Objekte mit ILM verwalten

StorageGRID software

NetApp
October 21, 2025

Inhalt

Objekte mit ILM verwalten

Objekte mit ILM verwalten

Die Regeln für das Information Lifecycle Management (ILM) in einer ILM-Richtlinie weisen StorageGRID an, wie Kopien von Objektdaten erstellt und verteilt und wie diese Kopien im Laufe der Zeit verwaltet werden.

Zu dieser Anleitung

Das Entwerfen und Implementieren von ILM-Regeln und -Richtlinien erfordert eine sorgfältige Planung. Sie müssen Ihre Betriebsanforderungen, die Topologie Ihres StorageGRID -Systems, Ihren Bedarf an Objektschutz und die verfügbaren Speichertypen verstehen. Anschließend müssen Sie festlegen, wie die verschiedenen Objekttypen kopiert, verteilt und gespeichert werden sollen.

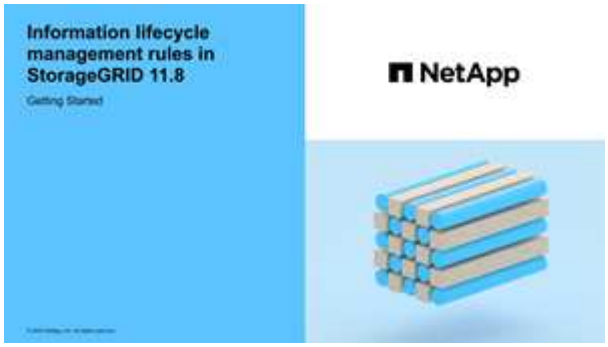
Verwenden Sie diese Anweisungen, um:

- Erfahren Sie mehr über StorageGRID ILM, einschließlich"wie ILM während der gesamten Lebensdauer eines Objekts funktioniert" .
- Erfahren Sie, wie Sie konfigurieren"Speicherpools" ,"Cloud-Speicherpools" , Und"ILM-Regeln" .
- Erfahren Sie, wie Sie"Erstellen, Simulieren und Aktivieren einer ILM-Richtlinie" das Objektdaten an einem oder mehreren Standorten schützt.
- Erfahren Sie, wie Sie"Objekte mit S3 Object Lock verwalten" , wodurch sichergestellt wird, dass Objekte in bestimmten S3-Buckets für einen bestimmten Zeitraum nicht gelöscht oder überschrieben werden.

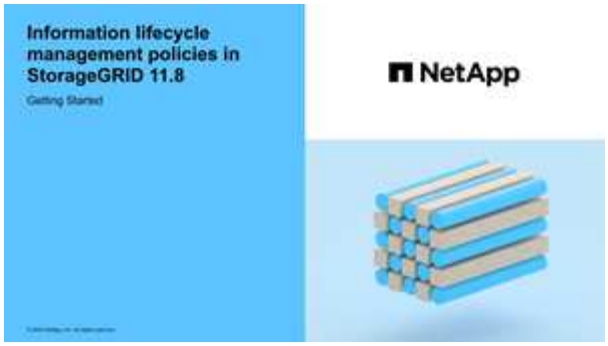
Mehr erfahren

Um mehr zu erfahren, sehen Sie sich diese Videos an:

- "Video: Übersicht über ILM-Regeln" .



- "Video: Übersicht über ILM-Richtlinien"



ILM und Objektlebenszyklus

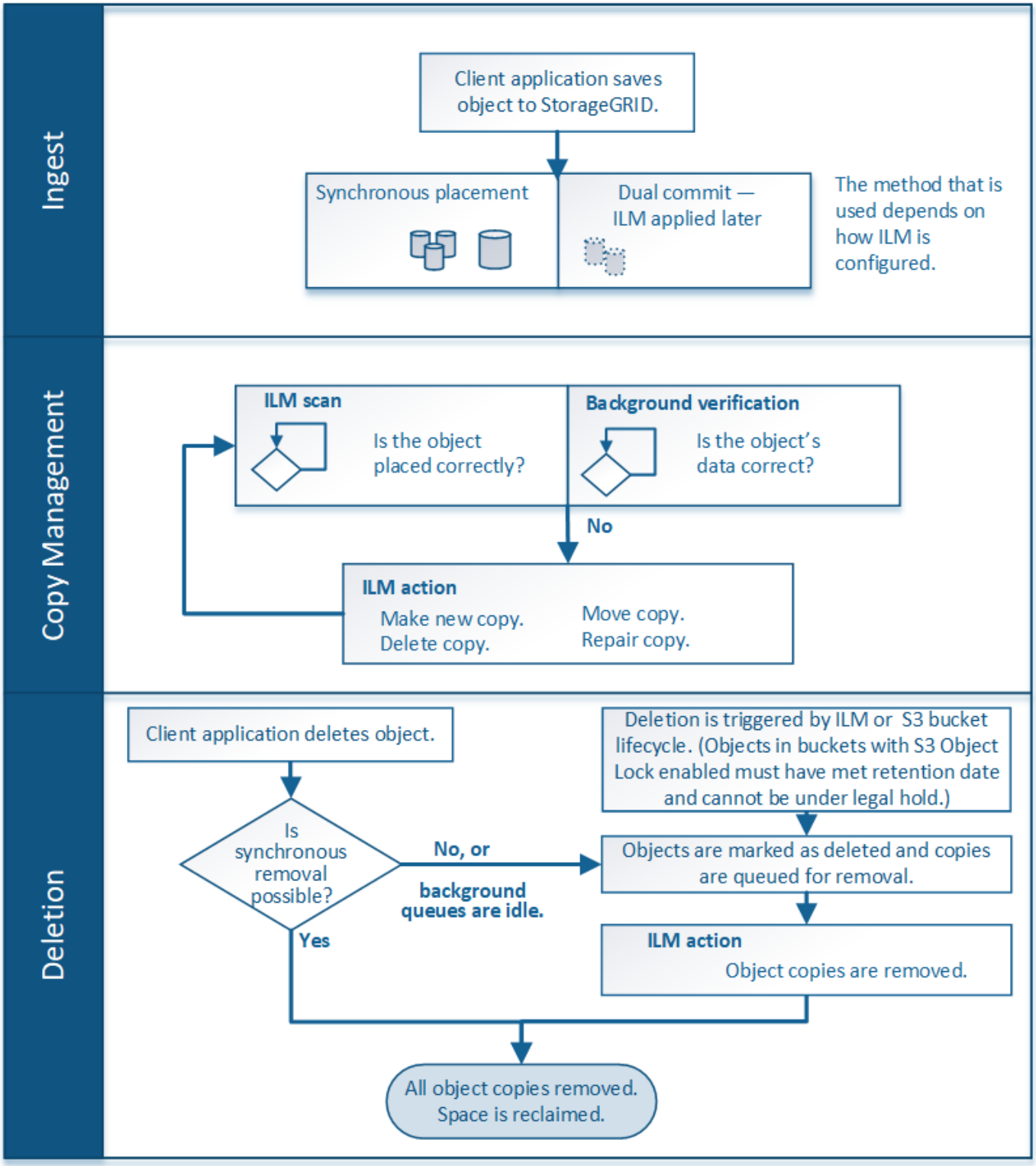
Funktionsweise von ILM während der gesamten Lebensdauer eines Objekts

Wenn Sie verstehen, wie StorageGRID ILM verwendet, um Objekte in jeder Phase ihres Lebenszyklus zu verwalten, können Sie eine effektivere Richtlinie entwerfen.

- **Aufnahme**: Die Aufnahme beginnt, wenn eine S3-Clientanwendung eine Verbindung herstellt, um ein Objekt im StorageGRID -System zu speichern, und ist abgeschlossen, wenn StorageGRID dem Client die Meldung „Aufnahme erfolgreich“ zurückgibt. Der Schutz der Objektdaten erfolgt während der Aufnahme entweder durch sofortiges Anwenden von ILM-Anweisungen (synchrone Platzierung) oder durch Erstellen von Zwischenkopien und späteres Anwenden von ILM (Dual Commit), je nachdem, wie die ILM-Anforderungen festgelegt wurden.
- **Kopienverwaltung**: Nachdem die Anzahl und Art der Objektkopien erstellt wurden, die in den Platzierungsanweisungen des ILM angegeben sind, verwaltet StorageGRID die Objektstandorte und schützt Objekte vor Verlust.
  - **ILM-Scan und -Auswertung**: StorageGRID scannt kontinuierlich die Liste der im Grid gespeicherten Objekte und prüft, ob die aktuellen Kopien die ILM-Anforderungen erfüllen. Wenn unterschiedliche Typen, Anzahlen oder Speicherorte von Objektkopien erforderlich sind, erstellt, löscht oder verschiebt StorageGRID Kopien nach Bedarf.
  - **Hintergrundüberprüfung**: StorageGRID führt kontinuierlich eine Hintergrundüberprüfung durch, um die Integrität der Objektdaten zu überprüfen. Wenn ein Problem gefunden wird, erstellt StorageGRID automatisch eine neue Objektkopie oder ein Ersatz-Löschcodiertes Objektfragment an einem Speicherort, der den aktuellen ILM-Anforderungen entspricht. Sehen "Überprüfen der Objektintegrität" .
- **Objektlöschung**: Die Verwaltung eines Objekts endet, wenn alle Kopien aus dem StorageGRID -System entfernt wurden. Objekte können aufgrund einer Löschanforderung eines Clients oder aufgrund einer Löschung durch ILM oder einer Löschung aufgrund des Ablaufs des Lebenszyklus eines S3-Buckets entfernt werden.

> ⓘ Objekte in einem Bucket mit aktivierter S3-Objektsperre können nicht gelöscht werden, wenn sie einer rechtlichen Sperre unterliegen oder wenn ein Aufbewahrungsdatum angegeben, aber noch nicht erreicht wurde.

Das Diagramm fasst zusammen, wie ILM während des gesamten Lebenszyklus eines Objekts funktioniert.



Wie Objekte aufgenommen werden

Aufnahmeoptionen

Wenn Sie eine ILM-Regel erstellen, geben Sie eine von drei Optionen zum Schutz von Objekten bei der Aufnahme an: Dual Commit, Streng oder Ausgewogen.

Je nach Ihrer Wahl erstellt StorageGRID Zwischenkopien und stellt die Objekte für eine spätere ILM-

Auswertung in die Warteschlange oder verwendet die synchrone Platzierung und erstellt sofort Kopien, um die ILM-Anforderungen zu erfüllen.

Flussdiagramm der Aufnahmeoptionen

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

Doppeltes Commit

Wenn Sie die Option „Dual Commit“ auswählen, erstellt StorageGRID sofort vorläufige Objektkopien auf zwei verschiedenen Speicherknoten und gibt die Meldung „Aufnahme erfolgreich“ an den Client zurück. Das Objekt wird zur ILM-Auswertung in die Warteschlange gestellt und später werden Kopien erstellt, die den Platzierungsanweisungen der Regel entsprechen. Wenn die ILM-Richtlinie nicht unmittelbar nach dem doppelten Commit verarbeitet werden kann, kann es einige Zeit dauern, bis der Site-Loss-Schutz erreicht ist.

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

- Sie verwenden ILM-Regeln für mehrere Standorte und die Latenzzeit bei der Clientaufnahme ist Ihr Hauptanliegen. Wenn Sie Dual Commit verwenden, müssen Sie sicherstellen, dass Ihr Grid die zusätzliche Arbeit des Erstellens und Entfernens der Dual-Commit-Kopien ausführen kann, wenn diese ILM nicht erfüllen. Speziell:
  - Die Netzbelastung muss gering genug sein, um einen ILM-Rückstau zu verhindern.
  - Das Grid muss über überschüssige Hardwareressourcen (IOPS, CPU, Speicher, Netzwerkbandbreite usw.) verfügen.
- Sie verwenden ILM-Regeln für mehrere Standorte und die WAN-Verbindung zwischen den Standorten weist normalerweise eine hohe Latenz oder begrenzte Bandbreite auf. In diesem Szenario kann die Verwendung der Option „Dual Commit“ dazu beitragen, Client-Timeouts zu verhindern. Bevor Sie sich für die Option „Dual Commit“ entscheiden, sollten Sie die Clientanwendung mit realistischen Arbeitslasten testen.

Ausgeglichen (Standard)

Wenn Sie die Option „Ausgewogen“ auswählen, verwendet StorageGRID auch die synchrone Platzierung bei der Aufnahme und erstellt sofort alle in den Platzierungsanweisungen der Regel angegebenen Kopien. Im Gegensatz zur Option „Streng“ verwendet StorageGRID stattdessen „Dual Commit“, wenn es nicht sofort alle Kopien erstellen kann. Wenn die ILM-Richtlinie Platzierungen auf mehreren Sites verwendet und kein sofortiger Schutz vor Site-Verlust erreicht werden kann, wird die Warnung „ILM-Platzierung nicht erreichbar“ ausgelöst.

Verwenden Sie die Option „Ausgewogen“, um die beste Kombination aus Datenschutz, Grid-Leistung und Aufnahmeerfolg zu erzielen. „Ausgeglichen“ ist die Standardoption im Assistenten „ILM-Regel erstellen“.

Strikt

Wenn Sie die Option „Streng“ auswählen, verwendet StorageGRID bei der Aufnahme die synchrone Platzierung und erstellt sofort alle in den Platzierungsanweisungen der Regel angegebenen Objektkopien. Die Aufnahme schlägt fehl, wenn StorageGRID nicht alle Kopien erstellen kann, beispielsweise weil ein erforderlicher Speicherort vorübergehend nicht verfügbar ist. Der Client muss den Vorgang wiederholen.

Verwenden Sie die Option „Streng“, wenn für Sie eine betriebliche oder gesetzliche Anforderung besteht, Objekte sofort nur an den in der ILM-Regel angegebenen Orten zu speichern. Um beispielsweise eine gesetzliche Anforderung zu erfüllen, müssen Sie möglicherweise die Option „Streng“ und einen erweiterten

Filter „Standortbeschränkung“ verwenden, um sicherzustellen, dass Objekte niemals in bestimmten Rechenzentren gespeichert werden.

Sehen "Beispiel 5: ILM-Regeln und -Richtlinien für striktes Aufnahmeverhalten" .

Vorteile, Nachteile und Einschränkungen der Aufnahmeoptionen

Wenn Sie die Vor- und Nachteile der drei Optionen zum Schutz von Daten bei der Aufnahme (Balanced, Strict oder Dual Commit) kennen, können Sie leichter entscheiden, welche Option Sie für eine ILM-Regel auswählen.

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

Vorteile der Optionen „Ausgewogen“ und „Streng“

Im Vergleich zum Dual Commit, bei dem während der Aufnahme Zwischenkopien erstellt werden, können die beiden synchronen Platzierungsoptionen die folgenden Vorteile bieten:

- **Bessere Datensicherheit**: Objektdaten werden sofort gemäß den Platzierungsanweisungen der ILM-Regel geschützt. Diese können so konfiguriert werden, dass sie vor einer Vielzahl von Fehlerbedingungen schützen, einschließlich des Ausfalls von mehr als einem Speicherort. Dual Commit kann nur vor dem Verlust einer einzigen lokalen Kopie schützen.
- **Effizienterer Grid-Betrieb**: Jedes Objekt wird bei der Aufnahme nur einmal verarbeitet. Da das StorageGRID -System keine Zwischenkopien verfolgen oder löschen muss, ist die Verarbeitungslast geringer und es wird weniger Datenbankspeicherplatz verbraucht.
- **(Ausgewogen) Empfohlen**: Die Option „Ausgewogen“ bietet optimale ILM-Effizienz. Die Verwendung der Option „Ausgewogen“ wird empfohlen, es sei denn, es ist ein striktes Aufnahmeverhalten erforderlich oder das Raster erfüllt alle Kriterien für die Verwendung von Dual Commit.
- **(Strenge) Sicherheit bezüglich der Objektstandorte**: Die Option „Strenge“ garantiert, dass Objekte sofort gemäß den Platzierungsanweisungen in der ILM-Regel gespeichert werden.

Nachteile der Optionen „Ausgewogen“ und „Streng“

Im Vergleich zu Dual Commit haben die Optionen Balanced und Strict einige Nachteile:

- **Längere Client-Aufnahmen**: Die Latenzen bei der Client-Aufnahme können länger sein. Wenn Sie die Optionen „Ausgewogen“ oder „Streng“ verwenden, wird die Meldung „Aufnahme erfolgreich“ erst dann an den Client zurückgegeben, wenn alle Erasure-Coded-Fragmente oder replizierten Kopien erstellt und gespeichert wurden. Allerdings erreichen die Objektdaten ihre endgültige Platzierung höchstwahrscheinlich viel schneller.
- **(Streng) Höhere Fehlerraten bei der Aufnahme**: Bei der Option „Streng“ schlägt die Aufnahme fehl, wenn StorageGRID nicht sofort alle in der ILM-Regel angegebenen Kopien erstellen kann. Wenn ein erforderlicher Speicherort vorübergehend offline ist oder wenn Netzwerkprobleme zu Verzögerungen beim Kopieren von Objekten zwischen Sites führen, kann es zu hohen Aufnahmefehlerraten kommen.
- **(Streng) Platzierungen von mehrteiligen S3-Uploads können unter bestimmten Umständen nicht wie erwartet erfolgen**: Bei „Streng“ erwarten Sie, dass Objekte entweder wie in der ILM-Regel beschrieben platziert werden oder dass die Aufnahme fehlschlägt. Bei einem mehrteiligen S3-Upload wird ILM jedoch für jeden Teil des Objekts beim Einlesen und für das gesamte Objekt ausgewertet, wenn der mehrteilige Upload abgeschlossen ist. Unter folgenden Umständen kann dies zu Platzierungen führen, die anders ausfallen als erwartet:
  - **Wenn sich ILM während eines laufenden S3-Multipart-Uploads ändert**: Da jeder Teil gemäß der Regel platziert wird, die beim Aufnehmen des Teils aktiv ist, erfüllen einige Teile des Objekts

möglicherweise nicht die aktuellen ILM-Anforderungen, wenn der Multipart-Upload abgeschlossen ist. In diesen Fällen schlägt die Aufnahme des Objekts nicht fehl. Stattdessen wird jedes Teil, das nicht richtig platziert ist, zur erneuten ILM-Bewertung in die Warteschlange gestellt und später an die richtige Position verschoben.

    - **Wenn ILM-Regeln nach Größe filtern**: Beim Auswerten von ILM für ein Teil filtert StorageGRID nach der Größe des Teils, nicht nach der Größe des Objekts. Dies bedeutet, dass Teile eines Objekts an Orten gespeichert werden können, die die ILM-Anforderungen für das gesamte Objekt nicht erfüllen. Wenn beispielsweise eine Regel angibt, dass alle Objekte mit 10 GB oder mehr bei DC1 gespeichert werden, während alle kleineren Objekte bei DC2 gespeichert werden, wird bei der Aufnahme jeder 1-GB-Teil eines 10-teiligen mehrteiligen Uploads bei DC2 gespeichert. Wenn ILM für das Objekt ausgewertet wird, werden alle Teile des Objekts nach DC1 verschoben.

- **(Streng) Die Aufnahme schlägt nicht fehl, wenn Objekt-Tags oder Metadaten aktualisiert werden und neu erforderliche Platzierungen nicht vorgenommen werden können**: Bei „Streng“ 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. Dies bedeutet, dass alle durch das Update ausgelösten Änderungen an der Objektplatzierung nicht sofort vorgenommen werden. Platzierungsänderungen werden vorgenommen, wenn ILM durch normale ILM-Hintergrundprozesse neu ausgewertet wird. Wenn erforderliche Platzierungsänderungen nicht vorgenommen werden können (beispielsweise weil ein neu erforderlicher Speicherort nicht verfügbar ist), behält das aktualisierte Objekt seine aktuelle Platzierung bei, bis die Platzierungsänderungen möglich sind.

Einschränkungen bei der Objektplatzierung mit den Optionen „Ausgewogen“ und „Streng“

Die Optionen „Ausgewogen“ oder „Streng“ können nicht für ILM-Regeln verwendet werden, die eine der folgenden Platzierungsanweisungen enthalten:

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

Diese Einschränkungen bestehen, weil StorageGRID keine synchronen Kopien in einem Cloud-Speicherpool erstellen kann und eine benutzerdefinierte Erstellungszeit bis zur Gegenwart reichen könnte.

Wie sich ILM-Regeln und Konsistenz auf den Datenschutz auswirken

Sowohl Ihre ILM-Regel als auch Ihre Wahl der Konsistenz wirken sich darauf aus, wie Objekte geschützt werden. Diese Einstellungen können interagieren.

Beispielsweise wirkt sich das für eine ILM-Regel ausgewählte Aufnahmeverhalten auf die anfängliche Platzierung von Objektkopien aus, während die beim Speichern eines Objekts verwendete Konsistenz die anfängliche Platzierung von Objektmetadaten beeinflusst. Da StorageGRID zur Erfüllung von Clientanforderungen Zugriff auf die Daten und Metadaten eines Objekts benötigt, kann die Auswahl passender Schutzebenen für Konsistenz und Aufnahmeverhalten einen besseren anfänglichen Datenschutz und vorhersehbarere Systemreaktionen bieten.

Hier ist eine kurze Zusammenfassung der Konsistenzwerte, die in StorageGRID verfügbar sind:

- **Alle**: Alle Knoten erhalten die Objektmetadaten sofort, andernfalls schlägt die Anforderung fehl.
- **Stark-global**: Objektmetadaten werden sofort an alle Sites verteilt. Garantiert Lese- und Schreibkonsistenz für alle Clientanforderungen auf allen Sites.
- **Strong-Site**: Objektmetadaten werden sofort an andere Knoten der Site verteilt. Garantiert die Lese- und Schreibkonsistenz für alle Clientanforderungen innerhalb einer Site.

- **Lesen nach neuem Schreiben**: Bietet Lese-nach-Schreib-Konsistenz für neue Objekte und letztendliche Konsistenz für Objektaktualisierungen. Bietet hohe Verfügbarkeit und Datenschutzgarantien. Für die meisten Fälle empfohlen.
- **Verfügbar**: Bietet letztendliche Konsistenz sowohl für neue Objekte als auch für Objektaktualisierungen. Verwenden Sie es für S3-Buckets nur nach Bedarf (z. B. für einen Bucket, der Protokollwerte enthält, die selten gelesen werden, oder für HEAD- oder GET-Operationen für nicht vorhandene Schlüssel). Wird für S3 FabricPool Buckets nicht unterstützt.

> Bevor Sie einen Konsistenzwert auswählen,"Lesen Sie die vollständige Beschreibung der Konsistenz" . Sie sollten die Vorteile und Einschränkungen verstehen, bevor Sie den Standardwert ändern.

Beispiel für die Interaktion von Konsistenz- und ILM-Regeln

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

- **ILM-Regel**: Erstellen Sie zwei Objektkopien, eine am lokalen Standort und eine an einem Remote-Standort. Verwenden Sie ein striktes Aufnahmeverhalten.
- **Konsistenz**: Stark global (Objektmetadaten werden sofort an alle Sites verteilt).

Wenn ein Client ein Objekt im Grid speichert, erstellt StorageGRID Kopien beider Objekte und verteilt Metadaten an beide Sites, bevor dem Client die Erfolgsmeldung zurückgegeben wird.

Zum Zeitpunkt der erfolgreichen Aufnahme der Nachricht ist das Objekt vollständig vor Verlust geschützt. Wenn beispielsweise die lokale Site kurz nach der Aufnahme verloren geht, sind am Remote-Standort weiterhin Kopien der Objektdaten und der Objektmetadaten vorhanden. Das Objekt ist vollständig abrufbar.

Wenn Sie stattdessen dieselbe ILM-Regel und die starke Site-Konsistenz verwenden, erhält der Client möglicherweise eine Erfolgsmeldung, nachdem die Objektdaten auf die Remote-Site repliziert wurden, aber bevor die Objektmetadaten dorthin verteilt werden. In diesem Fall entspricht das Schutzniveau der Objektmetadaten nicht dem Schutzniveau der Objektdaten. Wenn die lokale Site kurz nach der Aufnahme verloren geht, gehen die Objektmetadaten verloren. Das Objekt kann nicht abgerufen werden.

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

Ähnliche Informationen

"Beispiel 5: ILM-Regeln und -Richtlinien für striktes Aufnahmeverhalten"

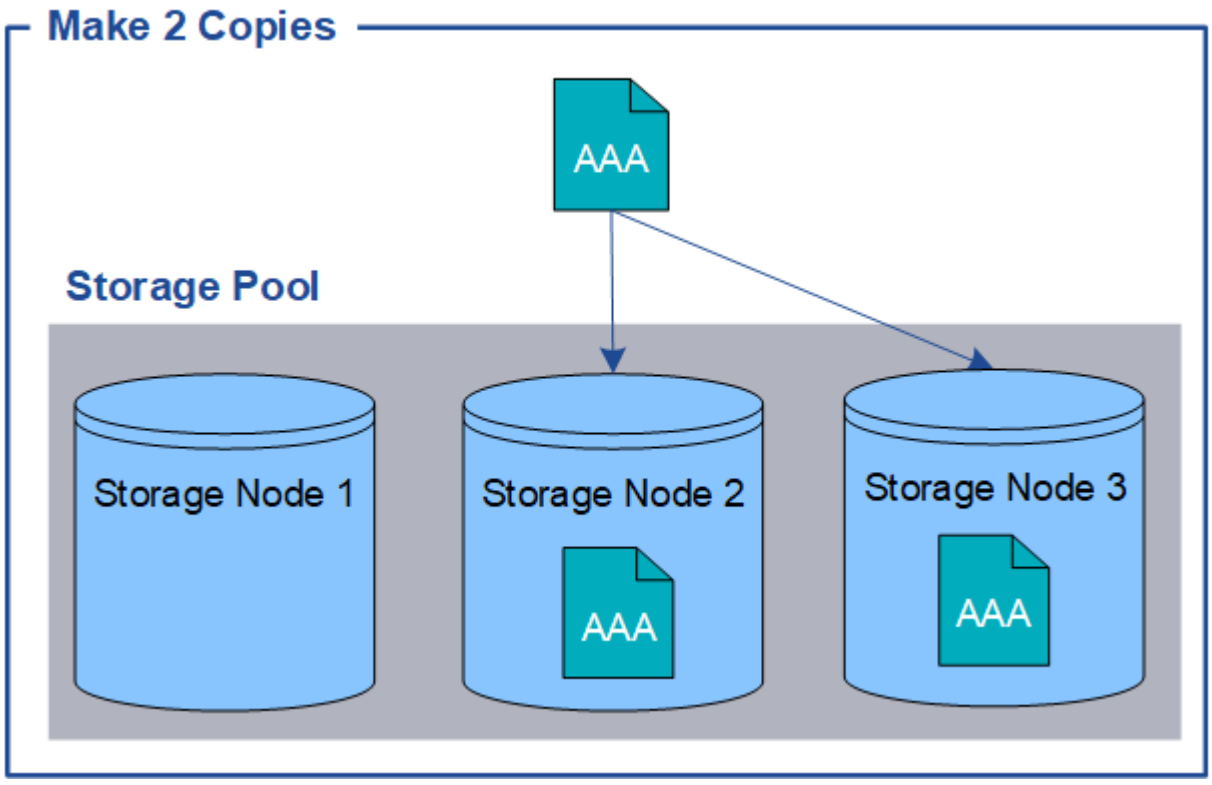
Wie Objekte gespeichert werden (Replikation oder Erasure Coding)

Was ist Replikation?

Die Replikation ist eine von zwei Methoden, die von StorageGRID zum Speichern von Objektdaten verwendet werden (die andere Methode ist Erasure Coding). Wenn Objekte einer ILM-Regel entsprechen, die Replikation verwendet, erstellt das System exakte Kopien der Objektdaten und speichert die Kopien auf Speicherknoten.

Wenn Sie eine ILM-Regel zum Erstellen replizierter Kopien konfigurieren, geben Sie an, wie viele Kopien erstellt werden sollen, wo diese Kopien abgelegt 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 Speicherpool abgelegt werden, der drei Speicherknoten enthält.



Wenn StorageGRID Objekte mit dieser Regel abgleicht, erstellt es zwei Kopien des Objekts und platziert jede Kopie auf einem anderen Speicherknoten im Speicherpool. Die beiden Kopien können auf zwei beliebigen der drei verfügbaren Speicherknoten platziert werden. In diesem Fall platzierte die Regel Objektkopien auf den Speicherknoten 2 und 3. Da zwei Kopien vorhanden sind, kann das Objekt abgerufen werden, wenn einer der Knoten im Speicherpool ausfällt.

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

Ähnliche Informationen

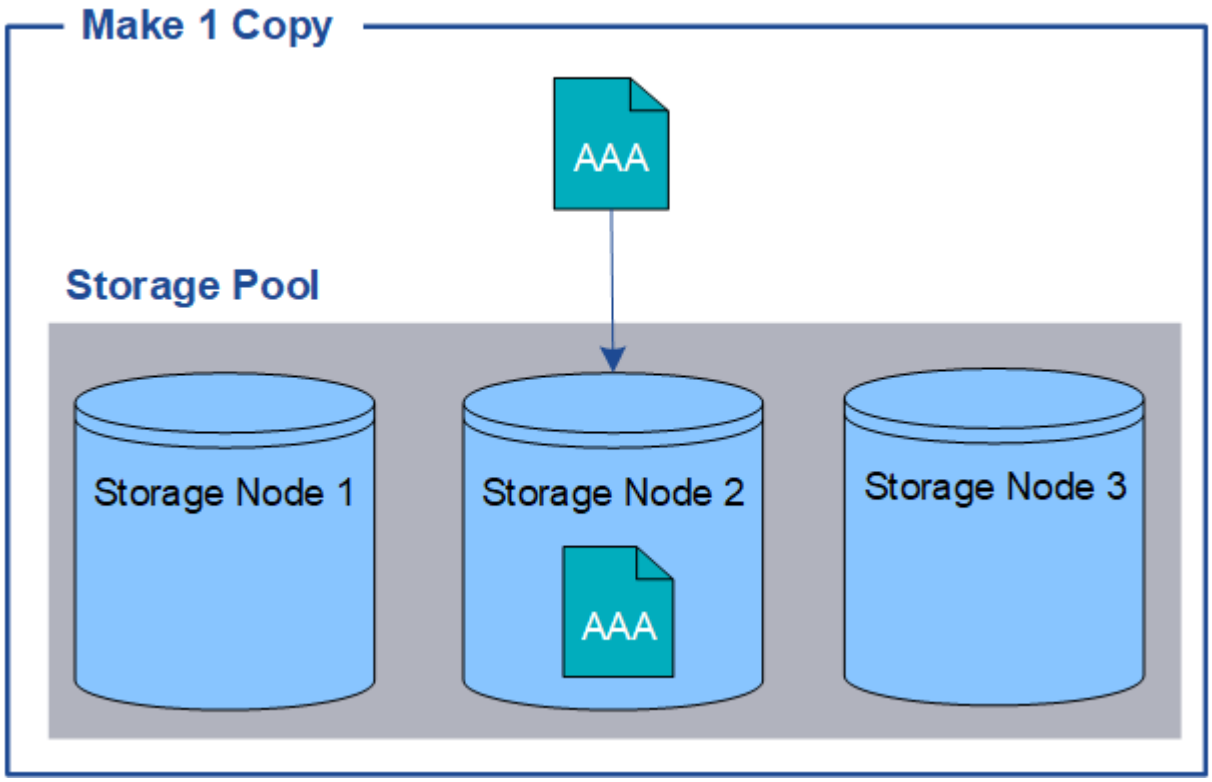
- "Was ist Erasure Coding"
- "Was ist ein Speicherpool?"
- "Aktivieren Sie den Site-Loss-Schutz durch Replikation und Erasure Coding"

Warum Sie keine Einzelkopiereplikation verwenden sollten

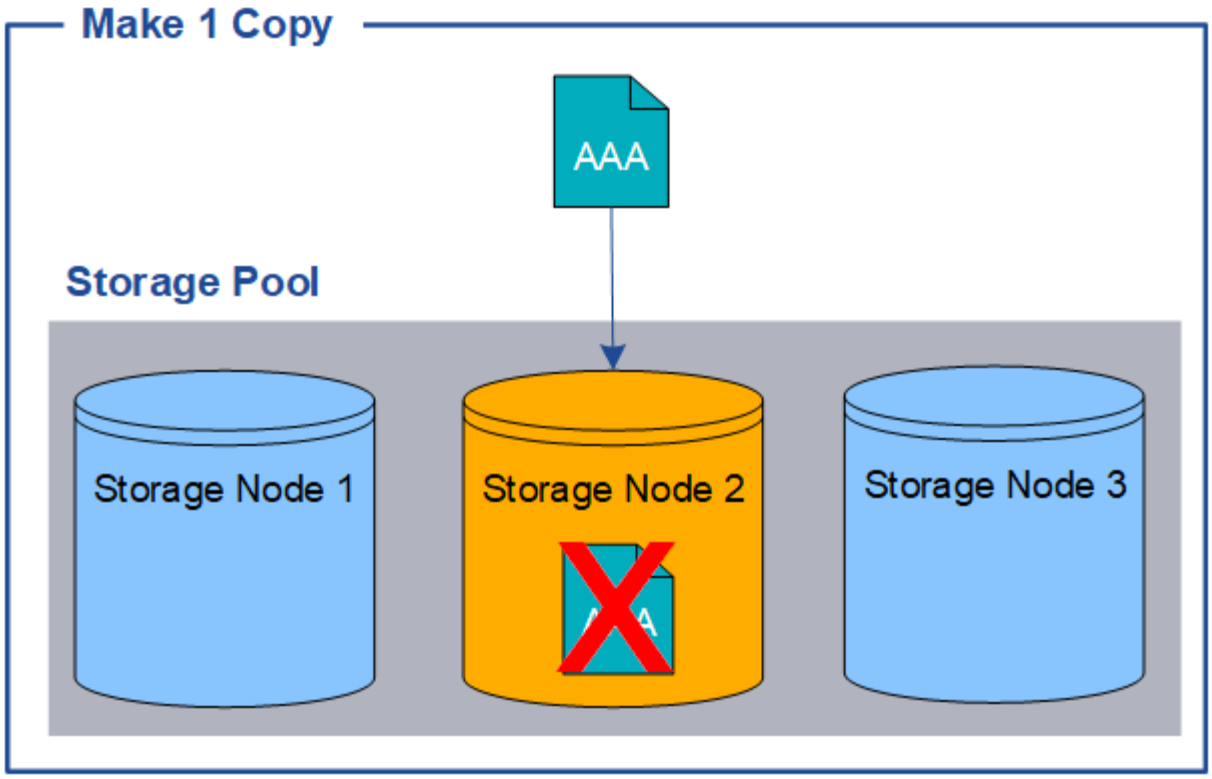
Wenn Sie eine ILM-Regel zum Erstellen replizierter Kopien erstellen, sollten Sie in den Platzierungsanweisungen immer mindestens zwei Kopien für einen beliebigen Zeitraum angeben.

Verwenden Sie keine ILM-Regel, die für einen bestimmten Zeitraum nur eine replizierte Kopie erstellt. Wenn nur eine replizierte Kopie eines Objekts vorhanden ist, geht dieses Objekt verloren, wenn ein Speicherknoten ausfällt oder einen schwerwiegenden Fehler aufweist. Auch während Wartungsvorgängen wie Upgrades verlieren Sie vorübergehend den Zugriff auf das Objekt.

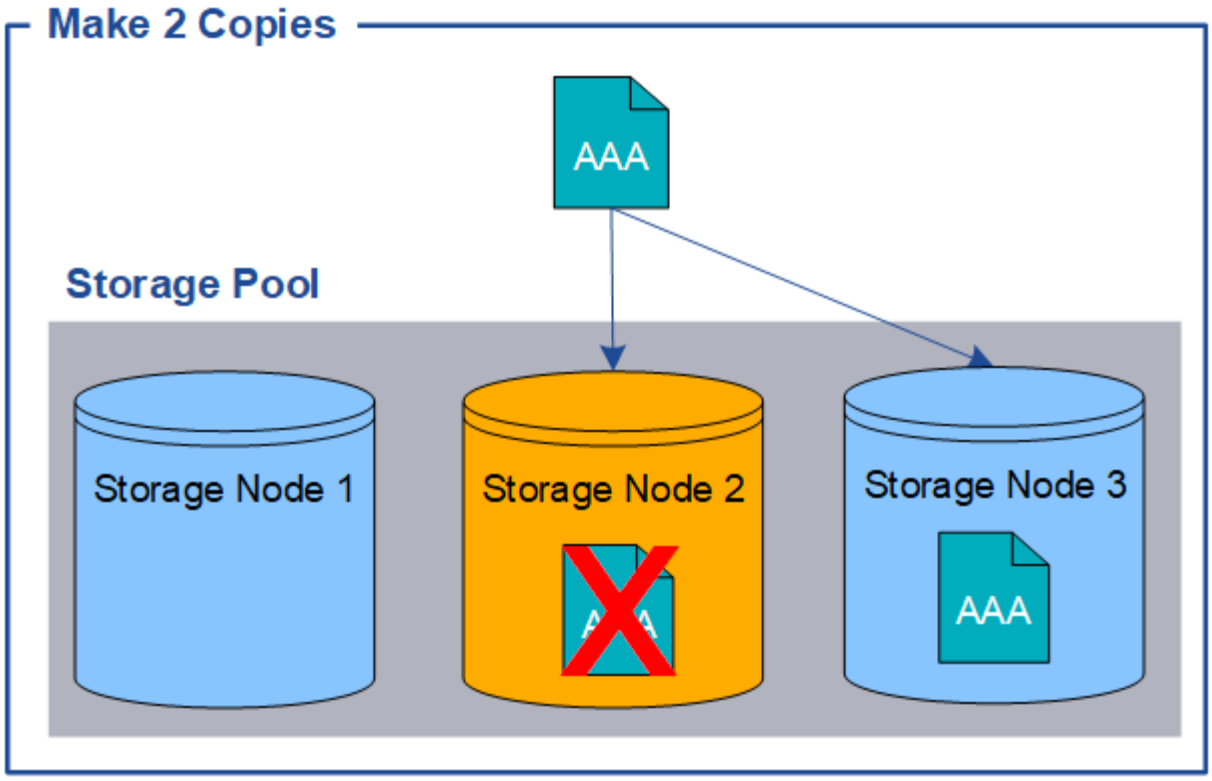
Im folgenden Beispiel gibt die ILM-Regel „1 Kopie erstellen“ an, dass eine replizierte Kopie eines Objekts in einem Speicherpool abgelegt wird, der drei Speicherknoten enthält. Wenn ein Objekt aufgenommen wird, das dieser Regel entspricht, platziert StorageGRID eine einzelne Kopie auf nur einem Speicherknoten.



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



Um den Verlust von Objektdaten zu vermeiden, sollten Sie immer mindestens zwei Kopien aller Objekte erstellen, die Sie durch Replikation schützen möchten. Wenn zwei oder mehr Kopien vorhanden sind, können Sie weiterhin auf das Objekt zugreifen, wenn ein Speicherknoten ausfällt oder offline geht.



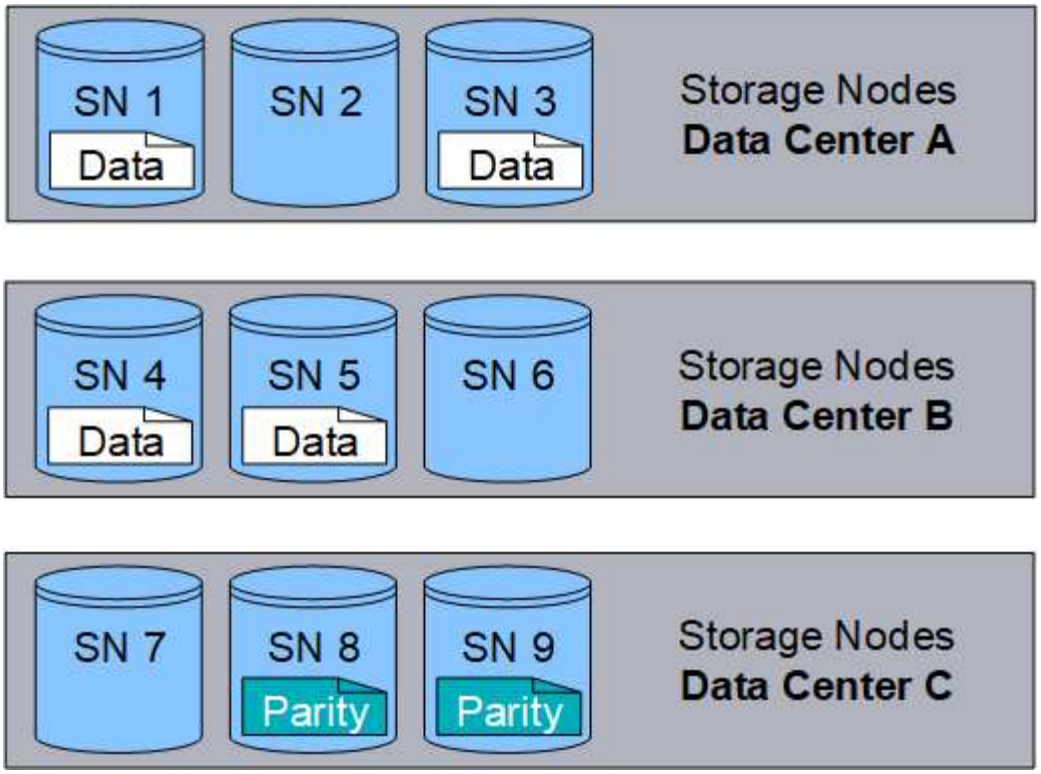
Was ist Erasure Coding?

Erasure Coding ist eine von zwei Methoden, die StorageGRID zum Speichern von Objektdaten verwendet (die andere Methode ist Replikation). Wenn Objekte einer ILM-Regel entsprechen, die Erasure Coding verwendet, werden diese Objekte in Datenfragmente aufgeteilt, zusätzliche Paritätsfragmente werden berechnet und jedes Fragment wird auf einem anderen Speicherknoten gespeichert.

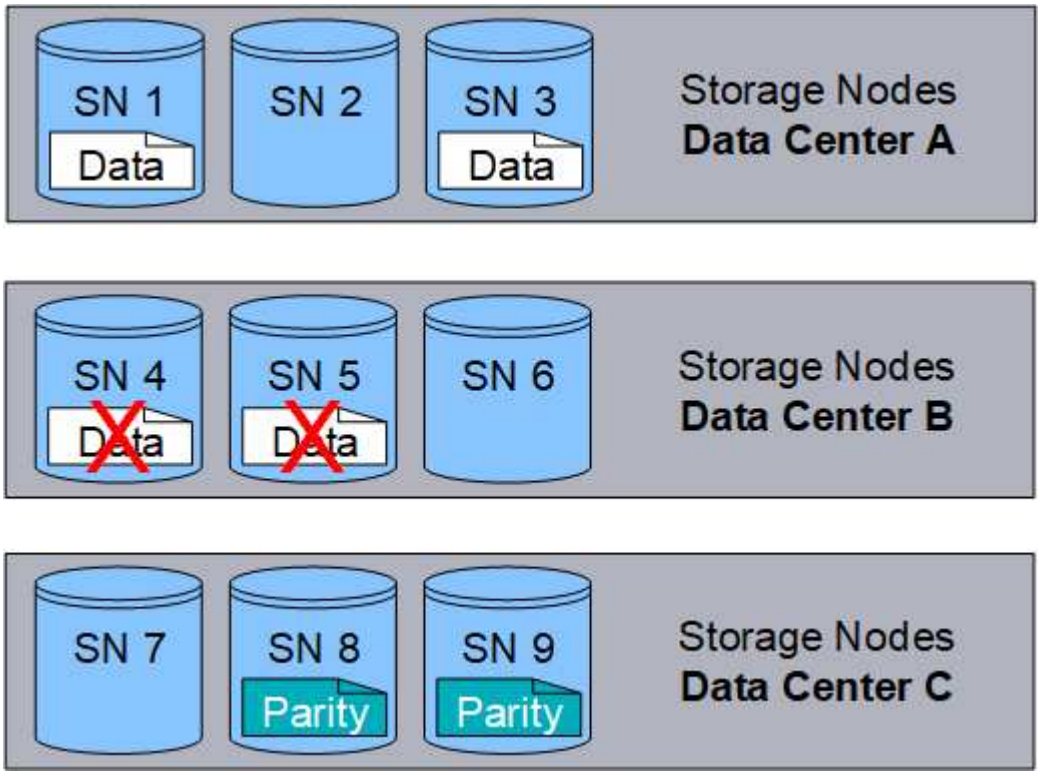
Beim Zugriff auf ein Objekt wird es anhand der gespeicherten Fragmente wieder zusammengesetzt. Wenn Daten oder ein Paritätsfragment beschädigt werden oder verloren gehen, kann der Erasure-Coding-Algorithmus dieses Fragment mithilfe einer Teilmenge der verbleibenden Daten und Paritätsfragmente wiederherstellen.

