



Objektmanagement mit ILM

StorageGRID

NetApp
October 03, 2025

Inhalt

Objektmanagement mit ILM	1
Verwalten von Objekten mit Information Lifecycle Management	1
Wie ILM im gesamten Leben eines Objekts funktioniert	1
Was ist eine ILM-Richtlinie	25
Was ist eine ILM-Regel	27
Erstellung von Speicherklassen, Speicherpools, EC-Profilen und Regionen	32
Erstellen einer ILM-Regel	85
ILM-Richtlinie erstellen	104
Arbeiten mit ILM-Regeln und ILM-Richtlinien	128
Verwalten von Objekten mit S3 Object Lock	133
Was ist S3 Object Lock?	133
Vergleich der S3-Objektsperre mit älterer Compliance	134
Workflow für S3 Objektsperre	136
Anforderungen für die S3-Objektsperre	138
Aktivieren der S3-Objektsperre global	142
Beseitigung von Konsistenzfehlern bei der Aktualisierung der S3-Objektsperre oder der alten Compliance-Konfiguration	144
Beispiele für ILM-Regeln und -Richtlinien	145
Beispiel 1: ILM-Regeln und -Richtlinie für Objekt-Storage	145
Beispiel 2: ILM-Regeln und Richtlinie für EC-Objektgrößen-Filterung	148
Beispiel 3: ILM-Regeln und -Richtlinie für besseren Schutz von Image-Dateien	150
Beispiel 4: ILM-Regeln und -Richtlinie für versionierte Objekte mit S3	153
Beispiel 5: ILM-Regeln und Richtlinie für striktes Ingest-Verhalten	157
Beispiel 6: Ändern einer ILM-Richtlinie	161
Beispiel 7: Konforme ILM-Richtlinie für S3 Object Lock	166

Objektmanagement mit ILM

Erfahren Sie, wie Sie Objekte mithilfe von Richtlinien und Regeln für den Informationslebenszyklus managen und S3 Object Lock verwenden, um gesetzliche Vorgaben für die Objektaufbewahrung zu erfüllen.

- ["Verwalten von Objekten mit Information Lifecycle Management"](#)
- ["Verwalten von Objekten mit S3 Object Lock"](#)
- ["Beispiele für ILM-Regeln und -Richtlinien"](#)

Verwalten von Objekten mit Information Lifecycle Management

Sie managen die Objekte in einem StorageGRID-System durch die Konfiguration von Regeln und Richtlinien für das Information Lifecycle Management (ILM). Die ILM-Regeln und Richtlinien erläutern StorageGRID, wie Kopien von Objektdaten erstellt und verteilt werden und wie diese Kopien im Laufe der Zeit gemanagt werden.

Für die Entwicklung und Implementierung von ILM-Regeln und der ILM-Richtlinie ist eine sorgfältige Planung erforderlich. 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.

- ["Funktionsweise von ILM während der gesamten Nutzungsdauer eines Objekts"](#)
- ["Was ist eine ILM-Richtlinie"](#)
- ["Was ist eine ILM-Regel"](#)
- ["Erstellung von Speicherklassen, Speicherpools, EC-Profilen und Regionen"](#)
- ["Erstellen einer ILM-Regel"](#)
- ["ILM-Richtlinie erstellen"](#)
- ["Arbeiten mit ILM-Regeln und ILM-Richtlinien"](#)

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.

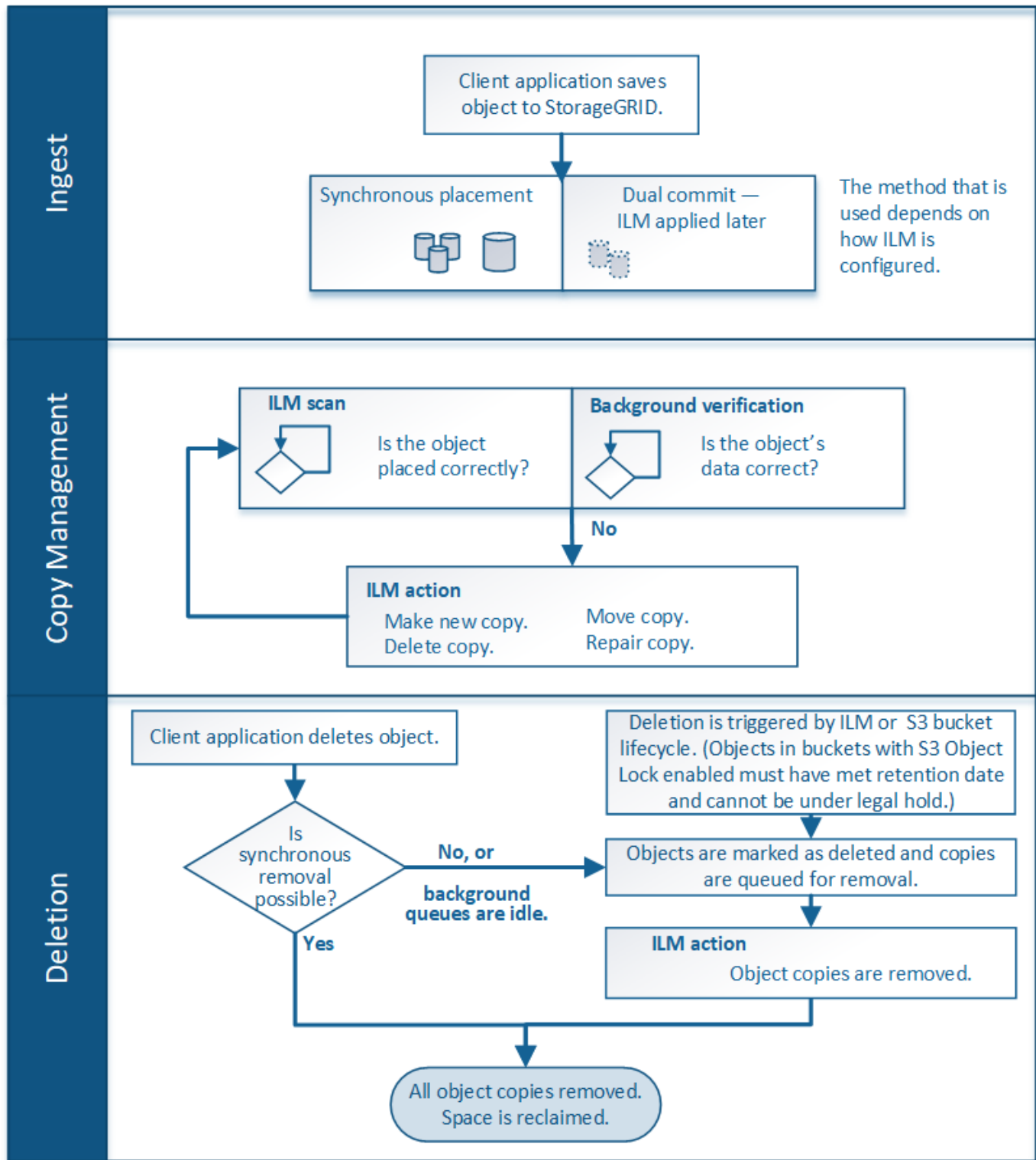
- **Aufnahme:** Aufnahme beginnt, wenn eine S3- oder Swift-Client-Anwendung eine Verbindung zum Speichern eines Objekts in das StorageGRID-System herstellt und abgeschlossen ist, wenn StorageGRID eine „Aufnahme erfolgreich“-Nachricht an den Client zurückgibt. Objektdaten werden bei der Aufnahme entweder 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 -Bewertung: StorageGRID scannt kontinuierlich die Liste der im Grid gespeicherten Objekte und überprüft, 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 Hintergrundüberprüfung 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. Anweisungen zum Monitoring und zur Fehlerbehebung von StorageGRID finden Sie in der Anleitung.
- **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-Objektsperre aktiviert ist, können nicht gelöscht werden, wenn sie sich unter einer gesetzlichen Aufbewahrungspflicht befinden oder wenn ein Aufbewahrungsdatum angegeben, aber noch nicht erfüllt wurde.

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



Verwandte Informationen

"Monitor Fehlerbehebung"

Aufnahme von Objekten

StorageGRID schützt Objekte bei der Aufnahme, entweder durch synchrones Platzieren oder durch Dual-Commit, wie in der ILM-Regel, die den Objekten entspricht.

Wenn ein S3- oder Swift-Client ein Objekt im Grid speichert, führt StorageGRID das Objekt mithilfe einer der folgenden beiden Methoden ein:

- **Synchronous Placement:** StorageGRID erstellt sofort alle Objektkopien, die zur Erfüllung der ILM-Anforderungen benötigt werden. StorageGRID sendet eine Nachricht „Aufnahme erfolgreich“ an den Client, wenn alle Kopien erstellt werden.

Wenn StorageGRID nicht sofort alle Objektkopien erstellen kann (z. B. weil ein erforderlicher Standort vorübergehend nicht verfügbar ist), sendet er entweder eine „Aufnahme fehlgeschlagen“-Nachricht an den Client. Es ist aber auch möglich, vorläufige Objektkopien zu erstellen und ILM später zu evaluieren. Dies hängt davon ab, welche Auswahl Sie bei der Erstellung der ILM-Regel getroffen haben.

- **Dual Commit:** StorageGRID erstellt sofort zwei Zwischenkopien des Objekts, jedes auf einem anderen Speicherknoten und sendet eine „Aufnahme erfolgreich“-Nachricht an den Client. StorageGRID Warteschlangen für die ILM-Bewertung.

Wenn StorageGRID die ILM-Bewertung durchführt, wird zunächst geprüft, ob die übergangsweisen Kopien die Anweisungen zur Platzierung in der ILM-Regel erfüllen. So könnten die beiden vorläufigen Kopien beispielsweise die Anweisungen in einer ILM-Regel mit zwei Kopien erfüllen, doch würden sie die Anweisungen in einer Regel für das Erasure Coding nicht erfüllen. Wenn die Zwischenkopien die ILM-Anweisungen nicht erfüllen, erstellt StorageGRID neue Objektkopien und löscht alle nicht benötigten Zwischenkopien.

Wenn StorageGRID nicht zwei Übergangskopien erstellen kann (z. B. wenn ein Netzwerkproblem die Erstellung der zweiten Kopie verhindert), wird StorageGRID nicht erneut versuchen. Aufnahme schlägt fehl.



S3- oder Swift-Clients können angeben, dass StorageGRID bei der Aufnahme eine einzelne Interimskopie erstellt `REDUCED_REDUNDANCY` Für die Speicherklasse. Weitere Informationen finden Sie in der Anleitung zur Implementierung eines S3- oder Swift-Clients.

StorageGRID verwendet standardmäßig die synchrone Platzierung, um Objekte bei der Aufnahme zu schützen.

Verwandte Informationen

["Datensicherungsoptionen für die Aufnahme"](#)

["S3 verwenden"](#)

["Verwenden Sie Swift"](#)

Datensicherungsoptionen für die Aufnahme

Bei der Erstellung einer ILM-Regel geben Sie eine von drei Optionen zum Schutz von Objekten bei ihrer Aufnahme an: Doppelte Provisionierung, Balance oder strikte. 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.

Doppelte Provisionierung

Wenn Sie die Option Dual Commit auswählen, erstellt StorageGRID sofort interim-Objektkopien auf zwei verschiedenen Storage-Nodes und gibt dem Client eine „Ingest Successful“-Nachricht zurück. Das Objekt

wird zur ILM-Evaluierung in eine Warteschlange gestellt und Kopien, die den Anweisungen zur Platzierung der Regel entsprechen, werden später erstellt.

Wann sollten Sie die Option Dual Commit verwenden

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. Bei der Verwendung von Dual-Commit müssen Sie sicherstellen, dass das Grid zusätzliche Aufgaben zur Erstellung und Entfernung 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.

Streng

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

Wann die strenge Option verwendet werden soll

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. Beispielsweise müssen Sie zur Einhaltung gesetzlicher Vorgaben unter Umständen die strenge Option und einen erweiterten Filter für Speicherortbeschränkungen verwenden, um zu gewährleisten, dass Objekte nie in einem bestimmten Rechenzentrum gespeichert werden.

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

Ausgeglichen

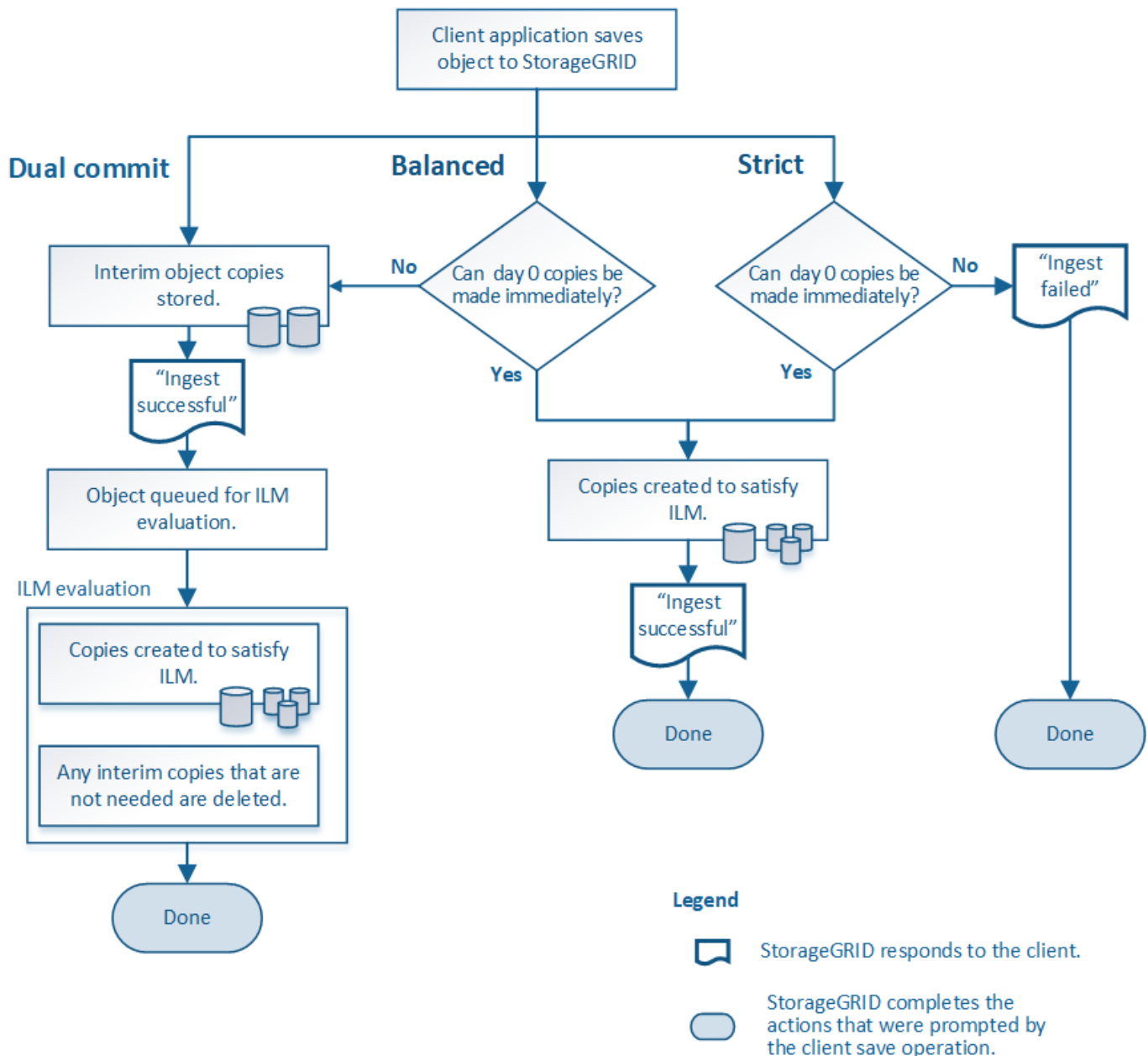
Wenn Sie die Option „Ausgleich“ auswählen, verwendet StorageGRID bei der Aufnahme auch die synchrone Platzierung und erstellt sofort alle Kopien, die in den Anweisungen zur Platzierung der Regel angegeben sind. Falls StorageGRID nicht sofort alle Kopien erstellen kann, verwendet er dagegen die doppelte Provisionierung.

Wann sollte die Option „Balance“ verwendet werden

Die ausgewogene Option erzielt die beste Kombination aus Datensicherung, Grid-Performance und Aufnahme-Erfolg. Balance ist die Standardoption im ILM-Regelassistenten.

Flussdiagramm mit drei Aufnahmeoptionen

Das Flussdiagramm zeigt, was passiert, wenn Objekte mit einer ILM-Regel abgeglichen werden, die eine dieser Aufnahmeoptionen verwendet.



Verwandte Informationen

["Aufnahme von Objekten"](#)

Vor- und Nachteile sowie Einschränkungen der Datensicherungsoptionen

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.

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 Option „Balanced“ wird empfohlen, es sei denn, es ist ein striktes Aufnahmeverhalten erforderlich oder das Grid erfüllt alle Kriterien für die Verwendung von Dual-Commit.
- **(strikt) 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 ausgeglichenen und strengen Optionen verwenden, wird eine „Aufnahme erfolgreich“-Meldung erst an den Client zurückgegeben, wenn alle mit Erasure Coding verschlüsselten Fragmente oder replizierte Kopien erstellt und gespeichert werden. Objektdaten werden allerdings sehr wahrscheinlich die endgültige Platzierung viel schneller erreichen.
- **(strenge) höhere Aufnahmeraten:** Bei der strikten Option schlägt die Aufnahme fehl, wenn StorageGRID nicht sofort alle Kopien erstellen kann, die in der ILM-Regel angegeben sind. 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 jedoch für jeden Teil des Objekts während der Aufnahme und für das Objekt als Ganzes bewertet, 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 werden alle Teile, die nicht korrekt platziert werden, zur ILM-Neubewertung in eine Warteschlange eingereiht und zu einem späteren Zeitpunkt an den richtigen Ort 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 Standorten gespeichert werden können, die die ILM-Anforderungen für das Objekt als Ganzes 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. Falls erforderliche Platzierungsänderungen nicht vorgenommen werden können (z. B. weil ein neu erforderlicher Standort nicht verfügbar ist), behält das aktualisierte Objekt seine aktuelle Platzierung vor, bis die Platzierungsänderungen möglich sind.

Einschränkungen bei der Platzierung von Objekten mit den ausgewogenen oder strengen Optionen

Die ausgewogenen oder strengen Optionen können nicht für ILM-Regeln verwendet werden, die eine der folgenden Anweisungen zur Platzierung haben:

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

Diese Einschränkungen sind vorhanden, da StorageGRID keine synchronen Kopien in einen Cloud-Speicherpool oder einen Archiv-Node erstellen kann und eine benutzerdefinierte Erstellungszeit auf die vorhandene auflösen kann.

Auswirkungen von ILM-Regeln und Konsistenzkontrollen auf die Datensicherung

Sowohl Ihre ILM-Regel als auch Ihre Wahl der Konsistenzkontrolle beeinflussen den Schutz von Objekten. Diese Einstellungen können interagieren.

Das für eine ILM-Regel ausgewählte Aufnahmeverhalten wirkt sich beispielsweise auf die anfängliche Platzierung von Objektkopien aus, während sich die beim Speichern eines Objekts verwendete Konsistenzkontrolle auf die anfängliche Platzierung von Objekt-Metadaten auswirkt. Da StorageGRID Zugriff auf die Metadaten eines Objekts und seine Daten benötigt, um Kundenanforderungen zu erfüllen, kann die Auswahl der passenden Sicherungsstufen für Konsistenz und Aufnahme-Verhalten eine bessere Erstsicherung und zuverlässigere Systemantworten ermöglichen.

Hier finden Sie eine kurze Zusammenfassung der in StorageGRID verfügbaren Konsistenzkontrollen:

- **Alle:** Alle Knoten erhalten sofort Objektmetadaten oder die Anfrage schlägt fehl.
- **Stark-global:** Objektmetadaten werden sofort auf alle Seiten 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:** Sorgt für die Konsistenz von Read-after-write für neue Objekte und eventuelle Konsistenz von Objekt-Updates. Hochverfügbarkeit und garantierte Datensicherung
- **Verfügbar** (eventuelle Konsistenz für KOPFOPERATIONEN): Verhält sich wie das "read-after-New-write" Konsistenzniveau, bietet aber nur eventuelle Konsistenz für DEN KOPFBETRIEB.



Lesen Sie vor Auswahl einer Konsistenzstufe die vollständige Beschreibung dieser Einstellungen in den Anweisungen zur Erstellung einer S3- oder Swift-Client-Applikation. Vor dem Ändern des Standardwerts sollten Sie die Vorteile und Einschränkungen kennen.

Beispiel für die Interaktion zwischen Konsistenzkontrolle und ILM-Regel

Angenommen, Sie haben ein Grid mit zwei Standorten mit der folgenden ILM-Regel und der folgenden Einstellung für die Konsistenzstufe:

- **ILM-Regel:** Erstellen Sie zwei Objektkopien, eine am lokalen Standort und eine an einem entfernten Standort. Das strikte Aufnahmeverhalten wird ausgewählt.
- **Konsistenzstufe:** "strong-global" (Objektmetadata werden sofort auf 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 Objektmetadata am Remote-Standort weiterhin. Das Objekt kann vollständig abgerufen werden.

Falls Sie stattdessen dieselbe ILM-Regel und die Konsistenzstufe „strong-Site“ verwendet haben, erhält der Client möglicherweise eine Erfolgsmeldung, nachdem die Objektdaten an den Remote Standort repliziert wurden, aber bevor die Objektmetadata dort verteilt werden. In diesem Fall entspricht die Sicherung von Objektmetadata nicht dem Schutzniveau für Objektdaten. Falls der lokale Standort kurz nach der Aufnahme verloren geht, gehen Objektmetadata verloren. Das Objekt kann nicht abgerufen werden.

Die Wechselbeziehung zwischen Konsistenzstufen und ILM-Regeln kann komplex sein. Wenden Sie sich an NetApp, wenn Sie Hilfe benötigen.

Verwandte Informationen

["Was ist Replizierung"](#)

["Verfahren zur Einhaltung von Datenkonsistenz \(Erasure Coding\)"](#)

["Was sind die Erasure Coding-Schemata"](#)

["Beispiel 5: ILM-Regeln und Richtlinie für striktes Ingest-Verhalten"](#)

["S3 verwenden"](#)

["Verwenden Sie Swift"](#)

Speicherung von Objekten (Replizierung oder Erasure Coding)

StorageGRID schützt Objekte vor Verlust, indem replizierte Kopien gespeichert oder nach dem Erasure Coding Kopien gespeichert werden. Sie geben den Typ der Kopien an, die in den Anweisungen zur Platzierung von ILM-Regeln erstellt werden sollen.

- ["Was ist Replizierung"](#)
- ["Warum sollten Sie keine Replizierung mit nur einer Kopie verwenden"](#)
- ["Verfahren zur Einhaltung von Datenkonsistenz \(Erasure Coding\)"](#)
- ["Was sind die Erasure Coding-Schemata"](#)
- ["Vor- und Nachteile sowie Anforderungen für Erasure Coding"](#)

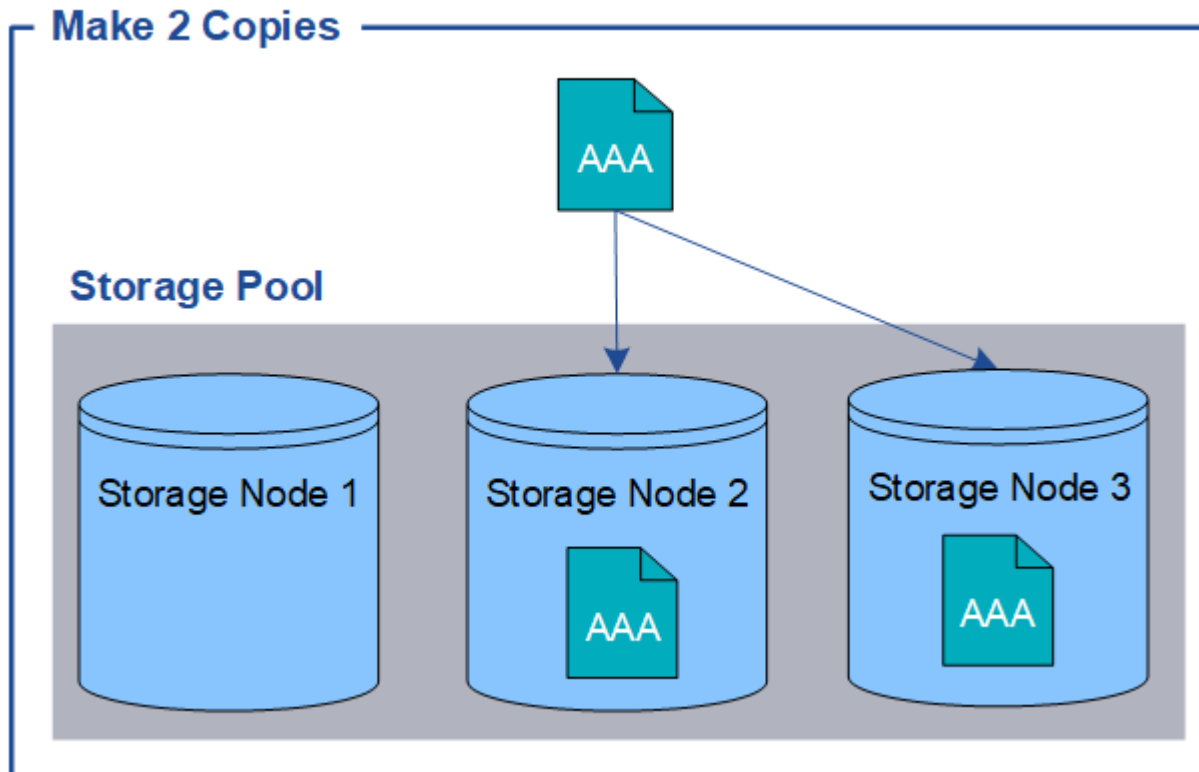
Was ist Replizierung

Die Replizierung ist eine von zwei Methoden, die von StorageGRID zum Speichern von Objektdaten verwendet werden. Wenn Objekte mit einer ILM-Regel übereinstimmen, die Replizierung verwendet, erstellt das System exakte Kopien von Objektdaten und

speichert die Kopien auf Storage-Nodes oder Archiv-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 ein Speicherpool"](#)

["Verwendung mehrerer Storage Pools zur standortübergreifenden Replizierung"](#)

Warum sollten Sie keine Replizierung mit nur einer Kopie verwenden

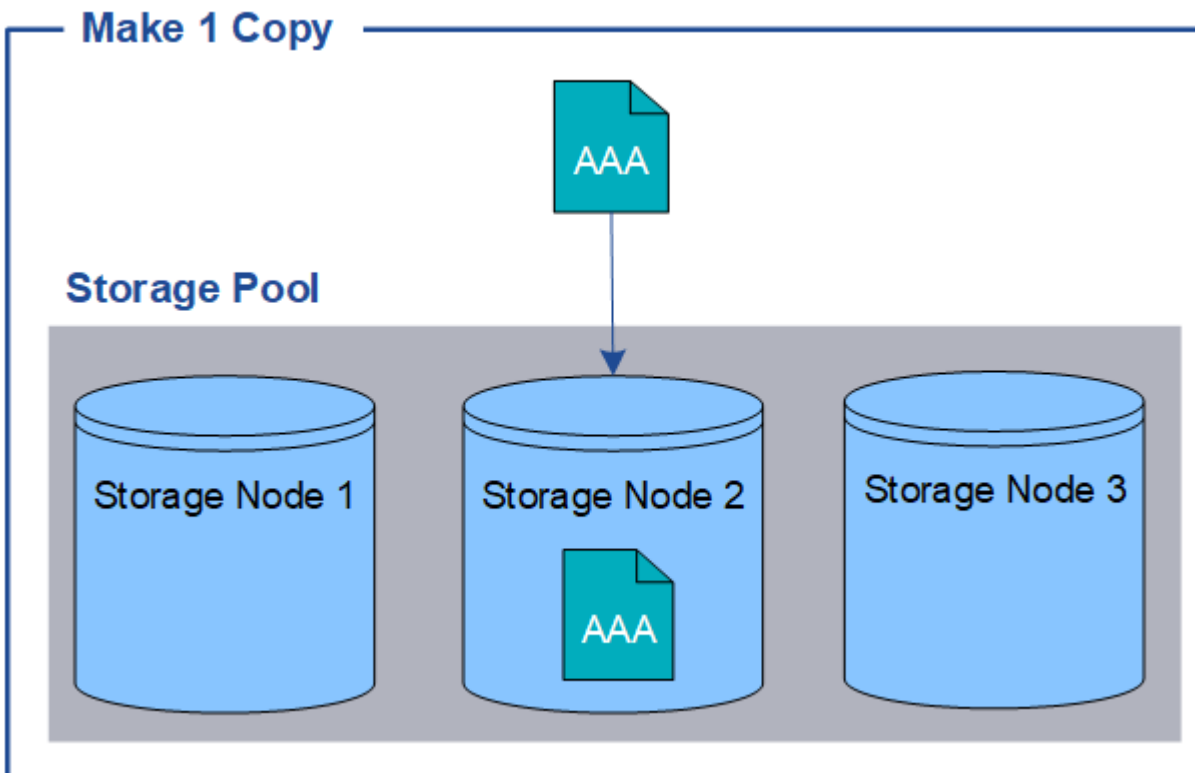
Beim Erstellen einer ILM-Regel zum Erstellen replizierter Kopien sollten Sie immer mindestens zwei Kopien für einen beliebigen Zeitraum in den Anweisungen zur

Platzierung angeben.



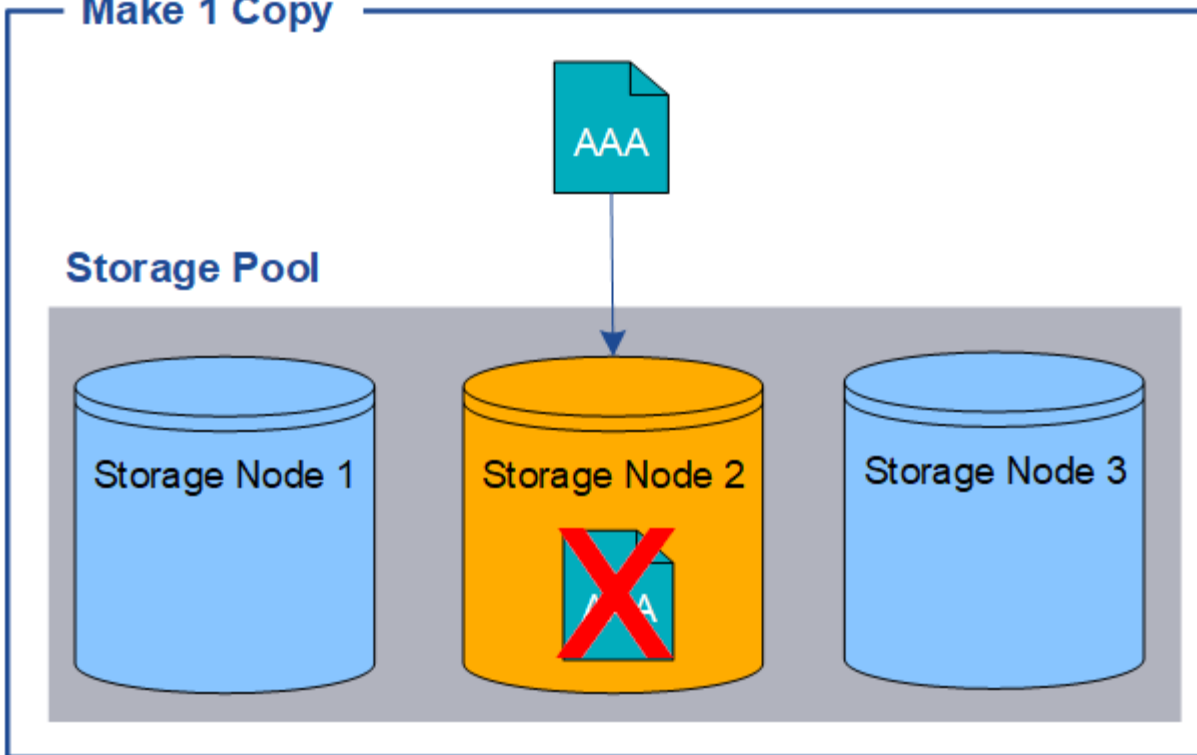
Verwenden Sie keine ILM-Regel, die immer nur eine replizierte Kopie erstellt. Wenn nur eine replizierte Kopie eines Objekts vorhanden ist, geht dieses Objekt verloren, wenn ein Speicherknoten ausfällt oder einen beträchtlichen Fehler hat. Während Wartungsarbeiten wie Upgrades verlieren Sie auch vorübergehend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

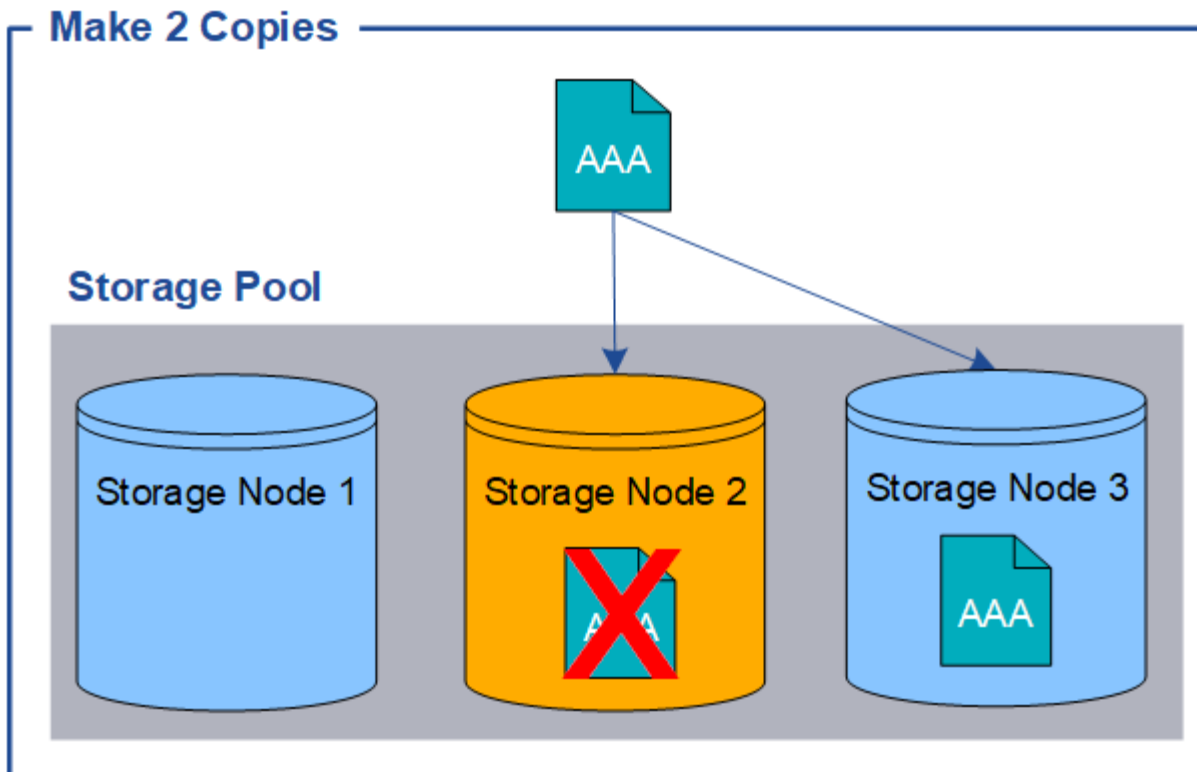


Wenn eine ILM-Regel nur eine replizierte Kopie eines Objekts erstellt, ist der Zugriff auf das Objekt möglich, wenn der Storage-Node nicht verfügbar ist. In diesem Beispiel verlieren Sie vorübergehend den Zugriff auf das Objekt AAA, wenn Storage Node 2 offline ist, z. B. während eines Upgrades oder eines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

Make 1 Copy



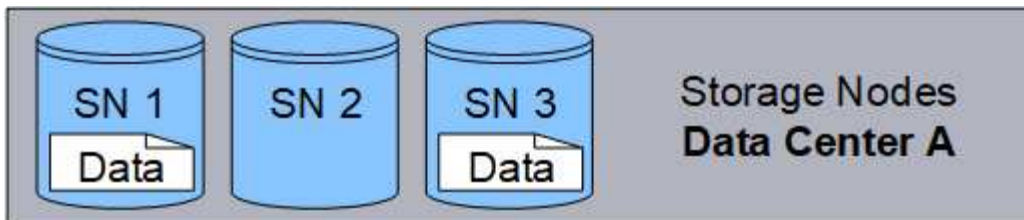
Um den Verlust von Objektdaten zu vermeiden, sollten immer mindestens zwei Kopien aller Objekte erstellt werden, die durch die Replizierung gesichert werden sollen. Wenn zwei oder mehr Kopien vorhanden sind, können Sie weiterhin auf das Objekt zugreifen, wenn ein Storage-Node ausfällt oder offline geht.



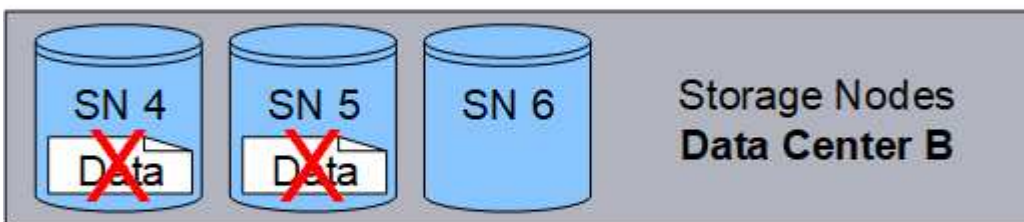
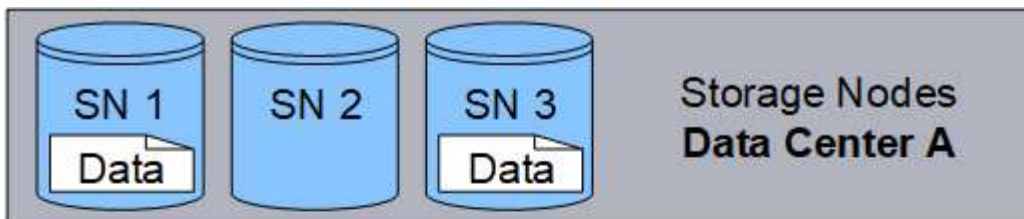
Verfahren zur Einhaltung von Datenkonsistenz (Erasure Coding)

Das Verfahren zur Einhaltung von Datenkonsistenz ist die zweite Methode, die von StorageGRID zum Speichern von Objektdaten verwendet wird. Wenn StorageGRID Objekte mit einer ILM-Regel übereinstimmt, die zur Erstellung von mit Datenkonsistenz versehenen Kopien konfiguriert ist, werden Objektdaten in Datenfragmente zerlegt, zusätzliche Paritätsfragmente berechnet und jedes Fragment 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.

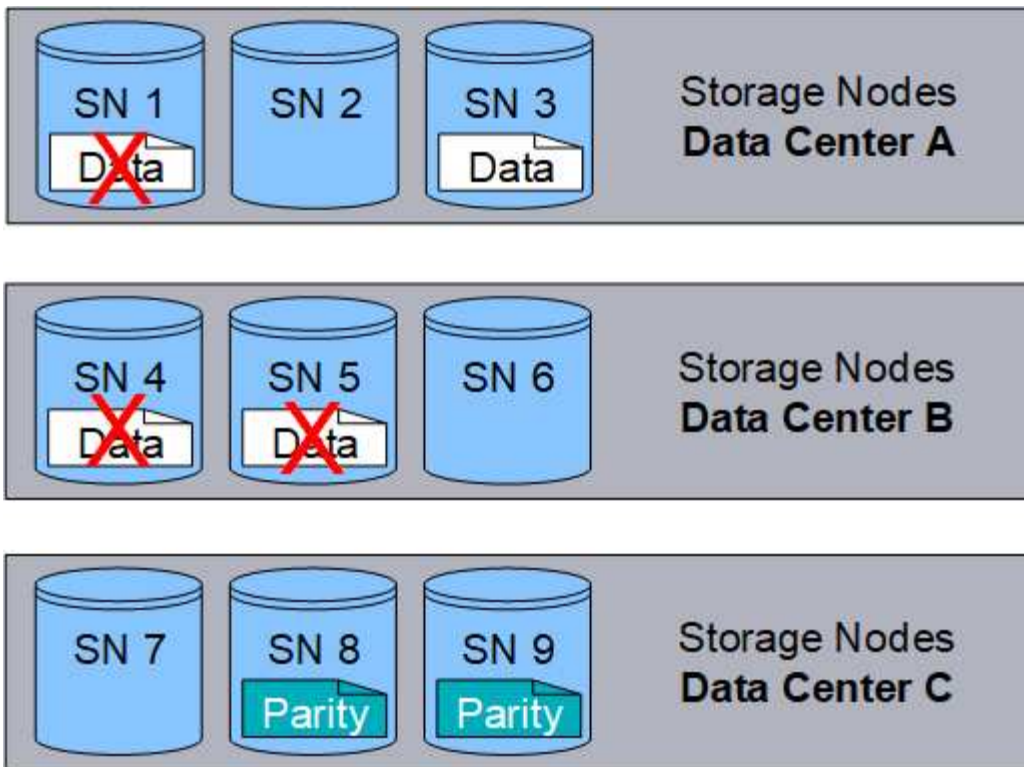
Im folgenden Beispiel wird der Algorithmus zur Einhaltung von Datenkonsistenz (Erasure Coding) für Objektdaten dargestellt. In diesem Beispiel verwendet die ILM-Regel ein 4+2-Schema zur Einhaltung von Datenkonsistenz. Jedes Objekt wird in vier gleiche Datenfragmente geteilt und aus den Objektdaten werden 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 Verfahren zur Einhaltung von Datenkonsistenz (Erasure Coding) in 4+2 erfordert mindestens neun Storage-Nodes mit drei Storage-Nodes an jedem der drei Standorte. 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. Bei einem Ausfall eines gesamten Datacenter-Standorts kann das Objekt weiterhin abgerufen oder repariert werden, solange alle anderen Fragmente verfügbar sind.



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



Verwandte Informationen

["Was ist ein Speicherpool"](#)

["Was sind die Erasure Coding-Schemata"](#)

["Konfigurieren von Erasure Coding-Profilen"](#)

Was sind die Erasure Coding-Schemata

Wenn Sie das Erasure Coding-Profil für eine ILM-Regel konfigurieren, wählen Sie ein verfügbares Codierungsschema zur Fehlerkorrektur aus, basierend darauf, wie viele Storage-Nodes und -Standorte den zu verwendenden Speicherpool bilden. Erasure Coding steuert die Anzahl von Datenfragmenten und die Anzahl der Parity-Fragmente für jedes Objekt.

