Objekte mit ILM verwalten

StorageGRID software

NetApp
July 23, 2026

Inhalt

Objekte mit ILM verwalten

Objekte mit ILM in StorageGRID verwalten

Die Regeln für das Informationslebenszyklusmanagement (ILM) in einer ILM-Richtlinie geben StorageGRID Anweisungen, wie Kopien von Objektdaten erstellt und verteilt werden und wie diese Kopien im Laufe der Zeit verwaltet werden.

Über diese Anweisungen

Die Entwicklung und Implementierung von ILM-Regeln und -Richtlinien erfordert sorgfältige Planung. Es ist erforderlich, die betrieblichen Anforderungen, die Topologie des StorageGRID Systems, die Anforderungen an den Objektschutz und die verfügbaren Speichertypen zu verstehen. Anschließend ist festzulegen, wie verschiedene Objekttypen kopiert, verteilt und gespeichert werden.

Diese Anweisungen dienen dazu:

- Informationen zu StorageGRID ILM, einschließlich "wie ILM während der gesamten Lebensdauer eines Objekts funktioniert".
- Informationen zur Konfiguration von "Storage Pools", "Cloud-Storage-Pools" und "ILM Regeln".
- Informationen dazu, wie "Erstellen, simulieren und Aktivieren einer ILM-Policy" Objektdaten über eine oder mehrere Standorte hinweg geschützt werden können.
- Informationen dazu, wie "Objekte mit S3 Object Lock verwalten" implementiert werden kann, was dazu beiträgt, dass Objekte in bestimmten S3-Buckets für einen festgelegten Zeitraum weder gelöscht noch überschrieben werden.

Mehr erfahren

Weitere Informationen bieten diese Videos:

Überblick über ILM-Regeln

Überblick über ILM-Richtlinien

ILM und Objektlebenszyklus

Wie ILM während des gesamten Lebenszyklus eines Objekts in StorageGRID funktioniert

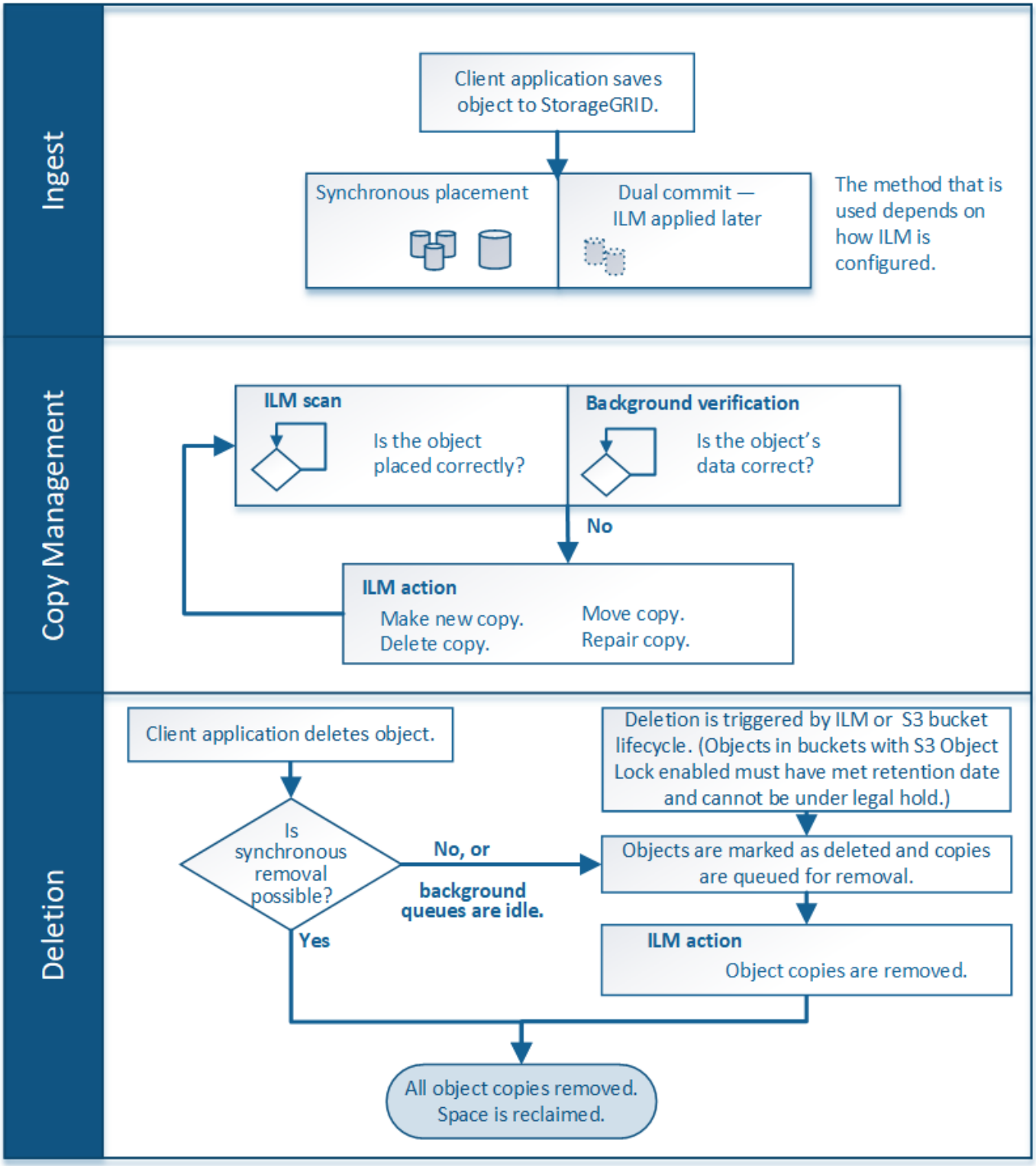
Das Verständnis dafür, wie StorageGRID ILM zur Verwaltung von Objekten in jeder Phase ihres Lebenszyklus einsetzt, kann bei der Entwicklung einer effektiveren Richtlinie unterstützen.

