Verwenden Sie StorageGRID

StorageGRID

NetApp
October 03, 2025

Inhalt

Verwenden Sie StorageGRID

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

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 Domänennamen (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.

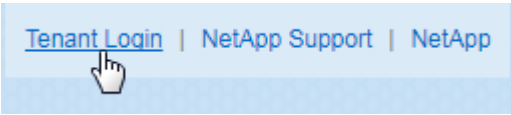
- Wenn die URL die 20-stellige Konto-ID des Mandanten nicht enthält, müssen Sie über diese Konto-ID verfügen.
- Sie müssen einen unterstützten Webbrowser verwenden.
- Cookies müssen in Ihrem Webbrowser aktiviert sein.
- Sie müssen über spezifische Zugriffsberechtigungen verfügen.

Schritte

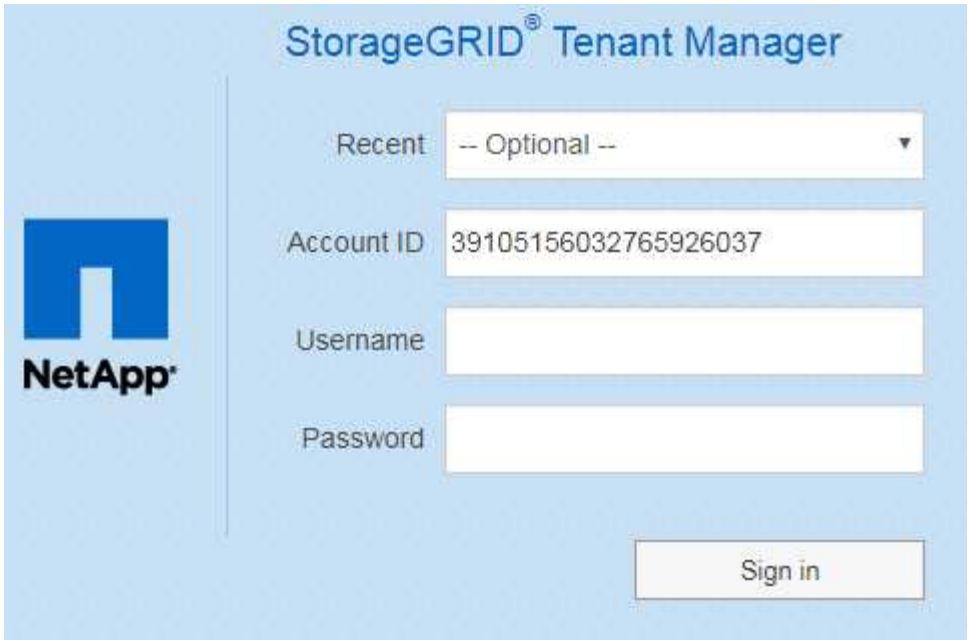
1. Starten Sie einen unterstützten Webbrowser.
2. Geben Sie in der Adressleiste des Browsers die URL für den Zugriff auf Tenant Manager ein.
3. Wenn Sie aufgefordert werden, eine Sicherheitswarnung zu erhalten, installieren Sie das Zertifikat mithilfe des Browser-Installationsassistenten.
4. Melden Sie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



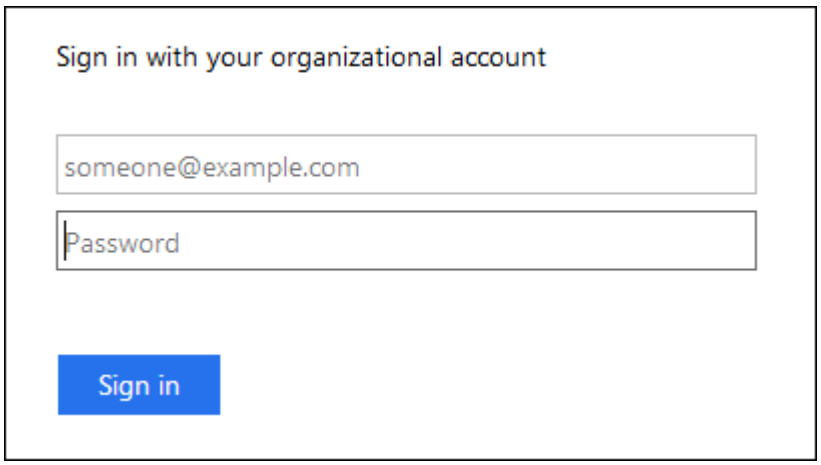
i. Wenn die 20-stellige Konto-ID des Mandanten nicht angezeigt wird, wählen Sie den Namen des Mandantenkontos aus, wenn er in der Liste der letzten Konten angezeigt wird, oder geben Sie die Konto-ID ein.

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:



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"

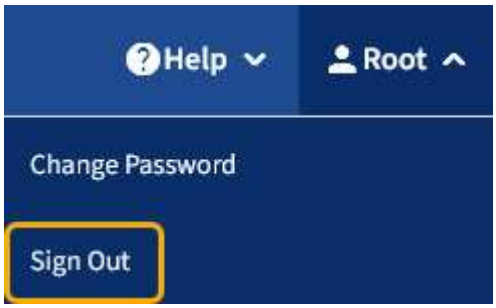
"Anforderungen an einen Webbrowser"

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	Sie sind vom Admin-Knoten abgemeldet. Die Anmeldeseite für den Mandanten-Manager wird angezeigt. **Hinweis:** Wenn Sie sich bei mehr als einem Admin-Knoten angemeldet haben, müssen Sie sich von jedem Knoten abmelden.

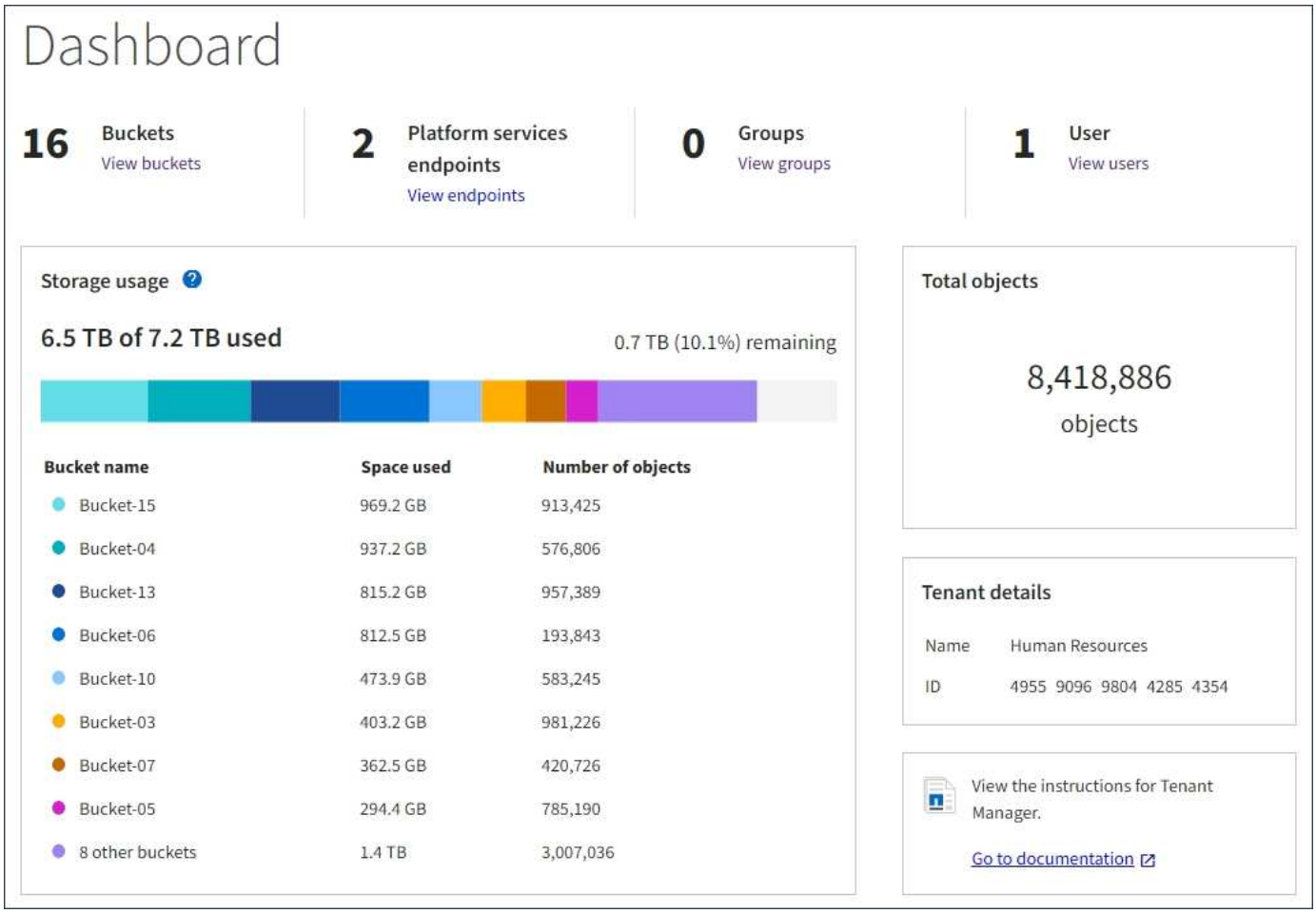
Option	Beschreibung
SSO aktiviert	Sie sind von allen Admin-Knoten abgemeldet, auf die Sie zugreifen konnten. Die Seite StorageGRID-Anmeldung wird angezeigt. Der Name des Mietkontos, auf das Sie gerade zugegriffen haben, wird als Standard im Dropdown-Menü **Letzte Konten** angegeben, und die **Konto-ID** des Mieters wird angezeigt. **Hinweis:** Wenn SSO aktiviert ist und Sie auch beim Grid Manager angemeldet sind, müssen Sie sich auch vom Grid Manager abmelden, um SSO abzumelden.

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.

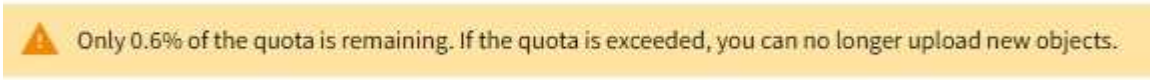
Bucket name	Space used	Number of objects
Bucket-02	944.7 GB	7,575
Bucket-09	899.6 GB	589,677
Bucket-15	889.6 GB	623,542
Bucket-06	846.4 GB	648,619
Bucket-07	730.8 GB	808,655
Bucket-04	700.8 GB	420,493
Bucket-11	663.5 GB	993,729
Bucket-03	656.9 GB	379,329
9 other buckets	2.3 TB	5,171,588

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.

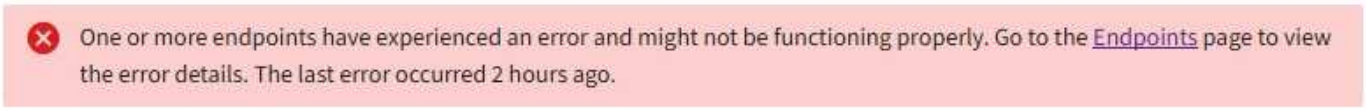


Wenn Sie Ihr Kontingent überschreiten, können Sie keine neuen Objekte hochladen.

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.



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	• 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
Swift	Festlegen der für Container verwendeten Konsistenzstufe

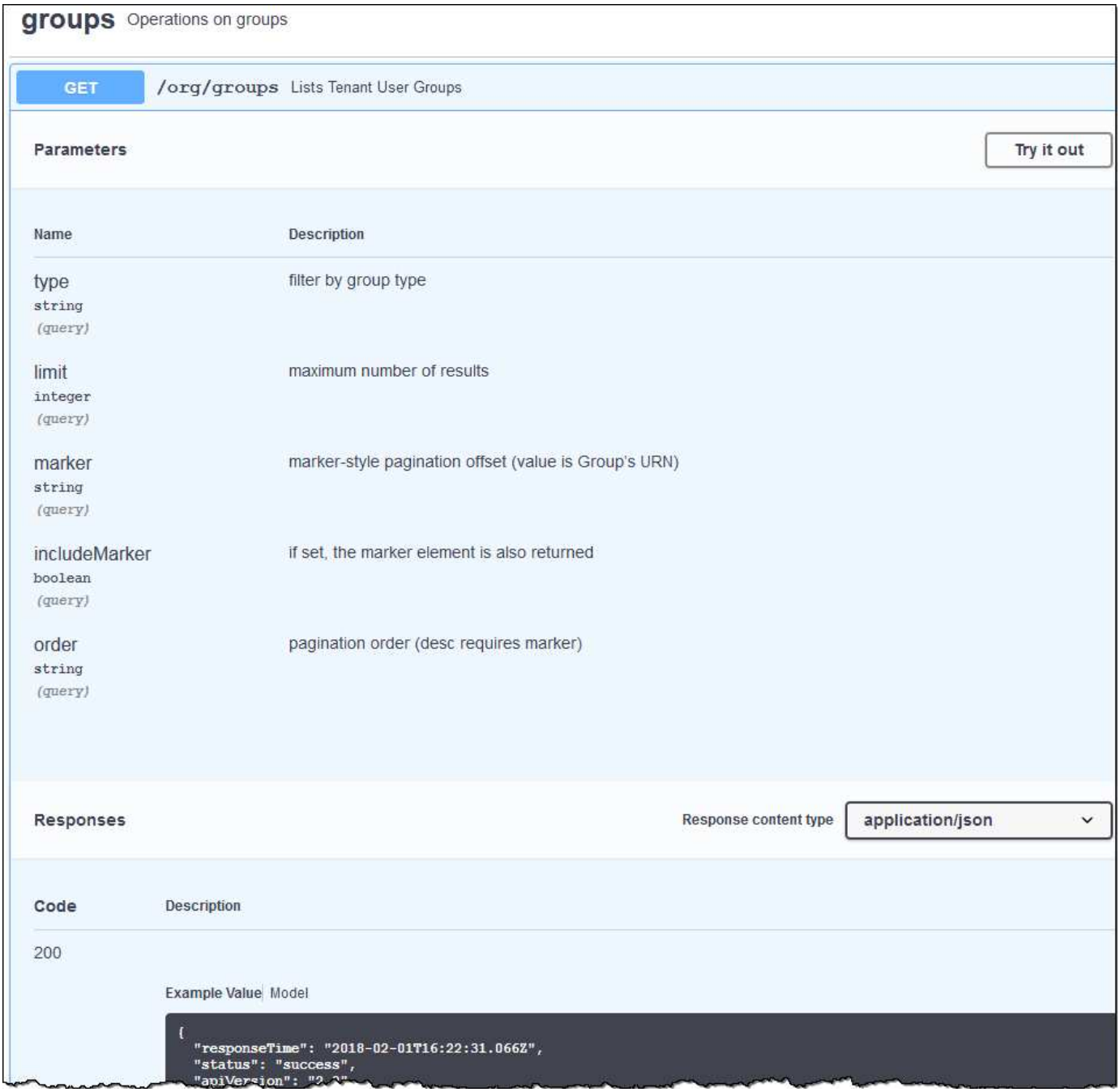
- **Deaktivierte Funktionen** — Funktionen zum Anzeigen von Funktionen, die möglicherweise deaktiviert

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.



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 angemelten Benutzers erstellt werden.

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

Um die Funktion zu aktivieren, 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

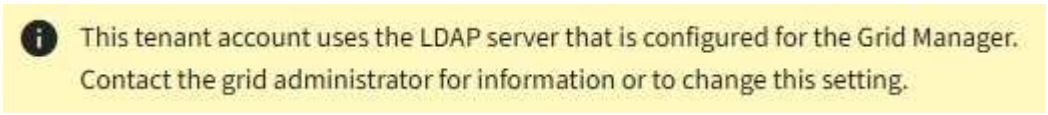
Sie können eine Identitätsföderation konfigurieren, wenn Mandantengruppen und Benutzer in einem anderen System wie Active Directory, OpenLDAP oder Oracle Directory Server verwaltet werden sollen.

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.



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	Bietet vollständigen Zugriff auf den Tenant Manager und die Mandanten-Management-API. **Hinweis:** Swift-Benutzer müssen Root Access-Berechtigung haben, um sich beim Mandantenkonto anzumelden.
Verwalter	Nur Swift Mandanten. Bietet vollständigen Zugriff auf die Swift Container und Objekte für dieses Mandantenkonto **Hinweis:** Swift-Benutzer müssen über die Swift-Administrator-Berechtigung verfügen, um alle Operationen mit der Swift REST-API auszuführen.
Management Ihrer eigenen S3 Credentials	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**.
Alle Buckets Verwalten	• 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. Benutzer, die diese Berechtigung nicht besitzen, sehen die Menüoption **Buckets** nicht. • Swift Mandanten: Ermöglicht Swift Benutzern die Kontrolle der Konsistenzstufe für Swift Container mithilfe der Mandanten-Management-API. **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.
Endpunkte Managen	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-Plattformservices verwendet werden. Benutzer, die diese Berechtigung nicht besitzen, sehen nicht die Menüoption **Platform Services Endpunkte**.

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**.

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.

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**.

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

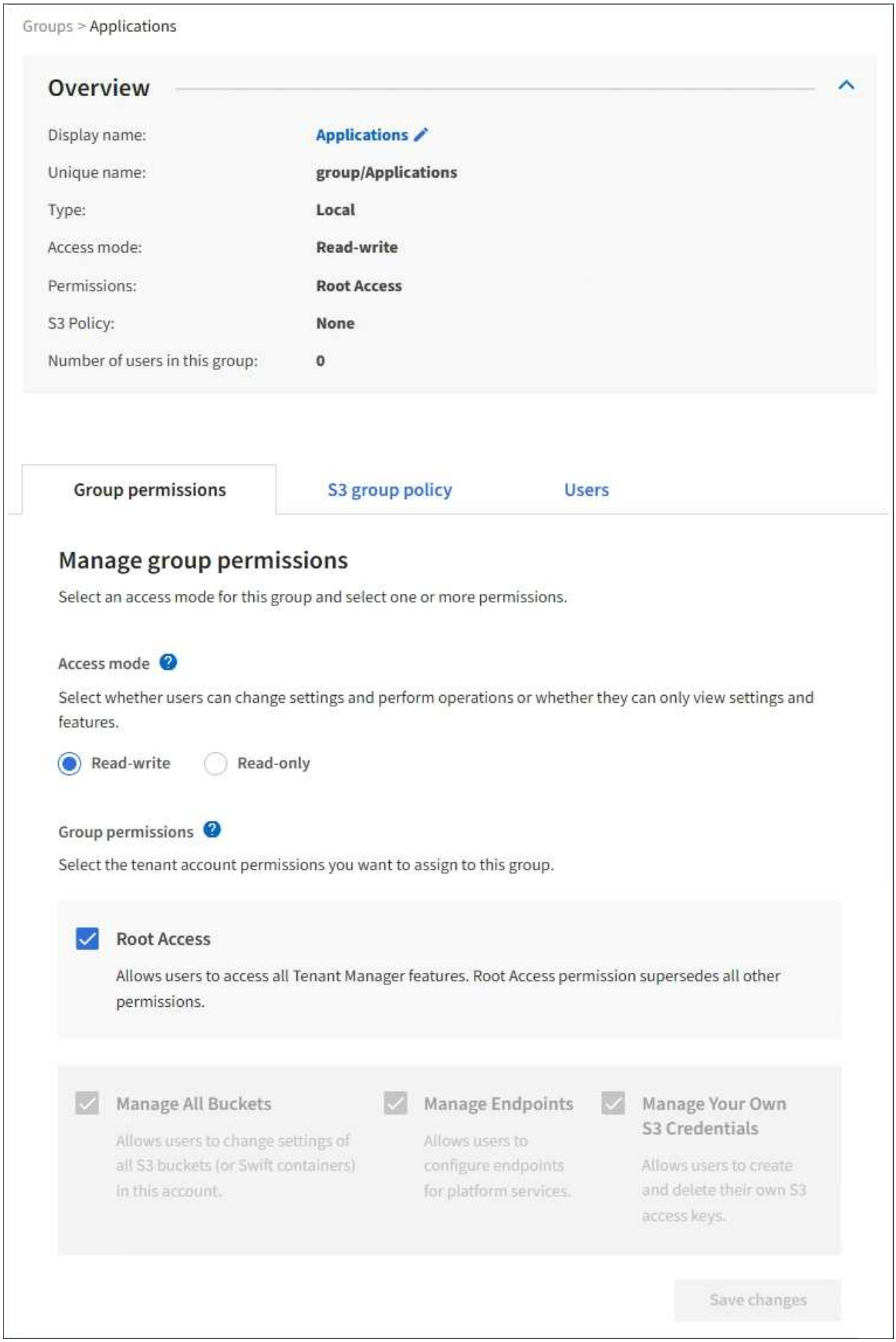
- Sie müssen über einen unterstützten Browser beim Tenant Manager angemeldet sein.
- Sie müssen einer Benutzergruppe mit Root Access-Berechtigung angehören.

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.


Groups > Applications
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

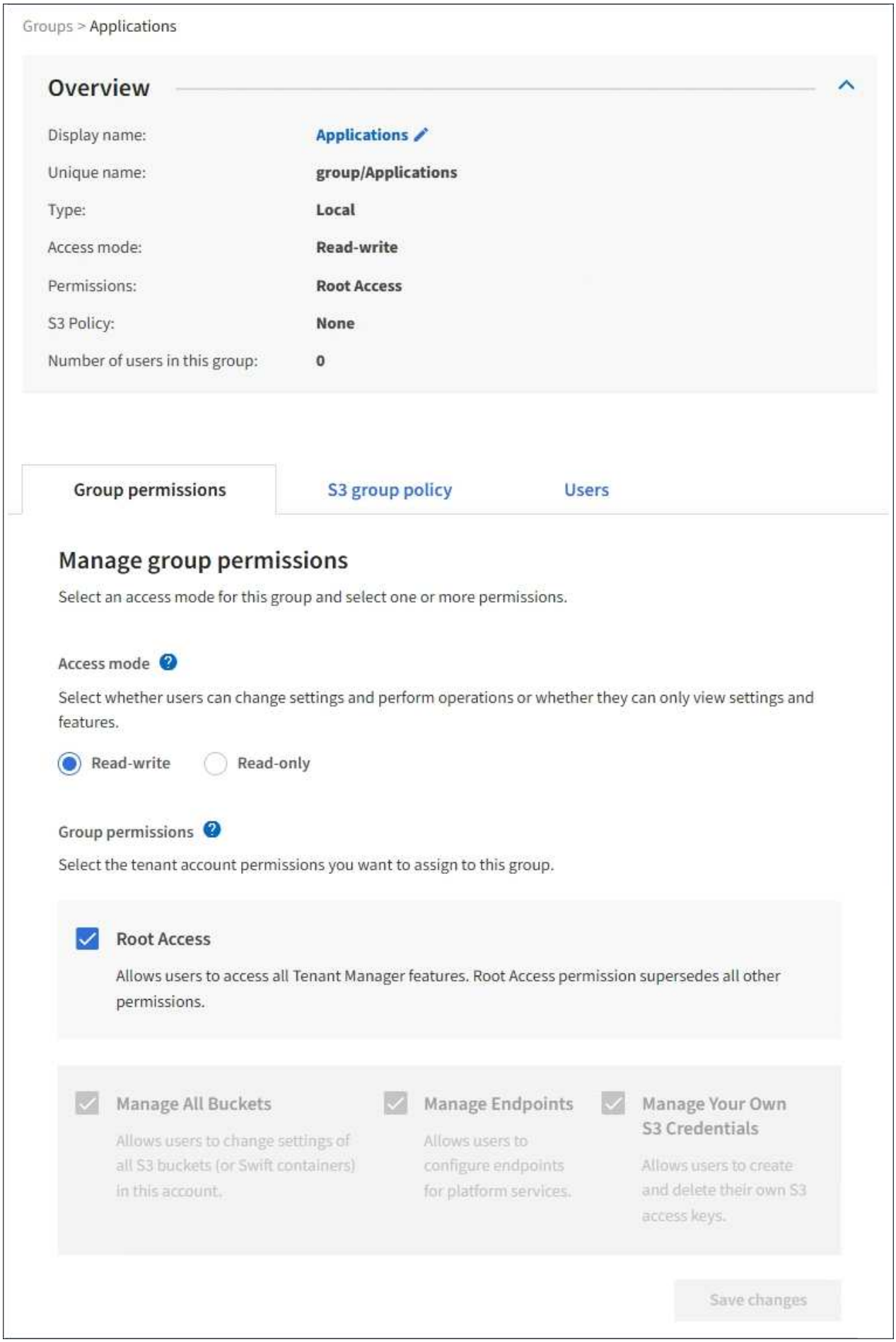
- Sie müssen über einen unterstützten Browser beim Tenant Manager angemeldet sein.
- Sie müssen einer Benutzergruppe mit Root Access-Berechtigung angehören.

Schritte

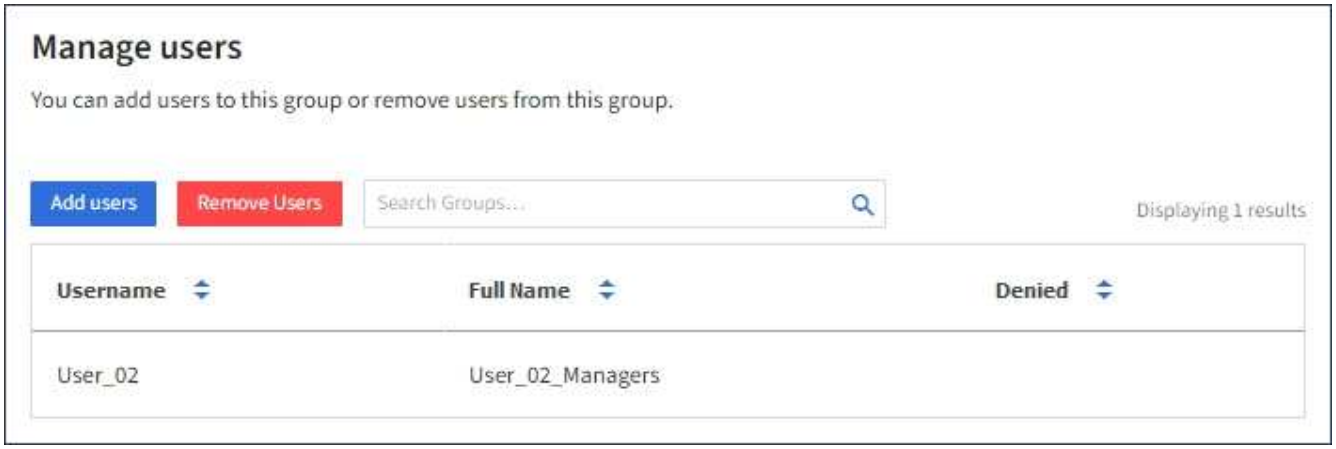
1. Wählen Sie **ZUGRIFFSVERWALTUNG** > **Gruppen**.
2. Wählen Sie den Namen der lokalen Gruppe aus, der Sie Benutzer hinzufügen möchten.

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

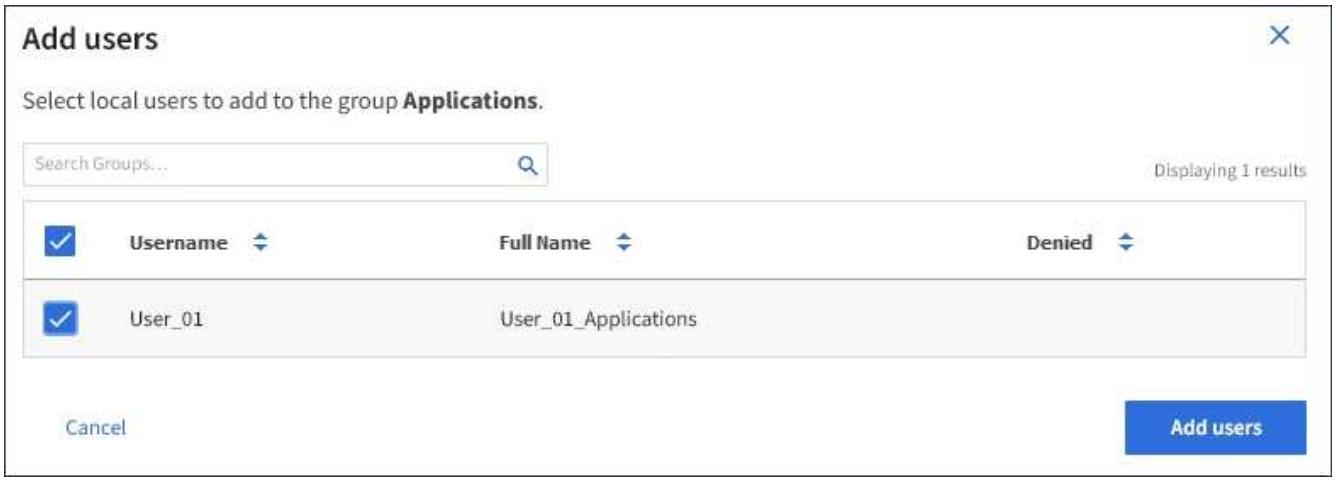
   Die Seite Gruppendetails wird angezeigt.


Groups > Applications
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**.



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



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.

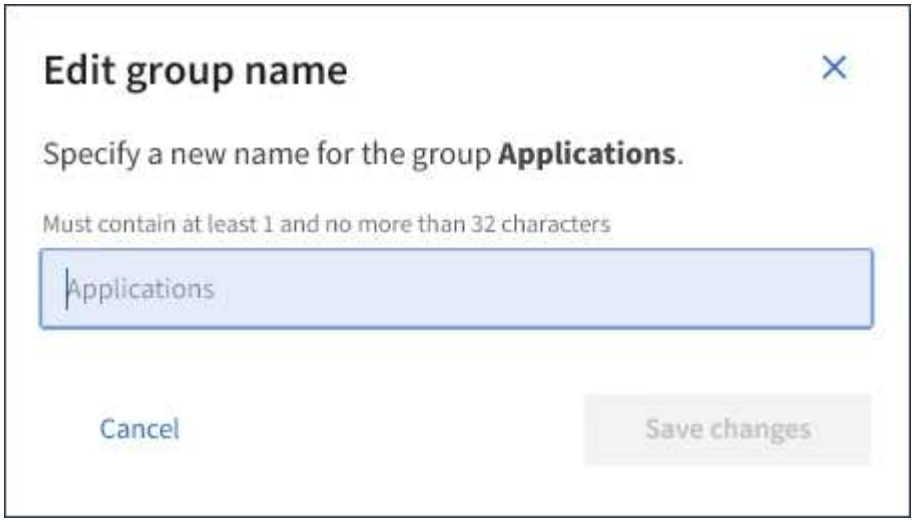
Was Sie benötigen

- 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.



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**.

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.

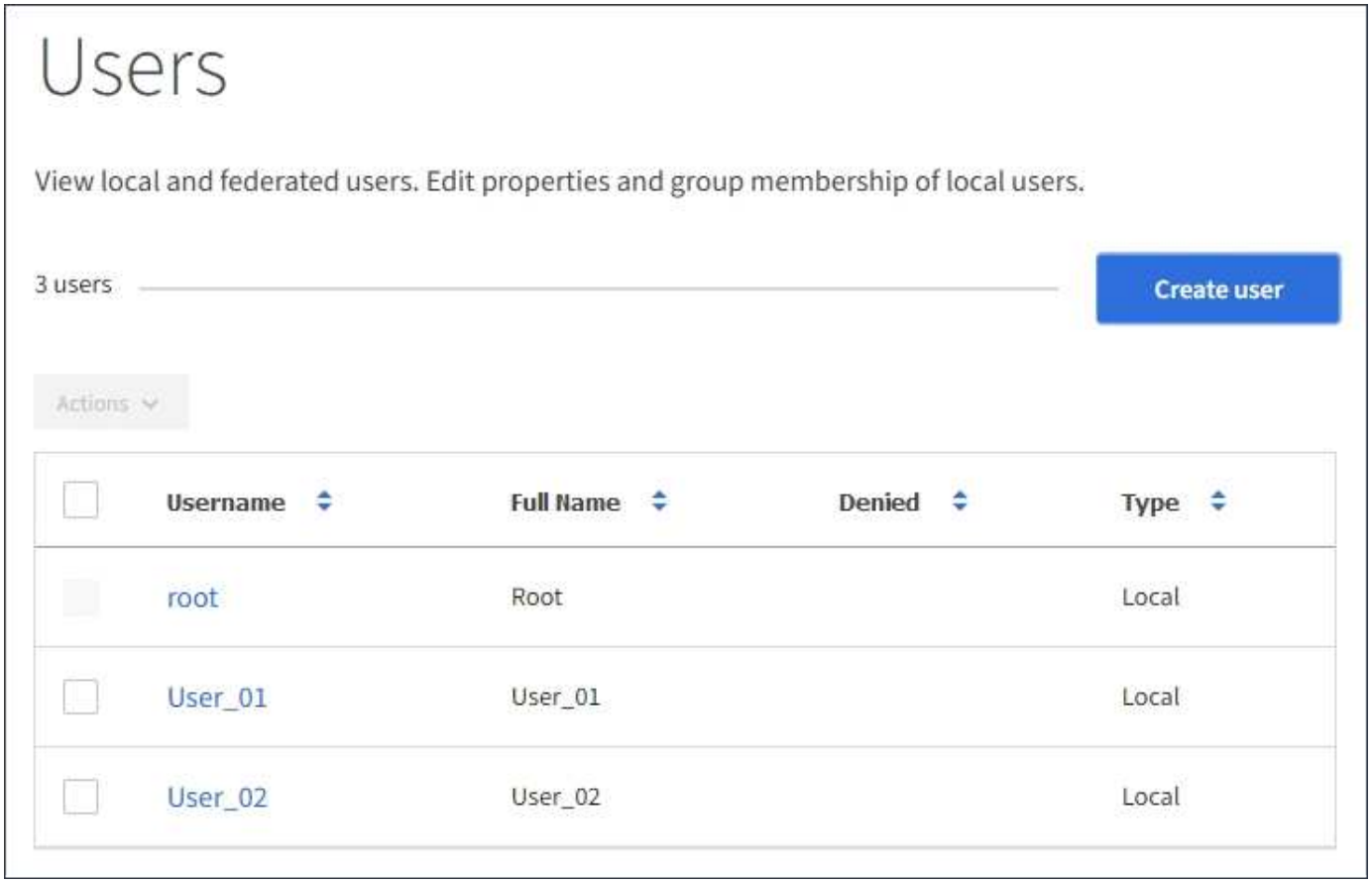
Was Sie benötigen

- 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**.



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 Bestätigungsdialogfeld **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.

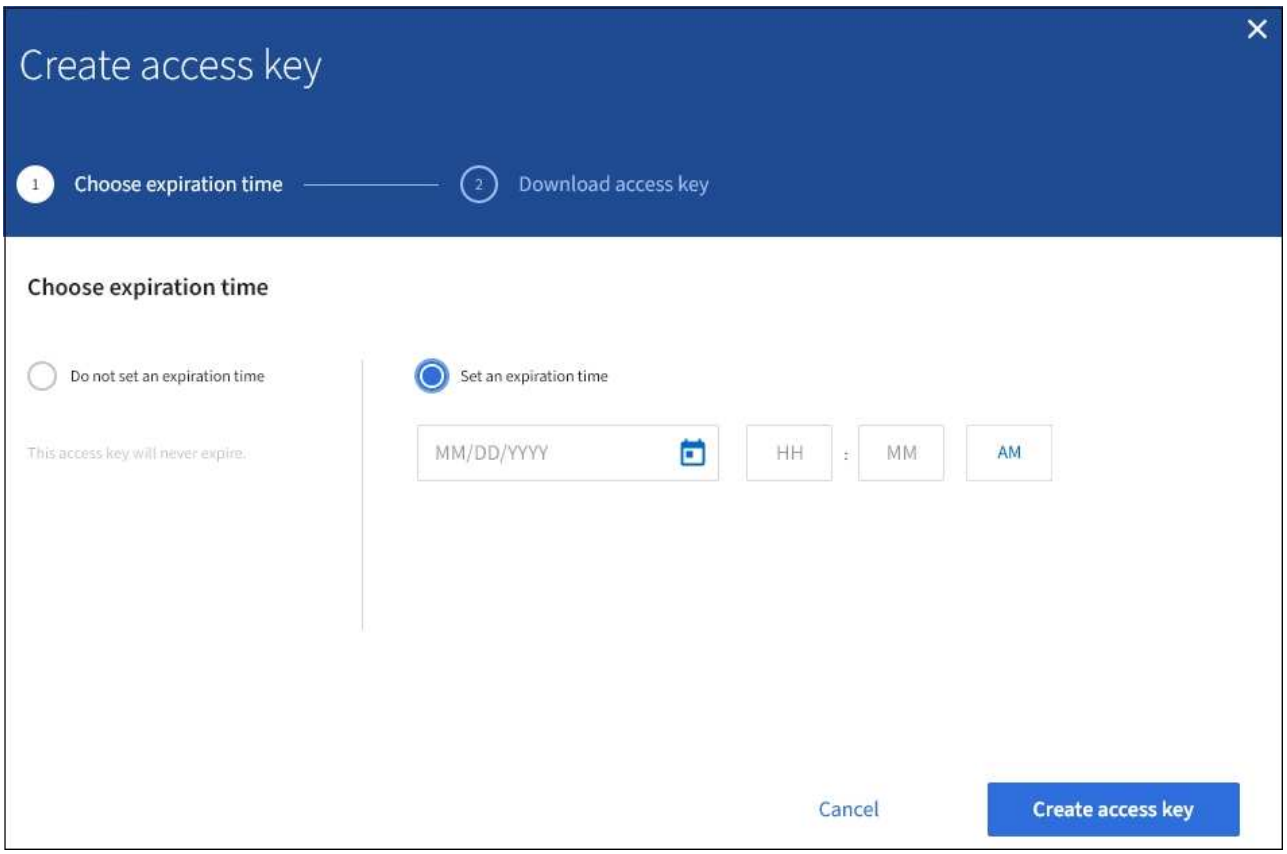
Sie können auf die S3-Buckets und Objekte aus Ihrem Konto zugreifen, indem Sie die Zugriffsschlüssel-ID und den geheimen Zugriffsschlüssel verwenden, die für Ihr Konto im Mandanten-Manager angezeigt werden. Aus diesem Grund schützen Sie Zugriffsschlüssel wie ein Passwort. Drehen Sie regelmäßig Zugriffsschlüssel, 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.

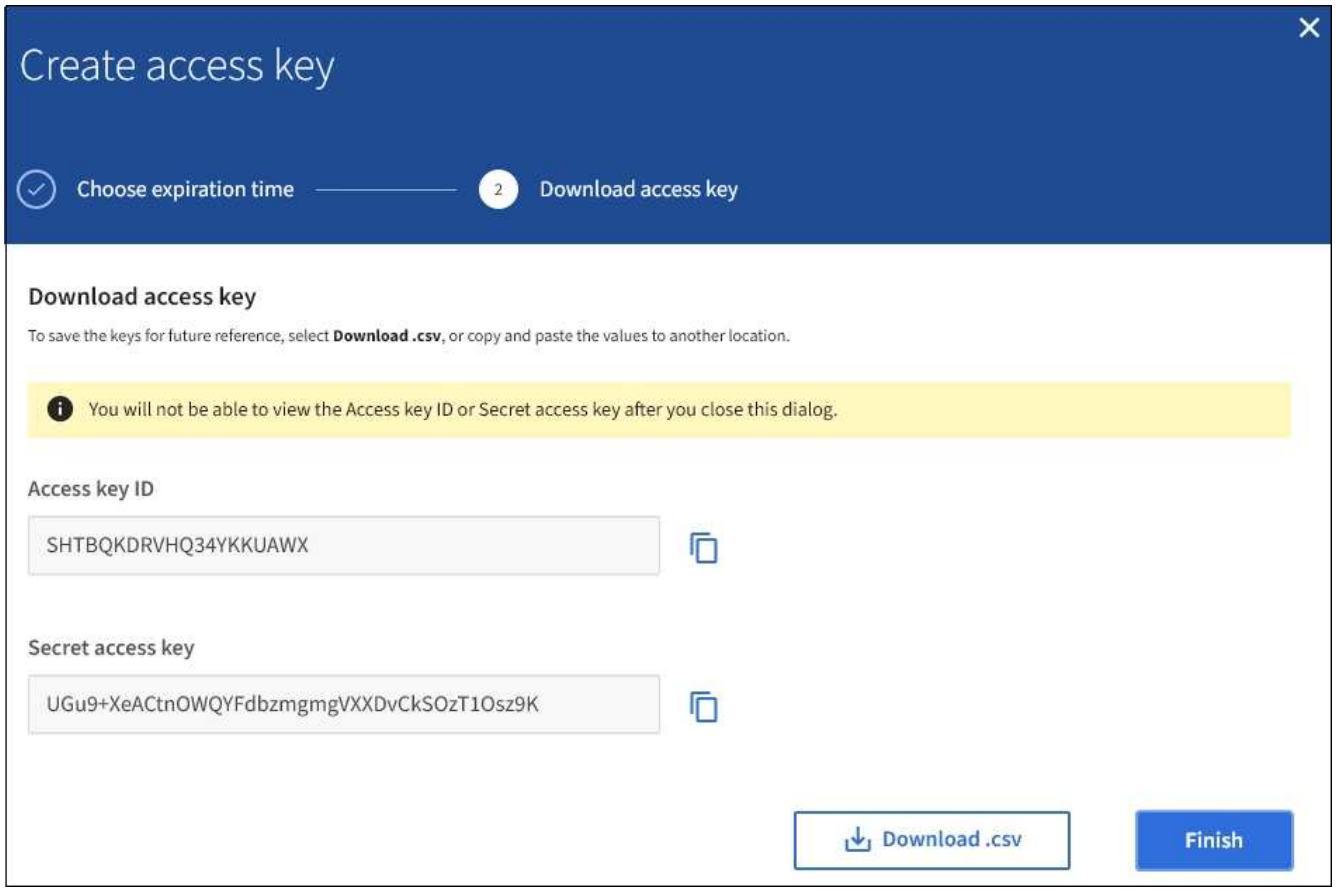


4. Wählen Sie **Zugriffsschlüssel erstellen**.

   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.



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

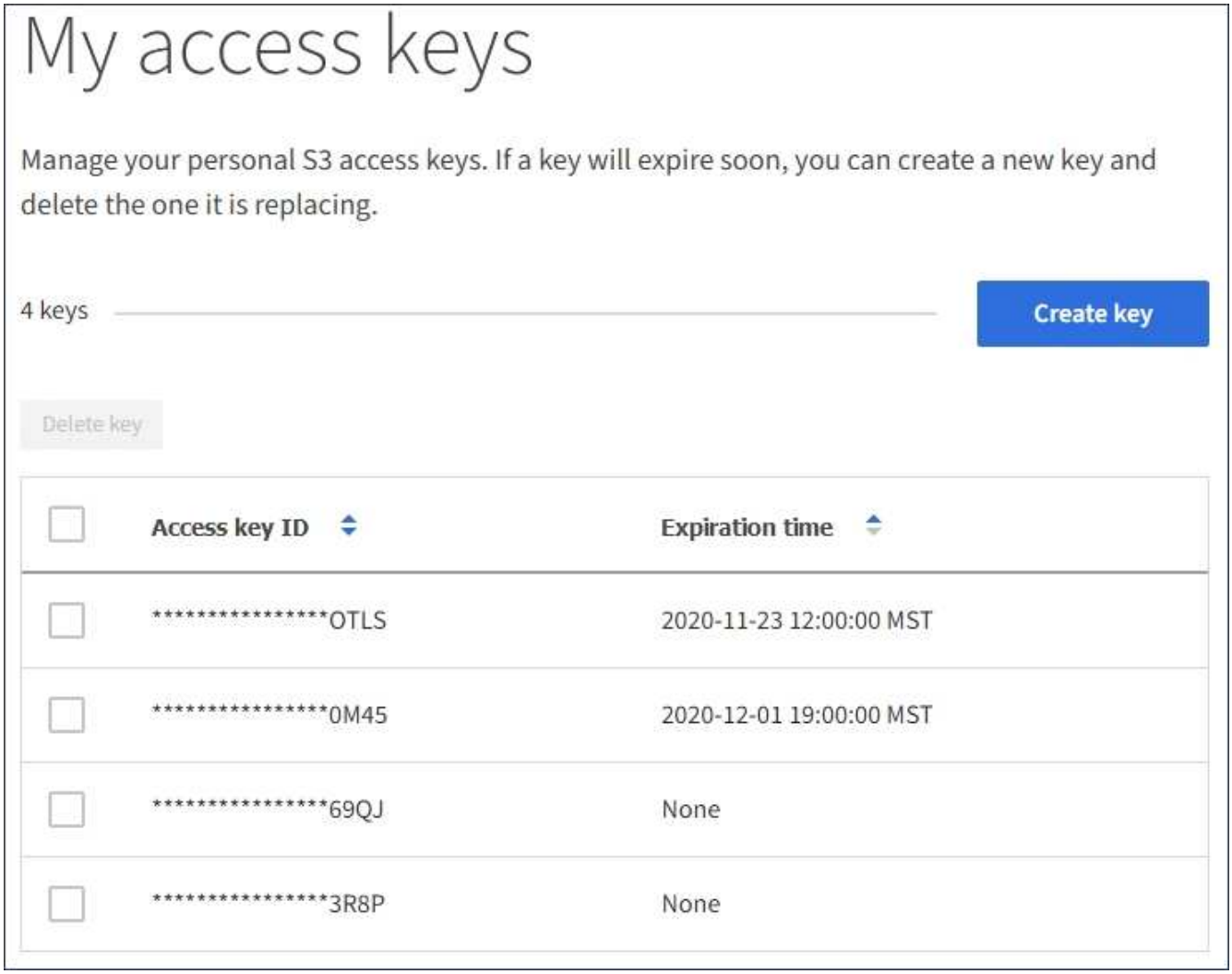
- Sie müssen über einen unterstützten Browser beim Tenant Manager angemeldet sein.
- Sie müssen über die Berechtigung zum Verwalten Ihrer eigenen S3-Anmeldedaten verfügen.

> 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.



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.

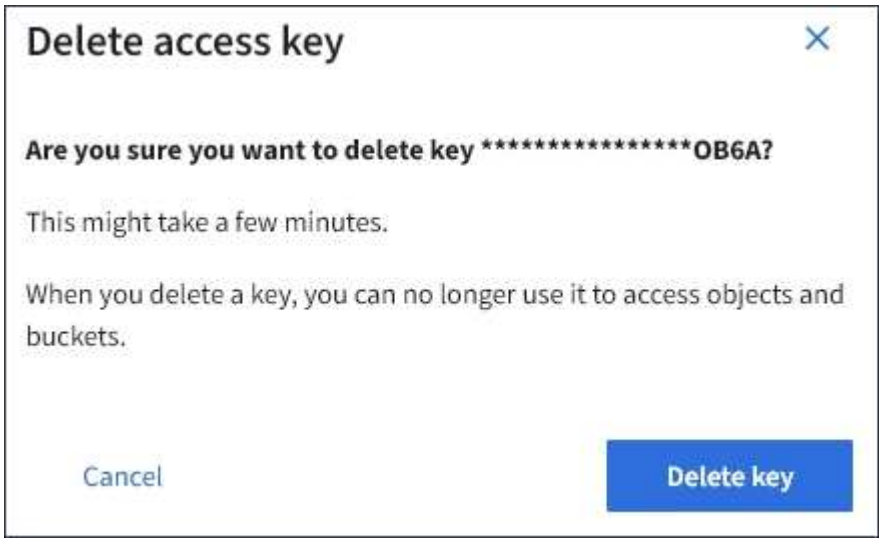
Schritte

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 Zugriffschlüssel, 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.

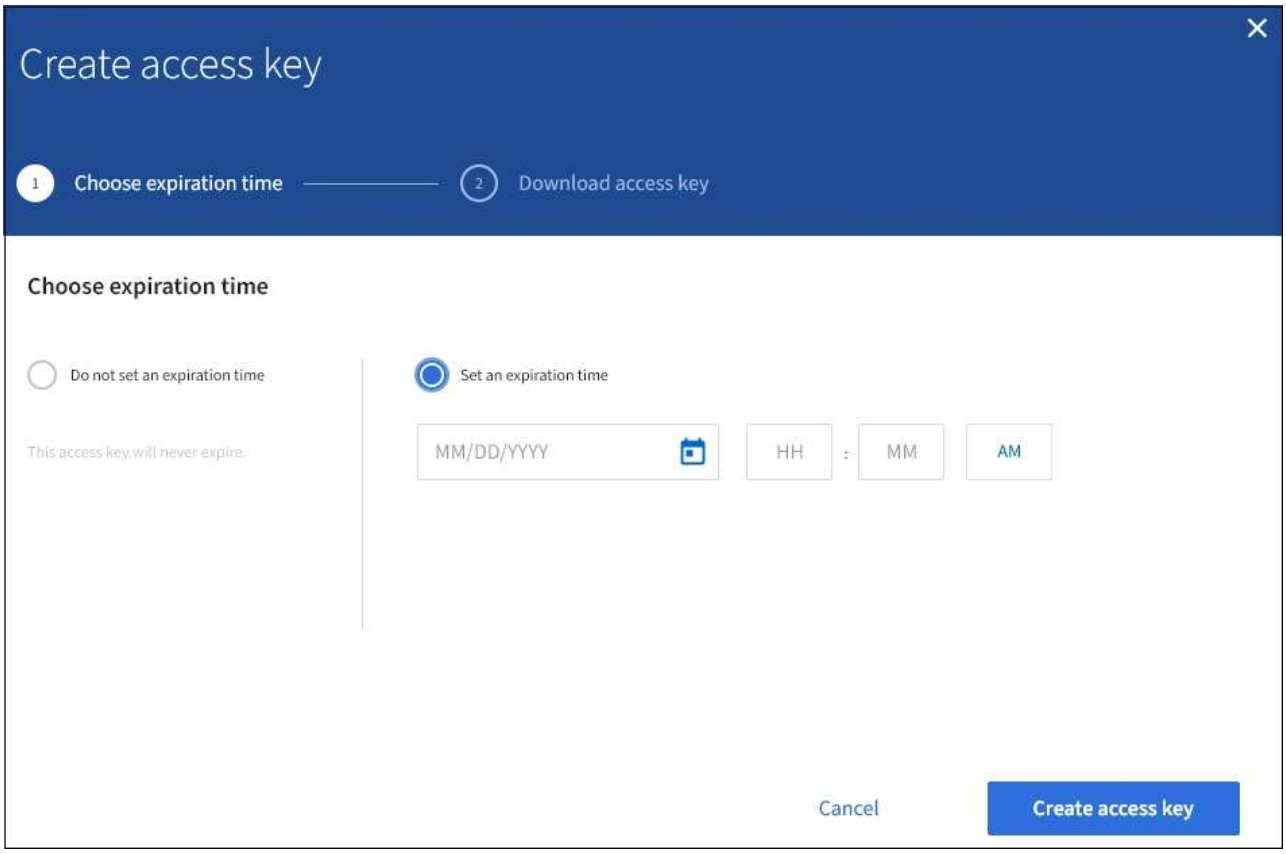
> Auf die S3-Buckets und Objekte, die zu einem Benutzer gehören, kann über die Zugriffsschlüssel-ID und den geheimen Zugriffsschlüssel zugegriffen werden, die für diesen Benutzer im Mandanten-Manager angezeigt werden. Aus diesem Grund schützen Sie Zugriffsschlüssel wie ein Passwort. Drehen Sie die Zugriffstasten 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.

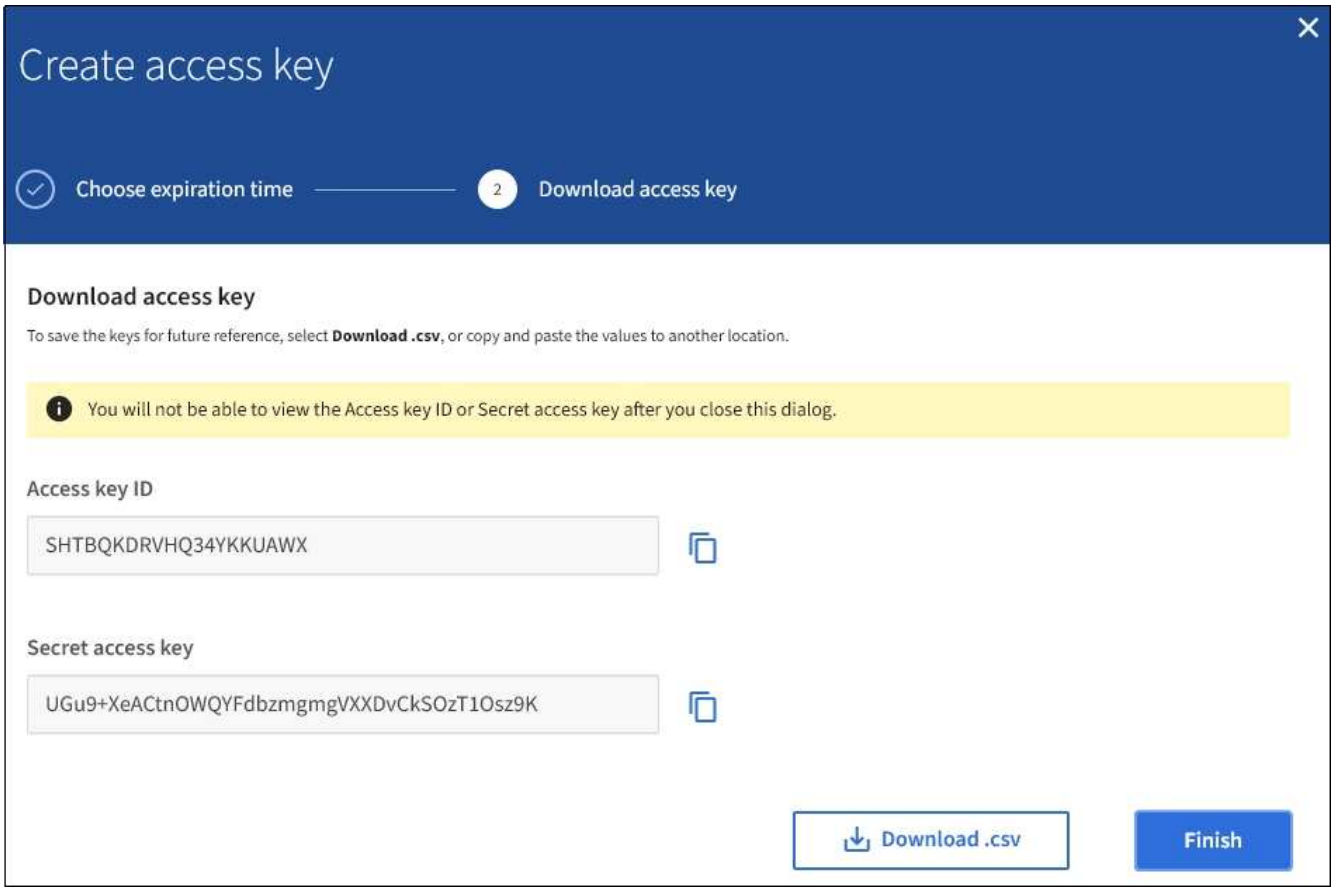


5. Wählen Sie **Zugriffsschlüssel erstellen**.

   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

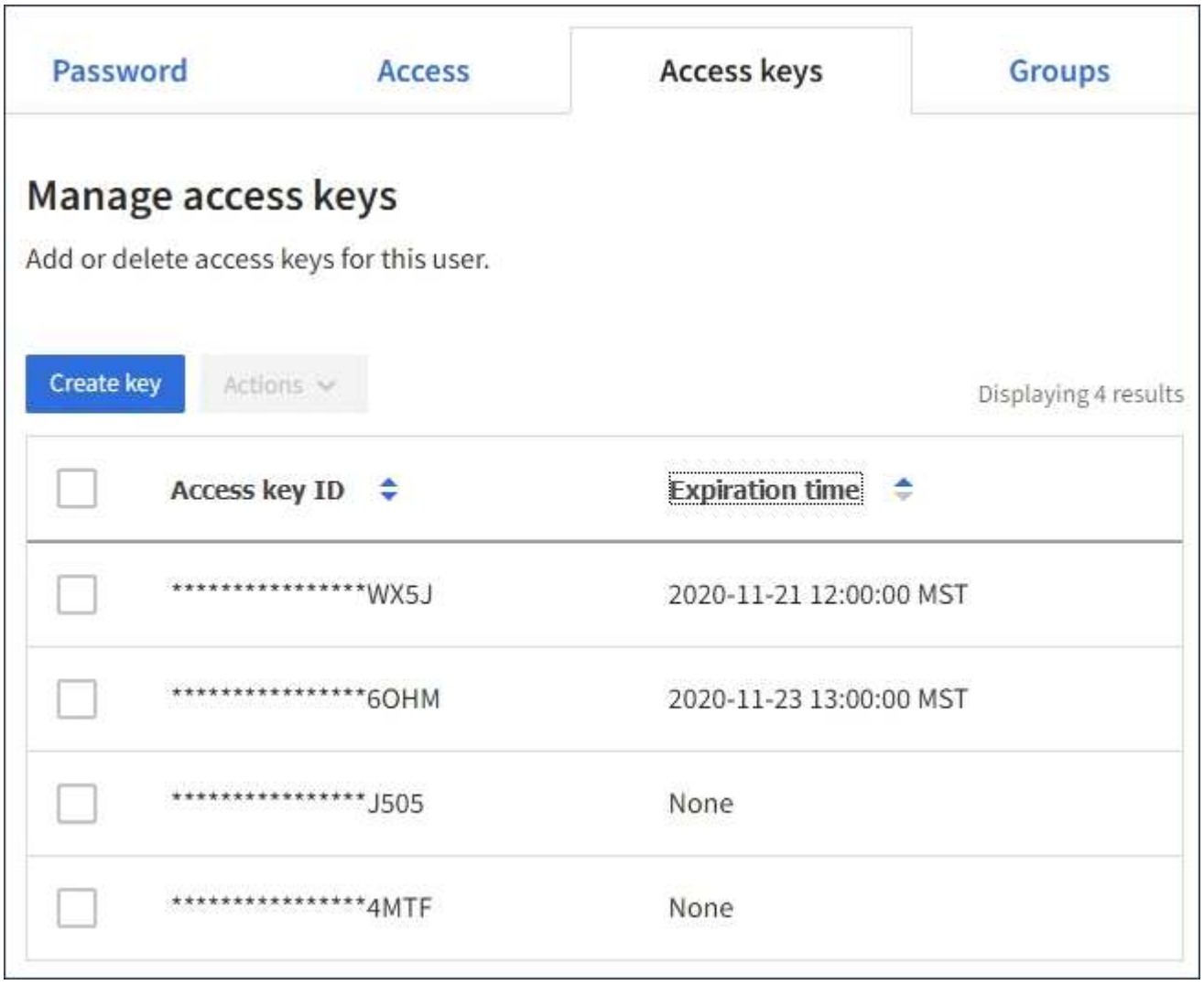
1. Wählen Sie **ZUGRIFFSVERWALTUNG** > **Benutzer**.

   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**.



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**.

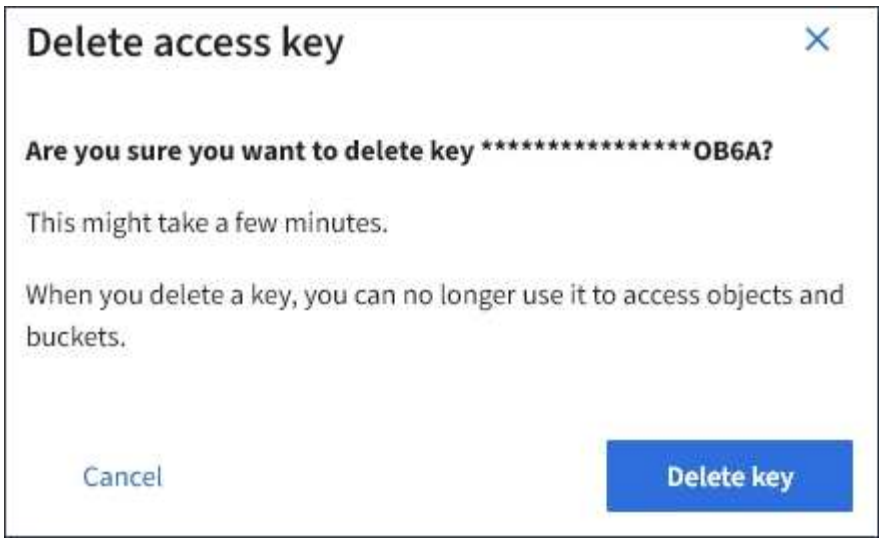
   Die Seite Benutzer wird angezeigt und listet die vorhandenen Benutzer auf.

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 Bestätigungsdialogfeld 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-Plattformservices managen.