Das StorageGRID-System verwendet den Reed-Solomon-Erasure-Coding-Algorithmus. Der Algorithmus schneidet ein Objekt in k Datenfragmente auf und berechnet m Paritätsfragmente. Die $k + m = n$ Fragmente sind auf n Speicherknoten verteilt, um die Datensicherung zu gewährleisten. Ein Objekt kann bis zu m verlorene oder beschädigte Fragmente erhalten. k Fragmente sind erforderlich, um ein Objekt abzurufen oder zu reparieren.

Verwenden Sie bei der Konfiguration eines Erasure Coding-Profiles die folgenden Richtlinien für Speicherpools:

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



Sie können kein Erasure Coding-Profil konfigurieren, wenn der Speicherpool 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 nicht den Standardspeicherpool, alle Speicherknoten oder einen Speicherpool, der den Standardstandort, Alle Standorte, enthält.
- Der Speicherpool sollte mindestens $k+m+1$ Storage-Nodes enthalten.

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

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

$$\text{disk space} = \text{object size} + (\text{object size} * \text{storage overhead})$$

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 von $k+m$ aus, das Ihren Anforderungen entspricht. Erasure Coding-Schemata mit einer geringeren Anzahl von Fragmenten werden insgesamt recheneffizienter, da weniger Fragmente pro Objekt erstellt und verteilt (oder abgerufen) werden. Je größer die Fragmentgröße ist, desto weniger Nodes können bei einer Erweiterung hinzugefügt werden, wenn mehr Storage benötigt wird. (Informationen zur Planung einer Speichererweiterung finden Sie in den Anweisungen zum erweitern von StorageGRID.)

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 Systeme bieten einen Schutz vor Schäden an den Standorten. Ein Standort kann verloren gehen, und das Objekt ist weiterhin verfügbar.

Für Erasure-Coding-Schemata, die Site-Loss-Schutz bieten, übersteigt die empfohlene Anzahl von Storage-Nodes im Speicherpool die Anzahl $k+m+1$, 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 % erzielt
6 + 2	4	3	12	Ja.	33 % erzielt
8 + 2	5	3	15	Ja.	25 % erzielt
6 + 3	3	4	12	Ja.	50 % erzielt
9 + 3	4	4	16	Ja.	33 % erzielt

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
2+1	3	3	9	Ja.	50 % erzielt
4+1	5	3	15	Ja.	25 % erzielt
6+1	7	3	21	Ja.	17 % erzielt
7 + 5	3	5	15	Ja.	71 % erzielt



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 Paritäts-Segmente erhöht (d. h. wenn m einen höheren Wert hat).
- **Netzverkehr:** Bei der Wiederherstellung nach Ausfällen erzeugt ein Schema mit mehr Fragmenten (das heißt, eine höhere 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 erforderliche Mindestanzahl an Storage-Nodes beträgt $k+m$, es wird jedoch 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 % erzielt
6 + 2	8	9	33 % erzielt
8 + 2	10	11	25 % erzielt
6 + 3	9	10	50 % erzielt
9 + 3	12	13	33 % erzielt
2+1	3	4	50 % erzielt
4+1	5	6	25 % erzielt
6+1	7	8	17 % erzielt
7 + 5	12	13	71 % erzielt

Verwandte Informationen

["Erweitern Sie Ihr Raster"](#)

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. Ein Objekt mit 10 MB, das an zwei Standorten repliziert wird, benötigt beispielsweise 20 MB Festplattenspeicher (zwei Kopien), während ein Objekt, das über drei Standorte mit einem Erasure Coding-Schema mit 6+3 codiert wird, nur 15 MB Festplattenspeicher in Anspruch nimmt.



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:

- Es ist eine größere Anzahl von Speicherknoten und Standorten erforderlich. Wenn Sie beispielsweise ein Erasure-Coding-Schema von 6+3 verwenden, müssen Sie mindestens drei Storage-Nodes an drei verschiedenen Standorten haben. Wenn Sie dagegen nur Objektdaten replizieren, benötigen Sie nur einen Storage Node für jede Kopie.
- Höhere Kosten und Komplexität der Storage-Erweiterungen. Um eine Implementierung mit Replizierung zu erweitern, fügen Sie einfach Storage-Kapazität an jedem Speicherort hinzu, an dem Objektkopien erstellt werden. 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 vorhandene Nodes zu 100 % voll sind, müssen Sie mindestens $k+m$ Storage-Nodes hinzufügen. Wenn jedoch vorhandene Nodes zu 70 % voll sind, können Sie zwei Nodes pro Standort hinzufügen und dennoch die nutzbare Storage-Kapazität maximieren. Weitere Informationen finden Sie in den Anweisungen zum Erweitern von StorageGRID.
- 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 und Verteilung auf Remote-Standorte codiert und über WAN-Verbindungen verteilt ist, dauern länger, bis es über ein Objekt abgerufen wird, das repliziert und lokal verfügbar ist (derselbe Standort, an 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.



Aufgrund des Overhead zum Managen der Anzahl von Fragmenten, die mit einer mit Erasure Coding verschlüsselten Kopie verbunden sind, sollten Sie für Objekte, die mindestens 200 KB groß sind, kein Erasure Coding verwenden.

- 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

Verwandte Informationen

["Erweitern Sie Ihr Raster"](#)

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 haben drei primäre Möglichkeiten, um zu steuern, wie lange ihre Objekte in StorageGRID gespeichert sind:

- 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 einer gesetzlichen Aufbewahrungspflicht befindet, kann nicht mit irgendeiner 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-Objektsperre werden durch ILM „Forever“ beibehalten. Nachdem jedoch eine Aufbewahrungsfrist erreicht ist, kann eine Objektversion durch eine Client-Anfrage oder den Ablauf des Bucket-Lebenszyklus gelöscht werden.

["Verwalten von Objekten 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.
- Ein S3- oder Swift-Client kann eine delete-Objektanforderung 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 steuern mithilfe von ILM-Speichieranweisungen, 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 unbefristet aufbewahrt, wenn „forever“ für die

Platzierungsanweisungen angegeben ist.

Unabhängig davon, wer die Aufbewahrung von Objekten steuert, steuern ILM-Einstellungen, welche Arten von Objektkopien (repliziert oder Erasure Coding) gespeichert werden und wo sich die Kopien befinden (Storage-Nodes, Cloud Storage Pools oder Archiv-Nodes).

Interaktion von S3-Bucket-Lebenszyklus und ILM

Die Aktion „Ablaufdatum“ in einem S3-Bucket-Lebenszyklus überschreibt immer die ILM-Einstellungen. 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

Speichern von zwei Kopien auf Storage-Nodes „Forever“

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

Speichern Sie zwei Kopien auf Storage-Nodes „Forever.“

Anforderung zum Löschen des Clients

Ausgestellt am 2024-03-31.

Ergebnis

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

Verwandte Informationen

["Verwalten von Objekten mit S3 Object Lock"](#)

["S3 verwenden"](#)

["Welche Anweisungen zur Platzierung der ILM-Regeln gibt es"](#)

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	<p>Wenn eine der folgenden Bedingungen zutrifft:</p> <ul style="list-style-type: none"> • Das automatische Löschen von Objekten wurde von einem der folgenden Ereignisse ausgelöst: <ul style="list-style-type: none"> ◦ 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. <p>Hinweis: Objekte in einem Bucket mit aktivierter S3-Objektsperre können nicht gelöscht werden, wenn sie sich unter einer gesetzlichen Sperre befinden oder wenn ein Aufbewahrungsdatum angegeben, aber noch nicht erfüllt wurde.</p> <ul style="list-style-type: none"> • Ein S3- oder Swift-Client fordert eine Löschung an. Eine oder mehrere der folgenden Bedingungen gilt: <ul style="list-style-type: none"> ◦ Kopien können nicht innerhalb von 30 Sekunden gelöscht werden, da z. B. ein Objektverzeichnis vorübergehend nicht verfügbar ist. ◦ Löschwarteschlangen im Hintergrund sind inaktiv.
Objekte werden sofort entfernt (synchrones Löschen)	<p>Wenn ein S3- oder Swift-Client eine Löschanfrage erstellt und alle der folgenden Bedingungen erfüllt sind:</p> <ul style="list-style-type: none"> • Alle Kopien können innerhalb von 30 Sekunden entfernt werden. • Warteschlangen zum Löschen im Hintergrund enthalten Objekte, die verarbeitet werden sollen.

Wenn S3- oder Swift-Clients Anforderungen löschen, beginnt StorageGRID mit dem Hinzufügen einer Reihe 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.

Allgemeines zum Löschen von Objekten in StorageGRID

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.
- Falls Sie die Löschrleistung während eines Massenlöschs genau überwachen, kann es vorkommen, dass sich die Löschrleistung nach dem Löschen einer bestimmten Anzahl von Objekten verlangsamt. Diese Änderung tritt auf, wenn StorageGRID von Objekten aus der Warteschlange zum Löschen auf das synchrone Löschen verschiebt. Die offensichtliche Reduzierung der Löschrleistung 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.

Beachten Sie, dass die zur Freigabe von Speicherplatz nach dem Löschen eines Objekts benötigte Zeit von mehreren Faktoren abhängt:

- 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 Clientlösungen 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 Anforderungen zum Löschen von Objekten nicht die aktuelle Version des Objekts und geben keinen freien Speicherplatz frei. Stattdessen erstellt eine Anforderung zum Löschen eines Objekts einfach eine Löschmarkierung als aktuelle Version des Objekts, wodurch die vorherige Version des Objekts „non-current.“

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 freien Speicherplatz zu erhalten, müssen Sie einen der folgenden Schritte ausführen:

- **S3-Clientanforderung:** Geben Sie die Objektversionsnummer in der S3-LÖSCHOBJEKTANFORDERUNG an (DELETE /object?versionId=ID). Beachten Sie, dass diese Anforderung nur Objektkopien für die angegebene Version entfernt (die anderen Versionen belegen noch Speicherplatz).
- **Bucket-Lebenszyklus:** Verwenden Sie das NoncurrentVersionExpiration Aktionen in der Bucket-Lifecycle-Konfiguration Wenn die angegebene Anzahl von nicht-currentDays erreicht ist, entfernt StorageGRID dauerhaft alle Kopien nicht aktueller Objektversionen. Diese Objektversionen können nicht wiederhergestellt werden.
- **ILM:** Fügen Sie zwei ILM-Regeln zu Ihrer ILM-Richtlinie hinzu. Verwenden Sie **nicht aktuelle Zeit** als Referenzzeit in der ersten Regel, um die nicht aktuellen Versionen des Objekts zu entsprechen. Verwenden Sie **Aufnahmezeit** in der zweiten Regel, um mit der aktuellen Version zu übereinstimmen. Die **nicht aktuelle Zeit**-Regel muss in der Regel über der **Aufnahmezeit**-Regel erscheinen.

Verwandte Informationen

["S3 verwenden"](#)

["Beispiel 4: ILM-Regeln und -Richtlinie für versionierte Objekte mit S3"](#)

Was ist eine ILM-Richtlinie

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.

Bewertung von Objekten durch eine ILM-Richtlinie

Die aktive ILM-Richtlinie für Ihr StorageGRID System steuert die Platzierung, Dauer und Datensicherung aller Objekte.

Wenn Clients Objekte in StorageGRID speichern, werden die Objekte anhand der bestellten ILM-Regeln in der aktiven Richtlinie 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 ausgewertet, bis eine Übereinstimmung erfolgt.
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 und kann keine Filter verwenden.

Beispiel für eine ILM-Richtlinie

In diesem Beispiel verwendet die ILM-Richtlinie drei ILM-Regeln.

Configure ILM Policy

Create a proposed policy by selecting and arranging rules. Then, save the policy and edit it later as required. Click Simulate to verify a saved policy using test objects. When you are ready, click Activate to make this policy the active ILM policy for the grid.

Name

Example ILM policy

Reason for change

New policy

Rules

1. Select the rules you want to add to the policy.

2. Determine the order in which the rules will be evaluated by dragging and dropping the rows. The default rule will be automatically placed at the end of the policy and cannot be moved.

+ Select Rules

	Default	Rule Name	Tenant Account	Actions
		Rule 1: 3 replicated copies for Tenant A	Tenant A (58889986524346589742)	
		Rule 2: Erasure coding for objects greater than 1 MB	—	
		Rule 3: 2 copies 2 data centers (default)	—	

Cancel

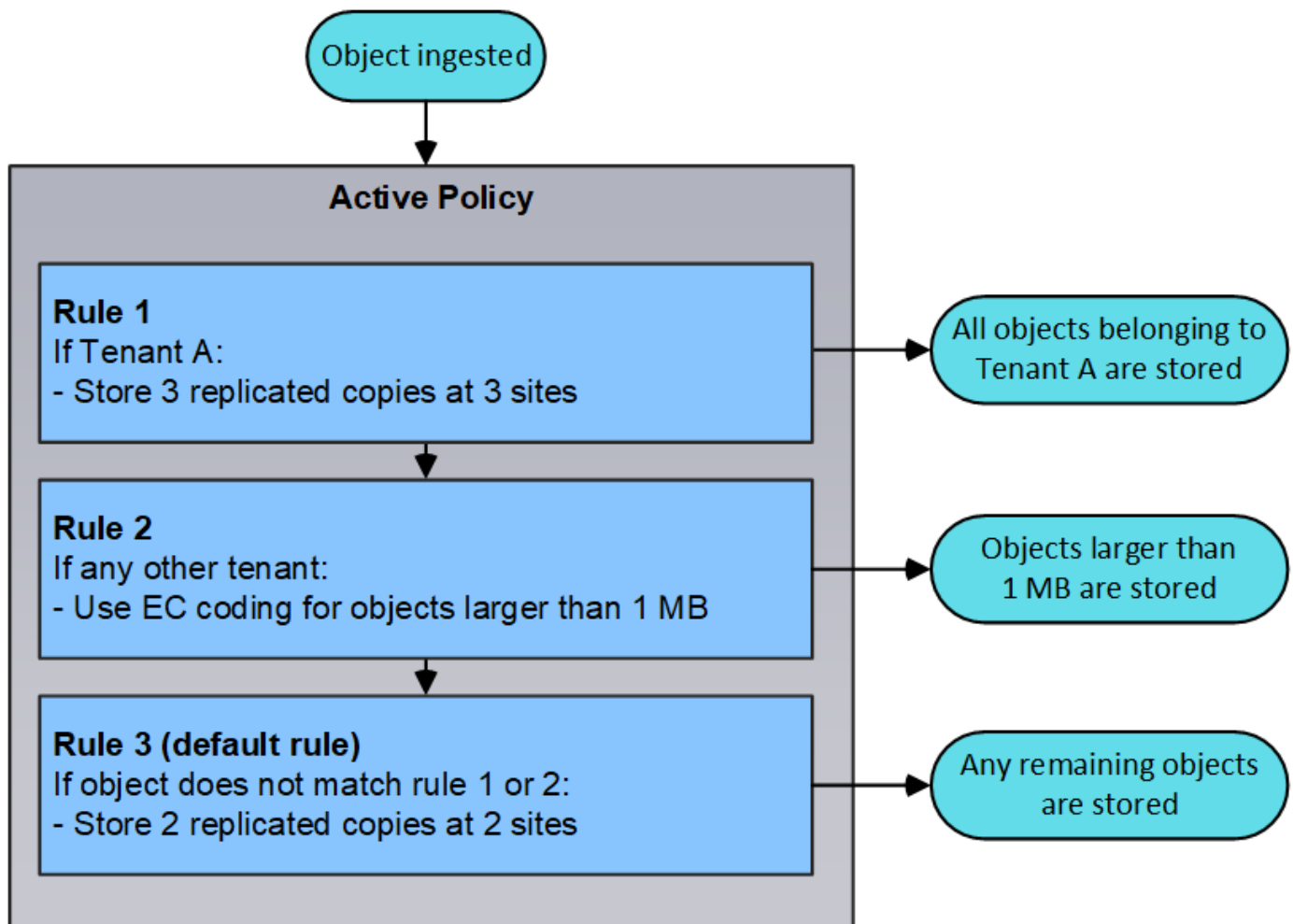
Save

In diesem Beispiel stimmt Regel 1 mit allen Objekten überein, die zu Mandant A gehören. Diese Objekte werden als drei replizierte Kopien an drei Standorten gespeichert. Objekte, die zu anderen Mietern gehören,

werden von Regel 1 nicht abgeglichen, so dass sie gegen Regel 2 ausgewertet werden.

Regel 2 entspricht allen Objekten anderer Mandanten, aber nur, wenn sie größer als 1 MB sind. Diese größeren Objekte werden mithilfe von 6+3 Erasure Coding an drei Standorten gespeichert. Regel 2 stimmt nicht mit Objekten 1 MB oder kleiner überein, daher werden diese Objekte gegen Regel 3 ausgewertet.

Regel 3 ist die letzte und Standardregel in der Richtlinie und verwendet keine Filter. Regel 3 erstellt zwei replizierte Kopien aller Objekte, die nicht mit Regel 1 oder Regel 2 übereinstimmt (Objekte, die nicht zu Mandant A gehören, die 1 MB oder kleiner sind).



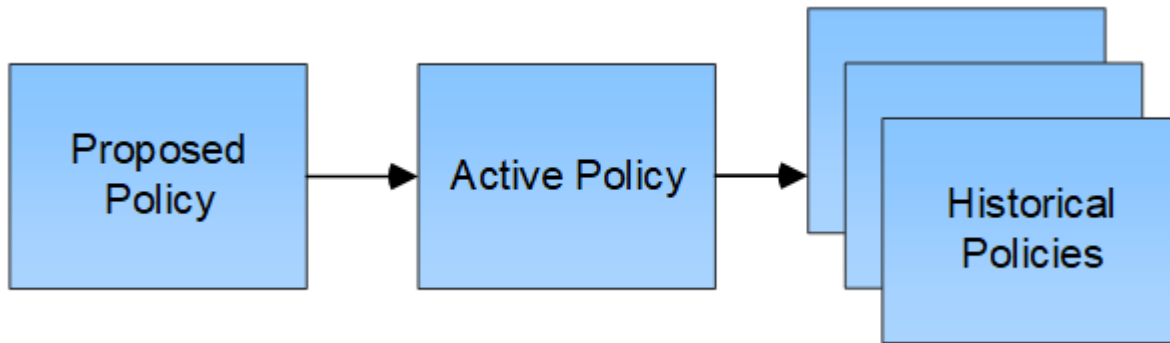
Welche vorgeschlagenen, aktiven und historischen Politiken sind

Jedes StorageGRID System muss über eine aktive ILM-Richtlinie verfügen. Ein StorageGRID System kann auch über eine vorgeschlagene ILM-Richtlinie und eine beliebige Anzahl an historischen Richtlinien verfügen.

Beim ersten Erstellen einer ILM-Richtlinie erstellen Sie eine vorgeschlagene Richtlinie, indem Sie eine oder mehrere ILM-Regeln auswählen und in einer bestimmten Reihenfolge anordnen. Nachdem Sie die vorgeschlagene Richtlinie simuliert haben, um ihr Verhalten zu bestätigen, aktivieren Sie sie, um die aktive Richtlinie zu erstellen.

Bei der Aktivierung einer neuen ILM-Richtlinie verwendet StorageGRID diese Richtlinie, um alle Objekte, einschließlich vorhandener Objekte und neu aufgenommener Objekte, zu managen. Vorhandene Objekte können an neue Standorte verschoben werden, wenn die ILM-Regeln der neuen Richtlinie implementiert werden.

Die Aktivierung der vorgeschlagenen Richtlinie führt dazu, dass die zuvor aktive Richtlinie zu einer historischen Politik wird. Historische ILM-Richtlinien können nicht gelöscht werden.



Verwandte Informationen

["ILM-Richtlinie erstellen"](#)

Was ist eine ILM-Regel

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 den Metadaten eines Objekts entspricht, legen die Anweisungen in der Regel fest, welche Aktionen StorageGRID zum Kopieren und Speichern des Objekts ergreift.

ILM-Regeln definieren:

- Welche Objekte sollten gespeichert werden. Eine Regel kann auf alle Objekte angewendet werden, oder Sie können Filter angeben, um zu identifizieren, für welche Objekte eine Regel gilt. Beispielsweise kann eine Regel nur für Objekte gelten, die mit bestimmten Mandantenkonten, bestimmten S3-Buckets oder Swift-Containern oder bestimmten Metadatenwerten verbunden sind.
- Speichertyp und -Standort. Objekte können auf Storage-Nodes, in Cloud-Storage-Pools oder auf Archiv-Nodes gespeichert werden.
- Der Typ der Objektkopien, die erstellt wurden. Kopien können repliziert oder Erasure Coding ausgeführt werden.
- Für replizierte Kopien die Anzahl der Kopien, die erstellt werden.
- Für Kopien mit Verfahren zur Einhaltung von Datenkonsistenz (Erasure Coding) wurde das Verfahren zur Einhaltung von Datenkonsistenz verwendet.
- Die Änderungen im Laufe der Zeit an dem Storage-Standort und den Kopprottypen eines Objekts.
- Schutz von Objektdaten bei Aufnahme von Objekten in das Grid (synchrone Platzierung oder Dual-Commit)

Objekt-Metadaten 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. Die Kopien werden gleichmäßig auf alle Storage Nodes verteilt.

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.
- **Aufnahmeverhalten:** Das Aufnahmeverhalten einer Regel definiert, was passiert, wenn ein S3- oder Swift-Client ein Objekt im Grid speichert. 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.

Beispiel für eine ILM-Regel

Diese Beispiel-ILM-Regel gilt für die Objekte, die zu Mandant A gehören. Es erstellt zwei replizierte Kopien dieser Objekte und speichert jede Kopie an einem anderen Standort. Die beiden Kopien werden „forever,“ aufbewahrt. Das bedeutet, dass StorageGRID sie nicht automatisch löscht. Stattdessen behält StorageGRID diese Objekte so lange bei, bis sie von einer Löschanfrage eines Clients oder nach Ablauf eines Bucket-Lebenszyklus gelöscht werden.

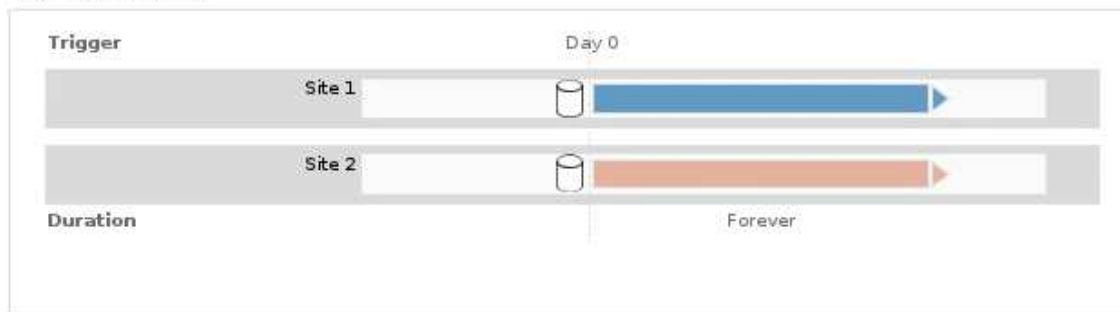
Diese Regel verwendet die ausgewogene Option für das Aufnahmeverhalten: Die Anweisung zur Platzierung an zwei Standorten wird angewendet, sobald Mandant A ein Objekt in StorageGRID speichert, es sei denn, es ist nicht möglich, sofort beide erforderlichen Kopien zu erstellen. Wenn z. B. Standort 2 nicht 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.

Two copies at two sites for Tenant A

Description: Applies only to Tenant A
Ingest Behavior: Balanced
Tenant Accounts: Tenant A (34176783492629515782)
Reference Time: Ingest Time
Filtering Criteria:

Matches all objects.

Retention Diagram:



Verwandte Informationen

["Datensicherungsoptionen für die Aufnahme"](#)

["Was ist ein Speicherpool"](#)

["Was ist ein Cloud-Storage-Pool"](#)

["Speicherung von Objekten \(Replizierung oder Erasure Coding\)"](#)

["Was ist die ILM-Regelfilterung"](#)

["Welche Anweisungen zur Platzierung der ILM-Regeln gibt es"](#)

Was ist die 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 handeln. Die Standardregel enthält Speicheranweisungen für Objekte, die nicht mit den Filtern in einer anderen Regel übereinstimmen.

Grundlegende Filter ermöglichen es Ihnen, unterschiedliche Regeln auf große, unterschiedliche Objektgruppen anzuwenden. Mit den grundlegenden Filtern auf der Seite „Grundlagen definieren“ des Assistenten zur Erstellung von ILM-Regeln können Sie eine Regel auf spezifische Mandantenkonten, bestimmte S3-Buckets

oder Swift-Container oder beides anwenden.

Create ILM Rule Step 1 of 3: Define Basics

Name

Description

Tenant Accounts (optional)

Select tenant accounts or enter tenant IDs

Bucket Name

matches all

Value

[Advanced filtering...](#) (0 defined)

Cancel

Next

Diese Grundfilter bieten 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.

Die Seite **Advanced Filtering** des Create ILM Rule Wizard gibt Ihnen granulare Kontrolle. Sie können Filter erstellen, um Objekte anhand der folgenden Objekteigenschaften auszuwählen:

- Aufnahmezeit
- Zeitpunkt des letzten Zugriffs
- Der Objektname (Schlüssel) ganz oder teilweise
- S3-Bucket-Region (Speicherortbeschränkung)
- Objektgröße
- Benutzer-Metadaten
- S3-Objekt-Tags

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 auch einfache und erweiterte 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 erweiterte Filter verwenden, um den spezifischen Objekttyp zu identifizieren, für den die Regel gilt.

Welche Anweisungen zur Platzierung der ILM-Regeln gibt es

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.

Beim Erstellen einer Speicheranweisung geben Sie an, wann die Platzierung zutrifft (der Zeitraum), welche Art von Kopien erstellt werden sollen (repliziert oder Erasure Coding) und wo die Kopien gespeichert werden (ein oder mehrere Speicherorte). Innerhalb einer einzigen Regel können Sie mehrere Platzierungen für einen Zeitraum festlegen und Anweisungen zur Platzierung für mehr als einen Zeitraum:

- Klicken Sie auf das Pluszeichen-Symbol, um mehr als eine Objektplatzierung während eines einzelnen Zeitraums festzulegen **+** Hinzufügen von mehr als einer Zeile für diesen Zeitraum.
- Wenn Sie für mehr als einen Zeitraum Objektplatzierungen angeben möchten, klicken Sie auf die Schaltfläche **Hinzufügen**, um den nächsten Zeitraum hinzuzufügen. Geben Sie dann eine oder mehrere Zeilen innerhalb des Zeitraums an.

Das Beispiel zeigt die Seite Platzierungen definieren im Assistenten „ILM-Regel erstellen“.

Placements Sort by start day

From day store for days Add Remove

Type Location Copies + x

Specifying multiple storage pools might cause data to be stored at the same site if the pools overlap. See [Managing objects with information lifecycle management](#) for more information.

Type Location Copies 1 + x

From day store Add Remove

Type Location Copies Temporary location 2 + x

1	Die erste Einstufungsanweisung hat zwei Linien für das erste Jahr: 1. In der ersten Zeile werden zwei replizierte Objektkopien an zwei Datacenter-Standorten erstellt. 2. Die zweite Zeile erstellt eine Kopie mit 6 und 3 zur Fehlerkorrektur codierten Kopien unter Verwendung von drei Datacenter-Standorten.
2	Die zweite Anleitung zur Platzierung erstellt zwei archivierte 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.

Erstellung von Speicherklassen, Speicherpools, EC-Profilen und Regionen

Bevor Sie die ILM-Regeln für Ihr StorageGRID System erstellen können, müssen Sie Objekt-Storage-Standorte definieren, die gewünschten Kopftypen festlegen und optional S3-Bereiche konfigurieren.

- ["Speicherklassen werden erstellt und zugewiesen"](#)
- ["Konfigurieren von Speicherpools"](#)
- ["Verwendung Von Cloud Storage Pools"](#)
- ["Konfigurieren von Erasure Coding-Profilen"](#)
- ["Regionen konfigurieren \(nur optional und S3\)"](#)

Speicherklassen werden erstellt und zugewiesen

Speicherklassen identifizieren den Speichertyp, der von einem Speicherknoten verwendet wird. Sie können Storage-Klassen erstellen, wenn ILM-Regeln bestimmte Objekte auf bestimmten Storage-Nodes anstatt auf allen Nodes am Standort platzieren sollen. Möglicherweise möchten Sie beispielsweise bestimmte Objekte auf Ihren schnellsten Storage-Nodes wie z. B. StorageGRID All-Flash Storage Appliances speichern.

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.
- Sie müssen über spezifische Zugriffsberechtigungen verfügen.

Über diese Aufgabe

Wenn Sie mehr als einen Storage-Typ verwenden, können Sie optional eine Storage-Klasse erstellen, um jeden Typ zu identifizieren. Beim Erstellen von Speicherklassen können Sie bei der Konfiguration von Speicherpools einen bestimmten Typ von Speicherknoten auswählen.

Wenn die Speicherklasse kein Problem ist (beispielsweise sind alle Speicherknoten identisch), können Sie dieses Verfahren überspringen und bei der Konfiguration von Speicherpools die Standardspeicherklasse Alle Speicherknoten verwenden.

Wenn Sie in einer Erweiterung einen neuen Storage-Node hinzufügen, wird dieser Node zur Standardspeicherklasse Alle Storage-Nodes hinzugefügt. Das Ergebnis:

- Wenn eine ILM-Regel einen Storage-Pool mit der Klasse „Alle Storage-Nodes“ verwendet, kann der neue Node unmittelbar nach Abschluss der Erweiterung verwendet werden.
- Wenn eine ILM-Regel einen Storage-Pool mit einer benutzerdefinierten Storage-Klasse verwendet, wird der neue Node erst verwendet, nachdem Sie den Node wie unten beschrieben manuell die benutzerdefinierte Storage-Klasse zugewiesen haben.




Beim Erstellen von Lagergütern nicht mehr als erforderlich Speicherklassen erstellen. Erstellen Sie beispielsweise nicht für jeden Storage-Node eine Storage-Klasse. 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.

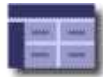
Schritte

1. Wählen Sie **ILM > Storage-Klasse** aus.

2. Speicherklasse erstellen:

- a. Klicken Sie für jede Speicherklasse, die Sie definieren möchten, auf **Einfügen**  Um eine Zeile hinzuzufügen und eine Bezeichnung für die Speicherklasse einzugeben.


Die Standard-Speicherstufe kann nicht geändert werden. Es ist für neue, während einer StorageGRID Systemerweiterung hinzugefügte Storage Nodes reserviert.












Storage Grades


Updated: 2017-05-26 11:22:39 MDT


Storage Grade Definitions

Storage Grade	Label	Actions
0	Default	
1	<input type="text" value="disk"/>	 

Storage Grades

LDR	Storage Grade	Actions
Data Center 1/DC1-S1/LDR	Default	
Data Center 1/DC1-S2/LDR	Default	
Data Center 1/DC1-S3/LDR	Default	
Data Center 2/DC2-S1/LDR	Default	
Data Center 2/DC2-S2/LDR	Default	
Data Center 2/DC2-S3/LDR	Default	
Data Center 3/DC3-S1/LDR	Default	
Data Center 3/DC3-S2/LDR	Default	
Data Center 3/DC3-S3/LDR	Default	

Apply Changes 

- a. Klicken Sie zum Bearbeiten einer vorhandenen Speicherklasse auf **Bearbeiten**  Und ändern Sie die Beschriftung nach Bedarf.




Speicherklassen können nicht gelöscht werden.

- b. Klicken Sie Auf **Änderungen Übernehmen**.










Diese Speicherklassen sind jetzt für die Zuordnung zu Speicherknoten verfügbar.

3. Weisen Sie einem Storage-Node eine Storage-Klasse zu:

- a. Klicken Sie für den LDR-Service jedes Speicherknotens auf **Bearbeiten**  Und wählen Sie eine

Speicherklasse aus der Liste aus.

Storage Grades

LDR	Storage Grade	Actions
Data Center 1/DC1-S1/LDR	Default	
Data Center 1/DC1-S2/LDR	Default disk	
Data Center 1/DC1-S3/LDR	Default	
Data Center 2/DC2-S1/LDR	Default	
Data Center 2/DC2-S2/LDR	Default	
Data Center 2/DC2-S3/LDR	Default	
Data Center 3/DC3-S1/LDR	Default	
Data Center 3/DC3-S2/LDR	Default	
Data Center 3/DC3-S3/LDR	Default	

Apply Changes 



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, wenn die ILM-Richtlinie aktiviert ist. Wenn die Zuweisung geändert wird, werden die Daten auf Basis der neuen Speicherklasse gespeichert.

a. Klicken Sie Auf **Änderungen Übernehmen**.

Konfigurieren von Speicherpools

Wenn Sie eine ILM-Regel definieren, verwenden Sie Speicherpools, um anzugeben, wo Objekte gespeichert werden. Bevor Sie einen Speicherpool erstellen, müssen Sie die Richtlinien für den Speicherpool überprüfen.

- ["Was ist ein Speicherpool"](#)
- ["Richtlinien zur Erstellung von Speicherpools"](#)
- ["Verwendung mehrerer Storage Pools zur standortübergreifenden Replizierung"](#)
- ["Verwenden eines Speicherpools als temporärer Speicherort \(veraltet\)"](#)
- ["Erstellen eines Speicherpools"](#)
- ["Anzeigen von Details zum Speicherpool"](#)
- ["Bearbeiten eines Speicherpools"](#)
- ["Entfernen eines Speicherpools"](#)

Was ist ein Speicherpool

Ein Speicherpool ist eine logische Gruppierung von Storage-Nodes oder Archiv-Nodes. Sie konfigurieren Speicherpools, um zu bestimmen, wo das StorageGRID-System

Objektdaten und den verwendeten Storage-Typ speichert.

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. Wenn Sie ILM-Regeln für die Replikation konfigurieren, wählen Sie einen oder mehrere Storage-Pools aus, die entweder Storage-Nodes oder Archiv-Nodes enthalten. Wenn Sie Erasure Coding-Profil erstellen, wählen Sie einen Speicherpool aus, der Storage-Nodes enthält.

Richtlinien zur Erstellung von Speicherpools

Befolgen Sie bei der Konfiguration und Verwendung von Speicherpools die folgenden Richtlinien.

Richtlinien für alle Speicherpools

- StorageGRID enthält einen Standard-Speicherpool, alle Storage-Nodes, der den Standardstandort, Alle Standorte und die Standard-Storage-Klasse, alle Storage-Nodes verwendet. Der Speicherpool Alle Storage-Nodes wird automatisch aktualisiert, wenn Sie neue Datacenter-Standorte hinzufügen.



Es wird nicht empfohlen, den Speicherpool für alle Storage-Nodes oder den Standort Alle Standorte zu verwenden, da diese Elemente automatisch aktualisiert werden, um neue Sites, die Sie in eine Erweiterung einfügen, einzubeziehen. Dies ist möglicherweise nicht das gewünschte Verhalten. Bevor Sie den Storage-Pool aller Storage-Nodes oder den Standardstandort verwenden, prüfen Sie sorgfältig die Richtlinien für replizierte und mit Erasure Coding gekennzeichnete Kopien.

- Halten Sie Storage-Pool-Konfigurationen so einfach wie möglich. Erstellen Sie nicht mehr Storage Pools 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.

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

- Erstellen Sie für jeden Standort einen anderen Speicherpool. Geben Sie dann in den Anweisungen zur Platzierung für jede Regel einen oder mehrere standortspezifische Speicherpools an. 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 für den neuen Standort. Aktualisieren Sie dann ILM-Regeln, um zu steuern, welche Objekte auf der neuen Site gespeichert werden.
- Verwenden Sie im Allgemeinen nicht den Standard-Speicherpool, alle Speicherknoten oder einen beliebigen Speicherpool, der den Standardstandort, Alle Standorte enthält.

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

- Sie können Archiv-Knoten nicht zum Löschen codierter Daten verwenden.
- Die Anzahl der im Storage-Pool enthaltenen Storage-Nodes und -Standorte bestimmen, welche Erasure Coding-Schemata zur Verfügung stehen.
- Wenn ein Speicherpool nur zwei Standorte umfasst, können Sie diesen Speicherpool nicht für Erasure Coding verwenden. Für einen Speicherpool mit zwei Standorten stehen keine Erasure Coding-Schemata zur Verfügung.
- Verwenden Sie im Allgemeinen nicht den Standardspeicherpool, alle Speicherknoten oder einen beliebigen Speicherpool, der den Standardstandort, Alle Standorte in einem beliebigen Erasure-Coding-Profil enthält.



Wenn in Ihrem Grid nur ein Standort enthalten ist, können Sie den Speicherpool „Alle Speicherknoten“ oder den Standardstandort „Alle Standorte“ in einem Erasure-Coding-Profil nicht verwenden. Dieses Verhalten verhindert, dass das Erasure Coding-Profil ungültig wird, wenn ein zweiter Standort hinzugefügt wird.

- Bei hohen Durchsatzanforderungen wird die Erstellung eines Storage-Pools mit mehreren Standorten nicht empfohlen, wenn die Netzwerklatenz zwischen Standorten größer als 100 ms ist. Mit steigender Latenz sinkt auch die Rate, mit der StorageGRID Objektfragmente erstellen, platzieren und abrufen kann, aufgrund des geringeren TCP-Netzwerkdurchsatzes erheblich. Die Abnahme des Durchsatzes wirkt sich auf die maximal erreichbaren Raten für Objekteinspeisung und -Abruf aus (wenn strenge oder ausgewogene als Aufnahmeverhalten ausgewählt werden) oder kann zu Backlogs in der ILM-Warteschlange führen (wenn Dual-Commit als Aufnahmeverhalten ausgewählt wird).
- 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.

Richtlinien für Speicherpools, die für archivierte Kopien verwendet werden

- Es kann kein Speicherpool erstellt werden, der sowohl Speicherknoten als auch Archivknoten enthält. Für archivierte Kopien ist ein Storage-Pool erforderlich, der nur Archiv-Nodes enthält.
- Wenn Sie einen Speicherpool verwenden, der Archivierungs-Nodes enthält, sollten Sie außerdem mindestens eine replizierte oder mit Erasure Coding versehende Kopie in einem Speicherpool mit Storage-Nodes verwalten.
- Wenn die globale S3-Objektsperre aktiviert ist und Sie eine konforme ILM-Regel erstellen, können Sie keinen Speicherpool verwenden, der auch Archiv-Nodes enthält. Anweisungen zum Verwalten von Objekten mit S3 Object Lock finden Sie in den Anleitungen.
- Wenn der Zieltyp eines Archiv-Node Cloud Tiering - Simple Storage Service (S3) lautet, muss sich der Archiv-Node im eigenen Storage-Pool befinden. Lesen Sie die Anweisungen zum Verwalten von StorageGRID.

Verwandte Informationen

["Was ist Replizierung"](#)

["Verfahren zur Einhaltung von Datenkonsistenz \(Erasure Coding\)"](#)

"Was sind die Erasure Coding-Schemata"

"Verwendung mehrerer Storage Pools zur standortübergreifenden Replizierung"

"Verwenden eines Speicherpools als temporärer Speicherort (veraltet)"

"Verwalten von Objekten mit S3 Object Lock"

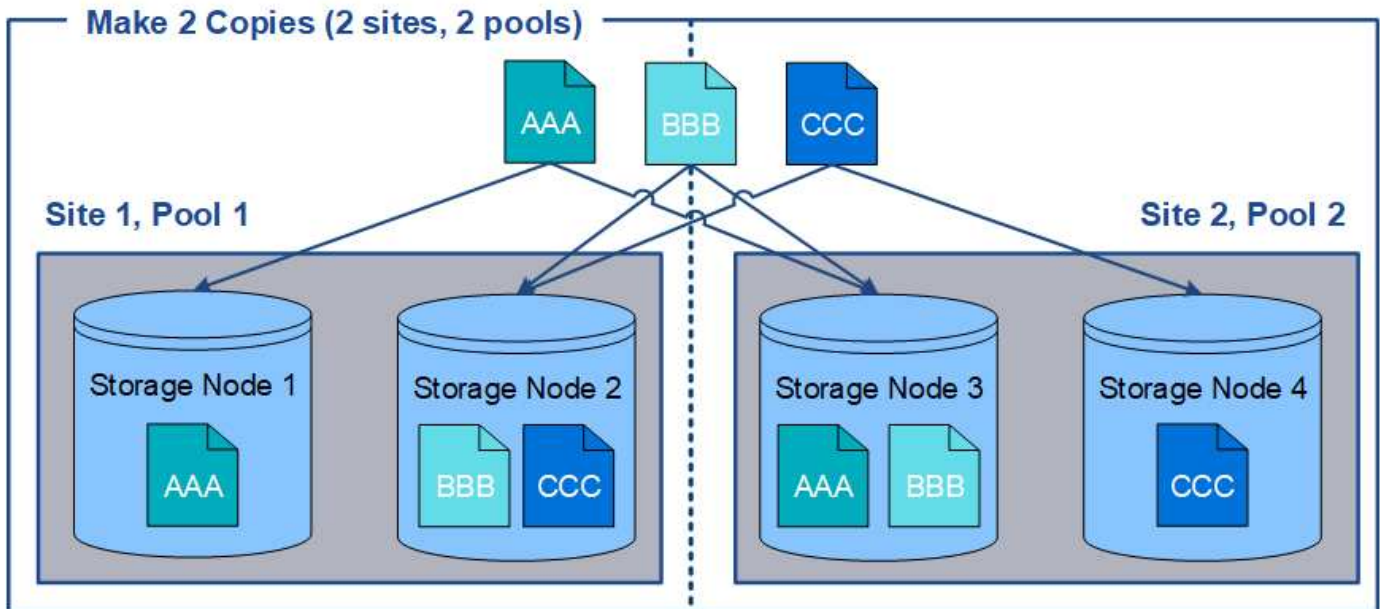
"StorageGRID verwalten"

Verwendung mehrerer Storage Pools zur standortübergreifenden Replizierung

Wenn Ihre StorageGRID-Implementierung mehr als einen Standort umfasst, können Sie den Site-Loss-Schutz durch die Erstellung eines Storage-Pools für jeden Standort aktivieren und in den Anweisungen zur Platzierung der Regeln beide Storage Pools angeben. Wenn Sie beispielsweise eine ILM-Regel konfigurieren, um zwei replizierte Kopien zu erstellen und Storage-Pools an zwei Standorten festzulegen, wird an jedem Standort eine Kopie jedes Objekts erstellt. Wenn Sie eine Regel für die Erstellung von zwei Kopien konfigurieren und drei Speicherpools festlegen, werden die Kopien verteilt, um die Festplattennutzung in den Speicherpools auszugleichen, während gleichzeitig sichergestellt wird, dass die beiden Kopien an unterschiedlichen Standorten gespeichert werden.

