



Verwenden Sie ein Mandantenkonto

StorageGRID 11.5

NetApp
April 11, 2024

Inhalt

- Verwenden Sie ein Mandantenkonto 1
 - Verwenden des Mandanten-Manager 1
 - Managen des Systemzugriffs für Mandantenbenutzer 15
 - Verwalten von S3-Mandantenkonten 37
 - Verwalten von S3-Platfformservices 67

Verwenden Sie ein Mandantenkonto

StorageGRID-Mandantenkonto nutzen

- ["Verwenden des Mandanten-Manager"](#)
- ["Managen des Systemzugriffs für Mandantenbenutzer"](#)
- ["Verwalten von S3-Mandantenkonten"](#)
- ["Verwalten von S3-Plattformservices"](#)

Verwenden des Mandanten-Manager

Der Tenant Manager ermöglicht das Management aller Aspekte eines StorageGRID-Mandantenkontos.

Mit dem Mandanten-Manager lässt sich die Storage-Auslastung eines Mandantenkontos überwachen und Benutzer mit Identitätsföderation bzw. durch das Erstellen von lokalen Gruppen und Benutzern managen. Bei S3-Mandantenkonten können Sie auch S3-Schlüssel managen, S3-Buckets managen und Plattform-Services konfigurieren.

Verwenden eines StorageGRID-Mandantenkontos

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

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

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

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



Wenn Sie das S3-Client-Protokoll verwenden, können Sie auch S3-Buckets und Bucket-Richtlinien verwenden, um Objekte zwischen den Abteilungen eines Unternehmens zu trennen. Sie müssen keine separaten Mandantenkonten erstellen. Anweisungen zur Implementierung von S3-Client-Applikationen finden Sie unter.

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

Erstellen von Mandantenkonten

Mandantenkonten werden von einem StorageGRID Grid-Administrator mit dem Grid Manager erstellt. Beim Erstellen eines Mandantenkontos gibt der Grid-Administrator die folgenden Informationen an:

- Anzeigename für den Mandanten (die Konto-ID des Mandanten wird automatisch zugewiesen und kann nicht geändert werden).
- Gibt an, ob das Mandantenkonto das S3 oder Swift verwenden wird
- Bei S3-Mandantenkonten: Unabhängig davon, ob das Mandantenkonto Plattform-Services nutzen darf. Wenn die Nutzung von Platfformdiensten zulässig ist, muss das Grid so konfiguriert werden, dass es seine Verwendung unterstützt.
- Optional: Ein Storage-Kontingent für das Mandantenkonto – die maximale Anzahl der Gigabyte, Terabyte oder Petabyte, die für die Mandantenobjekte verfügbar sind. Das Storage-Kontingent eines Mandanten stellt eine logische Menge (Objektgröße) und keine physische Menge (Größe auf der Festplatte) dar.
- Wenn die Identitätsföderation für das StorageGRID-System aktiviert ist, hat die föderierte Gruppe Root-Zugriffsberechtigungen, um das Mandantenkonto zu konfigurieren.
- Wenn Single Sign-On (SSO) nicht für das StorageGRID-System verwendet wird, gibt das Mandantenkonto seine eigene Identitätsquelle an oder teilt die Identitätsquelle des Grid mit, und zwar mit dem anfänglichen Passwort für den lokalen Root-Benutzer des Mandanten.

Grid-Administratoren können zudem die S3-Objektsperreinstellung für das StorageGRID System aktivieren, wenn S3-Mandantenkonten die gesetzlichen Anforderungen erfüllen müssen. Wenn S3 Object Lock aktiviert ist, können alle S3-Mandantenkonten konforme Buckets erstellen und managen.

Konfigurieren von S3-Mandanten

Nachdem ein S3-Mandantenkonto erstellt wurde, können Sie auf den Mandanten-Manager zugreifen, um Aufgaben wie die folgenden auszuführen:

- Einrichten von Identitätsföderation (es sei denn, die Identitätsquelle wird gemeinsam mit dem Grid verwendet) oder Erstellen lokaler Gruppen und Benutzer
- Verwalten von S3-Zugriffsschlüsseln
- Erstellung und Management von S3 Buckets, einschließlich konformer Buckets
- Verwenden von Plattform-Services (falls aktiviert)
- Monitoring der Storage-Auslastung



Während Sie mit Mandanten-Manager S3-Buckets erstellen und managen können, müssen Sie über S3-Zugriffsschlüssel verfügen und die S3-REST-API verwenden, um Objekte aufzunehmen und zu managen.

Konfiguration von Swift Mandanten

Nach der Erstellung eines Swift-Mandantenkontos können Benutzer mit Root Access-Berechtigung auf den Mandanten-Manager zugreifen, um Aufgaben wie die folgenden durchzuführen:

- Einrichten von Identitätsföderation (es sei denn, die Identitätsquelle wird gemeinsam mit dem Grid verwendet) und Erstellen lokaler Gruppen und Benutzer
- Monitoring der Storage-Auslastung



Swift-Benutzer müssen über die Root-Zugriffsberechtigung für den Zugriff auf den Mandanten-Manager verfügen. Die Root-Zugriffsberechtigung ermöglicht Benutzern jedoch nicht, sich in der Swift REST-API zu authentifizieren, um Container zu erstellen und Objekte aufzunehmen. Benutzer müssen über die Swift-Administratorberechtigung verfügen, um sich bei der Swift-REST-API zu authentifizieren.

Verwandte Informationen

["StorageGRID verwalten"](#)

["S3 verwenden"](#)

["Verwenden Sie Swift"](#)

Anforderungen an einen Webbrowser

Sie müssen einen unterstützten Webbrowser verwenden.

Webbrowser	Unterstützte Mindestversion
Google Chrome	87
Microsoft Edge	87
Mozilla Firefox	84

Sie sollten das Browserfenster auf eine empfohlene Breite einstellen.

Browserbreite	Pixel
Minimum	1024
Optimal	1280

Melden Sie sich beim Tenant Manager an

Sie greifen auf den Tenant Manager zu, indem Sie die URL für den Mandanten in die Adressleiste eines unterstützten Webbrowsers eingeben.

Was Sie benötigen

- Sie müssen über Ihre Anmeldedaten verfügen.
- Sie müssen über eine URL auf den Tenant Manager zugreifen können, die von Ihrem Grid-Administrator bereitgestellt wird. Die URL sieht wie ein Beispiel aus:

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

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

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

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

Die URL enthält immer entweder den vollständig qualifizierten Domännennamen (FQDN) oder die IP-Adresse, die für den Zugriff auf einen Admin-Node verwendet wird, und kann optional auch eine Portnummer, die 20-stellige Mandantenkontokennung oder beide enthalten.

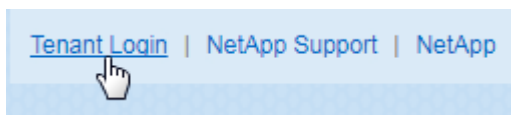
- Wenn die URL die 20-stellige Konto-ID des Mandanten nicht enthält, müssen Sie über diese Konto-ID verfügen.
- Sie müssen einen unterstützten Webbrowser verwenden.
- Cookies müssen in Ihrem Webbrowser aktiviert sein.
- Sie müssen über spezifische Zugriffsberechtigungen verfügen.

Schritte

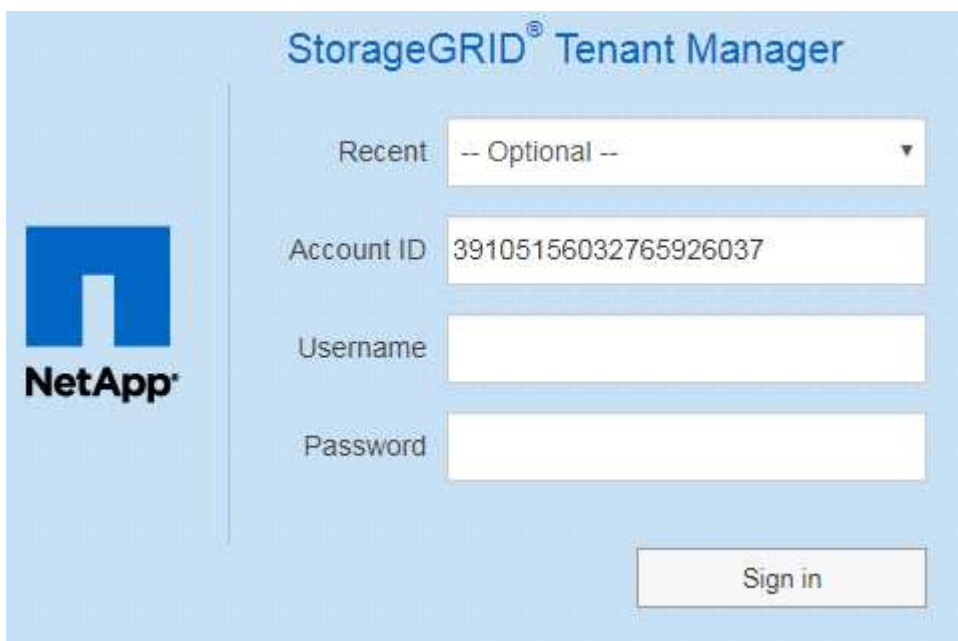
1. Starten Sie einen unterstützten Webbrowser.
2. Geben Sie in der Adressleiste des Browsers die URL für den Zugriff auf Tenant Manager ein.
3. Wenn Sie aufgefordert werden, eine Sicherheitswarnung zu erhalten, installieren Sie das Zertifikat mithilfe des Browser-Installationsassistenten.
4. Melden Sie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

Der Anmeldebildschirm, den Sie sehen, hängt von der eingegebenen URL ab und davon, ob Ihr Unternehmen Single Sign-On (SSO) verwendet. Sie sehen einen der folgenden Bildschirme:

- Die Anmeldeseite des Grid Manager. Klicken Sie oben rechts auf den Link **Tenant Login**.



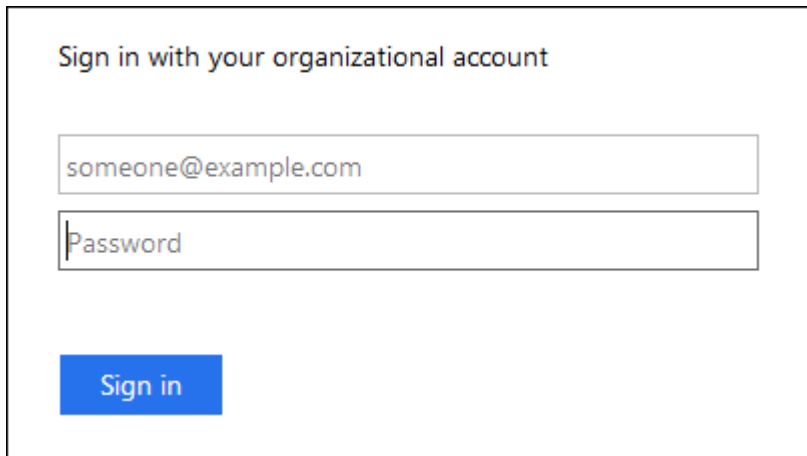
- Die Anmeldeseite von Tenant Manager. Das Feld **Konto-ID** ist möglicherweise bereits ausgefüllt, wie unten gezeigt.

A screenshot of the StorageGRID Tenant Manager login page. The page has a light blue background. On the left is the NetApp logo. The main content area contains the title 'StorageGRID® Tenant Manager' at the top. Below it is a 'Recent' dropdown menu with the text '-- Optional --'. Underneath are three input fields: 'Account ID' (pre-filled with '39105156032765926037'), 'Username', and 'Password'. At the bottom right is a 'Sign in' button.

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

Das Tenant Manager Dashboard wird angezeigt.

- Falls SSO-Seite Ihres Unternehmens im Grid aktiviert ist, Beispiel:



Sign in with your organizational account

someone@example.com

Password

Sign in

Geben Sie Ihre Standard-SSO-Anmeldedaten ein, und klicken Sie auf **Anmelden**.

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

Das Tenant Manager Dashboard wird angezeigt.

5. Wenn Sie ein erstes Kennwort von einer anderen Person erhalten haben, ändern Sie Ihr Kennwort, um Ihr Konto zu sichern. Wählen Sie **username > Passwort ändern**.



Wenn SSO für das StorageGRID-System aktiviert ist, können Sie Ihr Passwort nicht vom Mandanten-Manager ändern.

Verwandte Informationen

["StorageGRID verwalten"](#)

["Anforderungen an einen Webbrowser"](#)

Sich vom Tenant Manager abmelden

Wenn Sie mit dem Mandanten-Manager arbeiten, müssen Sie sich anmelden, um sicherzustellen, dass nicht autorisierte Benutzer nicht auf das StorageGRID-System zugreifen können. Wenn Sie Ihren Browser schließen, werden Sie möglicherweise aufgrund der Cookie-Einstellungen des Browsers nicht aus dem System abgesendet.

Schritte

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



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

Option	Beschreibung
SSO wird nicht verwendet	<p>Sie sind vom Admin-Knoten abgemeldet. Die Anmeldeseite für den Mandanten-Manager wird angezeigt.</p> <p>Hinweis: Wenn Sie sich bei mehr als einem Admin-Knoten angemeldet haben, müssen Sie sich von jedem Knoten abmelden.</p>
SSO aktiviert	<p>Sie sind von allen Admin-Knoten abgemeldet, auf die Sie zugreifen konnten. Die Seite StorageGRID-Anmeldung wird angezeigt. Der Name des Mietkontos, auf das Sie gerade zugegriffen haben, wird als Standard im Dropdown-Menü Letzte Konten angegeben, und die Konto-ID des Mieters wird angezeigt.</p> <p>Hinweis: Wenn SSO aktiviert ist und Sie auch beim Grid Manager angemeldet sind, müssen Sie sich auch vom Grid Manager abmelden, um SSO abzumelden.</p>

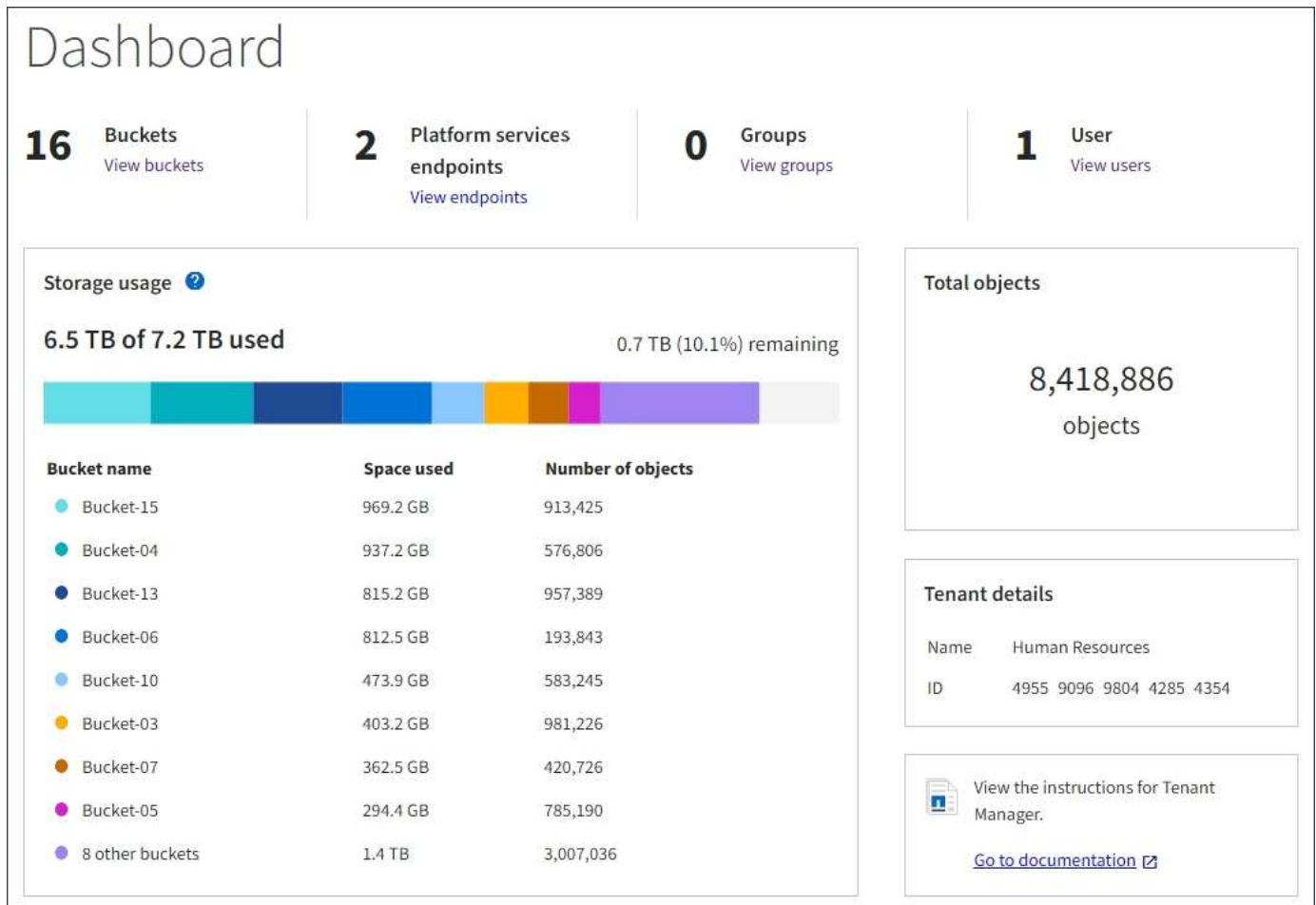
Informationen zum Tenant Manager Dashboard

Das Mandanten-Manager-Dashboard bietet einen Überblick über die Konfiguration eines Mandanten-Accounts sowie den Speicherplatz, der von Objekten in Buckets (S3) oder Containern (Swift) verwendet wird. Wenn der Mandant ein Kontingent hat, zeigt das Dashboard an, wie viel des Kontingents verwendet wird und wie viel übrig ist. Wenn beim Mandantenkonto Fehler auftreten, werden die Fehler im Dashboard angezeigt.



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

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



Zusammenfassung des Mandantenkontos

Oben im Dashboard sind folgende Informationen enthalten:

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

Sie können die Links auswählen, um die Details anzuzeigen.

Auf der rechten Seite des Dashboards sind folgende Informationen enthalten:

- Die Gesamtzahl der Objekte für den Mandanten.

Wenn bei einem S3-Konto keine Objekte aufgenommen wurden und Sie über die Berechtigung Stammzugriff verfügen, werden Startrichtlinien anstelle der Gesamtzahl der Objekte angezeigt.

- Name und ID des Mandantenkontos
- Ein Link zur StorageGRID-Dokumentation.

Storage- und Kontingentnutzung

Das Fenster Speichernutzung enthält die folgenden Informationen:

- Die Menge der Objektdaten für den Mandanten.



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

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



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

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

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



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

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

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


Warnmeldungen zur Kontingentnutzung

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

Wenn 90% oder mehr der Quote eines Mandanten verwendet wurden, wird die Meldung **Tenant Quotenverbrauch hoch** ausgelöst. Weitere Informationen finden Sie unter Alerts Referenz in den Anweisungen zum Monitoring und zur Fehlerbehebung von StorageGRID.

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

Wenn Sie Ihr Kontingent überschreiten, können Sie keine neuen Objekte hochladen.


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



Weitere Details sowie das Management von Regeln und Benachrichtigungen für Warnmeldungen finden Sie in den Anweisungen zum Monitoring und zur Fehlerbehebung von StorageGRID.

Endpunktfehler

Wenn Sie mithilfe des Grid Manager einen oder mehrere Endpunkte für die Verwendung mit Plattformdiensten konfiguriert haben, zeigt das Tenant Manager Dashboard eine Warnung an, wenn innerhalb der letzten sieben Tage Endpoint-Fehler aufgetreten sind.

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

Wenn Sie Details zu einem Endpunktfehler anzeigen möchten, wählen Sie Endpunkte aus, um die Seite Endpunkte anzuzeigen.

Verwandte Informationen

["Fehlerbehebung bei Endpoint-Fehlern bei Plattform-Services"](#)

["Monitor Fehlerbehebung"](#)

Das Mandantenmanagement-API von NetApp

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

Die Mandantenmanagement-API verwendet die Swagger Open Source API-Plattform. Swagger bietet eine intuitive Benutzeroberfläche, über die Entwickler und nicht-Entwickler mit der API interagieren können. Die

Swagger-Benutzeroberfläche bietet vollständige Details und Dokumentation für jeden API-Vorgang.

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

Schritte

1. Melden Sie sich beim Tenant Manager an.
2. Wählen Sie in der Kopfzeile des Mandanten-Managers die Option **Hilfe > API-Dokumentation** aus.

API-Betrieb

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

- **Account** — Betrieb auf dem aktuellen Mandantenkonto, einschließlich der Speicherung Informationen zur Nutzung.
- **Auth** — Operationen zur Authentifizierung der Benutzersitzung.

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

Informationen zur Verbesserung der Authentifizierungssicherheit finden Sie unter „Protecting Against Cross-Site Request Forgery“.



Wenn Single Sign-On (SSO) für das StorageGRID-System aktiviert ist, müssen Sie zur Authentifizierung verschiedene Schritte durchführen. Weitere Informationen finden Sie unter „Authentifizierung bei Aktivierung der einmaligen Anmeldung bei der API“ in den Anweisungen zum Verwalten von StorageGRID.

- **Config** — Operationen bezogen auf die Produktversion und Versionen der Mandantenmanagement-API. Sie können die Produktversion und die Hauptversionen der von dieser Version unterstützten API auflisten.
- **Container** — Betrieb auf S3 Buckets oder Swift Containern, wie folgt:

Protokoll	Berechtigung erlaubt
S3	<ul style="list-style-type: none">• Erstellen von konformen und nicht konformen Buckets• Ändern von Compliance-Einstellungen für ältere Versionen• Festlegen der Consistency Control für Vorgänge, die an Objekten ausgeführt werden• Erstellen, Aktualisieren und Löschen der CORS-Konfiguration eines Buckets• Aktivieren und Deaktivieren von Updates der letzten Zugriffszeit für Objekte• Verwalten der Konfigurationseinstellungen für Plattformservices, einschließlich CloudMirror-Replizierung, Benachrichtigungen und Suchintegration (Metadatenbenachrichtigung)• Leere Buckets werden gelöscht

Protokoll	Berechtigung erlaubt
Swift	Festlegen der für Container verwendeten Konsistenzstufe

- **Deaktivierte Funktionen** — Funktionen zum Anzeigen von Funktionen, die möglicherweise deaktiviert wurden.
- **Endpunkte** — Operationen zur Verwaltung eines Endpunkts. Endpunkte ermöglichen es einem S3-Bucket, einen externen Service für die Replizierung, Benachrichtigungen oder Suchintegration von StorageGRID CloudMirror zu verwenden.
- **Groups** — Operations zur Verwaltung lokaler Mandantengruppen und zum Abrufen von verbundenen Mandantengruppen aus einer externen Identitätsquelle.
- **Identity-Source** — Operationen, um eine externe Identitätsquelle zu konfigurieren und föderierte Gruppen- und Benutzerinformationen manuell zu synchronisieren.
- **Regionen** — Operationen zur Bestimmung, welche Regionen für das StorageGRID-System konfiguriert wurden.
- **s3** — Betrieb zum Managen von S3-Zugriffsschlüsseln für Mandantenbenutzer.
- **s3-Object-Lock** — Operationen zur Bestimmung der globalen S3-Objektsperre (Compliance) für das StorageGRID-System.
- **Benutzer** — Operationen zum Anzeigen und Verwalten von Mandantenbenutzern.

