Verwenden Sie StorageGRID

StorageGRID software

NetApp
February 12, 2026

Inhalt

Nutzung von StorageGRID Mandanten und Clients

Verwenden Sie ein Mandantenkonto

Verwenden Sie ein Mandantenkonto

Ein Mandantenkonto ermöglicht Ihnen die Verwendung der S3-REST-API (Simple Storage Service) zum Speichern und Abrufen von Objekten in einem StorageGRID System.

Was ist ein Mandantenkonto?

Jedes Mandantenkonto verfügt über eigene föderierte oder lokale Gruppen, Benutzer, S3 Buckets 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-Clientprotokoll verwenden, können Sie auch S3-Buckets und Bucket-Richtlinien verwenden, um Objekte zwischen den Abteilungen in einem Unternehmen zu trennen. Sie müssen keine separaten Mieterkonten erstellen. Siehe Anweisungen zur Implementierung"S3-Buckets und Bucket-Richtlinien" für 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 Mandantenname, Client-Typ (S3) und optionalem Storage-Kontingent.
- Berechtigungen für das Mandantenkonto, z. B. ob das Mandantenkonto S3-Plattformservices 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-Objektsperreneinstellung 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"können Sie 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

Obwohl Sie S3-Buckets mit dem Tenant Manager erstellen und managen können, müssen Sie ein oder "S3-Konsole"verwenden, "S3-Client"um Objekte aufzunehmen und zu managen.

So melden Sie sich an und melden sich ab

Melden Sie sich bei Tenant Manager an

Sie greifen auf den Tenant Manager zu, indem Sie die URL für den Tenant in die Adressleiste eines 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 einen "Unterstützter Webbrowser".
- Cookies sind in Ihrem Webbrowser aktiviert.
- Sie gehören zu einer Benutzergruppe mit "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**.
   - Die Anmeldeseite des Tenant Managers. Das Feld **Konto** ist möglicherweise bereits ausgefüllt.
     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 Ihrer Organisation.

     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.

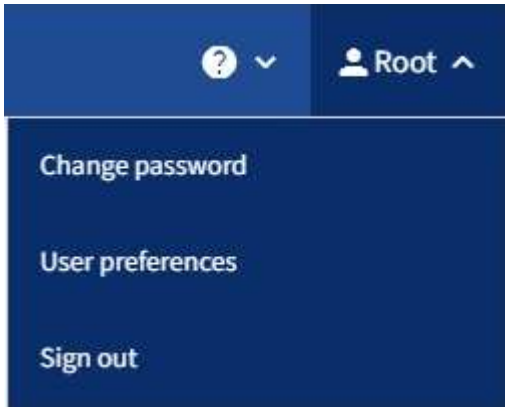
Melden Sie sich von Tenant Manager ab

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.

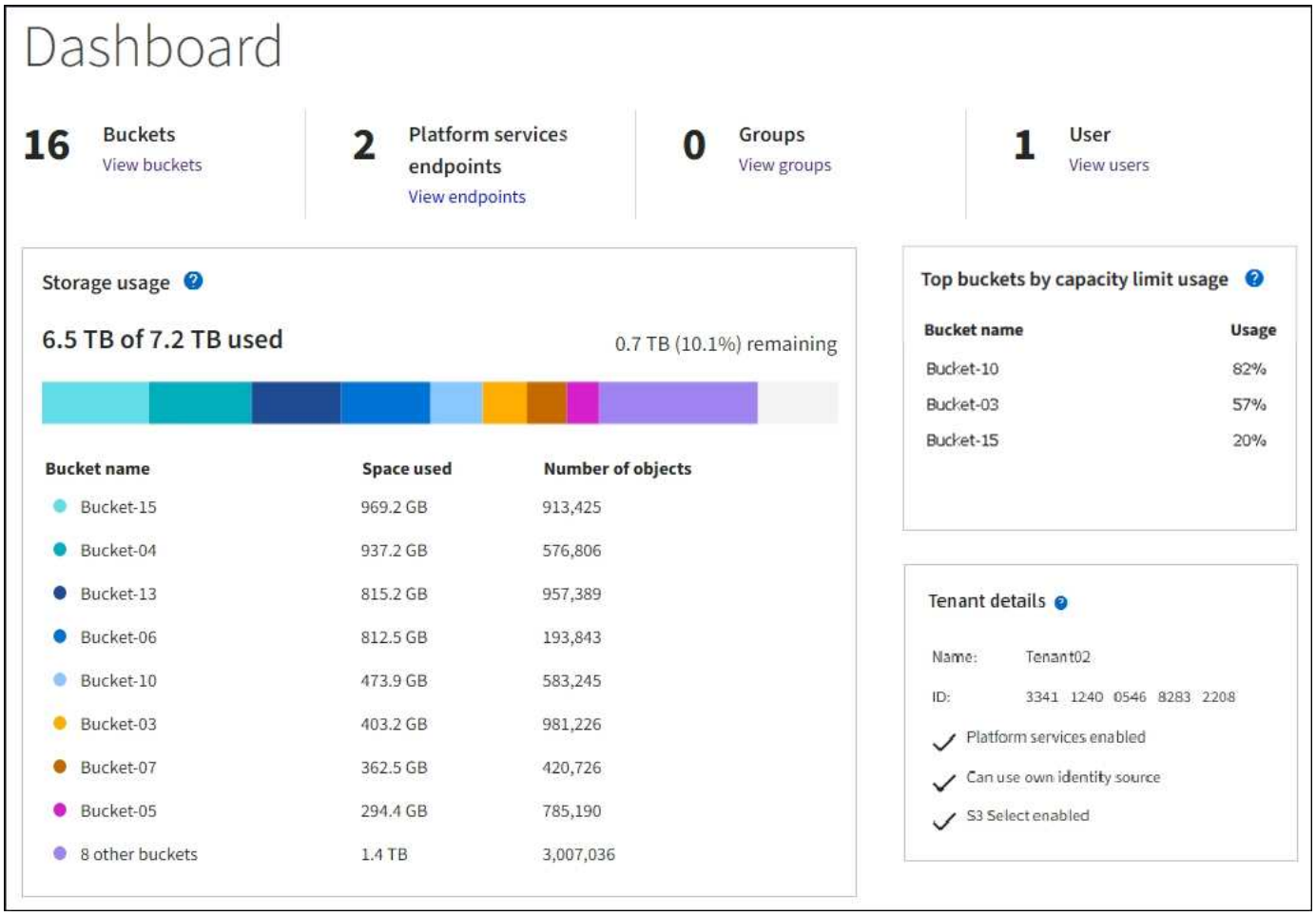
     Wenn SSO aktiviert ist und Sie sich auch beim Grid Manager angemeldet haben, müssen Sie sich auch vom Grid Manager abmelden, um sich von SSO abzumelden.

Mandantenmanager-Dashboard verstehen

Das Tenant Manager-Dashboard bietet einen Überblick über die Konfiguration eines Tenant-Kontos und die Menge an Speicherplatz, die von Objekten in den S3-Buckets des Tenant verwendet wird. Wenn der Mandant über ein Kontingent verfügt, zeigt das Dashboard an, wie viel des Kontingents genutzt wird und wie viel noch übrig ist. Wenn Fehler im Zusammenhang mit dem Mieterkonto auftreten, werden diese auf dem Dashboard angezeigt.

Die logische Größe aller Objekte, die zu diesem Mandanten gehören, umfasst unvollständige und laufende mehrteilige Uploads. Die Größe umfasst nicht den zusätzlichen physischen Speicherplatz, der für ILM-Richtlinien verwendet wird. Bei den Werten für den belegten Speicherplatz handelt es sich um Schätzungen. Diese Schätzungen werden durch den Zeitpunkt der Aufnahme, die Netzwerkkonnektivität und den Knotenstatus beeinflusst.

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



Informationen zum Mandantenkonto

Oben im Dashboard wird die Anzahl der konfigurierten Buckets oder Container, Gruppen und Benutzer angezeigt. Es zeigt auch die Anzahl der Endpunkte der Plattformdienste an, sofern diese konfiguriert wurden. Wählen Sie die Links aus, um die Details anzuzeigen.

Je nachdem"Berechtigungen für Mandantenmanagement", welche Optionen Sie konfiguriert haben und welche haben, werden im verbleibenden Dashboard verschiedene Kombinationen von Richtlinien, Storage-Nutzung, Objektinformationen und Angaben zu Mandanten angezeigt.

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 die Quota-Nutzungswarnungen aktiviert wurden, werden diese Warnmeldungen im Tenant Manager angezeigt, wenn die Quota niedrig oder überschritten ist, wie folgt:

- Wenn 90% oder mehr der Quote eines Mandanten verwendet wurden, wird die Meldung **Tenant Quotenverbrauch hoch** ausgelöst.

  Bitten Sie eventuell Ihren Grid-Administrator, die Quote zu erhöhen.

- Wenn Sie Ihre Quote überschreiten, erhalten Sie eine Benachrichtigung, dass Sie keine neuen Objekte hochladen können.

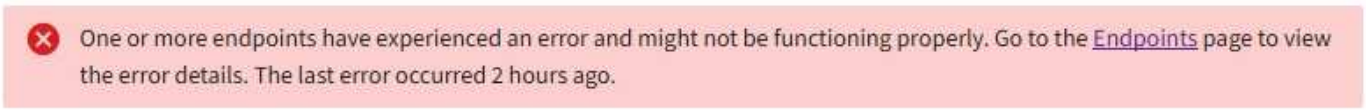
Kapazitätslimit für die Nutzung

Wenn Sie ein Kapazitätslimit für Ihre Buckets festgelegt haben, wird im Dashboard von Tenant Manager eine Liste der wichtigsten Buckets nach Kapazitätslimit angezeigt.

Wenn für einen Bucket keine Begrenzung festgelegt ist, ist seine Kapazität unbegrenzt. Wenn Ihr Mandantenkonto jedoch ein Storage-Gesamtkontingent hat und dieses Kontingent erreicht ist, können Sie unabhängig vom verbleibenden Kapazitätslimit eines Buckets nicht mehr Objekte aufnehmen.

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.



Um Details zu sehen"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-Vorgänge

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 Mandanten-Anmeldung geben Sie einen Benutzernamen, ein Passwort und eine accountId im JSON-Textkörper der Authentifizierungsanforderung (d. h. `POST /api/v3/authorize`) an. 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".

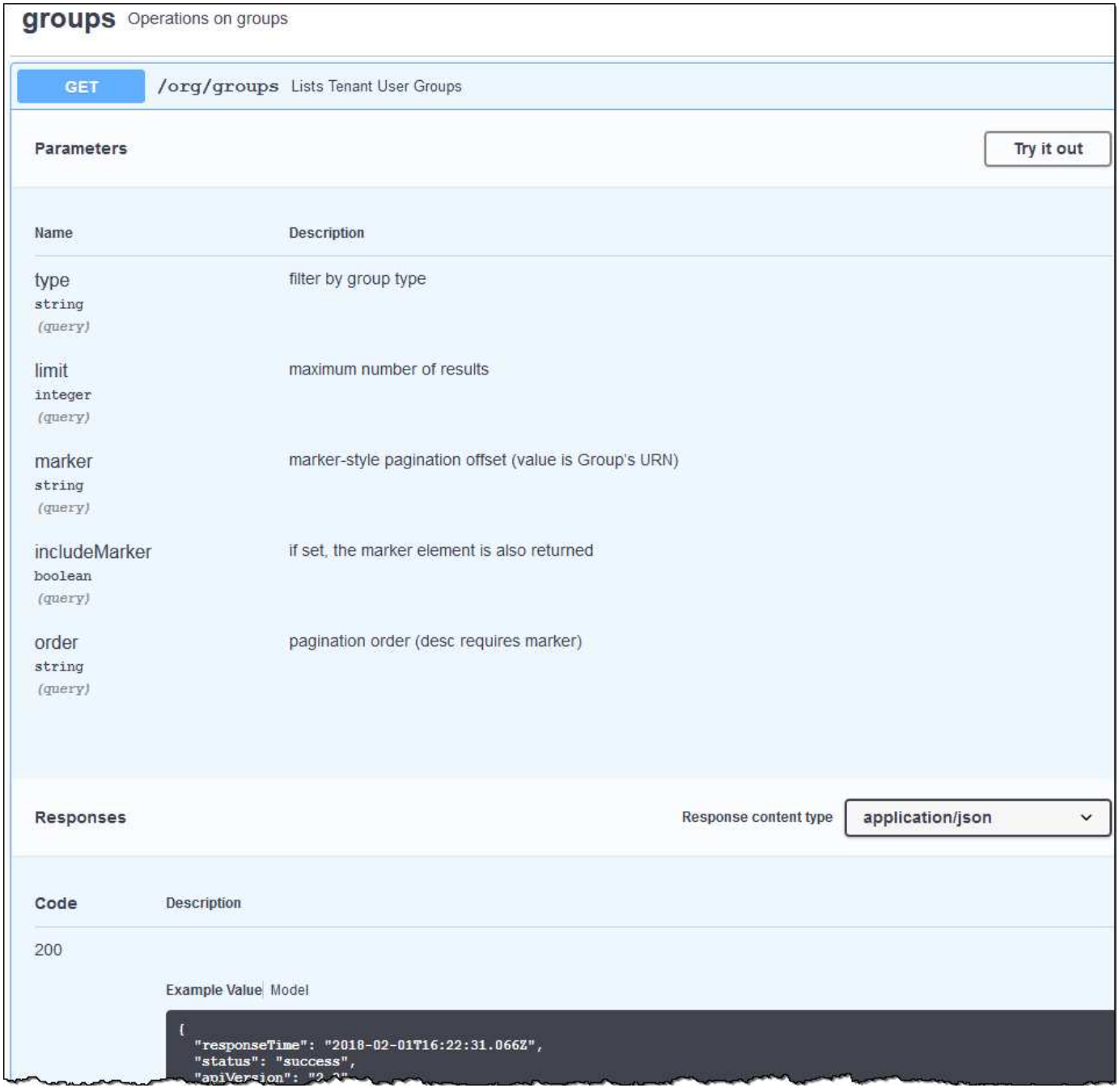
  > Wenn Single Sign-On (SSO) für das StorageGRID-System aktiviert ist, müssen Sie zur Authentifizierung verschiedene Schritte durchführen. Siehe "Anweisungen zur Verwendung der Grid Management API".

- **Config**: Operationen im Zusammenhang mit der Produktversion und den Versionen der Mandanten-Management-API. Sie können die Produktversion und die Hauptversionen der von dieser Version unterstützten API auflisten.
- **Container**: Vorgänge auf S3-Buckets.
- **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.



API-Anforderungen ausgeben

Alle API-Operationen, die Sie mit der API-Dokumentations-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. Weitere Informationen finden Sie im Abschnitt **config** der Dokumentation zur Swagger API"Grid Management API". 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, um eine Liste der unterstützten API-Hauptversionen zurückzugeben. 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 mit einem PATH-Parameter (`Api-Version: 4`)(`/api/v4` oder einem Header) angeben. 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 angemelten 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, setzen Sie den `csrfToken` Parameter während der Authentifizierung auf `true`. Der Standardwert ist `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, wird ein `GridCsrfToken` Cookie mit einem zufälligen Wert für die Anmeldung beim Grid Manager gesetzt, und das `AccountCsrfToken` Cookie wird mit einem zufälligen Wert für die Anmeldung beim 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:

- Die `X-Csrf-Token` Kopfzeile mit dem Wert der Kopfzeile auf den Wert des CSRF-Token-Cookies gesetzt.
- Für Endpunkte, die einen formularkodierten Körper akzeptieren: Einen `csrfToken` formularkodierten Anforderungskörper-Parameter.

Um den CSRF-Schutz zu konfigurieren, verwenden Sie "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

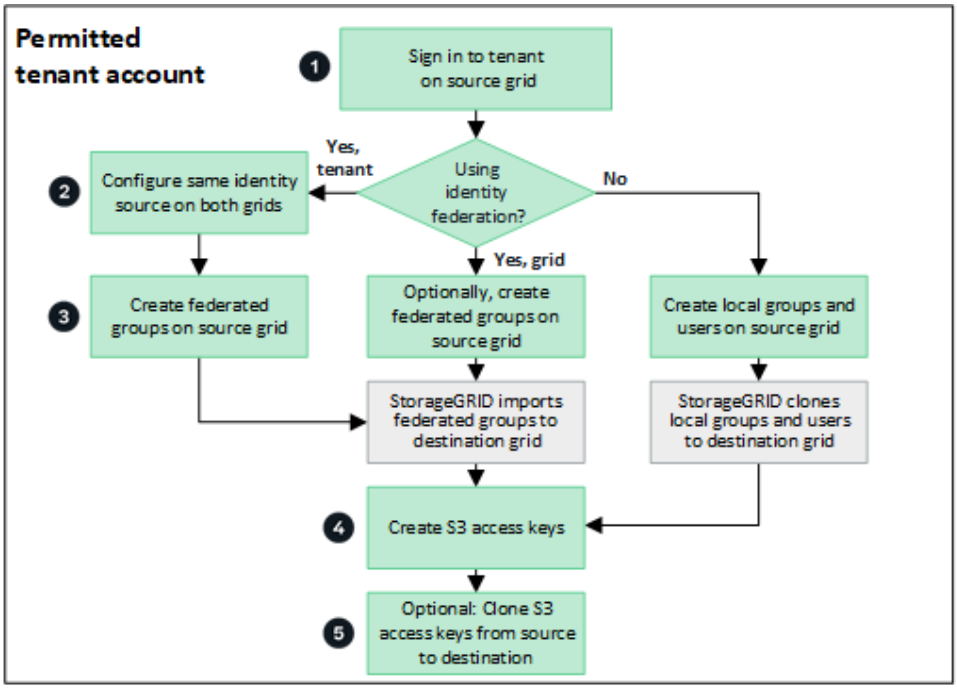
Wenn ein Mandant zur Verwendung einer Grid-Verbundverbindung erstellt oder bearbeitet wurde, wird dieser Mandant von einem StorageGRID System (dem Quellmandanten) auf ein anderes StorageGRID System (dem Replikatmandanten) repliziert. Nach der Replizierung des Mandanten werden alle Gruppen und Benutzer, 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 Mandanten-Kontoinformationen ist für Bucket-Objekte erforderlich"Grid-übergreifende Replizierung". 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:

Melden Sie sich beim Mandanten an

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

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".

Erstellen Sie Gruppen und Benutzer

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

- Wenn die Identity Federation für das gesamte StorageGRID System oder für Ihr Mandantenkonto konfiguriert wurde"Erstellen neuer Mandantengruppen", importieren Sie gebündelte Gruppen von der Identitätsquelle.
- Wenn Sie keine Identitätsföderation verwenden,"Erstellen Sie neue lokale Gruppen" und dann"Erstellen

Sie lokale Benutzer" .

4 **Erstellen von S3 Zugriffsschlüsseln**

Sie können "Erstellen Sie Ihre eigenen Zugriffsschlüssel" oder bis "Erstellen Sie die Zugriffsschlüssel eines anderen Benutzers"entweder im Quell- oder im Zielraster auf Buckets in diesem Raster zugreifen.

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, klont 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 Quell-Grid erstellen, klont StorageGRID diesen Benutzer automatisch in das Ziel-Grid. Sowohl der ursprüngliche Benutzer als auch sein Klon haben denselben vollständigen Namen, Benutzernamen und dieselbe Einstellung für **Zugriff verweigern**. Beide Benutzer gehören außerdem denselben Gruppen an. Anweisungen hierzu finden Sie unter"Benutzer managen" .

Aus Sicherheitsgründen werden lokale Benutzerkennwörter nicht in das Zielraster geklont. Wenn ein lokaler Benutzer auf den Mandantenmanager im Zielraster zugreifen muss, muss der Root-Benutzer für das Mandantenkonto ein Kennwort für diesen Benutzer im Zielraster hinzufügen. Anweisungen hierzu finden Sie unter"Benutzer managen" .

Im Quellraster erstellte Verbundgruppen werden geklont

Wenn die Anforderungen für die Verwendung des Kontoklons mit "Single Sign On"erfüllt sind und "Identitätsföderation"erfüllt wurden, werden föderierte 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 klont 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 Mandanten-Manager-API für die manuelle Eingabe in das Zielraster verwenden"Schlüssel klonen".

> 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 im Tenant Manager im Quellraster des Mandanten mit einem angemeldet"Unterstützter Webbrowser".

- Sie gehören zu einer Benutzergruppe mit dem "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. Verwenden des Tenant Manager auf dem Quellraster, "Erstellen Sie Ihre eigenen Zugriffsschlüssel" und laden Sie die Datei herunter `.csv`.
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.

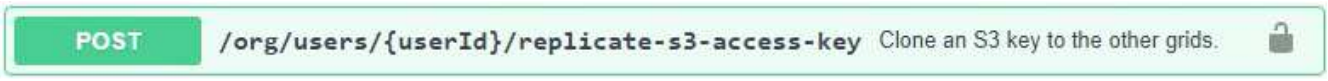
Schritte

1. Verwenden des Tenant Manager auf dem Quellraster, "Erstellen Sie die S3-Zugriffsschlüssel des anderen Benutzers" und laden Sie die Datei herunter `.csv`.
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.

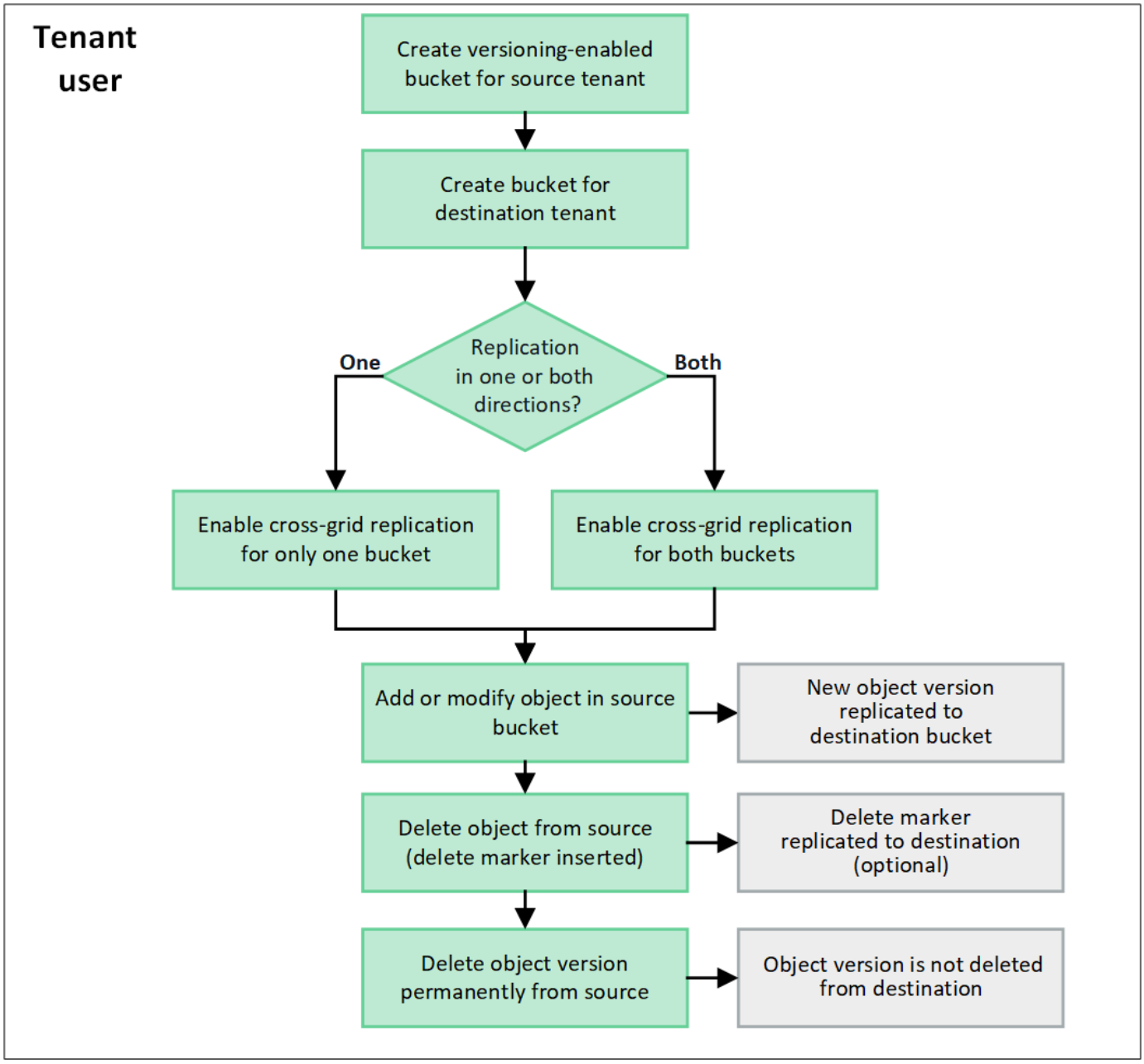
Grid-übergreifende Replizierung managen

Wenn Ihrem Mandantenkonto bei der Erstellung die Berechtigung **Grid Federation connection** verwenden 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 zum Konfigurieren der Cross-Grid-Replikation zwischen Buckets auf zwei Grids ausführen. Diese Schritte werden unterhalb des Diagramms ausführlicher beschrieben.



Konfiguration der Grid-übergreifenden Replizierung

Bevor Sie die Cross-Grid-Replikation verwenden können, müssen Sie sich bei den entsprechenden Mandantenkonten auf jedem Grid anmelden und zwei Buckets erstellen. Anschließend können Sie die Cross-Grid-Replikation für einen oder beide Buckets aktivieren.

Bevor Sie beginnen

- Sie haben die Anforderungen für die Cross-Grid-Replikation überprüft. Weitere Informationen finden Sie unter "Was ist Grid-übergreifende Replizierung" .
- Sie verwenden ein"Unterstützter Webbrowser" .
- Das Mandantenkonto verfügt über die Berechtigung **Grid-Föderationsverbindung verwenden** und auf beiden Grids sind identische Mandantenkonten vorhanden. Weitere Informationen finden Sie unter "Verwalten Sie die zulässigen Mandanten für die Grid Federation-Verbindung" .
- Der Mandantenbenutzer, als der Sie sich anmelden, ist bereits in beiden Rastern vorhanden und gehört zu einer Benutzergruppe mit der"Root-Zugriffsberechtigung" .
- Wenn Sie sich als lokaler Benutzer beim Zielraster des Mandanten anmelden, hat der Root-Benutzer für das Mandantenkonto ein Kennwort für Ihr Benutzerkonto in diesem Raster festgelegt.

Erstellen Sie zwei Buckets

Melden Sie sich als ersten Schritt bei den entsprechenden Mandantenkonten in jedem Raster an und erstellen Sie in jedem Raster einen Bucket.

