



Verwenden Sie StorageGRID

StorageGRID software

NetApp
October 21, 2025

Inhalt

Verwenden Sie StorageGRID Mandanten und -Clients	1
Verwenden eines Mandantenkontos	1
Verwenden eines Mandantenkontos	1
So melden Sie sich an und ab	2
Tenant Manager-Dashboard verstehen	7
Mandantenverwaltungs-API	10
Grid-Föderation-Verbindungen verwenden	14
Verwalten von Gruppen und Benutzern	25
S3-Zugriffsschlüssel verwalten	45
S3-Buckets verwalten	51
Verwalten von S3-Plattformdiensten	74
Verwenden Sie die S3 REST-API	107
Unterstützte Versionen und Updates der S3 REST API	107
Kurzreferenz: Unterstützte S3-API-Anfragen	110
Testen der S3 REST API-Konfiguration	129
So implementiert StorageGRID die S3 REST API	130
Unterstützung für Amazon S3 REST API	146
Benutzerdefinierte StorageGRID -Vorgänge	197
Bucket- und Gruppenzugriffsrichtlinien	218
In den Prüfprotokollen verfolgte S3-Operationen	245
Swift REST API verwenden (Ende der Lebensdauer)	246
Verwenden Sie die Swift REST-API	246

Verwenden Sie StorageGRID Mandanten und -Clients

Verwenden eines Mandantenkontos

Verwenden eines Mandantenkontos

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

Was ist ein Mieterkonto?

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

Mandantenkonten können verwendet werden, um gespeicherte Objekte nach verschiedenen Entitäten zu trennen. Beispielsweise können mehrere Mandantenkonten für einen der folgenden Anwendungsfälle verwendet werden:

- **Anwendungsfall für Unternehmen:** Wenn das StorageGRID -System innerhalb eines Unternehmens verwendet wird, kann der Objektspeicher des Grids nach den verschiedenen Abteilungen der Organisation getrennt sein. Beispielsweise kann es Mandantenkonten für die Marketingabteilung, die Kundensupportabteilung, die Personalabteilung usw. geben.



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 für Dienstanbieter:** Wenn das StorageGRID -System von einem Dienstanbieter verwendet wird, kann der Objektspeicher des Grids nach den verschiedenen Einheiten, die den Speicher mieten, getrennt sein. Beispielsweise kann es Mandantenkonten für Unternehmen A, Unternehmen B, Unternehmen C usw. geben.

So erstellen Sie ein Mieterkonto

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

- Grundlegende Informationen, einschließlich Mandantenname, Clienttyp (S3) und optionalem Speicherkontingent.
- Berechtigungen für das Mandantenkonto, z. B. ob das Mandantenkonto S3-Plattformdienste verwenden, seine eigene Identitätsquelle konfigurieren, S3 Select verwenden oder eine Grid-Föderationsverbindung verwenden kann.
- Der anfängliche Root-Zugriff für den Mandanten, basierend darauf, ob das StorageGRID -System lokale Gruppen und Benutzer, Identitätsföderation oder Single Sign-On (SSO) verwendet.

Darüber hinaus können Grid-Administratoren die S3 Object Lock-Einstellung für das StorageGRID -System aktivieren, wenn S3-Mandantenkonten gesetzliche Anforderungen erfüllen müssen. Wenn S3 Object Lock

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

Konfigurieren von S3-Mandanten

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

- Identitätsföderation einrichten (es sei denn, die Identitätsquelle wird mit dem Grid geteilt)
- Verwalten von Gruppen und Benutzern
- Verwenden Sie die Grid-Föderation für Kontoklone und Cross-Grid-Replikation
- S3-Zugriffsschlüssel verwalten
- Erstellen und Verwalten von S3-Buckets
- Verwenden Sie S3-Plattformdienste
- Verwenden Sie S3 Select
- Überwachen der Speichernutzung



Obwohl Sie S3-Buckets mit dem Tenant Manager erstellen und verwalten können, müssen Sie einen "[S3-Client](#)" oder "[S3-Konsole](#)" um Objekte aufzunehmen und zu verwalten.

So melden Sie sich an und ab

Sign in

Sie erreichen den Mandantenmanager, indem Sie die URL des Mandanten in die Adressleiste eines "[unterstützter Webbrowser](#)" .

Bevor Sie beginnen

- Sie haben Ihre Anmeldedaten.
- Sie verfügen über eine URL für den Zugriff auf den Mandanten-Manager, die Sie von Ihrem Grid-Administrator erhalten haben. Die URL sieht wie eines dieser Beispiele 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 vollqualifizierten Domänennamen (FQDN), die IP-Adresse eines Admin-Knotens oder die virtuelle IP-Adresse einer HA-Gruppe von Admin-Knoten. Es kann auch eine Portnummer, die 20-stellige Mandantenkonto-ID oder beides enthalten.

- Wenn die URL nicht die 20-stellige Konto-ID des Mandanten enthält, verfügen Sie über diese Konto-ID.
- Sie verwenden eine "[unterstützter Webbrowser](#)" .
- Cookies sind in Ihrem Webbrowser aktiviert.
- Sie gehören zu einer Benutzergruppe, die "[spezifische Zugriffsberechtigungen](#)" .

Schritte

1. Starten Sie eine "[unterstützter Webbrowser](#)" .
2. Geben Sie in der Adressleiste des Browsers die URL für den Zugriff auf den Tenant Manager ein.
3. Wenn eine Sicherheitswarnung angezeigt wird, installieren Sie das Zertifikat mithilfe des Installationsassistenten des Browsers.
4. Sign in .

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

Kein SSO verwenden

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

- Die Anmeldeseite des Grid Managers. Wählen Sie den Link **Mandantenanmeldung** aus.

The screenshot shows the login interface for the NetApp StorageGRID Grid Manager. At the top, the title 'NetApp StorageGRID® Grid Manager' is displayed. Below it, there are two input fields: 'Username' and 'Password'. A blue 'Sign in' button is positioned below the password field. At the bottom of the page, there is a footer with three links: 'Tenant sign in', 'NetApp support', and 'NetApp.com'. The 'Tenant sign in' link is highlighted with a green rectangular border.

- Die Anmeldeseite des Tenant Managers. Das Feld **Konto** ist möglicherweise bereits ausgefüllt, wie unten gezeigt.



Tenant Manager

Recent

Account

Username

Password

Sign in

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

i. Wenn die 20-stellige Konto-ID des Mandanten nicht angezeigt wird, wählen Sie den Namen des Mandantenkontos aus, wenn dieser in der Liste der letzten Konten angezeigt wird, oder geben Sie die Konto-ID ein.

ii. Geben Sie Ihren Benutzernamen und Ihr Passwort ein.

iii. Wählen Sie * Sign in*.

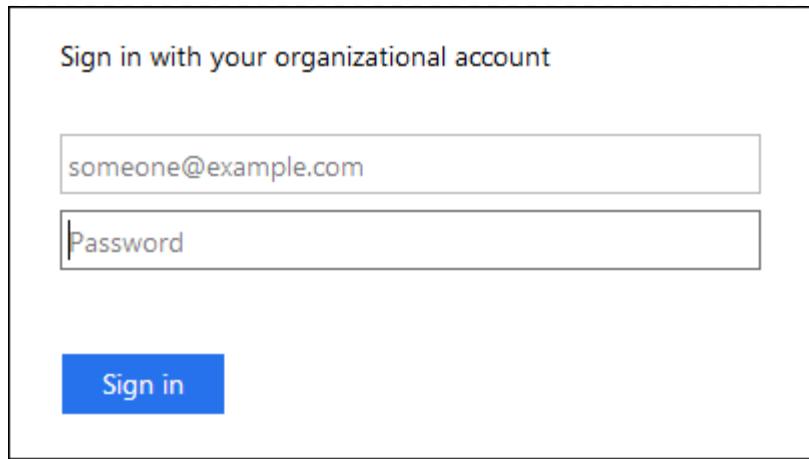
Das Tenant Manager-Dashboard wird angezeigt.

iv. Wenn Sie ein erstes Passwort von jemand anderem erhalten haben, wählen Sie **Benutzername > Passwort ändern**, um Ihr Konto zu sichern.

Verwenden von SSO

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

- Die SSO-Seite Ihrer Organisation. Beispiel:



Sign in with your organizational account

someone@example.com

Password

Sign in

Geben Sie Ihre Standard-SSO-Anmeldeinformationen ein und wählen Sie * Sign in*.

- Die SSO-Anmeldeseite des Tenant Managers.
 - i. Wenn die 20-stellige Konto-ID des Mandanten nicht angezeigt wird, wählen Sie den Namen des Mandantenkontos aus, wenn dieser in der Liste der letzten Konten angezeigt wird, oder geben Sie die Konto-ID ein.
 - ii. Wählen Sie * Sign in*.
 - iii. Sign in mit Ihren Standard-SSO-Anmeldeinformationen auf der SSO-Anmeldeseite Ihrer Organisation an.

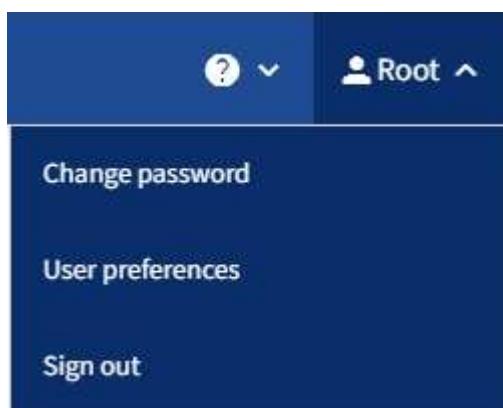
Das Tenant Manager-Dashboard wird angezeigt.

Vom Tenant Manager abmelden

Wenn Sie mit der Arbeit mit dem Tenant Manager fertig sind, müssen Sie sich abmelden, um sicherzustellen, dass nicht autorisierte Benutzer nicht auf das StorageGRID -System zugreifen können. Wenn Sie Ihren Browser schließen, werden Sie je nach den Cookie-Einstellungen Ihres Browsers möglicherweise nicht vom System abgemeldet.

Schritte

1. Suchen Sie das Dropdown-Menü für den Benutzernamen 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 des Tenant Managers wird angezeigt.



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

- Wenn SSO aktiviert ist:

Sie sind von allen Admin-Knoten abgemeldet, auf die Sie zugegriffen haben. Die StorageGRID Sign in wird angezeigt. Der Name des Mandantenkontos, auf das Sie gerade zugegriffen haben, wird standardmäßig im Dropdown-Menü **Letzte Konten** aufgeführt und die **Konto-ID** des Mandanten wird angezeigt.



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

Tenant Manager-Dashboard verstehen

Das Tenant Manager-Dashboard bietet einen Überblick über die Konfiguration eines Tenant-Kontos und den von Objekten in den Buckets (S3) oder Containern (Swift) des Tenant verwendeten Speicherplatz. 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.



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 im folgenden Beispiel aus:

Dashboard

16 Buckets
[View buckets](#)

2 Platform services endpoints
[View endpoints](#)

0 Groups
[View groups](#)

1 User
[View users](#)

Storage usage [?](#)

6.5 TB of 7.2 TB used

0.7 TB (10.1%) remaining



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

Top buckets by capacity limit usage [?](#)

Bucket name	Usage
Bucket-10	82%
Bucket-03	57%
Bucket-15	20%

Tenant details [?](#)

Name:	Tenant02
ID:	3341 1240 0546 8283 2208
<input checked="" type="checkbox"/> Platform services enabled	
<input checked="" type="checkbox"/> Can use own identity source	
<input checked="" type="checkbox"/> S3 Select enabled	

Mandantenkontoinformationen

Oben im Dashboard wird die Anzahl der konfigurierten Buckets oder Container, Gruppen und Benutzer angezeigt. Außerdem wird die Anzahl der Plattformdienst-Endpunkte angezeigt, sofern welche konfiguriert wurden. Wählen Sie die Links aus, um die Details anzuzeigen.

Abhängig von der "Berechtigungen zur Mandantenverwaltung" Abhängig von Ihren Einstellungen und den von Ihnen konfigurierten Optionen werden im Rest des Dashboards verschiedene Kombinationen aus Richtlinien, Speichernutzung, Objektinformationen und Mandantendetails angezeigt.

Speicher- und Kontingentnutzung

Das Fenster „Speichernutzung“ enthält die folgenden Informationen:

- Die Menge der Objektdaten für den Mandanten.

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

- Wenn ein Kontingent festgelegt ist, die Gesamtmenge des für Objektdaten verfügbaren Speicherplatzes sowie die Menge und der Prozentsatz des verbleibenden Speicherplatzes. Das Kontingent begrenzt die Menge der Objektdaten, die aufgenommen werden können.



Die Kontingentnutzung basiert auf internen Schätzungen und kann in einigen Fällen überschritten werden. Beispielsweise überprüft StorageGRID das Kontingent, wenn ein Mandant mit dem Hochladen von Objekten beginnt, und lehnt neue Aufnahmen ab, wenn der Mandant das Kontingent überschritten hat. StorageGRID berücksichtigt jedoch nicht die Größe des aktuellen Uploads, wenn es feststellt, ob das Kontingent überschritten wurde. Wenn Objekte gelöscht werden, kann es sein, dass ein Mandant vorübergehend daran gehindert wird, neue Objekte hochzuladen, bis die Kontingentnutzung neu berechnet wird. Die Berechnung der Kontingentnutzung kann 10 Minuten oder länger dauern.

- Ein Balkendiagramm, das die relativen Größen der größten Eimer oder Behälter darstellt.

Sie können den Cursor über ein beliebiges Diagrammsegment bewegen, um den gesamten von diesem Bucket oder Container belegten Speicherplatz anzuzeigen.



- Passend zum Balkendiagramm eine Liste der größten Buckets oder Container, einschließlich der Gesamtmenge 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 der Mandant mehr als neun Buckets oder Container hat, werden alle anderen Buckets oder Container zu einem einzigen Eintrag am Ende der Liste zusammengefasst.



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

Warnmeldungen zur Kontingentnutzung

Wenn im Grid Manager Warnmeldungen zur Kontingentnutzung aktiviert wurden, werden diese

Warnmeldungen im Tenant Manager angezeigt, wenn das Kontingent niedrig ist oder überschritten wird, und zwar wie folgt:

- Wenn 90 % oder mehr des Kontingents eines Mandanten genutzt wurden, wird die Warnung „Hohe Auslastung des Mandantenkontingents“ ausgelöst.

Bitten Sie Ihren Grid-Administrator, das Kontingent zu erhöhen.

- Wenn Sie Ihr Kontingent überschreiten, werden Sie durch eine Benachrichtigung darüber informiert, dass Sie keine neuen Objekte hochladen können.

Kapazitätslimitnutzung

Wenn Sie für Ihre Buckets eine Kapazitätsgrenze festgelegt haben, zeigt das Tenant Manager-Dashboard eine Liste der Top-Buckets nach Kapazitätsgrenzauslastung an.

Wenn für einen Bucket kein Limit festgelegt ist, ist seine Kapazität unbegrenzt. Wenn Ihr Mandantenkonto jedoch über ein Gesamtspeicherkontingent verfügt und dieses Kontingent erreicht ist, können Sie unabhängig von der verbleibenden Kapazitätsgrenze eines Buckets keine weiteren Objekte aufnehmen.

Endpunktfehler

Wenn Sie den Grid Manager verwendet haben, um einen oder mehrere Endpunkte für die Verwendung mit Plattformdiensten zu konfigurieren, zeigt das Tenant Manager-Dashboard eine Warnung an, wenn innerhalb der letzten sieben Tage Endpunktfehler aufgetreten sind.

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

Um Einzelheiten zu sehen über "Plattformdienst-Endpunktfehler", wählen Sie **Endpunkte** aus, um die Seite „Endpunkte“ anzuzeigen.

Mandantenverwaltungs-API

Grundlegendes zur API für die Mandantenverwaltung

Sie können Systemverwaltungsaufgaben mithilfe der Tenant Management REST API anstelle der Tenant Manager-Benutzeroberfläche ausführen. Beispielsweise möchten Sie die API möglicherweise verwenden, um Vorgänge zu automatisieren oder mehrere Entitäten, z. B. Benutzer, schneller zu erstellen.

Die Tenant Management API:

- Verwendet die Open-Source-API-Plattform Swagger. Swagger bietet eine intuitive Benutzeroberfläche, die Entwicklern und Nicht-Entwicklern die Interaktion mit der API ermöglicht. Die Swagger-Benutzeroberfläche bietet vollständige Details und Dokumentation für jeden API-Vorgang.
- Anwendung ["Versionierung zur Unterstützung unterbrechungsfreier Upgrades"](#).

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

1. Sign in .

2. Wählen Sie oben im Mandanten-Manager das Hilfesymbol und dann **API-Dokumentation** aus.

API-Operationen

Die Tenant Management API organisiert die verfügbaren API-Operationen in den folgenden Abschnitten:

- **Konto**: Vorgänge auf dem aktuellen Mandantenkonto, einschließlich des Abrufens von Informationen zur Speichernutzung.
- **auth**: Vorgänge zum Durchführen der Benutzersitzungsauthentifizierung.

Die Tenant Management API unterstützt das Bearer Token Authentication Scheme. Für die Anmeldung als Mandant geben Sie im JSON-Text der Authentifizierungsanfrage einen Benutzernamen, ein Kennwort und eine Konto-ID an (d. h. `POST /api/v3/authorize`). Wenn der Benutzer erfolgreich authentifiziert wurde, wird ein Sicherheitstoken zurückgegeben. Dieses Token muss im Header nachfolgender API-Anfragen bereitgestellt werden („Authorization: Bearer Token“).

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



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

- **config**: Vorgänge im Zusammenhang mit der Produktversion und den Versionen der Tenant Management API. Sie können die Produktversion und die Hauptversionen der von dieser Version unterstützten API auflisten.
- **Container**: Vorgänge an S3-Buckets oder Swift-Containern.
- **deaktivierte Funktionen**: Vorgänge zum Anzeigen von Funktionen, die möglicherweise deaktiviert wurden.
- **Endpunkte**: Vorgänge zum Verwalten eines Endpunkts. Endpunkte ermöglichen einem S3-Bucket die Verwendung eines externen Dienstes für die StorageGRID CloudMirror-Replikation, Benachrichtigungen oder Suchintegration.
- **grid-federation-connections**: Operationen an Grid-Föderationsverbindungen und Cross-Grid-Replikation.
- **Gruppen**: Vorgänge zum Verwalten lokaler Mandantengruppen und zum Abrufen föderierter Mandantengruppen aus einer externen Identitätsquelle.
- **Identitätsquelle**: Vorgänge zum Konfigurieren einer externen Identitätsquelle und zum manuellen Synchronisieren von föderierten Gruppen- und Benutzerinformationen.
- **ilm**: Vorgänge an den Einstellungen des Information Lifecycle Management (ILM).
- **Regionen**: Vorgänge zum Bestimmen, welche Regionen für das StorageGRID -System konfiguriert wurden.
- **s3**: Vorgänge zum Verwalten von S3-Zugriffsschlüsseln für Mandantenbenutzer.
- **s3-object-lock**: Vorgänge an globalen S3-Objektsperreinstellungen, die zur Unterstützung der Einhaltung gesetzlicher Vorschriften verwendet werden.
- **Benutzer**: Vorgänge zum Anzeigen und Verwalten von Mandantenbenutzern.

Details zum Vorgang

Wenn Sie die einzelnen API-Vorgänge erweitern, können Sie deren HTTP-Aktion, Endpunkt-URL, eine Liste aller erforderlichen oder optionalen Parameter, ein Beispiel für den Anforderungstext (falls erforderlich) und die

möglichen Antworten sehen.

API-Anfragen stellen



Alle API-Operationen, die Sie über die API-Dokumentationswebseite durchführen, sind Live-Operationen. Achten Sie darauf, dass Sie nicht versehentlich Konfigurationsdaten oder andere Daten erstellen, aktualisieren oder löschen.

Schritte

1. Wählen Sie die HTTP-Aktion aus, um die Anforderungsdetails anzuzeigen.
2. Stellen Sie fest, ob für die Anforderung zusätzliche Parameter erforderlich sind, beispielsweise eine Gruppen- oder Benutzer-ID. Besorgen Sie sich dann diese Werte. Möglicherweise müssen Sie zuerst eine andere API-Anfrage stellen, um die benötigten Informationen zu erhalten.
3. Stellen Sie fest, ob Sie den Beispielanforderungstext ändern müssen. Wenn ja, können Sie **Modell** auswählen, um die Anforderungen für jedes Feld zu erfahren.
4. Wählen Sie **Ausprobieren**.
5. Geben Sie alle erforderlichen Parameter an oder ändern Sie den Anforderungstext nach Bedarf.
6. Wählen Sie **Ausführen**.
7. Überprüfen Sie den Antwortcode, um festzustellen, ob die Anfrage erfolgreich war.

Versionierung der Mandantenverwaltungs-API

Die Tenant Management API verwendet Versionierung, um unterbrechungsfreie Upgrades zu unterstützen.

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

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

Die Hauptversion der API wird erhöht, wenn Änderungen vorgenommen werden, die mit älteren Versionen *nicht kompatibel* sind. Die Nebenversion der API wird erhöht, wenn Änderungen vorgenommen werden, die mit älteren Versionen *kompatibel* sind. Zu den kompatiblen Änderungen gehört das Hinzufügen neuer Endpunkte oder neuer Eigenschaften.

Das folgende Beispiel veranschaulicht, wie die API-Version je nach Art der vorgenommenen Änderungen erhöht wird.

Art der Änderung an der 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, ist nur die neueste Version der API aktiviert. Wenn Sie jedoch auf eine neue Funktionsversion von StorageGRID aktualisieren, 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 Swagger-API-Dokumentation. ["Grid-Management-API"](#) für weitere Informationen. Sie sollten die Unterstützung für die ältere Version deaktivieren, nachdem Sie alle API-Clients aktualisiert haben, um die neuere Version zu verwenden.

Veraltete Anfragen werden auf folgende Weise als veraltet gekennzeichnet:

- Der Antwortheader lautet „Deprecated: true“
- Der JSON-Antworttext enthält „deprecated“: true
- Zu nms.log wird eine veraltete Warnung hinzugefügt. Beispiel:

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

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

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

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

Angeben einer API-Version für eine Anfrage

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

```
curl https://[IP-Address]/api/v4/grid/accounts
curl -H "Api-Version: 4" https://[IP-Address]/api/grid/accounts
```

Schutz vor Cross-Site Request Forgery (CSRF)

Sie können zum Schutz vor Cross-Site Request Forgery (CSRF)-Angriffen auf StorageGRID beitragen, indem Sie CSRF-Token verwenden, um die Authentifizierung mithilfe von Cookies zu verbessern. Der Grid Manager und der Tenant Manager

aktivieren diese Sicherheitsfunktion automatisch. Andere API-Clients können bei der Anmeldung auswählen, ob sie diese aktivieren möchten.

Ein Angreifer, der eine Anfrage an eine andere Site auslösen kann (z. B. mit einem HTTP-Formular-POST), kann dafür sorgen, dass bestimmte Anfragen unter Verwendung der Cookies des angemeldeten Benutzers gestellt werden.

StorageGRID schützt durch die Verwendung von CSRF-Token vor CSRF-Angriffen. Wenn diese Option aktiviert ist, muss der Inhalt eines bestimmten Cookies mit dem Inhalt eines bestimmten Headers oder eines bestimmten POST-Body-Parameters übereinstimmen.

Um die Funktion zu aktivieren, legen Sie die `csrfToken` Parameter auf `true` während der Authentifizierung. Die Standardeinstellung 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 dies zutrifft, `GridCsrfToken` Cookie wird mit einem zufälligen Wert für Anmeldungen am Grid Manager gesetzt, und die `AccountCsrfToken` Für die Anmeldung beim Tenant Manager wird ein Cookie mit einem zufälligen Wert gesetzt.

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

- Der `X-Csrf-Token` Header, wobei der Wert des Headers auf den Wert des CSRF-Token-Cookies gesetzt ist.
- Für Endpunkte, die einen formkodierten Textkörper akzeptieren: A `csrfToken` formcodierter Anforderungstextparameter.

Um den CSRF-Schutz zu konfigurieren, verwenden Sie die "[Grid-Management-API](#)" oder "[Mandantenverwaltungs-API](#)".



Anfragen, für die ein CSRF-Token-Cookie gesetzt ist, erzwingen außerdem den Header „Content-Type: application/json“ für alle Anfragen, die einen JSON-Anforderungstext erwarten, als zusätzlichen Schutz vor CSRF-Angriffen.

Grid-Föderation-Verbindungen verwenden

Mandantengruppen und Benutzer klonen

Wenn ein Mandant erstellt oder bearbeitet wurde, um eine Grid-Föderation-Verbindung zu verwenden, wird dieser Mandant von einem StorageGRID -System (dem Quellmandanten) auf ein anderes StorageGRID System (dem Replikatmandanten) repliziert. Nachdem der Mandant repliziert wurde, werden alle dem Quellmandanten

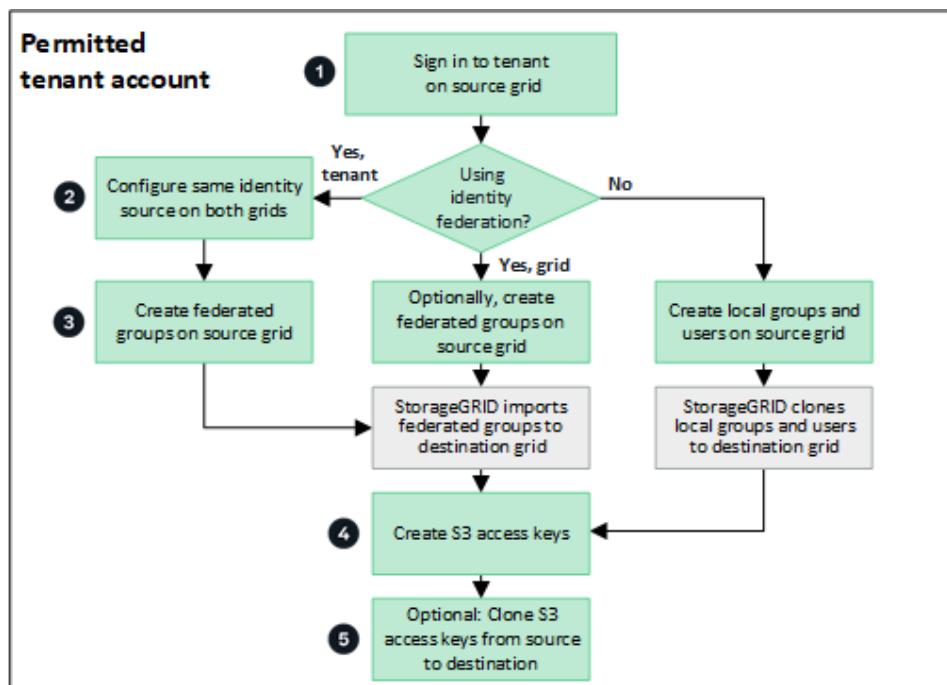
hinzugefügten Gruppen und Benutzer in den Replikatmandanten geklont.

Das StorageGRID -System, in dem der Mandant ursprünglich erstellt wurde, ist das **Quell-Grid** des Mandanten. Das StorageGRID -System, in dem der Mandant repliziert wird, ist das **Ziel-Grid** des Mandanten. Beide Mandantenkonten haben dieselbe Konto-ID, denselben Namen, dieselbe Beschreibung, dasselbe Speicherkontingent und dieselben zugewiesenen Berechtigungen, aber der Zielmandant hat zunächst kein Root-Benutzerkennwort. Weitere Einzelheiten finden Sie unter "[Was ist ein Kontoklon?](#)" Und "[Zulässige Mandanten verwalten](#)" .

Das Klonen von Mandantenkontoinformationen ist erforderlich für "[Cross-Grid-Replikation](#)" von Bucket-Objekten. Wenn Sie auf beiden Grids dieselben Mandantengruppen und Benutzer haben, können Sie auf beiden Grids auf die entsprechenden Buckets und Objekte zugreifen.

Mandanten-Workflow für Kontoklon

Wenn Ihr Mandantenkonto über die Berechtigung **Grid-Föderationsverbindung verwenden** verfügt, überprüfen Sie das Workflow-Diagramm, um die Schritte anzuzeigen, die Sie zum Klonen von Gruppen, Benutzern und S3-Zugriffsschlüsseln ausführen müssen.



Dies sind die wichtigsten Schritte im Workflow:

1

Beim Mandanten Sign in

Sign in (das Raster, in dem der Mandant ursprünglich erstellt wurde).

2

Optional: Konfigurieren Sie die Identitätsföderation

Wenn Ihr Mandantenkonto über die Berechtigung **Eigene Identitätsquelle verwenden** zur Verwendung föderierter Gruppen und Benutzer verfügt, konfigurieren Sie dieselbe Identitätsquelle (mit denselben Einstellungen) sowohl für das Quell- als auch das Zielmandantenkonto. Föderierte Gruppen und Benutzer können nicht geklont werden, es sei denn, beide Grids verwenden dieselbe Identitätsquelle. Anweisungen hierzu finden Sie unter "[Verwenden der Identitätsföderation](#)" .

3

Erstellen von Gruppen und Benutzern

Beginnen Sie beim Erstellen von Gruppen und Benutzern immer mit dem Quellraster des Mandanten. Wenn Sie eine neue Gruppe hinzufügen, klonen StorageGRID sie automatisch in das Zielraster.

- Wenn die Identitätsföderation für das gesamte StorageGRID -System oder für Ihr Mandantenkonto konfiguriert ist, ["Erstellen Sie neue Mandantengruppen"](#) durch Importieren föderierter Gruppen aus der Identitätsquelle.
- Wenn Sie keine Identitätsföderation verwenden, ["neue lokale Gruppen erstellen"](#) und dann ["lokale Benutzer erstellen"](#).

4

Erstellen von S3-Zugriffsschlüsseln

Du kannst ["Erstellen Sie Ihre eigenen Zugriffsschlüssel"](#) oder zu ["Erstellen Sie die Zugriffsschlüssel eines anderen Benutzers"](#) entweder auf dem Quell- oder dem Zielraster, um auf Buckets auf diesem Raster zuzugreifen.

5

Optional: S3-Zugriffsschlüssel klonen

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

Wie werden Gruppen, Benutzer und S3-Zugriffsschlüssel geklonnt?

Lesen Sie diesen Abschnitt, um zu verstehen, wie Gruppen, Benutzer und S3-Zugriffsschlüssel zwischen dem Mandantenquellraster und dem Mandantenzielraster geklonnt werden.

Lokale Gruppen, die im Quellraster erstellt wurden, werden geklont

Nachdem ein Mandantenkonto erstellt und in das Zielraster repliziert wurde, klonen StorageGRID automatisch alle lokalen Gruppen, die Sie zum Quellraster des Mandanten hinzufügen, in das Zielraster des Mandanten.

Sowohl die ursprüngliche Gruppe als auch ihr Klon haben denselben Zugriffsmodus, dieselben Gruppenberechtigungen und dieselbe S3-Gruppenrichtlinie. Anweisungen hierzu finden Sie unter ["Erstellen Sie Gruppen für den S3-Mandanten"](#).



Alle Benutzer, die Sie beim Erstellen einer lokalen Gruppe im Quellraster auswählen, werden nicht einbezogen, wenn die Gruppe in das Zielraster geklonnt wird. Wählen Sie aus diesem Grund beim Erstellen der Gruppe keine Benutzer aus. 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, klonen 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 ["Lokale Benutzer verwalten"](#).

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 "[Lokale Benutzer verwalten](#)".

Im Quellraster erstellte föderierte Gruppen werden geklont

Vorausgesetzt, die Voraussetzungen für die Verwendung des Kontoklonens mit "[Einmaliges Anmelden](#)" und "[Identitätsföderation](#)" erfüllt sind, werden föderierte Gruppen, die Sie für den Mandanten im Quellraster erstellen (importieren), automatisch auf den Mandanten im Zielraster geklont.

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

Nachdem Verbundgruppen für den Quellmandanten erstellt und auf den Zielmandanten geklont wurden, können sich Verbundbenutzer in beiden Rastern beim Mandanten anmelden.

S3-Zugriffsschlüssel können manuell geklont werden

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

Um Zugriffsschlüssel in den beiden Rastern zu verwalten, können Sie einen der folgenden Schritte ausführen:

- Wenn Sie nicht für jedes Raster die gleichen Schlüssel verwenden müssen, können Sie "[Erstellen Sie Ihre eigenen Zugriffsschlüssel](#)" oder "[Erstellen Sie die Zugriffsschlüssel eines anderen Benutzers](#)" auf jedem Raster.
- Wenn Sie die gleichen Schlüssel auf beiden Grids verwenden müssen, können Sie Schlüssel auf dem Quell-Grid erstellen und dann die Tenant Manager API verwenden, um manuell "[Klonen Sie die Schlüssel](#)" zum Zielraster.



Wenn Sie S3-Zugriffsschlüssel für einen Verbundbenutzer klonen, werden sowohl der Benutzer als auch die S3-Zugriffsschlüssel in den Zielmandanten geklont.

Zum Zielraster hinzugefügte Gruppen und Benutzer werden nicht geklont

Das Klonen erfolgt nur vom Quellraster des Mandanten zum Zielraster des Mandanten. Wenn Sie Gruppen und Benutzer im Zielraster des Mandanten erstellen oder importieren, klonnt StorageGRID diese Elemente nicht zurück in das Quellraster des Mandanten.

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 einem der Raster bearbeiten oder löschen, werden Ihre Änderungen nicht in das andere Raster geklont.

Klonen Sie S3-Zugriffsschlüssel mithilfe der API

Wenn Ihr Mandantenkonto über die Berechtigung **Grid-Föderationsverbindung verwenden** verfügt, können Sie die Mandantenverwaltungs-API verwenden, um S3-Zugriffsschlüssel vom Mandanten im Quell-Grid manuell auf den Mandanten im Ziel-Grid zu klonen.

Bevor Sie beginnen

- Das Mandantenkonto verfügt über die Berechtigung **Grid-Föderationsverbindung verwenden**.
- Die Grid-Föderation-Verbindung hat den **Verbindungsstatus Verbunden**.
- Sie sind beim Mandantenmanager im Quellraster des Mandanten angemeldet mit einem "[unterstützter Webbrowser](#)".
- Sie gehören einer Benutzergruppe an, die über die "[Verwalten Sie Ihre eigenen S3-Anmeldeinformationen 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 Verbundbenutzer klonen, werden sowohl der Benutzer als auch die S3-Zugriffsschlüssel dem Zielmandanten hinzugefügt.

Klonen Sie Ihre eigenen Zugriffsschlüssel

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

Schritte

1. Verwenden Sie den Mandantenmanager im Quellraster. "[Erstellen Sie Ihre eigenen Zugriffsschlüssel](#)" und laden Sie die .csv Datei.
2. Wählen Sie oben im Mandanten-Manager das Hilfesymbol und dann **API-Dokumentation** aus.
3. Wählen Sie im Abschnitt **s3** den folgenden Endpunkt aus:

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

POST [/org/users/current-user/replicate-s3-access-key](#) Clone the current user's S3 key to the other grids.

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

Achten Sie darauf, die doppelten Anführungszeichen um jede Zeichenfolge beizubehalten.

6. Wenn der Schlüssel abläuft, ersetzen Sie den Beispieleintrag für **expires** durch das Ablaufdatum und die Ablaufzeit als Zeichenfolge im ISO 8601-Daten-/Zeitformat (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 vorangestellte Komma).
7. Wählen Sie **Ausführen**.

8. Bestätigen Sie, dass der Serverantwortcode **204** lautet, was darauf hinweist, dass der Schlüssel erfolgreich in das Zielraster geklont wurde.

Klonen Sie die Zugriffsschlüssel eines anderen Benutzers

Sie können die Zugriffsschlüssel eines anderen Benutzers klonen, wenn dieser auf beiden Grids auf dieselben Buckets zugreifen muss.

Schritte

1. Verwenden Sie den Mandantenmanager im Quellraster. ["Erstellen Sie die S3-Zugriffsschlüssel des anderen Benutzers"](#) und laden Sie die `.csv` Datei.
2. Wählen Sie oben im Mandanten-Manager das Hilfesymbol und dann **API-Dokumentation** aus.
3. Besorgen Sie sich die Benutzer-ID. Sie benötigen diesen Wert, um die Zugriffsschlüssel des anderen Benutzers zu klonen.
 - a. Wählen Sie im Abschnitt **Benutzer** den folgenden Endpunkt aus:

```
GET /org/users
```

