Objektmanagement mit ILM

StorageGRID

NetApp
March 12, 2025

Inhalt

Objektmanagement mit ILM . . . 1
Objektmanagement mit ILM . . . 1
Informationen zu diesen Anweisungen . . . 1
Weitere Informationen . . . 1
ILM und Objekt-Lebenszyklus . . . 2
Wie ILM im gesamten Leben eines Objekts funktioniert . . . 2
Aufnahme von Objekten . . . 3
Speicherung von Objekten (Replizierung oder Erasure Coding) . . . 7
Wie die Aufbewahrung von Objekten bestimmt wird . . . 18
So werden Objekte gelöscht . . . 20
Speicherklassen erstellen und zuweisen . . . 23
Nutzung von Speicherpools . . . 26
Was ist ein Speicherpool? . . . 26
Richtlinien zur Erstellung von Speicherpools . . . 27
Schutz vor Standortausfällen . . . 28
Erstellen Sie einen Speicherpool . . . 30
Zeigen Sie Details zum Speicherpool an . . . 32
Speicherpool bearbeiten . . . 33
Entfernen Sie einen Speicherpool . . . 34
Verwendung Von Cloud Storage Pools . . . 35
Was ist ein Cloud-Storage-Pool? . . . 35
Lebenszyklus eines Cloud-Storage-Pool-Objekts . . . 36
Wann sollten Sie Cloud Storage Pools nutzen . . . 38
Überlegungen zu Cloud-Storage-Pools . . . 40
Vergleich der Replizierung von Cloud-Storage-Pools und CloudMirror . . . 43
Erstellen Sie einen Cloud-Storage-Pool . . . 44
Details zum Cloud-Storage-Pool anzeigen . . . 49
Bearbeiten eines Cloud-Speicherpools . . . 49
Entfernen Sie einen Cloud-Speicherpool . . . 50
Fehlerbehebung Bei Cloud Storage Pools . . . 51
Profile für das Erasure Coding managen . . . 55
Profildetails zum Erasure Coding anzeigen . . . 55
Umbenennen eines Profils für die Erasure Coding . . . 55
Deaktivieren Sie ein Erasure Coding-Profil . . . 56
Regionen konfigurieren (nur optional und S3) . . . 58
ILM-Regel erstellen . . . 60
Verwenden Sie ILM-Regeln zum Managen von Objekten . . . 60
Greifen Sie auf den Assistenten zum Erstellen einer ILM-Regel zu . . . 64
Schritt 1 von 3: Details eingeben . . . 65
Schritt 2 von 3: Definieren von Platzierungen . . . 69
Verwenden Sie die letzte Zugriffszeit in ILM-Regeln . . . 72
Schritt 3 von 3: Wählen Sie Ingest Behavior . . . 74
Erstellen einer Standard-ILM-Regel . . . 74

Managen von ILM-Richtlinien . . . 77
Verwenden Sie ILM-Richtlinien . . . 77
Erstellen von ILM-Richtlinien . . . 81
Beispiele für ILM-Richtliniensimulationen . . . 88
Managen von ILM-Richtlinien-Tags . . . 91
Überprüfen einer ILM-Richtlinie mit Objekt-Metadaten-Lookup . . . 92
Arbeiten mit ILM-Richtlinien und ILM-Regeln . . . 94
ILM-Richtlinien anzeigen . . . 94
Bearbeiten Sie eine ILM-Richtlinie . . . 95
Klonen einer ILM-Richtlinie . . . 95
Entfernen einer ILM-Richtlinie . . . 95
Zeigen Sie Einzelheiten zur ILM-Regel an . . . 96
Klonen einer ILM-Regel . . . 96
Bearbeiten einer ILM-Regel . . . 97
Entfernen einer ILM-Regel . . . 97
Anzeigen von ILM-Metriken . . . 98
Verwenden Sie die S3-Objektsperre . . . 99
Objekte managen mit S3 Object Lock . . . 99
S3 Objektsperraufgaben . . . 102
Anforderungen für die S3-Objektsperre . . . 103
Aktivieren Sie die S3-Objektsperre global . . . 105
Beheben Sie die Konsistenzfehler beim Aktualisieren der S3-Objektsperre oder der alten Compliance-Konfiguration . . . 107
Beispiele für ILM-Regeln und -Richtlinien . . . 107
Beispiel 1: ILM-Regeln und -Richtlinie für Objekt-Storage . . . 107
Beispiel 2: ILM-Regeln und Richtlinie für EC-Objektgrößen-Filterung . . . 110
Beispiel 3: ILM-Regeln und -Richtlinie für besseren Schutz von Image-Dateien . . . 111
Beispiel 4: ILM-Regeln und -Richtlinie für versionierte Objekte mit S3 . . . 113
Beispiel 5: ILM-Regeln und Richtlinie für striktes Ingest-Verhalten . . . 116
Beispiel 6: Ändern einer ILM-Richtlinie . . . 118
Beispiel 7: Konforme ILM-Richtlinie für S3 Object Lock . . . 123
Beispiel 8: Prioritäten für den S3-Bucket-Lebenszyklus und die ILM-Richtlinie . . . 126

Objektmanagement mit ILM

Objektmanagement mit ILM

Die Regeln für Information Lifecycle Management (ILM) einer ILM-Richtlinie erläutern StorageGRID, wie Kopien von Objektdaten erstellt und verteilt werden und wie diese Kopien über einen längeren Zeitraum gemanagt werden.

Informationen zu diesen Anweisungen

Die Entwicklung und Implementierung von ILM-Regeln und -Richtlinien erfordert eine sorgfältige Planung. Betriebliche Anforderungen, die Topologie des StorageGRID Systems, die Anforderungen an die Objektsicherung und die verfügbaren Storage-Typen sind unbedingt bekannt. Anschließend müssen Sie festlegen, wie unterschiedliche Objekttypen kopiert, verteilt und gespeichert werden sollen.

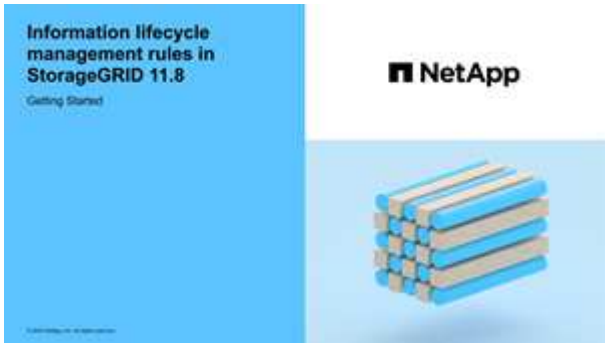
Mithilfe dieser Anweisungen können Sie:

- Erfahren Sie mehr über StorageGRID ILM, einschließlich "Wie ILM im gesamten Leben eines Objekts funktioniert".
- Erfahren Sie, wie Sie konfigurieren "Storage-Pools", "Cloud-Storage-Pools"und "ILM-Regeln".
- Erfahren Sie, wie sich "Erstellen, Simulieren und Aktivieren einer ILM-Richtlinie"Objektdaten an einem oder mehreren Standorten sichern lassen.
- Erfahren Sie, wie Sie "Managen von Objekten mit S3 Object Lock", um sicherzustellen, dass Objekte in bestimmten S3-Buckets nicht gelöscht oder für eine bestimmte Zeit überschrieben werden.

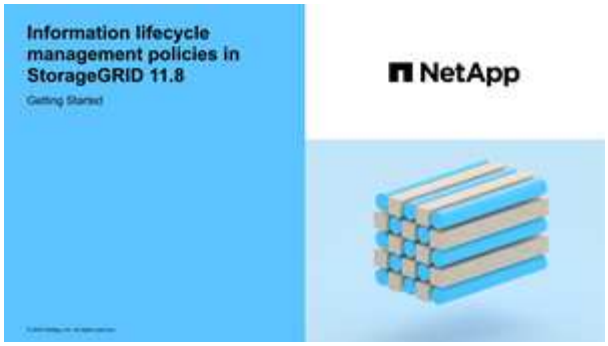
Weitere Informationen .

Sehen Sie sich die folgenden Videos an, um mehr zu erfahren:

- "Video: ILM-Regeln im Überblick".



- "Video: ILM-Richtlinien im Überblick"



ILM und Objekt-Lebenszyklus

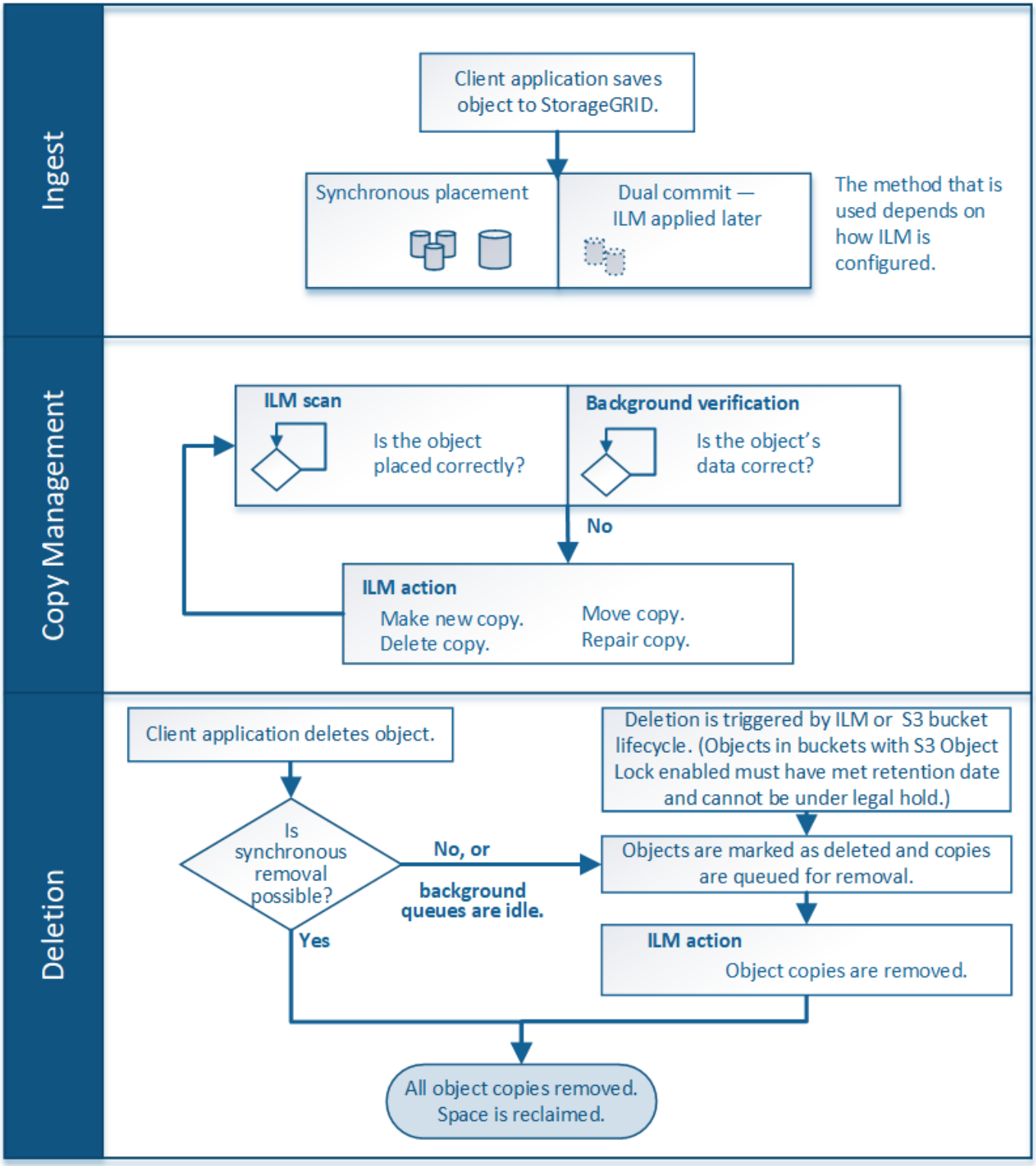
Wie ILM im gesamten Leben eines Objekts funktioniert

Wenn Sie verstehen, wie StorageGRID ILM für das Management von Objekten in jeder Lebensphase verwendet, können Sie eine effektivere Richtlinie entwickeln.

- **Ingest**: Ingest beginnt, wenn eine S3-Client-Anwendung eine Verbindung herstellt, um ein Objekt im StorageGRID-System zu speichern, und ist abgeschlossen, wenn StorageGRID eine Nachricht "erfolgreich aufgenommen" an den Client zurückgibt. Objektdaten werden bei der Aufnahme entweder durch sofortiges Anwenden von ILM-Anweisungen (synchrone Platzierung) oder durch Erstellen von zwischenzeitlichen Kopien und spätere Anwendung von ILM (Dual Commit) gesichert, je nachdem, wie die ILM-Anforderungen angegeben wurden.
- **Kopierverwaltung**: Nach dem Erstellen der Anzahl und des Typs der Objektkopien, die in den Anweisungen zur Platzierung des ILM angegeben sind, verwaltet StorageGRID Objektorte und schützt Objekte vor Verlust.
  - **ILM-Scan und -Auswertung**: StorageGRID scannt kontinuierlich die Liste der im Raster gespeicherten Objekte und prüft, ob die aktuellen Kopien den ILM-Anforderungen entsprechen. Wenn unterschiedliche Typen, Ziffern oder Standorte von Objektkopien erforderlich sind, erstellt, löscht oder verschiebt StorageGRID Kopien nach Bedarf.
  - **Hintergrundüberprüfung**: StorageGRID führt kontinuierlich eine Hintergrundprüfung durch, um die Integrität von Objektdaten zu überprüfen. Wenn ein Problem gefunden wird, erstellt StorageGRID automatisch eine neue Objektkopie oder ein durch Löschung codiertes Objektfragment für den Austausch, das die aktuellen ILM-Anforderungen erfüllt. Siehe "Überprüfen Sie die Objektintegrität".
- **Objektlöschung**: Verwaltung eines Objekts endet, wenn alle Kopien aus dem StorageGRID-System entfernt werden. Objekte können als Ergebnis einer Löschanforderung durch einen Client oder als Ergebnis eines Löschvorgangs durch ILM oder Löschung aufgrund des Ablaufs eines S3-Bucket-Lebenszyklus entfernt werden.

> Objekte in einem Bucket, für den die S3-Objektsperrung aktiviert ist, können nicht gelöscht werden, wenn sie sich unter einer Legal Hold befinden oder wenn ein Aufbewahrungsdatum angegeben, aber noch nicht erfüllt wurde.

Das Diagramm fasst die Funktionsweise von ILM im gesamten Lebenszyklus eines Objekts zusammen.



Aufnahme von Objekten

Aufnahmeoptionen

Wenn Sie eine ILM-Regel erstellen, geben Sie eine von drei Optionen zum Schutz der Objekte bei der Aufnahme an: Doppelter Commit, strenger oder ausgeglichener Storage.

Je nach Ihrer Wahl erstellt StorageGRID später vorläufige Kopien und Warteschlangen für die ILM-Bewertung.

Alternativ nutzt es die synchrone Platzierung und erstellt sofort Kopien zur Erfüllung der ILM-Anforderungen.

Flussdiagramm der Aufnahmeoptionen

Das Flussdiagramm zeigt, was passiert, wenn Objekte mit einer ILM-Regel abgeglichen werden, die jede der drei Aufnahmeoptionen nutzt.

Doppelte Provisionierung

Wenn Sie die Option „Dual Commit“ auswählen, erstellt StorageGRID sofort Zwischenobjektkopien auf zwei verschiedenen Speicherknoten und gibt eine Meldung „Ingest successful“ an den Client zurück. Das Objekt wird zur ILM-Evaluierung in eine Warteschlange gestellt und Kopien, die den Anweisungen zur Platzierung der Regel entsprechen, werden später erstellt. Wenn die ILM-Richtlinie nicht unmittelbar nach der doppelten Übertragung verarbeitet werden kann, kann der Schutz vor Standortausfällen eine Weile dauern.

Verwenden Sie in einem der folgenden Fälle die Dual-Commit-Option:

- Die wichtigsten Überlegungen dabei sind die Verwendung von ILM-Regeln für mehrere Standorte und die Client-Erfassungs-Latenz. Wenn Sie Dual Commit verwenden, müssen Sie sicherstellen, dass Ihr Grid die zusätzliche Arbeit beim Erstellen und Entfernen der Dual-Commit-Kopien ausführen kann, wenn sie ILM nicht erfüllen. Im Detail:
  - Die Last am Grid muss so gering sein, dass kein ILM-Rückstand mehr vorhanden ist.
  - Das Grid muss über überschüssige Hardware-Ressourcen verfügen (IOPS, CPU, Arbeitsspeicher, Netzwerkbandbreite usw.).
- Sie verwenden ILM-Regeln für mehrere Standorte und die WAN-Verbindung zwischen den Standorten weist normalerweise eine hohe Latenz oder eine begrenzte Bandbreite auf. In diesem Szenario kann die Verwendung der Dual-Commit-Option dazu beitragen, Client-Timeouts zu verhindern. Bevor Sie sich für die Dual Commit-Option entscheiden, sollten Sie die Client-Applikation mit realistischen Workloads testen.

Ausgeglichen (Standard)

Wenn Sie die Option „Ausgleich“ auswählen, verwendet StorageGRID bei der Aufnahme auch die synchrone Platzierung und erstellt sofort alle Kopien, die in den Anweisungen zur Platzierung der Regel angegeben sind. Wenn StorageGRID nicht sofort alle Kopien erstellen kann, verwendet man im Gegensatz zur strengen Option „Dual Commit“. Wenn die ILM-Richtlinie Platzierungen an mehreren Standorten verwendet und ein sofortiger Schutz vor Standortausfällen nicht erreicht werden kann, wird die Warnung **ILM-Platzierung nicht erreichbar** ausgelöst.

Die ausgewogene Option erzielt die beste Kombination aus Datensicherung, Grid-Performance und Aufnahme-Erfolg. Ausgeglichen ist die Standardoption im Assistenten zum Erstellen von ILM-Regeln.

Streng

Wenn Sie die strenge Option auswählen, verwendet StorageGRID bei der Aufnahme eine synchrone Platzierung und erstellt sofort alle Objektkopien, die in der Plazierung der Regel angegeben sind. Die Aufnahme schlägt fehl, wenn StorageGRID nicht alle Kopien erstellen kann, z. B. weil ein erforderlicher Speicherort vorübergehend nicht verfügbar ist. Der Client muss den Vorgang wiederholen.

Verwenden Sie die Option streng, wenn Sie eine betriebliche oder gesetzliche Anforderung haben, Objekte sofort nur an den in der ILM-Regel aufgeführten Standorten zu speichern. Um beispielsweise eine gesetzliche Vorgabe zu erfüllen, müssen Sie möglicherweise die Option „Strict“ und einen erweiterten Filter „Speicherortbeschränkung“ verwenden, um sicherzustellen, dass Objekte niemals in bestimmten Rechenzentren gespeichert werden.

Siehe "Beispiel 5: ILM-Regeln und Richtlinie für striktes Ingest-Verhalten".

Vorteile, Nachteile und Einschränkungen der Aufnahmsoptionen

Wenn Sie die vor- und Nachteile der drei Optionen zum Schutz von Daten bei der Aufnahme (ausgewogen, streng oder Dual-Commit) kennen, können Sie leichter entscheiden, welche für eine ILM-Regel ausgewählt werden soll.

Eine Übersicht über die Aufnahmeoptionen finden Sie unter "Aufnahmeoptionen".

Vorteile der ausgewogenen und strengen Optionen

Im Vergleich zu Dual-Commit, das während der Aufnahme zwischenzeitliche Kopien erstellt, bieten die zwei Optionen zur synchronen Platzierung folgende Vorteile:

- **Bessere Datensicherheit**: Objektdaten werden sofort gemäß den Anweisungen zur Platzierung der ILM-Regel geschützt, die so konfiguriert werden können, dass sie vor einer Vielzahl von Ausfallszenarien, einschließlich des Ausfalls von mehr als einem Speicherort, geschützt werden. Bei zwei Daten kann nur der Schutz vor dem Verlust einer einzelnen lokalen Kopie geschützt werden.
- **Effizienterer Netzbetrieb**: Jedes Objekt wird nur einmal verarbeitet, wie es aufgenommen wird. Da das StorageGRID System die Interimskopien nicht nachverfolgen oder löschen muss, sinkt der Verarbeitungsbedarf und der Datenbankspeicherplatz wird verringert.
- **(ausgewogen) Empfohlen**: Die ausgewogene Option bietet optimale ILM-Effizienz. Die Verwendung der Balanced-Option wird empfohlen, es sei denn, es ist ein striktes Aufnahmeverhalten erforderlich oder das Grid erfüllt alle Kriterien für die Verwendung von Dual Commit.
- **(striktes) Gewissheit über Objektstandorte**: Die strenge Option garantiert, dass Objekte sofort nach den Platzierungsanweisungen in der ILM-Regel gespeichert werden.

Nachteile der ausgewogenen und strengen Optionen

Im Vergleich zu Dual Commit haben die ausgewogenen und strengen Optionen einige Nachteile:

- **Längere Client-Ingest**: Client-Ingest-Latenzen können länger sein. Wenn Sie die Optionen „ausgeglichen“ oder „strikt“ verwenden, wird die Meldung „Einspielen erfolgreich“ erst dann an den Client zurückgegeben, wenn alle mit Löschvorgängen kodierten Fragmente oder replizierten Kopien erstellt und gespeichert wurden. Objektdaten werden allerdings sehr wahrscheinlich die endgültige Platzierung viel schneller erreichen.
- **(streng) höhere Aufnahmeraten**: Bei der strengen Option schlägt die Aufnahme fehl, wenn StorageGRID nicht sofort alle in der ILM-Regel angegebenen Kopien erstellen kann. Falls ein benötigter Speicherplatz vorübergehend offline ist oder Netzwerkprobleme auftreten, die zu Verzögerungen beim Kopieren von Objekten zwischen Standorten führen, ist unter Umständen ein hoher Aufnahmefehler zu beobachten.
- **(strict) S3-Multipart-Upload-Platzierungen sind unter Umständen nicht wie erwartet**: Bei strikter Prüfung erwarten Sie, dass Objekte entweder wie in der ILM-Regel beschrieben platziert werden oder dass die Aufnahme fehlschlägt. Bei einem S3-Multipart-Upload wird ILM für jeden aufgenommenen Teil des Objekts und für das gesamte Objekt evaluiert, wenn der mehrteilige Upload abgeschlossen ist. Unter den folgenden Umständen kann dies zu Platzierungen führen, die sich von Ihnen unterscheiden:
  - **Wenn sich ILM ändert, während ein S3-Multipart-Upload im Gange ist**: Da jedes Teil gemäß der Regel platziert wird, die bei der Aufnahme des Teils aktiv ist, entsprechen einige Teile des Objekts möglicherweise nicht den aktuellen ILM-Anforderungen, wenn der mehrteilige Upload abgeschlossen ist. In diesen Fällen schlägt die Aufnahme des Objekts nicht fehl. Stattdessen wird jedes Teil, das nicht korrekt platziert wird, in die Warteschlange für eine erneute ILM-Bewertung eingereiht und später an

den richtigen Speicherort verschoben.

    - **Wenn ILM-Regeln Filter auf Größe**: Bei der Bewertung von ILM für ein Teil filtert StorageGRID die Größe des Teils, nicht die Größe des Objekts. Das bedeutet, dass Teile eines Objekts an Orten gespeichert werden können, die die ILM-Anforderungen für das gesamte Objekt nicht erfüllen. Wenn z. B. eine Regel angibt, dass alle Objekte ab 10 GB auf DC1 gespeichert werden, während alle kleineren Objekte an DC2 gespeichert sind, wird bei Aufnahme jeder 1 GB-Teil eines 10-teiligen mehrteiligen Uploads auf DC2 gespeichert. Wenn ILM für das Objekt bewertet wird, werden alle Teile des Objekts auf DC1 verschoben.

- **(strict) Aufnahme scheitert nicht, wenn Objekt-Tags oder Metadaten aktualisiert werden und neu erforderliche Platzierungen nicht gemacht werden können**: Mit strikter, erwarten Sie, dass Objekte entweder wie in der ILM-Regel beschrieben platziert werden oder dass die Aufnahme fehlschlägt. Wenn Sie jedoch Metadaten oder Tags für ein Objekt aktualisieren, das bereits im Raster gespeichert ist, wird das Objekt nicht erneut aufgenommen. Das bedeutet, dass Änderungen an der Objektplatzierung, die durch die Aktualisierung ausgelöst werden, nicht sofort vorgenommen werden. Änderungen an der Platzierung werden vorgenommen, wenn ILM durch normale ILM-Prozesse im Hintergrund neu bewertet wird. Wenn erforderliche Platzierungsänderungen nicht vorgenommen werden können (z. B. weil ein neu erforderlicher Standort nicht verfügbar ist), behält das aktualisierte Objekt seine aktuelle Platzierung bei, bis die Platzierungsänderungen möglich sind.

Einschränkungen bei Objektplatzierungen mit den ausgewogenen und strengen Optionen

Die ausgewogenen oder strikten Optionen können nicht für ILM-Regeln verwendet werden, die über eine der folgenden Platzierungsanweisungen verfügen:

- Platzierung in einem Cloud-Storage-Pool am Tag 0
- Platzierungen in einem Cloud-Speicherpool, wenn die Regel eine benutzerdefinierte Erstellungszeit als Referenzzeit hat.

Diese Einschränkungen gibt es, weil StorageGRID nicht synchron Kopien in einen Cloud-Storage-Pool erstellen kann und eine benutzerdefinierte Erstellungszeit auf die Gegenwart auflösen könnte.

Wie ILM-Regeln und Konsistenz interagieren, um den Datenschutz zu beeinträchtigen

Sowohl Ihre ILM-Regel als auch Ihre Wahl der Konsistenz beeinflussen die Art und Weise, wie Objekte geschützt werden. Diese Einstellungen können interagieren.

Beispielsweise wirkt sich das für eine ILM-Regel ausgewählte Aufnahmeverhalten auf die anfängliche Platzierung von Objektkopien aus, während die beim Speichern eines Objekts verwendete Konsistenz sich auf die anfängliche Platzierung von Objekt-Metadaten auswirkt. StorageGRID benötigt zur Erfüllung von Clientanforderungen sowohl Zugriff auf die Daten eines Objekts als auch auf die Metadaten. Die Auswahl übereinstimmender Schutzebenen für die Konsistenz und das Aufnahmeverhalten kann zu einer besseren anfänglichen Datensicherung und besser vorhersehbaren Systemantworten führen.

Im Folgenden finden Sie eine kurze Zusammenfassung der Konsistenzwerte, die in StorageGRID verfügbar sind:

- **Alle**: Alle Knoten erhalten sofort Objektmetadaten, oder die Anfrage schlägt fehl.
- **Strong-global**: Objektmetadaten werden sofort an alle Standorte verteilt. Garantierte Konsistenz bei Lese-nach-Schreibvorgängen für alle Client-Anfragen an allen Standorten.
- **Strong-site**: Objektmetadaten werden sofort auf andere Knoten am Standort verteilt. Garantiert Konsistenz bei Lese-nach-Schreibvorgängen für alle Client-Anfragen innerhalb eines Standorts.
- **Read-after-New-write**: Bietet Read-after-write-Konsistenz für neue Objekte und eventuelle Konsistenz für

Objektaktualisierungen. Hochverfügbarkeit und garantierte Datensicherung Empfohlen für die meisten Fälle.

- **Verfügbar**: Bietet eventuelle Konsistenz für neue Objekte und Objekt-Updates. Verwenden Sie für S3-Buckets nur nach Bedarf (z. B. für einen Bucket mit Protokollwerten, die nur selten gelesen werden, oder für HEAD- oder GET-Vorgänge für nicht vorhandene Schlüssel). Nicht unterstützt für S3 FabricPool-Buckets.

> Bevor Sie einen Konsistenzwert auswählen, "Lesen Sie die vollständige Beschreibung der Konsistenz". Vor dem Ändern des Standardwerts sollten Sie die Vorteile und Einschränkungen kennen.

Beispiel für die Interaktion von Konsistenz- und ILM-Regeln

Angenommen, Sie haben ein Grid mit zwei Standorten mit der folgenden ILM-Regel und folgender Konsistenz:

- **ILM-Regel**: Erstellen Sie zwei Objektkopien, eine am lokalen Standort und eine an einem entfernten Standort. Strikte Aufnahme-Verhaltensweise
- **Konsistenz**: Stark-global (Objektmetadaten werden sofort an alle Standorte verteilt).

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

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

Wenn Sie stattdessen dieselbe ILM-Regel und die Konsistenz für starke Standorte verwenden, erhält der Client möglicherweise eine Erfolgsmeldung, nachdem die Objektdaten am Remote-Standort repliziert wurden, jedoch bevor die Objektmetadaten dort verteilt werden. In diesem Fall entspricht die Sicherung von Objektmetadaten nicht dem Schutzniveau für Objektdaten. Falls der lokale Standort kurz nach der Aufnahme verloren geht, gehen Objektmetadaten verloren. Das Objekt kann nicht abgerufen werden.

Die Beziehung zwischen Konsistenz- und ILM-Regeln kann komplex sein. Wenden Sie sich an den NetApp, wenn Sie Hilfe benötigen.

Verwandte Informationen

"Beispiel 5: ILM-Regeln und Richtlinie für striktes Ingest-Verhalten"

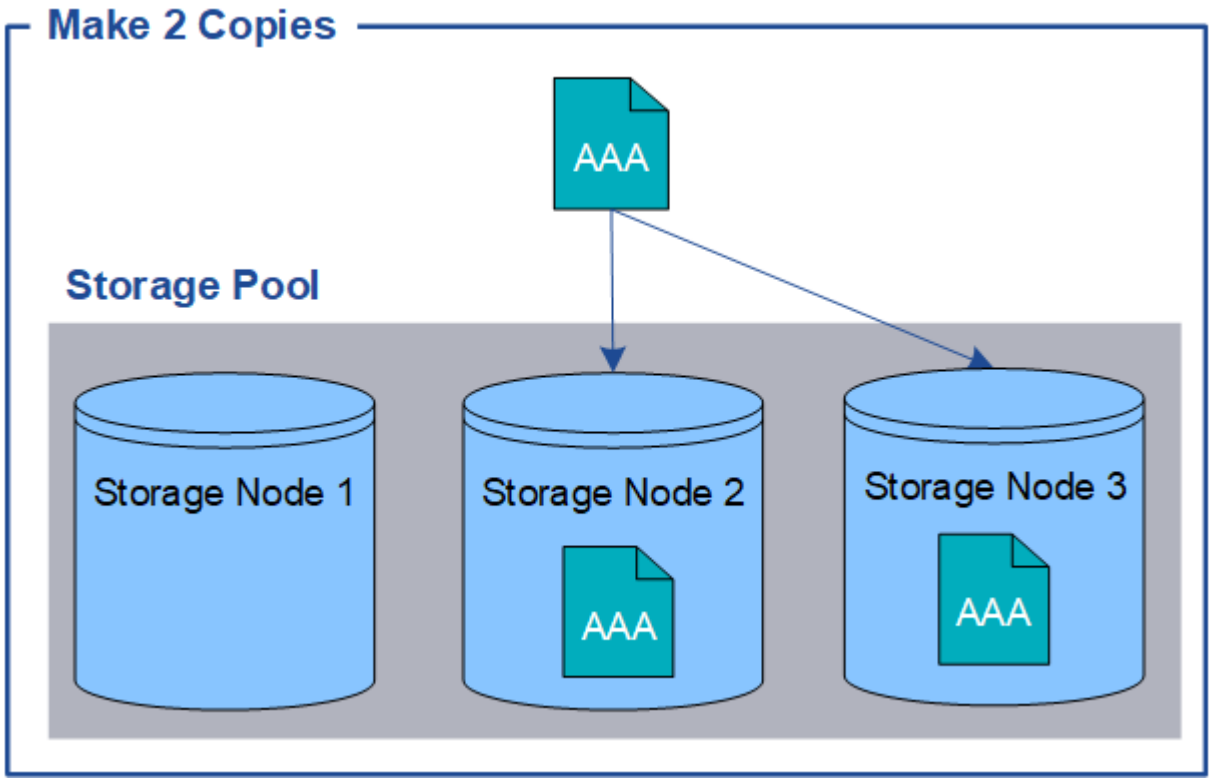
Speicherung von Objekten (Replizierung oder Erasure Coding)

Was ist Replikation?

Die Replizierung ist eine von zwei Methoden, die von StorageGRID zur Speicherung von Objektdaten verwendet werden (bei Erasure Coding handelt es sich um die andere Methode). Wenn Objekte mit einer ILM-Regel übereinstimmen, die Replizierung verwendet, erstellt das System exakte Kopien von Objektdaten und speichert die Kopien auf Storage Nodes.

Wenn Sie eine ILM-Regel zum Erstellen replizierter Kopien konfigurieren, geben Sie an, wie viele Kopien erstellt werden sollen, wo diese Kopien erstellt werden sollen und wie lange die Kopien an jedem Standort gespeichert werden sollen.

Im folgenden Beispiel gibt die ILM-Regel an, dass zwei replizierte Kopien jedes Objekts in einem Storage-Pool mit drei Storage-Nodes platziert werden.



Wenn StorageGRID Objekte mit dieser Regel übereinstimmt, werden zwei Kopien des Objekts erstellt, wobei jede Kopie auf einem anderen Storage-Node im Storage-Pool platziert wird. Die beiden Kopien können auf zwei der drei verfügbaren Storage-Nodes platziert werden. In diesem Fall wurden in der Regel Objektkopien auf Speicherknoten 2 und 3 platziert. Da es zwei Kopien gibt, kann das Objekt abgerufen werden, wenn einer der Nodes im Speicherpool ausfällt.

> StorageGRID kann nur eine replizierte Kopie eines Objekts auf einem beliebigen Storage Node speichern. Wenn Ihr Grid drei Storage-Nodes enthält und Sie eine ILM-Regel mit 4 Kopien erstellen, werden nur drei Kopien erstellt: Eine Kopie für jeden Storage-Node. Die Warnung **ILM-Platzierung unerreichbar** wird ausgelöst, um anzuzeigen, dass die ILM-Regel nicht vollständig angewendet werden konnte.

Verwandte Informationen

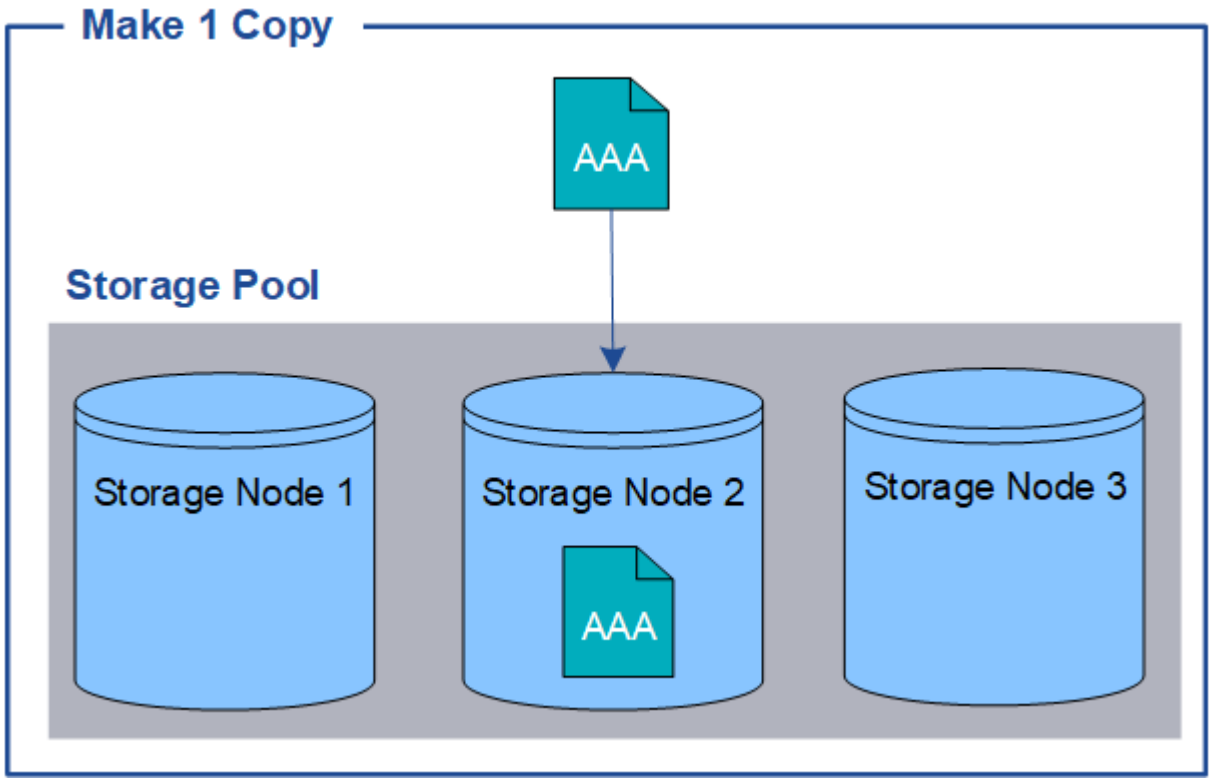
- "Was ist Erasure Coding"
- "Was ist ein Speicherpool"
- "Schutz vor Standortausfällen durch Replizierung und Erasure Coding"

Warum sollten Sie keine Replizierung mit nur einer Kopie verwenden

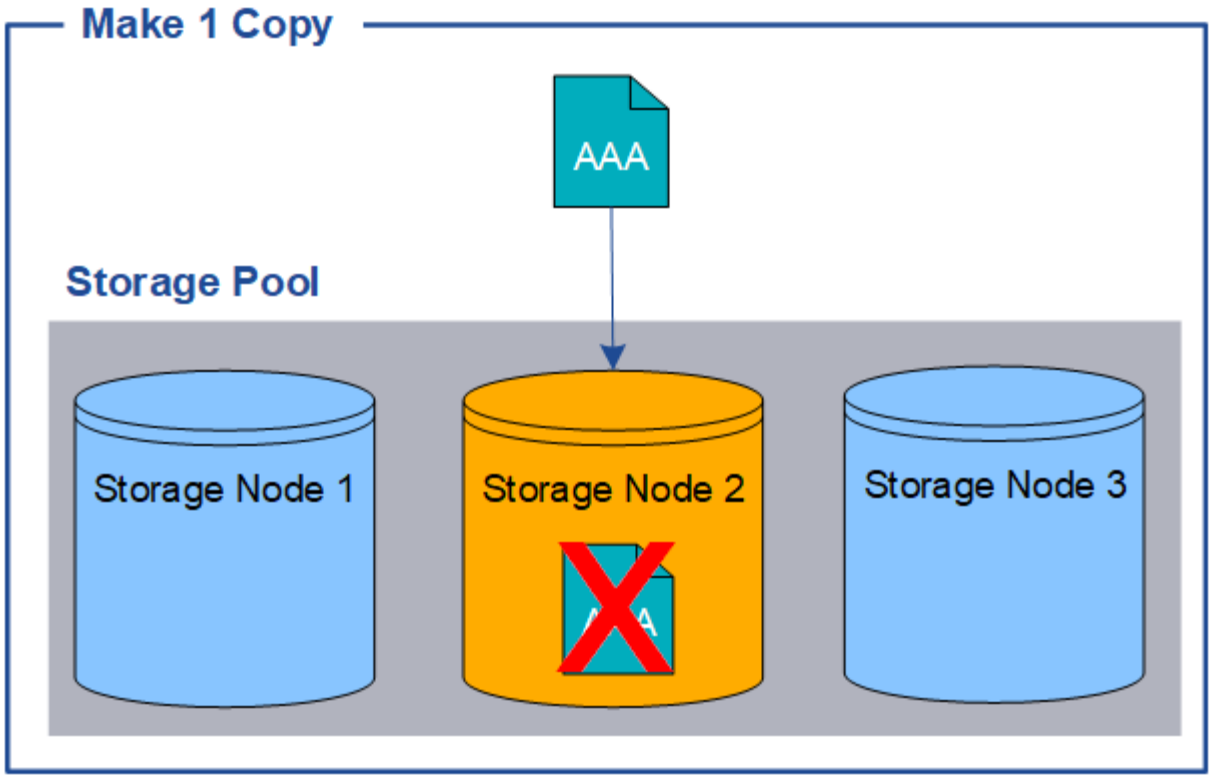
Beim Erstellen einer ILM-Regel zum Erstellen replizierter Kopien sollten Sie immer mindestens zwei Kopien für einen beliebigen Zeitraum in den Anweisungen zur Platzierung angeben.

Verwenden Sie keine ILM-Regel, die nur eine replizierte Kopie für einen beliebigen Zeitraum erstellt. Wenn nur eine replizierte Kopie eines Objekts vorhanden ist, geht dieses Objekt verloren, wenn ein Speicherknoten ausfällt oder einen beträchtlichen Fehler hat. Während Wartungsarbeiten wie Upgrades verlieren Sie auch vorübergehend den Zugriff auf das Objekt.

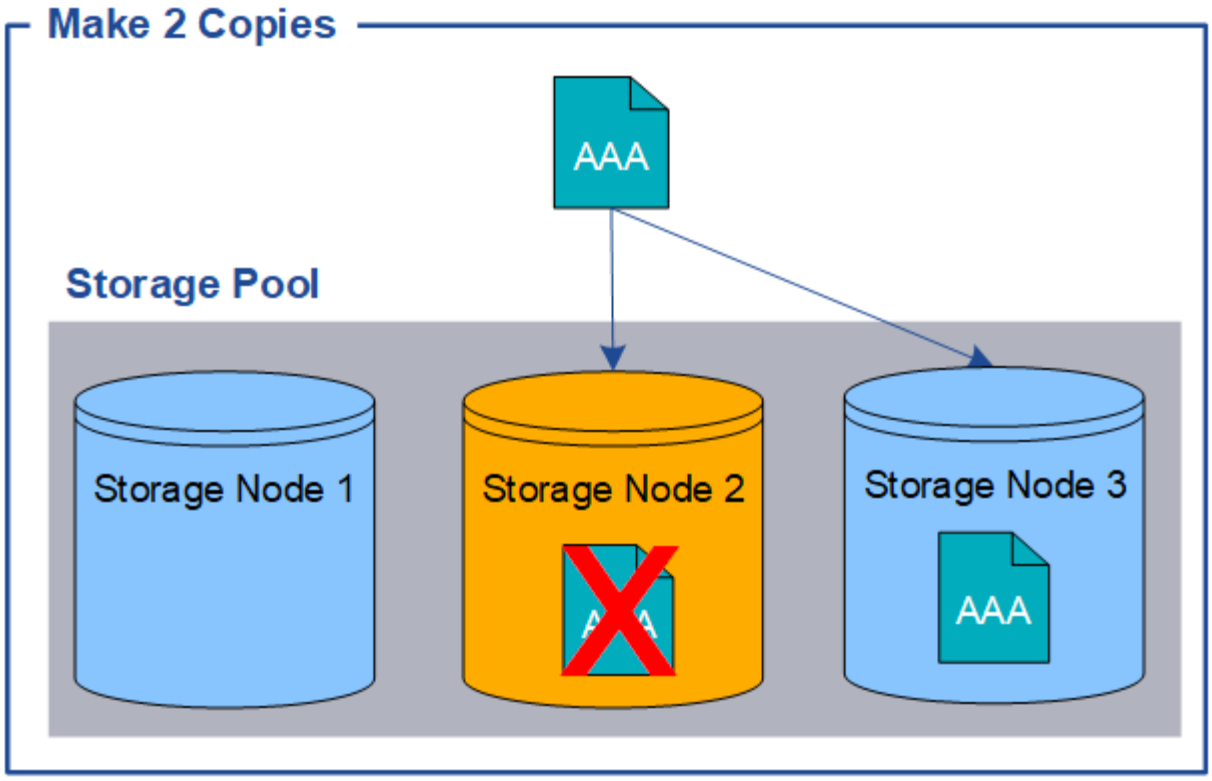
Im folgenden Beispiel gibt die ILM-Regel „1 Kopie erstellen“ an, dass eine replizierte Kopie eines Objekts in einem Speicherpool platziert wird, der drei Storage-Nodes enthält. Wenn ein Objekt aufgenommen wird, das dieser Regel entspricht, platziert StorageGRID eine einzelne Kopie auf nur einem Storage-Node.