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 beim Zielraster des Mandanten anmelden können, vergewissern Sie sich, dass der Root-Benutzer des Mandantenkontos ein Kennwort für Ihr Benutzerkonto festgelegt hat.

   b. Folgen Sie den Anweisungen zu "Erstellen eines S3-Buckets".

      Die Bucket-Namen und Regionen können in jedem Raster unterschiedlich sein.

   c. Wählen Sie auf der Registerkarte **Objekteinstellungen verwalten Objektversionierung aktivieren**.
   d. Wenn S3 Object Lock für Ihr StorageGRID System aktiviert ist, lesen Sie"Cross-Grid-Replikation mit S3 Object Lock" .
   e. Wählen Sie **Eimer erstellen**.
   f. Wählen Sie **Fertig**.
2. Wiederholen Sie diese Schritte, um einen Bucket für dasselbe Mandantenkonto im anderen Grid in der Grid-Föderationsverbindung 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. Ausgehend von einem Raster, dessen Objekte Sie replizieren möchten, aktivieren Sie"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**: Dem Quell-Bucket wird eine Löschmarkierung hinzugefügt, die jedoch nicht in den Ziel-Bucket repliziert wird.

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

Siehe"Was ist Grid-übergreifende Replizierung" für 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 erscheint eine Erfolgsmeldung. Zu diesem Bucket hinzugefügte Objekte werden jetzt automatisch in das andere Raster repliziert. **Cross-Grid-Replikation** wird auf der Bucket-Detailseite als aktivierte Funktion angezeigt.

2. Gehen Sie optional zum entsprechenden Bucket auf dem anderen Grid 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 zu einer Benutzergruppe mit dem "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 Ordnung ist, wird ein Erfolgsbanner angezeigt. Andernfalls wird eine Fehlermeldung angezeigt, die Sie und der Grid-Administrator zur Lösung des Problems verwenden können. Weitere Einzelheiten 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 das Deaktivieren der Cross-Grid-Replikation werden keine Objekte entfernt, die bereits zwischen Grids kopiert wurden. Beispielsweise können Objekte in `my-bucket` auf Grid 1, die kopiert wurden nach `my-bucket` auf Grid 2 werden nicht entfernt, wenn Sie die Cross-Grid-Replikation für diesen Bucket deaktivieren. Wenn Sie diese Objekte löschen möchten, müssen Sie sie manuell entfernen.
- Wenn die Grid-übergreifende Replizierung für jeden Buckets aktiviert wurde (d. h. wenn die Replikation in beide Richtungen erfolgt), können Sie die Grid-übergreifende Replizierung für einen oder beide Buckets deaktivieren. So können Sie beispielsweise die Replikation von Objekten von in Raster 1 nach in `my-bucket` Raster 2 deaktivieren `my-bucket`, während Sie weiterhin Objekte von in Raster 2 nach in Raster `my-bucket` 1 replizieren `my-bucket`.
- Sie müssen die Cross-Grid-Replikation deaktivieren, bevor Sie einem Mandanten die Berechtigung zur Verwendung der Grid-Föderationsverbindung entziehen können. Weitere Informationen finden Sie unter "Management zulässiger Mandanten" .
- Wenn Sie die Cross-Grid-Replikation für einen Bucket deaktivieren, der Objekte enthält, können Sie die Cross-Grid-Replikation nicht wieder aktivieren, es sei denn, Sie löschen alle Objekte sowohl aus dem Quell- als auch aus dem Ziel-Bucket.

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

Bevor Sie beginnen

- Sie verwenden ein"Unterstützter Webbrowser" .
- Sie gehören zu einer Benutzergruppe mit dem "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 Cross-Grid-Replikation für diesen Bucket deaktivieren möchten, geben Sie **Ja** in das Textfeld ein und wählen Sie **Deaktivieren** 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 beim Tenant Manager mit einem angemeldet"Unterstützter Webbrowser".
- Sie gehören zu einer Benutzergruppe mit dem "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.

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 darüber, 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 die Identitätsföderation für den Tenant Manager konfigurieren, wenn Sie möchten, dass Tenantgruppen und Benutzer in einem anderen System wie Active Directory, Microsoft Entra ID, OpenLDAP oder Oracle Directory Server verwaltet werden.

Bevor Sie beginnen

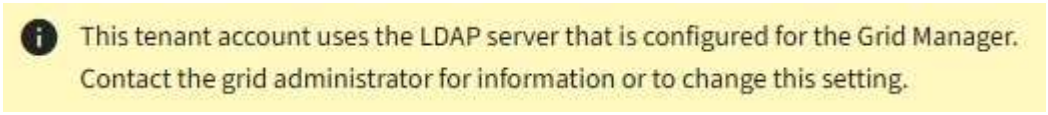
- Sie sind beim Tenant Manager angemeldet mit einem"Unterstützter Webbrowser" .
- Sie gehören zu einer Benutzergruppe mit dem "Root-Zugriffsberechtigung".
- Sie verwenden Active Directory, Microsoft Entra ID, OpenLDAP oder Oracle Directory Server als Identitätsanbieter.

  Wenn Sie einen LDAP v3-Dienst verwenden möchten, der nicht aufgeführt ist, 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.



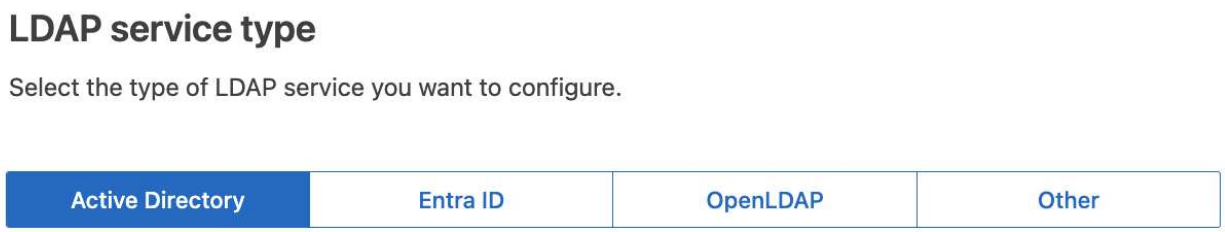
Konfiguration eingeben

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

Schritte

1. Wählen Sie **Zugriffsverwaltung** > **Identitätsföderation**.

2. Wählen Sie **Identitätsföderation aktivieren**.
3. Wählen Sie im Abschnitt LDAP-Servicetyp den Typ des LDAP-Dienstes aus, den Sie konfigurieren möchten.



   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 gleichbedeutend mit `sAMAccountName` für Active Directory und `uid` für OpenLDAP. Wenn Sie Oracle Directory Server konfigurieren, geben Sie `uid` .
   - **Benutzer-UUID**: Der Name des Attributs, das die permanente eindeutige Kennung eines LDAP-Benutzers enthält. Dieses Attribut ist gleichbedeutend mit `objectGUID` für Active Directory und `entryUUID` für OpenLDAP. Wenn Sie Oracle Directory Server konfigurieren, geben Sie `nsuniqueid` . Der Wert jedes Benutzers für das angegebene Attribut muss eine 32-stellige Hexadezimalzahl im 16-Byte- oder Zeichenfolgenformat sein, wobei Bindestriche ignoriert werden.
   - **Eindeutiger Gruppenname**: Der Name des Attributs, das die eindeutige Kennung einer LDAP-Gruppe enthält. Dieses Attribut ist gleichbedeutend mit `sAMAccountName` für Active Directory und `cn` für OpenLDAP. Wenn Sie Oracle Directory Server konfigurieren, geben Sie `cn` .
   - **Gruppen-UUID**: Der Name des Attributs, das die permanente eindeutige Kennung einer LDAP-Gruppe enthält. Dieses Attribut ist gleichbedeutend mit `objectGUID` für Active Directory und `entryUUID` für OpenLDAP. Wenn Sie Oracle Directory Server konfigurieren, geben Sie `nsuniqueid` . Der Wert jeder Gruppe für das angegebene Attribut muss eine 32-stellige Hexadezimalzahl im 16-Byte- oder Zeichenfolgenformat 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`
- **Eintritts-ID**: `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-Muster (AD- und Entra-ID)**: `[USERNAME]@*example*.com`
- **Anmeldenamenmuster auf niedrigerer Ebene (AD- und Entra-ID)**: `*example*\[USERNAME]`
- **Distinguished Namensmuster**: `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.
   ◦ **STARTLS verwenden**: Verwenden Sie STARTTLS, um die Kommunikation mit dem LDAP-Server zu sichern. Dies ist die empfohlene Option für Active Directory, OpenLDAP oder Andere, aber diese Option wird für Microsoft Entra ID nicht unterstützt.
   ◦ **LDAPS verwenden**: Die Option LDAPS (LDAP über SSL) verwendet TLS, um eine Verbindung zum

LDAP-Server herzustellen. Sie müssen diese Option für die Microsoft Entra ID auswählen.

- **TLS nicht verwenden**: Der Netzwerkverkehr zwischen dem StorageGRID -System und dem LDAP-Server wird nicht gesichert. Diese Option wird für die Microsoft Entra ID nicht unterstützt.

> Die Verwendung der Option **TLS nicht verwenden** wird nicht unterstützt, wenn Ihr Active Directory-Server die LDAP-Signierung 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.

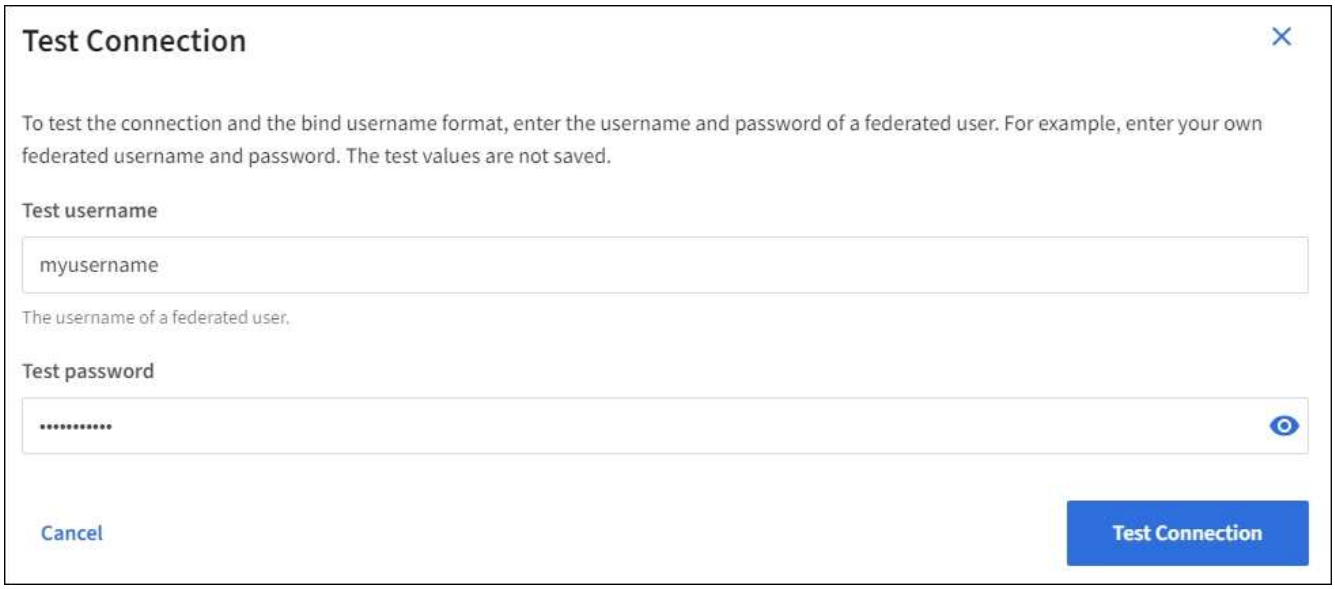
Testen Sie die Verbindung und speichern Sie die Konfiguration

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-Benutzernamenformat 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 /.



- 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 die Identitätsföderation für Gruppen und Benutzer vorübergehend oder dauerhaft deaktivieren. Wenn die Identitätsföderation deaktiviert ist, findet keine Kommunikation zwischen StorageGRID und der Identitätsquelle statt. Alle von Ihnen konfigurierten Einstellungen bleiben jedoch erhalten, sodass Sie die Identitätsföderation in Zukunft problemlos 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.

- Es findet keine Synchronisierung zwischen dem StorageGRID -System und der Identitätsquelle statt und es werden keine Warnungen für Konten ausgelöst, die nicht synchronisiert wurden.
- Das Kontrollkästchen **Identitätsföderation aktivieren** ist deaktiviert, wenn der Single Sign-On-Status (SSO) **Aktiviert** oder **Sandbox-Modus** ist. Der SSO-Status auf der Single Sign-On-Seite muss **Deaktiviert** sein, bevor Sie die Identitätsföderation deaktivieren können. Sehen "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, bei denen es sich nicht um Active Directory oder Microsoft Entra ID handelt, blockiert StorageGRID den S3-Zugriff für extern deaktivierte Benutzer nicht automatisch. Um den S3-Zugriff zu blockieren, löschen Sie 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 Pflege der umgekehrten Gruppenmitgliedschaft 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 Pflege der umgekehrten Gruppenmitgliedschaft 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

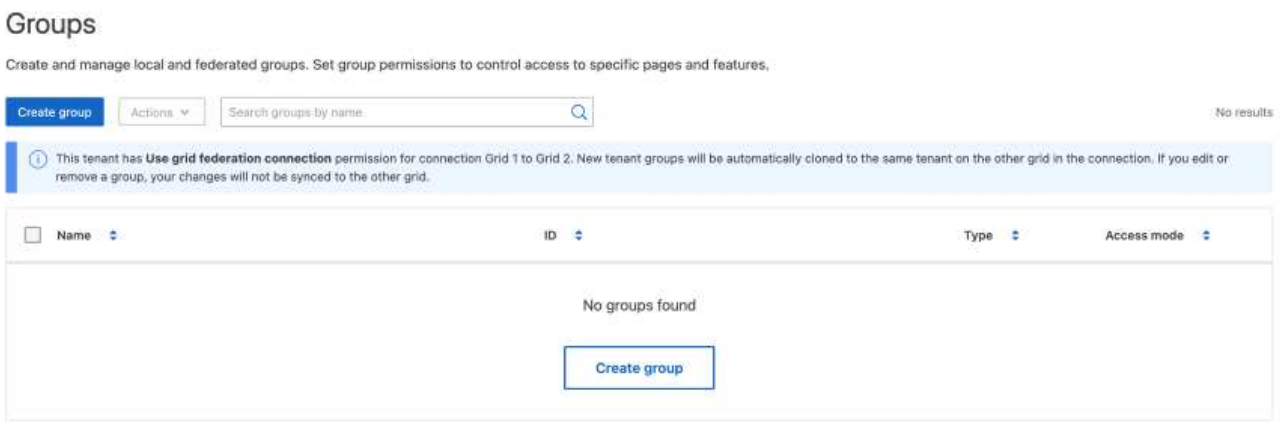
- Sie sind beim Tenant Manager mit einem angemeldet"Unterstützter Webbrowser".
- Sie gehören zu einer Benutzergruppe mit dem "Root-Zugriffsberechtigung".
- Wenn Sie planen, eine föderierte Gruppe "Konfigurierte Identitätsföderation"zu importieren, haben Sie , und die föderierte Gruppe ist bereits in der konfigurierten Identitätsquelle vorhanden.
- Wenn Ihr Mandantenkonto die Berechtigung **Grid Federation connection** verwenden hat, 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.



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 Name, der dem Attribut zugeordnet `sAMAccountName` ist. Bei OpenLDAP ist der eindeutige Name der dem Attribut zugeordnete Name `uid`.

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.

Gruppenrichtlinie	Beschreibung
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.
Ransomware-Minimierung	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. 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.
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.

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.

Berechtigung	Beschreibung	Details
Root-Zugriff	Bietet vollständigen Zugriff auf den Tenant Manager und die Mandanten-Management-API.	
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.

Berechtigung	Beschreibung	Details
Alle Buckets anzeigen	Ermöglicht Benutzern, alle Buckets und Bucket-Konfigurationen anzuzeigen.	Benutzer, die weder die Berechtigung Alle Buckets anzeigen noch die Berechtigung Alle Buckets verwalten haben, sehen die Menüoption **Buckets** nicht. Diese Berechtigung wird durch die Berechtigung „Alle Buckets verwalten“ ersetzt. Es hat keine Auswirkungen auf S3-Bucket- oder Gruppenrichtlinien, die von S3-Clients oder der S3-Konsole verwendet werden.
Managen aller Buckets	Ermöglicht Benutzern die Verwendung des Tenant Managers und der Tenant Management API zum Erstellen und Löschen von S3-Buckets und zum Verwalten der Einstellungen für alle S3-Buckets im Tenant-Konto, unabhängig von S3-Bucket- oder Gruppenrichtlinien.	Benutzer, die weder die Berechtigung Alle Buckets anzeigen noch die Berechtigung Alle Buckets verwalten haben, sehen die Menüoption **Buckets** nicht. Diese Berechtigung ersetzt die Berechtigung „Alle Buckets anzeigen“. Es hat keine Auswirkungen auf S3-Bucket- oder Gruppenrichtlinien, die von S3-Clients oder der S3-Konsole verwendet werden.
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 beim Tenant Manager mit einem angemeldet"Unterstützter Webbrowser".
- Sie gehören zu einer Benutzergruppe mit dem "Root-Zugriffsberechtigung".

Gruppe anzeigen oder bearbeiten

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

Schritte

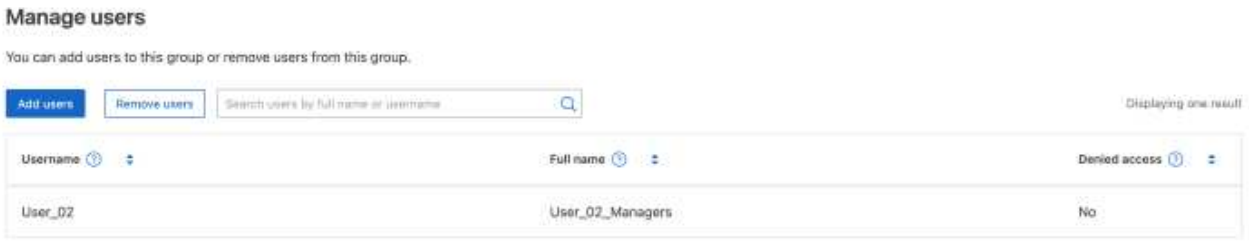
1. Wählen Sie **Zugriffsverwaltung** > **Gruppen**.
2. Überprüfen Sie die Informationen auf der Seite Gruppen, auf der grundlegende Informationen für alle lokalen und föderierten Gruppen für dieses Mandantenkonto aufgeführt sind.

   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. Sie können Wiederholen Sie einen Gruppenklon das gescheitert.
3. Wenn Sie den Namen der Gruppe ändern möchten:
   a. Aktivieren Sie das Kontrollkästchen für die Gruppe.
   b. Wählen Sie **Aktionen** > **Gruppenname 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 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** verwenden 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" für Details zu den einzugebenden Informationen.
   a. Ändern Sie im Abschnitt Übersicht den Anzeigenamen, indem Sie den Namen oder das Bearbeiten-Symbol 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**.

Wählen Sie optional eine andere S3-Gruppenrichtlinie aus oder geben Sie bei Bedarf die JSON-Zeichenfolge für eine benutzerdefinierte Richtlinie ein.

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. Sehen"Erstellen von Gruppen für einen S3-Mandanten" für Details zu den einzugebenden Informationen.
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 Bestätigungsdialogfeld wird angezeigt.
4. Wählen Sie **Gruppe löschen** oder **Gruppen löschen**.

Einrichten von AssumeRole

Bevor Sie beginnen

Sie müssen Administrator sein, um AssumeRole einzurichten.

Über diese Aufgabe

Um AssumeRole einzurichten, erstellen Sie die zu übernehmende Zielgruppe, falls die Gruppe noch nicht vorhanden ist. Bearbeiten Sie die S3-Richtlinie der Gruppe, um die zulässigen Aktionen für die Übernahme dieser Gruppe anzugeben. Bearbeiten Sie die S3-Vertrauensrichtlinie der Gruppe, um die vertrauenswürdigen Benutzer anzugeben, die die Gruppe mit der AssumeRole-API übernehmen dürfen.

Temporäre Sicherheitsanmeldeinformationen, die aus der Annahme dieser Gruppe erstellt werden, sind für eine begrenzte Dauer gültig. Die Sitzung dauert zwischen 15 Minuten und 12 Stunden, die Standardsitzung beträgt 1 Stunde. Wenn Sie den Benutzer aus der S3-Vertrauensrichtlinie der Gruppe entfernen, kann der Benutzer diese Gruppe nicht mehr übernehmen.

Schritte

1. Wählen Sie **Zugriffsverwaltung** > **Gruppen**.
2. Klicken Sie auf den Gruppennamen.
3. Wählen Sie die Registerkarte **S3-Vertrauensrichtlinie**.
4. Fügen Sie Ihre S3-Vertrauensrichtlinie hinzu, einschließlich einer Liste von Benutzern, die AssumeRole ausführen können.
5. Wählen Sie **Änderungen speichern**.
6. Wählen Sie die Registerkarte **S3-Gruppenrichtlinie**.
7. Bearbeiten Sie die S3-Richtlinie, um nur die erforderlichen S3-Aktionen für die vertrauenswürdigen

Benutzer anzugeben, die in der S3-Vertrauensrichtlinie dieser Gruppe hinzugefügt wurden.

8. Wählen Sie **Änderungen speichern**.

Beispiel einer AssumeRole S3-Vertrauensrichtlinie

```
{
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "sts:AssumeRole",
            "Principal": {
                "AWS": [
                    "urn:sgws:identity::1234567890:user/user1",
                    "arn:aws:iam::1234567890:user/user2"
                ]
            }
        }
    ]
}
```

Nachdem die Konfiguration abgeschlossen ist, können in der S3-Vertrauensrichtlinie aufgeführte Benutzer AssumeRole ausführen und Anmeldeinformationen erhalten. Die endgültigen Berechtigungen werden durch Gruppenrichtlinien, Bucket-Richtlinien und Sitzungsrichtlinien bestimmt. Weitere Informationen finden Sie unter "Verwenden von Zugriffsrichtlinien" .

Benutzer managen

Sie können lokale Benutzer erstellen und sie lokalen Gruppen zuweisen, um festzulegen, auf welche Funktionen diese Benutzer zugreifen können. Sie können auch föderierte Benutzer importieren. Der Tenant Manager umfasst 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 beim Tenant Manager mit einem angemeldet"Unterstützter Webbrowser".
- Sie gehören zu einer Benutzergruppe mit dem "Root-Zugriffsberechtigung".
- Wenn Ihr Mandantenkonto die Berechtigung **Grid Federation connection** verwenden hat, 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.

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. Sie können 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 **Aktionen** > **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. Einzelheiten dazu, was Sie eingeben müssen, finden Sie unterErstellen Sie einen lokalen Benutzer.
   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 **Access Keys Create key** aus und folgen Sie den 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.

Importieren von Verbundbenutzern

Sie können einen oder mehrere Verbundbenutzer (bis zu maximal 100 Benutzer) direkt in die Seite „Benutzer“ importieren.

Schritte

1. Wählen Sie **Zugriffsverwaltung** > **Benutzer**.
2. Wählen Sie **Verbundbenutzer importieren**.
3. Geben Sie die UUID oder den Benutzernamen für einen oder mehrere Verbundbenutzer ein.

   Fügen Sie bei mehreren Einträgen jede UUID oder jeden Benutzernamen in einer neuen Zeile hinzu.

4. Wählen Sie **Importieren**.

   Wenn der Import in das Feld „Benutzer“ für einen oder mehrere Benutzer fehlschlägt, führen Sie die folgenden Schritte aus:

   a. Erweitern Sie **Nicht importierte Benutzer** und wählen Sie **Benutzer kopieren**.
   b. Versuchen Sie den Import erneut, indem Sie **Zurück** auswählen und die kopierten Benutzer in das

Dialogfeld **Verbundbenutzer importieren** einfügen.

Nachdem Sie das Dialogfeld **Verbundbenutzer importieren** geschlossen haben, werden die Verbundbenutzerinformationen für die erfolgreich importierten Benutzer auf der Seite „Benutzer“ angezeigt.

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 **Aktionen** > **Benutzer duplizieren**.
4. Einzelheiten dazu, was Sie eingeben müssen, finden Sie unterErstellen Sie einen lokalen Benutzer.
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 von S3-Zugriffsschlüsseln

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 beim Tenant Manager mit einem angemeldet"Unterstützter Webbrowser".
- Sie gehören zu einer Benutzergruppe mit dem "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 den verfügen"Entsprechende Berechtigung", können Sie 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 "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 beim Tenant Manager mit einem angemeldet"Unterstützter Webbrowser".
- Sie gehören zu einer Benutzergruppe, die über die eigenen S3-Anmeldeinformationen verwalten "Berechtigung"verfügt.

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 beim Tenant Manager mit einem 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 beim Tenant Manager mit einem angemeldet"Unterstützter Webbrowser".
- Sie gehören zu einer Benutzergruppe mit dem "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 beim Tenant Manager mit einem 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 beim Tenant Manager mit einem 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, den Sie löschen möchten.
4. Wählen Sie **Aktionen** > **Ausgewählte Taste löschen**.
5. Wählen Sie im Bestätigungsdialogfeld **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 beim Tenant Manager mit einem 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 Object Lock-Eigenschaften von Buckets oder Objekten können erteilt werden durch"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.
- Wenn jeder Mandant 5,000 Buckets hat, verfügt jeder Storage-Node im Grid über mindestens 64 GB RAM.

> Jedes Raster kann maximal 100.000 Buckets enthalten, darunter"Zweigeimer" .

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	Ein Name für den Bucket, der die folgenden Regeln erfüllt: • Jedes StorageGRID System muss eindeutig sein (nicht nur innerhalb des Mandantenkontos). • Muss DNS-konform sein. • Muss 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. • Darf keine Punkte in Virtual-Hosted-Style-Anforderungen enthalten. Perioden verursachen Probleme bei der Überprüfung des Server-Platzhalterzertifikats. Weitere Informationen finden Sie im "Dokumentation der Amazon Web Services (AWS) zu den Bucket-Benennungsregeln". **Hinweis**: Sie können den Bucket-Namen nicht ändern, nachdem Sie den Bucket erstellt haben.

Feld	Beschreibung
Region	Der Bereich des Eimers. Ihr StorageGRID Administrator verwaltet die verfügbaren Regionen. Die Region eines Buckets kann sich auf die auf Objekte angewendete Datenschutzrichtlinie auswirken. Standardmäßig werden alle Buckets im `us-east-1` Region. Wenn die Standardregion auf eine andere Region als `us-east-1` , diese andere Region ist zunächst im Dropdown-Menü ausgewählt. **Hinweis**: Sie können die Region nicht ändern, nachdem Sie den Bucket erstellt haben.