- b. Wählen Sie **Ausprobieren**.
- c. Geben Sie alle Parameter an, die Sie beim Suchen von Benutzern verwenden möchten.
- 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
```

POST

[/org/users/{userId}/replicate-s3-access-key](#) Clone an S3 key to the other grids. 

5. Wählen Sie **Ausprobieren**.
6. Fügen Sie in das Textfeld **userId** die kopierte Benutzer-ID ein.
7. Ersetzen Sie im Textfeld **Body** die Beispieleinträge für **Beispielzugriffsschlüssel** und **Geheimer Zugriffsschlüssel** durch die Werte aus der `.csv`-Datei für diesen Benutzer.

Achten Sie darauf, die doppelten Anführungszeichen um die Zeichenfolge beizubehalten.

8. Wenn der Schlüssel abläuft, ersetzen Sie den Beispieleintrag für **expires** durch das Ablaufdatum und die Ablaufzeit als Zeichenfolge im ISO 8601-Daten-/Zeitformat (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 vorangestellte Komma).

9. Wählen Sie **Ausführen**.

10. Bestätigen Sie, dass der Serverantwortcode **204** lautet, was darauf hinweist, dass der Schlüssel erfolgreich in das Zielraster geklont wurde.

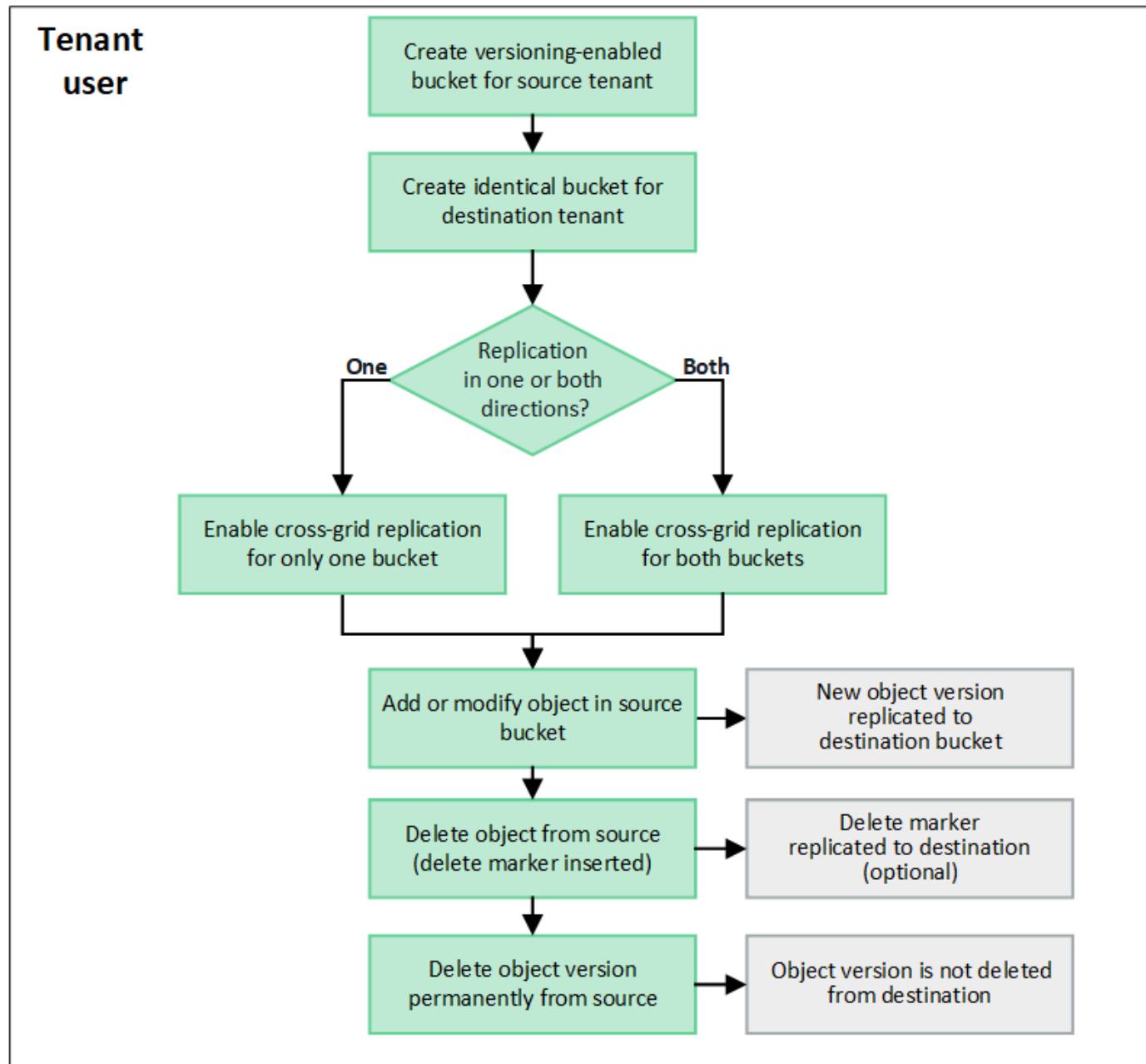
Verwalten der Cross-Grid-Replikation

Wenn Ihrem Mandantenkonto bei der Erstellung die Berechtigung **Grid-Föderationsverbindung verwenden** zugewiesen wurde, können Sie mithilfe der Cross-

Grid-Replikation Objekte automatisch zwischen Buckets im Quell-Grid des Mandanten und Buckets im Ziel-Grid des Mandanten replizieren. Die Cross-Grid-Replikation kann in eine oder beide Richtungen erfolgen.

Workflow für die Cross-Grid-Replikation

Das Workflow-Diagramm fasst die Schritte zusammen, die Sie zum Konfigurieren der Cross-Grid-Replikation zwischen Buckets auf zwei Grids ausführen. Diese Schritte werden im Folgenden genauer beschrieben.



Konfigurieren der Cross-Grid-Replikation

Bevor Sie die Cross-Grid-Replikation verwenden können, müssen Sie sich bei den entsprechenden Mandantenkonten auf jedem Grid anmelden und identische 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. Sehen "[Was ist Cross-Grid-Replikation?](#)" .
- Sie verwenden eine "[unterstützter Webbrowser](#)" .
- Das Mandantenkonto verfügt über die Berechtigung **Grid-Föderationsverbindung verwenden** und auf beiden Grids sind identische Mandantenkonten vorhanden. Sehen "[Verwalten Sie die zulässigen Mandanten für die Grid-Föderation-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 identische Eimer

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

Schritte

1. Erstellen Sie ausgehend von einem der Grids in der Grid-Föderationsverbindung einen neuen Bucket:
 - a. Sign in beim Mandantenkonto 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, um "[Erstellen Sie einen S3-Bucket](#)" .
 - c. Wählen Sie auf der Registerkarte **Objekteinstellungen verwalten** die Option **Objektversionierung aktivieren**.
 - d. Wenn S3 Object Lock für Ihr StorageGRID System aktiviert ist, aktivieren Sie S3 Object Lock nicht für den Bucket.
 - e. Wählen Sie **Bucket erstellen**.
 - f. Wählen Sie **Fertig**.
2. Wiederholen Sie diese Schritte, um einen identischen Bucket für dasselbe Mandantenkonto im anderen Grid in der Grid-Föderationsverbindung zu erstellen.



Je nach Bedarf kann jeder Bucket eine andere Region verwenden.

Aktivieren Sie die Cross-Grid-Replikation

Sie müssen diese Schritte ausführen, bevor Sie einem der Buckets Objekte hinzufügen.

Schritte

1. Ausgehend von einem Raster, dessen Objekte Sie replizieren möchten, aktivieren Sie "[Cross-Grid-Replikation in eine Richtung](#)" :
 - a. Sign in .
 - b. Wählen Sie im Dashboard **Buckets anzeigen** oder wählen Sie **STORAGE (S3) > Buckets**.

- c. Wählen Sie den Bucket-Namen aus der Tabelle aus, um auf die Bucket-Detailseite zuzugreifen.
- d. Wählen Sie die Registerkarte **Cross-Grid-Replikation**.
- e. Wählen Sie **Aktivieren** und überprüfen Sie die Liste der Anforderungen.
- f. Wenn alle Voraussetzungen erfüllt sind, wählen Sie die Grid-Föderation-Verbindung aus, die Sie verwenden möchten.
- g. Ändern Sie optional die Einstellung von **Löschmarkierungen replizieren**, um festzulegen, was im Zielraster geschieht, wenn ein S3-Client eine Löschanforderung an das Quellraster sendet, die keine Versions-ID enthält:
 - **Ja** (Standard): Dem Quell-Bucket wird eine Löschmarkierung 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.

Sehen "[Was ist Cross-Grid-Replikation?](#)" für Details.

- a. Ändern Sie optional die Einstellung der Auditkategorie **Gridübergreifende Replikation**, um das Volumen der Auditmeldungen zu verwalten:
 - **Fehler** (Standard): Nur fehlgeschlagene Cross-Grid-Replikationsanforderungen werden in die Prüfausgabe aufgenommen.
 - **Normal**: Alle Cross-Grid-Replikationsanforderungen werden einbezogen, wodurch das Volumen der Audit-Ausgabe erheblich erhöht wird.
- b. Überprüfen Sie Ihre Auswahl. Sie können diese Einstellungen nur ändern, wenn beide Buckets leer sind.
- c. Wählen Sie **Aktivieren und testen**.

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. Optional können Sie zum entsprechenden Eimer auf dem anderen Raster gehen und "[ermöglichen Cross-Grid-Replikation in beide Richtungen](#)".

Testen Sie die Replikation zwischen Grids

Wenn die Cross-Grid-Replikation für einen Bucket aktiviert ist, müssen Sie möglicherweise überprüfen, ob die Verbindung und die Cross-Grid-Replikation ordnungsgemäß funktionieren und ob die Quell- und Ziel-Buckets noch alle Anforderungen erfüllen (z. B. ist die Versionierung noch aktiviert).

Bevor Sie beginnen

- Sie verwenden eine "[unterstützter Webbrower](#)".
- Sie gehören einer Benutzergruppe an, die über die "[Root-Zugriffsberechtigung](#)".

Schritte

1. Sign in .
2. Wählen Sie im Dashboard **Buckets anzeigen** oder wählen Sie **STORAGE (S3) > Buckets**.
3. Wählen Sie den Bucket-Namen aus der Tabelle aus, um auf die Bucket-Detailseite zuzugreifen.
4. Wählen Sie die Registerkarte **Cross-Grid-Replikation**.
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 Informationen finden Sie unter "["Beheben von Grid-Föderationsfehlern"](#)" .

6. Wenn die Cross-Grid-Replikation so konfiguriert ist, dass sie in beide Richtungen erfolgt, gehen Sie zum entsprechenden Bucket im anderen Grid und wählen Sie **Verbindung testen** aus, um zu überprüfen, ob die Cross-Grid-Replikation in die andere Richtung funktioniert.

Deaktivieren der Cross-Grid-Replikation

Sie können die Cross-Grid-Replikation dauerhaft stoppen, wenn Sie keine Objekte mehr in das andere Grid kopieren möchten.

Beachten Sie Folgendes, bevor Sie die Cross-Grid-Replikation deaktivieren:

- 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 Cross-Grid-Replikation für jeden Bucket aktiviert wurde (d. h., wenn die Replikation in beide Richtungen erfolgt), können Sie die Cross-Grid-Replikation für einen oder beide Buckets deaktivieren. Beispielsweise möchten Sie möglicherweise die Replikation von Objekten deaktivieren von `my-bucket` auf Raster 1 bis `my-bucket` auf Grid 2, während weiterhin Objekte aus `my-bucket` auf Grid 2 zu `my-bucket` auf Raster 1.
- Sie müssen die Cross-Grid-Replikation deaktivieren, bevor Sie einem Mandanten die Berechtigung zur Verwendung der Grid-Föderationsverbindung entziehen können. Sehen "["Zulässige Mandanten verwalten"](#)" .
- 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.



Sie können die Replikation erst wieder aktivieren, wenn beide Buckets leer sind.

Bevor Sie beginnen

- Sie verwenden eine "["unterstützter Webbrowser"](#)" .
- Sie gehören einer Benutzergruppe an, die über die "["Root-Zugriffsberechtigung"](#)" .

Schritte

1. Beginnen Sie mit dem Grid, dessen Objekte Sie nicht mehr replizieren möchten, und beenden Sie die Grid-übergreifende Replikation für den Bucket:
 - a. Sign in .
 - b. Wählen Sie im Dashboard **Buckets anzeigen** oder wählen Sie **STORAGE (S3) > Buckets**.
 - c. Wählen Sie den Bucket-Namen aus der Tabelle aus, um auf die Bucket-Detailseite zuzugreifen.

d. Wählen Sie die Registerkarte **Cross-Grid-Replikation**.

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

2. Wenn die Cross-Grid-Replikation so konfiguriert wurde, dass sie in beide Richtungen erfolgt, gehen Sie zum entsprechenden Bucket auf dem anderen Grid und stoppen Sie die Cross-Grid-Replikation in die andere Richtung.

Grid-Föderation-Verbindungen anzeigen

Wenn Ihr Mandantenkonto über die Berechtigung **Grid-Föderationsverbindung verwenden** verfügt, können Sie die zulässigen Verbindungen anzeigen.

Bevor Sie beginnen

- Das Mandantenkonto verfügt über die Berechtigung **Grid-Föderationsverbindung verwenden**.
- Sie sind beim Tenant Manager angemeldet mit einem "[unterstützter Webbrowser](#)".
- Sie gehören einer Benutzergruppe an, die über die "[Root-Zugriffsberechtigung](#)".

Schritte

1. Wählen Sie **STORAGE (S3) > Grid-Föderationsverbindungen**.

Die Seite „Grid-Föderationsverbindung“ wird angezeigt und enthält eine Tabelle mit einer Zusammenfassung der folgenden Informationen:

Spalte	Beschreibung
Verbindungsname	Die Grid-Föderation-Verbindungen, für deren Verwendung dieser Mandant berechtigt ist.
Buckets mit Cross-Grid-Replikation	Für jede Grid-Föderationsverbindung die Mandanten-Buckets, für die die Cross-Grid-Replikation aktiviert ist. Zu diesen Buckets hinzugefügte Objekte werden in das andere Raster in der Verbindung repliziert.
Letzter Fehler	Für jede Grid-Föderationsverbindung der letzte Fehler, der ggf. beim Replizieren der Daten in das andere Grid aufgetreten ist. Sehen Löschen Sie den letzten Fehler .

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

Löschen Sie den letzten Fehler

In der Spalte **Letzter Fehler** kann aus einem der folgenden Gründe ein Fehler angezeigt werden:

- Die Quellobjektversion wurde nicht gefunden.

- Der Quell-Bucket wurde nicht gefunden.
- Der Ziel-Bucket wurde gelöscht.
- Der Ziel-Bucket wurde von einem anderen Konto neu erstellt.
- Die Versionsverwaltung des Ziel-Buckets ist ausgesetzt.
- Der Ziel-Bucket wurde vom selben Konto neu erstellt, ist jetzt aber nicht mehr versioniert.



In dieser Spalte wird nur der letzte aufgetretene Cross-Grid-Replikationsfehler angezeigt. Eventuell zuvor aufgetretene Fehler werden nicht angezeigt.

Schritte

- Wenn in der Spalte **Letzter Fehler** eine Meldung angezeigt wird, sehen Sie sich den Nachrichtentext an.

Dieser Fehler weist beispielsweise darauf hin, dass sich der Ziel-Bucket für die Cross-Grid-Replikation in einem ungültigen Zustand befand, möglicherweise weil die Versionierung ausgesetzt oder die S3-Objektsperre aktiviert war.

The screenshot shows a table titled 'Grid federation connections' with the following data:

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

- Führen Sie alle empfohlenen Aktionen aus. Wenn beispielsweise die Versionierung für den Ziel-Bucket für die Cross-Grid-Replikation ausgesetzt wurde, aktivieren Sie die Versionierung für diesen Bucket erneut.
- Wählen Sie die Verbindung aus der Tabelle aus.
- Wählen Sie **Fehler löschen**.
- Wählen Sie **Ja**, um die Nachricht zu löschen und den Systemstatus zu aktualisieren.
- Warten Sie 5–6 Minuten und nehmen Sie dann einen neuen Gegenstand in den Eimer. Vergewissern Sie sich, dass die Fehlermeldung nicht erneut angezeigt wird.



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

- Um festzustellen, ob Objekte aufgrund des Bucket-Fehlers nicht repliziert werden konnten, siehe "[Identifizieren und wiederholen Sie fehlgeschlagene Replikationsvorgänge](#)".

Verwalten von Gruppen und Benutzern

Verwenden der Identitätsföderation

Durch die Verwendung der Identitätsföderation lässt sich das Einrichten von

Mandantengruppen und Benutzern beschleunigen und Mandantenbenutzer können sich mit vertrauten Anmeldeinformationen beim Mandantenkonto anmelden.

Konfigurieren der Identitätsföderation für den Mandantenmanager

Sie können die Identitätsföderation für den Mandantenmanager konfigurieren, wenn Sie Mandantengruppen und Benutzer in einem anderen System wie Active Directory, Azure Active Directory (Azure AD), OpenLDAP oder Oracle Directory Server verwalten möchten.

Bevor Sie beginnen

- Sie sind beim Tenant Manager angemeldet mit einem "[unterstützter Webbrowser](#)" .
- Sie gehören einer Benutzergruppe an, die über die "[Root-Zugriffsberechtigung](#)" .
- Sie verwenden Active Directory, Azure AD, 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. Sehen [Richtlinien zum Konfigurieren des OpenLDAP-Servers](#) .
- Wenn Sie Transport Layer Security (TLS) für die Kommunikation mit dem LDAP-Server verwenden möchten, muss der Identitätsanbieter TLS 1.2 oder 1.3 verwenden. Sehen ["Unterstützte Verschlüsselungen für ausgehende TLS-Verbindungen"](#) .

Informationen zu diesem Vorgang

Ob Sie einen Identitätsföderationsdienst für Ihren Mandanten konfigurieren können, hängt davon ab, wie Ihr Mandantenkonto eingerichtet wurde. Ihr Mandant nutzt möglicherweise den für den Grid Manager konfigurierten Identitätsföderationsdienst gemeinsam. Wenn diese Meldung beim Zugriff auf die Seite „Identitätsföderation“ angezeigt wird, können Sie für diesen Mandanten keine separate föderierte Identitätsquelle konfigurieren.



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

Konfiguration eingeben

Wenn Sie die Identifizierungsföderation 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-Diensttyp“ den Typ des LDAP-Dienstes aus, den Sie konfigurieren möchten.

LDAP service type

Select the type of LDAP service you want to configure.

Active Directory

Azure

OpenLDAP

Other

Wählen Sie **Andere** 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 ein `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 ein `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 ein `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 ein `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-Diensttypen die erforderlichen LDAP-Server- und Netzwerkverbindungsinformationen im Abschnitt „LDAP-Server konfigurieren“ ein.

- **Hostname:** Der vollqualifizierte Domänenname (FQDN) oder die IP-Adresse des LDAP-Servers.
- **Port:** Der Port, der für die Verbindung mit dem LDAP-Server verwendet wird.



Der Standardport für STARTTLS ist 389 und der Standardport für LDAPS ist 636. Sie können jedoch jeden Port verwenden, solange Ihre Firewall richtig 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 Down-Level-Anmeldenamen oder den Benutzerprinzipalnamen angeben.

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
- **Azurblau:** accountEnabled Und userPrincipalName
- **Passwort:** Das mit dem Benutzernamen verknüpfte Passwort.



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

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



Die Werte für den **eindeutigen Gruppennamen** müssen innerhalb des **Gruppen-Basis-DN**, zu dem sie gehören, eindeutig sein.

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



Die Werte für den **Eindeutigen Benutzernamen** müssen innerhalb des **Benutzerbasis-DN**, zu dem sie gehören, eindeutig sein.

- **Bind-Benutzernamenformat** (optional): Das Standardbenutzernamenmuster, das StorageGRID verwenden soll, wenn das Muster nicht automatisch ermittelt werden kann.

Es wird empfohlen, das **Bind-Benutzernamenformat** anzugeben, da dies Benutzern die Anmeldung ermöglichen kann, wenn StorageGRID keine Bindung mit dem Dienstkonto herstellen kann.

Geben Sie eines dieser Muster ein:

- **UserPrincipalName-Muster (Active Directory und Azure):** [USERNAME]@example.com
- **Downlevel-Anmeldenamenmuster (Active Directory und Azure):** example\ [USERNAME]
- **Muster für eindeutige Namen:** CN=[USERNAME], CN=Users, DC=example, DC=com

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

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

- **STARTTLS 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 Azure nicht unterstützt.
- **LDAPS verwenden:** Die Option LDAPS (LDAP über SSL) verwendet TLS, um eine Verbindung zum LDAP-Server herzustellen. Sie müssen diese Option für Azure auswählen.
- **TLS nicht verwenden:** Der Netzwerkverkehr zwischen dem StorageGRID -System und dem LDAP-Server wird nicht gesichert. Diese Option wird für Azure 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, das zum Sichern der Verbindung verwendet wird.

- **CA-Zertifikat des Betriebssystems verwenden:** Verwenden Sie das standardmäßig auf dem Betriebssystem installierte 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 und fügen Sie es in das Textfeld „CA-Zertifikat“ 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-Benutzernamenformat, falls Sie eines angegeben haben.

Schritte

1. Wählen Sie **Verbindung testen**.
2. Wenn Sie kein Bind-Benutzernamenformat angegeben haben:
 - Bei gültigen Verbindungseinstellungen wird die Meldung „Verbindungstest erfolgreich“ angezeigt. Wählen Sie **Speichern**, um die Konfiguration zu speichern.
 - Bei ungültigen Verbindungseinstellungen erscheint die Meldung „Testverbindung konnte nicht hergestellt werden“. Wählen Sie **Schließen**. Beheben Sie dann alle Probleme und testen Sie die Verbindung erneut.
3. Wenn Sie ein Bind-Benutzernamenformat angegeben haben, geben Sie den Benutzernamen und das Kennwort eines gültigen Verbundbenutzers ein.

Geben Sie beispielsweise Ihren eigenen Benutzernamen und Ihr eigenes Passwort ein. Verwenden Sie im Benutzernamen keine Sonderzeichen wie @ oder /.

Test Connection

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

Test username

The username of a federated user.

Test password

Cancel

Test Connection

- Bei gültigen Verbindungseinstellungen wird die Meldung „Verbindungstest erfolgreich“ angezeigt. Wählen Sie **Speichern**, um die Konfiguration zu speichern.
- Wenn die Verbindungseinstellungen, das Bind-Benutzernamenformat oder der Testbenutzername und das Testkennwort ungültig sind, wird eine Fehlermeldung angezeigt. Beheben Sie alle Probleme und testen Sie die Verbindung erneut.

Synchronisierung mit Identitätsquelle erzwingen

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

Schritte

1. Gehen Sie zur Seite „Identitätsföderation“.
2. Wählen Sie oben auf der Seite **Sync-Server** aus.

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



Die Warnung **Fehler bei der Synchronisierung der Identitätsföderation** wird ausgelöst, wenn beim Synchronisieren föderierter Gruppen und Benutzer aus der Identitätsquelle ein Problem auftritt.

Identitätsföderation deaktivieren

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.

Informationen zu diesem Vorgang

Bevor Sie die Identitätsföderation deaktivieren, sollten Sie Folgendes beachten:

- Verbundbenutzer können sich nicht anmelden.
- Verbundbenutzer, die derzeit angemeldet sind, behalten den Zugriff auf das StorageGRID -System, bis ihre Sitzung abläuft, können sich nach Ablauf ihrer Sitzung jedoch nicht mehr 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 Single Sign-On (SSO) auf **Aktiviert** oder **Sandbox-Modus** eingestellt ist. Der SSO-Status auf der Single Sign-On-Seite muss **Deaktiviert** sein, bevor Sie die Identitätsföderation deaktivieren können. Sehen "["Deaktivieren der einmaligen Anmeldung"](#)" .

Schritte

1. Gehen Sie zur Seite „Identitätsföderation“.
2. Deaktivieren Sie das Kontrollkästchen **Identitätsföderation aktivieren**.

Richtlinien zum Konfigurieren des OpenLDAP-Servers

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



Bei Identitätsquellen, die nicht ActiveDirectory oder Azure sind, blockiert StorageGRID den S3-Zugriff 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.

Memberof- und Refint-Overlays

Die Memberof- und Refint-Overlays sollten aktiviert sein. Weitere Informationen finden Sie in den Anweisungen zur umgekehrten Pflege von Gruppenmitgliedschaften [imhttp://www.openldap.org/doc/admin24/index.html](http://www.openldap.org/doc/admin24/index.html)["OpenLDAP-Dokumentation: Administratorhandbuch Version 2.4"] .

Indizierung

Sie müssen die folgenden OpenLDAP-Attribute mit den angegebenen Indexschlüsselwörtern 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.

Informationen zur umgekehrten Pflege von Gruppenmitgliedschaften finden Sie [imhttp://www.openldap.org/doc/admin24/index.html](http://www.openldap.org/doc/admin24/index.html)["OpenLDAP-Dokumentation: Administratorhandbuch Version 2.4"] .

Verwalten von Mandantengruppen

Erstellen von Gruppen für einen S3-Mandanten

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

Bevor Sie beginnen

- Sie sind beim Tenant Manager angemeldet mit einem "[unterstützter Webbrowser](#)" .
- Sie gehören einer Benutzergruppe an, die über die "[Root-Zugriffsberechtigung](#)" .
- Wenn Sie eine föderierte Gruppe importieren möchten, müssen Sie "[konfigurierte Identitätsföderation](#)" , und die föderierte Gruppe ist bereits in der konfigurierten Identitätsquelle vorhanden.
- Wenn Ihr Mandantenkonto über die Berechtigung **Grid-Föderationsverbindung verwenden** verfügt, haben Sie den Workflow und die Überlegungen für "[Klonen von Mandantengruppen und Benutzern](#)" , und Sie sind beim Quellraster des Mandanten angemeldet.

Greifen Sie auf den Assistenten „Gruppe erstellen“ zu

Rufen Sie als ersten Schritt den Assistenten „Gruppe erstellen“ auf.

Schritte

1. Wählen Sie **ZUGRIFFSVERWALTUNG > Gruppen**.
2. Wenn Ihr Mandantenkonto über die Berechtigung **Grid-Föderationsverbindung verwenden** verfügt, bestätigen Sie, dass ein blaues Banner angezeigt wird, das darauf hinweist, dass neue Gruppen, die in diesem Grid erstellt werden, in denselben Mandanten im anderen Grid in der Verbindung geklont werden. Wenn dieses Banner nicht angezeigt wird, sind Sie möglicherweise beim Zielraster des Mandanten angemeldet.

Groups

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

0 groups

Create group

Actions

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

3. Wählen Sie **Gruppe erstellen**.

Wählen Sie einen Gruppentyp

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

Schritte

1. Wählen Sie die Registerkarte **Lokale Gruppe**, um eine lokale Gruppe zu erstellen, oder wählen Sie die Registerkarte **Verbundgruppe**, 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 Tenant Manager anmelden, obwohl sie Clientanwendungen verwenden können, um die Ressourcen des Mandanten basierend auf Gruppenberechtigungen zu verwalten.

2. Geben Sie den Namen der Gruppe ein.

- **Lokale Gruppe:** Geben Sie sowohl einen Anzeigenamen als auch einen eindeutigen Namen ein. Sie können den Anzeigenamen später bearbeiten.



Wenn Ihr Mandantenkonto über die Berechtigung **Grid-Föderationsverbindung verwenden** verfügt, tritt ein Klonfehler auf, wenn dieselbe **eindeutige Name** für den Mandanten im Zielgrid bereits vorhanden ist.

- **Föderierte Gruppe:** Geben Sie den eindeutigen Namen ein. Für Active Directory ist der eindeutige Name der Name, der mit dem `sAMAccountName` Attribut. Bei OpenLDAP ist der eindeutige Name der Name, der mit dem `uid` Attribut.

3. Wählen Sie **Weiter**.

Gruppenberechtigungen verwalten

Gruppenberechtigungen steuern, welche Aufgaben Benutzer im Tenant Manager und in der Tenant Management API ausführen können.

Schritte

1. Wählen Sie für **Zugriffsmodus** eine der folgenden Optionen aus:
 - **Lesen/Schreiben** (Standard): Benutzer können sich beim Tenant Manager anmelden und die Tenant Konfiguration verwalten.
 - **Schreibgeschützt**: Benutzer können Einstellungen und Funktionen nur anzeigen. Sie können im Tenant Manager oder in der Tenant Management API keine Änderungen vornehmen oder Vorgänge ausführen. Lokale Benutzer mit Leseberechtigung können ihre eigenen Passwörter ändern.



Wenn ein Benutzer mehreren Gruppen angehört und für eine der Gruppen der Lesezugriff aktiviert ist, hat der Benutzer nur Lesezugriff auf alle ausgewählten Einstellungen und Funktionen.

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

Sehen ["Berechtigungen zur Mandantenverwaltung"](#).

3. Wählen Sie **Weiter**.

S3-Gruppenrichtlinie festlegen

Die Gruppenrichtlinie bestimmt, welche S3-Zugriffsberechtigungen Benutzer haben.

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 mit einer Bucket-Richtlinie gewährt. Wenn Sie diese Option auswählen, hat standardmäßig nur der Root-Benutzer Zugriff auf S3-Ressourcen.
Nur-Lese-Zugriff	Benutzer in dieser Gruppe haben schreibgeschützten Zugriff auf S3-Ressourcen. Beispielsweise können Benutzer dieser Gruppe Objekte auflisten und Objektdaten, Metadaten und Tags lesen. Wenn Sie diese Option auswählen, wird die JSON-Zeichenfolge für eine schreibgeschützte Gruppenrichtlinie im Textfeld angezeigt. Sie können diese Zeichenfolge nicht bearbeiten.
Vollzugriff	Benutzer in dieser Gruppe haben vollen Zugriff auf S3-Ressourcen, einschließlich Buckets. Wenn Sie diese Option auswählen, wird die JSON-Zeichenfolge für eine Gruppenrichtlinie mit vollem Zugriff im Textfeld angezeigt. Sie können diese Zeichenfolge nicht bearbeiten.

Gruppenrichtlinie	Beschreibung
Ransomware-Minderung	<p>Diese Beispielrichtlinie gilt für alle Buckets dieses Mandanten. Benutzer in dieser Gruppe können allgemeine Aktionen ausführen, aber keine Objekte dauerhaft aus Buckets löschen, für die die Objektversionierung aktiviert ist.</p> <p>Tenant Manager-Benutzer mit der Berechtigung Alle Buckets verwalten können diese Gruppenrichtlinie außer Kraft setzen. Beschränken Sie die Berechtigung „Alle Buckets verwalten“ auf vertrauenswürdige Benutzer und verwenden Sie, sofern verfügbar, die Multi-Faktor-Authentifizierung (MFA).</p>
Brauch	<p>Den Benutzern in der Gruppe werden die Berechtigungen erteilt, die Sie im Textfeld angeben.</p>

2. Wenn Sie **Benutzerdefiniert** ausgewählt haben, geben Sie die Gruppenrichtlinie ein. Jede Gruppenrichtlinie hat eine Größenbeschränkung von 5.120 Byte. Sie müssen eine gültige Zeichenfolge im JSON-Format eingeben.

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

3. Wenn Sie eine lokale Gruppe erstellen, wählen Sie **Weiter**. Wenn Sie eine föderierte Gruppe erstellen, wählen Sie **Gruppe erstellen** und **Fertig**.

Benutzer hinzufügen (nur lokale Gruppen)

Sie können die Gruppe speichern, ohne Benutzer hinzuzufügen, oder Sie können optional bereits vorhandene lokale Benutzer hinzufügen.

 Wenn Ihr Mandantenkonto über die Berechtigung **Grid-Föderationsverbindung verwenden** verfügt, werden alle Benutzer, die Sie beim Erstellen einer lokalen Gruppe im Quell-Grid auswählen, nicht einbezogen, wenn die Gruppe in das Ziel-Grid geklont wird. Wählen Sie aus diesem Grund beim Erstellen der Gruppe keine Benutzer aus. 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**.

Die von Ihnen erstellte Gruppe wird in der Gruppenliste angezeigt.

Wenn Ihr Mandantenkonto über die Berechtigung **Grid-Föderationsverbindung verwenden** verfügt und Sie sich im Quell-Grid des Mandanten befinden, wird die neue Gruppe in das Ziel-Grid des Mandanten geklont. **Erfolg** wird als **Klonstatus** im Abschnitt „Übersicht“ der Detailseite der Gruppe angezeigt.

Erstellen Sie Gruppen für einen Swift-Mandanten

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

muss über die Berechtigung „Swift-Administrator“ verfügen, die zum Verwalten der Container und Objekte für ein Swift-Mandantenkonto erforderlich ist.



Die Unterstützung für Swift-Clientanwendungen ist veraltet und wird in einer zukünftigen Version entfernt.

Bevor Sie beginnen

- Sie sind beim Tenant Manager angemeldet mit einem "[unterstützter Webbrower](#)".
- Sie gehören einer Benutzergruppe an, die über die "[Root-Zugriffsberechtigung](#)".
- Wenn Sie eine föderierte Gruppe importieren möchten, müssen Sie "[konfigurierte Identitätsföderation](#)", und die föderierte Gruppe ist bereits in der konfigurierten Identitätsquelle vorhanden.

Greifen Sie auf den Assistenten „Gruppe erstellen“ zu

Schritte

Rufen Sie als ersten Schritt den Assistenten „Gruppe erstellen“ auf.

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

Wählen Sie einen Gruppentyp

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

Schritte

1. Wählen Sie die Registerkarte **Lokale Gruppe**, um eine lokale Gruppe zu erstellen, oder wählen Sie die Registerkarte **Verbundgruppe**, 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 Tenant Manager anmelden, obwohl sie Clientanwendungen verwenden können, um die Ressourcen des Mandanten basierend auf Gruppenberechtigungen zu verwalten.

2. Geben Sie den Namen der Gruppe ein.
 - **Lokale Gruppe:** Geben Sie sowohl einen Anzeigenamen als auch einen eindeutigen Namen ein. Sie können den Anzeigenamen später bearbeiten.
 - **Föderierte Gruppe:** Geben Sie den eindeutigen Namen ein. Für Active Directory ist der eindeutige Name der Name, der mit dem `sAMAccountName` Attribut. Bei OpenLDAP ist der eindeutige Name der Name, der mit dem `uid` Attribut.
3. Wählen Sie **Weiter**.

Gruppenberechtigungen verwalten

Gruppenberechtigungen steuern, welche Aufgaben Benutzer im Tenant Manager und in der Tenant Management API ausführen können.

Schritte

1. Wählen Sie für **Zugriffsmodus** eine der folgenden Optionen aus:

- **Lesen/Schreiben** (Standard): Benutzer können sich beim Tenant Manager anmelden und die Tenant Konfiguration verwalten.
- **Schreibgeschützt**: Benutzer können Einstellungen und Funktionen nur anzeigen. Sie können im Tenant Manager oder in der Tenant Management API keine Änderungen vornehmen oder Vorgänge ausführen. Lokale Benutzer mit Leseberechtigung können ihre eigenen Passwörter ändern.



Wenn ein Benutzer mehreren Gruppen angehört und für eine der Gruppen der Lesezugriff aktiviert ist, hat der Benutzer nur Lesezugriff auf alle ausgewählten Einstellungen und Funktionen.

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

Swift-Gruppenrichtlinie festlegen

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

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

Benutzer hinzufügen (nur lokale Gruppen)

Sie können die Gruppe speichern, ohne Benutzer hinzuzufügen, oder Sie können optional bereits vorhandene lokale Benutzer hinzufügen.

Schritte

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

Wenn Sie noch keine lokalen Benutzer erstellt haben, können Sie diese Gruppe auf der Seite „Benutzer“ zum Benutzer hinzufügen. Sehen ["Lokale Benutzer verwalten"](#).

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

Die von Ihnen erstellte Gruppe wird in der Gruppenliste angezeigt.

Berechtigungen zur Mandantenverwaltung

Überlegen Sie vor dem Erstellen einer Mandantengruppe, welche Berechtigungen Sie dieser Gruppe zuweisen möchten. Die Berechtigungen zur Mandantenverwaltung legen fest, welche Aufgaben Benutzer mit dem Mandantenmanager oder der Mandantenverwaltungs-API ausführen können. Ein Benutzer kann einer oder mehreren Gruppen angehören. Berechtigungen sind kumulativ, wenn ein Benutzer mehreren Gruppen angehört.

Um sich beim Tenant Manager anzumelden oder die Tenant Management API zu verwenden, müssen Benutzer einer Gruppe angehören, die über mindestens eine Berechtigung verfügt. Alle Benutzer, die sich anmelden können, können die folgenden Aufgaben ausführen:

- Dashboard anzeigen
- Das eigene Passwort ändern (für lokale Benutzer)

Bei allen Berechtigungen bestimmt die Einstellung „Zugriffsmodus“ der Gruppe, ob Benutzer Einstellungen ändern und Vorgänge ausführen können oder ob sie die zugehörigen Einstellungen und Funktionen nur anzeigen können.



Wenn ein Benutzer mehreren Gruppen angehört und für eine der Gruppen der Lesezugriff aktiviert ist, hat der Benutzer nur Lesezugriff auf alle ausgewählten Einstellungen und Funktionen.

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

Erlaubnis	Beschreibung	Details
Root-Zugriff	Bietet vollständigen Zugriff auf den Tenant Manager und die Tenant Management API.	Swift-Benutzer müssen über Root-Zugriffsberechtigungen verfügen, um sich beim Mandantenkonto anmelden zu können.
Administrator	Nur Swift-Mieter. Bietet vollständigen Zugriff auf die Swift-Container und -Objekte für dieses Mandantenkonto	Swift-Benutzer müssen über die Berechtigung „Swift-Administrator“ verfügen, um Vorgänge mit der Swift-REST-API ausführen zu können.
Verwalten Sie Ihre eigenen S3-Anmeldeinformationen	Ermöglicht Benutzern das Erstellen und Entfernen eigener S3-Zugriffsschlüssel.	Benutzer ohne diese Berechtigung sehen die Menüoption STORAGE (S3) > Meine S3-Zugriffsschlüssel nicht.
Alle Eimer anzeigen	<p>S3-Mandanten: Ermöglicht Benutzern, alle Buckets und Bucket-Konfigurationen anzuzeigen.</p> <p>Swift-Mandanten: Ermöglicht Swift-Benutzern, alle Container und Containerkonfigurationen mithilfe der Tenant Management API anzuzeigen.</p>	<p>Benutzer, die weder über die Berechtigung „Alle Buckets anzeigen“ noch über die Berechtigung „Alle Buckets verwalten“ verfügen, können die Menüoption Buckets nicht sehen.</p> <p>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.</p> <p>Sie können diese Berechtigung nur Swift-Gruppen über die Tenant Management API zuweisen. Sie können diese Berechtigung nicht mithilfe des Mandanten-Managers Swift-Gruppen zuweisen.</p>

Erlaubnis	Beschreibung	Details
Alle Buckets verwalten	<p>S3-Mandanten: Ermöglicht Benutzern die Verwendung des Mandantenmanagers und der Mandantenverwaltungs-API zum Erstellen und Löschen von S3-Buckets und zum Verwalten der Einstellungen für alle S3-Buckets im Mandantenkonto, unabhängig von S3-Bucket- oder Gruppenrichtlinien.</p> <p>Swift-Mandanten: Ermöglicht Swift-Benutzern, die Konsistenz für Swift-Container mithilfe der Tenant Management API zu steuern.</p>	<p>Benutzer, die weder über die Berechtigung „Alle Buckets anzeigen“ noch über die Berechtigung „Alle Buckets verwalten“ verfügen, können die Menüoption Buckets nicht sehen.</p> <p>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.</p> <p>Sie können diese Berechtigung nur Swift-Gruppen über die Tenant Management API zuweisen. Sie können diese Berechtigung nicht mithilfe des Mandanten-Managers Swift-Gruppen zuweisen.</p>
Verwalten von Endpunkten	Ermöglicht Benutzern die Verwendung des Tenant Managers oder der Tenant Management API zum Erstellen oder Bearbeiten von Plattformdienst-Endpunkten, die als Ziel für StorageGRID -Plattformdienste verwendet werden.	Benutzern ohne diese Berechtigung wird die Menüoption Plattformdienst-Endpunkte nicht angezeigt.
Registerkarte „S3-Konsole verwenden“	In Kombination mit der Berechtigung „Alle Buckets anzeigen“ oder „Alle Buckets verwalten“ können Benutzer Objekte über die Registerkarte „S3-Konsole“ auf der Detailseite für einen Bucket anzeigen und verwalten.	

Verwalten von Gruppen

Verwalten Sie Ihre Mandantengruppen nach Bedarf, um eine Gruppe anzuzeigen, zu bearbeiten oder zu duplizieren und mehr.

Bevor Sie beginnen

- Sie sind beim Tenant Manager angemeldet mit einem "[unterstützter Webbrowser](#)".
- Sie gehören einer Benutzergruppe an, die über die "[Root-Zugriffsberechtigung](#)".

Gruppe anzeigen oder bearbeiten

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

Schritte

- Wählen Sie **ZUGRIFFSVERWALTUNG > Gruppen**.
- Überprüfen Sie die Informationen auf der Seite „Gruppen“, auf der grundlegende Informationen zu allen lokalen und föderierten Gruppen für dieses Mandantenkonto aufgeführt sind.

Wenn das Mandantenkonto über die Berechtigung **Grid-Föderationsverbindung verwenden** verfügt und Sie Gruppen im Quell-Grid des Mandanten anzeigen:

- Eine Bannermeldung weist darauf hin, dass Ihre Änderungen nicht mit dem anderen Raster synchronisiert werden, wenn Sie eine Gruppe bearbeiten oder entfernen.
- Bei Bedarf zeigt eine Bannermeldung an, ob Gruppen nicht auf den Mandanten im Zielraster geklont wurden. Du kannst [Erneuter Versuch eines Gruppenklangs](#) das ist fehlgeschlagen.

3. Wenn Sie den Namen der Gruppe ändern möchten:

- Aktivieren Sie das Kontrollkästchen für die Gruppe.
- Wählen Sie **Aktionen > Gruppennamen bearbeiten**.
- Geben Sie den neuen Namen ein.
- Wählen Sie **Änderungen speichern**.

4. Wenn Sie weitere Details anzeigen oder zusätzliche 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 **Aktionen > Gruppendetails anzeigen**.

5. Sehen Sie sich den Abschnitt „Übersicht“ an, der für jede Gruppe die folgenden Informationen enthält:

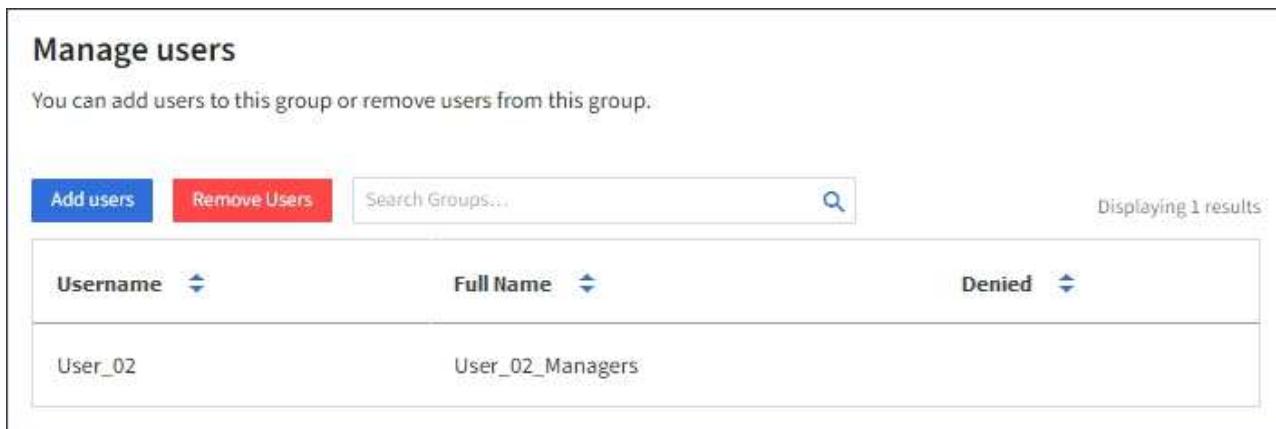
- Anzeigename
- Eindeutiger Name
- Typ
- Zugriffsmodus
- Berechtigungen
- S3-Richtlinie
- Anzahl der Benutzer in dieser Gruppe
- Zusätzliche Felder, wenn das Mandantenkonto über die Berechtigung **Grid-Föderationsverbindung verwenden** verfügt und Sie die Gruppe im Quell-Grid des Mandanten anzeigen:
 - Klonstatus, entweder **Erfolg** oder **Fehler**
 - Ein blaues Banner zeigt an, dass Ihre Änderungen nicht mit dem anderen Raster synchronisiert werden, wenn Sie diese Gruppe bearbeiten oder löschen.

6. Bearbeiten Sie die Gruppeneinstellungen nach Bedarf. Sehen ["Erstellen von Gruppen für einen S3-Mandanten"](#) Und ["Erstellen Sie Gruppen für einen Swift-Mandanten"](#) für Details zu den einzugebenden Informationen.

- Ändern Sie im Abschnitt „Übersicht“ den Anzeigennamen, indem Sie den Namen oder das Bearbeitungssymbol auswählen .
- Aktualisieren Sie auf der Registerkarte **Gruppenberechtigungen** die Berechtigungen und wählen Sie **Änderungen speichern**.
- Nehmen Sie auf der Registerkarte **Gruppenrichtlinie** die gewünschten Änderungen vor und wählen Sie **Änderungen speichern**.
 - Wenn Sie eine S3-Gruppe bearbeiten, wählen Sie optional eine andere S3-Gruppenrichtlinie aus oder geben Sie bei Bedarf die JSON-Zeichenfolge für eine benutzerdefinierte Richtlinie ein.
 - Wenn Sie eine Swift-Gruppe bearbeiten, aktivieren oder deaktivieren Sie optional das Kontrollkästchen **Swift-Administrator**.

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

- Wählen Sie die Registerkarte „Benutzer“ aus.



The screenshot shows a 'Manage users' interface. At the top, there are buttons for 'Add users' (blue) and 'Remove Users' (red), a search bar with placeholder 'Search Groups...', and a search icon. To the right, it says 'Displaying 1 results'. Below this is a table with three columns: 'Username', 'Full Name', and 'Denied'. The data row shows 'User_02' in the 'Username' column and 'User_02_Managers' in the 'Full Name' column. The 'Denied' column shows a downward arrow. The table has a header row with sorting arrows and a footer row with a single data entry.

- Wählen Sie **Benutzer hinzufügen**.

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

Oben rechts erscheint eine Erfolgsmeldung.

8. So entfernen Sie lokale Benutzer aus der Gruppe:

- Wählen Sie die Registerkarte „Benutzer“ aus.
- Wählen Sie **Benutzer entfernen**.
- Wählen Sie die Benutzer aus, die Sie entfernen möchten, und wählen Sie **Benutzer entfernen**.

Oben rechts erscheint eine Erfolgsmeldung.

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

Gruppe duplizieren

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



Wenn Ihr Mandantenkonto über die Berechtigung **Grid-Föderationsverbindung verwenden** verfügt und Sie eine Gruppe aus dem Quell-Grid des Mandanten duplizieren, wird die duplizierte Gruppe in das Ziel-Grid des Mandanten geklont.

Schritte

- Wählen Sie **ZUGRIFFSVERWALTUNG > Gruppen**.
- Aktivieren Sie das Kontrollkästchen für die Gruppe, die Sie duplizieren möchten.
- Wählen Sie **Aktionen > Gruppe duplizieren**.
- Sehen "[Erstellen von Gruppen für einen S3-Mandanten](#)" oder "[Erstellen Sie Gruppen für einen Swift-Mandanten](#)" für Details zu den einzugebenden Informationen.
- Wählen Sie **Gruppe erstellen**.

Gruppenklon erneut versuchen

So wiederholen Sie einen fehlgeschlagenen Klonvorgang:

1. Wählen Sie jede Gruppe aus, bei der unter dem Gruppennamen (*Klonen fehlgeschlagen*) angezeigt wird.
2. Wählen Sie **Aktionen > Gruppen klonen**.
3. Zeigen Sie den Status des Klonvorgangs auf der Detailseite jeder Gruppe an, die Sie klonen.

Weitere Informationen finden Sie unter "[Mandantengruppen und Benutzer klonen](#)" .

Löschen einer oder mehrerer Gruppen

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



Wenn Ihr Mandantenkonto über die Berechtigung **Grid-Föderationsverbindung verwenden** verfügt und Sie eine Gruppe löschen, löscht StorageGRID die entsprechende Gruppe im anderen Grid nicht. 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**.

Lokale Benutzer verwalten

Sie können lokale Benutzer erstellen und sie lokalen Gruppen zuweisen, um festzulegen, auf welche Funktionen diese Benutzer zugreifen können. Der Tenant Manager umfasst einen vordefinierten lokalen Benutzer namens „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 Tenant Management API anmelden, obwohl sie basierend auf Gruppenberechtigungen Clientanwendungen verwenden können, um auf die Ressourcen des Mandanten zuzugreifen.

Bevor Sie beginnen

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

Erstellen Sie einen lokalen Benutzer

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

Auf S3-Benutzer, die keiner Gruppe angehören, werden keine Verwaltungsberechtigungen oder S3-Gruppenrichtlinien angewendet. Diesen Benutzern wird möglicherweise über eine Bucket-Richtlinie Zugriff auf den S3-Bucket gewährt.

Swift-Benutzer, die keiner Gruppe angehören, verfügen weder über Verwaltungsberechtigungen noch über Zugriff auf Swift-Container.

Greifen Sie auf den Assistenten „Benutzer erstellen“ zu

Schritte

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

Wenn Ihr Mandantenkonto über die Berechtigung **Grid-Föderationsverbindung verwenden** verfügt, zeigt ein blaues Banner an, dass dies das Quell-Grid des Mandanten ist. Alle lokalen Benutzer, die Sie in diesem Raster erstellen, werden in das andere Raster in der Verbindung geklont.

2. Wählen Sie **Benutzer erstellen**.

Anmeldeinformationen eingeben

Schritte

1. Füllen Sie für den Schritt **Benutzeranmeldeinformationen eingeben** die folgenden Felder aus.

Feld	Beschreibung
Vollständiger Name	Der vollständige Name dieses Benutzers, beispielsweise der Vor- und Nachname einer Person oder der Name einer Anwendung.
Benutzername	Der Name, den dieser Benutzer zum Anmelden verwendet. Benutzernamen müssen eindeutig sein und können nicht geändert werden. Hinweis: Wenn Ihr Mandantenkonto über die Berechtigung Grid-Föderationsverbindung verwenden verfügt, tritt ein Klonfehler auf, wenn derselbe Benutzername für den Mandanten im Zielgrid bereits vorhanden ist.
Passwort und Passwort bestätigen	Das Kennwort, das der Benutzer zunächst bei der Anmeldung verwendet.
Zugriff verweigern	Wählen Sie Ja aus, um zu verhindern, dass sich dieser Benutzer beim Mandantenkonto anmeldet, auch wenn er möglicherweise noch einer oder mehreren Gruppen angehört. Wählen Sie beispielsweise Ja aus, um die Anmeldemöglichkeit eines Benutzers vorübergehend zu sperren.

2. Wählen Sie **Weiter**.

Zu Gruppen zuweisen

Schritte

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

Die Zuweisung eines Benutzers zu Gruppen ist optional. Wenn Sie möchten, können Sie beim Erstellen oder Bearbeiten von Gruppen Benutzer auswählen.

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

2. Wählen Sie **Benutzer erstellen**.

Wenn Ihr Mandantenkonto über die Berechtigung **Grid-Föderationsverbindung verwenden** verfügt und Sie sich im Quell-Grid des Mandanten befinden, wird der neue lokale Benutzer in das Ziel-Grid des Mandanten geklont. **Erfolg** wird als **Klonstatus** im Abschnitt „Übersicht“ der Detailseite des Benutzers angezeigt.

3. Wählen Sie **Fertig**, um zur Seite „Benutzer“ 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 zu allen lokalen und föderierten Benutzern für dieses Mandantenkonto aufgeführt sind.

Wenn das Mandantenkonto über die Berechtigung **Grid-Föderationsverbindung verwenden** verfügt und Sie den Benutzer im Quell-Grid des Mandanten anzeigen:

- Eine Bannermeldung weist darauf hin, dass Ihre Änderungen nicht mit dem anderen Raster synchronisiert werden, wenn Sie einen Benutzer bearbeiten oder entfernen.
- Bei Bedarf zeigt eine Bannermeldung an, ob Benutzer nicht in den Mandanten im Zielraster geklont wurden. Sie können [Wiederholen Sie den Versuch, einen fehlgeschlagenen Benutzerklon auszuführen](#)

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 zusätzliche 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. Sehen Sie sich den Abschnitt „Übersicht“ an, in dem für jeden Benutzer die folgenden Informationen angezeigt werden:

- Vollständiger Name
- Benutzername
- Benutzertyp
- Zugriff verweigert
- Zugriffsmodus
- Gruppenmitgliedschaft
- Zusätzliche Felder, wenn das Mandantenkonto über die Berechtigung **Grid-Föderationsverbindung verwenden** verfügt und Sie den Benutzer im Quell-Grid des Mandanten anzeigen:
 - Klonstatus, entweder **Erfolg** oder **Fehler**
 - Ein blaues Banner zeigt an, dass Ihre Änderungen nicht mit dem anderen Raster synchronisiert werden, wenn Sie diesen Benutzer bearbeiten.

6. Bearbeiten Sie die Benutzereinstellungen nach Bedarf. Sehen[Lokalen Benutzer erstellen](#) für Details zu den einzugebenden Informationen.

a. Ändern Sie im Abschnitt „Übersicht“ den vollständigen Namen, indem Sie den Namen oder das Bearbeitungssymbol 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 **Zugriff Nein** aus, um dem Benutzer die Anmeldung zu erlauben, oder wählen Sie **Ja** aus, um die Anmeldung des Benutzers zu verhindern. Wählen Sie dann **Änderungen speichern** aus.

d. Wählen Sie auf der Registerkarte **Zugriffsschlüssel** die Option **Schlüssel erstellen** und folgen Sie den Anweisungen für "Erstellen der S3-Zugriffsschlüssel eines anderen Benutzers".

e. Wählen Sie auf der Registerkarte **Gruppen** die Option **Gruppen bearbeiten** aus, um den Benutzer zu Gruppen hinzuzufügen oder aus Gruppen zu entfernen. Wählen Sie dann **Änderungen speichern**.

7. Bestätigen Sie, dass Sie für jeden geänderten Abschnitt die Option **Änderungen speichern** ausgewählt haben.

Duplizieren Sie den lokalen Benutzer

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



Wenn Ihr Mandantenkonto über die Berechtigung **Grid-Föderationsverbindung verwenden** verfügt und Sie einen Benutzer aus dem Quell-Grid des Mandanten duplizieren, wird der duplizierte Benutzer in das Ziel-Grid 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. Sehen[Lokalen Benutzer erstellen](#) für Details zu den einzugebenden Informationen.
5. Wählen Sie **Benutzer erstellen**.

Benutzerklon erneut versuchen

So wiederholen Sie einen fehlgeschlagenen Klonvorgang:

1. Wählen Sie jeden Benutzer aus, bei dem unter dem Benutzernamen (*Klonen fehlgeschlagen*) angezeigt wird.
2. Wählen Sie **Aktionen > Benutzer klonen**.
3. Zeigen Sie den Status des Klonvorgangs auf der Detailseite jedes Benutzers an, den Sie klonen.

Weitere Informationen finden Sie unter "[Mandantengruppen und Benutzer klonen](#)".

Löschen eines oder mehrerer lokaler Benutzer

Sie können einen oder mehrere lokale Benutzer dauerhaft löschen, die keinen Zugriff mehr auf das StorageGRID Mandantenkonto benötigen.

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

 Sie müssen die Verbundidentitätsquelle verwenden, um Verbundbenutzer 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**.

S3-Zugriffsschlüssel verwalten

S3-Zugriffsschlüssel verwalten

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 verwaltet werden:

- Benutzer mit der Berechtigung **Eigene S3-Anmeldeinformationen verwalten** 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 dem Mandanten vollständigen Zugriff auf alle Buckets und Objekte, sofern dies nicht ausdrücklich durch eine Bucket-Richtlinie deaktiviert wird.

StorageGRID unterstützt die Authentifizierung mit Signature Version 2 und Signature Version 4. Der kontoübergreifende Zugriff ist nicht zulässig, es sei denn, er wird ausdrücklich durch eine Bucket-Richtlinie aktiviert.

Erstellen Sie Ihre eigenen S3-Zugriffsschlüssel

Wenn Sie einen S3-Mandanten verwenden und über die entsprechende Berechtigung verfügen, können Sie Ihre eigenen S3-Zugriffsschlüssel erstellen. Sie benötigen einen Zugriffsschlüssel, um auf Ihre Buckets und Objekte zugreifen zu können.

Bevor Sie beginnen

- Sie sind beim Tenant Manager angemeldet mit einem "[unterstützter Webbrowser](#)" .
- Sie gehören einer Benutzergruppe an, die über die "[Verwalten Sie Ihre eigenen S3-Anmeldeinformationen oder Root-Zugriffsberechtigungen](#)" .

Informationen zu diesem Vorgang

Sie können einen oder mehrere S3-Zugriffsschlüssel erstellen, 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 Ihrem geheimen Zugriffsschlüssel. Erstellen Sie aus Sicherheitsgründen nicht mehr Schlüssel als nötig und löschen Sie die Schlüssel, die Sie nicht verwenden. Wenn Sie nur einen Schlüssel haben und dieser bald abläuft, erstellen Sie einen neuen Schlüssel, bevor der alte abläuft, und löschen Sie dann den alten.

Jeder Schlüssel kann eine bestimmte Ablaufzeit haben oder nicht ablaufen. Befolgen Sie diese Richtlinien für die Ablaufzeit:

- Legen Sie eine Ablaufzeit für Ihre Schlüssel fest, um Ihren Zugriff auf einen bestimmten Zeitraum zu beschränken. Durch das Festlegen einer kurzen Ablaufzeit können Sie Ihr Risiko verringern, wenn Ihre Zugriffsschlüssel-ID und Ihr geheimer Zugriffsschlüssel versehentlich offengelegt werden. Abgelaufene Schlüssel werden automatisch entfernt.
- Wenn das Sicherheitsrisiko in Ihrer Umgebung gering ist und Sie nicht regelmäßig neue Schlüssel erstellen müssen, müssen Sie für Ihre Schlüssel keine Ablaufzeit festlegen. Wenn Sie sich später entscheiden, neue Schlüssel zu erstellen, löschen Sie die alten Schlüssel manuell.

 Auf die zu Ihrem Konto gehörenden S3-Buckets und -Objekte kann mithilfe der Zugriffsschlüssel-ID und des geheimen Zugriffsschlüssels zugegriffen werden, die für Ihr Konto im Tenant Manager angezeigt werden. Schützen Sie daher Zugriffsschlüssel wie ein Passwort. Wechseln Sie die Zugriffsschlüssel regelmäßig, entfernen Sie alle nicht verwendeten Schlüssel aus Ihrem Konto und geben Sie sie niemals an andere Benutzer weiter.

Schritte

1. Wählen Sie **SPEICHER (S3) > Meine Zugriffsschlüssel**.

Die Seite „Meine Zugriffsschlüssel“ wird angezeigt und listet alle vorhandenen Zugriffsschlüssel auf.

2. Wählen Sie **Schlüssel erstellen**.

3. Führen Sie einen der folgenden Schritte aus:

- Wählen Sie **Keine Ablaufzeit festlegen**, um einen Schlüssel zu erstellen, der nicht abläuft. (Standard)
- Wählen Sie **Ablaufzeit festlegen** und legen Sie das Ablaufdatum und die Ablaufzeit fest.



Das Ablaufdatum kann maximal fünf Jahre ab dem aktuellen Datum liegen. Die Ablaufzeit kann mindestens eine Minute nach der aktuellen Zeit liegen.

4. Wählen Sie **Zugriffsschlüssel erstellen**.

Das Dialogfeld „Zugriffsschlüssel herunterladen“ wird angezeigt und listet Ihre Zugriffsschlüssel-ID und Ihren geheimen Zugriffsschlüssel auf.

5. Kopieren Sie die Zugriffsschlüssel-ID und den geheimen Zugriffsschlüssel 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 nicht, bis Sie diese Informationen kopiert oder heruntergeladen haben. Sie können keine Schlüssel kopieren oder herunterladen, nachdem das Dialogfeld geschlossen wurde.

6. Wählen Sie **Fertig**.

Der neue Schlüssel wird auf der Seite „Meine Zugriffsschlüssel“ aufgeführt.

7. Wenn Ihr Mandantenkonto über die Berechtigung **Grid-Föderationsverbindung verwenden** verfügt, können Sie optional die Mandantenverwaltungs-API verwenden, um S3-Zugriffsschlüssel vom Mandanten im Quell-Grid manuell auf den Mandanten im Ziel-Grid zu klonen. Sehen ["Klonen Sie S3-Zugriffsschlüssel mithilfe der API"](#).

Zeigen Sie Ihre S3-Zugriffsschlüssel an

Wenn Sie einen S3-Tenant verwenden und über die ["entsprechende Erlaubnis"](#) können Sie eine Liste Ihrer S3-Zugriffsschlüssel anzeigen. Sie können die Liste nach Ablaufzeit sortieren, um festzustellen, welche Schlüssel bald ablaufen. Bei Bedarf können Sie ["neue Schlüssel erstellen"](#) oder ["Schlüssel löschen"](#) die Sie nicht mehr verwenden.



Auf die zu Ihrem Konto gehörenden S3-Buckets und -Objekte kann mithilfe der Zugriffsschlüssel-ID und des geheimen Zugriffsschlüssels zugegriffen werden, die für Ihr Konto im Tenant Manager angezeigt werden. Schützen Sie daher Zugriffsschlüssel wie ein Passwort. Wechseln Sie die Zugriffsschlüssel regelmäßig, entfernen Sie alle nicht verwendeten Schlüssel aus Ihrem Konto und geben Sie sie niemals an andere Benutzer weiter.

Bevor Sie beginnen

- Sie sind beim Tenant Manager angemeldet mit einem ["unterstützter Webbrowser"](#).
- Sie gehören zu einer Benutzergruppe, die über die Berechtigung „S3-Anmeldeinformationen selbst verwalten“ verfügt. ["Erlaubnis"](#).

Schritte

1. Wählen Sie **SPEICHER (S3) > Meine Zugriffsschlüssel**.
2. Sortieren Sie auf der Seite „Meine Zugriffsschlüssel“ alle vorhandenen Zugriffsschlüssel nach **Ablaufzeit** oder **Zugriffsschlüssel-ID**.
3. Erstellen Sie bei 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 die neuen Schlüssel verwenden, ohne vorübergehend den Zugriff auf die Objekte im Konto zu verlieren.

Abgelaufene Schlüssel werden automatisch entfernt.

Löschen Sie Ihre eigenen S3-Zugriffsschlüssel

Wenn Sie einen S3-Mandanten verwenden und über die entsprechende Berechtigung verfügen, können Sie Ihre eigenen S3-Zugriffsschlüssel löschen. Nachdem ein Zugriffsschlüssel gelöscht wurde, kann er nicht mehr für den Zugriff auf die Objekte und Buckets im Mandantenkonto verwendet werden.

Bevor Sie beginnen

- Sie sind beim Tenant Manager angemeldet mit einem "[unterstützter Webbrowser](#)" .
- Sie haben die "[Verwalten Sie Ihre eigenen S3-Anmeldeinformationen](#)" .

 Auf die zu Ihrem Konto gehörenden S3-Buckets und -Objekte kann mithilfe der Zugriffsschlüssel-ID und des geheimen Zugriffsschlüssels zugegriffen werden, die für Ihr Konto im Tenant Manager angezeigt werden. Schützen Sie daher Zugriffsschlüssel wie ein Passwort. Wechseln Sie die Zugriffsschlüssel regelmäßig, entfernen Sie alle nicht verwendeten Schlüssel aus Ihrem Konto und geben Sie sie niemals an andere Benutzer weiter.

Schritte

1. Wählen Sie **SPEICHER (S3) > Meine Zugriffsschlüssel**.
2. Aktivieren Sie auf der Seite „Meine Zugriffsschlüssel“ das Kontrollkästchen für jeden Zugriffsschlüssel, den Sie entfernen möchten.
3. Wählen Sie **Löschtaste**.
4. Wählen Sie im Bestätigungsdialogfeld **Schlüssel löschen** aus.

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

Erstellen Sie die S3-Zugriffsschlüssel eines anderen Benutzers

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

Bevor Sie beginnen

- Sie sind beim Tenant Manager angemeldet mit einem "[unterstützter Webbrowser](#)" .
- Sie gehören einer Benutzergruppe an, die über die "[Root-Zugriffsberechtigung](#)" .

Informationen zu diesem Vorgang

Sie können einen oder mehrere S3-Zugriffsschlüssel für andere Benutzer erstellen, damit diese 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 dieser bald abläuft, erstellen Sie einen neuen Schlüssel, bevor der alte abläuft, und löschen Sie dann den alten.

Jeder Schlüssel kann eine bestimmte Ablaufzeit haben oder nicht ablaufen. Befolgen Sie diese Richtlinien für die Ablaufzeit:

- Legen Sie eine Ablaufzeit für die Schlüssel fest, um den Zugriff des Benutzers auf einen bestimmten Zeitraum zu beschränken. Durch Festlegen einer kurzen Ablaufzeit können Sie das Risiko verringern,

wenn die Zugriffsschlüssel-ID und der geheime Zugriffsschlüssel versehentlich offengelegt werden. Abgelaufene Schlüssel werden automatisch entfernt.

- Wenn das Sicherheitsrisiko in Ihrer Umgebung gering ist und Sie nicht regelmäßig neue Schlüssel erstellen müssen, müssen Sie für die Schlüssel keine Ablaufzeit festlegen. Wenn Sie sich später entscheiden, neue Schlüssel zu erstellen, löschen Sie die alten Schlüssel manuell.

 Auf die S3-Buckets und -Objekte eines Benutzers kann mithilfe der Zugriffsschlüssel-ID und des geheimen Zugriffsschlüssels zugegriffen werden, die für diesen Benutzer im Tenant Manager angezeigt werden. Schützen Sie daher Zugriffsschlüssel wie ein Passwort. Wechseln Sie die Zugriffsschlüssel regelmäßig, entfernen Sie alle nicht verwendeten Schlüssel aus dem Konto und geben Sie sie niemals an andere Benutzer weiter.

Schritte

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

Die Benutzerdetailseite wird angezeigt.

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



Das Ablaufdatum kann maximal fünf Jahre ab dem aktuellen Datum liegen. Die Ablaufzeit kann mindestens eine Minute nach der aktuellen Zeit liegen.

5. Wählen Sie **Zugriffsschlüssel erstellen**.

Das Dialogfeld „Zugriffsschlüssel herunterladen“ wird angezeigt und listet die Zugriffsschlüssel-ID und den geheimen Zugriffsschlüssel auf.

6. Kopieren Sie die Zugriffsschlüssel-ID und den geheimen Zugriffsschlüssel 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 nicht, bis 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 Benutzerdetailseite aufgeführt.

8. Wenn Ihr Mandantenkonto über die Berechtigung **Grid-Föderationsverbindung verwenden** verfügt, können Sie optional die Mandantenverwaltungs-API verwenden, um S3-Zugriffsschlüssel vom Mandanten im Quell-Grid manuell auf den Mandanten im Ziel-Grid zu klonen. Sehen ["Klonen Sie S3-Zugriffsschlüssel mithilfe der API"](#).

Anzeigen der S3-Zugriffsschlüssel eines anderen Benutzers

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 Ablaufzeit sortieren, um festzustellen, welche Schlüssel bald ablaufen. Bei Bedarf können Sie neue Schlüssel erstellen und nicht mehr verwendete Schlüssel löschen.

Bevor Sie beginnen

- Sie sind beim Tenant Manager angemeldet mit einem "[unterstützter Webbrower](#)" .
- Sie haben die "[Root-Zugriffsberechtigung](#)" .

 Auf die S3-Buckets und -Objekte eines Benutzers kann mithilfe der Zugriffsschlüssel-ID und des geheimen Zugriffsschlüssels zugegriffen werden, die für diesen Benutzer im Tenant Manager angezeigt werden. Schützen Sie daher Zugriffsschlüssel wie ein Passwort. Wechseln Sie die Zugriffsschlüssel regelmäßig, entfernen Sie alle nicht verwendeten Schlüssel aus dem Konto und geben Sie sie niemals an andere Benutzer weiter.

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 „Benutzerdetails“ **Zugriffsschlüssel** aus.
4. Sortieren Sie die Schlüssel nach **Ablaufzeit** oder **Zugriffsschlüssel-ID**.
5. Erstellen Sie bei Bedarf neue Schlüssel und löschen Sie nicht mehr verwendete Schlüssel manuell.

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

Abgelaufene Schlüssel werden automatisch entfernt.

Ähnliche Informationen

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

Löschen Sie die S3-Zugriffsschlüssel eines anderen Benutzers

Wenn Sie einen S3-Mandanten verwenden und über die entsprechenden Berechtigungen verfügen, können Sie die S3-Zugriffsschlüssel eines anderen Benutzers löschen. Nachdem ein Zugriffsschlüssel gelöscht wurde, kann er nicht mehr für den Zugriff auf die Objekte und Buckets im Mandantenkonto verwendet werden.

Bevor Sie beginnen

- Sie sind beim Tenant Manager angemeldet mit einem "[unterstützter Webbrower](#)" .
- Sie haben die "[Root-Zugriffsberechtigung](#)" .



Auf die S3-Buckets und -Objekte eines Benutzers kann mithilfe der Zugriffsschlüssel-ID und des geheimen Zugriffsschlüssels zugegriffen werden, die für diesen Benutzer im Tenant Manager angezeigt werden. Schützen Sie daher Zugriffsschlüssel wie ein Passwort. Wechseln Sie die Zugriffsschlüssel regelmäßig, entfernen Sie alle nicht verwendeten Schlüssel aus dem Konto und geben Sie sie niemals an andere Benutzer weiter.

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 „Benutzerdetails“ **Zugriffsschlüssel** aus und aktivieren Sie dann das Kontrollkästchen für jeden Zugriffsschlüssel, den Sie löschen möchten.
4. Wählen Sie **Aktionen > Ausgewählten Schlüssel löschen**.
5. Wählen Sie im Bestätigungsdialogfeld **Schlüssel löschen** aus.

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

S3-Buckets verwalten

Erstellen eines S3-Buckets

Mit dem Tenant Manager können Sie S3-Buckets für Objektdaten erstellen.

Bevor Sie beginnen

- Sie sind beim Tenant Manager angemeldet mit einem "[unterstützter Webbrowser](#)" .
- Sie gehören zu einer Benutzergruppe, die über Root-Zugriff oder die Möglichkeit verfügt, alle Buckets zu verwalten. "[Erlaubnis](#)" . 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 S3 Object Lock für einen Bucket aktivieren möchten, hat ein Grid-Administrator die globale S3 Object Lock-Einstellung für das StorageGRID System aktiviert und Sie haben die Anforderungen für S3 Object Lock-Buckets und -Objekte überprüft.
- Wenn jeder Mandant über 5.000 Buckets verfügt, verfügt jeder Speicherknoten im Grid über mindestens 64 GB RAM.



Jedes Raster kann maximal 100.000 Buckets enthalten.

Zugriff auf den Assistenten

Schritte

1. Wählen Sie im Dashboard **Buckets anzeigen** oder wählen Sie **STORAGE (S3) > Buckets**.
2. Wählen Sie **Bucket erstellen**.

Details eingeben

Schritte

1. Geben Sie Details zum Bucket ein.

Feld	Beschreibung
Bucket-Name	<p>Ein Name für den Bucket, der diesen Regeln entspricht:</p> <ul style="list-style-type: none">• Muss in jedem StorageGRID -System eindeutig sein (nicht nur innerhalb des Mandantenkontos).• Muss DNS-kompatibel sein.• Muss mindestens 3 und darf nicht mehr als 63 Zeichen enthalten.• Jedes Etikett muss mit einem Kleinbuchstaben oder einer Zahl beginnen und enden und darf nur Kleinbuchstaben, Zahlen und Bindestriche enthalten.• Darf in Anfragen im virtuell gehosteten Stil keine Punkte enthalten. Punkte verursachen Probleme bei der Überprüfung des Platzhalterzertifikats des Servers. <p>Weitere Informationen finden Sie im "Amazon Web Services (AWS)-Dokumentation zu Bucket-Benennungsregeln".</p> <p>Hinweis: Sie können den Bucket-Namen nach dem Erstellen des Buckets nicht mehr ändern.</p>
Region	<p>Die Region des Buckets.</p> <p>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 <code>us-east-1</code> Region.</p> <p>Hinweis: Sie können die Region nach dem Erstellen des Buckets nicht mehr ändern.</p>

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 bei Bedarf frühere Versionen eines Objekts abrufen. Sie müssen die Objektversionierung aktivieren, wenn der Bucket für die gitterübergreifende Replikation verwendet wird.

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

Aktivieren Sie die S3-Objektsperre für einen 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 diesem Bucket Objekte hinzufügen, die nicht geändert werden können. Möglicherweise können Sie diese Objekte oder den Bucket selbst nicht löschen.

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

3. Wenn Sie **S3-Objektsperre aktivieren** ausgewählt haben, aktivieren Sie optional **Standardaufbewahrung** für diesen 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 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 Bucket an.

Standardaufbewahrungsmodus	Beschreibung
Führung	<ul style="list-style-type: none">• Benutzer mit der s3:BypassGovernanceRetention Berechtigung kann die x-amz-bypass-governance-retention: true Anforderungsheader zum Umgehen der Aufbewahrungseinstellungen.• Diese Benutzer können eine Objektversion löschen, bevor ihr Aufbewahrungsdatum erreicht ist.• Diese Benutzer können das Aufbewahrungsdatum eines Objekts erhöhen, verringern oder entfernen.
Einhaltung	<ul style="list-style-type: none">• Das Objekt kann erst gelöscht werden, wenn sein 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. <p>Hinweis: Ihr Grid-Administrator muss Ihnen die Verwendung des Compliance-Modus gestatten.</p>

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

Die **Standardaufbewahrungsfrist** gibt an, wie lange neue Objekte, die diesem 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 Aufbewahrungsduer für den

Mandanten ist.

Eine *maximale* Aufbewahrungsduer, die zwischen 1 Tag und 100 Jahren liegen kann, wird festgelegt, wenn der Grid-Administrator den Mandanten erstellt. Wenn Sie eine *Standard*-Aufbewahrungsduer festlegen, darf diese den für die maximale Aufbewahrungsduer festgelegten Wert nicht überschreiten. Bitten Sie Ihren Grid-Administrator bei Bedarf, die maximale Aufbewahrungsduer zu verlängern oder zu verkürzen.

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

Die Kapazitätsgrenze ist die maximal verfügbare Kapazität für die Objekte dieses Buckets. Dieser Wert stellt eine logische Menge (Objektgröße) dar, keine physische Menge (Größe auf der Festplatte).

Wenn kein Limit festgelegt ist, ist die Kapazität für diesen Bucket unbegrenzt. Weitere Informationen finden Sie unter "[Kapazitätslimitnutzung](#)" für weitere Informationen.

5. Wählen Sie **Bucket erstellen**.

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

6. Wählen Sie optional **Zur Bucket-Detailseite**, um "[Bucket-Details anzeigen](#)" und führen Sie zusätzliche Konfigurationen durch.

Bucket-Details anzeigen

Sie können die Buckets in Ihrem Mandantenkonto einsehen.

Bevor Sie beginnen

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

Schritte

1. Wählen Sie im Dashboard **Buckets anzeigen** oder wählen Sie **STORAGE (S3) > Buckets**.

Die Seite „Buckets“ wird angezeigt.

2. Überprüfen Sie die Übersichtstabelle für jeden Bucket.

Sie können die Informationen je nach Bedarf nach beliebigen Spalten sortieren oder in der Liste vor- und zurückblättern.



Die angezeigten Werte für Objektanzahl, belegten Speicherplatz und Nutzung sind Schätzungen. Diese Schätzungen werden durch den Zeitpunkt der Aufnahme, die Netzwerkverfügbarkeit und den Knotenstatus beeinflusst. Wenn für Buckets die Versionierung aktiviert ist, werden gelöschte Objektversionen in die Objektzählung einbezogen.

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

Ob die S3-Objektsperre für den Bucket aktiviert ist.

Diese Spalte wird nur angezeigt, wenn die S3-Objektsperre für das Raster aktiviert ist. Diese Spalte zeigt auch Informationen zu allen älteren konformen Buckets an.

Region

Die Region des Buckets, die 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.

Verwendeter Speicherplatz

Die logische Größe aller Objekte im Bucket. Die logische Größe umfasst nicht den tatsächlichen Speicherplatz, der für replizierte oder löschedodierte Kopien oder für Objektmetadaten benötigt wird.

