ziel-Bucket aktivieren.</p> <p>Beachten Sie bei der Verwendung der Versionierung, dass die Bestellung von Objektversionen im Ziel-Bucket am besten ist und vom CloudMirror Service nicht garantiert wird, da Einschränkungen im S3-Protokoll bestehen.</p> <p>Hinweis: Versions-IDs für den Quell-Bucket in StorageGRID hängen nicht mit den Versions-IDs für den Ziel-Bucket zusammen.</p>

Überlegungen	Details
Tagging für Objektversionen	<p>Der CloudMirror-Dienst repliziert keine PutObjectTagging- oder DeleteObjectTagging-Anforderungen, die aufgrund von Einschränkungen im S3-Protokoll eine Versions-ID bereitstellen. Da Versions-IDs für Quelle und Ziel nicht miteinander verknüpft sind, kann nicht sichergestellt werden, dass ein Tag-Update auf eine bestimmte Versions-ID repliziert wird.</p> <p>Im Gegensatz dazu repliziert der CloudMirror-Dienst PutObjectTagging-Anfragen oder DeleteObjectTagging-Anfragen, die keine Versions-ID angeben. Diese Anforderungen aktualisieren die Tags für den aktuellen Schlüssel (oder die aktuellste Version, wenn der Bucket versioniert ist). Normale Missionen mit Tags (keine Tagging-Updates) werden ebenfalls repliziert.</p>
Mehrteilige Uploads und ETag Werte	<p>Bei der Spiegelung von Objekten, die mittels eines mehrteiligen Uploads hochgeladen wurden, bleiben die Teile vom CloudMirror-Service nicht erhalten. Als Ergebnis davon ist der ETag Der Wert für das gespiegelte Objekt unterscheidet sich vom ETag Wert des ursprünglichen Objekts.</p>
Mit SSE-C verschlüsselte Objekte (serverseitige Verschlüsselung mit vom Kunden bereitgestellten Schlüsseln)	<p>Der CloudMirror-Dienst unterstützt keine mit SSE-C verschlüsselten Objekte Wenn Sie versuchen, ein Objekt für die CloudMirror-Replikation in den Quell-Bucket aufzunehmen, und die Anforderung die SSE-C-Anfrageheader enthält, schlägt der Vorgang fehl.</p>
Bucket mit S3-Objektsperre aktiviert	<p>Wenn für die S3-Zielbucket-Replikation für CloudMirror S3 Object Lock aktiviert ist, schlägt der Versuch, die Bucket-Replikation (PutBucketReplication) zu konfigurieren, mit einem Fehler bei AccessDenied fehl.</p>

Plattform-Services-Endpunkte konfigurieren

Bevor Sie einen Plattformservice für einen Bucket konfigurieren können, müssen Sie mindestens einen Endpunkt als Ziel für den Plattformservice konfigurieren.

Der Zugriff auf Plattform-Services wird von einem StorageGRID Administrator nach Mandanten aktiviert. Um einen Endpunkt für Plattformservices zu erstellen oder zu verwenden, müssen Sie ein Mandantenbenutzer mit Berechtigungen zum Verwalten von Endpunkten oder Root-Zugriff in einem Grid sein, dessen Netzwerk so konfiguriert wurde, dass Storage-Nodes auf externe Endpunktressourcen zugreifen können. Für einen einzelnen Mandanten können Sie bis zu 500 Plattform-Services-Endpunkte konfigurieren. Weitere Informationen erhalten Sie von Ihrem StorageGRID Administrator.

Was ist ein Endpunkt für Plattformservices?

Wenn Sie einen Endpunkt für Plattformservices erstellen, geben Sie die Informationen an, die StorageGRID für den Zugriff auf das externe Ziel benötigt.

Wenn Sie beispielsweise Objekte aus einem StorageGRID-Bucket in einen Amazon S3-Bucket replizieren möchten, erstellen Sie einen Plattform-Services-Endpunkt, der die Informationen und Zugangsdaten enthält, die StorageGRID für den Zugriff auf den Ziel-Bucket auf Amazon benötigt.

Für jeden Plattformservice ist ein eigener Endpunkt erforderlich. Daher müssen Sie für jeden zu verwendenden Plattformservice mindestens einen Endpunkt konfigurieren. Nachdem Sie einen Endpunkt für Plattformservices

definiert haben, verwenden Sie den URN des Endpunkts als Ziel in der zum Aktivieren des Dienstes verwendeten Konfigurations-XML.

Sie können für mehrere Quell-Buckets denselben Endpunkt wie das Ziel verwenden. Beispielsweise könnten Sie mehrere Quell-Buckets konfigurieren, um Objektmetadaten an denselben Endpunkt für die Integration der Suchfunktion zu senden, sodass Sie Suchvorgänge über mehrere Buckets durchführen können. Sie können auch einen Quellbucket so konfigurieren, dass mehrere Endpunkte als Ziel verwendet werden. So können Sie beispielsweise Benachrichtigungen über die Objekterstellung an ein Amazon Simple Notification Service (Amazon SNS)-Thema senden und Benachrichtigungen über das Löschen von Objekten an ein zweites Amazon SNS-Thema senden.

Endpunkte für CloudMirror Replizierung

StorageGRID unterstützt Replizierungsendpunkte, die S3-Buckets darstellen. Diese Buckets können unter Umständen auf Amazon Web Services, derselben oder einer Remote-StorageGRID-Implementierung oder einem anderen Service gehostet werden.

Endpunkte für Benachrichtigungen

StorageGRID unterstützt Amazon SNS und Kafka Endpunkte. Simple Queue Service (SQS)- oder AWS Lambda-Endpunkte werden nicht unterstützt.

Bei Kafka-Endpunkten wird gegenseitiges TLS nicht unterstützt. Als Ergebnis, wenn Sie haben `ssl.client.auth` auf `required` einstellen In Ihrer Kafka-Broker-Konfiguration kann dies Probleme mit der Konfiguration von Kafka-Endpunkten verursachen.

Endpunkte für den Suchintegrations-Service

StorageGRID unterstützt Endpunkte für die Suchintegration, die Elasticsearch-Cluster darstellen. Diese Elasticsearch-Cluster können sich in einem lokalen Datacenter befinden oder in einer AWS Cloud oder an anderen Standorten gehostet werden.

Der Endpunkt der Suchintegration bezieht sich auf einen bestimmten Elasticsearch-Index und -Typ. Sie müssen den Index in Elasticsearch erstellen, bevor Sie den Endpunkt in StorageGRID erstellen, sonst schlägt die Erstellung des Endpunkts fehl. Sie müssen den Typ nicht erstellen, bevor Sie den Endpunkt erstellen. Bei Bedarf erstellt StorageGRID den Typ, wenn Objektmetadaten an den Endpunkt gesendet werden.

Verwandte Informationen

["StorageGRID verwalten"](#)

URN für Endpunkt von Plattformservices angeben

Wenn Sie einen Endpunkt für Plattformservices erstellen, müssen Sie einen eindeutigen Ressourcennamen (URN) angeben. Beim Erstellen einer Konfigurations-XML für den Plattfordienst verwenden Sie die URN als Referenz auf den Endpunkt. Der URN für jeden Endpunkt muss eindeutig sein.

StorageGRID validiert die Endpunkte der Plattformservices bei ihrer Erstellung. Bevor Sie einen Endpunkt für Plattformservices erstellen, vergewissern Sie sich, dass die im Endpunkt angegebene Ressource vorhanden ist und dass sie erreicht werden kann.

Elemente URN

Der URN für einen Endpunkt von Plattformservices muss mit beiden beginnen `arn:aws` Oder `urn:mystore`,

Wie folgt:

- Wenn der Service auf Amazon Web Services (AWS) gehostet wird, verwenden Sie `arn:aws`
- Wenn der Service auf der Google Cloud Platform (GCP) gehostet wird, verwenden Sie `arn:aws`
- Wenn der Service lokal gehostet wird, verwenden Sie `urn:mystore`

Wenn Sie beispielsweise den URN für einen CloudMirror-Endpoint angeben, der auf StorageGRID gehostet wird, kann der URN mit beginnen `urn:sgws`.

Das nächste Element des URN gibt den Typ des Plattform-Service wie folgt an:

Service	Typ
Replizierung von CloudMirror	s3
Benachrichtigungen	sns Oder kafka
Integration von Suchen	es

Wenn Sie beispielsweise weiterhin den URN für einen CloudMirror-Endpoint angeben möchten, der auf StorageGRID gehostet wird, fügen Sie hinzu `s3` Um zu erhalten `urn:sgws:s3`.

Das letzte Element des URN identifiziert die spezifische Zielressource am Ziel-URI.

Service	Bestimmte Ressource
Replizierung von CloudMirror	bucket-name
Benachrichtigungen	sns-topic-name Oder kafka-topic-name
Integration von Suchen	domain-name/index-name/type-name Hinweis: Wenn der Elasticsearch-Cluster nicht konfiguriert ist, um Indizes automatisch zu erstellen, müssen Sie den Index manuell erstellen, bevor Sie den Endpoint erstellen.

Urns für Services zum Hosten auf AWS und GCP

Für AWS und GCP-Einheiten ist der vollständige URN ein gültiger AWS ARN. Beispiel:

- CloudMirror-Replizierung:

```
arn:aws:s3:::bucket-name
```

- Benachrichtigungen:

```
arn:aws:sns:region:account-id:topic-name
```

- Integration von Suchen:

```
arn:aws:es:region:account-id:domain/domain-name/index-name/type-name
```



Für einen AWS Endpunkt zur Integration der Suchfunktion finden Sie hier `domain-name`.
Muss den Literalstring enthalten `domain/`, Wie hier gezeigt.

Urnen für vor Ort gehostete Services

Wenn Sie lokale gehostete Services anstelle von Cloud-Services nutzen, können Sie den URN auf jede Art und Weise angeben, die einen gültigen und eindeutigen URN erstellt, solange der URN die erforderlichen Elemente in der dritten und letzten Position enthält. Sie können die durch optional angezeigten Elemente leer lassen oder sie auf eine beliebige Weise angeben, die Ihnen bei der Identifizierung der Ressource und der eindeutigen URN-Funktion hilft. Beispiel:

- CloudMirror-Replizierung:

```
urn:mystore:s3:optional:optional:bucket-name
```

Für einen CloudMirror-Endpunkt, der auf StorageGRID gehostet wird, können Sie einen gültigen URN angeben, der mit `urn:sgws:` beginnt:

```
urn:sgws:s3:optional:optional:bucket-name
```

- Benachrichtigungen:

Geben Sie einen Endpunkt für den Amazon Simple Notification Service an:

```
urn:mystore:sns:optional:optional:sns-topic-name
```

Geben Sie einen Kafka-Endpunkt an:

```
urn:mystore:kafka:optional:optional:kafka-topic-name
```

- Integration von Suchen:

```
urn:mystore:es:optional:optional:domain-name/index-name/type-name
```



Für lokal gehostete Suchintegrationsendpunkte finden Sie auf `domain-name` Das Element kann eine beliebige Zeichenfolge sein, solange der URN des Endpunkts eindeutig ist.

Endpunkt für Plattformservices erstellen

Sie müssen mindestens einen Endpunkt des richtigen Typs erstellen, bevor Sie einen Plattfordienst aktivieren können.

Bevor Sie beginnen

- Sie sind mit einem beim Mandantenmanager angemeldet "[Unterstützter Webbrowser](#)".
- Die Plattformservices wurden für Ihr Mandantenkonto von einem StorageGRID-Administrator aktiviert.
- Sie gehören einer Benutzergruppe an, die über den verfügt "[Verwalten von Endpunkten oder Root-Zugriffsberechtigungen](#)".
- Die Ressource, auf die der Endpunkt der Plattformservices verweist, wurde erstellt:
 - CloudMirror Replizierung: S3 Bucket
 - Ereignisbenachrichtigung: Amazon Simple Notification Service (Amazon SNS) oder Kafka Thema
 - Suchbenachrichtigung: Elasticsearch-Index, wenn das Ziel-Cluster nicht konfiguriert ist, Indizes automatisch zu erstellen.
- Sie haben die Informationen über die Zielressource:
 - Host und Port für den Uniform Resource Identifier (URI)



Wenn Sie einen Bucket verwenden möchten, der auf einem StorageGRID-System als Endpunkt für die CloudMirror-Replizierung gehostet wird, wenden Sie sich an den Grid-Administrator, um die erforderlichen Werte zu bestimmen.

- Eindeutiger Ressourcenname (URN)

["URN für Endpunkt von Plattformservices angeben"](#)

- Authentifizierungsdaten (falls erforderlich):

Endpunkte der AWS-Integration für Suchanfragen

Für Endpunkte der AWS-Suchintegration können Sie die folgenden Anmeldedaten verwenden:

- Zugriffsschlüssel: Zugriffsschlüssel-ID und geheimer Zugriffsschlüssel
- Basic HTTP: Benutzername und Passwort
- CAP (C2S Access Portal): Temporäre Anmeldeinformationen URL, Server- und Client-Zertifikate, Clientschlüssel und eine optionale private Client-Schlüssel-Passphrase.

CloudMirror Replizierung und Amazon SNS-Endpunkte

Für die CloudMirror-Replizierung und Amazon SNS-Endpunkte können Sie die folgenden Anmeldedaten verwenden:

- Zugriffsschlüssel: Zugriffsschlüssel-ID und geheimer Zugriffsschlüssel
- CAP (C2S Access Portal): Temporäre Anmeldeinformationen URL, Server- und Client-Zertifikate, Clientschlüssel und eine optionale private Client-Schlüssel-Passphrase.

Kafka-Endpunkte

Für Kafka-Endpunkte können Sie die folgenden Anmeldeinformationen verwenden:

- SASL/PLAIN: Benutzername und Passwort
- SASL/SCRAM-SHA-256: Benutzername und Passwort
- SASL/SCRAM-SHA-512: Benutzername und Passwort

◦ Sicherheitszertifikat (bei Verwendung eines benutzerdefinierten CA-Zertifikats)

- Wenn die Elasticsearch-Sicherheitsfunktionen aktiviert sind, verfügen Sie über die Berechtigung zum Überwachen des Clusters für den Verbindungstest und entweder über die Berechtigung zum Schreibindex oder sowohl über die Index- als auch Löschindexberechtigungen für Dokumentaktualisierungen.

Schritte

1. Wählen Sie **STORAGE (S3) > Plattform-Services-Endpunkte** aus. Die Seite „Endpunkte der Plattformdienste“ wird angezeigt.
2. Wählen Sie **Endpunkt erstellen**.
3. Geben Sie einen Anzeigenamen ein, um den Endpunkt und seinen Zweck kurz zu beschreiben.

Der vom Endpunkt unterstützte Plattformservice wird neben dem Endpunktnamen angezeigt, wenn er auf der Seite Endpunkte aufgeführt wird. Sie müssen diese Informationen daher nicht in den Namen aufnehmen.

4. Geben Sie im Feld **URI** den eindeutigen Resource Identifier (URI) des Endpunkts an.

Verwenden Sie eines der folgenden Formate:

```
https://host:port  
http://host:port
```

Wenn Sie keinen Port angeben, werden die folgenden Standardports verwendet:

- Port 443 für HTTPS-URIs und Port 80 für HTTP-URIs (die meisten Endpunkte)
- Port 9092 für HTTPS- und HTTP-URIs (nur Kafka-Endpunkte)

Beispielsweise kann der URI für einen Bucket, der auf StorageGRID gehostet wird, folgende sein:

```
https://s3.example.com:10443
```

In diesem Beispiel `s3.example.com` Stellt den DNS-Eintrag für die virtuelle IP (VIP) der StorageGRID HA-Gruppe dar und `10443` Stellt den Port dar, der im Endpunkt des Load Balancer definiert ist.



Wenn dies möglich ist, sollten Sie eine Verbindung zu einer HA-Gruppe von Load-Balancing-Nodes herstellen, um einen Single Point of Failure zu vermeiden.

Auf ähnliche Weise kann der URI für einen Bucket sein, der auf AWS gehostet wird,:

```
https://s3-aws-region.amazonaws.com
```



Wenn der Endpunkt für den CloudMirror-Replikationsservice verwendet wird, fügen Sie den Bucket-Namen nicht in den URI ein. Sie fügen den Bucket-Namen in das Feld **URN** ein.

5. Geben Sie den eindeutigen Ressourcennamen (URN) für den Endpunkt ein.



Sie können die URN eines Endpunkts nicht ändern, nachdem der Endpunkt erstellt wurde.

6. Wählen Sie **Weiter**.

7. Wählen Sie einen Wert für **Authentifizierungstyp** aus.

Endpunkte der AWS-Integration für Suchanfragen

Geben Sie die Anmeldedaten für einen Endpunkt für die Integration der AWS-Suche ein oder laden Sie sie hoch.

Die von Ihnen eingegebenen Anmeldeinformationen müssen über Schreibberechtigungen für die Zielressource verfügen.

Authentifizierung styp	Beschreibung	Anmeldedaten
Anonym	Gibt anonymen Zugriff auf das Ziel. Funktioniert nur für Endpunkte, bei denen die Sicherheit deaktiviert ist.	Keine Authentifizierung.
Zugriffsschlüssel	Verwendet AWS Zugangsdaten für die Authentifizierung von Verbindungen mit dem Ziel	<ul style="list-style-type: none">• Zugriffsschlüssel-ID• Geheimer Zugriffsschlüssel
Basis-HTTP	Verwendet einen Benutzernamen und ein Passwort, um Verbindungen zum Ziel zu authentifizieren.	<ul style="list-style-type: none">• Benutzername• Passwort
KAPPE (C2S-Zugangportal)	Verwendet Zertifikate und Schlüssel zur Authentifizierung von Verbindungen zum Ziel.	<ul style="list-style-type: none">• URL für temporäre Anmeldeinformationen• Server-CA-Zertifikat (PEM-Datei-Upload)• Client-Zertifikat (PEM-Datei-Upload)• Privater Client-Schlüssel (Upload der PEM-Datei, verschlüsseltes OpenSSL-Format oder unverschlüsseltes privates Schlüsselformat)• Private Client-Schlüssel-Passphrase (optional)

CloudMirror Replizierung oder Amazon SNS-Endpunkte

Geben Sie die Anmeldeinformationen für eine CloudMirror-Replikation oder einen Amazon SNS-Endpunkt ein oder laden Sie sie hoch.

Die von Ihnen eingegebenen Anmeldeinformationen müssen über Schreibberechtigungen für die Zielressource verfügen.

Authentifizierung styp	Beschreibung	Anmeldedaten
Anonym	Gibt anonymen Zugriff auf das Ziel. Funktioniert nur für Endpunkte, bei denen die Sicherheit deaktiviert ist.	Keine Authentifizierung.
Zugriffsschlüssel	Verwendet AWS Zugangsdaten für die Authentifizierung von Verbindungen mit dem Ziel	<ul style="list-style-type: none"> • Zugriffsschlüssel-ID • Geheimer Zugriffsschlüssel
KAPPE (C2S-Zugangsportale)	Verwendet Zertifikate und Schlüssel zur Authentifizierung von Verbindungen zum Ziel.	<ul style="list-style-type: none"> • URL für temporäre Anmeldeinformationen • Server-CA-Zertifikat (PEM-Datei-Upload) • Client-Zertifikat (PEM-Datei-Upload) • Privater Client-Schlüssel (Upload der PEM-Datei, verschlüsseltes OpenSSL-Format oder unverschlüsseltes privates Schlüsselformat) • Private Client-Schlüssel-Passphrase (optional)

Kafka-Endpunkte

Geben Sie die Anmeldeinformationen für einen Kafka-Endpunkt ein oder laden Sie sie hoch.

Die von Ihnen eingegebenen Anmeldeinformationen müssen über Schreibberechtigungen für die Zielressource verfügen.

Authentifizierung styp	Beschreibung	Anmeldedaten
Anonym	Gibt anonymen Zugriff auf das Ziel. Funktioniert nur für Endpunkte, bei denen die Sicherheit deaktiviert ist.	Keine Authentifizierung.
SASL/PLAIN	Verwendet einen Benutzernamen und ein Kennwort mit Klartext, um Verbindungen zum Ziel zu authentifizieren.	<ul style="list-style-type: none"> • Benutzername • Passwort
SASL/SCRAM-SHA-256	Verwendet einen Benutzernamen und ein Kennwort mit einem Challenge-Response-Protokoll und SHA-256-Hashing, um Verbindungen zum Ziel zu authentifizieren.	<ul style="list-style-type: none"> • Benutzername • Passwort

Authentifizierung styp	Beschreibung	Anmeldedaten
SASL/SCRAM-SHA-512	Verwendet einen Benutzernamen und ein Kennwort mit einem Challenge-Response-Protokoll und SHA-512-Hashing, um Verbindungen zum Ziel zu authentifizieren.	<ul style="list-style-type: none"> • Benutzername • Passwort

Wählen Sie **Delegationsentnommene Authentifizierung verwenden** aus, wenn der Benutzername und das Passwort von einem Delegationstoken abgeleitet werden, das von einem Kafka-Cluster bezogen wurde.

- Wählen Sie **Weiter**.
- Wählen Sie eine Optionsschaltfläche für **Server überprüfen** aus, um auszuwählen, wie die TLS-Verbindung zum Endpunkt verifiziert wird.

Create endpoint ✕

✓ Enter details

✓ Select authentication type
Optional

3 Verify server
Optional

Verify server

Use this method to validate the certificate for TLS connections to the endpoint resource. If you select "Use custom CA certificate," copy and paste the custom security certificate in the text box.

Use custom CA certificate

Use operating system CA certificate

Do not verify certificate

```
-----BEGIN CERTIFICATE-----
abcdefghijklmnop123456780ABCDEFGHIJL
123456/7890ABCDEFabcdefghijklmnopABCD
-----END CERTIFICATE-----
```

Previous
Test and create endpoint

Typ der Zertifikatverifizierung	Beschreibung
Benutzerdefiniertes CA-Zertifikat verwenden	Verwenden Sie ein benutzerdefiniertes Sicherheitszertifikat. Wenn Sie diese Einstellung auswählen, kopieren Sie das benutzerdefinierte Sicherheitszertifikat in das Textfeld CA-Zertifikat .

Typ der Zertifikatverifizierung	Beschreibung
Verwenden Sie das CA-Zertifikat für das Betriebssystem	Verwenden Sie das auf dem Betriebssystem installierte Standard-Grid-CA-Zertifikat, um Verbindungen zu sichern.
Verifizieren Sie das Zertifikat nicht	Das für die TLS-Verbindung verwendete Zertifikat wird nicht verifiziert. Diese Option ist nicht sicher.

10. Wählen Sie **Test und Endpunkt erstellen**.

- Eine Erfolgsmeldung wird angezeigt, wenn der Endpunkt mit den angegebenen Anmeldeinformationen erreicht werden kann. Die Verbindung zum Endpunkt wird von einem Node an jedem Standort validiert.
- Wenn die Endpoint-Validierung fehlschlägt, wird eine Fehlermeldung angezeigt. Wenn Sie den Endpunkt ändern müssen, um den Fehler zu beheben, wählen Sie **Zurück zu Endpunktdetails** und aktualisieren Sie die Informationen. Wählen Sie anschließend **Test und Endpunkt erstellen** aus.



Die Erstellung von Endpunkten schlägt fehl, wenn Plattformdienste für Ihr Mandantenkonto nicht aktiviert sind. Wenden Sie sich an den StorageGRID-Administrator.

Nachdem Sie einen Endpunkt konfiguriert haben, können Sie mit seinem URN einen Plattformdienst konfigurieren.

Verwandte Informationen

["URN für Endpunkt von Plattformservices angeben"](#)

["CloudMirror-Replizierung konfigurieren"](#)

["Konfigurieren Sie Ereignisbenachrichtigungen"](#)

["Konfigurieren Sie den Suchintegrationsdienst"](#)

Testen der Verbindung für Endpunkt der Plattformservices

Wenn sich die Verbindung zu einem Plattformdienst geändert hat, können Sie die Verbindung für den Endpunkt testen, um zu überprüfen, ob die Zielressource existiert und ob sie mit den von Ihnen angegebenen Anmeldeinformationen erreicht werden kann.

Bevor Sie beginnen

- Sie sind mit einem beim Mandantenmanager angemeldet ["Unterstützter Webbrowser"](#).
- Sie gehören einer Benutzergruppe an, die über den verfügt ["Verwalten von Endpunkten oder Root-Zugriffsberechtigungen"](#).

Über diese Aufgabe

StorageGRID überprüft nicht, ob die Anmeldeinformationen die richtigen Berechtigungen haben.

Schritte

1. Wählen Sie **STORAGE (S3) > Plattform-Services-Endpunkte** aus.

Die Seite Endpunkte der Plattformservices wird angezeigt und zeigt die Liste der bereits konfigurierten Endpunkte der Plattformservices an.

Platform services endpoints

A platform services endpoint stores the information StorageGRID needs to use an external resource as a target for a platform service (CloudMirror replication, notifications, or search integration). You must configure an endpoint for each platform service you plan to use.

4 endpoints

Create endpoint

Delete endpoint

<input type="checkbox"/>	Display name ? ↕	Last error ? ↕	Type ? ↕	URI ? ↕	URN ? ↕
<input type="checkbox"/>	my-endpoint-1		S3 Bucket	http://10.96.104.167:10443	urn:sgws:s3:::bucket1
<input type="checkbox"/>	my-endpoint-2	✖ 2 hours ago	Search	http://10.96.104.30:9200	urn:sgws:es:::mydomain/sveloso/_doc
<input type="checkbox"/>	my-endpoint-3		Notifications	http://10.96.104.202:8080/	arn:aws:sns:us-west-2::example1
<input type="checkbox"/>	my-endpoint-4		S3 Bucket	http://10.96.104.167:10443	urn:sgws:s3:::bucket2

2. Wählen Sie den Endpunkt aus, dessen Verbindung Sie testen möchten.

Die Seite mit den Details des Endpunkts wird angezeigt.

Overview ↑

Display name: **my-endpoint-1** [✎](#)

Type: **S3 Bucket**

URI: **http://10.96.104.167:10443**

URN: **urn:sgws:s3:::bucket1**

Connection **Configuration**

Verify connection [?](#)

Some errors might continue to appear after they are resolved. To see if an error is current or to force the removal of a resolved error, select **Test connection**.

Test connection

3. Wählen Sie **Verbindung testen**.

- Eine Erfolgsmeldung wird angezeigt, wenn der Endpunkt mit den angegebenen Anmeldeinformationen erreicht werden kann. Die Verbindung zum Endpunkt wird von einem Node an jedem Standort validiert.
- Wenn die Endpoint-Validierung fehlschlägt, wird eine Fehlermeldung angezeigt. Wenn Sie den Endpunkt ändern müssen, um den Fehler zu beheben, wählen Sie **Konfiguration** und aktualisieren Sie die Informationen. Wählen Sie anschließend **Test und speichern Sie die Änderungen**.

Endpunkt der Plattformdienste bearbeiten

Sie können die Konfiguration für einen Endpunkt für Plattformdienste bearbeiten, um seinen Namen, URI oder andere Details zu ändern. Beispielsweise müssen Sie möglicherweise abgelaufene Anmeldedaten aktualisieren oder den URI so ändern, dass er zu einem Backup-Elasticsearch-Index für ein Failover weist. Sie können die URN für einen Endpunkt für Plattformdienste nicht ändern.

Bevor Sie beginnen

- Sie sind mit einem beim Mandantenmanager angemeldet "[Unterstützter Webbrowser](#)".
- Sie gehören einer Benutzergruppe an, die über den verfügt "[Verwalten von Endpunkten oder Root-Zugriffsberechtigungen](#)".

Schritte

1. Wählen Sie **STORAGE (S3) > Plattform-Services-Endpunkte** aus.

Die Seite Endpunkte der Plattformservices wird angezeigt und zeigt die Liste der bereits konfigurierten Endpunkte der Plattformservices an.

Platform services endpoints

A platform services endpoint stores the information StorageGRID needs to use an external resource as a target for a platform service (CloudMirror replication, notifications, or search integration). You must configure an endpoint for each platform service you plan to use.

4 endpoints Create endpoint

Delete endpoint

<input type="checkbox"/>	Display name ? ⬇	Last error ? ⬇	Type ? ⬇	URI ? ⬇	URN ? ⬇
<input type="checkbox"/>	my-endpoint-1		S3 Bucket	http://10.96.104.167:10443	urn:sgws:s3:::bucket1
<input type="checkbox"/>	my-endpoint-2	✖ 2 hours ago	Search	http://10.96.104.30:9200	urn:sgws:es:::mydomain/sveloso/_doc
<input type="checkbox"/>	my-endpoint-3		Notifications	http://10.96.104.202:8080/	arn:aws:sns:us-west-2::example1
<input type="checkbox"/>	my-endpoint-4		S3 Bucket	http://10.96.104.167:10443	urn:sgws:s3:::bucket2

2. Wählen Sie den Endpunkt aus, den Sie bearbeiten möchten.

Die Seite mit den Details des Endpunkts wird angezeigt.

3. Wählen Sie **Konfiguration**.

4. Ändern Sie bei Bedarf die Konfiguration des Endpunkts.



Sie können die URN eines Endpunkts nicht ändern, nachdem der Endpunkt erstellt wurde.

a. Um den Anzeigenamen für den Endpunkt zu ändern, wählen Sie das Bearbeiten-Symbol .

b. Ändern Sie bei Bedarf den URI.

c. Ändern Sie bei Bedarf den Authentifizierungstyp.

- Zur Authentifizierung des Zugriffsschlüssels ändern Sie den Schlüssel ggf. durch Auswahl von **S3-Schlüssel bearbeiten** und Einfügen einer neuen Zugriffsschlüssel-ID und eines geheimen Zugriffsschlüssels. Wenn Sie Ihre Änderungen abbrechen müssen, wählen Sie **S3-Taste Edit** rückgängig machen.
- Für die CAP-Authentifizierung (C2S Access Portal) ändern Sie die URL für temporäre Anmeldeinformationen oder die optionale private Passphrase für Clientschlüssel und laden Sie nach Bedarf neue Zertifikate und Schlüsseldateien hoch.



Der private Client-Schlüssel muss im OpenSSL-verschlüsselten Format oder unverschlüsseltem privaten Schlüssel vorliegen.

d. Ändern Sie bei Bedarf die Methode zur Überprüfung des Servers.

5. Wählen Sie **Test und speichern Sie die Änderungen**.

- Eine Erfolgsmeldung wird angezeigt, wenn der Endpunkt mit den angegebenen Anmeldeinformationen erreicht werden kann. Die Verbindung zum Endpunkt wird von einem Knoten an jedem Standort überprüft.
- Wenn die Endpoint-Validierung fehlschlägt, wird eine Fehlermeldung angezeigt. Ändern Sie den Endpunkt, um den Fehler zu beheben, und wählen Sie dann **Änderungen testen und speichern**.

Endpunkt für Plattformservices löschen

Sie können einen Endpunkt löschen, wenn Sie den zugeordneten Plattfordienst nicht mehr verwenden möchten.

Bevor Sie beginnen

- Sie sind mit einem beim Mandantenmanager angemeldet "[Unterstützter Webbrowser](#)".
- Sie gehören einer Benutzergruppe an, die über den verfügt "[Verwalten von Endpunkten oder Root-Zugriffsberechtigungen](#)".

Schritte

1. Wählen Sie **STORAGE (S3) > Plattform-Services-Endpunkte** aus.

Die Seite Endpunkte der Plattformservices wird angezeigt und zeigt die Liste der bereits konfigurierten Endpunkte der Plattformservices an.

Platform services endpoints

A platform services endpoint stores the information StorageGRID needs to use an external resource as a target for a platform service (CloudMirror replication, notifications, or search integration). You must configure an endpoint for each platform service you plan to use.

4 endpoints

Create endpoint

Delete endpoint

<input type="checkbox"/>	Display name	Last error	Type	URI	URN
<input type="checkbox"/>	my-endpoint-1		S3 Bucket	http://10.96.104.167:10443	urn:sgws:s3:::bucket1
<input type="checkbox"/>	my-endpoint-2	2 hours ago	Search	http://10.96.104.30:9200	urn:sgws:es:::mydomain/sveloso/_doc
<input type="checkbox"/>	my-endpoint-3		Notifications	http://10.96.104.202:8080/	arn:aws:sns:us-west-2::example1
<input type="checkbox"/>	my-endpoint-4		S3 Bucket	http://10.96.104.167:10443	urn:sgws:s3:::bucket2

2. Aktivieren Sie das Kontrollkästchen für jeden Endpunkt, den Sie löschen möchten.



Wenn Sie einen Endpunkt für Plattformservices löschen, der verwendet wird, wird der zugehörige Plattfordienst für alle Buckets deaktiviert, die den Endpunkt verwenden. Alle noch nicht abgeschlossenen Anfragen werden gelöscht. Neue Anfragen werden weiterhin generiert, bis Sie Ihre Bucket-Konfiguration so ändern, dass Sie nicht mehr auf den gelöschten URN verweisen. StorageGRID meldet diese Anfragen als nicht behebbare Fehler.

3. Wählen Sie **Aktionen** > **Endpunkt löschen**.

Eine Bestätigungsmeldung wird angezeigt.

Delete endpoint

Are you sure you want to delete endpoint my-endpoint-10?

This might take a few minutes.

When you delete an endpoint, you can no longer use it to access external resources.

[Cancel](#) [Delete endpoint](#)

4. Wählen Sie **Endpunkt löschen**.

Fehlerbehebung bei Endpunktfehlern bei Plattform-Services

Wenn StorageGRID versucht, mit einem Endpunkt für Plattformdienste zu kommunizieren, wird eine Meldung auf dem Dashboard angezeigt. Auf der Seite „Plattform-Services-Endpunkte“ wird in der Spalte „Letzte Fehler“ angezeigt, wie lange der Fehler bereits aufgetreten ist. Es wird kein Fehler angezeigt, wenn die Berechtigungen, die mit den Anmeldedaten eines Endpunkts verknüpft sind, falsch sind.

Ermitteln Sie, ob ein Fehler aufgetreten ist

Wenn in den letzten 7 Tagen Fehler am Endpunkt der Plattformdienste aufgetreten sind, zeigt das Mandantenmanager-Dashboard eine Warnmeldung an. Auf der Seite Plattform-Services-Endpunkte finden Sie weitere Details zum Fehler.

 One or more endpoints have experienced an error and might not be functioning properly. Go to the [Endpoints](#) page to view the error details. The last error occurred 2 hours ago.

Der gleiche Fehler, der auf dem Dashboard angezeigt wird, wird auch oben auf der Seite „Endpunkte für Plattformdienste“ angezeigt. So zeigen Sie eine detailliertere Fehlermeldung an:

Schritte

1. Wählen Sie in der Liste der Endpunkte den Endpunkt aus, der den Fehler hat.
2. Wählen Sie auf der Seite Details zum Endpunkt die Option **Verbindung** aus. Auf dieser Registerkarte wird nur der letzte Fehler für einen Endpunkt angezeigt und gibt an, wie lange der Fehler aufgetreten ist. Fehler, die das rote X-Symbol enthalten  Aufgetreten innerhalb der letzten 7 Tage.

Overview ^

Display name:	my-endpoint-2 
Type:	Search
URI:	http://10.96.104.30:9200
URN:	urn:sgws:es:::mydomain/sveloso/_doc

Connection

Configuration

Verify connection

Some errors might continue to appear after they are resolved. To see if an error is current or to force the removal of a resolved error, select **Test connection**.

Test connection

Last error details

 2 hours ago

Endpoint failure: Endpont has an AWS failure: RequestError: send request failed; caused by: url.Error; caused by: net:OpError; caused by: os.SyscallError (logID: 143H5UDUUKMGDRWJ)

Überprüfen Sie, ob der Fehler noch immer aktuell ist

Einige Fehler werden möglicherweise weiterhin in der Spalte **Letzter Fehler** angezeigt, auch nachdem sie behoben wurden. So prüfen Sie, ob ein Fehler aktuell ist oder das Entfernen eines behobenen Fehlers aus der Tabelle erzwingen:

Schritte

1. Wählen Sie den Endpunkt aus.

Die Seite mit den Details des Endpunkts wird angezeigt.

2. Wählen Sie **Verbindung > Verbindung testen**.

Durch die Auswahl von **Testverbindung** überprüft StorageGRID, ob der Endpunkt für Plattformdienste vorhanden ist und ob er mit den aktuellen Anmeldeinformationen erreicht werden kann. Die Verbindung zum Endpunkt wird von einem Node an jedem Standort validiert.

Beheben von Endpunktfehlern

Sie können die Meldung **Letzter Fehler** auf der Seite Details zum Endpunkt verwenden, um zu ermitteln, was

99

den Fehler verursacht. Bei einigen Fehlern müssen Sie möglicherweise den Endpunkt bearbeiten, um das Problem zu lösen. Beispielsweise kann ein CloudMirroring-Fehler auftreten, wenn StorageGRID nicht auf den Ziel-S3-Bucket zugreifen kann, da er nicht über die richtigen Zugriffsberechtigungen verfügt oder der Zugriffsschlüssel abgelaufen ist. Die Meldung lautet: „Entweder müssen die Endpunktanmeldeinformationen aktualisiert werden, oder der Zielzugriff muss aktualisiert werden.“ die Details lauten „AccessDenied“ oder „InvalidAccessKeyId“.

