Management von S3-Plattform-Services

StorageGRID software

NetApp
February 12, 2026

Inhalt

Management von S3-Plattform-Services

S3-Plattform-Services

Platform Services – Übersicht und Überlegungen

Bevor Sie Plattformservices implementieren, sollten Sie sich die Übersicht und die Überlegungen zur Verwendung dieser Services ansehen.

Informationen zu S3 finden Sie unter "S3-REST-API VERWENDEN".

Überblick über die Plattform-Services

Die StorageGRID Plattform-Services unterstützen Sie bei der Implementierung einer Hybrid-Cloud-Strategie, da Sie Ereignisbenachrichtigungen und Kopien von S3 Objekten und Objekt-Metadaten an externe Ziele senden können.

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 können Sie sowohl die als auch "Benachrichtigungen"einen StorageGRID S3 Bucket konfigurieren, damit Sie bestimmte Objekte auf den Amazon Simple Storage Service (S3) spiegeln können. Gleichzeitig könnten "CloudMirror Service"Sie eine Benachrichtigung über jedes dieser Objekte an die Monitoring-Applikation eines Drittanbieters senden, um Ihre AWS Ausgaben nachzuverfolgen.

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

Plattformdienste kommunizieren mit externen Endpunkten, die Sie mithilfe der"Mandanten-Manager" oder die"Mandantenmanagement-API" . Jeder Endpunkt stellt ein externes Ziel dar, beispielsweise einen StorageGRID S3-Bucket, einen Amazon Web Services-Bucket, ein Amazon SNS-Thema, einen Webhook-Endpunkt oder einen Elasticsearch-Cluster, der lokal, auf AWS oder anderswo gehostet wird.

Nachdem Sie einen externen Endpunkt erstellt haben, können Sie einen Plattformdienst für einen Bucket aktivieren, indem Sie dem Bucket eine XML-Konfiguration hinzufügen. Die XML-Konfiguration identifiziert die Objekte, auf 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:

- Wenn alle Objekte, deren Schlüssel mit beginnen, in einen Amazon S3-Bucket repliziert werden sollen `/images`, müssen Sie dem Quell-Bucket eine Replizierungskonfiguration hinzufügen.
- Wenn Sie auch Benachrichtigungen senden möchten, wenn diese Objekte im Bucket gespeichert sind, müssen Sie eine Benachrichtigungskonfiguration hinzufügen.
- Wenn Sie die Metadaten für diese Objekte indizieren möchten, müssen Sie die

Benachrichtigungskonfiguration für Metadaten 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	Siehe
Replizierung von CloudMirror	• GetBucketReplication • PutBucketReplication	• "Replizierung von CloudMirror" • "Operationen auf Buckets"
Benachrichtigungen	• GetBucketNotificationConfiguration • PutBucketNotificationKonfiguration	• "Benachrichtigungen" • "Operationen auf Buckets"
Integration von Suchen	• Konfiguration der Bucket-Metadaten-Benachrichtigungen ABRUFEN • PUT Bucket-Metadaten-Benachrichtigungskonfiguration	• "Integration von Suchen" • "Benutzerdefinierte Operationen von StorageGRID"

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.

Überlegungen	Details
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.
ILM-gesteuerte Objektlöschungen	Um dem Löschverhalten von AWS CRR und Amazon Simple Notification Service anzupassen, werden CloudMirror- und Ereignisbenachrichtigungsanforderungen nicht gesendet, wenn ein Objekt im Quell-Bucket aufgrund von StorageGRID-ILM-Regeln gelöscht wird. 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.
Kafka-Endpunkte werden verwendet	Bei Kafka-Endpunkten wird gegenseitiges TLS nicht unterstützt. Wenn Sie daher in Ihrer Kafka-Broker-Konfiguration auf festgelegt `required` haben `ssl.client.auth`, kann dies zu Problemen mit der Konfiguration von Kafka-Endpunkten führen. Für die Authentifizierung von Kafka-Endpunkten werden die folgenden Authentifizierungstypen verwendet. Diese Typen unterscheiden sich von denen, die für die Authentifizierung anderer Endpunkte verwendet werden, z. B. Amazon SNS, und erfordern Benutzername und Kennwort-Anmeldeinformationen. • SASL/PLAIN • SASL/SCRAM-SHA-256 • SASL/SCRAM-SHA-512 **Hinweis:** konfigurierte Speicher-Proxy-Einstellungen gelten nicht für Kafka-Plattform-Services-Endpunkte.

Überlegungen bei der Verwendung des CloudMirror Replikationsservice

Überlegungen	Details
Replikationsstatus	Der Header wird von StorageGRID nicht unterstützt `x-amz-replication-status`.