Wenn eine ILM-Regel nur eine replizierte Kopie eines Objekts erstellt, ist der Zugriff auf das Objekt möglich, wenn der Storage-Node nicht verfügbar ist. In diesem Beispiel verlieren Sie vorübergehend den Zugriff auf das Objekt AAA, wenn Storage Node 2 offline ist, z. B. während eines Upgrades oder eines anderen Wartungsverfahrens. Sie verlieren das Objekt AAA vollständig, wenn Storage Node 2 ausfällt.



Um den Verlust von Objektdaten zu vermeiden, sollten immer mindestens zwei Kopien aller Objekte erstellt werden, die durch die Replizierung gesichert werden sollen. Wenn zwei oder mehr Kopien vorhanden sind, können Sie weiterhin auf das Objekt zugreifen, wenn ein Storage-Node ausfällt oder offline geht.



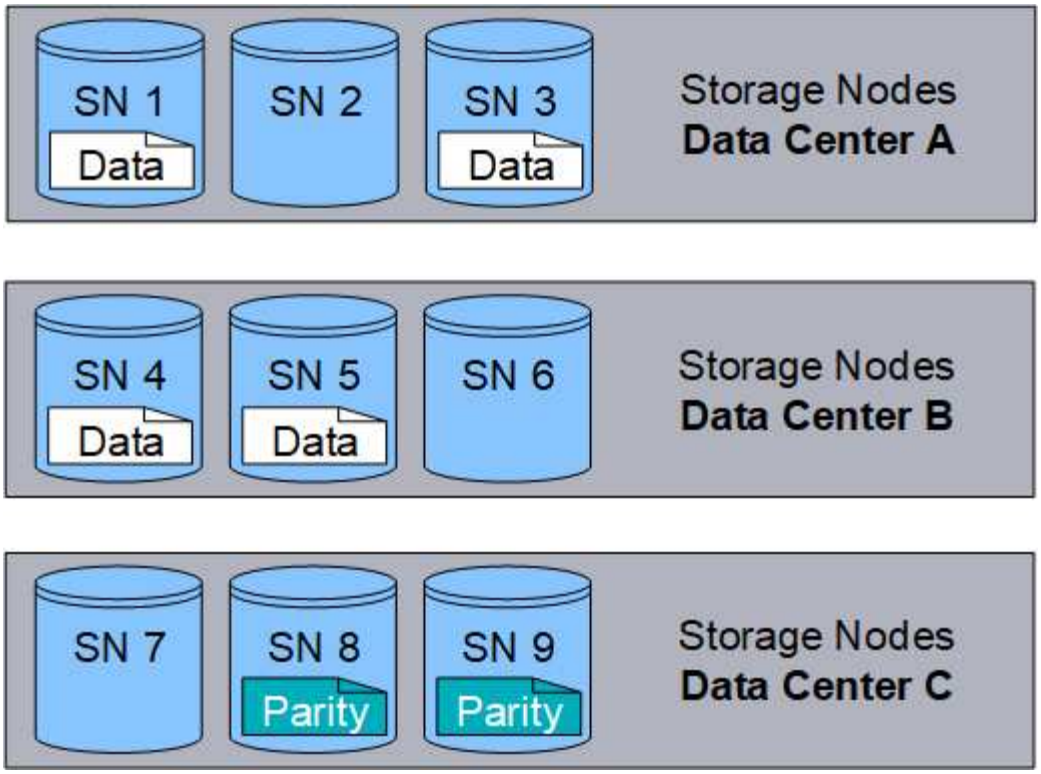
Was ist Erasure Coding?

Erasure Coding ist eine von zwei Methoden, die StorageGRID zum Speichern von Objektdaten verwendet (bei der Replizierung handelt es sich um die andere Methode). Wenn Objekte mit einer ILM-Regel übereinstimmen, die Erasure Coding verwendet, werden diese Objekte in Datenfragmente geteilt, weitere Paritätsfragmente werden berechnet und jedes Fragment wird auf einem anderen Storage Node gespeichert.

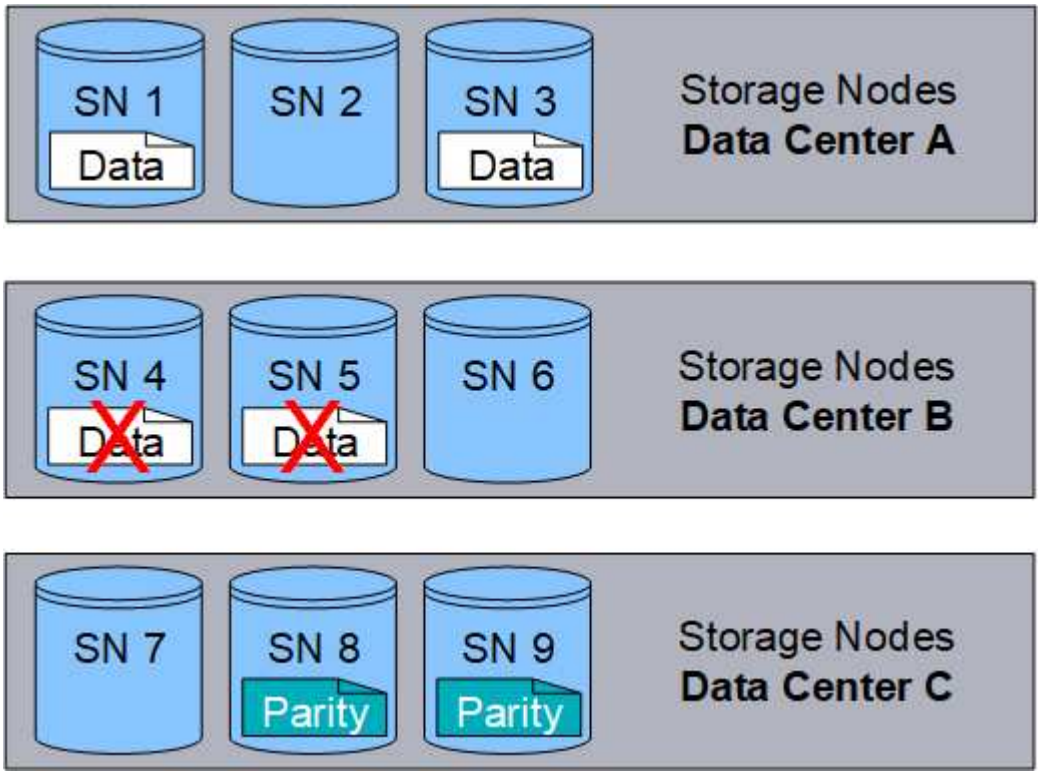
Wenn auf ein Objekt zugegriffen wird, wird es anhand der gespeicherten Fragmente neu zusammengesetzt. Wenn ein Daten oder ein Paritätsfragment beschädigt wird oder verloren geht, kann der Algorithmus zur Fehlerkorrektur dieses Fragment mit einer Teilmenge der verbleibenden Daten und Paritätsfragmente neu erstellen.

Beim Erstellen von ILM-Regeln erstellt StorageGRID Profile zur Einhaltung von Datenkonsistenz, die diese Regeln unterstützen. Sie können eine Liste von Erasure-Coding-Profilen anzeigen, "Umbenennen eines Profils für die Erasure Coding", oder "Deaktivieren Sie ein Erasure Coding-Profil, wenn es derzeit nicht in ILM-Regeln verwendet wird".

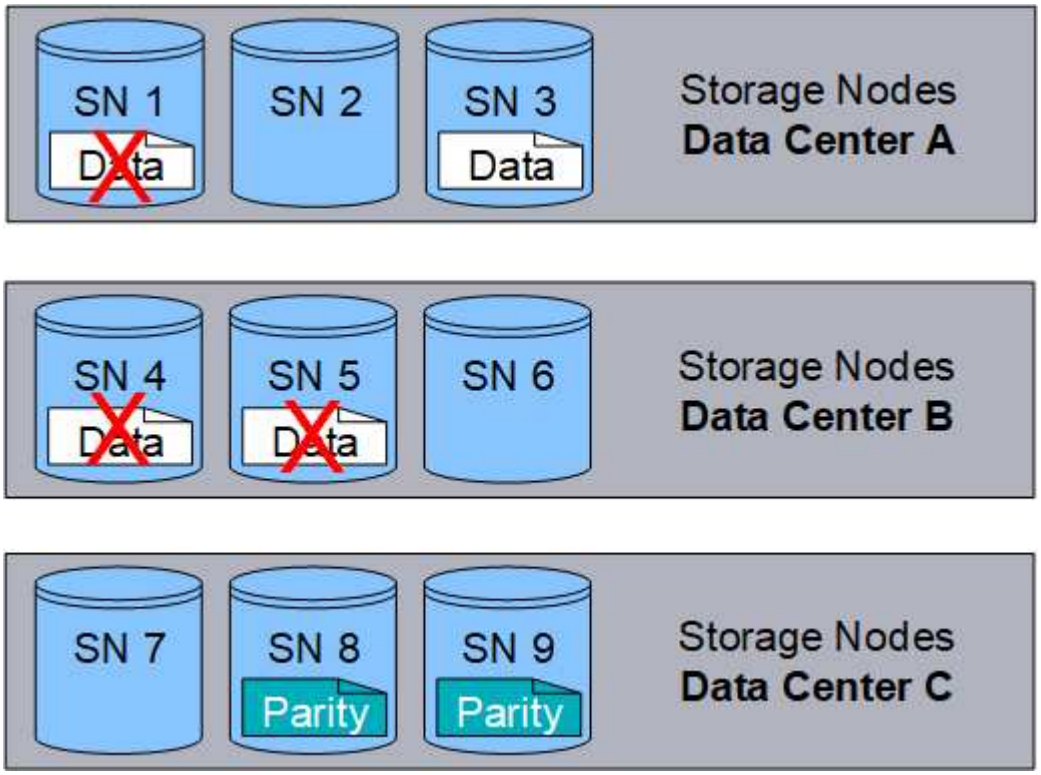
Im folgenden Beispiel wird der Algorithmus zur Einhaltung von Datenkonsistenz (Erasure Coding) für Objektdaten dargestellt. In diesem Beispiel verwendet die ILM-Regel ein 4+2-Schema zur Einhaltung von Datenkonsistenz. Jedes Objekt wird in vier gleiche Datenfragmente geteilt und aus den Objektdaten werden zwei Paritätsfragmente berechnet. Jedes der sechs Fragmente wird auf einem anderen Node über drei Datacenter-Standorte gespeichert, um Daten bei Node-Ausfällen oder Standortausfällen zu sichern.



Das 4+2 Erasure Coding-Schema kann auf verschiedene Weise konfiguriert werden. Sie können beispielsweise einen Speicherpool mit einem Standort konfigurieren, der sechs Storage-Nodes enthält. Für "Schutz vor Standortausfällen"können Sie einen Speicherpool verwenden, der drei Standorte mit drei Storage-Nodes an jedem Standort enthält. Ein Objekt kann abgerufen werden, solange vier der sechs Fragmente (Daten oder Parität) verfügbar sind. Bis zu zwei Fragmente können ohne Verlust der Objektdaten verloren gehen. Wenn ein ganzer Standort verloren geht, kann das Objekt dennoch abgerufen oder repariert werden, solange alle anderen Fragmente zugänglich bleiben.



Wenn mehr als zwei Speicherknoten verloren gehen, kann das Objekt nicht abgerufen werden.



Verwandte Informationen

- "Was ist Replikation"
- "Was ist ein Speicherpool"
- "Was sind Erasure Coding-Systeme"
- "Umbenennen eines Profils für die Erasure Coding"
- "Deaktivieren Sie ein Erasure Coding-Profil"

Was sind Erasure Coding-Systeme?

Erasure Coding steuert die Anzahl von Datenfragmenten und die Anzahl der Parity-Fragmente für jedes Objekt.

Wenn Sie eine ILM-Regel erstellen oder bearbeiten, wählen Sie ein verfügbares Schema für die Einhaltung von Datenkonsistenz aus. StorageGRID erstellt automatisch Schemata für die Einhaltung von Datenkonsistenz anhand der Anzahl der Storage-Nodes und Standorte des Storage-Pools, die Sie verwenden möchten.

Datensicherung

Das StorageGRID-System verwendet den Reed-Solomon-Erasure-Coding-Algorithmus. Der Algorithmus unterteilt ein Objekt in `k` Datenfragmente und berechnet `m` Paritätsfragmente.

Die `k + m = n` Fragmente werden über Storage-Nodes verteilt `n`, um folgende Datensicherungsmaßnahmen zu ermöglichen:

- Um ein Objekt abzurufen oder zu reparieren, `k` werden Fragmente benötigt.
- Ein Objekt kann verlorene oder beschädigte Fragmente erhalten `m`. Je höher der Wert von `m`, desto höher

die Ausfalltoleranz.

Die beste Datensicherung wird durch das Erasure Coding-Schema mit der höchsten Ausfalltoleranz für Nodes oder Volumes innerhalb eines Storage-Pools erreicht.

Storage Overhead

Der Speicher-Overhead eines Erasure-Coding-Schemas wird berechnet, indem die Anzahl der Paritäts-Fragmente (`m`durch die Anzahl der Datenfragmente geteilt wird (`k`). Der Storage Overhead lässt sich ermitteln, wie viel Festplattenspeicher jedes mit Erasure-Coding-Objekt benötigt:

*disk space = object size + (object size * storage overhead)*

Wenn Sie beispielsweise ein Objekt mit 10 MB unter Verwendung des Schemas von 4+2 speichern (mit einem Mehraufwand von 50 %), verbraucht das Objekt 15 MB Grid Storage. Wenn Sie dasselbe 10 MB große Objekt mit dem Schema 6+2 speichern (mit einem Mehraufwand von 33 %), verbraucht das Objekt etwa 13.3 MB.

Wählen Sie das Erasure Coding-Schema mit dem niedrigsten Gesamtwert `k+m`, der Ihren Anforderungen entspricht. Erasure Coding-Schemata mit einer geringeren Anzahl von Fragmenten sind aus folgenden Gründen recheneffizienter:

- Pro Objekt werden weniger Fragmente erstellt und verteilt (oder abgerufen)
- Sie zeigen eine bessere Performance, da die Fragmentgröße größer ist
- Das Hinzufügen von weniger Nodes in einem ist möglich "Erweiterung, wenn mehr Storage benötigt wird"

Richtlinien für Speicherpools

Verwenden Sie bei der Auswahl des Speicherpools für eine Regel, die eine Kopie mit Verfahren zur Fehlerkorrektur erstellt, die folgenden Richtlinien für Speicherpools:

- Der Speicherpool muss drei oder mehr Standorte oder exakt einen Standort umfassen.

  > Sie können kein Erasure Coding verwenden, wenn der Storage-Pool zwei Standorte umfasst.

  - Verfahren zur Einhaltung von Datenkonsistenz für Storage-Pools mit drei oder mehr Standorten
  - Verfahren zur Einhaltung von Datenkonsistenz für Storage-Pools an einem Standort
- Verwenden Sie keinen Speicherpool, der den Standort „Alle Standorte“ umfasst.
- Der Speicherpool sollte mindestens Storage Nodes enthalten *k+m* `+1`, die Objektdaten speichern können.

  > Storage-Nodes können während der Installation so konfiguriert werden, dass sie nur Objektmetadaten und keine Objektdaten enthalten. Weitere Informationen finden Sie unter "Typen von Storage-Nodes".

  Die Mindestanzahl der erforderlichen Storage-Nodes ist `k+m`. Durch mindestens einen zusätzlichen Storage-Node können jedoch Ingest- oder ILM-Backlogs verhindert werden, wenn ein erforderlicher Storage-Node vorübergehend nicht verfügbar ist.

Verfahren zur Einhaltung von Datenkonsistenz für Storage-Pools mit drei oder mehr Standorten

Die folgende Tabelle beschreibt die von StorageGRID derzeit unterstützten Erasure Coding-Schemata für

Storage-Pools, die drei oder mehr Standorte umfassen. Alle diese Maßnahmen bieten einen Standortausfallschutz. Ein Standort kann verloren gehen, und das Objekt ist weiterhin verfügbar.

Für Erasure Coding-Schemata, die Schutz vor Standortausfällen bieten, übersteigt die empfohlene Anzahl von Storage-Nodes im Speicherpool `k+m +1`, da für jeden Standort mindestens drei Storage-Nodes erforderlich sind.

Schema zur Einhaltung von Datenkonsistenz (Erasure Coding) (*k+m*)	Mindestanzahl der bereitgestellten Standorte	Empfohlene Anzahl von Storage-Nodes an jedem Standort	Insgesamt empfohlene Anzahl von Storage-Nodes	Schutz vor Standortausfällen?	Storage Overhead
4+2	3	3	9	Ja.	50 % erreicht
6+2	4	3	12	Ja.	33 % erreicht
8+2	5	3	15	Ja.	25 % erreicht
6+3	3	4	12	Ja.	50 % erreicht
9+3	4	4	16	Ja.	33 % erreicht
2+1	3	3	9	Ja.	50 % erreicht
4+1	5	3	15	Ja.	25 % erreicht
6+1	7	3	21	Ja.	17 % erreicht
7+5	3	5	15	Ja.	71 % erreicht

StorageGRID erfordert mindestens drei Storage-Nodes pro Standort. Für die Verwendung des Schemas 7+5 benötigt jeder Standort mindestens vier Speicherknoten. Es wird empfohlen, fünf Storage-Nodes pro Standort zu verwenden.

Bei der Auswahl eines Löschungsschemas, das Standortschutz bietet, sollte die relative Bedeutung der folgenden Faktoren in Einklang gestellt werden:

- **Anzahl der Fragmente**: Leistung und Expansionsflexibilität sind im Allgemeinen besser, wenn die Gesamtzahl der Fragmente geringer ist.
- **Fehlertoleranz**: Die Fehlertoleranz wird durch mehr Paritätssegmente erhöht (d.h. wenn `m` einen höheren Wert hat).
- **Netzwerkverkehr**: Bei der Wiederherstellung nach Ausfällen erzeugt die Verwendung eines Schemas mit mehr Fragmenten (also einer höheren Summe für `k+m`) mehr Netzwerkverkehr.
- **Storage Overhead**: Bei Systemen mit höherem Overhead wird mehr Speicherplatz pro Objekt benötigt.

Wenn Sie beispielsweise zwischen einem Schema 4+2 und dem Schema 6+3 (mit jeweils 50 % Storage Overhead) entscheiden, wählen Sie das Schema 6+3 aus, wenn eine zusätzliche Fehlertoleranz erforderlich ist. Wählen Sie das Schema 4+2 aus, wenn die Netzwerkressourcen begrenzt sind. Wenn alle anderen

Faktoren gleich sind, wählen Sie 4+2 aus, da die Gesamtzahl der Fragmente geringer ist.

Wenn Sie sich nicht sicher sind, welches Schema Sie verwenden möchten, wählen Sie 4+2 oder 6+3 aus, oder wenden Sie sich an den technischen Support.

Verfahren zur Einhaltung von Datenkonsistenz für Storage-Pools an einem Standort

Ein Storage-Pool an einem Standort unterstützt alle Erasure Coding-Schemata, die für drei oder mehr Standorte definiert sind, sofern der Standort über ausreichend Storage-Nodes verfügt.

Die Mindestanzahl der erforderlichen Storage-Nodes ist `k+m`, jedoch wird ein Speicherpool mit `k+m +1` Storage-Nodes empfohlen. Zum Beispiel erfordert das Verfahren zur Einhaltung von Datenkonsistenz (Erasure Coding) 2+1 einen Speicherpool mit mindestens drei Storage-Nodes, es werden jedoch vier Storage-Nodes empfohlen.

Schema zur Einhaltung von Datenkonsistenz (Erasure Coding) (*k+m*)	Mindestanzahl Storage-Nodes	Empfohlene Anzahl von Storage-Nodes	Storage Overhead
4+2	6	7	50 % erreicht
6+2	8	9	33 % erreicht
8+2	10	11	25 % erreicht
6+3	9	10	50 % erreicht
9+3	12	13	33 % erreicht
2+1	3	4	50 % erreicht
4+1	5	6	25 % erreicht
6+1	7	8	17 % erreicht
7+5	12	13	71 % erreicht

Vor- und Nachteile sowie Anforderungen für Erasure Coding

Bevor Sie sich entscheiden, ob Sie zum Schutz von Objektdaten mithilfe von Replizierungs- oder Erasure Coding vor Verlust schützen möchten, sollten Sie die Vorteile und Nachteile sowie die Anforderungen für Verfahren zur Einhaltung von Datenkonsistenz kennen.

Vorteile von Erasure Coding

Im Vergleich zur Replizierung bietet das Verfahren zur Einhaltung von Datenkonsistenz (Erasure Coding) verbesserte Zuverlässigkeit, Verfügbarkeit und Storage-Effizienz.

- **Zuverlässigkeit**: Die Zuverlässigkeit wird in Bezug auf Fehlertoleranz gemessen - das ist die Anzahl der gleichzeitigen Ausfälle, die ohne Datenverlust aufrechterhalten werden können. Mithilfe der Replizierung werden mehrere identische Kopien auf unterschiedlichen Nodes und über mehrere Standorte hinweg gespeichert. Bei der Einhaltung von Datenkonsistenz wird ein Objekt in Daten- und Paritätsfragmente codiert und über viele Nodes und Standorte verteilt. Diese Verteilung bietet Schutz vor Standort- und Node-Ausfällen. Im Vergleich zur Replizierung bietet Erasure Coding eine höhere Zuverlässigkeit bei vergleichbaren Storage-Kosten.
- **Verfügbarkeit**: Verfügbarkeit kann definiert werden als die Möglichkeit, Objekte abzurufen, wenn Speicherknoten ausfallen oder unzugänglich werden. Im Vergleich zur Replizierung bietet Erasure Coding eine höhere Verfügbarkeit bei vergleichbaren Storage-Kosten.
- **Storage-Effizienz**: Für ein ähnliches Maß an Verfügbarkeit und Zuverlässigkeit benötigen die durch das Erasure Coding geschützten Objekte weniger Speicherplatz als die gleichen Objekte, wenn sie durch Replikation geschützt sind. Beispielsweise belegt ein 10-MB-Objekt, das an zwei Standorten repliziert wird, 20 MB Festplattenspeicher (zwei Kopien), während ein Objekt, das zur Fehlerkorrektur codiert wird, an drei Standorten mit einem 6+3-Erasure-Coding-Schema nur 15 MB Festplattenspeicher belegt.

> ⓘ Der Festplattenspeicher für Objekte, die mit Erasure-Coding-Verfahren codiert wurden, wird als Objektgröße und als Storage Overhead berechnet. Der prozentuale Storage Overhead entspricht der Anzahl der Paritätsfragmente, geteilt durch die Anzahl an Datenfragmenten.

Nachteile des Erasure Coding

Im Vergleich zur Replizierung hat das Verfahren zur Einhaltung von Datenkonsistenz folgende Nachteile:

- Je nach Erasure Coding-Schema wird eine erhöhte Anzahl von Storage-Nodes und -Standorten empfohlen. Wenn Sie hingegen Objektdaten replizieren, benötigen Sie pro Kopie nur einen Storage Node. Siehe "Verfahren zur Einhaltung von Datenkonsistenz für Storage-Pools mit drei oder mehr Standorten" und "Verfahren zur Einhaltung von Datenkonsistenz für Storage-Pools an einem Standort".
- Höhere Kosten und Komplexität der Storage-Erweiterungen. Um eine Implementierung zu erweitern, bei der Replizierung verwendet wird, fügen Sie an jedem Ort, an dem Objektkopien erstellt werden, Storage-Kapazitäten hinzu. Um eine Implementierung zu erweitern, bei der Erasure Coding zum Einsatz kommt, müssen Sie sowohl das verwendete Verfahren zur Einhaltung von Datenkonsistenz als auch die Kapazität vorhandener Storage-Nodes in Betracht ziehen. Wenn Sie beispielsweise warten, bis die vorhandenen Nodes zu 100 % voll sind, müssen Sie mindestens Storage-Nodes hinzufügen `k+m`. Wenn Sie jedoch erweitern, wenn vorhandene Nodes zu 70 % voll sind, können Sie pro Standort zwei Nodes hinzufügen und gleichzeitig die nutzbare Storage-Kapazität maximieren. Weitere Informationen finden Sie unter "Erweitern Sie Storage-Kapazität für Objekte, die nach dem Erasure-Coding-Verfahren codiert wurden".
- Wenn Erasure Coding über geografisch verteilte Standorte hinweg verwendet wird, erhöht sich die Latenzzeiten beim Abruf. Die Objektfragmente für ein Objekt, das mit Erasure Coding versehen ist und über Remote-Standorte verteilt ist, benötigen über WAN-Verbindungen länger für den Abruf als ein Objekt, das repliziert und lokal verfügbar ist (der gleiche Standort, mit dem der Client eine Verbindung herstellt).
- Bei Verwendung von Erasure Coding für geografisch verteilte Standorte kommt ein höherer WAN-Netzwerkverkehr für Abrufvorgänge und Reparaturen zum Einsatz, insbesondere bei häufig abgerufenen Objekten oder bei Objektreparaturen über WAN-Netzwerkverbindungen.
- Wenn Sie standortübergreifend Erasure Coding verwenden, nimmt der maximale Objektdurchsatz ab, da die Netzwerklatenz zwischen Standorten zunimmt. Diese Abnahme ist auf die entsprechende Abnahme des TCP-Netzwerkdurchsatzes zurückzuführen, was sich darauf auswirkt, wie schnell das StorageGRID-System Objektfragmente speichern und abrufen kann.
- Höhere Auslastung von Computing-Ressourcen:

Wann sollte das Erasure Coding verwendet werden

Das Verfahren zur Einhaltung von Datenkonsistenz eignet sich am besten für folgende Anforderungen:

- Objekte größer als 1 MB.

> Das Verfahren zur Einhaltung von Datenkonsistenz eignet sich am besten für Objekte mit einer Größe von mehr als 1 MB. Verwenden Sie kein Erasure Coding für Objekte, die kleiner als 200 KB sind, um zu vermeiden, dass man sehr kleine Fragmente, die zur Fehlerkorrektur codiert wurden, managen muss.

- Langfristige oder kalte Storage-Lösung für selten abgerufene Inhalte
- Hohe Datenverfügbarkeit und -Zuverlässigkeit
- Schutz vor vollständigem Standort- und Node-Ausfall.
- Storage-Effizienz:
- Implementierungen an einem einzigen Standort, die eine effiziente Datensicherung benötigen und nur eine einzige Kopie mit Verfahren zur Einhaltung von Datenkonsistenz (Erasure Coding) als mehrere replizierte Kopien benötigen
- Implementierungen an mehreren Standorten, bei denen die Latenz zwischen den Standorten weniger als 100 ms beträgt

Wie die Aufbewahrung von Objekten bestimmt wird

StorageGRID bietet sowohl Grid-Administratoren als auch einzelnen Mandantenbenutzer Optionen, um die Speicherdauer von Objekten festzulegen. Im Allgemeinen haben alle von einem Mandantenbenutzer bereitgestellten Aufbewahrungsanweisungen Vorrang vor den Aufbewahrungsanweisungen, die vom Grid-Administrator bereitgestellt werden.

Wie Mandantenbenutzer die Aufbewahrung von Objekten steuern

Mandantenbenutzer können diese Methoden verwenden, um zu steuern, wie lange ihre Objekte in StorageGRID gespeichert werden:

- Wenn die globale S3-Objektsperrung für das Grid aktiviert ist, können Benutzer von S3-Mandanten Buckets erstellen, für die S3-Objektsperrung aktiviert ist, und dann für jeden Bucket einen **Standardaufbewahrungszeitraum** auswählen.
- Wenn die globale S3-Objektsperreneinstellung für das Grid aktiviert ist, können Nutzer von S3-Mandanten Buckets erstellen, deren S3-Objektsperre aktiviert ist. Anschließend können sie über die S3-REST-API Aufbewahrungseinstellungen für jede zu diesem Bucket hinzugefügte Objektversion festlegen.
  - Eine Objektversion, die sich unter einem Legal Hold befindet, kann mit keiner Methode gelöscht werden.
  - Bevor das Aufbewahrungsdatum einer Objektversion erreicht ist, kann diese Version nicht mit einer Methode gelöscht werden.
  - Objekte in Buckets mit aktivierter S3 Object Lock werden von ILM „Forever“ aufbewahrt. Nachdem jedoch eine Aufbewahrungsfrist erreicht ist, kann eine Objektversion durch eine Client-Anfrage oder den Ablauf des Bucket-Lebenszyklus gelöscht werden. Siehe "Objekte managen mit S3 Object Lock".
- Benutzer von S3-Mandanten können ihren Buckets eine Lifecycle-Konfiguration hinzufügen, für die eine Ablaufaktion festgelegt ist. Wenn ein Bucket-Lebenszyklus vorhanden ist, speichert StorageGRID ein Objekt, bis das Datum oder die Anzahl der Tage, die im Verfallsvorgang angegeben sind, erreicht ist, es sei

denn, der Client löscht das Objekt zuerst. Siehe "S3-Lebenszykluskonfiguration erstellen".

- Ein S3-Client kann eine Anfrage zum Löschen von Objekten ausgeben. StorageGRID priorisiert Löschanfragen von Clients immer über den S3-Bucket-Lebenszyklus oder ILM, wenn sie bestimmen, ob ein Objekt gelöscht oder aufbewahrt werden soll.

Grid-Administratoren steuern die Objektaufbewahrung

Grid-Administratoren können diese Methoden zur Steuerung der Objektaufbewahrung verwenden:

- Legen Sie für jeden Mandanten eine maximale Aufbewahrungsfrist für S3 Object Lock fest. Anschließend können Mandantenbenutzer für jeden ihrer Buckets einen standardmäßigen Aufbewahrungszeitraum festlegen. Der maximale Aufbewahrungszeitraum wird auch für neu aufgenommene Objekte für diesen Bucket durchgesetzt (das Aufbewahrungsdatum eines Objekts).
- Erstellen Sie eine ILM-Platzierungsanweisung, um zu steuern, wie lange Objekte gespeichert werden. Wenn Objekte mit einer ILM-Regel abgeglichen werden, speichert StorageGRID diese Objekte bis zum letzten Zeitraum der ILM-Regel verstrichen ist. Objekte werden auf unbestimmte Zeit aufbewahrt, wenn für die Platzierungsanweisungen „immer“ angegeben wird.
- Unabhängig davon, wer die Aufbewahrungsdauer von Objekten festlegt, legen ILM-Einstellungen fest, welche Typen von Objektkopien (repliziert oder Erasure-coded) gespeichert werden und wo sich die Kopien befinden (Storage Nodes oder Cloud Storage Pools).

Interaktion von S3-Bucket-Lebenszyklus und ILM

Wenn ein S3-Bucket-Lebenszyklus konfiguriert ist, überschreiben die Lifecycle-Ablaufaktionen die ILM-Richtlinie für Objekte, die mit dem Lifecycle-Filter übereinstimmen. Aus diesem Grund kann ein Objekt auch dann im Grid verbleiben, wenn ILM-Anweisungen zum Auflegen des Objekts verfallen sind.

Beispiele für die Aufbewahrung von Objekten

Die folgenden Beispiele sollten zur besseren Übersicht über die Interaktionen zwischen S3 Objektsperre, Bucket-Lebenszykluseinstellungen, Clientlöschanforderungen und ILM verwendet werden.

Beispiel 1: S3-Bucket-Lebenszyklus hält Objekte länger als ILM

ILM

Speichern von zwei Kopien für 1 Jahr (365 Tage)

Bucket-Lebenszyklus

Verfalle Objekte in 2 Jahren (730 Tage)

Ergebnis

StorageGRID speichert das Objekt 730 Tage lang. StorageGRID verwendet die Bucket-Lifecycle-Einstellungen, um zu bestimmen, ob ein Objekt gelöscht oder aufbewahrt werden soll.

> Wenn im Bucket-Lebenszyklus angegeben wird, dass Objekte länger aufbewahrt werden sollen als durch ILM angegeben, verwendet StorageGRID beim Bestimmen der Anzahl und des Typs der zu speichernden Kopien weiterhin die Anweisungen zur ILM-Platzierung. In diesem Beispiel werden zwei Kopien des Objekts von 366 bis 730 Tagen im StorageGRID gespeichert.

Beispiel 2: S3-Bucket-Lebenszyklus läuft Objekte vor ILM ab

ILM

Speichern von zwei Kopien für 2 Jahre (730 Tage)

Bucket-Lebenszyklus

Verfalle Objekte in 1 Jahr (365 Tage)

Ergebnis

StorageGRID löscht beide Kopien des Objekts nach Tag 365.

Beispiel 3: Beim Löschen von Clients wird der Bucket-Lebenszyklus und ILM überschrieben

ILM

„Ewig“ Speicherung von zwei Kopien auf Storage-Nodes

Bucket-Lebenszyklus

Verfalle Objekte in 2 Jahren (730 Tage)

Anforderung zum Löschen des Clients

Ausgestellt am 400. Tag

Ergebnis

StorageGRID löscht beide Kopien des Objekts am Tag 400 als Antwort auf die Anforderung zum Löschen des Clients.

Beispiel 4: S3 Object Lock überschreibt die Anforderung zum Löschen des Clients

S3-Objektsperre

Aufbewahrung bis zum Datum für eine Objektversion ist 2026-03-31. Eine gesetzliche Aufbewahrungspflichten sind nicht in Kraft.

Kompatible ILM-Regel

„Ewig“ Speicherung von zwei Kopien auf Storage-Nodes

Anforderung zum Löschen des Clients

Herausgegeben am 2024-03-31

Ergebnis

StorageGRID wird die Objektversion nicht löschen, da die Aufbewahrung bis zum Datum noch zwei Jahre entfernt ist.

So werden Objekte gelöscht

StorageGRID kann Objekte entweder als direkte Antwort auf eine Client-Anfrage oder automatisch aufgrund des Ablaufs eines S3-Bucket-Lebenszyklus oder der Anforderungen der ILM-Richtlinie löschen. Wenn Sie verstehen, auf welche Weise Objekte gelöscht werden können und wie StorageGRID Löschanfragen verarbeitet, können Sie Objekte effizienter managen.

StorageGRID kann Objekte auf eine von zwei Methoden löschen:

- Synchrones Löschen: Erhält StorageGRID eine Client-Löschanforderung, werden alle Objektkopien sofort

entfernt. Der Client wird informiert, dass das Löschen nach dem Entfernen der Kopien erfolgreich war.

- Objekte werden zum Löschen in die Warteschlange eingereiht: Wenn StorageGRID eine Löschanforderung empfängt, wird das Objekt zum Löschen in die Warteschlange verschoben. Der Client wird umgehend darüber informiert, dass das Löschen erfolgreich war. Objektkopien werden später durch ILM-Verarbeitung im Hintergrund entfernt.

Beim Löschen von Objekten verwendet StorageGRID die Methode, die das Löschen der Performance optimiert, mögliche Rückprotokolle für das Löschen minimiert und Speicherplatz am schnellsten freigegeben wird.

Die Tabelle fasst zusammen, wann StorageGRID die einzelnen Methoden verwendet.

Löschmethode	Wenn verwendet
Objekte werden zum Löschen in eine Warteschlange eingereiht	Wenn **eine** der folgenden Bedingungen zutrifft: • Das automatische Löschen von Objekten wurde von einem der folgenden Ereignisse ausgelöst: ◦ Das Ablaufdatum oder die Anzahl der Tage in der Lebenszykluskonfiguration für einen S3-Bucket erreicht ist. ◦ Der letzte in einer ILM-Regel angegebene Zeitraum ist abgelaufen. **Hinweis:** Objekte in einem Bucket, für den S3 Object Lock aktiviert ist, können nicht gelöscht werden, wenn sie sich unter einem Legal Hold befinden oder wenn ein Aufbewahrungsdatum angegeben, aber noch nicht erfüllt wurde. • Ein S3-Client fordert die Löschung an, und eine oder mehrere dieser Bedingungen sind zutreffend: ◦ Kopien können nicht innerhalb von 30 Sekunden gelöscht werden, da z. B. ein Objektspeicherort vorübergehend nicht verfügbar ist. ◦ Löschwarteschlangen im Hintergrund sind inaktiv.
Objekte werden sofort entfernt (synchrones Löschen)	Wenn ein S3-Client eine Löschanfrage abgibt und **alle** der folgenden Bedingungen erfüllt sind: • Alle Kopien können innerhalb von 30 Sekunden entfernt werden. • Warteschlangen zum Löschen im Hintergrund enthalten Objekte, die verarbeitet werden sollen.

Wenn S3-Clients Löschanforderungen durchführen, beginnt StorageGRID mit dem Hinzufügen von Objekten zur Löschwarteschlange. Anschließend wechselt er zur Durchführung des synchronen Löschvorgangs. Wenn sichergestellt wird, dass in der Warteschlange zum Löschen im Hintergrund Objekte verarbeitet werden, kann StorageGRID das Löschen von Löschungen effizienter verarbeiten, insbesondere bei Clients mit geringer Parallelität. Gleichzeitig wird verhindert, dass die Backlogs von Clients gelöscht werden.

Erforderliche Zeit zum Löschen von Objekten

Die Art und Weise, wie StorageGRID Objekte löscht, kann sich auf die Ausführung des Systems auswirken:

- Wenn StorageGRID das synchrone Löschen durchführt, kann StorageGRID bis zu 30 Sekunden dauern,

bis ein Ergebnis an den Client zurückgegeben wird. Das heißt, das Löschen kann scheinbar langsamer erfolgen, auch wenn Kopien tatsächlich schneller entfernt werden als wenn StorageGRID Objekte zum Löschen Warteschlangen.

- Wenn Sie die Löschleistung beim Löschen eines Großteils genau überwachen, wird möglicherweise nach dem Löschen einer bestimmten Anzahl von Objekten die Löschrate zu langsam angezeigt. Diese Änderung tritt auf, wenn StorageGRID von Objekten aus der Warteschlange zum Löschen auf das synchrone Löschen verschiebt. Die offensichtliche Reduzierung der Löschrate bedeutet nicht, dass Objektkopien langsamer entfernt werden. Im Gegenteil: Er zeigt an, dass durchschnittlich Speicherplatz schneller freigegeben wird.

Wenn Sie eine große Anzahl von Objekten löschen und Ihre Priorität darin besteht, Speicherplatz schnell freizugeben, ziehen Sie in Betracht, Objekte mithilfe einer Client-Anfrage zu löschen, anstatt sie mit ILM oder anderen Methoden zu löschen. Im Allgemeinen wird Speicherplatz schneller freigegeben, wenn das Löschen durch Clients durchgeführt wird, da StorageGRID das synchrone Löschen verwenden kann.

Die Zeit, die erforderlich ist, um nach dem Löschen eines Objekts Speicherplatz freizugeben, hängt von mehreren Faktoren ab:

- Gibt an, ob Objektkopien synchron entfernt werden oder später zur Entfernung in die Warteschlange verschoben werden (für Client-Löschanfragen).
- Weitere Faktoren wie die Anzahl der Objekte im Grid oder die Verfügbarkeit von Grid-Ressourcen, wenn Objektkopien zur Entfernung in eine Warteschlange verschoben werden (für Clientlöschungen und andere Methoden).

Löschen von S3-versionierten Objekten

Wenn die Versionierung für einen S3-Bucket aktiviert ist, befolgt StorageGRID das Verhalten von Amazon S3, wenn es auf Löschanfragen reagiert, unabhängig davon, ob diese Anfragen von einem S3-Client, dem Ablauf eines S3-Bucket-Lebenszyklus oder den Anforderungen der ILM-Richtlinie stammen.

Wenn Objekte versioniert sind, löschen Objekt-Löschanforderungen nicht die aktuelle Version des Objekts und geben keinen Speicherplatz frei. Stattdessen erzeugt eine Object delete-Anfrage eine Null-Byte-Löschmarkierung als aktuelle Version des Objekts, wodurch die vorherige Version des Objekts „noncurrent“ wird. Eine Markierung zum Löschen eines Objekts wird zu einer Markierung zum Löschen eines abgelaufenen Objekts, wenn es sich um die aktuelle Version handelt und keine nicht aktuellen Versionen vorhanden sind.

Auch wenn das Objekt nicht entfernt wurde, verhält sich StorageGRID so, als ob die aktuelle Version des Objekts nicht mehr verfügbar ist. Anfragen an dieses Objekt geben 404 nicht gefunden zurück. Da jedoch nicht aktuelle Objektdaten nicht entfernt wurden, können Anforderungen, die eine nicht aktuelle Version des Objekts angeben, erfolgreich ausgeführt werden.

Um beim Löschen versionierter Objekte Speicherplatz freizugeben oder Löschmarkierungen zu entfernen, verwenden Sie eine der folgenden Methoden:

- **S3 Client Request**: Geben Sie die Objektversion-ID in der S3 DELETE Object Request (`DELETE /object?versionId=ID`) an. Beachten Sie, dass diese Anforderung nur Objektkopien für die angegebene Version entfernt (die anderen Versionen belegen noch Speicherplatz).
- **Bucket-Lebenszyklus**: Verwenden Sie die `NoncurrentVersionExpiration` Aktion in der Bucket-Lebenszyklus-Konfiguration. Wenn die angegebene Anzahl von nicht-currentDays erreicht ist, entfernt StorageGRID dauerhaft alle Kopien nicht aktueller Objektversionen. Diese Objektversionen können nicht wiederhergestellt werden.

  Die `NewerNoncurrentVersions` Aktion in der Bucket-Lebenszyklus-Konfiguration gibt die Anzahl der

nicht aktuellen Versionen an, die in einem versionierten S3-Bucket aufbewahrt werden. Wenn mehr nicht aktuelle Versionen als angegeben vorhanden sind, entfernt StorageGRID die älteren Versionen, wenn der Wert „nicht aktuelle `NewerNoncurrentVersions` Tage“ abgelaufen ist. Der `NewerNoncurrentVersions` Schwellenwert überschreibt die von ILM bereitgestellten Lebenszyklusregeln. Das bedeutet, dass ein nicht aktuelles Objekt mit einer Version innerhalb `NewerNoncurrentVersions` dieses Schwellenwerts erhalten bleibt, wenn ILM seine Löschung anfordert.

Um abgelaufene Objekte zu entfernen, verwenden Sie die `Expiration` Aktion mit einem der folgenden Tags: `ExpiredObjectDeleteMarker`, , `Days` Oder `Date`.

- **ILM**: "Eine aktive Richtlinie klonen" Und fügen Sie der neuen Richtlinie zwei ILM-Regeln hinzu:
  - Erste Regel: Verwenden Sie "nicht aktuelle Zeit" als Referenzzeit, um mit den nicht aktuellen Versionen des Objekts zu übereinstimmen. "Schritt 1 (Details eingeben) des Assistenten zum Erstellen einer ILM-Regel"Wählen Sie unter **Ja** für die Frage „Diese Regel nur auf ältere Objektversionen anwenden (in S3 Buckets mit aktivierter Versionierung)?“ aus.
  - Zweite Regel: Verwenden Sie **Ingest time**, um die aktuelle Version anzupassen. Die Regel „nicht aktuelle Zeit“ muss in der Richtlinie über der Regel **Ingest Time** erscheinen.

    Um abgelaufene Objektlöschmarkierungen zu entfernen, verwenden Sie eine **Ingest Time**-Regel, um den aktuellen Löschmarkierungen zu entsprechen. Löschmarkierungen werden nur entfernt, wenn ein **Zeitraum** von **Tagen** abgelaufen ist und der aktuelle Löschmaker abgelaufen ist (es gibt keine nicht-aktuellen Versionen).
- **Objekte im Bucket löschen**: Verwenden Sie den Tenant Manager"Löschen Sie alle Objektversionen", um Marker aus einem Bucket zu löschen.

Beim Löschen eines versionierten Objekts erstellt StorageGRID als aktuelle Version des Objekts eine Löschmarkierung mit null Byte. Bevor ein versionierter Bucket gelöscht werden kann, müssen alle Objekte und Löschmarkierungen entfernt werden.