Wenn Sie den Endpunkt bearbeiten müssen, um einen Fehler zu beheben, wird durch Auswahl von **Änderungen testen und speichern** der aktualisierte Endpunkt von StorageGRID überprüft und bestätigt, dass er mit den aktuellen Anmeldeinformationen erreicht werden kann. Die Verbindung zum Endpunkt wird von einem Node an jedem Standort validiert.

Schritte

1. Wählen Sie den Endpunkt aus.
2. Wählen Sie auf der Seite Details zum Endpunkt die Option **Konfiguration** aus.
3. Bearbeiten Sie die Endpunktkonfiguration nach Bedarf.
4. Wählen Sie **Verbindung > Verbindung testen**.

Endpoint-Anmeldeinformationen mit unzureichenden Berechtigungen

Wenn StorageGRID einen Endpunkt für Plattformservices validiert, bestätigt er, dass die Anmeldeinformationen des Endpunkts zur Kontaktaufnahme mit der Zielressource verwendet werden können und eine grundlegende Überprüfung der Berechtigungen durchgeführt wird. StorageGRID validiert jedoch nicht alle für bestimmte Plattform-Services-Vorgänge erforderlichen Berechtigungen. Wenn Sie aus diesem Grund beim Versuch, einen Plattformdienst zu verwenden, einen Fehler erhalten (z. B. „403 Verboten“), überprüfen Sie die Berechtigungen, die mit den Anmeldedaten des Endpunkts verknüpft sind.

Verwandte Informationen

- [Verwaltung von StorageGRID > Fehlerbehebung für Plattformservices](#)
- ["Endpunkt für Plattformservices erstellen"](#)
- ["Testen der Verbindung für Endpunkt der Plattformservices"](#)
- ["Endpunkt der Plattformdienste bearbeiten"](#)

CloudMirror-Replizierung konfigurieren

Der ["CloudMirror Replikationsservice"](#) Zu den drei Plattform-Services von StorageGRID gehören. Mithilfe der CloudMirror Replizierung können Sie Objekte automatisch in einen externen S3-Bucket replizieren.

Bevor Sie beginnen

- Die Plattformservices wurden für Ihr Mandantenkonto von einem StorageGRID-Administrator aktiviert.
- Sie haben bereits einen Bucket erstellt, der als Replikationsquelle fungiert.
- Der Endpunkt, den Sie als Ziel für die CloudMirror-Replikation verwenden möchten, ist bereits vorhanden, und Sie haben seinen URN.
- Sie gehören einer Benutzergruppe an, die über den verfügt ["Managen aller Buckets oder Root-Zugriffsberechtigungen"](#). Diese Berechtigungen überschreiben die Berechtigungseinstellungen in Gruppen- oder Bucket-Richtlinien bei der Konfiguration des Buckets mithilfe des Mandanten-Manager.

Über diese Aufgabe

Die CloudMirror Replizierung kopiert Objekte von einem Quell-Bucket zu einem Ziel-Bucket, der in einem Endpunkt angegeben wird.



Die CloudMirror-Replizierung weist wichtige Ähnlichkeiten und Unterschiede zur Grid-übergreifenden Replizierungsfunktion auf. Weitere Informationen finden Sie unter "[Vergleichen Sie Grid-Replizierung und CloudMirror Replizierung](#)".

Um die CloudMirror-Replizierung für einen Bucket zu aktivieren, müssen Sie eine gültige XML-Bucket-Replizierungskonfiguration erstellen und anwenden. Die XML-Replikationskonfiguration muss den URN eines S3-Bucket-Endpunkts für jedes Ziel verwenden.



Die Replizierung wird für Quell- oder Ziel-Buckets nicht unterstützt, wenn S3 Object Lock aktiviert ist.

Allgemeine Informationen zur Bucket-Replizierung und deren Konfiguration finden Sie unter "[Amazon Simple Storage Service \(S3\) Dokumentation: Replizierung von Objekten](#)". Informationen zur Implementierung von GetBucketReplication, DeleteBucketReplication und PutketReplication durch StorageGRID finden Sie im "[Operationen auf Buckets](#)".

Wenn Sie die CloudMirror-Replizierung für einen Bucket aktivieren, der Objekte enthält, werden neue Objekte, die dem Bucket hinzugefügt wurden, repliziert, die vorhandenen Objekte in dem Bucket werden jedoch nicht repliziert. Sie müssen vorhandene Objekte aktualisieren, um die Replikation auszulösen.

Wenn Sie in der Replikationskonfiguration-XML eine Storage-Klasse angeben, verwendet StorageGRID diese Klasse, wenn Vorgänge mit dem Ziel-S3-Endpunkt durchgeführt werden. Der Ziel-Endpunkt muss auch die angegebene Storage-Klasse unterstützen. Befolgen Sie unbedingt die Empfehlungen des Zielsystemanbieters.

Schritte

1. Replizierung für Ihren Quell-Bucket aktivieren:

Verwenden Sie einen Texteditor, um die Replikationskonfiguration-XML zu erstellen, die für die Replikation erforderlich ist, wie in der S3-Replikations-API angegeben. Bei der XML-Konfiguration:

- Beachten Sie, dass StorageGRID nur V1 der Replizierungskonfiguration unterstützt. Das bedeutet, dass StorageGRID die Verwendung von nicht unterstützt `Filter` Element für Regeln und folgt V1-Konventionen zum Löschen von Objektversionen. Details finden Sie in der Amazon Dokumentation zur Replizierungskonfiguration.
- Verwenden Sie den URN eines S3-Bucket-Endpunkts als Ziel.
- Fügen Sie optional die hinzu `<StorageClass>` Und geben Sie eines der folgenden Elemente an:
 - `STANDARD`: Die Standard-Speicherklasse. Wenn Sie beim Hochladen eines Objekts keine Storage-Klasse angeben, wird der angezeigt `STANDARD` Storage-Klasse wird verwendet.
 - `STANDARD_IA`: (Standard - seltener Zugang.) Nutzen Sie diese Storage-Klasse für Daten, auf die seltener zugegriffen wird, aber bei Bedarf auch schnell zugegriffen werden muss.
 - `REDUCED_REDUNDANCY`: Verwenden Sie diese Speicherklasse für nicht kritische, reproduzierbare Daten, die mit weniger Redundanz gespeichert werden können als die `STANDARD` Storage-Klasse.
- Wenn Sie ein angeben `Role` In der XML-Konfiguration wird sie ignoriert. Dieser Wert wird von StorageGRID nicht verwendet.

```
<ReplicationConfiguration>
  <Role></Role>
  <Rule>
    <Status>Enabled</Status>
    <Prefix>2020</Prefix>
    <Destination>
      <Bucket>urn:sgws:s3:::2017-records</Bucket>
      <StorageClass>STANDARD</StorageClass>
    </Destination>
  </Rule>
</ReplicationConfiguration>
```

2. Wählen Sie **View Buckets** aus dem Dashboard, oder wählen Sie **STORAGE (S3) > Buckets**.
3. Wählen Sie den Namen des Quell-Buckets aus.

Die Seite mit den Bucket-Details wird angezeigt.

4. Wählen Sie **Plattform-Services > Replikation**.
5. Aktivieren Sie das Kontrollkästchen **Enable Replication**.
6. Fügen Sie die XML-Replikationskonfiguration in das Textfeld ein und wählen Sie **Änderungen speichern**.

Bucket options
Bucket access
Platform services

Replication
Disabled
^

Enable the CloudMirror replication service to copy objects from a source bucket to a destination bucket that is specified in an endpoint.

- Platform services must be enabled for your tenant account by a StorageGRID administrator.
- You must have already configured an endpoint for each destination bucket.
- You must specify the URN of each endpoint in the replication configuration XML for the source bucket.

Enable replication

Clear

```

<ReplicationConfiguration>
  <Role></Role>
  <Rule>
    <Status>Enabled</Status>
    <Prefix>2020</Prefix>
    <Destination>
      <Bucket>urn:sgws:s3:::2017-records</Bucket>
      <StorageClass>STANDARD</StorageClass>
    </Destination>
  </Rule>
</ReplicationConfiguration>

```

Save changes



Platformservices müssen für jedes Mandantenkonto von einem StorageGRID-Administrator mithilfe des Grid Manager oder der Grid Management API aktiviert werden. Wenden Sie sich an Ihren StorageGRID-Administrator, wenn beim Speichern der Konfigurations-XML ein Fehler auftritt.

7. Überprüfen Sie, ob die Replikation ordnungsgemäß konfiguriert ist:
 - a. Fügen Sie dem Quell-Bucket ein Objekt hinzu, das die in der Replizierungskonfiguration angegebenen Anforderungen für die Replizierung erfüllt.

In dem zuvor gezeigten Beispiel werden Objekte repliziert, die mit dem Präfix „2020“ übereinstimmen.

- b. Vergewissern Sie sich, dass das Objekt in den Ziel-Bucket repliziert wurde.

Bei kleinen Objekten wird die Replizierung schnell durchgeführt.

Verwandte Informationen

["Endpunkt für Plattformservices erstellen"](#)

Konfigurieren Sie Ereignisbenachrichtigungen

Der Benachrichtigungsservice ist einer der drei StorageGRID-Plattforddienste. Sie können Benachrichtigungen für einen Bucket aktivieren, um Informationen über angegebene Ereignisse an ein Ziel-Kafka-Cluster oder -Service zu senden, der den AWS Simple Notification Service (Amazon SNS) unterstützt.

Bevor Sie beginnen

- Die Plattformservices wurden für Ihr Mandantenkonto von einem StorageGRID-Administrator aktiviert.
- Sie haben bereits einen Bucket erstellt, der als Quelle für Benachrichtigungen fungiert.
- Der Endpunkt, den Sie als Ziel für Ereignisbenachrichtigungen verwenden möchten, ist bereits vorhanden, und Sie haben seine URN.
- Sie gehören einer Benutzergruppe an, die über den verfügt ["Managen aller Buckets oder Root-Zugriffsberechtigungen"](#). Diese Berechtigungen überschreiben die Berechtigungseinstellungen in Gruppen- oder Bucket-Richtlinien bei der Konfiguration des Buckets mithilfe des Mandanten-Manager.

Über diese Aufgabe

Sobald nach dem Konfigurieren von Ereignisbenachrichtigungen ein bestimmtes Ereignis für ein Objekt im Quell-Bucket auftritt, wird eine Benachrichtigung generiert und an das als Zielendpunkt verwendete Thema Amazon SNS oder Kafka gesendet. Um Benachrichtigungen für einen Bucket zu aktivieren, müssen Sie eine gültige XML-Benachrichtigungskonfiguration erstellen und anwenden. Die XML-ID für die Benachrichtigungskonfiguration muss den URN eines Endpunkt für Ereignisbenachrichtigungen für jedes Ziel verwenden.

Allgemeine Informationen zu Ereignisbenachrichtigungen und deren Konfiguration finden Sie in der Amazon-Dokumentation. Informationen darüber, wie StorageGRID die S3-Bucket-Benachrichtigungs-API implementiert, finden Sie im ["Anweisungen zur Implementierung von S3-Client-Applikationen"](#).

Wenn Sie Ereignisbenachrichtigungen für einen Bucket aktivieren, der Objekte enthält, werden Benachrichtigungen nur für Aktionen gesendet, die nach dem Speichern der Benachrichtigungskonfiguration ausgeführt werden.

Schritte

1. Benachrichtigungen für Ihren Quell-Bucket aktivieren:
 - Verwenden Sie einen Texteditor, um die XML-Benachrichtigungskonfiguration zu erstellen, die für die Aktivierung von Ereignisbenachrichtigungen erforderlich ist, wie in der S3-Benachrichtigungs-API angegeben.
 - Verwenden Sie bei der XML-Konfiguration den URN eines Endpunkt für Ereignisbenachrichtigungen als Zielthema.

```
<NotificationConfiguration>
  <TopicConfiguration>
    <Id>Image-created</Id>
    <Filter>
      <S3Key>
        <FilterRule>
          <Name>prefix</Name>
          <Value>images/</Value>
        </FilterRule>
      </S3Key>
    </Filter>
    <Topic>arn:aws:sns:us-east-1:050340950352:sgws-topic</Topic>
    <Event>s3:ObjectCreated:*</Event>
  </TopicConfiguration>
</NotificationConfiguration>
```

2. Wählen Sie im Mandantenmanager **STORAGE (S3) > Buckets** aus.
3. Wählen Sie den Namen des Quell-Buckets aus.

Die Seite mit den Bucket-Details wird angezeigt.

4. Wählen Sie **Plattform-Services > Ereignisbenachrichtigungen** aus.
5. Aktivieren Sie das Kontrollkästchen **Ereignisbenachrichtigungen aktivieren**.
6. Fügen Sie die XML-Benachrichtigungskonfiguration in das Textfeld ein und wählen Sie **Änderungen speichern**.

[Bucket options](#)
[Bucket access](#)
[Platform services](#)
[S3 Console](#)

Replication Disabled ▼

Event notifications Disabled ▲

Enable the event notification service for an S3 bucket if you want StorageGRID to send notifications about specified events to a destination Amazon Simple Notification Service (SNS) or a destination Apache Kafka cluster.

- Platform services must be enabled for your tenant account by a StorageGRID administrator.
- You must have already configured an endpoint for the destination of event notifications.
- You must specify the URN of that endpoint in the notification configuration XML for the source bucket.

Enable event notifications

[Clear](#)

```

<NotificationConfiguration>
  <TopicConfiguration>
    <Id>Image-created</Id>
    <Filter>
      <S3Key>
        <FilterRule>
          <Name>prefix</Name>
          <Value>images</Value>
        </FilterRule>
      </S3Key>
    </Filter>
  </TopicConfiguration>
</NotificationConfiguration>
  
```

[Save changes](#)



Plattformservices müssen für jedes Mandantenkonto von einem StorageGRID-Administrator mithilfe des Grid Manager oder der Grid Management API aktiviert werden. Wenden Sie sich an Ihren StorageGRID-Administrator, wenn beim Speichern der Konfigurations-XML ein Fehler auftritt.

7. Überprüfen Sie, ob Ereignisbenachrichtigungen richtig konfiguriert sind:

- a. Führen Sie eine Aktion für ein Objekt im Quell-Bucket durch, die die Anforderungen für das Auslösen einer Benachrichtigung erfüllt, wie sie in der Konfigurations-XML konfiguriert ist.

In diesem Beispiel wird eine Ereignisbenachrichtigung gesendet, sobald ein Objekt mit dem erstellt wird `images/` Präfix.

- b. Bestätigen Sie, dass eine Benachrichtigung an das Ziel-Thema Amazon SNS oder Kafka gesendet wurde.

Wenn Ihr Zielthema beispielsweise auf Amazon SNS gehostet wird, können Sie den Dienst so konfigurieren, dass Sie eine E-Mail senden, wenn die Benachrichtigung zugestellt wird.

```
{
  "Records": [
    {
      "eventVersion": "2.0",
      "eventSource": "sgws:s3",
      "eventTime": "2017-08-08T23:52:38Z",
      "eventName": "ObjectCreated:Put",
      "userIdentity": {
        "principalId": "11111111111111111111"
      },
      "requestParameters": {
        "sourceIPAddress": "193.51.100.20"
      },
      "responseElements": {
        "x-amz-request-id": "122047343"
      },
      "s3": {
        "s3SchemaVersion": "1.0",
        "configurationId": "Image-created",
        "bucket": {
          "name": "test1",
          "ownerIdentity": {
            "principalId": "11111111111111111111"
          },
          "arn": "arn:sgws:s3:::test1"
        },
        "object": {
          "key": "images/cat.jpg",
          "size": 0,
          "eTag": "d41d8cd98f00b204e9800998ecf8427e",
          "sequencer": "14D90402421461C7"
        }
      }
    }
  ]
}
```

+

Wenn die Benachrichtigung im Zielthema empfangen wird, haben Sie Ihren Quell-Bucket für StorageGRID-Benachrichtigungen erfolgreich konfiguriert.

Verwandte Informationen

["Informieren Sie sich über Benachrichtigungen für Buckets"](#)

["S3-REST-API VERWENDEN"](#)

["Endpoint für Plattformservices erstellen"](#)

Verwenden Sie den Suchintegrationsdienst

Der Suchintegrations-Service ist einer der drei StorageGRID Plattform-Services. Sie können diesen Service aktivieren, wenn ein Objekt erstellt, gelöscht oder seine Metadaten oder Tags aktualisiert wird, Objektmetadaten an einen Zielsuchindex zu senden.

Sie können die Suchintegration mit dem Mandanten-Manager konfigurieren, um eine benutzerdefinierte StorageGRID-Konfigurations-XML auf einen Bucket anzuwenden.



Da der Suchintegrationsdienst dazu führt, dass Objektmetadaten an ein Ziel gesendet werden, wird seine Konfigurations-XML als *Metadaten Notification Configuration XML* bezeichnet. Diese Konfigurations-XML unterscheidet sich von der XML-Konfiguration *notification*, die zur Aktivierung von Ereignisbenachrichtigungen verwendet wird.

Siehe ["Anweisungen zur Implementierung von S3-Client-Applikationen"](#) Weitere Informationen zu den folgenden benutzerdefinierten StorageGRID S3 REST-API-Operationen:

- Konfiguration für die Benachrichtigung über Bucket-Metadaten LÖSCHEN
- Konfiguration der Bucket-Metadaten-Benachrichtigungen ABRUFEN
- PUT Bucket-Metadaten-Benachrichtigungskonfiguration

Verwandte Informationen

["Konfigurations-XML für die Integration der Suche"](#)

["Objektmetadaten sind in Metadaten-Benachrichtigungen enthalten"](#)

["JSON durch den Suchintegrations-Service generiert"](#)

["Konfigurieren Sie den Suchintegrationsdienst"](#)

["S3-REST-API VERWENDEN"](#)

Konfigurations-XML für die Integration der Suche

Der Such-Integrationsdienst wird anhand einer Reihe von Regeln konfiguriert, die in `<MetadataNotificationConfiguration>` und `</MetadataNotificationConfiguration>` tags: Jede Regel gibt die Objekte an, auf die sich die Regel bezieht, und das Ziel, an dem StorageGRID die Metadaten dieser Objekte senden sollte.

Objekte können nach dem Präfix des Objektnamens gefiltert werden. Beispielsweise können Sie Metadaten für Objekte mit dem Präfix `images` an ein Ziel und die Metadaten für Objekte mit dem Präfix `videos` nach anderen. Konfigurationen mit überlappenden Präfixen sind nicht gültig und werden beim Einreichen

abgelehnt. Beispiel: Eine Konfiguration, die eine Regel für Objekte mit dem Präfix enthält `test` Und eine zweite Regel für Objekte mit dem Präfix `test2` Ist nicht zulässig.

Ziele müssen mit dem URN eines StorageGRID-Endpunkts angegeben werden, der für den Suchintegrationsdienst erstellt wurde. Diese Endpunkte beziehen sich auf einen Index und einen Typ, der in einem Elasticsearch-Cluster definiert ist.

```
<MetadataNotificationConfiguration>
  <Rule>
    <ID>Rule-1</ID>
    <Status>rule-status</Status>
    <Prefix>key-prefix</Prefix>
    <Destination>
      <Urn>arn:aws:es:region:account-
ID:domain/mydomain/myindex/mytype</Urn>
    </Destination>
  </Rule>
  <Rule>
    <ID>Rule-2</ID>
    ...
  </Rule>
  ...
</MetadataNotificationConfiguration>
```

In der Tabelle werden die Elemente in der XML-Konfiguration für die Metadatenbenachrichtigung beschrieben.

Name	Beschreibung	Erforderlich
MetadataNotificationKonfiguration	Container-Tag für Regeln zur Angabe von Objekten und Zielen für Metadatenbenachrichtigungen Enthält mindestens ein Regelelement.	Ja.
Regel	Container-Tag für eine Regel, die die Objekte identifiziert, deren Metadaten zu einem bestimmten Index hinzugefügt werden sollen. Regeln mit überlappenden Präfixen werden abgelehnt. Im MetadataNotificationConfiguration Element enthalten.	Ja.
ID	Eindeutige Kennung für die Regel. In das Element Regel aufgenommen.	Nein

Name	Beschreibung	Erforderlich
Status	<p>Der Status kann „aktiviert“ oder „deaktiviert“ sein. Für deaktivierte Regeln wird keine Aktion durchgeführt.</p> <p>In das Element Regel aufgenommen.</p>	Ja.
Präfix	<p>Objekte, die mit dem Präfix übereinstimmen, werden von der Regel beeinflusst und ihre Metadaten werden an das angegebene Ziel gesendet.</p> <p>Geben Sie ein leeres Präfix an, um alle Objekte zu entsprechen.</p> <p>In das Element Regel aufgenommen.</p>	Ja.
Ziel	<p>Container-Tag für das Ziel einer Regel.</p> <p>In das Element Regel aufgenommen.</p>	Ja.
Urne	<p>URNE des Ziels, an dem Objektmetadaten gesendet werden. Muss der URN eines StorageGRID-Endpunkts mit den folgenden Eigenschaften sein:</p> <ul style="list-style-type: none"> • es Muss das dritte Element sein. • Der URN muss mit dem Index und dem Typ enden, in dem die Metadaten gespeichert werden, im Formular <code>domain-name/myindex/mytype</code>. <p>Endpunkte werden mithilfe der Mandanten-Manager oder der Mandanten-Management-API konfiguriert. Sie nehmen folgende Form:</p> <ul style="list-style-type: none"> • <code>arn:aws:es:region:account-ID:domain/mydomain/myindex/mytype</code> • <code>urn:mysite:es:::mydomain/myindex/mytype</code> <p>Der Endpunkt muss konfiguriert werden, bevor die Konfigurations-XML gesendet wird, oder die Konfiguration schlägt mit einem Fehler 404 fehl.</p> <p>URNE ist im Element Ziel enthalten.</p>	Ja.

Verwenden Sie die XML-XML-Beispielkonfiguration für Metadatenbenachrichtigungen, um zu erfahren, wie Sie Ihre eigene XML erstellen.

Konfiguration der Metadatenbenachrichtigung für alle Objekte

In diesem Beispiel werden die Objektmetadaten für alle Objekte an dasselbe Ziel gesendet.

```

<MetadataNotificationConfiguration>
  <Rule>
    <ID>Rule-1</ID>
    <Status>Enabled</Status>
    <Prefix></Prefix>
    <Destination>
      <Urn>urn:myes:es:::sgws-notifications/test1/all</Urn>
    </Destination>
  </Rule>
</MetadataNotificationConfiguration>

```

Konfiguration der Metadatenbenachrichtigung mit zwei Regeln

In diesem Beispiel sind die Objektmetadaten für Objekte mit dem Präfix übereinstimmen /images An ein Ziel gesendet wird, während die Objektmetadaten für Objekte mit dem Präfix übereinstimmen /videos Wird an ein zweites Ziel gesendet.

```

<MetadataNotificationConfiguration>
  <Rule>
    <ID>Images-rule</ID>
    <Status>Enabled</Status>
    <Prefix>/images</Prefix>
    <Destination>
      <Urn>arn:aws:es:us-east-1:3333333:domain/es-
domain/graphics/imagetype</Urn>
    </Destination>
  </Rule>
  <Rule>
    <ID>Videos-rule</ID>
    <Status>Enabled</Status>
    <Prefix>/videos</Prefix>
    <Destination>
      <Urn>arn:aws:es:us-west-1:2222222:domain/es-
domain/graphics/videotype</Urn>
    </Destination>
  </Rule>
</MetadataNotificationConfiguration>

```

Verwandte Informationen

["S3-REST-API VERWENDEN"](#)

["Objektmetadaten sind in Metadaten-Benachrichtigungen enthalten"](#)

["JSON durch den Suchintegrations-Service generiert"](#)

["Konfigurieren Sie den Suchintegrationsdienst"](#)

Konfigurieren Sie den Suchintegrationsdienst

Der Suchintegrations-Service sendet Objektmetadaten an einen Zielindex bei jedem Erstellen, Löschen oder Aktualisieren der zugehörigen Metadaten oder Tags.

Bevor Sie beginnen

- Die Plattformservices wurden für Ihr Mandantenkonto von einem StorageGRID-Administrator aktiviert.
- Sie haben bereits einen S3-Bucket erstellt, dessen Inhalt Sie indizieren möchten.
- Der Endpunkt, den Sie als Ziel für den Suchintegrationsdienst verwenden möchten, ist bereits vorhanden, und Sie haben seinen URN.
- Sie gehören einer Benutzergruppe an, die über den verfügt "[Managen aller Buckets oder Root-Zugriffsberechtigungen](#)". Diese Berechtigungen überschreiben die Berechtigungseinstellungen in Gruppen- oder Bucket-Richtlinien bei der Konfiguration des Buckets mithilfe des Mandanten-Manager.

Über diese Aufgabe

Nachdem Sie den Such-Integrationservice für einen Quell-Bucket konfiguriert haben, werden beim Erstellen eines Objekts oder beim Aktualisieren der Metadaten oder Tags eines Objekts Objektmetadaten ausgelöst, die an den Ziel-Endpunkt gesendet werden. Wenn Sie den Suchintegrationservice für einen Bucket aktivieren, der bereits Objekte enthält, werden Metadatenbenachrichtigungen nicht automatisch für vorhandene Objekte gesendet. Sie müssen diese vorhandenen Objekte aktualisieren, um sicherzustellen, dass ihre Metadaten dem Zielsuchindex hinzugefügt werden.

Schritte

1. Verwenden Sie einen Texteditor, um die XML-Metadatenbenachrichtigung zu erstellen, die für die Integration der Suche erforderlich ist.
 - Informationen zur Integration der Suchfunktion finden Sie in den XML-Konfigurationsdaten.
 - Verwenden Sie beim Konfigurieren des XML den URN eines Endpunkt zur Integration der Suche als Ziel.

```
<MetadataNotificationConfiguration>
  <Rule>
    <Status>Enabled</Status>
    <Prefix></Prefix>
    <Destination>
      <Urn>arn:aws:es:us-east-
1:1111111111111111:domain/mydomain/myindex/mytype</Urn>
    </Destination>
  </Rule>
</MetadataNotificationConfiguration>
```

2. Wählen Sie im Mandantenmanager **STORAGE (S3) > Buckets** aus.
3. Wählen Sie den Namen des Quell-Buckets aus.

Die Seite mit den Bucket-Details wird angezeigt.

4. Wählen Sie **Plattform-Services > Integration suchen**
5. Aktivieren Sie das Kontrollkästchen **Enable search Integration**.

6. Fügen Sie die Konfiguration der Metadatenbenachrichtigung in das Textfeld ein, und wählen Sie **Änderungen speichern**.

The screenshot shows the 'Platform services' tab in the AWS S3 console. It features three sections: 'Replication' (Disabled), 'Event notifications' (Disabled), and 'Search integration' (Disabled). The 'Search integration' section includes a checkbox labeled 'Enable search integration' which is checked. Below this is a text area containing the following XML configuration:

```
<MetadataNotificationConfiguration>
  <Rule>
    <Status>Enabled</Status>
    <Prefix></Prefix>
    <Destination>
      <Urn>arn:aws:es:us-east-1:111111111111:domain/mydomain/myindex/mytype</Urn>
    </Destination>
  </Rule>
</MetadataNotificationConfiguration>
```

A 'Clear' button is located to the right of the text area, and a 'Save changes' button is at the bottom right.



Platformservices müssen für jedes Mandantenkonto von einem StorageGRID-Administrator aktiviert werden, der den Grid Manager oder die Management-API verwendet. Wenden Sie sich an Ihren StorageGRID-Administrator, wenn beim Speichern der Konfigurations-XML ein Fehler auftritt.

7. Überprüfen Sie, ob der Suchintegrationsdienst richtig konfiguriert ist:
- Fügen Sie dem Quell-Bucket ein Objekt hinzu, das die Anforderungen für das Auslösen einer Metadatenbenachrichtigung erfüllt, wie in der Konfigurations-XML angegeben.

In dem zuvor gezeigten Beispiel lösen alle Objekte, die dem Bucket hinzugefügt wurden, eine Metadatenbenachrichtigung aus.

- b. Bestätigen Sie, dass ein JSON-Dokument, das die Metadaten und Tags des Objekts enthält, zum im Endpunkt angegebenen Suchindex hinzugefügt wurde.

Nachdem Sie fertig sind

Bei Bedarf können Sie die Suchintegration für einen Bucket mithilfe einer der folgenden Methoden deaktivieren:

- Wählen Sie **STORAGE (S3) > Buckets** und deaktivieren Sie das Kontrollkästchen **Enable search Integration**.
- Wenn Sie die S3-API direkt verwenden, verwenden Sie eine Benachrichtigungsanforderung FÜR DELETE-Bucket-Metadaten. Anweisungen zur Implementierung von S3-Client-Applikationen finden Sie in der Anleitung.

Verwandte Informationen

["Den Suchintegrations-Service verstehen"](#)

["Konfigurations-XML für die Integration der Suche"](#)

["S3-REST-API VERWENDEN"](#)

["Endpunkt für Plattformservices erstellen"](#)

JSON durch den Suchintegrations-Service generiert

Wenn Sie den Such-Integrationservice für einen Bucket aktivieren, wird ein JSON-Dokument generiert und an den Zielpunkt gesendet, wenn Metadaten oder Tags hinzugefügt, aktualisiert oder gelöscht werden.

Dieses Beispiel zeigt ein Beispiel für den JSON, der generiert werden kann, wenn ein Objekt mit dem Schlüssel enthält `SGWS/Tagging.txt` Wird in einem Bucket mit dem Namen erstellt `test`. Der `test` Der Bucket ist nicht versioniert, daher der `versionId` Das Tag ist leer.

```

{
  "bucket": "test",
  "key": "SGWS/Tagging.txt",
  "versionId": "",
  "accountId": "86928401983529626822",
  "size": 38,
  "md5": "3d6c7634a85436eee06d43415012855",
  "region": "us-east-1",
  "metadata": {
    "age": "25"
  },
  "tags": {
    "color": "yellow"
  }
}

```

Objektmetadaten sind in Metadaten-Benachrichtigungen enthalten

In der Tabelle sind alle Felder aufgeführt, die im JSON-Dokument enthalten sind, die beim Aktivierung der Suchintegration an den Zielendpunkt gesendet werden.

Der Dokumentname umfasst, falls vorhanden, den Bucket-Namen, den Objektnamen und die Version-ID.

Typ	Elementname und -Beschreibung
Bucket- und Objektinformationen	bucket: Name des Eimers
key: Objektschlüsselname	versionID: Objektversion, für Objekte in versionierten Buckets
region: Eimer-Region, zum Beispiel us-east-1	System-Metadaten
size: Objektgröße (in Bytes) als sichtbar für einen HTTP-Client	md5: Objekt-Hash
Benutzer-Metadaten	metadata: Alle Benutzer-Metadaten für das Objekt, als Schlüssel-Wert-Paare key:value
Tags	tags: Alle für das Objekt definierten Objekttags, als Schlüsselwert-Paare key:value



Für Tags und Benutzer-Metadaten gibt StorageGRID Daten und Nummern an Elasticsearch als Strings oder als S3-Ereignisbenachrichtigungen weiter. Um Elasticsearch so zu konfigurieren, dass diese Strings als Daten oder Zahlen interpretiert werden, befolgen Sie die Elasticsearch-Anweisungen für die dynamische Feldzuordnung und die Zuordnung von Datumsformaten. Sie müssen die dynamischen Feldzuordnungen im Index aktivieren, bevor Sie den Suchintegrationsdienst konfigurieren. Nachdem ein Dokument indiziert wurde, können Sie die Feldtypen des Dokuments im Index nicht mehr bearbeiten.

S3-REST-API VERWENDEN

Von S3 REST API unterstützte Versionen und Updates

StorageGRID unterstützt die S3-API (Simple Storage Service), die als Satz Rest-Web-Services (Representational State Transfer) implementiert wird.

Dank der Unterstützung für die S3-REST-API können serviceorientierte Applikationen, die für S3-Web-Services entwickelt wurden, mit On-Premises-Objekt-Storage verbunden werden, der das StorageGRID-System verwendet. Es sind minimale Änderungen an der aktuellen Nutzung von S3-REST-API-Aufrufen einer Client-Applikation erforderlich.

Unterstützte Versionen

StorageGRID unterstützt die folgenden spezifischen Versionen von S3 und HTTP.

Element	Version
S3-API-Spezifikation	"Amazon Web Services (AWS) Dokumentation: Amazon Simple Storage Service API Reference"
HTTP	1.1 Weitere Informationen zu HTTP finden Sie unter HTTP/1.1 (RFCs 7230-35) . "IETF RFC 2616: Hypertext Transfer Protocol (HTTP/1.1)" Hinweis: StorageGRID unterstützt HTTP/1.1-Pipelining nicht.

Updates für die S3-REST-API-Unterstützung

Freigabe	Kommentare
11.8	Die Namen von S3-Vorgängen wurden entsprechend den in der verwendeten Namen aktualisiert "Amazon Web Services (AWS) Dokumentation: Amazon Simple Storage Service API Reference" .

Freigabe	Kommentare
11.7	<ul style="list-style-type: none"> • Hinzugefügt "Schnelle Referenz: Unterstützte S3-API-Anforderungen". • Zusätzliche Unterstützung für die Verwendung DES GOVERNANCE-Modus mit S3 Object Lock. • Zusätzliche Unterstützung für das StorageGRID-spezifische <code>x-ntap-sg-cgr-replication-status</code> Antwortkopf für GET Object- und HEAD-Objektanforderungen. Dieser Header stellt den Replikationsstatus eines Objekts für die Grid-übergreifende Replikation bereit. • SelectObjectContent Requests unterstützen nun Parkett-Objekte.
11.6	<ul style="list-style-type: none"> • Zusätzliche Unterstützung für die Verwendung von <code>partNumber</code> Anforderungsparameter in GET Object und HEAD Object Requests. • Zusätzliche Unterstützung für einen Standardaufbewahrungsmodus und einen Standardaufbewahrungszeitraum auf Bucket-Ebene für S3 Object Lock. • Zusätzliche Unterstützung für die <code>s3:object-lock-remaining-retention-days</code> Richtlinienbedingung-Schlüssel zum Festlegen des Bereichs zulässiger Aufbewahrungsfristen für Ihre Objekte. • Die maximale <i>recommended</i>-Größe für einen einzelnen PUT-Objekt-Vorgang wurde auf 5 gib (5,368,709,120 Bytes) geändert. Wenn Sie über Objekte mit einer Größe von mehr als 5 gib verfügen, verwenden Sie stattdessen mehrteilige Uploads.
11.5	<ul style="list-style-type: none"> • Zusätzliche Unterstützung für das Management der Bucket-Verschlüsselung • Unterstützung für S3 Object Lock und veraltete ältere Compliance-Anforderungen wurde hinzugefügt. • Zusätzliche Unterstützung beim LÖSCHEN mehrerer Objekte in versionierten Buckets. • Der <code>Content-MD5</code> Die Anforderungsüberschrift wird jetzt korrekt unterstützt.
11.4	<ul style="list-style-type: none"> • Unterstützung für DELETE Bucket-Tagging, GET Bucket-Tagging und PUT Bucket-Tagging. Kostenzuordnungstags werden nicht unterstützt. • Bei in StorageGRID 11.4 erstellten Buckets ist keine Beschränkung der Objektschlüsselnamen auf Performance-Best-Practices mehr erforderlich. • Zusätzliche Unterstützung für Bucket-Benachrichtigungen auf der <code>s3:ObjectRestore:Post</code> Ereignistyp. • Die Größenbeschränkungen von AWS für mehrere Teile werden nun durchgesetzt. Jedes Teil eines mehrteiligen Uploads muss zwischen 5 MiB und 5 gib liegen. Der letzte Teil kann kleiner als 5 MiB sein. • Unterstützung für TLS 1.3 hinzugefügt

Freigabe	Kommentare
11.3	<ul style="list-style-type: none"> • Zusätzliche Unterstützung für serverseitige Verschlüsselung von Objektdaten mit vom Kunden bereitgestellten Schlüsseln (SSE-C). • Unterstützung für VORGÄNGE IM Bucket-Lebenszyklus (nur Aktion „Ablauf“) und für den wurde hinzugefügt <code>x-amz-expiration</code> Kopfzeile der Antwort. • Aktualisiertes PUT-Objekt, PUT-Objekt – Copy und Multipart-Upload, um die Auswirkungen von ILM-Regeln zu beschreiben, die synchrone Platzierung bei der Aufnahme verwenden. • TLS 1.1-Chiffren werden nicht mehr unterstützt.
11.2	<p>Unterstützung für DIE WIEDERHERSTELLUNG NACH Objekten wurde hinzugefügt und kann in Cloud-Storage-Pools verwendet werden. Unterstützung für die Verwendung der AWS-Syntax für ARN, Richtlinienzustandsschlüssel und Richtlinienvariablen in Gruppen- und Bucket-Richtlinien Vorhandene Gruppen- und Bucket-Richtlinien, die die StorageGRID-Syntax verwenden, werden weiterhin unterstützt.</p> <p>Hinweis: die Verwendung von ARN/URN in anderen Konfigurationen JSON/XML, einschließlich derjenigen, die in benutzerdefinierten StorageGRID-Funktionen verwendet werden, hat sich nicht geändert.</p>
11.1	Zusätzliche Unterstützung für die Cross-Origin Resource Sharing (CORS), HTTP für S3-Clientverbindungen zu Grid-Nodes und Compliance-Einstellungen für Buckets.
11.0	Unterstützung für die Konfiguration von Plattform-Services (CloudMirror Replizierung, Benachrichtigungen und Elasticsearch-Integration) für Buckets. Außerdem wurden die Unterstützung für Objekt-Tagging-Speicherortbeschränkungen für Buckets und die verfügbare Konsistenz hinzugefügt.
10.4	Unterstützung für ILM-Scanning-Änderungen an Versionierung, Seitenaktualisierungen von Endpoint Domain-Namen, Bedingungen und Variablen in Richtlinien, Richtlinienbeispiele und die Berechtigung <code>PutOverwriteObject</code> .
10.3	Zusätzliche Unterstützung für Versionierung
10.2	Unterstützung für Gruppen- und Bucket-Zugriffsrichtlinien und für mehrteilige Kopien (Upload Part - Copy) hinzugefügt
10.1	Unterstützung für mehrteilige Uploads, virtuelle Hosted-Style-Anforderungen und v4 Authentifizierung
10.0	Die erste Unterstützung der S3-REST-API durch das StorageGRID-System. die derzeit unterstützte Version der <i>Simple Storage Service API Reference</i> lautet 2006-03-01.

