Verwalten von S3-Plattformdiensten

StorageGRID software

NetApp
October 21, 2025

Inhalt

Verwalten von S3-Plattformdiensten

S3-Plattformdienste

Übersicht und Überlegungen zu Plattformdiensten

Lesen Sie vor der Implementierung von Plattformdiensten die Übersicht und die Überlegungen zur Verwendung dieser Dienste.

Informationen zu S3 finden Sie unter"Verwenden Sie die S3 REST-API" .

Übersicht der Plattformdienste

Die StorageGRID -Plattformdienste können Ihnen bei der Implementierung einer Hybrid-Cloud-Strategie helfen, indem sie Ihnen das Senden von Ereignisbenachrichtigungen und Kopien von S3-Objekten und Objektmetadaten an externe Ziele ermöglichen.

Da sich der Zielspeicherort für Plattformdienste normalerweise außerhalb Ihrer StorageGRID Bereitstellung befindet, bieten Ihnen Plattformdienste die Leistung und Flexibilität, die Sie durch die Verwendung externer Speicherressourcen, Benachrichtigungsdienste und Such- oder Analysedienste für Ihre Daten erhalten.

Für einen einzelnen S3-Bucket kann jede beliebige Kombination von Plattformdiensten konfiguriert werden. Sie können beispielsweise sowohl die"CloudMirror-Dienst" Und"Benachrichtigungen" auf einem StorageGRID S3-Bucket, sodass Sie bestimmte Objekte auf den Amazon Simple Storage Service (S3) spiegeln können, während Sie zu jedem dieser Objekte eine Benachrichtigung an eine Überwachungsanwendung eines Drittanbieters senden, die Ihnen bei der Verfolgung Ihrer AWS-Ausgaben hilft.

> Die Nutzung der Plattformdienste muss für jedes Mandantenkonto von einem StorageGRID -Administrator über den Grid Manager oder die Grid Management API aktiviert werden.

So werden Plattformdienste konfiguriert

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

Nachdem Sie einen externen Endpunkt erstellt haben, können Sie einen Plattformdienst für einen Bucket aktivieren, indem Sie dem Bucket eine XML-Konfiguration hinzufügen. Die XML-Konfiguration identifiziert die Objekte, auf die der Bucket einwirken soll, die Aktion, die der Bucket ausführen soll, und den Endpunkt, den der Bucket für den Dienst verwenden soll.

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

- Wenn Sie alle Objekte möchten, deren Schlüssel mit `/images` Um in einen Amazon S3-Bucket repliziert zu werden, müssen Sie dem Quell-Bucket eine Replikationskonfiguration hinzufügen.
- Wenn Sie auch Benachrichtigungen senden möchten, wenn diese Objekte im Bucket gespeichert werden, müssen Sie eine Benachrichtigungskonfiguration hinzufügen.
- Wenn Sie die Metadaten für diese Objekte indizieren möchten, müssen Sie die Metadatenbenachrichtigungskonfiguration hinzufügen, die zum Implementieren der Suchintegration

verwendet wird.

Das Format für die XML-Konfiguration wird durch die S3-REST-APIs bestimmt, die zur Implementierung der StorageGRID -Plattformdienste verwendet werden:

Plattformdienst	S3 REST API	Siehe
CloudMirror-Replikation	• GetBucketReplication • PutBucketReplication	• "CloudMirror-Replikation" • "Operationen an Buckets"
Benachrichtigungen	• GetBucketNotificationConfiguration • PutBucketNotificationConfiguration	• "Benachrichtigungen" • "Operationen an Buckets"
Suchintegration	• GET Bucket-Metadaten-Benachrichtigungskonfiguration • Konfiguration der Benachrichtigung über PUT-Bucket-Metadaten	• "Suchintegration" • "Benutzerdefinierte StorageGRID -Vorgänge"

Überlegungen zur Verwendung von Plattformdiensten

Rücksichtnahme	Details
Zielendpunktüberwachung	Sie müssen die Verfügbarkeit jedes Zielendpunkts überwachen. Wenn die Verbindung zum Zielendpunkt über einen längeren Zeitraum unterbrochen ist und ein großer Rückstand an Anfragen besteht, schlagen weitere Clientanfragen (z. B. PUT-Anfragen) an StorageGRID fehl. Sie müssen diese fehlgeschlagenen Anfragen wiederholen, wenn der Endpunkt erreichbar ist.
Drosselung des Zielendpunkts	Die StorageGRID Software drosselt möglicherweise eingehende S3-Anfragen für einen Bucket, wenn die Rate, mit der die Anfragen gesendet werden, die Rate überschreitet, mit der der Zielendpunkt die Anfragen empfangen kann. Eine Drosselung tritt nur auf, wenn ein Rückstand an Anfragen besteht, die darauf warten, an den Zielendpunkt gesendet zu werden. Der einzige sichtbare Effekt besteht darin, dass die Ausführung eingehender S3-Anfragen länger dauert. Wenn Sie eine deutlich langsamere Leistung feststellen, sollten Sie die Aufnahmerate reduzieren oder einen Endpunkt mit höherer Kapazität verwenden. Wenn der Rückstand an Anfragen weiter wächst, schlagen Client-S3-Operationen (wie etwa PUT-Anfragen) letztendlich fehl. Bei CloudMirror-Anfragen ist die Leistung des Zielendpunkts wahrscheinlicher beeinträchtigt, da diese Anfragen in der Regel mehr Datenübertragungen beinhalten als Anfragen zur Suchintegration oder Ereignisbenachrichtigung.

Rücksichtnahme	Details
Bestellgarantien	StorageGRID garantiert die Reihenfolge der Vorgänge an einem Objekt innerhalb einer Site. Solange alle Vorgänge für ein Objekt innerhalb derselben Site erfolgen, entspricht der endgültige Objektstatus (für die Replikation) immer dem Status in StorageGRID. StorageGRID versucht nach besten Kräften, Anfragen zu ordnen, wenn Vorgänge über StorageGRID -Sites hinweg ausgeführt werden. Wenn Sie beispielsweise ein Objekt zunächst an Standort A schreiben und dasselbe Objekt später an Standort B überschreiben, ist nicht garantiert, dass das endgültige, von CloudMirror in den Ziel-Bucket replizierte Objekt das neuere Objekt ist.
ILM-gesteuerte Objektlöschungen	Um dem Löschverhalten von AWS CRR und Amazon Simple Notification Service zu entsprechen, werden CloudMirror- und Ereignisbenachrichtigungsanforderungen nicht gesendet, wenn ein Objekt im Quell-Bucket aufgrund von StorageGRID ILM-Regeln gelöscht wird. Beispielsweise werden keine CloudMirror- oder Ereignisbenachrichtigungsanforderungen gesendet, wenn eine ILM-Regel ein Objekt nach 14 Tagen löscht. Im Gegensatz dazu werden Suchintegrationsanforderungen gesendet, wenn Objekte aufgrund von ILM gelöscht werden.
Verwenden von Kafka-Endpunkten	Für Kafka-Endpunkte wird Mutual TLS nicht unterstützt. Wenn Sie also `ssl.client.auth` eingestellt auf `required` in Ihrer Kafka-Broker-Konfiguration kann es zu Problemen bei der Kafka-Endpunktkonfiguration kommen. Die Authentifizierung von Kafka-Endpunkten verwendet die folgenden Authentifizierungstypen. Diese Typen unterscheiden sich von denen, die für die Authentifizierung anderer Endpunkte wie Amazon SNS verwendet werden, und erfordern Anmeldeinformationen mit Benutzername und Kennwort. • SASL/PLAIN • SASL/SCRAM-SHA-256 • SASL/SCRAM-SHA-512 **Hinweis:** Konfigurierte Speicherproxyeinstellungen gelten nicht für Endpunkte der Kafka-Plattformdienste.

Überlegungen zur Verwendung des CloudMirror-Replikationsdienstes

Rücksichtnahme	Details
Replikationsstatus	StorageGRID unterstützt nicht die `x-amz-replication-status` Kopfzeile.

