Cloud Storage Pools verwenden

StorageGRID software

NetApp
July 23, 2026

Inhalt

Cloud Storage Pools verwenden

Erfahren Sie mehr über Cloud Storage Pools in StorageGRID

Ein Cloud Storage Pool ermöglicht die Nutzung von ILM, um Objektdaten außerhalb Ihres StorageGRID-Systems zu verschieben. Beispielsweise kann es sinnvoll sein, selten genutzte Objekte in kostengünstigeren Cloud-Storage wie Amazon S3 Glacier, S3 Glacier Deep Archive, Google Cloud oder die Archive-Zugriffsebene in Microsoft Azure Blob Storage zu verschieben. Ebenso kann eine Cloud-Sicherung der StorageGRID-Objekte zur Verbesserung der Disaster Recovery sinnvoll sein.

Aus ILM-Sicht ähnelt ein Cloud Storage Pool einem Speicherpool. Zum Speichern von Objekten an einem der beiden Speicherorte wird der Pool beim Erstellen der Platzierungsanweisungen für eine ILM-Regel ausgewählt. Während Speicherpools jedoch aus Storage Nodes innerhalb des StorageGRID Systems bestehen, besteht ein Cloud Storage Pool aus einem externen Bucket (S3) oder Container (Azure Blob storage).

Die Tabelle vergleicht Speicherpools mit Cloud Storage Pools und zeigt die wichtigsten Gemeinsamkeiten und Unterschiede.

	Storage-Pool	**Cloud Storage Pool**
Wie wird es erstellt?	Verwendung der Option **ILM** > **Storage pools** im Grid Manager.	Verwendung der Option **ILM** > **Storage pools** > **Cloud Storage Pools** im Grid Manager. Der externe Bucket oder Container muss eingerichtet werden, bevor der Cloud Storage Pool erstellt werden kann.
Wie viele Pools können Sie erstellen?	Unbegrenzt.	Bis zu 10.

	Storage-Pool	Cloud Storage Pool
Wo werden Objekte gespeichert ?	Auf einem oder mehreren Speicherknoten innerhalb von StorageGRID.	In einem Amazon S3 Bucket, einem Azure Blob Storage Container oder einer Google Cloud, die sich außerhalb des StorageGRID Systems befindet. Wenn der Cloud Storage Pool ein Amazon S3-Bucket ist: • Optional kann ein Bucket-Lebenszyklus konfiguriert werden, um Objekte in kostengünstigen Langzeit-Storage wie Amazon S3 Glacier oder S3 Glacier Deep Archive zu überführen. Das externe Storage-System muss die Glacier-Storage-Klasse und die S3 RestoreObject API unterstützen. • Cloud-Speicherpools können für die Verwendung mit AWS Commercial Cloud Services (C2S) erstellt werden, die die AWS Secret Region unterstützen. Wenn es sich bei dem Cloud Storage Pool um einen Azure Blob Storage Container handelt, verschiebt StorageGRID das Objekt in die Archivschicht. **Hinweis:** Im Allgemeinen sollte die Azure Blob Storage-Lebenszyklusverwaltung nicht für den Container konfiguriert werden, der für einen Cloud Storage Pool verwendet wird. RestoreObject-Vorgänge an Objekten im Cloud Storage Pool können durch den konfigurierten Lebenszyklus beeinträchtigt werden.
Was steuert die Platzierung von Objekten?	Eine ILM-Regel in den aktiven ILM-Richtlinien.	Eine ILM-Regel in den aktiven ILM-Richtlinien.
Welche Datenschutzmethode wird verwendet?	Replikation oder Löschcodierung.	Replikation.
Wie viele Kopien jedes Objekts sind zulässig?	Mehrere.	Eine Kopie im Cloud Storage Pool und optional eine oder mehrere Kopien in StorageGRID. **Hinweis:** Ein Objekt kann nicht gleichzeitig in mehr als einem Cloud Storage Pool gespeichert werden.
Welche Vorteile gibt es?	Objekte sind jederzeit schnell zugänglich.	Kostengünstiger Storage. **Hinweis**: FabricPool-Daten können nicht in Cloud Storage Pools verschoben werden.

Lebenszyklus eines Cloud Storage Pool-Objekts in StorageGRID

Vor der Implementierung von Cloud Storage Pools ist der Lebenszyklus der Objekte zu prüfen, die in den jeweiligen Typen von Cloud Storage Pools gespeichert werden.

S3: Lebenszyklus eines Cloud Storage Pool-Objekts

Die Schritte beschreiben die Lebenszyklusphasen eines Objekts, das in einem S3 Cloud Storage Pool gespeichert ist.

> „Glacier“ bezeichnet sowohl die Glacier Storage-Klasse als auch die Glacier Deep Archive Storage-Klasse, mit einer Ausnahme: Die Glacier Deep Archive Storage-Klasse unterstützt die Expedited-Wiederherstellungsebene nicht. Nur Bulk- oder Standard-Wiederherstellung wird unterstützt.

> Die Google Cloud Platform (GCP) unterstützt den Abruf von Objekten aus Langzeit-Storage, ohne dass ein POST Restore-Vorgang erforderlich ist.

1. **Objekt in StorageGRID gespeichert**

   Um den Lebenszyklus zu starten, speichert eine Clientanwendung ein Objekt in StorageGRID.

2. **Objekt in den S3 Cloud Storage Pool verschoben**
   - Wenn das Objekt mit einer ILM-Regel übereinstimmt, die einen S3 Cloud Storage Pool als Speicherort verwendet, verschiebt StorageGRID das Objekt in den externen S3-Bucket, der vom Cloud Storage Pool angegeben wird.
   - Sobald das Objekt in den S3 Cloud Storage Pool verschoben wurde, kann die Clientanwendung es mit einer S3 GetObject Anfrage von StorageGRID abrufen, sofern das Objekt nicht in den Glacier Storage überführt wurde.
3. **Objekt in Glacier überführt (nicht wiederherstellbarer Zustand)**
   - Optional kann das Objekt in Glacier Storage überführt werden. Beispielsweise kann der externe S3-Bucket eine Lifecycle-Konfiguration verwenden, um ein Objekt sofort oder nach einer bestimmten Anzahl von Tagen in Glacier Storage zu überführen.

     > Wenn Sie Objekte migrieren möchten, müssen Sie eine Lebenszykluskonfiguration für den externen S3-Bucket erstellen und eine Speicherlösung verwenden, die die Glacier Speicherklasse implementiert und die S3 RestoreObject API unterstützt.

   - Während des Übergangs kann die Clientanwendung eine S3 HeadObject-Anfrage verwenden, um den Status des Objekts zu überwachen.
4. **Objekt aus Glacier Storage wiederhergestellt**

   Wurde ein Objekt in den Glacier Storage verschoben, kann die Clientanwendung eine S3 RestoreObject-Anfrage senden, um eine wiederherstellbare Kopie im S3 Cloud Storage Pool wiederherzustellen. Die Anfrage gibt an, wie viele Tage die Kopie im Cloud Storage Pool verfügbar sein soll und welche Datenzugriffsebene für die Wiederherstellung verwendet werden soll (Expedited, Standard oder Bulk). Sobald das Ablaufdatum der wiederherstellbaren Kopie erreicht ist, wird die Kopie automatisch wieder in einen nicht wiederherstellbaren Zustand versetzt.

Existieren eine oder mehrere Kopien des Objekts auch auf Speicherknoten innerhalb StorageGRID, ist es nicht erforderlich, das Objekt durch eine RestoreObject-Anfrage von Glacier wiederherzustellen. Stattdessen kann die lokale Kopie direkt per GetObject-Anfrage abgerufen werden.