Die Aktualisierung dieses Werts kann bis zu 10 Minuten dauern.

Verwendung

Der verwendete Prozentsatz der Kapazitätsgrenze des Buckets, sofern eine festgelegt wurde.

Der Nutzungswert basiert auf internen Schätzungen und kann in Einzelfällen überschritten werden. Beispielsweise überprüft StorageGRID das Kapazitätsgrenze (sofern festgelegt), wenn ein Mandant mit dem Hochladen von Objekten beginnt, und lehnt neue Aufnahmen in diesen Bucket ab, wenn der Mandant das Kapazitätsgrenze überschritten hat. StorageGRID berücksichtigt jedoch nicht die Größe des aktuellen Uploads, wenn es feststellt, ob das Kapazitätsgrenze überschritten wurde. Wenn Objekte gelöscht werden, kann es einem Mandanten vorübergehend untersagt werden, neue Objekte in diesen Bucket hochzuladen, bis die Kapazitätsgrenzenutzung neu berechnet wird. Die Berechnungen können 10 Minuten oder länger dauern.

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

Kapazität

Falls festgelegt, die Kapazitätsgrenze für den Bucket.

Erstellungsdatum

Datum und Uhrzeit der Bucket-Erstellung. Diese Spalte ist standardmäßig ausgeblendet.

3. Um Details zu einem bestimmten Bucket anzuzeigen, wählen Sie den Bucket-Namen aus der Tabelle aus.
 - a. Sehen Sie sich 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 Kapazitätsgrenze-Nutzungsleiste 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**.

Achten Sie genau auf die Warnhinweise, die bei der Auswahl der einzelnen Optionen angezeigt werden. Weitere Informationen finden Sie unter:



- ["Alle Objekte in einem Bucket löschen"](#)
- ["Löschen eines Buckets"](#) (Eimer muss leer sein)

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

- **S3-Konsole:** Zeigen Sie die Objekte für den Bucket an. Weitere Informationen finden Sie unter ["Verwenden Sie die S3-Konsole"](#).
- **Bucket-Optionen:** Optionseinstellungen anzeigen oder ändern. Einige Einstellungen, wie z. B. S3 Object Lock, können nach der Erstellung des Buckets nicht mehr geändert werden.
 - ["Verwalten der Bucket-Konsistenz"](#)
 - ["Aktualisierungen der letzten Zugriffszeit"](#)
 - ["Kapazitätsgrenze"](#)
 - ["Objektversionierung"](#)
 - ["S3-Objektsperre"](#)
 - ["Standardmäßige Bucket-Aufbewahrung"](#)
 - ["Verwalten der Cross-Grid-Replikation"](#) (sofern für den Mieter zulässig)
- **Plattformdienste:** ["Plattformdienste verwalten"](#) (sofern für den Mieter zulässig)
- **Bucket-Zugriff:** Optionseinstellungen anzeigen oder ändern. Sie müssen über bestimmte Zugriffsberechtigungen verfügen.
 - Konfigurieren ["Cross-Origin-Ressourcenfreigabe \(CORS\)"](#) sodass der Bucket und die Objekte im Bucket für Webanwendungen in anderen Domänen zugänglich sind.
 - ["Benutzerzugriff steuern"](#) für einen S3-Bucket und Objekte in diesem Bucket.

Anwenden eines ILM-Richtlinientags auf einen Bucket

Wählen Sie basierend auf Ihren Objektspeicheranforderungen ein ILM-Richtlinien-Tag aus, das auf einen Bucket angewendet werden soll.

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



Vermeiden Sie die häufige Neuzuweisung des Richtlinien-Tags eines Buckets. Andernfalls können Leistungsprobleme auftreten.

Bevor Sie beginnen

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

Schritte

1. Wählen Sie im Dashboard **Buckets anzeigen** oder wählen Sie **STORAGE (S3) > Buckets**.

Die Seite „Buckets“ wird angezeigt. Sie können die Informationen je nach Bedarf nach beliebigen Spalten sortieren oder in der Liste vor- und zurückblättern.

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

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



Die angezeigten Werte für „Objektanzahl“ und „Benutzter Speicherplatz“ sind Schätzungen. Diese Schätzungen werden durch den Zeitpunkt der Aufnahme, die Netzwerkkonnektivität und den Knotenstatus beeinflusst. Wenn für Buckets die Versionierung aktiviert ist, werden gelöschte Objektversionen in die Objektzählung einbezogen.

3. Erweitern Sie auf der Registerkarte „Bucket-Optionen“ das Akkordeon „ILM-Richtlinientag“. Dieses Akkordeon wird nur angezeigt, wenn Ihr Grid-Administrator die Verwendung benutzerdefinierter Richtlinien-Tags aktiviert hat.
4. Lesen Sie die Beschreibung jedes Richtlinien-Tags, um zu bestimmen, welches Tag auf den Bucket angewendet werden soll.



Das Ändern des ILM-Richtlinientags für einen Bucket löst eine ILM-Neubewertung aller Objekte im Bucket aus. Wenn die neue Richtlinie Objekte für eine begrenzte Zeit aufbewahrt, werden ältere Objekte gelöscht.

5. Wählen Sie das Optionsfeld für das Tag aus, das Sie dem Bucket zuweisen möchten.

6. Wählen Sie **Änderungen speichern**. Ein neues S3-Bucket-Tag wird auf dem Bucket mit dem Schlüssel gesetzt `NTAP-SG-ILM-BUCKET-TAG` und der Wert des ILM-Richtlinien-Tag-Namens.



Stellen Sie sicher, dass Ihre S3-Anwendungen das neue Bucket-Tag nicht versehentlich überschreiben oder löschen. Wenn dieses Tag beim Anwenden eines neuen TagSets auf den Bucket weggelassen wird, werden die Objekte im Bucket wieder anhand der ILM-Standardrichtlinie ausgewertet.



Legen Sie ILM-Richtlinien-Tags fest und ändern Sie sie nur mithilfe des Tenant Managers oder der Tenant Manager-API, wo das ILM-Richtlinien-Tag validiert wird. Ändern Sie nicht die `NTAP-SG-ILM-BUCKET-TAG` ILM-Richtlinientag mithilfe der S3 PutBucketTagging-API oder der S3 DeleteBucketTagging-API.



Das Ändern des einem Bucket zugewiesenen Richtlinientags hat vorübergehende Auswirkungen auf die Leistung, während Objekte mithilfe der neuen ILM-Richtlinie neu ausgewertet werden.

Bucket-Richtlinie verwalten

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

Bevor Sie beginnen

- Sie sind beim Tenant Manager angemeldet mit einem "[unterstützter Webbrowser](#)".
- Sie gehören einer Benutzergruppe an, die über die "[Root-Zugriffsberechtigung](#)". Die Berechtigungen „Alle Buckets anzeigen“ und „Alle Buckets verwalten“ erlauben nur das Anzeigen.
- Sie haben überprüft, dass die erforderliche Anzahl an Speicherknoten und Sites verfügbar ist. Wenn an einem Standort zwei oder mehr Speicherknoten nicht verfügbar sind oder ein Standort nicht verfügbar ist, können diese Einstellungen möglicherweise nicht geändert werden.

Schritte

1. Wählen Sie **Buckets** und dann den Bucket aus, den Sie verwalten möchten.
2. Wählen Sie auf der Bucket-Detailseite **Bucket-Zugriff > Bucket-Richtlinie** aus.
3. Führen Sie einen der folgenden Schritte aus:
 - Geben Sie eine Bucket-Richtlinie ein, indem Sie das Kontrollkästchen **Richtlinie aktivieren** aktivieren. Geben Sie dann eine gültige Zeichenfolge im JSON-Format ein.

Jede Bucket-Richtlinie hat eine Größenbeschränkung von 20.480 Bytes.

 - Ändern Sie eine vorhandene Richtlinie, indem Sie die Zeichenfolge bearbeiten.
 - Deaktivieren Sie eine Richtlinie, indem Sie die Option **Richtlinie aktivieren** abwählen.

Ausführliche Informationen zu Bucket-Richtlinien, einschließlich Sprachsyntax und Beispielen, finden Sie unter "[Beispiele für Bucket-Richtlinien](#)".

Verwalten der Bucket-Konsistenz

Konsistenzwerte können verwendet werden, um die Verfügbarkeit von Bucket-Einstellungsänderungen anzugeben und um ein Gleichgewicht zwischen der Verfügbarkeit der Objekte innerhalb eines Buckets und der Konsistenz dieser Objekte über verschiedene Speicherknoten und Sites hinweg herzustellen. Sie können die Konsistenzwerte so ändern, dass sie von den Standardwerten abweichen, damit Clientanwendungen ihre Betriebsanforderungen erfüllen können.

Bevor Sie beginnen

- Sie sind beim Tenant Manager angemeldet mit einem "[unterstützter Webbrowser](#)".
- Sie gehören einer Benutzergruppe an, die über die "[Verwalten Sie alle Buckets oder Root-Zugriffsberechtigungen](#)". Diese Berechtigungen überschreiben die Berechtigungseinstellungen in Gruppen- oder Bucket-Richtlinien.

Richtlinien zur Eimerkonsistenz

Die Bucket-Konsistenz wird verwendet, um die Konsistenz für Clientanwendungen zu bestimmen, die sich auf Objekte innerhalb dieses S3-Buckets auswirken. Im Allgemeinen sollten Sie für Ihre Buckets die Konsistenz **Lesen nach neuem Schreiben** verwenden.

Konsistenz des Änderungs-Buckets

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



Wenn Sie die Konsistenz eines Buckets ändern, wird nur für die Objekte, die nach der Änderung aufgenommen werden, garantiert, dass sie der überarbeiteten Einstellung entsprechen.

Schritte

1. Wählen Sie im Dashboard **Buckets anzeigen** oder wählen Sie **STORAGE (S3) > Buckets**.
 2. Wählen Sie den Bucket-Namen aus der Tabelle aus.
- Die Bucket-Detailseite wird angezeigt.
3. Wählen Sie auf der Registerkarte **Bucket-Optionen** das ** Akkordeon aus.
 4. Wählen Sie eine Konsistenz für Vorgänge aus, die an den Objekten in diesem Bucket ausgeführt werden.
 - **Alle**: Bietet das höchste Maß an Konsistenz. Alle Knoten empfangen die Daten sofort, andernfalls schlägt die Anforderung fehl.
 - **Stark global**: Garantiert Lese-nach-Schreib-Konsistenz für alle Clientanforderungen auf allen Sites.
 - **Strong-Site**: Garantiert die Lese-nach-Schreib-Konsistenz für alle Clientanforderungen innerhalb einer Site.
 - **Lesen nach neuem Schreiben** (Standard): Bietet Lese-nach-Schreib-Konsistenz für neue Objekte und letztendliche Konsistenz für Objektaktualisierungen. Bietet hohe Verfügbarkeit und Datenschutzgarantien. Für die meisten Fälle empfohlen.
 - **Verfügbar**: Bietet letztendliche Konsistenz sowohl für neue Objekte als auch für Objektaktualisierungen. Verwenden Sie es für S3-Buckets nur nach Bedarf (z. B. für einen Bucket, der Protokollwerte enthält, die selten gelesen werden, oder für HEAD- oder GET-Operationen für nicht vorhandene Schlüssel). Wird für S3 FabricPool Buckets nicht unterstützt.
 5. Wählen Sie **Änderungen speichern**.

Was passiert, wenn Sie die Bucket-Einstellungen ändern?

Buckets verfügen über mehrere Einstellungen, die das Verhalten der Buckets und der Objekte in diesen Buckets beeinflussen.

Die folgenden Bucket-Einstellungen verwenden standardmäßig **starke** Konsistenz. Wenn an einem Standort zwei oder mehr Speicherknoten nicht verfügbar sind oder wenn ein Standort nicht verfügbar ist, sind Änderungen an diesen Einstellungen möglicherweise nicht möglich.

- "Löschen eines leeren Buckets im Hintergrund"
- "Letzter Zugriffszeitpunkt"
- "Bucket-Lebenszyklus"
- "Bucket-Richtlinie"
- "Bucket-Tagging"
- "Bucket-Versionierung"
- "S3-Objektsperre"
- "Bucket-Verschlüsselung"



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

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

- ["Konfiguration der Plattformdienste: Benachrichtigung, Replikation oder Suchintegration"](#)
- ["CORS-Konfiguration"](#)
- [Eimerkonsistenz ändern](#)

 Wenn die beim Ändern der Bucket-Einstellungen verwendete Standardkonsistenz nicht den Anforderungen der Client-Anwendung entspricht, können Sie die Konsistenz mithilfe der Consistency-Control Kopfzeile für die ["S3 REST API"](#) oder mithilfe der `reducedConsistency` oder `force` Optionen in der ["Mandantenverwaltungs-API"](#).

Aktivieren oder Deaktivieren der Aktualisierung der letzten Zugriffszeit

Wenn Grid-Administratoren die Regeln für das Information Lifecycle Management (ILM) für ein StorageGRID System erstellen, können sie optional angeben, dass der Zeitpunkt des letzten Zugriffs auf ein Objekt verwendet werden soll, um zu bestimmen, ob dieses Objekt an einen anderen Speicherort verschoben werden soll. Wenn Sie einen S3-Mandanten verwenden, können Sie solche Regeln nutzen, indem Sie Aktualisierungen 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 **Letzter Zugriffszeitpunkt** als erweiterten Filter oder als Referenzzeit verwendet. Sie können diese Anweisungen ignorieren, wenn Ihr StorageGRID System keine solche Regel enthält. Sehen ["Verwenden der letzten Zugriffszeit in ILM-Regeln"](#) für Details.

Bevor Sie beginnen

- Sie sind beim Tenant Manager angemeldet mit einem ["unterstützter Webbrowser"](#).
- Sie gehören einer Benutzergruppe an, die über die ["Verwalten Sie alle Buckets oder Root-Zugriffsberechtigungen"](#). Diese Berechtigungen überschreiben die Berechtigungseinstellungen in Gruppen- oder Bucket-Richtlinien.

Informationen zu diesem Vorgang

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

Um beispielsweise sicherzustellen, dass kürzlich angezeigte Objekte auf einem schnelleren Speicher 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 abgeholt wurden, sollten an einen externen Standort gebracht werden.

Standardmäßig sind Aktualisierungen der letzten Zugriffszeit deaktiviert. Wenn Ihr StorageGRID System eine ILM-Regel enthält, die die Option **Letzter Zugriffszeitpunkt** verwendet, und Sie möchten, dass diese Option auf Objekte in diesem Bucket angewendet wird, müssen Sie Aktualisierungen des letzten Zugriffszeitpunkts für die in dieser Regel angegebenen S3-Buckets aktivieren.



Das Aktualisieren der letzten Zugriffszeit beim Abrufen eines Objekts kann die StorageGRID Leistung verringern, insbesondere bei kleinen Objekten.

Bei Aktualisierungen der letzten Zugriffszeit kommt es zu Leistungseinbußen, da StorageGRID bei jedem Abrufen von Objekten die folgenden zusätzlichen Schritte ausführen muss:

- Aktualisieren Sie die Objekte mit neuen Zeitstempeln
- Fügen Sie die Objekte zur ILM-Warteschlange hinzu, damit sie anhand der aktuellen 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 bei aktivierter letzter Zugriffszeit	
	Letzte Zugriffszeit aktualisiert?	Objekt zur ILM-Auswertungswarteschlange hinzugefügt?	Letzte Zugriffszeit aktualisiert?	Objekt zur ILM-Auswertungswarteschlange hinzugefügt?
Anforderung zum Abrufen eines Objekts, seiner Zugriffskontrollliste oder seiner Metadaten	Nein	Nein	Ja	Ja
Anforderung zum Aktualisieren der Metadaten eines Objekts	Ja	Ja	Ja	Ja
Anfrage zum Auflisten von Objekten oder Objektversionen	Nein	Nein	Nein	Nein
Anforderung zum Kopieren eines Objekts von einem Bucket in einen anderen	<ul style="list-style-type: none">• Nein, für die Quellkopie• Ja, für die Zielkopie	<ul style="list-style-type: none">• Nein, für die Quellkopie• Ja, für die Zielkopie	<ul style="list-style-type: none">• Ja, für die Quellkopie• Ja, für die Zielkopie	<ul style="list-style-type: none">• Ja, für die Quellkopie• Ja, für die Zielkopie
Anfrage zum Abschließen eines mehrteiligen Uploads	Ja, für das montierte Objekt	Ja, für das montierte Objekt	Ja, für das montierte Objekt	Ja, für das montierte Objekt

Schritte

1. Wählen Sie im Dashboard **Buckets anzeigen** oder wählen Sie **STORAGE (S3) > Buckets**.
 2. Wählen Sie den Bucket-Namen aus der Tabelle aus.
- Die Bucket-Detailseite wird angezeigt.
3. Wählen Sie auf der Registerkarte **Bucket-Optionen** das Akkordeon **Aktualisierungen der letzten Zugriffszeit** aus.
 4. Aktivieren oder deaktivieren Sie Aktualisierungen der letzten Zugriffszeit.
 5. Wählen Sie **Änderungen speichern**.

Ändern der 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 angemeldet mit einem "[unterstützter Webbrowser](#)" .
- Sie gehören einer Benutzergruppe an, die über die "[Verwalten Sie alle Buckets oder Root-Zugriffsberechtigungen](#)" . Diese Berechtigungen überschreiben die Berechtigungseinstellungen in Gruppen- oder Bucket-Richtlinien.
- Sie haben überprüft, dass die erforderliche Anzahl an Speicherknoten und Sites verfügbar ist. Wenn an einem Standort zwei oder mehr Speicherknoten nicht verfügbar sind oder ein Standort nicht verfügbar ist, können diese Einstellungen möglicherweise nicht geändert werden.

Informationen zu diesem Vorgang

Sie können die Objektversionierung für einen Bucket aktivieren oder aussetzen. Nachdem Sie die Versionierung für einen Bucket aktiviert haben, kann dieser nicht mehr in einen nicht versionierten Zustand zurückversetzt werden. Sie können die Versionierung für den Bucket jedoch aussetzen.

- Deaktiviert: Die Versionierung wurde nie aktiviert
- Aktiviert: Versionierung ist aktiviert
- Ausgesetzt: Die Versionsverwaltung war zuvor aktiviert und ist ausgesetzt

Weitere Informationen finden Sie unter:

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

Schritte

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

Die Bucket-Detailseite wird angezeigt.

3. Wählen Sie auf der Registerkarte **Bucket-Optionen** das Akkordeon **Objektversionierung** aus.
4. Wählen Sie einen Versionsstatus für die Objekte in diesem Bucket aus.

Die Objektversionierung muss für einen Bucket aktiviert bleiben, der für die Cross-Grid-Replikation

verwendet wird. Wenn S3 Object Lock oder Legacy-Compliance aktiviert ist, sind die Optionen zur **Objektversionierung** deaktiviert.

Option	Beschreibung
Aktivieren der Versionsverwaltung	Aktivieren Sie die Objektversionierung, wenn Sie jede Version jedes Objekts in diesem Bucket speichern möchten. Sie können dann bei Bedarf frühere Versionen eines Objekts abrufen. Objekte, die sich bereits im Bucket befanden, werden versioniert, wenn sie von einem Benutzer geändert werden.
Versionsverwaltung aussetzen	Unterbrechen Sie die Objektversionierung, wenn Sie nicht mehr möchten, dass neue Objektversionen erstellt werden. Sie können weiterhin alle vorhandenen Objektversionen abrufen.

5. Wählen Sie **Änderungen speichern**.

Verwenden Sie S3 Object Lock, um Objekte beizubehalten

Sie können S3 Object Lock verwenden, wenn Buckets und Objekte den gesetzlichen Aufbewahrungsanforderungen entsprechen müssen.



Ihr Grid-Administrator muss Ihnen die Berechtigung zur Verwendung bestimmter Funktionen von S3 Object Lock erteilen.

Was ist S3 Object Lock?

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

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

Ein Bucket ohne S3-Objektsperre kann nur Objekte ohne angegebene Aufbewahrungseinstellungen enthalten. Für aufgenommene Objekte werden keine Aufbewahrungseinstellungen festgelegt.

Ein Bucket mit S3 Object Lock kann Objekte mit und ohne Aufbewahrungseinstellungen enthalten, die von S3-Clientanwendungen angegeben werden. Für einige aufgenommene Objekte gelten Aufbewahrungseinstellungen.

Ein Bucket mit S3 Object Lock und konfigurierter Standardaufbewahrung kann hochgeladene Objekte mit angegebenen Aufbewahrungseinstellungen und neue Objekte ohne Aufbewahrungseinstellungen enthalten. 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 davon unberührt.

Aufbewahrungsmodi

Die StorageGRID S3 Object Lock-Funktion unterstützt zwei Aufbewahrungsmodi, um unterschiedliche Schutzstufen auf Objekte anzuwenden. Diese Modi entsprechen den Aufbewahrungsmodi von Amazon S3.

- Im Compliance-Modus:
 - Das Objekt kann erst gelöscht werden, wenn sein 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 Sonderberechtigung können in Anfragen einen Bypass-Header verwenden, um bestimmte Aufbewahrungseinstellungen zu ändern.
 - Diese Benutzer können eine Objektversion löschen, bevor ihr Aufbewahrungsdatum erreicht ist.
 - Diese Benutzer können das Aufbewahrungsdatum eines Objekts erhöhen, verringern oder entfernen.

Aufbewahrungseinstellungen für Objektversionen

Wenn ein Bucket mit aktivierter S3-Objektsperre erstellt wird, können Benutzer mit der S3-Clientanwendung optional die folgenden Aufbewahrungseinstellungen für jedes dem Bucket hinzugefügte Objekt angeben:

- **Aufbewahrungsmodus:** Entweder Compliance oder Governance.
- **Aufbewahrungsdatum:** Wenn das Aufbewahrungsdatum einer Objektversion in der Zukunft liegt, kann das Objekt abgerufen, aber nicht gelöscht werden.
- **Rechtliche Sperre:** Durch Anwenden einer rechtlichen Sperre auf eine Objektversion wird dieses Objekt sofort gesperrt. Beispielsweise müssen Sie möglicherweise ein Objekt, das mit einer Untersuchung oder einem Rechtsstreit in Zusammenhang steht, rechtlich sperren. Eine rechtliche Sperre hat kein Ablaufdatum, sondern bleibt bestehen, bis sie ausdrücklich aufgehoben wird. Rechtliche Sperren sind unabhängig vom Aufbewahrungsdatum.



Wenn ein Objekt einer rechtlichen Sperre unterliegt, kann niemand das Objekt löschen, unabhängig von seinem Aufbewahrungsmodus.

Details zu den Objekteinstellungen finden Sie unter "["Verwenden Sie die S3 REST API, um S3 Object Lock zu konfigurieren"](#)".

Standardaufbewahrungseinstellung für Buckets

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

- **Standardaufbewahrungsmodus:** Entweder Compliance oder Governance.
- **Standardaufbewahrungszeitraum:** Wie lange neue Objektversionen, die diesem Bucket hinzugefügt werden, ab dem Tag ihrer Hinzufügung aufbewahrt werden sollen.

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

Sehen "["Erstellen eines S3-Buckets"](#)" Und "["Standardaufbewahrung für S3 Object Lock aktualisieren"](#)" .

S3 Object Lock-Aufgaben

Die folgenden Listen für Grid-Administratoren und Mandantenbenutzer enthalten die allgemeinen Aufgaben zur Verwendung der S3 Object Lock-Funktion.

Grid-Administrator

- Aktivieren Sie die globale S3-Objektsperreinstellung für das gesamte StorageGRID System.
- Stellen Sie sicher, dass die Richtlinien für das Information Lifecycle Management (ILM) *konform* sind; das heißt, sie erfüllen die "[Anforderungen an Buckets mit aktiverter S3-Objektsperre](#)".
- Erlauben Sie einem Mandanten bei Bedarf, Compliance als Aufbewahrungsmodus zu verwenden. Andernfalls ist nur der Governance-Modus zulässig.
- Legen Sie bei Bedarf eine maximale Aufbewahrungszeitdauer für einen Mandanten fest.

Mandantenbenutzer

- Überprüfen Sie die Überlegungen zu Buckets und Objekten mit S3 Object Lock.
- Wenden Sie sich bei Bedarf an den Grid-Administrator, um die globale S3-Objektsperreinstellung zu aktivieren und Berechtigungen festzulegen.
- Erstellen Sie Buckets mit aktiverter S3-Objektsperre.
- Konfigurieren Sie optional die Standardaufbewahrungseinstellungen für einen Bucket:
 - Standardaufbewahrungsmodus: Governance oder Compliance, sofern vom Grid-Administrator zugelassen.
 - Standardaufbewahrungszeitraum: Muss kleiner oder gleich dem vom Grid-Administrator festgelegten maximalen Aufbewahrungszeitraum sein.
- Verwenden Sie die S3-Clientanwendung, um Objekte hinzuzufügen und optional eine objektspezifische Aufbewahrung festzulegen:
 - Aufbewahrungsmodus: Governance oder Compliance, sofern vom Grid-Administrator zugelassen.
 - Aufbewahrungsdatum: Muss kleiner oder gleich dem vom Grid-Administrator festgelegten maximalen Aufbewahrungszeitraum sein.

Anforderungen für Buckets mit aktiverter S3-Objektsperre

- Wenn die globale S3-Objektsperre-Einstellung für das StorageGRID -System aktiviert ist, können Sie den Tenant Manager, die Tenant Management API oder die S3 REST API verwenden, um Buckets mit aktiverter S3-Objektsperre zu erstellen.
- Wenn Sie S3 Object Lock verwenden möchten, müssen Sie S3 Object Lock beim Erstellen des Buckets aktivieren. Sie können S3 Object Lock nicht für einen vorhandenen Bucket aktivieren.
- Wenn S3 Object Lock für einen Bucket aktiviert ist, aktiviert StorageGRID automatisch die Versionierung für diesen Bucket. Sie können die S3-Objektsperre nicht deaktivieren oder die Versionsverwaltung für den Bucket aussetzen.
- Optional können Sie mithilfe des Tenant Managers, der Tenant Management API oder der S3 REST API einen Standardaufbewahrungsmodus und eine Standardaufbewahrungszeitdauer für jeden Bucket angeben. Die Standardaufbewahrungseinstellungen des Buckets gelten nur für neue Objekte, die dem Bucket hinzugefügt werden und keine eigenen Aufbewahrungseinstellungen haben. Sie können diese Standardeinstellungen überschreiben, indem Sie beim Hochladen für jede Objektversion einen Aufbewahrungsmodus und ein Aufbewahrungsdatum angeben.
- Die Bucket-Lebenszykluskonfiguration wird für Buckets mit aktiverter S3-Objektsperre unterstützt.
- Die CloudMirror-Replikation wird für Buckets mit aktiverter S3-Objektsperre nicht unterstützt.

Anforderungen für Objekte in Buckets mit aktivierter S3-Objektsperre

- Um eine Objektversion zu schützen, können Sie Standardaufbewahrungseinstellungen für den Bucket oder Aufbewahrungseinstellungen für jede Objektversion angeben. Aufbewahrungseinstellungen auf Objektebene können mithilfe der S3-Clientanwendung oder der S3-REST-API angegeben werden.
- Aufbewahrungseinstellungen gelten für einzelne Objektversionen. Eine Objektversion kann sowohl über eine Aufbewahrungsfrist als auch über eine gesetzliche Aufbewahrungsfrist verfügen, über eine der beiden Einstellungen, aber nicht über die andere, oder über keine von beiden. Durch die Angabe eines Aufbewahrungsdatums oder einer Einstellung für die rechtliche Aufbewahrung eines Objekts 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 mit aktivierter S3-Objektsperre

Jedes Objekt, das in einem Bucket mit aktivierter S3-Objektsperre gespeichert wird, durchläuft die folgenden Phasen:

1. Objektaufnahme

Wenn eine Objektversion zu einem Bucket hinzugefügt wird, für den die S3-Objektsperre aktiviert ist, werden die Aufbewahrungseinstellungen wie folgt angewendet:

- Wenn für das Objekt Aufbewahrungseinstellungen angegeben sind, werden die Einstellungen auf Objektebene angewendet. Alle Standard-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 sind, 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 von StorageGRID mehrere Kopien für den angegebenen Aufbewahrungszeitraum gespeichert. Die genaue Anzahl und Art der Objektkopien sowie die Speicherorte werden durch die konformen Regeln in den aktiven ILM-Richtlinien bestimmt. Ob ein geschütztes Objekt vor Erreichen seines Aufbewahrungsdatums gelöscht werden kann, hängt von seinem Aufbewahrungsmodus ab.

- Wenn ein Objekt einer rechtlichen Sperre unterliegt, kann niemand das Objekt löschen, unabhängig von seinem Aufbewahrungsmodus.

Kann ich weiterhin ältere konforme Buckets verwalten?

Die S3 Object Lock-Funktion ersetzt die Compliance-Funktion, die in früheren StorageGRID Versionen verfügbar war. Wenn Sie konforme Buckets mit einer früheren Version von StorageGRID erstellt haben, können Sie die Einstellungen dieser Buckets weiterhin verwalten. Sie können jedoch keine neuen konformen Buckets mehr erstellen. Anweisungen hierzu finden Sie unter https://kb.netapp.com/Advice_and_Troubleshooting/Hybrid_Cloud_Infrastructure/StorageGRID/How_to_manage_legacy_Compliant_buckets_in_StorageGRID_11.5 [NetApp Knowledge Base: So verwalten Sie ältere konforme Buckets in StorageGRID 11.5].

Standardaufbewahrung für S3 Object Lock aktualisieren

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

Bevor Sie beginnen

- Sie sind beim Tenant Manager angemeldet mit einem "[unterstützter Webbrower](#)".
- Sie gehören einer Benutzergruppe an, die über die "[Verwalten Sie alle Buckets oder Root-Zugriffsberechtigungen](#)". Diese Berechtigungen überschreiben die Berechtigungseinstellungen in Gruppen- oder Bucket-Richtlinien.
- S3 Object Lock ist global für Ihr StorageGRID -System aktiviert und Sie haben S3 Object Lock beim Erstellen des Buckets aktiviert. Sehen "[Verwenden Sie S3 Object Lock, um Objekte beizubehalten](#)".

Schritte

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

Die Bucket-Detailseite wird angezeigt.

3. Wählen Sie auf der Registerkarte **Bucket-Optionen** das Akkordeon **S3-Objektsperre** aus.
4. Aktivieren oder deaktivieren Sie optional die **Standardaufbewahrung** für diesen Bucket.

Änderungen an dieser Einstellung gelten nicht für Objekte, die sich bereits im Bucket befinden, oder für Objekte, die möglicherweise eigene Aufbewahrungszeiträume haben.

5. Wenn **Standardaufbewahrung** aktiviert ist, geben Sie einen **Standardaufbewahrungsmodus** für den Bucket an.

Standardaufbewahrungsmodus	Beschreibung
Führung	<ul style="list-style-type: none">• Benutzer mit der <code>s3:BypassGovernanceRetention</code> Berechtigung kann die <code>x-amz-bypass-governance-retention: true</code> Anforderungsheader zum Umgehen der Aufbewahrungseinstellungen.• Diese Benutzer können eine Objektversion löschen, bevor ihr Aufbewahrungsdatum erreicht ist.• Diese Benutzer können das Aufbewahrungsdatum eines Objekts erhöhen, verringern oder entfernen.

Standardaufbewahrungsmodus	Beschreibung
Einhaltung	<ul style="list-style-type: none"> Das Objekt kann erst gelöscht werden, wenn sein 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. <p>Hinweis: Ihr Grid-Administrator muss Ihnen die Verwendung des Compliance-Modus gestatten.</p>

6. Wenn die **Standardaufbewahrung** aktiviert ist, geben Sie die **Standardaufbewahrungsduer** für den Bucket an.

Die **Standardaufbewahrungsfrist** gibt an, wie lange neue Objekte, die diesem 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 Aufbewahrungsduer für den Mandanten ist.

Eine *maximale* Aufbewahrungsduer, die zwischen 1 Tag und 100 Jahren liegen kann, wird festgelegt, wenn der Grid-Administrator den Mandanten erstellt. Wenn Sie eine *Standard*-Aufbewahrungsduer festlegen, darf diese den für die maximale Aufbewahrungsduer festgelegten Wert nicht überschreiten. Bitten Sie Ihren Grid-Administrator bei Bedarf, die maximale Aufbewahrungsduer zu verlängern oder zu verkürzen.

7. Wählen Sie **Änderungen speichern**.

Konfigurieren Sie Cross-Origin Resource Sharing (CORS)

Sie können Cross-Origin Resource Sharing (CORS) für einen S3-Bucket konfigurieren, wenn dieser Bucket und die darin enthaltenen Objekte für Webanwendungen in anderen Domänen zugänglich sein sollen.

Bevor Sie beginnen

- Sie sind beim Tenant Manager angemeldet mit einem "[unterstützter Webbrowser](#)" .
- Für GET CORS-Konfigurationsanfragen gehören Sie zu einer Benutzergruppe, die über die "[Berechtigung „Alle Buckets verwalten“](#) oder [„Alle Buckets anzeigen“](#)". Diese Berechtigungen überschreiben die Berechtigungseinstellungen in Gruppen- oder Bucket-Richtlinien.
- Für PUT CORS-Konfigurationsanfragen gehören Sie zu einer Benutzergruppe, die über die "[Berechtigung „Alle Buckets verwalten“](#)". Diese Berechtigung überschreibt die Berechtigungseinstellungen in Gruppen- oder Bucket-Richtlinien.
- Der "[Root-Zugriffsberechtigung](#)" bietet Zugriff auf alle CORS-Konfigurationsanforderungen.

Informationen zu diesem Vorgang

Cross-Origin Resource Sharing (CORS) ist ein Sicherheitsmechanismus, der es Client-Webanwendungen in einer Domäne ermöglicht, auf Ressourcen in einer anderen Domäne zuzugreifen. Angenommen, Sie verwenden einen S3-Bucket namens `Images` zum Speichern von Grafiken. Durch die Konfiguration von CORS für die `Images` Bucket, können Sie die Anzeige der Bilder in diesem Bucket auf der Website zulassen <http://www.example.com> .

CORS für einen Bucket aktivieren

Schritte

1. Verwenden Sie einen Texteditor, um das erforderliche XML zu erstellen. Dieses Beispiel zeigt das XML, das zum Aktivieren von CORS für einen S3-Bucket verwendet wird. Speziell:

- Ermöglicht jeder Domäne, GET-Anfragen an den Bucket zu senden
- Erlaubt nur die `http://www.example.com` Domäne zum Senden von GET-, POST- und DELETE-Anfragen
- Alle Anforderungsheader 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-Benutzerhandbuch"](#).

2. Wählen Sie im Dashboard **Buckets anzeigen** oder wählen Sie **STORAGE (S3) > Buckets**.

3. Wählen Sie den Bucket-Namen aus der Tabelle aus.

Die Bucket-Detailseite wird angezeigt.

4. Wählen Sie auf der Registerkarte **Bucket-Zugriff** 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 **Löschen** aus, um von vorne zu beginnen.
2. Wählen Sie **Änderungen speichern**.

CORS-Einstellung deaktivieren

Schritte

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

Objekte im Bucket löschen

Mit dem Tenant Manager können Sie die Objekte in einem oder mehreren Buckets löschen.

Überlegungen und Anforderungen

Beachten Sie vor der Durchführung dieser Schritte Folgendes:

- Wenn Sie die Objekte in einem Bucket löschen, entfernt StorageGRID dauerhaft alle Objekte und alle Objektversionen in jedem ausgewählten Bucket von allen Knoten und Sites in Ihrem StorageGRID System. StorageGRID entfernt auch alle zugehörigen Objektmetadaten. Sie können diese Informationen nicht wiederherstellen.
- Das Löschen aller Objekte in einem Bucket kann je nach Anzahl der Objekte, Objektkopien und gleichzeitigen Vorgängen Minuten, Tage oder sogar Wochen dauern.
- Wenn ein Eimer "[S3-Objektsperre aktiviert](#)" , kann es *Jahre* lang im Status **Objekte werden gelöscht: schreibgeschützt** verbleiben.



Ein Bucket, der S3 Object Lock verwendet, verbleibt im Status **Objekte werden gelöscht: schreibgeschützt**, bis das Aufbewahrungsdatum für alle Objekte erreicht ist und alle rechtlichen Sperren aufgehoben wurden.

- Während Objekte gelöscht werden, lautet der Status des Buckets **Objekte werden gelöscht: schreibgeschützt**. In diesem Zustand können Sie dem Bucket keine neuen Objekte hinzufügen.
- Wenn alle Objekte gelöscht wurden, bleibt der Bucket im schreibgeschützten Zustand. Sie können einen der folgenden Schritte ausführen:
 - Setzen Sie den Bucket wieder in den Schreibmodus und verwenden Sie ihn erneut für neue Objekte
 - Löschen Sie den Bucket
 - Behalten Sie den Bucket im schreibgeschützten Modus, um seinen Namen für die 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 Vorgänge „Objekte im Bucket löschen“ entfernt werden.
- Wenn für einen Bucket die Objektversionierung aktiviert ist, werden beim Löschen von Objekten keine Löschmarkierungen entfernt, die in StorageGRID 11.7 oder früher erstellt wurden. Informationen zum Löschen von Objekten in einem Bucket finden Sie in "[So werden versionierte S3-Objekte gelöscht](#)" .
- Wenn Sie "[Cross-Grid-Replikation](#)" , beachten Sie Folgendes:
 - Durch die Verwendung dieser Option werden keine Objekte aus dem Bucket im anderen Raster gelöscht.
 - Wenn Sie diese Option für den Quell-Bucket auswählen, wird die Warnung **Fehler bei der Grid-übergreifenden Replikation** ausgelöst, wenn Sie dem Ziel-Bucket im anderen Grid Objekte hinzufügen. Wenn Sie nicht garantieren können, dass niemand Objekte zum Bucket auf dem anderen Raster hinzufügt, "[Deaktivieren Sie die Cross-Grid-Replikation](#)" für diesen Bucket, bevor alle Bucket-

Objekte gelöscht werden.

Bevor Sie beginnen

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

Schritte

1. Wählen Sie im Dashboard **Buckets anzeigen** oder wählen Sie **STORAGE (S3) > Buckets**.

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

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 **Aktionen > Objekte im Bucket löschen**.

Detailseite

- a. Wählen Sie einen Bucket-Namen aus, um dessen 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 einigen Minuten:

- Auf der Bucket-Detailseite wird ein gelbes Statusbanner angezeigt. Der Fortschrittsbalken zeigt an, wie viel Prozent der Objekte gelöscht wurden.
- **(schreibgeschützt)** wird nach dem Bucket-Namen auf der Bucket-Detailseite angezeigt.
- **(Objekte löschen: schreibgeschützt)** wird neben dem Namen des Buckets auf der Seite „Buckets“ angezeigt.

5. Wählen Sie bei Bedarf während der Ausführung des Vorgangs **Löschen von Objekten stoppen** aus, um den Prozess anzuhalten. Wählen Sie dann optional **Objekte im Bucket löschen** aus, um den Vorgang fortzusetzen.

Wenn Sie „Löschen von Objekten beenden“ auswählen, wird der Bucket wieder in den Schreibmodus versetzt. Sie können jedoch nicht auf gelöschte 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 schreibgeschützt.

7. Führen Sie einen der folgenden Schritte aus:

- Verlassen Sie die Seite, um den Bucket im schreibgeschützten Modus zu belassen. Sie können beispielsweise einen leeren Bucket im schreibgeschützten Modus belassen, um den Bucket-Namen für

die zukünftige Verwendung zu reservieren.

- Löschen Sie den Bucket. Sie können **Bucket löschen** auswählen, um einen einzelnen Bucket zu löschen, oder zur Buckets-Seite zurückkehren und **Aktionen > Buckets löschen** auswählen, um mehr als einen Bucket zu entfernen.



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

- Bringen Sie den Bucket zurück in den Schreibmodus und verwenden Sie ihn optional für neue Objekte erneut. Sie können **Löschen von Objekten stoppen** für einen einzelnen Bucket auswählen oder zur Buckets-Seite zurückkehren und **Aktion > Löschen von Objekten stoppen** für mehr als einen Bucket auswählen.

S3-Bucket löschen

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

Bevor Sie beginnen

- Sie sind beim Tenant Manager angemeldet mit einem "[unterstützter Webbrowser](#)" .
- Sie gehören einer Benutzergruppe an, die über die "[Verwalten Sie alle Buckets oder Root-Zugriffsberechtigungen](#)" . Diese Berechtigungen überschreiben die Berechtigungseinstellungen in Gruppen- oder Bucket-Richtlinien.
- Die Buckets, die Sie löschen möchten, sind leer. Wenn die Buckets, die Sie löschen möchten, *nicht* leer sind, "[Objekte aus dem Bucket löschen](#)" .

Informationen zu diesem Vorgang

Diese Anweisungen beschreiben, wie Sie einen S3-Bucket mit dem Tenant Manager löschen. Sie können S3-Buckets auch löschen, indem Sie "[Mandantenverwaltungs-API](#)" oder die "[S3 REST API](#)" .

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

Schritte

1. Wählen Sie im Dashboard **Buckets anzeigen** oder wählen Sie **STORAGE (S3) > Buckets**.

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

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 **Aktionen > Buckets löschen**.

Detailseite

- a. Wählen Sie einen Bucket-Namen aus, um dessen Details anzuzeigen.
- b. Wählen Sie **Bucket 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, erscheint eine Fehlermeldung. Sie müssen "[alle Objekte und alle Löschmarkierungen im Bucket löschen](#)" bevor Sie den Bucket löschen können.

Verwenden Sie die S3-Konsole

Sie können die S3-Konsole verwenden, um die Objekte in einem S3-Bucket anzuzeigen und zu verwalten.

Mit der S3-Konsole können Sie:

- Objekte hochladen, herunterladen, umbenennen, kopieren, verschieben und löschen
- Objektversionen anzeigen, zurücksetzen, herunterladen und löschen
- Suche nach Objekten anhand des Präfixes
- Objekt-Tags verwalten
- Objektmetadaten anzeigen
- Ordner anzeigen, erstellen, umbenennen, kopieren, verschieben und löschen

Die S3-Konsole bietet in den gängigsten Fällen eine verbesserte Benutzererfahrung. Es ist nicht dafür gedacht, CLI- oder API-Operationen in allen Situationen zu ersetzen.

 Wenn die Verwendung der S3-Konsole dazu führt, dass Vorgänge zu lange dauern (z. B. Minuten oder Stunden), sollten Sie Folgendes in Betracht ziehen:

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

Bevor Sie beginnen

- Sie sind beim Tenant Manager angemeldet mit einem "[unterstützter Webbrowser](#)".
- Wenn Sie Objekte verwalten möchten, gehören Sie zu einer Benutzergruppe, die über die Root-Zugriffsberechtigung verfügt. Alternativ gehören Sie zu einer Benutzergruppe, die über die Berechtigung „Registerkarte „S3-Konsole verwenden“ und entweder die Berechtigung „Alle Buckets anzeigen“ oder „Alle Buckets verwalten“ verfügt. Sehen "[Berechtigungen zur Mandantenverwaltung](#)".
- Für den Benutzer wurde eine S3-Gruppen- oder Bucket-Richtlinie konfiguriert. Sehen "[Verwenden Sie 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 die "[Anleitung 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.

4. Wählen Sie * Sign in*.
5. Die Tabelle mit den Bucket-Objekten wird angezeigt. Sie können Objekte nach Bedarf verwalten.

Weitere Informationen

- **Suche nach Präfix:** Die Präfix-Suchfunktion sucht nur nach Objekten, die relativ zum aktuellen Ordner mit einem bestimmten Wort beginnen. Die Suche umfasst keine Objekte, die das Wort an anderer Stelle enthalten. Diese Regel gilt auch für Objekte innerhalb von Ordnern. Beispielsweise eine Suche nach `folder1/folder2/somefile-` würde Objekte zurückgeben, die innerhalb der `folder1/folder2/` Ordner und beginnen Sie mit dem Wort `somefile-` .
- **Drag & Drop:** Sie können Dateien per Drag & Drop aus dem Dateimanager Ihres Computers in die S3-Konsole ziehen. Sie können jedoch keine Ordner hochladen.
- **Operationen an Ordnern:** Wenn Sie einen Ordner verschieben, kopieren oder umbenennen, werden alle Objekte im Ordner einzeln aktualisiert, was einige Zeit dauern kann.
- **Dauerhaftes Löschen bei deaktivierter Bucket-Versionierung:** Wenn Sie ein Objekt in einem Bucket mit deaktivierter Versionierung überschreiben oder löschen, ist der Vorgang dauerhaft. Sehen "[Ändern der Objektversionierung für einen Bucket](#)" .

Verwalten von S3-Plattformdiensten

S3-Plattformdienste

Übersicht und Überlegungen zu Plattformdiensten

Lesen Sie vor der Implementierung von Plattformdiensten die Übersicht und die Überlegungen zur Verwendung dieser Dienste.

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

Übersicht der Plattformdienste

Die StorageGRID -Plattformdienste können Ihnen bei der Implementierung einer Hybrid-Cloud-Strategie helfen, indem sie Ihnen das Senden von Ereignisbenachrichtigungen und Kopien von S3-Objekten und Objektmetadaten an externe Ziele ermöglichen.

Da sich der Zielspeicherort für Plattformdienste normalerweise außerhalb Ihrer StorageGRID Bereitstellung befindet, bieten Ihnen Plattformdienste die Leistung und Flexibilität, die Sie durch die Verwendung externer Speicherressourcen, Benachrichtigungsdienste und Such- oder Analysedienste für Ihre Daten erhalten.

Für einen einzelnen S3-Bucket kann jede beliebige Kombination von Plattformdiensten konfiguriert werden. Sie können beispielsweise sowohl die "[CloudMirror-Dienst](#)" Und "[Benachrichtigungen](#)" auf einem StorageGRID S3-Bucket, sodass Sie bestimmte Objekte auf den Amazon Simple Storage Service (S3) spiegeln können, während Sie zu jedem dieser Objekte eine Benachrichtigung an eine Überwachungsanwendung eines Drittanbieters senden, die Ihnen bei der Verfolgung Ihrer AWS-Ausgaben hilft.



Die Nutzung der Plattformdienste muss für jedes Mandantenkonto von einem StorageGRID -Administrator über den Grid Manager oder die Grid Management API aktiviert werden.

So werden Plattformdienste konfiguriert

Plattformdienste kommunizieren mit externen Endpunkten, die Sie mithilfe der "[Mietermanager](#)" oder die "[Mandantenverwaltungs-API](#)" . Jeder Endpunkt stellt ein externes Ziel dar, beispielsweise einen

StorageGRID S3-Bucket, einen Amazon Web Services-Bucket, ein Amazon SNS-Thema 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 die der Bucket einwirken soll, die Aktion, die der Bucket ausführen soll, und den Endpunkt, den der Bucket für den Dienst verwenden soll.

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

- Wenn Sie alle Objekte möchten, deren Schlüssel mit `/images` enden, um in einen Amazon S3-Bucket repliziert zu werden, müssen Sie dem Quell-Bucket eine Replikationskonfiguration hinzufügen.
- Wenn Sie auch Benachrichtigungen senden möchten, wenn diese Objekte im Bucket gespeichert werden, müssen Sie eine Benachrichtigungskonfiguration hinzufügen.
- Wenn Sie die Metadaten für diese Objekte indizieren möchten, müssen Sie die Metadatenbenachrichtigungskonfiguration hinzufügen, die zum Implementieren der Suchintegration verwendet wird.

Das Format für die XML-Konfiguration wird durch die S3-REST-APIs bestimmt, die zur Implementierung der StorageGRID -Plattformdienste verwendet werden:

Plattformdienst	S3 REST API	Siehe
CloudMirror-Replikation	<ul style="list-style-type: none"> • <code>GetBucketReplication</code> • <code>PutBucketReplication</code> 	<ul style="list-style-type: none"> • "CloudMirror-Replikation" • "Operationen an Buckets"
Benachrichtigungen	<ul style="list-style-type: none"> • <code>GetBucketNotificationConfiguration</code> • <code>PutBucketNotificationConfiguration</code> 	<ul style="list-style-type: none"> • "Benachrichtigungen" • "Operationen an Buckets"
Suchintegration	<ul style="list-style-type: none"> • <code>GET Bucket-Metadaten-Benachrichtigungskonfiguration</code> • Konfiguration der Benachrichtigung über <code>PUT-Bucket-Metadaten</code> 	<ul style="list-style-type: none"> • "Suchintegration" • "Benutzerdefinierte StorageGRID -Vorgänge"

Überlegungen zur Verwendung von Plattformdiensten

Rücksichtnahme	Details
Zielendpunktüberwachung	Sie müssen die Verfügbarkeit jedes Zielendpunkts überwachen. Wenn die Verbindung zum Zielendpunkt über einen längeren Zeitraum unterbrochen ist und ein großer Rückstand an Anfragen besteht, schlagen weitere Clientanfragen (z. B. <code>PUT</code> -Anfragen) an StorageGRID fehl. Sie müssen diese fehlgeschlagenen Anfragen wiederholen, wenn der Endpunkt erreichbar ist.

Rücksichtnahme	Details
Drosselung des Zielendpunkts	<p>Die StorageGRID Software drosselt möglicherweise eingehende S3-Anfragen für einen Bucket, wenn die Rate, mit der die Anfragen gesendet werden, die Rate überschreitet, mit der der Zielendpunkt die Anfragen empfangen kann. Eine Drosselung tritt nur auf, wenn ein Rückstand an Anfragen besteht, die darauf warten, an den Zielendpunkt gesendet zu werden.</p> <p>Der einzige sichtbare Effekt besteht darin, dass die Ausführung eingehender S3-Anfragen länger dauert. Wenn Sie eine deutlich langsamere Leistung feststellen, sollten Sie die Aufnahmerate reduzieren oder einen Endpunkt mit höherer Kapazität verwenden. Wenn der Rückstand an Anfragen weiter wächst, schlagen Client-S3-Operationen (wie etwa PUT-Anfragen) letztendlich fehl.</p> <p>Bei CloudMirror-Anfragen ist die Leistung des Zielendpunkts wahrscheinlicher beeinträchtigt, da diese Anfragen in der Regel mehr Datenübertragungen beinhalten als Anfragen zur Suchintegration oder Ereignisbenachrichtigung.</p>
Bestellgarantien	<p>StorageGRID garantiert die Reihenfolge der Vorgänge an einem Objekt innerhalb einer Site. Solange alle Vorgänge für ein Objekt innerhalb derselben Site erfolgen, entspricht der endgültige Objektstatus (für die Replikation) immer dem Status in StorageGRID.</p> <p>StorageGRID versucht nach besten Kräften, Anfragen zu ordnen, wenn Vorgänge über StorageGRID -Sites hinweg ausgeführt werden. Wenn Sie beispielsweise ein Objekt zunächst an Standort A schreiben und dasselbe Objekt später an Standort B überschreiben, ist nicht garantiert, dass das endgültige, von CloudMirror in den Ziel-Bucket replizierte Objekt das neuere Objekt ist.</p>
ILM-gesteuerte Objektlöschungen	<p>Um dem Löschverhalten von AWS CRR und Amazon Simple Notification Service zu entsprechen, werden CloudMirror- und Ereignisbenachrichtigungsanforderungen nicht gesendet, wenn ein Objekt im Quell-Bucket aufgrund von StorageGRID ILM-Regeln gelöscht wird. Beispielsweise werden keine CloudMirror- oder Ereignisbenachrichtigungsanforderungen gesendet, wenn eine ILM-Regel ein Objekt nach 14 Tagen löscht.</p> <p>Im Gegensatz dazu werden Suchintegrationsanforderungen gesendet, wenn Objekte aufgrund von ILM gelöscht werden.</p>

Rücksichtnahme	Details
Verwenden von Kafka-Endpunkten	<p>Für Kafka-Endpunkte wird Mutual TLS nicht unterstützt. Wenn Sie also <code>ssl.client.auth</code> eingestellt auf <code>required</code> in Ihrer Kafka-Broker-Konfiguration kann es zu Problemen bei der Kafka-Endpunktkonfiguration kommen.</p> <p>Die Authentifizierung von Kafka-Endpunkten verwendet die folgenden Authentifizierungstypen. Diese Typen unterscheiden sich von denen, die für die Authentifizierung anderer Endpunkte wie Amazon SNS verwendet werden, und erfordern Anmeldeinformationen mit Benutzername und Kennwort.</p> <ul style="list-style-type: none"> • SASL/PLAIN • SASL/SCRAM-SHA-256 • SASL/SCRAM-SHA-512 <p>Hinweis: Konfigurierte Speicherproxyeinstellungen gelten nicht für Endpunkte der Kafka-Plattformdienste.</p>

Überlegungen zur Verwendung des CloudMirror-Replikationsdienstes

Rücksichtnahme	Details
Replikationsstatus	StorageGRID unterstützt nicht die <code>x-amz-replication-status</code> Kopfzeile.
Objektgröße	<p>Die maximale Größe für Objekte, die vom CloudMirror-Replikationsdienst in einen Ziel-Bucket repliziert werden können, beträgt 5 TiB, was der maximal unterstützten Objektgröße entspricht.</p> <p>Hinweis: Die maximal <i>empfohlene</i> Größe für einen einzelnen PutObject-Vorgang beträgt 5 GiB (5.368.709.120 Bytes). Wenn Sie Objekte haben, die größer als 5 GiB sind, verwenden Sie stattdessen den mehrteiligen Upload.</p>
Bucket-Versionierung und Versions-IDs	<p>Wenn für den Quell-S3-Bucket in StorageGRID die Versionierung aktiviert ist, sollten Sie auch die Versionierung für den Ziel-Bucket aktivieren.</p> <p>Beachten Sie bei der Verwendung der Versionierung, dass die Reihenfolge der Objektversionen im Ziel-Bucket nach bestem Wissen und Gewissen erfolgt und aufgrund von Einschränkungen im S3-Protokoll nicht vom CloudMirror-Dienst garantiert wird.</p> <p>Hinweis: Versions-IDs für den Quell-Bucket in StorageGRID stehen in keinem Zusammenhang mit den Versions-IDs für den Ziel-Bucket.</p>

Rücksichtnahme	Details
Tagging für Objektversionen	<p>Aufgrund von Einschränkungen im S3-Protokoll repliziert der CloudMirror-Dienst keine PutObjectTagging- oder DeleteObjectTagging-Anfragen, die eine Versions-ID bereitstellen. Da die Versions-IDs für Quelle und Ziel nicht miteinander verknüpft sind, kann nicht sichergestellt werden, dass eine Tag-Aktualisierung auf eine bestimmte Versions-ID repliziert wird.</p> <p>Im Gegensatz dazu repliziert der CloudMirror-Dienst PutObjectTagging-Anfragen oder DeleteObjectTagging-Anfragen, die keine Versions-ID angeben. Diese Anfragen aktualisieren die Tags für den neuesten Schlüssel (oder die neueste Version, wenn der Bucket versioniert ist). Normale Aufnahmen mit Tags (keine Tagging-Updates) werden ebenfalls repliziert.</p>
Mehrteilige Uploads und ETag Werte	Beim Spiegeln von Objekten, die mit einem mehrteiligen Upload hochgeladen wurden, behält der CloudMirror-Dienst die Teile nicht bei. Infolgedessen ETag Wert für das gespiegelte Objekt wird anders sein als der ETag Wert des ursprünglichen Objekts.
Mit SSE-C verschlüsselte Objekte (serverseitige Verschlüsselung mit vom Kunden bereitgestellten Schlüsseln)	Der CloudMirror-Dienst unterstützt keine mit SSE-C verschlüsselten Objekte. Wenn Sie versuchen, ein Objekt in den Quell-Bucket für die CloudMirror-Replikation aufzunehmen und die Anforderung die SSE-C-Anforderungsheader enthält, schlägt der Vorgang fehl.
Bucket mit aktiver S3-Objektsperre	Die Replikation wird für Quell- oder Ziel-Buckets mit aktiver S3-Objektsperre nicht unterstützt.

Grundlegendes zum CloudMirror-Replikationsdienst

Sie können die CloudMirror-Replikation für einen S3-Bucket aktivieren, wenn StorageGRID bestimmte, dem Bucket hinzugefügte Objekte in einen oder mehrere externe Ziel-Buckets repliziert.

Sie können beispielsweise die CloudMirror-Replikation verwenden, um bestimmte Kundendatensätze in Amazon S3 zu spiegeln und dann AWS-Dienste nutzen, um Analysen Ihrer Daten durchzuführen.



Die CloudMirror-Replikation wird nicht unterstützt, wenn im Quell-Bucket S3 Object Lock aktiviert ist.

CloudMirror und ILM

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

CloudMirror und Cross-Grid-Replikation

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

CloudMirror und S3-Buckets

Die CloudMirror-Replikation ist normalerweise so konfiguriert, dass ein externer S3-Bucket als Ziel verwendet wird. Sie können die Replikation jedoch auch so konfigurieren, dass eine andere StorageGRID Bereitstellung oder ein beliebiger S3-kompatibler Dienst verwendet wird.

Vorhandene Eimer

Wenn Sie die CloudMirror-Replikation für einen vorhandenen Bucket aktivieren, werden nur die neuen Objekte repliziert, die diesem Bucket hinzugefügt werden. Alle vorhandenen Objekte im Bucket werden nicht repliziert. Um die Replikation vorhandener Objekte zu erzwingen, können Sie die Metadaten des vorhandenen Objekts aktualisieren, indem Sie eine Objektkopie durchführen.



Wenn Sie die CloudMirror-Replikation zum Kopieren von Objekten an ein Amazon S3-Ziel verwenden, beachten Sie, dass Amazon S3 die Größe benutzerdefinierter Metadaten in jedem PUT-Anforderungsheader auf 2 KB begrenzt. Wenn ein Objekt benutzerdefinierte Metadaten größer als 2 KB hat, wird dieses Objekt nicht repliziert.

Mehrere Ziel-Buckets

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

Versionierte oder nicht versionierte Buckets

Sie können die CloudMirror-Replikation auf versionierten oder nicht versionierten Buckets konfigurieren. Die Ziel-Buckets können versioniert oder nicht versioniert sein. Sie können jede beliebige Kombination aus versionierten und nicht versionierten Buckets verwenden. Sie können beispielsweise einen versionierten Bucket als Ziel für einen nicht versionierten Quell-Bucket angeben oder umgekehrt. Sie können auch zwischen Buckets ohne Versionsnummer replizieren.

Löschen, Replikationsschleifen 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 im Ziel gelöscht. Wenn sowohl Quell- als auch Ziel-Buckets versioniert sind, wird die Löschmarkierung repliziert. Wenn der Ziel-Bucket nicht versioniert ist, wird beim Löschen eines Objekts im Quell-Bucket weder die Löschmarkierung in den Ziel-Bucket repliziert noch das Zielobjekt gelöscht.

Schutz vor Replikationsschleifen

Wenn Objekte in den Ziel-Bucket repliziert werden, markiert StorageGRID sie als „Replikate“. Ein StorageGRID Ziel-Bucket repliziert als Replikate markierte Objekte nicht erneut und schützt Sie so vor versehentlichen Replikationsschleifen. Diese Replikatmarkierung erfolgt intern für 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 einer Replik verwendet wird, ist `x-ntap-sg-replica`. Diese Markierung verhindert einen Kaskadenspiegel. StorageGRID unterstützt einen bidirektionalen CloudMirror zwischen zwei Grids.

Ereignisse im Ziel-Bucket

Die Eindeutigkeit und Reihenfolge der Ereignisse im Ziel-Bucket sind nicht garantiert. Aufgrund von Vorgängen, die zur Gewährleistung einer erfolgreichen Zustellung durchgeführt werden, kann es vorkommen, dass mehrere identische Kopien eines Quellobjekts an das Ziel übermittelt werden. In seltenen Fällen, wenn dasselbe Objekt gleichzeitig von zwei oder mehr verschiedenen StorageGRID Sites aktualisiert wird, stimmt die Reihenfolge der Vorgänge im Ziel-Bucket möglicherweise nicht mit der Reihenfolge der Ereignisse im Quell-Bucket überein.

Benachrichtigungen für Buckets verstehen

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

Sie können beispielsweise Warnmeldungen konfigurieren, die an Administratoren gesendet werden, wenn ein Objekt zu einem Bucket hinzugefügt wird, wobei die Objekte Protokolldateien darstellen, die mit einem kritischen Systemereignis verknüpft sind.

Ereignisbenachrichtigungen werden im Quell-Bucket wie in der Benachrichtigungskonfiguration angegeben erstellt und an das Ziel übermittelt. Wenn ein mit einem Objekt verknüpftes Ereignis erfolgreich ist, wird eine Benachrichtigung über dieses Ereignis erstellt und zur Übermittlung in die Warteschlange gestellt.

Die Eindeutigkeit und Reihenfolge der Benachrichtigungen sind nicht garantiert. Aufgrund von Vorgängen, die zur Gewährleistung einer erfolgreichen Zustellung durchgeführt werden, kann es sein, dass mehrere Benachrichtigungen zu einem Ereignis an das Ziel übermittelt werden. Und da die Übermittlung asynchron erfolgt, kann nicht garantiert werden, dass die zeitliche Reihenfolge der Benachrichtigungen am Ziel mit der Reihenfolge der Ereignisse im Quell-Bucket übereinstimmt, insbesondere bei Vorgängen, die von verschiedenen StorageGRID Sites stammen. Sie können die `sequencer` Geben Sie in der Ereignsnachricht den Schlüssel ein, 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:Objekt erstellt:
 - s3:ObjektErstellt:Put
 - s3:ObjektErstellt:Post
 - s3:ObjektErstellt:Kopie
 - s3:Objekterstellt:MehrteiligerUpload abgeschlossen
 - s3:Objekt entfernt:
 - s3:Objekt entfernt:Löschen
 - s3:Objekt entfernt:DeleteMarker erstellt
 - s3:ObjectRestore:Post
- Von StorageGRID gesendete Ereignisbenachrichtigungen verwenden das standardmäßige JSON-Format, enthalten jedoch einige Schlüssel nicht und verwenden für andere bestimmte Werte, wie in der Tabelle gezeigt:

Schlüsselname	StorageGRID -Wert
Ereignisquelle	sgws:s3
awsRegion	<i>nicht enthalten</i>
x-amz-id-2	<i>nicht enthalten</i>
arn	urn:sgws:s3:::bucket_name

Verstehen Sie den Suchintegrationsdienst

Sie können die Suchintegration für einen S3-Bucket aktivieren, wenn Sie einen externen Such- und Datenanalysedienst für Ihre Objektmetadaten verwenden möchten.

Der Suchintegrationsdienst ist ein benutzerdefinierter StorageGRID Dienst, der automatisch und asynchron S3-Objektmetadaten an einen Zielendpunkt sendet, wenn ein Objekt erstellt oder gelöscht wird oder seine Metadaten oder Tags aktualisiert werden. Sie können dann die vom Zieldienst bereitgestellten ausgefeilten Such-, Datenanalyse-, Visualisierungs- oder maschinellen Lerntools verwenden, um Ihre Objektdaten zu durchsuchen, zu analysieren und Erkenntnisse daraus zu gewinnen.

Sie können Ihre Buckets beispielsweise so konfigurieren, dass S3-Objektmetadaten an einen Remote-Elasticsearch-Dienst gesendet werden. Anschließend können Sie Elasticsearch verwenden, um Bucket-übergreifende Suchen durchzuführen und anspruchsvolle Analysen der in Ihren Objektmetadaten vorhandenen Muster durchzuführen.

Obwohl die Elasticsearch-Integration für einen Bucket mit aktiver S3-Objektsperre konfiguriert werden kann, werden die S3-Objektsperre-Metadaten (einschließlich „Aufbewahrungsdatum“ und „Legal Hold“-Status) der Objekte nicht in die an Elasticsearch gesendeten Metadaten aufgenommen.

 Da der Suchintegrationsdienst das Senden von Objektmetadaten an ein Ziel veranlasst, wird sein Konfigurations-XML als „*Metadaten*-Benachrichtigungskonfigurations-XML“ bezeichnet. Dieses Konfigurations-XML unterscheidet sich vom „Benachrichtigungskonfigurations-XML“, das zum Aktivieren von *Ereignis*-Benachrichtigungen verwendet wird.

Suchintegration und S3-Buckets

Sie können den Suchintegrationsdienst für jeden versionierten oder nicht versionierten Bucket aktivieren. Die Suchintegration wird konfiguriert, indem die XML-Konfigurationsdatei für Metadatenbenachrichtigungen mit dem Bucket verknüpft wird, der angibt, auf welche Objekte reagiert werden soll und das Ziel für die Objektmetadaten ist.

Metadatenbenachrichtigungen werden in Form eines JSON-Dokuments generiert, das den Bucket-Namen, den Objektnamen und die Versions-ID (sofern vorhanden) enthält. Jede Metadatenbenachrichtigung enthält zusätzlich zu allen Tags und Benutzermetadaten des Objekts einen Standardsatz von Systemmetadaten für das Objekt.

 Für Tags und Benutzermetadaten übergibt StorageGRID Daten und Zahlen als Zeichenfolgen oder als S3-Ereignisbenachrichtigungen an Elasticsearch. Um Elasticsearch so zu konfigurieren, dass diese Zeichenfolgen als Datumsangaben oder Zahlen interpretiert werden, befolgen Sie die Elasticsearch-Anweisungen zur dynamischen Feldzuordnung und zur 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.

Suchbenachrichtigungen

Metadatenbenachrichtigungen werden generiert und zur Zustellung in die Warteschlange gestellt, wenn:

- Ein Objekt wird erstellt.
- Ein Objekt wird gelöscht, auch wenn Objekte aufgrund der Ausführung der ILM-Richtlinie des Grids gelöscht werden.
- Objektmetadaten oder Tags werden hinzugefügt, aktualisiert oder gelöscht. Beim Update wird immer der komplette Satz an Metadaten und Tags gesendet – nicht nur die geänderten Werte.

Nachdem Sie einem Bucket XML-Metadatenbenachrichtigungskonfigurations-XML hinzugefügt haben, werden Benachrichtigungen für alle neuen Objekte gesendet, die Sie erstellen, und für alle Objekte, die Sie durch Aktualisieren der Daten, Benutzermetadaten oder Tags ändern. Es werden jedoch keine Benachrichtigungen für Objekte gesendet, die sich bereits im Bucket befanden. Um sicherzustellen, dass die Objektmetadaten für alle Objekte im Bucket an das Ziel gesendet werden, sollten Sie einen der folgenden Schritte ausführen:

- Konfigurieren Sie den Suchintegrationsdienst unmittelbar nach dem Erstellen des Buckets und vor dem Hinzufügen von Objekten.
- Führen Sie für alle Objekte, die sich bereits im Bucket befinden, eine Aktion aus, die das Senden einer Metadatenbenachrichtigung an das Ziel auslöst.

Suchintegrationsdienst und Elasticsearch

Der Suchintegrationsdienst StorageGRID unterstützt einen Elasticsearch-Cluster als Ziel. Wie bei den anderen Plattformdiensten wird das Ziel im Endpunkt angegeben, dessen URN im Konfigurations-XML für den Dienst verwendet wird. Verwenden Sie die ["NetApp Interoperabilitätsmatrix-Tool"](#) um die unterstützten Versionen von Elasticsearch zu ermitteln.

Verwalten von Plattformdienst-Endpunkten

Konfigurieren von Plattformdienstendpunkten

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

Der Zugriff auf Plattformdienste wird pro Mandant von einem StorageGRID -Administrator aktiviert. Um einen Plattformdienst-Endpunkt zu erstellen oder zu verwenden, müssen Sie ein Mandantenbenutzer mit der Berechtigung „Endpunkte verwalten“ oder „Root-Zugriff“ in einem Grid sein, dessen Netzwerk so konfiguriert wurde, dass Speicherknoten auf externe Endpunktressourcen zugreifen können. Für einen einzelnen Mandanten können Sie maximal 500 Plattformdienst-Endpunkte konfigurieren. Wenden Sie sich für weitere Informationen an Ihren StorageGRID Administrator.

Was ist ein Plattformdienst-Endpunkt?

Ein Plattformdienst-Endpunkt 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 Plattformdienst-Endpunkt, der die Informationen und Anmeldeinformationen enthält, die StorageGRID für den Zugriff auf den Ziel-Bucket bei Amazon benötigt.

Jeder Plattformdiensttyp erfordert einen eigenen Endpunkt. Sie müssen daher für jeden Plattformdienst, den Sie verwenden möchten, mindestens einen Endpunkt konfigurieren. Nachdem Sie einen Plattformdienst-Endpunkt definiert haben, verwenden Sie die URN des Endpunkts als Ziel in der Konfigurations-XML, die zum Aktivieren des Dienstes verwendet wird.

Sie können denselben Endpunkt als Ziel für mehr als einen Quell-Bucket verwenden. Sie können beispielsweise mehrere Quell-Buckets so konfigurieren, dass sie Objektmetadaten an denselben Suchintegrationsendpunkt senden, sodass Sie Suchvorgänge über mehrere Buckets hinweg durchführen können. Sie können einen Quell-Bucket auch so konfigurieren, dass er mehr als einen Endpunkt als Ziel verwendet. Dadurch können Sie beispielsweise Benachrichtigungen über die Objekterstellung an ein Amazon Simple Notification Service (Amazon SNS)-Thema und Benachrichtigungen über die Objektlöschung an ein zweites Amazon SNS-Thema senden.

Endpunkte für die CloudMirror-Replikation

StorageGRID unterstützt Replikationsendpunkte, die S3-Buckets darstellen. Diese Buckets können auf Amazon Web Services, derselben oder einer Remote- StorageGRID Bereitstellung oder einem anderen Dienst gehostet werden.

Endpunkte für Benachrichtigungen

StorageGRID unterstützt Amazon SNS- und Kafka-Endpunkte. Simple Queue Service (SQS) oder 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 Suchintegrationsdienst

StorageGRID unterstützt Suchintegrationsendpunkte, die Elasticsearch-Cluster darstellen. Diese Elasticsearch-Cluster können sich in einem lokalen Rechenzentrum befinden oder in einer AWS-Cloud oder anderswo 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 Endpunktterstellung fehl. Sie müssen den Typ nicht erstellen, bevor Sie den Endpunkt erstellen. StorageGRID erstellt den Typ bei Bedarf, wenn es Objektmetadaten an den Endpunkt sendet.

Ähnliche Informationen

["StorageGRID verwalten"](#)

Geben Sie die URN für den Plattformdienst-Endpunkt an

Wenn Sie einen Plattformdienste-Endpunkt erstellen, müssen Sie einen eindeutigen

Ressourcennamen (URN) angeben. Sie verwenden die URN, um auf den Endpunkt zu verweisen, wenn Sie eine XML-Konfiguration für den Plattformdienst erstellen. Die URN für jeden Endpunkt muss eindeutig sein.

StorageGRID validiert die Endpunkte der Plattformdienste, während Sie sie erstellen. Bevor Sie einen Plattformdienste-Endpunkt erstellen, bestätigen Sie, dass die im Endpunkt angegebene Ressource vorhanden und erreichbar ist.

URN-Elemente

Die URN für einen Plattformdienst-Endpunkt muss mit einem der folgenden Zeichen beginnen: `arn:aws` oder `urn:mysite`, wie folgt:

- Wenn der Dienst auf Amazon Web Services (AWS) gehostet wird, verwenden Sie `arn:aws`
- Wenn der Dienst 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, könnte die URN mit beginnen `urn:sgws`.

Das nächste Element der URN gibt den Typ des Plattformdienstes wie folgt an:

Service	Typ
CloudMirror-Replikation	<code>s3</code>
Benachrichtigungen	<code>sns</code> oder <code>kafka</code>
Suchintegration	<code>es</code>

Um beispielsweise weiterhin die URN für einen CloudMirror-Endpunkt anzugeben, der auf StorageGRID gehostet wird, würden Sie hinzufügen `s3` zu bekommen `urn:sgws:s3`.

Das letzte Element der URN identifiziert die spezifische Zielressource an der Ziel-URI.

Service	Spezifische Ressource
CloudMirror-Replikation	<code>bucket-name</code>
Benachrichtigungen	<code>sns-topic-name</code> oder <code>kafka-topic-name</code>
Suchintegration	<code>domain-name/index-name/type-name</code>

Hinweis: Wenn der Elasticsearch-Cluster **nicht** für die automatische Erstellung von Indizes konfiguriert ist, müssen Sie den Index manuell erstellen, bevor Sie den Endpunkt erstellen.

URNs für auf AWS und GCP gehostete Dienste

Für AWS- und GCP-Entitäten ist die vollständige URN eine gültige AWS-ARN. Beispiel:

- CloudMirror-Replikation:

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

- Benachrichtigungen:

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

- Suchintegration:

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



Für einen AWS-Suchintegrationsendpunkt ist der domain-name muss die Literalzeichenfolge enthalten domain/ , wie hier gezeigt.

URNs für lokal gehostete Dienste

Wenn Sie lokal gehostete Dienste anstelle von Cloud-Diensten verwenden, können Sie die URN auf jede beliebige Weise angeben, die eine gültige und eindeutige URN erstellt, solange die URN die erforderlichen Elemente an der dritten und letzten Stelle enthält. Sie können die optional angegebenen Elemente leer lassen oder sie auf eine beliebige Weise angeben, die Ihnen bei der Identifizierung der Ressource hilft und die URN eindeutig macht. Beispiel:

- CloudMirror-Replikation:

```
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 Amazon Simple Notification Service-Endpunkt an:

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

Geben Sie einen Kafka-Endpunkt an:

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

- Suchintegration:

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



Für lokal gehostete Suchintegrationsendpunkte gilt: domain-name Das Element kann eine beliebige Zeichenfolge sein, solange die URN des Endpunkts eindeutig ist.

Plattformdienst-Endpunkt erstellen

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

Bevor Sie beginnen

- Sie sind beim Tenant Manager angemeldet mit einem "[unterstützter Webbrowser](#)" .
- Die Plattformdienste wurden von einem StorageGRID Administrator für Ihr Mandantenkonto aktiviert.
- Sie gehören einer Benutzergruppe an, die über die "[Verwalten von Endpunkten oder Root-Zugriffsberechtigungen](#)" .
- Die vom Plattformdienst-Endpunkt referenzierte Ressource wurde erstellt:
 - CloudMirror-Replikation: S3-Bucket
 - Ereignisbenachrichtigung: Amazon Simple Notification Service (Amazon SNS) oder Kafka-Thema
 - Suchbenachrichtigung: Elasticsearch-Index, wenn der Zielcluster nicht für die automatische Erstellung von Indizes konfiguriert ist.
- Sie verfügen über die Informationen zur Zielressource:
 - Host und Port für den Uniform Resource Identifier (URI)



Wenn Sie einen auf einem StorageGRID -System gehosteten Bucket als Endpunkt für die CloudMirror-Replikation verwenden möchten, wenden Sie sich an den Grid-Administrator, um die einzugebenden Werte zu ermitteln.

- Eindeutiger Ressourcename (URN)

["Geben Sie die URN für den Plattformdienst-Endpunkt an"](#)

- Authentifizierungsdaten (falls erforderlich):

Suchintegrationsendpunkte

Für Suchintegrationsendpunkte können Sie die folgenden Anmeldeinformationen verwenden:

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

CloudMirror-Replikationsendpunkte

Für CloudMirror-Replikationsendpunkte können Sie die folgenden Anmeldeinformationen verwenden:

- Zugriffsschlüssel: Zugriffsschlüssel-ID und geheimer Zugriffsschlüssel
- CAP (C2S Access Portal): URL für temporäre Anmeldeinformationen, Server- und Client-Zertifikate, Client-Schlüssel und eine optionale Passphrase für den privaten Client-Schlüssel.

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 (bei Verwendung eines benutzerdefinierten CA-Zertifikats)

- Wenn die Elasticsearch-Sicherheitsfunktionen aktiviert sind, verfügen Sie über die Berechtigung zum Überwachen des Clusters für Konnektivitätstests und entweder über die Berechtigung zum Schreiben des Index oder über die Berechtigung zum Indexieren und Löschen des Index für Dokumentaktualisierungen.

Schritte

1. Wählen Sie **STORAGE (S3) > Plattformdienst-Endpunkte**. Die Seite „Plattformdienst-Endpunkte“ 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 Unique 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-URLs und Port 80 für HTTP-URLs (die meisten Endpunkte)
- Port 9092 für HTTPS und HTTP-URLs (nur Kafka-Endpunkte)

Beispielsweise könnte die URI für einen auf StorageGRID gehosteten Bucket wie folgt lauten:

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

In diesem Beispiel `s3.example.com` stellt den DNS-Eintrag für die virtuelle IP (VIP) der StorageGRID Hochverfügbarkeitsgruppe (HA) dar und 10443 stellt den im Load Balancer-Endpunkt definierten Port dar.



Wenn möglich, sollten Sie eine Verbindung zu einer HA-Gruppe von Lastausgleichsknoten herstellen, um einen einzelnen Fehlerpunkt zu vermeiden.

Ähnlich könnte die URI für einen auf AWS gehosteten Bucket lauten:

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



Wenn der Endpunkt für den CloudMirror-Replikationsdienst verwendet wird, schließen Sie den Bucket-Namen nicht in die URI ein. Sie geben 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 mehr ändern, nachdem der Endpunkt erstellt wurde.

6. Wählen Sie **Weiter**.

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

Suchintegrationsendpunkte

Geben Sie die Anmeldeinformationen für einen Suchintegrationsendpunkt ein oder laden Sie sie hoch.

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

Authentifizierungstyp	Beschreibung	Anmeldeinformationen
Anonym	Bietet anonymen Zugriff auf das Ziel. Funktioniert nur für Endpunkte, bei denen die Sicherheit deaktiviert ist.	Keine Authentifizierung.
Zugriffsschlüssel	Verwendet Anmeldeinformationen im AWS-Stil, um Verbindungen mit dem Ziel zu authentifizieren.	<ul style="list-style-type: none">• Zugriffsschlüssel-ID• Geheimer Zugriffsschlüssel
Grundlegendes HTTP	Verwendet einen Benutzernamen und ein Kennwort, um Verbindungen zum Ziel zu authentifizieren.	<ul style="list-style-type: none">• Benutzername• Passwort

CloudMirror-Replikationsendpunkte

Geben Sie die Anmeldeinformationen für einen CloudMirror-Replikationsendpunkt ein oder laden Sie sie hoch.

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

Authentifizierungstyp	Beschreibung	Anmeldeinformationen
Anonym	Bietet anonymen Zugriff auf das Ziel. Funktioniert nur für Endpunkte, bei denen die Sicherheit deaktiviert ist.	Keine Authentifizierung.
Zugriffsschlüssel	Verwendet Anmeldeinformationen im AWS-Stil, um Verbindungen mit dem Ziel zu authentifizieren.	<ul style="list-style-type: none">• Zugriffsschlüssel-ID• Geheimer Zugriffsschlüssel

Authentifizierungstyp	Beschreibung	Anmeldeinformationen
CAP (C2S-Zugangsportal)	Verwendet Zertifikate und Schlüssel, um Verbindungen zum Ziel zu authentifizieren.	<ul style="list-style-type: none"> • URL für temporäre Anmeldeinformationen • Server-CA-Zertifikat (PEM-Datei-Upload) • Client-Zertifikat (PEM-Datei-Upload) • Privater Clientschlüssel (PEM-Dateiupload, verschlüsseltes OpenSSL-Format oder unverschlüsseltes privates Schlüsselformat) • Passphrase für den privaten Clientschlüssel (optional)

Amazon SNS-Endpunkte

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

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

Authentifizierungstyp	Beschreibung	Anmeldeinformationen
Anonym	Bietet anonymen Zugriff auf das Ziel. Funktioniert nur für Endpunkte, bei denen die Sicherheit deaktiviert ist.	Keine Authentifizierung.
Zugriffsschlüssel	Verwendet Anmeldeinformationen im AWS-Stil, um Verbindungen mit dem Ziel zu authentifizieren.	<ul style="list-style-type: none"> • Zugriffsschlüssel-ID • Geheimer Zugriffsschlüssel

Kafka-Endpunkte

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

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

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

Authentifizierungstyp	Beschreibung	Anmeldeinformationen
SASL/PLAIN	Verwendet einen Benutzernamen und ein Kennwort im Klartext, um Verbindungen zum Ziel zu authentifizieren.	<ul style="list-style-type: none"> • Benutzername • Passwort
SASL/SCRAM-SHA-256	Verwendet einen Benutzernamen und ein Kennwort unter Verwendung eines Challenge-Response-Protokolls und SHA-256-Hashing, um Verbindungen zum Ziel zu authentifizieren.	<ul style="list-style-type: none"> • Benutzername • Passwort
SASL/SCRAM-SHA-512	Verwendet einen Benutzernamen und ein Kennwort unter Verwendung eines Challenge-Response-Protokolls und SHA-512-Hashing, um Verbindungen zum Ziel zu authentifizieren.	<ul style="list-style-type: none"> • Benutzername • Passwort

Wählen Sie **Authentifizierung über Delegation verwenden**, wenn Benutzername und Kennwort von einem Delegationstoken abgeleitet sind, das von einem Kafka-Cluster abgerufen wurde.

8. Wählen Sie **Weiter**.

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

Art der Zertifikatsprüfung	Beschreibung
Benutzerdefiniertes CA-Zertifikat verwenden	Verwenden Sie ein benutzerdefiniertes Sicherheitszertifikat. Wenn Sie diese Einstellung auswählen, kopieren Sie das benutzerdefinierte Sicherheitszertifikat und fügen Sie es in das Textfeld CA-Zertifikat ein.
CA-Zertifikat des Betriebssystems verwenden	Verwenden Sie das auf dem Betriebssystem installierte Standard-Grid-CA-Zertifikat, um Verbindungen zu sichern.
Zertifikat nicht überprüfen	Das für die TLS-Verbindung verwendete Zertifikat wird nicht überprüft. Diese Option ist nicht sicher.

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

- Wenn der Endpunkt mit den angegebenen Anmeldeinformationen erreicht werden kann, wird eine Erfolgsmeldung angezeigt. Die Verbindung zum Endpunkt wird von einem Knoten an jedem Standort validiert.
- Wenn die Endpunktvalidierung fehlschlägt, wird eine Fehlermeldung angezeigt. Wenn Sie den Endpunkt ändern müssen, um den Fehler zu beheben, wählen Sie **Zurück zu den Endpunktdetails** und aktualisieren Sie die Informationen. Wählen Sie dann **Testen und Endpunkt erstellen**.



Die Endpunktterstellung schlägt fehl, wenn Plattformdienste für Ihr Mandantenkonto nicht aktiviert sind. Wenden Sie sich an Ihren StorageGRID Administrator.

Nachdem Sie einen Endpunkt konfiguriert haben, können Sie dessen URN verwenden, um einen Plattformdienst zu konfigurieren.

Ähnliche Informationen

- ["Geben Sie die URN für den Plattformdienst-Endpunkt an"](#)
- ["Konfigurieren der CloudMirror-Replikation"](#)
- ["Konfigurieren von Ereignisbenachrichtigungen"](#)
- ["Suchintegrationsdienst konfigurieren"](#)

Testen Sie die Verbindung für den Plattformdienst-Endpunkt

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

Bevor Sie beginnen

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

Informationen zu diesem Vorgang

StorageGRID überprüft nicht, ob die Anmeldeinformationen über die richtigen Berechtigungen verfügen.

Schritte

1. Wählen Sie **STORAGE (S3) > Plattformdienst-Endpunkte**.

Die Seite „Plattformdienst-Endpunkte“ wird angezeigt und zeigt die Liste der bereits konfigurierten Plattformdienst-Endpunkte.

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

Die Seite mit den Endpunktdetails wird angezeigt.

3. Wählen Sie **Verbindung testen**.

- Wenn der Endpunkt mit den angegebenen Anmeldeinformationen erreicht werden kann, wird eine Erfolgsmeldung angezeigt. Die Verbindung zum Endpunkt wird von einem Knoten an jedem Standort validiert.
- Wenn die Endpunktvalidierung 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 dann **Testen und Änderungen speichern**.

Plattformdienst-Endpunkt bearbeiten

Sie können die Konfiguration für einen Plattformdienst-Endpunkt bearbeiten, um dessen Namen, URI oder andere Details zu ändern. Beispielsweise müssen Sie möglicherweise abgelaufene Anmeldeinformationen aktualisieren oder die URI ändern, damit sie für das

Failover auf einen Backup-Elasticsearch-Index verweist. Sie können die URN für einen Plattformdienst-Endpunkt nicht ändern.

Bevor Sie beginnen

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

Schritte

1. Wählen Sie **STORAGE (S3) > Plattformdienst-Endpunkte.**

Die Seite „Plattformdienst-Endpunkte“ wird angezeigt und zeigt die Liste der bereits konfigurierten Plattformdienst-Endpunkte.

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

Die Seite mit den Endpunktdetails wird angezeigt.

3. Wählen Sie **Konfiguration.**

4. Ändern Sie bei Bedarf die Konfiguration des Endpunkts.



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

a. Um den Anzeigenamen für den Endpunkt zu ändern, wählen Sie das Bearbeitungssymbol .

b. Ändern Sie die URI nach Bedarf.

c. Ändern Sie bei Bedarf den Authentifizierungstyp.

- Ändern Sie für die Zugriffsschlüsselauthentifizierung den Schlüssel nach Bedarf, indem Sie **S3-Schlüssel bearbeiten** auswählen und eine neue Zugriffsschlüssel-ID und einen geheimen Zugriffsschlüssel einfügen. Wenn Sie Ihre Änderungen abbrechen müssen, wählen Sie **S3-Schlüsselbearbeitung rückgängig machen**.
- Ändern Sie für die CAP-Authentifizierung (C2S Access Portal) die URL der temporären Anmeldeinformationen oder die optionale Passphrase für den privaten Clientschlüssel und laden Sie bei Bedarf neue Zertifikats- und Schlüsseldateien hoch.



Der private Schlüssel des Clients muss im verschlüsselten OpenSSL-Format oder im unverschlüsselten privaten Schlüsselformat vorliegen.

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

5. Wählen Sie **Testen und Änderungen speichern.**

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

Plattformdienst-Endpunkt löschen

Sie können einen Endpunkt löschen, wenn Sie den zugehörigen Plattformdienst nicht

mehr verwenden möchten.

Bevor Sie beginnen

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

Schritte

1. Wählen Sie **STORAGE (S3) > Plattformdienst-Endpunkte**.

Die Seite „Plattformdienst-Endpunkte“ wird angezeigt und zeigt die Liste der bereits konfigurierten Plattformdienst-Endpunkte.

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



Wenn Sie einen verwendeten Plattformdienst-Endpunkt löschen, wird der zugehörige Plattformdienst für alle Buckets deaktiviert, die den Endpunkt verwenden. Alle noch nicht abgeschlossenen Anfragen werden gelöscht. Alle neuen Anfragen werden weiterhin generiert, bis Sie Ihre Bucket-Konfiguration so ändern, dass sie nicht mehr auf die gelöschte URN verweist. StorageGRID meldet diese Anfragen als nicht behebbare Fehler.

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

Es wird eine Bestätigungsmeldung angezeigt.

4. Wählen Sie **Endpunkt löschen**.

Beheben von Fehlern bei Plattformdienst-Endpunkten

Wenn beim Versuch von StorageGRID, mit einem Plattformdienst-Endpunkt zu kommunizieren, ein Fehler auftritt, wird auf dem Dashboard eine Meldung angezeigt. Auf der Seite „Plattformdienst-Endpunkte“ gibt die Spalte „Letzter Fehler“ an, wie lange der Fehler her ist. Es wird kein Fehler angezeigt, wenn die mit den Anmeldeinformationen eines Endpunkts verknüpften Berechtigungen falsch sind.

Feststellen, ob ein Fehler aufgetreten ist

Wenn innerhalb der letzten 7 Tage Fehler am Endpunkt der Plattformdienste aufgetreten sind, wird im Tenant Manager-Dashboard eine Warnmeldung angezeigt. Weitere Einzelheiten zum Fehler finden Sie auf der Seite „Plattformdienst-Endpunkte“.



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

Derselbe Fehler, der auf dem Dashboard angezeigt wird, erscheint auch oben auf der Seite „Plattformdienst-Endpunkte“. So zeigen Sie eine ausführlichere Fehlermeldung an:

Schritte

1. Wählen Sie aus der Liste der Endpunkte den Endpunkt aus, bei dem der Fehler auftritt.
2. Wählen Sie auf der Seite mit den Endpunktdetails **Verbindung** aus. Auf dieser Registerkarte wird nur der

letzte Fehler für einen Endpunkt angezeigt und es wird angegeben, wie lange der Fehler her ist. Fehler, die das rote X-Symbol enthalten  innerhalb der letzten 7 Tage aufgetreten ist.

Prüfen, ob der Fehler noch aktuell ist

Einige Fehler werden möglicherweise auch nach ihrer Behebung weiterhin in der Spalte **Letzter Fehler** angezeigt. So können Sie feststellen, 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 Endpunktdetails wird angezeigt.

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

Wenn Sie **Verbindung testen** auswählen, überprüft StorageGRID, ob der Endpunkt der Plattformdienste vorhanden ist und mit den aktuellen Anmeldeinformationen erreicht werden kann. Die Verbindung zum Endpunkt wird von einem Knoten an jedem Standort validiert.

Beheben von Endpunktfehlern

Mithilfe der Meldung „Letzter Fehler“ auf der Seite mit den Endpunktdetails können Sie die Fehlerursache ermitteln. Bei einigen Fehlern müssen Sie möglicherweise den Endpunkt bearbeiten, um das Problem zu beheben. Beispielsweise kann ein CloudMirroring-Fehler auftreten, wenn StorageGRID nicht auf den Ziel-S3-Bucket zugreifen kann, weil es nicht über die richtigen Zugriffsberechtigungen verfügt oder der Zugriffsschlüssel abgelaufen ist. Die Meldung lautet: „Entweder müssen die Endpunktanmeldeinformationen oder der Zielzugriff aktualisiert werden“, und die Details lauten „AccessDenied“ oder „InvalidAccessKeyId“.

Wenn Sie den Endpunkt bearbeiten müssen, um einen Fehler zu beheben, führt die Auswahl von **Testen und Änderungen speichern** dazu, dass StorageGRID den aktualisierten Endpunkt validiert und bestätigt, dass er mit den aktuellen Anmeldeinformationen erreicht werden kann. Die Verbindung zum Endpunkt wird von einem Knoten an jedem Standort validiert.

Schritte

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

Endpunktanmeldeinformationen mit unzureichenden Berechtigungen

Wenn StorageGRID einen Plattformdienst-Endpunkt validiert, bestätigt es, dass die Anmeldeinformationen des Endpunkts zum Kontaktieren der Zielressource verwendet werden können, und führt eine grundlegende Berechtigungsprüfung durch. StorageGRID validiert jedoch nicht alle Berechtigungen, die für bestimmte Vorgänge der Plattformdienste erforderlich sind. Wenn Sie beim Versuch, einen Plattformdienst zu verwenden, eine Fehlermeldung erhalten (z. B. „403 Forbidden“), überprüfen Sie daher die mit den Anmeldeinformationen des Endpunkts verknüpften Berechtigungen.