- **Datenaufnahme**: Die Datenaufnahme beginnt, sobald eine S3-Clientanwendung eine Verbindung zum StorageGRID System herstellt, um ein Objekt zu speichern, und ist abgeschlossen, wenn StorageGRID dem Client die Meldung „ingest successful“ zurückgibt. Die Objektdaten werden während der Datenaufnahme geschützt, entweder durch sofortige Anwendung von ILM-Anweisungen (synchron Platzierung) oder durch Erstellung von Zwischenkopien und spätere Anwendung von ILM (dual commit), abhängig davon, wie die ILM-Anforderungen spezifiziert wurden.

- **Kopienverwaltung**: Nachdem die in den Platzierungsanweisungen des ILM festgelegte Anzahl und Art der Objektkopien erstellt wurden, verwaltet StorageGRID die Objektspeicherorte und schützt die Objekte vor Verlust.
  - **ILM-Scan und -Bewertung**: StorageGRID scannt kontinuierlich die Liste der im Grid gespeicherten Objekte und prüft, ob die aktuellen Kopien den ILM-Anforderungen entsprechen. Wenn andere Arten, Anzahlen oder Speicherorte von Objektkopien erforderlich sind, erstellt, löscht oder verschiebt StorageGRID die Kopien nach Bedarf.
  - **Hintergrundprüfung**: StorageGRID führt kontinuierlich eine Hintergrundprüfung durch, um die Integrität der Objektdaten zu überprüfen. Wenn ein Problem festgestellt wird, erstellt StorageGRID automatisch eine neue Objektkopie oder ein Ersatzfragment eines löschcodierten Objekts an einem Ort, der den aktuellen ILM-Anforderungen entspricht. Siehe "Objektintegrität verifizieren".
- **Objektlöschung**: Die Verwaltung eines Objekts endet, wenn alle Kopien aus dem StorageGRID System entfernt wurden. Objekte können infolge einer Löschanforderung eines Clients, durch Löschung durch ILM oder durch Löschung infolge des Ablaufs eines S3-Bucket-Lebenszyklus entfernt werden.

> Objekte in einem Bucket, für den S3 Object Lock aktiviert ist, können nicht gelöscht werden, wenn sie einer rechtlichen Aufbewahrung 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

ILM-Aufnahmeoptionen in StorageGRID

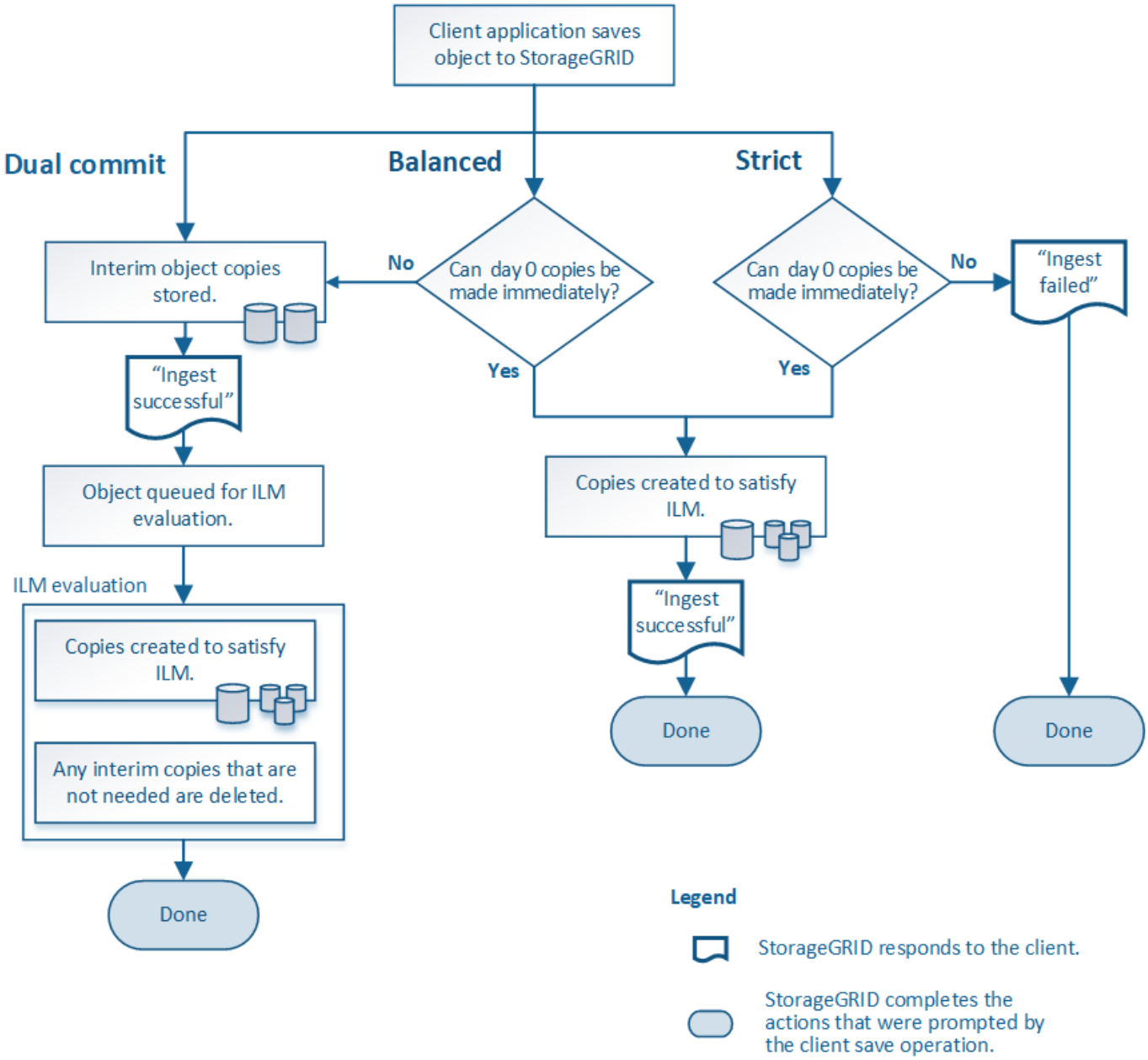
Beim Erstellen einer ILM-Regel wird eine von drei Optionen zum Schutz von Objekten beim Import angegeben: Dual commit, Strict oder Balanced.