5. **Objekt abgerufen**

   Sobald ein Objekt wiederhergestellt wurde, kann die Clientanwendung eine GetObject-Anfrage zum Abrufen des wiederhergestellten Objekts stellen.

Azure: Lebenszyklus eines Cloud Storage Pool Objekts

Die Schritte beschreiben die Lebenszyklusphasen eines Objekts, das in einem Azure Cloud Storage Pool gespeichert ist.

1. **Objekt in StorageGRID gespeichert**

   Um den Lebenszyklus zu starten, speichert eine Clientanwendung ein Objekt in StorageGRID.

2. **Objekt in Azure Cloud Storage Pool verschoben**

   Wenn das Objekt mit einer ILM-Regel übereinstimmt, die einen Azure Cloud Storage Pool als Speicherort verwendet, verschiebt StorageGRID das Objekt in den externen Azure Blob Storage Container, der vom Cloud Storage Pool angegeben wird.

3. **Objekt in die Archivebene verschoben (nicht abrufbarer Zustand)**

   Unmittelbar nach dem Verschieben des Objekts in den Azure Cloud Storage Pool wechselt StorageGRID das Objekt automatisch in die Azure Blob storage Archive-Ebene.

4. **Objekt aus der Archivebene wiederhergestellt**

   Wenn ein Objekt in die Archivierungsebene verschoben wurde, kann die Clientanwendung eine S3 RestoreObject-Anforderung senden, um eine wiederherstellbare Kopie im Azure Cloud Storage Pool wiederherzustellen.

   Wenn StorageGRID die RestoreObject empfängt, wird das Objekt vorübergehend in die Azure Blob storage Cool-Tier verschoben. Sobald das Ablaufdatum in der RestoreObject-Anfrage erreicht ist, wird das Objekt von StorageGRID wieder in die Archive-Tier verschoben.

   Existieren eine oder mehrere Kopien des Objekts auch auf Speicherknoten innerhalb StorageGRID, ist es nicht erforderlich, das Objekt durch eine RestoreObject Anfrage von der Archivzugriffsebene wiederherzustellen. Stattdessen kann die lokale Kopie direkt per GetObject Anfrage abgerufen werden.

5. **Objekt abgerufen**

   Sobald ein Objekt im Azure Cloud Storage Pool wiederhergestellt wurde, kann die Clientanwendung eine GetObject-Anfrage zum Abrufen des wiederhergestellten Objekts stellen.

Verwandte Informationen

"S3 REST-API verwenden"

Anwendungsfälle für Cloud Storage Pool in StorageGRID

Mit Cloud Storage Pools können Daten an einen externen Speicherort gesichert oder ausgelagert werden. Zusätzlich ist es möglich, Daten in mehr als einer Cloud zu sichern oder auszulagern.

StorageGRID Daten an einem externen Speicherort sichern

Sie können einen Cloud Storage Pool verwenden, um StorageGRID Objekte an einem externen Speicherort zu sichern.

Sind die Kopien in StorageGRID nicht zugänglich, können die Objektdaten im Cloud Storage Pool zur Bearbeitung von Clientanfragen verwendet werden. Es kann jedoch erforderlich sein, eine S3 RestoreObject Anfrage zu stellen, um auf die Sicherungskopie des Objekts im Cloud Storage Pool zuzugreifen.

Die Objektdaten in einem Cloud Storage Pool können auch zur Wiederherstellung von Daten verwendet werden, die in StorageGRID aufgrund eines Storage-Volume- oder Storage Node-Ausfalls verloren gegangen sind. Wenn sich die einzige verbleibende Kopie eines Objekts in einem Cloud Storage Pool befindet, stellt StorageGRID das Objekt vorübergehend wieder her und erstellt eine neue Kopie auf dem wiederhergestellten Storage Node.

Zur Implementierung einer Backup-Lösung:

1. Einen einzelnen Cloud Storage Pool erstellen.
2. Eine ILM-Regel konfigurieren, die gleichzeitig Objektkopien auf Storage Nodes (als replizierte oder erasure-coded Kopien) und eine einzelne Objektkopie im Cloud Storage Pool speichert.
3. Fügen Sie die Regel zu Ihrer ILM-Richtlinie hinzu. Anschließend die Richtlinie simulieren und aktivieren.

Tier-Daten von StorageGRID an externen Speicherort

Sie können einen Cloud Storage Pool verwenden, um Objekte außerhalb des StorageGRID Systems zu speichern. Beispielsweise kann es sein, dass eine große Anzahl von Objekten aufbewahrt werden muss, auf die jedoch voraussichtlich nur selten oder gar nicht zugegriffen wird. Ein Cloud Storage Pool kann genutzt werden, um die Objekte in kostengünstigeren Speicher zu verschieben und so Speicherplatz in StorageGRID freizugeben.

Zur Implementierung einer Tiering-Lösung:

1. Einen einzelnen Cloud Storage Pool erstellen.
2. Eine ILM-Regel konfigurieren, die selten verwendete Objekte von Storage Nodes in den Cloud Storage Pool verschiebt.
3. Fügen Sie die Regel zu Ihrer ILM-Richtlinie hinzu. Anschließend die Richtlinie simulieren und aktivieren.

Mehrere Cloud-Endpunkte verwalten

Sie können mehrere Cloud Storage Pool-Endpunkte konfigurieren, wenn Sie Objektdaten in mehr als einer Cloud tiern oder sichern möchten. Die Filter in Ihren ILM-Regeln ermöglichen die Angabe, welche Objekte in welchem Cloud Storage Pool gespeichert werden. Beispielsweise kann es gewünscht sein, Objekte bestimmter Mandanten oder Buckets in Amazon S3 Glacier und Objekte anderer Mandanten oder Buckets in Azure Blob storage zu speichern. Oder es kann erforderlich sein, Daten zwischen Amazon S3 Glacier und Azure Blob storage zu verschieben.

Bei der Verwendung mehrerer Cloud Storage Pool Endpunkte ist zu beachten, dass ein Objekt jeweils nur in einem Cloud Storage Pool gespeichert werden kann.

Zur Implementierung mehrerer Cloud-Endpunkte:

1. Bis zu 10 Cloud Storage Pools können erstellt werden.
2. Konfigurieren Sie ILM-Regeln, um die entsprechenden Objektdaten zum richtigen Zeitpunkt in jedem Cloud Storage Pool zu speichern. Beispielsweise können Objekte aus Bucket A in Cloud Storage Pool A und Objekte aus Bucket B in Cloud Storage Pool B gespeichert werden. Alternativ können Objekte zunächst für eine bestimmte Zeit in Cloud Storage Pool A gespeichert und anschließend in Cloud Storage Pool B verschoben werden.
3. Fügen Sie die Regeln Ihrer ILM-Richtlinie hinzu. Simulieren und aktivieren Sie anschließend die Richtlinie.

Anforderungen und Beschränkungen für Cloud Storage Pool in StorageGRID

Wenn Sie planen, einen Cloud Storage Pool zu verwenden, um Objekte aus dem StorageGRID System zu verschieben, sollten die Überlegungen zur Konfiguration und Verwendung von Cloud Storage Pools geprüft werden.