2. Wählen Sie **Weiter**.

Einstellungen verwalten

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 wird für die Cross-Grid-Replikation verwendet.
   - Sie möchten eine"Asteimer" aus diesem Eimer.

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.

   > Ihr Grid-Administrator muss Ihnen die Berechtigung erteilen"Verwenden Sie bestimmte Funktionen von S3 Object Lock".

   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
Governance	• Benutzer mit der `s3:BypassGovernanceRetention` Berechtigung können den Anforderungskopf verwenden `x-amz-bypass-governance-retention: true`, um die 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.
Compliance	• 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. **Hinweis**: Ihr Grid-Administrator muss Ihnen erlauben, den Compliance-Modus zu verwenden.

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 an, der kleiner oder gleich der maximalen Aufbewahrungsfrist für den Mandanten ist, wie vom Grid-Administrator festgelegt.

Eine *maximale* Aufbewahrungsfrist, die ein Wert von 1 Tag bis 100 Jahre sein kann, wird festgelegt, wenn der Grid-Administrator den Mandanten erstellt. Wenn Sie eine *default* Aufbewahrungsfrist festlegen, darf sie den für die maximale Aufbewahrungsfrist festgelegten Wert nicht überschreiten. Bitten Sie bei Bedarf Ihren Grid-Administrator, die maximale Aufbewahrungsfrist zu verlängern oder zu verkürzen.

4. Wählen Sie optional **Kapazitätslimit aktivieren** aus, geben Sie einen Wert ein und wählen Sie die Kapazitätseinheit aus.

Das Kapazitätslimit ist die maximale Kapazität, die für die Objekte dieses Buckets verfügbar ist. Dieser Wert stellt eine logische Menge (Objektgröße) und keine physische Menge (Größe auf Festplatte) dar.

Wenn kein Limit festgelegt ist, ist die Kapazität für diesen Bucket unbegrenzt. Weitere Informationen finden Sie unter "Kapazitätsgrenze" .

5. Wählen Sie optional **Objektanzahllimit aktivieren**.

Die Objektanzahlgrenze ist die maximale Anzahl von Objekten, die dieser Bucket enthalten kann. Dieser Wert stellt eine logische Menge (Objektanzahl) dar. Wenn kein Limit festgelegt ist, ist die Objektanzahl unbegrenzt.

6. Wählen Sie **Eimer erstellen**.

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

7. Wählen Sie optional **Gehe zu Bucket-Detailseite** zu "Bucket-Details anzeigen" und führen Sie zusätzliche Konfiguration durch.

Sie können auch"Erstellen Sie Zweig-Buckets" nach Bedarf.

Bucket-Details anzeigen

Sie können die Buckets in Ihrem Mandantenkonto anzeigen.

Bevor Sie beginnen

- Sie sind beim Tenant Manager mit einem angemeldet"Unterstützter Webbrowser".
- Sie gehören zu einer Benutzergruppe mit dem "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 Übersichtstabelle 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.

   > Bei den angezeigten Werten für Objektanzahl, belegter Speicherplatz und Nutzung handelt es sich um Schätzwerte. 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.

   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. Diese Spalte ist standardmäßig ausgeblendet.

Objektanzahl

Die Anzahl der Objekte in diesem Bucket. Wenn für Buckets die Versionierung aktiviert ist, sind nicht aktuelle Objektversionen in diesem Wert enthalten.

Wenn Objekte hinzugefügt oder gelöscht werden, wird dieser Wert möglicherweise nicht sofort aktualisiert.

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.

Die Aktualisierung dieses Werts kann bis zu 10 Minuten dauern.

Zu Verwenden

Der Prozentsatz, der vom Kapazitätslimit des Buckets verwendet wird, sofern ein Wert festgelegt wurde.

Der Nutzungswert basiert auf internen Schätzungen und kann in einigen Fällen überschritten werden. StorageGRID überprüft beispielsweise das Kapazitätslimit (sofern festgelegt), wenn ein Mandant beginnt, Objekte hochzuladen, und lehnt neue Ingest für diesen Bucket ab, wenn der Mandant das Kapazitätslimit überschritten hat. StorageGRID berücksichtigt jedoch nicht die Größe des aktuellen Uploads, wenn festgestellt wird, ob das Kapazitätslimit überschritten wurde. Wenn Objekte gelöscht werden, kann es vorkommen, dass ein Mandant vorübergehend verhindert wird, neue Objekte in diesen Bucket hochzuladen, bis die Auslastung der Kapazitätsgrenze neu berechnet wird. Die Berechnungen können 10 Minuten oder länger dauern.

Dieser Wert gibt die logische Größe und nicht die physische Größe an, die zum Speichern der Objekte und ihrer Metadaten erforderlich ist.

Kapazität

Wenn festgelegt, wird das Kapazitätslimit des Buckets festgelegt.

Erstellungsdatum

Datum und Uhrzeit der Erstellung des Buckets. Diese Spalte ist standardmäßig ausgeblendet.

3. Um Details für einen bestimmten Bucket anzuzeigen, wählen Sie den Bucket-Namen aus der Tabelle aus.
   a. Zeigen Sie die zusammenfassenden Informationen oben auf der Webseite an, um die Details für den Bucket zu bestätigen, z. B. Region und Objektanzahl.
   b. Zeigen Sie die Balken für die Kapazitätslimitnutzung und die Objektanzahllimitnutzung an. Wenn die Nutzung 100 % oder nahe 100 % beträgt, sollten Sie eine Erhöhung des Limits oder das Löschen einiger Objekte in Erwägung ziehen.
   c. Wählen Sie bei Bedarf **Objekte im Bucket löschen** und **Bucket löschen** aus.

Achten Sie bei der Auswahl dieser Optionen genau auf die Warnhinweise. Weitere Informationen finden Sie unter:

- "Löschen aller Objekte in einem Bucket"
- "Löschen eines Buckets" (Bucket muss leer sein)

   d. Zeigen Sie die Einstellungen für den Bucket auf den einzelnen Registerkarten nach Bedarf an, oder ändern Sie sie.

- **S3 Console**: Zeigt die Objekte für den Bucket an. Weitere Informationen finden Sie unter "Verwenden Sie die S3-Konsole".
- **Bucket-Optionen**: Optionen anzeigen oder ändern. Einige Einstellungen, wie z. B. S3 Object Lock, können nach dem Erstellen des Buckets nicht geändert werden.
  - "Management der Bucket-Konsistenz"
  - "Aktualisierung der Uhrzeit des letzten Zugriffs"
  - "Kapazitätsgrenze"
  - "Objektanzahllimit"
  - "Objektversionierung"
  - "S3-Objektsperre"
  - "Standardmäßige Bucket-Aufbewahrung"
  - "Grid-übergreifende Replizierung managen" (Falls für den Mieter zulässig)
- **Plattform-Services**: "Management von Plattform-Services" (Wenn für den Mieter erlaubt)
- **Bucket Access**: Optionen anzeigen oder ändern. Sie müssen über spezifische Zugriffsberechtigungen verfügen.
  - Konfigurieren"CORS für Buckets und Objekte" sodass der Bucket und die Objekte im Bucket für Webanwendungen in anderen Domänen zugänglich sind.
  - "Kontrolle des Benutzerzugriffs" Für einen S3-Bucket und Objekte in diesem Bucket.
- **Branches**: Zeigen Sie die Liste der Branch-Buckets für den Bucket an. "Erstellen Sie einen neuen Branch-Bucket oder verwalten Sie Branch-Buckets" .

Was ist ein Asteimer?

Ein Branch-Bucket bietet Zugriff auf Objekte in einem Bucket, wie sie zu einem bestimmten Zeitpunkt existierten.

Sie erstellen einen Branch-Bucket aus einem vorhandenen Bucket. Nachdem Sie einen Branch-Bucket erstellt haben, wird der ursprüngliche Bucket, aus dem er erstellt wurde, als *Basis-Bucket* bezeichnet. Darüber hinaus können Sie einen Branch-Bucket aus einem anderen Branch-Bucket erstellen.

Ein Branch-Bucket bietet Zugriff auf geschützte Daten, dient jedoch nicht als Backup. Um die Daten weiterhin zu schützen, verwenden Sie diese Funktionen für Basis-Buckets:

- "S3-Objektsperre"
- "Grid-übergreifende Replizierung"für Basiseimer
- "Bucket-Richtlinien"für versionierte Buckets zum Bereinigen alter Objektversionen

Beachten Sie die folgenden Merkmale von Zweig-Buckets:

- Sie können auf die Objekte in Zweig-Buckets zugreifen, indem Sie"S3-Konsole zum Herunterladen von Objekten" .
- Wenn Clients auf Objekte in einem Branch-Bucket zugreifen,"Zugriffsrichtlinien" und nicht die Richtlinien des Basis-Buckets bestimmen, ob der Zugriff gewährt oder verweigert wird.
- Objekte, die in einem Basis-Bucket erstellt werden, werden danach ausgewertet, wie"ILM-Regeln" auf den Basiseimer anwenden. In einem Branch-Bucket erstellte Objekte werden basierend darauf ausgewertet, wie ILM-Regeln auf den Branch-Bucket angewendet werden.

- Die Cross-Grid-Replikation wird für Branch-Buckets nicht unterstützt.
- Plattformdienste werden für Branch-Buckets nicht unterstützt.

Beispiele für die Verwendung von Branch Buckets

- Sie können einen Branch-Bucket verwenden, um beschädigte Objekte zu entfernen, indem Sie einen Branch-Bucket von einem Zeitpunkt vor dem Auftreten der Beschädigung erstellen und dann Anwendungen auf den Branch-Bucket statt auf den Basis-Bucket verweisen, der beschädigte Objekte enthält.
- Sie speichern Daten in einem versionierten Bucket. Es gab eine versehentliche Sicherheitslücke, die dazu führte, dass nach der Zeit *T* viele unerwünschte Objekte aufgenommen wurden. Sie können einen Branch-Bucket für den Vorher-Zeitwert *T* erstellen und Clientvorgänge an diesen Branch-Bucket umleiten. Dann werden den Clients nur Objekte angezeigt, die vor der Vorzeit *T* aufgenommen wurden.

Operationen an Objekten in Branch-Buckets

- Eine PUT-Objektoperation für einen Branch-Bucket erstellt ein Objekt im Branch.
- Eine GET-Objektoperation für einen Branch-Bucket ruft ein Objekt aus dem Branch ab. Wenn das Objekt im Zweig-Bucket nicht vorhanden ist, wird das Objekt aus dem Basis-Bucket abgerufen.
- Das Löschen von Objekten aus Branch-Buckets erfolgt wie folgt:

Betrieb	Ziel	Ergebnis	Objektsichtbarkeit im Basis-Bucket	Objektsichtbarkeit im Branch-Bucket
Löschen ohne Versionskennung	Basiseimer	Löschmarkierung wird nur für den Basis-Bucket erstellt	HEAD/GET gibt zurück, dass das Objekt nicht existiert, auf bestimmte Versionen kann jedoch noch zugegriffen werden	HEAD/GET gibt zurück, dass das Objekt vorhanden ist und auf bestimmte Versionen noch zugegriffen werden kann Die Löschmarkierung wäre nach dem Branch-Bucket erstellt worden `beforeTime`.
Löschen mit Versions-ID	Basiseimer	Eine bestimmte Objektversion wird sowohl für den Basis- als auch für den Zweig-Bucket gelöscht	HEAD/GET gibt zurück, dass die Objektversion nicht existiert	HEAD/GET gibt zurück, dass die Objektversion nicht existiert
Löschen ohne Versionskennung	Asteimer	Löschmarkierung wird nur für den Branch-Bucket erstellt	HEAD/GET gibt Objekt zurück (Basis-Bucket-Objekt nicht betroffen)	HEAD/GET gibt zurück, dass das Objekt nicht existiert
Löschen mit Versions-ID	Asteimer	Bestimmte Objektversionen werden nur für den Zweig-Bucket gelöscht	HEAD/GET gibt eine bestimmte Objektversion zurück (Basis-Bucket-Objekt nicht betroffen)	HEAD/GET gibt zurück, dass die Objektversion nicht existiert

Siehe auch"Löschen von S3-versionierten Objekten" .

Verwalten von Branch-Buckets

Verwenden Sie den Mandanten-Manager, um Details für Zweigstellen-Buckets zu erstellen und anzuzeigen.

Bevor Sie beginnen

- Sie haben sich beim Tenant Manager angemeldet mit einem"Unterstützter Webbrowser" .
- Sie gehören einer Benutzergruppe an, die über Root-Zugriff verfügt oder"Alle Berechtigungen für Buckets managen" . Diese Berechtigungen überschreiben die Berechtigungseinstellungen in Gruppen- oder Bucket-Richtlinien.
- Der Basis-Bucket, aus dem Sie einen Zweig erstellen möchten, hat"Versionierung aktiviert" .
- Sie sind der Eigentümer des Basis-Buckets.

Über diese Aufgabe

Beachten Sie die folgenden Informationen zu Branch-Buckets:

- Berechtigungen zum Festlegen von S3 Object Lock-Eigenschaften von Buckets oder Objekten können erteilt werden durch"Bucket-Richtlinie oder Gruppenrichtlinie" .
- Wenn Sie die Versionsverwaltung für den Basis-Bucket aussetzen, ist der Inhalt des Basis-Buckets in seinen Zweig-Buckets nicht mehr sichtbar.

> Nachdem Sie einen Branch-Bucket konfiguriert und erstellt haben, können Sie die Konfiguration nicht mehr ändern.

Branch-Bucket erstellen

Schritte

1. Wählen Sie **View Buckets** aus dem Dashboard, oder wählen Sie **STORAGE (S3)** > **Buckets**.
2. Wählen Sie den Bucket aus, aus dem Sie einen Zweig erstellen möchten (den „Basis-Bucket“).
3. Wählen Sie auf der Bucket-Detailseite **Branches** > **Branch-Bucket erstellen**.

   Die Schaltfläche **Branch-Bucket erstellen** ist deaktiviert, wenn für den Basis-Bucket keine Versionierung aktiviert ist.

Geben Sie Details ein

Schritte

1. Geben Sie Details zum Zweig-Bucket ein.

Feld	Beschreibung
Name des Branch-Buckets	Ein Name für den Branch-Bucket, der diesen Regeln entspricht: • Jedes StorageGRID System muss eindeutig sein (nicht nur innerhalb des Mandantenkontos). • Muss DNS-konform sein. • Muss 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. • Darf keine Punkte in Virtual-Hosted-Style-Anforderungen enthalten. Perioden verursachen Probleme bei der Überprüfung des Server-Platzhalterzertifikats. Weitere Informationen finden Sie im "Dokumentation der Amazon Web Services (AWS) zu den Bucket-Benennungsregeln". **Hinweis**: Sie können den Namen nach dem Erstellen des Branch-Buckets nicht mehr ändern.
Region (kann für Zweigstellen-Buckets nicht geändert werden)	Die Region des Zweig-Buckets. Die Region des Zweig-Buckets muss mit der Region des Basis-Buckets übereinstimmen, daher ist dieses Feld für Zweig-Buckets deaktiviert.
Vor der Zeit	Die Frist für den Zugriff auf im Basis-Bucket erstellte Objektversionen vom Zweig-Bucket aus. Der Branch-Bucket bietet Zugriff auf Objektversionen, die vor dem Zeitpunkt „Before“ erstellt wurden. „Vor der Zeit“ muss ein Datum und eine Uhrzeit sein, die vergangen sind. Es kann kein zukünftiges Datum sein.
Zweigschaufeltyp	• **Lesen/Schreiben**: Sie können Objekte oder Objektversionen im Branch-Bucket hinzufügen oder löschen. • **Schreibgeschützt**: Sie können Objekte im Branch-Bucket nicht ändern. **Hinweis**: Sie können den Branch-Bucket-Typ nur dann auf schreibgeschützt setzen, wenn der Branch-Bucket leer ist. Wenn der Typ für einen vorhandenen Branch-Bucket auf Lesen/Schreiben eingestellt ist und Sie nicht darin geschrieben haben, können Sie den Typ auf schreibgeschützt ändern.

2. Wählen Sie **Weiter**.

Objekteinstellungen verwalten (optional)

Die Objekteinstellungen für einen Zweig-Bucket wirken sich nicht auf die Objektversionen im Basis-Bucket aus.

Schritte

1. Wenn die globale Einstellung „S3 Object Lock“ aktiviert ist, aktivieren Sie optional „S3 Object Lock“ für den

Branch-Bucket. Um die S3-Objektsperre zu aktivieren, muss der Branch-Bucket ein Lese-/Schreib-Bucket sein.

Aktivieren Sie S3 Object Lock für einen Branch-Bucket nur, wenn Sie Objekte für einen festgelegten Zeitraum aufbewahren müssen, beispielsweise um bestimmte gesetzliche Anforderungen zu erfüllen. S3 Object Lock ist eine permanente Einstellung, mit der Sie das Löschen oder Überschreiben von Objekten für einen festgelegten Zeitraum oder auf unbestimmte Zeit verhindern können.

> Nachdem die S3-Objektsperreinstellung für einen Bucket aktiviert wurde, kann sie nicht mehr deaktiviert werden. Jeder mit den entsprechenden Berechtigungen kann dem Branch-Bucket Objekte hinzufügen, die nicht geändert werden können. Möglicherweise können Sie diese Objekte oder den Branch-Bucket selbst nicht löschen.

2. Wenn Sie **S3-Objektsperre aktivieren** ausgewählt haben, aktivieren Sie optional **Standardaufbewahrung** für den Branch-Bucket.

> Ihr Grid-Administrator muss Ihnen die Berechtigung erteilen"Verwenden Sie bestimmte Funktionen von S3 Object Lock".

Wenn die **Standardaufbewahrung** aktiviert ist, werden neue Objekte, die dem Branch-Bucket hinzugefügt werden, automatisch vor dem Löschen oder Überschreiben geschützt. Die Einstellung **Standardaufbewahrung** gilt nicht für Objekte, die über eigene Aufbewahrungszeiträume verfügen.

a. Wenn **Standardaufbewahrung** aktiviert ist, geben Sie einen **Standardaufbewahrungsmodus** für den Branch-Bucket an.

Standardaufbewahrungsmodus	Beschreibung
Governance	• Benutzer mit der `s3:BypassGovernanceRetention` Berechtigung können den Anforderungskopf verwenden `x-amz-bypass-governance-retention: true`, um die 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.
Compliance	• 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. **Hinweis**: Ihr Grid-Administrator muss Ihnen erlauben, den Compliance-Modus zu verwenden.

b. Wenn die **Standardaufbewahrung** aktiviert ist, geben Sie die **Standardaufbewahrungsdauer** für den Zweig-Bucket an.

Die **Standardaufbewahrungsfrist** gibt an, wie lange neue Objekte, die dem Branch-Bucket hinzugefügt werden, ab dem Zeitpunkt ihrer Aufnahme aufbewahrt werden sollen. Geben Sie einen Wert an, der kleiner oder gleich der vom Grid-Administrator festgelegten maximalen Aufbewahrungsdauer für den Mandanten ist.

Eine *maximale* Aufbewahrungsfrist, die ein Wert von 1 Tag bis 100 Jahre sein kann, wird festgelegt, wenn der Grid-Administrator den Mandanten erstellt. Wenn Sie eine *default* Aufbewahrungsfrist festlegen, darf sie den für die maximale Aufbewahrungsfrist festgelegten Wert nicht überschreiten. Bitten Sie bei Bedarf Ihren Grid-Administrator, die maximale Aufbewahrungsfrist zu verlängern oder zu verkürzen.

3. Wählen Sie optional **Kapazitätslimit aktivieren** aus.

   Die Kapazitätsgrenze ist die maximal verfügbare Kapazität für den Zweigstellen-Bucket. Dieser Wert stellt eine logische Menge (Objektgröße) dar, keine physische Menge (Größe auf der Festplatte).

   Wenn kein Limit festgelegt ist, ist die Kapazität für den Zweigstellen-Bucket unbegrenzt. Weitere Informationen finden Sie unter "Kapazitätsgrenze" für weitere Informationen.

   Diese Einstellung gilt nur für Objekte, die direkt in den Branch-Bucket aufgenommen werden, und nicht für Objekte, die vom Basis-Bucket über den Branch-Bucket sichtbar sind.

4. Wählen Sie optional **Objektanzahllimit aktivieren** aus.

   Die Objektanzahlgrenze ist die maximale Anzahl von Objekten, die der Zweig-Bucket enthalten kann. Dieser Wert stellt eine logische Menge (Objektanzahl) dar. Wenn kein Limit festgelegt ist, ist die Objektanzahl unbegrenzt.

   Diese Einstellung gilt nur für Objekte, die direkt in den Branch-Bucket aufgenommen werden, und nicht für Objekte, die vom Basis-Bucket über den Branch-Bucket sichtbar sind.

5. Wählen Sie **Eimer erstellen**.

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

6. Wählen Sie optional **Zur Bucket-Detailseite**, um"Details zum Branch-Bucket anzeigen" und führen Sie zusätzliche Konfigurationen durch.

   Auf der Bucket-Detailseite sind einige Konfigurationsoptionen im Zusammenhang mit der Änderung von Objekten für schreibgeschützte Buckets deaktiviert.

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 beim Tenant Manager mit einem angemeldet"Unterstützter Webbrowser".
- Sie gehören zu einer Benutzergruppe mit dem "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.

3. 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.
4. 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.

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

   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 das ILM-Richtlinien-Tag nicht `NTAP-SG-ILM-BUCKET-TAG` über die S3 PutBucketTagging API oder die 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 von Bucket-Richtlinien

Sie können den Benutzerzugriff für einen S3-Bucket und die Objekte in diesem Bucket steuern.

Bevor Sie beginnen

- Sie sind beim Tenant Manager mit einem angemeldet"Unterstützter Webbrowser".
- Sie gehören zu einer Benutzergruppe mit dem "Root-Zugriffsberechtigung". Die Berechtigungen Alle Buckets anzeigen und alle Buckets verwalten erlauben nur die Anzeige.
- Sie haben überprüft, ob die erforderliche Anzahl an Storage Nodes und Standorten verfügbar ist. 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.

Schritte

1. Wählen Sie **Buckets** aus, und wählen Sie dann den Bucket aus, den Sie verwalten möchten.
2. Wählen Sie auf der Seite mit den Bucket-Details **Bucket Access** > **Bucket Policy** aus.
3. Führen Sie einen der folgenden Schritte aus:
   - Geben Sie eine Bucket Policy ein, indem Sie das Kontrollkästchen **enable Policy** aktivieren. Geben Sie dann eine gültige JSON-formatierte Zeichenfolge ein.

     Jede Bucket-Richtlinie hat ein Größenlimit von 20,480 Byte.
   - Ändern Sie eine vorhandene Richtlinie, indem Sie die Zeichenfolge bearbeiten.
   - Deaktivieren Sie eine Richtlinie, indem Sie die Option **Richtlinie aktivieren** deaktivieren.

Ausführliche Informationen zu Bucket-Richtlinien, einschließlich Sprachtyntax und Beispielen, finden Sie unter "Beispiel für Bucket-Richtlinien".

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 beim Tenant Manager mit einem angemeldet"Unterstützter Webbrowser".
- Sie gehören zu einer Benutzergruppe mit dem "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 **Read-after-New-write** nicht den Anforderungen der Client-Anwendung entspricht, können Sie die Konsistenz ändern, indem Sie die Bucket-Konsistenz oder den Header festlegen `Consistency-Control`. Die `Consistency-Control` Kopfzeile 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"
- "Konfigurieren Sie StorageGRID CORS für Buckets und Objekte"
- Änderung der Bucket-Konsistenz

Wenn die Standardkonsistenz, die beim Ändern von Bucket-Einstellungen verwendet wird, nicht den Anforderungen der Client-Anwendung entspricht, können Sie die Konsistenz ändern, indem Sie den `Consistency-Control` Header für "S3-REST-API"oder verwenden, indem Sie die Optionen oder `force` im verwenden `reducedConsistency`"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. Weitere Informationen finden Sie unter "Verwenden Sie die letzte Zugriffszeit in ILM-Regeln" .

Bevor Sie beginnen

- Sie sind beim Tenant Manager mit einem angemeldet"Unterstützter Webbrowser".
- Sie gehören zu einer Benutzergruppe mit dem "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 der Metadaten eines Objekts, wenn eine HEAD-Operation ausgeführt wird	Nein	Nein	Nein	Nein
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 Auflisten von Objekten oder Objektversionen	Nein	Nein	Nein	Nein

Anforderung zum Kopieren eines Objekts von einem Bucket in einen anderen	• Nein, für die Quellkopie • Ja, für die Zielkopie	• Nein, für die Quellkopie • Ja, für die Zielkopie	• Ja, für die Quellkopie • Ja, für die Zielkopie	• 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 beim Tenant Manager mit einem angemeldet"Unterstützter Webbrowser".
- Sie gehören zu einer Benutzergruppe mit dem "Managen aller Buckets oder Root-Zugriffsberechtigungen". Diese Berechtigungen überschreiben die Berechtigungseinstellungen in Gruppen- oder Bucket-Richtlinien.
- Sie haben überprüft, ob die erforderliche Anzahl an Storage Nodes und Standorten verfügbar ist. 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.

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	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. Objekte, die sich bereits im Bucket befanden, werden versioniert, wenn sie von einem Benutzer geändert werden.
Die Versionierung unterbrechen	Unterbrechen Sie die Objektversionierung, wenn Sie keine neuen Objektversionen mehr erstellen möchten. Sie können weiterhin alle vorhandenen Objektversionen abrufen.

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.

Ihr Grid-Administrator muss Ihnen die Berechtigung erteilen, bestimmte Funktionen von S3 Object Lock zu verwenden.

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

Ein Bucket ohne S3 Object Lock kann nur Objekte ohne Aufbewahrungseinstellungen haben. Keine aufgenommenen Objekte verfügen über Aufbewahrungseinstellungen.

Ein Bucket mit S3 Object Lock kann Objekte mit und ohne Aufbewahrungseinstellungen haben, die von S3-Client-Applikationen angegeben wurden. Einige aufgenommene Objekte haben Aufbewahrungseinstellungen.

Ein Bucket mit S3 Object Lock und konfigurierter Standardaufbewahrung kann Objekte mit angegebenen Aufbewahrungseinstellungen und neue Objekte ohne Aufbewahrungseinstellungen hochgeladen haben. Die neuen Objekte verwenden die Standardeinstellung, da die Aufbewahrungseinstellung nicht auf Objektebene konfiguriert wurde.

Tatsächlich verfügen alle neu aufgenommenen Objekte über Aufbewahrungseinstellungen, wenn die Standardaufbewahrung konfiguriert ist. Vorhandene Objekte ohne Objektaufbewahrungseinstellungen bleiben hiervon unberührt.

Aufbewahrungsmodi

Die Objektsperrfunktion 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-Objektsperrung 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 Aufbewahrungspflichten haben 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.