Je nach Auswahl erstellt StorageGRID Zwischenkopien und stellt die Objekte zur späteren ILM-Auswertung in

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

Ablaufdiagramm der Aufnahmeoptionen

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



Dual Commit

Wenn Sie die Option „Dual commit“ auswählen, erstellt StorageGRID sofort temporäre Objektkopien auf zwei verschiedenen Storage Nodes und sendet eine „Ingest erfolgreich“-Meldung an den Client zurück. Das Objekt wird zur ILM-Auswertung in die Warteschlange gestellt, und Kopien, die den Platzierungsanweisungen der Regel entsprechen, werden später erstellt. Wenn die ILM-Policy nicht unmittelbar nach dem Dual commit verarbeitet werden kann, kann es einige Zeit dauern, bis der Schutz vor Standortverlust erreicht ist.

Die Option „Dual Commit“ kommt in einem der folgenden Fälle zum Einsatz:

- Sie verwenden Multi-Site-ILM-Regeln, wobei die Latenz beim Client-Ingest für Sie von größter Bedeutung ist. Bei Verwendung von Dual commit muss sichergestellt werden, dass Ihr Grid die zusätzlichen Aufgaben zum Erstellen und Entfernen der Dual-commit-Kopien bewältigen kann, falls diese die ILM-Anforderungen nicht erfüllen. Konkret:
  - Die Netzlast muss niedrig genug sein, um einen ILM-Rückstand zu vermeiden.
  - Das Grid muss über überschüssige Hardware-Ressourcen (IOPS, CPU, Speicher, Netzwerkbandbreite usw.) verfügen.
- Sie verwenden standortübergreifende ILM-Regeln, und die WAN-Verbindung zwischen den Standorten weist üblicherweise eine hohe Latenz oder begrenzte Bandbreite auf. In diesem Szenario kann die Option Dual commit dazu beitragen, Client-Timeouts zu verhindern. Vor der Auswahl der Option Dual commit empfiehlt sich ein Test der Client-Anwendung mit realistischen Arbeitslasten.

Ausgewogen (Standard)

Wenn die Option Balanced ausgewählt wird, verwendet StorageGRID ebenfalls die synchrone Platzierung beim Ingest und erstellt sofort alle in den Platzierungsanweisungen der Regel angegebenen Kopien. Im Gegensatz zur Option Strict verwendet StorageGRID, falls nicht alle Kopien sofort erstellt werden können, stattdessen Dual commit. Wenn die ILM-Richtlinie Platzierungen an mehreren Standorten vorsieht und ein sofortiger Schutz vor Standortverlust nicht erreicht werden kann, wird die Warnung **ILM placement unachievable** ausgelöst.

Die Option „Ausgewogen“ bietet die beste Kombination aus Datenschutz, Grid-Performance und erfolgreicher Datenerfassung. „Ausgewogen“ ist die Standardoption im Assistenten zum Erstellen von ILM-Regeln.

Strikt

Bei Auswahl der Option „Streng“ verwendet StorageGRID synchrone Platzierung beim Ingest und erstellt sofort alle in den Platzierungsanweisungen der Regel angegebenen Objektkopien. Der Ingest 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 Sie aufgrund betrieblicher oder regulatorischer Vorgaben Objekte ausschließlich an den in der ILM-Regel festgelegten Standorten speichern müssen. Um beispielsweise eine regulatorische Anforderung zu erfüllen, kann es erforderlich sein, die Option „Streng“ und einen erweiterten Filter für Standortbeschränkungen zu verwenden, um zu gewährleisten, dass Objekte niemals in bestimmten Rechenzentren gespeichert werden.