Allgemeine Überlegungen

- Im Allgemeinen ist Cloud-Archivspeicher wie Amazon S3 Glacier oder Azure Blob Storage eine kostengünstige Möglichkeit, Objektdaten zu speichern. Die Kosten für den Datenabruf aus Cloud-Archivspeicher sind jedoch relativ hoch. Um die niedrigsten Gesamtkosten zu erreichen, sollte berücksichtigt werden, wann und wie oft auf die Objekte im Cloud Storage Pool zugegriffen wird. Die Nutzung eines Cloud Storage Pool wird nur für Inhalte empfohlen, auf die voraussichtlich selten zugegriffen wird.
- Die Verwendung von Cloud Storage Pools mit FabricPool wird aufgrund der zusätzlichen Latenz beim Abrufen eines Objekts vom Cloud Storage Pool-Ziel nicht unterstützt.
- Objekte, für die die S3 Object Lock aktiviert ist, können nicht in Cloud Storage Pools platziert werden.
- Die folgenden Plattform-, Authentifizierungs- und Protokollkombinationen mit S3 Object lock werden für Cloud Storage Pools nicht unterstützt:
  - **Plattformen**: Google Cloud Platform und Azure
  - **Authentifizierungstypen**: Anonymer Zugriff
  - **Protokoll**: HTTP

Überlegungen zu den für Cloud Storage Pools verwendeten Ports

Um sicherzustellen, dass die ILM-Regeln Objekte in den und aus dem angegebenen Cloud Storage Pool verschieben können, müssen die Netzwerke konfiguriert werden, die die Storage Nodes Ihres Systems enthalten. Es muss sichergestellt werden, dass die folgenden Ports mit dem Cloud Storage Pool kommunizieren können.

Standardmäßig verwenden Cloud Storage Pools die folgenden Ports:

- **80**: Für Endpunkt-URIs, die mit http beginnen

- **443**: Für Endpunkt-URIs, die mit https beginnen

Sie können beim Erstellen oder Bearbeiten eines Cloud Storage Pools einen anderen Port angeben.

Wenn Sie einen nicht transparenten Proxyserver verwenden, muss auch "einen Speicherproxy konfigurieren" zugelassen werden, damit Nachrichten an externe Endpunkte wie einen Endpunkt im Internet gesendet werden können.

Kostenüberlegungen

Der Zugriff auf Speicher in der Cloud über einen Cloud Storage Pool erfordert eine Netzwerkverbindung zur Cloud. Die Kosten der Netzwerkinfrastruktur, die für den Zugriff auf die Cloud verwendet wird, sind unter Berücksichtigung der erwarteten Datenmenge, die zwischen StorageGRID und der Cloud über den Cloud Storage Pool übertragen wird, angemessen zu planen.

Wenn StorageGRID eine Verbindung zum externen Cloud Storage Pool-Endpunkt herstellt, sendet es verschiedene Anfragen, um die Konnektivität zu überwachen und sicherzustellen, dass die erforderlichen Operationen durchgeführt werden können. Während mit diesen Anfragen zusätzliche Kosten verbunden sind, sollten die Kosten für die Überwachung eines Cloud Storage Pools nur einen kleinen Bruchteil der Gesamtkosten für die Speicherung von Objekten in S3 oder Azure ausmachen.

Höhere Kosten können entstehen, wenn Objekte von einem externen Cloud Storage Pool-Endpunkt zurück zu StorageGRID verschoben werden müssen. Objekte können in folgenden Fällen zurück zu StorageGRID verschoben werden:

- Die einzige Kopie des Objekts befindet sich in einem Cloud Storage Pool und es wird entschieden, das Objekt stattdessen in StorageGRID zu speichern. In diesem Fall werden die ILM-Regeln und die Richtlinie neu konfiguriert. Bei der ILM-Auswertung sendet StorageGRID mehrere Anfragen, um das Objekt aus dem Cloud Storage Pool abzurufen. Anschließend erstellt StorageGRID die angegebene Anzahl lokal replizierter oder mit Erasure Coding versehener Kopien. Nachdem das Objekt zurück in StorageGRID verschoben wurde, wird die Kopie im Cloud Storage Pool gelöscht.
- Objekte gehen aufgrund eines Ausfalls des Storage Node verloren. Befindet sich die einzige verbleibende Kopie eines Objekts in einem Cloud Storage Pool, stellt StorageGRID das Objekt vorübergehend wieder her und erstellt eine neue Kopie auf dem wiederhergestellten Storage Node.

> Wenn Objekte aus einem Cloud Storage Pool zurück nach StorageGRID verschoben werden, sendet StorageGRID für jedes Objekt mehrere Anfragen an den Cloud Storage Pool-Endpunkt. Vor dem Verschieben einer großen Anzahl von Objekten empfiehlt es sich, den technischen Support zu kontaktieren, um den Zeitrahmen und die damit verbundenen Kosten abzuschätzen.

S3: Erforderliche Berechtigungen für den Cloud Storage Pool-Bucket

Die Richtlinien für den externen S3-Bucket, der für einen Cloud-Speicherpool verwendet wird, müssen StorageGRID die Berechtigung erteilen, ein Objekt in den Bucket zu verschieben, den Status eines Objekts abzurufen, ein Objekt bei Bedarf aus dem Glacier-Speicher wiederherzustellen und mehr. Idealerweise sollte StorageGRID Vollzugriff auf den Bucket haben (`s3:*`; ist dies jedoch nicht möglich, muss die Bucket-Richtlinie StorageGRID die folgenden S3-Berechtigungen gewähren:

- `s3:AbortMultipartUpload`
- `s3:DeleteObject`
- `s3:GetObject`

- `s3:ListBucket`
- `s3:ListBucketMultipartUploads`
- `s3:ListMultipartUploadParts`
- `s3:PutObject`
- `s3:RestoreObject`

S3: Überlegungen zum Lebenszyklus des externen Buckets

Die Verschiebung von Objekten zwischen StorageGRID und dem im Cloud Storage Pool angegebenen externen S3-Bucket wird durch ILM-Regeln und die aktiven ILM-Richtlinien in StorageGRID gesteuert. Im Gegensatz dazu wird die Übertragung von Objekten vom im Cloud Storage Pool angegebenen externen S3-Bucket zu Amazon S3 Glacier oder S3 Glacier Deep Archive (oder zu einer Speicherlösung, die die Glacier-Speicherklasse implementiert) durch die Lifecycle-Konfiguration dieses Buckets gesteuert.

Wenn Sie Objekte aus dem Cloud Storage Pool migrieren möchten, müssen Sie die entsprechende Lebenszykluskonfiguration im externen S3-Bucket erstellen und eine Speicherlösung verwenden, die die Glacier Speicherklasse implementiert und die S3 RestoreObject API unterstützt.

Angenommen, Sie möchten beispielsweise, dass alle Objekte, die von StorageGRID in den Cloud Storage Pool verschoben werden, sofort in Amazon S3 Glacier Storage überführt werden. Hierfür wird eine Lebenszykluskonfiguration auf dem externen S3-Bucket erstellt, die eine einzelne Aktion (**Transition**) wie folgt festlegt:

```
<LifecycleConfiguration>
  <Rule>
    <ID>Transition Rule</ID>
    <Filter>
       <Prefix></Prefix>
    </Filter>
    <Status>Enabled</Status>
    <Transition>
      <Days>0</Days>
      <StorageClass>GLACIER</StorageClass>
    </Transition>
  </Rule>
</LifecycleConfiguration>
```

Diese Regel würde alle Bucket-Objekte am Tag ihrer Erstellung (d. h. am Tag ihrer Verschiebung von StorageGRID in den Cloud Storage Pool) zu Amazon S3 Glacier überführen.

> Bei der Konfiguration des Lebenszyklus des externen Buckets sollten **Ablauf**-Aktionen niemals verwendet werden, um das Ablaufdatum von Objekten festzulegen. Ablauf-Aktionen führen dazu, dass das externe Speichersystem abgelaufene Objekte löscht. Wenn später versucht wird, auf ein abgelaufenes Objekt aus StorageGRID zuzugreifen, wird das gelöschte Objekt nicht gefunden.

Wenn Sie Objekte im Cloud Storage Pool in S3 Glacier Deep Archive (anstatt in Amazon S3 Glacier)

überführen möchten, geben Sie `<StorageClass>DEEP_ARCHIVE</StorageClass>` im Bucket-Lebenszyklus an. Es ist jedoch zu beachten, dass die `Expedited`-Speicherebene nicht zur Wiederherstellung von Objekten aus S3 Glacier Deep Archive verwendet werden kann.