Ähnliche Informationen

- [StorageGRID verwalten > Fehlerbehebung bei Plattformdiensten](#)

- "Plattformdienst-Endpunkt erstellen"
- "Testen Sie die Verbindung für den Plattformdienst-Endpunkt"
- "Plattformdienst-Endpunkt bearbeiten"

Konfigurieren der CloudMirror-Replikation

Um die CloudMirror-Replikation für einen Bucket zu aktivieren, erstellen und wenden Sie eine gültige XML-Konfiguration für die Bucket-Replikation an.

Bevor Sie beginnen

- Die Plattformdienste wurden von einem StorageGRID Administrator für Ihr Mandantenkonto 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 verfügen über seine URN.
- Sie gehören einer Benutzergruppe an, die über die "["Verwalten Sie alle Buckets oder Root-Zugriffsberechtigungen"](#)". Diese Berechtigungen überschreiben die Berechtigungseinstellungen in Gruppen- oder Bucket-Richtlinien, wenn der Bucket mit dem Tenant Manager konfiguriert wird.

Informationen zu diesem Vorgang

Die CloudMirror-Replikation kopiert Objekte aus einem Quell-Bucket in einen Ziel-Bucket, der in einem Endpunkt angegeben ist.

Allgemeine Informationen zur Bucket-Replikation und ihrer Konfiguration finden Sie unter "["Amazon Simple Storage Service \(S3\)-Dokumentation: Objekte replizieren"](#)". Informationen zur Implementierung von GetBucketReplication, DeleteBucketReplication und PutBucketReplication StorageGRID finden Sie im "["Operationen an Buckets"](#)".

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

Beachten Sie beim Konfigurieren der CloudMirror-Replikation die folgenden Anforderungen und Merkmale:

- Wenn Sie eine gültige XML-Konfiguration für die Bucket-Replikation erstellen und anwenden, muss diese für jedes Ziel die URN eines S3-Bucket-Endpunkts verwenden.
- Die Replikation wird für Quell- oder Ziel-Buckets mit aktiverter S3-Objektsperre nicht unterstützt.
- Wenn Sie die CloudMirror-Replikation für einen Bucket aktivieren, der Objekte enthält, werden dem Bucket neu hinzugefügte Objekte repliziert, die vorhandenen Objekte im Bucket werden jedoch nicht repliziert. Sie müssen vorhandene Objekte aktualisieren, um die Replikation auszulösen.
- Wenn Sie in der XML-Replikationskonfiguration eine Speicherklasse angeben, verwendet StorageGRID diese Klasse beim Ausführen von Vorgängen am Ziel-S3-Endpunkt. Der Zielendpunkt muss auch die angegebene Speicherklasse unterstützen. Befolgen Sie unbedingt alle Empfehlungen des Zielsystemanbieters.

Schritte

1. Aktivieren Sie die Replikation für Ihren Quell-Bucket:

- Verwenden Sie einen Texteditor, um die zum Aktivieren der Replikation erforderliche XML-Replikationskonfiguration zu erstellen, wie in der S3-Replikations-API angegeben.

- Beim Konfigurieren des XML:

- Beachten Sie, dass StorageGRID nur V1 der Replikationskonfiguration unterstützt. Dies bedeutet, dass StorageGRID die Verwendung des `Filter` Element für Regeln und befolgt V1-Konventionen zum Löschen von Objektversionen. Weitere Informationen finden Sie in der Amazon-Dokumentation zur Replikationskonfiguration.
- Verwenden Sie die URN eines S3-Bucket-Endpunkts als Ziel.
- Optional fügen Sie die `<StorageClass>` Element und geben Sie eine der folgenden Optionen an:
 - STANDARD: Die Standardspeicherklasse. Wenn Sie beim Hochladen eines Objekts keine Speicherklasse angeben, STANDARD Speicherklasse wird verwendet.
 - STANDARD_IA: (Standard – seltener Zugriff.) Verwenden Sie diese Speicherklasse für Daten, auf die weniger häufig zugegriffen wird, die aber dennoch bei Bedarf einen schnellen Zugriff erfordern.
 - REDUCED_REDUNDANCY: Verwenden Sie diese Speicherklasse für nicht kritische, reproduzierbare Daten, die mit weniger Redundanz gespeichert werden können als die STANDARD Speicherklasse.
- Wenn Sie eine `Role` im Konfigurations-XML 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 im Dashboard **Buckets anzeigen** oder wählen Sie **STORAGE (S3) > Buckets**.

3. Wählen Sie den Namen des Quell-Buckets aus.

Die Bucket-Detailseite wird angezeigt.

4. Wählen Sie **Plattformdienste > Replikation**.

5. Aktivieren Sie das Kontrollkästchen **Replikation aktivieren**.

6. Fügen Sie die XML-Replikationskonfiguration in das Textfeld ein und wählen Sie **Änderungen speichern**.



Plattformdienste müssen für jedes Mandantenkonto von einem StorageGRID Administrator mithilfe des Grid Managers oder der Grid Management-API aktiviert werden. Wenden Sie sich an Ihren StorageGRID -Administrator, wenn beim Speichern der XML-Konfiguration ein Fehler auftritt.

7. Überprüfen Sie, ob die Replikation richtig konfiguriert ist:

- a. Fügen Sie dem Quell-Bucket ein Objekt hinzu, das die in der Replikationskonfiguration angegebenen Anforderungen für die Replikation erfüllt.

Im zuvor gezeigten Beispiel werden Objekte repliziert, die mit dem Präfix „2020“ übereinstimmen.

- b. Bestätigen Sie, dass das Objekt in den Ziel-Bucket repliziert wurde.

Bei kleinen Objekten erfolgt die Replikation schnell.

Ähnliche Informationen

["Plattformdienst-Endpunkt erstellen"](#)

Konfigurieren von Ereignisbenachrichtigungen

Sie aktivieren Benachrichtigungen für einen Bucket, indem Sie eine XML-Benachrichtigungskonfiguration erstellen und den Tenant Manager verwenden, um die XML auf einen Bucket anzuwenden.

Bevor Sie beginnen

- Die Plattformdienste wurden von einem StorageGRID Administrator für Ihr Mandantenkonto aktiviert.
- Sie haben bereits einen Bucket erstellt, der als Benachrichtigungsquelle dient.
- Der Endpunkt, den Sie als Ziel für Ereignisbenachrichtigungen verwenden möchten, ist bereits vorhanden und Sie verfügen über seine URN.
- Sie gehören einer Benutzergruppe an, die über die ["Verwalten Sie alle Buckets oder Root-Zugriffsberechtigungen"](#). Diese Berechtigungen überschreiben die Berechtigungseinstellungen in Gruppen- oder Bucket-Richtlinien, wenn der Bucket mit dem Tenant Manager konfiguriert wird.

Informationen zu diesem Vorgang

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 Kafka oder Amazon SNS als URN eines Endpunkts angegeben ist.

Allgemeine Informationen zu Ereignisbenachrichtigungen und deren Konfiguration finden Sie im ["Amazon-Dokumentation"](#). Informationen zur Implementierung der S3-Bucket-Benachrichtigungskonfigurations-API durch StorageGRID finden Sie im ["Anweisungen zur Implementierung von S3-Clientanwendungen"](#).

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

- Wenn Sie eine gültige XML-Benachrichtigungskonfiguration erstellen und anwenden, muss für jedes Ziel die URN eines Endpunkts für Ereignisbenachrichtigungen verwendet werden.
- Obwohl die Ereignisbenachrichtigung für einen Bucket mit aktivierter S3-Objektsperre konfiguriert werden kann, werden die S3-Objektsperre-Metadaten (einschließlich „Aufbewahrungsdatum“ und „Legal Hold“-Status) der Objekte nicht in die Benachrichtigungsnachrichten aufgenommen.
- 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 Zielendpunkt verwendete Amazon SNS- oder Kafka-Thema 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. Aktivieren Sie Benachrichtigungen für Ihren Quell-Bucket:

- Verwenden Sie einen Texteditor, um die zum Aktivieren von Ereignisbenachrichtigungen erforderliche XML-Benachrichtigungskonfiguration zu erstellen, wie in der S3-Benachrichtigungs-API angegeben.
- Verwenden Sie beim Konfigurieren des XML die URN eines Endpunkts 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 Mandanten-Manager **STORAGE (S3) > Buckets**.

3. Wählen Sie den Namen des Quell-Buckets aus.

Die Bucket-Detailseite wird angezeigt.

4. Wählen Sie **Plattformdienste > Ereignisbenachrichtigungen**.

5. Aktivieren Sie das Kontrollkästchen **Ereignisbenachrichtigungen aktivieren**.

6. Fügen Sie die XML-Benachrichtigungskonfiguration in das Textfeld ein und wählen Sie **Änderungen speichern**.



Plattformdienste müssen für jedes Mandantenkonto von einem StorageGRID Administrator mithilfe des Grid Managers oder der Grid Management-API aktiviert werden. Wenden Sie sich an Ihren StorageGRID -Administrator, wenn beim Speichern der XML-Konfiguration ein Fehler auftritt.

7. Überprüfen Sie, ob die Ereignisbenachrichtigungen richtig konfiguriert sind:

- Führen Sie eine Aktion für ein Objekt im Quell-Bucket aus, das die Anforderungen zum Auslösen einer Benachrichtigung erfüllt, wie in der Konfigurations-XML konfiguriert.

Im Beispiel wird eine Ereignisbenachrichtigung gesendet, wenn ein Objekt mit dem `images/` Präfix.

- b. Bestätigen Sie, dass eine Benachrichtigung an das Zielthema Amazon SNS oder Kafka übermittelt wurde.

Wenn Ihr Zielthema beispielsweise auf Amazon SNS gehostet wird, können Sie den Dienst so konfigurieren, dass er Ihnen eine E-Mail sendet, wenn die Benachrichtigung zugestellt wird.

```
{  
  "Records": [  
    {  
      "eventVersion": "2.0",  
      "eventSource": "sgws:s3",  
      "eventTime": "2017-08-08T23:52:38Z",  
      "eventName": "ObjectCreated:Put",  
      "userIdentity": {  
        "principalId": "11111111111111111111"  
      },  
      "requestParameters": {  
        "sourceIPAddress": "193.51.100.20"  
      },  
      "responseElements": {  
        "x-amz-request-id": "122047343"  
      },  
      "s3": {  
        "s3SchemaVersion": "1.0",  
        "configurationId": "Image-created",  
        "bucket": {  
          "name": "test1",  
          "ownerIdentity": {  
            "principalId": "11111111111111111111"  
          },  
          "arn": "arn:sgws:s3:::test1"  
        },  
        "object": {  
          "key": "images/cat.jpg",  
          "size": 0,  
          "eTag": "d41d8cd98f00b204e9800998ecf8427e",  
          "sequencer": "14D90402421461C7"  
        }  
      }  
    }  
  ]  
}
```

+

Wenn die Benachrichtigung beim Zielthema empfangen wird, haben Sie Ihren Quell-Bucket erfolgreich für StorageGRID -Benachrichtigungen konfiguriert.

Ähnliche Informationen

["Benachrichtigungen für Buckets verstehen"](#)

["Verwenden Sie die S3 REST-API"](#)

["Plattformdienst-Endpunkt erstellen"](#)

Konfigurieren des Suchintegrationsdienstes

Sie aktivieren die Suchintegration für einen Bucket, indem Sie XML für die Suchintegration erstellen und den Tenant Manager verwenden, um das XML auf den Bucket anzuwenden.

Bevor Sie beginnen

- Die Plattformdienste wurden von einem StorageGRID Administrator für Ihr Mandantenkonto 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 verfügen über seine URN.
- Sie gehören einer Benutzergruppe an, die über die ["Verwalten Sie alle Buckets oder Root-Zugriffsberechtigungen"](#). Diese Berechtigungen überschreiben die Berechtigungseinstellungen in Gruppen- oder Bucket-Richtlinien, wenn der Bucket mit dem Tenant Manager konfiguriert wird.

Informationen zu diesem Vorgang

Nachdem Sie den Suchintegrationsdienst für einen Quell-Bucket konfiguriert haben, löst das Erstellen eines Objekts oder das Aktualisieren der Metadaten oder Tags eines Objekts das Senden von Objektmetadaten an den Zielpunkt aus.

Wenn Sie den Suchintegrationsdienst für einen Bucket aktivieren, der bereits Objekte enthält, werden für vorhandene Objekte nicht automatisch Metadatenbenachrichtigungen gesendet. Aktualisieren Sie diese vorhandenen Objekte, um sicherzustellen, dass ihre Metadaten zum Zielsuchindex hinzugefügt werden.

Schritte

1. Aktivieren Sie die Suchintegration für einen Bucket:

- Verwenden Sie einen Texteditor, um die XML-Metadatenbenachrichtigung zu erstellen, die zum Aktivieren der Suchintegration erforderlich ist.
- Verwenden Sie beim Konfigurieren des XML die URN eines Suchintegrationsendpunkts als Ziel.

Objekte können nach dem Präfix des Objektnamens gefiltert werden. Beispielsweise könnten Sie Metadaten für Objekte mit dem Präfix `images` zu einem Ziel und Metadaten für Objekte mit dem Präfix `videos` zu einem anderen. Konfigurationen mit überlappenden Präfixen sind ungültig und werden bei der Übermittlung abgelehnt. Beispielsweise eine Konfiguration, die eine Regel für Objekte mit dem Präfix `test` und eine zweite Regel für Objekte mit dem Präfix `test2` ist nicht erlaubt.

Bei Bedarf finden Sie weitere Informationen im [Beispiele für die Metadatenkonfigurations-XML](#).

```

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

```

Elemente in der XML-Konfiguration der Metadatenbenachrichtigung:

Name	Beschreibung	Erforderlich
Metadatenbenachrichtigungskonfiguration	<p>Container-Tag für Regeln, die zum Angeben der Objekte und des Ziels für Metadatenbenachrichtigungen verwendet werden.</p> <p>Enthält ein oder mehrere Regelemente.</p>	Ja
Regel	<p>Container-Tag für eine Regel, die die Objekte identifiziert, deren Metadaten einem angegebenen Index hinzugefügt werden sollen.</p> <p>Regeln mit überlappenden Präfixen werden abgelehnt.</p> <p>Im MetadataNotificationConfiguration-Element enthalten.</p>	Ja
AUSWEIS	<p>Eindeutige Kennung für die Regel.</p> <p>Im Regelement enthalten.</p>	Nein
Status	<p>Der Status kann „Aktiviert“ oder „Deaktiviert“ sein. Für deaktivierte Regeln werden keine Maßnahmen ergriffen.</p> <p>Im Regelement enthalten.</p>	Ja
Präfix	<p>Objekte, die dem Präfix entsprechen, sind von der Regel betroffen und ihre Metadaten werden an das angegebene Ziel gesendet.</p> <p>Um alle Objekte abzulegen, geben Sie ein leeres Präfix an.</p> <p>Im Regelement enthalten.</p>	Ja
Ziel	<p>Container-Tag für das Ziel einer Regel.</p> <p>Im Regelement enthalten.</p>	Ja

Name	Beschreibung	Erforderlich
Urne	<p>URN des Ziels, an das die Objektmetadaten gesendet werden. Muss die URN eines StorageGRID -Endpunkts mit den folgenden Eigenschaften sein:</p> <ul style="list-style-type: none"> • `es` muss das dritte Element sein. • Die URN muss mit dem Index und Typ enden, in dem die Metadaten gespeichert sind, in der Form domain-name/myindex/mytype . <p>Endpunkte werden mithilfe des Tenant Managers oder der Tenant Management API konfiguriert. Sie haben folgende Form:</p> <ul style="list-style-type: none"> • arn:aws:es:region:account-ID:domain/mydomain/myindex/mytype • urn:mysite:es:::mydomain/myindex/mytype <p>Der Endpunkt muss konfiguriert werden, bevor die Konfigurations-XML übermittelt wird, andernfalls schlägt die Konfiguration mit einem 404-Fehler fehl.</p> <p>URN ist im Zielelement enthalten.</p>	Ja

2. Wählen Sie im Tenant Manager **STORAGE (S3) > Buckets**.

3. Wählen Sie den Namen des Quell-Buckets aus.

Die Bucket-Detailseite wird angezeigt.

4. Wählen Sie **Plattformdienste > Suchintegration**

5. Aktivieren Sie das Kontrollkästchen **Suchintegration aktivieren**.

6. Fügen Sie die Metadaten-Benachrichtigungskonfiguration in das Textfeld ein und wählen Sie **Änderungen speichern**.



Plattformdienste müssen für jedes Mandantenkonto von einem StorageGRID Administrator mithilfe des Grid Managers oder der Management-API aktiviert werden. Wenden Sie sich an Ihren StorageGRID -Administrator, wenn beim Speichern der XML-Konfiguration ein Fehler auftritt.

7. Überprüfen Sie, ob der Suchintegrationsdienst richtig konfiguriert ist:

a. Fügen Sie dem Quell-Bucket ein Objekt hinzu, das die Anforderungen zum Auslösen einer Metadatenbenachrichtigung erfüllt, wie im Konfigurations-XML angegeben.

Im zuvor gezeigten Beispiel lösen alle zum Bucket hinzugefügten Objekte eine Metadatenbenachrichtigung aus.

b. Bestätigen Sie, dass dem im Endpunkt angegebenen Suchindex ein JSON-Dokument hinzugefügt wurde, das die Metadaten und Tags des Objekts enthält.

Nach Abschluss

Bei Bedarf können Sie die Suchintegration für einen Bucket mit einer der folgenden Methoden deaktivieren:

- Wählen Sie **STORAGE (S3) > Buckets** und deaktivieren Sie das Kontrollkästchen **Suchintegration aktivieren**.
- Wenn Sie die S3-API direkt verwenden, verwenden Sie eine Benachrichtigungsanforderung zum Löschen von Bucket-Metadaten. Siehe die Anweisungen zum Implementieren von S3-Clientanwendungen.

Beispiel: Metadaten-Benachrichtigungskonfiguration, 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 verwendet, die mit dem Präfix `/images` wird an ein Ziel gesendet, während Objektmetadaten für Objekte, die dem Präfix entsprechen `/videos` wird an ein zweites Ziel gesendet.

```

<MetadataNotificationConfiguration>
  <Rule>
    <ID>Images-rule</ID>
    <Status>Enabled</Status>
    <Prefix>/images</Prefix>
    <Destination>
      <Urn>arn:aws:es:us-east-1:3333333:domain/es-
domain/graphics/imagetype</Urn>
    </Destination>
  </Rule>
  <Rule>
    <ID>Videos-rule</ID>
    <Status>Enabled</Status>
    <Prefix>/videos</Prefix>
    <Destination>
      <Urn>arn:aws:es:us-west-1:2222222:domain/es-
domain/graphics/videotype</Urn>
    </Destination>
  </Rule>
</MetadataNotificationConfiguration>

```

Metadaten-Benachrichtigungsformat

Wenn Sie den Suchintegrationsdienst für einen Bucket aktivieren, wird jedes Mal, wenn Objektmetadaten oder Tags hinzugefügt, aktualisiert oder gelöscht werden, ein JSON-Dokument generiert und an den Zielpunkt gesendet.

Dieses Beispiel zeigt ein Beispiel des JSON, das generiert werden könnte, wenn ein Objekt mit dem Schlüssel SGWS/Tagging.txt wird in einem Bucket namens erstellt test. Der test Bucket ist nicht versioniert, also die `versionId`-Tag ist leer.

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

Im JSON-Dokument enthaltene Felder

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

Bucket- und Objektinformationen

bucket: Name des Buckets

key: Objektschlüsselname

versionID: Objektversion, für Objekte in versionierten Buckets

region: Bucket-Bereich, zum Beispiel us-east-1

Systemmetadaten

size: Objektgröße (in Bytes), wie sie für einen HTTP-Client sichtbar ist

md5: Objekt-Hash

Benutzermetadaten

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

key:value

Schlagwörter

tags: Alle für das Objekt definierten Objekt-Tags als Schlüssel-Wert-Paare

key:value

So zeigen Sie Ergebnisse in Elasticsearch an

Für Tags und Benutzermetadaten übergibt StorageGRID Daten und Zahlen als Zeichenfolgen oder als S3-Ereignisbenachrichtigungen an Elasticsearch. Um Elasticsearch so zu konfigurieren, dass diese Zeichenfolgen

als Datumsangaben oder Zahlen interpretiert werden, befolgen Sie die Elasticsearch-Anweisungen zur dynamischen Feldzuordnung und zur Zuordnung von Datumsformaten. Aktivieren Sie die dynamischen Feldzuordnungen im Index, bevor Sie den Suchintegrationsdienst konfigurieren. Nachdem ein Dokument indiziert wurde, können Sie die Feldtypen des Dokuments im Index nicht mehr bearbeiten.

Verwenden Sie die S3 REST-API

Unterstützte Versionen und Updates der S3 REST API

StorageGRID unterstützt die Simple Storage Service (S3)-API, die als Satz von Representational State Transfer (REST)-Webdiensten implementiert ist.

Durch die Unterstützung der S3 REST API können Sie serviceorientierte Anwendungen, die für S3-Webdienste entwickelt wurden, mit lokalem Objektspeicher verbinden, der das StorageGRID -System verwendet. Es sind nur minimale Änderungen an der aktuellen Verwendung von S3 REST-API-Aufrufen durch eine Clientanwendung erforderlich.

Unterstützte Versionen

StorageGRID unterstützt die folgenden spezifischen Versionen von S3 und HTTP.

Artikel	Version
S3-API-Spezifikation	"Amazon Web Services (AWS)-Dokumentation: Amazon Simple Storage Service API-Referenz"
HTTP	<p>1,1</p> <p>Weitere Informationen zu HTTP finden Sie unter HTTP/1.1 (RFCs 7230-35).</p> <p>"IETF RFC 2616: Hypertext Transfer Protocol (HTTP/1.1)"</p> <p>Hinweis: StorageGRID unterstützt kein HTTP/1.1-Pipelining.</p>

Aktualisierungen der S3 REST API-Unterstützung

Freigeben	Kommentare
11,9	<ul style="list-style-type: none"> • Unterstützung für vorberechnete SHA-256-Prüfsummenwerte für die folgenden Anfragen und unterstützten Header hinzugefügt. Mit dieser Funktion können Sie die Integrität hochgeladener Objekte überprüfen: <ul style="list-style-type: none"> ◦ CompleteMultipartUpload: x-amz-checksum-sha256 ◦ CreateMultipartUpload: x-amz-checksum-algorithm ◦ GetObject: x-amz-checksum-mode ◦ Kopfobjekt: x-amz-checksum-mode ◦ Teileliste ◦ PutObject: x-amz-checksum-sha256 ◦ UploadPart: x-amz-checksum-sha256 • Dem Grid-Administrator wurde die Möglichkeit hinzugefügt, die Aufbewahrungs- und Compliance-Einstellungen auf Mandantenebene zu steuern. Diese Einstellungen wirken sich auf die S3 Object Lock-Einstellungen aus. <ul style="list-style-type: none"> ◦ Standardaufbewahrungsmodus für Buckets und Objektaufbewahrungsmodus: Governance oder Compliance, sofern vom Grid-Administrator zugelassen. ◦ Standardaufbewahrungszeitraum des Buckets und Aufbewahrungsdatum des Objekts: Muss kleiner oder gleich dem zulässigen maximalen Aufbewahrungszeitraum sein, der vom Grid-Administrator festgelegt wurde. • Verbesserte Unterstützung für aws-chunked Inhaltskodierung und Streaming x-amz-content-sha256 Werte. Einschränkungen: <ul style="list-style-type: none"> ◦ Falls vorhanden, chunk-signature ist optional und nicht validiert ◦ Falls vorhanden, x-amz-trailer Inhalt wird ignoriert
11,8	<p>Die Namen der S3-Operationen wurden aktualisiert, damit sie mit den Namen übereinstimmen, die in der "Amazon Web Services (AWS)-Dokumentation: Amazon Simple Storage Service API-Referenz" .</p>
11,7	<ul style="list-style-type: none"> • Hinzugefügt "Kurzreferenz: Unterstützte S3-API-Anfragen" . • Unterstützung für die Verwendung des GOVERNANCE-Modus mit S3 Object Lock hinzugefügt. • Unterstützung für das StorageGRID-spezifische x-ntap-sg-cgr-replication-status Antwortheader für GET Object- und HEAD Object-Anfragen. Dieser Header gibt den Replikationsstatus eines Objekts für die Cross-Grid-Replikation an. • SelectObjectContent-Anfragen unterstützen jetzt Parquet-Objekte.

Freigeben	Kommentare
11,6	<ul style="list-style-type: none"> Unterstützung für die Verwendung von hinzugefügten <code>partNumber</code> Anforderungsparametern in GET-Objekt- und HEAD-Objektanforderungen. Unterstützung für einen Standardaufbewahrungsmodus und eine Standardaufbewahrungszeitdauer auf Bucket-Ebene für S3 Object Lock hinzugefügt. Zusätzliche Unterstützung für die <code>s3:object-lock-remaining-retention-days</code> Richtlinienbedingungsschlüssel, um den Bereich der zulässigen Aufbewahrungszeiträume für Ihre Objekte festzulegen. Die maximal <i>empfohlene</i> Größe für einen einzelnen PUT-Objektvorgang wurde auf 5 GiB (5.368.709.120 Bytes) geändert. Wenn Sie Objekte haben, die größer als 5 GiB sind, verwenden Sie stattdessen den mehrteiligen Upload.
11,5	<ul style="list-style-type: none"> Unterstützung für die Verwaltung der Bucket-Verschlüsselung hinzugefügt. Unterstützung für S3 Object Lock und veraltete Compliance-Anfragen hinzugefügt. Unterstützung für die Verwendung von DELETE Multiple Objects bei versionierten Buckets hinzugefügt. Der <code>Content-MD5</code> Anforderungsheader wird jetzt korrekt unterstützt.
11,4	<ul style="list-style-type: none"> Unterstützung für DELETE-Bucket-Tagging, GET-Bucket-Tagging und PUT-Bucket-Tagging hinzugefügt. Kostenzuordnungs-Tags werden nicht unterstützt. Für in StorageGRID 11.4 erstellte Buckets ist die Einschränkung von Objektschlüsselnamen zur Einhaltung der Best Practices für die Leistung nicht mehr erforderlich. Unterstützung für Bucket-Benachrichtigungen hinzugefügt auf der <code>s3:ObjectRestore:Post</code> Ereignistyp. AWS-Größenbeschränkungen für mehrteilige Teile werden jetzt erzwungen. Jeder Teil eines mehrteiligen Uploads muss zwischen 5 MiB und 5 GiB groß sein. Der letzte Teil kann kleiner als 5 MiB sein. Unterstützung für TLS 1.3 hinzugefügt
11,3	<ul style="list-style-type: none"> Unterstützung für die serverseitige Verschlüsselung von Objektdaten mit vom Kunden bereitgestellten Schlüsseln (SSE-C) hinzugefügt. Unterstützung für DELETE-, GET- und PUT-Bucket-Lebenszyklusoperationen (nur Ablaufaktion) und für die <code>x-amz-expiration</code> Antwortheader. PUT-Objekt, PUT-Objekt – Kopieren und mehrteiliger Upload aktualisiert, um die Auswirkungen von ILM-Regeln zu beschreiben, die eine synchrone Platzierung bei der Aufnahme verwenden. TLS 1.1-Chiffren werden nicht mehr unterstützt.

Freigeben	Kommentare
11,2	<p>Unterstützung für die POST-Objektwiederherstellung zur Verwendung mit Cloud-Speicherpools hinzugefügt. Unterstützung für die Verwendung der AWS-Syntax für ARN, Richtlinienbedingungsschlüssel und Richtlinienvariablen in Gruppen- und Bucket-Richtlinien hinzugefügt. Vorhandene Gruppen- und Bucket-Richtlinien, die die StorageGRID Syntax verwenden, werden weiterhin unterstützt.</p> <p>Hinweis: Die Verwendung von ARN/URN in anderen JSON/XML-Konfigurationen, einschließlich der in benutzerdefinierten StorageGRID -Funktionen verwendeten, hat sich nicht geändert.</p>
11,1	<p>Unterstützung für Cross-Origin Resource Sharing (CORS), HTTP für S3-Clientverbindungen zu Grid-Knoten und Compliance-Einstellungen für Buckets hinzugefügt.</p>
11,0	<p>Unterstützung für die Konfiguration von Plattformdiensten (CloudMirror-Replikation, Benachrichtigungen und Elasticsearch-Suchintegration) für Buckets hinzugefügt. Außerdem wurde Unterstützung für die Objektmarkierung, Standortbeschränkungen für Buckets und die verfügbare Konsistenz hinzugefügt.</p>
10,4	<p>Unterstützung für ILM-Scan-Änderungen an der Versionierung, Aktualisierungen der Seite „Endpoint Domain Names“, Bedingungen und Variablen in Richtlinien, Richtlinienbeispielen und der Berechtigung „PutOverwriteObject“ hinzugefügt.</p>
10,3	<p>Unterstützung für Versionierung hinzugefügt.</p>
10,2	<p>Unterstützung für Gruppen- und Bucket-Zugriffsrichtlinien sowie für mehrteilige Kopien (Upload-Teil – Kopie) hinzugefügt.</p>
10,1	<p>Unterstützung für mehrteilige Uploads, Anfragen im virtuellen gehosteten Stil und v4-Authentifizierung hinzugefügt.</p>
10,0	<p>Erste Unterstützung der S3 REST API durch das StorageGRID -System. Die aktuell unterstützte Version der <i>Simple Storage Service API Reference</i> ist der 01.03.2006.</p>

Kurzreferenz: Unterstützte S3-API-Anfragen

Auf dieser Seite wird zusammengefasst, wie StorageGRID die APIs des Amazon Simple Storage Service (S3) unterstützt.

Diese Seite enthält nur die S3-Operationen, die von StorageGRID unterstützt werden.



Um die AWS-Dokumentation für jeden Vorgang anzuzeigen, wählen Sie den Link in der Überschrift aus.

Allgemeine URI-Abfrageparameter und Anforderungsheader

Sofern nicht anders angegeben, werden die folgenden allgemeinen URI-Abfrageparameter unterstützt:

- `versionId`(wie für Objektoperationen erforderlich)

Sofern nicht anders angegeben, werden die folgenden allgemeinen Anforderungsheader unterstützt:

- `Authorization`
- `Connection`
- `Content-Length`
- `Content-MD5`
- `Content-Type`
- `Date`
- `Expect`
- `Host`
- `x-amz-date`

Ähnliche Informationen

- ["Details zur S3 REST API-Implementierung"](#)
- ["Amazon Simple Storage Service API-Referenz: Allgemeine Anforderungsheader"](#)

"AbortMultipartUpload"

URI-Abfrageparameter und Anforderungsheader

StorageGRID unterstützt alle [allgemeine Parameter und Header](#) für diese Anfrage, plus diesen zusätzlichen URI-Abfrageparameter:

- `uploadId`

Anforderungstext

Keine

StorageGRID -Dokumentation

["Vorgänge für mehrteilige Uploads"](#)

"CompleteMultipartUpload"

URI-Abfrageparameter und Anforderungsheader

StorageGRID unterstützt alle [allgemeine Parameter und Header](#) für diese Anfrage, plus diesen zusätzlichen URI-Abfrageparameter:

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

XML-Tags des Anforderungstexts

StorageGRID unterstützt die folgenden XML-Tags im Anforderungstext:

- `ChecksumSHA256`
- `CompleteMultipartUpload`

- ETag
- Part
- PartNumber

StorageGRID -Dokumentation

["CompleteMultipartUpload"](#)

"Objekt kopieren"

URI-Abfrageparameter und Anforderungsheader

StorageGRID unterstützt alle [allgemeine Parameter und Header](#) für diese Anfrage, plus diese zusätzlichen Header:

- 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>

Anforderungstext

Keine

StorageGRID -Dokumentation

["Objekt kopieren"](#)

"Bucket erstellen"

URI-Abfrageparameter und Anforderungsheader

StorageGRID unterstützt alle [allgemeine Parameter und Header](#) für diese Anfrage, plus diese zusätzlichen Header:

- x-amz-bucket-object-lock-enabled

Anforderungstext

StorageGRID unterstützt alle Anforderungstextparameter, die zum Zeitpunkt der Implementierung von der Amazon S3 REST-API definiert wurden.

StorageGRID -Dokumentation

["Operationen an Buckets"](#)

"CreateMultipartUpload"

URI-Abfrageparameter und Anforderungsheader

StorageGRID unterstützt alle [allgemeine Parameter und Header](#) für diese Anfrage, plus diese zusätzlichen Header:

- 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>

Anforderungstext

Keine

StorageGRID -Dokumentation

["CreateMultipartUpload"](#)

"Bucket löschen"

URI-Abfrageparameter und Anforderungsheader

StorageGRID unterstützt alle [allgemeine Parameter und Header](#) für diese Anfrage.

StorageGRID -Dokumentation

["Operationen an Buckets"](#)

"BucketCors löschen"

URI-Abfrageparameter und Anforderungsheader

StorageGRID unterstützt alle [allgemeine Parameter und Header](#) für diese Anfrage.

Anforderungstext

Keine

StorageGRID -Dokumentation

["Operationen an Buckets"](#)

"DeleteBucketEncryption"

URI-Abfrageparameter und Anforderungsheader

StorageGRID unterstützt alle [allgemeine Parameter und Header](#) für diese Anfrage.

Anforderungstext

Keine

StorageGRID -Dokumentation

["Operationen an Buckets"](#)

"DeleteBucketLifecycle"

URI-Abfrageparameter und Anforderungsheader

StorageGRID unterstützt alle [allgemeine Parameter und Header](#) für diese Anfrage.

Anforderungstext

Keine

StorageGRID -Dokumentation

- ["Operationen an Buckets"](#)
- ["Erstellen einer S3-Lebenszykluskonfiguration"](#)

"DeleteBucketPolicy"

URI-Abfrageparameter und Anforderungsheader

StorageGRID unterstützt alle [allgemeine Parameter und Header](#) für diese Anfrage.

Anforderungstext

Keine

StorageGRID -Dokumentation

["Operationen an Buckets"](#)

["DeleteBucketReplication"](#)

URI-Abfrageparameter und Anforderungsheader

StorageGRID unterstützt alle[allgemeine Parameter und Header](#) für diese Anfrage.

Anforderungstext

Keine

StorageGRID -Dokumentation

["Operationen an Buckets"](#)

["BucketTagging löschen"](#)

URI-Abfrageparameter und Anforderungsheader

StorageGRID unterstützt alle[allgemeine Parameter und Header](#) für diese Anfrage.

Anforderungstext

Keine

StorageGRID -Dokumentation

["Operationen an Buckets"](#)

["Objekt löschen"](#)

URI-Abfrageparameter und Anforderungsheader

StorageGRID unterstützt alle[allgemeine Parameter und Header](#) für diese Anfrage, plus diesen zusätzlichen Anfrageheader:

- x-amz-bypass-governance-retention

Anforderungstext

Keine

StorageGRID -Dokumentation

["Operationen an Objekten"](#)

["Objekte löschen"](#)

URI-Abfrageparameter und Anforderungsheader

StorageGRID unterstützt alle[allgemeine Parameter und Header](#) für diese Anfrage, plus diesen zusätzlichen Anfrageheader:

- x-amz-bypass-governance-retention

Anforderungstext

StorageGRID unterstützt alle Anforderungstextparameter, die zum Zeitpunkt der Implementierung von der Amazon S3 REST-API definiert wurden.

StorageGRID -Dokumentation

["Operationen an Objekten"](#)

["DeleteObjectTagging"](#)

StorageGRID unterstützt alle[allgemeine Parameter und Header](#) für diese Anfrage.

Anforderungstext

Keine

StorageGRID -Dokumentation

["Operationen an Objekten"](#)

["GetBucketAcl"](#)

URI-Abfrageparameter und Anforderungsheader

StorageGRID unterstützt alle[allgemeine Parameter und Header](#) für diese Anfrage.

Anforderungstext

Keine

StorageGRID -Dokumentation

["Operationen an Buckets"](#)

["GetBucketCors"](#)

URI-Abfrageparameter und Anforderungsheader

StorageGRID unterstützt alle[allgemeine Parameter und Header](#) für diese Anfrage.

Anforderungstext

Keine

StorageGRID -Dokumentation

["Operationen an Buckets"](#)

["GetBucketEncryption"](#)

URI-Abfrageparameter und Anforderungsheader

StorageGRID unterstützt alle[allgemeine Parameter und Header](#) für diese Anfrage.

Anforderungstext

Keine

StorageGRID -Dokumentation

["Operationen an Buckets"](#)

["GetBucketLifecycleConfiguration"](#)

URI-Abfrageparameter und Anforderungsheader

StorageGRID unterstützt alle[allgemeine Parameter und Header](#) für diese Anfrage.

Anforderungstext

Keine

StorageGRID -Dokumentation

- "Operationen an Buckets"
- "Erstellen einer S3-Lebenszykluskonfiguration"

"BucketLocation abrufen"

URI-Abfrageparameter und Anforderungsheader

StorageGRID unterstützt alle [allgemeine Parameter und Header](#) für diese Anfrage.

Anforderungstext

Keine

StorageGRID -Dokumentation

["Operationen an Buckets"](#)

"GetBucketNotificationConfiguration"

URI-Abfrageparameter und Anforderungsheader

StorageGRID unterstützt alle [allgemeine Parameter und Header](#) für diese Anfrage.

Anforderungstext

Keine

StorageGRID -Dokumentation

["Operationen an Buckets"](#)

"GetBucketPolicy"

URI-Abfrageparameter und Anforderungsheader

StorageGRID unterstützt alle [allgemeine Parameter und Header](#) für diese Anfrage.

Anforderungstext

Keine

StorageGRID -Dokumentation

["Operationen an Buckets"](#)

"GetBucketReplication"

URI-Abfrageparameter und Anforderungsheader

StorageGRID unterstützt alle [allgemeine Parameter und Header](#) für diese Anfrage.

Anforderungstext

Keine

StorageGRID -Dokumentation

["Operationen an Buckets"](#)

"GetBucketTagging"

URI-Abfrageparameter und Anforderungsheader

StorageGRID unterstützt alle [allgemeine Parameter und Header](#) für diese Anfrage.

Anforderungstext

Keine

StorageGRID -Dokumentation

"Operationen an Buckets"

"GetBucketVersioning"

URI-Abfrageparameter und Anforderungsheader

StorageGRID unterstützt alle [allgemeine Parameter und Header](#) für diese Anfrage.

Anforderungstext

Keine

StorageGRID -Dokumentation

"Operationen an Buckets"

"GetObject"

URI-Abfrageparameter und Anforderungsheader

StorageGRID unterstützt alle [allgemeine Parameter und Header](#) für diese Anfrage, plus diese 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

Anforderungstext

Keine

StorageGRID -Dokumentation

["GetObject"](#)

["GetObjectAcl"](#)

URI-Abfrageparameter und Anforderungsheader

StorageGRID unterstützt alle[allgemeine Parameter und Header](#) für diese Anfrage.

Anforderungstext

Keine

StorageGRID -Dokumentation

["Operationen an Objekten"](#)

["GetObjectLegalHold"](#)

URI-Abfrageparameter und Anforderungsheader

StorageGRID unterstützt alle[allgemeine Parameter und Header](#) für diese Anfrage.

Anforderungstext

Keine

StorageGRID -Dokumentation

["Verwenden Sie die S3 REST API, um S3 Object Lock zu konfigurieren"](#)

["GetObjectLockConfiguration"](#)

URI-Abfrageparameter und Anforderungsheader

StorageGRID unterstützt alle[allgemeine Parameter und Header](#) für diese Anfrage.

Anforderungstext

Keine

StorageGRID -Dokumentation

["Verwenden Sie die S3 REST API, um S3 Object Lock zu konfigurieren"](#)

["GetObjectRetention"](#)

URI-Abfrageparameter und Anforderungsheader

StorageGRID unterstützt alle[allgemeine Parameter und Header](#) für diese Anfrage.

Anforderungstext

Keine

StorageGRID -Dokumentation

["Verwenden Sie die S3 REST API, um S3 Object Lock zu konfigurieren"](#)

"GetObjectTagging"

URI-Abfrageparameter und Anforderungsheader

StorageGRID unterstützt alle [allgemeine Parameter und Header](#) für diese Anfrage.

Anforderungstext

Keine

StorageGRID -Dokumentation

["Operationen an Objekten"](#)

"Kopfeimer"

URI-Abfrageparameter und Anforderungsheader

StorageGRID unterstützt alle [allgemeine Parameter und Header](#) für diese Anfrage.

Anforderungstext

Keine

StorageGRID -Dokumentation

["Operationen an Buckets"](#)

"HeadObject"

URI-Abfrageparameter und Anforderungsheader

StorageGRID unterstützt alle [allgemeine Parameter und Header](#) für diese Anfrage, plus diese zusätzlichen Header:

- 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

Anforderungstext

Keine

StorageGRID -Dokumentation

["HeadObject"](#)

"Buckets auflisten"

URI-Abfrageparameter und Anforderungsheader

StorageGRID unterstützt alle [allgemeine Parameter und Header](#) für diese Anfrage.

Anforderungstext

Keine

StorageGRID -Dokumentation

[Operationen auf dem Dienst](#) › [ListBuckets](#)

"ListMultipartUploads"

URI-Abfrageparameter und Anforderungsheader

StorageGRID unterstützt alle [allgemeine Parameter und Header](#) für diese Anfrage, plus diese zusätzlichen Parameter:

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

Anforderungstext

Keine

StorageGRID -Dokumentation

["ListMultipartUploads"](#)

"ListObjects"

URI-Abfrageparameter und Anforderungsheader

StorageGRID unterstützt alle [allgemeine Parameter und Header](#) für diese Anfrage, plus diese zusätzlichen Parameter:

- delimiter
- encoding-type
- marker
- max-keys
- prefix

Anforderungstext

Keine

StorageGRID -Dokumentation

["Operationen an Buckets"](#)

"ListObjectsV2"

URI-Abfrageparameter und Anforderungsheader

StorageGRID unterstützt alle [allgemeine Parameter und Header](#) für diese Anfrage, plus diese zusätzlichen Parameter:

- continuation-token
- delimiter
- encoding-type
- fetch-owner
- max-keys
- prefix
- start-after

Anforderungstext

Keine

StorageGRID -Dokumentation

["Operationen an Buckets"](#)

"ListObjectVersions"

URI-Abfrageparameter und Anforderungsheader

StorageGRID unterstützt alle [allgemeine Parameter und Header](#) für diese Anfrage, plus diese zusätzlichen Parameter:

- delimiter
- encoding-type
- key-marker
- max-keys
- prefix
- version-id-marker

Anforderungstext

Keine

StorageGRID -Dokumentation

["Operationen an Buckets"](#)

"Teileliste"

URI-Abfrageparameter und Anforderungsheader

StorageGRID unterstützt alle [allgemeine Parameter und Header](#) für diese Anfrage, plus diese zusätzlichen Parameter:

- max-parts

- part-number-marker
- uploadId

Anforderungstext

Keine

StorageGRID -Dokumentation

["ListMultipartUploads"](#)

"PutBucketCors"

URI-Abfrageparameter und Anforderungsheader

StorageGRID unterstützt alle[allgemeine Parameter und Header](#) für diese Anfrage.

Anforderungstext

StorageGRID unterstützt alle Anforderungstextparameter, die zum Zeitpunkt der Implementierung von der Amazon S3 REST-API definiert wurden.

StorageGRID -Dokumentation

["Operationen an Buckets"](#)

"PutBucketEncryption"

URI-Abfrageparameter und Anforderungsheader

StorageGRID unterstützt alle[allgemeine Parameter und Header](#) für diese Anfrage.

XML-Tags des Anforderungstexts

StorageGRID unterstützt die folgenden XML-Tags im Anforderungstext:

- ApplyServerSideEncryptionByDefault
- Rule
- ServerSideEncryptionConfiguration
- SSEAlgorithm

StorageGRID -Dokumentation

["Operationen an Buckets"](#)

"PutBucketLifecycleConfiguration"

URI-Abfrageparameter und Anforderungsheader

StorageGRID unterstützt alle[allgemeine Parameter und Header](#) für diese Anfrage.

XML-Tags des Anforderungstexts

StorageGRID unterstützt die folgenden XML-Tags im Anforderungstext:

- And
- Days
- Expiration

- ExpiredObjectDeleteMarker
- Filter
- ID
- Key
- LifecycleConfiguration
- NewerNoncurrentVersions
- NoncurrentDays
- NoncurrentVersionExpiration
- Prefix
- Rule
- Status
- Tag
- Value

StorageGRID -Dokumentation

- ["Operationen an Buckets"](#)
- ["Erstellen einer S3-Lebenszykluskonfiguration"](#)

"PutBucketNotificationConfiguration"

URI-Abfrageparameter und Anforderungsheader

StorageGRID unterstützt alle [allgemeine Parameter und Header](#) für diese Anfrage.

XML-Tags des Anforderungstexts

StorageGRID unterstützt die folgenden XML-Tags im Anforderungstext:

- Event
- Filter
- FilterRule
- Id
- Name
- NotificationConfiguration
- Prefix
- S3Key
- Suffix
- Topic
- TopicConfiguration
- Value

StorageGRID -Dokumentation

"Operationen an Buckets"

"PutBucketPolicy"

URI-Abfrageparameter und Anforderungsheader

StorageGRID unterstützt alle [allgemeine Parameter und Header](#) für diese Anfrage.

Anforderungstext

Einzelheiten zu den unterstützten JSON-Body-Feldern finden Sie unter ["Verwenden Sie Bucket- und Gruppenzugriffsrichtlinien"](#).

"PutBucketReplication"

URI-Abfrageparameter und Anforderungsheader

StorageGRID unterstützt alle [allgemeine Parameter und Header](#) für diese Anfrage.

XML-Tags des Anforderungstexts

- Bucket
- Destination
- Prefix
- ReplicationConfiguration
- Rule
- Status
- StorageClass

StorageGRID -Dokumentation

"Operationen an Buckets"

"PutBucketTagging"

URI-Abfrageparameter und Anforderungsheader

StorageGRID unterstützt alle [allgemeine Parameter und Header](#) für diese Anfrage.

Anforderungstext

StorageGRID unterstützt alle Anforderungstextparameter, die zum Zeitpunkt der Implementierung von der Amazon S3 REST-API definiert wurden.

StorageGRID -Dokumentation

"Operationen an Buckets"

"PutBucketVersioning"

URI-Abfrageparameter und Anforderungsheader

StorageGRID unterstützt alle [allgemeine Parameter und Header](#) für diese Anfrage.

Anforderungstextparameter

StorageGRID unterstützt die folgenden Anforderungstextparameter:

- VersioningConfiguration

- Status

StorageGRID -Dokumentation

"Operationen an Buckets"

"PutObject"

URI-Abfrageparameter und Anforderungsheader

StorageGRID unterstützt alle [allgemeine Parameter und Header](#) für diese Anfrage, plus diese zusätzlichen Header:

- 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>`

Anforderungstext

- Binärdaten des Objekts

StorageGRID -Dokumentation

"PutObject"

"PutObjectLegalHold"

URI-Abfrageparameter und Anforderungsheader

StorageGRID unterstützt alle [allgemeine Parameter und Header](#) für diese Anfrage.

Anforderungstext

StorageGRID unterstützt alle Anforderungstextparameter, die zum Zeitpunkt der Implementierung von der Amazon S3 REST-API definiert wurden.

StorageGRID -Dokumentation

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

"PutObjectLockConfiguration"

URI-Abfrageparameter und Anforderungsheader

StorageGRID unterstützt alle [allgemeine Parameter und Header](#) für diese Anfrage.

Anforderungstext

StorageGRID unterstützt alle Anforderungstextparameter, die zum Zeitpunkt der Implementierung von der Amazon S3 REST-API definiert wurden.

StorageGRID -Dokumentation

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

"PutObjectRetention"

URI-Abfrageparameter und Anforderungsheader

StorageGRID unterstützt alle [allgemeine Parameter und Header](#) für diese Anfrage, plus diesen zusätzlichen Header:

- x-amz-bypass-governance-retention

Anforderungstext

StorageGRID unterstützt alle Anforderungstextparameter, die zum Zeitpunkt der Implementierung von der Amazon S3 REST-API definiert wurden.

StorageGRID -Dokumentation

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

"PutObjectTagging"

URI-Abfrageparameter und Anforderungsheader

StorageGRID unterstützt alle [allgemeine Parameter und Header](#) für diese Anfrage.

Anforderungstext

StorageGRID unterstützt alle Anforderungstextparameter, die zum Zeitpunkt der Implementierung von der Amazon S3 REST-API definiert wurden.

StorageGRID -Dokumentation

"Operationen an Objekten"

"RestoreObject"

URI-Abfrageparameter und Anforderungsheader

StorageGRID unterstützt alle [allgemeine Parameter und Header](#) für diese Anfrage.

Anforderungstext

Einzelheiten zu den unterstützten Body-Feldern finden Sie unter ["RestoreObject"](#).

["SelectObjectContent"](#)

URI-Abfrageparameter und Anforderungsheader

StorageGRID unterstützt alle [allgemeine Parameter und Header](#) für diese Anfrage.

Anforderungstext

Einzelheiten zu den unterstützten Textfeldern finden Sie hier:

- ["Verwenden Sie S3 Select"](#)
- ["SelectObjectContent"](#)

["UploadPart"](#)

URI-Abfrageparameter und Anforderungsheader

StorageGRID unterstützt alle [allgemeine Parameter und Header](#) für diese Anfrage, plus diese 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

Anforderungstext

- Binärdaten des Teils

StorageGRID -Dokumentation

["UploadPart"](#)

["UploadPartCopy"](#)

URI-Abfrageparameter und Anforderungsheader

StorageGRID unterstützt alle [allgemeine Parameter und Header](#) für diese Anfrage, plus diese 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

Anforderungstext

Keine

StorageGRID -Dokumentation

["UploadPartCopy"](#)

Testen der S3 REST API-Konfiguration

Sie können die Amazon Web Services Command Line Interface (AWS CLI) verwenden, um Ihre Verbindung zum System zu testen und zu überprüfen, ob Sie Objekte lesen und schreiben können.

Bevor Sie beginnen

- Sie haben die AWS CLI von heruntergeladen und installiert ["aws.amazon.com/cli"](#) .
- Optional haben Sie ["einen Load Balancer-Endpunkt erstellt"](#) . Andernfalls kennen Sie die IP-Adresse des Speicherknotens, mit dem Sie eine Verbindung herstellen möchten, und die zu verwendende Portnummer. Sehen ["IP-Adressen und Ports für Clientverbindungen"](#) .
- Du hast ["ein S3-Mandantenkonto erstellt"](#) .
- Sie haben sich beim Mandanten angemeldet und ["einen Zugriffsschlüssel erstellt"](#) .

Einzelheiten zu diesen Schritten finden Sie unter ["Konfigurieren von Clientverbindungen"](#) .