Rücksichtnahme	Details
Objektgröße	Die maximale Größe für Objekte, die vom CloudMirror-Replikationsdienst in einen Ziel-Bucket repliziert werden können, beträgt 5 TiB, was der maximal *unterstützten* Objektgröße entspricht. **Hinweis**: Die maximal *empfohlene* Größe für einen einzelnen PutObject-Vorgang beträgt 5 GiB (5.368.709.120 Bytes). Wenn Sie Objekte haben, die größer als 5 GiB sind, verwenden Sie stattdessen den mehrteiligen Upload.
Bucket-Versionierung und Versions-IDs	Wenn für den Quell-S3-Bucket in StorageGRID die Versionierung aktiviert ist, sollten Sie auch die Versionierung für den Ziel-Bucket aktivieren. Beachten Sie bei der Verwendung der Versionierung, dass die Reihenfolge der Objektversionen im Ziel-Bucket nach bestem Wissen und Gewissen erfolgt und aufgrund von Einschränkungen im S3-Protokoll nicht vom CloudMirror-Dienst garantiert wird. **Hinweis**: Versions-IDs für den Quell-Bucket in StorageGRID stehen in keinem Zusammenhang mit den Versions-IDs für den Ziel-Bucket.
Tagging für Objektversionen	Aufgrund von Einschränkungen im S3-Protokoll repliziert der CloudMirror-Dienst keine PutObjectTagging- oder DeleteObjectTagging-Anfragen, die eine Versions-ID bereitstellen. Da die Versions-IDs für Quelle und Ziel nicht miteinander verknüpft sind, kann nicht sichergestellt werden, dass eine Tag-Aktualisierung auf eine bestimmte Versions-ID repliziert wird. Im Gegensatz dazu repliziert der CloudMirror-Dienst PutObjectTagging-Anfragen oder DeleteObjectTagging-Anfragen, die keine Versions-ID angeben. Diese Anfragen aktualisieren die Tags für den neuesten Schlüssel (oder die neueste Version, wenn der Bucket versioniert ist). Normale Aufnahmen mit Tags (keine Tagging-Updates) werden ebenfalls repliziert.
Mehrteilige Uploads und `ETag` Werte	Beim Spiegeln von Objekten, die mit einem mehrteiligen Upload hochgeladen wurden, behält der CloudMirror-Dienst die Teile nicht bei. Infolgedessen `ETag` Wert für das gespiegelte Objekt wird anders sein als der `ETag` Wert des ursprünglichen Objekts.
Mit SSE-C verschlüsselte Objekte (serverseitige Verschlüsselung mit vom Kunden bereitgestellten Schlüsseln)	Der CloudMirror-Dienst unterstützt keine mit SSE-C verschlüsselten Objekte. Wenn Sie versuchen, ein Objekt in den Quell-Bucket für die CloudMirror-Replikation aufzunehmen und die Anforderung die SSE-C-Anforderungsheader enthält, schlägt der Vorgang fehl.
Bucket mit aktivierter S3-Objektsperre	Die Replikation wird für Quell- oder Ziel-Buckets mit aktivierter S3-Objektsperre nicht unterstützt.

Grundlegendes zum CloudMirror-Replikationsdienst

Sie können die CloudMirror-Replikation für einen S3-Bucket aktivieren, wenn StorageGRID bestimmte, dem Bucket hinzugefügte Objekte in einen oder mehrere

externe Ziel-Buckets repliziert.

Sie können beispielsweise die CloudMirror-Replikation verwenden, um bestimmte Kundendatensätze in Amazon S3 zu spiegeln und dann AWS-Dienste nutzen, um Analysen Ihrer Daten durchzuführen.

> Die CloudMirror-Replikation wird nicht unterstützt, wenn im Quell-Bucket S3 Object Lock aktiviert ist.

CloudMirror und ILM

Die CloudMirror-Replikation funktioniert unabhängig von den aktiven ILM-Richtlinien des Grids. Der CloudMirror-Dienst repliziert Objekte, sobald sie im Quell-Bucket gespeichert sind, und liefert sie so schnell wie möglich an den Ziel-Bucket. Die Bereitstellung replizierter Objekte wird ausgelöst, wenn die Objektaufnahme erfolgreich ist.

CloudMirror und Cross-Grid-Replikation

Die CloudMirror-Replikation weist wichtige Ähnlichkeiten und Unterschiede zur Cross-Grid-Replikationsfunktion auf. Weitere Informationen finden Sie unter "Vergleichen Sie Cross-Grid-Replikation und CloudMirror-Replikation" .

CloudMirror und S3-Buckets

Die CloudMirror-Replikation ist normalerweise so konfiguriert, dass ein externer S3-Bucket als Ziel verwendet wird. Sie können die Replikation jedoch auch so konfigurieren, dass eine andere StorageGRID Bereitstellung oder ein beliebiger S3-kompatibler Dienst verwendet wird.

Vorhandene Eimer

Wenn Sie die CloudMirror-Replikation für einen vorhandenen Bucket aktivieren, werden nur die neuen Objekte repliziert, die diesem Bucket hinzugefügt werden. Alle vorhandenen Objekte im Bucket werden nicht repliziert. Um die Replikation vorhandener Objekte zu erzwingen, können Sie die Metadaten des vorhandenen Objekts aktualisieren, indem Sie eine Objektkopie durchführen.

> Wenn Sie die CloudMirror-Replikation zum Kopieren von Objekten an ein Amazon S3-Ziel verwenden, beachten Sie, dass Amazon S3 die Größe benutzerdefinierter Metadaten in jedem PUT-Anforderungsheader auf 2 KB begrenzt. Wenn ein Objekt benutzerdefinierte Metadaten größer als 2 KB hat, wird dieses Objekt nicht repliziert.

Mehrere Ziel-Buckets

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

Versionierte oder nicht versionierte Buckets

Sie können die CloudMirror-Replikation auf versionierten oder nicht versionierten Buckets konfigurieren. Die Ziel-Buckets können versioniert oder nicht versioniert sein. Sie können jede beliebige Kombination aus versionierten und nicht versionierten Buckets verwenden. Sie können beispielsweise einen versionierten Bucket als Ziel für einen nicht versionierten Quell-Bucket angeben oder umgekehrt. Sie können auch zwischen Buckets ohne Versionsnummer replizieren.

Löschung, Replikationsschleifen und Ereignisse

Löschverhalten

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

Schutz vor Replikationsschleifen

Wenn Objekte in den Ziel-Bucket repliziert werden, markiert StorageGRID sie als „Replikate“. Ein StorageGRID Ziel-Bucket repliziert als Replikate markierte Objekte nicht erneut und schützt Sie so vor versehentlichen Replikationsschleifen. Diese Replikatmarkierung erfolgt intern für StorageGRID und hindert Sie nicht daran, AWS CRR zu nutzen, wenn Sie einen Amazon S3-Bucket als Ziel verwenden.

> ⓘ Der benutzerdefinierte Header, der zum Markieren einer Replik verwendet wird, ist `x-ntap-sg-replica` . Diese Markierung verhindert einen Kaskadenspiegel. StorageGRID unterstützt einen bidirektionalen CloudMirror zwischen zwei Grids.

Ereignisse im Ziel-Bucket

Die Eindeutigkeit und Reihenfolge der Ereignisse im Ziel-Bucket sind nicht garantiert. Aufgrund von Vorgängen, die zur Gewährleistung einer erfolgreichen Zustellung durchgeführt werden, kann es vorkommen, dass mehrere identische Kopien eines Quellobjekts an das Ziel übermittelt werden. In seltenen Fällen, wenn dasselbe Objekt gleichzeitig von zwei oder mehr verschiedenen StorageGRID Sites aktualisiert wird, stimmt die Reihenfolge der Vorgänge im Ziel-Bucket möglicherweise nicht mit der Reihenfolge der Ereignisse im Quell-Bucket überein.

Benachrichtigungen für Buckets verstehen

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

Sie können beispielsweise Warnmeldungen konfigurieren, die an Administratoren gesendet werden, wenn ein Objekt zu einem Bucket hinzugefügt wird, wobei die Objekte Protokolldateien darstellen, die mit einem kritischen Systemereignis verknüpft sind.

Ereignisbenachrichtigungen werden im Quell-Bucket wie in der Benachrichtigungskonfiguration angegeben erstellt und an das Ziel übermittelt. Wenn ein mit einem Objekt verknüpftes Ereignis erfolgreich ist, wird eine Benachrichtigung über dieses Ereignis erstellt und zur Übermittlung in die Warteschlange gestellt.

