Verwendung Von Cloud Storage Pools

StorageGRID

NetApp
March 12, 2025

Inhalt

Verwendung Von Cloud Storage Pools

Was ist ein Cloud-Storage-Pool?

In einem Cloud Storage Pool können Sie ILM verwenden, um Objektdaten aus Ihrem StorageGRID System zu verschieben. Beispielsweise können Sie selten genutzte Objekte auf kostengünstigeren Cloud-Storage verschieben, wie z. B. Amazon S3 Glacier, S3 Glacier Deep Archive, Google Cloud oder die Archiv-Zugriffs-Tier in Microsoft Azure Blob Storage. Alternativ möchten Sie auch ein Cloud-Backup von StorageGRID Objekten beibehalten, um die Disaster Recovery zu verbessern.

Aus einer ILM-Perspektive ähnelt ein Cloud-Storage-Pool einem Storage-Pool. Um Objekte an beiden Standorten zu speichern, wählen Sie den Pool aus, wenn Sie die Anweisungen zur Platzierung einer ILM-Regel erstellen. Während Storage-Pools 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-Speicherpools und zeigt die grundlegenden Ähnlichkeiten und Unterschiede.

	Storage-Pool	**Cloud-Storage-Pool**
Wie wird sie erstellt?	Verwenden der Option **ILM** > **Storage Pools** im Grid Manager.	Verwenden der Option **ILM** > **Speicherpools** > **Cloud-Speicherpools** im Grid Manager. Sie müssen den externen Bucket oder Container einrichten, bevor Sie den Cloud Storage-Pool erstellen können.
Wie viele Pools können Sie erstellen?	Unbegrenzt.	Bis zu 10.

	Storage-Pool	Cloud-Storage-Pool
Wo werden Objekte gespeichert ?	Auf einem oder mehreren Storage-Nodes innerhalb von StorageGRID.	In einem Amazon S3-Bucket, Azure Blob-Storage-Container oder Google Cloud, der außerhalb des StorageGRID-Systems liegt Wenn der Cloud Storage Pool ein Amazon S3-Bucket ist: • Optional kann ein Bucket-Lebenszyklus konfiguriert werden, um Objekte auf kostengünstigen Langzeit-Storage wie Amazon S3 Glacier oder S3 Glacier Deep Archive zu verschieben. Das externe Speichersystem muss die Glacier Storage-Klasse und die S3 RestoreObject API unterstützen. • Sie können Cloud-Storage-Pools zur Verwendung mit AWS Commercial Cloud Services (C2S) erstellen, die die AWS Secret Region unterstützen. Wenn der Cloud-Storage-Pool ein Azure Blob-Storage-Container ist, überträgt StorageGRID das Objekt auf die Archiv-Tier. **Hinweis:** im Allgemeinen sollten Sie Azure Blob Storage-Lifecycle-Management nicht für den Container konfigurieren, der für einen Cloud-Speicherpool verwendet wird. RestoreObject-Vorgänge für Objekte im Cloud-Storage-Pool können vom konfigurierten Lebenszyklus beeinflusst werden.
Welche Kontrollen steuern die Objektplatzierung?	Eine ILM-Regel in den aktiven ILM-Richtlinien.	Eine ILM-Regel in den aktiven ILM-Richtlinien.
Welche Datenschutzmethode wird verwendet?	Replizierung oder Erasure Coding:	Replizierung:
Wie viele Kopien jedes Objekts sind erlaubt?	Mehrere:	Eine Kopie im Cloud-Storage-Pool und optional eine oder mehrere Kopien in StorageGRID. **Hinweis:** ein Objekt kann zu keinem Zeitpunkt in mehr als einem Cloud-Speicherpool gespeichert werden.
Worin liegen die Vorteile?	Objekte sind jederzeit schnell abrufbar.	Kostengünstiger Storage: **Hinweis**: FabricPool-Daten können nicht in Cloud-Speicherpools verschoben werden.

Lebenszyklus eines Cloud-Storage-Pool-Objekts

Überprüfen Sie vor der Implementierung von Cloud-Storage-Pools den Lebenszyklus der

Objekte, die in jedem Typ von Cloud-Storage-Pool gespeichert sind.

S3: Lebenszyklus eines Cloud-Storage-Pool-Objekts

In den Schritten werden die Lebenszyklusphasen eines Objekts beschrieben, das in einem S3-Cloud-Storage-Pool gespeichert ist.

> ⓘ „Glacier“ bezieht sich sowohl auf die Storage-Klasse von Glacier als auch auf die Storage-Klasse von Glacier Deep Archive. Eine Ausnahme bildet dabei die Storage-Klasse Glacier Deep Archive, die die Restore-Ebene mit Express nicht unterstützt. Nur Bulk- oder Standard-Abruf wird unterstützt.

> ⓘ Die Google Cloud Platform (GCP) unterstützt den Abruf von Objekten aus langfristigem Storage ohne EINE WIEDERHERSTELLUNG NACH DER WIEDERHERSTELLUNG.

1. **Objekt gespeichert in StorageGRID**

   Zum Starten des Lebenszyklus speichert eine Client-Applikation ein Objekt in StorageGRID.

2. **Objekt in 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 vom Cloud-Storage-Pool angegebenen externen S3-Bucket.
   - Wenn das Objekt in den S3-Cloud-Storage-Pool verschoben wurde, kann die Client-Applikation es mithilfe einer S3-GetObject-Anforderung von StorageGRID abrufen, es sei denn, das Objekt wurde in Glacier Storage verschoben.
3. **Objekt ist auf Glacier umgestiegen (nicht-Retrieable-Zustand)**
   - Optional kann das Objekt auf Glacier Storage verschoben werden. Der externe S3-Bucket verwendet beispielsweise möglicherweise Lifecycle-Konfigurationen, um ein Objekt sofort oder nach einigen Tagen in Glacier Storage zu verschieben.

     > ⓘ Wenn Sie Objekte überführen möchten, müssen Sie eine Lifecycle-Konfiguration für den externen S3-Bucket erstellen. Außerdem müssen Sie eine Storage-Lösung verwenden, die die Glacier Storage-Klasse implementiert und die S3 RestoreObject API unterstützt.

   - Während des Übergangs kann die Client-Anwendung eine S3-HeadObject-Anforderung verwenden, um den Status des Objekts zu überwachen.
4. **Objekt vom Glacier-Speicher wiederhergestellt**

   Wenn ein Objekt in Glacier Storage migriert wurde, kann die Client-Applikation eine Anfrage zu S3 RestoreObject senden, um eine abrufbare Kopie im S3-Cloud-Storage-Pool wiederherzustellen. Die Anfrage gibt an, wie viele Tage die Kopie im Cloud Storage Pool und auf die Datenzugriffsebene für den Wiederherstellungsvorgang (Expedited, Standard oder Bulk) verfügbar sein soll. Wenn das Ablaufdatum der abrufbaren Kopie erreicht ist, wird die Kopie automatisch in einen nicht aufrufbaren Zustand zurückgeführt.

   > ⓘ Wenn innerhalb von StorageGRID auch eine oder mehrere Kopien des Objekts auf Storage-Nodes vorhanden sind, muss das Objekt über eine Wiederherstellungs-Objekt-Anforderung von Glacier nicht wiederhergestellt werden. Stattdessen kann die lokale Kopie mithilfe einer GetObject-Anforderung direkt abgerufen werden.