Während Sie ILM-Regeln erstellen, erstellt StorageGRID Erasure-Coding-Profile, die diese Regeln unterstützen. Sie können eine Liste der Erasure-Coding-Profile anzeigen,"Umbenennen eines Erasure-Coding-Profils" , oder"Deaktivieren Sie ein Erasure-Coding-Profil, wenn es derzeit in keinen ILM-Regeln verwendet wird." .

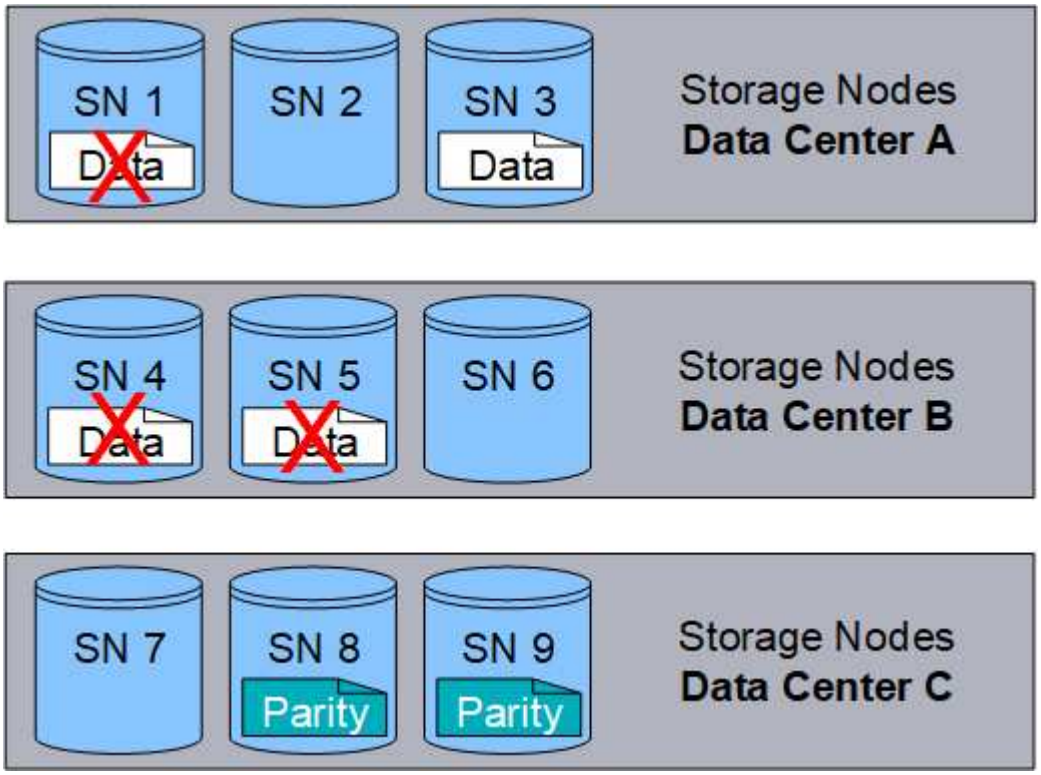
Das folgende Beispiel veranschaulicht die Verwendung eines Erasure-Coding-Algorithmus auf die Daten eines Objekts. In diesem Beispiel verwendet die ILM-Regel ein 4+2-Erasure-Coding-Schema. Jedes Objekt wird in vier gleiche Datenfragmente aufgeteilt und aus den Objektdaten werden zwei Paritätsfragmente berechnet. Jedes der sechs Fragmente wird auf einem anderen Knoten an drei Rechenzentrumsstandorten gespeichert, um Datenschutz bei Knotenausfällen oder Standortverlust zu gewährleisten.



Das 4+2-Erasure-Coding-Schema kann auf verschiedene Arten konfiguriert werden. Sie können beispielsweise einen Single-Site-Speicherpool konfigurieren, der sechs Speicherknoten enthält. Für"Site-Loss-Schutz" können Sie einen Speicherpool mit drei Standorten und jeweils drei Speicherknoten an jedem Standort verwenden. Ein Objekt kann abgerufen werden, solange vier der sechs Fragmente (Daten oder Parität) verfügbar bleiben. Bis zu zwei Fragmente können verloren gehen, ohne dass die Objektdaten verloren gehen. Wenn eine ganze Site verloren geht, kann das Objekt immer noch geborgen oder repariert werden, solange alle anderen Fragmente zugänglich bleiben.



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



Ähnliche Informationen

- "Was ist Replikation?"
- "Was ist ein Speicherpool?"
- "Was sind Erasure-Coding-Schemata?"
- "Umbenennen eines Erasure-Coding-Profils"
- "Deaktivieren eines Erasure-Coding-Profils"

Was sind Erasure-Coding-Schemata?

Erasure-Coding-Schemata steuern, wie viele Datenfragmente und wie viele Paritätsfragmente für jedes Objekt erstellt werden.

Wenn Sie eine ILM-Regel erstellen oder bearbeiten, wählen Sie ein verfügbares Erasure-Coding-Schema aus. StorageGRID erstellt automatisch Erasure-Coding-Schemata basierend auf der Anzahl der Speicherknoten und Sites, aus denen der Speicherpool besteht, den Sie verwenden möchten.

Datenschutz

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

Der `k + m = n` Fragmente sind verteilt über `n` Speicherknoten bieten Datenschutz wie folgt:

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

Den besten Datenschutz bietet das Erasure-Coding-Schema mit der höchsten Knoten- oder Volume-Ausfalltoleranz innerhalb eines Speicherpools.

Speicheraufwand

Der Speicheraufwand eines Erasure-Coding-Schemas wird berechnet, indem die Anzahl der Paritätsfragmente geteilt wird(`m`) durch die Anzahl der Datenfragmente(`k`). Mithilfe des Speicher-Overheads können Sie berechnen, wie viel Speicherplatz jedes Erasure-Codierte Objekt benötigt:

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

Wenn Sie beispielsweise ein 10 MB großes Objekt mit dem 4+2-Schema speichern (das einen Speicher-Overhead von 50 % hat), verbraucht das Objekt 15 MB Grid-Speicher. Wenn Sie dasselbe 10 MB große Objekt mit dem 6+2-Schema speichern (das einen Speicher-Overhead von 33 % hat), verbraucht das Objekt ungefähr 13,3 MB.

Wählen Sie das Erasure-Coding-Schema mit dem niedrigsten Gesamtwert von `k+m` das Ihren Bedürfnissen entspricht. Erasure-Coding-Verfahren mit einer geringeren Anzahl von Fragmenten sind rechnerisch effizienter, weil:

- Pro Objekt werden weniger Fragmente erstellt und verteilt (oder abgerufen)
- Sie weisen eine bessere Leistung auf, da die Fragmentgröße größer ist
- Sie können erfordern, dass weniger Knoten in einem"Erweiterung, wenn mehr Speicherplatz benötigt wird"

Richtlinien für Speicherpools

Beachten Sie bei der Auswahl des Speicherpools für eine Regel zum Erstellen einer Löschcodierten Kopie die folgenden Richtlinien für Speicherpools:

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

  > Sie können Erasure Coding nicht verwenden, wenn der Speicherpool zwei Standorte umfasst.

  - Erasure-Coding-Schemata für Speicherpools mit drei oder mehr Standorten
  - Erasure-Coding-Schemata für Speicherpools an einem Standort
- Verwenden Sie keinen Speicherpool, der die Site „Alle Sites“ enthält.
- Der Speicherpool sollte mindestens *`k+m`* `+1` Speicherknoten, die Objektdaten speichern können.

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

  Die Mindestanzahl der erforderlichen Speicherknoten beträgt `k+m` . Wenn jedoch mindestens ein zusätzlicher Speicherknoten vorhanden ist, können Aufnahmefehler oder ILM-Rückstände vermieden werden, wenn ein erforderlicher Speicherknoten vorübergehend nicht verfügbar ist.

Erasure-Coding-Schemata für Speicherpools mit drei oder mehr Standorten

Die folgende Tabelle beschreibt die Erasure-Coding-Schemata, die derzeit von StorageGRID für Speicherpools mit drei oder mehr Standorten unterstützt werden. Alle diese Systeme bieten Schutz vor Standortverlust. Eine

Site kann verloren gehen, und das Objekt ist weiterhin zugänglich.

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

Erasure-Coding-Schema (*k+m*)	Mindestanzahl bereitgestellter Sites	Empfohlene Anzahl von Speicherknoten an jedem Standort	Empfohlene Gesamtzahl an Speicherknoten	Schutz vor Site-Verlust?	Speicheraufwand
4+2	3	3	9	Ja	50 %
6+2	4	3	12	Ja	33 %
8+2	5	3	15	Ja	25 %
6+3	3	4	12	Ja	50 %
9+3	4	4	16	Ja	33 %
2+1	3	3	9	Ja	50 %
4+1	5	3	15	Ja	25 %
6+1	7	3	21	Ja	17 %
7+5	3	5	15	Ja	71 %

StorageGRID erfordert mindestens drei Speicherknoten pro Site. Um das 7+5-Schema zu verwenden, benötigt jeder Standort mindestens vier Speicherknoten. Es wird empfohlen, fünf Speicherknoten pro Site zu verwenden.

Wägen Sie bei der Auswahl eines Löschcodierungsschemas, das Site-Schutz bietet, die relative Bedeutung der folgenden Faktoren ab:

- **Anzahl der Fragmente**: Leistung und Erweiterungsflexibilität sind im Allgemeinen besser, wenn die Gesamtzahl der Fragmente geringer ist.
- **Fehlertoleranz**: Die Fehlertoleranz wird durch mehr Paritätssegmente erhöht (d. h. wenn `m` hat einen höheren Wert.)
- **Netzwerkverkehr**: Bei der Wiederherstellung nach Fehlern wird ein Schema mit mehr Fragmenten verwendet (d. h. eine höhere Gesamtzahl für `k+m`) erzeugt mehr Netzwerkverkehr.
- **Speicher-Overhead**: Schemata mit höherem Overhead erfordern mehr Speicherplatz pro Objekt.

Wenn Sie sich beispielsweise zwischen einem 4+2-Schema und einem 6+3-Schema entscheiden (die beide einen Speicher-Overhead von 50 % haben), wählen Sie das 6+3-Schema, wenn zusätzliche Fehlertoleranz erforderlich ist. Wählen Sie das 4+2-Schema, wenn die Netzwerkressourcen eingeschränkt sind. Wenn alle anderen Faktoren gleich sind, wählen Sie 4+2, da dies eine geringere Gesamtzahl an Fragmenten ergibt.

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

Erasure-Coding-Schemata für Speicherpools an einem Standort

Ein Speicherpool für einen Standort unterstützt alle für drei oder mehr Standorte definierten Erasure-Coding-Schemata, vorausgesetzt, der Standort verfügt über genügend Speicherknoten.

Die Mindestanzahl der erforderlichen Speicherknoten beträgt `k+m` , sondern ein Speicherpool mit `k+m +1` Speicherknoten werden empfohlen. Beispielsweise erfordert das 2+1-Erasure-Coding-Schema einen Speicherpool mit mindestens drei Speicherknoten, empfohlen werden jedoch vier Speicherknoten.

Erasure-Coding-Schema (*k+m*)	Mindestanzahl an Speicherknoten	Empfohlene Anzahl von Speicherknoten	Speicheraufwand
4+2	6	7	50 %
6+2	8	9	33 %
8+2	10	11	25 %
6+3	9	10	50 %
9+3	12	13	33 %
2+1	3	4	50 %
4+1	5	6	25 %
6+1	7	8	17 %
7+5	12	13	71 %

Vorteile, Nachteile und Voraussetzungen für Erasure Coding

Bevor Sie sich entscheiden, ob Sie Replikation oder Erasure Coding zum Schutz von Objektdaten vor Verlust verwenden, sollten Sie die Vor- und Nachteile sowie die Anforderungen von Erasure Coding verstehen.

Vorteile der Erasure Coding

Im Vergleich zur Replikation bietet Erasure Coding eine verbesserte Zuverlässigkeit, Verfügbarkeit und Speichereffizienz.

- **Zuverlässigkeit**: Die Zuverlässigkeit wird anhand der Fehlertoleranz gemessen, d. h. anhand der Anzahl gleichzeitiger Fehler, die ohne Datenverlust toleriert werden können. Bei der Replikation werden mehrere identische Kopien auf verschiedenen Knoten und an verschiedenen Standorten gespeichert. Beim Erasure Coding wird ein Objekt in Daten- und Paritätsfragmente kodiert und auf viele Knoten und Standorte verteilt. Diese Verteilung bietet sowohl Site- als auch Knotenausfallschutz. Im Vergleich zur Replikation bietet

Erasure Coding eine verbesserte Zuverlässigkeit bei vergleichbaren Speicherkosten.

- **Verfügbarkeit**: Verfügbarkeit kann als die Fähigkeit definiert werden, Objekte abzurufen, wenn Speicherknoten ausfallen oder nicht mehr zugänglich sind. Im Vergleich zur Replikation bietet Erasure Coding eine höhere Verfügbarkeit bei vergleichbaren Speicherkosten.
- **Speichereffizienz**: Bei vergleichbarer Verfügbarkeit und Zuverlässigkeit verbrauchen durch Erasure Coding geschützte Objekte weniger Speicherplatz als dieselben Objekte, die durch Replikation geschützt wären. Beispielsweise verbraucht ein 10 MB großes Objekt, das an zwei Standorten repliziert wird, 20 MB Speicherplatz (zwei Kopien), während ein Objekt, das an drei Standorten mit einem 6+3-Erasure-Coding-Schema löschcodiert wird, nur 15 MB Speicherplatz verbraucht.

> ⓘ Der Speicherplatz für Erasure-Codierte Objekte wird aus der Objektgröße plus Speicher-Overhead berechnet. Der Prozentsatz des Speicher-Overheads ist die Anzahl der Paritätsfragmente geteilt durch die Anzahl der Datenfragmente.

Nachteile der Erasure Coding

Im Vergleich zur Replikation weist Erasure Coding folgende Nachteile auf:

- Je nach Erasure-Coding-Schema wird eine erhöhte Anzahl von Speicherknoten und -standorten empfohlen. Wenn Sie dagegen Objektdaten replizieren, benötigen Sie nur einen Speicherknoten für jede Kopie. Sehen"Erasure-Coding-Schemata für Speicherpools mit drei oder mehr Standorten" Und"Erasure-Coding-Schemata für Speicherpools an einem Standort" .
- Erhöhte Kosten und Komplexität von Speichererweiterungen. Um eine Bereitstellung zu erweitern, die Replikation verwendet, fügen Sie an jedem Standort, an dem Objektkopien erstellt werden, Speicherkapazität hinzu. Um eine Bereitstellung zu erweitern, die Erasure Coding verwendet, müssen Sie sowohl das verwendete Erasure-Coding-Schema als auch den Füllstand vorhandener Speicherknoten berücksichtigen. Wenn Sie beispielsweise warten, bis vorhandene Knoten zu 100 % belegt sind, müssen Sie mindestens `k+m` Speicherknoten. Wenn Sie jedoch erweitern, wenn die vorhandenen Knoten zu 70 % belegt sind, können Sie zwei Knoten pro Site hinzufügen und trotzdem die nutzbare Speicherkapazität maximieren. Weitere Informationen finden Sie unter "Speicherkapazität für Erasure-Coded-Objekte hinzufügen" .
- Bei der Verwendung von Erasure Coding an geografisch verteilten Standorten kommt es zu längeren Abruflatenzen. Das Abrufen der Objektfragmente für ein Objekt, das mit einem Erasure Code versehen und über Remote-Standorte verteilt ist, über WAN-Verbindungen dauert länger als das Abrufen eines Objekts, das repliziert und lokal verfügbar ist (derselbe Standort, mit dem der Client eine Verbindung herstellt).
- Wenn Sie Erasure Coding an geografisch verteilten Standorten verwenden, kommt es zu einer höheren Auslastung des WAN-Netzwerkverkehrs für Abrufe und Reparaturen, insbesondere bei häufig abgerufenen Objekten oder für Objektreparaturen über WAN-Netzwerkverbindungen.
- Wenn Sie Erasure Coding standortübergreifend verwenden, sinkt der maximale Objektdurchsatz stark, da die Netzwerklatenz zwischen den Standorten zunimmt. Dieser Rückgang ist auf den entsprechenden Rückgang des TCP-Netzwerkdurchsatzes zurückzuführen, der sich darauf auswirkt, wie schnell das StorageGRID -System Objektfragmente speichern und abrufen kann.
- Höhere Nutzung von Rechenressourcen.

Wann wird Erasure Coding verwendet?

Erasure Coding eignet sich am besten für folgende Anforderungen:

- Objekte mit einer Größe von mehr als 1 MB.

Erasure Coding eignet sich am besten für Objekte, die größer als 1 MB sind. Verwenden Sie Erasure Coding nicht für Objekte, die kleiner als 200 KB sind, um den Verwaltungsaufwand für sehr kleine Erasure-Coding-Fragmente zu vermeiden.

- Langzeit- oder Cold-Storage für selten abgerufene Inhalte.
- Hohe Datenverfügbarkeit und Zuverlässigkeit.
- Schutz vor vollständigen Site- und Knotenausfällen.
- Speichereffizienz.
- Einzelstandortbereitstellungen, die einen effizienten Datenschutz mit nur einer einzigen löschcodierten Kopie anstelle mehrerer replizierter Kopien erfordern.
- Bereitstellungen an mehreren Standorten, bei denen die Latenz zwischen den Standorten weniger als 100 ms beträgt.

So wird die Objektaufbewahrung bestimmt

StorageGRID bietet sowohl Grid-Administratoren als auch einzelnen Mandantenbenutzern Optionen zum Angeben der Speicherdauer von Objekten. Im Allgemeinen haben alle Aufbewahrungsanweisungen eines Mandantenbenutzers Vorrang vor den Aufbewahrungsanweisungen des Grid-Administrators.

So steuern Mandantenbenutzer die Objektaufbewahrung

Mandantenbenutzer können mit diesen Methoden steuern, wie lange ihre Objekte in StorageGRID gespeichert werden:

- Wenn die globale S3-Objektsperreinstellung für das Raster aktiviert ist, können S3-Mandantenbenutzer Buckets mit aktivierter S3-Objektsperre erstellen und dann für jeden Bucket eine **Standardaufbewahrungsdauer** auswählen.
- Wenn die globale Einstellung „S3 Object Lock“ für das Raster aktiviert ist, können S3-Mandantenbenutzer Buckets mit aktivierter S3 Object Lock erstellen und dann die S3 REST-API verwenden, um Einstellungen für das Aufbewahrungsdatum und die gesetzliche Aufbewahrung für jede diesem Bucket hinzugefügte Objektversion festzulegen.
  - Eine Objektversion, die einer rechtlichen Sperre unterliegt, kann mit keiner Methode gelöscht werden.
  - Bevor das Aufbewahrungsdatum einer Objektversion erreicht ist, kann diese Version mit keiner Methode gelöscht werden.
  - Objekte in Buckets mit aktivierter S3-Objektsperre werden von ILM „für immer“ aufbewahrt. Nach Erreichen des Aufbewahrungsdatums kann eine Objektversion jedoch durch eine Clientanforderung oder den Ablauf des Bucket-Lebenszyklus gelöscht werden. Sehen "Verwalten von Objekten mit S3 Object Lock" .
- S3-Tenant-Benutzer können ihren Buckets eine Lebenszykluskonfiguration hinzufügen, die eine Ablaufaktion angibt. Wenn ein Bucket-Lebenszyklus vorhanden ist, speichert StorageGRID ein Objekt, bis das in der Ablaufaktion angegebene Datum oder die Anzahl der Tage erreicht ist, es sei denn, der Client löscht das Objekt zuerst. Sehen "Erstellen einer S3-Lebenszykluskonfiguration" .
- Ein S3-Client kann eine Anforderung zum Löschen eines Objekts stellen. StorageGRID priorisiert Client-Löschanforderungen immer gegenüber dem S3-Bucket-Lebenszyklus oder ILM, wenn entschieden wird, ob ein Objekt gelöscht oder behalten werden soll.

So steuern Grid-Administratoren die Objektaufbewahrung

Grid-Administratoren können die Objektaufbewahrung mithilfe dieser Methoden steuern:

- Legen Sie für jeden Mandanten eine maximale Aufbewahrungsdauer für S3 Object Lock fest. Anschließend können Mandantenbenutzer für jeden ihrer Buckets eine Standardaufbewahrungsdauer festlegen. Die maximale Aufbewahrungsdauer wird auch für alle neu aufgenommenen Objekte für diesen Bucket erzwungen (Aufbewahrungsdatum des Objekts).
- Erstellen Sie ILM-Platzierungsanweisungen, um zu steuern, wie lange Objekte gespeichert werden. Wenn Objekte mit einer ILM-Regel übereinstimmen, speichert StorageGRID diese Objekte, bis der letzte Zeitraum in der ILM-Regel abgelaufen ist. Objekte bleiben unbegrenzt erhalten, wenn für die Platzierungsanweisungen „für immer“ angegeben ist.
- Unabhängig davon, wer kontrolliert, wie lange Objekte aufbewahrt werden, steuern die ILM-Einstellungen, welche Arten von Objektkopien (repliziert oder löschcodiert) gespeichert werden und wo sich die Kopien befinden (Speicherknoten oder Cloud-Speicherpools).

So interagieren S3-Bucket-Lebenszyklus und ILM

Wenn ein S3-Bucket-Lebenszyklus konfiguriert ist, überschreiben die Aktionen zum Ablauf des Lebenszyklus die ILM-Richtlinie für Objekte, die dem Lebenszyklusfilter entsprechen. Dies kann dazu führen, dass ein Objekt auch dann noch auf dem Raster verbleibt, wenn keine ILM-Anweisungen zum Platzieren des Objekts mehr vorliegen.

Beispiele für die Objektaufbewahrung

Um die Interaktionen zwischen S3 Object Lock, Bucket-Lebenszykluseinstellungen, Client-Löschanforderungen und ILM besser zu verstehen, betrachten Sie die folgenden Beispiele.

Beispiel 1: Der S3-Bucket-Lebenszyklus speichert Objekte länger als ILM

ILM

Bewahren Sie zwei Kopien für 1 Jahr (365 Tage) auf

Bucket-Lebenszyklus

Objekte laufen in 2 Jahren (730 Tagen) ab

Ergebnis

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

> Wenn der Bucket-Lebenszyklus vorgibt, dass Objekte länger aufbewahrt werden sollen als von ILM angegeben, verwendet StorageGRID weiterhin die ILM-Platzierungsanweisungen, um die Anzahl und den Typ der zu speichernden Kopien zu bestimmen. In diesem Beispiel werden von Tag 366 bis 730 weiterhin zwei Kopien des Objekts in StorageGRID gespeichert.

Beispiel 2: S3-Bucket-Lebenszyklus lässt Objekte vor ILM ablaufen

ILM

Bewahren Sie zwei Kopien 2 Jahre lang (730 Tage) auf.

Bucket-Lebenszyklus

Objekte laufen in 1 Jahr (365 Tagen) ab

Ergebnis

StorageGRID löscht beide Kopien des Objekts nach Tag 365.

Beispiel 3: Client-Löschen überschreibt Bucket-Lebenszyklus und ILM

ILM

Speichern Sie zwei Kopien „für immer“ auf Speicherknoten

Bucket-Lebenszyklus

Objekte laufen in 2 Jahren (730 Tagen) ab

Client-Löschanforderung

Ausgestellt am Tag 400

Ergebnis

StorageGRID löscht beide Kopien des Objekts am Tag 400 als Antwort auf die Löschanforderung des Clients.

Beispiel 4: S3 Object Lock überschreibt Client-Löschanforderung

S3-Objektsperre

Das Aufbewahrungsdatum für eine Objektversion ist der 31.03.2026. Eine rechtliche Sperre besteht nicht.

Konforme ILM-Regel

Speichern Sie zwei Kopien „für immer“ auf Speicherknoten

Client-Löschanforderung

Ausgestellt am 31.03.2024

Ergebnis

StorageGRID löscht die Objektversion nicht, da das Aufbewahrungsdatum noch 2 Jahre entfernt ist.

So werden Objekte gelöscht

StorageGRID kann Objekte entweder als direkte Reaktion auf eine Clientanforderung oder automatisch aufgrund des Ablaufs eines S3-Bucket-Lebenszyklus oder der Anforderungen der ILM-Richtlinie löschen. Wenn Sie die verschiedenen Möglichkeiten zum Löschen von Objekten und die Art und Weise verstehen, wie StorageGRID Löschanforderungen verarbeitet, können Sie Objekte effizienter verwalten.

StorageGRID kann zum Löschen von Objekten eine von zwei Methoden verwenden:

- Synchrones Löschen: Wenn StorageGRID eine Löschanforderung des Clients erhält, werden alle Objektkopien sofort entfernt. Nach dem Entfernen der Kopien wird dem Kunden mitgeteilt, dass die Löschung erfolgreich war.
- Objekte werden zum Löschen in die Warteschlange gestellt: Wenn StorageGRID eine Löschanforderung erhält, wird das Objekt zum Löschen in die Warteschlange gestellt und der Client wird sofort darüber informiert, dass das Löschen erfolgreich war. Objektkopien werden später durch die ILM-Hintergrundverarbeitung entfernt.

Beim Löschen von Objekten verwendet StorageGRID die Methode, die die Löschleistung optimiert, potenzielle

Löschrückstände minimiert und Speicherplatz am schnellsten freigibt.

Die Tabelle fasst zusammen, wann StorageGRID welche Methode verwendet.

Methode zum Durchführen des Löschvorgangs	Bei Verwendung
Objekte werden zum Löschen in die Warteschlange gestellt	Wenn **eine** der folgenden Bedingungen zutrifft: • Die automatische Objektlöschung wurde durch eines der folgenden Ereignisse ausgelöst: ◦ Das Ablaufdatum oder die Anzahl der Tage in der Lebenszykluskonfiguration für einen S3-Bucket ist erreicht. ◦ Der letzte in einer ILM-Regel angegebene Zeitraum ist abgelaufen. **Hinweis:** Objekte in einem Bucket mit aktivierter S3-Objektsperre können nicht gelöscht werden, wenn sie einer rechtlichen Sperre unterliegen oder wenn ein Aufbewahrungsdatum angegeben, aber noch nicht erreicht wurde. • Ein S3-Client fordert die Löschung an und eine oder mehrere der folgenden Bedingungen sind erfüllt: ◦ Kopien können nicht innerhalb von 30 Sekunden gelöscht werden, weil beispielsweise ein Objektstandort vorübergehend nicht verfügbar ist. ◦ Hintergrundlöschwarteschlangen sind inaktiv.
Objekte werden sofort entfernt (synchrones Löschen)	Wenn ein S3-Client eine Löschanforderung stellt und **alle** der folgenden Bedingungen erfüllt sind: • Alle Kopien können innerhalb von 30 Sekunden entfernt werden. • Hintergrundlöschwarteschlangen enthalten zu verarbeitende Objekte.

Wenn S3-Clients Löschanforderungen stellen, beginnt StorageGRID damit, Objekte zur Löschwarteschlange hinzuzufügen. Anschließend wird auf die synchrone Löschung umgeschaltet. Indem sichergestellt wird, dass die Löschwarteschlange im Hintergrund über zu verarbeitende Objekte verfügt, kann StorageGRID Löschvorgänge effizienter verarbeiten, insbesondere bei Clients mit geringer Parallelität. Gleichzeitig wird ein Löschrückstau bei Clients vermieden.

Zum Löschen von Objekten erforderliche Zeit

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

- Wenn StorageGRID eine synchrone Löschung durchführt, kann es bis zu 30 Sekunden dauern, bis StorageGRID ein Ergebnis an den Client zurückgibt. Dies bedeutet, dass das Löschen scheinbar langsamer erfolgt, obwohl Kopien tatsächlich schneller entfernt werden, als dies der Fall ist, wenn StorageGRID Objekte zum Löschen in die Warteschlange stellt.
- Wenn Sie die Löschleistung während einer Massenlöschung genau überwachen, stellen Sie möglicherweise fest, dass die Löschrate nach dem Löschen einer bestimmten Anzahl von Objekten langsam zu sein scheint. Diese Änderung tritt ein, wenn StorageGRID von der Warteschlangeneinreihung von Objekten zum Löschen zur synchronen Löschung übergeht. Die scheinbare Verringerung der

Löschrate bedeutet nicht, dass Objektkopien langsamer entfernt werden. Im Gegenteil, es deutet darauf hin, dass im Durchschnitt nun schneller Platz freigegeben wird.

Wenn Sie eine große Anzahl von Objekten löschen und Ihre Priorität darin besteht, schnell Speicherplatz freizugeben, sollten Sie zum Löschen von Objekten eine Clientanforderung verwenden, anstatt sie mit ILM oder anderen Methoden zu löschen. Im Allgemeinen wird Speicherplatz schneller freigegeben, wenn die Löschung durch Clients erfolgt, da StorageGRID synchrones Löschen verwenden kann.

Die zum Freigeben von Speicherplatz nach dem Löschen eines Objekts erforderliche Zeit hängt von mehreren Faktoren ab:

- Ob Objektkopien synchron entfernt oder zur späteren Entfernung in die Warteschlange gestellt werden (für Client-Löschanforderungen).
- Andere Faktoren wie die Anzahl der Objekte im Grid oder die Verfügbarkeit von Grid-Ressourcen, wenn Objektkopien zum Entfernen in die Warteschlange gestellt werden (sowohl für Client-Löschvorgänge als auch für andere Methoden).

So werden versionierte S3-Objekte gelöscht

Wenn die Versionierung für einen S3-Bucket aktiviert ist, folgt StorageGRID beim Antworten auf Löschanforderungen dem Verhalten von Amazon S3, unabhängig davon, ob diese Anforderungen von einem S3-Client, dem Ablauf eines S3-Bucket-Lebenszyklus oder den Anforderungen der ILM-Richtlinie stammen.

Wenn Objekte versioniert sind, löschen Objektlöschanforderungen nicht die aktuelle Version des Objekts und geben keinen Speicherplatz frei. Stattdessen erstellt eine Objektlöschanforderung eine Null-Byte-Löschmarkierung als aktuelle Version des Objekts, wodurch die vorherige Version des Objekts „nicht aktuell“ wird. Eine Objektlöschmarkierung wird zu einer abgelaufenen Objektlöschmarkierung, wenn es sich um die aktuelle Version handelt und keine nicht aktuellen Versionen vorhanden sind.

Obwohl das Objekt nicht entfernt wurde, verhält sich StorageGRID so, als ob die aktuelle Version des Objekts nicht mehr verfügbar wäre. Anfragen an dieses Objekt geben 404 NotFound zurück. Da jedoch nicht aktuelle Objektdaten nicht entfernt wurden, können Anforderungen, die eine nicht aktuelle Version des Objekts angeben, erfolgreich sein.

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

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

  Der `NewerNoncurrentVersions` Die Aktion in der Bucket-Lebenszykluskonfiguration gibt die Anzahl der nicht aktuellen Versionen an, die in einem versionierten S3-Bucket beibehalten werden. Wenn mehr nicht aktuelle Versionen vorhanden sind als `NewerNoncurrentVersions` gibt an, dass StorageGRID die älteren Versionen entfernt, wenn der Wert „NoncurrentDays“ abgelaufen ist. Der `NewerNoncurrentVersions` Schwellenwert überschreibt die von ILM bereitgestellten Lebenszyklusregeln, d. h. ein nicht aktuelles Objekt mit einer Version innerhalb des `NewerNoncurrentVersions` Der Schwellenwert bleibt erhalten, wenn ILM seine Löschung anfordert.

  Um abgelaufene Objektlöschmarkierungen zu entfernen, verwenden Sie die `Expiration` Aktion mit

einem der folgenden Tags: `ExpiredObjectDeleteMarker` , `Days` , oder `Date` .

- **ILM**:"Klonen einer aktiven Richtlinie" und fügen Sie der neuen Richtlinie zwei ILM-Regeln hinzu:
  - Erste Regel: Verwenden Sie „Nicht aktuelle Zeit“ als Referenzzeit, um die nicht aktuellen Versionen des Objekts abzugleichen. In"Schritt 1 (Details eingeben) des Assistenten „ILM-Regel erstellen“" , wählen Sie **Ja** für die Frage „Diese Regel nur auf ältere Objektversionen anwenden (in S3-Buckets mit aktivierter Versionierung)?“
  - Zweite Regel: Verwenden Sie die **Aufnahmezeit**, um sie an die aktuelle Version anzupassen. Die Regel „Nicht aktuelle Zeit“ muss in der Richtlinie über der Regel **Aufnahmezeit** erscheinen.

    Um abgelaufene Objektlöschmarkierungen zu entfernen, verwenden Sie eine **Aufnahmezeit**-Regel, um die aktuellen Löschmarkierungen abzugleichen. Löschmarkierungen werden nur entfernt, wenn ein **Zeitraum** von **Tagen** verstrichen ist und die aktuelle Löschmarkierung abgelaufen ist (es gibt keine nicht aktuellen Versionen).

- **Objekte im Bucket löschen**: Verwenden Sie den Mandantenmanager, um"alle Objektversionen löschen" , einschließlich Löschmarkierungen, aus einem Bucket.

Wenn ein versioniertes Objekt gelöscht wird, erstellt StorageGRID eine Null-Byte-Löschmarkierung als aktuelle Version des Objekts. Alle Objekte und Löschmarkierungen müssen entfernt werden, bevor ein versionierter Bucket gelöscht werden kann.

- In StorageGRID 11.7 oder früher erstellte Löschmarkierungen können nur über S3-Clientanforderungen entfernt werden. Sie werden nicht durch ILM, Bucket-Lebenszyklusregeln oder Löschvorgänge für Objekte in Buckets entfernt.
- Löschmarkierungen aus einem Bucket, der in StorageGRID 11.8 oder höher erstellt wurde, können durch ILM, Bucket-Lebenszyklusregeln, Löschvorgänge für Objekte in Buckets oder eine explizite S3-Client-Löschung entfernt werden.

Ähnliche Informationen

- "Verwenden Sie die S3 REST-API"
- "Beispiel 4: ILM-Regeln und -Richtlinien für versionierte S3-Objekte"

Erstellen und Zuweisen von Speicherklassen

Speicherklassen identifizieren den von einem Speicherknoten verwendeten Speichertyp. Sie können Speicherklassen erstellen, wenn Sie möchten, dass ILM-Regeln bestimmte Objekte auf bestimmten Speicherknoten platzieren.

Bevor Sie beginnen

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

Informationen zu diesem Vorgang

Wenn Sie StorageGRID zum ersten Mal installieren, wird jedem Speicherknoten in Ihrem System automatisch die Speicherklasse **Standard** zugewiesen. Bei Bedarf können Sie optional benutzerdefinierte Speicherklassen definieren und diese verschiedenen Speicherknoten zuweisen.

Durch die Verwendung benutzerdefinierter Speicherklassen können Sie ILM-Speicherpools erstellen, die nur einen bestimmten Typ von Speicherknoten enthalten. Beispielsweise möchten Sie möglicherweise, dass bestimmte Objekte auf Ihren schnellsten Speicherknoten gespeichert werden, wie etwa StorageGRID -All

-Flash-Speichergeräten.

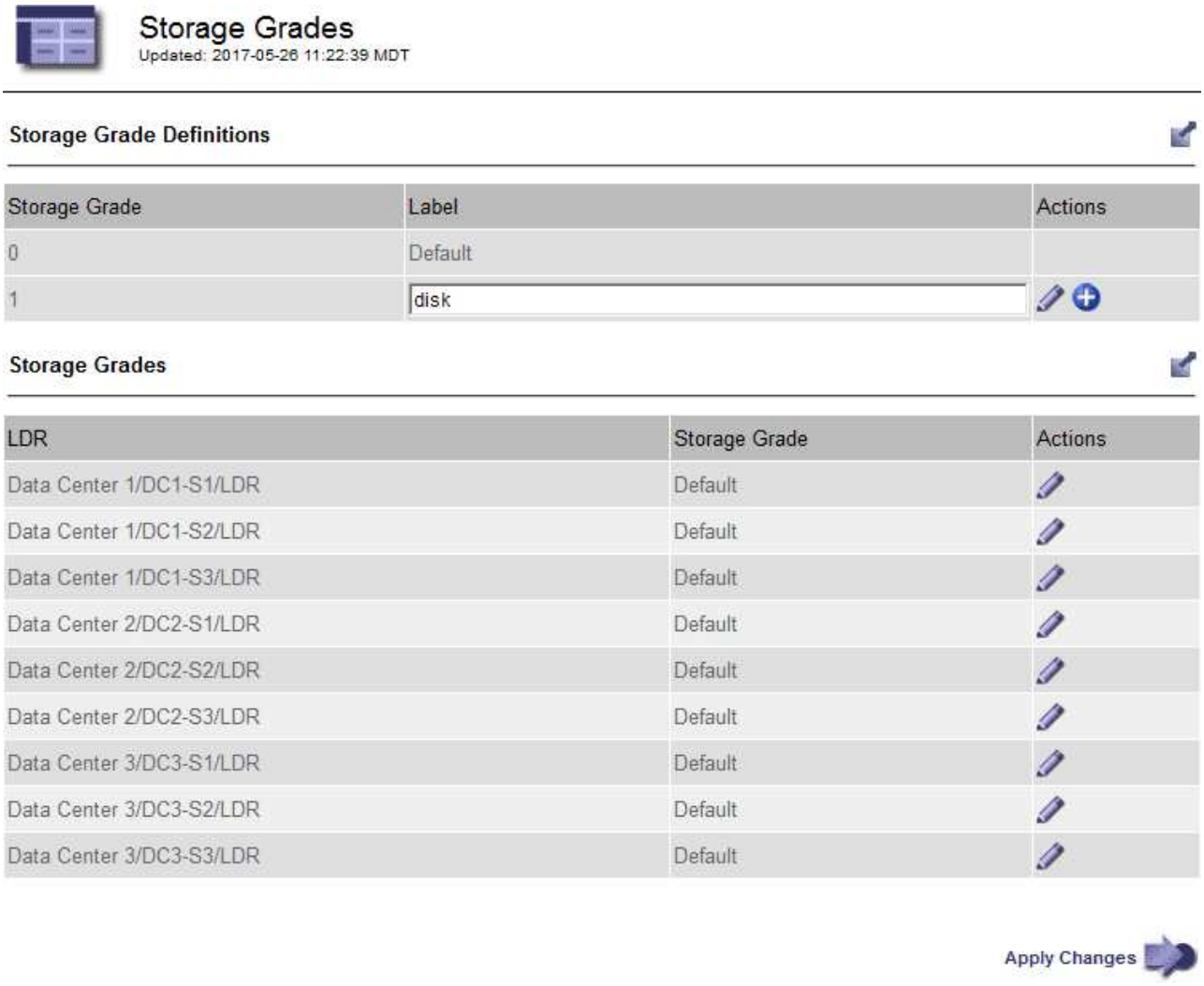
> Speicherknoten können während der Installation so konfiguriert werden, dass sie nur Objektmetadaten und keine Objektdaten enthalten. Nur Metadaten-Speicherknoten kann keine Speicherklasse zugewiesen werden. Weitere Informationen finden Sie unter "Arten von Speicherknoten" .

Wenn die Speicherqualität kein Problem darstellt (z. B. wenn alle Speicherknoten identisch sind), können Sie dieses Verfahren überspringen und die Option **beinhaltet alle Speicherqualitäten** für die Speicherqualität verwenden, wenn Sie"Speicherpools erstellen" . Durch diese Auswahl wird sichergestellt, dass der Speicherpool jeden Speicherknoten am Standort umfasst, unabhängig von seiner Speicherklasse.

> Erstellen Sie nicht mehr Speicherklassen als nötig. Erstellen Sie beispielsweise nicht für jeden Speicherknoten eine eigene Speicherklasse. Weisen Sie stattdessen jeder Speicherklasse zwei oder mehr Knoten zu. Nur einem Knoten zugewiesene Speicherklassen können zu ILM-Rückständen führen, wenn dieser Knoten nicht mehr verfügbar ist.

Schritte

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



c. Wählen Sie **Änderungen übernehmen**.

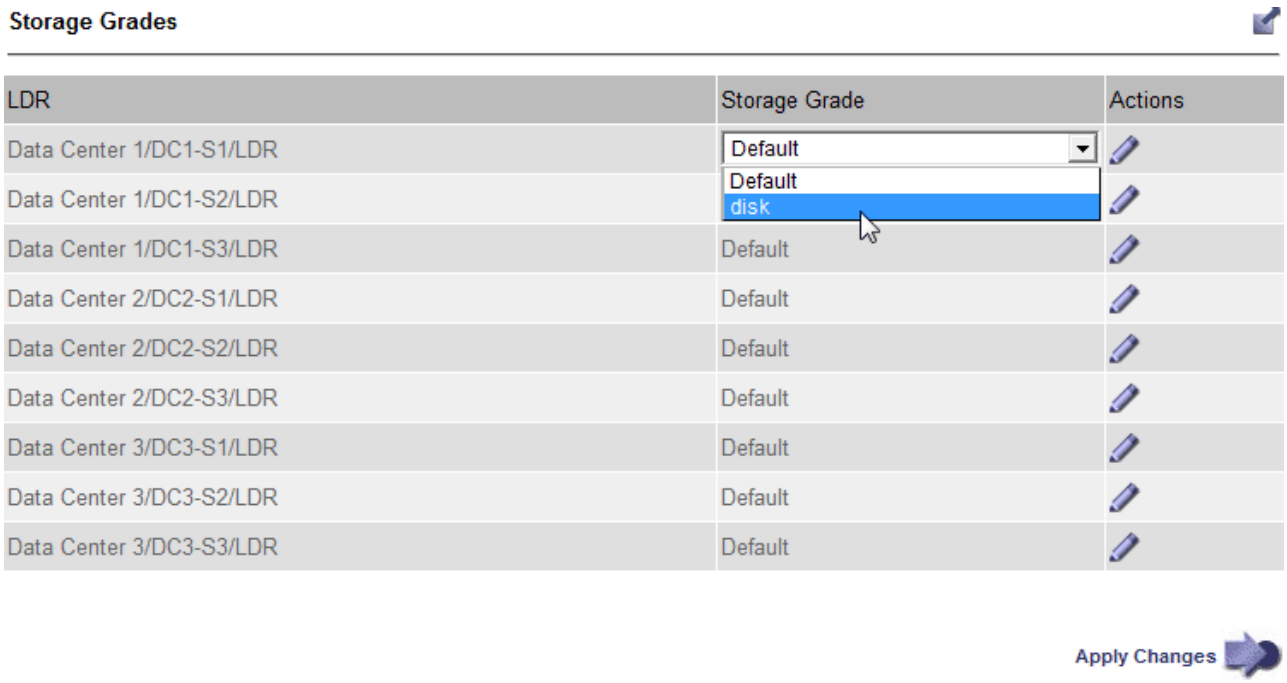
d. Wenn Sie ein gespeichertes Etikett ändern möchten, wählen Sie optional **Bearbeiten*** **und wählen Sie *Änderungen übernehmen**.