Betriebsdetails

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

groups Operations on groups

GET

/org/groups Lists Tenant User Groups

Parameters

Try it out

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

Responses

Response content type

application/json

Code Description

200

Example Value Model

```
{
  "responseTime": "2018-02-01T16:22:31.066Z",
  "status": "success",
  "apiVersion": "2.1"
}
```

API-Anforderungen werden ausgegeben



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

Schritte

1. Klicken Sie auf die HTTP-Aktion, um die Anfragedetails anzuzeigen.
2. Stellen Sie fest, ob für die Anforderung zusätzliche Parameter erforderlich sind, z. B. eine Gruppe oder eine Benutzer-ID. Dann erhalten Sie diese Werte. Sie müssen möglicherweise zuerst eine andere API-Anfrage stellen, um die Informationen zu erhalten, die Sie benötigen.
3. Bestimmen Sie, ob Sie den Text für die Beispielanforderung ändern müssen. In diesem Fall können Sie auf **Modell** klicken, um die Anforderungen für jedes Feld zu erfahren.

4. Klicken Sie auf **Probieren Sie es aus**.
5. Geben Sie alle erforderlichen Parameter ein, oder ändern Sie den Anforderungskörper nach Bedarf.
6. Klicken Sie Auf **Ausführen**.
7. Überprüfen Sie den Antwortcode, um festzustellen, ob die Anfrage erfolgreich war.

Verwandte Informationen

["Schutz vor standortübergreifenden Anfrageschmieden \(CSRF\)"](#)

["StorageGRID verwalten"](#)

Mandantenmanagement-API-Versionierung

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

Diese Anforderungs-URL gibt beispielsweise Version 3 der API an.

```
https://hostname_or_ip_address/api/v3/authorize
```

Die Hauptversion der Mandantenmanagement-API wird angestoßen, wenn Änderungen vorgenommen werden, die mit älteren Versionen **nicht kompatibel** sind. Die Nebenversion der Mandantenmanagement-API wird angestoßen, wenn Änderungen vorgenommen werden, dass **kompatibel** mit älteren Versionen sind. Zu den kompatiblen Änderungen gehört das Hinzufügen neuer Endpunkte oder neuer Eigenschaften. Das folgende Beispiel zeigt, wie die API-Version basierend auf dem Typ der vorgenommenen Änderungen angestoßen wird.

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

Wenn die StorageGRID-Software zum ersten Mal installiert wird, ist nur die neueste Version der Mandantenmanagement-API aktiviert. Wenn StorageGRID jedoch auf eine neue Funktionsversion aktualisiert wird, haben Sie weiterhin Zugriff auf die ältere API-Version für mindestens eine StorageGRID-Funktionsversion.

Veraltete Anfragen werden wie folgt als veraltet markiert:

- Der Antwortkopf ist "Deprecated: True"
- Der JSON-Antwortkörper enthält „veraltet“: Wahr

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

Verwenden Sie die folgende API-Anforderung, um eine Liste der unterstützten API-Hauptversionen anzuzeigen:

```
GET https://{{IP-Address}}/api/versions
{
  "responseTime": "2019-01-10T20:41:00.845Z",
  "status": "success",
  "apiVersion": "3.0",
  "data": [
    2,
    3
  ]
}
```

Angeben einer API-Version für eine Anforderung

Sie können die API-Version mithilfe eines Pfadparameters angeben (`/api/v3`) Oder eine Kopfzeile (`Api-Version: 3`). Wenn Sie beide Werte angeben, überschreibt der Kopfzeilenwert den Pfadwert.

```
curl https://[IP-Address]/api/v3/grid/accounts

curl -H "Api-Version: 3" https://[IP-Address]/api/grid/accounts
```

Schutz vor standortübergreifenden Anfrageschmieden (CSRF)

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

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

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

Um die Funktion zu aktivieren, stellen Sie die ein `csrfToken` Parameter an `true` Während der Authentifizierung. Die Standardeinstellung lautet `false`.


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

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

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

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

Weitere Beispiele und Details finden Sie in der Online-API-Dokumentation.



Anforderungen, die über ein CSRF-Token-Cookie-Set verfügen, werden auch die durchsetzen `"Content-Type: application/json"` Kopfzeile für jede Anfrage, die einen JSON-Anforderungskörper als zusätzlichen Schutz gegen CSRF-Angriffe erwartet.

Managen des Systemzugriffs für Mandantenbenutzer

Sie gewähren Benutzern Zugriff auf ein Mandantenkonto, indem Sie Gruppen von einer föderierten Identitätsquelle importieren und Verwaltungsberechtigungen zuweisen. Außerdem können lokale Mandantengruppen und Benutzer erstellt werden, es sei denn, Single Sign On (SSO) gilt für das gesamte StorageGRID System.

- ["Identitätsföderation verwenden"](#)
- ["Verwalten von Gruppen"](#)
- ["Verwalten von lokalen Benutzern"](#)

Identitätsföderation verwenden

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

- ["Konfigurieren einer föderierten Identitätsquelle"](#)
- ["Synchronisierung mit der Identitätsquelle erzwingen"](#)
- ["Identitätsföderation deaktivieren"](#)

Konfigurieren einer föderierten Identitätsquelle

Sie können eine Identitätsföderation konfigurieren, wenn Mandantengruppen und Benutzer in einem anderen System wie Active Directory, OpenLDAP oder Oracle Directory Server verwaltet werden sollen.

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Tenant Manager angemeldet sein.
- Sie müssen über spezifische Zugriffsberechtigungen verfügen.
- Sie müssen Active Directory, OpenLDAP oder Oracle Directory Server als Identitäts-Provider verwenden. Wenn Sie einen nicht aufgeführten LDAP v3-Dienst verwenden möchten, müssen Sie sich an den technischen Support wenden.
- Wenn Sie Transport Layer Security (TLS) für die Kommunikation mit dem LDAP-Server verwenden möchten, muss der Identitäts-Provider TLS 1.2 oder 1.3 verwenden.

Über diese Aufgabe

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



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

Schritte

1. Wählen Sie *** ACCESS MANAGEMENT* > Identity Federation**.
2. Wählen Sie **Identitätsföderation aktivieren**.
3. Wählen Sie im Abschnitt LDAP-Diensttyp **Active Directory**, **OpenLDAP** oder **Other** aus.

Wenn Sie **OpenLDAP** wählen, konfigurieren Sie den OpenLDAP-Server. Weitere Informationen zur Konfiguration eines OpenLDAP-Servers finden Sie in den Richtlinien.

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

4. Wenn Sie **Sonstige** ausgewählt haben, füllen Sie die Felder im Abschnitt LDAP-Attribute aus.
 - **Eindeutiger Benutzername**: Der Name des Attributs, das die eindeutige Kennung eines LDAP-Benutzers enthält. Dieses Attribut ist äquivalent zu `sAMAccountName` Für Active Directory und `uid` Für OpenLDAP. Wenn Sie Oracle Directory Server konfigurieren, geben Sie ein `uid`.
 - **Benutzer-UUID**: Der Name des Attributs, das den permanenten eindeutigen Identifier eines LDAP-Benutzers enthält. Dieses Attribut ist äquivalent zu `objectGUID` Für Active Directory und `entryUUID` Für OpenLDAP. Wenn Sie Oracle Directory Server konfigurieren, geben Sie ein `nsuniqueid`. Der Wert jedes Benutzers für das angegebene Attribut muss eine 32-stellige Hexadezimalzahl im 16-Byte- oder String-Format sein, wobei Bindestriche ignoriert werden.
 - **Group Unique Name**: Der Name des Attributs, das den eindeutigen Identifier einer LDAP-Gruppe enthält. Dieses Attribut ist äquivalent zu `sAMAccountName` Für Active Directory und `cn` Für OpenLDAP. Wenn Sie Oracle Directory Server konfigurieren, geben Sie ein `cn`.

- **Group UUID:** Der Name des Attributs, das den permanenten eindeutigen Identifier einer LDAP-Gruppe enthält. Dieses Attribut ist äquivalent zu `objectGUID` Für Active Directory und `entryUUID` Für OpenLDAP. Wenn Sie Oracle Directory Server konfigurieren, geben Sie ein `nsuniqueid`. Der Wert jeder Gruppe für das angegebene Attribut muss eine 32-stellige Hexadezimalzahl im 16-Byte- oder String-Format sein, wobei Bindestriche ignoriert werden.

5. Geben Sie im Abschnitt LDAP-Server konfigurieren die erforderlichen Informationen zum LDAP-Server und zur Netzwerkverbindung ein.

- **Hostname:** Der Server-Hostname oder die IP-Adresse des LDAP-Servers.
- **Port:** Der Port, über den eine Verbindung zum LDAP-Server hergestellt wird. Der Standardport für STARTTLS ist 389 und der Standardport für LDAPS ist 636. Sie können jedoch jeden beliebigen Port verwenden, solange Ihre Firewall korrekt konfiguriert ist.
- **Benutzername:** Der vollständige Pfad des Distinguished Name (DN) für den Benutzer, der eine Verbindung zum LDAP-Server herstellt. Für Active Directory können Sie auch den unten angegebenen Anmeldenamen oder den Benutzerprinzipalnamen festlegen.

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

- `sAMAccountName` Oder `uid`
- `objectGUID`, `entryUUID`, Oder `nsuniqueid`
- `cn`
- `memberOf` Oder `isMemberOf`

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

Die **Group Unique Name**-Werte müssen innerhalb der **Group-Basis-DN**, zu der sie gehören, eindeutig sein.

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

Die **User Unique Name**-Werte müssen innerhalb der **User Base DN**, zu der sie gehören, eindeutig sein.

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

- **Verwenden Sie STARTTLS (empfohlen):** Verwenden Sie STARTTLS, um die Kommunikation mit dem LDAP-Server zu sichern. Dies ist die empfohlene Option.
- **LDAPS verwenden:** Die Option LDAPS (LDAP über SSL) verwendet TLS, um eine Verbindung zum LDAP-Server herzustellen. Diese Option wird aus Kompatibilitätsgründen unterstützt.
- **Verwenden Sie keine TLS:** Der Netzwerkverkehr zwischen dem StorageGRID-System und dem LDAP-Server wird nicht gesichert.

Diese Option wird nicht unterstützt, wenn Ihr Active Directory-Server die LDAP-Signatur erzwingt. Sie müssen STARTTLS oder LDAPS verwenden.

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

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

8. Wählen Sie **Verbindung testen**, um die Verbindungseinstellungen für den LDAP-Server zu validieren.

Wenn die Verbindung gültig ist, wird oben rechts auf der Seite eine Bestätigungsmeldung angezeigt.

9. Wenn die Verbindung gültig ist, wählen Sie **Speichern**.

Der folgende Screenshot zeigt Beispielkonfigurationswerte für einen LDAP-Server, der Active Directory verwendet.

Verwandte Informationen

["Mandantenmanagement-Berechtigungen"](#)

["Richtlinien für die Konfiguration eines OpenLDAP-Servers"](#)

Richtlinien für die Konfiguration eines OpenLDAP-Servers

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

Überlagerungen in Memberof und Refint

Die Überlagerungen Memberof und Refint sollten aktiviert sein. Weitere Informationen finden Sie im Administratorhandbuch für OpenLDAP in den Anweisungen zur Wartung der Reverse-Group-Mitgliedschaft.

Indizierung

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

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

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

Weitere Informationen zur Wartung der Umkehrgruppenmitgliedschaft finden Sie im Administratorhandbuch für OpenLDAP.

Synchronisierung mit der Identitätsquelle erzwingen

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

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Tenant Manager angemeldet sein.
- Sie müssen über spezifische Zugriffsberechtigungen verfügen.
- Die gespeicherte Identitätsquelle muss aktiviert sein.

Schritte

1. Wählen Sie * ACCESS MANAGEMENT* > **Identity Federation**.

Die Seite Identitätsföderation wird angezeigt. Die Schaltfläche **Sync Server** befindet sich oben rechts auf der Seite.



Wenn die gespeicherte Identitätsquelle nicht aktiviert ist, ist die Schaltfläche **Sync Server** nicht aktiv.

2. Wählen Sie **Sync Server**.

Eine Bestätigungsmeldung zeigt an, dass die Synchronisierung erfolgreich gestartet wurde.

Verwandte Informationen

["Mandantenmanagement-Berechtigungen"](#)

Identitätsföderation deaktivieren

Wenn Sie einen Identitätsföderationsdienst für diesen Mandanten konfiguriert haben, können Sie die Identitätsföderation für Mandanten und Benutzer vorübergehend oder dauerhaft deaktivieren. Wenn die Identitätsföderation deaktiviert ist, besteht keine Kommunikation zwischen dem StorageGRID-System und der Identitätsquelle. Allerdings bleiben alle von Ihnen konfigurierten Einstellungen erhalten, sodass Sie die Identitätsföderation zukünftig einfach wieder aktivieren können.

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Tenant Manager angemeldet sein.
- Sie müssen über spezifische Zugriffsberechtigungen verfügen.

Über diese Aufgabe

Bevor Sie die Identitätsföderation deaktivieren, sollten Sie Folgendes beachten:

- Verbundene Benutzer können sich nicht anmelden.
- Föderierte Benutzer, die derzeit angemeldet sind, erhalten bis zum Ablauf ihrer Sitzung Zugriff auf das Mandantenkonto, können sich jedoch nach Ablauf ihrer Sitzung nicht anmelden.
- Es erfolgt keine Synchronisierung zwischen dem StorageGRID-System und der Identitätsquelle.

Schritte

1. Wählen Sie * ACCESS MANAGEMENT* > **Identity Federation**.
2. Deaktivieren Sie das Kontrollkästchen * Identitätsföderation aktivieren*.
3. Wählen Sie **Speichern**.

Verwandte Informationen

["Mandantenmanagement-Berechtigungen"](#)

Verwalten von Gruppen

Sie weisen Benutzergruppen Berechtigungen zu, um zu steuern, welche Aufgaben Mandantenbenutzer durchführen können. Sie können föderierte Gruppen aus einer Identitätsquelle importieren, z. B. Active Directory oder OpenLDAP, oder Sie können lokale Gruppen erstellen.



Wenn Single Sign-On (SSO) für Ihr StorageGRID-System aktiviert ist, können sich lokale Benutzer nicht beim Mandanten-Manager anmelden, obwohl sie auf Basis der Gruppenberechtigungen auf S3- und Swift-Ressourcen zugreifen können.

Mandantenmanagement-Berechtigungen

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

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

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

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



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

Sie können einer Gruppe die folgenden Berechtigungen zuweisen. Beachten Sie, dass S3-Mandanten und Swift-Mandanten unterschiedliche Gruppenberechtigungen haben. Änderungen können aufgrund des Caching bis zu 15 Minuten dauern.

Berechtigung	Beschreibung
Root-Zugriff	<p>Bietet vollständigen Zugriff auf den Tenant Manager und die Mandanten-Management-API.</p> <p>Hinweis: Swift-Benutzer müssen Root Access-Berechtigung haben, um sich beim Mandantenkonto anzumelden.</p>
Verwalter	<p>Nur Swift Mandanten. Bietet vollständigen Zugriff auf die Swift Container und Objekte für dieses Mandantenkonto</p> <p>Hinweis: Swift-Benutzer müssen über die Swift-Administrator-Berechtigung verfügen, um alle Operationen mit der Swift REST-API auszuführen.</p>
Management Ihrer eigenen S3 Credentials	<p>Nur S3-Mandanten. Benutzer können ihre eigenen S3-Zugriffsschlüssel erstellen und entfernen. Benutzer, die diese Berechtigung nicht besitzen, sehen nicht die Menüoption STORAGE (S3) > Meine S3-Zugriffstasten.</p>
Alle Buckets Verwalten	<ul style="list-style-type: none"> • S3-Mandanten: Ermöglicht Benutzern die Nutzung des Mandanten-Manager und der Mandanten-Management-API, um S3-Buckets zu erstellen und zu löschen sowie die Einstellungen für alle S3-Buckets im Mandantenkonto zu managen, unabhängig von S3-Bucket- oder Gruppenrichtlinien. <p>Benutzer, die diese Berechtigung nicht besitzen, sehen die Menüoption Buckets nicht.</p> <ul style="list-style-type: none"> • Swift Mandanten: Ermöglicht Swift Benutzern die Kontrolle der Konsistenzstufe für Swift Container mithilfe der Mandanten-Management-API. <p>Hinweis: Sie können Swift-Gruppen nur die Berechtigung Alle Buckets verwalten aus der Mandantenmanagement-API zuweisen. Sie können diese Berechtigung nicht Swift-Gruppen mit dem Tenant Manager zuweisen.</p>
Endpunkte Managen	<p>Nur S3-Mandanten. Ermöglicht Benutzern, Endpunkte mithilfe des Mandanten-Managers oder der Mandanten-Management-API zu erstellen oder zu bearbeiten, die als Ziel für StorageGRID-Platformservices verwendet werden.</p> <p>Benutzer, die diese Berechtigung nicht besitzen, sehen nicht die Menüoption Platform Services Endpunkte.</p>

Verwandte Informationen

["S3 verwenden"](#)

["Verwenden Sie Swift"](#)

Erstellen von Gruppen für einen S3-Mandanten

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

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Tenant Manager angemeldet sein.
- Sie müssen einer Benutzergruppe mit Root Access-Berechtigung angehören.
- Wenn Sie eine föderierte Gruppe importieren möchten, haben Sie einen Identitätsverbund konfiguriert, und die föderierte Gruppe ist bereits in der konfigurierten Identitätsquelle vorhanden.

Schritte

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

Groups

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

2 groups Create group

Actions ▾

<input type="checkbox"/>	Name ↕	ID ↕	Type ↕	Access mode ↕
<input type="checkbox"/>	Applications	22cc2e27-88ee-4461-a8c6-30b550beeeec0	Local	Read-write
<input type="checkbox"/>	Managers	8b15b131-1d21-4539-93ad-f2298347c4d8	Local	Read-write

← Previous **1** Next →

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

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

4. Geben Sie den Namen der Gruppe ein.
 - **Lokale Gruppe**: Geben Sie einen Anzeigenamen und einen eindeutigen Namen ein. Sie können den Anzeigenamen später bearbeiten.
 - **Federated Group**: Geben Sie den eindeutigen Namen ein. Bei Active Directory ist der eindeutige Name der dem zugeordneten Name `sAMAccountName` Attribut. Bei OpenLDAP ist der eindeutige Name der Name, der dem zugeordnet ist `uid` Attribut.
5. Wählen Sie **Weiter**.
6. Wählen Sie einen Zugriffsmodus aus. Wenn ein Benutzer zu mehreren Gruppen gehört und eine beliebige Gruppe auf schreibgeschützt eingestellt ist, hat der Benutzer schreibgeschützten Zugriff auf alle ausgewählten Einstellungen und Funktionen.
 - **Lesen-Schreiben** (Standard): Benutzer können sich bei Tenant Manager anmelden und die Mandantenkonfiguration verwalten.

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

7. Wählen Sie die Gruppenberechtigungen für diese Gruppe aus.

Weitere Informationen zu Berechtigungen für die Mandantenverwaltung finden Sie unter.

8. Wählen Sie **Weiter**.

9. Wählen Sie eine Gruppenrichtlinie aus, um zu bestimmen, über welche S3-Zugriffsrechte die Mitglieder dieser Gruppe verfügen.

- **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 nur der Root-Benutzer standardmäßig Zugriff auf S3-Ressourcen.
- **Schreibgeschützter Zugriff:** Benutzer in dieser Gruppe haben schreibgeschützten Zugriff auf S3-Ressourcen. Benutzer in dieser Gruppe können beispielsweise Objekte auflisten und Objektdaten, Metadaten und Tags lesen. Wenn Sie diese Option auswählen, wird im Textfeld der JSON-String für eine schreibgeschützte Gruppenrichtlinie angezeigt. Sie können diesen String nicht bearbeiten.
- **Vollzugriff:** Benutzer in dieser Gruppe haben vollen Zugriff auf S3-Ressourcen, einschließlich Buckets. Wenn Sie diese Option auswählen, wird im Textfeld der JSON-String für eine Richtlinie mit vollem Zugriff angezeigt. Sie können diesen String nicht bearbeiten.
- **Benutzerdefiniert:** Benutzern in der Gruppe werden die Berechtigungen erteilt, die Sie im Textfeld angeben. Anweisungen zur Implementierung einer S3-Client-Applikation finden Sie in den detaillierten Informationen zu Gruppenrichtlinien, einschließlich Sprachsyntax und Beispielen.

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

In diesem Beispiel dürfen Mitglieder der Gruppe nur einen Ordner auflisten und darauf zugreifen, der ihrem Benutzernamen (Schlüsselpräfix) im angegebenen Bucket entspricht. Beachten Sie, dass bei der Festlegung der Privatsphäre dieser Ordner Zugriffsberechtigungen aus anderen Gruppenrichtlinien und der Bucket-Richtlinie berücksichtigt werden sollten.

No S3 Access

Read Only Access

Full Access

Custom
(Must be a valid JSON formatted string.)

```

{
  "Statement": [
    {
      "Sid": "AllowListBucketOfASpecificUserPrefix",
      "Effect": "Allow",
      "Action": "s3:ListBucket",
      "Resource": "arn:aws:s3:::department-bucket",
      "Condition": {
        "StringLike": {
          "s3:prefix": "${aws:username}/*"
        }
      }
    },
    {
      "Sid": "AllowUserSpecificActionsOnlyInTheSpecificFolder",
      "Effect": "Allow",
      "Action": "s3:*Object",
      "Resource": "arn:aws:s3:::department-bucket/${aws:username}/*"
    }
  ]
}

```

11. Wählen Sie die Schaltfläche aus, die angezeigt wird, je nachdem, ob Sie eine föderierte Gruppe oder eine lokale Gruppe erstellen:

- Verbundgruppe: **Gruppe erstellen**
- Lokale Gruppe: **Weiter**

Wenn Sie eine lokale Gruppe erstellen, wird Schritt 4 (Benutzer hinzufügen) angezeigt, nachdem Sie **Weiter** ausgewählt haben. Dieser Schritt wird nicht für föderierte Gruppen angezeigt.

12. Aktivieren Sie das Kontrollkästchen für jeden Benutzer, den Sie der Gruppe hinzufügen möchten, und wählen Sie dann **Gruppe erstellen**.

Optional können Sie die Gruppe speichern, ohne Benutzer hinzuzufügen. Sie können der Gruppe später Benutzer hinzufügen oder die Gruppe auswählen, wenn Sie neue Benutzer hinzufügen.

13. Wählen Sie **Fertig**.

Die von Ihnen erstellte Gruppe wird in der Gruppenliste angezeigt. Änderungen können aufgrund des Caching bis zu 15 Minuten dauern.