Azure: Überlegungen zur Zugriffsebene

Beim Konfigurieren eines Azure-Speicherkontos kann die Standardzugriffsebene auf Hot oder Cool festgelegt werden. Beim Erstellen eines Speicherkontos zur Verwendung mit einem Cloud Storage Pool sollte die Hot-Ebene als Standardebene verwendet werden. Auch wenn StorageGRID die Ebene beim Verschieben von Objekten in den Cloud Storage Pool sofort auf Archive setzt, stellt die Verwendung der Standardeinstellung Hot sicher, dass keine Gebühr für die vorzeitige Löschung von Objekten aus der Cool-Ebene vor Ablauf der 30-tägigen Mindestaufbewahrungsfrist berechnet wird.

Azure: Lebenszyklusverwaltung wird nicht unterstützt

Die Azure Blob Storage-Lebenszyklusverwaltung sollte nicht für den Container verwendet werden, der mit einem Cloud Storage Pool genutzt wird. Lebenszyklusvorgänge könnten mit den Vorgängen des Cloud Storage Pools interferieren.

Verwandte Informationen

"Einen Cloud Storage Pool erstellen"

Cloud-Speicherpools und CloudMirror Replikation in StorageGRID

Zu Beginn der Nutzung von Cloud Storage Pools kann es hilfreich sein, die Gemeinsamkeiten und Unterschiede zwischen Cloud Storage Pools und dem StorageGRID CloudMirror Replikationsdienst zu verstehen.

	Cloud Storage Pool	CloudMirror Replikationsdienst
Was ist der Hauptzweck?	Dient als Archivziel. Die Objektkopie im Cloud Storage Pool kann die einzige Kopie des Objekts sein oder eine zusätzliche Kopie. Das heißt, anstatt zwei Kopien vor Ort zu behalten, kann eine Kopie innerhalb von StorageGRID und eine Kopie im Cloud Storage Pool aufbewahrt werden.	Ermöglicht einem Mandanten, Objekte automatisch von einem Bucket in StorageGRID (Quelle) in einen externen S3 Bucket (Ziel) zu replizieren. Erstellt eine unabhängige Kopie eines Objekts in einer unabhängigen S3 Infrastruktur.
Wie ist es aufgebaut?	Definiert auf die gleiche Weise wie Speicherpools, mithilfe des Grid Managers oder der Grid Management API. Kann als Speicherort in einer ILM-Regel ausgewählt werden. Während ein Speicherpool aus einer Gruppe von Storage Nodes besteht, wird ein Cloud Storage Pool über einen Remote-S3- oder Azure-Endpunkt (IP-Adresse, Anmeldeinformationen usw.) definiert.	Ein Mandantenbenutzer kann durch Definition eines CloudMirror-Endpunkts (IP-Adresse, Anmeldeinformationen usw.) mithilfe des Tenant Managers oder der S3-API "konfiguriert die CloudMirror Replikation" arbeiten. Nachdem der CloudMirror-Endpunkt eingerichtet wurde, kann jeder Bucket, der diesem Mandantenkonto gehört, so konfiguriert werden, dass er auf den CloudMirror-Endpunkt verweist.

	Cloud Storage Pool	CloudMirror Replikationsdienst
Wer ist für die Einrichtung verantwortlich?	Typischerweise verwaltet ein Grid-Administrator	Typischerweise ist ein Mieterbenutzer
Was ist das Ziel?	• Jede kompatible S3-Infrastruktur (einschließlich Amazon S3) • Azure Blob Archive Tier • Google Cloud Platform (GCP)	• Jede kompatible S3-Infrastruktur (einschließlich Amazon S3) • Google Cloud Platform (GCP)
Was führt dazu, dass Objekte an das Ziel verschoben werden?	Eine oder mehrere ILM-Regeln in den aktiven ILM-Richtlinien. Die ILM-Regeln definieren, welche Objekte StorageGRID in den Cloud Storage Pool verschiebt und wann die Objekte verschoben werden.	Der Vorgang des Einlesens eines neuen Objekts in einen Quell-Bucket, der mit einem CloudMirror Endpoint konfiguriert wurde. Objekte, die sich bereits vor der Konfiguration des Buckets mit dem CloudMirror Endpoint im Quell-Bucket befanden, werden nicht repliziert, es sei denn, sie werden geändert.
Wie werden Objekte abgerufen?	Anwendungen müssen Anfragen an StorageGRID stellen, um Objekte abzurufen, die in einen Cloud Storage Pool verschoben wurden. Wenn die einzige Kopie eines Objekts in den Archivspeicher verschoben wurde, verwaltet StorageGRID den Wiederherstellungsprozess, sodass das Objekt abgerufen werden kann.	Da die gespiegelte Kopie im Ziel-Bucket eine unabhängige Kopie ist, können Anwendungen das Objekt abrufen, indem sie Anfragen entweder an StorageGRID oder an das S3-Ziel senden. Beispielsweise kann CloudMirror Replikation verwendet werden, um Objekte an eine Partnerorganisation zu spiegeln. Der Partner kann mit eigenen Anwendungen Objekte direkt vom S3-Ziel lesen oder aktualisieren. Die Nutzung von StorageGRID ist nicht erforderlich.
Ist ein direktes Auslesen vom Ziel möglich?	Nein. Objekte, die in einen Cloud-Speicherpool verschoben werden, werden von StorageGRID verwaltet. Leseanfragen müssen an StorageGRID gerichtet werden (und StorageGRID ist für den Abruf aus dem Cloud-Speicherpool verantwortlich).	Ja, da die gespiegelte Kopie eine unabhängige Kopie ist.
Was passiert, wenn ein Objekt aus der Quelle gelöscht wird?	Das Objekt wird auch aus dem Cloud Storage Pool gelöscht.	Der Löschvorgang wird nicht repliziert. Ein gelöschtes Objekt existiert nicht mehr im StorageGRID Bucket, ist aber weiterhin im Ziel-Bucket vorhanden. Ebenso können Objekte im Ziel-Bucket gelöscht werden, ohne dass dies Auswirkungen auf die Quelle hat.

	Cloud Storage Pool	CloudMirror Replikationsdienst
Wie erfolgt der Zugriff auf Objekte nach einem Katastrophenfall (StorageGRID System nicht betriebsbereit)?	Ausgefallene StorageGRID Knoten müssen wiederhergestellt werden. Während dieses Vorgangs können Kopien replizierter Objekte mithilfe der Kopien im Cloud Storage Pool wiederhergestellt werden.	Die Objektkopien im CloudMirror Ziel sind unabhängig von StorageGRID, sodass auf sie direkt zugegriffen werden kann, bevor die StorageGRID Knoten wiederhergestellt sind.

Erstellen Sie einen Cloud Storage Pool in StorageGRID

Ein Cloud Storage Pool spezifiziert einen einzelnen externen Amazon S3-Bucket, einen anderen S3-kompatiblen Anbieter oder einen Azure Blob Storage-Container.

Beim Erstellen eines Cloud-Speicherpools werden der Name und der Speicherort des externen Buckets oder Containers angegeben, den StorageGRID zum Speichern von Objekten verwendet, der Cloud-Anbietertyp (Amazon S3/GCP oder Azure Blob Storage) sowie die Informationen, die StorageGRID für den Zugriff auf den externen Bucket oder Container benötigt.

StorageGRID validiert den Cloud-Speicherpool, sobald er gespeichert wird, daher muss sichergestellt sein, dass der im Cloud-Speicherpool angegebene Bucket oder Container existiert und erreichbar ist.