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

Vorteile, Nachteile und Einschränkungen der ILM-Ingest-Optionen in StorageGRID

Das Verständnis der Vor- und Nachteile der drei Optionen zum Schutz von Daten bei der Datenerfassung (Balanced, Strict oder Dual commit) kann bei der Entscheidung unterstützen, welche Option für eine ILM-Regel ausgewählt wird.

Eine Übersicht über die Aufnahmeoptionen ist unter "Aufnahmeoptionen" zu finden.

Vorteile der Optionen „Ausgewogen“ und „Streng“

Im Vergleich zu Dual Commit, das während der Datenaufnahme Zwischenkopien erstellt, können die beiden synchronen Platzierungsoptionen folgende Vorteile bieten:

- **Verbesserte Datensicherheit**: Objektdaten werden gemäß den Platzierungsanweisungen der ILM-Regel

sofort geschützt, die so konfiguriert werden können, dass sie gegen eine Vielzahl von Ausfallszenarien schützen, einschließlich des Ausfalls von mehr als einem Speicherort. Dual Commit kann nur gegen den Verlust einer einzelnen lokalen Kopie schützen.

- **Effizienterer Grid-Betrieb**: Jedes Objekt wird nur einmal verarbeitet, sobald es erfasst wird. Da das StorageGRID System keine Zwischenkopien verfolgen oder löschen muss, fällt eine geringere Verarbeitungslast an und es wird weniger Datenbankspeicherplatz benötigt.
- **(Ausgewogen) Empfohlen**: Die Option „Ausgewogen“ bietet optimale ILM-Effizienz. Die Verwendung der Option „Ausgewogen“ wird empfohlen, es sei denn, ein striktes Aufnahmeverhalten ist erforderlich oder das Grid erfüllt alle Kriterien für die Verwendung von Dual commit.
- **(Strenge) Gewissheit über Objektpositionen**: Die Option Strict garantiert, dass Objekte gemäß den Platzierungsanweisungen in der ILM-Regel sofort gespeichert werden.

Nachteile der Optionen „Balanced“ und „Strict“

Im Vergleich zu Dual commit weisen die Optionen Balanced und Strict einige Nachteile auf:

- **Längere Client-Datenerfassung**: Die Latenzzeiten für die Client-Datenerfassung können länger sein. Bei Verwendung der Optionen „Balanced“ oder „Strict“ wird eine Meldung „Datenerfassung erfolgreich“ erst dann an den Client zurückgegeben, wenn alle Erasure-Coding-Fragmente oder Replikatkopien erstellt und gespeichert wurden. Die Objektdaten erreichen ihren endgültigen Speicherort jedoch höchstwahrscheinlich deutlich schneller.
- **(Streng) Höhere Fehlerraten beim Ingest**: Bei der Option „Streng“ schlägt der Ingest fehl, wenn StorageGRID nicht sofort alle in der ILM-Regel festgelegten Kopien erstellen kann. Hohe Fehlerraten beim Ingest können auftreten, wenn ein erforderlicher Speicherort vorübergehend offline ist oder Netzwerkprobleme das Kopieren von Objekten zwischen Standorten verzögern.
- **(Strenge) Platzierungen bei S3-Multipart-Uploads entsprechen unter Umständen nicht den Erwartungen**: Mit der Einstellung "Strict" wird erwartet, dass Objekte entweder gemäß der ILM-Regel platziert werden oder der Ingest fehlschlägt. Bei einem S3-Multipart-Upload wird ILM jedoch für jeden Teil des Objekts während des Ingests und für das gesamte Objekt nach Abschluss des Multipart-Uploads ausgewertet. In den folgenden Fällen kann dies zu Platzierungen führen, die von den Erwartungen abweichen:
  - **Ändert sich ILM während eines laufenden S3-Multipart-Uploads**: Da jeder Teil gemäß der zum Zeitpunkt der Aufnahme aktiven Regel platziert wird, erfüllen einige Teile des Objekts nach Abschluss des Multipart-Uploads möglicherweise nicht die aktuellen ILM-Anforderungen. In diesen Fällen schlägt die Aufnahme des Objekts nicht fehl. Stattdessen wird jeder nicht korrekt platzierte Teil zur erneuten ILM-Bewertung in die Warteschlange gestellt und später an den korrekten Speicherort verschoben.
  - **Wenn ILM-Regeln nach Größe filtern**: Bei der Auswertung der ILM für einen Teil filtert StorageGRID nach der Größe des Teils, nicht nach der Größe des Objekts. Das bedeutet, dass Teile eines Objekts an Orten gespeichert werden können, die die ILM-Anforderungen für das Objekt als Ganzes nicht erfüllen. Wenn beispielsweise eine Regel festlegt, dass alle Objekte mit 10 GB oder mehr in DC1 gespeichert werden, während alle kleineren Objekte in DC2 gespeichert werden, wird beim Hochladen jedes 1-GB-Teil eines 10-teiligen Multipart-Uploads in DC2 gespeichert. Wenn ILM für das Objekt ausgewertet wird, werden alle Teile des Objekts nach DC1 verschoben.
- **(Streng) Das Ingest schlägt nicht fehl, wenn Objekt-Tags oder Metadaten aktualisiert werden und neu erforderliche Platzierungen nicht vorgenommen werden können**: Mit Strict wird erwartet, dass Objekte entweder wie in der ILM-Regel beschrieben platziert werden oder das Ingest fehlschlägt. Wenn jedoch Metadaten oder Tags für ein bereits im Grid gespeichertes Objekt aktualisiert werden, wird das Objekt nicht erneut ingestiert. Das bedeutet, dass Änderungen an der Objektplatzierung, die durch die Aktualisierung ausgelöst werden, nicht sofort vorgenommen werden. Platzierungsänderungen erfolgen, wenn ILM durch normale Hintergrund-ILM-Prozesse neu ausgewertet wird. Wenn erforderliche Platzierungsänderungen nicht vorgenommen werden können (zum Beispiel, 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 Storage Pool am Tag 0.
- Platzierungen in einem Cloud Storage Pool, wenn die Regel eine benutzerdefinierte Erstellungszeit als Referenzzeit hat.