5. **Objekt abgerufen**

   Nachdem ein Objekt wiederhergestellt wurde, kann die Client-Anwendung eine GetObject-Anforderung zum Abrufen des wiederhergestellten Objekts ausgeben.

Azure: Lebenszyklus eines Cloud-Storage-Pool-Objekts

In den Schritten werden die Lebenszyklusphasen eines Objekts beschrieben, das in einem Azure Cloud Storage-Pool gespeichert ist.

1. **Objekt gespeichert in StorageGRID**

   Zum Starten des Lebenszyklus speichert eine Client-Applikation ein Objekt in StorageGRID.

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

   Wenn das Objekt einer ILM-Regel entspricht, 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 Archivebene (nicht-Retrieable-Status)** umgestiegen

   Unmittelbar nach dem Verschieben des Objekts in den Azure Cloud Storage Pool überträgt StorageGRID das Objekt automatisch auf die Azure Blob Storage-Archivebene.

4. **Objekt vom Archiv Tier** wiederhergestellt

   Wenn ein Objekt in die Archivierungs-Tier migriert wurde, kann die Client-Applikation eine Anfrage für S3-Wiederherstellungs-Objekt ausgeben, um eine abrufbare Kopie im Azure Cloud-Storage-Pool wiederherzustellen.

   Wenn StorageGRID das RestoreObject empfängt, wechselt es das Objekt vorübergehend in die Cool-Tier des Azure Blob-Speichers. Sobald das Ablaufdatum in der Anfrage zum Wiederherstellungobjekt erreicht ist, wechselt StorageGRID das Objekt zurück in die Archiv-Tier.

   > Wenn eine oder mehrere Kopien des Objekts auch auf Speicherknoten innerhalb von StorageGRID vorhanden sind, muss das Objekt nicht über die Zugriffsebene Archiv wiederhergestellt werden, indem eine Anforderung für RestoreObject ausgegeben wird. Stattdessen kann die lokale Kopie mithilfe einer GetObject-Anforderung direkt abgerufen werden.

5. **Objekt abgerufen**

   Nachdem ein Objekt im Azure Cloud Storage Pool wiederhergestellt wurde, kann die Client-Anwendung eine GetObject-Anforderung zum Abrufen des wiederhergestellten Objekts ausgeben.

Verwandte Informationen

"S3-REST-API VERWENDEN"

Wann sollten Sie Cloud Storage Pools nutzen

Mit Cloud Storage Pools können Sie Daten an einem externen Ort sichern oder per

Tiering übertragen. Darüber hinaus können Daten in mehreren Clouds gesichert oder per Tiering verschoben werden.

Backup von StorageGRID Daten an einem externen Speicherort

Sie können einen Cloud-Speicherpool verwenden, um StorageGRID Objekte an einem externen Ort zu sichern.

Wenn der Zugriff auf die Kopien in StorageGRID nicht möglich ist, können die Objektdaten im Cloud-Storage-Pool für Client-Anforderungen verwendet werden. Möglicherweise müssen Sie jedoch eine Anfrage für S3 RestoreObject ausgeben, um auf die Backup-Objektkopie im Cloud-Storage-Pool zuzugreifen.

Die Objektdaten in einem Cloud Storage Pool können auch verwendet werden, um bei einem Ausfall eines Storage-Volumes oder eines Storage-Nodes verlorene Daten von StorageGRID wiederherzustellen. 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.

So implementieren Sie eine Backup-Lösung:

1. Erstellen Sie einen einzelnen Cloud-Storage-Pool.
2. Konfiguration einer ILM-Regel, die Objektkopien gleichzeitig auf Storage Nodes (als replizierte oder Erasure-codierte Kopien) und einer einzelnen Objektkopie im Cloud Storage Pool speichert
3. Fügen Sie die Regel zur ILM-Richtlinie hinzu. Anschließend simulieren und aktivieren Sie die Richtlinie.

Daten-Tiering von StorageGRID auf externen Standort

Sie können einen Cloud-Speicherpool verwenden, um Objekte außerhalb des StorageGRID Systems zu speichern. Angenommen, Sie haben eine große Anzahl von Objekten, die Sie aufbewahren müssen, aber Sie erwarten, dass Sie auf diese Objekte selten zugreifen, wenn überhaupt. Mit einem Cloud-Storage-Pool können Sie die Objekte auf kostengünstigeren Storage verschieben und Speicherplatz in StorageGRID freigeben.

So implementieren Sie eine Tiering-Lösung:

1. Erstellen Sie einen einzelnen Cloud-Storage-Pool.
2. Konfiguration einer ILM-Regel, die selten genutzte Objekte von Storage-Nodes in den Cloud Storage-Pool verschiebt
3. Fügen Sie die Regel zur ILM-Richtlinie hinzu. Anschließend simulieren und aktivieren Sie die Richtlinie.

Diverse Cloud-Endpunkte beibehalten

Sie können diverse Cloud-Storage-Pool-Endpunkte konfigurieren, wenn Objektdaten in mehr als einer Cloud verschoben oder gesichert werden sollen. Mit den Filtern Ihrer ILM-Regeln können Sie festlegen, welche Objekte in den einzelnen Cloud Storage-Pools gespeichert werden. Beispielsweise können Sie Objekte von einigen Mandanten oder Buckets in Amazon S3 Glacier und Objekte von anderen Mandanten oder Buckets im Azure Blob Storage speichern. Alternativ können Sie Daten zwischen Amazon S3 Glacier und Azure Blob Storage verschieben.

Bei der Nutzung mehrerer Cloud-Storage-Pool-Endpunkte sollte berücksichtigt werden, dass ein Objekt nur in einem Cloud-Storage-Pool gleichzeitig gespeichert werden kann.

So implementieren Sie diverse Cloud-Endpunkte:

1. Erstellung von bis zu 10 Cloud-Storage-Pools
2. Konfiguration von ILM-Regeln, um die entsprechenden Objektdaten zur entsprechenden Zeit in jedem Cloud-Storage-Pool zu speichern Speichern Sie beispielsweise Objekte aus Bucket A in Cloud-Storage-Pool A und speichern Sie Objekte aus Bucket B in Cloud-Storage-Pool B. oder speichern Sie Objekte in Cloud-Storage-Pool A für einen gewissen Zeitraum und verschieben Sie sie dann in Cloud-Storage-Pool B.
3. Fügen Sie Regeln zu Ihrer ILM-Richtlinie hinzu. Anschließend simulieren und aktivieren Sie die Richtlinie.

Überlegungen zu Cloud-Storage-Pools

Wenn Sie einen Cloud Storage Pool zum Verschieben von Objekten aus dem StorageGRID System verwenden möchten, müssen Sie die Überlegungen für die Konfiguration und Verwendung von Cloud Storage Pools prüfen.