Bevor Sie beginnen

- Sie sind mit einem "unterstützte Webbrowser" beim Grid Manager angemeldet.
- Sie haben die "Erforderliche Zugriffsberechtigungen".
- Sie haben die "Überlegungen zu Cloud Storage Pools" überprüft.
- Der vom Cloud Storage Pool referenzierte externe Bucket oder Container existiert bereits, und Sie haben die Informationen zum Service-Endpunkt.
- Um auf den Bucket oder Container zuzugreifen, steht Ihnen die Kontoinformationen für den Authentifizierungstyp zur Auswahl.

Schritte

1. Wählen Sie **ILM** > **Speicherpools** > **Cloud Storage Pools**.
2. **Erstellen** auswählen und anschließend die folgenden Informationen eingeben:

Feld	Beschreibung
Name des Cloud Storage Pool	Ein Name, der den Cloud Storage Pool und seinen Zweck kurz beschreibt. Ein Name, der bei der Konfiguration von ILM-Regeln leicht zu identifizieren ist.

Feld	Beschreibung
Anbietertyp	Welcher Cloud-Anbieter für diesen Cloud Storage Pool verwendet wird: • **Amazon S3/GCP**: Diese Option gilt für einen Amazon S3, Commercial Cloud Services (C2S) S3, Google Cloud Platform (GCP) oder einen anderen S3-kompatiblen Anbieter. • **Azure Blob Storage**
Bucket oder Container	Der Name des externen S3-Buckets oder Azure-Containers. Dieser Wert kann nach dem Speichern des Cloud Storage Pools nicht mehr geändert werden.

3. Basierend auf Ihrer Auswahl des Anbietertyps sind die Service-Endpunktinformationen einzugeben.

Amazon S3/GCP

a. Für das Protokoll entweder HTTPS oder HTTP auswählen.

> HTTP-Verbindungen sollten nicht für sensible Daten verwendet werden.

b. Geben Sie den Hostnamen ein. Beispiel:

`s3-aws-region.amazonaws.com`

c. Wählen Sie den URL-Stil aus:

Option	Beschreibung
Automatische Erkennung	Es wird versucht, anhand der angegebenen Informationen automatisch zu erkennen, welcher URL-Stil verwendet werden soll. Wenn beispielsweise eine IP-Adresse angegeben wird, verwendet StorageGRID eine URL im Pfadstil. Diese Option sollte nur ausgewählt werden, wenn nicht bekannt ist, welcher spezifische Stil verwendet werden soll.
Virtuell gehosteter Stil	Eine virtual-hosted-style-URL kann verwendet werden, um auf den Bucket zuzugreifen. Virtual-hosted-style-URLs enthalten den Bucket-Namen als Teil des Domainnamens. Beispiel: `https://bucket-name.s3.company.com/key-name`
Pfadstil	Verwenden Sie eine URL im Pfadformat, um auf den Bucket zuzugreifen. URLs im Pfadformat enthalten den Bucket-Namen am Ende. Beispiel: `https://s3.company.com/bucket-name/key-name` **Hinweis:** Die Option „URL im Pfadstil“ wird nicht empfohlen und wird in einer zukünftigen Version von StorageGRID nicht mehr unterstützt.

d. Optional kann die Portnummer eingegeben oder der Standardport verwendet werden: 443 für HTTPS oder 80 für HTTP.

Azure Blob Storage

a. Geben Sie die URI für den Service-Endpunkt in einem der folgenden Formate ein.

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

Beispiel: `https://myaccount.blob.core.windows.net:443`

Wenn kein Port angegeben wird, wird standardmäßig Port 443 für HTTPS und Port 80 für HTTP verwendet.

4. Wählen Sie **Weiter**. Anschließend den Authentifizierungstyp auswählen und die erforderlichen Informationen für den Cloud Storage Pool Endpoint eingeben:

Zugangsschlüssel

Für Amazon S3/GCP oder andere S3-kompatible Anbieter

a. **Zugriffsschlüssel-ID**: Die Zugriffsschlüssel-ID für das Konto angeben, dem der externe Bucket gehört.
b. **Geheimer Zugriffsschlüssel**: Der geheime Zugriffsschlüssel ist einzugeben.

IAM Roles Anywhere

Für den AWS IAM Roles Anywhere Dienst

StorageGRID verwendet den AWS Security Token Service (STS), um dynamisch ein kurzlebiges Token zum Zugriff auf AWS-Ressourcen zu generieren.

a. **AWS IAM Roles Anywhere Region**: Die Region für den Cloud Storage Pool auswählen. Zum Beispiel `us-east-1`.
b. **Trust anchor URN**: Geben Sie die URN des Trust Anchors ein, der Anforderungen für kurzlebige STS-Anmeldeinformationen validiert. Kann eine Root- oder Intermediate-CA sein.
c. **Profil-URN**: Geben Sie die URN des IAM Roles Anywhere Profils ein, das die Rollen auflistet, die von allen vertrauenswürdigen Personen übernommen werden können.
d. **Rollen-URN**: Die URN der IAM-Rolle eingeben, die von jeder vertrauenswürdigen Person übernommen werden kann.
e. **Sitzungsdauer**: Die Dauer der temporären Sicherheitsanmeldeinformationen und der Rollensitzung eingeben. Mindestens 15 Minuten und höchstens 12 Stunden eingeben.
f. **Server-CA-Zertifikat** (optional): Ein oder mehrere vertrauenswürdige CA-Zertifikate im PEM-Format zur Überprüfung des IAM Roles Anywhere Servers. Wenn dieses Zertifikat weggelassen wird, findet keine Überprüfung des Servers statt.
g. **End-entity certificate**: Der öffentliche Schlüssel des vom Trust Anchor signierten X509-Zertifikats im PEM-Format. AWS IAM Roles Anywhere verwendet diesen Schlüssel, um ein STS-Token auszustellen.
h. **Privater Schlüssel der End-Entity**: Der private Schlüssel für das End-Entity-Zertifikat.

CAP (C2S-Zugangsportal)

Für Commercial Cloud Services (C2S) S3-Service

a. **URL für temporäre Anmeldeinformationen**: Die vollständige URL, die StorageGRID verwendet, um temporäre Anmeldeinformationen vom CAP-Server abzurufen, einschließlich aller erforderlichen und optionalen API-Parameter, die Ihrem C2S-Konto zugewiesen sind.
b. **Server-CA-Zertifikat**: **Durchsuchen** auswählen und das CA-Zertifikat hochladen, das StorageGRID zur Verifizierung des CAP-Servers verwendet. Das Zertifikat muss PEM-kodiert und von einer geeigneten staatlichen Zertifizierungsstelle (CA) ausgestellt sein.
c. **Clientzertifikat**: **Durchsuchen** auswählen und das Zertifikat hochladen, das StorageGRID zur Identifizierung gegenüber dem CAP-Server verwendet. Das Clientzertifikat muss PEM-kodiert sein, von einer geeigneten Government Certificate Authority (CA) ausgestellt sein und Zugriff auf Ihr C2S-Konto haben.
d. **Privater Client-Schlüssel**: **Durchsuchen** auswählen und den PEM-kodierten privaten Schlüssel für das Client-Zertifikat hochladen.
e. Wenn der private Schlüssel des Clients verschlüsselt ist, ist die Passphrase zum Entschlüsseln

des privaten Schlüssels des Clients einzugeben. Andernfalls bleibt das Feld **Passphrase für den privaten Schlüssel des Clients** leer.

> Wenn das Clientzertifikat verschlüsselt wird, ist das herkömmliche Format für die Verschlüsselung zu verwenden. Das PKCS #8-Verschlüsselungsformat wird nicht unterstützt.