Sie können keine Speichergrade löschen.

3. Weisen Sie Speicherknoten neue Speicherklassen zu:

a. Suchen Sie den Speicherknoten in der LDR-Liste und wählen Sie das Symbol *Bearbeiten* .

b. Wählen Sie aus der Liste die entsprechende Speicherklasse aus.



Weisen Sie einem bestimmten Speicherknoten nur einmal eine Speicherklasse zu. Ein nach einem Ausfall wiederhergestellter Speicherknoten behält die zuvor zugewiesene Speicherklasse bei. Ändern Sie diese Zuweisung nicht, nachdem die ILM-Richtlinie aktiviert wurde. Bei einer Änderung der Zuordnung werden die Daten entsprechend der neuen Speicherklasse gespeichert.

a. Wählen Sie **Änderungen übernehmen**.

Verwenden von Speicherpools

Was ist ein Speicherpool?

Ein Speicherpool ist eine logische Gruppierung von Speicherknoten.

Wenn Sie StorageGRID installieren, wird automatisch ein Speicherpool pro Site erstellt. Sie können je nach Bedarf zusätzliche Speicherpools für Ihre Speicheranforderungen konfigurieren.

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

Speicherpools haben zwei Attribute:

- **Speicherqualität**: Bei Speicherknoten die relative Leistung des zugrunde liegenden Speichers.
- **Standort**: Das Rechenzentrum, in dem Objekte gespeichert werden.

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

Richtlinien zum Erstellen von Speicherpools

Konfigurieren und verwenden Sie Speicherpools, um Datenverlust durch die Verteilung der Daten auf mehrere Standorte zu verhindern. Für replizierte Kopien und Erasure-Coded-Kopien sind unterschiedliche Speicherpoolkonfigurationen erforderlich.

Sehen "Beispiele für die Aktivierung des Site-Loss-Schutzes durch Replikation und Erasure Coding" .

Richtlinien für alle Speicherpools

- Halten Sie die Speicherpoolkonfigurationen so einfach wie möglich. Erstellen Sie nicht mehr Speicherpools als nötig.
- Erstellen Sie Speicherpools mit so vielen Knoten wie möglich. Jeder Speicherpool sollte zwei oder mehr Knoten enthalten. Ein Speicherpool mit unzureichenden Knoten kann zu ILM-Rückständen führen, wenn ein Knoten nicht mehr verfügbar ist.
- Vermeiden Sie das Erstellen oder Verwenden von Speicherpools, die sich überschneiden (einen oder mehrere gleiche Knoten enthalten). Wenn sich Speicherpools überschneiden, kann es sein, dass mehrere Kopien der Objektdaten auf demselben Knoten gespeichert werden.
- Verwenden Sie im Allgemeinen nicht den Speicherpool „Alle Speicherknoten“ (StorageGRID 11.6 und früher) oder die Site „Alle Sites“. Diese Elemente werden automatisch aktualisiert, um alle neuen Sites einzuschließen, die Sie in einer Erweiterung hinzufügen. Dies entspricht möglicherweise nicht dem gewünschten Verhalten.

Richtlinien für Speicherpools, die für replizierte Kopien verwendet werden

- Zum Schutz vor Site-Loss mit"Replikation" , geben Sie einen oder mehrere standortspezifische Speicherpools in der"Platzierungsanweisungen für jede ILM-Regel" .

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

  Durch die Verwendung eines Speicherpools für jeden Standort wird sichergestellt, dass replizierte Objektkopien genau dort abgelegt werden, wo Sie es erwarten (z. B. eine Kopie jedes Objekts an jedem Standort zum Schutz vor Standortverlust).

- Wenn Sie in einer Erweiterung eine Site hinzufügen, erstellen Sie einen neuen Speicherpool, der nur die neue Site enthält. Dann,"ILM-Regeln aktualisieren" um zu steuern, welche Objekte auf der neuen Site gespeichert werden.
- Wenn die Anzahl der Kopien geringer ist als die Anzahl der Speicherpools, verteilt das System die Kopien, um die Festplattennutzung gleichmäßig auf die Pools zu verteilen.
- Wenn sich die Speicherpools überschneiden (dieselben Speicherknoten enthalten), werden alle Kopien des Objekts möglicherweise nur an einem Standort gespeichert. Sie müssen sicherstellen, dass die ausgewählten Speicherpools nicht dieselben Speicherknoten enthalten.

Richtlinien für Speicherpools, die für Erasure-Coded-Kopien verwendet werden

- Zum Schutz vor Site-Loss mit"Löschcodierung" , erstellen Sie Speicherpools, die aus mindestens drei Sites bestehen. Wenn ein Speicherpool nur zwei Standorte umfasst, können Sie diesen Speicherpool nicht für Erasure Coding verwenden. Für einen Speicherpool mit zwei Standorten sind keine Erasure-Coding-Schemata verfügbar.
- Die Anzahl der im Speicherpool enthaltenen Speicherknoten und Sites bestimmt, welche"Erasure-Coding-Schemata" sind verfügbar.

- Wenn möglich, sollte ein Speicherpool mehr als die Mindestanzahl an Speicherknoten enthalten, die für das von Ihnen ausgewählte Erasure-Coding-Schema erforderlich sind. Wenn Sie beispielsweise ein 6+3-Erasure-Coding-Schema verwenden, müssen Sie über mindestens neun Speicherknoten verfügen. Es wird jedoch empfohlen, mindestens einen zusätzlichen Speicherknoten pro Site zu haben.
- Verteilen Sie die Speicherknoten so gleichmäßig wie möglich auf die Standorte. Um beispielsweise ein 6+3-Erasure-Coding-Schema zu unterstützen, konfigurieren Sie einen Speicherpool, der mindestens drei Speicherknoten an drei Standorten umfasst.
- Wenn Sie hohe Durchsatzanforderungen haben, wird die Verwendung eines Speicherpools mit mehreren Sites nicht empfohlen, wenn die Netzwerklatenz zwischen den Sites größer als 100 ms ist. Mit zunehmender Latenz nimmt die Rate, mit der StorageGRID Objektfragmente erstellen, platzieren und abrufen kann, aufgrund des geringeren TCP-Netzwerkdurchsatzes stark ab.

  Die Verringerung des Durchsatzes wirkt sich auf die maximal erreichbaren Raten der Objektaufnahme und des Objektabrufs aus (wenn „Balanced“ oder „Strict“ als Aufnahmeverhalten ausgewählt ist) oder kann zu Rückständen in der ILM-Warteschlange führen (wenn „Dual Commit“ als Aufnahmeverhalten ausgewählt ist). Sehen "ILM-Regelaufnahmeverhalten" .

> Wenn Ihr Grid nur eine Site umfasst, können Sie den Speicherpool „Alle Speicherknoten“ (StorageGRID 11.6 und früher) oder die Site „Alle Sites“ in einem Erasure-Coding-Profil nicht verwenden. Dieses Verhalten verhindert, dass das Profil ungültig wird, wenn eine zweite Site hinzugefügt wird.

Aktivieren Sie den Site-Loss-Schutz

Wenn Ihre StorageGRID Bereitstellung mehr als einen Standort umfasst, können Sie Replikation und Erasure Coding mit entsprechend konfigurierten Speicherpools verwenden, um einen Schutz vor Standortverlust zu aktivieren.

Replikation und Erasure Coding erfordern unterschiedliche Speicherpoolkonfigurationen:

- Um die Replikation zum Schutz vor Site-Verlust zu nutzen, verwenden Sie die standortspezifischen Speicherpools, die während der StorageGRID -Installation automatisch erstellt werden. Erstellen Sie anschließend ILM-Regeln mit"Platzierungsanweisungen" die mehrere Speicherpools angeben, sodass an jedem Standort eine Kopie jedes Objekts abgelegt wird.
- Um Erasure Coding zum Schutz vor Site-Loss zu verwenden,"Erstellen Sie Speicherpools, die aus mehreren Sites bestehen" . Erstellen Sie dann ILM-Regeln, die einen Speicherpool verwenden, der aus mehreren Sites und allen verfügbaren Erasure-Coding-Schemata besteht.

> Bei der Konfiguration Ihrer StorageGRID -Bereitstellung für den Site-Loss-Schutz müssen Sie auch die Auswirkungen von"Aufnahmeoptionen" Und"Konsistenz" .

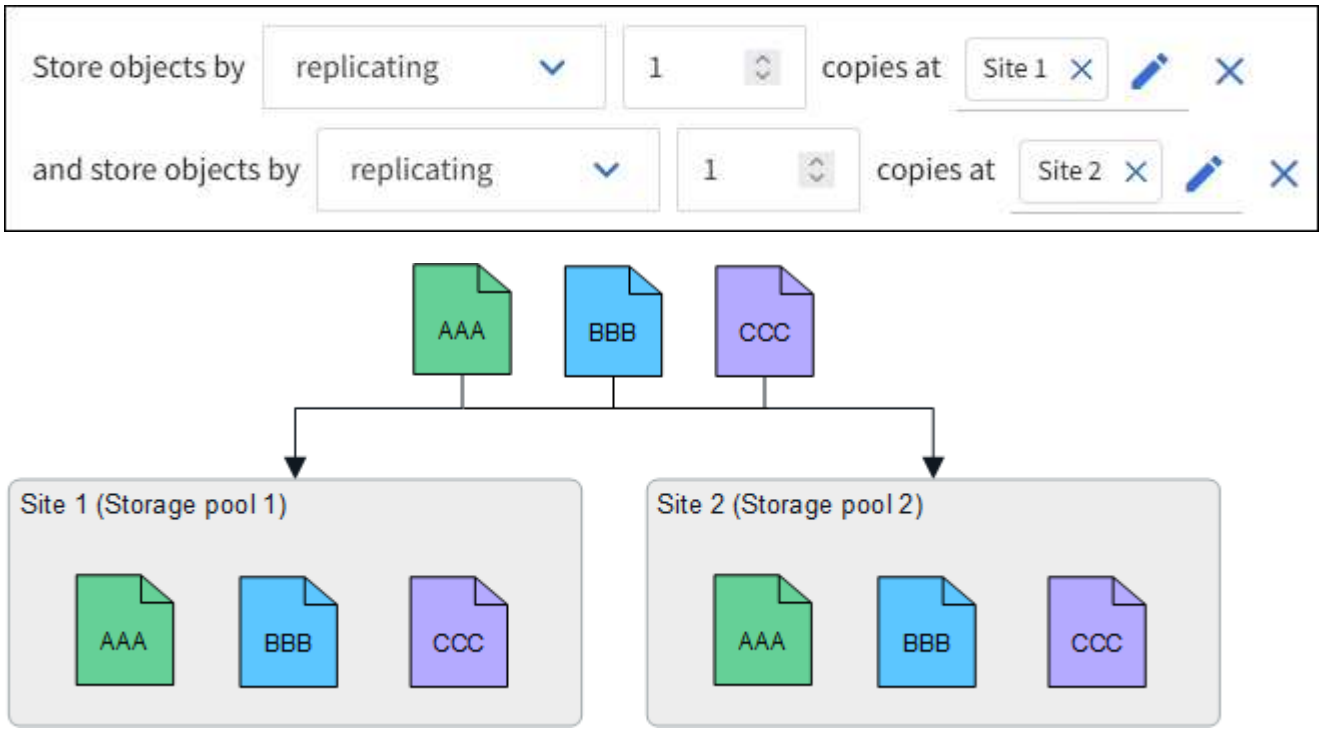
Replikationsbeispiel

Standardmäßig wird während der StorageGRID -Installation für jede Site ein Speicherpool erstellt. Wenn Sie über Speicherpools verfügen, die nur aus einem Standort bestehen, können Sie ILM-Regeln konfigurieren, die zum Schutz vor Standortverlust die Replikation verwenden. In diesem Beispiel:

- Speicherpool 1 enthält Standort 1
- Speicherpool 2 enthält Standort 2
- Die ILM-Regel enthält zwei Platzierungen:

- Speichern Sie Objekte, indem Sie 1 Kopie an Standort 1 replizieren
- Speichern Sie Objekte, indem Sie 1 Kopie an Standort 2 replizieren

ILM-Regelplatzierungen:



Bei Verlust eines Standorts sind Kopien der Objekte am anderen Standort verfügbar.

Beispiel für Erasure Coding

Wenn Sie über Speicherpools verfügen, die aus mehr als einem Standort pro Speicherpool bestehen, können Sie ILM-Regeln konfigurieren, die Erasure Coding zum Schutz vor Standortverlust verwenden. In diesem Beispiel:

- Speicherpool 1 enthält die Standorte 1 bis 3
- Die ILM-Regel enthält eine Platzierung: Speichern Sie Objekte durch Erasure Coding mit einem 4+2 EC-Schema im Speicherpool 1, der drei Standorte enthält

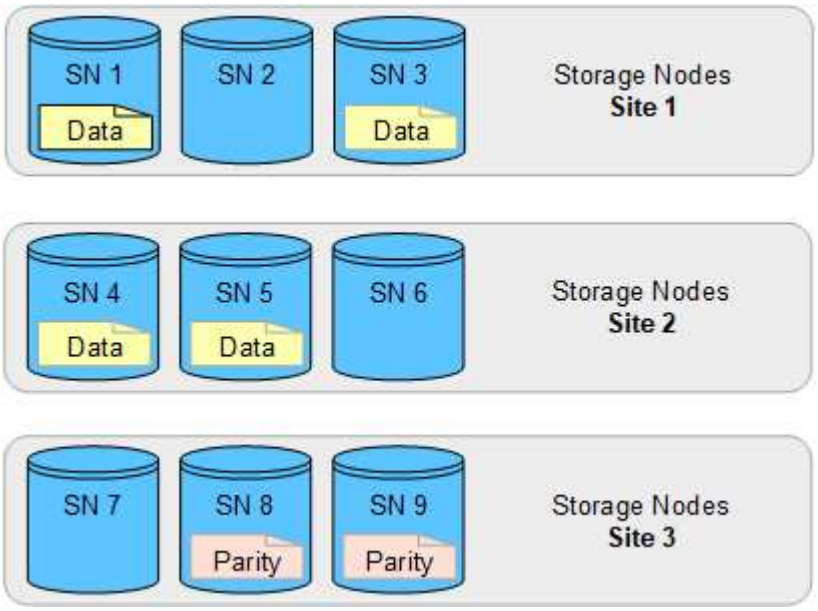
ILM-Regelplatzierungen:

In diesem Beispiel:

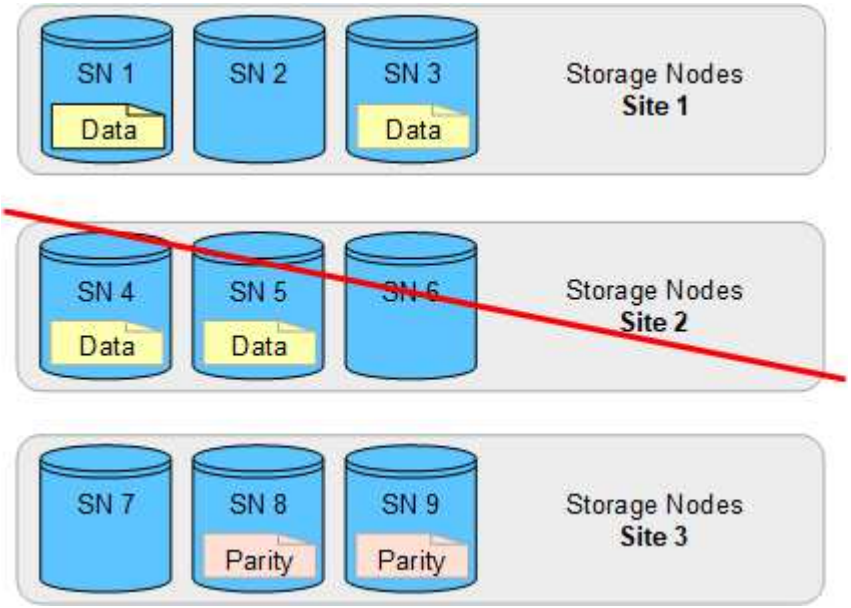
- Die ILM-Regel verwendet ein 4+2-Erasure-Coding-Schema.
- Jedes Objekt wird in vier gleiche Datenfragmente aufgeteilt und aus den Objektdaten werden zwei Paritätsfragmente berechnet.
- Jedes der sechs Fragmente wird auf einem anderen Knoten an drei Rechenzentrumsstandorten gespeichert, um Datenschutz bei Knotenausfällen oder Standortverlust zu gewährleisten.

Erasure Coding ist in Speicherpools zulässig, die eine beliebige Anzahl von Standorten enthalten, *außer* zwei Standorten.

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



Wenn eine Site verloren geht, können die Daten dennoch wiederhergestellt werden:



Erstellen eines Speicherpools

Sie erstellen Speicherpools, um zu bestimmen, wo das StorageGRID -System Objektdaten speichert und welche Art von Speicher verwendet wird. Jeder Speicherpool umfasst einen oder mehrere Standorte und eine oder mehrere Speicherklassen.

Wenn Sie StorageGRID 11.9 auf einem neuen Grid installieren, werden für jeden Standort automatisch Speicherpools erstellt. Wenn Sie jedoch StorageGRID 11.6 oder früher ursprünglich installiert haben, werden Speicherpools nicht automatisch für jede Site erstellt.

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

Bevor Sie beginnen

- Sie sind beim Grid Manager angemeldet mit einem"unterstützter Webbrowser" .
- Du hast"spezifische Zugriffsberechtigungen" .
- Sie haben die Richtlinien zum Erstellen von Speicherpools gelesen.

Informationen zu diesem Vorgang

Speicherpools bestimmen, wo Objektdaten gespeichert werden. Die Anzahl der benötigten Speicherpools hängt von der Anzahl der Sites in Ihrem Grid und von den gewünschten Kopietypen ab: repliziert oder erasure-coded.

- Erstellen Sie für die Replikation und die Erasure Coding-Funktion für einzelne Standorte einen Speicherpool für jeden Standort. Wenn Sie beispielsweise replizierte Objektkopien an drei Standorten speichern möchten, erstellen Sie drei Speicherpools.
- Erstellen Sie für die Erasure Coding-Funktion an drei oder mehr Standorten einen Speicherpool, der für jeden Standort einen Eintrag enthält. Wenn Sie beispielsweise Erasure-Code-Objekte an drei Standorten verwalten möchten, erstellen Sie einen Speicherpool.

> Schließen Sie die Site „Alle Sites“ nicht in einen Speicherpool ein, der in einem Erasure-Coding-Profil verwendet wird. Fügen Sie stattdessen für jede Site, in der löschcodierte Daten gespeichert werden, einen separaten Eintrag zum Speicherpool hinzu. Sehendieser Schritt für ein Beispiel.

- Wenn Sie über mehr als eine Speicherklasse verfügen, erstellen Sie keinen Speicherpool, der verschiedene Speicherklassen an einem einzigen Standort umfasst. Siehe die"Richtlinien zum Erstellen von Speicherpools" .

Schritte

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

   Auf der Registerkarte „Speicherpools“ werden alle definierten Speicherpools aufgelistet.

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

2. Um einen neuen Speicherpool zu erstellen, wählen Sie **Erstellen**.
3. Geben Sie einen eindeutigen Namen für den Speicherpool ein. Verwenden Sie einen Namen, der beim Konfigurieren von Erasure-Coding-Profilen und ILM-Regeln leicht zu identifizieren ist.
4. Wählen Sie aus der Dropdown-Liste **Site** eine Site für diesen Speicherpool aus.

   Wenn Sie eine Site auswählen, wird die Anzahl der Speicherknoten in der Tabelle automatisch aktualisiert.

   Verwenden Sie die Site „Alle Sites“ grundsätzlich nicht in einem Speicherpool. ILM-Regeln, die einen All-Sites-Speicherpool verwenden, platzieren Objekte an jedem verfügbaren Standort, wodurch Sie weniger Kontrolle über die Objektplatzierung haben. Außerdem verwendet ein All-Sites-Speicherpool die Speicherknoten an einem neuen Standort sofort, was möglicherweise nicht dem von Ihnen erwarteten Verhalten entspricht.

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

   Die Speicherklasse, *umfasst alle Speicherklassen*, umfasst alle Speicherknoten am ausgewählten Standort. Wenn Sie zusätzliche Speicherklassen für die Speicherknoten in Ihrem Raster erstellt haben, werden diese in der Dropdown-Liste aufgeführt.

6. Wenn Sie den Speicherpool in einem Erasure-Coding-Profil für mehrere Sites verwenden möchten, wählen Sie **Weitere Knoten hinzufügen**, um dem Speicherpool für jede Site einen Eintrag hinzuzufügen.

   > Sie werden gewarnt, wenn Sie für eine Site mehr als einen Eintrag mit unterschiedlichen Speicherklassen hinzufügen.

   Um einen Eintrag zu entfernen, wählen Sie das Löschsymbol ✕ .

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

   Der neue Speicherpool wird der Liste hinzugefügt.

Anzeigen von Speicherpooldetails

Sie können die Details eines Speicherpools anzeigen, um festzustellen, wo der Speicherpool verwendet wird und welche Knoten und Speicherklassen enthalten sind.

Bevor Sie beginnen

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

Schritte

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

   Die Tabelle „Speicherpools“ enthält die folgenden Informationen für jeden Speicherpool, der Speicherknoten enthält:

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

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

   Die Detailseite für den Speicherpool wird angezeigt.

3. Sehen Sie sich die Registerkarte **Knoten** an, um mehr über die im Speicherpool enthaltenen Speicherknoten zu erfahren.

   Die Tabelle enthält für jeden Knoten die folgenden Informationen:

- Knotenname
- Sitename
- Lagerqualität
- Speichernutzung: Der Prozentsatz des gesamten nutzbaren Speicherplatzes für Objektdaten, der für den Speicherknoten verwendet wurde.

> Derselbe Wert für die Speichernutzung (%) wird auch im Diagramm „Speichernutzung – Objektdaten“ für jeden Speicherknoten angezeigt (wählen Sie **KNOTEN** > ***Speicherknoten*** > **Speicher**).

4. Sehen Sie sich die Registerkarte **ILM-Nutzung** an, um festzustellen, ob der Speicherpool derzeit in ILM-Regeln oder Erasure-Coding-Profilen verwendet wird.
5. Optional können Sie auf die **ILM-Regelseite** gehen, um mehr über die Regeln zu erfahren und diese zu verwalten, die den Speicherpool verwenden.

   Siehe die"Anleitung zum Arbeiten mit ILM-Regeln" .

Speicherpool bearbeiten

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

Bevor Sie beginnen

- Sie sind beim Grid Manager angemeldet mit einem"unterstützter Webbrowser" .
- Du hast"spezifische Zugriffsberechtigungen" .
- Sie haben die"Richtlinien zum Erstellen von Speicherpools" .
- Wenn Sie einen Speicherpool bearbeiten möchten, der von einer Regel in der aktiven ILM-Richtlinie verwendet wird, haben Sie berücksichtigt, wie sich Ihre Änderungen auf die Platzierung der Objektdaten auswirken.

Informationen zu diesem Vorgang

Wenn Sie einem Speicherpool, der in der aktiven ILM-Richtlinie verwendet wird, einen neuen Standort oder eine neue Speicherklasse hinzufügen, beachten Sie, dass die Speicherknoten am neuen Standort oder in der neuen Speicherklasse nicht automatisch verwendet werden. Um StorageGRID zur Verwendung einer neuen Site oder Speicherklasse zu zwingen, müssen Sie nach dem Speichern des bearbeiteten Speicherpools eine neue ILM-Richtlinie aktivieren.

Schritte

1. Wählen Sie **ILM** > **Speicherpools**.
2. Aktivieren Sie das Kontrollkästchen für den Speicherpool, den Sie bearbeiten möchten.

   Sie können den Speicherpool „Alle Speicherknoten“ (StorageGRID 11.6 und früher) nicht bearbeiten.

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

   Sie können den Standort oder die Speicherklasse nicht ändern, wenn der Speicherpool in einem Erasure-

Coding-Profil verwendet wird und die Änderung dazu führen würde, dass das Erasure-Coding-Schema ungültig wird. Wenn beispielsweise ein in einem Erasure-Coding-Profil verwendeter Speicherpool derzeit eine Speicherklasse mit nur einem Standort enthält, können Sie keine Speicherklasse mit zwei Standorten verwenden, da die Änderung das Erasure-Coding-Schema ungültig machen würde.

> Durch das Hinzufügen oder Entfernen von Sites aus einem vorhandenen Speicherpool werden keine vorhandenen, löschcodierten Daten verschoben. Wenn Sie die vorhandenen Daten von der Site verschieben möchten, müssen Sie einen neuen Speicherpool und ein neues EC-Profil erstellen, um die Daten neu zu kodieren.

6. Wählen Sie **Speichern**.

Nach Abschluss

Wenn Sie einem in der aktiven ILM-Richtlinie verwendeten Speicherpool eine neue Site oder Speicherklasse hinzugefügt haben, aktivieren Sie eine neue ILM-Richtlinie, um StorageGRID zur Verwendung der neuen Site oder Speicherklasse zu zwingen. Klonen Sie beispielsweise Ihre vorhandene ILM-Richtlinie und aktivieren Sie dann den Klon. Sehen "Arbeiten mit ILM-Regeln und ILM-Richtlinien" .

Entfernen eines Speicherpools

Sie können einen Speicherpool entfernen, der nicht verwendet wird.

Bevor Sie beginnen

- Sie sind beim Grid Manager angemeldet mit einem"unterstützter Webbrowser" .
- Sie haben die"erforderliche Zugriffsberechtigungen" .

Schritte

1. Wählen Sie **ILM** > **Speicherpools**.
2. Sehen Sie sich die Spalte „ILM-Nutzung“ in der Tabelle an, um festzustellen, ob Sie den Speicherpool entfernen können.

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

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

Verwenden Sie Cloud-Speicherpools

Was ist ein Cloud-Speicherpool?

Mit einem Cloud-Speicherpool können Sie mithilfe von ILM Objektdaten außerhalb Ihres StorageGRID Systems verschieben. Beispielsweise möchten Sie möglicherweise selten aufgerufene Objekte in einen kostengünstigeren Cloud-Speicher verschieben, etwa Amazon S3 Glacier, S3 Glacier Deep Archive, Google Cloud oder die Archivzugriffsebene im Microsoft Azure Blob-Speicher. Oder Sie möchten möglicherweise ein Cloud-Backup

von StorageGRID -Objekten verwalten, um die Notfallwiederherstellung zu verbessern.

Aus ILM-Sicht ähnelt ein Cloud-Speicherpool einem Speicherpool. Um Objekte an einem der beiden Speicherorte zu speichern, wählen Sie den Pool aus, wenn Sie die Platzierungsanweisungen für eine ILM-Regel erstellen. Während Speicherpools jedoch aus Speicherknoten innerhalb des StorageGRID Systems bestehen, besteht ein Cloud-Speicherpool aus einem externen Bucket (S3) oder Container (Azure Blob-Speicher).

Die Tabelle vergleicht Speicherpools mit Cloud-Speicherpools und zeigt die allgemeinen Ähnlichkeiten und Unterschiede.

	Speicherpool	**Cloud-Speicherpool**
Wie entsteht es?	Verwenden Sie die Option **ILM** > **Speicherpools** im Grid Manager.	Verwenden Sie die Option **ILM** > **Speicherpools** > **Cloud-Speicherpools** im Grid Manager. Sie müssen den externen Bucket oder Container einrichten, bevor Sie den Cloud Storage Pool erstellen können.
Wie viele Pools können Sie erstellen?	Unbegrenzt.	Bis zu 10.
Wo werden Objekte gespeichert ?	Auf einem oder mehreren Speicherknoten innerhalb von StorageGRID.	In einem Amazon S3-Bucket, Azure Blob-Speichercontainer oder Google Cloud, der sich außerhalb des StorageGRID Systems befindet. Wenn der Cloud Storage Pool ein Amazon S3-Bucket ist: • Sie können optional einen Bucket-Lebenszyklus konfigurieren, um Objekte in einen kostengünstigen Langzeitspeicher wie Amazon S3 Glacier oder S3 Glacier Deep Archive zu verschieben. Das externe Speichersystem muss die Glacier-Speicherklasse und die S3 RestoreObject-API unterstützen. • Sie können Cloud-Speicherpools zur Verwendung mit AWS Commercial Cloud Services (C2S) erstellen, die die AWS Secret Region unterstützen. Wenn es sich bei dem Cloud-Speicherpool um einen Azure Blob-Speichercontainer handelt, überträgt StorageGRID das Objekt in die Archivebene. **Hinweis:** Konfigurieren Sie die Lebenszyklusverwaltung des Azure Blob-Speichers grundsätzlich nicht für den Container, der für einen Cloud-Speicherpool verwendet wird. RestoreObject-Vorgänge für Objekte im Cloud-Speicherpool können durch den konfigurierten Lebenszyklus beeinflusst werden.

	Speicherpool	Cloud-Speicherpool
Was steuert die Objektplatzierung?	Eine ILM-Regel in den aktiven ILM-Richtlinien.	Eine ILM-Regel in den aktiven ILM-Richtlinien.
Welche Datenschutzmethode wird verwendet?	Replikation oder Erasure Coding.	Replikation.
Wie viele Kopien jedes Objekts sind zulässig?	Mehrere.	Eine Kopie im Cloud Storage Pool und optional eine oder mehrere Kopien in StorageGRID. **Hinweis:** Sie können ein Objekt nicht gleichzeitig in mehr als einem Cloud-Speicherpool speichern.
Was sind die Vorteile?	Objekte sind jederzeit schnell zugänglich.	Kostengünstige Lagerung. **Hinweis**: FabricPool Daten können nicht in Cloud-Speicherpools gestaffelt werden.

Lebenszyklus eines Cloud Storage Pool-Objekts

Überprüfen Sie vor der Implementierung von Cloud-Speicherpools den Lebenszyklus der Objekte, die in den einzelnen Arten von Cloud-Speicherpools gespeichert sind.

S3: Lebenszyklus eines Cloud Storage Pool-Objekts

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

> „Glacier“ bezieht sich sowohl auf die Speicherklasse Glacier als auch auf die Speicherklasse Glacier Deep Archive, mit einer Ausnahme: Die Speicherklasse Glacier Deep Archive unterstützt die Ebene „Expedited Restore“ nicht. Es wird nur der Massen- oder Standardabruf unterstützt.

> Die Google Cloud Platform (GCP) unterstützt das Abrufen von Objekten aus dem Langzeitspeicher, ohne dass ein POST-Wiederherstellungsvorgang erforderlich ist.

1. *Objekt in StorageGRID gespeichert *

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

2. **Objekt in S3 Cloud Storage Pool verschoben**
   - Wenn das Objekt einer ILM-Regel entspricht, die einen S3-Cloud-Speicherpool als Speicherort verwendet, verschiebt StorageGRID das Objekt in den vom Cloud-Speicherpool angegebenen externen S3-Bucket.

- Wenn das Objekt in den S3 Cloud Storage Pool verschoben wurde, kann die Clientanwendung es mithilfe einer S3 GetObject-Anforderung von StorageGRID abrufen, es sei denn, das Objekt wurde in den Glacier-Speicher verschoben.

3. **Objekt in Glacier überführt (nicht abrufbarer Zustand)**
   - Optional kann das Objekt in den Glacier-Speicher übertragen werden. Beispielsweise kann der externe S3-Bucket die Lebenszykluskonfiguration verwenden, um ein Objekt sofort oder nach einer bestimmten Anzahl von Tagen in den Glacier-Speicher zu übertragen.

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

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

   Wenn ein Objekt in den Glacier-Speicher verschoben wurde, kann die Clientanwendung eine S3 RestoreObject-Anforderung ausgeben, um eine abrufbare Kopie im S3 Cloud Storage Pool wiederherzustellen. Die Anforderung gibt an, wie viele Tage die Kopie im Cloud-Speicherpool verfügbar sein soll und welche Datenzugriffsebene für den Wiederherstellungsvorgang verwendet werden soll (Beschleunigt, Standard oder Massen). Wenn das Ablaufdatum der abrufbaren Kopie erreicht ist, wird die Kopie automatisch in einen nicht abrufbaren Zustand zurückversetzt.

   Wenn eine oder mehrere Kopien des Objekts auch auf Speicherknoten innerhalb von StorageGRID vorhanden sind, ist es nicht erforderlich, das Objekt durch Ausgeben einer RestoreObject-Anforderung aus Glacier wiederherzustellen. Stattdessen kann die lokale Kopie direkt mithilfe einer GetObject-Anforderung abgerufen werden.

5. **Objekt abgerufen**

   Sobald ein Objekt wiederhergestellt wurde, kann die Clientanwendung eine GetObject-Anforderung ausgeben, um das wiederhergestellte Objekt abzurufen.

Azure: Lebenszyklus eines Cloud Storage Pool-Objekts

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

1. *Objekt in StorageGRID gespeichert *

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

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

   Wenn das Objekt einer ILM-Regel entspricht, die einen Azure Cloud Storage Pool als Speicherort verwendet, verschiebt StorageGRID das Objekt in den vom Cloud Storage Pool angegebenen externen Azure Blob-Speichercontainer.

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

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

4. **Objekt aus Archivebene wiederhergestellt**

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

   Wenn StorageGRID das RestoreObject empfängt, überträgt es das Objekt vorübergehend in die Cool-Ebene des Azure Blob-Speichers. Sobald das Ablaufdatum in der RestoreObject-Anforderung erreicht ist, überträgt StorageGRID das Objekt zurück in die Archivebene.

   > ⓘ Wenn eine oder mehrere Kopien des Objekts auch auf Speicherknoten innerhalb von StorageGRID vorhanden sind, ist es nicht erforderlich, das Objekt durch Ausgeben einer RestoreObject-Anforderung aus der Archivzugriffsebene wiederherzustellen. Stattdessen kann die lokale Kopie direkt mithilfe einer GetObject-Anforderung abgerufen werden.

5. **Objekt abgerufen**

   Sobald ein Objekt im Azure Cloud Storage Pool wiederhergestellt wurde, kann die Clientanwendung eine GetObject-Anforderung ausgeben, um das wiederhergestellte Objekt abzurufen.

Ähnliche Informationen

"Verwenden Sie die S3 REST-API"

Wann Sie Cloud-Speicherpools verwenden sollten

Mithilfe von Cloud-Speicherpools können Sie Daten an einem externen Speicherort sichern oder stufenweise speichern. Darüber hinaus können Sie Daten in mehr als einer Cloud sichern oder stufenweise speichern.

Sichern Sie StorageGRID Daten an einem externen Speicherort

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

Wenn auf die Kopien in StorageGRID nicht zugegriffen werden kann, können die Objektdaten im Cloud Storage Pool zum Bearbeiten von Clientanforderungen verwendet werden. Möglicherweise müssen Sie jedoch eine S3 RestoreObject-Anforderung stellen, um auf die Sicherungsobjektkopie im Cloud-Speicherpool zuzugreifen.

Die Objektdaten in einem Cloud-Speicherpool können auch verwendet werden, um Daten wiederherzustellen, die aufgrund eines Speichervolumes oder Speicherknotenausfalls aus StorageGRID verloren gegangen sind. Wenn sich die einzige verbleibende Kopie eines Objekts in einem Cloud-Speicherpool befindet, stellt StorageGRID das Objekt vorübergehend wieder her und erstellt eine neue Kopie auf dem wiederhergestellten Speicherknoten.

So implementieren Sie eine Backup-Lösung:

1. Erstellen Sie einen einzelnen Cloud-Speicherpool.
2. Konfigurieren Sie eine ILM-Regel, die gleichzeitig Objektkopien auf Speicherknoten (als replizierte oder erasure-coded Kopien) und eine einzelne Objektkopie im Cloud-Speicherpool speichert.
3. Fügen Sie die Regel zu Ihrer ILM-Richtlinie hinzu. Simulieren und aktivieren Sie dann die Richtlinie.

Daten von StorageGRID an einen externen Speicherort verschieben

Sie können einen Cloud-Speicherpool verwenden, um Objekte außerhalb des StorageGRID Systems zu speichern. Nehmen wir beispielsweise an, Sie müssen eine große Anzahl von Objekten aufbewahren, rechnen aber damit, dass Sie nur selten oder nie auf diese Objekte zugreifen werden. Sie können einen Cloud-Speicherpool verwenden, um die Objekte auf kostengünstigeren Speicher zu verschieben und Speicherplatz in StorageGRID freizugeben.

So implementieren Sie eine Tiering-Lösung:

1. Erstellen Sie einen einzelnen Cloud-Speicherpool.
2. Konfigurieren Sie eine ILM-Regel, die selten verwendete Objekte von Speicherknoten in den Cloud-Speicherpool verschiebt.
3. Fügen Sie die Regel zu Ihrer ILM-Richtlinie hinzu. Simulieren und aktivieren Sie dann die Richtlinie.

Verwalten Sie mehrere Cloud-Endpunkte

Sie können mehrere Cloud Storage Pool-Endpunkte konfigurieren, wenn Sie Objektdaten in mehreren Clouds schichten oder sichern möchten. Mit den Filtern in Ihren ILM-Regeln können Sie angeben, welche Objekte in jedem Cloud-Speicherpool gespeichert werden. Beispielsweise möchten Sie möglicherweise Objekte einiger Mandanten oder Buckets in Amazon S3 Glacier und Objekte anderer Mandanten oder Buckets im Azure Blob-Speicher speichern. Oder Sie möchten Daten zwischen Amazon S3 Glacier und Azure Blob Storage verschieben.

> Wenn Sie mehrere Cloud Storage Pool-Endpunkte verwenden, beachten Sie, dass ein Objekt jeweils nur in einem Cloud Storage Pool gespeichert werden kann.

So implementieren Sie mehrere Cloud-Endpunkte:

1. Erstellen Sie bis zu 10 Cloud-Speicherpools.
2. Konfigurieren Sie ILM-Regeln, um die entsprechenden Objektdaten zum entsprechenden Zeitpunkt in jedem Cloud-Speicherpool zu speichern. Speichern Sie beispielsweise Objekte aus Bucket A in Cloud Storage Pool A und Objekte aus Bucket B in Cloud Storage Pool B. Oder speichern Sie Objekte für eine gewisse Zeit in Cloud Storage Pool A und verschieben Sie sie dann in Cloud Storage Pool B.
3. Fügen Sie die Regeln zu Ihrer ILM-Richtlinie hinzu. Simulieren und aktivieren Sie dann die Richtlinie.

Überlegungen zu Cloud-Speicherpools

Wenn Sie planen, einen Cloud-Speicherpool zum Verschieben von Objekten aus dem StorageGRID System zu verwenden, müssen Sie die Überlegungen zur Konfiguration und Verwendung von Cloud-Speicherpools überprüfen.

Allgemeine Überlegungen

- Im Allgemeinen ist Cloud-Archivspeicher wie Amazon S3 Glacier oder Azure Blob Storage ein kostengünstiger Ort zum Speichern von Objektdaten. Allerdings sind die Kosten für den Abruf von Daten aus Cloud-Archivspeichern relativ hoch. Um die Gesamtkosten so gering wie möglich zu halten, müssen Sie berücksichtigen, wann und wie oft Sie auf die Objekte im Cloud-Speicherpool zugreifen. Die Verwendung eines Cloud-Speicherpools wird nur für Inhalte empfohlen, auf die Sie voraussichtlich nur selten zugreifen.
- Die Verwendung von Cloud Storage Pools mit FabricPool wird aufgrund der zusätzlichen Latenz beim

Abrufen eines Objekts vom Cloud Storage Pool-Ziel nicht unterstützt.

- Objekte mit aktivierter S3-Objektsperre können nicht in Cloud-Speicherpools platziert werden.
- Wenn für den Ziel-S3-Bucket eines Cloud Storage Pools die S3-Objektsperre aktiviert ist, schlägt der Versuch, die Bucket-Replikation (PutBucketReplication) zu konfigurieren, mit einem AccessDenied-Fehler fehl.
- Die folgenden Plattform-, Authentifizierungs- und Protokollkombinationen mit S3-Objektsperre werden für Cloud-Speicherpools nicht unterstützt:
  - **Plattformen**: Google Cloud Platform und Azure
  - **Authentifizierungstypen**: IAM Roles Anywhere und anonymer Zugriff
  - **Protokoll**: HTTP

Überlegungen zu den für Cloud Storage Pools verwendeten Ports

Um sicherzustellen, dass die ILM-Regeln Objekte zum und vom angegebenen Cloud-Speicherpool verschieben können, müssen Sie das Netzwerk oder die Netzwerke konfigurieren, die die Speicherknoten Ihres Systems enthalten. Sie müssen sicherstellen, dass die folgenden Ports mit dem Cloud-Speicherpool kommunizieren können.

Standardmäßig verwenden Cloud Storage Pools die folgenden Ports:

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

Sie können beim Erstellen oder Bearbeiten eines Cloud-Speicherpools einen anderen Port angeben.

Wenn Sie einen nicht-transparenten Proxy-Server verwenden, müssen Sie außerdem"Konfigurieren eines Speicherproxys" um das Senden von Nachrichten an externe Endpunkte zu ermöglichen, beispielsweise an einen Endpunkt im Internet.

Überlegungen zu den Kosten

Der Zugriff auf Speicher in der Cloud mithilfe eines Cloud-Speicherpools erfordert eine Netzwerkverbindung zur Cloud. Sie müssen die Kosten der Netzwerkinfrastruktur berücksichtigen, die Sie für den Zugriff auf die Cloud verwenden, und diese entsprechend bereitstellen, basierend auf der Datenmenge, die Sie voraussichtlich mithilfe des Cloud Storage Pools zwischen StorageGRID und der Cloud verschieben werden.

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

Wenn Sie Objekte von einem externen Cloud Storage Pool-Endpunkt zurück zu StorageGRID verschieben müssen, können höhere Kosten anfallen. In einem der folgenden Fälle können Objekte zurück zu StorageGRID verschoben werden:

- Die einzige Kopie des Objekts befindet sich in einem Cloud-Speicherpool und Sie entscheiden sich, das Objekt stattdessen in StorageGRID zu speichern. In diesem Fall konfigurieren Sie Ihre ILM-Regeln und -Richtlinien neu. Bei der ILM-Auswertung sendet StorageGRID mehrere Anfragen, um das Objekt aus dem Cloud-Speicherpool abzurufen. StorageGRID erstellt dann lokal die angegebene Anzahl replizierter oder löschcodierter Kopien. Nachdem das Objekt zurück zu StorageGRID verschoben wurde, wird die Kopie im Cloud Storage Pool gelöscht.

- Aufgrund eines Speicherknotenfehlers gehen Objekte verloren. Wenn sich die einzige verbleibende Kopie eines Objekts in einem Cloud-Speicherpool befindet, stellt StorageGRID das Objekt vorübergehend wieder her und erstellt eine neue Kopie auf dem wiederhergestellten Speicherknoten.

> Wenn Objekte aus einem Cloud Storage Pool zurück zu StorageGRID verschoben werden, sendet StorageGRID für jedes Objekt mehrere Anfragen an den Endpunkt des Cloud Storage Pools. Bevor Sie eine große Anzahl von Objekten verschieben, wenden Sie sich an den technischen Support, um Hilfe bei der Schätzung des Zeitrahmens und der damit verbundenen Kosten zu erhalten.