Allgemeine Überlegungen

- Im Allgemeinen ist Cloud-Archiv-Storage, wie Amazon S3 Glacier oder Azure Blob Storage, ein kostengünstiger Ort für die Speicherung von Objektdaten. Die Kosten für den Abruf von Daten aus dem Cloud-Archiv-Storage sind jedoch relativ hoch. Um die niedrigsten Gesamtkosten zu erreichen, müssen Sie berücksichtigen, wann und wie oft Sie auf die Objekte im Cloud Storage Pool zugreifen. Die Verwendung eines Cloud-Storage-Pools wird nur für Inhalte empfohlen, auf die Sie voraussichtlich nur selten zugreifen.
- Die Verwendung von Cloud Storage Pools mit FabricPool wird nicht unterstützt, weil die zusätzliche Latenz zum Abrufen eines Objekts aus dem Cloud-Storage-Pool-Ziel hinzugefügt wird.
- Objekte mit aktivierter S3-Objektsperre können nicht in Cloud-Storage-Pools platziert werden.
- Wenn für den Ziel-S3-Bucket für einen Cloud-Storage-Pool die S3-Objektsperre aktiviert ist, schlägt der Versuch, die Bucket-Replizierung (PutBucketReplication) zu konfigurieren, mit einem Fehler bei AccessDenied fehl.
- Die folgenden Plattform-, Authentifizierungs- und Protokollkombinationen mit S3 Object Lock werden für Cloud Storage Pools nicht unterstützt:
  - **Plattformen**: Google Cloud Platform und Azure
  - **Authentifizierungstypen**: IAM-Rollen überall und anonymer Zugriff
  - **Protokoll**: HTTP

Überlegungen zu den Ports, die für Cloud-Storage-Pools verwendet werden

Um sicherzustellen, dass die ILM-Regeln Objekte in den und aus dem angegebenen Cloud Storage-Pool verschieben können, müssen Sie das Netzwerk oder die Netzwerke konfigurieren, die Storage-Nodes Ihres Systems enthalten. Sie müssen sicherstellen, dass die folgenden Ports mit dem Cloud-Speicherpool kommunizieren können.

Standardmäßig verwenden Cloud-Speicherpools die folgenden Ports:

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

Sie können einen anderen Port angeben, wenn Sie einen Cloud-Speicherpool erstellen oder bearbeiten.

Wenn Sie einen nicht transparenten Proxy-Server verwenden, müssen Sie auch "Konfigurieren Sie einen

Speicher-Proxy"zulassen, dass Nachrichten an externe Endpunkte wie z. B. einen Endpunkt im Internet gesendet werden.

Überlegungen zu Kosten

Der Zugriff auf den Storage in der Cloud mit einem Cloud Storage Pool erfordert Netzwerkkonnektivität zur Cloud. Dabei müssen die Kosten der Netzwerkinfrastruktur berücksichtigt werden, die für den Zugriff auf die Cloud und die entsprechende Bereitstellung gemäß der Datenmenge verwendet werden, die Sie voraussichtlich zwischen StorageGRID und der Cloud mithilfe des Cloud-Storage-Pools verschieben möchten.

Wenn sich StorageGRID mit dem Endpunkt eines externen Cloud-Storage-Pools verbinden, werden diverse Anfragen zur Überwachung der Konnektivität bearbeitet, um sicherzustellen, dass die IT die erforderlichen Operationen ausführen kann. Während mit diesen Anforderungen einige zusätzliche Kosten verbunden sind, dürfen die Kosten für die Überwachung eines Cloud Storage Pools nur einen kleinen Bruchteil der Gesamtkosten für das Speichern von Objekten in S3 oder Azure ausmachen.

Es können jedoch weitere erhebliche Kosten entstehen, wenn Sie Objekte von einem externen Endpunkt eines Cloud-Storage-Pools zurück auf StorageGRID verschieben müssen. Objekte können in einem der folgenden Fälle zurück auf StorageGRID verschoben werden:

- Die einzige Kopie des Objekts befindet sich in einem Cloud-Storage-Pool, und Sie entscheiden, das Objekt stattdessen in StorageGRID zu speichern. In diesem Fall konfigurieren Sie Ihre ILM-Regeln und -Richtlinien neu. Wenn eine ILM-Bewertung erfolgt, gibt StorageGRID mehrere Anforderungen aus, um das Objekt aus dem Cloud Storage Pool abzurufen. StorageGRID erstellt dann lokal die angegebene Anzahl von replizierten oder mit Erasure Coding verschlüsselten Kopien. Nachdem das Objekt zurück in den StorageGRID verschoben wurde, wird die Kopie im Cloud-Speicherpool gelöscht.
- Objekte sind aufgrund eines Ausfalls des Storage-Nodes verloren. 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.

> ⓘ Wenn Objekte von einem Cloud-Storage-Pool aus zurück zu StorageGRID verschoben werden, gibt StorageGRID diverse Anfragen an den Cloud-Storage-Pool-Endpunkt für jedes Objekt aus. Bevor Sie eine große Anzahl von Objekten verschieben, wenden Sie sich an den technischen Support, um den Zeitrahmen und die damit verbundenen Kosten zu schätzen.

S3: Für den Cloud Storage Pool Bucket sind Berechtigungen erforderlich

Die Richtlinien für den externen S3-Bucket, der für einen Cloud-Storage-Pool verwendet wird, müssen StorageGRID die Berechtigung erteilen, ein Objekt in den Bucket zu verschieben, den Status eines Objekts zu abrufen oder bei Bedarf ein Objekt aus Glacier-Storage wiederherzustellen usw. Idealerweise sollte StorageGRID vollen Kontrollzugriff auf den Bucket haben (`s3:*`); sollte dies jedoch nicht möglich sein, muss die Bucket-Richtlinie StorageGRID die folgenden S3-Berechtigungen erteilen:

- `s3:AbortMultipartUpload`
- `s3:DeleteObject`
- `s3:GetObject`
- `s3:ListBucket`
- `s3:ListBucketMultipartUploads`
- `s3:ListMultipartUploadParts`

- `s3:PutObject`
- `s3:RestoreObject`

S3: Überlegungen für den Lebenszyklus externer Buckets

Das Verschieben von Objekten zwischen StorageGRID und dem im Cloud Storage Pool angegebenen externen S3 Bucket wird über ILM-Regeln und die aktiven ILM-Richtlinien in StorageGRID gesteuert. Im Gegensatz dazu wird die Transition von Objekten vom im Cloud Storage Pool angegebenen externen S3-Bucket auf Amazon S3 Glacier oder S3 Glacier Deep Archive (oder auf eine Storage-Lösung, die die Glacier Storage-Klasse implementiert) über die Lifecycle-Konfiguration dieses Buckets gesteuert.

Wenn Sie Objekte aus dem Cloud Storage Pool migrieren möchten, müssen Sie die entsprechende Lifecycle-Konfiguration auf dem externen S3-Bucket erstellen. Außerdem müssen Sie eine Storage-Lösung verwenden, die die Glacier Storage-Klasse implementiert und die S3 RestoreObject API unterstützt.

Wenn Sie beispielsweise möchten, dass alle Objekte, die von StorageGRID in den Cloud-Storage-Pool verschoben werden, sofort in Amazon S3 Glacier Storage migriert werden. Sie würden eine Lebenszykluskonfiguration auf dem externen S3-Bucket erstellen, 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 an dem Tag der Erstellung auf Amazon S3 Glacier übertragen (d. h. an dem Tag, an dem sie von StorageGRID in den Cloud-Storage-Pool verschoben wurden).

> Wenn Sie den Lebenszyklus des externen Buckets konfigurieren, verwenden Sie niemals **Expiration**-Aktionen, um zu definieren, wann Objekte ablaufen. Durch Ablaufaktionen wird das Löschen abgelaufener Objekte im externen Speichersystem verursacht. Wenn Sie später versuchen, von StorageGRID auf ein abgelaufenes Objekt zuzugreifen, wird das gelöschte Objekt nicht gefunden.