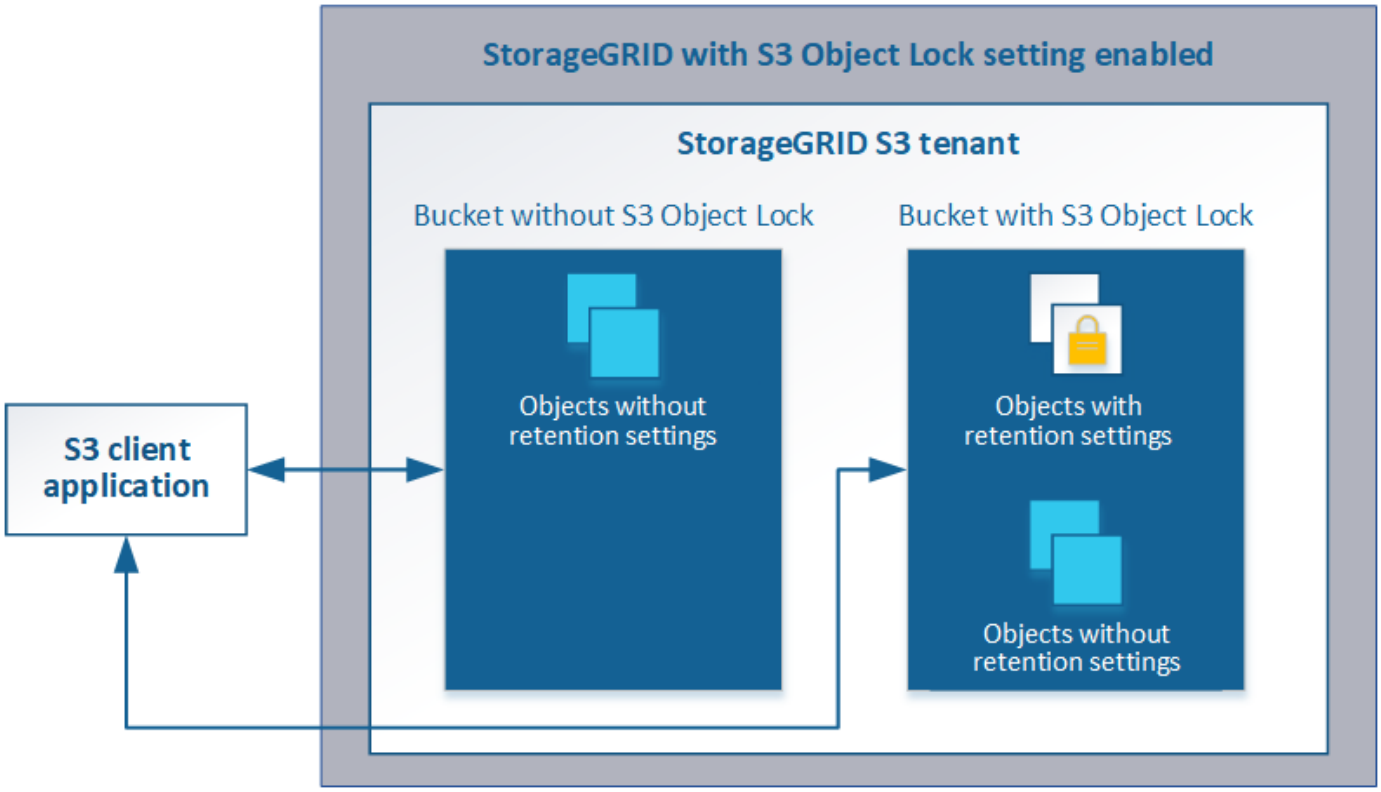
Verwenden der S3-Objektsperre

Sie können die S3-Objektsperrfunktion 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 Aufbewahrungspflichten 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.

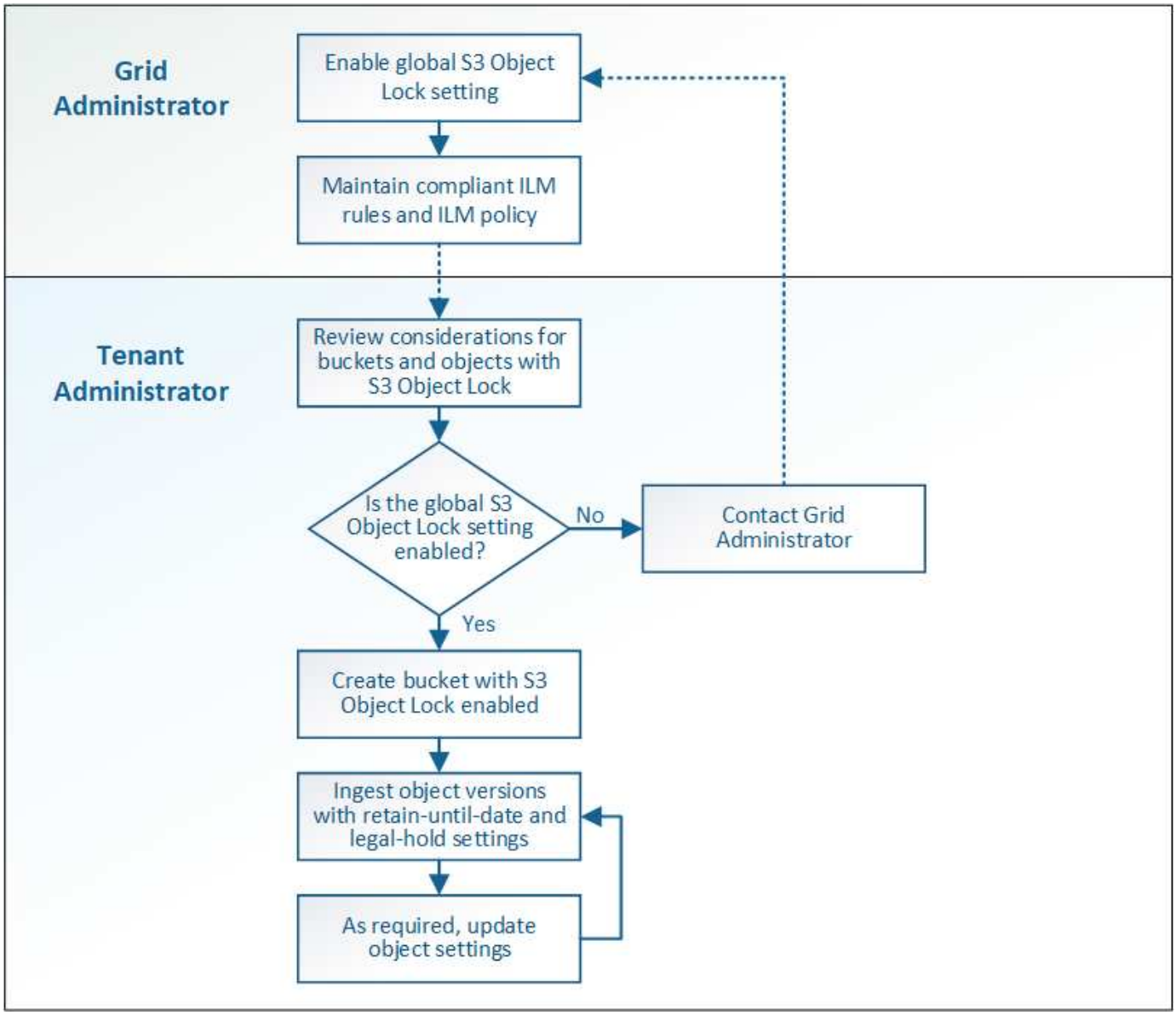
"NetApp Knowledge Base: Management älterer, konformer Buckets für StorageGRID 11.5"

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-Objektsperreneinstellung 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"

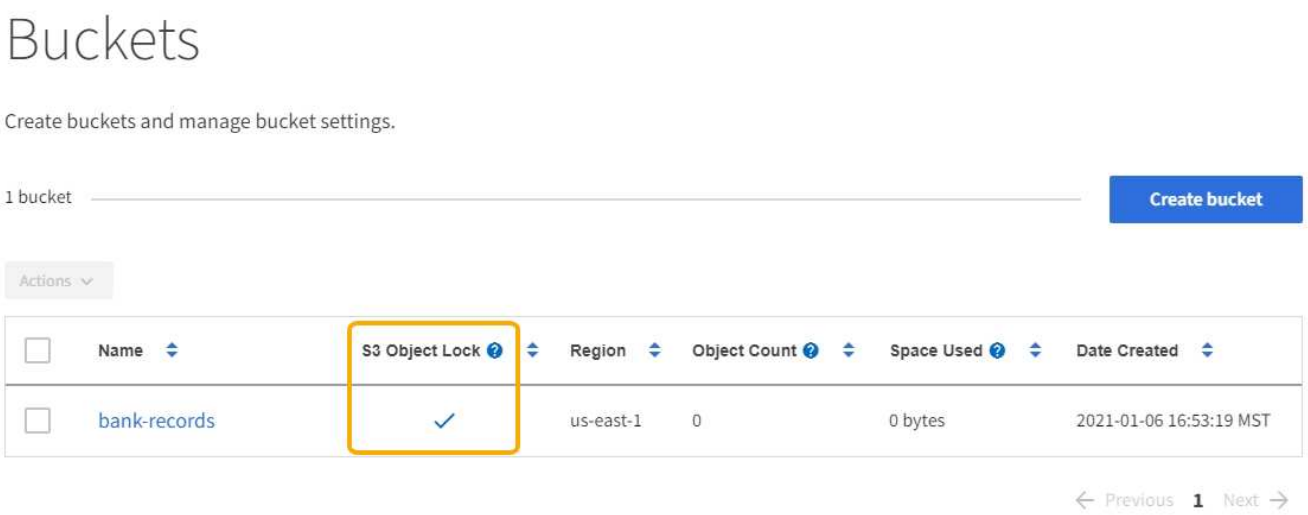
Anforderungen für die S3-Objektsperre

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.



- 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

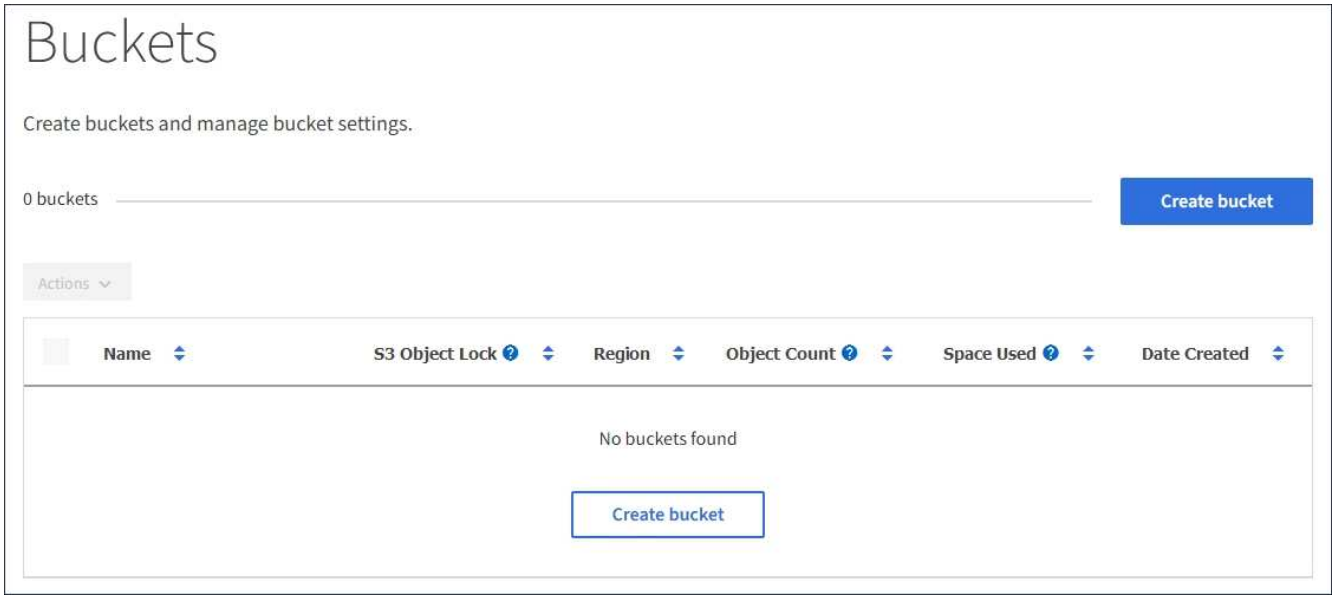
- Sie müssen über einen unterstützten Browser beim Tenant Manager angemeldet sein.
- Sie müssen einer Benutzergruppe angehören, die über die Berechtigung Alle Buckets verwalten oder Root Access verfügt. Diese Berechtigungen überschreiben die Berechtigungseinstellungen in Gruppen- oder Bucket-Richtlinien.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

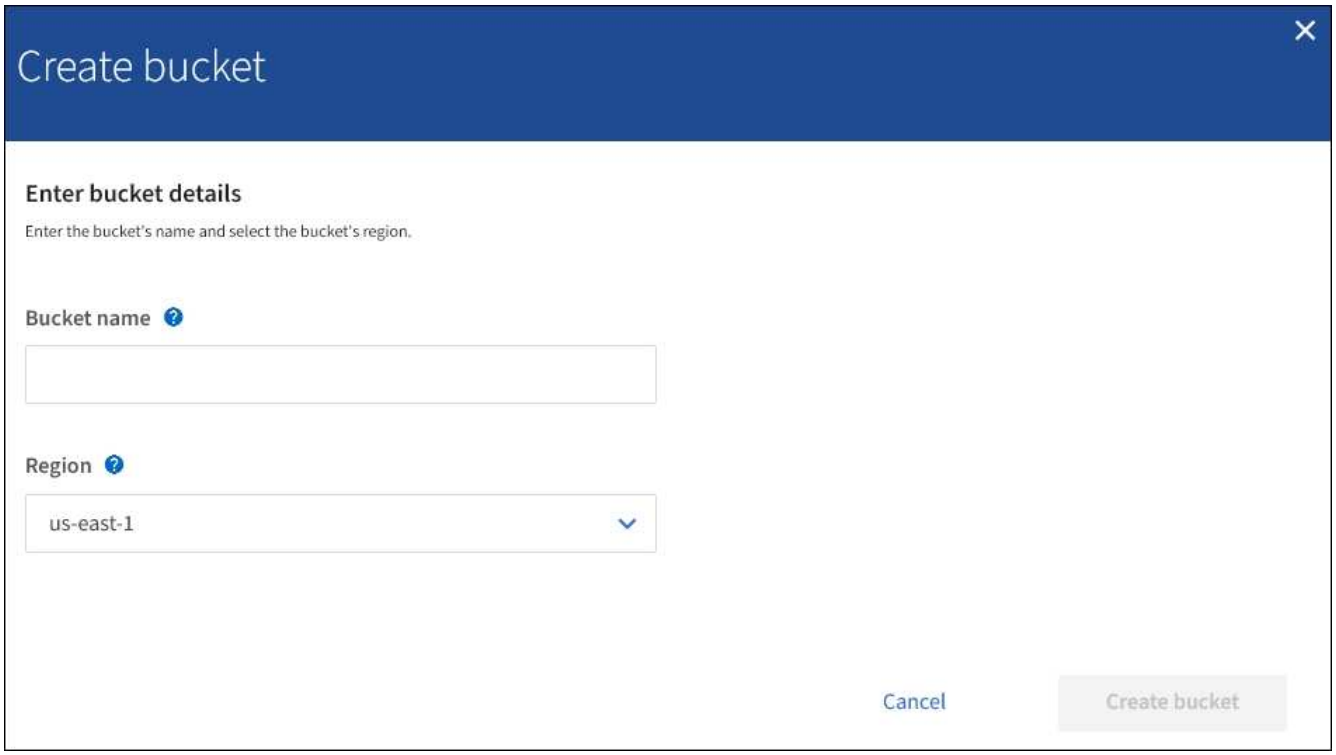
1. Wählen Sie **STORAGE (S3)** > **Buckets** aus.

   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.

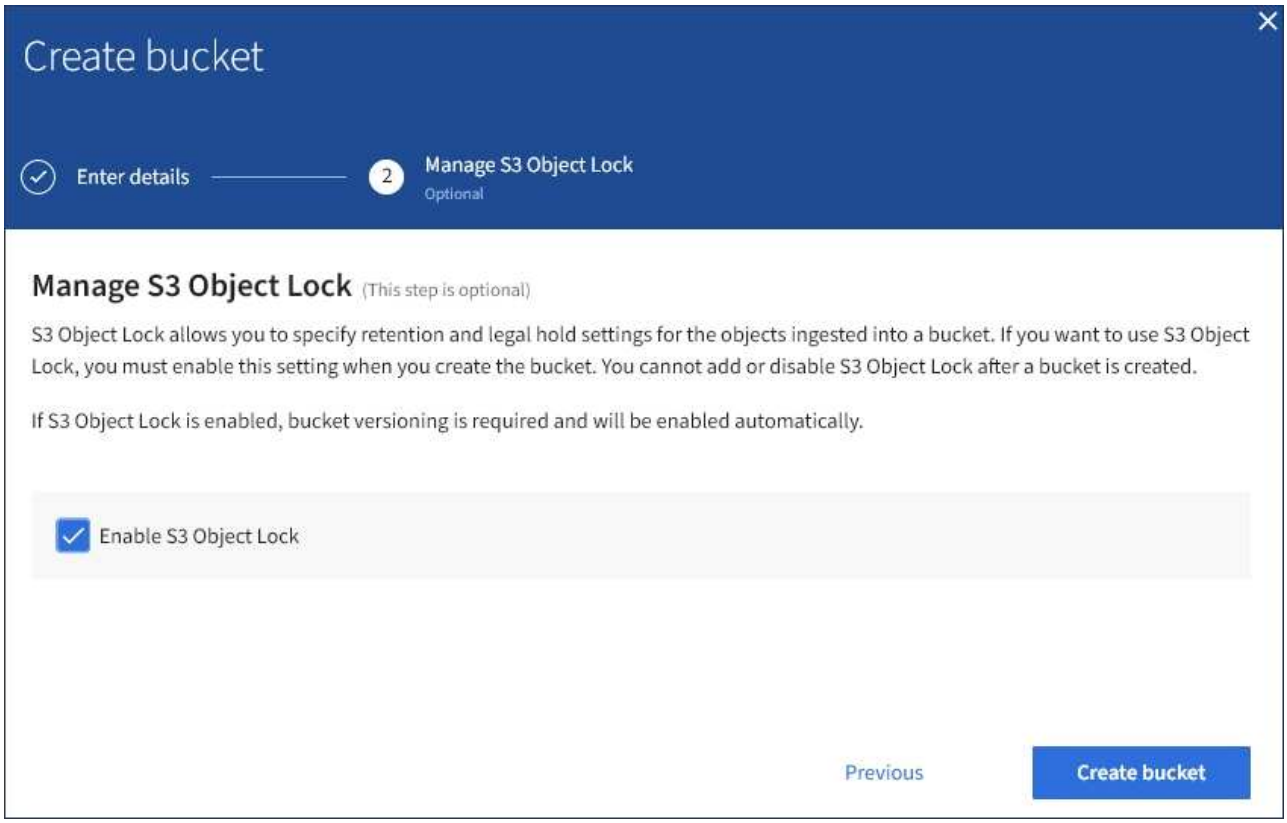
Weitere Informationen finden Sie in der Dokumentation zu Amazon Web Services (AWS).

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 erstellt `us-east-1` Werden.

   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 Aufbewahrungs-Einstellungen 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.

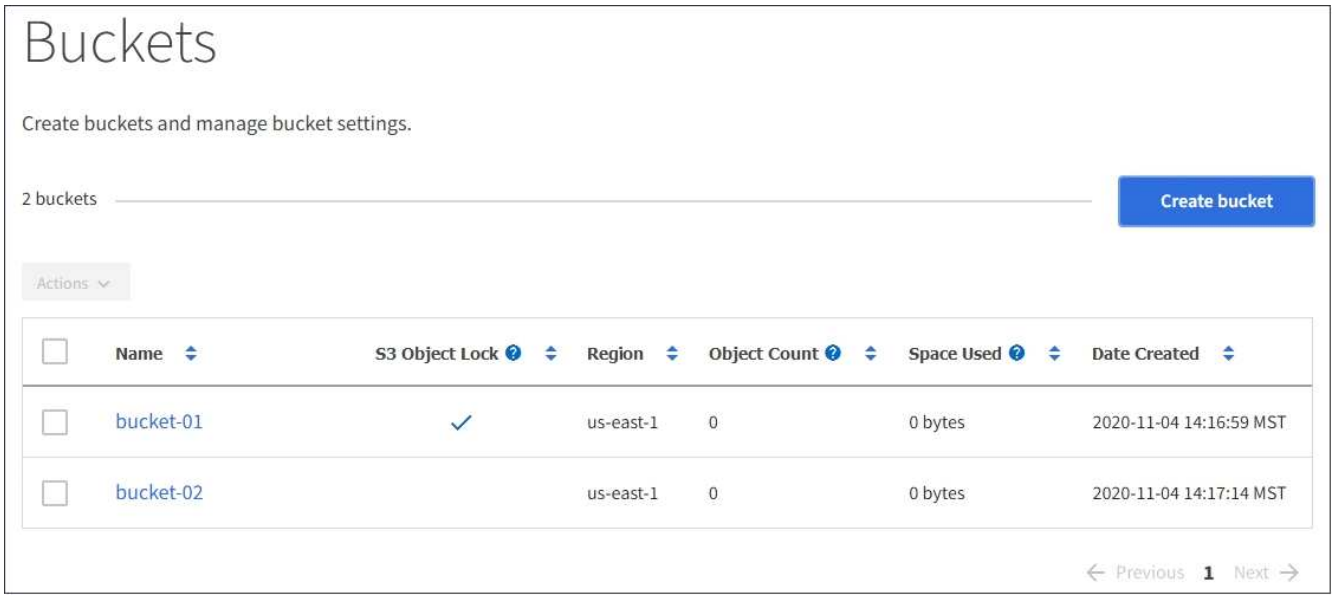
Was Sie benötigen

- 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.



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.

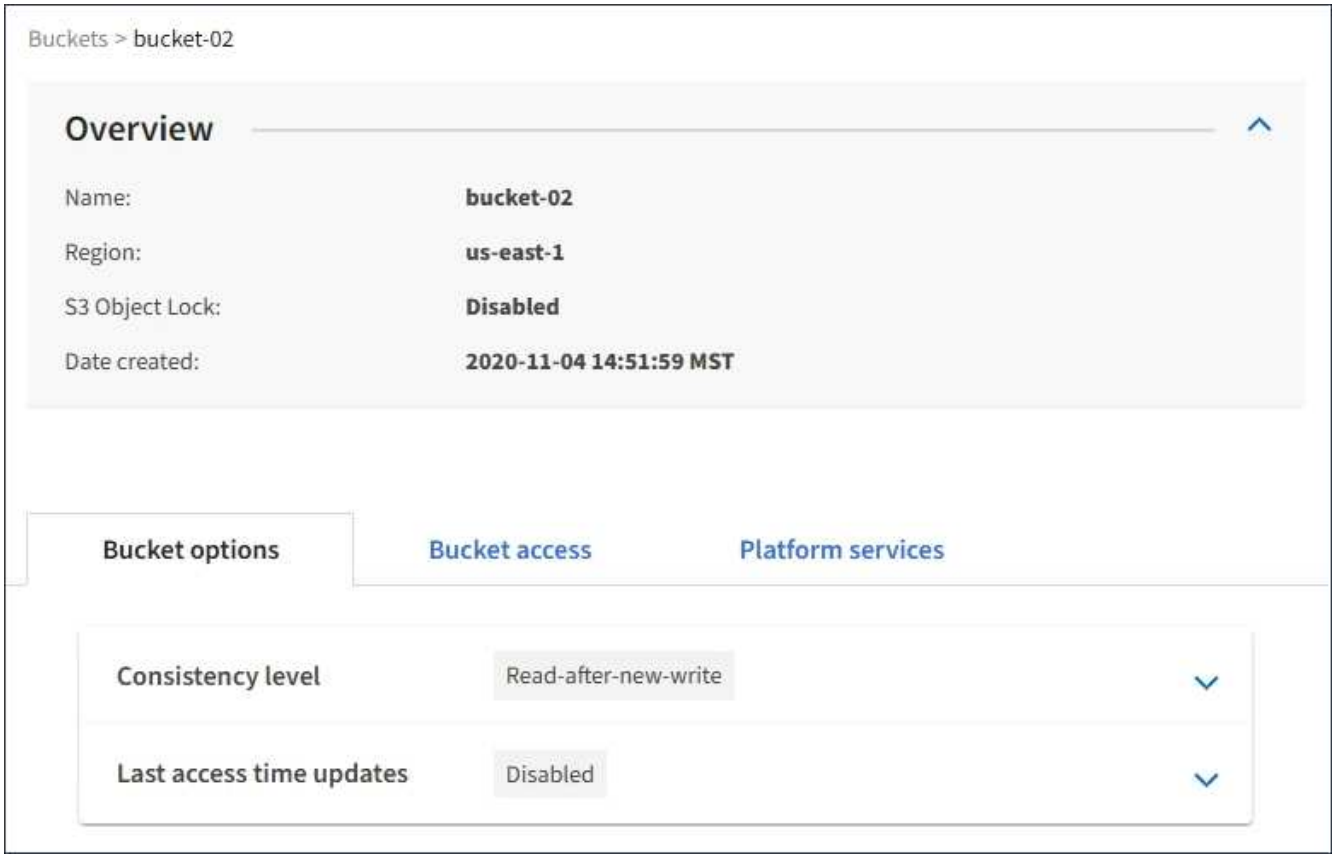
   > Die angezeigten Werte für Objektanzahl und verwendeter Speicherplatz sind Schätzungen. Diese Schätzungen sind vom Zeitpunkt der Aufnahme, der Netzwerkverbindung und des Node-Status betroffen.

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.



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 Suchintegrationsservice"

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.

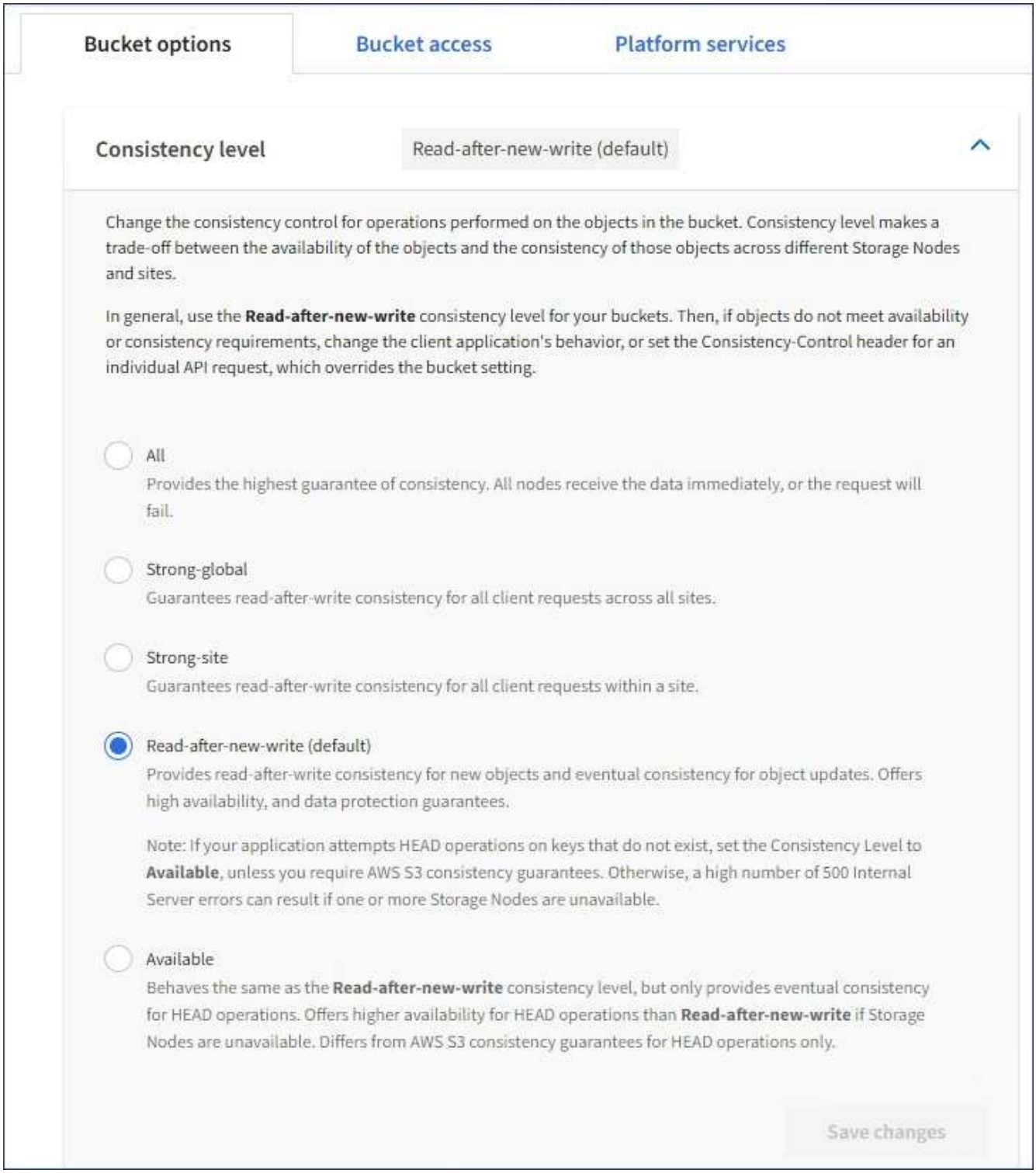
> Wenn Sie die Konsistenzstufe eines Buckets ändern, werden nur die Objekte, die nach der Änderung aufgenommen werden, garantiert, um die überarbeitete Ebene zu erfüllen.

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.



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)	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. **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.
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.

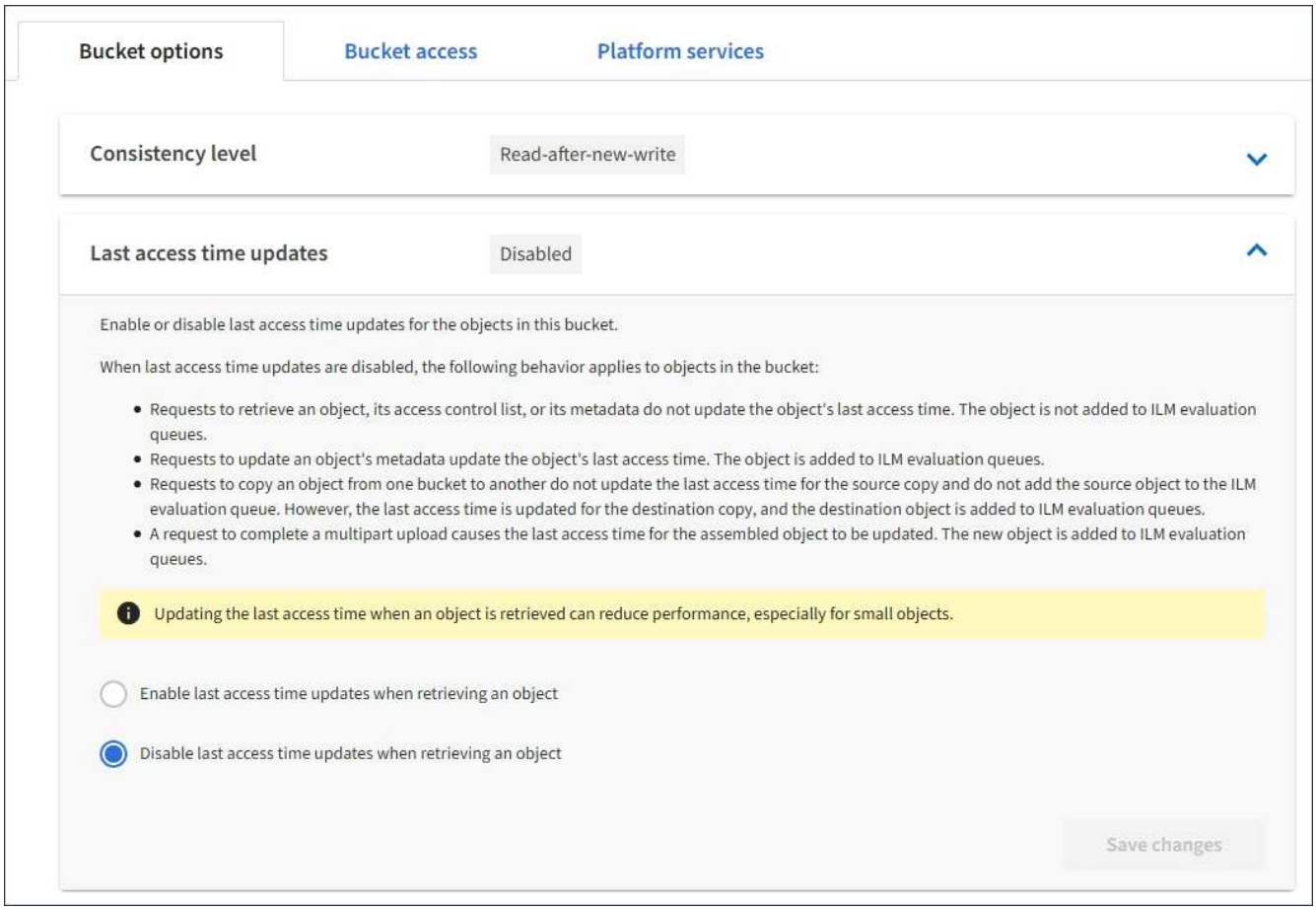
Anforderung zum Aktualisieren der Metadaten eines Objekts	Ja.	Ja.	Ja.	Ja.
Anforderung zum Kopieren eines Objekts von einem Bucket in einen anderen	• Nein, für die Quellkopie • Ja, für die Zielkopie	• Nein, für die Quellkopie • Ja, für die Zielkopie	• Ja, für die Quellkopie • Ja, für die Zielkopie	• Ja, für die Quellkopie • Ja, für die Zielkopie
Anforderung zum Abschließen eines mehrteiligen Uploads	Ja, für das zusammengesetzte Objekt	Ja, für das zusammengesetzte Objekt	Ja, für das zusammengesetzte Objekt	Ja, für das zusammengesetzte Objekt

Schritte

1. Wählen Sie **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.



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.

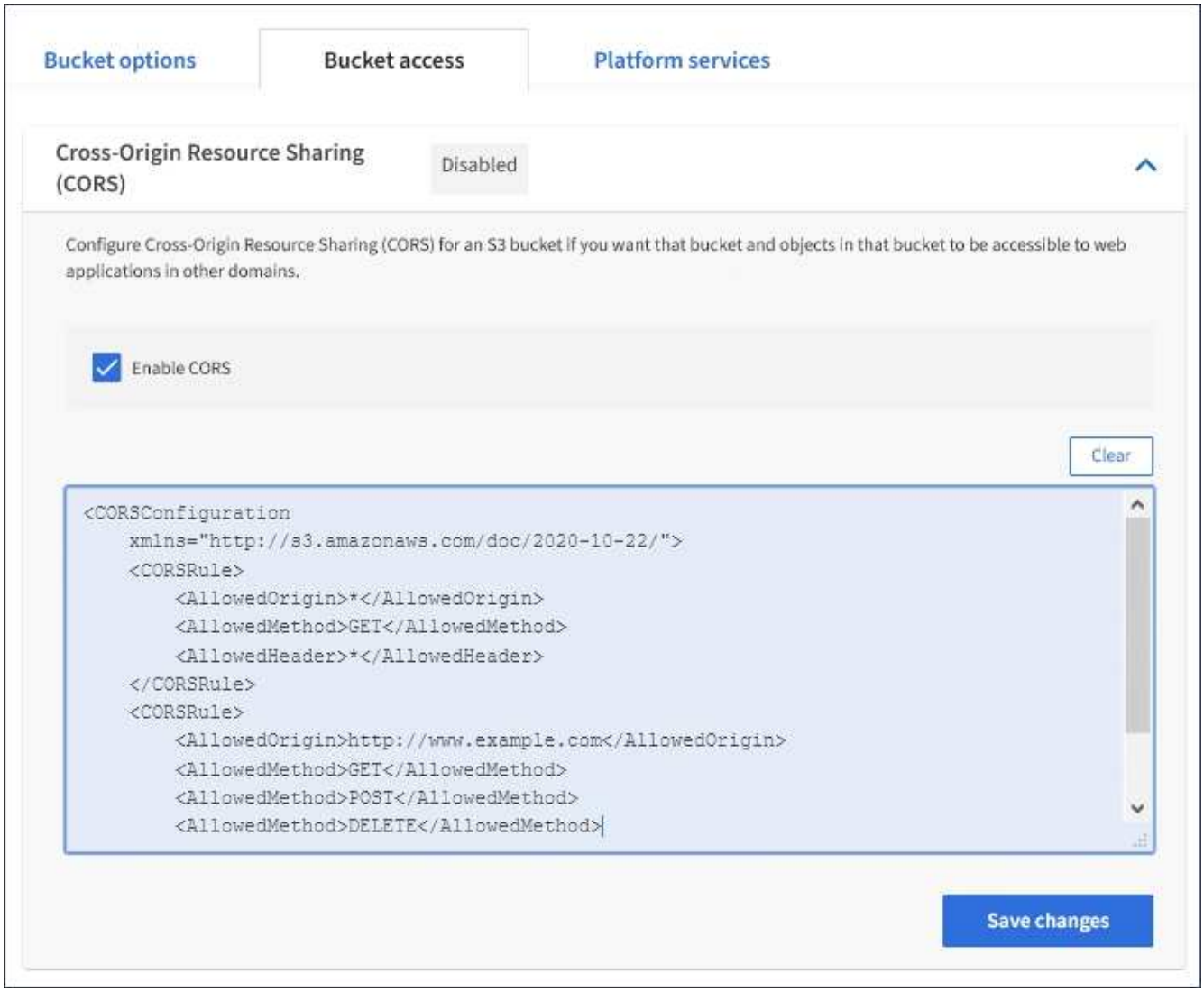
   ```
   <CORSConfiguration
       xmlns="http://s3.amazonaws.com/doc/2020-10-22/">
       <CORSRule>
           <AllowedOrigin>*</AllowedOrigin>
           <AllowedMethod>GET</AllowedMethod>
           <AllowedHeader>*</AllowedHeader>
       </CORSRule>
       <CORSRule>
           <AllowedOrigin>http://www.example.com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



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.

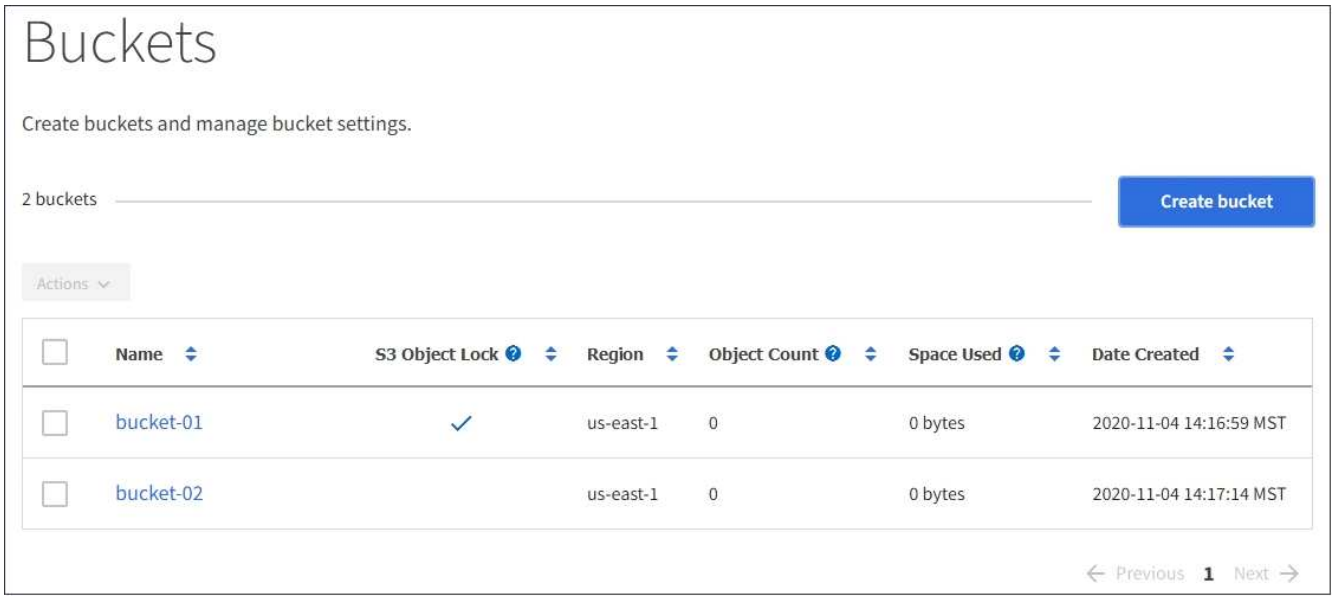
Ein S3-Bucket kann nicht gelöscht werden, wenn er Objekte oder nicht aktuelle Objektversionen enthält.

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.

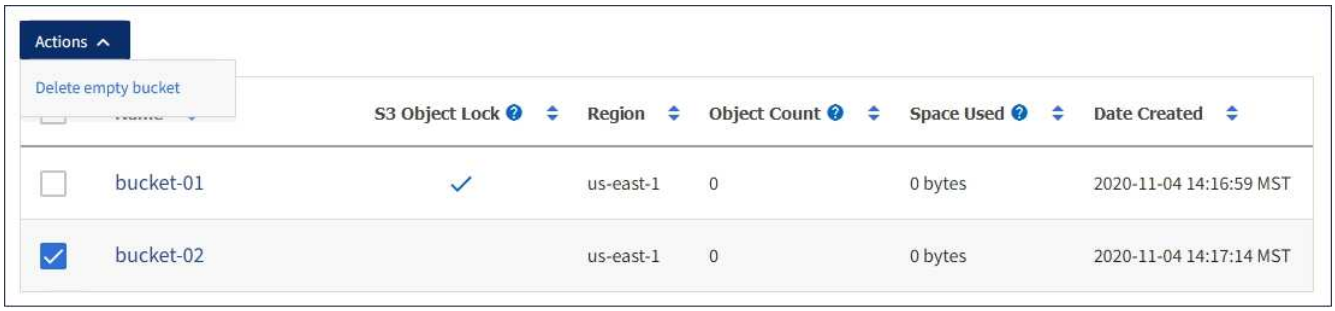
   Die Seite Buckets wird angezeigt und zeigt alle vorhandenen S3-Buckets an.



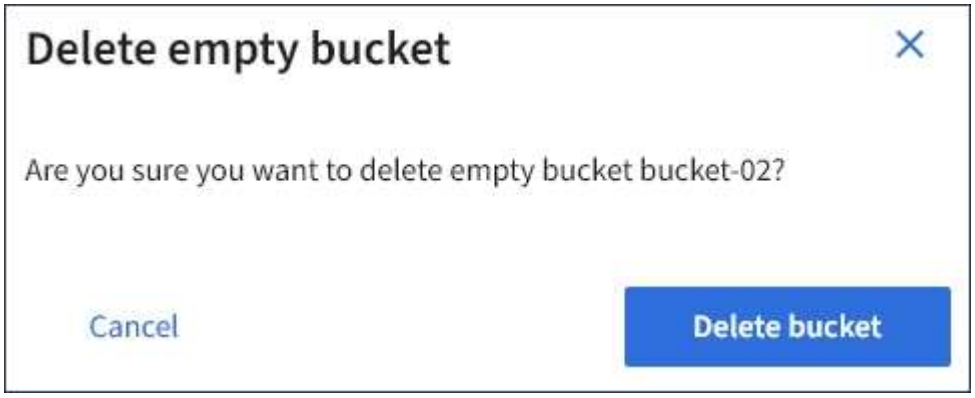
2. Aktivieren Sie das Kontrollkästchen für den leeren Bucket, den Sie löschen möchten.

   Das Menü Aktionen ist aktiviert.

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



   Eine Bestätigungsmeldung wird angezeigt.



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.

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-Objektsperrmetadaten (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 Plattformdiensten muss für jedes Mandantenkonto durch einen StorageGRID-Administrator aktiviert werden, der den Grid Manager oder die Grid Management API verwendet.

Die Konfiguration von Plattform-Services

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 Plattformdienst, 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	• GET Bucket-Replizierung • PUT Bucket-Replizierung
Benachrichtigungen	• Bucket-Benachrichtigung ABRUFEN • PUT Bucket-Benachrichtigung
Integration von Suchen	• Konfiguration der Bucket-Metadaten-Benachrichtigungen ABRUFEN • PUT Bucket-Metadaten-Benachrichtigungskonfiguration Diese Vorgänge sind individuell für StorageGRID.

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-Anforderungs-Kopfzeile 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 Löschmarkierung repliziert. Wenn der Ziel-Bucket nicht versioniert ist, wird durch das Löschen eines Objekts im Quell-Bucket der Löschmarker 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 Liefererfolgs durchgeführt werden. Da die Bereitstellung asynchron ist, entspricht die Reihenfolge der Benachrichtigungen am Ziel nicht der Reihenfolge der Ereignisse auf dem Quell-Bucket. Dies gilt insbesondere für Vorgänge, die von unterschiedlichen StorageGRID-Standorten stammen. Sie können 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	`sgws:s3`
AwsRegion	Nicht enthalten
X-amz-id-2	Nicht enthalten
arn	`urn:sgws:s3:::bucket_name`

Verwandte Informationen

"Ereignisbenachrichtigungen werden konfiguriert"

Beschreibung des Suchintegrationsservice

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 befanden. Um sicherzustellen, dass Objektmetadaten für alle Objekte im Bucket an das Ziel gesendet werden, sollten Sie eines der folgenden Aktionen durchführen:

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

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 Suchintegrationsservice"

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

Überlegungen	Details
ILM-gesteuerte Objektlöschungen	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. Suchintegrationsanfragen werden dagegen gesendet, wenn Objekte aufgrund von ILM gelöscht werden.

Überlegungen bei der Verwendung des CloudMirror Replikationsservice

Überlegungen	Details
Replikationsstatus	StorageGRID unterstützt das nicht `x-amz-replication-status` 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	Wenn die Versionierung im S3-Quell-Bucket von StorageGRID aktiviert ist, sollten Sie auch die Versionierung für den Ziel-Bucket aktivieren. Beachten Sie bei der Verwendung der Versionierung, dass die Bestellung von Objektversionen im Ziel-Bucket am besten ist und vom CloudMirror Service nicht garantiert wird, da Einschränkungen im S3-Protokoll bestehen. **Hinweis**: Version-IDs für den Quell-Bucket in StorageGRID stehen nicht im Zusammenhang mit den Version-IDs für den Ziel-Bucket.

Tagging für Objektversionen	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. 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.
Mehrteilige Uploads und `ETag` Werte	Bei der Spiegelung von Objekten, die mittels eines mehrteiligen Uploads hochgeladen wurden, bleiben die Teile vom CloudMirror-Service nicht erhalten. Als Ergebnis davon ist der `ETag` Der Wert für das gespiegelte Objekt unterscheidet sich vom `ETag` Wert des ursprünglichen Objekts.
Mit SSE-C verschlüsselte Objekte (serverseitige Verschlüsselung mit vom Kunden bereitgestellten Schlüsseln)	Der CloudMirror-Dienst unterstützt keine mit SSE-C verschlüsselten Objekte Wenn Sie versuchen, ein Objekt für die CloudMirror-Replikation in den Quell-Bucket aufzunehmen, und die Anforderung die SSE-C-Anfrageheader enthält, schlägt der Vorgang fehl.
Bucket mit S3-Objektsperre aktiviert	Wenn der Ziel-S3-Bucket für CloudMirror-Replikation S3-Objektsperre aktiviert ist, schlägt der Replikationsvorgang mit einem AccessDenied-Fehler fehl.

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

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

Elemente URN

Der URN für einen Endpunkt von Plattformservices 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:mysite:s3:optional:optional:bucket-name
```

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

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

- Benachrichtigungen:

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

- Integration von Suchen:

```
urn:mysite: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 Plattformdienst 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)

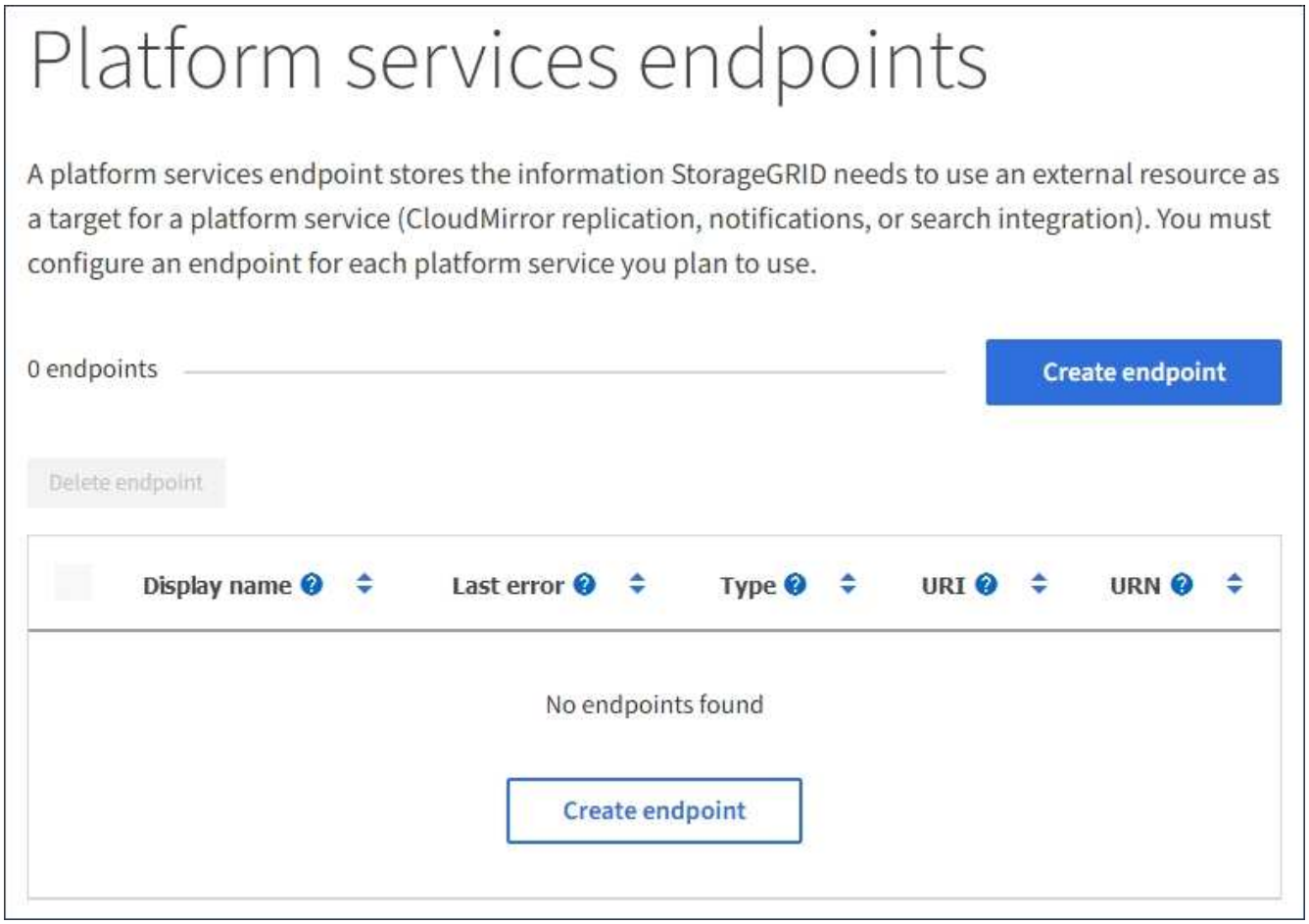
    "Festlegen des URN für einen Endpunkt der Plattformdienste"

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

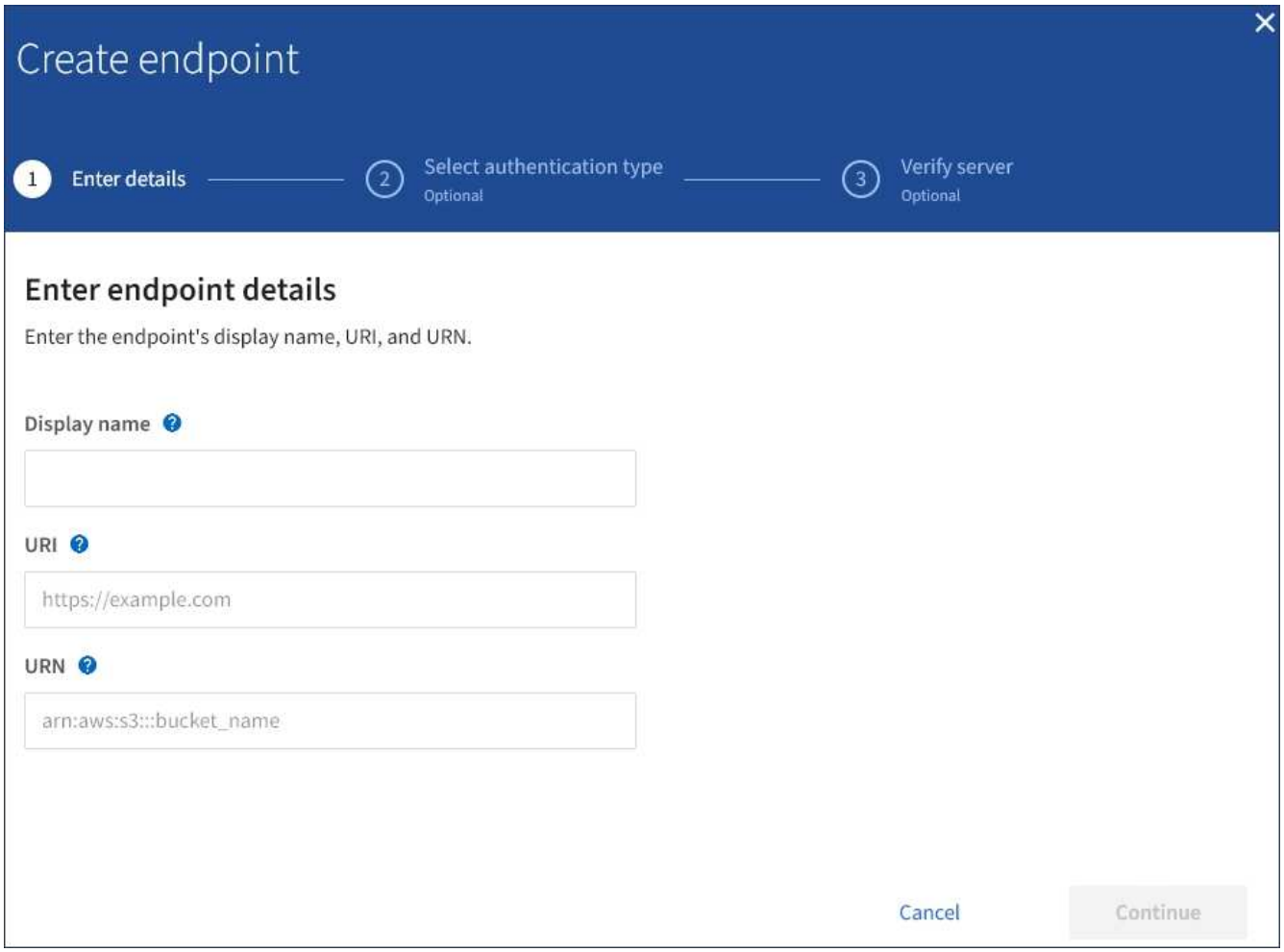
Schritte

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

   Die Seite „Endpunkte der Plattformdienste“ wird angezeigt.



2. Wählen Sie **Endpunkt erstellen**.



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

   Der vom Endpunkt unterstützte Plattformdienst 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,:

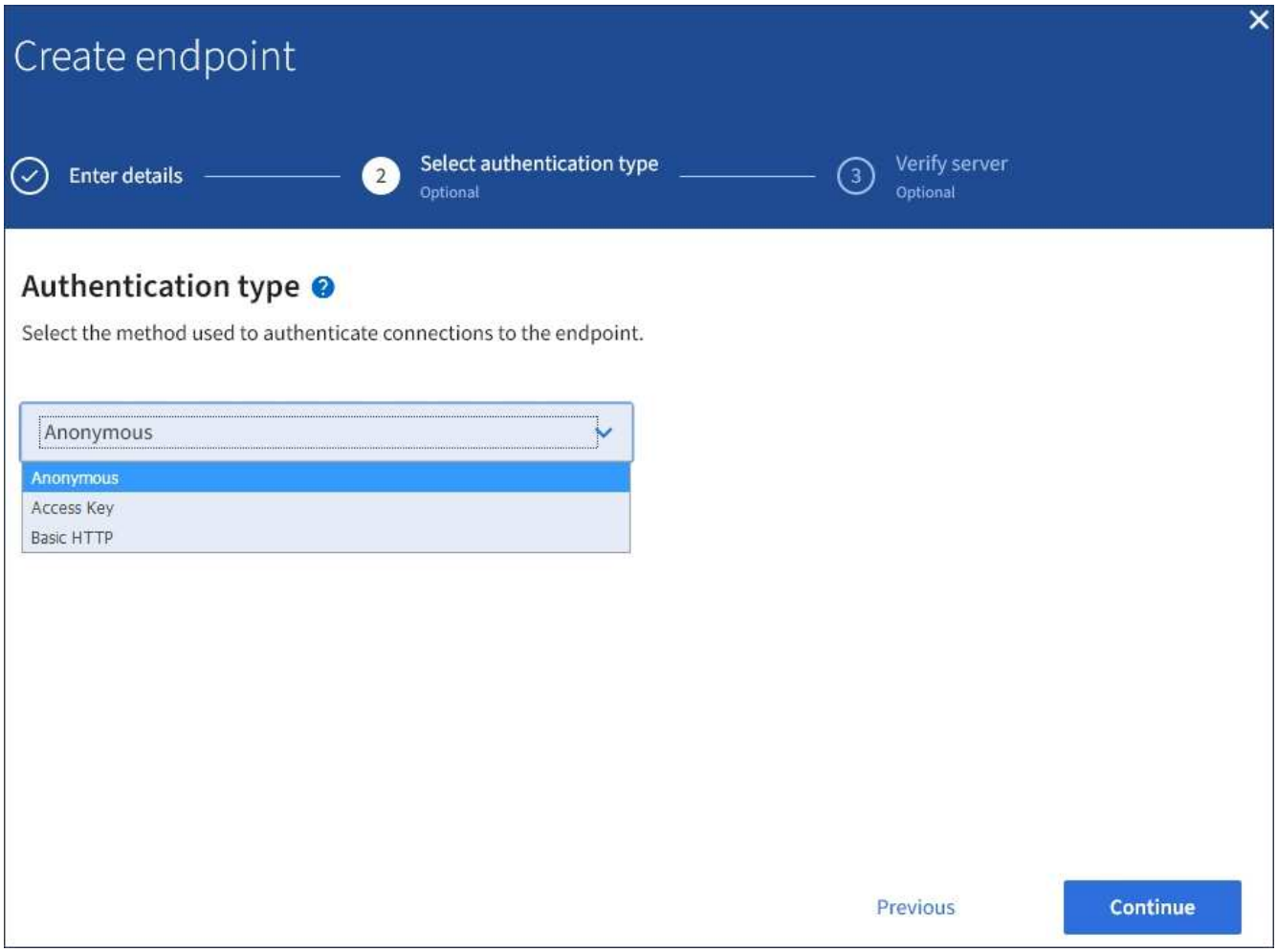
```
https://s3-aws-region.amazonaws.com
```

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.

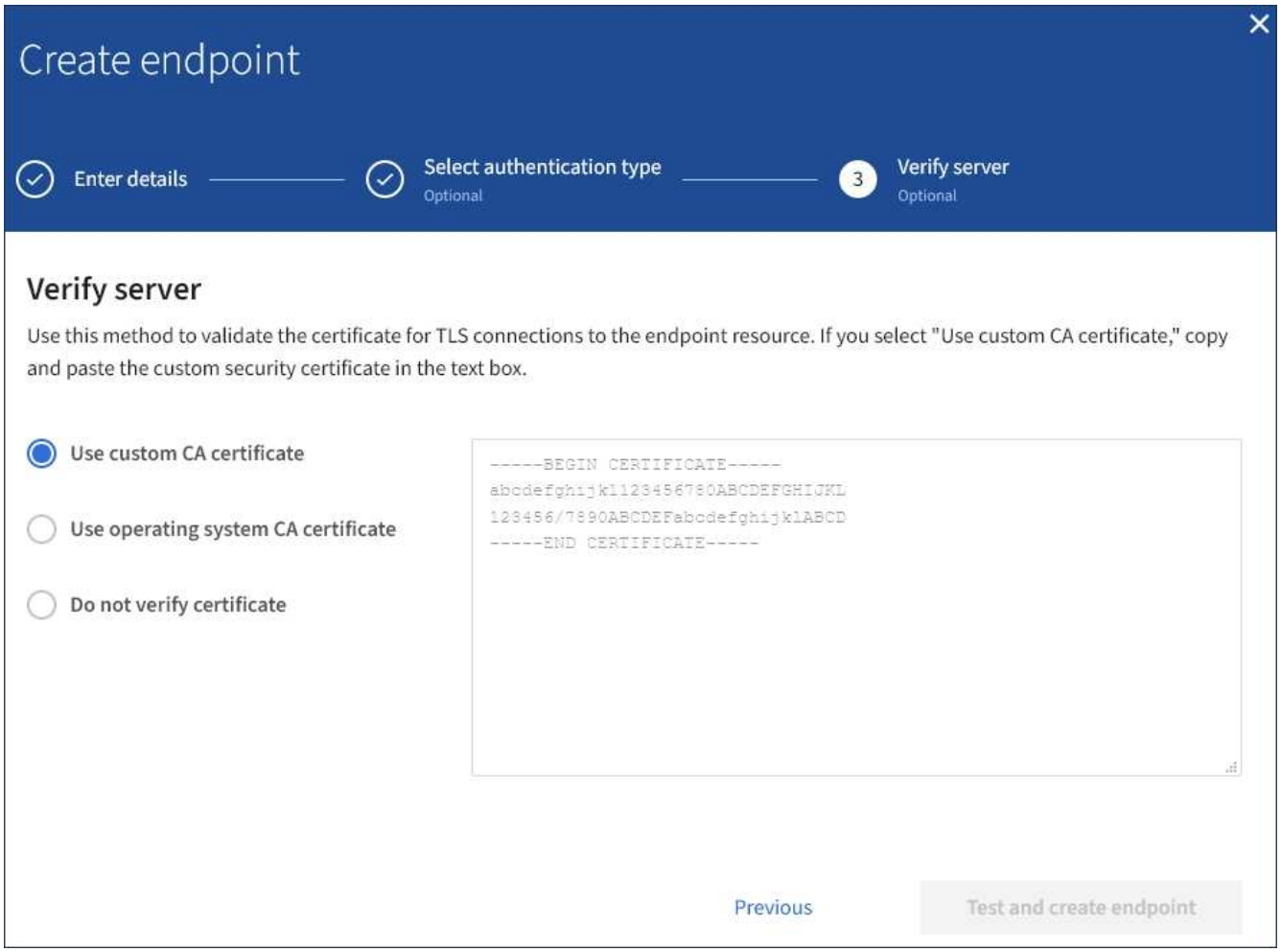
6. Wählen Sie **Weiter**.
7. Wählen Sie einen Wert für **Authentifizierungstyp** aus, und geben Sie dann die erforderlichen Anmeldedaten ein.



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

Authentifizierungstyp	Beschreibung	Anmeldedaten
Anonym	Gibt anonymen Zugriff auf das Ziel. Funktioniert nur für Endpunkte, bei denen die Sicherheit deaktiviert ist.	Keine Authentifizierung.
Zugriffsschlüssel	Verwendet AWS Zugangsdaten für die Authentifizierung von Verbindungen mit dem Ziel	• Zugriffsschlüssel-ID • Geheimer Zugriffsschlüssel
Basis-HTTP	Verwendet einen Benutzernamen und ein Passwort, um Verbindungen zum Ziel zu authentifizieren.	• 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.



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.

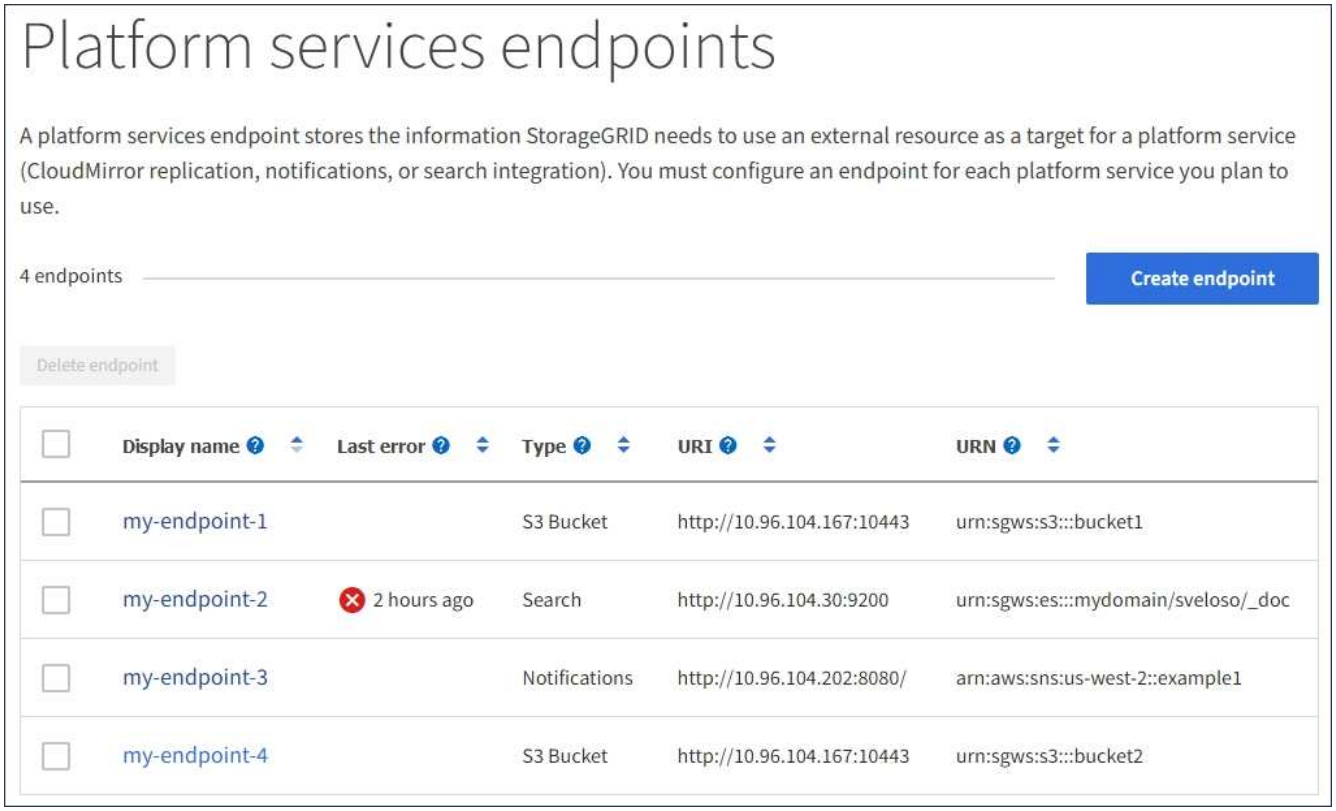
Über diese Aufgabe

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

Schritte

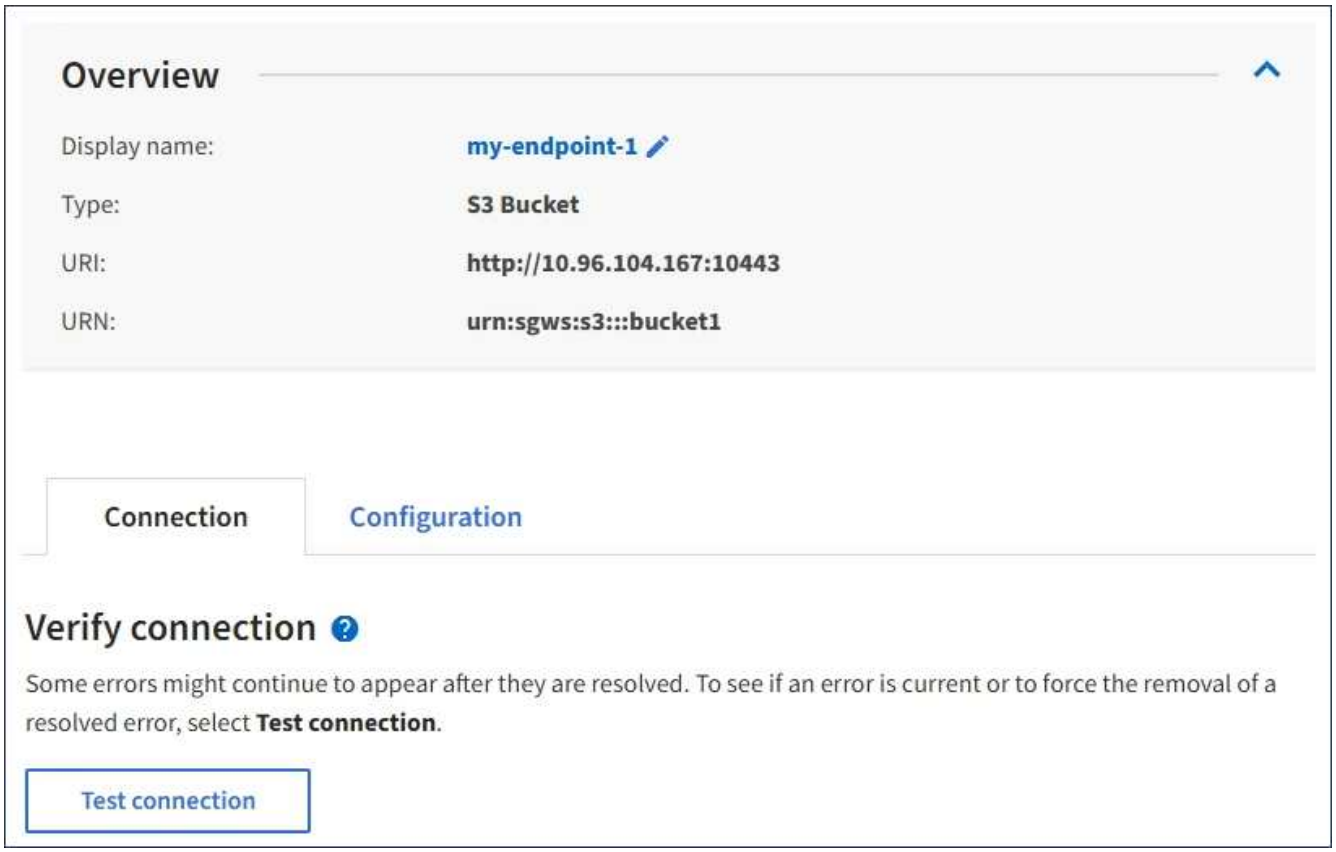
1. Wählen Sie **STORAGE (S3)** > **Plattform-Services-Endpunkte** aus.

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



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

   Die Seite mit den Details des Endpunkts wird angezeigt.



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

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.

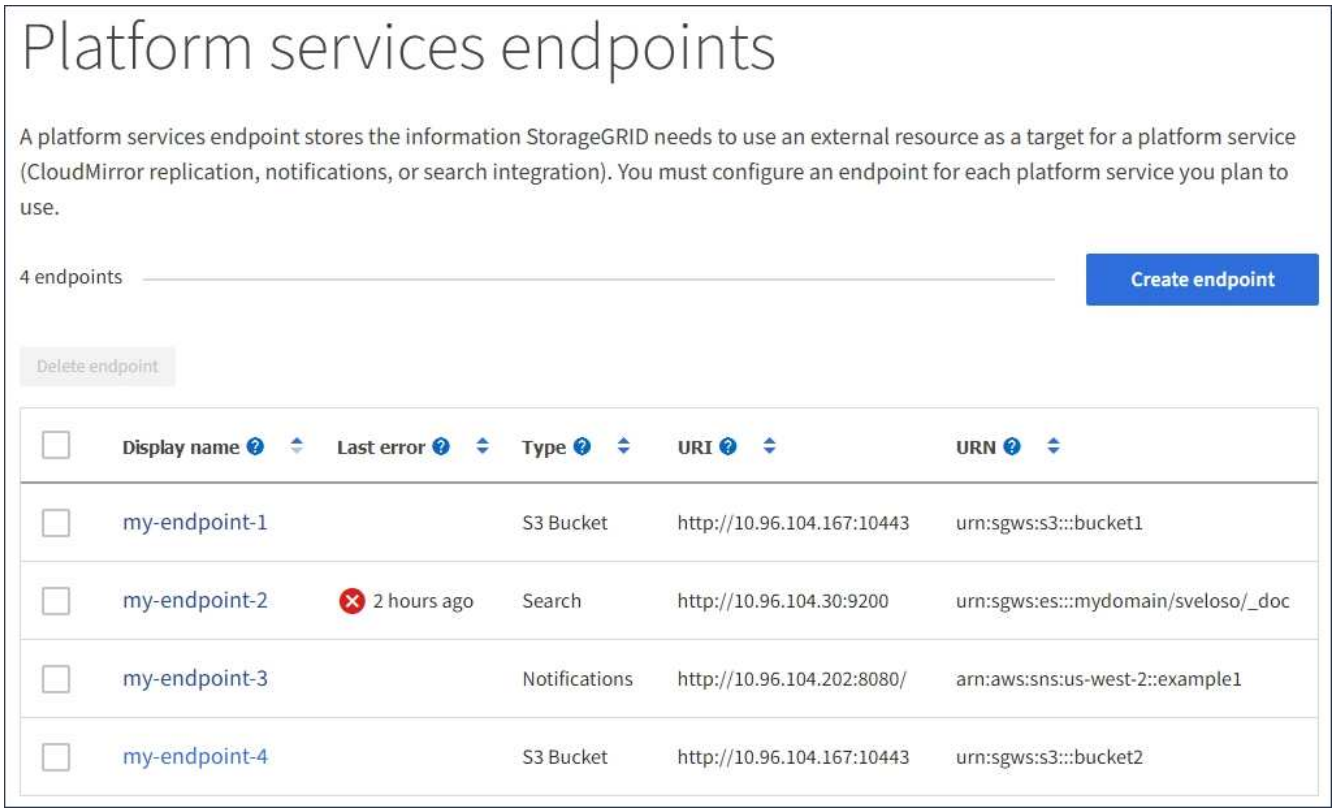
Was Sie benötigen

- 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.

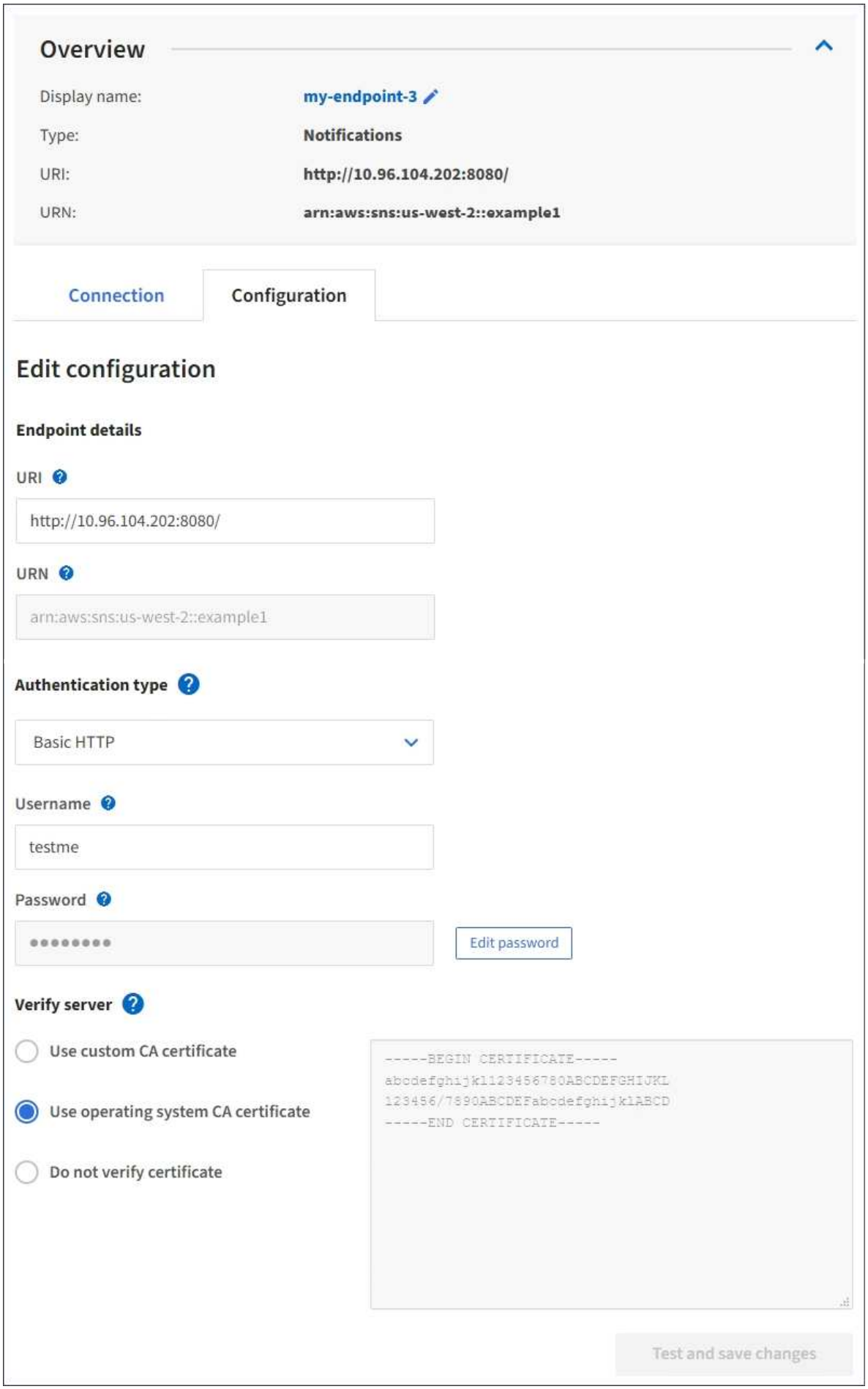
   Die Seite Endpunkte der Plattformservices wird angezeigt und zeigt die Liste der bereits konfigurierten Endpunkte der Plattformservices an.



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-----
abcdefghijkl123456780ABCDEFGHIJKL
123456/7890ABCDEFabcdefghijklABCD
-----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 Plattformdienst nicht mehr verwenden möchten.

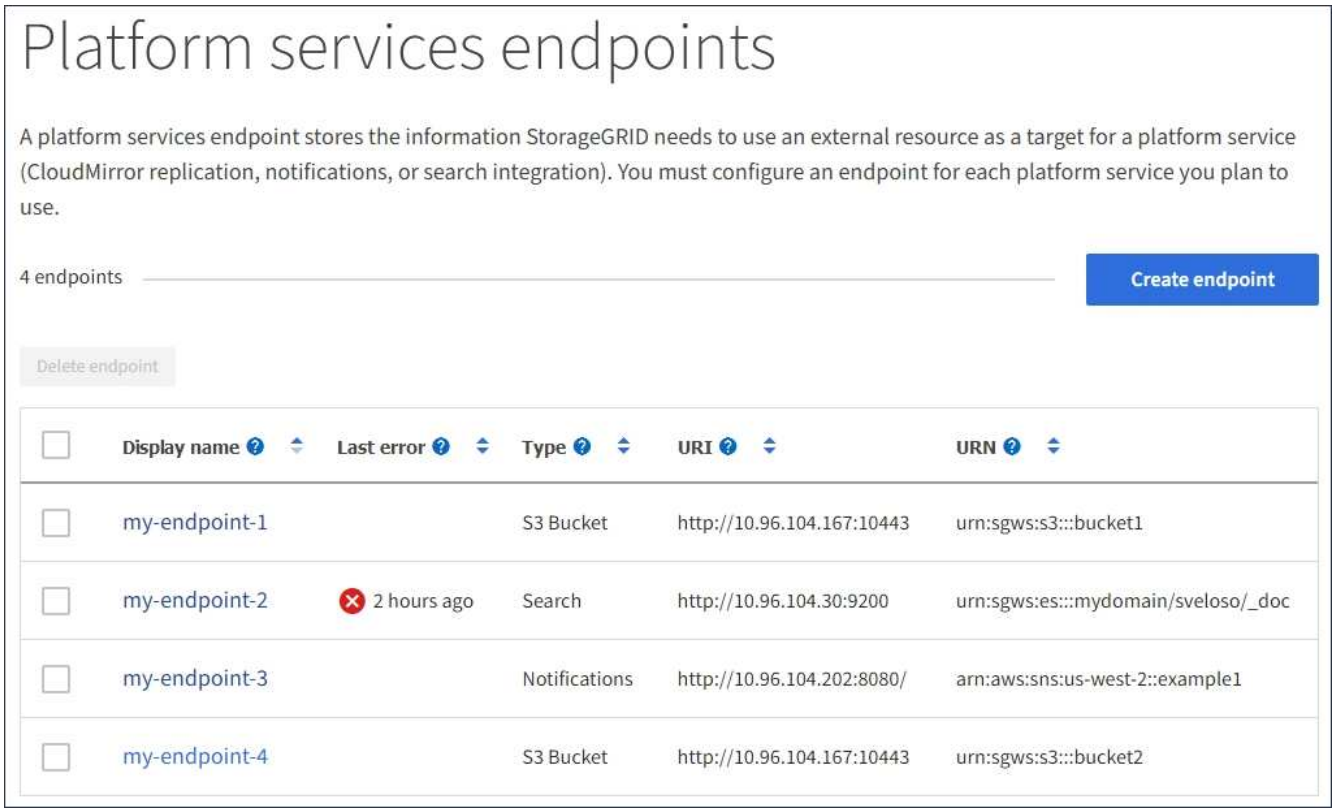
Was Sie benötigen

- 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.

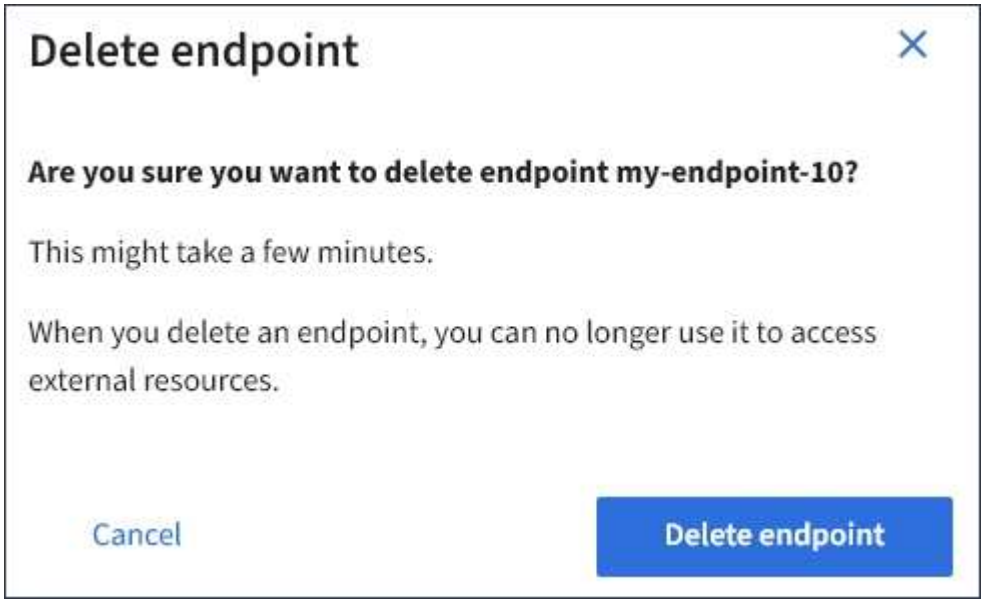


2. Aktivieren Sie das Kontrollkästchen für jeden zu löschenden Endpunkt.

> 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.



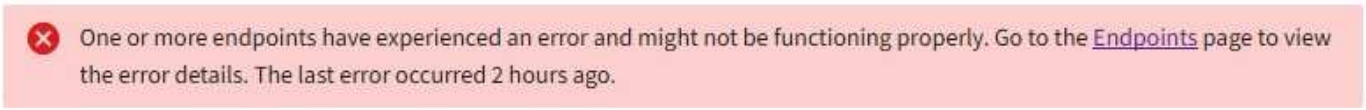
4. Wählen Sie **Endpunkt löschen**.

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

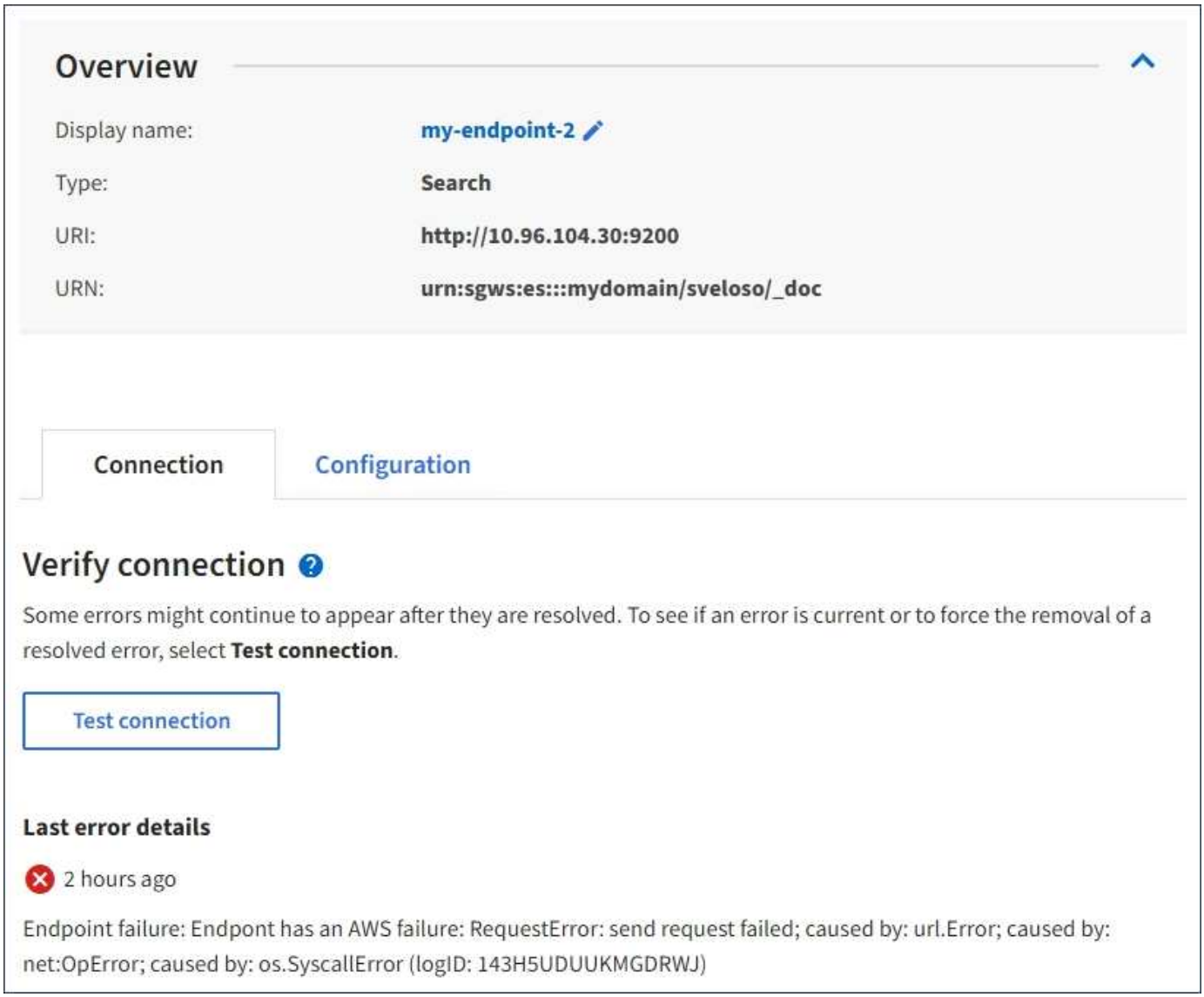
Wenn in den letzten 7 Tagen Endpoint-Fehler bei Plattformservices aufgetreten sind, zeigt das Tenant Manager Dashboard eine Warnmeldung an. Auf der Seite Plattform-Services-Endpunkte finden Sie weitere Details zum Fehler.



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.



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 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 Plattformdienst 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 Zielsystemanbieter.

Schritte

1. Replizierung für Ihren Quell-Bucket aktivieren:

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

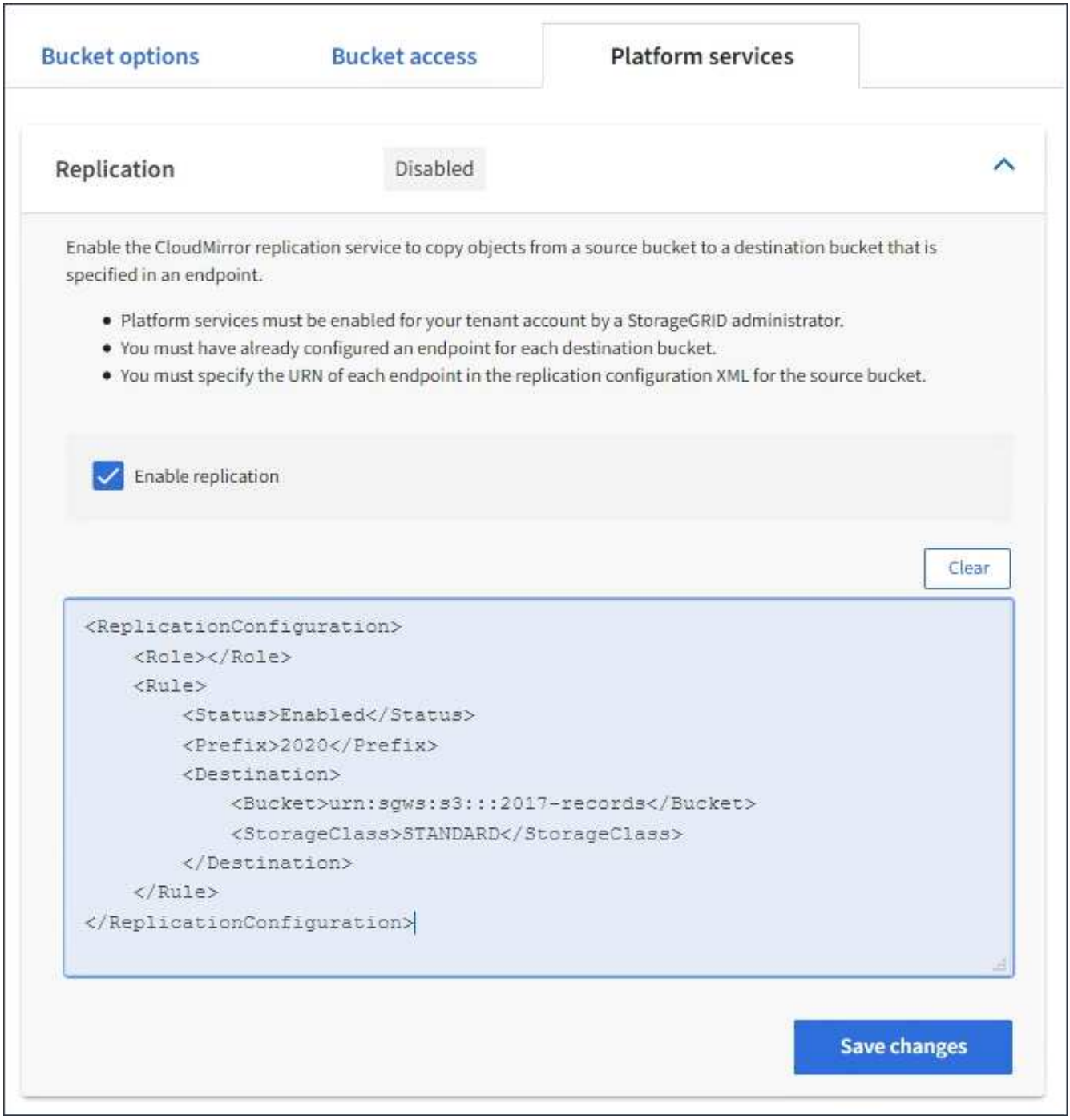
   - Beachten Sie, dass StorageGRID nur V1 der Replizierungskonfiguration unterstützt. Das bedeutet, dass StorageGRID die Verwendung von nicht unterstützt `Filter` Element für Regeln und folgt V1-Konventionen zum Löschen von Objektversionen. Details finden Sie in der Amazon Dokumentation zur Replizierungskonfiguration.
   - 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**.



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

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

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

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

Bei kleinen Objekten wird die Replizierung schnell durchgeführt.

Verwandte Informationen

"Allgemeines zum CloudMirror Replikationsservice"

"S3 verwenden"

"Erstellen eines Endpunkts für Plattformservices"

Ereignisbenachrichtigungen werden konfiguriert

Der Benachrichtigungsservice ist einer der drei StorageGRID-Plattformdienste. 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-Manager.

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

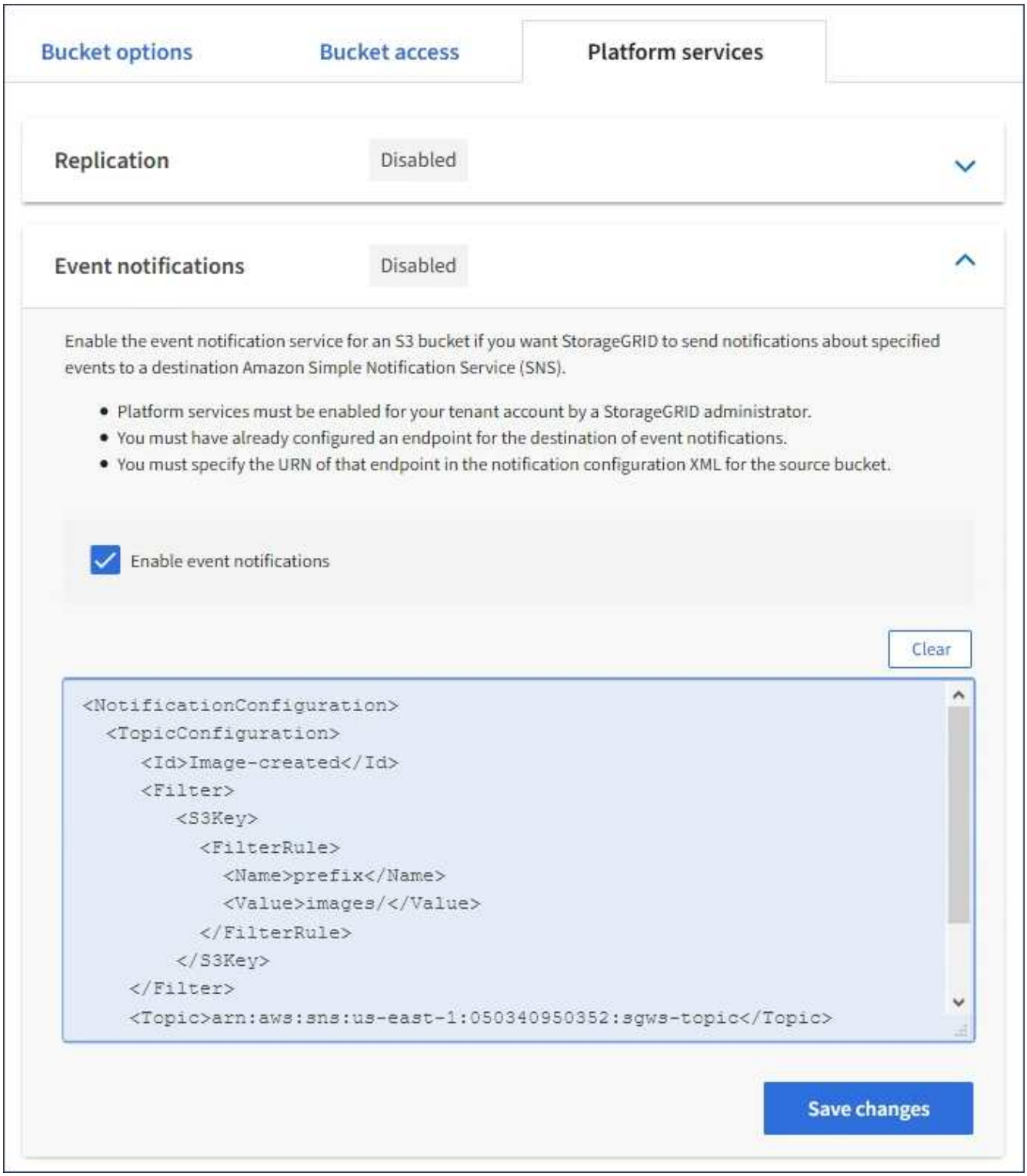
1. Benachrichtigungen für Ihren Quell-Bucket aktivieren:
    - Verwenden Sie einen Texteditor, um die XML-Benachrichtigungskonfiguration zu erstellen, die für die Aktivierung von Ereignisbenachrichtigungen erforderlich ist, wie in der S3-Benachrichtigungs-API angegeben.
    - Verwenden Sie bei der XML-Konfiguration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



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

7. Überprüfen Sie, ob Ereignisbenachrichtigungen richtig konfiguriert sind:

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

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

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

Verwandte Informationen

"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 Suchintegrationsservice"

"S3 verwenden"

Konfigurations-XML für die Integration der Suche

Der Such-Integrationsservice 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 senden `/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 enthält `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 Regelelement.	Ja.
Regel	Container-Tag für eine Regel, die die Objekte identifiziert, deren Metadaten zu einem bestimmten Index hinzugefügt werden sollen. Regeln mit überlappenden Präfixen werden abgelehnt. Im MetadataNotificationConfiguration Element enthalten.	Ja.
ID	Eindeutige Kennung für die Regel. In das Element Regel aufgenommen.	Nein

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

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-1:3333333:domain/es-
domain/graphics/imagetype</Urn>
        </Destination>
    </Rule>
    <Rule>
        <ID>Videos-rule</ID>
        <Status>Enabled</Status>
        <Prefix>/videos</Prefix>
        <Destination>
           <Urn>arn:aws:es:us-west-1:22222222:domain/es-
domain/graphics/videotype</Urn>
        </Destination>
    </Rule>
</MetadataNotificationConfiguration>
```

Verwandte Informationen

"S3 verwenden"

"Vom Suchintegrations-Service generierter JSON"

"Konfigurieren des Suchintegrationsservice"

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-Integrationsservice für einen Quell-Bucket konfiguriert haben, werden beim Erstellen eines Objekts oder beim Aktualisieren der Metadaten oder Tags eines Objekts Objektmetadaten ausgelöst, die an den Ziel-Endpunkt gesendet werden. Wenn Sie den Such-Integrationsservice 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

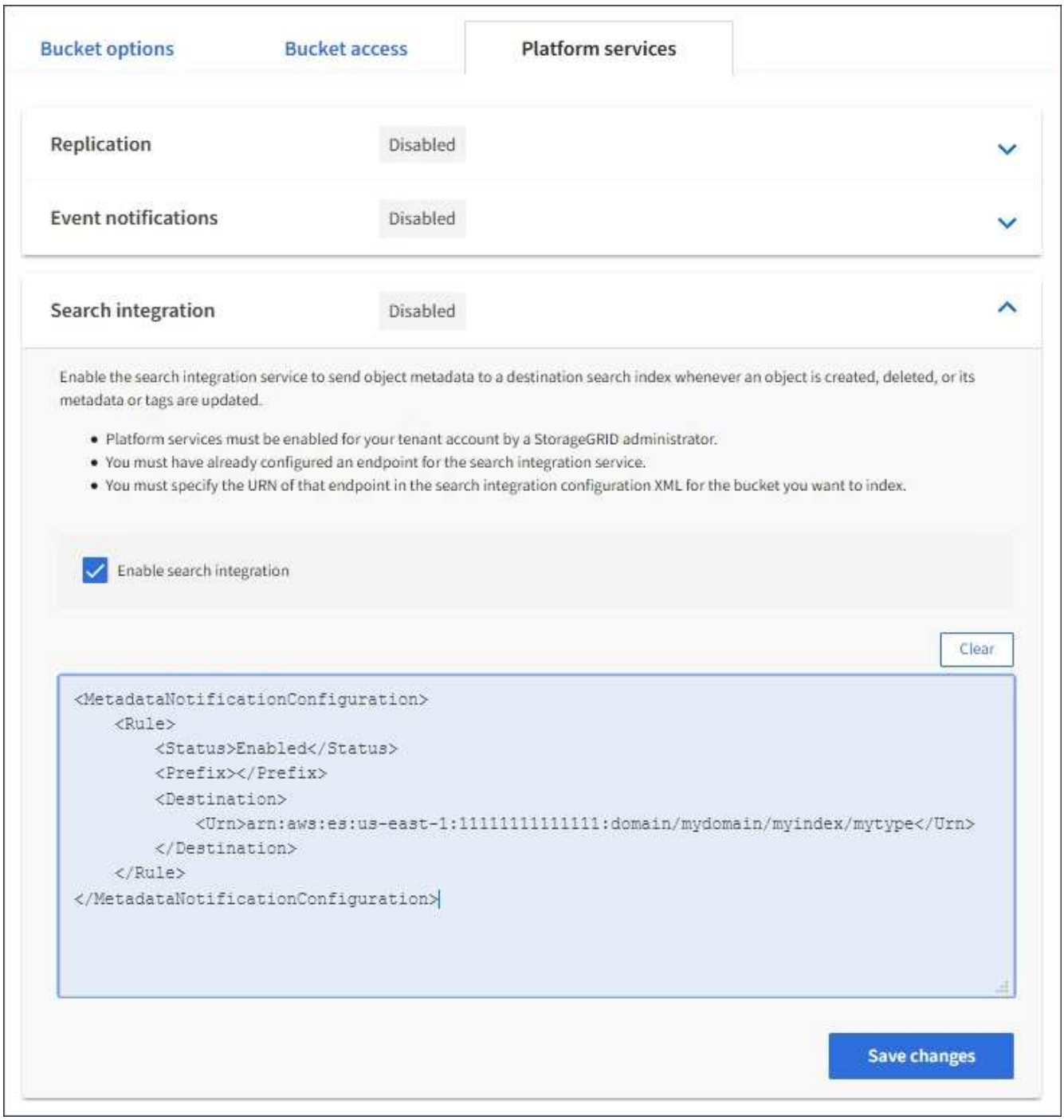
1. Verwenden Sie einen Texteditor, um die XML-XML-Metadatenbenachrichtigung zu erstellen, die für die Integration der Suche erforderlich ist.
   - Informationen zur Integration der Suchfunktion finden Sie in den XML-Konfigurationsdaten.
   - Verwenden Sie beim Konfigurieren des XML den URN eines Endpunkt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

```
<MetadataNotificationConfiguration>
 <Rule>
    <Status>Enabled</Status>
    <Prefix></Prefix>
    <Destination>
       <Urn>arn:aws:es:us-east-
1:11111111111111: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**.



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

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

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

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

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

Nachdem Sie fertig sind

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

- Wählen Sie **STORAGE (S3)** > **Buckets** 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 Suchintegrationsservice"

"Konfigurations-XML für die Integration der Suche"

"S3 verwenden"

"Erstellen eines Endpunkts für Plattformservices"

Vom Suchintegrations-Service generierter JSON

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

Dieses Beispiel zeigt ein Beispiel für den JSON, der generiert werden 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.

S3 verwenden

Lesen Sie, wie Client-Applikationen die S3-API für die Schnittstelle mit dem StorageGRID-System nutzen.

- "Unterstützung für die S3-REST-API"
- "Mandantenkonten und -Verbindungen werden konfiguriert"
- "So implementiert StorageGRID die S3-REST-API"
- "Unterstützte Vorgänge und Einschränkungen durch S3-REST-API"
- "StorageGRID S3 REST-API-Operationen"
- "Bucket- und Gruppenzugriffsrichtlinien"
- "Sicherheit wird für DIE REST API konfiguriert"
- "Monitoring und Auditing von Vorgängen"
- "Vorteile von aktiven, inaktiven und gleichzeitigen HTTP-Verbindungen"

Unterstützung für die S3-REST-API

StorageGRID unterstützt die S3-API (Simple Storage Service), die als Satz Rest-Web-Services (Representational State Transfer) implementiert wird. Dank der Unterstützung der S3-REST-API können serviceorientierte Applikationen, die für S3-Webservices entwickelt wurden, mit On-Premises-Objekt-Storage über das StorageGRID System verbunden werden. Hierfür sind nur minimale Änderungen an der aktuellen Nutzung von S3-REST-API-Aufrufen einer Client-Applikation erforderlich.

- "Änderungen an der Unterstützung für die S3-REST-API"
- "Unterstützte Versionen"
- "Unterstützung von StorageGRID Plattform-Services"

Änderungen an der Unterstützung für die S3-REST-API

Bei Änderungen an der Unterstützung des StorageGRID-Systems für die S3-REST-API sollten Sie auf sich aufmerksam machen.

Freigabe	Kommentare
11.5	• Zusätzliche Unterstützung für das Management der Bucket-Verschlüsselung • Unterstützung für S3 Object Lock und veraltete ältere Compliance-Anforderungen wurde hinzugefügt. • Zusätzliche Unterstützung beim LÖSCHEN mehrerer Objekte in versionierten Buckets. • Der `Content-MD5` Die Anforderungsüberschrift wird jetzt korrekt unterstützt.
11.4	• Unterstützung für DELETE Bucket-Tagging, GET Bucket-Tagging und PUT Bucket-Tagging. Kostenzuordnungs-Tags werden nicht unterstützt. • Bei in StorageGRID 11.4 erstellten Buckets ist keine Beschränkung der Objektschlüsselnamen auf Performance-Best-Practices mehr erforderlich. • Zusätzliche Unterstützung für Bucket-Benachrichtigungen auf der `s3:ObjectRestore:Post` Ereignistyp. • Die Größenbeschränkungen von AWS für mehrere Teile werden nun durchgesetzt. Jedes Teil eines mehrteiligen Uploads muss zwischen 5 MiB und 5 gib liegen. Der letzte Teil kann kleiner als 5 MiB sein. • Zusätzliche Unterstützung für TLS 1.3 und aktualisierte Liste der unterstützten TLS-Chiffre-Suites. • Der CLB-Service ist veraltet.
11.3	• Zusätzliche Unterstützung für serverseitige Verschlüsselung von Objektdaten mit vom Kunden bereitgestellten Schlüsseln (SSE-C). • Unterstützung für VORGÄNGE IM Bucket-Lebenszyklus (nur Aktion „Ablauf“) und für den wurde hinzugefügt `x-amz-expiration` Kopfzeile der Antwort. • Aktualisiertes PUT-Objekt, PUT-Objekt – Copy und Multipart-Upload, um die Auswirkungen von ILM-Regeln zu beschreiben, die synchrone Platzierung bei der Aufnahme verwenden. • Aktualisierte Liste der unterstützten TLS-Cipher-Suites. TLS 1.1-Chiffren werden nicht mehr unterstützt.

Freigabe	Kommentare
11.2	Unterstützung für DIE WIEDERHERSTELLUNG NACH Objekten wurde hinzugefügt und kann in Cloud-Storage-Pools verwendet werden. Unterstützung für die Verwendung der AWS-Syntax für ARN, Richtlinienzustandsschlüssel und Richtlinienvariablen in Gruppen- und Bucket-Richtlinien Vorhandene Gruppen- und Bucket-Richtlinien, die die StorageGRID-Syntax verwenden, werden weiterhin unterstützt. **Hinweis:** die Verwendung von ARN/URN in anderen Konfigurationen JSON/XML, einschließlich derjenigen, die in benutzerdefinierten StorageGRID-Funktionen verwendet werden, hat sich nicht geändert.
11.1	Zusätzliche Unterstützung für Cross-Origin Resource Sharing (CORS), HTTP für S3-Client-Verbindungen zu Grid-Nodes und Compliance-Einstellungen für Buckets.
11.0	Unterstützung für die Konfiguration von Plattform-Services (CloudMirror Replizierung, Benachrichtigungen und Elasticsearch-Integration) für Buckets. Außerdem werden Einschränkungen für Objektkennzeichnung bei Buckets sowie die verfügbaren Einstellungen für die Konsistenzsteuerung unterstützt.
10.4	Unterstützung für ILM-Scanning-Änderungen an Versionierung, Seitenaktualisierungen von Endpoint Domain-Namen, Bedingungen und Variablen in Richtlinien, Richtlinienbeispiele und die Berechtigung PutOverwriteObject.
10.3	Zusätzliche Unterstützung für Versionierung
10.2	Unterstützung für Gruppen- und Bucket-Zugriffsrichtlinien und für mehrteilige Kopien (Upload Part - Copy) hinzugefügt
10.1	Unterstützung für mehrteilige Uploads, virtuelle Hosted-Style-Anforderungen und v4 Authentifizierung
10.0	Die erste Unterstützung der S3-REST-API durch das StorageGRID-System.die derzeit unterstützte Version der *Simple Storage Service API Reference* lautet 2006-03-01.

Unterstützte Versionen

StorageGRID unterstützt die folgenden spezifischen Versionen von S3 und HTTP.

Element	Version
S3-Spezifikation	*Simple Storage Service API Reference* 2006-03-01
HTTP	1.1 Weitere Informationen zu HTTP finden Sie unter HTTP/1.1 (RFCs 7230-35). **Hinweis**: StorageGRID unterstützt HTTP/1.1-Pipelining nicht.

Verwandte Informationen

"IETF RFC 2616: Hypertext Transfer Protocol (HTTP/1.1)"

"Amazon Web Services (AWS) Dokumentation: Amazon Simple Storage Service API Reference"

Unterstützung von StorageGRID Plattform-Services

Mithilfe der StorageGRID Plattform-Services können StorageGRID-Mandantenkonten externe Services wie einen Remote-S3-Bucket, einen SNS-Endpunkt (Simple Notification Service) oder ein Elasticsearch-Cluster verwenden, um die Services eines Grids zu erweitern.

In der folgenden Tabelle sind die verfügbaren Plattform-Services und die zur Konfiguration verwendeten S3-APIs zusammengefasst.

Plattform-Service	Zweck	Zum Konfigurieren des Service wird die S3-API verwendet
Replizierung von CloudMirror	Repliziert Objekte aus einem StorageGRID-Quell-Bucket in den konfigurierten Remote-S3-Bucket	PUT Bucket-Replizierung
Benachrichtigungen	Sendet Benachrichtigungen zu Ereignissen in einem StorageGRID-Quell-Bucket an einen konfigurierten SNS-Endpunkt (Simple Notification Service).	PUT Bucket-Benachrichtigung
Integration von Suchen	Sendet Objektmetadaten für Objekte, die in einem StorageGRID Bucket gespeichert sind, an einen konfigurierten Elasticsearch-Index.	PUT Bucket-Metadaten-Benachrichtigung **Hinweis:** Dies ist ein StorageGRID Custom S3 API.

Ein Grid-Administrator muss die Nutzung von Plattformservices für ein Mandantenkonto aktivieren, bevor sie

verwendet werden können. Anschließend muss ein Mandantenadministrator einen Endpunkt erstellen, der für den Remote-Service im Mandantenkonto steht. Dieser Schritt ist erforderlich, bevor ein Service konfiguriert werden kann.

Empfehlungen für die Nutzung von Plattform-Services

Vor der Verwendung von Plattform-Services müssen Sie die folgenden Empfehlungen beachten:

- NetApp empfiehlt, nicht mehr als 100 aktive Mandanten mit S3-Anforderungen zu zulassen, die eine CloudMirror-Replizierung, Benachrichtigungen und Suchintegration erfordern. Mehr als 100 aktive Mandanten können zu einer langsameren S3-Client-Performance führen.
- Wenn bei einem S3-Bucket im StorageGRID System sowohl die Versionierung als auch die CloudMirror-Replizierung aktiviert sind, empfiehlt NetApp, dass auf dem Zielendpunkt auch die S3-Bucket-Versionierung aktiviert ist. So kann die CloudMirror-Replizierung ähnliche Objektversionen auf dem Endpunkt generieren.
- Die CloudMirror-Replizierung wird nicht unterstützt, wenn im Quell-Bucket S3-Objektsperre aktiviert ist.
- Die CloudMirror-Replikation schlägt mit einem AccessDenied-Fehler fehl, wenn auf dem Ziel-Bucket ältere Compliance-Funktionen aktiviert sind.

Verwandte Informationen

"Verwenden Sie ein Mandantenkonto"

"StorageGRID verwalten"

"Operationen auf Buckets"

"PUT Anforderung der Bucket-Metadaten-Benachrichtigung"

Mandantenkonten und -Verbindungen werden konfiguriert

Wenn StorageGRID konfiguriert wird, um Verbindungen von Client-Applikationen zu akzeptieren, müssen ein oder mehrere Mandantenkonten erstellt und die Verbindungen eingerichtet werden.

Erstellen und Konfigurieren von S3-Mandantenkonten

Bevor S3-API-Clients Objekte auf StorageGRID speichern und abrufen können, ist ein S3-Mandantenkonto erforderlich. Jedes Mandantenkonto hat seine eigene Konto-ID, Gruppen und Benutzer sowie Container und Objekte.

S3-Mandantenkonten werden von einem StorageGRID Grid-Administrator erstellt, der den Grid Manager oder die Grid Management API verwendet. Beim Erstellen eines S3-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 Plattform-Services nutzen darf. Wenn die Nutzung von Plattformdiensten 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.

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

- Richten Sie einen Identitätsverbund ein (es sei denn, die Identitätsquelle wird gemeinsam mit dem Grid verwendet), und erstellen Sie lokale Gruppen und Benutzer
- Managen von S3-Zugriffsschlüsseln
- Erstellung und Management von S3-Buckets, einschließlich Buckets, für die S3-Objektsperre aktiviert ist
- Verwenden von Plattform-Services (falls aktiviert)
- Monitoring der Storage-Auslastung

> Benutzer von S3-Mandanten können mit Mandanten-Manager S3-Buckets erstellen und managen. Dafür sind jedoch S3-Zugriffsschlüssel sowie die S3-REST-API erforderlich, um Objekte aufzunehmen und zu managen.

Verwandte Informationen

"StorageGRID verwalten"

"Verwenden Sie ein Mandantenkonto"

Wie Client-Verbindungen konfiguriert werden können

Ein Grid-Administrator trifft Konfigurationsmöglichkeiten, die Einfluss darauf haben, wie S3-Clients sich mit StorageGRID verbinden, um Daten zu speichern und abzurufen. Die spezifischen Informationen, die benötigt werden, um eine Verbindung herzustellen, hängen von der gewählten Konfiguration ab.

Client-Applikationen können Objekte speichern oder abrufen, indem sie eine Verbindung mit folgenden Komponenten herstellen:

- Der Lastverteilungsservice an Admin-Nodes oder Gateway-Nodes oder optional die virtuelle IP-Adresse einer HA-Gruppe (High Availability, Hochverfügbarkeit) von Admin-Nodes oder Gateway-Nodes
- Der CLB-Dienst auf Gateway-Knoten oder optional die virtuelle IP-Adresse einer Hochverfügbarkeitsgruppe von Gateway-Knoten

> Der CLB-Service ist veraltet. Clients, die vor der Version StorageGRID 11.3 konfiguriert wurden, können den CLB-Service auf Gateway-Knoten weiterhin verwenden. Alle anderen Client-Applikationen, die zum Lastausgleich vom StorageGRID abhängig sind, sollten über den Load Balancer Service eine Verbindung herstellen.

- Storage-Nodes mit oder ohne externen Load Balancer

Bei der Konfiguration von StorageGRID kann ein Grid-Administrator den Grid-Manager oder die Grid-Management-API verwenden, um die folgenden Schritte auszuführen, die alle optional sind:

1. Konfigurieren von Endpunkten für den Load Balancer Service.

Sie müssen Endpunkte konfigurieren, um den Load Balancer Service verwenden zu können. Der Lastverteilungsservice an Admin-Nodes oder Gateway-Nodes verteilt eingehende Netzwerkverbindungen von Client-Anwendungen auf Storage-Nodes. Beim Erstellen eines Load Balancer-Endpunkts gibt der StorageGRID-Administrator eine Portnummer an, ob der Endpunkt HTTP- oder HTTPS-Verbindungen akzeptiert, der Client-Typ (S3 oder Swift), der den Endpunkt verwendet, und das für HTTPS-Verbindungen zu verwendende Zertifikat (falls zutreffend).

2. Konfigurieren Sie Nicht Vertrauenswürdige Client-Netzwerke.

   Wenn ein StorageGRID-Administrator das Clientnetzwerk eines Node so konfiguriert, dass es nicht vertrauenswürdig ist, akzeptiert der Knoten nur eingehende Verbindungen im Clientnetzwerk an Ports, die explizit als Load Balancer-Endpunkte konfiguriert sind.

3. Konfigurieren Sie Hochverfügbarkeitsgruppen.

   Wenn ein Administrator eine HA-Gruppe erstellt, werden die Netzwerkschnittstellen mehrerer Admin-Nodes oder Gateway-Nodes in einer aktiv-Backup-Konfiguration platziert. Client-Verbindungen werden mithilfe der virtuellen IP-Adresse der HA-Gruppe hergestellt.

Weitere Informationen zu den einzelnen Optionen finden Sie in den Anweisungen zur Administration von StorageGRID.

Verwandte Informationen

"StorageGRID verwalten"

Zusammenfassung: IP-Adressen und Ports für Client-Verbindungen

Client-Applikationen stellen mithilfe der IP-Adresse eines Grid-Node und der Port-Nummer eines Service auf diesem Node eine Verbindung zu StorageGRID her. Bei Konfiguration von Hochverfügbarkeitsgruppen (High Availability, HA) können Client-Applikationen eine Verbindung über die virtuelle IP-Adresse der HA-Gruppe herstellen.

Zum Erstellen von Client-Verbindungen erforderliche Informationen

Die Tabelle fasst die verschiedenen Möglichkeiten zusammen, wie Clients eine Verbindung zu StorageGRID sowie zu den für die einzelnen Verbindungstypen verwendeten IP-Adressen und Ports herstellen können. Wenden Sie sich an Ihren StorageGRID-Administrator, um weitere Informationen zu erhalten, oder lesen Sie die Anweisungen zur Administration von StorageGRID, um eine Beschreibung der Informationen im Grid-Manager zu erhalten.

Wo eine Verbindung hergestellt wird	Dienst, mit dem der Client verbunden ist	IP-Adresse	Port
HA-Gruppe	Lastausgleich	Virtuelle IP-Adresse einer HA-Gruppe	• Endpunkt-Port des Load Balancer
HA-Gruppe	CLB **Hinweis:** der CLB-Service ist veraltet.	Virtuelle IP-Adresse einer HA-Gruppe	S3-Standard-Ports: • HTTPS: 8082 • HTTP: 8084

Wo eine Verbindung hergestellt wird	Dienst, mit dem der Client verbunden ist	IP-Adresse	Port
Admin-Node	Lastausgleich	IP-Adresse des Admin-Knotens	• Endpunkt-Port des Load Balancer
Gateway-Node	Lastausgleich	IP-Adresse des Gateway-Node	• Endpunkt-Port des Load Balancer
Gateway-Node	CLB **Hinweis:** der CLB-Service ist veraltet.	IP-Adresse des Gateway-Node **Hinweis:** standardmäßig sind HTTP-Ports für CLB und LDR nicht aktiviert.	S3-Standard-Ports: • HTTPS: 8082 • HTTP: 8084
Storage-Node	LDR	IP-Adresse des Speicherknoten	S3-Standard-Ports: • HTTPS: 18082 • HTTP: 18084

Beispiel

Verwenden Sie eine strukturierte URL, wie unten gezeigt, um einen S3-Client mit dem Load Balancer-Endpunkt einer HA-Gruppe von Gateway-Nodes zu verbinden:

- `https://VIP-of-HA-group:_LB-endpoint-port_`

Wenn beispielsweise die virtuelle IP-Adresse der HA-Gruppe 192.0.2.5 lautet und die Portnummer eines S3 Load Balancer Endpunkts 10443 ist, kann ein S3-Client die folgende URL zur Verbindung mit StorageGRID verwenden:

- `https://192.0.2.5:10443`

Ein DNS-Name kann für die IP-Adresse konfiguriert werden, die Clients zum Herstellen der Verbindung mit StorageGRID verwenden. Wenden Sie sich an Ihren Netzwerkadministrator vor Ort.

Verwandte Informationen

"StorageGRID verwalten"

Entscheidung über die Verwendung von HTTPS- oder HTTP-Verbindungen

Wenn Client-Verbindungen mit einem Load Balancer-Endpunkt hergestellt werden, müssen Verbindungen über das Protokoll (HTTP oder HTTPS) hergestellt werden, das für diesen Endpunkt angegeben wurde. Um HTTP für Client-Verbindungen zu Storage-Nodes oder zum CLB-Dienst auf Gateway-Knoten zu verwenden, müssen Sie dessen Verwendung aktivieren.

Wenn Client-Anwendungen eine Verbindung zu Speicherknoten oder zum CLB-Dienst auf Gateway-Knoten herstellen, müssen sie für alle Verbindungen verschlüsseltes HTTPS verwenden. Optional können Sie weniger sichere HTTP-Verbindungen aktivieren, indem Sie im Grid Manager die Option **HTTP-Verbindung** aktivieren auswählen. Eine Client-Anwendung kann beispielsweise HTTP verwenden, wenn die Verbindung zu einem Speicherknoten in einer nicht produktiven Umgebung getestet wird.

Achten Sie bei der Aktivierung von HTTP für ein Produktionsraster darauf, dass die Anforderungen unverschlüsselt gesendet werden.

Der CLB-Service ist veraltet.

Wenn die Option **HTTP-Verbindung aktivieren** ausgewählt ist, müssen Clients für HTTP unterschiedliche Ports verwenden als für HTTPS. Lesen Sie die Anweisungen zum Verwalten von StorageGRID.

Verwandte Informationen

"StorageGRID verwalten"

"Vorteile von aktiven, inaktiven und gleichzeitigen HTTP-Verbindungen"

Endpoint-Domain-Namen für S3-Anforderungen

Bevor Sie S3-Domänennamen für Client-Anforderungen verwenden können, muss ein StorageGRID-Administrator das System so konfigurieren, dass Verbindungen angenommen werden, die S3-Domänennamen im S3-Pfadstil und virtuelle S3-Hosted-Style-Anforderungen verwenden.

Über diese Aufgabe

Um Ihnen die Verwendung von virtuellen S3-Hosted-Style-Anforderungen zu ermöglichen, muss ein Grid-Administrator die folgenden Aufgaben durchführen:

- Verwenden Sie den Grid-Manager, um dem StorageGRID System die S3-Endpunkt-Domain-Namen hinzuzufügen.
- Stellen Sie sicher, dass das Zertifikat, das der Client für HTTPS-Verbindungen zu StorageGRID verwendet, für alle vom Client erforderlichen Domänennamen signiert ist.

  Beispiel: Wenn der Endpunkt lautet `s3.company.com`, Der Grid-Administrator muss sicherstellen, dass das Zertifikat, das für HTTPS-Verbindungen verwendet wird, das umfasst `s3.company.com` endpunkt und Wildcard-alternativer Name (SAN) des Endpunkts: `*.s3.company.com`.

- Konfigurieren Sie den vom Client verwendeten DNS-Server, um DNS-Datensätze mit den Endpunktdomänennamen, einschließlich aller erforderlichen Platzhalterdatensätze, einzuschließen.

Wenn der Client über den Load Balancer-Service eine Verbindung herstellt, ist das Zertifikat, das der Grid-Administrator konfiguriert, das Zertifikat für den vom Client verwendeten Load Balancer-Endpunkt.

Jeder Load Balancer-Endpunkt verfügt über ein eigenes Zertifikat, und jeder Endpunkt kann so konfiguriert werden, dass verschiedene Endpunkt-Domain-Namen erkannt werden.

Wenn der Client Storage-Knoten oder den CLB-Dienst auf Gateway-Knoten verbindet, ist das Zertifikat, das der Grid-Administrator konfiguriert, das einzelne benutzerdefinierte Serverzertifikat, das für das Grid verwendet wird.

Der CLB-Service ist veraltet.

Weitere Informationen finden Sie in den Anweisungen zum Verwalten von StorageGRID.

Nach Abschluss dieser Schritte können Sie virtuelle Anfragen im Hosted-Style verwenden (z. B. `bucket.s3.company.com`).

Verwandte Informationen

"StorageGRID verwalten"

"Sicherheit wird für DIE REST API konfiguriert"

Testen Ihrer S3-REST-API-Konfiguration

Mit der Amazon Web Services Command Line Interface (AWS CLI) können Sie die Verbindung zum System testen und überprüfen, ob Sie Objekte lesen und in das System schreiben können.

Was Sie benötigen

- Sie müssen die AWS CLI von heruntergeladen und installiert haben "aws.amazon.com/cli".
- Sie müssen ein S3-Mandantenkonto im StorageGRID System erstellt haben.

Schritte

1. Konfigurieren Sie die Einstellungen für Amazon Web Services so, dass Sie das im StorageGRID System erstellte Konto verwenden:
   a. Konfigurationsmodus aufrufen: `aws configure`
   b. Geben Sie die AWS Zugriffsschlüssel-ID für das erstellte Konto ein.
   c. Geben Sie den AWS-Schlüssel für den geheimen Zugriff für das erstellte Konto ein.
   d. Geben Sie die Standardregion ein, die verwendet werden soll, z. B. US-East-1.
   e. Geben Sie das zu verwendende Standardausgabeformat ein, oder drücken Sie **Enter**, um JSON auszuwählen.
2. Erstellen eines Buckets:

   ```
   aws s3api --endpoint-url https://10.96.101.17:10443
   --no-verify-ssl create-bucket --bucket testbucket
   ```

   Wenn der Bucket erfolgreich erstellt wurde, wird der Speicherort des Buckets zurückgegeben, wie im folgenden Beispiel zu sehen:

   ```
   "Location": "/testbucket"
   ```

3. Hochladen eines Objekts.

   ```
   aws s3api --endpoint-url https://10.96.101.17:10443 --no-verify-ssl
   put-object --bucket testbucket --key s3.pdf --body C:\s3-
   test\upload\s3.pdf
   ```

   Wenn das Objekt erfolgreich hochgeladen wurde, wird ein ETAG zurückgegeben, der ein Hash der Objektdaten ist.

4. Listen Sie den Inhalt des Buckets auf, um zu überprüfen, ob das Objekt hochgeladen wurde.