Überlegungen	Details
Objektgröße	Die maximale Größe für Objekte, die vom CloudMirror-Replikationsservice in einen Ziel-Bucket repliziert werden können, beträgt 5 tib. Dies ist die gleiche wie die maximal *unterstützte* Objektgröße. **Hinweis**: Die maximale *recommended* Größe für einen einzelnen PutObject-Vorgang beträgt 5 gib (5,368,709,120 Bytes). Wenn Sie über Objekte mit einer Größe von mehr als 5 gib verfügen, verwenden Sie stattdessen mehrteilige Uploads.
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**: Versions-IDs für den Quell-Bucket in StorageGRID hängen nicht mit den Versions-IDs für den Ziel-Bucket zusammen.
Tagging für Objektversionen	Der CloudMirror-Dienst repliziert keine PutObjectTagging- oder DeleteObjectTagging-Anforderungen, die aufgrund von Einschränkungen im S3-Protokoll eine Versions-ID bereitstellen. Da Versions-IDs für Quelle und Ziel nicht miteinander verknüpft sind, kann nicht sichergestellt werden, dass ein Tag-Update auf eine bestimmte Versions-ID repliziert wird. Im Gegensatz dazu repliziert der CloudMirror-Dienst PutObjectTagging-Anfragen oder DeleteObjectTagging-Anfragen, die keine Versions-ID angeben. Diese 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. Daher weicht der `ETag` Wert für das gespiegelte Objekt vom Wert des ursprünglichen Objekts ab `ETag`.
Mit SSE-C verschlüsselte Objekte (serverseitige Verschlüsselung mit vom Kunden bereitgestellten Schlüsseln)	Der CloudMirror-Dienst unterstützt keine Objekte, die mit SSE-C verschlüsselt sind. Wenn Sie versuchen, ein Objekt für die CloudMirror-Replikation in den Quell-Bucket aufzunehmen und die Anforderung die SSE-C-Anforderungsheader enthält, schlägt der Vorgang fehl.
Bucket mit S3-Objektsperre aktiviert	Die Replizierung wird für Quell- oder Ziel-Buckets nicht unterstützt, wenn S3 Object Lock aktiviert ist.

Verstehen Sie den CloudMirror Replizierungsservice

Sie können die CloudMirror-Replizierung für einen S3-Bucket aktivieren, wenn StorageGRID bestimmte Objekte replizieren soll, die dem Bucket hinzugefügt wurden, in

einen oder mehrere externe Ziel-Buckets.

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.

CloudMirror und ILM

Die CloudMirror Replizierung wird unabhängig von den aktiven ILM-Richtlinien des Grids durchgeführt. 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.

CloudMirror und Grid-Replizierung

Die CloudMirror-Replizierung weist wichtige Ähnlichkeiten und Unterschiede zur Grid-übergreifenden Replizierungsfunktion auf. Siehe "Vergleichen Sie Grid-Replizierung und CloudMirror Replizierung".

CloudMirror und S3-Buckets

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.

Vorhandene Buckets

Wenn Sie die CloudMirror-Replizierung für einen vorhandenen Bucket aktivieren, werden nur die neuen Objekte repliziert, die diesem Bucket hinzugefügt wurden. Alle vorhandenen Objekte in dem 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 zum Kopieren von Objekten an ein Amazon S3 Ziel CloudMirror Replizierung verwenden, beachten Sie, dass Amazon S3 die Größe der benutzerdefinierten Metadaten innerhalb jedes PUT-Anforderungsheaders auf 2 KB beschränkt. Wenn in einem Objekt benutzerdefinierte Metadaten größer als 2 KB sind, wird dieses Objekt nicht repliziert.

Mehrere Ziel-Buckets

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

Versionierte oder unversionierte Buckets

Die CloudMirror-Replizierung kann für versionierte oder unversionierte Buckets konfiguriert werden. Ziel-Buckets können mit einer Versionskontrolle oder ohne Versionskontrolle versioniert werden. 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.

Löschen, Replikations-Loops und Ereignisse

Löschverhalten

Entspricht dem Löschverhalten des Amazon S3-Dienstes, Cross-Region Replication (CRR). Durch das Löschen eines Objekts in einem Quell-Bucket wird niemals ein repliziertes Objekt auf dem Ziel gelöscht. Wenn sowohl Quell- als auch Ziel-Buckets versioniert sind, wird die Löschmarkierung repliziert. Wenn der Ziel-Bucket nicht versioniert ist, repliziert das Löschen eines Objekts im Quell-Bucket nicht die Löschmarkierung auf den Ziel-Bucket oder löscht das Zielobjekt nicht.

Schutz vor Replikations-Loops

Wenn Objekte in den Ziel-Bucket repliziert werden, kennzeichnet StorageGRID sie als „Replikate“. Ein Ziel-StorageGRID-Bucket repliziert nicht wieder als Replikate markierte Objekte und schützt Sie vor versehentlichen Replikations-Loops. Diese Replikatmarkierung ist intern bei StorageGRID und hindert Sie nicht daran, AWS CRR zu nutzen, wenn Sie einen Amazon S3-Bucket als Ziel verwenden.

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

Ereignisse im Ziel-Bucket

Die Einzigartigkeit und Reihenfolge von Ereignissen 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.

Informieren Sie sich über Benachrichtigungen für Buckets

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

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.

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 Eindeutigkeit 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 den Schlüssel in der Ereignismeldung verwenden `sequencer`, um die Reihenfolge der Ereignisse für ein bestimmtes Objekt zu bestimmen, wie in der Amazon S3-Dokumentation beschrieben.

StorageGRID-Ereignisbenachrichtigungen folgen mit einigen Einschränkungen der Amazon S3-API.