Wenn Sie Objekte im Cloud-Storage-Pool auf das S3-Glacier-Deep Archive übertragen möchten (nicht auf Amazon S3 Glacier), geben Sie diese im Bucket-Lebenszyklus an `<StorageClass>DEEP_ARCHIVE</StorageClass>`. Beachten Sie jedoch, dass Sie die Tier nicht verwenden können `Expedited`, um Objekte aus dem S3 Glacier Deep Archive wiederherzustellen.

Azure: Überlegungen für Zugriffsebene

Wenn Sie ein Azure-Speicherkonto konfigurieren, können Sie die Standard-Zugriffsebene auf „Hot“ oder „Cool“ festlegen. Wenn Sie ein Speicherkonto für die Verwendung mit einem Cloud-Speicherpool erstellen, sollten Sie den Hot-Tier als Standardebene verwenden. Auch wenn StorageGRID beim Verschieben von Objekten in den Cloud-Speicherpool sofort den Tier auf Archivierung setzt, stellt mit einer Standardeinstellung von Hot sicher, dass für Objekte, die vor dem 30-Tage-Minimum aus dem Cool Tier entfernt wurden, keine Gebühr für vorzeitiges Löschen berechnet wird.

Azure: Lifecycle-Management nicht unterstützt

Verwenden Sie das Azure Blob Storage-Lifecycle-Management nicht für den Container, der mit einem Cloud-Storage-Pool verwendet wird. Lifecycle-Operationen beeinträchtigen möglicherweise Cloud-Storage-Pool-Vorgänge.

Verwandte Informationen

"Erstellen Sie einen Cloud-Storage-Pool"

Vergleich der Replizierung von Cloud-Storage-Pools und CloudMirror

Wenn Sie mit Cloud-Speicherpools beginnen, wäre es möglicherweise hilfreich, die Ähnlichkeiten und Unterschiede zwischen Cloud-Speicherpools und dem Replizierungsservice für StorageGRID CloudMirror zu verstehen.

	Cloud-Storage-Pool	CloudMirror Replikationsservice
Was ist der primäre Zweck?	Fungiert als Archivziel. Die Objektkopie im Cloud-Storage-Pool kann die einzige Kopie des Objekts sein oder es kann eine zusätzliche Kopie sein. Das heißt, statt zwei Kopien vor Ort zu behalten, kann eine Kopie im StorageGRID behalten und eine Kopie an den Cloud-Storage-Pool senden.	Ermöglicht einem Mandanten, automatisch Objekte aus 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 eingerichtet?	Definiert auf dieselbe Weise wie Speicherpools, mit dem Grid Manager oder der Grid-Management-API. Kann als Speicherort in einer ILM-Regel ausgewählt werden. Während ein Storage-Pool aus einer Gruppe von Storage-Nodes besteht, wird ein Cloud-Storage-Pool mit einem Remote-S3- oder Azure-Endpunkt (IP-Adresse, Zugangsdaten usw.) definiert.	Ein Mandantenbenutzer"Konfiguration der CloudMirror-Replizierung", indem er einen CloudMirror-Endpunkt (IP-Adresse, Anmeldedaten usw.) über den Tenant Manager oder die S3-API definiert. Nachdem der CloudMirror Endpunkt eingerichtet wurde, können alle Buckets dieses Mandantenkontos so konfiguriert werden, dass sie auf den CloudMirror Endpunkt verweisen.
Wer ist für die Einrichtung zuständig?	In der Regel ist ein Grid-Administrator erforderlich	In der Regel ein Mandantenbenutzer

	Cloud-Storage-Pool	CloudMirror Replikationsservice
Was ist das Ziel?	• Alle kompatiblen S3-Infrastrukturen (einschließlich Amazon S3) • Azure Blob Archivebene • Google Cloud Platform (GCP)	• Alle kompatiblen S3-Infrastrukturen (einschließlich Amazon S3) • Google Cloud Platform (GCP)
Was bewirkt, dass Objekte zum Ziel verschoben werden?	Mindestens eine ILM-Regel in den aktiven ILM-Richtlinien. Die ILM-Regeln legen fest, welche Objekte die StorageGRID in den Cloud-Storage-Pool verschoben und wann sie verschoben werden.	Aufnahme eines neuen Objekts in einen Quell-Bucket, der mit einem CloudMirror-Endpunkt konfiguriert wurde Objekte, die sich im Quell-Bucket befanden, bevor der Bucket mit dem CloudMirror-Endpunkt konfiguriert wurde, werden nur repliziert, wenn sie geändert wurden.
Wie werden Objekte abgerufen?	Applikationen müssen Anfragen an StorageGRID stellen, um Objekte abzurufen, die in einen Cloud-Speicherpool verschoben wurden. Wenn die einzige Kopie eines Objekts in den Archiv-Storage verschoben wurde, managt StorageGRID den Prozess der Wiederherstellung des Objekts, um es abgerufen werden zu können.	Da die gespiegelte Kopie im Ziel-Bucket eine unabhängige Kopie ist, können Applikationen das Objekt abrufen. Dazu müssen sie Anfragen entweder an StorageGRID oder an das S3-Ziel stellen. Angenommen, Sie verwenden CloudMirror Replizierung, um Objekte auf eine Partnerorganisation zu spiegeln. Der Partner kann mithilfe eigener Applikationen Objekte direkt vom S3-Ziel lesen oder aktualisieren. Die Verwendung von StorageGRID ist nicht erforderlich.
Können Sie direkt vom Ziel lesen?	Es werden keine Objekte, die in einen Cloud-Storage-Pool verschoben werden, von StorageGRID gemanagt. Leseanforderungen müssen an StorageGRID gerichtet sein (und StorageGRID ist für den Abruf aus Cloud Storage Pool verantwortlich).	Ja, da die gespiegelte Kopie eine unabhängige Kopie ist.
Was geschieht, wenn ein Objekt aus der Quelle gelöscht wird?	Das Objekt wird auch aus dem Cloud-Speicher-Pool gelöscht.	Die Löschaktion wird nicht repliziert. Ein gelöschtes Objekt ist nicht mehr im StorageGRID-Bucket vorhanden, ist jedoch weiterhin im Ziel-Bucket vorhanden. Ebenso können Objekte im Ziel-Bucket gelöscht werden, ohne dass die Quelle beeinträchtigt wird.

	Cloud-Storage-Pool	CloudMirror Replikationsservice
Wie greifen Sie nach einem Ausfall auf Objekte zu (StorageGRID System nicht betriebsbereit)?	Fehlerhafte StorageGRID-Knoten müssen wiederhergestellt werden. Während dieses Prozesses können Kopien replizierter Objekte mithilfe der Kopien im Cloud Storage Pool wiederhergestellt werden.	Die Objektkopien im CloudMirror Zielsystem sind unabhängig von StorageGRID, sodass sie direkt vor dem Recovery der StorageGRID-Nodes zugänglich sind.

Erstellen Sie einen Cloud-Storage-Pool

Ein Cloud-Storage-Pool gibt einen einzelnen externen Amazon S3-Bucket oder einen anderen S3-kompatiblen Provider oder einen Azure Blob-Storage-Container an.