Schnelle Referenz: Unterstützte S3-API-Anforderungen

Auf dieser Seite wird zusammengefasst, wie StorageGRID Amazon Simple Storage

Service (S3) APIs unterstützt.

Diese Seite umfasst nur die S3-Vorgänge, die von StorageGRID unterstützt werden.



Um die AWS Dokumentation für jeden Vorgang anzuzeigen, klicken Sie in der Überschrift auf den Link.

Allgemeine URI-Abfrageparameter und Anforderungsheader

Sofern nicht angegeben, werden die folgenden gängigen URI-Abfrageparameter unterstützt:

- `versionId` (Bei Bedarf für Objekt-Operationen)

Sofern nicht anders angegeben, werden die folgenden gängigen Anforderungsheader unterstützt:

- `Authorization`
- `Connection`
- `Content-Length`
- `Content-MD5`
- `Content-Type`
- `Date`
- `Expect`
- `Host`
- `x-amz-date`

Verwandte Informationen

- ["Details zur S3-REST-API-Implementierung"](#)
- ["Amazon Simple Storage Service API-Referenz: Common Request Header"](#)

"AbortMeh rteilaUpload"

URI-Abfrageparameter und Anforderungskopfzeilen

StorageGRID unterstützt alle [Allgemeine Parameter und Kopfzeilen](#) Für diese Anforderung plus diesen zusätzlichen URI-Abfrageparameter:

- `uploadId`

Text anfordern

Keine

StorageGRID-Dokumentation

["Vorgänge für mehrteilige Uploads"](#)

"CompleteMultipartUpload"

URI-Abfrageparameter und Anforderungskopfzeilen

StorageGRID unterstützt alle [Allgemeine Parameter und Kopfzeilen](#) Für diese Anforderung plus diesen

zusätzlichen URI-Abfrageparameter:

- uploadId

Text-XML-Tags anfordern

StorageGRID unterstützt folgende XML-Tags für Anforderungstext:

- CompleteMultipartUpload
- ETag
- Part
- PartNumber

StorageGRID-Dokumentation

["CompleteMultipartUpload"](#)

["CopyObject"](#)

URI-Abfrageparameter und Anforderungskopfzeilen

StorageGRID unterstützt alle [Allgemeine Parameter und Kopfzeilen](#) Für diese Anfrage, plus diese zusätzlichen Kopfzeilen:

- x-amz-copy-source
- x-amz-copy-source-if-match
- x-amz-copy-source-if-modified-since
- x-amz-copy-source-if-none-match
- x-amz-copy-source-if-unmodified-since
- 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-metadata-directive
- x-amz-object-lock-legal-hold
- x-amz-object-lock-mode
- x-amz-object-lock-retain-until-date
- x-amz-server-side-encryption
- x-amz-server-side-encryption-customer-algorithm
- x-amz-server-side-encryption-customer-key
- x-amz-server-side-encryption-customer-key-MD5
- x-amz-storage-class
- x-amz-tagging
- x-amz-tagging-directive

- x-amz-meta-<metadata-name>

Text anfordern

Keine

StorageGRID-Dokumentation

["CopyObject"](#)

"CreateBucket"

URI-Abfrageparameter und Anforderungskopfzeilen

StorageGRID unterstützt alle [Allgemeine Parameter und Kopfzeilen](#) Für diese Anfrage, plus diese zusätzlichen Kopfzeilen:

- x-amz-bucket-object-lock-enabled

Text anfordern

StorageGRID unterstützt alle Parameter des Abforderungskörpers, die zum Zeitpunkt der Implementierung von der Amazon S3 REST-API definiert wurden.

StorageGRID-Dokumentation

["Operationen auf Buckets"](#)

"CreateMultipartUpload"

URI-Abfrageparameter und Anforderungskopfzeilen

StorageGRID unterstützt alle [Allgemeine Parameter und Kopfzeilen](#) Für diese Anfrage, plus diese zusätzlichen Kopfzeilen:

- Cache-Control
- Content-Disposition
- Content-Encoding
- Content-Language
- Expires
- x-amz-server-side-encryption
- x-amz-storage-class
- x-amz-server-side-encryption-customer-algorithm
- x-amz-server-side-encryption-customer-key
- x-amz-server-side-encryption-customer-key-MD5
- x-amz-tagging
- x-amz-object-lock-mode
- x-amz-object-lock-retain-until-date
- x-amz-object-lock-legal-hold
- x-amz-meta-<metadata-name>

Text anfordern

Keine

StorageGRID-Dokumentation

["CreateMultipartUpload"](#)

"DeleteBucket"

URI-Abfrageparameter und Anforderungskopfzeilen

StorageGRID unterstützt alle [Allgemeine Parameter und Kopfzeilen](#) Für diese Anfrage.

StorageGRID-Dokumentation

["Operationen auf Buckets"](#)

"DeleteBucketCors"

URI-Abfrageparameter und Anforderungskopfzeilen

StorageGRID unterstützt alle [Allgemeine Parameter und Kopfzeilen](#) Für diese Anfrage.

Text anfordern

Keine

StorageGRID-Dokumentation

["Operationen auf Buckets"](#)

"DeleteBucketEncryption"

URI-Abfrageparameter und Anforderungskopfzeilen

StorageGRID unterstützt alle [Allgemeine Parameter und Kopfzeilen](#) Für diese Anfrage.

Text anfordern

Keine

StorageGRID-Dokumentation

["Operationen auf Buckets"](#)

"DeleteBucketLifecycle"

URI-Abfrageparameter und Anforderungskopfzeilen

StorageGRID unterstützt alle [Allgemeine Parameter und Kopfzeilen](#) Für diese Anfrage.

Text anfordern

Keine

StorageGRID-Dokumentation

- ["Operationen auf Buckets"](#)
- ["S3-Lebenszykluskonfiguration erstellen"](#)

"DeleteBucketRichtlinien"

URI-Abfrageparameter und Anforderungskopfzeilen

StorageGRID unterstützt alle [Allgemeine Parameter und Kopfzeilen](#) Für diese Anfrage.

Text anfordern

Keine

StorageGRID-Dokumentation

["Operationen auf Buckets"](#)

"DeleteBucketReplication"

URI-Abfrageparameter und Anforderungskopfzeilen

StorageGRID unterstützt alle [Allgemeine Parameter und Kopfzeilen](#) Für diese Anfrage.

Text anfordern

Keine

StorageGRID-Dokumentation

["Operationen auf Buckets"](#)

"DeleteBucketTagging"

URI-Abfrageparameter und Anforderungskopfzeilen

StorageGRID unterstützt alle [Allgemeine Parameter und Kopfzeilen](#) Für diese Anfrage.

Text anfordern

Keine

StorageGRID-Dokumentation

["Operationen auf Buckets"](#)

"DeleteObject"

URI-Abfrageparameter und Anforderungskopfzeilen

StorageGRID unterstützt alle [Allgemeine Parameter und Kopfzeilen](#) Für diese Anforderung plus diesen zusätzlichen Anforderungsheader:

- `x-amz-bypass-governance-retention`

Text anfordern

Keine

StorageGRID-Dokumentation

["Operationen für Objekte"](#)

"Objekte deObjekteObjekte"

URI-Abfrageparameter und Anforderungskopfzeilen

StorageGRID unterstützt alle [Allgemeine Parameter und Kopfzeilen](#) Für diese Anforderung plus diesen zusätzlichen Anforderungsheader:

- `x-amz-bypass-governance-retention`

Text anfordern

StorageGRID unterstützt alle Parameter des Anforderungskörpers, die zum Zeitpunkt der Implementierung von der Amazon S3 REST-API definiert wurden.

StorageGRID-Dokumentation

["Operationen für Objekte"](#)

"DeleteObjectTagging"

StorageGRID unterstützt alle [Allgemeine Parameter und Kopfzeilen](#) Für diese Anfrage.

Text anfordern

Keine

StorageGRID-Dokumentation

["Operationen für Objekte"](#)

"GetBucketAcl"

URI-Abfrageparameter und Anforderungskopfzeilen

StorageGRID unterstützt alle [Allgemeine Parameter und Kopfzeilen](#) Für diese Anfrage.

Text anfordern

Keine

StorageGRID-Dokumentation

["Operationen auf Buckets"](#)

"GetBucketCors"

URI-Abfrageparameter und Anforderungskopfzeilen

StorageGRID unterstützt alle [Allgemeine Parameter und Kopfzeilen](#) Für diese Anfrage.

Text anfordern

Keine

StorageGRID-Dokumentation

["Operationen auf Buckets"](#)

"GetBucketEncryption"

URI-Abfrageparameter und Anforderungskopfzeilen

StorageGRID unterstützt alle [Allgemeine Parameter und Kopfzeilen](#) Für diese Anfrage.

Text anfordern

Keine

StorageGRID-Dokumentation

["Operationen auf Buckets"](#)

"GetBucketLifecycleKonfiguration"

URI-Abfrageparameter und Anforderungskopfzeilen

StorageGRID unterstützt alle [Allgemeine Parameter und Kopfzeilen](#) Für diese Anfrage.

Text anfordern

Keine

StorageGRID-Dokumentation

- ["Operationen auf Buckets"](#)
- ["S3-Lebenszykluskonfiguration erstellen"](#)

"GetBucketLocation"

URI-Abfrageparameter und Anforderungskopfzeilen

StorageGRID unterstützt alle [Allgemeine Parameter und Kopfzeilen](#) Für diese Anfrage.

Text anfordern

Keine

StorageGRID-Dokumentation

["Operationen auf Buckets"](#)

"GetBucketNotificationConfiguration"

URI-Abfrageparameter und Anforderungskopfzeilen

StorageGRID unterstützt alle [Allgemeine Parameter und Kopfzeilen](#) Für diese Anfrage.

Text anfordern

Keine

StorageGRID-Dokumentation

["Operationen auf Buckets"](#)

"GetBucketPolicy"

URI-Abfrageparameter und Anforderungskopfzeilen

StorageGRID unterstützt alle [Allgemeine Parameter und Kopfzeilen](#) Für diese Anfrage.

Text anfordern

Keine

StorageGRID-Dokumentation

["Operationen auf Buckets"](#)

"GetBucketReplication"

URI-Abfrageparameter und Anforderungskopfzeilen

StorageGRID unterstützt alle [Allgemeine Parameter und Kopfzeilen](#) Für diese Anfrage.

Text anfordern

Keine

StorageGRID-Dokumentation

["Operationen auf Buckets"](#)

"GetBucketTagging"

URI-Abfrageparameter und Anforderungskopfeilen

StorageGRID unterstützt alle [Allgemeine Parameter und Kopfzeilen](#) Für diese Anfrage.

Text anfordern

Keine

StorageGRID-Dokumentation

["Operationen auf Buckets"](#)

"GetBucketVersioning"

URI-Abfrageparameter und Anforderungskopfeilen

StorageGRID unterstützt alle [Allgemeine Parameter und Kopfzeilen](#) Für diese Anfrage.

Text anfordern

Keine

StorageGRID-Dokumentation

["Operationen auf Buckets"](#)

"GetObject"

URI-Abfrageparameter und Anforderungskopfeilen

StorageGRID unterstützt alle [Allgemeine Parameter und Kopfzeilen](#) Für diese Anforderung plus die folgenden zusätzlichen URI-Abfrageparameter:

- partNumber
- response-cache-control
- response-content-disposition
- response-content-encoding
- response-content-language
- response-content-type
- response-expires

Und diese zusätzlichen Anforderungsheader:

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

- If-Match
- If-Modified-Since
- If-None-Match
- If-Unmodified-Since

Text anfordern

Keine

StorageGRID-Dokumentation

["GetObject"](#)

"GetObjectAcl"

URI-Abfrageparameter und Anforderungskopfzeilen

StorageGRID unterstützt alle [Allgemeine Parameter und Kopfzeilen](#) Für diese Anfrage.

Text anfordern

Keine

StorageGRID-Dokumentation

["Operationen für Objekte"](#)

"GetObjectLegalHold"

URI-Abfrageparameter und Anforderungskopfzeilen

StorageGRID unterstützt alle [Allgemeine Parameter und Kopfzeilen](#) Für diese Anfrage.

Text anfordern

Keine

StorageGRID-Dokumentation

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

"GetObjectLockConfiguration"

URI-Abfrageparameter und Anforderungskopfzeilen

StorageGRID unterstützt alle [Allgemeine Parameter und Kopfzeilen](#) Für diese Anfrage.

Text anfordern

Keine

StorageGRID-Dokumentation

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

"GetObjectRetention"

URI-Abfrageparameter und Anforderungskopfzeilen

StorageGRID unterstützt alle [Allgemeine Parameter und Kopfzeilen](#) Für diese Anfrage.

Text anfordern

Keine

StorageGRID-Dokumentation

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

"GetObjectTagging"

URI-Abfrageparameter und Anforderungskopfzeilen

StorageGRID unterstützt alle [Allgemeine Parameter und Kopfzeilen](#) Für diese Anfrage.

Text anfordern

Keine

StorageGRID-Dokumentation

["Operationen für Objekte"](#)

"HeadBucket"

URI-Abfrageparameter und Anforderungskopfzeilen

StorageGRID unterstützt alle [Allgemeine Parameter und Kopfzeilen](#) Für diese Anfrage.

Text anfordern

Keine

StorageGRID-Dokumentation

["Operationen auf Buckets"](#)

"HeadObject"

URI-Abfrageparameter und Anforderungskopfzeilen

StorageGRID unterstützt alle [Allgemeine Parameter und Kopfzeilen](#) Für diese Anfrage, plus diese zusätzlichen Kopfzeilen:

- x-amz-server-side-encryption-customer-algorithm
- x-amz-server-side-encryption-customer-key
- x-amz-server-side-encryption-customer-key-MD5
- If-Match
- If-Modified-Since
- If-None-Match
- If-Unmodified-Since
- Range

Text anfordern

Keine

StorageGRID-Dokumentation

["HeadObject"](#)

"ListBuchs"

URI-Abfrageparameter und Anforderungskopfzeilen

StorageGRID unterstützt alle [Allgemeine Parameter und Kopfzeilen](#) Für diese Anfrage.

Text anfordern

Keine

StorageGRID-Dokumentation

[Operationen für den Dienst > ListBuckets](#)

"ListMultipartUploads"

URI-Abfrageparameter und Anforderungskopfzeilen

StorageGRID unterstützt alle [Allgemeine Parameter und Kopfzeilen](#) Für diese Anforderung plus die folgenden zusätzlichen Parameter:

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

Text anfordern

Keine

StorageGRID-Dokumentation

["ListMultipartUploads"](#)

"ListObjekte"

URI-Abfrageparameter und Anforderungskopfzeilen

StorageGRID unterstützt alle [Allgemeine Parameter und Kopfzeilen](#) Für diese Anforderung plus die folgenden zusätzlichen Parameter:

- delimiter
- encoding-type
- marker
- max-keys
- prefix

Text anfordern

Keine

StorageGRID-Dokumentation

["Operationen auf Buckets"](#)

"ListObjekteV2"

URI-Abfrageparameter und Anforderungskopfzeilen

StorageGRID unterstützt alle [Allgemeine Parameter und Kopfzeilen](#) Für diese Anforderung plus die folgenden zusätzlichen Parameter:

- continuation-token
- delimiter
- encoding-type
- fetch-owner
- max-keys
- prefix
- start-after

Text anfordern

Keine

StorageGRID-Dokumentation

["Operationen auf Buckets"](#)

"ListObjectVersions"

URI-Abfrageparameter und Anforderungskopfzeilen

StorageGRID unterstützt alle [Allgemeine Parameter und Kopfzeilen](#) Für diese Anforderung plus die folgenden zusätzlichen Parameter:

- delimiter
- encoding-type
- key-marker
- max-keys
- prefix
- version-id-marker

Text anfordern

Keine

StorageGRID-Dokumentation

["Operationen auf Buckets"](#)

"ListenTeile"

URI-Abfrageparameter und Anforderungskopfzeilen

StorageGRID unterstützt alle [Allgemeine Parameter und Kopfzeilen](#) Für diese Anforderung plus die folgenden zusätzlichen Parameter:

- max-parts

- part-number-marker
- uploadId

Text anfordern

Keine

StorageGRID-Dokumentation

["ListMultipartUploads"](#)

"PutBucketCors"

URI-Abfrageparameter und Anforderungskopfzeilen

StorageGRID unterstützt alle [Allgemeine Parameter und Kopfzeilen](#) Für diese Anfrage.

Text anfordern

StorageGRID unterstützt alle Parameter des Anforderungskörpers, die zum Zeitpunkt der Implementierung von der Amazon S3 REST-API definiert wurden.

StorageGRID-Dokumentation

["Operationen auf Buckets"](#)

"PutBucketEncryption"

URI-Abfrageparameter und Anforderungskopfzeilen

StorageGRID unterstützt alle [Allgemeine Parameter und Kopfzeilen](#) Für diese Anfrage.

Text-XML-Tags anfordern

StorageGRID unterstützt folgende XML-Tags für Anforderungstext:

- ApplyServerSideEncryptionByDefault
- Rule
- ServerSideEncryptionConfiguration
- SSEAlgorithm

StorageGRID-Dokumentation

["Operationen auf Buckets"](#)

"PutBucketLifecycleKonfiguration"

URI-Abfrageparameter und Anforderungskopfzeilen

StorageGRID unterstützt alle [Allgemeine Parameter und Kopfzeilen](#) Für diese Anfrage.

Text-XML-Tags anfordern

StorageGRID unterstützt folgende XML-Tags für Anforderungstext:

- And
- Days
- Expiration

- ExpiredObjectDeleteMarker
- Filter
- ID
- Key
- LifecycleConfiguration
- NewerNoncurrentVersions
- NoncurrentDays
- NoncurrentVersionExpiration
- Prefix
- Rule
- Status
- Tag
- Value

StorageGRID-Dokumentation

- ["Operationen auf Buckets"](#)
- ["S3-Lebenszykluskonfiguration erstellen"](#)

"PutBucketNotificationKonfiguration"

URI-Abfrageparameter und Anforderungskopfzeilen

StorageGRID unterstützt alle [Allgemeine Parameter und Kopfzeilen](#) Für diese Anfrage.

Text-XML-Tags anfordern

StorageGRID unterstützt folgende XML-Tags für Anforderungstext:

- Event
- Filter
- FilterRule
- Id
- Name
- NotificationConfiguration
- Prefix
- S3Key
- Suffix
- Topic
- TopicConfiguration
- Value

StorageGRID-Dokumentation

["Operationen auf Buckets"](#)

"PutBucketPolicy"

URI-Abfrageparameter und Anforderungskopfzeilen

StorageGRID unterstützt alle [Allgemeine Parameter und Kopfzeilen](#) Für diese Anfrage.

Text anfordern

Weitere Informationen zu den unterstützten JSON-Textfeldern finden Sie unter ["Verwendung von Bucket- und Gruppenzugriffsrichtlinien"](#).

"PutBucketReplication"

URI-Abfrageparameter und Anforderungskopfzeilen

StorageGRID unterstützt alle [Allgemeine Parameter und Kopfzeilen](#) Für diese Anfrage.

Text-XML-Tags anfordern

- Bucket
- Destination
- Prefix
- ReplicationConfiguration
- Rule
- Status
- StorageClass

StorageGRID-Dokumentation

["Operationen auf Buckets"](#)

"PutBucketTagging"

URI-Abfrageparameter und Anforderungskopfzeilen

StorageGRID unterstützt alle [Allgemeine Parameter und Kopfzeilen](#) Für diese Anfrage.

Text anfordern

StorageGRID unterstützt alle Parameter des Anforderungskörpers, die zum Zeitpunkt der Implementierung von der Amazon S3 REST-API definiert wurden.

StorageGRID-Dokumentation

["Operationen auf Buckets"](#)

"PutBucketVersioning"

URI-Abfrageparameter und Anforderungskopfzeilen

StorageGRID unterstützt alle [Allgemeine Parameter und Kopfzeilen](#) Für diese Anfrage.

Body-Parameter anfordern

StorageGRID unterstützt die folgenden Parameter des Anfragenkörpers:

- VersioningConfiguration
- Status

StorageGRID-Dokumentation

"Operationen auf Buckets"

"PutObject"

URI-Abfrageparameter und Anforderungskopfzeilen

StorageGRID unterstützt alle [Allgemeine Parameter und Kopfzeilen](#) Für diese Anfrage, plus diese zusätzlichen Kopfzeilen:

- Cache-Control
- Content-Disposition
- Content-Encoding
- Content-Language
- x-amz-server-side-encryption
- x-amz-storage-class
- x-amz-server-side-encryption-customer-algorithm
- x-amz-server-side-encryption-customer-key
- x-amz-server-side-encryption-customer-key-MD5
- x-amz-tagging
- x-amz-object-lock-mode
- x-amz-object-lock-retain-until-date
- x-amz-object-lock-legal-hold
- x-amz-meta-`<metadata-name>`

Text anfordern

- Binäre Daten des Objekts

StorageGRID-Dokumentation

"PutObject"

"PutObjectLegalHold"

URI-Abfrageparameter und Anforderungskopfzeilen

StorageGRID unterstützt alle [Allgemeine Parameter und Kopfzeilen](#) Für diese Anfrage.

Text anfordern

StorageGRID unterstützt alle Parameter des Abforderungskörpers, die zum Zeitpunkt der Implementierung von der Amazon S3 REST-API definiert wurden.

StorageGRID-Dokumentation

"Konfigurieren Sie die S3-Objektsperre über die S3-REST-API"

"PutObjectLockKonfiguration"

URI-Abfrageparameter und Anforderungskopfzeilen

StorageGRID unterstützt alle [Allgemeine Parameter und Kopfzeilen](#) Für diese Anfrage.

Text anfordern

StorageGRID unterstützt alle Parameter des Abforderungskörpers, die zum Zeitpunkt der Implementierung von der Amazon S3 REST-API definiert wurden.

StorageGRID-Dokumentation

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

"PutObjectRetention"

URI-Abfrageparameter und Anforderungskopfzeilen

StorageGRID unterstützt alle [Allgemeine Parameter und Kopfzeilen](#) Für diese Anfrage, plus diese zusätzliche Kopfzeile:

- `x-amz-bypass-governance-retention`

Text anfordern

StorageGRID unterstützt alle Parameter des Abforderungskörpers, die zum Zeitpunkt der Implementierung von der Amazon S3 REST-API definiert wurden.

StorageGRID-Dokumentation

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

"PutObjectTagging"

URI-Abfrageparameter und Anforderungskopfzeilen

StorageGRID unterstützt alle [Allgemeine Parameter und Kopfzeilen](#) Für diese Anfrage.

Text anfordern

StorageGRID unterstützt alle Parameter des Abforderungskörpers, die zum Zeitpunkt der Implementierung von der Amazon S3 REST-API definiert wurden.

StorageGRID-Dokumentation

["Operationen für Objekte"](#)

"Objekt restoreObject"

URI-Abfrageparameter und Anforderungskopfzeilen

StorageGRID unterstützt alle [Allgemeine Parameter und Kopfzeilen](#) Für diese Anfrage.

Text anfordern

Weitere Informationen zu den unterstützten Textfeldern finden Sie unter ["Objekt restoreObject"](#).

"SelektierObjectContent"

URI-Abfrageparameter und Anforderungskopfzeilen

StorageGRID unterstützt alle [Allgemeine Parameter und Kopfzeilen](#) Für diese Anfrage.

Text anfordern

Weitere Informationen zu den unterstützten Textfeldern finden Sie in den folgenden Informationen:

- ["Verwenden Sie S3 Select"](#)
- ["SelektierObjectContent"](#)

"UploadTeil"

URI-Abfrageparameter und Anforderungskopfzeilen

StorageGRID unterstützt alle [Allgemeine Parameter und Kopfzeilen](#) Für diese Anforderung plus die folgenden zusätzlichen URI-Abfrageparameter:

- partNumber
- uploadId

Und diese zusätzlichen Anforderungsheader:

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

Text anfordern

- Binäre Daten des Teils

StorageGRID-Dokumentation

["UploadTeil"](#)

["UploadPartCopy"](#)

URI-Abfrageparameter und Anforderungskopfzeilen

StorageGRID unterstützt alle [Allgemeine Parameter und Kopfzeilen](#) Für diese Anforderung plus die folgenden zusätzlichen URI-Abfrageparameter:

- partNumber
- uploadId

Und diese zusätzlichen Anforderungsheader:

- x-amz-copy-source
- x-amz-copy-source-if-match
- x-amz-copy-source-if-modified-since
- x-amz-copy-source-if-none-match
- x-amz-copy-source-if-unmodified-since
- x-amz-copy-source-range
- x-amz-server-side-encryption-customer-algorithm
- x-amz-server-side-encryption-customer-key

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

Text anfordern

Keine

StorageGRID-Dokumentation

["UploadPartCopy"](#)

Testen der S3-REST-API-Konfiguration

Sie können die Amazon Web Services Command Line Interface (AWS CLI) verwenden, um die Verbindung zum System zu testen und zu überprüfen, ob Objekte gelesen und geschrieben werden können.

Bevor Sie beginnen

- Sie haben die AWS CLI von heruntergeladen und installiert "[aws.amazon.com/cli](#)".
- Optional haben Sie "[Ein Load Balancer-Endpunkt wurde erstellt](#)". Andernfalls kennen Sie die IP-Adresse des zu verbindenden Storage-Node und die zu verwendende Port-Nummer. Siehe "[IP-Adressen und Ports für Client-Verbindungen](#)".
- Das ist schon "[S3-Mandantenkonto wurde erstellt](#)".
- Sie haben sich beim Mieter und angemeldet "[Zugriffsschlüssel erstellt](#)".

Weitere Informationen zu diesen Schritten finden Sie unter "[Client-Verbindungen konfigurieren](#)".

Schritte

1. Konfigurieren Sie die AWS-CLI-Einstellungen so, dass das im StorageGRID-System erstellte Konto verwendet wird:
 - a. Konfigurationsmodus aufrufen: `aws configure`
 - b. Geben Sie die Zugriffsschlüssel-ID für das von Ihnen erstellte Konto ein.
 - c. Geben Sie den geheimen Zugriffsschlüssel für das von Ihnen erstellte Konto ein.
 - d. Geben Sie die Standardregion ein, die verwendet werden soll. Beispiel: `us-east-1`.
 - e. Geben Sie das zu verwendende Standardausgabeformat ein, oder drücken Sie **Enter**, um JSON auszuwählen.
2. Erstellen eines Buckets:

In diesem Beispiel wird davon ausgegangen, dass Sie einen Load Balancer-Endpunkt für die Verwendung der IP-Adresse 10.96.101.17 und des Ports 10443 konfiguriert haben.

```
aws s3api --endpoint-url https://10.96.101.17:10443
--no-verify-ssl create-bucket --bucket testbucket
```

Wenn der Bucket erfolgreich erstellt wurde, wird der Speicherort des Buckets zurückgegeben, wie im folgenden Beispiel zu sehen:

```
"Location": "/testbucket"
```

3. Hochladen eines Objekts.

```
aws s3api --endpoint-url https://10.96.101.17:10443 --no-verify-ssl  
put-object --bucket testbucket --key s3.pdf --body C:\s3-  
test\upload\s3.pdf
```

Wenn das Objekt erfolgreich hochgeladen wurde, wird ein ETAG zurückgegeben, der ein Hash der Objektdaten ist.

4. Listen Sie den Inhalt des Buckets auf, um zu überprüfen, ob das Objekt hochgeladen wurde.

```
aws s3api --endpoint-url https://10.96.101.17:10443 --no-verify-ssl  
list-objects --bucket testbucket
```

5. Löschen Sie das Objekt.

```
aws s3api --endpoint-url https://10.96.101.17:10443 --no-verify-ssl  
delete-object --bucket testbucket --key s3.pdf
```

6. Löschen Sie den Bucket.

```
aws s3api --endpoint-url https://10.96.101.17:10443 --no-verify-ssl  
delete-bucket --bucket testbucket
```

So implementiert StorageGRID die S3-REST-API

In Konflikt stehende Clientanforderungen

Widersprüchliche Clientanforderungen, wie z. B. zwei Clients, die in denselben Schlüssel schreiben, werden auf der Grundlage der „neuesten Wins“ gelöst.

Der Zeitpunkt für die Bewertung „neuester Erfolge“ basiert auf dem Zeitpunkt, an dem das StorageGRID System eine bestimmte Anforderung abgeschlossen hat und nicht auf dem Zeitpunkt, an dem S3-Clients einen Vorgang starten.

Konsistenzwerte

Konsistenz bietet ein Gleichgewicht zwischen der Verfügbarkeit der Objekte und der

Konsistenz dieser Objekte über verschiedene Storage-Nodes und Standorte hinweg. Sie können die Konsistenz entsprechend den Anforderungen Ihrer Anwendung ändern.

Standardmäßig garantiert StorageGRID eine Lese-/Nachher-Konsistenz für neu erstellte Objekte. Jeder GET nach einem erfolgreich abgeschlossenen PUT wird in der Lage sein, die neu geschriebenen Daten zu lesen. Überschreibungen vorhandener Objekte, Metadatenaktualisierungen und -Löschungen sind schließlich konsistent. Überschreibungen dauern in der Regel nur wenige Sekunden oder Minuten, können jedoch bis zu 15 Tage in Anspruch nehmen.

Wenn Sie Objektoperationen mit einer anderen Konsistenz durchführen möchten, haben Sie folgende Möglichkeiten:

- Geben Sie eine Konsistenz für an [Jeden Eimer](#).
- Geben Sie eine Konsistenz für an [Jeder API-Vorgang](#).
- Ändern Sie die standardmäßige Konsistenz für das gesamte Grid, indem Sie eine der folgenden Aufgaben ausführen:
 - Gehen Sie im Grid Manager zu **CONFIGURATION > System > Storage settings > Default Consistency**.
 - .



Eine Änderung der Konsistenz für das gesamte Grid gilt nur für Buckets, die nach der Änderung der Einstellung erstellt wurden. Informationen zur Bestimmung der Details einer Änderung finden Sie im Auditprotokoll unter `/var/local/log` (suche nach **Konsistenzstufe**).

Konsistenzwerte

Die Konsistenz wirkt sich auf die Verteilung der Metadaten, die StorageGRID zum Nachverfolgen von Objekten verwendet, auf die Nodes aus und damit auf die Verfügbarkeit von Objekten für Client-Anforderungen.

Sie können die Konsistenz für einen Bucket oder eine API-Operation auf einen der folgenden Werte festlegen:

- **All**: Alle Knoten erhalten die Daten sofort, oder die Anfrage schlägt fehl.
- **Strong-global**: Garantiert Lese-nach-Schreiben-Konsistenz für alle Client-Anfragen über alle Standorte hinweg.
- **Strong-site**: Garantiert Lese-nach-Schreiben Konsistenz für alle Client-Anfragen innerhalb einer Site.
- **Read-after-New-write**: (Standard) bietet Read-after-write-Konsistenz für neue Objekte und eventuelle Konsistenz für Objektaktualisierungen. Hochverfügbarkeit und garantierte Datensicherung Empfohlen für die meisten Fälle.
- **Verfügbar**: Bietet eventuelle Konsistenz für neue Objekte und Objekt-Updates. Verwenden Sie für S3-Buckets nur nach Bedarf (z. B. für einen Bucket mit Protokollwerten, die nur selten gelesen werden, oder für HEAD- oder GET-Vorgänge für nicht vorhandene Schlüssel). Nicht unterstützt für S3 FabricPool-Buckets.

Verwenden Sie die Konsistenz „Read-after-New-write“ und „available“

Wenn ein HEAD- oder GET-Vorgang die Konsistenz von Read-after-New-write verwendet, führt StorageGRID die Suche in mehreren Schritten durch:

- Es sieht zunächst das Objekt mit einer niedrigen Konsistenz.

- Wenn diese Suche fehlschlägt, wiederholt sie die Suche beim nächsten Konsistenzwert, bis sie eine Konsistenz erreicht, die dem Verhalten für Strong-Global entspricht.

Wenn eine HEAD- oder GET-Operation die Konsistenz „Read-after-New-write“ verwendet, das Objekt aber nicht existiert, erreicht die Objekt-Lookup immer eine Konsistenz, die dem Verhalten für strong-global entspricht. Da für diese Konsistenz mehrere Kopien der Objektmetadaten an jedem Standort verfügbar sein müssen, können Sie eine hohe Anzahl von 500 internen Serverfehlern erhalten, wenn zwei oder mehr Storage-Nodes am selben Standort nicht verfügbar sind.

Sofern Sie keine Konsistenzgarantien ähnlich Amazon S3 benötigen, können Sie diese Fehler für HEAD- und GET-Operationen verhindern, indem Sie die Konsistenz auf „verfügbar“ setzen. Wenn ein HEAD- oder GET-Betrieb die „verfügbare“ Konsistenz verwendet, bietet StorageGRID letztendlich nur Konsistenz. Bei einem fehlgeschlagenen Vorgang wird nicht erneut versucht, die Konsistenz zu erhöhen, daher müssen nicht mehrere Kopien der Objekt-Metadaten verfügbar sein.

Geben Sie die Konsistenz für den API-Vorgang an

Um die Konsistenz für eine individuelle API-Operation festzulegen, müssen die Konsistenzwerte für den Vorgang unterstützt werden, und Sie müssen die Konsistenz in der Anforderungsheader angeben. In diesem Beispiel wird die Konsistenz für eine GetObject-Operation auf „strong-site“ gesetzt.

```
GET /bucket/object HTTP/1.1
Date: date
Authorization: authorization name
Host: host
Consistency-Control: strong-site
```



Sie müssen für die PutObject- und GetObject-Operationen dieselbe Konsistenz verwenden.

Geben Sie die Konsistenz für Bucket an

Zum Festlegen der Konsistenz für Bucket können Sie die StorageGRID verwenden ["PUT Bucket-Konsistenz"](#) Anfrage. Oder Sie können ["Ändern der Konsistenz eines Buckets"](#) Aus dem Mandantenmanager.

Beachten Sie beim Festlegen der Konsistenz für einen Bucket Folgendes:

- Durch das Festlegen der Konsistenz für einen Bucket wird bestimmt, welche Konsistenz für S3-Vorgänge verwendet wird, die an den Objekten in der Bucket oder in der Bucket-Konfiguration durchgeführt werden. Er hat keine Auswirkungen auf die Vorgänge auf dem Bucket selbst.
- Die Konsistenz einer einzelnen API-Operation überschreibt die Konsistenz für den Bucket.
- Im Allgemeinen sollten Buckets die Standardkonsistenz „Read-after-New-write“ verwenden. Wenn die Anforderungen nicht korrekt funktionieren, ändern Sie das Client-Verhalten der Anwendung, wenn möglich. Oder konfigurieren Sie den Client so, dass die Konsistenz für jede API-Anforderung angegeben wird. Legen Sie die Konsistenz auf Bucket-Ebene nur als letzte Option fest.

wie Konsistenz- und ILM-Regeln interagieren, um den Datenschutz zu beeinträchtigen

Sowohl Ihre Wahl der Konsistenz als auch Ihre ILM-Regel beeinflussen die Art und Weise, wie Objekte geschützt werden. Diese Einstellungen können interagieren.

Beispielsweise wirkt sich die bei der Speicherung eines Objekts verwendete Konsistenz auf die anfängliche

Platzierung von Objekt-Metadaten aus, während das für die ILM-Regel ausgewählte Aufnahmeverhalten sich auf die anfängliche Platzierung von Objektkopien auswirkt. StorageGRID benötigt zur Erfüllung von Clientanfragen Zugriff auf die Metadaten und die Daten eines Objekts. Durch die Auswahl einer passenden Sicherungsstufe für die Konsistenz und das Aufnahmeverhalten können die Daten am Anfang besser gesichert und Systemantworten besser vorhersehbar sein.