Azure Blob Storage

Nur für Azure Blob Storage, nur Shared Key

a. **Kontoname**: Der Name des Speicherkontos, dem der externe Container gehört, wird eingegeben.
b. **Kontoschlüssel**: Der geheime Schlüssel für das Speicherkonto wird eingegeben.

Diese Werte sind im Azure-Portal zu finden.

Anonym

Es werden keine weiteren Informationen benötigt.

5. Wählen Sie **Weiter**. Anschließend die gewünschte Art der Serververifizierung auswählen:

Option	Beschreibung
Root-CA-Zertifikate im Storage Node OS verwenden	Die auf dem Betriebssystem installierten Grid-CA-Zertifikate sichern die Verbindungen.
Benutzerdefiniertes CA-Zertifikat verwenden	Verwenden Sie ein benutzerdefiniertes CA-Zertifikat. **Durchsuchen** auswählen und das PEM-kodierte Zertifikat hochladen.
Zertifikat nicht überprüfen	Die Auswahl dieser Option bedeutet, dass TLS-Verbindungen zum Cloud-Speicherpool nicht sicher sind.

6. **Speichern** auswählen.

   Wenn Sie einen Cloud-Speicherpool speichern, führt StorageGRID Folgendes aus:

   - Prüft, ob der Bucket oder Container und der Service-Endpunkt existieren und ob sie mit den von Ihnen angegebenen Anmeldeinformationen erreichbar sind.
   - Schreibt eine Markierungsdatei in den Bucket oder Container, um ihn als Cloud Storage Pool zu kennzeichnen. Entfernen Sie diese Datei, die den Namen `x-ntap-sgws-cloud-pool-uuid` trägt, niemals.

     Schlägt die Validierung des Cloud Storage Pool fehl, erhalten Sie eine Fehlermeldung, die den Grund für den Fehler erläutert. Beispielsweise kann ein Fehler gemeldet werden, wenn ein Zertifikatsfehler vorliegt oder der von Ihnen angegebene Bucket oder Container noch nicht existiert.

7. Wenn ein Fehler auftritt, siehe die "Anleitung zur Fehlerbehebung bei Cloud Storage Pools", beheben Sie eventuelle Probleme und versuchen Sie anschließend erneut, den Cloud Storage Pool zu speichern.

Details zum Cloud Storage Pool in StorageGRID anzeigen

Sie können die Details eines Cloud Storage Pool einsehen, um festzustellen, wo er verwendet wird und welche Knoten und Speicherklassen enthalten sind.

Bevor Sie beginnen

- Sie sind mit einem "unterstützte Webbrowser" beim Grid Manager angemeldet.
- Du hast "spezifische Zugriffsberechtigungen".

Schritte

1. Wählen Sie **ILM** > **Speicherpools** > **Cloud Storage Pools**.

   Die Tabelle „Cloud Storage Pools“ enthält die folgenden Informationen für jeden Cloud Storage Pool, der Storage Nodes umfasst:

   - **Name**: Der eindeutige Anzeigename des Pools.
   - **URI**: Der Uniform Resource Identifier des Cloud Storage Pools.
   - **Anbietertyp**: Welcher Cloud-Provider wird für diesen Cloud Storage Pool verwendet.
   - **Container**: Der Name des Buckets, der für den Cloud Storage Pool verwendet wird.
   - **ILM-Nutzung**: Wie der Pool aktuell genutzt wird. Ein Cloud Storage Pool kann ungenutzt sein oder in einer oder mehreren ILM-Regeln, Erasure-Coding-Profilen oder beidem verwendet werden.
   - **Letzter Fehler**: Der letzte Fehler, der bei einer Integritätsprüfung dieses Cloud Storage Pools festgestellt wurde.

2. Details zu einem bestimmten Cloud Storage Pool werden angezeigt, wenn dessen Name ausgewählt wird.

   Die Detailseite für den Pool wird angezeigt.

3. Auf der Registerkarte **Authentifizierung** werden der Authentifizierungstyp für diesen Cloud Storage Pool angezeigt und die Authentifizierungsdetails können bearbeitet werden.
4. Auf der Registerkarte **Serververifizierung** sind Informationen zu Verifizierungsdetails, die Möglichkeit zur Bearbeitung der Verifizierung, zum Herunterladen eines neuen Zertifikats oder zum Kopieren der Zertifikat-PEM verfügbar.
5. Die Registerkarte **ILM usage** zeigt an, ob der Cloud Storage Pool aktuell in ILM-Regeln oder Erasure-Coding-Profilen verwendet wird.
6. Optional kann die **ILM-Regelseite** aufgerufen werden, um "Informationen zu allen Regeln erhalten und diese verwalten" zu verwenden, die den Cloud Storage Pool nutzen.

Bearbeiten Sie einen Cloud Storage Pool in StorageGRID

Sie können einen Cloud Storage Pool bearbeiten, um seinen Namen, den Service-Endpunkt oder andere Details zu ändern; der S3-Bucket oder der Azure-Container für einen Cloud Storage Pool kann jedoch nicht geändert werden.

Bevor Sie beginnen

- Sie sind mit einem "unterstützte Webbrowser" beim Grid Manager angemeldet.
- Du hast "spezifische Zugriffsberechtigungen".

- Sie haben die "Überlegungen zu Cloud Storage Pools" überprüft.

Schritte

1. Wählen Sie **ILM** > **Speicherpools** > **Cloud Storage Pools**.

   Die Tabelle „Cloud Storage Pools“ listet die vorhandenen Cloud Storage Pools auf.

2. Aktivieren Sie das Kontrollkästchen für den Cloud Storage Pool, den Sie bearbeiten möchten, und wählen Sie dann **Actions** > **Edit**.

   Alternativ den Namen des Cloud Storage Pool auswählen und anschließend **Bearbeiten** wählen.

3. Bei Bedarf können der Name des Cloud Storage Pool, der Service-Endpunkt, die Authentifizierungsdaten oder die Methode zur Zertifikatsüberprüfung geändert werden.

   > Sie können den Anbietertyp, den S3-Bucket oder den Azure-Container für einen Cloud Storage Pool nicht ändern.

   Wenn zuvor ein Server- oder Clientzertifikat hochgeladen wurde, lässt sich die **Zertifikatdetails** -Akkordeonleiste erweitern, um das aktuell verwendete Zertifikat anzuzeigen.

4. **Speichern** auswählen.

   Wenn ein Cloud-Speicherpool gespeichert wird, validiert StorageGRID, dass der Bucket oder Container und der Service-Endpunkt existieren und dass sie mit den angegebenen Anmeldeinformationen erreichbar sind.

   Schlägt die Validierung des Cloud Storage Pool fehl, wird eine Fehlermeldung angezeigt. Beispielsweise könnte eine Fehlermeldung erscheinen, wenn ein Zertifikatsfehler vorliegt.

   Siehe die Anweisungen für "Fehlerbehebung bei Cloud Storage Pools", das Problem beheben und anschließend erneut versuchen, den Cloud Storage Pool zu speichern.

Entfernen Sie einen Cloud-Speicherpool in StorageGRID

Sie können einen Cloud Storage Pool entfernen, wenn er in einer ILM-Regel nicht verwendet wird und keine Objektdaten enthält.

Bevor Sie beginnen

- Sie sind mit einem "unterstützte Webbrowser" beim Grid Manager angemeldet.
- Sie haben die "Erforderliche Zugriffsberechtigungen".

Bei Bedarf kann ILM verwendet werden, um Objektdaten zu verschieben.

Enthält der zu entfernende Cloud Storage Pool Objektdaten, muss ILM verwendet werden, um die Daten an einen anderen Speicherort zu verschieben. Beispielsweise können die Daten auf Storage Nodes in Ihrem Grid oder in einen anderen Cloud Storage Pool verschoben werden.