  Details 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-Objektsperrung 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 Objektsperraufgaben

Die folgenden Listen für Grid-Administratoren und Mandantenbenutzer enthalten die allgemeinen Aufgaben für die Verwendung der S3 Objektsperrfunktion.

Grid-Administrator

- Globale S3-Objektsperrung für das gesamte StorageGRID-System aktivieren.
- Stellen Sie sicher, dass die Richtlinien für Information Lifecycle Management (ILM) den *Compliance-Anforderungen entsprechen*, "Anforderungen für Buckets mit aktivierter S3-Objektsperrung"d. h. dass sie die erfüllen.
- Erlauben Sie einem Mandanten nach Bedarf, Compliance als Aufbewahrungsmodus zu verwenden. Andernfalls ist nur der Governance-Modus zulässig.
- Legen Sie bei Bedarf eine maximale Aufbewahrungsfrist für einen Mandanten fest.

Mandantenbenutzer

- Überlegungen für Buckets und Objekte mit S3 Object Lock prüfen.
- Wenden Sie sich bei Bedarf an den Grid-Administrator, um die globale S3 Object Lock-Einstellung zu aktivieren und Berechtigungen festzulegen.
- Erstellen von Buckets mit aktivierter S3-Objektsperre
- Optional können Sie Standardaufbewahrungseinstellungen für einen Bucket konfigurieren:
  - Standardaufbewahrungsmodus: Governance oder Compliance, falls vom Grid-Administrator zugelassen.
  - Standardaufbewahrungszeitraum: Muss kleiner oder gleich der maximalen Aufbewahrungsfrist sein, die vom Grid-Administrator festgelegt wurde.
- Fügen Sie mithilfe der S3-Client-Applikation Objekte hinzu und legen Sie optional die objektspezifische Aufbewahrung fest:
  - Aufbewahrungsmodus. Governance oder Compliance, falls vom Grid-Administrator zugelassen.
  - Bis-Datum beibehalten: Muss kleiner oder gleich dem sein, was durch die vom Grid-Administrator festgelegte maximale Aufbewahrungsfrist zulässig ist.

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 beim Tenant Manager mit einem angemeldet"Unterstützter Webbrowser".
- Sie gehören zu einer Benutzergruppe mit dem "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
Governance	• Benutzer mit der `s3:BypassGovernanceRetention` Berechtigung können den Anforderungskopf verwenden `x-amz-bypass-governance-retention: true`, um die 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.

Standardaufbewahrungsmodus	Beschreibung
Compliance	• 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. **Hinweis**: Ihr Grid-Administrator muss Ihnen erlauben, den Compliance-Modus zu verwenden.

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 an, der kleiner oder gleich der maximalen Aufbewahrungsfrist für den Mandanten ist, wie vom Grid-Administrator festgelegt.

   Eine *maximale* Aufbewahrungsfrist, die ein Wert von 1 Tag bis 100 Jahre sein kann, wird festgelegt, wenn der Grid-Administrator den Mandanten erstellt. Wenn Sie eine *default* Aufbewahrungsfrist festlegen, darf sie den für die maximale Aufbewahrungsfrist festgelegten Wert nicht überschreiten. Bitten Sie bei Bedarf Ihren Grid-Administrator, die maximale Aufbewahrungsfrist zu verlängern oder zu verkürzen.

7. Wählen Sie **Änderungen speichern**.

Konfigurieren Sie StorageGRID CORS für Buckets und Objekte

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 beim Tenant Manager mit einem angemeldet"Unterstützter Webbrowser".
- Für GET CORS-Konfigurationsanforderungen gehören Sie einer Benutzergruppe an, die den hat"Managen aller Buckets oder Anzeigen aller Buckets Berechtigung". Diese Berechtigungen überschreiben die Berechtigungseinstellungen in Gruppen- oder Bucket-Richtlinien.
- Für PUT CORS-Konfigurationsanforderungen gehören Sie einer Benutzergruppe "Alle Berechtigungen für Buckets managen"an, die den hat. Diese Berechtigung überschreibt die Berechtigungseinstellungen in Gruppen- oder Bucket-Richtlinien.
- Der "Root-Zugriffsberechtigung" bietet Zugriff auf alle CORS-Konfigurationsanforderungen.

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 die Konfiguration von CORS für den `Images` Bucket können Sie die Bilder in diesem Bucket auf der Website anzeigen lassen `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. Im Detail:
   - Ermöglicht jeder Domäne, GET-Anforderungen an den Bucket zu senden
   - Ermöglicht der Domäne nur `http://www.example.com` das Senden von GET-, POST- und LÖSCHANFRAGEN
   - Alle Anforderungskopfzeilen 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 User 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**.

Verwandte Informationen

"Konfigurieren Sie StorageGRID CORS für eine Verwaltungsschnittstelle"

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 Bucket hat"S3-Objektsperre aktiviert", könnte er für *Jahre* im Status **delete objects: Read-only** verbleiben.

  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. Siehe Informationen zum Löschen von Objekten in einem Bucket in "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 für diesen Bucket hinzufügt, "Deaktivieren Sie die Grid-übergreifende Replizierung"bevor alle Bucket-Objekte gelöscht werden.

Bevor Sie beginnen

- Sie sind beim Tenant Manager mit einem angemeldet"Unterstützter Webbrowser".
- Sie gehören zu einer Benutzergruppe mit dem "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

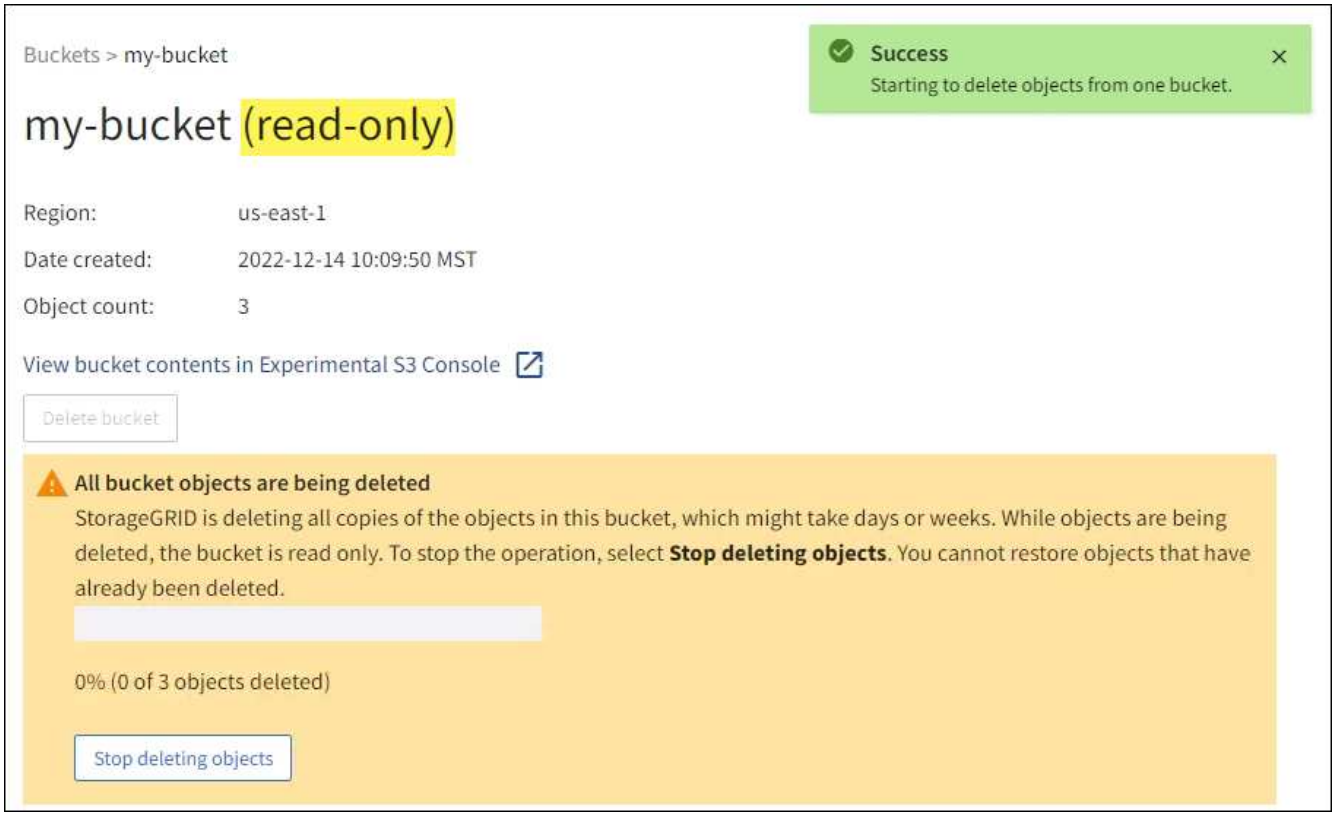
   a. Wählen Sie einen Bucket-Namen aus, um die Details anzuzeigen.

   b. Wählen Sie **Objekte im Bucket löschen**.

3. Wenn das Bestätigungsdialogfeld 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.

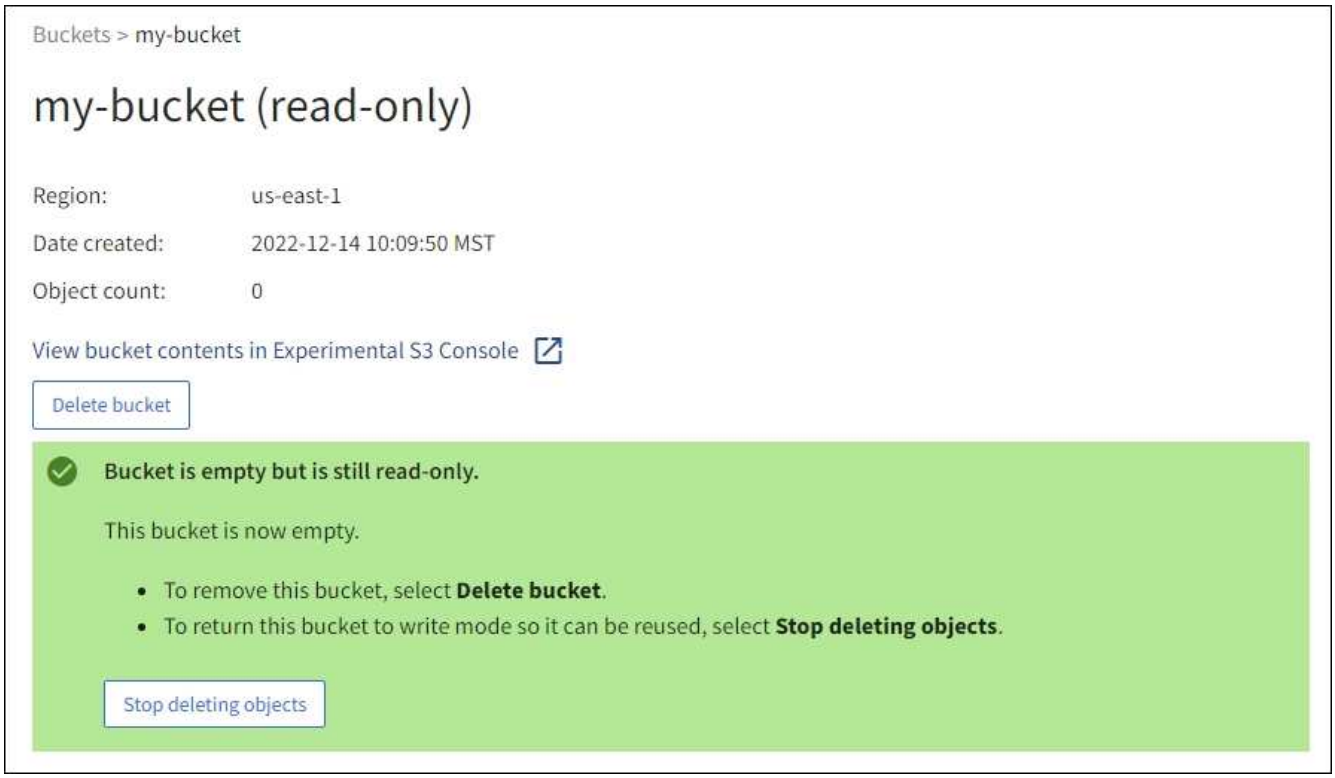


5. Wählen Sie, wie erforderlich, während der Vorgang ausgeführt wird, **Löschen von Objekten stoppen**, um den Prozess anzuhalten. Wählen Sie dann optional **Objekte im Bucket löschen** aus, um den Prozess fortzusetzen.

   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 Löschmarkierungen erhalten. Um den Bucket zu löschen, müssen Sie alle verbleibenden Löschmarkierungen 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 beim Tenant Manager mit einem angemeldet"Unterstützter Webbrowser".
- Sie gehören zu einer Benutzergruppe mit dem "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, *Not* 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 mithilfe der oder der löschen"Mandantenmanagement-API""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 Bestätigungsdialogfeld 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. Sie müssen "Löschen Sie alle Objekte und alle Löschmarkierungen im Bucket"den Bucket löschen, bevor Sie ihn 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 beim Tenant Manager mit einem 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. Sehen "Verwendung von Bucket- und Gruppenzugriffsrichtlinien" .
- Sie kennen die Zugriffsschlüssel-ID und den geheimen Zugriffsschlüssel des Benutzers. Optional haben Sie eine `.csv` Datei, die diese Informationen enthält. Siehe "Anweisungen zum Erstellen von Zugriffsschlüsseln".

Schritte

1. Wählen Sie **Speicher** > **Buckets** > ***Bucketname***.
2. Wählen Sie die Registerkarte S3-Konsole aus.
3. Fügen Sie die Zugriffsschlüssel-ID und den geheimen Zugriffsschlüssel in die Felder ein. Andernfalls wählen Sie **Zugriffsschlüssel hochladen** und wählen Sie Ihre `.csv` Datei aus.
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. Zum Beispiel würde eine Suche nach `folder1/folder2/somefile-` Objekte zurückgeben, die sich innerhalb des Ordners befinden `folder1/folder2/` und mit dem Wort beginnen `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

S3-Plattform-Services

Platform Services – Übersicht und Überlegungen

Bevor Sie Plattformservices implementieren, sollten Sie sich die Übersicht und die Überlegungen zur Verwendung dieser Services ansehen.

Informationen zu S3 finden Sie unter "S3-REST-API VERWENDEN".

Überblick über die Plattform-Services

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.

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 können Sie sowohl die als auch "Benachrichtigungen"einen StorageGRID S3 Bucket konfigurieren, damit Sie bestimmte Objekte auf den Amazon Simple Storage Service (S3) spiegeln können. Gleichzeitig könnten "CloudMirror Service"Sie eine Benachrichtigung über jedes dieser Objekte an die Monitoring-Applikation eines Drittanbieters senden, um Ihre AWS Ausgaben nachzuverfolgen.

> 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

Plattformdienste kommunizieren mit externen Endpunkten, die Sie mithilfe der"Mandanten-Manager" oder die"Mandantenmanagement-API" . Jeder Endpunkt stellt ein externes Ziel dar, beispielsweise einen StorageGRID S3-Bucket, einen Amazon Web Services-Bucket, ein Amazon SNS-Thema, einen Webhook-Endpunkt oder einen Elasticsearch-Cluster, der lokal, auf AWS oder anderswo gehostet wird.

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 alle Objekte, deren Schlüssel mit beginnen, in einen Amazon S3-Bucket repliziert werden sollen `/images`, 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 Benachrichtigungskonfiguration für Metadaten 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	• GetBucketReplication • PutBucketReplication	• "Replizierung von CloudMirror" • "Operationen auf Buckets"
Benachrichtigungen	• GetBucketNotificationConfiguration • PutBucketNotificationKonfiguration	• "Benachrichtigungen" • "Operationen auf Buckets"
Integration von Suchen	• Konfiguration der Bucket-Metadaten-Benachrichtigungen ABRUFEN • PUT Bucket-Metadaten-Benachrichtigungskonfiguration	• "Integration von Suchen" • "Benutzerdefinierte Operationen von StorageGRID"

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.
Drosselung des Zielendpunkts	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. 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 Aufnahmerate 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. 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.

Überlegungen	Details
Bestellgarantien	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. 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.
ILM-gesteuerte Objektlöschungen	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. Suchintegrationsanfragen werden dagegen gesendet, wenn Objekte aufgrund von ILM gelöscht werden.
Kafka-Endpunkte werden verwendet	Bei Kafka-Endpunkten wird gegenseitiges TLS nicht unterstützt. Wenn Sie daher in Ihrer Kafka-Broker-Konfiguration auf festgelegt `required` haben `ssl.client.auth`, kann dies zu Problemen mit der Konfiguration von Kafka-Endpunkten führen. 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 Benutzername und Kennwort-Anmeldeinformationen. • SASL/PLAIN • SASL/SCRAM-SHA-256 • SASL/SCRAM-SHA-512 **Hinweis:** konfigurierte Speicher-Proxy-Einstellungen gelten nicht für Kafka-Plattform-Services-Endpunkte.

Überlegungen bei der Verwendung des CloudMirror Replikationsservice

Überlegungen	Details
Replikationsstatus	Der Header wird von StorageGRID nicht unterstützt `x-amz-replication-status`.

Überlegungen	Details
Objektgröße	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 *unterstützte* Objektgröße. **Hinweis**: Die maximale *recommended* 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.
Bucket-Versionierung und VersionIDs	Wenn die Versionierung im S3-Quell-Bucket von StorageGRID aktiviert ist, sollten Sie auch die Versionierung für den Ziel-Bucket aktivieren. 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. **Hinweis**: Versions-IDs für den Quell-Bucket in StorageGRID hängen nicht mit den Versions-IDs für den Ziel-Bucket zusammen.
Tagging für Objektversionen	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. 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.
Mehrteilige Uploads und `ETag` Werte	Bei der Spiegelung von Objekten, die mittels eines mehrteiligen Uploads hochgeladen wurden, bleiben die Teile vom CloudMirror-Service nicht erhalten. Daher weicht der `ETag` Wert für das gespiegelte Objekt vom Wert des ursprünglichen Objekts ab `ETag`.
Mit SSE-C verschlüsselte Objekte (serverseitige Verschlüsselung mit vom Kunden bereitgestellten Schlüsseln)	Der CloudMirror-Dienst unterstützt keine Objekte, die mit SSE-C verschlüsselt sind. Wenn Sie versuchen, ein Objekt für die CloudMirror-Replikation in den Quell-Bucket aufzunehmen und die Anforderung die SSE-C-Anforderungsheader enthält, schlägt der Vorgang fehl.
Bucket mit S3-Objektsperre aktiviert	Die Replizierung wird für Quell- oder Ziel-Buckets nicht unterstützt, wenn S3 Object Lock aktiviert ist.

Verstehen Sie den CloudMirror Replizierungsservice

Sie können die CloudMirror-Replizierung für einen S3-Bucket aktivieren, wenn StorageGRID bestimmte Objekte replizieren soll, die dem Bucket hinzugefügt wurden, in

einen oder mehrere externe Ziel-Buckets.

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.

CloudMirror und ILM

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.

CloudMirror und Grid-Replizierung

Die CloudMirror-Replizierung weist wichtige Ähnlichkeiten und Unterschiede zur Grid-übergreifenden Replizierungsfunktion auf. Siehe "Vergleichen Sie Grid-Replizierung und CloudMirror Replizierung".

CloudMirror und S3-Buckets

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.

Vorhandene Buckets

Wenn Sie die CloudMirror-Replizierung für einen vorhandenen Bucket aktivieren, werden nur die neuen Objekte repliziert, die diesem Bucket hinzugefügt wurden. 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.

Mehrere Ziel-Buckets

Um Objekte in einem einzelnen Bucket auf mehrere Ziel-Buckets zu replizieren, geben Sie das Ziel für jede Regel in der XML-Replikationskonfiguration an. Ein Objekt kann nicht gleichzeitig in mehr als einen Bucket repliziert werden.

Versionierte oder unversionierte Buckets

Die CloudMirror-Replizierung kann für versionierte oder unversionierte Buckets konfiguriert werden. Ziel-Buckets können mit einer Versionskontrolle oder ohne Versionskontrolle versioniert werden. 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.

Löschen, Replikations-Loops und Ereignisse

Löschverhalten

Entspricht dem Löschverhalten des Amazon S3-Dienstes, Cross-Region Replication (CRR). Durch das Löschen eines Objekts in einem Quell-Bucket wird niemals ein repliziertes Objekt auf dem Ziel gelöscht. Wenn sowohl Quell- als auch Ziel-Buckets versioniert sind, wird die Löschmarkierung repliziert. Wenn der Ziel-Bucket nicht versioniert ist, repliziert das Löschen eines Objekts im Quell-Bucket nicht die Löschmarkierung auf den Ziel-Bucket oder löscht das Zielobjekt nicht.

Schutz vor Replikations-Loops

Wenn Objekte in den Ziel-Bucket repliziert werden, kennzeichnet StorageGRID sie als „Replikate“. Ein Ziel-StorageGRID-Bucket repliziert nicht wieder als Replikate markierte Objekte und schützt Sie vor versehentlichen Replikations-Loops. Diese Replikatmarkierung ist intern bei StorageGRID und hindert Sie nicht daran, AWS CRR zu nutzen, wenn Sie einen Amazon S3-Bucket als Ziel verwenden.

Der benutzerdefinierte Header, der 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.

Ereignisse im Ziel-Bucket

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.

Informieren Sie sich über Benachrichtigungen für Buckets

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

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.

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 den Schlüssel in der Ereignismeldung verwenden `sequencer`, um die Reihenfolge der Ereignisse für ein bestimmtes Objekt zu bestimmen, wie in der Amazon S3-Dokumentation beschrieben.

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

- 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 Suchintegrationsservice ist ein individueller StorageGRID-Service, der S3-Objektmetadaten automatisch und asynchron an einen Zielendpunkt sendet, wenn ein Objekt erstellt oder gelöscht oder seine Metadaten oder Tags 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 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 mit aktivierter S3 Object Lock konfiguriert werden, die S3 Object Lock-Metadaten (einschließlich des Aufbewahrungsdatums und des Status der Legal Hold) der Objekte werden jedoch nicht in die an Elasticsearch gesendeten Metadaten aufgenommen.

> Da der Suchintegrationsdienst dazu führt, dass Objektmetadaten an ein Ziel gesendet werden, wird seine Konfigurations-XML als "*Metadaten* Benachrichtigungskonfiguration XML" bezeichnet. Diese Konfigurations-XML unterscheidet sich von der XML-Benachrichtigungskonfiguration, die für die Aktivierung von *Event*-Benachrichtigungen verwendet wird.

Suchintegration und S3 Buckets

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.

Metadatenbenachrichtigungen werden in Form eines JSON-Dokuments mit dem Namen, der ggf. den Bucket-Namen, den Objektnamen und die Version-ID enthält generiert. 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 suchen

Metadatenbenachrichtigungen werden immer dann generiert und in die Warteschlange für die Zustellung gestellt, wenn:

- 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 befanden. 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.

Suchintegrationsservice und Elasticsearch

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 den "NetApp Interoperabilitäts-Matrix-Tool", um die unterstützten Versionen von Elasticsearch zu bestimmen.

Verwalten von Plattform-Services-Endpunkten

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 Plattformdienste 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?

Ein Endpunkt für Plattformdienste gibt 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, Kafka und Webhook-Endpunkte. Simple Queue Service (SQS) und AWS Lambda-Endpunkte werden nicht unterstützt.

Für Kafka-Endpunkte wird Mutual TLS nicht unterstützt. Wenn Sie also `ssl.client.auth` eingestellt auf `required` in Ihrer Kafka-Broker-Konfiguration kann es zu Problemen bei der Kafka-Endpunktkonfiguration kommen.

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 Plattformdienst 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 der Plattformdienste muss mit entweder oder `urn:mysite`, wie folgt beginnen `arn:aws`:

- 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 Dienst lokal gehostet wird, verwenden Sie `urn:mysite`

Wenn Sie beispielsweise die URN für einen CloudMirror-Endpunkt angeben, der auf StorageGRID gehostet wird, beginnt die URN möglicherweise mit `urn:sgws`.

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

Service	Typ
Replizierung von CloudMirror	`s3`
Benachrichtigungen	`sns`, `kafka` , oder `webhook`
Integration von Suchen	`es`

Wenn Sie beispielsweise weiterhin die URN für einen CloudMirror-Endpunkt angeben möchten, der auf StorageGRID gehostet wird, fügen Sie zu get `urn:sgws:s3` hinzu `s3`.

Bei den meisten Endpunkten identifiziert das letzte Element der URN die spezifische Zielressource an der Ziel-URI, zum Beispiel: `sns-topic-name` .

Bei Webhook-Endpunkten ist die Zielressource die Ziel-URI selbst.

Service	Bestimmte Ressource
Replizierung von CloudMirror	`bucket-name`
Benachrichtigungen	`sns-topic-name` Oder `kafka-topic-name` **Hinweis:** Bei Webhook-Endpunkten kann das letzte Element der URN eine beliebige Zeichenfolge sein, solange die URN des Endpunkts eindeutig ist.
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 Endpunkt 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 Endpunkt der AWS-Suchintegration muss der `domain-name` die Literalzeichenfolge enthalten `domain/`, wie hier dargestellt.