Das folgende Beispiel zeigt, was passieren kann, wenn eine ILM-Regel replizierte Objektkopien in einen einzelnen Storage-Pool mit Storage Nodes von zwei Standorten platziert. Da das System alle verfügbaren Nodes im Storage-Pool zum Speichern der replizierten Kopien verwendet, kann es alle Kopien von einigen Objekten innerhalb eines der Standorte platzieren. In diesem Beispiel speicherte das System zwei Kopien von Objekt AAA auf Storage Nodes an Standort 1 und zwei Kopien von Objekt CCC auf Storage Nodes an Standort 2. Nur Objekt BBB ist geschützt, wenn eine der Standorte ausfällt oder nicht mehr zugänglich ist.

Im Gegensatz dazu zeigt dieses Beispiel, wie Objekte gespeichert werden, wenn Sie mehrere Speicherpools verwenden. Im Beispiel gibt die ILM-Regel an, dass zwei replizierte Kopien jedes Objekts erstellt und die Kopien auf zwei Storage-Pools verteilt werden. Jeder Speicherpool enthält alle Storage-Nodes an einem Standort. Da an jedem Standort eine Kopie jedes Objekts gespeichert wird, werden Objektdaten gegen Standortausfall oder Nichtverfügbarkeit geschützt.



Beachten Sie bei der Verwendung mehrerer Speicherpools die folgenden Regeln:

- Wenn Sie n Kopien erstellen, müssen Sie n oder mehr Speicherpools hinzufügen. Wenn eine Regel beispielsweise für die Erstellung von drei Kopien konfiguriert ist, müssen Sie drei oder mehr Speicherpools angeben.
- 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 kleiner als die Anzahl der Storage-Pools ist, verteilt das System die Kopien, um die Festplattennutzung auf den ausgeglichenen Pools zu halten, und um sicherzustellen, dass mindestens zwei Kopien nicht im selben Storage-Pool gespeichert werden.
- 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 die gleichen Speicherknoten enthalten.

Verwenden eines Speicherpools als temporärer Speicherort (veraltet)

Wenn Sie eine ILM-Regel mit einer Objektplatzierung erstellen, die einen einzelnen Storage-Pool umfasst, werden Sie aufgefordert, einen zweiten Storage-Pool anzugeben, der als temporärer Speicherort verwendet werden soll.

Temporäre Speicherorte wurden veraltet und werden in einer zukünftigen Version entfernt. Sie sollten einen Speicherpool nicht als temporären Speicherort für eine neue ILM-Regel auswählen.



Wenn Sie das strikte Aufnahmeverhalten auswählen (Schritt 3 des Assistenten zur Erstellung von ILM-Regeln), wird der temporäre Speicherort ignoriert.

Verwandte Informationen

["Datensicherungsoptionen für die Aufnahme"](#)

Erstellen eines Speicherpools

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.

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.
- Sie müssen über spezifische Zugriffsberechtigungen verfügen.
- Sie müssen die Richtlinien zum Erstellen von Speicherpools überprüft haben.

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. Wählen Sie das Plus-Symbol **+**. So fügen Sie für jede Site einen Eintrag hinzu:



Schließen Sie den standardmäßigen Standort „Alle Standorte“ nicht in einen Speicherpool ein, der in einem Erasure-Coding-Profil verwendet wird. Fügen Sie stattdessen für jeden Standort, der Daten mit dem Erasure Coding speichert, einen separaten Eintrag in den Storage-Pool ein. Siehe [Diesem Schritt](#) Beispiel:

- Wenn Sie über mehrere Speicherklassen verfügen, erstellen Sie keinen Speicherpool, der unterschiedliche Speicherklassen an einem einzelnen Standort enthält.

"Richtlinien zur Erstellung von Speicherpools"

Schritte

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

Die Seite Speicherpools wird angezeigt und listet alle definierten Speicherpools auf.

Storage Pools

Storage Pools

A storage pool is a logical group of Storage Nodes or Archive Nodes and is used in ILM rules to determine where object data is stored.

+ Create ✎ Edit ✕ Remove 👁 View Details					
Name ⓘ	Used Space ⓘ	Free Space ⓘ	Total Capacity ⓘ	ILM Usage ⓘ	
• All Storage Nodes	1.10 MB	102.90 TB	102.90 TB	Used in 1 ILM rule	

Displaying 1 storage pool.

Cloud Storage Pools

You can add Cloud Storage Pools to ILM rules to store objects outside of the StorageGRID system. A Cloud Storage Pool defines how to access the external bucket or container where objects will be stored.

+ Create ✎ Edit ✕ Remove ✖ Clear Error			
--	--	--	--

No Cloud Storage Pools found.

Die Liste umfasst den systemstandardmäßigen Speicherpool, alle Speicherknoten, der den systemstandardmäßigen Standort, Alle Standorte und die Standard-Speicherkategorie Alle Speicherknoten verwendet.



Da der Speicherpool für alle Storage-Nodes beim Hinzufügen neuer Datacenter-Standorte automatisch aktualisiert wird, wird die Verwendung dieses Speicherpools in ILM-Regeln nicht empfohlen.

2. Um einen neuen Speicherpool zu erstellen, wählen Sie **Erstellen**.

Das Dialogfeld Speicherpool erstellen wird angezeigt.

Create Storage Pool

- For replication and single-site erasure coding, create a storage pool for each site.
- For erasure coding at three or more sites, click + to add each site to a single storage pool.
- Do not add more than one storage grade for a single site.

Name

Site

-- Choose One --

Storage Grade

All Storage Nodes

+

Viewing Storage Pool -

Site Name	Archive Nodes	Storage Nodes
-----------	---------------	---------------

Cancel

Save

3. Geben Sie einen eindeutigen Namen für den Speicherpool ein.

Verwenden Sie einen Namen, der bei der Konfiguration von Erasure Coding-Profilen und ILM-Regeln leicht zu identifizieren ist.

4. Wählen Sie aus der Dropdown-Liste **Standort** einen Standort für diesen Speicherpool aus.

Wenn Sie einen Standort auswählen, wird die Anzahl der Speicherknoten und Archivknoten in der Tabelle automatisch aktualisiert.

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

Die standardmäßige Speicherkategorie „Alle Speicherknoten“ enthält alle Speicherknoten am ausgewählten Standort. Die Standard-Speicherkategorie Archiv-Knoten umfasst alle Archiv-Knoten am ausgewählten Standort. Wenn Sie zusätzliche Speicherkategorien für die Speicherknoten in Ihrem Raster erstellt haben, werden diese im Dropdown-Menü aufgelistet.

6. Wenn Sie den Speicherpool in einem Erasure Coding-Profil für mehrere Standorte verwenden möchten, wählen Sie  So fügen Sie dem Speicherpool einen Eintrag für jeden Standort hinzu.

Create Storage Pool

- For replication and single-site erasure coding, create a storage pool for each site.
- For erasure coding at three or more sites, select + to add each site to a single storage pool.
- Do not select more than one storage grade for a single site.

Name:

Site: <input type="text" value="Data Center 1"/>	Storage Grade: <input type="text" value="All Storage Nodes"/>	<input type="button" value="✕"/>
Site: <input type="text" value="Data Center 2"/>	Storage Grade: <input type="text" value="All Storage Nodes"/>	<input type="button" value="✕"/>
Site: <input type="text" value="Data Center 3"/>	Storage Grade: <input type="text" value="All Storage Nodes"/>	<input type="button" value="+"/> <input type="button" value="✕"/>

Viewing Storage Pool - All 3 Sites for Erasure Coding

Site Name	Archive Nodes	Storage Nodes
Data Center 1	0	3
Data Center 2	0	3
Data Center 3	0	3

You are creating a multi-site storage pool, which should not be used for replication or single-site erasure coding.

Cancel

Save



Sie können keine doppelten Einträge erstellen oder einen Speicherpool erstellen, der sowohl die Speicherklasse **Archivknoten** als auch jede Speicherklasse enthält, die Speicherknoten enthält.

Sie sind gewarnt, wenn Sie mehr als einen Eintrag für einen Standort, aber mit verschiedenen Speicherklassen hinzufügen.

Um einen Eintrag zu entfernen, wählen Sie ✕.

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

Der neue Speicherpool wird der Liste hinzugefügt.

Verwandte Informationen

["Richtlinien zur Erstellung von Speicherpools"](#)

Anzeigen von Details zum Speicherpool

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.

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.

- Sie müssen über spezifische Zugriffsberechtigungen verfügen.

Schritte

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

Die Seite Speicherpools wird angezeigt. Auf dieser Seite werden alle definierten Speicherpools aufgelistet.

Storage Pools

Storage Pools

A storage pool is a logical group of Storage Nodes or Archive Nodes and is used in ILM rules to determine where object data is stored.

<div> + Create Edit Remove View Details </div>					
	Name ⓘ	Used Space ⓘ	Free Space ⓘ	Total Capacity ⓘ	ILM Usage ⓘ
<input checked="" type="radio"/>	All Storage Nodes	1.88 MB	2.80 TB	2.80 TB	Used in 1 ILM rule
<input type="radio"/>	DC1	621.77 KB	932.42 GB	932.42 GB	Used in 2 ILM rules
<input type="radio"/>	DC2	675.82 KB	932.42 GB	932.42 GB	Used in 2 ILM rules
<input type="radio"/>	DC3	578.95 KB	932.42 GB	932.42 GB	Used in 1 ILM rule
<input type="radio"/>	All 3 Sites	1.88 MB	2.80 TB	2.80 TB	Used in 1 ILM rule and 1 EC profile
<input type="radio"/>	Archive	—	—	—	—

Displaying 6 storage pools.

Cloud Storage Pools

You can add Cloud Storage Pools to ILM rules to store objects outside of the StorageGRID system. A Cloud Storage Pool defines how to access the external bucket or container where objects will be stored.

<div> + Create Edit Remove Clear Error </div>			
No Cloud Storage Pools found.			

Die Tabelle enthält die folgenden Informationen zu den einzelnen Storage-Pools, einschließlich Storage-Nodes:

- **Name:** Der eindeutige Anzeigename des Speicherpools.
- **Verwendeter Platz:** Die Menge an Speicherplatz, die derzeit zum Speichern von Objekten im Speicherpool verwendet wird.
- **Freier Raum:** Der Speicherplatz, der zur Speicherung von Objekten im Speicherpool verfügbar bleibt.
- **Gesamtkapazität:** Die Größe des Speicherpools, die der gesamten nutzbaren Menge an Objektdaten für alle Knoten im Speicherpool entspricht.
- **ILM-Nutzung:** Wie der Speicherpool derzeit genutzt wird. Ein Storage-Pool kann ungenutzt sein oder auch in einem oder mehreren ILM-Regeln, Erasure Coding-Profilen oder beidem verwendet werden.



Ein Speicherpool kann nicht entfernt werden, wenn er verwendet wird.

2. Um Details zu einem bestimmten Speicherpool anzuzeigen, wählen Sie das entsprechende Optionsfeld aus, und wählen Sie **Details anzeigen**.

Der Storage Pool Details Modal wird angezeigt.

3. Auf der Registerkarte **enthaltene Knoten** erfahren Sie mehr über die Speicherknoten oder Archivknoten,

die im Speicherpool enthalten sind.

Storage Pool Details - DC1		
<div>Nodes IncludedILM Usage</div>		
Number of Nodes: 3 Storage Grade: All Storage Nodes		
Node Name	Site Name	Used (%) ⓘ
DC1-S1	Data Center 1	0.000%
DC1-S2	Data Center 1	0.000%
DC1-S3	Data Center 1	0.000%
Close		

Die Tabelle enthält die folgenden Informationen für jeden Node:

- Node-Name
- Standortname
- Genutzt (%): Für Storage-Nodes, der Prozentsatz des insgesamt nutzbaren Speicherplatzes für Objektdaten, der verwendet wurde. Dieser Wert enthält keine Objektmetadaten.



Der gleiche verwendete (%) Wert wird auch im Diagramm Speicher verwendet - Objektdaten für jeden Speicherknoten angezeigt (wählen Sie **Knoten** > **Speicherknoten** > **Speicher**).

4. Wählen Sie die Registerkarte **ILM-Nutzung** aus, um festzustellen, ob der Speicherpool derzeit in ILM-Regeln oder Erasure Coding-Profilen verwendet wird.

In diesem Beispiel wird der DC1-Speicherpool in drei ILM-Regeln verwendet: Zwei Regeln, die sich in der aktiven ILM-Richtlinie befinden, und eine Regel, die nicht in der aktiven Richtlinie ist.

Storage Pool Details - DC1	
<div>Nodes IncludedILM Usage</div>	
<div>ILM Rules Using the Storage Pool</div> <div>The following ILM rules in the active ILM policy (Example ILM policy) use this storage pool.<ul style="list-style-type: none">• 3 copies for Account01• 2 copies for smaller objects1 ILM rule that is not in the active ILM policy uses this storage pool.<p>If you want to remove this storage pool, you must delete or edit every rule where it is used. Go to the ILM Rules page ⓘ</p></div>	
<div>EC Profiles Using the Storage Pool</div> <div>No Erasure Coding profiles use this storage pool.</div>	
Close	



Sie können einen Speicherpool nicht entfernen, wenn er in einer ILM-Regel verwendet wird.

In diesem Beispiel wird der Speicherpool „Alle 3 Standorte“ in einem Erasure Coding-Profil verwendet. Dieses Erasure Coding-Profil wird wiederum von einer ILM-Regel in der aktiven ILM-Richtlinie verwendet.

Storage Pool Details - All 3 Sites

Nodes Included

ILM Usage

ILM Rules Using the Storage Pool

The following ILM rules in the active ILM policy (Example ILM policy) use this storage pool.

- EC larger objects

If you want to remove this storage pool, you must delete or edit every rule where it is used. Go to the [ILM Rules page](#)

EC Profiles Using the Storage Pool

The following Erasure Coding profiles use this storage pool.

Profile Name	Profile Status
6 plus 3	Used in 1 ILM Rule

Close



Ein Speicherpool kann nicht entfernt werden, wenn er in einem Erasure Coding-Profil verwendet wird.

5. Klicken Sie optional auf die Seite **ILM-Regeln**, um mehr über die Regeln zu erfahren und diese zu verwalten, die den Speicherpool verwenden.

Anweisungen zum Arbeiten mit ILM-Regeln finden Sie in der Anleitung.

6. Wenn Sie die Details des Speicherpools anzeigen, wählen Sie **Schließen**.

Verwandte Informationen

["Arbeiten mit ILM-Regeln und ILM-Richtlinien"](#)

Bearbeiten eines Speicherpools

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

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.
- Sie müssen über spezifische Zugriffsberechtigungen verfügen.
- Sie müssen die Richtlinien zum Erstellen von Speicherpools überprüft haben.
- Wenn Sie einen Speicherpool bearbeiten möchten, der von einer Regel in der aktiven ILM-Richtlinie verwendet wird, müssen Sie prüfen, wie sich Ihre Änderungen auf die Platzierung der Objektdaten auswirken.

Über diese Aufgabe

Wenn Sie einem Speicherpool, der in der aktiven ILM-Richtlinie verwendet wird, eine neue Speicherklasse hinzufügen, beachten Sie, dass die Speicherknoten in der neuen Speicherklasse nicht automatisch verwendet werden. Damit StorageGRID die Verwendung einer neuen Storage-Klasse erzwingen kann, müssen Sie eine neue ILM-Richtlinie aktivieren, nachdem Sie den bearbeiteten Speicherpool gespeichert haben.

Schritte

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

Die Seite Speicherpools wird angezeigt.

2. Wählen Sie das Optionsfeld für den Speicherpool aus, den Sie bearbeiten möchten.

Der Speicherpool Alle Speicherknoten 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 die Standort- oder Speicherklasse nicht ändern, wenn der Speicherpool in einem Erasure-Coding-Profil verwendet wird und die Änderung das Erasure-Coding-Schema ungültig machen würde. Wenn beispielsweise ein Speicherpool, der in einem Erasure-Coding-Profil verwendet wird, derzeit eine Speicherklasse mit nur einem Standort enthält, können Sie eine Speicherklasse mit zwei Standorten nicht verwenden, da die Änderung das Erasure-Coding-Schema ungültig machen würde.

6. Wählen Sie **Speichern**.

Nachdem Sie fertig sind

Wenn Sie einem Storage-Pool, der in der aktiven ILM-Richtlinie verwendet wird, eine neue Storage-Klasse hinzugefügt haben, aktivieren Sie eine neue ILM-Richtlinie, um die Verwendung der neuen Storage-Klasse durch StorageGRID zu erzwingen. Klonen Sie beispielsweise Ihre vorhandene ILM-Richtlinie und aktivieren Sie dann den Klon.

Entfernen eines Speicherpools

Sie können einen Speicherpool entfernen, der nicht verwendet wird.

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.
- Sie müssen über spezifische Zugriffsberechtigungen verfügen.

Schritte

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

Die Seite Speicherpools wird angezeigt.

2. Sehen Sie sich die Spalte ILM-Nutzung in der Tabelle an, um zu bestimmen, ob Sie den Speicherpool entfernen können.

Ein Speicherpool kann nicht entfernt werden, wenn er in einer ILM-Regel oder in einem Erasure Coding-Profil verwendet wird. Wählen Sie nach Bedarf **Details anzeigen > ILM-Nutzung** aus, um festzustellen,

wo ein Speicherpool verwendet wird.

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

Verwendung Von Cloud Storage Pools

Mithilfe von Cloud-Storage-Pools können StorageGRID Objekte an einen externen Storage-Standort wie S3 Glacier oder Microsoft Azure Blob Storage verschoben werden. Durch das Verschieben von Objekten außerhalb des Grid können Sie von einem kostengünstigen Storage Tier für die Langzeitarchivierung profitieren.

- ["Was ist ein Cloud-Storage-Pool"](#)
- ["Lebenszyklus eines Cloud-Storage-Pool-Objekts"](#)
- ["Wann sollten Sie Cloud Storage Pools nutzen"](#)
- ["Überlegungen zu Cloud-Storage-Pools"](#)
- ["Vergleich von Cloud Storage Pools und CloudMirror Replizierung"](#)
- ["Erstellen eines Cloud-Speicherpools"](#)
- ["Bearbeiten eines Cloud-Speicherpools"](#)
- ["Entfernen eines Cloud-Speicherpools"](#)
- ["Fehlerbehebung Bei 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 möchten Sie selten genutzte Objekte in kostengünstigeren Cloud-Storage verschieben, wie z. B. Amazon S3 Glacier, S3 Glacier Deep Archive oder die Archive Access 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 oder Archiv-Nodes innerhalb des StorageGRID-Systems bestehen, besteht ein Cloud Storage Pool aus einem externen Bucket (S3) oder Container (Azure Blob-Storage).

Die folgende Tabelle vergleicht Storage-Pools mit Cloud Storage Pools und zeigt die grundlegenden Ähnlichkeiten und Unterschiede.

	Storage-Pool	Cloud-Storage-Pool
Wie wird sie erstellt?	<p>Verwenden der Option ILM > Storage Pools im Grid Manager.</p> <p>Sie müssen Speicherklassen einrichten, bevor Sie den Speicherpool erstellen können.</p>	<p>Verwenden der Option ILM > Storage Pools im Grid Manager.</p> <p>Sie müssen den externen Bucket oder Container einrichten, bevor Sie den Cloud Storage-Pool erstellen können.</p>
Wie viele Pools können Sie erstellen?	Unbegrenzt.	Bis zu 10.
Wo werden Objekte gespeichert?	Auf einem oder mehreren Speicherknoten oder Archivknoten innerhalb von StorageGRID.	<p>In einem Amazon S3-Bucket oder Azure Blob-Storage-Container, der nicht zum StorageGRID System integriert ist</p> <p>Wenn der Cloud Storage Pool ein Amazon S3-Bucket ist:</p> <ul style="list-style-type: none"> • 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 Storage-System muss die Glacier Storage-Klasse und die S3 POST Object Restore API unterstützen. • Sie können Cloud-Storage-Pools zur Verwendung mit AWS Commercial Cloud Services (C2S) erstellen, die die AWS Secret Region unterstützen. <p>Wenn der Cloud-Storage-Pool ein Azure Blob-Storage-Container ist, überträgt StorageGRID das Objekt auf die Archiv-Tier.</p> <p>Hinweis: Konfigurieren Sie generell nicht das Lifecycle-Management für Azure Blob Storage für den Container, der für einen Cloud-Storage-Pool verwendet wird. Die Wiederherstellung VON OBJEKTEN NACH DER Objekt-WIEDERHERSTELLUNG im Cloud-Storage-Pool kann vom konfigurierten Lebenszyklus betroffen sein.</p>
Welche Kontrollen steuern die Objektplatzierung?	Eine ILM-Regel in der aktiven ILM-Richtlinie.	Eine ILM-Regel in der aktiven ILM-Richtlinie.

	Storage-Pool	Cloud-Storage-Pool
Welche Datensicherungsmethode 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: Sie können ein Objekt nicht in mehr als einem Cloud-Speicherpool speichern.
Worin liegen die Vorteile?	Objekte sind jederzeit schnell abrufbar.	Kostengünstiger Storage:

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.

Verwandte Informationen

[S3: Lebenszyklus eines Cloud-Storage-Pool-Objekts](#)

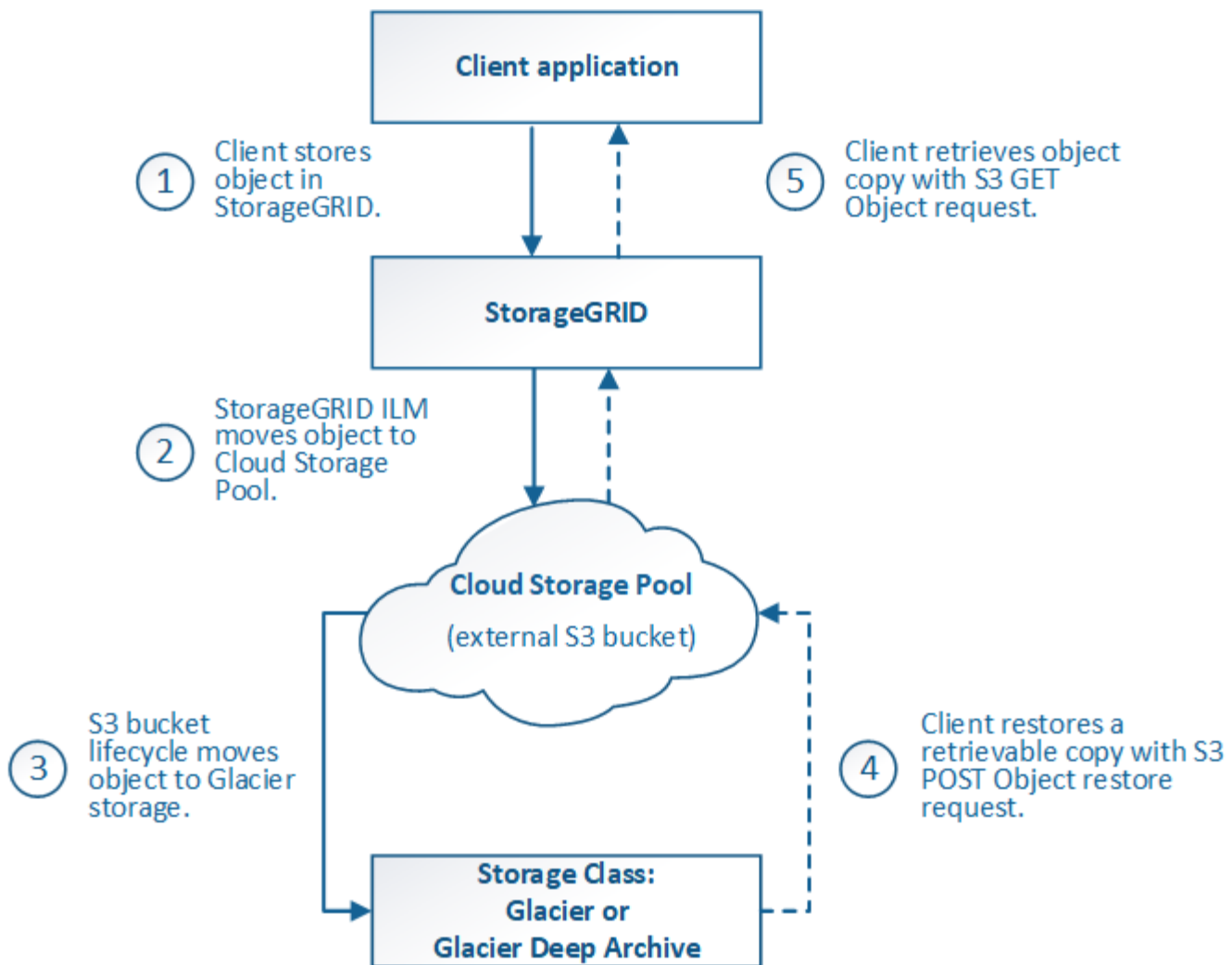
[Azure: Lebenszyklus eines Cloud-Storage-Pool-Objekts\]](#)

S3: Lebenszyklus eines Cloud-Storage-Pool-Objekts

Die Abbildung zeigt die Lebenszyklusphasen eines Objekts, das in einem S3 Cloud-Storage-Pool gespeichert ist.



In der Abbildung und den Erläuterungen bezieht sich „Glacier“ sowohl auf die Glacier Storage-Klasse als auch auf die Glacier Deep Archive Storage-Klasse. Eine Ausnahme bilden die Glacier Deep Archive Storage-Klasse, die Expedited Restore Tier nicht unterstützt. Nur Bulk- oder Standard-Abruf wird unterstützt.



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.
- Sobald das Objekt in den S3-Cloud-Storage-Pool verschoben wurde, kann die Client-Applikation es mithilfe einer S3-GET-Objektanforderung von StorageGRID abrufen, es sei denn, das Objekt wurde auf Glacier Storage migriert.

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 verschieben möchten, müssen Sie eine Lebenszykluskonfiguration für den externen S3-Bucket erstellen. Außerdem ist eine Storage-Lösung erforderlich, die die Glacier Storage-Klasse implementiert und die S3-API FÜR DIE WIEDERHERSTELLUNG NACH Objekten unterstützt.



Verwenden Sie Cloud-Storage-Pools nicht für Objekte, die von Swift-Clients aufgenommen wurden. Swift unterstützt keine Wiederherstellungsanforderungen NACH dem Objekt, daher kann StorageGRID keine Swift Objekte abrufen, die auf S3 Glacier Storage verschoben wurden. Die Ausgabe einer Swift GET Objektanforderung zum Abrufen dieser Objekte schlägt fehl (403 Verbotene).

- Während des Übergangs kann die Client-Applikation mithilfe einer S3 HEAD Object-Anfrage den Status des Objekts überwachen.

4. Objekt vom Glacier-Speicher wiederhergestellt

Wenn ein Objekt in den Glacier Storage verschoben wurde, kann die Client-Applikation eine S3-POST-Object-Wiederherstellungsanforderung ausgeben, um eine abrufbare Kopie in den 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 eine oder mehrere Kopien des Objekts auch auf Speicherknoten innerhalb von StorageGRID vorhanden sind, muss das Objekt nicht von Glacier wiederhergestellt werden, indem eine Anforderung zur Wiederherstellung NACH dem Objekt gestellt wird. Stattdessen kann die lokale Kopie direkt mit Hilfe einer GET Object-Anforderung abgerufen werden.

5. Objekt abgerufen

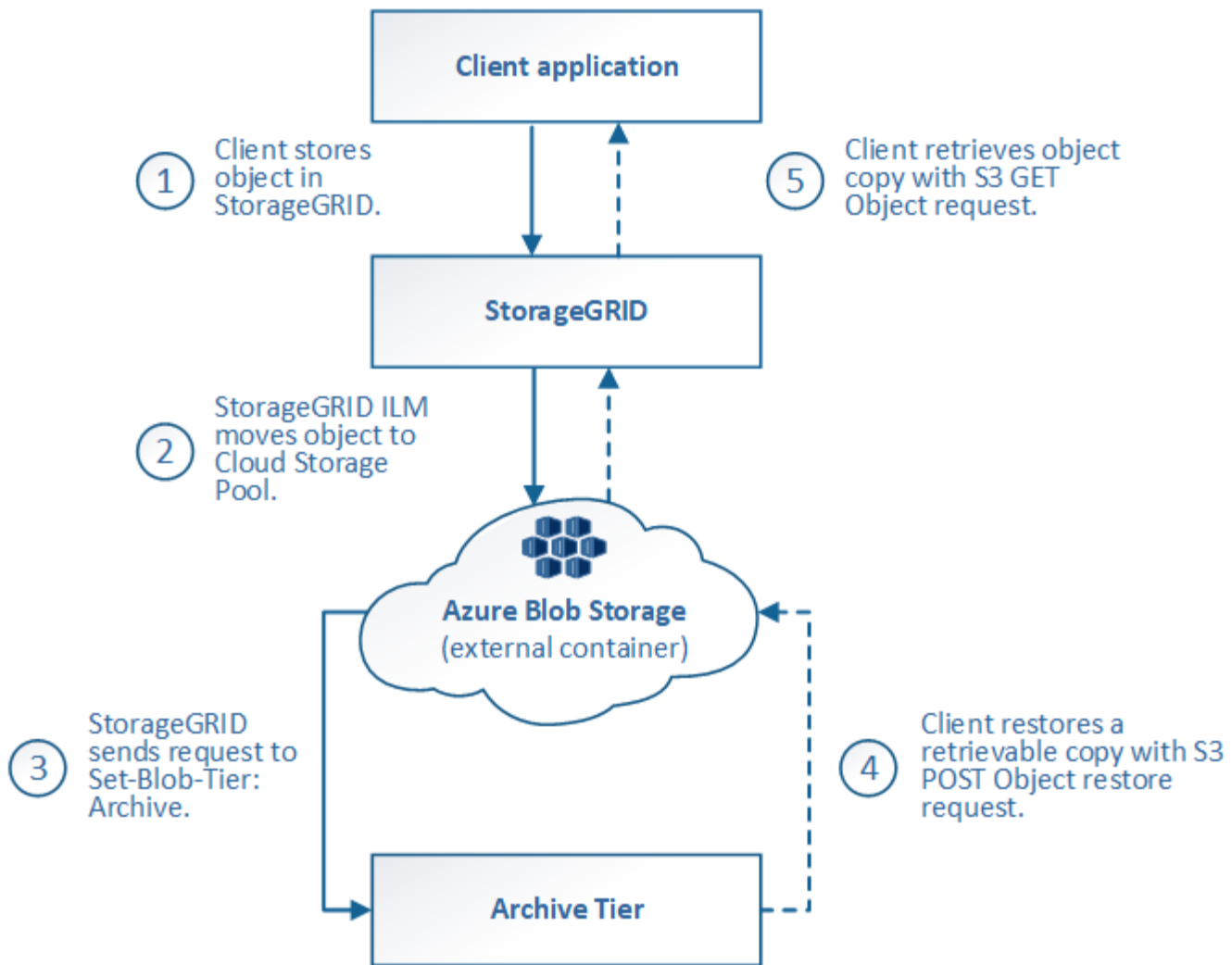
Sobald ein Objekt wiederhergestellt ist, kann die Client-Applikation eine GET Object-Anforderung ausgeben, um das wiederhergestellte Objekt abzurufen.

Verwandte Informationen

["S3 verwenden"](#)

Azure: Lebenszyklus eines Cloud-Storage-Pool-Objekts

Die Abbildung zeigt die Lebenszyklusphasen eines Objekts, 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

Wird das Objekt mit einer ILM-Regel abgeglichen, 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 festgelegt wurde.



Verwenden Sie Cloud-Storage-Pools nicht für Objekte, die von Swift-Clients aufgenommen wurden. Swift unterstützt keine Anfragen zur WIEDERHERSTELLUNG NACH einem Objekt, daher kann StorageGRID keine Swift Objekte abrufen, die auf die Azure Blob Storage-Archivebene übertragen wurden. Die Ausgabe einer Swift GET Objektanforderung zum Abrufen dieser Objekte schlägt fehl (403 Verbotene).

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 Archivebene migriert wurde, kann die Client-Applikation eine S3-RÜCKSTELLUNGSANFRAGE aus DEM NACHBEARBEITUNGSOBJEKT senden, um eine abrufbare Kopie in den Azure Cloud Storage Pool wiederherzustellen.

Wenn StorageGRID die POST-Objekt-Wiederherstellung empfängt, wird das Objekt vorübergehend in den Azure Blob-Storage Cool-Tier verlagert. Sobald das Ablaufdatum in der Wiederherstellungsanforderung FÜR NACHOBJEKTE erreicht ist, überträgt StorageGRID das Objekt zurück in die Archivebene.



Wenn eine oder mehrere Kopien des Objekts auch auf Storage-Nodes innerhalb von StorageGRID vorhanden sind, muss das Objekt durch Ausgabe einer Anforderung zur WIEDERHERSTELLUNG NACH DEM Objekt nicht aus der Zugriffsebene für Archive wiederhergestellt werden. Stattdessen kann die lokale Kopie direkt mit Hilfe einer GET Object-Anforderung abgerufen werden.

5. Objekt abgerufen

Sobald ein Objekt im Azure Cloud Storage Pool wiederhergestellt ist, kann die Client-Applikation EINE GET Object-Anfrage stellen, um das wiederhergestellte Objekt abzurufen.

Wann sollten Sie Cloud Storage Pools nutzen

Cloud Storage Pools können in verschiedenen Anwendungsfällen deutliche Vorteile bieten.

Sichern von StorageGRID Daten an einem externen Standort

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 Anforderung zur Wiederherstellung VON S3-OBJEKTEN NACH DEM Wiederherstellen 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.

Tiering von Daten von StorageGRID an externen Speicherort

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 mehrere Cloud-Storage-Pools konfigurieren, wenn Sie Objektdaten auf mehreren Clouds abstufen oder sichern möchten. Mit den Filtern Ihrer ILM-Regeln können Sie festlegen, welche Objekte in den einzelnen Cloud Storage-Pools gespeichert werden. Beispielsweise möchten Sie Objekte von einigen Mandanten oder Buckets in Amazon S3 Glacier und Objekten von anderen Mandanten oder Buckets im Azure Blob Storage speichern. Alternativ können Sie Daten zwischen Amazon S3 Glacier und Azure Blob Storage verschieben. Bei dem Einsatz mehrerer Cloud-Storage-Pools ist zu beachten, dass ein Objekt immer nur in einem Cloud-Storage-Pool 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 für eine gewisse Zeit im Cloud Storage Pool A 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.
- Verwenden Sie Cloud-Storage-Pools nicht für Objekte, die von Swift-Clients aufgenommen wurden. Swift unterstützt keine Anforderungen für DIE WIEDERHERSTELLUNG NACH dem Objekt, sodass StorageGRID keine Swift Objekte abrufen kann, die auf S3 Glacier Storage oder in die Azure Blob Storage-Archivebene verschoben wurden. Die Ausgabe einer Swift GET Objektanforderung zum Abrufen dieser Objekte schlägt fehl (403 Verbotene).
- 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.

Zum Erstellen eines Cloud-Storage-Pools erforderliche Informationen

Bevor Sie einen Cloud Storage Pool erstellen können, müssen Sie den externen S3-Bucket oder den externen

Azure Blob-Storage-Container erstellen, den Sie für den Cloud Storage Pool verwenden werden. Wenn Sie dann den Cloud-Speicherpool in StorageGRID erstellen, müssen Sie die folgenden Informationen angeben:

- Der Provider-Typ: Amazon S3 oder Azure Blob Storage
- Wenn Sie Amazon S3 auswählen, ob der Cloud-Storage-Pool für die Verwendung mit der AWS Secret Region (**CAP (C2S Access Portal)**) verwendet werden soll.
- Der genaue Name des Buckets oder Containers.
- Der Service-Endpunkt für den Zugriff auf den Bucket oder Container
- Die für den Zugriff auf den Bucket oder Container erforderliche Authentifizierung:
 - **S3**: Optional eine Zugriffsschlüssel-ID und ein geheimer Zugriffsschlüssel.
 - **C2S**: Die vollständige URL zum Abrufen temporärer Anmeldeinformationen vom CAP-Server; ein Server-CA-Zertifikat, ein Clientzertifikat, ein privater Schlüssel für das Clientzertifikat und, wenn der private Schlüssel verschlüsselt ist, die Passphrase zum Entschlüsseln.
 - **Azure Blob Storage**: Ein Kontoname und Kontoschlüssel. Diese Anmeldedaten müssen über vollständige Berechtigungen für den Container verfügen.
- Optional kann ein individuelles CA-Zertifikat zum Überprüfen der TLS-Verbindungen mit dem Bucket oder Container genutzt werden.

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

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

Wenn Sie einen nicht transparenten Proxyserver verwenden, müssen Sie auch einen Speicher-Proxy konfigurieren, damit Nachrichten an externe Endpunkte gesendet werden können, z. B. an einen Endpunkt im Internet.

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 müssen Sie einfach Ihre ILM-Regeln und -Richtlinien neu konfigurieren. 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 Bucket-Richtlinie für den externen S3-Bucket, der für Cloud Storage Pool verwendet wird, muss StorageGRID-Berechtigung erteilen, ein Objekt in den Bucket zu verschieben, den Status eines Objekts zu erhalten, bei Bedarf ein Objekt aus dem Glacier Storage wiederherzustellen usw. Idealerweise sollte StorageGRID über vollständigen Kontrollzugriff auf den Bucket verfügen (`s3:*`). Ist dies jedoch nicht möglich, 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 durch ILM-Regeln und die aktive ILM-Richtlinie 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 verschieben möchten, müssen Sie eine entsprechende Lebenszykluskonfiguration auf dem externen S3-Bucket erstellen. Außerdem muss eine Storage-Lösung verwendet werden, die die Glacier Storage-Klasse implementiert und die S3-API FÜR DIE WIEDERHERSTELLUNG NACH Objekten 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 zum S3 Glacier Deep Archive verschieben möchten (statt zu Amazon S3 Glacier), geben Sie an `<StorageClass>DEEP_ARCHIVE</StorageClass>` Im Bucket-Lebenszyklus: Beachten Sie jedoch, dass Sie das nicht verwenden können `Expedited` Tier zur Wiederherstellung von Objekten aus S3 Glacier Deep Archive.

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

Verwandte Informationen

["Erstellen eines Cloud-Speicherpools"](#)

["S3: Angeben von Authentifizierungsdetails für einen Cloud Storage-Pool"](#)

"C2S S3: Angeben von Authentifizierungsdetails für einen Cloud-Storage-Pool"

"Azure: Angeben von Authentifizierungsdetails für einen Cloud Storage-Pool"

"StorageGRID verwalten"

Vergleich von Cloud Storage Pools und CloudMirror Replizierung

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?	Ein Cloud-Storage-Pool fungiert als Archivziel. Die Objektkopie im Cloud-Storage-Pool kann die einzige Kopie des Objekts sein oder es kann eine zusätzliche Kopie sein. Das bedeutet, dass Sie nicht mehr zwei Kopien lokal aufbewahren müssen, sondern nur eine Kopie innerhalb von StorageGRID aufbewahren und eine Kopie an den Cloud-Storage-Pool senden können.	Der CloudMirror Replikationsservice ermöglicht einem Mandanten, Objekte automatisch von einem Bucket in StorageGRID (Quelle) auf einen externen S3 Bucket (Ziel) zu replizieren. Bei der CloudMirror-Replizierung wird eine unabhängige Kopie eines Objekts in einer unabhängigen S3-Infrastruktur erstellt.
Wie ist es eingerichtet?	Cloud-Storage-Pools werden mit Grid Manager oder Grid-Management-API auf dieselbe Weise wie Storage-Pools definiert. Sie können einen Cloud-Storage-Pool als Speicherort in einer ILM-Regel auswählen. 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 konfiguriert die CloudMirror-Replizierung mithilfe des Tenant Manager oder der S3-API durch Definition eines CloudMirror-Endpunkts (IP-Adresse, Anmeldeinformationen usw.). 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?	<ul style="list-style-type: none">• Alle kompatiblen S3-Infrastrukturen (einschließlich Amazon S3)• Azure Blob Archiveebene	<ul style="list-style-type: none">• Alle kompatiblen S3-Infrastrukturen (einschließlich Amazon S3)
Was bewirkt, dass Objekte zum Ziel verschoben werden?	Ein oder mehrere ILM-Regeln in der aktiven ILM-Richtlinie. Die ILM-Regeln legen fest, welche Objekte die StorageGRID in den Cloud-Storage-Pool verschoben und wann sie verschoben werden.	Das Einspeisen eines neuen Objekts in einen Quell-Bucket, der mit einem CloudMirror-Endpunkt konfiguriert wurde. Objekte, die sich vor der Konfiguration mit dem CloudMirror-Endpunkt im Quell-Bucket befanden, werden nicht repliziert, es sei denn, sie werden modifiziert.

	Cloud-Storage-Pool	CloudMirror Replikationsservice
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 Replikierung, 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?	Nein Objekte, die in einen Cloud-Storage-Pool verschoben werden, 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 im Cloud-Speicherpool gelöscht.	Die Löschaktion wird nicht repliziert. Ein gelöscht 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.

Verwandte Informationen

["StorageGRID verwalten"](#)

Erstellen eines Cloud-Speicherpools

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

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.
- Sie müssen über spezifische Zugriffsberechtigungen verfügen.
- Sie müssen die Richtlinien zum Konfigurieren von Cloud-Speicherpools überprüft haben.
- Der externe Bucket oder Container, auf den der Cloud-Storage-Pool verweist, muss vorhanden sein.
- Für den Zugriff auf den Bucket oder Container müssen alle Authentifizierungsinformationen vorhanden sein.

Über diese Aufgabe

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

Schritte

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

Die Seite Speicherpools wird angezeigt. Diese Seite enthält zwei Abschnitte: Speicherpools und Cloud-Speicherpools.

Storage Pools

Storage Pools

A storage pool is a logical group of Storage Nodes or Archive Nodes and is used in ILM rules to determine where object data is stored.

+ Create Edit Remove View Details

Name ?	Used Space ?	Free Space ?	Total Capacity ?	ILM Usage ?
All Storage Nodes	1.10 MB	102.90 TB	102.90 TB	Used in 1 ILM rule

Displaying 1 storage pool.

Cloud Storage Pools

You can add Cloud Storage Pools to ILM rules to store objects outside of the StorageGRID system. A Cloud Storage Pool defines how to access the external bucket or container where objects will be stored.

+ Create Edit Remove Clear Error

No Cloud Storage Pools found.

2. Klicken Sie im Abschnitt Cloud-Speicherpools auf der Seite auf **Erstellen**.

Das Dialogfeld Cloud-Speicherpool erstellen wird angezeigt.

Create Cloud Storage Pool

Display Name
?

Provider Type
?

▼

Bucket or Container
?