- Die folgenden Ereignistypen werden unterstützt:
  - s3:ObjectCreated:

- s3:ObjectCreated:Put
- s3:ObjectCreated:Post
- s3:ObjectCreated:Copy
- s3:ObjectCreated:CompleteMultipartUpload
- s3:ObjectRemoved:
- s3:ObjectRemoved:Löschen
- s3:ObjectRemoved:DeleteMarkerCreated
- s3:ObjectRestore:Post

- Aus StorageGRID gesendete Ereignisbenachrichtigungen verwenden das Standard-JSON-Format, enthalten aber keine Schlüssel und verwenden bestimmte Werte für andere, wie in der Tabelle gezeigt:

Schlüsselname	Wert von StorageGRID
EventSource	`sgws:s3`
AwsRegion	*Nicht enthalten*
X-amz-id-2	*Nicht enthalten*
arn	`urn:sgws:s3:::bucket_name`

Den Suchintegrations-Service verstehen

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

Der Suchintegrationsservice ist ein individueller StorageGRID-Service, der S3-Objektmetadaten automatisch und asynchron an einen Zielendpunkt sendet, wenn ein Objekt erstellt oder gelöscht oder seine Metadaten oder Tags 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 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 mit aktivierter S3 Object Lock konfiguriert werden, die S3 Object Lock-Metadaten (einschließlich des Aufbewahrungsdatums und des Status der Legal Hold) der Objekte werden jedoch nicht in die an Elasticsearch gesendeten Metadaten aufgenommen.

> Da der Suchintegrationsdienst dazu führt, dass Objektmetadaten an ein Ziel gesendet werden, wird seine Konfigurations-XML als "*Metadaten* Benachrichtigungskonfiguration XML" bezeichnet. Diese Konfigurations-XML unterscheidet sich von der XML-Benachrichtigungskonfiguration, die für die Aktivierung von *Event*-Benachrichtigungen verwendet wird.

Suchintegration und S3 Buckets

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.

Metadatenbenachrichtigungen werden in Form eines JSON-Dokuments mit dem Namen, der ggf. den Bucket-Namen, den Objektnamen und die Version-ID enthält generiert. 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 mehr bearbeiten.

Benachrichtigungen suchen

Metadatenbenachrichtigungen werden immer dann generiert und in die Warteschlange für die Zustellung gestellt, wenn:

- 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. Es werden jedoch keine Benachrichtigungen 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.

Suchintegrationsservice und Elasticsearch

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. Verwenden Sie den "NetApp Interoperabilitäts-Matrix-Tool", um die unterstützten Versionen von Elasticsearch zu bestimmen.

Verwalten von Plattform-Services-Endpunkten

Plattform-Services-Endpunkte konfigurieren

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 Plattformdienste zu erstellen oder zu verwenden, müssen Sie ein Mandantenbenutzer mit Berechtigungen zum Verwalten von Endpunkten oder Root-Zugriff in einem Grid sein, dessen Netzwerk so konfiguriert wurde, dass Storage-Nodes auf externe Endpunktressourcen zugreifen können. Für einen einzelnen Mandanten können Sie bis zu 500 Plattform-Services-Endpunkte konfigurieren. Weitere Informationen erhalten Sie von Ihrem StorageGRID Administrator.

Was ist ein Endpunkt für Plattformservices?

Ein Endpunkt für Plattformdienste gibt die Informationen an, die StorageGRID für den Zugriff auf das externe Ziel benötigt.

Wenn Sie beispielsweise Objekte aus einem StorageGRID-Bucket in einen Amazon S3-Bucket replizieren möchten, erstellen Sie einen Plattform-Services-Endpunkt, der die Informationen und Zugangsdaten enthält, die StorageGRID für den Zugriff auf den Ziel-Bucket auf Amazon 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 Quellbucket so konfigurieren, dass mehrere Endpunkte als Ziel verwendet werden. So können Sie beispielsweise Benachrichtigungen über die Objekterstellung an ein Amazon Simple Notification Service (Amazon SNS)-Thema senden und Benachrichtigungen über das Löschen von Objekten an ein zweites Amazon SNS-Thema 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 Amazon SNS, Kafka und Webhook-Endpunkte. Simple Queue Service (SQS) und AWS Lambda-Endpunkte werden nicht unterstützt.

Für Kafka-Endpunkte wird Mutual TLS nicht unterstützt. Wenn Sie also `ssl.client.auth` eingestellt auf `required` in Ihrer Kafka-Broker-Konfiguration kann es zu Problemen bei der Kafka-Endpunktkonfiguration kommen.

Endpunkte für den 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 an anderen Standorten 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"

URN für Endpunkt von Plattformservices angeben

Wenn Sie einen Endpunkt für Plattformservices erstellen, müssen Sie einen eindeutigen Ressourcennamen (URN) angeben. Beim Erstellen einer Konfigurations-XML für den Plattformdienst verwenden Sie die URN als Referenz auf den Endpunkt. 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 der Plattformdienste muss mit entweder oder `urn:mysite`, wie folgt beginnen `arn:aws`:

- Wenn der Service auf Amazon Web Services (AWS) gehostet wird, verwenden Sie `arn:aws`
- Wenn der Service auf der Google Cloud Platform (GCP) gehostet wird, verwenden Sie `arn:aws`
- Wenn der Dienst lokal gehostet wird, verwenden Sie `urn:mysite`

Wenn Sie beispielsweise die URN für einen CloudMirror-Endpunkt angeben, der auf StorageGRID gehostet wird, beginnt die URN möglicherweise mit `urn:sgws`.