S3: Für den Cloud Storage Pool-Bucket erforderliche Berechtigungen

Die Richtlinien für den externen S3-Bucket, der für einen Cloud Storage Pool verwendet wird, müssen StorageGRID die Berechtigung erteilen, ein Objekt in den Bucket zu verschieben, den Status eines Objekts abzurufen, ein Objekt bei Bedarf aus dem Glacier-Speicher wiederherzustellen und mehr. Idealerweise sollte StorageGRID vollen Zugriff auf den Bucket haben(`s3:*`); wenn dies jedoch nicht möglich ist, 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 zum Lebenszyklus des externen Buckets

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

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

Angenommen, Sie möchten, dass alle Objekte, die von StorageGRID in den Cloud Storage Pool verschoben werden, sofort in den Amazon S3 Glacier-Speicher übertragen werden. Sie würden eine Lebenszykluskonfiguration auf dem externen S3-Bucket erstellen, die eine einzelne Aktion (**Übergang**) wie folgt angibt:

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

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

> Verwenden Sie beim Konfigurieren des Lebenszyklus des externen Buckets niemals **Ablauf** -Aktionen, um zu definieren, wann Objekte ablaufen. Ablaufaktionen führen dazu, dass das externe Speichersystem abgelaufene Objekte löscht. Wenn Sie später versuchen, auf ein abgelaufenes Objekt von StorageGRID zuzugreifen, wird das gelöschte Objekt nicht gefunden.

Wenn Sie Objekte im Cloud Storage Pool in das S3 Glacier Deep Archive (statt in Amazon S3 Glacier) übertragen möchten, geben Sie an `<StorageClass>DEEP_ARCHIVE</StorageClass>` im Bucket-Lebenszyklus. Beachten Sie jedoch, dass Sie die `Expedited` Ebene zum Wiederherstellen von Objekten aus S3 Glacier Deep Archive.

Azure: Überlegungen zur Zugriffsebene

Wenn Sie ein Azure-Speicherkonto konfigurieren, können Sie die Standardzugriffsebene auf „Heiß“ oder „Kalt“ festlegen. Wenn Sie ein Speicherkonto zur Verwendung mit einem Cloud-Speicherpool erstellen, sollten Sie die Hot-Tier-Ebene als Standardebene verwenden. Obwohl StorageGRID die Stufe sofort auf „Archiv“ setzt, wenn es Objekte in den Cloud Storage Pool verschiebt, stellt die Verwendung der Standardeinstellung „Hot“ sicher, dass Ihnen für Objekte, die vor Ablauf der Mindestdauer von 30 Tagen aus der Stufe „Cool“ entfernt werden, keine Gebühr für die vorzeitige Löschung berechnet wird.

Azure: Lebenszyklusverwaltung wird nicht unterstützt

Verwenden Sie für den mit einem Cloud-Speicherpool verwendeten Container nicht die Azure Blob-Speicherlebenszyklusverwaltung. Die Lebenszyklusvorgänge können die Vorgänge des Cloud Storage Pools beeinträchtigen.

Ähnliche Informationen

"Erstellen Sie einen Cloud-Speicherpool"

Vergleichen Sie Cloud Storage Pools und CloudMirror-Replikation

Wenn Sie mit der Verwendung von Cloud Storage Pools beginnen, kann es hilfreich sein, die Ähnlichkeiten und Unterschiede zwischen Cloud Storage Pools und dem

StorageGRID CloudMirror-Replikationsdienst zu verstehen.

	Cloud-Speicherpool	CloudMirror-Replikationsdienst
Was ist der Hauptzweck?	Fungiert als Archivierungsziel. Die Objektkopie im Cloud Storage Pool kann die einzige Kopie des Objekts oder eine zusätzliche Kopie sein. Das heißt, anstatt zwei Kopien vor Ort aufzubewahren, können Sie eine Kopie in StorageGRID aufbewahren und eine Kopie an den Cloud Storage Pool senden.	Ermöglicht einem Mandanten, Objekte automatisch aus einem Bucket in StorageGRID (Quelle) in einen externen S3-Bucket (Ziel) zu replizieren. Erstellt eine unabhängige Kopie eines Objekts in einer unabhängigen S3-Infrastruktur.
Wie ist es eingerichtet?	Auf die gleiche Weise wie Speicherpools definiert, mithilfe des Grid Managers oder der Grid Management API. Kann als Platzierungsort in einer ILM-Regel ausgewählt werden. Während ein Speicherpool aus einer Gruppe von Speicherknoten besteht, wird ein Cloud-Speicherpool mithilfe eines Remote-S3- oder Azure-Endpunkts (IP-Adresse, Anmeldeinformationen usw.) definiert.	Ein Mandantenbenutzer"konfiguriert die CloudMirror-Replikation" durch Definieren eines CloudMirror-Endpunkts (IP-Adresse, Anmeldeinformationen usw.) mithilfe des Tenant Managers oder der S3-API. Nachdem der CloudMirror-Endpunkt eingerichtet wurde, kann jeder Bucket, der diesem Mandantenkonto gehört, so konfiguriert werden, dass er auf den CloudMirror-Endpunkt verweist.
Wer ist für die Einrichtung verantwortlich?	Normalerweise ist ein Grid-Administrator	Normalerweise ist ein Mieterbenutzer
Was ist das Ziel?	• Jede kompatible S3-Infrastruktur (einschließlich Amazon S3) • Azure Blob Archive-Ebene • Google Cloud Platform (GCP)	• Jede kompatible S3-Infrastruktur (einschließlich Amazon S3) • Google Cloud Platform (GCP)
Was bewirkt, dass Objekte zum Ziel verschoben werden?	Eine oder mehrere ILM-Regeln in den aktiven ILM-Richtlinien. Die ILM-Regeln definieren, welche Objekte StorageGRID in den Cloud Storage Pool verschiebt und wann die Objekte verschoben werden.	Der Vorgang der Aufnahme eines neuen Objekts in einen Quell-Bucket, der mit einem CloudMirror-Endpunkt konfiguriert wurde. Objekte, die im Quell-Bucket vorhanden waren, bevor der Bucket mit dem CloudMirror-Endpunkt konfiguriert wurde, werden nicht repliziert, es sei denn, sie werden geändert.

	Cloud-Speicherpool	CloudMirror-Replikationsdienst
Wie werden Objekte abgerufen?	Anwendungen müssen Anfragen an StorageGRID stellen, um Objekte abzurufen, die in einen Cloud-Speicherpool verschoben wurden. Wenn die einzige Kopie eines Objekts in den Archivspeicher übertragen wurde, verwaltet StorageGRID den Wiederherstellungsprozess des Objekts, sodass es abgerufen werden kann.	Da es sich bei der gespiegelten Kopie im Ziel-Bucket um eine unabhängige Kopie handelt, können Anwendungen das Objekt abrufen, indem sie Anfragen entweder an StorageGRID oder an das S3-Ziel senden. Angenommen, Sie verwenden die CloudMirror-Replikation, um Objekte in eine Partnerorganisation zu spiegeln. Der Partner kann seine eigenen Anwendungen verwenden, um Objekte direkt vom S3-Ziel zu lesen oder zu aktualisieren. Die Verwendung von StorageGRID ist nicht erforderlich.
Können Sie direkt vom Ziel lesen?	Nein. In einen Cloud-Speicherpool verschobene Objekte werden von StorageGRID verwaltet. Leseanforderungen müssen an StorageGRID gerichtet werden (und StorageGRID ist für den Abruf aus dem Cloud Storage Pool verantwortlich).	Ja, da es sich bei der gespiegelten Kopie um eine unabhängige Kopie handelt.
Was passiert, wenn ein Objekt aus der Quelle gelöscht wird?	Das Objekt wird auch aus dem Cloud-Speicherpool gelöscht.	Die Löschaktion wird nicht repliziert. Ein gelöschtes Objekt ist im StorageGRID Bucket nicht mehr vorhanden, im Ziel-Bucket jedoch weiterhin. Ebenso können Objekte im Ziel-Bucket gelöscht werden, ohne dass dies Auswirkungen auf die Quelle hat.
Wie greifen Sie nach einem Desaster (StorageGRID-System nicht betriebsbereit) auf Objekte zu?	Ausgefallene StorageGRID Knoten müssen wiederhergestellt werden. Während dieses Vorgangs können Kopien replizierter Objekte mithilfe der Kopien im Cloud-Speicherpool wiederhergestellt werden.	Die Objektkopien im CloudMirror-Ziel sind unabhängig von StorageGRID, sodass auf sie direkt zugegriffen werden kann, bevor die StorageGRID Knoten wiederhergestellt werden.

Erstellen Sie einen Cloud-Speicherpool

Ein Cloud-Speicherpool gibt einen einzelnen externen Amazon S3-Bucket oder einen anderen S3-kompatiblen Anbieter oder einen Azure Blob-Speichercontainer an.

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

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

Bevor Sie beginnen

- Sie sind beim Grid Manager angemeldet mit einem"unterstützter Webbrowser" .
- Sie haben die"erforderliche Zugriffsberechtigungen" .
- Sie haben die"Überlegungen zu Cloud-Speicherpools" .
- Der externe Bucket oder Container, auf den der Cloud Storage Pool verweist, ist bereits vorhanden und Sie haben dieInformationen zum Dienstendpunkt .
- Um auf den Eimer oder Behälter zuzugreifen, haben Sie dieKontoinformationen für den Authentifizierungstyp du wirst wählen.

Schritte

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

Feld	Beschreibung
Name des Cloud-Speicherpools	Ein Name, der den Cloud-Speicherpool und seinen Zweck kurz beschreibt. Verwenden Sie einen Namen, der beim Konfigurieren von ILM-Regeln leicht zu identifizieren ist.
Anbietertyp	Welchen Cloud-Anbieter verwenden Sie für diesen Cloud-Speicherpool: • **Amazon S3/GCP**: Wählen Sie diese Option für einen Amazon S3, Commercial Cloud Services (C2S) S3, Google Cloud Platform (GCP) oder einen anderen S3-kompatiblen Anbieter. • **Azure Blob-Speicher**
Eimer oder Behälter	Der Name des externen S3-Buckets oder Azure-Containers. Sie können diesen Wert nicht mehr ändern, nachdem der Cloud-Speicherpool gespeichert wurde.

3. Geben Sie basierend auf Ihrem ausgewählten Providertyp die Service-Endpunktinformationen ein.

Amazon S3/GCP

a. Wählen Sie als Protokoll entweder HTTPS oder HTTP aus.

> Verwenden Sie keine HTTP-Verbindungen für vertrauliche Daten.

b. Geben Sie den Hostnamen ein. Beispiel:

`s3-aws-region.amazonaws.com`

c. Wählen Sie den URL-Stil aus:

Option	Beschreibung
Automatische Erkennung	Versuchen Sie, anhand der bereitgestellten Informationen automatisch zu erkennen, welcher URL-Stil verwendet werden soll. Wenn Sie beispielsweise eine IP-Adresse angeben, verwendet StorageGRID eine URL im Pfadstil. Wählen Sie diese Option nur, wenn Sie nicht wissen, welchen bestimmten Stil Sie verwenden sollen.
Virtuell gehosteter Stil	Verwenden Sie eine URL im virtuell gehosteten Stil, um auf den Bucket zuzugreifen. URLs im virtuell gehosteten Stil enthalten den Bucket-Namen als Teil des Domänennamens. Beispiel: `https://bucket-name.s3.company.com/key-name`
Pfad-Stil	Verwenden Sie eine URL im Pfadstil, um auf den Bucket zuzugreifen. URLs im Pfadstil enthalten am Ende den Bucket-Namen. Beispiel: `https://s3.company.com/bucket-name/key-name` **Hinweis:** Die URL-Option im Pfadstil wird nicht empfohlen und wird in einer zukünftigen Version von StorageGRID veraltet sein.

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

Azure Blob Storage

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

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

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

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

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

Zugriffsschlüssel

Für Amazon S3/GCP oder andere S3-kompatible Anbieter

a. **Zugriffsschlüssel-ID**: Geben Sie die Zugriffsschlüssel-ID für das Konto ein, dem der externe Bucket gehört.
b. **Geheimer Zugriffsschlüssel**: Geben Sie den geheimen Zugriffsschlüssel ein.

IAM-Rollen überall

Für den AWS IAM Roles Anywhere-Dienst

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

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

CAP (C2S-Zugangsportal)

Für Commercial Cloud Services (C2S) S3-Dienst

a. **URL für temporäre Anmeldeinformationen**: Geben Sie die vollständige URL ein, die StorageGRID verwendet, um temporäre Anmeldeinformationen vom CAP-Server abzurufen, einschließlich aller erforderlichen und optionalen API-Parameter, die Ihrem C2S-Konto zugewiesen sind.
b. **Server-CA-Zertifikat**: Wählen Sie **Durchsuchen** und laden Sie das CA-Zertifikat hoch, das StorageGRID zur Überprüfung des CAP-Servers verwenden wird. Das Zertifikat muss PEM-kodiert und von einer entsprechenden staatlichen Zertifizierungsstelle (CA) ausgestellt sein.
c. **Client-Zertifikat**: Wählen Sie **Durchsuchen** und laden Sie das Zertifikat hoch, mit dem StorageGRID sich beim CAP-Server identifiziert. Das Client-Zertifikat muss PEM-codiert sein, von einer entsprechenden staatlichen Zertifizierungsstelle (CA) ausgestellt worden sein und Zugriff auf Ihr C2S-Konto haben.
d. **Privater Schlüssel des Clients**: Wählen Sie **Durchsuchen** und laden Sie den PEM-codierten privaten Schlüssel für das Client-Zertifikat hoch.

e. Wenn der private Schlüssel des Clients verschlüsselt ist, geben Sie die Passphrase zum Entschlüsseln des privaten Schlüssels des Clients ein. Andernfalls lassen Sie das Feld **Passphrase für den privaten Clientschlüssel** leer.

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

Azure Blob Storage

Für Azure Blob Storage, nur gemeinsam genutzter Schlüssel

a. **Kontoname**: Geben Sie den Namen des Speicherkontos ein, dem der externe Container gehört

b. **Kontoschlüssel**: Geben Sie den geheimen Schlüssel für das Speicherkonto ein

Sie können diese Werte über das Azure-Portal ermitteln.

Anonym

Es sind keine weiteren Angaben erforderlich.

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

Option	Beschreibung
Verwenden Sie Stamm-CA-Zertifikate im Storage Node OS	Verwenden Sie die auf dem Betriebssystem installierten Grid CA-Zertifikate, um Verbindungen zu sichern.
Benutzerdefiniertes CA-Zertifikat verwenden	Verwenden Sie ein benutzerdefiniertes CA-Zertifikat. Wählen Sie **Durchsuchen** und laden Sie das PEM-codierte Zertifikat hoch.
Zertifikat nicht überprüfen	Wenn Sie diese Option auswählen, sind TLS-Verbindungen zum Cloud-Speicherpool nicht sicher.

6. Wählen Sie **Speichern**.

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

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

     Wenn die Validierung des Cloud Storage Pools fehlschlägt, erhalten Sie eine Fehlermeldung mit der Erklärung, warum die Validierung fehlgeschlagen ist. Beispielsweise kann ein Fehler gemeldet werden, wenn ein Zertifikatsfehler vorliegt oder wenn der von Ihnen angegebene Bucket oder Container noch nicht vorhanden ist.

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

Details zum Cloud-Speicherpool anzeigen

Sie können die Details eines Cloud-Speicherpools anzeigen, um festzustellen, wo er verwendet wird und welche Knoten und Speicherklassen enthalten sind.

Bevor Sie beginnen

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

Schritte

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

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

   - **Name**: Der eindeutige Anzeigename des Pools.
   - **URI**: Der Uniform Resource Identifier des Cloud Storage Pools.
   - **Anbietertyp**: Welcher Cloud-Anbieter wird für diesen Cloud-Speicherpool verwendet.
   - **Container**: Der Name des Buckets, der für den Cloud Storage Pool verwendet wird.
   - **ILM-Nutzung**: Wie der Pool derzeit genutzt wird. Ein Cloud-Speicherpool wird möglicherweise nicht verwendet oder in einer oder mehreren ILM-Regeln, Erasure-Coding-Profilen oder beidem verwendet.
   - **Letzter Fehler**: Der letzte Fehler, der während einer Integritätsprüfung dieses Cloud-Speicherpools erkannt wurde.

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

   Die Detailseite für den Pool wird angezeigt.

3. Sehen Sie sich die Registerkarte **Authentifizierung** an, um mehr über den Authentifizierungstyp für diesen Cloud-Speicherpool zu erfahren und die Authentifizierungsdetails zu bearbeiten.
4. Sehen Sie sich die Registerkarte **Serverüberprüfung** an, um mehr über die Überprüfungsdetails zu erfahren, die Überprüfung zu bearbeiten, ein neues Zertifikat herunterzuladen oder das Zertifikat PEM zu kopieren.
5. Sehen Sie sich die Registerkarte **ILM-Nutzung** an, um festzustellen, ob der Cloud-Speicherpool derzeit in ILM-Regeln oder Erasure-Coding-Profilen verwendet wird.
6. Optional können Sie auf die **ILM-Regelseite** gehen, um"Informieren Sie sich über alle Regeln und verwalten Sie diese." die den Cloud-Speicherpool verwenden.

Bearbeiten eines Cloud-Speicherpools

Sie können einen Cloud-Speicherpool bearbeiten, um seinen Namen, den Dienstendpunkt oder andere Details zu ändern. Sie können jedoch den S3-Bucket oder Azure-Container für einen Cloud-Speicherpool nicht ändern.

Bevor Sie beginnen

- Sie sind beim Grid Manager angemeldet mit einem"unterstützter Webbrowser" .
- Du hast"spezifische Zugriffsberechtigungen" .
- Sie haben die"Überlegungen zu Cloud-Speicherpools" .

Schritte

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

   In der Tabelle „Cloud Storage Pools“ sind die vorhandenen Cloud Storage Pools aufgeführt.

2. Aktivieren Sie das Kontrollkästchen für den Cloud-Speicherpool, den Sie bearbeiten möchten, und wählen Sie dann **Aktionen** > **Bearbeiten**.

   Alternativ können Sie den Namen des Cloud-Speicherpools und dann **Bearbeiten** auswählen.

3. Ändern Sie nach Bedarf den Namen des Cloud-Speicherpools, den Dienstendpunkt, die Authentifizierungsdaten oder die Methode zur Zertifikatsüberprüfung.

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

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

4. Wählen Sie **Speichern**.

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

   Wenn die Validierung des Cloud Storage Pools fehlschlägt, wird eine Fehlermeldung angezeigt. Beispielsweise kann ein Fehler gemeldet werden, wenn ein Zertifikatsfehler vorliegt.

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

Entfernen eines Cloud-Speicherpools

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

Bevor Sie beginnen

- Sie sind beim Grid Manager angemeldet mit einem"unterstützter Webbrowser" .
- Sie haben die"erforderliche Zugriffsberechtigungen" .

Verwenden Sie bei Bedarf ILM, um Objektdaten zu verschieben

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

Schritte

1. Wählen Sie **ILM** > **Speicherpools** > **Cloud-Speicherpools**.
2. Sehen Sie sich die Spalte „ILM-Nutzung“ in der Tabelle an, um festzustellen, ob Sie den Cloud-Speicherpool entfernen können.

   Sie können einen Cloud-Speicherpool nicht entfernen, wenn er in einer ILM-Regel oder in einem Erasure-

Coding-Profil verwendet wird.

3. Wenn der Cloud-Speicherpool verwendet wird, wählen Sie ***Name des Cloud-Speicherpools*** > **ILM-Nutzung**.
4. "Klonen Sie jede ILM-Regel"das derzeit Objekte im Cloud-Speicherpool platziert, die Sie entfernen möchten.
5. Bestimmen Sie, wohin Sie die vorhandenen Objekte verschieben möchten, die von jeder geklonten Regel verwaltet werden.

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

6. Bearbeiten Sie jede der geklonten Regeln.

   Wählen Sie in Schritt 2 des Assistenten zum Erstellen einer ILM-Regel den neuen Speicherort aus dem Feld **Kopien in** aus.

7. "Erstellen einer neuen ILM-Richtlinie"und ersetzen Sie jede der alten Regeln durch eine geklonte Regel.
8. Aktivieren Sie die neue Richtlinie.
9. Warten Sie, bis ILM Objekte aus dem Cloud-Speicherpool entfernt und am neuen Speicherort abgelegt hat.

Cloud-Speicherpool löschen

Wenn der Cloud-Speicherpool leer ist und in keinen ILM-Regeln verwendet wird, können Sie ihn löschen.

Bevor Sie beginnen

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

  Wenn Sie versuchen, einen Cloud-Speicherpool zu entfernen, der Objekte enthält, tritt ein Fehler auf. Sehen "Fehlerbehebung bei Cloud-Speicherpools" .

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

Schritte

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

Fehlerbehebung bei Cloud-Speicherpools

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

Feststellen, ob ein Fehler aufgetreten ist

StorageGRID führt einen einfachen Integritätscheck für jeden Cloud Storage Pool durch, indem es das bekannte Objekt liest `x-ntap-sgws-cloud-pool-uuid` um sicherzustellen, dass auf den Cloud Storage Pool zugegriffen werden kann und dieser ordnungsgemäß funktioniert. Wenn StorageGRID auf einen Fehler am Endpunkt stößt, führt es jede Minute eine Integritätsprüfung von jedem Speicherknoten aus durch. Wenn der Fehler behoben ist, werden die Integritätsprüfungen beendet. Wenn bei einer Integritätsprüfung ein Problem erkannt wird, wird in der Spalte „Letzter Fehler“ der Tabelle „Cloud-Speicherpools“ auf der Seite „Speicherpools“ eine Meldung angezeigt.

Die Tabelle zeigt den zuletzt erkannten Fehler für jeden Cloud-Speicherpool und gibt an, wie lange der Fehler her ist.

Darüber hinaus wird eine Warnung **Verbindungsfehler im Cloud Storage Pool** ausgelöst, wenn die Integritätsprüfung erkennt, dass innerhalb der letzten 5 Minuten ein oder mehrere neue Fehler im Cloud Storage Pool aufgetreten sind. Wenn Sie eine E-Mail-Benachrichtigung zu dieser Warnung erhalten, gehen Sie zur Seite „Speicherpools“ (wählen Sie **ILM** > **Speicherpools**), überprüfen Sie die Fehlermeldungen in der Spalte „Letzter Fehler“ und beachten Sie die nachstehenden Richtlinien zur Fehlerbehebung.

Überprüfen Sie, ob ein Fehler behoben wurde

Nachdem Sie alle zugrunde liegenden Probleme behoben haben, können Sie feststellen, ob der Fehler behoben wurde. Wählen Sie auf der Seite „Cloud-Speicherpool“ den Endpunkt aus und wählen Sie „Fehler löschen“ aus. Eine Bestätigungsmeldung zeigt an, dass StorageGRID den Fehler für den Cloud Storage Pool behoben hat.

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

Fehler: Integritätsprüfung fehlgeschlagen. Fehler vom Endpunkt

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

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

Fehler: Dieser Cloud-Speicherpool enthält unerwartete Inhalte

Dieser Fehler kann auftreten, wenn Sie versuchen, einen Cloud-Speicherpool zu erstellen, zu bearbeiten oder zu löschen. Dieser Fehler tritt auf, wenn der Bucket oder Container Folgendes enthält: `x-ntap-sgws-cloud-pool-uuid` Markerdatei, aber diese Datei verfügt nicht über das Metadatenfeld mit der erwarteten UUID.

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

Versuchen Sie, das Problem mit einem der folgenden Schritte zu beheben:

- Wenn Sie einen neuen Cloud Storage Pool konfigurieren und der Bucket die `x-ntap-sgws-cloud-`

`pool-uuid` Datei und zusätzliche Objektschlüssel ähnlich dem folgenden Beispiel, erstellen Sie einen neuen Bucket und verwenden Sie stattdessen diesen neuen Bucket.

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

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

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

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

Dieser Fehler kann unter den folgenden Umständen auftreten:

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

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

Um das Problem zu beheben, überprüfen Sie die Fehlermeldung vom Endpunkt.

- Wenn die Fehlermeldung enthält `Get *url*: EOF` , überprüfen Sie, dass der für den Cloud Storage Pool verwendete Dienstendpunkt kein HTTP 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 Speicherknoten den Zugriff auf den für den Cloud-Speicherpool verwendeten Dienstendpunkt ermöglicht.
- Wenn der Fehler auf eine nicht unterstützte Plattform, Authentifizierung oder ein nicht unterstütztes Protokoll zurückzuführen ist, wechseln Sie zu einer unterstützten Konfiguration mit S3 Object Lock und versuchen Sie erneut, den neuen Cloud Storage Pool zu speichern.
- Versuchen Sie bei allen anderen Endpunkt-Fehlermeldungen eine oder mehrere der folgenden Methoden:
  - Erstellen Sie einen externen Container oder Bucket mit demselben Namen, den Sie für den Cloud Storage Pool eingegeben haben, und versuchen Sie erneut, den neuen Cloud Storage Pool zu speichern.
  - Korrigieren Sie den Container- oder Bucket-Namen, den Sie für den Cloud Storage Pool angegeben haben, und versuchen Sie erneut, den neuen Cloud Storage Pool zu speichern.

Fehler: Das CA-Zertifikat konnte nicht analysiert werden.

Dieser Fehler kann auftreten, wenn Sie versuchen, einen Cloud-Speicherpool zu erstellen oder zu bearbeiten. Der Fehler tritt auf, wenn StorageGRID das Zertifikat, das Sie beim Konfigurieren des Cloud Storage Pools eingegeben haben, nicht analysieren konnte.

Um das Problem zu beheben, überprüfen Sie das von Ihnen bereitgestellte CA-Zertifikat auf Probleme.

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

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

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

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

- Überprüfen Sie, ob der mit dem konfigurierten Zugriffsschlüssel verknüpfte Benutzer über die erforderlichen Berechtigungen verfügt.
- Bearbeiten Sie den Cloud-Speicherpool mit Anmeldeinformationen, die über die erforderlichen 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 kann auftreten, wenn Sie versuchen, einen Cloud-Speicherpool zu löschen. Dieser Fehler weist darauf hin, dass ein Verbindungs- oder Konfigurationsproblem StorageGRID daran hindert, den Inhalt des Cloud Storage Pool-Buckets zu lesen.

Um das Problem zu beheben, überprüfen Sie die Fehlermeldung vom Endpunkt.

Fehler: In diesem Bucket wurden bereits Objekte platziert

Dieser Fehler kann auftreten, wenn Sie versuchen, einen Cloud-Speicherpool zu löschen. Sie können einen Cloud-Speicherpool nicht löschen, wenn er Daten enthält, die von ILM dorthin verschoben wurden, Daten, die sich im Bucket befanden, bevor Sie den Cloud-Speicherpool konfiguriert haben, oder Daten, die nach der Erstellung des Cloud-Speicherpools von einer anderen Quelle in den Bucket gelegt wurden.

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

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

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

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

Dieser Fehler kann auftreten, wenn Sie einen nicht transparenten Speicherproxy zwischen Speicherknoten und dem für den Cloud-Speicherpool verwendeten externen S3-Endpunkt konfiguriert haben. 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 auflösen oder es liegt ein externes Netzwerkproblem vor.

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

- Überprüfen Sie die Einstellungen für den Cloud-Speicherpool (**ILM** > **Speicherpools**).

- Überprüfen Sie die Netzwerkkonfiguration des Speicherproxyservers.

Fehler: Das X.509-Zertifikat hat seine Gültigkeitsdauer überschritten

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

Versuchen Sie, das Problem mit den folgenden Schritten zu beheben:

- Aktualisieren Sie das für die Authentifizierung beim Cloud-Speicherpool konfigurierte Zertifikat.
- Stellen Sie sicher, dass alle Warnungen zum Ablauf des Zertifikats in diesem Cloud-Speicherpool behoben werden.

Ähnliche Informationen

"Lebenszyklus eines Cloud Storage Pool-Objekts"

Verwalten von Erasure-Coding-Profilen

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

Bevor Sie beginnen

- Sie sind beim Grid Manager angemeldet mit einem"unterstützter Webbrowser" .
- Sie haben die"erforderliche Zugriffsberechtigungen" .

Details zum Erasure-Coding-Profil anzeigen

Sie können die Details eines Erasure-Coding-Profils anzeigen, um dessen Status, das verwendete Erasure-Coding-Schema und andere Informationen zu ermitteln.

Schritte

1. Wählen Sie **KONFIGURATION** > **System** > **Erasure Coding**.
2. Wählen Sie das Profil aus. Die Detailseite für das Profil wird angezeigt.
3. Optional können Sie auf der Registerkarte „ILM-Regeln“ eine Liste der ILM-Regeln anzeigen, die das Profil verwenden, sowie die ILM-Richtlinien, die diese Regeln verwenden.
4. Optional können Sie auf der Registerkarte „Speicherknoten“ Details zu jedem Speicherknoten im Speicherpool des Profils anzeigen, z. B. den Standort und die Speichernutzung.

Umbenennen eines Erasure-Coding-Profils

Möglicherweise möchten Sie ein Erasure-Coding-Profil umbenennen, um deutlicher zu machen, was das Profil macht.

Schritte

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

3. Wählen Sie **Umbenennen**.
4. Geben Sie einen eindeutigen Namen für das Erasure-Coding-Profil ein.

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

   > Die Namen der Erasure-Coding-Profile müssen eindeutig sein. Wenn Sie den Namen eines vorhandenen Profils verwenden, tritt ein Validierungsfehler auf, auch wenn dieses Profil deaktiviert wurde.

5. Wählen Sie **Speichern**.

Deaktivieren eines Erasure-Coding-Profils

Sie können ein Erasure-Coding-Profil deaktivieren, wenn Sie es nicht mehr verwenden möchten und das Profil derzeit in keinen ILM-Regeln verwendet wird.

> Stellen Sie sicher, dass keine Vorgänge zur Reparatur von Erasure-Code-Daten oder Außerbetriebnahmen im Gange sind. Wenn Sie versuchen, ein Erasure-Coding-Profil zu deaktivieren, während einer dieser Vorgänge ausgeführt wird, wird eine Fehlermeldung zurückgegeben.

Informationen zu diesem Vorgang

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

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

Schritte

1. Wählen Sie **KONFIGURATION** > **System** > **Erasure Coding**.
2. Überprüfen Sie auf der Registerkarte „Aktiv“ die Spalte **Status**, um sicherzustellen, dass das Erasure-Coding-Profil, das Sie deaktivieren möchten, in keinen ILM-Regeln verwendet wird.

   Sie können ein Erasure-Coding-Profil nicht deaktivieren, wenn es in einer ILM-Regel verwendet wird. Im Beispiel wird das Profil 2+1 Data Center 1 in mindestens einer ILM-Regel verwendet.

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

3. Wenn das Profil in einer ILM-Regel verwendet wird, gehen Sie folgendermaßen vor:
   a. Wählen Sie **ILM** > **Regeln**.
   b. Wählen Sie jede Regel aus und überprüfen Sie das Aufbewahrungsdiagramm, um festzustellen, ob die Regel das Erasure-Coding-Profil verwendet, das Sie deaktivieren möchten.

c. Wenn die ILM-Regel das Erasure-Coding-Profil verwendet, das Sie deaktivieren möchten, ermitteln Sie, ob die Regel in einer ILM-Richtlinie verwendet wird.

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

Wo wurde das Profil verwendet?	**Zusätzliche Schritte vor der Deaktivierung des Profils**	**Beachten Sie diese zusätzlichen Anweisungen**
Wird nie in einer ILM-Regel verwendet	Keine weiteren Schritte erforderlich. Fahren Sie mit diesem Verfahren fort.	*Keiner*
In einer ILM-Regel, die noch nie in einer ILM-Richtlinie verwendet wurde	i. Bearbeiten oder löschen Sie alle betroffenen ILM-Regeln. 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"

Wo wurde das Profil verwendet?	Zusätzliche Schritte vor der Deaktivierung des Profils	Beachten Sie diese zusätzlichen Anweisungen
In einer ILM-Regel, die sich derzeit in einer aktiven ILM-Richtlinie befindet	i. Klonen Sie die Richtlinie. ii. Entfernen Sie die ILM-Regel, die das Erasure-Coding-Profil verwendet. iii. Fügen Sie eine oder mehrere neue ILM-Regeln hinzu, um sicherzustellen, dass Objekte geschützt sind. iv. Speichern, simulieren und aktivieren Sie die neue Richtlinie. v. Warten Sie, bis die neue Richtlinie angewendet wird und vorhandene Objekte basierend auf den von Ihnen hinzugefügten neuen Regeln an neue Speicherorte verschoben werden. **Hinweis:** Abhängig von der Anzahl der Objekte und der Größe Ihres StorageGRID -Systems kann es Wochen oder sogar Monate dauern, bis ILM-Vorgänge die Objekte basierend auf den neuen ILM-Regeln an neue Speicherorte verschieben. Sie können zwar gefahrlos versuchen, ein Erasure-Coding-Profil zu deaktivieren, solange es noch mit Daten verknüpft ist, der Deaktivierungsvorgang schlägt jedoch fehl. Eine Fehlermeldung informiert Sie, wenn das Profil noch nicht zur Deaktivierung bereit ist. 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.	"Erstellen einer ILM-Richtlinie" "Arbeiten mit ILM-Regeln und ILM-Richtlinien"

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

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

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

> Sie können mehrere Profile gleichzeitig zur Deaktivierung auswählen, solange die einzelnen Profile nicht in einer Regel verwendet werden.

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

Ergebnisse

- Wenn StorageGRID das Erasure-Coding-Profil deaktivieren kann, lautet sein Status „Deaktiviert“. Sie können dieses Profil nicht mehr für eine ILM-Regel auswählen. Sie können ein deaktiviertes Profil nicht reaktivieren.
- Wenn StorageGRID das Profil nicht deaktivieren kann, wird eine Fehlermeldung angezeigt. Beispielsweise erscheint eine Fehlermeldung, wenn noch Objektdaten mit diesem Profil verknüpft sind. Möglicherweise müssen Sie mehrere Wochen warten, bevor Sie den Deaktivierungsvorgang erneut versuchen.

Regionen konfigurieren (optional und nur S3)

ILM-Regeln können Objekte basierend auf den Regionen filtern, in denen S3-Buckets erstellt werden, sodass Sie Objekte aus verschiedenen Regionen an verschiedenen Speicherorten speichern können.

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

> Sie können die Region für einen Bucket nicht mehr ändern, nachdem der Bucket erstellt wurde.

Bevor Sie beginnen

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

Informationen zu diesem Vorgang

Beim Erstellen eines S3-Buckets können Sie angeben, dass der Bucket in einer bestimmten Region erstellt werden soll. Durch die Angabe einer Region kann sich der Bucket geografisch in der Nähe seiner Benutzer befinden, wodurch die Latenz optimiert, die Kosten minimiert und gesetzliche Anforderungen erfüllt werden können.

Wenn Sie eine ILM-Regel erstellen, möchten Sie möglicherweise die mit einem S3-Bucket verknüpfte Region als erweiterten Filter verwenden. Sie können beispielsweise eine Regel entwerfen, die nur für Objekte in S3-Buckets gilt, die im `us-west-2` Region. Sie können dann angeben, dass Kopien dieser Objekte auf Speicherknoten an einem Rechenzentrumsstandort innerhalb dieser Region abgelegt werden, um die Latenz zu optimieren.

Befolgen Sie beim Konfigurieren von Regionen die folgenden Richtlinien:

- Standardmäßig werden alle Buckets als zugehörig betrachtet zum `us-east-1` Region.
- Sie müssen die Regionen mit dem Grid Manager erstellen, bevor Sie beim Erstellen von Buckets mit dem Tenant Manager oder der Tenant Management 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 Regionsnamen verwenden. Bei Regionsnamen wird zwischen Groß- und Kleinschreibung unterschieden. Gültige Zeichen sind Zahlen, Buchstaben und Bindestriche.

  > ⓘ EU wird nicht als Alias für eu-west-1 betrachtet. Wenn Sie die Region EU oder eu-west-1 verwenden möchten, müssen Sie den genauen Namen verwenden.

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

  Eine ungültige Region kann entstehen, wenn Sie eine Region als erweiterten Filter in einer ILM-Regel verwenden, diese Region aber später löschen, oder wenn Sie die Grid Management-API zum Erstellen einer Regel verwenden und eine Region angeben, 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 jemals den erweiterten Filter „Standortbeschränkung“ verwenden möchten, um Objekte in diesem Bucket zu finden.

Schritte

1. Wählen Sie **ILM** > **Regionen**.

   Die Seite „Regionen“ wird mit einer Liste der aktuell definierten Regionen angezeigt. **Region 1** zeigt die Standardregion, `us-east-1` , die nicht geändert oder entfernt werden können.

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

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

   Sie müssen genau diesen Regionsnamen als LocationConstraint-Anforderungselement verwenden, wenn Sie den entsprechenden S3-Bucket erstellen.

3. Um eine nicht verwendete Region zu entfernen, wählen Sie das Löschsymbol ✕ .

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

4. Wenn Sie mit den Änderungen fertig sind, wählen Sie **Speichern**.

   Sie können diese Regionen jetzt im Abschnitt „Erweiterte Filter“ in Schritt 1 des Assistenten „ILM-Regel erstellen“ auswählen. Sehen "Verwenden Sie erweiterte Filter in ILM-Regeln" .

ILM-Regel erstellen

Verwenden Sie ILM-Regeln zum Verwalten von Objekten

Zum Verwalten von Objekten erstellen Sie einen Satz von Regeln für das Information Lifecycle Management (ILM) und organisieren diese in einer ILM-Richtlinie.

Jedes in das System aufgenommene Objekt wird anhand der aktiven Richtlinie bewertet. Wenn eine Regel in der Richtlinie mit den Metadaten eines Objekts übereinstimmt, bestimmen die Anweisungen in der Regel, welche Aktionen StorageGRID zum Kopieren und Speichern dieses Objekts ausführt.

> ⓘ Objektmetadaten werden nicht durch ILM-Regeln verwaltet. Stattdessen werden Objektmetadaten in einer Cassandra-Datenbank in einem sogenannten Metadatenspeicher gespeichert. Um die Daten vor Verlust zu schützen, werden an jedem Standort automatisch drei Kopien der Objektmetadaten verwaltet.

Elemente einer ILM-Regel

Eine ILM-Regel besteht aus drei Elementen:

- **Filterkriterien**: Die grundlegenden und erweiterten Filter einer Regel definieren, auf welche Objekte die Regel angewendet wird. Wenn ein Objekt allen Filtern entspricht, wendet StorageGRID die Regel an und erstellt die in den Platzierungsanweisungen der Regel angegebenen Objektkopien.
- **Platzierungsanweisungen**: Die Platzierungsanweisungen einer Regel definieren die Anzahl, den Typ und den Speicherort von Objektkopien. Jede Regel kann eine Abfolge von Platzierungsanweisungen enthalten, um die Anzahl, den Typ und den Speicherort von Objektkopien im Laufe der Zeit zu ändern. Wenn der Zeitraum für eine Platzierung abläuft, werden die Anweisungen in der nächsten Platzierung automatisch von der nächsten ILM-Bewertung angewendet.
- **Aufnahmeverhalten**: Über das Aufnahmeverhalten einer Regel können Sie auswählen, wie die durch die Regel gefilterten Objekte bei der Aufnahme geschützt werden (wenn ein S3-Client ein Objekt im Raster speichert).

ILM-Regelfilterung

Wenn Sie eine ILM-Regel erstellen, geben Sie Filter an, um zu identifizieren, auf welche Objekte die Regel angewendet wird.

Im einfachsten Fall verwendet eine Regel möglicherweise keine Filter. Jede Regel, die keine Filter verwendet, gilt für alle Objekte und muss daher die letzte (Standard-)Regel in einer ILM-Richtlinie sein. Die Standardregel bietet Speicheranweisungen für Objekte, die nicht den Filtern einer anderen Regel entsprechen.

- Mithilfe von Basisfiltern können Sie unterschiedliche Regeln auf große, unterschiedliche Objektgruppen anwenden. Mit diesen Filtern können Sie eine Regel auf bestimmte Mandantenkonten, bestimmte S3-Buckets oder beides anwenden.

  Mithilfe von Basisfiltern können Sie auf einfache Weise unterschiedliche Regeln auf eine große Anzahl von Objekten anwenden. Beispielsweise müssen die Finanzunterlagen Ihres Unternehmens möglicherweise gespeichert werden, um gesetzliche Anforderungen zu erfüllen, während Daten der Marketingabteilung möglicherweise gespeichert werden müssen, um den täglichen Betrieb zu erleichtern. Nachdem Sie für jede Abteilung separate Mandantenkonten erstellt oder die Daten der verschiedenen Abteilungen in separate S3-Buckets aufgeteilt haben, können Sie ganz einfach eine Regel erstellen, die für alle Finanzunterlagen gilt, und eine zweite Regel, die für alle Marketingdaten gilt.

- Erweiterte Filter geben Ihnen eine detaillierte Kontrolle. Sie können Filter erstellen, um Objekte basierend auf den folgenden Objekteigenschaften auszuwählen:
  - Aufnahmezeit
  - Letzter Zugriffszeitpunkt
  - Der gesamte oder ein Teil des Objektnamens (Schlüssel)
  - Standortbeschränkung (nur S3)
  - Objektgröße
  - Benutzermetadaten
  - Objekt-Tag (nur S3)

Sie können Objekte nach ganz bestimmten Kriterien filtern. Beispielsweise werden Objekte, die in der Bildgebungsabteilung eines Krankenhauses gespeichert sind, möglicherweise häufig verwendet, wenn sie weniger als 30 Tage alt sind, und danach nur noch selten, während Objekte, die Informationen zu Patientenbesuchen enthalten, möglicherweise in die Abrechnungsabteilung in der Zentrale des Gesundheitsnetzwerks kopiert werden müssen. Sie können Filter erstellen, die jeden Objekttyp anhand des Objektnamens, der Größe, der S3-Objekt-Tags oder anderer relevanter Kriterien identifizieren, und dann separate Regeln erstellen, um jeden Objektsatz entsprechend zu speichern.

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

Anweisungen zur Platzierung von ILM-Regeln

Platzierungsanweisungen bestimmen, wo, wann und wie Objektdaten gespeichert werden. Eine ILM-Regel kann eine oder mehrere Platzierungsanweisungen enthalten. Jede Platzierungsanweisung gilt jeweils für einen Zeitraum.