```
aws s3api --endpoint-url https://10.96.101.17:10443 --no-verify-ssl
list-objects --bucket testbucket
```

5. Löschen Sie das Objekt.

```
aws s3api --endpoint-url https://10.96.101.17:10443 --no-verify-ssl
delete-object --bucket testbucket --key s3.pdf
```

6. Löschen Sie den Bucket.

```
aws s3api --endpoint-url https://10.96.101.17:10443 --no-verify-ssl
delete-bucket --bucket testbucket
```

So implementiert StorageGRID die S3-REST-API

Eine Client-Applikation kann S3-REST-API-Aufrufe zur Verbindung mit StorageGRID nutzen, um Buckets zu erstellen, zu löschen und zu ändern sowie Objekte zu speichern und abzurufen.

- "In Konflikt stehende Clientanforderungen"
- "Konsistenzkontrollen"
- "Managen von Objekten durch StorageGRID ILM-Regeln"
- "Objektversionierung"
- "Empfehlungen für die Implementierung der S3-REST-API"

In Konflikt stehende Clientanforderungen

Widersprüchliche Clientanforderungen, wie z. B. zwei Clients, die in denselben Schlüssel schreiben, werden auf „`latest-WINS`“-Basis gelöst.

Der Zeitpunkt für die Auswertung „`latest-WINS`“ basiert darauf, wann das StorageGRID System eine bestimmte Anfrage abschließt, und nicht auf, wenn S3-Clients einen Vorgang starten.

Konsistenzkontrollen

Konsistenzkontrollen ermöglichen je nach Anforderung eine Kompromiss zwischen der Verfügbarkeit der Objekte und der Konsistenz dieser Objekte über verschiedene Storage-Nodes und -Standorte.

Standardmäßig garantiert StorageGRID eine Lese-/Nachher-Konsistenz für neu erstellte Objekte. Jeder GET nach einem erfolgreich abgeschlossenen PUT wird in der Lage sein, die neu geschriebenen Daten zu lesen. Überschreibungen vorhandener Objekte, Metadatenaktualisierungen und -Löschungen sind schließlich konsistent. Überschreibungen dauern in der Regel nur wenige Sekunden oder Minuten, können jedoch bis zu 15 Tage in Anspruch nehmen.

Wenn Sie Objektvorgänge auf einer anderen Konsistenzstufe ausführen möchten, können Sie für jeden Bucket oder für jeden API-Vorgang eine Konsistenzkontrolle angeben.

Konsistenzkontrollen

Die Konsistenzkontrolle beeinflusst die Verteilung der Metadaten, die StorageGRID zum Verfolgen von Objekten zwischen Nodes verwendet, und somit die Verfügbarkeit von Objekten für Client-Anforderungen.

Sie können die Konsistenzkontrolle für einen Bucket- oder API-Vorgang auf einen der folgenden Werte festlegen:

Konsistenzkontrolle	Beschreibung
Alle	Alle Nodes erhalten die Daten sofort, sonst schlägt die Anfrage fehl.
Stark global	Garantierte Konsistenz bei Lese-nach-Schreibvorgängen für alle Client-Anfragen an allen Standorten.
Stark vor Ort	Garantiert Konsistenz bei Lese-nach-Schreibvorgängen für alle Client-Anfragen innerhalb eines Standorts.
Read-after-New-Write-Funktion	(Standard) konsistente Lese-/Schreibvorgänge für neue Objekte und eventuelle Konsistenz bei Objekt-Updates. Hochverfügbarkeit und garantierte Datensicherung Entspricht den Amazon S3 -Konsistenzgarantien. **Hinweis:** Wenn Ihre Anwendung HEAD Requests für Objekte verwendet, die nicht vorhanden sind, erhalten Sie möglicherweise eine hohe Anzahl von 500 internen Serverfehlern, wenn ein oder mehrere Speicherknoten nicht verfügbar sind. Um diese Fehler zu vermeiden, setzen Sie das Consistency Control auf „`available`“, es sei denn, Sie benötigen Konsistenzgarantien ähnlich wie Amazon S3.
Verfügbar (eventuelle Konsistenz für DEN HAUPTBETRIEB)	Verhält sich wie die Konsistenzstufe „`read-after-New-write`“, bietet aber nur eventuelle Konsistenz für DEN KOPFBETRIEB. Bietet höhere Verfügbarkeit FÜR HEAD-Operationen als „`read-after-New-write`“, wenn Storage Nodes nicht verfügbar sind. Unterschied zu Amazon S3 Konsistenzgarantien nur für HEAD-Operationen.

Verwenden der Consistency Controls „`read-after-New-write`“ und „`available`“

Wenn ein KOPF- oder GET-Vorgang die Konsistenzkontrolle „`read-after-New-write`“ verwendet oder EIN GET-Vorgang die Konsistenzkontrolle „`available`“ verwendet, führt StorageGRID die Suche in mehreren Schritten durch:

- Es sieht zunächst das Objekt mit einer niedrigen Konsistenz.
- Falls dieses Lookup fehlschlägt, wird das Lookup auf der nächsten Konsistenzebene wiederholt, bis es die höchste Konsistenzstufe „`all`,“ erreicht, sodass alle Kopien der Objektmetadaten verfügbar sein müssen.

Wenn ein KOPF- oder GET-Vorgang die Konsistenzkontrolle „`read-after-New-write`“ verwendet, aber das Objekt nicht vorhanden ist, erreicht die Objekt-Lookup immer die Konsistenzstufe „`all`“. Da auf dieser Konsistenzstufe alle Kopien der Objektmetadaten verfügbar sein müssen, können Sie eine hohe Anzahl von 500 Fehlern des internen Servers erhalten, wenn ein oder mehrere Storage-Nodes nicht verfügbar sind.

Sofern Sie keine Konsistenzgarantien wie Amazon S3 benötigen, können Sie diese Fehler bei DEN HEAD-Operationen vermeiden, indem Sie die Consistency Control auf „`available`“ setzen. Wenn ein HAUPTBETRIEB die Konsistenzkontrolle „`Available`“ verwendet, bietet StorageGRID eventuell nur Konsistenz. Ein fehlgeschlagener Vorgang wird erst wieder versucht, wenn es die Konsistenzstufe „`all`“ erreicht. Daher müssen nicht alle Kopien der Objektmetadaten verfügbar sein.

Angeben der Consistency Control für einen API-Vorgang

Um die Consistency Control für einen einzelnen API-Vorgang festzulegen, müssen für den Vorgang Konsistenzkontrollen unterstützt werden, und Sie müssen die Consistency Control in der Anforderungs-Kopfzeile angeben. In diesem Beispiel wird die Consistency Control auf “strong-site” für EINE GET Object Operation gesetzt.

```
GET /bucket/object HTTP/1.1
Date: date
Authorization: <em>authorization name</em>
Host: <em>host</em>
Consistency-Control: strong-site
```

> Sie müssen für DEN PUT-Objekt- und DEN GET-Objektbetrieb dasselbe Konsistenzsteuerelement verwenden.

Angeben der Konsistenzkontrolle für einen Bucket

Zum Festlegen der Konsistenzkontrolle für Bucket können Sie die StorageGRID PUT Bucket-Konsistenzanforderung und DIE ANFORDERUNG FÜR GET-Bucket-Konsistenz verwenden. Alternativ können Sie den Tenant Manager oder die Mandantenmanagement-API verwenden.

Beachten Sie beim Festlegen der Konsistenzkontrollen für einen Bucket Folgendes:

- Durch das Festlegen der Konsistenzkontrolle für einen Bucket wird festgelegt, welche Konsistenzkontrolle für S3-Operationen verwendet wird, die für Objekte im Bucket oder in der Bucket-Konfiguration durchgeführt werden. Er hat keine Auswirkungen auf die Vorgänge auf dem Bucket selbst.
- Die Konsistenzkontrolle für einen einzelnen API-Vorgang überschreibt die Konsistenzkontrolle für den Bucket.
- Im Allgemeinen sollte für Buckets die standardmäßige Konsistenzkontrolle verwendet werden, „`read-after-New-write.`“ Wenn Anforderungen nicht korrekt funktionieren, ändern Sie das Verhalten des Anwendungs-Clients, wenn möglich. Oder konfigurieren Sie den Client so, dass für jede API-Anforderung das Consistency Control angegeben wird. Legen Sie die Consistency Control auf Bucket-Ebene nur als letztes Resort fest.

Konsistenzkontrollen und ILM-Regeln interagieren, um die Datensicherung zu beeinträchtigen

Die Wahl der Konsistenzkontrolle und der ILM-Regel haben Auswirkungen auf den Schutz von Objekten. Diese Einstellungen können interagieren.

Die beim Speichern eines Objekts verwendete Konsistenzkontrolle beeinflusst beispielsweise die anfängliche Platzierung von Objekt-Metadaten, während das für die ILM-Regel ausgewählte Aufnahmeverhalten sich auf die anfängliche Platzierung von Objektkopien auswirkt. Da StorageGRID Zugriff auf die Metadaten eines Objekts und seine Daten benötigt, um Kundenanforderungen zu erfüllen, kann die Auswahl der passenden Sicherungsstufen für Konsistenz und Aufnahme-Verhalten eine bessere Erstsicherung und zuverlässigere Systemantworten ermöglichen.

Die folgenden Aufnahmeverhalten stehen für ILM-Regeln zur Verfügung:

- **Streng**: Alle in der ILM-Regel angegebenen Kopien müssen erstellt werden, bevor der Erfolg an den Client zurückgesendet wird.
- **Ausgewogen**: StorageGRID versucht bei der Aufnahme alle in der ILM-Regel festgelegten Kopien zu erstellen; wenn dies nicht möglich ist, werden Zwischenkopien erstellt und der Erfolg an den Client zurückgesendet. Die Kopien, die in der ILM-Regel angegeben sind, werden, wenn möglich gemacht.
- **Dual Commit**: StorageGRID erstellt sofort Zwischenkopien des Objekts und gibt den Erfolg an den Kunden zurück. Kopien, die in der ILM-Regel angegeben sind, werden nach Möglichkeit erstellt.

> Lesen Sie vor der Auswahl des Aufnahmeverhaltens für eine ILM-Regel die vollständige Beschreibung dieser Einstellungen in den Anweisungen zum Managen von Objekten mit Information Lifecycle Management.

Beispiel für die Interaktion zwischen Konsistenzkontrolle und ILM-Regel

Angenommen, Sie haben ein Grid mit zwei Standorten mit der folgenden ILM-Regel und der folgenden Einstellung für die Konsistenzstufe:

- **ILM-Regel**: Erstellen Sie zwei Objektkopien, eine am lokalen Standort und eine an einem entfernten Standort. Das strikte Aufnahmeverhalten wird ausgewählt.
- **Konsistenzstufe**: “strong-global” (Objektmetadaten werden sofort auf alle Standorte verteilt.)

Wenn ein Client ein Objekt im Grid speichert, erstellt StorageGRID sowohl Objektkopien als auch verteilt Metadaten an beiden Standorten, bevor der Kunde zum Erfolg zurückkehrt.

Das Objekt ist zum Zeitpunkt der Aufnahme der Nachricht vollständig gegen Verlust geschützt. Wenn beispielsweise der lokale Standort kurz nach der Aufnahme verloren geht, befinden sich Kopien der Objektdaten und der Objektmetadaten am Remote-Standort weiterhin. Das Objekt kann vollständig abgerufen werden.

Falls Sie stattdessen dieselbe ILM-Regel und die Konsistenzstufe „`strong-site`“ verwendet haben, erhält der Client möglicherweise eine Erfolgsmeldung, nachdem Objektdaten an den Remote-Standort repliziert wurden, doch bevor die Objektmetadaten dort verteilt werden. In diesem Fall entspricht die Sicherung von Objektmetadaten nicht dem Schutzniveau für Objektdaten. Falls der lokale Standort kurz nach der Aufnahme verloren geht, gehen Objektmetadaten verloren. Das Objekt kann nicht abgerufen werden.

Die Wechselbeziehung zwischen Konsistenzstufen und ILM-Regeln kann komplex sein. Wenden Sie sich an NetApp, wenn Sie Hilfe benötigen.

Verwandte Informationen

"Objektmanagement mit ILM"

"Get Bucket-Konsistenzanforderung"

"PUT Bucket-Konsistenzanforderung"

Managen von Objekten durch StorageGRID ILM-Regeln

Der Grid-Administrator erstellt Informationen Lifecycle Management (ILM)-Regeln für das Management von Objektdaten, die von S3-REST-API-Client-Applikationen in das StorageGRID-System aufgenommen werden. Diese Regeln werden dann zur ILM-Richtlinie hinzugefügt, um zu bestimmen, wie und wo Objektdaten im Laufe der Zeit gespeichert werden.

ILM-Einstellungen bestimmen die folgenden Aspekte eines Objekts:

- **Geographie**

  Der Speicherort der Objektdaten kann entweder im StorageGRID-System (Storage-Pool) oder in einem Cloud-Storage-Pool gespeichert werden.

- * Speicherklasse*

  Storage-Typ zur Speicherung von Objektdaten, z. B. Flash oder rotierende Festplatte

- **Verlustschutz**

  Wie viele Kopien erstellt werden und welche Arten von Kopien erstellt werden: Replizierung, Erasure Coding oder beides.

- **Aufbewahrung**

  Es ändert sich im Laufe der Zeit, wie Objektdaten verwaltet werden, wo sie gespeichert sind und wie sie vor Verlust geschützt sind.

- **Schutz während der Aufnahme**

  Methode zum Schutz von Objektdaten bei der Aufnahme: Synchrone Platzierung (mit ausgeglichenen oder strengen Optionen für das Aufnahmeverhalten) oder Erstellung von vorläufigen Kopien (unter Verwendung der Option Dual-Commit)

ILM-Regeln können Objekte filtern und auswählen. Bei mit S3 aufgenommenen Objekten können ILM-Regeln Objekte auf Basis der folgenden Metadaten filtern:

- Mandantenkonto
- Bucket-Name
- Aufnahmezeit
- Taste
- Zeitpunkt Des Letzten Zugriffs

Standardmäßig werden Updates der letzten Zugriffszeit für alle S3 Buckets deaktiviert. Wenn Ihr StorageGRID System eine ILM-Regel enthält, die die Option „Last Access Time“ verwendet, müssen Sie für die in dieser Regel angegebenen S3-Buckets Updates für die letzte Zugriffszeit aktivieren. Sie können Updates der letzten Zugriffszeit mithilfe der Anforderung PUT Bucket Last Access Time, des Checkbox **S3** > **Buckets** > **Letzter Zugriffszeitpunkt konfigurieren** im Tenant Manager oder mithilfe der Tenant Management API aktivieren. Beachten Sie bei der Aktivierung von Updates der letzten Zugriffszeit, dass die Performance von StorageGRID möglicherweise reduziert wird, insbesondere bei Systemen mit kleinen Objekten.

- Speicherortbeschränkung
- Objektgröße
- Benutzermetadaten
- Objekt-Tag

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

Verwandte Informationen

"Verwenden Sie ein Mandantenkonto"

"Objektmanagement mit ILM"

"PUT Anforderung der Uhrzeit des letzten Bucket-Zugriffs"

Objektversionierung

Sie können mithilfe der Versionierung mehrere Versionen eines Objekts aufbewahren, das vor versehentlichem Löschen von Objekten schützt und Ihnen das Abrufen und Wiederherstellen älterer Versionen eines Objekts ermöglicht.

Das StorageGRID System implementiert Versionierung mit Unterstützung für die meisten Funktionen und weist einige Einschränkungen auf. StorageGRID unterstützt bis zu 1,000 Versionen jedes Objekts.

Die Objektversionierung kann mit StorageGRID Information Lifecycle Management (ILM) oder mit der S3 Bucket Lifecycle-Konfiguration kombiniert werden. Sie müssen für jeden Bucket die Versionierung aktivieren, um diese Funktion für den Bucket zu aktivieren. Jedem Objekt im Bucket wird eine Version-ID zugewiesen, die vom StorageGRID-System generiert wird.

Die Verwendung von MFA (Multi-Faktor-Authentifizierung) Löschen wird nicht unterstützt.

Die Versionierung kann nur auf Buckets aktiviert werden, die mit StorageGRID Version 10.3 oder höher erstellt wurden.

ILM und Versionierung

ILM-Richtlinien werden auf jede Version eines Objekts angewendet. Ein ILM-Scanprozess scannt kontinuierlich alle Objekte und bewertet sie anhand der aktuellen ILM-Richtlinie neu. Alle Änderungen, die Sie an ILM-Richtlinien vornehmen, werden auf alle zuvor aufgenommenen Objekte angewendet. Dies umfasst bereits aufgenommene Versionen, wenn die Versionierung aktiviert ist. Beim ILM-Scannen werden neue ILM-Änderungen an zuvor aufgenommenen Objekten angewendet.

Bei S3-Objekten in mit Versionierung aktivierten Buckets können Sie mithilfe der Versionierung ILM-Regeln erstellen, die nicht aktuelle Zeit als Referenzzeit verwenden. Wenn ein Objekt aktualisiert wird, werden seine vorherigen Versionen nicht aktuell. Mithilfe eines nicht aktuellen Zeitfilters können Sie Richtlinien erstellen, die die Auswirkungen früherer Objektversionen auf den Storage verringern.

> Wenn Sie eine neue Version eines Objekts über einen mehrteiligen Upload-Vorgang hochladen, wird der nicht aktuelle Zeitpunkt für die Originalversion des Objekts angezeigt, wenn der mehrteilige Upload für die neue Version erstellt wurde, nicht erst nach Abschluss des mehrteiligen Uploads. In begrenzten Fällen kann die nicht aktuelle Zeit der ursprünglichen Version Stunden oder Tage früher als die Zeit für die aktuelle Version sein.

Anweisungen zum Managen von Objekten mit Information Lifecycle Management finden Sie in den Anweisungen, wie z. B. eine ILM-Richtlinie für versionierte Objekte mit S3 enthält.

Verwandte Informationen

"Objektmanagement mit ILM"

Empfehlungen für die Implementierung der S3-REST-API

Bei der Implementierung der S3-REST-API zur Verwendung mit StorageGRID sollten Sie diese Empfehlungen beachten.

Empfehlungen für Köpfe zu nicht vorhandenen Objekten

Wenn Ihre Anwendung regelmäßig prüft, ob ein Objekt in einem Pfad existiert, in dem Sie nicht erwarten, dass das Objekt tatsächlich vorhanden ist, sollten Sie die Konsistenzkontrolle „`available`“ verwenden. Verwenden Sie zum Beispiel die Konsistenzkontrolle „`Available`“, wenn Ihre Anwendung einen Speicherort vor DEM ANSETZEN an sie leitet.

Andernfalls werden möglicherweise 500 Fehler des internen Servers angezeigt, wenn ein oder mehrere Speicherknoten nicht verfügbar sind.

Sie können die Konsistenzkontrolle „`Available`“ für jeden Bucket mithilfe der PUT Bucket-Konsistenzanforderung festlegen oder Sie können die Konsistenzkontrolle in der Anforderungs-Kopfzeile für einen einzelnen API-Vorgang festlegen.

Empfehlungen für Objektschlüssel

Bei Buckets, die in StorageGRID 11.4 oder höher erstellt wurden, ist es nicht mehr erforderlich, Objektschlüsselnamen auf die Performance-Best-Practices zu beschränken. Sie können jetzt beispielsweise Zufallswerte für die ersten vier Zeichen von Objektschlüsselnamen verwenden.

Befolgen Sie bei Buckets, die in Versionen vor StorageGRID 11.4 erstellt wurden, weiterhin die folgenden Empfehlungen für Objektschlüsselnamen:

- Als die ersten vier Zeichen von Objektschlüsseln sollten Sie keine Zufallswerte verwenden. Dies steht im Gegensatz zu der früheren AWS Empfehlung für wichtige Präfixe. Stattdessen sollten Sie nicht-zufällige, nicht-eindeutige Präfixe verwenden, wie z. B. `image`.
- Wenn Sie die frühere Empfehlung von AWS befolgen, zufällige und eindeutige Zeichen in Schlüsselpräfixen zu verwenden, sollten Sie die Objektschlüssel mit einem Verzeichnisnamen vorschreiben. Verwenden Sie dieses Format:

```
mybucket/mydir/f8e3-image3132.jpg
```

Anstelle dieses Formats:

```
mybucket/f8e3-image3132.jpg
```

Empfehlungen für „`Range reads`“

Wenn die Option **komprimiere gespeicherte Objekte** ausgewählt ist (**Konfiguration** > **Grid-Optionen**), sollten S3-Client-Anwendungen verhindern, DASS GET-Objekt-Operationen ausgeführt werden, die einen Bereich von Bytes angeben. Diese Vorgänge „`range Read`“ sind ineffizient, da StorageGRID die Objekte effektiv dekomprimieren muss, um auf die angeforderten Bytes zugreifen zu können. GET-Objektvorgänge, die einen kleinen Byte-Bereich von einem sehr großen Objekt anfordern, sind besonders ineffizient, beispielsweise ist es sehr ineffizient, einen Bereich von 10 MB von einem komprimierten 50-GB-Objekt zu lesen.

Wenn Bereiche von komprimierten Objekten gelesen werden, können Client-Anforderungen eine Zeitdauer haben.

> ⓘ Wenn Sie Objekte komprimieren müssen und Ihre Client-Applikation Bereichslesevorgänge verwenden muss, erhöhen Sie die Zeitüberschreitung beim Lesen der Anwendung.

Verwandte Informationen

"Konsistenzkontrollen"

"PUT Bucket-Konsistenzanforderung"

"StorageGRID verwalten"

Unterstützte Vorgänge und Einschränkungen durch S3-REST-API

Das StorageGRID System implementiert die Simple Storage Service API (API Version 2006-03-01) mit Unterstützung der meisten Operationen und mit einigen Einschränkungen. Wenn Sie S3 REST-API-Client-Applikationen integrieren, sind die Implementierungsdetails bekannt.

Das StorageGRID System unterstützt sowohl Virtual-Hosted-Style-Anforderungen als auch Anforderungen im Pfadstil.

- "Authentifizierung von Anforderungen"
- "Betrieb auf dem Service"
- "Operationen auf Buckets"
- "Benutzerdefinierte Vorgänge für Buckets"
- "Operationen für Objekte"
- "Vorgänge für mehrteilige Uploads"
- "Fehlerantworten"

Umgang mit Daten

Die StorageGRID Implementierung der S3-REST-API unterstützt nur gültige HTTP-Datumsformate.

Das StorageGRID-System unterstützt nur gültige HTTP-Datumsformate für alle Header, die Datumswerte akzeptieren. Der Zeitbereich des Datums kann im Greenwich Mean Time (GMT)-Format oder im UTC-Format (Universal Coordinated Time) ohne Zeitzonenversatz angegeben werden (+0000 muss angegeben werden). Wenn Sie die einschließen `x-amz-date` Kopfzeile in Ihrer Anfrage, es überschreibt alle Werte, die in der Kopfzeile der Datumsanforderung angegeben sind. Bei Verwendung von AWS Signature Version 4, das `x-amz-date` Die Kopfzeile muss in der signierten Anforderung vorhanden sein, da die Datumsüberschrift nicht unterstützt wird.

Allgemeine Anfragemöpfe

Das StorageGRID System unterstützt gemeinsame Anfrageheader, die von der *Simple Storage Service API Reference* definiert wurden, mit einer Ausnahme.

Kopfzeile der Anfrage	Implementierung
Autorisierung	Vollständige Unterstützung für AWS Signature Version 2 Unterstützung für AWS Signature Version 4, mit folgenden Ausnahmen: • Der SHA256-Wert wird für den Körper der Anforderung nicht berechnet. Der vom Benutzer eingereichte Wert wird ohne Validierung angenommen, als ob der Wert `UNSIGNED-PAYLOAD` War für die vorgesehen `x-amz-content-sha256` Kopfzeile.
X-amz-Sicherheits-Token	Nicht implementiert. Kehrt Zurück `XNotImplemented`.

Allgemeine Antwortkopfzeilen

Das StorageGRID System unterstützt alle gängigen Antwortheader, die durch die *Simple Storage Service API Reference* definiert wurden. Eine Ausnahme bilden die Antwort.

Kopfzeile der Antwort	Implementierung
X-amz-id-2	Nicht verwendet

Verwandte Informationen

"Amazon Web Services (AWS) Dokumentation: Amazon Simple Storage Service API Reference"

Authentifizierung von Anforderungen

Das StorageGRID-System unterstützt über die S3-API sowohl authentifizierten als auch anonymen Zugriff auf Objekte.

Die S3-API unterstützt Signature Version 2 und Signature Version 4 zur Authentifizierung von S3-API-Anforderungen.

Authentifizierte Anfragen müssen mit Ihrer Zugriffsschlüssel-ID und Ihrem geheimen Zugriffsschlüssel signiert werden.

Das StorageGRID System unterstützt zwei Authentifizierungsmethoden: Den HTTP `Authorization` Kopfzeile und Verwendung von Abfrageparametern.

Verwenden der HTTP-Autorisierungsüberschrift

Das HTTP `Authorization` Kopfzeile wird von allen S3-API-Operationen verwendet außer anonymen Anfragen, sofern dies durch die Bucket-Richtlinie zulässig ist. Der `Authorization` Der Header enthält alle erforderlichen Signierungsdaten, um eine Anforderung zu authentifizieren.

Abfrageparameter werden verwendet

Sie können Abfrageparameter verwenden, um Authentifizierungsinformationen zu einer URL hinzuzufügen. Dies wird als Vorsignierung der URL bezeichnet, mit der ein temporärer Zugriff auf bestimmte Ressourcen gewährt werden kann. Benutzer mit der vorsignierten URL müssen den geheimen Zugriffsschlüssel nicht kennen, um auf die Ressource zugreifen zu können, wodurch Sie einen eingeschränkten Zugriff auf eine Ressource durch Dritte ermöglichen können.

Betrieb auf dem Service

Das StorageGRID System unterstützt die folgenden Vorgänge beim Service.

Betrieb	Implementierung
GET Service	Wird mit dem gesamten Amazon S3-REST-API-Verhalten implementiert.
GET Storage-Auslastung	Der Antrag ZUR GET Storage-Nutzung gibt Ihnen die Gesamtzahl des verwendeten Storage durch ein Konto und für jeden mit dem Account verknüpften Bucket an. Dies ist eine Operation auf dem Dienst mit einem Pfad von / und einem benutzerdefinierten Abfrageparameter (`?x-ntap-sg-usage`) Hinzugefügt.
OPTIONEN /	Client-Applikationen können Probleme haben `OPTIONS /` Anfragen an den S3-Port auf einem Storage-Node ohne die Zugangsdaten für die S3-Authentifizierung, um zu ermitteln, ob der Storage-Node verfügbar ist. Sie können diese Anforderung zum Monitoring verwenden oder um zu ermöglichen, dass externe Load Balancer eingesetzt werden, wenn ein Storage-Node ausfällt.

Verwandte Informationen

"Storage-Nutzungsanforderung ABRUFEN"

Operationen auf Buckets

Das StorageGRID System unterstützt für jedes S3-Mandantenkonto maximal 1,000 Buckets.

Einschränkungen für Bucket-Namen folgen den regionalen Beschränkungen für AWS US Standard. Sie sollten sie jedoch noch weiter auf DNS-Namenskonventionen beschränken, um Anfragen im Stil von virtuellen S3-Hosted-Style zu unterstützen.

"Amazon Web Services (AWS) Dokumentation: Bucket-Einschränkungen und -Einschränkungen"

"Endpoint-Domain-Namen für S3-Anforderung"

Operationen „GET Bucket“ (Listenobjekte) und „GET Bucket-Versionen“ unterstützen die StorageGRID-Konsistenzkontrollen.

Sie können überprüfen, ob für einzelne Buckets Updates zur letzten Zugriffszeit aktiviert oder deaktiviert wurden.

In der folgenden Tabelle wird beschrieben, wie StorageGRID S3-REST-API-Bucket-Operationen implementiert Um einen dieser Vorgänge durchzuführen, müssen die erforderlichen Anmeldedaten für den Zugriff für das Konto bereitgestellt werden.

Betrieb	Implementierung
Bucket LÖSCHEN	Wird mit dem gesamten Amazon S3-REST-API-Verhalten implementiert.
Bucket-Cors LÖSCHEN	Durch diesen Vorgang wird die CORS-Konfiguration für den Bucket gelöscht.
Bucket-Verschlüsselung LÖSCHEN	Bei diesem Vorgang wird die Standardverschlüsselung aus dem Bucket gelöscht. Vorhandene verschlüsselte Objekte bleiben verschlüsselt, neue dem Bucket hinzugefügte Objekte werden jedoch nicht verschlüsselt.
Bucket-Lebenszyklus LÖSCHEN	Bei diesem Vorgang wird die Lebenszyklukonfiguration aus dem Bucket gelöscht.
Bucket-Richtlinie LÖSCHEN	Bei diesem Vorgang wird die Richtlinie gelöscht, die dem Bucket zugeordnet ist.
Bucket-Replizierung LÖSCHEN	Bei diesem Vorgang wird die an den Bucket angeschlossene Replizierungskonfiguration gelöscht.
Bucket-Tagging LÖSCHEN	Dieser Vorgang verwendet das `tagging` unterressource, um alle Tags aus einem Bucket zu entfernen

Betrieb	Implementierung
Get Bucket (Listenobjekte), Version 1 und Version 2	Dieser Vorgang gibt einige oder alle (bis zu 1,000) Objekte in einem Bucket zurück. Die Speicherklasse für Objekte kann einen von zwei Werten haben, auch wenn das Objekt mit aufgenommen wurde `REDUCED_REDUNDANCY` Option für Storage-Klasse: • `STANDARD`, Die angibt, dass das Objekt in einem Speicherpool gespeichert wird, der aus Storage-Nodes besteht. • `GLACIER`, Dies bedeutet, dass das Objekt in den vom Cloud-Speicherpool angegebenen externen Bucket verschoben wurde. Wenn der Bucket eine große Anzahl von gelöschten Schlüsseln enthält, die dasselbe Präfix haben, kann die Antwort einige enthalten `CommonPrefixes` Die keine Schlüssel enthalten.
Bucket-acl ABRUFEN	Dieser Vorgang gibt eine positive Antwort und die ID, DisplayName und die Erlaubnis des Bucket-Besitzers zurück, was darauf hinweist, dass der Besitzer vollen Zugriff auf den Bucket hat.
Bucket-Cors ABRUFEN	Dieser Vorgang gibt den zurück `cors` Konfiguration für den Bucket.
Get Bucket-Verschlüsselung	Dieser Vorgang gibt die Standardverschlüsselungskonfiguration für den Bucket zurück.
BUCKET-Lebenszyklus ABRUFEN	Dieser Vorgang gibt die Lifecycle-Konfiguration für den Bucket zurück.
Bucket-Speicherort ABRUFEN	Dieser Vorgang gibt die Region zurück, die mit dem festgelegt wurde `LocationConstraint` Element in DER PUT Bucket Anforderung. Wenn der Eimer-Bereich ist `us-east-1`, Eine leere Zeichenfolge wird für die Region zurückgegeben.
Bucket-Benachrichtigung ABRUFEN	Dieser Vorgang gibt die Benachrichtigungskonfiguration an den Bucket zurück.
Get Bucket-Objektversionen	Mit LESEZUGRIFF auf einen Bucket erfolgt dieser Vorgang mit dem `versions` unterressource listet Metadaten aller Versionen von Objekten im Bucket auf.

Betrieb	Implementierung
Get Bucket-Richtlinie	Dieser Vorgang gibt die Richtlinie zurück, die dem Bucket zugeordnet ist.
GET Bucket-Replizierung	Dieser Vorgang gibt die am Bucket angeschlossene Replizierungskonfiguration zurück.
Get Bucket-Tagging	Dieser Vorgang verwendet das `tagging` unterressource, um alle Tags für einen Bucket zurückzugeben
Get Bucket-Versionierung	Diese Implementierung verwendet das `versioning` subressource zur Rückgabe des Versionierungsstatus eines Buckets. Der zurückgegebene Versionierungsstatus gibt an, ob der Bucket die Version „`Unversioniert`“ oder die Version „`Enabled`“ oder „`Suspended`“ lautet.
Konfiguration der Objektsperre ABRUFEN	Dieser Vorgang legt fest, ob die S3-Objektsperre für einen Bucket aktiviert ist. "Verwenden der S3-Objektsperre"
EIMER	Dieser Vorgang bestimmt, ob ein Bucket vorhanden ist und Sie über die Berechtigung zum Zugriff auf ihn verfügen.

Betrieb	Implementierung
Put Bucket	Durch diesen Vorgang wird ein neuer Bucket erstellt. Mit dem Erstellen des Buckets werden Sie zum Bucket-Eigentümer. • Bucket-Namen müssen die folgenden Regeln einhalten: ◦ Jedes StorageGRID System muss eindeutig sein (nicht nur innerhalb des Mandantenkontos). ◦ Muss DNS-konform sein. ◦ 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. • Standardmäßig werden Buckets im erstellt `us-east-1` Region; jedoch können Sie die verwenden `LocationConstraint` Anforderungselement im Anforderungskörper, um eine andere Region anzugeben. Bei Verwendung des `LocationConstraint` Element, Sie müssen den genauen Namen einer Region angeben, die mit dem Grid Manager oder der Grid Management API definiert wurde. Wenden Sie sich an Ihren Systemadministrator, wenn Sie den Namen der zu verwendenden Region nicht kennen. **Hinweis**: Ein Fehler tritt auf, wenn Ihre PUT Bucket-Anforderung eine Region verwendet, die nicht in StorageGRID definiert wurde. • Sie können die einschließen `x-amz-bucket-object-lock-enabled` Kopfzeile zum Erstellen eines Buckets anfordern, wobei S3-Objektsperre aktiviert ist. Sie müssen die S3-Objektsperre aktivieren, wenn Sie den Bucket erstellen. Sie können S3 Object Lock nicht hinzufügen oder deaktivieren, nachdem ein Bucket erstellt wurde. Für die S3-Objektsperre ist eine Bucket-Versionierung erforderlich. Diese wird bei der Erstellung des Buckets automatisch aktiviert.

Betrieb	Implementierung
Bucket-Cors EINGEBEN	Mit diesem Vorgang wird die CORS-Konfiguration für einen Bucket festgelegt, damit der Bucket die Cross-Origin-Requests bedienen kann. CORS (Cross-Origin Resource Sharing) ist ein Sicherheitsmechanismus, mit dem Client-Webanwendungen in einer Domäne auf Ressourcen in einer anderen Domäne zugreifen können. Angenommen, Sie verwenden einen S3-Bucket mit dem Namen `images` Zum Speichern von Grafiken. Durch Festlegen der CORS-Konfiguration für das `images` Bucket: Sie können zulassen, dass die Bilder in diesem Bucket auf der Website angezeigt werden `http://www.example.com`.
Bucket-Verschlüsselung	Dieser Vorgang legt den Standardverschlüsselungsstatus eines vorhandenen Buckets fest. Bei aktivierter Verschlüsselung auf Bucket-Ebene sind alle neuen dem Bucket hinzugefügten Objekte verschlüsselt.StorageGRID unterstützt serverseitige Verschlüsselung mit von StorageGRID gemanagten Schlüsseln. Wenn Sie die Konfigurationsregel für die serverseitige Verschlüsselung angeben, legen Sie die fest `SSEAlgorithm` Parameter an `AES256`, Und verwenden Sie nicht die `KMSMasterKeyID` Parameter. Die Standardverschlüsselungskonfiguration von Buckets wird ignoriert, wenn in der Anfrage für das Hochladen von Objekten bereits eine Verschlüsselung angegeben ist (d. h., wenn die Anforderung den umfasst `x-amz-server-side-encryption-*` Kopfzeile der Anfrage).

Betrieb	Implementierung
PUT Bucket-Lebenszyklus	Dieser Vorgang erstellt eine neue Lifecycle-Konfiguration für den Bucket oder ersetzt eine vorhandene Lifecycle-Konfiguration. StorageGRID unterstützt in einer Lebenszykluskonfiguration bis zu 1,000 Lebenszyklusregeln. Jede Regel kann die folgenden XML-Elemente enthalten: • Ablauf (Tage, Datum) • NoncurrentVersionExpiration (NoncurrentDays) • Filter (Präfix, Tag) • Status • ID StorageGRID bietet folgende Maßnahmen nicht: • AbortInsetteMultipartUpload • ExpiredObjectDeleteMarker • Übergang Informationen dazu, wie die Aktion zum Ablauf in einem Bucket-Lebenszyklus mit den Anweisungen zur ILM-Platzierung interagiert, finden Sie unter „`wie ILM während der gesamten Lebensdauer eines Objekts funktioniert`“ in den Anweisungen für das Management von Objekten mit Information Lifecycle Management. **Hinweis**: Die Konfiguration des Bucket-Lebenszyklus kann für Buckets verwendet werden, für die S3-Objektsperre aktiviert ist. Die Bucket-Lebenszykluskonfiguration wird jedoch für ältere kompatible Buckets nicht unterstützt.

Betrieb	Implementierung

PUT Bucket-Benachrichtigung	Mit diesem Vorgang werden Benachrichtigungen für den Bucket mithilfe der im Anfraentext enthaltenen XML-Benachrichtigungskonfiguration konfiguriert. Sie sollten folgende Implementierungsdetails kennen:
	
	• StorageGRID unterstützt SNS-Themen (Simple Notification Service) als Ziele. Simple Queue Service (SQS)- oder Amazon Lambda-Endpunkte werden nicht unterstützt.
	• Das Ziel für Benachrichtigungen muss als URN eines StorageGRID-Endpunkts angegeben werden. Endpunkte können mit dem Mandanten-Manager oder der Mandanten-Management-API erstellt werden.
	
	Der Endpunkt muss vorhanden sein, damit die Benachrichtigungskonfiguration erfolgreich ausgeführt werden kann. Wenn der Endpunkt nicht vorhanden ist, A `400 Bad Request` Der Code gibt einen Fehler zurück `InvalidArgument`.
	
	• 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 folgenden Liste gezeigt:
	• **EventSource**
	
	`sgws:s3`
	
	• **AwsRegion**
	
	Nicht enthalten
	
	• * X-amz-id-2*
	
	Nicht enthalten
	
	• **arn**
	
	`urn:sgws:s3:::bucket_name`

Betrieb	Implementierung
Bucket-Richtlinie	Dieser Vorgang legt die Richtlinie fest, die an den Bucket gebunden ist.

Betrieb	Implementierung
PUT Bucket-Replizierung	Dieser Vorgang konfiguriert die StorageGRID CloudMirror-Replikation für den Bucket mithilfe der im Anforderungsgremium bereitgestellten Replikationskonfigurations-XML. Für die CloudMirror-Replikation sollten Sie die folgenden Implementierungsdetails beachten: • StorageGRID unterstützt nur V1 der Replizierungskonfiguration. Das bedeutet, dass StorageGRID die Verwendung von nicht unterstützt `Filter` Element für Regeln und folgt V1-Konventionen zum Löschen von Objektversionen. Details finden Sie in der Amazon Dokumentation zur Replizierungskonfiguration. • Die Bucket-Replizierung kann für versionierte oder nicht versionierte Buckets konfiguriert werden. • Sie können in jeder Regel der XML-Replikationskonfiguration einen anderen Ziel-Bucket angeben. Ein Quell-Bucket kann auf mehrere Ziel-Bucket replizieren. • Ziel-Buckets müssen als URN der StorageGRID-Endpunkte angegeben werden, wie im Mandantenmanager oder der Mandantenmanagement-API angegeben. Der Endpunkt muss vorhanden sein, damit die Replizierungskonfiguration erfolgreich ausgeführt werden kann. Wenn der Endpunkt nicht vorhanden ist, schlägt die Anforderung als a fehl `400 Bad Request`. In der Fehlermeldung steht: `Unable to save the replication policy. The specified endpoint URN does not exist: URN`. • Sie müssen kein angeben `Role` In der Konfigurations-XML. Dieser Wert wird von StorageGRID nicht verwendet und wird bei der Einreichung ignoriert. • Wenn Sie die Storage-Klasse aus der XML-Konfiguration weglassen, verwendet StorageGRID das `STANDARD` Standardmäßig Storage-Klasse. • Wenn Sie ein Objekt aus dem Quell-Bucket löschen oder den Quell-Bucket selbst löschen, sieht das Verhalten der regionsübergreifenden Replizierung wie folgt aus: ◦ Wenn Sie das Objekt oder Bucket vor der Replizierung löschen, wird das Objekt/Bucket nicht repliziert, und Sie werden nicht benachrichtigt. Wenn Sie das Objekt oder Bucket nach der

Betrieb	Implementierung
PUT Bucket-Tagging	Dieser Vorgang verwendet das `tagging` unterressource, um einen Satz von Tags für einen Bucket hinzuzufügen oder zu aktualisieren Beachten Sie beim Hinzufügen von Bucket-Tags die folgenden Einschränkungen: • StorageGRID und Amazon S3 unterstützen für jeden Bucket bis zu 50 Tags. • Tags, die einem Bucket zugeordnet sind, müssen eindeutige Tag-Schlüssel haben. Ein Tag-Schlüssel kann bis zu 128 Unicode-Zeichen lang sein. • Die Tag-Werte können bis zu 256 Unicode-Zeichen lang sein. • Bei den Schlüsseln und Werten wird die Groß-/Kleinschreibung beachtet.
PUT Bucket-Versionierung	Diese Implementierung verwendet das `versioning` unterressource, um den Versionierungsstatus eines vorhandenen Buckets festzulegen. Sie können den Versionierungsstatus mit einem der folgenden Werte festlegen: • Aktiviert: Versionierung für die Objekte im Bucket Alle dem Bucket hinzugefügten Objekte erhalten eine eindeutige Version-ID. • Suspendiert: Deaktiviert die Versionierung für die Objekte im Bucket. Alle dem Bucket hinzugefügten Objekte erhalten die Version-ID `null`.

Verwandte Informationen

"Amazon Web Services (AWS) Dokumentation: Regionsübergreifende Replizierung"

"Konsistenzkontrollen"

"Anforderung der Uhrzeit des letzten Bucket-Zugriffs ABRUFEN"

"Bucket- und Gruppenzugriffsrichtlinien"

"Verwenden der S3-Objektsperre"

"S3-Vorgänge werden in den Audit-Protokollen protokolliert"

"Objektmanagement mit ILM"

"Verwenden Sie ein Mandantenkonto"

Erstellen einer S3-Lebenszykluskonfiguration

Sie können eine S3-Lebenszyklukonfiguration erstellen, um zu steuern, wann bestimmte Objekte aus dem StorageGRID System gelöscht werden.

Das einfache Beispiel in diesem Abschnitt veranschaulicht, wie eine S3-Lebenszykluskonfiguration das Löschen bestimmter Objekte aus bestimmten S3-Buckets kontrollieren kann. Das Beispiel in diesem Abschnitt dient nur zu Illustrationszwecken. Alle Details zum Erstellen von S3-Lebenszykluskonfigurationen finden Sie im Abschnitt zum Lifecycle Management von Objekten im *Amazon Simple Storage Service Developer Guide*. Beachten Sie, dass StorageGRID nur Aktionen nach Ablauf unterstützt. Es werden keine Aktionen zur Transition unterstützt.

"Amazon Simple Storage Service Developer Guide: Lifecycle Management von Objekten"

Was für eine Lebenszykluskonfiguration ist

Eine Lifecycle-Konfiguration ist ein Satz von Regeln, die auf die Objekte in bestimmten S3-Buckets angewendet werden. Jede Regel gibt an, welche Objekte betroffen sind und wann diese Objekte ablaufen (an einem bestimmten Datum oder nach einigen Tagen).

StorageGRID unterstützt in einer Lebenszykluskonfiguration bis zu 1,000 Lebenszyklusregeln. Jede Regel kann die folgenden XML-Elemente enthalten:

- Ablauf: Löschen eines Objekts, wenn ein bestimmtes Datum erreicht wird oder wenn eine bestimmte Anzahl von Tagen erreicht wird, beginnend mit dem Zeitpunkt der Aufnahme des Objekts.
- NoncurrentVersionExpiration: Löschen Sie ein Objekt, wenn eine bestimmte Anzahl von Tagen erreicht wird, beginnend ab dem Zeitpunkt, an dem das Objekt nicht mehr aktuell wurde.
- Filter (Präfix, Tag)
- Status
- ID

Wenn Sie eine Lifecycle-Konfiguration auf einen Bucket anwenden, überschreiben die Lifecycle-Einstellungen für den Bucket immer die StorageGRID-ILM-Einstellungen. StorageGRID verwendet die Verfallseinstellungen für den Bucket und nicht ILM, um zu bestimmen, ob bestimmte Objekte gelöscht oder aufbewahrt werden sollen.

Aus diesem Grund kann ein Objekt aus dem Grid entfernt werden, obwohl die Speicheranweisungen in einer ILM-Regel noch auf das Objekt gelten. Alternativ kann ein Objekt auch dann im Grid aufbewahrt werden, wenn eine ILM-Platzierungsanleitung für das Objekt abgelaufen ist. Weitere Informationen finden Sie unter „`Funktionsweise von ILM während der gesamten Lebensdauer eines Objekts`“ in den Anweisungen zum Verwalten von Objekten mit Information Lifecycle Management.

> Die Bucket-Lifecycle-Konfiguration kann für Buckets verwendet werden, für die S3-Objektsperre aktiviert ist. Die Bucket-Lifecycle-Konfiguration wird jedoch für ältere Buckets, die Compliance verwenden, nicht unterstützt.

StorageGRID unterstützt den Einsatz der folgenden Bucket-Operationen zum Management der Lebenszykluskonfigurationen:

- Bucket-Lebenszyklus LÖSCHEN
- BUCKET-Lebenszyklus ABRUFEN
- PUT Bucket-Lebenszyklus

Erstellen der Lebenszykluskonfiguration

Als erster Schritt beim Erstellen einer Lebenszykluskonfiguration erstellen Sie eine JSON-Datei mit einem oder mehreren Regeln. Diese JSON-Datei enthält beispielsweise drei Regeln:

1. Regel 1 gilt nur für Objekte, die mit dem Präfix übereinstimmen `category1/` Und das hat ein `key2` Der Wert von `tag2`. Der `Expiration` Der Parameter gibt an, dass Objekte, die dem Filter entsprechen, um Mitternacht am 22. August 2020 ablaufen.
2. Regel 2 gilt nur für Objekte, die mit dem Präfix übereinstimmen `category2/`. Der `Expiration` Parameter gibt an, dass Objekte, die dem Filter entsprechen, 100 Tage nach der Aufnahme ablaufen.

   > Regeln, die eine Anzahl von Tagen angeben, sind relativ zu dem Zeitpunkt, an dem das Objekt aufgenommen wurde. Wenn das aktuelle Datum das Aufnahmedatum plus die Anzahl der Tage überschreitet, werden einige Objekte möglicherweise aus dem Bucket entfernt, sobald die Lebenszykluskonfiguration angewendet wird.

3. Regel 3 gilt nur für Objekte, die dem Präfix entsprechen `category3/`. Der `Expiration` Parameter gibt an, dass nicht aktuelle Versionen übereinstimmender Objekte 50 Tage nach deren Nichtstrom ablaufen.

```
{
    "Rules": [
        {
            "ID": "rule1",
            "Filter": {
                "And": {
                    "Prefix": "category1/",
                    "Tags": [
                        {
                            "Key": "key2",
                            "Value": "tag2"
                        }
                    ]
                }
            },
            "Expiration": {
                "Date": "2020-08-22T00:00:00Z"
            },
            "Status": "Enabled"
        },
        {
            "ID": "rule2",
            "Filter": {
                "Prefix": "category2/"
            },
            "Expiration": {
                "Days": 100
            },
            "Status": "Enabled"
        },
        {
            "ID": "rule3",
            "Filter": {
                "Prefix": "category3/"
            },
            "NoncurrentVersionExpiration": {
                "NoncurrentDays": 50
            },
            "Status": "Enabled"
        }
    ]
}
```

Anwenden einer Lebenszykluskonfiguration auf einen Bucket

Nachdem Sie die Lifecycle-Konfigurationsdatei erstellt haben, wenden Sie sie durch Ausgabe einer PUT Bucket Lifecycle-Anforderung auf einen Bucket an.

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

```
aws s3api --endpoint-url <StorageGRID endpoint> put-bucket-lifecycle-
configuration
--bucket testbucket --lifecycle-configuration file://bktjson.json
```

Um zu überprüfen, ob eine Lifecycle-Konfiguration erfolgreich auf den Bucket angewendet wurde, geben Sie eine ANFORDERUNG FÜR DEN GET Bucket-Lebenszyklus aus. Beispiel:

```
aws s3api --endpoint-url <StorageGRID endpoint> get-bucket-lifecycle-
configuration
 --bucket testbucket
```

Eine erfolgreiche Antwort zeigt die Konfiguration des Lebenszyklus, die Sie gerade angewendet haben.

Überprüfung, ob der Bucket-Lebenszyklus für ein Objekt gilt

Sie können feststellen, ob eine Ablaufregel in der Lebenszykluskonfiguration auf ein bestimmtes Objekt angewendet wird, wenn Sie eine PUT-Objekt-, HEAD-Objekt- oder GET-Objektanforderung ausgeben. Wenn eine Regel zutrifft, enthält die Antwort ein `Expiration` Parameter, der angibt, wann das Objekt abläuft und welche Ablaufregel übereinstimmt.

> Da der Bucket-Lebenszyklus ILM überschreibt, wird der `expiry-date` Hier wird das tatsächliche Datum angezeigt, an dem das Objekt gelöscht wird. Weitere Informationen finden Sie unter „`wie die Aufbewahrung von Objekten bestimmt wird`“ in den Anweisungen zur Durchführung der StorageGRID-Administration.

Zum Beispiel, diese PUT Objekt Anfrage wurde am 22. Juni 2020 und platziert ein Objekt in der `testbucket` Eimer.

```
aws s3api --endpoint-url <StorageGRID endpoint> put-object
--bucket testbucket --key obj2test2 --body bktjson.json
```

Die Erfolgsreaktion zeigt an, dass das Objekt in 100 Tagen (01. Oktober 2020) abläuft und dass es mit Regel 2 der Lebenszykluskonfiguration übereinstimmt.

```
{
      *"Expiration": "expiry-date=\"Thu, 01 Oct 2020 09:07:49 GMT\", rule-
id=\"rule2\"",
      "ETag": "\"9762f8a803bc34f5340579d4446076f7\""
}
```

Diese HEAD Object-Anfrage wurde beispielsweise verwendet, um Metadaten für dasselbe Objekt im Testbucket zu erhalten.

```
aws s3api --endpoint-url <StorageGRID endpoint> head-object
--bucket testbucket --key obj2test2
```

Die Erfolgsreaktion umfasst die Metadaten des Objekts und gibt an, dass das Objekt in 100 Tagen abläuft und dass es mit Regel 2 übereinstimmt.