Im Folgenden "[Aufnahmeoptionen](#)" Sind für ILM-Regeln verfügbar:

Doppelte Provisionierung

StorageGRID erstellt sofort Zwischenkopien des Objekts und gibt den Erfolg an den Client zurück. Kopien, die in der ILM-Regel angegeben sind, werden nach Möglichkeit erstellt.

Streng

Bevor der Erfolg an den Client zurückgegeben wird, müssen alle in der ILM-Regel angegebenen Kopien erstellt werden.

Ausgeglichen

StorageGRID versucht, bei der Aufnahme alle in der ILM-Regel angegebenen Kopien zu erstellen. Ist dies nicht möglich, werden Zwischenkopien erstellt und der Erfolg wird an den Client zurückgegeben. Die Kopien, die in der ILM-Regel angegeben sind, werden, wenn möglich gemacht.

Beispiel für die Interaktion der Konsistenz- und ILM-Regel

Angenommen, Sie haben ein Grid mit zwei Standorten mit der folgenden ILM-Regel und folgender Konsistenz:

- **ILM-Regel:** Erstellen Sie zwei Objektkopien, eine am lokalen Standort und eine an einem entfernten Standort. Strikte Aufnahme-Verhaltensweise
- **Konsistenz:** Stark-global (Objektmetadaten werden sofort an alle Standorte verteilt).

Wenn ein Client ein Objekt im Grid speichert, erstellt StorageGRID sowohl Objektkopien als auch verteilt Metadaten an beiden Standorten, bevor der Kunde zum Erfolg zurückkehrt.

Das Objekt ist zum Zeitpunkt der Aufnahme der Nachricht vollständig gegen Verlust geschützt. Wenn beispielsweise der lokale Standort kurz nach der Aufnahme verloren geht, befinden sich Kopien der Objektdaten und der Objektmetadaten am Remote-Standort weiterhin. Das Objekt kann vollständig abgerufen werden.

Wenn Sie stattdessen dieselbe ILM-Regel und die Konsistenz für starke Standorte verwenden, erhält der Client möglicherweise eine Erfolgsmeldung, nachdem die Objektdaten am Remote-Standort repliziert wurden, jedoch bevor die Objektmetadaten dort verteilt werden. In diesem Fall entspricht die Sicherung von Objektmetadaten nicht dem Schutzniveau für Objektdaten. Falls der lokale Standort kurz nach der Aufnahme verloren geht, gehen Objektmetadaten verloren. Das Objekt kann nicht abgerufen werden.

Die Beziehung zwischen Konsistenz- und ILM-Regeln kann komplex sein. Wenden Sie sich an den NetApp, wenn Sie Hilfe benötigen.

Objektversionierung

Sie können den Versionsstatus eines Buckets festlegen, wenn Sie mehrere Versionen jedes Objekts beibehalten möchten. Die Aktivierung der Versionierung für einen Bucket kann zum Schutz vor versehentlichem Löschen von Objekten beitragen und ermöglicht es Ihnen, frühere Versionen eines Objekts abzurufen und wiederherzustellen.

Das StorageGRID System implementiert Versionierung mit Unterstützung für die meisten Funktionen und weist einige Einschränkungen auf. StorageGRID unterstützt bis zu 1,000 Versionen jedes Objekts.

Die Objektversionierung kann mit StorageGRID Information Lifecycle Management (ILM) oder mit der S3 Bucket Lifecycle-Konfiguration kombiniert werden. Sie müssen die Versionierung für jeden Bucket explizit aktivieren. Wenn die Versionierung für einen Bucket aktiviert ist, wird jedem dem Bucket hinzugefügten Objekt eine Versions-ID zugewiesen, die vom StorageGRID System generiert wird.

Die Verwendung von MFA (Multi-Faktor-Authentifizierung) Löschen wird nicht unterstützt.



Die Versionierung kann nur auf Buckets aktiviert werden, die mit StorageGRID Version 10.3 oder höher erstellt wurden.

ILM und Versionierung

ILM-Richtlinien werden auf jede Version eines Objekts angewendet. Ein ILM-Scanprozess scannt kontinuierlich alle Objekte und bewertet sie anhand der aktuellen ILM-Richtlinie neu. Alle Änderungen, die Sie an ILM-Richtlinien vornehmen, werden auf alle zuvor aufgenommenen Objekte angewendet. Dies umfasst bereits aufgenommene Versionen, wenn die Versionierung aktiviert ist. Beim ILM-Scannen werden neue ILM-Änderungen an zuvor aufgenommenen Objekten angewendet.

Bei S3-Objekten in versionierungsfähigen Buckets können Sie mithilfe der Versionsunterstützung ILM-Regeln erstellen, die „nicht aktuelle Zeit“ als Referenzzeit verwenden. (Wählen Sie **Ja** für die Frage „Diese Regel nur auf ältere Objektversionen anwenden?“ aus. Zoll ["Schritt 1 des Assistenten zum Erstellen einer ILM-Regel"](#)). Wenn ein Objekt aktualisiert wird, werden seine vorherigen Versionen nicht aktuell. Mithilfe eines Filters „nicht aktuelle Zeit“ können Sie Richtlinien erstellen, die die Auswirkungen vorheriger Objektversionen auf den Storage verringern.



Wenn Sie eine neue Version eines Objekts über einen mehrteiligen Upload-Vorgang hochladen, wird der nicht aktuelle Zeitpunkt für die Originalversion des Objekts angezeigt, wenn der mehrteilige Upload für die neue Version erstellt wurde, nicht erst nach Abschluss des mehrteiligen Uploads. In begrenzten Fällen kann die nicht aktuelle Zeit der ursprünglichen Version Stunden oder Tage früher als die Zeit für die aktuelle Version sein.

Verwandte Informationen

- ["Löschen von S3-versionierten Objekten"](#)
- ["ILM-Regeln und Richtlinien für versionierte S3-Objekte \(Beispiel 4\)"](#).

Konfigurieren Sie die S3-Objektsperre über die S3-REST-API

Wenn die globale S3-Objektsperre für Ihr StorageGRID-System aktiviert ist, können Sie Buckets mit aktivierter S3-Objektsperre erstellen. Sie können für jeden Bucket oder die Aufbewahrungseinstellungen für jede Objektversion die Standardaufbewahrung festlegen.

Aktivieren der S3-Objektsperre für einen Bucket

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

S3 Object Lock ist eine permanente Einstellung, die nur beim Erstellen eines Buckets aktiviert werden kann. Sie können S3-Objektsperre nicht hinzufügen oder deaktivieren, nachdem ein Bucket erstellt wurde.

Verwenden Sie eine der folgenden Methoden, um S3 Object Lock für einen Bucket zu aktivieren:

- Erstellen Sie den Bucket mit Tenant Manager. Siehe "[S3-Bucket erstellen](#)".
- Erstellen Sie den Bucket mithilfe einer CreateBucket-Anforderung mit dem `x-amz-bucket-object-lock-enabled` Kopfzeile der Anfrage. Siehe "[Operationen auf Buckets](#)".

S3 Object Lock erfordert eine Bucket-Versionierung, die beim Erstellen des Buckets automatisch aktiviert wird. Die Versionierung für den Bucket kann nicht unterbrochen werden. Siehe "[Objektversionierung](#)".

Standardeinstellungen für die Aufbewahrung eines Buckets

Wenn S3 Object Lock für einen Bucket aktiviert ist, können Sie optional die Standardaufbewahrung für den Bucket aktivieren und einen Standardaufbewahrungsmodus und die Standardaufbewahrungsdauer festlegen.

Standardaufbewahrungsmodus

- Im COMPLIANCE-Modus:
 - Das Objekt kann erst gelöscht werden, wenn das Aufbewahrungsdatum erreicht ist.
 - Das Aufbewahrungsdatum des Objekts kann erhöht, aber nicht verringert werden.
 - Das Aufbewahrungsdatum des Objekts kann erst entfernt werden, wenn dieses Datum erreicht ist.
- Im GOVERNANCE-Modus:
 - Benutzer mit `s3:BypassGovernanceRetention` Berechtigung kann den verwenden `x-amz-bypass-governance-retention: true` Kopfzeile anfordern, um Aufbewahrungseinstellungen zu umgehen.
 - Diese Benutzer können eine Objektversion löschen, bevor das Aufbewahrungsdatum erreicht ist.
 - Diese Benutzer können das Aufbewahrungsdatum eines Objekts erhöhen, verringern oder entfernen.

Standardaufbewahrungszeitraum

Für jeden Bucket kann ein Standardaufbewahrungszeitraum in Jahren oder Tagen angegeben werden.

Festlegen der Standardaufbewahrung für einen Bucket

Verwenden Sie eine der folgenden Methoden, um die Standardaufbewahrung für einen Bucket festzulegen:

- Managen Sie die Bucket-Einstellungen über den Tenant Manager. Siehe "[Erstellen eines S3-Buckets](#)" Und "[Aktualisieren Sie die S3 Object Lock-Standardaufbewahrung](#)".
- Geben Sie eine PutObjectLockConfiguration-Anforderung für den Bucket aus, um den Standardmodus und die Standardanzahl von Tagen oder Jahren festzulegen.

PutObjectLockKonfiguration

Mit der PutObjectLockConfiguration-Anforderung können Sie den Standardaufbewahrungsmodus und den Standardaufbewahrungszeitraum für einen Bucket festlegen und ändern, für den S3 Object Lock aktiviert ist. Sie können auch zuvor konfigurierte Standardeinstellungen entfernen.

Wenn neue Objektversionen in den Bucket aufgenommen werden, wird der standardmäßige Aufbewahrungsmodus angewendet, wenn `x-amz-object-lock-mode` Und `x-amz-object-lock-retain-until-date` Sind nicht angegeben. Der Standardaufbewahrungszeitraum wird verwendet, um das Aufbewahrungsdatum von IF zu berechnen `x-amz-object-lock-retain-until-date` Ist nicht

angegeben.

Wenn der Standardaufbewahrungszeitraum nach der Aufnahme einer Objektversion geändert wird, bleibt das „bis-Aufbewahrung“-Datum der Objektversion identisch und wird im neuen Standardaufbewahrungszeitraum nicht neu berechnet.

Sie müssen die haben `s3:PutBucketObjectLockConfiguration` Berechtigung, oder Konto `root`, um diesen Vorgang abzuschließen.

Der `Content-MD5` Der Anforderungskopf muss in der PUT-Anforderung angegeben werden.

Anforderungsbeispiel

In diesem Beispiel wird S3 Object Lock für einen Bucket aktiviert und der Standardaufbewahrungsmodus auf COMPLIANCE und der Standardaufbewahrungszeitraum auf 6 Jahre festgelegt.

```
PUT /bucket?object-lock HTTP/1.1
Accept-Encoding: identity
Content-Length: 308
Host: host
Content-MD5: request header
User-Agent: s3sign/1.0.0 requests/2.24.0 python/3.8.2
X-Amz-Date: date
X-Amz-Content-SHA256: authorization-string
Authorization: authorization-string

<ObjectLockConfiguration>
  <ObjectLockEnabled>Enabled</ObjectLockEnabled>
  <Rule>
    <DefaultRetention>
      <Mode>COMPLIANCE</Mode>
      <Years>6</Years>
    </DefaultRetention>
  </Rule>
</ObjectLockConfiguration>
```

Bestimmen der Standardaufbewahrung für einen Bucket

Verwenden Sie eine der folgenden Methoden, um zu ermitteln, ob S3 Object Lock für einen Bucket aktiviert ist und den Standardaufbewahrungsmodus und den Standardaufbewahrungszeitraum anzuzeigen:

- Zeigen Sie den Bucket im Tenant Manager an. Siehe "[S3 Buckets anzeigen](#)".
- Stellen Sie eine `GetObjectLockConfiguration`-Anforderung aus.

GetObjectLockConfiguration

Mit der `GetObjectLockConfiguration`-Anforderung können Sie festlegen, ob S3 Object Lock für einen Bucket aktiviert ist. Wenn diese Option aktiviert ist, können Sie prüfen, ob für den Bucket ein Standardaufbewahrungsmodus und eine Aufbewahrungsfrist konfiguriert sind.

Wenn neue Objektversionen in den Bucket aufgenommen werden, wird der standardmäßige Aufbewahrungsmodus angewendet, wenn `x-amz-object-lock-mode` ist nicht angegeben. Der Standardaufbewahrungszeitraum wird verwendet, um das Aufbewahrungsdatum von IF zu berechnen `x-amz-object-lock-retain-until-date` ist nicht angegeben.

Sie müssen die haben `s3:GetBucketObjectLockConfiguration` Berechtigung, oder Konto `root`, um diesen Vorgang abzuschließen.

Anforderungsbeispiel

```
GET /bucket?object-lock HTTP/1.1
Host: host
Accept-Encoding: identity
User-Agent: aws-cli/1.18.106 Python/3.8.2 Linux/4.4.0-18362-Microsoft
botocore/1.17.29
x-amz-date: date
x-amz-content-sha256: authorization-string
Authorization: authorization-string
```

Antwortbeispiel

```
HTTP/1.1 200 OK
x-amz-id-2:
iVmcB7OXXJRkRH1FiVq1151/T24gRfpwpuZrEG11Bb9ImOMAAe98oxSpX1knabA0LTvBYJpSIX
k=
x-amz-request-id: B34E94CACB2CEF6D
Date: Fri, 04 Sep 2020 22:47:09 GMT
Transfer-Encoding: chunked
Server: AmazonS3

<?xml version="1.0" encoding="UTF-8"?>
<ObjectLockConfiguration xmlns="http://s3.amazonaws.com/doc/2006-03-01/">
  <ObjectLockEnabled>Enabled</ObjectLockEnabled>
  <Rule>
    <DefaultRetention>
      <Mode>COMPLIANCE</Mode>
      <Years>6</Years>
    </DefaultRetention>
  </Rule>
</ObjectLockConfiguration>
```

Festlegen von Aufbewahrungseinstellungen für ein Objekt

Ein Bucket mit aktivierter S3-Objektsperre kann eine Kombination von Objekten mit und ohne Aufbewahrungseinstellungen für S3-Objektsperre enthalten.

Aufbewahrungseinstellungen auf Objektebene werden über die S3-REST-API angegeben. Die Aufbewahrungseinstellungen für ein Objekt überschreiben alle Standardaufbewahrungseinstellungen für den Bucket.

Sie können für jedes Objekt die folgenden Einstellungen festlegen:

- **Retention Mode:** Entweder COMPLIANCE oder GOVERNANCE.
- **Bis-Datum behalten:** Ein Datum, das angibt, wie lange die Objektversion von StorageGRID beibehalten werden muss.
 - Wenn im COMPLIANCE-Modus das Aufbewahrungsdatum in der Zukunft liegt, kann das Objekt abgerufen, aber nicht geändert oder gelöscht werden. Das Aufbewahrungsdatum kann erhöht werden, aber dieses Datum kann nicht verringert oder entfernt werden.
 - Im GOVERNANCE-Modus können Benutzer mit besonderer Berechtigung die Einstellung „bis zum Datum behalten“ umgehen. Sie können eine Objektversion löschen, bevor der Aufbewahrungszeitraum abgelaufen ist. Außerdem können sie das Aufbewahrungsdatum erhöhen, verringern oder sogar entfernen.
- **Legal Hold:** Die Anwendung eines gesetzlichen Hold auf eine Objektversion sperrt diesen Gegenstand sofort. Beispielsweise müssen Sie ein Objekt, das mit einer Untersuchung oder einem Rechtsstreit zusammenhängt, rechtlich festhalten. Eine gesetzliche Aufbewahrungspflichten haben kein Ablaufdatum, bleiben aber bis zur ausdrücklichen Entfernung erhalten.

Die Legal Hold-Einstellung für ein Objekt ist unabhängig vom Aufbewahrungsmodus und dem Aufbewahrungsdatum. Befindet sich eine Objektversion unter einem Legal Hold, kann diese Version nicht gelöscht werden.

Wenn Sie beim Hinzufügen einer Objektversion zu einem Bucket S3-Objektsperreinstellungen angeben möchten, geben Sie ein "PutObject", "CopyObject", Oder "CreateMultipartUpload" Anfrage.

Sie können Folgendes verwenden:

- `x-amz-object-lock-mode`, Die COMPLIANCE oder GOVERNANCE sein können (Groß-/Kleinschreibung beachten).



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

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

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

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

- Der `Content-MD5` Der Anforderungskopf ist erforderlich `x-amz-object-lock-*` Request Header ist in der `PutObject` Anfrage vorhanden. `Content-MD5` Ist für `CopyObject` oder `CreateMultipartUpload` nicht erforderlich.
- Wenn für den Bucket die S3-Objektsperre nicht aktiviert ist und ein `x-amz-object-lock-*` Der Anforderungskopf ist vorhanden, es wird ein 400-Fehler (`InvalidRequest`) zurückgegeben.
- Die `PutObject`-Anfrage unterstützt die Verwendung von `x-amz-storage-class: REDUCED_REDUNDANCY` Passend zum Verhalten von AWS. Wird ein Objekt jedoch mit aktivierter S3-Objektsperre in einen Bucket aufgenommen, führt `StorageGRID` immer eine `Dual-Commit-Aufnahme` durch.
- Eine nachfolgende `GET`- oder `HeadObject`-Versionsantwort enthält die Header `x-amz-object-lock-mode`, `x-amz-object-lock-retain-until-date`, und `x-amz-object-lock-legal-hold`, Wenn konfiguriert und wenn der Anforderungssender die richtige hat `s3:Get*` Berechtigungen.

Sie können das verwenden `s3:object-lock-remaining-retention-days` Policy Condition Key zur Begrenzung der minimalen und maximalen zulässigen Aufbewahrungsfristen für Ihre Objekte.

Aktualisieren von Aufbewahrungseinstellungen für ein Objekt

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

- `PutObjectLegalHold`

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

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

So verwenden Sie **DEN GOVERNANCE-Modus**

Benutzer, die über das verfügen `s3:BypassGovernanceRetention` Berechtigung kann die aktiven Aufbewahrungseinstellungen eines Objekts umgehen, das `DEN GOVERNANCE-Modus` verwendet. Alle **LÖSCHVORGÄNGE** oder `PutObjectRetention` müssen den enthalten `x-amz-bypass-governance-retention:true` Kopfzeile der Anfrage. Diese Benutzer können die folgenden zusätzlichen Vorgänge ausführen:

- Führen Sie `DeleteObject`- oder `DeleteObjects`-Vorgänge durch, um eine Objektversion vor Ablauf des Aufbewahrungszeitraums zu löschen.

Objekte, die sich unter einem `Legal Hold` befinden, können nicht gelöscht werden. `Legal Hold` muss **DEAKTIVIERT** sein.

- Führen Sie PutObjectRetention-Vorgänge durch, die den Modus einer Objektversion vor Ablauf DER Aufbewahrungsfrist von GOVERNANCE in COMPLIANCE ändern.

Die Änderung des Modus von COMPLIANCE zu GOVERNANCE ist niemals zulässig.

- Führen Sie PutObjectRetention-Operationen aus, um die Aufbewahrungsfrist einer Objektversion zu erhöhen, zu verringern oder zu entfernen.

Verwandte Informationen

- ["Objekte managen mit S3 Object Lock"](#)
- ["Verwenden Sie S3 Objektsperre, um Objekte beizubehalten"](#)
- ["Amazon Simple Storage Service Benutzerhandbuch: S3 Object Lock verwenden"](#)

S3-Lebenszykluskonfiguration erstellen

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

Das einfache Beispiel in diesem Abschnitt veranschaulicht, wie eine S3-Lebenszykluskonfiguration das Löschen bestimmter Objekte aus bestimmten S3-Buckets kontrollieren kann. Das Beispiel in diesem Abschnitt dient nur zu Illustrationszwecken. Weitere Informationen zum Erstellen von S3-Lebenszykluskonfigurationen finden Sie unter ["Amazon Simple Storage Service User Guide: Objekt-Lifecycle-Management"](#). Beachten Sie, dass StorageGRID nur Aktionen nach Ablauf unterstützt. Es werden keine Aktionen zur Transition unterstützt.

Welche Lifecycle-Konfiguration ist

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

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

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

Jedes Objekt folgt den Aufbewahrungseinstellungen eines S3 Bucket-Lebenszyklus oder einer ILM-Richtlinie. Wenn ein S3-Bucket-Lebenszyklus konfiguriert ist, überschreiben die Lifecycle-Ablaufaktionen die ILM-Richtlinie für Objekte, die mit dem Bucket-Lifecycle-Filter übereinstimmen. Objekte, die nicht mit dem Bucket-Lebenszyklusfilter übereinstimmen, verwenden die Aufbewahrungseinstellungen der ILM-Richtlinie. Wenn ein Objekt mit einem Bucket-Lebenszyklusfilter übereinstimmt und keine Ablaufaktionen explizit angegeben werden, werden die Aufbewahrungseinstellungen der ILM-Richtlinie nicht verwendet, und es wird impliziert, dass Objektversionen für immer aufbewahrt werden. Siehe ["Beispielprioritäten für den S3-Bucket-Lebenszyklus und die ILM-Richtlinie"](#).

Aus diesem Grund kann ein Objekt aus dem Grid entfernt werden, obwohl die Speicheranweisungen in einer

ILM-Regel noch auf das Objekt gelten. Alternativ kann ein Objekt auch dann im Grid aufbewahrt werden, wenn eine ILM-Platzierungsanleitung für das Objekt abgelaufen ist. Weitere Informationen finden Sie unter ["Funktionsweise von ILM während der gesamten Nutzungsdauer eines Objekts"](#).



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

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

- DeleteBucketLifecycle
- GetBucketLifecycleKonfiguration
- PutBucketLifecycleKonfiguration

Lebenszykluskonfiguration erstellen

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

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



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

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

```

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

```

Lifecycle-Konfiguration auf Bucket anwenden

Nachdem Sie die Lebenszykluskonfigurationsdatei erstellt haben, wenden Sie sie auf einen Bucket an, indem Sie eine Anforderung von `PutBucketLifecycleConfiguration` ausgeben.

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

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

Um zu überprüfen, ob eine Lebenszykluskonfiguration erfolgreich auf den Bucket angewendet wurde, geben Sie eine `GetBucketLifecycleConfiguration`-Anforderung aus. Beispiel:

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

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

Überprüfen, ob der Bucket-Lebenszyklus für das Objekt gilt

Sie können festlegen, ob eine Ablaufregel in der Lebenszykluskonfiguration für ein bestimmtes Objekt gilt, wenn Sie eine `PutObject`-, `HeadObject`- oder `GetObject`-Anforderung ausgeben. Wenn eine Regel zutrifft, enthält die Antwort ein `Expiration` Parameter, der angibt, wann das Objekt abläuft und welche Ablaufregel übereinstimmt.



Da der Bucket-Lebenszyklus ILM überschreibt, wird der `expiry-date` Hier wird das tatsächliche Datum angezeigt, an dem das Objekt gelöscht wird. Weitere Informationen finden Sie unter "[Wie die Aufbewahrung von Objekten bestimmt wird](#)".

Zum Beispiel wurde diese `PutObject`-Anforderung am 22. Juni 2020 ausgegeben und setzt ein Objekt in der `testbucket` Eimer.

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

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

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

Diese HeadObject-Anforderung wurde beispielsweise verwendet, um Metadaten für dasselbe Objekt im testbucket-Bucket zu erhalten.

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

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

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



Für Buckets mit aktivierter Versionierung wird der angezeigte `x-amz-expiration` Antwortkopf gilt nur für aktuelle Versionen von Objekten.

Empfehlungen für die Implementierung der S3-REST-API

Bei der Implementierung der S3-REST-API zur Verwendung mit StorageGRID sollten Sie diese Empfehlungen beachten.

Empfehlungen für Köpfe zu nicht vorhandenen Objekten

Wenn Ihre Anwendung regelmäßig prüft, ob ein Objekt an einem Pfad existiert, wo Sie nicht erwarten, dass das Objekt tatsächlich existiert, sollten Sie die Option „verfügbar“ verwenden. **Konsistenz**. Sie sollten beispielsweise die Konsistenz „verfügbar“ verwenden, wenn Ihre Anwendung einen Speicherort vorgibt, bevor Sie ihn verwenden.

Wenn der HAUPTVORGANG das Objekt nicht findet, erhalten Sie möglicherweise eine hohe Anzahl von 500 internen Serverfehlern, wenn zwei oder mehr Storage Nodes am selben Standort nicht verfügbar sind oder ein Remote-Standort nicht erreichbar ist.

Sie können die „verfügbaren“ Konsistenz für jeden Bucket mithilfe von festlegen **PUT Bucket-Konsistenz**

Anforderung oder Sie können die Konsistenz in der Anforderungsheader für eine einzelne API-Operation angeben.

Empfehlungen für Objektschlüssel

Befolgen Sie diese Empfehlungen für Objektschlüsselnamen auf Basis des ersten Erstellts des Buckets.

Buckets, die in StorageGRID 11.4 oder früher erstellt wurden

- Verwenden Sie keine Zufallswerte als die ersten vier Zeichen von Objektschlüsseln. Dies steht im Gegensatz zu der früheren AWS Empfehlung für wichtige Präfixe. Verwenden Sie stattdessen nicht zufällige, nicht eindeutige Präfixe, z. B. `image`.
- Wenn Sie der früheren AWS-Empfehlung folgen, zufällige und eindeutige Zeichen in Schlüsselpräfixen zu verwenden, setzen Sie den Objektschlüsseln einen Verzeichnisnamen vor. Verwenden Sie dieses Format:

```
mybucket/mydir/f8e3-image3132.jpg
```

Anstelle dieses Formats:

```
mybucket/f8e3-image3132.jpg
```

Buckets, die in StorageGRID 11.4 oder höher erstellt wurden

Es ist nicht erforderlich, Objektschlüsselnamen auf die Best Practices für die Performance zu beschränken. In den meisten Fällen können Sie zufällige Werte für die ersten vier Zeichen von Objektschlüsselnamen verwenden.



Eine Ausnahme ist ein S3-Workload, der nach kurzer Zeit kontinuierlich alle Objekte entfernt. Um die Auswirkungen auf die Performance in diesem Anwendungsfall zu minimieren, variieren Sie alle tausend Objekte mit einem ähnlichen Datum einen führenden Teil des Schlüsselnamens. Angenommen, ein S3-Client schreibt in der Regel 2,000 Objekte/Sekunde, und die ILM- oder Bucket-Lifecycle-Richtlinie entfernt alle Objekte nach drei Tagen. Um die Auswirkungen auf die Performance zu minimieren, können Sie Schlüssel anhand eines Musters wie folgt benennen: `/mybucket/mydir/yyyymmddhhmmss-random_UUID.jpg`

Empfehlungen für „Range Reads“

Wenn der "[Globale Option zum Komprimieren gespeicherter Objekte](#)" Ist aktiviert, sollten S3-Client-Anwendungen die Ausführung von `GetObject`-Operationen vermeiden, die einen Bereich von Bytes angeben, die zurückgegeben werden sollen. Diese Vorgänge beim Lesen von Range sind ineffizient, da StorageGRID Objekte effektiv dekomprimieren muss, um auf die angeforderten Bytes zuzugreifen. `GetObject` Operationen, die einen kleinen Bereich von Bytes von einem sehr großen Objekt anfordern, sind besonders ineffizient; zum Beispiel ist es ineffizient, einen 10 MB Bereich von einem 50 GB komprimierten Objekt zu lesen.

Wenn Bereiche von komprimierten Objekten gelesen werden, können Client-Anforderungen eine Zeitdauer haben.



Wenn Sie Objekte komprimieren müssen und Ihre Client-Applikation Bereichslesevorgänge verwenden muss, erhöhen Sie die Zeitüberschreitung beim Lesen der Anwendung.

Unterstützung für Amazon S3-REST-API

Details zur S3-REST-API-Implementierung

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

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

Umgang mit Daten

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

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

Allgemeine Anfragemöpfe

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

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

Allgemeine Antwortkopfzeilen

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

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

Authentifizieren von Anfragen

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

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

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

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

Verwenden Sie den HTTP-Autorisierungskopf

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

Abfrageparameter verwenden

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

Betrieb auf dem Service

Das StorageGRID System unterstützt die folgenden Vorgänge beim Service.

Betrieb	Implementierung
ListBuchs (Zuvor „GET Service“ genannt)	Wird mit dem gesamten Amazon S3-REST-API-Verhalten implementiert. Änderungen vorbehalten.
GET Storage-Auslastung	Das StorageGRID " GET Storage-Auslastung " Die Anforderung gibt an, wie viel Speicherplatz von einem Konto und für jeden mit dem Konto verknüpften Bucket insgesamt verwendet wird. Dies ist eine Operation auf dem Dienst mit einem Pfad von / und einem benutzerdefinierten Abfrageparameter (<code>?x-ntap-sg-usage</code>) Hinzugefügt.
OPTIONEN /	Client-Applikationen können Probleme haben <code>OPTIONS</code> / Anfragen an den S3-Port auf einem Storage-Node ohne die Zugangsdaten für die S3-Authentifizierung, um zu ermitteln, ob der Storage-Node verfügbar ist. Sie können diese Anforderung zum Monitoring verwenden oder um zu ermöglichen, dass externe Load Balancer eingesetzt werden, wenn ein Storage-Node ausfällt.

Operationen auf Buckets

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

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

Weitere Informationen finden Sie im Folgenden:

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

Die Operationen ListObjects (GET Bucket) und ListObjectVersions (GET Bucket Object Versions) unterstützen StorageGRID ["Konsistenzwerte"](#).

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

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

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

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

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

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

Betrieb	Implementierung
<p>PutBucketNotificationKonfiguration</p> <p>(Zuvor namens „PUT Bucket“-Benachrichtigung)</p>	<p>Konfiguriert Benachrichtigungen für den Bucket mithilfe der XML-Benachrichtigungskonfiguration, die im Anforderungskörper enthalten ist. Sie sollten folgende Implementierungsdetails kennen:</p> <ul style="list-style-type: none"> • StorageGRID unterstützt als Ziele Amazon Simple Notification Service (Amazon SNS) oder Kafka-Themen. SQS (Simple Queue Service)- oder Amazon Lambda-Endpunkte werden nicht unterstützt. • Das Ziel für Benachrichtigungen muss als URN eines StorageGRID-Endpunkts angegeben werden. Endpunkte können mit dem Mandanten-Manager oder der Mandanten-Management-API erstellt werden. <p>Der Endpunkt muss vorhanden sein, damit die Benachrichtigungskonfiguration erfolgreich ausgeführt werden kann. Wenn der Endpunkt nicht vorhanden ist, A 400 Bad Request Der Code gibt einen Fehler zurück InvalidArgument.</p> <ul style="list-style-type: none"> • Sie können keine Benachrichtigung für die folgenden Ereignistypen konfigurieren. Diese Ereignistypen werden nicht unterstützt. <ul style="list-style-type: none"> ◦ s3:ReducedRedundancyLostObject ◦ s3:ObjectRestore:Completed • Aus StorageGRID gesendete Ereignisbenachrichtigungen verwenden das JSON-Standardformat, außer dass sie einige Schlüssel nicht enthalten und bestimmte Werte für andere verwenden, wie in der folgenden Liste gezeigt: <ul style="list-style-type: none"> ◦ EventSource <li style="padding-left: 20px;">sgws:s3 ◦ AwsRegion <li style="padding-left: 20px;">Nicht enthalten ◦ * X-amz-id-2* <li style="padding-left: 20px;">Nicht enthalten ◦ arn <li style="padding-left: 20px;">urn:sgws:s3:::bucket_name
<p>PutBucketPolicy</p>	<p>Legt die dem Bucket angehängte Richtlinie fest. Siehe "Verwendung von Bucket- und Gruppenzugriffsrichtlinien".</p>

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

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

Operationen für Objekte

Operationen für Objekte

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

Die folgenden Bedingungen gelten für alle Objektvorgänge:

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

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

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

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

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

Verwenden Sie S3 Select

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



Nicht aufgeführte Elemente werden nicht unterstützt.

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

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

Klauseln

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

Datentypen

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

Operatoren

Logische Operatoren

- UND
- NICHT
- ODER

Vergleichsoperatoren

- <
- >
- ≪=
- >=
- =
- =
- <>

- !=
- ZWISCHEN
- IN

Operatoren für die Musteranpassung

- GEFÄLLT MIR
- _
- %

Einheitliche Operatoren

- IST NULL
- IST NICHT NULL

Mathematische Operatoren

- +
- -
- *
- /
- %

StorageGRID folgt der Priorität des Amazon S3 Select-Operators.

Aggregatfunktionen

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

Bedingte Funktionen

- FALL
- ZUSAMMENSCHMELZEN
- NULL LIF

Konvertierungsfunktionen

- CAST (für unterstützten Datentyp)

Datumsfunktionen

- DATUM_HINZUFÜGEN
- DATE_DIFF

- EXTRAHIEREN
- TO_STRING
- TO_ZEITSTEMPEL
- UTCNOW

Zeichenfolgenfunktionen

- CHAR_LENGTH, CHARACTER_LENGTH
- NIEDRIGER
- TEILSTRING
- TRIMMEN
- OBEN

Serverseitige Verschlüsselung

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

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

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

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



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



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

Verwenden Sie SSE

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

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

Der SSE-Anforderungsheader wird durch die folgenden Objektoperationen unterstützt:

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

Verwenden Sie SSE-C

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

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

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

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

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

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

- Sie müssen https verwenden.



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

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



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

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

Verwandte Informationen

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

CopyObject

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

Konflikte lösen

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

Objektgröße

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

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



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

UTF-8 Zeichen in Benutzermetadaten

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

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

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

Unterstützte Anfrageheader

Die folgenden Anfragezeilen werden unterstützt:

- `Content-Type`
- `x-amz-copy-source`
- `x-amz-copy-source-if-match`
- `x-amz-copy-source-if-none-match`
- `x-amz-copy-source-if-unmodified-since`
- `x-amz-copy-source-if-modified-since`
- `x-amz-meta-`, Gefolgt von einem Name-Wert-Paar mit benutzerdefinierten Metadaten
- `x-amz-metadata-directive`: Der Standardwert ist `COPY`, Mit der Sie das Objekt und die zugehörigen Metadaten kopieren können.

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

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

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

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

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

- **SSE-Anfragezeilen:**
 - `x-amz-copy-source-server-side-encryption-customer-algorithm`
 - `x-amz-copy-source-server-side-encryption-customer-key`

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

Siehe [Anforderungsheader für serverseitige Verschlüsselung](#)

Nicht unterstützte Anforderungsheader

Die folgenden Anforderungsheader werden nicht unterstützt:

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

Optionen der Storage-Klasse

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

- STANDARD

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

- REDUCED_REDUNDANCY

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



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

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

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

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

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

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

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

Anforderungsheader für serverseitige Verschlüsselung

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

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



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

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



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

Versionierung

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

GetObject

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

GetObject- und mehrteilige Objekte

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

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

UTF-8 Zeichen in Benutzermetadaten

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

Nicht unterstützte Anforderungsüberschrift

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

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

Versionierung

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

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

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

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



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

Verhalten von `GetObject` for Cloud Storage Pool Objects

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



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

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

Mehrteilige oder segmentierte Objekte in einem Cloud Storage-Pool

Wenn Sie ein mehrteilige Objekt hochgeladen StorageGRID oder ein großes Objekt in Segmente aufgeteilt

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

In diesen Fällen:

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

GetObject- und Grid-übergreifende Replikation

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

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



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

HeadObject

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

HeadObject- und mehrteilige Objekte

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

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

UTF-8 Zeichen in Benutzermetadaten

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

geben den nicht zurück `x-amz-missing-meta` Kopfzeile, wenn der Schlüsselname oder -Wert nicht druckbare Zeichen enthält.

Nicht unterstützte Anforderungsüberschrift

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

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

Versionierung

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

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

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

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



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

HeadObject-Antworten für Cloud-Storage-Pool-Objekte

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

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

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

Status des Objekts	Antwort auf HeadObject
Objekt, das in StorageGRID aufgenommen wurde, durch ILM jedoch noch nicht evaluiert wurde, oder Objekt, das in einem herkömmlichen Storage-Pool gespeichert ist oder Erasure Coding verwendet	200 OK (Es wird keine spezielle Antwortheader zurückgegeben.)

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

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

Mehrteilige oder segmentierte Objekte in Cloud Storage Pool

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

HeadObject- und Grid-übergreifende Replikation

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

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



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

PutObject

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

Konflikte lösen

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

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

Objektgröße

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

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



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

Größe der Benutzer-Metadaten

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

UTF-8 Zeichen in Benutzermetadaten

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

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

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

Grenzwerte für Objekt-Tags

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

Objekteigentümer

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

Unterstützte Anfrageheader

Die folgenden Anfragezeilen werden unterstützt:

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

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

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

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

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

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

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

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

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

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



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

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

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

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

- SSE-Anfragezeilen:

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

Siehe [Anforderungsheader für serverseitige Verschlüsselung](#)

Nicht unterstützte Anforderungsheader

Die folgenden Anforderungsheader werden nicht unterstützt:

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

Optionen der Storage-Klasse

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

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

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

- STANDARD (Standard)
 - **Dual Commit:** Wenn die ILM-Regel die Dual Commit-Option für das Aufnahmeverhalten angibt, sobald ein Objekt aufgenommen wird, wird eine zweite Kopie dieses Objekts erstellt und auf einen anderen Storage Node verteilt (Dual Commit). Bei Bewertung des ILM bestimmt StorageGRID, ob diese ersten Zwischenkopien die Anweisungen zur Platzierung in der Regel erfüllen. Ist dies nicht der Fall, müssen möglicherweise neue Objektkopien an unterschiedlichen Standorten erstellt werden, und die ersten Zwischenkopien müssen eventuell gelöscht werden.
 - **Ausgeglichen:** Wenn die ILM-Regel die Option ausgeglichen angibt und StorageGRID nicht sofort alle in der Regel angegebenen Kopien erstellen kann, erstellt StorageGRID zwei Zwischenkopien auf verschiedenen Speicherknoten.