Wenn Sie Platzierungsanweisungen erstellen:

- Sie beginnen mit der Angabe der Referenzzeit, die bestimmt, wann die Platzierungsanweisungen beginnen. Der Referenzzeitpunkt kann der Zeitpunkt der Aufnahme eines Objekts, der Zugriff auf ein Objekt, der Zeitpunkt, zu dem ein versioniertes Objekt nicht mehr aktuell ist, oder ein benutzerdefinierter

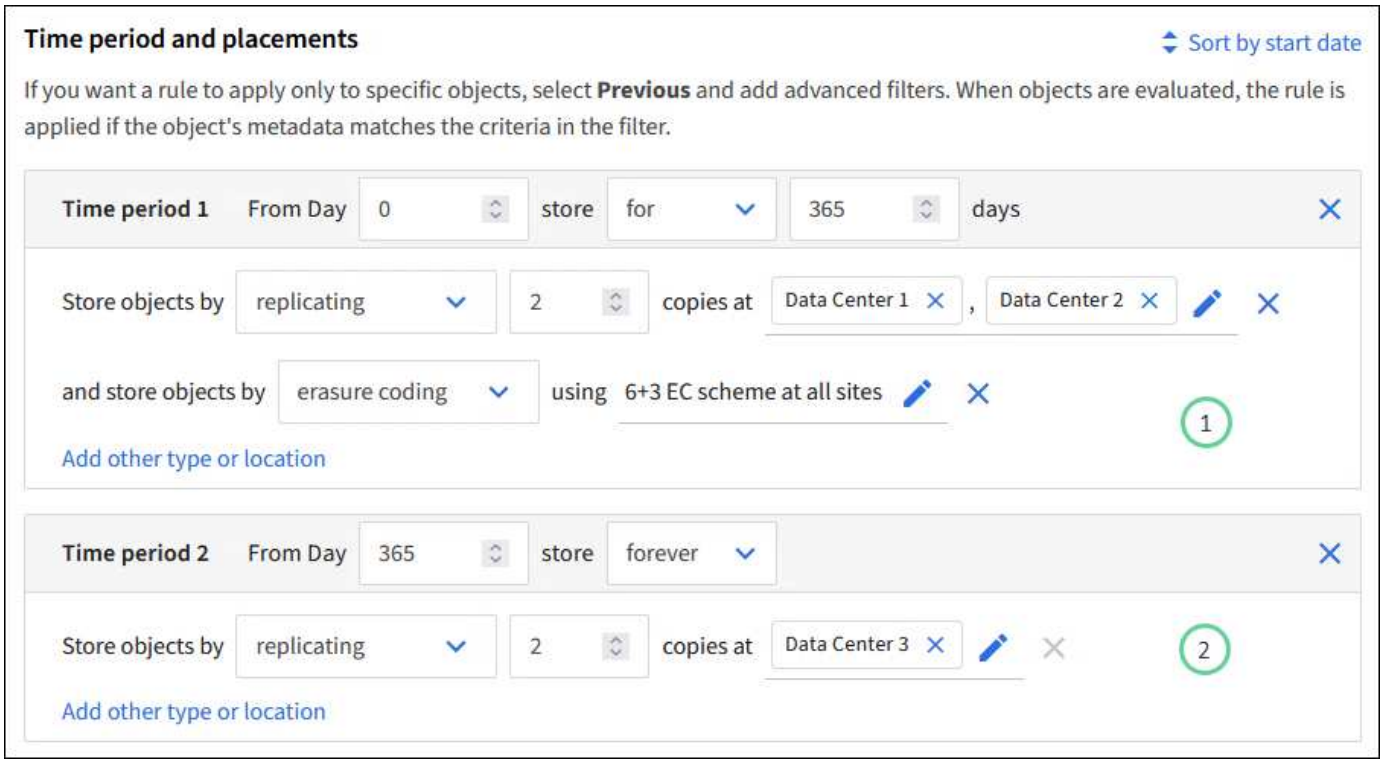
Zeitpunkt sein.

- Als Nächstes geben Sie an, wann die Platzierung relativ zur Referenzzeit angewendet wird. Beispielsweise kann eine Platzierung am Tag 0 beginnen und 365 Tage lang andauern, relativ zum Zeitpunkt der Aufnahme des Objekts.
- Abschließend geben Sie die Art der Kopien (Replikation oder Erasure Coding) und den Speicherort der Kopien an. Beispielsweise möchten Sie möglicherweise zwei replizierte Kopien an zwei verschiedenen Standorten speichern.

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

- Um Objekte während eines einzelnen Zeitraums an mehreren Standorten zu platzieren, wählen Sie **Anderen Typ oder Standort hinzufügen** aus, um für diesen Zeitraum mehr als eine Zeile hinzuzufügen.
- Um Objekte an verschiedenen Orten in unterschiedlichen Zeiträumen zu platzieren, wählen Sie **Weiteren Zeitraum hinzufügen**, um den nächsten Zeitraum hinzuzufügen. Geben Sie dann eine oder mehrere Zeilen innerhalb des Zeitraums an.

Das Beispiel zeigt zwei Platzierungsanweisungen auf der Seite „Platzierungen definieren“ des Assistenten „ILM-Regel erstellen“.



Die erste Platzierungsanweisung (1) hat zwei Zeilen für das erste Jahr:

- Die erste Zeile erstellt zwei replizierte Objektkopien an zwei Rechenzentrumsstandorten.
- Die zweite Zeile erstellt eine 6+3-Löschcode-Kopie unter Verwendung aller Rechenzentrumsstandorte.

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

Wenn Sie den Satz von Platzierungsanweisungen für eine Regel definieren, müssen Sie sicherstellen, dass

mindestens eine Platzierungsanweisung am Tag 0 beginnt, dass keine Lücken zwischen den von Ihnen definierten Zeiträumen bestehen und dass die letzte Platzierungsanweisung entweder für immer oder so lange gilt, bis Sie keine Objektkopien mehr benötigen.

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

ILM-Regelaufnahmeverhalten

Das Aufnahmeverhalten steuert, ob Objektkopien sofort gemäß den Anweisungen in der Regel platziert werden oder ob Zwischenkopien erstellt werden und die Platzierungsanweisungen später angewendet werden. Für ILM-Regeln sind die folgenden Aufnahmeverhalten verfügbar:

- **Ausgeglichen**: StorageGRID versucht, bei der Aufnahme alle in der ILM-Regel angegebenen Kopien zu erstellen. Wenn dies nicht möglich ist, werden Zwischenkopien erstellt und der Erfolg wird an den Client zurückgegeben. Die in der ILM-Regel angegebenen Kopien werden nach Möglichkeit erstellt.
- **Streng**: Alle in der ILM-Regel angegebenen Kopien müssen erstellt werden, bevor dem Client der Erfolg gemeldet wird.
- **Dual Commit**: StorageGRID erstellt sofort Zwischenkopien des Objekts und meldet den Erfolg an den Client. Wenn möglich, werden die in der ILM-Regel angegebenen Kopien erstellt.

Ähnliche Informationen

- "Aufnahmeoptionen"
- "Vorteile, Nachteile und Einschränkungen der Aufnahmeoptionen"
- "Wie sich Konsistenz und ILM-Regeln auf den Datenschutz auswirken"

Beispiel einer ILM-Regel

Beispielsweise könnte eine ILM-Regel Folgendes festlegen:

- Gilt nur für die Objekte, die Mieter A gehören.
- Erstellen Sie zwei replizierte Kopien dieser Objekte und speichern Sie jede Kopie an einem anderen Ort.
- Bewahren Sie die beiden Kopien „für immer“ auf, was bedeutet, dass StorageGRID sie nicht automatisch löscht. Stattdessen behält StorageGRID diese Objekte, bis sie durch eine Löschanforderung des Clients oder durch Ablauf eines Bucket-Lebenszyklus gelöscht werden.
- Verwenden Sie die Option „Ausgewogen“ 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, beide erforderlichen Kopien sofort zu erstellen.

  Wenn beispielsweise Site 2 nicht erreichbar ist, wenn Mandant A ein Objekt speichert, erstellt StorageGRID zwei Zwischenkopien auf Speicherknoten an Site 1. Sobald Site 2 verfügbar ist, erstellt StorageGRID die erforderliche Kopie an diesem Site.

Ähnliche Informationen

- "Was ist ein Speicherpool?"
- "Was ist ein Cloud-Speicherpool?"

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

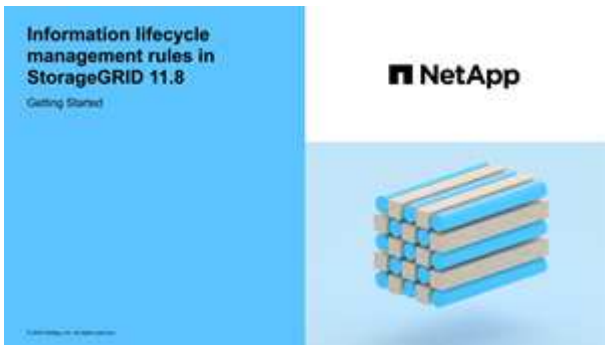
Mithilfe von ILM-Regeln können Sie die Platzierung von Objektdaten im Laufe der Zeit

verwalten. Zum Erstellen einer ILM-Regel verwenden Sie den Assistenten „ILM-Regel erstellen“.

> Wenn Sie die Standard-ILM-Regel für eine Richtlinie erstellen möchten, folgen Sie den"Anleitung zum Erstellen einer Standard-ILM-Regel" stattdessen.

Bevor Sie beginnen

- Sie sind beim Grid Manager angemeldet mit einem"unterstützter Webbrowser" .
- Du hast"spezifische Zugriffsberechtigungen" .
- Wenn Sie festlegen möchten, für welche Mandantenkonten diese Regel gilt, haben Sie die"Berechtigung für Mandantenkonten" oder Sie kennen die Konto-ID für jedes Konto.
- Wenn die Regel Objekte anhand der Metadaten zum letzten Zugriffszeitpunkt filtern soll, müssen Aktualisierungen des letzten Zugriffszeitpunkts durch den S3-Bucket aktiviert werden.
- Sie haben alle Cloud-Speicherpools konfiguriert, die Sie verwenden möchten. Sehen "Cloud-Speicherpool erstellen" .
- Sie kennen die"Aufnahmeoptionen" .
- Wenn Sie eine konforme Regel für die Verwendung mit S3 Object Lock erstellen müssen, sind Sie vertraut mit dem"Anforderungen für S3 Object Lock" .
- Optional haben Sie das Video angesehen: "Video: Übersicht über ILM-Regeln" .



Informationen zu diesem Vorgang

Beim Erstellen von ILM-Regeln:

- Berücksichtigen Sie die Topologie und Speicherkonfigurationen des StorageGRID -Systems.
- Überlegen Sie, welche Arten von Objektkopien Sie erstellen möchten (repliziert oder löschcodiert) und wie viele Kopien jedes Objekts erforderlich sind.
- Bestimmen Sie, welche Arten von Objektmetadaten in den Anwendungen verwendet werden, die eine Verbindung zum StorageGRID -System herstellen. ILM-Regeln filtern Objekte basierend auf ihren Metadaten.
- Überlegen Sie, wo Sie Objektkopien im Laufe der Zeit platzieren möchten.
- Entscheiden Sie, welche Aufnahmeoption verwendet werden soll (Balanced, Strict oder Dual Commit).

Schritte

1. Wählen Sie **ILM** > **Regeln**.
2. Wählen Sie **Erstellen**. "Schritt 1 (Details eingeben)"des Assistenten „ILM-Regel erstellen“ wird angezeigt.

Schritt 1 von 3: Details eingeben

Im Schritt **Details eingeben** des Assistenten „ILM-Regel erstellen“ können Sie einen Namen und eine Beschreibung für die Regel eingeben und Filter für die Regel definieren.

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

Informationen zu diesem Vorgang

Bei der Bewertung eines Objekts anhand einer"ILM-Regel" , StorageGRID vergleicht die Objektmetadaten mit den Filtern der Regel. Wenn die Objektmetadaten allen Filtern entsprechen, verwendet StorageGRID die Regel, um das Objekt zu platzieren. Sie können eine Regel entwerfen, die auf alle Objekte angewendet wird, oder Sie können grundlegende Filter angeben, beispielsweise ein oder mehrere Mandantenkonten oder Bucket-Namen, oder erweiterte Filter, beispielsweise die Größe des Objekts oder Benutzermetadaten.

Schritte

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

   Sie sollten den Zweck bzw. die Funktion der Regel beschreiben, damit Sie die Regel später wiedererkennen.

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

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

4. Geben Sie optional die S3-Buckets an, für die diese Regel gilt.

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

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

   Wenn Sie **Ja** wählen, wird automatisch "Nicht aktuelle Zeit" als Referenzzeit ausgewählt in"Schritt 2 des Assistenten „ILM-Regel erstellen“" .

   > Die nicht aktuelle Zeit gilt nur für S3-Objekte in Buckets mit aktivierter Versionierung. Sehen"Operationen an Buckets, PutBucketVersioning" Und"Verwalten von Objekten mit S3 Object Lock" .

   Mit dieser Option können Sie die Speicherbelastung versionierter Objekte reduzieren, indem Sie nach nicht aktuellen Objektversionen filtern. Sehen "Beispiel 4: ILM-Regeln und -Richtlinien für versionierte S3-Objekte" .

6. Wählen Sie optional **Erweiterten Filter hinzufügen** aus, um zusätzliche Filter anzugeben.

   Wenn Sie keine erweiterte Filterung konfigurieren, gilt die Regel für alle Objekte, die den grundlegenden Filtern entsprechen. Weitere Informationen zur erweiterten Filterung finden Sie unterVerwenden Sie erweiterte Filter in ILM-Regeln UndAngeben mehrerer Metadatentypen und -werte .

7. Wählen Sie **Weiter**. "Schritt 2 (Platzierungen definieren)"des Assistenten „ILM-Regel erstellen“ wird

angezeigt.

Verwenden Sie erweiterte Filter in ILM-Regeln

Mithilfe der erweiterten Filterung können Sie ILM-Regeln erstellen, die basierend auf ihren Metadaten nur für bestimmte Objekte gelten. Wenn Sie die erweiterte Filterung für eine Regel einrichten, wählen Sie den Typ der abzugleichenden Metadaten aus, wählen einen Operator aus und geben einen Metadatenwert an. Bei der Auswertung von Objekten wird die ILM-Regel nur auf die Objekte angewendet, deren Metadaten dem erweiterten Filter entsprechen.

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

Metadatentyp	Unterstützte Operatoren	Metadatenwert
Aufnahmezeit	• Ist • ist nicht • ist vor • ist am oder vor • ist nach • ist am oder nach	Uhrzeit und Datum der Aufnahme des Objekts. **Hinweis:** Um Ressourcenprobleme beim Aktivieren einer neuen ILM-Richtlinie zu vermeiden, können Sie den erweiterten Filter „Aufnahmezeit“ in jeder Regel verwenden, die den Speicherort einer großen Anzahl vorhandener Objekte ändern könnte. Legen Sie die Aufnahmezeit so fest, dass sie größer oder gleich der ungefähren Zeit ist, zu der die neue Richtlinie in Kraft tritt, um sicherzustellen, dass vorhandene Objekte nicht unnötig verschoben werden.
Schlüssel	• gleich • ist nicht gleich • enthält • enthält nicht • beginnt mit • beginnt nicht mit • endet mit • endet nicht mit	Der gesamte oder ein Teil eines eindeutigen S3-Objektschlüssels. Beispielsweise möchten Sie möglicherweise Objekte abgleichen, die mit enden `.txt` oder beginnen Sie mit `test-object/` .
Letzter Zugriffszeitpunkt	• Ist • ist nicht • ist vor • ist am oder vor • ist nach • ist am oder nach	Uhrzeit und Datum des letzten Abrufs (Lesens oder Anzeigens) des Objekts. **Hinweis:** Wenn Sie planen,"letzte Zugriffszeit verwenden" Als erweiterter Filter müssen Aktualisierungen der letzten Zugriffszeit für den S3-Bucket aktiviert werden.

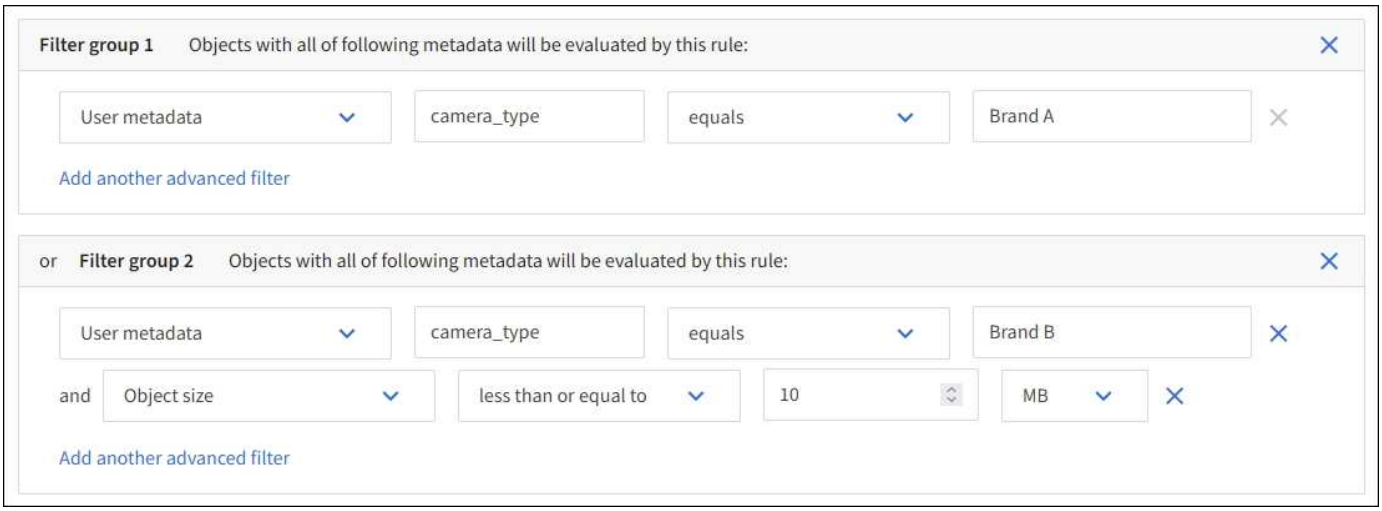
Metadatentyp	Unterstützte Operatoren	Metadatenwert
Standortbeschränkung (nur S3)	• gleich • ist nicht gleich	Die Region, in der ein S3-Bucket erstellt wurde. Verwenden Sie **ILM** > **Regionen**, um die angezeigten Regionen zu definieren. **Hinweis:** Ein Wert von us-east-1 entspricht Objekten in Buckets, die in der Region us-east-1 erstellt wurden, sowie Objekten in Buckets, für die keine Region angegeben ist. Sehen "Regionen konfigurieren (optional und nur S3)" .
Objektgröße	• gleich • ist nicht gleich • weniger als • kleiner oder gleich • größer als • größer oder gleich	Die Größe des Objekts. Erasure Coding eignet sich am besten für Objekte, die größer als 1 MB sind. Verwenden Sie Erasure Coding nicht für Objekte, die kleiner als 200 KB sind, um den Verwaltungsaufwand für sehr kleine Erasure-Coding-Fragmente zu vermeiden.
Benutzermetadaten	• enthält • endet mit • gleich • existiert • beginnt mit • enthält nicht • endet nicht mit • ist nicht gleich • existiert nicht • beginnt nicht mit	Schlüssel-Wert-Paar, wobei **Benutzermetadatenname** der Schlüssel und **Metadatenwert** der Wert ist. Um beispielsweise nach Objekten zu filtern, die Benutzermetadaten von `color=blue` , geben Sie an `color` für **Benutzermetadatenname**, `equals` für den Betreiber und `blue` für **Metadatenwert**. **Hinweis:** Bei Benutzermetadatennamen wird die Groß-/Kleinschreibung nicht beachtet; bei Benutzermetadatenwerten hingegen schon.
Objekt-Tag (nur S3)	• enthält • endet mit • gleich • existiert • beginnt mit • enthält nicht • endet nicht mit • ist nicht gleich • existiert nicht • beginnt nicht mit	Schlüssel-Wert-Paar, wobei **Objekt-Tag-Name** der Schlüssel und **Objekt-Tag-Wert** der Wert ist. Um beispielsweise nach Objekten zu filtern, die den Objekttag `Image=True` , geben Sie an `Image` für **Objekt-Tag-Name**, `equals` für den Betreiber und `True` für **Objekt-Tag-Wert**. **Hinweis:** Bei Objekt-Tag-Namen und Objekt-Tag-Werten wird zwischen Groß- und Kleinschreibung unterschieden. Sie müssen diese Elemente genau so eingeben, wie sie für das Objekt definiert wurden.

Angeben mehrerer Metadatentypen und -werte

Wenn Sie erweiterte Filter definieren, können Sie mehrere Metadatentypen und mehrere Metadatenwerte angeben. Wenn Sie beispielsweise möchten, dass eine Regel auf Objekte mit einer Größe zwischen 10 MB und 100 MB zutrifft, wählen Sie den Metadatentyp **Objektgröße** aus und geben zwei Metadatenwerte an.

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

Durch die Verwendung mehrerer Einträge haben Sie eine genaue Kontrolle darüber, welche Objekte abgeglichen werden. Im folgenden Beispiel gilt die Regel für Objekte, die als Wert der Benutzermetadaten „camera_type“ die Marke A oder Marke B haben. Die Regel gilt jedoch nur für Objekte der Marke B, die kleiner als 10 MB sind.



Schritt 2 von 3: Platzierungen definieren

Im Schritt **Platzierungen definieren** des Assistenten „ILM-Regel erstellen“ können Sie die Platzierungsanweisungen definieren, die bestimmen, wie lange Objekte gespeichert werden, welche Art von Kopien (repliziert oder löschcodiert), welcher Speicherort und wie viele Kopien es sein sollen.

> Bei den gezeigten Screenshots handelt es sich um Beispiele. Ihre Ergebnisse können je nach Ihrer StorageGRID -Version variieren.

Informationen zu diesem Vorgang

Eine ILM-Regel kann eine oder mehrere Platzierungsanweisungen enthalten. Jede Platzierungsanweisung gilt jeweils für einen Zeitraum. Wenn Sie mehr als eine Anweisung 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 Platzierungsanweisung kann mehrere Zeilen umfassen, wenn Sie verschiedene Arten von Kopien erstellen oder während dieses Zeitraums verschiedene Standorte verwenden möchten.

In diesem Beispiel speichert die ILM-Regel für das erste Jahr eine replizierte Kopie an Standort 1 und eine replizierte Kopie an Standort 2. Nach einem Jahr wird eine 2+1-Löschcode-Kopie erstellt und nur an einem Standort gespeichert.

Schritte

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

Option	Beschreibung
Aufnahmezeit	Der Zeitpunkt, zu dem das Objekt aufgenommen wurde.
Letzter Zugriffszeitpunkt	Der Zeitpunkt, zu dem das Objekt zuletzt abgerufen (gelesen oder angezeigt) wurde. Um diese Option zu verwenden, müssen Aktualisierungen der letzten Zugriffszeit für den S3-Bucket aktiviert werden. Weitere Informationen finden Sie unter "Verwenden der letzten Zugriffszeit in ILM-Regeln" .
Benutzerdefinierte Erstellungszeit	Eine in benutzerdefinierten Metadaten angegebene Zeit.
Nicht aktuelle Zeit	"Nicht aktuelle Zeit" wird automatisch ausgewählt, wenn Sie **Ja** für die Frage "Diese Regel nur auf ältere Objektversionen anwenden (in S3-Buckets mit aktivierter Versionierung)?" in"Schritt 1 des Assistenten „ILM-Regel erstellen“" .

   Wenn Sie eine *konforme* Regel erstellen möchten, müssen Sie **Aufnahmezeit** auswählen. Weitere Informationen finden Sie unter "Verwalten von Objekten mit S3 Object Lock" .

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

   Sie möchten beispielsweise angeben, wo Objekte im ersten Jahr gespeichert werden sollen (*Ab Tag 0 365 Tage lang speichern*). Mindestens eine Anweisung muss am Tag 0 beginnen.

3. Wenn Sie replizierte Kopien erstellen möchten:
   a. Wählen Sie aus der Dropdown-Liste **Objekte speichern nach** die Option **Replikation** aus.
   b. Wählen Sie die Anzahl der Kopien aus, die Sie erstellen möchten.

      Wenn Sie die Anzahl der Kopien auf 1 ändern, wird eine Warnung angezeigt. Eine ILM-Regel, die für einen bestimmten Zeitraum nur eine replizierte Kopie erstellt, birgt das Risiko eines dauerhaften Datenverlusts. Weitere Informationen finden Sie unter "Warum Sie keine Einzelkopiereplikation verwenden sollten" .

      Um das Risiko zu vermeiden, führen Sie eine oder mehrere der folgenden Aktionen aus:

      - Erhöhen Sie die Anzahl der Kopien für den Zeitraum.

- Fügen Sie Kopien zu anderen Speicherpools oder einem Cloud-Speicherpool hinzu.
- Wählen Sie **Erasure Coding** anstelle von **Replikation**.

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

c. Wählen Sie im Feld **Kopien auf** die Speicherpools aus, die Sie hinzufügen möchten.

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

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

   Wenn Sie mehr als einen Speicherpool angeben, beachten Sie die folgenden Regeln:

   - Die Anzahl der Kopien kann nicht größer sein als die Anzahl der Speicherpools.
   - Wenn die Anzahl der Kopien der Anzahl der Speicherpools entspricht, wird in jedem Speicherpool eine Kopie des Objekts gespeichert.
   - Wenn die Anzahl der Kopien geringer ist als die Anzahl der Speicherpools, wird eine Kopie am Aufnahmestandort gespeichert. Anschließend verteilt das System die verbleibenden Kopien, um die Festplattennutzung auf die Pools auszubalancieren und gleichzeitig sicherzustellen, dass kein Standort mehr als eine Kopie eines Objekts erhält.
   - Wenn sich die Speicherpools überschneiden (dieselben Speicherknoten enthalten), werden alle Kopien des Objekts möglicherweise nur an einem Standort gespeichert. Geben Sie aus diesem Grund nicht den Speicherpool „Alle Speicherknoten“ (StorageGRID 11.6 und früher) und einen anderen Speicherpool an.

4. Wenn Sie eine löschcodierte Kopie erstellen möchten:

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

      Erasure Coding eignet sich am besten für Objekte, die größer als 1 MB sind. Verwenden Sie Erasure Coding nicht für Objekte, die kleiner als 200 KB sind, um den Verwaltungsaufwand für sehr kleine Erasure-Coding-Fragmente zu vermeiden.

   b. Wenn Sie keinen Objektgrößenfilter für einen Wert größer als 200 KB hinzugefügt haben, wählen Sie **Zurück**, um zu Schritt 1 zurückzukehren. Wählen Sie dann **Erweiterten Filter hinzufügen** und legen Sie einen **Objektgrößen**-Filter auf einen Wert größer als 200 KB fest.

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

      Der Speicherort für eine Erasure-Coded-Kopie umfasst den Namen des Erasure-Coding-Schemas, gefolgt vom Namen des Speicherpools.

   Die verfügbaren Erasure-Coding-Schemata sind durch die Anzahl der Speicherknoten im von Ihnen ausgewählten Speicherpool begrenzt. A `Recommended` Das Abzeichen erscheint neben den Schemata, die entweder die"bester Schutz oder geringster Speicheraufwand" .

5. Optional:

a. Wählen Sie **Anderen Typ oder Speicherort hinzufügen**, um zusätzliche Kopien an anderen Speicherorten zu erstellen.

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

> Das Löschen von Objekten erfolgt auf Grundlage der folgenden Einstellungen:
>
> - Objekte werden am Ende des letzten Zeitraums automatisch gelöscht, sofern nicht ein anderer Zeitraum mit **für immer** endet.
> - Je nach"Bucket- und Tenant-Aufbewahrungsdauereinstellungen" , werden Objekte möglicherweise nicht gelöscht, selbst wenn die ILM-Aufbewahrungsfrist endet.

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

a. Wählen Sie in der Dropdownliste **Objekte speichern nach** die Option **Replikation** aus.

b. Wählen Sie das Feld **Kopien auf** und dann einen Cloud-Speicherpool aus.

Beachten Sie bei der Verwendung von Cloud-Speicherpools die folgenden Regeln:

- Sie können in einer einzelnen Platzierungsanweisung nicht mehr als einen Cloud-Speicherpool auswählen. Ebenso können Sie in derselben Platzierungsanweisung keinen Cloud-Speicherpool und keinen Speicherpool auswählen.
- Sie können in einem bestimmten Cloud-Speicherpool nur eine Kopie eines Objekts speichern. Wenn Sie **Kopien** auf 2 oder mehr einstellen, wird eine Fehlermeldung angezeigt.
- Sie können in keinem Cloud-Speicherpool gleichzeitig mehr als eine Objektkopie speichern. Eine Fehlermeldung wird angezeigt, wenn mehrere Platzierungen, die einen Cloud-Speicherpool verwenden, überlappende Daten aufweisen oder wenn mehrere Zeilen in derselben Platzierung einen Cloud-Speicherpool verwenden.
- Sie können ein Objekt in einem Cloud-Speicherpool speichern, während das Objekt gleichzeitig als replizierte oder löschcodierte Kopie in StorageGRID gespeichert wird. Allerdings müssen Sie in der Platzierungsanweisung für den Zeitraum mehrere Zeilen angeben, damit Sie für jeden Standort die Anzahl und Art der Kopien festlegen können.

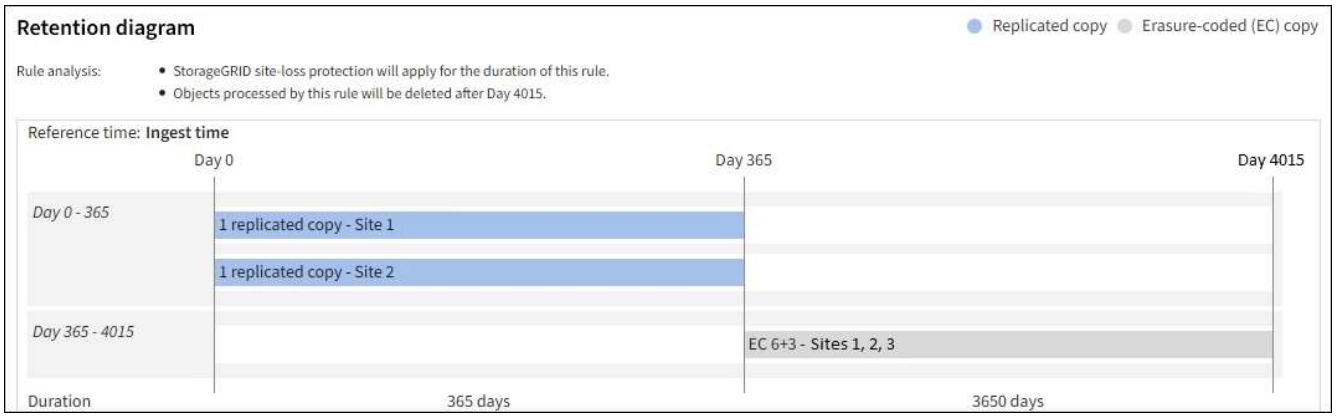
7. Bestätigen Sie im Retentionsdiagramm Ihre Platzierungsanweisungen.

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

Im Abschnitt „Regelanalyse“ des Retention-Diagramms heißt es:

- Für die Dauer dieser Regelung gilt der Site-Loss-Schutz von StorageGRID .
- Von dieser Regel verarbeitete Objekte werden nach Tag 4015 gelöscht.

Siehe "Aktivieren Sie den Site-Loss-Schutz."



8. Wählen Sie **Weiter**. "Schritt 3 (Aufnahmeverhalten auswählen)"des Assistenten „ILM-Regel erstellen“ wird angezeigt.

Verwenden der letzten Zugriffszeit in ILM-Regeln

Sie können die letzte Zugriffszeit als Referenzzeit in einer ILM-Regel verwenden. Beispielsweise möchten Sie möglicherweise Objekte, die in den letzten drei Monaten angezeigt wurden, auf lokalen Speicherknoten belassen und Objekte, die nicht so kürzlich angezeigt wurden, an einen externen Standort verschieben. Sie können die letzte Zugriffszeit auch als erweiterten Filter verwenden, wenn eine ILM-Regel nur auf Objekte angewendet werden soll, auf die zuletzt an einem bestimmten Datum zugegriffen wurde.

Informationen zu diesem Vorgang

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

- Wenn Sie die letzte Zugriffszeit als Referenzzeit verwenden, beachten Sie, dass das Ändern der letzten Zugriffszeit für ein Objekt keine sofortige ILM-Auswertung auslöst. Stattdessen werden die Platzierungen des Objekts bewertet und das Objekt wird nach Bedarf verschoben, wenn ILM das Objekt im Hintergrund auswertet. Dies kann nach dem Zugriff auf das Objekt zwei Wochen oder länger dauern.

  Berücksichtigen Sie diese Latenz beim Erstellen von ILM-Regeln basierend auf der letzten Zugriffszeit und vermeiden Sie Platzierungen mit kurzen Zeiträumen (weniger als ein Monat).

- Wenn Sie die letzte Zugriffszeit als erweiterten Filter oder als Referenzzeit verwenden, müssen Sie die Aktualisierung der letzten Zugriffszeit für S3-Buckets aktivieren. Sie können die"Mietermanager" oder die"Mandantenverwaltungs-API" .

  Aktualisierungen der letzten Zugriffszeit sind für S3-Buckets standardmäßig deaktiviert.

  Beachten Sie, dass die Aktivierung von Updates zur letzten Zugriffszeit die Leistung beeinträchtigen kann, insbesondere in Systemen mit kleinen Objekten. Die Leistungseinbußen entstehen dadurch, dass StorageGRID die Objekte bei jedem Abrufen mit neuen Zeitstempeln aktualisieren muss.

In der folgenden Tabelle ist zusammengefasst, ob die letzte Zugriffszeit für alle Objekte im Bucket für verschiedene Arten von Anforderungen aktualisiert wird.

Art der Anfrage	Ob die Zeit des letzten Zugriffs aktualisiert wird, wenn die Aktualisierung der Zeit des letzten Zugriffs deaktiviert ist	Ob die Zeit des letzten Zugriffs aktualisiert wird, wenn die Aktualisierung der Zeit des letzten Zugriffs aktiviert ist
Anforderung zum Abrufen eines Objekts, seiner Zugriffskontrollliste oder seiner Metadaten	Nein	Ja
Anforderung zum Aktualisieren der Metadaten eines Objekts	Ja	Ja
Anforderung zum Kopieren eines Objekts von einem Bucket in einen anderen	• Nein, für die Quellkopie • Ja, für die Zielkopie	• Ja, für die Quellkopie • Ja, für die Zielkopie
Anfrage zum Abschließen eines mehrteiligen Uploads	Ja, für das montierte Objekt	Ja, für das montierte Objekt

Schritt 3 von 3: Aufnahmeverhalten auswählen

Im Schritt **Aufnahmeverhalten auswählen** des Assistenten „ILM-Regel erstellen“ können Sie auswählen, wie die durch diese Regel gefilterten Objekte bei der Aufnahme geschützt werden.

Informationen zu diesem Vorgang

StorageGRID kann Zwischenkopien erstellen und die Objekte für eine spätere ILM-Auswertung in die Warteschlange stellen oder Kopien erstellen, um die Platzierungsanweisungen der Regel sofort zu erfüllen.

Schritte

1. Wählen Sie die"Aufnahmeverhalten" zu verwenden.

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

   > Sie können die Option „Ausgewogen“ oder „Streng“ nicht verwenden, wenn die Regel eine dieser Platzierungen verwendet:
   >
   > - Ein Cloud-Speicherpool am Tag 0
   > - Ein Cloud-Speicherpool, wenn die Regel eine benutzerdefinierte Erstellungszeit als Referenzzeit verwendet
   >
   > Sehen "Beispiel 5: ILM-Regeln und -Richtlinien für striktes Aufnahmeverhalten" .

2. Wählen Sie **Erstellen**.

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

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

Erstellen einer ILM-Standardregel

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

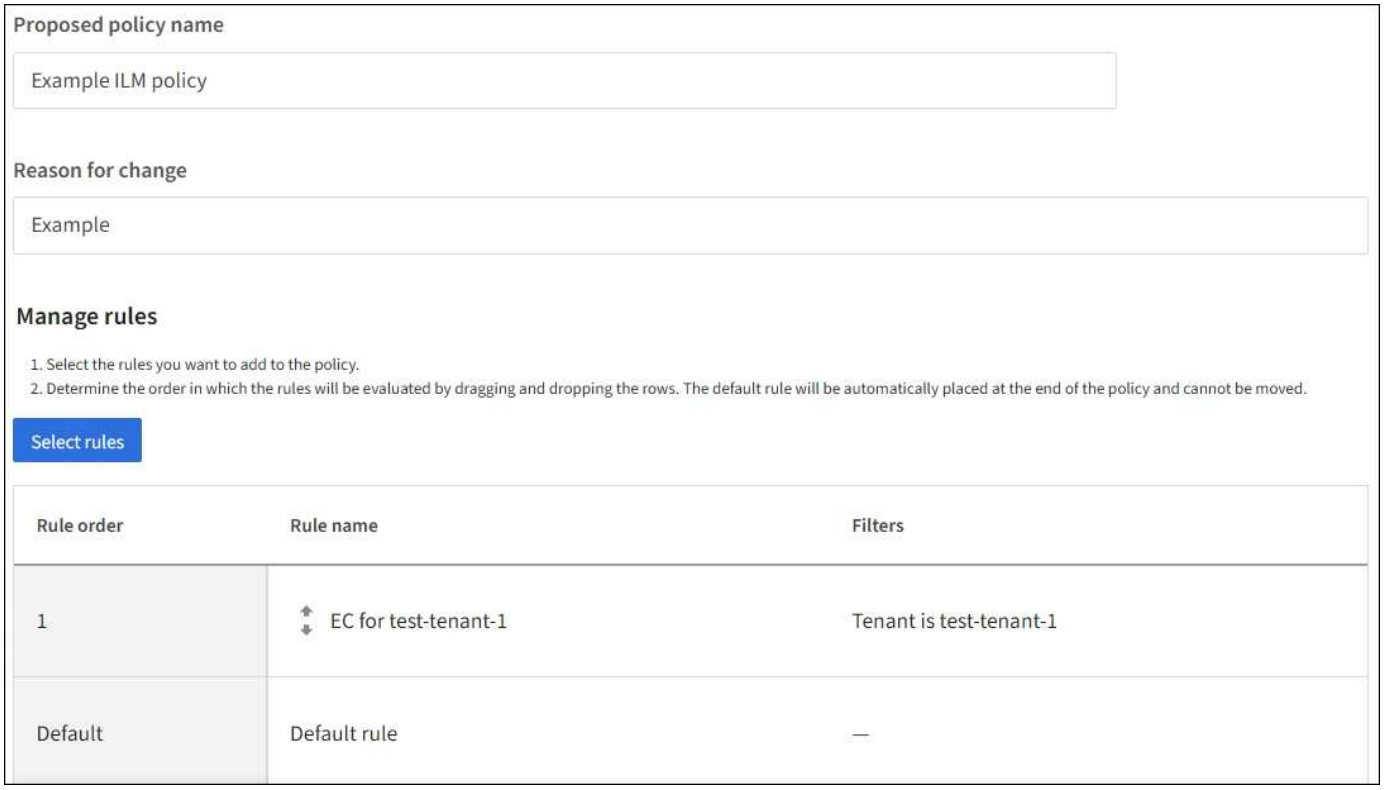
Bevor Sie beginnen

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

Informationen zu diesem Vorgang

Die Standardregel ist die letzte Regel, die in einer ILM-Richtlinie ausgewertet wird, daher kann sie keine Filter verwenden. Die Platzierungsanweisungen für die Standardregel werden auf alle Objekte angewendet, die keiner anderen Regel in der Richtlinie entsprechen.

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



Beachten Sie beim Erstellen der Standardregel die folgenden Anforderungen:

- Die Standardregel wird automatisch als letzte Regel platziert, wenn Sie sie einer Richtlinie hinzufügen.
- Die Standardregel kann keine grundlegenden oder erweiterten Filter verwenden.
- Die Standardregel muss für alle Objektversionen gelten.
- Die Standardregel sollte replizierte Kopien erstellen.

Verwenden Sie keine Regel, die Erasure-Coded-Kopien erstellt, als Standardregel für eine Richtlinie. Erasure-Coding-Regeln sollten einen erweiterten Filter verwenden, um zu verhindern, dass kleinere Objekte mit Erasure-Coding behandelt werden.

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

Schritte

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

   Schritt 1 (Details eingeben) des Assistenten „ILM-Regel erstellen“ wird angezeigt.

3. Geben Sie im Feld **Regelname** 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 für alle Mandantenkonten gelten.

6. Belassen Sie die Dropdown-Auswahl „Bucket-Name“ auf **gilt für alle Buckets**.

   Die Standardregel muss für alle S3-Buckets gelten.

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

   Die Standardregel kann keine Filter angeben.

9. Wählen Sie **Weiter**.

   Schritt 2 (Platzierungen definieren) wird angezeigt.

10. Wählen Sie für die Referenzzeit eine beliebige Option aus.

    Wenn Sie die Standardantwort **Nein** auf die Frage „Diese Regel nur auf ältere Objektversionen anwenden?“ beibehalten haben, Nicht aktuelle Zeiten werden nicht in die Pulldown-Liste aufgenommen. Die Standardregel muss für alle Objektversionen gelten.

11. Geben Sie die Platzierungsanweisungen für die Standardregel an.
    - Die Standardregel sollte Objekte für immer behalten. Wenn Sie eine neue Richtlinie aktivieren und die Standardregel Objekte nicht für immer beibehält, wird eine Warnung angezeigt. Sie müssen bestätigen, dass dies das von Ihnen erwartete Verhalten ist.
    - Die Standardregel sollte replizierte Kopien erstellen.

Verwenden Sie keine Regel, die Erasure-Coded-Kopien erstellt, als Standardregel für eine Richtlinie. Erasure-Coding-Regeln sollten den erweiterten Filter **Objektgröße (MB) größer als 200 KB** enthalten, um zu verhindern, dass kleinere Objekte einem Erasure-Coding unterzogen werden.

- Wenn Sie die globale S3-Objektsperreinstellung verwenden (oder aktivieren möchten), muss die Standardregel konform sein:
  - Es müssen mindestens zwei replizierte Objektkopien oder eine Erasure-Coded-Kopie erstellt werden.
  - Diese Kopien müssen für die gesamte Dauer jeder Zeile in den Platzierungsanweisungen auf den Speicherknoten vorhanden sein.
  - Objektkopien können nicht in einem Cloud-Speicherpool gespeichert werden.
  - Mindestens eine Zeile der Platzierungsanweisungen muss am Tag 0 beginnen, wobei die Aufnahmezeit als Referenzzeit verwendet wird.
  - Mindestens eine Zeile der Platzierungsanweisungen muss „für immer“ lauten.

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

    Schritt 3 (Aufnahmeverhalten auswählen) wird angezeigt.

14. Wählen Sie die zu verwendende Aufnahmeoption und wählen Sie **Erstellen**.

Verwalten von ILM-Richtlinien

Verwenden von ILM-Richtlinien

Eine Richtlinie für das Information Lifecycle Management (ILM) ist ein geordneter Satz von ILM-Regeln, der bestimmt, wie das StorageGRID -System Objektdaten im Laufe der Zeit verwaltet.

> Eine falsch konfigurierte ILM-Richtlinie kann zu einem nicht wiederherstellbaren Datenverlust führen. Bevor Sie eine ILM-Richtlinie aktivieren, überprüfen Sie die ILM-Richtlinie und ihre ILM-Regeln sorgfältig und simulieren Sie dann die ILM-Richtlinie. Stellen Sie immer sicher, dass die ILM-Richtlinie wie vorgesehen funktioniert.

Standard-ILM-Richtlinie

Wenn Sie StorageGRID installieren und Sites hinzufügen, wird automatisch eine Standard-ILM-Richtlinie wie folgt erstellt:

- Wenn Ihr Raster eine Site enthält, enthält die Standardrichtlinie eine Standardregel, die zwei Kopien jedes Objekts an dieser Site repliziert.
- Wenn Ihr Raster mehr als eine Site enthält, repliziert die Standardregel eine Kopie jedes Objekts an jeder Site.