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

Service	Typ
Replizierung von CloudMirror	`s3`
Benachrichtigungen	`sns`, `kafka` , oder `webhook`
Integration von Suchen	`es`

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

Bei den meisten Endpunkten identifiziert das letzte Element der URN die spezifische Zielressource an der Ziel-URI, zum Beispiel: `sns-topic-name` .

Bei Webhook-Endpunkten ist die Zielressource die Ziel-URI selbst.

Service	Bestimmte Ressource
Replizierung von CloudMirror	`bucket-name`
Benachrichtigungen	`sns-topic-name` Oder `kafka-topic-name` **Hinweis:** Bei Webhook-Endpunkten kann das letzte Element der URN eine beliebige Zeichenfolge sein, solange die URN des Endpunkts eindeutig ist.
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 zum Hosten auf AWS und GCP

Für AWS und GCP-Einheiten ist der vollständige 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 Endpunkt der AWS-Suchintegration muss der `domain-name` die Literalzeichenfolge enthalten `domain/`, wie hier dargestellt.

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 eine gültige URN angeben, die mit beginnt `urn:sgws`:

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

- Benachrichtigungen:

  Geben Sie einen Endpunkt für den Amazon Simple Notification Service an:

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

  Geben Sie einen Kafka-Endpunkt an:

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

  Geben Sie einen Webhook-Endpunkt an:

  ```
  urn:mysite:webhook:optional:optional:webhook-name
  ```

- Integration von Suchen:

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

  Für lokal gehostete Suchendpunkte kann das `domain-name` Element eine beliebige Zeichenfolge sein, solange die URN des Endpunkts eindeutig ist.

Endpunkt für Plattformservices erstellen

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

Bevor Sie beginnen

- Sie sind beim Tenant Manager mit einem angemeldet"Unterstützter Webbrowser".
- Die Plattformservices wurden für Ihr Mandantenkonto von einem StorageGRID-Administrator aktiviert.
- Sie gehören zu einer Benutzergruppe mit dem "Verwalten von Endpunkten oder Root-Zugriffsberechtigungen".
- Die vom Plattformdienste-Endpunkt referenzierte Ressource wurde erstellt:
  - CloudMirror Replizierung: S3 Bucket

- Ereignisbenachrichtigung: Amazon Simple Notification Service (Amazon SNS)-Thema, Kafka-Thema oder Webhook-Endpunkt
- Suchbenachrichtigung: Elasticsearch-Index, wenn der Zielcluster nicht für die automatische Erstellung von Indizes konfiguriert ist.

- Sie haben die Informationen über die Zielressource:
  - 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)

    "URN für Endpunkt von Plattformservices angeben"

  - Authentifizierungsdaten (falls erforderlich):

    Endpunkte für die Suchintegration

    Für Endpunkte der Suchintegration können Sie die folgenden Anmeldeinformationen verwenden:

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

    Endpunkte der CloudMirror Replizierung

    Für CloudMirror-Replikations-Endpunkte können Sie die folgenden Anmeldedaten verwenden:

    - Zugriffsschlüssel: Zugriffsschlüssel-ID und geheimer Zugriffsschlüssel
    - CAP (C2S Access Portal): Temporäre Anmeldeinformationen URL, Server- und Client-Zertifikate, Clientschlüssel und eine optionale private Client-Schlüssel-Passphrase.

    Amazon SNS-Endpunkte

    Für Amazon SNS-Endpunkte können Sie die folgenden Anmeldeinformationen verwenden:

    - Zugriffsschlüssel: Zugriffsschlüssel-ID und geheimer Zugriffsschlüssel

    Kafka-Endpunkte

    Für Kafka-Endpunkte können Sie die folgenden Anmeldeinformationen verwenden:

    - SASL/PLAIN: Benutzername und Passwort
    - SASL/SCRAM-SHA-256: Benutzername und Passwort
    - SASL/SCRAM-SHA-512: Benutzername und Passwort

  - Sicherheitszertifikat (falls eine Zertifikatsüberprüfung erforderlich ist)
- Wenn die Elasticsearch-Sicherheitsfunktionen aktiviert sind, verfügen Sie über die Berechtigung zum Überwachen des Clusters für den Verbindungstest und entweder über die Berechtigung zum Schreibindex oder sowohl über die Index- als auch Löschindexberechtigungen für Dokumentaktualisierungen.

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 Typ des Plattformdienstes, den der Endpunkt unterstützt, wird neben dem Endpunktnamen angezeigt, wenn dieser auf der Seite „Endpunkte“ aufgeführt ist. Sie müssen diese Information also nicht in den Namen aufnehmen.

