Verwenden eines Mandantenkontos

StorageGRID software

NetApp
October 21, 2025

Inhalt

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 .

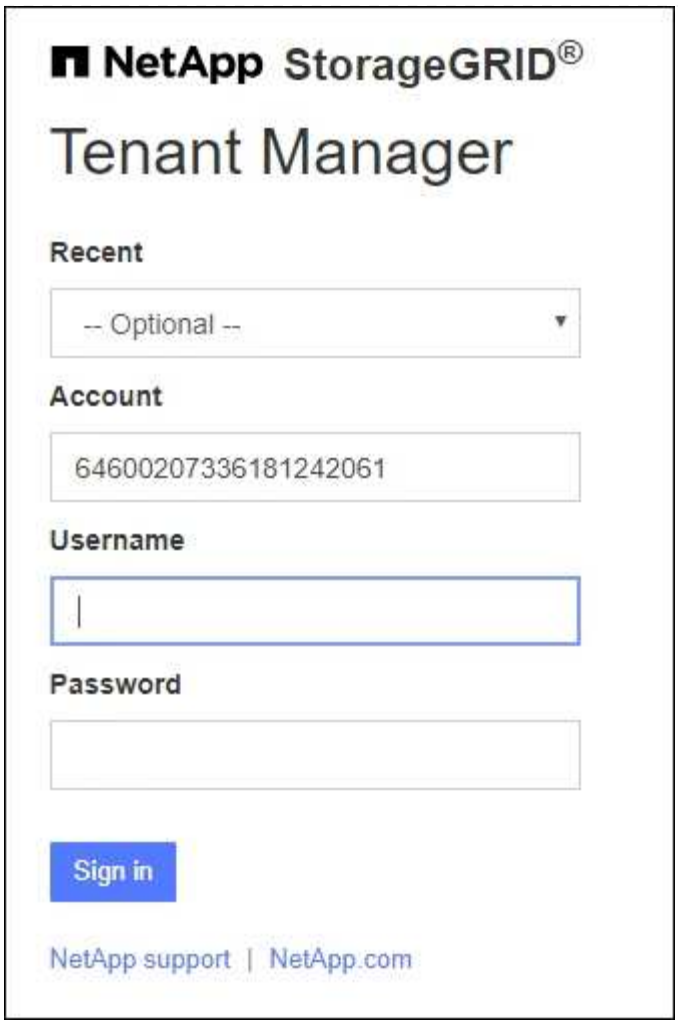
   Der angezeigte Anmeldebildschirm hängt von der eingegebenen URL ab und davon, ob Single Sign-On (SSO) für StorageGRID konfiguriert wurde.

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.

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



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*.

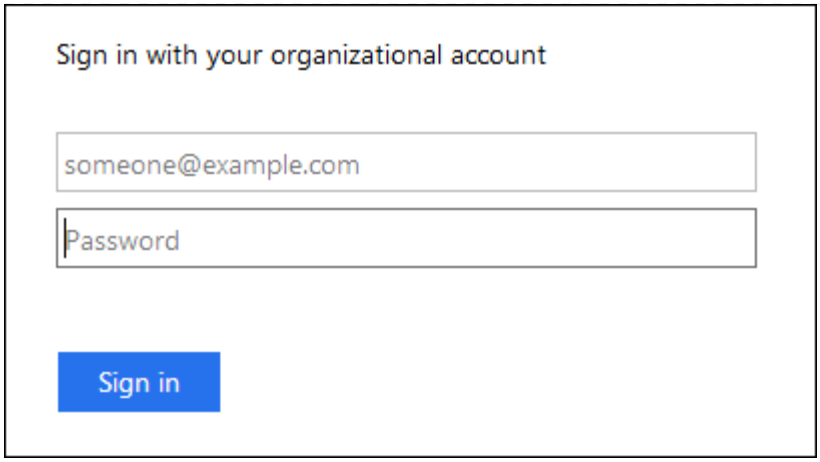
Das Tenant Manager-Dashboard wird angezeigt.

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:



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.

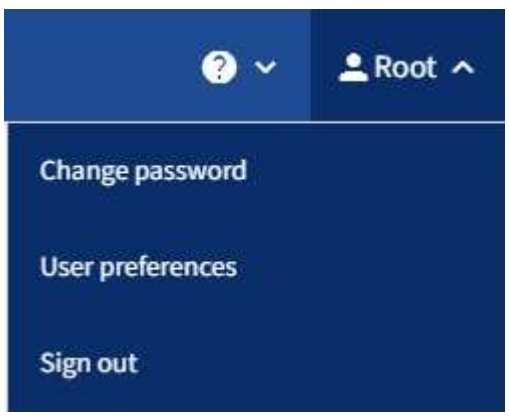
  Das Tenant Manager-Dashboard wird angezeigt.