```
{
      "AcceptRanges": "bytes",
      *"Expiration": "expiry-date=\"Thu, 01 Oct 2020 09:07:48 GMT\", rule-
id=\"rule2\"",
      "LastModified": "2020-06-23T09:07:48+00:00",
      "ContentLength": 921,
      "ETag": "\"9762f8a803bc34f5340579d4446076f7\""
      "ContentType": "binary/octet-stream",
      "Metadata": {}
}
```

Verwandte Informationen

"Operationen auf Buckets"

"Objektmanagement mit ILM"

Benutzerdefinierte Vorgänge für Buckets

Das StorageGRID System unterstützt benutzerdefinierte Bucket-Vorgänge, die der S3-REST-API hinzugefügt wurden und sich speziell auf das System bezieht.

In der folgenden Tabelle sind die von StorageGRID unterstützten benutzerdefinierten Bucket-Vorgänge aufgeführt.

Betrieb	Beschreibung	Finden Sie weitere Informationen
Get Bucket-Konsistenz	Gibt die auf einen bestimmten Bucket angewendete Konsistenzstufe zurück.	"Get Bucket-Konsistenzanforderung"

Betrieb	Beschreibung	Finden Sie weitere Informationen
PUT Bucket-Konsistenz	Legt die Konsistenzstufe für einen bestimmten Bucket fest.	"PUT Bucket-Konsistenzanforderung"
ZEITPUNKT des letzten Zugriffs FÜR den Bucket ABRUFEN	Gibt an, ob Updates der letzten Zugriffszeit für einen bestimmten Bucket aktiviert oder deaktiviert wurden.	"Anforderung der Uhrzeit des letzten Bucket-Zugriffs ABRUFEN"
PUT Bucket-Zeit für den letzten Zugriff	Hiermit können Sie Updates der letzten Zugriffszeit für einen bestimmten Bucket aktivieren oder deaktivieren.	"PUT Anforderung der Uhrzeit des letzten Bucket-Zugriffs"
Konfiguration für die Benachrichtigung über Bucket-Metadaten LÖSCHEN	Löscht die XML-Konfiguration für die Metadatenbenachrichtigung, die mit einem bestimmten Bucket verknüpft ist.	"Konfigurationsanforderung für Bucket-Metadaten-Benachrichtigungen LÖSCHEN"
Konfiguration der Bucket-Metadaten-Benachrichtigungen ABRUFEN	Gibt die XML-XML-Benachrichtigungskonfiguration für Metadaten zurück, die einem bestimmten Bucket zugeordnet ist.	"Konfigurationsanforderung FÜR Bucket-Metadaten-Benachrichtigungen ABRUFEN"
PUT Bucket-Metadaten-Benachrichtigungskonfiguration	Konfiguriert den Metadaten-Benachrichtigungsdienst für einen Bucket	"PUT Anforderung der Bucket-Metadaten-Benachrichtigung"
Bucket-Änderungen für Compliance	Veraltet und nicht unterstützt: Sie können keine neuen Buckets mit aktivierter Compliance mehr erstellen.	"Veraltet: PUT Bucket-Request-Änderungen aus Compliance-Gründen"
Bucket-Compliance	Veraltet, aber unterstützt: Gibt die Compliance-Einstellungen zurück, die derzeit für einen vorhandenen Legacy-konformen Bucket wirksam sind.	"Veraltet: GET Bucket-Compliance-Anforderung"
BUCKET-Compliance	Veraltet, aber unterstützt: Ermöglicht es Ihnen, die Compliance-Einstellungen für einen vorhandenen, älteren konformen Bucket zu ändern.	"Veraltet: PUT Bucket-Compliance-Anforderung"

Verwandte Informationen

"S3-Vorgänge werden in den Audit-Protokollen protokolliert"

Operationen für Objekte

In diesem Abschnitt wird beschrieben, wie das StorageGRID System S3-REST-API-Vorgänge für Objekte implementiert.

- "Verwenden der S3-Objektsperre"
- "Mit Servver-seitiger Verschlüsselung"
- "GET Objekt"
- "HEAD Objekt"
- "WIEDERHERSTELLUNG VON POSTOBJEKTEN"
- "PUT Objekt"
- "PUT Objekt - Kopieren"

Die folgenden Bedingungen gelten für alle Objektvorgänge:

- StorageGRID Consistency Controls werden von allen Operationen für Objekte unterstützt, mit Ausnahme der folgenden:
  - GET Objekt-ACL
  - `OPTIONS /`
  - LEGALE Aufbewahrung des Objekts EINGEBEN
  - AUFBEWAHRUNG von Objekten
- Widersprüchliche Clientanforderungen, wie z. B. zwei Clients, die in denselben Schlüssel schreiben, werden auf „`latest-WINS`“-Basis gelöst. Der Zeitpunkt für die „`latest-WINS` “ -Bewertung basiert auf dem Zeitpunkt, an dem das StorageGRID System eine bestimmte Anfrage abschließt, und nicht auf dem, wenn S3-Clients einen Vorgang starten.
- Alle Objekte in einem StorageGRID-Bucket sind im Eigentum des Bucket-Inhabers. Dies umfasst Objekte, die von einem anonymen Benutzer oder einem anderen Konto erstellt wurden.
- Auf Datenobjekte, die über Swift in das StorageGRID-System aufgenommen werden, kann nicht über S3 zugegriffen werden.

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

Betrieb	Implementierung
Objekt LÖSCHEN	Multi-Faktor Authentication (MFA) und Response Header `x-amz-mfa` Werden nicht unterstützt. Bei der Verarbeitung einer LÖSCHOBJEKTANFORDERUNG versucht StorageGRID, alle Kopien des Objekts sofort von allen gespeicherten Speicherorten zu entfernen. Wenn erfolgreich, gibt StorageGRID sofort eine Antwort an den Client zurück. Falls nicht alle Kopien innerhalb von 30 Sekunden entfernt werden können (z. B. weil ein Standort vorübergehend nicht verfügbar ist), warteschlangen StorageGRID die Kopien zum Entfernen und zeigen dann den Erfolg des Clients an. **Versionierung** Um eine bestimmte Version zu entfernen, muss der Anforderer der Bucket-Eigentümer sein und den verwenden `versionId` unterressource. Durch die Verwendung dieser Unterressource wird die Version dauerhaft gelöscht. Wenn der `versionId` Entspricht einer Löschen-Markierung, dem Antwortkopf `x-amz-delete-marker` Wird auf festgelegt `true`. • Wird ein Objekt ohne gelöscht `versionId` unterressource auf einem Bucket mit Versionsfunktion führt zur Generierung einer Löschmarkierung. Der `versionId` Für die Löschen-Markierung wird mit dem zurückgegeben `x-amz-version-id` Kopfzeile der Antwort und das `x-amz-delete-marker` Der Antwortkopf wird auf festgelegt `true`. • Wird ein Objekt ohne gelöscht `versionId` unterressource in einem Version suspended Bucket führt es zu einer dauerhaften Löschung einer bereits vorhandenen 'null' Version oder eines 'null' Löschmarker und der Generierung eines neuen 'null' Löschmarker. Der `x-amz-delete-marker` Der Antwortkopf wird auf festgelegt `true`. **Hinweis**: In bestimmten Fällen können für ein Objekt mehrere Löschen-Marker vorhanden sein.
LÖSCHEN Sie mehrere Objekte	Multi-Faktor Authentication (MFA) und Response Header `x-amz-mfa` Werden nicht unterstützt. In derselben Anforderungsmeldung können mehrere Objekte gelöscht werden.

Betrieb	Implementierung
Objekt-Tagging LÖSCHEN	Verwendet das `tagging` unterressource, um alle Tags aus einem Objekt zu entfernen. Wird mit dem gesamten Amazon S3-REST-API-Verhalten implementiert. **Versionierung** Wenn der `versionId` Der Abfrageparameter wird in der Anforderung nicht angegeben. Der Vorgang löscht alle Tags von der neuesten Version des Objekts in einem versionierten Bucket. Wenn die aktuelle Version des Objekts ein Löschen-Marker ist, wird mit dem ein Status „`MethodNotAllowed`“ zurückgegeben `x-amz-delete-marker` Antwortkopfzeile auf gesetzt `true`.
GET Objekt	"GET Objekt"
GET Objekt-ACL	Wenn für das Konto die erforderlichen Zugangsdaten bereitgestellt werden, gibt der Vorgang eine positive Antwort und die ID, DisplayName und die Berechtigung des Objekteigentümers zurück und gibt an, dass der Eigentümer vollen Zugriff auf das Objekt hat.
HOLD-Aufbewahrung für Objekte	"Verwenden der S3-Objektsperre"
Aufbewahrung von Objekten	"Verwenden der S3-Objektsperre"
GET Objekt-Tagging	Verwendet das `tagging` unterressource, um alle Tags für ein Objekt zurückzugeben. Wird mit dem gesamten Amazon S3-REST-API-Verhalten implementiert **Versionierung** Wenn der `versionId` Der Abfrageparameter wird in der Anforderung nicht angegeben. Der Vorgang gibt alle Tags der neuesten Version des Objekts in einem versionierten Bucket zurück. Wenn die aktuelle Version des Objekts ein Löschen-Marker ist, wird mit dem ein Status „`MethodNotAllowed`“ zurückgegeben `x-amz-delete-marker` Antwortkopfzeile auf gesetzt `true`.
HEAD Objekt	"HEAD Objekt"
WIEDERHERSTELLUNG VON POSTOBJEKTEN	"WIEDERHERSTELLUNG VON POSTOBJEKTEN"

Betrieb	Implementierung
PUT Objekt	"PUT Objekt"
PUT Objekt - Kopieren	"PUT Objekt - Kopieren"
LEGALE Aufbewahrung des Objekts EINGEBEN	"Verwenden der S3-Objektsperre"
AUFBEWAHRUNG von Objekten	"Verwenden der S3-Objektsperre"

Betrieb	Implementierung
PUT Objekt-Tagging	Verwendet das `tagging` unterressource, um einem vorhandenen Objekt einen Satz von Tags hinzuzufügen. Wird mit dem gesamten Amazon S3-REST-API-Verhalten implementiert **Tag-Updates und Aufnahmeverhalten** Wenn Sie PUT Objekt-Tagging zum Aktualisieren der Tags eines Objekts verwenden, nimmt StorageGRID das Objekt nicht erneut auf. Das bedeutet, dass die in der übereinstimmenden ILM-Regel angegebene Option für das Aufnahmeverhalten nicht verwendet wird. Sämtliche durch das Update ausgelösten Änderungen an der Objektplatzierung werden vorgenommen, wenn ILM durch normale ILM-Prozesse im Hintergrund neu bewertet wird. Das bedeutet, dass, wenn die ILM-Regel die strikte Option für das Ingest-Verhalten verwendet, keine Maßnahmen ergriffen werden, wenn die erforderlichen Objektplatzierungen nicht durchgeführt werden können (z. B. weil ein neu benötigter Speicherort nicht verfügbar ist). Das aktualisierte Objekt behält seine aktuelle Platzierung bei, bis die erforderliche Platzierung möglich ist. • Konflikte lösen* Widersprüchliche Clientanforderungen, wie z. B. zwei Clients, die in denselben Schlüssel schreiben, werden auf „`latest-WINS`“-Basis gelöst. Der Zeitpunkt für die „`latest-WINS` “ -Bewertung basiert auf dem Zeitpunkt, an dem das StorageGRID System eine bestimmte Anfrage abschließt, und nicht auf dem, wenn S3-Clients einen Vorgang starten. **Versionierung** Wenn der `versionId` Der Abfrageparameter wird in der Anforderung nicht angegeben, und der Vorgang fügt Tags zur aktuellen Version des Objekts in einem versionierten Bucket hinzu. Wenn die aktuelle Version des Objekts ein Löschen-Marker ist, wird mit dem ein Status „`MethodNotAllowed`“ zurückgegeben `x-amz-delete-marker` Antwortkopfzeile auf gesetzt `true`.

Verwandte Informationen

"Konsistenzkontrollen"

"S3-Vorgänge werden in den Audit-Protokollen protokolliert"

Wenn die globale S3-Objektsperre für Ihr StorageGRID System aktiviert ist, können Sie Buckets mit aktivierter S3-Objektsperre erstellen und dann für jede zu diesem Bucket addieren Objektversion noch bis dato und Legal-Hold-Einstellungen festlegen.

Mit S3 Object Lock können Sie Einstellungen auf Objektebene angeben, um das Löschen oder Überschreiben von Objekten für einen bestimmten Zeitraum oder für einen bestimmten Zeitraum zu verhindern.

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.

Aktivieren der S3-Objektsperre für einen Bucket

Wenn die globale S3-Objektsperreneinstellung für Ihr StorageGRID-System aktiviert ist, können Sie bei der Erstellung jedes Buckets optional die S3-Objektsperre aktivieren. Sie können eine der folgenden Methoden verwenden:

- Erstellen Sie den Bucket mit Tenant Manager.

  "Verwenden Sie ein Mandantenkonto"

- Erstellen Sie den Bucket mithilfe einer PUT-Bucket-Anforderung zusammen mit dem `x-amz-bucket-object-lock_enabled` Kopfzeile der Anfrage.

  "Operationen auf Buckets"

Sie können S3 Object Lock nicht hinzufügen oder deaktivieren, nachdem der Bucket erstellt wurde. Für die S3-Objektsperre ist eine Bucket-Versionierung erforderlich. Diese wird bei der Erstellung des Buckets automatisch aktiviert.

Ein Bucket mit aktivierter S3-Objektsperre kann eine Kombination von Objekten mit und ohne S3-ObjektLock-Einstellungen enthalten. StorageGRID unterstützt nicht die Standard-Aufbewahrung der Objekte in S3 Objektsperren-Buckets, daher wird der Vorgang PUT Object Lock Configuration nicht unterstützt.

Ermitteln, ob die S3-Objektsperre für einen Bucket aktiviert ist

Um festzustellen, ob die S3-Objektsperre aktiviert ist, verwenden Sie die Konfigurationsanforderung FÜR DIE OBJEKTSPERRE ABRUFEN.

"Operationen auf Buckets"

Erstellen eines Objekts mit S3 Object Lock Einstellungen

Zum Festlegen von S3-Objektsperreinstellungen beim Hinzufügen einer Objektversion zu einem Bucket mit aktivierter S3-Objektsperre geben Sie ein PUT-Objekt aus, PUT Object - Copy oder initiieren Sie die Anforderung zum Hochladen mehrerer Teile. Verwenden Sie die folgenden Anfrageheader.

> Sie müssen die S3-Objektsperre aktivieren, wenn Sie einen Bucket erstellen. Sie können S3 Object Lock nicht hinzufügen oder deaktivieren, nachdem ein Bucket erstellt wurde.

- `x-amz-object-lock-mode`, Die COMPLIANCE sein muss (Groß-/Kleinschreibung muss beachtet werden).

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

- `x-amz-object-lock-retain-until-date`
  - Der Wert für „bis-Datum beibehalten“ muss das Format aufweisen `2020-08-10T21:46:00Z`. Fraktionale Sekunden sind zulässig, aber nur 3 Dezimalstellen bleiben erhalten (Präzision in Millisekunden). Andere ISO 8601-Formate sind nicht zulässig.
  - Das „Aufbewahrung bis“-Datum muss in der Zukunft liegen.
- `x-amz-object-lock-legal-hold`

  Wenn die gesetzliche Aufbewahrungspflichten LIEGEN (Groß-/Kleinschreibung muss beachtet werden), wird das Objekt unter einer gesetzlichen Aufbewahrungspflichten platziert. Wenn die gesetzliche Aufbewahrungspflichten AUS DEM WEG gehen, wird keine gesetzliche Aufbewahrungspflichten platziert. Jeder andere Wert führt zu einem 400-Fehler (InvalidArgument).

Wenn Sie eine dieser Anfrageheadern verwenden, beachten Sie die folgenden Einschränkungen:

- Der `Content-MD5` Der Anforderungskopf ist erforderlich `x-amz-object-lock-*` In DER PUT-Objektanforderung ist eine Anforderungsüberschrift vorhanden. `Content-MD5` Ist für PUT Object – Copy oder Initiierung von mehrteiligen Uploads nicht erforderlich.
- Wenn für den Bucket die S3-Objektsperre nicht aktiviert ist und ein `x-amz-object-lock-*` Der Anforderungskopf ist vorhanden, es wird ein 400-Fehler (InvalidRequest) zurückgegeben.
- Die PUT-Objektanforderung unterstützt die Verwendung von `x-amz-storage-class: REDUCED_REDUNDANCY` Passend zum Verhalten von AWS. Wird ein Objekt jedoch mit aktivierter S3-Objektsperre in einen Bucket aufgenommen, führt StorageGRID immer eine Dual-Commit-Aufnahme durch.
- Eine nachfolgende ANTWORT AUF GET- oder HEAD Object-Version enthält die Kopfzeilen `x-amz-object-lock-mode`, `x-amz-object-lock-retain-until-date`, und `x-amz-object-lock-legal-hold`, Wenn konfiguriert und wenn der Anforderungssender die richtige hat `s3:Get*` Berechtigungen.
- Eine Anfrage zur späteren LÖSCHUNG von Objekten oder ZUM LÖSCHEN von Objektversionen schlägt fehl, wenn sie sich vor dem Datum der Aufbewahrung bis zum Datum befindet oder wenn eine gesetzliche Aufbewahrungspflichten vorliegen.

Einstellungen für die S3-Objektsperre werden aktualisiert

Wenn Sie die Einstellungen für die gesetzliche Aufbewahrungs- oder Aufbewahrungseinstellung einer vorhandenen Objektversion aktualisieren müssen, können Sie die folgenden Vorgänge der Unterressource des Objekts ausführen:

- `PUT Object legal-hold`

  Wenn der neue Legal-Hold-Wert AKTIVIERT ist, wird das Objekt unter einer gesetzlichen Aufbewahrungspflichten platziert. Wenn DER Rechtsvorenthalten-Wert DEAKTIVIERT ist, wird die gesetzliche Aufbewahrungspflichten aufgehoben.

- `PUT Object retention`
  - Der Moduswert muss COMPLIANCE sein (Groß-/Kleinschreibung muss beachtet werden).
  - Der Wert für „bis-Datum beibehalten“ muss das Format aufweisen `2020-08-10T21:46:00Z`. Fraktionale Sekunden sind zulässig, aber nur 3 Dezimalstellen bleiben erhalten (Präzision in Millisekunden). Andere ISO 8601-Formate sind nicht zulässig.
  - Wenn eine Objektversion über ein vorhandenes Aufbewahrungsdatum verfügt, können Sie sie nur erhöhen. Der neue Wert muss in der Zukunft liegen.

Verwandte Informationen

"Objektmanagement mit ILM"

"Verwenden Sie ein Mandantenkonto"

"PUT Objekt"

"PUT Objekt - Kopieren"

"Initiieren Von Mehrteiligen Uploads"

"Objektversionierung"

"Amazon Simple Storage Service Benutzerhandbuch: S3 Object Lock verwenden"

Mit serverseitiger Verschlüsselung

Die serverseitige Verschlüsselung schützt Ihre Objektdaten im Ruhezustand. StorageGRID verschlüsselt die Daten beim Schreiben des Objekts und entschlüsselt sie beim Zugriff auf das Objekt.

Wenn Sie die serverseitige Verschlüsselung verwenden möchten, können Sie eine der zwei Optionen auswählen, die sich gegenseitig ausschließen, je nachdem, wie die Verschlüsselungsschlüssel verwaltet werden:

- **SSE (serverseitige Verschlüsselung mit von StorageGRID verwalteten Schlüsseln)**: Bei der Ausgabe einer S3-Anfrage zum Speichern eines Objekts verschlüsselt StorageGRID das Objekt mit einem eindeutigen Schlüssel. Wenn Sie zum Abrufen des Objekts eine S3-Anforderung ausstellen, entschlüsselt StorageGRID das Objekt mithilfe des gespeicherten Schlüssels.
- **SSE-C (serverseitige Verschlüsselung mit vom Kunden bereitgestellten Schlüsseln)**: Wenn Sie eine S3-Anfrage zum Speichern eines Objekts ausgeben, geben Sie Ihren eigenen Verschlüsselungsschlüssel an. Wenn Sie ein Objekt abrufen, geben Sie denselben Verschlüsselungsschlüssel wie in Ihrer Anfrage ein. Stimmen die beiden Verschlüsselungsschlüssel überein, wird das Objekt entschlüsselt und die Objektdaten zurückgegeben.

  StorageGRID managt zwar alle Objektverschlüsselung und Entschlüsselungsvorgänge, muss aber die von Ihnen zur Verfügung gelegten Verschlüsselungsschlüssel verwalten.

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

  > Wenn ein Objekt mit SSE oder SSE-C verschlüsselt wird, werden sämtliche Verschlüsselungseinstellungen auf Bucket- oder Grid-Ebene ignoriert.

Verwenden von SSE

Um ein Objekt mit einem eindeutigen, von StorageGRID gemanagten Schlüssel zu verschlüsseln, verwenden Sie die folgende Anforderungsüberschrift:

```
x-amz-server-side-encryption
```

Der SSE-Anforderungsheader wird durch die folgenden Objektoperationen unterstützt:

- PUT Objekt
- PUT Objekt - Kopieren
- Initiieren Von Mehrteiligen Uploads

SSE-C verwenden

Um ein Objekt mit einem eindeutigen Schlüssel zu verschlüsseln, den Sie verwalten, verwenden Sie drei Anforderungsheader:

Kopfzeile der Anfrage	Beschreibung
`x-amz-server-side-encryption-customer-algorithm`	Geben Sie den Verschlüsselungsalgorithmus an. Der Kopfzeilenwert muss sein `AES256`.
`x-amz-server-side-encryption-customer-key`	Geben Sie den Verschlüsselungsschlüssel an, der zum Verschlüsseln oder Entschlüsseln des Objekts verwendet wird. Der Wert für den Schlüssel muss 256-Bit, base64-codiert sein.
`x-amz-server-side-encryption-customer-key-MD5`	Geben Sie den MD5-Digest des Verschlüsselungsschlüssels gemäß RFC 1321 an, der dafür sorgt, dass der Verschlüsselungsschlüssel fehlerfrei übertragen wurde. Der Wert für das MD5 Digest muss base64-kodiert 128-Bit sein.

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

- GET Objekt
- HEAD Objekt
- PUT Objekt
- PUT Objekt - Kopieren
- Initiieren Von Mehrteiligen Uploads
- Hochladen Von Teilen
- Hochladen Von Teilen - Kopieren

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

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

- Sie müssen https verwenden.

> StorageGRID lehnt alle über http gestellten Anfragen bei der Verwendung von SSE-C. ab Aus Sicherheitsgründen sollten Sie jeden Schlüssel, den Sie versehentlich über http senden, in Betracht ziehen, um kompromittiert zu werden. Entsorgen Sie den Schlüssel, und drehen Sie ihn nach Bedarf.

- Der ETag in der Antwort ist nicht das MD5 der Objektdaten.
- Sie müssen die Zuordnung von Schlüsseln zu Objekten managen. StorageGRID speichert keine Schlüssel. Sie sind für die Nachverfolgung des Verschlüsselungsschlüssels verantwortlich, den Sie für jedes Objekt bereitstellen.
- Wenn Ihr Bucket mit Versionierung aktiviert ist, sollte für jede Objektversion ein eigener Verschlüsselungsschlüssel vorhanden sein. Sie sind verantwortlich für das Tracking des Verschlüsselungsschlüssels, der für jede Objektversion verwendet wird.
- Da Sie Verschlüsselungsschlüssel auf Client-Seite verwalten, müssen Sie auch zusätzliche Schutzmaßnahmen, wie etwa die Rotation von Schlüsseln, auf Client-Seite verwalten.

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

- Wenn die CloudMirror-Replikation für den Bucket konfiguriert ist, können Sie SSE-C-Objekte nicht aufnehmen. Der Aufnahmevorgang schlägt fehl.

Verwandte Informationen

"GET Objekt"

"HEAD Objekt"

"PUT Objekt"

"PUT Objekt - Kopieren"

"Initiieren Von Mehrteiligen Uploads"

"Hochladen Von Teilen"

"Hochladen Von Teilen - Kopieren"

"Amazon S3 Entwicklerleitfaden: Schutz von Daten durch serverseitige Verschlüsselung mit vom Kunden bereitgestellten Verschlüsselungsschlüsseln (SSE-C)"

GET Objekt

Sie können die S3-GET-Objektanfrage verwenden, um ein Objekt aus einem S3-Bucket abzurufen.

Teilenummer-Anforderungsparameter wird nicht unterstützt

Der `partNumber` Der Anforderungsparameter wird für GET-Objektanforderungen nicht unterstützt. Sie können keine Anforderung ZUM ABRUFEN eines bestimmten Teils eines mehrteiligen Objekts ausführen. Ein nicht implementierter Fehler 501 wird mit folgender Meldung zurückgegeben:

```
GET Object by partNumber is not implemented
```

Kopfzeilen zur serverseitigen Verschlüsselung mit vom Kunden bereitgestellten Verschlüsselungsschlüsseln anfordern (SSE-C)

Verwenden Sie alle drei Kopfzeilen, wenn das Objekt mit einem eindeutigen Schlüssel verschlüsselt ist, den Sie angegeben haben.

- `x-amz-server-side-encryption-customer-algorithm`: Angabe `AES256`.
- `x-amz-server-side-encryption-customer-key`: Geben Sie Ihren Verschlüsselungsschlüssel für das Objekt an.
- `x-amz-server-side-encryption-customer-key-MD5`: Geben Sie den MD5-Digest des Verschlüsselungsschlüssels des Objekts an.

> Die von Ihnen zur Verfügung gelegten Schlüssel werden niemals gespeichert. Wenn Sie einen Verschlüsselungsschlüssel verlieren, verlieren Sie das entsprechende Objekt. Bevor Sie vom Kunden zur Sicherung von Objektdaten bereitgestellte Schlüssel verwenden, prüfen Sie die Überlegungen unter „`serverseitige Verschlüsselung verwenden.`“

UTF-8 Zeichen in Benutzermetadaten

StorageGRID parst oder interpretiert die entgangenen UTF-8-Zeichen nicht in benutzerdefinierten Metadaten. ABFRAGEN für ein Objekt mit entgangenen UTF-8 Zeichen in benutzerdefinierten Metadaten WERDEN nicht zurückgegeben `x-amz-missing-meta` Kopfzeile, wenn der Schlüsselname oder -Wert nicht druckbare Zeichen enthält.

Nicht unterstützte Anforderungsüberschrift

Die folgende Anforderungsüberschrift wird nicht unterstützt und kehrt zurück `XNotImplemented`:

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

Versionierung

Wenn A `versionId` unterressource wird nicht angegeben. Der Vorgang ruft die aktuellste Version des Objekts in einem versionierten Bucket ab. Wenn die aktuelle Version des Objekts eine Löschmarkierung ist, wird mit dem ein Status „`not found`“ zurückgegeben `x-amz-delete-marker` Antwortkopfzeile auf gesetzt `true`.

Verhalten DES GET Object für Cloud-Storage-Pool-Objekte

Wenn ein Objekt in einem Cloud-Storage-Pool gespeichert wurde (siehe Anweisungen zum Managen von Objekten mit Information Lifecycle Management), hängt das Verhalten einer GET-Objektanforderung vom Status des Objekts ab. Weitere Informationen finden Sie unter „`HEAD Object`“.

> Wenn ein Objekt in einem Cloud-Storage-Pool gespeichert ist und eine oder mehrere Kopien des Objekts auch im Grid vorhanden sind, werden GET-Objektanfragen versuchen, Daten aus dem Grid abzurufen, bevor sie aus dem Cloud-Storage-Pool abgerufen werden.

Status des Objekts	Verhalten VON GET Object
Objekt, das in StorageGRID aufgenommen wurde, durch ILM jedoch noch nicht evaluiert wurde, oder Objekt, das in einem herkömmlichen Storage-Pool gespeichert ist oder Erasure Coding verwendet	`200 OK` Eine Kopie des Objekts wird abgerufen.
Objekt in Cloud-Storage-Pool, ist aber noch nicht in einen Zustand übergegangen, der nicht abrufbar ist	`200 OK` Eine Kopie des Objekts wird abgerufen.
Das Objekt wurde in einen nicht aufrufbaren Zustand überführt	`403 Forbidden`, `InvalidObjectState` Verwenden Sie eine Wiederherstellungsanforderung FÜR DAS OBJEKT NACH DEM Wiederherstellen, um das Objekt in einen aufrufbaren Zustand wiederherzustellen.
Objekt wird aus einem nicht aufrufbaren Zustand wiederhergestellt	`403 Forbidden`, `InvalidObjectState` Warten Sie, bis die Anforderung zur Wiederherstellung DES POSTOBJEKTS abgeschlossen ist.
Das Objekt wird im Cloud-Storage-Pool vollständig wiederhergestellt	`200 OK` Eine Kopie des Objekts wird abgerufen.

Mehrteilige oder segmentierte Objekte in einem Cloud Storage-Pool

Wenn Sie ein mehrteilige Objekt hochgeladen StorageGRID oder ein großes Objekt in Segmente aufgeteilt haben, bestimmt StorageGRID, ob das Objekt im Cloud-Storage-Pool verfügbar ist, indem Sie eine Teilmenge der Teile oder Segmente des Objekts testen. In manchen Fällen wird eine GET Object-Anforderung möglicherweise falsch zurückgegeben `200 OK` Wenn bereits Teile des Objekts in einen nicht aufrufbaren Zustand überführt wurden oder Teile des Objekts noch nicht wiederhergestellt wurden.

In diesen Fällen:

- Die GET Object-Anforderung gibt möglicherweise einige Daten zurück, stoppt jedoch mitten durch die Übertragung.
- Eine nachfolgende GET Object-Anforderung kann zurückgegeben werden `403 Forbidden`.

Verwandte Informationen

"Mit serverseitiger Verschlüsselung"

"Objektmanagement mit ILM"

"WIEDERHERSTELLUNG VON POSTOBJEKTEN"

"S3-Vorgänge werden in den Audit-Protokollen protokolliert"

HEAD Objekt

Mithilfe der S3 HEAD Object-Anfrage können Metadaten von einem Objekt abgerufen werden, ohne das Objekt selbst zurückzugeben. Wenn das Objekt in einem Cloud Storage Pool gespeichert ist, können Sie MITHILFE VON HEAD Object den Übergangsstatus des Objekts bestimmen.

Kopfzeilen zur serverseitigen Verschlüsselung mit vom Kunden bereitgestellten Verschlüsselungsschlüsseln anfordern (SSE-C)

Verwenden Sie alle drei dieser Kopfzeilen, wenn das Objekt mit einem eindeutigen Schlüssel verschlüsselt ist, den Sie angegeben haben.

- `x-amz-server-side-encryption-customer-algorithm`: Angabe `AES256`.
- `x-amz-server-side-encryption-customer-key`: Geben Sie Ihren Verschlüsselungsschlüssel für das Objekt an.
- `x-amz-server-side-encryption-customer-key-MD5`: Geben Sie den MD5-Digest des Verschlüsselungsschlüssels des Objekts an.

> Die von Ihnen zur Verfügung gelegten Schlüssel werden niemals gespeichert. Wenn Sie einen Verschlüsselungsschlüssel verlieren, verlieren Sie das entsprechende Objekt. Bevor Sie vom Kunden zur Sicherung von Objektdaten bereitgestellte Schlüssel verwenden, prüfen Sie die Überlegungen unter „`serverseitige Verschlüsselung verwenden.`“

UTF-8 Zeichen in Benutzermetadaten

StorageGRID parst oder interpretiert die entgangenen UTF-8-Zeichen nicht in benutzerdefinierten Metadaten. HEAD-Anfragen für ein Objekt mit entgangenen UTF-8 Zeichen in benutzerdefinierten Metadaten geben den nicht zurück `x-amz-missing-meta` Kopfzeile, wenn der Schlüsselname oder -Wert nicht druckbare Zeichen enthält.

Nicht unterstützte Anforderungsüberschrift

Die folgende Anforderungsüberschrift wird nicht unterstützt und kehrt zurück `XNotImplemented`:

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

Antwortkopfzeilen für Cloud-Storage-Pool-Objekte

Wenn das Objekt in einem Cloud-Storage-Pool gespeichert ist (siehe Anweisungen zum Verwalten von Objekten mit Information Lifecycle Management), werden die folgenden Antwortheader zurückgegeben:

- `x-amz-storage-class: GLACIER`
- `x-amz-restore`

Die Antwortheader liefern Informationen zum Status eines Objekts beim Verschieben in einen Cloud Storage Pool, beim Wechsel in einen nicht abrufbaren Zustand und wieder verfügbar.

Status des Objekts	Reaktion auf HEAD Objekt
Objekt, das in StorageGRID aufgenommen wurde, durch ILM jedoch noch nicht evaluiert wurde, oder Objekt, das in einem herkömmlichen Storage-Pool gespeichert ist oder Erasure Coding verwendet	`200 OK` (Es wird keine spezielle Antwortheader zurückgegeben.)

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

Das Objekt ist in den nicht aufrufbaren Zustand übergegangen, aber mindestens eine Kopie ist auch im Grid vorhanden	`200 OK`
	
	`x-amz-storage-class: GLACIER`
	
	`x-amz-restore: ongoing-request="false", expiry-date="Sat, 23 July 20 2030 00:00:00 GMT"`
	
	Der Wert für `expiry-date` Wird in der Zukunft auf eine ferne Zeit gesetzt.
	
	Hinweis: Wenn die Kopie im Raster nicht verfügbar ist (z. B. ein Speicherknoten ist nicht verfügbar), müssen Sie eine ANFRAGE ZUR WIEDERHERSTELLUNG DES POSTOBJEKTS stellen, um die Kopie aus dem Cloud-Speicherpool wiederherzustellen, bevor Sie das Objekt erfolgreich abrufen können.

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

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

Status des Objekts	Reaktion auf HEAD Objekt

Das Objekt wird im Cloud-Storage-Pool vollständig wiederhergestellt	`200 OK`
	
	`x-amz-storage-class: GLACIER`
	
	`x-amz-restore: ongoing-request="false", expiry-date="Sat, 23 July 20 2018 00:00:00 GMT"`
	
	Der `expiry-date` Gibt an, wann das Objekt im Cloud Storage Pool wieder in einen Zustand zurückversetzt werden soll, der nicht abrufbar ist.

Mehrteilige oder segmentierte Objekte in einem Cloud Storage-Pool

Wenn Sie ein mehrteilige Objekt hochgeladen StorageGRID oder ein großes Objekt in Segmente aufgeteilt haben, bestimmt StorageGRID, ob das Objekt im Cloud-Storage-Pool verfügbar ist, indem Sie eine Teilmenge der Teile oder Segmente des Objekts testen. In einigen Fällen wird möglicherweise eine HEAD Object-Anfrage falsch zurückgegeben `x-amz-restore: ongoing-request="false"` Wenn bereits Teile des Objekts in einen nicht aufrufbaren Zustand überführt wurden oder Teile des Objekts noch nicht wiederhergestellt wurden.

Versionierung

Wenn A `versionId` unterressource wird nicht angegeben. Der Vorgang ruft die aktuellste Version des Objekts in einem versionierten Bucket ab. Wenn die aktuelle Version des Objekts eine Löschmarkierung ist, wird mit dem ein Status „`not found`“ zurückgegeben `x-amz-delete-marker` Antwortkopfzeile auf gesetzt `true`.

Verwandte Informationen

"Mit serverseitiger Verschlüsselung"

"Objektmanagement mit ILM"

"WIEDERHERSTELLUNG VON POSTOBJEKTEN"

"S3-Vorgänge werden in den Audit-Protokollen protokolliert"

WIEDERHERSTELLUNG VON POSTOBJEKTEN

Sie können die Wiederherstellungsanforderung für S3-OBJEKTE NACH DEM Posten verwenden, um ein Objekt wiederherzustellen, das in einem Cloud-Storage-Pool gespeichert ist.

Unterstützter Anforderungstyp

StorageGRID unterstützt nur ANFRAGEN zur WIEDERHERSTELLUNG EINES Objekts NACH DEM WIEDERHERSTELLEN. Das unterstützt nicht `SELECT` Art der Wiederherstellung. Wählen Sie Rückgabeanforderungen aus `XNotImplemented`.

Versionierung

Geben Sie optional an `versionId` Zum Wiederherstellen einer bestimmten Version eines Objekts in einem versionierten Bucket Wenn Sie nicht angeben `versionId`, Die neueste Version des Objekts wird wiederhergestellt

Verhalten DER WIEDERHERSTELLUNG NACH Objekten in Cloud-Storage-Pool-Objekten

Wenn ein Objekt in einem Cloud-Storage-Pool gespeichert wurde (siehe Anweisungen zum Managen von Objekten mit Information Lifecycle Management), weist eine Anfrage zur WIEDERHERSTELLUNG NACH dem Objekt auf Basis des Status des Objekts das folgende Verhalten auf. Weitere Informationen finden Sie unter „`HEAD Object`“.

> Wenn ein Objekt in einem Cloud-Storage-Pool gespeichert wird und eine oder mehrere Kopien des Objekts auch im Grid vorhanden sind, muss das Objekt nicht durch eine Wiederherstellungsanforderung FÜR DAS POSTOBJEKT wiederhergestellt werden. Stattdessen kann die lokale Kopie direkt mit Hilfe einer GET Object-Anforderung abgerufen werden.

Status des Objekts	Verhalten DER WIEDERHERSTELLUNG NACH Objekten
Objekt wird in StorageGRID aufgenommen, aber noch nicht durch ILM evaluiert oder Objekt befindet sich nicht in einem Cloud-Storage-Pool	`403 Forbidden`, `InvalidObjectState`
Objekt in Cloud-Storage-Pool, ist aber noch nicht in einen Zustand übergegangen, der nicht abrufbar ist	`200 OK` Es werden keine Änderungen vorgenommen. **Hinweis**: Bevor ein Objekt in einen nicht wiederrufbaren Zustand überführt wurde, können Sie dessen nicht ändern `expiry-date`.
Das Objekt wurde in einen nicht aufrufbaren Zustand überführt	`202 Accepted` Stellt eine abrufbare Kopie des Objekts für die im Anforderungstext angegebene Anzahl an Tagen in den Cloud-Speicher-Pool wieder her. Am Ende dieses Zeitraums wird das Objekt in einen nicht aufrufbaren Zustand zurückgeführt. Verwenden Sie optional den `Tier` Element anfordern, um zu bestimmen, wie lange der Wiederherstellungsauftrag dauern wird (`Expedited`, `Standard`, Oder `Bulk`). Wenn Sie nicht angeben `Tier`, Das `Standard` Tier wird verwendet. **Achtung**: Wenn ein Objekt auf das S3 Glacier Deep Archive migriert wurde oder der Cloud Storage Pool Azure Blob Storage verwendet, kann es nicht über den wiederhergestellt werden `Expedited` Ebene: Der folgende Fehler wird zurückgegeben `403 Forbidden`, `InvalidTier`: `Retrieval option is not supported by this storage class.`

Status des Objekts	Verhalten DER WIEDERHERSTELLUNG NACH Objekten
Objekt wird aus einem nicht aufrufbaren Zustand wiederhergestellt	`409 Conflict`, `RestoreAlreadyInProgress`
Das Objekt wird im Cloud-Storage-Pool vollständig wiederhergestellt	`200 OK` **Hinweis:** Wenn ein Objekt in einen aufrufbaren Zustand wiederhergestellt wurde, können Sie dessen ändern `expiry-date` Indem Sie die Anforderung zur Wiederherstellung DES POSTOBJEKTS mit einem neuen Wert für neu ausgeben `Days`. Das Wiederherstellungsdatum wird zum Zeitpunkt der Anfrage aktualisiert.

Verwandte Informationen

"Objektmanagement mit ILM"

"HEAD Objekt"

"S3-Vorgänge werden in den Audit-Protokollen protokolliert"

PUT Objekt

Sie können die S3 PUT-Objektanforderung verwenden, um einem Bucket ein Objekt hinzuzufügen.

Konflikte lösen

Widersprüchliche Clientanforderungen, wie z. B. zwei Clients, die in denselben Schlüssel schreiben, werden auf „`latest-WINS`“-Basis gelöst. Der Zeitpunkt für die Auswertung „`latest-WINS`“ basiert darauf, wann das StorageGRID System eine bestimmte Anfrage abschließt, und nicht auf, wenn S3-Clients einen Vorgang starten.

Objektgröße

StorageGRID unterstützt Objekte mit einer Größe von bis zu 5 TB.

Größe der Benutzer-Metadaten

Amazon S3 begrenzt die Größe der benutzerdefinierten Metadaten innerhalb jeder PUT-Anforderung-Kopfzeile auf 2 KB. StorageGRID begrenzt die Benutzermetadaten auf 24 KiB. Die Größe der benutzerdefinierten Metadaten wird gemessen, indem die Summe der Anzahl Bytes in der UTF-8-Codierung jedes Schlüssels und jeden Wert angegeben wird.

UTF-8 Zeichen in Benutzermetadaten

Wenn eine Anfrage UTF-8-Werte im Schlüsselnamen oder -Wert der benutzerdefinierten Metadaten enthält, ist das StorageGRID-Verhalten nicht definiert.

StorageGRID parst oder interpretiert keine entgangenen UTF-8-Zeichen, die im Schlüsselnamen oder -Wert

der benutzerdefinierten Metadaten enthalten sind. Entgangenen UTF-8 Zeichen werden als ASCII-Zeichen behandelt:

- PUT-, PUT-Objekt-Copy-, GET- und HEAD-Anforderungen sind erfolgreich, wenn benutzerdefinierte Metadaten entgangenen UTF-8-Zeichen enthalten.
- StorageGRID gibt den nicht zurück `x-amz-missing-meta` Kopfzeile, wenn der interpretierte Wert des Schlüsselnamens oder -Wertes undruckbare Zeichen enthält.

Grenzwerte für Objekt-Tags

Sie können neue Objekte mit Tags hinzufügen, wenn Sie sie hochladen, oder Sie können sie zu vorhandenen Objekten hinzufügen. StorageGRID und Amazon S3 unterstützen bis zu 10 Tags für jedes Objekt. Tags, die einem Objekt zugeordnet sind, müssen über eindeutige Tag-Schlüssel verfügen. Ein Tag-Schlüssel kann bis zu 128 Unicode-Zeichen lang sein, und Tag-Werte können bis zu 256 Unicode-Zeichen lang sein. Bei den Schlüsseln und Werten wird die Groß-/Kleinschreibung beachtet.

Objekteigentümer

In StorageGRID sind alle Objekte Eigentum des Bucket-Besitzers-Kontos, einschließlich der Objekte, die von einem Konto ohne Eigentümer oder einem anonymen Benutzer erstellt wurden.

Unterstützte Anfrageheader

Die folgenden Anfragezeilen werden unterstützt:

- `Cache-Control`
- `Content-Disposition`
- `Content-Encoding`

  Wenn Sie angeben `aws-chunked` Für `Content-Encoding`StorageGRID überprüft die folgenden Elemente nicht:

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

  Die Chunked-Übertragungscodierung wird unterstützt, wenn `aws-chunked` Zudem wird das Nutzlastsignieren verwendet.

- `x-amz-meta-`, Gefolgt von einem Name-Wert-Paar mit benutzerdefinierten Metadaten.

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

Format:

```
x-amz-meta-<em>name</em>: <em>value</em>
```

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

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

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

> Eine ILM-Regel kann nicht sowohl eine **benutzerdefinierte Erstellungszeit** für die Referenzzeit als auch die ausgewogenen oder strengen Optionen für das Aufnahmeverhalten verwenden. Beim Erstellen der ILM-Regel wird ein Fehler zurückgegeben.

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

"Verwenden der S3-Objektsperre"

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

"Unterstützte Vorgänge und Einschränkungen durch S3-REST-API"

Nicht unterstützte Anforderungsheader

Die folgenden Anfragezeilen werden nicht unterstützt:

- Der `x-amz-acl` Die Anforderungsüberschrift wird nicht unterstützt.
- Der `x-amz-website-redirect-location` Die Anforderungsüberschrift wird nicht unterstützt und gibt zurück `XNotImplemented`.

Optionen der Storage-Klasse

Der `x-amz-storage-class` Die Anfrageüberschrift wird unterstützt. Der Wert, der für eingereicht wurde `x-amz-storage-class` Beeinträchtigt, wie StorageGRID Objektdaten während der Aufnahme schützt und nicht

die Anzahl der persistenten Kopien des Objekts im StorageGRID System (das durch ILM bestimmt wird)

Wenn die ILM-Regel, die zu einem aufgenommene Objekt passt, die strikte Option für das Aufnahmeverhalten verwendet, wird der aktiviert `x-amz-storage-class` Kopfzeile hat keine Wirkung.

Für können die folgenden Werte verwendet werden `x-amz-storage-class`:

- `STANDARD` (Standard)
  - **Dual Commit**: Wenn die ILM-Regel die Dual Commit-Option für das Aufnahmeverhalten angibt, sobald ein Objekt aufgenommen wird, wird eine zweite Kopie dieses Objekts erstellt und auf einen anderen Storage Node verteilt (Dual Commit). Nach der Bewertung des ILM bestimmt StorageGRID, ob diese anfänglichen vorläufigen Kopien den Anweisungen zur Platzierung in der Regel entsprechen. Andernfalls müssen möglicherweise neue Objektkopien an verschiedenen Standorten erstellt werden, wobei die anfänglichen vorläufigen Kopien unter Umständen gelöscht werden müssen.
  - **Ausgewogen**: Wenn die ILM-Regel die ausgewogene Option angibt und StorageGRID nicht sofort alle Kopien erstellen kann, die in der Regel angegeben sind, erstellt StorageGRID zwei Zwischenkopien auf unterschiedlichen Storage-Nodes.

    Wenn StorageGRID sofort alle Objektkopien erstellen kann, die in der ILM-Regel (synchrone Platzierung) angegeben sind, wird der angezeigt `x-amz-storage-class` Kopfzeile hat keine Wirkung.

- `REDUCED_REDUNDANCY`
  - **Dual Commit**: Wenn die ILM-Regel die Dual Commit-Option für das Aufnahmeverhalten angibt, erstellt StorageGRID bei Aufnahme des Objekts eine einzelne Interimskopie (Single Commit).
  - **Ausgewogen**: Wenn die ILM-Regel die ausgewogene Option angibt, erstellt StorageGRID nur eine einzige Zwischenkopie, wenn das System nicht sofort alle in der Regel festgelegten Kopien erstellen kann. Wenn StorageGRID eine synchrone Platzierung durchführen kann, hat diese Kopfzeile keine Auswirkung. Der `REDUCED_REDUNDANCY` Am besten eignet sich die Option, wenn die ILM-Regel, die mit dem Objekt übereinstimmt, eine einzige replizierte Kopie erstellt. In diesem Fall verwenden `REDUCED_REDUNDANCY` Eine zusätzliche Objektkopie kann bei jedem Aufnahmevorgang nicht mehr erstellt und gelöscht werden.

  Verwenden der `REDUCED_REDUNDANCY` Unter anderen Umständen wird eine Option nicht empfohlen. `REDUCED_REDUNDANCY` Erhöhte das Risiko von Objektdatenverlusten bei der Aufnahme Beispielsweise können Sie Daten verlieren, wenn die einzelne Kopie zunächst auf einem Storage Node gespeichert wird, der ausfällt, bevor eine ILM-Evaluierung erfolgen kann.

Achtung: Nur eine Kopie für einen beliebigen Zeitraum zu haben bedeutet, dass Daten dauerhaft verloren gehen. Wenn nur eine replizierte Kopie eines Objekts vorhanden ist, geht dieses Objekt verloren, wenn ein Speicherknoten ausfällt oder einen beträchtlichen Fehler hat. Während Wartungsarbeiten wie Upgrades verlieren Sie auch vorübergehend den Zugriff auf das Objekt.

Angeben `REDUCED_REDUNDANCY` Wirkt sich nur darauf aus, wie viele Kopien erstellt werden, wenn ein Objekt zum ersten Mal aufgenommen wird. Er hat keine Auswirkungen auf die Anzahl der Kopien des Objekts, wenn das Objekt von der aktiven ILM-Richtlinie geprüft wird, und führt nicht dazu, dass Daten auf einer niedrigeren Redundanzebene im StorageGRID System gespeichert werden.

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

Anforderungsheader für serverseitige Verschlüsselung

Sie können die folgenden Anforderungsheader verwenden, um ein Objekt mit serverseitiger Verschlüsselung zu verschlüsseln. Die Optionen SSE und SSE-C schließen sich gegenseitig aus.

- **SSE**: Verwenden Sie den folgenden Header, wenn Sie das Objekt mit einem eindeutigen Schlüssel verschlüsseln möchten, der von StorageGRID verwaltet wird.
  - `x-amz-server-side-encryption`
- **SSE-C**: Verwenden Sie alle drei dieser Header, wenn Sie das Objekt mit einem eindeutigen Schlüssel verschlüsseln möchten, den Sie bereitstellen und verwalten.
  - `x-amz-server-side-encryption-customer-algorithm`: Angabe `AES256`.
  - `x-amz-server-side-encryption-customer-key`: Geben Sie Ihren Verschlüsselungsschlüssel für das neue Objekt an.
  - `x-amz-server-side-encryption-customer-key-MD5`: Geben Sie den MD5-Digest des Verschlüsselungsschlüssels des neuen Objekts an.

Achtung: die von Ihnen zur Verfügung stellen Verschlüsselungsschlüssel werden nie gespeichert. Wenn Sie einen Verschlüsselungsschlüssel verlieren, verlieren Sie das entsprechende Objekt. Bevor Sie vom Kunden zur Sicherung von Objektdaten bereitgestellte Schlüssel verwenden, prüfen Sie die Überlegungen unter „`serverseitige Verschlüsselung verwenden.`“

Hinweis: Wenn ein Objekt mit SSE oder SSE-C verschlüsselt ist, werden alle Verschlüsselungseinstellungen auf Bucket-Ebene oder Grid-Ebene ignoriert.

Versionierung

Wenn die Versionierung für einen Bucket aktiviert ist, ist dies ein eindeutiger `versionId` Wird automatisch für die Version des zu speichernden Objekts generiert. Das `versionId` Wird auch in der Antwort mit zurückgegeben `x-amz-version-id` Kopfzeile der Antwort.

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

Verwandte Informationen

"Objektmanagement mit ILM"

"Operationen auf Buckets"

"S3-Vorgänge werden in den Audit-Protokollen protokolliert"

"Mit serverseitiger Verschlüsselung"

"Wie Client-Verbindungen konfiguriert werden können"

PUT Objekt - Kopieren

Sie können das S3 PUT Object – Copy-Request verwenden, um eine Kopie eines Objekts zu erstellen, das bereits in S3 gespeichert ist. Ein PUT Object - Copy-Vorgang ist der gleiche wie ein GET und dann ein PUT.

Konflikte lösen

Widersprüchliche Clientanforderungen, wie z. B. zwei Clients, die in denselben Schlüssel schreiben, werden auf „`latest-WINS`“-Basis gelöst. Der Zeitpunkt für die Auswertung „`latest-WINS`“ basiert darauf, wann das StorageGRID System eine bestimmte Anfrage abschließt, und nicht auf, wenn S3-Clients einen Vorgang starten.

Objektgröße

StorageGRID unterstützt Objekte mit einer Größe von bis zu 5 TB.

UTF-8 Zeichen in Benutzermetadaten

Wenn eine Anfrage UTF-8-Werte im Schlüsselnamen oder -Wert der benutzerdefinierten Metadaten enthält, ist das StorageGRID-Verhalten nicht definiert.

StorageGRID parst oder interpretiert keine entgangenen UTF-8-Zeichen, die im Schlüsselnamen oder -Wert der benutzerdefinierten Metadaten enthalten sind. Entgangenen UTF-8 Zeichen werden als ASCII-Zeichen behandelt:

- Anforderungen sind erfolgreich, wenn benutzerdefinierte Metadaten entgangenen UTF-8 Zeichen enthalten.
- StorageGRID gibt den nicht zurück `x-amz-missing-meta` Kopfzeile, wenn der interpretierte Wert des Schlüsselnamens oder -Wertes undruckbare Zeichen enthält.

Unterstützte Anfrageheader

Die folgenden Anfragezeilen werden unterstützt:

- `Content-Type`
- `x-amz-copy-source`
- `x-amz-copy-source-if-match`
- `x-amz-copy-source-if-none-match`
- `x-amz-copy-source-if-unmodified-since`
- `x-amz-copy-source-if-modified-since`
- `x-amz-meta-`, Gefolgt von einem Name-Wert-Paar mit benutzerdefinierten Metadaten
- `x-amz-metadata-directive`: Der Standardwert ist `COPY`, Mit der Sie das Objekt und die zugehörigen Metadaten kopieren können.

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

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

  Sie können angeben `REPLACE` Um die vorhandenen Tags beim Kopieren des Objekts zu überschreiben oder die Tags zu aktualisieren.

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

"Verwenden der S3-Objektsperre"

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

"Anforderungsheader für serverseitige Verschlüsselung"

Nicht unterstützte Anforderungsheader

Die folgenden Anfragezeilen werden nicht unterstützt:

- `Cache-Control`
- `Content-Disposition`
- `Content-Encoding`
- `Content-Language`
- `Expires`
- `x-amz-website-redirect-location`

Optionen der Storage-Klasse

Der `x-amz-storage-class` Der Anforderungsheader wird unterstützt und hat Auswirkungen auf die Anzahl der Objektkopien, die StorageGRID erstellt, wenn die übereinstimmende ILM-Regel ein Aufnahmeverhalten der doppelten Übertragung oder Ausgewogenheit angibt.

- `STANDARD`

  (Standard) gibt einen Dual-Commit-Aufnahmevorgang an, wenn die ILM-Regel die Option Dual Commit verwendet oder wenn die Option Balance auf das Erstellen von Zwischenkopien zurückgreift.

- `REDUCED_REDUNDANCY`

  Gibt einen Single-Commit-Aufnahmevorgang an, wenn die ILM-Regel die Option Dual Commit verwendet oder wenn die Option Balance zur Erstellung zwischenzeitaler Kopien zurückgreift.

Wenn Sie ein Objekt in einen Bucket aufnehmen, während S3-Objektsperre aktiviert ist, wird das angezeigt `REDUCED_REDUNDANCY` Option wird ignoriert. Wenn Sie ein Objekt in einen Legacy-konformen Bucket aufnehmen, wird der `REDUCED_REDUNDANCY` Option gibt einen Fehler zurück. StorageGRID führt immer eine doppelte Einspeisung durch, um Compliance-Anforderungen zu erfüllen.

Verwenden von x-amz-copy-source in PUT Object - Copy

Wenn der Quell-Bucket und der Schlüssel im angegeben sind `x-amz-copy-source` Kopfzeile: Unterscheidet sich vom Ziel-Bucket und -Schlüssel, eine Kopie der Quell-Objektdaten wird auf das Ziel geschrieben.

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

- SIE können PUT Object – Copy nicht verwenden, um ein vorhandenes Objekt zu verschlüsseln oder die Verschlüsselung eines vorhandenen Objekts zu ändern. Wenn Sie den bereitstellen `x-amz-server-side-encryption` Kopfzeile oder der `x-amz-server-side-encryption-customer-algorithm` Header, StorageGRID lehnt die Anforderung ab und gibt sie zurück `XNotImplemented`.
- Die in der übereinstimmenden ILM-Regel angegebene Option für das Aufnahmeverhalten wird nicht verwendet. Sämtliche durch das Update ausgelösten Änderungen an der Objektplatzierung werden vorgenommen, wenn ILM durch normale ILM-Prozesse im Hintergrund neu bewertet wird.

  Das bedeutet, dass, wenn die ILM-Regel die strikte Option für das Ingest-Verhalten verwendet, keine Maßnahmen ergriffen werden, wenn die erforderlichen Objektplatzierungen nicht durchgeführt werden können (z. B. weil ein neu benötigter Speicherort nicht verfügbar ist). Das aktualisierte Objekt behält seine aktuelle Platzierung bei, bis die erforderliche Platzierung möglich ist.

Anforderungsheader für serverseitige Verschlüsselung

Wenn Sie die serverseitige Verschlüsselung verwenden, hängen die von Ihnen zur Verfügung gestellen Anfrageheadern davon ab, ob das Quellobjekt verschlüsselt ist und ob Sie das Zielobjekt verschlüsseln möchten.

- Wenn das Quellobjekt mit einem vom Kunden bereitgestellten Schlüssel (SSE-C) verschlüsselt wird, müssen Sie die folgenden drei Header in die ANFORDERUNG PUT Object - Copy einschließen, damit das Objekt entschlüsselt und kopiert werden kann:
  - `x-amz-copy-source-server-side-encryption-customer-algorithm` Angeben `AES256`.
  - `x-amz-copy-source-server-side-encryption-customer-key` Geben Sie den Verschlüsselungsschlüssel an, den Sie beim Erstellen des Quellobjekts angegeben haben.
  - `x-amz-copy-source-server-side-encryption-customer-key-MD5`: Geben Sie den MD5-Digest an, den Sie beim Erstellen des Quellobjekts angegeben haben.
- Wenn Sie das Zielobjekt (die Kopie) mit einem eindeutigen Schlüssel verschlüsseln möchten, den Sie bereitstellen und verwalten, müssen Sie die folgenden drei Header angeben:
  - `x-amz-server-side-encryption-customer-algorithm`: Angabe `AES256`.
  - `x-amz-server-side-encryption-customer-key`: Geben Sie einen neuen Verschlüsselungsschlüssel für das Zielobjekt an.

- `x-amz-server-side-encryption-customer-key-MD5`: Geben Sie den MD5-Digest des neuen Verschlüsselungsschlüssels an.

Achtung: die von Ihnen zur Verfügung stellen Verschlüsselungsschlüssel werden nie gespeichert. Wenn Sie einen Verschlüsselungsschlüssel verlieren, verlieren Sie das entsprechende Objekt. Bevor Sie vom Kunden zur Sicherung von Objektdaten bereitgestellte Schlüssel verwenden, prüfen Sie die Überlegungen unter „`serverseitige Verschlüsselung verwenden.`“

- Wenn Sie das Zielobjekt (die Kopie) mit einem eindeutigen Schlüssel verschlüsseln möchten, der von StorageGRID (SSE) verwaltet wird, fügen Sie diesen Header in das PUT Object - Copy Request ein:
  - `x-amz-server-side-encryption`

Hinweis: Das `server-side-encryption` Der Wert des Objekts kann nicht aktualisiert werden. Erstellen Sie stattdessen eine Kopie mit einer neuen `server-side-encryption` Nutzen `x-amz-metadata-directive`: `REPLACE`.

Versionierung

Wenn der Quell-Bucket versioniert ist, können Sie den verwenden `x-amz-copy-source` Kopfzeile zum Kopieren der neuesten Version eines Objekts. Zum Kopieren einer bestimmten Version eines Objekts müssen Sie explizit die Version angeben, die kopiert werden soll `versionId` unterressource. Wenn der Ziel-Bucket versioniert ist, wird die generierte Version im zurückgegeben `x-amz-version-id` Kopfzeile der Antwort. Wenn die Versionierung für den Ziel-Bucket ausgesetzt ist, dann `x-amz-version-id` Gibt einen Wert „`null`“ zurück.

Verwandte Informationen

"Objektmanagement mit ILM"

"Mit serverseitiger Verschlüsselung"

"S3-Vorgänge werden in den Audit-Protokollen protokolliert"

"PUT Objekt"

Vorgänge für mehrteilige Uploads

In diesem Abschnitt wird beschrieben, wie StorageGRID Vorgänge für mehrteilige Uploads unterstützt.

- "Mehrteilige Uploads auflisten"
- "Initiieren Von Mehrteiligen Uploads"
- "Hochladen Von Teilen"
- "Hochladen Von Teilen - Kopieren"
- "Abschließen Von Mehrteiligen Uploads"

Die folgenden Bedingungen und Hinweise gelten für alle mehrteiligen Uploadvorgänge:

- Sie sollten nicht mehr als 1,000 gleichzeitige mehrteilige Uploads in einen einzelnen Bucket durchführen, da die Ergebnisse der „List Multipart Uploads“-Abfragen für diesen Bucket möglicherweise unvollständige Ergebnisse liefern.

- StorageGRID setzt AWS Größenbeschränkungen für mehrere Teile durch. S3-Clients müssen folgende Richtlinien einhalten:
  - Jedes Teil eines mehrteiligen Uploads muss zwischen 5 MiB (5,242,880 Byte) und 5 gib (5,368,709,120 Byte) liegen.
  - Der letzte Teil kann kleiner als 5 MiB (5,242,880 Byte) sein.
  - Im Allgemeinen sollten die Teilemaße so groß wie möglich sein. Verwenden Sie z. B. für ein Objekt mit 100 gib die Teilenummer 5 gib. Da jedes Teil als einzigartiges Objekt betrachtet wird, verringert der StorageGRID-Metadaten-Overhead durch große Teilgrößen.
  - Verwenden Sie für Objekte, die kleiner als 5 gib sind, stattdessen einen Upload ohne mehrere Teile.
- ILM wird für jeden Teil eines mehrteiligen Objekts bei Aufnahme und für das Objekt als Ganzes, wenn der Multipart-Upload abgeschlossen ist, bewertet, wenn die ILM-Regel das strenge oder ausgeglichene Aufnahmeverhalten verwendet. Sie sollten sich bewusst sein, wie dies die Objekt- und Teileplatzierung beeinflusst:
  - Wenn sich ILM-Änderungen während des Hochladen mehrerer S3-Teile ändern, erfüllt der mehrteilige Upload einige Teile des Objekts möglicherweise nicht die aktuellen ILM-Anforderungen. Nicht korrekt platzierte Teile werden zur ILM-Neubewertung in die Warteschlange verschoben und werden später an den richtigen Ort verschoben.
  - Bei der Evaluierung von ILM für ein Teil filtert StorageGRID nach der Größe des Teils und nicht der Größe des Objekts. Das bedeutet, dass Teile eines Objekts an Standorten gespeichert werden können, die die ILM-Anforderungen für das Objekt als Ganzes nicht erfüllen. Wenn z. B. eine Regel angibt, dass alle Objekte ab 10 GB auf DC1 gespeichert werden, während alle kleineren Objekte an DC2 gespeichert sind, wird bei Aufnahme jeder 1 GB-Teil eines 10-teiligen mehrteiligen Uploads auf DC2 gespeichert. Wenn ILM für das Objekt als Ganzes bewertet wird, werden alle Teile des Objekts auf DC1 verschoben.
- Alle mehrteiligen Uploadvorgänge unterstützen die StorageGRID-Konsistenzkontrollen.
- Falls erforderlich, können Sie die Verschlüsselung auf Serverseite mit mehrteiligen Uploads verwenden. Um SSE (serverseitige Verschlüsselung mit über StorageGRID gemanagten Schlüsseln) zu verwenden, müssen Sie das angeben `x-amz-server-side-encryption` Kopfzeile anfordern in der Anfrage zum Senden von mehrteiligen Uploads. Um SSE-C (serverseitige Verschlüsselung mit vom Kunden bereitgestellten Schlüsseln) zu verwenden, geben Sie in der Anfrage zum Hochladen von mehreren Teilen und bei jeder nachfolgenden Anfrage zum Hochladen von Teilen dieselben Schlüsselkopfzeilen an.

Betrieb	Implementierung
Mehrteilige Uploads Auflisten	Siehe "Mehrteilige Uploads Auflisten"
Initiieren Von Mehrteiligen Uploads	Siehe "Initiieren Von Mehrteiligen Uploads"
Hochladen Von Teilen	Siehe "Hochladen Von Teilen"
Hochladen Von Teilen - Kopieren	Siehe "Hochladen Von Teilen - Kopieren"
Abschließen Von Mehrteiligen Uploads	Siehe "Abschließen Von Mehrteiligen Uploads"
Abbrechen Von Mehrteiligen Uploads	Wird mit dem gesamten Amazon S3-REST-API-Verhalten implementiert

Betrieb	Implementierung
Teile Auflisten	Wird mit dem gesamten Amazon S3-REST-API-Verhalten implementiert

Verwandte Informationen

"Konsistenzkontrollen"

"Mit serverseitiger Verschlüsselung"

Mehrteilige Uploads Auflisten

In der Operation „Mehrteilige Uploads auflisten“ werden derzeit mehrteilige Uploads für einen Bucket aufgeführt.

Die folgenden Anforderungsparameter werden unterstützt:

- `encoding-type`
- `max-uploads`
- `key-marker`
- `prefix`
- `upload-id-marker`

Der `delimiter` Der Parameter der Anforderung wird nicht unterstützt.

Versionierung

Mehrteilige Uploads bestehen aus separaten Vorgängen zum Initiieren des Uploads, Auflisten von Uploads, Hochladen von Teilen, Zusammenbauen der hochgeladenen Teile und Abschließen des Uploads. Wenn der Vorgang zum vollständigen Hochladen mehrerer Teile ausgeführt wird, ist dies der Punkt, an dem Objekte erstellt werden (und gegebenenfalls versioniert).

Initiieren Von Mehrteiligen Uploads

Mit dem Vorgang „Mehrteilerupload initiieren“ wird ein mehrtei. Upload für ein Objekt initiiert und eine Upload-ID zurückgegeben.

Der `x-amz-storage-class` Die Anfrageüberschrift wird unterstützt. Der Wert, der für eingereicht wurde `x-amz-storage-class` Beeinträchtigt, wie StorageGRID Objektdaten während der Aufnahme schützt und nicht die Anzahl der persistenten Kopien des Objekts im StorageGRID System (das durch ILM bestimmt wird)

Wenn die ILM-Regel, die zu einem aufgenommene Objekt passt, die strikte Option für das Aufnahmeverhalten verwendet, wird der aktiviert `x-amz-storage-class` Kopfzeile hat keine Wirkung.

Für können die folgenden Werte verwendet werden `x-amz-storage-class`:

- `STANDARD` (Standard)
  - **Dual Commit**: Wenn die ILM-Regel die Dual Commit-Option für das Aufnahmeverhalten angibt, sobald ein Objekt aufgenommen wird, wird eine zweite Kopie dieses Objekts erstellt und auf einen anderen

Storage Node verteilt (Dual Commit). Nach der Bewertung des ILM bestimmt StorageGRID, ob diese anfänglichen vorläufigen Kopien den Anweisungen zur Platzierung in der Regel entsprechen. Andernfalls müssen möglicherweise neue Objektkopien an verschiedenen Standorten erstellt werden, wobei die anfänglichen vorläufigen Kopien unter Umständen gelöscht werden müssen.

- **Ausgewogen**: Wenn die ILM-Regel die ausgewogene Option angibt und StorageGRID nicht sofort alle Kopien erstellen kann, die in der Regel angegeben sind, erstellt StorageGRID zwei Zwischenkopien auf unterschiedlichen Storage-Nodes.

  Wenn StorageGRID sofort alle Objektkopien erstellen kann, die in der ILM-Regel (synchrone Platzierung) angegeben sind, wird der angezeigt `x-amz-storage-class` Kopfzeile hat keine Wirkung.

- `REDUCED_REDUNDANCY`

  - **Dual Commit**: Wenn die ILM-Regel die Dual Commit-Option für das Aufnahmeverhalten angibt, erstellt StorageGRID bei Aufnahme des Objekts eine einzelne Interimskopie (Single Commit).
  - **Ausgewogen**: Wenn die ILM-Regel die ausgewogene Option angibt, erstellt StorageGRID nur eine einzige Zwischenkopie, wenn das System nicht sofort alle in der Regel festgelegten Kopien erstellen kann. Wenn StorageGRID eine synchrone Platzierung durchführen kann, hat diese Kopfzeile keine Auswirkung. Der `REDUCED_REDUNDANCY` Am besten eignet sich die Option, wenn die ILM-Regel, die mit dem Objekt übereinstimmt, eine einzige replizierte Kopie erstellt. In diesem Fall verwenden `REDUCED_REDUNDANCY` Eine zusätzliche Objektkopie kann bei jedem Aufnahmevorgang nicht mehr erstellt und gelöscht werden.

  Verwenden der `REDUCED_REDUNDANCY` Unter anderen Umständen wird eine Option nicht empfohlen. `REDUCED_REDUNDANCY` Erhöhte das Risiko von Objektdatenverlusten bei der Aufnahme Beispielsweise können Sie Daten verlieren, wenn die einzelne Kopie zunächst auf einem Storage Node gespeichert wird, der ausfällt, bevor eine ILM-Evaluierung erfolgen kann.

Achtung: Nur eine Kopie für einen beliebigen Zeitraum zu haben bedeutet, dass Daten dauerhaft verloren gehen. Wenn nur eine replizierte Kopie eines Objekts vorhanden ist, geht dieses Objekt verloren, wenn ein Speicherknoten ausfällt oder einen beträchtlichen Fehler hat. Während Wartungsarbeiten wie Upgrades verlieren Sie auch vorübergehend den Zugriff auf das Objekt.

Angeben `REDUCED_REDUNDANCY` Wirkt sich nur darauf aus, wie viele Kopien erstellt werden, wenn ein Objekt zum ersten Mal aufgenommen wird. Er hat keine Auswirkungen auf die Anzahl der Kopien des Objekts, wenn das Objekt von der aktiven ILM-Richtlinie geprüft wird, und führt nicht dazu, dass Daten auf einer niedrigeren Redundanzebene im StorageGRID System gespeichert werden.

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

Die folgenden Anfragezeilen werden unterstützt:

- `Content-Type`
- `x-amz-meta-`, Gefolgt von einem Name-Wert-Paar mit benutzerdefinierten Metadaten

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

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

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

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

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

> Wird Hinzugefügt `creation-time` Da benutzerdefinierte Metadaten nicht zulässig sind, wenn Sie einem Bucket hinzufügen, auf dem die ältere Compliance aktiviert ist, ein Objekt. Ein Fehler wird zurückgegeben.

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

"Verwenden der S3-Objektsperre"

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

"Unterstützte Vorgänge und Einschränkungen durch S3-REST-API"

> Informationen zum Umgang von UTF-8-Zeichen mit StorageGRID finden Sie in der Dokumentation ZU PUT Object.

Anforderungsheader für serverseitige Verschlüsselung

Sie können die folgenden Anforderungsheader verwenden, um ein mehrteitiges Objekt mit serverseitiger Verschlüsselung zu verschlüsseln. Die Optionen SSE und SSE-C schließen sich gegenseitig aus.

- **SSE**: Verwenden Sie den folgenden Header in der Anfrage Multipart hochladen, wenn Sie das Objekt mit einem eindeutigen Schlüssel verschlüsseln möchten, der von StorageGRID verwaltet wird. Geben Sie diese Kopfzeile in keiner der Anforderungen zum Hochladen von Teilen an.
  - `x-amz-server-side-encryption`
- **SSE-C**: Verwenden Sie alle drei dieser Header in der Anfrage zum Initiate Multipart Upload (und in jeder nachfolgenden Anfrage zum Hochladen von Teilen), wenn Sie das Objekt mit einem eindeutigen Schlüssel verschlüsseln möchten, den Sie bereitstellen und verwalten.

- `x-amz-server-side-encryption-customer-algorithm`: Angabe `AES256`.
- `x-amz-server-side-encryption-customer-key`: Geben Sie Ihren Verschlüsselungsschlüssel für das neue Objekt an.
- `x-amz-server-side-encryption-customer-key-MD5`: Geben Sie den MD5-Digest des Verschlüsselungsschlüssels des neuen Objekts an.

Achtung: die von Ihnen zur Verfügung stellen Verschlüsselungsschlüssel werden nie gespeichert. Wenn Sie einen Verschlüsselungsschlüssel verlieren, verlieren Sie das entsprechende Objekt. Bevor Sie vom Kunden zur Sicherung von Objektdaten bereitgestellte Schlüssel verwenden, prüfen Sie die Überlegungen unter „`serverseitige Verschlüsselung verwenden.`“

Nicht unterstützte Anforderungsheader

Die folgende Anforderungsüberschrift wird nicht unterstützt und kehrt zurück `XNotImplemented`

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

Versionierung

Mehrteilige Uploads bestehen aus separaten Vorgängen zum Initiieren des Uploads, Auflisten von Uploads, Hochladen von Teilen, Zusammenbauen der hochgeladenen Teile und Abschließen des Uploads. Objekte werden erstellt (und gegebenenfalls versioniert), wenn der Vorgang zum Hochladen mehrerer Teile abgeschlossen ist.

Verwandte Informationen

"Objektmanagement mit ILM"

"Mit serverseitiger Verschlüsselung"

"PUT Objekt"

Hochladen Von Teilen

Der Vorgang „Teile hochladen“ lädt ein Teil in einem mehrteiligen Upload für ein Objekt hoch.

Unterstützte Anfrageheader

Die folgenden Anfragezeilen werden unterstützt:

- `Content-Length`
- `Content-MD5`

Anforderungsheader für serverseitige Verschlüsselung

Wenn Sie die SSE-C-Verschlüsselung für die Anfrage zum Hochladen von mehreren Teilen angegeben haben, müssen Sie die folgenden Anfrageheader in jede Anfrage zum Hochladen von Teilen angeben:

- `x-amz-server-side-encryption-customer-algorithm`: Angabe `AES256`.
- `x-amz-server-side-encryption-customer-key`: Geben Sie denselben Verschlüsselungsschlüssel an, den Sie in der Anfrage zum Hochladen von mehreren Teilen angegeben haben.

- `x-amz-server-side-encryption-customer-key-MD5`: Geben Sie den gleichen MD5-Digest an, den Sie in der Anfrage zum Hochladen mehrerer Teile angegeben haben.

> Die von Ihnen zur Verfügung gelegten Schlüssel werden niemals gespeichert. Wenn Sie einen Verschlüsselungsschlüssel verlieren, verlieren Sie das entsprechende Objekt. Bevor Sie vom Kunden zur Sicherung von Objektdaten bereitgestellte Schlüssel verwenden, prüfen Sie die Überlegungen unter „`serverseitige Verschlüsselung verwenden.`“

Versionierung

Mehrteilige Uploads bestehen aus separaten Vorgängen zum Initiieren des Uploads, Auflisten von Uploads, Hochladen von Teilen, Zusammenbauen der hochgeladenen Teile und Abschließen des Uploads. Objekte werden erstellt (und gegebenenfalls versioniert), wenn der Vorgang zum Hochladen mehrerer Teile abgeschlossen ist.

Verwandte Informationen

"Mit serverseitiger Verschlüsselung"

Hochladen Von Teilen - Kopieren

Der Vorgang „Teil hochladen – Kopieren“ lädt einen Teil eines Objekts hoch, indem Daten aus einem vorhandenen Objekt als Datenquelle kopiert werden.

Der Vorgang „Hochladen von Teilen – Kopieren“ ist mit dem Verhalten der gesamten Amazon S3-REST-API implementiert.

Diese Anforderung liest und schreibt die Objektdaten, die in angegeben wurden `x-amz-copy-source-range` Innerhalb des StorageGRID-Systems.

Die folgenden Anfragezeilen werden unterstützt:

- `x-amz-copy-source-if-match`
- `x-amz-copy-source-if-none-match`
- `x-amz-copy-source-if-unmodified-since`
- `x-amz-copy-source-if-modified-since`

Anforderungsheader für serverseitige Verschlüsselung

Wenn Sie die SSE-C-Verschlüsselung für die Anfrage zum Hochladen von mehreren Teilen angegeben haben, müssen Sie die folgenden Anforderungsheader auch in jeden Upload Part - Copy request angeben:

- `x-amz-server-side-encryption-customer-algorithm`: Angabe `AES256`.
- `x-amz-server-side-encryption-customer-key`: Geben Sie denselben Verschlüsselungsschlüssel an, den Sie in der Anfrage zum Hochladen von mehreren Teilen angegeben haben.
- `x-amz-server-side-encryption-customer-key-MD5`: Geben Sie den gleichen MD5-Digest an, den Sie in der Anfrage zum Hochladen mehrerer Teile angegeben haben.

Wenn das Quellobjekt mit einem vom Kunden bereitgestellten Schlüssel (SSE-C) verschlüsselt wird, müssen Sie die folgenden drei Header in die Anfrage „Teil hochladen – Kopieren“ aufnehmen, damit das Objekt entschlüsselt und anschließend kopiert werden kann:

- `x-amz-copy-source-server-side-encryption-customer-algorithm`: Angabe `AES256`.
- `x-amz-copy-source-server-side-encryption-customer-key`: Geben Sie den Verschlüsselungsschlüssel an, den Sie beim Erstellen des Quellobjekts angegeben haben.
- `x-amz-copy-source-server-side-encryption-customer-key-MD5`: Geben Sie den MD5-Digest an, den Sie beim Erstellen des Quellobjekts angegeben haben.

> Die von Ihnen zur Verfügung gelegten Schlüssel werden niemals gespeichert. Wenn Sie einen Verschlüsselungsschlüssel verlieren, verlieren Sie das entsprechende Objekt. Bevor Sie vom Kunden zur Sicherung von Objektdaten bereitgestellte Schlüssel verwenden, prüfen Sie die Überlegungen unter „`serverseitige Verschlüsselung verwenden.`“

Versionierung

Mehrteilige Uploads bestehen aus separaten Vorgängen zum Initiieren des Uploads, Auflisten von Uploads, Hochladen von Teilen, Zusammenbauen der hochgeladenen Teile und Abschließen des Uploads. Objekte werden erstellt (und gegebenenfalls versioniert), wenn der Vorgang zum Hochladen mehrerer Teile abgeschlossen ist.

Abschließen Von Mehrteiligen Uploads

Der komplette mehrteilige Upload-Vorgang führt einen mehrteiligen Upload eines Objekts durch, indem die zuvor hochgeladenen Teile zusammengebaut werden.

Konflikte lösen

Widersprüchliche Clientanforderungen, wie z. B. zwei Clients, die in denselben Schlüssel schreiben, werden auf „`latest-WINS`“-Basis gelöst. Der Zeitpunkt für die Auswertung „`latest-WINS`“ basiert darauf, wann das StorageGRID System eine bestimmte Anfrage abschließt, und nicht auf, wenn S3-Clients einen Vorgang starten.

Objektgröße

StorageGRID unterstützt Objekte mit einer Größe von bis zu 5 TB.

Anfragekopfzeilen

Der `x-amz-storage-class` Der Anforderungsheader wird unterstützt und hat Auswirkungen auf die Anzahl der Objektkopien, die StorageGRID erstellt, wenn die übereinstimmende ILM-Regel ein Aufnahmeverhalten der doppelten Übertragung oder Ausgewogenheit angibt.

- `STANDARD`

  (Standard) gibt einen Dual-Commit-Aufnahmevorgang an, wenn die ILM-Regel die Option Dual Commit verwendet oder wenn die Option Balance auf das Erstellen von Zwischenkopien zurückgreift.

- `REDUCED_REDUNDANCY`

  Gibt einen Single-Commit-Aufnahmevorgang an, wenn die ILM-Regel die Option Dual Commit verwendet oder wenn die Option Balance zur Erstellung zwischenzeitaler Kopien zurückgreift.

Wenn Sie ein Objekt in einen Bucket aufnehmen, während S3-Objektsperre aktiviert ist, wird das angezeigt `REDUCED_REDUNDANCY` Option wird ignoriert. Wenn Sie ein Objekt in einen Legacy-konformen Bucket aufnehmen, wird der `REDUCED_REDUNDANCY` Option gibt einen Fehler zurück. StorageGRID führt immer eine doppelte Einspeisung durch, um Compliance-Anforderungen zu erfüllen.

Wenn ein mehrtei. Upload nicht innerhalb von 15 Tagen abgeschlossen wird, wird der Vorgang als inaktiv markiert und alle zugehörigen Daten werden aus dem System gelöscht.

Der `ETag` Der zurückgegebene Wert ist keine MD5-Summe der Daten, sondern folgt der Implementierung der Amazon S3-API `ETag` Wert für mehrteilige Objekte.

Versionierung

Durch diesen Vorgang ist ein mehrtei. Upload abgeschlossen. Wenn die Versionierung für einen Bucket aktiviert ist, wird diese Objektversion nach Abschluss des mehrteiligen Uploads erstellt.

Wenn die Versionierung für einen Bucket aktiviert ist, ist dies ein eindeutiger `versionId` Wird automatisch für die Version des zu speichernden Objekts generiert. Das `versionId` Wird auch in der Antwort mit zurückgegeben `x-amz-version-id` Kopfzeile der Antwort.

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

Wenn die Versionierung für einen Bucket aktiviert ist, erstellt das Abschließen eines mehrteiligen Uploads immer eine neue Version, selbst wenn mehrere Teile gleichzeitig auf denselben Objektschlüssel hochgeladen wurden. Wenn die Versionierung für einen Bucket nicht aktiviert ist, ist es möglich, einen mehrteiligen Upload zu initiieren und dann einen weiteren mehrteiligen Upload zu initiieren und zuerst auf demselben Objektschlüssel abzuschließen. In Buckets, die nicht versioniert sind, hat der mehrteilige Upload, der den letzten Teil abschließt, Vorrang.

Fehlgeschlagene Replikation, Benachrichtigung oder Metadatenbenachrichtigung

Wenn der Bucket, in dem der mehrteilige Upload stattfindet, für einen Plattformdienst konfiguriert ist, ist der mehrteilige Upload erfolgreich, auch wenn die zugehörige Replizierungs- oder Benachrichtigungsaktion fehlschlägt.

In diesem Fall wird im Grid Manager on Total Events (SMTT) ein Alarm ausgelöst. In der Meldung Letztes Ereignis wird „`Fehler beim Veröffentlichen von Benachrichtigungen für Bucket-nameobject key`“ für das letzte Objekt angezeigt, dessen Benachrichtigung fehlgeschlagen ist. (Um diese Meldung anzuzeigen, wählen Sie **Knoten** > ***Speicherknoten*** > **Ereignisse**. Letztes Ereignis oben in der Tabelle anzeigen.) Ereignismeldungen sind auch in aufgeführt `/var/local/log/bycast-err.log`.

Ein Mandant kann die fehlgeschlagene Replizierung oder Benachrichtigung auslösen, indem die Metadaten oder Tags des Objekts aktualisiert werden. Ein Mieter kann die vorhandenen Werte erneut einreichen, um unerwünschte Änderungen zu vermeiden.

Verwandte Informationen

"Objektmanagement mit ILM"

Fehlerantworten

Das StorageGRID System unterstützt alle zutreffenden S3-REST-API-Standardfehlerantworten. Darüber hinaus fügt die StorageGRID Implementierung mehrere individuelle Antworten hinzu.

Unterstützte S3-API-Fehlercodes

Name	HTTP-Status
AccessDenied	403 Verbotene
BadDigest	400 Fehlerhafte Anfrage
BucketAlreadyExists	409 Konflikt
BucketNotEmpty	409 Konflikt
IncompleteBody	400 Fehlerhafte Anfrage
Interner Fehler	500 Fehler Des Internen Servers
InvalidAccessKey ID	403 Verbotene
InvalidArgument	400 Fehlerhafte Anfrage
InvalidBucketName	400 Fehlerhafte Anfrage
InvalidBucketState	409 Konflikt
InvalidDigest	400 Fehlerhafte Anfrage
InvalidVerschlüsselungAlgorithmFehler	400 Fehlerhafte Anfrage
InvalidTeil	400 Fehlerhafte Anfrage
InvalidPartOrder	400 Fehlerhafte Anfrage
InvalidRange	416 Angeforderter Bereich Nicht Zu Unterprüfbar
InvalidRequest	400 Fehlerhafte Anfrage
InvalidStorageClass	400 Fehlerhafte Anfrage
InvalidTag	400 Fehlerhafte Anfrage

Name	HTTP-Status
InvalidURI	400 Fehlerhafte Anfrage
KeyTooLong	400 Fehlerhafte Anfrage
MalformedXML	400 Fehlerhafte Anfrage
MetadataTooLarge	400 Fehlerhafte Anfrage
MethodenAlled	405 Methode Nicht Zulässig
MissingContentLänge	411 Länge Erforderlich
MissingRequestBodyError	400 Fehlerhafte Anfrage
MissingSecurityHeader	400 Fehlerhafte Anfrage
NoSuchBucket	404 Nicht Gefunden
NoSuchKey	404 Nicht Gefunden
NoSuchUpload	404 Nicht Gefunden
NotImplemsted	501 Nicht Implementiert
NoSuchBucketRichtlinien	404 Nicht Gefunden
ObjektLockKonfigurationNotgefundenFehler	404 Nicht Gefunden
Vorbedingungen nicht möglich	412 Voraussetzung Fehlgeschlagen
AnforderungTimeTooSkewed	403 Verbotene
Servicenicht verfügbar	503 Service Nicht Verfügbar
SignalDoesNotMatch	403 Verbotene
TooManyDickets	400 Fehlerhafte Anfrage
UserKeyMustBespezifiziert	400 Fehlerhafte Anfrage

Benutzerdefinierte StorageGRID-Fehlercodes

Name	Beschreibung	HTTP-Status
XBucketLifecycleNotAlled	In einem zuvor konformen Bucket ist die Konfiguration des Bucket-Lebenszyklus nicht zulässig	400 Fehlerhafte Anfrage
XBucketPolicyParseException	Fehler beim Parsen der JSON der empfangenen Bucket-Richtlinie.	400 Fehlerhafte Anfrage
XComplianceKonflict	Vorgang aufgrund von Compliance-Einstellungen abgelehnt.	403 Verbotene
XComplianceReducedRAID-RedundanzVerbotenen	Reduzierte Redundanz ist in einem älteren, konformen Bucket nicht zulässig	400 Fehlerhafte Anfrage
XMaxBucketPolicyLengthexceed	Ihre Richtlinie überschreitet die maximal zulässige Länge der Bucket-Richtlinie.	400 Fehlerhafte Anfrage
XMissingInternRequestHeader	Eine Kopfzeile einer internen Anforderung fehlt.	400 Fehlerhafte Anfrage
XNoSuchBucketCompliance	Für den angegebenen Bucket ist die veraltete Compliance nicht aktiviert.	404 Nicht Gefunden
XNotAcceptable	Die Anforderung enthält mindestens einen Übernehmen-Header, der nicht erfüllt werden konnte.	406 Nicht Akzeptabel
XNotImplemsted	Die von Ihnen gestellte Anfrage beinhaltet Funktionen, die nicht implementiert sind.	501 Nicht Implementiert

StorageGRID S3 REST-API-Operationen

Auf der S3-REST-API wurden Vorgänge hinzugefügt, die speziell für das StorageGRID-System gelten.

Get Bucket-Konsistenzanforderung

Die GET Bucket-Konsistenzanforderung ermöglicht es Ihnen, das auf einen bestimmten Bucket angewendete Konsistenzlevel zu bestimmen.

Die standardmäßigen Konsistenzkontrollen garantieren „Read-after-Write“ für neu erstellte Objekte.

Sie müssen über die berechtigung s3:GetBucketConsistency verfügen oder als Account root vorliegen, um diesen Vorgang abzuschließen.

Anforderungsbeispiel