Verwandte Informationen

["Mandantenmanagement-Berechtigungen"](#)

["S3 verwenden"](#)

Erstellen von Gruppen für einen Swift Mandanten

Sie können Zugriffsberechtigungen für ein Swift-Mandantenkonto verwalten, indem Sie

föderierte Gruppen importieren oder lokale Gruppen erstellen. Mindestens eine Gruppe muss über die Swift-Administratorberechtigung verfügen, die zur Verwaltung der Container und Objekte für ein Swift-Mandantenkonto erforderlich ist.

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Tenant Manager angemeldet sein.
- Sie müssen einer Benutzergruppe mit Root Access-Berechtigung angehören.
- Wenn Sie eine föderierte Gruppe importieren möchten, haben Sie einen Identitätsverbund konfiguriert, und die föderierte Gruppe ist bereits in der konfigurierten Identitätsquelle vorhanden.

Schritte

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

Groups

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

2 groups Create group

Actions

<input type="checkbox"/>	Name	ID	Type	Access mode
<input type="checkbox"/>	Applications	22cc2e27-88ee-4461-a8c6-30b550beee0	Local	Read-write
<input type="checkbox"/>	Managers	8b15b131-1d21-4539-93ad-f2298347c4d8	Local	Read-write

← Previous 1 Next →

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

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

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

6. Wählen Sie einen Zugriffsmodus aus. Wenn ein Benutzer zu mehreren Gruppen gehört und eine beliebige Gruppe auf schreibgeschützt eingestellt ist, hat der Benutzer schreibgeschützten Zugriff auf alle ausgewählten Einstellungen und Funktionen.
 - **Lesen-Schreiben** (Standard): Benutzer können sich bei Tenant Manager anmelden und die Mandantenkonfiguration verwalten.
 - **Schreibgeschützt**: Benutzer können nur Einstellungen und Funktionen anzeigen. Sie können keine Änderungen vornehmen oder Vorgänge in der Mandanten-Manager- oder Mandantenmanagement-API ausführen. Lokale schreibgeschützte Benutzer können ihre eigenen Passwörter ändern.
7. Legen Sie die Gruppenberechtigung fest.
 - Aktivieren Sie das Kontrollkästchen **Root Access**, wenn sich Benutzer bei der Tenant Manager- oder Mandantenmanagement-API anmelden müssen. (Standard)
 - Deaktivieren Sie das Kontrollkästchen **Root Access**, wenn Benutzer keinen Zugriff auf die Tenant Manager- oder Mandantenmanagement-API benötigen. Deaktivieren Sie beispielsweise das Kontrollkästchen für Anwendungen, die nicht auf den Mandanten zugreifen müssen. Weisen Sie dann die **Swift Administrator**-Berechtigung zu, damit diese Benutzer Container und Objekte verwalten können.
8. Wählen Sie **Weiter**.
9. Aktivieren Sie das Kontrollkästchen **Swift Administrator**, wenn der Benutzer die Swift REST API verwenden muss.

Swift-Benutzer müssen über die Root-Zugriffsberechtigung für den Zugriff auf den Mandanten-Manager verfügen. Die Root-Zugriffsberechtigung ermöglicht Benutzern jedoch nicht, sich in der Swift REST-API zu authentifizieren, um Container zu erstellen und Objekte aufzunehmen. Benutzer müssen über die Swift-Administratorberechtigung verfügen, um sich bei der Swift-REST-API zu authentifizieren.

10. Wählen Sie die Schaltfläche aus, die angezeigt wird, je nachdem, ob Sie eine föderierte Gruppe oder eine lokale Gruppe erstellen:
 - Verbundgruppe: **Gruppe erstellen**
 - Lokale Gruppe: **Weiter**

Wenn Sie eine lokale Gruppe erstellen, wird Schritt 4 (Benutzer hinzufügen) angezeigt, nachdem Sie **Weiter** ausgewählt haben. Dieser Schritt wird nicht für föderierte Gruppen angezeigt.

11. Aktivieren Sie das Kontrollkästchen für jeden Benutzer, den Sie der Gruppe hinzufügen möchten, und wählen Sie dann **Gruppe erstellen**.

Optional können Sie die Gruppe speichern, ohne Benutzer hinzuzufügen. Sie können die Gruppe später Benutzer hinzufügen oder die Gruppe auswählen, wenn Sie neue Benutzer erstellen.

12. Wählen Sie **Fertig**.

Die von Ihnen erstellte Gruppe wird in der Gruppenliste angezeigt. Änderungen können aufgrund des Caching bis zu 15 Minuten dauern.

Verwandte Informationen

["Mandantenmanagement-Berechtigungen"](#)

["Verwenden Sie Swift"](#)

Anzeigen und Bearbeiten von Gruppendetails

Wenn Sie die Details für eine Gruppe anzeigen, können Sie den Anzeigenamen, Berechtigungen, Richtlinien und die Benutzer, die zu der Gruppe gehören, ändern.

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Tenant Manager angemeldet sein.
- Sie müssen einer Benutzergruppe mit Root Access-Berechtigung angehören.

Schritte

1. Wählen Sie **ZUGRIFFSVERWALTUNG > Gruppen**.
2. Wählen Sie den Namen der Gruppe aus, deren Details Sie anzeigen oder bearbeiten möchten.

Alternativ können Sie **Aktionen > Gruppendetails anzeigen** wählen.

Die Seite Gruppendetails wird angezeigt. Im folgenden Beispiel wird die Seite mit den S3-Gruppendetails angezeigt.

Overview

Display name:	Applications 
Unique name:	group/Applications
Type:	Local
Access mode:	Read-write
Permissions:	Root Access
S3 Policy:	None
Number of users in this group:	0

Group permissions

S3 group policy

Users

Manage group permissions

Select an access mode for this group and select one or more permissions.

Access mode

Select whether users can change settings and perform operations or whether they can only view settings and features.

Read-write Read-only

Group permissions

Select the tenant account permissions you want to assign to this group.

Root Access

Allows users to access all Tenant Manager features. Root Access permission supersedes all other permissions.

Manage All Buckets

Allows users to change settings of all S3 buckets (or Swift containers) in this account.

Manage Endpoints

Allows users to configure endpoints for platform services.

Manage Your Own S3 Credentials

Allows users to create and delete their own S3 access keys.

Save changes

3. Nehmen Sie bei Bedarf Änderungen an den Gruppeneinstellungen vor.



Um sicherzustellen, dass Ihre Änderungen gespeichert werden, wählen Sie **Änderungen speichern** aus, nachdem Sie Änderungen in jedem Abschnitt vorgenommen haben. Wenn Ihre Änderungen gespeichert sind, wird oben rechts auf der Seite eine Bestätigungsmeldung angezeigt.

a. Wählen Sie optional den Anzeigenamen oder das Bearbeitungssymbol aus  Um den Anzeigenamen zu aktualisieren.

Sie können den eindeutigen Namen einer Gruppe nicht ändern. Sie können den Anzeigenamen für eine föderierte Gruppe nicht bearbeiten.

b. Optional können Sie die Berechtigungen aktualisieren.

c. Nehmen Sie für die Gruppenrichtlinie die entsprechenden Änderungen für Ihren S3- oder Swift-Mandanten vor.

- Wenn Sie eine Gruppe für einen S3-Mandanten bearbeiten, wählen Sie optional eine andere S3-Gruppenrichtlinie aus. Wenn Sie eine benutzerdefinierte S3-Richtlinie auswählen, aktualisieren Sie den JSON-String wie erforderlich.
- Wenn Sie eine Gruppe für einen Swift-Mandanten bearbeiten, aktivieren oder deaktivieren Sie das Kontrollkästchen **Swift Administrator**.

Weitere Informationen zum Swift Administrator erhalten Sie in den Anweisungen zum Erstellen von Gruppen für einen Swift-Mandanten.

d. Optional können Benutzer hinzugefügt oder entfernt werden.

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

Änderungen können aufgrund des Caching bis zu 15 Minuten dauern.

Verwandte Informationen

["Erstellen von Gruppen für einen S3-Mandanten"](#)

["Erstellen von Gruppen für einen Swift Mandanten"](#)

Hinzufügen von Benutzern zu einer lokalen Gruppe

Sie können bei Bedarf Benutzer zu einer lokalen Gruppe hinzufügen.

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Tenant Manager angemeldet sein.
- Sie müssen einer Benutzergruppe mit Root Access-Berechtigung angehören.

Schritte

1. Wählen Sie **ZUGRIFFSVERWALTUNG > Gruppen**.
2. Wählen Sie den Namen der lokalen Gruppe aus, der Sie Benutzer hinzufügen möchten.

Alternativ können Sie **Aktionen > Gruppendetails anzeigen** wählen.

Die Seite Gruppendetails wird angezeigt.

Overview

Display name:	Applications 
Unique name:	group/Applications
Type:	Local
Access mode:	Read-write
Permissions:	Root Access
S3 Policy:	None
Number of users in this group:	0

Group permissions

S3 group policy

Users

Manage group permissions

Select an access mode for this group and select one or more permissions.

Access mode

Select whether users can change settings and perform operations or whether they can only view settings and features.

Read-write Read-only

Group permissions

Select the tenant account permissions you want to assign to this group.

Root Access

Allows users to access all Tenant Manager features. Root Access permission supersedes all other permissions.

Manage All Buckets

Allows users to change settings of all S3 buckets (or Swift containers) in this account.

Manage Endpoints

Allows users to configure endpoints for platform services.

Manage Your Own S3 Credentials

Allows users to create and delete their own S3 access keys.

Save changes

3. Wählen Sie **Benutzer verwalten** und dann **Benutzer hinzufügen**.

Username	Full Name	Denied
User_02	User_02_Managers	

4. Wählen Sie die Benutzer aus, die Sie der Gruppe hinzufügen möchten, und wählen Sie dann **Benutzer hinzufügen**.

<input checked="" type="checkbox"/>	Username	Full Name	Denied
<input checked="" type="checkbox"/>	User_01	User_01_Applications	

In der oberen rechten Ecke der Seite wird eine Bestätigungsmeldung angezeigt. Änderungen können aufgrund des Caching bis zu 15 Minuten dauern.

Gruppennamen bearbeiten

Sie können den Anzeigenamen für eine Gruppe bearbeiten. Sie können den eindeutigen Namen für eine Gruppe nicht bearbeiten.

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Tenant Manager angemeldet sein.
- Sie müssen einer Benutzergruppe mit Root Access-Berechtigung angehören.

Schritte

1. Wählen Sie **ZUGRIFFSVERWALTUNG > Gruppen**.
2. Aktivieren Sie das Kontrollkästchen für die Gruppe, deren Anzeigename Sie bearbeiten möchten.
3. Wählen Sie **Aktionen > Gruppenname bearbeiten**.

Das Dialogfeld Gruppenname bearbeiten wird angezeigt.

Edit group name ✕

Specify a new name for the group **Applications**.

Must contain at least 1 and no more than 32 characters

Applications

Cancel Save changes

4. Wenn Sie eine lokale Gruppe bearbeiten, aktualisieren Sie den Anzeigenamen nach Bedarf.

Sie können den eindeutigen Namen einer Gruppe nicht ändern. Sie können den Anzeigenamen für eine föderierte Gruppe nicht bearbeiten.

5. Wählen Sie **Änderungen speichern**.

In der oberen rechten Ecke der Seite wird eine Bestätigungsmeldung angezeigt. Änderungen können aufgrund des Caching bis zu 15 Minuten dauern.

Verwandte Informationen

["Mandantenmanagement-Berechtigungen"](#)

Duplizieren einer Gruppe

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

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Tenant Manager angemeldet sein.
- Sie müssen einer Benutzergruppe mit Root Access-Berechtigung angehören.

Schritte

1. Wählen Sie **ZUGRIFFSVERWALTUNG > Gruppen**.
2. Aktivieren Sie das Kontrollkästchen für die Gruppe, die Sie duplizieren möchten.
3. Wählen Sie **Gruppe duplizieren**. Weitere Details zum Erstellen einer Gruppe finden Sie in den Anweisungen zum Erstellen von Gruppen für einen S3-Mandanten oder für einen Swift-Mandanten.
4. Wählen Sie die Registerkarte **Lokale Gruppe** aus, um eine lokale Gruppe zu erstellen, oder wählen Sie die Registerkarte **Federated Group** aus, um eine Gruppe aus der zuvor konfigurierten Identitätsquelle zu importieren.

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

5. Geben Sie den Namen der Gruppe ein.

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

6. Wählen Sie **Weiter**.

7. Ändern Sie bei Bedarf die Berechtigungen für diese Gruppe.

8. Wählen Sie **Weiter**.

9. Wenn Sie eine Gruppe für einen S3-Mandanten duplizieren, wählen Sie bei Bedarf aus den Optionsfeldern **S3-Richtlinie hinzufügen** eine andere Richtlinie aus. Wenn Sie eine benutzerdefinierte Richtlinie ausgewählt haben, aktualisieren Sie den JSON-String wie erforderlich.

10. Wählen Sie **Gruppe erstellen**.

Verwandte Informationen

["Erstellen von Gruppen für einen S3-Mandanten"](#)

["Erstellen von Gruppen für einen Swift Mandanten"](#)

["Mandantenmanagement-Berechtigungen"](#)

Löschen einer Gruppe

Sie können eine Gruppe aus dem System löschen. Benutzer, die nur zu dieser Gruppe gehören, können sich nicht mehr beim Mandantenmanager anmelden oder das Mandantenkonto verwenden.

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Tenant Manager angemeldet sein.
- Sie müssen einer Benutzergruppe mit Root Access-Berechtigung angehören.

Schritte

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

Groups

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

2 groups Create group

Actions ▼

<input type="checkbox"/>	Name ↕	ID ↕	Type ↕	Access mode ↕
<input type="checkbox"/>	Applications	22cc2e27-88ee-4461-a8c6-30b550beee0	Local	Read-write
<input type="checkbox"/>	Managers	8b15b131-1d21-4539-93ad-f2298347c4d8	Local	Read-write

← Previous **1** Next →

2. Aktivieren Sie die Kontrollkästchen für die Gruppen, die Sie löschen möchten.
3. Wählen Sie **Aktionen** > **Gruppe löschen**.

Eine Bestätigungsmeldung wird angezeigt.

4. Wählen Sie **Gruppe löschen**, um zu bestätigen, dass Sie die in der Bestätigungsmeldung angegebenen Gruppen löschen möchten.

In der oberen rechten Ecke der Seite wird eine Bestätigungsmeldung angezeigt. Änderungen können aufgrund des Caching bis zu 15 Minuten dauern.

Verwandte Informationen

["Mandantenmanagement-Berechtigungen"](#)

Verwalten von lokalen Benutzern

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

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Tenant Manager angemeldet sein.
- Sie müssen zu einer Lese-/Schreib-Benutzergruppe mit Root Access-Berechtigung gehören.



Wenn Single Sign-On (SSO) für Ihr StorageGRID-System aktiviert ist, können sich lokale Benutzer nicht beim Mandanten-Manager oder bei der Mandantenmanagement-API anmelden, auch wenn sie mithilfe von S3- oder Swift-Client-Applikationen auf die Ressourcen des Mandanten zugreifen können, basierend auf Gruppenberechtigungen.

Zugriff auf die Seite Benutzer

Wählen Sie **ZUGRIFFSVERWALTUNG > Benutzer**.

Users

View local and federated users. Edit properties and group membership of local users.

3 users Create user

Actions ▾

<input type="checkbox"/>	Username ▾	Full Name ▾	Denied ▾	Type ▾
<input type="checkbox"/>	root	Root		Local
<input type="checkbox"/>	User_01	User_01		Local
<input type="checkbox"/>	User_02	User_02		Local

Erstellen lokaler Benutzer

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

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

Swift-Benutzer, die keiner Gruppe angehören, haben weder Managementberechtigungen noch Swift-Container-Zugriff.

Schritte

1. Wählen Sie **Benutzer erstellen**.
2. Füllen Sie die folgenden Felder aus.
 - **Vollständiger Name:** Der vollständige Name für diesen Benutzer, zum Beispiel der vor- und Nachname einer Person oder der Name einer Anwendung.
 - **Benutzername:** Der Name, den dieser Benutzer zur Anmeldung verwendet. Benutzernamen müssen eindeutig sein und können nicht geändert werden.
 - **Passwort:** Ein Passwort, das bei der Anmeldung des Benutzers verwendet wird.
 - **Passwort bestätigen:** Geben Sie dasselbe Passwort ein, das Sie im Feld Passwort eingegeben haben.

- **Zugriff verweigern:** Wenn Sie **Ja** wählen, kann sich dieser Benutzer nicht beim Mandantenkonto anmelden, obwohl der Benutzer noch zu einer oder mehreren Gruppen gehört.

Als Beispiel können Sie diese Funktion verwenden, um die Fähigkeit eines Benutzers, sich anzumelden, vorübergehend auszusetzen.

3. Wählen Sie **Weiter**.

4. Weisen Sie den Benutzer einer oder mehreren lokalen Gruppen zu.

Benutzer, die keiner Gruppe angehören, haben keine Verwaltungsberechtigungen. Berechtigungen sind kumulativ. Benutzer haben alle Berechtigungen für alle Gruppen, denen sie angehören.

5. Wählen Sie **Benutzer erstellen**.

Änderungen können aufgrund des Caching bis zu 15 Minuten dauern.

Benutzerdetails werden bearbeitet


Wenn Sie die Details für einen Benutzer bearbeiten, können Sie den vollständigen Namen und das Kennwort des Benutzers ändern, den Benutzer zu verschiedenen Gruppen hinzufügen und verhindern, dass der Benutzer auf den Mandanten zugreift.

Schritte

1. Wählen Sie in der Liste Benutzer den Namen des Benutzers aus, dessen Details Sie anzeigen oder bearbeiten möchten.

Alternativ können Sie das Kontrollkästchen für den Benutzer aktivieren und dann **Aktionen > Benutzerdetails anzeigen** wählen.

2. Nehmen Sie bei Bedarf Änderungen an den Benutzereinstellungen vor.

a. Ändern Sie den vollständigen Namen des Benutzers nach Bedarf, indem Sie den vollständigen Namen oder das Bearbeiten-Symbol auswählen  Im Abschnitt Übersicht.

Sie können den Benutzernamen nicht ändern.

b. Ändern Sie auf der Registerkarte **Passwort** das Kennwort des Benutzers nach Bedarf.

c. Auf der Registerkarte **Zugriff** können Sie sich anmelden (wählen Sie **Nein**) oder verhindern, dass sich der Benutzer bei Bedarf anmelden kann (wählen Sie **Ja**).

d. Fügen Sie auf der Registerkarte **Groups** den Benutzer zu Gruppen hinzu, oder entfernen Sie den Benutzer aus Gruppen nach Bedarf.

e. Wählen Sie nach Bedarf für jeden Abschnitt **Änderungen speichern**.

Änderungen können aufgrund des Caching bis zu 15 Minuten dauern.

Lokale Benutzer werden dupliziert

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

Schritte

1. Wählen Sie in der Liste Benutzer den Benutzer aus, den Sie duplizieren möchten.

2. Wählen Sie **Benutzer duplizieren**.

3. Ändern Sie die folgenden Felder für den neuen Benutzer.

- **Vollständiger Name:** Der vollständige Name für diesen Benutzer, zum Beispiel der vor- und Nachname einer Person oder der Name einer Anwendung.
- **Benutzername:** Der Name, den dieser Benutzer zur Anmeldung verwendet. Benutzernamen müssen eindeutig sein und können nicht geändert werden.
- **Passwort:** Ein Passwort, das bei der Anmeldung des Benutzers verwendet wird.
- **Passwort bestätigen:** Geben Sie dasselbe Passwort ein, das Sie im Feld Passwort eingegeben haben.
- **Zugriff verweigern:** Wenn Sie **Ja** wählen, kann sich dieser Benutzer nicht beim Mandantenkonto anmelden, obwohl der Benutzer noch zu einer oder mehreren Gruppen gehört.

Als Beispiel können Sie diese Funktion verwenden, um die Fähigkeit eines Benutzers, sich anzumelden, vorübergehend auszusetzen.

4. Wählen Sie **Weiter**.

5. Wählen Sie eine oder mehrere lokale Gruppen aus.

Benutzer, die keiner Gruppe angehören, haben keine Verwaltungsberechtigungen. Berechtigungen sind kumulativ. Benutzer haben alle Berechtigungen für alle Gruppen, denen sie angehören.

6. Wählen Sie **Benutzer erstellen**.

Änderungen können aufgrund des Caching bis zu 15 Minuten dauern.

Lokale Benutzer werden gelöscht

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

Mit dem Tenant Manager können Sie lokale Benutzer löschen, aber keine föderierten Benutzer. Sie müssen die föderierte Identitätsquelle verwenden, um verbundene Benutzer zu löschen.

Schritte

1. Aktivieren Sie in der Liste Benutzer das Kontrollkästchen für den lokalen Benutzer, den Sie löschen möchten.
2. Wählen Sie **Aktionen > Benutzer löschen**.
3. Wählen Sie im Bestätigungsdialoefeld **Benutzer löschen** aus, um zu bestätigen, dass Sie den Benutzer aus dem System löschen möchten.

Änderungen können aufgrund des Caching bis zu 15 Minuten dauern.

Verwandte Informationen

["Mandantenmanagement-Berechtigungen"](#)

Verwalten von S3-Mandantenkonten

Mandanten-Manager können S3-Zugriffsschlüssel managen und S3-Buckets erstellen und managen.

- ["Verwalten von S3-Zugriffsschlüsseln"](#)
- ["Management von S3-Buckets"](#)

Verwalten von S3-Zugriffsschlüsseln

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

Über diese Aufgabe

S3-Zugriffsschlüssel können wie folgt gemanagt werden:

- Benutzer, die über die **Verwalten Ihrer eigenen S3-Anmeldeinformationen**-Berechtigung verfügen, können eigene S3-Zugriffsschlüssel erstellen oder entfernen.
- Benutzer mit der Berechtigung * Root Access* können die Zugriffsschlüssel für das S3-Stammkonto und alle anderen Benutzer verwalten. Root-Zugriffsschlüssel bieten vollständigen Zugriff auf alle Buckets und Objekte für Mandanten, sofern nicht ausdrücklich von einer Bucket-Richtlinie deaktiviert wurde.

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

Erstellen Ihrer eigenen S3-Zugriffsschlüssel

Wenn Sie einen S3-Mandanten verwenden und über die entsprechenden Berechtigungen verfügen, können Sie Ihre eigenen S3-Zugriffsschlüssel erstellen. Für den Zugriff auf Buckets und Objekte im S3-Mandantenkonto ist ein Zugriffsschlüssel erforderlich.

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Tenant Manager angemeldet sein.
- Sie müssen über die Berechtigung zum Verwalten Ihrer eigenen S3-Anmeldedaten verfügen.

Über diese Aufgabe

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

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

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



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

Schritte

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

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

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

1 Choose expiration time ————— 2 Download access key

Choose expiration time

Do not set an expiration time

This access key will never expire.

Set an expiration time

MM/DD/YYYY HH : MM AM

Cancel **Create access key**

4. Wählen Sie **Zugriffsschlüssel erstellen**.

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

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



Schließen Sie dieses Dialogfeld erst, wenn Sie diese Informationen kopiert oder heruntergeladen haben.

Create access key


Choose expiration time ————— 2 Download access key

Download access key


To save the keys for future reference, select **Download .csv**, or copy and paste the values to another location.



i You will not be able to view the Access key ID or Secret access key after you close this dialog.