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.

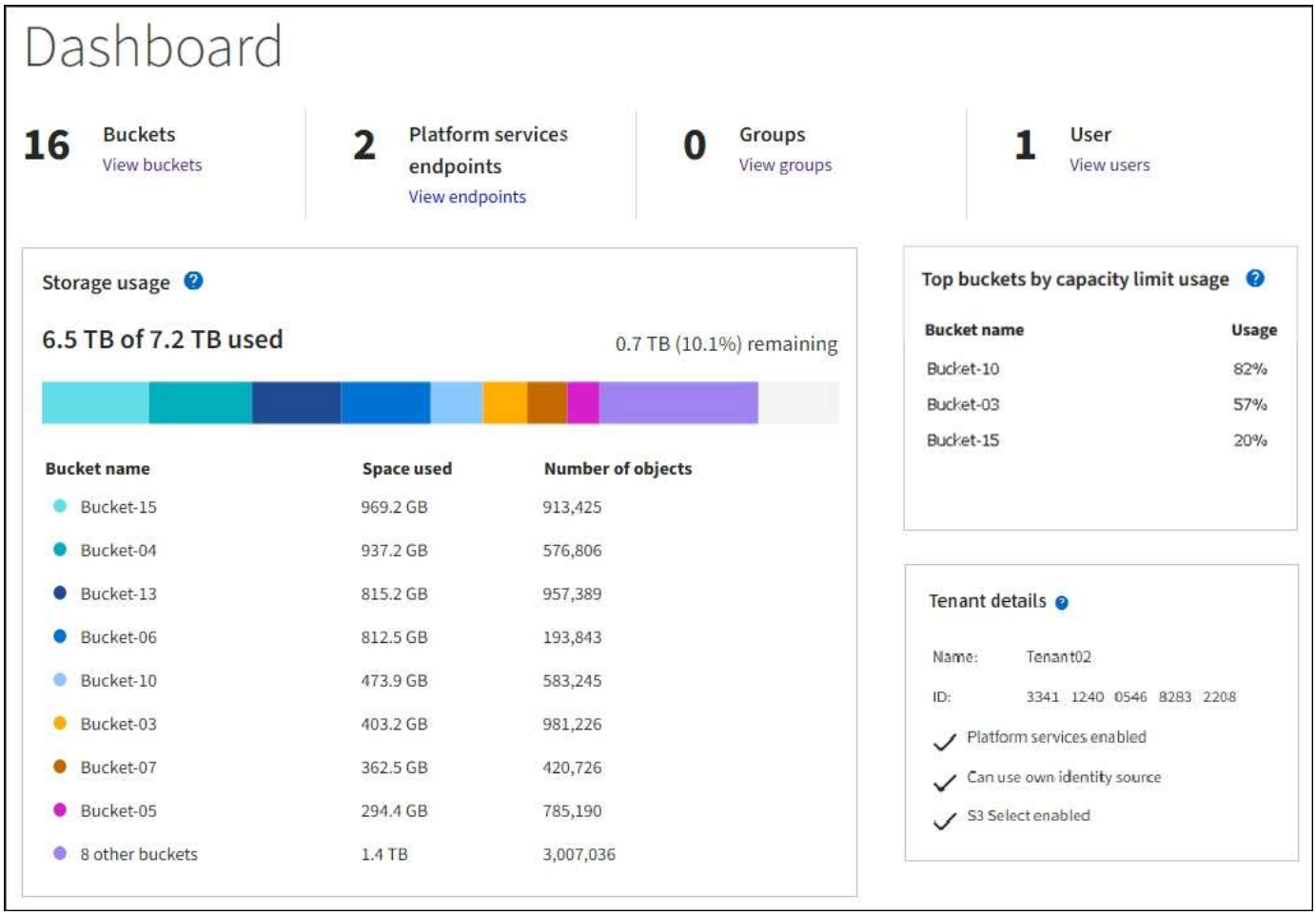
> Wenn SSO aktiviert ist und Sie auch beim Grid Manager angemeldet sind, müssen Sie sich auch beim Grid Manager abmelden, um sich von SSO abzumelden.

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:



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.

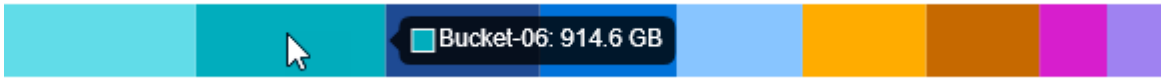
  Dieser Wert gibt die Gesamtmenge der hochgeladenen Objektdaten an und stellt nicht den Speicherplatz dar, der zum Speichern von Kopien dieser Objekte und ihrer Metadaten verwendet wird.

- 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.