- In StorageGRID 11.7 oder älteren Versionen erstellte Löschmarkierungen können nur über S3-Client-Anfragen entfernt werden. Sie werden nicht durch ILM, Bucket-Lifecycle-Regeln oder Objekte in Bucket-Operationen gelöscht.
- Löschmarkierungen aus einem Bucket, der in StorageGRID 11.8 oder höher erstellt wurde, können durch ILM, Bucket-Lifecycle-Regeln, Löschen von Objekten in Bucket-Operationen oder explizite S3-Client-Löschung entfernt werden.

Verwandte Informationen

- "S3-REST-API VERWENDEN"
- "Beispiel 4: ILM-Regeln und -Richtlinie für versionierte Objekte mit S3"

Speicherklassen erstellen und zuweisen

Speicherklassen identifizieren den Speichertyp, der von einem Speicherknoten verwendet wird. Sie können Storage-Klassen erstellen, wenn ILM-Regeln bestimmte Objekte auf bestimmten Storage-Nodes platzieren sollen.

Bevor Sie beginnen

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

- Sie haben "Bestimmte Zugriffsberechtigungen".

Über diese Aufgabe

Wenn Sie StorageGRID zum ersten Mal installieren, wird die Speicherklasse **Default** automatisch jedem Speicherknoten in Ihrem System zugewiesen. Nach Bedarf können Sie optional benutzerdefinierte Storage-Klassen definieren und sie verschiedenen Storage-Nodes zuweisen.

Mit benutzerdefinierten Speicherqualitäten können Sie ILM-Speicherpools erstellen, die nur einen bestimmten Typ von Speicher-Node enthalten. Möglicherweise möchten Sie beispielsweise bestimmte Objekte auf Ihren schnellsten Storage-Nodes wie z. B. StorageGRID All-Flash Storage Appliances speichern.

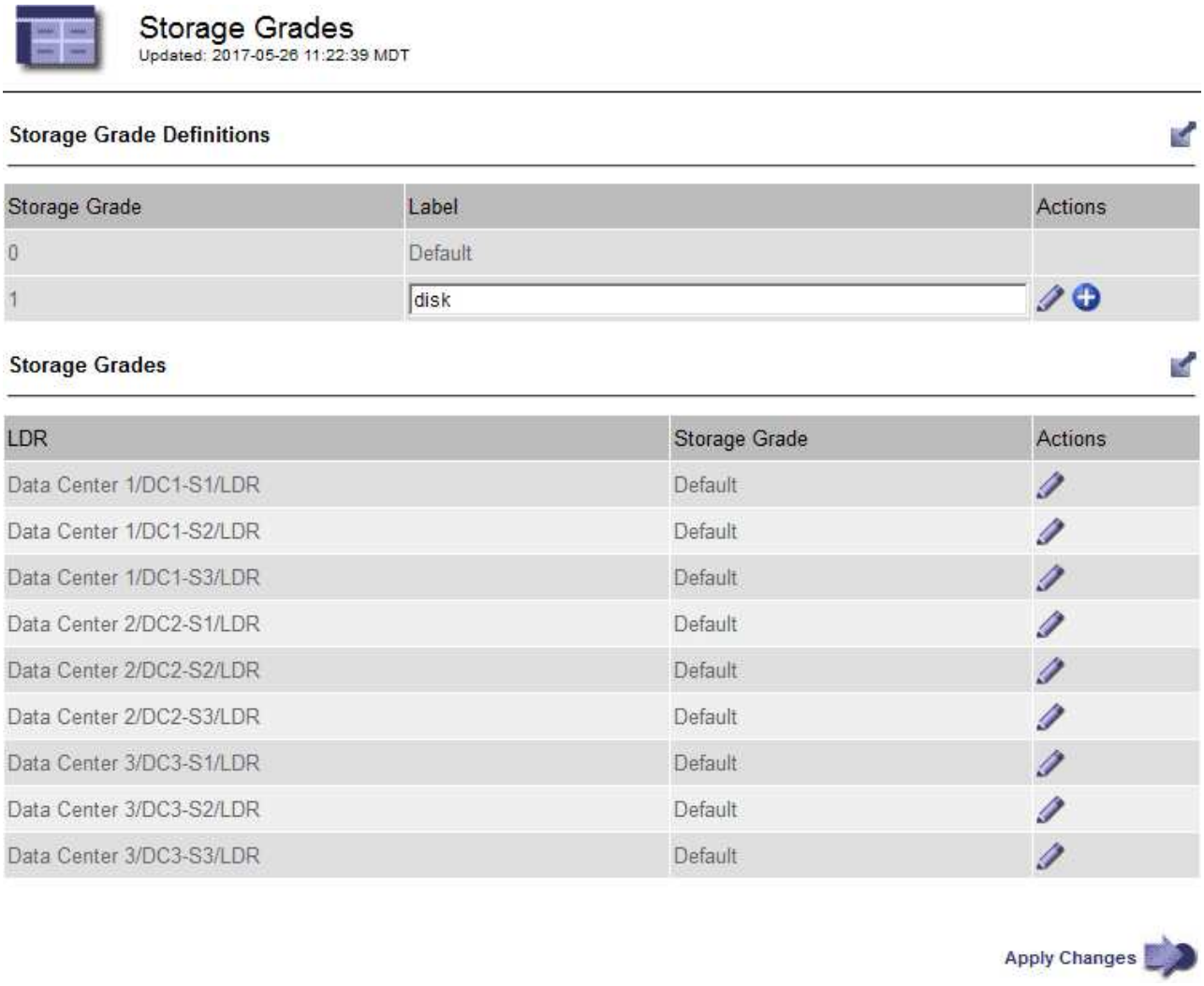
> Storage-Nodes können während der Installation so konfiguriert werden, dass sie nur Objektmetadaten und keine Objektdaten enthalten. Storage-Nodes, die nur Metadaten enthalten, können keiner Storage-Klasse zugewiesen werden. Weitere Informationen finden Sie unter "Typen von Storage-Nodes".

Wenn die Speichergüte kein Problem ist (zum Beispiel sind alle Speicherknoten identisch), können Sie dieses Verfahren überspringen und die Auswahl **includes all Storage grades** für die Speicherklasse verwenden, wenn Sie "Erstellen von Speicherpools". Mit dieser Auswahl wird sichergestellt, dass der Speicherpool jeden Storage Node am Standort umfasst, unabhängig von seiner Speicherklasse.

> Erstellen Sie nicht mehr Storage-Klassen als erforderlich. Erstellen Sie beispielsweise keine Storage-Klasse für jeden Storage-Node. Weisen Sie jede Storage-Klasse zwei oder mehr Nodes zu. Storage-Klassen, die nur einem Node zugewiesen sind, können ILM-Backlogs verursachen, wenn der Node nicht mehr verfügbar ist.

Schritte

1. Wählen Sie **ILM** > **Speicherklassen**.
2. Benutzerdefinierte Storage-Klassen definieren:
   a. Wählen Sie für jede benutzerdefinierte Speicherklasse, die Sie hinzufügen möchten, *Einfügen* , um eine Zeile hinzuzufügen.
   b. Geben Sie eine beschreibende Bezeichnung ein.



c. Wählen Sie **Änderungen Anwenden**.

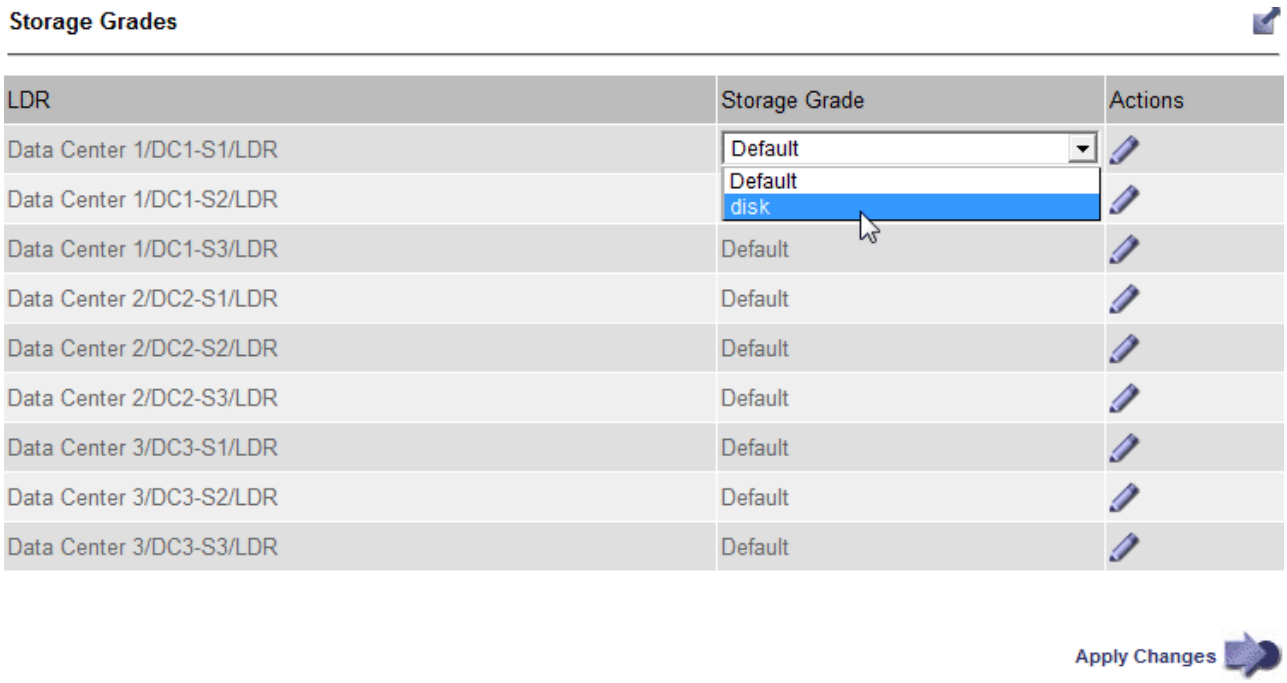
d. Wenn Sie ein gespeichertes Label ändern möchten, wählen Sie optional **Bearbeiten** und dann *Änderungen übernehmen*.

> Speicherqualitäten können nicht gelöscht werden.

3. Storage-Nodes neue Storage-Klassen zuweisen:

a. Suchen Sie den Storage Node in der LDR-Liste und wählen Sie das entsprechende Symbol aus.

b. Wählen Sie den entsprechenden Speichergrad aus der Liste aus.



Weisen Sie einem bestimmten Speicherknoten nur einmal eine Speicherklasse zu. Bei einem nach einem Ausfall wiederhergestellten Storage-Node wird die zuvor zugewiesene Storage-Klasse erhalten. Ändern Sie diese Zuweisung nicht, nachdem die ILM-Richtlinie aktiviert wurde. Wenn die Zuweisung geändert wird, werden die Daten auf Basis der neuen Speicherklasse gespeichert.

a. Wählen Sie **Änderungen Anwenden**.

Nutzung von Speicherpools

Was ist ein Speicherpool?

Ein Speicherpool ist eine logische Gruppierung von Storage-Nodes.

Bei der Installation von StorageGRID wird automatisch ein Speicherpool pro Standort erstellt. Sie können zusätzliche Speicherpools je nach Bedarf konfigurieren.

Storage-Nodes können während der Installation so konfiguriert werden, dass sie Objektdaten und Objektmetadaten oder nur Objektmetadaten enthalten. Nur Metadaten-Storage-Nodes können nicht in Storage-Pools verwendet werden. Weitere Informationen finden Sie unter "Typen von Storage-Nodes".

Storage-Pools haben zwei Attribute:

- **Speicherklasse**: Für Storage-Nodes, die relative Performance beim Sichern von Speicher.
- **Standort**: Das Rechenzentrum, in dem Objekte gespeichert werden.

Storage-Pools werden in ILM-Regeln verwendet, um zu bestimmen, wo Objektdaten gespeichert werden und welcher Storage-Typ verwendet wird. Wenn Sie ILM-Regeln für die Replikation konfigurieren, wählen Sie einen oder mehrere Speicherpools aus.

Richtlinien zur Erstellung von Speicherpools

Konfiguration und Verwendung von Speicherpools zur Absicherung gegen Datenverluste durch Verteilung von Daten über mehrere Standorte hinweg Für replizierte Kopien und Kopien, die zur Fehlerkorrektur codiert wurden, sind unterschiedliche Konfigurationen von Storage-Pools erforderlich.

Siehe "Beispiele für den Schutz vor Standortausfällen durch Replikation und Erasure Coding".

Richtlinien für alle Speicherpools

- Halten Sie Storage-Pool-Konfigurationen so einfach wie möglich. Erstellen Sie nicht mehr Speicherpools als nötig.
- Erstellung von Storage-Pools mit so vielen Nodes wie möglich Jeder Storage-Pool sollte zwei oder mehr Nodes enthalten. Ein Storage-Pool mit unzureichenden Nodes kann ILM-Backlogs verursachen, wenn ein Node nicht mehr verfügbar ist.
- Vermeiden Sie es, Storage-Pools zu erstellen oder zu verwenden, die sich überlappen (einen oder mehrere derselben Nodes enthalten). Bei Überschneidungen von Storage-Pools kann es sein, dass mehrere Kopien von Objektdaten auf demselben Node gespeichert werden.
- Verwenden Sie im Allgemeinen nicht den Speicherpool Alle Speicherknoten (StorageGRID 11.6 und früher) oder den Standort Alle Standorte. Diese Elemente werden automatisch aktualisiert, um alle neuen Sites, die Sie einer Erweiterung hinzufügen, aufzunehmen, was möglicherweise nicht das gewünschte Verhalten ist.

Richtlinien für Storage-Pools, die für replizierte Kopien verwendet werden

- "Replizierung"Geben Sie für den Schutz vor Standortausfällen mit einen oder mehrere standortspezifische Speicherpools im "Anweisungen zur Platzierung der einzelnen ILM-Regeln"an.

  Während der StorageGRID-Installation wird für jeden Standort automatisch ein Storage-Pool erstellt.

  Durch die Verwendung eines Storage Pools für jeden Standort wird sichergestellt, dass replizierte Objektkopien genau an den erwarteten Ort platziert werden (z. B. eine Kopie jedes Objekts an jedem Standort zum Site-Loss-Schutz).

- Wenn Sie einer Erweiterung einen Standort hinzufügen, erstellen Sie einen neuen Speicherpool, der nur den neuen Standort enthält. Dann, "Aktualisieren Sie die ILM-Regeln" um zu steuern, welche Objekte auf dem neuen Standort gespeichert werden.
- Wenn die Anzahl der Kopien geringer ist als die Anzahl der Speicherpools, verteilt das System die Kopien, um die Festplattennutzung zwischen den Pools auszugleichen.
- Wenn sich die Speicherpools überschneiden (die gleichen Storage-Nodes enthalten), werden möglicherweise alle Kopien des Objekts an nur einem Standort gespeichert. Sie müssen sicherstellen, dass die ausgewählten Speicherpools nicht dieselben Speicher-Nodes enthalten.

Richtlinien für Storage-Pools, die für Kopien mit Verfahren zur Einhaltung von Datenkonsistenz (Erasure Coding) verwendet werden

- "Erasure Coding"Erstellen Sie für den Schutz vor Standortausfällen mithilfe von Speicherpools, die aus mindestens drei Standorten bestehen. Wenn ein Storage-Pool nur zwei Standorte umfasst, kann dieser Storage-Pool nicht für Erasure Coding verwendet werden. Für einen Speicherpool mit zwei Standorten stehen keine Erasure Coding-Schemata zur Verfügung.

- Die Anzahl der im Speicherpool enthaltenen Speicher-Nodes und Standorte bestimmt, welche "Erasure Coding-Schemata"verfügbar sind.
- Wenn möglich, sollte ein Speicherpool mehr als die Mindestanzahl an Speicherknoten enthalten, die für das ausgewählte Erasure-Coding-Schema erforderlich ist. Wenn Sie beispielsweise ein 6+3-Schema zur Codierung von Löschverfahren verwenden, müssen Sie mindestens neun Storage-Nodes haben. Es wird jedoch empfohlen, mindestens einen zusätzlichen Storage-Node pro Standort zu haben.
- Verteilen Sie Storage Nodes so gleichmäßig wie möglich auf Standorte. Um beispielsweise ein 6+3 Erasure Coding-Schema zu unterstützen, konfigurieren Sie einen Storage-Pool, der mindestens drei Storage-Nodes an drei Standorten enthält.
- Wenn Sie hohe Durchsatzanforderungen haben, wird die Verwendung eines Speicherpools mit mehreren Standorten nicht empfohlen, wenn die Netzwerklatenz zwischen Standorten mehr als 100 ms beträgt. Mit steigender Latenz sinkt auch die Rate, mit der StorageGRID Objektfragmente erstellen, platzieren und abrufen kann, aufgrund des geringeren TCP-Netzwerkdurchsatzes erheblich.

  Der Rückgang des Durchsatzes wirkt sich auf die maximal erreichbaren Raten bei der Aufnahme und dem Abruf von Objekten aus (wenn Balance oder Strict als Aufnahmeverhalten ausgewählt werden) oder kann zu ILM-Warteschlangen-Backlogs führen (wenn Dual Commit als Aufnahmeverhalten ausgewählt wird). Siehe "ILM-Regel Aufnahme-Verhalten".

> Wenn Ihr Grid nur einen Standort umfasst, können Sie den Speicherpool Alle Storage-Nodes (StorageGRID 11.6 und früher) oder den Standort Alle Standorte in einem Erasure-Coding-Profil nicht verwenden. Dieses Verhalten verhindert, dass das Profil ungültig wird, wenn ein zweiter Standort hinzugefügt wird.

Schutz vor Standortausfällen

Wenn die Implementierung von StorageGRID mehrere Standorte umfasst, können Sie für den Schutz vor Standortausfällen Replizierung und Erasure Coding mit entsprechend konfigurierten Storage-Pools verwenden.

Für Replizierung und Erasure Coding sind unterschiedliche Storage-Pool-Konfigurationen erforderlich:

- Um die Replikation zum Schutz vor Standortausfällen zu verwenden, verwenden Sie die standortspezifischen Speicherpools, die bei der StorageGRID-Installation automatisch erstellt werden. Erstellen Sie dann ILM-Regeln, mit "Anweisungen zur Platzierung" denen mehrere Storage-Pools angegeben werden, sodass von jedem Objekt eine Kopie an jedem Standort platziert wird.
- Um das Verfahren zum Schutz vor Standortausfällen zu verwenden, "Erstellen Sie Speicherpools, die aus mehreren Standorten bestehen". Erstellen Sie dann ILM-Regeln, die einen Storage-Pool verwenden, der aus mehreren Standorten und einem beliebigen verfügbaren Erasure-Coding-Schema besteht.

> Wenn Sie Ihre StorageGRID-Bereitstellung für den Schutz vor Standortausfällen konfigurieren, müssen Sie auch die Auswirkungen von und berücksichtigen"Aufnahmeoptionen""Konsistenz".

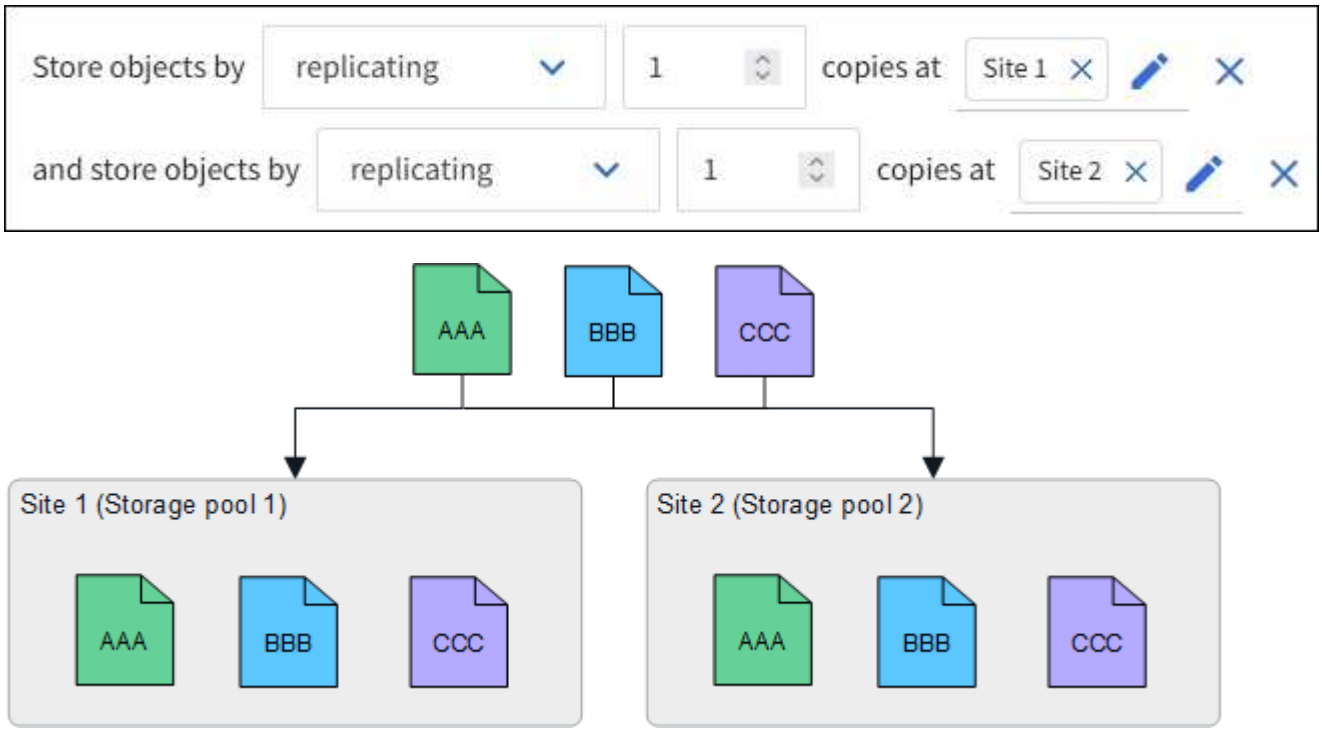
Beispiel für die Replikation

Standardmäßig wird während der StorageGRID-Installation ein Speicherpool für jeden Standort erstellt. Wenn Speicherpools nur aus einem Standort bestehen, können Sie ILM-Regeln konfigurieren, die die Replikation für den Schutz vor Standortausfällen verwenden. In diesem Beispiel:

- Speicherpool 1 enthält Standort 1

- Speicherpool 2 enthält Standort 2
- Die ILM-Regel enthält zwei Platzierungen:
  - Speichern Sie Objekte, indem Sie 1 Kopie an Standort 1 replizieren
  - Speichern Sie Objekte, indem Sie 1 Kopie an Standort 2 replizieren

ILM-Regelplatzierungen:



Wenn ein Standort verloren geht, sind Kopien der Objekte am anderen Standort verfügbar.

Beispiel für Erasure Coding

Wenn Storage-Pools aus mehr als einem Standort pro Storage-Pool bestehen, können Sie ILM-Regeln konfigurieren, die Erasure Coding für Site-Loss-Schutz verwenden. In diesem Beispiel:

- Speicherpool 1 enthält die Standorte 1 bis 3
- Die ILM-Regel enthält eine Platzierung: Speichern Sie Objekte mithilfe eines Erasure Coding mithilfe eines 4+2 EC-Schemas in Storage Pool 1, das drei Standorte enthält

ILM-Regelplatzierungen:

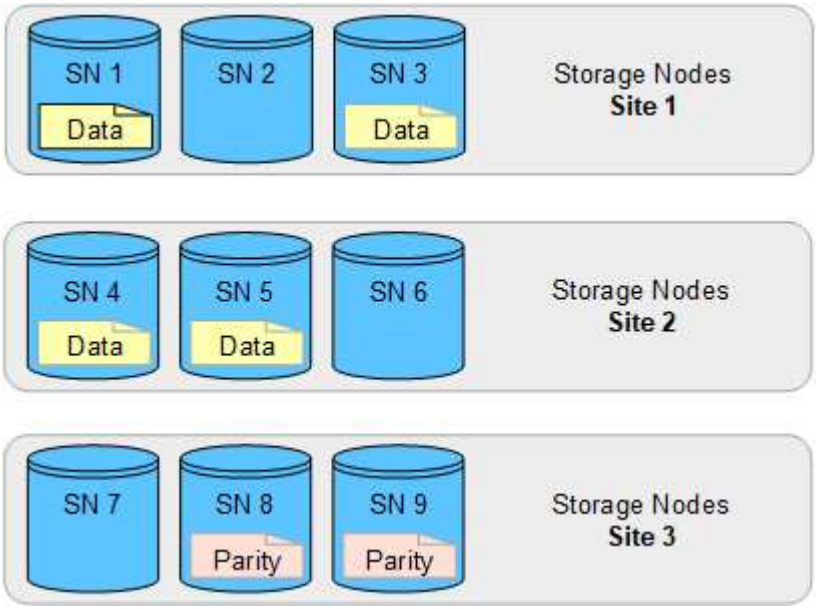
In diesem Beispiel:

- Die ILM-Regel verwendet ein 4+2 Erasure Coding-Schema.
- Jedes Objekt wird in vier gleiche Datenfragmente geteilt und aus den Objektdaten werden zwei Paritätsfragmente berechnet.

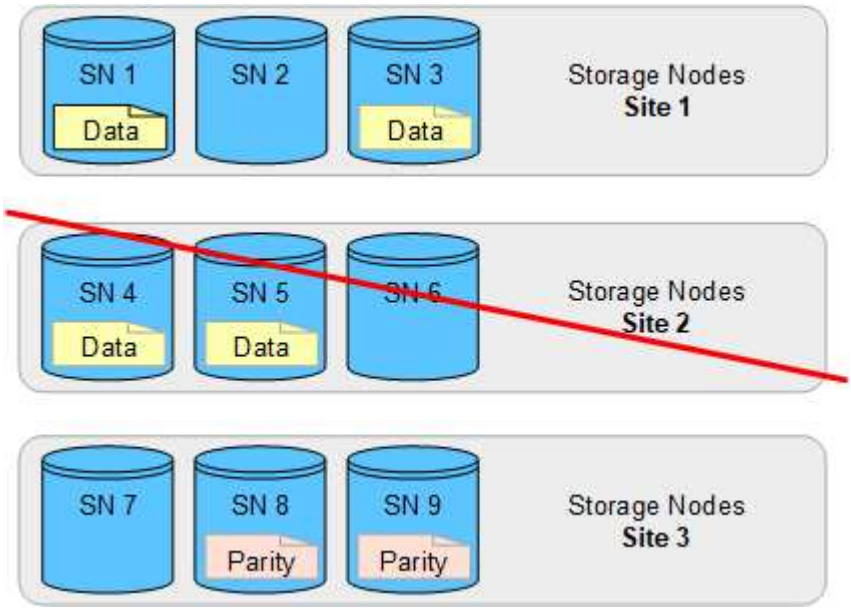
- Jedes der sechs Fragmente wird auf einem anderen Node über drei Datacenter-Standorte gespeichert, um Daten bei Node-Ausfällen oder Standortausfällen zu sichern.

> Erasure Coding ist in Speicherpools erlaubt, die eine beliebige Anzahl von Standorten mit Ausnahme von zwei Standorten enthalten.

ILM-Regel gemäß 4+2 Erasure-Coding-Schema:



Wenn ein Standort verloren geht, können die Daten immer noch wiederhergestellt werden:



Erstellen Sie einen Speicherpool

Sie erstellen Storage-Pools, um zu bestimmen, wo das StorageGRID-System Objektdaten und den verwendeten Storage-Typ speichert. Jeder Speicherpool umfasst einen oder mehrere Standorte und eine oder mehrere Speicherklassen.

> Wenn Sie StorageGRID 11.9 in einem neuen Grid installieren, werden für jeden Standort automatisch Speicherpools erstellt. Wenn Sie StorageGRID 11.6 oder eine frühere Version installiert haben, werden Speicherpools jedoch nicht automatisch für jeden Standort erstellt.

Wenn Sie Cloud-Speicherpools erstellen möchten, um Objektdaten außerhalb Ihres StorageGRID-Systems zu speichern, lesen Sie die "Informationen zur Verwendung von Cloud Storage Pools".

Bevor Sie beginnen

- Sie sind im Grid Manager mit einem angemeldet"Unterstützter Webbrowser".
- Sie haben "Bestimmte Zugriffsberechtigungen".
- Sie haben die Richtlinien zum Erstellen von Speicherpools überprüft.

Über diese Aufgabe

Storage Pools legen fest, wo Objektdaten gespeichert sind. Die Anzahl der erforderlichen Storage-Pools hängt von der Anzahl der Standorte in Ihrem Grid und den gewünschten Kopien ab: Repliziert oder Erasure Coding.

- Für Replizierung und Erasure Coding für einen Standort erstellen Sie für jeden Standort einen Storage-Pool. Wenn Sie beispielsweise replizierte Objektkopien an drei Standorten speichern möchten, erstellen Sie drei Storage Pools.
- Erstellen Sie für das Erasure Coding an drei oder mehr Standorten einen Storage-Pool mit einem Eintrag für jeden Standort. Wenn Sie beispielsweise Objekte aus drei Standorten löschen möchten, erstellen Sie einen Speicherpool.

> Schließen Sie den Standort Alle Standorte nicht in einen Speicherpool ein, der in einem Erasure-Coding-Profil verwendet wird. Fügen Sie stattdessen für jeden Standort, der mit Erasure Coded Daten speichert, einen separaten Eintrag zum Speicherpool hinzu. Ein Beispiel finden Sie unterDiesem Schritt.

- Wenn Sie mehr als eine Storage-Klasse verwenden, sollten Sie an einem einzelnen Standort keinen Storage-Pool erstellen, der verschiedene Storage-Klassen umfasst. Siehe "Richtlinien zur Erstellung von Speicherpools".

Schritte

1. Wählen Sie **ILM** > **Storage Pools** aus.

   Auf der Registerkarte Speicherpools werden alle definierten Speicherpools aufgeführt.

   > Bei Neuinstallationen von StorageGRID 11.6 oder früher wird der Speicherpool Alle Speicherknoten automatisch aktualisiert, sobald Sie neue Rechenzentrumsstandorte hinzufügen. Verwenden Sie diesen Pool nicht in ILM-Regeln.

2. Um einen neuen Speicherpool zu erstellen, wählen Sie **Erstellen**.
3. Geben Sie einen eindeutigen Namen für den Speicherpool ein. Verwenden Sie einen Namen, der sich leicht identifizieren lässt, wenn Sie Profile zur Einhaltung von Datenkonsistenz und ILM-Regeln konfigurieren.
4. Wählen Sie aus der Dropdown-Liste **Standort** einen Standort für diesen Speicherpool aus.

   Wenn Sie einen Standort auswählen, wird die Anzahl der Storage-Nodes in der Tabelle automatisch aktualisiert.

Im Allgemeinen sollten Sie den Standort „Alle Standorte“ nicht in einem Speicherpool verwenden. ILM-Regeln, die einen Storage-Pool an allen Standorten verwenden, platzieren Objekte an jedem beliebigen verfügbaren Standort, wodurch Sie weniger Kontrolle über die Objektplatzierung haben. Außerdem verwendet ein Speicherpool für alle Standorte sofort die Speicherknoten an einem neuen Standort, was möglicherweise nicht das erwartete Verhalten ist.

5. Wählen Sie aus der Dropdown-Liste **Speichergrad** den Speichertyp aus, der verwendet werden soll, wenn eine ILM-Regel diesen Speicherpool verwendet.

   Die Speicherklasse *umfasst alle Speicherklassen* und umfasst alle Speicher-Nodes am ausgewählten Standort. Wenn Sie zusätzliche Speicherklassen für die Speicherknoten in Ihrem Raster erstellt haben, werden diese im Dropdown-Menü aufgelistet.

6. Wenn Sie den Speicherpool in einem Profil für die mehrstufige Erasure Coding verwenden möchten, wählen Sie **Weitere Knoten hinzufügen** aus, um dem Speicherpool einen Eintrag für jeden Standort hinzuzufügen.

   > Sie werden gewarnt, wenn Sie mehr als einen Eintrag mit unterschiedlichen Speicherqualitäten für einen Standort hinzufügen.

   Um einen Eintrag zu entfernen, wählen Sie das Löschen-Symbol ✕.

7. Wenn Sie mit Ihrer Auswahl zufrieden sind, wählen Sie **Speichern**.

   Der neue Speicherpool wird der Liste hinzugefügt.

Zeigen Sie Details zum Speicherpool an

Sie können die Details eines Speicherpools anzeigen, um zu bestimmen, wo der Speicherpool verwendet wird, und um zu sehen, welche Nodes und Speicherklassen enthalten sind.

Bevor Sie beginnen

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

Schritte

1. Wählen Sie **ILM** > **Storage Pools** aus.

   Die Tabelle Speicherpools enthält die folgenden Informationen für jeden Speicherpool, der Speicher-Nodes umfasst:

   - **Name**: Der eindeutige Anzeigename des Speicherpools.
   - **Knotenanzahl**: Die Anzahl der Knoten im Speicherpool.
   - **Speichernutzung**: Der Prozentsatz des gesamten nutzbaren Speicherplatzes, der für Objektdaten auf diesem Knoten verwendet wurde. Dieser Wert enthält keine Objektmetadaten.
   - **Gesamtkapazität**: Die Größe des Speicherpools, die der Gesamtmenge des nutzbaren Speicherplatzes für Objektdaten für alle Knoten im Speicherpool entspricht.
   - **ILM-Nutzung**: Wie der Speicherpool derzeit genutzt wird. Ein Storage-Pool wird möglicherweise nicht verwendet, oder er kann in einem oder mehreren ILM-Regeln, Erasure-Coding-Profilen oder beiden

verwendet werden.

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

   Die Detailseite für den Speicherpool wird angezeigt.

3. Sehen Sie sich die Registerkarte **Nodes** an, um mehr über die im Speicherpool enthaltenen Speicher-Nodes zu erfahren.

   Die Tabelle enthält die folgenden Informationen für jeden Node:

   - Node-Name
   - Standortname
   - Storage-Klasse
   - Speichernutzung: Der Prozentsatz des gesamten nutzbaren Speicherplatzes für Objektdaten, der für den Speicher-Node verwendet wurde.

   > Der gleiche Wert für die Speichernutzung (%) wird auch im Diagramm Speicher verwendet - Objektdaten für jeden Speicherknoten angezeigt (wählen Sie **NODES** > ***Storage Node*** > **Storage**).

4. Prüfen Sie auf der Registerkarte **ILM-Nutzung**, ob der Speicherpool derzeit in ILM-Regeln oder Erasure-Coding-Profilen verwendet wird.
5. Optional können Sie auf der Seite **ILM-Regeln** weitere Informationen zu den Regeln erhalten, die den Speicherpool verwenden.

   Siehe "Anweisungen zum Arbeiten mit ILM-Regeln".

Speicherpool bearbeiten

Sie können einen Speicherpool bearbeiten, um seinen Namen zu ändern oder Standorte und Speicherklassen zu aktualisieren.

Bevor Sie beginnen

- Sie sind im Grid Manager mit einem angemeldet"Unterstützter Webbrowser".
- Sie haben "Bestimmte Zugriffsberechtigungen".
- Sie haben die überprüft"Richtlinien für die Erstellung von Speicherpools".
- Wenn Sie einen Speicherpool bearbeiten möchten, der von einer Regel in der aktiven ILM-Richtlinie verwendet wird, haben Sie überlegt, wie sich Ihre Änderungen auf die Platzierung von Objektdaten auswirken.

Über diese Aufgabe

Wenn Sie einen neuen Standort oder eine Speicherklasse zu einem Speicherpool hinzufügen, der in der aktiven ILM-Richtlinie verwendet wird, beachten Sie, dass die Speicherknoten am neuen Standort oder der Speicherklasse nicht automatisch verwendet werden. Um StorageGRID zu zwingen, einen neuen Standort oder eine neue Speicherklasse zu verwenden, müssen Sie eine neue ILM-Richtlinie aktivieren, nachdem Sie den bearbeiteten Speicherpool gespeichert haben.

Schritte

1. Wählen Sie **ILM** > **Storage Pools** aus.

2. Aktivieren Sie das Kontrollkästchen für den Speicherpool, den Sie bearbeiten möchten.

   Der Speicherpool „Alle Speicherknoten“ (StorageGRID 11.6 und früher) kann nicht bearbeitet werden.

3. Wählen Sie **Bearbeiten**.
4. Ändern Sie bei Bedarf den Namen des Speicherpools.
5. Wählen Sie bei Bedarf andere Standorte und Lagersorten aus.

   Sie können den Standort oder die Storage-Klasse nicht ändern, wenn der Speicherpool in einem Erasure-Coding-Profil verwendet wird und die Änderung dazu führen würde, dass das Erasure-Coding-Schema ungültig wird. Wenn beispielsweise ein Storage-Pool in einem Profil für Erasure Coding derzeit eine Storage-Klasse mit nur einem Standort umfasst, können Sie eine Storage-Klasse mit zwei Standorten nicht verwenden, da das Erasure Coding-Schema durch die Änderung ungültig würde.

   > Beim Hinzufügen oder Entfernen von Standorten aus einem vorhandenen Storage-Pool werden vorhandene Daten, die nach der Erasure-Coding-Verschlüsselung codiert wurden, nicht verschoben. Wenn Sie die vorhandenen Daten vom Standort verschieben möchten, müssen Sie einen neuen Speicherpool und ein neues EC-Profil erstellen, um die Daten neu zu kodieren.

6. Wählen Sie **Speichern**.

Nachdem Sie fertig sind

Wenn Sie einem Speicherpool, der in der aktiven ILM-Richtlinie verwendet wird, einen neuen Standort oder eine neue Storage-Klasse hinzugefügt haben, aktivieren Sie eine neue ILM-Richtlinie, um StorageGRID zu zwingen, den neuen Standort oder die neue Storage-Klasse zu verwenden. Klonen Sie beispielsweise Ihre vorhandene ILM-Richtlinie und aktivieren Sie dann den Klon. Siehe "Arbeiten Sie mit ILM-Regeln und ILM-Richtlinien".

Entfernen Sie einen Speicherpool

Sie können einen Speicherpool entfernen, der nicht verwendet wird.

Bevor Sie beginnen

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

Schritte

1. Wählen Sie **ILM** > **Storage Pools** aus.
2. Überprüfen Sie in der Spalte ILM-Nutzung in der Tabelle, ob Sie den Speicherpool entfernen können.

   Sie können einen Storage-Pool nicht entfernen, wenn er in einer ILM-Regel oder in einem Erasure-Coding-Profil verwendet wird. Wählen Sie bei Bedarf ***Storage Pool Name*** > **ILM usage**, um zu bestimmen, wo der Speicherpool verwendet wird.

3. Wenn der Speicherpool, den Sie entfernen möchten, nicht verwendet wird, aktivieren Sie das Kontrollkästchen.
4. Wählen Sie **Entfernen**.
5. Wählen Sie **OK**.

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
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)

	Cloud-Storage-Pool	CloudMirror Replikationsservice
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.
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.
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"

Profile für das Erasure Coding managen

Sie können die Details für ein Erasure-Coding-Profil anzeigen und bei Bedarf ein Profil umbenennen. Sie können ein Profil für Erasure Coding deaktivieren, wenn es derzeit nicht in ILM-Regeln verwendet wird.

Bevor Sie beginnen

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

Profildetails zum Erasure Coding anzeigen

Sie können die Details eines Profils zur Fehlerkorrektur anzeigen, um dessen Status, das verwendete Schema zur Fehlerkorrektur sowie weitere Informationen zu bestimmen.

Schritte

1. Wählen Sie **CONFIGURATION** > **System** > **Erasure Coding**.
2. Wählen Sie das Profil aus. Die Detailseite für das Profil wird angezeigt.
3. Optional können Sie auf der Registerkarte ILM-Regeln eine Liste der ILM-Regeln anzeigen, die das Profil verwenden, sowie die ILM-Richtlinien, die diese Regeln verwenden.
4. Optional können Sie die Registerkarte Storage Nodes anzeigen, um Details zu jedem Storage Node im Speicherpool des Profils anzuzeigen, z. B. den Standort, an dem er sich befindet, und die Speichernutzung.

Umbenennen eines Profils für die Erasure Coding

Möglicherweise möchten Sie ein Erasure Coding-Profil umbenennen, um die Funktionen des Profils offensichtlicher zu machen.

Schritte

1. Wählen Sie **CONFIGURATION** > **System** > **Erasure Coding**.
2. Wählen Sie das Profil aus, das Sie umbenennen möchten.
3. Wählen Sie **Umbenennen**.

4. Geben Sie einen eindeutigen Namen für das Erasure-Coding-Profil ein.

   Der Name des Erasure Coding-Profils wird in der Platzierungsanweisung für eine ILM-Regel an den Namen des Speicherpools angehängt.

   > Profilnamen für das Erasure Coding müssen eindeutig sein. Ein Validierungsfehler tritt auf, wenn Sie den Namen eines vorhandenen Profils verwenden, auch wenn dieses Profil deaktiviert wurde.

5. Wählen Sie **Speichern**.

Deaktivieren Sie ein Erasure Coding-Profil

Sie können ein Profil zur Einhaltung von Datenkonsistenz deaktivieren, wenn Sie dessen Verwendung nicht mehr planen und das Profil derzeit in keiner ILM-Regel verwendet wird.

> Sie müssen sicherstellen, dass keine Datenreparaturen mit Erasure-Coded-Verfahren durchgeführt werden oder Ausmusterung durchgeführt wird. Wenn Sie versuchen, ein Erasure-Coding-Profil zu deaktivieren, während eines dieser Vorgänge ausgeführt wird, wird eine Fehlermeldung ausgegeben.

Über diese Aufgabe

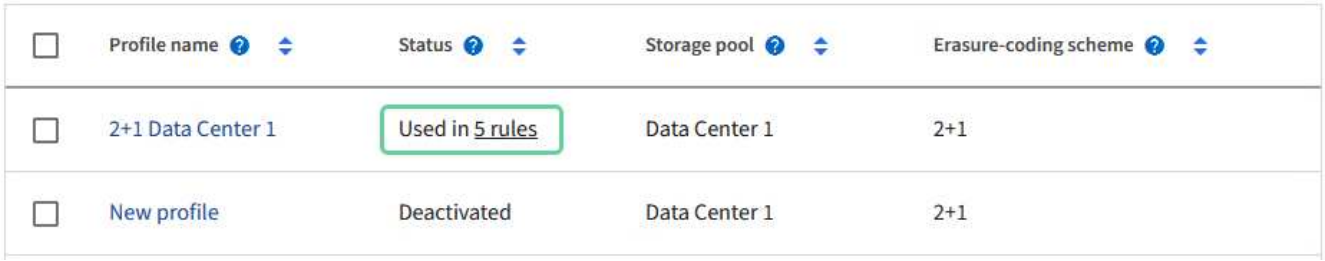
StorageGRID verhindert, dass Sie ein Erasure Coding-Profil deaktivieren, wenn eine der folgenden Bedingungen zutrifft:

- Das Erasure Coding-Profil wird derzeit in einer ILM-Regel verwendet.
- Das Erasure Coding-Profil wird in keiner ILM-Regel mehr verwendet, es existieren jedoch noch Objektdaten und Paritätsfragmente für das Profil.

Schritte

1. Wählen Sie **CONFIGURATION** > **System** > **Erasure Coding**.
2. Überprüfen Sie auf der Registerkarte aktiv die Spalte **Status**, um zu bestätigen, dass das zu deaktivierende Erasure-Coding-Profil in keiner ILM-Regel verwendet wird.

   Sie können ein Profil für Erasure Coding nicht deaktivieren, wenn es in einer ILM-Regel verwendet wird. In diesem Beispiel wird das Profil 2+1 Rechenzentrum 1 in mindestens einer ILM-Regel verwendet.