Schritte

1. Konfigurieren Sie die AWS CLI-Einstellungen, um das Konto zu verwenden, das Sie im StorageGRID -System erstellt haben:
 - a. Wechseln Sie in den Konfigurationsmodus: `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 zu verwendende Standardregion ein. Beispiel: `us-east-1` .
 - e. Geben Sie das zu verwendende Standardausgabeformat ein oder drücken Sie die Eingabetaste, um JSON auszuwählen.
2. Erstellen Sie einen Bucket.

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 ist:

```
"Location": "/testbucket"
```

3. Laden Sie ein Objekt hoch.

```
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

Widersprüchliche Clientanforderungen

Widersprüchliche Clientanforderungen, beispielsweise wenn zwei Clients auf denselben Schlüssel schreiben, werden nach dem Prinzip „Latest Wins“ gelöst.

Der Zeitpunkt für die Auswertung der „Latest Wins“ basiert darauf, wann das StorageGRID -System eine bestimmte Anfrage abschließt, und nicht darauf, wann S3-Clients einen Vorgang beginnen.

Konsistenzwerte

Konsistenz sorgt für ein Gleichgewicht zwischen der Verfügbarkeit der Objekte und der Konsistenz dieser Objekte über verschiedene Speicherknoten und Standorte hinweg. Sie können die Konsistenz je nach Anwendungsfall 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. Die Ausbreitung von Überschreibungen dauert im Allgemeinen Sekunden oder Minuten, kann aber bis zu 15 Tage dauern.

Wenn Sie Objektoperationen mit einer anderen Konsistenz durchführen möchten, können Sie:

- Geben Sie eine Konsistenz für [jeder Eimer](#) .
- Geben Sie eine Konsistenz für [jede API-Operation](#) .
- Ändern Sie die standardmäßige rasterweite Konsistenz, indem Sie eine der folgenden Aufgaben ausführen:
 - Gehen Sie im Grid Manager zu **KONFIGURATION > System > Speichereinstellungen > Standardkonsistenz**.
 - .



Eine Änderung der rasterweiten Konsistenz gilt nur für Buckets, die nach der Änderung der Einstellung erstellt wurden. Um die Details einer Änderung zu ermitteln, sehen Sie sich das Audit-Protokoll an unter `/var/local/log` (Suche nach **Konsistenzebene**).

Konsistenzwerte

Die Konsistenz wirkt sich darauf aus, wie die Metadaten, die StorageGRID zum Verfolgen von Objekten verwendet, zwischen Knoten verteilt werden und somit auf 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 die Daten sofort, andernfalls schlägt die Anfrage fehl.
- **Stark global**: Garantiert Lese-nach-Schreib-Konsistenz für alle Clientanforderungen auf allen Sites.
- **Strong-Site**: Garantiert die Lese-nach-Schreib-Konsistenz für alle Clientanforderungen innerhalb einer Site.
- **Lesen nach neuem Schreiben**: (Standard) Bietet Lese-nach-Schreib-Konsistenz für neue Objekte und letztendliche Konsistenz für Objektaktualisierungen. Bietet hohe Verfügbarkeit und Datenschutzgarantien. Für die meisten Fälle empfohlen.
- **Verfügbar**: Bietet letztendliche Konsistenz sowohl für neue Objekte als auch für Objektaktualisierungen. Verwenden Sie es für S3-Buckets nur nach Bedarf (z. B. für einen Bucket, der Protokollwerte enthält, die selten gelesen werden, oder für HEAD- oder GET-Operationen für nicht vorhandene Schlüssel). Wird für S3 FabricPool Buckets nicht unterstützt.

Verwenden Sie die Konsistenz „Lesen nach neuem Schreiben“ und „Verfügbar“.

Wenn ein HEAD- oder GET-Vorgang die Konsistenz „Lesen nach neuem Schreiben“ verwendet, führt StorageGRID die Suche in mehreren Schritten wie folgt durch:

- Es sucht zunächst mit geringer Konsistenz nach dem Objekt.
- Wenn diese Suche fehlschlägt, wird die Suche beim nächsten Konsistenzwert wiederholt, bis eine Konsistenz erreicht wird, die dem Verhalten für „stark global“ entspricht.

Wenn ein HEAD- oder GET-Vorgang die Konsistenz „Lesen nach neuem Schreiben“ verwendet, das Objekt jedoch nicht vorhanden ist, erreicht die Objektsuche immer eine Konsistenz, die dem Verhalten für „Strong-Global“ entspricht. Da für diese Konsistenz mehrere Kopien der Objektmetadaten an jedem Standort verfügbar sein müssen, kann es zu einer hohen Anzahl interner Serverfehler vom Typ 500 kommen, wenn zwei oder mehr Speicherknoten am selben Standort nicht verfügbar sind.

Sofern Sie keine Konsistenzgarantien ähnlich denen von Amazon S3 benötigen, können Sie diese Fehler bei HEAD- und GET-Vorgängen verhindern, indem Sie die Konsistenz auf „Verfügbar“ setzen. Wenn ein HEAD- oder GET-Vorgang die Konsistenz „Verfügbar“ verwendet, bietet StorageGRID nur die letztendliche Konsistenz. Ein fehlgeschlagener Vorgang wird bei zunehmender Konsistenz nicht wiederholt, sodass es nicht erforderlich ist, dass mehrere Kopien der Objektmetadaten verfügbar sind.

Konsistenz für API-Operation angeben

Um die Konsistenz für eine einzelne API-Operation festzulegen, müssen die Konsistenzwerte für die Operation unterstützt werden und Sie müssen die Konsistenz im Anforderungsheader angeben. In diesem Beispiel wird die Konsistenz für einen GetObject-Vorgang auf „Strong-Site“ festgelegt.

```
GET /bucket/object HTTP/1.1
Date: date
Authorization: authorization name
Host: host
Consistency-Control: strong-site
```



Sie müssen für die PutObject- und GetObject-Vorgänge dieselbe Konsistenz verwenden.

Konsistenz für Bucket angeben

Um die Konsistenz für den Bucket festzulegen, können Sie das StorageGRID verwenden "[PUT Bucket-Konsistenz](#)" Anfrage. Oder Sie können "[die Konsistenz eines Eimers ändern](#)" vom Mieterverwalter.

Beachten Sie beim Festlegen der Konsistenz für einen Bucket Folgendes:

- Durch das Festlegen der Konsistenz für einen Bucket wird bestimmt, welche Konsistenz für S3-Operationen verwendet wird, die an den Objekten im Bucket oder an der Bucket-Konfiguration ausgeführt werden. Es hat keine Auswirkungen auf Vorgänge am Bucket selbst.
- Die Konsistenz für einen einzelnen API-Vorgang überschreibt die Konsistenz für den Bucket.
- Im Allgemeinen sollten Buckets die Standardkonsistenz „Lesen nach neuem Schreiben“ verwenden. Wenn Anfragen nicht richtig funktionieren, ändern Sie nach Möglichkeit das Verhalten des Anwendungsclients. Oder konfigurieren Sie den Client so, dass die Konsistenz für jede API-Anforderung angegeben wird. Stellen Sie die Konsistenz auf Eimerebene nur als letztes Mittel ein.

[[Wie Konsistenzkontrollen und ILM-Regeln zusammenwirken]] Wie Konsistenz- und ILM-Regeln den Datenschutz beeinflussen

Sowohl Ihre Wahl der Konsistenz als auch Ihre ILM-Regel wirken sich darauf aus, wie Objekte geschützt werden. Diese Einstellungen können interagieren.

Beispielsweise wirkt sich die beim Speichern eines Objekts verwendete Konsistenz auf die anfängliche Platzierung der Objektmetadaten aus, während das für die ILM-Regel ausgewählte Aufnahmeverhalten die anfängliche Platzierung der Objektkopien beeinflusst. Da StorageGRID zur Erfüllung von Clientanforderungen Zugriff auf die Metadaten und Daten eines Objekts benötigt, kann die Auswahl passender Schutzebenen für Konsistenz und Aufnahmeverhalten einen besseren anfänglichen Datenschutz und vorhersehbarere Systemreaktionen bieten.

Die folgende "Aufnahmeverhalten" stehen für ILM-Regeln zur Verfügung:

Doppeltes Commit

StorageGRID erstellt sofort Zwischenkopien des Objekts und meldet dem Client den Erfolg. Wenn möglich, werden die in der ILM-Regel angegebenen Kopien erstellt.

Strikt

Alle in der ILM-Regel angegebenen Kopien müssen erstellt werden, bevor dem Client der Erfolg gemeldet wird.

Ausgewogen

StorageGRID versucht, bei der Aufnahme alle in der ILM-Regel angegebenen Kopien zu erstellen. Wenn dies nicht möglich ist, werden Zwischenkopien erstellt und der Erfolg wird an den Client zurückgegeben. Die in der ILM-Regel angegebenen Kopien werden nach Möglichkeit erstellt.

Beispiel für die Interaktion zwischen Konsistenz- und ILM-Regel

Angenommen, Sie haben ein Grid mit zwei Sites mit der folgenden ILM-Regel und der folgenden Konsistenz:

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

Wenn ein Client ein Objekt im Grid speichert, erstellt StorageGRID Kopien beider Objekte und verteilt Metadaten an beide Sites, bevor dem Client die Erfolgsmeldung zurückgegeben wird.

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 am Remote-Standort weiterhin Kopien der Objektdaten und der Objektmetadaten vorhanden. Das Objekt ist 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-Site 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 Wechselbeziehung zwischen Konsistenz und ILM-Regeln kann komplex sein. Wenden Sie sich an NetApp, wenn Sie Hilfe benötigen.

Objektversionierung

Sie können den Versionsstatus eines Buckets festlegen, wenn Sie mehrere Versionen jedes Objekts behalten möchten. Durch Aktivieren der Versionierung für einen Bucket können Sie vor dem versehentlichen Löschen von Objekten schützen und frühere Versionen eines Objekts abrufen und wiederherstellen.

Das StorageGRID -System implementiert Versionierung mit Unterstützung für die meisten Funktionen und mit einigen Einschränkungen. StorageGRID unterstützt bis zu 10.000 Versionen jedes Objekts.

Die Objektversionierung kann mit StorageGRID Information Lifecycle Management (ILM) oder mit der S3-Bucket-Lebenszykluskonfiguration 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) zum Löschen wird nicht unterstützt.



Die Versionierung kann nur für 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 wertet sie anhand der aktuellen ILM-Richtlinie neu aus. Alle Änderungen, die Sie an ILM-Richtlinien vornehmen, werden auf alle zuvor aufgenommenen Objekte angewendet. Dies schließt zuvor aufgenommene Versionen ein, wenn die Versionierung aktiviert ist. Beim ILM-Scannen werden neue ILM-Änderungen auf zuvor aufgenommene Objekte angewendet.

Für S3-Objekte in Buckets mit aktiverter Versionierung können Sie mit der Versionierungsunterstützung ILM-Regeln erstellen, die „Nicht aktuelle Zeit“ als Referenzzeit verwenden (wählen Sie **Ja** für die Frage „Diese Regel nur auf ältere Objektversionen anwenden?“ in ["Schritt 1 des Assistenten „ILM-Regel erstellen“"](#)). Wenn ein Objekt aktualisiert wird, werden seine vorherigen Versionen nicht mehr aktuell. Mithilfe eines Filters „Nicht aktuelle Zeit“ können Sie Richtlinien erstellen, die die Speicherauswirkungen früherer Objektversionen reduzieren.



Wenn Sie eine neue Version eines Objekts mithilfe eines mehrteiligen Uploadvorgangs hochladen, gibt die nicht aktuelle Zeit für die ursprüngliche Version des Objekts an, wann der mehrteilige Upload für die neue Version erstellt wurde, und nicht, wann der mehrteilige Upload abgeschlossen wurde. In seltenen Fällen kann die nicht aktuelle Zeit der Originalversion Stunden oder Tage vor der Zeit der aktuellen Version liegen.

Ähnliche Informationen

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

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

Wenn die globale S3-Objektsperre-Einstellung für Ihr StorageGRID System aktiviert ist, können Sie Buckets mit aktiverter S3-Objektsperre erstellen. Sie können die Standardaufbewahrung für jeden Bucket oder Aufbewahrungseinstellungen für jede Objektversion angeben.

So aktivieren Sie die S3-Objektsperre für einen Bucket

Wenn die globale S3-Objektsperre-Einstellung für Ihr StorageGRID System aktiviert ist, können Sie die S3-Objektsperre optional aktivieren, wenn Sie jeden Bucket erstellen.

S3 Object Lock ist eine permanente Einstellung, die nur aktiviert werden kann, wenn Sie einen Bucket erstellen. Sie können die S3-Objektsperre nicht hinzufügen oder deaktivieren, nachdem ein Bucket erstellt

wurde.

Um die S3-Objektsperre für einen Bucket zu aktivieren, verwenden Sie eine der folgenden Methoden:

- Erstellen Sie den Bucket mit dem Tenant Manager. Sehen "[S3-Bucket erstellen](#)" .
- Erstellen Sie den Bucket mithilfe einer CreateBucket-Anforderung mit dem `x-amz-bucket-object-lock-enabled` Anforderungsheader. Sehen "[Operationen an Buckets](#)" .

S3 Object Lock erfordert eine Bucket-Versionierung, die beim Erstellen des Buckets automatisch aktiviert wird. Sie können die Versionsverwaltung für den Bucket nicht aussetzen. Sehen "[Objektversionierung](#)" .

Standardaufbewahrungseinstellungen für einen Bucket

Wenn S3 Object Lock für einen Bucket aktiviert ist, können Sie optional die Standardaufbewahrung für den Bucket aktivieren und einen Standardaufbewahrungsmodus und eine Standardaufbewahrungsdauer angeben.

Standardaufbewahrungsmodus

- Im COMPLIANCE-Modus:
 - Das Objekt kann erst gelöscht werden, wenn sein 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 kann die `x-amz-bypass-governance-retention: true` Anforderungsheader zum Umgehen der Aufbewahrungseinstellungen.
 - Diese Benutzer können eine Objektversion löschen, bevor ihr Aufbewahrungsdatum erreicht ist.
 - Diese Benutzer können das Aufbewahrungsdatum eines Objekts erhöhen, verringern oder entfernen.

Standardaufbewahrungsdauer

Für jeden Bucket kann eine Standardaufbewahrungsdauer in Jahren oder Tagen angegeben werden.

So legen Sie die Standardaufbewahrung für einen Bucket fest

Um die Standardaufbewahrung für einen Bucket festzulegen, verwenden Sie eine der folgenden Methoden:

- Verwalten Sie die Bucket-Einstellungen über den Tenant Manager. Sehen "[Erstellen eines S3-Buckets](#)" Und "[Standardaufbewahrung für S3 Object Lock aktualisieren](#)" .
- Geben Sie eine PutObjectLockConfiguration-Anforderung für den Bucket aus, um den Standardmodus und die Standardanzahl von Tagen oder Jahren anzugeben.

PutObjectLockConfiguration

Mit der PutObjectLockConfiguration-Anforderung können Sie den Standardaufbewahrungsmodus und die Standardaufbewahrungsdauer für einen Bucket festlegen und ändern, bei dem S3 Object Lock aktiviert ist. Sie können auch zuvor konfigurierte Standardaufbewahrungseinstellungen entfernen.

Wenn neue Objektversionen in den Bucket aufgenommen werden, wird der Standardaufbewahrungsmodus angewendet, wenn `x-amz-object-lock-mode` Und `x-amz-object-lock-retain-until-date` sind nicht angegeben. Die Standardaufbewahrungsfrist wird zur Berechnung des Aufbewahrungs-bis-Datums

verwendet, wenn `x-amz-object-lock-retain-until-date` ist nicht angegeben.

Wenn die Standardaufbewahrungsfrist nach der Aufnahme einer Objektversion geändert wird, bleibt das Aufbewahrungsdatum der Objektversion gleich und wird nicht anhand der neuen Standardaufbewahrungsfrist neu berechnet.

Sie müssen über die `s3:PutBucketObjectLockConfiguration` Berechtigung oder Root-Konto sein, um diesen Vorgang abzuschließen.

Der Content-MD5 Der Anforderungsheader muss in der PUT-Anforderung angegeben werden.

Anforderungsbeispiel

Dieses Beispiel aktiviert S3 Object Lock für einen Bucket und legt den Standardaufbewahrungsmodus auf COMPLIANCE und die Standardaufbewahrungsdauer auf 6 Jahre fest.

```
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>
```

So bestimmen Sie die Standardaufbewahrung für einen Bucket

Um festzustellen, ob S3 Object Lock für einen Bucket aktiviert ist, und um den Standardaufbewahrungsmodus und die Aufbewahrungsdauer anzuzeigen, verwenden Sie eine der folgenden Methoden:

- Zeigen Sie den Bucket im Mandanten-Manager an. Sehen "["S3-Buckets anzeigen"](#) .
- Geben Sie eine `GetObjectLockConfiguration`-Anforderung aus.

GetObjectLockConfiguration

Mit der `GetObjectLockConfiguration`-Anforderung können Sie feststellen, ob die S3-Objektsperre für einen Bucket aktiviert ist. Wenn dies der Fall ist, können Sie prüfen, ob für den Bucket ein Standardaufbewahrungsmodus und eine Standardaufbewahrungsdauer konfiguriert sind.

Wenn neue Objektversionen in den Bucket aufgenommen werden, wird der Standardaufbewahrungsmodus angewendet, wenn `x-amz-object-lock-mode` ist nicht angegeben. Die Standardaufbewahrungsfrist wird zur Berechnung des Aufbewahrungs-bis-Datums verwendet, wenn `x-amz-object-lock-retain-until-date` ist nicht angegeben.

Sie müssen über die `s3:GetBucketObjectLockConfiguration` Berechtigung oder Root-Konto sein, um diesen Vorgang abzuschließen.

Anforderungsbeispiel

```
GET /bucket?object-lock HTTP/1.1
Host: host
Accept-Encoding: identity
User-Agent: aws-cli/1.18.106 Python/3.8.2 Linux/4.4.0-18362-Microsoft
botocore/1.17.29
x-amz-date: date
x-amz-content-sha256: authorization-string
Authorization: authorization-string
```

Antwortbeispiel

```
HTTP/1.1 200 OK
x-amz-id-2:
iVmcB70XXJRkRH1F1vq1151/T24gRfpwpuZrEG11Bb9ImOMAAe98oxSpX1knabA0LTvBYJpSIX
k=
x-amz-request-id: B34E94CACB2CEF6D
Date: Fri, 04 Sep 2020 22:47:09 GMT
Transfer-Encoding: chunked
Server: AmazonS3

<?xml version="1.0" encoding="UTF-8"?>
<ObjectLockConfiguration xmlns="http://s3.amazonaws.com/doc/2006-03-01/">
  <ObjectLockEnabled>Enabled</ObjectLockEnabled>
  <Rule>
    <DefaultRetention>
      <Mode>COMPLIANCE</Mode>
      <Years>6</Years>
    </DefaultRetention>
  </Rule>
</ObjectLockConfiguration>
```

So legen Sie Aufbewahrungseinstellungen für ein Objekt fest

Ein Bucket mit aktiverter S3 Object Lock kann eine Kombination aus Objekten mit und ohne S3 Object Lock-Aufbewahrungseinstellungen enthalten.

Aufbewahrungseinstellungen auf Objektebene werden mithilfe der S3 REST-API angegeben. Die Aufbewahrungseinstellungen für ein Objekt überschreiben alle Standardaufbewahrungseinstellungen für den Bucket.

Sie können für jedes Objekt die folgenden Einstellungen festlegen:

- **Aufbewahrungsmodus:** Entweder COMPLIANCE oder GOVERNANCE.
- **Aufbewahrungsdatum:** Ein Datum, das angibt, wie lange die Objektversion von StorageGRID aufbewahrt werden muss.
 - Wenn das Aufbewahrungsdatum im COMPLIANCE-Modus in der Zukunft liegt, kann das Objekt zwar abgerufen, aber nicht geändert oder gelöscht werden. Das Aufbewahrungsdatum kann verlängert werden, es kann jedoch nicht verkürzt oder entfernt werden.
 - Im GOVERNANCE-Modus können Benutzer mit Sonderberechtigung die Einstellung „Aufbewahren bis Datum“ umgehen. Sie können eine Objektversion löschen, bevor ihre Aufbewahrungsfrist abgelaufen ist. Sie können das Aufbewahrungsdatum auch verlängern, verkürzen oder sogar entfernen.
- **Rechtliche Sperre:** Durch Anwenden einer rechtlichen Sperre auf eine Objektversion wird dieses Objekt sofort gesperrt. Beispielsweise müssen Sie möglicherweise ein Objekt, das mit einer Untersuchung oder einem Rechtsstreit in Zusammenhang steht, rechtlich sperren. Eine rechtliche Sperre hat kein Ablaufdatum, sondern bleibt bestehen, bis sie ausdrücklich aufgehoben wird.

Die Einstellung für die rechtliche Aufbewahrung eines Objekts ist unabhängig vom Aufbewahrungsmodus und dem Aufbewahrungsdatum. Wenn eine Objektversion einer rechtlichen Sperre unterliegt, kann niemand diese Version löschen.

Um S3 Object Lock-Einstellungen anzugeben, wenn Sie einem Bucket eine Objektversion hinzufügen, führen Sie einen "[PutObject](#)" , "[Objekt kopieren](#)" , oder "[CreateMultipartUpload](#)" Anfrage.

Sie können Folgendes verwenden:

- `x-amz-object-lock-mode`, wobei COMPLIANCE oder GOVERNANCE (Groß-/Kleinschreibung beachten) lauten kann.



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

- `x-amz-object-lock-retain-until-date`
 - Der Wert für das Retain-until-Datum muss das Format haben `2020-08-10T21:46:00Z` . Sekundenbruchteile sind zulässig, es bleiben jedoch nur 3 Dezimalstellen erhalten (Millisekundengenauigkeit). Andere ISO 8601-Formate sind nicht zulässig.
 - Das Aufbewahrungsdatum muss in der Zukunft liegen.
- `x-amz-object-lock-legal-hold`

Wenn die rechtliche Sperre aktiviert ist (Groß-/Kleinschreibung beachten), wird das Objekt einer rechtlichen Sperre unterzogen. Wenn die rechtliche Sperre deaktiviert ist, wird keine rechtliche Sperre verhängt. Jeder andere Wert führt zu einem 400 Bad Request (InvalidArgument)-Fehler.

Wenn Sie einen dieser Anforderungsheader verwenden, beachten Sie die folgenden Einschränkungen:

- Der Content-MD5 Anforderungsheader ist erforderlich, falls vorhanden `x-amz-object-lock-*` Der Anforderungsheader ist in der PutObject-Anforderung vorhanden. Content-MD5 ist für CopyObject oder

CreateMultipartUpload nicht erforderlich.

- Wenn für den Bucket die S3-Objektsperre nicht aktiviert ist und ein `x-amz-object-lock-*` Wenn kein Anforderungsheader vorhanden ist, wird der Fehler „400 Bad Request (InvalidRequest)“ zurückgegeben.
- Die PutObject-Anforderung unterstützt die Verwendung von `x-amz-storage-class: REDUCED_REDUNDANCY` um dem AWS-Verhalten zu entsprechen. Wenn jedoch ein Objekt in einen Bucket mit aktiverter S3-Objektsperre aufgenommen wird, führt StorageGRID immer eine Aufnahme mit doppeltem Commit 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 über die richtige `s3:Get*` Berechtigungen.

Sie können die `s3:object-lock-remaining-retention-days` Richtlinienbedingungsschlüssel, um die minimal und maximal zulässigen Aufbewahrungsfristen für Ihre Objekte zu begrenzen.

So aktualisieren Sie die Aufbewahrungseinstellungen für ein Objekt

Wenn Sie die Einstellungen für die gesetzliche Aufbewahrungspflicht oder die Aufbewahrungsdauer für eine vorhandene Objektversion aktualisieren müssen, können Sie die folgenden Vorgänge für die Objektunterressource ausführen:

- `PutObjectLegalHold`

Wenn der neue Wert für die rechtliche Sperre EIN ist, wird das Objekt einer rechtlichen Sperre unterzogen. Wenn der Legal-Hold-Wert auf „AUS“ gesetzt ist, wird der Legal Hold aufgehoben.

- `PutObjectRetention`

- Der Moduswert kann `COMPLIANCE` oder `GOVERNANCE` sein (Groß-/Kleinschreibung beachten).
- Der Wert für das Retain-until-Datum muss das Format haben `2020-08-10T21:46:00Z` . Sekundenbruchteile sind zulässig, es bleiben jedoch nur 3 Dezimalstellen erhalten (Millisekundengenauigkeit). Andere ISO 8601-Formate sind nicht zulässig.
- Wenn für eine Objektversion ein vorhandenes Aufbewahrungsdatum vorhanden ist, können Sie dieses nur erhöhen. Der neue Wert muss in der Zukunft liegen.

So verwenden Sie den GOVERNANCE-Modus

Benutzer mit der `s3:BypassGovernanceRetention` Die Berechtigung kann die aktiven Aufbewahrungseinstellungen eines Objekts umgehen, das den `GOVERNANCE`-Modus verwendet. Alle `DELETE`- oder `PutObjectRetention`-Vorgänge müssen Folgendes enthalten: `x-amz-bypass-governance-retention:true` Anforderungsheader. Diese Benutzer können die folgenden zusätzlichen Vorgänge ausführen:

- Führen Sie die Vorgänge „`DeleteObject`“ oder „`DeleteObjects`“ aus, um eine Objektversion zu löschen, bevor ihre Aufbewahrungsfrist abgelaufen ist.

Objekte, die einer rechtlichen Sperre unterliegen, können nicht gelöscht werden. Die rechtliche Sperre muss deaktiviert sein.

- Führen Sie `PutObjectRetention`-Vorgänge durch, die den Modus einer Objektversion von `GOVERNANCE` in `COMPLIANCE` ändern, bevor die Aufbewahrungsfrist des Objekts abgelaufen ist.

Ein Wechsel des Modus von `COMPLIANCE` zu `GOVERNANCE` ist niemals zulässig.

- Führen Sie PutObjectRetention-Vorgänge durch, um die Aufbewahrungszeit einer Objektversion zu erhöhen, zu verringern oder zu entfernen.

Ähnliche Informationen

- ["Verwalten von Objekten mit S3 Object Lock"](#)
- ["Verwenden Sie S3 Object Lock, um Objekte beizubehalten"](#)
- ["Amazon Simple Storage Service-Benutzerhandbuch: Sperren von Objekten"](#)

Erstellen einer S3-Lebenszykluskonfiguration

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

Das einfache Beispiel in diesem Abschnitt veranschaulicht, wie eine S3-Lebenszykluskonfiguration steuern kann, wann bestimmte Objekte aus bestimmten S3-Buckets gelöscht werden (ablaufen). Das Beispiel in diesem Abschnitt dient nur zur Veranschaulichung. Ausführliche Informationen zum Erstellen von S3-Lebenszykluskonfigurationen finden Sie unter ["Amazon Simple Storage Service-Benutzerhandbuch: Objekt-Lebenszyklusverwaltung"](#). Beachten Sie, dass StorageGRID nur Ablaufaktionen unterstützt, keine Übergangsaktionen.

Was ist eine Lebenszykluskonfiguration?

Eine Lebenszykluskonfiguration 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 einer bestimmten Anzahl von Tagen).

StorageGRID unterstützt bis zu 1.000 Lebenszyklusregeln in einer Lebenszykluskonfiguration. Jede Regel kann die folgenden XML-Elemente enthalten:

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

Jedes Objekt folgt den Aufbewahrungseinstellungen entweder eines S3-Bucket-Lebenszyklus oder einer ILM-Richtlinie. Wenn ein S3-Bucket-Lebenszyklus konfiguriert ist, überschreiben die Aktionen zum Ablauf des Lebenszyklus die ILM-Richtlinie für Objekte, die dem Bucket-Lebenszyklusfilter entsprechen. Objekte, die nicht dem Bucket-Lebenszyklusfilter entsprechen, verwenden die Aufbewahrungseinstellungen der ILM-Richtlinie. Wenn ein Objekt einem Bucket-Lebenszyklusfilter entspricht und keine Ablaufaktionen explizit angegeben sind, werden die Aufbewahrungseinstellungen der ILM-Richtlinie nicht verwendet und es wird davon ausgegangen, dass Objektversionen für immer aufbewahrt werden. Sehen ["Beispieldokumentation für den S3-Bucket-Lebenszyklus und die ILM-Richtlinie"](#).

Dies kann dazu führen, dass ein Objekt aus dem Raster entfernt wird, obwohl die Platzierungsanweisungen in einer ILM-Regel weiterhin für das Objekt gelten. Oder ein Objekt kann auf dem Raster verbleiben, auch wenn alle ILM-Platzierungsanweisungen für das Objekt abgelaufen sind. Weitere Informationen finden Sie unter ["Funktionsweise von ILM während der gesamten Lebensdauer eines Objekts"](#).



Die Bucket-Lebenszykluskonfiguration kann mit Buckets verwendet werden, bei denen S3 Object Lock aktiviert ist. Für ältere konforme Buckets wird die Bucket-Lebenszykluskonfiguration jedoch nicht unterstützt.

StorageGRID unterstützt die Verwendung der folgenden Bucket-Operationen zur Verwaltung von Lebenszykluskonfigurationen:

- DeleteBucketLifecycle
- GetBucketLifecycleConfiguration
- PutBucketLifecycleConfiguration

Lebenszykluskonfiguration erstellen

Als ersten Schritt beim Erstellen einer Lebenszykluskonfiguration erstellen Sie eine JSON-Datei, die eine oder mehrere Regeln enthält. Diese JSON-Datei enthält beispielsweise die folgenden drei Regeln:

1. Regel 1 gilt nur für Objekte, die dem Präfix entsprechen `category1/` und die haben eine `key2` Wert von `tag2`. Der `Expiration` Der 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` Der Parameter gibt an, dass Objekte, die dem Filter entsprechen, 100 Tage nach ihrer Aufnahme ablaufen.



Regeln, die eine Anzahl von Tagen angeben, beziehen sich auf den Zeitpunkt der Aufnahme des Objekts. 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` Der Parameter gibt an, dass alle nicht aktuellen Versionen übereinstimmender Objekte 50 Tage, nachdem sie nicht mehr aktuell sind, 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"  
        }  
    ]  
}
```

Lebenszykluskonfiguration auf Bucket anwenden

Nachdem Sie die Lebenszyklus-Konfigurationsdatei erstellt haben, wenden Sie sie auf einen Bucket an, indem Sie eine PutBucketLifecycleConfiguration-Anforderung senden.

Diese Anfrage wendet die Lebenszykluskonfiguration in der Beispieldatei auf Objekte in einem Bucket namens testbucket .

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

Um zu überprüfen, ob eine Lebenszykluskonfiguration erfolgreich auf den Bucket angewendet wurde, senden Sie eine GetBucketLifecycleConfiguration-Anforderung. Beispiel:

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

Eine erfolgreiche Antwort listet die Lebenszykluskonfiguration auf, die Sie gerade angewendet haben.

Überprüfen Sie, ob das Ablaufdatum des Bucket-Lebenszyklus für das Objekt gilt

Sie können beim Ausgeben einer PutObject-, HeadObject- oder GetObject-Anforderung feststellen, ob eine Ablaufregel in der Lebenszykluskonfiguration auf ein bestimmtes Objekt zutrifft. Wenn eine Regel zutrifft, enthält die Antwort eine `Expiration` Parameter, der angibt, wann das Objekt abläuft und welche Ablaufregel erfüllt wurde.



Da der Bucket-Lebenszyklus ILM außer Kraft setzt, `expiry-date` angezeigt wird das tatsächliche Datum, an dem das Objekt gelöscht wird. Weitere Informationen finden Sie unter ["So wird die Objektaufbewahrung bestimmt"](#) .

Beispielsweise wurde diese PutObject-Anforderung am 22. Juni 2020 ausgegeben und platziert ein Objekt in der testbucket Eimer.

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

Die Erfolgsantwort gibt an, dass das Objekt in 100 Tagen (01. Oktober 2020) abläuft und dass es Regel 2 der Lebenszykluskonfiguration entspricht.

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

Beispielsweise wurde diese HeadObject-Anforderung verwendet, um Metadaten für dasselbe Objekt im Testbucket-Bucket abzurufen.

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

Die Erfolgsantwort enthält die Metadaten des Objekts und gibt an, dass das Objekt in 100 Tagen abläuft und Regel 2 entspricht.

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



Für Buckets mit aktivierter Versionierung gilt: `x-amz-expiration` Der Antwortheader gilt nur für aktuelle Versionen von Objekten.

Empfehlungen zur Implementierung der S3 REST API

Sie sollten diese Empfehlungen befolgen, wenn Sie die S3 REST-API zur Verwendung mit StorageGRID implementieren.

Empfehlungen für HEADs 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.

Andernfalls kann es vorkommen, dass Sie, wenn der HEAD-Vorgang das Objekt nicht findet, eine große Anzahl interner Serverfehler vom Typ 500 erhalten, wenn zwei oder mehr Speicherknoten am selben Standort nicht verfügbar sind oder ein Remote-Standort nicht erreichbar ist.

Sie können die "Verfügbare" Konsistenz für jeden Bucket mithilfe der ["PUT Bucket-Konsistenz"](#) Anfrage, oder

Sie können die Konsistenz im Anfrageheader für eine einzelne API-Operation angeben.

Empfehlungen für Objektschlüssel

Befolgen Sie diese Empfehlungen für Objektschlüsselnamen, basierend auf dem Zeitpunkt der ersten Erstellung des Buckets.

Buckets, die in StorageGRID 11.4 oder früher erstellt wurden

- Verwenden Sie keine zufälligen Werte als die ersten vier Zeichen der Objektschlüssel. Dies steht im Gegensatz zur früheren AWS-Empfehlung für Schlüsselpräfixe. Verwenden Sie stattdessen nicht zufällige, nicht eindeutige Präfixe, wie etwa `image`.
- Wenn Sie der früheren AWS-Empfehlung folgen, zufällige und eindeutige Zeichen in Schlüsselpräfixen zu verwenden, stellen Sie den Objektschlüsseln einen Verzeichnisnamen voran. Das heißt, verwenden Sie dieses Format:

`mybucket/mydir/f8e3-image3132.jpg`

Anstelle dieses Formats:

`mybucket/f8e3-image3132.jpg`

In StorageGRID 11.4 oder höher erstellte Buckets

Eine Einschränkung der Objektschlüsselnamen zur Einhaltung der Best Practices für die Leistung ist nicht erforderlich. In den meisten Fällen können Sie für die ersten vier Zeichen von Objektschlüsselnamen zufällige Werte verwenden.

Eine Ausnahme hiervon stellt ein S3-Workload dar, der kontinuierlich alle Objekte nach kurzer Zeit entfernt. Um die Auswirkungen auf die Leistung in diesem Anwendungsfall zu minimieren, variieren Sie alle paar tausend Objekte einen führenden Teil des Schlüsselnamens mit etwas wie dem Datum. Nehmen wir beispielsweise an, dass ein S3-Client normalerweise 2.000 Objekte/Sekunde schreibt und die ILM- oder Bucket-Lebenszyklusrichtlinie alle Objekte nach drei Tagen entfernt. Um die Auswirkungen auf die Leistung zu minimieren, können Sie Schlüssel nach einem Muster wie diesem benennen: `/mybucket/mydir/yyyyymmddhhmmss-random_UUID.jpg`

Empfehlungen für „Range Reads“

Wenn die "globale Option zum Komprimieren gespeicherter Objekte" aktiviert ist, sollten S3-Clientanwendungen die Durchführung von GetObject-Operationen vermeiden, die einen zurückzugebenden Bytebereich angeben. Diese „Range Read“-Operationen sind ineffizient, da StorageGRID die Objekte effektiv dekomprimieren muss, um auf die angeforderten Bytes zuzugreifen. GetObject-Operationen, die einen kleinen Bytebereich aus einem sehr großen Objekt anfordern, sind besonders ineffizient. Beispielsweise ist es ineffizient, einen 10 MB großen Bereich aus einem komprimierten 50 GB-Objekt zu lesen.

Wenn Bereiche aus komprimierten Objekten gelesen werden, kann es bei Clientanforderungen zu einer Zeitüberschreitung kommen.



Wenn Sie Objekte komprimieren müssen und Ihre Clientanwendung Bereichslesevorgänge verwenden muss, erhöhen Sie das Lesezeitlimit für die 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 für die meisten Vorgänge und mit einigen Einschränkungen. Sie müssen die Implementierungsdetails verstehen, wenn Sie S3 REST API-Clientanwendungen integrieren.

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

Datumsverarbeitung

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

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

Allgemeine Anforderungsheader

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

Anforderungsheader	Durchführung
Genehmigung	Volle Unterstützung für AWS Signature Version 2 Unterstützung für AWS Signature Version 4, mit folgenden Ausnahmen: <ul style="list-style-type: none">Wenn Sie den tatsächlichen Nutzlastprüfsummenwert in <code>x-amz-content-sha256</code> wird der Wert ohne Validierung akzeptiert, als ob der Wert <code>UNSIGNED-PAYLOAD</code> für den Header vorgesehen war. Wenn Sie eine <code>x-amz-content-sha256</code> Header-Wert, der impliziert aws-chunked Streaming (z. B. <code>STREAMING-AWS4-HMAC-SHA256-PAYLOAD</code>), werden die Chunk-Signaturen nicht anhand der Chunk-Daten überprüft.
<code>x-amz-Sicherheitstoken</code>	Nicht implementiert. Rückgaben <code>xNotImplemented</code> .

Allgemeine Antwortheader

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

Antwortheadern	Durchführung
x-amz-id-2	Nicht verwendet

Authentifizieren von Anfragen

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

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

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

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

Verwenden Sie den HTTP-Autorisierungsheader

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

Verwenden von Abfrageparametern

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

Vorgänge für den Dienst

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

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

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

Operationen an Buckets

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

Jedes Raster kann maximal 100.000 Buckets enthalten.

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

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

Weitere Informationen finden Sie im Folgenden:

- ["Amazon Simple Storage Service-Benutzerhandbuch: Bucket-Kontingente, Einschränkungen und Begrenzungen"](#)
- ["Konfigurieren von S3-Endpunktdomänennamen"](#)

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

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

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

Betrieb	Durchführung
Bucket erstellen	<p>Erstellt einen neuen Bucket. Indem Sie den Bucket erstellen, werden Sie zum Bucket-Eigentümer.</p> <ul style="list-style-type: none"> Bucket-Namen müssen den folgenden Regeln entsprechen: <ul style="list-style-type: none"> Muss in jedem StorageGRID -System eindeutig sein (nicht nur innerhalb des Mandantenkontos). Muss DNS-kompatibel sein. Muss mindestens 3 und darf nicht mehr als 63 Zeichen enthalten. Kann eine Reihe von einem oder mehreren Labels sein, wobei benachbarte Labels durch einen Punkt getrennt sind. Jedes Etikett muss mit einem Kleinbuchstaben oder einer Zahl beginnen und enden und darf nur Kleinbuchstaben, Zahlen und Bindestriche enthalten. Darf nicht wie eine IP-Adresse im Textformat aussehen. In Anfragen im virtuell gehosteten Stil sollten keine Punkte verwendet werden. Punkte verursachen Probleme bei der Überprüfung des Platzhalterzertifikats des Servers. Standardmäßig werden Buckets im <code>us-east-1</code> Region; Sie können jedoch die <code>LocationConstraint</code> Anforderungselement im Anforderungstext, um eine andere Region anzugeben. Bei Verwendung der <code>LocationConstraint</code> Element müssen Sie den genauen Namen einer Region angeben, die mit dem Grid Manager oder der Grid Management API definiert wurde. Wenden Sie sich an Ihren Systemadministrator, wenn Sie den zu verwendenden Regionsnamen nicht kennen. <p>Hinweis: Es tritt ein Fehler auf, wenn Ihre CreateBucket-Anforderung eine Region verwendet, die nicht in StorageGRID definiert wurde.</p> <ul style="list-style-type: none"> Sie können Folgendes einschließen: <code>x-amz-bucket-object-lock-enabled</code> Anforderungsheader zum Erstellen eines Buckets mit aktivierter S3-Objektsperre. Sehen ""Verwenden Sie die S3 REST API, um S3 Object Lock zu konfigurieren" . <p>Sie müssen S3 Object Lock aktivieren, wenn Sie den Bucket erstellen. Sie können die S3-Objektsperre nicht hinzufügen oder deaktivieren, nachdem ein Bucket erstellt wurde. S3 Object Lock erfordert eine Bucket-Versionierung, die automatisch aktiviert wird, wenn Sie den Bucket erstellen.</p>
Bucket löschen	Löscht den Bucket.
BucketCors löschen	Löscht die CORS-Konfiguration für den Bucket.
DeleteBucketEncryption	Löscht die Standardverschlüsselung aus dem Bucket. Vorhandene verschlüsselte Objekte bleiben verschlüsselt, aber alle neuen Objekte, die dem Bucket hinzugefügt werden, werden nicht verschlüsselt.

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

Betrieb	Durchführung
GetBucketTagging	<p>Verwendet die <code>tagging</code> Unterressource, um alle Tags für einen Bucket zurückzugeben.</p> <p>Achtung: Wenn für diesen Bucket ein nicht standardmäßiger ILM-Richtlinientag festgelegt ist, wird ein <code>NTAP-SG-ILM-BUCKET-TAG</code> Bucket-Tag mit einem ihm zugewiesenen Wert. Ändern oder entfernen Sie dieses Tag nicht.</p>
GetBucketVersioning	<p>Diese Implementierung verwendet die <code>versioning</code> Unterressource, um den Versionsstatus eines Buckets zurückzugeben.</p> <ul style="list-style-type: none"> • <code>blank</code>: Die Versionierung wurde nie aktiviert (Bucket ist „Unversioned“) • Aktiviert: Versionierung ist aktiviert • Ausgesetzt: Die Versionsverwaltung war zuvor aktiviert und ist ausgesetzt
GetObjectLockConfiguration	<p>Gibt den Standardaufbewahrungsmodus und die Standardaufbewahrungsdauer des Buckets zurück, sofern konfiguriert.</p> <p>Sehen "Verwenden Sie die S3 REST API, um S3 Object Lock zu konfigurieren".</p>
Kopfeimer	<p>Stellt fest, ob ein Bucket vorhanden ist und Sie über die Berechtigung verfügen, darauf zuzugreifen.</p> <p>Dieser Vorgang gibt Folgendes zurück:</p> <ul style="list-style-type: none"> • <code>x-ntap-sg-bucket-id</code>: Die UUID des Buckets im UUID-Format. • <code>x-ntap-sg-trace-id</code>: Die eindeutige Trace-ID der zugehörigen Anfrage.
ListObjects und ListObjectsV2 (früher GET Bucket genannt)	<p>Gibt einige oder alle (bis zu 1.000) Objekte in einem Bucket zurück. Die Speicherklasse für Objekte kann einen von zwei Werten haben, auch wenn das Objekt mit dem <code>REDUCED_REDUNDANCY</code> Speicherklassenoption:</p> <ul style="list-style-type: none"> • <code>STANDARD</code>, was darauf hinweist, dass das Objekt in einem Speicherpool gespeichert ist, der aus Speicherknoten besteht. • <code>GLACIER</code>, was darauf hinweist, dass das Objekt in den vom Cloud Storage Pool angegebenen externen Bucket verschoben wurde. <p>Wenn der Bucket eine große Anzahl gelöschter Schlüssel mit demselben Präfix enthält, kann die Antwort einige <code>CommonPrefixes</code> die keine Schlüssel enthalten.</p>
ListObjectVersions (zuvor GET Bucket Object-Versionen genannt)	<p>Mit Lesezugriff auf einen Bucket kann dieser Vorgang mit dem <code>versions</code> Die Unterressource listet Metadaten aller Versionen von Objekten im Bucket auf.</p>

Betrieb	Durchführung
PutBucketCors	<p>Legt die CORS-Konfiguration für einen Bucket fest, sodass der Bucket Cross-Origin-Anfragen verarbeiten kann. Cross-Origin Resource Sharing (CORS) ist ein Sicherheitsmechanismus, der es Client-Webanwendungen in einer Domäne ermöglicht, auf Ressourcen in einer anderen Domäne zuzugreifen. Angenommen, Sie verwenden einen S3-Bucket namens <code>images</code> zum Speichern von Grafiken. Durch Festlegen der CORS-Konfiguration für die <code>images</code> Bucket, können Sie die Anzeige der Bilder in diesem Bucket auf der Website zulassen</p> <p><code>http://www.example.com</code>.</p>
PutBucketEncryption	<p>Legt den Standardverschlüsselungsstatus eines vorhandenen Buckets fest. Wenn die Verschlüsselung auf Bucket-Ebene aktiviert ist, werden alle neuen Objekte, die dem Bucket hinzugefügt werden, verschlüsselt. StorageGRID unterstützt serverseitige Verschlüsselung mit von StorageGRID verwalteten Schlüsseln. Wenn Sie die serverseitige Verschlüsselungskonfigurationsregel angeben, legen Sie die <code>SSEAlgorithm</code> Parameter auf <code>AES256</code> und verwenden Sie nicht die <code>KMSMasterKeyID</code> Parameter.</p> <p>Die Standardverschlüsselungskonfiguration des Buckets wird ignoriert, wenn die Objekt-Upload-Anforderung bereits eine Verschlüsselung angibt (d. h. wenn die Anforderung die <code>x-amz-server-side-encryption-*</code> Anforderungsheader).</p>
PutBucketLifecycleConfiguration (früher PUT Bucket-Lebenszyklus genannt)	<p>Erstellt eine neue Lebenszykluskonfiguration für den Bucket oder ersetzt eine vorhandene Lebenszykluskonfiguration. StorageGRID unterstützt bis zu 1.000 Lebenszyklusregeln in einer Lebenszykluskonfiguration. Jede Regel kann die folgenden XML-Elemente enthalten:</p> <ul style="list-style-type: none"> • Ablauf (Tage, Datum, <code>ExpiredObjectDeleteMarker</code>) • <code>NoncurrentVersionExpiration</code> (<code>NewerNoncurrentVersions</code>, <code>NoncurrentDays</code>) • Filter (Präfix, Tag) • Status • AUSWEIS <p>StorageGRID unterstützt diese Aktionen nicht:</p> <ul style="list-style-type: none"> • <code>AbbruchUnvollständigMehrteiliger Upload</code> • Übergang <p>Sehen "Erstellen einer S3-Lebenszykluskonfiguration". Informationen dazu, wie die Ablaufaktion in einem Bucket-Lebenszyklus mit ILM-Platzierungsanweisungen interagiert, finden Sie unter "Funktionsweise von ILM während der gesamten Lebensdauer eines Objekts".</p> <p>Hinweis: Die Bucket-Lebenszykluskonfiguration kann mit Buckets verwendet werden, bei denen S3 Object Lock aktiviert ist, die Bucket-Lebenszykluskonfiguration wird jedoch für ältere konforme Buckets nicht unterstützt.</p>

Betrieb	Durchführung
PutBucketNotificationConfiguration (früher PUT Bucket-Benachrichtigung genannt)	<p>Konfiguriert Benachrichtigungen für den Bucket mithilfe der im Anforderungstext enthaltenen Benachrichtigungskonfigurations-XML. Sie sollten sich der folgenden Implementierungsdetails bewusst sein:</p> <ul style="list-style-type: none"> StorageGRID unterstützt Amazon Simple Notification Service (Amazon SNS) oder Kafka-Themen als Ziele. Simple Queue Service (SQS) oder Amazon Lambda-Endpunkte werden nicht unterstützt. Das Ziel für Benachrichtigungen muss als URN eines StorageGRID Endpunkts angegeben werden. Endpunkte können mit dem Tenant Manager oder der Tenant Management API erstellt werden. <p>Der Endpunkt muss vorhanden sein, damit die Benachrichtigungskonfiguration erfolgreich ist. Wenn der Endpunkt nicht existiert, wird ein 400 Bad Request Fehler mit dem Code zurückgegeben <code>InvalidArgumentException</code>.</p> <ul style="list-style-type: none"> Für die folgenden Ereignistypen können Sie keine Benachrichtigung konfigurieren. Diese Ereignistypen werden nicht unterstützt. <ul style="list-style-type: none"> <code>s3:ReducedRedundancyLostObject</code> <code>s3:ObjectRestore:Completed</code> Von StorageGRID gesendete Ereignisbenachrichtigungen verwenden das standardmäßige JSON-Format, mit der Ausnahme, dass sie einige Schlüssel nicht enthalten und für andere bestimmte Werte verwenden, wie in der folgenden Liste gezeigt: <ul style="list-style-type: none"> Ereignisquelle <ul style="list-style-type: none"> <code>sgws:s3</code> awsRegion <ul style="list-style-type: none"> nicht enthalten x-amz-id-2 <ul style="list-style-type: none"> nicht enthalten arn <ul style="list-style-type: none"> <code>urn:sgws:s3:::bucket_name</code>
PutBucketPolicy	Legt die dem Bucket zugeordnete Richtlinie fest. Sehen " "Verwenden Sie Bucket- und Gruppenzugriffsrichtlinien" ".

Betrieb	Durchführung
PutBucketReplication	<p>Konfiguriert "StorageGRID CloudMirror-Replikation" für den Bucket unter Verwendung der im Anforderungstext bereitgestellten XML-Replikationskonfiguration. Bei der CloudMirror-Replikation sollten Sie die folgenden Implementierungsdetails beachten:</p> <ul style="list-style-type: none"> StorageGRID unterstützt nur V1 der Replikationskonfiguration. Dies bedeutet, dass StorageGRID die Verwendung des <code>Filter</code> Element für Regeln und befolgt V1-Konventionen zum Löschen von Objektversionen. Weitere Einzelheiten finden Sie unter "Amazon Simple Storage Service-Benutzerhandbuch: Replikationskonfiguration" . Die Bucket-Replikation kann für versionierte oder nicht versionierte Buckets konfiguriert werden. Sie können in jeder Regel der XML-Replikationskonfiguration einen anderen Ziel-Bucket angeben. Ein Quell-Bucket kann in mehr als einen Ziel-Bucket repliziert werden. Ziel-Buckets müssen als URN von StorageGRID -Endpunkten angegeben werden, wie im Tenant Manager oder der Tenant Management API angegeben. Sehen "Konfigurieren der CloudMirror-Replikation" . <p>Der Endpunkt muss vorhanden sein, damit die Replikationskonfiguration erfolgreich ist. Wenn der Endpunkt nicht existiert, schlägt die Anfrage fehl, da 400 Bad Request Die Fehlermeldung lautet: <code>Unable to save the replication policy. The specified endpoint URN does not exist: URN.</code></p> <ul style="list-style-type: none"> Sie müssen <code>Role</code> im Konfigurations-XML. Dieser Wert wird von StorageGRID nicht verwendet und wird ignoriert, wenn er übermittelt wird. Wenn Sie die Speicherklasse aus der Konfigurations-XML weglassen, verwendet StorageGRID die <code>STANDARD</code> Speicherklasse standardmäßig. Wenn Sie ein Objekt aus dem Quell-Bucket oder den Quell-Bucket selbst löschen, ist das regionsübergreifende Replikationsverhalten wie folgt: <ul style="list-style-type: none"> Wenn Sie das Objekt oder den Bucket löschen, bevor es repliziert wurde, wird das Objekt/der Bucket nicht repliziert und Sie werden nicht benachrichtigt. Wenn Sie das Objekt oder den Bucket nach der Replikation löschen, folgt StorageGRID dem standardmäßigen Löschverhalten von Amazon S3 für V1 der regionsübergreifenden Replikation.