Access key ID

SHTBQKDRVHQ34YKKUAWX 

Secret access key

UGu9+XeACtnOWQYFdbzmgmgVXXDvCkSOzT1Osz9K 

6. Wählen Sie **Fertig**.

Die neue Taste wird auf der Seite eigene Zugriffsschlüssel angezeigt. Änderungen können aufgrund des Caching bis zu 15 Minuten dauern.

Verwandte Informationen

["Mandantenmanagement-Berechtigungen"](#)

Anzeigen der S3-Zugriffsschlüssel

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

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Tenant Manager angemeldet sein.
- Sie müssen über die Berechtigung zum Verwalten Ihrer eigenen S3-Anmeldedaten verfügen.



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

Schritte

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

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

4 keys [Create key](#)

[Delete key](#)

<input type="checkbox"/>	Access key ID ⌵	Expiration time ⌵
<input type="checkbox"/>	*****OTLS	2020-11-23 12:00:00 MST
<input type="checkbox"/>	*****0M45	2020-12-01 19:00:00 MST
<input type="checkbox"/>	*****69QJ	None
<input type="checkbox"/>	*****3R8P	None

2. Sortieren Sie die Tasten nach **Ablaufzeit** oder **Zugriffsschlüssel-ID**.
3. Erstellen Sie nach Bedarf neue Schlüssel und löschen Sie manuell nicht mehr verwendete Schlüssel.

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

Abgelaufene Schlüssel werden automatisch entfernt.

Verwandte Informationen

["Erstellen Ihrer eigenen S3-Zugriffsschlüssel"](#)

["Löschen Ihrer eigenen S3-Zugriffsschlüssel"](#)

Löschen Ihrer eigenen S3-Zugriffsschlüssel

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

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

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Tenant Manager angemeldet sein.
- Sie müssen über die Berechtigung zum Verwalten Ihrer eigenen S3-Anmeldedaten verfügen.



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

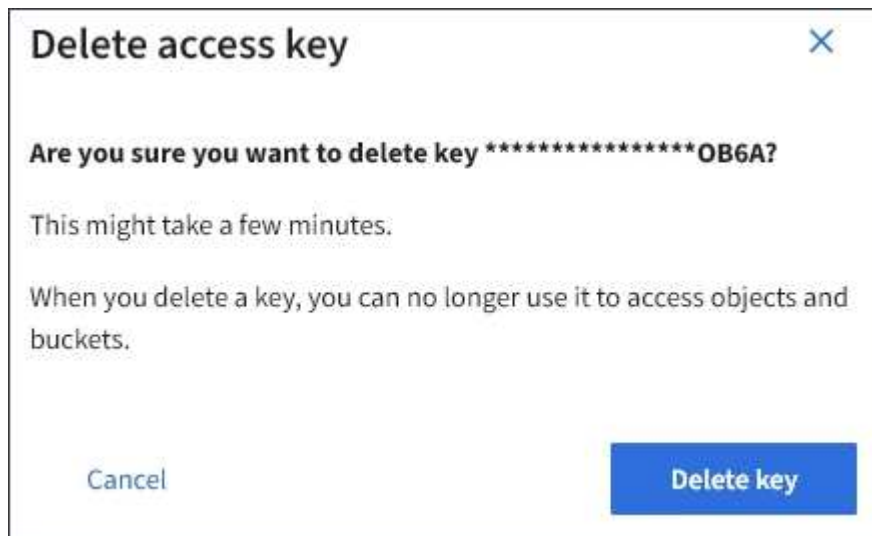
Schritte

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

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

2. Aktivieren Sie das Kontrollkästchen für jeden Zugriffsschlüssel, den Sie entfernen möchten.
3. Wählen Sie * Taste löschen*.

Ein Bestätigungsdialogfeld wird angezeigt.



4. Wählen Sie * Taste löschen*.

In der oberen rechten Ecke der Seite wird eine Bestätigungsmeldung angezeigt. Änderungen können aufgrund des Caching bis zu 15 Minuten dauern.

Verwandte Informationen

["Mandantenmanagement-Berechtigungen"](#)

Erstellen von S3-Zugriffsschlüsseln eines anderen Benutzers

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

verfügen, können Sie S3-Zugriffsschlüssel für andere Benutzer erstellen, beispielsweise Applikationen, die Zugriff auf Buckets und Objekte benötigen.

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Tenant Manager angemeldet sein.
- Sie müssen über die Berechtigung Root Access verfügen.

Über diese Aufgabe

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

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

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



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

Schritte

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

Die Seite mit den Benutzerdetails wird angezeigt.

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


Create access key

1 Choose expiration time ————— 2 Download access key

Choose expiration time

Do not set an expiration time
This access key will never expire.

Set an expiration time

MM/DD/YYYY  HH : MM AM

Cancel **Create access key**

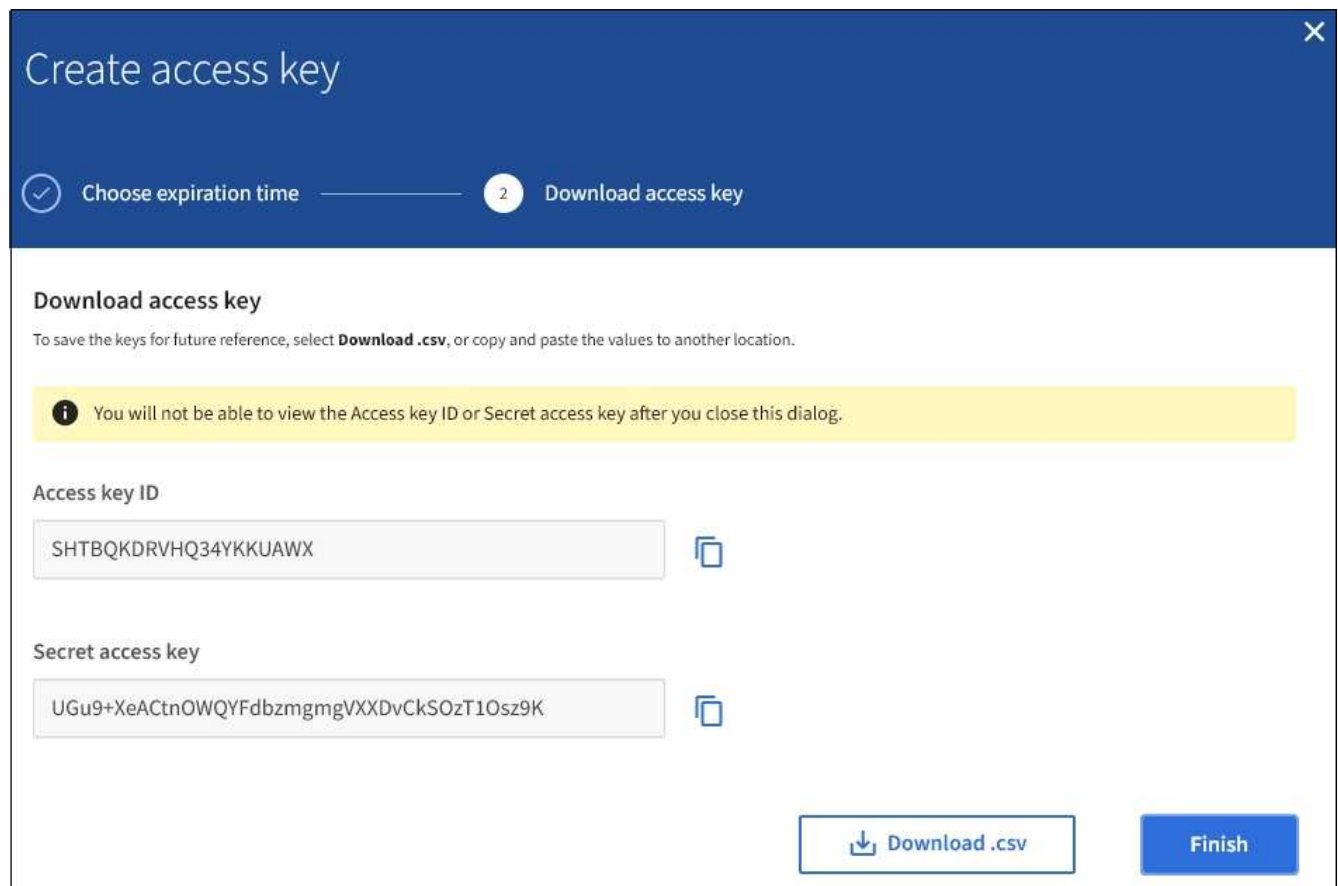
5. Wählen Sie **Zugriffsschlüssel erstellen**.

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

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



Schließen Sie dieses Dialogfeld erst, wenn Sie diese Informationen kopiert oder heruntergeladen haben.



7. Wählen Sie **Fertig**.

Der neue Schlüssel wird auf der Registerkarte Zugriffsschlüssel der Seite mit den Benutzerdetails angezeigt. Änderungen können aufgrund des Caching bis zu 15 Minuten dauern.

Verwandte Informationen

["Mandantenmanagement-Berechtigungen"](#)

Anzeigen der S3-Zugriffstasten eines anderen Benutzers

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

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Tenant Manager angemeldet sein.
- Sie müssen über die Berechtigung Root Access verfügen.



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

Schritte

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

Die Seite Benutzer wird angezeigt und listet die vorhandenen Benutzer auf.

2. Wählen Sie den Benutzer aus, dessen S3-Zugriffstasten Sie anzeigen möchten.

Die Seite Benutzerdetails wird angezeigt.

3. Wählen Sie **Zugriffstasten**.

<input type="checkbox"/>	Access key ID	Expiration time
<input type="checkbox"/>	*****WX5J	2020-11-21 12:00:00 MST
<input type="checkbox"/>	*****6OHM	2020-11-23 13:00:00 MST
<input type="checkbox"/>	*****J505	None
<input type="checkbox"/>	*****4MTF	None

4. Sortieren Sie die Tasten nach **Ablaufzeit** oder **Zugriffsschlüssel-ID**.

5. Erstellen Sie bei Bedarf neue Schlüssel und löschen Sie manuell die nicht mehr verwendeten Schlüssel.

Wenn Sie neue Schlüssel erstellen, bevor die vorhandenen Schlüssel ablaufen, kann der Benutzer mit der

Verwendung der neuen Schlüssel beginnen, ohne vorübergehend den Zugriff auf die Objekte im Konto zu verlieren.

Abgelaufene Schlüssel werden automatisch entfernt.

Verwandte Informationen

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

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

Löschen 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 löschen. Nach dem Löschen eines Zugriffsschlüssels kann dieser nicht mehr für den Zugriff auf die Objekte und Buckets im Mandantenkonto verwendet werden.

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Tenant Manager angemeldet sein.
- Sie müssen über die Berechtigung Root Access verfügen.



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

Schritte

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

Die Seite Benutzer wird angezeigt und listet die vorhandenen Benutzer auf.

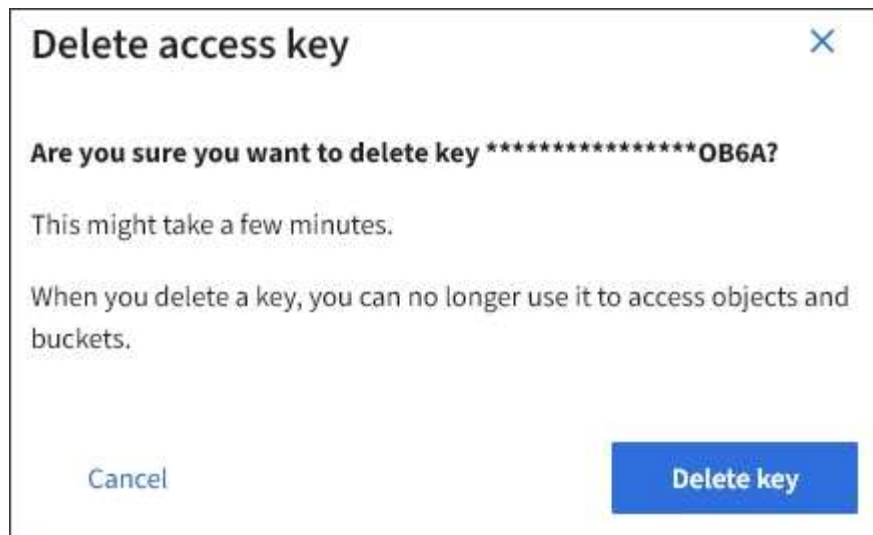
2. Wählen Sie den Benutzer aus, dessen S3-Zugriffsschlüssel Sie managen möchten.

Die Seite Benutzerdetails wird angezeigt.

3. Wählen Sie **Zugriffstasten** aus, und aktivieren Sie dann das Kontrollkästchen für jeden zu löschenden Zugriffsschlüssel.

4. Wählen Sie **Aktionen > Ausgewählte Taste löschen**.

Ein Bestätigungsdiaologfeld wird angezeigt.



5. Wählen Sie * Taste löschen*.

In der oberen rechten Ecke der Seite wird eine Bestätigungsmeldung angezeigt. Änderungen können aufgrund des Caching bis zu 15 Minuten dauern.

Verwandte Informationen

["Mandantenmanagement-Berechtigungen"](#)

Management von S3-Buckets

Wenn Sie einen S3-Mandanten mit entsprechenden Berechtigungen verwenden, können Sie S3-Buckets erstellen, anzeigen und löschen, Einstellungen für Konsistenzstufen aktualisieren, Cross-Origin Resource Sharing (CORS) konfigurieren, Einstellungen für Updates der letzten Zugriffszeit aktivieren bzw. deaktivieren und S3-Platformservices managen.

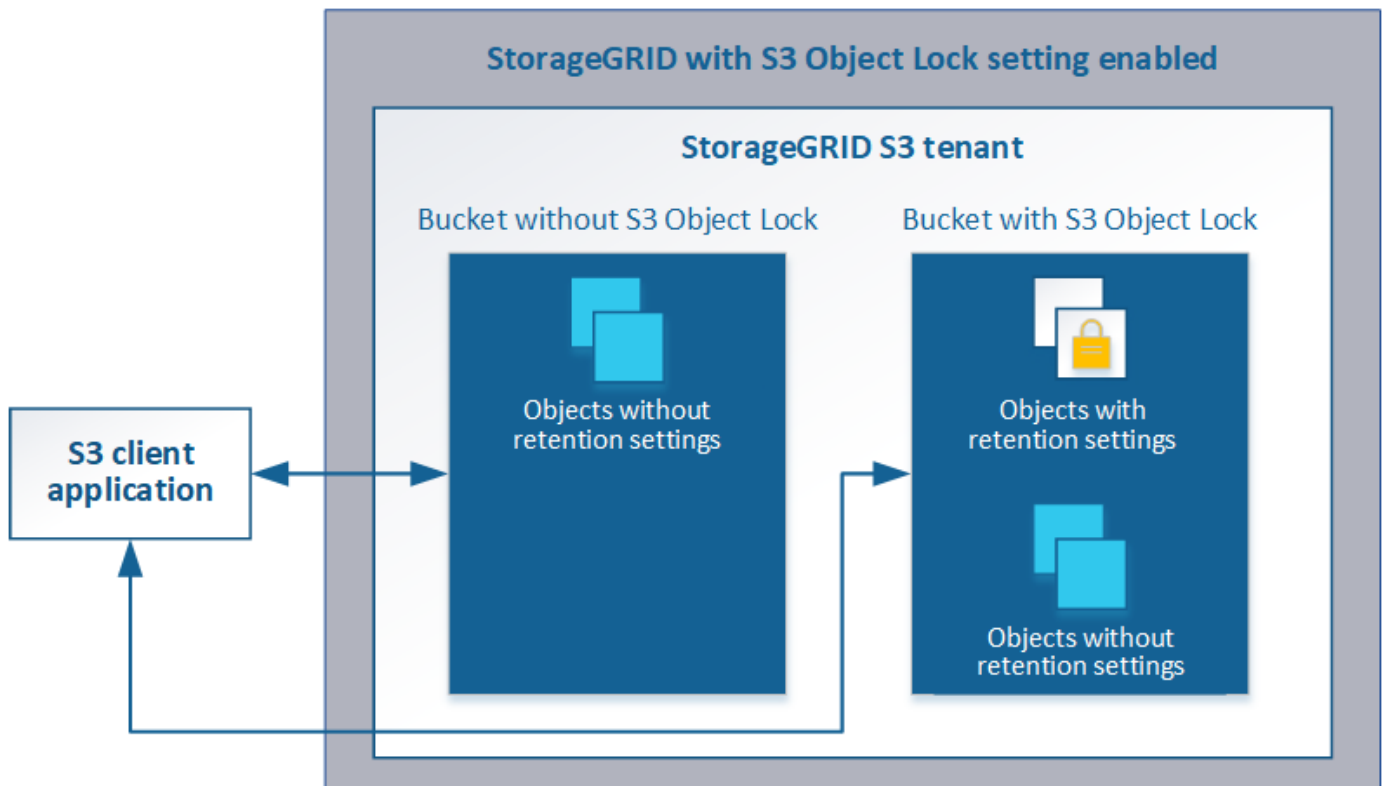
Verwenden der S3-Objektsperre

Sie können die S3-Objektsperrefunktion in StorageGRID verwenden, wenn Ihre Objekte die gesetzlichen Aufbewahrungsvorgaben erfüllen müssen.

Was ist S3 Object Lock?

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

Wenn die globale S3-Objektsperre für ein StorageGRID-System aktiviert ist, kann ein S3-Mandantenkonto Buckets mit oder ohne aktivierte S3-Objektsperre erstellen. Wenn in einem Bucket S3-Objektsperre aktiviert ist, können S3-Client-Applikationen optional Aufbewahrungseinstellungen für jede Objektversion in diesem Bucket angeben. Eine Objektversion muss über Aufbewahrungseinstellungen verfügen, die durch S3 Object Lock geschützt werden sollen.



Die StorageGRID S3 Objektsperre bietet einen einheitlichen Aufbewahrungsmodus, der dem Amazon S3-Compliance-Modus entspricht. Standardmäßig kann eine geschützte Objektversion nicht von einem Benutzer überschrieben oder gelöscht werden. Die StorageGRID S3-Objektsperre unterstützt keinen Governance-Modus und erlaubt Benutzern mit speziellen Berechtigungen nicht, Aufbewahrungseinstellungen zu umgehen oder geschützte Objekte zu löschen.

Wenn in einem Bucket S3-Objektsperre aktiviert ist, kann die S3-Client-Applikation beim Erstellen oder Aktualisieren eines Objekts optional eine oder beide der folgenden Aufbewahrungseinstellungen auf Objektebene angeben:

- **Bis-Datum aufbewahren:** Wenn das Aufbewahrungsdatum einer Objektversion in der Zukunft liegt, kann das Objekt abgerufen, aber nicht geändert oder gelöscht werden. Bei Bedarf kann das Aufbewahrungsdatum eines Objekts erhöht werden, dieses Datum kann jedoch nicht verringert werden.
- **Legal Hold:** Die Anwendung eines gesetzlichen Hold auf eine Objektversion sperrt diesen Gegenstand sofort. Beispielsweise müssen Sie ein Objekt, das mit einer Untersuchung oder einem Rechtsstreit zusammenhängt, rechtlich festhalten. Eine gesetzliche Aufbewahrungspflicht haben kein Ablaufdatum, bleiben aber bis zur ausdrücklichen Entfernung erhalten. Die gesetzlichen Aufbewahrungspflichten sind unabhängig von der bisherigen Aufbewahrungsfrist.

Weitere Informationen zu diesen Einstellungen finden Sie unter „Using S3 object Lock“ in "[Unterstützte Vorgänge und Einschränkungen durch S3-REST-API](#)".

Management älterer, konformer Buckets

Die S3-Objektsperre ersetzt die in früheren StorageGRID-Versionen verfügbare Compliance-Funktion. Wenn Sie mithilfe einer früheren Version von StorageGRID konforme Buckets erstellt haben, können Sie die Einstellungen dieser Buckets weiterhin verwalten. Sie können jedoch keine neuen, konformen Buckets mehr erstellen. Weitere Informationen finden Sie im NetApp Knowledge Base Artikel.

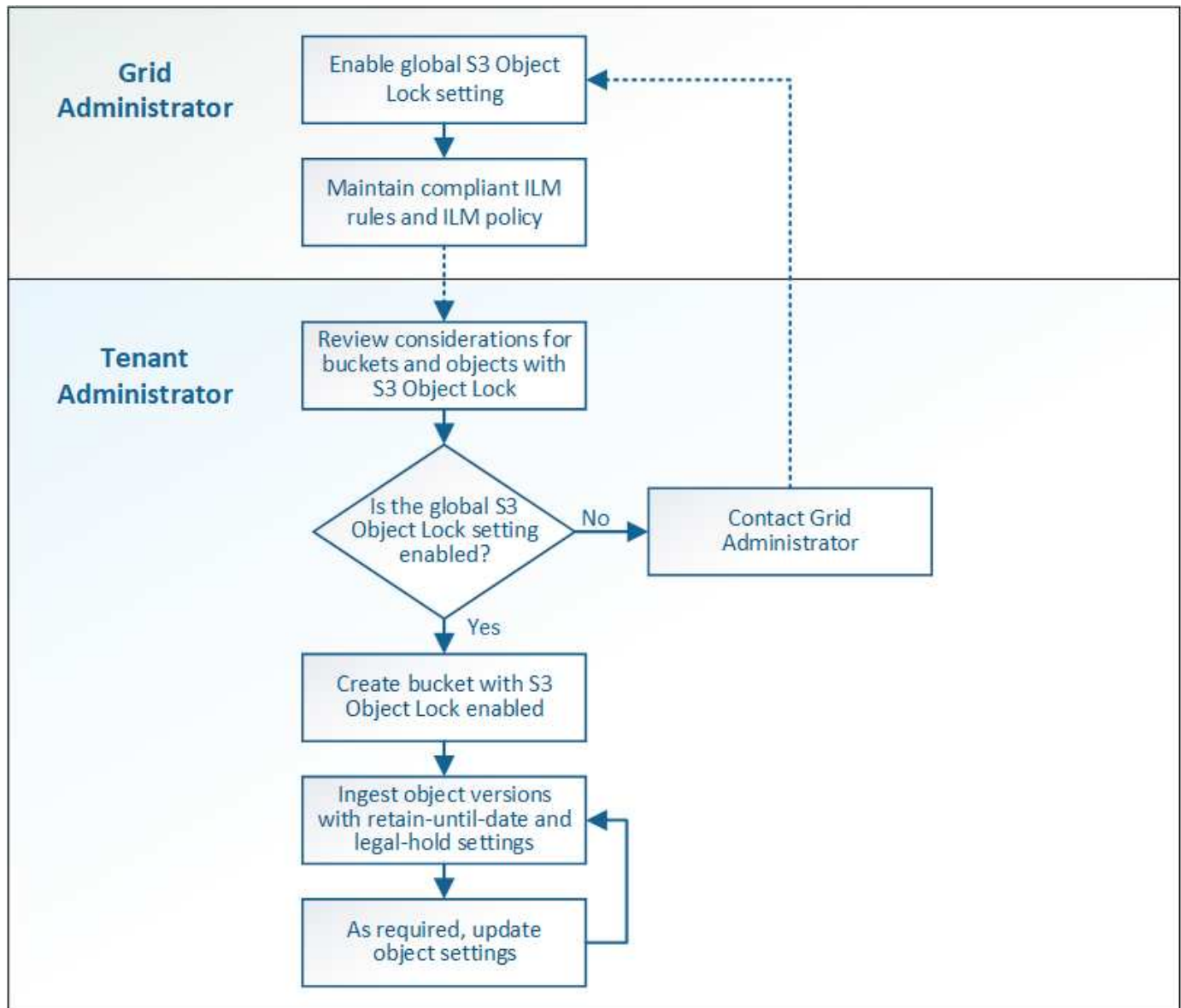
["NetApp Knowledge Base: Management älterer, konformer Buckets für StorageGRID 11.5"](#)

S3-Objektsperre-Workflow

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

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

Nachdem die globale S3-Objektsperre aktiviert wurde, können Sie Buckets mit aktivierter S3-Objektsperre erstellen. Anschließend können Sie mithilfe der S3-Client-Applikation optional Aufbewahrungseinstellungen für jede Objektversion angeben.