Profile name	Status	Storage pool	Erasure-coding scheme
2+1 Data Center 1	Used in 5 rules	Data Center 1	2+1
New profile	Deactivated	Data Center 1	2+1

3. Wenn das Profil in einer ILM-Regel verwendet wird, führen Sie die folgenden Schritte aus:
   a. Wählen Sie **ILM** > **Regeln**.
   b. Wählen Sie jede Regel aus, und prüfen Sie das Aufbewahrungsdiagramm, um festzustellen, ob die Regel das zu deaktivierende Profil für die Löschcodierung verwendet.
   c. Wenn die ILM-Regel das Profil für die Erasure Coding verwendet, das Sie deaktivieren möchten,

bestimmen Sie, ob die Regel in einer ILM-Richtlinie verwendet wird.

d. Führen Sie die zusätzlichen Schritte in der Tabelle aus, je nachdem, wo das Erasure-Coding-Profil verwendet wird.

Wo wurde das Profil verwendet?	Weitere Schritte, die vor dem Deaktivieren des Profils ausgeführt werden müssen	Beachten Sie diese zusätzlichen Anweisungen
Nie in einer ILM-Regel verwendet	Weitere Schritte sind nicht erforderlich. Fahren Sie mit diesem Verfahren fort.	*Keine*
In einer ILM-Regel, die noch nie in einer ILM-Richtlinie verwendet wurde	i. Alle betroffenen ILM-Regeln bearbeiten oder löschen. Wenn Sie die Regel bearbeiten, entfernen Sie alle Platzierungen, die das Erasure-Coding-Profil verwenden. ii. Fahren Sie mit diesem Verfahren fort.	"Arbeiten Sie mit ILM-Regeln und ILM-Richtlinien"
In einer ILM-Regel, die sich derzeit in einer aktiven ILM-Richtlinie befindet	i. Klonen Sie die Richtlinie. ii. Entfernen Sie die ILM-Regel, die das Profil für die Fehlerkorrektur verwendet. iii. Fügen Sie mindestens eine neue ILM-Regel hinzu, um die Sicherheit von Objekten zu gewährleisten. iv. Speichern, simulieren und aktivieren Sie die neue Richtlinie. v. Warten Sie, bis die neue Richtlinie angewendet wird und vorhandene Objekte basierend auf den neuen Regeln, die Sie hinzugefügt haben, an neue Orte verschoben werden. **Hinweis:** abhängig von der Anzahl der Objekte und der Größe Ihres StorageGRID-Systems kann es Wochen oder sogar Monate dauern, bis ILM-Vorgänge die Objekte auf der Grundlage der neuen ILM-Regeln an neue Orte verschieben. Obwohl Sie sicher versuchen können, ein Erasure-Coding-Profil zu deaktivieren, während es noch mit Daten verknüpft ist, schlägt die Deaktivierung fehl. Eine Fehlermeldung informiert Sie darüber, ob das Profil noch nicht deaktiviert werden kann. vi. Bearbeiten oder löschen Sie die Regel, die Sie aus der Richtlinie entfernt haben. Wenn Sie die Regel bearbeiten, entfernen Sie alle Platzierungen, die das Erasure-Coding-Profil verwenden. vii. Fahren Sie mit diesem Verfahren fort.	"ILM-Richtlinie erstellen" "Arbeiten Sie mit ILM-Regeln und ILM-Richtlinien"

Wo wurde das Profil verwendet?	Weitere Schritte, die vor dem Deaktivieren des Profils ausgeführt werden müssen	Beachten Sie diese zusätzlichen Anweisungen
In einer ILM-Regel, die sich derzeit in einer ILM-Richtlinie befindet	i. Bearbeiten Sie die Richtlinie. ii. Entfernen Sie die ILM-Regel, die das Profil für die Fehlerkorrektur verwendet. iii. Fügen Sie ein oder mehrere neue ILM-Regeln hinzu, um sicherzustellen, dass alle Objekte geschützt sind. iv. Speichern Sie die Richtlinie. v. Bearbeiten oder löschen Sie die Regel, die Sie aus der Richtlinie entfernt haben. Wenn Sie die Regel bearbeiten, entfernen Sie alle Platzierungen, die das Erasure-Coding-Profil verwenden. vi. Fahren Sie mit diesem Verfahren fort.	"ILM-Richtlinie erstellen" "Arbeiten Sie mit ILM-Regeln und ILM-Richtlinien"

e. Aktualisieren Sie die Seite Erasure-Coding-Profile, um sicherzustellen, dass das Profil nicht in einer ILM-Regel verwendet wird.

4. Wenn das Profil nicht in einer ILM-Regel verwendet wird, aktivieren Sie das Optionsfeld und wählen Sie **Deaktivieren**. Das Dialogfeld Löschen-Kodungsprofil deaktivieren wird angezeigt.

> Sie können mehrere Profile auswählen, die gleichzeitig deaktiviert werden sollen, solange jedes Profil in keiner Regel verwendet wird.

5. Wenn Sie sicher sind, dass Sie das Profil deaktivieren möchten, wählen Sie **Deactivate**.

Ergebnisse

- Wenn StorageGRID das Erasure-Coding-Profil deaktivieren kann, ist sein Status deaktiviert. Sie können dieses Profil nicht mehr für eine ILM-Regel auswählen. Ein deaktiviertes Profil kann nicht reaktiviert werden.
- Wenn StorageGRID das Profil nicht deaktivieren kann, wird eine Fehlermeldung angezeigt. Wenn Objektdaten weiterhin mit diesem Profil verknüpft sind, wird beispielsweise eine Fehlermeldung angezeigt. Sie müssen möglicherweise mehrere Wochen warten, bevor Sie den Deaktivierungsprozess erneut versuchen.

Regionen konfigurieren (nur optional und S3)

ILM-Regeln können Objekte auf Basis der Bereiche filtern, in denen S3-Buckets erstellt werden, und so Objekte aus verschiedenen Regionen an unterschiedlichen Storage-Standorten speichern.

Wenn Sie einen S3-Bucket-Bereich als Filter in einer Regel verwenden möchten, müssen Sie zuerst die Regionen erstellen, die von den Buckets in Ihrem System verwendet werden können.

> Sie können den Bereich für einen Bucket nicht ändern, nachdem der Bucket erstellt wurde.

Bevor Sie beginnen

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

Über diese Aufgabe

Beim Erstellen eines S3-Buckets können Sie angeben, dass er in einer bestimmten Region erstellt wird. Wenn Sie eine Region angeben, kann der Bucket sich in geografischer Nähe zu seinen Benutzern befinden, um die Latenz zu optimieren, Kosten zu minimieren und gesetzliche Anforderungen zu erfüllen.

Wenn Sie eine ILM-Regel erstellen, möchten Sie die Region, die einem S3-Bucket zugeordnet ist, möglicherweise als erweiterten Filter verwenden. Beispielsweise können Sie eine Regel entwerfen, die nur für Objekte in S3-Buckets gilt, die in der Region erstellt `us-west-2` wurden. Sie können dann angeben, die Kopien dieser Objekte an Storage-Nodes an einem Datacenter-Standort innerhalb dieser Region platziert werden, um die Latenz zu optimieren.

Befolgen Sie bei der Konfiguration von Regionen die folgenden Richtlinien:

- Standardmäßig gehören alle Buckets zur `us-east-1` Region.
- Sie müssen die Regionen mit dem Grid Manager erstellen, bevor Sie beim Erstellen von Buckets mithilfe der Mandanten-Manager- oder Mandantenmanagement-API oder mit dem LocationConstraint-Anforderungselement für S3 PUT-Bucket-API-Anforderungen eine nicht standardmäßige Region angeben können. Ein Fehler tritt auf, wenn eine PUT-Bucket-Anforderung eine Region verwendet, die nicht in StorageGRID definiert wurde.
- Sie müssen beim Erstellen des S3-Buckets den genauen Regionalnamen verwenden. Bei Regionalnamen wird zwischen Groß- und Kleinschreibung unterschieden. Gültige Zeichen sind Zahlen, Buchstaben und Bindestriche.

  > ⓘ Die EU gilt nicht als ein Alias für eu-West-1. Wenn Sie die Region EU oder eu-West-1 nutzen möchten, müssen Sie den genauen Namen verwenden.

- Sie können eine Region nicht löschen oder ändern, wenn sie in einer Regel verwendet wird, die einer Richtlinie zugewiesen ist (aktiv oder inaktiv).
- Wenn Sie eine ungültige Region als erweiterten Filter in einer ILM-Regel verwenden, können Sie diese Regel nicht zu einer Richtlinie hinzufügen.

  Eine ungültige Region kann sich ergeben, wenn Sie eine Region als erweiterten Filter in einer ILM-Regel verwenden, diese Region jedoch später löschen oder wenn Sie die Grid-Management-API zum Erstellen einer Regel und zum Festlegen einer Region verwenden, die Sie nicht definiert haben.

- Wenn Sie eine Region löschen, nachdem Sie sie zum Erstellen eines S3-Buckets verwendet haben, müssen Sie die Region erneut hinzufügen, wenn Sie den erweiterten Filter Speicherungsbedingung verwenden möchten, um Objekte in diesem Bucket zu finden.

Schritte

1. Wählen Sie **ILM** > **Regionen**.

   Die Seite Regionen wird angezeigt, wobei die derzeit definierten Regionen aufgelistet sind. **Region 1** zeigt die Standardregion an, `us-east-1` die weder geändert noch entfernt werden kann.

2. So fügen Sie eine Region hinzu:
   a. Wählen Sie **Weitere Region hinzufügen**.

b. Geben Sie den Namen einer Region ein, die Sie beim Erstellen von S3-Buckets verwenden möchten.

   Sie müssen diesen genauen Regionalnamen als LocationConstraint Request Element verwenden, wenn Sie den entsprechenden S3-Bucket erstellen.

3. Um einen nicht verwendeten Bereich zu entfernen, wählen Sie das Löschen-Symbol ✕.

   Wenn Sie versuchen, eine Region zu entfernen, die derzeit in einer Richtlinie (aktiv oder inaktiv) verwendet wird, wird eine Fehlermeldung angezeigt.

4. Wenn Sie Änderungen vorgenommen haben, wählen Sie **Speichern**.

   Sie können diese Bereiche nun im Abschnitt Erweiterte Filter in Schritt 1 des Assistenten zum Erstellen von ILM-Regeln auswählen. Siehe "Verwenden Sie erweiterte Filter in ILM-Regeln".

ILM-Regel erstellen

Verwenden Sie ILM-Regeln zum Managen von Objekten

Zum Managen von Objekten erstellen Sie eine Reihe von Regeln für das Information Lifecycle Management (ILM) und organisieren diese in eine ILM-Richtlinie.

Jedes im System aufgenommene Objekt wird anhand der aktiven Richtlinie ausgewertet. Wenn eine Regel in der Richtlinie mit den Metadaten eines Objekts übereinstimmt, bestimmen die Anweisungen in der Regel, welche Aktionen StorageGRID zum Kopieren und Speichern des Objekts ergreift.

> ⓘ Objektmetadaten werden nicht durch ILM-Regeln gemanagt. Stattdessen werden Objekt-Metadaten in einer Cassandra-Datenbank in einem sogenannten Metadaten-Speicher gespeichert. Drei Kopien von Objekt-Metadaten werden automatisch an jedem Standort aufbewahrt, um die Daten vor Verlust zu schützen.

Elemente einer ILM-Regel

Eine ILM-Regel besteht aus drei Elementen:

- **Filterkriterien**: Die Basis- und erweiterten Filter einer Regel definieren, für welche Objekte die Regel gilt. Wenn ein Objekt allen Filtern entspricht, wendet StorageGRID die Regel an und erstellt die Objektkopien, die in den Platzierungsanweisungen der Regel angegeben sind.
- **Platzierungsanweisungen**: Die Platzierungsanweisungen einer Regel definieren die Zahl, den Typ und den Ort von Objektkopien. Jede Regel kann eine Reihe von Anweisungen zur Platzierung enthalten, um die Anzahl, den Typ und den Standort der Objektkopien im Laufe der Zeit zu ändern. Wenn der Zeitraum für eine Platzierung abgelaufen ist, werden die Anweisungen in der nächsten Platzierung automatisch bei der nächsten ILM-Bewertung angewendet.
- **Ingest Behavior**: Das Ingest Behavior einer Regel erlaubt Ihnen zu wählen, wie die Objekte, die durch die Regel gefiltert werden, geschützt werden, wenn sie aufgenommen werden (wenn ein S3-Client ein Objekt im Grid speichert).

ILM-Regelfilterung

Wenn Sie eine ILM-Regel erstellen, geben Sie Filter an, um zu identifizieren, für welche Objekte die Regel gilt.

Im einfachsten Fall verwendet eine Regel möglicherweise keine Filter. Alle Regeln, die keine Filter verwenden,

gelten für alle Objekte. Daher muss es sich um die letzte (standardmäßige) Regel in einer ILM-Richtlinie handelt. Die Standardregel enthält Speicheranweisungen für Objekte, die nicht mit den Filtern einer anderen Regel übereinstimmen.

- Grundlegende Filter ermöglichen es Ihnen, unterschiedliche Regeln auf große, unterschiedliche Objektgruppen anzuwenden. Mit diesen Filtern können Sie eine Regel auf bestimmte Mandantenkonten, bestimmte S3-Buckets oder beides anwenden.

  Grundlegende Filter geben Ihnen eine einfache Möglichkeit, verschiedene Regeln auf eine große Anzahl von Objekten anzuwenden. So müssen beispielsweise die Finanzdaten Ihres Unternehmens möglicherweise gespeichert werden, um gesetzliche Vorgaben einzuhalten. Daten aus der Marketing-Abteilung müssen möglicherweise gespeichert werden, um den täglichen Betrieb zu erleichtern. Nach der Erstellung separater Mandantenkonten für jede Abteilung oder nach Trennung von Daten aus den verschiedenen Abteilungen in separate S3 Buckets können Sie problemlos eine Regel erstellen, die für alle Finanzdaten und eine zweite Regel gilt für alle Marketingdaten.

- Erweiterte Filter geben Ihnen eine präzise Kontrolle. Sie können Filter erstellen, um Objekte anhand der folgenden Objekteigenschaften auszuwählen:
  - Aufnahmezeit
  - Zeitpunkt des letzten Zugriffs
  - Der Objektname (Schlüssel) ganz oder teilweise
  - Speicherortbeschränkung (nur S3)
  - Objektgröße
  - Benutzer-Metadaten
  - Objekt-Tag (nur S3)

Sie können Objekte nach sehr spezifischen Kriterien filtern. So können beispielsweise Objekte, die von der Bildgebungsabteilung eines Krankenhauses gespeichert sind, häufig verwendet werden, wenn sie weniger als 30 Tage alt und selten danach sind, während Objekte, die Angaben zu Patientenbesuchen enthalten, möglicherweise in die Rechnungsabteilung des Gesundheitsnetzwerks kopiert werden müssen. Sie können Filter erstellen, die jeden Objekttyp anhand von Objektnamen, -Größe, S3-Objekt-Tags oder anderen relevanten Kriterien identifizieren. Anschließend können separate Regeln erstellt werden, um jeden Objektsatz entsprechend zu speichern.

Sie können Filter nach Bedarf in einer einzigen Regel kombinieren. Beispielsweise möchte die Marketingabteilung große Bilddateien anders speichern als die Lieferantendaten, während die Personalabteilung Personaldatensätze in einer bestimmten Region und in einer bestimmten Richtlinie zentral speichern muss. In diesem Fall können Sie Regeln erstellen, die nach Mandantenkonto filtern, um die Datensätze von jeder Abteilung zu trennen, während Sie in jeder Regel Filter verwenden, um den spezifischen Objekttyp zu identifizieren, auf den die Regel angewendet wird.

Anweisungen zur Platzierung von ILM-Regeln

Eine Anleitung zur Platzierung bestimmt, wo, wann und wie Objektdaten gespeichert werden. Eine ILM-Regel kann eine oder mehrere Anweisungen zur Platzierung enthalten. Jede Einstufungsanweisung gilt für einen einzelnen Zeitraum.

Wenn Sie Anweisungen zur Platzierung erstellen:

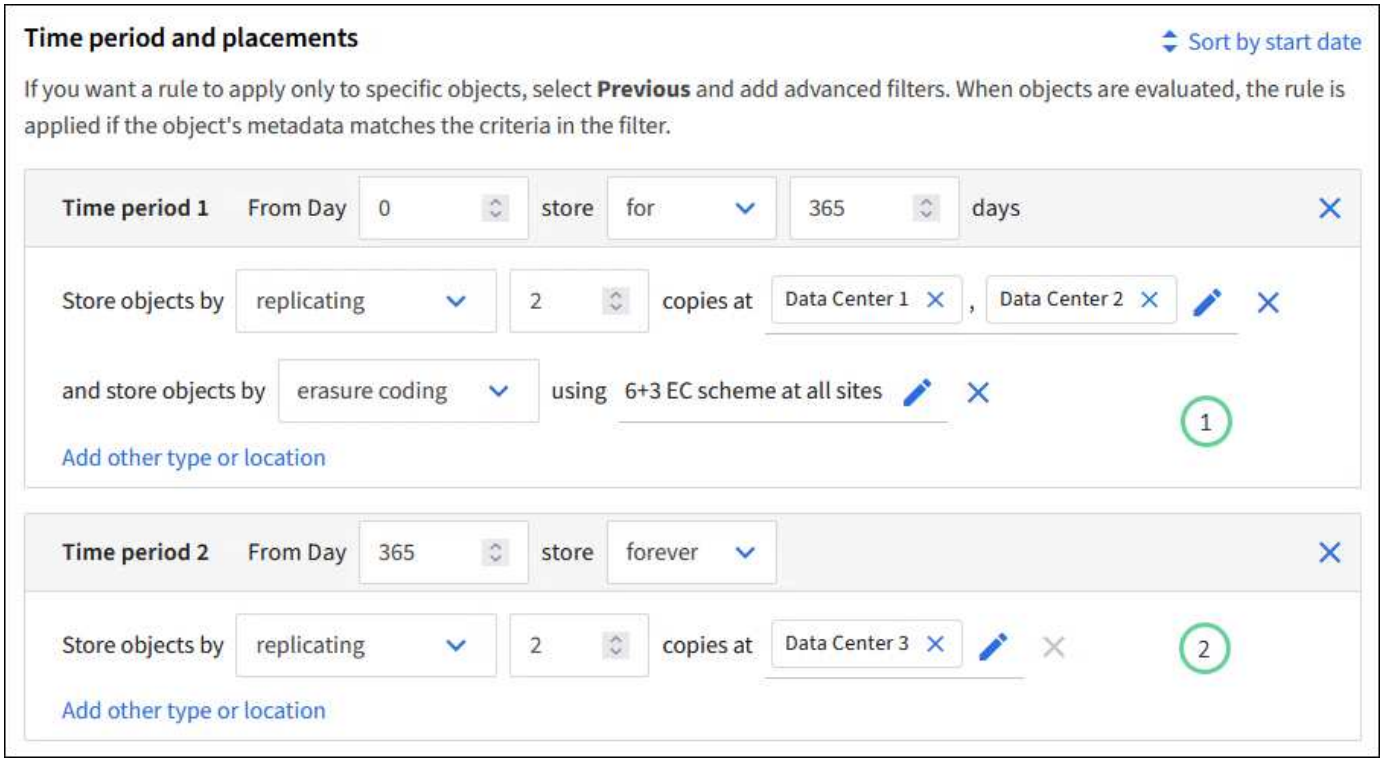
- Sie beginnen mit der Angabe der Referenzzeit, die bestimmt, wann die Platzierungsanweisungen beginnen. Die Referenzzeit kann sein, wenn ein Objekt aufgenommen wird, wenn auf ein Objekt zugegriffen wird, wenn ein versioniertes Objekt nicht mehr aktuell wird oder eine benutzerdefinierte Zeit.

- Als Nächstes geben Sie an, wann die Platzierung in Bezug auf die Referenzzeit gelten soll. Beispielsweise kann eine Platzierung am Tag 0 beginnen und 365 Tage lang fortgesetzt werden, relativ zu dem Zeitpunkt, zu dem das Objekt aufgenommen wurde.
- Schließlich geben Sie die Art der Kopien (Replizierung oder Erasure Coding) und den Speicherort der Kopien an. So können Sie beispielsweise zwei replizierte Kopien an zwei unterschiedlichen Standorten speichern.

Jede Regel kann mehrere Platzierungen für einen einzigen Zeitraum und verschiedene Platzierungen für unterschiedliche Zeiträume definieren.

- Um Objekte in einem Zeitraum an mehreren Orten zu platzieren, wählen Sie **anderen Typ oder Standort hinzufügen**, um mehr als eine Zeile für diesen Zeitraum hinzuzufügen.
- Um Objekte an verschiedenen Orten in verschiedenen Zeiträumen zu platzieren, wählen Sie **weiteren Zeitraum hinzufügen**, um den nächsten Zeitraum hinzuzufügen. Geben Sie dann eine oder mehrere Zeilen innerhalb des Zeitraums an.

Das Beispiel zeigt zwei Platzierungsanweisungen auf der Seite Platzierungen definieren des Assistenten zum Erstellen einer ILM-Regel.



Der erste Einstufungsunterricht (1) hat zwei Linien für das erste Jahr:

- In der ersten Zeile werden zwei replizierte Objektkopien an zwei Datacenter-Standorten erstellt.
- Die zweite Zeile erstellt eine Kopie, die unter Verwendung aller Datacenter-Standorte nach der Erasure-Coded-Funktion 6+3 enthält.

Die zweite Einstufungsanweisung (2) erstellt zwei Kopien nach einem Jahr und speichert diese Kopien für immer.

Wenn Sie den Satz von Anweisungen zur Platzierung für eine Regel definieren, müssen Sie sicherstellen, dass

mindestens eine Platzierungsanweisung an Tag 0 beginnt, dass zwischen den von Ihnen definierten Zeiträumen keine Lücken bestehen. Und dass die abschließende Anweisung zum Platzieren entweder für immer oder bis Sie keine Objektkopien mehr benötigen.

Da jeder Zeitraum in der Regel abläuft, werden die Anweisungen zur Inhaltsplatzierung für den nächsten Zeitraum angewendet. Neue Objektkopien werden erstellt und nicht benötigte Kopien werden gelöscht.

ILM-Regel Aufnahme-Verhalten

Das Aufnahmeverhalten steuert, ob Objektkopien sofort nach den Anweisungen in der Regel platziert werden oder ob zwischenzeitliche Kopien erstellt und die Speicheranweisungen später angewendet werden. Die folgenden Aufnahmeverhalten stehen für ILM-Regeln zur Verfügung:

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

Verwandte Informationen

- "Aufnahmeoptionen"
- "Vorteile, Nachteile und Einschränkungen der Aufnahmsoptionen"
- "Zusammenspiel von Konsistenz- und ILM-Regeln zur Beeinträchtigung der Datensicherung"

Beispiel für eine ILM-Regel

Eine ILM-Regel könnte beispielsweise Folgendes angeben:

- Nur auf die Objekte anwenden, die zu Mandant A gehören
- Erstellen Sie zwei replizierte Kopien dieser Objekte und speichern Sie jede Kopie an einem anderen Standort.
- Behalten Sie die beiden Kopien „für immer“ bei, was bedeutet, dass sie von StorageGRID nicht automatisch gelöscht werden. Stattdessen behält StorageGRID diese Objekte so lange bei, bis sie von einer Löschanfrage eines Clients oder nach Ablauf eines Bucket-Lebenszyklus gelöscht werden.
- Verwenden Sie die ausgewogene Option für das Aufnahmeverhalten: Die Anweisung zur Platzierung von zwei Standorten wird angewendet, sobald Mandant A ein Objekt in StorageGRID speichert, es sei denn, es ist nicht möglich, sofort beide erforderlichen Kopien zu erstellen.

  Wenn z. B. Standort 2 nicht erreichbar ist, wenn Mandant A ein Objekt speichert, erstellt StorageGRID zwei Zwischenkopien auf Storage-Nodes an Standort 1. Sobald Standort 2 verfügbar wird, erstellt StorageGRID die erforderliche Kopie an diesem Standort.

Verwandte Informationen

- "Was ist ein Speicherpool"
- "Was ist ein Cloud-Storage-Pool"

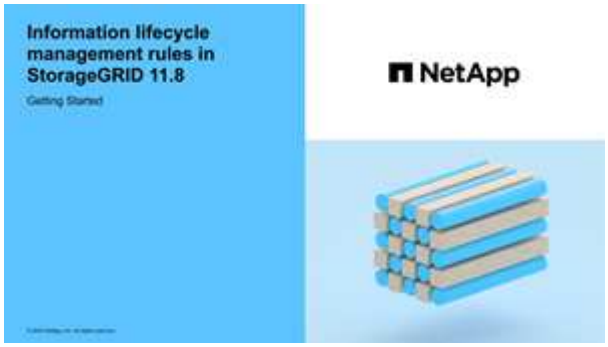
Greifen Sie auf den Assistenten zum Erstellen einer ILM-Regel zu

ILM-Regeln ermöglichen es Ihnen, die Platzierung von Objektdaten im Laufe der Zeit zu managen. Zum Erstellen einer ILM-Regel verwenden Sie den Assistenten zum Erstellen einer ILM-Regel.

Wenn Sie die standardmäßige ILM-Regel für eine Richtlinie erstellen möchten, befolgen Sie stattdessen die "Anweisungen zum Erstellen einer standardmäßigen ILM-Regel"Anweisungen.

Bevor Sie beginnen

- Sie sind im Grid Manager mit einem angemeldet"Unterstützter Webbrowser".
- Sie haben "Bestimmte Zugriffsberechtigungen".
- Wenn Sie angeben möchten, für welche Mandantenkonten diese Regel gilt, verfügen Sie über die oder Sie kennen die "Berechtigung für Mandantenkonten"Konto-ID für jedes Konto.
- Wenn die Regel Objekte nach Metadaten der Uhrzeit des letzten Zugriffs filtern soll, müssen die Updates der Uhrzeit des letzten Zugriffs durch S3 Bucket aktiviert werden.
- Sie haben alle Cloud-Storage-Pools konfiguriert, die Sie verwenden möchten. Siehe "Cloud Storage Pool Erstellen".
- Sie kennen die "Aufnahmeoptionen".
- Wenn Sie eine konforme Regel für die Verwendung mit S3 Object Lock erstellen müssen, sind Sie mit dem vertraut"Anforderungen für die S3-Objektsperre".
- Optional haben Sie sich das Video angesehen: "Video: ILM-Regeln im Überblick".



Über diese Aufgabe

Wenn ILM-Regeln erstellt werden:

- Dabei sind die Topologie und Storage-Konfigurationen des StorageGRID Systems zu berücksichtigen.
- Überlegen Sie, welche Objektkopien Sie erstellen möchten (repliziert oder Erasure Coded) und wie viele Kopien jedes Objekts benötigt werden.
- Legen Sie fest, welche Typen von Objekt-Metadaten in den Applikationen verwendet werden, die sich mit dem StorageGRID System verbinden. ILM-Regeln filtern Objekte auf Basis ihrer Metadaten.
- Dabei sollten Sie berücksichtigen, wo Sie Objektkopien über einen längeren Zeitraum ablegen möchten.
- Entscheiden Sie, welche Aufnahmeoption verwendet werden soll (ausgeglichen, streng oder doppelte Übertragung).

Schritte

1. Wählen Sie **ILM** > **Regeln**.
2. Wählen Sie **Erstellen**. "Schritt 1 (Details eingeben)" Des Assistenten zum Erstellen einer ILM-Regel wird angezeigt.

Schritt 1 von 3: Details eingeben

Im Schritt **Details eingeben** des Assistenten zum Erstellen einer ILM-Regel können Sie einen Namen und eine Beschreibung für die Regel eingeben und Filter für die Regel definieren.

Die Eingabe einer Beschreibung und das Definieren von Filtern für die Regel sind optional.

Über diese Aufgabe

Bei der Auswertung eines Objekts "ILM-Regel"mit einem vergleicht StorageGRID die Objektmetadaten mit den Filtern der Regel. Wenn die Objektmetadaten mit allen Filtern übereinstimmen, verwendet StorageGRID die Regel, um das Objekt abzulegen. Sie können eine Regel für alle Objekte entwerfen oder grundlegende Filter angeben, z. B. ein oder mehrere Mandantenkonten und Bucket-Namen oder erweiterte Filter, wie z. B. Größe des Objekts oder Benutzermetadaten.

Schritte

1. Geben Sie im Feld **Name** einen eindeutigen Namen für die Regel ein.
2. Geben Sie optional im Feld **Beschreibung** eine kurze Beschreibung für die Regel ein.

   Sie sollten den Zweck oder die Funktion der Regel beschreiben, damit Sie die Regel später erkennen können.

3. Wählen Sie optional ein oder mehrere S3-Mandantenkonten aus, auf die diese Regel angewendet wird. Wenn diese Regel für alle Mandanten gilt, lassen Sie dieses Feld leer.

   Wenn Sie weder über die Berechtigung für den Root-Zugriff noch über die Berechtigung für die Mandantenkonten verfügen, können Sie keine Mandanten aus der Liste auswählen. Geben Sie stattdessen die Mandanten-ID ein, oder geben Sie mehrere IDs als durch Komma getrennte Zeichenfolge ein.

4. Optional können Sie die S3-Buckets angeben, für die diese Regel gilt.

   Wenn **gilt für alle Buckets** ausgewählt ist (Standard), gilt die Regel für alle S3 Buckets.

5. Wählen Sie für S3-Mandanten optional **Yes** aus, um die Regel nur auf ältere Objektversionen in S3-Buckets anzuwenden, für die die Versionierung aktiviert ist.

   Wenn Sie **Yes** auswählen, wird automatisch für die Referenzzeit in die Option „Zeitdauer nicht aktuell“ ausgewählt"Schritt 2 des Assistenten zum Erstellen einer ILM-Regel".

   > Die nicht aktuelle Zeit gilt nur für S3 Objekte in versionierungsfähigen Buckets. Siehe "Operationen auf Buckets, PutketVersioning" und "Objekte managen mit S3 Object Lock".

   Mit dieser Option können Sie die Auswirkungen versionierter Objekte auf den Speicher reduzieren, indem Sie nach nicht aktuellen Objektversionen filtern. Siehe "Beispiel 4: ILM-Regeln und -Richtlinie für versionierte Objekte mit S3".

6. Wählen Sie optional **Erweiterten Filter hinzufügen**, um weitere Filter festzulegen.

Wenn Sie keine erweiterte Filterung konfigurieren, gilt die Regel für alle Objekte, die den Grundfiltern entsprechen. Weitere Informationen zum erweiterten Filtern finden Sie unter Verwenden Sie erweiterte Filter in ILM-Regeln und Geben Sie mehrere Metadatentypen und -Werte an.

7. Wählen Sie **Weiter**. "Schritt 2 (Platzierungen definieren)" Des Assistenten zum Erstellen einer ILM-Regel wird angezeigt.

Verwenden Sie erweiterte Filter in ILM-Regeln

Mit der erweiterten Filterung können Sie ILM-Regeln erstellen, die sich nur auf bestimmte Objekte anwenden lassen, basierend auf ihren Metadaten. Wenn Sie die erweiterte Filterung für eine Regel einrichten, wählen Sie den Metadatentyp aus, der übereinstimmen soll, wählen Sie einen Operator aus und geben einen Metadatenwert an. Wenn Objekte ausgewertet werden, wird die ILM-Regel nur auf Objekte angewendet, die Metadaten enthalten, die dem erweiterten Filter entsprechen.

Die Tabelle zeigt die Metadatentypen, die Sie in den erweiterten Filtern angeben können, die Operatoren, die Sie für jeden Metadatentyp verwenden können, und die erwarteten Metadaten.

Metadatentyp	Unterstützte Operatoren	Metadatenwert
Aufnahmezeit	• Ist • Ist es nicht • Ist vorher • Ist ein oder vorher • Ist nachher • Ist ein oder nach	Uhrzeit und Datum, an dem das Objekt aufgenommen wurde. **Hinweis:** um Ressourcenprobleme bei der Aktivierung einer neuen ILM-Richtlinie zu vermeiden, können Sie den erweiterten Filter für die Einspielzeit in jeder Regel verwenden, die den Speicherort einer großen Anzahl vorhandener Objekte ändern könnte. Legen Sie für die Aufnahme-Zeit den Wert fest, der ungefähr der Zeit entspricht, zu der die neue Richtlinie in Kraft tritt, um sicherzustellen, dass vorhandene Objekte nicht unnötig verschoben werden.
Taste	• Gleich • Ist nicht gleich • Enthält • Enthält nicht • Beginnt mit • Startet nicht mit • Endet mit • Endet nicht mit	Ein eindeutiger S3-Objektschlüssel oder Teile davon. Sie können z. B. Objekte zuordnen, die mit enden `.txt` oder mit beginnen `test-object/`.

Metadatentyp	Unterstützte Operatoren	Metadatenwert
Zeitpunkt des letzten Zugriffs	• Ist • Ist es nicht • Ist vorher • Ist ein oder vorher • Ist nachher • Ist ein oder nach	Uhrzeit und Datum, an dem das Objekt zuletzt abgerufen wurde (gelesen oder angezeigt). **Hinweis:** Wenn Sie einen erweiterten Filter verwenden möchten"Letzte Zugriffszeit verwenden", müssen die Updates für die Uhrzeit des letzten Zugriffs für den S3-Bucket aktiviert sein.
Speicherortbeschränkung (nur S3)	• Gleich • Ist nicht gleich	Die Region, in der ein S3-Bucket erstellt wurde. Verwenden Sie **ILM** > **Regionen**, um die angezeigten Regionen zu definieren. **Hinweis:** Ein Wert von US-East-1 entspricht Objekten in Eimern, die in der Region US-East-1 erstellt wurden, sowie Objekten in Buckets, die keine Region angegeben haben. Siehe "Regionen konfigurieren (nur optional und S3)".
Objektgröße	• Gleich • Ist nicht gleich • Kleiner als • Kleiner als oder gleich • Größer als • Größer als oder gleich	Die Größe des Objekts. Das Verfahren zur Einhaltung von Datenkonsistenz eignet sich am besten für Objekte mit einer Größe von mehr als 1 MB. Verwenden Sie kein Erasure Coding für Objekte, die kleiner als 200 KB sind, um zu vermeiden, dass man sehr kleine Fragmente, die zur Fehlerkorrektur codiert wurden, managen muss.
Benutzer-Metadaten	• Enthält • Endet mit • Gleich • Vorhanden • Beginnt mit • Enthält nicht • Endet nicht mit • Ist nicht gleich • Nicht vorhanden • Startet nicht mit	Schlüssel-Wert-Paar, wobei **Benutzer-Metadaten-Name** der Schlüssel und **Metadaten-Wert** der Wert ist. Wenn Sie beispielsweise nach Objekten filtern möchten, die Benutzermetadaten von haben `color=blue`, geben Sie für **Name der Benutzermetadaten**, für den Operator und `blue` für **Metadatenwert** **`equals`** an `color`. **Hinweis:** Benutzer-Metadaten-Namen sind nicht zwischen Groß- und Kleinschreibung zu beachten; Benutzer-Metadaten-Werte sind Groß- und Kleinschreibung zu beachten.

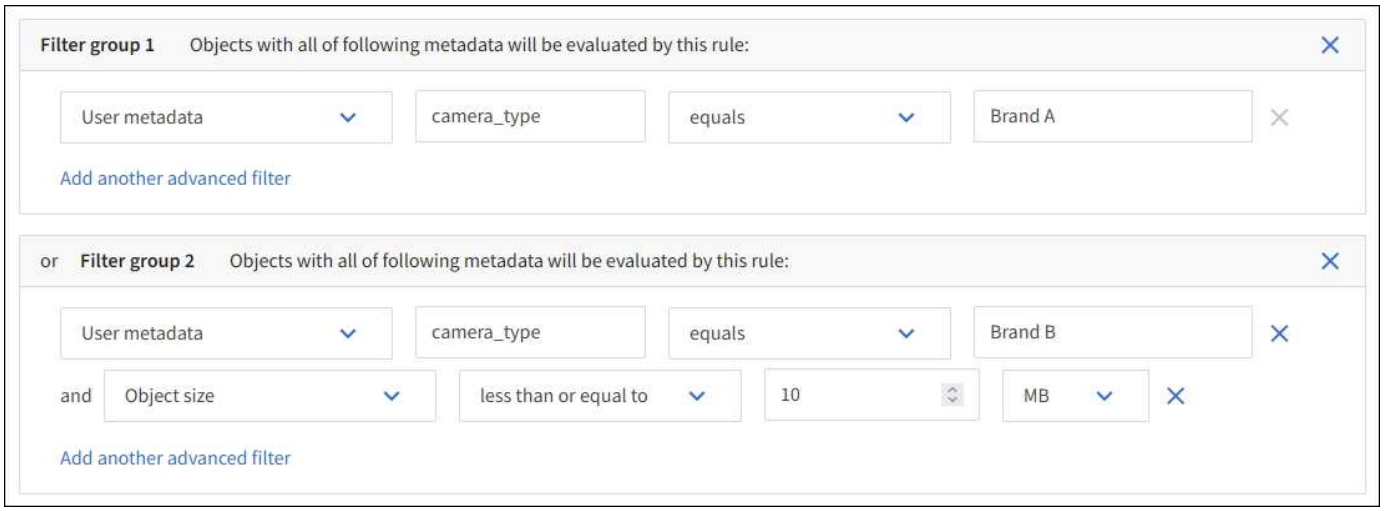
Metadatentyp	Unterstützte Operatoren	Metadatenwert
Objekt-Tag (nur S3)	• Enthält • Endet mit • Gleich • Vorhanden • Beginnt mit • Enthält nicht • Endet nicht mit • Ist nicht gleich • Nicht vorhanden • Startet nicht mit	Schlüssel-Wert-Paar, wobei **Objekt-Tag-Name** der Schlüssel und **Objekt-Tag-Wert** der Wert ist. Wenn Sie beispielsweise nach Objekten filtern möchten, die ein Objekt-Tag von haben `Image=True`, geben Sie für **Objekt-Tag-Name**, `equals` für den Operator und `True` für **Objekt-Tag-Wert** an `Image`. **Hinweis:** Objekt-Tag-Namen und Objekt-Tag-Werte sind Groß- und Kleinschreibung. Sie müssen diese Elemente genau so eingeben, wie sie für das Objekt definiert wurden.

Geben Sie mehrere Metadatentypen und -Werte an

Wenn Sie die erweiterte Filterung definieren, können Sie mehrere Metadatentypen und mehrere Metadatenwerte angeben. Wenn Sie beispielsweise eine Regel mit Objekten zwischen 10 MB und 100 MB Größe vergleichen möchten, wählen Sie den Metadatentyp **Objektgröße** aus und geben zwei Metadatenwerte an.

- Der erste Metadatenwert gibt Objekte an, die größer oder gleich 10 MB sind.
- Der zweite Metadatenwert gibt Objekte an, die kleiner als oder gleich 100 MB sind.

Durch die Verwendung mehrerer Einträge können Sie genau steuern, welche Objekte abgeglichen werden. Im folgenden Beispiel gilt die Regel für Objekte, die Marke A oder Marke B als Wert der Benutzermetadaten Camera_type haben. Die Regel gilt jedoch nur für Objekte der Marke B, die kleiner als 10 MB sind.



Schritt 2 von 3: Definieren von Platzierungen

Im Schritt **Platzierungen definieren** des Assistenten zum Erstellen von ILM-Regeln können Sie die Platzierungsanweisungen definieren, die festlegen, wie lange Objekte gespeichert werden, welche Art von Kopien (repliziert oder Erasure-coded), den Speicherort und die Anzahl der Kopien.

> Die gezeigten Screenshots sind Beispiele. Die Ergebnisse können je nach StorageGRID-Version variieren.

Über diese Aufgabe

Eine ILM-Regel kann eine oder mehrere Anweisungen zur Platzierung enthalten. Jede Einstufungsanweisung gilt für einen einzelnen Zeitraum. Wenn Sie mehrere Befehle verwenden, müssen die Zeiträume zusammenhängend sein, und mindestens eine Anweisung muss am Tag 0 beginnen. Die Anweisungen können entweder für immer fortgesetzt werden oder bis Sie keine Objektkopien mehr benötigen.

Jede Anweisung für die Platzierung kann mehrere Zeilen haben, wenn Sie verschiedene Arten von Kopien erstellen oder verschiedene Standorte während dieses Zeitraums verwenden möchten.

In diesem Beispiel speichert die ILM-Regel eine replizierte Kopie an Standort 1 und eine replizierte Kopie am Standort 2 im ersten Jahr. Nach einem Jahr wird eine 2+1-Kopie mit Erasure-Coding-Verfahren an nur einem Standort erstellt und gespeichert.

Schritte

1. Wählen Sie unter **Referenzzeit** den Zeittyp aus, der bei der Berechnung der Startzeit für eine Platzierungsanweisung verwendet werden soll.

Option	Beschreibung
Aufnahmezeit	Die Zeit, zu der das Objekt aufgenommen wurde.

Option	Beschreibung
Zeitpunkt des letzten Zugriffs	Die Zeit, zu der das Objekt zuletzt abgerufen (gelesen oder angezeigt) wurde. Um diese Option zu verwenden, müssen für den S3-Bucket Updates zur Uhrzeit des letzten Zugriffs aktiviert sein. Siehe "Verwenden Sie die letzte Zugriffszeit in ILM-Regeln".
Benutzerdefinierte Erstellungszeit	Eine in benutzerdefinierten Metadaten angegebene Zeit.
Nicht aktuelle Zeit	„Nicht aktuelle Zeit“ wird automatisch ausgewählt, wenn Sie **Ja** für die Frage „Diese Regel nur auf ältere Objektversionen anwenden (in S3 Buckets mit aktivierter Versionierung)?“ in ausgewählt "Schritt 1 des Assistenten zum Erstellen einer ILM-Regel"haben.

Wenn Sie eine *compliant* -Regel erstellen möchten, müssen Sie **Ingest time** auswählen. Siehe "Objekte managen mit S3 Object Lock".

2. Geben Sie im Abschnitt **Zeitraum und Platzierungen** eine Startzeit und eine Dauer für den ersten Zeitraum ein.

   Sie können beispielsweise festlegen, wo Objekte für das erste Jahr gespeichert werden sollen (*von Tag 0 für 365 Tage*). Mindestens eine Anweisung muss am Tag 0 beginnen.

3. So erstellen Sie replizierte Kopien:

   a. Wählen Sie aus der Dropdown-Liste **Objekte speichern nach** die Option **Replizieren** aus.

   b. Wählen Sie die Anzahl der Kopien aus, die Sie erstellen möchten.

      Wenn Sie die Anzahl der Kopien in 1 ändern, wird eine Warnung angezeigt. Eine ILM-Regel, die immer nur eine replizierte Kopie erstellt, gefährdet Daten permanent. Siehe "Warum sollten Sie keine Replizierung mit nur einer Kopie verwenden".

      Um dieses Risiko zu vermeiden, führen Sie einen oder mehrere der folgenden Schritte aus:

      - Erhöhen Sie die Anzahl der Kopien für den Zeitraum.
      - Fügen Sie Kopien zu anderen Speicherpools oder zu einem Cloud-Speicherpool hinzu.
      - Wählen Sie **Erasure Coding** anstelle von **replizierung**.

        Sie können diese Warnung ohne Bedenken ignorieren, wenn diese Regel bereits mehrere Kopien für alle Zeiträume erstellt.

   c. Wählen Sie im Feld **copies at** die Speicherpools aus, die Sie hinzufügen möchten.

      Wenn Sie nur einen Speicherpool angeben, beachten Sie, dass StorageGRID nur eine replizierte Kopie eines Objekts auf einem beliebigen Speicherknoten speichern kann. Wenn Ihr Raster drei Storage-Nodes enthält und Sie 4 als Anzahl der Kopien auswählen, werden nur drei Kopien erstellt—eine Kopie für jeden Storage-Node.

      Die Warnung **ILM-Platzierung unerreichbar** wird ausgelöst, um anzuzeigen, dass die ILM-Regel nicht vollständig angewendet werden konnte.