Betrieb	Durchführung
PutBucketTagging	<p>Verwendet die <code>tagging</code> Unterressource zum Hinzufügen oder Aktualisieren eines Satzes von Tags für einen Bucket. Beachten Sie beim Hinzufügen von Bucket-Tags die folgenden Einschränkungen:</p> <ul style="list-style-type: none"> • Sowohl StorageGRID als auch Amazon S3 unterstützen bis zu 50 Tags für jeden Bucket. • Mit einem Bucket verknüpfte Tags müssen eindeutige Tag-Schlüssel haben. Ein Tag-Schlüssel kann bis zu 128 Unicode-Zeichen lang sein. • Tag-Werte können bis zu 256 Unicode-Zeichen lang sein. • Bei Schlüsseln und Werten wird zwischen Groß- und Kleinschreibung unterschieden. <p>Achtung: Wenn für diesen Bucket ein nicht standardmäßiger ILM-Richtlinientag festgelegt ist, wird ein <code>NTAP-SG-ILM-BUCKET-TAG</code> Bucket-Tag mit einem ihm zugewiesenen Wert. Stellen Sie sicher, dass die <code>NTAP-SG-ILM-BUCKET-TAG</code> Das Bucket-Tag ist mit dem zugewiesenen Wert in allen PutBucketTagging-Anfragen enthalten. Ändern oder entfernen Sie dieses Tag nicht.</p> <p>Hinweis: Dieser Vorgang überschreibt alle aktuellen Tags, die der Bucket bereits hat. Wenn vorhandene Tags aus dem Set weggelassen werden, werden diese Tags für den Bucket entfernt.</p>
PutBucketVersioning	<p>Verwendet die <code>versioning</code> Unterressource zum Festlegen des Versionsstatus eines vorhandenen Buckets. Sie können den Versionsstatus mit einem der folgenden Werte festlegen:</p> <ul style="list-style-type: none"> • Aktiviert: Aktiviert die Versionierung für die Objekte im Bucket. Alle dem Bucket hinzugefügten Objekte erhalten eine eindeutige Versions-ID. • Angehalten: Deaktiviert die Versionierung für die Objekte im Bucket. Alle zum Bucket hinzugefügten Objekte erhalten die Versions-ID <code>null</code>.
PutObjectLockConfiguration	<p>Konfiguriert oder entfernt den Standardaufbewahrungsmodus und die Standardaufbewahrungszeit des Buckets.</p> <p>Wenn die Standardaufbewahrungszeit geändert wird, bleibt das Aufbewahrungsdatum vorhandener Objektversionen gleich und wird nicht anhand der neuen Standardaufbewahrungszeit neu berechnet.</p> <p>Sehen "Verwenden Sie die S3 REST API, um S3 Object Lock zu konfigurieren" für detaillierte Informationen.</p>

Operationen an Objekten

Operationen an Objekten

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

Für alle Objektoperationen gelten folgende Bedingungen:

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

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

Betrieb	Durchführung
Objekt löschen	<p>Multi-Faktor-Authentifizierung (MFA) und der Antwortheader <code>x-amz-mfa</code> werden nicht unterstützt.</p> <p>Bei der Verarbeitung einer <code>DeleteObject</code>-Anforderung versucht StorageGRID, alle Kopien des Objekts sofort von allen gespeicherten Standorten zu entfernen. Bei Erfolg gibt StorageGRID sofort eine Antwort an den Client zurück. Wenn nicht alle Kopien innerhalb von 30 Sekunden entfernt werden können (z. B. weil ein Speicherort vorübergehend nicht verfügbar ist), stellt StorageGRID die Kopien zur Entfernung in die Warteschlange und zeigt dem Client anschließend den Erfolg an.</p> <p>Versionierung</p> <p>Um eine bestimmte Version zu entfernen, muss der Anforderer der Bucket-Eigentümer sein und die <code>versionId</code> Unterressource. Durch die Verwendung dieser Unterressource wird die Version dauerhaft gelöscht. Wenn die <code>versionId</code> entspricht einem Löschmarker, der Antwortheader <code>x-amz-delete-marker</code> wird zurückgegeben auf <code>true</code>.</p> <ul style="list-style-type: none"> Wenn ein Objekt gelöscht wird, ohne dass <code>versionId</code> Unterressource auf einem Bucket mit aktiver Versionierung, führt dies zur Generierung einer Löschmarkierung. Der <code>versionId</code> für die Löschmarkierung wird mit dem <code>x-amz-version-id</code> Antwortheader und der <code>x-amz-delete-marker</code> Der Antwortheader wird auf <code>true</code>. Wenn ein Objekt gelöscht wird, ohne dass <code>versionId</code> Unterressource auf einem Bucket mit ausgesetzter Versionierung, führt dies zu einer dauerhaften Löschung einer bereits vorhandenen „Null“-Version oder eines „Null“-Löschmarkers und zur Generierung eines neuen „Null“-Löschmarkers. Der <code>x-amz-delete-marker</code> Der Antwortheader wird auf <code>true</code>. <p>Hinweis: In bestimmten Fällen können für ein Objekt mehrere Löschmarkierungen vorhanden sein.</p> <p>Sehen "Verwenden Sie die S3 REST API, um S3 Object Lock zu konfigurieren" um zu erfahren, wie Sie Objektversionen im GOVERNANCE-Modus löschen.</p>

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

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

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

Verwenden Sie S3 Select

StorageGRID unterstützt die folgenden Amazon S3 Select-Klauseln, Datentypen und

Operatoren für die "SelectObjectContent-Befehl" .



Nicht aufgeführte Artikel werden nicht unterstützt.

Informationen zur Syntax finden Sie unter "[SelectObjectContent](#)" . Weitere Informationen zu S3 Select finden Sie im "[AWS-Dokumentation für S3 Select](#)" .

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

Klauseln

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

Datentypen

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

Betreiber

Logische Operatoren

- UND
- NICHT
- ODER

Vergleichsoperatoren

- <
- >
- ⇐
- >=
- =
- =
- <>
- !=
- ZWISCHEN

- IN

Mustervergleichsoperatoren

- WIE
- _
- %

Unitäre Operatoren

- IST NULL
- IST NICHT NULL

Mathematische Operatoren

- +
- -
- *
- /
- %

StorageGRID folgt der Priorität des Amazon S3 Select-Operators.

Aggregatfunktionen

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

Bedingte Funktionen

- FALL
- VERSCHMELZEN
- NULLIF

Konvertierungsfunktionen

- CAST (für unterstützten Datentyp)

Datumsfunktionen

- DATE_ADD
- DATE_DIFF
- EXTRAKT
- TO_STRING

- TO_TIMESTAMP
- UTCNOW

Zeichenfolgenfunktionen

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

Verwenden Sie serverseitige Verschlüsselung

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

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

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

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



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



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

Verwenden Sie SSE

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

x-amz-server-side-encryption

Der SSE-Anforderungsheader wird von den folgenden Objektoperationen unterstützt:

- "[PutObject](#)"
- "[Objekt kopieren](#)"
- "[CreateMultipartUpload](#)"

Verwenden Sie SSE-C

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

Anforderungsheader	Beschreibung
x-amz-server-side-encryption-customer-algorithm	Geben Sie den Verschlüsselungsalgorithmus an. Der Headerwert muss AES256 .
x-amz-server-side-encryption-customer-key	Geben Sie den Verschlüsselungsschlüssel an, der zum Verschlüsseln oder Entschlüsseln des Objekts verwendet wird. Der Wert für den Schlüssel muss 256 Bit lang und base64-codiert sein.
x-amz-server-side-encryption-customer-key-MD5	Geben Sie den MD5-Digest des Verschlüsselungsschlüssels gemäß RFC 1321 an, der verwendet wird, um sicherzustellen, dass der Verschlüsselungsschlüssel fehlerfrei übertragen wurde. Der Wert für den MD5-Digest muss base64-codiert und 128 Bit lang sein.

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

- "[GetObject](#)"
- "[HeadObject](#)"
- "[PutObject](#)"
- "[Objekt kopieren](#)"
- "[CreateMultipartUpload](#)"
- "[UploadPart](#)"
- "[UploadPartCopy](#)"

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

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

- Sie müssen https verwenden.



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

- Der ETag in der Antwort ist nicht der MD5 der Objektdaten.
- Sie müssen die Zuordnung von Verschlüsselungsschlüsseln zu Objekten verwalten. StorageGRID speichert keine Verschlüsselungsschlüssel. Sie sind für die Nachverfolgung des

Verschlüsselungsschlüssels verantwortlich, den Sie für jedes Objekt bereitstellen.

- Wenn für Ihren Bucket die Versionierung aktiviert ist, sollte jede Objektversion über einen eigenen Verschlüsselungsschlüssel verfügen. Sie sind für die Nachverfolgung des für jede Objektversion verwendeten Verschlüsselungsschlüssels verantwortlich.
- Da Sie die Verschlüsselungsschlüssel auf der Clientseite verwalten, müssen Sie auch alle zusätzlichen Sicherheitsvorkehrungen, wie etwa die Schlüsselrotation, auf der Clientseite verwalten.



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

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

Ähnliche Informationen

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

Objekt kopieren

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

Konflikte lösen

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

Objektgröße

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

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



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

UTF-8-Zeichen in Benutzermetadaten

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

StorageGRID analysiert oder interpretiert keine Escape-UTF-8-Zeichen, die im Schlüsselnamen oder -wert

benutzerdefinierter Metadaten enthalten sind. Escape-UTF-8-Zeichen werden als ASCII-Zeichen behandelt:

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

Unterstützte Anforderungsheader

Die folgenden Anforderungsheader werden unterstützt:

- Content-Type
- x-amz-copy-source
- x-amz-copy-source-if-match
- x-amz-copy-source-if-none-match
- x-amz-copy-source-if-unmodified-since
- x-amz-copy-source-if-modified-since
- x-amz-meta-, gefolgt von einem Name-Wert-Paar mit benutzerdefinierten Metadaten
- x-amz-metadata-directive: Der Standardwert ist COPY , wodurch Sie das Objekt und die zugehörigen Metadaten kopieren können.

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

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

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

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

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

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

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

Sehen [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 in das neue Objekt. Dieses Verhalten gilt unabhängig davon, ob Sie versuchen, x-amz-checksum-algorithm in der Objektanforderung.

- x-amz-website-redirect-location

Speicherklassenoptionen

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

- STANDARD

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

- REDUCED_REDUNDANCY

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



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

Verwenden von x-amz-copy-source in CopyObject

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

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

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

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

Anforderungsheader für serverseitige Verschlüsselung

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

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



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

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



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

Versionierung

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

GetObject

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

GetObject und mehrteilige Objekte

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

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

UTF-8-Zeichen in Benutzermetadaten

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

Unterstützter Anforderungsheader

Der folgende Anforderungsheader wird unterstützt:

- `x-amz-checksum-mode: Enabled`

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

Nicht unterstützter Anforderungsheader

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

- x-amz-website-redirect-location

Versionierung

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

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

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

- `x-amz-server-side-encryption-customer-algorithm`: Angeben `AES256` .
- `x-amz-server-side-encryption-customer-key`: Geben Sie Ihren Verschlüsselungsschlüssel für das Objekt an.
- `x-amz-server-side-encryption-customer-key-MD5`: Geben Sie den MD5-Digest des Verschlüsselungsschlüssels des Objekts an.

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

Verhalten von GetObject für Cloud Storage Pool-Objekte

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

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

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

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

Mehrteilige oder segmentierte Objekte in einem Cloud-Speicherpool

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

In diesen Fällen:

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

GetObject und Cross-Grid-Replikation

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

Netz	Replikationsstatus
Quelle	<ul style="list-style-type: none"> ABGESCHLOSSEN: Die Replikation war erfolgreich. AUSSTEHEND: Das Objekt wurde noch nicht repliziert. FEHLER: Die Replikation ist mit einem dauerhaften Fehler fehlgeschlagen. Der Fehler muss von einem Benutzer behoben werden.
Ziel	REPLICA: Das Objekt wurde aus dem Quellraster repliziert.



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

HeadObject

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

Übergangszustand des Objekts zu bestimmen.

HeadObject und mehrteilige Objekte

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

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

UTF-8-Zeichen in Benutzermetadaten

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

Unterstützter Anforderungsheader

Der folgende Anforderungsheader wird unterstützt:

- `x-amz-checksum-mode`

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

Nicht unterstützter Anforderungsheader

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

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

Versionierung

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

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

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

- `x-amz-server-side-encryption-customer-algorithm`: Angeben `AES256` .
- `x-amz-server-side-encryption-customer-key`: Geben Sie Ihren Verschlüsselungsschlüssel für das Objekt an.
- `x-amz-server-side-encryption-customer-key-MD5`: Geben Sie den MD5-Digest des Verschlüsselungsschlüssels des Objekts an.



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

HeadObject-Antworten für Cloud Storage Pool-Objekte

Wenn das Objekt in einem "[Cloud-Speicherpool](#)" werden die folgenden Antwortheader zurückgegeben:

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

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

Zustand des Objekts	Antwort auf HeadObject
In StorageGRID aufgenommenes, aber noch nicht von ILM ausgewertetes Objekt oder Objekt, das in einem herkömmlichen Speicherpool oder mithilfe von Erasure Coding gespeichert ist	200 OK (Es wird kein spezieller Antwortheader zurückgegeben.)
Objekt im Cloud-Speicherpool, aber noch nicht in einen nicht abrufbaren Zustand übergegangen	200 OK <code>x-amz-storage-class: GLACIER</code> <code>x-amz-restore: ongoing-request="false", expiry-date="Sat, 23 July 20 2030 00:00:00 GMT"</code> Bis das Objekt in einen nicht abrufbaren Zustand überführt wird, ist der Wert für <code>expiry-date</code> auf einen fernen Zeitpunkt in der Zukunft festgelegt. Der genaue Zeitpunkt des Übergangs wird vom StorageGRID -System nicht gesteuert.

Zustand des Objekts	Antwort auf HeadObject
Das Objekt ist in den nicht abrufbaren Zustand übergegangen, aber mindestens eine Kopie ist auch im Raster vorhanden	<p>200 OK</p> <p>x-amz-storage-class: GLACIER</p> <p>x-amz-restore: ongoing-request="false", expiry-date="Sat, 23 July 20 2030 00:00:00 GMT"</p> <p>Der Wert für expiry-date ist auf einen fernen Zeitpunkt in der Zukunft festgelegt.</p> <p>Hinweis: Wenn die Kopie im Grid nicht verfügbar ist (z. B. weil ein Storage Node ausgefallen ist), müssen Sie eine "RestoreObject" Fordern Sie die Wiederherstellung der Kopie aus dem Cloud-Speicherpool an, bevor Sie das Objekt erfolgreich abrufen können.</p>
Das Objekt ist in einen nicht abrufbaren Zustand übergegangen und es ist keine Kopie im Raster vorhanden	<p>200 OK</p> <p>x-amz-storage-class: GLACIER</p>
Objekt wird gerade aus einem nicht abrufbaren Zustand wiederhergestellt	<p>200 OK</p> <p>x-amz-storage-class: GLACIER</p> <p>x-amz-restore: ongoing-request="true"</p>
Objekt vollständig im Cloud-Speicherpool wiederhergestellt	<p>200 OK</p> <p>x-amz-storage-class: GLACIER</p> <p>x-amz-restore: ongoing-request="false", expiry-date="Sat, 23 July 20 2018 00:00:00 GMT"</p> <p>Der expiry-date gibt an, wann das Objekt im Cloud-Speicherpool in einen nicht abrufbaren Zustand zurückversetzt wird.</p>

Mehrteilige oder segmentierte Objekte im Cloud Storage Pool

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

HeadObject und Cross-Grid-Replikation

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

Netz	Replikationsstatus
Quelle	<ul style="list-style-type: none">ABGESCHLOSSEN: Die Replikation war erfolgreich.AUSSTEHEND: Das Objekt wurde noch nicht repliziert.FEHLER: Die Replikation ist mit einem dauerhaften Fehler fehlgeschlagen. Der Fehler muss von einem Benutzer behoben werden.
Ziel	REPLICA : Das Objekt wurde aus dem Quellraster repliziert.



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

PutObject

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

Konflikte lösen

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

Objektgröße

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

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



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

Größe der Benutzermetadaten

Amazon S3 begrenzt die Größe benutzerdefinierter Metadaten innerhalb jedes PUT-Anforderungsheaders auf 2 KB. StorageGRID begrenzt Benutzermetadaten auf 24 KiB. Die Größe benutzerdefinierter Metadaten wird gemessen, indem die Summe der Anzahl der Bytes in der UTF-8-Kodierung jedes Schlüssels und Werts

berechnet wird.

UTF-8-Zeichen in Benutzermetadaten

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

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

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

Objekt-Tag-Grenzwerte

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

Objektbesitz

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

Unterstützte Anforderungsheader

Die folgenden Anforderungsheader werden unterstützt:

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

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

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

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

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

Verwenden Sie beim Angeben des Name-Wert-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 `creation-time` als Name der Metadaten, die aufzeichnen, wann das Objekt erstellt wurde. Beispiel:

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

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



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

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

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

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

Sehen [Anforderungsheader für serverseitige Verschlüsselung](#)

Nicht unterstützte Anforderungsheader

Die folgenden Anforderungsheader werden nicht unterstützt:

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

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

Speicherklassenoptionen

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

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

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

- STANDARD(Standard)

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

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

- REDUCED_REDUNDANCY

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

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

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

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

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

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

Anforderungsheader für serverseitige Verschlüsselung

Sie können die folgenden Anforderungsheader verwenden, um ein Objekt mit serverseitiger Verschlüsselung zu verschlüsseln. Die Optionen SSE und SSE-C schließen sich gegenseitig aus.

- **SSE:** Verwenden Sie den folgenden Header, wenn Sie das Objekt mit einem eindeutigen, von StorageGRID verwalteten Schlüssel verschlüsseln möchten.

◦ `x-amz-server-side-encryption`

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

- **SSE-C:** Verwenden Sie alle drei Header, wenn Sie das Objekt mit einem eindeutigen Schlüssel verschlüsseln möchten, den Sie bereitstellen und verwalten.

◦ `x-amz-server-side-encryption-customer-algorithm`: Angeben AES256 .

◦ `x-amz-server-side-encryption-customer-key`: Geben Sie Ihren Verschlüsselungsschlüssel für das neue Objekt an.

◦ `x-amz-server-side-encryption-customer-key-MD5`: Geben Sie den MD5-Digest des Verschlüsselungsschlüssels des neuen Objekts an.

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

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

Versionierung

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

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

Signaturberechnungen für den Autorisierungsheader

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

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



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

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

Ähnliche Informationen

- "[Objekte mit ILM verwalten](#)"
- "[Amazon Simple Storage Service API-Referenz: PutObject](#)"

RestoreObject

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

Unterstützter Anfragetyp

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

Versionierung

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

Verhalten von `RestoreObject` bei Cloud Storage Pool-Objekten

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



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

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

`SelectObjectContent`

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

Weitere Informationen finden Sie unter ["Amazon Simple Storage Service API-Referenz: SelectObjectContent"](#).

Bevor Sie beginnen

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

Beispiel für die CSV-Anforderungssyntax

```

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

```

Beispiel für die Parquet-Anforderungssyntax

```

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

```

SQL-Abfragebeispiel

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

```

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

```

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

```

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

```

AWS-CLI-Nutzungsbeispiel (CSV)

```

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

```

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

```

Alabama,4779736,4854803,1.5705260708959658022953568983726297854
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

```

AWS-CLI-Nutzungsbeispiel (Parquet)

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

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

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

Vorgänge für mehrteilige Uploads

Vorgänge für mehrteilige Uploads

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

Für alle mehrteiligen Uploadvorgänge gelten die folgenden Bedingungen und Hinweise:

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

- Wenn sich ILM während eines laufenden S3-Multipart-Uploads ändert, erfüllen einige Teile des Objekts nach Abschluss des Multipart-Uploads möglicherweise nicht die aktuellen ILM-Anforderungen. Alle Teile, die nicht richtig platziert sind, werden zur erneuten ILM-Bewertung in die Warteschlange gestellt und später an die richtige Position verschoben.
- Bei der Auswertung von ILM für ein Teil filtert StorageGRID nach der Größe des Teils, nicht nach der Größe des Objekts. Dies bedeutet, dass Teile eines Objekts an Orten gespeichert werden können, die die ILM-Anforderungen für das gesamte Objekt nicht erfüllen. Wenn beispielsweise eine Regel angibt, dass alle Objekte mit 10 GB oder mehr bei DC1 gespeichert werden, während alle kleineren Objekte bei DC2 gespeichert werden, wird jeder 1-GB-Teil eines 10-teiligen mehrteiligen Uploads bei der Aufnahme bei DC2 gespeichert. Wenn ILM jedoch für das gesamte Objekt ausgewertet wird, werden alle Teile des Objekts nach DC1 verschoben.
- Alle mehrteiligen Upload-Vorgänge unterstützen StorageGRID "[Konsistenzwerte](#)" .
- Wenn ein Objekt per mehrteiligem Upload aufgenommen wird, "[Schwellenwert für Objektsegmentierung \(1 GiB\)](#)" wird nicht angewendet.
- Bei Bedarf können Sie "[serverseitige Verschlüsselung](#)" mit mehrteiligen Uploads. Um SSE (serverseitige Verschlüsselung mit StorageGRID-verwalteten Schlüsseln) zu verwenden, schließen Sie die `x-amz-server-side-encryption` Anforderungsheader nur in der `CreateMultipartUpload`-Anforderung. Um SSE-C (serverseitige Verschlüsselung mit vom Kunden bereitgestellten Schlüsseln) zu verwenden, geben Sie in der `CreateMultipartUpload`-Anforderung und in jeder nachfolgenden `UploadPart`-Anforderung dieselben drei Anforderungsheader für Verschlüsselungsschlüssel an.

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

CompleteMultipartUpload

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



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

Konflikte lösen

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

Unterstützte Anforderungsheader

Die folgenden Anforderungsheader werden unterstützt:

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

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

- `STANDARD`

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

- `REDUCED_REDUNDANCY`

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



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



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



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

Nicht unterstützte Anforderungsheader

Die folgenden Anforderungsheader werden nicht unterstützt:

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

Versionierung

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

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

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

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

Fehlgeschlagene Replikation, Benachrichtigung oder Metadatenbenachrichtigung

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

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

Weitere Informationen finden Sie unter ["Fehlerbehebung bei Plattformdiensten"](#).

CreateMultipartUpload

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

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

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

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

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

werden.

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

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

- **REDUCED_REDUNDANCY**

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

Verwenden des `REDUCED_REDUNDANCY` Unter anderen Umständen wird diese Option nicht empfohlen.

`REDUCED_REDUNDANCY` erhöht das Risiko eines Objektdatenverlusts während der Aufnahme.

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

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

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

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

Unterstützte Anforderungsheader

Die folgenden Anforderungsheader werden unterstützt:

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

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

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

Verwenden Sie beim Angeben des Name-Wert-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 creation-time als Name der Metadaten, die aufzeichnen, wann das Objekt erstellt wurde. Beispiel:

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

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



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

- S3 Object Lock-Anforderungsheader:

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

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

["Verwenden Sie die S3 REST API, um S3 Object Lock zu konfigurieren"](#)

- SSE-Anforderungsheader:

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

[Anforderungsheader für serverseitige Verschlüsselung](#)



Informationen zur Verarbeitung von UTF-8-Zeichen durch StorageGRID finden Sie unter ["PutObject"](#) .

[Anforderungsheader für serverseitige Verschlüsselung](#)

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

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

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

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

Nicht unterstützte Anforderungsheader

Der folgende Anforderungsheader wird nicht unterstützt:

- x-amz-website-redirect-location

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

Versionierung

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

ListMultipartUploads

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

Die folgenden Anforderungsparameter werden unterstützt:

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

- Date
- Authorization

Versionierung

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

UploadPart

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

Unterstützte Anforderungsheader

Die folgenden Anforderungsheader werden unterstützt:

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

Anforderungsheader für serverseitige Verschlüsselung

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

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

 Die von Ihnen bereitgestellten Verschlüsselungsschlüssel werden niemals gespeichert. Wenn Sie einen Verschlüsselungsschlüssel verlieren, verlieren Sie das entsprechende Objekt. Bevor Sie vom Kunden bereitgestellte Schlüssel zum Sichern von Objektdaten verwenden, lesen Sie die Hinweise in „[Verwenden Sie serverseitige Verschlüsselung](#)“.

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

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

Nicht unterstützte Anforderungsheader

Die folgenden Anforderungsheader werden nicht unterstützt:

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

Versionierung

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

UploadPartCopy

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

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

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

Die folgenden Anforderungsheader werden unterstützt:

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

Anforderungsheader für serverseitige Verschlüsselung

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

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

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

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

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

Versionierung

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

Fehlerantworten

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

Unterstützte S3-API-Fehlercodes

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

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

Benutzerdefinierte StorageGRID -Fehlercodes

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

Benutzerdefinierte StorageGRID -Vorgänge

Benutzerdefinierte StorageGRID -Vorgänge

Das StorageGRID -System unterstützt benutzerdefinierte Vorgänge, die der 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.

Betrieb	Beschreibung
"PUT Bucket-Konsistenz"	Legt die Konsistenz fest, die auf einen bestimmten Bucket angewendet wird.
"GET Bucket – Letzte Zugriffszeit"	Gibt zurück, ob Aktualisierungen der letzten Zugriffszeit für einen bestimmten Bucket aktiviert oder deaktiviert sind.
"PUT Bucket: Letzte Zugriffszeit"	Ermöglicht Ihnen, Aktualisierungen der letzten Zugriffszeit für einen bestimmten Bucket zu aktivieren oder zu deaktivieren.
"Konfiguration der Benachrichtigung über DELETE-Bucket-Metadaten"	Löscht die XML-Metadatenbenachrichtigungskonfiguration, die einem bestimmten Bucket zugeordnet ist.
"GET Bucket-Metadaten-Benachrichtigungskonfiguration"	Gibt die XML-Konfigurationsdatei für Metadatenbenachrichtigungen zurück, die einem bestimmten Bucket zugeordnet ist.
"Konfiguration der Benachrichtigung über PUT-Bucket-Metadaten"	Konfiguriert den Metadaten-Benachrichtigungsdienst für einen Bucket.
"GET-Speichernutzung"	Gibt die Gesamtspeichermenge an, die von einem Konto und jedem mit dem Konto verknüpften Bucket verwendet wird.
"Veraltet: CreateBucket mit Compliance-Einstellungen"	Veraltet und nicht unterstützt: Sie können keine neuen Buckets mehr erstellen, wenn Compliance aktiviert ist.
"Veraltet: GET Bucket-Konformität"	Veraltet, aber unterstützt: Gibt die aktuell gültigen Compliance-Einstellungen für einen vorhandenen Legacy-Compliant-Bucket zurück.
"Veraltet: PUT-Bucket-Konformität"	Veraltet, aber unterstützt: Ermöglicht Ihnen, die Compliance-Einstellungen für einen vorhandenen Legacy-Compliant-Bucket zu ändern.

GET Bucket-Konsistenz

Mit der Anforderung „GET Bucket Consistency“ können Sie die Konsistenz ermitteln, die auf einen bestimmten Bucket angewendet wird.

Die Standardkonsistenz ist so eingestellt, dass für neu erstellte Objekte das Lesen nach dem Schreiben gewährleistet ist.

Sie müssen über die Berechtigung s3:GetBucketConsistency verfügen oder Root-Kontoinhaber sein, um diesen Vorgang abzuschließen.

Anforderungsbeispiel

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

Antwort

In der Antwort-XML <Consistency> gibt einen der folgenden Werte zurück:

Konsistenz	Beschreibung
alle	Alle Knoten empfangen die Daten sofort, andernfalls schlägt die Anforderung fehl.
stark-global	Garantiert Lese- und Schreibkonsistenz für alle Clientanforderungen auf allen Sites.
starke Site	Garantiert die Lese- und Schreibkonsistenz für alle Clientanforderungen innerhalb einer Site.
Lesen nach neuem Schreiben	(Standard) Bietet Read-After-Write-Konsistenz für neue Objekte und letztendliche Konsistenz für Objektaktualisierungen. Bietet hohe Verfügbarkeit und Datenschutzgarantien. Für die meisten Fälle empfohlen.
verfügbar	Bietet letztendliche Konsistenz sowohl für neue Objekte als auch für Objektaktualisierungen. Verwenden Sie es für S3-Buckets nur nach Bedarf (z. B. für einen Bucket, der Protokollwerte enthält, die selten gelesen werden, oder für HEAD- oder GET-Operationen für nicht vorhandene Schlüssel). Wird für S3 FabricPool Buckets nicht unterstützt.

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>
```

Ähnliche Informationen

["Konsistenzwerte"](#)

PUT Bucket-Konsistenz

Mit der PUT-Bucket-Konsistenzanforderung können Sie die Konsistenz angeben, die auf Vorgänge angewendet werden soll, die an einem Bucket ausgeführt werden.

Die Standardkonsistenz ist so eingestellt, dass für neu erstellte Objekte das Lesen nach dem Schreiben gewährleistet ist.

Bevor Sie beginnen

Sie müssen über die Berechtigung „s3:PutBucketConsistency“ verfügen oder Root-Kontoinhaber sein, um diesen Vorgang abzuschließen.

Anfrage

Der `x-ntap-sg-consistency` Der Parameter muss einen der folgenden Werte enthalten:

Konsistenz	Beschreibung
alle	Alle Knoten empfangen die Daten sofort, andernfalls schlägt die Anforderung fehl.
stark-global	Garantiert Lese- und Schreibkonsistenz für alle Clientanforderungen auf allen Sites.
starke Site	Garantiert die Lese- und Schreibkonsistenz für alle Clientanforderungen innerhalb einer Site.
Lesen nach neuem Schreiben	(Standard) Bietet Read-After-Write-Konsistenz für neue Objekte und letztendliche Konsistenz für Objektaktualisierungen. Bietet hohe Verfügbarkeit und Datenschutzgarantien. Für die meisten Fälle empfohlen.
verfügbar	Bietet letztendliche Konsistenz sowohl für neue Objekte als auch für Objektaktualisierungen. Verwenden Sie es für S3-Buckets nur nach Bedarf (z. B. für einen Bucket, der Protokollwerte enthält, die selten gelesen werden, oder für HEAD- oder GET-Operationen für nicht vorhandene Schlüssel). Wird für S3 FabricPool Buckets nicht unterstützt.

Hinweis: Im Allgemeinen sollten Sie die Konsistenz „Lesen nach neuem Schreiben“ verwenden. Wenn Anfragen nicht richtig funktionieren, ändern Sie nach Möglichkeit das Verhalten des Anwendungsclients. Oder konfigurieren Sie den Client so, dass die Konsistenz für jede API-Anforderung angegeben wird. Stellen Sie die Konsistenz auf Eimerebene nur als letztes Mittel ein.

Anforderungsbeispiel

```
PUT /bucket?x-ntap-sg-consistency=strong-global HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

Ähnliche Informationen

["Konsistenzwerte"](#)

GET Bucket – Letzte Zugriffszeit

Mit der Anforderung „GET Bucket last access time“ können Sie feststellen, ob Aktualisierungen der letzten Zugriffszeit für einzelne Buckets aktiviert oder deaktiviert sind.

Sie müssen über die Berechtigung s3:GetBucketLastAccessTime verfügen oder Root-Kontobenutzer sein, 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 Aktualisierungen 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: Letzte Zugriffszeit

Mit der Anforderung „PUT Bucket Last Access Time“ können Sie Aktualisierungen der letzten Zugriffszeit für einzelne Buckets aktivieren oder deaktivieren. Das Deaktivieren der Aktualisierung der letzten Zugriffszeit verbessert die Leistung und ist die

Standardeinstellung für alle Buckets, die mit Version 10.3.0 oder höher erstellt wurden.

Sie müssen über die Berechtigung s3:PutBucketLastAccessTime für einen Bucket verfügen oder Konto-Root sein, um diesen Vorgang abzuschließen.

Ab StorageGRID Version 10.3 sind Aktualisierungen der letzten Zugriffszeit für alle neuen Buckets standardmäßig deaktiviert. Wenn Sie Buckets haben, die mit einer früheren Version von StorageGRID erstellt wurden, und Sie das neue Standardverhalten übernehmen möchten, müssen Sie die Aktualisierung der letzten Zugriffszeit für jeden dieser früheren Buckets explizit deaktivieren. Sie können Aktualisierungen der letzten Zugriffszeit mithilfe der Anforderung „PUT Bucket-Letzte Zugriffszeit“ oder auf der Detailseite für einen Bucket im Mandanten-Manager aktivieren oder deaktivieren. Sehen ["Aktivieren oder Deaktivieren der Aktualisierung der letzten Zugriffszeit"](#).

Wenn die Aktualisierung der letzten Zugriffszeit für einen Bucket deaktiviert ist, wird das folgende Verhalten auf Vorgänge im Bucket angewendet:

- GetObject-, GetObjectAcl-, GetObjectTagging- und HeadObject-Anfragen aktualisieren die letzte Zugriffszeit nicht. Das Objekt wird nicht zu Warteschlangen für die Auswertung des Information Lifecycle Management (ILM) hinzugefügt.
- CopyObject- und PutObjectTagging-Anfragen, die nur die Metadaten aktualisieren, aktualisieren auch die letzte Zugriffszeit. Das Objekt wird zur ILM-Auswertung zu Warteschlangen hinzugefügt.
- Wenn Aktualisierungen der letzten Zugriffszeit für den Quell-Bucket deaktiviert sind, aktualisieren CopyObject-Anfragen die letzte Zugriffszeit für den Quell-Bucket nicht. Das kopierte Objekt wird nicht zu den Warteschlangen für die ILM-Auswertung für den Quell-Bucket hinzugefügt. Für das Ziel aktualisieren CopyObject-Anfragen jedoch immer die letzte Zugriffszeit. Die Kopie des Objekts wird zur ILM-Auswertung zu Warteschlangen hinzugefügt.
- CompleteMultipartUpload-Anfragen aktualisieren die letzte Zugriffszeit. Das fertige Objekt wird zur ILM-Auswertung in die Warteschlangen aufgenommen.

Anforderungsbeispiele

Dieses Beispiel aktiviert die letzte Zugriffszeit für einen Bucket.

```
PUT /bucket?x-ntap-sg-lastaccesstime=enabled HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

Dieses Beispiel deaktiviert die letzte Zugriffszeit für einen Bucket.

```
PUT /bucket?x-ntap-sg-lastaccesstime=disabled HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

Konfiguration der Benachrichtigung über DELETE-Bucket-Metadaten

Mit der Konfigurationsanforderung „DELETE Bucket-Metadaten-Benachrichtigung“ 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 Konto-Root sein, um diesen Vorgang abzuschließen.

Anforderungsbeispiel

Dieses Beispiel zeigt das Deaktivieren des Suchintegrationsdienstes für einen Bucket.

```
DELETE /test1?x-ntap-sg-metadata-notification HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

GET Bucket-Metadaten-Benachrichtigungskonfiguration

Mit der Konfigurationsanforderung „GET Bucket-Metadatenbenachrichtigung“ können Sie die Konfigurations-XML abrufen, die zum Konfigurieren der Suchintegration für einzelne Buckets verwendet wird.

Sie müssen über die Berechtigung s3:GetBucketMetadataNotification verfügen oder Root-Kontoinhaber sein, um diesen Vorgang abzuschließen.

Anforderungsbeispiel

Diese Anfrage ruft die Metadaten-Benachrichtigungskonfiguration für den Bucket mit dem Namen ab. bucket .

```
GET /bucket?x-ntap-sg-metadata-notification HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

Antwort

Der Antworttext enthält die Metadatenbenachrichtigungskonfiguration für den Bucket. Mit der Konfiguration der Metadatenbenachrichtigung können Sie festlegen, wie der Bucket für die Suchintegration konfiguriert wird. Das heißt, Sie können feststellen, welche Objekte indiziert werden 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 Metadatenbenachrichtigungskonfiguration umfasst eine oder mehrere Regeln. Jede Regel gibt die Objekte an, auf die sie angewendet wird, und das Ziel, an das StorageGRID Objektmetadaten senden soll. Ziele müssen mithilfe der URN eines StorageGRID Endpunkts angegeben werden.

Name	Beschreibung	Erforderlich
Metadatenbenachrichtigungskonfiguration	Container-Tag für Regeln, die zum Angeben der Objekte und des Ziels für Metadatenbenachrichtigungen verwendet werden. Enthält ein oder mehrere Regelemente.	Ja
Regel	Container-Tag für eine Regel, die die Objekte identifiziert, deren Metadaten einem angegebenen Index hinzugefügt werden sollen. Regeln mit überlappenden Präfixen werden abgelehnt. Im MetadataNotificationConfiguration-Element enthalten.	Ja
AUSWEIS	Eindeutige Kennung für die Regel. Im Regelement enthalten.	Nein
Status	Der Status kann „Aktiviert“ oder „Deaktiviert“ sein. Für deaktivierte Regeln werden keine Maßnahmen ergriffen. Im Regelement enthalten.	Ja

Name	Beschreibung	Erforderlich
Präfix	<p>Objekte, die dem Präfix entsprechen, sind von der Regel betroffen und ihre Metadaten werden an das angegebene Ziel gesendet.</p> <p>Um alle Objekte abzugleichen, geben Sie ein leeres Präfix an.</p> <p>Im Regelement enthalten.</p>	Ja
Ziel	<p>Container-Tag für das Ziel einer Regel.</p> <p>Im Regelement enthalten.</p>	Ja
Urne	<p>URN des Ziels, an das die Objektmetadaten gesendet werden. Muss die URN eines StorageGRID-Endpunkts mit den folgenden Eigenschaften sein:</p> <ul style="list-style-type: none"> • `es` muss das dritte Element sein. • Die URN muss mit dem Index und Typ enden, in dem die Metadaten gespeichert sind, in der Form <code>domain-name/myindex/mytype</code>. <p>Endpunkte werden mithilfe des Tenant Managers oder der Tenant Management API konfiguriert. Sie haben folgende Form:</p> <ul style="list-style-type: none"> • <code>arn:aws:es:_region:account-ID_:domain/mydomain/myindex/mytype</code> • <code>urn:mysite:es:::mydomain/myindex/mytype</code> <p>Der Endpunkt muss konfiguriert werden, bevor die Konfigurations-XML übermittelt wird, andernfalls schlägt die Konfiguration mit einem 404-Fehler fehl.</p> <p>Die Urne ist im Zielelement enthalten.</p>	Ja

Antwortbeispiel

Das XML, das zwischen den

`<MetadataNotificationConfiguration></MetadataNotificationConfiguration>` Tags zeigen, wie die Integration mit einem Suchintegrationsendpunkt für den Bucket konfiguriert ist. In diesem Beispiel werden Objektmetadaten an einen Elasticsearch-Index namens gesendet. `current` und geben Sie den Namen ein 2017 das in einer AWS-Domäne namens 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>

```

Ähnliche Informationen

["Verwenden eines Mandantenkontos"](#)

Konfiguration der Benachrichtigung über PUT-Bucket-Metadaten

Mit der Konfigurationsanforderung für die Benachrichtigung über PUT-Bucket-Metadaten können Sie den Suchintegrationsdienst für einzelne Buckets aktivieren. Die XML-Konfigurations-XML für die Metadatenbenachrichtigung, die Sie im Anforderungstext angeben, gibt die Objekte an, deren Metadaten an den Zielsuchindex gesendet werden.

Sie müssen über die Berechtigung s3:PutBucketMetadataNotification für einen Bucket verfügen oder Konto-Root sein, um diesen Vorgang abzuschließen.

Anfrage

Die Anfrage muss die Metadatenbenachrichtigungskonfiguration im Anfragetext enthalten. Jede Metadatenbenachrichtigungskonfiguration umfasst eine oder mehrere Regeln. Jede Regel gibt die Objekte an, auf die sie angewendet wird, und das Ziel, an das StorageGRID Objektmetadaten senden soll.

Objekte können nach dem Präfix des Objektnamens gefiltert werden. Beispielsweise könnten Sie Metadaten für Objekte mit dem Präfix /images zu einem Ziel und Objekte mit dem Präfix /videos zu einem anderen.

Konfigurationen mit überlappenden Präfixen sind ungültig und werden bei der Übermittlung abgelehnt. Beispielsweise eine Konfiguration, die eine Regel für Objekte mit dem Präfix test und eine zweite Regel für Objekte mit dem Präfix test2 wäre nicht erlaubt.

Ziele müssen mithilfe der URN eines StorageGRID Endpunkts angegeben werden. Der Endpunkt muss vorhanden sein, wenn die Konfiguration der Metadatenbenachrichtigung übermittelt wird, sonst schlägt die

Anfrage fehl, da 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:account-
ID:domain/mydomain/myindex/mytype</Urn>
    </Destination>
  </Rule>
  <Rule>
    <ID>Rule-2</ID>
    ...
  </Rule>
  ...
</MetadataNotificationConfiguration>
```

Die Tabelle beschreibt die Elemente in der XML-Konfiguration der Metadatenbenachrichtigung.

Name	Beschreibung	Erforderlich
Metadatenbenachrichtigungskonfiguration	Container-Tag für Regeln, die zum Angeben der Objekte und des Ziels für Metadatenbenachrichtigungen verwendet werden. Enthält ein oder mehrere Regelelemente.	Ja
Regel	Container-Tag für eine Regel, die die Objekte identifiziert, deren Metadaten einem angegebenen Index hinzugefügt werden sollen. Regeln mit überlappenden Präfixen werden abgelehnt. Im MetadataNotificationConfiguration-Element enthalten.	Ja
AUSWEIS	Eindeutige Kennung für die Regel. Im Regelement enthalten.	Nein

Name	Beschreibung	Erforderlich
Status	<p>Der Status kann „Aktiviert“ oder „Deaktiviert“ sein. Für deaktivierte Regeln werden keine Maßnahmen ergriffen.</p> <p>Im Regelement enthalten.</p>	Ja
Präfix	<p>Objekte, die dem Präfix entsprechen, sind von der Regel betroffen und ihre Metadaten werden an das angegebene Ziel gesendet.</p> <p>Um alle Objekte abzulegen, geben Sie ein leeres Präfix an.</p> <p>Im Regelement enthalten.</p>	Ja
Ziel	<p>Container-Tag für das Ziel einer Regel.</p> <p>Im Regelement enthalten.</p>	Ja
Urne	<p>URN des Ziels, an das die Objektmetadaten gesendet werden. Muss die URN eines StorageGRID-Endpunkts mit den folgenden Eigenschaften sein:</p> <ul style="list-style-type: none"> • `es` muss das dritte Element sein. • Die URN muss mit dem Index und Typ enden, in dem die Metadaten gespeichert sind, in der Form domain-name/myindex/mytype . <p>Endpunkte werden mithilfe des Tenant Managers oder der Tenant Management API konfiguriert. Sie haben folgende Form:</p> <ul style="list-style-type: none"> • arn:aws:es:region:account-ID:domain/mydomain/myindex/mytype • urn:mysite:es:::mydomain/myindex/mytype <p>Der Endpunkt muss konfiguriert werden, bevor die Konfigurations-XML übermittelt wird, andernfalls schlägt die Konfiguration mit einem 404-Fehler fehl.</p> <p>Die Urne ist im Zielelement enthalten.</p>	Ja

Anforderungsbeispiele

Dieses Beispiel zeigt die Aktivierung der Suchintegration 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 verwendet, die mit dem Präfix `/images` wird an ein Ziel gesendet, während Objektmetadaten für Objekte, die dem Präfix entsprechen `/videos` wird an ein zweites Ziel gesendet.

```

PUT /graphics?x-ntap-sg-metadata-notification HTTP/1.1
Date: date
Authorization: authorization string
Host: host

<MetadataNotificationConfiguration>
  <Rule>
    <ID>Images-rule</ID>
    <Status>Enabled</Status>
    <Prefix>/images</Prefix>
    <Destination>
      <Urn>arn:aws:es:us-east-1:3333333:domain/es-
domain/graphics/imagetype</Urn>
    </Destination>
  </Rule>
  <Rule>
    <ID>Videos-rule</ID>
    <Status>Enabled</Status>
    <Prefix>/videos</Prefix>
    <Destination>
      <Urn>arn:aws:es:us-west-1:2222222:domain/es-
domain/graphics/videotype</Urn>
    </Destination>
  </Rule>
</MetadataNotificationConfiguration>

```

Vom Suchintegrationsdienst generiertes JSON

Wenn Sie den Suchintegrationsdienst für einen Bucket aktivieren, wird jedes Mal, wenn Objektmetadaten oder Tags hinzugefügt, aktualisiert oder gelöscht werden, ein JSON-Dokument generiert und an den Zielendpunkt gesendet.

Dieses Beispiel zeigt ein Beispiel des JSON, das generiert werden könnte, wenn ein Objekt mit dem Schlüssel SGWS/Tagging.txt wird in einem Bucket namens erstellt test. Der test Bucket ist nicht versioniert, also die `versionId`-Tag ist leer.

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

In Metadatenbenachrichtigungen enthaltene Objektmetadaten

In der Tabelle sind alle Felder aufgeführt, die im JSON-Dokument enthalten sind, das an den Zielendpunkt gesendet wird, wenn die Suchintegration aktiviert ist.

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

Typ	Artikelname	Beschreibung
Bucket- und Objektinformationen	Eimer	Name des Buckets
Bucket- und Objektinformationen	Schlüssel	Objektschlüsselname
Bucket- und Objektinformationen	Versions-ID	Objektversion für Objekte in versionierten Buckets
Bucket- und Objektinformationen	Region	Bucket-Region, zum Beispiel us-east-1
Systemmetadaten	Größe	Objektgröße (in Bytes), wie sie für einen HTTP-Client sichtbar ist
Systemmetadaten	md5	Objekt-Hash
Benutzermetadaten	Metadaten key:value	Alle Benutzermetadaten für das Objekt als Schlüssel-Wert-Paare
Schlagwörter	Schlagworte key:value	Alle für das Objekt definierten Objekt-Tags als Schlüssel-Wert-Paare

 Für Tags und Benutzermetadaten übergibt StorageGRID Daten und Zahlen als Zeichenfolgen oder als S3-Ereignisbenachrichtigungen an Elasticsearch. Um Elasticsearch so zu konfigurieren, dass diese Zeichenfolgen als Datumsangaben oder Zahlen interpretiert werden, befolgen Sie die Elasticsearch-Anweisungen zur dynamischen Feldzuordnung und zur 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.

Ähnliche Informationen

["Verwenden eines Mandantenkontos"](#)

GET-Speichernutzungsanforderung

Die Anforderung „GET Storage Usage“ gibt Auskunft über die Gesamtmenge des von einem Konto und jedem mit dem Konto verknüpften Bucket verwendeten Speichers.

Die Menge des von einem Konto und seinen Buckets verwendeten Speichers kann durch eine modifizierte ListBuckets-Anfrage mit dem `x-ntap-sg-usage` Abfrageparameter. Die Bucket-Speichernutzung wird getrennt von den vom System verarbeiteten PUT- und DELETE-Anfragen verfolgt. Es kann zu einer gewissen Verzögerung kommen, bevor die Nutzungswerte den erwarteten Werten auf Grundlage der Verarbeitung von Anfragen entsprechen, insbesondere wenn das System stark ausgelastet ist.

Standardmäßig versucht StorageGRID , Nutzungsinformationen mithilfe einer starken globalen Konsistenz abzurufen. Wenn keine starke globale Konsistenz erreicht werden kann, versucht StorageGRID , die Nutzungsinformationen mit einer starken Site-Konsistenz abzurufen.

Sie müssen über die Berechtigung `s3>ListAllMyBuckets` verfügen oder Root-Kontoinhaber sein, um diesen Vorgang abzuschließen.

Anforderungsbeispiel

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

Antwortbeispiel

Dieses Beispiel zeigt ein Konto mit vier Objekten und 12 Byte Daten in zwei Buckets. 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 dazu bei, ObjectCount Und DataBytes Werte in der Antwort. Löschmarkierungen werden nicht hinzugefügt zum ObjectCount gesamt.

Ähnliche Informationen

["Konsistenzwerte"](#)

Veraltete Bucket-Anfragen für Legacy-Compliance

Veraltete Bucket-Anfragen für Legacy-Compliance

Möglicherweise müssen Sie die StorageGRID S3 REST-API verwenden, um Buckets zu verwalten, die mit der alten Compliance-Funktion erstellt wurden.

Compliance-Funktion veraltet

Die StorageGRID Compliance-Funktion, die in früheren StorageGRID Versionen verfügbar war, ist veraltet und wurde durch S3 Object Lock ersetzt.

Wenn Sie zuvor die globale Compliance-Einstellung aktiviert haben, ist die globale S3-Objektsperreinstellung in StorageGRID 11.6 aktiviert. Sie können keine neuen Buckets mehr erstellen, wenn Compliance aktiviert ist. Bei Bedarf können Sie jedoch die StorageGRID S3 REST API verwenden, um vorhandene ältere konforme Buckets zu verwalten.

- ["Verwenden Sie die S3 REST API, um S3 Object Lock zu konfigurieren"](#)
- ["Objekte mit ILM verwalten"](#)
- ["NetApp Knowledge Base: So verwalten Sie ältere konforme Buckets in StorageGRID 11.5"](#)

Veraltete Compliance-Anfragen:

- ["Veraltet – PUT-Bucket-Anforderungsänderungen zur Einhaltung der Vorschriften"](#)

Das XML-Element SGCompliance ist veraltet. Bisher konnten Sie dieses benutzerdefinierte StorageGRID Element in den optionalen XML-Anforderungstext von PUT-Bucket-Anforderungen aufnehmen, um einen konformen Bucket zu erstellen.

- ["Veraltet – GET Bucket-Konformität"](#)

Die GET Bucket-Compliance-Anforderung ist veraltet. Sie können diese Anfrage jedoch weiterhin verwenden, um die aktuell geltenden Compliance-Einstellungen für einen vorhandenen Legacy-Compliant-Bucket zu ermitteln.

- ["Veraltet – PUT-Bucket-Konformität"](#)

Die PUT-Bucket-Compliance-Anforderung ist veraltet. Sie können diese Anfrage jedoch weiterhin verwenden, um die Compliance-Einstellungen für einen vorhandenen Legacy-Compliant-Bucket zu ändern. Sie können beispielsweise einen vorhandenen Bucket auf Legal Hold setzen oder seine Aufbewahrungszeit verlängern.

Veraltet: CreateBucket-Anforderungsänderungen zur Einhaltung der Vorschriften

Das XML-Element SGCompliance ist veraltet. Bisher konnten Sie dieses benutzerdefinierte StorageGRID Element in den optionalen XML-Anforderungstext von CreateBucket-Anforderungen aufnehmen, um einen konformen Bucket zu erstellen.