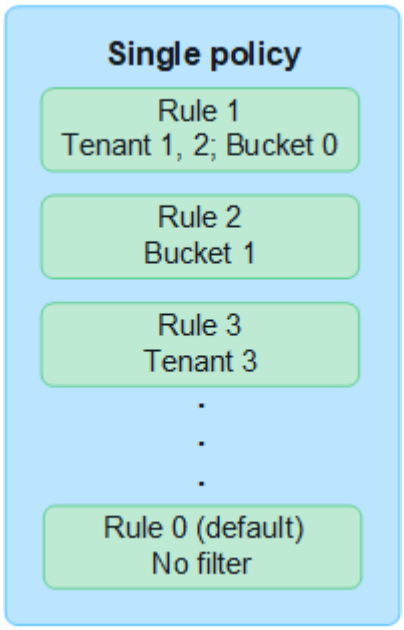
Wenn die Standardrichtlinie Ihren Speicheranforderungen nicht entspricht, können Sie Ihre eigenen Regeln und Richtlinien erstellen. Sehen"Erstellen einer ILM-Regel" Und"Erstellen einer ILM-Richtlinie" .

Eine oder mehrere aktive ILM-Richtlinien?

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

Eine Richtlinie

Wenn Ihr Grid ein einfaches Datenschutzschema mit wenigen mandanten- und bucketspezifischen Regeln verwendet, verwenden Sie eine einzelne aktive ILM-Richtlinie. Die ILM-Regeln können Filter enthalten, um verschiedene Buckets oder Mandanten zu verwalten.



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

Mehrere Richtlinien

Um den Mietern unterschiedliche Servicequalitätsoptionen bereitzustellen, können Sie mehrere aktive Richtlinien gleichzeitig haben. Jede Richtlinie kann bestimmte Mandanten, S3-Buckets und Objekte verwalten. Wenn Sie eine Richtlinie für einen bestimmten Satz von Mandanten oder Objekten anwenden oder ändern, sind die auf andere Mandanten und Objekte angewendeten Richtlinien davon nicht betroffen.

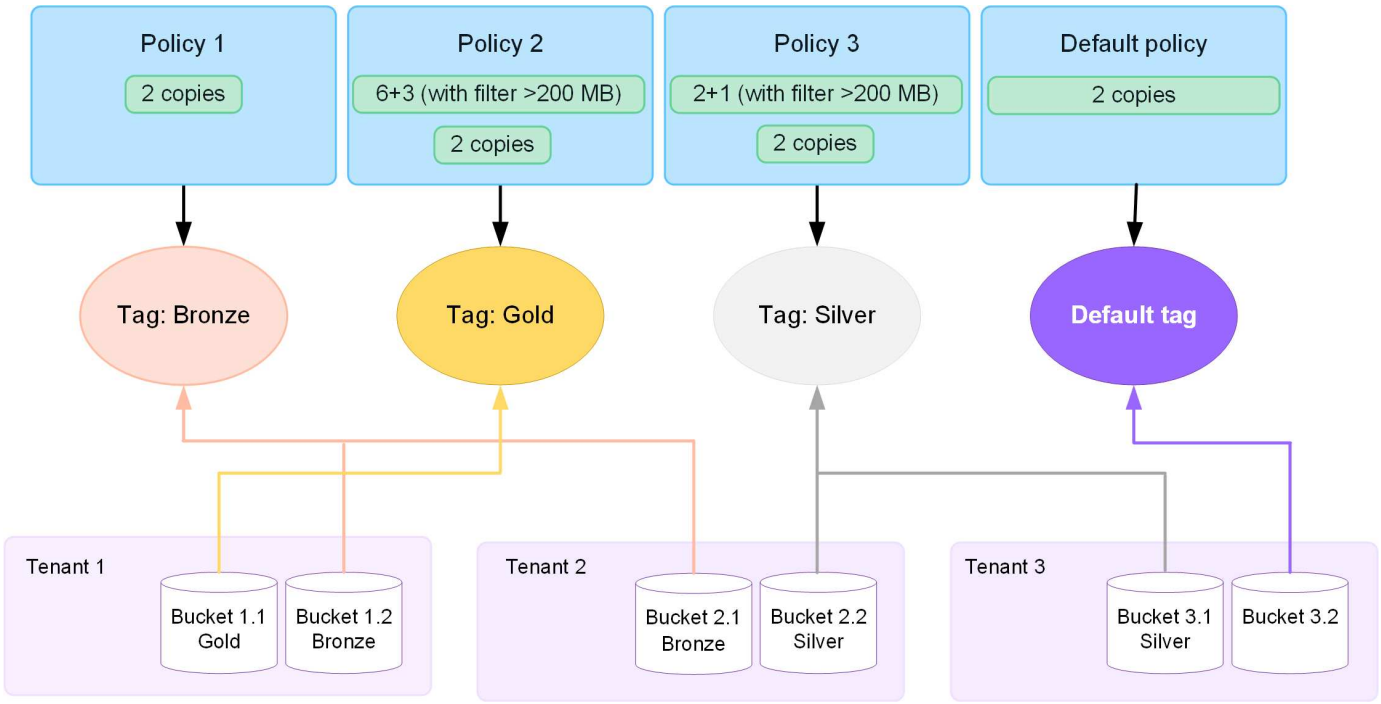
ILM-Richtlinientags

Wenn Sie es Mandanten ermöglichen möchten, problemlos zwischen mehreren Datenschutzrichtlinien pro Bucket zu wechseln, verwenden Sie mehrere ILM-Richtlinien mit *ILM-Richtlinien-Tags*. Sie weisen jeder ILM-Richtlinie ein Tag zu, und anschließend markieren Mandanten einen Bucket, um die Richtlinie auf diesen Bucket anzuwenden. Sie können ILM-Richtlinien-Tags nur auf S3-Buckets festlegen.

Sie könnten beispielsweise drei Tags mit den Namen „Gold“, „Silber“ und „Bronze“ haben. Sie können jedem Tag eine ILM-Richtlinie zuweisen, basierend darauf, wie lange und wo diese Richtlinie Objekte speichert. Mieter können durch Markieren ihrer Buckets auswählen, welche Richtlinie verwendet werden soll. Ein Bucket mit der Kennzeichnung „Gold“ wird durch die Gold-Richtlinie verwaltet und erhält die Datenschutz- und Leistungsstufe „Gold“.

Standard-ILM-Richtlinientag

Bei der Installation von StorageGRID wird automatisch ein standardmäßiges ILM-Richtlinientag erstellt. Jedes Raster muss über eine aktive Richtlinie verfügen, die dem Standardtag zugewiesen ist. Die Standardrichtlinie gilt für alle nicht markierten S3-Buckets.



Wie bewertet eine ILM-Richtlinie Objekte?

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

Wenn Clients Objekte in StorageGRID speichern, werden die Objekte anhand des geordneten Satzes von ILM-Regeln in der Richtlinie wie folgt ausgewertet:

1. Wenn die Filter für die erste Regel in der Richtlinie mit einem Objekt übereinstimmen, wird das Objekt gemäß dem Aufnahmeverhalten dieser Regel aufgenommen und gemäß den Platzierungsanweisungen 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 gefunden wird.
3. Wenn keine Regeln mit einem Objekt übereinstimmen, werden das Aufnahmeverhalten und die Platzierungsanweisungen für die Standardregel in der Richtlinie angewendet. Die Standardregel ist die letzte Regel in einer Richtlinie. Die Standardregel muss für alle Mandanten, alle S3-Buckets und alle Objektversionen gelten und darf keine erweiterten Filter verwenden.

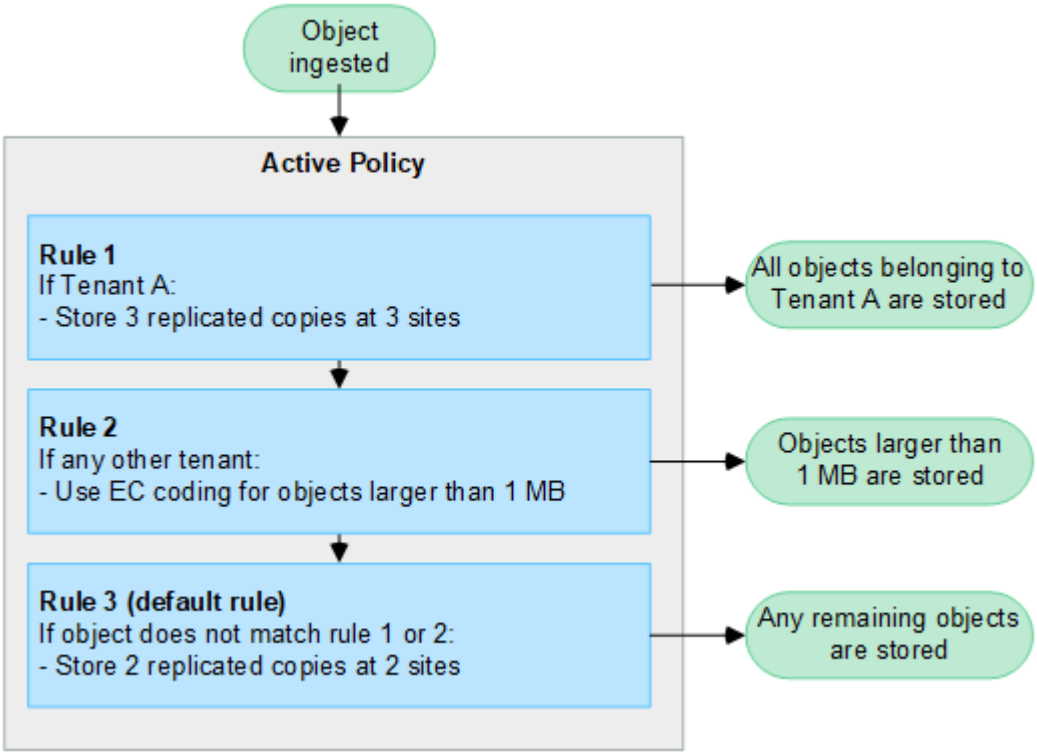
Beispiel einer ILM-Richtlinie

Beispielsweise könnte eine ILM-Richtlinie drei ILM-Regeln enthalten, die Folgendes festlegen:

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

- Stimmt nicht mit Objekten überein, die 1 MB oder kleiner sind. Daher werden diese Objekte anhand von Regel 3 ausgewertet.

- **Regel 3: 2 Kopien, 2 Rechenzentren** (Standard)
  - Ist die letzte und Standardregel in der Richtlinie. Verwendet keine Filter.
  - Erstellen Sie zwei replizierte Kopien aller Objekte, die nicht mit Regel 1 oder Regel 2 übereinstimmen (Objekte, die nicht zu Mandant A gehören und 1 MB oder kleiner sind).



Was sind aktive und inaktive Richtlinien?

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

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

Wenn Sie eine ILM-Richtlinie aktivieren, verwendet StorageGRID diese Richtlinie zum Verwalten aller Objekte, einschließlich vorhandener und neu aufgenommener Objekte. Vorhandene Objekte werden möglicherweise an neue Speicherorte verschoben, wenn die ILM-Regeln in der neuen Richtlinie implementiert werden.

Wenn Sie mehrere ILM-Richtlinien gleichzeitig aktivieren und Mandanten Richtlinien-Tags auf S3-Buckets anwenden, werden die Objekte in jedem Bucket entsprechend der dem Tag zugewiesenen Richtlinie verwaltet.

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

Überlegungen zum Erstellen einer ILM-Richtlinie

- Verwenden Sie in Testsystemen nur die vom System bereitgestellte Richtlinie „Baseline 2-Kopienrichtlinie“. Für StorageGRID 11.6 und früher verwendet die Regel „2 Kopien erstellen“ in dieser Richtlinie den

Speicherpool „Alle Speicherknoten“, der alle Sites enthält. Wenn Ihr StorageGRID -System über mehr als einen Standort verfügt, können zwei Kopien eines Objekts am selben Standort platziert werden.

> Der Speicherpool „Alle Speicherknoten“ wird während der Installation von StorageGRID 11.6 und früher automatisch erstellt. Wenn Sie auf eine neuere Version von StorageGRID aktualisieren, bleibt der Pool „Alle Speicherknoten“ weiterhin vorhanden. Wenn Sie StorageGRID 11.7 oder höher als Neuinstallation installieren, wird der Pool „Alle Speicherknoten“ nicht erstellt.

- Berücksichtigen Sie beim Entwerfen einer neuen Richtlinie alle verschiedenen Objekttypen, die in Ihr Raster aufgenommen werden könnten. Stellen Sie sicher, dass die Richtlinie Regeln zum Abgleichen und Platzieren dieser Objekte nach Bedarf enthält.
- Halten Sie die ILM-Richtlinie so einfach wie möglich. Dadurch werden potenziell gefährliche Situationen vermieden, in denen Objektdaten nicht wie vorgesehen geschützt sind, wenn im Laufe der Zeit Änderungen am StorageGRID -System vorgenommen werden.
- Stellen Sie sicher, dass die Regeln in der Richtlinie in der richtigen Reihenfolge stehen. Wenn die Richtlinie aktiviert ist, werden neue und vorhandene Objekte von den Regeln in der aufgeführten Reihenfolge (von oben beginnend) ausgewertet. Wenn beispielsweise die erste Regel in einer Richtlinie mit einem Objekt übereinstimmt, wird dieses Objekt von keiner anderen Regel ausgewertet.
- Die letzte Regel in jeder ILM-Richtlinie ist die Standard-ILM-Regel, die keine Filter verwenden kann. Wenn ein Objekt keiner anderen Regel entspricht, 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 Standorts eines vorhandenen Objekts kann zu vorübergehenden Ressourcenproblemen führen, wenn die neuen Platzierungen ausgewertet und implementiert werden.

Erstellen von ILM-Richtlinien

Erstellen Sie eine oder mehrere ILM-Richtlinien, um Ihre Servicequalitätsanforderungen zu erfüllen.

Wenn Sie über eine aktive ILM-Richtlinie verfügen, können Sie dieselben ILM-Regeln auf alle Mandanten und Buckets anwenden.

Wenn Sie über mehrere aktive ILM-Richtlinien verfügen, können Sie die entsprechenden ILM-Regeln auf bestimmte Mandanten und Buckets anwenden, um mehrere Servicequalitätsanforderungen zu erfüllen.

Erstellen einer ILM-Richtlinie

Informationen zu diesem Vorgang

Bevor Sie Ihre eigene Richtlinie erstellen, überprüfen Sie, ob die"Standard-ILM-Richtlinie" entspricht nicht Ihren Speicheranforderungen.

> Verwenden Sie in Testsystemen nur die vom System bereitgestellten Richtlinien, 2 Kopien der Richtlinie (für Grids mit einem Standort) oder 1 Kopie pro Standort (für Grids mit mehreren Standorten). Für StorageGRID 11.6 und früher verwendet die Standardregel in dieser Richtlinie den Speicherpool „Alle Speicherknoten“, der alle Sites enthält. Wenn Ihr StorageGRID -System über mehr als einen Standort verfügt, können zwei Kopien eines Objekts am selben Standort platziert werden.

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

Bevor Sie beginnen

- Sie sind beim Grid Manager angemeldet mit einem"unterstützter Webbrowser" .
- Sie haben die"erforderliche Zugriffsberechtigungen" .
- Du hast"erstellte ILM-Regeln" basierend darauf, ob S3 Object Lock aktiviert ist.

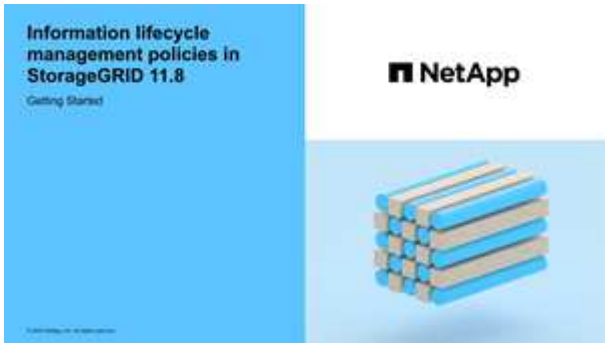
  S3-Objektsperre nicht aktiviert

  - Du hast"die ILM-Regeln erstellt" Sie der Richtlinie hinzufügen möchten. Bei Bedarf können Sie eine Richtlinie speichern, zusätzliche Regeln erstellen und dann die Richtlinie bearbeiten, um die neuen Regeln hinzuzufügen.
  - Du hast"eine Standard-ILM-Regel erstellt" das keine Filter enthält.

  S3-Objektsperre aktiviert

  - Der"Die globale S3-Objektsperreinstellung ist bereits aktiviert" für das StorageGRID -System.
  - Du hast"erstellte die konformen und nicht konformen ILM-Regeln" Sie der Richtlinie hinzufügen möchten. Bei Bedarf können Sie eine Richtlinie speichern, zusätzliche Regeln erstellen und dann die Richtlinie bearbeiten, um die neuen Regeln hinzuzufügen.
  - Du hast"eine Standard-ILM-Regel erstellt" für die konforme Richtlinie.

- Optional haben Sie das Video angesehen: "Video: Übersicht über ILM-Richtlinien"



Siehe auch "Verwenden von ILM-Richtlinien".

Schritte

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

   Wenn die globale Einstellung „S3 Object Lock“ aktiviert ist, wird auf der Seite „ILM-Richtlinien“ angezeigt, welche ILM-Regeln konform sind.

2. Bestimmen Sie, wie Sie die ILM-Richtlinie erstellen möchten.

Neue Richtlinie erstellen

a. Wählen Sie **Richtlinie erstellen**.

Vorhandene Richtlinie klonen

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

Vorhandene Richtlinie bearbeiten

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

3. Geben Sie im Feld **Richtlinienname** einen eindeutigen Namen für die Richtlinie ein.
4. Geben Sie optional im Feld **Grund für die Änderung** den Grund für die Erstellung einer neuen Richtlinie ein.
5. Um der Richtlinie Regeln hinzuzufügen, wählen Sie **Regeln auswählen**. Wählen Sie einen Regelnamen aus, um die Einstellungen für diese Regel anzuzeigen.

   Wenn Sie eine Richtlinie klonen:

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

S3-Objektsperre nicht aktiviert

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

   Die Standardregel gilt für alle Objekte, die keiner anderen Regel in der Richtlinie entsprechen. Die Standardregel kann keine Filter verwenden und wird immer zuletzt ausgewertet.

   > Verwenden Sie die Regel „2 Kopien erstellen“ nicht als Standardregel für eine Richtlinie. Die Regel „2 Kopien erstellen“ verwendet einen einzelnen Speicherpool, „Alle Speicherknoten“, der alle Sites enthält. Wenn Ihr StorageGRID -System über mehr als einen Standort verfügt, können zwei Kopien eines Objekts am selben Standort platziert werden.

S3-Objektsperre aktiviert

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

   Die Regelliste enthält nur die konformen Regeln und verwendet keine Filter.

   > Verwenden Sie die Regel „2 Kopien erstellen“ nicht als Standardregel für eine Richtlinie. Die Regel „2 Kopien erstellen“ verwendet einen einzelnen Speicherpool, „Alle Speicherknoten“, der alle Sites enthält. Wenn Sie diese Regel verwenden, können mehrere Kopien eines Objekts auf derselben Site platziert werden.

b. Wenn Sie eine andere „Standardregel“ für Objekte in nicht konformen S3-Buckets benötigen, wählen Sie **Eine Regel ohne Filter für nicht konforme S3-Buckets einschließen** und wählen Sie eine nicht konforme Regel aus, die keinen Filter verwendet.

   Beispielsweise möchten Sie möglicherweise einen Cloud-Speicherpool verwenden, um Objekte in Buckets zu speichern, für die S3 Object Lock nicht aktiviert ist.

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

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

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

   Im Fenster „Richtlinie erstellen“ werden nun die von Ihnen ausgewählten Regeln aufgelistet. Die Standardregel steht am Ende, die anderen Regeln darüber.

   Wenn S3 Object Lock aktiviert ist und Sie auch eine nicht konforme „Standardregel“ ausgewählt haben, wird diese Regel als vorletzte Regel in der Richtlinie hinzugefügt.

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

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

   Sie können die Standardregel nicht verschieben. Wenn die S3-Objektsperre aktiviert ist, können Sie die nicht konforme „Standard“-Regel auch nicht verschieben, falls eine solche ausgewählt wurde.

   Sie müssen bestätigen, dass die ILM-Regeln in der richtigen Reihenfolge sind. Wenn die Richtlinie aktiviert ist, werden neue und vorhandene Objekte von den Regeln in der aufgeführten Reihenfolge (von oben beginnend) ausgewertet.

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

Simulieren einer Richtlinie

Simulieren Sie eine Richtlinie an Testobjekten, bevor Sie die Richtlinie aktivieren und auf Ihre Produktionsdaten anwenden.

Bevor Sie beginnen

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

Schritte

1. Mithilfe eines S3-Clients oder der"S3-Konsole" , nehmen Sie die zum Testen jeder Regel erforderlichen Objekte auf.
2. Aktivieren Sie auf der Seite „ILM-Richtlinien“ das Kontrollkästchen für die Richtlinie und wählen Sie dann **Simulieren** aus.
3. Geben Sie im Feld **Objekt** den S3 ein `bucket/object-key` für ein Testobjekt. Beispiel: `bucket-01/filename.png` .
4. Wenn die S3-Versionierung aktiviert ist, geben Sie optional eine Versions-ID für das Objekt in das Feld **Versions-ID** ein.
5. Wählen Sie **Simulieren**.
6. Bestätigen Sie im Abschnitt „Simulationsergebnisse“, dass jedes Objekt der richtigen Regel entspricht.
7. Um festzustellen, welcher Speicherpool oder welches Erasure-Coding-Profil wirksam ist, wählen Sie den Namen der übereinstimmenden Regel aus, um zur Seite mit den Regeldetails zu gelangen.

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

Ergebnisse

Alle Änderungen an den Richtlinienregeln werden in den Simulationsergebnissen widergespiegelt und zeigen die neue und die vorherige Übereinstimmung an. Das Fenster „Richtlinie simulieren“ behält die von Ihnen getesteten Objekte bei, bis Sie entweder **Alle löschen** oder das Symbol „Entfernen“ auswählen ✕ für jedes Objekt in der Simulationsergebnisliste.

Ähnliche Informationen

"Beispielsimulationen für ILM-Richtlinien"

Aktivieren einer Richtlinie

Wenn Sie eine einzelne neue ILM-Richtlinie aktivieren, werden vorhandene und neu aufgenommene Objekte von dieser Richtlinie verwaltet. Wenn Sie mehrere Richtlinien aktivieren, bestimmen die den Buckets zugewiesenen ILM-Richtlinien-Tags die zu verwaltenden Objekte.

Bevor Sie eine neue Richtlinie aktivieren:

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

> ⚠ Fehler in einer ILM-Richtlinie können zu nicht wiederherstellbarem Datenverlust führen.

Informationen zu diesem Vorgang

Wenn Sie eine ILM-Richtlinie aktivieren, verteilt das System die neue Richtlinie an alle Knoten. Allerdings wird die neue aktive Richtlinie möglicherweise erst wirksam, wenn alle Grid-Knoten für den Empfang der neuen Richtlinie verfügbar sind. In einigen Fällen wartet das System mit der Implementierung einer neuen aktiven Richtlinie, um sicherzustellen, dass Rasterobjekte nicht versehentlich entfernt werden. Speziell:

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

Schritte

Befolgen Sie die Schritte zum Aktivieren einer oder mehrerer Richtlinien:

Aktivieren Sie eine Richtlinie

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

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

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

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

Mehrere Richtlinien aktivieren

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

> Wenn mehrere Tags verwendet werden und Mandanten Richtlinien-Tags häufig Buckets neu zuweisen, kann dies die Grid-Leistung beeinträchtigen. Wenn Sie nicht vertrauenswürdige Mandanten haben, sollten Sie in Erwägung ziehen, nur das Standard-Tag zu verwenden.

1. Wählen Sie **ILM** > **Richtlinien-Tags**.
2. Wählen Sie **Erstellen**.
3. Geben Sie im Dialogfeld „Richtlinientag erstellen“ einen Tagnamen und optional eine Beschreibung für das Tag ein.

   > Tag-Namen und -Beschreibungen sind für Mieter sichtbar. Wählen Sie Werte aus, die den Mandanten dabei helfen, eine fundierte Entscheidung zu treffen, wenn sie Richtlinien-Tags auswählen, die sie ihren Buckets zuweisen möchten. Wenn die zugewiesene Richtlinie beispielsweise das Löschen von Objekten nach einer bestimmten Zeit vorsieht, können Sie dies in der Beschreibung mitteilen. Geben Sie in diese Felder keine vertraulichen Informationen ein.

4. Wählen Sie **Tag erstellen**.
5. Wählen Sie in der Tabelle mit den ILM-Richtlinien-Tags im Pulldown-Menü eine Richtlinie aus, die dem Tag zugewiesen werden soll.
6. Wenn in der Spalte „Richtlinieneinschränkungen“ Warnungen angezeigt werden, wählen Sie

Richtliniendetails anzeigen aus, um die Richtlinie zu überprüfen.

7. Stellen Sie sicher, dass jede Richtlinie die Daten wie erwartet verwaltet.
8. Wählen Sie **Zugewiesene Richtlinien aktivieren**. Oder wählen Sie **Änderungen löschen**, um die Richtlinienzuweisung zu entfernen.
9. Lesen Sie im Dialogfeld „Richtlinien mit neuen Tags aktivieren“ die Beschreibungen, wie die einzelnen Tags, Richtlinien und Regeln Objekte verwalten. Nehmen Sie die erforderlichen Änderungen vor, um sicherzustellen, dass die Richtlinien die Objekte wie erwartet verwalten.
10. Wenn Sie sicher sind, dass Sie die Richtlinien aktivieren möchten, geben Sie **Ja** in das Textfeld ein und wählen Sie dann **Richtlinien aktivieren**.

Ähnliche Informationen

"Beispiel 6: Ändern einer ILM-Richtlinie"

Beispielsimulationen für ILM-Richtlinien

Die Beispiele für ILM-Richtliniensimulationen bieten Richtlinien zum Strukturieren und Ändern von Simulationen für Ihre Umgebung.

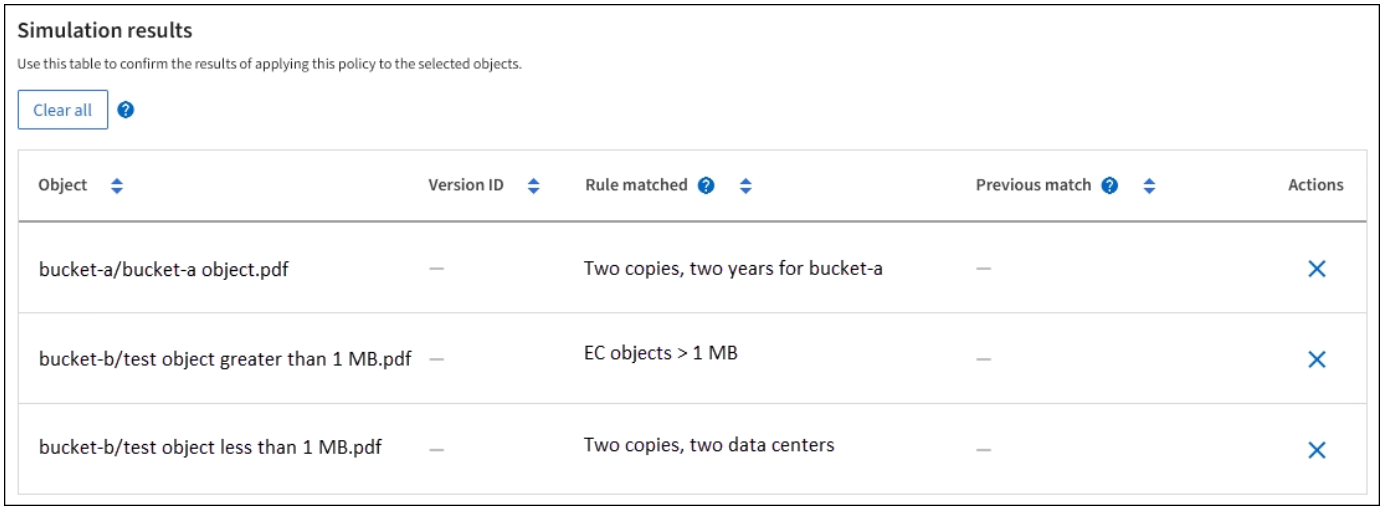
Beispiel 1: Regeln beim Simulieren einer ILM-Richtlinie überprüfen

In diesem Beispiel wird beschrieben, wie Regeln beim Simulieren einer Richtlinie überprüft werden.

In diesem Beispiel wird die **Beispiel-ILM-Richtlinie** anhand der aufgenommenen Objekte in zwei Buckets simuliert. Die Richtlinie umfasst die folgenden drei Regeln:

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

Bestätigen Sie nach der Simulation der Richtlinie, dass jedes Objekt der richtigen Regel entspricht.



In diesem Beispiel:

- `bucket-a/bucket-a object.pdf`stimmte mit der ersten Regel überein, die nach Objekten filtert in `bucket-a`.
- `bucket-b/test object greater than 1 MB.pdf`ist in `bucket-b`, also entsprach es nicht der ersten Regel. Stattdessen wurde es von der zweiten Regel, die nach Objekten größer als 1 MB filtert, korrekt abgeglichen.
- `bucket-b/test object less than 1 MB.pdf`stimmte nicht mit den Filtern in den ersten beiden Regeln überein, daher wird es durch die Standardregel platziert, die keine Filter enthält.

Beispiel 2: Regeln beim Simulieren einer ILM-Richtlinie neu anordnen

Dieses Beispiel zeigt, wie Sie Regeln neu anordnen können, um die Ergebnisse beim Simulieren einer Richtlinie zu ändern.

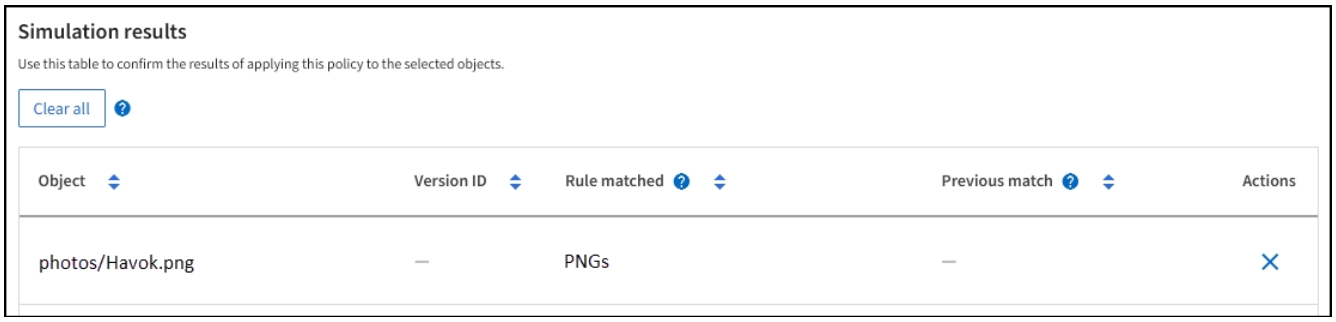
In diesem Beispiel wird die **Demo**-Richtlinie simuliert. Diese Richtlinie, die zum Auffinden von Objekten mit den Benutzermetadaten „series=x-men“ dient, umfasst die folgenden drei Regeln:

- Die erste Regel, **PNGs**, filtert nach Schlüsselnamen, die auf enden `.png`.
- Die zweite Regel, **X-men**, gilt nur für Objekte für Mieter A und filtert nach `series=x-men` Benutzermetadaten.
- Die letzte Regel, **Zwei Kopien, zwei Rechenzentren**, ist die Standardregel, die auf alle Objekte zutrifft, die nicht den ersten beiden Regeln entsprechen.

Schritte

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

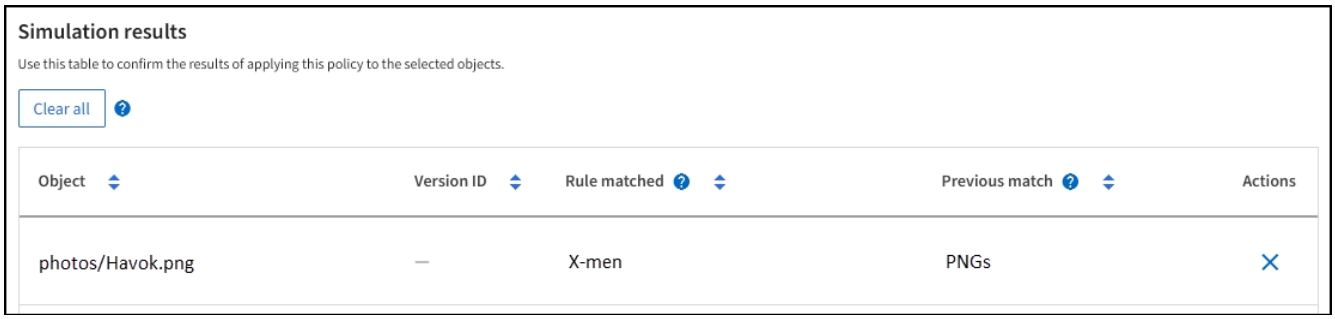
   Die Simulationsergebnisse werden angezeigt und zeigen, dass die `Havok.png` Das Objekt wurde mit der **PNGs**-Regel abgeglichen.

   Jedoch, `Havok.png` sollte die **X-Men**-Regel testen.

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

Die zuvor getesteten Objekte werden anhand der aktualisierten Richtlinie erneut ausgewertet und die neuen Simulationsergebnisse werden angezeigt. Im Beispiel zeigt die Spalte Regelübereinstimmung, dass die `Havok.png` Das Objekt entspricht jetzt wie erwartet der X-Men-Metadatenregel. Die Spalte „Vorherige Übereinstimmung“ zeigt, dass die PNG-Regel mit dem Objekt in der vorherigen Simulation übereinstimmte.



Beispiel 3: Korrigieren einer Regel beim Simulieren einer ILM-Richtlinie

Dieses Beispiel zeigt, wie Sie eine Richtlinie simulieren, eine Regel in der Richtlinie korrigieren und die Simulation fortsetzen.

In diesem Beispiel wird die **Demo**-Richtlinie simuliert. Mit dieser Richtlinie sollen Objekte gefunden werden, die `series=x-men` Benutzermetadaten. Allerdings kam es zu unerwarteten Ergebnissen bei der Simulation dieser Politik gegenüber der `Beast.jpg` Objekt. Anstatt der X-Men-Metadatenregel zu entsprechen, entsprach das Objekt der Standardregel „Zwei Kopien, zwei Rechenzentren“.

Wenn ein Testobjekt nicht mit der erwarteten Regel in der Richtlinie übereinstimmt, müssen Sie jede Regel in der Richtlinie prüfen und etwaige Fehler beheben.

Schritte

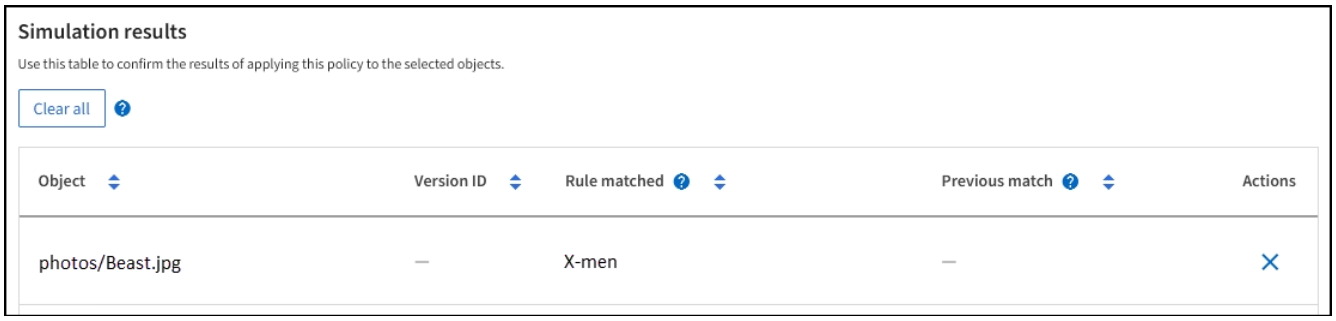
1. Wählen Sie **Fertig**, um das Dialogfeld „Richtlinie simulieren“ zu schließen. Wählen Sie auf der Detailseite der Richtlinie **Aufbewahrungsdiagramm** aus. Wählen Sie dann je nach Bedarf für jede Regel **Alle erweitern** oder **Details anzeigen** aus.
2. Überprüfen Sie das Mandantenkonto, die Referenzzeit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

   Nehmen wir beispielsweise an, dass die Metadaten für die X-Men-Regel als „x-men01“ statt als „x-men“ eingegeben wurden.

3. Um den Fehler zu beheben, korrigieren Sie die Regel wie folgt:
   - Wenn die Regel Teil der Richtlinie ist, können Sie die Regel entweder klonen oder aus der Richtlinie entfernen und dann bearbeiten.
   - Wenn die Regel Teil der aktiven Richtlinie ist, müssen Sie die Regel klonen. Sie können eine Regel aus der aktiven Richtlinie weder bearbeiten noch entfernen.

4. Führen Sie die Simulation erneut durch.

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



Verwalten von ILM-Richtlinientags

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

Bevor Sie beginnen

- Sie sind beim Grid Manager angemeldet mit einem"unterstützter Webbrowser" .
- Sie haben die"erforderliche Zugriffsberechtigungen" .

Anzeigen von ILM-Richtlinientagdetails

So zeigen Sie die Details für ein Tag an:

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

ILM-Richtlinientag bearbeiten

> Tag-Namen und -Beschreibungen sind für Mieter sichtbar. Wählen Sie Werte aus, die den Mandanten dabei helfen, eine fundierte Entscheidung zu treffen, wenn sie Richtlinien-Tags auswählen, die sie ihren Buckets zuweisen möchten. Wenn die zugewiesene Richtlinie beispielsweise das Löschen von Objekten nach einer bestimmten Zeit vorsieht, können Sie dies in der Beschreibung mitteilen. Geben Sie in diese Felder keine vertraulichen Informationen ein.

So bearbeiten Sie die Beschreibung für ein vorhandenes Tag:

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

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

3. Ändern Sie die Tag-Beschreibung nach Bedarf

4. Wählen Sie **Speichern**.

ILM-Richtlinientag entfernen

Wenn Sie ein Richtlinien-Tag entfernen, wird auf alle Buckets, denen dieses Tag zugewiesen ist, die Standardrichtlinie angewendet.

So entfernen Sie ein Tag:

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

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

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

Überprüfen einer ILM-Richtlinie mit der Objektmetadatensuche

Nachdem Sie eine ILM-Richtlinie aktiviert haben, nehmen Sie repräsentative Testobjekte in das StorageGRID -System auf und führen Sie dann eine Objektmetadatensuche durch, um zu bestätigen, dass Kopien wie beabsichtigt erstellt und an den richtigen Speicherorten abgelegt werden.

Bevor Sie beginnen

Sie haben eine Objektkennung, die eine der folgenden sein kann: * **UUID**: Die universell eindeutige Kennung des Objekts. * **CBID**: Die eindeutige Kennung des Objekts innerhalb von StorageGRID. Sie können die CBID eines Objekts aus dem Prüfprotokoll abrufen. Geben Sie die CBID in Großbuchstaben ein. * **S3-Bucket und Objektschlüssel**: Wenn ein Objekt über die S3-Schnittstelle aufgenommen wird, verwendet die Clientanwendung eine Kombination aus Bucket und Objektschlüssel, um das Objekt zu speichern und zu identifizieren. Wenn der S3-Bucket versioniert ist und Sie mithilfe des Bucket- und Objektschlüssels eine bestimmte Version eines S3-Objekts nachschlagen möchten, verfügen Sie über die **Versions-ID**.

Schritte

1. Nehmen Sie das Objekt auf.
2. Wählen Sie **ILM** > **Objektmetadatensuche**.
3. Geben Sie die Kennung des Objekts in das Feld **Kennung** ein. Sie können eine UUID, CBID oder einen S3-Bucket/Objektschlüssel eingeben.
4. Geben Sie optional eine Versions-ID für das Objekt ein (nur S3).
5. Wählen Sie **Nachschlagen**.

   Die Ergebnisse der Objektmetadatensuche werden angezeigt. Auf dieser Seite sind die folgenden Arten von Informationen aufgeführt:

   - Systemmetadaten, wie Objekt-ID (UUID), Ergebnistyp (Objekt, Löschmarkierung, S3-Bucket) und logische Größe des Objekts. Weitere Einzelheiten finden Sie im Beispiel-Screenshot unten.
   - Alle benutzerdefinierten Schlüssel-Wert-Paare der Benutzermetadaten, die mit dem Objekt verknüpft sind.
   - Bei S3-Objekten alle mit dem Objekt verknüpften Schlüssel-Wert-Paare des Objekt-Tags.

- Bei replizierten Objektkopien der aktuelle Speicherort jeder Kopie.
- Bei Erasure-Coded-Objektkopien der aktuelle Speicherort jedes Fragments.
- Bei Objektkopien in einem Cloud Storage Pool 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 Segmentkennungen und Datengrößen. Bei Objekten mit mehr als 100 Segmenten werden nur die ersten 100 Segmente angezeigt.
- Alle Objektmetadaten im unverarbeiteten, internen Speicherformat. Diese Rohmetadaten umfassen interne Systemmetadaten, deren Beibehaltung von Version zu Version nicht garantiert ist.

6. Bestätigen Sie, dass das Objekt am richtigen Ort bzw. an den richtigen Orten gespeichert ist und dass es sich um den richtigen Kopietyp handelt.

   Wenn die Audit-Option aktiviert ist, können Sie das Audit-Protokoll auch auf die Meldung „ORLM-Objektregeln erfüllt“ überwachen. Die ORLM-Auditnachricht kann Ihnen weitere Informationen zum Status des ILM-Bewertungsprozesses liefern, sie kann Ihnen jedoch keine Informationen zur Richtigkeit der Platzierung der Objektdaten oder zur Vollständigkeit der ILM-Richtlinie geben. Dies müssen Sie selbst bewerten. Weitere Informationen finden Sie unter "Überprüfen der Überwachungsprotokolle" .

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

> Der folgende Screenshot ist ein Beispiel. Ihre Ergebnisse variieren je nach Ihrer StorageGRID Version.

System Metadata

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

Replicated Copies

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

Raw Metadata

Ähnliche Informationen

"Verwenden Sie die S3 REST-API"

Arbeiten mit ILM-Richtlinien und ILM-Regeln

Wenn sich Ihre Speicheranforderungen ändern, müssen Sie möglicherweise zusätzliche Richtlinien implementieren oder die mit einer Richtlinie verknüpften ILM-Regeln ändern. Sie können ILM-Metriken anzeigen, um die Systemleistung zu bestimmen.

Bevor Sie beginnen

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

ILM-Richtlinien anzeigen

So zeigen Sie aktive und inaktive ILM-Richtlinien und den Richtlinienaktivierungsverlauf an:

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

> Wenn Sie die Details einer Richtlinie mit dem Status „Bearbeitet“ oder „Gelöscht“ anzeigen, wird eine Meldung angezeigt, die darauf hinweist, dass Sie die Version der Richtlinie anzeigen, die für den angegebenen Zeitraum aktiv war und seitdem bearbeitet oder gelöscht wurde.

Bearbeiten einer ILM-Richtlinie

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

So bearbeiten Sie eine Richtlinie:

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

> Eine falsch konfigurierte ILM-Richtlinie kann zu einem nicht wiederherstellbaren Datenverlust führen. Bevor Sie eine ILM-Richtlinie aktivieren, überprüfen Sie die ILM-Richtlinie und ihre ILM-Regeln sorgfältig und simulieren Sie dann die ILM-Richtlinie. Stellen Sie immer sicher, dass die ILM-Richtlinie wie vorgesehen funktioniert.