Schritte

1. Wählen Sie **ILM** > **Speicherpools** > **Cloud Storage Pools**.
2. Sehen Sie in der Tabelle in der Spalte „ILM-Nutzung“ nach, um festzustellen, ob der Cloud Storage Pool

entfernt werden kann.

Ein Cloud Storage Pool kann nicht entfernt werden, wenn er in einer ILM-Regel oder in einem Erasure-Coding-Profil verwendet wird.

3. Wenn der Cloud Storage Pool verwendet wird, ***cloud storage pool name*** > **ILM usage** auswählen.
4. "Jede ILM-Regel klonen"derzeit Objekte im Cloud Storage Pool platziert, den Sie entfernen möchten.
5. Bestimmen Sie, wohin die vorhandenen Objekte verschoben werden sollen, die von jeder geklonten Regel verwaltet werden.

   Sie können einen oder mehrere Speicherpools oder einen anderen Cloud Storage Pool verwenden.

6. Bearbeiten Sie jede der geklonten Regeln.

   Im zweiten Schritt des Assistenten zum Erstellen von ILM-Regeln wird der neue Speicherort im Feld **Kopien bei** ausgewählt.

7. "Eine neue ILM Richtlinie erstellen" und jede der alten Regeln durch eine geklonte Regel ersetzen.
8. Die neue Richtlinie wird aktiviert.
9. Warten Sie, bis ILM die Objekte aus dem Cloud Storage Pool entfernt und am neuen Speicherort abgelegt hat.

Cloud Storage Pool löschen

Wenn der Cloud Storage Pool leer ist und in keiner ILM-Regel verwendet wird, kann er gelöscht werden.

Bevor Sie beginnen

- Sie haben alle ILM-Regeln entfernt, die möglicherweise den Pool verwendet haben.
- Sie haben bestätigt, dass der S3-Bucket oder der Azure-Container keine Objekte enthält.

  Beim Versuch, einen Cloud Storage Pool zu entfernen, der Objekte enthält, tritt ein Fehler auf. Siehe "Fehlerbehebung bei Cloud Storage Pools".

> ⓘ Wenn Sie einen Cloud-Speicherpool erstellen, schreibt StorageGRID eine Markierungsdatei in den Bucket oder Container, um ihn als Cloud-Speicherpool zu kennzeichnen. Entfernen Sie diese Datei mit dem Namen `x-ntap-sgws-cloud-pool-uuid` nicht.

Schritte

1. Wählen Sie **ILM** > **Speicherpools** > **Cloud Storage Pools**.
2. Wenn in der Spalte „ILM-Nutzung“ angezeigt wird, dass Cloud Storage Pool nicht verwendet wird, das Kontrollkästchen auswählen.
3. **Aktionen** > **Entfernen** auswählen.
4. Wählen Sie **OK**.

Fehlerbehebung bei Cloud Storage Pools in StorageGRID

Diese Schritte zur Fehlerbehebung unterstützen bei der Behebung von Fehlern, die beim Erstellen, Bearbeiten oder Löschen eines Cloud Storage Pool auftreten können.

Feststellen, ob ein Fehler aufgetreten ist

StorageGRID führt für jeden Cloud Storage Pool eine einfache Integritätsprüfung durch, indem das bekannte Objekt `x-ntap-sgws-cloud-pool-uuid` ausgelesen wird, um sicherzustellen, dass auf den Cloud Storage Pool zugegriffen werden kann und er ordnungsgemäß funktioniert. Wenn StorageGRID einen Fehler am Endpoint feststellt, wird von jedem Storage Node aus jede Minute eine Integritätsprüfung durchgeführt. Sobald der Fehler behoben ist, werden die Integritätsprüfungen gestoppt. Wird bei einer Integritätsprüfung ein Problem erkannt, erscheint eine Meldung in der Spalte „Last error“ der Tabelle „Cloud Storage Pools“ auf der Seite „Storage pools“.

Die Tabelle zeigt den zuletzt erkannten Fehler für jeden Cloud Storage Pool und gibt an, wie lange der Fehler zurückliegt.

Zusätzlich wird eine Warnung wegen eines **Verbindungsfehlers im Cloud Storage Pool** ausgelöst, wenn die Integritätsprüfung einen oder mehrere neue Cloud Storage Pool-Fehler innerhalb der letzten 5 Minuten feststellt. Bei Erhalt einer E-Mail-Benachrichtigung zu dieser Warnung kann die Seite „Speicherpools“ aufgerufen werden (Auswahl von **ILM** > **Speicherpools**), die Fehlermeldungen in der Spalte „Letzter Fehler“ können überprüft werden, und die unten stehenden Richtlinien zur Fehlerbehebung bieten weitere Informationen.

Überprüfung, ob ein Fehler behoben wurde

Nachdem alle zugrunde liegenden Probleme behoben wurden, kann festgestellt werden, ob der Fehler behoben ist. Auf der Seite Cloud Storage Pool den Endpunkt auswählen und **Fehler löschen** wählen. Eine Bestätigungsmeldung zeigt an, dass StorageGRID den Fehler für den Cloud Storage Pool gelöscht hat.

Wenn das zugrunde liegende Problem behoben ist, wird die Fehlermeldung nicht mehr angezeigt. Wenn das zugrunde liegende Problem jedoch nicht behoben wurde (oder ein anderer Fehler auftritt), wird die Fehlermeldung innerhalb weniger Minuten in der Spalte Last error angezeigt.

Fehler: Integritätsprüfung fehlgeschlagen. Fehler vom Endpunkt

Dieser Fehler kann auftreten, wenn die S3 Object Lock-Funktion mit Standardaufbewahrung für Ihren Amazon S3-Bucket aktiviert wird, nachdem dieser Bucket für einen Cloud Storage Pool verwendet wurde. Dieser Fehler tritt auf, wenn der PUT-Vorgang keinen HTTP-Header mit einem Nutzlast-Prüfsumme-Wert wie `Content-MD5` enthält. Dieser Header-Wert ist von AWS für PUT-Vorgänge in Buckets mit aktivierter S3 Object Lock-Funktion erforderlich.

Um dieses Problem zu beheben, die Schritte in "Bearbeiten eines Cloud Storage Pools" befolgen, ohne Änderungen vorzunehmen. Dadurch wird die Validierung der Cloud Storage Pool Konfiguration ausgelöst, die das S3 Object Lock Flag in einer Cloud Storage Pool Endpunktkonfiguration automatisch erkennt und aktualisiert.

Fehler: Dieser Cloud Storage Pool enthält unerwartete Inhalte

Dieser Fehler kann auftreten, wenn Sie versuchen, einen Cloud Storage Pool zu erstellen, zu bearbeiten oder zu löschen. Dieser Fehler tritt auf, wenn der Bucket oder Container die `x-ntap-sgws-cloud-pool-uuid` Markerdatei enthält, diese Datei jedoch kein Metadatenfeld mit der erwarteten UUID aufweist.

Normalerweise wird dieser Fehler nur angezeigt, wenn Sie einen neuen Cloud Storage Pool erstellen und eine andere Instanz von StorageGRID bereits denselben Cloud Storage Pool verwendet.

Einer dieser Schritte kann zur Behebung des Problems beitragen:

- Wenn Sie einen neuen Cloud Storage Pool konfigurieren und der Bucket die `x-ntap-sgws-cloud-pool-uuid` Datei und zusätzliche Objektschlüssel ähnlich dem folgenden Beispiel enthält, sollte ein neuer Bucket erstellt und stattdessen dieser neue Bucket verwendet werden.

  Beispiel für einen zusätzlichen Objektschlüssel: `my-bucket.3E64CF2C-B74D-4B7D-AFE7-AD28BC18B2F6.1727326606730410`

- Wenn die `x-ntap-sgws-cloud-pool-uuid` Datei das einzige Objekt im Bucket ist, sollte diese Datei gelöscht werden.