Wenn Sie einen Cloud-Storage-Pool erstellen, geben Sie den Namen und den Speicherort des externen Buckets oder Containers an, den StorageGRID zum Speichern von Objekten verwendet, den Cloud-Provider-Typ (Amazon S3/GCP oder Azure Blob Storage) und die Informationen, die StorageGRID für den Zugriff auf den externen Bucket oder Container benötigt.

StorageGRID validiert den Cloud-Storage-Pool, sobald Sie ihn speichern. Sie müssen also sicherstellen, dass der im Cloud-Speicherpool angegebene Bucket oder Container vorhanden ist und erreichbar ist.

Bevor Sie beginnen

- Sie sind im Grid Manager mit einem angemeldet"Unterstützter Webbrowser".
- Sie haben die "Erforderliche Zugriffsberechtigungen".
- Sie haben die überprüft"Überlegungen zu Cloud-Storage-Pools".
- Der externe Bucket oder Container, auf den der Cloud-Speicherpool verweist, ist bereits vorhanden, und Sie haben die Informationen zum Service-Endpunkt.
- Um auf den Bucket oder Container zuzugreifen, haben Sie die Kontoinformationen für den AuthentifizierungstypWahl.

Schritte

1. Wählen Sie **ILM** > **Speicherpools** > **Cloud-Speicherpools**.
2. Wählen Sie **Create**, und geben Sie die folgenden Informationen ein:

Feld	Beschreibung
Name des Cloud-Storage-Pools	Ein Name, der kurz den Cloud Storage Pool und dessen Zweck beschreibt. Verwenden Sie einen Namen, der leicht zu erkennen ist, wann Sie ILM-Regeln konfigurieren.

Feld	Beschreibung
Anbietertyp	Welcher Cloud-Provider nutzen Sie für diesen Cloud-Storage-Pool? • **Amazon S3/GCP**: Wählen Sie diese Option für einen Amazon S3, Commercial Cloud Services (C2S) S3, Google Cloud Platform (GCP) oder einen anderen S3-kompatiblen Anbieter. • * Azure Blob Storage*
Eimer oder Container	Der Name des externen S3-Buckets oder Azure-Containers. Sie können diesen Wert nicht ändern, nachdem der Cloud-Speicherpool gespeichert wurde.

3. Geben Sie auf Grundlage der Auswahl des Anbietertyps die Informationen zum Service-Endpunkt ein.

Amazon S3/GCP

a. Wählen Sie für das Protokoll entweder HTTPS oder HTTP aus.

> Verwenden Sie keine HTTP-Verbindungen für sensible Daten.

b. Geben Sie den Hostnamen ein. Beispiel:

`s3-aws-region.amazonaws.com`

c. URL-Stil auswählen:

Option	Beschreibung
Automatische Erkennung	Versuchen Sie, basierend auf den bereitgestellten Informationen automatisch zu erkennen, welchen URL-Stil verwendet werden soll. Wenn Sie beispielsweise eine IP-Adresse angeben, verwendet StorageGRID eine URL im Pfadstil. Wählen Sie diese Option nur aus, wenn Sie nicht wissen, welcher Stil verwendet werden soll.
Virtual-Hosted-Style	Verwenden Sie eine URL im virtuellen Hosted-Stil, um auf den Bucket zuzugreifen. Virtuelle gehostete URLs enthalten den Bucket-Namen als Teil des Domain-Namens. Beispiel: `https://bucket-name.s3.company.com/key-name`
Pfadstil	Verwenden Sie eine URL im Pfadstil, um auf den Bucket zuzugreifen. URLs im Pfadstil enthalten am Ende den Bucket-Namen Beispiel: `https://s3.company.com/bucket-name/key-name` **Hinweis:** die URL-Option im Pfadstil wird nicht empfohlen und wird in einer zukünftigen Version von StorageGRID veraltet sein.

d. Geben Sie optional die Portnummer ein, oder verwenden Sie den Standardport: 443 für HTTPS oder 80 für HTTP.

Azure Blob Storage

a. Geben Sie unter Verwendung eines der folgenden Formate den URI für den Service-Endpunkt ein.

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

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

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

4. Wählen Sie **Weiter**. Wählen Sie dann den Authentifizierungstyp aus und geben Sie die erforderlichen Informationen für den Endpunkt des Cloud-Storage-Pools ein:

Zugriffsschlüssel

Für Amazon S3/GCP oder einen anderen S3-kompatiblen Anbieter

a. **Zugriffsschlüssel-ID**: Geben Sie die Zugriffsschlüssel-ID für das Konto ein, das den externen Bucket besitzt.
b. **Geheimer Zugriffsschlüssel**: Geben Sie den geheimen Zugriffsschlüssel ein.

IAM-Rollen überall

Für AWS IAM Roles Anywhere Service

StorageGRID erstellt mit dem AWS Security Token Service (STS) dynamisch ein kurzlebiges Token für den Zugriff auf AWS Ressourcen.

a. **AWS IAM Roles Anywhere Region**: Wählen Sie die Region für den Cloud-Speicherpool aus. `us-east-1`Beispiel: .
b. **Trust Anchor URN**: Geben Sie die URN des Vertrauensankers ein, der Anfragen nach kurzlebigen STS-Anmeldeinformationen validiert. Kann eine Stamm- oder Zwischenzertifizierungsstelle sein.
c. **Profil-URN**: Geben Sie die URN des IAM Roles Anywhere-Profils ein, das die Rollen auflistet, die für alle vertrauenswürdigen Personen angenommen werden können.
d. **Role URN**: Geben Sie die URN der IAM-Rolle ein, die für alle Vertrauten angenommen werden kann.
e. **Sitzungsdauer**: Geben Sie die Dauer der temporären Sicherheitsanmeldeinformationen und der Rollensitzung ein. Geben Sie mindestens 15 Minuten und nicht mehr als 12 Stunden ein.
f. **Server-CA-Zertifikat** (optional): Ein oder mehrere vertrauenswürdige CA-Zertifikate im PEM-Format zur Überprüfung des IAM-Roles Anywhere-Servers. Wenn der Server weggelassen wird, wird er nicht verifiziert.
g. **End-Entity-Zertifikat**: Der öffentliche Schlüssel im PEM-Format des vom Vertrauensanker signierten X509-Zertifikats. AWS IAM Roles Anywhere verwendet diesen Schlüssel, um ein STS-Token auszustellen.
h. **End-entity privater Schlüssel**: Der private Schlüssel für das End-entity-Zertifikat.

KAPPE (C2S-Zugangsportal)

Für Commercial Cloud Services (C2S) S3 Service

a. **URL für temporäre Anmeldeinformationen**: Geben Sie die vollständige URL ein, die StorageGRID zum Abrufen temporärer Anmeldeinformationen vom CAP-Server verwendet, einschließlich aller erforderlichen und optionalen API-Parameter, die Ihrem C2S-Konto zugewiesen sind.
b. **Server-CA-Zertifikat**: Wählen Sie **Durchsuchen** und laden Sie das CA-Zertifikat hoch, das StorageGRID zur Überprüfung des CAP-Servers verwendet. Das Zertifikat muss PEM-codiert und von einer entsprechenden Zertifizierungsstelle ausgestellt werden.
c. **Clientzertifikat**: Wählen Sie **Browse** und laden Sie das Zertifikat hoch, das StorageGRID zur Identifikation auf den CAP-Server verwendet. Das Kundenzertifikat muss PEM-codiert sein, von einer entsprechenden Zertifizierungsstelle ausgestellt werden und Zugriff auf Ihr C2S-Konto erhalten.
d. **Privater Client-Schlüssel**: Wählen Sie **Browse** und laden Sie den PEM-kodierten privaten Schlüssel für das Client-Zertifikat hoch.

e. Wenn der private Clientschlüssel verschlüsselt ist, geben Sie die Passphrase zum Entschlüsseln des privaten Clientschlüssels ein. Andernfalls lassen Sie das Feld **Client Private Key Passphrase** leer.