Wenn Sie mehr als einen Speicherpool angeben, beachten Sie folgende Regeln:

- Die Anzahl der Kopien darf nicht größer sein als die Anzahl der Speicherpools.
- Wenn die Anzahl der Kopien der Anzahl der Storage-Pools entspricht, wird in jedem Storage-Pool eine Kopie des Objekts gespeichert.
- Wenn die Anzahl der Kopien geringer ist als die Anzahl der Storage-Pools, wird eine Kopie am Aufnahmeport gespeichert, und das System verteilt die restlichen Kopien, um die Festplattennutzung unter den Pools gleichmäßig zu halten. Dabei wird sichergestellt, dass kein Standort mehr als eine Kopie eines Objekts erhält.
- Wenn sich die Speicherpools überschneiden (die gleichen Storage-Nodes enthalten), werden möglicherweise alle Kopien des Objekts an nur einem Standort gespeichert. Geben Sie daher nicht den Speicherpool Alle Speicherknoten (StorageGRID 11.6 und früher) und einen anderen Speicherpool an.

4. Wenn Sie eine Kopie mit Verfahren zur Einhaltung von Datenkonsistenz (Erasure Coding) erstellen möchten:

   a. Wählen Sie aus der Dropdown-Liste **Objekte speichern nach** die Option **Erasure Coding** aus.

   > Das Verfahren zur Einhaltung von Datenkonsistenz eignet sich am besten für Objekte mit einer Größe von mehr als 1 MB. Verwenden Sie kein Erasure Coding für Objekte, die kleiner als 200 KB sind, um zu vermeiden, dass man sehr kleine Fragmente, die zur Fehlerkorrektur codiert wurden, managen muss.

   b. Wenn Sie keinen Filter für die Objektgröße für einen Wert größer als 200 KB hinzugefügt haben, wählen Sie **Zurück**, um zu Schritt 1 zurückzukehren. Wählen Sie dann **Add an Advanced Filter** und setzen Sie einen **Object size** Filter auf einen Wert größer als 200 KB.

   c. Wählen Sie den Speicherpool aus, den Sie hinzufügen möchten, und das Erasure-Coding-Schema, das Sie verwenden möchten.

      Der Speicherort für eine Kopie, die nach der Fehlerkorrektur codiert wurde, enthält den Namen des Erasure Coding-Schemas und den Namen des Storage-Pools.

   Verfügbare Schemata zur Einhaltung von Datenkonsistenz werden durch die Anzahl der Storage-Nodes im ausgewählten Storage-Pool begrenzt. `Recommended`Neben den Schemata, die entweder die "Beste Sicherung oder geringster Storage Overhead".

5. Optional:

   a. Wählen Sie **anderen Typ oder Speicherort hinzufügen**, um weitere Kopien an verschiedenen Standorten zu erstellen.

   b. Wählen Sie **weiteren Zeitraum hinzufügen**, um verschiedene Zeiträume hinzuzufügen.

   > Objektlöschungen werden auf Basis der folgenden Einstellungen vorgenommen:
   >
   > - Objekte werden am Ende des letzten Zeitraums automatisch gelöscht, es sei denn, ein anderer Zeitraum endet mit **forever**.
   > - Je nach "Einstellungen für den Aufbewahrungszeitraum von Buckets und Mandanten"werden Objekte möglicherweise auch dann nicht gelöscht, wenn der ILM-Aufbewahrungszeitraum endet.

6. Wenn Sie Objekte in einem Cloud-Speicherpool speichern möchten:

a. Wählen Sie in der Dropdown-Liste **Objekte speichern nach Replizieren** aus.

b. Wählen Sie das Feld **copies at** aus, und wählen Sie dann einen Cloud-Speicherpool aus.

   Beachten Sie bei der Verwendung von Cloud-Storage-Pools folgende Regeln:

   - Sie können nicht mehr als einen Cloud Storage-Pool in einer einzelnen Anweisung auswählen. Ebenso können Sie keinen Cloud-Storage-Pool und keinen Storage-Pool in derselben Anweisung auswählen.
   - Sie können nur eine Kopie eines Objekts in einem beliebigen Cloud Storage Pool speichern. Wenn Sie **Copies** auf 2 oder mehr setzen, wird eine Fehlermeldung angezeigt.
   - Es können nicht mehr als eine Objektkopie gleichzeitig in einem Cloud-Storage-Pool gespeichert werden. Eine Fehlermeldung wird angezeigt, wenn mehrere Platzierungen, die einen Cloud-Speicher-Pool verwenden, sich überschneidende Daten aufweisen oder wenn mehrere Zeilen derselben Platzierung einen Cloud-Storage-Pool verwenden.
   - Das Objekt kann in einem Cloud-Storage-Pool zur selben Zeit gespeichert werden, als replizierte oder Erasure-Coded-Kopien in StorageGRID. Sie müssen jedoch für den Zeitraum mehr als eine Zeile in die Platzierungsanweisung aufnehmen, damit Sie die Anzahl und die Typen der Kopien für jeden Speicherort angeben können.

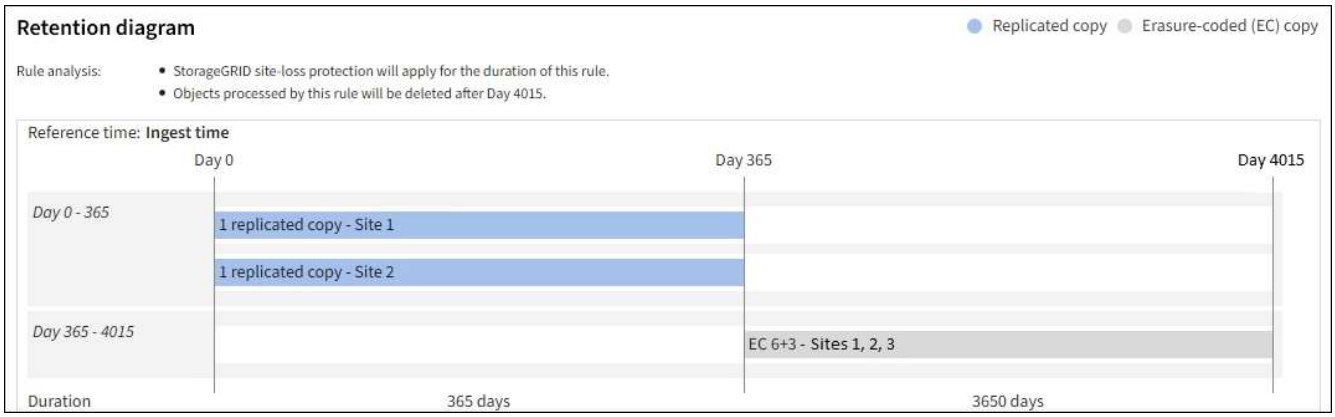
7. Bestätigen Sie im Aufbewahrungsdiagramm Ihre Platzierungsanweisungen.

   In diesem Beispiel speichert die ILM-Regel eine replizierte Kopie an Standort 1 und eine replizierte Kopie am Standort 2 im ersten Jahr. Nach einem Jahr und für weitere 10 Jahre wird eine 6+3 Erasure-coded Kopie an drei Standorten gespeichert. Nach insgesamt 11 Jahren werden die Objekte aus StorageGRID gelöscht.

   Im Abschnitt Regelanalyse des Aufbewahrungsdiagramms steht Folgendes:

   - Für die Dauer dieser Regel gilt eine StorageGRID-Sicherung gegen vor-Ort-Verlust.
   - Durch diese Regel verarbeitete Objekte werden nach Tag 4015 gelöscht.

     Siehe "Schutz vor Standortausfällen"



8. Wählen Sie **Weiter**. "Schritt 3 (Aufnahmeverhalten auswählen)" Des Assistenten zum Erstellen einer ILM-Regel wird angezeigt.

Verwenden Sie die letzte Zugriffszeit in ILM-Regeln

Sie können die Uhrzeit des letzten Zugriffs als Referenzzeit in einer ILM-Regel verwenden. Sie möchten beispielsweise Objekte, die in den letzten drei Monaten auf

lokalen Speicherknoten angezeigt wurden, während Sie Objekte verschieben, die noch nicht in letzter Zeit an einen externen Standort betrachtet wurden. Sie können die Uhrzeit des letzten Zugriffs auch als erweiterten Filter verwenden, wenn eine ILM-Regel nur auf Objekte angewendet werden soll, auf die an einem bestimmten Datum zuletzt zugegriffen wurde.

Über diese Aufgabe

Bevor Sie die letzte Zugriffszeit in einer ILM-Regel verwenden, sollten Sie die folgenden Überlegungen durchgehen:

- Wenn Sie die Uhrzeit des letzten Zugriffs als Referenzzeit verwenden, beachten Sie, dass die Änderung der Uhrzeit des letzten Zugriffs für ein Objekt keine sofortige ILM-Bewertung auslöst. Stattdessen werden die Platzierungen des Objekts bewertet und das Objekt nach Bedarf verschoben, wenn im Hintergrund ILM das Objekt bewertet wird. Dies kann zwei Wochen oder länger dauern, nachdem auf das Objekt zugegriffen wurde.

  Berücksichtigen Sie diese Latenz bei der Erstellung von ILM-Regeln auf der Grundlage der letzten Zugriffszeit und vermeiden Sie Platzierungen, die kurze Zeiträume (weniger als einen Monat) verwenden.

- Wenn Sie die letzte Zugriffszeit als erweiterten Filter oder als Referenzzeit verwenden, müssen Sie die Updates der letzten Zugriffszeit für S3-Buckets aktivieren. Sie können die oder die verwenden"Mandanten-Manager""Mandantenmanagement-API".

  Updates der Uhrzeit des letzten Zugriffs sind für S3 Buckets standardmäßig deaktiviert.

  Beachten Sie, dass eine Aktualisierung der letzten Zugriffszeit die Performance beeinträchtigen kann, insbesondere bei Systemen mit kleinen Objekten. Die Auswirkungen auf die Performance werden dadurch erzielt, dass StorageGRID die Objekte bei jedem Abruf mit neuen Zeitstempel aktualisieren muss.

In der folgenden Tabelle wird zusammengefasst, ob die Uhrzeit des letzten Zugriffs für alle Objekte im Bucket für verschiedene Arten von Anforderungen aktualisiert wird.

Art der Anfrage	Gibt an, ob die letzte Zugriffszeit aktualisiert wird, wenn die Updates der letzten Zugriffszeit deaktiviert sind	Gibt an, ob die letzte Zugriffszeit aktualisiert wird, wenn die Updates der letzten Zugriffszeit aktiviert sind
Anforderung zum Abrufen eines Objekts, seiner Zugriffssteuerungsliste oder seiner Metadaten	Nein	Ja.
Anforderung zum Aktualisieren der Metadaten eines Objekts	Ja.	Ja.
Anforderung zum Kopieren eines Objekts von einem Bucket in einen anderen	• Nein, für die Quellkopie • Ja, für die Zielkopie	• Ja, für die Quellkopie • Ja, für die Zielkopie

Art der Anfrage	Gibt an, ob die letzte Zugriffszeit aktualisiert wird, wenn die Updates der letzten Zugriffszeit deaktiviert sind	Gibt an, ob die letzte Zugriffszeit aktualisiert wird, wenn die Updates der letzten Zugriffszeit aktiviert sind
Anforderung zum Abschließen eines mehrteiligen Uploads	Ja, für das zusammengesetzte Objekt	Ja, für das zusammengesetzte Objekt

Schritt 3 von 3: Wählen Sie Ingest Behavior

Im Schritt **Einspielverhalten auswählen** des Assistenten zum Erstellen von ILM-Regeln können Sie festlegen, wie die von dieser Regel gefilterten Objekte bei der Aufnahme geschützt werden.

Über diese Aufgabe

StorageGRID erstellt Zwischenkopien und stellt die Objekte später zur ILM-Evaluierung in einen Warteschleife. Außerdem kann es Kopien erstellen, um sofort die Anweisungen zur Platzierung der Regel zu erfüllen.

Schritte

1. Wählen Sie die zu verwendende aus"Aufnahmeverhalten".

   Weitere Informationen finden Sie unter "Vorteile, Nachteile und Einschränkungen der Aufnahmsoptionen".

   Sie können die Option „ausgeglichen“ oder „streng“ nicht verwenden, wenn die Regel eine dieser Platzierungen verwendet:

   - Ein Cloud-Storage-Pool am Tag 0
   - Ein Cloud-Speicherpool, wenn die Regel eine benutzerdefinierte Erstellungszeit als Referenzzeit verwendet

   Siehe "Beispiel 5: ILM-Regeln und Richtlinie für striktes Ingest-Verhalten".

2. Wählen Sie **Erstellen**.

   Die ILM-Regel wird erstellt. Die Regel wird erst aktiv, wenn sie zu einem hinzugefügt und diese Richtlinie aktiviert wird"ILM-Richtlinie".

   Um die Details der Regel anzuzeigen, wählen Sie den Namen der Regel auf der Seite ILM-Regeln aus.

Erstellen einer Standard-ILM-Regel

Bevor Sie eine ILM-Richtlinie erstellen, müssen Sie eine Standardregel erstellen, um Objekte zu platzieren, die nicht mit einer anderen Regel in der Richtlinie übereinstimmt. Die Standardregel kann keine Filter verwenden. Die Lösung muss für alle Mandanten, alle Buckets und alle Objektversionen gelten.

Bevor Sie beginnen

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

Über diese Aufgabe

Die Standardregel ist die letzte Regel, die in einer ILM-Richtlinie evaluiert werden muss, sodass keine Filter verwendet werden können. Die Platzierungsanweisungen für die Standardregel werden auf alle Objekte angewendet, die nicht mit einer anderen Regel in der Richtlinie übereinstimmen.

In diesem Beispiel gilt die erste Regel nur für Objekte, die zu Test-Tenant-1 gehören. Die letzte Standardregel gilt für Objekte, die zu allen anderen Mandantenkonten gehören.

Beachten Sie beim Erstellen der Standardregel die folgenden Anforderungen:

- Die Standardregel wird automatisch als letzte Regel gesetzt, wenn Sie sie einer Richtlinie hinzufügen.
- Die Standardregel kann keine einfachen oder erweiterten Filter verwenden.
- Die Standardregel muss auf alle Objektversionen angewendet werden.
- Die Standardregel sollte replizierte Kopien erstellen.

> Verwenden Sie keine Regel, die Kopien, die nach der Löschung codiert wurden, als Standardregel für eine Richtlinie erstellt. Für die Einhaltung von Datenkonsistenz sollte ein erweiterter Filter verwendet werden, um zu verhindern, dass kleinere Objekte gelöscht werden.

- Im Allgemeinen sollte die Standardregel Objekte für immer aufbewahren.
- Wenn Sie die globale S3-Objektsperrung verwenden (oder aktivieren möchten), muss die Standardregel konform sein.

Schritte

1. Wählen Sie **ILM** > **Regeln**.
2. Wählen Sie **Erstellen**.

Schritt 1 (Details eingeben) des Assistenten zum Erstellen von ILM-Regeln wird angezeigt.

3. Geben Sie einen eindeutigen Namen für die Regel in das Feld **Regelname** ein.
4. Geben Sie optional im Feld **Beschreibung** eine kurze Beschreibung für die Regel ein.
5. Lassen Sie das Feld **Tenant Accounts** leer.

   Die Standardregel muss auf alle Mandantenkonten angewendet werden.

6. Lassen Sie die Dropdown-Liste „Bucket Name“ als **gilt für alle Buckets** gelten.

   Die Standardregel muss auf alle S3-Buckets angewendet werden.

7. Behalten Sie die Standardantwort **Nein** für die Frage „Diese Regel nur auf ältere Objektversionen anwenden (in S3 Buckets mit aktivierter Versionierung)?“ bei.
8. Fügen Sie keine erweiterten Filter hinzu.

   Die Standardregel kann keine Filter angeben.

9. Wählen Sie **Weiter**.

   Schritt 2 (Platzierungen definieren) wird angezeigt.

10. Wählen Sie für Referenzzeit eine beliebige Option aus.

    Wenn Sie die Standardantwort, **Nein**, für die Frage beibehalten haben: "Wenden Sie diese Regel nur auf ältere Objektversionen an?" Nicht aktuelle Zeit wird nicht in die Pulldown-Liste aufgenommen. Die Standardregel muss alle Objektversionen anwenden.

11. Legen Sie die Anweisungen für die Platzierung der Standardregel fest.
    - Die Standardregel sollte Objekte für immer aufbewahren. Wenn die Standardregel Objekte nicht dauerhaft enthält, wird eine Warnung angezeigt, wenn Sie eine neue Richtlinie aktivieren. Sie müssen bestätigen, dass dies das Verhalten ist, das Sie erwarten.
    - Die Standardregel sollte replizierte Kopien erstellen.

      > Verwenden Sie keine Regel, die Kopien, die nach der Löschung codiert wurden, als Standardregel für eine Richtlinie erstellt. Die Regeln für das Erasure Coding sollten den erweiterten Filter **Object size (MB) größer als 200 KB** enthalten, um zu verhindern, dass kleinere Objekte Erasure-codiert werden.

    - Wenn Sie die globale S3-Objektsperre verwenden (oder diese aktivieren möchten), muss die Standardregel konform sein:
      - Die IT muss mindestens zwei replizierte Objektkopien oder eine Kopie mit Verfahren zur Fehlerkorrektur erstellen.
      - Diese Kopien müssen auf Storage-Nodes während der gesamten Dauer jeder Zeile in der Plazierung vorhanden sein.
      - Objektkopien können nicht in einem Cloud-Storage-Pool gespeichert werden.
      - Mindestens eine Zeile der Platzierungsanweisungen muss am Tag 0 beginnen, wobei die Einspielzeit als Referenzzeit verwendet wird.
      - Mindestens eine Zeile der Platzierungsanweisungen muss „für immer“ lauten.

12. Sehen Sie sich das Aufbewahrungsdiagramm an, um Ihre Platzierungsanweisungen zu bestätigen.
13. Wählen Sie **Weiter**.

    Schritt 3 (Aufnahmeverhalten auswählen) wird angezeigt.

14. Wählen Sie die zu verwendende Ingest-Option und dann **Create**.

Managen von ILM-Richtlinien

Verwenden Sie ILM-Richtlinien

Eine Information Lifecycle Management-Richtlinie (ILM) ist ein bestellter Satz von ILM-Regeln, die bestimmen, wie das StorageGRID System Objektdaten über einen längeren Zeitraum managt.

> Eine falsch konfigurierte ILM-Richtlinie kann zu nicht wiederherstellbaren Datenverlusten führen. Prüfen Sie vor der Aktivierung einer ILM-Richtlinie die ILM-Richtlinie und ihre ILM-Regeln sorgfältig und simulieren Sie anschließend die ILM-Richtlinie. Vergewissern Sie sich immer, dass die ILM-Richtlinie wie vorgesehen funktioniert.

Standardmäßige ILM-Richtlinie

Bei der Installation von StorageGRID und dem Hinzufügen von Standorten wird automatisch eine standardmäßige ILM-Richtlinie erstellt:

- Wenn Ihr Raster einen Standort enthält, enthält die Standardrichtlinie eine Standardregel, die zwei Kopien jedes Objekts an diesem Standort repliziert.
- Wenn Ihr Raster mehr als einen Standort enthält, repliziert die Standardregel eine Kopie jedes Objekts an jedem Standort.

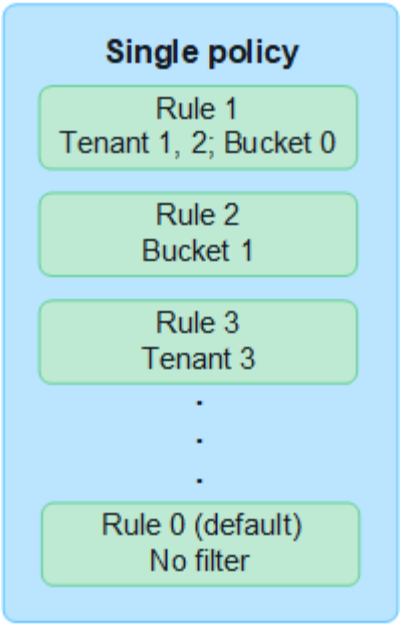
Entspricht die Standardrichtlinie nicht Ihren Storage-Anforderungen, können Sie eigene Regeln und Richtlinien erstellen. Siehe "Erstellen einer ILM-Regel" und "ILM-Richtlinie erstellen".

Eine oder viele aktive ILM-Richtlinien?

Sie können eine oder mehrere aktive ILM-Richtlinien gleichzeitig haben.

Eine Richtlinie

Wenn Ihr Grid ein einfaches Datensicherungsschema mit wenigen mandantenspezifischen und bucketspezifischen Regeln verwenden wird, verwenden Sie eine einzelne aktive ILM-Richtlinie. Die ILM-Regeln können Filter für das Management verschiedener Buckets oder Mandanten enthalten.



Wenn sich nur eine Richtlinie und die Anforderungen eines Mandanten ändern, müssen Sie eine neue ILM-Richtlinie erstellen oder die vorhandene Richtlinie klonen, um Änderungen anzuwenden, zu simulieren und dann die neue ILM-Richtlinie zu aktivieren. Änderungen an der ILM-Richtlinie können zu Objektverschiebungen führen, die viele Tage in Anspruch nehmen können und zu Systemlatenz führen.

Mehrere Richtlinien

Um Mandanten verschiedene Quality-of-Service-Optionen zur Verfügung zu stellen, können Sie mehrere aktive Richtlinien gleichzeitig bereitstellen. Jede Richtlinie kann bestimmte Mandanten, S3 Buckets und Objekte managen. Wenn Sie eine Richtlinie für einen bestimmten Satz von Mandanten oder Objekten anwenden oder ändern, werden die auf andere Mandanten und Objekte angewendeten Richtlinien nicht beeinträchtigt.

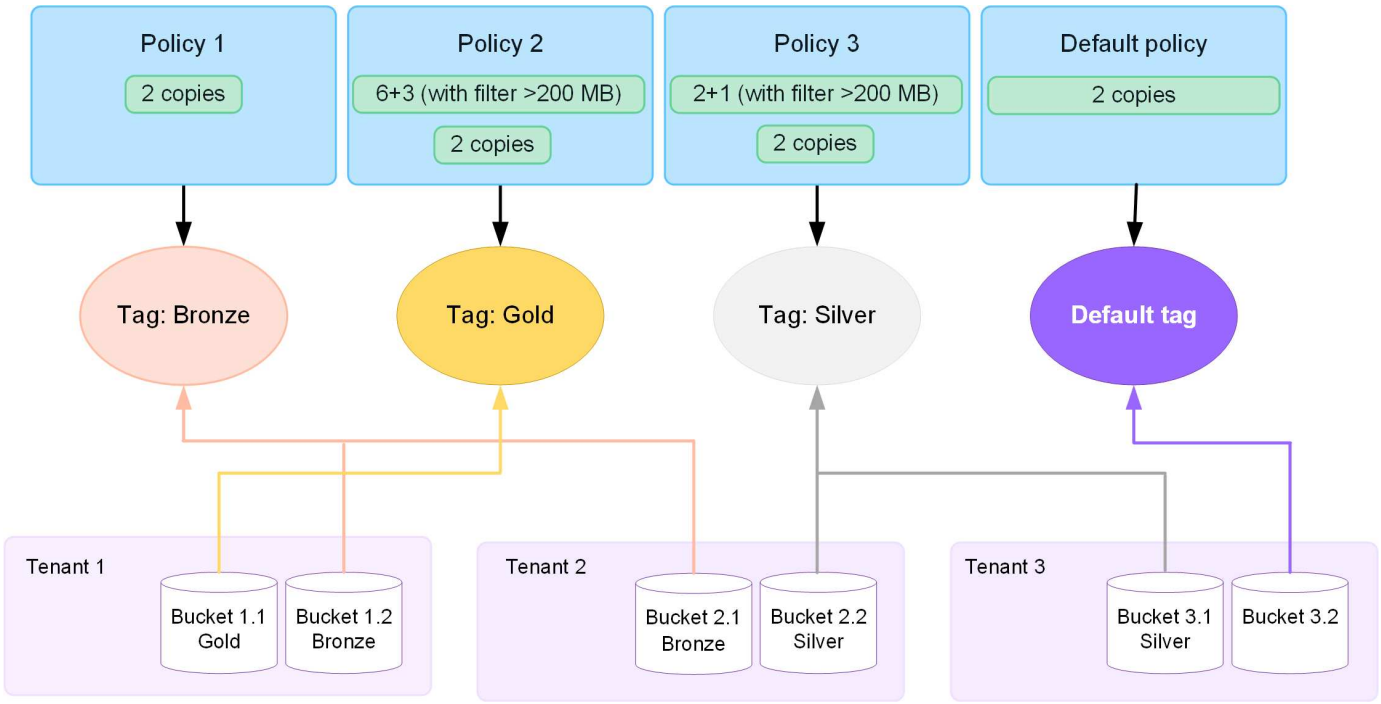
ILM-Richtlinien-Tags

Wenn Mandanten einfach pro Bucket zwischen mehreren Datensicherungsrichtlinien wechseln möchten, verwenden Sie mehrere ILM-Richtlinien mit *ILM-Richtlinien-Tags*. Sie weisen jede ILM-Richtlinie einem Tag zu und markieren dann Mandanten einen Bucket, um die Richtlinie auf diesen Bucket anzuwenden. Sie können ILM-Richtlinien-Tags nur für S3 Buckets festlegen.

Sie können beispielsweise drei Tags mit den Namen Gold, Silber und Bronze haben. Sie können jedem Tag eine ILM-Richtlinie zuweisen. Diese richtet sich nach der Dauer und dem Speicherort von Objekten, die in dieser Richtlinie gespeichert sind. Mandanten können durch Tagging ihrer Buckets die zu verwendende Richtlinie auswählen. Ein mit Gold gekennzeichneter Bucket wird durch die Gold-Richtlinie gemanagt und erhält das Gold-Level für Datensicherung und Performance.

Standard-ILM-Richtlinien-Tag

Bei der Installation von StorageGRID wird automatisch ein Standard-ILM-Richtlinien-Tag erstellt. Jedes Raster muss über eine aktive Richtlinie verfügen, die dem Standard-Tag zugewiesen ist. Die Standardrichtlinie gilt für alle S3-Buckets ohne Tag.



Wie evaluiert eine ILM-Richtlinie Objekte?

Eine aktive ILM-Richtlinie steuert die Platzierung, Dauer und Datensicherung von Objekten.

Wenn Clients Objekte auf StorageGRID speichern, werden die Objekte anhand der in der Richtlinie festgelegten ILM-Regeln bewertet:

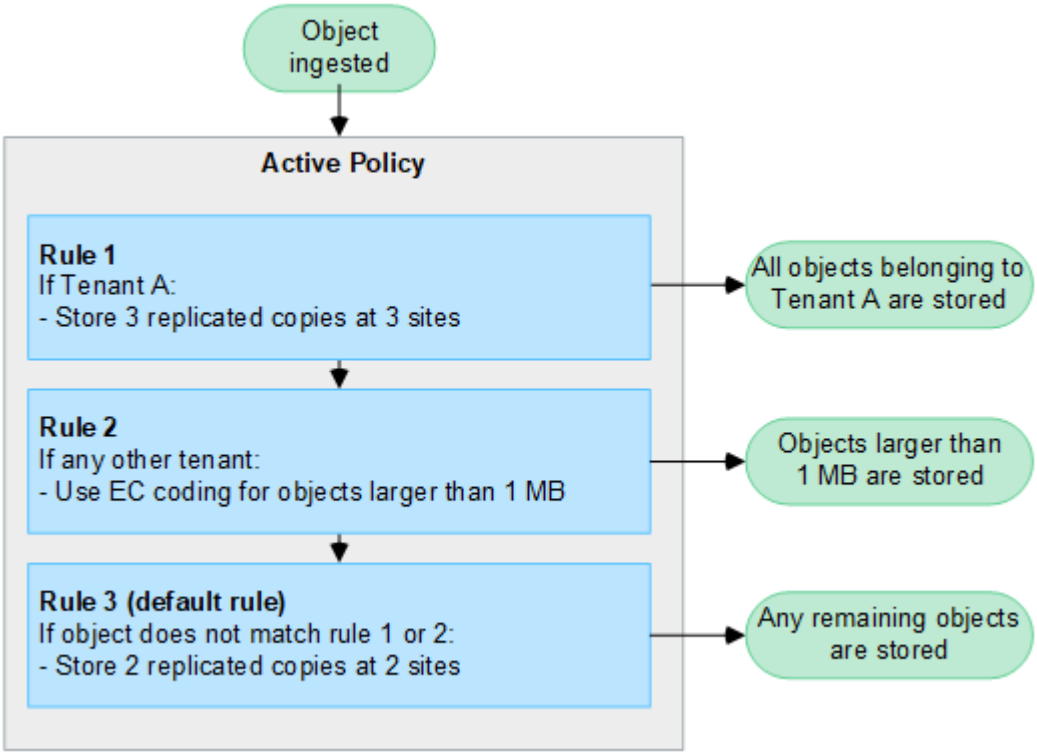
1. Wenn die Filter für die erste Regel in der Richtlinie mit einem Objekt übereinstimmen, wird das Objekt gemäß dem Aufnahmeverhalten der Regel aufgenommen und gemäß den Anweisungen zur Platzierung dieser Regel gespeichert.
2. Wenn die Filter für die erste Regel nicht mit dem Objekt übereinstimmen, wird das Objekt anhand jeder nachfolgenden Regel in der Richtlinie bewertet, bis eine Übereinstimmung vorgenommen wird.
3. Stimmen keine Regeln mit einem Objekt überein, werden das Aufnahmeverhalten und die Anweisungen zur Platzierung der Standardregel in der Richtlinie angewendet. Die Standardregel ist die letzte Regel in einer Richtlinie. Die Standardregel muss für alle Mandanten, alle S3-Buckets und alle Objektversionen gelten und kann keine erweiterten Filter verwenden.

Beispiel für eine ILM-Richtlinie

Eine ILM-Richtlinie könnte beispielsweise drei ILM-Regeln enthalten, die Folgendes angeben:

- **Regel 1: Replizierte Kopien für Mandant A**
  - Alle Objekte, die zu Mandant A gehören, abgleichen
  - Speichern Sie diese Objekte als drei replizierte Kopien an drei Standorten.
  - Objekte, die zu anderen Mandanten gehören, werden nicht mit Regel 1 abgeglichen, daher werden sie mit Regel 2 verglichen.
- **Regel 2: Erasure Coding für Objekte größer als 1 MB**
  - Alle Objekte von anderen Mandanten abgleichen, aber nur, wenn sie größer als 1 MB sind. Diese größeren Objekte werden mithilfe von 6+3 Erasure Coding an drei Standorten gespeichert.

    - Entspricht nicht Objekten mit einer Größe von 1 MB oder weniger, daher werden diese Objekte mit Regel 3 verglichen.
- **Regel 3: 2 Exemplare 2 Rechenzentren** (Standard)
    - Ist die letzte und Standardregel in der Richtlinie. Verwendet keine Filter.
    - Erstellen Sie zwei replizierte Kopien aller Objekte, die nicht mit Regel 1 oder Regel 2 übereinstimmen (Objekte, die nicht zu Mandant A gehören und mindestens 1 MB groß sind).



Was sind aktive und inaktive Richtlinien?

Jedes StorageGRID System muss über mindestens eine aktive ILM-Richtlinie verfügen. Wenn Sie mehr als eine aktive ILM-Richtlinie festlegen möchten, erstellen Sie ILM-Richtlinien-Tags und weisen jedem Tag eine Richtlinie zu. Mandanten wenden dann Tags auf S3-Buckets an. Die Standardrichtlinie wird auf alle Objekte in Buckets angewendet, denen kein Richtlinien-Tag zugewiesen ist.

Beim ersten Erstellen einer ILM-Richtlinie wählen Sie eine oder mehrere ILM-Regeln aus und ordnen sie in einer bestimmten Reihenfolge an. Nachdem Sie die Richtlinie simuliert haben, um ihr Verhalten zu bestätigen, aktivieren Sie sie.

Wenn Sie eine ILM-Richtlinie aktivieren, verwendet StorageGRID diese Richtlinie für das Management aller Objekte, einschließlich vorhandener Objekte und neu aufgenommenen Objekte. Vorhandene Objekte können an neue Standorte verschoben werden, wenn die ILM-Regeln der neuen Richtlinie implementiert werden.

Wenn Sie mehrere ILM-Richtlinien gleichzeitig aktivieren und Mandanten Richtlinien-Tags auf S3-Buckets anwenden, werden die Objekte in jedem Bucket gemäß der Richtlinie gemanagt, die dem Tag zugewiesen ist.

Ein StorageGRID-System verfolgt den Verlauf der aktivierten oder deaktivierten Richtlinien.

Überlegungen bei der Erstellung einer ILM-Richtlinie

- Verwenden Sie die vom System bereitgestellte Richtlinie, Richtlinie für Baseline 2 Kopien, nur in Testsystemen. Für StorageGRID 11.6 und frühere Versionen verwendet die Regel 2 Kopien erstellen in

dieser Richtlinie den Speicherpool Alle Speicherknoten, der alle Standorte enthält. Wenn Ihr StorageGRID System über mehrere Standorte verfügt, können zwei Kopien eines Objekts an demselben Standort platziert werden.

> Der Speicherpool Alle Speicherknoten wird automatisch während der Installation von StorageGRID 11.6 und früher erstellt. Wenn Sie ein Upgrade auf eine höhere Version von StorageGRID durchführen, ist der Pool Alle Storage-Nodes weiterhin vorhanden. Wenn Sie StorageGRID 11.7 oder höher als neue Installation installieren, wird der Pool Alle Speicherknoten nicht erstellt.

- Berücksichtigen Sie beim Entwurf einer neuen Richtlinie alle unterschiedlichen Objekttypen, die in das Grid aufgenommen werden können. Stellen Sie sicher, dass die Richtlinie Regeln enthält, die mit diesen Objekten übereinstimmen und sie nach Bedarf platziert werden können.
- Halten Sie die ILM-Richtlinie so einfach wie möglich. Dadurch werden potenziell gefährliche Situationen vermieden, in denen Objektdaten nicht wie vorgesehen geschützt werden, wenn im Laufe der Zeit Änderungen am StorageGRID System vorgenommen werden.
- Stellen Sie sicher, dass die Regeln in der Richtlinie in der richtigen Reihenfolge sind. Wenn die Richtlinie aktiviert ist, werden neue und vorhandene Objekte anhand der Regeln in der angegebenen Reihenfolge bewertet, die oben beginnen. Wenn z. B. die erste Regel in einer Richtlinie mit einem Objekt übereinstimmt, wird dieses Objekt nicht von einer anderen Regel bewertet.
- Die letzte Regel in jeder ILM-Richtlinie ist die standardmäßige ILM-Regel, die keine Filter verwenden kann. Wenn ein Objekt nicht mit einer anderen Regel übereinstimmt, steuert die Standardregel, wo das Objekt platziert wird und wie lange es aufbewahrt wird.
- Überprüfen Sie vor der Aktivierung einer neuen Richtlinie alle Änderungen, die die Richtlinie an der Platzierung vorhandener Objekte vornimmt. Das Ändern des Speicherorts eines vorhandenen Objekts kann zu vorübergehenden Ressourcenproblemen führen, wenn die neuen Platzierungen ausgewertet und implementiert werden.

Erstellen von ILM-Richtlinien

Erstellen Sie eine oder mehrere ILM-Richtlinien, um Ihre Quality-of-Service-Anforderungen zu erfüllen.

Dank einer aktiven ILM-Richtlinie können Sie dieselben ILM-Regeln auf alle Mandanten und Buckets anwenden.

Durch mehrere aktive ILM-Richtlinien können Sie die entsprechenden ILM-Regeln auf bestimmte Mandanten und Buckets anwenden, um mehrere Quality-of-Service-Anforderungen zu erfüllen.

ILM-Richtlinie erstellen

Über diese Aufgabe

Vergewissern Sie sich vor dem Erstellen Ihrer eigenen Richtlinie, dass der die "Standardmäßige ILM-Richtlinie"Storage-Anforderungen nicht erfüllt.

> Verwenden Sie in Testsystemen nur die vom System bereitgestellten Richtlinien, 2 Kopien Policy (für Raster mit einem Standort) oder 1 Kopie pro Standort (für Raster mit mehreren Standorten). Für StorageGRID 11.6 und früher verwendet die Standardregel in dieser Richtlinie den Speicherpool Alle Speicherknoten, der alle Standorte enthält. Wenn Ihr StorageGRID System über mehrere Standorte verfügt, können zwei Kopien eines Objekts an demselben Standort platziert werden.

Wenn der "Die Einstellung für die globale S3-Objektsperre wurde aktiviert", müssen Sie sicherstellen, dass die ILM-Richtlinie den Anforderungen von Buckets entspricht, für die S3 Object Lock aktiviert ist. Befolgen Sie in diesem Abschnitt die Anweisungen, die erwähnen, dass S3 Object Lock aktiviert ist.

Bevor Sie beginnen

- Sie sind im Grid Manager mit einem angemeldet"Unterstützter Webbrowser".
- Sie haben die "Erforderliche Zugriffsberechtigungen".
- Sie "ILM-Regeln wurden erstellt"basieren darauf, ob S3 Object Lock aktiviert ist.

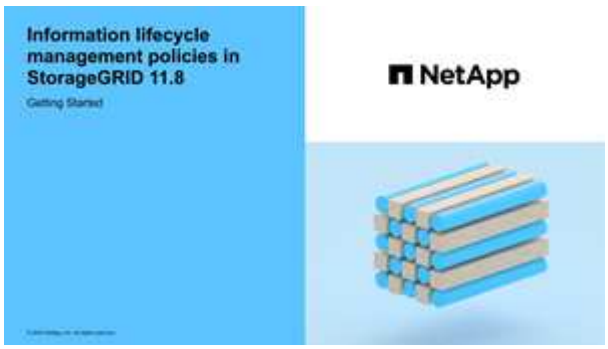
  S3 Objektsperre nicht aktiviert

  - Sie müssen "ILM-Regeln erstellt"der Richtlinie hinzufügen. Nach Bedarf können Sie eine Richtlinie speichern, zusätzliche Regeln erstellen und die Richtlinie dann bearbeiten, um die neuen Regeln hinzuzufügen.
  - Sie haben"Eine Standard-ILM-Regel wurde erstellt", dass keine Filter enthält.

  S3-Objektsperre aktiviert

  - Der "Die Einstellung für die globale S3-Objektsperre ist bereits aktiviert" für das StorageGRID-System.
  - Sie müssen "Erstellung der konformen und nicht konformen ILM-Regeln"der Richtlinie hinzufügen. Nach Bedarf können Sie eine Richtlinie speichern, zusätzliche Regeln erstellen und die Richtlinie dann bearbeiten, um die neuen Regeln hinzuzufügen.
  - Sie haben "Eine Standard-ILM-Regel wurde erstellt" für die Richtlinie, die konform ist.

- Optional haben Sie sich das Video angesehen: "Video: ILM-Richtlinien im Überblick"



Siehe auch "Verwenden Sie ILM-Richtlinien".

Schritte

1. Wählen Sie **ILM** > **Richtlinien**.

   Wenn die globale S3 Object Lock-Einstellung aktiviert ist, gibt die Seite ILM-Richtlinien an, welche ILM-Regeln konform sind.

2. Legen Sie fest, wie die ILM-Richtlinie erstellt werden soll.

Erstellen einer neuen Richtlinie

a. Wählen Sie **Richtlinie erstellen**.

Vorhandene Richtlinie klonen

a. Aktivieren Sie das Kontrollkästchen für die Richtlinie, mit der Sie beginnen möchten, und wählen Sie dann **Clone** aus.

Vorhandene Richtlinie bearbeiten

a. Wenn eine Richtlinie inaktiv ist, können Sie sie bearbeiten. Aktivieren Sie das Kontrollkästchen für die inaktive Richtlinie, mit der Sie beginnen möchten, und wählen Sie dann **Bearbeiten** aus.

3. Geben Sie im Feld **Richtlinienname** einen eindeutigen Namen für die Richtlinie ein.
4. Geben Sie optional im Feld **Änderungsgrund** den Grund ein, aus dem Sie eine neue Richtlinie erstellen.
5. Um der Richtlinie Regeln hinzuzufügen, wählen Sie **Regeln auswählen**. Wählen Sie einen Regelnamen aus, um die Einstellungen für diese Regel anzuzeigen.

   Beim Klonen einer Richtlinie:

   - Die von der Richtlinie, die Sie klonen, verwendeten Regeln sind ausgewählt.
   - Wenn die Richtlinie, die Sie klonen, Regeln ohne Filter verwendet hat, die nicht die Standardregel waren, werden Sie aufgefordert, alle Regeln außer einer dieser Regeln zu entfernen.
   - Wenn die Standardregel einen Filter verwendet hat, werden Sie aufgefordert, eine neue Standardregel auszuwählen.
   - Wenn die Standardregel nicht die letzte Regel war, können Sie die Regel an das Ende der neuen Richtlinie verschieben.

S3 Objektsperre nicht aktiviert

a. Wählen Sie eine Standardregel für die Richtlinie aus. Um eine neue Standardregel zu erstellen, wählen Sie **ILM-Regelseite** aus.

   Die Standardregel gilt für alle Objekte, die nicht mit einer anderen Regel in der Richtlinie übereinstimmen. Die Standardregel kann keine Filter verwenden und wird immer zuletzt ausgewertet.

   > Verwenden Sie nicht die Regel 2 Kopien erstellen als Standardregel für eine Richtlinie. Die Regel 2 Kopien erstellen verwendet einen einzelnen Speicherpool, alle Speicherknoten, der alle Standorte enthält. Wenn Ihr StorageGRID System über mehrere Standorte verfügt, können zwei Kopien eines Objekts an demselben Standort platziert werden.

S3-Objektsperre aktiviert

a. Wählen Sie eine Standardregel für die Richtlinie aus. Um eine neue Standardregel zu erstellen, wählen Sie **ILM-Regelseite** aus.

   Die Liste der Regeln enthält nur die Regeln, die konform sind und keine Filter verwenden.

   > Verwenden Sie nicht die Regel 2 Kopien erstellen als Standardregel für eine Richtlinie. Die Regel 2 Kopien erstellen verwendet einen einzelnen Speicherpool, alle Speicherknoten, der alle Standorte enthält. Wenn Sie diese Regel verwenden, können mehrere Kopien eines Objekts auf demselben Standort platziert werden.

b. Wenn Sie eine andere "Standard"-Regel für Objekte in nicht konformen S3-Buckets benötigen, wählen Sie **eine Regel ohne Filter für nicht konforme S3-Buckets** aus und wählen Sie eine nicht konforme Regel aus, die keinen Filter verwendet.

   Sie können beispielsweise einen Cloud-Storage-Pool verwenden, um Objekte in Buckets zu speichern, für die die S3-Objektsperre nicht aktiviert ist.

   > Sie können nur eine nicht kompatible Regel auswählen, die keinen Filter verwendet.

Siehe auch "Beispiel 7: Konforme ILM-Richtlinie für S3 Object Lock".

6. Wenn Sie mit der Auswahl der Standardregel fertig sind, wählen Sie **Weiter**.
7. Wählen Sie für den Schritt andere Regeln alle anderen Regeln aus, die Sie der Richtlinie hinzufügen möchten. Diese Regeln verwenden mindestens einen Filter (Mandantenkonto, Bucket-Name, erweiterter Filter oder nicht aktuelle Referenzzeit). Wählen Sie dann **Select**.

   Im Fenster Richtlinie erstellen werden nun die ausgewählten Regeln aufgelistet. Die Standardregel ist am Ende, mit den anderen Regeln darüber.

   Wenn S3 Object Lock aktiviert ist und Sie auch eine nicht konforme "Standard"-Regel ausgewählt haben, wird diese Regel als die vorletzte Regel in der Richtlinie hinzugefügt.

Eine Warnung wird angezeigt, wenn eine Regel Objekte nicht für immer behält. Wenn Sie diese Richtlinie aktivieren, müssen Sie bestätigen, dass StorageGRID Objekte löschen soll, wenn die Platzierungsanweisungen für die Standardregel abgelaufen sind (es sei denn, ein Bucket-Lebenszyklus hält die Objekte für einen längeren Zeitraum).

8. Ziehen Sie die Zeilen für die nicht standardmäßigen Regeln, um die Reihenfolge zu bestimmen, in der diese Regeln ausgewertet werden.

   Sie können die Standardregel nicht verschieben. Wenn S3 Object Lock aktiviert ist, können Sie die nicht konforme Standardregel auch nicht verschieben, wenn eine ausgewählt wurde.