Verwandte Informationen

["Objektmanagement mit ILM"](#)

Anforderungen für die S3-Objektsperre

Bevor Sie die S3-Objektsperre für einen Bucket aktivieren, überprüfen Sie die Anforderungen für S3-Objektsperren-Buckets und -Objekte sowie den Lebenszyklus von Objekten in Buckets, wobei S3-Objektsperre aktiviert ist.

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

- Wenn die globale S3-Objektsperre für das StorageGRID System aktiviert ist, können Sie die Buckets mit aktivierter S3-Objektsperre über den Mandantenmanager, die Mandantenmanagement-API oder die S3-REST-API erstellen.

In diesem Beispiel aus dem Tenant Manager wird ein Bucket angezeigt, in dem S3 Object Lock aktiviert ist.

Buckets

Create buckets and manage bucket settings.

1 bucket Create bucket

Actions ▾

<input type="checkbox"/>	Name ▾	S3 Object Lock ? ▾	Region ▾	Object Count ? ▾	Space Used ? ▾	Date Created ▾
<input type="checkbox"/>	bank-records	✓	us-east-1	0	0 bytes	2021-01-06 16:53:19 MST

← Previous **1** Next →

- Wenn Sie die S3-Objektsperre verwenden möchten, müssen Sie beim Erstellen des Buckets die S3-Objektsperre aktivieren. Sie können die S3-Objektsperre für einen vorhandenen Bucket nicht aktivieren.
- Bucket-Versionierung ist mit S3 Object Lock erforderlich. Wenn die S3-Objektsperre für einen Bucket aktiviert ist, ermöglicht StorageGRID automatisch die Versionierung für diesen Bucket.
- Nachdem Sie einen Bucket mit aktivierter S3-Objektsperre erstellt haben, können Sie die S3-Objektsperre oder die Versionierung für diesen Bucket nicht deaktivieren.
- Ein StorageGRID-Bucket mit aktivierter S3-Objektsperre hat keinen standardmäßigen Aufbewahrungszeitraum. Stattdessen kann die S3-Client-Applikation optional für jede Objektversion, die zu diesem Bucket hinzugefügt wird, ein Aufbewahrungsdatum und eine Einstellung für die Aufbewahrung gemäß den gesetzlichen Aufbewahrungspflichten festlegen.
- Bucket-Lifecycle-Konfiguration wird für S3-Objekt-Lifecycle-Buckets unterstützt.
- Die CloudMirror-Replizierung wird für Buckets nicht unterstützt, wenn S3-Objektsperre aktiviert ist.

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

- Die S3-Client-Applikation muss Aufbewahrungseinstellungen für jedes Objekt angeben, das durch die S3-Objektsperre geschützt werden muss.
- Sie können das Aufbewahrungsdatum für eine Objektversion erhöhen, diesen Wert jedoch nie reduzieren.
- Wenn Sie über eine ausstehende rechtliche oder behördliche Untersuchung informiert werden, können Sie relevante Informationen erhalten, indem Sie eine gesetzliche Aufbewahrungspflichten auf eine Objektversion setzen. Wenn eine Objektversion unter einer gesetzlichen Aufbewahrungspflichten liegt,

kann das Objekt nicht aus StorageGRID gelöscht werden, auch wenn es seine Aufbewahrungsfrist bis zum letzten Tag erreicht hat. Sobald die gesetzliche Aufbewahrungspflichten aufgehoben sind, kann die Objektversion gelöscht werden, wenn das Aufbewahrungsdatum erreicht ist.

- Für die S3-Objektsperre ist die Verwendung versionierter Buckets erforderlich. Aufbewahrungseinstellungen gelten für einzelne Objektversionen. Eine Objektversion kann sowohl eine Aufbewahrungsfrist als auch eine gesetzliche Haltungseinstellung haben, eine jedoch nicht die andere oder keine. Wenn Sie eine Aufbewahrungsfrist oder eine gesetzliche Aufbewahrungseinstellung für ein Objekt angeben, wird nur die in der Anforderung angegebene Version geschützt. Sie können neue Versionen des Objekts erstellen, während die vorherige Version des Objekts gesperrt bleibt.

Lebenszyklus von Objekten in Buckets, wobei S3 Objektsperre aktiviert ist

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

1. Objektaufnahme

- Beim Hinzufügen einer Objektversion zu einem Bucket mit aktivierter S3-Objektsperre kann die S3-Client-Applikation optional Aufbewahrungseinstellungen für das Objekt festlegen (bis dato, gesetzliche Aufbewahrungspflichten oder beides). StorageGRID generiert dann Metadaten für dieses Objekt, einschließlich einer eindeutigen Objekt-ID (UUID) sowie Datum und Uhrzeit der Aufnahme.
- Nach der Aufnahme einer Objektversion mit Aufbewahrungseinstellungen können seine Daten und benutzerdefinierten S3-Metadaten nicht mehr geändert werden.
- StorageGRID speichert die Objektmetadaten unabhängig von den Objektdaten. Es behält drei Kopien aller Objektmetadaten an jedem Standort.

2. Aufbewahrung von Objekten

- StorageGRID speichert mehrere Kopien des Objekts. Die genaue Anzahl und Art der Kopien und der Speicherorte werden durch die konformen Regeln in der aktiven ILM-Richtlinie festgelegt.

3. Löschen von Objekten

- Ein Objekt kann gelöscht werden, wenn sein Aufbewahrungsdatum erreicht ist.
- Ein Objekt, das sich unter einer gesetzlichen Aufbewahrungspflichten befindet, kann nicht gelöscht werden.

Erstellen eines S3-Buckets

Sie können im Mandanten-Manager S3-Buckets für Objektdaten erstellen. Wenn Sie einen Bucket erstellen, müssen Sie Namen und Region des Bucket angeben. Wenn die globale S3-Objektsperre für das StorageGRID-System aktiviert ist, können Sie optional die S3-Objektsperre für den Bucket aktivieren.

Was Sie benötigen

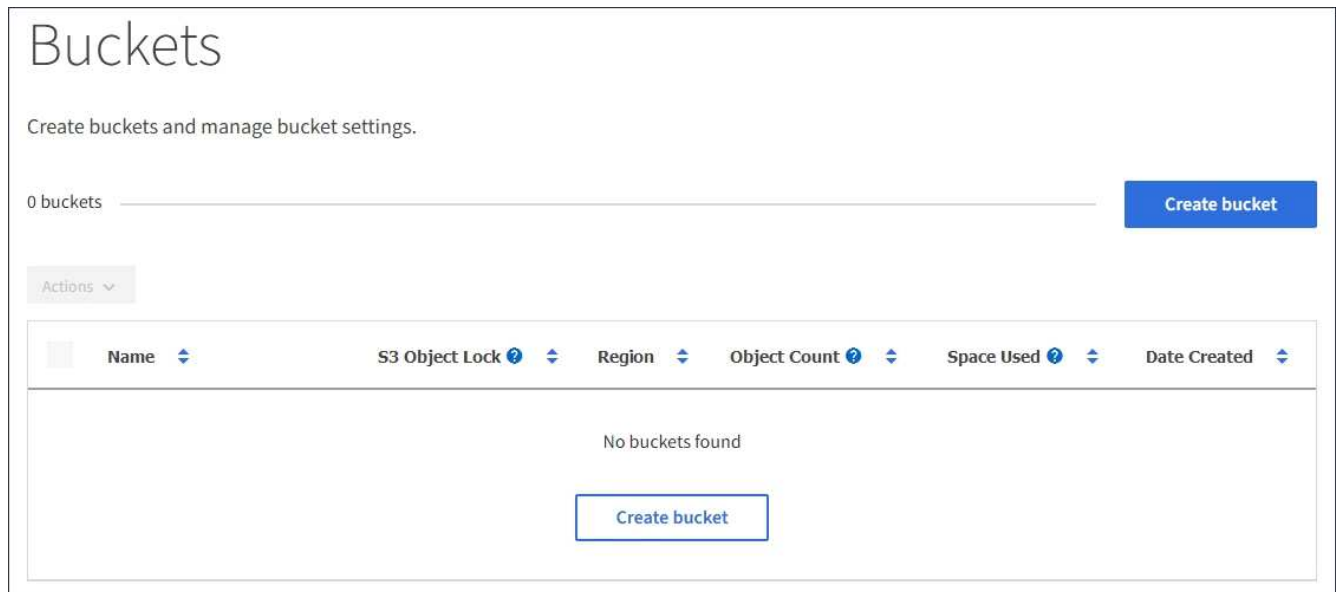
- Sie müssen über einen unterstützten Browser beim Tenant Manager angemeldet sein.
- Sie müssen einer Benutzergruppe angehören, die über die Berechtigung Alle Buckets verwalten oder Root Access verfügt. Diese Berechtigungen überschreiben die Berechtigungseinstellungen in Gruppen- oder Bucket-Richtlinien.
- Wenn Sie einen Bucket mit S3-Objektsperre erstellen möchten, muss die globale S3-Objektsperre für das StorageGRID-System aktiviert worden sein und Sie müssen die Anforderungen für S3-Objektsperren-Buckets und -Objekte überprüft haben.

["Verwenden der S3-Objektsperre"](#)

Schritte

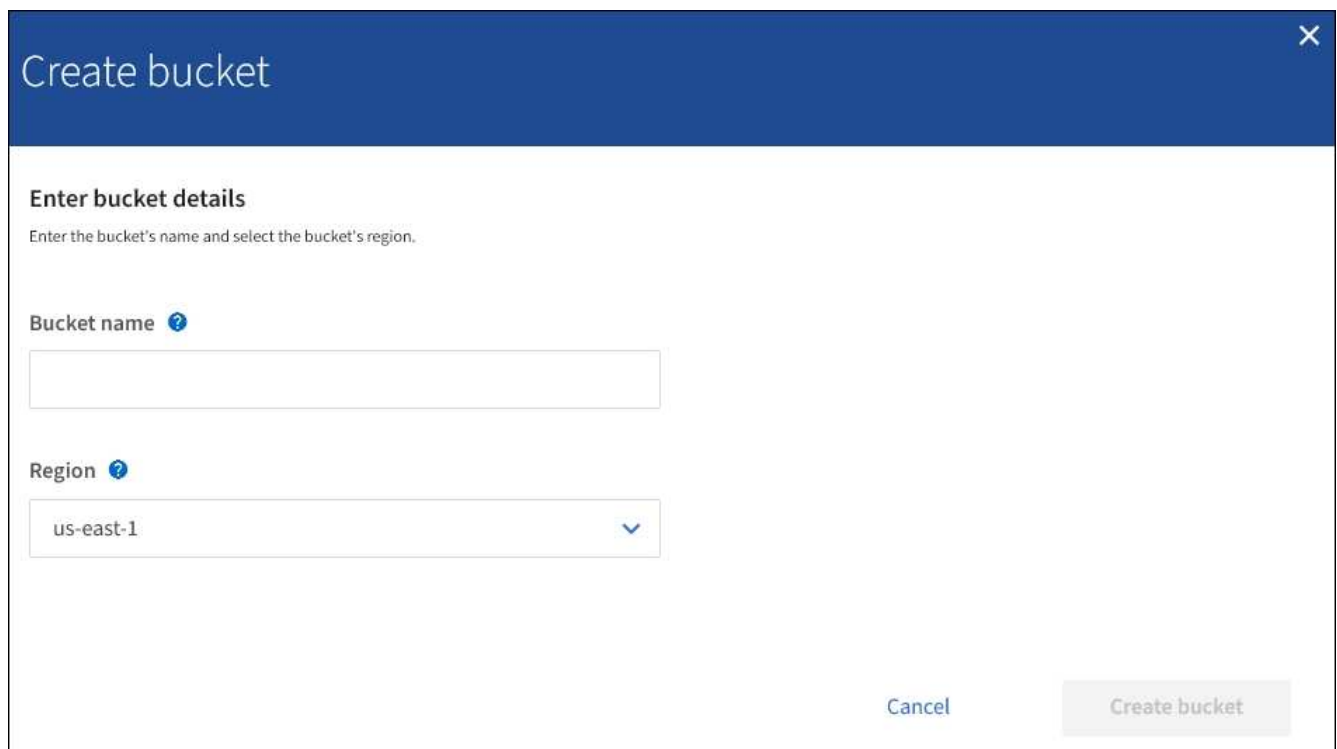
1. Wählen Sie **STORAGE (S3) > Buckets** aus.

Die Seite Buckets wird angezeigt und listet alle Buckets auf, die bereits erstellt wurden.



2. Wählen Sie **Eimer erstellen**.

Der Bucket-Assistent Erstellen wird angezeigt.



Wenn die globale S3-Objektsperre aktiviert ist, enthält Create Bucket einen zweiten Schritt zum Managen der S3-Objektsperre für den Bucket.

3. Geben Sie einen eindeutigen Namen für den Bucket ein.



Sie können den Bucket-Namen nach dem Erstellen des Buckets nicht ändern.

Bucket-Namen müssen folgende Regeln einhalten:

- Jedes StorageGRID System muss eindeutig sein (nicht nur innerhalb des Mandantenkontos).
- Muss DNS-konform sein.
- Darf mindestens 3 und nicht mehr als 63 Zeichen enthalten.
- Kann eine Reihe von einer oder mehreren Etiketten sein, wobei angrenzende Etiketten durch einen Zeitraum getrennt sind. Jedes Etikett muss mit einem Kleinbuchstaben oder einer Zahl beginnen und enden. Es können nur Kleinbuchstaben, Ziffern und Bindestriche verwendet werden.
- Darf nicht wie eine Text-formatierte IP-Adresse aussehen.
- Perioden sollten nicht in Anforderungen im virtuellen gehosteten Stil verwendet werden. Perioden verursachen Probleme bei der Überprüfung des Server-Platzhalterzertifikats.



Weitere Informationen finden Sie in der Dokumentation zu Amazon Web Services (AWS).

4. Wählen Sie die Region für diesen Bucket aus.

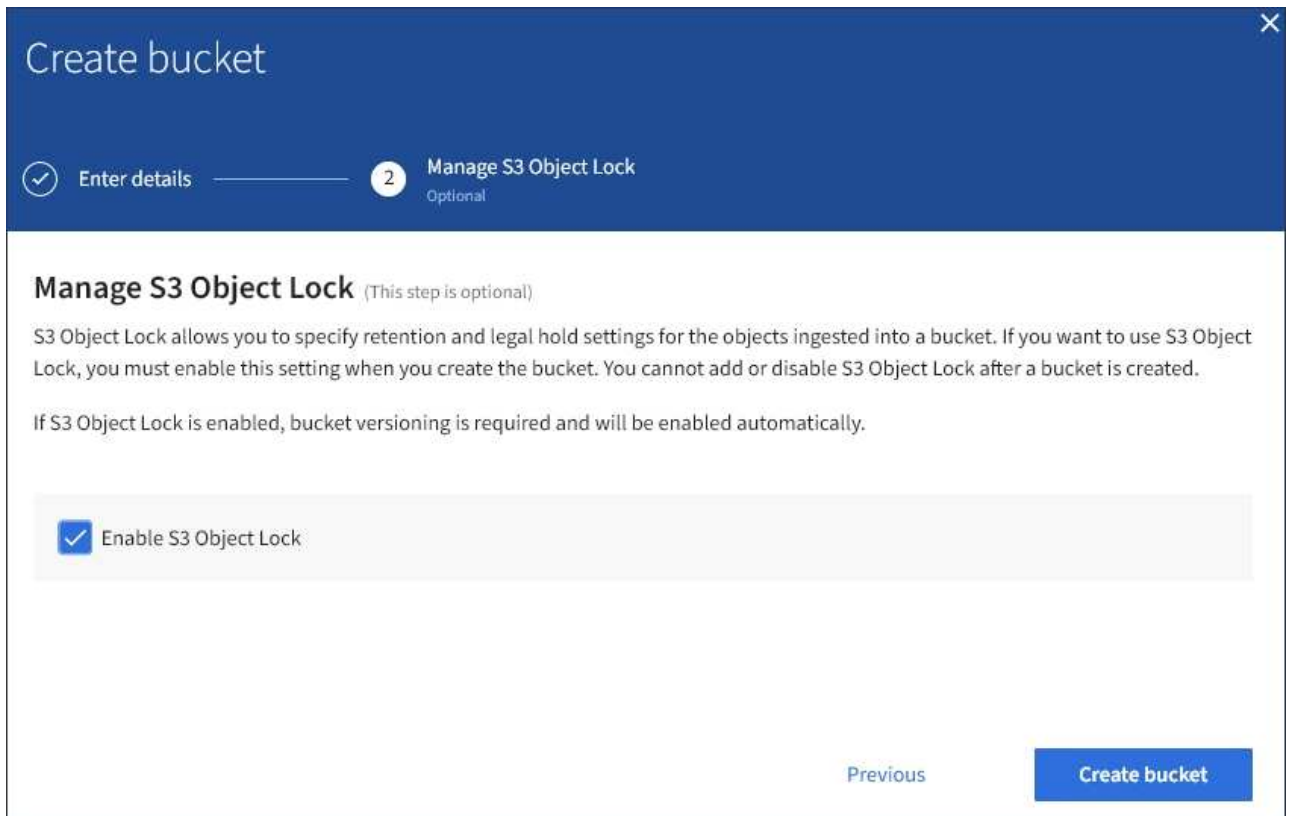
Der StorageGRID-Administrator managt die verfügbaren Regionen. Die Regionen eines Buckets können die Datensicherungsrichtlinie, die auf Objekte angewendet wird, beeinflussen. Standardmäßig werden alle Buckets im erstellten `us-east-1` erstellt.



Nach dem Erstellen des Buckets können Sie die Region nicht ändern.

5. Wählen Sie **Eimer erstellen** oder **Weiter**.

- Wenn die globale S3-Objektsperre nicht aktiviert ist, wählen Sie **Bucket erstellen** aus. Der Bucket wird erstellt und der Tabelle auf der Seite Buckets hinzugefügt.
- Wenn die globale S3-Objektsperre aktiviert ist, wählen Sie **Weiter**. Schritt 2, S3-Objektsperre verwalten, wird angezeigt.



6. Aktivieren Sie optional das Kontrollkästchen, um die S3-Objektsperre für diesen Bucket zu aktivieren.

S3-Objektsperre muss für den Bucket aktiviert sein, bevor eine S3-Client-Applikation für die dem Bucket hinzugefügten Objekte Haltungs- bis datums- und gesetzliche Aufbewahrungseinstellungen festlegen kann.



Sie können die S3-Objektsperre nach dem Erstellen des Buckets nicht aktivieren oder deaktivieren.



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

7. Wählen Sie **Eimer erstellen**.

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

Verwandte Informationen

["Objektmanagement mit ILM"](#)

["Das Mandantenmanagement-API von NetApp"](#)

["S3 verwenden"](#)

Anzeigen von S3-Bucket-Details

Sie können eine Liste der Buckets und Bucket-Einstellungen in Ihrem Mandantenkonto anzeigen.

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Tenant Manager angemeldet sein.

Schritte

1. Wählen Sie **STORAGE (S3) > Buckets** aus.

Die Seite Buckets wird angezeigt und enthält alle Buckets für das Mandantenkonto.

<input type="checkbox"/>	Name	S3 Object Lock	Region	Object Count	Space Used	Date Created
<input type="checkbox"/>	bucket-01	✓	us-east-1	0	0 bytes	2020-11-04 14:16:59 MST
<input type="checkbox"/>	bucket-02		us-east-1	0	0 bytes	2020-11-04 14:17:14 MST

2. Überprüfen Sie die Informationen für jeden Bucket.

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

- Name: Der eindeutige Name des Buckets, der nicht geändert werden kann.
- S3 Object Lock: Ob S3 Object Lock für diesen Bucket aktiviert ist.

Diese Spalte wird nicht angezeigt, wenn die globale S3-Objektsperre deaktiviert ist. In dieser Spalte werden außerdem Informationen für alle Buckets angezeigt, die für die Konformität mit älteren Daten verwendet wurden.

- Region: Die Eimer-Region, die nicht geändert werden kann.
- Objektanzahl: Die Anzahl der Objekte in diesem Bucket.
- Verwendeter Speicherplatz: Die logische Größe aller Objekte in diesem Bucket. Die logische Größe umfasst nicht den tatsächlich benötigten Speicherplatz für replizierte oder Erasure Coding-Kopien oder für Objekt-Metadaten.
- Erstellungsdatum: Das Datum und die Uhrzeit, zu der der Bucket erstellt wurde.



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

3. Um die Einstellungen für einen Bucket anzuzeigen und zu managen, wählen Sie den Bucket-Namen aus.

Die Seite mit den Bucket-Details wird angezeigt.

Auf dieser Seite können Sie die Einstellungen für Bucket-Optionen, Bucket-Zugriff und Plattform-Services anzeigen und bearbeiten.

Weitere Informationen zur Konfiguration der einzelnen Einstellungen oder des Plattform-Service finden Sie in den Anweisungen.

The screenshot shows the AWS IAM console interface for a bucket named 'bucket-02'. The breadcrumb navigation at the top reads 'Buckets > bucket-02'. Below this is an 'Overview' section with the following details:

Name:	bucket-02
Region:	us-east-1
S3 Object Lock:	Disabled
Date created:	2020-11-04 14:51:59 MST

Below the overview are three tabs: 'Bucket options' (selected), 'Bucket access', and 'Platform services'. Under the 'Bucket options' tab, there are two settings:

Consistency level	Read-after-new-write	▼
Last access time updates	Disabled	▼

Verwandte Informationen

["Ändern der Konsistenzstufe"](#)

["Aktivieren oder Deaktivieren von Updates der letzten Zugriffszeit"](#)

["Konfigurieren der Cross-Origin Resource Sharing \(CORS\)"](#)

["CloudMirror-Replizierung wird konfiguriert"](#)

["Ereignisbenachrichtigungen werden konfiguriert"](#)

["Konfigurieren des Suchintegrationservice"](#)

Ändern der Konsistenzstufe

Wenn Sie einen S3-Mandanten verwenden, können Sie mithilfe des Mandanten Manager oder der Mandanten-Management-API die Konsistenzkontrolle für Vorgänge ändern, die in den Objekten in S3 Buckets ausgeführt werden.

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Tenant Manager angemeldet sein.

- Sie müssen einer Benutzergruppe angehören, die über die Berechtigung Alle Buckets verwalten oder Root Access verfügt. Diese Berechtigungen überschreiben die Berechtigungseinstellungen in Gruppen- oder Bucket-Richtlinien.