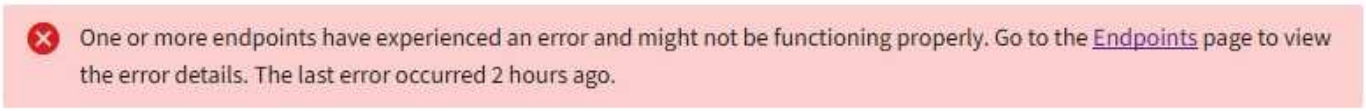
Kapazitätslimitnutzung

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



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)

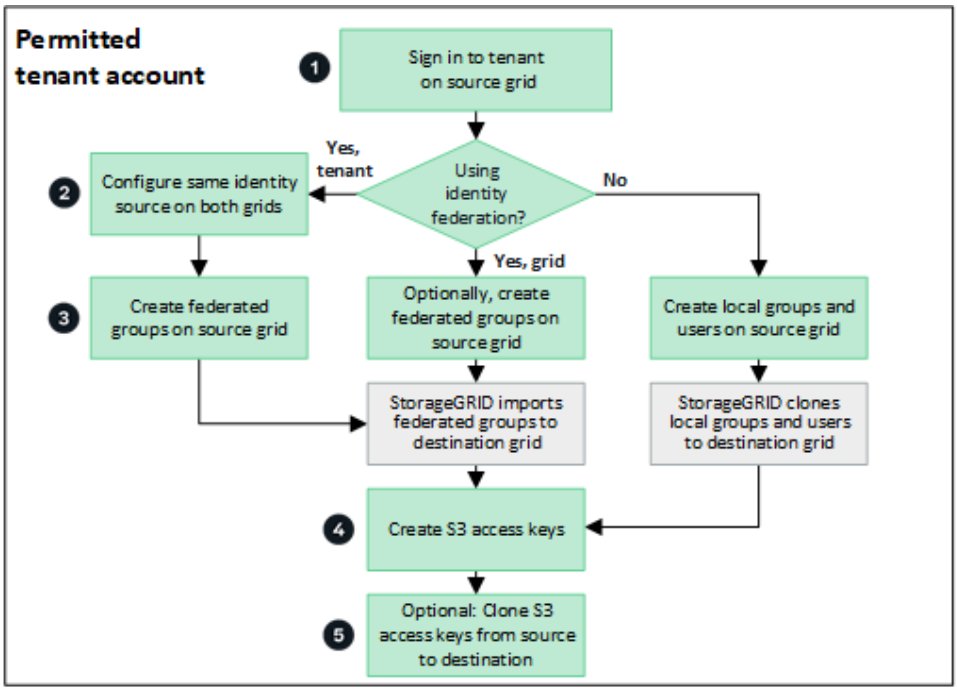
repliziert. Nachdem der Mandant repliziert wurde, werden alle dem Quellmandanten hinzugefügten Gruppen und Benutzer in den Replikatmandanten geklont.

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:

Beim Mandanten Sign in

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

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, klont 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 geklont?

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

Lokale Gruppen, die im Quellraster erstellt wurden, werden geklont

Nachdem ein Mandantenkonto erstellt und in das Zielraster repliziert wurde, klont StorageGRID automatisch alle lokalen Gruppen, die Sie 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 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.

Lokale Benutzer, die im Quellraster erstellt wurden, werden geklont

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

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.

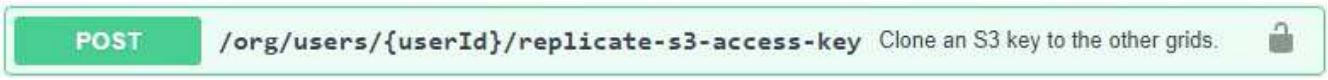
Schritte

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`

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.