Wenn StorageGRID sofort alle Objektkopien erstellen kann, die in der ILM-Regel (synchrone Platzierung) angegeben sind, wird der angezeigt `x-amz-storage-class` Kopfzeile hat keine Wirkung.

- `REDUCED_REDUNDANCY`

- **Dual Commit:** Wenn die ILM-Regel die Dual Commit-Option für das Aufnahmeverhalten angibt, erstellt StorageGRID bei Aufnahme des Objekts eine einzelne Interimskopie (Single Commit).
- **Ausgeglichen:** Wenn die ILM-Regel die Option ausgeglichen angibt, erstellt StorageGRID nur eine Zwischenkopie, wenn das System nicht sofort alle in der Regel angegebenen Kopien erstellen kann. Wenn StorageGRID eine synchrone Platzierung durchführen kann, hat diese Kopfzeile keine Auswirkung.

Der `REDUCED_REDUNDANCY` Am besten eignet sich die Option, wenn die ILM-Regel, die mit dem Objekt übereinstimmt, eine einzige replizierte Kopie erstellt. In diesem Fall verwenden `REDUCED_REDUNDANCY` Eine zusätzliche Objektkopie kann bei jedem Aufnahmevorgang nicht mehr erstellt und gelöscht werden.

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



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

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



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

Anforderungsheader für serverseitige Verschlüsselung

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

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



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



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

Versionierung

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

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

Signaturberechnungen für den Autorisierungskopf

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

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



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

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

Verwandte Informationen

["Objektmanagement mit ILM"](#)

Objekt `restoreObject`

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

Unterstützter Anforderungstyp

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

Versionierung

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

wiederhergestellt

Verhalten von RestoreObject auf Cloud-Storage-Pool-Objekten

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



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

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

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

SelektierObjectContent

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

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

Bevor Sie beginnen

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

Beispiel für eine CSV-Anfrage-Syntax

```

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

```

Beispiel für die Syntax der Parkettanforderung

```

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

```

Beispiel für eine SQL-Abfrage

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

```

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

```

Die ersten Zeilen der abzufragenden Datei, SUB-EST2020_ALL.csv, So aussehen:

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

Beispiel für die Verwendung von AWS und CLI (CSV)

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

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

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

Beispiel für die Nutzung von AWS-CLI (Parkett)

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

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

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

Vorgänge für mehrteilige Uploads

Operationen für mehrteilige Uploads: Übersicht

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

Die folgenden Bedingungen und Hinweise gelten für alle mehrteiligen Uploadvorgänge:

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

Objekts möglicherweise nicht die aktuellen ILM-Anforderungen, wenn der mehrteilige Upload abgeschlossen ist. Alle nicht korrekt platzierten Teile werden in die Warteschlange zur erneuten ILM-Bewertung gestellt und später an den richtigen Ort verschoben.

- Bei der Evaluierung von ILM für ein Teil filtert StorageGRID nach der Größe des Teils und nicht der Größe des Objekts. Das bedeutet, dass Teile eines Objekts an Orten gespeichert werden können, die die ILM-Anforderungen für das gesamte Objekt nicht erfüllen. Wenn z. B. in einer Regel festgelegt wird, dass alle Objekte mit 10 GB oder mehr bei DC1 gespeichert werden, während alle kleineren Objekte bei DC2 gespeichert sind, wird jeder 1-GB-Teil eines 10-teiligen mehrteiligen Uploads bei DC2 beim Einspielen gespeichert. Wird ILM für das gesamte Objekt evaluiert, werden alle Teile des Objekts nach DC1 verschoben.
- Alle mehrteiligen Uploads unterstützen StorageGRID "[Konsistenzwerte](#)".
- Nach Bedarf können Sie verwenden "[Serverseitige Verschlüsselung](#)" Mit mehrteiligen Uploads. Um SSE (serverseitige Verschlüsselung mit über StorageGRID gemanagten Schlüsseln) zu verwenden, müssen Sie das angeben `x-amz-server-side-encryption` Request Header nur in der `CreateMultipartUpload`-Anforderung. Um SSE-C (serverseitige Verschlüsselung mit vom Kunden bereitgestellten Schlüsseln) zu verwenden, geben Sie in der `CreateMultipartUpload`-Anforderung und in jeder nachfolgenden `UploadPart`-Anforderung die gleichen drei Verschlüsselungsschlüsselanforderungsheader an.

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

CompleteMultipartUpload

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

Konflikte lösen

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

Anfragekopfzeilen

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

- STANDARD

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

- REDUCED_REDUNDANCY

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



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



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

Versionierung

Durch diesen Vorgang ist ein mehrteiliger Upload abgeschlossen. Wenn die Versionierung für einen Bucket aktiviert ist, wird die Objektversion nach Abschluss des mehrteiligen Uploads erstellt.

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

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



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

Fehlgeschlagene Replikation, Benachrichtigung oder Metadatenbenachrichtigung

Wenn der Bucket, in dem der mehrteilige Upload stattfindet, für einen Plattformdienst konfiguriert ist, ist der

mehrteilige Upload erfolgreich, auch wenn die zugehörige Replizierungs- oder Benachrichtigungsaktion fehlschlägt.

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

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

CreateMultipartUpload

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

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

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

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

- STANDARD (Standard)
 - **Dual Commit:** Wenn die ILM-Regel die Option Dual Commit Ingest angibt, wird, sobald ein Objekt aufgenommen wird, eine zweite Kopie dieses Objekts erstellt und an einen anderen Storage Node verteilt (Dual Commit). Bei Bewertung des ILM bestimmt StorageGRID, ob diese ersten Zwischenkopien die Anweisungen zur Platzierung in der Regel erfüllen. Ist dies nicht der Fall, müssen möglicherweise neue Objektkopien an unterschiedlichen Standorten erstellt werden, und die ersten Zwischenkopien müssen eventuell gelöscht werden.
 - **Ausgeglichen:** Wenn die ILM-Regel die Option ausgeglichen angibt und StorageGRID nicht sofort alle in der Regel angegebenen Kopien erstellen kann, erstellt StorageGRID zwei Zwischenkopien auf verschiedenen Speicherknoten.

Wenn StorageGRID sofort alle Objektkopien erstellen kann, die in der ILM-Regel (synchrone Platzierung) angegeben sind, wird der angezeigt `x-amz-storage-class` Kopfzeile hat keine Wirkung.

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

`REDUCED_REDUNDANCY` Eine zusätzliche Objektkopie kann bei jedem Aufnahmevorgang nicht mehr erstellt und gelöscht werden.

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



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

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



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

Die folgenden Anfragezeilen werden unterstützt:

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

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

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

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

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

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



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

- S3-Objektsperungs-Anfrageheader:

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

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

"Konfigurieren Sie die S3-Objektsperre über die S3-REST-API"

- SSE-Anfragezeilen:

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

Anforderungsheader für serverseitige Verschlüsselung



Informationen darüber, wie StorageGRID UTF-8-Zeichen verarbeitet, finden Sie unter "PutObject".

Anforderungsheader für serverseitige Verschlüsselung

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

- **SSE:** Verwenden Sie den folgenden Header in der CreateMultipartUpload-Anfrage, wenn Sie das Objekt mit einem eindeutigen Schlüssel verschlüsseln möchten, der von StorageGRID verwaltet wird. Geben Sie diesen Header in keiner der UploadPart-Anforderungen an.

- x-amz-server-side-encryption

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

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



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

Nicht unterstützte Anforderungsheader

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

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

Versionierung

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

ListMultipartUploads

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

Die folgenden Anforderungsparameter werden unterstützt:

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

Versionierung

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

UploadTeil

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

Unterstützte Anfrageheader

Die folgenden Anfragezeilen werden unterstützt:

- `Content-Length`
- `Content-MD5`

Anforderungsheader für serverseitige Verschlüsselung

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

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



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

Versionierung

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

UploadPartCopy

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

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

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

Die folgenden Anfragezeilen werden unterstützt:

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

Anforderungsheader für serverseitige Verschlüsselung

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

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

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

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



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

Versionierung

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

Fehlerantworten

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

Unterstützte S3-API-Fehlercodes

Name	HTTP-Status
AccessDenied	403 Verbotene
BadDigest	400 Fehlerhafte Anfrage
BucketAlreadyExists	409 Konflikt
BucketNotEmpty	409 Konflikt
IncompleteBody	400 Fehlerhafte Anfrage
Interner Fehler	500 Fehler Des Internen Servers
InvalidAccessKey ID	403 Verbotene
InvalidArgument	400 Fehlerhafte Anfrage
InvalidBucketName	400 Fehlerhafte Anfrage
InvalidBucketState	409 Konflikt

Name	HTTP-Status
InvalidDigest	400 Fehlerhafte Anfrage
InvalidVerschlüsselungAlgorithmFehler	400 Fehlerhafte Anfrage
InvalidTeil	400 Fehlerhafte Anfrage
InvalidPartOrder	400 Fehlerhafte Anfrage
InvalidRange	416 Angeforderter Bereich Nicht Zu Unterprüfbar
InvalidRequest	400 Fehlerhafte Anfrage
InvalidStorageClass	400 Fehlerhafte Anfrage
InvalidTag	400 Fehlerhafte Anfrage
InvalidURI	400 Fehlerhafte Anfrage
KeyTooLong	400 Fehlerhafte Anfrage
MalformedXML	400 Fehlerhafte Anfrage
MetadataTooLarge	400 Fehlerhafte Anfrage
MethodenAlled	405 Methode Nicht Zulässig
MissingContentLänge	411 Länge Erforderlich
MissingRequestBodyError	400 Fehlerhafte Anfrage
MissingSecurityHeader	400 Fehlerhafte Anfrage
NoSuchBucket	404 Nicht Gefunden
NoSuchKey	404 Nicht Gefunden
NoSuchUpload	404 Nicht Gefunden
NotImplemsted	501 Nicht Implementiert
NoSuchBucketRichtlinien	404 Nicht Gefunden
ObjektLockKonfigurationNotgefundenFehler	404 Nicht Gefunden

Name	HTTP-Status
Vorbedingungen nicht möglich	412 Voraussetzung Fehlgeschlagen
AnforderungTimeTooSkewed	403 Verbotene
Servicenicht verfügbar	503 Service Nicht Verfügbar
SignalDoesNotMatch	403 Verbotene
TooManyDickets	400 Fehlerhafte Anfrage
UserKeyMustBespezifiziert	400 Fehlerhafte Anfrage

Benutzerdefinierte StorageGRID-Fehlercodes

Name	Beschreibung	HTTP-Status
XBucketLifecycleNotAlled	In einem zuvor konformen Bucket ist die Konfiguration des Bucket-Lebenszyklus nicht zulässig	400 Fehlerhafte Anfrage
XBucketPolicyParseException	Fehler beim Parsen der JSON der empfangenen Bucket-Richtlinie.	400 Fehlerhafte Anfrage
XComplianceKonflikt	Vorgang aufgrund von Compliance-Einstellungen abgelehnt.	403 Verbotene
XComplianceReducedRAID-RedundanzVerbotenen	Reduzierte Redundanz ist in einem älteren, konformen Bucket nicht zulässig	400 Fehlerhafte Anfrage
XMaxBucketPolicyLengthexceed	Ihre Richtlinie überschreitet die maximal zulässige Länge der Bucket-Richtlinie.	400 Fehlerhafte Anfrage
XMissingInternRequestHeader	Eine Kopfzeile einer internen Anforderung fehlt.	400 Fehlerhafte Anfrage
XNoSuchBucketCompliance	Für den angegebenen Bucket ist die veraltete Compliance nicht aktiviert.	404 Nicht Gefunden
XNotAcceptable	Die Anforderung enthält mindestens einen Übernehmen-Header, der nicht erfüllt werden konnte.	406 Nicht Akzeptabel
XNotImplemsted	Die von Ihnen gestellte Anfrage beinhaltet Funktionen, die nicht implementiert sind.	501 Nicht Implementiert

Benutzerdefinierte Operationen von StorageGRID

Benutzerdefinierte StorageGRID Operationen: Überblick

Das StorageGRID System unterstützt benutzerdefinierte Vorgänge, die zur S3-REST-API hinzugefügt werden.

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

Betrieb	Beschreibung
"Get Bucket-Konsistenz"	Gibt die Konsistenz zurück, die auf einen bestimmten Bucket angewendet wird.
"PUT Bucket-Konsistenz"	Legt die Konsistenz fest, die auf einen bestimmten Bucket angewendet wird.
"ZEITPUNKT des letzten Zugriffs FÜR den Bucket ABRUFEN"	Gibt an, ob Updates der letzten Zugriffszeit für einen bestimmten Bucket aktiviert oder deaktiviert wurden.
"PUT Bucket-Zeit für den letzten Zugriff"	Hiermit können Sie Updates der letzten Zugriffszeit für einen bestimmten Bucket aktivieren oder deaktivieren.
"Konfiguration für die Benachrichtigung über Bucket-Metadaten LÖSCHEN"	Löscht die XML-Konfiguration für die Metadatenbenachrichtigung, die mit einem bestimmten Bucket verknüpft ist.
"Konfiguration der Bucket-Metadaten-Benachrichtigungen ABRUFEN"	Gibt die XML-XML-Benachrichtigungskonfiguration für Metadaten zurück, die einem bestimmten Bucket zugeordnet ist.
"PUT Bucket-Metadaten-Benachrichtigungskonfiguration"	Konfiguriert den Metadaten-Benachrichtigungsdienst für einen Bucket
"GET Storage-Auslastung"	Gibt an, wie viel Speicherplatz von einem Konto und für jeden mit dem Konto verknüpften Bucket insgesamt verwendet wird.
"Veraltet: CreateBucket mit Compliance-Einstellungen"	Veraltet und nicht unterstützt: Sie können keine neuen Buckets mit aktivierter Compliance mehr erstellen.
"Veraltet: EINHALTUNG von Bucket ABRUFEN"	Veraltet, aber unterstützt: Gibt die Compliance-Einstellungen zurück, die derzeit für einen vorhandenen Legacy-konformen Bucket wirksam sind.
"Veraltet: EINHALTUNG VON PUT Bucket"	Veraltet, aber unterstützt: Ermöglicht es Ihnen, die Compliance-Einstellungen für einen vorhandenen, älteren konformen Bucket zu ändern.

Get Bucket-Konsistenz

Mit der Konsistenzanforderung für GET Bucket können Sie die Konsistenz bestimmen, die auf einen bestimmten Bucket angewendet wird.

Die Standardkonsistenz ist so festgelegt, dass „Read-after-write“ für neu erstellte Objekte garantiert wird.

Sie müssen über die Berechtigung `s3:GetBucketConsistency` verfügen oder als Account root vorliegen, um diesen Vorgang abzuschließen.

Anforderungsbeispiel

```
GET /bucket?x-ntap-sg-consistency HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

Antwort

In der XML-Antwortantwort `<Consistency>` Gibt einen der folgenden Werte zurück:

Konsistenz	Beschreibung
Alle	Alle Nodes erhalten die Daten sofort, sonst schlägt die Anfrage fehl.
Stark global	Garantierte Konsistenz bei Lese-nach-Schreibvorgängen für alle Client-Anfragen an allen Standorten.
Stark vor Ort	Garantiert Konsistenz bei Lese-nach-Schreibvorgängen für alle Client-Anfragen innerhalb eines Standorts.
Read-after-New-Write-Funktion	(Standard) konsistente Lese-/Schreibvorgänge für neue Objekte und eventuelle Konsistenz bei Objekt-Updates. Hochverfügbarkeit und garantierte Datensicherung Empfohlen für die meisten Fälle.
Verfügbar	Bietet eventuelle Konsistenz für neue Objekte und Objektaktualisierungen. Verwenden Sie für S3-Buckets nur nach Bedarf (z. B. für einen Bucket mit Protokollwerten, die nur selten gelesen werden, oder für HEAD- oder GET-Vorgänge für nicht vorhandene Schlüssel). Nicht unterstützt für S3 FabricPool-Buckets.

Antwortbeispiel

```
HTTP/1.1 200 OK
Date: Fri, 18 Sep 2020 01:02:18 GMT
Connection: CLOSE
Server: StorageGRID/11.5.0
x-amz-request-id: 12345
Content-Length: 127
Content-Type: application/xml

<?xml version="1.0" encoding="UTF-8"?>
<Consistency xmlns="http://s3.storagegrid.com/doc/2015-02-01/">read-after-
new-write</Consistency>
```

Verwandte Informationen

["Konsistenzwerte"](#)

PUT Bucket-Konsistenz

Mit der Konsistenzanforderung für PUT-Bucket können Sie die Konsistenz angeben, die auf Vorgänge angewendet werden soll, die auf einen Bucket ausgeführt wurden.

Die Standardkonsistenz ist so festgelegt, dass „Read-after-write“ für neu erstellte Objekte garantiert wird.

Bevor Sie beginnen

Sie müssen über die berechtigung `s3:PutBucketConsistency` verfügen oder als Account root vorliegen, um diesen Vorgang abzuschließen.

Anfrage

Der `x-ntap-sg-consistency` Parameter muss einen der folgenden Werte enthalten:

Konsistenz	Beschreibung
Alle	Alle Nodes erhalten die Daten sofort, sonst schlägt die Anfrage fehl.
Stark global	Garantierte Konsistenz bei Lese-nach-Schreibvorgängen für alle Client-Anfragen an allen Standorten.
Stark vor Ort	Garantiert Konsistenz bei Lese-nach-Schreibvorgängen für alle Client-Anfragen innerhalb eines Standorts.
Read-after-New-Write-Funktion	(Standard) konsistente Lese-/Schreibvorgänge für neue Objekte und eventuelle Konsistenz bei Objekt-Updates. Hochverfügbarkeit und garantierte Datensicherung Empfohlen für die meisten Fälle.

Konsistenz	Beschreibung
Verfügbar	Bietet eventuelle Konsistenz für neue Objekte und Objektaktualisierungen. Verwenden Sie für S3-Buckets nur nach Bedarf (z. B. für einen Bucket mit Protokollwerten, die nur selten gelesen werden, oder für HEAD- oder GET-Vorgänge für nicht vorhandene Schlüssel). Nicht unterstützt für S3 FabricPool-Buckets.

Anmerkung: im Allgemeinen sollten Sie die "Read-after-New-write" Konsistenz verwenden. Wenn die Anforderungen nicht korrekt funktionieren, ändern Sie das Client-Verhalten der Anwendung, wenn möglich. Oder konfigurieren Sie den Client so, dass die Konsistenz für jede API-Anforderung angegeben wird. Legen Sie die Konsistenz auf Bucket-Ebene nur als letzte Option fest.

Anforderungsbeispiel

```
PUT /bucket?x-ntap-sg-consistency=strong-global HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

Verwandte Informationen

["Konsistenzwerte"](#)

ZEITPUNKT des letzten Zugriffs FÜR den Bucket ABRUFEN

In der Anforderung „letzte Bucket-Zugriffszeit“ KÖNNEN Sie festlegen, ob Updates der letzten Zugriffszeit für einzelne Buckets aktiviert oder deaktiviert sind.

Sie müssen über die berechtigung `s3:GetBucketLastAccessTime` verfügen oder als Kontostamm vorliegen, um diesen Vorgang abzuschließen.

Anforderungsbeispiel

```
GET /bucket?x-ntap-sg-lastaccesstime HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

Antwortbeispiel

Dieses Beispiel zeigt, dass Updates der letzten Zugriffszeit für den Bucket aktiviert sind.

```
HTTP/1.1 200 OK
Date: Sat, 29 Nov 2015 01:02:18 GMT
Connection: CLOSE
Server: StorageGRID/10.3.0
x-amz-request-id: 12345
Content-Length: 127
Content-Type: application/xml

<?xml version="1.0" encoding="UTF-8"?>
<LastAccessTime xmlns="http://s3.storagegrid.com/doc/2015-02-01/">enabled
</LastAccessTime>
```

PUT Bucket-Zeit für den letzten Zugriff

In der ANFORDERUNG PUT Bucket Last Access Time können Sie Updates der letzten Zugriffszeit für einzelne Buckets aktivieren oder deaktivieren. Durch das Deaktivieren von Updates der letzten Zugriffszeit wird die Performance verbessert. Dies ist die Standardeinstellung für alle Buckets, die mit Version 10.3 oder höher erstellt wurden.

Sie müssen über die s3:PutBucketLastAccessTime-Berechtigung für einen Bucket verfügen oder als Account-Root dienen, um diesen Vorgang abzuschließen.



Ab StorageGRID Version 10.3 sind Updates der letzten Zugriffszeit für alle neuen Buckets standardmäßig deaktiviert. Wenn Sie Buckets haben, die mit einer früheren Version von StorageGRID erstellt wurden und denen das neue Standardverhalten entsprechen möchten, müssen Sie für jeden dieser früheren Buckets explizit die Updates der letzten Zugriffszeit deaktivieren. Sie können Updates für die letzte Zugriffszeit mithilfe der Anforderung zum Zeitpunkt des letzten Zugriffs für Bucket oder über die Detailseite für einen Bucket im Tenant Manager aktivieren oder deaktivieren. Siehe "[Aktiviert bzw. deaktiviert Updates der letzten Zugriffszeit](#)".

Wenn Updates der letzten Zugriffszeit für einen Bucket deaktiviert wurden, wird das folgende Verhalten auf die Vorgänge auf dem Bucket angewendet:

- GetObject-, GetObjectAcl-, GetObjectTagging- und HeadObject-Anforderungen aktualisieren nicht die letzte Zugriffszeit. Das Objekt wird zur Bewertung des Information Lifecycle Management (ILM) nicht zu Warteschlangen hinzugefügt.
- CopyObject- und PutObjectTagging-Anfragen, die nur die Metadaten aktualisieren, aktualisieren ebenfalls die letzte Zugriffszeit. Das Objekt wird Warteschlangen für die ILM-Bewertung hinzugefügt.
- Wenn Updates zur letzten Zugriffszeit für den Quell-Bucket deaktiviert sind, aktualisieren CopyObject-Anforderungen nicht die letzte Zugriffszeit für den Quell-Bucket. Das kopierte Objekt wird nicht zu Warteschlangen für die ILM-Bewertung für den Quell-Bucket hinzugefügt. CopyObject-Anforderungen aktualisieren jedoch immer die letzte Zugriffszeit für das Ziel. Die Kopie des Objekts wird zu Warteschlangen für eine ILM-Bewertung hinzugefügt.
- CompleteMultipartUpload-Anforderungen werden zum Zeitpunkt des letzten Zugriffs aktualisiert. Das fertiggestellte Objekt wird zur ILM-Bewertung zu Warteschlangen hinzugefügt.

Beispiele anfordern

Dieses Beispiel ermöglicht die Zeit des letzten Zugriffs für einen Bucket.

```
PUT /bucket?x-ntap-sg-lastaccesstime=enabled HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

Dieses Beispiel deaktiviert die Zeit des letzten Zugriffs für einen Bucket.

```
PUT /bucket?x-ntap-sg-lastaccesstime=disabled HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

Konfiguration für die Benachrichtigung über Bucket-Metadaten LÖSCHEN

Mit der Konfigurationsanforderung FÜR DIE BENACHRICHTIGUNG „BUCKET-Metadaten LÖSCHEN“ können Sie den Suchintegrationsdienst für einzelne Buckets deaktivieren, indem Sie die Konfigurations-XML löschen.

Sie müssen über die berechtigung `s3:DeleteBucketMetadataNotification` für einen Bucket verfügen oder als Account-Root dienen, um diesen Vorgang abzuschließen.

Anforderungsbeispiel

Dieses Beispiel zeigt die Deaktivierung des Suchintegrationservice für einen Bucket.

```
DELETE /test1?x-ntap-sg-metadata-notification HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

Konfiguration der Bucket-Metadaten-Benachrichtigungen ABRUFEN

Die Konfigurationsanforderung FÜR GET Bucket-Metadaten-Benachrichtigungen ermöglicht es Ihnen, die Konfigurations-XML abzurufen, die zur Konfiguration der Suchintegration für einzelne Buckets verwendet wird.

Sie müssen über die berechtigung `s3:GetBucketMetadataNotification` verfügen oder als Kontowurzel dienen, um diesen Vorgang abzuschließen.

Anforderungsbeispiel

Diese Anforderung ruft die Konfiguration der Metadatenbenachrichtigung für den Bucket ab `bucket`.

```
GET /bucket?x-ntap-sg-metadata-notification HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

Antwort

Der Response Body umfasst die Konfiguration der Metadaten-Benachrichtigung für den Bucket. Anhand der Konfiguration der Metadatenbenachrichtigung können Sie festlegen, wie der Bucket für die Suchintegration konfiguriert ist. So können Unternehmen ermitteln, welche Objekte indiziert sind und an welche Endpunkte ihre Objektmetadaten gesendet werden.

```
<MetadataNotificationConfiguration>
  <Rule>
    <ID>Rule-1</ID>
    <Status>rule-status</Status>
    <Prefix>key-prefix</Prefix>
    <Destination>
      <Urn>arn:aws:es:_region:account-
ID_:domain/_mydomain/myindex/mytype_</Urn>
    </Destination>
  </Rule>
  <Rule>
    <ID>Rule-2</ID>
    ...
  </Rule>
  ...
</MetadataNotificationConfiguration>
```

Jede Konfiguration für die Metadatenbenachrichtigung enthält mindestens ein Regeln. Jede Regel gibt die Objekte an, die auf sie angewendet werden, und das Ziel, an dem StorageGRID Objekt-Metadaten senden soll. Ziele müssen mit dem URN eines StorageGRID-Endpunkts angegeben werden.

Name	Beschreibung	Erforderlich
MetadataNotificationKonfiguration	Container-Tag für Regeln zur Angabe von Objekten und Zielen für Metadatenbenachrichtigungen Enthält mindestens ein Regelement.	Ja.

Name	Beschreibung	Erforderlich
Regel	<p>Container-Tag für eine Regel, die die Objekte identifiziert, deren Metadaten zu einem bestimmten Index hinzugefügt werden sollen.</p> <p>Regeln mit überlappenden Präfixen werden abgelehnt.</p> <p>Im MetadataNotificationConfiguration Element enthalten.</p>	Ja.
ID	<p>Eindeutige Kennung für die Regel.</p> <p>In das Element Regel aufgenommen.</p>	Nein
Status	<p>Der Status kann „aktiviert“ oder „deaktiviert“ sein. Für deaktivierte Regeln wird keine Aktion durchgeführt.</p> <p>In das Element Regel aufgenommen.</p>	Ja.
Präfix	<p>Objekte, die mit dem Präfix übereinstimmen, werden von der Regel beeinflusst und ihre Metadaten werden an das angegebene Ziel gesendet.</p> <p>Geben Sie ein leeres Präfix an, um alle Objekte zu entsprechen.</p> <p>In das Element Regel aufgenommen.</p>	Ja.
Ziel	<p>Container-Tag für das Ziel einer Regel.</p> <p>In das Element Regel aufgenommen.</p>	Ja.

Name	Beschreibung	Erforderlich
Urne	<p>URNE des Ziels, an dem Objektmetadaten gesendet werden. Muss der URN eines StorageGRID-Endpunkts mit den folgenden Eigenschaften sein:</p> <ul style="list-style-type: none"> • es Muss das dritte Element sein. • Der URN muss mit dem Index und dem Typ enden, in dem die Metadaten gespeichert werden, im Formular <code>domain-name/myindex/mytype</code>. <p>Endpunkte werden mithilfe der Mandanten-Manager oder der Mandanten-Management-API konfiguriert. Sie nehmen folgende Form:</p> <ul style="list-style-type: none"> • <code>arn:aws:es:_region:account-ID_:domain/mydomain/myindex/mytype</code> • <code>urn:mysite:es:::mydomain/myindex/mytype</code> <p>Der Endpunkt muss konfiguriert werden, bevor die Konfigurations-XML gesendet wird, oder die Konfiguration schlägt mit einem Fehler 404 fehl.</p> <p>Urne ist im Element Ziel enthalten.</p>	Ja.

Antwortbeispiel

Die XML, die zwischen dem enthalten ist

```
<MetadataNotificationConfiguration></MetadataNotificationConfiguration>
```

tags zeigen, wie die Integration in einen Endpunkt zur Integration der Suchfunktion für den Bucket konfiguriert wird. In diesem Beispiel werden Objektmetadaten an einen Elasticsearch-Index mit dem Namen `current` gesendet. Und geben Sie den Namen ein `2017`. Das wird in einer AWS-Domäne mit dem Namen `records` gehostet.

```
HTTP/1.1 200 OK
Date: Thu, 20 Jul 2017 18:24:05 GMT
Connection: KEEP-ALIVE
Server: StorageGRID/11.0.0
x-amz-request-id: 3832973499
Content-Length: 264
Content-Type: application/xml
```

```
<MetadataNotificationConfiguration>
  <Rule>
    <ID>Rule-1</ID>
    <Status>Enabled</Status>
    <Prefix>2017</Prefix>
    <Destination>
      <Urn>arn:aws:es:us-east-
1:3333333:domain/records/current/2017</Urn>
    </Destination>
  </Rule>
</MetadataNotificationConfiguration>
```

Verwandte Informationen

["Verwenden Sie ein Mandantenkonto"](#)

PUT Bucket-Metadaten-Benachrichtigungskonfiguration

Die Konfigurationsanforderung FÜR PUT Bucket-Metadaten-Benachrichtigungen ermöglicht es Ihnen, den Such-Integrationservice für einzelne Buckets zu aktivieren. Die XML-Konfiguration für die Metadatenbenachrichtigung, die Sie im Anforderungsindex angeben, gibt die Objekte an, deren Metadaten an den Zielsuchindex gesendet werden.

Sie müssen über die Berechtigung `s3:PutBucketMetadataNotification` für einen Bucket verfügen oder als Account-Root dienen, um diesen Vorgang abzuschließen.

Anfrage

Die Anforderung muss die Konfiguration der Metadatenbenachrichtigung in der Anfragentext enthalten. Jede Konfiguration für die Metadatenbenachrichtigung enthält mindestens ein Regeln. Jede Regel gibt die Objekte an, auf die sie angewendet wird, und das Ziel, an dem StorageGRID Metadaten senden soll.

Objekte können nach dem Präfix des Objektnamens gefiltert werden. Beispielsweise können Sie Metadaten für Objekte mit dem Präfix `/images` an ein Ziel und Objekte mit dem Präfix `/videos` nach anderen.

Konfigurationen mit überlappenden Präfixen sind nicht gültig und werden beim Einreichen abgelehnt. Beispiel: Eine Konfiguration, die eine Regel für Objekte mit dem Präfix `test` und eine zweite Regel für Objekte mit dem Präfix `test2` nicht erlaubt.

Ziele müssen mit dem URN eines StorageGRID-Endpunkts angegeben werden. Der Endpunkt muss

vorhanden sein, wenn die Konfiguration der Metadatenbenachrichtigung gesendet wird oder die Anforderung als fehlschlägt 400 Bad Request. In der Fehlermeldung steht: Unable to save the metadata notification (search) policy. The specified endpoint URN does not exist: URN.

```

<MetadataNotificationConfiguration>
  <Rule>
    <ID>Rule-1</ID>
    <Status>rule-status</Status>
    <Prefix>key-prefix</Prefix>
    <Destination>
      <Urn>arn:aws:es:region:account-
ID:domain/mydomain/myindex/mytype</Urn>
    </Destination>
  </Rule>
  <Rule>
    <ID>Rule-2</ID>
    ...
  </Rule>
  ...
</MetadataNotificationConfiguration>

```

In der Tabelle werden die Elemente in der XML-Konfiguration für die Metadatenbenachrichtigung beschrieben.

Name	Beschreibung	Erforderlich
MetadataNotificationKonfiguration	Container-Tag für Regeln zur Angabe von Objekten und Zielen für Metadatenbenachrichtigungen Enthält mindestens ein Regelement.	Ja.
Regel	Container-Tag für eine Regel, die die Objekte identifiziert, deren Metadaten zu einem bestimmten Index hinzugefügt werden sollen. Regeln mit überlappenden Präfixen werden abgelehnt. Im MetadataNotificationConfiguration Element enthalten.	Ja.
ID	Eindeutige Kennung für die Regel. In das Element Regel aufgenommen.	Nein
Status	Der Status kann „aktiviert“ oder „deaktiviert“ sein. Für deaktivierte Regeln wird keine Aktion durchgeführt. In das Element Regel aufgenommen.	Ja.

Name	Beschreibung	Erforderlich
Präfix	<p>Objekte, die mit dem Präfix übereinstimmen, werden von der Regel beeinflusst und ihre Metadaten werden an das angegebene Ziel gesendet.</p> <p>Geben Sie ein leeres Präfix an, um alle Objekte zu entsprechen.</p> <p>In das Element Regel aufgenommen.</p>	Ja.
Ziel	<p>Container-Tag für das Ziel einer Regel.</p> <p>In das Element Regel aufgenommen.</p>	Ja.
Urne	<p>URNE des Ziels, an dem Objektmetadaten gesendet werden. Muss der URN eines StorageGRID-Endpunkts mit den folgenden Eigenschaften sein:</p> <ul style="list-style-type: none"> • es Muss das dritte Element sein. • Der URN muss mit dem Index und dem Typ enden, in dem die Metadaten gespeichert werden, im Formular <code>domain-name/myindex/mytype</code>. <p>Endpunkte werden mithilfe der Mandanten-Manager oder der Mandanten-Management-API konfiguriert. Sie nehmen folgende Form:</p> <ul style="list-style-type: none"> • <code>arn:aws:es:region:account-ID:domain/mydomain/myindex/mytype</code> • <code>urn:mysite:es:::mydomain/myindex/mytype</code> <p>Der Endpunkt muss konfiguriert werden, bevor die Konfigurations-XML gesendet wird, oder die Konfiguration schlägt mit einem Fehler 404 fehl.</p> <p>Urne ist im Element Ziel enthalten.</p>	Ja.

Beispiele anfordern

Dieses Beispiel zeigt die Aktivierung der Integration von Suchvorgängen für einen Bucket. In diesem Beispiel werden die Objektmetadaten für alle Objekte an dasselbe Ziel gesendet.

```
PUT /test1?x-ntap-sg-metadata-notification HTTP/1.1
Date: date
Authorization: authorization string
Host: host

<MetadataNotificationConfiguration>
  <Rule>
    <ID>Rule-1</ID>
    <Status>Enabled</Status>
    <Prefix></Prefix>
    <Destination>
      <Urn>urn:sgws:es:::sgws-notifications/test1/all</Urn>
    </Destination>
  </Rule>
</MetadataNotificationConfiguration>
```

In diesem Beispiel sind die Objektmetadaten für Objekte mit dem Präfix übereinstimmen `/images` An ein Ziel gesendet wird, während die Objektmetadaten für Objekte mit dem Präfix übereinstimmen `/videos` Wird an ein zweites Ziel gesendet.

```

PUT /graphics?x-ntap-sg-metadata-notification HTTP/1.1
Date: date
Authorization: authorization string
Host: host

<MetadataNotificationConfiguration>
  <Rule>
    <ID>Images-rule</ID>
    <Status>Enabled</Status>
    <Prefix>/images</Prefix>
    <Destination>
      <Urn>arn:aws:es:us-east-1:33333333:domain/es-
domain/graphics/imagetype</Urn>
    </Destination>
  </Rule>
  <Rule>
    <ID>Videos-rule</ID>
    <Status>Enabled</Status>
    <Prefix>/videos</Prefix>
    <Destination>
      <Urn>arn:aws:es:us-west-1:22222222:domain/es-
domain/graphics/videotype</Urn>
    </Destination>
  </Rule>
</MetadataNotificationConfiguration>

```

Vom Suchintegrations-Service generierter JSON

Wenn Sie den Such-Integrationservice für einen Bucket aktivieren, wird ein JSON-Dokument generiert und an den Zielpunkt gesendet, wenn Metadaten oder Tags hinzugefügt, aktualisiert oder gelöscht werden.

Dieses Beispiel zeigt ein Beispiel für den JSON, der generiert werden kann, wenn ein Objekt mit dem Schlüssel enthält `SGWS/Tagging.txt` Wird in einem Bucket mit dem Namen erstellt `test`. Der `test` Der Bucket ist nicht versioniert, daher der `versionId` Das Tag ist leer.