Diese Einschränkungen bestehen, weil StorageGRID keine synchronen Kopien in einen Cloud Storage Pool erstellen kann und eine vom Benutzer definierte Erstellungszeit auf die Gegenwart aufgelöst werden könnte.

Wie ILM-Regeln und Konsistenz zusammenwirken und den Datenschutz beeinflussen

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

Das für eine ILM-Regel ausgewählte Aufnahmeverhalten beeinflusst beispielsweise die anfängliche Platzierung von Objektkopien, während die beim Speichern eines Objekts verwendete Konsistenz die anfängliche Platzierung der Objektmetadaten bestimmt. Da StorageGRID sowohl auf die Daten als auch auf die Metadaten eines Objekts zugreifen muss, um Clientanfragen zu erfüllen, kann die Auswahl übereinstimmender Schutzstufen für Konsistenz und Aufnahmeverhalten einen besseren anfänglichen Datenschutz und vorhersehbarere Systemreaktionen bieten.

Hier ist eine kurze Zusammenfassung der in StorageGRID verfügbaren Konsistenzwerte:

- **Alle**: Alle Knoten erhalten die Objektmetadaten sofort oder die Anfrage schlägt fehl.
- **Stark-global**: Gewährleistet Lese-nach-Schreib-Konsistenz für alle Clientanfragen an allen Standorten. Bei konfigurierter Quorum-Semantik gelten folgende Verhaltensweisen:
  - Ermöglicht die Standortausfalltoleranz für Clientanfragen bei Grids mit drei oder mehr Standorten. Grids mit nur zwei Standorten bieten keine Standortausfalltoleranz.
  - Die folgenden S3-Operationen sind bei einem Standortausfall nicht erfolgreich:
    - DeleteBucketEncryption
    - PutBucketBranch
    - PutBucketEncryption
    - PutBucketVersioning
    - PutObjectLegalHold
    - PutObjectLockConfiguration
    - PutObjectRetention

  Falls erforderlich kann "StorageGRID Quorumsemantik für starke globale Konsistenz konfigurieren" verwendet werden.
- **Strong-site**: Objektmetadaten werden sofort an andere Knoten am Standort verteilt. Garantiert Lese-nach-Schreib-Konsistenz für alle Clientanfragen innerhalb eines Standorts.
- **Read-after-new-write**: Gewährleistet Lesekonsistenz nach dem Schreiben für neue Objekte und letztendliche Konsistenz für Objektaktualisierungen. Bietet hohe Verfügbarkeit und Garantien für den

Datenschutz. Empfohlen für die meisten Fälle.

- **Verfügbar**: Gewährleistet letztendliche Konsistenz sowohl für neue Objekte als auch für Objektaktualisierungen. Für S3-Buckets nur bei Bedarf verwenden (zum Beispiel für einen Bucket, der Log-Werte enthält, die selten gelesen werden, oder für HEAD- oder GET-Operationen auf Schlüsseln, die nicht existieren). Nicht unterstützt für S3 FabricPool Buckets.

> Bevor Sie einen Konsistenzwert auswählen, "die vollständige Beschreibung der Konsistenz". Es ist wichtig, die Vorteile und Einschränkungen zu verstehen, bevor der Standardwert geändert wird.

Beispiel dafür, wie Konsistenz- und ILM-Regeln miteinander interagieren können

Angenommen, Sie verfügen über ein Drei-Standort-Grid mit der folgenden ILM-Regel und der folgenden Konsistenz:

- **ILM-Regel**: Drei Objektkopien werden erstellt, eine am lokalen Standort und je eine an jedem Remote-Standort. Das strikte Aufnahmeverhalten wird verwendet.
- **Konsistenz**: Stark-global (Objektmetadaten werden sofort an mehrere Standorte verteilt).

Wenn ein Client ein Objekt im Grid speichert, erstellt StorageGRID alle drei Objektkopien und verteilt Metadaten an mehrere Standorte, bevor dem Client eine Erfolgsmeldung zurückgegeben wird.