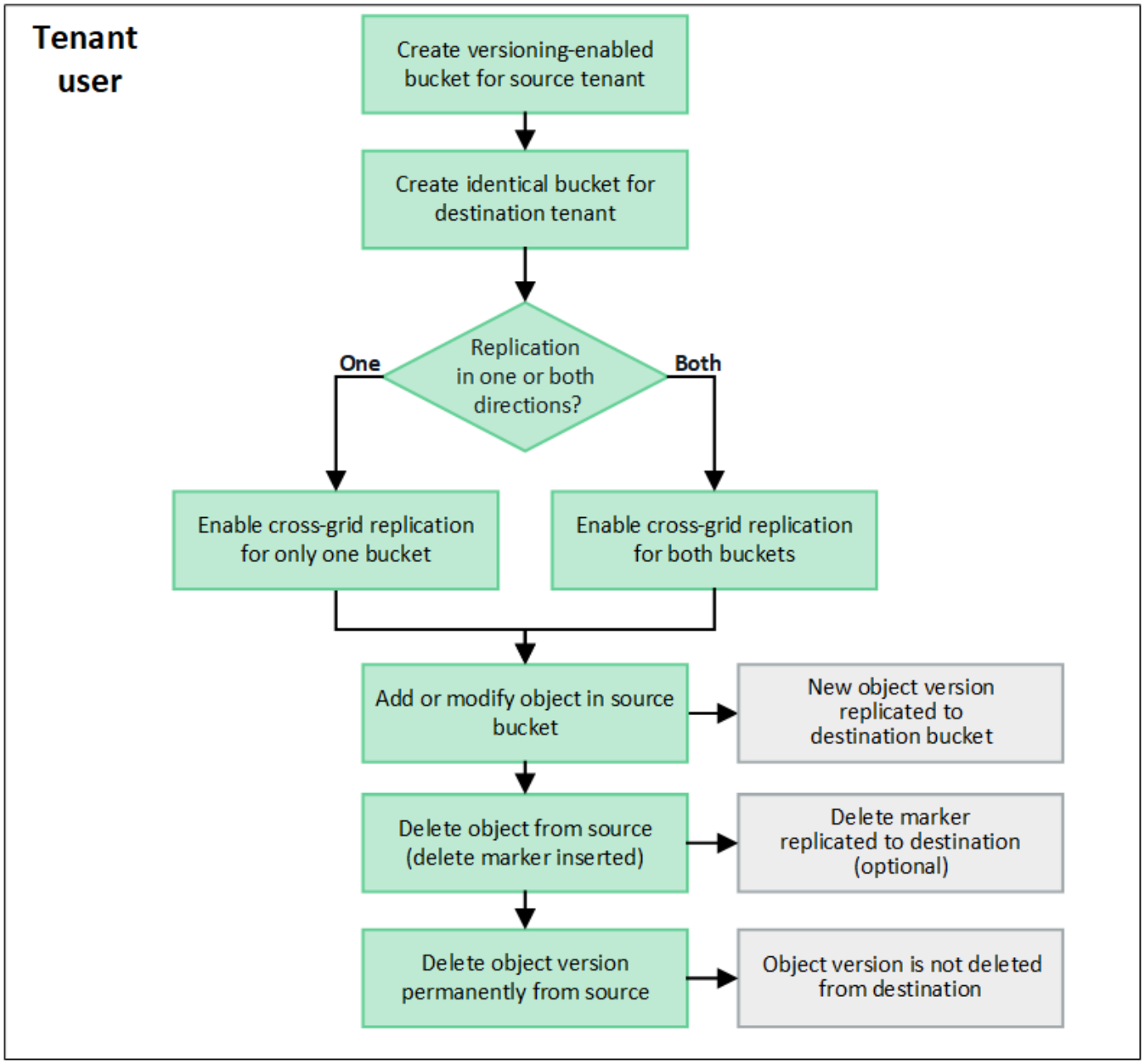
Verwalten der Cross-Grid-Replikation

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 Webbrowser" .
- 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" .

Lösche 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

1. 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.

2. 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.
3. Wählen Sie die Verbindung aus der Tabelle aus.
4. Wählen Sie **Fehler löschen**.
5. Wählen Sie **Ja**, um die Nachricht zu löschen und den Systemstatus zu aktualisieren.
6. 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.

7. 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

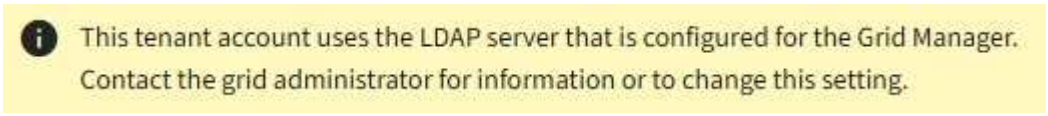
- Sie sind beim Tenant Manager angemeldet mit einem"unterstützter Webbrowser" .
- Sie gehören einer Benutzergruppe an, die über die"Root-Zugriffsberechtigung" .
- Sie verwenden Active Directory, Azure AD, OpenLDAP oder Oracle Directory Server als Identitätsanbieter.

> ⓘ 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.