   Sie müssen sich vergewissern, dass die ILM-Regeln in der richtigen Reihenfolge sind. Wenn die Richtlinie aktiviert ist, werden neue und vorhandene Objekte anhand der Regeln in der angegebenen Reihenfolge bewertet, die oben beginnen.

9. Wählen Sie bei Bedarf **Regeln auswählen**, um Regeln hinzuzufügen oder zu entfernen.
10. Wenn Sie fertig sind, wählen Sie **Speichern**.
11. Wiederholen Sie diese Schritte, um zusätzliche ILM-Richtlinien zu erstellen.
12. Simulation einer ILM-Richtlinie. Sie sollten eine Richtlinie immer simulieren, bevor Sie sie aktivieren, um sicherzustellen, dass sie wie erwartet funktioniert.

Simulieren Sie eine Richtlinie

Simulieren Sie eine Richtlinie für Testobjekte, bevor Sie die Richtlinie aktivieren und auf Ihre Produktionsdaten anwenden.

Bevor Sie beginnen

- Sie kennen den S3-Bucket/Objektschlüssel für jedes Objekt, das Sie testen möchten.

Schritte

1. Mit einem S3-Client oder dem "S3-Konsole", die Objekte aufnehmen, die zum Testen jeder Regel erforderlich sind.
2. Aktivieren Sie auf der Seite ILM Policies das Kontrollkästchen für die Policy, und wählen Sie dann **Simulate** aus.
3. Geben Sie im Feld **Objekt** den S3 für ein Testobjekt ein `bucket/object-key`. `bucket-01/filename.png`Beispiel: .
4. Wenn die S3-Versionierung aktiviert ist, geben Sie optional eine Versions-ID für das Objekt in das Feld **Versions-ID** ein.
5. Wählen Sie **Simulieren**.
6. Bestätigen Sie im Abschnitt Simulationsergebnisse, dass jedes Objekt mit der richtigen Regel abgeglichen wurde.
7. Um festzustellen, welches Profil für den Speicherpool oder die Erasure Coding-Funktion verwendet wird, wählen Sie den Namen der übereinstimmenden Regel aus, um zur Seite mit den Regeldetails zu gelangen.

Prüfen Sie alle Änderungen an der Platzierung vorhandener replizierter und Erasure Coded Objekte. Das Ändern des Speicherorts eines vorhandenen Objekts kann zu vorübergehenden Ressourcenproblemen führen, wenn die neuen Platzierungen ausgewertet und implementiert werden.

Ergebnisse

Alle Änderungen an den Regeln der Richtlinie werden in den Simulationsergebnissen angezeigt und zeigen den neuen Match und den vorherigen Match an. Das Fenster Richtlinie simulieren behält die getesteten Objekte bei, bis Sie entweder **Alle löschen** oder das Symbol Entfernen für jedes Objekt in der Liste Simulationsergebnisse auswählen.

Verwandte Informationen

"Beispiele für ILM-Richtliniensimulationen"

Aktivieren Sie eine Richtlinie

Wenn Sie eine einzelne neue ILM-Richtlinie aktivieren, werden vorhandene Objekte und neu aufgenommene Objekte von dieser Richtlinie gemanagt. Wenn Sie mehrere Richtlinien aktivieren, bestimmen die zu verwaltenden Objekte anhand von ILM-Richtlinien-Tags, die Buckets zugewiesen sind.

Bevor Sie eine neue Richtlinie aktivieren, gehen Sie wie folgt vor:

1. Simulieren Sie die Richtlinie, um zu bestätigen, dass sie sich wie erwartet verhält.
2. Prüfen Sie alle Änderungen an der Platzierung vorhandener replizierter und Erasure Coded Objekte. Das Ändern des Speicherorts eines vorhandenen Objekts kann zu vorübergehenden Ressourcenproblemen führen, wenn die neuen Platzierungen ausgewertet und implementiert werden.

Fehler in einer ILM-Richtlinie können zu nicht wiederherstellbaren Datenverlusten führen.

Über diese Aufgabe

Wenn Sie eine ILM-Richtlinie aktivieren, verteilt das System die neue Richtlinie auf alle Nodes. Die neue aktive Richtlinie tritt jedoch möglicherweise erst in Kraft, wenn alle Grid-Nodes zur Verfügung stehen, um die neue Richtlinie zu erhalten. In einigen Fällen wartet das System auf die Implementierung einer neuen aktiven Richtlinie, um sicherzustellen, dass Grid-Objekte nicht versehentlich entfernt werden. Im Detail:

- Wenn Sie Richtlinienänderungen vornehmen, die **Datenredundanz oder Datenaufbewahrungszeit erhöhen**, werden diese Änderungen sofort implementiert. Wenn Sie beispielsweise eine neue Richtlinie aktivieren, die eine Regel mit drei Kopien anstelle einer Regel mit zwei Kopien enthält, wird diese Richtlinie sofort implementiert, da sie die Datenredundanz erhöht.
- Wenn Sie Richtlinienänderungen vornehmen, die **Datenredundanz oder Datenaufbewahrungszeit verringern könnten**, werden diese Änderungen erst implementiert, wenn alle Grid-Knoten verfügbar sind. Wenn Sie beispielsweise eine neue Richtlinie aktivieren, die eine Regel mit zwei Kopien anstelle einer Regel mit drei Kopien verwendet, wird die neue Richtlinie auf der Registerkarte „Aktive Richtlinie“ angezeigt. Sie wird jedoch erst wirksam, wenn alle Nodes online und verfügbar sind.

Schritte

Führen Sie die Schritte zum Aktivieren einer oder mehrerer Richtlinien aus:

Aktivieren Sie eine Richtlinie

Führen Sie diese Schritte aus, wenn nur eine aktive Richtlinie vorhanden ist. Wenn Sie bereits über eine oder mehrere aktive Richtlinien verfügen und zusätzliche Richtlinien aktivieren, befolgen Sie die Schritte zum Aktivieren mehrerer Richtlinien.

1. Wenn Sie bereit sind, eine Richtlinie zu aktivieren, wählen Sie **ILM** > **Richtlinien** aus.

   Alternativ können Sie eine einzelne Richtlinie auf der Seite **ILM** > **Richtlinien-Tags** aktivieren.

2. Aktivieren Sie auf der Registerkarte Policies das Kontrollkästchen für die Richtlinie, die Sie aktivieren möchten, und wählen Sie dann **Activate** aus.
3. Befolgen Sie den entsprechenden Schritt:
   - Wenn Sie in einer Warnmeldung aufgefordert werden, zu bestätigen, dass Sie die Richtlinie aktivieren möchten, wählen Sie **OK**.
   - Wenn eine Warnmeldung mit Details zur Richtlinie angezeigt wird:
     i. Überprüfen Sie die Details, um sicherzustellen, dass die Richtlinie Daten wie erwartet managt.
     ii. Wenn die Standardregel Objekte für eine begrenzte Anzahl von Tagen speichert, überprüfen Sie das Aufbewahrungsdiagramm, und geben Sie diese Anzahl von Tagen in das Textfeld ein.
     iii. Wenn die Standardregel Objekte für immer speichert, aber eine oder mehrere andere Regeln eine eingeschränkte Aufbewahrung haben, geben Sie **yes** in das Textfeld ein.
     iv. Wählen Sie **Richtlinie aktivieren**.

Aktivieren Sie mehrere Richtlinien

Um mehrere Richtlinien zu aktivieren, müssen Sie Tags erstellen und jedem Tag eine Richtlinie zuweisen.

> Wenn mehrere Tags verwendet werden und Mandanten häufig Richtlinien-Tags Buckets zuweisen, kann die Grid-Performance beeinträchtigt werden. Wenn Sie nicht vertrauenswürdige Mandanten haben, sollten Sie nur das Standard-Tag verwenden.

1. Wählen Sie **ILM** > **Policy-Tags** aus.
2. Wählen Sie **Erstellen**.
3. Geben Sie im Dialogfeld Create Policy Tag einen Tag-Namen und optional eine Beschreibung für das Tag ein.

   > Tag-Namen und -Beschreibungen sind für Mandanten sichtbar. Wählen Sie Werte aus, die Mandanten bei der Auswahl von Richtlinien-Tags helfen, die ihren Buckets zugewiesen werden sollen, eine fundierte Entscheidung zu treffen. Wenn die zugewiesene Richtlinie beispielsweise Objekte nach einem bestimmten Zeitraum löscht, können Sie dies in der Beschreibung mitteilen. Nehmen Sie in diesen Feldern keine vertraulichen Informationen auf.

4. Wählen Sie **Tag erstellen**.
5. Wählen Sie in der Tabelle ILM-Richtlinien-Tags mit dem Pulldown-Menü eine Richtlinie aus, die dem Tag zugewiesen werden soll.
6. Wenn Warnungen in der Spalte Richtlinieneinschränkungen angezeigt werden, wählen Sie **Richtliniendetails anzeigen**, um die Richtlinie zu überprüfen.

7. Stellen Sie sicher, dass jede Richtlinie die Daten wie erwartet managt.
8. Wählen Sie **zugewiesene Richtlinien aktivieren**. Oder wählen Sie **Änderungen löschen**, um die Richtlinienzuweisung zu entfernen.
9. Überprüfen Sie im Dialogfeld „Richtlinien mit neuen Tags aktivieren“ die Beschreibungen, wie die einzelnen Tags, Richtlinien und Regeln Objekte verwalten. Nehmen Sie bei Bedarf Änderungen vor, um sicherzustellen, dass die Objekte in den Richtlinien wie erwartet gemanagt werden.
10. Wenn Sie sicher sind, dass Sie die Richtlinien aktivieren möchten, geben Sie **yes** in das Textfeld ein, und wählen Sie dann **Activate Policies** aus.

Verwandte Informationen

"Beispiel 6: Ändern einer ILM-Richtlinie"

Beispiele für ILM-Richtliniensimulationen

Die Beispiele für ILM-Richtliniensimulationen bieten Richtlinien zur Strukturierung und Änderung von Simulationen für Ihre Umgebung.

Beispiel 1: Überprüfung von Regeln bei der Simulation einer ILM-Richtlinie

In diesem Beispiel wird beschrieben, wie Regeln bei der Simulation einer Richtlinie überprüft werden.

In diesem Beispiel wird die **Beispiel ILM-Richtlinie** für die aufgenommene Objekte in zwei Buckets simuliert. Die Richtlinie umfasst drei Regeln:

- Die erste Regel, **zwei Kopien, zwei Jahre für Eimer-A**, gilt nur für Objekte in Eimer-a.
- Die zweite Regel, **EC-Objekte > 1 MB**, gilt für alle Buckets, aber für Filter auf Objekten größer als 1 MB.
- Die dritte Regel, **zwei Kopien, zwei Rechenzentren**, ist die Standardregel. Er enthält keine Filter und verwendet keine nicht aktuelle Referenzzeit.

Bestätigen Sie nach der Simulation der Richtlinie, dass jedes Objekt mit der richtigen Regel abgeglichen wurde.

In diesem Beispiel:

- `bucket-a/bucket-a object.pdf` Die erste Regel, die nach Objekten in gefiltert wird, wurde korrekt

zugeordnet `bucket-a`.

- `bucket-b/test object greater than 1 MB.pdf` Ist in `bucket-b`, also hat es nicht mit der ersten Regel übereinstimmen. Stattdessen wurde sie durch die zweite Regel korrekt abgeglichen, die nach Objekten mit einer Größe von mehr als 1 MB filtert.
- `bucket-b/test object less than 1 MB.pdf` Entspricht nicht den Filtern in den ersten beiden Regeln, daher wird sie von der Standardregel platziert, die keine Filter enthält.

Beispiel 2: Ordnen Sie Regeln bei der Simulation einer ILM-Richtlinie neu an

Dieses Beispiel zeigt, wie Sie Regeln neu anordnen können, um die Ergebnisse bei der Simulation einer Richtlinie zu ändern.

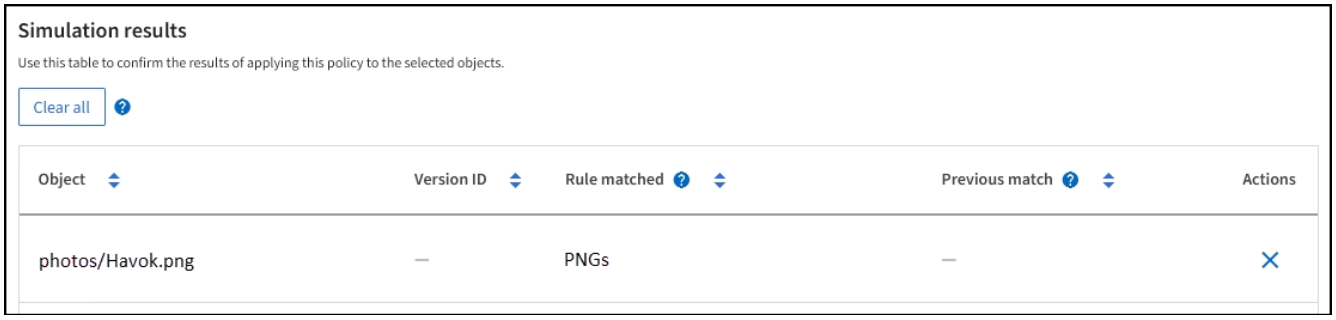
In diesem Beispiel wird die **Demo**-Richtlinie simuliert. Diese Richtlinie, die zum Auffinden von Objekten mit Metadaten für Benutzer der Serie=x-men bestimmt ist, enthält drei Regeln:

- Die erste Regel, **PNGs**, filtert nach Schlüsselnamen, die in enden `.png`.
- Die zweite Regel, **X-men**, gilt nur für Objekte für Mandant A und Filter für `series=x-men` Benutzermetadaten.
- Die letzte Regel, **two copies two Data Centers**, ist die Standardregel, die allen Objekten entspricht, die nicht den ersten beiden Regeln entsprechen.

Schritte

1. Nachdem Sie die Regeln hinzugefügt und die Richtlinie gespeichert haben, wählen Sie **Simulieren**.
2. Geben Sie im Feld **Object** den S3-Bucket/Object-Key für ein Testobjekt ein und wählen Sie **Simulate** aus.

   Die Simulationsergebnisse werden angezeigt und zeigen an, dass das `Havok.png` Objekt mit der Regel **PNGs** abgeglichen wurde.

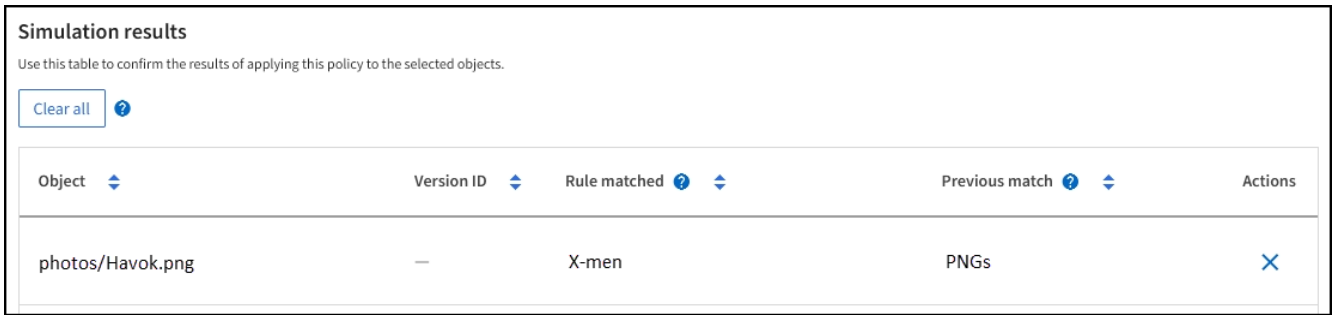


   Allerdings `Havok.png` sollte die **X-Men**-Regel getestet werden.

3. Um das Problem zu lösen, ordnen Sie die Regeln neu an.
   a. Wählen Sie **Finish**, um das Fenster ILM-Richtlinie simulieren zu schließen.
   b. Wählen Sie **Bearbeiten**, um die Richtlinie zu bearbeiten.
   c. Ziehen Sie die **X-Men**-Regel an den Anfang der Liste.
   d. Wählen Sie **Speichern**.
4. Wählen Sie **Simulieren**.

   Die zuvor getesteten Objekte werden anhand der aktualisierten Richtlinie neu bewertet und die neuen Simulationsergebnisse angezeigt. In dem Beispiel zeigt die Spalte Rule Matched, dass das `Havok.png`

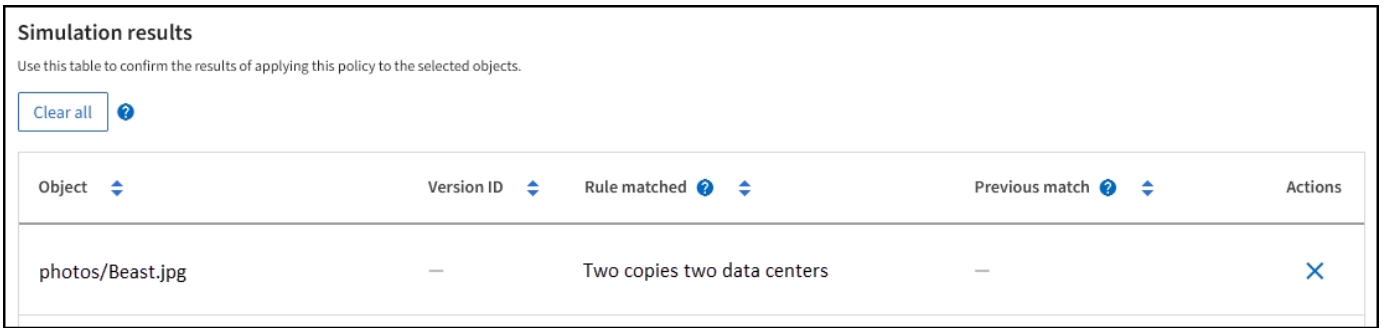
Objekt nun wie erwartet mit der X-men-Metadatenregel übereinstimmt. In der Spalte Vorheriger Abgleich wird angezeigt, dass die PNGs-Regel mit dem Objekt in der vorherigen Simulation übereinstimmt.



Beispiel 3: Korrigieren Sie eine Regel bei der Simulation einer ILM-Richtlinie

Dieses Beispiel zeigt, wie eine Richtlinie simuliert, eine Regel in der Richtlinie korrigiert und die Simulation fortgesetzt wird.

In diesem Beispiel wird die **Demo**-Richtlinie simuliert. Diese Richtlinie zielt darauf ab, Objekte zu finden, für die `series=x-men` Benutzermetadaten vorhanden sind. Bei der Simulation dieser Richtlinie gegen das Objekt traten jedoch unerwartete Ergebnisse auf `Beast.jpg`. Anstatt die X-Men-Metadatenregel zu entsprechen, kopiert das Objekt die Standardregel. Zwei Rechenzentren werden kopiert.



Wenn ein Testobjekt nicht mit der erwarteten Regel in der Richtlinie übereinstimmt, müssen Sie jede Regel in der Richtlinie überprüfen und eventuelle Fehler korrigieren.

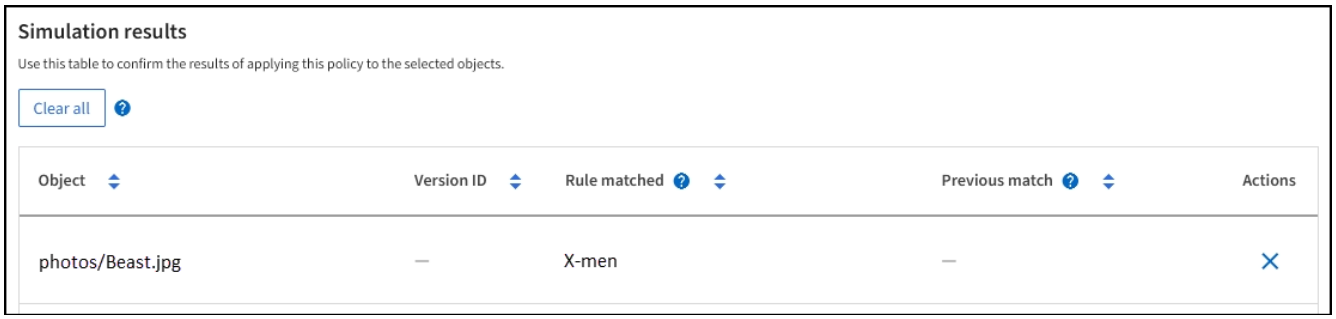
Schritte

1. Wählen Sie **Fertig**, um das Dialogfeld Richtlinie simulieren zu schließen. Wählen Sie auf der Detailseite für die Richtlinie **Aufbewahrungsdiagramm** aus. Wählen Sie dann **Alle erweitern** oder **Details anzeigen** für jede Regel nach Bedarf aus.
2. Prüfen Sie das Mandantenkonto der Regel, die Referenzzeit und die Filterkriterien.

   Angenommen, die Metadaten für die X-men-Regel wurden als „x-men01“ anstelle von „x-men“ eingegeben.

3. Um den Fehler zu beheben, korrigieren Sie die Regel wie folgt:
   - Wenn die Regel Teil der Richtlinie ist, können Sie entweder die Regel klonen oder die Regel aus der Richtlinie entfernen und sie dann bearbeiten.
   - Wenn die Regel Teil der aktiven Richtlinie ist, müssen Sie die Regel klonen. Sie können keine Regel aus der aktiven Richtlinie bearbeiten oder entfernen.
4. Führen Sie die Simulation erneut aus.

In diesem Beispiel entspricht die korrigierte X-Men-Regel nun wie erwartet dem `Beast.jpg` Objekt basierend auf den `series=x-men` Benutzermetadaten.



Managen von ILM-Richtlinien-Tags

Sie können die Details der ILM-Richtlinien-Tags anzeigen, ein Tag bearbeiten oder ein Tag entfernen.

Bevor Sie beginnen

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

Zeigen Sie die Details des ILM-Richtlinien-Tags an

So zeigen Sie die Details für ein Tag an:

1. Wählen Sie **ILM** > **Policy-Tags** aus.
2. Wählen Sie den Namen der Richtlinie aus der Tabelle aus. Die Detailseite für das Tag wird angezeigt.
3. Zeigen Sie auf der Detailseite den vorherigen Verlauf der zugewiesenen Richtlinien an.
4. Zeigen Sie eine Richtlinie an, indem Sie sie auswählen.

ILM-Richtlinien-Tag bearbeiten

> Tag-Namen und -Beschreibungen sind für Mandanten sichtbar. Wählen Sie Werte aus, die Mandanten bei der Auswahl von Richtlinien-Tags helfen, die ihren Buckets zugewiesen werden sollen, eine fundierte Entscheidung zu treffen. Wenn die zugewiesene Richtlinie beispielsweise Objekte nach einem bestimmten Zeitraum löscht, können Sie dies in der Beschreibung mitteilen. Nehmen Sie in diesen Feldern keine vertraulichen Informationen auf.

So bearbeiten Sie die Beschreibung eines vorhandenen Tags:

1. Wählen Sie **ILM** > **Policy-Tags** aus.
2. Aktivieren Sie das Kontrollkästchen für das Tag, und wählen Sie dann **Bearbeiten**.

   Alternativ können Sie den Namen des Tags auswählen. Die Detailseite für das Tag wird angezeigt, und Sie können auf dieser Seite **Bearbeiten** auswählen.

3. Ändern Sie die Tag-Beschreibung nach Bedarf
4. Wählen Sie **Speichern**.

Entfernen Sie das ILM-Richtlinien-Tag

Wenn Sie ein Policy-Tag entfernen, wird für alle Buckets, denen dieses Tag zugewiesen ist, die Standard-Richtlinie angewendet.

So entfernen Sie ein Tag:

1. Wählen Sie **ILM** > **Policy-Tags** aus.
2. Aktivieren Sie das Kontrollkästchen für das Tag, und wählen Sie dann **Entfernen**. Ein Bestätigungsdialogfeld wird angezeigt.

   Alternativ können Sie den Namen des Tags auswählen. Die Detailseite für das Tag wird angezeigt, und Sie können auf dieser Seite **Entfernen** auswählen.

3. Wählen Sie **Ja**, um das Tag zu löschen.

Überprüfen einer ILM-Richtlinie mit Objekt-Metadaten-Lookup

Nachdem Sie eine ILM-Richtlinie aktiviert haben, nehmen Sie repräsentative Testobjekte in das StorageGRID System auf und führen Sie dann eine Objekt-Metadaten-Suche durch, um zu bestätigen, dass Kopien wie vorgesehen erstellt und an den richtigen Stellen platziert werden.

Bevor Sie beginnen

Sie haben einen Objektbezeichner, der einer der folgenden sein kann: * **UUID**: Der universell eindeutige Bezeichner des Objekts. * **CBID**: Die eindeutige Kennung des Objekts in StorageGRID. Sie können die CBID eines Objekts aus dem Prüfprotokoll abrufen. Geben Sie die CBID in Großbuchstaben ein. * **S3-Bucket und Objektschlüssel**: Wenn ein Objekt über die S3-Schnittstelle aufgenommen wird, verwendet die Client-Applikation eine Bucket- und Objektschlüsselkombination, um das Objekt zu speichern und zu identifizieren. Wenn der S3-Bucket versioniert ist und Sie eine bestimmte Version eines S3-Objekts mithilfe des Bucket und Objektschlüssels nachsehen möchten, steht Ihnen die **Version-ID** zur Verfügung.

Schritte

1. Aufnahme des Objekts.
2. Wählen Sie **ILM** > **Object Metadata Lookup**.
3. Geben Sie die Kennung des Objekts in das Feld **Kennung** ein. Sie können eine UUID, eine CBID oder einen S3-Bucket/Objektschlüssel eingeben.
4. Optional können Sie eine Version-ID für das Objekt eingeben (nur S3).
5. Wählen Sie **Look Up**.

   Die Ergebnisse der Objektmetadaten werden angezeigt. Auf dieser Seite werden die folgenden Informationstypen aufgeführt:

   - Systemmetadaten, z. B. Objekt-ID (UUID), Ergebnistyp (Objekt, Löschmarkierung, S3 Bucket) und logische Größe des Objekts Weitere Informationen finden Sie im Beispiel-Screenshot unten.
   - Alle mit dem Objekt verknüpften Schlüssel-Wert-Paare für benutzerdefinierte Benutzer-Metadaten.
   - Bei S3-Objekten sind alle dem Objekt zugeordneten Objekt-Tag-Schlüsselwert-Paare enthalten.
   - Der aktuelle Storage-Standort jeder Kopie für replizierte Objektkopien
   - Für Objektkopien mit Erasure-Coding-Verfahren wird der aktuelle Speicherort der einzelnen Fragmente

gespeichert.

- Bei Objektkopien in einem Cloud Storage Pool befindet sich der Speicherort des Objekts, einschließlich des Namens des externen Buckets und der eindeutigen Kennung des Objekts.
- Für segmentierte Objekte und mehrteilige Objekte, eine Liste von Objektsegmenten einschließlich Segment-IDs und Datengrößen. Bei Objekten mit mehr als 100 Segmenten werden nur die ersten 100 Segmente angezeigt.
- Alle Objekt-Metadaten im nicht verarbeiteten internen Speicherformat. Diese RAW-Metadaten enthalten interne System-Metadaten, die nicht garantiert werden, dass sie über Release bis Release beibehalten werden.

6. Vergewissern Sie sich, dass das Objekt am richtigen Speicherort und an den richtigen Stellen gespeichert ist und dass es den richtigen Kopiertyp hat.

   Wenn die Option „Audit“ aktiviert ist, können Sie auch das Audit-Protokoll für die Meldung „ORLM-Objektregeln erfüllt“ überwachen. Die ORLM-Audit-Meldung kann Ihnen weitere Informationen über den Status des ILM-Evaluierungsprozesses liefern, kann Ihnen jedoch keine Informationen über die Richtigkeit der Platzierung der Objektdaten oder die Vollständigkeit der ILM-Richtlinie geben. Das müssen Sie selbst beurteilen. Weitere Informationen finden Sie unter "Prüfung von Audit-Protokollen".

Das folgende Beispiel zeigt die Ergebnisse für die Suche nach Objektmetadaten für ein S3-Testobjekt, das als zwei replizierte Kopien gespeichert ist.

Der folgende Screenshot ist ein Beispiel. Die Ergebnisse variieren je nach StorageGRID-Version.

System Metadata

Object ID	A12E96FF-B13F-4905-9E9E-45373F6E7DA8
Name	testobject
Container	source
Account	t-1582139188
Size	5.24 MB
Creation Time	2020-02-19 12:15:59 PST
Modified Time	2020-02-19 12:15:59 PST

Replicated Copies

Node	Disk Path
99-97	/var/local/rangedb/2/p/06/0B/00nM8H$|TFbnQQ}|CV2E
99-99	/var/local/rangedb/1/p/12/0A/00nM8H$|TFboW28|CXG%

Raw Metadata


```
{
    "TYPE": "CTNT",
    "CHND": "A12E96FF-B13F-4905-9E9E-45373F6E7DA8",
    "NAME": "testobject",
    "CBID": "0x8823DE7EC7C10416",
    "PHND": "FEA0AE51-534A-11EA-9FCD-31FF00C36D56",
    "PPTH": "source",
    "META": {
        "BASE": {
            "PAWS": "2",
```


Verwandte Informationen

"S3-REST-API VERWENDEN"

Arbeiten mit ILM-Richtlinien und ILM-Regeln

Wenn sich Ihre Speicheranforderungen ändern, müssen Sie möglicherweise zusätzliche Richtlinien einrichten oder die ILM-Regeln ändern, die einer Richtlinie zugeordnet sind. Sie können ILM-Metriken anzeigen, um die Systemperformance zu ermitteln.

Bevor Sie beginnen

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

ILM-Richtlinien anzeigen

So zeigen Sie aktive und inaktive ILM-Richtlinien und den Verlauf der Richtlinienaktivierung an:

1. Wählen Sie **ILM** > **Richtlinien**.
2. Wählen Sie **Policies**, um eine Liste der aktiven und inaktiven Policies anzuzeigen. In der Tabelle werden der Name der einzelnen Richtlinien, die Tags aufgeführt, denen die Richtlinie zugewiesen ist, und ob die Richtlinie aktiv oder inaktiv ist.
3. Wählen Sie **Aktivierungsverlauf** aus, um eine Liste der Start- und Enddaten für die Richtlinien anzuzeigen.
4. Wählen Sie einen Richtliniennamen aus, um die Details für die Richtlinie anzuzeigen.

> Wenn Sie die Details einer Richtlinie anzeigen, deren Status bearbeitet oder gelöscht ist, wird eine Meldung angezeigt, in der Sie die Version der Richtlinie anzeigen, die für den angegebenen Zeitraum aktiv war und seitdem bearbeitet oder gelöscht wurde.

Bearbeiten Sie eine ILM-Richtlinie

Sie können nur eine inaktive Richtlinie bearbeiten. Wenn Sie eine aktive Richtlinie bearbeiten möchten, deaktivieren Sie sie, oder erstellen Sie einen Klon, und bearbeiten Sie den Klon.

So bearbeiten Sie eine Richtlinie:

1. Wählen Sie **ILM** > **Richtlinien**.
2. Aktivieren Sie das Kontrollkästchen für die Richtlinie, die Sie bearbeiten möchten, und wählen Sie dann **Bearbeiten**.
3. Bearbeiten Sie die Richtlinie, indem Sie die Anweisungen in befolgen"Erstellen von ILM-Richtlinien".
4. Simulieren Sie die Richtlinie, bevor Sie sie erneut aktivieren.

> Eine falsch konfigurierte ILM-Richtlinie kann zu nicht wiederherstellbaren Datenverlusten führen. Prüfen Sie vor der Aktivierung einer ILM-Richtlinie die ILM-Richtlinie und ihre ILM-Regeln sorgfältig und simulieren Sie anschließend die ILM-Richtlinie. Vergewissern Sie sich immer, dass die ILM-Richtlinie wie vorgesehen funktioniert.

Klonen einer ILM-Richtlinie

So klonen Sie eine ILM-Richtlinie:

1. Wählen Sie **ILM** > **Richtlinien**.
2. Aktivieren Sie das Kontrollkästchen für die Richtlinie, die Sie klonen möchten, und wählen Sie dann **Clone** aus.
3. Erstellen Sie eine neue Richtlinie, beginnend mit der von Ihnen geklonten Richtlinie, indem Sie den Anweisungen in folgen"Erstellen von ILM-Richtlinien".

> Eine falsch konfigurierte ILM-Richtlinie kann zu nicht wiederherstellbaren Datenverlusten führen. Prüfen Sie vor der Aktivierung einer ILM-Richtlinie die ILM-Richtlinie und ihre ILM-Regeln sorgfältig und simulieren Sie anschließend die ILM-Richtlinie. Vergewissern Sie sich immer, dass die ILM-Richtlinie wie vorgesehen funktioniert.

Entfernen einer ILM-Richtlinie

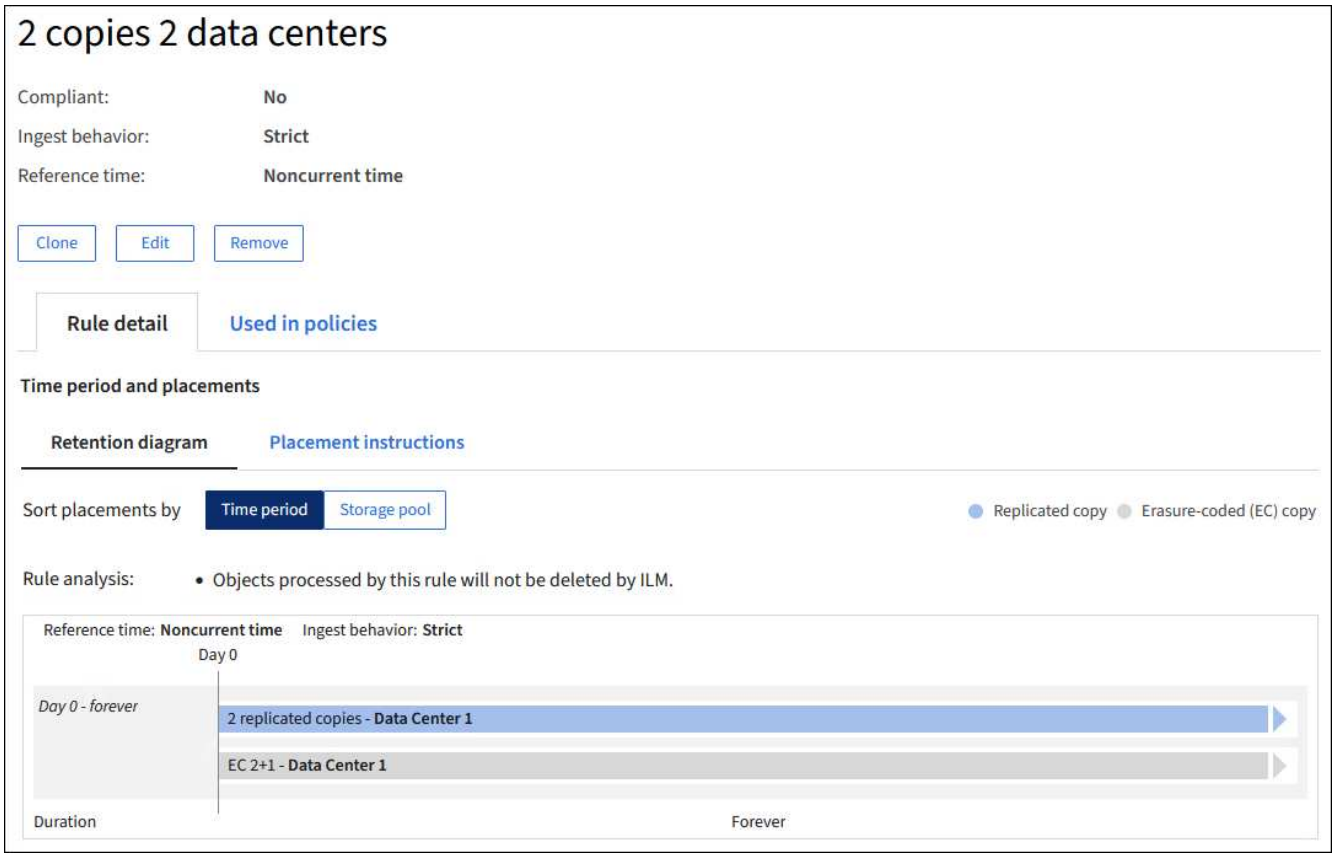
Sie können eine ILM-Richtlinie nur entfernen, wenn sie inaktiv ist. So entfernen Sie eine Richtlinie:

1. Wählen Sie **ILM** > **Richtlinien**.
2. Aktivieren Sie das Kontrollkästchen für die inaktive Richtlinie, die Sie entfernen möchten.
3. Wählen Sie **Entfernen**.

Zeigen Sie Einzelheiten zur ILM-Regel an

So zeigen Sie die Details für eine ILM-Regel an, einschließlich des Aufbewahrungsdiagramms und der Anweisungen zur Platzierung der Regel:

1. Wählen Sie **ILM** > **Regeln**.
2. Wählen Sie den Namen der Regel aus, deren Details Sie anzeigen möchten. Beispiel:



Darüber hinaus können Sie auf der Detailseite eine Regel klonen, bearbeiten oder entfernen. Sie können keine Regel bearbeiten oder entfernen, wenn sie in einer Richtlinie verwendet wird.

Klonen einer ILM-Regel

Sie können eine vorhandene Regel klonen, wenn Sie eine neue Regel erstellen möchten, die einige der Einstellungen der vorhandenen Regel verwendet. Wenn Sie eine Regel bearbeiten müssen, die in einer Richtlinie verwendet wird, klonen Sie stattdessen die Regel und nehmen Änderungen am Klon vor. Nachdem Sie Änderungen am Klon vorgenommen haben, können Sie die ursprüngliche Regel aus der Richtlinie entfernen und sie bei Bedarf durch die geänderte Version ersetzen.

Sie können eine ILM-Regel nicht klonen, wenn sie mit StorageGRID Version 10.2 oder früher erstellt wurde.

Schritte

1. Wählen Sie **ILM** > **Regeln**.
2. Aktivieren Sie das Kontrollkästchen für die Regel, die Sie klonen möchten, und wählen Sie dann **Clone** aus. Alternativ wählen Sie den Regelnamen aus, und wählen Sie dann auf der Seite mit den Regeldetails **Clone** aus.
3. Aktualisieren Sie die geklonte Regel, indem Sie die Schritte für und befolgenBearbeiten einer ILM-Regel"Verwenden erweiterter Filter in ILM-Regeln".

   Beim Klonen einer ILM-Regel müssen Sie einen neuen Namen eingeben.

Bearbeiten einer ILM-Regel

Möglicherweise müssen Sie eine ILM-Regel bearbeiten, um einen Filter oder eine Platzierungsanweisung zu ändern.

Sie können eine Regel nicht bearbeiten, wenn sie in einer ILM-Richtlinie verwendet wird. Stattdessen können Sie Regel klonendie geklonte Kopie beliebig ändern.

> Eine falsch konfigurierte ILM-Richtlinie kann zu nicht wiederherstellbaren Datenverlusten führen. Prüfen Sie vor der Aktivierung einer ILM-Richtlinie die ILM-Richtlinie und ihre ILM-Regeln sorgfältig und simulieren Sie anschließend die ILM-Richtlinie. Vergewissern Sie sich immer, dass die ILM-Richtlinie wie vorgesehen funktioniert.

Schritte

1. Wählen Sie **ILM** > **Regeln**.
2. Bestätigen Sie, dass die zu bearbeitende Regel in keiner ILM-Richtlinie verwendet wird.
3. Wenn die Regel, die Sie bearbeiten möchten, nicht verwendet wird, aktivieren Sie das Kontrollkästchen für die Regel und wählen Sie **Aktionen** > **Bearbeiten**. Alternativ wählen Sie den Namen der Regel aus, und wählen Sie dann auf der Seite mit den Regeldetails **Bearbeiten** aus.
4. Führen Sie die Schritte des Assistenten zum Bearbeiten von ILM-Regeln aus. Befolgen Sie bei Bedarf die Schritte für "Erstellen einer ILM-Regel" und "Verwenden erweiterter Filter in ILM-Regeln".

   Beim Bearbeiten einer ILM-Regel können Sie ihren Namen nicht ändern.

Entfernen einer ILM-Regel

Um die Liste der aktuellen ILM-Regeln kontrollierbar zu halten, entfernen Sie alle ILM-Regeln, die Sie wahrscheinlich nicht verwenden werden.

Schritte

So entfernen Sie eine ILM-Regel, die derzeit in einer aktiven Richtlinie verwendet wird:

1. Klonen Sie die Richtlinie.
2. Entfernen Sie die ILM-Regel aus dem Richtlinienklon.
3. Speichern, simulieren und aktivieren Sie die neue Richtlinie, um sicherzustellen, dass Objekte wie erwartet geschützt sind.
4. Gehen Sie zu den Schritten zum Entfernen einer ILM-Regel, die derzeit in einer inaktiven Richtlinie verwendet wird.

So entfernen Sie eine ILM-Regel, die derzeit in einer inaktiven Richtlinie verwendet wird:

1. Wählen Sie die inaktive Richtlinie aus.
2. Entfernen Sie die ILM-Regel aus der Richtlinie oder Entfernen Sie die Richtlinie.
3. Fahren Sie mit den Schritten zum Entfernen einer derzeit nicht verwendeten ILM-Regel fort.

So entfernen Sie eine derzeit nicht verwendete ILM-Regel:

1. Wählen Sie **ILM** > **Regeln**.
2. Bestätigen Sie, dass die Regel, die Sie entfernen möchten, in keiner Richtlinie verwendet wird.
3. Wenn die Regel, die Sie entfernen möchten, nicht verwendet wird, wählen Sie die Regel aus und wählen Sie **Aktionen** > **Entfernen** aus. Sie können mehrere Regeln auswählen und alle gleichzeitig entfernen.
4. Wählen Sie **Yes**, um zu bestätigen, dass Sie die ILM-Regel entfernen möchten.

Anzeigen von ILM-Metriken

Sie können Metriken für ILM anzeigen, z. B. die Anzahl der Objekte in der Warteschlange und die Evaluierungsrate. Sie können diese Kennzahlen überwachen, um die Systemperformance zu ermitteln. Eine große Warteschlange oder Evaluierungsrate zeigt möglicherweise an, dass das System nicht mit der Aufnahmerate Schritt halten kann, die Auslastung der Client-Applikationen zu hoch ist oder dass ein ungewöhnlicher Zustand vorliegt.