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

Azure Blob Storage

Für Azure Blob Storage, nur gemeinsam genutzter Schlüssel

a. **Kontoname**: Geben Sie den Namen des Speicherkontos ein, das den externen Container besitzt
b. **Kontoschlüssel**: Geben Sie den geheimen Schlüssel für das Speicherkonto ein

Im Azure-Portal finden Sie diese Werte.

Anonym

Es sind keine zusätzlichen Informationen erforderlich.

5. Wählen Sie **Weiter**. Wählen Sie dann die Art der Serverüberprüfung aus, die Sie verwenden möchten:

Option	Beschreibung
Verwenden Sie Stammzertifizierungsstellen-Zertifikate in Storage Node OS	Verwenden Sie zum Sichern der Verbindungen die auf dem Betriebssystem installierten Grid CA-Zertifikate.
Benutzerdefiniertes CA-Zertifikat verwenden	Verwenden Sie ein benutzerdefiniertes CA-Zertifikat. Wählen Sie **Browse** und laden Sie das PEM-kodierte Zertifikat hoch.
Verifizieren Sie das Zertifikat nicht	Wenn Sie diese Option auswählen, sind TLS-Verbindungen zum Cloud-Storage-Pool nicht sicher.

6. Wählen Sie **Speichern**.

   Beim Speichern eines Cloud-Speicherpools führt StorageGRID Folgendes aus:

   - Überprüft, ob der Bucket oder Container und der Service-Endpunkt vorhanden sind und ob sie mit den von Ihnen angegebenen Anmeldedaten erreicht werden können.
   - Schreibt eine Markierungsdatei in den Bucket oder Container, um sie als Cloud-Storage-Pool zu identifizieren. Entfernen Sie niemals diese Datei, die den Namen `x-ntap-sgws-cloud-pool-uuid`hat.

     Wenn die Validierung des Cloud-Storage-Pools fehlschlägt, erhalten Sie eine Fehlermeldung, die erklärt, warum die Validierung fehlgeschlagen ist. Beispielsweise kann ein Fehler gemeldet werden, wenn ein Zertifikatfehler vorliegt oder der Bucket oder Container, den Sie angegeben haben, nicht bereits vorhanden ist.

7. Wenn ein Fehler auftritt, lesen Sie die "Anweisungen zur Fehlerbehebung bei Cloud Storage Pools", Beheben Sie alle Probleme, und versuchen Sie dann erneut, den Cloud-Speicherpool zu speichern.

Details zum Cloud-Storage-Pool anzeigen

Sie können die Details eines Cloud-Storage-Pools anzeigen, um zu bestimmen, wo er verwendet wird, und um anzuzeigen, welche Nodes und Storage-Klassen enthalten sind.

Bevor Sie beginnen

- Sie sind im Grid Manager mit einem angemeldet"Unterstützter Webbrowser".
- Sie haben "Bestimmte Zugriffsberechtigungen".

Schritte

1. Wählen Sie **ILM** > **Speicherpools** > **Cloud-Speicherpools**.

   Die Tabelle „Cloud Storage Pools“ enthält die folgenden Informationen zu jedem Cloud-Storage-Pool, der Storage-Nodes umfasst:

   - **Name**: Der eindeutige Anzeigename des Pools.
   - **URI**: Der Uniform Resource Identifier des Cloud Storage Pools.
   - **Provider-Typ**: Welcher Cloud-Provider wird für diesen Cloud-Speicherpool verwendet?
   - **Container**: Der Name des Buckets, der für den Cloud-Speicherpool verwendet wird.
   - **ILM-Nutzung**: Wie der Pool derzeit genutzt wird. Ein Cloud Storage-Pool wird möglicherweise nicht verwendet oder kann in einem oder mehreren ILM-Regeln, Erasure-Coding-Profilen oder beiden verwendet werden.
   - **Letzter Fehler**: Der letzte Fehler, der bei einer Integritätsprüfung dieses Cloud-Speicherpools festgestellt wurde.

2. Um Details zu einem bestimmten Cloud-Speicherpool anzuzeigen, wählen Sie dessen Namen aus.

   Die Detailseite für den Pool wird angezeigt.

3. Sehen Sie sich die Registerkarte **Authentifizierung** an, um mehr über den Authentifizierungstyp für diesen Cloud-Speicherpool zu erfahren und die Authentifizierungsdetails zu bearbeiten.
4. Sehen Sie sich die Registerkarte **Server-Überprüfung** an, um mehr über Überprüfungsdetails zu erfahren, die Überprüfung zu bearbeiten, ein neues Zertifikat herunterzuladen oder das Zertifikat-PEM zu kopieren.
5. Auf der Registerkarte **ILM-Nutzung** können Sie feststellen, ob der Cloud-Speicherpool derzeit in ILM-Regeln oder Profilen für die Erasure Coding verwendet wird.
6. Gehen Sie optional zur Seite **ILM-Regeln**, um den Cloud-Speicherpool zu "Informieren Sie sich über alle Regeln und verwalten Sie sie"verwenden.

Bearbeiten eines Cloud-Speicherpools

Sie können einen Cloud-Storage-Pool bearbeiten, um dessen Namen, Service-Endpunkt oder andere Details zu ändern. Sie können jedoch nicht den S3-Bucket oder Azure-Container für einen Cloud-Storage-Pool ändern.

Bevor Sie beginnen

- Sie sind im Grid Manager mit einem angemeldet"Unterstützter Webbrowser".
- Sie haben "Bestimmte Zugriffsberechtigungen".

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

Schritte

1. Wählen Sie **ILM** > **Speicherpools** > **Cloud-Speicherpools**.

   In der Tabelle Cloud-Storage-Pools werden die vorhandenen Cloud-Storage-Pools aufgeführt.

2. Aktivieren Sie das Kontrollkästchen für den Cloud-Speicherpool, den Sie bearbeiten möchten, und wählen Sie dann **actions** > **Edit** aus.

   Alternativ wählen Sie den Namen des Cloud Storage Pools aus und wählen dann **Bearbeiten**.

3. Ändern Sie ggf. den Namen, den Service-Endpunkt, die Authentifizierungsdaten oder die Zertifizierungsverifizierungsmethode des Cloud Storage Pools.

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

   Wenn Sie zuvor ein Server- oder Client-Zertifikat hochgeladen haben, können Sie das Akkordeon **Certificate Details** erweitern, um das aktuell verwendete Zertifikat zu überprüfen.

4. Wählen Sie **Speichern**.

   Wenn Sie einen Cloud-Storage-Pool speichern, überprüft StorageGRID, ob der Bucket oder Container und der Service-Endpunkt vorhanden sind. Ob sie mit den von Ihnen angegebenen Zugangsdaten erreicht werden können.

   Wenn die Validierung des Cloud-Speicherpools fehlschlägt, wird eine Fehlermeldung angezeigt. Ein Fehler kann z. B. gemeldet werden, wenn ein Zertifikatfehler vorliegt.