Klonen einer ILM-Richtlinie

So klonen Sie eine ILM-Richtlinie:

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

> Eine falsch konfigurierte ILM-Richtlinie kann zu einem nicht wiederherstellbaren Datenverlust führen. Bevor Sie eine ILM-Richtlinie aktivieren, überprüfen Sie die ILM-Richtlinie und ihre ILM-Regeln sorgfältig und simulieren Sie dann die ILM-Richtlinie. Stellen Sie immer sicher, dass die ILM-Richtlinie wie vorgesehen funktioniert.

Entfernen einer ILM-Richtlinie

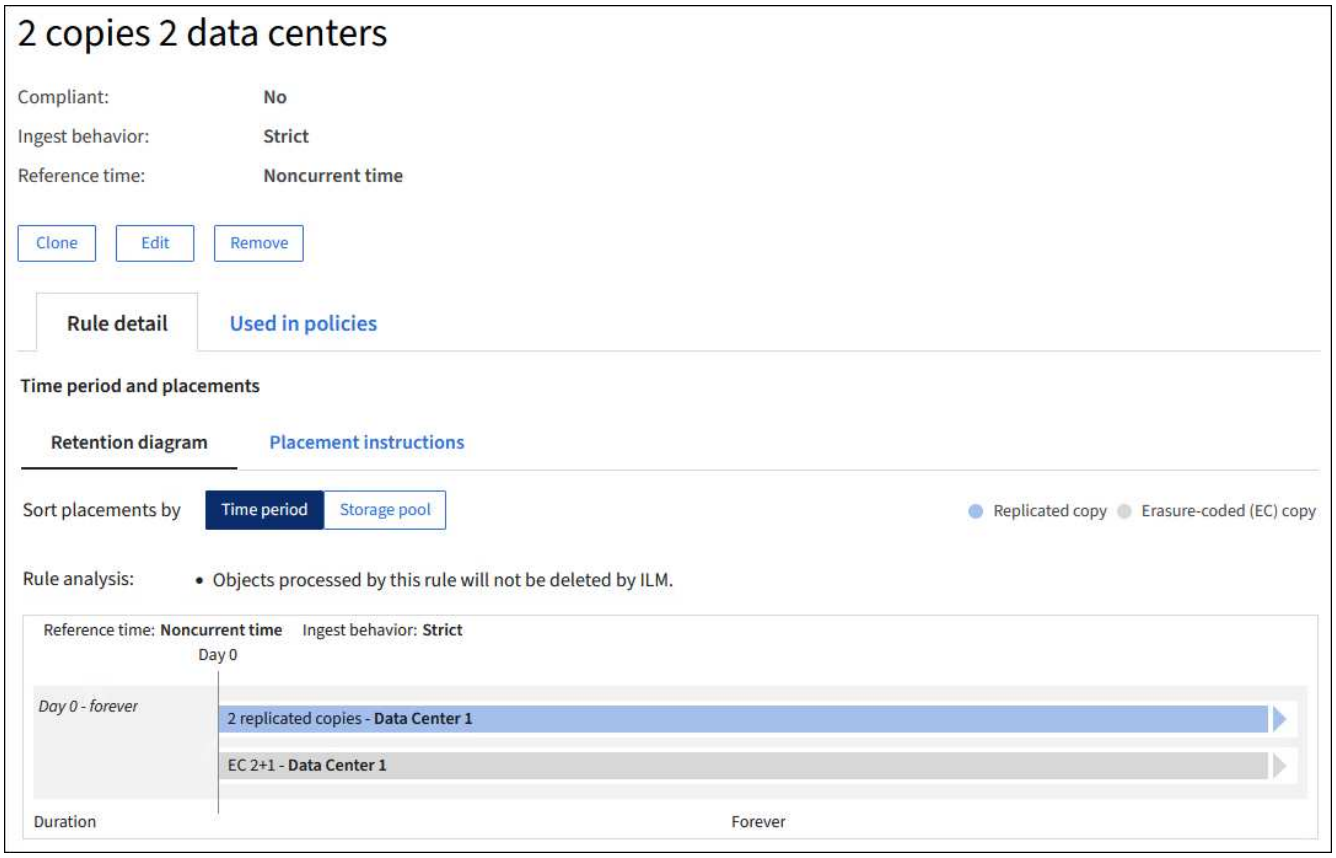
Sie können eine ILM-Richtlinie nur entfernen, wenn sie inaktiv ist. So entfernen Sie eine Richtlinie:

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

Anzeigen von ILM-Regeldetails

So zeigen Sie die Details einer ILM-Regel an, einschließlich des Aufbewahrungsdiagramms und der Platzierungsanweisungen für die Regel:

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



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

Klonen einer ILM-Regel

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

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

Schritte

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

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

Bearbeiten einer ILM-Regel

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

Sie können eine Regel nicht bearbeiten, wenn sie in einer ILM-Richtlinie verwendet wird. Stattdessen können SieKlonen Sie die Regel und nehmen Sie alle erforderlichen Änderungen an der geklonten Kopie vor.

Eine falsch konfigurierte ILM-Richtlinie kann zu einem nicht wiederherstellbaren Datenverlust führen. Bevor Sie eine ILM-Richtlinie aktivieren, überprüfen Sie die ILM-Richtlinie und ihre ILM-Regeln sorgfältig und simulieren Sie dann die ILM-Richtlinie. Stellen Sie immer sicher, dass die ILM-Richtlinie wie vorgesehen funktioniert.

Schritte

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

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

Entfernen einer ILM-Regel

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

Schritte

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

1. Klonen Sie die Richtlinie.
2. Entfernen Sie die ILM-Regel aus dem Richtlinienklon.

3. Speichern, simulieren und aktivieren Sie die neue Richtlinie, um sicherzustellen, dass Objekte wie erwartet geschützt sind.
4. Fahren Sie mit den Schritten zum Entfernen einer ILM-Regel fort, die derzeit in einer inaktiven Richtlinie verwendet wird.

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

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

So entfernen Sie eine ILM-Regel, die derzeit nicht verwendet wird:

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

Anzeigen von ILM-Metriken

Sie können Kennzahlen für ILM anzeigen, beispielsweise die Anzahl der Objekte in der Warteschlange und die Auswertungsrate. Sie können diese Metriken überwachen, um die Systemleistung zu bestimmen. Eine große Warteschlange oder Auswertungsrate kann darauf hinweisen, dass das System mit der Aufnahmerate nicht Schritt halten kann, die Belastung durch die Clientanwendungen zu hoch ist oder ein anormaler Zustand vorliegt.

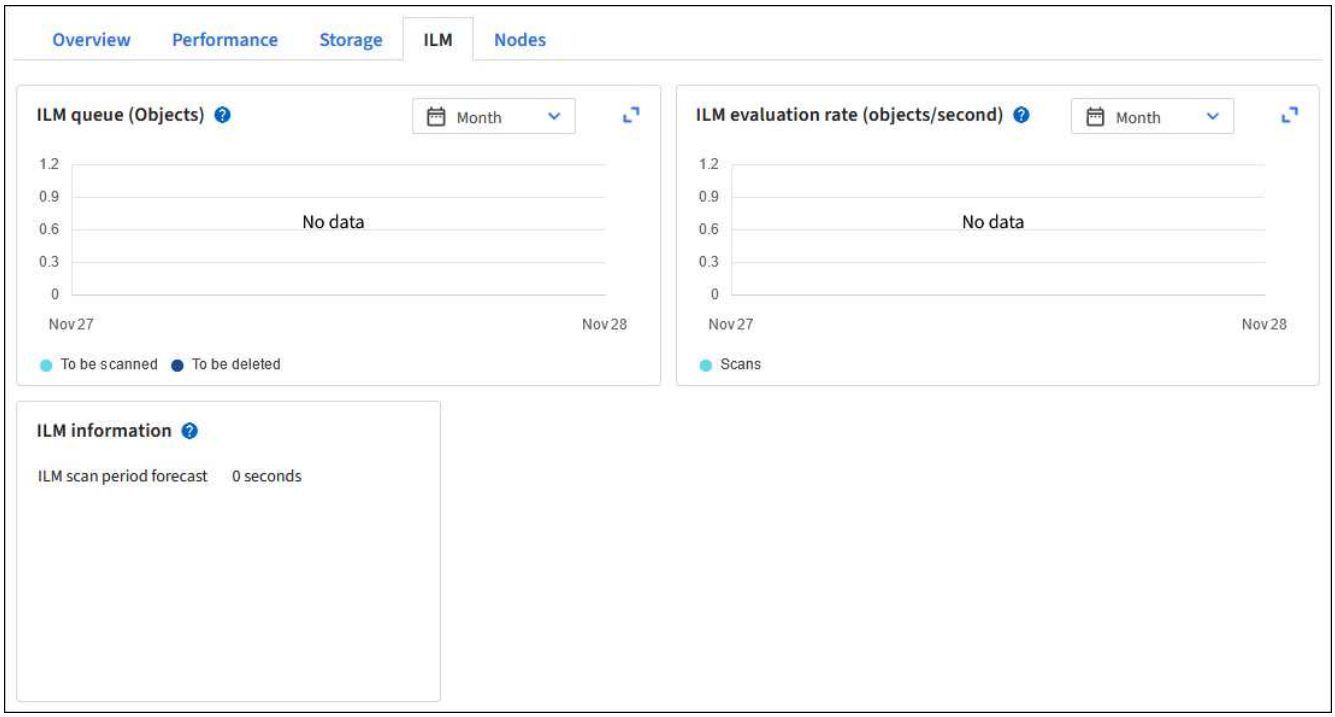
Schritte

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

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

2. Überwachen Sie die Metriken auf der Registerkarte „ILM“.

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



S3-Objektsperre verwenden

Verwalten von Objekten mit S3 Object Lock

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

Was ist S3 Object Lock?

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

Wenn die globale S3-Objektsperre-Einstellung für ein StorageGRID -System aktiviert ist, kann ein S3-Mandantenkonto Buckets mit oder ohne aktivierte S3-Objektsperre erstellen. Wenn für einen Bucket die S3-Objektsperre aktiviert ist, ist eine Bucket-Versionierung erforderlich und wird automatisch aktiviert.

Ein Bucket ohne S3-Objektsperre kann nur Objekte ohne angegebene Aufbewahrungseinstellungen enthalten. Für aufgenommene Objekte werden keine Aufbewahrungseinstellungen festgelegt.

Ein Bucket mit S3 Object Lock kann Objekte mit und ohne Aufbewahrungseinstellungen enthalten, die von S3-Clientanwendungen angegeben werden. Für einige aufgenommene Objekte gelten Aufbewahrungseinstellungen.

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

Tatsächlich verfügen alle neu aufgenommenen Objekte über Aufbewahrungseinstellungen, wenn die

Standardaufbewahrung konfiguriert ist. Vorhandene Objekte ohne Objektaufbewahrungseinstellungen bleiben davon unberührt.

Aufbewahrungsmodi

Die StorageGRID S3 Object Lock-Funktion unterstützt zwei Aufbewahrungsmodi, um unterschiedliche Schutzstufen auf Objekte anzuwenden. Diese Modi entsprechen den Aufbewahrungsmodi von Amazon S3.

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

Aufbewahrungseinstellungen für Objektversionen

Wenn ein Bucket mit aktivierter S3-Objektsperre erstellt wird, können Benutzer mit der S3-Clientanwendung optional die folgenden Aufbewahrungseinstellungen für jedes dem Bucket hinzugefügte Objekt angeben:

- **Aufbewahrungsmodus**: Entweder Compliance oder Governance.
- **Aufbewahrungsdatum**: Wenn das Aufbewahrungsdatum einer Objektversion in der Zukunft liegt, kann das Objekt abgerufen, aber nicht gelöscht werden.
- **Rechtliche Sperre**: Durch Anwenden einer rechtlichen Sperre auf eine Objektversion wird dieses Objekt sofort gesperrt. Beispielsweise müssen Sie möglicherweise ein Objekt, das mit einer Untersuchung oder einem Rechtsstreit in Zusammenhang steht, rechtlich sperren. Eine rechtliche Sperre hat kein Ablaufdatum, sondern bleibt bestehen, bis sie ausdrücklich aufgehoben wird. Rechtliche Sperren sind unabhängig vom Aufbewahrungsdatum.

  > Wenn ein Objekt einer rechtlichen Sperre unterliegt, kann niemand das Objekt löschen, unabhängig von seinem Aufbewahrungsmodus.

  Details zu den Objekteinstellungen finden Sie unter"Verwenden Sie die S3 REST API, um S3 Object Lock zu konfigurieren" .

Standardaufbewahrungseinstellung für Buckets

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

- **Standardaufbewahrungsmodus**: Entweder Compliance oder Governance.
- **Standardaufbewahrungszeitraum**: Wie lange neue Objektversionen, die diesem Bucket hinzugefügt werden, ab dem Tag ihrer Hinzufügung aufbewahrt werden sollen.

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

Sehen"Erstellen eines S3-Buckets" Und"Standardaufbewahrung für S3 Object Lock aktualisieren" .

Vergleich von S3 Object Lock mit herkömmlicher Compliance

Die S3-Objektsperre ersetzt die Compliance-Funktion, die in früheren StorageGRID Versionen verfügbar war. Da die S3 Object Lock-Funktion den Anforderungen von Amazon S3 entspricht, wird die proprietäre StorageGRID Compliance-Funktion, die jetzt als „Legacy Compliance“ bezeichnet wird, dadurch verworfen.

> Die globale Compliance-Einstellung ist veraltet. Wenn Sie diese Einstellung mit einer früheren Version von StorageGRID aktiviert haben, wird die Einstellung „S3 Object Lock“ automatisch aktiviert. Sie können StorageGRID weiterhin verwenden, um die Einstellungen vorhandener konformer Buckets zu verwalten. Sie können jedoch keine neuen konformen Buckets erstellen. Weitere Einzelheiten finden Sie unter "NetApp Knowledge Base: So verwalten Sie ältere konforme Buckets in StorageGRID 11.5" .

Wenn Sie die alte Compliance-Funktion in einer früheren Version von StorageGRID verwendet haben, können Sie in der folgenden Tabelle nachlesen, wie sie im Vergleich zur S3 Object Lock-Funktion in StorageGRID abschneidet.

	S3-Objektsperre	**Compliance (alt)**
Wie wird die Funktion global aktiviert?	Wählen Sie im Grid Manager **KONFIGURATION** > **System** > **S3-Objektsperre**.	Wird nicht mehr unterstützt.
Wie wird die Funktion für einen Bucket aktiviert?	Benutzer müssen S3 Object Lock aktivieren, wenn sie mit dem Tenant Manager, der Tenant Management API oder der S3 REST API einen neuen Bucket erstellen.	Wird nicht mehr unterstützt.
Wird Bucket-Versionierung unterstützt?	Ja. Bucket-Versionierung ist erforderlich und wird automatisch aktiviert, wenn S3 Object Lock für den Bucket aktiviert ist.	NEIN.
Wie wird die Objektaufbewahrung eingestellt?	Benutzer können für jede Objektversion ein Aufbewahrungsdatum oder für jeden Bucket eine Standardaufbewahrungsdauer festlegen.	Benutzer müssen eine Aufbewahrungsfrist für den gesamten Bucket festlegen. Die Aufbewahrungsfrist gilt für alle Objekte im Bucket.

	S3-Objektsperre	Compliance (alt)
Kann die Aufbewahrungsdauer geändert werden?	• Im Compliance-Modus kann das Aufbewahrungsdatum für eine Objektversion erhöht, aber nie verringert werden. • Im Governance-Modus können Benutzer mit Sonderberechtigungen die Aufbewahrungseinstellungen eines Objekts verringern oder sogar entfernen.	Die Aufbewahrungsdauer eines Buckets kann verlängert, aber niemals verkürzt werden.
Wo wird die rechtliche Aufbewahrung kontrolliert?	Benutzer können für jede Objektversion im Bucket eine rechtliche Sperre festlegen oder aufheben.	Für den Bucket wird eine rechtliche Sperre verhängt, die sich auf alle Objekte im Bucket auswirkt.
Wann können Objekte gelöscht werden?	• Im Compliance-Modus kann eine Objektversion nach Erreichen des Aufbewahrungsdatums gelöscht werden, vorausgesetzt, das Objekt unterliegt keiner rechtlichen Sperre. • Im Governance-Modus können Benutzer mit Sonderberechtigungen ein Objekt löschen, bevor das Aufbewahrungsdatum erreicht ist, vorausgesetzt, das Objekt unterliegt keiner rechtlichen Sperre.	Ein Objekt kann nach Ablauf der Aufbewahrungsfrist gelöscht werden, vorausgesetzt, der Bucket unterliegt keiner rechtlichen Sperre. Objekte können automatisch oder manuell gelöscht werden.
Wird die Bucket-Lebenszykluskonfiguration unterstützt?	Ja	Nein

S3 Object Lock-Aufgaben

Als Grid-Administrator müssen Sie sich eng mit den Mandantenbenutzern abstimmen, um sicherzustellen, dass die Objekte auf eine Weise geschützt werden, die ihren Aufbewahrungsanforderungen entspricht.

> Das Anwenden von Mandanteneinstellungen im gesamten Grid kann je nach Netzwerkkonnektivität, Knotenstatus und Cassandra-Vorgängen 15 Minuten oder länger dauern.

Die folgenden Listen für Grid-Administratoren und Mandantenbenutzer enthalten die allgemeinen Aufgaben zur Verwendung der S3 Object Lock-Funktion.

Grid-Administrator

- Aktivieren Sie die globale S3-Objektsperreinstellung für das gesamte StorageGRID System.
- Stellen Sie sicher, dass die Richtlinien für das Information Lifecycle Management (ILM) *konform* sind; das heißt, sie erfüllen die"Anforderungen an Buckets mit aktivierter S3-Objektsperre" .
- Erlauben Sie einem Mandanten bei Bedarf, Compliance als Aufbewahrungsmodus zu verwenden. Andernfalls ist nur der Governance-Modus zulässig.
- Legen Sie bei Bedarf eine maximale Aufbewahrungsdauer für einen Mandanten fest.

Mandantenbenutzer

- Überprüfen Sie die Überlegungen zu Buckets und Objekten mit S3 Object Lock.
- Wenden Sie sich bei Bedarf an den Grid-Administrator, um die globale S3-Objektsperreinstellung zu aktivieren und Berechtigungen festzulegen.
- Erstellen Sie Buckets mit aktivierter S3-Objektsperre.
- Konfigurieren Sie optional die Standardaufbewahrungseinstellungen für einen Bucket:
  - Standardaufbewahrungsmodus: Governance oder Compliance, sofern vom Grid-Administrator zugelassen.
  - Standardaufbewahrungszeitraum: Muss kleiner oder gleich dem vom Grid-Administrator festgelegten maximalen Aufbewahrungszeitraum sein.
- Verwenden Sie die S3-Clientanwendung, um Objekte hinzuzufügen und optional eine objektspezifische Aufbewahrung festzulegen:
  - Aufbewahrungsmodus. Governance oder Compliance, sofern vom Grid-Administrator zugelassen.
  - Aufbewahrungsdatum: Muss kleiner oder gleich dem vom Grid-Administrator festgelegten maximalen Aufbewahrungszeitraum sein.

Anforderungen für S3 Object Lock

Sie müssen die Anforderungen zum Aktivieren der globalen S3 Object Lock-Einstellung, die Anforderungen zum Erstellen konformer ILM-Regeln und ILM-Richtlinien sowie die Einschränkungen überprüfen, die StorageGRID für Buckets und Objekte auferlegt, die S3 Object Lock verwenden.

Voraussetzungen für die Verwendung der globalen S3 Object Lock-Einstellung

- Sie müssen die globale S3-Objektsperreinstellung mithilfe des Grid Managers oder der Grid Management API aktivieren, bevor ein S3-Mandant einen Bucket mit aktivierter S3-Objektsperre erstellen kann.
- Durch Aktivieren der globalen S3-Objektsperre können alle S3-Mandantenkonten Buckets mit aktivierter S3-Objektsperre erstellen.
- Nachdem Sie die globale S3-Objektsperreinstellung aktiviert haben, können Sie die Einstellung nicht mehr deaktivieren.
- Sie können die globale S3-Objektsperre nur aktivieren, wenn die Standardregel in allen aktiven ILM-Richtlinien *konform* ist (d. h., die Standardregel muss den Anforderungen von Buckets mit aktivierter S3-Objektsperre entsprechen).
- Wenn die globale Einstellung „S3-Objektsperre“ aktiviert ist, können Sie keine neue ILM-Richtlinie erstellen oder eine vorhandene ILM-Richtlinie aktivieren, es sei denn, die Standardregel in der Richtlinie ist konform. Nachdem die globale S3-Objektsperreinstellung aktiviert wurde, zeigen die Seiten mit den ILM-Regeln und ILM-Richtlinien an, welche ILM-Regeln konform sind.

Anforderungen an konforme ILM-Regeln

Wenn Sie die globale S3-Objektsperreinstellung aktivieren möchten, müssen Sie sicherstellen, dass die Standardregel in allen aktiven ILM-Richtlinien konform ist. Eine konforme Regel erfüllt die Anforderungen sowohl von Buckets mit aktivierter S3-Objektsperre als auch von allen vorhandenen Buckets mit aktivierter Legacy-Compliance:

- Es müssen mindestens zwei replizierte Objektkopien oder eine Erasure-Coded-Kopie erstellt werden.
- Diese Kopien müssen für die gesamte Dauer jeder Zeile in den Platzierungsanweisungen auf den Speicherknoten vorhanden sein.
- Objektkopien können nicht in einem Cloud-Speicherpool gespeichert werden.
- Mindestens eine Zeile der Platzierungsanweisungen muss am Tag 0 beginnen, wobei **Aufnahmezeit** als Referenzzeit verwendet wird.
- Mindestens eine Zeile der Platzierungsanweisungen muss „für immer“ lauten.

Anforderungen für ILM-Richtlinien

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

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

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

Anforderungen für Buckets mit aktivierter S3-Objektsperre

- Wenn die globale S3-Objektsperre-Einstellung für das StorageGRID -System aktiviert ist, können Sie den Tenant Manager, die Tenant Management API oder die S3 REST API verwenden, um Buckets mit aktivierter S3-Objektsperre zu erstellen.
- Wenn Sie S3 Object Lock verwenden möchten, müssen Sie S3 Object Lock beim Erstellen des Buckets aktivieren. Sie können S3 Object Lock nicht für einen vorhandenen Bucket aktivieren.
- Wenn S3 Object Lock für einen Bucket aktiviert ist, aktiviert StorageGRID automatisch die Versionierung für diesen Bucket. Sie können die S3-Objektsperre nicht deaktivieren oder die Versionsverwaltung für den Bucket aussetzen.
- Optional können Sie mithilfe des Tenant Managers, der Tenant Management API oder der S3 REST API einen Standardaufbewahrungsmodus und eine Standardaufbewahrungsdauer für jeden Bucket angeben. Die Standardaufbewahrungseinstellungen des Buckets gelten nur für neue Objekte, die dem Bucket hinzugefügt werden und keine eigenen Aufbewahrungseinstellungen haben. Sie können diese Standardeinstellungen überschreiben, indem Sie beim Hochladen für jede Objektversion einen Aufbewahrungsmodus und ein Aufbewahrungsdatum angeben.
- Die Bucket-Lebenszykluskonfiguration wird für Buckets mit aktivierter S3-Objektsperre unterstützt.
- Die CloudMirror-Replikation wird für Buckets mit aktivierter S3-Objektsperre nicht unterstützt.

Anforderungen für Objekte in Buckets mit aktivierter S3-Objektsperre

- Um eine Objektversion zu schützen, können Sie Standardaufbewahrungseinstellungen für den Bucket oder Aufbewahrungseinstellungen für jede Objektversion angeben. Aufbewahrungseinstellungen auf Objektebene können mithilfe der S3-Clientanwendung oder der S3-REST-API angegeben werden.
- Aufbewahrungseinstellungen gelten für einzelne Objektversionen. Eine Objektversion kann sowohl über eine Aufbewahrungsfrist als auch über eine gesetzliche Aufbewahrungsfrist verfügen, über eine der beiden Einstellungen, aber nicht über die andere, oder über keine von beiden. Durch die Angabe eines Aufbewahrungsdatums oder einer Einstellung für die rechtliche Aufbewahrung eines Objekts 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 mit aktivierter S3-Objektsperre

Jedes Objekt, das in einem Bucket mit aktivierter S3-Objektsperre gespeichert wird, durchläuft die folgenden Phasen:

1. **Objektaufnahme**

   Wenn eine Objektversion zu einem Bucket hinzugefügt wird, für den die S3-Objektsperre aktiviert ist, werden die Aufbewahrungseinstellungen wie folgt angewendet:

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

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

2. **Objektaufbewahrung und -löschung**

   Von jedem geschützten Objekt werden von StorageGRID mehrere Kopien für den angegebenen Aufbewahrungszeitraum gespeichert. Die genaue Anzahl und Art der Objektkopien sowie die Speicherorte werden durch die konformen Regeln in den aktiven ILM-Richtlinien bestimmt. Ob ein geschütztes Objekt vor Erreichen seines Aufbewahrungsdatums gelöscht werden kann, hängt von seinem Aufbewahrungsmodus ab.

   - Wenn ein Objekt einer rechtlichen Sperre unterliegt, kann niemand das Objekt löschen, unabhängig von seinem Aufbewahrungsmodus.

Ähnliche Informationen

- "Erstellen eines S3-Buckets"
- "Standardaufbewahrung für S3 Object Lock aktualisieren"
- "Verwenden Sie die S3 REST API, um S3 Object Lock zu konfigurieren"
- "Beispiel 7: Konforme ILM-Richtlinie für S3 Object Lock"

S3 Object Lock global aktivieren

Wenn ein S3-Mandantenkonto beim Speichern von Objektdaten gesetzliche

Anforderungen erfüllen muss, müssen Sie S3 Object Lock für Ihr gesamtes StorageGRID System aktivieren. Durch Aktivieren der globalen S3 Object Lock-Einstellung kann jeder S3-Mandantenbenutzer Buckets und Objekte mit S3 Object Lock erstellen und verwalten.

Bevor Sie beginnen

- Sie haben die"Root-Zugriffsberechtigung" .
- Sie sind beim Grid Manager angemeldet mit einem"unterstützter Webbrowser" .
- Sie haben den S3 Object Lock-Workflow überprüft und verstehen die Überlegungen.
- Sie haben bestätigt, dass die Standardregel in der aktiven ILM-Richtlinie konform ist. Sehen"Erstellen einer ILM-Standardregel" für Details.

Informationen zu diesem Vorgang

Ein Grid-Administrator muss die globale S3-Objektsperreinstellung aktivieren, damit Mandantenbenutzer neue Buckets erstellen können, bei denen S3-Objektsperrung aktiviert ist. Nachdem diese Einstellung aktiviert wurde, kann sie nicht mehr deaktiviert werden.

Überprüfen Sie die Compliance-Einstellungen vorhandener Mandanten, nachdem Sie die globale S3-Objektsperreinstellung aktiviert haben. Wenn Sie diese Einstellung aktivieren, hängen die S3 Object Lock-Einstellungen pro Mandant von der StorageGRID Version zum Zeitpunkt der Mandantenerstellung ab.

> Die globale Compliance-Einstellung ist veraltet. Wenn Sie diese Einstellung mit einer früheren Version von StorageGRID aktiviert haben, wird die Einstellung „S3 Object Lock“ automatisch aktiviert. Sie können StorageGRID weiterhin verwenden, um die Einstellungen vorhandener konformer Buckets zu verwalten. Sie können jedoch keine neuen konformen Buckets erstellen. Weitere Einzelheiten finden Sie unter "NetApp Knowledge Base: So verwalten Sie ältere konforme Buckets in StorageGRID 11.5" .

Schritte

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

   Die Seite „S3-Objektsperreinstellungen“ wird angezeigt.

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

   Ein Bestätigungsdialogfeld wird angezeigt und erinnert Sie daran, dass Sie S3 Object Lock nach der Aktivierung nicht mehr deaktivieren können.

4. Wenn Sie sicher sind, dass Sie S3 Object Lock dauerhaft für Ihr gesamtes System aktivieren möchten, wählen Sie **OK**.

   Wenn Sie **OK** auswählen:

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

Beheben Sie Konsistenzfehler beim Aktualisieren der S3 Object Lock- oder Legacy-Compliance-Konfiguration

Wenn ein Rechenzentrumsstandort oder mehrere Speicherknoten an einem Standort nicht mehr verfügbar sind, müssen Sie den S3-Tenant-Benutzern möglicherweise dabei helfen, Änderungen an der S3-Objektsperre oder der alten Compliance-Konfiguration vorzunehmen.

Mandantenbenutzer, die Buckets mit aktivierter S3-Objektsperre (oder Legacy-Compliance) haben, können bestimmte Einstellungen ändern. Beispielsweise muss ein Mandantenbenutzer, der S3 Object Lock verwendet, möglicherweise eine Objektversion unter rechtliche Sperre stellen.

Wenn ein Mandantenbenutzer die Einstellungen für einen S3-Bucket oder eine Objektversion aktualisiert, versucht StorageGRID , die Bucket- oder Objektmetadaten im gesamten Grid sofort zu aktualisieren. Wenn das System die Metadaten nicht aktualisieren kann, weil ein Rechenzentrumsstandort oder mehrere Speicherknoten nicht verfügbar sind, gibt es einen Fehler zurück:

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

Um diesen Fehler zu beheben, führen Sie die folgenden Schritte aus:

1. Versuchen Sie, alle Speicherknoten oder Sites so schnell wie möglich wieder verfügbar zu machen.
2. Wenn Sie nicht in der Lage sind, an jedem Standort genügend Speicherknoten verfügbar zu machen, wenden Sie sich an den technischen Support. Dieser kann Ihnen bei der Wiederherstellung der Knoten helfen und sicherstellen, dass Änderungen im gesamten Grid konsistent angewendet werden.
3. Sobald das zugrunde liegende Problem behoben wurde, erinnern Sie den Mandantenbenutzer daran, seine Konfigurationsänderungen erneut zu versuchen.

Ähnliche Informationen

- "Verwenden eines Mandantenkontos"
- "Verwenden Sie die S3 REST-API"
- "Wiederherstellen und pflegen"

Beispiele für ILM-Regeln und -Richtlinien

Beispiel 1: ILM-Regeln und -Richtlinien für Objektspeicher

Sie können die folgenden Beispielregeln und -richtlinien als Ausgangspunkt verwenden, wenn Sie eine ILM-Richtlinie definieren, um Ihre Anforderungen an den Objektschutz und die Objektaufbewahrung zu erfüllen.

> Die folgenden ILM-Regeln und -Richtlinien sind nur Beispiele. Es gibt viele Möglichkeiten, ILM-Regeln zu konfigurieren. Bevor Sie eine neue Richtlinie aktivieren, simulieren Sie sie, um sicherzustellen, dass sie wie vorgesehen funktioniert und Inhalte vor Verlust schützt.

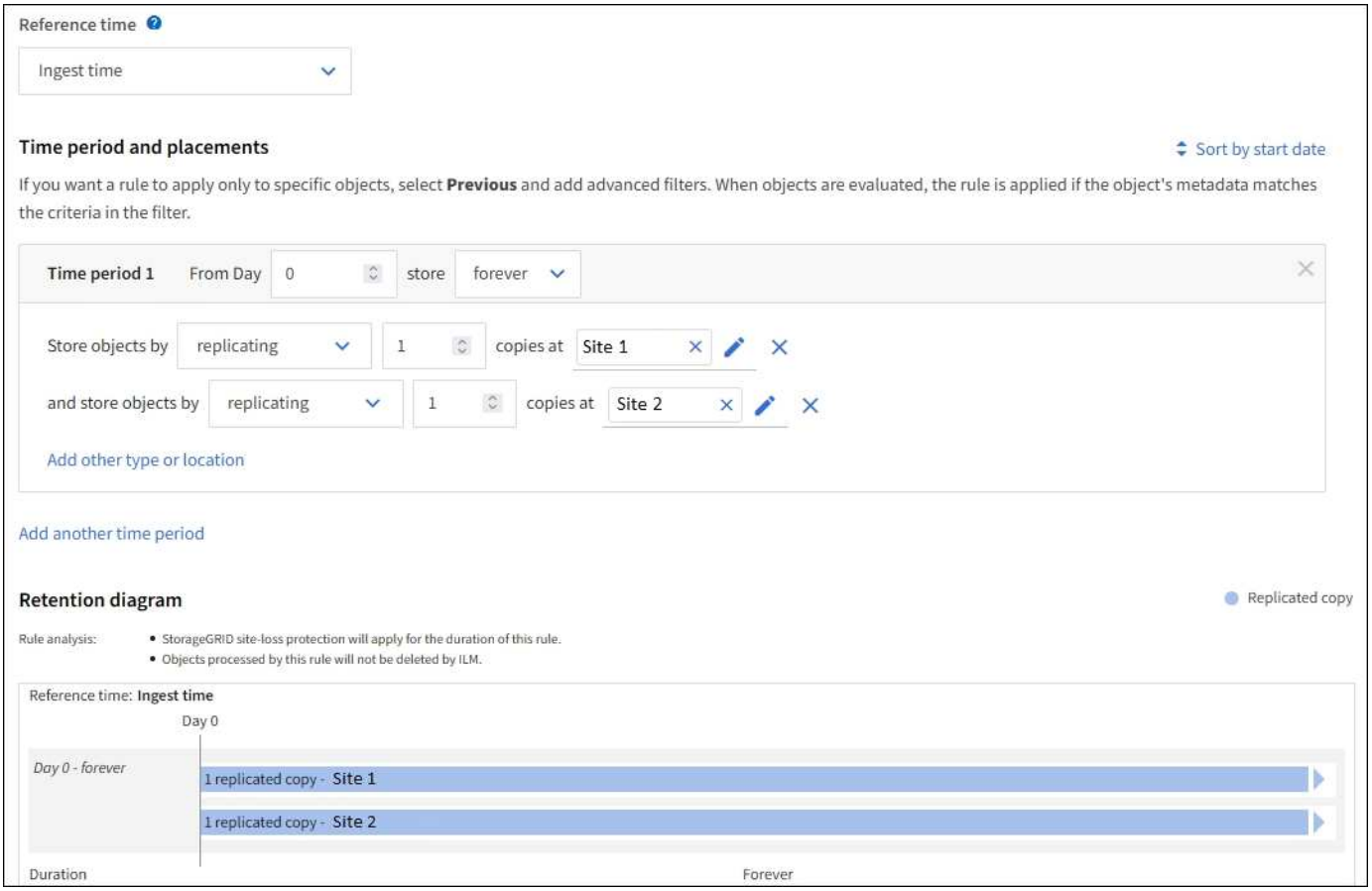
ILM-Regel 1 für Beispiel 1: Objektdaten auf zwei Sites kopieren

Diese beispielhafte ILM-Regel kopiert Objektdaten in Speicherpools an zwei Standorten.

Regeldefinition	Beispielwert
Speicherpools an einem Standort	Zwei Speicherpools, die jeweils unterschiedliche Sites enthalten, mit den Namen Site 1 und Site 2.
Regelname	Zwei Kopien, zwei Standorte
Referenzzeit	Aufnahmezeit
Platzierungen	Behalten Sie vom Tag 0 bis in alle Ewigkeit eine replizierte Kopie an Standort 1 und eine replizierte Kopie an Standort 2.

Im Abschnitt „Regelanalyse“ des Retention-Diagramms heißt es:

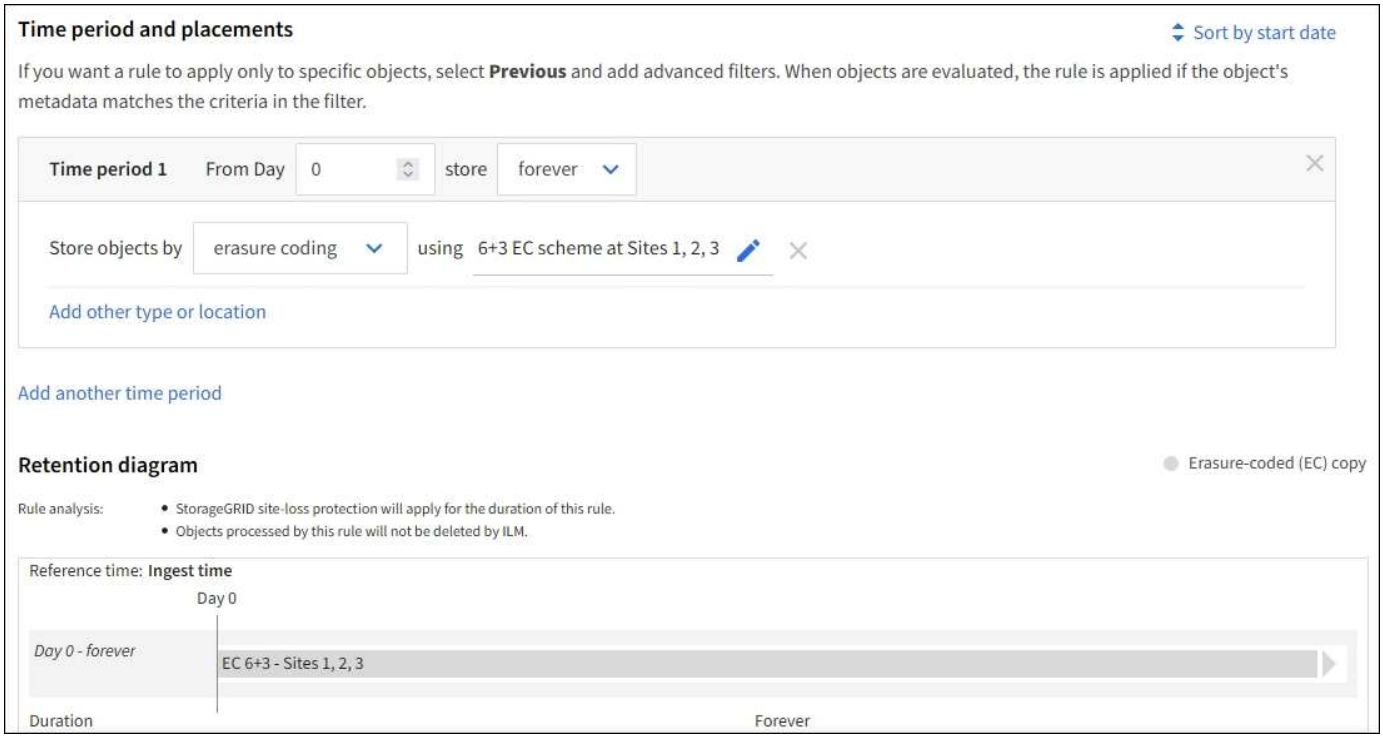
- Für die Dauer dieser Regelung gilt der Site-Loss-Schutz von StorageGRID .
- Von dieser Regel verarbeitete Objekte werden von ILM nicht gelöscht.



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

Dieses Beispiel einer ILM-Regel verwendet ein Erasure-Coding-Profil und einen S3-Bucket, um zu bestimmen, wo und wie lange das Objekt gespeichert wird.

Regeldefinition	Beispielwert
Speicherpool mit mehreren Standorten	• Ein Speicherpool an drei Standorten (Standorte 1, 2, 3) • Verwenden Sie das 6+3-Löschcodierungsschema
Regelname	S3 Bucket Finanzaufzeichnungen
Referenzzeit	Aufnahmezeit
Platzierungen	Erstellen Sie für Objekte im S3-Bucket mit dem Namen „finance-records“ eine Erasure-Coding-Kopie im Pool, der durch das Erasure-Coding-Profil angegeben ist. Bewahren Sie diese Kopie für immer auf.

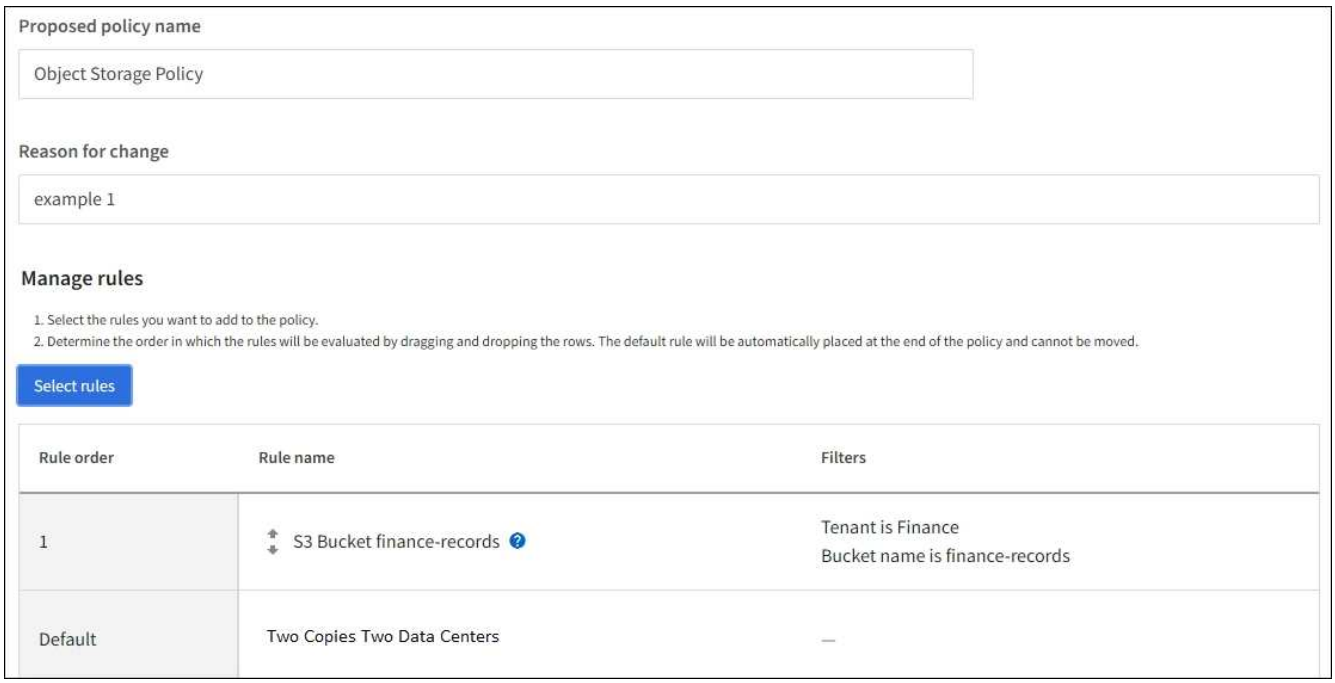


ILM-Richtlinie für Beispiel 1

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

Eine typische ILM-Richtlinie für ein Grid mit mehreren Standorten könnte ILM-Regeln wie die folgenden enthalten:

- Speichern Sie beim Ingest alle Objekte, die zum S3-Bucket mit dem Namen gehören `finance-records` in einem Speicherpool, der drei Standorte enthält. Verwenden Sie 6+3-Löschcodierung.
- Wenn ein Objekt nicht der ersten ILM-Regel entspricht, verwenden Sie die ILM-Standardregel der Richtlinie „Zwei Kopien, zwei Rechenzentren“, um eine Kopie dieses Objekts an Standort 1 und eine Kopie an Standort 2 zu speichern.



Ähnliche Informationen

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

Beispiel 2: ILM-Regeln und -Richtlinien für die EC-Objektgrößenfilterung

Sie können die folgenden Beispielregeln und -richtlinien als Ausgangspunkt verwenden, um eine ILM-Richtlinie zu definieren, die nach Objektgröße filtert, um die empfohlenen EC-Anforderungen zu erfüllen.

Die folgenden ILM-Regeln und -Richtlinien sind nur Beispiele. Es gibt viele Möglichkeiten, ILM-Regeln zu konfigurieren. Bevor Sie eine neue Richtlinie aktivieren, simulieren Sie sie, um sicherzustellen, dass sie wie vorgesehen funktioniert und Inhalte vor Verlust schützt.