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:mysite:s3:optional:optional:bucket-name
```

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

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

- Benachrichtigungen:

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

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

  Geben Sie einen Kafka-Endpunkt an:

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

  Geben Sie einen Webhook-Endpunkt an:

  ```
  urn:mysite:webhook:optional:optional:webhook-name
  ```

- Integration von Suchen:

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

  > ⓘ Für lokal gehostete Suchendpunkte kann das `domain-name` Element eine beliebige Zeichenfolge sein, solange die URN des Endpunkts eindeutig ist.

Endpunkt für Plattformservices erstellen

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

Bevor Sie beginnen

- Sie sind beim Tenant Manager mit einem angemeldet"Unterstützter Webbrowser".
- Die Plattformservices wurden für Ihr Mandantenkonto von einem StorageGRID-Administrator aktiviert.
- Sie gehören zu einer Benutzergruppe mit dem "Verwalten von Endpunkten oder Root-Zugriffsberechtigungen".
- Die vom Plattformdienste-Endpunkt referenzierte Ressource wurde erstellt:
  - CloudMirror Replizierung: S3 Bucket

- Ereignisbenachrichtigung: Amazon Simple Notification Service (Amazon SNS)-Thema, Kafka-Thema oder Webhook-Endpunkt
- Suchbenachrichtigung: Elasticsearch-Index, wenn der Zielcluster nicht für die automatische Erstellung von Indizes konfiguriert ist.

- 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 für die Suchintegration

    Für Endpunkte der Suchintegration können Sie die folgenden Anmeldeinformationen verwenden:

    - Zugriffsschlüssel: Zugriffsschlüssel-ID und geheimer Zugriffsschlüssel
    - Basic HTTP: Benutzername und Passwort

    Endpunkte der CloudMirror Replizierung

    Für CloudMirror-Replikations-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.

    Amazon SNS-Endpunkte

    Für Amazon SNS-Endpunkte können Sie die folgenden Anmeldeinformationen verwenden:

    - Zugriffsschlüssel: Zugriffsschlüssel-ID und geheimer Zugriffsschlüssel

    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 (falls eine Zertifikatsüberprüfung erforderlich ist)
- 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 Typ des Plattformdienstes, den der Endpunkt unterstützt, wird neben dem Endpunktnamen angezeigt, wenn dieser auf der Seite „Endpunkte“ aufgeführt ist. Sie müssen diese Information also 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 (High Availability, Hochverfügbarkeit) dar und `10443` stellt den im Load Balancer-Endpunkt definierten Port dar.

   > 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.

Wenn Sie eine Authentifizierung für Webhook-Endpunkte wünschen, konfigurieren Sie Mutual Transport Layer Security (mTLS) inSchritt 9 .

Endpunkte für die Suchintegration

Geben Sie die Anmeldeinformationen für einen Endpunkt für die Suchintegration 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	• Zugriffsschlüssel-ID • Geheimer Zugriffsschlüssel
Basis-HTTP	Verwendet einen Benutzernamen und ein Passwort, um Verbindungen zum Ziel zu authentifizieren.	• Benutzername • Passwort

Endpunkte der CloudMirror Replizierung

Geben Sie die Anmeldeinformationen für einen CloudMirror-Replikations-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	• Zugriffsschlüssel-ID • Geheimer Zugriffsschlüssel

Authentifizierungstyp	Beschreibung	Anmeldedaten
KAPPE (C2S-Zugangsportal)	Verwendet Zertifikate und Schlüssel zur Authentifizierung von Verbindungen zum Ziel.	• 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)

Amazon SNS-Endpunkte

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

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

Authentifizierungstyp	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	• Zugriffsschlüssel-ID • Geheimer Zugriffsschlüssel

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.

Authentifizierungstyp	Beschreibung	Anmeldedaten
Anonym	Gibt anonymen Zugriff auf das Ziel. Funktioniert nur für Endpunkte, bei denen die Sicherheit deaktiviert ist.	Keine Authentifizierung.

Authentifizierungstyp	Beschreibung	Anmeldedaten
SASL/PLAIN	Verwendet einen Benutzernamen und ein Kennwort mit Klartext, um Verbindungen zum Ziel zu authentifizieren.	• 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.	• Benutzername • Passwort
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.	• 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.

8. Wählen Sie **Weiter**.
9. Wählen Sie ein Optionsfeld für **Zertifikate überprüfen**, um auszuwählen, wie die TLS-Verbindung zum Endpunkt überprüft wird.

Die meisten Endpunkte

Überprüfen Sie die TLS-Verbindung für Suchintegration, CloudMirror-Replikation, Amazon SNS oder Kafka-Endpunkte.

Typ der Zertifikatverifizierung	Beschreibung
TLS	Validiert das Serverzertifikat für TLS-Verbindungen zur Endpunktressource.
Deaktiviert	Die Zertifikatsüberprüfung ist deaktiviert. Diese Option ist nicht sicher.
Benutzerdefiniertes CA-Zertifikat verwenden	Das benutzerdefinierte CA-Zertifikat wird verwendet, um die Identität des Servers beim Herstellen einer Verbindung mit dem Endpunkt zu überprüfen.
Verwenden Sie das CA-Zertifikat für das Betriebssystem	Verwenden Sie das auf dem Betriebssystem installierte Standard-Grid-CA-Zertifikat, um Verbindungen zu sichern.

Nur Webhook-Endpunkte

Überprüfen Sie die TLS-Verbindung für Webhook-Endpunkte.

Typ der Zertifikatverifizierung	Beschreibung
TLS	Validiert das Serverzertifikat für TLS-Verbindungen zur Endpunktressource.
mTLS	Validiert die Client- und Serverzertifikate für gegenseitige TLS-Verbindungen zur Endpunktressource.
Deaktiviert	Die Zertifikatsüberprüfung ist deaktiviert. Diese Option ist nicht sicher.
Benutzerdefiniertes CA-Zertifikat verwenden	Das benutzerdefinierte CA-Zertifikat wird verwendet, um die Identität des Servers beim Herstellen einer Verbindung mit dem Endpunkt zu überprüfen.

Wenn Sie **mTLS** auswählen, werden diese Optionen verfügbar.

Typ der Zertifikatverifizierung	Beschreibung
Serverzertifikat nicht überprüfen	Deaktiviert die Serverzertifikatsüberprüfung, was bedeutet, dass die Identität des Servers nicht überprüft wird. Diese Option ist nicht sicher.
Client-Zertifikat	Das Client-Zertifikat wird verwendet, um die Identität des Clients bei der Verbindung mit dem Endpunkt zu überprüfen.

Typ der Zertifikatverifizierung	Beschreibung
Privater Clientschlüssel	Der private Schlüssel für das Client-Zertifikat. Bei Verschlüsselung muss das traditionelle Format PKCS #1 verwendet werden (das Format PKCS #8 wird nicht unterstützt).
Passphrase für den privaten Clientschlüssel	Die Passphrase zum Entschlüsseln des privaten Clientschlüssels. Wenn der private Schlüssel nicht verschlüsselt ist, lassen Sie dieses Feld leer.

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 beim Tenant Manager mit einem angemeldet"Unterstützter Webbrowser".
- Sie gehören zu einer Benutzergruppe mit dem "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.

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

   Die Seite mit den Details des Endpunkts wird angezeigt.

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 beim Tenant Manager mit einem angemeldet"Unterstützter Webbrowser".
- Sie gehören zu einer Benutzergruppe mit dem "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.

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 Symbol Bearbeiten .
   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 von Zertifikaten.

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 Plattformdienst nicht mehr verwenden möchten.

Bevor Sie beginnen

- Sie sind beim Tenant Manager mit einem angemeldet"Unterstützter Webbrowser".
- Sie gehören zu einer Benutzergruppe mit dem "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.

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 Plattformdienst 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.

4. Wählen Sie **Endpunkt löschen**.

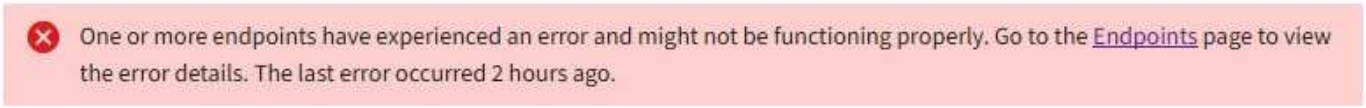
Fehlerbehebung bei Endpunktfehlern bei Plattform-Services

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.



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, traten innerhalb der letzten 7 Tage auf.

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 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

Um die CloudMirror-Replizierung für einen Bucket zu aktivieren, erstellen Sie eine gültige XML-Bucket-Replizierungskonfiguration und wenden sie an.

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 zu einer Benutzergruppe mit dem "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.

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

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".

Beachten Sie bei der Konfiguration der CloudMirror-Replikation die folgenden Anforderungen und Merkmale:

- Wenn Sie eine gültige XML-Bucket-Replizierungskonfiguration erstellen und anwenden, muss diese für jedes Ziel die URN eines S3-Bucket-Endpunkts verwenden.
- Die Replizierung wird für Quell- oder Ziel-Buckets nicht unterstützt, wenn S3 Object Lock aktiviert ist.
- 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 Zielsystemanbieter.

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 des Elements für Regeln nicht unterstützt `Filter` und V1-Konventionen für das Löschen von Objektversionen befolgt. Details finden Sie in der Amazon Dokumentation zur Replizierungskonfiguration.
     - Verwenden Sie den URN eines S3-Bucket-Endpunkts als Ziel.
     - Fügen Sie optional das Element hinzu `<StorageClass>`, und geben Sie eine der folgenden Optionen an:
       - `STANDARD`: Die Standard-Speicherklasse. Wenn Sie beim Hochladen eines Objekts keine Storage-Klasse angeben, wird die `STANDARD` Storage-Klasse verwendet.
       - `STANDARD_IA`: (Standard - seltener Zugang.) Nutzen Sie diese Storage-Klasse für Daten, auf die weniger häufig zugegriffen wird, die bei Bedarf aber noch schnellen Zugriff erfordern.
       - `REDUCED_REDUNDANCY`: Verwenden Sie diese Storage-Klasse für nicht kritische, reproduzierbare Daten, die mit weniger Redundanz gespeichert werden können als die `STANDARD` Storage-Klasse.
     - Wenn Sie in der Konfigurations-XML ein angeben `Role`, wird es 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**.

   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 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

Sie aktivieren Benachrichtigungen für einen Bucket, indem Sie XML für die Benachrichtigungskonfiguration erstellen und den Tenant Manager zum Anwenden des XML-Codes auf einen Bucket verwenden.

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 zu einer Benutzergruppe mit dem "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

Sie konfigurieren Ereignisbenachrichtigungen, indem Sie die Benachrichtigungskonfigurations-XML mit einem Quell-Bucket verknüpfen. Die XML-Benachrichtigungskonfiguration folgt den S3-Konventionen zum Konfigurieren von Bucket-Benachrichtigungen, wobei das Zielthema Amazon SNS, das Kafka-Thema oder der Webhook-Endpunkt als URN eines Endpunkts angegeben wird.

Allgemeine Informationen zu Ereignisbenachrichtigungen und deren Konfiguration finden Sie im "Amazon Dokumentation". Informationen darüber, wie StorageGRID die S3-Bucket-Benachrichtigungs-API implementiert, finden Sie im "Anweisungen zur Implementierung von S3-Client-Applikationen".

Beachten Sie beim Konfigurieren von Ereignisbenachrichtigungen für einen Bucket die folgenden Anforderungen und Merkmale:

- Wenn Sie eine gültige XML-Benachrichtigungskonfiguration erstellen und anwenden, muss die URN eines Ereignisbenachrichtigungs-Endpunkts für jedes Ziel verwendet werden.
- Obwohl die Ereignisbenachrichtigung für einen Bucket mit aktivierter S3 Object Lock konfiguriert werden kann, werden die S3 Object Lock-Metadaten (einschließlich Aufbewahrungszeitraum bis sowie Status der gesetzlichen Sperrzeit) der Objekte in den Benachrichtigungen nicht berücksichtigt.
- Nachdem Sie Ereignisbenachrichtigungen konfiguriert haben, wird jedes Mal, wenn ein bestimmtes Ereignis für ein Objekt im Quell-Bucket eintritt, eine Benachrichtigung generiert und an das als Ziel verwendete Amazon SNS-Thema, Kafka-Thema oder den Webhook-Endpunkt gesendet.
- 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 Tenant Manager **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**.

   > 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, wenn ein Objekt mit dem Präfix erstellt `images/` wird.

   b. Bestätigen Sie, dass eine Benachrichtigung an das Zielthema Amazon SNS, Kafka-Thema oder den Webhook-Endpunkt übermittelt 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":"11111111111111111"
         },
         "requestParameters":{
            "sourceIPAddress":"193.51.100.20"
         },
         "responseElements":{
            "x-amz-request-id":"122047343"
         },
         "s3":{
            "s3SchemaVersion":"1.0",
            "configurationId":"Image-created",
            "bucket":{
               "name":"test1",
               "ownerIdentity":{
                  "principalId":"11111111111111111"
               },
               "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"

- "Endpunkt für Plattformservices erstellen"

Konfigurieren Sie den Suchintegrationsdienst

Sie aktivieren die Suchintegration für einen Bucket, indem Sie XML für die Suchintegration erstellen und den Tenant Manager zum Anwenden des XML-Codes auf den Bucket verwenden.

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 zu einer Benutzergruppe mit dem "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-Integrationsservice 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 Suchintegrationsservice für einen Bucket aktivieren, der bereits Objekte enthält, werden Metadatenbenachrichtigungen nicht automatisch für vorhandene Objekte gesendet. Aktualisieren Sie diese vorhandenen Objekte, um sicherzustellen, dass ihre Metadaten zum Zielsuchindex hinzugefügt werden.

Schritte

1. Suchintegration für einen Bucket aktivieren:
    - Verwenden Sie einen Texteditor, um die XML-XML-Metadatenbenachrichtigung zu erstellen, die für die Integration der Suche erforderlich ist.
    - Verwenden Sie beim Konfigurieren des XML den URN eines Endpunkt zur Integration der Suche als Ziel.

      Objekte können nach dem Präfix des Objektnamens gefiltert werden. Beispielsweise können Sie Metadaten für Objekte mit dem Präfix an ein Ziel und Metadaten für Objekte mit `videos` dem Präfix an ein anderes senden `images`. Konfigurationen mit überlappenden Präfixen sind nicht gültig und werden bei der Übermittlung abgelehnt. Beispielsweise ist eine Konfiguration, die eine Regel für Objekte mit dem Präfix und eine zweite Regel für Objekte mit dem Präfix `test2` enthält `test`, nicht zulässig.

      Bei Bedarf siehe Beispiele für die Metadatenkonfiguration XML.

```
<MetadataNotificationConfiguration>
 <Rule>
    <Status>Enabled</Status>
    <Prefix></Prefix>
    <Destination>
       <Urn>/Urn>
       </Destination>
 </Rule>
</MetadataNotificationConfiguration>
```

Elemente in der XML-Konfigurationskonfiguration für Metadatenbenachrichtigungen:

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
Status	Der Status kann „aktiviert“ oder „deaktiviert“ sein. Für deaktivierte Regeln wird keine Aktion durchgeführt. In das Element Regel aufgenommen.	Ja.
Präfix	Objekte, die mit dem Präfix übereinstimmen, werden von der Regel beeinflusst und ihre Metadaten werden an das angegebene Ziel gesendet. Geben Sie ein leeres Präfix an, um alle Objekte zu entsprechen. In das Element Regel aufgenommen.	Ja.
Ziel	Container-Tag für das Ziel einer Regel. In das Element Regel aufgenommen.	Ja.

Name	Beschreibung	Erforderlich
Urne	URNE des Ziels, an dem Objektmetadaten gesendet werden. Muss der URN eines StorageGRID-Endpunkts mit den folgenden Eigenschaften sein: • `es` Muss das dritte Element sein. • Die URN muss mit dem Index und dem Typ enden, in dem die Metadaten gespeichert sind, in der Form `domain-name/myindex/mytype`. Endpunkte werden mithilfe der Mandanten-Manager oder der Mandanten-Management-API konfiguriert. Sie nehmen folgende Form: • `arn:aws:es:region:account-ID:domain/mydomain/myindex/mytype` • `urn:mysite:es:::mydomain/myindex/mytype` Der Endpunkt muss konfiguriert werden, bevor die Konfigurations-XML gesendet wird, oder die Konfiguration schlägt mit einem Fehler 404 fehl. URNE ist im Element Ziel enthalten.	Ja.

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**.

   Plattformservices 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:
   a. 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.

Beispiel: Konfiguration der Metadatenbenachrichtigung, die für alle Objekte gilt

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>
```

Beispiel: Konfiguration der Metadatenbenachrichtigung mit zwei Regeln

In diesem Beispiel werden Objektmetadaten für Objekte mit dem Präfix `/images` an ein Ziel gesendet, während Objektmetadaten für Objekte mit dem Präfix `/videos` an ein zweites Ziel gesendet werden.

```
<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-1:22222222:domain/es-
domain/graphics/videotype</Urn>
        </Destination>
    </Rule>
</MetadataNotificationConfiguration>
```

Benachrichtigungsformat für Metadaten

Wenn Sie den Such-Integrationsservice für einen Bucket aktivieren, wird ein JSON-Dokument generiert und an den Zielendpunkt gesendet, wenn Metadaten oder Tags hinzugefügt, aktualisiert oder gelöscht werden.

Dieses Beispiel zeigt ein Beispiel für den JSON, der generiert werden könnte, wenn ein Objekt mit dem Schlüssel in einem Bucket mit `SGWS/Tagging.txt` dem Namen erstellt wird `test`. Der `test` Bucket ist nicht versioniert, daher ist das `versionId` Tag leer.

```
{
  "bucket": "test",
  "key": "SGWS/Tagging.txt",
  "versionId": "",
  "accountId": "86928401983529626822",
  "size": 38,
  "md5": "3d6c7634a85436eee06d43415012855",
  "region":"us-east-1",
  "metadata": {
    "age": "25"
  },
  "tags": {
    "color": "yellow"
  }
}
```

Im JSON-Dokument enthaltene Felder

Der Dokumentname umfasst, falls vorhanden, den Bucket-Namen, den Objektnamen und die Version-ID.

Bucket- und Objektinformationen

`bucket`: Name des Eimer

`key`: Name des Objektschlüssels

`versionID`: Objektversion, für Objekte in versionierten Buckets

`region`: Bucket-Region, zum Beispiel `us-east-1`

System-Metadaten

`size`: Objektgröße (in Bytes) als für einen HTTP-Client sichtbar

`md5`: Objekt-Hash

Benutzer-Metadaten

`metadata`: Alle Benutzermetadaten für das Objekt, als Schlüssel-Wert-Paare

`key:value`

Tags

`tags`: Alle Objektanhänger, die für das Objekt definiert sind, als Schlüssel-Wert-Paare

`key:value`

So zeigen Sie Ergebnisse in Elasticsearch an

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. Aktivieren Sie die dynamischen Feldzuordnungen auf dem Index, 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 STS, S3 und HTTP:

Element	Version
STS AssumeRole-API-Spezifikation	"Amazon Web Services (AWS)-Dokumentation: Amazon Assumerole API-Referenz" Weitere Informationen zu AssumeRole finden Sie unter"Einrichten von AssumeRole" .
S3-API-Spezifikation	"AWS-Dokumentation: Amazon Simple Storage Service API-Referenz"
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
12,0	• Unterstützung für Cross-Origin Resource Sharing (CORS) für eine Verwaltungsschnittstelle hinzugefügt, die es einer anderen Domäne ermöglicht, mithilfe von Verwaltungs-APIs auf Daten in StorageGRID zuzugreifen. "Weitere Informationen ." . • Unterstützung für STS AssumeRole und Sitzungsrichtlinie hinzugefügt. Sehen "ein Beispiel für eine Sitzungsrichtlinie" . Sie können AssumeRole unter Mandantengruppen einrichten.

Freigabe	Kommentare
11,9	• Unterstützung für vorberechnete SHA-256-Prüfsummenwerte für die folgenden Anforderungen und unterstützten Header wurde hinzugefügt. Mit dieser Funktion können Sie die Integrität hochgeladener Objekte überprüfen: ◦ CompleteMultipartUpload: `x-amz-checksum-sha256` ◦ CreateMultipartUpload: `x-amz-checksum-algorithm` ◦ GetObject: `x-amz-checksum-mode` ◦ Kopfobjekt: `x-amz-checksum-mode` ◦ ListenTeile ◦ PutObject: `x-amz-checksum-sha256` ◦ UploadPart: `x-amz-checksum-sha256` • Der Grid-Administrator kann die Aufbewahrungs- und Compliance-Einstellungen auf Mandantenebene kontrollieren. Diese Einstellungen wirken sich auf die Einstellungen der S3-Objektsperre aus. ◦ Standardaufbewahrungsmodus und Objektaufbewahrungsmodus mit Buckets: Governance oder Compliance, sofern vom Grid-Administrator zugelassen. ◦ Standardaufbewahrungszeitraum für Bucket und Objektaufbewahrung bis Datum: Muss kleiner oder gleich dem sein, was durch den vom Grid-Administrator festgelegten maximalen Aufbewahrungszeitraum zulässig ist. • Verbesserte Unterstützung von `aws-chunked` Kodierungs- und Streaming-Werten für Inhalte `x-amz-content-sha256`. Einschränkungen: ◦ Falls vorhanden, `chunk-signature` ist optional und nicht validiert ◦ Wenn vorhanden, `x-amz-trailer` wird der Inhalt ignoriert
11,8	Die Namen der S3-Vorgänge wurden aktualisiert, um sie mit den in der verwendeten Namen "Amazon Web Services (AWS) Dokumentation: Amazon Simple Storage Service API Reference" zu vergleichen.
11,7	• Hinzugefügt "Schnelle Referenz: Unterstützte S3-API-Anforderungen". • Zusätzliche Unterstützung für die Verwendung DES GOVERNANCE-Modus mit S3 Object Lock. • Unterstützung für den StorageGRID-spezifischen Antwortheader für GET Object- und HEAD-Objektanforderungen wurde hinzugefügt `x-ntap-sg-cgr-replication-status`. Dieser Header stellt den Replikationsstatus eines Objekts für die Grid-übergreifende Replikation bereit. • SelectObjectContent Requests unterstützen nun Parkett-Objekte.

Freigabe	Kommentare
11,6	• Unterstützung für die Verwendung des Anforderungsparameters in GET Object und HEAD Object Requests hinzugefügt `partNumber`. • Zusätzliche Unterstützung für einen Standardaufbewahrungsmodus und einen Standardaufbewahrungszeitraum auf Bucket-Ebene für S3 Object Lock. • Unterstützung für den Richtlinienzustandsschlüssel hinzugefügt `s3:object-lock-remaining-retention-days`, um den Bereich der zulässigen Aufbewahrungsfristen für Ihre Objekte festzulegen. • Die maximale *recommended*-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	• 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 `Content-MD5` Anforderungskopf wird jetzt korrekt unterstützt.
11,4	• 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. • Unterstützung für Bucket-Benachrichtigungen für den Ereignistyp hinzugefügt `s3:ObjectRestore:Post`. • 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
11,3	• Zusätzliche Unterstützung für serverseitige Verschlüsselung von Objektdaten mit vom Kunden bereitgestellten Schlüsseln (SSE-C). • Unterstützung für DIE Lebenszyklusoperationen „DELETE“, „GET“ und „PUT“ (nur Ablaufaktion) und für den Antwortheader hinzugefügt `x-amz-expiration`. • 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.

Freigabe	Kommentare
11,2	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. **Hinweis:** die Verwendung von ARN/URN in anderen Konfigurationen JSON/XML, einschließlich derjenigen, die in benutzerdefinierten StorageGRID-Funktionen verwendet werden, hat sich nicht geändert.
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 PutOverwriteObject.
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	Erste Unterstützung der S3 REST API durch das StorageGRID -System. Die derzeit unterstützte Version der *Simple Storage Service API Reference* ist 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"

"AbortMehrteilaUpload"

URI-Abfrageparameter und Anforderungskopfzeilen

StorageGRID unterstützt alle Allgemeine Parameter und Kopfzeilendieser Anforderung sowie den zusätzlichen URI-Abfrageparameter:

- `uploadId`

Text anfordern

Keine

StorageGRID-Dokumentation

"Vorgänge für mehrteilige Uploads"

"CompleteMultipartUpload"

URI-Abfrageparameter und Anforderungskopfzeilen

StorageGRID unterstützt alle Allgemeine Parameter und Kopfzeilendieser Anforderung sowie den zusätzlichen URI-Abfrageparameter:

- `uploadId`
- `x-amz-checksum-sha256`

Text-XML-Tags anfordern

StorageGRID unterstützt folgende XML-Tags für Anforderungstext:

- `ChecksumSHA256`
- `CompleteMultipartUpload`

- `ETag`
- `Part`
- `PartNumber`

StorageGRID-Dokumentation

"CompleteMultipartUpload"

"CopyObject"

URI-Abfrageparameter und Anforderungskopfzeilen

StorageGRID unterstützt alle Allgemeine Parameter und Kopfzeilendieser Anforderung sowie die folgenden 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 Kopfzeilendieser Anforderung sowie die folgenden 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 Kopfzeilendieser Anforderung sowie die folgenden zusätzlichen Kopfzeilen:

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

StorageGRID-Dokumentation

"Operationen auf Buckets"

"DeleteBucketCors"

URI-Abfrageparameter und Anforderungskopfzeilen

StorageGRID unterstützt alle Allgemeine Parameter und Kopfzeilendieser Anforderung.

Text anfordern

Keine

StorageGRID-Dokumentation

"Operationen auf Buckets"

"DeleteBucketEncryption"

URI-Abfrageparameter und Anforderungskopfzeilen

StorageGRID unterstützt alle Allgemeine Parameter und Kopfzeilendieser Anforderung.

Text anfordern

Keine

StorageGRID-Dokumentation

"Operationen auf Buckets"

"DeleteBucketLifecycle"

URI-Abfrageparameter und Anforderungskopfzeilen

StorageGRID unterstützt alle Allgemeine Parameter und Kopfzeilendieser Anforderung.

Text anfordern

Keine

StorageGRID-Dokumentation

- "Operationen auf Buckets"
- "S3-Lebenszykluskonfiguration erstellen"

"DeleteBucketRichtlinien"

URI-Abfrageparameter und Anforderungskopfzeilen

StorageGRID unterstützt alle Allgemeine Parameter und Kopfzeilendieser Anforderung.

Text anfordern

Keine

StorageGRID-Dokumentation

"Operationen auf Buckets"

"DeleteBucketReplication"

URI-Abfrageparameter und Anforderungskopfzeilen

StorageGRID unterstützt alle Allgemeine Parameter und Kopfzeilendieser Anforderung.

Text anfordern

Keine

StorageGRID-Dokumentation

"Operationen auf Buckets"

"DeleteBucketTagging"

URI-Abfrageparameter und Anforderungskopfzeilen

StorageGRID unterstützt alle Allgemeine Parameter und Kopfzeilendieser Anforderung.

Text anfordern

Keine

StorageGRID-Dokumentation

"Operationen auf Buckets"

"DeleteObject"

URI-Abfrageparameter und Anforderungskopfzeilen

StorageGRID unterstützt alle Allgemeine Parameter und Kopfzeilendieser Anforderung plus den folgenden 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 Kopfzeilendieser Anforderung plus den folgenden zusätzlichen Anforderungsheader:

- `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

"Operationen für Objekte"

"DeleteObjectTagging"

StorageGRID unterstützt alle Allgemeine Parameter und Kopfzeilendieser Anforderung.

Text anfordern

Keine

StorageGRID-Dokumentation

"Operationen für Objekte"

"GetBucketAcl"

URI-Abfrageparameter und Anforderungskopfzeilen

StorageGRID unterstützt alle Allgemeine Parameter und Kopfzeilendieser Anforderung.

Text anfordern

Keine

StorageGRID-Dokumentation

"Operationen auf Buckets"

"GetBucketCors"

URI-Abfrageparameter und Anforderungskopfzeilen

StorageGRID unterstützt alle Allgemeine Parameter und Kopfzeilendieser Anforderung.

Text anfordern

Keine

StorageGRID-Dokumentation

"Operationen auf Buckets"

"GetBucketEncryption"

URI-Abfrageparameter und Anforderungskopfzeilen

StorageGRID unterstützt alle Allgemeine Parameter und Kopfzeilendieser Anforderung.