Cancel

Save

3. Geben Sie die folgenden Informationen ein:

Feld	Beschreibung
Anzeigenname	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.
Art Des Anbieters	<p>Welcher Cloud-Provider nutzen Sie für diesen Cloud-Storage-Pool?</p> <ul style="list-style-type: none"> • Amazon S3 (wählen Sie diese Option für einen S3- oder C2S S3-Cloud-Storage-Pool) • Azure Blob Storage <p>Hinweis: Wenn Sie einen Provider-Typ auswählen, werden unten auf der Seite die Abschnitte „Service Endpoint“, „Authentifizierung“ und „Server-Überprüfung“ angezeigt.</p>
Bucket oder Container	Der Name des externen S3-Buckets oder Azure-Containers, der für den Cloud-Storage-Pool erstellt wurde. Der hier angegebene Name muss exakt mit dem Bucket oder Container-Namen übereinstimmen, oder die Erstellung von Cloud-Storage-Pool schlägt fehl. Sie können diesen Wert nicht ändern, nachdem der Cloud-Speicherpool gespeichert wurde.

4. Schließen Sie die Abschnitte „Service Endpoint“, „Authentifizierung“ und „Server-Verifizierung“ der Seite basierend auf dem ausgewählten Provider-Typ ab.

- ["S3: Angeben von Authentifizierungsdetails für einen Cloud Storage-Pool"](#)
- ["C2S S3: Angeben von Authentifizierungsdetails für einen Cloud-Storage-Pool"](#)
- ["Azure: Angeben von Authentifizierungsdetails für einen Cloud Storage-Pool"](#)

S3: Angeben von Authentifizierungsdetails für einen Cloud Storage-Pool

Wenn Sie einen Cloud Storage Pool für S3 erstellen, müssen Sie den Authentifizierungstyp für den Cloud Storage Pool-Endpunkt auswählen. Sie können Anonymous angeben oder eine Zugriffsschlüssel-ID und einen geheimen

Zugriffsschlüssel eingeben.

Was Sie benötigen

- Sie müssen die Basisinformationen für den Cloud-Speicherpool eingeben und **Amazon S3** als Provider-Typ angegeben haben.

Create Cloud Storage Pool

Display Name ⓘ

S3 Cloud Storage Pool

Provider Type ⓘ

Amazon S3 ▼

Bucket or Container ⓘ

my-s3-bucket

Service Endpoint

Protocol ⓘ

☐ HTTP ☒ HTTPS

Hostname ⓘ

example.com or 0.0.0.0

Port (optional) ⓘ

443

Authentication

Authentication Type ⓘ

▼

Server Verification

Certificate Validation ⓘ

Use operating system CA certificate ▼

Cancel

Save

- Wenn Sie die Authentifizierung für Zugriffsschlüssel verwenden, müssen Sie die Zugriffsschlüssel-ID und den geheimen Zugriffsschlüssel für den externen S3-Bucket kennen.

Schritte

1. Geben Sie im Abschnitt * Service Endpoint* folgende Informationen an:
 - a. Wählen Sie das Protokoll aus, das bei der Verbindung mit dem Cloud-Storage-Pool verwendet werden soll.

Das Standardprotokoll ist HTTPS.

- b. Geben Sie den Serverhostnamen oder die IP-Adresse des Cloud-Speicherpools ein.

Beispiel:

`s3-aws-region.amazonaws.com`



Geben Sie den Bucket-Namen nicht in dieses Feld ein. Sie fügen den Bucket-Namen in das Feld **Bucket oder Container** ein.

- a. Geben Sie optional den Port an, der bei der Verbindung mit dem Cloud Storage Pool verwendet werden soll.

Lassen Sie dieses Feld leer, um den Standardport Port 443 für HTTPS oder Port 80 für HTTP zu verwenden.

2. Wählen Sie im Abschnitt **Authentifizierung** den Authentifizierungstyp aus, der für den Cloud-Storage-Pool-Endpunkt erforderlich ist.

Option	Beschreibung
Zugriffsschlüssel	Für den Zugriff auf den Cloud Storage Pool-Bucket sind eine Zugriffsschlüssel-ID und ein geheimer Zugriffsschlüssel erforderlich.
Anonym	Jeder hat Zugriff auf den Cloud-Storage-Pool-Bucket. Eine Zugriffsschlüssel-ID und ein geheimer Zugriffsschlüssel sind nicht erforderlich.
KAPPE (C2S-Zugangsportal)	Wird nur für C2S S3 verwendet. Gehen Sie zu "C2S S3: Angeben von Authentifizierungsdetails für einen Cloud-Storage-Pool" .

3. Wenn Sie den Zugriffsschlüssel ausgewählt haben, geben Sie die folgenden Informationen ein:

Option	Beschreibung
Zugriffsschlüssel-ID	Zugriffsschlüssel-ID für das Konto, das den externen Bucket besitzt
Geheimer Zugriffsschlüssel	Der zugehörige Schlüssel für den geheimen Zugriff.

4. Wählen Sie im Abschnitt Server Verification die Methode aus, mit der das Zertifikat für TLS-Verbindungen zum Cloud Storage Pool validiert werden soll:

Option	Beschreibung
Verwenden Sie das CA-Zertifikat für das Betriebssystem	Verwenden Sie die auf dem Betriebssystem installierten Standard-CA-Zertifikate, um Verbindungen zu sichern.
Benutzerdefiniertes CA-Zertifikat verwenden	Verwenden Sie ein benutzerdefiniertes CA-Zertifikat. Klicken Sie auf Neu auswählen , und laden Sie das PEM-codierte CA-Zertifikat hoch.

Option	Beschreibung
Verifizieren Sie das Zertifikat nicht	Das für die TLS-Verbindung verwendete Zertifikat wird nicht verifiziert.

5. Klicken Sie Auf **Speichern**.

Beim Speichern eines Cloud-Speicherpools führt StorageGRID Folgendes aus:

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

Wenn die Validierung des Cloud-Storage-Pools fehlschlägt, erhalten Sie eine Fehlermeldung, die erklärt, warum die Validierung fehlgeschlagen ist. Möglicherweise wird ein Fehler gemeldet, wenn ein Zertifikatfehler vorliegt oder der angegebene Bucket nicht bereits vorhanden ist.

! Error

422: Unprocessable Entity

Validation failed. Please check the values you entered for errors.

Cloud Pool test failed. Could not create or update Cloud Pool. Error from endpoint: NoSuchBucket: The specified bucket does not exist. status code: 404, request id: 4211567681, host id:

OK

Lesen Sie die Anweisungen zur Fehlerbehebung bei Cloud-Speicherpools, beheben Sie das Problem und versuchen Sie dann, den Cloud-Speicherpool erneut zu speichern.

Verwandte Informationen

["Fehlerbehebung Bei Cloud Storage Pools"](#)

C2S S3: Angeben von Authentifizierungsdetails für einen Cloud-Storage-Pool

Wenn Sie den S3-Service (Commercial Cloud Services, C2S) als Cloud-Storage-Pool verwenden möchten, müssen Sie C2S Access Portal (CAP) als Authentifizierungstyp konfigurieren, damit StorageGRID temporäre Anmeldedaten für den Zugriff auf den S3-Bucket in Ihrem C2S-Konto anfordern kann.

Was Sie benötigen

- Sie müssen die Basisinformationen für einen Amazon S3 Cloud-Storage-Pool, einschließlich des Service-Endpunkts, eingegeben haben.
- Sie müssen die vollständige URL kennen, die StorageGRID zum Abrufen temporärer Anmeldeinformationen vom CAP-Server verwendet, einschließlich aller erforderlichen und optionalen API-Parameter, die Ihrem C2S-Konto zugewiesen sind.
- Sie müssen über ein Server-CA-Zertifikat verfügen, das von einer entsprechenden Behörde ausgestellt

wurde. StorageGRID verwendet dieses Zertifikat, um die Identität des CAP-Servers zu überprüfen. Das Server-CA-Zertifikat muss die PEM-Kodierung verwenden.

- Sie müssen über ein Clientzertifikat verfügen, das von einer entsprechenden Behörde ausgestellt wurde. StorageGRID verwendet dieses Zertifikat zur Identität des CAP-Servers. Das Clientzertifikat muss PEM-Kodierung verwenden und Zugriff auf Ihr C2S-Konto haben.
- Sie benötigen einen PEM-kodierten privaten Schlüssel für das Clientzertifikat.
- Wenn der private Schlüssel für das Clientzertifikat verschlüsselt ist, müssen Sie die Passphrase zum Entschlüsseln besitzen.

Schritte

1. Wählen Sie im Abschnitt **Authentifizierung** im Dropdown-Menü **Authentifizierungstyp** die Option **CAP (C2S Access Portal)** aus.

Die C2S-Authentifizierungsfelder werden angezeigt.

Create Cloud Storage Pool

Display Name ⓘ

S3 Cloud Storage Pool

Provider Type ⓘ

Amazon S3 ▼

Bucket or Container ⓘ

my-s3-bucket

Service Endpoint

Protocol ⓘ

☐ HTTP

☒ HTTPS

Hostname ⓘ

s3-aws-region.amazonaws.com

Port (optional) ⓘ

443

Authentication

Authentication Type ⓘ

CAP (C2S Access Portal) ▼

Temporary Credentials URL ⓘ

https://example.com/CAP/api/v1/credentials?agency=my

Server CA Certificate ⓘ

Select New

Client Certificate ⓘ

Select New

Client Private Key ⓘ

Select New

Client Private Key Passphrase
(optional) ⓘ

Server Verification

Certificate Validation ⓘ

Use operating system CA certificate ▼

Cancel

Save

2. Geben Sie die folgenden Informationen an:

- a. Geben Sie unter **URL für temporäre Anmeldeinformationen** 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. Klicken Sie für **Server-CA-Zertifikat** auf **Neu auswählen** und laden Sie das PEM-codierte CA-Zertifikat hoch, das StorageGRID zur Überprüfung des CAP-Servers verwendet.
- c. Klicken Sie für **Clientzertifikat** auf **Neu auswählen** und laden Sie das PEM-kodierte Zertifikat, das StorageGRID zur Identifizierung auf den CAP-Server verwendet.
- d. Klicken Sie für **Client Private Key** auf **Select New** und laden Sie den PEM-kodierten privaten Schlüssel für das Clientzertifikat hoch.

Wenn der private Schlüssel verschlüsselt ist, muss das traditionelle Format verwendet werden. (Das verschlüsselte PKCS #8-Format wird nicht unterstützt.)

- 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.

3. Geben Sie im Abschnitt Server-Überprüfung folgende Informationen an:

- a. Wählen Sie für **Zertifikatvalidierung** * Benutzerdefiniertes CA-Zertifikat verwenden* aus.
- b. Klicken Sie auf **Neu auswählen**, und laden Sie das PEM-codierte CA-Zertifikat hoch.

4. Klicken Sie Auf **Speichern**.

Beim Speichern eines Cloud-Speicherpools führt StorageGRID Folgendes aus:

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

Wenn die Validierung des Cloud-Storage-Pools fehlschlägt, erhalten Sie eine Fehlermeldung, die erklärt, warum die Validierung fehlgeschlagen ist. Möglicherweise wird ein Fehler gemeldet, wenn ein Zertifikatfehler vorliegt oder der angegebene Bucket nicht bereits vorhanden ist.

! Error

422: Unprocessable Entity

Validation failed. Please check the values you entered for errors.

Cloud Pool test failed. Could not create or update Cloud Pool. Error from endpoint: NoSuchBucket:
The specified bucket does not exist. status code: 404, request id: 4211567681, host id:

OK

Lesen Sie die Anweisungen zur Fehlerbehebung bei Cloud-Speicherpools, beheben Sie das Problem und versuchen Sie dann, den Cloud-Speicherpool erneut zu speichern.

Verwandte Informationen

Azure: Angeben von Authentifizierungsdetails für einen Cloud Storage-Pool

Wenn Sie einen Cloud Storage Pool für Azure Blob Storage erstellen, müssen Sie einen Kontonamen und Kontoschlüssel für den externen Container angeben, den StorageGRID zum Speichern von Objekten verwendet.

Was Sie benötigen

- Sie müssen die Basisinformationen für den Cloud Storage Pool eingeben und **Azure Blob Storage** als Provider-Typ angegeben haben. **Gemeinsamer Schlüssel** wird im Feld **Authentifizierungstyp** angezeigt.

Create Cloud Storage Pool

Display Name ⓘ

Azure Cloud Storage Pool

Provider Type ⓘ

Azure Blob Storage ▼

Bucket or Container ⓘ

my-azure-container

Service Endpoint

URI ⓘ

https://myaccount.blob.core.windows.net

Authentication

Authentication Type ⓘ

Shared Key

Account Name ⓘ

Account Key ⓘ

Server Verification

Certificate Validation ⓘ

Use operating system CA certificate ▼

Cancel

Save

- Sie müssen den URI (Unified Resource Identifier) kennen, der für den Zugriff auf den Blob-Storage-

Container verwendet wird, der für den Cloud Storage-Pool verwendet wird.

- Sie müssen den Namen des Speicherkontos und den geheimen Schlüssel kennen. Im Azure-Portal finden Sie diese Werte.

Schritte

1. Geben Sie im Abschnitt **Service Endpoint** den Uniform Resource Identifier (URI) ein, der für den Zugriff auf den Blob-Storage-Container verwendet wird, der für den Cloud-Storage-Pool verwendet wird.

Geben Sie den URI in einem der folgenden Formate an:

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

Wenn Sie keinen Port angeben, wird standardmäßig der Port 443 für HTTPS-URIs verwendet, und Port 80 wird für HTTP-URIs verwendet. + * Beispiel-URI für Azure Blob Storage-Container*:

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

2. Geben Sie im Abschnitt **Authentifizierung** folgende Informationen an:
 - a. Geben Sie für **Kontoname** den Namen des Blob-Speicherkontos ein, der den externen Service-Container besitzt.
 - b. Geben Sie für **Kontenschlüssel** den geheimen Schlüssel für das Blob-Speicherkonto ein.



Für Azure-Endpunkte ist die Authentifizierung mit gemeinsamem Schlüssel erforderlich.

3. Wählen Sie im Abschnitt **Server Verification** die Methode aus, mit der das Zertifikat für TLS-Verbindungen zum Cloud-Speicherpool validiert werden soll:

Option	Beschreibung
Verwenden Sie das CA-Zertifikat für das Betriebssystem	Verwenden Sie die auf dem Betriebssystem installierten Standard-CA-Zertifikate, um Verbindungen zu sichern.
Benutzerdefiniertes CA-Zertifikat verwenden	Verwenden Sie ein benutzerdefiniertes CA-Zertifikat. Klicken Sie auf Neu auswählen , und laden Sie das PEM-kodierte Zertifikat hoch.
Verifizieren Sie das Zertifikat nicht	Das für die TLS-Verbindung verwendete Zertifikat wird nicht verifiziert.

4. Klicken Sie Auf **Speichern**.

Beim Speichern eines Cloud-Speicherpools führt StorageGRID Folgendes aus:

- Überprüft, ob der Container und die URI vorhanden sind und ob sie mit den von Ihnen angegebenen Zugangsdaten erreicht werden können.
- Schreibt eine Markierungsdatei in den Container, um sie als Cloud-Storage-Pool zu identifizieren. Entfernen Sie niemals diese Datei, die benannt ist `x-ntap-sgws-cloud-pool-uuid`.

Wenn die Validierung des Cloud-Storage-Pools fehlschlägt, erhalten Sie eine Fehlermeldung, die erklärt, warum die Validierung fehlgeschlagen ist. Möglicherweise wird ein Fehler gemeldet, wenn ein Zertifikatfehler vorliegt oder der angegebene Container nicht bereits vorhanden ist.

Lesen Sie die Anweisungen zur Fehlerbehebung bei Cloud-Speicherpools, beheben Sie das Problem und versuchen Sie dann, den Cloud-Speicherpool erneut zu speichern.

Verwandte Informationen

["Fehlerbehebung Bei Cloud Storage Pools"](#)

Bearbeiten eines Cloud-Speicherpools

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

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.
- Sie müssen über spezifische Zugriffsberechtigungen verfügen.
- Sie müssen die Richtlinien zum Konfigurieren von Cloud-Speicherpools überprüft haben.

Schritte

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

Die Seite Speicherpools wird angezeigt. In der Tabelle Cloud-Storage-Pools werden die vorhandenen Cloud-Storage-Pools aufgeführt.

Cloud Storage Pools

You can add Cloud Storage Pools to ILM rules to store objects outside of the StorageGRID system. A Cloud Storage Pool defines how to access the external bucket or container where objects will be stored.

+ Create	✎ Edit	✕ Remove	Clear Error			
	Pool Name	URI	Pool Type	Container	Used in ILM Rule	Last Error
<input checked="" type="radio"/>	azure-endpoint	https://storagegrid.blob.core.windows.net	azure	azure-3	✓	
<input type="radio"/>	s3-endpoint	https://s3.amazonaws.com	s3	s3-1	✓	
						Displaying 2 pools.

2. Wählen Sie das Optionsfeld für den Cloud-Storage-Pool, den Sie bearbeiten möchten.
3. Klicken Sie Auf **Bearbeiten**.
4. Ändern Sie bei Bedarf den Anzeigenamen, den Dienstendpunkt, die Authentifizierungsdaten oder die Methode zur Zertifikatvalidierung.



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 Clientzertifikat hochgeladen haben, können Sie **Aktuell anzeigen** auswählen, um das aktuell verwendete Zertifikat zu überprüfen.

5. Klicken Sie Auf **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 Zertifikatsfehler vorliegt.

Lesen Sie die Anweisungen zur Fehlerbehebung bei Cloud-Speicherpools, beheben Sie das Problem und versuchen Sie dann, den Cloud-Speicherpool erneut zu speichern.

Verwandte Informationen

["Überlegungen zu Cloud-Storage-Pools"](#)

["Fehlerbehebung Bei Cloud Storage Pools"](#)

Entfernen eines Cloud-Speicherpools

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

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.
- Sie müssen über spezifische Zugriffsberechtigungen verfügen.
- 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 diese Datei nicht, die den Namen trägt `x-ntap-sgws-cloud-pool-uuid`.

- Sie haben bereits alle ILM-Regeln entfernt, die den Pool möglicherweise verwendet haben.

Schritte

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

Die Seite Speicherpools wird angezeigt.

2. Wählen Sie das Optionsfeld für einen Cloud-Storage-Pool aus, der derzeit nicht in einer ILM-Regel verwendet wird.

Sie können einen Cloud-Storage-Pool nicht entfernen, wenn er in einer ILM-Regel verwendet wird. Die Schaltfläche **Entfernen** ist deaktiviert.

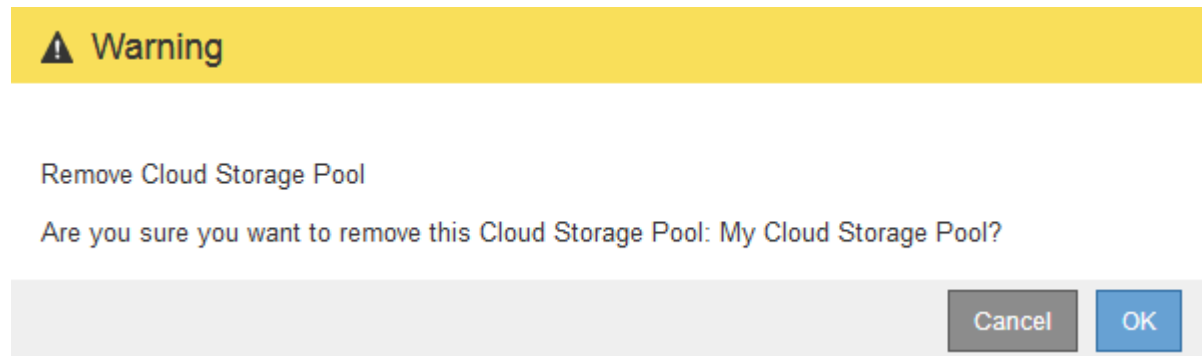
Cloud Storage Pools

You can add Cloud Storage Pools to ILM rules to store objects outside of the StorageGRID system. A Cloud Storage Pool defines how to access the external bucket or container where objects will be stored.

<div>+ Create Edit ✕ Remove Clear Error</div>						
	Pool Name	URI	Pool Type	Container	Used in ILM Rule	Last Error
<input checked="" type="radio"/>	azure-endpoint	https://storagegrid.blob.core.windows.net	azure	azure-3	✓	
<input type="radio"/>	s3-endpoint	https://s3.amazonaws.com	s3	s3-1	✓	
Displaying 2 pools.						

3. Klicken Sie Auf **Entfernen**.

Eine Bestätigungsmeldung wird angezeigt.



4. Klicken Sie auf **OK**.

Der Cloud-Speicherpool wird entfernt.

Verwandte Informationen

["Fehlerbehebung Bei Cloud Storage Pools"](#)

Fehlerbehebung Bei Cloud Storage Pools

Wenn beim Erstellen, Bearbeiten oder Löschen eines Cloud-Speicherpools Fehler auftreten, führen Sie diese Schritte zur Fehlerbehebung durch.

Ermitteln, ob ein Fehler aufgetreten ist

StorageGRID führt einmal pro Minute eine einfache Zustandsprüfung für jeden Cloud Storage Pool durch, um sicherzustellen, dass auf den Cloud Storage Pool zugegriffen werden kann und dass er ordnungsgemäß funktioniert. Wenn die Zustandsprüfung ein Problem feststellt, wird in der Spalte „Letzter Fehler“ der Tabelle „Cloud Storage Pools“ auf der Seite „Speicherpools“ eine Meldung 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.

Cloud Storage Pools

You can add Cloud Storage Pools to ILM rules to store objects outside of the StorageGRID system. A Cloud Storage Pool defines how to access the external bucket or container where objects will be stored.

<div><div>+ Create</div><div>Edit</div><div>Remove</div><div>Clear Error</div></div>					
	Pool Name	URI	Pool Type	Container	Used in ILM Rule
<input checked="" type="radio"/>	S3	10.96.106.142:18082	s3	s3	✓
Endpoint failure: DC2-S1-106-147: Could not create or update Cloud Storage Pool. Error from endpoint: RequestError: send request failed caused by: Get https://10.96.106.142:18082/s3-targetbucket/x-ntap-sgws-cloud-pool-uuid: net/http: request canceled while waiting for connection (Client.Timeout exceeded while awaiting headers) 8 minutes ago					
<input type="radio"/>	Azure	http://pboerkoe@10.96.100.254:10000/d-evstoreaccount1	azure	azure	✓

Displaying 2 pools.

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 Warnmeldung erhalten, gehen Sie auf die Seite Storage Pool (wählen Sie **ILM > Storage Pools**), überprüfen Sie die Fehlermeldungen in der Spalte Letzter

Fehler und lesen Sie die nachfolgenden Hinweise zur Fehlerbehebung.

Überprüfen, 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 das Optionsfeld für den Endpunkt aus, und klicken Sie auf **Fehler löschen**. Eine Bestätigungsmeldung gibt an, dass StorageGRID den Fehler für den Cloud-Speicherpool gelöscht hat.

Error successfully cleared. This error might reappear if the underlying problem is not resolved.



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

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 den enthält `x-ntap-sgws-cloud-pool-uuid` Markierungsdatei, aber diese Datei verfügt nicht über die erwartete UUID.

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.

Versuchen Sie mit diesen Schritten das Problem zu beheben:

- Vergewissern Sie sich, dass niemand in Ihrem Unternehmen diesen Cloud-Speicherpool verwendet.
- Löschen Sie die `x-ntap-sgws-cloud-pool-uuid` Datei und versuchen Sie erneut, den Cloud-Speicherpool zu konfigurieren.

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

Dieser Fehler wird möglicherweise auftreten, wenn Sie versuchen, einen Cloud-Speicherpool zu erstellen oder zu bearbeiten. Dieser Fehler zeigt an, dass eine Art von Verbindungs- oder Konfigurationsproblem darin besteht, dass StorageGRID das Schreiben in den Cloud Storage Pool verhindert.

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

- Wenn die Fehlermeldung enthält `Get url: EOF`, Überprüfen Sie, ob der Service-Endpunkt für den Cloud Storage Pool das HTTP-Protokoll 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 Storage-Knoten Zugriff auf den Service-Endpunkt erlaubt, der für den Cloud Storage Pool verwendet wird.
- 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 Anmeldedaten besitzen keine Leseberechtigung für den Bucket.
- Der für den Cloud-Storage-Pool verwendete Bucket enthält nicht den `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. Ein Cloud-Storage-Pool kann nicht gelöscht werden, wenn er Daten enthält, die durch ILM verschoben wurden, Daten, die sich vor dem Konfigurieren des Cloud-Storage-Pools im Bucket befand, 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:

- Folgen Sie den Anweisungen, um Objekte in „Lifecycle eines Cloud-Storage-Pool-Objekts zurück in StorageGRID zu verschieben.“
- 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 gelöscht 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 zwischen Storage-Nodes einen nicht transparenten Storage Proxy und den 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-Storage-Pools 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**).
- Überprüfen Sie die Netzwerkkonfiguration des Storage Proxy-Servers.

Verwandte Informationen

["Lebenszyklus eines Cloud-Storage-Pool-Objekts"](#)

Konfigurieren von Erasure Coding-Profilen

Sie konfigurieren Erasure Coding-Profile, indem Sie einen Storage Pool mit einem Erasure Coding-Schema wie 6+3 verknüpfen. Wenn Sie dann die Anweisungen zur Platzierung einer ILM-Regel konfigurieren, können Sie das Erasure Coding-Profil auswählen. Entspricht ein Objekt der Regel, werden Daten- und Paritätsfragmente erstellt und gemäß dem Erasure Coding-Schema an die Storage-Standorte im Storage Pool verteilt.

- ["Erstellen eines Erasure Coding-Profils"](#)
- ["Umbenennen eines Erasure Coding-Profils"](#)
- ["Deaktivieren eines Erasure Coding-Profils"](#)

Erstellen eines Erasure Coding-Profils

Um ein Erasure Coding-Profil zu erstellen, verknüpfen Sie einen Speicherpool mit Storage-Nodes mit einem Codierungsschema zur Fehlerkorrektur. Diese Verknüpfung bestimmt die Anzahl der erstellten Daten und Paritäts-Fragmente und wo das System diese Fragmente verteilt.

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.
- Sie müssen über spezifische Zugriffsberechtigungen verfügen.
- Sie müssen einen Speicherpool erstellt haben, der genau einen Standort oder einen Speicherpool umfasst, der drei oder mehr Standorte umfasst. Für einen Storage Pool mit nur zwei Standorten stehen keine Erasure Coding-Schemata zur Verfügung.

Über diese Aufgabe

Die in Erasure Coding-Profilen verwendeten Storage-Pools müssen exakt einen oder drei oder mehr Standorte umfassen. Wenn Sie Standortredundanz bereitstellen möchten, muss der Speicherpool mindestens drei Standorte aufweisen.



Sie müssen einen Speicherpool auswählen, der Speicherknoten enthält. Sie können Archiv-Knoten nicht zum Löschen codierter Daten verwenden.

Schritte

1. Wählen Sie **ILM > Erasure Coding** aus.

Die Seite Erasure Coding Profiles wird angezeigt.

Erasure Coding Profiles

An Erasure Coding profile determines how many data and parity fragments are created and where those fragments are stored.

To create an Erasure Coding profile, select a [storage pool](#) and an erasure coding scheme. The storage pool must include Storage Nodes from exactly one site or from three or more sites. If you want to provide site redundancy, the storage pool must include nodes from at least three sites.

To deactivate an Erasure Coding profile that you no longer plan to use, first remove it from all ILM rules. Then, if the profile is still associated with object data, wait for those objects to be moved to new locations based on the new rules in the active ILM policy. Depending on the number of objects and the size of your StorageGRID system, it might take weeks or even months for the objects to be moved.

See [Managing objects with information lifecycle management](#) for important details.

[+ Create](#) [Rename](#) [Deactivate](#)

Profile	Status	Storage Pool	Storage Nodes	Sites	Erasure Code	Storage Overhead (%)	Storage Node Redundancy	Site Redundancy
---------	--------	--------------	---------------	-------	--------------	----------------------	-------------------------	-----------------

No Erasure Coding profiles found.

2. Klicken Sie Auf **Erstellen**.

Das Dialogfeld EC-Profil erstellen wird angezeigt.

Create EC Profile

You cannot change the selected scheme and storage pool after saving the profile.

Profile Name

Storage Pool

Cancel

Save

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

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



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

From day store [Add](#) [Remove](#)

Type Location Copies [+](#) [x](#)

Erasure Coding profile name

Storage pool name

4. Wählen Sie den Speicherpool aus, den Sie für dieses Erasure Coding-Profil erstellt haben.



Wenn Ihr Grid derzeit nur einen Standort enthält, können Sie den Standardspeicherpool, alle Speicherknoten oder einen beliebigen Speicherpool, der den Standardstandort, Alle Standorte enthält, nicht verwenden. Dieses Verhalten verhindert, dass das Erasure Coding-Profil ungültig wird, wenn ein zweiter Standort hinzugefügt wird.



Wenn ein Speicherpool genau zwei Standorte umfasst, kann er nicht für Erasure Coding verwendet werden. Für einen Speicherpool mit zwei Standorten stehen keine Erasure Coding-Schemata zur Verfügung.

Wenn Sie einen Speicherpool auswählen, wird die Liste der verfügbaren Erasure-Coding-Schemata angezeigt, basierend auf der Anzahl der Speicherknoten und Standorte im Pool.

Create EC Profile

You cannot change the selected scheme and storage pool after saving the profile.

Profile Name  6 plus 3

Storage Pool  All 3 Sites

9 Storage Nodes across 3 site(s)

Scheme

	Erasure Code 	Storage Overhead (%) 	Storage Node Redundancy 	Site Redundancy 
<input checked="" type="radio"/>	6+3	50%	3	Yes
<input type="radio"/>	2+1	50%	1	Yes
<input type="radio"/>	4+2	50%	2	Yes

Cancel

Save

Die folgenden Informationen sind für jedes verfügbare Erasure Coding-Schema aufgeführt:

- **Erasure Code:** Der Name des Erasure-Codierungsschemas im folgenden Format: Datenfragmente + Paritätsfragmente.
- **Storage Overhead (%):** Der zusätzliche Speicher, der für Paritäts-Fragmente im Verhältnis zur Datengröße des Objekts benötigt wird. Storage Overhead = Gesamtzahl der Parity-Fragmente / Gesamtzahl an Datenfragmenten
- **Speicherknoten-Redundanz:** Die Anzahl der Speicherknoten, die verloren gehen können, während weiterhin die Fähigkeit, Objektdaten abzurufen.
- **Standortredundanz:** Ob der ausgewählte Lösocode die Objektdaten bei Verlust eines Standorts abrufen lässt.

Um Standortredundanz zu unterstützen, muss der ausgewählte Speicherpool mehrere Standorte umfassen, von denen jeder über genügend Storage-Nodes verfügt, damit jeder Standort verloren geht. Beispielsweise muss der ausgewählte Speicherpool mindestens drei Standorte mit mindestens drei Storage-Nodes an jedem Standort enthalten, um die Standortredundanz mithilfe eines Erasure Coding-Schemas von 6+3 zu unterstützen.

In den folgenden Fällen werden Meldungen angezeigt:

- Der ausgewählte Speicherpool bietet keine Standortredundanz. Die folgende Meldung wird erwartet, wenn der ausgewählte Speicherpool nur einen Standort umfasst. Sie können dieses Erasure Coding-Profil in ILM-Regeln verwenden, um sich vor Node-Ausfällen zu schützen.

Scheme

	Erasure Code ?	Storage Overhead (%) ?	Storage Node Redundancy ?	Site Redundancy ?
<input checked="" type="radio"/>	2+1	50%	1	No

The selected storage pool and erasure coding scheme cannot protect object data from loss if a site is lost.
To provide site redundancy, the storage pool must have at least three sites.

- Der ausgewählte Speicherpool erfüllt nicht die Anforderungen für ein Erasure Coding-Schema. Zum Beispiel wird die folgende Meldung erwartet, wenn der ausgewählte Speicherpool genau zwei Standorte umfasst. Um Objektdaten mit Erasure Coding zu sichern, müssen Sie einen Storage-Pool mit genau einem Standort oder einem Storage-Pool mit drei oder mehr Standorten auswählen.

Scheme

	Erasure Code ?	Storage Overhead (%) ?	Storage Node Redundancy ?	Site Redundancy ?
--	----------------	------------------------	---------------------------	-------------------

No erasure coding schemes are supported for the selected storage pool because it contains two sites. You must select a storage pool that contains exactly one site or a storage pool that contains at least three sites.

- Das Grid enthält nur einen Standort, und Sie haben den Standardspeicherpool, alle Speicherknoten oder einen beliebigen Speicherpool ausgewählt, der den Standardstandort, Alle Standorte enthält.

Create EC Profile

You cannot change the selected scheme and storage pool after saving the profile.

Profile Name

Storage Pool ▼
3 Storage Nodes across 1 site(s)

Scheme

	Erasure Code	Storage Overhead (%)	Storage Node Redundancy	Site Redundancy

No erasure coding schemes are available for the selected storage pool. The storage pool includes the **All Sites** site, so it cannot be used in an Erasure Coding profile for a one-site grid.


Cancel


Save

- Das von Ihnen ausgewählte Erasure Coding-Schema und der ausgewählte Speicherpool überschneiden sich mit einem anderen Erasure Coding-Profil.

Create EC Profile

You cannot change the selected scheme and storage pool after saving the profile.

Profile Name  2 plus 1 for three sites

Storage Pool  All 3 Sites

9 Storage Nodes across 3 site(s)

Scheme

	Erasure Code 	Storage Overhead (%) 	Storage Node Redundancy 	Site Redundancy 
<input type="radio"/>	6+3	50%	3	Yes
<input checked="" type="radio"/>	2+1	50%	1	Yes
<input type="radio"/>	4+2	50%	2	Yes

The selected storage pool and erasure coding scheme overlap an existing Erasure Coding profile. Use caution if you apply this new profile to objects already protected by the other profile. When a new profile is applied to existing erasure-coded objects, entirely new erasure-coded fragments are created, which might cause resource issues.

Cancel

Save

In diesem Beispiel wird eine Warnmeldung angezeigt, weil ein anderes Erasure Coding-Profil das 2+1-Schema verwendet und der Speicherpool für das andere Profil auch einen der Standorte im Speicherpool Alle 3 Standorte verwendet.

Obwohl Sie nicht daran gehindert werden, dieses neue Profil zu erstellen, müssen Sie sehr vorsichtig sein, wenn Sie es in der ILM-Richtlinie verwenden. Wird dieses neue Profil auf vorhandene Objekte angewendet, die mit Erasure-Coding-Verfahren versehen sind und bereits durch das andere Profil geschützt sind, erstellt StorageGRID einen völlig neuen Satz von Objektfragmenten. Die vorhandenen 2+1-Fragmente werden nicht wiederverwendet. Bei der Migration von einem Erasure Coding-Profil zum anderen können Ressourcenprobleme auftreten, auch wenn die Erasure Coding-Schemata identisch sind.

5. Wenn mehr als ein Erasure-Coding-Schema aufgeführt ist, wählen Sie das gewünschte Schema aus.

Bei der Entscheidung, welches Erasure-Coding-Schema verwendet werden soll, sollten Sie die Fehlertoleranz (die durch mehr Paritätssegmente erzielt wird) mit den Anforderungen des Netzwerkverkehrs für Reparaturen abgleichen (mehr Fragmente entsprechen mehr Netzwerkverkehr). Wenn Sie beispielsweise zwischen einem Schema 4+2 und 6+3 entscheiden, wählen Sie das Schema 6+3 aus, wenn zusätzliche Parität und Fehlertoleranz erforderlich sind. Wählen Sie das Schema 4+2 aus, wenn die Netzwerkressourcen eingeschränkt sind, um den Netzwerkverbrauch bei Node-Reparaturen zu reduzieren.

6. Klicken Sie Auf **Speichern**.

Umbenennen eines Erasure Coding-Profiles

Vielleicht möchten Sie ein Erasure Coding-Profil umbenennen, um es offensichtlicher zu machen, was das Profil tut.

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.

- Sie müssen über spezifische Zugriffsberechtigungen verfügen.

Schritte

1. Wählen Sie **ILM > Erasure Coding** aus.

Die Seite Erasure Coding Profiles wird angezeigt. Die Schaltflächen **Umbenennen** und **Deaktivieren** sind beide deaktiviert.

<div> + Create ✎ Rename ⏻ Deactivate </div>									
Profile	Status	Storage Pool	Storage Nodes	Sites	Erasure Code	Storage Overhead (%)	Storage Node Redundancy	Site Redundancy	
<input type="radio"/> DC1 2-1		DC1	3	1	2+1	50	1	No	
<input type="radio"/> DC2 2-1		DC2	3	1	2+1	50	1	No	
<input type="radio"/> DC3 2-1		DC3	3	1	2+1	50	1	No	
<input checked="" type="radio"/> All sites 6-3	Deactivated	All 3 Sites	9	3	6+3	50	3	Yes	

2. Wählen Sie das Profil aus, das Sie umbenennen möchten.

Die Schaltflächen **Umbenennen** und **Deaktivieren** werden aktiviert.

3. Klicken Sie Auf **Umbenennen**.

Das Dialogfeld EC-Profil umbenennen wird angezeigt.

Rename EC Profile

Profile Name

Cancel

Save

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

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

From day
store

Add Remove

Type
Location
Copies

+ x

Erasure Coding profile name

Storage pool name



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

5. Klicken Sie Auf **Speichern**.

Deaktivieren eines Erasure Coding-Profiles

Sie können ein Erasure Coding-Profil deaktivieren, wenn Sie es nicht mehr verwenden


möchten und wenn das Profil derzeit in keiner ILM-Regel verwendet wird.

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.
- Sie müssen über spezifische Zugriffsberechtigungen verfügen.
- Sie müssen bestätigt haben, dass keine entsprechend dem Erasure-Coding-Verfahren zur Reparatur von Daten oder zur Ausmusterung durchgeführten Verfahren ausgeführt werden. Wenn Sie versuchen, ein Erasure Coding-Profil zu deaktivieren, während einer dieser Vorgänge ausgeführt wird, wird eine Fehlermeldung zurückgegeben.

Über diese Aufgabe

Wenn Sie ein Erasure Coding-Profil deaktivieren, wird das Profil auf der Seite Erasure Coding Profiles weiterhin angezeigt, der Status ist jedoch **deactivated**.

+ Create	 Rename	 Deactivate							
	Profile	Status	Storage Pool	Storage Nodes	Sites	Erasure Code	Storage Overhead (%)	Storage Node Redundancy	Site Redundancy
<input type="radio"/>	DC1 2-1		DC1	3	1	2+1	50	1	No
<input type="radio"/>	DC2 2-1		DC2	3	1	2+1	50	1	No
<input type="radio"/>	DC3 2-1		DC3	3	1	2+1	50	1	No
<input checked="" type="radio"/>	All sites 6-3	Deactivated	All 3 Sites	9	3	6+3	50	3	Yes

Sie können kein deaktiviertes Erasure-Coding-Profil mehr verwenden. Ein deaktiviertes Profil wird nicht angezeigt, wenn Sie die Platzierungsanweisungen für eine ILM-Regel erstellen. Ein deaktiviertes Profil kann nicht reaktiviert werden.

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

- Das Erasure Coding-Profil wird derzeit in einer ILM-Regel verwendet.
- Das Erasure Coding-Profil wird in keiner ILM-Regel mehr verwendet. Objektdaten und Paritätsfragmente für das Profil sind jedoch weiterhin vorhanden.



Schritte

1. Wählen Sie **ILM > Erasure Coding** aus.

Die Seite Erasure Coding Profiles wird angezeigt. Die Schaltflächen **Umbenennen** und **Deaktivieren** sind beide deaktiviert.

2. Überprüfen Sie in der Spalte **Status**, ob das zu deaktivierungssyquente Erasure-Coding-Profil nicht in ILM-Regeln verwendet wird.

Ein Erasure Coding-Profil kann nicht deaktiviert werden, wenn es in einer ILM-Regel verwendet wird. Im Beispiel wird das **2_1 EC-Profil** in mindestens einer ILM-Regel verwendet.

+ Create	 Rename	 Deactivate							
	Profile	Status	Storage Pool	Storage Nodes	Sites	Erasure Code	Storage Overhead (%)	Storage Node Redundancy	Site Redundancy
<input type="radio"/>	2_1 EC Profile	Used In ILM Rule	DC1	3	1	2+1	50	1	No
<input type="radio"/>	Site 1 EC Profile	Deactivated	DC1	3	1	2+1	50	1	No

3. Wenn das Profil in einer ILM-Regel verwendet wird, führen Sie die folgenden Schritte aus:

- a. Wählen Sie **ILM > Regeln**.
- b. Wählen Sie für jede der aufgeführten Regeln das Optionsfeld aus, und überprüfen Sie das Aufbewahrungsdigramm, um festzustellen, ob die Regel das Erasure-Coding-Profil verwendet, das Sie deaktivieren möchten.

Im Beispiel verwendet die Regel **drei Seiten-EC für größere Objekte** einen Speicherpool mit dem Namen **Alle 3 Standorte** und das Profil **Alle Standorte 6-3** Erasure Coding. Dieses Symbol repräsentiert die Profile von Erasure Coding:

ILM Rules
Information lifecycle management (ILM) rules determine how and where object data is stored over time. Every object ingested into StorageGRID is evaluated against the ILM rules that make up the active ILM policy. Use this page to manage and view ILM rules. You cannot edit or remove an ILM rule that is used by an active or proposed ILM policy.

+ Create

Clone

Edit

Remove

Name	Used In Active Policy	Used In Proposed Policy
2 copy replication for smaller objects		
Three site EC for larger objects	✓	
Make 2 Copies		

Three site EC for larger objects

Description:

6-3 erasure coding at 3 sites for objects larger than 200 KB

Ingest Behavior:

Balanced

Reference Time:

Ingest Time

Filtering Criteria:

Matches all of the following metadata:

System Metadata

Object Size (MB)

greater than

0.2

Retention Diagram:

Trigger

Day 0

All 3 Sites
(All sites 6-3)

Forever

- a. Wenn die ILM-Regel das Erasure Coding-Profil verwendet, das Sie deaktivieren möchten, stellen Sie fest, ob die Regel entweder in der aktiven ILM-Richtlinie oder in einer vorgeschlagenen Richtlinie verwendet wird.

Im Beispiel wird die Regel **drei Standorte EC für größere Objekte** in der aktiven ILM-Richtlinie verwendet.