Das Objekt ist zum Zeitpunkt der erfolgreichen Datenerfassung vollständig vor Verlust geschützt. Wenn beispielsweise der lokale Standort kurz nach der Datenerfassung ausfällt, sind Kopien sowohl der Objektdaten als auch der Objektmetadaten weiterhin an den Remote-Standorten vorhanden. Das Objekt ist von den anderen Standorten vollständig abrufbar.

Wenn stattdessen dieselbe ILM-Regel und die starke Standortkonsistenz verwendet werden, kann der Client eine Erfolgsmeldung erhalten, nachdem die Objektdaten auf die Remote-Standorte repliziert wurden, aber bevor die Objektmetadaten dort verteilt sind. In diesem Fall entspricht der Schutzgrad der Objektmetadaten nicht dem Schutzgrad der Objektdaten. Geht der lokale Standort kurz nach der Aufnahme verloren, 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, falls Sie Unterstützung benötigen.

Verwandte Informationen

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

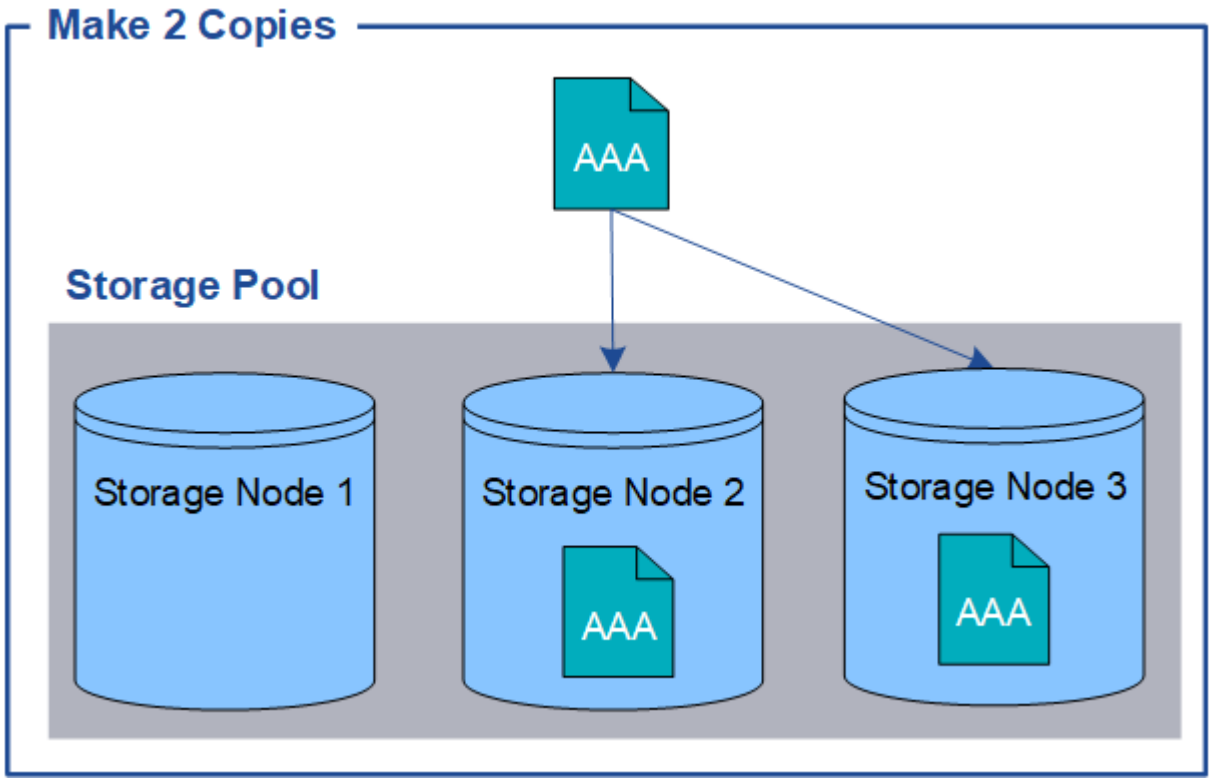
Wie Objekte gespeichert werden (Replikation oder Erasure Coding)

Erfahren Sie mehr über die Replikation in StorageGRID

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

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

Im folgenden Beispiel legt die ILM-Regel fest, dass zwei replizierte Kopien jedes Objekts in einem Speicherpool mit drei Storage Nodes abgelegt werden.



Wenn StorageGRID Objekte dieser Regel zuordnet, erstellt es zwei Kopien des Objekts und platziert jede Kopie auf einem anderen Storage Node im Speicherpool. Die beiden Kopien können auf zwei beliebigen der drei verfügbaren Storage Nodes platziert werden. In diesem Fall hat die Regel die Objektkopien auf Storage Node 2 und 3 platziert. Da zwei Kopien vorhanden sind, kann das Objekt wiederhergestellt werden, falls einer der Nodes im Speicherpool ausfällt.

> StorageGRID kann auf jedem Storage Node nur eine replizierte Kopie eines Objekts speichern. Wenn Ihr Grid drei Storage Nodes umfasst und eine ILM-Regel für vier Kopien erstellt wird, werden nur drei Kopien erstellt, jeweils eine pro Storage Node. Die Warnung **ILM placement unachievable** wird ausgelöst, um anzuzeigen, dass die ILM-Regel nicht vollständig angewendet werden konnte.