Über diese Aufgabe

Die Konsistenzstufe sorgt für einen Kompromiss zwischen der Verfügbarkeit der Objekte und der Konsistenz dieser Objekte über verschiedene Speicherknoten und Standorte hinweg. Im Allgemeinen sollten Sie für Ihre Buckets die Konsistenzstufe **Read-after-New-write** verwenden. Wenn die Konsistenzstufe **Read-after-New-write** nicht den Anforderungen der Client-Anwendung entspricht, können Sie die Konsistenzstufe ändern, indem Sie die Bucket-Konsistenzstufe oder die verwenden `Consistency-Control` Kopfzeile. Der `Consistency-Control` Kopfzeile setzt die Bucket-Konsistenzstufe außer Kraft.



Wenn Sie die Konsistenzstufe eines Buckets ändern, werden nur die Objekte, die nach der Änderung aufgenommen werden, garantiert, um die überarbeitete Ebene zu erfüllen.

Schritte

1. Wählen Sie **STORAGE (S3) > Buckets** aus.
2. Wählen Sie den Bucket-Namen aus der Liste aus.

Die Seite mit den Bucket-Details wird angezeigt.

3. Wählen Sie **Bucket-Optionen > Konsistenzstufe** aus.

Bucket options
Bucket access
Platform services

Consistency level
Read-after-new-write (default)
⤴

Change the consistency control for operations performed on the objects in the bucket. Consistency level makes a trade-off between the availability of the objects and the consistency of those objects across different Storage Nodes and sites.

In general, use the **Read-after-new-write** consistency level for your buckets. Then, if objects do not meet availability or consistency requirements, change the client application's behavior, or set the Consistency-Control header for an individual API request, which overrides the bucket setting.

- All**
Provides the highest guarantee of consistency. All nodes receive the data immediately, or the request will fail.
- Strong-global**
Guarantees read-after-write consistency for all client requests across all sites.
- Strong-site**
Guarantees read-after-write consistency for all client requests within a site.
- Read-after-new-write (default)**
Provides read-after-write consistency for new objects and eventual consistency for object updates. Offers high availability, and data protection guarantees.

Note: If your application attempts HEAD operations on keys that do not exist, set the Consistency Level to **Available**, unless you require AWS S3 consistency guarantees. Otherwise, a high number of 500 Internal Server errors can result if one or more Storage Nodes are unavailable.

- Available**
Behaves the same as the **Read-after-new-write** consistency level, but only provides eventual consistency for HEAD operations. Offers higher availability for HEAD operations than **Read-after-new-write** if Storage Nodes are unavailable. Differs from AWS S3 consistency guarantees for HEAD operations only.

Save changes

4. Wählen Sie eine Konsistenzstufe für Operationen aus, die an den Objekten in diesem Bucket durchgeführt werden.

Konsistenzstufe	Beschreibung
Alle	Alle Nodes erhalten die Daten sofort, sonst schlägt die Anfrage fehl.

Konsistenzstufe	Beschreibung
Stark global	Garantierte Konsistenz bei Lese-nach-Schreibvorgängen für alle Client-Anfragen an allen Standorten.
Stark vor Ort	Garantiert Konsistenz bei Lese-nach-Schreibvorgängen für alle Client-Anfragen innerhalb eines Standorts.
Read-after-New-Write (Standard)	<p>Ermöglicht Konsistenz von Lese- nach Schreibvorgängen für neue Objekte und die eventuelle Konsistenz von Objekt-Updates. Hochverfügbarkeit und garantierte Datensicherung Entspricht den Amazon S3 -Konsistenzgarantien.</p> <p>Hinweis: Wenn Ihre Anwendung versucht, HEAD-Operationen auf Schlüssel, die nicht vorhanden sind, setzen Sie die Consistency Level auf available, es sei denn, Sie benötigen Amazon S3 Consistency Guarantees. Andernfalls kann eine hohe Anzahl von 500 internen Serverfehlern führen, wenn ein oder mehrere Speicherknoten nicht verfügbar sind.</p>
Verfügbar (eventuelle Konsistenz für DEN HAUPTBETRIEB)	Verhält sich wie die Konsistenz Read-after-New-write , bietet aber nur eventuelle Konsistenz für DEN KOPFBETRIEB. Bietet höhere Verfügbarkeit für DEN HAUPTBETRIEB als Read-after-New-write , wenn Speicherknoten nicht verfügbar sind. Unterschied zu Amazon S3 Konsistenzgarantien nur für HEAD-Operationen.

5. Wählen Sie **Änderungen speichern**.

Verwandte Informationen

["Mandantenmanagement-Berechtigungen"](#)

Aktivieren oder Deaktivieren von Updates der letzten Zugriffszeit

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

Diese Anweisungen gelten nur für StorageGRID-Systeme, die mindestens eine ILM-Regel enthalten, die die Option **Last Access Time** in ihrer Platzierungsanleitung verwendet. Sie können diese Anweisungen ignorieren, wenn Ihr StorageGRID System eine solche Regel nicht enthält.

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Tenant Manager angemeldet sein.
- Sie müssen einer Benutzergruppe angehören, die über die Berechtigung Alle Buckets verwalten oder Root Access verfügt. Diese Berechtigungen überschreiben die Berechtigungseinstellungen in Gruppen- oder Bucket-Richtlinien.

Letzter Zugriffszeitpunkt ist eine der Optionen für die **Referenzzeit**-Platzierungsanweisung für eine ILM-Regel. Durch Festlegen der Referenzzeit für eine Regel auf Letzter Zugriffszeit können Grid-Administratoren

festlegen, dass Objekte an bestimmten Speicherorten platziert werden, basierend auf dem Zeitpunkt, an dem diese Objekte zuletzt abgerufen wurden (gelesen oder angezeigt).

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

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



Weitere Informationen finden Sie in den Anweisungen zum Verwalten von Objekten mit Information Lifecycle Management.

Standardmäßig werden Updates zur letzten Zugriffszeit deaktiviert. Wenn Ihr StorageGRID-System eine ILM-Regel enthält, die die Option **Last Access Time** verwendet und diese Option auf Objekte in diesem Bucket angewendet werden soll, müssen Sie Aktualisierungen für die letzte Zugriffszeit für die in dieser Regel festgelegten S3-Buckets aktivieren.



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

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

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

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

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

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

Schritte

1. Wählen Sie **STORAGE (S3) > Buckets** aus.
2. Wählen Sie den Bucket-Namen aus der Liste aus.

Die Seite mit den Bucket-Details wird angezeigt.

3. Wählen Sie **Bucket-Optionen > Letzte Aktualisierung der Zugriffszeit** aus.
4. Wählen Sie das entsprechende Optionsfeld aus, um Aktualisierungen der letzten Zugriffszeit zu aktivieren oder zu deaktivieren.

Bucket options
Bucket access
Platform services

Consistency level Read-after-new-write ▼

Last access time updates Disabled ▲

Enable or disable last access time updates for the objects in this bucket.

When last access time updates are disabled, the following behavior applies to objects in the bucket:

- Requests to retrieve an object, its access control list, or its metadata do not update the object's last access time. The object is not added to ILM evaluation queues.
- Requests to update an object's metadata update the object's last access time. The object is added to ILM evaluation queues.
- Requests to copy an object from one bucket to another do not update the last access time for the source copy and do not add the source object to the ILM evaluation queue. However, the last access time is updated for the destination copy, and the destination object is added to ILM evaluation queues.
- A request to complete a multipart upload causes the last access time for the assembled object to be updated. The new object is added to ILM evaluation queues.

i Updating the last access time when an object is retrieved can reduce performance, especially for small objects.

Enable last access time updates when retrieving an object
 Disable last access time updates when retrieving an object

Save changes

5. Wählen Sie **Änderungen speichern**.

Verwandte Informationen

["Mandantenmanagement-Berechtigungen"](#)

["Objektmanagement mit ILM"](#)

Konfigurieren der Cross-Origin Resource Sharing (CORS)

Die Cross-Origin Resource Sharing (CORS) kann für einen S3-Bucket konfiguriert werden, wenn für Web-Applikationen in anderen Domänen auf diesen Bucket und Objekte in diesem Bucket zugegriffen werden soll.

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Tenant Manager angemeldet sein.
- Sie müssen einer Benutzergruppe angehören, die über die Berechtigung Alle Buckets verwalten oder Root Access verfügt. Diese Berechtigungen überschreiben die Berechtigungseinstellungen in Gruppen- oder Bucket-Richtlinien.

Über diese Aufgabe

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

Schritte

1. Verwenden Sie einen Texteditor, um die XML-Datei zu erstellen, die für die Aktivierung von CORS erforderlich ist.

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

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

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

2. Wählen Sie im Tenant Manager **STORAGE (S3) > Buckets** aus.
3. Wählen Sie den Bucket-Namen aus der Liste aus.

Die Seite mit den Bucket-Details wird angezeigt.

4. Wählen Sie **Bucket-Zugriff > Cross-Origin Resource Sharing (CORS)** aus.
5. Aktivieren Sie das Kontrollkästchen * CORS aktivieren*.
6. Fügen Sie die CORS-Konfigurations-XML in das Textfeld ein und wählen Sie **Änderungen speichern**.

Bucket options
Bucket access
Platform services

Cross-Origin Resource Sharing (CORS)

Disabled

^

Configure Cross-Origin Resource Sharing (CORS) for an S3 bucket if you want that bucket and objects in that bucket to be accessible to web applications in other domains.

Enable CORS

```

<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>
  </CORSRule>
</CORSConfiguration>

```

7. Um die CORS-Einstellung für den Bucket zu ändern, aktualisieren Sie die CORS-Konfigurations-XML im Textfeld oder wählen Sie **Löschen**, um neu zu starten. Wählen Sie dann **Änderungen speichern**.
8. Um CORS für den Bucket zu deaktivieren, deaktivieren Sie das Kontrollkästchen **CORS** aktivieren* und wählen dann **Änderungen speichern** aus.

Löschen eines S3-Buckets

Sie können den Mandanten-Manager verwenden, um einen leeren S3-Bucket zu löschen.

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Tenant Manager angemeldet sein.
- Sie müssen einer Benutzergruppe angehören, die über die Berechtigung Alle Buckets verwalten oder Root Access verfügt. Diese Berechtigungen überschreiben die Berechtigungseinstellungen in Gruppen- oder Bucket-Richtlinien.

Über diese Aufgabe

Diese Anweisungen beschreiben das Löschen eines S3-Buckets mithilfe von Tenant Manager. Sie können auch S3-Buckets mithilfe der Mandantenmanagement-API oder der S3-REST-API löschen.

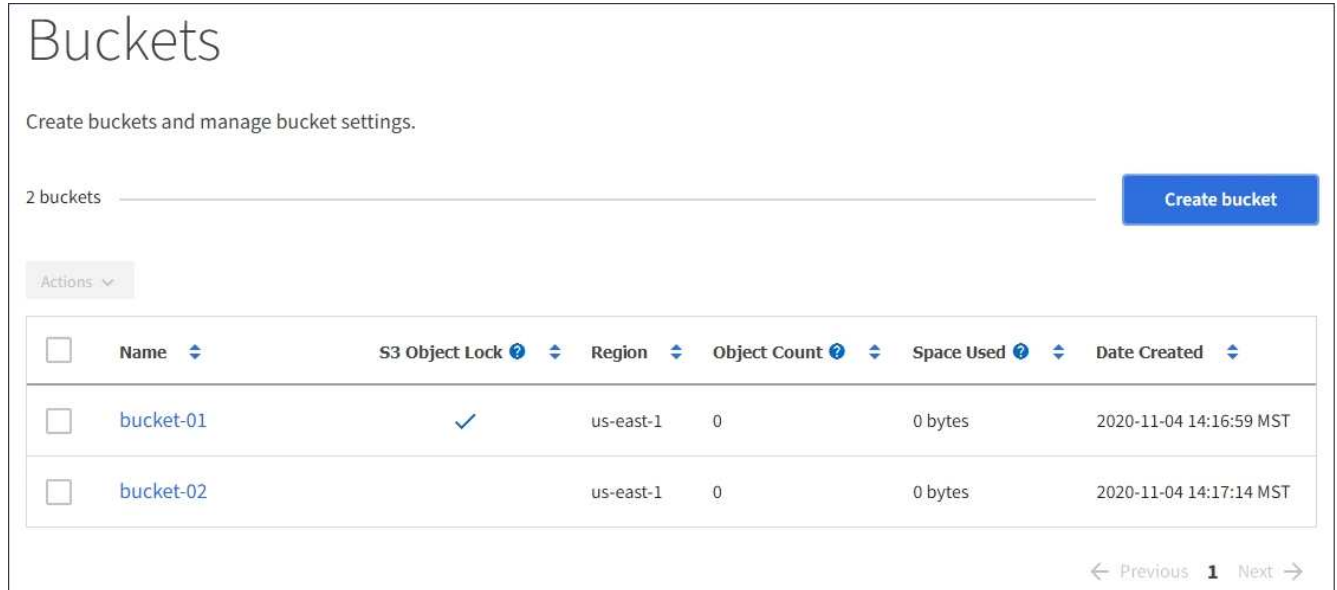
Ein S3-Bucket kann nicht gelöscht werden, wenn er Objekte oder nicht aktuelle Objektversionen enthält.

Informationen zum Löschen von S3-versionierten Objekten finden Sie in den Anweisungen zum Managen von Objekten mit Information Lifecycle Management.

Schritte

1. Wählen Sie **STORAGE (S3) > Buckets** aus.

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



The screenshot shows the AWS S3 Buckets console. At the top, it says "Buckets" and "Create buckets and manage bucket settings." Below that, it indicates "2 buckets" and has a "Create bucket" button. A table lists the buckets with columns for Name, S3 Object Lock, Region, Object Count, Space Used, and Date Created. The table contains two rows: bucket-01 and bucket-02, both in the us-east-1 region with 0 objects and 0 bytes used. An "Actions" dropdown menu is visible above the table.

<input type="checkbox"/>	Name	S3 Object Lock	Region	Object Count	Space Used	Date Created
<input type="checkbox"/>	bucket-01	✓	us-east-1	0	0 bytes	2020-11-04 14:16:59 MST
<input type="checkbox"/>	bucket-02		us-east-1	0	0 bytes	2020-11-04 14:17:14 MST

2. Aktivieren Sie das Kontrollkästchen für den leeren Bucket, den Sie löschen möchten.

Das Menü Aktionen ist aktiviert.

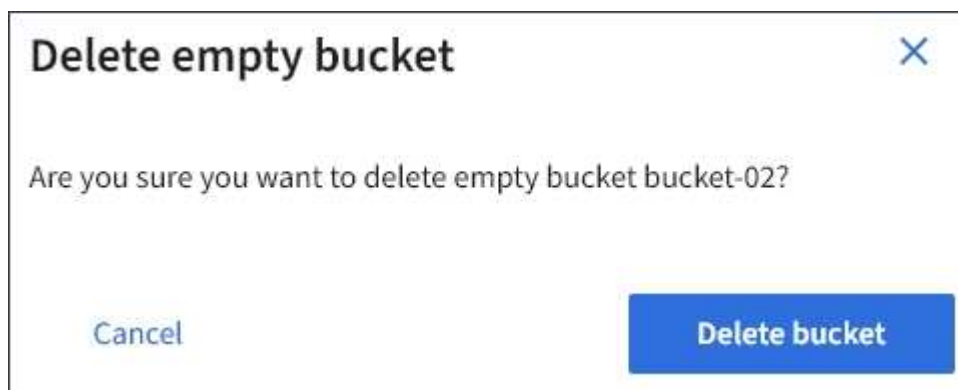
3. Wählen Sie im Menü Aktionen die Option **leerer Eimer löschen** aus.



The screenshot shows the AWS S3 Buckets console with the "Actions" dropdown menu open for bucket-02. The "Delete empty bucket" option is selected. The table below shows bucket-02 with a checked checkbox in the first column.

<input type="checkbox"/>	Name	S3 Object Lock	Region	Object Count	Space Used	Date Created
<input type="checkbox"/>	bucket-01	✓	us-east-1	0	0 bytes	2020-11-04 14:16:59 MST
<input checked="" type="checkbox"/>	bucket-02		us-east-1	0	0 bytes	2020-11-04 14:17:14 MST

Eine Bestätigungsmeldung wird angezeigt.



The screenshot shows a confirmation dialog box titled "Delete empty bucket". The text inside asks "Are you sure you want to delete empty bucket bucket-02?". There are two buttons at the bottom: "Cancel" and "Delete bucket".

4. Wenn Sie sicher sind, dass Sie den Bucket löschen möchten, wählen Sie **Bucket löschen**.

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

Wenn der Bucket nicht leer ist, wird eine Fehlermeldung angezeigt. Sie müssen alle Objekte löschen, bevor Sie den Bucket löschen können.



Unable to delete the bucket because it is not empty. You must delete all objects before you can delete this bucket.

Verwandte Informationen

["Objektmanagement mit ILM"](#)

Verwalten von S3-Plattformservices

Wenn die Nutzung von Plattform-Services für Ihr S3-Mandantenkonto zulässig ist, können Sie Plattform-Services verwenden, um externe Services zu nutzen und die Replizierung und Benachrichtigungen von CloudMirror und die Integration von S3-Buckets zu konfigurieren.

- ["Um welche Plattform-Services geht es"](#)
- ["Überlegungen bei der Verwendung von Plattform-Services"](#)
- ["Konfigurieren von Endpunkten für Plattformservices"](#)
- ["CloudMirror-Replizierung wird konfiguriert"](#)
- ["Ereignisbenachrichtigungen werden konfiguriert"](#)
- ["Verwenden des Suchintegrationsdienstes"](#)

Um welche Plattform-Services geht es

StorageGRID Plattform-Services unterstützen Sie bei der Implementierung einer Hybrid-Cloud-Strategie.

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

- **CloudMirror Replikation:** Der StorageGRID CloudMirror Replikationsservice wird verwendet, um bestimmte Objekte von einem StorageGRID-Bucket auf ein bestimmtes externes Ziel zu spiegeln.

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



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

- **Benachrichtigungen:** Per Bucket-Ereignisbenachrichtigungen werden verwendet, um Benachrichtigungen

über bestimmte Aktionen, die an Objekten ausgeführt werden, an einen bestimmten externen Amazon Simple Notification Service™ (SNS) zu senden.

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



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

- **Suchintegrationsdienst:** Der Suchintegrationsdienst dient dazu, S3-Objektmetadaten an einen bestimmten Elasticsearch-Index zu senden, in dem die Metadaten mit dem externen Dienst durchsucht oder analysiert werden können.

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



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

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

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



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

Die Konfiguration von Plattform-Services

Plattform-Services kommunizieren mit externen Endpunkten, die Sie mit dem Tenant Manager oder der Mandantenmanagement-API konfigurieren. Jeder Endpunkt stellt ein externes Ziel dar, beispielsweise einen StorageGRID S3-Bucket, einen Amazon Web Services-Bucket, ein SNS-Thema (Simple Notification Service) oder ein lokal gehostetes Elasticsearch-Cluster, in AWS oder an anderer Stelle.

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

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

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

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

Plattform-Service	S3-REST-API
Replizierung von CloudMirror	<ul style="list-style-type: none"> • GET Bucket-Replizierung • PUT Bucket-Replizierung
Benachrichtigungen	<ul style="list-style-type: none"> • Bucket-Benachrichtigung ABRUFEN • PUT Bucket-Benachrichtigung
Integration von Suchen	<ul style="list-style-type: none"> • Konfiguration der Bucket-Metadaten-Benachrichtigungen ABRUFEN • PUT Bucket-Metadaten-Benachrichtigungskonfiguration <p>Diese Vorgänge sind individuell für StorageGRID.</p>

Anweisungen zur Implementierung von S3-Client-Applikationen finden Sie in der Anleitung, wie StorageGRID diese APIs implementiert.

Verwandte Informationen

["S3 verwenden"](#)

["Allgemeines zum CloudMirror Replikationsservice"](#)

["Allgemeines zu Benachrichtigungen für Buckets"](#)

["Beschreibung des Suchintegrationsservice"](#)

["Überlegungen bei der Verwendung von Plattform-Services"](#)

Allgemeines zum CloudMirror Replikationsservice

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

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

Wenn Sie die CloudMirror-Replizierung für einen vorhandenen Bucket aktivieren, werden nur die neuen, zu

diesem Bucket hinzugefügten Objekte repliziert. Alle bestehenden Objekte im Bucket werden nicht repliziert. Um die Replizierung von vorhandenen Objekten zu erzwingen, können Sie die Metadaten des vorhandenen Objekts durch eine Objektkopie aktualisieren.



Wenn Sie mithilfe von CloudMirror-Replizierung Objekte in ein AWS S3-Ziel kopieren, beachten Sie, dass Amazon S3 die Größe benutzerdefinierter Metadaten in jeder PUT-Anforderungskopfzeile auf 2 KB beschränkt. Wenn in einem Objekt benutzerdefinierte Metadaten größer als 2 KB sind, wird dieses Objekt nicht repliziert.

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

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

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

Beim Replizieren der Objekte zum Ziel-Bucket markiert StorageGRID sie als „`replica`“. Ein StorageGRID-Zielbucket repliziert keine Objekte, die als Replikate markiert sind, und schützt Sie nicht vor versehentlichen Replikationsschleifen. Diese Replikatmarkierung ist intern in StorageGRID und verhindert nicht, dass Sie AWS CRR verwenden, wenn Sie einen Amazon S3-Bucket als Ziel verwenden.



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

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

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

Verwandte Informationen

["CloudMirror-Replizierung wird konfiguriert"](#)

Allgemeines zu Benachrichtigungen für Buckets

Sie können die Ereignisbenachrichtigung für einen S3-Bucket aktivieren, wenn StorageGRID Benachrichtigungen zu bestimmten Ereignissen an einen Amazon Simple Notification Service (SNS) als Ziel senden soll.

Sie können Ereignisbenachrichtigungen konfigurieren, indem Sie eine XML-Benachrichtigungskonfiguration mit einem Quell-Bucket verknüpfen. Die Benachrichtigungskonfiguration-XML folgt den S3-Konventionen für die Konfiguration von Bucket-Benachrichtigungen, wobei das Ziel-SNS-Thema als URN eines Endpunkts angegeben ist.

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

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

Unterstützte Benachrichtigungen und Meldungen

Die StorageGRID-Ereignisbenachrichtigung folgt der Amazon S3-API und unterliegt folgenden Einschränkungen:

- Sie können keine Benachrichtigung für die folgenden Ereignistypen konfigurieren. Diese Ereignistypen werden **nicht** unterstützt.
 - `s3:ReducedRedundancyLostObject`
 - `s3:ObjectRestore:Completed`
- Von StorageGRID gesendete Ereignisbenachrichtigungen verwenden das Standard-JSON-Format, mit der Ausnahme, dass sie einige Schlüssel nicht enthalten und bestimmte Werte für andere verwenden, wie in der Tabelle dargestellt:

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

Verwandte Informationen

["Ereignisbenachrichtigungen werden konfiguriert"](#)

Beschreibung des Suchintegrationservice

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

Der Suchintegrations-Service ist ein benutzerdefinierter StorageGRID Service, der automatisch und asynchron

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

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

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



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

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

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

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

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

Der StorageGRID Such-Integrationsservice unterstützt ein Elasticsearch-Cluster als Ziel. Wie bei den anderen Plattformdiensten wird das Ziel im Endpunkt angegeben, dessen URN in der Konfigurations-XML für den Dienst verwendet wird. Ermitteln Sie mit dem *Interoperability Matrix Tool* die unterstützten Versionen von Elasticsearch.