- b. Führen Sie die zusätzlichen Schritte in der Tabelle aus, wobei 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.	None

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 noch nie in einer ILM-Richtlinie verwendet wurde	<ul style="list-style-type: none"> 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 mit ILM-Regeln und ILM-Richtlinien"
In einer ILM-Regel, die sich derzeit in der aktiven ILM-Richtlinie befindet	<ul style="list-style-type: none"> i. Klonen der aktiven Richtlinie ii. Entfernen Sie die ILM-Regel, die das Erasure Coding-Profil 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. <p>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.</p> <p>Während 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.</p> <ul style="list-style-type: none"> 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. 	<ul style="list-style-type: none"> • "ILM-Richtlinie erstellen" • "Arbeiten 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 vorgeschlagenen ILM-Richtlinie befindet	<ul style="list-style-type: none"> i. Bearbeiten Sie die vorgeschlagene Richtlinie. ii. Entfernen Sie die ILM-Regel, die das Erasure Coding-Profil verwendet. iii. Fügen Sie ein oder mehrere neue ILM-Regeln hinzu, um sicherzustellen, dass alle Objekte geschützt sind. iv. Speichern Sie die vorgeschlagene 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. 	<ul style="list-style-type: none"> • "ILM-Richtlinie erstellen" • "Arbeiten mit ILM-Regeln und ILM-Richtlinien"
In einer ILM-Regel, die sich in einer historischen ILM-Richtlinie befindet	<ul style="list-style-type: none"> i. Bearbeiten oder löschen Sie die Regel. Wenn Sie die Regel bearbeiten, entfernen Sie alle Platzierungen, die das Erasure Coding-Profil verwenden. (Die Regel wird nun als historische Regel in der historischen Richtlinie angezeigt.) ii. Fahren Sie mit diesem Verfahren fort. 	<ul style="list-style-type: none"> • "Arbeiten mit ILM-Regeln und ILM-Richtlinien"

c. Aktualisieren Sie die Seite Erasure Coding Profiles, 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 EC-Profil deaktivieren wird angezeigt.



5. Wenn Sie sicher sind, dass Sie das Profil deaktivieren möchten, wählen Sie **Deactivate**.
- Wenn StorageGRID das Erasure-Coding-Profil deaktivieren kann, lautet sein Status **deaktiviert**. Sie können dieses Profil nicht mehr für eine ILM-Regel auswählen.

- 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.

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.
- Sie müssen über spezifische Zugriffsberechtigungen verfügen.

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. Sie können zum Beispiel eine Regel entwerfen, die sich nur auf Objekte bezieht, die in den in us-West-2 erstellten S3-Buckets gelten. 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 zu 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 regionalen Namen wird zwischen Groß- und Kleinschreibung unterschieden. Das Unternehmen muss mindestens 2 und nicht mehr als 32 Zeichen enthalten. 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.

- Eine Region kann nicht gelöscht oder geändert werden, wenn sie derzeit in der aktiven ILM-Richtlinie oder der vorgeschlagenen ILM-Richtlinie verwendet wird.
- Wenn die Region, die als erweiterter Filter in einer ILM-Regel verwendet wird, ungültig ist, kann diese Regel noch zur vorgeschlagenen Richtlinie hinzugefügt werden. Es tritt jedoch ein Fehler auf, wenn Sie versuchen, die vorgeschlagene Richtlinie zu speichern oder zu aktivieren. (Eine ungültige Region kann dazu führen, dass Sie eine Region als erweiterten Filter in einer ILM-Regel verwenden, diese Region später jedoch löschen oder wenn Sie die Grid Management API verwenden, um eine Regel zu erstellen und eine Region anzugeben, 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, `us-east-1`, Die nicht geändert oder entfernt werden kann.

Regions (optional and S3 only)

Define any regions you want to use for the Location Constraint advanced filter in ILM rules. Then, use these exact names when creating S3 buckets. (Region names are case sensitive.)

The screenshot shows the 'Regions' page in the AWS IAM console. It displays a table with two regions: 'Region 1' with the name 'us-east-1 (required)' and 'Region 2' with the name 'us-west-1'. The 'us-east-1' region is marked as required and is disabled. The 'us-west-1' region is active. To the right of the 'us-west-1' entry are plus and minus icons for adding or removing regions. Below the table is a blue 'Save' button.

2. So fügen Sie eine Region hinzu:

- a. Klicken Sie auf das INSERT-Symbol **+** Rechts neben dem letzten Eintrag.
- 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 eine nicht verwendete Region zu entfernen, klicken Sie auf das Löschsymbolsymbol **×**.

Wenn Sie versuchen, eine Region zu entfernen, die derzeit in der aktiven Richtlinie oder der vorgeschlagenen Richtlinie verwendet wird, wird eine Fehlermeldung angezeigt.

4. Wenn Sie Änderungen vorgenommen haben, klicken Sie auf **Speichern**.

Sie können diese Regionen nun aus der Liste **Location Constraint** auf der Seite Advanced Filtering des Assistenten Create ILM rule auswählen.

Verwandte Informationen

["Verwendung erweiterter Filter in ILM-Regeln"](#)

Erstellen einer ILM-Regel

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

Bevor Sie beginnen

- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.
- Sie müssen über spezifische Zugriffsberechtigungen verfügen.
- Wenn Sie angeben möchten, für welche Mandantenkonten diese Regel gilt, müssen Sie über die Berechtigung für Mandantenkonten verfügen, oder Sie müssen die Konto-ID für jedes Konto kennen.
- Wenn die Regel Objekte nach Metadaten der letzten Zugriffszeit filtern soll, müssen Updates der letzten Zugriffszeit für S3 oder für Swift nach Container aktiviert werden.
- Falls Sie replizierte Kopien erstellen, müssen Sie alle Storage-Pools oder Cloud-Storage-Pools konfiguriert haben, die Sie verwenden möchten.
- Wenn Sie Kopien mit Erasure Coding erstellen, müssen Sie ein Erasure Coding-Profil konfiguriert haben.
- Sie müssen mit dem vertraut sein ["Datensicherungsoptionen für die Aufnahme"](#).
- Wenn Sie eine konforme Regel für die Verwendung mit S3 Object Lock erstellen müssen, müssen Sie mit dem vertraut sein ["Anforderungen für die S3-Objektsperre"](#).



Verwenden Sie stattdessen dieses Verfahren, um die ILM-Standardregel für eine Richtlinie zu erstellen: ["Erstellen einer Standard-ILM-Regel"](#).

Über diese Aufgabe

Wenn ILM-Regeln erstellt werden:

- Dabei sind die Topologie und Storage-Konfigurationen des StorageGRID Systems zu berücksichtigen.
- Es sollte berücksichtigt werden, welche Arten von Objektkopien Sie erstellen möchten (replizierte oder Erasure Coding) und wie viele Kopien der einzelnen Objekte erforderlich sind.
- 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, welche Option für die Datensicherungsoption bei Aufnahme verwendet werden soll (ausgewogen, streng oder Dual-Commit)

Schritte

1. Wählen Sie **ILM > Regeln**.

Die Seite ILM-Regeln wird angezeigt, wobei die Bestandsregel 2 Kopien erstellen soll, ausgewählt.

ILM Rules

Information lifecycle management (ILM) rules determine how and where object data is stored over time. Every object ingested into StorageGRID is evaluated against the ILM rules that make up the active ILM policy. Use this page to manage and view ILM rules. You cannot edit or remove an ILM rule that is used by an active or proposed ILM policy.

[+ Create](#) [Clone](#) [Edit](#) [Remove](#)

Name	Used In Active Policy	Used In Proposed Policy
Make 2 Copies	✓	

Make 2 Copies

Ingest Behavior: Dual commit

Reference Time: Ingest Time

Filtering Criteria:

Matches all objects.

Retention Diagram:

Trigger

Day 0

All Storage Nodes

Duration

Forever



Die Seite ILM-Regeln sieht etwas anders aus, wenn die globale S3-Objektsperre für das StorageGRID System aktiviert wurde. Die Übersichtstabelle enthält eine **Compliant**-Spalte, und die Details für die ausgewählte Regel enthalten ein **Compliant**-Feld.

2. Wählen Sie **Erstellen**.

Schritt 1 (Grundlagen definieren) des Assistenten „ILM-Regel erstellen“ wird angezeigt. Auf der Seite Grundlagen definieren können Sie definieren, für welche Objekte die Regel gilt.

Verwandte Informationen

["S3 verwenden"](#)

["Verwenden Sie Swift"](#)

["Konfigurieren von Erasure Coding-Profilen"](#)

["Konfigurieren von Speicherpools"](#)

["Verwendung Von Cloud Storage Pools"](#)

["Datensicherungsoptionen für die Aufnahme"](#)

["Verwalten von Objekten mit S3 Object Lock"](#)

Schritt 1 von 3: Grundlagen definieren

Schritt 1 (Grundlagen definieren) des Assistenten „ILM-Regel erstellen“ ermöglicht es Ihnen, die grundlegenden und erweiterten Filter der Regel zu definieren.

Über diese Aufgabe

Bei der Bewertung eines Objekts mit einer ILM-Regel vergleicht StorageGRID die Objekt-Metadaten 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.

Create ILM Rule Step 1 of 3: Define Basics

Name

Description

Tenant Accounts (optional)

Bucket Name

[Advanced filtering...](#) (0 defined)

Cancel

Next

Schritte

1. Geben Sie im Feld **Name** einen eindeutigen Namen für die Regel ein.

Sie müssen 1 bis 64 Zeichen eingeben.

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.

Name

Description

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

Wenn Sie nicht über die Berechtigung Stammzugriff oder 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. Geben Sie optional die S3-Buckets oder Swift-Container an, für die diese Regel gilt.

Wenn **entspricht allen** ausgewählt ist (Standard), gilt die Regel für alle S3-Buckets oder Swift-Container.

5. Wählen Sie optional **Erweiterte Filterung**, um zusätzliche Filter festzulegen.

Wenn Sie keine erweiterte Filterung konfigurieren, gilt die Regel für alle Objekte, die den grundlegenden Filtern entsprechen.



Wenn diese Regel mit dem Löschen kodierte Kopien erstellt, wählen Sie **Erweiterte Filterung**. Fügen Sie dann den erweiterten Filter **Objektgröße (MB)** hinzu und setzen Sie ihn auf **größer als 0.2**. Der Größenfilter stellt sicher, dass Objekte, die 2 MB oder kleiner sind, nicht gelöscht werden.

6. Wählen Sie **Weiter**.

Schritt 2 (Platzierungen definieren) wird angezeigt.

Verwandte Informationen

["Was ist die ILM-Regelfilterung"](#)

["Verwendung erweiterter Filter in ILM-Regeln"](#)

["Schritt 2 von 3: Definieren von Platzierungen"](#)

Verwendung erweiterter 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 (Mikrosekunden)	<ul style="list-style-type: none">• Gleich• Ist nicht gleich• Kleiner als• Weniger als oder gleich• Größer als• Größer als oder gleich	<p>Uhrzeit und Datum, an dem das Objekt aufgenommen wurde.</p> <p>Hinweis: 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 die Aufnahmezeit auf größer oder gleich der ungefähren Zeit fest, zu der die neue Richtlinie in Kraft tritt, um sicherzustellen, dass vorhandene Objekte nicht unnötig verschoben werden.</p>
Taste	<ul style="list-style-type: none">• Gleich• Ist nicht gleich• Enthält• Enthält nicht• Beginnt mit• Startet nicht mit• Endet mit• Endet nicht mit	<p>Der gesamte Objektschlüssel oder Teil eines eindeutigen S3- oder Swift-Objektschlüssels.</p> <p>Beispielsweise können Sie Objekte, die mit enden, aufeinander abstimmen <code>.txt</code> Oder beginnen Sie mit <code>test-object/</code>.</p>

Metadatatyp	Unterstützte Operatoren	Metadatenwert
Zeitpunkt des letzten Zugriffs (Mikrosekunden)	<ul style="list-style-type: none"> • Gleich • Ist nicht gleich • Kleiner als • Weniger als oder gleich • Größer als • Größer als oder gleich • Vorhanden • Nicht vorhanden 	<p>Uhrzeit und Datum, an dem das Objekt zuletzt abgerufen wurde (gelesen oder angezeigt).</p> <p>Hinweis: Wenn Sie die letzte Zugriffszeit als erweiterten Filter verwenden möchten, müssen Updates der letzten Zugriffszeit für den S3-Bucket oder Swift-Container aktiviert sein.</p> <p>"Verwenden der Zeit für den letzten Zugriff in ILM-Regeln"</p>
Speicherortbeschränkung (nur S3)	<ul style="list-style-type: none"> • Gleich • Ist nicht gleich 	<p>Die Region, in der ein S3-Bucket erstellt wurde. Verwenden Sie ILM > Regionen, um die angezeigten Regionen zu definieren.</p> <p>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.</p> <p>"Regionen konfigurieren (nur optional und S3)"</p>
Objektgröße (MB)	<ul style="list-style-type: none"> • Gleich • Nicht gleich • Kleiner als • Weniger als oder gleich • Größer als • Größer als oder gleich 	<p>Die Größe des Objekts in MB.</p> <p>Um nach Objektgrößen kleiner als 1 MB zu filtern, geben Sie einen Dezimalwert ein. Stellen Sie beispielsweise den erweiterten Filter Objektgröße (MB) auf größer als 0.2 für jede Regel ein, die eine Löschkopie erstellt. Mit dieser Einstellung wird sichergestellt, dass das Erasure Coding nicht für Objekte mit einer Größe von 200 KB verwendet wird.</p> <p>Hinweis: Ihr Browsertyp und die Gebietseinstellungen steuern, ob Sie einen Punkt oder ein Komma als Dezimaltrennzeichen verwenden müssen.</p>

Metadatentyp	Unterstützte Operatoren	Metadatenwert
Benutzermetadaten	<ul style="list-style-type: none"> • Enthält • Endet mit • Gleich • Vorhanden • Enthält nicht • Endet nicht mit • Ist nicht gleich • Nicht vorhanden • Startet nicht mit • Beginnt mit 	<p>Schlüssel-Wert-Paar, wobei User Metadata Name der Schlüssel ist und User Metadata Value der Wert ist.</p> <p>Zum Beispiel nach Objekten mit Benutzer-Metadaten von <code>filtern color=blue</code>, Spezifizieren <code>color</code> Für User Metadata Name, <code>equals</code> Für den Bediener, und <code>blue</code> Für User Metadata Value.</p> <p>Hinweis: Benutzer-Metadaten Namen sind nicht Groß-/Kleinschreibung; Benutzer-Metadaten-Werte sind Groß-/Kleinschreibung.</p>
Objekt-Tag (nur S3)	<ul style="list-style-type: none"> • Enthält • Endet mit • Gleich • Vorhanden • Enthält nicht • Endet nicht mit • Ist nicht gleich • Nicht vorhanden • Startet nicht mit • Beginnt mit 	<p>Schlüssel-Wert-Paar, wobei Objekt-Tag-Name der Schlüssel und Objekt-Tag-Wert der Wert ist.</p> <p>Zum Beispiel, um nach Objekten zu filtern, die ein Objekt-Tag von haben <code>Image=True</code>, Spezifizieren <code>Image</code> Für Objekt-Tag-Name, <code>equals</code> Für den Bediener, und <code>True</code> Für Objekt-Tag-Wert.</p> <p>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.</p>

Angeben mehrerer Metadatentypen und -Werte

Wenn Sie die erweiterte Filterung definieren, können Sie mehrere Metadatentypen und mehrere Metadatenwerte angeben. Wenn Sie beispielsweise eine Regel für Objekte zwischen 10 MB und 100 MB Größe festlegen möchten, wählen Sie den Metadatentyp **Objektgröße** aus und geben zwei Metadaten 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.

Advanced Filtering

Use advanced filtering if you want a rule to apply only to specific objects. You can filter objects based on their system metadata, user metadata, or object tags (S3 only). When objects are evaluated, the rule is applied if the object's metadata matches the criteria in the advanced filter.

Objects between 10 and 100 MB

Matches all of the following metadata:

Object Size (MB)	greater than or equals	10	 
Object Size (MB)	less than or equals	100	 
 			

Cancel

Remove Filters

Save

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

Advanced Filtering

Use advanced filtering if you want a rule to apply only to specific objects. You can filter objects based on their system metadata, user metadata, or object tags (S3 only). When objects are evaluated, the rule is applied if the object's metadata matches the criteria in the advanced filter.

Multiple filters

Matches all of the following metadata:

User Metadata

camera_type

equals

Brand A

+

x

+

x

Or matches all of the following metadata:

User Metadata

camera_type

equals

Brand B

+

x

Object Size (MB)

less than or equals

10

+

x

+

x

Cancel

Remove Filters

Save

Verwandte Informationen

["Verwenden der Zeit für den letzten Zugriff in ILM-Regeln"](#)

["Regionen konfigurieren \(nur optional und S3\)"](#)

Schritt 2 von 3: Definieren von Platzierungen

Schritt 2 (Platzierungen definieren) des Assistenten zur Erstellung von ILM-Regeln können Sie die Anweisungen zur Platzierung festlegen, um festzulegen, wie lange Objekte gespeichert werden, wie viel Kopien (repliziert oder Erasure Coding), den Storage-Standort und die Anzahl der Kopien erstellt werden.

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.

Diese Beispiel-ILM-Regel erstellt zwei replizierte Kopien für das erste Jahr. Jede Kopie wird in einem Speicherpool an einem anderen Standort gespeichert. Nach einem Jahr wird eine 2+1-Kopie mit Erasure-

Coding-Verfahren an nur einem Standort erstellt und gespeichert.

Create ILM Rule Step 2 of 3: Define Placements

Configure placement instructions to specify how you want objects matched by this rule to be stored.

Example rule
Two copies for one year, then EC forever

Reference Time
Ingest Time

Placements Sort by start day

From day 0 store for 365 days Add Remove

Type replicated Location DC1 x DC2 x Add Pool Copies 2 + x

Specifying multiple storage pools might cause data to be stored at the same site if the pools overlap. See [Managing objects with information lifecycle management](#) for more information.

From day 365 store forever Add Remove

Type erasure coded Location DC1 (2 plus 1) Copies 1 + x

Retention Diagram Refresh

Trigger

Day 0

Year 1

Duration

1 years

Forever

DC1

DC2

DC1 (2 plus 1)

Cancel

Back

Next

Schritte

1. Wählen Sie für **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.
Zeitpunkt Des Letzten Zugriffs	<div>Die Zeit, zu der das Objekt zuletzt abgerufen (gelesen oder angezeigt) wurde.</div> <div>Hinweis: um diese Option zu nutzen, müssen Updates zur letzten Zugriffszeit für den S3-Bucket oder Swift-Container aktiviert sein.</div> <div>"Verwenden der Zeit für den letzten Zugriff in ILM-Regeln"</div>

94

Option	Beschreibung
Nicht Aktuelle Zeit	<p>Die Zeit, in der eine Objektversion nicht mehr aktuell wurde, weil eine neue Version aufgenommen und als aktuelle Version ersetzt wurde.</p> <p>Hinweis: die nicht aktuelle Zeit gilt nur für S3-Objekte in Versionierungsfähigen Buckets.</p> <p>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 S3-Objekte.“</p>
Benutzerdefinierte Erstellungszeit	Eine in benutzerdefinierten Metadaten angegebene Zeit.



Wenn Sie eine konforme Regel erstellen möchten, müssen Sie **Aufnahmezeit** auswählen.

2. Wählen Sie im Abschnitt **Platzierungen** eine Startzeit und eine Dauer für den ersten Zeitraum aus.

Sie können beispielsweise festlegen, wo Objekte für das erste Jahr gespeichert werden sollen („day 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 **Typ** die Option **repliziert** aus.
- b. Wählen Sie im Feld **Standort** für jeden Speicherpool, den Sie hinzufügen möchten, **Pool hinzufügen** aus.

Wenn Sie nur einen Speicherpool angeben, beachten Sie, dass StorageGRID nur eine replizierte Kopie eines Objekts auf einem beliebigen Speicherknoten speichern kann. Wenn Ihr Grid 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 kleiner als die Anzahl der Storage-Pools ist, verteilt das System die Kopien, damit die Festplattennutzung zwischen den Pools ausgeglichen bleibt. Gleichzeitig wird sichergestellt, dass an keinem Standort mehr als eine Kopie eines Objekts gespeichert wird.
- Wenn sich die Speicherpools überschneiden (die gleichen Storage-Nodes enthalten), werden möglicherweise alle Kopien des Objekts an nur einem Standort gespeichert. Geben Sie aus diesem Grund nicht den Standardpool Alle Speicherknoten und einen anderen Speicherpool an.

Placements ⓘ Sort by start day

From day store **Add** **Remove**

Type Location Copies + x

Specifying multiple storage pools might cause data to be stored at the same site if the pools overlap. See [Managing objects with information lifecycle management](#) for more information.

c. 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. Wenn nur eine replizierte Kopie eines Objekts während eines Zeitraums vorhanden ist, geht dieses Objekt verloren, wenn ein Storage Node ausfällt oder einen beträchtlichen Fehler aufweist. Während Wartungsarbeiten wie Upgrades verlieren Sie auch vorübergehend den Zugriff auf das Objekt.



Placements ⓘ Sort by start day

From day store **Add** **Remove**

Type Location **Copies** Temporary location + x

An ILM rule that creates only one replicated copy for any time period puts data at risk of permanent loss. [View additional details](#).

Um diese Risiken zu vermeiden, führen Sie einen oder mehrere der folgenden Schritte aus:

- Erhöhen Sie die Anzahl der Kopien für den Zeitraum.
- Klicken Sie auf das Pluszeichen-Symbol **+** Um während des Zeitraums zusätzliche Kopien zu erstellen. Wählen Sie dann einen anderen Speicherpool oder einen Cloud-Speicherpool aus.
- Wählen Sie **Erase Coded** für Typ, statt **repliziert**. Sie können diese Warnung ohne Bedenken ignorieren, wenn diese Regel bereits mehrere Kopien für alle Zeiträume erstellt.

d. Wenn Sie nur einen Speicherpool angegeben haben, ignorieren Sie das Feld **temporärer Standort**.



Temporäre Speicherorte sind veraltet und werden in einer zukünftigen Version entfernt.

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

- a. Wählen Sie aus der Dropdown-Liste **Typ** die Option **repliziert** aus.
- b. Wählen Sie im Feld **Ort** die Option **Pool hinzufügen** aus. Wählen Sie dann einen Cloud-Speicherpool aus.

From day store **Add** **Remove**

Type Location **Copies** + x

Add Pool

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

- Sie können nicht mehr als einen Cloud-Storage-Pool in einer einzelnen Speicheranweisung auswählen. Auf ähnliche Weise können Sie keinen Cloud-Storage-Pool und einen Storage-Pool in derselben Speicheranweisung auswählen.

Type Location Copies

If you want to use a Cloud Storage Pool, you must remove any other storage pools or Cloud Storage Pools from this placement instruction.

- 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.
- Sie können nicht mehr als eine Objektkopie in einem Cloud-Speicherpool gleichzeitig speichern. 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.

Placements [?](#) Sort by start day

From day store days

Type	Location	Copies	
<input type="text" value="replicated"/>	<input type="text" value="csp1"/> <input type="text" value="Add Pool"/>	<input type="text" value="1"/>	<input type="button" value="+"/> <input type="button" value="x"/>
<input type="text" value="replicated"/>	<input type="text" value="csp2"/> <input type="text" value="Add Pool"/>	<input type="text" value="1"/>	<input type="button" value="+"/> <input type="button" value="x"/>

A rule cannot store more than one object copy in any Cloud Storage Pool at the same time. You must remove one of the Cloud Storage Pools (csp1, csp2) or use multiple placement instructions with dates that do not overlap. **Overlapping days:** 0-10.

To see the overlapping days on the Retention Diagram, click Refresh.

Retention Diagram [?](#)

- Ein Objekt kann in einem Cloud-Storage-Pool gleichzeitig gespeichert werden, als replizierte oder als Erasure Coding-Kopie in StorageGRID. Wie in diesem Beispiel gezeigt wird, müssen Sie für den Zeitraum jedoch mehr als eine Zeile in die Platzierungsanweisung aufnehmen, damit Sie die Anzahl und die Art der Kopien für jeden Standort angeben können.

Placements [?](#)

From day store days

Type	Location	Copies
<input type="text" value="replicated"/>	<input type="text" value="DC1"/> <input type="text" value="DC2"/> <input type="text" value="Add Pool"/>	<input type="text" value="2"/>
<input type="text" value="replicated"/>	<input type="text" value="testpool2"/> <input type="text" value="Add Pool"/>	<input type="text" value="1"/>

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

- a. Wählen Sie aus der Dropdown-Liste **Typ** die Option **Löschvorgang codiert** aus.

Die Anzahl der Kopien ändert sich in 1. Es wird eine Warnung angezeigt, wenn die Regel keinen erweiterten Filter besitzt, um Objekte zu ignorieren, die 200 KB oder kleiner sind.

Do not use erasure coding for objects that are 200 KB or smaller. Select Back to return to Step 1. Then, use Advanced filtering to set the Object Size (MB) filter to "greater than 0.2".



Verwenden Sie kein Erasure Coding für Objekte mit einer Größe von mehr als 200 KB, um den Overhead zu vermeiden, der bei dem Management sehr kleiner, mit Erasure Coding codierter Fragmente verbunden ist.

- b. Wenn die Warnung Objektgröße angezeigt wurde, führen Sie die folgenden Schritte aus, um sie zu löschen:
- Wählen Sie **Zurück**, um zu Schritt 1 zurückzukehren.
 - Wählen Sie **Erweiterte Filterung**.
 - Setzen Sie den Filter Objektgröße (MB) auf „größer als 0.2“.
- c. Wählen Sie den Speicherort aus.

Der Speicherort für eine Kopie mit Erasure-Coding-Verfahren umfasst den Namen des Speicherpools, gefolgt vom Namen des Erasure Coding-Profiles.

6. Optional können Sie verschiedene Zeiträume hinzufügen oder zusätzliche Kopien an verschiedenen Standorten erstellen:

- Klicken Sie auf das Plus-Symbol, um während des gleichen Zeitraums zusätzliche Kopien an einem anderen Ort zu erstellen.
- Klicken Sie auf **Hinzufügen**, um den Anweisungen zur Platzierung einen anderen Zeitraum hinzuzufügen.



Objekte werden am Ende des Endzeitraums automatisch gelöscht, es sei denn, der Endzeitraum endet mit **forever**.

7. Klicken Sie auf **Aktualisieren**, um das Aufbewahrungsdigramm zu aktualisieren und die Anweisungen zur Platzierung zu bestätigen.

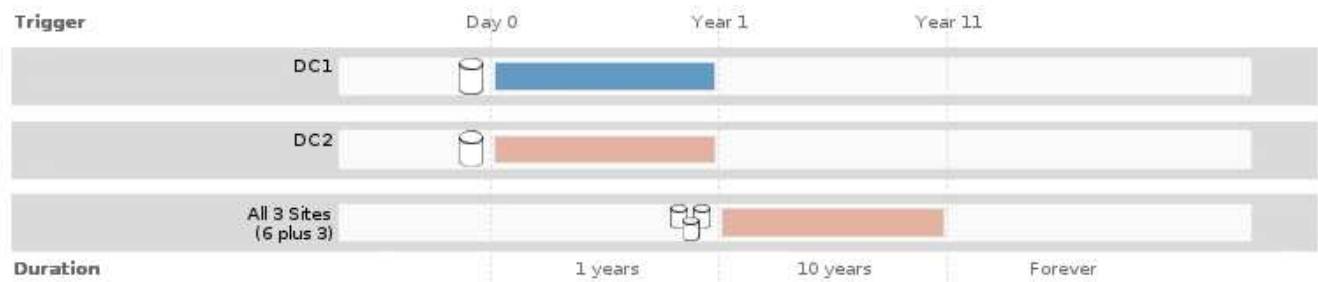
Jede Zeile im Diagramm zeigt an, wo und wann Objektkopien platziert werden. Der Kopiertyp wird durch eines der folgenden Symbole dargestellt:

	Replizierte Kopie
	Kopie mit Erasure Coding – eine Kopie



Cloud-Storage-Pool-Kopie

In diesem Beispiel werden zwei replizierte Kopien für ein Jahr in zwei Speicherpools (DC1 und DC2) gespeichert. Anschließend wird eine Kopie mit Erasure Coding für weitere 10 Jahre gespeichert. Dabei wird ein 6+3 Erasure Coding-Schema an drei Standorten verwendet. Nach 11 Jahren werden die Objekte aus StorageGRID gelöscht.



8. Klicken Sie Auf **Weiter**.

Schritt 3 (Ingest Behavior definieren) wird angezeigt.

Verwandte Informationen

["Welche Anweisungen zur Platzierung der ILM-Regeln gibt es"](#)

["Beispiel 4: ILM-Regeln und -Richtlinie für versionierte Objekte mit S3"](#)

["Warum sollten Sie keine Replizierung mit nur einer Kopie verwenden"](#)

["Verwalten von Objekten mit S3 Object Lock"](#)

["Verwenden eines Speicherpools als temporärer Speicherort \(veraltet\)"](#)

["Schritt 3 von 3: Definieren des Aufnahmeverhaltens"](#)

Verwenden der Zeit für den letzten Zugriff in ILM-Regeln

Sie können den Zeitpunkt 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 den Zeitpunkt des letzten Zugriffs auch als erweiterten Filter verwenden, wenn eine ILM-Regel nur für Objekte gelten soll, auf die zuletzt an einem bestimmten Datum zugegriffen wurde.

Über diese Aufgabe

Bevor Sie den Zeitpunkt des letzten Zugriffs in einer ILM-Regel verwenden, prüfen Sie die folgenden Aspekte:

- Wenn Sie den Zeitpunkt des letzten Zugriffs als Referenzzeit verwenden, beachten Sie, dass durch das Ändern der Uhrzeit für den letzten Zugriff für ein Objekt keine sofortige ILM-Evaluierung ausgelöst wird. 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, die auf Last Access Time basieren, und vermeiden Sie Platzierungen, die kurze Zeiträume (weniger als einen Monat) nutzen.

- Wenn Sie den Zeitpunkt des letzten Zugriffs als erweiterten Filter oder als Referenzzeit verwenden, müssen Sie die Updates der letzten Zugriffszeit für S3-Buckets aktivieren. Sie können den Tenant Manager oder die Mandantenmanagement-API verwenden.



Updates der letzten Zugriffszeit sind immer für Swift Container aktiviert. Für S3 Buckets sind sie jedoch 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.

Die folgende Tabelle fasst zusammen, ob die letzte Zugriffszeit für alle Objekte im Bucket für unterschiedliche Anträgen aktualisiert wird.

Art der Anfrage	Gibt an, ob die letzte Zugriffszeit aktualisiert wird, wenn Updates der letzten Zugriffszeit deaktiviert sind	Ob die letzte Zugriffszeit aktualisiert wird, wenn 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	<ul style="list-style-type: none">• Nein, für die Quellkopie• Ja, für die Zielkopie	<ul style="list-style-type: none">• Ja, für die Quellkopie• Ja, für die Zielkopie
Anforderung zum Abschließen eines mehrteiligen Uploads	Ja, für das zusammengesetzte Objekt	Ja, für das zusammengesetzte Objekt

Verwandte Informationen

["S3 verwenden"](#)

["Verwenden Sie ein Mandantenkonto"](#)

Schritt 3 von 3: Definieren des Aufnahmeverhaltens

Schritt 3 (Ingest Behavior definieren) des Assistenten Create ILM Rule ermöglicht es Ihnen, festzulegen, wie die Objekte, die von dieser Regel gefiltert werden, beim Einnehmen 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.

Create ILM Rule Step 3 of 3: Define ingest behavior

Select the data protection option to use when objects are ingested:

- ☐ **Strict**
Always uses this rule's placements on ingest. Ingest fails when this rule's placements are not possible.
- ☒ **Balanced**
Optimum ILM efficiency. Attempts this rule's placements on ingest. Creates interim copies when that is not possible.
- ☐ **Dual commit**
Creates interim copies on ingest and applies this rule's placements later.

Cancel Back Save

Schritte

1. Wählen Sie die Datenschutzoption aus, die verwendet werden soll, wenn Objekte aufgenommen werden:

Option	Beschreibung
Streng	Verwendet bei der Aufnahme immer die Platzierungen dieser Regel. Einspeisung scheitert, wenn die Platzierungen dieser Regel nicht möglich sind.
Ausgeglichen	Optimale ILM-Effizienz: Versucht die Platzierungen dieser Regel bei der Aufnahme. Erstellt zwischenzeitliche Kopien, wenn dies nicht möglich ist.
Doppelte Provisionierung	Erstellt vorläufige Kopien bei der Aufnahme und wendet die Platzierung dieser Regel später an.

Balance bietet eine Kombination aus Datensicherheit und Effizienz, die in den meisten Fällen geeignet ist. Zur Erfüllung spezifischer Anforderungen wird in der Regel eine strenge oder doppelte Provisionierung verwendet.

Weitere Informationen finden Sie unter „welche Datensicherungsoptionen für die Aufnahme“ und „vor- und Nachteile jeder Datensicherungsoption“.



Wenn Sie die Option streng oder ausgewogen auswählen und die Regel eine der folgenden Platzierungen verwendet, wird eine Fehlermeldung angezeigt:

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

2. Klicken Sie Auf **Speichern**.

Die ILM-Regel wird gespeichert. Die Regel bleibt erst aktiv, wenn sie zu einer ILM-Richtlinie hinzugefügt und diese Richtlinie aktiviert wird.

Verwandte Informationen

["Datensicherungsoptionen für die Aufnahme"](#)

["Vor- und Nachteile sowie Einschränkungen der Datensicherungsoptionen"](#)

["Beispiel 5: ILM-Regeln und Richtlinie für striktes Ingest-Verhalten"](#)

["ILM-Richtlinie erstellen"](#)

Erstellen einer Standard-ILM-Regel

Jede ILM-Richtlinie muss über eine Standardregel verfügen, die keine Objekte filtert. Vor dem Erstellen einer ILM-Richtlinie müssen Sie mindestens eine ILM-Regel erstellen, die als Standardregel für die Richtlinie verwendet werden kann.

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.
- Sie müssen über spezifische Zugriffsberechtigungen verfügen.

Über diese Aufgabe

Die Standardregel ist die letzte Regel, die in einer ILM-Richtlinie ausgewertet werden muss. Daher kann sie keine Filter verwenden. Die Anweisungen zur Platzierung der Standardregel werden auf alle Objekte angewendet, die nicht mit einer anderen Regel in der Richtlinie abgeglichen werden.

In dieser Beispielrichtlinie gilt die erste Regel nur für Objekte, die zu Mandant A gehören. Die letzte Standardregel gilt für Objekte, die zu allen anderen Mandantenkonten gehören.

+ Select Rules			
Default	Rule Name	Tenant Account	Actions
	Erasure Coding for Tenant A 	Tenant A (94793396288150002349)	✕
✓	2 Copies 2 Data Centers 	Ignore	✕

Beachten Sie beim Erstellen der Standardregel die folgenden Anforderungen:

- Die Standardregel wird automatisch als letzte Regel in der Richtlinie gesetzt.
- Die Standardregel kann keine einfachen oder erweiterten Filter verwenden.
- Die Standardregel sollte replizierte Kopien erstellen.



Verwenden Sie keine Regel, die Kopien, die zur Fehlerkorrektur codiert wurden, als Standardregel für eine Richtlinie erstellt. Für Verfahren zur Einhaltung von Datenkonsistenz (Erasure Coding) sollte ein erweiterter Filter verwendet werden, um zu verhindern, dass bei kleineren Objekten die Codierung von Datenkonsistenz erfolgt.

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

Schritte

1. Wählen Sie **ILM > Regeln**.

Die Seite ILM-Regeln wird angezeigt.

2. Wählen Sie **Erstellen**.

Schritt 1 (Grundlagen definieren) des Assistenten „ILM-Regel erstellen“ wird angezeigt.

3. Geben Sie im Feld **Name** einen eindeutigen Namen für die Regel ein.

4. Geben Sie optional im Feld **Beschreibung** eine kurze Beschreibung für die Regel ein.

5. Lassen Sie das Feld **Mandantenkonten** leer.

Die Standardregel muss auf alle Mandantenkonten angewendet werden.

6. Lassen Sie das Feld **Bucket Name** leer.

Die Standardregel muss auf alle S3-Buckets und Swift-Container angewendet werden.

7. Wählen Sie nicht **Advanced Filtering** aus

Die Standardregel kann keine Filter angeben.

8. Wählen Sie **Weiter**.

Schritt 2 (Platzierungen definieren) wird angezeigt.

9. 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 zur Fehlerkorrektur codiert wurden, als Standardregel für eine Richtlinie erstellt. Erasure-Coding-Regeln sollten den erweiterten Filter **Objektgröße (MB) von mehr als 0.2** enthalten, um zu verhindern, dass kleinere Objekte gelöscht 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 Platzierung vorhanden sein.
 - Objektkopien können nicht in einem Cloud-Storage-Pool gespeichert werden.
 - Objektkopien können nicht auf Archiv-Knoten gespeichert werden.
 - Mindestens eine Zeile der Anweisungen für die Platzierung muss am Tag 0 beginnen, wobei die Aufnahmezeit als Referenzzeit verwendet wird.
 - Mindestens eine Zeile der Platzierungsanweisungen muss „Forever“ sein.

10. Klicken Sie auf **Aktualisieren**, um das Aufbewahrungsdigramm zu aktualisieren und die Anweisungen zur Platzierung zu bestätigen.

11. Klicken Sie Auf **Weiter**.

Schritt 3 (Ingest Behavior definieren) wird angezeigt.

12. Wählen Sie die Datenschutzooption aus, die verwendet werden soll, wenn Objekte aufgenommen werden, und wählen Sie **Speichern**.

ILM-Richtlinie erstellen

Bei der Erstellung einer ILM-Richtlinie wählen Sie zunächst die ILM-Regeln aus und ordnen sie an. Anschließend überprüfen Sie das Verhalten Ihrer vorgeschlagenen Richtlinie, indem Sie sie mit zuvor aufgenommenen Objekten simulieren. Wenn Sie damit zufrieden sind, dass die vorgeschlagene Richtlinie wie vorgesehen funktioniert, können Sie sie aktivieren, um die aktive Richtlinie zu erstellen.



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.

Überlegungen bei der Erstellung einer ILM-Richtlinie

- Verwenden Sie die integrierte Systemrichtlinie Basis-2-Kopien-Richtlinie nur in Testsystemen. Die Regel 2 Kopien erstellen in dieser Richtlinie verwendet 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.
- 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 einer Richtlinie mit einem Objekt übereinstimmt, wird diese Regel nicht durch eine andere Regel ausgewertet.
- Die letzte Regel in jeder ILM-Richtlinie ist die Standard-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.

Verwandte Informationen

["Was ist eine ILM-Richtlinie"](#)

["Beispiel 6: Ändern einer ILM-Richtlinie"](#)

Erstellen einer vorgeschlagenen ILM-Richtlinie

Sie können eine vorgeschlagene ILM-Richtlinie von Grund auf erstellen oder die aktuelle

aktive Richtlinie klonen, wenn Sie mit demselben Regelsatz beginnen möchten.

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.
- Sie müssen über spezifische Zugriffsberechtigungen verfügen.
- Sie müssen die ILM-Regeln erstellt haben, die Sie der vorgeschlagenen Richtlinie hinzufügen möchten. Bei Bedarf können Sie eine vorgeschlagene Richtlinie speichern, zusätzliche Regeln erstellen und die vorgeschlagene Richtlinie bearbeiten, um die neuen Regeln hinzuzufügen.
- Sie müssen eine Standard-ILM-Regel für die Richtlinie erstellt haben, die keine Filter enthält.

["Erstellen einer Standard-ILM-Regel"](#)

Über diese Aufgabe

Typische Gründe für die Erstellung einer vorgeschlagenen ILM-Richtlinie sind:

- Sie haben einen neuen Standort hinzugefügt und müssen neue ILM-Regeln verwenden, um Objekte an diesem Standort zu platzieren.
- Sie müssen einen Standort außer Betrieb nehmen und alle Regeln, die sich auf den Standort beziehen, entfernen.
- Sie haben einen neuen Mandanten mit besonderen Anforderungen an die Datensicherheit hinzugefügt.
- Sie haben damit begonnen, einen Cloud-Storage-Pool zu verwenden.



Verwenden Sie die integrierte Systemrichtlinie Basis-2-Kopien-Richtlinie nur in Testsystemen. Die Regel 2 Kopien erstellen in dieser Richtlinie verwendet 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 die globale S3-Objektsperre aktiviert wurde, sind die Schritte zum Erstellen einer Richtlinie etwas unterschiedlich. Sie müssen sicherstellen, dass die ILM-Richtlinie die Anforderungen von Buckets erfüllt, für die S3 Object Lock aktiviert ist.

["Erstellen einer ILM-Richtlinie, nachdem S3 Object Lock aktiviert ist"](#)

Schritte

1. Wählen Sie **ILM > Richtlinien**.

Die Seite ILM-Richtlinien wird angezeigt. Auf dieser Seite können Sie die Liste der vorgeschlagenen, aktiven und historischen Richtlinien überprüfen; erstellen, bearbeiten, Oder entfernen Sie eine vorgeschlagene Richtlinie, klonen Sie die aktive Richtlinie oder lesen Sie die Details zu einer Richtlinie.

ILM Policies

Review the proposed, active, and historical policies. You can create, edit, or delete a proposed policy; clone the active policy; or view the details for any policy.

+ Create Proposed Policy
Clone
Edit
Remove

Policy Name	Policy State	Start Date	End Date
Baseline 2 Copies Policy	Active	2017-07-17 12:00:45 MDT	

Viewing Active Policy - Baseline 2 Copies Policy

Review the rules in this policy. If this is a proposed policy, click Simulate to verify the policy and then click Activate to make the policy active.

Rules are evaluated in order, starting from the top.

Rule Name	Default	Tenant Account
Make 2 Copies	✓	Ignore

Simulate
Activate

2. Legen Sie fest, wie Sie die vorgeschlagene ILM-Richtlinie erstellen möchten.

Option	Schritte
Erstellen Sie eine neue vorgeschlagene Richtlinie, für die keine Regeln bereits ausgewählt sind	<p>a. Wenn derzeit eine vorgeschlagene ILM-Richtlinie vorhanden ist, wählen Sie diese Richtlinie aus, und klicken Sie auf Entfernen.</p> <p>Sie können keine neue vorgeschlagene Richtlinie erstellen, wenn eine vorgeschlagene Richtlinie bereits vorhanden ist.</p> <p>b. Klicken Sie Auf Vorgeschlagene Richtlinie Erstellen.</p>
Erstellen Sie eine vorgeschlagene Richtlinie auf der Grundlage der aktiven Richtlinie	<p>a. Wenn derzeit eine vorgeschlagene ILM-Richtlinie vorhanden ist, wählen Sie diese Richtlinie aus, und klicken Sie auf Entfernen.</p> <p>Sie können die aktive Richtlinie nicht klonen, wenn eine vorgeschlagene Richtlinie bereits vorhanden ist.</p> <p>b. Wählen Sie die aktive Richtlinie aus der Tabelle aus.</p> <p>c. Klicken Sie Auf Clone.</p>
Bearbeiten Sie die vorhandene vorgeschlagene Richtlinie	<p>a. Wählen Sie die vorgeschlagene Richtlinie aus der Tabelle aus.</p> <p>b. Klicken Sie Auf Bearbeiten.</p>

Das Dialogfeld ILM-Richtlinie konfigurieren wird angezeigt.