Text anfordern

Keine

StorageGRID-Dokumentation

"Operationen auf Buckets"

"GetBucketLifecycleKonfiguration"

URI-Abfrageparameter und Anforderungskopfzeilen

StorageGRID unterstützt alle Allgemeine Parameter und Kopfzeilendieser Anforderung.

Text anfordern

Keine

StorageGRID-Dokumentation

- "Operationen auf Buckets"
- "S3-Lebenszykluskonfiguration erstellen"

"GetBucketLocation"

URI-Abfrageparameter und Anforderungskopfzeilen

StorageGRID unterstützt alle Allgemeine Parameter und Kopfzeilendieser Anforderung.

Text anfordern

Keine

StorageGRID-Dokumentation

"Operationen auf Buckets"

"GetBucketNotificationConfiguration"

URI-Abfrageparameter und Anforderungskopfzeilen

StorageGRID unterstützt alle Allgemeine Parameter und Kopfzeilendieser Anforderung.

Text anfordern

Keine

StorageGRID-Dokumentation

"Operationen auf Buckets"

"GetBucketPolicy"

URI-Abfrageparameter und Anforderungskopfzeilen

StorageGRID unterstützt alle Allgemeine Parameter und Kopfzeilendieser Anforderung.

Text anfordern

Keine

StorageGRID-Dokumentation

"Operationen auf Buckets"

"GetBucketReplication"

URI-Abfrageparameter und Anforderungskopfzeilen

StorageGRID unterstützt alle Allgemeine Parameter und Kopfzeilendieser Anforderung.

Text anfordern

Keine

StorageGRID-Dokumentation

"Operationen auf Buckets"

"GetBucketTagging"

URI-Abfrageparameter und Anforderungskopfzeilen

StorageGRID unterstützt alle Allgemeine Parameter und Kopfzeilendieser Anforderung.

Text anfordern

Keine

StorageGRID-Dokumentation

"Operationen auf Buckets"

"GetBucketVersioning"

URI-Abfrageparameter und Anforderungskopfzeilen

StorageGRID unterstützt alle Allgemeine Parameter und Kopfzeilendieser Anforderung.

Text anfordern

Keine

StorageGRID-Dokumentation

"Operationen auf Buckets"

"GetObject"

URI-Abfrageparameter und Anforderungskopfzeilen

StorageGRID unterstützt alle Allgemeine Parameter und Kopfzeilen für diese Anforderung plus die folgenden zusätzlichen URI-Abfrageparameter:

- `x-amz-checksum-mode`
- `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 Kopfzeilendieser Anforderung.

Text anfordern

Keine

StorageGRID-Dokumentation

"Operationen für Objekte"

"GetObjectLegalHold"

URI-Abfrageparameter und Anforderungskopfzeilen

StorageGRID unterstützt alle Allgemeine Parameter und Kopfzeilendieser Anforderung.

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 Kopfzeilendieser Anforderung.

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 Kopfzeilendieser Anforderung.

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 Kopfzeilendieser Anforderung.

Text anfordern

Keine

StorageGRID-Dokumentation

"Operationen für Objekte"

"HeadBucket"

URI-Abfrageparameter und Anforderungskopfzeilen

StorageGRID unterstützt alle Allgemeine Parameter und Kopfzeilendieser Anforderung.

Text anfordern

Keine

StorageGRID-Dokumentation

"Operationen auf Buckets"

"HeadObject"

URI-Abfrageparameter und Anforderungskopfzeilen

StorageGRID unterstützt alle Allgemeine Parameter und Kopfzeilendieser Anforderung sowie die folgenden zusätzlichen Kopfzeilen:

- `x-amz-checksum-mode`
- `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 Kopfzeilendieser Anforderung.

Text anfordern

Keine

StorageGRID-Dokumentation

Operationen für den Dienst › ListBuckets

"ListMultipartUploads"

URI-Abfrageparameter und Anforderungskopfzeilen

StorageGRID unterstützt alle Allgemeine Parameter und Kopfzeilendieser Anforderung sowie die folgenden zusätzlichen Parameter:

- `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 Kopfzeilendieser Anforderung sowie 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 Kopfzeilendieser Anforderung sowie 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 Kopfzeilendieser Anforderung sowie 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 Kopfzeilendieser Anforderung sowie 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 Kopfzeilendieser Anforderung.

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"

"PutBucketEncryption"

URI-Abfrageparameter und Anforderungskopfzeilen

StorageGRID unterstützt alle Allgemeine Parameter und Kopfzeilendieser Anforderung.

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 Kopfzeilendieser Anforderung.

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 Kopfzeilendieser Anforderung.

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 Kopfzeilendieser Anforderung.

Text anfordern

Einzelheiten zu den unterstützten JSON-Body-Feldern finden Sie unter"Verwendung von Bucket- und Gruppenzugriffsrichtlinien" .

"PutBucketReplication"

URI-Abfrageparameter und Anforderungskopfzeilen

StorageGRID unterstützt alle Allgemeine Parameter und Kopfzeilendieser Anforderung.

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 Kopfzeilendieser Anforderung.

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"

"PutBucketVersioning"

URI-Abfrageparameter und Anforderungskopfzeilen

StorageGRID unterstützt alle Allgemeine Parameter und Kopfzeilendieser Anforderung.

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 Kopfzeilendieser Anforderung sowie die folgenden zusätzlichen Kopfzeilen:

- `Cache-Control`
- `Content-Disposition`
- `Content-Encoding`
- `Content-Language`
- `Expires`
- `x-amz-checksum-sha256`
- `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 Kopfzeilendieser Anforderung.

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 Kopfzeilendieser Anforderung.

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 Kopfzeilendieser Anforderung sowie diesen zusätzlichen Header:

- `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 Kopfzeilendieser Anforderung.

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 Kopfzeilendieser Anforderung.

Text anfordern

Weitere Informationen zu den unterstützten Körperfeldern finden Sie unter "Objekt restoreObject".

"SelektierObjectContent"

URI-Abfrageparameter und Anforderungskopfzeilen

StorageGRID unterstützt alle Allgemeine Parameter und Kopfzeilendieser Anforderung.

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-checksum-sha256`
- `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".
- Sie haben "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. `us-east-1`Beispiel: .
   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.

Konsistenz

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 die Lese-nach-Schreib-Konsistenz für neu erstellte Objekte. Jeder GET nach einem erfolgreich abgeschlossenen PUT kann die neu geschriebenen Daten lesen. Überschreibungen vorhandener Objekte, Metadatenaktualisierungen und Löschungen sind letztendlich konsistent.

Wenn Sie Objektoperationen mit einer anderen Konsistenz durchführen möchten, haben Sie folgende Möglichkeiten:

- Geben Sie eine Konsistenz fürJeden Eimer .
- Geben Sie eine Konsistenz für 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 **Konfiguration** > **System** > **Speichereinstellungen** > **Standard-Bucket-Konsistenz**.
  - .

> Eine Änderung der Konsistenz für das gesamte Grid gilt nur für Buckets, die nach der Änderung der Einstellung erstellt wurden. Informationen zu den Details einer Änderung finden Sie im Auditprotokoll unter `/var/local/log` (Suche nach **consistenzLevel**).

Konsistenzwerte

Die Konsistenz wirkt sich darauf aus, wie die Metadaten, die StorageGRID zum Verfolgen von Objekten verwendet, zwischen den Knoten verteilt werden. Konsistenz beeinflusst die Verfügbarkeit von Objekten für Clientanforderungen.

Sie können die Konsistenz für einen Bucket oder eine API-Operation auf einen der folgenden Werte festlegen:

- **Alle**: Alle Knoten erhalten sofort Objektmetadaten, oder die Anfrage schlägt fehl.
- **Stark global**: Garantiert Lese-nach-Schreib-Konsistenz für alle Clientanforderungen auf allen Sites. Wenn Quorum-Semantiken konfiguriert sind, gelten die folgenden Verhaltensweisen:
  - Ermöglicht Site-Fehlertoleranz für Clientanforderungen, wenn Grids drei oder mehr Sites haben. Zwei-Site-Grids verfügen über keine Site-Ausfalltoleranz.
  - Die folgenden S3-Vorgänge sind nicht erfolgreich, wenn eine Site ausgefallen ist:
    - DeleteBucketEncryption
    - PutBucketBranch
    - PutBucketEncryption
    - PutBucketVersioning
    - PutObjectLegalHold

- PutObjectLockKonfiguration
- PutObjectRetention

Bei Bedarf können Sie "Konfigurieren Sie die StorageGRID Quorum-Semantik für starke globale Konsistenz" .

- **Strong-site**: Objektmetadaten werden sofort auf andere Knoten am Standort verteilt. Garantiert Konsistenz bei Lese-nach-Schreibvorgängen für alle Client-Anfragen innerhalb eines Standorts.
- **Read-after-New-write**: 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.

Konsistenz für Bucket angeben

Zum Festlegen der Konsistenz für Bucket können Sie die StorageGRID-Anforderung verwenden"PUT Bucket-Konsistenz". Sie können dies aber auch "Ändern der Konsistenz eines Buckets"über den Tenant Manager tun.

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 den Datenschutz beeinflussen

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.

Folgende "Aufnahmeoptionen" Informationen 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 drei Standorten mit der folgenden ILM-Regel und der folgenden Konsistenz:

- **ILM-Regel**: Erstellen Sie drei Objektkopien, eine am lokalen Standort und eine an jedem Remote-Standort. Verwenden Sie ein striktes Aufnahmeverhalten.
- **Konsistenz**: Stark global (Objektmetadaten werden sofort an mehrere Sites verteilt).

Wenn ein Client ein Objekt im Grid speichert, erstellt StorageGRID alle drei Objektkopien und verteilt Metadaten an mehrere Sites, bevor es dem Client die Erfolgsmeldung meldet.

Zum Zeitpunkt der erfolgreichen Aufnahme der Nachricht ist das Objekt vollständig vor Verlust geschützt. Wenn beispielsweise die lokale Site kurz nach der Aufnahme verloren geht, sind an den Remote-Sites weiterhin Kopien der Objektdaten und der Objektmetadaten vorhanden. Das Objekt ist von den anderen Standorten vollständig abrufbar.

Wenn Sie stattdessen dieselbe ILM-Regel und die starke Site-Konsistenz verwenden, erhält der Client möglicherweise eine Erfolgsmeldung, nachdem die Objektdaten auf die Remote-Sites repliziert wurden, aber bevor die Objektmetadaten dorthin verteilt werden. In diesem Fall entspricht das Schutzniveau der Objektmetadaten nicht dem Schutzniveau der Objektdaten. Wenn die lokale Site kurz nach der Aufnahme verloren geht, gehen die 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 10,000 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 ermöglicht die Versionsunterstützung, ILM-Regeln zu erstellen, die als Referenzzeit „nicht aktuelle Zeit“ verwenden (wählen Sie **Ja** für die Frage „Diese Regel nur auf ältere Objektversionen anwenden?“ in "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-Objektsperrung für Ihr StorageGRID-System aktiviert ist, können Sie Buckets mit aktivierter S3-Objektsperrung 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-Objektsperreneinstellung 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` Anforderungsheader. 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 der `s3:BypassGovernanceRetention` Berechtigung können den Anforderungskopf verwenden `x-amz-bypass-governance-retention: true`, um die 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 Standardaufbewahrungsmodus angewendet, sofern `x-amz-object-lock-mode` diese `x-amz-object-lock-retain-until-date` nicht angegeben sind. Der Standardaufbewahrungszeitraum wird verwendet, um das Aufbewahrungsdatum zu berechnen, wenn `x-amz-object-lock-retain-until-date` nicht angegeben ist.

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 über die Berechtigung verfügen oder Konto root sein, um `s3:PutBucketObjectLockConfiguration` diesen Vorgang abzuschließen.

Der `Content-MD5` 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 Standardaufbewahrungsmodus angewendet, wenn `x-amz-object-lock-mode` nicht angegeben ist. Der Standardaufbewahrungszeitraum wird verwendet, um das Aufbewahrungsdatum zu berechnen, wenn `x-amz-object-lock-retain-until-date` nicht angegeben ist.

Sie müssen über die Berechtigung verfügen oder Konto root sein, um `s3:GetBucketObjectLockConfiguration` 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/T24gRfpwpuZrEG11Bb9ImOMAAe98oxSpXlknabA0LTvBYJpSIX
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-Objektsperrung kann eine Kombination von Objekten mit und ohne Aufbewahrungseinstellungen für S3-Objektsperrung 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.

Um die S3-Objektsperreinstellungen beim Hinzufügen einer Objektversion zu einem Bucket anzugeben, geben Sie eine "PutObject", , "CopyObject"oder "CreateMultipartUpload"-Anforderung aus.

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

- `x-amz-object-lock-retain-until-date`
    - Der Wert „bis zum Datum behalten“ muss im Format `2020-08-10T21:46:00Z`vorliegen. 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` Anforderungsheader ist erforderlich, wenn `x-amz-object-lock-*` in der PutObject-Anforderung ein Anforderungsheader vorhanden ist. `Content-MD5` Ist für CopyObject oder CreateMultipartUpload nicht erforderlich.
- Wenn im Bucket die S3-Objektsperre nicht aktiviert ist und eine `x-amz-object-lock-*` Anforderungsheader vorhanden ist, wird ein Fehler 400 Bad Request (InvalidRequest) zurückgegeben.
- Die PutObject-Anfrage unterstützt die Verwendung von `x-amz-storage-class: REDUCED_REDUNDANCY`, um AWS-Verhalten abzugleichen. 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`, sofern konfiguriert und der Absender der Anfrage die richtigen Berechtigungen hat `s3:Get*`.

Sie können den Richtlinienkonditionsschlüssel verwenden `s3:object-lock-remaining-retention-days`, um die minimalen und maximal zulässigen Aufbewahrungsfristen für Ihre Objekte einzuschränken.

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 „bis zum Datum behalten“ muss im Format `2020-08-10T21:46:00Z`vorliegen. 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 mit der `s3:BypassGovernanceRetention` Berechtigung können die aktiven Aufbewahrungseinstellungen eines Objekts umgehen, das den GOVERNANCE-Modus verwendet. Alle LÖSCHVORGÄNGE oder PutObjectRetention müssen den Anforderungsheader enthalten `x-amz-bypass-governance-retention:true`. 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 User Guide: Sperren Von Objekten"

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. Alle Details 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

Lebenszyklukonfiguration 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 dem Präfix/ entsprechen `category1` und den Wert `tag2` haben `key2`. Der `Expiration` Parameter gibt an, dass Objekte, die dem Filter entsprechen, am 22. August 2020 um Mitternacht 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 ihrer 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 alle nicht aktuellen Versionen übereinstimmender Objekte 50 Tage nach ihrer Nichtaktueller 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 PutkBucketLifecycleConfiguration ausgeben.

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

```
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 angewendet wird, enthält die Antwort einen `Expiration` Parameter, der angibt, wann das Objekt abläuft und welche Ablaufregel abgeglichen wurde.

> Da der Bucket-Lebenszyklus ILM außer Kraft setzt, wird als tatsächliches Datum angezeigt, an dem `expiry-date` 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 legt ein Objekt in den `testbucket` Bucket.