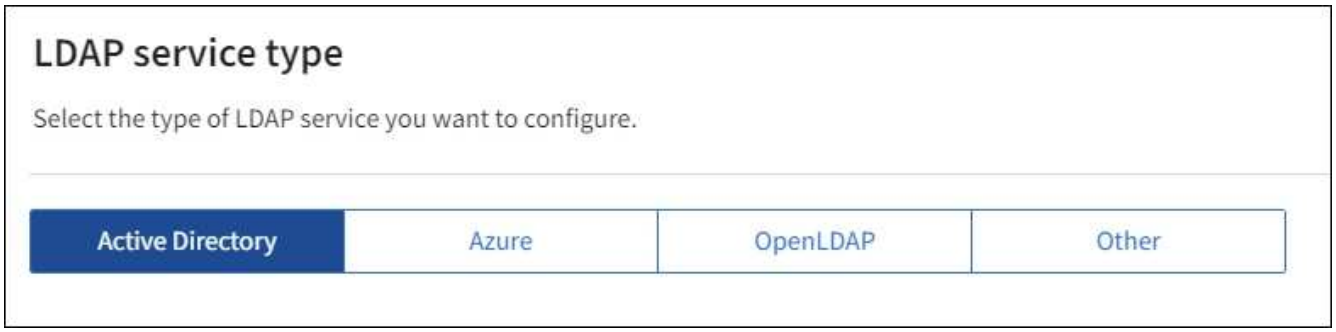


Konfiguration eingeben

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.



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.
   ◦ **STARTLS verwenden**: Verwenden Sie STARTTLS, um die Kommunikation mit dem LDAP-Server zu sichern. Dies ist die empfohlene Option für Active Directory, OpenLDAP oder Andere, aber diese Option wird für 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.

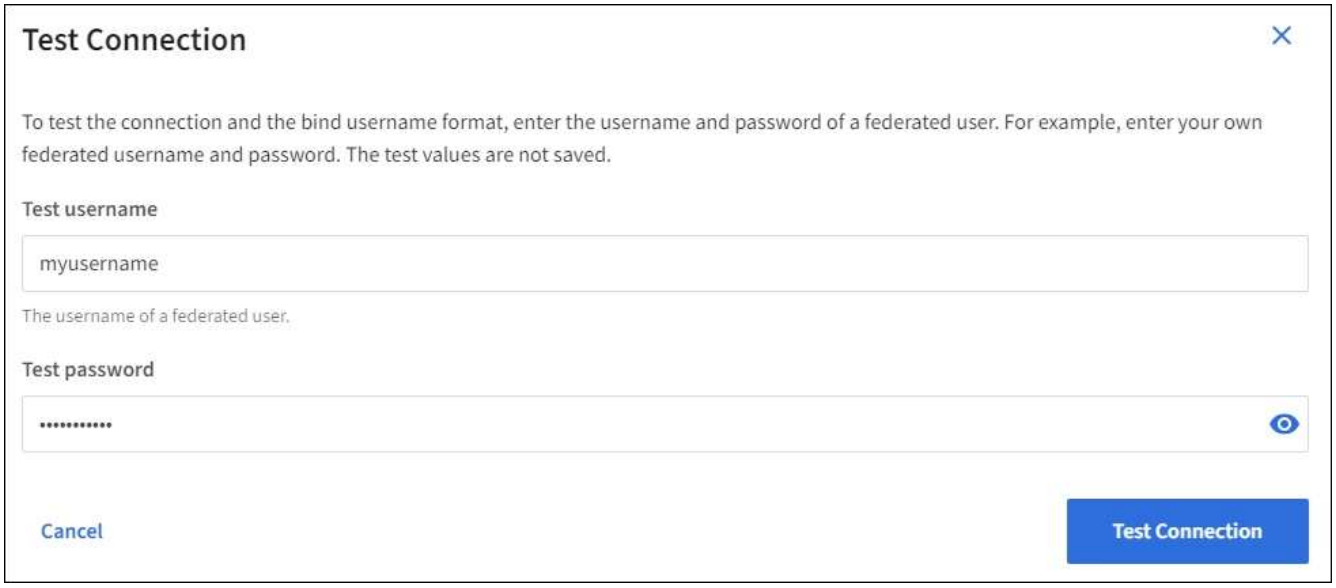
Testen Sie die Verbindung und speichern Sie die Konfiguration

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 /.



- 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["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["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.

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 derselbe **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	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).
Brauch	Den Benutzern in der Gruppe werden die Berechtigungen erteilt, die Sie im Textfeld angeben.

2. Wenn Sie **Benutzerdefiniert** ausgewählt haben, geben Sie die Gruppenrichtlinie ein. Jede Gruppenrichtlinie hat eine Größenbeschränkung von 5.120 Byte. Sie müssen 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 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.

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	**S3-Mandanten**: Ermöglicht Benutzern, alle Buckets und Bucket-Konfigurationen anzuzeigen. **Swift-Mandanten**: Ermöglicht Swift-Benutzern, alle Container und Containerkonfigurationen mithilfe der Tenant Management API anzuzeigen.	Benutzer, die weder über die Berechtigung „Alle Buckets anzeigen“ noch über die Berechtigung „Alle Buckets verwalten“ verfügen, können die Menüoption **Buckets** nicht sehen. 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. 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.