```
GET /bucket?x-ntap-sg-consistency HTTP/1.1
Date: <em>date</em>
Authorization: <em>authorization string</em>
Host: <em>host</em>
```

Antwort

In der XML-Antwortantwort `<Consistency>` Gibt einen der folgenden Werte zurück:

Konsistenzkontrolle	Beschreibung
Alle	Alle Nodes erhalten die Daten sofort, sonst schlägt die Anfrage fehl.
Stark global	Garantierte Konsistenz bei Lese-nach-Schreibvorgängen für alle Client-Anfragen an allen Standorten.
Stark vor Ort	Garantiert Konsistenz bei Lese-nach-Schreibvorgängen für alle Client-Anfragen innerhalb eines Standorts.
Read-after-New-Write-Funktion	(Standard) konsistente Lese-/Schreibvorgänge für neue Objekte und eventuelle Konsistenz bei Objekt-Updates. Hochverfügbarkeit und garantierte Datensicherung Entspricht den Amazon S3 -Konsistenzgarantien. **Hinweis:** Wenn Ihre Anwendung HEAD Requests für Objekte verwendet, die nicht vorhanden sind, erhalten Sie möglicherweise eine hohe Anzahl von 500 internen Serverfehlern, wenn ein oder mehrere Speicherknoten nicht verfügbar sind. Um diese Fehler zu vermeiden, setzen Sie das Consistency Control auf „`available`“, es sei denn, Sie benötigen Konsistenzgarantien ähnlich wie Amazon S3.
Verfügbar (eventuelle Konsistenz für DEN HAUPTBETRIEB)	Verhält sich wie die Konsistenzstufe „`read-after-New-write`“, bietet aber nur eventuelle Konsistenz für DEN KOPFBETRIEB. Bietet höhere Verfügbarkeit FÜR HEAD-Operationen als „`read-after-New-write`“, wenn Storage Nodes nicht verfügbar sind. Unterschied zu Amazon S3 Konsistenzgarantien nur für HEAD-Operationen.

Antwortbeispiel

```
HTTP/1.1 200 OK
Date: Fri, 18 Sep 2020 01:02:18 GMT
Connection: CLOSE
Server: StorageGRID/11.5.0
x-amz-request-id: 12345
Content-Length: 127
Content-Type: application/xml

<?xml version="1.0" encoding="UTF-8"?>
<Consistency xmlns="http://s3.storagegrid.com/doc/2015-02-01/">read-after-
new-write</Consistency>
```

Verwandte Informationen

"Konsistenzkontrollen"

PUT Bucket-Konsistenzanforderung

In der PUT Bucket-Konsistenzanforderung können Sie die Konsistenzstufe für Operationen angeben, die in einem Bucket durchgeführt werden.

Die standardmäßigen Konsistenzkontrollen garantieren „Read-after-Write“ für neu erstellte Objekte.

Sie müssen über die berechtigung s3:PutBucketConsistency verfügen oder als Account root vorliegen, um diesen Vorgang abzuschließen.

Anfrage

Der `x-ntap-sg-consistency` Parameter muss einen der folgenden Werte enthalten:

Konsistenzkontrolle	Beschreibung
Alle	Alle Nodes erhalten die Daten sofort, sonst schlägt die Anfrage fehl.
Stark global	Garantierte Konsistenz bei Lese-nach-Schreibvorgängen für alle Client-Anfragen an allen Standorten.
Stark vor Ort	Garantiert Konsistenz bei Lese-nach-Schreibvorgängen für alle Client-Anfragen innerhalb eines Standorts.

Konsistenzkontrolle	Beschreibung
Read-after-New-Write-Funktion	(Standard) konsistente Lese-/Schreibvorgänge für neue Objekte und eventuelle Konsistenz bei Objekt-Updates. Hochverfügbarkeit und garantierte Datensicherung Entspricht den Amazon S3 -Konsistenzgarantien. **Hinweis:** Wenn Ihre Anwendung HEAD Requests für Objekte verwendet, die nicht vorhanden sind, erhalten Sie möglicherweise eine hohe Anzahl von 500 internen Serverfehlern, wenn ein oder mehrere Speicherknoten nicht verfügbar sind. Um diese Fehler zu vermeiden, setzen Sie das Consistency Control auf „`available`“, es sei denn, Sie benötigen Konsistenzgarantien ähnlich wie Amazon S3.
Verfügbar (eventuelle Konsistenz für DEN HAUPTBETRIEB)	Verhält sich wie die Konsistenzstufe „`read-after-New-write`“, bietet aber nur eventuelle Konsistenz für DEN KOPFBETRIEB. Bietet höhere Verfügbarkeit FÜR HEAD-Operationen als „`read-after-New-write`“, wenn Storage Nodes nicht verfügbar sind. Unterschied zu Amazon S3 Konsistenzgarantien nur für HEAD-Operationen.

Hinweis: im Allgemeinen sollten Sie den Wert der Consistency consistency consistency control “read-after-New-write” verwenden. Wenn Anforderungen nicht korrekt funktionieren, ändern Sie das Verhalten des Anwendungs-Clients, wenn möglich. Oder konfigurieren Sie den Client so, dass für jede API-Anforderung das Consistency Control angegeben wird. Legen Sie die Consistency Control auf Bucket-Ebene nur als letztes Resort fest.

Anforderungsbeispiel

```
PUT /bucket?x-ntap-sg-consistency=strong-global HTTP/1.1
Date: <em>date</em>
Authorization: <em>authorization string</em>
Host: <em>host</em>
```

Verwandte Informationen

"Konsistenzkontrollen"

Anforderung der Uhrzeit des letzten Bucket-Zugriffs ABRUFEN

In der Anforderung „letzte Bucket-Zugriffszeit“ KÖNNEN Sie festlegen, ob Updates der letzten Zugriffszeit für einzelne Buckets aktiviert oder deaktiviert sind.

Sie müssen über die berechtigung s3:GetBucketLastAccessTime verfügen oder als Kontostamm vorliegen, um diesen Vorgang abzuschließen.

Anforderungsbeispiel

```
GET /bucket?x-ntap-sg-lastaccesstime HTTP/1.1
Date: <em>date</em>
Authorization: <em>authorization string</em>
Host: <em>host</em>
```

Antwortbeispiel

Dieses Beispiel zeigt, dass Updates der letzten Zugriffszeit für den Bucket aktiviert sind.

```
HTTP/1.1 200 OK
Date: Sat, 29 Nov 2015 01:02:18 GMT
Connection: CLOSE
Server: StorageGRID/10.3.0
x-amz-request-id: 12345
Content-Length: 127
Content-Type: application/xml

<?xml version="1.0" encoding="UTF-8"?>
<LastAccessTime xmlns="http://s3.storagegrid.com/doc/2015-02-01/">enabled
</LastAccessTime>
```

PUT Anforderung der Uhrzeit des letzten Bucket-Zugriffs

In der ANFORDERUNG PUT Bucket Last Access Time können Sie Updates der letzten Zugriffszeit für einzelne Buckets aktivieren oder deaktivieren. Durch das Deaktivieren von Updates der letzten Zugriffszeit wird die Performance verbessert. Dies ist die Standardeinstellung für alle Buckets, die mit Version 10.3 oder höher erstellt wurden.

Sie müssen über die s3:PutBucketLastAccessTime-Berechtigung für einen Bucket verfügen oder als Account-Root dienen, um diesen Vorgang abzuschließen.

> Ab StorageGRID Version 10.3 sind Updates der letzten Zugriffszeit für alle neuen Buckets standardmäßig deaktiviert. Wenn Sie Buckets haben, die mit einer früheren Version von StorageGRID erstellt wurden und denen das neue Standardverhalten entsprechen möchten, müssen Sie für jeden dieser früheren Buckets explizit die Updates der letzten Zugriffszeit deaktivieren. Sie können Updates zum letzten Zugriffszeitpunkt mithilfe der Anforderung PUT Bucket Last Access Time, des Checkbox **S3** > **Buckets** > **Letzte Zugriffseinstellung ändern** im Tenant Manager oder der Tenant Management API aktivieren oder deaktivieren.

Wenn Updates der letzten Zugriffszeit für einen Bucket deaktiviert wurden, wird das folgende Verhalten auf die Vorgänge auf dem Bucket angewendet:

- Anforderungen FÜR GET Object, GET Object ACL, GET Object Tagging und HEAD Object aktualisieren die letzte Zugriffszeit nicht. Das Objekt wird zur Bewertung des Information Lifecycle Management (ILM) nicht zu Warteschlangen hinzugefügt.
- PUT Object – Copy and PUT Objekt-Tagging-Anforderungen, die nur die Metadaten aktualisieren, werden

auch die letzte Zugriffszeit aktualisiert. Das Objekt wird Warteschlangen für die ILM-Bewertung hinzugefügt.

- Wenn Updates der letzten Zugriffszeit für den Quell-Bucket deaktiviert sind, AKTUALISIERT PUT Object – Copy Requests nicht die letzte Zugriffszeit für den Quell-Bucket. Das kopierte Objekt wird nicht zu Warteschlangen für die ILM-Bewertung für den Quell-Bucket hinzugefügt. ALLERDINGS FÜR das Ziel PUT Object - Kopieranforderungen immer die letzte Zugriffszeit aktualisieren. Die Kopie des Objekts wird zu Warteschlangen für eine ILM-Bewertung hinzugefügt.
- Abschließen von mehrteiligen Upload-Anfragen, die die letzte Zugriffszeit aktualisieren. Das fertiggestellte Objekt wird zur ILM-Bewertung zu Warteschlangen hinzugefügt.

Beispiele anfordern

Dieses Beispiel ermöglicht die Zeit des letzten Zugriffs für einen Bucket.

```
PUT /bucket?x-ntap-sg-lastaccesstime=enabled HTTP/1.1
Date: <em>date</em>
Authorization: <em>authorization string</em>
Host: <em>host</em>
```

Dieses Beispiel deaktiviert die Zeit des letzten Zugriffs für einen Bucket.

```
PUT /bucket?x-ntap-sg-lastaccesstime=disabled HTTP/1.1
Date: <em>date</em>
Authorization: <em>authorization string</em>
Host: <em>host</em>
```

Verwandte Informationen

"Verwenden Sie ein Mandantenkonto"

Konfigurationsanforderung für Bucket-Metadaten-Benachrichtigungen LÖSCHEN

Mit der Konfigurationsanforderung FÜR DIE BENACHRICHTIGUNG „BUCKET-Metadaten LÖSCHEN“ können Sie den Suchintegrationsdienst für einzelne Buckets deaktivieren, indem Sie die Konfigurations-XML löschen.

Sie müssen über die berechtigung s3:DeleteBucketMetadataNotification für einen Bucket verfügen oder als Account-Root dienen, um diesen Vorgang abzuschließen.

Anforderungsbeispiel

Dieses Beispiel zeigt die Deaktivierung des Suchintegrationsservice für einen Bucket.

```
DELETE /test1?x-ntap-sg-metadata-notification HTTP/1.1
Date: <em>date</em>
Authorization: <em>authorization string</em>
Host: <em>host</em>
```

Konfigurationsanforderung FÜR Bucket-Metadaten-Benachrichtigungen ABRUFEN

Die Konfigurationsanforderung FÜR GET Bucket-Metadaten-Benachrichtigungen ermöglicht es Ihnen, die Konfigurations-XML abzurufen, die zur Konfiguration der Suchintegration für einzelne Buckets verwendet wird.

Sie müssen über die berechtigung s3:GetBucketMetadataNotification verfügen oder als Kontowurzel dienen, um diesen Vorgang abzuschließen.

Anforderungsbeispiel

Diese Anforderung ruft die Konfiguration der Metadatenbenachrichtigung für den Bucket ab `bucket`.

```
GET /bucket?x-ntap-sg-metadata-notification HTTP/1.1
Date: <em>date</em>
Authorization: <em>authorization string</em>
Host: <em>host</em>
```

Antwort

Der Response Body umfasst die Konfiguration der Metadaten-Benachrichtigung für den Bucket. Anhand der Konfiguration der Metadatenbenachrichtigung können Sie festlegen, wie der Bucket für die Suchintegration konfiguriert ist. So können Unternehmen ermitteln, welche Objekte indiziert sind und an welche Endpunkte ihre Objektmetadaten gesendet werden.

```
<MetadataNotificationConfiguration>
    <Rule>
        <ID>Rule-1</ID>
        <Status>rule-status</Status>
        <Prefix>key-prefix</Prefix>
        <Destination>
           <Urn>arn:aws:es:_region:account-
ID_:domain/_mydomain/myindex/mytype_</Urn>
        </Destination>
    </Rule>
    <Rule>
        <ID>Rule-2</ID>
         ...
    </Rule>
     ...
</MetadataNotificationConfiguration>
```

Jede Konfiguration für die Metadatenbenachrichtigung enthält mindestens ein Regeln. Jede Regel gibt die Objekte an, die auf sie angewendet werden, und das Ziel, an dem StorageGRID Objekt-Metadaten senden soll. Ziele müssen mit dem URN eines StorageGRID-Endpunkts angegeben werden.

Name	Beschreibung	Erforderlich
MetadataNotificationKonfiguration	Container-Tag für Regeln zur Angabe von Objekten und Zielen für Metadatenbenachrichtigungen Enthält mindestens ein Regelelement.	Ja.
Regel	Container-Tag für eine Regel, die die Objekte identifiziert, deren Metadaten zu einem bestimmten Index hinzugefügt werden sollen. Regeln mit überlappenden Präfixen werden abgelehnt. Im MetadataNotificationConfiguration Element enthalten.	Ja.
ID	Eindeutige Kennung für die Regel. In das Element Regel aufgenommen.	Nein
Status	Der Status kann „aktiviert“ oder „deaktiviert“ sein. Für deaktivierte Regeln wird keine Aktion durchgeführt. In das Element Regel aufgenommen.	Ja.
Präfix	Objekte, die mit dem Präfix übereinstimmen, werden von der Regel beeinflusst und ihre Metadaten werden an das angegebene Ziel gesendet. Geben Sie ein leeres Präfix an, um alle Objekte zu entsprechen. In das Element Regel aufgenommen.	Ja.
Ziel	Container-Tag für das Ziel einer Regel. In das Element Regel aufgenommen.	Ja.

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

Antwortbeispiel

Die XML, die zwischen dem enthalten ist `<MetadataNotificationConfiguration></MetadataNotificationConfiguration>` tags zeigen, wie die Integration in einen Endpunkt zur Integration der Suchfunktion für den Bucket konfiguriert wird. In diesem Beispiel werden Objektmetadaten an einen Elasticsearch-Index mit dem Namen gesendet `current` Und geben Sie den Namen ein `2017` Das wird in einer AWS-Domäne mit dem Namen gehostet `records`.

```
HTTP/1.1 200 OK
Date: Thu, 20 Jul 2017 18:24:05 GMT
Connection: KEEP-ALIVE
Server: StorageGRID/11.0.0
x-amz-request-id: 3832973499
Content-Length: 264
Content-Type: application/xml

<MetadataNotificationConfiguration>
    <Rule>
        <ID>Rule-1</ID>
        <Status>Enabled</Status>
        <Prefix>2017</Prefix>
        <Destination>
           <Urn>arn:aws:es:us-east-
1:3333333:domain/records/current/2017</Urn>
        </Destination>
    </Rule>
</MetadataNotificationConfiguration>
```

Verwandte Informationen

"Verwenden Sie ein Mandantenkonto"

PUT Anforderung der Bucket-Metadaten-Benachrichtigung

Die Konfigurationsanforderung FÜR PUT Bucket-Metadaten-Benachrichtigungen ermöglicht es Ihnen, den Such-Integrationsservice für einzelne Buckets zu aktivieren. Die XML-XML-Konfiguration für die Metadatenbenachrichtigung, die Sie im Anforderungsindex angeben, gibt die Objekte an, deren Metadaten an den Zielsuchindex gesendet werden.

Sie müssen über die berechtigung s3:PutBucketMetadataNotification für einen Bucket verfügen oder als Account-Root dienen, um diesen Vorgang abzuschließen.

Anfrage

Die Anforderung muss die Konfiguration der Metadatenbenachrichtigung in der Anfraentext enthalten. Jede Konfiguration für die Metadatenbenachrichtigung enthält mindestens ein Regeln. Jede Regel gibt die Objekte an, auf die sie angewendet wird, und das Ziel, an dem StorageGRID Metadaten senden soll.

Objekte können nach dem Präfix des Objektnamens gefiltert werden. Beispielsweise können Sie Metadaten für Objekte mit dem Präfix senden `/images` An ein Ziel und 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 enthielt `test` Und eine zweite Regel für Objekte mit dem Präfix `test2` Nicht erlaubt.

Ziele müssen mit dem URN eines StorageGRID-Endpunkts angegeben werden. Der Endpunkt muss vorhanden sein, wenn die Konfiguration der Metadatenbenachrichtigung gesendet wird oder die Anforderung als fehlschlägt `400 Bad Request`. In der Fehlermeldung steht: `Unable to save the metadata`

notification (search) policy. The specified endpoint URN does not exist: *URN*.

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

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

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

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

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

Beispiele anfordern

Dieses Beispiel zeigt die Aktivierung der Integration von Suchvorgängen für einen Bucket. In diesem Beispiel werden die Objektmetadaten für alle Objekte an dasselbe Ziel gesendet.

```
PUT /test1?x-ntap-sg-metadata-notification HTTP/1.1
Date: <em>date</em>
Authorization: <em>authorization string</em>
Host: <em>host</em>

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

In diesem Beispiel 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.

```
PUT /graphics?x-ntap-sg-metadata-notification HTTP/1.1
Date: <em>date</em>
Authorization: <em>authorization string</em>
Host: <em>host</em>

<MetadataNotificationConfiguration>
    <Rule>
        <ID>Images-rule</ID>
        <Status>Enabled</Status>
        <Prefix>/images</Prefix>
        <Destination>
           <Urn>arn:aws:es:us-east-1:3333333:domain/es-
domain/graphics/imagetype</Urn>
        </Destination>
    </Rule>
    <Rule>
        <ID>Videos-rule</ID>
        <Status>Enabled</Status>
        <Prefix>/videos</Prefix>
        <Destination>
           <Urn>arn:aws:es:us-west-1:22222222:domain/es-
domain/graphics/videotype</Urn>
        </Destination>
    </Rule>
</MetadataNotificationConfiguration>
```

Verwandte Informationen

"Verwenden Sie ein Mandantenkonto"

Vom Suchintegrations-Service generierter JSON

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

Dieses Beispiel zeigt ein Beispiel für den JSON, der generiert werden 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	Beschreibung
Bucket- und Objektinformationen	Eimer	Name des Buckets
Bucket- und Objektinformationen	Taste	Name des Objektschlüssels
Bucket- und Objektinformationen	VersionID	Objektversion für Objekte in versionierten Buckets
Bucket- und Objektinformationen	Werden	Beispielsweise Bucket-Region `us-east-1`
System-Metadaten	Größe	Objektgröße (in Byte) wie für einen HTTP-Client sichtbar
System-Metadaten	md5	Objekt-Hash
Benutzer-Metadaten	Metadaten *`key:value`*	Alle Benutzer-Metadaten des Objekts als Schlüssel-Wert-Paare
Tags	tags *`key:value`*	Alle für das Objekt definierten Objekt-Tags als Schlüsselwert-Paare

Hinweis: für Tags und Benutzer-Metadaten übergibt StorageGRID Daten und Nummern als Strings oder als S3-Ereignisbenachrichtigungen an Elasticsearch. 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.

Storage-Nutzungsanforderung ABRUFEN

Der Antrag ZUR GET Storage-Nutzung gibt Ihnen die Gesamtzahl des verwendeten Storage durch ein Konto und für jeden mit dem Account verknüpften Bucket an.

Die Menge des von einem Konto und seinen Buckets verwendeten Speichers kann durch eine geänderte GET-Service-Anforderung beim abgerufen werden `x-ntap-sg-usage` Abfrageparameter. Die Nutzung des Bucket-Storage wird getrennt von DEN PUT- und LÖSCHANFRAGEN, die vom System verarbeitet werden, nachverfolgt. Es kann zu einer gewissen Verzögerung kommen, bevor die Nutzungswerte auf der Grundlage der Verarbeitung von Anfragen den erwarteten Werten entsprechen, insbesondere wenn das System unter hoher Belastung steht.

StorageGRID versucht standardmäßig, Nutzungsdaten mithilfe einer starken globalen Konsistenz abzurufen. Wenn keine „stabile globale“ Konsistenz erreicht werden kann, versucht StorageGRID, die Nutzungsinformationen in einer starken Konsistenz des Standorts abzurufen.

Sie müssen über die s3:ListAllMyBuchets-Berechtigung verfügen oder als Kontostamm vorliegen, um diese Operation abzuschließen.

Anforderungsbeispiel

```
GET /?x-ntap-sg-usage HTTP/1.1
Date: <em>date</em>
Authorization: <em>authorization string</em>
Host: <em>host</em>
```

Antwortbeispiel

Dieses Beispiel zeigt ein Konto, das vier Objekte und 12 Bytes Daten in zwei Buckets enthält. Jeder Bucket enthält zwei Objekte und sechs Bytes Daten.

```
HTTP/1.1 200 OK
Date: Sat, 29 Nov 2015 00:49:05 GMT
Connection: KEEP-ALIVE
Server: StorageGRID/10.2.0
x-amz-request-id: 727237123
Content-Length: 427
Content-Type: application/xml

<?xml version="1.0" encoding="UTF-8"?>
<UsageResult xmlns="http://s3.storagegrid.com/doc/2015-02-01">
<CalculationTime>2014-11-19T05:30:11.000000Z</CalculationTime>
<ObjectCount>4</ObjectCount>
<DataBytes>12</DataBytes>
<Buckets>
<Bucket>
<Name>bucket1</Name>
<ObjectCount>2</ObjectCount>
<DataBytes>6</DataBytes>
</Bucket>
<Bucket>
<Name>bucket2</Name>
<ObjectCount>2</ObjectCount>
<DataBytes>6</DataBytes>
</Bucket>
</Buckets>
</UsageResult>
```

Versionierung

Jede gespeicherte Objektversion trägt zum bei `ObjectCount` Und `DataBytes` Werte in der Antwort. Markierungen löschen werden dem nicht hinzugefügt `ObjectCount` Gesamt:

Verwandte Informationen

"Konsistenzkontrollen"

Veraltete Bucket-Anforderungen für ältere Compliance

Möglicherweise müssen Sie die StorageGRID S3 REST-API zum Management von Buckets verwenden, die mit der älteren Compliance-Funktion erstellt wurden.

Compliance-Funktion veraltet

Die in früheren StorageGRID-Versionen verfügbare Funktion für die StorageGRID-Konformität ist veraltet und wurde durch S3-Objektsperre ersetzt.

Wenn Sie zuvor die Einstellung für globale Konformität aktiviert haben, wird die globale S3-Objektsperre beim Upgrade auf StorageGRID 11.5 automatisch aktiviert. Neue Buckets können nicht mehr mit aktivierter Compliance erstellt werden. Trotzdem können Sie bei Bedarf die StorageGRID S3 REST-API verwenden, um

alle vorhandenen, älteren, konformen Buckets zu managen.

"Verwenden der S3-Objektsperre"

"Objektmanagement mit ILM"

"NetApp Knowledge Base: Management älterer, konformer Buckets für StorageGRID 11.5"

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

Das SGCompliance XML-Element ist veraltet. Zuvor könnten Sie dieses benutzerdefinierte StorageGRID-Element in das optionale XML-Anforderungsgremium VON PUT Bucket-Anforderungen integrieren, um einen konformen Bucket zu erstellen.

> Die in früheren StorageGRID-Versionen verfügbare Funktion für die StorageGRID-Konformität ist veraltet und wurde durch S3-Objektsperre ersetzt.

"Verwenden der S3-Objektsperre"

"Objektmanagement mit ILM"

"NetApp Knowledge Base: Management älterer, konformer Buckets für StorageGRID 11.5"

Mit aktivierter Compliance können keine neuen Buckets mehr erstellt werden. Die folgende Fehlermeldung wird zurückgegeben, wenn Sie versuchen, die Put Bucket-Anforderung zur Compliance-Erstellung eines neuen Compliance-Buckets zu verwenden:

```
The Compliance feature is deprecated.
Contact your StorageGRID administrator if you need to create new Compliant
buckets.
```

Verwandte Informationen

"Objektmanagement mit ILM"

"Verwenden Sie ein Mandantenkonto"

Veraltet: GET Bucket-Compliance-Anforderung

Die ANFORDERUNG „GET Bucket-Compliance“ ist veraltet. Sie können diese Anforderung jedoch weiterhin verwenden, um die derzeit für einen vorhandenen, älteren, konformen Bucket geltenden Compliance-Einstellungen zu bestimmen.

> Die in früheren StorageGRID-Versionen verfügbare Funktion für die StorageGRID-Konformität ist veraltet und wurde durch S3-Objektsperre ersetzt.

"Verwenden der S3-Objektsperre"

"Objektmanagement mit ILM"

"NetApp Knowledge Base: Management älterer, konformer Buckets für StorageGRID 11.5"

Um diesen Vorgang abzuschließen, müssen Sie über die berechtigung s3:GetBucketCompliance verfügen

oder als Stammverzeichnis für das Konto verfügen.

Anforderungsbeispiel

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

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

Antwortbeispiel

In der XML-Antwortantwort `<SGCompliance>` Führt die für den Bucket verwendeten Compliance-Einstellungen auf. Dieses Beispiel zeigt die Compliance-Einstellungen für einen Bucket, in dem jedes Objekt ein Jahr lang (525,600 Minuten) aufbewahrt wird, beginnend mit der Aufnahme des Objekts in das Grid. Derzeit ist keine gesetzliche Aufbewahrungspflichten auf diesem Bucket vorhanden. Jedes Objekt wird nach einem Jahr automatisch gelöscht.

```
HTTP/1.1 200 OK
Date: <em>date</em>
Connection: <em>connection</em>
Server: StorageGRID/11.1.0
x-amz-request-id: <em>request ID</em>
Content-Length: <em>length</em>
Content-Type: application/xml

<SGCompliance>
  <RetentionPeriodMinutes>525600</RetentionPeriodMinutes>
  <LegalHold>false</LegalHold>
  <AutoDelete>true</AutoDelete>
</SGCompliance>
```

Name	Beschreibung
WiederholungPeriodMinuten	Die Länge des Aufbewahrungszeitraums für Objekte, die diesem Bucket hinzugefügt wurden, in Minuten Der Aufbewahrungszeitraum beginnt, wenn das Objekt in das Raster aufgenommen wird.

Name	Beschreibung
LegalAlte	• Wahr: Dieser Bucket befindet sich derzeit in einer gesetzlichen Aufbewahrungspflichten. Objekte in diesem Bucket können erst gelöscht werden, wenn die gesetzliche Aufbewahrungsphase aufgehoben wurde, auch wenn ihre Aufbewahrungsfrist abgelaufen ist. • Falsch: Dieser Eimer steht derzeit nicht unter einer gesetzlichen Aufbewahrungspflichten. Objekte in diesem Bucket können nach Ablauf ihres Aufbewahrungszeitraums gelöscht werden.
Automatisches Löschen	• Wahr: Die Objekte in diesem Bucket werden automatisch gelöscht, sobald ihre Aufbewahrungsfrist abgelaufen ist, es sei denn, der Bucket unterliegt einer gesetzlichen Aufbewahrungspflichten. • False: Die Objekte in diesem Bucket werden nicht automatisch gelöscht, wenn die Aufbewahrungsfrist abgelaufen ist. Sie müssen diese Objekte manuell löschen, wenn Sie sie löschen müssen.

Fehlerantworten

Wenn der Bucket nicht für konform erstellt wurde, lautet der HTTP-Statuscode für die Antwort `404 Not Found`, Mit einem S3-Fehlercode von `XNoSuchBucketCompliance`.

Verwandte Informationen

"Objektmanagement mit ILM"

"Verwenden Sie ein Mandantenkonto"

Veraltet: PUT Bucket-Compliance-Anforderung

Die PUT Bucket-Compliance-Anforderung ist veraltet. Sie können diese Anforderung jedoch weiterhin verwenden, um die Compliance-Einstellungen für einen vorhandenen Bucket zu ändern, der die Compliance-Anforderungen erfüllt. Sie können beispielsweise einen vorhandenen Bucket auf „Legal Hold“ platzieren oder den Aufbewahrungszeitraum erhöhen.

> Die in früheren StorageGRID-Versionen verfügbare Funktion für die StorageGRID-Konformität ist veraltet und wurde durch S3-Objektsperre ersetzt.

"Verwenden der S3-Objektsperre"

"Objektmanagement mit ILM"

"NetApp Knowledge Base: Management älterer, konformer Buckets für StorageGRID 11.5"

Sie müssen über die s3:PutBucketCompliance-Berechtigung verfügen oder als Kontoroot vorliegen, um diesen Vorgang abzuschließen.

Wenn Sie eine PUT Bucket-Compliance-Anforderung ausgeben, müssen Sie für jedes Feld der Compliance-Einstellungen einen Wert angeben.

Anforderungsbeispiel

In dieser Beispielanforderung werden die Compliance-Einstellungen für den Bucket mit dem Namen geändert `mybucket`. In diesem Beispiel befinden sich die Objekte in `mybucket` Wird nun für zwei Jahre (1,051,200 Minuten) statt für ein Jahr beibehalten, beginnend mit dem Zeitpunkt, an dem das Objekt in das Grid aufgenommen wird. Es gibt keine gesetzliche Aufbewahrungspflichten auf diesem Bucket. Jedes Objekt wird nach zwei Jahren automatisch gelöscht.

```
PUT /mybucket/?x-ntap-sg-compliance HTTP/1.1
Date: <em>date</em>
Authorization: <em>authorization name</em>
Host: <em>host</em>
Content-Length: 152

<SGCompliance>
  <RetentionPeriodMinutes>1051200</RetentionPeriodMinutes>
  <LegalHold>false</LegalHold>
  <AutoDelete>true</AutoDelete>
</SGCompliance>
```

Name	Beschreibung
WiederholungPeriodMinuten	Die Länge des Aufbewahrungszeitraums für Objekte, die diesem Bucket hinzugefügt wurden, in Minuten Der Aufbewahrungszeitraum beginnt, wenn das Objekt in das Raster aufgenommen wird. **Achtung:** Wenn Sie einen neuen Wert für RetentionPeriodMinutes angeben, müssen Sie einen Wert angeben, der der aktuellen Aufbewahrungsdauer des Buckets entspricht oder größer ist. Nach der Festlegung des Aufbewahrungszeitraums des Buckets können Sie diesen Wert nicht verringern; Sie können ihn nur erhöhen.
LegalAlte	• Wahr: Dieser Bucket befindet sich derzeit in einer gesetzlichen Aufbewahrungspflichten. Objekte in diesem Bucket können erst gelöscht werden, wenn die gesetzliche Aufbewahrungsphase aufgehoben wurde, auch wenn ihre Aufbewahrungsfrist abgelaufen ist. • Falsch: Dieser Eimer steht derzeit nicht unter einer gesetzlichen Aufbewahrungspflichten. Objekte in diesem Bucket können nach Ablauf ihres Aufbewahrungszeitraums gelöscht werden.

Name	Beschreibung
Automatisches Löschen	• Wahr: Die Objekte in diesem Bucket werden automatisch gelöscht, sobald ihre Aufbewahrungsfrist abgelaufen ist, es sei denn, der Bucket unterliegt einer gesetzlichen Aufbewahrungspflichten. • False: Die Objekte in diesem Bucket werden nicht automatisch gelöscht, wenn die Aufbewahrungsfrist abgelaufen ist. Sie müssen diese Objekte manuell löschen, wenn Sie sie löschen müssen.

Konsistenzstufe für Compliance-Einstellungen

Wenn Sie die Compliance-Einstellungen für einen S3-Bucket mit EINER PUT-Bucket-Compliance-Anforderung aktualisieren, versucht StorageGRID, die Metadaten des Buckets im Grid zu aktualisieren. Standardmäßig verwendet StorageGRID die Konsistenzstufe **stark global**, um zu gewährleisten, dass alle Datacenter-Standorte und alle Storage-Nodes mit Bucket-Metadaten Lese-/Schreibzugriff für die geänderten Compliance-Einstellungen erhalten.

Wenn StorageGRID die Konsistenzstufe **stark-global** nicht erreichen kann, da ein Datacenter-Standort oder mehrere Speicherknoten an einem Standort nicht verfügbar sind, lautet der HTTP-Statuscode für die Antwort `503 Service Unavailable.`

Wenn Sie diese Antwort erhalten, müssen Sie sich an den Grid-Administrator wenden, um sicherzustellen, dass die erforderlichen Storage-Services so schnell wie möglich verfügbar gemacht werden. Wenn der Grid-Administrator nicht in der Lage ist, an jedem Standort ausreichend Storage-Nodes zur Verfügung zu stellen, wird Sie vom technischen Support möglicherweise dazu gebracht, die ausgefallene Anforderung erneut zu versuchen, indem Sie die Konsistenzstufe für * strong-Site* erzwingen.

> Erzwingen Sie niemals die * Strong-site* Consistency Level für PUT Bucket Compliance, es sei denn, Sie wurden dazu durch den technischen Support angewiesen, und es sei denn, Sie verstehen die möglichen Folgen der Verwendung dieser Ebene.

Wenn die Consistency Level auf **strong-site** reduziert wird, garantiert StorageGRID, dass aktualisierte Compliance-Einstellungen Lese-nach-Write-Konsistenz nur für Client-Anfragen innerhalb einer Site haben. Das bedeutet, dass das StorageGRID System vorübergehend mehrere inkonsistente Einstellungen für diesen Bucket bietet, bis alle Standorte und Storage-Nodes verfügbar sind. Die inkonsistenten Einstellungen können zu unerwarteten und unerwünschten Verhaltensweisen führen. Wenn Sie beispielsweise einen Bucket unter „Legal Hold“ platzieren und Sie eine niedrigere Konsistenzstufe erzwingen, sind die vorherigen Compliance-Einstellungen (d. h. „Legal Hold off“) des Buckets für einige Datacenter-Standorte möglicherweise weiterhin wirksam. Aus diesem Grund können Objekte, die Ihrer Meinung nach in einer gesetzlichen Wartefrist liegen, nach Ablauf ihres Aufbewahrungszeitraums entweder durch den Benutzer oder durch AutoDelete gelöscht werden, sofern diese Option aktiviert ist.

Um die Verwendung der Konsistenzstufe * Strong-site* zu erzwingen, geben Sie die PUT Bucket Compliance-Anforderung erneut aus und schließen Sie die ein `Consistency-Control` HTTP-Request-Header, wie folgt:

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

Fehlerantworten

- Wenn der Bucket nicht für konform erstellt wurde, lautet der HTTP-Statuscode für die Antwort `404 Not Found`.
- Wenn `RetentionPeriodMinutes` In der Anforderung ist kleiner als der aktuelle Aufbewahrungszeitraum des Buckets, lautet der HTTP-Statuscode `400 Bad Request`.

Verwandte Informationen

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

"Verwenden Sie ein Mandantenkonto"

"Objektmanagement mit ILM"

Bucket- und Gruppenzugriffsrichtlinien

StorageGRID verwendet die Richtliniensprache für Amazon Web Services (AWS), um S3-Mandanten die Kontrolle des Zugriffs auf Buckets und Objekte innerhalb dieser Buckets zu ermöglichen. Das StorageGRID System implementiert eine Untermenge der S3-REST-API-Richtliniensprache. Zugriffsrichtlinien für die S3 API werden in JSON geschrieben.

Zugriffsrichtlinien – Überblick

Von StorageGRID werden zwei Arten von Zugriffsrichtlinien unterstützt:

- **Bucket-Richtlinien**, die mit DER GET Bucket-Richtlinie konfiguriert sind, PUT Bucket-Richtlinie und S3-API-Operationen FÜR die Bucket-Richtlinie LÖSCHEN. Bucket-Richtlinien sind mit Buckets verknüpft, so dass sie so konfiguriert sind, dass sie den Zugriff durch Benutzer im Bucket-Eigentümerkonto oder andere Konten an den Bucket und die darin befindlichen Objekte steuern. Eine Bucket-Richtlinie gilt nur für einen Bucket und möglicherweise auch für mehrere Gruppen.
- **Gruppenrichtlinien**, die mit dem Tenant Manager oder der Mandantenmanagement-API konfiguriert sind. Gruppenrichtlinien sind einer Gruppe im Konto zugeordnet, sodass sie so konfiguriert sind, dass sie der Gruppe ermöglichen, auf bestimmte Ressourcen zuzugreifen, die dem Konto gehören. Eine Gruppenrichtlinie gilt nur für eine Gruppe und möglicherweise für mehrere Buckets.

StorageGRID Bucket und Gruppenrichtlinien folgen einer bestimmten Grammatik, die von Amazon definiert wurde. Innerhalb jeder Richtlinie gibt es eine Reihe von Richtlinienerklärungen, und jede Aussage enthält die folgenden Elemente:

- Statement-ID (Sid) (optional)
- Wirkung
- Principal/NotPrincipal
- Ressource/Ressource
- Aktion/Notaktion

- Bedingung (optional)

Richtlinienaussagen werden mithilfe dieser Struktur erstellt, um Berechtigungen anzugeben: <Effekt> gewähren, um <Principal> <Aktion> auf <Ressource> durchzuführen, wenn <Bedingung> angewendet wird.

Jedes Richtlinienelement wird für eine bestimmte Funktion verwendet:

Element	Beschreibung
Sid	Das Sid-Element ist optional. Der Sid ist nur als Beschreibung für den Benutzer gedacht. Diese wird vom StorageGRID System gespeichert, aber nicht interpretiert.
Wirkung	Verwenden Sie das Effektelement, um festzustellen, ob die angegebenen Vorgänge zulässig oder verweigert werden. Sie müssen anhand der Schlüsselwörter für unterstütztes Aktionselement Operationen identifizieren, die für Buckets oder Objekte zugelassen (oder verweigert) werden.
Principal/NotPrincipal	Benutzer, Gruppen und Konten können auf bestimmte Ressourcen zugreifen und bestimmte Aktionen ausführen. Wenn in der Anfrage keine S3-Signatur enthalten ist, ist ein anonymer Zugriff durch Angabe des Platzhalterzeichens (*) als Principal zulässig. Standardmäßig hat nur das Konto-Root Zugriff auf Ressourcen, die dem Konto gehören. Sie müssen nur das Hauptelement in einer Bucket-Richtlinie angeben. Bei Gruppenrichtlinien ist die Gruppe, der die Richtlinie zugeordnet ist, das implizite Prinzipalelement.
Ressource/Ressource	Das Ressourcenelement identifiziert Buckets und Objekte. Sie können Buckets und Objekten über den ARN (Amazon Resource Name) Berechtigungen gewähren oder verweigern, um die Ressource zu identifizieren.
Aktion/Notaktion	Die Elemente Aktion und Wirkung sind die beiden Komponenten von Berechtigungen. Wenn eine Gruppe eine Ressource anfordert, wird ihnen entweder der Zugriff auf die Ressource gewährt oder verweigert. Der Zugriff wird verweigert, es sei denn, Sie weisen ausdrücklich Berechtigungen zu, aber Sie können explizites Ablehnen verwenden, um eine von einer anderen Richtlinie gewährte Berechtigung zu überschreiben.

Element	Beschreibung
Zustand	Das Bedingungselement ist optional. Unter Bedingungen können Sie Ausdrücke erstellen, um zu bestimmen, wann eine Richtlinie angewendet werden soll.

Im Element Aktion können Sie das Platzhalterzeichen (*) verwenden, um alle Vorgänge oder eine Untermenge von Vorgängen anzugeben. Diese Aktion entspricht beispielsweise Berechtigungen wie s3:GetObject, s3:PutObject und s3:DeleteObject.

```
s3:*Object
```

Im Element Ressource können Sie die Platzhalterzeichen (*) und (?) verwenden. Während das Sternchen (*) mit 0 oder mehr Zeichen übereinstimmt, ist das Fragezeichen (?) Entspricht einem beliebigen Zeichen.

Im Principal-Element werden Platzhalterzeichen nicht unterstützt, außer wenn anonymer Zugriff festgelegt wird, der allen die Berechtigung erteilt. Sie legen beispielsweise den Platzhalter (*) als Principal-Wert fest.

```
"Principal":"*"
```

Im folgenden Beispiel verwendet die Anweisung die Elemente „Effekt“, „Principal“, „Aktion“ und „Ressource“. Dieses Beispiel zeigt eine vollständige Bucket-Richtlinienanweisung, die den Principals, die Admin-Gruppe, mit dem Effekt „Zulassen“ erhält `federated-group/admin` Und der Finanzgruppe `federated-group/finance`, Berechtigungen zur Durchführung der Aktion `s3:ListBucket` Auf dem genannten Bucket `mybucket` Und der Aktion `s3:GetObject` Auf allen Objekten in diesem Bucket.