Die Eindeutigkeit und Reihenfolge der Benachrichtigungen sind nicht garantiert. Aufgrund von Vorgängen, die zur Gewährleistung einer erfolgreichen Zustellung durchgeführt werden, kann es sein, dass mehrere Benachrichtigungen zu einem Ereignis an das Ziel übermittelt werden. Und da die Übermittlung asynchron erfolgt, kann nicht garantiert werden, dass die zeitliche Reihenfolge der Benachrichtigungen am Ziel mit der Reihenfolge der Ereignisse im Quell-Bucket übereinstimmt, insbesondere bei Vorgängen, die von verschiedenen StorageGRID Sites stammen. Sie können die `sequencer` Geben Sie in der Ereignisnachricht den Schlüssel ein, um die Reihenfolge der Ereignisse für ein bestimmtes Objekt zu bestimmen, wie in der Amazon S3-Dokumentation beschrieben.

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

- Die folgenden Ereignistypen werden unterstützt:

- s3:Objekt erstellt:
- s3:ObjektErstellt:Put
- s3:ObjektErstellt:Post
- s3:ObjektErstellt:Kopie
- s3:Objekterstellt:MehrteiligerUpload abgeschlossen
- s3:Objekt entfernt:
- s3:Objekt entfernt:Löschen
- s3:Objekt entfernt:DeleteMarker erstellt
- s3:ObjectRestore:Post

- Von StorageGRID gesendete Ereignisbenachrichtigungen verwenden das standardmäßige JSON-Format, enthalten jedoch einige Schlüssel nicht und verwenden für andere bestimmte Werte, wie in der Tabelle gezeigt:

Schlüsselname	StorageGRID -Wert
Ereignisquelle	`sgws:s3`
awsRegion	*nicht enthalten*
x-amz-id-2	*nicht enthalten*
arn	`urn:sgws:s3:::bucket_name`

Verstehen Sie den Suchintegrationsdienst

Sie können die Suchintegration für einen S3-Bucket aktivieren, wenn Sie einen externen Such- und Datenanalysedienst für Ihre Objektmetadaten verwenden möchten.

Der Suchintegrationsdienst ist ein benutzerdefinierter StorageGRID Dienst, der automatisch und asynchron S3-Objektmetadaten an einen Zielendpunkt sendet, wenn ein Objekt erstellt oder gelöscht wird oder seine Metadaten oder Tags aktualisiert werden. Sie können dann die vom Zieldienst bereitgestellten ausgefeilten Such-, Datenanalyse-, Visualisierungs- oder maschinellen Lerntools verwenden, um Ihre Objektdaten zu durchsuchen, zu analysieren und Erkenntnisse daraus zu gewinnen.

Sie können Ihre Buckets beispielsweise so konfigurieren, dass S3-Objektmetadaten an einen Remote-Elasticsearch-Dienst gesendet werden. Anschließend können Sie Elasticsearch verwenden, um Bucket-übergreifende Suchen durchzuführen und anspruchsvolle Analysen der in Ihren Objektmetadaten vorhandenen Muster durchzuführen.

Obwohl die Elasticsearch-Integration für einen Bucket mit aktivierter S3-Objektsperre konfiguriert werden kann, werden die S3-Objektsperre-Metadaten (einschließlich „Aufbewahrungsdatum“ und „Legal Hold“-Status) der Objekte nicht in die an Elasticsearch gesendeten Metadaten aufgenommen.

> Da der Suchintegrationsdienst das Senden von Objektmetadaten an ein Ziel veranlasst, wird sein Konfigurations-XML als „*Metadaten*-Benachrichtigungskonfigurations-XML“ bezeichnet. Dieses Konfigurations-XML unterscheidet sich vom „Benachrichtigungskonfigurations-XML“, das zum Aktivieren von *Ereignis*-Benachrichtigungen verwendet wird.

Suchintegration und S3-Buckets

Sie können den Suchintegrationsdienst für jeden versionierten oder nicht versionierten Bucket aktivieren. Die Suchintegration wird konfiguriert, indem die XML-Konfigurationsdatei für Metadatenbenachrichtigungen mit dem Bucket verknüpft wird, der angibt, auf welche Objekte reagiert werden soll und das Ziel für die Objektmetadaten ist.

Metadatenbenachrichtigungen werden in Form eines JSON-Dokuments generiert, das den Bucket-Namen, den Objektnamen und die Versions-ID (sofern vorhanden) enthält. Jede Metadatenbenachrichtigung enthält zusätzlich zu allen Tags und Benutzermetadaten des Objekts einen Standardsatz von Systemmetadaten für das Objekt.

> Für Tags und Benutzermetadaten übergibt StorageGRID Daten und Zahlen als Zeichenfolgen oder als S3-Ereignisbenachrichtigungen an Elasticsearch. Um Elasticsearch so zu konfigurieren, dass diese Zeichenfolgen als Datumsangaben oder Zahlen interpretiert werden, befolgen Sie die Elasticsearch-Anweisungen zur dynamischen Feldzuordnung und zur Zuordnung von Datumsformaten. Sie müssen die dynamischen Feldzuordnungen im Index aktivieren, bevor Sie den Suchintegrationsdienst konfigurieren. Nachdem ein Dokument indiziert wurde, können Sie die Feldtypen des Dokuments im Index nicht mehr bearbeiten.

Suchbenachrichtigungen

Metadatenbenachrichtigungen werden generiert und zur Zustellung in die Warteschlange gestellt, wenn:

- Ein Objekt wird erstellt.
- Ein Objekt wird gelöscht, auch wenn Objekte aufgrund der Ausführung der ILM-Richtlinie des Grids gelöscht werden.
- Objektmetadaten oder Tags werden hinzugefügt, aktualisiert oder gelöscht. Beim Update wird immer der komplette Satz an Metadaten und Tags gesendet – nicht nur die geänderten Werte.

Nachdem Sie einem Bucket XML-Metadatenbenachrichtigungskonfigurations-XML hinzugefügt haben, werden Benachrichtigungen für alle neuen Objekte gesendet, die Sie erstellen, und für alle Objekte, die Sie durch Aktualisieren der Daten, Benutzermetadaten oder Tags ändern. Es werden jedoch keine Benachrichtigungen für Objekte gesendet, die sich bereits im Bucket befanden. Um sicherzustellen, dass die Objektmetadaten für alle Objekte im Bucket an das Ziel gesendet werden, sollten Sie einen der folgenden Schritte ausführen:

- Konfigurieren Sie den Suchintegrationsdienst unmittelbar nach dem Erstellen des Buckets und vor dem Hinzufügen von Objekten.
- Führen Sie für alle Objekte, die sich bereits im Bucket befinden, eine Aktion aus, die das Senden einer Metadatenbenachrichtigung an das Ziel auslöst.

Suchintegrationsdienst und Elasticsearch

Der Suchintegrationsdienst StorageGRID unterstützt einen Elasticsearch-Cluster als Ziel. Wie bei den anderen Plattformdiensten wird das Ziel im Endpunkt angegeben, dessen URN im Konfigurations-XML für den Dienst verwendet wird. Verwenden Sie die "NetApp Interoperabilitätsmatrix-Tool" um die unterstützten Versionen von Elasticsearch zu ermitteln.

Verwalten von Plattformdienst-Endpunkten

Konfigurieren von Plattformdienstendpunkten

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

Der Zugriff auf Plattformdienste wird pro Mandant von einem StorageGRID -Administrator aktiviert. Um einen Plattformdienst-Endpunkt zu erstellen oder zu verwenden, müssen Sie ein Mandantenbenutzer mit der Berechtigung „Endpunkte verwalten“ oder „Root-Zugriff“ in einem Grid sein, dessen Netzwerk so konfiguriert wurde, dass Speicherknoten auf externe Endpunktressourcen zugreifen können. Für einen einzelnen Mandanten können Sie maximal 500 Plattformdienst-Endpunkte konfigurieren. Wenden Sie sich für weitere Informationen an Ihren StorageGRID Administrator.

Was ist ein Plattformdienst-Endpunkt?

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

Wenn Sie beispielsweise Objekte aus einem StorageGRID Bucket in einen Amazon S3-Bucket replizieren möchten, erstellen Sie einen Plattformdienst-Endpunkt, der die Informationen und Anmeldeinformationen enthält, die StorageGRID für den Zugriff auf den Ziel-Bucket bei Amazon benötigt.

Jeder Plattformdiensttyp erfordert einen eigenen Endpunkt. Sie müssen daher für jeden Plattformdienst, den Sie verwenden möchten, mindestens einen Endpunkt konfigurieren. Nachdem Sie einen Plattformdienst-Endpunkt definiert haben, verwenden Sie die URN des Endpunkts als Ziel in der Konfigurations-XML, die zum Aktivieren des Dienstes verwendet wird.