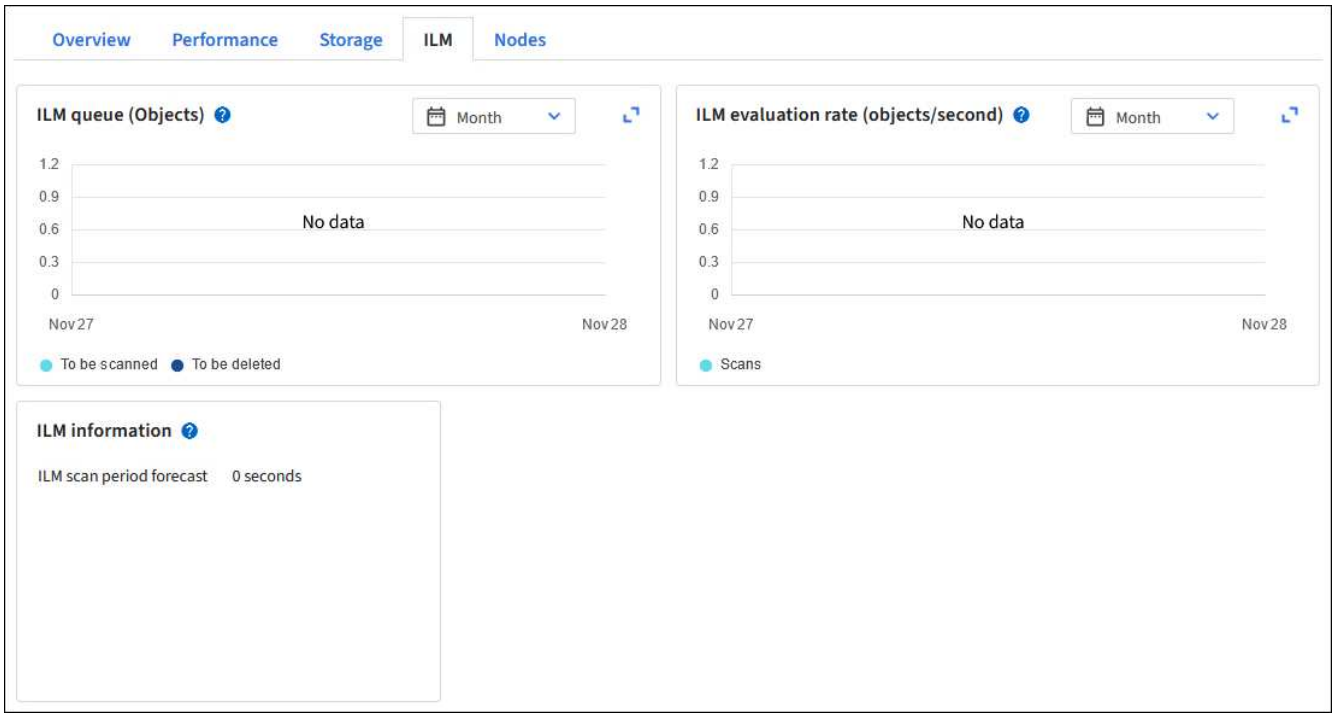
Schritte

1. Wählen Sie **Dashboard** > **ILM**.

   Da das Dashboard angepasst werden kann, ist die Registerkarte ILM möglicherweise nicht verfügbar.

2. Überwachen Sie die Kennzahlen auf der Registerkarte ILM.

   Sie können das Fragezeichen auswählen, um eine Beschreibung der Elemente auf der Registerkarte ILM anzuzeigen.



Verwenden Sie die S3-Objektsperre

Objekte managen mit S3 Object Lock

Als Grid-Administrator können Sie S3 Object Lock für Ihr StorageGRID System aktivieren und eine konforme ILM-Richtlinie implementieren. So können Sie sicherstellen, dass Objekte in bestimmten S3 Buckets nicht für einen bestimmten Zeitraum gelöscht oder überschrieben werden.

Was ist S3 Object Lock?

Die Funktion StorageGRID S3 Object Lock ist eine Objektschutzlösung, die der S3 Object Lock in Amazon Simple Storage Service (Amazon S3) entspricht.

Wenn die globale S3-Objektsperrung für ein StorageGRID-System aktiviert ist, kann ein S3-Mandantenkonto Buckets mit oder ohne S3-Objektsperrung erstellen. Wenn für einen Bucket die S3 Object Lock aktiviert ist, ist die Bucket-Versionierung erforderlich und wird automatisch aktiviert.

Ein Bucket ohne S3 Object Lock kann nur Objekte ohne Aufbewahrungseinstellungen haben. Keine aufgenommenen Objekte verfügen über Aufbewahrungseinstellungen.

Ein Bucket mit S3 Object Lock kann Objekte mit und ohne Aufbewahrungseinstellungen haben, die von S3-Client-Applikationen angegeben wurden. Einige aufgenommene Objekte haben Aufbewahrungseinstellungen.

Ein Bucket mit S3 Object Lock und konfigurierter Standardaufbewahrung kann Objekte mit angegebenen Aufbewahrungseinstellungen und neue Objekte ohne Aufbewahrungseinstellungen hochgeladen haben. Die neuen Objekte verwenden die Standardeinstellung, da die Aufbewahrungseinstellung nicht auf Objektebene konfiguriert wurde.

Tatsächlich verfügen alle neu aufgenommenen Objekte über Aufbewahrungseinstellungen, wenn die Standardaufbewahrung konfiguriert ist. Vorhandene Objekte ohne Objektaufbewahrungseinstellungen bleiben

hiervon unberührt.

Aufbewahrungsmodi

Die Objektsperrfunktion StorageGRID S3 unterstützt zwei Aufbewahrungsmodi, um verschiedene Schutzstufen auf Objekte anzuwenden. Diese Modi entsprechen den Amazon S3 Aufbewahrungsmodi.

- Im Compliance-Modus:
  - Das Objekt kann erst gelöscht werden, wenn das Aufbewahrungsdatum erreicht ist.
  - Das Aufbewahrungsdatum des Objekts kann erhöht, aber nicht verringert werden.
  - Das Aufbewahrungsdatum des Objekts kann erst entfernt werden, wenn dieses Datum erreicht ist.
- Im Governance-Modus:
  - Benutzer mit besonderer Berechtigung können in Anfragen einen Überbrückungskopf verwenden, um bestimmte Aufbewahrungseinstellungen zu ändern.
  - Diese Benutzer können eine Objektversion löschen, bevor das Aufbewahrungsdatum erreicht ist.
  - Diese Benutzer können das Aufbewahrungsdatum eines Objekts erhöhen, verringern oder entfernen.

Aufbewahrungseinstellungen für Objektversionen

Wenn ein Bucket mit aktivierter S3-Objektsperrung erstellt wird, können Benutzer mithilfe der S3-Client-Applikation optional die folgenden Aufbewahrungseinstellungen für jedes Objekt angeben, das dem Bucket hinzugefügt wird:

- **Retention Mode**: Entweder Compliance oder Governance.
- **Rebeat-until-date**: Wenn das Aufbewahrungsdatum einer Objektversion in der Zukunft liegt, kann das Objekt abgerufen, aber nicht gelöscht werden.
- **Legal Hold**: Die Anwendung eines gesetzlichen Hold auf eine Objektversion sperrt diesen Gegenstand sofort. Beispielsweise müssen Sie ein Objekt, das mit einer Untersuchung oder einem Rechtsstreit zusammenhängt, rechtlich festhalten. Eine gesetzliche Aufbewahrungspflichten haben kein Ablaufdatum, bleiben aber bis zur ausdrücklichen Entfernung erhalten. Die gesetzlichen Aufbewahrungspflichten sind unabhängig von der bisherigen Aufbewahrungsfrist.

  > Befindet sich ein Objekt unter einer Legal Hold-Funktion, kann das Objekt unabhängig vom Aufbewahrungsmodus nicht gelöscht werden.

  Details zu den Objekteinstellungen finden Sie unter "Konfigurieren Sie die S3-Objektsperre über die S3-REST-API".

Standardeinstellung für die Aufbewahrung von Buckets

Wenn ein Bucket mit aktivierter S3-Objektsperrung erstellt wurde, können Benutzer optional die folgenden Standardeinstellungen für den Bucket angeben:

- **Default Retention Mode**: Entweder Compliance oder Governance.
- **Default Retention Period**: Wie lange neue Objektversionen, die zu diesem Bucket hinzugefügt wurden, beibehalten werden sollen, beginnend mit dem Tag, an dem sie hinzugefügt werden.

Die Standard-Bucket-Einstellungen gelten nur für neue Objekte, die keine eigenen Aufbewahrungseinstellungen haben. Vorhandene Bucket-Objekte werden nicht beeinflusst, wenn Sie diese Standardeinstellungen hinzufügen oder ändern.

Siehe "Erstellen eines S3-Buckets" und "Aktualisieren Sie die S3 Object Lock-Standardaufbewahrung".

Vergleich der S3-Objektsperre mit älterer Compliance

Die S3-Objektsperre ersetzt die in früheren StorageGRID-Versionen verfügbare Compliance-Funktion. Da die S3-Objektsperrfunktion den Anforderungen von Amazon S3 entspricht, ist die proprietäre StorageGRID-Compliance-Funktion, die jetzt als „Legacy-Compliance“ bezeichnet wird, veraltet.

> ⓘ Die globale Compliance-Einstellung ist veraltet. Wenn Sie diese Einstellung mit einer früheren Version von StorageGRID aktiviert haben, wird die Einstellung S3 Objektsperre automatisch aktiviert. Sie können die Einstellungen vorhandener konformer Buckets weiterhin mit StorageGRID managen. Es ist jedoch nicht möglich, neue konforme Buckets zu erstellen. Weitere Informationen finden Sie unter "NetApp Knowledge Base: Management älterer, konformer Buckets für StorageGRID 11.5".

Wenn Sie die ältere Compliance-Funktion in einer früheren Version von StorageGRID verwendet haben, lesen Sie die folgende Tabelle, um zu erfahren, wie sie mit der S3-Objektsperrfunktion in StorageGRID verglichen wird.

	S3-Objektsperre	**Compliance (alt)**
Wie wird die Funktion global aktiviert?	Wählen Sie im Grid Manager die Option **KONFIGURATION** > **System** > **S3 Object Lock**.	Wird nicht mehr unterstützt.
Wie wird die Funktion für einen Bucket aktiviert?	Benutzer müssen die S3-Objektsperre aktivieren, wenn ein neuer Bucket mithilfe des Mandantenmanagers, der Mandantenmanagement-API oder der S3-REST-API erstellt wird.	Wird nicht mehr unterstützt.
Wird die Bucket-Versionierung unterstützt?	Ja. Die Bucket-Versionierung ist erforderlich und wird automatisch aktiviert, wenn S3 Object Lock für den Bucket aktiviert ist.	Nein
Wie wird die Objektaufbewahrung festgelegt?	Benutzer können für jede Objektversion ein bis-Datum für die Aufbewahrung festlegen oder für jeden Bucket einen Standardaufbewahrungszeitraum festlegen.	Benutzer müssen eine Aufbewahrungsfrist für den gesamten Bucket festlegen. Der Aufbewahrungszeitraum gilt für alle Objekte im Bucket.

	S3-Objektsperre	Compliance (alt)
Kann der Aufbewahrungszeitraum geändert werden?	• Im Compliance-Modus kann das Aufbewahrungsdatum für eine Objektversion erhöht, aber nicht verringert werden. • Im Governance-Modus können Benutzer mit speziellen Berechtigungen die Aufbewahrungseinstellungen eines Objekts verringern oder sogar entfernen.	Die Aufbewahrungsfrist eines Buckets kann erhöht, aber nie verringert werden.
Wo wird die gesetzliche Aufbewahrungspflichten kontrolliert?	Benutzer können für jede Objektversion im Bucket rechtliche Aufbewahrungspflichten platzieren oder eine gesetzliche Aufbewahrungspflichten aufheben.	Auf dem Bucket werden gesetzliche Aufbewahrungspflichten angebracht, die alle Objekte im Bucket betreffen.
Wann können Objekte gelöscht werden?	• Im Compliance-Modus kann eine Objektversion nach Erreichen des Aufbewahrungsdatums gelöscht werden, vorausgesetzt, das Objekt befindet sich nicht im Legal Hold. • Im Governance-Modus können Benutzer mit speziellen Berechtigungen ein Objekt löschen, bevor das Aufbewahrungsdatum erreicht wird, vorausgesetzt, das Objekt befindet sich nicht unter Legal Hold.	Ein Objekt kann nach Ablauf des Aufbewahrungszeitraums gelöscht werden, sofern der Bucket nicht unter der gesetzlichen Aufbewahrungspflichten liegt. Objekte können automatisch oder manuell gelöscht werden.
Wird die Bucket-Lifecycle-Konfiguration unterstützt?	Ja.	Nein

S3 Objektsperraufgaben

Als Grid-Administrator müssen Sie sich eng mit den Mandantenbenutzern abstimmen, um sicherzustellen, dass die Objekte so geschützt sind, dass sie ihren Aufbewahrungsanforderungen entsprechen.

Das Anwenden von Mandanteneinstellungen für das Grid kann je nach Netzwerkkonnektivität, Node-Status und Cassandra-Vorgängen 15 Minuten oder länger dauern.

Die folgenden Listen für Grid-Administratoren und Mandantenbenutzer enthalten die allgemeinen Aufgaben für die Verwendung der S3 Objektsperrfunktion.

Grid-Administrator

- Globale S3-Objektsperrung für das gesamte StorageGRID-System aktivieren.
- Stellen Sie sicher, dass die Richtlinien für Information Lifecycle Management (ILM) den *Compliance-Anforderungen entsprechen*, "Anforderungen für Buckets mit aktivierter S3-Objektsperrung"d. h. dass sie die erfüllen.
- Erlauben Sie einem Mandanten nach Bedarf, Compliance als Aufbewahrungsmodus zu verwenden. Andernfalls ist nur der Governance-Modus zulässig.
- Legen Sie bei Bedarf eine maximale Aufbewahrungsfrist für einen Mandanten fest.

Mandantenbenutzer

- Überlegungen für Buckets und Objekte mit S3 Object Lock prüfen.
- Wenden Sie sich bei Bedarf an den Grid-Administrator, um die globale S3 Object Lock-Einstellung zu aktivieren und Berechtigungen festzulegen.
- Erstellen von Buckets mit aktivierter S3-Objektsperre
- Optional können Sie Standardaufbewahrungseinstellungen für einen Bucket konfigurieren:
  - Standardaufbewahrungsmodus: Governance oder Compliance, falls vom Grid-Administrator zugelassen.
  - Standardaufbewahrungszeitraum: Muss kleiner oder gleich der maximalen Aufbewahrungsfrist sein, die vom Grid-Administrator festgelegt wurde.
- Fügen Sie mithilfe der S3-Client-Applikation Objekte hinzu und legen Sie optional die objektspezifische Aufbewahrung fest:
  - Aufbewahrungsmodus. Governance oder Compliance, falls vom Grid-Administrator zugelassen.
  - Bis-Datum beibehalten: Muss kleiner oder gleich dem sein, was durch die vom Grid-Administrator festgelegte maximale Aufbewahrungsfrist zulässig ist.

Anforderungen für die S3-Objektsperre

Sie müssen die Anforderungen für die Aktivierung der globalen S3-Objektsperre, die Anforderungen für die Erstellung konformer ILM-Regeln und ILM-Richtlinien sowie die Einschränkungen prüfen, die StorageGRID für Buckets und Objekte, die S3 Objektsperre verwenden, festlegen.

Anforderungen für die Verwendung der globalen S3-Objektsperre

- Sie müssen die globale S3-Objektsperreneinstellung mithilfe des Grid-Managers oder der Grid-Management-API aktivieren, bevor ein S3-Mandant einen Bucket erstellen kann, dessen S3-Objektsperre aktiviert ist.
- Wenn Sie die globale S3-Objektsperre aktivieren, können alle S3-Mandantenkonten Buckets erstellen, wobei S3-Objektsperre aktiviert ist.
- Nachdem Sie die globale S3-Objektsperrung aktiviert haben, können Sie die Einstellung nicht deaktivieren.
- Die globale S3 Object Lock kann nur aktiviert werden, wenn die Standardregel in allen aktiven ILM-Richtlinien „*compliant*“ lautet. (Das heißt, die Standardregel muss die Anforderungen von Buckets mit aktivierter S3 Object Lock erfüllen.)
- Wenn die globale S3-Objektsperrung aktiviert ist, können Sie keine neue ILM-Richtlinie erstellen oder eine vorhandene ILM-Richtlinie aktivieren, es sei denn, die Standardregel in der Richtlinie ist konform. Nach Aktivierung der globalen S3 Object Lock-Einstellung geben die ILM-Regeln und ILM-Richtlinien-Seiten an,

welche ILM-Regeln konform sind.

Anforderungen für konforme ILM-Regeln

Wenn Sie die globale S3-Objektsperrung aktivieren möchten, müssen Sie sicherstellen, dass die Standardregel in allen aktiven ILM-Richtlinien konform ist. Eine konforme Regel erfüllt die Anforderungen beider Buckets durch aktivierte S3-Objektsperre und alle vorhandenen Buckets, für die Compliance aktiviert ist:

- Die IT muss mindestens zwei replizierte Objektkopien oder eine Kopie mit Verfahren zur Fehlerkorrektur erstellen.
- Diese Kopien müssen auf Storage-Nodes während der gesamten Dauer jeder Zeile in der Plazierung vorhanden sein.
- Objektkopien können nicht in einem Cloud-Storage-Pool gespeichert werden.
- Mindestens eine Zeile der Platzierungsanweisungen muss am Tag 0 beginnen, wobei **Ingest time** als Referenzzeit verwendet wird.
- Mindestens eine Zeile der Platzierungsanweisungen muss „für immer“ lauten.

Anforderungen für ILM-Richtlinien

Wenn die globale S3 Object Lock-Einstellung aktiviert ist, können aktive und inaktive ILM-Richtlinien sowohl konforme als auch nicht konforme Regeln enthalten.

- Die Standardregel in einer aktiven oder inaktiven ILM-Richtlinie muss konform sein.
- Nicht konforme Regeln gelten nur für Objekte in Buckets, für die die S3-Objektsperre nicht aktiviert ist oder die die ältere Compliance-Funktion nicht aktiviert hat.
- Konforme Regeln können auf Objekte in jedem Bucket angewendet werden; S3-Objektsperre oder vorhandene Compliance muss für den Bucket nicht aktiviert werden.

"Beispiel einer konformen ILM-Richtlinie für S3 Object Lock"

Anforderungen für Buckets, bei denen die S3-Objektsperre aktiviert ist

- Wenn die globale S3-Objektsperre für das StorageGRID System aktiviert ist, können Sie die Buckets mit aktivierter S3-Objektsperre über den Mandantenmanager, die Mandantenmanagement-API oder die S3-REST-API erstellen.
- Wenn Sie die S3-Objektsperre verwenden möchten, müssen Sie beim Erstellen des Buckets die S3-Objektsperre aktivieren. Sie können die S3-Objektsperre für einen vorhandenen Bucket nicht aktivieren.
- Wenn die S3-Objektsperre für einen Bucket aktiviert ist, ermöglicht StorageGRID automatisch die Versionierung für diesen Bucket. Sie können S3 Object Lock nicht deaktivieren oder die Versionierung für den Bucket nicht unterbrechen.
- Optional können Sie mithilfe von Tenant Manager, der Mandanten-Management-API oder der S3-REST-API für jeden Bucket einen Standardaufbewahrungsmodus und einen Aufbewahrungszeitraum angeben. Die Standardaufbewahrungseinstellungen des Buckets gelten nur für neue Objekte, die dem Bucket hinzugefügt wurden und keine eigenen Aufbewahrungseinstellungen haben. Sie können diese Standardeinstellungen außer Kraft setzen, indem Sie einen Aufbewahrungsmodus und das Aufbewahrungsdatum für jede Objektversion festlegen, wenn sie hochgeladen wird.
- Die Konfiguration des Bucket-Lebenszyklus wird für Buckets unterstützt, für die S3 Object Lock aktiviert ist.
- Die CloudMirror-Replizierung wird für Buckets nicht unterstützt, wenn S3-Objektsperre aktiviert ist.

Anforderungen für Objekte in Buckets, bei denen die S3-Objektsperre aktiviert ist

- Zum Schutz einer Objektversion können Sie Standardaufbewahrungseinstellungen für den Bucket angeben oder Aufbewahrungseinstellungen für jede Objektversion angeben. Aufbewahrungseinstellungen auf Objektebene können mit der S3-Client-Applikation oder der S3-REST-API angegeben werden.
- Aufbewahrungseinstellungen gelten für einzelne Objektversionen. Eine Objektversion kann sowohl eine Aufbewahrungsfrist als auch eine gesetzliche Haltungseinstellung haben, eine jedoch nicht die andere oder keine. Wenn Sie eine Aufbewahrungsfrist oder eine gesetzliche Aufbewahrungseinstellung für ein Objekt angeben, wird nur die in der Anforderung angegebene Version geschützt. Sie können neue Versionen des Objekts erstellen, während die vorherige Version des Objekts gesperrt bleibt.

Lebenszyklus von Objekten in Buckets, wobei S3 Objektsperre aktiviert ist

Jedes in einem Bucket gespeicherte Objekt mit aktivierter S3 Object Lock durchlaufen die folgenden Phasen:

1. **Objektaufnahme**

   Wenn einem Bucket eine Objektversion hinzugefügt wird, für die S3 Object Lock aktiviert ist, werden die Aufbewahrungseinstellungen wie folgt angewendet:

   - Wenn für das Objekt Aufbewahrungseinstellungen angegeben werden, werden die Einstellungen auf Objektebene angewendet. Alle standardmäßigen Bucket-Einstellungen werden ignoriert.
   - Wenn für das Objekt keine Aufbewahrungseinstellungen angegeben sind, werden die Standard-Bucket-Einstellungen angewendet, sofern diese vorhanden sind.
   - Wenn für das Objekt oder den Bucket keine Aufbewahrungseinstellungen angegeben wurden, ist das Objekt nicht durch S3 Object Lock geschützt.

   Wenn Aufbewahrungseinstellungen angewendet werden, sind sowohl das Objekt als auch alle benutzerdefinierten S3-Metadaten geschützt.

2. **Objektaufbewahrung und -Löschung**

   Von jedem geschützten Objekt werden innerhalb StorageGRID des angegebenen Aufbewahrungszeitraums mehrere Kopien gespeichert. Die genaue Anzahl und Art der Objektkopien sowie der Speicherort werden durch konforme Regeln in den aktiven ILM-Richtlinien bestimmt. Ob ein geschütztes Objekt gelöscht werden kann, bevor das Aufbewahrungsdatum erreicht ist, hängt vom Aufbewahrungsmodus ab.

   - Befindet sich ein Objekt unter einer Legal Hold-Funktion, kann das Objekt unabhängig vom Aufbewahrungsmodus nicht gelöscht werden.

Verwandte Informationen

- "Erstellen eines S3-Buckets"
- "Aktualisieren Sie die S3 Object Lock-Standardaufbewahrung"
- "Konfigurieren Sie die S3-Objektsperre über die S3-REST-API"
- "Beispiel 7: Konforme ILM-Richtlinie für S3 Object Lock"

Aktivieren Sie die S3-Objektsperre global

Falls ein S3-Mandantenkonto Vorschriften beim Speichern von Objektdaten einhalten muss, muss die S3-Objektsperre für Ihr gesamtes StorageGRID System aktiviert werden. Wenn Sie die globale S3-Objektsperre aktivieren, können alle S3-Mandantenbenutzer

Buckets und Objekte mit S3 Object Lock erstellen und verwalten.

Bevor Sie beginnen

- Sie haben die "Root-Zugriffsberechtigung".
- Sie sind im Grid Manager mit einem angemeldet"Unterstützter Webbrowser".
- Sie haben den S3-Objektsperrworkflow überprüft und die Überlegungen verstanden.
- Sie haben bestätigt, dass die Standardregel in der aktiven ILM-Richtlinie konform ist. Weitere Informationen finden Sie unter "Erstellen einer Standard-ILM-Regel" .

Über diese Aufgabe

Ein Grid-Administrator muss die globale S3-Objektsperre aktivieren, damit Mandantenbenutzer neue Buckets erstellen können, für die S3-Objektsperre aktiviert ist. Nachdem diese Einstellung aktiviert ist, kann sie nicht deaktiviert werden.

Überprüfen Sie die Compliance-Einstellungen vorhandener Mandanten, nachdem Sie die globale S3 Object Lock-Einstellung aktiviert haben. Wenn Sie diese Einstellung aktivieren, hängen die Einstellungen für die S3-Objektsperrung pro Mandant vom StorageGRID-Release zum Zeitpunkt der Erstellung des Mandanten ab.

> Die globale Compliance-Einstellung ist veraltet. Wenn Sie diese Einstellung mit einer früheren Version von StorageGRID aktiviert haben, wird die Einstellung S3 Objektsperre automatisch aktiviert. Sie können die Einstellungen vorhandener konformer Buckets weiterhin mit StorageGRID managen. Es ist jedoch nicht möglich, neue konforme Buckets zu erstellen. Weitere Informationen finden Sie unter "NetApp Knowledge Base: Management älterer, konformer Buckets für StorageGRID 11.5".

Schritte

1. Wählen Sie **KONFIGURATION** > **System** > **S3 Objektsperre**.

   Die Seite Einstellungen für die S3-Objektsperre wird angezeigt.

2. Wählen Sie **S3-Objektsperre aktivieren**.
3. Wählen Sie **Anwenden**.

   Ein Bestätigungsdialogfeld wird angezeigt, in dem Sie daran erinnert werden, dass Sie die S3-Objektsperre nicht deaktivieren können, nachdem sie aktiviert wurde.

4. Wenn Sie sicher sind, dass Sie die S3-Objektsperre für Ihr gesamtes System dauerhaft aktivieren möchten, wählen Sie **OK**.

   Wenn Sie **OK** wählen:

   - Wenn die Standardregel in der aktiven ILM-Richtlinie konform ist, ist S3 Object Lock jetzt für das gesamte Grid aktiviert und kann nicht deaktiviert werden.
   - Wenn die Standardregel nicht kompatibel ist, wird ein Fehler angezeigt. Sie müssen eine neue ILM-Richtlinie erstellen und aktivieren, die eine konforme Regel als Standardregel enthält. Wählen Sie **OK**. Erstellen Sie anschließend eine neue Richtlinie, simulieren Sie sie und aktivieren Sie sie. Anweisungen finden Sie unter "ILM-Richtlinie erstellen" .

Beheben Sie die Konsistenzfehler beim Aktualisieren der S3-Objektsperre oder der alten Compliance-Konfiguration

Wenn ein Datacenter-Standort oder mehrere Storage-Nodes an einem Standort nicht mehr verfügbar sind, müssen Benutzer von S3-Mandanten unter Umständen Änderungen an der S3-Objektsperre oder älterer Compliance-Konfiguration vornehmen.

Mandantenbenutzer, deren Buckets mit aktivierter S3 Object Lock (oder älterer Compliance) vorhanden sind, können bestimmte Einstellungen ändern. Beispielsweise muss ein Mandantenbenutzer, der S3 Object Lock verwendet, eine Objektversion unter die gesetzliche Aufbewahrungspflichten legen.

Wenn ein Mandantenbenutzer die Einstellungen für einen S3-Bucket oder eine Objektversion aktualisiert, versucht StorageGRID, die Bucket- oder Objektmetadaten sofort im Grid zu aktualisieren. Wenn das System die Metadaten nicht aktualisieren kann, weil ein Datacenter-Standort oder mehrere Storage-Nodes nicht verfügbar sind, wird ein Fehler zurückgegeben:

```
503: Service Unavailable
Unable to update compliance settings because the settings can't be
consistently applied on enough storage services. Contact your grid
administrator for assistance.
```

Gehen Sie wie folgt vor, um diesen Fehler zu beheben:

1. Versuchen Sie, alle Storage-Nodes oder -Sites so schnell wie möglich wieder verfügbar zu machen.
2. Wenn Sie nicht in der Lage sind, an jedem Standort ausreichend Storage-Nodes zur Verfügung zu stellen, wenden Sie sich an den technischen Support, der Sie beim Wiederherstellen von Nodes unterstützt und sicherstellt, dass Änderungen konsistent im gesamten Grid angewendet werden.
3. Sobald das zugrunde liegende Problem behoben ist, erinnern Sie den Mandantenbenutzer daran, ihre Konfigurationsänderungen erneut zu versuchen.

Verwandte Informationen

- "Verwenden Sie ein Mandantenkonto"
- "S3-REST-API VERWENDEN"
- "Recovery und Wartung"

Beispiele für ILM-Regeln und -Richtlinien

Beispiel 1: ILM-Regeln und -Richtlinie für Objekt-Storage

Die folgenden Beispielregeln und -Richtlinien dienen als Ausgangspunkt bei der Definition einer ILM-Richtlinie zur Erfüllung der Anforderungen an Objektschutz und -Aufbewahrung.

Die folgenden ILM-Regeln und -Richtlinien sind nur Beispiele. Es gibt viele Möglichkeiten zur Konfiguration von ILM-Regeln. Simulieren Sie vor der Aktivierung einer neuen Richtlinie, um zu bestätigen, dass sie so funktioniert, wie sie zum Schutz von Inhalten vor Verlust vorgesehen ist.

ILM-Regel 1, z. B. 1: Objektdaten an zwei Standorte kopieren

Dieses Beispiel einer ILM-Regel kopiert Objektdaten in Storage-Pools an zwei Standorten.

Regeldefinition	Beispielwert
Speicherpools an einem Standort	Zwei Speicherpools, die jeweils unterschiedliche Standorte mit den Namen Standort 1 und Standort 2 enthalten.
Regelname	Zwei Kopien Zwei Standorte
Referenzzeit	Aufnahmezeit
Platzierungen	Bewahren Sie an Tag 0 bis für immer eine replizierte Kopie an Standort 1 und eine replizierte Kopie an Standort 2 auf.

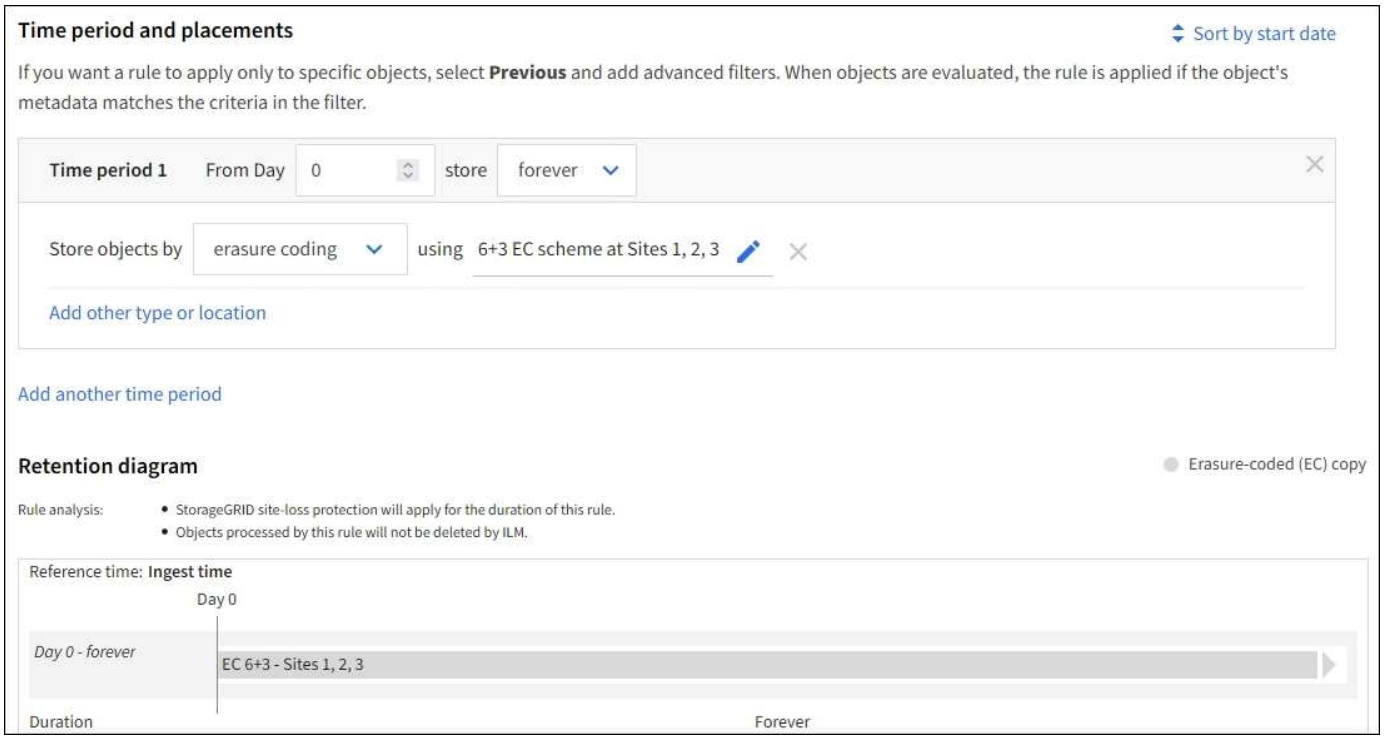
Im Abschnitt Regelanalyse des Aufbewahrungsdiagramms steht Folgendes:

- Für die Dauer dieser Regel gilt eine StorageGRID-Sicherung gegen vor-Ort-Verlust.
- Von dieser Regel verarbeitete Objekte werden nicht durch ILM gelöscht.

ILM-Regel 2 beispielsweise 1: Profil für Erasure Coding mit Bucket-Matching

Diese ILM-Regel verwendet ein Profil zur Fehlerkorrektur und einen S3-Bucket, um zu bestimmen, wo und wie lange das Objekt gespeichert ist.

Regeldefinition	Beispielwert
Speicherpool mit mehreren Standorten	• Ein Speicherpool an drei Standorten (Standorte 1, 2, 3) • Verwenden Sie das Erasure Coding-Schema für 6+3
Regelname	S3 Bucket-Finanzdaten
Referenzzeit	Aufnahmezeit
Platzierungen	Erstellen Sie für Objekte in dem S3-Bucket mit dem Namen „Finance-Records“ eine Kopie, die nach Erasure-Coding-Profil angegeben ist und nach der Erasure-Coding-Code codiert wurde. Bewahren Sie diese Kopie für immer auf.

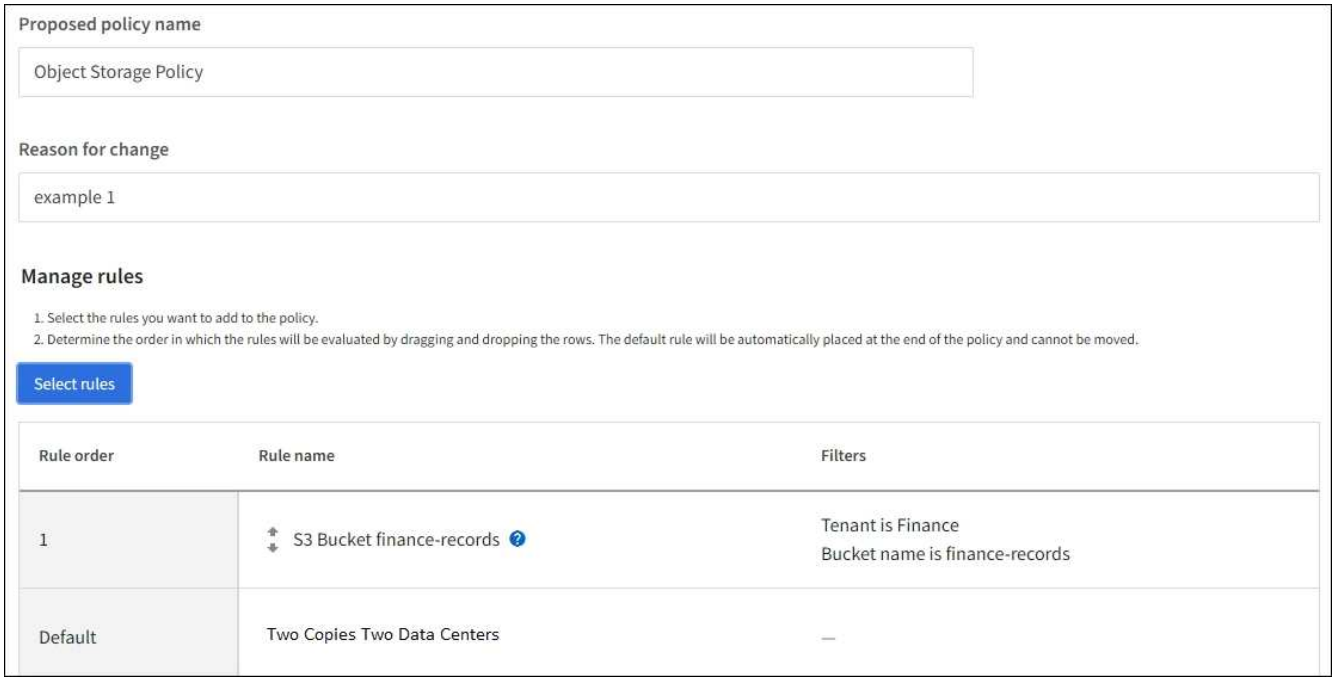


ILM-Richtlinie für Beispiel 1

In der Praxis sind die meisten ILM-Richtlinien einfach, obwohl das StorageGRID System Ihnen die Entwicklung ausgefeilter und komplexer ILM-Richtlinien ermöglicht.

Eine typische ILM-Richtlinie für ein Grid mit mehreren Standorten kann beispielsweise folgende ILM-Regeln umfassen:

- Speichern Sie bei der Aufnahme alle Objekte, die zum S3-Bucket gehören und in einem Storage-Pool mit drei Standorten benannt `finance-records` sind. Verwenden Sie 6+3 Erasure Coding.
- Wenn ein Objekt nicht mit der ersten ILM-Regel übereinstimmt, verwenden Sie die standardmäßige ILM-Regel der Richtlinie, zwei Kopien von zwei Rechenzentren, um eine Kopie dieses Objekts an Standort 1 und eine Kopie an Standort 2 zu speichern.



Verwandte Informationen

- "Verwenden Sie ILM-Richtlinien"
- "Erstellen von ILM-Richtlinien"

Beispiel 2: ILM-Regeln und Richtlinie für EC-Objektgrößen-Filterung

Die folgenden Beispielregeln und -Richtlinien dienen als Ausgangspunkt für die Definition einer ILM-Richtlinie, die nach Objektgröße gefiltert wird, um empfohlene EC-Anforderungen zu erfüllen.

Die folgenden ILM-Regeln und -Richtlinien sind nur Beispiele. Es gibt viele Möglichkeiten zur Konfiguration von ILM-Regeln. Simulieren Sie vor der Aktivierung einer neuen Richtlinie, um zu bestätigen, dass sie so funktioniert, wie sie zum Schutz von Inhalten vor Verlust vorgesehen ist.

ILM-Regel 1 beispielsweise 2: Verwenden Sie EC für Objekte über 1 MB

In diesem Beispiel werden Objekte mit einer ILM-Regel gelöscht, die größer als 1 MB sind.

Das Verfahren zur Einhaltung von Datenkonsistenz eignet sich am besten für Objekte mit einer Größe von mehr als 1 MB. Verwenden Sie kein Erasure Coding für Objekte, die kleiner als 200 KB sind, um zu vermeiden, dass man sehr kleine Fragmente, die zur Fehlerkorrektur codiert wurden, managen muss.

Regeldefinition	Beispielwert
Regelname	Nur EC-Objekte > 1 MB
Referenzzeit	Aufnahmezeit

Regeldefinition	Beispielwert
Erweiterter Filter für Objektgröße	Objektgröße größer als 1 MB
Platzierungen	Erstellen Sie eine Kopie mit 2+1-Verfahren zur Fehlerkorrektur mit drei Standorten

ILM-Regel 2 beispielsweise 2: Zwei replizierte Kopien

Diese Beispiel-ILM-Regel erstellt zwei replizierte Kopien und filtert nicht nach Objektgröße. Diese Regel ist die Standardregel für die Richtlinie. Da die erste Regel alle Objekte mit einer Größe von mehr als 1 MB filtert, gilt diese Regel nur für Objekte, die 1 MB oder kleiner sind.

Regeldefinition	Beispielwert
Regelname	Zwei Replizierte Kopien
Referenzzeit	Aufnahmezeit
Erweiterter Filter für Objektgröße	Keine
Platzierungen	Bewahren Sie an Tag 0 bis für immer eine replizierte Kopie an Standort 1 und eine replizierte Kopie an Standort 2 auf.

ILM-Richtlinie beispielsweise 2: Verwenden Sie EC für Objekte über 1 MB

Dieses Beispiel für die ILM-Richtlinie umfasst zwei ILM-Regeln:

- Die erste Löschregel kodiert alle Objekte, die größer als 1 MB sind.
- Die zweite (Standard-) ILM-Regel erstellt zwei replizierte Kopien. Da Objekte größer als 1 MB nach Regel 1 herausgefiltert wurden, gilt Regel 2 nur für Objekte, die 1 MB oder kleiner sind.

Beispiel 3: ILM-Regeln und -Richtlinie für besseren Schutz von Image-Dateien

Anhand der folgenden Beispielregeln und -Richtlinien können Sie sicherstellen, dass Bilder mit mehr als 1 MB Löschcode erhalten und dass zwei Kopien aus kleineren Bildern erstellt werden.

Die folgenden ILM-Regeln und -Richtlinien sind nur Beispiele. Es gibt viele Möglichkeiten zur Konfiguration von ILM-Regeln. Simulieren Sie vor der Aktivierung einer neuen Richtlinie, um zu bestätigen, dass sie so funktioniert, wie sie zum Schutz von Inhalten vor Verlust vorgesehen ist.

ILM-Regel 1 beispielsweise 3: Verwenden Sie EC für Bilddateien über 1 MB

Diese Beispiel ILM-Regel verwendet erweiterte Filterung zur Löschung von Code aller Bilddateien größer als 1 MB.

> Das Verfahren zur Einhaltung von Datenkonsistenz eignet sich am besten für Objekte mit einer Größe von mehr als 1 MB. Verwenden Sie kein Erasure Coding für Objekte, die kleiner als 200 KB sind, um zu vermeiden, dass man sehr kleine Fragmente, die zur Fehlerkorrektur codiert wurden, managen muss.

Regeldefinition	Beispielwert
Regelname	EC-Bilddateien > 1 MB
Referenzzeit	Aufnahmezeit
Erweiterter Filter für Objektgröße	Objektgröße größer als 1 MB
Erweiterte Filter für Schlüssel	• Endet mit .jpg • Endet mit .png
Platzierungen	Erstellen Sie eine Kopie mit 2+1-Verfahren zur Fehlerkorrektur mit drei Standorten

Da diese Regel als erste Regel in der Richtlinie konfiguriert ist, gilt die Anweisung für die Platzierung von Löschcodes nur für Dateien mit einer Größe von mehr als 1 MB.

ILM-Regel 2 beispielsweise 3: Erstellen Sie 2 replizierte Kopien für alle verbleibenden Image-Dateien

Diese Beispiel-ILM-Regel verwendet erweiterte Filterung, um anzugeben, dass kleinere Bilddateien repliziert werden. Da die erste Regel in der Richtlinie bereits Bilddateien mit einer Größe von mehr als 1 MB übereinstimmt, gilt diese Regel für Bilddateien mit einer Größe von 1 MB.

Regeldefinition	Beispielwert
Regelname	2 Kopien für Bilddateien
Referenzzeit	Aufnahmezeit
Erweiterte Filter für Schlüssel	• Endet mit .jpg • Endet mit .png
Platzierungen	Erstellung von 2 replizierten Kopien in zwei Storage Pools

ILM-Richtlinie beispielsweise 3: Besserer Schutz für Image-Dateien

Dieses Beispiel enthält drei Regeln für die ILM-Richtlinie:

- Die erste Löschregel kodiert alle Bilddateien größer als 1 MB.
- Die zweite Regel erstellt zwei Kopien aller verbleibenden Bilddateien (d. h. Bilder, die 1 MB oder kleiner sind).
- Die Standardregel gilt für alle übrigen Objekte (d. h. alle nicht-Image-Dateien).

Rule order	Rule name	Filters
1	EC image files > 1 MB	Object size is greater than 1 MB
2	2 copies for small images	Object size is less than or equal to 200 KB
Default	Default rule	—

Beispiel 4: ILM-Regeln und -Richtlinie für versionierte Objekte mit S3

Wenn Sie einen S3-Bucket mit aktivierter Versionierung haben, können Sie die nicht aktuellen Objektversionen verwalten, indem Sie Regeln in Ihre ILM-Richtlinie einarbeiten, die die „nicht aktuelle Zeit“ als Referenzzeit verwenden.

> Wenn Sie eine begrenzte Aufbewahrungszeit für Objekte angeben, werden diese Objekte nach Erreichen des Zeitraums dauerhaft gelöscht. Stellen Sie sicher, dass Sie verstehen, wie lange die Objekte beibehalten werden.

Wie in diesem Beispiel dargestellt, können Sie den von versionierten Objekten verwendeten Storage mithilfe unterschiedlicher Anweisungen zur Platzierung von nicht aktuellen Objektversionen steuern.

Die folgenden ILM-Regeln und -Richtlinien sind nur Beispiele. Es gibt viele Möglichkeiten zur Konfiguration von ILM-Regeln. Simulieren Sie vor der Aktivierung einer neuen Richtlinie, um zu bestätigen, dass sie so funktioniert, wie sie zum Schutz von Inhalten vor Verlust vorgesehen ist.