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

   Verwenden Sie eines der folgenden Formate:

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

   Wenn Sie keinen Port angeben, werden die folgenden Standardports verwendet:

   - Port 443 für HTTPS-URIs und Port 80 für HTTP-URIs (die meisten Endpunkte)
   - Port 9092 für HTTPS- und HTTP-URIs (nur Kafka-Endpunkte)

   Beispielsweise 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 (High Availability, Hochverfügbarkeit) dar und `10443` stellt den im Load Balancer-Endpunkt definierten Port dar.

   > Wenn dies möglich ist, sollten Sie eine Verbindung zu einer HA-Gruppe von Load-Balancing-Nodes herstellen, 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, fügen 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 die URN eines Endpunkts nicht ändern, nachdem der Endpunkt erstellt wurde.

6. Wählen Sie **Weiter**.
7. Wählen Sie einen Wert für **Authentifizierungstyp** aus.

Wenn Sie eine Authentifizierung für Webhook-Endpunkte wünschen, konfigurieren Sie Mutual Transport Layer Security (mTLS) inSchritt 9 .

Endpunkte für die Suchintegration

Geben Sie die Anmeldeinformationen für einen Endpunkt für die Suchintegration ein, oder laden Sie sie hoch.

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

Authentifizierung styp	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

Endpunkte der CloudMirror Replizierung

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

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

Authentifizierung styp	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

Authentifizierungstyp	Beschreibung	Anmeldedaten
KAPPE (C2S-Zugangsportal)	Verwendet Zertifikate und Schlüssel zur Authentifizierung von Verbindungen zum Ziel.	• URL für temporäre Anmeldeinformationen • Server-CA-Zertifikat (PEM-Datei-Upload) • Client-Zertifikat (PEM-Datei-Upload) • Privater Client-Schlüssel (Upload der PEM-Datei, verschlüsseltes OpenSSL-Format oder unverschlüsseltes privates Schlüsselformat) • Private Client-Schlüssel-Passphrase (optional)

Amazon SNS-Endpunkte

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

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

Kafka-Endpunkte

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

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.

Authentifizierungstyp	Beschreibung	Anmeldedaten
SASL/PLAIN	Verwendet einen Benutzernamen und ein Kennwort mit Klartext, um Verbindungen zum Ziel zu authentifizieren.	• Benutzername • Passwort
SASL/SCRAM-SHA-256	Verwendet einen Benutzernamen und ein Kennwort mit einem Challenge-Response-Protokoll und SHA-256-Hashing, um Verbindungen zum Ziel zu authentifizieren.	• Benutzername • Passwort
SASL/SCRAM-SHA-512	Verwendet einen Benutzernamen und ein Kennwort mit einem Challenge-Response-Protokoll und SHA-512-Hashing, um Verbindungen zum Ziel zu authentifizieren.	• Benutzername • Passwort

Wählen Sie **Delegationsentnommene Authentifizierung verwenden** aus, wenn der Benutzername und das Passwort von einem Delegationstoken abgeleitet werden, das von einem Kafka-Cluster bezogen wurde.

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

Die meisten Endpunkte

Überprüfen Sie die TLS-Verbindung für Suchintegration, CloudMirror-Replikation, Amazon SNS oder Kafka-Endpunkte.

Typ der Zertifikatverifizierung	Beschreibung
TLS	Validiert das Serverzertifikat für TLS-Verbindungen zur Endpunktressource.
Deaktiviert	Die Zertifikatsüberprüfung ist deaktiviert. Diese Option ist nicht sicher.
Benutzerdefiniertes CA-Zertifikat verwenden	Das benutzerdefinierte CA-Zertifikat wird verwendet, um die Identität des Servers beim Herstellen einer Verbindung mit dem Endpunkt zu überprüfen.
Verwenden Sie das CA-Zertifikat für das Betriebssystem	Verwenden Sie das auf dem Betriebssystem installierte Standard-Grid-CA-Zertifikat, um Verbindungen zu sichern.

Nur Webhook-Endpunkte

Überprüfen Sie die TLS-Verbindung für Webhook-Endpunkte.

Typ der Zertifikatverifizierung	Beschreibung
TLS	Validiert das Serverzertifikat für TLS-Verbindungen zur Endpunktressource.
mTLS	Validiert die Client- und Serverzertifikate für gegenseitige TLS-Verbindungen zur Endpunktressource.
Deaktiviert	Die Zertifikatsüberprüfung ist deaktiviert. Diese Option ist nicht sicher.
Benutzerdefiniertes CA-Zertifikat verwenden	Das benutzerdefinierte CA-Zertifikat wird verwendet, um die Identität des Servers beim Herstellen einer Verbindung mit dem Endpunkt zu überprüfen.

Wenn Sie **mTLS** auswählen, werden diese Optionen verfügbar.

Typ der Zertifikatverifizierung	Beschreibung
Serverzertifikat nicht überprüfen	Deaktiviert die Serverzertifikatsüberprüfung, was bedeutet, dass die Identität des Servers nicht überprüft wird. Diese Option ist nicht sicher.
Client-Zertifikat	Das Client-Zertifikat wird verwendet, um die Identität des Clients bei der Verbindung mit dem Endpunkt zu überprüfen.