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": [
          "arn:aws:iam::27233906934684427525:federated-group/admin",
          "arn:aws:iam::27233906934684427525:federated-group/finance"
        ]
      },
      "Action": [
        "s3:ListBucket",
        "s3:GetObject"
      ],
      "Resource": [
        "arn:aws:iam:s3:::mybucket",
        "arn:aws:iam:s3:::mybucket/*"
      ]
    }
  ]
}
```

Die Bucket-Richtlinie hat eine Größenbeschränkung von 20,480 Byte, und die Gruppenrichtlinie hat ein Größenlimit von 5,120 Byte.

Verwandte Informationen

"Verwenden Sie ein Mandantenkonto"

Einstellungen zur Konsistenzkontrolle für Richtlinien

Standardmäßig sind alle Aktualisierungen, die Sie an Gruppenrichtlinien vornehmen, letztendlich konsistent. Sobald eine Gruppenrichtlinie konsistent wird, können die Änderungen aufgrund von Richtlinien-Caching weitere 15 Minuten dauern. Standardmäßig sind alle Updates an den Bucket-Richtlinien ebenfalls konsistent.

Sie können bei Bedarf die Konsistenzgarantien für Bucket-Richtlinienaktualisierungen ändern. Beispielsweise könnte eine Änderung an einer Bucket-Richtlinie aus Sicherheitsgründen so schnell wie möglich wirksam werden.

In diesem Fall können Sie entweder die einstellen `Consistency-Control` Kopfzeile in der ANFORDERUNG DER PUT Bucket-Richtlinie, oder Sie können die PUT-Bucket-Konsistenzanforderung verwenden. Wenn Sie die Consistency Control für diese Anfrage ändern, müssen Sie den Wert **all** verwenden, der die höchste Garantie für die Konsistenz von Lesen nach dem Schreiben bietet. Wenn Sie einen anderen Wert für Consistency Control in einer Kopfzeile für die PUT Bucket Consistency Request angeben, wird die Anforderung abgelehnt. Wenn Sie einen anderen Wert für eine PUT Bucket Policy Request angeben, wird der Wert ignoriert. Sobald eine Bucket-Richtlinie konsistent ist, können die Änderungen aufgrund des Richtlinien-Caching weitere 8 Sekunden dauern.

Wenn Sie die Konsistenzstufe auf **alle** setzen, um eine neue Bucket-Richtlinie früher wirksam zu machen, stellen Sie die Bucket-Level-Kontrolle sicher, dass sie wieder auf ihren ursprünglichen Wert zurückgestellt wird, wenn Sie fertig sind. Andernfalls wird für alle zukünftigen Bucket-Anforderungen die **all**-Einstellung verwendet.

Verwenden des ARN in den Richtlinienerklärungen

In den Richtlinienerklärungen wird das ARN in Haupt- und Ressourcenelementen verwendet.

- Verwenden Sie diese Syntax, um die S3-Ressource ARN anzugeben:

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

- Verwenden Sie diese Syntax, um die Identitätressource ARN (Benutzer und Gruppen) festzulegen:

```
arn:aws:iam::account_id:root
arn:aws:iam::account_id:user/user_name
arn:aws:iam::account_id:group/group_name
arn:aws:iam::account_id:federated-user/user_name
arn:aws:iam::account_id:federated-group/group_name
```

Weitere Überlegungen:

- Sie können das Sternchen (*) als Platzhalter verwenden, um Null oder mehr Zeichen im Objektschlüssel zu entsprechen.
- Internationale Zeichen, die im Objektschlüssel angegeben werden können, sollten mit JSON UTF-8 oder mit JSON \U Escape Sequenzen codiert werden. Die prozentuale Kodierung wird nicht unterstützt.

  "RFC 2141 URN Syntax"

  Der HTTP-Anforderungskörper für DEN PUT Bucket-Richtlinienvorgang muss mit charset=UTF-8 codiert werden.

Festlegen von Ressourcen in einer Richtlinie

In Richtlinienausrechnungen können Sie mithilfe des Elements Ressourcen den Bucket oder das Objekt angeben, für das Berechtigungen zulässig oder verweigert werden.

- Jede Richtlinienanweisung erfordert ein Ressourcenelement. In einer Richtlinie werden Ressourcen durch das Element gekennzeichnet `Resource`, Oder alternativ , `NotResource` Für Ausschluss.
- Sie legen Ressourcen mit einer S3-Ressource ARN fest. Beispiel:

```
"Resource": "arn:aws:s3:::mybucket/*"
```

- Sie können Richtlinienvariablen auch innerhalb des Objektschlüssels verwenden. Beispiel:

```
"Resource": "arn:aws:s3:::mybucket/home/${aws:username}/*"
```

- Der Ressourcenwert kann einen Bucket angeben, der beim Erstellen einer Gruppenrichtlinie noch nicht vorhanden ist.

Verwandte Informationen

"Festlegen von Variablen in einer Richtlinie"

Prinzipale in einer Richtlinie angeben

Verwenden Sie das Hauptelement, um das Benutzer-, Gruppen- oder Mandantenkonto zu identifizieren, das über die Richtlinienanweisung Zugriff auf die Ressource erlaubt/verweigert wird.

- Jede Richtlinienanweisung in einer Bucket-Richtlinie muss ein Principal Element enthalten. Richtlinienerklärungen in einer Gruppenpolitik benötigen das Hauptelement nicht, da die Gruppe als Hauptbestandteil verstanden wird.
- In einer Richtlinie werden die Prinzipien durch das Element „`Principal,`“ oder alternativ „`NotPrincipal`“ für den Ausschluss gekennzeichnet.
- Kontobasierte Identitäten müssen mit einer ID oder einem ARN angegeben werden:

```
"Principal": { "AWS": "account_id"}
"Principal": { "AWS": "identity_arn" }
```

- In diesem Beispiel wird die Mandanten-Account-ID 27233906934684427525 verwendet, die das Konto-Root und alle Benutzer im Konto enthält:

```
 "Principal": { "AWS": "27233906934684427525" }
```

- Sie können nur das Konto-Root angeben:

```
"Principal": { "AWS": "arn:aws:iam::27233906934684427525:root" }
```

- Sie können einen bestimmten föderierten Benutzer („Alex“) angeben:

```
"Principal": { "AWS": "arn:aws:iam::27233906934684427525:federated-
user/Alex" }
```

- Sie können eine bestimmte föderierte Gruppe („Manager“) angeben:

```
"Principal": { "AWS": "arn:aws:iam::27233906934684427525:federated-
group/Managers"  }
```

- Sie können einen anonymen Principal angeben:

```
"Principal": "*"
```

- Um Mehrdeutigkeiten zu vermeiden, können Sie die Benutzer-UUID anstelle des Benutzernamens verwenden:

```
arn:aws:iam::27233906934684427525:user-uuid/de305d54-75b4-431b-adb2-
eb6b9e546013
```

  Angenommen, Alex verlässt zum Beispiel die Organisation und den Benutzernamen `Alex` Wird gelöscht. Wenn ein neuer Alex der Organisation beitritt und dem gleichen zugewiesen wird `Alex` Benutzername: Der neue Benutzer erbt möglicherweise unbeabsichtigt die dem ursprünglichen Benutzer gewährten Berechtigungen.

- Der Hauptwert kann einen Gruppen-/Benutzernamen angeben, der beim Erstellen einer Bucket-Richtlinie noch nicht vorhanden ist.

Festlegen von Berechtigungen in einer Richtlinie

In einer Richtlinie wird das Aktionselement verwendet, um Berechtigungen einer Ressource zuzulassen/zu verweigern. Es gibt eine Reihe von Berechtigungen, die Sie in einer Richtlinie festlegen können, die durch das Element „Aktion“ gekennzeichnet sind, oder alternativ durch „NotAction“ für den Ausschluss. Jedes dieser Elemente wird bestimmten S3-REST-API-Operationen zugeordnet.

In den Tabellen werden die Berechtigungen aufgeführt, die auf Buckets angewendet werden, sowie die Berechtigungen, die für Objekte gelten.

Amazon S3 nutzt jetzt die Berechtigung s3:PutReplicationConfiguration sowohl für DIE PUT- als AUCH DELETE-Bucket-Replizierungsaktionen. StorageGRID verwendet für jede Aktion separate Berechtigungen, die mit der ursprünglichen Amazon S3 Spezifikation übereinstimmt.

EIN LÖSCHEN wird ausgeführt, wenn ein PUT zum Überschreiben eines vorhandenen Werts verwendet wird.

Berechtigungen, die für Buckets gelten

Berechtigungen	S3-REST-API-OPERATIONEN	Individuell für StorageGRID
s3:CreateBucket	Put Bucket	
s3:DeleteBucket	Bucket LÖSCHEN	
s3:DeleteBucketMetadataBenachrichtigung	Konfiguration für die Benachrichtigung über Bucket-Metadaten LÖSCHEN	Ja.

Berechtigungen	S3-REST-API-OPERATIONEN	Individuell für StorageGRID
s3:DeleteBucketPolicy	Bucket-Richtlinie LÖSCHEN	
s3:DeleteReplicationConfiguration	Bucket-Replizierung LÖSCHEN	Ja, separate Berechtigungen für PUT und DELETE*
s3:GetBucketAcl	Bucket-ACL ABRUFEN	
s3:GetBucketCompliance	GET Bucket-Compliance (veraltet)	Ja.
s3:GetBucketConsistency	Get Bucket-Konsistenz	Ja.
s3:GetBucketCORS	Bucket-Cors ABRUFEN	
s3:GetVerschlüsselungKonfiguration	Get Bucket-Verschlüsselung	
s3:GetBucketLastAccessTime	ZEITPUNKT des letzten Zugriffs FÜR den Bucket ABRUFEN	Ja.
s3:GetBucketLocation	Bucket-Speicherort ABRUFEN	
s3:GetBucketMetadataBenachrichtigung	Konfiguration der Bucket-Metadaten-Benachrichtigungen ABRUFEN	Ja.
s3:GetBucketBenachrichtigung	Bucket-Benachrichtigung ABRUFEN	
s3:GetBucketObjectLockConfiguration	Konfiguration der Objektsperre ABRUFEN	
s3:GetBucketPolicy	Get Bucket-Richtlinie	
s3:GetBucketTagging	Get Bucket-Tagging	
s3:GetBucketVersionierung	Get Bucket-Versionierung	
s3:GetLifecycleKonfiguration	BUCKET-Lebenszyklus ABRUFEN	
s3:GetReplicationConfiguration	GET Bucket-Replizierung	
s3:ListAllMyBuchs	• GET Service • GET Storage-Auslastung	Ja, für GET Storage Usage

Berechtigungen	S3-REST-API-OPERATIONEN	Individuell für StorageGRID
s3:ListBucket	• Bucket ABRUFEN (Objekte auflisten) • EIMER • WIEDERHERSTELLUNG VON POSTOBJEKTEN	
s3:ListBucketMultipartUploads	• Mehrteilige Uploads Auflisten • WIEDERHERSTELLUNG VON POSTOBJEKTEN	
s3:ListBucketVersions	Get Bucket-Versionen	
s3:PutBucketCompliance	PUT Bucket-Compliance (veraltet)	Ja.
s3:PutBucketConsistency	PUT Bucket-Konsistenz	Ja.
s3:PutBucketCORS	• Bucket Cors† LÖSCHEN • Bucket-Cors EINGEBEN	
s3:PutVerschlüsselungKonfiguration	• Bucket-Verschlüsselung LÖSCHEN • Bucket-Verschlüsselung	
s3:PutBucketLastAccessTime	PUT Bucket-Zeit für den letzten Zugriff	Ja.
s3:PutBucketMetadataBenachrichtigung	PUT Bucket-Metadaten-Benachrichtigungskonfiguration	Ja.
s3:PutBucketNotification	PUT Bucket-Benachrichtigung	
s3:PutBucketObjectLockConfiguration	Geben Sie Bucket mit dem EIN `x-amz-bucket-object-lock-enabled: true` Kopfzeile anfordern (erfordert auch die Berechtigung s3:CreateBucket)	
s3:PutBucketPolicy	Bucket-Richtlinie	
s3:PutBucketTagging	• Bucket-Tagging† löschen • PUT Bucket-Tagging	
s3:PutBucketVersionierung	PUT Bucket-Versionierung	

Berechtigungen	S3-REST-API-OPERATIONEN	Individuell für StorageGRID
s3:PutLifecycleKonfiguration	• Bucket-Lebenszyklus LÖSCHEN† • PUT Bucket-Lebenszyklus	
s3:PuteReplikationKonfiguration	PUT Bucket-Replizierung	Ja, separate Berechtigungen für PUT und DELETE*

Berechtigungen, die sich auf Objekte beziehen

Berechtigungen	S3-REST-API-OPERATIONEN	Individuell für StorageGRID
s3:AbortMehrteilaUpload	• Abbrechen Von Mehrteiligen Uploads • WIEDERHERSTELLUNG VON POSTOBJEKTEN	
s3:DeleteObject	• Objekt LÖSCHEN • LÖSCHEN Sie mehrere Objekte • WIEDERHERSTELLUNG VON POSTOBJEKTEN	
s3:DeleteObjectTagging	Objekt-Tagging LÖSCHEN	
s3:DeleteObjectVersionTagging	Objekt-Tagging LÖSCHEN (eine bestimmte Version des Objekts)	
s3:DeleteObjectVersion	Objekt LÖSCHEN (eine bestimmte Version des Objekts)	
s3:GetObject	• GET Objekt • HEAD Objekt • WIEDERHERSTELLUNG VON POSTOBJEKTEN	
s3:GetObjectAcl	GET Objekt-ACL	
s3:GetObjectLegalOld	HOLD-Aufbewahrung für Objekte	
s3:GetObjectRetention	Aufbewahrung von Objekten	
s3:GetObjectTagging	Get Objekt-Tagging	

Berechtigungen	S3-REST-API-OPERATIONEN	Individuell für StorageGRID
s3:GetObjectVersionTagging	GET Object Tagging (eine bestimmte Version des Objekts)	
s3:GetObjectVersion	GET Object (eine bestimmte Version des Objekts)	
s3:ListeMultipartUploadParts	Teile auflisten, Objekt WIEDERHERSTELLEN	
s3:PutObject	• PUT Objekt • PUT Objekt - Kopieren • WIEDERHERSTELLUNG VON POSTOBJEKTEN • Initiieren Von Mehrteiligen Uploads • Abschließen Von Mehrteiligen Uploads • Hochladen Von Teilen • Hochladen Von Teilen - Kopieren	
s3:PuttObjectLegalOld	LEGALE Aufbewahrung des Objekts EINGEBEN	
s3:PutObjectRetention	AUFBEWAHRUNG von Objekten	
s3:PuttObjectTagging	PUT Objekt-Tagging	
s3:PuttObjectVersionTagging	PUT Objekt-Tagging (eine bestimmte Version des Objekts)	
s3:PutOverwrite Object	• PUT Objekt • PUT Objekt - Kopieren • PUT Objekt-Tagging • Objekt-Tagging LÖSCHEN • Abschließen Von Mehrteiligen Uploads	Ja.
s3:RestoreObject	WIEDERHERSTELLUNG VON POSTOBJEKTEN	

Verwenden der Berechtigung PutOverwriteObject

die s3:PutOverwriteObject-Berechtigung ist eine benutzerdefinierte StorageGRID-Berechtigung, die für Vorgänge gilt, die Objekte erstellen oder aktualisieren. Durch diese Berechtigung wird festgelegt, ob der Client die Daten, benutzerdefinierte Metadaten oder S3-Objekt-Tagging überschreiben kann.

Mögliche Einstellungen für diese Berechtigung sind:

- **Zulassen**: Der Client kann ein Objekt überschreiben. Dies ist die Standardeinstellung.
- **Deny**: Der Client kann ein Objekt nicht überschreiben. Wenn die Option „Ablehnen“ eingestellt ist, funktioniert die Berechtigung „PutOverwriteObject“ wie folgt:
  - Wenn ein vorhandenes Objekt auf demselben Pfad gefunden wird:
    - Die Daten des Objekts, benutzerdefinierte Metadaten oder S3 Objekt-Tagging können nicht überschrieben werden.
    - Alle laufenden Aufnahmevorgänge werden abgebrochen und ein Fehler wird zurückgegeben.
    - Wenn die S3-Versionierung aktiviert ist, verhindert die Einstellung Deny, dass PUT Objekt-Tagging oder DELETE Objekt-Tagging die TagSet für ein Objekt und seine nicht aktuellen Versionen ändert.
  - Wenn ein vorhandenes Objekt nicht gefunden wird, hat diese Berechtigung keine Wirkung.
- Wenn diese Berechtigung nicht vorhanden ist, ist der Effekt der gleiche, als ob Allow-were gesetzt wurden.

> Wenn die aktuelle S3-Richtlinie eine Überschreibung zulässt und die Berechtigung PutOverwriteObject auf Deny gesetzt ist, kann der Client die Daten eines Objekts, benutzerdefinierte Metadaten oder Objekt-Tagging nicht überschreiben. Wenn zusätzlich das Kontrollkästchen **Client Modification** verhindern* aktiviert ist (**Configuration** > **Grid Options**), überschreibt diese Einstellung die Einstellung der PutOverwriteObject-Berechtigung.

Verwandte Informationen

"Beispiele für S3-Gruppenrichtlinien"

Festlegen von Bedingungen in einer Richtlinie

Die Bedingungen legen fest, wann eine Richtlinie in Kraft sein wird. Die Bedingungen bestehen aus Bedienern und Schlüsselwertpaaren.

Bedingungen Verwenden Sie Key-Value-Paare für die Auswertung. Ein Bedingungselement kann mehrere Bedingungen enthalten, und jede Bedingung kann mehrere Schlüsselwert-Paare enthalten. Der Bedingungsblock verwendet das folgende Format:

```
Condition: {
     <em>condition_type</em>: {
          <em>condition_key</em>: <em>condition_values</em>
```

Im folgenden Beispiel verwendet die IPAddress-Bedingung den SourceIp-Bedingungsschlüssel.

```
"Condition": {
    "IpAddress": {
      "aws:SourceIp": "54.240.143.0/24"
        ...
},
        ...
```

Unterstützte Bedingungsoperatoren

Bedingungsoperatoren werden wie folgt kategorisiert:

- Zeichenfolge
- Numerisch
- Boolesch
- IP-Adresse
- Null-Prüfung

Bedingungsoperatoren	Beschreibung
StringEquals	Vergleicht einen Schlüssel mit einem Zeichenfolgenwert, der auf exakter Übereinstimmung basiert (Groß-/Kleinschreibung wird beachtet).
StringNotEquals	Vergleicht einen Schlüssel mit einem Zeichenfolgenwert, der auf negatives Matching basiert (Groß-/Kleinschreibung wird beachtet).
StringEqusIgnoreCase	Vergleicht einen Schlüssel mit einem Zeichenfolgenwert, der auf exakter Übereinstimmung basiert (Groß-/Kleinschreibung wird ignoriert).
StringNotEqualesIgnoreCase	Vergleicht einen Schlüssel mit einem String-Wert, der auf negatives Matching basiert (Groß-/Kleinschreibung wird ignoriert).
StringLike	Vergleicht einen Schlüssel mit einem Zeichenfolgenwert, der auf exakter Übereinstimmung basiert (Groß-/Kleinschreibung wird beachtet). Kann * und ? Platzhalterzeichen.
StringNotLike	Vergleicht einen Schlüssel mit einem Zeichenfolgenwert, der auf negatives Matching basiert (Groß-/Kleinschreibung wird beachtet). Kann * und ? Platzhalterzeichen.
Ziffern	Vergleicht einen Schlüssel mit einem numerischen Wert, der auf exakter Übereinstimmung basiert.

Bedingungsoperatoren	Beschreibung
ZiffernNotequals	Vergleicht einen Schlüssel mit einem numerischen Wert, der auf negatives Matching basiert.
NumericGreaterThan	Vergleicht einen Schlüssel mit einem numerischen Wert, der auf „`größer als`“-Übereinstimmung basiert.
ZahlungGreaterThanEquals	Vergleicht einen Schlüssel mit einem numerischen Wert, der auf „`größer als oder gleich`“-Übereinstimmung basiert.
NumericLessThan	Vergleicht einen Schlüssel mit einem numerischen Wert, der auf „`weniger als`“-Übereinstimmung basiert.
ZahlungWenigerThanEquals	Vergleicht einen Schlüssel mit einem numerischen Wert, der auf „`kleiner als oder gleich`“-Übereinstimmung basiert.
Bool	Vergleicht einen Schlüssel mit einem Booleschen Wert auf der Grundlage von „`true“ oder „false`“-Übereinstimmung.
IP-Adresse	Vergleicht einen Schlüssel mit einer IP-Adresse oder einem IP-Adressbereich.
NotIpAddress	Vergleicht einen Schlüssel mit einer IP-Adresse oder einem IP-Adressbereich, basierend auf negatiertem Abgleich.
Null	Überprüft, ob im aktuellen Anforderungskontext ein Bedingungsschlüssel vorhanden ist.

Unterstützte Bedingungsschlüssel

Kategorie	Die entsprechenden Bedingungsschlüssel	Beschreibung
IP-Operatoren	aws:SourceIp	Vergleicht mit der IP-Adresse, von der die Anfrage gesendet wurde. Kann für Bucket- oder Objektvorgänge verwendet werden **Hinweis:** wurde die S3-Anfrage über den Lastbalancer-Dienst auf Admin-Knoten und Gateways-Knoten gesendet, wird dies mit der IP-Adresse verglichen, die vor dem Load Balancer Service liegt. **Hinweis**: Wenn ein Drittanbieter-, nicht-transparenter Load Balancer verwendet wird, wird dies mit der IP-Adresse dieses Load Balancer verglichen. Alle `X-Forwarded-For` Kopfzeile wird ignoriert, da seine Gültigkeit nicht ermittelt werden kann.
Ressource/Identität	aws:Benutzername	Vergleicht mit dem Benutzernamen des Absenders, von dem die Anfrage gesendet wurde. Kann für Bucket- oder Objektvorgänge verwendet werden
S3:ListBucket und S3:ListBucketVersions Berechtigungen	s3:Trennzeichen	Vergleicht mit dem Parameter Trennzeichen, der in einer Anforderung GET Bucket oder GET Bucket Object Version angegeben ist.
S3:ListBucket und S3:ListBucketVersions Berechtigungen	s3:max-keys	Vergleicht den Parameter max-keys, der in einer Anforderung FÜR GET Bucket oder GET Bucket Object-Versionen angegeben ist.
S3:ListBucket und S3:ListBucketVersions Berechtigungen	s3:Präfix	Vergleicht mit dem Präfixparameter, der in einer Anforderung FÜR GET Bucket oder GET Bucket Object-Versionen angegeben ist.

Festlegen von Variablen in einer Richtlinie

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

In diesem Beispiel die Variable `${aws:username}` Ist Teil des Ressourcenelements:

```
"Resource": "arn:aws:s3:::_bucket-name/home_/${aws:username}/*"
```

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

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

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

Erstellen von Richtlinien, die eine besondere Handhabung erfordern

Manchmal kann eine Richtlinie Berechtigungen erteilen, die für die Sicherheit oder die Gefahr für einen fortgesetzten Betrieb gefährlich sind, z. B. das Sperren des Root-Benutzers des Kontos. Die StorageGRID S3-REST-API-Implementierung ist bei der Richtlinienvalidierung weniger restriktiv als Amazon, aber auch bei der Richtlinienbewertung streng.

Richtlinienbeschreibung	Richtlinientyp	Verhalten von Amazon	Verhalten von StorageGRID
Verweigern Sie sich selbst irgendwelche Berechtigungen für das Root-Konto	Eimer	Gültig und durchgesetzt, aber das Root-Benutzerkonto behält die Berechtigung für alle S3 Bucket-Richtlinienvorgänge bei	Gleich
Verweigern Sie selbst jegliche Berechtigungen für Benutzer/Gruppe	Gruppieren	Gültig und durchgesetzt	Gleich
Erlauben Sie einer fremden Kontogruppe jegliche Berechtigung	Eimer	Ungültiger Principal	Gültig, aber die Berechtigungen für alle S3-Bucket-Richtlinienvorgänge geben bei Richtlinienzugelassen durch eine Richtlinie einen nicht zugelassenen 405-Method-Fehler zurück
Berechtigung für ein ausländisches Konto oder einen Benutzer zulassen	Eimer	Gültig, aber die Berechtigungen für alle S3-Bucket-Richtlinienvorgänge geben bei Richtlinienzugelassen durch eine Richtlinie einen nicht zugelassenen 405-Method-Fehler zurück	Gleich
Alle Berechtigungen für alle Aktionen zulassen	Eimer	Gültig, aber Berechtigungen für alle S3-Bucket-Richtlinienvorgänge geben einen 405 Methode nicht erlaubten Fehler für das ausländische Konto Root und Benutzer zurück	Gleich
Alle Berechtigungen für alle Aktionen verweigern	Eimer	Gültig und durchgesetzt, aber das Root-Benutzerkonto behält die Berechtigung für alle S3 Bucket-Richtlinienvorgänge bei	Gleich

Richtlinienbeschreibung	Richtlinientyp	Verhalten von Amazon	Verhalten von StorageGRID
Principal ist ein nicht existierender Benutzer oder eine Gruppe	Eimer	Ungültiger Principal	Gültig
Die Ressource ist ein nicht existierender S3-Bucket	Gruppieren	Gültig	Gleich
Principal ist eine lokale Gruppe	Eimer	Ungültiger Principal	Gültig
Policy gewährt einem nicht-Inhaberkonto (einschließlich anonymer Konten) Berechtigungen zum PUT von Objekten	Eimer	Gültig. Objekte sind Eigentum des Erstellerkontos, und die Bucket-Richtlinie gilt nicht. Das Ersteller-Konto muss über Objekt-ACLs Zugriffsrechte für das Objekt gewähren.	Gültig. Der Eigentümer der Objekte ist das Bucket-Owner-Konto. Bucket-Richtlinie gilt.

WORM-Schutz (Write Once, Read Many)

Sie können WORM-Buckets (Write-Once-Read-Many) erstellen, um Daten, benutzerdefinierte Objekt-Metadaten und S3-Objekt-Tagging zu sichern. SIE konfigurieren die WORM-Buckets, um das Erstellen neuer Objekte zu ermöglichen und Überschreibungen oder das Löschen vorhandener Inhalte zu verhindern. Verwenden Sie einen der hier beschriebenen Ansätze.

Um sicherzustellen, dass Überschreibungen immer verweigert werden, können Sie:

- Wählen Sie im Grid Manager die Option **Konfiguration** > **Grid-Optionen** und aktivieren Sie das Kontrollkästchen **Client-Änderung verhindern**.
- Wenden Sie die folgenden Regeln und S3-Richtlinien an:
  - Fügen Sie der S3-Richtlinie einen PutOverwriteObject DENY-Vorgang hinzu.
  - Fügen Sie der S3-Richtlinie einen DeleteObject DENY-Vorgang hinzu.
  - Fügen Sie der S3-Richtlinie einen PUT Object ALLOW-Vorgang hinzu.

> Wenn DeleteObject in einer S3-Richtlinie VERWEIGERT wird, verhindert dies nicht, dass ILM Objekte löscht, wenn eine Regel wie „`Zero Copies after 30 days`“ vorhanden ist.

> Selbst wenn all diese Regeln und Richtlinien angewendet werden, schützen sie sich nicht vor gleichzeitigen Schreibvorgängen (siehe Situation A). Sie schützen vor sequenziellen Überschreibungen (siehe Situation B).

Situation A: Gleichzeitige Schreibvorgänge (nicht bewacht)

```
/mybucket/important.doc
PUT#1 ---> OK
PUT#2 -------> OK
```

Situation B: Sequentielle abgeschlossene Überschreibungen (bewacht gegen)

```
/mybucket/important.doc
PUT#1 -------> PUT#2 ---X (denied)
```

Verwandte Informationen

"Objektmanagement mit ILM"

"Erstellen von Richtlinien, die eine besondere Handhabung erfordern"

"Managen von Objekten durch StorageGRID ILM-Regeln"

"Beispiele für S3-Gruppenrichtlinien"

Beispiele für S3-Richtlinien

Verwenden Sie die Beispiele in diesem Abschnitt, um StorageGRID-Zugriffsrichtlinien für Buckets und Gruppen zu erstellen.

Beispiele für S3-Bucket-Richtlinien

Bucket-Richtlinien geben die Zugriffsberechtigungen für den Bucket an, mit dem die Richtlinie verknüpft ist. Bucket-Richtlinien werden mithilfe der S3-PutBucketPolicy-API konfiguriert.

Eine Bucket-Richtlinie kann mithilfe der AWS CLI wie folgt konfiguriert werden:

```
> aws s3api put-bucket-policy --bucket examplebucket --policy
<em>file://policy.json</em>
```

Beispiel: Lesezugriff auf einen Bucket zulassen

In diesem Beispiel darf jeder, auch anonym, Objekte im Bucket auflisten und get-Objektvorgänge an allen Objekten im Bucket durchführen. Alle anderen Operationen werden abgelehnt. Beachten Sie, dass diese Richtlinie möglicherweise nicht besonders nützlich ist, da niemand außer dem Konto-Root über Berechtigungen zum Schreiben in den Bucket verfügt.

```
{
  "Statement": [
    {
      "Sid": "AllowEveryoneReadOnlyAccess",
      "Effect": "Allow",
      "Principal": "*",
      "Action": [ "s3:GetObject", "s3:ListBucket" ],
      "Resource":
["arn:aws:s3:::examplebucket","arn:aws:s3:::examplebucket/*"]
    }
  ]
}
```

Beispiel: Jeder in einem Konto Vollzugriff zulassen, und jeder in einem anderen Konto hat nur Lesezugriff auf einen Bucket

In diesem Beispiel ist jedem in einem bestimmten Konto der vollständige Zugriff auf einen Bucket gestattet, während jeder in einem anderen angegebenen Konto nur die Liste des Buckets und die Durchführung von GetObject-Operationen für Objekte im Bucket erlaubt ist, die mit dem beginnen `shared/` Objektschlüsselpräfix.

> In StorageGRID sind Objekte, die von einem nicht-Inhaberkonto erstellt wurden (einschließlich anonymer Konten), Eigentum des Bucket-Inhaberkontos. Die Bucket-Richtlinie gilt für diese Objekte.

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "95390887230002558202"
      },
      "Action": "s3:*",
      "Resource": [
        "arn:aws:s3:::examplebucket",
        "arn:aws:s3:::examplebucket/*"
      ]
    },
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "31181711887329436680"
      },
      "Action": "s3:GetObject",
      "Resource": "arn:aws:s3:::examplebucket/shared/*"
    },
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "31181711887329436680"
      },
      "Action": "s3:ListBucket",
      "Resource": "arn:aws:s3:::examplebucket",
      "Condition": {
        "StringLike": {
          "s3:prefix": "shared/*"
        }
      }
    }
  ]
}
```

Beispiel: Lesezugriff für einen Bucket und vollständiger Zugriff durch angegebene Gruppe

In diesem Beispiel dürfen alle, einschließlich anonym, den Bucket auflisten und GET-Objektvorgänge für alle Objekte im Bucket durchführen, während nur Benutzer der Gruppe gehören `Marketing` Im angegebenen Konto ist Vollzugriff erlaubt.

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::95390887230002558202:federated-
group/Marketing"
      },
      "Action": "s3:*",
      "Resource": [
        "arn:aws:s3:::examplebucket",
        "arn:aws:s3:::examplebucket/*"
      ]
    },
    {
      "Effect": "Allow",
      "Principal": "*",
      "Action": ["s3:ListBucket","s3:GetObject"],
      "Resource": [
        "arn:aws:s3:::examplebucket",
        "arn:aws:s3:::examplebucket/*"
      ]
    }
  ]
}
```

Beispiel: Jeder Lese- und Schreibzugriff auf einen Bucket zulassen, wenn Client im IP-Bereich ist

In diesem Beispiel darf jeder, einschließlich anonym, den Bucket auflisten und beliebige Objektvorgänge an allen Objekten im Bucket durchführen, vorausgesetzt, dass die Anforderungen aus einem bestimmten IP-Bereich stammen (54.240.143.0 bis 54.240.143.255, außer 54.240.143.188). Alle anderen Vorgänge werden abgelehnt, und alle Anfragen außerhalb des IP-Bereichs werden abgelehnt.

```
{
  "Statement": [
    {
      "Sid": "AllowEveryoneReadWriteAccessIfInSourceIpRange",
      "Effect": "Allow",
      "Principal": "*",
      "Action": [ "s3:*Object", "s3:ListBucket" ],
      "Resource":
["arn:aws:s3:::examplebucket","arn:aws:s3:::examplebucket/*"],
      "Condition": {
        "IpAddress": {"aws:SourceIp": "54.240.143.0/24"},
        "NotIpAddress": {"aws:SourceIp": "54.240.143.188"}
      }
    }
  ]
}
```

Beispiel: Vollständigen Zugriff auf einen Bucket zulassen, der ausschließlich von einem festgelegten föderierten Benutzer verwendet wird

In diesem Beispiel ist dem föderierten Benutzer Alex der vollständige Zugriff auf das erlaubt `examplebucket` Bucket und seine Objekte. Alle anderen Benutzer, einschließlich ‘root’, werden ausdrücklich allen Operationen verweigert. Beachten Sie jedoch, dass ‘root’ niemals die Berechtigungen zum Put/get/DeleteBucketPolicy verweigert wird.

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::95390887230002558202:federated-user/Alex"
      },
      "Action": [
        "s3:*"
      ],
      "Resource": [
        "arn:aws:s3:::examplebucket",
        "arn:aws:s3:::examplebucket/*"
      ]
    },
    {
      "Effect": "Deny",
      "NotPrincipal": {
        "AWS": "arn:aws:iam::95390887230002558202:federated-user/Alex"
      },
      "Action": [
        "s3:*"
      ],
      "Resource": [
        "arn:aws:s3:::examplebucket",
        "arn:aws:s3:::examplebucket/*"
      ]
    }
  ]
}
```

Beispiel: PutOverwriteObject-Berechtigung

In diesem Beispiel ist der `Deny` Effect für PutOverwriteObject und DeleteObject stellt sicher, dass niemand die Daten, benutzerdefinierte Metadaten und S3-Objekt-Tagging überschreiben oder löschen kann.

```
{
  "Statement": [
    {
      "Effect": "Deny",
      "Principal": "*",
      "Action": [
        "s3:PutOverwriteObject",
        "s3:DeleteObject",
        "s3:DeleteObjectVersion"
      ],
      "Resource": "arn:aws:s3:::wormbucket/*"
    },
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::95390887230002558202:federated-
group/SomeGroup"

},
      "Action": "s3:ListBucket",
      "Resource": "arn:aws:s3:::wormbucket"
    },
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::95390887230002558202:federated-
group/SomeGroup"

},
      "Action": "s3:*",
      "Resource": "arn:aws:s3:::wormbucket/*"
    }
  ]
}
```

Verwandte Informationen

"Operationen auf Buckets"

Beispiele für S3-Gruppenrichtlinien

Gruppenrichtlinien legen die Zugriffsberechtigungen für die Gruppe fest, der die Richtlinie zugeordnet ist. Es gibt keine `Principal` Element in der Richtlinie, da sie implizit ist. Gruppenrichtlinien werden mit dem Tenant Manager oder der API konfiguriert.

Beispiel: Festlegen der Gruppenrichtlinie mit Tenant Manager

Wenn Sie den Tenant Manager zum Hinzufügen oder Bearbeiten einer Gruppe verwenden, können Sie auswählen, wie Sie die Gruppenrichtlinie erstellen möchten, die definiert, welche S3-Zugriffsberechtigungen Mitglieder dieser Gruppe haben. Gehen Sie wie folgt vor:

- **Kein S3-Zugriff**: Standardoption. Benutzer in dieser Gruppe haben keinen Zugriff auf S3-Ressourcen, es sei denn, der Zugriff wird mit einer Bucket-Richtlinie gewährt. Wenn Sie diese Option auswählen, hat 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.

  In diesem Beispiel dürfen Mitglieder der Gruppe nur ihren spezifischen Ordner (Schlüsselpräfix) im angegebenen Bucket auflisten und darauf zugreifen.

Beispiel: Vollständigen Zugriff auf alle Buckets zulassen

In diesem Beispiel sind alle Mitglieder der Gruppe berechtigt, vollständigen Zugriff auf alle Buckets des Mandantenkontos zu erhalten, sofern nicht ausdrücklich von der Bucket-Richtlinie abgelehnt wurde.

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

Beispiel: Schreibgeschützter Zugriff auf alle Buckets für Gruppen zulassen

In diesem Beispiel haben alle Mitglieder der Gruppe schreibgeschützten Zugriff auf S3-Ressourcen, sofern nicht ausdrücklich von der Bucket-Richtlinie abgelehnt wird. Benutzer in dieser Gruppe können beispielsweise Objekte auflisten und Objektdaten, Metadaten und Tags lesen.

```
{
  "Statement": [
    {
      "Sid": "AllowGroupReadOnlyAccess",
      "Effect": "Allow",
      "Action": [
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "s3:ListBucketVersions",
        "s3:GetObject",
        "s3:GetObjectTagging",
        "s3:GetObjectVersion",
        "s3:GetObjectVersionTagging"
      ],
      "Resource": "arn:aws:s3:::*"
    }
  ]
}
```

Beispiel: Gruppenmitglieder haben vollen Zugriff auf ihre „`folder`“ in einem Bucket

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

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

Verwandte Informationen

"Verwenden Sie ein Mandantenkonto"

"Verwenden der Berechtigung PutOverwriteObject"

"WORM-Schutz (Write Once, Read Many)"

Sicherheit wird für DIE REST API konfiguriert

Sie sollten die für DIE REST API implementierten Sicherheitsmaßnahmen überprüfen und verstehen, wie Sie Ihr System sichern können.

So bietet StorageGRID Sicherheit für DIE REST-API

Sie sollten verstehen, wie das StorageGRID System die Sicherheit, Authentifizierung und Autorisierung für DIE REST-API implementiert.

StorageGRID setzt die folgenden Sicherheitsmaßnahmen ein.

- Die Client-Kommunikation mit dem Load Balancer-Service erfolgt über HTTPS, wenn HTTPS für den Load Balancer-Endpunkt konfiguriert ist.

  Wenn Sie einen Endpunkt für den Load Balancer konfigurieren, kann HTTP optional aktiviert werden. Möglicherweise möchten Sie beispielsweise HTTP für Tests oder andere Zwecke verwenden, die nicht aus der Produktion stammen. Weitere Informationen finden Sie in den Anweisungen zum Verwalten von StorageGRID.

- Standardmäßig verwendet StorageGRID HTTPS für die Client-Kommunikation mit Speicherknoten und den CLB-Service auf Gateway-Knoten.

  HTTP kann optional für diese Verbindungen aktiviert werden. Möglicherweise möchten Sie beispielsweise HTTP für Tests oder andere Zwecke verwenden, die nicht aus der Produktion stammen. Weitere Informationen finden Sie in den Anweisungen zum Verwalten von StorageGRID.

  Der CLB-Service ist veraltet.

- Die Kommunikation zwischen StorageGRID und dem Client wird über TLS verschlüsselt.
- Die Kommunikation zwischen dem Load Balancer-Service und den Speicherknoten innerhalb des Grid wird verschlüsselt, ob der Load Balancer-Endpunkt für die Annahme von HTTP- oder HTTPS-Verbindungen konfiguriert ist.
- Clients müssen HTTP-Authentifizierungskopfzeilen an StorageGRID bereitstellen, um REST-API-Vorgänge durchzuführen.

Sicherheitszertifikate und Clientanwendungen

Clients können eine Verbindung zum Lastverteilungsservice auf Gateway-Knoten oder Admin-Nodes, direkt zu Storage-Nodes oder zum CLB-Dienst auf Gateway-Nodes herstellen.

Clientanwendungen können in jedem Fall TLS-Verbindungen herstellen, indem sie entweder ein vom Grid-Administrator hochgeladenes benutzerdefiniertes Serverzertifikat oder ein vom StorageGRID-System generiertes Zertifikat verwenden:

- Wenn Client-Anwendungen eine Verbindung zum Load Balancer-Service herstellen, verwenden sie dazu das Zertifikat, das für den spezifischen Load Balancer-Endpunkt konfiguriert wurde, der für die Verbindung verwendet wurde. Jeder Endpunkt verfügt über ein eigenes Zertifikat, entweder ein vom Grid-Administrator hochgeladenes benutzerdefiniertes Serverzertifikat oder ein Zertifikat, das der Grid-Administrator bei der Konfiguration des Endpunkts in StorageGRID generiert hat.
- Wenn Client-Anwendungen eine direkte Verbindung zu einem Speicherknoten oder zum CLB-Dienst auf Gateway-Knoten herstellen, verwenden sie entweder die vom System generierten Serverzertifikate, die bei der Installation des StorageGRID-Systems (die von der Systemzertifikatbehörde signiert sind) für Speicherknoten generiert wurden. Oder ein einzelnes benutzerdefiniertes Serverzertifikat, das von einem Grid-Administrator für das Grid bereitgestellt wird.

Die Clients sollten so konfiguriert werden, dass sie der Zertifizierungsstelle vertrauen, die unabhängig davon, welches Zertifikat sie zum Erstellen von TLS-Verbindungen verwenden, unterzeichnet hat.

Informationen StorageGRID zum Konfigurieren von Load Balancer-Endpunkten finden Sie in den Anweisungen zum Hinzufügen eines einzelnen benutzerdefinierten Serverzertifikats für TLS-Verbindungen direkt zu Storage-Nodes oder zum CLB-Dienst auf Gateway-Nodes.

Zusammenfassung

Die folgende Tabelle zeigt, wie Sicherheitsprobleme in den S3 und Swift REST-APIs implementiert werden:

Sicherheitsproblem	Implementierung für REST-API
Verbindungssicherheit	TLS

Sicherheitsproblem	Implementierung für REST-API
Serverauthentifizierung	X.509-Serverzertifikat, das von der System-CA oder vom Administrator zur Verfügung gestellten benutzerdefinierten Serverzertifikat unterzeichnet wurde
Client-Authentifizierung	• S3: S3-Konto (Zugriffsschlüssel-ID und geheimer Zugriffsschlüssel) • Swift: Swift-Konto (Benutzername und Passwort)
Client-Autorisierung	• S3: Bucket-Eigentümerschaft und alle anwendbaren Richtlinien für die Zugriffssteuerung • Swift: Administratorrollenzugriff

Verwandte Informationen

"StorageGRID verwalten"

Unterstützte Hashing- und Verschlüsselungsalgorithmen für TLS-Bibliotheken

Das StorageGRID System unterstützt eine begrenzte Anzahl von Chiffren-Suites, die Client-Anwendungen beim Einrichten einer TLS-Sitzung (Transport Layer Security) verwenden können.

Unterstützte Versionen von TLS

StorageGRID unterstützt TLS 1.2 und TLS 1.3.

SSLv3 und TLS 1.1 (oder frühere Versionen) werden nicht mehr unterstützt.

Unterstützte Chiffren-Suiten

TLS-Version	IANA Name der Chiffre Suite
1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
1.2	TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256
1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
1.3	TLS_AES_256_GCM_SHA384
1.3	TLS_CHACHA20_POLY1305_SHA256
1.3	TLS_AES_128_GCM_SHA256

Veraltete Chiffre-Suiten

Die folgenden Chiffren Suiten sind veraltet. Die Unterstützung für diese Chiffren wird in einer zukünftigen Version entfernt.

IANA-Name
TLS_RSA_WITH_AES_128_GCM_SHA256
TLS_RSA_WITH_AES_256_GCM_SHA384

Verwandte Informationen

"Wie Client-Verbindungen konfiguriert werden können"

Monitoring und Auditing von Vorgängen

Kunden können Workloads und die Effizienz für Client-Vorgänge überwachen, indem sie Transaktionstrends für das gesamte Grid oder bestimmte Nodes anzeigen. Sie können Audit-Meldungen zur Überwachung von Client-Vorgängen und -Transaktionen verwenden.

- "Monitoring der Objekteinspeisung und -Abrufraten"
- "Aufrufen und Prüfen von Prüfprotokollen"

Monitoring der Objekteinspeisung und -Abrufraten

Die Überwachung von Objekteraufnahmeraten und -Abruffraten sowie von Metriken für Objektanzahl, -Abfragen und -Verifizierung Sie können die Anzahl der erfolgreichen und fehlgeschlagenen Versuche von Client-Applikationen anzeigen, Objekte in StorageGRID zu lesen, zu schreiben und zu ändern.

Schritte

1. Melden Sie sich über einen unterstützten Browser beim Grid Manager an.
2. Suchen Sie im Dashboard den Abschnitt Protokollvorgänge.

   In diesem Abschnitt wird die Anzahl der Client-Vorgänge zusammengefasst, die vom StorageGRID System durchgeführt werden. Die Protokollraten werden über die letzten zwei Minuten Durchschnitt.

3. Wählen Sie **Knoten**.
4. Klicken Sie auf der Startseite Knoten (Bereitstellungsebene) auf die Registerkarte **Load Balancer**.

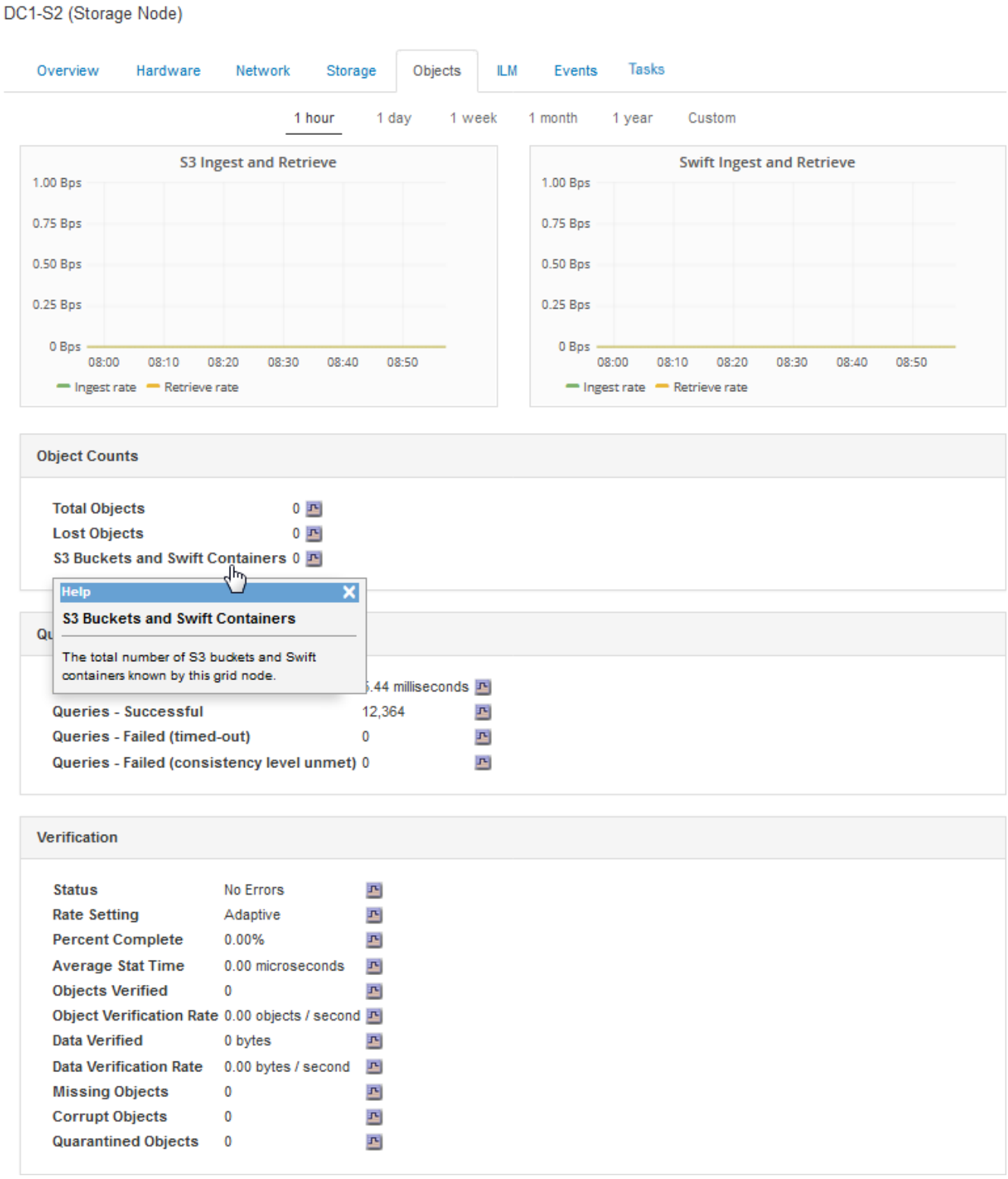
   Die Diagramme zeigen Trends für den gesamten Client-Datenverkehr an Load Balancer-Endpunkte im Raster. Sie können ein Zeitintervall in Stunden, Tagen, Wochen, Monaten oder Jahren auswählen. Oder Sie können ein benutzerdefiniertes Intervall anwenden.

5. Klicken Sie auf der Startseite Knoten (Bereitstellungsebene) auf die Registerkarte **Objekte**.

   Das Diagramm zeigt die Aufnahme- und Abrufraten Ihres gesamten StorageGRID Systems in Byte pro Sekunde sowie insgesamt Bytes. Sie können ein Zeitintervall in Stunden, Tagen, Wochen, Monaten oder Jahren auswählen. Oder Sie können ein benutzerdefiniertes Intervall anwenden.

6. Um Informationen zu einem bestimmten Speicherknoten anzuzeigen, wählen Sie den Knoten aus der Liste auf der linken Seite aus, und klicken Sie auf die Registerkarte **Objekte**.

   Das Diagramm zeigt die Aufnahme- und Abrufraten des Objekts für diesen Speicherknoten. Die Registerkarte enthält außerdem Kennzahlen für Objektanzahl, Abfragen und Verifizierung. Sie können auf die Beschriftungen klicken, um die Definitionen dieser Metriken anzuzeigen.



7. Wenn Sie noch mehr Details wünschen:

a. Wählen Sie **Support** > **Tools** > **Grid Topology** Aus.

b. Wählen Sie ***site*** > **Übersicht** > **Haupt**.

   Im Abschnitt API-Vorgänge werden zusammenfassende Informationen für das gesamte Raster angezeigt.

c. Wählen Sie ***Storage Node*** > **LDR** > ***Client-Anwendung*** > **Übersicht** > **Main** aus

   Im Abschnitt „Vorgänge“ werden zusammenfassende Informationen für den ausgewählten Speicherknoten angezeigt.

Aufrufen und Prüfen von Prüfprotokollen

Audit-Meldungen werden von StorageGRID-Diensten generiert und in Text-Log-Dateien gespeichert. API-spezifische Audit-Meldungen in den Audit-Protokollen stellen kritische Daten zum Monitoring von Sicherheit, Betrieb und Performance bereit, die Ihnen bei der Bewertung des Systemzustands helfen können.

Was Sie benötigen

- Sie müssen über spezifische Zugriffsberechtigungen verfügen.
- Sie müssen die haben `Passwords.txt` Datei:
- Sie müssen die IP-Adresse eines Admin-Knotens kennen.

Über diese Aufgabe

Der Name der aktiven Audit-Log-Datei `audit.log`, Und es wird auf Admin-Knoten gespeichert.

Einmal am Tag wird die aktive audit.log-Datei gespeichert und eine neue `audit.log` Datei wird gestartet. Der Name der gespeicherten Datei gibt an, wann sie gespeichert wurde, im Format *`yyyy-mm-dd.txt`*.

Nach einem Tag wird die gespeicherte Datei komprimiert und im Format umbenannt *`yyyy-mm-dd.txt.gz`*, Die das ursprüngliche Datum bewahrt.

Dieses Beispiel zeigt die aktive `audit.log` Datei, Datei des Vortags (`2018-04-15.txt`), und die komprimierte Datei für den Vortag (`2018-04-14.txt.gz`).

```
audit.log
2018-04-15.txt
2018-04-14.txt.gz
```

Schritte

1. Melden Sie sich bei einem Admin-Knoten an:

   a. Geben Sie den folgenden Befehl ein:
   `ssh admin@primary_Admin_Node_IP`

   b. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:

2. Gehen Sie zu dem Verzeichnis, das die Audit-Log-Dateien enthält:

   ```
   cd /var/local/audit/export
   ```

3. Sehen Sie sich die aktuelle oder gespeicherte Audit-Protokolldatei nach Bedarf an.

S3-Vorgänge werden in den Audit-Protokollen protokolliert

Verschiedene Bucket-Vorgänge und Objektvorgänge werden in den StorageGRID-Prüfprotokollen verfolgt.

Bucket-Vorgänge werden in den Audit-Protokollen protokolliert

- Bucket LÖSCHEN
- Bucket-Tagging LÖSCHEN
- LÖSCHEN Sie mehrere Objekte
- Bucket ABRUFEN (Objekte auflisten)
- Get Bucket-Objektversionen
- Get Bucket-Tagging
- EIMER
- Put Bucket
- BUCKET-Compliance
- PUT Bucket-Tagging
- PUT Bucket-Versionierung

Objektvorgänge werden in den Audit-Protokollen protokolliert

- Abschließen Von Mehrteiligen Uploads
- Hochladen von Teilen (wenn die ILM-Regel das strenge oder ausgeglichene Aufnahmeverhalten verwendet)
- Hochladen von Teilen – Kopieren (Wenn die ILM-Regel das strenge oder ausgeglichene Aufnahmeverhalten verwendet)
- Objekt LÖSCHEN
- GET Objekt
- HEAD Objekt
- WIEDERHERSTELLUNG VON POSTOBJEKTEN
- PUT Objekt
- PUT Objekt - Kopieren

Verwandte Informationen

"Operationen auf Buckets"

"Operationen für Objekte"

Vorteile von aktiven, inaktiven und gleichzeitigen HTTP-Verbindungen

Die Konfiguration von HTTP-Verbindungen kann sich auf die Performance des StorageGRID-Systems auswirken. Die Konfigurationen unterscheiden sich je nachdem, ob die HTTP-Verbindung aktiv oder inaktiv ist oder Sie mehrere Verbindungen

gleichzeitig haben.

Sie können die Performance-Vorteile für die folgenden Arten von HTTP-Verbindungen identifizieren:

- Inaktive HTTP-Verbindungen
- Aktive HTTP-Verbindungen
- Gleichzeitige HTTP-Verbindungen

Verwandte Informationen

- "Vorteile, wenn inaktive HTTP-Verbindungen offen gehalten werden"
- "Vorteile von aktiven HTTP-Verbindungen"
- "Vorteile gleichzeitiger HTTP-Verbindungen"
- "Trennung von HTTP-Verbindungspools für Lese- und Schreibvorgänge"

Vorteile, wenn inaktive HTTP-Verbindungen offen gehalten werden

Sie sollten HTTP-Verbindungen auch dann offen halten, wenn Client-Anwendungen inaktiv sind, um Client-Anwendungen die Ausführung folgender Transaktionen über die offene Verbindung zu ermöglichen. Basierend auf Systemmessungen und Integrationserfahrungen sollten Sie eine inaktive HTTP-Verbindung für maximal 10 Minuten offen halten. StorageGRID schließt möglicherweise automatisch eine HTTP-Verbindung, die länger als 10 Minuten im Ruhezustand bleibt.

Open- und Idle-HTTP-Verbindungen bieten folgende Vorteile:

- Niedrigere Latenz von dem Zeitpunkt, zu dem das StorageGRID System feststellt, dass eine HTTP-Transaktion durchgeführt werden muss, bis zum Zeitpunkt, zu dem das StorageGRID System die Transaktion ausführen kann

  Die geringere Latenz ist der Hauptvorteil, insbesondere aufgrund der für die Einrichtung von TCP/IP- und TLS-Verbindungen benötigten Zeit.

- Erhöhte Datenübertragungsrate durch Priming des TCP/IP Slow-Start-Algorithmus mit zuvor durchgeführten Transfers
- Sofortige Benachrichtigung über mehrere Klassen von Fehlerbedingungen, die die Verbindung zwischen Client-Anwendung und StorageGRID-System unterbrechen

Die Bestimmung, wie lange eine Leerlaufverbindung offen bleiben-soll, ist ein Kompromiss zwischen den Vorteilen des langsamen Starts, der mit der bestehenden Verbindung verbunden ist, und der idealen Zuweisung der Verbindung zu internen Systemressourcen.

Vorteile von aktiven HTTP-Verbindungen

Bei Verbindungen direkt zu Storage-Nodes oder zum CLB-Dienst (veraltet) auf Gateway-Knoten sollten Sie die Dauer einer aktiven HTTP-Verbindung auf maximal 10 Minuten beschränken, auch wenn die HTTP-Verbindung kontinuierlich Transaktionen durchführt.

Die Bestimmung der maximalen Dauer, die eine Verbindung offen halten-sollte, ist ein Kompromiss zwischen den Vorteilen der Verbindungspersistenz und der idealen Zuweisung der Verbindung zu internen Systemressourcen.

Für Client-Verbindungen zu Storage-Nodes oder zum CLB-Service bietet die Beschränkung aktiver HTTP-Verbindungen folgende Vorteile:

- Ermöglicht einen optimalen Lastausgleich über das StorageGRID System hinweg.

  Bei der Nutzung des CLB-Dienstes sollten Sie lange-durchlebte TCP/IP-Verbindungen verhindern, um den Lastenausgleich über das StorageGRID-System zu optimieren. Sie sollten Client-Anwendungen so konfigurieren, dass die Dauer jeder HTTP-Verbindung verfolgt und die HTTP-Verbindung nach einer festgelegten Zeit geschlossen wird, damit die HTTP-Verbindung wiederhergestellt und ausgeglichen werden kann.

  Der CLB-Dienst gleicht die Last über das StorageGRID-System aus, wenn eine Client-Anwendung eine HTTP-Verbindung herstellt. Im Laufe der Zeit ist eine HTTP-Verbindung möglicherweise nicht mehr optimal, da sich die Anforderungen für den Lastausgleich ändern. Das System führt den besten Lastenausgleich durch, wenn Client-Anwendungen für jede Transaktion eine separate HTTP-Verbindung herstellen, jedoch die wesentlich wertvolleren Gewinne, die mit persistenten Verbindungen verbunden sind, zunichte machen.

  Der CLB-Service ist veraltet.

- Ermöglicht Client-Anwendungen, HTTP-Transaktionen an LDR-Dienste mit verfügbarem Speicherplatz zu leiten.
- Ermöglicht das Starten von Wartungsvorgängen.

  Einige Wartungsverfahren beginnen erst, nachdem alle laufenden HTTP-Verbindungen abgeschlossen sind.

Bei Client-Verbindungen zum Load Balancer-Service kann eine Begrenzung der Dauer offener Verbindungen nützlich sein, um einige Wartungsverfahren zeitnah starten zu können. Wenn die Dauer der Clientverbindungen nicht begrenzt ist, kann es mehrere Minuten dauern, bis aktive Verbindungen automatisch beendet werden.

Vorteile gleichzeitiger HTTP-Verbindungen

Sie sollten mehrere TCP/IP-Verbindungen zum StorageGRID-System offen halten, um Parallelität zu ermöglichen, was die Performance steigert. Die optimale Anzahl paralleler Verbindungen hängt von einer Vielzahl von Faktoren ab.

Gleichzeitige HTTP-Verbindungen bieten die folgenden Vorteile:

- Geringere Latenz

  Transaktionen können sofort gestartet werden, anstatt auf die Durchführung anderer Transaktionen zu warten.

- Erhöhter Durchsatz

  Das StorageGRID System kann parallele Transaktionen durchführen und den aggregierten Transaktionsdurchsatz erhöhen.

Client-Anwendungen sollten mehrere HTTP-Verbindungen einrichten. Wenn eine Client-Anwendung eine Transaktion durchführen muss, kann sie eine vorhandene Verbindung auswählen und sofort verwenden, die

derzeit keine Transaktion verarbeitet.

Die Topologie jedes StorageGRID-Systems weist einen unterschiedlichen Spitzendurchsatz für gleichzeitige Transaktionen und Verbindungen auf, bevor die Performance abnimmt. Spitzendurchsatz hängt von Faktoren wie Computing-Ressourcen, Netzwerkressourcen, Storage-Ressourcen und WAN-Links ab. Ebenfalls ausschlaggebend ist die Anzahl der Server und Services sowie die Anzahl der vom StorageGRID System unterstützten Applikationen.

StorageGRID Systeme unterstützen oft mehrere Client-Applikationen. Beachten Sie dies, wenn Sie die maximale Anzahl gleichzeitiger Verbindungen bestimmen, die von einer Client-Anwendung verwendet wird. Wenn die Client-Anwendung aus mehreren Softwareeinheiten besteht, die jeweils Verbindungen zum StorageGRID-System herstellen, sollten Sie alle Verbindungen zwischen den Einheiten hinzufügen. In den folgenden Situationen müssen Sie möglicherweise die maximale Anzahl gleichzeitiger Verbindungen anpassen:

- Die Topologie des StorageGRID Systems beeinflusst die maximale Anzahl gleichzeitiger Transaktionen und Verbindungen, die das System unterstützen kann.
- Client-Applikationen, die über ein Netzwerk mit begrenzter Bandbreite mit dem StorageGRID-System interagieren, müssen möglicherweise das Maß an Parallelität verringern, um sicherzustellen, dass einzelne Transaktionen in einem angemessenen Zeitraum durchgeführt werden.
- Wenn viele Client-Applikationen das StorageGRID System gemeinsam nutzen, muss möglicherweise der Grad an Parallelität reduziert werden, um das Überschreiten der Systemgrenzen zu vermeiden.

Trennung von HTTP-Verbindungspools für Lese- und Schreibvorgänge

Es können separate Pools von HTTP-Verbindungen für Lese- und Schreibvorgänge genutzt werden, inklusive Kontrolle darüber, wie viele aus einem Pool jeweils verwendet werden. Separate Pools von HTTP-Verbindungen ermöglichen eine bessere Kontrolle von Transaktionen und einen besseren Lastausgleich.

Client-Applikationen können Lasten erzeugen, die sich auf Abruf dominant (Lesen) oder stark speichern (Schreiben). Mit separaten Pools von HTTP-Verbindungen für Lese- und Schreibtransaktionen können Sie den Umfang der einzelnen Pools für Lese- und Schreibtransaktionen anpassen.

Verwenden Sie Swift

Lesen Sie, wie Client-Applikationen die OpenStack Swift API zur Schnittstelle mit dem StorageGRID System nutzen.

- "Unterstützung für OpenStack Swift API in StorageGRID"
- "Mandantenkonten und -Verbindungen werden konfiguriert"
- "Von Swift UNTERSTÜTZTE REST-API-Operationen"
- "StorageGRID Swift REST-API-Operationen"
- "Sicherheit wird für DIE REST API konfiguriert"
- "Monitoring und Auditing von Vorgängen"

Unterstützung für OpenStack Swift API in StorageGRID

StorageGRID unterstützt die folgenden spezifischen Versionen von Swift und HTTP.

Element	Version
Swift-Spezifikation	OpenStack Swift Objekt Storage API v1 ab November 2015
HTTP	1.1 Weitere Informationen zu HTTP finden Sie unter HTTP/1.1 (RFCs 7230-35). **Hinweis**: StorageGRID unterstützt HTTP/1.1-Pipelining nicht.

Verwandte Informationen

"OpenStack: Objekt-Storage-API"

Geschichte der Unterstützung von Swift API in StorageGRID

Bei Änderungen an der Unterstützung des StorageGRID-Systems für die Swift REST-API sollten Sie auf dieser hinweisen.

Freigabe	Kommentare
11.5	Schwache Konsistenzkontrolle entfernt. Stattdessen wird die verfügbare Konsistenzstufe verwendet.
11.4	Unterstützung für TLS 1.3 und aktualisierte Liste der unterstützten TLS-Chiffre-Suites hinzugefügt. CLB ist veraltet. Beschreibung der Wechselbeziehung zwischen ILM und Konsistenzeinstellung hinzugefügt
11.3	Aktualisierte PUT-Objektvorgänge zur Beschreibung der Auswirkungen von ILM-Regeln, die synchrone Platzierung bei der Aufnahme verwenden (die ausgewogenen und strengen Optionen für das Aufnahmeverhalten) Eine zusätzliche Beschreibung der Client-Verbindungen, die Load Balancer-Endpunkte oder Hochverfügbarkeitsgruppen verwenden. Aktualisierte Liste der unterstützten TLS-Cipher-Suites. TLS 1.1-Chiffren werden nicht mehr unterstützt.
11.2	Kleine redaktionelle Änderungen des Dokuments.
11.1	Zusätzlicher Support für die Verwendung von HTTP für Swift-Client-Verbindungen zu Grid-Nodes. Die Definitionen der Konsistenzkontrollen wurden aktualisiert.
11.0	Hinzugefügter Support für 1,000 Container für jedes Mandantenkonto.

Freigabe	Kommentare
10.3	Administrative Aktualisierungen und Korrekturen des Dokuments. Abschnitte zum Konfigurieren von benutzerdefinierten Serverzertifikaten entfernt.
10.2	Unterstützung der Swift API durch das StorageGRID System zu Beginn. Die derzeit unterstützte Version ist OpenStack Swift Object Storage API v1.

So implementiert StorageGRID die Swift REST API

Eine Client-Applikation kann mithilfe von Swift REST-API-Aufrufen eine Verbindung zu Storage-Nodes und Gateway-Nodes herstellen, um Container zu erstellen und Objekte zu speichern und abzurufen. Dadurch können serviceorientierte Applikationen, die für OpenStack Swift entwickelt wurden, mit lokalem Objekt-Storage des StorageGRID Systems verbunden werden.

Swift Objekt-Management

Nach der Aufnahme von Swift Objekten im StorageGRID System werden sie von den Regeln für Information Lifecycle Management (ILM) der aktiven ILM-Richtlinie des Systems gemanagt. Die ILM-Regeln und -Richtlinie bestimmen, wie StorageGRID Kopien von Objektdaten erstellt und verteilt und wie diese Kopien mit der Zeit gemanagt werden. Eine ILM-Regel kann beispielsweise für Objekte in bestimmten Swift Containern gelten und möglicherweise angeben, dass mehrere Objektkopien für eine bestimmte Anzahl von Jahren in mehreren Datacentern gespeichert werden.

Wenden Sie sich an Ihren StorageGRID-Administrator, wenn Sie wissen müssen, welche Auswirkungen die ILM-Regeln und Richtlinien des Grid auf die Objekte in Ihrem Swift-Mandantenkonto haben.

In Konflikt stehende Clientanforderungen

Widersprüchliche Clientanforderungen, wie z. B. zwei Clients, die in denselben Schlüssel schreiben, werden auf „`latest-WINS`“-Basis gelöst. Der Zeitpunkt für die Auswertung „`latest-WINS`“ basiert darauf, wann das StorageGRID System eine bestimmte Anfrage abschließt und nicht auf, wenn Swift-Clients einen Vorgang starten.

Konsistenzgarantien und -Kontrollen

Standardmäßig bietet StorageGRID Lese-/Nachher-Konsistenz für neu erstellte Objekte und schließlich die Konsistenz von Objekt-Updates und HEAD-Operationen. Jeder GET nach einem erfolgreich abgeschlossenen PUT wird in der Lage sein, die neu geschriebenen Daten zu lesen. Überschreibungen vorhandener Objekte, Metadatenaktualisierungen und -Löschungen sind schließlich konsistent. Überschreibungen dauern in der Regel nur wenige Sekunden oder Minuten, können jedoch bis zu 15 Tage in Anspruch nehmen.

StorageGRID ermöglicht Ihnen außerdem die Kontrolle der Konsistenz einzelner Container. Sie können die Consistency Control ändern, um je nach Anforderung zwischen der Verfügbarkeit der Objekte und der Konsistenz dieser Objekte in verschiedenen Storage Nodes und Standorten einen Kompromiss zwischen der Verfügbarkeit der Objekte herzustellen.

Verwandte Informationen

"Objektmanagement mit ILM"

"ABRUFEN der Container-Konsistenzanforderung"

"PUT Container-Konsistenzanforderung"

Empfehlungen für die Implementierung der Swift REST API

Bei der Implementierung der Swift REST API zur Verwendung mit StorageGRID sollten Sie diese Empfehlungen beachten.