Falls diese Schritte in Ihrem Fall nicht zutreffen, kontaktieren Sie den Support.

Fehler: Cloud Storage Pool konnte nicht erstellt oder aktualisiert werden. Fehler vom Endpoint

Dieser Fehler kann unter folgenden Umständen auftreten:

- Wenn versucht wird, einen Cloud Storage Pool zu erstellen oder zu bearbeiten.
- Wenn während der Konfiguration eines neuen Cloud-Speicherpools eine nicht unterstützte Plattform-, Authentifizierungs- oder Protokollkombination mit S3 Object Lock ausgewählt wird. Siehe "Überlegungen zu Cloud Storage Pools".

Dieser Fehler weist darauf hin, dass ein Verbindungs- oder Konfigurationsproblem StorageGRID daran hindert, in den Cloud Storage Pool zu schreiben.

Zur Behebung des Problems sollte die Fehlermeldung des Endpunkts überprüft werden.

- Wenn die Fehlermeldung `Get *url*: EOF` enthält, ist zu prüfen, ob der für den Cloud Storage Pool verwendete Service-Endpunkt nicht HTTP für einen Container oder Bucket verwendet, der HTTPS erfordert.
- Wenn die Fehlermeldung `Get *url*: net/http: request canceled while waiting for connection` enthält, prüfen Sie, ob die Netzwerkkonfiguration den Storage Nodes den Zugriff auf den für den Cloud Storage Pool verwendeten Service-Endpunkt ermöglicht.
- Falls der Fehler auf eine nicht unterstützte Plattform, Authentifizierung oder ein nicht unterstütztes Protokoll zurückzuführen ist, sollte zu einer unterstützten Konfiguration mit S3 Object Lock gewechselt und anschließend versucht werden, den neuen Cloud Storage Pool erneut zu speichern.
- Bei allen anderen Endpunktfehlermeldungen können eine oder mehrere der folgenden Maßnahmen in Betracht gezogen werden:
  - Erstellen Sie einen externen Container oder Bucket mit demselben Namen, den Sie für den Cloud Storage Pool eingegeben haben, und versuchen Sie erneut, den neuen Cloud Storage Pool zu speichern.
  - Korrigieren Sie den Container- oder Bucket-Namen, den Sie für den Cloud Storage Pool angegeben haben, und versuchen Sie erneut, den neuen Cloud Storage Pool zu speichern.

Fehler: CA-Zertifikat konnte nicht analysiert werden

Dieser Fehler kann auftreten, wenn Sie versuchen, einen Cloud Storage Pool zu erstellen oder zu bearbeiten. Der Fehler tritt auf, wenn StorageGRID das von Ihnen beim Konfigurieren des Cloud Storage Pool eingegebene Zertifikat nicht parsen konnte.

Zur Behebung des Problems sollte das bereitgestellte CA-Zertifikat auf Fehler überprüft werden.

Fehler: Ein Cloud Storage Pool mit dieser ID wurde nicht gefunden

Dieser Fehler kann auftreten, wenn Sie versuchen, einen Cloud Storage Pool zu bearbeiten oder zu löschen. Dieser Fehler tritt auf, wenn der Endpoint eine 404-Antwort zurückgibt, was Folgendes bedeuten kann:

- Die für den Cloud Storage Pool verwendeten Anmeldeinformationen haben keine Leseberechtigung für den Bucket.
- Der für den Cloud Storage Pool verwendete Bucket enthält die `x-ntap-sgws-cloud-pool-uuid` Markerdatei nicht.

Führen Sie einen oder mehrere dieser Schritte aus, um das Problem zu beheben:

- Es sollte überprüft werden, ob der Benutzer, der dem konfigurierten Zugriffsschlüssel zugeordnet ist, über die erforderlichen Berechtigungen verfügt.
- Den Cloud Storage Pool mit Anmeldeinformationen bearbeiten, die über die erforderlichen Berechtigungen verfügen.
- Wenn die Berechtigungen korrekt sind, sollte der Support kontaktiert werden.

Fehler: Der Inhalt des Cloud-Speicherpools konnte nicht überprüft werden. Fehler vom Endpunkt

Dieser Fehler kann auftreten, wenn Sie versuchen, einen Cloud Storage Pool zu löschen. Dieser Fehler weist darauf hin, dass ein Verbindungs- oder Konfigurationsproblem StorageGRID daran hindert, den Inhalt des Cloud Storage Pool Buckets zu lesen.

Zur Behebung des Problems sollte die Fehlermeldung des Endpunkts überprüft werden.

Fehler: In diesem Bucket wurden bereits Objekte platziert

Dieser Fehler kann auftreten, wenn Sie versuchen, einen Cloud Storage Pool zu löschen. Ein Cloud Storage Pool kann nicht gelöscht werden, wenn er Daten enthält, die von ILM dorthin verschoben wurden, Daten, die sich vor der Konfiguration des Cloud Storage Pools im Bucket befanden, oder Daten, die nach der Erstellung des Cloud Storage Pools von einer anderen Quelle in den Bucket eingefügt wurden.

Führen Sie einen oder mehrere dieser Schritte aus, um das Problem zu beheben:

- Die Anweisungen zum Zurückverschieben von Objekten nach StorageGRID finden sich unter „Lebenszyklus eines Cloud-Speicherpool-Objekts“.
- Wenn Sie sicher sind, dass die verbleibenden Objekte nicht von ILM im Cloud Storage Pool abgelegt wurden, die Objekte manuell aus dem Bucket löschen.

> ⓘ Löschen Sie niemals manuell Objekte aus einem Cloud-Speicherpool, die möglicherweise von ILM dort abgelegt wurden. Wenn später versucht wird, auf ein manuell gelöschtes Objekt aus StorageGRID zuzugreifen, wird das gelöschte Objekt nicht gefunden.

Fehler: Beim Versuch, den Cloud-Speicherpool zu erreichen, ist beim Proxy ein externer Fehler aufgetreten.

Dieser Fehler kann auftreten, wenn ein nicht transparenter Speicherproxy zwischen den Storage Nodes und dem externen S3-Endpunkt verwendet wird, der für den Cloud Storage Pool genutzt wird. Dieser Fehler tritt auf, wenn der externe Proxyserver den Cloud Storage Pool-Endpunkt nicht erreichen kann. Beispielsweise

kann der DNS-Server den Hostnamen möglicherweise nicht auflösen oder es liegt ein externes Netzwerkproblem vor.

Führen Sie einen oder mehrere dieser Schritte aus, um das Problem zu beheben:

- Die Einstellungen für den Cloud Storage Pool (**ILM** > **Storage pools**) prüfen.
- Die Netzwerkkonfiguration des Proxyservers prüfen.

Fehler: Das X.509-Zertifikat befindet sich außerhalb des Gültigkeitszeitraums.

Dieser Fehler kann auftreten, wenn Sie versuchen, einen Cloud Storage Pool zu löschen. Dieser Fehler tritt auf, wenn die Authentifizierung ein X.509-Zertifikat erfordert, um sicherzustellen, dass der richtige externe Cloud Storage Pool validiert wird und der externe Pool leer ist, bevor die Cloud Storage Pool Konfiguration gelöscht wird.

Folgende Schritte können zur Behebung des Problems unternommen werden:

- Das für die Authentifizierung im Cloud Storage Pool konfigurierte Zertifikat wird aktualisiert.
- Stellen Sie sicher, dass alle Warnungen zum Ablauf von Zertifikaten in diesem Cloud Storage Pool behoben sind.

Verwandte Informationen

"Lebenszyklus eines Cloud Storage Pool-Objekts"