Typ der Zertifikatverifizierung	Beschreibung
Privater Clientschlüssel	Der private Schlüssel für das Client-Zertifikat. Bei Verschlüsselung muss das traditionelle Format PKCS #1 verwendet werden (das Format PKCS #8 wird nicht unterstützt).
Passphrase für den privaten Clientschlüssel	Die Passphrase zum Entschlüsseln des privaten Clientschlüssels. Wenn der private Schlüssel nicht verschlüsselt ist, lassen Sie dieses Feld leer.

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 Erstellung von Endpunkten 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

- "URN für Endpunkt von Plattformservices angeben"
- "CloudMirror-Replizierung konfigurieren"
- "Konfigurieren Sie Ereignisbenachrichtigungen"
- "Konfigurieren Sie den Suchintegrationsdienst"

Testen der Verbindung für 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.

Bevor Sie beginnen

- Sie sind beim Tenant Manager mit einem angemeldet"Unterstützter Webbrowser".
- Sie gehören zu einer Benutzergruppe mit dem "Verwalten von Endpunkten oder Root-Zugriffsberechtigungen".

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**.

Endpunkt der Plattformdienste bearbeiten

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 die URN für einen Endpunkt für Plattformdienste nicht ändern.

Bevor Sie beginnen

- Sie sind beim Tenant Manager mit einem angemeldet"Unterstützter Webbrowser".
- Sie gehören zu einer Benutzergruppe mit dem "Verwalten von Endpunkten oder Root-Zugriffsberechtigungen".

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**.
4. Ändern Sie bei Bedarf die Konfiguration des Endpunkts.

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

   a. Um den Anzeigenamen für den Endpunkt zu ändern, wählen Sie das Symbol Bearbeiten .
   b. Ändern Sie bei Bedarf den URI.
   c. Ändern Sie bei Bedarf den Authentifizierungstyp.
      - 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.

- Für die CAP-Authentifizierung (C2S Access Portal) ändern Sie die URL für temporäre Anmeldeinformationen oder die optionale private Passphrase für Clientschlüssel und laden Sie nach Bedarf neue Zertifikate und Schlüsseldateien hoch.

> Der private Client-Schlüssel muss im OpenSSL-verschlüsselten Format oder unverschlüsseltem privaten Schlüssel vorliegen.

d. Ändern Sie bei Bedarf die Methode zur Überprüfung von Zertifikaten.

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**.

Endpunkt für Plattformservices löschen

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

Bevor Sie beginnen

- Sie sind beim Tenant Manager mit einem angemeldet"Unterstützter Webbrowser".
- Sie gehören zu einer Benutzergruppe mit dem "Verwalten von Endpunkten oder Root-Zugriffsberechtigungen".

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 Endpunkt, den Sie löschen möchten.

> 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**.

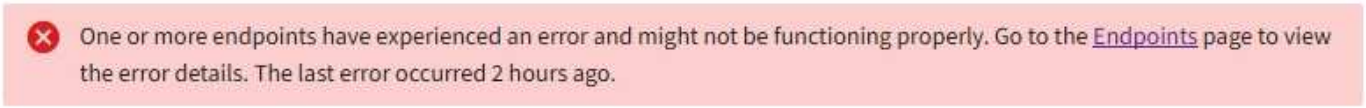
Fehlerbehebung bei Endpunktfehlern bei Plattform-Services

Wenn StorageGRID versucht, mit einem Endpunkt für Plattformdienste zu kommunizieren, wird eine Meldung auf dem Dashboard 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 Sie, ob ein Fehler aufgetreten ist

Wenn in den letzten 7 Tagen Fehler am Endpunkt der Plattformdienste aufgetreten sind, zeigt das Mandantenmanager-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 auch oben auf der Seite „Endpunkte für Plattformdienste“ 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, traten innerhalb der letzten 7 Tage auf.

Überprüfen Sie, ob der Fehler noch immer 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.

Beheben 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 müssen die Endpunktanmeldeinformationen aktualisiert werden, oder der Zielzugriff muss aktualisiert werden.“ die Details lauten „AccessDenied“ oder „InvalidAccessKeyId“.

Wenn Sie den Endpunkt bearbeiten müssen, um einen Fehler zu beheben, wird durch Auswahl von **Änderungen testen und speichern** der aktualisierte Endpunkt von StorageGRID überprüft und bestätigt,

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 aus diesem Grund beim Versuch, einen Plattformdienst zu verwenden, einen Fehler erhalten (z. B. „403 Verboten“), überprüfen Sie die Berechtigungen, die mit den Anmeldedaten des Endpunkts verknüpft sind.

Verwandte Informationen

- **Verwaltung von StorageGRID › Fehlerbehebung für Plattformservices**
- "Endpunkt für Plattformservices erstellen"
- "Testen der Verbindung für Endpunkt der Plattformservices"
- "Endpunkt der Plattformdienste bearbeiten"

CloudMirror-Replizierung konfigurieren

Um die CloudMirror-Replizierung für einen Bucket zu aktivieren, erstellen Sie eine gültige XML-Bucket-Replizierungskonfiguration und wenden sie an.

Bevor Sie beginnen

- Die Plattformservices wurden für Ihr Mandantenkonto von einem StorageGRID-Administrator aktiviert.
- Sie haben bereits einen Bucket erstellt, der als Replikationsquelle fungiert.
- Der Endpunkt, den Sie als Ziel für die CloudMirror-Replikation verwenden möchten, ist bereits vorhanden, und Sie haben seinen URN.
- Sie gehören zu einer Benutzergruppe mit dem "Managen aller Buckets oder Root-Zugriffsberechtigungen". 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.