```
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": {}
}
```

Bei Buckets mit aktivierter Versionierung gilt der `x-amz-expiration` Antwortheader 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 routinemäßig prüft, ob ein Objekt an einem Pfad existiert, an dem Sie das Objekt nicht erwarten, sollten Sie die Option "Verfügbar" verwenden."Konsistenz" . Sie sollten beispielsweise die Konsistenz „Verfügbar“ verwenden, wenn Ihre Anwendung einen HEAD für einen Speicherort vor dem PUT anwendet.

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 „verfügbare“ Konsistenz für jeden Bucket mithilfe der Anforderung festlegen "PUT Bucket-Konsistenz"oder die Konsistenz in der Anforderungsheader für eine einzelne API-Operation angeben.

Empfehlungen für Objektschlüssel

Befolgen Sie diese Empfehlungen für Objektschlüsselnamen auf Basis des ersten Erstells 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, wiez. 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"aktiviert ist, 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 Zeitzonenversatz angegeben werden (+0000 muss angegeben werden). Wenn Sie die Kopfzeile in Ihre Anfrage aufnehmen `x-amz-date`, wird ein Wert überschrieben, der in der Kopfzeile der Datumsanforderung angegeben ist. Bei Verwendung von AWS Signature Version 4 muss der `x-amz-date` Header in der signierten Anfrage vorhanden sein, da der Datumskopf 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: • Wenn Sie den tatsächlichen Wert der Payload Checksumme in angeben `x-amz-content-sha256`, wird der Wert ohne Validierung akzeptiert, als ob der Wert `UNSIGNED-PAYLOAD` für den Header angegeben worden wäre. Wenn Sie einen Header-Wert angeben `x-amz-content-sha256`, der Streaming impliziert `aws-chunked` (z. B. STREAMING-AWS4-HMAC-SHA256-PAYLOAD), werden die Chunk-Signaturen nicht gegen die Chunk-Daten verifiziert.

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`Header und die Abfrageparameter.

Verwenden Sie den HTTP-Autorisierungskopf

Der HTTP- `Authorization`Header wird von allen S3-API-Operationen außer „Anonyme Anfragen“ verwendet, sofern dies durch die Bucket-Richtlinie zulässig ist. Die `Authorization` Kopfzeile enthält alle erforderlichen Signaturinformationen zur Authentifizierung einer Anforderung.

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	In der StorageGRID"GET Storage-Auslastung"-Anfrage wird der von einem Konto insgesamt und für jeden mit dem Konto verknüpften Bucket verwendete Storage angezeigt. Dies ist eine Operation auf dem Dienst mit einem Pfad von / und einem benutzerdefinierten Abfrageparameter (`?x-ntap-sg-usage`) hinzugefügt.
OPTIONEN /	Client-Anwendungen können `OPTIONS /` Anfragen an den S3-Port auf einem Storage-Node ausgeben, ohne S3-Authentifizierungsdaten bereitzustellen, um festzustellen, 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 5,000 Buckets.

Jedes Grid kann maximal 100,000 Buckets enthalten.

Um 5,000 Buckets zu unterstützen, muss jeder Storage Node im Grid mindestens 64 GB RAM aufweisen.

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-Kontingente, Einschränkungen und Einschränkungen"
- "Konfigurieren Sie die Domänennamen des S3-Endpunkts"

Die Operationen ListObjects (GET Bucket) und ListObjectVersions (GET Bucket-Objektversionen) 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	Erstellt einen neuen Bucket. Mit dem Erstellen des Buckets werden Sie zum Bucket-Eigentümer. • Bucket-Namen müssen die folgenden Regeln einhalten: ◦ Jedes StorageGRID System muss eindeutig sein (nicht nur innerhalb des Mandantenkontos). ◦ Muss DNS-konform sein. ◦ Muss 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 in der Region erstellt `us-east-1`. Sie können jedoch das Anforderungselement im Anforderungskörper verwenden `LocationConstraint`, um einen anderen Bereich anzugeben. Wenn Sie das Element verwenden `LocationConstraint`, müssen Sie den genauen Namen einer Region angeben, die mit dem Grid Manager oder der Grid Management API definiert wurde. Wenden Sie sich an Ihren Systemadministrator, wenn Sie den zu verwendenden Regionalnamen nicht kennen. **Hinweis**: Ein Fehler tritt auf, wenn Ihre CreateBucket-Anforderung eine Region verwendet, die nicht in StorageGRID definiert wurde. • Sie können den Anforderungsheader einschließen `x-amz-bucket-object-lock-enabled`, um einen Bucket mit aktivierter S3 Object Lock zu erstellen. Siehe "Konfigurieren Sie die S3-Objektsperre über die S3-REST-API". 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.
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	Verwendet die `tagging` Unterressource, um alle Tags aus einem Bucket zu entfernen. **Achtung**: Wenn für diesen Bucket ein nicht standardmäßiges ILM-Policy-Tag gesetzt ist, wird ein Bucket-Tag mit einem ihm zugewiesenen Wert vorhanden sein `NTAP-SG-ILM-BUCKET-TAG`. Stellen Sie keine DeleteBucketTagging-Anforderung aus, wenn ein `NTAP-SG-ILM-BUCKET-TAG` Bucket-Tag vorhanden ist. Geben Sie stattdessen eine Anforderung für das PutkBucketTagging nur mit dem `NTAP-SG-ILM-BUCKET-TAG` Tag und dem ihm zugewiesenen Wert aus, um alle anderen Tags aus dem Bucket zu entfernen. Ändern oder entfernen Sie das Bucket-Tag nicht `NTAP-SG-ILM-BUCKET-TAG`.
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 die Konfiguration für den Bucket zurück `cors`.
GetBucketEncryption	Gibt die Standardverschlüsselungskonfiguration für den Bucket zurück.
GetBucketLifecycleKonfiguration (Zuvor GET Bucket-Lebenszyklus genannt)	Gibt die Lebenszykluskonfiguration für den Bucket zurück. Siehe "S3-Lebenszykluskonfiguration erstellen".
GetBucketLocation	Gibt die Region zurück, die mit dem Element in der Anforderung CreateBucket festgelegt wurde `LocationConstraint`. Wenn der Bereich des Buckets ist `us-east-1`, wird eine leere Zeichenfolge für die Region zurückgegeben.
GetBucketNotificationConfiguration (Zuvor namens „GET Bucket“-Benachrichtigung)	Gibt die Benachrichtigungskonfiguration zurück, die mit dem Bucket verbunden ist.
GetBucketPolicy	Gibt die dem Bucket angehängte Richtlinie zurück.
GetBucketReplication	Gibt die Replikationskonfiguration zurück, die mit dem Bucket verbunden ist.

Betrieb	Implementierung
GetBucketTagging	Verwendet die `tagging` Unterressource, um alle Tags für einen Bucket zurückzugeben. **Achtung**: Wenn für diesen Bucket ein nicht standardmäßiges ILM-Policy-Tag gesetzt ist, wird ein Bucket-Tag mit einem ihm zugewiesenen Wert vorhanden sein `NTAP-SG-ILM-BUCKET-TAG`. Ändern oder entfernen Sie dieses Tag nicht.
GetBucketVersioning	Diese Implementierung verwendet die `versioning` Subressource, um den Versionsstatus eines Buckets zurückzugeben. • *Blank*: Die Versionierung wurde nie aktiviert (Bucket ist „unversioniert“) • Aktiviert: Versionierung ist aktiviert • Suspendiert: Die Versionierung war zuvor aktiviert und wird ausgesetzt
GetObjectLockConfiguration	Gibt den Standardaufbewahrungsmodus für Bucket und den Standardaufbewahrungszeitraum zurück, sofern konfiguriert. Siehe "Konfigurieren Sie die S3-Objektsperre über die S3-REST-API".
HeadBucket	Legt fest, ob ein Bucket vorhanden ist und Sie über die Berechtigung verfügen, darauf zuzugreifen. Dieser Vorgang liefert Folgendes zurück: • `x-ntap-sg-bucket-id`: Die UUID des Buckets im UUID-Format. • `x-ntap-sg-trace-id`: Die eindeutige Trace-ID der zugehörigen Anforderung.

Betrieb	Implementierung
ListObjects und ListObjectsV2 (Zuvor benannt nach „GET Bucket“)	Gibt einige oder alle (bis zu 1,000) Objekte in einem Bucket zurück. Die Storage-Klasse für Objekte kann einen der beiden Werte haben, selbst wenn das Objekt mit der Option Storage-Klasse aufgenommen wurde `REDUCED_REDUNDANCY`: • `STANDARD`, Das angibt, dass das Objekt in einem Speicherpool mit Storage Nodes gespeichert ist. • `GLACIER`, Das angibt, dass das Objekt in den externen Bucket verschoben wurde, der vom Cloud-Speicherpool angegeben wurde. Wenn der Bucket eine große Anzahl von gelöschten Schlüsseln mit dem gleichen Präfix enthält, kann die Antwort einige `CommonPrefixes` enthalten, die keine Schlüssel enthalten. Für die HeadObject- und ListObject-Anfragen gibt StorageGRID die LastModified-Zeitstempel mit unterschiedlicher Genauigkeit zurück, während AWS die Zeitstempel mit der gleichen Genauigkeit zurückgibt, wie in den folgenden Beispielen gezeigt: • StorageGRID HeadObject: "LastModified": "2024-09-26T16:43:24+00:00" • StorageGRID ListObject: "LastModified": "2024-09-26T16:43:24.931000+00:00" • AWS HeadObject: "LastModified": "2023-10-17T00:19:54+00:00" • AWS ListObject: "LastModified": "2023-10-17T00:19:54+00:00"
ListObjectVersions (Zuvor namens „GET Bucket Object Versions“)	Mit LESEZUGRIFF auf einen Bucket wird dieser Vorgang mit den Unterressourcen-Listen Metadaten aller Versionen von Objekten im Bucket verwendet `versions`.
PutBucketCors	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 `images` zum Speichern von Grafiken. Durch die Einstellung der CORS-Konfiguration für den `images` Bucket können Sie die Bilder in diesem Bucket auf der Website anzeigen lassen `http://www.example.com`.

Betrieb	Implementierung
PutBucketEncryption	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 serverseitige Verschlüsselungskonfigurationsregel angeben, setzen Sie den `SSEAlgorithm` Parameter auf `AES256`, und verwenden Sie den Parameter nicht `KMSMasterKeyID`. Die Standardverschlüsselungskonfiguration von Buckets wird ignoriert, wenn in der Objekt-Upload-Anforderung bereits Verschlüsselung angegeben ist (d. h. wenn die Anforderung den Anforderungsheader enthält `x-amz-server-side-encryption-*`).
PutBucketLifecycleKonfiguration (Zuvor PUT Bucket-Lebenszyklus genannt)	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: • Ablauf (Tage, Datum, ErstrecktObjectDeleteMarker) • Nicht-aktuellVersionAblauf (NewerNichtaktuellVersionen, nicht aktuelleTage) • Filter (Präfix, Tag) • Status • ID StorageGRID bietet folgende Maßnahmen nicht: • AbortInsetteMultipartUpload • Übergang 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". **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.

Betrieb	Implementierung

PutBucketNotificationKonfiguration
 	
(Zuvor namens „PUT Bucket“-Benachrichtigung)
	Konfiguriert Benachrichtigungen für den Bucket mithilfe der XML-Benachrichtigungskonfiguration, die im Anforderungskörper enthalten ist. Sie sollten folgende Implementierungsdetails kennen:
	
	• StorageGRID unterstützt Amazon Simple Notification Service (Amazon SNS)-Themen, Kafka-Themen oder Webhook-Endpunkte als Ziele. Simple Queue Service (SQS) oder AWS 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.
	
	Der Endpunkt muss vorhanden sein, damit die Benachrichtigungskonfiguration erfolgreich ausgeführt werden kann. Wenn der Endpunkt nicht vorhanden ist, wird ein `400 Bad Request` Fehler mit dem Code zurückgegeben `InvalidArgument`.
	
	• Sie können keine Benachrichtigung für die folgenden Ereignistypen konfigurieren. Diese Ereignistypen werden **nicht** unterstützt.
	◦ `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:
	◦ **EventSource**
	
	`sgws:s3`
	
	◦ **AwsRegion**
	
	Nicht enthalten
	
	◦ * X-amz-id-2*
	
	Nicht enthalten
	
	◦ **arn**
	
	`urn:sgws:s3:::bucket_name`

PutBucketPolicy	Legt die dem Bucket zugeordnete Richtlinie fest. Sehen "Verwendung von Bucket- und Gruppenzugriffsrichtlinien" .

Betrieb	Implementierung
PutBucketReplication	Konfiguration "StorageGRID CloudMirror Replizierung" für den Bucket mithilfe der im Anforderungskörper bereitgestellten XML-Replikationskonfiguration Für die CloudMirror-Replikation sollten Sie die folgenden Implementierungsdetails beachten: • StorageGRID unterstützt nur V1 der Replizierungskonfiguration. Das bedeutet, dass StorageGRID die Verwendung des Elements für Regeln nicht unterstützt `Filter` und V1-Konventionen für das Löschen von Objektversionen befolgt. 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". Der Endpunkt muss vorhanden sein, damit die Replizierungskonfiguration erfolgreich ausgeführt werden kann. Wenn der Endpunkt nicht existiert, schlägt die Anforderung als fehl. Die Fehlermeldung lautet `400 Bad Request: Unable to save the replication policy. The specified endpoint URN does not exist: URN.` • Sie müssen kein in der Konfigurations-XML angeben `Role`. Dieser Wert wird von StorageGRID nicht verwendet und wird bei der Einreichung ignoriert. • Wenn Sie die Storage-Klasse aus dem Konfigurations-XML nicht angeben, verwendet StorageGRID standardmäßig die `STANDARD` 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: ◦ 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	Verwendet die `tagging` Unterressource, um einen Satz von Tags für einen Bucket hinzuzufügen oder zu aktualisieren. Beachten Sie beim Hinzufügen von Bucket-Tags die folgenden Einschränkungen: • 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. **Achtung**: Wenn für diesen Bucket ein nicht standardmäßiges ILM-Policy-Tag gesetzt ist, wird ein Bucket-Tag mit einem ihm zugewiesenen Wert vorhanden sein `NTAP-SG-ILM-BUCKET-TAG`. Stellen Sie sicher, dass das `NTAP-SG-ILM-BUCKET-TAG` Bucket-Tag in allen PutBucketTagging-Anforderungen mit dem zugewiesenen Wert enthalten ist. Ändern oder entfernen Sie dieses Tag nicht. **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.
PutBucketVersioning	Verwendet die `versioning` Unterressource, um den Versionsstatus eines vorhandenen Buckets festzulegen. Sie können den Versionierungsstatus mit einem der folgenden Werte festlegen: • 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 Versions-ID `null`.
PutObjectLockKonfiguration	Konfiguriert oder entfernt den Standardaufbewahrungsmodus und den Standardaufbewahrungszeitraum für Bucket. Wenn der Standardaufbewahrungszeitraum geändert wird, bleiben die bisherigen Objektversionen unverändert und werden im neuen Standardaufbewahrungszeitraum nicht neu berechnet. Weitere Informationen finden Sie unter"Konfigurieren Sie die S3-Objektsperre über die S3-REST-API".

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 an 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.

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

Betrieb	Implementierung
DeleteObject	Multi-Faktor-Authentifizierung (MFA) und der Antwortheader `x-amz-mfa` werden nicht unterstützt. 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. **Versionierung** Zum Entfernen einer bestimmten Version muss der Anforderer der Bucket-Eigentümer sein und die Unterressource verwenden `versionId`. Durch die Verwendung dieser Unterressource wird die Version dauerhaft gelöscht. Wenn das `versionId` einer Löschmarkierung entspricht, wird die Antwortkopfzeile `x-amz-delete-marker` auf gesetzt zurückgegeben `true`. • Wenn ein Objekt ohne die Unterressource in einem Bucket gelöscht wird `versionId`, bei dem die Versionierung aktiviert ist, wird eine Löschmarkierung generiert. Der `versionId` für die Löschmarkierung wird mit dem Antwortheader zurückgegeben `x-amz-version-id`, und der `x-amz-delete-marker` Antwortheader wird auf gesetzt zurückgegeben `true`. • Wenn ein Objekt ohne die Unterressource in einem Bucket gelöscht wird `versionId`, bei dem die Versionierung ausgesetzt ist, führt dies zu einer dauerhaften Löschung einer bereits vorhandenen Null-Version oder einer Null-Löschmarkierung und zur Generierung einer neuen Null-Löschmarkierung. Der `x-amz-delete-marker` Antwortheader wird auf gesetzt zurückgegeben `true`. **Hinweis**: In bestimmten Fällen können für ein Objekt mehrere Löschen-Marker vorhanden sein. Weitere Informationen zum Löschen von Objektversionen im GOVERNANCE-Modus finden Sie unter"Konfigurieren Sie die S3-Objektsperre über die S3-REST-API".

Betrieb	Implementierung
Objekte deObjekteObjekte (Zuvor benanntes DELETE mehrere Objekte)	Multi-Faktor-Authentifizierung (MFA) und der Antwortheader `x-amz-mfa` werden nicht unterstützt. In derselben Anforderungsmeldung können mehrere Objekte gelöscht werden. Weitere Informationen zum Löschen von Objektversionen im GOVERNANCE-Modus finden Sie unter"Konfigurieren Sie die S3-Objektsperre über die S3-REST-API".
DeleteObjectTagging	Verwendet die `tagging` Unterressource, um alle Tags aus einem Objekt zu entfernen. **Versionierung** Wenn der `versionId` Abfrageparameter in der Anforderung nicht angegeben ist, werden alle Tags aus der neuesten Version des Objekts in einem versionierten Bucket gelöscht. Wenn es sich bei der aktuellen Version des Objekts um eine Löschmarkierung handelt, wird der Status „MethodenNotAllowed“ zurückgegeben, wobei der `x-amz-delete-marker` Antwortkopf auf gesetzt `true` ist.
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	Verwendet die `tagging` Unterressource, um alle Tags für ein Objekt zurückzugeben. **Versionierung** Wenn der `versionId` Abfrageparameter in der Anforderung nicht angegeben ist, gibt der Vorgang 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“ zurückgegeben, wobei der `x-amz-delete-marker` Antwortkopf auf gesetzt `true` ist.
HeadObject	"HeadObject"
Objekt restoreObject	"Objekt restoreObject"

Betrieb	Implementierung
PutObject	"PutObject"
CopyObject (Zuvor PUT Object – Copy genannt)	"CopyObject"
PutObjectLegalHold	"Konfigurieren Sie die S3-Objektsperre über die S3-REST-API"
PutObjectRetention	"Konfigurieren Sie die S3-Objektsperre über die S3-REST-API"

Betrieb	Implementierung
PutObjectTagging	Verwendet die `tagging` Unterressource, um einem vorhandenen Objekt einen Satz von Tags hinzuzufügen. **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. **Tag-Updates und Ingest-Verhalten** 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. 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. **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. **Versionierung** Wenn der `versionId` Abfrageparameter in der Anforderung nicht angegeben ist, fügt der Vorgang Tags zur neuesten 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“ zurückgegeben, wobei der `x-amz-delete-marker` Antwortkopf auf gesetzt `true` ist.
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 siehe "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-kodiert 128-Bit sein.

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

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

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

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

- Sie müssen https verwenden.

> StorageGRID lehnt alle Anfragen ab, die über http bei Verwendung von SSE-C gestellt werden. Aus Sicherheitsgründen sollten Sie jeden Schlüssel, den Sie versehentlich mit http senden, als kompromittiert betrachten. Entsorgen Sie den Schlüssel, und drehen Sie ihn nach Bedarf.

- Der ETag in der Antwort ist nicht das MD5 der Objektdaten.
- Sie müssen die Zuordnung von Schlüsseln zu Objekten managen. StorageGRID speichert keine

Schlüssel. Sie sind für die Nachverfolgung des Verschlüsselungsschlüssels verantwortlich, den Sie für jedes Objekt bereitstellen.

- Wenn Ihr Bucket mit Versionierung aktiviert ist, sollte für jede Objektversion ein eigener Verschlüsselungsschlüssel vorhanden sein. Sie sind verantwortlich für das Tracking des Verschlüsselungsschlüssels, der für jede Objektversion verwendet wird.
- Da Sie Verschlüsselungsschlüssel auf Client-Seite verwalten, müssen Sie auch zusätzliche Schutzmaßnahmen, wie etwa die Rotation von Schlüsseln, auf Client-Seite verwalten.

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

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

Verwandte Informationen

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

CopyObject

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

Konflikte lösen

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

Objektgröße

Die maximale *recommended* Größe für eine einzelne PutObject-Operation beträgt 5 gib (5,368,709,120 Bytes). Falls 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 Header nicht zurück `x-amz-missing-meta`, wenn der interpretierte Wert des Schlüsselnamens oder -Wertes nicht druckbare 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, das benutzerdefinierte Metadaten enthält
- `x-amz-metadata-directive`: Der Standardwert ist `COPY`, mit dem Sie das Objekt und die zugehörigen Metadaten kopieren können.

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

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

  Sie können festlegen `REPLACE`, dass die vorhandenen Tags beim Kopieren des Objekts überschrieben oder die Tags aktualisiert werden sollen.

- S3-Objektsperrungs-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-checksum-algorithm`

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

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

Optionen der Storage-Klasse

Der `x-amz-storage-class` Anforderungsheader wird unterstützt und beeinflusst, wie viele Objektkopien StorageGRID erstellt, wenn die passende ILM-Regel den doppelten Commit oder den ausgewogenen verwendet"Aufnahme-Option".

- `STANDARD`

  (Standard) gibt einen Dual-Commit-Aufnahmevorgang 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-Aufnahmevorgang an, wenn die ILM-Regel die Option Dual Commit verwendet oder wenn die Option Balance zur Erstellung zwischenzeitaler Kopien zurückgreift.

  > Wenn Sie ein Objekt in einen Bucket mit aktivierter S3-Objektsperrung aufnehmen, wird die `REDUCED_REDUNDANCY` Option ignoriert. Wenn Sie ein Objekt in einen Legacy-konformen Bucket aufnehmen, gibt die `REDUCED_REDUNDANCY` Option einen Fehler zurück. StorageGRID führt immer eine doppelte Einspeisung durch, um Compliance-Anforderungen zu erfüllen.

Verwenden von x-amz-copy-source in CopyObject

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

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

- Sie können CopyObject nicht verwenden, um ein vorhandenes Objekt zu verschlüsseln oder die Verschlüsselung eines vorhandenen Objekts zu ändern. Wenn Sie den Header oder den `x-amz-server-side-encryption-customer-algorithm` Header liefern `x-amz-server-side-encryption`, lehnt StorageGRID die Anfrage ab und gibt 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 Anfrage Header Sie angeben, hängt davon ab, ob das Quellobjekt verschlüsselt ist und ob Sie planen, das Zielobjekt zu verschlüsseln.

- 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`: Spezifizieren `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`: Spezifizieren `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, lesen Sie die Überlegungen für "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 einem neuen `server-side-encryption` Wert mit `x-amz-metadata-directive: REPLACE`.

Versionierung

Wenn der Quell-Bucket versioniert ist, können Sie die Kopfzeile verwenden `x-amz-copy-source`, um die neueste Version eines Objekts zu kopieren. Um eine bestimmte Version eines Objekts zu kopieren, müssen Sie explizit die Version angeben, die mit der Unterressource kopiert werden soll `versionId`. Wenn der Ziel-Bucket versioniert ist, wird die generierte Version im Antwortheader zurückgegeben `x-amz-version-id`. Wenn die Versionierung für den Ziel-Bucket unterbrochen wird, `x-amz-version-id` gibt der Wert „Null“ zurück.

GetObject

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

GetObject- und mehrteilige Objekte

Mit dem Anforderungsparameter können `partNumber` Sie einen bestimmten Teil eines mehrteiligen oder segmentierten Objekts abrufen. Das `x-amz-mp-parts-count` Antwortelement gibt an, wie viele Teile das Objekt hat.

Sie können sowohl für segmentierte/mehrteilige Objekte als auch für nicht segmentierte/nicht mehrteilige Objekte auf 1 setzen `partNumber`. Das Antwortelement wird jedoch `x-amz-mp-parts-count` 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 liefern den Header nicht zurück `x-amz-missing-meta`, wenn der Schlüsselname oder -Wert nicht druckbare Zeichen enthält.

Unterstützte Anforderungsheader

Der folgende Anforderungskopf wird unterstützt:

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

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

Nicht unterstützte Anforderungsüberschrift

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

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

Versionierung

Wenn `versionId` keine Unterressource angegeben wird, ruft der Vorgang 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“ zurückgegeben, wobei der `x-amz-delete-marker` Antwortkopf auf gesetzt `true` ist.

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`: Spezifizieren `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 Objektschlüssels 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, lesen Sie die Überlegungen in "Serverseitige Verschlüsselung".

Verhalten von GetObject for Cloud Storage Pool Objects

Wenn ein Objekt in einem gespeichert wurde"Cloud-Storage-Pool", hängt das Verhalten einer GetObject-Anforderung vom Zustand des Objekts ab. Weitere Informationen finden Sie unter"HeadObject".

> 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 GetObject
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.

Status des Objekts	Verhalten von GetObject
Das Objekt wurde in einen nicht aufrufbaren Zustand überführt	`403 Forbidden`, `InvalidObjectState` Verwenden Sie eine "Objekt restoreObject" Anforderung, um das Objekt in einem abrufbaren Zustand wiederherzustellen.
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 einige Teile des Objekts bereits in einen nicht abrufbaren Status überführt wurden oder wenn 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-Anfrage kann zurückgegeben werden `403 Forbidden`.

GetObject- und Grid-übergreifende Replikation

Wenn Sie und "Grid-übergreifende Replizierung"für einen Bucket verwenden"Grid-Verbund", kann der S3-Client den Replikationsstatus eines Objekts überprüfen, indem er eine GetObject-Anforderung ausgibt. Die Antwort enthält den StorageGRID-spezifischen `x-ntap-sg-cgr-replication-status` Antwortheader, der einen der folgenden Werte enthält:

Raster	Replikationsstatus
Quelle	• **ABGESCHLOSSEN**: 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.

> Der Header wird von StorageGRID nicht unterstützt `x-amz-replication-status`.

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 Übergangsstatus des Objekts zu bestimmen.

HeadObject- und mehrteilige Objekte

Mit dem Anforderungsparameter können Sie `partNumber` Metadaten für einen bestimmten Teil eines mehrteiligen oder segmentierten Objekts abrufen. Das `x-amz-mp-parts-count` Antwortelement gibt an, wie viele Teile das Objekt hat.

Sie können sowohl für segmentierte/mehrteilige Objekte als auch für nicht segmentierte/nicht mehrteilige Objekte auf 1 setzen `partNumber`. Das Antwortelement wird jedoch `x-amz-mp-parts-count` 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 Requests for an object with escaped UTF-8 characters in user-defined metadata liefern den Header nicht zurück `x-amz-missing-meta`, wenn der Schlüsselname oder -Wert nicht druckbare Zeichen enthält.

Unterstützte Anforderungsheader

Der folgende Anforderungskopf wird unterstützt:

- `x-amz-checksum-mode`

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

Nicht unterstützte Anforderungsüberschrift

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

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

Versionierung

Wenn `versionId` keine Unterressource angegeben wird, ruft der Vorgang 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“ zurückgegeben, wobei der `x-amz-delete-marker` Antwortkopf auf gesetzt `true` ist.

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`: Spezifizieren `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 Objektschlüssels 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, lesen Sie die Überlegungen in "Serverseitige Verschlüsselung".

HeadObject-Antworten für Cloud-Storage-Pool-Objekte

Wenn das Objekt in einem gespeichert ist"Cloud-Storage-Pool", werden die folgenden Antwortkopfzeilen 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.)

Objekt in Cloud-Storage-Pool, ist aber noch nicht in einen Zustand übergegangen, der nicht abrufbar ist	`200 OK`
	
	`x-amz-storage-class: GLACIER`
	
	`x-amz-restore: ongoing-request="false", expiry-date="Sat, 23 July 20 2030 00:00:00 GMT"`
	
	Bis das Objekt in einen nicht abrufbaren Zustand übergeht, wird der Wert für `expiry-date` in der Zukunft auf eine ferne Zeit gesetzt. Die genaue Zeit der Transition wird nicht durch das StorageGRID System gesteuert.

Status des Objekts	Antwort auf HeadObject

Das Objekt ist in den nicht aufrufbaren Zustand übergegangen, aber mindestens eine Kopie ist auch im Grid vorhanden	`200 OK`
	
	`x-amz-storage-class: GLACIER`
	
	`x-amz-restore: ongoing-request="false", expiry-date="Sat, 23 July 20 2030 00:00:00 GMT"`
	
	Der Wert für `expiry-date` wird auf eine ferne Zeit in der Zukunft gesetzt.
	
	Hinweis: Wenn die Kopie im Raster nicht verfügbar ist (z. B. ein Storage Node ist ausgefallen), müssen Sie eine Anforderung zur Wiederherstellung der Kopie aus dem Cloud Storage Pool ausgeben"Objekt restoreObject", bevor Sie das Objekt erfolgreich abrufen können.

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

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

Das Objekt wird im Cloud-Storage-Pool vollständig wiederhergestellt	`200 OK`
	
	`x-amz-storage-class: GLACIER`
	
	`x-amz-restore: ongoing-request="false", expiry-date="Sat, 23 July 20 2018 00:00:00 GMT"`
	
	Das `expiry-date` gibt an, wann das Objekt im Cloud-Speicherpool in einen nicht abrufbaren Zustand zurückkehrt.

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 kann eine HeadObject-Anforderung falsch zurückgegeben werden `x-amz-restore: ongoing-request="false"`, wenn einige Teile des Objekts bereits in einen nicht abrufbaren Status überführt wurden oder wenn Teile des Objekts noch nicht wiederhergestellt wurden.

HeadObject- und Grid-übergreifende Replikation

Wenn Sie und "Grid-übergreifende Replizierung"für einen Bucket verwenden"Grid-Verbund", kann der S3-Client mit einer HeadObject-Anforderung den Replikationsstatus eines Objekts überprüfen. Die Antwort enthält den StorageGRID-spezifischen `x-ntap-sg-cgr-replication-status` Antwortheader, der einen der folgenden Werte enthält:

Raster	Replikationsstatus
Quelle	• **ABGESCHLOSSEN**: 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.

Der Header wird von StorageGRID nicht unterstützt `x-amz-replication-status`.

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). Falls 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 Header nicht zurück `x-amz-missing-meta`, wenn der interpretierte Wert des Schlüsselnamens oder -Wertes nicht druckbare 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 für `Content-Encoding`StorageGRID angeben, `aws-chunked` werden die folgenden Elemente nicht überprüft:

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

Die Chunked-Transferkodierung wird unterstützt, wenn `aws-chunked` auch das Signieren der Nutzlast verwendet wird.

- `x-amz-checksum-sha256`
- `x-amz-meta-`, Gefolgt von einem Name-Wert-Paar, das benutzerdefinierte Metadaten enthält.

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

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

  Wenn Sie die Option **Benutzerdefinierte Erstellungszeit** als Referenzzeit für eine ILM-Regel verwenden möchten, müssen Sie als Name der Metadaten verwenden, `creation-time` die beim Erstellen des Objekts aufgezeichnet werden. 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-Objektsperrungs-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:

- `If-Match`
- `If-None-Match`
- `x-amz-acl`
- `x-amz-sdk-checksum-algorithm`
- `x-amz-trailer`
- `x-amz-website-redirect-location`

  Der `x-amz-website-redirect-location` Header gibt zurück `XNotImplemented`.

Optionen der Storage-Klasse

Der `x-amz-storage-class` Anforderungskopf wird unterstützt. Der für eingereichte Wert `x-amz-storage-class` hat einen Einfluss darauf, wie StorageGRID Objektdaten bei der Aufnahme schützt, und nicht darauf, wie viele persistente Kopien des Objekts im StorageGRID System gespeichert werden (durch ILM bestimmt).

Wenn die ILM-Regel, die einem aufgenommenen Objekt entspricht, die Option „Strict Ingest“ verwendet, hat der `x-amz-storage-class` Header keine Auswirkungen.

Folgende Werte können verwendet werden für `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 in der ILM-Regel angegebenen Objektkopien erstellen kann (synchrone Platzierung), hat der `x-amz-storage-class` Header keine Auswirkungen.

- `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. Diese `REDUCED_REDUNDANCY` Option ist am besten geeignet, wenn die mit dem Objekt übereinstimmende ILM-Regel eine einzige replizierte Kopie erstellt. In diesem Fall `REDUCED_REDUNDANCY` entfällt bei jedem Einspielvorgang die unnötige Erstellung und Löschung einer zusätzlichen Objektkopie.

Die Verwendung der `REDUCED_REDUNDANCY` Option wird in anderen Fällen nicht empfohlen. `REDUCED_REDUNDANCY` Erhöhtes 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.

Die Angabe `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 mit aktivierter S3-Objektsperrung aufnehmen, wird die `REDUCED_REDUNDANCY` Option ignoriert. Wenn Sie ein Objekt in einen Legacy-konformen Bucket aufnehmen, gibt die `REDUCED_REDUNDANCY` Option 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`

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

- **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`: Spezifizieren `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, lesen Sie die Überlegungen für "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, wird automatisch ein eindeutiges `versionId` Objekt für die Version des gespeicherten Objekts generiert. Dies `versionId` wird auch in der Antwort über den Antwortheader zurückgegeben `x-amz-version-id`.

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

Signaturberechnungen für den Autorisierungskopf

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

- StorageGRID erfordert nicht, `host` dass Header in enthalten `CanonicalHeaders` sind.
- StorageGRID muss nicht `Content-Type` in enthalten sein `CanonicalHeaders`.
- StorageGRID erfordert nicht, `x-amz-*` dass Header in enthalten `CanonicalHeaders` sind.

> Als allgemeine Best Practice sollten Sie diese Kopfzeilen immer in einschließen `CanonicalHeaders`, um sicherzustellen, dass sie verifiziert sind. Wenn Sie diese Kopfzeilen 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"
- "Amazon Simple Storage Service API-Referenz: PutObject"

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. Die Art der Wiederherstellung wird nicht unterstützt `SELECT`. Wählen Sie Rückgabeanforderungen `XNotImplemented`.

Versionierung

Optional können Sie angeben `versionId`, eine bestimmte Version eines Objekts in einem versionierten Bucket wiederherzustellen. Wenn Sie nicht angeben `versionId`, wird die neueste Version des Objekts wiederhergestellt

Verhalten von RestoreObject auf Cloud-Storage-Pool-Objekten

Wenn ein Objekt in einem gespeichert wurde"Cloud-Storage-Pool", hat eine RestoreObject-Anforderung das folgende Verhalten, basierend auf dem Zustand des Objekts. Weitere Informationen finden Sie unter"HeadObject".

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 `expiry-date`.
Das Objekt wurde in einen nicht aufrufbaren Zustand überführt	`202 Accepted` Stellt eine abrufbare Kopie des Objekts für die im Anforderungskörper angegebene Anzahl von Tagen im Cloud-Speicherpool wieder her. Am Ende dieses Zeitraums wird das Objekt in einen nicht aufrufbaren Zustand zurückgeführt. Verwenden Sie optional das `Tier` Anforderungselement, um festzulegen, wie lange der Wiederherstellungsjob dauern wird(`Expedited` `Standard`, bis er beendet ist, , oder `Bulk`). Wenn Sie nicht angeben `Tier`, wird der `Standard` Tier verwendet. **Wichtig**: Wenn ein Objekt in S3 Glacier Deep Archive migriert wurde oder der Cloud Storage Pool Azure Blob Storage verwendet, können Sie es nicht mithilfe der Tier wiederherstellen `Expedited`. 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`
Das Objekt wird im Cloud-Storage-Pool vollständig wiederhergestellt	`200 OK` **Hinweis:** Wenn ein Objekt in einen abrufbaren Zustand zurückgestellt wurde, können Sie es ändern `expiry-date`, indem Sie die RestoreObject-Anfrage mit einem neuen Wert für neu ausgeben `Days`. 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.
- Sie haben `s3:GetObject` die 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 Datei, die abgefragt werden sollen, `SUB-EST2020_ALL.csv` sehen wie folgt aus:

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

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`, sehen wie folgt aus:

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

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

Vorgänge für mehrteilige Uploads

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 ausgewertet, wenn die ILM-Regel die ausgewogene oder strikte 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 Upload-Vorgänge unterstützen StorageGRID"Konsistenzwerte" .
- Wenn ein Objekt mit mehrteiligen Uploads aufgenommen wird, wird das "Schwellenwert für Objektsegmentierung (1 gib)"nicht angewendet.
- Je nach Bedarf können Sie mit mehrteiligen Uploads verwenden"Serverseitige Verschlüsselung". Um SSE (serverseitige Verschlüsselung mit StorageGRID-verwalteten Schlüsseln) zu verwenden, fügen Sie den `x-amz-server-side-encryption` Anforderungsheader nur in die CreateMultipartUpload-Anforderung ein. 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.
- Ein mehrteiliges hochgeladenes Objekt ist in einem"Asteimer" wenn die Aufnahme vor dem „Before“-Zeitstempel des Basis-Buckets begonnen wurde, unabhängig davon, wann der Upload abgeschlossen ist.

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

CompleteMultipartUpload

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

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

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.

Unterstützte Anfrageheader

Die folgenden Anfragezeilen werden unterstützt:

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

  Der `x-amz-storage-class` Header wirkt sich darauf aus, wie viele Objektkopien StorageGRID erstellt, wenn die passende ILM-Regel den angibt"Doppelte Provisionierung oder ausgewogene Aufnahmeoption".

- `STANDARD`

  (Standard) gibt einen Dual-Commit-Aufnahmevorgang 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-Aufnahmevorgang an, wenn die ILM-Regel die Option Dual Commit verwendet oder wenn die Option Balance zur Erstellung zwischenzeitaler Kopien zurückgreift.

  Wenn Sie ein Objekt in einen Bucket mit aktivierter S3-Objektsperrung aufnehmen, wird die `REDUCED_REDUNDANCY` Option ignoriert. Wenn Sie ein Objekt in einen Legacy-konformen Bucket aufnehmen, gibt die `REDUCED_REDUNDANCY` Option einen Fehler zurück. StorageGRID führt immer eine doppelte Einspeisung durch, um Compliance-Anforderungen zu erfüllen.

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

Nicht unterstützte Anforderungsheader

Die folgenden Anforderungsheader werden nicht unterstützt:

- `If-Match`
- `If-None-Match`

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

Versionierung

Durch diesen Vorgang ist ein mehrtei. 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, wird automatisch ein eindeutiges `versionId` Objekt für die Version des gespeicherten Objekts generiert. Dies `versionId` wird auch in der Antwort über den Antwortheader zurückgegeben `x-amz-version-id`.

Wenn die Versionierung unterbrochen wird, wird die Objektversion mit einer 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.

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.

Siehe "Fehlerbehebung bei Plattform-Services".

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` Anforderungskopf wird unterstützt. Der für eingereichte Wert `x-amz-storage-class` hat einen Einfluss darauf, wie StorageGRID Objektdaten bei der Aufnahme schützt, und nicht darauf, wie viele persistente Kopien des Objekts im StorageGRID System gespeichert werden (durch ILM bestimmt).

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

Folgende Werte können verwendet werden für `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 in der ILM-Regel angegebenen Objektkopien erstellen kann (synchrone Platzierung), hat der `x-amz-storage-class` Header keine Auswirkungen.

- `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. Diese `REDUCED_REDUNDANCY` Option ist am besten geeignet, wenn die mit dem Objekt übereinstimmende ILM-Regel eine einzige replizierte Kopie erstellt. In diesem Fall `REDUCED_REDUNDANCY` entfällt bei jedem Einspielvorgang die unnötige Erstellung und Löschung einer zusätzlichen Objektkopie.

  Die Verwendung der `REDUCED_REDUNDANCY` Option wird in anderen Fällen nicht empfohlen. `REDUCED_REDUNDANCY` Erhöhtes 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.

Die Angabe `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 mit aktivierter S3-Objektsperrung aufnehmen, wird die `REDUCED_REDUNDANCY` Option ignoriert. Wenn Sie ein Objekt in einen Legacy-konformen Bucket aufnehmen, gibt die `REDUCED_REDUNDANCY` Option einen Fehler zurück. StorageGRID führt immer eine doppelte Einspeisung durch, um Compliance-Anforderungen zu erfüllen.

Unterstützte Anfrageheader

Die folgenden Anfragezeilen werden unterstützt:

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

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

- `x-amz-meta-`, Gefolgt von einem Name-Wert-Paar, das benutzerdefinierte Metadaten enthält

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

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

  Wenn Sie die Option **Benutzerdefinierte Erstellungszeit** als Referenzzeit für eine ILM-Regel verwenden möchten, müssen Sie als Name der Metadaten verwenden, `creation-time` die beim Erstellen des Objekts aufgezeichnet werden. Beispiel:

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

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

  > Das Hinzufügen `creation-time` als benutzerdefinierte Metadaten ist nicht zulässig, wenn Sie einem Bucket ein Objekt hinzufügen, für das ältere Compliance-Funktionen aktiviert sind. Ein Fehler wird zurückgegeben.

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

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

  "Konfigurieren Sie die S3-Objektsperre über die S3-REST-API"

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

    Anforderungsheader für serverseitige Verschlüsselung

    > Informationen darüber, wie StorageGRID UTF-8-Zeichen verarbeitet, finden Sie unter "PutObject".

Anforderungsheader für serverseitige Verschlüsselung

Sie können die folgenden Anforderungsheader verwenden, um ein mehrteitiges 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`: Spezifizieren `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, lesen Sie die Überlegungen für "Serverseitige Verschlüsselung".

Nicht unterstützte Anforderungsheader

Der folgende Anforderungskopf wird nicht unterstützt:

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

  Der `x-amz-website-redirect-location` Header gibt zurück `XNotImplemented`.

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:

- `x-amz-checksum-sha256`
- `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`: Spezifizieren `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, lesen Sie die Überlegungen in "Serverseitige Verschlüsselung".

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

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

Nicht unterstützte Anforderungsheader

Die folgenden Anforderungsheader werden nicht unterstützt:

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

- `x-amz-trailer`

Versionierung

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 im StorageGRID-System angegeben `x-amz-copy-source-range` sind.

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`: Spezifizieren `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`: Spezifizieren `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, lesen Sie die Überlegungen in "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
InvalidDigest	400 Fehlerhafte Anfrage
InvalidVerschlüsselungAlgorithmFehler	400 Fehlerhafte Anfrage
InvalidTeil	400 Fehlerhafte Anfrage

Name	HTTP-Status
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
Vorbedingungen nicht möglich	412 Voraussetzung Fehlgeschlagen
AnforderungTimeTooSkewed	403 Verbotene
Servicenicht verfügbar	503 Service Nicht Verfügbar

Name	HTTP-Status
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
XComplianceKonflict	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 Operationen von StorageGRID

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-Antwort `<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

"Konsistenz"

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.
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

"Konsistenz"

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 Suchintegrationsservice 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 Metadaten-Benachrichtigungskonfiguration für den Bucket namens `bucket`ab.