Sie können denselben Endpunkt als Ziel für mehr als einen Quell-Bucket verwenden. Sie können beispielsweise mehrere Quell-Buckets so konfigurieren, dass sie Objektmetadaten an denselben Suchintegrationsendpunkt senden, sodass Sie Suchvorgänge über mehrere Buckets hinweg durchführen können. Sie können einen Quell-Bucket auch so konfigurieren, dass er mehr als einen Endpunkt als Ziel verwendet. Dadurch können Sie beispielsweise Benachrichtigungen über die Objekterstellung an ein Amazon Simple Notification Service (Amazon SNS)-Thema und Benachrichtigungen über die Objektlöschung an ein zweites Amazon SNS-Thema senden.

Endpunkte für die CloudMirror-Replikation

StorageGRID unterstützt Replikationsendpunkte, die S3-Buckets darstellen. Diese Buckets können auf Amazon Web Services, derselben oder einer Remote- StorageGRID Bereitstellung oder einem anderen Dienst gehostet werden.

Endpunkte für Benachrichtigungen

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

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

Endpunkte für den Suchintegrationsdienst

StorageGRID unterstützt Suchintegrationsendpunkte, die Elasticsearch-Cluster darstellen. Diese Elasticsearch-Cluster können sich in einem lokalen Rechenzentrum befinden oder in einer AWS-Cloud oder anderswo gehostet werden.

Der Endpunkt der Suchintegration bezieht sich auf einen bestimmten Elasticsearch-Index und -Typ. Sie müssen den Index in Elasticsearch erstellen, bevor Sie den Endpunkt in StorageGRID erstellen, sonst schlägt die Endpunkterstellung fehl. Sie müssen den Typ nicht erstellen, bevor Sie den Endpunkt erstellen. StorageGRID erstellt den Typ bei Bedarf, wenn es Objektmetadaten an den Endpunkt sendet.

Ähnliche Informationen

"StorageGRID verwalten"

Geben Sie die URN für den Plattformdienst-Endpunkt an

Wenn Sie einen Plattformdienste-Endpunkt erstellen, müssen Sie einen eindeutigen Ressourcennamen (URN) angeben. Sie verwenden die URN, um auf den Endpunkt zu verweisen, wenn Sie eine XML-Konfiguration für den Plattformdienst erstellen. Die URN für jeden Endpunkt muss eindeutig sein.

StorageGRID validiert die Endpunkte der Plattformdienste, während Sie sie erstellen. Bevor Sie einen Plattformdienste-Endpunkt erstellen, bestätigen Sie, dass die im Endpunkt angegebene Ressource vorhanden und erreichbar ist.

URN-Elemente

Die URN für einen Plattformdienst-Endpunkt muss mit einem der folgenden Zeichen beginnen: `arn:aws` oder `urn:mysite` , wie folgt:

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

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

Das nächste Element der URN gibt den Typ des Plattformdienstes wie folgt an:

Service	Typ
CloudMirror-Replikation	`s3`
Benachrichtigungen	`sns`oder `kafka`
Suchintegration	`es`

Um beispielsweise weiterhin die URN für einen CloudMirror-Endpunkt anzugeben, der auf StorageGRID gehostet wird, würden Sie hinzufügen `s3` zu bekommen `urn:sgws:s3` .

Das letzte Element der URN identifiziert die spezifische Zielressource an der Ziel-URI.

Service	Spezifische Ressource
CloudMirror-Replikation	`bucket-name`
Benachrichtigungen	`sns-topic-name`oder `kafka-topic-name`
Suchintegration	`domain-name/index-name/type-name` **Hinweis:** Wenn der Elasticsearch-Cluster **nicht** für die automatische Erstellung von Indizes konfiguriert ist, müssen Sie den Index manuell erstellen, bevor Sie den Endpunkt erstellen.

URNs für auf AWS und GCP gehostete Dienste

Für AWS- und GCP-Entitäten ist die vollständige URN eine gültige AWS-ARN. Beispiel:

- CloudMirror-Replikation:

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

- Benachrichtigungen:

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

- Suchintegration:

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

> Für einen AWS-Suchintegrationsendpunkt ist der `domain-name` muss die Literalzeichenfolge enthalten `domain/` , wie hier gezeigt.

URNs für lokal gehostete Dienste

Wenn Sie lokal gehostete Dienste anstelle von Cloud-Diensten verwenden, können Sie die URN auf jede beliebige Weise angeben, die eine gültige und eindeutige URN erstellt, solange die URN die erforderlichen Elemente an der dritten und letzten Stelle enthält. Sie können die optional angegebenen Elemente leer lassen oder sie auf eine beliebige Weise angeben, die Ihnen bei der Identifizierung der Ressource hilft und die URN eindeutig macht. Beispiel:

- CloudMirror-Replikation:

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

Für einen CloudMirror-Endpunkt, der auf StorageGRID gehostet wird, können Sie eine gültige URN

angeben, die mit beginnt `urn:sgws` :

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

- Benachrichtigungen:

  Geben Sie einen Amazon Simple Notification Service-Endpunkt an:

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

  Geben Sie einen Kafka-Endpunkt an:

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

- Suchintegration:

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

  > Für lokal gehostete Suchintegrationsendpunkte gilt: `domain-name` Das Element kann eine beliebige Zeichenfolge sein, solange die URN des Endpunkts eindeutig ist.

Plattformdienst-Endpunkt erstellen

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

Bevor Sie beginnen

- Sie sind beim Tenant Manager angemeldet mit einem"unterstützter Webbrowser" .
- Die Plattformdienste wurden von einem StorageGRID Administrator für Ihr Mandantenkonto aktiviert.
- Sie gehören einer Benutzergruppe an, die über die"Verwalten von Endpunkten oder Root-Zugriffsberechtigungen" .
- Die vom Plattformdienst-Endpunkt referenzierte Ressource wurde erstellt:
  - CloudMirror-Replikation: S3-Bucket
  - Ereignisbenachrichtigung: Amazon Simple Notification Service (Amazon SNS) oder Kafka-Thema
  - Suchbenachrichtigung: Elasticsearch-Index, wenn der Zielcluster nicht für die automatische Erstellung von Indizes konfiguriert ist.
- Sie verfügen über die Informationen zur Zielressource:
  - Host und Port für den Uniform Resource Identifier (URI)

Wenn Sie einen auf einem StorageGRID -System gehosteten Bucket als Endpunkt für die CloudMirror-Replikation verwenden möchten, wenden Sie sich an den Grid-Administrator, um die einzugebenden Werte zu ermitteln.

- Eindeutiger Ressourcenname (URN)

  "Geben Sie die URN für den Plattformdienst-Endpunkt an"

- Authentifizierungsdaten (falls erforderlich):

  Suchintegrationsendpunkte

  Für Suchintegrationsendpunkte können Sie die folgenden Anmeldeinformationen verwenden:

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

  CloudMirror-Replikationsendpunkte

  Für CloudMirror-Replikationsendpunkte können Sie die folgenden Anmeldeinformationen verwenden:

  - Zugriffsschlüssel: Zugriffsschlüssel-ID und geheimer Zugriffsschlüssel
  - CAP (C2S Access Portal): URL für temporäre Anmeldeinformationen, Server- und Client-Zertifikate, Client-Schlüssel und eine optionale Passphrase für den privaten Client-Schlüssel.

  Amazon SNS-Endpunkte

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

  - Zugriffsschlüssel: Zugriffsschlüssel-ID und geheimer Zugriffsschlüssel

  Kafka-Endpunkte

  Für Kafka-Endpunkte können Sie die folgenden Anmeldeinformationen verwenden:

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

- Sicherheitszertifikat (bei Verwendung eines benutzerdefinierten CA-Zertifikats)

- Wenn die Elasticsearch-Sicherheitsfunktionen aktiviert sind, verfügen Sie über die Berechtigung zum Überwachen des Clusters für Konnektivitätstests und entweder über die Berechtigung zum Schreiben des Index oder über die Berechtigung zum Indexieren und Löschen des Index für Dokumentaktualisierungen.

Schritte

1. Wählen Sie **STORAGE (S3)** > **Plattformdienst-Endpunkte**. Die Seite „Plattformdienst-Endpunkte“ wird angezeigt.
2. Wählen Sie **Endpunkt erstellen**.
3. Geben Sie einen Anzeigenamen ein, um den Endpunkt und seinen Zweck kurz zu beschreiben.