Allgemeine Informationen zur Bucket-Replikation und deren Konfiguration finden Sie unter "Amazon Simple Storage Service (S3) Dokumentation: Replizierung von Objekten". Informationen über die Implementierung von GetBucketReplication, DeleteBucketReplication und PutketReplication durch StorageGRID finden Sie unter "Operationen auf Buckets".

Die CloudMirror-Replizierung weist wichtige Ähnlichkeiten und Unterschiede zur Grid-übergreifenden Replizierungsfunktion auf. Weitere Informationen finden Sie unter "Vergleichen Sie Grid-Replizierung und CloudMirror Replizierung".

Beachten Sie bei der Konfiguration der CloudMirror-Replikation die folgenden Anforderungen und Merkmale:

- Wenn Sie eine gültige XML-Bucket-Replizierungskonfiguration erstellen und anwenden, muss diese für jedes Ziel die URN eines S3-Bucket-Endpunkts verwenden.
- Die Replizierung wird für Quell- oder Ziel-Buckets nicht unterstützt, wenn S3 Object Lock aktiviert ist.
- Wenn Sie die CloudMirror-Replizierung für einen Bucket aktivieren, der Objekte enthält, werden neue Objekte, die dem Bucket hinzugefügt wurden, repliziert, die vorhandenen Objekte in dem Bucket werden jedoch nicht repliziert. 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 des Elements für Regeln nicht unterstützt `Filter` und V1-Konventionen für das Löschen von Objektversionen befolgt. Details finden Sie in der Amazon Dokumentation zur Replizierungskonfiguration.
     - Verwenden Sie den URN eines S3-Bucket-Endpunkts als Ziel.
     - Fügen Sie optional das Element hinzu `<StorageClass>`, und geben Sie eine der folgenden Optionen an:
       - `STANDARD`: Die Standard-Speicherklasse. Wenn Sie beim Hochladen eines Objekts keine Storage-Klasse angeben, wird die `STANDARD` Storage-Klasse verwendet.
       - `STANDARD_IA`: (Standard - seltener Zugang.) Nutzen Sie diese Storage-Klasse für Daten, auf die weniger häufig zugegriffen wird, die bei Bedarf aber noch schnellen Zugriff erfordern.
       - `REDUCED_REDUNDANCY`: Verwenden Sie diese Storage-Klasse für nicht kritische, reproduzierbare Daten, die mit weniger Redundanz gespeichert werden können als die `STANDARD` Storage-Klasse.
     - Wenn Sie in der Konfigurations-XML ein angeben `Role`, wird es ignoriert. Dieser Wert wird von StorageGRID nicht verwendet.

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

2. Wählen Sie **View Buckets** aus dem Dashboard, oder wählen Sie **STORAGE (S3)** > **Buckets**.
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 **Enable Replication**.
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

"Endpunkt für Plattformservices erstellen"

Konfigurieren Sie Ereignisbenachrichtigungen

Sie aktivieren Benachrichtigungen für einen Bucket, indem Sie XML für die Benachrichtigungskonfiguration erstellen und den Tenant Manager zum Anwenden des XML-Codes auf einen Bucket verwenden.

Bevor Sie beginnen

- Die Plattformservices wurden für Ihr Mandantenkonto von einem StorageGRID-Administrator aktiviert.
- Sie haben bereits einen Bucket erstellt, der als Quelle für Benachrichtigungen fungiert.
- Der Endpunkt, den Sie als Ziel für Ereignisbenachrichtigungen verwenden möchten, ist bereits vorhanden, und Sie haben seine URN.
- Sie gehören zu einer Benutzergruppe mit dem "Managen aller Buckets oder Root-Zugriffsberechtigungen". Diese Berechtigungen überschreiben die Berechtigungseinstellungen in Gruppen- oder Bucket-Richtlinien bei der Konfiguration des Buckets mithilfe des Mandanten-Manager.

Über diese Aufgabe

Sie konfigurieren Ereignisbenachrichtigungen, indem Sie die Benachrichtigungskonfigurations-XML mit einem Quell-Bucket verknüpfen. Die XML-Benachrichtigungskonfiguration folgt den S3-Konventionen zum Konfigurieren von Bucket-Benachrichtigungen, wobei das Zielthema Amazon SNS, das Kafka-Thema oder der Webhook-Endpunkt als URN eines Endpunkts angegeben wird.

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

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

- Wenn Sie eine gültige XML-Benachrichtigungskonfiguration erstellen und anwenden, muss die URN eines Ereignisbenachrichtigungs-Endpunkts für jedes Ziel verwendet werden.
- Obwohl die Ereignisbenachrichtigung für einen Bucket mit aktivierter S3 Object Lock konfiguriert werden kann, werden die S3 Object Lock-Metadaten (einschließlich Aufbewahrungszeitraum bis sowie Status der gesetzlichen Sperrzeit) der Objekte in den Benachrichtigungen nicht berücksichtigt.
- Nachdem Sie Ereignisbenachrichtigungen konfiguriert haben, wird jedes Mal, wenn ein bestimmtes Ereignis für ein Objekt im Quell-Bucket eintritt, eine Benachrichtigung generiert und an das als Ziel verwendete Amazon SNS-Thema, Kafka-Thema oder den Webhook-Endpunkt gesendet.
- Wenn Sie Ereignisbenachrichtigungen für einen Bucket aktivieren, der Objekte enthält, werden Benachrichtigungen nur für Aktionen gesendet, die nach dem Speichern der Benachrichtigungskonfiguration ausgeführt werden.