```

{
  "bucket": "test",
  "key": "SGWS/Tagging.txt",
  "versionId": "",
  "accountId": "86928401983529626822",
  "size": 38,
  "md5": "3d6c7634a85436eee06d43415012855",
  "region": "us-east-1",
  "metadata": {
    "age": "25"
  },
  "tags": {
    "color": "yellow"
  }
}

```

Objektmetadaten sind in Metadaten-Benachrichtigungen enthalten

In der Tabelle sind alle Felder aufgeführt, die im JSON-Dokument enthalten sind, die beim Aktivierung der Suchintegration an den Zielendpunkt gesendet werden.

Der Dokumentname umfasst, falls vorhanden, den Bucket-Namen, den Objektnamen und die Version-ID.

Typ	Elementname	Beschreibung
Bucket- und Objektinformationen	Eimer	Name des Buckets
Bucket- und Objektinformationen	Taste	Name des Objektschlüssels
Bucket- und Objektinformationen	VersionID	Objektversion für Objekte in versionierten Buckets
Bucket- und Objektinformationen	Werden	Beispielsweise Bucket-Region <code>us-east-1</code>
System-Metadaten	Größe	Objektgröße (in Byte) wie für einen HTTP-Client sichtbar
System-Metadaten	md5	Objekt-Hash
Benutzer-Metadaten	Metadaten <i>key:value</i>	Alle Benutzer-Metadaten des Objekts als Schlüssel-Wert-Paare
Tags	tags <i>key:value</i>	Alle für das Objekt definierten Objekt-Tags als Schlüsselwert-Paare



Für Tags und Benutzer-Metadaten gibt StorageGRID Daten und Nummern an Elasticsearch als Strings oder als S3-Ereignisbenachrichtigungen weiter. Um Elasticsearch so zu konfigurieren, dass diese Strings als Daten oder Zahlen interpretiert werden, befolgen Sie die Elasticsearch-Anweisungen für die dynamische Feldzuordnung und die Zuordnung von Datumsformaten. Sie müssen die dynamischen Feldzuordnungen im Index aktivieren, bevor Sie den Suchintegrationsdienst konfigurieren. Nachdem ein Dokument indiziert wurde, können Sie die Feldtypen des Dokuments im Index nicht mehr bearbeiten.

Verwandte Informationen

["Verwenden Sie ein Mandantenkonto"](#)

Storage-Nutzungsanforderung ABRUFEN

Der Antrag ZUR GET Storage-Nutzung gibt Ihnen die Gesamtzahl des verwendeten Storage durch ein Konto und für jeden mit dem Account verknüpften Bucket an.

Die Menge des von einem Konto und seinen Buckets verwendeten Speichers kann über eine modifizierte ListBuckets-Anforderung mit dem abgerufen werden `x-ntap-sg-usage` Abfrageparameter. Die Nutzung des Bucket-Storage wird getrennt von DEN PUT- und LÖSCHANFRAGEN, die vom System verarbeitet werden, nachverfolgt. Es kann zu einer gewissen Verzögerung kommen, bevor die Nutzungswerte auf der Grundlage der Verarbeitung von Anfragen den erwarteten Werten entsprechen, insbesondere wenn das System unter hoher Belastung steht.

StorageGRID versucht standardmäßig, Nutzungsdaten mithilfe einer starken globalen Konsistenz abzurufen. Wenn eine starke globale Konsistenz nicht erreicht werden kann, versucht StorageGRID, die Verwendungsinformationen in einer starken Site-Konsistenz abzurufen.

Sie müssen über die `s3:ListAllMyBuckets`-Berechtigung verfügen oder als Kontostamm vorliegen, um diese Operation abzuschließen.

Anforderungsbeispiel

```
GET /?x-ntap-sg-usage HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

Antwortbeispiel

Dieses Beispiel zeigt ein Konto, das vier Objekte und 12 Bytes Daten in zwei Buckets enthält. Jeder Bucket enthält zwei Objekte und sechs Bytes Daten.

```
HTTP/1.1 200 OK
Date: Sat, 29 Nov 2015 00:49:05 GMT
Connection: KEEP-ALIVE
Server: StorageGRID/10.2.0
x-amz-request-id: 727237123
Content-Length: 427
Content-Type: application/xml

<?xml version="1.0" encoding="UTF-8"?>
<UsageResult xmlns="http://s3.storagegrid.com/doc/2015-02-01">
<CalculationTime>2014-11-19T05:30:11.000000Z</CalculationTime>
<ObjectCount>4</ObjectCount>
<DataBytes>12</DataBytes>
<Buckets>
<Bucket>
<Name>bucket1</Name>
<ObjectCount>2</ObjectCount>
<DataBytes>6</DataBytes>
</Bucket>
<Bucket>
<Name>bucket2</Name>
<ObjectCount>2</ObjectCount>
<DataBytes>6</DataBytes>
</Bucket>
</Buckets>
</UsageResult>
```

Versionierung

Jede gespeicherte Objektversion trägt zum bei `ObjectCount` Und `DataBytes` Werte in der Antwort. Löschmarkierungen werden dem nicht hinzugefügt `ObjectCount` Gesamt:

Verwandte Informationen

["Konsistenzwerte"](#)

Veraltete Bucket-Anforderungen für ältere Compliance

Veraltete Bucket-Anforderungen für ältere Compliance

Möglicherweise müssen Sie die StorageGRID S3 REST-API zum Management von Buckets verwenden, die mit der älteren Compliance-Funktion erstellt wurden.

Compliance-Funktion veraltet

Die in früheren StorageGRID-Versionen verfügbare Funktion für die StorageGRID-Konformität ist veraltet und wurde durch S3-Objektsperre ersetzt.

Wenn Sie zuvor die Einstellung für globale Konformität aktiviert haben, ist die globale S3-Objektsperre in StorageGRID 11.6 aktiviert. Neue Buckets können nicht mehr mit aktivierter Compliance erstellt werden. Trotzdem können Sie bei Bedarf die StorageGRID S3 REST-API verwenden, um alle vorhandenen, älteren, konformen Buckets zu managen.

- ["Konfigurieren Sie die S3-Objektsperre über die S3-REST-API"](#)
- ["Objektmanagement mit ILM"](#)
- ["NetApp Knowledge Base: Management älterer, konformer Buckets für StorageGRID 11.5"](#)

Veraltete Compliance-Anforderungen:

- ["Veraltet – PUT Bucket-Anforderung-Änderungen aus Compliance-Gründen"](#)

Das SGCompliance XML-Element ist veraltet. Zuvor könnten Sie dieses benutzerdefinierte StorageGRID-Element in das optionale XML-Anforderungsgremium VON PUT Bucket-Anforderungen integrieren, um einen konformen Bucket zu erstellen.

- ["Veraltet – BUCKET-Compliance ABRUFEN"](#)

Die ANFORDERUNG „GET Bucket-Compliance“ ist veraltet. Sie können diese Anforderung jedoch weiterhin verwenden, um die derzeit für einen vorhandenen, älteren, konformen Bucket geltenden Compliance-Einstellungen zu bestimmen.

- ["Veraltet – EINHALTUNG VON PUT Bucket"](#)

Die PUT Bucket-Compliance-Anforderung ist veraltet. Sie können diese Anforderung jedoch weiterhin verwenden, um die Compliance-Einstellungen für einen vorhandenen Bucket zu ändern, der die Compliance-Anforderungen erfüllt. Sie können beispielsweise einen vorhandenen Bucket auf „Legal Hold“ platzieren oder den Aufbewahrungszeitraum erhöhen.

Veraltet: CreateBucket fordert Änderungen für Compliance an

Das SGCompliance XML-Element ist veraltet. Zuvor könnten Sie dieses benutzerdefinierte StorageGRID-Element in den optionalen XML-Anforderungskörper von CreateBucket-Anforderungen aufnehmen, um einen konformen Bucket zu erstellen.



Die in früheren StorageGRID-Versionen verfügbare Funktion für die StorageGRID-Konformität ist veraltet und wurde durch S3-Objektsperre ersetzt. Im Folgenden finden Sie weitere Informationen:

- ["Konfigurieren Sie die S3-Objektsperre über die S3-REST-API"](#)
- ["NetApp Knowledge Base: Management älterer, konformer Buckets für StorageGRID 11.5"](#)

Mit aktivierter Compliance können keine neuen Buckets mehr erstellt werden. Die folgende Fehlermeldung wird zurückgegeben, wenn Sie versuchen, die Änderungen der CreateBucket-Anforderung für die Compliance zu verwenden, um einen neuen konformen Bucket zu erstellen:

```
The Compliance feature is deprecated.  
Contact your StorageGRID administrator if you need to create new Compliant  
buckets.
```

Veraltet: Anforderung FÜR Bucket-Compliance ABRUFEN

Die ANFORDERUNG „GET Bucket-Compliance“ ist veraltet. Sie können diese Anforderung jedoch weiterhin verwenden, um die derzeit für einen vorhandenen, älteren, konformen Bucket geltenden Compliance-Einstellungen zu bestimmen.



Die in früheren StorageGRID-Versionen verfügbare Funktion für die StorageGRID-Konformität ist veraltet und wurde durch S3-Objektsperre ersetzt. Im Folgenden finden Sie weitere Informationen:

- ["Konfigurieren Sie die S3-Objektsperre über die S3-REST-API"](#)
- ["NetApp Knowledge Base: Management älterer, konformer Buckets für StorageGRID 11.5"](#)

Um diesen Vorgang abzuschließen, müssen Sie über die Berechtigung `s3:GetBucketCompliance` verfügen oder als Stammverzeichnis für das Konto verfügen.

Anforderungsbeispiel

In dieser Beispielanforderung können Sie die Compliance-Einstellungen für den Bucket mit dem Namen `mybucket` festlegen.

```
GET /mybucket/?x-ntap-sg-compliance HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

Antwortbeispiel

In der XML-Antwortantwort `<SGCompliance>` führt die für den Bucket verwendeten Compliance-Einstellungen auf. Dieses Beispiel zeigt die Compliance-Einstellungen für einen Bucket, in dem jedes Objekt ein Jahr lang (525,600 Minuten) aufbewahrt wird, beginnend mit der Aufnahme des Objekts in das Grid. Derzeit ist keine gesetzliche Aufbewahrungspflicht auf diesem Bucket vorhanden. Jedes Objekt wird nach einem Jahr automatisch gelöscht.

```
HTTP/1.1 200 OK
Date: date
Connection: connection
Server: StorageGRID/11.1.0
x-amz-request-id: request ID
Content-Length: length
Content-Type: application/xml

<SGCompliance>
  <RetentionPeriodMinutes>525600</RetentionPeriodMinutes>
  <LegalHold>>false</LegalHold>
  <AutoDelete>>true</AutoDelete>
</SGCompliance>
```

Name	Beschreibung
WiederholungPeriodMinuten	Die Länge des Aufbewahrungszeitraums für Objekte, die diesem Bucket hinzugefügt wurden, in Minuten Der Aufbewahrungszeitraum beginnt, wenn das Objekt in das Raster aufgenommen wird.
LegalAlte	<ul style="list-style-type: none"> • Wahr: Dieser Bucket befindet sich derzeit in einer gesetzlichen Aufbewahrungspflichten. Objekte in diesem Bucket können erst gelöscht werden, wenn der Legal Hold aufgehoben wurde, auch wenn ihre Aufbewahrungsfrist abgelaufen ist. • Falsch: Dieser Eimer steht derzeit nicht unter einer gesetzlichen Aufbewahrungspflichten. Objekte in diesem Bucket können nach Ablauf ihres Aufbewahrungszeitraums gelöscht werden.
Automatisches Löschen	<ul style="list-style-type: none"> • Wahr: Die Objekte in diesem Bucket werden automatisch gelöscht, sobald ihre Aufbewahrungsfrist abgelaufen ist, es sei denn, der Bucket unterliegt einer gesetzlichen Aufbewahrungspflichten. • False: Die Objekte in diesem Bucket werden nicht automatisch gelöscht, wenn die Aufbewahrungsfrist abgelaufen ist. Sie müssen diese Objekte manuell löschen, wenn Sie sie löschen müssen.

Fehlerantworten

Wenn der Bucket nicht für konform erstellt wurde, lautet der HTTP-Statuscode für die Antwort 404 Not Found, Mit einem S3-Fehlercode von XNoSuchBucketCompliance.

Veraltet: PUT Bucket-Compliance-Anforderung

Die PUT Bucket-Compliance-Anforderung ist veraltet. Sie können diese Anforderung jedoch weiterhin verwenden, um die Compliance-Einstellungen für einen vorhandenen Bucket zu ändern, der die Compliance-Anforderungen erfüllt. Sie können beispielsweise einen vorhandenen Bucket auf „Legal Hold“ platzieren oder den Aufbewahrungszeitraum erhöhen.



Die in früheren StorageGRID-Versionen verfügbare Funktion für die StorageGRID-Konformität ist veraltet und wurde durch S3-Objektsperre ersetzt. Im Folgenden finden Sie weitere Informationen:

- ["Konfigurieren Sie die S3-Objektsperre über die S3-REST-API"](#)
- ["NetApp Knowledge Base: Management älterer, konformer Buckets für StorageGRID 11.5"](#)

Sie müssen über die s3:PutBucketCompliance-Berechtigung verfügen oder als Kontoroot vorliegen, um diesen Vorgang abzuschließen.

Wenn Sie eine PUT Bucket-Compliance-Anforderung ausgeben, müssen Sie für jedes Feld der Compliance-Einstellungen einen Wert angeben.

Anforderungsbeispiel

In dieser Beispielanforderung werden die Compliance-Einstellungen für den Bucket mit dem Namen geändert `mybucket`. In diesem Beispiel befinden sich die Objekte in `mybucket` Wird nun für zwei Jahre (1,051,200 Minuten) statt für ein Jahr beibehalten, beginnend mit dem Zeitpunkt, an dem das Objekt in das Grid aufgenommen wird. Es gibt keine gesetzliche Aufbewahrungspflichten auf diesem Bucket. Jedes Objekt wird nach zwei Jahren automatisch gelöscht.

```
PUT /mybucket/?x-ntap-sg-compliance HTTP/1.1
Date: date
Authorization: authorization name
Host: host
Content-Length: 152

<SGCompliance>
  <RetentionPeriodMinutes>1051200</RetentionPeriodMinutes>
  <LegalHold>>false</LegalHold>
  <AutoDelete>>true</AutoDelete>
</SGCompliance>
```

Name	Beschreibung
WiederholungPeriodMinuten	<p>Die Länge des Aufbewahrungszeitraums für Objekte, die diesem Bucket hinzugefügt wurden, in Minuten Der Aufbewahrungszeitraum beginnt, wenn das Objekt in das Raster aufgenommen wird.</p> <p>Wichtig Wenn Sie einen neuen Wert für <code>RetentionPeriodMinutes</code> angeben, müssen Sie einen Wert angeben, der der aktuellen Aufbewahrungsfrist des Buckets entspricht oder größer ist. Nachdem die Aufbewahrungsfrist des Buckets festgelegt wurde, können Sie diesen Wert nicht verringern, sondern nur erhöhen.</p>
LegalAlte	<ul style="list-style-type: none">• Wahr: Dieser Bucket befindet sich derzeit in einer gesetzlichen Aufbewahrungspflichten. Objekte in diesem Bucket können erst gelöscht werden, wenn der Legal Hold aufgehoben wurde, auch wenn ihre Aufbewahrungsfrist abgelaufen ist.• Falsch: Dieser Eimer steht derzeit nicht unter einer gesetzlichen Aufbewahrungspflichten. Objekte in diesem Bucket können nach Ablauf ihres Aufbewahrungszeitraums gelöscht werden.
Automatisches Löschen	<ul style="list-style-type: none">• Wahr: Die Objekte in diesem Bucket werden automatisch gelöscht, sobald ihre Aufbewahrungsfrist abgelaufen ist, es sei denn, der Bucket unterliegt einer gesetzlichen Aufbewahrungspflichten.• False: Die Objekte in diesem Bucket werden nicht automatisch gelöscht, wenn die Aufbewahrungsfrist abgelaufen ist. Sie müssen diese Objekte manuell löschen, wenn Sie sie löschen müssen.

Konsistenz für Compliance-Einstellungen

Wenn Sie die Compliance-Einstellungen für einen S3-Bucket mit EINER PUT-Bucket-Compliance-Anforderung aktualisieren, versucht StorageGRID, die Metadaten des Buckets im Grid zu aktualisieren. Standardmäßig verwendet StorageGRID die **strong-global**-Konsistenz, um sicherzustellen, dass alle Datacenter-Standorte und alle Speicher-Nodes, die Bucket-Metadaten enthalten, für die geänderten Compliance-Einstellungen eine Lese-nach-Schreiben-Konsistenz aufweisen.

Wenn StorageGRID die **strong-global**-Konsistenz nicht erreichen kann, weil ein Rechenzentrum oder mehrere Speicherknoten an einem Standort nicht verfügbar sind, lautet der HTTP-Statuscode für die Antwort `503 Service Unavailable`.

Wenn Sie diese Antwort erhalten, müssen Sie sich an den Grid-Administrator wenden, um sicherzustellen, dass die erforderlichen Storage-Services so schnell wie möglich verfügbar gemacht werden. Wenn der Grid-Administrator nicht in der Lage ist, genügend Speicher-Nodes an jedem Standort zur Verfügung zu stellen, kann der technische Support Sie auffordern, die fehlgeschlagene Anforderung erneut zu versuchen, indem Sie die Konsistenz von **strong-site** erzwingen.



Erzwingen Sie niemals die * strong-site* Konsistenz für PUT Bucket Compliance, es sei denn, Sie wurden von der technischen Unterstützung dazu angewiesen, und es sei denn, Sie verstehen die möglichen Konsequenzen, die sich aus der Verwendung dieses Levels ergeben.

Wenn die Konsistenz auf **strong-site** reduziert wird, garantiert StorageGRID, dass aktualisierte Compliance-Einstellungen nur für Client-Anforderungen innerhalb eines Standorts Lese-nach-Schreiben-Konsistenz aufweisen. Das bedeutet, dass das StorageGRID System vorübergehend mehrere inkonsistente Einstellungen für diesen Bucket bietet, bis alle Standorte und Storage-Nodes verfügbar sind. Die inkonsistenten Einstellungen können zu unerwarteten und unerwünschten Verhaltensweisen führen. Wenn Sie beispielsweise einen Bucket unter einen Legal Hold setzen und eine niedrigere Konsistenz erzwingen, könnten die vorherigen Compliance-Einstellungen des Buckets (d. h. Legal Hold off) an einigen Rechenzentrumsstandorten weiterhin wirksam sein. Aus diesem Grund können Objekte, die Ihrer Meinung nach in einer gesetzlichen Wartefrist liegen, nach Ablauf ihres Aufbewahrungszeitraums entweder durch den Benutzer oder durch AutoDelete gelöscht werden, sofern diese Option aktiviert ist.

Um die Verwendung der * strong-site*-Konsistenz zu erzwingen, geben Sie die Anforderung zur Einhaltung der PUT Bucket-Compliance erneut aus und fügen Sie die ein `Consistency-Control` HTTP-Request-Header, wie folgt:

```
PUT /mybucket/?x-ntap-sg-compliance HTTP/1.1
Consistency-Control: strong-site
```

Fehlerantworten

- Wenn der Bucket nicht für konform erstellt wurde, lautet der HTTP-Statuscode für die Antwort `404 Not Found`.
- Wenn `RetentionPeriodMinutes` in der Anforderung ist kleiner als der aktuelle Aufbewahrungszeitraum des Buckets, lautet der HTTP-Statuscode `400 Bad Request`.

Verwandte Informationen

["Veraltet: PUT Bucket-Request-Änderungen aus Compliance-Gründen"](#)

Bucket- und Gruppenzugriffsrichtlinien

Verwendung von Bucket- und Gruppenzugriffsrichtlinien

StorageGRID verwendet die Richtlinienensprache für Amazon Web Services (AWS), um S3-Mandanten die Kontrolle des Zugriffs auf Buckets und Objekte innerhalb dieser Buckets zu ermöglichen. Das StorageGRID System implementiert eine Untermenge der S3-REST-API-Richtliniensprache. Zugriffsrichtlinien für die S3 API werden in JSON geschrieben.

Zugriffsrichtlinien – Überblick

Von StorageGRID werden zwei Arten von Zugriffsrichtlinien unterstützt:

- **Bucket-Richtlinien**, die mit den Operationen GetBucket Policy, PutBucket Policy und DeleteBucket Policy S3 verwaltet werden. Bucket-Richtlinien sind mit Buckets verknüpft, so dass sie so konfiguriert sind, dass sie den Zugriff durch Benutzer im Bucket-Eigentümerkonto oder andere Konten an den Bucket und die darin befindlichen Objekte steuern. Eine Bucket-Richtlinie gilt nur für einen Bucket und möglicherweise auch für mehrere Gruppen.
- **Gruppenrichtlinien**, die mit dem Tenant Manager oder der Mandantenmanagement-API konfiguriert sind. Gruppenrichtlinien sind einer Gruppe im Konto zugeordnet, sodass sie so konfiguriert sind, dass sie der Gruppe ermöglichen, auf bestimmte Ressourcen zuzugreifen, die dem Konto gehören. Eine Gruppenrichtlinie gilt nur für eine Gruppe und möglicherweise für mehrere Buckets.



Es gibt keine Unterschiede in der Priorität zwischen Gruppen- und Bucket-Richtlinien.

StorageGRID Bucket und Gruppenrichtlinien folgen einer bestimmten Grammatik, die von Amazon definiert wurde. Innerhalb jeder Richtlinie gibt es eine Reihe von Richtlinienerklärungen, und jede Aussage enthält die folgenden Elemente:

- Statement-ID (Sid) (optional)
- Wirkung
- Principal/NotPrincipal
- Ressource/Ressource
- Aktion/Notaktion
- Bedingung (optional)

Richtlinienaussagen werden mithilfe dieser Struktur erstellt, um Berechtigungen anzugeben: <Effekt> gewähren, um <Principal> <Aktion> auf <Ressource> durchzuführen, wenn <Bedingung> angewendet wird.

Jedes Richtlinienelement wird für eine bestimmte Funktion verwendet:

Element	Beschreibung
Sid	Das Sid-Element ist optional. Der Sid ist nur als Beschreibung für den Benutzer gedacht. Diese wird vom StorageGRID System gespeichert, aber nicht interpretiert.

Element	Beschreibung
Wirkung	Verwenden Sie das Effektelement, um festzustellen, ob die angegebenen Vorgänge zulässig oder verweigert werden. Sie müssen anhand der Schlüsselwörter für unterstütztes Aktionselement Operationen identifizieren, die für Buckets oder Objekte zugelassen (oder verweigert) werden.
Principal/NotPrincipal	Benutzer, Gruppen und Konten können auf bestimmte Ressourcen zugreifen und bestimmte Aktionen ausführen. Wenn in der Anfrage keine S3-Signatur enthalten ist, ist ein anonymer Zugriff durch Angabe des Platzhalterzeichens (*) als Principal zulässig. Standardmäßig hat nur das Konto-Root Zugriff auf Ressourcen, die dem Konto gehören. Sie müssen nur das Hauptelement in einer Bucket-Richtlinie angeben. Bei Gruppenrichtlinien ist die Gruppe, der die Richtlinie zugeordnet ist, das implizite Prinzipalelement.
Ressource/Ressource	Das Ressourcenelement identifiziert Buckets und Objekte. Sie können Buckets und Objekten über den ARN (Amazon Resource Name) Berechtigungen gewähren oder verweigern, um die Ressource zu identifizieren.
Aktion/Notaktion	Die Elemente Aktion und Wirkung sind die beiden Komponenten von Berechtigungen. Wenn eine Gruppe eine Ressource anfordert, wird ihnen entweder der Zugriff auf die Ressource gewährt oder verweigert. Der Zugriff wird verweigert, es sei denn, Sie weisen ausdrücklich Berechtigungen zu, aber Sie können explizites Ablehnen verwenden, um eine von einer anderen Richtlinie gewährte Berechtigung zu überschreiben.
Zustand	Das Bedingungelement ist optional. Unter Bedingungen können Sie Ausdrücke erstellen, um zu bestimmen, wann eine Richtlinie angewendet werden soll.

Im Element Aktion können Sie das Platzhalterzeichen (*) verwenden, um alle Vorgänge oder eine Untermenge von Vorgängen anzugeben. Diese Aktion entspricht beispielsweise Berechtigungen wie s3:GetObject, s3:PutObject und s3>DeleteObject.

```
s3:*Object
```

Im Element Ressource können Sie die Platzhalterzeichen (*) und (?) verwenden. Während das Sternchen (*) mit 0 oder mehr Zeichen übereinstimmt, ist das Fragezeichen (?) Entspricht einem beliebigen Zeichen.

Im Hauptelement werden Platzhalterzeichen nicht unterstützt, außer zum Festlegen eines anonymen Zugriffs, der allen Personen die Berechtigung gewährt. Sie legen beispielsweise den Platzhalter (*) als Principal-Wert fest.

```
"Principal": "*"
```

```
"Principal": {"AWS": "*"}
```

Im folgenden Beispiel verwendet die Anweisung die Elemente „Effekt“, „Principal“, „Aktion“ und „Ressource“. Dieses Beispiel zeigt eine vollständige Bucket-Richtlinienanweisung, die den Principals, die Admin-Gruppe, mit dem Effekt „Zulassen“ erhält `federated-group/admin` Und der Finanzgruppe `federated-group/finance`, Berechtigungen zur Durchführung der Aktion `s3:ListBucket` Auf dem genannten Bucket `mybucket` Und der Aktion `s3:GetObject` Auf allen Objekten in diesem Bucket.

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": [
          "arn:aws:iam::27233906934684427525:federated-group/admin",
          "arn:aws:iam::27233906934684427525:federated-group/finance"
        ]
      },
      "Action": [
        "s3:ListBucket",
        "s3:GetObject"
      ],
      "Resource": [
        "arn:aws:iam:s3:::mybucket",
        "arn:aws:iam:s3:::mybucket/*"
      ]
    }
  ]
}
```

Die Bucket-Richtlinie hat eine Größenbeschränkung von 20,480 Byte, und die Gruppenrichtlinie hat ein Größenlimit von 5,120 Byte.

Konsistenz von Richtlinien

Standardmäßig sind alle Aktualisierungen, die Sie an Gruppenrichtlinien vornehmen, letztendlich konsistent. Wenn eine Gruppenrichtlinie konsistent wird, können die Änderungen aufgrund des Caching von Richtlinien weitere 15 Minuten in Anspruch nehmen. Standardmäßig sind alle Updates an Bucket-Richtlinien stark konsistent.

Sie können bei Bedarf die Konsistenzgarantien für Bucket-Richtlinienaktualisierungen ändern. Beispielsweise kann es vorkommen, dass eine Änderung an einer Bucket-Richtlinie bei einem Standortausfall verfügbar ist.

In diesem Fall können Sie entweder die einstellen `Consistency-Control` Header in der Anforderung „PutBucket Policy“, oder Sie können die Anforderung „PUT Bucket Consistency Request“ verwenden. Wenn eine Bucket-Richtlinie konsistent wird, können die Änderungen durch das Caching von Richtlinien zusätzliche 8 Sekunden in Anspruch nehmen.



Wenn Sie die Konsistenz auf einen anderen Wert setzen, um eine temporäre Situation zu umgehen, stellen Sie sicher, dass die Einstellung auf Bucket-Ebene wieder auf ihren ursprünglichen Wert zurückgesetzt wird, wenn Sie fertig sind. Andernfalls wird für alle zukünftigen Bucket-Anforderungen die geänderte Einstellung verwendet.

Verwenden Sie ARN in den Richtlinienenerklärungen

In den Richtlinienenerklärungen wird das ARN in Haupt- und Ressourcenelementen verwendet.

- Verwenden Sie diese Syntax, um die S3-Ressource ARN anzugeben:

```
arn:aws:s3:::bucket-name
arn:aws:s3:::bucket-name/object_key
```

- Verwenden Sie diese Syntax, um die Identitätsressource ARN (Benutzer und Gruppen) festzulegen:

```
arn:aws:iam::account_id:root
arn:aws:iam::account_id:user/user_name
arn:aws:iam::account_id:group/group_name
arn:aws:iam::account_id:federated-user/user_name
arn:aws:iam::account_id:federated-group/group_name
```

Weitere Überlegungen:

- Sie können das Sternchen (*) als Platzhalter verwenden, um Null oder mehr Zeichen im Objektschlüssel zu entsprechen.
- Internationale Zeichen, die im Objektschlüssel angegeben werden können, sollten mit JSON UTF-8 oder mit JSON \U Escape Sequenzen codiert werden. Die prozentuale Kodierung wird nicht unterstützt.

["RFC 2141 URN Syntax"](#)

Der HTTP-Anforderungskörper für den PutBucketPolicy-Vorgang muss mit `charset=UTF-8` codiert werden.

Geben Sie Ressourcen in einer Richtlinie an

In Richtlinienausrechnungen können Sie mithilfe des Elements Ressourcen den Bucket oder das Objekt angeben, für das Berechtigungen zulässig oder verweigert werden.

- Jede Richtlinienanweisung erfordert ein Ressourcenelement. In einer Richtlinie werden Ressourcen durch das Element gekennzeichnet `Resource`, Oder alternativ `NotResource` Für Ausschluss.
- Sie legen Ressourcen mit einer S3-Ressource ARN fest. Beispiel:

```
"Resource": "arn:aws:s3:::mybucket/*"
```

- Sie können Richtlinienvariablen auch innerhalb des Objektschlüssels verwenden. Beispiel:

```
"Resource": "arn:aws:s3:::mybucket/home/${aws:username}/*"
```

- Der Ressourcenwert kann einen Bucket angeben, der beim Erstellen einer Gruppenrichtlinie noch nicht vorhanden ist.

Principals in einer Policy angeben

Verwenden Sie das Hauptelement, um das Benutzer-, Gruppen- oder Mandantenkonto zu identifizieren, das über die Richtlinianweisung Zugriff auf die Ressource erlaubt/verweigert wird.

- Jede Richtlinianweisung in einer Bucket-Richtlinie muss ein Principal Element enthalten. Richtlinianweisungen in einer Gruppenrichtlinie benötigen das Hauptelement nicht, da die Gruppe als Hauptelement verstanden wird.
- In einer Richtlinie werden Prinzipale durch das Element „Principal“ oder alternativ „NotPrincipal“ für den Ausschluss gekennzeichnet.
- Kontobasierte Identitäten müssen mit einer ID oder einem ARN angegeben werden:

```
"Principal": { "AWS": "account_id" }  
"Principal": { "AWS": "identity_arn" }
```

- In diesem Beispiel wird die Mandanten-Account-ID 27233906934684427525 verwendet, die das Konto-Root und alle Benutzer im Konto enthält:

```
"Principal": { "AWS": "27233906934684427525" }
```

- Sie können nur das Konto-Root angeben:

```
"Principal": { "AWS": "arn:aws:iam::27233906934684427525:root" }
```

- Sie können einen bestimmten föderierten Benutzer („Alex“) angeben:

```
"Principal": { "AWS": "arn:aws:iam::27233906934684427525:federated-  
user/Alex" }
```

- Sie können eine bestimmte föderierte Gruppe („Manager“) angeben:

```
"Principal": { "AWS": "arn:aws:iam::27233906934684427525:federated-  
group/Managers" }
```

- Sie können einen anonymen Principal angeben:

```
"Principal": "*" 
```

- Um Mehrdeutigkeiten zu vermeiden, können Sie die Benutzer-UUID anstelle des Benutzernamens verwenden:

```
arn:aws:iam::27233906934684427525:user-uuid/de305d54-75b4-431b-adb2-  
eb6b9e546013
```

Angenommen, Alex verlässt zum Beispiel die Organisation und den Benutzernamen `Alex` Wird gelöscht. Wenn ein neuer Alex der Organisation beitrifft und dem gleichen zugewiesen wird `Alex` Benutzernamen: Der neue Benutzer erbt möglicherweise unbeabsichtigt die dem ursprünglichen Benutzer gewährten Berechtigungen.

- Der Hauptwert kann einen Gruppen-/Benutzernamen angeben, der beim Erstellen einer Bucket-Richtlinie noch nicht vorhanden ist.

Legen Sie Berechtigungen in einer Richtlinie fest

In einer Richtlinie wird das Aktionselement verwendet, um Berechtigungen einer Ressource zuzulassen/zu verweigern. Es gibt eine Reihe von Berechtigungen, die Sie in einer Richtlinie festlegen können, die durch das Element „Aktion“ gekennzeichnet sind, oder alternativ durch „NotAction“ für den Ausschluss. Jedes dieser Elemente wird bestimmten S3-REST-API-Operationen zugeordnet.

In den Tabellen werden die Berechtigungen aufgeführt, die auf Buckets angewendet werden, sowie die Berechtigungen, die für Objekte gelten.



Amazon S3 verwendet jetzt die `s3:PutReplicationConfiguration`-Berechtigung sowohl für die `PutBucketReplication`- als auch für die `DeleteBucketReplication`-Aktionen. `StorageGRID` verwendet für jede Aktion separate Berechtigungen, die mit der ursprünglichen Amazon S3 Spezifikation übereinstimmt.



Ein Löschen wird durchgeführt, wenn ein `Put` zum Überschreiben eines vorhandenen Werts verwendet wird.

Berechtigungen, die für Buckets gelten

Berechtigungen	S3-REST-API-OPERATIONEN	Individuell für StorageGRID
s3:CreateBucket	CreateBucket	Ja. Hinweis: Nur in Gruppenrichtlinien verwenden.
s3>DeleteBucket	DeleteBucket	
s3>DeleteBucketMetadataBenachrichtigung	Konfiguration für die Benachrichtigung über Bucket-Metadaten LÖSCHEN	Ja.
s3>DeleteBucketPolicy	DeleteBucketRichtlinien	
s3>DeleteReplicationConfiguration	DeleteBucketReplication	Ja, separate Berechtigungen für PUT und DELETE
s3:GetBucketAcl	GetBucketAcl	
s3:GetBucketCompliance	GET Bucket-Compliance (veraltet)	Ja.
s3:GetBucketConsistency	Get Bucket-Konsistenz	Ja.
s3:GetBucketCORS	GetBucketCors	
s3:GetVerschlüsselungKonfiguration	GetBucketEncryption	
s3:GetBucketLastAccessTime	ZEITPUNKT des letzten Zugriffs FÜR den Bucket ABRUFEN	Ja.
s3:GetBucketLocation	GetBucketLocation	
s3:GetBucketMetadataBenachrichtigung	Konfiguration der Bucket-Metadaten-Benachrichtigungen ABRUFEN	Ja.
s3:GetBucketBenachrichtigung	GetBucketNotificationConfiguration	
s3:GetBucketObjectLockConfiguration	GetObjectLockConfiguration	
s3:GetBucketPolicy	GetBucketPolicy	
s3:GetBucketTagging	GetBucketTagging	
s3:GetBucketVersionierung	GetBucketVersioning	

Berechtigungen	S3-REST-API-OPERATIONEN	Individuell für StorageGRID
s3:GetLifecycleKonfiguration	GetBucketLifecycleKonfiguration	
s3:GetReplicationKonfiguration	GetBucketReplication	
s3>ListAllMyBuchs	<ul style="list-style-type: none"> ListBuchs GET Storage-Auslastung 	<p>Ja, für DIE GET Storage-Nutzung.</p> <p>Hinweis: Nur in Gruppenrichtlinien verwenden.</p>
s3>ListBucket	<ul style="list-style-type: none"> ListObjekte HeadBucket Objekt restoreObject 	
s3>ListBucketMultipartUploads	<ul style="list-style-type: none"> ListMultipartUploads Objekt restoreObject 	
s3>ListBucketVersions	Get Bucket-Versionen	
s3:PutBucketCompliance	PUT Bucket-Compliance (veraltet)	Ja.
s3:PutBucketConsistency	PUT Bucket-Konsistenz	Ja.
s3:PutBucketCORS	<ul style="list-style-type: none"> DeleteBucketCors† PutBucketCors 	
s3:PutVerschlüsselungKonfiguration	<ul style="list-style-type: none"> DeleteBucketEncryption PutBucketEncryption 	
s3:PutBucketLastAccessTime	PUT Bucket-Zeit für den letzten Zugriff	Ja.
s3:PutBucketMetadataBenachrichtigung	PUT Bucket-Metadaten-Benachrichtigungskonfiguration	Ja.
s3:PutBucketNotification	PutBucketNotificationKonfiguration	

Berechtigungen	S3-REST-API-OPERATIONEN	Individuell für StorageGRID
s3:PutBucketObjectLockConfiguration	<ul style="list-style-type: none"> • Erstellen Sie Bucket mit dem <code>x-amz-bucket-object-lock-enabled: true</code> Kopfzeile anfordern (erfordert auch die Berechtigung <code>s3:CreateBucket</code>) • PutObjectLockKonfiguration 	
s3:PutBucketPolicy	PutBucketPolicy	
s3:PutBucketTagging	<ul style="list-style-type: none"> • DeleteBucketTagging† • PutBucketTagging 	
s3:PutBucketVersionierung	PutBucketVersioning	
s3:PutLifecycleKonfiguration	<ul style="list-style-type: none"> • DeleteBucketLifecycle† • PutBucketLifecycleKonfiguration 	
s3:PutReplikationKonfiguration	PutBucketReplication	Ja, separate Berechtigungen für PUT und DELETE

Berechtigungen, die sich auf Objekte beziehen

Berechtigungen	S3-REST-API-OPERATIONEN	Individuell für StorageGRID
s3:AbortMeh rteilaUpload	<ul style="list-style-type: none"> • AbortMeh rteilaUpload • Objekt restoreObject 	
s3:BypassGovernanceAufbewahrung	<ul style="list-style-type: none"> • DeleteObject • Objekte deObjekteObjekte • PutObjectRetention 	
s3>DeleteObject	<ul style="list-style-type: none"> • DeleteObject • Objekte deObjekteObjekte • Objekt restoreObject 	
s3>DeleteObjectTagging	DeleteObjectTagging	
s3>DeleteObjectVersionTagging	DeleteObjectTagging (eine spezifische Version des Objekts)	

Berechtigungen	S3-REST-API-OPERATIONEN	Individuell für StorageGRID
s3:DeleteObjectVersion	DeleteObject (eine bestimmte Version des Objekts)	
s3:GetObject	<ul style="list-style-type: none"> • GetObject • HeadObject • Objekt restoreObject • SelektierObjectContent 	
s3:GetObjectAcl	GetObjectAcl	
s3:GetObjectLegalOld	GetObjectLegalHold	
s3:GetObjectRetention	GetObjectRetention	
s3:GetObjectTagging	GetObjectTagging	
s3:GetObjectVersionTagging	GetObjectTagging (eine spezifische Version des Objekts)	
s3:GetObjectVersion	GetObject (eine spezifische Version des Objekts)	
s3:ListeMultipartUploadParts	ListParts, RestoreObject	
s3:PutObject	<ul style="list-style-type: none"> • PutObject • CopyObject • Objekt restoreObject • CreateMultipartUpload • CompleteMultipartUpload • UploadTeil • UploadPartCopy 	
s3:PutObjectLegalOld	PutObjectLegalHold	
s3:PutObjectRetention	PutObjectRetention	
s3:PutObjectTagging	PutObjectTagging	
s3:PutObjectVersionTagging	PutObjectTagging (eine spezifische Version des Objekts)	

Berechtigungen	S3-REST-API-OPERATIONEN	Individuell für StorageGRID
s3:PutOverwrite Object	<ul style="list-style-type: none"> • PutObject • CopyObject • PutObjectTagging • DeleteObjectTagging • CompleteMultipartUpload 	Ja.
s3:RestoreObject	Objekt restoreObject	

Verwenden Sie PutOverwriteObject-Berechtigung

die s3:PutOverwriteObject-Berechtigung ist eine benutzerdefinierte StorageGRID-Berechtigung, die für Vorgänge gilt, die Objekte erstellen oder aktualisieren. Durch diese Berechtigung wird festgelegt, ob der Client die Daten, benutzerdefinierte Metadaten oder S3-Objekt-Tagging überschreiben kann.