Verwandte Informationen

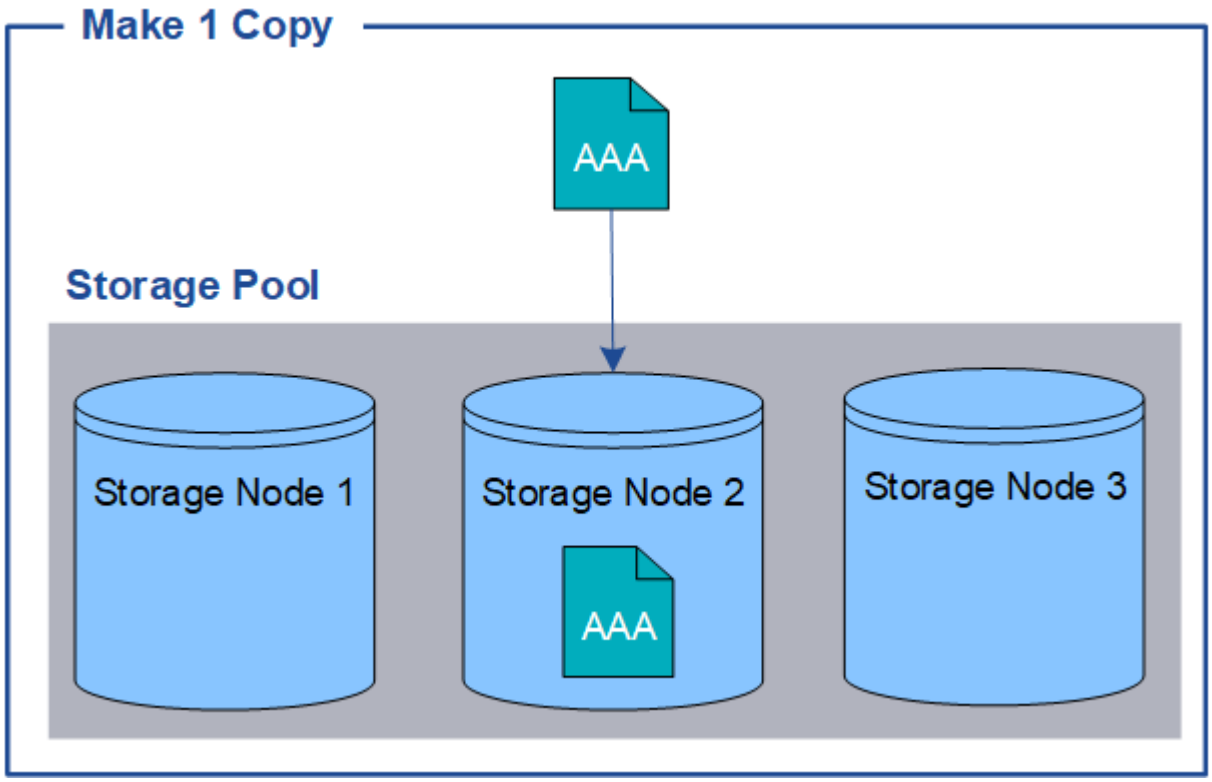
- "Was ist Erasure Coding"
- "Was ist ein Storage-Pool"
- "Schutz vor Standortverlust durch Replikation und Erasure Coding ermöglichen"

Risiken der Einzelkopie-Replikation in StorageGRID

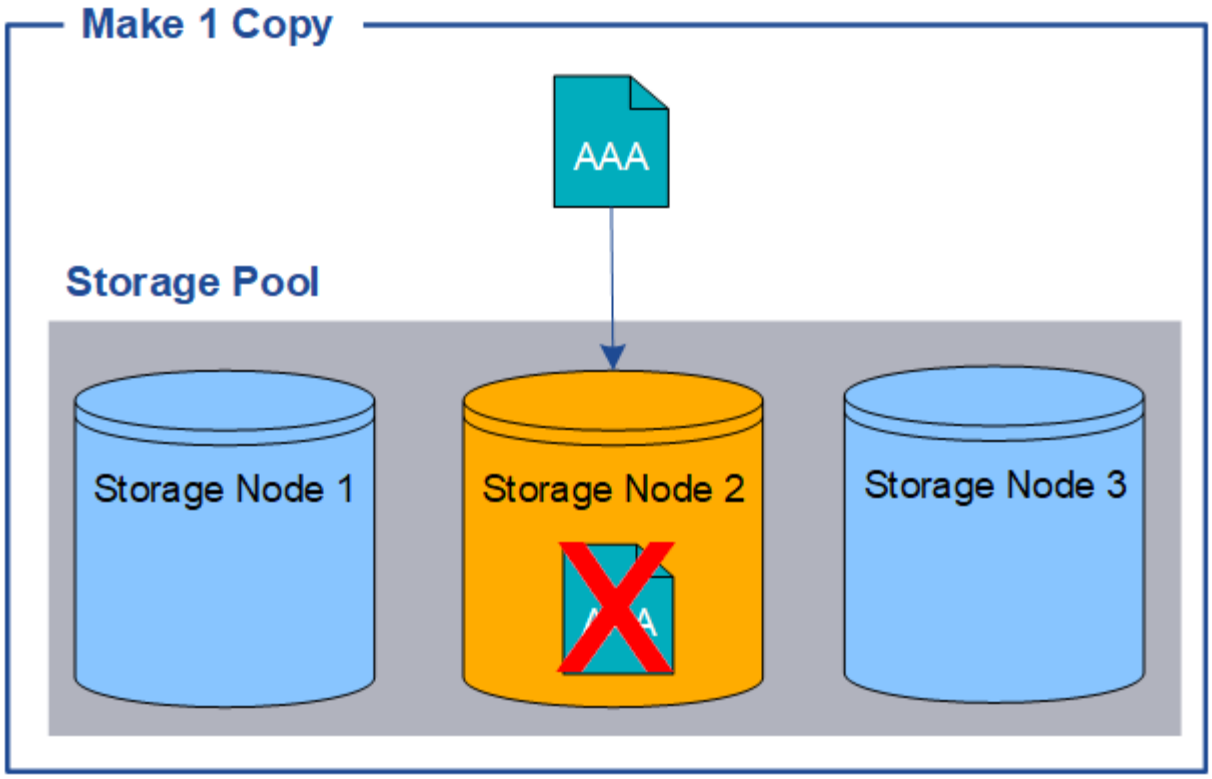
Wenn eine ILM-Regel zum Erstellen replizierter Kopien erstellt wird, sollten in den Platzierungsanweisungen immer mindestens zwei Kopien für jeden Zeitraum angegeben werden.