```
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 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
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	Objekte, die mit dem Präfix übereinstimmen, werden von der Regel beeinflusst und ihre Metadaten werden an das angegebene Ziel gesendet. Geben Sie ein leeres Präfix an, um alle Objekte zu entsprechen. In das Element Regel aufgenommen.	Ja.
Ziel	Container-Tag für das Ziel einer Regel. In das Element Regel aufgenommen.	Ja.
Urne	URNE des Ziels, an dem Objektmetadaten gesendet werden. Muss der URN eines StorageGRID-Endpunkts mit den folgenden Eigenschaften sein: • `es` Muss das dritte Element sein. • Die URN muss mit dem Index und dem Typ enden, in dem die Metadaten gespeichert sind, in der Form `domain-name/myindex/mytype`. Endpunkte werden mithilfe der Mandanten-Manager oder der Mandanten-Management-API konfiguriert. Sie nehmen folgende Form: • `arn:aws:es:_region:account-ID_:domain/mydomain/myindex/mytype` • `urn:mysite:es:::mydomain/myindex/mytype` Der Endpunkt muss konfiguriert werden, bevor die Konfigurations-XML gesendet wird, oder die Konfiguration schlägt mit einem Fehler 404 fehl. Urne ist im Element Ziel enthalten.	Ja.

Antwortbeispiel

Die XML-Datei zwischen den `<MetadataNotificationConfiguration></MetadataNotificationConfiguration>` Tags zeigt, wie die Integration mit einem Endpunkt für die Suchintegration für den Bucket konfiguriert ist. In diesem Beispiel werden Objektmetadaten an einen Elasticsearch-Index mit dem Namen und dem Typ `2017` gesendet `current`, der in einer AWS-Domäne mit dem Namen gehostet wird `records`.

```
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-Integrationsservice für einzelne Buckets zu aktivieren. Die XML-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 Anfraentext 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 an ein Ziel und Objekte mit dem `/videos` Präfix an ein anderes senden `/images`.

Konfigurationen mit überlappenden Präfixen sind nicht gültig und werden beim Einreichen abgelehnt. Eine Konfiguration, die beispielsweise eine Regel für Objekte mit dem Präfix und eine zweite Regel für Objekte mit dem `test2` Präfix enthält `test`, ist nicht zulässig.

Ziele müssen mit dem URN eines StorageGRID-Endpunkts angegeben werden. Der Endpunkt muss

vorhanden sein, wenn die Metadaten-Benachrichtigungskonfiguration übermittelt wird, oder die Anforderung schlägt als fehl `400 Bad Request`. Die Fehlermeldung lautet: `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 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
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	Objekte, die mit dem Präfix übereinstimmen, werden von der Regel beeinflusst und ihre Metadaten werden an das angegebene Ziel gesendet. Geben Sie ein leeres Präfix an, um alle Objekte zu entsprechen. In das Element Regel aufgenommen.	Ja.
Ziel	Container-Tag für das Ziel einer Regel. In das Element Regel aufgenommen.	Ja.
Urne	URNE des Ziels, an dem Objektmetadaten gesendet werden. Muss der URN eines StorageGRID-Endpunkts mit den folgenden Eigenschaften sein: • `es` Muss das dritte Element sein. • Die URN muss mit dem Index und dem Typ enden, in dem die Metadaten gespeichert sind, in der Form `domain-name/myindex/mytype`. Endpunkte werden mithilfe der Mandanten-Manager oder der Mandanten-Management-API konfiguriert. Sie nehmen folgende Form: • `arn:aws:es:region:account-ID:domain/mydomain/myindex/mytype` • `urn:mysite:es:::mydomain/myindex/mytype` Der Endpunkt muss konfiguriert werden, bevor die Konfigurations-XML gesendet wird, oder die Konfiguration schlägt mit einem Fehler 404 fehl. Urne ist im Element Ziel enthalten.	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 werden Objektmetadaten für Objekte mit dem Präfix `/images` an ein Ziel gesendet, während Objektmetadaten für Objekte mit dem Präfix `/videos` an ein zweites Ziel gesendet werden.

```
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-1:3333333: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-1:22222222:domain/es-
domain/graphics/videotype</Urn>
        </Destination>
    </Rule>
</MetadataNotificationConfiguration>
```

Vom Suchintegrations-Service generierter JSON

Wenn Sie den Such-Integrationsservice für einen Bucket aktivieren, wird ein JSON-Dokument generiert und an den Zielendpunkt gesendet, wenn Metadaten oder Tags hinzugefügt, aktualisiert oder gelöscht werden.

Dieses Beispiel zeigt ein Beispiel für den JSON, der generiert werden könnte, wenn ein Objekt mit dem Schlüssel in einem Bucket mit `SGWS/Tagging.txt` dem Namen erstellt wird `test`. Der `test` Bucket ist nicht versioniert, daher ist das `versionId` Tag 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	Beispiel: Bucket-Region `us-east-1`
System-Metadaten	Größe	Objektgröße (in Byte) wie für einen HTTP-Client sichtbar

Typ	Elementname	Beschreibung
System-Metadaten	md5	Objekt-Hash
Benutzer-Metadaten	Metadaten *key:value*	Alle Benutzer-Metadaten des Objekts als Schlüssel-Wert-Paare
Tags	Tags *key:value*	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 durch eine modifizierte ListBuckets-Anforderung mit dem Abfrageparameter abgerufen `x-ntap-sg-usage` werden. 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:ListAllMyBuchets-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 zu den `ObjectCount` Werten und `DataBytes` in der Antwort bei. Löschmarkierungen werden nicht zur Gesamtmenge hinzugefügt `ObjectCount`.

Verwandte Informationen

"Konsistenz"

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 ANFORDERUNG „PUT Bucket-Compliance“ 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

Mit dieser Beispielanforderung können Sie die Compliance-Einstellungen für den Bucket mit dem Namen festlegen `mybucket`.

```
GET /mybucket/?x-ntap-sg-compliance HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

Antwortbeispiel

In der XML-Antwort `<SGCompliance>` werden die für den Bucket verwendeten Compliance-Einstellungen aufgeführt. 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 Aufbewahrungspflichten 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	• 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	• 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 als konform angelegt wurde, lautet der HTTP-Statuscode für die Antwort `404 Not Found` , mit einem S3-Fehlercode von `XNoSuchBucketCompliance`.

Veraltet: PUT Bucket Compliance Request

Die ANFORDERUNG „PUT Bucket-Compliance“ 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 werden Objekte in nun für zwei Jahre (1,051,200 Minuten) statt für ein Jahr aufbewahrt, beginnend bei der Aufnahme des Objekts in `mybucket` das Raster. 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	Die Länge des Aufbewahrungszeitraums für Objekte, die diesem Bucket hinzugefügt wurden, in Minuten Der Aufbewahrungszeitraum beginnt, wenn das Objekt in das Raster aufgenommen wird. **Wichtig** Wenn Sie einen neuen Wert für RetentionPeriodMinutes 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.

Name	Beschreibung
LegalAlte	• 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	• 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 Konsistenz von **strong-site** zu erzwingen, geben Sie die Anforderung für die Einhaltung von PUT Bucket erneut aus und fügen Sie den `Consistency-Control` HTTP-

Anforderungsheader wie folgt ein:

```
PUT /mybucket/?x-ntap-sg-compliance HTTP/1.1
Consistency-Control: strong-site
```

Fehlerantworten

- Wenn der Bucket nicht für die Konformität erstellt wurde, lautet der HTTP-Statuscode für die Antwort `404 Not Found`.
- Wenn `RetentionPeriodMinutes` in der Anforderung weniger als die aktuelle Aufbewahrungsfrist des Buckets liegt, lautet der HTTP-Statuscode `400 Bad Request`.

Verwandte Informationen

"Veraltet: PUT Bucket-Request-Änderungen aus Compliance-Gründen"

Verwalten von Zugriffsrichtlinien

Verwenden von Zugriffsrichtlinien

StorageGRID verwendet die Richtliniensprache 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

StorageGRID unterstützt drei Arten von Zugriffsrichtlinien:

- **Bucket-Richtlinien**, die mit den Operationen GetBucket Policy, PutBucket Policy und DeleteBucket Policy S3 API oder der Tenant Manager- oder Tenant Management API 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.
- **Sitzungsrichtlinien**, die Teil einer AssumeRole-Anforderung sind. Sitzungsrichtlinien gelten nur für die jeweilige Sitzung und definieren zusätzlich zu den durch die Gruppen- und Bucket-Richtlinie gewährten Berechtigungen die Berechtigungen, die der Benutzer hat.

> Es gibt keinen Unterschied in der Priorität zwischen Gruppen-, Bucket- und Sitzungsrichtlinien.

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.
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 Bedingungselement 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-Policy-Anweisung, die den Effekt „allow“ verwendet, um den Principals, der Admin-Gruppe und der Finanzgruppe `federated-group/finance` Berechtigungen zur Ausführung der Aktion `s3:ListBucket` für den Bucket namens und die Aktion `s3:GetObject` für alle Objekte innerhalb dieses Buckets `mybucket` zu geben `federated-group/admin`.

```
{
  "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:s3:::mybucket",
        "arn:aws: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 den Header in der Anforderung „PutBucket Policy“ festlegen `Consistency-Control` oder die Konsistenzanforderung „PUT Bucket“ 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.

Was ist eine Sitzungsrichtlinie?

Eine Sitzungsrichtlinie ist eine Zugriffsrichtlinie, die die während einer bestimmten Sitzung verfügbaren Berechtigungen vorübergehend einschränkt, beispielsweise wenn ein Benutzer eine Gruppe übernimmt. Eine Sitzungsrichtlinie kann nur eine Teilmenge der Berechtigungen zulassen und keine zusätzlichen Berechtigungen erteilen. Die Gruppe selbst verfügt möglicherweise über umfassendere Berechtigungen.

Verwenden Sie ARN in den Richtlinienerklärungen

In den Richtlinienerklärungen 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 Identitätressource 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 oder alternativ `NotResource` zum Ausschluss gekennzeichnet `Resource`.
- 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 Richtlinienanweisung Zugriff auf die Ressource erlaubt/verweigert wird.

- Jede Richtlinienanweisung in einer Bucket-Richtlinie muss ein Principal Element enthalten. Richtlinienanweisungen 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 die Organisation und der Benutzername `Alex` wird gelöscht. Wenn ein neuer Alex der Organisation Beitritt und demselben Benutzernamen zugewiesen wird `Alex`, erbt der neue Benutzer möglicherweise unbeabsichtigt die Berechtigungen, die dem ursprünglichen Benutzer gewährt wurden.

- 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.

Berechtigungen	S3-REST-API-OPERATIONEN	Individuell für StorageGRID
s3:GetBucketBenachrichtigung	GetBucketNotificationConfiguration	
s3:GetBucketObjectLockConfiguration	GetObjectLockConfiguration	
s3:GetBucketPolicy	GetBucketPolicy	
s3:GetBucketTagging	GetBucketTagging	
s3:GetBucketVersionierung	GetBucketVersioning	
s3:GetLifecycleKonfiguration	GetBucketLifecycleKonfiguration	
s3:GetReplicationConfiguration	GetBucketReplication	
s3:ListAllMyBuchs	• ListBuchs • GET Storage-Auslastung	Ja, für DIE GET Storage-Nutzung. **Hinweis**: Nur in Gruppenrichtlinien verwenden.
s3:ListBucket	• ListObjekte • HeadBucket • Objekt restoreObject	
s3:ListBucketMultipartUploads	• ListMultipartUploads • Objekt restoreObject	
s3:ListBucketVersions	Get Bucket-Versionen	
s3:PutBucketCompliance	PUT Bucket-Compliance (veraltet)	Ja.
s3:PutBucketConsistency	PUT Bucket-Konsistenz	Ja.
s3:PutBucketCORS	• DeleteBucketCors† • PutBucketCors	
s3:PutVerschlüsselungKonfiguration	• DeleteBucketEncryption • PutBucketEncryption	
s3:PutBucketLastAccessTime	PUT Bucket-Zeit für den letzten Zugriff	Ja.

Berechtigungen	S3-REST-API-OPERATIONEN	Individuell für StorageGRID
s3:PutBucketMetadataBenachrichtigung	PUT Bucket-Metadaten-Benachrichtigungskonfiguration	Ja.
s3:PutBucketNotification	PutBucketNotificationKonfiguration	
s3:PutBucketObjectLockConfiguration	• CreateBucket mit dem `x-amz-bucket-object-lock-enabled: true` Anforderungsheader (erfordert auch die Berechtigung s3:CreateBucket) • PutObjectLockKonfiguration	
s3:PutBucketPolicy	PutBucketPolicy	
s3:PutBucketTagging	• DeleteBucketTagging† • PutBucketTagging	
s3:PutBucketVersionierung	PutBucketVersioning	
s3:PutLifecycleKonfiguration	• DeleteBucketLifecycle† • PutBucketLifecycleKonfiguration	
s3:PuteReplikationKonfiguration	PutBucketReplication	Ja, separate Berechtigungen für PUT und DELETE

Berechtigungen, die sich auf Objekte beziehen

Berechtigungen	S3-REST-API-OPERATIONEN	Individuell für StorageGRID
s3:AbortMehrteilaUpload	• AbortMehrteilaUpload • Objekt restoreObject	
s3:BypassGovernanceAufbewahrung	• DeleteObject • Objekte deObjekteObjekte • PutObjectRetention	
s3:DeleteObject	• DeleteObject • Objekte deObjekteObjekte • Objekt restoreObject	

Berechtigungen	S3-REST-API-OPERATIONEN	Individuell für StorageGRID
s3:DeleteObjectTagging	DeleteObjectTagging	
s3:DeleteObjectVersionTagging	DeleteObjectTagging (eine spezifische Version des Objekts)	
s3:DeleteObjectVersion	DeleteObject (eine bestimmte Version des Objekts)	
s3:GetObject	• 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	• PutObject • CopyObject • Objekt restoreObject • CreateMultipartUpload • CompleteMultipartUpload • UploadTeil • UploadPartCopy	
s3:PuttObjectLegalOld	PutObjectLegalHold	
s3:PutObjectRetention	PutObjectRetention	

Berechtigungen	S3-REST-API-OPERATIONEN	Individuell für StorageGRID
s3:PuttObjectTagging	PutObjectTagging	
s3:PuttObjectVersionTagging	PutObjectTagging (eine spezifische Version des Objekts)	
s3:PutOverwrite Object	• 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 das Überschreiben zulässt und die Berechtigung „PutOverwriteObject“ auf „Verweigern“ gesetzt ist, kann der Client die Daten, benutzerdefinierten Metadaten oder Objektmarkierungen eines Objekts nicht überschreiben. Wenn außerdem das Kontrollkästchen **Client-Änderung verhindern** aktiviert ist (**Konfiguration** > **Sicherheitseinstellungen** > **Netzwerk und Objekte**), überschreibt diese Einstellung die Einstellung der PutOverwriteObject-Berechtigung.

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 Bedingungselement 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).
StringEqusIgnoreCase	Vergleicht einen Schlüssel mit einem Zeichenfolgenwert, der auf exakter Übereinstimmung basiert (Groß-/Kleinschreibung wird ignoriert).
StringNotEqualesIgnoreCase	Vergleicht einen Schlüssel mit einem String-Wert, der auf negatives Matching basiert (Groß-/Kleinschreibung wird ignoriert).

Bedingungsoperatoren	Beschreibung
StringLike	Vergleicht einen Schlüssel mit einem Zeichenfolgenwert, der auf exakter Übereinstimmung basiert (Groß-/Kleinschreibung wird beachtet). Kann * und ? Platzhalterzeichen enthalten.
StringNotLike	Vergleicht einen Schlüssel mit einem Zeichenfolgenwert, der auf negatives Matching basiert (Groß-/Kleinschreibung wird beachtet). Kann * und ? Platzhalterzeichen enthalten.
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 negatiertem Abgleich.
Null	Überprüft, ob im aktuellen Anforderungskontext ein Bedingungsschlüssel vorhanden ist.
IfExists	Wird an jeden Bedingungsoperator außer der Nullbedingung angehängt, um das Fehlen dieses Bedingungsschlüssels zu prüfen. Gibt TRUE zurück, wenn der Bedingungsschlüssel nicht vorhanden ist.

Unterstützte Bedingungsschlüssel

Zustandsschlüssel	Aktionen	Beschreibung
aws:SourceIp	IP-Operatoren	Vergleicht mit der IP-Adresse, von der die Anfrage gesendet wurde. Kann für Bucket- oder Objektvorgänge verwendet werden **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. **Hinweis**: Wenn ein Drittanbieter-, nicht-transparenter Load Balancer verwendet wird, wird dies mit der IP-Adresse dieses Load Balancer verglichen. Jede `X-Forwarded-For` Kopfzeile wird ignoriert, da ihre Gültigkeit nicht ermittelt werden kann.
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 3:GetObjectTagging s3:GetObjectVersion s3:GetObjectVersionAkl s3:GetObjectVersionTagging s3:PutObjectAcl s3:PuttObjectTagging s3:PutObjectVersionAcl s3:PuttObjectVersionTagging	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:Objektsperrmodus	s3:PutObject	Vergleichbar mit dem `object-lock-mode` aus dem Anforderungsheader in der PutObject-, CopyObject- und CreateMultipartUpload-Anforderung erweitert.
s3:Objektsperrmodus	s3:PutObjectRetention	Vergleichbar mit dem `object-lock-mode` aus dem XML-Textkörper in der PutObjectRetention-Anforderung erweitert.
s3:verbleibende Object-Lock-Retention-Tage	s3:PutObject	Vergleicht das im Anforderungskopf angegebene oder aus dem Standardaufbewahrungszeitraum berechnete Aufbewahrungsdatum `x-amz-object-lock-retain-until-date`, um sicherzustellen, dass diese Werte innerhalb des zulässigen Bereichs für die folgenden Anforderungen liegen: • 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:PuttObjectTagging s3:PuttObjectVersionTagging	Erfordert einen bestimmten Tag-Schlüssel und einen bestimmten Wert, wenn die Objektanforderung Tagging beinhaltet.
s3:x-amz-serverseitige-Verschlüsselung-Kundenalgorithmus	s3:PutObject	Vergleichbar mit dem `sse-customer-algorithm` oder zum `copy-source-sse-customer-algorithm` aus dem Anforderungsheader in den Anforderungen PutObject, CopyObject, CreateMultipartUpload, UploadPart, UploadPartCopy und CompleteMultipartUpload erweitert.

Geben Sie Variablen in einer Richtlinie an

Sie können Variablen in Richtlinien verwenden, um die Richtlinieninformationen auszufüllen, wenn sie verfügbar sind. Sie können Richtlinienvariablen im Element und in Stringvergleiche im `Condition` Element verwenden `Resource`.

In diesem Beispiel ist die Variable `${aws:username}` Teil des Elements Ressource:

```
"Resource": "arn:aws:s3:::bucket-name/home/${aws:username}/*"
```

In diesem Beispiel ist die Variable `${aws:username}` Teil des Bedingungswerts im Bedingungsblock:

```
"Condition": {
    "StringLike": {
      "s3:prefix": "${aws:username}/*"
        ...
},
        ...
```

Variabel	Beschreibung
`${aws:SourceIp}`	Verwendet den SourceIp-Schlüssel als bereitgestellte Variable.
`${aws:username}`	Verwendet den Benutzernamen-Schlüssel als bereitgestellte Variable.
`${s3:prefix}`	Verwendet den Service-spezifischen Präfixschlüssel als bereitgestellte Variable.
`${s3:max-keys}`	Verwendet die Service-spezifische max-keys als die angegebene Variable.
`${*}`	Sonderzeichen. Verwendet das Zeichen als Literal * -Zeichen.
`${?}`	Sonderzeichen. Verwendet das Zeichen als Literal ? Zeichen.
`${$}`	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 Richtlinienvalidierung 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
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

Richtlinienbeschreibung	Richtlinientyp	Verhalten von Amazon	Verhalten von StorageGRID
Principal ist eine lokale Gruppe	Eimer	Ungültiger Principal	Gültig
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 **Konfiguration** > **Sicherheit** > **Sicherheitseinstellungen** > **Netzwerk und Objekte** 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"
- "Beispiel einer Sitzungsrichtlinie"
- "Objektmanagement mit ILM"
- "Verwenden Sie ein Mandantenkonto"

Beispiel für eine Sitzungsrichtlinie

Verwenden Sie das folgende Beispiel, um eine StorageGRID -Sitzungsrichtlinie zu erstellen.

Beispiel: Einrichten einer Sitzungsrichtlinie, die den Objektabruf ermöglicht

In diesem Beispiel darf der Sitzungsprinzipal nur Objekte aus Bucket1 abrufen. Alle anderen Aktionen werden implizit verweigert, mit Ausnahme von StorageGRID-spezifischen Aktionen, wie z. B. der Verwendung des"s3:PutOverwrite Object" Erlaubnis. Die Sitzungsrichtlinie kann beim Aufruf der AssumeRole-API als JSON-Datei bereitgestellt werden.

```
{
  "Statement": [
    {
      "Action": "s3:GetObject",
      "Effect": "Allow",
      "Resource": "arn:aws:s3:::bucket1/*"
    }
  ]
}
```

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. Sie konfigurieren eine Bucket-Richtlinie mithilfe der S3-PutBucketPolicy-API über eines der folgenden Tools:

- "Mandanten-Manager".
- AWS CLI mit diesem Befehl (siehe "Operationen auf Buckets"):

```
> 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 hat jeder in einem bestimmten Konto vollen Zugriff auf einen Bucket, während jeder in einem anderen angegebenen Konto nur berechtigt ist, den Bucket aufzulisten und GetObject-Operationen für Objekte im Bucket durchzuführen, beginnend mit dem `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, die der Gruppe im angegebenen Konto angehören, `Marketing` vollen Zugriff erhalten.

```
{
  "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 hat der föderierte Benutzer Alex vollen Zugriff auf den `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 stellt der `Deny` Effekt für PutOverwriteObject und DeleteObject sicher, dass niemand die Objektdaten, benutzerdefinierten 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 kein `Principal` Element in der Richtlinie, weil es 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 Objektvorgängen 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 (Ende des Lebenszyklus)

Nutzen Sie die Swift REST API

Die Unterstützung für die Swift-API hat das Ende ihres Lebenszyklus erreicht und wird in einer zukünftigen Version entfernt.

Swift-Details wurden aus dieser Version der doc-Site entfernt. Siehe "StorageGRID 11.8: Verwenden Sie Swift REST API".