Die StorageGRID Compliance-Funktion, die in früheren StorageGRID Versionen verfügbar war, ist veraltet und wurde durch S3 Object Lock ersetzt. Weitere Einzelheiten finden Sie im Folgenden:



- ["Verwenden Sie die S3 REST API, um S3 Object Lock zu konfigurieren"](#)
- ["NetApp Knowledge Base: So verwalten Sie ältere konforme Buckets in StorageGRID 11.5"](#)

Sie können keine neuen Buckets mehr erstellen, wenn Compliance aktiviert ist. Die folgende Fehlermeldung wird zurückgegeben, wenn Sie versuchen, mithilfe der CreateBucket-Anforderungsänderungen für die Konformität einen neuen konformen Bucket zu erstellen:

The Compliance feature is deprecated.

Contact your StorageGRID administrator if you need to create new Compliant buckets.

Veraltet: GET Bucket-Compliance-Anforderung

Die GET Bucket-Compliance-Anforderung ist veraltet. Sie können diese Anfrage jedoch weiterhin verwenden, um die aktuell geltenden Compliance-Einstellungen für einen vorhandenen Legacy-Compliant-Bucket zu ermitteln.

Die StorageGRID Compliance-Funktion, die in früheren StorageGRID Versionen verfügbar war, ist veraltet und wurde durch S3 Object Lock ersetzt. Weitere Einzelheiten finden Sie im Folgenden:



- ["Verwenden Sie die S3 REST API, um S3 Object Lock zu konfigurieren"](#)
- ["NetApp Knowledge Base: So verwalten Sie ältere konforme Buckets in StorageGRID 11.5"](#)

Sie müssen über die Berechtigung `s3:GetBucketCompliance` verfügen oder Root-Kontoinhaber sein, um diesen Vorgang abzuschließen.

Anforderungsbeispiel

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

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

Antwortbeispiel

In der Antwort-XML `<SGCompliance>` listet die für den Bucket geltenden Compliance-Einstellungen auf. Diese Beispielantwort zeigt die Compliance-Einstellungen für einen Bucket, in dem jedes Objekt ab dem Zeitpunkt der Aufnahme des Objekts in das Grid ein Jahr lang (525.600 Minuten) aufbewahrt wird. Für diesen Bucket besteht derzeit keine rechtliche Sperre. 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
Aufbewahrungszeit in Minuten	Die Länge der Aufbewahrungsfrist für diesen Bucket hinzugefügte Objekte in Minuten. Die Aufbewahrungsfrist beginnt, wenn das Objekt in das Raster aufgenommen wird.
LegalHold	<ul style="list-style-type: none"> • True: Dieser Bucket unterliegt derzeit einer rechtlichen Sperre. Objekte in diesem Bucket können erst gelöscht werden, wenn die rechtliche Sperre aufgehoben wird, auch wenn ihre Aufbewahrungsfrist abgelaufen ist. • Falsch: Dieser Bucket unterliegt derzeit keiner rechtlichen Sperre. Objekte in diesem Bucket können gelöscht werden, wenn ihre Aufbewahrungsfrist abgelaufen ist.
AutoDelete	<ul style="list-style-type: none"> • True: Die Objekte in diesem Bucket werden automatisch gelöscht, wenn ihre Aufbewahrungsfrist abläuft, es sei denn, der Bucket unterliegt einer rechtlichen Sperre. • Falsch: Die Objekte in diesem Bucket werden nicht automatisch gelöscht, wenn die Aufbewahrungsfrist abläuft. Sie müssen diese Objekte manuell löschen, wenn Sie sie löschen müssen.

Fehlerantworten

Wenn der Bucket nicht konform erstellt wurde, lautet der HTTP-Statuscode für die Antwort 404 Not Found , mit einem S3-Fehlercode von XNoSuchBucketCompliance .

Veraltet: PUT Bucket-Compliance-Anforderung

Die PUT-Bucket-Compliance-Anforderung ist veraltet. Sie können diese Anfrage jedoch weiterhin verwenden, um die Compliance-Einstellungen für einen vorhandenen Legacy-Compliant-Bucket zu ändern. Sie können beispielsweise einen vorhandenen Bucket auf Legal Hold setzen oder seine Aufbewahrungszeit verlängern.

Die StorageGRID Compliance-Funktion, die in früheren StorageGRID Versionen verfügbar war, ist veraltet und wurde durch S3 Object Lock ersetzt. Weitere Einzelheiten finden Sie im Folgenden:



- ["Verwenden Sie die S3 REST API, um S3 Object Lock zu konfigurieren"](#)
- ["NetApp Knowledge Base: So verwalten Sie ältere konforme Buckets in StorageGRID 11.5"](#)

Sie müssen über die Berechtigung s3:PutBucketCompliance verfügen oder Root-Kontobenutzer sein, um diesen Vorgang abzuschließen.

Sie müssen für jedes Feld der Compliance-Einstellungen einen Wert angeben, wenn Sie eine PUT-Bucket-Compliance-Anforderung stellen.

Anforderungsbeispiel

Diese Beispielanforderung ändert die Compliance-Einstellungen für den Bucket mit dem Namen `mybucket` . In diesem Beispiel werden Objekte in `mybucket` werden nun zwei Jahre (1.051.200 Minuten) statt einem Jahr

aufbewahrt, beginnend mit der Aufnahme des Objekts in das Grid. Für diesen Bucket besteht keine rechtliche Sperre. 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
Aufbewahrungszeit in Minuten	Die Länge der Aufbewahrungszeit für diesen Bucket hinzugefügte Objekte in Minuten. Die Aufbewahrungszeit beginnt, wenn das Objekt in das Raster aufgenommen wird. Wichtig Wenn Sie einen neuen Wert für RetentionPeriodMinutes angeben, müssen Sie einen Wert angeben, der gleich oder größer als die aktuelle Aufbewahrungszeit des Buckets ist. Nachdem die Aufbewahrungszeit des Buckets festgelegt wurde, können Sie diesen Wert nicht mehr verringern, sondern nur erhöhen.
LegalHold	<ul style="list-style-type: none">True: Dieser Bucket unterliegt derzeit einer rechtlichen Sperre. Objekte in diesem Bucket können erst gelöscht werden, wenn die rechtliche Sperre aufgehoben wird, auch wenn ihre Aufbewahrungszeit abgelaufen ist.Falsch: Dieser Bucket unterliegt derzeit keiner rechtlichen Sperre. Objekte in diesem Bucket können gelöscht werden, wenn ihre Aufbewahrungszeit abgelaufen ist.
AutoDelete	<ul style="list-style-type: none">True: Die Objekte in diesem Bucket werden automatisch gelöscht, wenn ihre Aufbewahrungszeit abläuft, es sei denn, der Bucket unterliegt einer rechtlichen Sperre.Falsch: Die Objekte in diesem Bucket werden nicht automatisch gelöscht, wenn die Aufbewahrungszeit abläuft. 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 gesamten Grid zu aktualisieren. Standardmäßig verwendet StorageGRID die **starke globale** Konsistenz, um zu gewährleisten, dass alle Rechenzentrumsstandorte und alle Speicherknoten, die Bucket-Metadaten enthalten, für die geänderten

Compliance-Einstellungen eine Lese-nach-Schreib-Konsistenz aufweisen.

Wenn StorageGRID die **Starke globale** Konsistenz nicht erreichen kann, weil ein Rechenzentrumsstandort 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 Speicherdienele so schnell wie möglich bereitgestellt werden. Wenn der Grid-Administrator nicht in der Lage ist, genügend Speicherknoten an jedem Standort verfügbar zu machen, weist Sie der technische Support möglicherweise an, die fehlgeschlagene Anfrage zu wiederholen, indem er die **Strong-Site**-Konsistenz erzwingt.

 Erzwingen Sie niemals die **Strong-Site**-Konsistenz für die PUT-Bucket-Konformität, es sei denn, Sie wurden vom technischen Support dazu aufgefordert und sind sich der möglichen Konsequenzen der Verwendung dieser Ebene bewusst.

Wenn die Konsistenz auf **Strong-Site** reduziert wird, garantiert StorageGRID, dass aktualisierte Compliance-Einstellungen nur für Clientanforderungen innerhalb einer Site eine Read-After-Write-Konsistenz aufweisen. Dies bedeutet, dass das StorageGRID -System vorübergehend mehrere inkonsistente Einstellungen für diesen Bucket haben könnte, bis alle Sites und Storage Nodes verfügbar sind. Die inkonsistenten Einstellungen können zu unerwartetem und unerwünschtem Verhalten führen. Wenn Sie beispielsweise einen Bucket einer rechtlichen Sperre unterziehen und eine geringere Konsistenz erzwingen, bleiben die vorherigen Compliance-Einstellungen des Buckets (d. h. die rechtliche Sperre) an einigen Rechenzentrumsstandorten möglicherweise weiterhin wirksam. Dies hat zur Folge, dass Objekte, die Ihrer Meinung nach rechtlich gesperrt sind, nach Ablauf ihrer Aufbewahrungsfrist möglicherweise gelöscht werden, entweder durch den Benutzer oder durch AutoDelete (sofern aktiviert).

Um die Verwendung der **Strong-site**-Konsistenz zu erzwingen, stellen Sie die PUT Bucket-Compliance-Anforderung erneut aus und schließen Sie die `Consistency-Control` HTTP-Anforderungsheader, wie folgt:

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

Fehlerantworten

- Wenn der Bucket nicht konform erstellt wurde, lautet der HTTP-Statuscode für die Antwort 404 Not Found .
- Wenn `RetentionPeriodMinutes` in der Anfrage kleiner ist als die aktuelle Aufbewahrungsduer des Buckets, lautet der HTTP-Statuscode 400 Bad Request .

Ähnliche Informationen

["Veraltet: PUT-Bucket-Anforderungsänderungen zur Einhaltung der Vorschriften"](#)

Bucket- und Gruppenzugriffsrichtlinien

Verwenden Sie Bucket- und Gruppenzugriffsrichtlinien

StorageGRID verwendet die Richtliniensprache von Amazon Web Services (AWS), um S3-Mietern die Kontrolle über den Zugriff auf Buckets und Objekte in diesen Buckets zu ermöglichen. Das StorageGRID -System implementiert eine Teilmenge der S3 REST API-

Richtliniensprache. Zugriffsrichtlinien für die S3-API sind in JSON geschrieben.

Übersicht über die Zugriffsrichtlinie

StorageGRID unterstützt zwei Arten von Zugriffsrichtlinien.

- **Bucket-Richtlinien**, die mithilfe der S3-API-Operationen GetBucketPolicy, PutBucketPolicy und DeleteBucketPolicy oder der Tenant Manager- oder Tenant Management-API verwaltet werden. Bucket-Richtlinien sind an Buckets angehängt und daher so konfiguriert, dass sie den Zugriff von Benutzern im Bucket-Eigentümerkonto oder anderen Konten auf den Bucket und die darin enthaltenen Objekte steuern. Eine Bucket-Richtlinie gilt nur für einen Bucket und möglicherweise für mehrere Gruppen.
- **Gruppenrichtlinien**, die mithilfe des Tenant Managers oder der Tenant Management API konfiguriert werden. Gruppenrichtlinien sind einer Gruppe im Konto zugeordnet und daher so konfiguriert, dass diese Gruppe auf bestimmte Ressourcen zugreifen kann, die diesem Konto gehören. Eine Gruppenrichtlinie gilt nur für eine Gruppe und möglicherweise mehrere Buckets.



Es gibt keinen Unterschied in der Priorität zwischen Gruppen- und Bucket-Richtlinien.

StorageGRID Bucket- und Gruppenrichtlinien folgen einer bestimmten, von Amazon definierten Grammatik. Innerhalb jeder Richtlinie befindet sich ein Array von Richtlinienanweisungen und jede Anweisung enthält die folgenden Elemente:

- Anweisungs-ID (Sid) (optional)
- Wirkung
- Auftraggeber/NichtAuftraggeber
- Ressource/NichtRessource
- Aktion/NichtAktion
- Bedingung (optional)

Richtlinienanweisungen werden mithilfe dieser Struktur erstellt, um Berechtigungen anzugeben: Gewähren Sie <Effekt>, um <Principal> die Ausführung von <Aktion> auf <Ressource> zu erlauben/verweigern, wenn <Bedingung> zutrifft.

Jedes Richtlinienelement wird für eine bestimmte Funktion verwendet:

Element	Beschreibung
Sid	Das Sid-Element ist optional. Die Sid dient lediglich als Beschreibung für den Benutzer. Es wird gespeichert, aber nicht vom StorageGRID-System interpretiert.
Wirkung	Verwenden Sie das Effect-Element, um festzulegen, ob die angegebenen Vorgänge zulässig oder verweigert werden. Sie müssen Vorgänge, die Sie für Buckets oder Objekte zulassen (oder verweigern), mithilfe der unterstützten Schlüsselwörter des Aktionselements identifizieren.

Element	Beschreibung
Auftraggeber/NichtAuftraggeber	<p>Sie können Benutzern, Gruppen und Konten den Zugriff auf bestimmte Ressourcen und die Ausführung bestimmter Aktionen gestatten. Wenn in der Anfrage keine S3-Signatur enthalten ist, wird der anonyme Zugriff durch Angabe des Platzhalterzeichens (*) als Prinzipal zugelassen. Standardmäßig hat nur der Konto-Root Zugriff auf die Ressourcen, die dem Konto gehören.</p> <p>Sie müssen nur das Principal-Element in einer Bucket-Richtlinie angeben. Bei Gruppenrichtlinien ist die Gruppe, an die die Richtlinie angehängt ist, das implizite Principal-Element.</p>
Ressource/NichtRessource	<p>Das Ressourcenelement identifiziert Buckets und Objekte. Sie können Berechtigungen für Buckets und Objekte erteilen oder verweigern, indem Sie den Amazon Resource Name (ARN) zur Identifizierung der Ressource verwenden.</p>
Aktion/NichtAktion	<p>Die Elemente „Aktion“ und „Effekt“ sind die beiden Komponenten von Berechtigungen. Wenn eine Gruppe eine Ressource anfordert, wird ihr der Zugriff auf die Ressource entweder gewährt oder verweigert. Der Zugriff wird verweigert, sofern Sie keine ausdrücklichen Berechtigungen erteilen. Sie können jedoch eine durch eine andere Richtlinie erteilte Berechtigung durch eine explizite Verweigerung außer Kraft setzen.</p>
Zustand	<p>Das Bedingungselement ist optional. Mithilfe von Bedingungen können Sie Ausdrücke erstellen, um zu bestimmen, wann eine Richtlinie angewendet werden soll.</p>

Im Aktionselement können Sie das Platzhalterzeichen (*) verwenden, um alle Vorgänge oder eine Teilmenge von Vorgängen anzugeben. Diese Aktion entspricht beispielsweise Berechtigungen wie s3:GetObject, s3:PutObject und s3:DeleteObject.

```
s3:*Object
```

Im Ressourcenelement können Sie die Platzhalterzeichen (*) und (?) verwenden. Während das Sternchen (*) 0 oder mehr Zeichen entspricht, entspricht das Fragezeichen (?) einem beliebigen einzelnen Zeichen.

Im Principal-Element werden Platzhalterzeichen nur zum Festlegen des anonymen Zugriffs unterstützt, der jedem die Berechtigung erteilt. Beispielsweise legen Sie das Platzhalterzeichen (*) als Hauptwert fest.

```
"Principal": "*"
```

```
"Principal": {"AWS": "*"} 
```

Im folgenden Beispiel verwendet die Anweisung die Elemente „Effect“, „Principal“, „Action“ und „Resource“. Dieses Beispiel zeigt eine vollständige Bucket-Richtlinienanweisung, die den Effekt "Zulassen" verwendet, um

den Principals, der Admin-Gruppe `federated-group/admin` und die Finanzgruppe `federated-group/finance`, Berechtigungen zum Ausführen der Aktion `s3>ListBucket` auf dem Eimer namens `mybucket` und die Aktion `s3GetObject` auf allen Objekten in diesem Bucket.

```
{  
  "Statement": [  
    {  
      "Effect": "Allow",  
      "Principal": {  
        "AWS": [  
          "arn:aws:iam::27233906934684427525:federated-group/admin",  
          "arn:aws:iam::27233906934684427525:federated-group/finance"  
        ]  
      },  
      "Action": [  
        "s3>ListBucket",  
        "s3GetObject"  
      ],  
      "Resource": [  
        "arn:aws:s3:::mybucket",  
        "arn:aws:s3:::mybucket/*"  
      ]  
    }  
  ]  
}
```

Die Bucket-Richtlinie hat eine Größenbeschränkung von 20.480 Bytes und die Gruppenrichtlinie eine Größenbeschränkung von 5.120 Bytes.

Konsistenz für Richtlinien

Standardmäßig sind alle Aktualisierungen, die Sie an Gruppenrichtlinien vornehmen, letztendlich konsistent. Wenn eine Gruppenrichtlinie konsistent wird, kann es aufgrund der Richtlinienzwischenspeicherung weitere 15 Minuten dauern, bis die Änderungen wirksam werden. Standardmäßig sind alle Aktualisierungen, die Sie an Bucket-Richtlinien vornehmen, streng konsistent.

Bei Bedarf können Sie die Konsistenzgarantien für Bucket-Richtlinienaktualisierungen ändern. Beispielsweise möchten Sie möglicherweise, dass eine Änderung an einer Bucket-Richtlinie während eines Site-Ausfalls verfügbar ist.

In diesem Fall können Sie entweder die `Consistency-Control` Header in der `PutBucketPolicy`-Anforderung, oder Sie können die `PUT Bucket`-Konsistenzanforderung verwenden. Wenn eine Bucket-Richtlinie konsistent wird, kann es aufgrund der Richtlinienzwischenspeicherung weitere 8 Sekunden dauern, bis die Änderungen wirksam werden.

 Wenn Sie die Konsistenz auf einen anderen Wert einstellen, um eine vorübergehende Situation zu umgehen, denken Sie daran, die Einstellung auf Bucket-Ebene wieder auf den ursprünglichen Wert zurückzusetzen, wenn Sie fertig sind. Andernfalls verwenden alle zukünftigen Bucket-Anfragen die geänderte Einstellung.

Verwenden Sie ARN in Richtlinienanweisungen

In Richtlinienanweisungen wird die ARN in den Elementen „Principal“ und „Resource“ verwendet.

- Verwenden Sie diese Syntax, um die S3-Ressourcen-ARN anzugeben:

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

- Verwenden Sie diese Syntax, um die ARN der Identitätsressource (Benutzer und Gruppen) anzugeben:

```
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 abzugleichen.
- Internationale Zeichen, die im Objektschlüssel angegeben werden können, sollten mit JSON UTF-8 oder mit JSON \u-Escapesequenzen codiert werden. Prozentkodierung wird nicht unterstützt.

["RFC 2141 URN-Syntax"](#)

Der HTTP-Anforderungstext für den PutBucketPolicy-Vorgang muss mit charset=UTF-8 codiert sein.

Angeben von Ressourcen in einer Richtlinie

In Richtlinienanweisungen können Sie das Ressourcenelement verwenden, um den Bucket oder das Objekt anzugeben, für das Berechtigungen erteilt oder verweigert werden.

- Jede Richtlinienanweisung erfordert ein Ressourcenelement. In einer Richtlinie werden Ressourcen durch das Element gekennzeichnet `Resource` oder alternativ `NotResource` zum Ausschluss.
- Sie geben Ressourcen mit einer S3-Ressourcen-ARN an. Beispiel:

```
"Resource": "arn:aws:s3:::mybucket/*"
```

- Sie können auch RichtlinienvARIABLEN 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.

Angeben von Prinzipalen in einer Richtlinie

Verwenden Sie das Principal-Element, um den Benutzer, die Gruppe oder das Mandantenkonto zu identifizieren, dem durch die Richtlinienanweisung der Zugriff auf die Ressource gestattet bzw. verweigert wird.

- Jede Richtlinienanweisung in einer Bucket-Richtlinie muss ein Principal-Element enthalten. Richtlinienanweisungen in einer Gruppenrichtlinie benötigen das Principal-Element nicht, da die Gruppe als Auftraggeber verstanden wird.
- In einer Richtlinie werden Auftraggeber durch das Element „Principal“ oder alternativ „NotPrincipal“ zum Ausschluss gekennzeichnet.
- Kontobasierte Identitäten müssen mithilfe einer ID oder einer ARN angegeben werden:

```
"Principal": { "AWS": "account_id"}  
"Principal": { "AWS": "identity_arn" }
```

- In diesem Beispiel wird die Mandantenkonto-ID 27233906934684427525 verwendet, die das Stammkonto und alle Benutzer im Konto umfasst:

```
"Principal": { "AWS": "27233906934684427525" }
```

- Sie können nur das Stammkonto angeben:

```
"Principal": { "AWS": "arn:aws:iam::27233906934684427525:root" }
```

- Sie können einen bestimmten Verbundbenutzer („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 Auftraggeber angeben:

```
"Principal": "*"
```

- Um Mehrdeutigkeiten zu vermeiden, können Sie anstelle des Benutzernamens die Benutzer-UUID verwenden:

```
arn:aws:iam::27233906934684427525:user-uuid/de305d54-75b4-431b-adb2-eb6b9e546013
```

Nehmen wir beispielsweise an, Alex verlässt die Organisation und der Benutzername Alex wird gelöscht. Wenn ein neuer Alex in die Organisation eintritt und ihm die gleiche Alex Benutzernamen, könnte der neue Benutzer unbeabsichtigt die dem ursprünglichen Benutzer erteilten Berechtigungen erben.

- Der Principalwert kann einen Gruppen-/Benutzernamen angeben, der beim Erstellen einer Bucket-Richtlinie noch nicht vorhanden ist.

Festlegen von Berechtigungen in einer Richtlinie

In einer Richtlinie wird das Aktionselement verwendet, um Berechtigungen für eine Ressource zuzulassen/zu verweigern. Es gibt eine Reihe von Berechtigungen, die Sie in einer Richtlinie angeben können. Diese werden durch das Element „Action“ oder alternativ „NotAction“ zum Ausschluss gekennzeichnet. Jedes dieser Elemente ist bestimmten S3 REST-API-Operationen zugeordnet.

In den Tabellen sind die Berechtigungen aufgeführt, die für Buckets gelten, und die Berechtigungen, die für Objekte gelten.



Amazon S3 verwendet jetzt die Berechtigung s3:PutReplicationConfiguration sowohl für die Aktionen PutBucketReplication als auch DeleteBucketReplication. StorageGRID verwendet für jede Aktion separate Berechtigungen, was der ursprünglichen Amazon S3-Spezifikation entspricht.



Ein Löschen wird ausgeführt, wenn ein Put zum Überschreiben eines vorhandenen Werts verwendet wird.

Berechtigungen, die für Buckets gelten

Berechtigungen	S3 REST API-Operationen	Benutzerdefiniert für StorageGRID
s3:Bucket erstellen	Bucket erstellen	Ja. Hinweis: Nur in Gruppenrichtlinien verwenden.
s3:Bucket löschen	Bucket löschen	
s3:DeleteBucketMetadataNotification	Konfiguration der Benachrichtigung über DELETE-Bucket-Metadaten	Ja
s3:DeleteBucketPolicy	DeleteBucketPolicy	
s3:Replikationskonfiguration löschen	DeleteBucketReplication	Ja, separate Berechtigungen für PUT und DELETE

Berechtigungen	S3 REST API-Operationen	Benutzerdefiniert für StorageGRID
s3:GetBucketAcl	GetBucketAcl	
s3:GetBucketCompliance	GET Bucket-Konformität (veraltet)	Ja
s3:GetBucketConsistency	GET Bucket-Konsistenz	Ja
s3:GetBucketCORS	GetBucketCors	
s3:GetEncryptionConfiguration	GetBucketEncryption	
s3:GetBucketLastAccessTime	GET Bucket – Letzte Zugriffszeit	Ja
s3:GetBucketLocation	BucketLocation abrufen	
s3:GetBucketMetadataNotification	GET Bucket-Metadaten-Benachrichtigungskonfiguration	Ja
s3:GetBucketNotification	GetBucketNotificationConfiguration	
s3:GetBucketObjectLockConfiguration	GetObjectLockConfiguration	
s3:GetBucketPolicy	GetBucketPolicy	
s3:GetBucketTagging	GetBucketTagging	
s3:GetBucketVersioning	GetBucketVersioning	
s3:GetLifecycleConfiguration	GetBucketLifecycleConfiguration	
s3:GetReplicationConfiguration	GetBucketReplication	
s3:ListeAlleMeineBuckets	<ul style="list-style-type: none"> • Buckets auflisten • GET-Speichernutzung 	Ja, für die GET-Speichernutzung. Hinweis: Nur in Gruppenrichtlinien verwenden.
s3>ListBucket	<ul style="list-style-type: none"> • ListObjects • Kopfeimer • RestoreObject 	

Berechtigungen	S3 REST API-Operationen	Benutzerdefiniert für StorageGRID
s3>ListBucketMultipartUploads	<ul style="list-style-type: none"> • ListMultipartUploads • RestoreObject 	
s3>ListBucketVersions	GET Bucket-Versionen	
s3PutBucketCompliance	PUT-Bucket-Konformität (veraltet)	Ja
s3PutBucketConsistency	PUT Bucket-Konsistenz	Ja
s3PutBucketCORS	<ul style="list-style-type: none"> • DeleteBucketCors† • PutBucketCors 	
s3PutEncryptionConfiguration	<ul style="list-style-type: none"> • DeleteBucketEncryption • PutBucketEncryption 	
s3PutBucketLastAccessTime	PUT Bucket: Letzte Zugriffszeit	Ja
s3PutBucketMetadataNotification	Konfiguration der Benachrichtigung über PUT-Bucket-Metadaten	Ja
s3PutBucketNotification	PutBucketNotificationConfiguration	
s3PutBucketObjectLockConfiguration	<ul style="list-style-type: none"> • CreateBucket mit dem x-amz-bucket-object-lock-enabled: true Anforderungsheader (erfordert auch die Berechtigung s3:CreateBucket) • PutObjectLockConfiguration 	
s3PutBucketPolicy	PutBucketPolicy	
s3PutBucketTagging	<ul style="list-style-type: none"> • BucketTagging löschen† • PutBucketTagging 	
s3PutBucketVersioning	PutBucketVersioning	
s3PutLifecycleConfiguration	<ul style="list-style-type: none"> • DeleteBucketLifecycle† • PutBucketLifecycleConfiguration 	
s3PutReplicationConfiguration	PutBucketReplication	Ja, separate Berechtigungen für PUT und DELETE

Berechtigungen, die für Objekte gelten

Berechtigungen	S3 REST API-Operationen	Benutzerdefiniert für StorageGRID
s3:AbortMultipartUpload	<ul style="list-style-type: none"> AbortMultipartUpload RestoreObject 	
s3:BypassGovernanceRetention	<ul style="list-style-type: none"> Objekt löschen Objekte löschen PutObjectRetention 	
s3:Objekt löschen	<ul style="list-style-type: none"> Objekt löschen Objekte löschen RestoreObject 	
s3:DeleteObjectTagging	DeleteObjectTagging	
s3:DeleteObjectVersionTagging	DeleteObjectTagging (eine bestimmte Version des Objekts)	
s3:DeleteObjectVersion	DeleteObject (eine bestimmte Version des Objekts)	
s3:GetObject	<ul style="list-style-type: none"> GetObject HeadObject RestoreObject SelectObjectContent 	
s3:GetObjectAcl	GetObjectAcl	
s3:GetObjectLegalHold	GetObjectLegalHold	
s3:GetObjectRetention	GetObjectRetention	
s3:GetObjectTagging	GetObjectTagging	
s3:GetObjectVersionTagging	GetObjectTagging (eine bestimmte Version des Objekts)	
s3:GetObjectVersion	GetObject (eine bestimmte Version des Objekts)	
s3>ListMultipartUploadParts	ListParts, RestoreObject	

Berechtigungen	S3 REST API-Operationen	Benutzerdefiniert für StorageGRID
s3:PutObject	<ul style="list-style-type: none"> • PutObject • Objekt kopieren • RestoreObject • CreateMultipartUpload • CompleteMultipartUpload • UploadPart • UploadPartCopy 	
s3:PutObjectLegalHold	PutObjectLegalHold	
s3:PutObjectRetention	PutObjectRetention	
s3:PutObjectTagging	PutObjectTagging	
s3:PutObjectVersionTagging	PutObjectTagging (eine bestimmte Version des Objekts)	
s3:PutOverwriteObject	<ul style="list-style-type: none"> • PutObject • Objekt kopieren • PutObjectTagging • DeleteObjectTagging • CompleteMultipartUpload 	Ja
s3:RestoreObject	RestoreObject	

PutOverwriteObject-Berechtigung verwenden

Die Berechtigung s3:PutOverwriteObject ist eine benutzerdefinierte StorageGRID Berechtigung, die für Vorgänge gilt, die Objekte erstellen oder aktualisieren. Die Einstellung dieser Berechtigung bestimmt, ob der Client die Daten, benutzerdefinierten Metadaten oder S3-Objektmarkierungen eines Objekts überschreiben kann.

Mögliche Einstellungen für diese Berechtigung sind:

- **Zulassen:** Der Client kann ein Objekt überschreiben. Dies ist die Standardeinstellung.
- **Ablehnen:** Der Client kann ein Objekt nicht überschreiben. Wenn die Berechtigung „PutOverwriteObject“ auf „Verweigern“ gesetzt ist, funktioniert sie wie folgt:
 - Wenn ein vorhandenes Objekt am gleichen Pfad gefunden wird:
 - Die Daten, benutzerdefinierten Metadaten oder S3-Objektmarkierungen des Objekts können nicht überschrieben werden.
 - Alle laufenden Aufnahmevergänge werden abgebrochen und ein Fehler zurückgegeben.

- Wenn die S3-Versionierung aktiviert ist, verhindert die Einstellung „Verweigern“, dass PutObjectTagging- oder DeleteObjectTagging-Vorgänge 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 die Wirkung dieselbe, als ob „Zulassen“ gesetzt wäre.

 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 Berechtigung „PutOverwriteObject“.

Bedingungen in einer Richtlinie angeben

Bedingungen definieren, wann eine Richtlinie in Kraft tritt. Bedingungen bestehen aus Operatoren und Schlüssel-Wert-Paaren.

Bedingungen verwenden Schlüssel-Wert-Paare zur Auswertung. Ein Bedingungselement kann mehrere Bedingungen enthalten und jede Bedingung kann mehrere Schlüssel-Wert-Paare enthalten. Der Bedingungsblock verwendet das folgende Format:

```
Condition: {
  condition_type: {
    condition_key: condition_values
  }
}
```

Im folgenden Beispiel verwendet die Bedingung „IpAddress“ den Bedingungsschlüssel „SourceIp“.

```
"Condition": {
  "IpAddress": {
    "aws:SourceIp": "54.240.143.0/24"
    ...
  },
  ...
}
```

Unterstützte Bedingungsoperatoren

Bedingungsoperatoren werden wie folgt kategorisiert:

- Zeichenfolge
- Numerisch
- Boolescher Wert
- IP-Adresse
- Nullprüfung

Bedingungsoperatoren	Beschreibung
StringEquals	Vergleicht einen Schlüssel mit einem Zeichenfolgenwert auf Basis einer genauen Übereinstimmung (Groß-/Kleinschreibung beachten).
StringNotEquals	Vergleicht einen Schlüssel mit einem Zeichenfolgenwert basierend auf negierter Übereinstimmung (Groß-/Kleinschreibung beachten).
StringEqualsIgnoreCase	Vergleicht einen Schlüssel mit einem Zeichenfolgenwert basierend auf einer genauen Übereinstimmung (Groß-/Kleinschreibung wird ignoriert).
StringNotEqualsIgnoreCase	Vergleicht einen Schlüssel mit einem Zeichenfolgenwert basierend auf negierter Übereinstimmung (Groß-/Kleinschreibung wird ignoriert).
StringLike	Vergleicht einen Schlüssel mit einem Zeichenfolgenwert auf Basis einer genauen Übereinstimmung (Groß-/Kleinschreibung beachten). Kann die Platzhalterzeichen * und ? enthalten.
StringNotLike	Vergleicht einen Schlüssel mit einem Zeichenfolgenwert basierend auf negierter Übereinstimmung (Groß-/Kleinschreibung beachten). Kann die Platzhalterzeichen * und ? enthalten.
NumericEquals	Vergleicht einen Schlüssel mit einem numerischen Wert auf Basis einer exakten Übereinstimmung.
NumericNotEquals	Vergleicht einen Schlüssel mit einem numerischen Wert basierend auf negierter Übereinstimmung.
NumerischGrößerAls	Vergleicht einen Schlüssel mit einem numerischen Wert basierend auf einer „Größer-als“-Übereinstimmung.
NumerischGrößerAlsGleich	Vergleicht einen Schlüssel mit einem numerischen Wert basierend auf der Übereinstimmung „größer als oder gleich“.
NumericLessThan	Vergleicht einen Schlüssel mit einem numerischen Wert basierend auf einer „kleiner als“-Übereinstimmung.
NumerischKleinerAlsGleich	Vergleicht einen Schlüssel mit einem numerischen Wert basierend auf der Übereinstimmung „kleiner als oder gleich“.
Bool	Vergleicht einen Schlüssel mit einem Booleschen Wert basierend auf der Übereinstimmung „wahr oder falsch“.
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 negierter Übereinstimmung.

Bedingungsoperatoren	Beschreibung
Null	Überprüft, ob im aktuellen Anforderungskontext ein Bedingungsschlüssel vorhanden ist.

Unterstützte Bedingungsschlüsse

Bedingungsschlüssel	Aktionen	Beschreibung
aws:SourceIp	IP-Betreiber	<p>Wird mit der IP-Adresse verglichen, von der die Anfrage gesendet wurde. Kann für Bucket- oder Objektoperationen verwendet werden.</p> <p>Hinweis: Wenn die S3-Anforderung über den Load Balancer-Dienst auf Admin-Knoten und Gateway-Knoten gesendet wurde, wird dies mit der IP-Adresse vor dem Load Balancer-Dienst verglichen.</p> <p>Hinweis: Wenn ein nicht transparenter Load Balancer eines Drittanbieters verwendet wird, wird dies mit der IP-Adresse dieses Load Balancers verglichen. Beliebig X-Forwarded-For Header wird ignoriert, da seine Gültigkeit nicht festgestellt werden kann.</p>
aws:Benutzername	Ressource/Identität	Wird mit dem Benutzernamen des Absenders verglichen, von dem die Anfrage gesendet wurde. Kann für Bucket- oder Objektoperationen verwendet werden.
s3:Trennzeichen	s3>ListBucket und s3>ListBucketVersions-Berechtigungen	Wird mit dem in einer ListObjects- oder ListObjectVersions-Anforderung angegebenen Trennzeichenparameter verglichen.

Bedingungsschlüssel	Aktionen	Beschreibung
s3:ExistingObjectTag/<Tag-Schlüssel>	s3:DeleteObjectTagging s3:DeleteObjectVersionTagging s3:GetObject s3:GetObjectAcl s3:GetObjectTagging s3:GetObjectVersion s3:GetObjectVersionAcl s3:GetObjectVersionTagging s3:PutObjectAcl s3:PutObjectTagging s3:PutObjectVersionAcl s3:PutObjectVersionTagging	Erfordert, dass das vorhandene Objekt über den spezifischen Tag-Schlüssel und -Wert verfügt.
s3:max-Schlüssel	s3>ListBucket und s3>ListBucketVersions-Berechtigungen	Wird mit dem in einer ListObjects- oder ListObjectVersions-Anforderung angegebenen Max-Keys-Parameter verglichen.
s3:Objektsperre-verbleibende-Aufbewahrungstage	s3:PutObject	<p>Vergleicht mit dem Aufbewahrungsdatum, das in der x-amz-object-lock-retain-until-date Anforderungsheader oder berechnet aus der Standardaufbewahrungsdauer des Buckets, um sicherzustellen, dass diese Werte innerhalb des zulässigen Bereichs für die folgenden Anforderungen liegen:</p> <ul style="list-style-type: none"> PutObject Objekt kopieren CreateMultipartUpload
s3:Objektsperre-verbleibende-Aufbewahrungstage	s3:PutObjectRetention	Vergleicht mit dem in der PutObjectRetention-Anforderung angegebenen Aufbewahrungsdatum, um sicherzustellen, dass es innerhalb des zulässigen Bereichs liegt.

Bedingungsschlüssel	Aktionen	Beschreibung
s3:Präfix	s3>ListBucket und s3>ListBucketVersions-Berechtigungen	Wird mit dem in einer ListObjects- oder ListObjectVersions-Anforderung angegebenen Präfixparameter verglichen.
s3:RequestObjectTag/<Tag-Schlüssel>	s3:PutObject s3:PutObjectTagging s3:PutObjectVersionTagging	Erfordert einen bestimmten Tag-Schlüssel und -Wert, wenn die Objektanforderung Tagging enthält.

Angeben von Variablen in einer Richtlinie

Sie können Variablen in Richtlinien verwenden, um Richtlinieninformationen einzufügen, wenn diese verfügbar sind. Sie können Richtlinienvariablen in der `Resource` Element und in Stringvergleichen im `Condition` Element.

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

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

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

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

Variable	Beschreibung
<code> \${aws:SourceIp}</code>	Verwendet den Sourcelp-Schlüssel als bereitgestellte Variable.
<code> \${aws:username}</code>	Verwendet den Benutzernamenschlüssel als bereitgestellte Variable.
<code> \${s3:prefix}</code>	Verwendet den dienstspezifischen Präfixschlüssel als bereitgestellte Variable.
<code> \${s3:max-keys}</code>	Verwendet den dienstspezifischen Max-Keys-Schlüssel als bereitgestellte Variable.
<code> \${*}</code>	Sonderzeichen. Verwendet das Zeichen als wörtliches *-Zeichen.

Variable	Beschreibung
<code>\$(?)</code>	Sonderzeichen. Verwendet das Zeichen als wörtliches ?-Zeichen.
<code>\$(\$)</code>	Sonderzeichen. Verwendet das Zeichen als wörtliches \$-Zeichen.

Erstellen Sie Richtlinien, die eine besondere Behandlung erfordern

Manchmal kann eine Richtlinie Berechtigungen erteilen, die eine Gefahr für die Sicherheit oder den laufenden Betrieb darstellen, wie etwa das Sperren des Root-Benutzers des Kontos. Die StorageGRID S3 REST-API-Implementierung ist bei der Richtlinienvalidierung weniger restriktiv als Amazon, bei der Richtlinienauswertung jedoch ebenso streng.

Richtlinienbeschreibung	Richtlinientyp	Amazon-Verhalten	StorageGRID -Verhalten
Verweigern Sie sich selbst alle Berechtigungen für das Root-Konto	Eimer	Gültig und erzwungen, aber das Root-Benutzerkonto behält die Berechtigung für alle S3-Bucket-Richtlinienvorgänge	Dasselbe
Sich selbst alle Berechtigungen für Benutzer/Gruppe verweigern	Gruppe	Gültig und durchgesetzt	Dasselbe
Erteilen Sie einer fremden Kontogruppe alle Berechtigungen	Eimer	Ungültiger Auftraggeber	Gültig, aber Berechtigungen für alle S3-Bucket-Richtlinienvorgänge geben einen 405-Methodenfehler zurück, wenn sie durch eine Richtlinie erlaubt sind
Erteilen Sie einem fremden Root- oder Benutzerkonto alle Berechtigungen	Eimer	Gültig, aber Berechtigungen für alle S3-Bucket-Richtlinienvorgänge geben einen 405-Methodenfehler zurück, wenn sie durch eine Richtlinie erlaubt sind	Dasselbe
Jedem die Berechtigung für alle Aktionen erteilen	Eimer	Gültig, aber Berechtigungen für alle S3-Bucket-Richtlinienvorgänge geben einen 405-Methode nicht zulässig-Fehler für das Stammkonto und die Benutzer des Fremdkontos zurück	Dasselbe

Richtlinienbeschreibung	Richtlinientyp	Amazon-Verhalten	StorageGRID -Verhalten
Allen die Berechtigung für alle Aktionen verweigern	Eimer	Gültig und erzwungen, aber das Root-Benutzerkonto behält die Berechtigung für alle S3-Bucket-Richtlinienvorgänge	Dasselbe
Der Auftraggeber ist ein nicht vorhandener Benutzer oder eine nicht vorhandene Gruppe.	Eimer	Ungültiger Auftraggeber	Gültig
Ressource ist ein nicht vorhandener S3-Bucket	Gruppe	Gültig	Dasselbe
Principal ist eine lokale Gruppe	Eimer	Ungültiger Auftraggeber	Gültig
Die Richtlinie erteilt Nichtbesitzerkonten (einschließlich anonymer Konten) die Berechtigung, Objekte abzulegen.	Eimer	Gültig. Objekte sind Eigentum des Erstellerkontos und die Bucket-Richtlinie gilt nicht. Das Erstellerkonto muss mithilfe von Objekt-ACLs Zugriffsberechtigungen für das Objekt erteilen.	Gültig. Objekte sind Eigentum des Bucket-Eigentümerkontos. Es gilt die Bucket-Richtlinie.

WORM-Schutz (Write-Once-Read-Many)

Sie können WORM-Buckets (Write-Once-Read-Many) erstellen, um Daten, benutzerdefinierte Objektmetadaten und S3-Objekt-Tagging zu schützen. Sie konfigurieren die WORM-Buckets, um die Erstellung neuer Objekte zu ermöglichen und das Überschreiben oder 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 eine PutOverwriteObject DENY-Operation hinzu.
 - Fügen Sie der S3-Richtlinie eine DeleteObject DENY-Operation hinzu.
 - Fügen Sie der S3-Richtlinie eine PutObject ALLOW-Operation hinzu.



Das Festlegen von „DeleteObject“ auf „DENY“ in einer S3-Richtlinie verhindert nicht, dass ILM Objekte löscht, wenn eine Regel wie „Null Kopien nach 30 Tagen“ vorhanden ist.



Selbst wenn alle diese Regeln und Richtlinien angewendet werden, schützen sie nicht vor gleichzeitigen Schreibvorgängen (siehe Situation A). Sie schützen vor sequenziellen Überschreibungen (siehe Situation B).

Situation A: Gleichzeitige Schreibvorgänge (nicht geschützt)

```
/mybucket/important.doc  
PUT#1 ---> OK  
PUT#2 -----> OK
```

Situation B: Sequentielles Überschreiben abgeschlossen (vorbeugend)

```
/mybucket/important.doc  
PUT#1 -----> PUT#2 ---X (denied)
```

Ähnliche Informationen

- ["So verwalten StorageGRID ILM-Regeln Objekte"](#)
- ["Beispiele für Bucket-Richtlinien"](#)
- ["Beispiele für Gruppenrichtlinien"](#)
- ["Objekte mit ILM verwalten"](#)
- ["Verwenden eines Mandantenkontos"](#)

Beispiele für Bucket-Richtlinien

Verwenden Sie die Beispiele in diesem Abschnitt, um StorageGRID Zugriffsrichtlinien für Buckets zu erstellen.

Bucket-Richtlinien geben die Zugriffsberechtigungen für den Bucket an, an den die Richtlinie angehängt ist. Sie konfigurieren eine Bucket-Richtlinie mithilfe der S3 PutBucketPolicy-API über eines dieser Tools:

- ["Mietermanager"](#) .
- AWS CLI mit diesem Befehl (siehe["Operationen an Buckets"](#)):

```
> aws s3api put-bucket-policy --bucket examplebucket --policy  
file://policy.json
```

Beispiel: Allen Lesezugriff auf einen Bucket gewähren

In diesem Beispiel darf jeder, auch anonyme Benutzer, Objekte im Bucket auflisten und GetObject-Operationen für alle Objekte im Bucket ausführen. Alle anderen Vorgänge werden abgelehnt. Beachten Sie, dass diese Richtlinie möglicherweise nicht besonders nützlich ist, da niemand außer dem Konto-Root über die Berechtigung 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: Erlauben Sie allen Benutzern eines Kontos den Vollzugriff und allen Benutzern eines anderen Kontos den Lesezugriff auf einen Bucket.

In diesem Beispiel erhält jeder in einem angegebenen Konto vollen Zugriff auf einen Bucket, während jeder in einem anderen angegebenen Konto nur den Bucket auflisten und GetObject-Operationen für Objekte im Bucket ausführen darf, beginnend mit dem shared/ Objektschlüsselpräfix.



In StorageGRID sind Objekte, die von einem Nicht-Eigentümerkonto (einschließlich anonymer Konten) erstellt wurden, Eigentum des Bucket-Eigentümerkontos. Für diese Objekte gilt die Bucket-Richtlinie.

```
{
  "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: Erlauben Sie allen nur Lesezugriff auf einen Bucket und Vollzugriff für eine bestimmte Gruppe

In diesem Beispiel darf jeder, auch anonym, den Bucket auflisten und GetObject-Operationen für alle Objekte im Bucket durchführen, während nur Benutzer der Gruppe Marketing im angegebenen Konto wird der volle Zugriff gewährt.

```
{
  "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: Erlauben Sie jedem Lese- und Schreibzugriff auf einen Bucket, wenn sich der Client im IP-Bereich befindet

In diesem Beispiel darf jeder, auch anonyme Benutzer, den Bucket auflisten und beliebige Objektoperationen für alle Objekte im Bucket ausführen, vorausgesetzt, die Anforderungen stammen aus einem angegebenen IP-Bereich (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: Vollzugriff auf einen Bucket ausschließlich durch einen angegebenen Verbundbenutzer zulassen

In diesem Beispiel erhält der Verbundbenutzer Alex vollen Zugriff auf die examplebucket Bucket und seine Objekte. Allen anderen Benutzern, einschließlich „root“, werden sämtliche Vorgänge ausdrücklich verweigert. Beachten Sie jedoch, dass „root“ niemals die Berechtigung 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 Deny Die Wirkung von PutOverwriteObject und DeleteObject stellt sicher, dass niemand die Daten, benutzerdefinierten Metadaten und S3-Objektmarkierungen des Objekts 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/*"
    }
  ]
}

```

Beispiele für Gruppenrichtlinien

Verwenden Sie die Beispiele in diesem Abschnitt, um StorageGRID Zugriffsrichtlinien für Gruppen zu erstellen.

Gruppenrichtlinien geben die Zugriffsberechtigungen für die Gruppe an, der die Richtlinie zugeordnet ist. Es gibt keine Principal Element in der Richtlinie, da es implizit ist. Gruppenrichtlinien werden mithilfe des Tenant Managers oder der API konfiguriert.

Beispiel: Festlegen der Gruppenrichtlinie mit dem Mandanten-Manager

Wenn Sie im Mandanten-Manager eine Gruppe hinzufügen oder bearbeiten, können Sie eine Gruppenrichtlinie auswählen, um festzulegen, welche S3-Zugriffsberechtigungen die Mitglieder dieser Gruppe haben. Sehen "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 mit einer Bucket-Richtlinie gewährt. Wenn Sie diese Option auswählen, hat standardmäßig nur der Root-Benutzer Zugriff auf S3-Ressourcen.
- **Nur-Lesezugriff:** Benutzer in dieser Gruppe haben nur Lesezugriff auf S3-Ressourcen. Beispielsweise können Benutzer dieser Gruppe Objekte auflisten und Objektdaten, Metadaten und Tags lesen. Wenn Sie diese Option auswählen, wird die JSON-Zeichenfolge für eine schreibgeschützte Gruppenrichtlinie im Textfeld angezeigt. Sie können diese Zeichenfolge nicht bearbeiten.
- **Vollzugriff:** Benutzer in dieser Gruppe haben vollen Zugriff auf S3-Ressourcen, einschließlich Buckets. Wenn Sie diese Option auswählen, wird die JSON-Zeichenfolge für eine Gruppenrichtlinie mit vollem Zugriff im Textfeld angezeigt. Sie können diese Zeichenfolge nicht bearbeiten.
- **Ransomware-Minderung:** Diese Beispielrichtlinie gilt für alle Buckets dieses Mandanten. Benutzer in dieser Gruppe können allgemeine Aktionen ausführen, aber keine Objekte dauerhaft aus Buckets löschen, für die die Objektversionierung aktiviert ist.

Tenant Manager-Benutzer mit der Berechtigung „Alle Buckets verwalten“ können diese Gruppenrichtlinie außer Kraft setzen. Beschränken Sie die Berechtigung „Alle Buckets verwalten“ auf vertrauenswürdige Benutzer und verwenden Sie, sofern verfügbar, die Multi-Faktor-Authentifizierung (MFA).

- **Benutzerdefiniert:** Benutzern in der Gruppe werden die Berechtigungen erteilt, die Sie im Textfeld angeben.

Beispiel: Gruppe vollen Zugriff auf alle Buckets gewähren

In diesem Beispiel wird allen Mitgliedern der Gruppe der vollständige Zugriff auf alle Buckets gewährt, die dem Mandantenkonto gehören, sofern die Bucket-Richtlinie diesen Zugriff nicht ausdrücklich verweigert.

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

Beispiel: Gruppe schreibgeschützten Zugriff auf alle Buckets gewähren

In diesem Beispiel haben alle Mitglieder der Gruppe schreibgeschützten Zugriff auf S3-Ressourcen, sofern dies nicht ausdrücklich durch die Bucket-Richtlinie verweigert wird. Beispielsweise können Benutzer dieser Gruppe 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 gewähren

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 des Datenschutzes 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}/*"
    }
  ]
}

```

In den Prüfprotokollen verfolgte S3-Operationen

Audit-Nachrichten werden von StorageGRID -Diensten generiert und in Textprotokolldateien gespeichert. Sie können die S3-spezifischen Prüfmeldungen im Prüfprotokoll überprüfen, um Details zu Bucket- und Objektvorgängen zu erhalten.

In den Audit-Protokollen verfolgte Bucket-Operationen

- Bucket erstellen
- Bucket löschen
- BucketTagging löschen
- Objekte löschen
- GetBucketTagging
- Kopfeimer
- ListObjects
- ListObjectVersions
- PUT Bucket-Konformität
- PutBucketTagging
- PutBucketVersioning

In den Überwachungsprotokollen verfolgte Objektvorgänge

- CompleteMultipartUpload
- Objekt kopieren
- Objekt löschen
- GetObject
- HeadObject
- PutObject
- RestoreObject
- Objekt auswählen
- UploadPart (wenn eine ILM-Regel eine ausgeglichene oder strikte Aufnahme verwendet)
- UploadPartCopy (wenn eine ILM-Regel eine ausgeglichene oder strikte Aufnahme verwendet)

Ähnliche Informationen

- ["Zugriff auf die Überwachungsprotokolldatei"](#)
- ["Client schreibt Prüfmeldungen"](#)
- ["Client liest Audit-Nachrichten"](#)

Swift REST API verwenden (Ende der Lebensdauer)

Verwenden Sie die Swift REST-API

Der Support für die Swift-API hat das Ende seiner Lebensdauer erreicht und wird in einer zukünftigen Version entfernt.



Swift-Details wurden aus dieser Version der Dokumentationssite entfernt. Sehen ["StorageGRID 11.8: Swift REST API verwenden"](#).

Copyright-Informationen

Copyright © 2025 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtsinhabers in keiner Form und durch keine Mittel – weder grafische noch elektronische oder mechanische, einschließlich Fotokopieren, Aufnehmen oder Speichern in einem elektronischen Abrufsystem – auch nicht in Teilen, vervielfältigt werden.

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

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

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

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

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

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

Markeninformationen

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