Erlaubnis	Beschreibung	Details
Alle Buckets verwalten	**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. **Swift-Mandanten**: Ermöglicht Swift-Benutzern, die Konsistenz für Swift-Container mithilfe der Tenant Management API zu steuern.	Benutzer, die weder über die Berechtigung „Alle Buckets anzeigen“ noch über die Berechtigung „Alle Buckets verwalten“ verfügen, können die Menüoption **Buckets** nicht sehen. 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. 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.
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

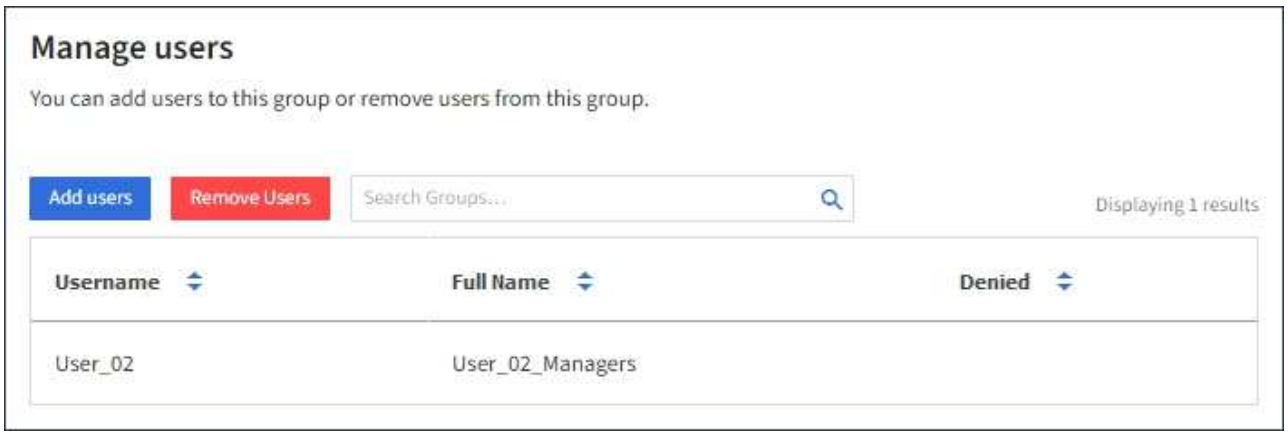
1. Wählen Sie **ZUGRIFFSVERWALTUNG** > **Gruppen**.
2. Überprüfen Sie die Informationen auf der Seite „Gruppen“, auf der grundlegende Informationen zu allen lokalen und föderierten Gruppen für dieses Mandantenkonto aufgeführt sind.

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 kannstErneuter Versuch eines Gruppenklons das ist fehlgeschlagen.

3. Wenn Sie den Namen der Gruppe ändern möchten:
   a. Aktivieren Sie das Kontrollkästchen für die Gruppe.
   b. Wählen Sie **Aktionen** > **Gruppennamen 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 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.
   a. Ändern Sie im Abschnitt „Übersicht“ den Anzeigenamen, indem Sie den Namen oder das Bearbeitungssymbol auswählen .
   b. Aktualisieren Sie auf der Registerkarte **Gruppenberechtigungen** die Berechtigungen und wählen Sie **Änderungen speichern**.
   c. Nehmen Sie auf der Registerkarte **Gruppenrichtlinie** 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:
   a. Wählen Sie die Registerkarte „Benutzer“ aus.



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

      Oben rechts erscheint eine Erfolgsmeldung.

8. So entfernen Sie lokale Benutzer aus der Gruppe:
   a. Wählen Sie die Registerkarte „Benutzer“ aus.
   b. Wählen Sie **Benutzer entfernen**.
   c. Wählen Sie die Benutzer aus, die Sie entfernen möchten, und wählen Sie **Benutzer entfernen**.

      Oben rechts 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

1. Wählen Sie **ZUGRIFFSVERWALTUNG** > **Gruppen**.
2. Aktivieren Sie das Kontrollkästchen für die Gruppe, die Sie duplizieren möchten.
3. Wählen Sie **Aktionen** > **Gruppe duplizieren**.
4. Sehen"Erstellen von Gruppen für einen S3-Mandanten" oder"Erstellen Sie Gruppen für einen Swift-Mandanten" für Details zu den einzugebenden Informationen.
5. 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. SehenLokalen 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. SehenLokalen 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 Webbrowser" .
- 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 Webbrowser" .
- 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	Ein Name für den Bucket, der diesen Regeln entspricht: • 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. Weitere Informationen finden Sie im "Amazon Web Services (AWS)-Dokumentation zu Bucket-Benennungsregeln" . **Hinweis**: Sie können den Bucket-Namen nach dem Erstellen des Buckets nicht mehr ändern.
Region	Die Region des Buckets. Ihr StorageGRID Administrator verwaltet die verfügbaren Regionen. Die Region eines Buckets kann sich auf die auf Objekte angewendete Datenschutzrichtlinie auswirken. Standardmäßig werden alle Buckets im `us-east-1` Region. **Hinweis**: Sie können die Region nach dem Erstellen des Buckets nicht mehr ändern.