   Der Typ des Plattformdienstes, den der Endpunkt unterstützt, wird neben dem Endpunktnamen angezeigt,

wenn dieser auf der Seite „Endpunkte“ aufgeführt ist. Sie müssen diese Information also nicht in den Namen aufnehmen.

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

   Verwenden Sie eines der folgenden Formate:

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

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

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

   Beispielsweise könnte die URI für einen auf StorageGRID gehosteten Bucket wie folgt lauten:

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

   In diesem Beispiel `s3.example.com` stellt den DNS-Eintrag für die virtuelle IP (VIP) der StorageGRID Hochverfügbarkeitsgruppe (HA) dar und `10443` stellt den im Load Balancer-Endpunkt definierten Port dar.

   > Wenn möglich, sollten Sie eine Verbindung zu einer HA-Gruppe von Lastausgleichsknoten herstellen, um einen einzelnen Fehlerpunkt zu vermeiden.

   Ähnlich könnte die URI für einen auf AWS gehosteten Bucket lauten:

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

   > Wenn der Endpunkt für den CloudMirror-Replikationsdienst verwendet wird, schließen Sie den Bucket-Namen nicht in die URI ein. Sie geben den Bucket-Namen in das Feld **URN** ein.

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

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

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

Suchintegrationsendpunkte

Geben Sie die Anmeldeinformationen für einen Suchintegrationsendpunkt ein oder laden Sie sie hoch.

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

Authentifizierungstyp	Beschreibung	Anmeldeinformationen
Anonym	Bietet anonymen Zugriff auf das Ziel. Funktioniert nur für Endpunkte, bei denen die Sicherheit deaktiviert ist.	Keine Authentifizierung.
Zugriffsschlüssel	Verwendet Anmeldeinformationen im AWS-Stil, um Verbindungen mit dem Ziel zu authentifizieren.	• Zugriffsschlüssel-ID • Geheimer Zugriffsschlüssel
Grundlegendes HTTP	Verwendet einen Benutzernamen und ein Kennwort, um Verbindungen zum Ziel zu authentifizieren.	• Benutzername • Passwort

CloudMirror-Replikationsendpunkte

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

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

Authentifizierungstyp	Beschreibung	Anmeldeinformationen
Anonym	Bietet anonymen Zugriff auf das Ziel. Funktioniert nur für Endpunkte, bei denen die Sicherheit deaktiviert ist.	Keine Authentifizierung.
Zugriffsschlüssel	Verwendet Anmeldeinformationen im AWS-Stil, um Verbindungen mit dem Ziel zu authentifizieren.	• Zugriffsschlüssel-ID • Geheimer Zugriffsschlüssel

Authentifizierungstyp	Beschreibung	Anmeldeinformationen
CAP (C2S-Zugangsportal)	Verwendet Zertifikate und Schlüssel, um Verbindungen zum Ziel zu authentifizieren.	• URL für temporäre Anmeldeinformationen • Server-CA-Zertifikat (PEM-Datei-Upload) • Client-Zertifikat (PEM-Datei-Upload) • Privater Clientschlüssel (PEM-Dateiupload, verschlüsseltes OpenSSL-Format oder unverschlüsseltes privates Schlüsselformat) • Passphrase für den privaten Clientschlüssel (optional)

Amazon SNS-Endpunkte

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

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

Authentifizierungstyp	Beschreibung	Anmeldeinformationen
Anonym	Bietet anonymen Zugriff auf das Ziel. Funktioniert nur für Endpunkte, bei denen die Sicherheit deaktiviert ist.	Keine Authentifizierung.
Zugriffsschlüssel	Verwendet Anmeldeinformationen im AWS-Stil, um Verbindungen mit dem Ziel zu authentifizieren.	• Zugriffsschlüssel-ID • Geheimer Zugriffsschlüssel

Kafka-Endpunkte

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

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

Authentifizierungstyp	Beschreibung	Anmeldeinformationen
Anonym	Bietet anonymen Zugriff auf das Ziel. Funktioniert nur für Endpunkte, bei denen die Sicherheit deaktiviert ist.	Keine Authentifizierung.

Authentifizierungstyp	Beschreibung	Anmeldeinformationen
SASL/PLAIN	Verwendet einen Benutzernamen und ein Kennwort im Klartext, um Verbindungen zum Ziel zu authentifizieren.	• Benutzername • Passwort
SASL/SCRAM-SHA-256	Verwendet einen Benutzernamen und ein Kennwort unter Verwendung eines Challenge-Response-Protokolls und SHA-256-Hashing, um Verbindungen zum Ziel zu authentifizieren.	• Benutzername • Passwort
SASL/SCRAM-SHA-512	Verwendet einen Benutzernamen und ein Kennwort unter Verwendung eines Challenge-Response-Protokolls und SHA-512-Hashing, um Verbindungen zum Ziel zu authentifizieren.	• Benutzername • Passwort

Wählen Sie **Authentifizierung über Delegation verwenden**, wenn Benutzername und Kennwort von einem Delegationstoken abgeleitet sind, das von einem Kafka-Cluster abgerufen wurde.

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

Art der Zertifikatsprüfung	Beschreibung
Benutzerdefiniertes CA-Zertifikat verwenden	Verwenden Sie ein benutzerdefiniertes Sicherheitszertifikat. Wenn Sie diese Einstellung auswählen, kopieren Sie das benutzerdefinierte Sicherheitszertifikat und fügen Sie es in das Textfeld **CA-Zertifikat** ein.
CA-Zertifikat des Betriebssystems verwenden	Verwenden Sie das auf dem Betriebssystem installierte Standard-Grid-CA-Zertifikat, um Verbindungen zu sichern.
Zertifikat nicht überprüfen	Das für die TLS-Verbindung verwendete Zertifikat wird nicht überprüft. Diese Option ist nicht sicher.

10. Wählen Sie **Endpunkt testen und erstellen**.
    - Wenn der Endpunkt mit den angegebenen Anmeldeinformationen erreicht werden kann, wird eine Erfolgsmeldung angezeigt. Die Verbindung zum Endpunkt wird von einem Knoten an jedem Standort validiert.
    - Wenn die Endpunktvalidierung fehlschlägt, wird eine Fehlermeldung angezeigt. Wenn Sie den Endpunkt ändern müssen, um den Fehler zu beheben, wählen Sie **Zurück zu den Endpunktdetails** und aktualisieren Sie die Informationen. Wählen Sie dann **Testen und Endpunkt erstellen**.

Die Endpunkterstellung schlägt fehl, wenn Plattformdienste für Ihr Mandantenkonto nicht aktiviert sind. Wenden Sie sich an Ihren StorageGRID Administrator.

Nachdem Sie einen Endpunkt konfiguriert haben, können Sie dessen URN verwenden, um einen Plattformdienst zu konfigurieren.

Ähnliche Informationen

- "Geben Sie die URN für den Plattformdienst-Endpunkt an"
- "Konfigurieren der CloudMirror-Replikation"
- "Konfigurieren von Ereignisbenachrichtigungen"
- "Suchintegrationsdienst konfigurieren"

Testen Sie die Verbindung für den Plattformdienst-Endpunkt

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

Bevor Sie beginnen

- Sie sind beim Tenant Manager angemeldet mit einem"unterstützter Webbrowser" .
- Sie gehören einer Benutzergruppe an, die über die"Verwalten von Endpunkten oder Root-Zugriffsberechtigungen" .

Informationen zu diesem Vorgang

StorageGRID überprüft nicht, ob die Anmeldeinformationen über die richtigen Berechtigungen verfügen.

Schritte

1. Wählen Sie **STORAGE (S3)** > **Plattformdienst-Endpunkte**.

   Die Seite „Plattformdienst-Endpunkte“ wird angezeigt und zeigt die Liste der bereits konfigurierten Plattformdienst-Endpunkte.

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

   Die Seite mit den Endpunktdetails wird angezeigt.

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

Plattformdienst-Endpunkt bearbeiten

Sie können die Konfiguration für einen Plattformdienst-Endpunkt bearbeiten, um dessen Namen, URI oder andere Details zu ändern. Beispielsweise müssen Sie möglicherweise

abgelaufene Anmeldeinformationen aktualisieren oder die URI ändern, damit sie für das Failover auf einen Backup-Elasticsearch-Index verweist. Sie können die URN für einen Plattformdienst-Endpunkt nicht ändern.