ILM-Regel 1 für Beispiel 2: Verwenden Sie EC für Objekte größer als 1 MB

Dieses Beispiel einer ILM-Regel löscht Codes für Objekte, die größer als 1 MB sind.

Erasure Coding eignet sich am besten für Objekte, die größer als 1 MB sind. Verwenden Sie Erasure Coding nicht für Objekte, die kleiner als 200 KB sind, um den Verwaltungsaufwand für sehr kleine Erasure-Coding-Fragmente zu vermeiden.

Regeldefinition	Beispielwert
Regelname	Nur EC-Objekte > 1 MB
Referenzzeit	Aufnahmezeit
Erweiterter Filter für Objektgröße	Objektgröße größer als 1 MB

Regeldefinition	Beispielwert
Platzierungen	Erstellen Sie eine 2+1-Löschcodierte Kopie mit drei Standorten

ILM-Regel 2 für Beispiel 2: Zwei replizierte Kopien

Diese beispielhafte ILM-Regel erstellt zwei replizierte Kopien und filtert nicht nach Objektgröße. Diese Regel ist die Standardregel für die Richtlinie. Da die erste Regel alle Objekte herausfiltert, die größer als 1 MB sind, gilt diese Regel nur für Objekte, die 1 MB oder kleiner sind.

Regeldefinition	Beispielwert
Regelname	Zwei replizierte Kopien
Referenzzeit	Aufnahmezeit
Erweiterter Filter für Objektgröße	Keine
Platzierungen	Behalten Sie vom Tag 0 bis in alle Ewigkeit eine replizierte Kopie an Standort 1 und eine replizierte Kopie an Standort 2.

ILM-Richtlinie für Beispiel 2: Verwenden Sie EC für Objekte größer als 1 MB

Dieses Beispiel einer ILM-Richtlinie enthält zwei ILM-Regeln:

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

Beispiel 3: ILM-Regeln und -Richtlinien für besseren Schutz von Bilddateien

Mithilfe der folgenden Beispielregeln und -richtlinien können Sie sicherstellen, dass Bilder, die größer als 1 MB sind, mit einem Löschcode versehen werden und dass von kleineren Bildern zwei Kopien erstellt werden.

> Die folgenden ILM-Regeln und -Richtlinien sind nur Beispiele. Es gibt viele Möglichkeiten, ILM-Regeln zu konfigurieren. Bevor Sie eine neue Richtlinie aktivieren, simulieren Sie sie, um sicherzustellen, dass sie wie vorgesehen funktioniert und Inhalte vor Verlust schützt.

ILM-Regel 1 für Beispiel 3: Verwenden Sie EC für Bilddateien größer als 1 MB

Dieses Beispiel einer ILM-Regel verwendet erweiterte Filterung, um den Code aller Bilddateien, die größer als 1 MB sind, zu löschen.

Erasure Coding eignet sich am besten für Objekte, die größer als 1 MB sind. Verwenden Sie Erasure Coding nicht für Objekte, die kleiner als 200 KB sind, um den Verwaltungsaufwand für sehr kleine Erasure-Coding-Fragmente zu vermeiden.

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

Da diese Regel als erste Regel in der Richtlinie konfiguriert ist, gilt die Platzierungsanweisung für die Löschcodierung nur für JPG- und PNG-Dateien, die größer als 1 MB sind.

ILM-Regel 2 für Beispiel 3: Erstellen Sie 2 replizierte Kopien für alle verbleibenden Bilddateien

Dieses Beispiel einer ILM-Regel verwendet erweiterte Filterung, um anzugeben, dass kleinere Bilddateien repliziert werden. Da die erste Regel in der Richtlinie bereits Bilddateien mit einer Größe von über 1 MB zugeordnet hat, gilt diese Regel für Bilddateien mit einer Größe von 1 MB oder weniger.

Regeldefinition	Beispielwert
Regelname	2 Kopien für Bilddateien
Referenzzeit	Aufnahmezeit

Regeldefinition	Beispielwert
Erweiterte Filter für Schlüssel	• Endet mit .jpg • Endet mit .png
Platzierungen	Erstellen Sie 2 replizierte Kopien in zwei Speicherpools

ILM-Richtlinie für Beispiel 3: Besserer Schutz für Bilddateien

Dieses Beispiel einer ILM-Richtlinie umfasst drei Regeln:

- Die erste Regel löscht alle Bilddateien, die größer als 1 MB sind.
- Die zweite Regel erstellt zwei Kopien aller verbleibenden Bilddateien (d. h. Bilder mit einer Größe von 1 MB oder weniger).
- Die Standardregel gilt für alle verbleibenden Objekte (d. h. alle Nicht-Bilddateien).

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

Beispiel 4: ILM-Regeln und -Richtlinien für versionierte S3-Objekte

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

Wenn Sie für Objekte eine begrenzte Aufbewahrungsdauer angeben, werden diese Objekte nach Ablauf der Zeitspanne dauerhaft gelöscht. Stellen Sie sicher, dass Sie wissen, wie lange die Objekte aufbewahrt werden.

Wie dieses Beispiel zeigt, können Sie die von versionierten Objekten verwendete Speichermenge steuern, indem Sie für nicht aktuelle Objektversionen unterschiedliche Platzierungsanweisungen verwenden.

Die folgenden ILM-Regeln und -Richtlinien sind nur Beispiele. Es gibt viele Möglichkeiten, ILM-Regeln zu konfigurieren. Bevor Sie eine neue Richtlinie aktivieren, simulieren Sie sie, um sicherzustellen, dass sie wie vorgesehen funktioniert und Inhalte vor Verlust schützt.

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

Ähnliche Informationen

"So werden Objekte gelöscht"

ILM-Regel 1 für Beispiel 4: Drei Kopien 10 Jahre lang aufbewahren

Diese beispielhafte ILM-Regel speichert eine Kopie jedes Objekts 10 Jahre lang an drei Standorten.

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

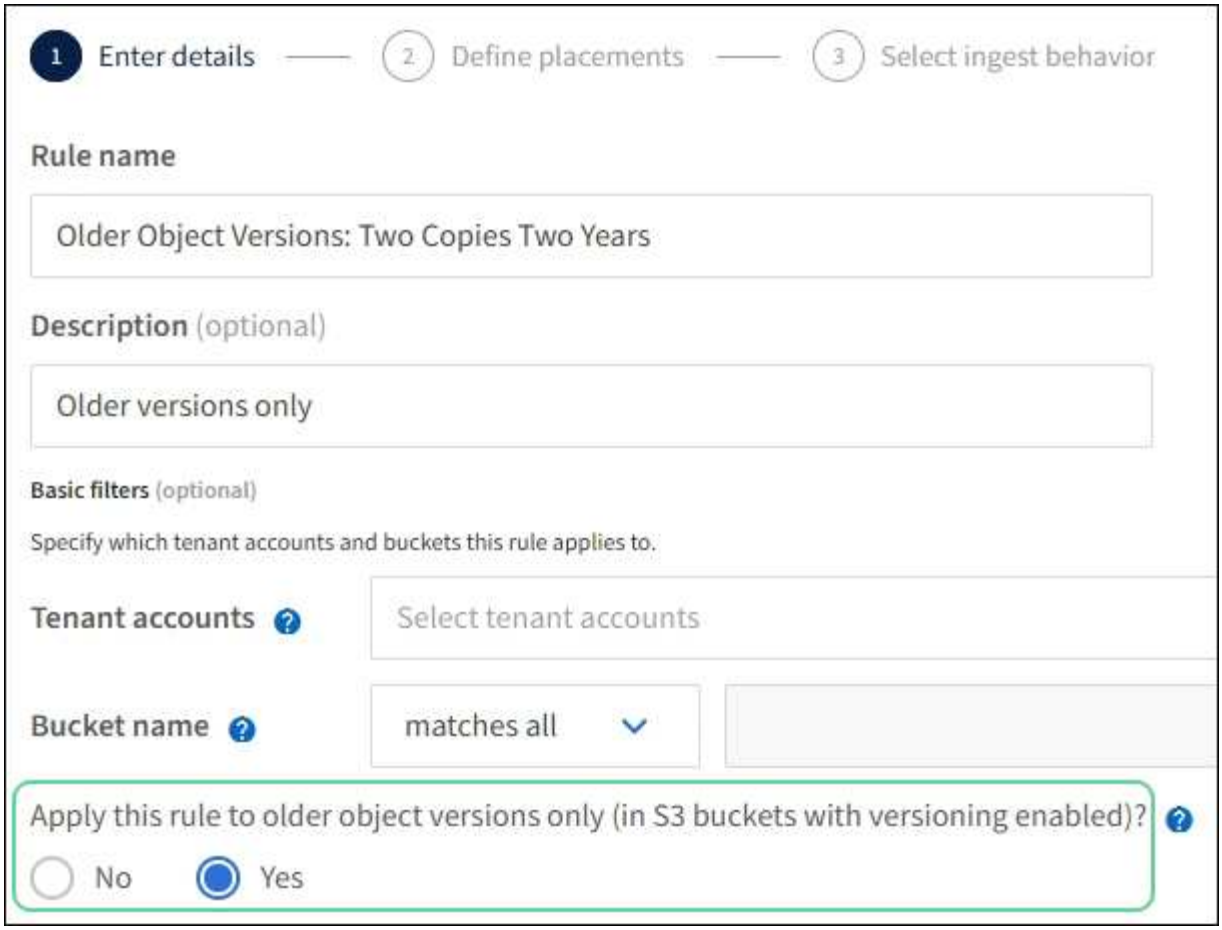
Regeldefinition	Beispielwert
Speicherpools	Drei Speicherpools, die jeweils aus unterschiedlichen Rechenzentren bestehen und als Site 1, Site 2 und Site 3 bezeichnet werden.
Regelname	Drei Kopien, zehn Jahre
Referenzzeit	Aufnahmezeit
Platzierungen	Bewahren Sie am Tag 0 drei replizierte Kopien 10 Jahre lang (3.652 Tage) auf, eine an Standort 1, eine an Standort 2 und eine an Standort 3. Löschen Sie nach 10 Jahren alle Kopien des Objekts.

ILM-Regel 2 für Beispiel 4: Zwei Kopien nicht aktueller Versionen für 2 Jahre aufbewahren

Dieses Beispiel einer ILM-Regel speichert zwei Kopien der nicht aktuellen Versionen eines versionierten S3-Objekts für zwei Jahre.

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

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



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

Regeldefinition	Beispielwert
Speicherpools	Zwei Speicherpools, jeweils in unterschiedlichen Rechenzentren, Standort 1 und Standort 2.
Regelname	Nicht aktuelle Versionen: Zwei Kopien, zwei Jahre
Referenzzeit	Nicht aktuelle Zeit Wird automatisch ausgewählt, wenn Sie im Assistenten „ILM-Regel erstellen“ bei der Frage „Diese Regel nur auf ältere Objektversionen anwenden (in S3-Buckets mit aktivierter Versionierung)?“ **Ja** auswählen.
Platzierungen	Bewahren Sie am Tag 0 relativ 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 2 Jahre (730 Tage) lang auf, eine an Standort 1 und eine an Standort 2. Löschen Sie nach zwei Jahren die nicht aktuellen Versionen.

ILM-Richtlinie für Beispiel 4: S3-versionierte Objekte

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

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

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

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

- Erstellen Sie beim Einlesen drei replizierte Kopien und speichern Sie an jedem der drei Standorte eine Kopie. Bewahren Sie Kopien der aktuellen Objektversion 10 Jahre lang auf.

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

- Alle nicht aktuellen Objektversionen würden mit der ersten Regel abgeglichen. Wenn eine nicht aktuelle Objektversion älter als 2 Jahre ist, wird sie von ILM dauerhaft gelöscht (alle Kopien der nicht aktuellen Version werden aus dem Grid entfernt).
- Die zweite Regel würde mit der aktuellen Objektversion übereinstimmen. Wenn die aktuelle Objektversion 10 Jahre lang gespeichert wurde, fügt der ILM-Prozess eine Löschmarkierung als aktuelle Version des Objekts hinzu und macht die vorherige Objektversion zu „nicht aktuell“. Bei der nächsten ILM-Auswertung wird diese nicht aktuelle Version mit der ersten Regel abgeglichen. Infolgedessen wird die Kopie an Standort 3 gelöscht und die beiden Kopien an Standort 1 und Standort 2 werden für weitere zwei Jahre gespeichert.

Beispiel 5: ILM-Regeln und -Richtlinien für striktes Aufnahmeverhalten

Sie können einen Standortfilter und das strikte Aufnahmeverhalten in einer Regel verwenden, um zu verhindern, dass Objekte an einem bestimmten Rechenzentrumsstandort gespeichert werden.

In diesem Beispiel möchte ein in Paris ansässiger Mieter einige Objekte aus rechtlichen Gründen nicht außerhalb der EU lagern. Andere Objekte, einschließlich aller Objekte aus anderen Mandantenkonten, können entweder im Pariser Rechenzentrum oder im US-Rechenzentrum gespeichert werden.

> Die folgenden ILM-Regeln und -Richtlinien sind nur Beispiele. Es gibt viele Möglichkeiten, ILM-Regeln zu konfigurieren. Bevor Sie eine neue Richtlinie aktivieren, simulieren Sie sie, um sicherzustellen, dass sie wie vorgesehen funktioniert und Inhalte vor Verlust schützt.

Ähnliche Informationen

- "Aufnahmeoptionen"
- "ILM-Regel erstellen: Aufnahmeverhalten auswählen"

ILM-Regel 1 für Beispiel 5: Strikte Aufnahme zur Gewährleistung des Pariser Rechenzentrums

Dieses Beispiel einer ILM-Regel verwendet das strikte Aufnahmeverhalten, um zu gewährleisten, dass Objekte, die von einem in Paris ansässigen Mandanten in S3-Buckets mit der auf die Region „eu-west-3“ (Paris) eingestellten Region gespeichert werden, niemals im US-Rechenzentrum gespeichert werden.

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

Regeldefinition	Beispielwert
Mieterkonto	Pariser Mieter
Erweiterter Filter	Standortbeschränkung entspricht eu-west-3
Speicherpools	Standort 1 (Paris)
Regelname	Strenge Aufnahme zur Gewährleistung des Pariser Rechenzentrums
Referenzzeit	Aufnahmezeit
Platzierungen	Behalten Sie am Tag 0 zwei replizierte Kopien für immer an Standort 1 (Paris).
Aufnahmeverhalten	Strikt. Verwenden Sie beim Aufnehmen immer die Platzierungen dieser Regel. Die Aufnahme schlägt fehl, wenn es nicht möglich ist, zwei Kopien des Objekts im Pariser Rechenzentrum zu speichern.

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

Dieses Beispiel einer ILM-Regel verwendet das ausgewogene Aufnahmeverhalten, um optimale ILM-Effizienz für alle Objekte bereitzustellen, die nicht der ersten Regel entsprechen. Von allen Objekten, die dieser Regel entsprechen, werden zwei Kopien gespeichert – eine im US-Rechenzentrum und eine im Pariser Rechenzentrum. Kann die Regel nicht sofort erfüllt werden, werden Zwischenkopien an einem beliebigen verfügbaren Ort gespeichert.

Diese Regel gilt für Objekte, die zu einem beliebigen Mandanten und einer beliebigen Region gehören.

Regeldefinition	Beispielwert
Mieterkonto	Ignorieren
Erweiterter Filter	*Nicht angegeben*
Speicherpools	Standort 1 (Paris) und Standort 2 (USA)
Regelname	2 Kopien 2 Rechenzentren

Regeldefinition	Beispielwert
Referenzzeit	Aufnahmezeit
Platzierungen	Bewahren Sie am Tag 0 zwei replizierte Kopien für immer in zwei Rechenzentren auf
Aufnahmeverhalten	Ausgewogen. Objekte, die dieser Regel entsprechen, werden nach Möglichkeit entsprechend den Platzierungsanweisungen der Regel platziert. Andernfalls werden Zwischenkopien an jedem verfügbaren Ort erstellt.

ILM-Richtlinie für Beispiel 5: Kombinieren von Aufnahmeverhalten

Die beispielhafte ILM-Richtlinie umfasst zwei Regeln mit unterschiedlichem Aufnahmeverhalten.

Eine ILM-Richtlinie, die zwei verschiedene Aufnahmeverhalten verwendet, kann ILM-Regeln wie die folgenden enthalten:

- Speichern Sie Objekte, die zum Pariser Mandanten gehören und deren S3-Bucket-Region auf eu-west-3 (Paris) eingestellt ist, nur im Pariser Rechenzentrum. Die Aufnahme schlägt fehl, wenn das Pariser Rechenzentrum nicht verfügbar ist.
- Speichern Sie alle anderen Objekte (einschließlich derjenigen, die zum Pariser Mandanten gehören, aber eine andere Bucket-Region haben) sowohl im US-Rechenzentrum als auch im Pariser Rechenzentrum. Erstellen Sie Zwischenkopien an einem beliebigen verfügbaren Ort, wenn die Platzierungsanweisung nicht erfüllt werden kann.

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

- Alle Objekte, die zum Pariser Mandanten gehören und deren S3-Bucket-Region auf „eu-west-3“ eingestellt ist, werden mit der ersten Regel abgeglichen und im Pariser Rechenzentrum gespeichert. Da die erste Regel die strikte Aufnahme 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 der Objekte, die zum Paris-Mandanten gehören und bei denen die S3-Bucket-Region nicht auf „eu-west-3“ eingestellt ist. In jedem Rechenzentrum wird eine Kopie jedes Objekts gespeichert. Da die zweite Regel jedoch eine ausgewogene Aufnahme verwendet, werden bei Nichtverfügbarkeit eines Rechenzentrums zwei Zwischenkopien an einem beliebigen verfügbaren Standort gespeichert.

Beispiel 6: Ändern einer ILM-Richtlinie

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

Bevor Sie eine Richtlinie ändern, müssen Sie verstehen, wie sich Änderungen an ILM-Platzierungen vorübergehend auf die Gesamtleistung eines StorageGRID Systems auswirken können.

In diesem Beispiel wurde im Rahmen einer Erweiterung ein neuer StorageGRID Standort hinzugefügt und es muss eine neue aktive ILM-Richtlinie implementiert werden, um Daten am neuen Standort zu speichern. Um eine neue aktive Richtlinie zu implementieren, müssen Sie zunächst"Erstellen einer Richtlinie" . Anschließend müssen Sie"simulieren" und dann"aktivieren" die neue Richtlinie.

Die folgenden ILM-Regeln und -Richtlinien sind nur Beispiele. Es gibt viele Möglichkeiten, ILM-Regeln zu konfigurieren. Bevor Sie eine neue Richtlinie aktivieren, simulieren Sie sie, um sicherzustellen, dass sie wie vorgesehen funktioniert und Inhalte vor Verlust schützt.

Auswirkungen der Änderung einer ILM-Richtlinie auf die Leistung

Wenn Sie eine neue ILM-Richtlinie aktivieren, kann die Leistung Ihres StorageGRID -Systems vorübergehend beeinträchtigt werden, insbesondere wenn die Platzierungsanweisungen in der neuen Richtlinie erfordern, dass viele vorhandene Objekte an neue Speicherorte verschoben werden.

Wenn Sie eine neue ILM-Richtlinie aktivieren, verwendet StorageGRID diese zum Verwalten aller Objekte, einschließlich vorhandener und neu aufgenommener Objekte. Überprüfen Sie vor der Aktivierung einer neuen ILM-Richtlinie alle Änderungen an der Platzierung vorhandener replizierter und löschcodierter Objekte. Das Ändern des Standorts eines vorhandenen Objekts kann zu vorübergehenden Ressourcenproblemen führen, wenn die neuen Platzierungen ausgewertet und implementiert werden.

Um sicherzustellen, dass eine neue ILM-Richtlinie keinen Einfluss auf die Platzierung vorhandener replizierter und erasure-coded Objekte hat, können Sie"Erstellen Sie eine ILM-Regel mit einem Aufnahmezeitfilter" . Beispiel: **Aufnahmezeit *ist am oder nach <Datum und Uhrzeit>***, sodass die neue Regel nur für Objekte gilt, die am oder nach dem angegebenen Datum und der angegebenen Uhrzeit aufgenommen wurden.

Zu den Arten von ILM-Richtlinienänderungen, die die Leistung von StorageGRID vorübergehend beeinträchtigen können, gehören die folgenden:

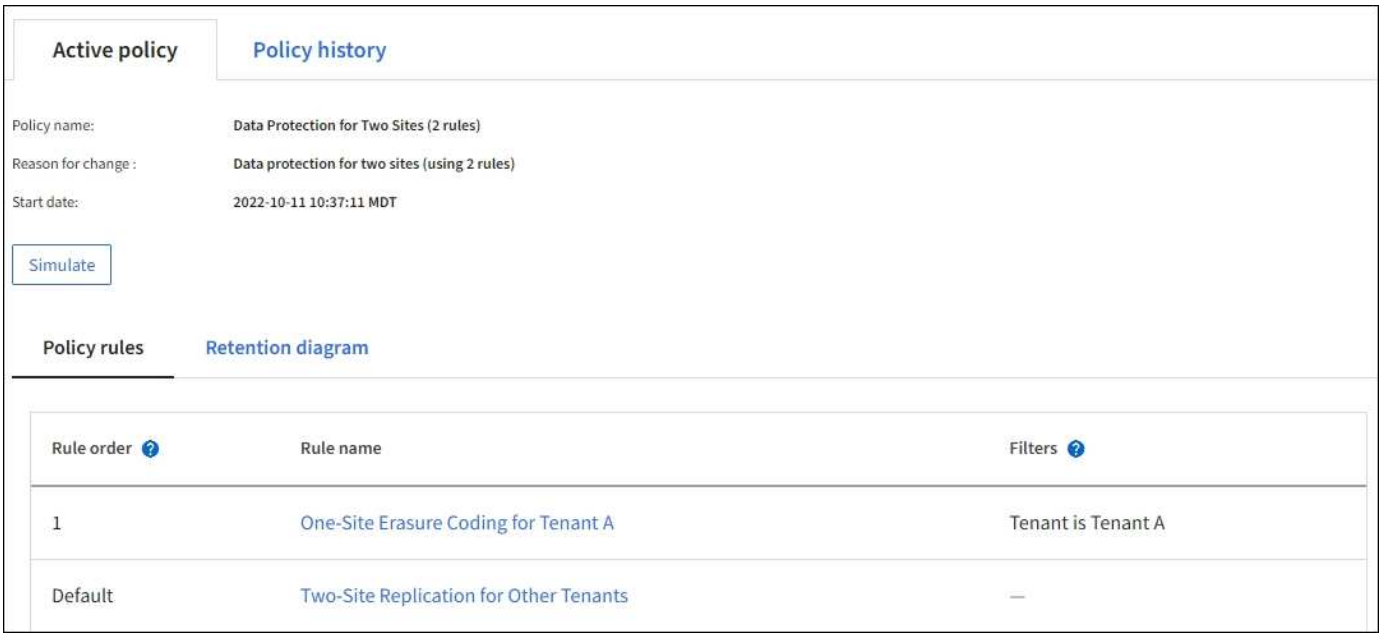
- Anwenden eines anderen Erasure-Coding-Profils auf vorhandene Erasure-Coding-Objekte.

  StorageGRID betrachtet jedes Erasure-Coding-Profil als einzigartig und verwendet Erasure-Coding-Fragmente nicht erneut, wenn ein neues Profil verwendet wird.

- Ändern des Typs der Kopien, die für vorhandene Objekte erforderlich sind. Beispielsweise das Konvertieren eines großen Prozentsatzes replizierter Objekte in Erasure-Coded-Objekte.
- Verschieben von Kopien vorhandener Objekte an einen völlig anderen Ort; beispielsweise das Verschieben einer großen Anzahl von Objekten in oder aus einem Cloud-Speicherpool oder zu oder von einem Remote-Standort.

Aktive ILM-Richtlinie für Beispiel 6: Datenschutz an zwei Standorten

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



In dieser ILM-Richtlinie werden Objekte des Mandanten A durch 2+1-Löschcodierung an einem einzelnen Standort geschützt, während Objekte aller anderen Mandanten über zwei Standorte hinweg durch 2-Kopien-Replikation geschützt werden.

Regel 1: One-Site-Erasure-Coding für Mandant A

Regeldefinition	Beispielwert
Regelname	One-Site Erasure Coding für Mieter A
Mandantenkonto	Mieter A
Speicherpool	Standort 1
Platzierungen	2+1 Erasure Coding in Site 1 von Tag 0 bis für immer

Regel 2: Zwei-Site-Replikation für andere Mandanten

Regeldefinition	Beispielwert
Regelname	Zwei-Site-Replikation für andere Mandanten
Mandantenkonto	Ignorieren
Speicherpools	Standort 1 und Standort 2
Platzierungen	Zwei replizierte Kopien vom Tag 0 bis in alle Ewigkeit: eine Kopie an Standort 1 und eine Kopie an Standort 2.

ILM-Richtlinie für Beispiel 6: Datenschutz an drei Standorten

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

Nachdem der Grid-Administrator eine Erweiterung zum Hinzufügen der neuen Site durchgeführt hatte, erstellte er zwei neue Speicherpools: einen Speicherpool für Site 3 und einen Speicherpool, der alle drei Sites enthält (nicht derselbe wie der Standardspeicherpool „Alle Speicherknoten“). Anschließend erstellte der Administrator zwei neue ILM-Regeln und eine neue ILM-Richtlinie, die dem Schutz der Daten an allen drei Standorten dienen soll.

Wenn diese neue ILM-Richtlinie aktiviert wird, werden Objekte von Mandant A durch 2+1-Löschcodierung an drei Standorten geschützt, während Objekte anderer Mandanten (und kleinere Objekte von Mandant A) an drei Standorten durch 3-Kopien-Replikation geschützt werden.

Regel 1: Drei-Site-Löschcodierung für Mandant A

Regeldefinition	Beispielwert
Regelname	Drei-Site-Erasure-Coding für Mieter A
Mandantenkonto	Mieter A
Speicherpool	Alle 3 Standorte (einschließlich Standort 1, Standort 2 und Standort 3)
Platzierungen	2+1 Erasure Coding an allen 3 Standorten vom Tag 0 bis für immer

Regel 2: Drei-Standort-Replikation für andere Mandanten

Regeldefinition	Beispielwert
Regelname	Drei-Site-Replikation für andere Mandanten
Mandantenkonto	Ignorieren
Speicherpools	Standort 1, Standort 2 und Standort 3
Platzierungen	Drei replizierte Kopien vom Tag 0 bis in alle Ewigkeit: eine Kopie an Standort 1, eine Kopie an Standort 2 und eine Kopie an Standort 3.

Aktivieren der ILM-Richtlinie für Beispiel 6

Wenn Sie eine neue ILM-Richtlinie aktivieren, werden vorhandene Objekte möglicherweise an neue Speicherorte verschoben oder es werden neue Objektkopien für vorhandene Objekte erstellt, basierend auf den Platzierungsanweisungen in neuen oder aktualisierten Regeln.

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

Wenn Sie eine neue ILM-Richtlinie aktivieren, verwendet StorageGRID diese zum Verwalten aller Objekte, einschließlich vorhandener und neu aufgenommener Objekte. Überprüfen Sie vor der Aktivierung einer neuen ILM-Richtlinie alle Änderungen an der Platzierung vorhandener replizierter und löschcodierter Objekte. Das Ändern des Standorts eines vorhandenen Objekts kann zu vorübergehenden Ressourcenproblemen führen, wenn die neuen Platzierungen ausgewertet und implementiert werden.

Was passiert, wenn sich die Anweisungen zur Erasure-Codierung ändern?

In der derzeit aktiven ILM-Richtlinie für dieses Beispiel werden Objekte des Mandanten A mithilfe von 2+1-Löschcodierung an Standort 1 geschützt. In der neuen ILM-Richtlinie werden Objekte des Mandanten A mithilfe von 2+1-Löschcodierung an den Standorten 1, 2 und 3 geschützt.

Wenn die neue ILM-Richtlinie aktiviert wird, werden die folgenden ILM-Vorgänge ausgeführt:

- Neue, von Mandant A aufgenommene Objekte werden in zwei Datenfragmente aufgeteilt und ein Paritätsfragment wird hinzugefügt. Anschließend wird jedes der drei Fragmente an einem anderen Ort gespeichert.
- Die vorhandenen Objekte des Mandanten A werden während des laufenden ILM-Scan-Prozesses neu ausgewertet. Da die ILM-Platzierungsanweisungen ein neues Erasure-Coding-Profil verwenden, werden völlig neue Erasure-Coding-Fragmente erstellt und an die drei Standorte verteilt.

Die vorhandenen 2+1-Fragmente an Standort 1 werden nicht wiederverwendet. StorageGRID betrachtet jedes Erasure-Coding-Profil als einzigartig und verwendet Erasure-Coding-Fragmente nicht erneut, wenn ein neues Profil verwendet wird.

Was passiert, wenn sich Replikationsanweisungen ändern?

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

Wenn die neue ILM-Richtlinie aktiviert wird, werden die folgenden ILM-Vorgänge ausgeführt:

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

Auswirkungen der Aktivierung dieser Richtlinie auf die Leistung

Wenn die ILM-Richtlinie in diesem Beispiel aktiviert wird, wird die Gesamtleistung dieses StorageGRID Systems vorübergehend beeinträchtigt. Es werden mehr Grid-Ressourcen als üblich benötigt, um neue Erasure-Code-Fragmente für die vorhandenen Objekte von Mandant A und neue replizierte Kopien an Standort 3 für die vorhandenen Objekte anderer Mandanten zu erstellen.

Aufgrund der Änderung der ILM-Richtlinie kann es bei Lese- und Schreibanforderungen des Clients vorübergehend zu höheren Latenzen als normal kommen. Die Latenzen werden wieder auf ein normales Niveau zurückkehren, nachdem die Platzierungsanweisungen im gesamten Raster vollständig implementiert

wurden.

Um Ressourcenprobleme beim Aktivieren einer neuen ILM-Richtlinie zu vermeiden, können Sie den erweiterten Filter „Aufnahmezeit“ in jeder Regel verwenden, die den Speicherort einer großen Anzahl vorhandener Objekte ändern könnte. Legen Sie die Aufnahmezeit so fest, dass sie größer oder gleich der ungefähren Zeit ist, 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 Geschwindigkeit, mit der Objekte nach einer Änderung der ILM-Richtlinie verarbeitet werden, verlangsamen oder erhöhen müssen.

Beispiel 7: Konforme ILM-Richtlinie für S3 Object Lock

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

Wenn Sie die alte Compliance-Funktion in früheren StorageGRID Versionen verwendet haben, können Sie dieses Beispiel auch zur Verwaltung aller vorhandenen Buckets verwenden, bei denen die alte Compliance-Funktion aktiviert ist.

Die folgenden ILM-Regeln und -Richtlinien sind nur Beispiele. Es gibt viele Möglichkeiten, ILM-Regeln zu konfigurieren. Bevor Sie eine neue Richtlinie aktivieren, simulieren Sie sie, um sicherzustellen, dass sie wie vorgesehen funktioniert und Inhalte vor Verlust schützt.

Ähnliche Informationen

- "Verwalten von Objekten mit S3 Object Lock"
- "Erstellen einer ILM-Richtlinie"

Bucket und Objekte für S3 Object Lock-Beispiel

In diesem Beispiel hat ein S3-Mandantenkonto mit dem Namen Bank of ABC den Mandantenmanager verwendet, um einen Bucket mit aktivierter S3-Objektsperre zum Speichern wichtiger Bankdaten zu erstellen.

Bucket-Definition	Beispielwert
Mandantenkontoname	Bank von ABC
Bucket-Name	Bankunterlagen
Bucket-Region	us-east-1 (Standard)

Jedes Objekt und jede Objektversion, die zum Bucket „Bankunterlagen“ hinzugefügt wird, verwendet 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.
`legal hold`	„AUS“ (Nicht wirksam) Eine rechtliche Sperre kann für jede Objektversion jederzeit während der Aufbewahrungsfrist verhängt oder aufgehoben werden. Wenn ein Objekt einer rechtlichen Sperre unterliegt, kann das Objekt nicht gelöscht werden, auch wenn `retain-until-date` erreicht ist.

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

Diese beispielhafte ILM-Regel gilt nur für das S3-Mandantenkonto mit dem Namen Bank of ABC. Es passt zu jedem Objekt in der `bank-records` Bucket und verwendet dann Erasure Coding, um das Objekt auf Speicherknoten an drei Rechenzentrumsstandorten unter Verwendung eines 6+3-Erasure-Coding-Profils zu speichern. Diese Regel erfüllt die Anforderungen von Buckets mit aktivierter S3-Objektsperre: Eine Kopie wird vom Tag 0 bis in alle Ewigkeit auf den Speicherknoten aufbewahrt, wobei die Aufnahmezeit als Referenzzeit verwendet wird.

Regeldefinition	Beispielwert
Regelname	Konforme Regel: EC-Objekte im Bankaufzeichnungs-Bucket – Bank of ABC
Mandantenkonto	Bank von ABC
Bucket-Name	`bank-records`
Erweiterter Filter	Objektgröße (MB) größer als 1 **Hinweis:** Dieser Filter stellt sicher, dass Erasure Coding nicht für Objekte mit 1 MB oder weniger verwendet wird.

Regeldefinition	Beispielwert
Referenzzeit	Aufnahmezeit
Platzierungen	Ab Tag 0 für immer speichern
Erasure-Coding-Profil	• Erstellen Sie eine Löschcodierte Kopie auf Speicherknoten an drei Rechenzentrumsstandorten • Verwendet das 6+3-Erasure-Coding-Schema

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

Diese beispielhafte ILM-Regel speichert zunächst zwei replizierte Objektkopien auf Speicherknoten. Nach einem Jahr wird eine Kopie dauerhaft in einem Cloud-Speicherpool gespeichert. Da diese Regel einen Cloud-Speicherpool verwendet, ist sie nicht konform und gilt nicht für Objekte in Buckets mit aktivierter S3-Objektsperre.

Regeldefinition	Beispielwert
Regelname	Nicht konforme Regel: Cloud-Speicherpool verwenden
Mandantenkonten	Nicht angegeben
Bucket-Name	Nicht angegeben, gilt aber nur für Buckets, bei denen S3 Object Lock (oder die alte Compliance-Funktion) nicht aktiviert ist.
Erweiterter Filter	Nicht angegeben

Regeldefinition	Beispielwert
Referenzzeit	Aufnahmezeit
Platzierungen	• Bewahren Sie am Tag 0 zwei replizierte Kopien auf Speicherknoten in Rechenzentrum 1 und Rechenzentrum 2 für 365 Tage auf • Behalten Sie nach einem Jahr eine replizierte Kopie für immer in einem Cloud-Speicherpool

ILM-Regel 3 für S3 Object Lock-Beispiel: Standardregel

Diese beispielhafte ILM-Regel kopiert Objektdaten in Speicherpools in zwei Rechenzentren. Diese konforme Regel ist als Standardregel in der ILM-Richtlinie konzipiert. Es enthält keine Filter, verwendet nicht die nicht aktuelle Referenzzeit und erfüllt die Anforderungen von Buckets mit aktivierter S3-Objektsperre: Zwei Objektkopien werden von Tag 0 bis auf unbestimmte Zeit auf Speicherknoten aufbewahrt, wobei Ingest als Referenzzeit verwendet wird.

Regeldefinition	Beispielwert
Regelname	Standardkonforme Regel: Zwei Kopien, zwei Rechenzentren
Mieterkonto	Nicht angegeben
Bucket-Name	Nicht angegeben
Erweiterter Filter	Nicht angegeben

Regeldefinition	Beispielwert
Referenzzeit	Aufnahmezeit

Regeldefinition	Beispielwert
Platzierungen	Bewahren Sie von Tag 0 bis in alle Ewigkeit zwei replizierte Kopien auf – eine auf Speicherknoten in Rechenzentrum 1 und eine auf Speicherknoten in Rechenzentrum 2.

Konforme ILM-Richtlinie für S3 Object Lock-Beispiel

Um eine ILM-Richtlinie zu erstellen, die alle Objekte in Ihrem System wirksam schützt, einschließlich der Objekte in Buckets mit aktivierter S3-Objektsperre, müssen Sie ILM-Regeln auswählen, die die Speicheranforderungen für alle Objekte erfüllen. Anschließend müssen Sie die Richtlinie simulieren und aktivieren.

Regeln zur Richtlinie hinzufügen

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

1. Eine konforme Regel, die Erasure Coding verwendet, um Objekte mit mehr als 1 MB in einem bestimmten Bucket mit aktivierter S3-Objektsperre zu schützen. Die Objekte werden vom Tag 0 bis in alle Ewigkeit auf Speicherknoten gespeichert.
2. Eine nicht konforme Regel, die ein Jahr lang zwei replizierte Objektkopien auf Speicherknoten erstellt und dann eine Objektkopie dauerhaft in einen Cloud-Speicherpool verschiebt. Diese Regel gilt nicht für Buckets mit aktivierter S3-Objektsperre, da diese einen Cloud-Speicherpool verwenden.
3. Die standardmäßige konforme Regel, die vom Tag 0 bis in alle Ewigkeit zwei replizierte Objektkopien auf Speicherknoten erstellt.

Simulieren Sie die Richtlinie

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

- Die erste Regel stimmt nur mit Testobjekten überein, die im Bucket „Bankdatensätze“ für den Mandanten der Bank of ABC größer als 1 MB sind.
- Die zweite Regel gleicht alle Objekte in allen nicht konformen Buckets für alle anderen Mandantenkonten ab.
- Die Standardregel trifft auf diese Objekte zu:
  - Objekte mit 1 MB oder weniger im Bucket „Bankunterlagen“ für den Mandanten der Bank of ABC.
  - Objekte in jedem anderen Bucket, für den S3 Object Lock für alle anderen Mandantenkonten aktiviert ist.

Aktivieren der Richtlinie

Wenn Sie vollständig davon überzeugt sind, dass die neue Richtlinie die Objektdaten wie erwartet schützt, können Sie sie aktivieren.

Beispiel 8: Prioritäten für den S3-Bucket-Lebenszyklus und die ILM-Richtlinie

Abhängig von Ihrer Lebenszykluskonfiguration folgen Objekte entweder den

Aufbewahrungseinstellungen des S3-Bucket-Lebenszyklus oder einer ILM-Richtlinie.

Beispiel für den Bucket-Lebenszyklus, der Vorrang vor der ILM-Richtlinie hat

ILM-Richtlinie

- Regel basierend auf einem nicht aktuellen Zeitbezug: Am Tag 0 X Kopien 20 Tage lang aufbewahren
- Regel basierend auf der Aufnahmezeitreferenz (Standard): Am Tag 0 X Kopien 50 Tage lang aufbewahren

Bucket-Lebenszyklus

```
"Filter": {"Prefix": "docs/"}, "Expiration": {"Days": 100},
"NoncurrentVersionExpiration": {"NoncurrentDays": 5}
```

Ergebnis

- Ein Objekt mit dem Namen „docs/text“ wird aufgenommen. Es entspricht dem Bucket-Lebenszyklusfilter des Präfixes „docs/“.
  - Nach 100 Tagen wird eine Löschmarkierung erstellt und „docs/text“ wird nicht mehr aktuell.
  - Nach 5 Tagen, insgesamt 105 Tage seit der Aufnahme, wird „docs/text“ gelöscht.
  - Nach 95 Tagen, also insgesamt 200 Tagen seit der Aufnahme und 100 Tagen seit der Erstellung des Löschmarkers, wird der abgelaufene Löschmarker gelöscht.
- Ein Objekt mit dem Namen „Video/Film“ wird aufgenommen. Es entspricht nicht dem Filter und verwendet die ILM-Aufbewahrungsrichtlinie.
  - Nach 50 Tagen wird eine Löschmarkierung erstellt und „Video/Film“ wird nicht mehr aktuell.
  - Nach 20 Tagen, also insgesamt 70 Tagen seit der Aufnahme, wird „Video/Film“ gelöscht.
  - Nach 30 Tagen, also insgesamt 100 Tagen seit der Aufnahme und 50 Tagen seit der Erstellung des Löschmarkers, wird der abgelaufene Löschmarker gelöscht.

Beispiel für den Bucket-Lebenszyklus mit impliziter ewiger Aufbewahrung

ILM-Richtlinie

- Regel basierend auf einem nicht aktuellen Zeitbezug: Am Tag 0 X Kopien 20 Tage lang aufbewahren
- Regel basierend auf der Aufnahmezeitreferenz (Standard): Am Tag 0 X Kopien 50 Tage lang aufbewahren

Bucket-Lebenszyklus

```
"Filter": {"Prefix": "docs/"}, "Expiration": {"ExpiredObjectDeleteMarker":
true}
```

Ergebnis

- Ein Objekt mit dem Namen „docs/text“ wird aufgenommen. Es entspricht dem Bucket-Lebenszyklusfilter des Präfixes „docs/“.

  Der `Expiration` Die Aktion gilt nur für abgelaufene Löschmarkierungen, was bedeutet, dass alles andere (beginnend mit „docs/“) für immer erhalten bleibt.

  Löschmarkierungen, die mit „docs/“ beginnen, werden entfernt, wenn sie ablaufen.

- Ein Objekt mit dem Namen „Video/Film“ wird aufgenommen. Es entspricht nicht dem Filter und verwendet die ILM-Aufbewahrungsrichtlinie.

- Nach 50 Tagen wird eine Löschmarkierung erstellt und „Video/Film“ wird nicht mehr aktuell.
- Nach 20 Tagen, also insgesamt 70 Tagen seit der Aufnahme, wird „Video/Film“ gelöscht.
- Nach 30 Tagen, also insgesamt 100 Tagen seit der Aufnahme und 50 Tagen seit der Erstellung des Löschmarkers, wird der abgelaufene Löschmarker gelöscht.

Beispiel für die Verwendung des Bucket-Lebenszyklus zum Duplizieren von ILM und Bereinigen abgelaufener Löschmarkierungen

ILM-Richtlinie

- Regel basierend auf einem nicht aktuellen Zeitbezug: Am Tag 0 X Kopien 20 Tage lang aufbewahren
- Regel basierend auf der Aufnahmezeitreferenz (Standard): Am Tag 0 X Kopien für immer behalten

Bucket-Lebenszyklus

```
"Filter": {}, "Expiration": {"ExpiredObjectDeleteMarker": true},
"NoncurrentVersionExpiration": {"NoncurrentDays": 20}
```

Ergebnis

- Die ILM-Richtlinie wird im Bucket-Lebenszyklus dupliziert.
  - Die „Für immer“-Regel der ILM-Richtlinie ist darauf ausgelegt, Objekte manuell zu entfernen und nicht aktuelle Versionen nach 20 Tagen zu bereinigen. Folglich behält die Aufnahmezeitregel abgelaufene Löschmarkierungen für immer bei.
  - Der Bucket-Lebenszyklus dupliziert das Verhalten der ILM-Richtlinie und fügt hinzu `"ExpiredObjectDeleteMarker": true` , wodurch Löschmarkierungen entfernt werden, sobald sie abgelaufen sind
- Ein Gegenstand wird verschluckt. Kein Filter bedeutet, dass der Bucket-Lebenszyklus für alle Objekte gilt und die ILM-Aufbewahrungseinstellungen überschreibt.
  - Wenn ein Mandant eine Anforderung zum Löschen eines Objekts ausgibt, wird eine Löschmarkierung erstellt und das Objekt wird nicht mehr aktuell.
  - Nach 20 Tagen wird das nicht aktuelle Objekt gelöscht und die Löschmarkierung läuft ab.
  - Kurz darauf wird der abgelaufene Löschmarker gelöscht.