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	• 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	• 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. **Hinweis**: Ihr Grid-Administrator muss Ihnen die Verwendung des Compliance-Modus gestatten.

b. Wenn die **Standardaufbewahrung** aktiviert ist, geben Sie die **Standardaufbewahrungsdauer** 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 Aufbewahrungsdauer für den Mandanten ist.

Eine *maximale* Aufbewahrungsdauer, die zwischen 1 Tag und 100 Jahren liegen kann, wird festgelegt, wenn der Grid-Administrator den Mandanten erstellt. Wenn Sie eine *Standard*-Aufbewahrungsdauer festlegen, darf diese den für die maximale Aufbewahrungsdauer festgelegten Wert nicht überschreiten. Bitten Sie Ihren Grid-Administrator bei Bedarf, die maximale Aufbewahrungsdauer 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 Netzwerkkonnektivität 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 löschcodierte 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 Kapazitätslimit (sofern festgelegt), wenn ein Mandant mit dem Hochladen von Objekten beginnt, und lehnt neue Aufnahmen in diesen Bucket ab, wenn der Mandant das Kapazitätslimit überschritten hat. StorageGRID berücksichtigt jedoch nicht die Größe des aktuellen Uploads, wenn es feststellt, ob das Kapazitätslimit überschritten wurde. Wenn Objekte gelöscht werden, kann es einem Mandanten vorübergehend untersagt werden, neue Objekte in diesen Bucket hochzuladen, bis die Kapazitätslimitnutzung 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 Kapazitätslimit-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	• Nein, für die Quellkopie • Ja, für die Zielkopie	• Nein, für die Quellkopie • Ja, für die Zielkopie	• Ja, für die Quellkopie • Ja, für die Zielkopie	• Ja, für die Quellkopie • Ja, für die Zielkopie
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 aktivierter 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 Aufbewahrungsdauer 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 aktivierter 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 aktivierter 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 aktivierter 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 Standardaufbewahrungsdauer 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 aktivierter S3-Objektsperre unterstützt.
- Die CloudMirror-Replikation wird für Buckets mit aktivierter 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 unterhttps://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 Standardaufbewahrungsdauer festlegen.

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.
- 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	• 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.

Standardaufbewahrungsmodus	Beschreibung
Einhaltung	• 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. **Hinweis**: Ihr Grid-Administrator muss Ihnen die Verwendung des Compliance-Modus gestatten.

6. Wenn die **Standardaufbewahrung** aktiviert ist, geben Sie die **Standardaufbewahrungsdauer** 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 Aufbewahrungsdauer für den Mandanten ist.

   Eine *maximale* Aufbewahrungsdauer, die zwischen 1 Tag und 100 Jahren liegen kann, wird festgelegt, wenn der Grid-Administrator den Mandanten erstellt. Wenn Sie eine *Standard*-Aufbewahrungsdauer festlegen, darf diese den für die maximale Aufbewahrungsdauer festgelegten Wert nicht überschreiten. Bitten Sie Ihren Grid-Administrator bei Bedarf, die maximale Aufbewahrungsdauer 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` 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	• GetBucketReplication • PutBucketReplication	• "CloudMirror-Replikation" • "Operationen an Buckets"
Benachrichtigungen	• GetBucketNotificationConfiguration • PutBucketNotificationConfiguration	• "Benachrichtigungen" • "Operationen an Buckets"
Suchintegration	• GET Bucket-Metadaten-Benachrichtigungskonfiguration • Konfiguration der Benachrichtigung über PUT-Bucket-Metadaten	• "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. PUT-Anfragen) an StorageGRID fehl. Sie müssen diese fehlgeschlagenen Anfragen wiederholen, wenn der Endpunkt erreichbar ist.
Drosselung des Zielendpunkts	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. 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. 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.
Bestellgarantien	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. 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.
ILM-gesteuerte Objektlöschungen	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. Im Gegensatz dazu werden Suchintegrationsanforderungen gesendet, wenn Objekte aufgrund von ILM gelöscht werden.

Rücksichtnahme	Details
Verwenden von Kafka-Endpunkten	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. 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. • SASL/PLAIN • SASL/SCRAM-SHA-256 • SASL/SCRAM-SHA-512 **Hinweis:** Konfigurierte Speicherproxyeinstellungen gelten nicht für Endpunkte der Kafka-Plattformdienste.