Verwandte Informationen

["NetApp Interoperabilitäts-Matrix-Tool"](#)

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

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

"Vom Suchintegrations-Service generierter JSON"

"Konfigurieren des Suchintegrationservice"

Überlegungen bei der Verwendung von Plattform-Services

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

Überlegungen bei der Verwendung von Plattform-Services

Überlegungen	Details
Ziel-Endpoint-Monitoring	<p>Sie müssen die Verfügbarkeit jedes Zielendpunkts überwachen. Wenn die Verbindung zum Zielendpunkt über einen längeren Zeitraum unterbrochen wird und ein großer Rückstand von Anfragen besteht, schlagen zusätzliche Clientanforderungen (wie Z. B. PUT-Anforderungen) an StorageGRID fehl. Sie müssen diese fehlgeschlagenen Anforderungen erneut versuchen, wenn der Endpunkt erreichbar ist.</p>
Drosselung des Zielendpunkts	<p>StorageGRID kann eingehende S3-Anfragen für einen Bucket drosseln, wenn die Rate, mit der die Anforderungen gesendet werden, die Rate übersteigt, mit der der Zielendpunkt die Anforderungen empfangen kann. Eine Drosselung tritt nur auf, wenn ein Rückstand von Anfragen besteht, die auf den Zielendpunkt warten.</p> <p>Der einzige sichtbare Effekt besteht darin, dass die eingehenden S3-Anforderungen länger in Anspruch nehmen. Wenn Sie die Performance deutlich schlechter erkennen, sollten Sie die Aufnahmerate reduzieren oder einen Endpunkt mit höherer Kapazität verwenden. Falls der Rückstand von Anforderungen weiterhin wächst, scheitern Client-S3-Vorgänge (wie Z. B. PUT-Anforderungen) letztendlich.</p> <p>CloudMirror-Anforderungen sind wahrscheinlicher von der Performance des Zielendpunkts betroffen, da diese Anfragen in der Regel mehr Datentransfer beinhalten als Anfragen zur Suchintegration oder Ereignisbenachrichtigung.</p>
Bestellgarantien	<p>StorageGRID garantiert die Bestellung von Vorgängen an einem Objekt innerhalb eines Standorts. Solange sich alle Vorgänge für ein Objekt innerhalb desselben Standorts befinden, entspricht der endgültige Objektstatus (für die Replizierung) immer dem Status in StorageGRID.</p> <p>StorageGRID unternimmt alle Anstrengungen, Anfragen zu bestellen, wenn die Vorgänge an verschiedenen StorageGRID Standorten durchgeführt werden. Wenn Sie beispielsweise ein Objekt zunächst an Standort A schreiben und später dasselbe Objekt an Standort B überschreiben, ist das von CloudMirror in den Ziel-Bucket replizierte Objekt nicht garantiert, dass es sich um das neuere Objekt handelt.</p>

Überlegungen	Details
ILM-gesteuerte Objektlöschungen	<p>CloudMirror und Ereignisbenachrichtigungen werden nicht gesendet, wenn ein Objekt im Quell-Bucket aufgrund von StorageGRID ILM-Regeln gelöscht wird, um das Löschverhalten der AWS CRR- und SNS-Services anzupassen. Beispiel: Es werden keine Anfragen für CloudMirror- oder Ereignisbenachrichtigungen gesendet, wenn eine ILM-Regel ein Objekt nach 14 Tagen löscht.</p> <p>Suchintegrationsanfragen werden dagegen gesendet, wenn Objekte aufgrund von ILM gelöscht werden.</p>

Überlegungen bei der Verwendung des CloudMirror Replikationsservice

Überlegungen	Details
Replikationsstatus	StorageGRID unterstützt das nicht <code>x-amz-replication-status</code> Kopfzeile.
Objektgröße	Die maximale Größe für Objekte, die vom CloudMirror-Replikationsservice in einen Ziel-Bucket repliziert werden können, beträgt 5 TB. Dies ist die gleiche wie die von StorageGRID unterstützte maximale Objektgröße.
Bucket-Versionierung und VersionIDs	<p>Wenn die Versionierung im S3-Quell-Bucket von StorageGRID aktiviert ist, sollten Sie auch die Versionierung für den Ziel-Bucket aktivieren.</p> <p>Beachten Sie bei der Verwendung der Versionierung, dass die Bestellung von Objektversionen im Ziel-Bucket am besten ist und vom CloudMirror Service nicht garantiert wird, da Einschränkungen im S3-Protokoll bestehen.</p> <p>Hinweis: Version-IDs für den Quell-Bucket in StorageGRID stehen nicht im Zusammenhang mit den Version-IDs für den Ziel-Bucket.</p>

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

Verwandte Informationen

["S3 verwenden"](#)

Konfigurieren von Endpunkten für Plattformservices

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

Der Zugriff auf Plattform-Services wird von einem StorageGRID Administrator nach Mandanten aktiviert. Um einen Endpunkt für Plattformservices zu erstellen oder zu verwenden, müssen Sie ein Mandantenbenutzer mit Berechtigung zum Verwalten von Endpunkten oder Root-Zugriff in einem Grid sein, dessen Netzwerk konfiguriert wurde, damit Storage-Nodes auf externe Endpoint-Ressourcen zugreifen können. Weitere Informationen erhalten Sie von Ihrem StorageGRID Administrator.

Was ist ein Endpunkt für Plattformservices

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

Wenn Sie beispielsweise Objekte von einem StorageGRID-Bucket auf einen S3-Bucket replizieren möchten, erstellen Sie einen Endpunkt für Plattformservices, der die Informationen und Anmeldeinformationen enthält, die StorageGRID für den Zugriff auf den Ziel-Bucket von AWS benötigt.

Für jeden Plattformservice ist ein eigener Endpunkt erforderlich. Daher müssen Sie für jeden zu verwendenden Plattformservice mindestens einen Endpunkt konfigurieren. Nachdem Sie einen Endpunkt für Plattformservices definiert haben, verwenden Sie den URN des Endpunkts als Ziel in der zum Aktivieren des Dienstes verwendeten Konfigurations-XML.

Sie können für mehrere Quell-Buckets denselben Endpunkt wie das Ziel verwenden. Beispielsweise könnten Sie mehrere Quell-Buckets konfigurieren, um Objektmetadaten an denselben Endpunkt für die Integration der Suchfunktion zu senden, sodass Sie Suchvorgänge über mehrere Buckets durchführen können. Sie können auch einen Quell-Bucket so konfigurieren, dass mehrere Endpunkte als Ziel verwendet werden. Dies ermöglicht es Ihnen, z. B. Benachrichtigungen zur Objekterstellung an ein SNS-Thema zu senden und Benachrichtigungen zum Löschen von Objekten an ein zweites SNS-Thema zu senden.

Endpunkte für CloudMirror Replizierung

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

Endpunkte für Benachrichtigungen

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

Endpunkte für den Suchintegrations-Service

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

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

Verwandte Informationen

["StorageGRID verwalten"](#)

Festlegen des URN für einen Endpunkt der Plattformdienste

Wenn Sie einen Endpunkt für Plattformservices erstellen, müssen Sie einen eindeutigen Ressourcennamen (URN) angeben. Sie verwenden den URN, um auf den Endpunkt zu verweisen, wenn Sie Konfigurations-XML für den Plattformdienst erstellen. Der URN für jeden Endpunkt muss eindeutig sein.

StorageGRID validiert die Endpunkte der Plattformservices bei ihrer Erstellung. Bevor Sie einen Endpunkt für

Platformservices erstellen, vergewissern Sie sich, dass die im Endpunkt angegebene Ressource vorhanden ist und dass sie erreicht werden kann.

Elemente URN

Der URN für einen Endpunkt von Platformservices muss mit beiden beginnen `arn:aws` Oder `urn:mysite`, Wie folgt:

- Wenn der Service auf AWS gehostet wird, verwenden Sie `arn:aws`.
- Wenn der Service lokal gehostet wird, verwenden Sie `urn:mysite`

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

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

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

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

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

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

Urns für Services, die auf AWS gehostet werden

Für AWS Einheiten ist Complete URN ein gültiger AWS ARN. Beispiel:

- CloudMirror-Replizierung:

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

- Benachrichtigungen:

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

- Integration von Suchen:

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



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

Urnen für vor Ort gehostete Services

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

- CloudMirror-Replizierung:

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

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

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

- Benachrichtigungen:

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

- Integration von Suchen:

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



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

Erstellen eines Endpunkts für Plattformservices

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

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Tenant Manager angemeldet sein.
- Plattform-Services müssen von einem StorageGRID-Administrator für Ihr Mandantenkonto aktiviert werden.
- Sie müssen einer Benutzergruppe angehören, die über die Berechtigung Endpunkte verwalten verfügt.
- Die Ressource, auf die der Endpunkt der Plattformservices verweist, muss erstellt worden sein:
 - CloudMirror Replizierung: S3 Bucket
 - Ereignisbenachrichtigung: SNS-Thema
 - Suchbenachrichtigung: Elasticsearch-Index, wenn das Ziel-Cluster nicht konfiguriert ist, Indizes automatisch zu erstellen.
- Sie müssen über die Informationen zur Zielressource verfügen:
 - Host und Port für den Uniform Resource Identifier (URI)



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

- Eindeutiger Ressourcenname (URN)

"Festlegen des URN für einen Endpunkt der Plattfordienste"

- Authentifizierungsdaten (falls erforderlich):
 - Zugriffsschlüssel: Zugriffsschlüssel-ID und geheimer Zugriffsschlüssel
 - Basic HTTP: Benutzername und Passwort
- Sicherheitszertifikat (bei Verwendung eines benutzerdefinierten CA-Zertifikats)

Schritte

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

Die Seite „Endpunkte der Plattfordienste“ wird angezeigt.

Platform services endpoints

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

0 endpoints

Create endpoint

Delete endpoint

	Display name ?	Last error ?	Type ?	URI ?	URN ?
No endpoints found					
<p>Create endpoint</p>					

2. Wählen Sie **Endpoint erstellen**.

Create endpoint ✕

1 Enter details

2 Select authentication type
Optional

3 Verify server
Optional

Enter endpoint details

Enter the endpoint's display name, URI, and URN.

Display name ?

URI ?

URN ?

Cancel
Continue

3. Geben Sie einen Anzeigenamen ein, um den Endpunkt und seinen Zweck kurz zu beschreiben.

Der vom Endpunkt unterstützte Plattforddienst wird neben dem Endpunkt-Namen angezeigt, wenn er auf der Seite Endpoints aufgeführt wird. Sie müssen diese Informationen also nicht in den Namen einfügen.

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

Verwenden Sie eines der folgenden Formate:

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

Wenn Sie keinen Port angeben, wird Port 443 für HTTPS-URIs verwendet, und Port 80 wird für HTTP-URIs verwendet.

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

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

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



Wenn möglich, sollten Sie sich mit einer HA-Gruppe von Lastausgleichs Nodes verbinden, um einen Single Point of Failure zu vermeiden.

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

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



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

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



Sie können den URN eines Endpunktes nicht ändern, nachdem der Endpunkt erstellt wurde.

6. Wählen Sie **Weiter**.

7. Wählen Sie einen Wert für **Authentifizierungstyp** aus, und geben Sie dann die erforderlichen Anmeldedaten ein.

Create endpoint

1 Enter details — 2 Select authentication type (Optional) — 3 Verify server (Optional)

Authentication type ?

Select the method used to authenticate connections to the endpoint.

Anonymous ✓

Anonymous

Access Key

Basic HTTP

Previous Continue

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

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

8. Wählen Sie **Weiter**.

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

Create endpoint ✕

✓ Enter details

✓ Select authentication type
Optional

3 Verify server
Optional

Verify server

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

Use custom CA certificate

Use operating system CA certificate

Do not verify certificate

```
-----BEGIN CERTIFICATE-----
abcdefghijklmnop123456780ABCDEFGHIJKL
123456/7890ABCDEFabcdefghijklmnopLABCD
-----END CERTIFICATE-----
```

Previous
Test and create endpoint

Typ der Zertifikatverifizierung	Beschreibung
Benutzerdefiniertes CA-Zertifikat verwenden	Verwenden Sie ein benutzerdefiniertes Sicherheitszertifikat. Wenn Sie diese Einstellung auswählen, kopieren Sie das benutzerdefinierte Sicherheitszertifikat in das Textfeld CA-Zertifikat .
Verwenden Sie das CA-Zertifikat für das Betriebssystem	Verwenden Sie das auf dem Betriebssystem installierte Standard-CA-Zertifikat, um Verbindungen zu sichern.
Verifizieren Sie das Zertifikat nicht	Das für die TLS-Verbindung verwendete Zertifikat wird nicht verifiziert. Diese Option ist nicht sicher.

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

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



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

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

Verwandte Informationen

["Festlegen des URN für einen Endpunkt der Plattformdienste"](#)

["CloudMirror-Replizierung wird konfiguriert"](#)

["Ereignisbenachrichtigungen werden konfiguriert"](#)

["Konfigurieren des Suchintegrationsservice"](#)

Testen der Verbindung für einen Endpunkt der Plattformservices

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

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Tenant Manager angemeldet sein.
- Sie müssen einer Benutzergruppe angehören, die über die Berechtigung Endpunkte verwalten verfügt.

Über diese Aufgabe

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

Schritte

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

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

Platform services endpoints

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

4 endpoints [Create endpoint](#)


[Delete endpoint](#)

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

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

Die Seite mit den Details des Endpunkts wird angezeigt.

Overview ^

Display name:	my-endpoint-1 
Type:	S3 Bucket
URI:	http://10.96.104.167:10443
URN:	urn:sgws:s3:::bucket1

ConnectionConfiguration

Verify connection

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

Test connection

3. Wählen Sie **Verbindung testen**.

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

Bearbeiten eines Endpunkts für Plattformservices

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

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Tenant Manager angemeldet sein.
- Sie müssen einer Benutzergruppe angehören, die über die Berechtigung Endpunkte verwalten verfügt.

Schritte

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

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







Platform services endpoints

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

4 endpoints

Create endpoint

Delete endpoint

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

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

Die Seite mit den Details des Endpunkts wird angezeigt.

3. Wählen Sie **Konfiguration**.

Overview

Display name: **my-endpoint-3** 

Type: **Notifications**

URI: **http://10.96.104.202:8080/**

URN: **arn:aws:sns:us-west-2::example1**

Connection

Configuration

Edit configuration

Endpoint details

URI 

http://10.96.104.202:8080/

URN 

arn:aws:sns:us-west-2::example1

Authentication type

Basic HTTP 

Username 

testme

Password 

••••••••

Edit password

Verify server

- Use custom CA certificate
- Use operating system CA certificate
- Do not verify certificate


```
-----BEGIN CERTIFICATE-----  
abcdefghijklmnop123456780ABCDEFGHIJKL  
123456/7890ABCDEFabcdefghijklmnop1ABCD  
-----END CERTIFICATE-----
```

Test and save changes

4. Ändern Sie bei Bedarf die Konfiguration des Endpunkts.



Sie können den URN eines Endpunktes nicht ändern, nachdem der Endpunkt erstellt wurde.

- a. Um den Anzeigenamen für den Endpunkt zu ändern, wählen Sie das Bearbeiten-Symbol .
- b. Ändern Sie bei Bedarf den URI.
- c. Ändern Sie bei Bedarf den Authentifizierungstyp.
 - Ändern Sie für die grundlegende HTTP-Authentifizierung den Benutzernamen nach Bedarf. Ändern Sie das Passwort nach Bedarf, indem Sie **Passwort bearbeiten** und das neue Passwort eingeben. Wenn Sie Ihre Änderungen abbrechen müssen, wählen Sie **Passwort zurücksetzen Bearbeiten**.
 - Zur Authentifizierung des Zugriffsschlüssels ändern Sie den Schlüssel ggf. durch Auswahl von **S3-Schlüssel bearbeiten** und Einfügen einer neuen Zugriffsschlüssel-ID und eines geheimen Zugriffsschlüssels. Wenn Sie Ihre Änderungen abbrechen müssen, wählen Sie **S3-Taste Edit** rückgängig machen.
- d. Ändern Sie bei Bedarf die Methode zur Überprüfung des Servers.

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

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

Verwandte Informationen

["Erstellen eines Endpunkts für Plattformservices"](#)

Löschen eines Endpunkts für Plattformservices

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

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Tenant Manager angemeldet sein.
- Sie müssen einer Benutzergruppe angehören, die die Berechtigung **Endpunkte verwalten** besitzt.

Schritte

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

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

Platform services endpoints

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

4 endpoints

Create endpoint

Delete endpoint

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

2. Aktivieren Sie das Kontrollkästchen für jeden zu löschenden Endpunkt.



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

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

Eine Bestätigungsmeldung wird angezeigt.

Delete endpoint

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

This might take a few minutes.

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

Cancel Delete endpoint


4. Wählen Sie **Endpunkt löschen**.

Fehlerbehebung bei Endpoint-Fehlern bei Plattform-Services

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


Ermitteln, ob ein Fehler aufgetreten ist

Wenn in den letzten 7 Tagen Endpoint-Fehler bei Plattformservices aufgetreten sind, zeigt das Tenant Manager Dashboard eine Warnmeldung an. Auf der Seite Plattform-Services-Endpunkte finden Sie weitere Details zum Fehler.


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

Der gleiche Fehler, der auf dem Dashboard angezeigt wird, wird ebenfalls oben auf der Seite „Plattform-Services-Endpunkte“ angezeigt. So zeigen Sie eine detailliertere Fehlermeldung an:

Schritte

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

Overview ^

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

Connection


Configuration

Verify connection

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

Test connection

Last error details

 2 hours ago

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

Überprüfen, ob ein Fehler noch aktuell ist

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

Schritte

1. Wählen Sie den Endpunkt aus.

Die Seite mit den Details des Endpunkts wird angezeigt.

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

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

Beseitigung von Endpunktfehlern

Sie können die Meldung **Letzter Fehler** auf der Seite Details zum Endpunkt verwenden, um zu ermitteln, was den Fehler verursacht. Bei einigen Fehlern müssen Sie möglicherweise den Endpunkt bearbeiten, um das

92

Problem zu lösen. Beispielsweise kann ein CloudMirroring-Fehler auftreten, wenn StorageGRID nicht auf den Ziel-S3-Bucket zugreifen kann, da er nicht über die richtigen Zugriffsberechtigungen verfügt oder der Zugriffsschlüssel abgelaufen ist. Die Meldung lautet „entweder die Anmeldeinformationen des Endpunkts oder der Zielzugriff muss aktualisiert werden,“ und die Details lauten „AccessDenied“ oder „InvalidAccessKeyId“.

Wenn Sie den Endpunkt bearbeiten müssen, um einen Fehler zu beheben: Durch die Auswahl von **Änderungen testen und speichern** wird StorageGRID den aktualisierten Endpunkt validieren und bestätigen, dass er mit den aktuellen Anmeldeinformationen erreicht werden kann. Die Verbindung zum Endpunkt wird von einem Node an jedem Standort validiert.

Schritte

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

Endpoint-Anmeldeinformationen mit unzureichenden Berechtigungen

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

Zusätzliche Plattform-Services Fehlerbehebung

Weitere Informationen zur Fehlerbehebung bei Plattform-Services finden Sie in den Anweisungen für die Administration von StorageGRID.

["StorageGRID verwalten"](#)

Verwandte Informationen

["Erstellen eines Endpunkts für Plattformservices"](#)

["Testen der Verbindung für einen Endpunkt der Plattformservices"](#)

["Bearbeiten eines Endpunkts für Plattformservices"](#)

CloudMirror-Replizierung wird konfiguriert

Der CloudMirror Replikationsservice ist einer der drei StorageGRID Plattform-Services. Mithilfe der CloudMirror Replizierung können Sie Objekte automatisch in einen externen S3-Bucket replizieren.

Was Sie benötigen

- Plattform-Services müssen von einem StorageGRID-Administrator für Ihr Mandantenkonto aktiviert werden.
- Sie müssen bereits einen Bucket erstellt haben, um als Replikationsquelle zu fungieren.
- Der Endpunkt, den Sie als Ziel für die CloudMirror-Replikation verwenden möchten, muss bereits

vorhanden sein, und Sie müssen über seinen URN verfügen.

- Sie müssen zu einer Benutzergruppe gehören, die über die Berechtigung Alle Buckets verwalten oder Stammzugriff verfügt, sodass Sie die Einstellungen für alle S3-Buckets in Ihrem Mandantenkonto verwalten können. Diese Berechtigungen überschreiben die Berechtigungseinstellungen in Gruppen- oder Bucket-Richtlinien bei der Konfiguration des Buckets mithilfe des Mandanten-Manager.

Über diese Aufgabe

Die CloudMirror Replizierung kopiert Objekte von einem Quell-Bucket zu einem Ziel-Bucket, der in einem Endpunkt angegeben wird. Um die CloudMirror-Replikation für einen Bucket zu aktivieren, müssen Sie eine gültige Bucket-Replizierungskonfiguration-XML erstellen und anwenden. Die XML-Replikationskonfiguration muss den URN eines S3-Bucket-Endpunkts für jedes Ziel verwenden.



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

Allgemeine Informationen zur Bucket-Replizierung und deren Konfiguration finden Sie in der Amazon-Dokumentation zur regionsübergreifenden Replizierung (CRR). Informationen dazu, wie StorageGRID die S3-Bucket-Replizierungskonfigurations-API implementiert, finden Sie in den Anweisungen zur Implementierung von S3-Client-Applikationen.

Wenn Sie die CloudMirror-Replizierung auf einem Bucket aktivieren, der Objekte enthält, werden neue, dem Bucket hinzugefügte Objekte repliziert, die vorhandenen Objekte jedoch nicht im Bucket. Sie müssen vorhandene Objekte aktualisieren, um die Replikation auszulösen.

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

Schritte

1. Replizierung für Ihren Quell-Bucket aktivieren:

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

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


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

2. Wählen Sie im Mandantenmanager **STORAGE (S3) > Buckets** aus.
3. Wählen Sie den Namen des Quell-Buckets aus.

Die Seite mit den Bucket-Details wird angezeigt.

4. Wählen Sie **Plattform-Services > Replikation**.
5. Aktivieren Sie das Kontrollkästchen * Replikation aktivieren*.
6. Fügen Sie die XML-Replikationskonfiguration in das Textfeld ein und wählen Sie **Änderungen speichern**.

Bucket options
Bucket access
Platform services

Replication
Disabled
^

Enable the CloudMirror replication service to copy objects from a source bucket to a destination bucket that is specified in an endpoint.

- Platform services must be enabled for your tenant account by a StorageGRID administrator.
- You must have already configured an endpoint for each destination bucket.
- You must specify the URN of each endpoint in the replication configuration XML for the source bucket.

Enable replication

Clear

```

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

```

Save changes



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

7. Überprüfen Sie, ob die Replikation ordnungsgemäß konfiguriert ist:
 - a. Fügen Sie dem Quell-Bucket ein Objekt hinzu, das die in der Replizierungskonfiguration angegebenen Anforderungen für die Replizierung erfüllt.