Schritte

1. 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 Tenant Manager **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, wenn ein Objekt mit dem Präfix erstellt `images/` wird.

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

      Wenn Ihr Zielthema beispielsweise auf Amazon SNS gehostet wird, können Sie den Dienst 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

- "Informieren Sie sich über Benachrichtigungen für Buckets"
- "S3-REST-API VERWENDEN"
- "Endpunkt für Plattformservices erstellen"

Konfigurieren Sie den Suchintegrationsdienst

Sie aktivieren die Suchintegration für einen Bucket, indem Sie XML für die Suchintegration erstellen und den Tenant Manager zum Anwenden des XML-Codes auf den Bucket verwenden.

Bevor Sie beginnen

- Die Plattformservices wurden für Ihr Mandantenkonto von einem StorageGRID-Administrator aktiviert.
- Sie haben bereits einen S3-Bucket erstellt, dessen Inhalt Sie indizieren möchten.
- Der Endpunkt, den Sie als Ziel für den Suchintegrationsdienst verwenden möchten, ist bereits vorhanden, und Sie haben seinen URN.
- Sie gehören zu einer Benutzergruppe mit dem "Managen aller Buckets oder Root-Zugriffsberechtigungen". 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 Suchintegrationsservice für einen Bucket aktivieren, der bereits Objekte enthält, werden Metadatenbenachrichtigungen nicht automatisch für vorhandene Objekte gesendet. Aktualisieren Sie diese vorhandenen Objekte, um sicherzustellen, dass ihre Metadaten zum Zielsuchindex hinzugefügt werden.

Schritte

1. Suchintegration für einen Bucket aktivieren:
    - Verwenden Sie einen Texteditor, um die XML-XML-Metadatenbenachrichtigung zu erstellen, die für die Integration der Suche erforderlich ist.
    - Verwenden Sie beim Konfigurieren des XML den URN eines Endpunkt zur Integration der Suche als Ziel.

      Objekte können nach dem Präfix des Objektnamens gefiltert werden. Beispielsweise können Sie Metadaten für Objekte mit dem Präfix an ein Ziel und Metadaten für Objekte mit `videos` dem Präfix an ein anderes senden `images`. Konfigurationen mit überlappenden Präfixen sind nicht gültig und werden bei der Übermittlung abgelehnt. Beispielsweise ist eine Konfiguration, die eine Regel für Objekte mit dem Präfix und eine zweite Regel für Objekte mit dem Präfix `test2` enthält `test`, nicht zulässig.

      Bei Bedarf siehe Beispiele für die Metadatenkonfiguration XML.

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

Elemente in der XML-Konfigurationskonfiguration für Metadatenbenachrichtigungen:

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. • Die URN muss mit dem Index und dem Typ enden, in dem die Metadaten gespeichert sind, in der Form `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.

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 **Enable search Integration**.
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** und deaktivieren Sie das Kontrollkästchen **Enable search Integration**.
- 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.

Beispiel: Konfiguration der Metadatenbenachrichtigung, die für alle Objekte gilt

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

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

Beispiel: Konfiguration der Metadatenbenachrichtigung mit zwei Regeln

In diesem Beispiel werden Objektmetadaten für Objekte mit dem Präfix `/images` an ein Ziel gesendet, während Objektmetadaten für Objekte mit dem Präfix `/videos` an ein zweites Ziel gesendet werden.

```
<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>
```

Benachrichtigungsformat für Metadaten

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 könnte, wenn ein Objekt mit dem Schlüssel in einem Bucket mit `SGWS/Tagging.txt` dem Namen erstellt wird `test`. Der `test` Bucket ist nicht versioniert, daher ist das `versionId` Tag leer.

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

Im JSON-Dokument enthaltene Felder

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

Bucket- und Objektinformationen

`bucket`: Name des Eimer

`key`: Name des Objektschlüssels

`versionID`: Objektversion, für Objekte in versionierten Buckets

`region`: Bucket-Region, zum Beispiel `us-east-1`

System-Metadaten

`size`: Objektgröße (in Bytes) als für einen HTTP-Client sichtbar

`md5`: Objekt-Hash

Benutzer-Metadaten

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

`key:value`

Tags

`tags`: Alle Objektanhänger, die für das Objekt definiert sind, als Schlüssel-Wert-Paare

`key:value`

So zeigen Sie Ergebnisse in Elasticsearch an

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. Aktivieren Sie die dynamischen Feldzuordnungen auf dem Index, bevor Sie den Suchintegrationsdienst konfigurieren. Nachdem ein Dokument indiziert wurde, können Sie die Feldtypen des Dokuments im Index nicht mehr bearbeiten.