Überlegungen zur Verwendung des CloudMirror-Replikationsdienstes

Rücksichtnahme	Details
Replikationsstatus	StorageGRID unterstützt nicht die `x-amz-replication-status` Kopfzeile.
Objektgröße	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. **Hinweis**: 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 stattdessen den mehrteiligen Upload.
Bucket-Versionierung und Versions-IDs	Wenn für den Quell-S3-Bucket in StorageGRID die Versionierung aktiviert ist, sollten Sie auch die Versionierung für den Ziel-Bucket aktivieren. 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. **Hinweis**: Versions-IDs für den Quell-Bucket in StorageGRID stehen in keinem Zusammenhang mit den Versions-IDs für den Ziel-Bucket.

Rücksichtnahme	Details
Tagging für Objektversionen	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. 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.
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 aktivierter S3-Objektsperre	Die Replikation wird für Quell- oder Ziel-Buckets mit aktivierter 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-Replikation" .

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.

Löschung, 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 Ereignisnachricht 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`

Schlüsselname	StorageGRID -Wert
awsRegion	*nicht enthalten*
x-amz-id-2	*nicht enthalten*
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 aktivierter 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 Endpunkterstellung 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	`s3`
Benachrichtigungen	`sns`oder `kafka`
Suchintegration	`es`

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	`bucket-name`
Benachrichtigungen	`sns-topic-name`oder `kafka-topic-name`
Suchintegration	`domain-name/index-name/type-name` **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 Ressourcenname (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-URIs und Port 80 für HTTP-URIs (die meisten Endpunkte)
- Port 9092 für HTTPS und HTTP-URIs (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.	• Zugriffsschlüssel-ID • Geheimer Zugriffsschlüssel
Grundlegendes HTTP	Verwendet einen Benutzernamen und ein Kennwort, um Verbindungen zum Ziel zu authentifizieren.	• 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.	• Zugriffsschlüssel-ID • Geheimer Zugriffsschlüssel

Authentifizierungstyp	Beschreibung	Anmeldeinformationen
CAP (C2S-Zugangsportal)	Verwendet Zertifikate und Schlüssel, um Verbindungen zum Ziel zu authentifizieren.	• 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.	• 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.	• 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.	• 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.	• 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 Endpunkterstellung 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.

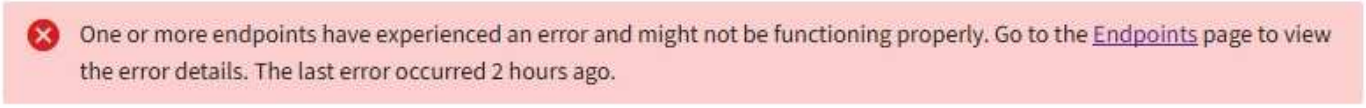
4. Wählen Sie **Endpunkt löschen**.

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“.



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 aktivierter 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:
   a. 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":"11111111111111111"
         },
         "requestParameters":{
            "sourceIPAddress":"193.51.100.20"
         },
         "responseElements":{
            "x-amz-request-id":"122047343"
         },
         "s3":{
            "s3SchemaVersion":"1.0",
            "configurationId":"Image-created",
            "bucket":{
               "name":"test1",
               "ownerIdentity":{
                  "principalId":"11111111111111111"
               },
               "arn":"arn:sgws:s3:::test1"
            },
            "object":{
               "key":"images/cat.jpg",
               "size":0,
               "eTag":"d41d8cd98f00b204e9800998ecf8427e",
               "sequencer":"14D90402421461C7"
            }
         }
      }
   ]
}
```


+ Wenn die Benachrichtigung 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 Zielendpunkt 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 imBeispiele 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	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 Regelelement enthalten.	Nein
Status	Der Status kann „Aktiviert“ oder „Deaktiviert“ sein. Für deaktivierte Regeln werden keine Maßnahmen ergriffen. Im Regelelement enthalten.	Ja
Präfix	Objekte, die dem Präfix entsprechen, sind von der Regel betroffen und ihre Metadaten werden an das angegebene Ziel gesendet. Um alle Objekte abzugleichen, geben Sie ein leeres Präfix an. Im Regelelement enthalten.	Ja
Ziel	Container-Tag für das Ziel einer Regel. Im Regelelement enthalten.	Ja

Name	Beschreibung	Erforderlich
Urne	URN des Ziels, an das die Objektmetadaten gesendet werden. Muss die URN eines StorageGRID -Endpunkts mit den folgenden Eigenschaften sein: • `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` . Endpunkte werden mithilfe des Tenant Managers oder der Tenant Management API konfiguriert. Sie haben folgende Form: • `arn:aws:es:region:account-ID:domain/mydomain/myindex/mytype` • `urn:mysite:es:::mydomain/myindex/mytype` Der Endpunkt muss konfiguriert werden, bevor die Konfigurations-XML übermittelt wird, andernfalls schlägt die Konfiguration mit einem 404-Fehler fehl. URN ist im Zielelement enthalten.	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-1:22222222: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 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"
  }
}
```

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.