Um eine ILM-Richtliniensimulation für eine nicht aktuelle Version eines Objekts durchzuführen, müssen Sie die UUID oder CBID der Objektversion kennen. Um die UUID und die CBID zu finden, verwenden Sie"Objekt-Metadaten-Suche", solange das Objekt noch aktuell ist.

Verwandte Informationen

"So werden Objekte gelöscht"

ILM-Regel 1 beispielsweise 4: Speichern Sie drei Kopien für 10 Jahre

Diese ILM-Regel speichert eine Kopie jedes Objekts über einen Zeitraum von 10 Jahren an drei Standorten.

Diese Regel gilt für alle Objekte, unabhängig davon, ob sie versioniert sind.

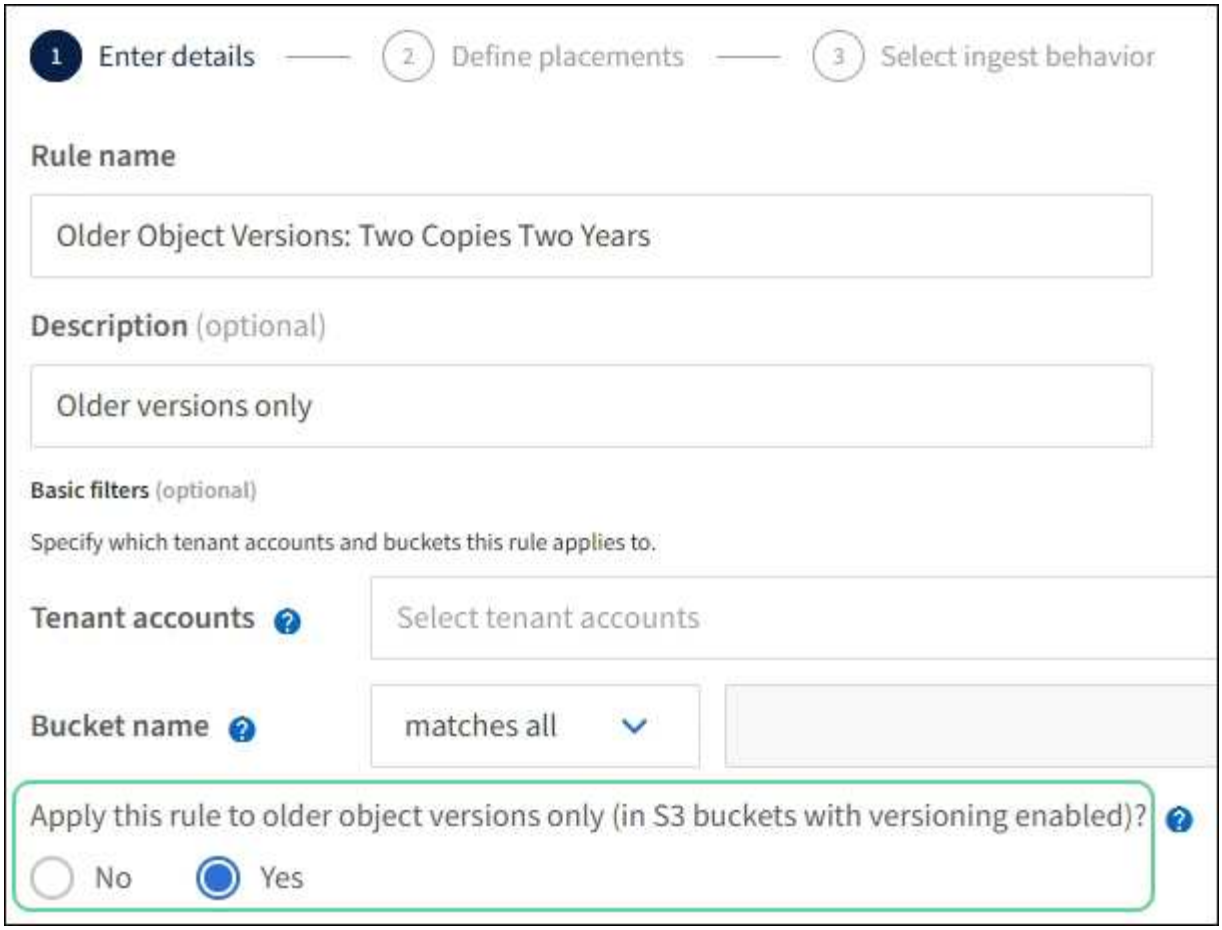
Regeldefinition	Beispielwert
Storage-Pools	Drei Speicherpools, die jeweils aus verschiedenen Rechenzentren mit den Namen Standort 1, Standort 2 und Standort 3 bestehen.
Regelname	Drei Kopien Zehn Jahre
Referenzzeit	Aufnahmezeit
Platzierungen	An Tag 0 sollten Sie drei replizierte Kopien 10 Jahre (3,652 Tage), eine an Standort 1, eine an Standort 2 und eine an Standort 3 aufbewahren. Löschen Sie Ende 10 Jahre alle Kopien des Objekts.

ILM-Regel 2 beispielsweise 4: Speichern Sie zwei Kopien nicht aktueller Versionen für zwei Jahre

In diesem Beispiel wird eine ILM-Regel zwei Kopien der nicht aktuellen Versionen eines versionierten S3 Objekts für zwei Jahre gespeichert.

Da ILM-Regel 1 für alle Versionen des Objekts gilt, müssen Sie eine weitere Regel erstellen, um nicht aktuelle Versionen herauszufiltern.

Um eine Regel zu erstellen, die als Referenzzeit „nicht aktuelle Zeit“ verwendet, wählen Sie **Ja** für die Frage „Diese Regel nur auf ältere Objektversionen anwenden (in S3 Buckets mit aktivierter Versionierung)?“ aus. Gehen Sie in Schritt 1 (Details eingeben) des Assistenten zum Erstellen einer ILM-Regel vor. Wenn Sie **Yes** auswählen, wird *noncurrent time* automatisch für die Referenzzeit ausgewählt, und Sie können keine andere Referenzzeit auswählen.



In diesem Beispiel werden nur zwei Kopien der nicht aktuellen Versionen gespeichert und diese Kopien für zwei Jahre gespeichert.

Regeldefinition	Beispielwert
Storage-Pools	Zwei Speicherpools, jeweils in verschiedenen Rechenzentren, Standort 1 und Standort 2.
Regelname	Nicht Aktuelle Versionen: Zwei Kopien Zwei Jahre
Referenzzeit	Nicht aktuelle Zeit Wird automatisch ausgewählt, wenn Sie **Yes** für die Frage „Diese Regel nur auf ältere Objektversionen anwenden (in S3 Buckets mit aktivierter Versionierung)?“ auswählen. Im Assistenten zum Erstellen einer ILM-Regel.
Platzierungen	An Tag 0 relativ zur nicht aktuellen Zeit (d. h. ab dem Tag, an dem die Objektversion zur nicht aktuellen Version wird), behalten Sie zwei replizierte Kopien der nicht aktuellen Objektversionen für 2 Jahre (730 Tage), eine in Standort 1 und eine in Standort 2. Löschen Sie Ende 2 Jahre die nicht aktuellen Versionen.

ILM-Richtlinie z. B. 4: S3-versionierte Objekte

Wenn Sie ältere Versionen eines Objekts anders als die aktuelle Version verwalten möchten, müssen Regeln, die „nicht aktuelle Zeit“ als Referenzzeit verwenden, in der ILM-Richtlinie vor Regeln erscheinen, die auf die aktuelle Objektversion Anwendung finden.

Eine ILM-Richtlinie für S3-versionierte Objekte kann ILM-Regeln wie die folgenden umfassen:

- Bewahren Sie alle älteren (nicht aktuellen) Versionen jedes Objekts für 2 Jahre auf, beginnend mit dem Tag, an dem die Version nicht mehr aktuell wurde.

> Die Regeln für „nicht aktuelle Zeit“ müssen in der Richtlinie vor den Regeln erscheinen, die für die aktuelle Objektversion gelten. Andernfalls werden die nicht aktuellen Objektversionen niemals mit der Regel „nicht aktuelle Zeit“ abgeglichen.

- Bei der Einspeisung können Sie drei replizierte Kopien erstellen und eine Kopie an jedem der drei Standorte speichern. Bewahren Sie 10 Jahre lang Kopien der aktuellen Objektversion auf.

Wenn Sie die Beispielrichtlinie simulieren, erwarten Sie, dass Testobjekte wie folgt bewertet werden:

- Alle nicht aktuellen Objektversionen würden mit der ersten Regel abgeglichen. Wenn eine nicht aktuelle Objektversion älter als zwei Jahre ist, wird diese durch ILM dauerhaft gelöscht (alle Kopien der nicht aktuellen Version, die aus dem Grid entfernt wurde).
- Die aktuelle Objektversion würde mit der zweiten Regel abgeglichen. Wenn die aktuelle Objektversion über einen Zeitraum von 10 Jahren gespeichert wurde, fügt der ILM-Prozess eine delete-Markierung als aktuelle Version des Objekts hinzu und macht die vorherige Objektversion „noncurrent“. Bei der nächsten ILM-Evaluierung stimmt diese nicht aktuelle Version mit der ersten Regel überein. Dadurch wird die Kopie an Standort 3 gelöscht und die beiden Kopien an Standort 1 und Standort 2 werden für weitere 2 Jahre gespeichert.

Beispiel 5: ILM-Regeln und Richtlinie für striktes Ingest-Verhalten

Ein Speicherortfilter und das strikte Aufnahmeverhalten in einer Regel verhindern, dass Objekte an einem bestimmten Datacenter-Standort gespeichert werden.

In diesem Beispiel will ein Mieter mit Sitz in Paris aufgrund von regulatorischen Bedenken einige Objekte nicht außerhalb der EU speichern. Andere Objekte, einschließlich aller Objekte aus anderen Mandantenkonten, können entweder im Rechenzentrum von Paris oder im Rechenzentrum der USA gespeichert werden.

> Die folgenden ILM-Regeln und -Richtlinien sind nur Beispiele. Es gibt viele Möglichkeiten zur Konfiguration von ILM-Regeln. Simulieren Sie vor der Aktivierung einer neuen Richtlinie, um zu bestätigen, dass sie so funktioniert, wie sie zum Schutz von Inhalten vor Verlust vorgesehen ist.

Verwandte Informationen

- "Aufnahmeoptionen"
- "Erstellen Sie eine ILM-Regel: Wählen Sie Ingest Behavior aus"

ILM-Regel 1 beispielsweise 5: Strenge Einspeisung für das Pariser Rechenzentrum

In diesem Beispiel verwendet die ILM-Regel das strikte Ingest-Verhalten, um zu gewährleisten, dass Objekte, die von einem in Paris ansässigen Mieter in S3-Buckets gespeichert werden, wobei die Region auf eu-West-3 Region (Paris) eingestellt ist, nie im US-Rechenzentrum gespeichert werden.

Diese Regel gilt für Objekte, die zum Pariser Mieter gehören und die S3-Bucket-Region auf eu-West-3 (Paris) eingestellt ist.

Regeldefinition	Beispielwert
Mandantenkonto	Mieter von Paris
Erweiterter Filter	Die Positionsbeschränkung entspricht eu-West-3
Storage-Pools	Standort 1 (Paris)
Regelname	Strenge Einspeisung für ein Pariser Rechenzentrum
Referenzzeit	Aufnahmezeit
Platzierungen	An Tag 0 bewahren Sie zwei replizierte Kopien für immer in Standort 1 (Paris) auf.
Aufnahmeverhalten	Streng. Verwenden Sie bei der Einspeisung immer die Platzierungen dieser Regel. Die Aufnahme schlägt fehl, wenn es nicht möglich ist, zwei Kopien des Objekts im Pariser Rechenzentrum zu speichern.

ILM-Regel 2 beispielsweise 5: Ausgewogene Aufnahme für andere Objekte

Diese Beispiel-ILM-Regel verwendet das ausgewogene Ingest-Verhalten, um optimale ILM-Effizienz für Objekte zu erzielen, die nicht der ersten Regel zugeordnet sind. Zwei Kopien aller Objekte, die dieser Regel entsprechen, werden gespeichert - eins im US-Rechenzentrum und eins im Pariser Rechenzentrum. Wenn die Regel nicht sofort erfüllt werden kann, werden Zwischenkopien an jedem verfügbaren Ort gespeichert.

Diese Regel gilt für Objekte, die einem beliebigen Mieter und einer beliebigen Region angehören.

Regeldefinition	Beispielwert
Mandantenkonto	Ignorieren
Erweiterter Filter	*Nicht angegeben*
Storage-Pools	Standort 1 (Paris) und Standort 2 (USA)
Regelname	2 Kopien 2 Datacenter
Referenzzeit	Aufnahmezeit
Platzierungen	Am Tag 0 werden zwei replizierte Kopien für immer in zwei Datacentern aufbewahrt

Regeldefinition	Beispielwert
Aufnahmeverhalten	Ausgeglichen. Objekte, die dieser Regel entsprechen, werden nach Möglichkeit gemäß den Anweisungen zur Platzierung der Regel platziert. Andernfalls werden an jedem beliebigen Ort vorläufige Kopien angefertigt.

ILM-Richtlinie z. B. 5: Kombination von Aufnahmeverhalten

Die ILM-Beispielrichtlinie enthält zwei Regeln mit unterschiedlichen Aufnahmeverhalten.

Eine ILM-Richtlinie, die zwei unterschiedliche Aufnahmeverhalten nutzt, kann ILM-Regeln wie die folgenden umfassen:

- Speichern Sie Objekte, die zum Pariser Mieter gehören und die S3-Bucket-Region auf eu-West-3 (Paris) gesetzt ist, nur im Datacenter in Paris. Aufnahme fehlgeschlagen, wenn das Pariser Rechenzentrum nicht verfügbar ist.
- Speichern Sie alle anderen Objekte (einschließlich solcher, die zum Pariser Mieter gehören, jedoch über eine andere Bucket-Region verfügen) sowohl im US-Rechenzentrum als auch im Pariser Rechenzentrum. Erstellen Sie Zwischenkopien an einem beliebigen verfügbaren Speicherort, wenn die Platzierungsanweisung nicht erfüllt werden kann.

Wenn Sie die Beispielrichtlinie simulieren, erwarten Sie, dass Testobjekte wie folgt bewertet werden:

- Alle Objekte, die zum Pariser Mieter gehören und die S3-Bucket-Region auf eu-West-3 gesetzt haben, werden mit der ersten Regel abgeglichen und im Pariser Rechenzentrum gespeichert. Da die erste Regel strenge Einspeisung verwendet, werden diese Objekte nie im US-Rechenzentrum gespeichert. Wenn die Storage-Nodes im Pariser Datacenter nicht verfügbar sind, schlägt die Aufnahme fehl.
- Alle anderen Objekte werden mit der zweiten Regel abgeglichen, einschließlich Objekte, die zum Pariser Mieter gehören und für die die S3-Bucket-Region nicht auf eu-West-3 gesetzt ist. In jedem Datacenter wird eine Kopie jedes Objekts gespeichert. Da die zweite Regel jedoch eine ausgewogene Aufnahme verwendet und ein Datacenter nicht zur Verfügung steht, werden zwei Übergangskopien an jedem verfügbaren Standort gespeichert.

Beispiel 6: Ändern einer ILM-Richtlinie

Wenn Ihr Datenschutz geändert werden muss oder Sie neue Standorte hinzufügen, können Sie eine neue ILM-Richtlinie erstellen und aktivieren.

Vor dem Ändern einer Richtlinie muss verstanden werden, wie Änderungen an ILM-Platzierungen die Gesamt-Performance eines StorageGRID Systems vorübergehend beeinträchtigen können.

In diesem Beispiel wurde eine neue StorageGRID-Site mit einer Erweiterung hinzugefügt, und für die Speicherung von Daten am neuen Standort muss eine neue aktive ILM-Richtlinie implementiert werden. Um eine neue aktive Richtlinie zu implementieren, zuerst "Erstellen Sie eine Richtlinie". Danach müssen Sie "Simulieren"und dann "Aktivieren" die neue Richtlinie.

> Die folgenden ILM-Regeln und -Richtlinien sind nur Beispiele. Es gibt viele Möglichkeiten zur Konfiguration von ILM-Regeln. Simulieren Sie vor der Aktivierung einer neuen Richtlinie, um zu bestätigen, dass sie so funktioniert, wie sie zum Schutz von Inhalten vor Verlust vorgesehen ist.

Wie sich eine Änderung einer ILM-Richtlinie auf die Performance auswirkt

Wenn Sie eine neue ILM-Richtlinie aktivieren, wird die Performance Ihres StorageGRID Systems möglicherweise vorübergehend beeinträchtigt, insbesondere dann, wenn aufgrund der Platzierungsanweisungen in der neuen Richtlinie viele vorhandene Objekte an einen neuen Standort verschoben werden müssen.

Bei der Aktivierung einer neuen ILM-Richtlinie verwendet StorageGRID sie zum Management aller Objekte, einschließlich vorhandener Objekte und neu aufgenommener Objekte. Prüfen Sie vor der Aktivierung einer neuen ILM-Richtlinie alle Änderungen an der Platzierung vorhandener replizierter und Erasure Coding-Objekte. Das Ändern des Speicherorts eines vorhandenen Objekts kann zu vorübergehenden Ressourcenproblemen führen, wenn die neuen Platzierungen ausgewertet und implementiert werden.

Sie können sicherstellen, dass eine neue ILM-Richtlinie die Platzierung vorhandener replizierter und Erasure-Coded-Objekte nicht beeinträchtigt"Erstellen Sie eine ILM-Regel mit einem Filter für die Aufnahmezeit". Zum Beispiel ist **Ingest time *am oder nach <date and time>***, so dass die neue Regel nur für Objekte gilt, die am oder nach dem angegebenen Datum und der angegebenen Uhrzeit aufgenommen wurden.

Folgende Arten von ILM-Richtlinienänderungen, die vorübergehend Auswirkungen auf die StorageGRID Performance haben:

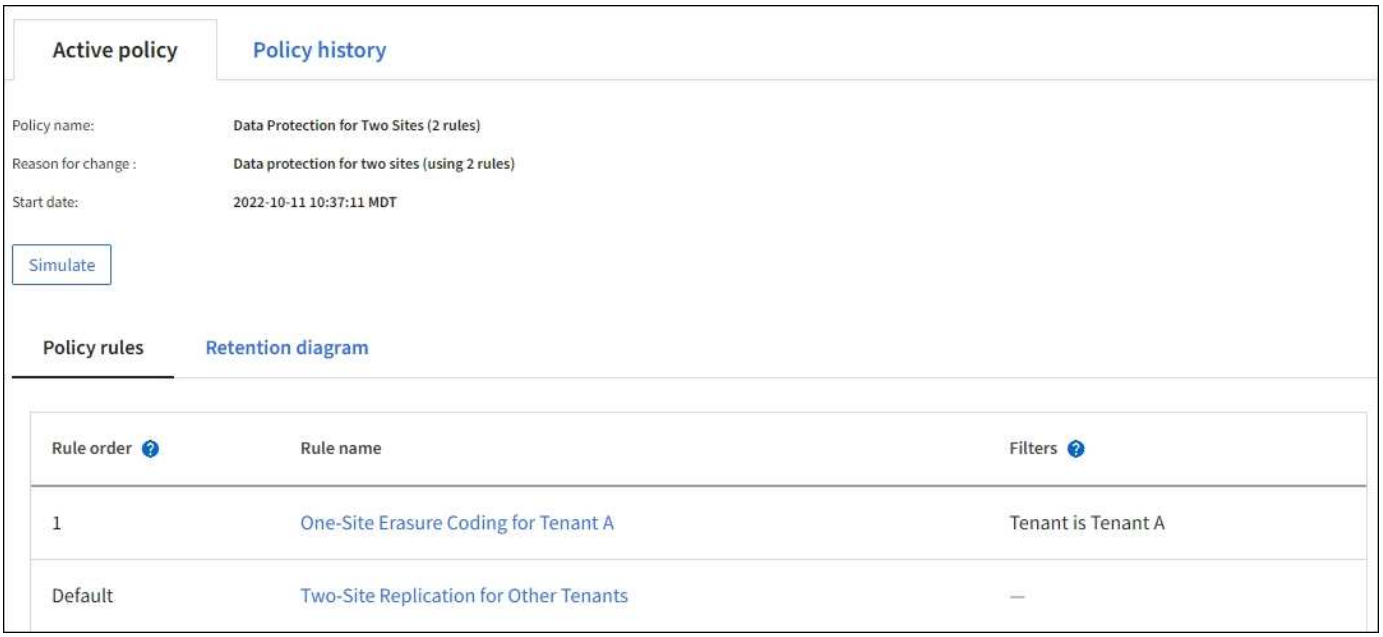
- Anwenden eines anderen Erasure Coding-Profils auf vorhandene Objekte, die zur Fehlerkorrektur codiert wurden

  > StorageGRID erachtet jedes Erasure Coding-Profil als einzigartig und verwendet beim Einsatz eines neuen Profils keine Fragmente des Erasure Coding-Codes mehr.

- Ändern des für vorhandene Objekte erforderlichen Kopientyps; z. B. Konvertieren eines großen Anteils replizierter Objekte in Objekte mit Erasure-Coding-Verfahren.
- Kopien vorhandener Objekte werden an einen völlig anderen Speicherort verschoben, z. B. um eine große Anzahl von Objekten in einen oder aus einem Cloud-Storage-Pool oder an einen Remote-Standort zu verschieben.

Aktive ILM-Richtlinie z. B. 6: Datensicherung an zwei Standorten

In diesem Beispiel wurde die aktive ILM-Richtlinie ursprünglich für ein StorageGRID System mit zwei Standorten konzipiert und verwendet zwei ILM-Regeln.



In dieser ILM-Richtlinie werden Objekte, die von Mandanten A gehören, durch Erasure Coding von 2+1 an einem Standort geschützt, während Objekte, die zu allen anderen Mandanten gehören, durch die Replizierung mit zwei Kopien über zwei Standorte hinweg geschützt sind.

Regel 1: Erasure Coding für einen Standort für Mandant A

Regeldefinition	Beispielwert
Regelname	Erasure Coding für einen Standort für Mandant A
Mandantenkonto	Mandant A
Storage-Pool	Standort 1
Platzierungen	2+1 Erasure Coding in Standort 1 vom Tag 0 bis ewig

Regel 2: Replizierung zwischen zwei Standorten für andere Mandanten

Regeldefinition	Beispielwert
Regelname	Replizierung an zwei Standorten für andere Mandanten
Mandantenkonto	Ignorieren
Storage-Pools	Standort 1 und Standort 2
Platzierungen	Zwei replizierte Kopien von Tag 0 auf ewig: Eine Kopie an Standort 1 und eine Kopie an Standort 2.

ILM-Richtlinie für Beispiel 6: Datensicherung an drei Standorten

In diesem Beispiel wird die ILM-Richtlinie durch eine neue Richtlinie für ein StorageGRID System mit drei Standorten ersetzt.

Nach einer Erweiterung zum Hinzufügen des neuen Standorts erstellte der Grid-Administrator zwei neue Speicherpools: Einen Speicherpool für Standort 3 und einen Speicherpool mit allen drei Standorten (nicht mit dem Standardspeicherpool Alle Storage-Nodes). Anschließend erstellte der Administrator zwei neue ILM-Regeln und eine neue ILM-Richtlinie, die für den Schutz von Daten an allen drei Standorten konzipiert wurde.

Bei Aktivierung dieser neuen ILM-Richtlinie werden Objekte, die von Mandant A gehören, an drei Standorten durch 2+1 Erasure Coding geschützt, während Objekte, die zu anderen Mandanten gehören (und kleinere Objekte von Mandanten A), durch Replizierung mit 3 Kopien über drei Standorte hinweg gesichert werden.

Regel 1: Erasure Coding für drei Standorte für Mandant A

Regeldefinition	Beispielwert
Regelname	Three-Site Erasure Coding für Mandant A
Mandantenkonto	Mandant A
Storage-Pool	Alle 3 Standorte (einschließlich Standort 1, Standort 2 und Standort 3)
Platzierungen	2+1 Erasure Coding in allen 3 Standorten vom Tag 0 bis für immer

Regel 2: Replizierung an drei Standorten für andere Mandanten

Regeldefinition	Beispielwert
Regelname	Replikation von drei Standorten für andere Mandanten
Mandantenkonto	Ignorieren
Storage-Pools	Standort 1, Standort 2 und Standort 3
Platzierungen	Drei replizierte Kopien von Tag 0 bis ewig: Eine Kopie an Standort 1, eine Kopie an Standort 2 und eine Kopie an Standort 3.

Aktivieren der ILM-Richtlinie, z. B. 6

Wenn Sie eine neue ILM-Richtlinie aktivieren, werden vorhandene Objekte auf Basis der Anweisungen zur Platzierung in neuen oder aktualisierten Regeln möglicherweise an neue Standorte verschoben oder neue Objektkopien für vorhandene Objekte erstellt.

Fehler in einer ILM-Richtlinie können zu nicht wiederherstellbaren Datenverlusten führen. Prüfen und simulieren Sie die Richtlinie sorgfältig, bevor Sie sie aktivieren, um sicherzustellen, dass sie wie vorgesehen funktioniert.

Bei der Aktivierung einer neuen ILM-Richtlinie verwendet StorageGRID sie zum Management aller Objekte, einschließlich vorhandener Objekte und neu aufgenommener Objekte. Prüfen Sie vor der Aktivierung einer neuen ILM-Richtlinie alle Änderungen an der Platzierung vorhandener replizierter und Erasure Coding-Objekte. Das Ändern des Speicherorts eines vorhandenen Objekts kann zu vorübergehenden Ressourcenproblemen führen, wenn die neuen Platzierungen ausgewertet und implementiert werden.

Was passiert, wenn sich die Anweisungen zur Einhaltung von Datenkonsistenz ändern

In der derzeit aktiven ILM-Richtlinie für dieses Beispiel sind Objekte, die zu Mandant A gehören, durch den Erasure Coding 2+1 an Standort 1 geschützt. In der neuen ILM-Richtlinie werden Objekte von Mandant A durch Erasure Coding 2+1 an Standorten 1, 2 und 3 geschützt.

Wenn die neue ILM-Richtlinie aktiviert ist, werden die folgenden ILM-Vorgänge durchgeführt:

- Neue von Mandanten A aufgenommene Objekte werden in zwei Datenfragmente aufgeteilt und ein Paritätsfragment wird hinzugefügt. Dann wird jedes der drei Fragmente an einem anderen Ort gespeichert.
- Die vorhandenen Objekte, die von Mandant A gehören, werden bei der laufenden ILM-Überprüfung neu bewertet. Da die ILM-Anweisungen für die Platzierung ein neues Erasure-Coding-Profil verwenden, werden völlig neue Fragmente erstellt und an die drei Standorte verteilt, die zur Fehlerkorrektur codiert wurden.

Die vorhandenen 2+1-Fragmente an Standort 1 werden nicht wiederverwendet. StorageGRID erachtet jedes Erasure Coding-Profil als einzigartig und verwendet beim Einsatz eines neuen Profils keine Fragmente des Erasure Coding-Codes mehr.

Was geschieht, wenn sich Replikationsanweisungen ändern

In der derzeit aktiven ILM-Richtlinie für dieses Beispiel werden Objekte anderer Mandanten mithilfe von zwei replizierten Kopien in Storage Pools an Standorten 1 und 2 geschützt. In der neuen ILM-Richtlinie werden Objekte anderer Mandanten mit drei replizierten Kopien in Storage Pools an Standorten 1, 2 und 3 gesichert.

Wenn die neue ILM-Richtlinie aktiviert ist, werden die folgenden ILM-Vorgänge durchgeführt:

- Wenn ein anderer Mandant als Mandant A ein neues Objekt aufnimmt, erstellt StorageGRID drei Kopien und speichert eine Kopie an jedem Standort.
- Vorhandene Objekte, die zu diesen anderen Mandanten gehören, werden bei der laufenden ILM-Überprüfung neu bewertet. Da die vorhandenen Objektkopien an Standort 1 und Standort 2 weiterhin die Replizierungsanforderungen der neuen ILM-Regel erfüllen, muss StorageGRID nur eine neue Kopie des Objekts für Standort 3 erstellen.

Auswirkungen der Aktivierung dieser Richtlinie auf die Performance

Wenn die ILM-Richtlinie in diesem Beispiel aktiviert ist, wirkt sich dies vorübergehend auf die Gesamtleistung dieses StorageGRID-Systems aus. Wenn die Grid-Ressourcen höher als die normalen Level sind, werden neue Fragmente, die nach der Fehlerkorrektur codiert wurden, für vorhandene Objekte von Mandant A und neue replizierte Kopien an Standort 3 für vorhandene Objekte anderer Mandanten erstellt.

Aufgrund der Änderung der ILM-Richtlinie können Lese- und Schreibanfragen von Clients vorübergehend höhere Latenzen aufweisen als die normalen Latenzen. Die Latenzen kehren wieder auf die normalen Werte zurück, nachdem die Anweisungen zur Platzierung im gesamten Grid vollständig implementiert wurden.

Um Ressourcenprobleme bei der Aktivierung einer neuen ILM-Richtlinie zu vermeiden, können Sie den

erweiterten Filter für die Aufnahmezeit in jeder Regel verwenden, die den Speicherort einer großen Anzahl vorhandener Objekte ändern könnte. Legen Sie für die Aufnahme-Zeit den Wert fest, der ungefähr der Zeit entspricht, zu der die neue Richtlinie in Kraft tritt, um sicherzustellen, dass vorhandene Objekte nicht unnötig verschoben werden.

Wenden Sie sich an den technischen Support, wenn Sie die Verarbeitungsgeschwindigkeit von Objekten nach einer ILM-Richtlinienänderung verlangsamen oder erhöhen müssen.

Beispiel 7: Konforme ILM-Richtlinie für S3 Object Lock

Sie können den S3-Bucket, ILM-Regeln und ILM-Richtlinie in diesem Beispiel als Ausgangspunkt verwenden, wenn Sie eine ILM-Richtlinie definieren, um die Objektschutz- und Aufbewahrungsanforderungen für Objekte in Buckets zu erfüllen, wenn S3-Objektsperre aktiviert ist.

Wenn Sie die Funktion „ältere Compliance“ in früheren StorageGRID Versionen verwendet haben, können Sie dieses Beispiel auch zur Verwaltung vorhandener Buckets verwenden, in denen die alte Compliance-Funktion aktiviert ist.

Die folgenden ILM-Regeln und -Richtlinien sind nur Beispiele. Es gibt viele Möglichkeiten zur Konfiguration von ILM-Regeln. Simulieren Sie vor der Aktivierung einer neuen Richtlinie, um zu bestätigen, dass sie so funktioniert, wie sie zum Schutz von Inhalten vor Verlust vorgesehen ist.

Verwandte Informationen

- "Objekte managen mit S3 Object Lock"
- "ILM-Richtlinie erstellen"

Bucket und Objekte für S3 Object Lock Beispiel

In diesem Beispiel hat ein S3-Mandantenkonto mit der Bezeichnung „Bank of ABC“ durch den Mandanten-Manager einen Bucket erstellt, der mit S3-Objektsperre aktiviert wurde, um kritische Bankdatensätze zu speichern.

Bucket-Definition	Beispielwert
Name Des Mandantenkontos	Bank von ABC
Bucket-Name	bankaufzeichnungen
Bucket-Region	US-East-1 (Standard)

Für jedes Objekt und jede Objektversion, die dem Bucket für Bankdatensätze hinzugefügt wird, werden die folgenden Werte für und `legal hold`-Einstellungen verwendet `retain-until-date`.

Einstellung für jedes Objekt	Beispielwert
`retain-until-date`	„2030-12-30T23:59:59Z“ (30. Dezember 2030) Jede Objektversion hat eine eigene `retain-until-date` Einstellung. Diese Einstellung kann erhöht, aber nicht verringert werden.
`legal hold`	„AUS“ (nicht in Kraft) Eine gesetzliche Aufbewahrungsphase kann jederzeit während der Aufbewahrungsfrist auf jeder Objektversion platziert oder aufgehoben werden. Befindet sich ein Objekt unter einem Legal Hold, kann das Objekt auch dann nicht gelöscht werden, wenn das `retain-until-date` erreicht wurde.

ILM-Regel 1 für S3 Object Lock – Beispiel: Profil für Erasure Coding mit Bucket-Matching

Diese Beispiel-ILM-Regel gilt nur für das S3-Mandantenkonto namens Bank of ABC. Die Applikation wird einem beliebigen Objekt im `bank-records` Bucket zugeordnet und das Objekt dann mithilfe eines 6+3 Erasure Coding-Profils auf Storage Nodes an drei Datacenter-Standorten gespeichert. Diese Regel erfüllt die Anforderungen von Buckets mit aktivierter S3 Object Lock: Eine Kopie wird auf Storage-Nodes vom Tag 0 bis dauerhaft aufbewahrt. Als Referenzzeit wird die Aufnahmezeit verwendet.

Regeldefinition	Beispielwert
Regelname	Konforme Regel: EC-Objekte in Bank-Records Bucket - Bank of ABC
Mandantenkonto	Bank von ABC
Bucket-Name	`bank-records`
Erweiterter Filter	Objektgröße (MB) größer als 1 **Hinweis:** dieser Filter sorgt dafür, dass das Erasure Coding nicht für Objekte mit einer Größe von 1 MB verwendet wird.

Regeldefinition	Beispielwert
Referenzzeit	Aufnahmezeit
Platzierungen	Ab Tag 0 dauerhaft speichern
Profil für Erasure Coding	• Erstellen einer mit Erasure Coding verschlüsselten Kopie auf Storage-Nodes an drei Datacenter-Standorten • Verwendet das Erasure Coding-Schema 6+3

ILM-Regel 2 für S3 Object Lock Beispiel: Nicht konforme Regel

Diese Beispiel-ILM-Regel speichert zunächst zwei replizierte Objektkopien auf Storage Nodes. Nach einem Jahr wird für immer eine Kopie auf einem Cloud-Storage-Pool gespeichert. Da diese Regel einen Cloud-Storage-Pool verwendet, ist diese nicht konform und gilt nicht für Objekte in Buckets, deren S3-Objektsperre aktiviert ist.

Regeldefinition	Beispielwert
Regelname	Nicht konforme Regel: Cloud Storage Pool
Mandantenkonten	Nicht angegeben
Bucket-Name	Nicht angegeben, gilt aber nur für Buckets, für die die S3-Objektsperre (oder die ältere Compliance-Funktion) nicht aktiviert ist.
Erweiterter Filter	Nicht angegeben

Regeldefinition	Beispielwert
Referenzzeit	Aufnahmezeit
Platzierungen	• Halten Sie am Tag 0 zwei replizierte Kopien auf Storage Nodes in Datacenter 1 und Datacenter 2 für 365 Tage • Nach einem Jahr sollte eine replizierte Kopie immer in einem Cloud-Storage-Pool aufbewahrt werden

ILM-Regel 3 für S3 Object Lock Beispiel: Standardregel

Diese Beispiel-ILM-Regel kopiert Objektdaten in Storage-Pools in zwei Datacentern. Diese konforme Regel wurde als Standardregel in der ILM-Richtlinie konzipiert. Es enthält keine Filter, verwendet keine nicht aktuelle Referenzzeit und erfüllt die Anforderungen von Buckets mit aktivierter S3 Objektsperre: Zwei Objektkopien werden auf Storage-Nodes aufbewahrt von Tag 0 bis für immer und verwenden die Aufnahme als Referenzzeit.

Regeldefinition	Beispielwert
Regelname	Standard-konforme Regel: Zwei Kopien zwei Rechenzentren
Mandantenkonto	Nicht angegeben
Bucket-Name	Nicht angegeben
Erweiterter Filter	Nicht angegeben

Regeldefinition	Beispielwert
Referenzzeit	Aufnahmezeit

Regeldefinition	Beispielwert
Platzierungen	Halten Sie von Tag 0 bis für immer zwei replizierte Kopien bereit – eins auf Storage-Nodes im Datacenter 1 und eins auf Storage-Nodes im Datacenter 2.

Konforme ILM-Richtlinie für S3 Object Lock Beispiel

Zum Erstellen einer ILM-Richtlinie, die alle Objekte in Ihrem System effektiv schützt, auch in Buckets, deren S3-Objektsperre aktiviert ist, müssen Sie ILM-Regeln auswählen, die die Storage-Anforderungen für alle Objekte erfüllen. Anschließend müssen Sie die Richtlinie simulieren und aktivieren.

Fügen Sie der Richtlinie Regeln hinzu

In diesem Beispiel umfasst die ILM-Richtlinie drei ILM-Regeln in der folgenden Reihenfolge:

1. Eine konforme Regel, die Erasure Coding verwendet, um Objekte mit einer Größe von mehr als 1 MB in einem bestimmten Bucket zu schützen. Dabei ist S3 Object Lock aktiviert. Die Objekte werden von Tag 0 bis für immer auf Speicherknoten gespeichert.
2. Eine nicht konforme Regel, die zwei replizierte Objektkopien auf Storage-Nodes für ein Jahr erstellt und dann eine Objektkopie für immer in einen Cloud Storage Pool verschiebt. Diese Regel gilt nicht für Buckets, für die S3-Objektsperre aktiviert ist, da sie einen Cloud-Storage-Pool verwendet.
3. Die standardmäßige, konforme Regel, die zwei replizierte Objektkopien auf Storage-Nodes erstellt, von Tag 0 bis für immer.

Simulieren Sie die Richtlinie

Nachdem Sie Ihrer Richtlinie Regeln hinzugefügt, eine Standard-konforme Regel ausgewählt und die anderen Regeln angeordnet haben, sollten Sie die Richtlinie simulieren, indem Sie Objekte aus dem Bucket mit aktivierter S3 Object Lock und aus anderen Buckets testen. Wenn Sie beispielsweise die Beispielrichtlinie simulieren, erwarten Sie, dass Testobjekte wie folgt bewertet werden:

- Die erste Regel entspricht nur Testobjekten, die mehr als 1 MB in den Bucket-Bankdatensätzen für den Mandanten der Bank of ABC enthalten sind.
- Die zweite Regel entspricht allen Objekten in allen nicht-konformen Buckets für alle anderen Mandantenkonten.
- Die Standardregel stimmt mit den folgenden Objekten überein:
  - Objekte mit einer Größe von 1 MB oder kleiner in den Bucket-Bankaufzeichnungen für den Mandanten der Bank of ABC
  - Objekte in jedem anderen Bucket, bei dem die S3-Objektsperre für alle anderen Mandantenkonten aktiviert ist

Aktivieren Sie die Richtlinie

Wenn Sie mit der neuen Richtlinie zufrieden sind, dass Objektdaten wie erwartet geschützt werden, können Sie sie aktivieren.

Beispiel 8: Prioritäten für den S3-Bucket-Lebenszyklus und die ILM-Richtlinie

Je nach Lifecycle-Konfiguration folgen Objekte den Aufbewahrungseinstellungen

entweder des S3 Bucket-Lebenszyklus oder einer ILM-Richtlinie.

Beispiel für einen Bucket-Lebenszyklus, der Priorität gegenüber der ILM-Richtlinie hat

ILM-Richtlinie

- Regel basiert auf nicht aktueller Zeitreferenz: An Tag 0, bewahren Sie X Kopien 20 Tage lang auf
- Regel basierend auf Referenz zur Aufnahmezeit (Standard): An Tag 0 sollten X Kopien 50 Tage lang aufbewahrt werden

Bucket-Lebenszyklus

```
"Filter": {"Prefix": "docs/"}, "Expiration": {"Days": 100},
"NoncurrentVersionExpiration": {"NoncurrentDays": 5}
```

Ergebnis

- Ein Objekt namens „docs/Text“ wird aufgenommen. Es entspricht dem Bucket-Lebenszyklusfilter des Präfixes „docs/“.
  - Nach 100 Tagen wird eine Löschmarkierung erstellt und "docs/Text" wird nicht mehr aktuell.
  - Nach 5 Tagen, insgesamt 105 Tage seit Aufnahme, wird "docs/Text" gelöscht.
  - Nach 95 Tagen, also insgesamt 200 Tagen seit der Aufnahme und 100 Tagen seit der Löschmarkierung, wird die abgelaufene Löschmarkierung gelöscht.
- Ein Objekt namens „Video/Film“ wird aufgenommen. Er stimmt nicht mit dem Filter überein und verwendet die ILM-Aufbewahrungsrichtlinie.
  - Nach 50 Tagen wird eine Löschmarkierung erstellt und "Video/Film" wird nicht mehr aktuell.
  - Nach 20 Tagen, insgesamt 70 Tage seit der Aufnahme, "Video/Film" wird gelöscht.
  - Nach 30 Tagen, also insgesamt 100 Tagen seit der Aufnahme und 50 Tagen seit der Löschmarkierung, wird die abgelaufene Löschmarkierung gelöscht.

Beispiel für den Bucket-Lebenszyklus, der implizit dauerhaft hält

ILM-Richtlinie

- Regel basiert auf nicht aktueller Zeitreferenz: An Tag 0, bewahren Sie X Kopien 20 Tage lang auf
- Regel basierend auf Referenz zur Aufnahmezeit (Standard): An Tag 0 sollten X Kopien 50 Tage lang aufbewahrt werden

Bucket-Lebenszyklus

```
"Filter": {"Prefix": "docs/"}, "Expiration": {"ExpiredObjectDeleteMarker":
true}
```

Ergebnis

- Ein Objekt namens „docs/Text“ wird aufgenommen. Es entspricht dem Bucket-Lebenszyklusfilter des Präfixes „docs/“.

  Die `Expiration` Aktion gilt nur für abgelaufene Löschmarkierungen, was bedeutet, alles andere für immer zu behalten (beginnend mit "docs/").

  Löschmarkierungen, die mit „docs/“ beginnen, werden entfernt, wenn sie abgelaufen sind.

- Ein Objekt namens „Video/Film“ wird aufgenommen. Er stimmt nicht mit dem Filter überein und verwendet die ILM-Aufbewahrungsrichtlinie.

- Nach 50 Tagen wird eine Löschmarkierung erstellt und "Video/Film" wird nicht mehr aktuell.
- Nach 20 Tagen, insgesamt 70 Tage seit der Aufnahme, "Video/Film" wird gelöscht.
- Nach 30 Tagen, also insgesamt 100 Tagen seit der Aufnahme und 50 Tagen seit der Löschmarkierung, wird die abgelaufene Löschmarkierung gelöscht.

Beispiel für die Verwendung von Bucket-Lebenszyklus zur Duplizierung von ILM und zur Bereinigung abgelaufener Löschmarkierungen

ILM-Richtlinie

- Regel basiert auf nicht aktueller Zeitreferenz: An Tag 0, bewahren Sie X Kopien 20 Tage lang auf
- Regel basierend auf Referenz zur Aufnahmezeit (Standard): An Tag 0, X Kopien für immer aufbewahren

Bucket-Lebenszyklus

```
"Filter": {}, "Expiration": {"ExpiredObjectDeleteMarker": true},
"NoncurrentVersionExpiration": {"NoncurrentDays": 20}
```

Ergebnis

- Die ILM-Richtlinie wird im Bucket-Lebenszyklus dupliziert.
  - Die „Forever“-Richtlinie zielt darauf ab, Objekte manuell zu entfernen und nicht aktuelle Versionen nach 20 Tagen zu bereinigen. Folglich behält die Ingest-Time-Regel abgelaufene Löschmarkierungen für immer bei.
  - Der Bucket-Lebenszyklus dupliziert das Verhalten der ILM-Richtlinie beim Hinzufügen `"ExpiredObjectDeleteMarker": true`, was Löschmarkierungen entfernt, wenn sie abgelaufen sind
- Ein Objekt wird aufgenommen. Kein Filter bedeutet, dass der Bucket-Lebenszyklus auf alle Objekte angewendet und die ILM-Aufbewahrungseinstellungen außer Kraft gesetzt wird.
  - Wenn eine Serviceeinheit eine Anfrage zum Löschen von Objekten ausgibt, wird eine Löschmarkierung erstellt und das Objekt wird nicht mehr aktuell.
  - Nach 20 Tagen wird das nicht aktuelle Objekt gelöscht und die Löschmarkierung ist abgelaufen.
  - Kurz danach wird die abgelaufene Löschmarkierung gelöscht.