Empfehlungen für Köpfe zu nicht vorhandenen Objekten

Wenn Ihre Anwendung regelmäßig prüft, ob ein Objekt in einem Pfad existiert, in dem Sie nicht erwarten, dass das Objekt tatsächlich vorhanden ist, sollten Sie die Konsistenzkontrolle „`available`“ verwenden. Sie sollten z. B. die Konsistenzkontrolle „`Available`“ verwenden, wenn Ihre Anwendung EINEN HEAD-Vorgang an einem Speicherort ausführt, bevor Sie einen PUT-Vorgang an diesen Ort ausführen.

Andernfalls werden möglicherweise 500 Fehler des internen Servers angezeigt, wenn ein oder mehrere Speicherknoten nicht verfügbar sind.

Sie können die Konsistenzkontrolle „`verfügbar`“ für jeden Container mithilfe der PUT Container-Konsistenzanforderung festlegen.

Empfehlungen für Objektnamen

Als die ersten vier Zeichen von Objektnamen sollten keine Zufallswerte verwendet werden. Stattdessen sollten Sie nicht-zufällige, nicht-eindeutige Präfixe verwenden, wie z. B. Bild.

Wenn Sie in Objektnamen-Präfixen zufällige und eindeutige Zeichen verwenden müssen, sollten Sie die Objektnamen mit einem Verzeichnisnamen vorschreiben. Verwenden Sie dieses Format:

```
mycontainer/mydir/f8e3-image3132.jpg
```

Anstelle dieses Formats:

```
mycontainer/f8e3-image3132.jpg
```

Empfehlungen für „`Range reads`“

Wenn die Option **komprimiere gespeicherte Objekte** ausgewählt ist (**Konfiguration** > **Systemeinstellungen** > **Grid-Optionen**), sollten Swift-Client-Anwendungen vermeiden, GET-Objektoperationen durchzuführen, die einen Bereich von Bytes angeben. Diese Vorgänge „`range Read`“ sind ineffizient, da StorageGRID die Objekte effektiv dekomprimieren muss, um auf die angeforderten Bytes zugreifen zu können. GET-Objektvorgänge, die einen kleinen Byte-Bereich von einem sehr großen Objekt anfordern, sind besonders ineffizient, beispielsweise ist es sehr ineffizient, einen Bereich von 10 MB von einem komprimierten 50-GB-Objekt zu lesen.

Wenn Bereiche von komprimierten Objekten gelesen werden, können Client-Anforderungen eine Zeitdauer haben.

Wenn Sie Objekte komprimieren müssen und Ihre Client-Applikation Bereichslesevorgänge verwenden muss, erhöhen Sie die Zeitüberschreitung beim Lesen der Anwendung.

Verwandte Informationen

"ABRUFEN der Container-Konsistenzanforderung"

"PUT Container-Konsistenzanforderung"

"StorageGRID verwalten"

Mandantenkonten und -Verbindungen werden konfiguriert

Wenn StorageGRID konfiguriert wird, um Verbindungen von Client-Applikationen zu akzeptieren, müssen ein oder mehrere Mandantenkonten erstellt und die Verbindungen eingerichtet werden.

Erstellen und Konfigurieren von Swift Mandantenkonten

Bevor Swift API-Clients Objekte auf StorageGRID speichern und abrufen können, ist ein Swift-Mandantenkonto erforderlich. Jedes Mandantenkonto hat seine eigene Konto-ID, Gruppen und Benutzer sowie Container und Objekte.

Swift-Mandantenkonten werden von einem StorageGRID Grid-Administrator mit dem Grid Manager oder der Grid Management API erstellt.

Beim Erstellen eines Swift-Mandantenkontos gibt der Grid-Administrator folgende Informationen an:

- Anzeigename für den Mandanten (die Konto-ID des Mandanten wird automatisch zugewiesen und kann nicht geändert werden)
- 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 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.
- Wenn SSO aktiviert ist, hat die föderierte Gruppe Root-Zugriffsberechtigungen, um das Mandantenkonto zu konfigurieren.

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"

"Verwenden Sie ein Mandantenkonto"

"Unterstützte Swift-API-Endpunkte"

Wie Client-Verbindungen konfiguriert werden können

Ein Grid-Administrator trifft Konfigurationsmöglichkeiten, die Einfluss darauf haben, wie Swift-Clients sich mit StorageGRID verbinden, um Daten zu speichern und abzurufen. Die spezifischen Informationen, die benötigt werden, um eine Verbindung herzustellen, hängen von der gewählten Konfiguration ab.

Client-Applikationen können Objekte speichern oder abrufen, indem sie eine Verbindung mit folgenden Komponenten herstellen:

- Der Lastverteilungsservice an Admin-Nodes oder Gateway-Nodes oder optional die virtuelle IP-Adresse einer HA-Gruppe (High Availability, Hochverfügbarkeit) von Admin-Nodes oder Gateway-Nodes
- Der CLB-Dienst auf Gateway-Knoten oder optional die virtuelle IP-Adresse einer Hochverfügbarkeitsgruppe von Gateway-Knoten

> Der CLB-Service ist veraltet. Clients, die vor der Version StorageGRID 11.3 konfiguriert wurden, können den CLB-Service auf Gateway-Knoten weiterhin verwenden. Alle anderen Client-Applikationen, die zum Lastausgleich vom StorageGRID abhängig sind, sollten über den Load Balancer Service eine Verbindung herstellen.

- Storage-Nodes mit oder ohne externen Load Balancer

Bei der Konfiguration von StorageGRID kann ein Grid-Administrator den Grid-Manager oder die Grid-Management-API verwenden, um die folgenden Schritte auszuführen, die alle optional sind:

1. Konfigurieren von Endpunkten für den Load Balancer Service.

   Sie müssen Endpunkte konfigurieren, um den Load Balancer Service verwenden zu können. Der Lastverteilungsservice an Admin-Nodes oder Gateway-Nodes verteilt eingehende Netzwerkverbindungen von Client-Anwendungen auf Storage-Nodes. Beim Erstellen eines Load Balancer-Endpunkts gibt der StorageGRID-Administrator eine Portnummer an, ob der Endpunkt HTTP- oder HTTPS-Verbindungen akzeptiert, der Client-Typ (S3 oder Swift), der den Endpunkt verwendet, und das für HTTPS-Verbindungen zu verwendende Zertifikat (falls zutreffend).

2. Konfigurieren Sie Nicht Vertrauenswürdige Client-Netzwerke.

   Wenn ein StorageGRID-Administrator das Clientnetzwerk eines Node so konfiguriert, dass es nicht vertrauenswürdig ist, akzeptiert der Knoten nur eingehende Verbindungen im Clientnetzwerk an Ports, die explizit als Load Balancer-Endpunkte konfiguriert sind.

3. Konfigurieren Sie Hochverfügbarkeitsgruppen.

   Wenn ein Administrator eine HA-Gruppe erstellt, werden die Netzwerkschnittstellen mehrerer Admin-Nodes oder Gateway-Nodes in einer aktiv-Backup-Konfiguration platziert. Client-Verbindungen werden mithilfe der virtuellen IP-Adresse der HA-Gruppe hergestellt.

Weitere Informationen zu den einzelnen Optionen finden Sie in den Anweisungen zur Administration von StorageGRID.

Zusammenfassung: IP-Adressen und Ports für Client-Verbindungen

Client-Applikationen stellen mithilfe der IP-Adresse eines Grid-Node und der Port-Nummer eines Service auf diesem Node eine Verbindung zu StorageGRID her. Bei Konfiguration von Hochverfügbarkeitsgruppen (High Availability, HA) können Client-Applikationen eine Verbindung über die virtuelle IP-Adresse der HA-Gruppe herstellen.

Zum Erstellen von Client-Verbindungen erforderliche Informationen

Die Tabelle fasst die verschiedenen Möglichkeiten zusammen, wie Clients eine Verbindung zu StorageGRID sowie zu den für die einzelnen Verbindungstypen verwendeten IP-Adressen und Ports herstellen können. Wenden Sie sich an Ihren StorageGRID-Administrator, um weitere Informationen zu erhalten, oder lesen Sie die Anweisungen zur Administration von StorageGRID, um eine Beschreibung der Informationen im Grid-Manager zu erhalten.

Wo eine Verbindung hergestellt wird	Dienst, mit dem der Client verbunden ist	IP-Adresse	Port
HA-Gruppe	Lastausgleich	Virtuelle IP-Adresse einer HA-Gruppe	• Endpunkt-Port des Load Balancer
HA-Gruppe	CLB **Hinweis:** der CLB-Service ist veraltet.	Virtuelle IP-Adresse einer HA-Gruppe	Swift-Standardports: • HTTPS: 8083 • HTTP: 8085
Admin-Node	Lastausgleich	IP-Adresse des Admin-Knotens	• Endpunkt-Port des Load Balancer
Gateway-Node	Lastausgleich	IP-Adresse des Gateway-Node	• Endpunkt-Port des Load Balancer
Gateway-Node	CLB **Hinweis:** der CLB-Service ist veraltet.	IP-Adresse des Gateway-Node **Hinweis:** standardmäßig sind HTTP-Ports für CLB und LDR nicht aktiviert.	Swift-Standardports: • HTTPS: 8083 • HTTP: 8085
Storage-Node	LDR	IP-Adresse des Speicherknoten	Swift-Standardports: • HTTPS: 18083 • HTTP: 18085

Beispiel

Verwenden Sie eine strukturierte URL, wie unten gezeigt, um einen Swift-Client mit dem Load Balancer-Endpunkt einer HA-Gruppe von Gateway-Nodes zu verbinden:

- `https://VIP-of-HA-group:LB-endpoint-port`

Wenn beispielsweise die virtuelle IP-Adresse der HA-Gruppe 192.0.2.6 lautet und die Portnummer eines Swift Load Balancer Endpunkts 10444 ist, kann ein Swift-Client die folgende URL zur Verbindung mit StorageGRID verwenden:

- `https://192.0.2.6:10444`

Ein DNS-Name kann für die IP-Adresse konfiguriert werden, die Clients zum Herstellen der Verbindung mit StorageGRID verwenden. Wenden Sie sich an Ihren Netzwerkadministrator vor Ort.

Entscheidung über die Verwendung von HTTPS- oder HTTP-Verbindungen

Wenn Client-Verbindungen mit einem Load Balancer-Endpunkt hergestellt werden, müssen Verbindungen über das Protokoll (HTTP oder HTTPS) hergestellt werden, das für diesen Endpunkt angegeben wurde. Um HTTP für Client-Verbindungen zu Storage-Nodes oder zum CLB-Dienst auf Gateway-Knoten zu verwenden, müssen Sie dessen Verwendung aktivieren.

Wenn Client-Anwendungen eine Verbindung zu Speicherknoten oder zum CLB-Dienst auf Gateway-Knoten herstellen, müssen sie für alle Verbindungen verschlüsseltes HTTPS verwenden. Optional können Sie weniger sichere HTTP-Verbindungen aktivieren, indem Sie im Grid Manager die Option **HTTP-Verbindung** aktivieren auswählen. Eine Client-Anwendung kann beispielsweise HTTP verwenden, wenn die Verbindung zu einem Speicherknoten in einer nicht produktiven Umgebung getestet wird.

> Achten Sie bei der Aktivierung von HTTP für ein Produktionsraster darauf, dass die Anforderungen unverschlüsselt gesendet werden.

> Der CLB-Service ist veraltet.

Wenn die Option **HTTP-Verbindung aktivieren** ausgewählt ist, müssen Clients für HTTP unterschiedliche Ports verwenden als für HTTPS. Lesen Sie die Anweisungen zum Verwalten von StorageGRID.

Verwandte Informationen

"StorageGRID verwalten"

Testen der Verbindung in der Swift API-Konfiguration

Mit der Swift CLI können Sie die Verbindung zum StorageGRID System testen und überprüfen, ob Sie Objekte lesen und in das System schreiben können.

Was Sie benötigen

- Sie müssen Python-swiftclient, den Swift-Befehlszeilen-Client, heruntergeladen und installiert haben.
- Im StorageGRID System müssen Sie ein Swift Mandantenkonto haben.

Über diese Aufgabe

Wenn Sie keine Sicherheit konfiguriert haben, müssen Sie die hinzufügen `--insecure` Flag auf jeden dieser Befehle.

Schritte

1. Fragen Sie die Info-URL für Ihre StorageGRID Swift Implementierung:

```
swift
-U <Tenant_Account_ID:Account_User_Name>
-K <User_Password>
-A https://<FQDN | IP>:<Port>/info
capabilities
```

Dies reicht aus, um zu testen, ob Ihre Swift-Implementierung funktionsfähig ist. Um die Kontenkonfiguration durch Speichern eines Objekts weiter zu testen, fahren Sie mit den zusätzlichen Schritten fort.

2. Legen Sie ein Objekt in den Container:

```
touch test_object
swift
-U <Tenant_Account_ID:Account_User_Name>
-K <User_Password>
-A https://<FQDN | IP>:<Port>/auth/v1.0
upload test_container test_object
--object-name test_object
```

3. Holen Sie sich den Container, um das Objekt zu überprüfen:

```
swift
-U <Tenant_Account_ID:Account_User_Name>
-K <User_Password>
-A https://<FQDN | IP>:<Port>/auth/v1.0
list test_container
```

4. Löschen Sie das Objekt:

```
swift
-U <Tenant_Account_ID:Account_User_Name>
-K <User_Password>
-A https://<FQDN | IP>:<Port>/auth/v1.0
delete test_container test_object
```

5. Löschen Sie den Container:

```
swift
-U `<_Tenant_Account_ID:Account_User_Name_>`
-K `<_User_Password_>`
-A `\https://<_FQDN_ | _IP_>:<_Port_>/auth/v1.0'
delete test_container
```

Verwandte Informationen

"Erstellen und Konfigurieren von Swift Mandantenkonten"

"Sicherheit wird für DIE REST API konfiguriert"

Von Swift UNTERSTÜTZTE REST-API-Operationen

Das StorageGRID System unterstützt die meisten Operationen in der OpenStack Swift API. Informieren Sie sich vor der Integration von Swift REST API Clients mit StorageGRID über die Implementierungsdetails für Konto-, Container- und Objektvorgänge.

Von StorageGRID unterstützte Vorgänge

Die folgenden Swift-API-Operationen werden unterstützt:

- "Konto-Operationen"
- "Container-Operationen"
- "Objekt-Operationen"

Gemeinsame Antwortheader für alle Vorgänge

Das StorageGRID-System implementiert alle gemeinsamen Header für unterstützte Vorgänge, wie sie von der OpenStack Swift Objekt-Storage-API v1 definiert wurden.

Verwandte Informationen

"OpenStack: Objekt-Storage-API"

Unterstützte Swift-API-Endpunkte

StorageGRID unterstützt die folgenden Swift-API-Endpunkte: Die Info-URL, die auth-URL und die Storage-URL.

Info-URL

Sie können die Funktionen und Einschränkungen der StorageGRID-Swift-Implementierung bestimmen, indem Sie eine GET-Anfrage an die Swift-Basis-URL mit dem /info-Pfad senden.

```
https://FQDN | Node IP:Swift Port/info/
```

In der Anfrage:

- *`FQDN`* Ist der vollständig qualifizierte Domain-Name.
- *`Node IP`* Ist die IP-Adresse für den Storage-Node oder den Gateway-Node im StorageGRID-Netzwerk.
- *`Swift Port`* Ist die Portnummer, die für Swift-API-Verbindungen auf dem Storage-Node oder Gateway-Node verwendet wird.

Die folgende Info-URL würde beispielsweise Informationen von einem Storage-Node mit der IP-Adresse von 10.99.106.103 anfordern und Port 18083 verwenden.

```
https://10.99.106.103:18083/info/
```

Die Antwort umfasst die Funktionen der Swift-Implementierung als JSON-Wörterbuch. Ein Client-Tool kann die JSON-Antwort analysieren, um die Funktionen der Implementierung zu bestimmen und sie als Einschränkungen für nachfolgende Storage-Vorgänge zu verwenden.

Die StorageGRID-Implementierung von Swift ermöglicht nicht authentifizierten Zugriff auf die Info-URL.

Auth-URL

Ein Client kann die Swift auth URL verwenden, um sich als Benutzer eines Mandantenkontos zu authentifizieren.

```
https://FQDN | Node IP:Swift Port/auth/v1.0/
```

Sie müssen die Mandanten-Konto-ID, den Benutzernamen und das Passwort als Parameter in angeben `X-Auth-User` Und `X-Auth-Key` Anforderungs-Header wie folgt:

```
X-Auth-User: Tenant_Account_ID:Username

X-Auth-Key: Password
```

In den Kopfzeilen der Anfrage:

- *`Tenant_Account_ID`* Ist die Account-ID, die StorageGRID beim Erstellen des Swift-Mandanten zugewiesen hat. Dies ist die gleiche Mandantenkonto-ID, die auf der Anmeldeseite des Mandanten-Managers verwendet wird.
- *`Username`* Ist der Name eines im Mandanten-Manager erstellten Benutzers. Dieser Benutzer muss einer Gruppe angehören, die über die Swift Administrator-Berechtigung verfügt. Der Root-Benutzer des Mandanten kann nicht für die Verwendung der Swift REST API konfiguriert werden.

  Wenn Identity Federation für das Mandantenkonto aktiviert ist, geben Sie den Benutzernamen und das Passwort des föderierten Benutzers vom LDAP-Server an. Geben Sie alternativ den Domänennamen des LDAP-Benutzers an. Beispiel:

  ```
  X-Auth-User: Tenant_Account_ID:Username@Domain_Name
  ```

- *`Password`* Ist das Passwort für den Mandantenbenutzer. Benutzerpasswörter werden im Mandanten-Manager erstellt und gemanagt.

Als Antwort auf eine erfolgreiche Authentifizierungsanforderung werden eine Storage-URL und ein auth-Token zurückgegeben:

```
X-Storage-Url: https://FQDN | Node_IP:Swift_Port/v1/Tenant_Account_ID

X-Auth-Token: token

X-Storage-Token: token
```

Das Token ist standardmäßig für 24 Stunden ab der Erzeugung gültig.

Token werden für ein bestimmtes Mandantenkonto generiert. Ein gültiges Token für ein Konto ermächtigt einen Benutzer nicht, auf ein anderes Konto zuzugreifen.

Storage-URL

Eine Client-Applikation kann Swift-REST-API-Aufrufe ausstellen, um unterstützte Konto-, Container- und Objektvorgänge mit einem Gateway-Node oder Storage-Node durchzuführen. Storage-Anforderungen werden an die in der Authentifizierungsantwort zurückgegebene Storage-URL adressiert. Die Anforderung muss auch die Kopfzeile von X-Auth-Token und den Wert enthalten, der von der auth-Anforderung zurückgegeben wurde.

```
https://FQDN | IP:Swift_Port/v1/Tenant_Account_ID

[/container][/object]

X-Auth-Token: token
```

Einige Kopf für Speicherantwort, die Nutzungsstatistiken enthalten, geben möglicherweise keine genauen Zahlen für kürzlich geänderte Objekte wieder. Es kann einige Minuten dauern, bis genaue Zahlen in diesen Kopfzeilen angezeigt werden.

Die folgenden Antwortkopfzeilen für Konto- und Container-Vorgänge sind Beispiele für solche, die Nutzungsstatistiken enthalten:

- `X-Account-Bytes-Used`
- `X-Account-Object-Count`
- `X-Container-Bytes-Used`
- `X-Container-Object-Count`

Verwandte Informationen

"Wie Client-Verbindungen konfiguriert werden können"

"Erstellen und Konfigurieren von Swift Mandantenkonten"

"Konto-Operationen"

"Container-Operationen"

"Objekt-Operationen"

Konto-Operationen

Die folgenden Swift-API-Vorgänge werden bei Accounts durchgeführt.

GET Konto

Dieser Vorgang ruft die Containerliste ab, die mit den Statistiken zur Konto- und Kontonutzung verknüpft ist.

Der folgende Parameter für die Anfrage ist erforderlich:

- `Account`

Die folgende Anfrageüberschrift ist erforderlich:

- `X-Auth-Token`

Die folgenden unterstützten Abfrageparameter sind optional:

- `Delimiter`
- `End_marker`
- `Format`
- `Limit`
- `Marker`
- `Prefix`

Eine erfolgreiche Ausführung gibt die folgenden Header mit einer „`HTTP/1.1 204 No Content`“-Antwort zurück, wenn das Konto gefunden wurde und keine Container oder die Containerliste leer ist; oder eine „`HTTP/1.1 200 OK`“-Antwort, wenn das Konto gefunden wurde und die Containerliste nicht leer ist:

- `Accept-Ranges`
- `Content-Length`
- `Content-Type`
- `Date`
- `X-Account-Bytes-Used`
- `X-Account-Container-Count`
- `X-Account-Object-Count`
- `X-Timestamp`
- `X-Trans-Id`

HEAD Konto

Mit dieser Operation werden Kontoinformationen und Statistiken von einem Swift-Konto abgerufen.

Der folgende Parameter für die Anfrage ist erforderlich:

- `Account`

Die folgende Anfrageüberschrift ist erforderlich:

- `X-Auth-Token`

Bei einer erfolgreichen Ausführung werden die folgenden Header mit einer „`HTTP/1.1 204 No Content`“-Antwort zurückgegeben:

- `Accept-Ranges`
- `Content-Length`
- `Date`
- `X-Account-Bytes-Used`
- `X-Account-Container-Count`
- `X-Account-Object-Count`

- `X-Timestamp`
- `X-Trans-Id`

Verwandte Informationen

"In den Audit-Protokollen werden Swift-Vorgänge nachverfolgt"

Container-Operationen

StorageGRID unterstützt maximal 1,000 Container pro Swift Konto. Die folgenden Swift-API-Vorgänge werden auf Containern durchgeführt.

Container LÖSCHEN

Durch diesen Vorgang wird ein leerer Container aus einem Swift-Konto in einem StorageGRID-System entfernt.

Die folgenden Anfrageparameter sind erforderlich:

- `Account`
- `Container`

Die folgende Anfrageüberschrift ist erforderlich:

- `X-Auth-Token`

Eine erfolgreiche Ausführung gibt die folgenden Kopfzeilen mit einer HTTP/1.1 204 No Content-Antwort zurück:

- `Content-Length`
- `Content-Type`
- `Date`
- `X-Trans-Id`

GET Container

Dieser Vorgang ruft die dem Container zugeordnete Objektliste sowie die Containerstatistiken und Metadaten in einem StorageGRID System ab.

Die folgenden Anfrageparameter sind erforderlich:

- `Account`
- `Container`

Die folgende Anfrageüberschrift ist erforderlich:

- `X-Auth-Token`

Die folgenden unterstützten Abfrageparameter sind optional:

- `Delimiter`

- `End_marker`
- `Format`
- `Limit`
- `Marker`
- `Path`
- `Prefix`

Eine erfolgreiche Ausführung liefert die folgenden Header mit einer "HTTP/1.1 200 success" oder einer "HTTP/1.1 204 No Content"-Antwort:

- `Accept-Ranges`
- `Content-Length`
- `Content-Type`
- `Date`
- `X-Container-Bytes-Used`
- `X-Container-Object-Count`
- `X-Timestamp`
- `X-Trans-Id`

KOPF Behälter

Dieser Vorgang ruft Containerstatistiken und Metadaten aus einem StorageGRID System ab.

Die folgenden Anfrageparameter sind erforderlich:

- `Account`
- `Container`

Die folgende Anfrageüberschrift ist erforderlich:

- `X-Auth-Token`

Eine erfolgreiche Ausführung gibt die folgenden Kopfzeilen mit einer HTTP/1.1 204 No Content-Antwort zurück:

- `Accept-Ranges`
- `Content-Length`
- `Date`
- `X-Container-Bytes-Used`
- `X-Container-Object-Count`
- `X-Timestamp`
- `X-Trans-Id`

Legen Sie den Behälter

Durch diesen Vorgang wird ein Container für ein Konto in einem StorageGRID-System erstellt.

Die folgenden Anfrageparameter sind erforderlich:

- `Account`
- `Container`

Die folgende Anfrageüberschrift ist erforderlich:

- `X-Auth-Token`

Eine erfolgreiche Ausführung gibt die folgenden Header mit einer "HTTP/1.1 201 created" oder "HTTP/1.1 202 Accepted" (falls der Container bereits unter diesem Konto existiert) Antwort zurück:

- `Content-Length`
- `Date`
- `X-Timestamp`
- `X-Trans-Id`

Container-Name muss im StorageGRID-Namespace eindeutig sein. Wenn der Container unter einem anderen Konto vorhanden ist, wird der folgende Header zurückgegeben: „HTTP/1.1 409-Konflikt“.

Verwandte Informationen

"In den Audit-Protokollen werden Swift-Vorgänge nachverfolgt"

Objekt-Operationen

Die folgenden Swift-API-Vorgänge werden an Objekten durchgeführt.

Delete Objekt

Durch diesen Vorgang werden der Inhalt und die Metadaten eines Objekts aus dem StorageGRID System gelöscht.

Die folgenden Anfrageparameter sind erforderlich:

- `Account`
- `Container`
- `Object`

Die folgende Anfrageüberschrift ist erforderlich:

- `X-Auth-Token`

Bei einer erfolgreichen Ausführung werden die folgenden Antwortheadern mit einem zurückgegeben `HTTP/1.1 204 No Content` Antwort:

- `Content-Length`

- `Content-Type`
- `Date`
- `X-Trans-Id`

Bei der Verarbeitung einer LÖSCHOBJEKTANFORDERUNG versucht StorageGRID, alle Kopien des Objekts sofort von allen gespeicherten Speicherorten zu entfernen. Wenn erfolgreich, gibt StorageGRID sofort eine Antwort an den Client zurück. Falls nicht alle Kopien innerhalb von 30 Sekunden entfernt werden können (z. B. weil ein Standort vorübergehend nicht verfügbar ist), warteschlangen StorageGRID die Kopien zum Entfernen und zeigen dann den Erfolg des Clients an.

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

GET Objekt

Dieser Vorgang ruft den Objektinhalt ab und ruft die Objektmetadaten von einem StorageGRID System ab.

Die folgenden Anfrageparameter sind erforderlich:

- `Account`
- `Container`
- `Object`

Die folgende Anfrageüberschrift ist erforderlich:

- `X-Auth-Token`

Die folgenden Anfragezeilen sind optional:

- `Accept-Encoding`
- `If-Match`
- `If-Modified-Since`
- `If-None-Match`
- `If-Unmodified-Since`
- `Range`

Bei einer erfolgreichen Ausführung werden die folgenden Kopfzeilen mit einem zurückgegeben `HTTP/1.1 200 OK` Antwort:

- `Accept-Ranges`
- `Content-Disposition`, Nur wenn zurückgegeben `Content-Disposition` Es wurden Metadaten festgelegt
- `Content-Encoding`, Nur wenn zurückgegeben `Content-Encoding` Es wurden Metadaten festgelegt
- `Content-Length`
- `Content-Type`

- `Date`
- `ETag`
- `Last-Modified`
- `X-Timestamp`
- `X-Trans-Id`

HEAD Objekt

Dieser Vorgang ruft Metadaten und Eigenschaften eines aufgenommene Objekts von einem StorageGRID System ab.

Die folgenden Anfrageparameter sind erforderlich:

- `Account`
- `Container`
- `Object`

Die folgende Anfrageüberschrift ist erforderlich:

- `X-Auth-Token`

Eine erfolgreiche Ausführung gibt die folgenden Header mit einer HTTP/1.1 200 OK-Antwort zurück:

- `Accept-Ranges`
- `Content-Disposition`, Nur wenn zurückgegeben `Content-Disposition` Es wurden Metadaten festgelegt
- `Content-Encoding`, Nur wenn zurückgegeben `Content-Encoding` Es wurden Metadaten festgelegt
- `Content-Length`
- `Content-Type`
- `Date`
- `ETag`
- `Last-Modified`
- `X-Timestamp`
- `X-Trans-Id`

PUT Objekt

Durch diesen Vorgang wird ein neues Objekt mit Daten und Metadaten erstellt oder ein vorhandenes Objekt durch Daten und Metadaten in einem StorageGRID System ersetzt.

StorageGRID unterstützt Objekte mit einer Größe von bis zu 5 TB.

> Widersprüchliche Clientanforderungen, wie z. B. zwei Clients, die in denselben Schlüssel schreiben, werden auf „`latest-WINS`“-Basis gelöst. Der Zeitpunkt für die Auswertung „`latest-WINS`“ basiert darauf, wann das StorageGRID System eine bestimmte Anfrage abschließt und nicht auf, wenn Swift-Clients einen Vorgang starten.

Die folgenden Anfrageparameter sind erforderlich:

- `Account`
- `Container`
- `Object`

Die folgende Anfrageüberschrift ist erforderlich:

- `X-Auth-Token`

Die folgenden Anfragezeilen sind optional:

- `Content-Disposition`
- `Content-Encoding`

  Verwenden Sie keine Punkte `Content-Encoding` Wenn die ILM-Regel für ein Objekt Objekte nach der Größe filtert und synchrone Platzierung bei der Aufnahme verwendet wird (die ausgewogenen oder strengen Optionen für das Aufnahmeverhalten).

- `Transfer-Encoding`

  Verwenden Sie keine komprimierten oder chunked `Transfer-Encoding` Wenn die ILM-Regel für ein Objekt Objekte nach der Größe filtert und synchrone Platzierung bei der Aufnahme verwendet wird (die ausgewogenen oder strengen Optionen für das Aufnahmeverhalten).

- `Content-Length`

  Wenn eine ILM-Regel Objekte nach Größe filtert und bei der Aufnahme synchrone Platzierung verwendet, müssen Sie angeben `Content-Length`.

  > Wenn Sie diese Richtlinien für nicht befolgen `Content-Encoding`, `Transfer-Encoding`, und `Content-Length`, StorageGRID muss das Objekt speichern, bevor es die Objektgröße bestimmen kann und die ILM-Regel anwenden kann. Das heißt, StorageGRID muss standardmäßig vorläufige Kopien eines Objekts bei der Aufnahme erstellen. Das heißt, StorageGRID muss die Dual-Commit-Option für das Ingest-Verhalten verwenden.

  Weitere Informationen zur synchronen Platzierung und zu ILM-Regeln finden Sie in den Anweisungen zum Managen von Objekten mit Information Lifecycle Management.

- `Content-Type`
- `ETag`
- `X-Object-Meta-<name\>` (Objektbezogene Metadaten)

  Wenn Sie die Option **Benutzerdefinierte Erstellungszeit** als Referenzzeit für eine ILM-Regel verwenden möchten, müssen Sie den Wert in einem benutzerdefinierten Header mit dem Namen speichern `X-`

`Object-Meta-Creation-Time`. Beispiel:

```
X-Object-Meta-Creation-Time: 1443399726
```

Dieses Feld wird seit dem 1. Januar 1970 als Sekunden ausgewertet.

- `X-Storage-Class: reduced_redundancy`

  Diese Kopfzeile wirkt sich darauf aus, wie viele Objektkopien StorageGRID erstellt werden, wenn die ILM-Regel, die mit einem aufgenommenen Objekt übereinstimmt, ein Aufnahmeverhalten der Dual-Commit oder Balance angibt.

  - **Dual Commit**: Wenn die ILM-Regel die Dual Commit-Option für das Aufnahmeverhalten angibt, erstellt StorageGRID bei Aufnahme des Objekts eine einzelne Interimskopie (Single Commit).
  - **Ausgewogen**: Wenn die ILM-Regel die ausgewogene Option angibt, erstellt StorageGRID nur eine einzige Zwischenkopie, wenn das System nicht sofort alle in der Regel festgelegten Kopien erstellen kann. Wenn StorageGRID eine synchrone Platzierung durchführen kann, hat diese Kopfzeile keine Auswirkung.

    Der `reduced_redundancy` Kopfzeile eignet sich am besten, wenn die ILM-Regel, die dem Objekt entspricht, eine einzige replizierte Kopie erstellt. In diesem Fall verwenden `reduced_redundancy` Eine zusätzliche Objektkopie kann bei jedem Aufnahmevorgang nicht mehr erstellt und gelöscht werden.

    Verwenden der `reduced_redundancy` Header wird unter anderen Umständen nicht empfohlen, da dies das Risiko für den Verlust von Objektdaten während der Aufnahme erhöht. Beispielsweise können Sie Daten verlieren, wenn die einzelne Kopie zunächst auf einem Storage Node gespeichert wird, der ausfällt, bevor eine ILM-Evaluierung erfolgen kann.

    > ⓘ Da nur eine Kopie zu einem beliebigen Zeitpunkt repliziert werden kann, sind Daten einem ständigen Verlust ausgesetzt. Wenn nur eine replizierte Kopie eines Objekts vorhanden ist, geht dieses Objekt verloren, wenn ein Speicherknoten ausfällt oder einen beträchtlichen Fehler hat. Während Wartungsarbeiten wie Upgrades verlieren Sie auch vorübergehend den Zugriff auf das Objekt.

  Beachten Sie, dass Sie angeben `reduced_redundancy` Wirkt sich nur darauf aus, wie viele Kopien erstellt werden, wenn ein Objekt zum ersten Mal aufgenommen wird. Er hat keine Auswirkungen auf die Anzahl der Kopien des Objekts, wenn das Objekt von der aktiven ILM-Richtlinie geprüft wird, und führt nicht dazu, dass Daten auf einer niedrigeren Redundanzebene im StorageGRID System gespeichert werden.

Eine erfolgreiche Ausführung gibt die folgenden Header mit einer "HTTP/1.1 201 created"-Antwort zurück:

- `Content-Length`
- `Content-Type`
- `Date`
- `ETag`
- `Last-Modified`

- `X-Trans-Id`

Verwandte Informationen

"Objektmanagement mit ILM"

"In den Audit-Protokollen werden Swift-Vorgänge nachverfolgt"

OPTIONEN anfordern

Die OPTIONEN Request überprüft die Verfügbarkeit eines einzelnen Swift Service. Die OPTIONSANFORDERUNG wird vom in der URL angegebenen Speicherknoten oder Gateway-Node verarbeitet.

OPTIONEN

Client-Anwendungen können zum Beispiel eine OPTIONSANFORDERUNG an den Swift-Port auf einem Storage Node stellen, ohne Swift-Authentifizierungsdaten bereitzustellen, um zu ermitteln, ob der Storage-Node verfügbar ist. Sie können diese Anforderung zum Monitoring verwenden oder um externen Lastausgleich zu ermöglichen, wenn ein Storage-Node ausfällt.

Bei Verwendung mit der Info-URL oder der Speicher-URL gibt die OPTIONSMETHODE eine Liste der unterstützten Verben für die angegebene URL zurück (z. B. KOPF, GET, OPTIONEN und PUT). DIE OPTIONSMETHODE kann nicht mit der auth URL verwendet werden.

Der folgende Parameter für die Anfrage ist erforderlich:

- `Account`

Die folgenden Anfrageparameter sind optional:

- `Container`
- `Object`

Bei einer erfolgreichen Ausführung werden die folgenden Header mit einer „`HTTP/1.1 204 No Content`“-Antwort zurückgegeben. Für die ANFORDERUNG VON OPTIONEN an die Speicher-URL ist nicht erforderlich, dass das Ziel vorhanden ist.

- `Allow` (Eine Liste der unterstützten Verben für die angegebene URL, z. B. „KOPF“, „ABRUFEN“, „OPTIONEN“, Und PUT)
- `Content-Length`
- `Content-Type`
- `Date`
- `X-Trans-Id`

Verwandte Informationen

"Unterstützte Swift-API-Endpunkte"

Fehlerantworten bei Swift-API-Operationen

Das Verständnis möglicher Fehlerantworten kann Ihnen bei der Fehlerbehebung helfen.

Wenn während eines Vorgangs Fehler auftreten, werden möglicherweise die folgenden HTTP-Statuscodes zurückgegeben:

Swift-Fehlername	HTTP-Status
AccountNameTooLong, ContainerNameTooLong, HeaderTooBig, InvalidContainerName, InvalidRequest, InvalidURI, MetadataNameTooLong, MetadaValueTooBig, MissingSecurityHeader, ObjectNameTooLong, TooManyContainers, TooManyMetadataItems, TotalMetadaTooLarge	400 Fehlerhafte Anfrage
AccessDenied	403 Verbotene
ContainerNotEmpty, ContainerAlreadyExists	409 Konflikt
Interner Fehler	500 Fehler Des Internen Servers
InvalidRange	416 Angeforderter Bereich Nicht Zu Unterprüfbar
MethodenAlled	405 Methode Nicht Zulässig
MissingContentLänge	411 Länge Erforderlich
Nicht gefunden	404 Nicht Gefunden
NotImplemsted	501 Nicht Implementiert
Vorbedingungen nicht möglich	412 Voraussetzung Fehlgeschlagen
ResourceNotFound	404 Nicht Gefunden
Nicht Autorisiert	401 Nicht Autorisiert
Nicht verarbeitbarEntity	422 Nicht Verarbeitbare Einheit

StorageGRID Swift REST-API-Operationen

Speziell für das StorageGRID System wurden Vorgänge zur Swift REST API hinzugefügt.

ABRUFEN der Container-Konsistenzanforderung

Die Konsistenzstufe sorgt für einen Kompromiss zwischen der Verfügbarkeit der Objekte und der Konsistenz dieser Objekte über verschiedene Speicherknoten und Standorte hinweg. Die GET Container-Konsistenzanforderung ermöglicht es Ihnen, die auf einen bestimmten Container angewendete Konsistenzstufe zu bestimmen.

Anfrage

HTTP-Header anfordern	Beschreibung
`X-Auth-Token`	Gibt das Swift-Authentifizierungs-Token für das Konto an, das für die Anforderung verwendet werden soll.
`x-ntap-sg-consistency`	Gibt den Anforderungstyp an, wobei `true` = GET Containerkonsistenz, und `false` = get Container.
`Host`	Der Hostname, auf den die Anforderung gerichtet ist.

Anforderungsbeispiel

```
GET /v1/28544923908243208806/Swift container
X-Auth-Token: SGRD_3a877009a2d24cb1801587bfa9050f29
x-ntap-sg-consistency: true
Host: test.com
```

Antwort

HTTP-Kopfzeile für Antwort	Beschreibung
`Date`	Datum und Uhrzeit der Antwort.
`Connection`	Ob die Verbindung zum Server offen oder geschlossen ist.
`X-Trans-Id`	Die eindeutige Transaktions-ID für die Anforderung.
`Content-Length`	Die Länge des Reaktionskörpers.

HTTP-Kopfzeile für Antwort	Beschreibung
`x-ntap-sg-consistency`	Die auf den Container angewendete Konsistenzkontrollebene. Folgende Werte werden unterstützt: • **Alle**: Alle Knoten erhalten die Daten sofort oder die Anfrage schlägt fehl. • **Strong-global**: Garantiert Lese-After-Write-Konsistenz für alle Kundenanfragen über alle Standorte hinweg. • **Strong-site**: Garantiert Lese-After-Write Konsistenz für alle Kundenanfragen innerhalb einer Site. • **Read-after-New-write**: Sorgt für die Konsistenz von Read-after-write für neue Objekte und eventuelle Konsistenz von Objekt-Updates. Hochverfügbarkeit und garantierte Datensicherung **Hinweis**: Wenn Ihre Anwendung HEAD Requests für Objekte verwendet, die nicht existieren, erhalten Sie möglicherweise eine hohe Anzahl von 500 internen Serverfehlern, wenn ein oder mehrere Speicherknoten nicht verfügbar sind. Um diese Fehler zu vermeiden, verwenden Sie die Ebene „`Available`“. • **Verfügbar** (eventuelle Konsistenz für KOPFOPERATIONEN): Verhält sich wie das “read-after-New-write” Konsistenzniveau, bietet aber nur eventuelle Konsistenz für DEN KOPFBETRIEB. Bietet höhere Verfügbarkeit FÜR HEAD-Operationen als „`read-after-New-write`“, wenn Storage Nodes nicht verfügbar sind.

Antwortbeispiel

```
HTTP/1.1 204 No Content
Date: Sat, 29 Nov 2015 01:02:18 GMT
Connection: CLOSE
X-Trans-Id: 1936575373
Content-Length: 0
x-ntap-sg-consistency: strong-site
```

Verwandte Informationen

"Verwenden Sie ein Mandantenkonto"

PUT Container-Konsistenzanforderung

Die PUT Container-Konsistenzanforderung ermöglicht es Ihnen, die Konsistenzstufe für die Operationen anzugeben, die auf einem Container ausgeführt werden. Standardmäßig werden neue Container mithilfe der Konsistenzstufe „`read-after-New-write`“ erstellt.

Anfrage

HTTP-Header anfordern	Beschreibung
`X-Auth-Token`	Swift Authentifizierungs-Token für das Konto zur Verwendung für die Anforderung.
`x-ntap-sg-consistency`	Die Konsistenzkontrollebene gilt für Container-Operationen. Folgende Werte werden unterstützt: • **Alle**: Alle Knoten erhalten die Daten sofort oder die Anfrage schlägt fehl. • **Strong-global**: Garantiert Lese-After-Write-Konsistenz für alle Kundenanfragen über alle Standorte hinweg. • **Strong-site**: Garantiert Lese-After-Write Konsistenz für alle Kundenanfragen innerhalb einer Site. • **Read-after-New-write**: Sorgt für die Konsistenz von Read-after-write für neue Objekte und eventuelle Konsistenz von Objekt-Updates. Hochverfügbarkeit und garantierte Datensicherung **Hinweis**: Wenn Ihre Anwendung HEAD Requests für Objekte verwendet, die nicht existieren, erhalten Sie möglicherweise eine hohe Anzahl von 500 internen Serverfehlern, wenn ein oder mehrere Speicherknoten nicht verfügbar sind. Um diese Fehler zu vermeiden, verwenden Sie die Ebene „`Available`“. • **Verfügbar** (eventuelle Konsistenz für KOPFOPERATIONEN): Verhält sich wie das “read-after-New-write” Konsistenzniveau, bietet aber nur eventuelle Konsistenz für DEN KOPFBETRIEB. Bietet höhere Verfügbarkeit FÜR HEAD-Operationen als „`read-after-New-write`“, wenn Storage Nodes nicht verfügbar sind.
`Host`	Der Hostname, auf den die Anforderung gerichtet ist.

Konsistenzkontrollen und ILM-Regeln interagieren, um die Datensicherung zu beeinträchtigen

Die Wahl der Konsistenzkontrolle und der ILM-Regel haben Auswirkungen auf den Schutz von Objekten. Diese Einstellungen können interagieren.

Die beim Speichern eines Objekts verwendete Konsistenzkontrolle beeinflusst beispielsweise die anfängliche Platzierung von Objekt-Metadaten, während das für die ILM-Regel ausgewählte Aufnahmeverhalten sich auf die anfängliche Platzierung von Objektkopien auswirkt. Da StorageGRID Zugriff auf die Metadaten eines Objekts und seine Daten benötigt, um Kundenanforderungen zu erfüllen, kann die Auswahl der passenden Sicherungsstufen für Konsistenz und Aufnahme-Verhalten eine bessere Erstsicherung und zuverlässigere Systemantworten ermöglichen.

Die folgenden Aufnahmeverhalten stehen für ILM-Regeln zur Verfügung:

- **Streng**: Alle in der ILM-Regel angegebenen Kopien müssen erstellt werden, bevor der Erfolg an den Client zurückgesendet wird.
- **Ausgewogen**: StorageGRID versucht bei der Aufnahme alle in der ILM-Regel festgelegten Kopien zu erstellen; wenn dies nicht möglich ist, werden Zwischenkopien erstellt und der Erfolg an den Client zurückgesendet. Die Kopien, die in der ILM-Regel angegeben sind, werden, wenn möglich gemacht.
- **Dual Commit**: StorageGRID erstellt sofort Zwischenkopien des Objekts und gibt den Erfolg an den Kunden zurück. Kopien, die in der ILM-Regel angegeben sind, werden nach Möglichkeit erstellt.

> Lesen Sie vor der Auswahl des Aufnahmeverhaltens für eine ILM-Regel die vollständige Beschreibung dieser Einstellungen in den Anweisungen zum Managen von Objekten mit Information Lifecycle Management.

Beispiel für die Interaktion zwischen Konsistenzkontrolle und ILM-Regel

Angenommen, Sie haben ein Grid mit zwei Standorten mit der folgenden ILM-Regel und der folgenden Einstellung für die Konsistenzstufe:

- **ILM-Regel**: Erstellen Sie zwei Objektkopien, eine am lokalen Standort und eine an einem entfernten Standort. Das strikte Aufnahmeverhalten wird ausgewählt.
- **Konsistenzstufe**: “strong-global” (Objektmetadaten werden sofort auf alle Standorte verteilt.)

Wenn ein Client ein Objekt im Grid speichert, erstellt StorageGRID sowohl Objektkopien als auch verteilt Metadaten an beiden Standorten, bevor der Kunde zum Erfolg zurückkehrt.

Das Objekt ist zum Zeitpunkt der Aufnahme der Nachricht vollständig gegen Verlust geschützt. Wenn beispielsweise der lokale Standort kurz nach der Aufnahme verloren geht, befinden sich Kopien der Objektdaten und der Objektmetadaten am Remote-Standort weiterhin. Das Objekt kann vollständig abgerufen werden.

Falls Sie stattdessen dieselbe ILM-Regel und die Konsistenzstufe „`strong-Site`“ verwendet haben, erhält der Client möglicherweise eine Erfolgsmeldung, nachdem die Objektdaten an den Remote Standort repliziert wurden, aber bevor die Objektmetadaten dort verteilt werden. In diesem Fall entspricht die Sicherung von Objektmetadaten nicht dem Schutzniveau für Objektdaten. Falls der lokale Standort kurz nach der Aufnahme verloren geht, gehen Objektmetadaten verloren. Das Objekt kann nicht abgerufen werden.

Die Wechselbeziehung zwischen Konsistenzstufen und ILM-Regeln kann komplex sein. Wenden Sie sich an NetApp, wenn Sie Hilfe benötigen.

Anforderungsbeispiel

```
PUT /v1/28544923908243208806/_Swift container_
X-Auth-Token: SGRD_3a877009a2d24cb1801587bfa9050f29
x-ntap-sg-consistency: strong-site
Host: test.com
```

Antwort

HTTP-Kopfzeile für Antwort	Beschreibung
`Date`	Datum und Uhrzeit der Antwort.
`Connection`	Ob die Verbindung zum Server offen oder geschlossen ist.
`X-Trans-Id`	Die eindeutige Transaktions-ID für die Anforderung.
`Content-Length`	Die Länge des Reaktionskörpers.

Antwortbeispiel

```
HTTP/1.1 204 No Content
Date: Sat, 29 Nov 2015 01:02:18 GMT
Connection: CLOSE
X-Trans-Id: 1936575373
Content-Length: 0
```

Verwandte Informationen

"Verwenden Sie ein Mandantenkonto"

Sicherheit wird für DIE REST API konfiguriert

Sie sollten die für DIE REST API implementierten Sicherheitsmaßnahmen überprüfen und verstehen, wie Sie Ihr System sichern können.

So bietet StorageGRID Sicherheit für DIE REST-API

Sie sollten verstehen, wie das StorageGRID System die Sicherheit, Authentifizierung und Autorisierung für DIE REST-API implementiert.

StorageGRID setzt die folgenden Sicherheitsmaßnahmen ein.

- Die Client-Kommunikation mit dem Load Balancer-Service erfolgt über HTTPS, wenn HTTPS für den Load Balancer-Endpunkt konfiguriert ist.

  Wenn Sie einen Endpunkt für den Load Balancer konfigurieren, kann HTTP optional aktiviert werden.

Möglicherweise möchten Sie beispielsweise HTTP für Tests oder andere Zwecke verwenden, die nicht aus der Produktion stammen. Weitere Informationen finden Sie in den Anweisungen zum Verwalten von StorageGRID.

- Standardmäßig verwendet StorageGRID HTTPS für die Client-Kommunikation mit Speicherknoten und den CLB-Service auf Gateway-Knoten.

  HTTP kann optional für diese Verbindungen aktiviert werden. Möglicherweise möchten Sie beispielsweise HTTP für Tests oder andere Zwecke verwenden, die nicht aus der Produktion stammen. Weitere Informationen finden Sie in den Anweisungen zum Verwalten von StorageGRID.

  Der CLB-Service ist veraltet.

- Die Kommunikation zwischen StorageGRID und dem Client wird über TLS verschlüsselt.
- Die Kommunikation zwischen dem Load Balancer-Service und den Speicherknoten innerhalb des Grid wird verschlüsselt, ob der Load Balancer-Endpunkt für die Annahme von HTTP- oder HTTPS-Verbindungen konfiguriert ist.
- Clients müssen HTTP-Authentifizierungskopfzeilen an StorageGRID bereitstellen, um REST-API-Vorgänge durchzuführen.

Sicherheitszertifikate und Clientanwendungen

Clients können eine Verbindung zum Lastverteilungsservice auf Gateway-Knoten oder Admin-Nodes, direkt zu Storage-Nodes oder zum CLB-Dienst auf Gateway-Nodes herstellen.

Clientanwendungen können in jedem Fall TLS-Verbindungen herstellen, indem sie entweder ein vom Grid-Administrator hochgeladenes benutzerdefiniertes Serverzertifikat oder ein vom StorageGRID-System generiertes Zertifikat verwenden:

- Wenn Client-Anwendungen eine Verbindung zum Load Balancer-Service herstellen, verwenden sie dazu das Zertifikat, das für den spezifischen Load Balancer-Endpunkt konfiguriert wurde, der für die Verbindung verwendet wurde. Jeder Endpunkt verfügt über ein eigenes Zertifikat, entweder ein vom Grid-Administrator hochgeladenes benutzerdefiniertes Serverzertifikat oder ein Zertifikat, das der Grid-Administrator bei der Konfiguration des Endpunkts in StorageGRID generiert hat.
- Wenn Client-Anwendungen eine direkte Verbindung zu einem Speicherknoten oder zum CLB-Dienst auf Gateway-Knoten herstellen, verwenden sie entweder die vom System generierten Serverzertifikate, die bei der Installation des StorageGRID-Systems (die von der Systemzertifikatbehörde signiert sind) für Speicherknoten generiert wurden. Oder ein einzelnes benutzerdefiniertes Serverzertifikat, das von einem Grid-Administrator für das Grid bereitgestellt wird.

Die Clients sollten so konfiguriert werden, dass sie der Zertifizierungsstelle vertrauen, die unabhängig davon, welches Zertifikat sie zum Erstellen von TLS-Verbindungen verwenden, unterzeichnet hat.

Informationen StorageGRID zum Konfigurieren von Load Balancer-Endpunkten finden Sie in den Anweisungen zum Hinzufügen eines einzelnen benutzerdefinierten Serverzertifikats für TLS-Verbindungen direkt zu Storage-Nodes oder zum CLB-Dienst auf Gateway-Nodes.

Zusammenfassung

Die folgende Tabelle zeigt, wie Sicherheitsprobleme in den S3 und Swift REST-APIs implementiert werden:

Sicherheitsproblem	Implementierung für REST-API
Verbindungssicherheit	TLS
Serverauthentifizierung	X.509-Serverzertifikat, das von der System-CA oder vom Administrator zur Verfügung gestellten benutzerdefinierten Serverzertifikat unterzeichnet wurde
Client-Authentifizierung	• S3: S3-Konto (Zugriffsschlüssel-ID und geheimer Zugriffsschlüssel) • Swift: Swift-Konto (Benutzername und Passwort)
Client-Autorisierung	• S3: Bucket-Eigentümerschaft und alle anwendbaren Richtlinien für die Zugriffssteuerung • Swift: Administratorrollenzugriff

Verwandte Informationen

"StorageGRID verwalten"

Unterstützte Hashing- und Verschlüsselungsalgorithmen für TLS-Bibliotheken

Das StorageGRID System unterstützt eine begrenzte Anzahl von Chiffren-Suites, die Client-Anwendungen beim Einrichten einer TLS-Sitzung (Transport Layer Security) verwenden können.

Unterstützte Versionen von TLS

StorageGRID unterstützt TLS 1.2 und TLS 1.3.

SSLv3 und TLS 1.1 (oder frühere Versionen) werden nicht mehr unterstützt.

Unterstützte Chiffren-Suiten

TLS-Version	IANA Name der Chiffre Suite
1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
1.3	TLS_AES_256_GCM_SHA384
TLS_CHACHA20_POLY1305_SHA256	TLS_AES_128_GCM_SHA256

Veraltete Chiffre-Suiten

Die folgenden Chiffren Suiten sind veraltet. Die Unterstützung für diese Chiffren wird in einer zukünftigen Version entfernt.

IANA-Name
TLS_RSA_WITH_AES_128_GCM_SHA256
TLS_RSA_WITH_AES_256_GCM_SHA384

Verwandte Informationen

"Wie Client-Verbindungen konfiguriert werden können"

Monitoring und Auditing von Vorgängen

Kunden können Workloads und die Effizienz für Client-Vorgänge überwachen, indem sie Transaktionstrends für das gesamte Grid oder bestimmte Nodes anzeigen. Sie können Audit-Meldungen zur Überwachung von Client-Vorgängen und -Transaktionen verwenden.

Monitoring der Objekteinspeisung und -Abrufraten

Die Überwachung von Objekteraufnahmeraten und -Abruffraten sowie von Metriken für Objektanzahl, -Abfragen und -Verifizierung Sie können die Anzahl der erfolgreichen und fehlgeschlagenen Versuche von Client-Applikationen anzeigen, Objekte in StorageGRID zu lesen, zu schreiben und zu ändern.

Schritte

1. Melden Sie sich über einen unterstützten Browser beim Grid Manager an.
2. Suchen Sie im Dashboard den Abschnitt Protokollvorgänge.

   In diesem Abschnitt wird die Anzahl der Client-Vorgänge zusammengefasst, die vom StorageGRID System durchgeführt werden. Die Protokollraten werden über die letzten zwei Minuten Durchschnitt.

3. Wählen Sie **Knoten**.
4. Klicken Sie auf der Startseite Knoten (Bereitstellungsebene) auf die Registerkarte **Load Balancer**.

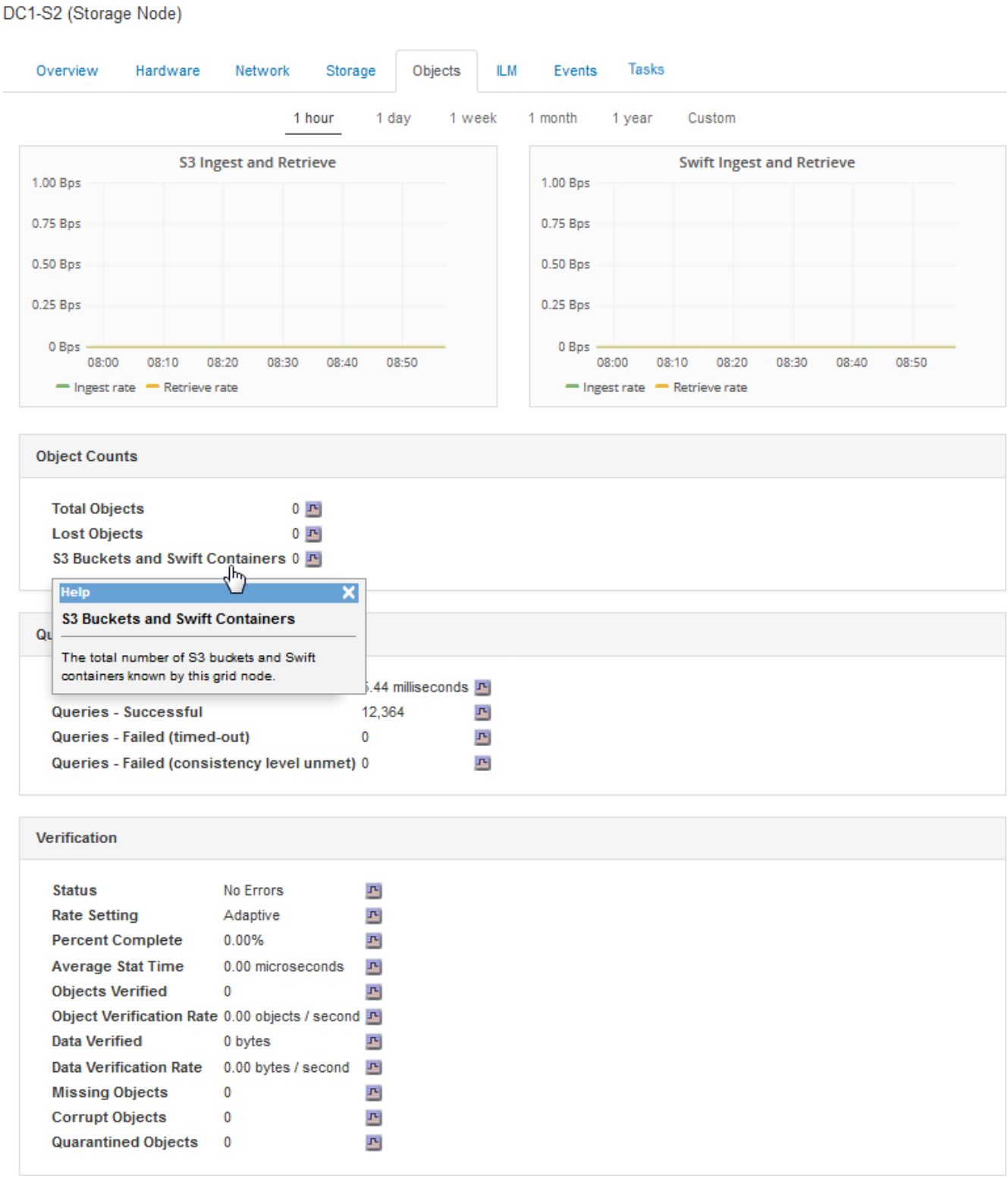
   Die Diagramme zeigen Trends für den gesamten Client-Datenverkehr an Load Balancer-Endpunkte im Raster. Sie können ein Zeitintervall in Stunden, Tagen, Wochen, Monaten oder Jahren auswählen. Oder Sie können ein benutzerdefiniertes Intervall anwenden.

5. Klicken Sie auf der Startseite Knoten (Bereitstellungsebene) auf die Registerkarte **Objekte**.

   Das Diagramm zeigt die Aufnahme- und Abrufraten Ihres gesamten StorageGRID Systems in Byte pro Sekunde sowie insgesamt Bytes. Sie können ein Zeitintervall in Stunden, Tagen, Wochen, Monaten oder Jahren auswählen. Oder Sie können ein benutzerdefiniertes Intervall anwenden.

6. Um Informationen zu einem bestimmten Speicherknoten anzuzeigen, wählen Sie den Knoten aus der Liste auf der linken Seite aus, und klicken Sie auf die Registerkarte **Objekte**.

   Das Diagramm zeigt die Aufnahme- und Abrufraten des Objekts für diesen Speicherknoten. Die Registerkarte enthält außerdem Kennzahlen für Objektanzahl, Abfragen und Verifizierung. Sie können auf die Beschriftungen klicken, um die Definitionen dieser Metriken anzuzeigen.



7. Wenn Sie noch mehr Details wünschen:
   a. Wählen Sie **Support** > **Tools** > **Grid Topology** Aus.
   b. Wählen Sie ***site*** > **Übersicht** > **Haupt**.

      Im Abschnitt API-Vorgänge werden zusammenfassende Informationen für das gesamte Raster angezeigt.

c. Wählen Sie ***Storage Node*** > **LDR** > ***Client-Anwendung*** > **Übersicht** > **Main** aus

Im Abschnitt „Vorgänge“ werden zusammenfassende Informationen für den ausgewählten Speicherknoten angezeigt.

Aufrufen und Prüfen von Prüfprotokollen

Audit-Meldungen werden von StorageGRID-Diensten generiert und in Text-Log-Dateien gespeichert. API-spezifische Audit-Meldungen in den Audit-Protokollen stellen kritische Daten zum Monitoring von Sicherheit, Betrieb und Performance bereit, die Ihnen bei der Bewertung des Systemzustands helfen können.

Was Sie benötigen

- Sie müssen über spezifische Zugriffsberechtigungen verfügen.
- Sie müssen die haben `Passwords.txt` Datei:
- Sie müssen die IP-Adresse eines Admin-Knotens kennen.

Über diese Aufgabe

Der Name der aktiven Audit-Log-Datei `audit.log`, Und es wird auf Admin-Knoten gespeichert.

Einmal am Tag wird die aktive audit.log-Datei gespeichert und eine neue audit.log-Datei gestartet. Der Name der gespeicherten Datei gibt an, wann sie gespeichert wurde, im Format `yyyy-mm-dd.txt`.

Nach einem Tag wird die gespeicherte Datei komprimiert und im Format umbenannt `yyyy-mm-dd.txt.gz`, Die das ursprüngliche Datum bewahrt.

Dieses Beispiel zeigt die aktive audit.log-Datei, die Datei des Vortags (2018-04-15.txt) und die komprimierte Datei für den Vortag (`2018-04-14.txt.gz`).

```
audit.log
2018-04-15.txt
2018-04-14.txt.gz
```

Schritte

1. Melden Sie sich bei einem Admin-Knoten an:
   a. Geben Sie den folgenden Befehl ein: `ssh admin@primary_Admin_Node_IP`
   b. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:
2. Gehen Sie zu dem Verzeichnis, das die Audit-Log-Dateien enthält:`cd /var/local/audit/export`
3. Sehen Sie sich die aktuelle oder gespeicherte Audit-Protokolldatei nach Bedarf an.

Verwandte Informationen

"Prüfung von Audit-Protokollen"

In den Audit-Protokollen werden Swift-Vorgänge nachverfolgt

Alle erfolgreichen Vorgänge zum LÖSCHEN, ABRUFEN, NACHFÜHREN, POSTEN und PUT werden im StorageGRID Audit-Protokoll verfolgt. Fehler werden weder protokolliert, noch sind Info-, Auth- oder OPTIONSANFORDERUNGEN.

Weitere Informationen zu den für die folgenden Swift-Vorgänge erfassten Informationen finden Sie unter *Audit-Meldungen*.

Konto-Operationen

- GET Konto
- HEAD Konto

Container-Operationen

- Container LÖSCHEN
- GET Container
- KOPF Behälter
- Legen Sie den Behälter

Objekt-Operationen

- Delete Objekt
- GET Objekt
- HEAD Objekt
- PUT Objekt

Verwandte Informationen

"Prüfung von Audit-Protokollen"

"Konto-Operationen"

"Container-Operationen"

"Objekt-Operationen"