Bevor Sie beginnen

- Sie sind beim Tenant Manager angemeldet mit einem"unterstützter Webbrowser" .
- Sie gehören einer Benutzergruppe an, die über die"Verwalten von Endpunkten oder Root-Zugriffsberechtigungen" .

Schritte

1. Wählen Sie **STORAGE (S3)** > **Plattformdienst-Endpunkte**.

   Die Seite „Plattformdienst-Endpunkte“ wird angezeigt und zeigt die Liste der bereits konfigurierten Plattformdienst-Endpunkte.

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

   Die Seite mit den Endpunktdetails wird angezeigt.

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

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

   a. Um den Anzeigenamen für den Endpunkt zu ändern, wählen Sie das Bearbeitungssymbol .
   b. Ändern Sie die URI nach Bedarf.
   c. Ändern Sie bei Bedarf den Authentifizierungstyp.
      - Ändern Sie für die Zugriffsschlüsselauthentifizierung den Schlüssel nach Bedarf, indem Sie **S3-Schlüssel bearbeiten** auswählen und eine neue Zugriffsschlüssel-ID und einen geheimen Zugriffsschlüssel einfügen. Wenn Sie Ihre Änderungen abbrechen müssen, wählen Sie **S3-Schlüsselbearbeitung rückgängig machen**.
      - Ändern Sie für die CAP-Authentifizierung (C2S Access Portal) die URL der temporären Anmeldeinformationen oder die optionale Passphrase für den privaten Clientschlüssel und laden Sie bei Bedarf neue Zertifikats- und Schlüsseldateien hoch.

        Der private Schlüssel des Clients muss im verschlüsselten OpenSSL-Format oder im unverschlüsselten privaten Schlüsselformat vorliegen.

   d. Ändern Sie bei Bedarf die Methode zur Überprüfung des Servers.
5. Wählen Sie **Testen und Änderungen speichern**.
   - Wenn der Endpunkt mit den angegebenen Anmeldeinformationen erreicht werden kann, wird eine Erfolgsmeldung angezeigt. Die Verbindung zum Endpunkt wird von einem Knoten an jedem Standort überprüft.
   - Wenn die Endpunktvalidierung fehlschlägt, wird eine Fehlermeldung angezeigt. Ändern Sie den Endpunkt, um den Fehler zu beheben, und wählen Sie dann **Testen und Änderungen speichern** aus.

Plattformdienst-Endpunkt löschen

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

Bevor Sie beginnen

- Sie sind beim Tenant Manager angemeldet mit einem"unterstützter Webbrowser" .
- Sie gehören einer Benutzergruppe an, die über die"Verwalten von Endpunkten oder Root-Zugriffsberechtigungen" .

Schritte

1. Wählen Sie **STORAGE (S3)** > **Plattformdienst-Endpunkte**.

   Die Seite „Plattformdienst-Endpunkte“ wird angezeigt und zeigt die Liste der bereits konfigurierten Plattformdienst-Endpunkte.

2. Aktivieren Sie das Kontrollkästchen für jeden Endpunkt, den Sie löschen möchten.

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

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

   Es wird eine Bestätigungsmeldung angezeigt.

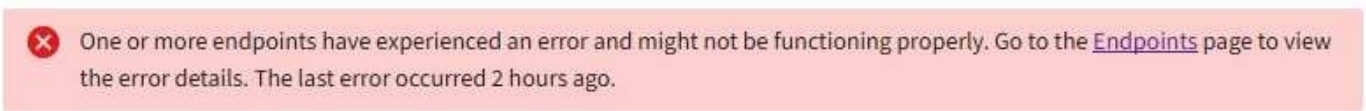
4. Wählen Sie **Endpunkt löschen**.

Beheben von Fehlern bei Plattformdienst-Endpunkten

Wenn beim Versuch von StorageGRID , mit einem Plattformdienst-Endpunkt zu kommunizieren, ein Fehler auftritt, wird auf dem Dashboard eine Meldung angezeigt. Auf der Seite „Plattformdienst-Endpunkte“ gibt die Spalte „Letzter Fehler“ an, wie lange der Fehler her ist. Es wird kein Fehler angezeigt, wenn die mit den Anmeldeinformationen eines Endpunkts verknüpften Berechtigungen falsch sind.

Feststellen, ob ein Fehler aufgetreten ist

Wenn innerhalb der letzten 7 Tage Fehler am Endpunkt der Plattformdienste aufgetreten sind, wird im Tenant Manager-Dashboard eine Warnmeldung angezeigt. Weitere Einzelheiten zum Fehler finden Sie auf der Seite „Plattformdienst-Endpunkte“.



Derselbe Fehler, der auf dem Dashboard angezeigt wird, erscheint auch oben auf der Seite „Plattformdienst-Endpunkte“. So zeigen Sie eine ausführlichere Fehlermeldung an:

Schritte

1. Wählen Sie aus der Liste der Endpunkte den Endpunkt aus, bei dem der Fehler auftritt.
2. Wählen Sie auf der Seite mit den Endpunktdetails **Verbindung** aus. Auf dieser Registerkarte wird nur der letzte Fehler für einen Endpunkt angezeigt und es wird angegeben, wie lange der Fehler her ist. Fehler, die das rote X-Symbol enthalten  innerhalb der letzten 7 Tage aufgetreten ist.

Prüfen, ob der Fehler noch aktuell ist

Einige Fehler werden möglicherweise auch nach ihrer Behebung weiterhin in der Spalte **Letzter Fehler** angezeigt. So können Sie feststellen, ob ein Fehler aktuell ist, oder das Entfernen eines behobenen Fehlers aus der Tabelle erzwingen:

Schritte

1. Wählen Sie den Endpunkt aus.

   Die Seite mit den Endpunktdetails wird angezeigt.

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

Wenn Sie **Verbindung testen** auswählen, überprüft StorageGRID , ob der Endpunkt der Plattformdienste vorhanden ist und mit den aktuellen Anmeldeinformationen erreicht werden kann. Die Verbindung zum Endpunkt wird von einem Knoten an jedem Standort validiert.

Beheben von Endpunktfehlern

Mithilfe der Meldung „Letzter Fehler“ auf der Seite mit den Endpunktdetails können Sie die Fehlerursache ermitteln. Bei einigen Fehlern müssen Sie möglicherweise den Endpunkt bearbeiten, um das Problem zu beheben. Beispielsweise kann ein CloudMirroring-Fehler auftreten, wenn StorageGRID nicht auf den Ziel-S3-Bucket zugreifen kann, weil es nicht über die richtigen Zugriffsberechtigungen verfügt oder der Zugriffsschlüssel abgelaufen ist. Die Meldung lautet: „Entweder müssen die Endpunktanmeldeinformationen oder der Zielzugriff aktualisiert werden“, und die Details lauten „AccessDenied“ oder „InvalidAccessKeyId“.

Wenn Sie den Endpunkt bearbeiten müssen, um einen Fehler zu beheben, führt die Auswahl von **Testen und Änderungen speichern** dazu, dass StorageGRID den aktualisierten Endpunkt validiert und bestätigt, dass er mit den aktuellen Anmeldeinformationen erreicht werden kann. Die Verbindung zum Endpunkt wird von einem Knoten an jedem Standort validiert.

Schritte

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

Endpunktanmeldeinformationen mit unzureichenden Berechtigungen

Wenn StorageGRID einen Plattformdienst-Endpunkt validiert, bestätigt es, dass die Anmeldeinformationen des Endpunkts zum Kontaktieren der Zielressource verwendet werden können, und führt eine grundlegende Berechtigungsprüfung durch. StorageGRID validiert jedoch nicht alle Berechtigungen, die für bestimmte Vorgänge der Plattformdienste erforderlich sind. Wenn Sie beim Versuch, einen Plattformdienst zu verwenden, eine Fehlermeldung erhalten (z. B. „403 Forbidden“), überprüfen Sie daher die mit den Anmeldeinformationen des Endpunkts verknüpften Berechtigungen.

Ähnliche Informationen

- **StorageGRID verwalten › Fehlerbehebung bei Plattformdiensten**
- "Plattformdienst-Endpunkt erstellen"
- "Testen Sie die Verbindung für den Plattformdienst-Endpunkt"
- "Plattformdienst-Endpunkt bearbeiten"

Konfigurieren der CloudMirror-Replikation

Um die CloudMirror-Replikation für einen Bucket zu aktivieren, erstellen und wenden Sie eine gültige XML-Konfiguration für die Bucket-Replikation an.