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

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

Bei kleinen Objekten wird die Replizierung schnell durchgeführt.

Verwandte Informationen

["Allgemeines zum CloudMirror Replikationsservice"](#)

["S3 verwenden"](#)

["Erstellen eines Endpunkts für Plattformservices"](#)

Ereignisbenachrichtigungen werden konfiguriert

Der Benachrichtigungsservice ist einer der drei StorageGRID-Plattdienste. Sie können Benachrichtigungen aktivieren, damit ein Bucket Informationen zu bestimmten Ereignissen an einen Zieldienst sendet, der den AWS Simple Notification Service™ (SNS) unterstützt.

Was Sie benötigen

- Plattform-Services müssen von einem StorageGRID-Administrator für Ihr Mandantenkonto aktiviert werden.
- Sie müssen bereits einen Bucket erstellt haben, um als Quelle für Benachrichtigungen zu fungieren.
- Der Endpunkt, den Sie als Ziel für Ereignisbenachrichtigungen verwenden möchten, muss bereits vorhanden sein, und Sie müssen über seinen URN verfügen.
- Sie müssen zu einer Benutzergruppe gehören, die über die Berechtigung Alle Buckets verwalten oder Stammzugriff verfügt, sodass Sie die Einstellungen für alle S3-Buckets in Ihrem Mandantenkonto verwalten können. Diese Berechtigungen überschreiben die Berechtigungseinstellungen in Gruppen- oder Bucket-Richtlinien bei der Konfiguration des Buckets mithilfe des Mandanten-Managers.

Über diese Aufgabe

Nachdem Sie Ereignisbenachrichtigungen konfiguriert haben, wird eine Benachrichtigung generiert und an das Thema Simple Notification Service (SNS) gesendet, das als Zielendpunkt verwendet wird, sobald ein bestimmtes Ereignis für ein Objekt im Quell-Bucket eintritt. Um Benachrichtigungen für einen Bucket zu aktivieren, müssen Sie eine gültige XML-Benachrichtigungskonfiguration erstellen und anwenden. Die XML-ID für die Benachrichtigungskonfiguration muss den URN eines Endpunkt für Ereignisbenachrichtigungen für jedes Ziel verwenden.

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

Wenn Sie Ereignisbenachrichtigungen für einen Bucket aktivieren, der Objekte enthält, werden Benachrichtigungen nur für Aktionen gesendet, die nach dem Speichern der Benachrichtigungskonfiguration ausgeführt werden.

Schritte

1. Benachrichtigungen für Ihren Quell-Bucket aktivieren:
 - Verwenden Sie einen Texteditor, um die XML-Benachrichtigungskonfiguration zu erstellen, die für die Aktivierung von Ereignisbenachrichtigungen erforderlich ist, wie in der S3-Benachrichtigungs-API angegeben.
 - Verwenden Sie bei der XML-Konfiguration den URN eines Endpunkt für Ereignisbenachrichtigungen

als Zielthema.

```
<NotificationConfiguration>
  <TopicConfiguration>
    <Id>Image-created</Id>
    <Filter>
      <S3Key>
        <FilterRule>
          <Name>prefix</Name>
          <Value>images/</Value>
        </FilterRule>
      </S3Key>
    </Filter>
    <Topic>arn:aws:sns:us-east-1:050340950352:sgws-topic</Topic>
    <Event>s3:ObjectCreated:*</Event>
  </TopicConfiguration>
</NotificationConfiguration>
```

2. Wählen Sie im Mandantenmanager **STORAGE (S3) > Buckets** aus.
3. Wählen Sie den Namen des Quell-Buckets aus.

Die Seite mit den Bucket-Details wird angezeigt.

4. Wählen Sie **Plattform-Services > Ereignisbenachrichtigungen** aus.
5. Aktivieren Sie das Kontrollkästchen **Ereignisbenachrichtigungen aktivieren**.
6. Fügen Sie die XML-Benachrichtigungskonfiguration in das Textfeld ein und wählen Sie **Änderungen speichern**.

Bucket options
Bucket access
Platform services

Replication
Disabled
▼

Event notifications
Disabled
▲

Enable the event notification service for an S3 bucket if you want StorageGRID to send notifications about specified events to a destination Amazon Simple Notification Service (SNS).

- Platform services must be enabled for your tenant account by a StorageGRID administrator.
- You must have already configured an endpoint for the destination of event notifications.
- You must specify the URN of that endpoint in the notification configuration XML for the source bucket.

Enable event notifications

```

<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>
    
```



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

7. Überprüfen Sie, ob Ereignisbenachrichtigungen richtig konfiguriert sind:

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

In diesem Beispiel wird eine Ereignisbenachrichtigung gesendet, sobald ein Objekt mit dem erstellt wird `images/` Präfix.

- b. Bestätigen Sie, dass eine Benachrichtigung an das Ziel-SNS-Thema gesendet wurde.

Wenn beispielsweise Ihr Zielthema im AWS Simple Notification Service (SNS) gehostet wird, können Sie den Service so konfigurieren, dass Sie eine E-Mail senden, wenn die Benachrichtigung zugestellt wird.

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

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

Verwandte Informationen

["Allgemeines zu Benachrichtigungen für Buckets"](#)

["S3 verwenden"](#)

["Erstellen eines Endpunkts für Plattformservices"](#)

Verwenden des Suchintegrationsdienstes

Der Suchintegrations-Service ist einer der drei StorageGRID Plattform-Services. Sie können diesen Service aktivieren, wenn ein Objekt erstellt, gelöscht oder seine Metadaten oder Tags aktualisiert wird, Objektmetadaten an einen Zielsuchindex zu senden.

Sie können die Suchintegration mit dem Mandanten-Manager konfigurieren, um eine benutzerdefinierte StorageGRID-Konfigurations-XML auf einen Bucket anzuwenden.



Da der Suchintegrationsdienst dazu führt, dass Objektmetadaten an ein Ziel gesendet werden, wird seine Konfigurations-XML als *Metadaten Notification Configuration XML* bezeichnet. Diese Konfigurations-XML unterscheidet sich von der XML-Konfiguration *notification*, die zur Aktivierung von Ereignisbenachrichtigungen verwendet wird.

Anweisungen zur Implementierung von S3-Client-Applikationen finden Sie in der Anleitung zu den folgenden benutzerdefinierten StorageGRID S3-REST-API-Vorgängen:

- Konfigurationsanforderung für Bucket-Metadaten-Benachrichtigungen LÖSCHEN
- Konfigurationsanforderung FÜR Bucket-Metadaten-Benachrichtigungen ABRUFEN
- PUT Anforderung der Bucket-Metadaten-Benachrichtigung

Verwandte Informationen

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

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

["Vom Suchintegrations-Service generierter JSON"](#)

["Konfigurieren des Suchintegrationservice"](#)

["S3 verwenden"](#)

Konfigurations-XML für die Integration der Suche

Der Such-Integrationservice wird anhand einer Reihe von Regeln konfiguriert, die in enthalten sind `<MetadataNotificationConfiguration>` Und `</MetadataNotificationConfiguration>` tags: Jede Regel gibt die Objekte an, auf die sich die Regel bezieht, und das Ziel, an dem StorageGRID die Metadaten dieser Objekte senden sollte.

Objekte können nach dem Präfix des Objektnamens gefiltert werden. Beispielsweise können Sie Metadaten für Objekte mit dem Präfix `/images` an ein Ziel und die Metadaten für Objekte mit dem Präfix `/videos` nach anderen. Konfigurationen mit sich überschneidenden Präfixen sind ungültig und werden beim Einreichen abgelehnt. Beispiel: Eine Konfiguration, die eine Regel für Objekte mit dem Präfix `test` und eine zweite Regel für Objekte mit dem Präfix `test2` ist nicht zulässig.

Ziele müssen mit dem URN eines StorageGRID-Endpunkts angegeben werden, der für den Suchintegrationsdienst erstellt wurde. Diese Endpunkte beziehen sich auf einen Index und einen Typ, der in einem Elasticsearch-Cluster definiert ist.

```
<MetadataNotificationConfiguration>
  <Rule>
    <ID>Rule-1</ID>
    <Status>rule-status</Status>
    <Prefix>key-prefix</Prefix>
    <Destination>
      <Urn>arn:aws:es:region:account-
ID:domain/mydomain/myindex/mytype</Urn>
    </Destination>
  </Rule>
  <Rule>
    <ID>Rule-2</ID>
    ...
  </Rule>
  ...
</MetadataNotificationConfiguration>
```

In der Tabelle werden die Elemente in der XML-Konfiguration für die Metadatenbenachrichtigung beschrieben.

Name	Beschreibung	Erforderlich
MetadataNotificationKonfiguration	Container-Tag für Regeln zur Angabe von Objekten und Zielen für Metadatenbenachrichtigungen Enthält mindestens ein Regelement.	Ja.
Regel	Container-Tag für eine Regel, die die Objekte identifiziert, deren Metadaten zu einem bestimmten Index hinzugefügt werden sollen. Regeln mit überlappenden Präfixen werden abgelehnt. Im MetadataNotificationConfiguration Element enthalten.	Ja.

Name	Beschreibung	Erforderlich
ID	<p>Eindeutige Kennung für die Regel.</p> <p>In das Element Regel aufgenommen.</p>	Nein
Status	<p>Der Status kann „aktiviert“ oder „deaktiviert“ sein. Für deaktivierte Regeln wird keine Aktion durchgeführt.</p> <p>In das Element Regel aufgenommen.</p>	Ja.
Präfix	<p>Objekte, die mit dem Präfix übereinstimmen, werden von der Regel beeinflusst und ihre Metadaten werden an das angegebene Ziel gesendet.</p> <p>Geben Sie ein leeres Präfix an, um alle Objekte zu entsprechen.</p> <p>In das Element Regel aufgenommen.</p>	Ja.
Ziel	<p>Container-Tag für das Ziel einer Regel.</p> <p>In das Element Regel aufgenommen.</p>	Ja.
Urne	<p>URNE des Ziels, an dem Objektmetadaten gesendet werden. Muss der URN eines StorageGRID-Endpunkts mit den folgenden Eigenschaften sein:</p> <ul style="list-style-type: none"> • es Muss das dritte Element sein. • Der URN muss mit dem Index und dem Typ enden, in dem die Metadaten gespeichert werden, im Formular <code>domain-name/myindex/mytype</code>. <p>Endpunkte werden mithilfe der Mandanten-Manager oder der Mandanten-Management-API konfiguriert. Sie nehmen folgende Form:</p> <ul style="list-style-type: none"> • <code>arn:aws:es:region:account-ID:domain/mydomain/myindex/mytype</code> • <code>urn:mysite:es:::mydomain/myindex/mytype</code> <p>Der Endpunkt muss konfiguriert werden, bevor die Konfigurations-XML gesendet wird, oder die Konfiguration schlägt mit einem Fehler 404 fehl.</p> <p>Urne ist im Element Ziel enthalten.</p>	Ja.

Verwenden Sie die XML-XML-Beispielkonfiguration für Metadatenbenachrichtigungen, um zu erfahren, wie Sie Ihre eigene XML erstellen.

Konfiguration der Metadatenbenachrichtigung für alle Objekte

In diesem Beispiel werden die Objektmetadaten für alle Objekte an dasselbe Ziel gesendet.

```
<MetadataNotificationConfiguration>
  <Rule>
    <ID>Rule-1</ID>
    <Status>Enabled</Status>
    <Prefix></Prefix>
    <Destination>
      <Urn>urn:myes:es:::sgws-notifications/test1/all</Urn>
    </Destination>
  </Rule>
</MetadataNotificationConfiguration>
```

Konfiguration der Metadatenbenachrichtigung mit zwei Regeln

In diesem Beispiel sind die Objektmetadaten für Objekte mit dem Präfix übereinstimmen `/images` An ein Ziel gesendet wird, während die Objektmetadaten für Objekte mit dem Präfix übereinstimmen `/videos` Wird an ein zweites Ziel gesendet.

```
<MetadataNotificationConfiguration>
  <Rule>
    <ID>Images-rule</ID>
    <Status>Enabled</Status>
    <Prefix>/images</Prefix>
    <Destination>
      <Urn>arn:aws:es:us-east-1:33333333:domain/es-
domain/graphics/imagetype</Urn>
    </Destination>
  </Rule>
  <Rule>
    <ID>Videos-rule</ID>
    <Status>Enabled</Status>
    <Prefix>/videos</Prefix>
    <Destination>
      <Urn>arn:aws:es:us-west-1:22222222:domain/es-
domain/graphics/videotype</Urn>
    </Destination>
  </Rule>
</MetadataNotificationConfiguration>
```

Verwandte Informationen

["S3 verwenden"](#)

["Vom Suchintegrations-Service generierter JSON"](#)

Konfigurieren des Suchintegrationservice

Der Suchintegrations-Service sendet Objektmetadaten an einen Zielindex bei jedem Erstellen, Löschen oder Aktualisieren der zugehörigen Metadaten oder Tags.

Was Sie benötigen

- Plattform-Services müssen von einem StorageGRID-Administrator für Ihr Mandantenkonto aktiviert werden.
- Sie müssen bereits einen S3-Bucket erstellt haben, dessen Inhalt Sie indexieren möchten.
- Der Endpunkt, den Sie als Ziel für den Suchintegrationsdienst verwenden möchten, muss bereits vorhanden sein, und Sie müssen seinen URN haben.
- Sie müssen zu einer Benutzergruppe gehören, die über die Berechtigung Alle Buckets verwalten oder Stammzugriff verfügt, sodass Sie die Einstellungen für alle S3-Buckets in Ihrem Mandantenkonto verwalten können. Diese Berechtigungen überschreiben die Berechtigungseinstellungen in Gruppen- oder Bucket-Richtlinien bei der Konfiguration des Buckets mithilfe des Mandanten-Manager.

Über diese Aufgabe

Nachdem Sie den Such-Integrationservice für einen Quell-Bucket konfiguriert haben, werden beim Erstellen eines Objekts oder beim Aktualisieren der Metadaten oder Tags eines Objekts Objektmetadaten ausgelöst, die an den Ziel-Endpunkt gesendet werden. Wenn Sie den Such-Integrationservice für einen Bucket aktivieren, der bereits Objekte enthält, werden Metadatenbenachrichtigungen nicht automatisch für vorhandene Objekte gesendet. Sie müssen diese vorhandenen Objekte aktualisieren, um sicherzustellen, dass ihre Metadaten dem Zielsuchindex hinzugefügt werden.

Schritte

1. Verwenden Sie einen Texteditor, um die XML-Metadatenbenachrichtigung zu erstellen, die für die Integration der Suche erforderlich ist.
 - Informationen zur Integration der Suchfunktion finden Sie in den XML-Konfigurationsdaten.
 - Verwenden Sie beim Konfigurieren des XML den URN eines Endpunkt zur Integration der Suche als Ziel.

```
<MetadataNotificationConfiguration>
  <Rule>
    <Status>Enabled</Status>
    <Prefix></Prefix>
    <Destination>
      <Urn>arn:aws:es:us-east-
1:1111111111111111:domain/mydomain/myindex/mytype</Urn>
    </Destination>
  </Rule>
</MetadataNotificationConfiguration>
```

2. Wählen Sie im Mandantenmanager **STORAGE (S3) > Buckets** aus.
3. Wählen Sie den Namen des Quell-Buckets aus.

Die Seite mit den Bucket-Details wird angezeigt.

4. Wählen Sie **Plattform-Services > Integration suchen**
5. Aktivieren Sie das Kontrollkästchen **Suchintegration aktivieren**.
6. Fügen Sie die Konfiguration der Metadatenbenachrichtigung in das Textfeld ein, und wählen Sie **Änderungen speichern**.

Bucket options **Bucket access** **Platform services**

Replication Disabled

Event notifications Disabled

Search integration Disabled

Enable the search integration service to send object metadata to a destination search index whenever an object is created, deleted, or its metadata or tags are updated.

- Platform services must be enabled for your tenant account by a StorageGRID administrator.
- You must have already configured an endpoint for the search integration service.
- You must specify the URN of that endpoint in the search integration configuration XML for the bucket you want to index.

Enable search integration

Clear

```
<MetadataNotificationConfiguration>
  <Rule>
    <Status>Enabled</Status>
    <Prefix></Prefix>
    <Destination>
      <Urn>arn:aws:es:us-east-1:111111111111:domain/mydomain/myindex/mytype</Urn>
    </Destination>
  </Rule>
</MetadataNotificationConfiguration>
```

Save changes



Platformservices müssen für jedes Mandantenkonto von einem StorageGRID-Administrator aktiviert werden, der den Grid Manager oder die Management-API verwendet. Wenden Sie sich an Ihren StorageGRID-Administrator, wenn beim Speichern der Konfigurations-XML ein Fehler auftritt.

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

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

In dem zuvor gezeigten Beispiel lösen alle Objekte, die dem Bucket hinzugefügt wurden, eine Metadatenbenachrichtigung aus.

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

Nachdem Sie fertig sind

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

- Wählen Sie **STORAGE (S3) > Buckets** aus, und deaktivieren Sie das Kontrollkästchen **Suchintegration aktivieren**.
- Wenn Sie die S3-API direkt verwenden, verwenden Sie eine Benachrichtigungsanforderung FÜR DELETE-Bucket-Metadaten. Anweisungen zur Implementierung von S3-Client-Applikationen finden Sie in der Anleitung.

Verwandte Informationen

["Beschreibung des Suchintegrationservice"](#)

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

["S3 verwenden"](#)

["Erstellen eines Endpunkts für Plattformservices"](#)

Vom Suchintegrations-Service generierter JSON

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

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

```

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

```

Objektmetadaten sind in Metadaten-Benachrichtigungen enthalten

In der Tabelle sind alle Felder aufgeführt, die im JSON-Dokument enthalten sind, die beim Aktivierung der Suchintegration an den Zielendpunkt gesendet werden.

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

Typ	Elementname und -Beschreibung
Bucket- und Objektinformationen	bucket: Name des Eimers
key: Objektschlüsselname	versionID: Objektversion, für Objekte in versionierten Buckets
region: Eimer-Region, zum Beispiel us-east-1	System-Metadaten
size: Objektgröße (in Bytes) als sichtbar für einen HTTP-Client	md5: Objekt-Hash
Benutzer-Metadaten	metadata: Alle Benutzer-Metadaten für das Objekt, als Schlüssel-Wert-Paare key:value
Tags	tags: Alle für das Objekt definierten Objekttags, als Schlüsselwert-Paare key:value



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

Copyright-Informationen

Copyright © 2024 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtinhabers in keiner Form und durch keine Mittel – weder grafische noch elektronische oder mechanische, einschließlich Fotokopieren, Aufnehmen oder Speichern in einem elektronischen Abrufsystem – auch nicht in Teilen, vervielfältigt werden.

Software, die von urheberrechtlich geschütztem NetApp Material abgeleitet wird, unterliegt der folgenden Lizenz und dem folgenden Haftungsausschluss:

DIE VORLIEGENDE SOFTWARE WIRD IN DER VORLIEGENDEN FORM VON NETAPP ZUR VERFÜGUNG GESTELLT, D. H. OHNE JEGLICHE EXPLIZITE ODER IMPLIZITE GEWÄHRLEISTUNG, EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE STILLSCHWEIGENDE GEWÄHRLEISTUNG DER MARKTGÄNGIGKEIT UND EIGNUNG FÜR EINEN BESTIMMTEN ZWECK, DIE HIERMIT AUSGESCHLOSSEN WERDEN. NETAPP ÜBERNIMMT KEINERLEI HAFTUNG FÜR DIREKTE, INDIREKTE, ZUFÄLLIGE, BESONDERE, BEISPIELHAFT SCHÄDEN ODER FOLGESCHÄDEN (EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE BESCHAFFUNG VON ERSATZWAREN ODER -DIENSTLEISTUNGEN, NUTZUNGS-, DATEN- ODER GEWINNVERLUSTE ODER UNTERBRECHUNG DES GESCHÄFTSBETRIEBS), UNABHÄNGIG DAVON, WIE SIE VERURSACHT WURDEN UND AUF WELCHER HAFTUNGSTHEORIE SIE BERUHEN, OB AUS VERTRAGLICH FESTGELEGTER HAFTUNG, VERSCHULDENSUNABHÄNGIGER HAFTUNG ODER DELIKTSHAFTUNG (EINSCHLIESSLICH FAHRLÄSSIGKEIT ODER AUF ANDEREM WEGE), DIE IN IRGEND EINER WEISE AUS DER NUTZUNG DIESER SOFTWARE RESULTIEREN, SELBST WENN AUF DIE MÖGLICHKEIT DERARTIGER SCHÄDEN HINGEWIESEN WURDE.

NetApp behält sich das Recht vor, die hierin beschriebenen Produkte jederzeit und ohne Vorankündigung zu ändern. NetApp übernimmt keine Verantwortung oder Haftung, die sich aus der Verwendung der hier beschriebenen Produkte ergibt, es sei denn, NetApp hat dem ausdrücklich in schriftlicher Form zugestimmt. Die Verwendung oder der Erwerb dieses Produkts stellt keine Lizenzierung im Rahmen eines Patentrechts, Markenrechts oder eines anderen Rechts an geistigem Eigentum von NetApp dar.

Das in diesem Dokument beschriebene Produkt kann durch ein oder mehrere US-amerikanische Patente, ausländische Patente oder anhängige Patentanmeldungen geschützt sein.

ERLÄUTERUNG ZU „RESTRICTED RIGHTS“: Nutzung, Vervielfältigung oder Offenlegung durch die US-Regierung unterliegt den Einschränkungen gemäß Unterabschnitt (b)(3) der Klausel „Rights in Technical Data – Noncommercial Items“ in DFARS 252.227-7013 (Februar 2014) und FAR 52.227-19 (Dezember 2007).

Die hierin enthaltenen Daten beziehen sich auf ein kommerzielles Produkt und/oder einen kommerziellen Service (wie in FAR 2.101 definiert) und sind Eigentum von NetApp, Inc. Alle technischen Daten und die Computersoftware von NetApp, die unter diesem Vertrag bereitgestellt werden, sind gewerblicher Natur und wurden ausschließlich unter Verwendung privater Mittel entwickelt. Die US-Regierung besitzt eine nicht ausschließliche, nicht übertragbare, nicht unterlizenzierbare, weltweite, limitierte unwiderrufliche Lizenz zur Nutzung der Daten nur in Verbindung mit und zur Unterstützung des Vertrags der US-Regierung, unter dem die Daten bereitgestellt wurden. Sofern in den vorliegenden Bedingungen nicht anders angegeben, dürfen die Daten ohne vorherige schriftliche Genehmigung von NetApp, Inc. nicht verwendet, offengelegt, vervielfältigt, geändert, aufgeführt oder angezeigt werden. Die Lizenzrechte der US-Regierung für das US-Verteidigungsministerium sind auf die in DFARS-Klausel 252.227-7015(b) (Februar 2014) genannten Rechte beschränkt.

Markeninformationen

NETAPP, das NETAPP Logo und die unter <http://www.netapp.com/TM> aufgeführten Marken sind Marken von NetApp, Inc. Andere Firmen und Produktnamen können Marken der jeweiligen Eigentümer sein.