Wenn Sie eine neue vorgeschlagene Richtlinie erstellen, sind alle Felder leer und es werden keine Regeln ausgewählt.

Configure ILM Policy

Create a proposed policy by selecting and arranging rules. Then, save the policy and edit it later as required. Click Simulate to verify a saved policy using test objects. When you are ready, click Activate to make this policy the active ILM policy for the grid.

Name

Reason for change

Rules

1. Select the rules you want to add to the policy.
2. Determine the order in which the rules will be evaluated by dragging and dropping the rows. The default rule will be automatically placed at the end of the policy and cannot be moved.

+ Select Rules

Default	Rule Name	Tenant Account	Actions
---------	-----------	----------------	---------

No rules selected.

Cancel

Save

Wenn Sie die aktive Richtlinie klonen, zeigt das Feld **Name** den Namen der aktiven Richtlinie an, der durch eine Versionsnummer („v2“ im Beispiel angehängt wird). Die in der aktiven Richtlinie verwendeten Regeln werden ausgewählt und in ihrer aktuellen Reihenfolge angezeigt.

Name

Baseline 2 Copies Policy (v2)

Reason for change

3. Geben Sie im Feld **Name** einen eindeutigen Namen für die vorgeschlagene Richtlinie ein.

Sie müssen mindestens 1 und nicht mehr als 64 Zeichen eingeben. Wenn Sie die aktive Richtlinie klonen, können Sie den aktuellen Namen mit der angehängten Versionsnummer verwenden oder einen neuen Namen eingeben.

4. Geben Sie im Feld **Grund für Änderung** den Grund für die Erstellung einer neuen Policy ein.

Sie müssen mindestens 1 und nicht mehr als 128 Zeichen eingeben.

5. Um der Richtlinie Regeln hinzuzufügen, wählen Sie **Regeln auswählen**.

Das Dialogfeld Regeln für Richtlinie auswählen wird angezeigt, in dem alle definierten Regeln aufgeführt sind. 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 mit einer Schaltfläche die Regel an das Ende der neuen Richtlinie

verschieben.

Select Rules for Policy

Select Default Rule

This list shows the rules that do not use any filters. Select one rule to be the default rule for the policy. The default rule applies to any objects that do not match another rule in the policy and is always evaluated last. The default rule should retain objects forever.

	Rule Name
<input checked="" type="radio"/>	2 copies at 2 data centers
<input type="radio"/>	2 copies at 2 data centers for 2 years
<input type="radio"/>	Make 2 Copies

Select Other Rules

The other rules in a policy are evaluated before the default rule and must use at least one filter. Each rule in this list uses at least one filter (tenant account, bucket name, or an advanced filter, such as object size).

	Rule Name	Tenant Account
<input type="checkbox"/>	1-site EC	—
<input type="checkbox"/>	3-site EC	—

Cancel

Apply

6. Wählen Sie einen Regelnamen oder das Symbol für weitere Details aus So zeigen Sie die Einstellungen für diese Regel an:

Dieses Beispiel zeigt die Details einer ILM-Regel, die zwei Kopien an zwei Standorten erstellt.

Two-Site Replication for Other Tenants

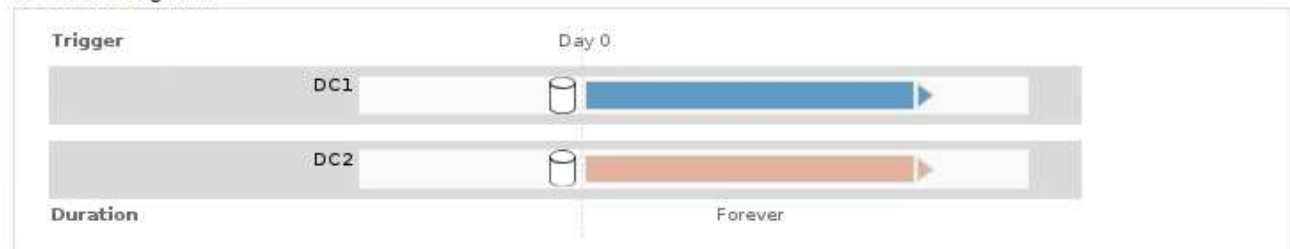
Description: Two-Site Replication for Other Tenants

Ingest Behavior: Balanced

Reference Time: Ingest Time

Filtering Criteria: Matches all objects.

Retention Diagram:



Close

7. Wählen Sie im Abschnitt **Standardregel auswählen** eine Standardregel für die vorgeschlagene Richtlinie aus.

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



Wenn im Abschnitt Standardregel auswählen keine Regel aufgeführt wird, müssen Sie die Seite ILM-Richtlinie beenden und eine Standardregel erstellen.

"Erstellen einer Standard-ILM-Regel"



Verwenden Sie die Regel „2-Kopien-Bestand erstellen“ nicht 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.

- Wählen Sie im Abschnitt **Weitere Regeln** alle weiteren Regeln aus, die Sie in die Richtlinie aufnehmen möchten.

Die anderen Regeln werden vor der Standardregel evaluiert und müssen mindestens einen Filter verwenden (Mandantenkonto, Bucket-Name oder erweiterten Filter, wie Objektgröße).

- Wenn Sie die Auswahl von Regeln abgeschlossen haben, wählen Sie **Anwenden**.

Die ausgewählten Regeln werden aufgelistet. Die Standardregel ist am Ende, mit den anderen Regeln darüber.

Rules

- Select the rules you want to add to the policy.
- Determine the order in which the rules will be evaluated by dragging and dropping the rows. The default rule will be automatically placed at the end of the policy and cannot be moved.

+ Select Rules				
	Default	Rule Name	Tenant Account	Actions
⬆️⬆️		3-site EC	Ignore	✖
⬆️⬆️		1-site EC	Ignore	✖
	✓	2 copies at 2 data centers	Ignore	✖
				Cancel Save

Eine Warnung wird angezeigt, wenn die Standardregel Objekte nicht dauerhaft enthält. 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 länger).



	Default	Rule Name	Tenant Account	Actions
⬆️⬆️		3-site EC	Ignore	✖
⬆️⬆️		1-site EC	Ignore	✖
	✓	2 copies at 2 data centers for 2 years	Ignore	✖

The default ILM rule in this policy does not retain objects forever. Confirm this is the behavior you expect. Otherwise, any objects that are not matched by another rule will be deleted after 720 days.

- Ziehen Sie die Zeilen für die nicht standardmäßigen Regeln per Drag-and-Drop, um die Reihenfolge zu bestimmen, in der diese Regeln ausgewertet werden.

Sie können die Standardregel nicht verschieben.



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.

11. Klicken Sie bei Bedarf auf das Löschsymbol . Wenn Sie Regeln löschen möchten, die in der Richtlinie nicht enthalten sein sollen, oder wählen Sie **Regeln auswählen**, um weitere Regeln hinzuzufügen.
12. Wenn Sie fertig sind, wählen Sie **Speichern**.

Die Seite ILM-Richtlinien wird aktualisiert:

- Die von Ihnen gespeicherte Richtlinie wird als Vorschlag angezeigt. Die vorgeschlagenen Richtlinien haben kein Start- und Enddatum.
- Die Schaltflächen **Simulate** und **Activate** sind aktiviert.

ILM Policies

Review the proposed, active, and historical policies. You can create, edit, or delete a proposed policy; clone the active policy; or view the details for any policy.

+ Create Proposed Policy	Clone	Edit	Remove
Policy Name	Policy State	Start Date	End Date
<input checked="" type="radio"/> Data Protection for Three Sites	Proposed		
<input type="radio"/> Data Protection for Two Sites	Active	2020-09-18 16:01:24 MDT	
<input type="radio"/> Baseline 2 Copies Policy	Historical	2020-09-17 21:32:57 MDT	2020-09-18 16:01:24 MDT

Viewing Proposed Policy - Data Protection for Three Sites

Before activating a new ILM policy:

- Review and carefully simulate the policy. Errors in an ILM policy can cause irreparable data loss.
- Review any changes to the placement of existing replicated and erasure-coded objects. Changing an existing object's location might result in temporary resource issues when the new placements are evaluated and implemented.

See [Managing objects with information lifecycle management](#) for more information.

This policy contains a rule that makes an erasure-coded copy. Confirm that at least one rule uses the Object Size advanced filter to prevent objects that are 200 KB or smaller from being erasure coded. See [Managing objects with information lifecycle management](#) for more information.

Review the rules in this policy. If this is a proposed policy, click Simulate to verify the policy and then click Activate to make the policy active.

Reason for change: Added a third site

Rules are evaluated in order, starting from the top.

Rule Name	Default	Tenant Account
One-Site Erasure Coding for Tenant A		Tenant A (20033011709864740158)
Three-Site Replication for Other Tenants	✓	Ignore

[Simulate](#)

[Activate](#)

13. Gehen Sie zu ["Simulation einer ILM-Richtlinie"](#).

Verwandte Informationen

["Was ist eine ILM-Richtlinie"](#)

["Verwalten von Objekten mit S3 Object Lock"](#)

Erstellen einer ILM-Richtlinie, nachdem S3 Object Lock aktiviert ist

Wenn die globale S3-Objektsperre aktiviert ist, unterscheiden sich die Schritte zum Erstellen einer Richtlinie geringfügig. Sie müssen sicherstellen, dass die ILM-Richtlinie die Anforderungen von Buckets erfüllt, für die S3 Object Lock aktiviert ist.

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.
- Sie müssen über spezifische Zugriffsberechtigungen verfügen.
- Die globale S3-Objektsperre muss bereits für das StorageGRID-System aktiviert sein.



Wenn die globale S3-Objektsperre nicht aktiviert wurde, verwenden Sie stattdessen die allgemeinen Anweisungen zum Erstellen einer vorgeschlagenen Richtlinie.

["Erstellen einer vorgeschlagenen ILM-Richtlinie"](#)

- Sie müssen die konformen und nicht konformen ILM-Regeln erstellt haben, die Sie der vorgeschlagenen Richtlinie hinzufügen möchten. Bei Bedarf können Sie eine vorgeschlagene Richtlinie speichern, zusätzliche Regeln erstellen und die vorgeschlagene Richtlinie bearbeiten, um die neuen Regeln hinzuzufügen.

["Beispiel 7: Konforme ILM-Richtlinie für S3 Object Lock"](#)

- Sie müssen eine konforme Standard-ILM-Regel für die Richtlinie erstellt haben.

["Erstellen einer Standard-ILM-Regel"](#)

Schritte

1. Wählen Sie **ILM > Richtlinien**.

Die Seite ILM-Richtlinien wird angezeigt. Wenn die globale S3-Objektsperreneinstellung aktiviert ist, zeigt die Seite ILM-Richtlinien an, welche ILM-Regeln konform sind.

ILM Policies

Review the proposed, active, and historical policies. You can create, edit, or delete a proposed policy; clone the active policy; or view the details for any policy.

+ Create Proposed Policy

Clone

Edit

Remove

Policy Name	Policy State	Start Date	End Date
Baseline 2 Copies Policy	Active	2021-02-04 01:04:29 MST	

Viewing Active Policy - Baseline 2 Copies Policy

Review the rules in this policy. If this is a proposed policy, click Simulate to verify the policy and then click Activate to make the policy active.

Rules are evaluated in order, starting from the top. The policy's default rule must be compliant.

Rule Name	Default	Compliant	Tenant Account
Make 2 Copies	✓	✓	Ignore

Simulate

Activate

2. Geben Sie im Feld **Name** einen eindeutigen Namen für die vorgeschlagene Richtlinie ein.

Sie müssen mindestens 1 und nicht mehr als 64 Zeichen eingeben.

3. Geben Sie im Feld **Grund für Änderung** den Grund für die Erstellung einer neuen Policy ein.

Sie müssen mindestens 1 und nicht mehr als 128 Zeichen eingeben.

4. Um der Richtlinie Regeln hinzuzufügen, wählen Sie **Regeln auswählen**.

Das Dialogfeld Regeln für Richtlinie auswählen wird angezeigt, in dem alle definierten Regeln aufgeführt sind.

- Im Abschnitt Standardregel auswählen werden die Regeln aufgeführt, die für eine konforme Richtlinie standardmäßig gelten können. Es enthält konforme Regeln, die keine Filter verwenden.
- Im Abschnitt andere Regeln auswählen werden die anderen für diese Richtlinie ausgewählten Compliance- und nicht-konformen Regeln aufgeführt.

Select Rules for Policy

Select Default Rule

This list shows the rules that are compliant and do not use any filters. Select one rule to be the default rule for the policy. The default rule applies to any objects that do not match another rule in the policy and is always evaluated last.

	Rule Name
<input type="radio"/>	Default Compliant Rule: Two Copies Two Data Centers
<input type="radio"/>	Make 2 Copies

Select Other Rules

The other rules in a policy are evaluated before the default rule. If you need a different "default" rule for objects in non-compliant S3 buckets, select one non-compliant rule that does not use a filter. Any other rules in the policy must use at least one filter (tenant account, bucket name, or an advanced filter, such as object size).

	Rule Name	Compliant	Uses Filter	Is Selectable
<input type="checkbox"/>	Compliant Rule: EC for bank-records bucket - Bank of AB C	✓	✓	Yes
<input type="checkbox"/>	Non-Compliant Rule: Use Cloud Storage Pool			Yes

Cancel

Apply

5. Wählen Sie einen Regelnamen oder das Symbol für weitere Details aus So zeigen Sie die Einstellungen für diese Regel an:

6. Wählen Sie im Abschnitt **Standardregel auswählen** eine Standardregel für die vorgeschlagene Richtlinie aus.

In der Tabelle in diesem Abschnitt werden nur die Regeln aufgeführt, die kompatibel sind und keine Filter verwenden.



Wenn im Abschnitt Standardregel auswählen keine Regel aufgeführt wird, müssen Sie die Seite ILM-Richtlinie beenden und eine konforme Standardregel erstellen.

["Erstellen einer Standard-ILM-Regel"](#)



Verwenden Sie die Regel „2-Kopien-Bestand erstellen“ nicht 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.

7. Wählen Sie im Abschnitt **Weitere Regeln** alle weiteren Regeln aus, die Sie in die Richtlinie aufnehmen möchten.

- a. Wenn Sie für Objekte in nicht-konformen S3-Buckets eine andere „default“-Regel benötigen, wählen Sie optional eine nicht konforme Regel aus, die keinen Filter verwendet.

Beispielsweise möchten Sie einen Cloud-Storage-Pool oder einen Archiv-Node verwenden, um Objekte in Buckets zu speichern, in denen die S3-Objektsperre nicht aktiviert ist.



Sie können nur eine nicht kompatible Regel auswählen, die keinen Filter verwendet. Sobald Sie eine Regel auswählen, wird in der Spalte **ist wählbar Nein** für alle anderen nicht-konformen Regeln ohne Filter angezeigt.

- a. Wählen Sie alle anderen konformen oder nicht konformen Regeln aus, die Sie in der Richtlinie verwenden möchten.

Die anderen Regeln müssen mindestens einen Filter verwenden (Mandantenkonto, Bucket-Name oder erweiterte Filter, wie Objektgröße).

8. Wenn Sie die Regeln ausgewählt haben, wählen Sie **Anwenden**.

Die ausgewählten Regeln werden aufgelistet. Die Standardregel ist am Ende, mit den anderen Regeln darüber. Wenn Sie auch eine nicht-konforme Regel „default“ ausgewählt haben, wird diese Regel als zweite zu letzte Regel in der Richtlinie hinzugefügt.

In diesem Beispiel ist die letzte Regel, 2 Kopien 2 Rechenzentren, die Standardregel: Sie ist kompatibel und hat keine Filter. Die zweite bis letzte Regel – Cloud Storage Pool – verfügt ebenfalls über keine Filter, ist aber nicht konform.

Configure ILM Policy

Create a proposed policy by selecting and arranging rules. Then, save the policy and edit it later as required. Click Simulate to verify a saved policy using test objects. When you are ready, click Activate to make this policy the active ILM policy for the grid.

Name

Reason for change

Rules

1. Select the rules you want to add to the policy.
2. Determine the order in which the rules will be evaluated by dragging and dropping the rows. The default rule (and any non-compliant rule without a filter) will be automatically placed at the end of the policy and cannot be moved.

Select Rules

Default	Rule Name	Compliant	Tenant Account	Actions
	Compliant Rule: EC for bank-records bucket - Bank of ABC	✓	Bank of ABC (90767802913525281639)	
	Non-Compliant Rule: Use Cloud Storage Pool		Ignore	
✓	Default Compliant Rule: Two Copies Two Data Centers	✓	Ignore	

Cancel

Save

9. Ziehen Sie die Zeilen für die nicht standardmäßigen Regeln per Drag-and-Drop, um die Reihenfolge zu bestimmen, in der diese Regeln ausgewertet werden.

Sie können die Standardregel oder die nicht-konforme Regel „default“ nicht verschieben.



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.

10. Klicken Sie bei Bedarf auf das Löschsymbolsymbol Wenn Sie Regeln löschen möchten, die in der Richtlinie nicht enthalten sein sollen, oder wählen Sie **Regeln auswählen**, um weitere Regeln hinzuzufügen.
11. Wenn Sie fertig sind, wählen Sie **Speichern**.

Die Seite ILM-Richtlinien wird aktualisiert:

- Die von Ihnen gespeicherte Richtlinie wird als Vorschlag angezeigt. Die vorgeschlagenen Richtlinien haben kein Start- und Enddatum.
- Die Schaltflächen **Simulate** und **Activate** sind aktiviert.

ILM Policies

Review the proposed, active, and historical policies. You can create, edit, or delete a proposed policy; clone the active policy; or view the details for any policy.

[+ Create Proposed Policy](#) [Clone](#) [Edit](#) [Remove](#)

Policy Name	Policy State	Start Date	End Date
Compliant ILM Policy for S3 Object Lock	Proposed		
Compliant ILM Policy	Active	2021-02-05 16:22:53 MST	
Non-Compliant ILM policy	Historical	2021-02-05 15:17:05 MST	2021-02-05 16:22:53 MST
Baseline 2 Copies Policy	Historical	2021-02-04 21:35:52 MST	2021-02-05 15:17:05 MST

Viewing Proposed Policy - Compliant ILM Policy for S3 Object Lock

Before activating a new ILM policy:

- Review and carefully simulate the policy. Errors in an ILM policy can cause irreparable data loss.
- Review any changes to the placement of existing replicated and erasure-coded objects. Changing an existing object's location might result in temporary resource issues when the new placements are evaluated and implemented.

See [Managing objects with information lifecycle management](#) for more information.

This policy contains a rule that makes an erasure-coded copy. Confirm that at least one rule uses the Object Size advanced filter to prevent objects that are 200 KB or smaller from being erasure coded. See [Managing objects with information lifecycle management](#) for more information.

Review the rules in this policy. If this is a proposed policy, click Simulate to verify the policy and then click Activate to make the policy active.

Reason for change: [Example policy](#)

Rules are evaluated in order, starting from the top. The policy's default rule must be compliant.

Rule Name	Default	Compliant	Tenant Account
Compliant Rule: EC for bank-records bucket - Bank of ABC 🔗		✓	Bank of ABC (90767802913525281639)
Non-Compliant Rule: Use Cloud Storage Pool 🔗			Ignore
Default Compliant Rule: Two Copies Two Data Centers 🔗	✓	✓	Ignore

[Simulate](#) [Activate](#)

12. Gehen Sie zu "[Simulation einer ILM-Richtlinie](#)".

Simulation einer ILM-Richtlinie

Sie sollten eine vorgeschlagene Richtlinie für Testobjekte simulieren, bevor Sie die Richtlinie aktivieren und auf Ihre Produktionsdaten anwenden. Das Simulationsfenster bietet eine eigenständige Umgebung, die zum Testen von Richtlinien sicher ist, bevor sie aktiviert und auf Daten in der Produktionsumgebung angewendet werden.

Was Sie benötigen


- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.
- Sie müssen über spezifische Zugriffsberechtigungen verfügen.
- Sie müssen den S3-Bucket/Objektschlüssel oder den Swift-Container/Objektnamen für jedes Objekt, das Sie testen möchten, kennen und diese Objekte bereits aufgenommen haben.

Über diese Aufgabe

Sie müssen sorgfältig die Objekte auswählen, die die vorgeschlagene Richtlinie testen soll. Um eine Richtlinie gründlich zu simulieren, sollten Sie mindestens ein Objekt für jeden Filter in jeder Regel testen.

Wenn eine Richtlinie beispielsweise eine Regel enthält, mit der Objekte in Bucket A und eine andere Regel übereinstimmen, um Objekte in Bucket B zu entsprechen, müssen Sie mindestens ein Objekt aus Bucket A und ein Objekt aus Bucket B auswählen, um die Richtlinie gründlich zu testen. Wenn die Richtlinie eine Standardregel zum Platzieren aller anderen Objekte enthält, müssen Sie mindestens ein Objekt aus einem anderen Bucket testen.

Bei der Simulation einer Richtlinie gelten folgende Überlegungen:

- Nachdem Sie Änderungen an einer Richtlinie vorgenommen haben, speichern Sie die vorgeschlagene Richtlinie. Dann simulieren Sie das Verhalten der gespeicherten vorgeschlagenen Richtlinie.
- Wenn Sie eine Richtlinie simulieren, filtern die ILM-Regeln in der Richtlinie die Testobjekte ab, sodass Sie sehen können, welche Regel auf jedes Objekt angewendet wurde. Es werden jedoch keine Objektkopien erstellt und keine Objekte abgelegt. Wenn Sie eine Simulation ausführen, ändern Sie Ihre Daten, Regeln oder Richtlinien in keiner Weise.
- Auf der Seite Simulation werden die von Ihnen getesteten Objekte gespeichert, bis Sie die Seite ILM-Richtlinien schließen, wegnavigieren oder aktualisieren.
- Simulation gibt den Namen der übereinstimmenden Regel zurück. Um festzustellen, welcher Speicherpool oder welches Erasure-Coding-Profil wirksam ist, können Sie das Aufbewahrungsdiagramm anzeigen, indem Sie auf den Regelnamen oder das Detailsymbol klicken .
- Wenn die S3-Versionierung aktiviert ist, wird die Richtlinie nur mit der aktuellen Objektversion simuliert.

Schritte

1. Wählen Sie die Regeln aus und ordnen Sie sie an, und speichern Sie die vorgeschlagene Richtlinie.

Die Richtlinie in diesem Beispiel hat drei Regeln:

Regelname	Filtern	Kopentyp	Aufbewahrung
X-men	<ul style="list-style-type: none">• Mandant A• Benutzer-Metadaten (Serie=x-men)	2 Kopien in zwei Rechenzentren	2 Jahre
PNGs	Die Schlüssel enden mit .png	2 Kopien in zwei Rechenzentren	5 Jahre
Zwei Kopien Zwei Datacenter	<i>Keine</i>	2 Kopien in zwei Rechenzentren	Für Immer

Viewing Proposed Policy - Example ILM policy

Before activating a new ILM policy:

- Review and carefully simulate the policy. Errors in an ILM policy can cause irreparable data loss.
- Review any changes to the placement of existing replicated and erasure-coded objects. Changing an existing object's location might result in temporary resource issues when the new placements are evaluated and implemented.

See [Managing objects with information lifecycle management](#) for more information.

Review the rules in this policy. If this is a proposed policy, click Simulate to verify the policy and then click Activate to make the policy active.

Reason for change: Example policy

Rules are evaluated in order, starting from the top.

Rule Name	Default	Tenant Account
X-men 		Tenant A (94793396288150002349)
PNGs 		Ignore
Two Copies at Two Data Centers 	✓	Ignore

Simulate

Activate

2. Klicken Sie Auf **Simulieren**.

Das Dialogfeld Simulation ILM-Richtlinie wird angezeigt.

3. Geben Sie im Feld **Object** den S3-Bucket/Object-Key oder den Swift-Container/Object-Name für ein Testobjekt ein und klicken Sie auf **Simulate**.



Wenn Sie ein Objekt angeben, das nicht aufgenommen wurde, wird eine Meldung angezeigt.

4. Bestätigen Sie unter **Simulationsergebnisse**, dass jedes Objekt mit der richtigen Regel übereinstimmt.

In dem Beispiel wird der verwendet `Havok.png` Und `Warpath.jpg` Objekte wurden durch die X-Men-Regel korrekt abgeglichen. Der `Fullsteam.png` Objekt, das nicht enthält `series=x-men` Benutzermetadaten, wurde nicht mit der X-Men-Regel abgeglichen, wurde aber von der PNGs-Regel korrekt abgeglichen. Die Standardregel wurde nicht verwendet, da alle drei Objekte mit anderen Regeln abgeglichen wurden.

Simulate ILM Policy - Demo

Simulates the active ILM policy or, if there is a proposed ILM policy, simulates the proposed ILM policy. Use this simulation to test the current configuration of ILM rules and determine whether ILM rules copy and place object data as intended.

Object

Simulation Results ?

Object	Rule Matched	Previous Match	
photos/Havok.png	X-men		✗
photos/Warpath.jpg	X-men		✗
photos/Fullsteam.png	PNGs		✗

Beispiele für die Simulation von ILM-Richtlinien

Diese Beispiele zeigen, wie Sie ILM-Regeln durch Simulation der ILM-Richtlinie vor der Aktivierung überprüfen können.

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

Dieses Beispiel zeigt, wie Regeln bei der Simulation einer vorgeschlagenen 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 Objects > 1 MB**, gilt für alle Buckets, aber für Filter auf Objekten größer als 1 MB.
- Die dritte Regel ist die Standardregel und enthält keine Filter.

Viewing Proposed Policy - Example ILM policy

Before activating a new ILM policy:

- Review and carefully simulate the policy. Errors in an ILM policy can cause irreparable data loss.
- Review any changes to the placement of existing replicated and erasure-coded objects. Changing an existing object's location might result in temporary resource issues when the new placements are evaluated and implemented.

See [Managing objects with information lifecycle management](#) for more information.

This policy contains a rule that makes an erasure-coded copy. Confirm that at least one rule uses the Object Size advanced filter to prevent objects that are 200 KB or smaller from being erasure coded. See [Managing objects with information lifecycle management](#) for more information.

Review the rules in this policy. If this is a proposed policy, click Simulate to verify the policy and then click Activate to make the policy active.

Reason for change: Example policy

Rules are evaluated in order, starting from the top.

Rule Name	Default	Tenant Account
Two copies, two years for bucket-a 		—
EC objects > 1 MB 		—
Two copies, two data centers 	✓	—

[Simulate](#) [Activate](#)

Schritte

1. Klicken Sie nach dem Hinzufügen der Regeln und dem Speichern der Richtlinie auf **Simulieren**.

Das Dialogfeld ILM-Richtlinie simulieren wird angezeigt.

2. Geben Sie im Feld **Object** den S3-Bucket/Object-Key oder den Swift-Container/Object-Name für ein Testobjekt ein und klicken Sie auf **Simulate**.

Die Simulationsergebnisse werden angezeigt und zeigen an, welche Regel in der Richtlinie zu jedem getesteten Objekt passt.

Simulate ILM Policy - Example ILM policy

Simulates the active ILM policy or, if there is a proposed ILM policy, simulates the proposed ILM policy. Use this simulation to test the current configuration of ILM rules and determine whether ILM rules copy and place object data as intended.

Object: [Simulate](#)

Simulation Results

Object	Rule Matched	Previous Match	
bucket-a/bucket-a object.pdf	Two copies, two years for bucket-a 		✗
bucket-b/test object greater than 1 MB.pdf	EC objects > 1 MB 		✗
bucket-b/test object less than 1 MB.pdf	Two copies, two data centers 		✗

[Finish](#)

3. Vergewissern Sie sich, dass jedes Objekt mit der richtigen Regel übereinstimmt.

In diesem Beispiel:

- a. bucket-a/bucket-a object.pdf Die erste Regel, die nach Objekten in filtert, wurde richtig zugeordnet bucket-a.
- b. bucket-b/test object greater than 1 MB.pdf Ist in bucket-b, So dass es nicht mit der ersten Regel. Stattdessen wurde sie durch die zweite Regel korrekt abgeglichen, die nach Objekten mit

einer Größe von mehr als 1 MB filtert.

- c. `bucket-b/test object less than 1 MB.pdf` Stimmt nicht mit den Filtern in den ersten beiden Regeln überein, so wird sie durch die Standardregel platziert, die keine Filter enthält.

Beispiel 2: Neuordnung von Regeln bei der Simulation einer vorgeschlagenen ILM-Richtlinie

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 enden `.png`.
- Die zweite Regel, **X-Men**, gilt nur für Objekte für Mieter A und Filter für `series=x-men` Benutzer-Metadaten:
- Die letzte Regel, **zwei Kopien zwei Rechenzentren**, ist die Standardregel, die alle Objekte, die nicht mit den ersten beiden Regeln übereinstimmen, übereinstimmt.

Viewing Proposed Policy - Demo

Before activating a new ILM policy:

- Review and carefully simulate the policy. Errors in an ILM policy can cause irreparable data loss.
- Review any changes to the placement of existing replicated and erasure-coded objects. Changing an existing object's location might result in temporary resource issues when the new placements are evaluated and implemented.

See [Managing objects with information lifecycle management](#) for more information.

Review the rules in this policy. If this is a proposed policy, click Simulate to verify the policy and then click Activate to make the policy active.

Reason for change:

Rules are evaluated in order, starting from the top.

Rule Name	Default	Tenant Account
PNGs		Ignore
X-men		Tenant A (24365814597594524591)
Two copies two data centers	✓	Ignore

SimulateActivate

Schritte

1. Klicken Sie nach dem Hinzufügen der Regeln und dem Speichern der Richtlinie auf **Simulieren**.
2. Geben Sie im Feld **Object** den S3-Bucket/Object-Key oder den Swift-Container/Object-Name für ein Testobjekt ein und klicken Sie auf **Simulate**.


Die Simulationsergebnisse werden angezeigt, wobei das angezeigt wird `Havok.png`. Das Objekt wurde durch die **PNGs**-Regel abgeglichen.

Simulate ILM Policy - Demo

Simulates the active ILM policy or, if there is a proposed ILM policy, simulates the proposed ILM policy. Use this simulation to test the current configuration of ILM rules and determine whether ILM rules copy and place object data as intended.

Object

Simulation Results

Object	Rule Matched	Previous Match	
photos/Havok.png	PNGs 		

Allerdings die Regel, dass die Havok.png Das Objekt war für den Test die **X-Men**-Regel gedacht.

3. Um das Problem zu lösen, ordnen Sie die Regeln neu an.
 - a. Klicken Sie auf **Fertig stellen**, um die Seite ILM-Richtlinie simulieren zu schließen.
 - b. Klicken Sie auf **Bearbeiten**, um die Richtlinie zu bearbeiten.
 - c. Ziehen Sie die **X-Men**-Regel an den Anfang der Liste.

Configure ILM Policy

Create a proposed policy by selecting and arranging rules. Then, save the policy and edit it later as required. Click Simulate to verify a saved policy using test objects. When you are ready, click Activate to make this policy the active ILM policy for the grid.

Name

Reason for change

Rules

1. Select the rules you want to add to the policy.
2. Determine the order in which the rules will be evaluated by dragging and dropping the rows. The default rule will be automatically placed at the end of the policy and cannot be moved.

	Default	Rule Name	Tenant Account	Actions
		X-men 	Tenant A (48713995194927812566)	
		PNGs 	—	
		Two copies, two data centers 	—	

- d. Klicken Sie Auf **Speichern**.

4. Klicken Sie Auf **Simulieren**.

Die zuvor getesteten Objekte werden anhand der aktualisierten Richtlinie neu bewertet und die neuen Simulationsergebnisse angezeigt. Im Beispiel wird in der Spalte Regel zugeordnet das angezeigt Havok.png Das Objekt entspricht jetzt wie erwartet der X-Men-Metadatenregel. Die Spalte Vorheriger Abgleich zeigt an, dass die PNGs-Regel mit dem Objekt in der vorherigen Simulation übereinstimmt.

Simulate ILM Policy - Demo

Simulates the active ILM policy or, if there is a proposed ILM policy, simulates the proposed ILM policy. Use this simulation to test the current configuration of ILM rules and determine whether ILM rules copy and place object data as intended.

Object

Simulate

Simulation Results

Object	Rule Matched	Previous Match	
photos/Havok.png	X-men 	PNGs 	

Finish



Wenn Sie auf der Seite Richtlinien konfigurieren bleiben, können Sie eine Richtlinie nach Änderungen erneut simulieren, ohne die Namen der Testobjekte erneut eingeben zu müssen.

Beispiel 3: Korrektur einer Regel bei der Simulation einer vorgeschlagenen 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 dient zum Suchen von Objekten, die über solche verfügen `series=x-men` Benutzer-Metadaten: Bei der Simulation dieser Richtlinie gegen die traten jedoch unerwartete Ergebnisse auf `Beast.jpg` Objekt: Anstatt die X-Men-Metadatenregel zu entsprechen, kopiert das Objekt die Standardregel. Zwei Rechenzentren werden kopiert.



Simulate ILM Policy - Demo

Simulates the active ILM policy or, if there is a proposed ILM policy, simulates the proposed ILM policy. Use this simulation to test the current configuration of ILM rules and determine whether ILM rules copy and place object data as intended.

Object

Simulate


Simulation Results

Object	Rule Matched	Previous Match	
photos/Beast.jpg	Two copies two data centers 		

Finish

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. Zeigen Sie für jede Regel in der Richtlinie die Regeleinstellungen an, indem Sie auf den Regelnamen oder das Symbol Weitere Details klicken  In jedem Dialogfeld, in dem die Regel angezeigt wird.
2. Prüfen Sie das Mandantenkonto der Regel, die Referenzzeit und die Filterkriterien.

In diesem Beispiel enthält die Metadaten für die X-Men-Regel einen Fehler. Der Metadatenwert wurde als „x-men1“ anstelle von „x-men.“ eingegeben.

X-men

Ingest Behavior: Balanced
Tenant Account: 06846027571548027538
Reference Time: Ingest Time
Filtering Criteria:

Matches all of the following metadata:

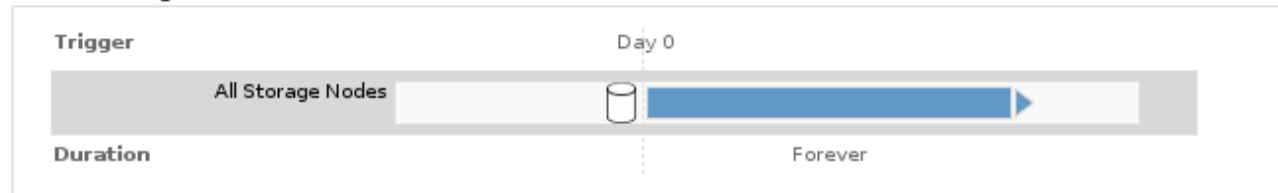
User Metadata

series

equals

x-men1

Retention Diagram:



Close

3. Um den Fehler zu beheben, korrigieren Sie die Regel wie folgt:

- Wenn die Regel Teil der vorgeschlagenen 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 eine Regel nicht bearbeiten oder aus der aktiven Richtlinie entfernen.

Option	Beschreibung
Klonen der Regel	<ol style="list-style-type: none">Wählen Sie ILM > Regeln.Wählen Sie die falsche Regel aus, und klicken Sie auf Clone.Ändern Sie die falschen Informationen, und klicken Sie auf Speichern.Wählen Sie ILM > Richtlinien.Wählen Sie die vorgeschlagene Richtlinie aus, und klicken Sie auf Bearbeiten.Klicken Sie Auf Regeln Auswählen.Aktivieren Sie das Kontrollkästchen für die neue Regel, deaktivieren Sie das Kontrollkästchen für die ursprüngliche Regel, und klicken Sie auf Anwenden.Klicken Sie Auf Speichern.

Option	Beschreibung
Bearbeiten der Regel	<ol style="list-style-type: none"> Wählen Sie die vorgeschlagene Richtlinie aus, und klicken Sie auf Bearbeiten. Klicken Sie auf das Löschsymbol ✖ Um die falsche Regel zu entfernen, und klicken Sie auf Speichern. Wählen Sie ILM > Regeln. Wählen Sie die falsche Regel aus, und klicken Sie auf Bearbeiten. Ändern Sie die falschen Informationen, und klicken Sie auf Speichern. Wählen Sie ILM > Richtlinien. Wählen Sie die vorgeschlagene Richtlinie aus, und klicken Sie auf Bearbeiten. Wählen Sie die korrigierte Regel aus, klicken Sie auf Anwenden und klicken Sie auf Speichern.

4. Führen Sie die Simulation erneut aus.



Da Sie zur Bearbeitung der Regel nicht mehr auf der Seite ILM-Richtlinien navigiert haben, werden die zuvor für die Simulation eingegebenen Objekte nicht mehr angezeigt. Sie müssen die Namen der Objekte erneut eingeben.

In diesem Beispiel entspricht die korrigierte X-Men-Regel nun dem `Beast.jpg` Objekt auf Grundlage des `series=x-men` Benutzer-Metadaten, wie erwartet.

Simulate ILM Policy - Demo

Simulates the active ILM policy or, if there is a proposed ILM policy, simulates the proposed ILM policy. Use this simulation to test the current configuration of ILM rules and determine whether ILM rules copy and place object data as intended.

Object

Simulation Results ?

Object	Rule Matched	Previous Match	
photos/Beast.jpg	X-men		✖

Aktivieren der ILM-Richtlinie

Wenn Sie einer vorgeschlagenen ILM-Richtlinie ILM-Regeln hinzufügen, die Richtlinie simulieren und bestätigen, dass es sich wie erwartet verhält, sind Sie bereit, die vorgeschlagene Richtlinie zu aktivieren.

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.
- Sie müssen über spezifische Zugriffsberechtigungen verfügen.
- Sie müssen die vorgeschlagene ILM-Richtlinie gespeichert und simuliert haben.



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.

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.

- Nehmen Richtlinienänderungen vor, die die Datenredundanz oder Aufbewahrungszeit verbessern, 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.
- Bei Richtlinienänderungen, die Datenredundanz oder -Langlebigkeit verringern könnten, werden diese Änderungen erst implementiert, wenn alle Grid-Nodes 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 als „aktiv,“ gekennzeichnet. Sie wird jedoch nicht wirksam, bis alle Knoten online und verfügbar sind.

Schritte

1. Wenn Sie bereit sind, eine vorgeschlagene Richtlinie zu aktivieren, wählen Sie die Richtlinie auf der Seite ILM-Richtlinien aus, und klicken Sie auf **Aktivieren**.

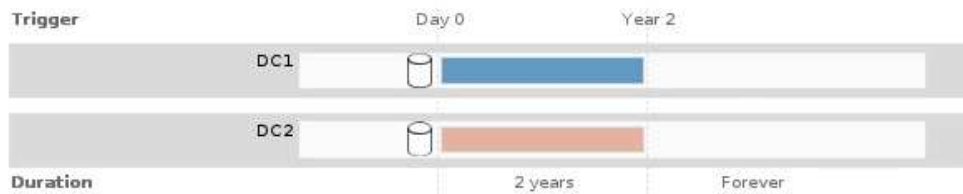
Es wird eine Warnmeldung angezeigt, in der Sie aufgefordert werden, zu bestätigen, dass Sie die vorgeschlagene Richtlinie aktivieren möchten.

Eine Eingabeaufforderung wird in der Warnmeldung angezeigt, wenn die Standardregel für die Richtlinie Objekte nicht für immer enthält. In diesem Beispiel zeigt das Aufbewahrungsdigramm, dass die Standardregel Objekte nach 2 Jahren löscht. Sie müssen **2** in das Textfeld eingeben, um zu bestätigen, dass Objekte, die nicht mit einer anderen Regel in der Richtlinie übereinstimmt, nach 2 Jahren aus StorageGRID entfernt werden.

⚠ Activate the proposed policy

Errors in an ILM policy can cause irreparable data loss. Review and test the policy carefully before activating.

The default rule in this policy does not retain objects forever. Confirm this is the behavior you want by referring to the retention diagram for the default rule:



Now, complete the following prompt:

Any objects that are not matched by another rule in this policy will be deleted after years.

Are you sure you want to activate the proposed policy?

Cancel

OK

2. Klicken Sie auf **OK**.

Ergebnis

Wenn eine neue ILM-Richtlinie aktiviert wurde:

- Die Richtlinie wird in der Tabelle auf der Seite ILM-Richtlinien mit einem Status von „aktiv“ angezeigt. Der Eintrag Startdatum gibt das Datum und die Uhrzeit an, zu der die Richtlinie aktiviert wurde.

ILM Policies

Review the proposed, active, and historical policies. You can create, edit, or delete a proposed policy; clone the active policy; or view the details for any policy.

+ Create Proposed Policy Clone Edit Remove			
Policy Name	Policy State	Start Date	End Date
<input checked="" type="radio"/> New Policy	Active	2017-07-20 18:49:53 MDT	
<input type="radio"/> Baseline 2 Copies Policy	Historical	2017-07-19 21:24:30 MDT	2017-07-20 18:49:53 MDT

- Die zuvor aktive Richtlinie wird mit dem Status „Historische Richtlinien“ angezeigt. Die Einträge Startdatum und Enddatum geben an, wann die Richtlinie aktiv wurde und wann sie nicht mehr wirksam war.

Verwandte Informationen

["Beispiel 6: Ändern einer ILM-Richtlinie"](#)

Überprüfen einer ILM-Richtlinie mit Objekt-Metadaten-Lookup

Sobald Sie eine ILM-Richtlinie aktiviert haben, sollten Sie repräsentative Testobjekte in das StorageGRID System aufnehmen. Anschließend sollten Sie eine Objektmetadaten abfragen durchführen, um zu bestätigen, ob Kopien wie vorgesehen erstellt und an den richtigen Orten platziert werden.

Was Sie benötigen

- Sie müssen über eine Objektkennung verfügen, die einer der folgenden sein kann:
 - UUID:** Der Universally Unique Identifier des Objekts. Geben Sie die UUID in allen Großbuchstaben ein.

- **CBID:** Die eindeutige Kennung des Objekts in StorageGRID. Sie können die CBID eines Objekts aus dem Prüfprotokoll abrufen. Geben Sie die CBID in allen Großbuchstaben ein.
- **S3-Bucket und Objektschlüssel:** Bei Aufnahme eines Objekts über die S3-Schnittstelle verwendet die Client-Applikation eine Bucket- und Objektschlüsselkombination, um das Objekt zu speichern und zu identifizieren.
- **Swift Container und Objektname:** Wenn ein Objekt über die Swift-Schnittstelle aufgenommen wird, verwendet die Client-Anwendung eine Container- und Objektname-Kombination, um das Objekt zu speichern und zu identifizieren.

Schritte

1. Aufnahme des Objekts.
2. Wählen Sie **ILM > Objekt Metadaten Lookup** aus.
3. Geben Sie die Kennung des Objekts in das Feld **Kennung** ein.