Bevor Sie beginnen

- Die Plattformdienste wurden von einem StorageGRID Administrator für Ihr Mandantenkonto aktiviert.
- Sie haben bereits einen Bucket erstellt, der als Replikationsquelle fungiert.
- Der Endpunkt, den Sie als Ziel für die CloudMirror-Replikation verwenden möchten, ist bereits vorhanden und Sie verfügen über seine URN.
- Sie gehören einer Benutzergruppe an, die über die"Verwalten Sie alle Buckets oder Root-Zugriffsberechtigungen" . Diese Berechtigungen überschreiben die Berechtigungseinstellungen in Gruppen- oder Bucket-Richtlinien, wenn der Bucket mit dem Tenant Manager konfiguriert wird.

Informationen zu diesem Vorgang

Die CloudMirror-Replikation kopiert Objekte aus einem Quell-Bucket in einen Ziel-Bucket, der in einem Endpunkt angegeben ist.

Allgemeine Informationen zur Bucket-Replikation und ihrer Konfiguration finden Sie unter "Amazon Simple Storage Service (S3)-Dokumentation: Objekte replizieren" . Informationen zur Implementierung von GetBucketReplication, DeleteBucketReplication und PutBucketReplication StorageGRID finden Sie im"Operationen an Buckets" .

> Die CloudMirror-Replikation weist wichtige Ähnlichkeiten und Unterschiede zur Cross-Grid-Replikationsfunktion auf. Weitere Informationen finden Sie unter"Vergleichen Sie Cross-Grid-Replikation und CloudMirror-Replikation" .

Beachten Sie beim Konfigurieren der CloudMirror-Replikation die folgenden Anforderungen und Merkmale:

- Wenn Sie eine gültige XML-Konfiguration für die Bucket-Replikation erstellen und anwenden, muss diese für jedes Ziel die URN eines S3-Bucket-Endpunkts verwenden.
- Die Replikation wird für Quell- oder Ziel-Buckets mit aktivierter S3-Objektsperre nicht unterstützt.
- Wenn Sie die CloudMirror-Replikation für einen Bucket aktivieren, der Objekte enthält, werden dem Bucket neu hinzugefügte Objekte repliziert, die vorhandenen Objekte im Bucket werden jedoch nicht repliziert. Sie müssen vorhandene Objekte aktualisieren, um die Replikation auszulösen.
- Wenn Sie in der XML-Replikationskonfiguration eine Speicherklasse angeben, verwendet StorageGRID diese Klasse beim Ausführen von Vorgängen am Ziel-S3-Endpunkt. Der Zielendpunkt muss auch die angegebene Speicherklasse unterstützen. Befolgen Sie unbedingt alle Empfehlungen des Zielsystemanbieters.

Schritte

1. Aktivieren Sie die Replikation für Ihren Quell-Bucket:

- Verwenden Sie einen Texteditor, um die zum Aktivieren der Replikation erforderliche XML-Replikationskonfiguration zu erstellen, wie in der S3-Replikations-API angegeben.
- Beim Konfigurieren des XML:
  - Beachten Sie, dass StorageGRID nur V1 der Replikationskonfiguration unterstützt. Dies bedeutet, dass StorageGRID die Verwendung des `Filter` Element für Regeln und befolgt V1-Konventionen zum Löschen von Objektversionen. Weitere Informationen finden Sie in der Amazon-Dokumentation zur Replikationskonfiguration.
  - Verwenden Sie die URN eines S3-Bucket-Endpunkts als Ziel.
  - Optional fügen Sie die `<StorageClass>` Element und geben Sie eine der folgenden Optionen an:
    - `STANDARD`: Die Standardspeicherklasse. Wenn Sie beim Hochladen eines Objekts keine Speicherklasse angeben, `STANDARD` Speicherklasse wird verwendet.
    - `STANDARD_IA`: (Standard – seltener Zugriff.) Verwenden Sie diese Speicherklasse für Daten, auf die weniger häufig zugegriffen wird, die aber dennoch bei Bedarf einen schnellen Zugriff erfordern.
    - `REDUCED_REDUNDANCY`: Verwenden Sie diese Speicherklasse für nicht kritische, reproduzierbare Daten, die mit weniger Redundanz gespeichert werden können als die `STANDARD` Speicherklasse.
  - Wenn Sie eine `Role` im Konfigurations-XML wird es ignoriert. Dieser Wert wird von StorageGRID nicht verwendet.

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

2. Wählen Sie im Dashboard **Buckets anzeigen** oder wählen Sie **STORAGE (S3)** > **Buckets**.
3. Wählen Sie den Namen des Quell-Buckets aus.

   Die Bucket-Detailseite wird angezeigt.

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

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

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

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

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

      Bei kleinen Objekten erfolgt die Replikation schnell.

Ähnliche Informationen

"Plattformdienst-Endpunkt erstellen"

Konfigurieren von Ereignisbenachrichtigungen

Sie aktivieren Benachrichtigungen für einen Bucket, indem Sie eine XML-Benachrichtigungskonfiguration erstellen und den Tenant Manager verwenden, um die XML auf einen Bucket anzuwenden.

Bevor Sie beginnen

- Die Plattformdienste wurden von einem StorageGRID Administrator für Ihr Mandantenkonto aktiviert.
- Sie haben bereits einen Bucket erstellt, der als Benachrichtigungsquelle dient.
- Der Endpunkt, den Sie als Ziel für Ereignisbenachrichtigungen verwenden möchten, ist bereits vorhanden und Sie verfügen über seine URN.
- Sie gehören einer Benutzergruppe an, die über die"Verwalten Sie alle Buckets oder Root-Zugriffsberechtigungen" . Diese Berechtigungen überschreiben die Berechtigungseinstellungen in Gruppen- oder Bucket-Richtlinien, wenn der Bucket mit dem Tenant Manager konfiguriert wird.

Informationen zu diesem Vorgang

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

Allgemeine Informationen zu Ereignisbenachrichtigungen und deren Konfiguration finden Sie im "Amazon-Dokumentation" . Informationen zur Implementierung der S3-Bucket-Benachrichtigungskonfigurations-API durch StorageGRID finden Sie im"Anweisungen zur Implementierung von S3-Clientanwendungen" .

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

- Wenn Sie eine gültige XML-Benachrichtigungskonfiguration erstellen und anwenden, muss für jedes Ziel die URN eines Endpunkts für Ereignisbenachrichtigungen verwendet werden.
- Obwohl die Ereignisbenachrichtigung für einen Bucket mit aktivierter S3-Objektsperre konfiguriert werden kann, werden die S3-Objektsperre-Metadaten (einschließlich „Aufbewahrungsdatum“ und „Legal Hold“-Status) der Objekte nicht in die Benachrichtigungsnachrichten aufgenommen.
- Nachdem Sie Ereignisbenachrichtigungen konfiguriert haben, wird jedes Mal, wenn ein bestimmtes Ereignis für ein Objekt im Quell-Bucket eintritt, eine Benachrichtigung generiert und an das als Zielendpunkt verwendete Amazon SNS- oder Kafka-Thema gesendet.

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

Schritte

1. Aktivieren Sie Benachrichtigungen für Ihren Quell-Bucket:
   - Verwenden Sie einen Texteditor, um die zum Aktivieren von Ereignisbenachrichtigungen erforderliche XML-Benachrichtigungskonfiguration zu erstellen, wie in der S3-Benachrichtigungs-API angegeben.
   - Verwenden Sie beim Konfigurieren des XML die URN eines Endpunkts für Ereignisbenachrichtigungen als Zielthema.

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

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

   Die Bucket-Detailseite wird angezeigt.

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

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

7. Überprüfen Sie, ob die Ereignisbenachrichtigungen richtig konfiguriert sind:
   a. Führen Sie eine Aktion für ein Objekt im Quell-Bucket aus, das die Anforderungen zum Auslösen einer Benachrichtigung erfüllt, wie in der Konfigurations-XML konfiguriert.

Im Beispiel wird eine Ereignisbenachrichtigung gesendet, wenn ein Objekt mit dem `images/` Präfix.

b. Bestätigen Sie, dass eine Benachrichtigung an das Zielthema Amazon SNS oder Kafka übermittelt wurde.

