Verwalten von Plattformdienst-Endpunkten

StorageGRID software

NetApp
October 21, 2025

Inhalt

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.

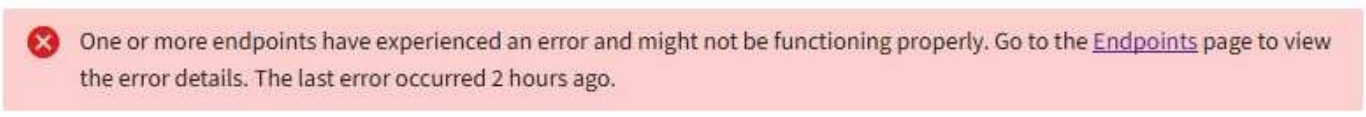
4. Wählen Sie **Endpunkt löschen**.

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"