   Lesen Sie die Anweisungen für "Fehlerbehebung bei Cloud Storage Pools", Beheben Sie das Problem, und versuchen Sie dann erneut, den Cloud-Speicherpool zu speichern.

Entfernen Sie einen Cloud-Speicherpool

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

Bevor Sie beginnen

- Sie sind im Grid Manager mit einem angemeldet"Unterstützter Webbrowser".
- Sie haben die "Erforderliche Zugriffsberechtigungen".

Verwenden Sie bei Bedarf ILM, um Objektdaten zu verschieben

Wenn der Cloud Storage Pool, den Sie entfernen möchten, Objektdaten enthält, müssen Sie ILM verwenden, um die Daten an einen anderen Speicherort zu verschieben. Sie können die Daten beispielsweise in Storage Nodes in Ihrem Grid oder in einen anderen Cloud-Storage-Pool verschieben.

Schritte

1. Wählen Sie **ILM** > **Speicherpools** > **Cloud-Speicherpools**.
2. Prüfen Sie in der Spalte „ILM-Nutzung“ der Tabelle, ob Sie den Cloud Storage-Pool entfernen können.

Sie können einen Cloud Storage-Pool nicht entfernen, wenn er in einer ILM-Regel oder in einem Erasure-Coding-Profil verwendet wird.

3. Wenn der Cloud Storage Pool verwendet wird, wählen Sie ***Cloud Storage Pool Name*** > **ILM usage** aus.
4. "Klonen jeder ILM-Regel" Damit werden Objekte im Cloud-Storage-Pool platziert, den Sie entfernen möchten.
5. Legen Sie fest, wo die vorhandenen Objekte, die von den einzelnen von Ihnen geklonten Regeln verwaltet werden, verschoben werden sollen.

   Sie können einen oder mehrere Speicherpools oder einen anderen Cloud-Speicherpool verwenden.

6. Bearbeiten Sie jede der von Ihnen geklonten Regeln.

   Wählen Sie für Schritt 2 des Assistenten zum Erstellen von ILM-Regeln den neuen Speicherort aus dem Feld **copies at** aus.

7. "Neue ILM-Richtlinie erstellen" Und ersetzen Sie jede der alten Regeln durch eine geklonte Regel.
8. Aktivieren Sie die neue Richtlinie.
9. Warten Sie, bis ILM Objekte aus dem Cloud Storage-Pool entfernt und an dem neuen Speicherort platziert hat.

Cloud Storage-Pool Löschen

Wenn der Cloud Storage Pool leer ist und in keiner ILM-Regel verwendet wird, können Sie ihn löschen.

Bevor Sie beginnen

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

  Ein Fehler tritt auf, wenn Sie versuchen, einen Cloud-Speicherpool zu entfernen, wenn er Objekte enthält. Siehe "Fehlerbehebung Bei Cloud Storage Pools".

> ⓘ Beim Erstellen eines Cloud Storage-Pools schreibt StorageGRID eine Markierungsdatei in den Bucket oder Container, um sie als Cloud-Storage-Pool zu identifizieren. Entfernen Sie nicht diese Datei, die den Namen hat `x-ntap-sgws-cloud-pool-uuid`.

Schritte

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

Fehlerbehebung Bei Cloud Storage Pools

Verwenden Sie diese Fehlerbehebungsschritte, um Fehler zu beheben, die beim Erstellen, Bearbeiten oder Löschen eines Cloud-Speicherpools auftreten können.

Ermitteln Sie, ob ein Fehler aufgetreten ist

StorageGRID führt eine einfache Integritätsprüfung für jeden Cloud-Storage-Pool durch, indem das bekannte Objekt gelesen `x-ntap-sgws-cloud-pool-uuid` wird, um sicherzustellen, dass auf den Cloud-Storage-Pool zugegriffen werden kann und ordnungsgemäß funktioniert. Wenn bei StorageGRID ein Fehler am Endpunkt auftritt, wird jede Minute von jedem Speicher-Node aus eine Integritätsprüfung durchgeführt. Wenn der Fehler behoben ist, werden die Zustandsprüfungen beendet. Wenn eine Integritätsprüfung ein Problem erkennt, wird eine Meldung in der Spalte Letzter Fehler der Tabelle Cloud-Speicherpools auf der Seite Speicherpools angezeigt.

In der Tabelle ist der aktuellste Fehler aufgeführt, der bei den einzelnen Cloud-Storage-Pools erkannt wurde. Der Fehler ist vor langer Zeit aufgetreten.

Zusätzlich wird eine Meldung mit * Cloud Storage Pool Verbindungsfehler* ausgelöst, wenn die Systemprüfung feststellt, dass innerhalb der letzten 5 Minuten ein oder mehrere neue Cloud Storage Pool-Fehler aufgetreten sind. Wenn Sie eine E-Mail-Benachrichtigung für diese Warnung erhalten, gehen Sie zur Seite Speicherpools (wählen Sie **ILM** > **Speicherpools**), überprüfen Sie die Fehlermeldungen in der Spalte Letzter Fehler und lesen Sie die unten stehenden Richtlinien zur Fehlerbehebung.

Überprüfen Sie, ob ein Fehler behoben wurde

Nach der Behebung von Problemen können Sie feststellen, ob der Fehler behoben ist. Wählen Sie auf der Seite Cloud Storage Pool den Endpunkt aus, und wählen Sie **Fehler löschen** aus. Eine Bestätigungsmeldung gibt an, dass StorageGRID den Fehler für den Cloud-Speicherpool gelöscht hat.

Wenn das zugrunde liegende Problem behoben wurde, 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 Letzter Fehler angezeigt.

Fehler: Integritätsprüfung fehlgeschlagen. Fehler vom Endpunkt

Dieser Fehler kann auftreten, wenn Sie S3-Objektsperre mit Standardaufbewahrung für Ihren Amazon S3-Bucket aktivieren, nachdem Sie diesen Bucket für einen Cloud-Storage-Pool verwenden. Dieser Fehler tritt auf, wenn der PUT-Vorgang keinen HTTP-Header mit einem Payload-Prüfsummenwert wie hat `Content-MD5`. Dieser Header-Wert wird von AWS für DAS PUT von Vorgängen in Buckets benötigt, für die S3 Object Lock aktiviert ist.

Um dieses Problem zu beheben, führen Sie die Schritte unter "Bearbeiten eines Cloud-Speicherpools"aus, ohne Änderungen vorzunehmen. Diese Aktion löst die Validierung der Cloud-Storage-Pool-Konfiguration aus, die das S3 Object Lock-Flag auf einer Cloud-Storage-Pool-Endpunktkonfiguration automatisch erkennt und aktualisiert.

Fehler: Dieser Cloud-Speicherpool enthält unerwartete Inhalte

Dieser Fehler wird möglicherweise auftreten, wenn Sie versuchen, einen Cloud-Speicherpool zu erstellen, zu bearbeiten oder zu löschen. Dieser Fehler tritt auf, wenn der Bucket oder Container die Markierungsdatei enthält `x-ntap-sgws-cloud-pool-uuid`, aber diese Datei nicht das Metadatenfeld mit der erwarteten UUID hat.

In der Regel wird dieser Fehler nur angezeigt, wenn Sie einen neuen Cloud Storage-Pool erstellen, und eine andere Instanz von StorageGRID verwendet bereits den gleichen Cloud Storage-Pool.