Wenn Ihr Zielthema beispielsweise auf Amazon SNS gehostet wird, können Sie den Dienst so konfigurieren, dass er Ihnen eine E-Mail sendet, wenn die Benachrichtigung zugestellt wird.


```
{
   "Records":[
      {
         "eventVersion":"2.0",
         "eventSource":"sgws:s3",
         "eventTime":"2017-08-08T23:52:38Z",
         "eventName":"ObjectCreated:Put",
         "userIdentity":{
            "principalId":"11111111111111111"
         },
         "requestParameters":{
            "sourceIPAddress":"193.51.100.20"
         },
         "responseElements":{
            "x-amz-request-id":"122047343"
         },
         "s3":{
            "s3SchemaVersion":"1.0",
            "configurationId":"Image-created",
            "bucket":{
               "name":"test1",
               "ownerIdentity":{
                  "principalId":"11111111111111111"
               },
               "arn":"arn:sgws:s3:::test1"
            },
            "object":{
               "key":"images/cat.jpg",
               "size":0,
               "eTag":"d41d8cd98f00b204e9800998ecf8427e",
               "sequencer":"14D90402421461C7"
            }
         }
      }
   ]
}
```


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

Ähnliche Informationen

"Benachrichtigungen für Buckets verstehen"

"Verwenden Sie die S3 REST-API"

"Plattformdienst-Endpunkt erstellen"

Konfigurieren des Suchintegrationsdienstes

Sie aktivieren die Suchintegration für einen Bucket, indem Sie XML für die Suchintegration erstellen und den Tenant Manager verwenden, um das XML auf den Bucket anzuwenden.

Bevor Sie beginnen

- Die Plattformdienste wurden von einem StorageGRID Administrator für Ihr Mandantenkonto aktiviert.
- Sie haben bereits einen S3-Bucket erstellt, dessen Inhalt Sie indizieren möchten.
- Der Endpunkt, den Sie als Ziel für den Suchintegrationsdienst verwenden möchten, ist bereits vorhanden und Sie verfügen über seine URN.
- Sie gehören einer Benutzergruppe an, die über die"Verwalten Sie alle Buckets oder Root-Zugriffsberechtigungen" . Diese Berechtigungen überschreiben die Berechtigungseinstellungen in Gruppen- oder Bucket-Richtlinien, wenn der Bucket mit dem Tenant Manager konfiguriert wird.

Informationen zu diesem Vorgang

Nachdem Sie den Suchintegrationsdienst für einen Quell-Bucket konfiguriert haben, löst das Erstellen eines Objekts oder das Aktualisieren der Metadaten oder Tags eines Objekts das Senden von Objektmetadaten an den Zielendpunkt aus.

Wenn Sie den Suchintegrationsdienst für einen Bucket aktivieren, der bereits Objekte enthält, werden für vorhandene Objekte nicht automatisch Metadatenbenachrichtigungen gesendet. Aktualisieren Sie diese vorhandenen Objekte, um sicherzustellen, dass ihre Metadaten zum Zielsuchindex hinzugefügt werden.

Schritte

1. Aktivieren Sie die Suchintegration für einen Bucket:
    - Verwenden Sie einen Texteditor, um die XML-Metadatenbenachrichtigung zu erstellen, die zum Aktivieren der Suchintegration erforderlich ist.
    - Verwenden Sie beim Konfigurieren des XML die URN eines Suchintegrationsendpunkts als Ziel.

      Objekte können nach dem Präfix des Objektnamens gefiltert werden. Beispielsweise könnten Sie Metadaten für Objekte mit dem Präfix `images` zu einem Ziel und Metadaten für Objekte mit dem Präfix `videos` zu einem anderen. Konfigurationen mit überlappenden Präfixen sind ungültig und werden bei der Übermittlung abgelehnt. Beispielsweise eine Konfiguration, die eine Regel für Objekte mit dem Präfix `test` und eine zweite Regel für Objekte mit dem Präfix `test2` ist nicht erlaubt.

      Bei Bedarf finden Sie weitere Informationen imBeispiele für die Metadatenkonfigurations-XML .

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

Elemente in der XML-Konfiguration der Metadatenbenachrichtigung:

Name	Beschreibung	Erforderlich
Metadatenbenachrichtigungskonfiguration	Container-Tag für Regeln, die zum Angeben der Objekte und des Ziels für Metadatenbenachrichtigungen verwendet werden. Enthält ein oder mehrere Regelelemente.	Ja
Regel	Container-Tag für eine Regel, die die Objekte identifiziert, deren Metadaten einem angegebenen Index hinzugefügt werden sollen. Regeln mit überlappenden Präfixen werden abgelehnt. Im MetadataNotificationConfiguration-Element enthalten.	Ja
AUSWEIS	Eindeutige Kennung für die Regel. Im Regelelement enthalten.	Nein
Status	Der Status kann „Aktiviert“ oder „Deaktiviert“ sein. Für deaktivierte Regeln werden keine Maßnahmen ergriffen. Im Regelelement enthalten.	Ja
Präfix	Objekte, die dem Präfix entsprechen, sind von der Regel betroffen und ihre Metadaten werden an das angegebene Ziel gesendet. Um alle Objekte abzugleichen, geben Sie ein leeres Präfix an. Im Regelelement enthalten.	Ja
Ziel	Container-Tag für das Ziel einer Regel. Im Regelelement enthalten.	Ja

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

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

   Die Bucket-Detailseite wird angezeigt.

4. Wählen Sie **Plattformdienste** > **Suchintegration**
5. Aktivieren Sie das Kontrollkästchen **Suchintegration aktivieren**.
6. Fügen Sie die Metadaten-Benachrichtigungskonfiguration in das Textfeld ein und wählen Sie **Änderungen speichern**.

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

7. Überprüfen Sie, ob der Suchintegrationsdienst richtig konfiguriert ist:
   a. Fügen Sie dem Quell-Bucket ein Objekt hinzu, das die Anforderungen zum Auslösen einer Metadatenbenachrichtigung erfüllt, wie im Konfigurations-XML angegeben.

      Im zuvor gezeigten Beispiel lösen alle zum Bucket hinzugefügten Objekte eine Metadatenbenachrichtigung aus.

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

Nach Abschluss

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

- Wählen Sie **STORAGE (S3)** > **Buckets** und deaktivieren Sie das Kontrollkästchen **Suchintegration aktivieren**.
- Wenn Sie die S3-API direkt verwenden, verwenden Sie eine Benachrichtigungsanforderung zum Löschen von Bucket-Metadaten. Siehe die Anweisungen zum Implementieren von S3-Clientanwendungen.

Beispiel: Metadaten-Benachrichtigungskonfiguration, die für alle Objekte gilt

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

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

Beispiel: Konfiguration der Metadatenbenachrichtigung mit zwei Regeln

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

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

Metadaten-Benachrichtigungsformat

Wenn Sie den Suchintegrationsdienst für einen Bucket aktivieren, wird jedes Mal, wenn Objektmetadaten oder Tags hinzugefügt, aktualisiert oder gelöscht werden, ein JSON-Dokument generiert und an den Zielendpunkt gesendet.

Dieses Beispiel zeigt ein Beispiel des JSON, das generiert werden könnte, wenn ein Objekt mit dem Schlüssel `SGWS/Tagging.txt` wird in einem Bucket namens erstellt `test` . Der `test` Bucket ist nicht versioniert, also die `versionId` -Tag ist leer.

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

Im JSON-Dokument enthaltene Felder

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

Bucket- und Objektinformationen

`bucket`: Name des Buckets

`key`: Objektschlüsselname

`versionID`: Objektversion, für Objekte in versionierten Buckets

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

Systemmetadaten

`size`: Objektgröße (in Bytes), wie sie für einen HTTP-Client sichtbar ist

`md5`: Objekt-Hash

Benutzermetadaten

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

`key:value`

Schlagwörter

`tags`: Alle für das Objekt definierten Objekt-Tags als Schlüssel-Wert-Paare

`key:value`

So zeigen Sie Ergebnisse in Elasticsearch an

Für Tags und Benutzermetadaten übergibt StorageGRID Daten und Zahlen als Zeichenfolgen oder als S3-Ereignisbenachrichtigungen an Elasticsearch. Um Elasticsearch so zu konfigurieren, dass diese Zeichenfolgen

als Datumsangaben oder Zahlen interpretiert werden, befolgen Sie die Elasticsearch-Anweisungen zur dynamischen Feldzuordnung und zur Zuordnung von Datumsformaten. Aktivieren Sie die dynamischen Feldzuordnungen im Index, bevor Sie den Suchintegrationsdienst konfigurieren. Nachdem ein Dokument indiziert wurde, können Sie die Feldtypen des Dokuments im Index nicht mehr bearbeiten.

Copyright-Informationen

Markeninformationen