Sie können eine UUID, CBID, S3 Bucket/Objektschlüssel oder Swift Container/Objektname eingeben.

Object Metadata Lookup

Enter the identifier for any object stored in the grid to view its metadata.

Identifier

source/testobject

Look Up

4. Klicken Sie Auf **Look Up**.

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

- Systemmetadaten, einschließlich Objekt-ID (UUID), Objektname, Name des Containers, Mandantenkontenname oder -ID, logische Größe des Objekts, Datum und Uhrzeit der ersten Erstellung des Objekts sowie Datum und Uhrzeit der letzten Änderung des Objekts.
- 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.

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

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": {
      "PALS": "2",

```

5. Vergewissern Sie sich, dass das Objekt am richtigen Ort und an den richtigen Stellen gespeichert ist und dass es sich um den richtigen Kopiertyp handelt.



Wenn die Option „Audit“ aktiviert ist, können Sie auch das Audit-Protokoll für die Meldung „ORLM-Objektregeln erfüllt“ überwachen. Die ORLM-Prüfmeldung kann Ihnen mehr Informationen über den Status des ILM-Auswertungsprozesses zur Verfügung stellen, jedoch kann sie Ihnen keine Informationen über die Richtigkeit der Platzierung der Objektdaten oder die Vollständigkeit der ILM-Richtlinie liefern. Das müssen Sie selbst beurteilen. Weitere Informationen finden Sie in den Informationen zum Verständnis von Überwachungsmeldungen.

Verwandte Informationen

["Prüfung von Audit-Protokollen"](#)

["S3 verwenden"](#)

["Verwenden Sie Swift"](#)

Arbeiten mit ILM-Regeln und ILM-Richtlinien

Sobald Sie ILM-Regeln und eine ILM-Richtlinie erstellt haben, können Sie sie weiterhin verwenden und ihre Konfiguration an die sich ändernden Storage-Anforderungen anpassen.

Löschen einer ILM-Regel

Löschen Sie alle ILM-Regeln, die Sie wahrscheinlich nicht verwenden, um die Liste der aktuellen ILM-Regeln überschaubar zu halten.

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.
- Sie müssen über spezifische Zugriffsberechtigungen verfügen.



Eine ILM-Regel kann nicht gelöscht werden, wenn sie derzeit in der aktiven Richtlinie oder in der vorgeschlagenen Richtlinie verwendet wird. Wenn Sie eine ILM-Regel löschen müssen, die eine Richtlinie verwendet, müssen Sie zuerst die folgenden Schritte durchführen:

1. Klonen Sie die aktive Richtlinie, oder bearbeiten Sie die vorgeschlagene Richtlinie.
2. Entfernen Sie die ILM-Regel aus der Richtlinie.
3. Speichern, simulieren und aktivieren Sie die neue Richtlinie, um sicherzustellen, dass Objekte wie erwartet geschützt sind.

Schritte

1. Wählen Sie **ILM > Regeln**.
2. Überprüfen Sie den Tabelleneintrag für die Regel, die Sie entfernen möchten.

Vergewissern Sie sich, dass die Regel nicht in der aktiven ILM-Richtlinie oder der vorgeschlagenen ILM-Richtlinie verwendet wird.

3. Wenn die Regel, die Sie entfernen möchten, nicht verwendet wird, wählen Sie die Optionsschaltfläche und wählen Sie **Entfernen**.
4. Wählen Sie **OK** aus, um zu bestätigen, dass Sie die ILM-Regel löschen möchten.

Die ILM-Regel wird gelöscht.

Wenn Sie eine Regel löschen, die in einer historischen Richtlinie verwendet wird, wird ein ⓘ
Wenn Sie die Richtlinie anzeigen, wird das Symbol für die Regel angezeigt. Dies bedeutet, dass die Regel zu einer historischen Regel geworden ist.

Viewing Historical Policy - Example ILM policy

Review the rules in this policy. If this is a proposed policy, click Simulat

Reason for change: new policy

Rules are evaluated in order, starting from the top

Rule Name

Erasure code larger objects

2 copies 2 sites ⓘ

This is a historical ILM rule.
Historical rules are rules that
were included a policy and then
edited or deleted after the policy
became historical.

Verwandte Informationen

["ILM-Richtlinie erstellen"](#)

Bearbeiten einer ILM-Regel

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

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.
- Sie müssen über spezifische Zugriffsberechtigungen verfügen.

Über diese Aufgabe

Eine Regel kann nicht bearbeitet werden, wenn sie in der vorgeschlagenen ILM-Richtlinie oder der aktiven ILM-Richtlinie verwendet wird. Stattdessen können Sie diese Regeln klonen und erforderliche Änderungen an der geklonten Kopie vornehmen. Sie können auch die ILM-Regel (2 Kopien erstellen) oder ILM-Regeln, die vor StorageGRID Version 10.3 erstellt wurden, nicht bearbeiten.



Bevor Sie einer aktiven ILM-Richtlinie eine bearbeitete Regel hinzufügen, müssen Sie beachten, dass eine Änderung der Anweisungen zur Platzierung eines Objekts zu einer erhöhten Systemauslastung führen kann.

Schritte

1. Wählen Sie **ILM > Regeln**.

Die Seite ILM-Regeln wird angezeigt. Diese Seite zeigt alle verfügbaren Regeln an und gibt an, welche Regeln in der aktiven Richtlinie oder in der vorgeschlagenen Richtlinie verwendet werden.

ILM Rules

Information lifecycle management (ILM) rules determine how and where object data is stored over time. Every object ingested into the StorageGRID Webscale is evaluated against the ILM rules that make up the active ILM policy. Use this page to manage and view ILM rules. You cannot edit or remove an ILM rule that is used by an active or proposed ILM policy.

<div><div>+ Create</div><div> Edit</div><div> Clone</div><div> Remove</div></div>		
Name	Used In Active Policy	Used In Proposed Policy
<input type="radio"/> Make 2 Copies	✓	✓
<input type="radio"/> PNGs		✓
<input checked="" type="radio"/> JPGs		
<input type="radio"/> X-men		✓

2. Wählen Sie eine Regel aus, die nicht verwendet wird, und klicken Sie auf **Bearbeiten**.

Der Assistent zum Bearbeiten der ILM-Regel wird geöffnet.

Edit ILM Rule Step 1 of 3: Define Basics

Name

JPGs

Description

Tenant Accounts (optional)

Tenant-01 (16229710975421005503) ✕

Tenant-04 (83132053388229808098) ✕

Bucket Name

contains

▼

az-01

Advanced filtering... (0 defined)


Cancel

Next

3. Füllen Sie die Seiten des Assistenten zur Bearbeitung von ILM-Regeln aus und befolgen Sie die Schritte zum Erstellen einer ILM-Regel, und verwenden Sie gegebenenfalls erweiterte Filter.

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

4. Klicken Sie Auf **Speichern**.

Wenn Sie eine Regel bearbeiten, die in einer historischen Richtlinie verwendet wird, wird ein  Wenn Sie die Richtlinie anzeigen, wird das Symbol für die Regel angezeigt. Dies bedeutet, dass die Regel zu einer historischen Regel geworden ist.

Viewing Historical Policy - Example ILM policy

Review the rules in this policy. If this is a proposed policy, click Simulat

Reason for change: new policy

Rules are evaluated in order, starting from the top

Rule Name

Erasure code larger objects

2 copies 2 sites  

This is a historical ILM rule.
Historical rules are rules that
were included a policy and then
edited or deleted after the policy
became historical.

Verwandte Informationen

["Erstellen einer ILM-Regel"](#)

["Verwendung erweiterter Filter in ILM-Regeln"](#)

Klonen einer ILM-Regel

Eine Regel kann nicht bearbeitet werden, wenn sie in der vorgeschlagenen ILM-Richtlinie oder der aktiven ILM-Richtlinie verwendet wird. Stattdessen können Sie eine Regel klonen und alle erforderlichen Änderungen an der geklonten Kopie vornehmen. Anschließend können Sie die ursprüngliche Regel bei Bedarf aus der vorgeschlagenen Richtlinie entfernen und durch die geänderte Version ersetzen. Sie können keine ILM-Regel klonen, wenn sie mit StorageGRID Version 10.2 oder früher erstellt wurde.

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.
- Sie müssen über spezifische Zugriffsberechtigungen verfügen.

Über diese Aufgabe

Bevor Sie einer aktiven ILM-Richtlinie eine geklonte Regel hinzufügen, sollten Sie beachten, dass eine Änderung der Anweisungen zur Platzierung eines Objekts zu einer erhöhten Systemauslastung führen kann.

Schritte

1. Wählen Sie **ILM > Regeln**.

Die Seite ILM-Regeln wird angezeigt.

ILM Rules

Information lifecycle management (ILM) rules determine how and where object data is stored over time. Every object ingested into the StorageGRID Webscale is evaluated against the ILM rules that make up the active ILM policy. Use this page to manage and view ILM rules. You cannot edit or remove an ILM rule that is used by an active or proposed ILM policy.

<div><div>+ Create</div><div> Edit</div><div> Clone</div><div> Remove</div></div>			
	Name	Used In Active Policy	Used In Proposed Policy
<input type="radio"/>	Make 2 Copies	✓	✓
<input type="radio"/>	PNGs		✓
<input checked="" type="radio"/>	JPGs		
<input type="radio"/>	X-men		✓

2. Wählen Sie die ILM-Regel aus, die Sie klonen möchten, und klicken Sie auf **Clone**.

Der Assistent für die Erstellung von ILM-Regeln wird geöffnet.

3. Aktualisieren Sie die geklonte Regel, indem Sie die Schritte zum Bearbeiten einer ILM-Regel und Verwenden erweiterter Filter ausführen.

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

4. Klicken Sie Auf **Speichern**.

Die neue ILM-Regel wird erstellt.

Verwandte Informationen

["Arbeiten mit ILM-Regeln und ILM-Richtlinien"](#)

["Verwendung erweiterter Filter in ILM-Regeln"](#)

Anzeigen der Aktivitätswarteschlange für ILM-Richtlinien

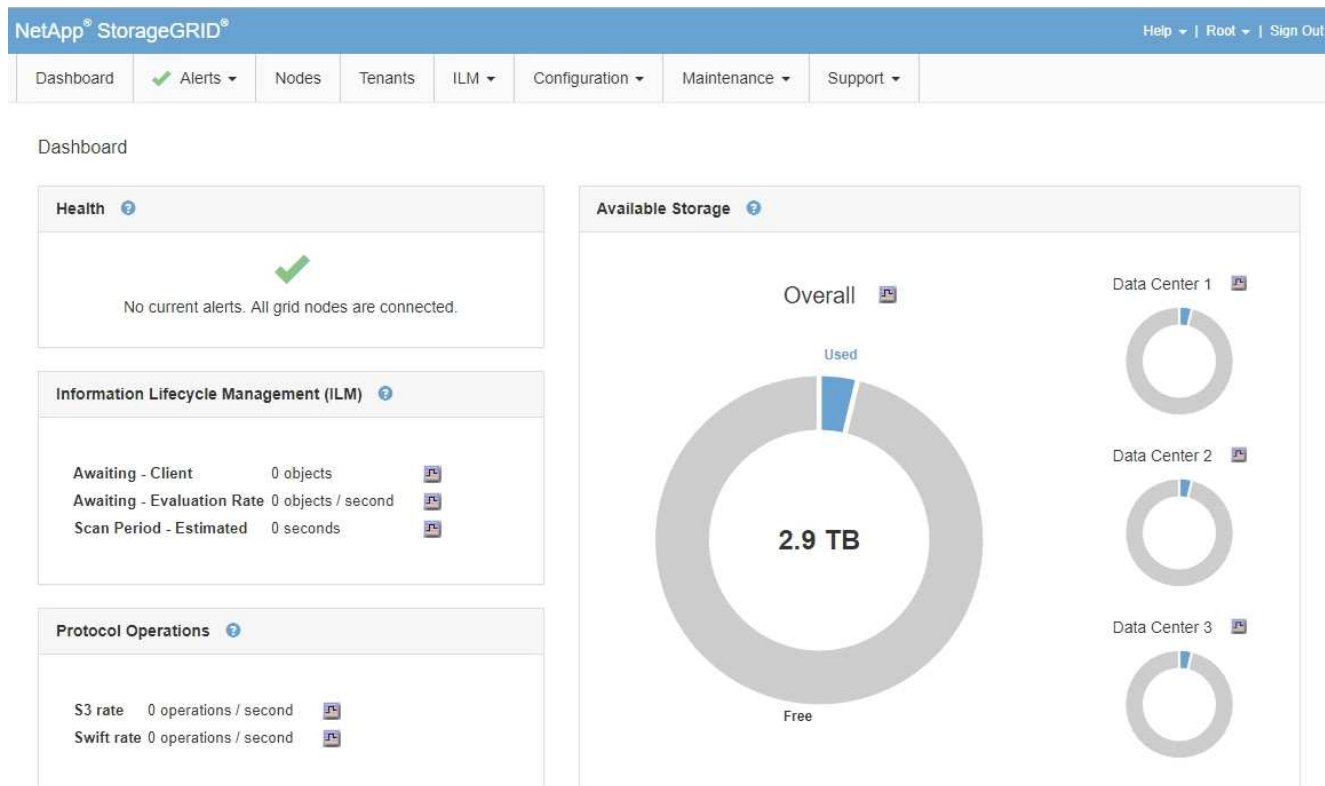
Sie können jederzeit die Anzahl der Objekte anzeigen, die sich in der Warteschlange befinden, die mit der ILM-Richtlinie bewertet werden sollen. Möglicherweise möchten Sie die ILM-Verarbeitungswarteschlange überwachen, um die System-Performance zu ermitteln. Eine große Warteschlange könnte darauf hindeuten, dass das System nicht mit der Aufnahmerate Schritt halten kann, dass die Last von den Client-Anwendungen zu groß ist oder dass ein anormaler Zustand vorhanden ist.

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.
- Sie müssen über spezifische Zugriffsberechtigungen verfügen.

Schritte

1. Wählen Sie **Dashboard**.



2. Überwachen Sie den Abschnitt Information Lifecycle Management (ILM).

Sie können auf das Fragezeichen klicken Um eine Beschreibung der Elemente in diesem Abschnitt anzuzeigen.

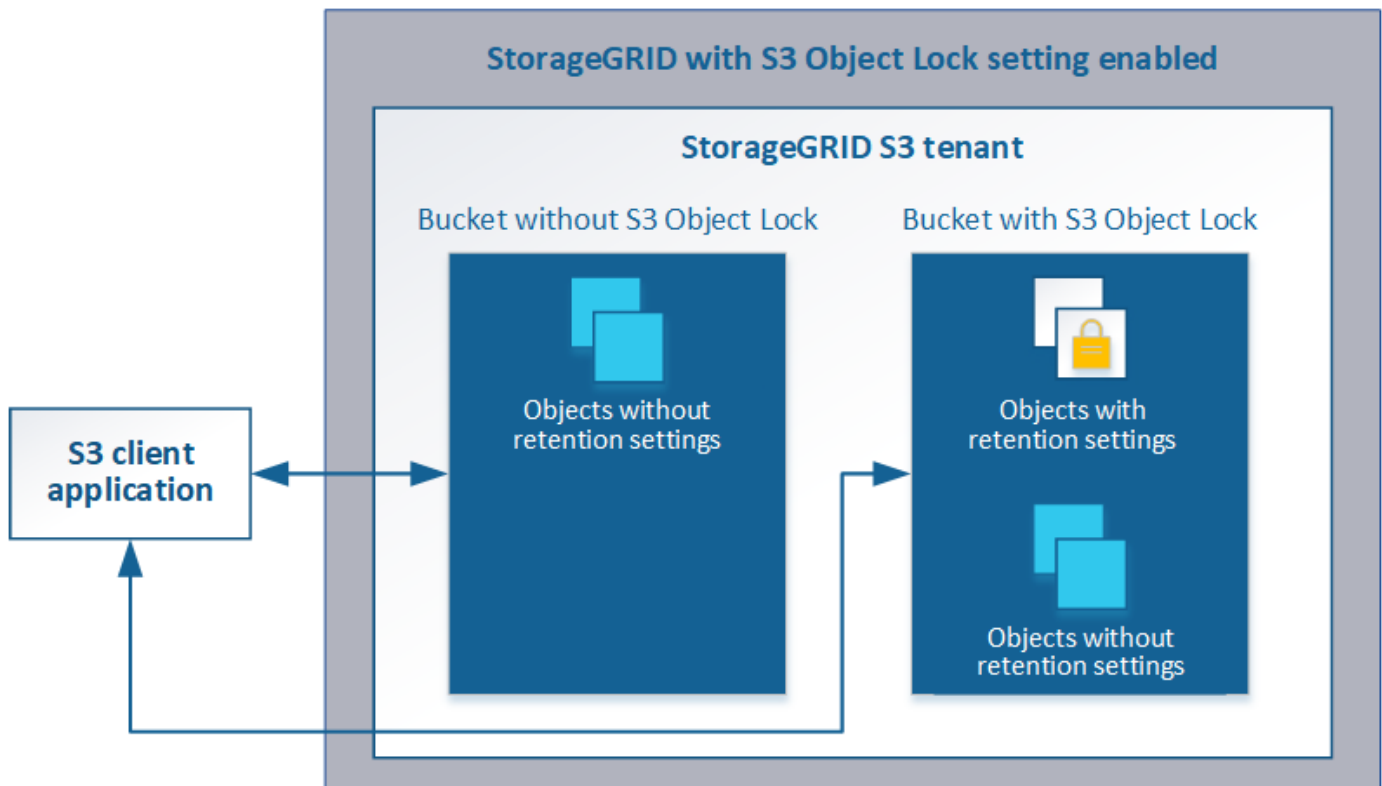
Verwalten von Objekten mit S3 Object Lock

Als Grid-Administrator können Sie die S3 Objektsperre für Ihr StorageGRID System aktivieren und eine konforme ILM-Richtlinie implementieren. So wird sichergestellt, dass Objekte in bestimmten S3-Buckets nicht für eine bestimmte Zeit 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-Objektsperre für ein StorageGRID-System aktiviert ist, kann ein S3-Mandantenkonto Buckets mit oder ohne aktivierte S3-Objektsperre erstellen. Wenn in einem Bucket S3-Objektsperre aktiviert ist, können S3-Client-Applikationen optional Aufbewahrungseinstellungen für jede Objektversion in diesem Bucket angeben. Eine Objektversion muss über Aufbewahrungseinstellungen verfügen, die durch S3 Object Lock geschützt werden sollen.



Die StorageGRID S3 Objektsperre bietet einen einheitlichen Aufbewahrungsmodus, der dem Amazon S3-Compliance-Modus entspricht. Standardmäßig kann eine geschützte Objektversion nicht von einem Benutzer überschrieben oder gelöscht werden. Die StorageGRID S3-Objektsperre unterstützt keinen Governance-Modus und erlaubt Benutzern mit speziellen Berechtigungen nicht, Aufbewahrungseinstellungen zu umgehen oder geschützte Objekte zu löschen.

Wenn in einem Bucket S3-Objektsperre aktiviert ist, kann die S3-Client-Applikation beim Erstellen oder Aktualisieren eines Objekts optional eine oder beide der folgenden Aufbewahrungseinstellungen auf Objektebene angeben:

- **Bis-Datum aufbewahren:** Wenn das Aufbewahrungsdatum einer Objektversion in der Zukunft liegt, kann das Objekt abgerufen, aber nicht geändert oder gelöscht werden. Bei Bedarf kann das Aufbewahrungsdatum eines Objekts erhöht werden, dieses Datum kann jedoch nicht verringert 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 Aufbewahrungspflicht haben kein Ablaufdatum, bleiben aber bis zur ausdrücklichen Entfernung erhalten. Die gesetzlichen Aufbewahrungspflichten sind unabhängig von der bisherigen Aufbewahrungsfrist.

Weitere Informationen zu diesen Einstellungen finden Sie unter „Using S3 object Lock“ in ["Unterstützte Vorgänge und Einschränkungen durch S3-REST-API"](#).

Vergleich der S3-Objektsperre mit älterer Compliance

Die S3-Objektsperrefunktion in StorageGRID 11.5 ersetzt die in früheren StorageGRID-Versionen verfügbare Compliance-Funktion. Da die neue S3-Objektsperrefunktion den Amazon S3-Anforderungen entspricht, depretiert sie die proprietäre StorageGRID-Compliance-Funktion, die jetzt als „Legacy-Compliance“ bezeichnet wird.

Wenn Sie zuvor die globale Compliance-Einstellung aktiviert haben, wird die neue globale S3-Objektsperre beim Upgrade auf StorageGRID 11.5 automatisch aktiviert. Mandantenbenutzer können keine neuen Buckets erstellen, für die in StorageGRID 11.5 die Compliance aktiviert ist. Mandantenbenutzer können jedoch nach Bedarf alle vorhandenen, Compliance-Buckets weiterhin verwenden und managen. Dazu gehören auch die Durchführung der folgenden Aufgaben:

- Einbinden neuer Objekte in einen vorhandenen Bucket, für den veraltete Compliance aktiviert ist
- Verlängern der Aufbewahrungsfrist für einen vorhandenen Bucket, für den die veraltete Compliance-Funktion aktiviert ist
- Ändern der Einstellung zum automatischen Löschen für einen vorhandenen Bucket, für den die alte Compliance aktiviert ist
- Wenn Sie einen gesetzlichen Aufbewahrungspflichten auf einem vorhandenen Bucket platzieren, für den die veraltete Compliance-Funktion aktiviert ist.
- Anheben eines gesetzlichen Haltes

"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-Objektsperrefunktion in StorageGRID verglichen wird.

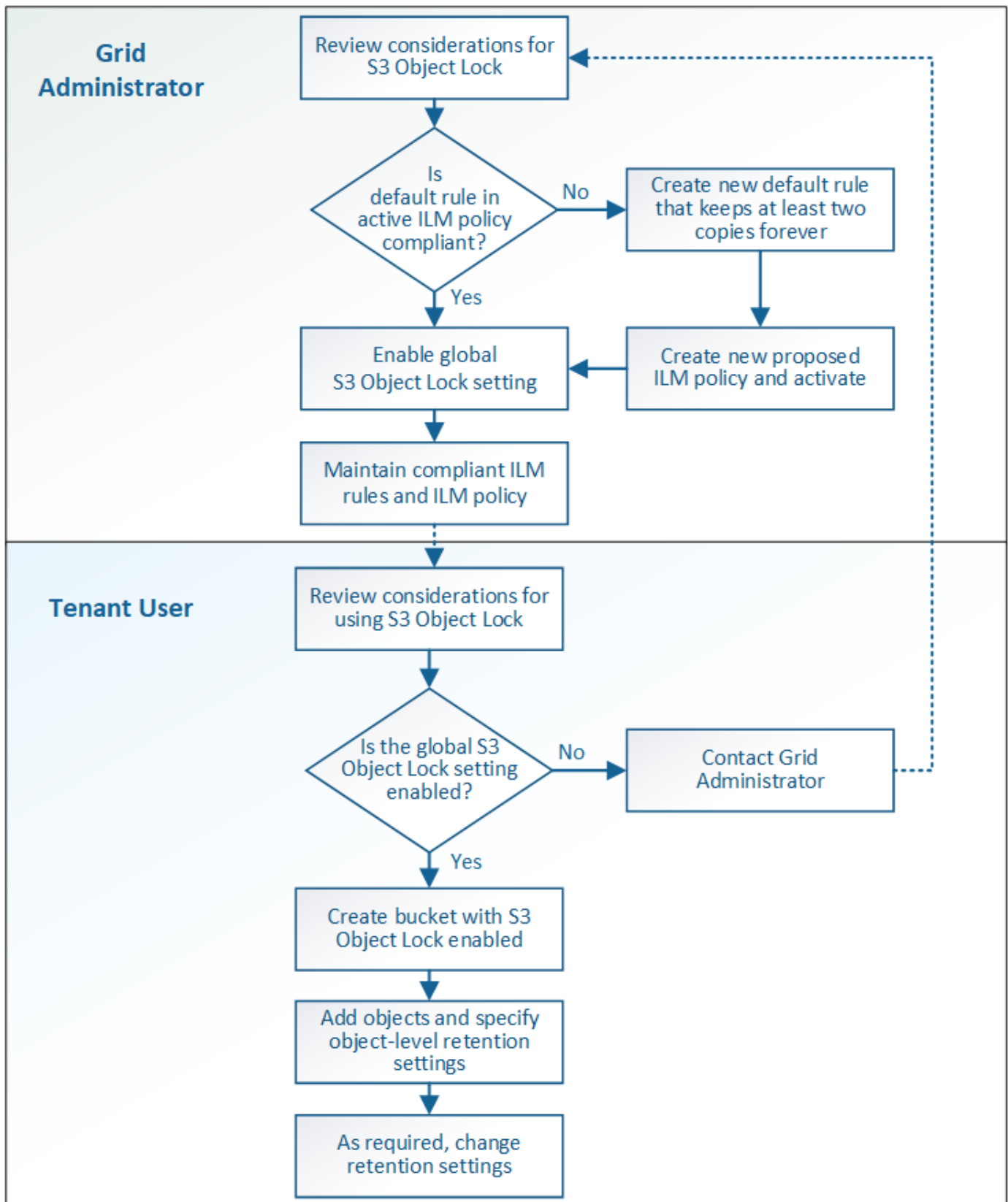
	S3-Objektsperre (neu)	Compliance (alt)
Wie wird die Funktion global aktiviert?	Wählen Sie im Grid Manager die Option Konfiguration > Systemeinstellungen > S3 Objektsperre .	Wird nicht mehr unterstützt. Hinweis: Wenn Sie zuvor die globale Compliance-Einstellung aktiviert haben, wird die globale S3-Objektsperre automatisch aktiviert, wenn Sie auf StorageGRID 11.5 aktualisieren.
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.	Benutzer können keine neuen Buckets mehr erstellen, für die Compliance aktiviert ist. Sie können jedoch auch weiterhin vorhandene konforme Buckets hinzufügen.
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 Die alte Compliance-Funktion ermöglicht keine Bucket-Versionierung.
Wie wird die Objektaufbewahrung festgelegt?	Benutzer können für jede Objektversion ein „bis-Datum beibehalten“ festlegen.	Benutzer müssen eine Aufbewahrungsfrist für den gesamten Bucket festlegen. Der Aufbewahrungszeitraum gilt für alle Objekte im Bucket.

	S3-Objektsperre (neu)	Compliance (alt)
Kann ein Bucket Standardeinstellungen für Aufbewahrung und Aufbewahrung gesetzlicher Aufbewahrungspflichten haben?	Nein Für StorageGRID-Buckets, für die S3-Objektsperre aktiviert ist, ist kein Standardaufbewahrungszeitraum vorhanden. Stattdessen können Sie für jede Objektversion ein „bis-Aufbewahrung“-Datum angeben.	Ja.
Kann der Aufbewahrungszeitraum geändert werden?	Die Aufbewahrung bis zum Datum für eine Objektversion kann erhöht, aber nie verkleinert werden.	Die Aufbewahrungsfrist des 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?	Eine Objektversion kann nach Erreichen des Aufbewahrungsdatums gelöscht werden, vorausgesetzt, das Objekt befindet sich nicht in der gesetzlichen Aufbewahrungspflichten.	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

Workflow für S3 Objektsperre

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 Workflow-Diagramm zeigt die grundlegenden Schritte zur Verwendung der S3-Objektsperre. Die Schritte werden vom Grid-Administrator und von Mandantenbenutzern durchgeführt.



Den Grid-Administratoren stehen

Wie das Workflow-Diagramm zeigt, muss ein Grid-Administrator zwei übergeordnete Aufgaben durchführen, bevor S3-Mandanten S3-Objektsperre verwenden können:

1. Erstellen Sie mindestens eine kompatible ILM-Regel und stellen Sie diese Regel in der aktiven ILM-Richtlinie zur Standardregel bereit.
2. Aktivieren Sie die globale S3-Objektsperre für das gesamte StorageGRID-System.

Aufgaben für Mandanten

Nach Aktivierung der globalen S3-Objektsperre können Mandanten die folgenden Aufgaben ausführen:

1. Erstellen Sie Buckets, für die S3-Objektsperre aktiviert ist.
2. Fügen Sie diesen Buckets Objekte hinzu, und legen Sie Aufbewahrungszeiträume auf Objektebene sowie Einstellungen für die Aufbewahrung rechtlicher Daten fest.
3. Aktualisieren Sie je nach Bedarf eine Aufbewahrungsfrist oder ändern Sie die Einstellung für die gesetzliche Aufbewahrungspflichten für ein einzelnes Objekt.

Verwandte Informationen

["Verwenden Sie ein Mandantenkonto"](#)

["S3 verwenden"](#)

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-Objektsperre aktiviert haben, können Sie die Einstellung nicht deaktivieren.
- Die globale S3-Objektsperre kann nur aktiviert werden, wenn die Standardregel in der aktiven ILM-Richtlinie *konform* ist (das heißt, die Standardregel muss die Anforderungen von Buckets erfüllen, wenn S3 Object Lock aktiviert ist).
- Wenn die globale S3 Object Lock-Einstellung aktiviert ist, können Sie keine neue vorgeschlagene ILM-Richtlinie erstellen oder eine vorhandene vorgeschlagene ILM-Richtlinie aktivieren, wenn die Standardregel in der Richtlinie nicht konform ist. Nachdem die globale S3 Object Lock-Einstellung aktiviert wurde, geben die Seiten ILM-Regeln und ILM-Richtlinien an, welche ILM-Regeln konform sind.

Im folgenden Beispiel führt die Seite ILM-Regeln drei Regeln auf, die mit Buckets kompatibel sind, bei denen S3 Object Lock aktiviert ist.

<div> <div>+ Create</div> <div>Clone</div> <div>Edit</div> <div>Remove</div> </div>			
Name	Compliant	Used In Active Policy	Used In Proposed Policy
Make 2 Copies	✓	✓	
Compliant Rule: EC for objects in bank-records bucket	✓		
2 copies 10 years, Archive forever			
2 Copies 2 Data Centers	✓		

Compliant Rule: EC for objects in bank-records bucket

Description:

2+1 EC at one site

Ingest Behavior:

Balanced

Compliant:

Yes

Tenant Accounts:

Bank of ABC (94793396288150002349)

Bucket Name:

equals 'bank-records'

Reference Time:

Ingest Time

Anforderungen für konforme ILM-Regeln

Wenn Sie die globale S3-Objektsperre aktivieren möchten, müssen Sie sicherstellen, dass die Standardregel in Ihrer aktiven ILM-Richtlinie 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 Platzierung vorhanden sein.
- Objektkopien können nicht in einem Cloud-Storage-Pool gespeichert werden.
- Objektkopien können nicht auf Archiv-Knoten gespeichert werden.
- Mindestens eine Zeile der Platzierungsanweisungen muss am Tag 0 beginnen und als Referenzzeit **Aufnahmezeit** verwenden.
- Mindestens eine Zeile der Platzierungsanweisungen muss „Forever“ sein.

Diese Regel erfüllt beispielsweise die Anforderungen von Buckets, wenn die S3-Objektsperre aktiviert ist. Es werden zwei replizierte Objektkopien von der Aufnahmezeit (Tag 0) bis „` für immer“ gespeichert. Die Objekte werden auf Storage-Nodes in zwei Datacentern gespeichert.

Compliant rule: 2 replicated copies at 2 sites

Description:

2 replicated copies on Storage Nodes from Day 0 to Forever

Ingest Behavior:

Balanced

Compliant:

Yes

Tenant Accounts:

Bank of ABC (94793396288150002349)

Reference Time:

Ingest Time

Filtering Criteria:

Matches all objects.

Retention Diagram:

Trigger

Day 0

dc1

dc2

Duration

Forever

Anforderungen für aktive und vorgeschlagene ILM-Richtlinien

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

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

Eine ILM-konforme Richtlinie kann folgende drei Regeln umfassen:

1. Eine konforme Regel, die Erasure-codierte Kopien der Objekte in einem bestimmten Bucket erstellt und bei aktivierter S3-Objektsperre aktiviert ist. Die EC-Kopien werden von Tag 0 bis für immer auf Storage-Nodes gespeichert.
2. Eine nicht konforme Regel, die zwei replizierte Objektkopien auf Storage-Nodes für ein Jahr erstellt und dann eine Objektkopie zu Archivierungs-Nodes verschiebt und die Kopie für immer speichert. Diese Regel gilt nur für Buckets, für die die S3-Objektsperre oder ältere Compliance nicht aktiviert ist, da nur eine Objektkopie für immer gespeichert wird und Archiv-Nodes verwendet werden.
3. Eine konforme Standardregel, die zwei replizierte Objektkopien auf Storage-Nodes von Tag 0 bis für immer erstellt. Diese Regel gilt für alle Objekte in jedem Bucket, die nicht durch die ersten beiden Regeln herausgefiltert wurden.

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.

In diesem Beispiel aus dem Tenant Manager wird ein Bucket angezeigt, in dem S3 Object Lock aktiviert ist.

Buckets

Create buckets and manage bucket settings.

1 bucket

Create bucket

Actions ▾						
<input type="checkbox"/>	Name ▾	S3 Object Lock ? ▾	Region ▾	Object Count ? ▾	Space Used ? ▾	Date Created ▾
<input type="checkbox"/>	bank-records	✓	us-east-1	0	0 bytes	2021-01-06 16:53:19 MST

← Previous 1 Next →

- 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.
- Bucket-Versionierung ist mit S3 Object Lock erforderlich. Wenn die S3-Objektsperre für einen Bucket aktiviert ist, ermöglicht StorageGRID automatisch die Versionierung für diesen Bucket.

- Nachdem Sie einen Bucket mit aktivierter S3-Objektsperre erstellt haben, können Sie die S3-Objektsperre oder die Versionierung für diesen Bucket nicht deaktivieren.
- Ein StorageGRID-Bucket mit aktivierter S3-Objektsperre hat keinen standardmäßigen Aufbewahrungszeitraum. Stattdessen kann die S3-Client-Applikation optional für jede Objektversion, die zu diesem Bucket hinzugefügt wird, ein Aufbewahrungsdatum und eine Einstellung für die Aufbewahrung gemäß den gesetzlichen Aufbewahrungspflichten festlegen.
- Bucket-Lifecycle-Konfiguration wird für S3-Objekt-Lifecycle-Buckets unterstützt.
- 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

- Die S3-Client-Applikation muss Aufbewahrungseinstellungen für jedes Objekt angeben, das durch die S3-Objektsperre geschützt werden muss.
- Sie können das Aufbewahrungsdatum für eine Objektversion erhöhen, diesen Wert jedoch nie reduzieren.
- Wenn Sie über eine ausstehende rechtliche oder behördliche Untersuchung informiert werden, können Sie relevante Informationen erhalten, indem Sie eine gesetzliche Aufbewahrungspflichten auf eine Objektversion setzen. Wenn eine Objektversion unter einer gesetzlichen Aufbewahrungspflichten liegt, kann das Objekt nicht aus StorageGRID gelöscht werden, auch wenn es seine Aufbewahrungsfrist bis zum letzten Tag erreicht hat. Sobald die gesetzliche Aufbewahrungspflichten aufgehoben sind, kann die Objektversion gelöscht werden, wenn das Aufbewahrungsdatum erreicht ist.
- Für die S3-Objektsperre ist die Verwendung versionierter Buckets erforderlich. 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 Objekt, das in einem Bucket mit aktivierter S3-Objektsperre gespeichert wird, durchläuft drei Phasen:

1. Objektaufnahme

- Beim Hinzufügen einer Objektversion zu einem Bucket mit aktivierter S3-Objektsperre kann die S3-Client-Applikation optional Aufbewahrungseinstellungen für das Objekt festlegen (bis dato, gesetzliche Aufbewahrungspflichten oder beides). StorageGRID generiert dann Metadaten für dieses Objekt, einschließlich einer eindeutigen Objekt-ID (UUID) sowie Datum und Uhrzeit der Aufnahme.
- Nach der Aufnahme einer Objektversion mit Aufbewahrungseinstellungen können seine Daten und benutzerdefinierten S3-Metadaten nicht mehr geändert werden.
- StorageGRID speichert die Objektmetadaten unabhängig von den Objektdaten. Es behält drei Kopien aller Objektmetadaten an jedem Standort.

2. Aufbewahrung von Objekten

- StorageGRID speichert mehrere Kopien des Objekts. Die genaue Anzahl und Art der Kopien und der Speicherorte werden durch die konformen Regeln in der aktiven ILM-Richtlinie festgelegt.

3. Löschen von Objekten

- Ein Objekt kann gelöscht werden, wenn sein Aufbewahrungsdatum erreicht ist.
- Ein Objekt, das sich unter einer gesetzlichen Aufbewahrungspflichten befindet, kann nicht gelöscht werden.

Verwandte Informationen

["Verwenden Sie ein Mandantenkonto"](#)

["S3 verwenden"](#)

["Vergleich der S3-Objektsperre mit älterer Compliance"](#)

["Beispiel 7: Konforme ILM-Richtlinie für S3 Object Lock"](#)

["Prüfung von Audit-Protokollen"](#)

Aktivieren der 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.

Was Sie benötigen

- Sie müssen über die Berechtigung Root Access verfügen.
- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.
- Sie müssen den S3 Object Lock Workflow überprüft haben, und Sie müssen die Überlegungen verstehen.
- Die Standardregel in der aktiven ILM-Richtlinie muss konform sein.

["Erstellen einer Standard-ILM-Regel"](#)

["ILM-Richtlinie erstellen"](#)

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.



Wenn Sie die globale Compliance-Einstellung mit einer früheren Version von StorageGRID aktiviert haben, wird die neue S3-Objektsperre automatisch aktiviert, wenn Sie auf StorageGRID Version 11.5 aktualisieren. Sie können StorageGRID weiterhin zum Management der Einstellungen vorhandener konformer Buckets verwenden. Es ist jedoch nicht mehr möglich, neue konforme Buckets zu erstellen.

["NetApp Knowledge Base: Management älterer, konformer Buckets für StorageGRID 11.5"](#)

Schritte

1. Wählen Sie **Konfiguration > Systemeinstellungen > S3 Objektsperre**.

Die Seite Einstellungen für die S3-Objektsperre wird angezeigt.

S3 Object Lock Settings

Enable S3 Object Lock for your entire StorageGRID system if S3 tenant accounts need to satisfy regulatory compliance requirements when saving object data. After this setting is enabled, it cannot be disabled.

S3 Object Lock

Before enabling S3 Object Lock, you must ensure that the default rule in the active ILM policy is compliant. A compliant rule satisfies the requirements of buckets with S3 Object Lock enabled.

- It must create at least two replicated object copies or one erasure-coded copy.
- These copies must exist on Storage Nodes for the entire duration of each line in the placement instructions.
- Object copies cannot be saved on Archive Nodes.
- At least one line of the placement instructions must start at day 0, using Ingest Time as the reference time.
- At least one line of the placement instructions must be "forever".

☐ Enable S3 Object Lock

Apply

Wenn Sie die globale Compliance-Einstellung mit einer früheren Version von StorageGRID aktiviert haben, enthält die Seite den folgenden Hinweis:

The S3 Object Lock setting replaces the legacy Compliance setting. When this setting is enabled, tenant users can create buckets with S3 Object Lock enabled. Tenants who previously created buckets for the legacy Compliance feature can manage their existing buckets, but can no longer create new buckets with legacy Compliance enabled. See [Managing objects with information lifecycle management](#) for information.

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

3. Wählen Sie **Anwenden**.

Ein Bestätigungsdialogfeld wird angezeigt und Sie werden daran erinnert, dass Sie die S3-Objektsperre nach ihrer Aktivierung nicht deaktivieren können.

Info

Enable S3 Object Lock

Are you sure you want to enable S3 Object Lock for the grid? You cannot disable S3 Object Lock after it has been enabled.

Cancel

OK

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 die S3-Objektsperre nun für das gesamte Grid aktiviert und kann nicht deaktiviert werden.
- Wenn die Standardregel nicht konform ist, erscheint ein Fehler, der angibt, dass Sie eine neue ILM-Richtlinie erstellen und aktivieren müssen, die eine konforme Regel als Standardregel enthält. Wählen Sie **OK**, und erstellen Sie eine neue vorgeschlagene Richtlinie, simulieren Sie sie und aktivieren Sie sie.

! Error

422: Unprocessable Entity

Validation failed. Please check the values you entered for errors.

The default rule in the active ILM policy is not compliant.

OK

Nachdem Sie fertig sind

Nachdem Sie die globale S3 Object Lock-Einstellung aktiviert haben, sollten Sie möglicherweise eine neue ILM-Richtlinie erstellen. Nach Aktivierung der Einstellung kann die ILM-Richtlinie optional sowohl eine konforme Standardregel als auch eine nicht konforme Standardregel enthalten. Beispielsweise möchten Sie eine nicht-konforme Regel verwenden, die keine Filter für Objekte in Buckets enthält, für die die S3-Objektsperre nicht aktiviert ist.

Verwandte Informationen

["Erstellen einer ILM-Richtlinie, nachdem S3 Object Lock aktiviert ist"](#)

["Erstellen einer ILM-Regel"](#)

["ILM-Richtlinie erstellen"](#)

["Vergleich der S3-Objektsperre mit älterer Compliance"](#)

Beseitigung von Konsistenzfehlern bei der Aktualisierung 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, da ein Datacenter-Standort oder mehrere Speicherknoten nicht verfügbar sind, wird eine Fehlermeldung angezeigt. Im Detail:

- Mandantenmanager Benutzer sehen die folgende Fehlermeldung:
- Mandantenmanagement-API-Benutzer und S3-API-Benutzer erhalten einen Antwortcode von 503 `Service Unavailable` Mit ähnlichem Nachrichtentext.

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 verwenden"](#)

["Verwalten Sie erholen"](#)

Beispiele für ILM-Regeln und -Richtlinien

Die Beispiele in diesem Abschnitt dienen als Ausgangspunkt für Ihre eigenen ILM-Regeln und -Richtlinien.

- ["Beispiel 1: ILM-Regeln und -Richtlinie für Objekt-Storage"](#)
- ["Beispiel 2: ILM-Regeln und Richtlinie für EC-Objektgrößen-Filterung"](#)
- ["Beispiel 3: ILM-Regeln und -Richtlinie für besseren Schutz von Image-Dateien"](#)
- ["Beispiel 4: ILM-Regeln und -Richtlinie für versionierte Objekte mit S3"](#)
- ["Beispiel 5: ILM-Regeln und Richtlinie für striktes Ingest-Verhalten"](#)
- ["Beispiel 6: Ändern einer ILM-Richtlinie"](#)
- ["Beispiel 7: Konforme ILM-Richtlinie für S3 Object Lock"](#)

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. Vor der Aktivierung einer neuen Richtlinie sollte die vorgeschlagene Richtlinie simuliert werden, um zu bestätigen, dass sie wie vorgesehen funktioniert, um Inhalte vor Verlust zu schützen.

ILM-Regel 1 beispielsweise 1: Objektdaten in zwei Datacenter kopieren

Diese Beispiel-ILM-Regel kopiert Objektdaten in Storage-Pools in zwei Datacentern.

Regeldefinition	Beispielwert
Storage-Pools	Zwei Speicherpools, jeweils in verschiedenen Datacentern, genannt Storage Pool DC1 und Storage Pool DC2.

Regeldefinition	Beispielwert
Regelname	Zwei Kopien Zwei Datacenter
Referenzzeit	Aufnahmezeit
Platzierung Von Inhalten	Am Tag 0, behalten Sie zwei replizierte Kopien für immer - eins im Storage Pool DC1 und eine im Storage Pool DC2.

Edit ILM Rule Step 2 of 3: Define Placements

Configure placement instructions to specify how you want objects matched by this rule to be stored.

Two Copies Two Data Centers

Reference Time
Ingest Time

Placements
Sort by start day

From day 0 store forever
Add Remove

Type replicated Location Storage Pool DC1 Storage Pool DC2 Add Pool Copies 2

Specifying multiple storage pools might cause data to be stored at the same site if the pools overlap. See [Managing objects with information lifecycle management](#) for more information.

Retention Diagram
Refresh

Trigger
Day 0

Storage Pool DC1
Storage Pool DC2

Duration
Forever

Cancel Back Next

ILM-Regel 2 zum Beispiel 1: Erasure Coding-Profil mit Bucket-Übereinstimmung

In diesem Beispiel wird eine ILM-Regel verwendet ein Erasure Coding-Profil und einen S3-Bucket, um zu bestimmen, wo und wie lange das Objekt gespeichert wird.

Regeldefinition	Beispielwert
Verfahren Zur Einhaltung Von Datenkonsistenz	<ul style="list-style-type: none"> Ein Storage-Pool für drei Datacenter (alle 3 Standorte) Verwenden Sie das Erasure Coding-Schema für 6+3
Regelname	EC für S3-Bucket-Finanzdatensätze
Referenzzeit	Aufnahmezeit

Regeldefinition	Beispielwert
Platzierung Von Inhalten	Erstellen Sie für Objekte im S3-Bucket mit Namen „Finance-Records“ eine Kopie mit Erasure-Coding-Verfahren im Pool, der durch das Erasure Coding-Profil festgelegt wird. Bewahren Sie diese Kopie für immer auf.

Create ILM Rule
Step 2 of 3: Define Placements

Configure placement instructions to specify how you want objects matched by this rule to be stored.

EC for S3 bucket finance-records

Reference Time
Ingest Time

Placements
Sort by start day

From day
0
store
forever
Add
Remove

Type
erasure coded
Location
All 3 sites (6 plus 3)
Copies
1
+
x

Retention Diagram
Refresh

Trigger
Day 0
Duration
All 3 sites (6 plus 3)
Forever

Cancel
Back
Next

ILM-Richtlinie z. B. 1

Mit dem StorageGRID System entwickeln Sie ausgereifte und komplexe ILM-Richtlinien. In der Praxis sind jedoch die meisten ILM-Richtlinien einfach.

Eine typische ILM-Richtlinie für eine Topologie mit mehreren Standorten kann ILM-Regeln wie die folgenden umfassen:

- Bei der Aufnahme sollten Sie Verfahren zur Einhaltung von Datenkonsistenz (Erasure Coding) in 6+3 verwenden, um alle Objekte zu speichern, die dem S3-Bucket mit dem Namen gehören `finance-records` Über drei Datacenter verteilt.
- Wenn ein Objekt nicht mit der ersten ILM-Regel übereinstimmt, verwenden Sie die Standard-ILM-Regel der Richtlinie, zwei Kopien von zwei Rechenzentren, um eine Kopie dieses Objekts in zwei Rechenzentren zu speichern, DC1 und DC2.

Configure ILM Policy

Create a proposed policy by selecting and arranging rules. Then, save the policy and edit it later as required. Click Simulate to verify a saved policy using test objects. When you are ready, click Activate to make this policy the active ILM policy for the grid.

Name Object Storage Policy

Reason for change new proposed policy

Rules

1. Select the rules you want to add to the policy.
2. Determine the order in which the rules will be evaluated by dragging and dropping the rows. The default rule will be automatically placed at the end of the policy and cannot be moved.

+ Select Rules

	Default	Rule Name	Tenant Account	Actions
		EC for S3 bucket finance-records	Ignore	✕
	✓	Two Copies Two Data Centers	Ignore	✕

Cancel

Save

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. Vor der Aktivierung einer neuen Richtlinie sollte die vorgeschlagene Richtlinie simuliert werden, um zu bestätigen, dass sie wie vorgesehen funktioniert, um Inhalte vor Verlust zu schützen.

ILM-Regel 1 beispielsweise 2: Verwenden Sie EC für alle Objekte, die größer als 200 KB sind

In diesem Beispiel werden alle Objekte, die größer als 200 KB sind (0.20 MB), mit einer ILM-Regel gelöscht.

Regeldefinition	Beispielwert
Regelname	Nur EC-Objekte > 200 KB
Referenzzeit	Aufnahmezeit
Erweiterte Filterung für Objektgröße	Objektgröße (MB) größer als 0.20
Platzierung Von Inhalten	Erstellen Sie eine Kopie mit 2+1-Verfahren zur Fehlerkorrektur mit drei Standorten