Führen Sie einen der folgenden Schritte aus, um das Problem zu beheben:

- Wenn Sie einen neuen Cloud-Storage-Pool konfigurieren und der Bucket die Datei und zusätzliche Objektschlüssel enthält, die `x-ntap-sgws-cloud-pool-uuid` dem folgenden Beispiel ähneln, erstellen Sie einen neuen Bucket und verwenden Sie stattdessen diesen neuen Bucket.

  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, löschen Sie diese Datei.

Wenn diese Schritte nicht auf Ihr Szenario zutreffen, wenden Sie sich an den Support.

Fehler: Cloud-Speicherpool konnte nicht erstellt oder aktualisiert werden. Fehler vom Endpunkt

Dieser Fehler kann unter den folgenden Umständen auftreten:

- Wenn Sie versuchen, einen Cloud-Speicherpool zu erstellen oder zu bearbeiten.
- Wenn Sie während der Konfiguration eines neuen Cloud Storage-Pools eine nicht unterstützte Plattform-, Authentifizierungs- oder Protokollkombination mit S3 Object Lock auswählen. Siehe "Überlegungen zu Cloud-Storage-Pools".

Dieser Fehler zeigt an, dass ein Verbindungs- oder Konfigurationsproblem verhindert, dass StorageGRID in den Cloud-Speicherpool schreibt.

Überprüfen Sie die Fehlermeldung vom Endpunkt, um das Problem zu beheben.

- Wenn die Fehlermeldung enthält `Get *url*: EOF`, überprüfen Sie, ob der für den Cloud-Speicher-Pool verwendete Service-Endpunkt HTTP nicht für einen Container oder Bucket verwendet, der HTTPS erfordert.
- Wenn die Fehlermeldung enthält `Get *url*: net/http: request canceled while waiting for connection`, überprüfen Sie, ob die Netzwerkkonfiguration es Storage Nodes ermöglicht, auf den für den Cloud-Speicherpool verwendeten Dienstendpunkt zuzugreifen.
- Wenn der Fehler auf eine nicht unterstützte Plattform, Authentifizierung oder ein nicht unterstütztes Protokoll zurückzuführen ist, wechseln Sie zu einer unterstützten Konfiguration mit S3 Object Lock, und versuchen Sie erneut, den neuen Cloud Storage Pool zu speichern.
- Versuchen Sie bei allen anderen Fehlermeldungen am Endpunkt eine oder mehrere der folgenden Optionen:
  - Erstellen Sie einen externen Container oder Bucket mit demselben Namen, den Sie für den Cloud-Storage-Pool eingegeben haben, und versuchen Sie, den neuen Cloud-Storage-Pool erneut zu speichern.
  - Korrigieren Sie den für den Cloud Storage Pool angegebenen Container- oder Bucket-Namen und versuchen Sie, den neuen Cloud Storage-Pool erneut zu speichern.

Fehler: Fehler beim Parsen des CA-Zertifikats

Dieser Fehler wird möglicherweise auftreten, wenn Sie versuchen, einen Cloud-Speicherpool zu erstellen oder zu bearbeiten. Der Fehler tritt auf, wenn StorageGRID das bei der Konfiguration des Cloud-Speicherpools eingegebene Zertifikat nicht analysieren konnte.

Überprüfen Sie zum Beheben des Problems das von Ihnen bereitgestellte CA-Zertifikat auf Probleme.

Fehler: Ein Cloud-Speicherpool mit dieser ID wurde nicht gefunden

Dieser Fehler wird möglicherweise auftreten, wenn Sie versuchen, einen Cloud-Speicherpool zu bearbeiten oder zu löschen. Dieser Fehler tritt auf, wenn der Endpunkt eine 404-Antwort zurückgibt. Dies kann eine der folgenden Optionen bedeuten:

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

Versuchen Sie mindestens einen der folgenden Schritte, um das Problem zu beheben:

- Stellen Sie sicher, dass der dem konfigurierten Zugriffsschlüssel zugeordnete Benutzer über die erforderlichen Berechtigungen verfügt.
- Bearbeiten Sie den Cloud Storage Pool mit Zugangsdaten, die über die entsprechenden Berechtigungen verfügen.
- Wenn die Berechtigungen korrekt sind, wenden Sie sich an den Support.

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

Dieser Fehler wird möglicherweise auftreten, wenn Sie versuchen, einen Cloud-Speicherpool zu löschen. Dieser Fehler zeigt an, dass eine Art von Verbindungs- oder Konfigurationsproblem darin besteht, dass StorageGRID den Inhalt des Cloud Storage Pool Buckets liest.

Überprüfen Sie die Fehlermeldung vom Endpunkt, um das Problem zu beheben.

Fehler: Objekte wurden bereits in diesen Bucket platziert

Dieser Fehler wird möglicherweise auftreten, wenn Sie versuchen, einen Cloud-Speicherpool zu löschen. Sie können einen Cloud-Storage-Pool nicht löschen, wenn er Daten enthält, die durch ILM dorthin verschoben wurden, Daten, die sich vor dem Konfigurieren des Cloud-Storage-Pools im Bucket befinden, oder Daten, die nach der Erstellung des Cloud-Storage-Pools von einer anderen Quelle in den Bucket verschoben wurden.

Versuchen Sie mindestens einen der folgenden Schritte, um das Problem zu beheben:

- Befolgen Sie die Anweisungen zum Verschieben von Objekten zurück zu StorageGRID im „Lebenszyklus eines Cloud-Storage-Pool-Objekts“.
- Wenn Sie sicher sind, dass die verbleibenden Objekte nicht durch ILM im Cloud-Storage-Pool platziert wurden, löschen Sie die Objekte manuell aus dem Bucket.

> ⓘ Löschen Sie nie Objekte manuell aus einem Cloud-Storage-Pool, der eventuell durch ILM gespeichert wurde. Wenn Sie später versuchen, auf ein manuell gelöschtes Objekt aus StorageGRID zuzugreifen, wird das gelöschte Objekt nicht gefunden.

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

Dieser Fehler kann auftreten, wenn Sie einen nicht-transparenten Storage-Proxy zwischen den Storage-Nodes und dem externen S3-Endpunkt konfiguriert haben, der für den Cloud-Storage-Pool verwendet wird. Dieser

Fehler tritt auf, wenn der externe Proxyserver den Endpunkt des Cloud-Speicherpools nicht erreichen kann. Beispielsweise kann der DNS-Server den Hostnamen möglicherweise nicht lösen, oder es könnte ein externes Netzwerkproblem geben.

Versuchen Sie mindestens einen der folgenden Schritte, um das Problem zu beheben:

- Überprüfen Sie die Einstellungen für den Cloud Storage Pool (**ILM** > **Storage Pools**).
- Prüfen Sie die Netzwerkkonfiguration des Storage-Proxy-Servers.

Fehler: X.509-Zertifikat ist außerhalb des Gültigkeitszeitraums

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

Versuchen Sie mit diesen Schritten das Problem zu beheben:

- Aktualisieren Sie das Zertifikat, das für die Authentifizierung am Cloud Storage Pool konfiguriert ist.
- Stellen Sie sicher, dass alle Warnungen zum Ablauf des Zertifikats in diesem Cloud-Storage-Pool behoben sind.

Verwandte Informationen

"Lebenszyklus eines Cloud-Storage-Pool-Objekts"