Mögliche Einstellungen für diese Berechtigung sind:

- **Zulassen:** Der Client kann ein Objekt überschreiben. Dies ist die Standardeinstellung.
- **Deny:** Der Client kann ein Objekt nicht überschreiben. Wenn die Option „Ablehnen“ eingestellt ist, funktioniert die Berechtigung „PutOverwriteObject“ wie folgt:
 - Wenn ein vorhandenes Objekt auf demselben Pfad gefunden wird:
 - Die Daten, benutzerdefinierten Metadaten oder S3-Objekt-Tagging des Objekts können nicht überschrieben werden.
 - Alle laufenden Aufnahmevorgänge werden abgebrochen und ein Fehler wird zurückgegeben.
 - Wenn die S3-Versionierung aktiviert ist, verhindert die Einstellung Deny, dass PutObjectTagging- oder DeleteObjectTagging-Operationen das TagSet für ein Objekt und seine nicht aktuellen Versionen ändern.
 - Wenn ein vorhandenes Objekt nicht gefunden wird, hat diese Berechtigung keine Wirkung.
- Wenn diese Berechtigung nicht vorhanden ist, ist der Effekt der gleiche, als ob Allow-were gesetzt wurden.



Wenn die aktuelle S3-Richtlinie Überschreiben zulässt und die PutOverwriteObject-Berechtigung auf Deny festgelegt ist, kann der Client die Daten, benutzerdefinierten Metadaten oder Objekt-Tagging eines Objekts nicht überschreiben. Wenn zusätzlich das Kontrollkästchen **Client-Änderung verhindern** aktiviert ist (**KONFIGURATION > Sicherheitseinstellungen > Netzwerk und Objekte**), setzt diese Einstellung die Einstellung der PutOverwriteObject-Berechtigung außer Kraft.

Legen Sie Bedingungen in einer Richtlinie fest

Die Bedingungen legen fest, wann eine Richtlinie in Kraft sein wird. Die Bedingungen bestehen aus Bedienern und Schlüsselwertpaaren.

Bedingungen Verwenden Sie Key-Value-Paare für die Auswertung. Ein Bedingungelement kann mehrere Bedingungen enthalten, und jede Bedingung kann mehrere Schlüsselwert-Paare enthalten. Der Bedingungsblock verwendet das folgende Format:

```
Condition: {
  condition_type: {
    condition_key: condition_values
```

Im folgenden Beispiel verwendet die IPAddress-Bedingung den SourceIp-Bedingungsschlüssel.

```
"Condition": {
  "IpAddress": {
    "aws:SourceIp": "54.240.143.0/24"
    ...
  },
  ...
```

Unterstützte Bedingungsoperatoren

Bedingungsoperatoren werden wie folgt kategorisiert:

- Zeichenfolge
- Numerisch
- Boolesch
- IP-Adresse
- Null-Prüfung

Bedingungsoperatoren	Beschreibung
StringEquals	Vergleicht einen Schlüssel mit einem Zeichenfolgenwert, der auf exakter Übereinstimmung basiert (Groß-/Kleinschreibung wird beachtet).
StringNotEquals	Vergleicht einen Schlüssel mit einem Zeichenfolgenwert, der auf negatives Matching basiert (Groß-/Kleinschreibung wird beachtet).
StringEquisgnoreCase	Vergleicht einen Schlüssel mit einem Zeichenfolgenwert, der auf exakter Übereinstimmung basiert (Groß-/Kleinschreibung wird ignoriert).
StringNotEquisgnoreCase	Vergleicht einen Schlüssel mit einem String-Wert, der auf negatives Matching basiert (Groß-/Kleinschreibung wird ignoriert).
StringLike	Vergleicht einen Schlüssel mit einem Zeichenfolgenwert, der auf exakter Übereinstimmung basiert (Groß-/Kleinschreibung wird beachtet). Kann * und ? Platzhalterzeichen.
StringNotLike	Vergleicht einen Schlüssel mit einem Zeichenfolgenwert, der auf negatives Matching basiert (Groß-/Kleinschreibung wird beachtet). Kann * und ? Platzhalterzeichen.

Bedingungsoperatoren	Beschreibung
Ziffern	Vergleicht einen Schlüssel mit einem numerischen Wert, der auf exakter Übereinstimmung basiert.
ZiffernNotequals	Vergleicht einen Schlüssel mit einem numerischen Wert, der auf negatives Matching basiert.
NumericGreaterThan	Vergleicht einen Schlüssel mit einem numerischen Wert basierend auf dem „größer als“-Vergleich.
ZahlungGreaterThanEquals	Vergleicht einen Schlüssel mit einem numerischen Wert basierend auf dem „größer als oder gleich“-Vergleich.
NumericLessThan	Vergleicht einen Schlüssel mit einem numerischen Wert basierend auf „weniger als“-Übereinstimmung.
ZahlungWenigerThanEquals	Vergleicht einen Schlüssel mit einem numerischen Wert basierend auf dem „kleiner als oder gleich“-Vergleich.
Bool	Vergleicht einen Schlüssel mit einem booleschen Wert basierend auf „true“ oder „false“-Matching.
IP-Adresse	Vergleicht einen Schlüssel mit einer IP-Adresse oder einem IP-Adressbereich.
NotIpAddress	Vergleicht einen Schlüssel mit einer IP-Adresse oder einem IP-Adressbereich, basierend auf negatierem Abgleich.
Null	Überprüft, ob im aktuellen Anforderungskontext ein Bedingungsschlüssel vorhanden ist.

Unterstützte Bedingungsschlüssel

Zustandsschlüssel	Aktionen	Beschreibung
aws:SourceIp	IP-Operatoren	<p>Vergleicht mit der IP-Adresse, von der die Anfrage gesendet wurde. Kann für Bucket- oder Objektvorgänge verwendet werden</p> <p>Hinweis: wurde die S3-Anfrage über den Lastbalancer-Dienst auf Admin-Knoten und Gateways-Knoten gesendet, wird dies mit der IP-Adresse verglichen, die vor dem Load Balancer Service liegt.</p> <p>Hinweis: Wenn ein Drittanbieter-, nicht-transparenter Load Balancer verwendet wird, wird dies mit der IP-Adresse dieses Load Balancer verglichen. Alle <code>X-Forwarded-For</code> Kopfzeile wird ignoriert, da ihre Gültigkeit nicht ermittelt werden kann.</p>
aws:Benutzername	Ressource/Identität	Vergleicht mit dem Benutzernamen des Absenders, von dem die Anfrage gesendet wurde. Kann für Bucket- oder Objektvorgänge verwendet werden
s3:Trennzeichen	s3:ListBucket und s3:ListBucketVersions Berechtigungen	Wird mit dem in einer ListObjects- oder ListObjectVersions-Anforderung angegebenen Trennzeichen-Parameter verglichen.
s3:ExistingObjectTag/<tag-key>	s3:DeleteObjectTagging s3:DeleteObjectVersionTagging s3:GetObject s3:GetObjectAcl s3:GetObjectTagging s3:GetObjectVersion s3:GetObjectVersionAcl s3:GetObjectVersionTagging s3:PutObjectAcl s3:PutObjectTagging s3:PutObjectVersionAcl s3:PutObjectVersionTagging	Erfordert, dass das vorhandene Objekt über den spezifischen Tag-Schlüssel und -Wert verfügt.

Zustandsschlüssel	Aktionen	Beschreibung
s3:max-keys	s3:ListBucket und s3:ListBucketVersions Berechtigungen	Wird mit dem Parameter max-keys verglichen, der in einer ListObjects- oder ListObjectVersions-Anforderung angegeben ist.
s3:verbleibende Object-Lock-Retention-Tage	s3:PutObject	Vergleicht mit dem in angegebenen Aufbewahrungsdatum x-amz-object-lock-retain-until-date Kopfzeile anfordern oder berechnet aus der Standardaufbewahrungsdauer des Buckets, um sicherzustellen, dass diese Werte innerhalb des zulässigen Bereichs für die folgenden Anforderungen liegen: <ul style="list-style-type: none"> • PutObject • CopyObject • CreateMultipartUpload
s3:verbleibende Object-Lock-Retention-Tage	s3:PutObjectRetention	Vergleicht das in der PutObjectRetention-Anfrage angegebene Aufbewahrungsdatum, um sicherzustellen, dass es innerhalb des zulässigen Bereichs liegt.
s3:Präfix	s3:ListBucket und s3:ListBucketVersions Berechtigungen	Wird mit dem Präfix-Parameter verglichen, der in einer ListObjects- oder ListObjectVersions-Anforderung angegeben ist.
s3:RequestObjectTag/<tag-key>	s3:PutObject s3:PutObjectTagging s3:PutObjectVersionTagging	Erfordert einen bestimmten Tag-Schlüssel und einen bestimmten Wert, wenn die Objektanforderung Tagging beinhaltet.

Geben Sie Variablen in einer Richtlinie an

Sie können Variablen in Richtlinien verwenden, um die Richtlinieninformationen auszufüllen, wenn sie verfügbar sind. Sie können Richtlinienvariablen in verwenden `Resource` Element und in String-Vergleichen im `Condition` Element:

In diesem Beispiel die Variable `${aws:username}` Ist Teil des Ressourcenelements:

```
"Resource": "arn:aws:s3:::bucket-name/home/${aws:username}/*"
```

In diesem Beispiel die Variable `${aws:username}` Ist Teil des Bedingungs Wertes im Bedingungsblock:

```

"Condition": {
  "StringLike": {
    "s3:prefix": "${aws:username}/*"
    ...
  },
  ...
}

```

Variabel	Beschreibung
<code>\${aws:SourceIp}</code>	Verwendet den SourceIp-Schlüssel als bereitgestellte Variable.
<code>\${aws:username}</code>	Verwendet den Benutzernamen-Schlüssel als bereitgestellte Variable.
<code>\${s3:prefix}</code>	Verwendet den Service-spezifischen Präfixschlüssel als bereitgestellte Variable.
<code>\${s3:max-keys}</code>	Verwendet die Service-spezifische max-keys als die angegebene Variable.
<code>\${*}</code>	Sonderzeichen. Verwendet das Zeichen als Literal * -Zeichen.
<code>\${?}</code>	Sonderzeichen. Verwendet den Charakter als Literal ? Zeichen.
<code>\${\$}</code>	Sonderzeichen. Verwendet das Zeichen als Literal USD Zeichen.

Erstellen von Richtlinien, die eine spezielle Handhabung erfordern

Manchmal kann eine Richtlinie Berechtigungen erteilen, die für die Sicherheit oder die Gefahr für einen fortgesetzten Betrieb gefährlich sind, z. B. das Sperren des Root-Benutzers des Kontos. Die StorageGRID S3-REST-API-Implementierung ist bei der Richtlinienuvalidierung weniger restriktiv als Amazon, aber auch bei der Richtlinienbewertung streng.

Richtlinienbeschreibung	Richtlinientyp	Verhalten von Amazon	Verhalten von StorageGRID
Verweigern Sie sich selbst irgendwelche Berechtigungen für das Root-Konto	Eimer	Gültig und durchgesetzt, aber das Root-Benutzerkonto behält die Berechtigung für alle S3 Bucket-Richtlinienvorgänge bei	Gleich
Verweigern Sie selbst jegliche Berechtigungen für Benutzer/Gruppe	Gruppieren	Gültig und durchgesetzt	Gleich

Richtlinienbeschreibung	Richtlinientyp	Verhalten von Amazon	Verhalten von StorageGRID
Erlauben Sie einer fremden Kontogruppe jegliche Berechtigung	Eimer	Ungültiger Principal	Gültig, aber die Berechtigungen für alle S3-Bucket-Richtlinienvorgänge geben bei Richtlinienzugelassen durch eine Richtlinie einen nicht zugelassenen 405-Method-Fehler zurück
Berechtigung für ein ausländisches Konto oder einen Benutzer zulassen	Eimer	Gültig, aber die Berechtigungen für alle S3-Bucket-Richtlinienvorgänge geben bei Richtlinienzugelassen durch eine Richtlinie einen nicht zugelassenen 405-Method-Fehler zurück	Gleich
Alle Berechtigungen für alle Aktionen zulassen	Eimer	Gültig, aber Berechtigungen für alle S3-Bucket-Richtlinienvorgänge geben einen 405 Methode nicht erlaubten Fehler für das ausländische Konto Root und Benutzer zurück	Gleich
Alle Berechtigungen für alle Aktionen verweigern	Eimer	Gültig und durchgesetzt, aber das Root-Benutzerkonto behält die Berechtigung für alle S3 Bucket-Richtlinienvorgänge bei	Gleich
Principal ist ein nicht existierender Benutzer oder eine Gruppe	Eimer	Ungültiger Principal	Gültig
Die Ressource ist ein nicht existierender S3-Bucket	Gruppieren	Gültig	Gleich
Principal ist eine lokale Gruppe	Eimer	Ungültiger Principal	Gültig

Richtlinienbeschreibung	Richtlinientyp	Verhalten von Amazon	Verhalten von StorageGRID
Die Richtlinie gewährt einem Konto ohne Eigentümer (einschließlich anonymer Konten) Berechtigungen zum Setzen von Objekten.	Eimer	Gültig. Objekte sind Eigentum des Erstellerkontos, und die Bucket-Richtlinie gilt nicht. Das Ersteller-Konto muss über Objekt-ACLs Zugriffsrechte für das Objekt gewähren.	Gültig. Der Eigentümer der Objekte ist das Bucket-Owner-Konto. Bucket-Richtlinie gilt.

WORM-Schutz (Write Once, Read Many)

Sie können WORM-Buckets (Write-Once-Read-Many) erstellen, um Daten, benutzerdefinierte Objekt-Metadaten und S3-Objekt-Tagging zu sichern. SIE konfigurieren die WORM-Buckets, um das Erstellen neuer Objekte zu ermöglichen und Überschreibungen oder das Löschen vorhandener Inhalte zu verhindern. Verwenden Sie einen der hier beschriebenen Ansätze.

Um sicherzustellen, dass Überschreibungen immer verweigert werden, können Sie:

- Gehen Sie im Grid Manager zu **CONFIGURATION > Security > Security settings > Network and Objects** und aktivieren Sie das Kontrollkästchen **Client-Änderung verhindern**.
- Wenden Sie die folgenden Regeln und S3-Richtlinien an:
 - Fügen Sie der S3-Richtlinie einen PutOverwriteObject DENY-Vorgang hinzu.
 - Fügen Sie der S3-Richtlinie einen DeleteObject DENY-Vorgang hinzu.
 - Fügen Sie der S3-Richtlinie einen PutObject ALLOW-Vorgang hinzu.



Wenn in einer S3-Richtlinie DeleteObject auf DENY festgelegt wird, verhindert dies nicht, dass ILM Objekte löscht, wenn eine Regel wie „Zero Copies after 30 days“ vorhanden ist.



Selbst wenn alle diese Regeln und Richtlinien angewendet werden, schützen sie sich nicht vor gleichzeitigen Schreibvorgängen (siehe Situation A). Sie schützen vor sequenziellen Überschreibungen (siehe Situation B).

Situation A: Gleichzeitige Schreibvorgänge (nicht bewacht)

```
/mybucket/important.doc
PUT#1 ---> OK
PUT#2 -----> OK
```

Situation B: Sequentielle abgeschlossene Überschreibungen (bewacht gegen)

```
/mybucket/important.doc
PUT#1 -----> PUT#2 ---X (denied)
```

Verwandte Informationen

- ["Managen von Objekten durch StorageGRID ILM-Regeln"](#)
- ["Beispiel für Bucket-Richtlinien"](#)
- ["Beispiel für Gruppenrichtlinien"](#)
- ["Objektmanagement mit ILM"](#)
- ["Verwenden Sie ein Mandantenkonto"](#)

Beispiel für Bucket-Richtlinien

Mithilfe der Beispiele in diesem Abschnitt können Sie StorageGRID-Zugriffsrichtlinien für Buckets erstellen.

Bucket-Richtlinien geben die Zugriffsberechtigungen für den Bucket an, mit dem die Richtlinie verknüpft ist. Bucket-Richtlinien werden mithilfe der S3-PutBucketPolicy-API konfiguriert. Siehe ["Operationen auf Buckets"](#).

Eine Bucket-Richtlinie kann mithilfe der AWS CLI wie folgt konfiguriert werden:

```
> aws s3api put-bucket-policy --bucket examplebucket --policy
file://policy.json
```

Beispiel: Lesezugriff auf einen Bucket zulassen

In diesem Beispiel darf jeder, auch anonym, Objekte im Bucket auflisten und GetObject-Operationen für alle Objekte im Bucket ausführen. Alle anderen Operationen werden abgelehnt. Beachten Sie, dass diese Richtlinie möglicherweise nicht besonders nützlich ist, da niemand außer dem Konto root über Berechtigungen zum Schreiben in den Bucket verfügt.

```
{
  "Statement": [
    {
      "Sid": "AllowEveryoneReadOnlyAccess",
      "Effect": "Allow",
      "Principal": "*",
      "Action": [ "s3:GetObject", "s3:ListBucket" ],
      "Resource":
[ "arn:aws:s3:::examplebucket", "arn:aws:s3:::examplebucket/*" ]
    }
  ]
}
```

Beispiel: Jeder in einem Konto Vollzugriff zulassen, und jeder in einem anderen Konto hat nur Lesezugriff auf einen Bucket

In diesem Beispiel ist jedem in einem bestimmten Konto der vollständige Zugriff auf einen Bucket gestattet, während jeder in einem anderen angegebenen Konto nur die Liste des Buckets und die Durchführung von GetObject-Operationen für Objekte im Bucket erlaubt ist, die mit dem beginnenden `shared/` Objektschlüsselpräfix.



In StorageGRID sind Objekte, die von einem nicht-Inhaberkonto erstellt wurden (einschließlich anonymer Konten), Eigentum des Bucket-Inhaberkontos. Die Bucket-Richtlinie gilt für diese Objekte.

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "95390887230002558202"
      },
      "Action": "s3:*",
      "Resource": [
        "arn:aws:s3:::examplebucket",
        "arn:aws:s3:::examplebucket/*"
      ]
    },
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "31181711887329436680"
      },
      "Action": "s3:GetObject",
      "Resource": "arn:aws:s3:::examplebucket/shared/*"
    },
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "31181711887329436680"
      },
      "Action": "s3:ListBucket",
      "Resource": "arn:aws:s3:::examplebucket",
      "Condition": {
        "StringLike": {
          "s3:prefix": "shared/*"
        }
      }
    }
  ]
}
```

Beispiel: Lesezugriff für einen Bucket und vollständiger Zugriff durch angegebene Gruppe

In diesem Beispiel kann jeder, einschließlich anonym, den Bucket auflisten und GetObject-Operationen für alle Objekte im Bucket ausführen, während nur Benutzer der Gruppe angehören `Marketing` Im angegebenen Konto ist Vollzugriff erlaubt.

```

{
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::95390887230002558202:federated-
group/Marketing"
      },
      "Action": "s3:*",
      "Resource": [
        "arn:aws:s3:::examplebucket",
        "arn:aws:s3:::examplebucket/*"
      ]
    },
    {
      "Effect": "Allow",
      "Principal": "*",
      "Action": ["s3:ListBucket", "s3:GetObject"],
      "Resource": [
        "arn:aws:s3:::examplebucket",
        "arn:aws:s3:::examplebucket/*"
      ]
    }
  ]
}

```

Beispiel: Jeder Lese- und Schreibzugriff auf einen Bucket zulassen, wenn Client im IP-Bereich ist

In diesem Beispiel darf jeder, einschließlich anonym, den Bucket auflisten und beliebige Objektvorgänge an allen Objekten im Bucket durchführen, vorausgesetzt, dass die Anforderungen aus einem bestimmten IP-Bereich stammen (54.240.143.0 bis 54.240.143.255, außer 54.240.143.188). Alle anderen Vorgänge werden abgelehnt, und alle Anfragen außerhalb des IP-Bereichs werden abgelehnt.

```

{
  "Statement": [
    {
      "Sid": "AllowEveryoneReadWriteAccessIfInSourceIpRange",
      "Effect": "Allow",
      "Principal": "*",
      "Action": [ "s3:*Object", "s3:ListBucket" ],
      "Resource":
["arn:aws:s3:::examplebucket", "arn:aws:s3:::examplebucket/*"],
      "Condition": {
        "IpAddress": {"aws:SourceIp": "54.240.143.0/24"},
        "NotIpAddress": {"aws:SourceIp": "54.240.143.188"}
      }
    }
  ]
}

```

Beispiel: Vollständigen Zugriff auf einen Bucket zulassen, der ausschließlich von einem festgelegten föderierten Benutzer verwendet wird

In diesem Beispiel ist dem föderierten Benutzer Alex der vollständige Zugriff auf das erlaubt `examplebucket` Bucket und seine Objekte. Alle anderen Benutzer, einschließlich 'root', werden ausdrücklich allen Operationen verweigert. Beachten Sie jedoch, dass 'root' niemals die Berechtigungen zum Put/get/DeleteBucketPolicy verweigert wird.

```

{
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::95390887230002558202:federated-user/Alex"
      },
      "Action": [
        "s3:*"
      ],
      "Resource": [
        "arn:aws:s3:::examplebucket",
        "arn:aws:s3:::examplebucket/*"
      ]
    },
    {
      "Effect": "Deny",
      "NotPrincipal": {
        "AWS": "arn:aws:iam::95390887230002558202:federated-user/Alex"
      },
      "Action": [
        "s3:*"
      ],
      "Resource": [
        "arn:aws:s3:::examplebucket",
        "arn:aws:s3:::examplebucket/*"
      ]
    }
  ]
}

```

Beispiel: PutOverwriteObject-Berechtigung

In diesem Beispiel ist der `Deny` Effect für `PutOverwriteObject` und `DeleteObject` stellt sicher, dass niemand die Daten, benutzerdefinierte Metadaten und S3-Objekt-Tagging überschreiben oder löschen kann.

```

{
  "Statement": [
    {
      "Effect": "Deny",
      "Principal": "*",
      "Action": [
        "s3:PutOverwriteObject",
        "s3:DeleteObject",
        "s3:DeleteObjectVersion"
      ],
      "Resource": "arn:aws:s3:::wormbucket/*"
    },
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::95390887230002558202:federated-
group/SomeGroup"
      },
      "Action": "s3:ListBucket",
      "Resource": "arn:aws:s3:::wormbucket"
    },
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::95390887230002558202:federated-
group/SomeGroup"
      },
      "Action": "s3:*",
      "Resource": "arn:aws:s3:::wormbucket/*"
    }
  ]
}

```

Beispiel für Gruppenrichtlinien

Verwenden Sie die Beispiele in diesem Abschnitt, um StorageGRID-Zugriffsrichtlinien für Gruppen zu erstellen.

Gruppenrichtlinien legen die Zugriffsberechtigungen für die Gruppe fest, der die Richtlinie zugeordnet ist. Es gibt keine `Principal` Element in der Richtlinie, weil sie implizit ist. Gruppenrichtlinien werden mit dem Tenant Manager oder der API konfiguriert.

Beispiel: Legen Sie eine Gruppenrichtlinie mit Tenant Manager fest

Wenn Sie eine Gruppe im Tenant Manager hinzufügen oder bearbeiten, können Sie eine Gruppenrichtlinie auswählen, um festzulegen, über welche S3-Zugriffsberechtigungen die Mitglieder dieser Gruppe verfügen. Siehe "[Erstellen von Gruppen für einen S3-Mandanten](#)".

- **Kein S3-Zugriff:** Standardoption. Benutzer in dieser Gruppe haben keinen Zugriff auf S3-Ressourcen, es sei denn, der Zugriff wird über eine Bucket-Richtlinie gewährt. Wenn Sie diese Option auswählen, hat nur der Root-Benutzer standardmäßig Zugriff auf S3-Ressourcen.
- **Schreibgeschützter Zugriff:** Benutzer in dieser Gruppe haben schreibgeschützten Zugriff auf S3-Ressourcen. Benutzer in dieser Gruppe können beispielsweise Objekte auflisten und Objektdaten, Metadaten und Tags lesen. Wenn Sie diese Option auswählen, wird im Textfeld der JSON-String für eine schreibgeschützte Gruppenrichtlinie angezeigt. Diese Zeichenfolge kann nicht bearbeitet werden.
- **Vollzugriff:** Benutzer in dieser Gruppe haben vollen Zugriff auf S3-Ressourcen, einschließlich Buckets. Wenn Sie diese Option auswählen, wird im Textfeld der JSON-String für eine Richtlinie mit vollem Zugriff angezeigt. Diese Zeichenfolge kann nicht bearbeitet werden.
- **Ransomware Mitigation:** Diese Beispielrichtlinie gilt für alle Buckets für diesen Mandanten. Benutzer in dieser Gruppe können allgemeine Aktionen ausführen, aber Objekte aus Buckets, für die die Objektversionierung aktiviert ist, nicht dauerhaft löschen.

Mandanten-Manager-Benutzer mit der Berechtigung zum Verwalten aller Buckets können diese Gruppenrichtlinie überschreiben. Beschränken Sie die Berechtigung zum Verwalten aller Buckets auf vertrauenswürdige Benutzer und verwenden Sie die Multi-Faktor-Authentifizierung (MFA), sofern verfügbar.

- **Benutzerdefiniert:** Benutzern in der Gruppe werden die Berechtigungen erteilt, die Sie im Textfeld angeben.

Beispiel: Vollständigen Zugriff auf alle Buckets zulassen

In diesem Beispiel sind alle Mitglieder der Gruppe berechtigt, vollständigen Zugriff auf alle Buckets des Mandantenkontos zu erhalten, sofern nicht ausdrücklich von der Bucket-Richtlinie abgelehnt wurde.

```
{
  "Statement": [
    {
      "Action": "s3:*",
      "Effect": "Allow",
      "Resource": "arn:aws:s3:::*"
    }
  ]
}
```

Beispiel: Schreibgeschützter Zugriff auf alle Buckets für Gruppen zulassen

In diesem Beispiel haben alle Mitglieder der Gruppe schreibgeschützten Zugriff auf S3-Ressourcen, sofern nicht ausdrücklich von der Bucket-Richtlinie abgelehnt wird. Benutzer in dieser Gruppe können beispielsweise Objekte auflisten und Objektdaten, Metadaten und Tags lesen.

```

{
  "Statement": [
    {
      "Sid": "AllowGroupReadOnlyAccess",
      "Effect": "Allow",
      "Action": [
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "s3:ListBucketVersions",
        "s3:GetObject",
        "s3:GetObjectTagging",
        "s3:GetObjectVersion",
        "s3:GetObjectVersionTagging"
      ],
      "Resource": "arn:aws:s3:::*"
    }
  ]
}

```

Beispiel: Gruppenmitgliedern vollen Zugriff nur auf ihren "Ordner" in einem Bucket erlauben

In diesem Beispiel dürfen Mitglieder der Gruppe nur ihren spezifischen Ordner (Schlüsselpräfix) im angegebenen Bucket auflisten und darauf zugreifen. Beachten Sie, dass bei der Festlegung der Privatsphäre dieser Ordner Zugriffsberechtigungen aus anderen Gruppenrichtlinien und der Bucket-Richtlinie berücksichtigt werden sollten.

```

{
  "Statement": [
    {
      "Sid": "AllowListBucketOfASpecificUserPrefix",
      "Effect": "Allow",
      "Action": "s3:ListBucket",
      "Resource": "arn:aws:s3:::department-bucket",
      "Condition": {
        "StringLike": {
          "s3:prefix": "${aws:username}/*"
        }
      }
    },
    {
      "Sid": "AllowUserSpecificActionsOnlyInTheSpecificUserPrefix",
      "Effect": "Allow",
      "Action": "s3:*Object",
      "Resource": "arn:aws:s3:::department-bucket/${aws:username}/*"
    }
  ]
}

```

S3-Vorgänge werden in den Audit-Protokollen protokolliert

Audit-Meldungen werden von StorageGRID-Diensten generiert und in Text-Log-Dateien gespeichert. Sie können die S3-spezifischen Audit-Meldungen im Revisionsprotokoll prüfen, um Details zu Bucket- und Objektivorgängen zu abrufen.

Bucket-Vorgänge werden in den Audit-Protokollen protokolliert

- CreateBucket
- DeleteBucket
- DeleteBucketTagging
- Objekte deObjekteObjekte
- GetBucketTagging
- HeadBucket
- ListObjekte
- ListObjectVersions
- BUCKET-Compliance
- PutBucketTagging
- PutBucketVersioning

Objektvorgänge werden in den Audit-Protokollen protokolliert

- CompleteMultipartUpload
- CopyObject
- DeleteObject
- GetObject
- HeadObject
- PutObject
- Objekt restoreObject
- Wählen Sie Objekt aus
- UploadPart (wenn eine ILM-Regel ausgeglichene oder strikte Aufnahme verwendet)
- UploadPartCopy (wenn eine ILM-Regel ausgeglichene oder strikte Aufnahme verwendet)

Verwandte Informationen

- ["Zugriff auf die Audit-Log-Datei"](#)
- ["Audit-Meldungen des Clients schreiben"](#)
- ["Client liest Audit-Meldungen"](#)

Swift REST API verwenden (veraltet)

Übersicht über die Swift REST API

Client-Applikationen können die OpenStack Swift API zur Schnittstelle mit dem StorageGRID System nutzen.



Die Unterstützung für Swift-Client-Anwendungen wurde veraltet und wird in einer zukünftigen Version entfernt.

StorageGRID unterstützt die folgenden spezifischen Versionen von Swift und HTTP.

Element	Version
Swift-Spezifikation	OpenStack Swift Objekt Storage API v1 ab November 2015
HTTP	1.1 Weitere Informationen zu HTTP finden Sie unter HTTP/1.1 (RFCs 7230-35) . Hinweis: StorageGRID unterstützt HTTP/1.1-Pipelining nicht.

Verwandte Informationen

["OpenStack: Objekt-Storage-API"](#)

Geschichte der Unterstützung von Swift API in StorageGRID

Bei Änderungen an der Unterstützung des StorageGRID-Systems für die Swift REST-API sollten Sie auf dieser hinweisen.

Freigabe	Kommentare
11.8	
11.7	Die Unterstützung für Swift-Client-Anwendungen wurde veraltet und wird in einer zukünftigen Version entfernt.
11.6	Kleine redaktionelle Änderungen.
11.5	Schwache Konsistenz wurde entfernt. Stattdessen wird die verfügbare Konsistenz verwendet.
11.4	Unterstützung für TLS 1.3 hinzugefügt. Beschreibung des Zusammenhangs zwischen ILM und Konsistenz hinzugefügt.
11.3	Aktualisierte PUT-Objektvorgänge zur Beschreibung der Auswirkungen von ILM-Regeln, die synchrone Platzierung bei der Aufnahme verwenden (die ausgewogenen und strengen Optionen für das Aufnahmeverhalten) Eine zusätzliche Beschreibung der Client-Verbindungen, die Load Balancer-Endpunkte oder Hochverfügbarkeitsgruppen verwenden. TLS 1.1-Chiffren werden nicht mehr unterstützt.
11.2	Kleine redaktionelle Änderungen des Dokuments.
11.1	Zusätzlicher Support für die Verwendung von HTTP für Swift-Client-Verbindungen zu Grid-Nodes. Die Definitionen der Konsistenzwerte wurden aktualisiert.
11.0	Hinzugefügter Support für 1,000 Container für jedes Mandantenkonto.
10.3	Administrative Aktualisierungen und Korrekturen des Dokuments. Abschnitte zum Konfigurieren von benutzerdefinierten Serverzertifikaten entfernt.
10.2	Unterstützung der Swift API durch das StorageGRID System zu Beginn. Die derzeit unterstützte Version ist OpenStack Swift Object Storage API v1.

So implementiert StorageGRID Swift REST API

Eine Client-Applikation kann mithilfe von Swift REST-API-Aufrufen eine Verbindung zu Storage-Nodes und Gateway-Nodes herstellen, um Container zu erstellen und Objekte zu speichern und abzurufen. Dadurch können serviceorientierte Applikationen, die für OpenStack Swift entwickelt wurden, mit lokalem Objekt-Storage des StorageGRID Systems verbunden werden.

Swift Objekt-Management

Nachdem Swift Objekte in das StorageGRID System aufgenommen wurden, werden sie durch die Regeln für Information Lifecycle Management (ILM) in den aktiven ILM-Richtlinien gemanagt. ["ILM-Regeln"](#) Und ["ILM-Richtlinien"](#) Legen Sie fest, wie StorageGRID Kopien von Objektdaten erstellt und verteilt und wie diese Kopien über einen längeren Zeitraum gemanagt werden. Eine ILM-Regel kann beispielsweise für Objekte in bestimmten Swift Containern gelten und möglicherweise angeben, dass mehrere Objektkopien für eine bestimmte Anzahl von Jahren in mehreren Datacentern gespeichert werden.

Wenden Sie sich an Ihren NetApp Professional Services Berater oder StorageGRID Administrator, wenn Sie Informationen darüber benötigen, wie sich die ILM-Regeln und -Richtlinien des Grids auf die Objekte in Ihrem Swift Mandantenkonto auswirken.

In Konflikt stehende Clientanforderungen

Widersprüchliche Clientanforderungen, wie z. B. zwei Clients, die in denselben Schlüssel schreiben, werden auf der Grundlage der „neuesten Wins“ gelöst. Der Zeitpunkt für die Bewertung „neuester Erfolge“ basiert darauf, wann das StorageGRID System eine bestimmte Anfrage abschließt und nicht darauf, wann Swift-Clients einen Vorgang starten.

Konsistenzgarantien und -Kontrollen

Standardmäßig bietet StorageGRID Lese-/Nachher-Konsistenz für neu erstellte Objekte und schließlich die Konsistenz von Objekt-Updates und HEAD-Operationen. Alle ["GET"](#) Nach erfolgreichem Abschluss ["PUT"](#) Kann die neu geschriebenen Daten lesen. Überschreibungen vorhandener Objekte, Metadatenaktualisierungen und -Löschungen sind schließlich konsistent. Überschreibungen dauern in der Regel nur wenige Sekunden oder Minuten, können jedoch bis zu 15 Tage in Anspruch nehmen.

StorageGRID ermöglicht Ihnen außerdem die Kontrolle der Konsistenz einzelner Container. Konsistenzwerte bieten ein Gleichgewicht zwischen der Verfügbarkeit der Objekte und der Konsistenz dieser Objekte über verschiedene Storage Nodes und Standorte hinweg, wie es von Ihrer Anwendung gefordert wird.

Empfehlungen für die Implementierung von Swift REST API

Bei der Implementierung der Swift REST API zur Verwendung mit StorageGRID sollten Sie diese Empfehlungen beachten.

Empfehlungen für Köpfe zu nicht vorhandenen Objekten

Wenn Ihre Anwendung regelmäßig prüft, ob ein Objekt in einem Pfad vorhanden ist, in dem Sie nicht erwarten, dass das Objekt tatsächlich existiert, sollten Sie die Konsistenz „verfügbar“ verwenden. Sie sollten beispielsweise die Konsistenz „verfügbar“ verwenden, wenn Ihre Anwendung einen HAUPTVORGANG an einem Speicherort durchführt, bevor Sie einen PUT-Vorgang an diesem Speicherort durchführen.

Andernfalls werden möglicherweise 500 Fehler des internen Servers angezeigt, wenn ein oder mehrere Speicherknoten nicht verfügbar sind.

Sie können die Konsistenz für jeden Container mithilfe von festlegen ["PUT Container-Konsistenzanforderung"](#). Sie können die Konsistenz „verfügbar“ für jeden Container mithilfe von anzeigen ["ABRUFEN der Container-Konsistenzanforderung"](#).

Empfehlungen für Objektnamen

Bei Containern, die in StorageGRID 11.4 oder höher erstellt wurden, ist keine Beschränkung der Objektnamen auf die Performance-Best Practices mehr erforderlich. Sie können jetzt beispielsweise Zufallswerte für die

ersten vier Zeichen von Objektnamen verwenden.

Befolgen Sie bei Containern, die in Versionen vor StorageGRID 11.4 erstellt wurden, weiterhin diese Empfehlungen für Objektnamen:

- Als die ersten vier Zeichen von Objektnamen sollten keine Zufallswerte verwendet werden. Dies steht im Gegensatz zu der früheren AWS Empfehlung für Namenspräfixe. Stattdessen sollten Sie nicht-zufällige, nicht-eindeutige Präfixe verwenden, wie z. B. `image`.
- Wenn Sie die frühere Empfehlung von AWS befolgen, zufällige und eindeutige Zeichen in Namenspräfixen zu verwenden, sollten Sie die Objektnamen mit einem Verzeichnisnamen vorschreiben. Verwenden Sie dieses Format:

```
mycontainer/mydir/f8e3-image3132.jpg
```

Anstelle dieses Formats:

```
mycontainer/f8e3-image3132.jpg
```

Empfehlungen für „Range Reads“

Wenn der "[Globale Option zum Komprimieren gespeicherter Objekte](#)" Ist aktiviert, sollten Swift-Client-Anwendungen die Ausführung VON GET-Objektoperationen vermeiden, die einen Bereich von Bytes angeben, die zurückgegeben werden sollen. Diese Vorgänge beim Lesen von Range sind ineffizient, da StorageGRID Objekte effektiv dekomprimieren muss, um auf die angeforderten Bytes zuzugreifen. GET-Objektvorgänge, die einen kleinen Byte-Bereich von einem sehr großen Objekt anfordern, sind besonders ineffizient, beispielsweise ist es sehr ineffizient, einen Bereich von 10 MB von einem komprimierten 50-GB-Objekt zu lesen.

Wenn Bereiche von komprimierten Objekten gelesen werden, können Client-Anforderungen eine Zeitdauer haben.



Wenn Sie Objekte komprimieren müssen und Ihre Client-Applikation Bereichslesevorgänge verwenden muss, erhöhen Sie die Zeitüberschreitung beim Lesen der Anwendung.

Testen der REST API-Konfiguration von Swift

Sie können die Swift CLI verwenden, um die Verbindung zum StorageGRID System zu testen und zu überprüfen, ob Objekte gelesen und geschrieben werden können.

Bevor Sie beginnen

- Sie haben den Swift-Befehlszeilenclient heruntergeladen und installiert: "[SwiftStack: python-wiftclient](#)"
- Optional haben Sie "[Ein Load Balancer-Endpunkt wurde erstellt](#)". Andernfalls kennen Sie die IP-Adresse des zu verbindenden Storage-Node und die zu verwendende Port-Nummer. Siehe "[IP-Adressen und Ports für Client-Verbindungen](#)".
- Das ist schon "[Swift Mandantenkonto erstellt](#)".
- Sie haben sich beim Mandantenkonto angemeldet und mindestens eine Gruppe und einen Benutzer erstellt. Siehe "[Erstellen von Gruppen für einen Swift Mandanten](#)".



Swift-Mandanten-Benutzer müssen über die Administratorgruppe verfügen, um sich bei der Swift-REST-API authentifizieren zu können.

Über diese Aufgabe

Wenn Sie keine Sicherheit konfiguriert haben, müssen Sie die hinzufügen `--insecure` Flag auf jeden dieser Befehle.

Schritte

1. Fragen Sie die Info-URL für Ihre StorageGRID Swift Implementierung:

```
swift
-U <Tenant_Account_ID:Account_User_Name>
-K <User_Password>
-A https://<FQDN | IP>:<Port>/info
capabilities
```

Dies reicht aus, um zu testen, ob Ihre Swift-Implementierung funktionsfähig ist. Um die Kontenkonfiguration durch Speichern eines Objekts weiter zu testen, fahren Sie mit den zusätzlichen Schritten fort.

2. Legen Sie ein Objekt in den Container:

```
touch test_object
swift
-U <Tenant_Account_ID:Account_User_Name>
-K <User_Password>
-A https://<FQDN | IP>:<Port>/auth/v1.0
upload test_container test_object
--object-name test_object
```

3. Holen Sie sich den Container, um das Objekt zu überprüfen:

```
swift
-U <Tenant_Account_ID:Account_User_Name>
-K <User_Password>
-A https://<FQDN | IP>:<Port>/auth/v1.0
list test_container
```

4. Löschen Sie das Objekt:

```
swift
-U <Tenant_Account_ID:Account_User_Name>
-K <User_Password>
-A https://<FQDN | IP>:<Port>/auth/v1.0
delete test_container test_object
```

5. Löschen Sie den Container:

```
swift
-U `<_Tenant_Account_ID:Account_User_Name_>`
-K `<_User_Password_>`
-A `\"https://<_FQDN_ | _IP_>:<_Port_>/auth/v1.0`
delete test_container
```

Von Swift UNTERSTÜTZTE REST-API-Operationen

Das StorageGRID System unterstützt die meisten Operationen in der OpenStack Swift API. Informieren Sie sich vor der Integration von Swift REST API Clients mit StorageGRID über die Implementierungsdetails für Konto-, Container- und Objektvorgänge.

Von StorageGRID unterstützte Vorgänge

Die folgenden Swift-API-Operationen werden unterstützt:

- ["Konto-Operationen"](#)
- ["Container-Operationen"](#)
- ["Objekt-Operationen"](#)

Gemeinsame Answerheader für alle Vorgänge

Das StorageGRID-System implementiert alle gemeinsamen Header für unterstützte Vorgänge, wie sie von der OpenStack Swift Objekt-Storage-API v1 definiert wurden.

Verwandte Informationen

["OpenStack: Objekt-Storage-API"](#)

Unterstützte Swift-API-Endpunkte

StorageGRID unterstützt die folgenden Swift-API-Endpunkte: Die Info-URL, die auth-URL und die Storage-URL.

Info-URL

Sie können die Funktionen und Einschränkungen der StorageGRID-Swift-Implementierung bestimmen, indem Sie eine GET-Anfrage an die Swift-Basis-URL mit dem /info-Pfad senden.

`https://FQDN | Node IP:Swift Port/info/`

In der Anfrage:

- *FQDN* Ist der vollständig qualifizierte Domain-Name.
- *Node IP* Ist die IP-Adresse für den Storage-Node oder den Gateway-Node im StorageGRID-Netzwerk.
- *Swift Port* Ist die Portnummer, die für Swift-API-Verbindungen auf dem Storage-Node oder Gateway-Node verwendet wird.

Die folgende Info-URL würde beispielsweise Informationen von einem Storage-Node mit der IP-Adresse von 10.99.106.103 anfordern und Port 18083 verwenden.

`https://10.99.106.103:18083/info/`

Die Antwort umfasst die Funktionen der Swift-Implementierung als JSON-Wörterbuch. Ein Client-Tool kann die JSON-Antwort analysieren, um die Funktionen der Implementierung zu bestimmen und sie als Einschränkungen für nachfolgende Storage-Vorgänge zu verwenden.

Die StorageGRID-Implementierung von Swift ermöglicht nicht authentifizierten Zugriff auf die Info-URL.

Auth-URL

Ein Client kann die Swift auth URL verwenden, um sich als Benutzer eines Mandantenkontos zu authentifizieren.

`https://FQDN | Node IP:Swift Port/auth/v1.0/`

Sie müssen die Mandanten-Konto-ID, den Benutzernamen und das Passwort als Parameter in angeben `x-Auth-User` Und `x-Auth-Key` Anforderungs-Header wie folgt:

`X-Auth-User: Tenant_Account_ID:Username`

`X-Auth-Key: Password`

In den Kopfzeilen der Anfrage:

- *Tenant_Account_ID* Ist die Account-ID, die StorageGRID beim Erstellen des Swift-Mandanten zugewiesen hat. Dies ist die gleiche Mandantenkonto-ID, die auf der Anmeldeseite des Mandanten-Managers verwendet wird.
- *Username* Ist der Name eines im Mandanten-Manager erstellten Benutzers. Dieser Benutzer muss einer Gruppe angehören, die über die Swift Administrator-Berechtigung verfügt. Der Root-Benutzer des Mandanten kann nicht für die Verwendung der Swift REST API konfiguriert werden.

Wenn Identity Federation für das Mandantenkonto aktiviert ist, geben Sie den Benutzernamen und das Passwort des föderierten Benutzers vom LDAP-Server an. Geben Sie alternativ den Domänennamen des LDAP-Benutzers an. Beispiel:

`X-Auth-User: Tenant_Account_ID:Username@Domain_Name`

- *Password* Ist das Passwort für den Mandantenbenutzer. Benutzerpasswörter werden im Mandanten-Manager erstellt und gemanagt.

Als Antwort auf eine erfolgreiche Authentifizierungsanforderung werden eine Storage-URL und ein auth-Token zurückgegeben:

```
X-Storage-Url: https://FQDN | Node_IP:Swift_Port/v1/Tenant_Account_ID
```

```
X-Auth-Token: token
```

```
X-Storage-Token: token
```

Das Token ist standardmäßig für 24 Stunden ab der Erzeugung gültig.

Token werden für ein bestimmtes Mandantenkonto generiert. Ein gültiges Token für ein Konto ermächtigt einen Benutzer nicht, auf ein anderes Konto zuzugreifen.

Storage-URL

Eine Client-Applikation kann Swift-REST-API-Aufrufe ausstellen, um unterstützte Konto-, Container- und Objektvorgänge mit einem Gateway-Node oder Storage-Node durchzuführen. Storage-Anforderungen werden an die in der Authentifizierungsantwort zurückgegebene Storage-URL adressiert. Die Anforderung muss auch die Kopfzeile von X-Auth-Token und den Wert enthalten, der von der auth-Anforderung zurückgegeben wurde.

```
https://FQDN | IP:Swift_Port/v1/Tenant_Account_ID
```

```
[/container] [/object]
```

```
X-Auth-Token: token
```

Einige Kopf für Speicherantwort, die Nutzungsstatistiken enthalten, geben möglicherweise keine genauen Zahlen für kürzlich geänderte Objekte wieder. Es kann einige Minuten dauern, bis genaue Zahlen in diesen Kopfzeilen angezeigt werden.

Die folgenden Antwortkopfzeilen für Konto- und Container-Vorgänge sind Beispiele für solche, die Nutzungsstatistiken enthalten:

- X-Account-Bytes-Used
- X-Account-Object-Count
- X-Container-Bytes-Used
- X-Container-Object-Count

Verwandte Informationen

["Mandantenkonten und -Verbindungen konfigurieren"](#)

["Konto-Operationen"](#)

["Container-Operationen"](#)

["Objekt-Operationen"](#)

Konto-Operationen

Die folgenden Swift-API-Vorgänge werden bei Accounts durchgeführt.

GET Konto

Dieser Vorgang ruft die Containerliste ab, die mit den Statistiken zur Konto- und Kontonutzung verknüpft ist.

Der folgende Parameter für die Anfrage ist erforderlich:

- Account

Die folgende Anfrageüberschrift ist erforderlich:

- X-Auth-Token

Die folgenden unterstützten Abfrageparameter sind optional:

- Delimiter
- End_marker
- Format
- Limit
- Marker
- Prefix

Bei einer erfolgreichen Ausführung werden die folgenden Header mit einer Antwort „HTTP/1.1 204 No Content“ zurückgegeben, wenn das Konto gefunden wird und keine Container hat oder die Containerliste leer ist; oder eine „HTTP/1.1 200 OK“-Antwort, wenn das Konto gefunden wird und die Containerliste nicht leer ist:

- Accept-Ranges
- Content-Length
- Content-Type
- Date
- X-Account-Bytes-Used
- X-Account-Container-Count
- X-Account-Object-Count
- X-Timestamp
- X-Trans-Id

HAUPTKONTO

Mit dieser Operation werden Kontoinformationen und Statistiken von einem Swift-Konto abgerufen.

Der folgende Parameter für die Anfrage ist erforderlich:

- Account

Die folgende Anfrageüberschrift ist erforderlich:

- X-Auth-Token

Eine erfolgreiche Ausführung gibt die folgenden Kopfzeilen mit einer HTTP/1.1 204 No Content-Antwort zurück:

- Accept-Ranges
- Content-Length
- Date
- X-Account-Bytes-Used
- X-Account-Container-Count
- X-Account-Object-Count
- X-Timestamp
- X-Trans-Id

Verwandte Informationen

["In den Audit-Protokollen werden Swift-Vorgänge nachverfolgt"](#)

Container-Operationen

StorageGRID unterstützt maximal 1,000 Container pro Swift Konto. Die folgenden Swift-API-Vorgänge werden auf Containern durchgeführt.

Container LÖSCHEN

Durch diesen Vorgang wird ein leerer Container aus einem Swift-Konto in einem StorageGRID-System entfernt.

Die folgenden Anfrageparameter sind erforderlich:

- Account
- Container

Die folgende Anfrageüberschrift ist erforderlich:

- X-Auth-Token

Eine erfolgreiche Ausführung gibt die folgenden Kopfzeilen mit einer HTTP/1.1 204 No Content-Antwort zurück:

- Content-Length
- Content-Type
- Date
- X-Trans-Id

GET Container

Dieser Vorgang ruft die dem Container zugeordnete Objektliste sowie die Containerstatistiken und Metadaten in einem StorageGRID System ab.

Die folgenden Anfrageparameter sind erforderlich:

- Account
- Container

Die folgende Anfrageüberschrift ist erforderlich:

- X-Auth-Token

Die folgenden unterstützten Abfrageparameter sind optional:

- Delimiter
- End_marker
- Format
- Limit
- Marker
- Path
- Prefix

Eine erfolgreiche Ausführung liefert die folgenden Header mit einer "HTTP/1.1 200 success" oder einer "HTTP/1.1 204 No Content"-Antwort:

- Accept-Ranges
- Content-Length
- Content-Type
- Date
- X-Container-Bytes-Used
- X-Container-Object-Count
- X-Timestamp
- X-Trans-Id

KOPF Behälter

Dieser Vorgang ruft Containerstatistiken und Metadaten aus einem StorageGRID System ab.

Die folgenden Anfrageparameter sind erforderlich:

- Account
- Container

Die folgende Anfrageüberschrift ist erforderlich:

- X-Auth-Token

Eine erfolgreiche Ausführung gibt die folgenden Kopfzeilen mit einer HTTP/1.1 204 No Content-Antwort

zurück:

- Accept-Ranges
- Content-Length
- Date
- X-Container-Bytes-Used
- X-Container-Object-Count
- X-Timestamp
- X-Trans-Id

Legen Sie den Behälter

Durch diesen Vorgang wird ein Container für ein Konto in einem StorageGRID-System erstellt.

Die folgenden Anfrageparameter sind erforderlich:

- Account
- Container

Die folgende Anfrageüberschrift ist erforderlich:

- X-Auth-Token

Eine erfolgreiche Ausführung gibt die folgenden Header mit einer "HTTP/1.1 201 created" oder "HTTP/1.1 202 Accepted" (falls der Container bereits unter diesem Konto existiert) Antwort zurück:

- Content-Length
- Date
- X-Timestamp
- X-Trans-Id

Container-Name muss im StorageGRID-Namespace eindeutig sein. Wenn der Container unter einem anderen Konto vorhanden ist, wird der folgende Header zurückgegeben: „HTTP/1.1 409-Konflikt“.

Verwandte Informationen

["Monitoring und Prüfung von Vorgängen"](#)

Objekt-Operationen

Die folgenden Swift-API-Vorgänge werden an Objekten durchgeführt. Diese Vorgänge können im nachverfolgt werden ["StorageGRID Prüfprotokoll"](#).

Delete Objekt

Durch diesen Vorgang werden der Inhalt und die Metadaten eines Objekts aus dem StorageGRID System gelöscht.

Die folgenden Anfrageparameter sind erforderlich:

- Account
- Container
- Object

Die folgende Anfrageüberschrift ist erforderlich:

- X-Auth-Token

Bei einer erfolgreichen Ausführung werden die folgenden Antwortheadern mit einem zurückgegeben HTTP/1.1 204 No Content Antwort:

- Content-Length
- Content-Type
- Date
- X-Trans-Id

Bei der Verarbeitung einer LÖSCHOBJEKTANFORDERUNG versucht StorageGRID, alle Kopien des Objekts sofort von allen gespeicherten Speicherorten zu entfernen. Wenn erfolgreich, gibt StorageGRID sofort eine Antwort an den Client zurück. Wenn nicht innerhalb von 30 Sekunden alle Kopien entfernt werden können (z. B. weil ein Speicherort vorübergehend nicht verfügbar ist), stellt StorageGRID die Kopien in eine Warteschlange zur Entfernung und zeigt dann den Erfolg des Clients an.

Weitere Informationen finden Sie unter ["So werden Objekte gelöscht"](#).

GET Objekt

Dieser Vorgang ruft den Objekthinhalte ab und ruft die Objektmetadaten von einem StorageGRID System ab.

Die folgenden Anfrageparameter sind erforderlich:

- Account
- Container
- Object

Die folgende Anfrageüberschrift ist erforderlich:

- X-Auth-Token

Die folgenden Anfragezeilen sind optional:

- Accept-Encoding
- If-Match
- If-Modified-Since
- If-None-Match
- If-Unmodified-Since
- Range

Bei einer erfolgreichen Ausführung werden die folgenden Kopfzeilen mit einem zurückgegeben HTTP/1.1 200 OK Antwort:

- Accept-Ranges
- Content-Disposition, Nur wenn zurückgegeben Content-Disposition Es wurden Metadaten festgelegt
- Content-Encoding, Nur wenn zurückgegeben Content-Encoding Es wurden Metadaten festgelegt
- Content-Length
- Content-Type
- Date
- ETag
- Last-Modified
- X-Timestamp
- X-Trans-Id

HEAD-Objekt

Dieser Vorgang ruft Metadaten und Eigenschaften eines aufgenommene Objekts von einem StorageGRID System ab.

Die folgenden Anfrageparameter sind erforderlich:

- Account
- Container
- Object

Die folgende Anfrageüberschrift ist erforderlich:

- X-Auth-Token

Eine erfolgreiche Ausführung gibt die folgenden Header mit einer HTTP/1.1 200 OK-Antwort zurück:

- Accept-Ranges
- Content-Disposition, Nur wenn zurückgegeben Content-Disposition Es wurden Metadaten festgelegt
- Content-Encoding, Nur wenn zurückgegeben Content-Encoding Es wurden Metadaten festgelegt
- Content-Length
- Content-Type
- Date
- ETag
- Last-Modified
- X-Timestamp

- X-Trans-Id

PUT Objekt

Durch diesen Vorgang wird ein neues Objekt mit Daten und Metadaten erstellt oder ein vorhandenes Objekt durch Daten und Metadaten in einem StorageGRID System ersetzt.

StorageGRID unterstützt Objekte mit einer Größe von bis zu 5 tib (5,497,558,138,880 Byte).



Widersprüchliche Clientanforderungen, wie z. B. zwei Clients, die in denselben Schlüssel schreiben, werden auf der Grundlage der „neuesten Wins“ gelöst. Der Zeitpunkt für die Bewertung „neuester Erfolge“ basiert darauf, wann das StorageGRID System eine bestimmte Anfrage abschließt und nicht darauf, wann Swift-Clients einen Vorgang starten.

Die folgenden Anfrageparameter sind erforderlich:

- Account
- Container
- Object

Die folgende Anfrageüberschrift ist erforderlich:

- X-Auth-Token

Die folgenden Anfragezeilen sind optional:

- Content-Disposition
- Content-Encoding

Verwenden Sie keine Schrottbecherungen `Content-Encoding` Wenn die ILM-Regel für ein Objekt Objekte nach der Größe filtert und synchrone Platzierung bei der Aufnahme verwendet wird (die ausgewogenen oder strengen Optionen für das Aufnahmeverhalten).

- Transfer-Encoding

Verwenden Sie keine komprimierten oder chunked `Transfer-Encoding` Wenn die ILM-Regel für ein Objekt Objekte nach der Größe filtert und synchrone Platzierung bei der Aufnahme verwendet wird (die ausgewogenen oder strengen Optionen für das Aufnahmeverhalten).

- Content-Length

Wenn eine ILM-Regel Objekte nach Größe filtert und bei der Aufnahme synchrone Platzierung verwendet, müssen Sie angeben `Content-Length`.



Wenn Sie diese Richtlinien für nicht befolgen `Content-Encoding`, `Transfer-Encoding`, und `Content-Length`, StorageGRID muss das Objekt speichern, bevor es die Objektgröße bestimmen kann und die ILM-Regel anwenden kann. Das heißt, StorageGRID muss standardmäßig vorläufige Kopien eines Objekts bei der Aufnahme erstellen. Das heißt, StorageGRID muss die Dual-Commit-Option für das Ingest-Verhalten verwenden.

Weitere Informationen zur synchronen Platzierung und zu ILM-Regeln finden Sie unter

"Datensicherungsoptionen für die Aufnahme".

- Content-Type
- ETag
- X-Object-Meta-<name\> (Objektbezogene Metadaten)

Wenn Sie die Option **User Defined Creation Time** als Referenzzeit für eine ILM-Regel verwenden möchten, müssen Sie den Wert in einem benutzerdefinierten Header namens `speichern X-Object-Meta-Creation-Time`. Beispiel:

```
X-Object-Meta-Creation-Time: 1443399726
```

Dieses Feld wird seit dem 1. Januar 1970 als Sekunden ausgewertet.

- X-Storage-Class: `reduced_redundancy`

Diese Kopfzeile wirkt sich darauf aus, wie viele Objektkopien StorageGRID erstellt werden, wenn die ILM-Regel, die mit einem aufgenommenen Objekt übereinstimmt, ein Aufnahmeverhalten der Dual-Commit oder Balance angibt.

- **Dual Commit:** Wenn die ILM-Regel die Dual Commit-Option für das Aufnahmeverhalten angibt, erstellt StorageGRID bei Aufnahme des Objekts eine einzelne Interimskopie (Single Commit).
- **Ausgeglichen:** Wenn die ILM-Regel die Option ausgeglichen angibt, erstellt StorageGRID nur eine Zwischenkopie, wenn das System nicht sofort alle in der Regel angegebenen Kopien erstellen kann. Wenn StorageGRID eine synchrone Platzierung durchführen kann, hat diese Kopfzeile keine Auswirkung.

Der `reduced_redundancy` Kopfzeile eignet sich am besten, wenn die ILM-Regel, die dem Objekt entspricht, eine einzige replizierte Kopie erstellt. In diesem Fall verwenden `reduced_redundancy` Eine zusätzliche Objektkopie kann bei jedem Aufnahmeverfahren nicht mehr erstellt und gelöscht werden.

Verwenden der `reduced_redundancy` Header wird unter anderen Umständen nicht empfohlen, da dies das Risiko für den Verlust von Objektdaten während der Aufnahme erhöht. Beispielsweise können Sie Daten verlieren, wenn die einzelne Kopie zunächst auf einem Storage Node gespeichert wird, der ausfällt, bevor eine ILM-Evaluierung erfolgen kann.



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

Beachten Sie, dass Sie angeben `reduced_redundancy` Wirkt sich nur darauf aus, wie viele Kopien erstellt werden, wenn ein Objekt zum ersten Mal aufgenommen wird. Es hat keine Auswirkungen darauf, wie viele Kopien des Objekts erstellt werden, wenn das Objekt durch die aktiven ILM-Richtlinien evaluiert wird. Außerdem werden Daten nicht mit niedrigerer Redundanz im StorageGRID System gespeichert.

Eine erfolgreiche Ausführung gibt die folgenden Header mit einer "HTTP/1.1 201 created"-Antwort zurück:

- Content-Length
- Content-Type
- Date
- ETag
- Last-Modified
- X-Trans-Id

OPTIONEN anfordern

Die OPTIONEN Request überprüft die Verfügbarkeit eines einzelnen Swift Service. Die OPTIONSANFORDERUNG wird vom in der URL angegebenen Speicherknoten oder Gateway-Node verarbeitet.

OPTIONEN

Client-Anwendungen können zum Beispiel eine OPTIONSANFORDERUNG an den Swift-Port auf einem Storage Node stellen, ohne Swift-Authentifizierungsdaten bereitzustellen, um zu ermitteln, ob der Storage-Node verfügbar ist. Sie können diese Anforderung zum Monitoring verwenden oder um externen Lastausgleich zu ermöglichen, wenn ein Storage-Node ausfällt.

Bei Verwendung mit der Info-URL oder der Speicher-URL gibt die OPTIONSMETHODE eine Liste der unterstützten Verben für die angegebene URL zurück (z. B. KOPF, GET, OPTIONEN und PUT). Die OPTIONSMETHODE kann nicht mit der AuthentifizURL verwendet werden.

Der folgende Parameter für die Anfrage ist erforderlich:

- Account

Die folgenden Anfrageparameter sind optional:

- Container
- Object

Bei einer erfolgreichen Ausführung werden die folgenden Header mit der Antwort „HTTP/1.1 204 No Content“ zurückgegeben. Für die ANFORDERUNG VON OPTIONEN an die Speicher-URL ist nicht erforderlich, dass das Ziel vorhanden ist.

- Allow (Eine Liste der unterstützten Verben für die angegebene URL, z. B. „KOPF“, „ABRUFEN“, „OPTIONEN“, Und PUT)
- Content-Length
- Content-Type
- Date
- X-Trans-Id

Verwandte Informationen

["Unterstützte Swift-API-Endpunkte"](#)

Fehlerantworten bei Swift-API-Operationen

Das Verständnis möglicher Fehlerantworten kann Ihnen bei der Fehlerbehebung helfen.

Wenn während eines Vorgangs Fehler auftreten, werden möglicherweise die folgenden HTTP-Statuscodes zurückgegeben:

Swift-Fehlername	HTTP-Status
AccountNameTooLong, ContainerNameTooLong, HeaderTooBig, InvalidContainerName, InvalidRequest, InvalidURI, MetadataNameTooLong, MetadaValueTooBig, MissingSecurityHeader, ObjectNameTooLong, TooManyContainers, TooManyMetadataltems, TotalMetadaTooLarge	400 Fehlerhafte Anfrage
AccessDenied	403 Verbotene
ContainerNotEmpty, ContainerAlreadyExists	409 Konflikt
Interner Fehler	500 Fehler Des Internen Servers
InvalidRange	416 Angeforderter Bereich Nicht Zu Unterprüfbar
MethodenAlled	405 Methode Nicht Zulässig
MissingContentLänge	411 Länge Erforderlich
Nicht gefunden	404 Nicht Gefunden
NotImplemsted	501 Nicht Implementiert
Vorbedingungen nicht möglich	412 Voraussetzung Fehlgeschlagen
ResourceNotFound	404 Nicht Gefunden
Nicht Autorisiert	401 Nicht Autorisiert
Nicht verarbeitbarEntity	422 Nicht Verarbeitbare Einheit

StorageGRID Swift REST-API-Operationen

Speziell für das StorageGRID System wurden Vorgänge zur Swift REST API hinzugefügt.

ABRUFEN der Container-Konsistenzanforderung

"**Konsistenzwerte**" Sorgen Sie für ein Gleichgewicht zwischen der Verfügbarkeit der Objekte und der Konsistenz dieser Objekte über verschiedene Storage-Nodes und Standorte hinweg. Mit der GET-Container-

Konsistenzanforderung können Sie die Konsistenz bestimmen, die auf einen bestimmten Container angewendet wird.

Anfrage

HTTP-Header anfordern	Beschreibung
X-Auth-Token	Gibt das Swift-Authentifizierungs-Token für das Konto an, das für die Anforderung verwendet werden soll.
X-ntap-sg-Konsistenz	Gibt den Anforderungstyp an, wobei <code>true</code> = GET Containerkonsistenz, und <code>false</code> = get Container.
Host	Der Hostname, auf den die Anforderung gerichtet ist.

Anforderungsbeispiel

```
GET /v1/28544923908243208806/Swift container
X-Auth-Token: SGRD_3a877009a2d24cb1801587bfa9050f29
x-ntap-sg-consistency: true
Host: test.com
```

Antwort

HTTP-Kopfzeile für Antwort	Beschreibung
Datum	Datum und Uhrzeit der Antwort.
Verbindung	Ob die Verbindung zum Server offen oder geschlossen ist.
X-Trans-ID	Die eindeutige Transaktions-ID für die Anforderung.
Inhaltslänge	Die Länge des Reaktionskörpers.

HTTP-Kopfzeile für Antwort	Beschreibung
X-ntap-sg-Konsistenz	<p>Die Konsistenz, die auf den Container angewendet wird. Folgende Werte werden unterstützt:</p> <p>All: Alle Knoten erhalten die Daten sofort, oder die Anfrage schlägt fehl.</p> <p>Strong-global: Garantiert Lese-nach-Schreiben-Konsistenz für alle Client-Anfragen über alle Standorte hinweg.</p> <p>Strong-site: Garantiert Lese-nach-Schreiben Konsistenz für alle Client-Anfragen innerhalb einer Site.</p> <p>Read-after-New-write: (Standard) bietet Read-after-write-Konsistenz für neue Objekte und eventuelle Konsistenz für Objektaktualisierungen. Hochverfügbarkeit und garantierte Datensicherung Empfohlen für die meisten Fälle.</p> <p>Verfügbar: Bietet eventuelle Konsistenz für neue Objekte und Objekt-Updates. Verwenden Sie für S3-Buckets nur nach Bedarf (z. B. für einen Bucket mit Protokollwerten, die nur selten gelesen werden, oder für HEAD- oder GET-Vorgänge für nicht vorhandene Schlüssel). Nicht unterstützt für S3 FabricPool-Buckets.</p>

Antwortbeispiel

```
HTTP/1.1 204 No Content
Date: Sat, 29 Nov 2015 01:02:18 GMT
Connection: CLOSE
X-Trans-Id: 1936575373
Content-Length: 0
x-ntap-sg-consistency: strong-site
```

PUT Container-Konsistenzanforderung

Mit der Konsistenzanforderung für PUT-Container können Sie die Konsistenz angeben, die auf Vorgänge angewendet werden soll, die auf einen Container ausgeführt werden. Standardmäßig werden neue Container mit der Konsistenz „Read-after-New-write“ erstellt.

Anfrage

HTTP-Header anfordern	Beschreibung
X-Auth-Token	Swift Authentifizierungs-Token für das Konto zur Verwendung für die Anforderung.

HTTP-Header anfordern	Beschreibung
X-ntap-sg-Konsistenz	<p>Die Konsistenz, die auf Vorgänge auf dem Container angewendet werden soll. Folgende Werte werden unterstützt:</p> <p>All: Alle Knoten erhalten die Daten sofort, oder die Anfrage schlägt fehl.</p> <p>Strong-global: Garantiert Lese-nach-Schreiben-Konsistenz für alle Client-Anfragen über alle Standorte hinweg.</p> <p>Strong-site: Garantiert Lese-nach-Schreiben Konsistenz für alle Client-Anfragen innerhalb einer Site.</p> <p>Read-after-New-write: (Standard) bietet Read-after-write-Konsistenz für neue Objekte und eventuelle Konsistenz für Objektaktualisierungen. Hochverfügbarkeit und garantierte Datensicherung Empfohlen für die meisten Fälle.</p> <p>Verfügbar: Bietet eventuelle Konsistenz für neue Objekte und Objekt-Updates. Verwenden Sie für S3-Buckets nur nach Bedarf (z. B. für einen Bucket mit Protokollwerten, die nur selten gelesen werden, oder für HEAD- oder GET-Vorgänge für nicht vorhandene Schlüssel). Nicht unterstützt für S3 FabricPool-Buckets.</p>
Host	Der Hostname, auf den die Anforderung gerichtet ist.

Zusammenspiel von Konsistenz- und ILM-Regeln zur Beeinträchtigung der Datensicherung

Beide Ihre Wahl "**Konsistenzwert**" Ihre ILM-Regel wirkt sich darüber hinaus auf den Schutz von Objekten aus. Diese Einstellungen können interagieren.

Die beim Speichern eines Objekts verwendete Konsistenz wirkt sich beispielsweise auf die anfängliche Platzierung von Objekt-Metadaten aus, während der "**Aufnahmeverhalten**" Die für die ILM-Regel ausgewählt wurde, wirkt sich auf die anfängliche Platzierung von Objektkopien aus. StorageGRID benötigt zur Erfüllung von Clientanfragen Zugriff auf die Metadaten und die Daten eines Objekts. Durch die Auswahl einer passenden Sicherungsstufe für die Konsistenz und das Aufnahmeverhalten können die Daten am Anfang besser gesichert und Systemantworten besser vorhersehbar sein.

Beispiel für die Interaktion von Konsistenz- und ILM-Regeln

Angenommen, Sie haben ein Grid mit zwei Standorten mit der folgenden ILM-Regel und folgender Konsistenz:

- **ILM-Regel:** Erstellen Sie zwei Objektkopien, eine am lokalen Standort und eine an einem entfernten Standort. Das strikte Aufnahmeverhalten wird ausgewählt.
- **: "Strong-global" (Objektmetadaten werden sofort an alle Standorte verteilt.)

Wenn ein Client ein Objekt im Grid speichert, erstellt StorageGRID sowohl Objektkopien als auch verteilt Metadaten an beiden Standorten, bevor der Kunde zum Erfolg zurückkehrt.

Das Objekt ist zum Zeitpunkt der Aufnahme der Nachricht vollständig gegen Verlust geschützt. Wenn beispielsweise der lokale Standort kurz nach der Aufnahme verloren geht, befinden sich Kopien der Objektdaten und der Objektmetadaten am Remote-Standort weiterhin. Das Objekt kann vollständig abgerufen werden.

Wenn Sie stattdessen dieselbe ILM-Regel und die Konsistenz von „starken Standorten“ verwenden, erhält der Client möglicherweise eine Erfolgsmeldung, nachdem die Objektdaten am Remote-Standort repliziert wurden, aber bevor die Objektmetadaten dort verteilt werden. In diesem Fall entspricht die Sicherung von Objektmetadaten nicht dem Schutzniveau für Objektdaten. Falls der lokale Standort kurz nach der Aufnahme verloren geht, gehen Objektmetadaten verloren. Das Objekt kann nicht abgerufen werden.

Die Beziehung zwischen Konsistenz- und ILM-Regeln kann komplex sein. Wenden Sie sich an NetApp, wenn Sie Hilfe benötigen.

Anforderungsbeispiel

```
PUT /v1/28544923908243208806/_Swift_container_  
X-Auth-Token: SGRD_3a877009a2d24cb1801587bfa9050f29  
x-ntap-sg-consistency: strong-site  
Host: test.com
```

Antwort

HTTP-Kopfzeile für Antwort	Beschreibung
Date	Datum und Uhrzeit der Antwort.
Connection	Ob die Verbindung zum Server offen oder geschlossen ist.
X-Trans-Id	Die eindeutige Transaktions-ID für die Anforderung.
Content-Length	Die Länge des Reaktionskörpers.

Antwortbeispiel

```
HTTP/1.1 204 No Content  
Date: Sat, 29 Nov 2015 01:02:18 GMT  
Connection: CLOSE  
X-Trans-Id: 1936575373  
Content-Length: 0
```

In den Audit-Protokollen werden Swift-Vorgänge nachverfolgt

Alle erfolgreichen Vorgänge zum LÖSCHEN, ABRUFEN, NACHFÜHREN, POSTEN und PUT werden im StorageGRID Audit-Protokoll verfolgt. Fehler und Info-, auth- oder OPTIONS-Anforderungen werden nicht protokolliert.

Konto-Operationen

- ["GET Konto"](#)

- "HAUPTKONTO"

Container-Operationen

- "Container LÖSCHEN"
- "GET Container"
- "KOPF Behälter"
- "Legen Sie den Behälter"

Objekt-Operationen

- "Delete Objekt"
- "GET Objekt"
- "HEAD-Objekt"
- "PUT Objekt"

Verwandte Informationen

- "Zugriff auf die Audit-Log-Datei"
- "Audit-Meldungen des Clients schreiben"
- "Client liest Audit-Meldungen"

Copyright-Informationen

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

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

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

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

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

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

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

Markeninformationen

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