Advanced Filtering

Use advanced filtering if you want a rule to apply only to specific objects. You can filter objects based on their system metadata, user metadata, or object tags (S3 only). When objects are evaluated, the rule is applied if the object's metadata matches the criteria in the advanced filter.

EC only objects > 200 KB

Matches all of the following metadata:

Object Size (MB) greater than 0.2

In den Anweisungen zur Platzierung wird angegeben, dass eine Kopie mit 2+1-Erasure-Coding-Verfahren unter Verwendung aller drei Standorte erstellt wird.

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 zweite Regel in der Richtlinie. Da ILM-Regel 1 beispielsweise 2 alle Objekte gefiltert, die größer als 200 KB sind, gilt ILM-Regel 2 beispielsweise nur für Objekte mit einer Größe von 200 KB.

Regeldefinition	Beispielwert
Regelname	Zwei Replizierte Kopien
Referenzzeit	Aufnahmezeit
Erweiterte Filterung für Objektgröße	Keine
Platzierung Von Inhalten	Erstellen Sie zwei replizierte Kopien, und speichern Sie sie in zwei Rechenzentren, DC1 und DC2

Configure placement instructions to specify how you want objects matched by this rule to be stored.

Two replicated copies

Reference Time
Ingest Time

Placements
Sort by start day

From day 0 store forever
Add Remove

Type replicated Location DC1 x DC2 x Add Pool Copies 2 + x

Specifying multiple storage pools might cause data to be stored at the same site if the pools overlap. See [Managing objects with information lifecycle management](#) for more information.

Retention Diagram Refresh

Trigger
Day 0

DC1
DC2

Duration
Forever

Cancel Back Next

ILM-Richtlinie beispielsweise 2: Verwenden Sie EC für Objekte, die größer als 200 KB sind

In dieser Beispielrichtlinie werden Objekte mit einer Größe von mehr als 200 KB Erasure-Coding ausgeführt. Von allen anderen Objekten werden zwei replizierte Kopien erstellt.

Diese ILM-Richtlinie für das Beispiel umfasst die folgenden ILM-Regeln:

- Löschcode für alle Objekte, die größer als 200 KB sind.
- Wenn ein Objekt nicht mit der ersten ILM-Regel übereinstimmt, erstellen Sie zwei replizierte Kopien dieses Objekts mithilfe der Standard-ILM-Regel. Da Objekte mit einer Größe von mehr als 200 KB nach Regel 1 herausgefiltert wurden, gilt Regel 2 nur für Objekte, die 200 KB oder kleiner sind.

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

Mithilfe der folgenden Beispielregeln und -Richtlinie können Sie sicherstellen, dass Bilder mit einer Größe von mehr als 200 KB gelöscht werden und drei Kopien von kleineren Images erstellt werden.



Die folgenden ILM-Regeln und -Richtlinien sind nur Beispiele. Es gibt viele Möglichkeiten zur Konfiguration von ILM-Regeln. Vor der Aktivierung einer neuen Richtlinie sollte die vorgeschlagene Richtlinie simuliert werden, um zu bestätigen, dass sie wie vorgesehen funktioniert, um Inhalte vor Verlust zu schützen.

ILM-Regel 1 beispielsweise 3: Verwenden Sie EC für Bilddateien, die größer als 200 KB sind

Diese Beispiel ILM-Regel verwendet erweiterte Filterung zur Löschung von Code aller Bilddateien, die größer

als 200 KB sind.

Regeldefinition	Beispielwert
Regelname	EC-Bilddateien > 200 KB
Referenzzeit	Aufnahmezeit
Erweiterte Filterung für Benutzermetadaten	Der Metadaten­typ des Benutzers entspricht den Bilddateien
Erweiterte Filterung für Objektgröße	Objektgröße (MB) größer als 0.2
Platzierung Von Inhalten	Erstellen Sie eine Kopie mit 2+1-Verfahren zur Fehlerkorrektur mit drei Standorten

Advanced Filtering

Use advanced filtering if you want a rule to apply only to specific objects. You can filter objects based on their system metadata, user metadata, or object tags (S3 only). When objects are evaluated, the rule is applied if the object's metadata matches the criteria in the advanced filter.

EC image files > 200 KB

Matches all of the following metadata:

User Metadata▼typeequals▼image+×

Object Size (MB)▼greater than▼0.2+×

+×

Cancel

Remove Filters

Save

Da diese Regel als erste Regel in der Richtlinie konfiguriert ist, gilt die Anweisung zur Platzierung von Erasure Coding nur für Bilder, die größer als 200 KB sind.

ILM-Regel 2 beispielsweise 3: Replizieren Sie 3 Kopien für alle übrigen Image-Dateien

Diese Beispiel-ILM-Regel verwendet erweiterte Filterung, um anzugeben, dass Bilddateien repliziert werden.

Regeldefinition	Beispielwert
Regelname	3 Kopien für Bilddateien

Regeldefinition	Beispielwert
Referenzzeit	Aufnahmezeit
Erweiterte Filterung für Benutzermetadaten	Der Metadatatyp des Benutzers entspricht den Bilddateien
Platzierung Von Inhalten	Erstellen Sie 3 replizierte Kopien in allen Storage-Nodes

Advanced Filtering

Use advanced filtering if you want a rule to apply only to specific objects. You can filter objects based on their system metadata, user metadata, or object tags (S3 only). When objects are evaluated, the rule is applied if the object's metadata matches the criteria in the advanced filter.

3 copies for image files

Matches all of the following metadata:

User Metadata
▼
type
equals
▼
image
+
x

+
x

Cancel
Remove Filters
Save

Da die erste Regel in der Richtlinie bereits Bilddateien mit einer Größe von mehr als 200 KB übereinstimmt, gelten diese Platzierungsanweisungen nur für Bilddateien mit einer Größe von 200 KB.

3 copies for image files

Reference Time
Ingest Time

Placements
Sort by start day

From day
0
store
forever
Add
Remove

Type
replicated
Location
DC1
DC2
DC3
Add Pool
Copies
3
+
x

Specifying multiple storage pools might cause data to be stored at the same site if the pools overlap. See [Managing objects with information lifecycle management](#) for more information.

Retention Diagram
Refresh

Trigger
Day 0
Duration
Forever

Cancel
Back
Next

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

In diesem Beispiel erstellt die ILM-Richtlinie drei ILM-Regeln, die eine Richtlinie erstellen, die beim Löschen von Image-Dateien, die größer als 200 KB (0.2 MB) sind, replizierte Kopien für Image-Dateien erstellt, die mindestens 200 KB groß sind, und zwei replizierte Kopien für alle Dateien erstellt, die nicht mit dem Image verknüpft sind.

In diesem Beispiel enthält die ILM-Richtlinie folgende Regeln:

- Löschen Code alle Bilddateien größer als 200 KB.
- Erstellen Sie drei Kopien aller verbleibenden Bilddateien (d. h. Bilder, die 200 KB oder kleiner sind).
- Wenden Sie die Standardregel auf alle übrigen Objekte an (d. h. alle nicht-Image-Dateien).

Viewing Active Policy - Better protection for image files

Review the rules in this policy. If this is a proposed policy, click Simulate to verify the policy and then click Activate to make the policy active.

Reason for change: ILM policy for example 3

Rules are evaluated in order, starting from the top.

Rule Name	Default	Tenant Account
EC only objects > 200 KB		Ignore
3 copies for image files		Ignore
Make 2 Copies	✓	Ignore

Simulate
Activate

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 **nicht aktuelle Zeit** als Referenzzeit verwenden.

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. Vor der Aktivierung einer neuen Richtlinie sollte die vorgeschlagene Richtlinie simuliert werden, um zu bestätigen, dass sie wie vorgesehen funktioniert, um Inhalte vor Verlust zu schützen.



Wenn Sie ILM-Richtlinien erstellen, um nicht aktuelle Objektversionen zu managen, beachten Sie, dass Sie zum Simulieren der Richtlinie die UUID oder CBID der Objektversion kennen müssen. Um die UUID und die CBID eines Objekts zu finden, verwenden Sie Object Metadata Lookup, während das Objekt noch aktuell ist.

Verwandte Informationen

["Löschen von S3-versionierten Objekten"](#)

["Überprüfen einer ILM-Richtlinie mit Objekt-Metadaten-Lookup"](#)

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

In diesem Beispiel wird eine ILM-Regel für 10 Jahre eine Kopie jedes Objekts in drei Datacentern gespeichert.

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

Regeldefinition	Beispielwert
Storage-Pools	Drei Storage-Pools mit den Namen DC1, DC2 und DC3.
Regelname	Drei Kopien Zehn Jahre
Referenzzeit	Aufnahmezeit
Platzierung Von Inhalten	Am Tag 0 behalten Sie drei replizierte Kopien für 10 Jahre (3,652 Tage), eins in DC1, eins in DC2 und eins in DC3. Löschen Sie Ende 10 Jahre alle Kopien des Objekts.

Configure placement instructions to specify how you want objects matched by this rule to be stored.

Three Copies Ten Years
 Save three copies for ten years

Reference Time Ingest Time

Placements Sort by start day

From day 0 store for 3652 days Add Remove

Type replicated Location DC1 DC2 DC3 Add Pool Copies 3 + -

Specifying multiple storage pools might cause data to be stored at the same site if the pools overlap. See [Managing objects with information lifecycle management](#) for more information.

Retention Diagram Refresh

The diagram shows three horizontal bars representing storage durations for DC1, DC2, and DC3. Each bar starts at 'Day 0' and ends at 'Day 3652'. Below the bars, the duration is labeled '3652 days' and 'Forever'.

Cancel Back Next

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. Diese Regel verwendet die Option **nicht aktuelle Zeit** für Referenzzeit.

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 mit den Namen DC1 und DC2 an verschiedenen Rechenzentren.
Regelname	Nicht Aktuelle Versionen: Zwei Kopien Zwei Jahre
Referenzzeit	Nicht Aktuelle Zeit
Platzierung Von Inhalten	Am Tag 0 im Verhältnis zur nicht aktuellen Zeit (d.h. ab dem Tag, an dem die Objektversion zur nicht aktuellen Version wird) zwei replizierte Kopien der nicht aktuellen Objektversionen für 2 Jahre (730 Tage), eines in DC1 und eines in DC2. Löschen Sie Ende 2 Jahre die nicht aktuellen Versionen.

Noncurrent Versions: Two Copies Two Years

Save two copies of noncurrent versions for two years

Reference Time

Noncurrent Time

Placements

Sort by start day

From day

0

store

for

730

days

Add

Remove

Type

replicated

Location

DC1

DC2

Add Pool

Copies

2

+

×

Specifying multiple storage pools might cause data to be stored at the same site if the pools overlap. See [Managing objects with information lifecycle management](#) for more information.

Retention Diagram

Refresh

Trigger

Day 0

Year 2

DC1

DC2

Duration

2 years

Forever

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 für die aktuelle Objektversion gelten.

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 nicht aktuellen Zeitregeln müssen in der Richtlinie vor den Regeln erscheinen, die für die aktuelle Objektversion gelten. Andernfalls werden die nicht aktuellen Objektversionen niemals mit der nicht aktuellen Zeitregel abgeglichen.

- Bei Aufnahme der Daten werden drei replizierte Kopien erstellt und eine Kopie an jedem der drei Datacenter gespeichert. Bewahren Sie 10 Jahre lang Kopien der aktuellen Objektversion auf.

Configure ILM Policy

Create a proposed policy by selecting and arranging rules. Then, save the policy and edit it later as required. Click Simulate to verify a saved policy using test objects. When you are ready, click Activate to make this policy the active ILM policy for the grid.



Name **ILM Policy for S3 Versioned Objects**

Reason for change store 3 copies of current version for 10 years and 2 copies of noncurrent versions for 2 years

Rules

1. Select the rules you want to add to the policy.
2. Determine the order in which the rules will be evaluated by dragging and dropping the rows. The default rule will be automatically placed at the end of the policy and cannot be moved.

+ Select Rules

Default	Rule Name	Tenant Account	Actions
	Noncurrent Versions: Two Copies Two Years 	Ignore	
✓	Three Copies Ten Years 	Ignore	

The default ILM rule in this policy does not retain objects forever. Confirm this is the behavior you expect. Otherwise, any objects that are not matched by another rule will be deleted after 3652 days.

Cancel

Save

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).



Um nicht aktuelle Objektversionen zu simulieren, müssen Sie die UUID oder CBID dieser Version verwenden. Während das Objekt noch aktuell ist, können Sie Object Metadata Lookup verwenden, um seine UUID und CBID zu finden.

- Die aktuelle Objektversion würde mit der zweiten Regel abgeglichen. Wenn die aktuelle Objektversion 10 Jahre lang gespeichert wurde, fügt der ILM-Prozess als aktuelle Version des Objekts eine Löschmarkierung hinzu und macht die vorherige Objektversion „non current“. Bei der nächsten ILM-Bewertung wird diese nicht aktuelle Version der ersten Regel zugeordnet. Dadurch wird die Kopie bei DC3 gelöscht und die beiden Kopien bei DC1 und DC2 für weitere 2 Jahre gespeichert.

Verwandte Informationen

["Überprüfen einer ILM-Richtlinie mit Objekt-Metadaten-Lookup"](#)

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. Vor der Aktivierung einer neuen Richtlinie sollte die vorgeschlagene Richtlinie simuliert werden, um zu bestätigen, dass sie wie vorgesehen funktioniert, um Inhalte vor Verlust zu schützen.

Verwandte Informationen

["Aufnahme von Objekten"](#)

["Schritt 3 von 3: Definieren des Aufnahmeverhaltens"](#)

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
Erweiterte Filterung	Standortbeschränkung entspricht eu-West-3
Storage-Pools	DC1 (Paris)
Regelname	Strenge Einspeisung für ein Pariser Rechenzentrum
Referenzzeit	Aufnahmezeit
Platzierung Von Inhalten	Am Tag 0, zwei replizierte Kopien für immer in DC1 (Paris)
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.

Strict ingest to guarantee Paris data center

Description: Strict ingest to guarantee Paris data center
Ingest Behavior: Strict
Tenant Account: Paris tenant (25580610012441844135)
Reference Time: Ingest Time
Filtering Criteria:

Matches all of the following metadata:

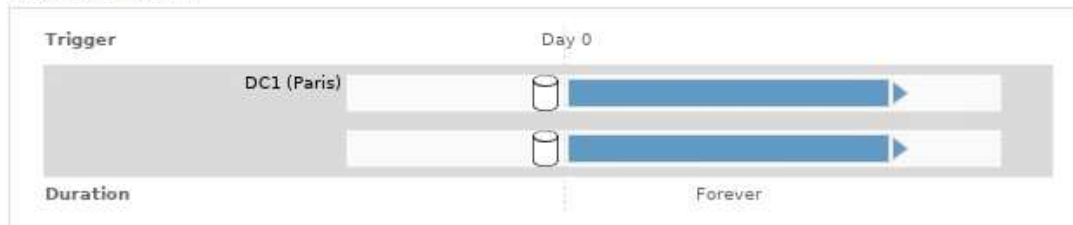
System Metadata

Location Constraint (S3 only)

equals

eu-west-3

Retention Diagram:



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 an jedem verfügbaren Ort Zwischenkopien abgelegt.

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

Regeldefinition	Beispielwert
Mandantenkonto	Ignorieren
Erweiterte Filterung	<i>Nicht angegeben</i>
Storage-Pools	DC1 (Paris) und DC2 (USA)
Regelname	2 Kopien 2 Datacenter
Referenzzeit	Aufnahmezeit
Platzierung Von Inhalten	Am Tag 0 werden zwei replizierte Kopien für immer in zwei Datacentern aufbewahrt
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.

2 Copies 2 Data Centers

Description: 2 Copies 2 Data Centers

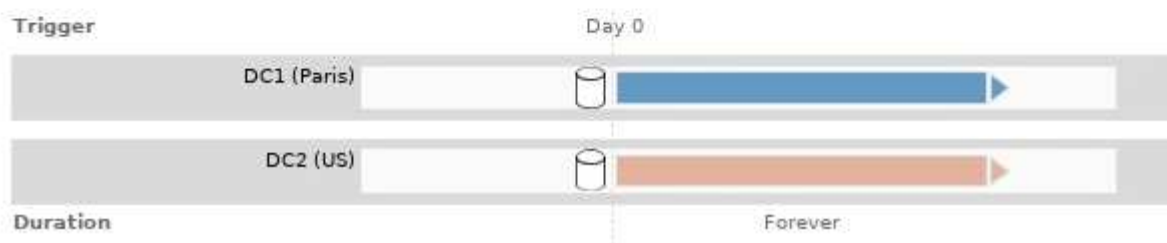
Ingest Behavior: Balanced

Reference Time: Ingest Time

Filtering Criteria:

Matches all objects.

Retention Diagram:



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 Ort, wenn die Platzierungsanweisung nicht erfüllt werden kann.

Configure ILM Policy

Create a proposed policy by selecting and arranging rules. Then, save the policy and edit it later as required. Click Simulate to verify a saved policy using test objects. When you are ready, click Activate to make this policy the active ILM policy for the grid.

Name

Example policy for Strict ingest


Reason for change

Do not store certain objects for Paris tenant in US

Rules

1. Select the rules you want to add to the policy.
2. Determine the order in which the rules will be evaluated by dragging and dropping the rows. The default rule will be automatically placed at the end of the policy and cannot be moved.

+ Select Rules

Default	Rule Name	Tenant Account	Actions
	Strict ingest to guarantee Paris data center 	Paris tenant (25580610012441844135)	✕
✓	2 Copies 2 Data Centers 	Ignore	✕

Cancel

Save

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 Speicherknoten im Pariser Rechenzentrum nicht verfügbar sind, schlägt die Aufnahme fehl.
- Alle anderen Objekte werden mit der zweiten Regel abgeglichen, einschließlich Objekte, die zum Pariser Mieter gehören und die die S3-Bucket-Region nicht auf eu-West-3 gesetzt hat. 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

Möglicherweise müssen Sie eine neue ILM-Richtlinie erstellen und aktivieren, wenn sich Ihre Datensicherungsanforderungen ändern oder Sie neue Standorte hinzufügen.

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 in einer Erweiterung hinzugefügt. Die aktive ILM-Richtlinie muss überarbeitet werden, um Daten am neuen Standort zu speichern.



Die folgenden ILM-Regeln und -Richtlinien sind nur Beispiele. Es gibt viele Möglichkeiten zur Konfiguration von ILM-Regeln. Vor der Aktivierung einer neuen Richtlinie sollte die vorgeschlagene Richtlinie simuliert werden, um zu bestätigen, dass sie wie vorgesehen funktioniert, um Inhalte vor Verlust zu schützen.

Wie wirkt sich die Änderung einer ILM-Richtlinie auf die Performance aus

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.

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

- Anwenden eines anderen Profils zur Einhaltung von Datenkonsistenz (Erasure Coding) auf vorhandene Objekte mit Verfahren zur Fehlerkorrektur.



StorageGRID hält jedes Erasure Coding-Profil für einzigartig und verwendet bei Verwendung eines neuen Profils keine Erasure Coding-Fragmente.

- 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.

Verwandte Informationen

["ILM-Richtlinie erstellen"](#)

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.

ILM Policies

Review the proposed, active, and historical policies. You can create, edit, or delete a proposed policy; clone the active policy; or view the details for any policy.

+ Create Proposed Policy
Clone
Edit
Remove

Policy Name	Policy State	Start Date	End Date
<input checked="" type="radio"/> Data Protection for Two Sites	Active	2020-06-10 16:42:09 MDT	
<input type="radio"/> Baseline 2 Copies Policy	Historical	2020-06-09 21:48:34 MDT	2020-06-10 16:42:09 MDT

Viewing Active Policy - Data Protection for Two Sites

Review the rules in this policy. If this is a proposed policy, click Simulate to verify the policy and then click Activate to make the policy active.

Reason for change: Data Protection for Two Sites

Rules are evaluated in order, starting from the top.

Rule Name	Default	Tenant Account
One-Site Erasure Coding for Tenant A		Tenant A (49752734300032812036)
Two-Site Replication for Other Tenants	✓	Ignore

Simulate
Activate

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.



Die erste Regel in diesem Beispiel verwendet einen erweiterten Filter, um sicherzustellen, dass das Erasure Coding nicht für kleine Objekte verwendet wird. Alle Objekte von Mandanten A, die kleiner als 200 KB sind, werden durch die zweite Regel geschützt, die Replikation verwendet.

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	Datacenter 1
Platzierung Von Inhalten	2+1 Erasure Coding in Datacenter 1 – von Tag 0 bis für immer

Regel 2: Replizierung zwischen zwei Standorten für andere Mandanten

Regeldefinition	Beispielwert
Regelname	Replizierung an zwei Standorten für andere Mandanten
Mandantenkonto	Ignorieren
Storage-Pools	Datacenter 1 und Datacenter 2

Regeldefinition	Beispielwert
Platzierung Von Inhalten	Zwei replizierte Kopien von Tag 0 bis für immer: Eine Kopie im Datacenter 1 und eine Kopie im Datacenter 2.

Vorgeschlagene ILM-Richtlinie z. B. 6: Datensicherung an drei Standorten

In diesem Beispiel wird die ILM-Richtlinie für ein StorageGRID System mit drei Standorten aktualisiert.

Nach Durchführung einer Erweiterung zum Hinzufügen des neuen Standorts erstellte der Grid-Administrator zwei neue Speicherpools: Einen Speicherpool für Data Center 3 und einen Speicherpool mit allen drei Standorten (nicht identisch mit dem Standardspeicherpool für alle Storage-Nodes). Anschließend erstellte der Administrator zwei neue ILM-Regeln und eine neue vorgeschlagene ILM-Richtlinie, die auf den Schutz von Daten an allen drei Standorten ausgelegt ist.

Viewing Proposed Policy - Data Protection for Three Sites

Before activating a new ILM policy:

- Review and carefully simulate the policy. Errors in an ILM policy can cause irreparable data loss.
- Review any changes to the placement of existing replicated and erasure-coded objects. Changing an existing object's location might result in temporary resource issues when the new placements are evaluated and implemented.

See [Managing objects with information lifecycle management](#) for more information.

This policy contains a rule that makes an erasure-coded copy. Confirm that at least one rule uses the Object Size advanced filter to prevent objects that are 200 KB or smaller from being erasure coded. See [Managing objects with information lifecycle management](#) for more information.

Review the rules in this policy. If this is a proposed policy, click Simulate to verify the policy and then click Activate to make the policy active.

Reason for change: Data Protection for Three Sites

Rules are evaluated in order, starting from the top.

Rule Name	Default	Tenant Account
Three-Site Erasure Coding for Tenant A		Tenant A (49752734300032812036)
Three-Site Replication for Other Tenants	✓	Ignore

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 Datacenter (einschließlich Datacenter 1, Datacenter 2 und Datacenter 3)
Platzierung Von Inhalten	2+1 Erasure Coding in allen 3 Datacentern von 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	Datacenter 1, Datacenter 2 und Datacenter 3
Platzierung Von Inhalten	Drei replizierte Kopien von Tag 0 bis für immer: Eine Kopie im Datacenter 1, eine Kopie im Datacenter 2 und eine Kopie im Datacenter 3.

Aktivierung der vorgeschlagenen ILM-Richtlinie beispielsweise 6

Wenn Sie eine neue vorgeschlagene ILM-Richtlinie aktivieren, können vorhandene Objekte an neue Orte verschoben oder neue Objektkopien für vorhandene Objekte erstellt werden, basierend auf den Anweisungen zur Platzierung in neuen oder aktualisierten Regeln.



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 werden Objekte, die von Mandant A gehören, durch Erasure Coding von 2+1 in Datacenter 1 geschützt. In der neuen vorgeschlagenen ILM-Richtlinie werden Objekte, die von Mandant A gehören, durch Erasure Coding (2+1) in Datacentern 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. Anschließend wird jedes der drei Fragmente in einem anderen Rechenzentrum gespeichert.
- Die vorhandenen Objekte, die von Mandant A gehören, werden bei der laufenden ILM-Überprüfung neu bewertet. Da die ILM-Speicheranweisungen ein neues Erasure Coding-Profil verwenden, werden vollständig neue Fragmente mit Erasure-Coding-Verfahren erstellt und auf die drei Datacenter verteilt.



Die vorhandenen 2+1-Fragmente im Datacenter 1 werden nicht wiederverwendet. StorageGRID hält jedes Erasure Coding-Profil für einzigartig und verwendet bei Verwendung eines neuen Profils keine Erasure Coding-Fragmente.

Was geschieht, wenn sich Replikationsanweisungen ändern

In der derzeit aktiven ILM-Richtlinie für dieses Beispiel werden Objekte, die andere Mandanten gehören, durch zwei replizierte Kopien in Storage-Pools in Datacenter 1 und 2 geschützt. In der neuen ILM-Richtlinie werden Objekte, die zu anderen Mandanten gehören, durch drei replizierte Kopien in Storage-Pools in Datacenter 1, 2 und 3 geschützt.

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

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

Auswirkungen der Aktivierung dieser Richtlinie auf die Performance

Wenn die vorgeschlagene ILM-Richtlinie in diesem Beispiel aktiviert ist, wird die Gesamtleistung dieses StorageGRID Systems vorübergehend beeinträchtigt. Höher als die normalen Grid-Ressourcen sind erforderlich, um neue, mit Erasure Coding codierte Fragmente für vorhandene Objekte von Mandanten A und neue replizierte Kopien im Datacenter 3 für vorhandene Objekte anderer Mandanten zu erstellen.

Aufgrund der Änderung der ILM-Richtlinie können Lese- und Schreib Anfragen 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 die Aufnahmezeit auf größer oder gleich der ungefähren Zeit fest, 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. Vor der Aktivierung einer neuen Richtlinie sollte die vorgeschlagene Richtlinie simuliert werden, um zu bestätigen, dass sie wie vorgesehen funktioniert, um Inhalte vor Verlust zu schützen.

Verwandte Informationen

["Verwalten von Objekten 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)

Buckets

Create buckets and manage bucket settings.

1 bucket Create bucket

Actions ▾

<input type="checkbox"/>	Name ▾	S3 Object Lock ? ▾	Region ▾	Object Count ? ▾	Space Used ? ▾	Date Created ▾
<input type="checkbox"/>	bank-records	✓	us-east-1	0	0 bytes	2021-01-06 16:53:19 MST

← Previous 1 Next →

Jedes Objekt und jede Objektversion, die dem Bucket für die Bankdatensätze hinzugefügt wird, verwenden die folgenden Werte für retain-until-date Und legal hold Einstellungen.

Einstellung für jedes Objekt	Beispielwert
retain-until-date	"2030-12-30T23:59:59Z" (30. Dezember 2030) Jede Objektversion hat ihre eigene retain-until-date Einstellung. Diese Einstellung kann erhöht, aber nicht verringert werden.

Einstellung für jedes Objekt	Beispielwert
legal hold	<p>"OFF" (Nicht wirksam)</p> <p>Eine gesetzliche Aufbewahrungsphase kann jederzeit während der Aufbewahrungsfrist auf jeder Objektversion platziert oder aufgehoben werden. Wenn ein Objekt unter einer gesetzlichen Aufbewahrungspflichten steht, kann das Objekt auch dann nicht gelöscht werden, wenn der <code>retain-until-date</code> Wurde erreicht.</p>

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

Diese Beispiel-ILM-Regel gilt nur für das S3-Mandantenkonto namens Bank of ABC. Sie entspricht jedem Objekt im `bank-records` Bucket und verwendet dann Erasure Coding, um das Objekt mithilfe eines 6+3 Erasure Coding-Profiles auf Storage Nodes an drei Datacenter-Standorten zu speichern. Diese Regel erfüllt die Anforderungen von Buckets bei aktivierter S3-Objektsperre: Eine Kopie, die gemäß Erasure-Coding-Verfahren in Storage-Nodes von Tag 0 bis für immer gespeichert wird, wobei die Aufnahmezeit als Referenzzeit verwendet wird.

Regeldefinition	Beispielwert
Regelname	Konforme Regel: EC-Objekte in Bankaufzeichnungseimer - Bank of ABC
Mandantenkonto	Bank von ABC
Bucket-Name	<code>bank-records</code>
Erweiterte Filterung	<p>Objektgröße (MB) größer als 0.20</p> <p>Hinweis: dieser Filter sorgt dafür, dass das Erasure Coding nicht für Objekte mit einer Größe von 200 KB verwendet wird.</p>

Create ILM Rule Step 1 of 3: Define Basics

Name

Description

Tenant Accounts (optional)

Bucket Name

[Advanced filtering...](#) (0 defined)

Cancel

Next

Regeldefinition	Beispielwert
Referenzzeit	Aufnahmezeit
Platzierungen	Ab Tag 0 dauerhaft speichern
Verfahren Zur Einhaltung Von Datenkonsistenz	<ul style="list-style-type: none"> • Erstellen einer mit Erasure Coding verschlüsselten Kopie auf Storage-Nodes an drei Datacenter-Standorten • Verwendet das Erasure Coding-Schema 6+3

Edit ILM Rule Step 2 of 3: Define Placements

Configure placement instructions to specify how you want objects matched by this rule to be stored.

Compliant Rule: EC objects in bank-record bucket - Bank of ABC

Reference Time

Ingest Time

Placements
Sort by start day

From day

0

store

forever

Add Remove

Type

erasure coded

Location

Three Data Centers (6 plus 3)

Copies

1

+ x

Retention Diagram
Refresh

Trigger

Three Data Centers (6 plus 3)

Duration

Day 0

Forever

Cancel Back Save

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: Nutzung Von 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.
Erweiterte Filterung	Nicht angegeben

Name	Non-Compliant Rule: Use Cloud Storage Pool	
Description	DC1 and 2 for 1 year then move to CSP	
Tenant Accounts (optional) 	Select tenant accounts or enter tenant IDs	
Bucket Name	matches all ▼	Value
Advanced filtering... (0 defined)		

Cancel

Next

Regeldefinition	Beispielwert
Referenzzeit	Aufnahmezeit
Platzierungen	<ul style="list-style-type: none">• 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 und erfüllt die Anforderungen von Buckets mit aktivierter S3-Objektsperre: Es werden zwei Objektkopien auf Storage-Nodes von Tag 0 bis für immer aufbewahrt, wobei die Aufnahme als Referenzzeit verwendet wird.

Regeldefinition	Beispielwert
Regelname	Standard-Compliance-Regel: Zwei Kopien Zwei Datacenter
Mandantenkonto	Nicht angegeben
Bucket-Name	Nicht angegeben
Erweiterte Filterung	Nicht angegeben

Name

Description

Tenant Accounts (optional)

Bucket Name

[Advanced filtering...](#) (0 defined)

Cancel Next

Regeldefinition	Beispielwert
Referenzzeit	Aufnahmezeit
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.

Compliant Rule: Two Copies Two Data Centers

Reference Time

Placements [?](#) [Sort by start day](#)

From day store [Add](#) [Remove](#)

Type Location Copies [+](#) [x](#)

Specifying multiple storage pools might cause data to be stored at the same site if the pools overlap. See [Managing objects with information lifecycle management](#) for more information.

Retention Diagram [?](#) [Refresh](#)

Trigger Day 0

Data Center 1

Data Center 2

Duration Forever

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 vorgeschlagene Richtlinie simulieren und aktivieren.

Hinzufügen von Regeln zu der Richtlinie

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 200 KB in

einem bestimmten Bucket zu schützen, wobei S3 Object Lock aktiviert ist. 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.

Configure ILM Policy

Create a proposed policy by selecting and arranging rules. Then, save the policy and edit it later as required. Click Simulate to verify a saved policy using test objects. When you are ready, click Activate to make this policy the active ILM policy for the grid.

Name

Reason for change

Rules

1. Select the rules you want to add to the policy.
2. Determine the order in which the rules will be evaluated by dragging and dropping the rows. The default rule (and any non-compliant rule without a filter) will be automatically placed at the end of the policy and cannot be moved.

[+ Select Rules](#)

Default	Rule Name	Compliant	Tenant Account	Actions
	Compliant Rule: EC for bank-records bucket - Bank of ABC	✓	Bank of ABC (90767802913525281639)	✗
	Non-Compliant Rule: Use Cloud Storage Pool		Ignore	✗
✓	Default Compliant Rule: Two Copies Two Data Centers	✓	Ignore	✗

Cancel

Save

Simulation der vorgeschlagenen Richtlinie

Nachdem Sie in Ihrer vorgeschlagenen Richtlinie Regeln hinzugefügt, eine standardkonforme Regel ausgewählt und die anderen Regeln festgelegt haben, sollten Sie die Richtlinie simulieren, indem Sie Objekte aus dem Bucket testen, wobei S3 Object Lock aktiviert ist und aus anderen Buckets. Wenn Sie beispielsweise die Beispielrychtlinie simulieren, erwarten Sie, dass Testobjekte wie folgt bewertet werden:

- Die erste Regel entspricht nur Testobjekten, die in den Bucket-Bankdatensätzen für den Mandanten der Bank of ABC größer als 200 KB 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 200 KB 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

Richtlinie wird aktiviert

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

Sie sie aktivieren.

Copyright-Informationen

Copyright © 2025 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtsinhabers in keiner Form und durch keine Mittel – weder grafische noch elektronische oder mechanische, einschließlich Fotokopieren, Aufnehmen oder Speichern in einem elektronischen Abrufsystem – auch nicht in Teilen, vervielfältigt werden.

Software, die von urheberrechtlich geschütztem NetApp Material abgeleitet wird, unterliegt der folgenden Lizenz und dem folgenden Haftungsausschluss:

DIE VORLIEGENDE SOFTWARE WIRD IN DER VORLIEGENDEN FORM VON NETAPP ZUR VERFÜGUNG GESTELLT, D. H. OHNE JEGLICHE EXPLIZITE ODER IMPLIZITE GEWÄHRLEISTUNG, EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE STILLSCHWEIGENDE GEWÄHRLEISTUNG DER MARKTGÄNGIGKEIT UND EIGNUNG FÜR EINEN BESTIMMTEN ZWECK, DIE HIERMIT AUSGESCHLOSSEN WERDEN. NETAPP ÜBERNIMMT KEINERLEI HAFTUNG FÜR DIREKTE, INDIREKTE, ZUFÄLLIGE, BESONDERE, BEISPIELHAFTE SCHÄDEN ODER FOLGESCHÄDEN (EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE BESCHAFFUNG VON ERSATZWAREN ODER -DIENSTLEISTUNGEN, NUTZUNGS-, DATEN- ODER GEWINNVERLUSTE ODER UNTERBRECHUNG DES GESCHÄFTSBETRIEBS), UNABHÄNGIG DAVON, WIE SIE VERURSACHT WURDEN UND AUF WELCHER HAFTUNGSTHEORIE SIE BERUHEN, OB AUS VERTRAGLICH FESTGELEGTER HAFTUNG, VERSCHULDENSUNABHÄNGIGER HAFTUNG ODER DELIKTSHAFTUNG (EINSCHLIESSLICH FAHRLÄSSIGKEIT ODER AUF ANDEREM WEGE), DIE IN IRGEND EINER WEISE AUS DER NUTZUNG DIESER SOFTWARE RESULTIEREN, SELBST WENN AUF DIE MÖGLICHKEIT DERARTIGER SCHÄDEN HINGEWIESEN WURDE.

NetApp behält sich das Recht vor, die hierin beschriebenen Produkte jederzeit und ohne Vorankündigung zu ändern. NetApp übernimmt keine Verantwortung oder Haftung, die sich aus der Verwendung der hier beschriebenen Produkte ergibt, es sei denn, NetApp hat dem ausdrücklich in schriftlicher Form zugestimmt. Die Verwendung oder der Erwerb dieses Produkts stellt keine Lizenzierung im Rahmen eines Patentrechts, Markenrechts oder eines anderen Rechts an geistigem Eigentum von NetApp dar.

Das in diesem Dokument beschriebene Produkt kann durch ein oder mehrere US-amerikanische Patente, ausländische Patente oder anhängige Patentanmeldungen geschützt sein.

ERLÄUTERUNG ZU „RESTRICTED RIGHTS“: Nutzung, Vervielfältigung oder Offenlegung durch die US-Regierung unterliegt den Einschränkungen gemäß Unterabschnitt (b)(3) der Klausel „Rights in Technical Data – Noncommercial Items“ in DFARS 252.227-7013 (Februar 2014) und FAR 52.227-19 (Dezember 2007).

Die hierin enthaltenen Daten beziehen sich auf ein kommerzielles Produkt und/oder einen kommerziellen Service (wie in FAR 2.101 definiert) und sind Eigentum von NetApp, Inc. Alle technischen Daten und die Computersoftware von NetApp, die unter diesem Vertrag bereitgestellt werden, sind gewerblicher Natur und wurden ausschließlich unter Verwendung privater Mittel entwickelt. Die US-Regierung besitzt eine nicht ausschließliche, nicht übertragbare, nicht unterlizenzierbare, weltweite, limitierte unwiderrufliche Lizenz zur Nutzung der Daten nur in Verbindung mit und zur Unterstützung des Vertrags der US-Regierung, unter dem die Daten bereitgestellt wurden. Sofern in den vorliegenden Bedingungen nicht anders angegeben, dürfen die Daten ohne vorherige schriftliche Genehmigung von NetApp, Inc. nicht verwendet, offengelegt, vervielfältigt, geändert, aufgeführt oder angezeigt werden. Die Lizenzrechte der US-Regierung für das US-Verteidigungsministerium sind auf die in DFARS-Klausel 252.227-7015(b) (Februar 2014) genannten Rechte beschränkt.

Markeninformationen

NETAPP, das NETAPP Logo und die unter <http://www.netapp.com/TM> aufgeführten Marken sind Marken von NetApp, Inc. Andere Firmen und Produktnamen können Marken der jeweiligen Eigentümer sein.