Es sollte keine ILM-Regel verwendet werden, die nur eine replizierte Kopie für einen bestimmten Zeitraum erstellt. Existiert nur eine replizierte Kopie eines Objekts, geht dieses Objekt verloren, wenn ein Storage Node ausfällt oder einen schwerwiegenden Fehler aufweist. Auch während Wartungsarbeiten wie Upgrades ist der Zugriff auf das Objekt vorübergehend nicht möglich.

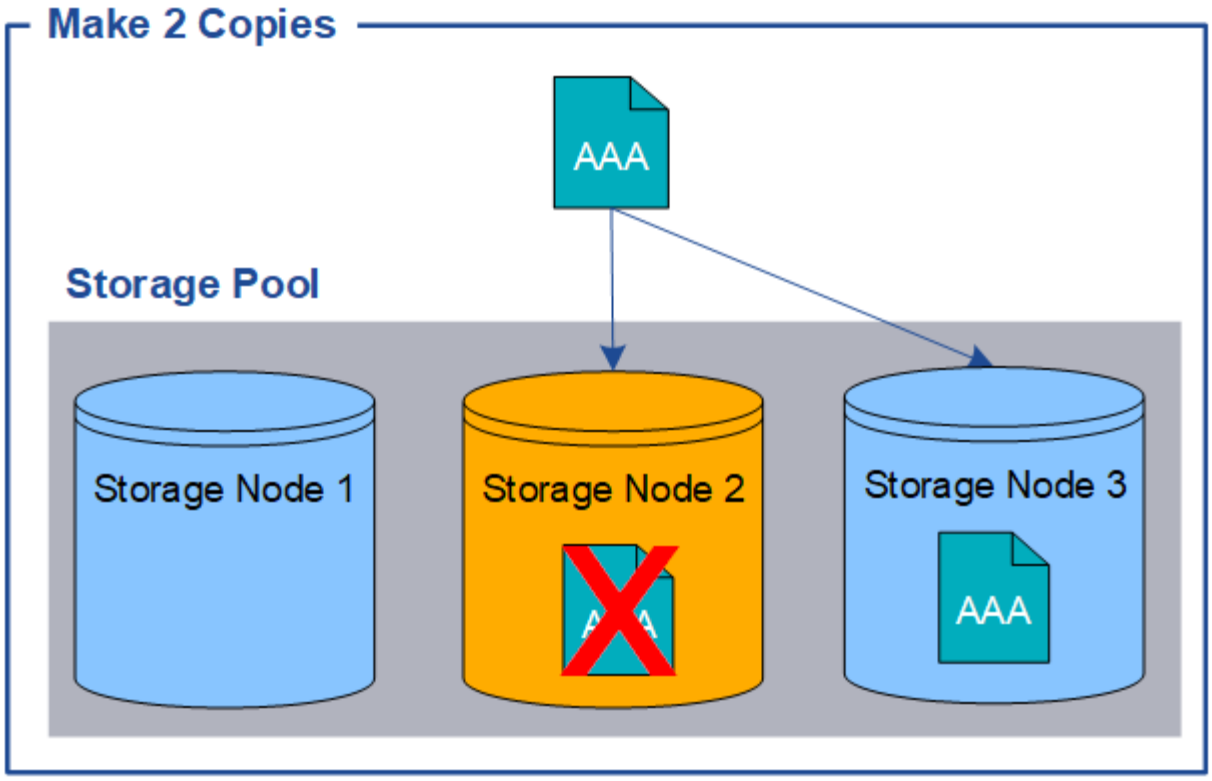
Im folgenden Beispiel legt die ILM-Regel „1 Kopie erstellen“ fest, dass eine replizierte Kopie eines Objekts in einem Speicherpool mit drei Storage Nodes abgelegt wird. Wenn ein Objekt, das dieser Regel entspricht, aufgenommen wird, platziert StorageGRID eine einzelne Kopie auf genau einem Storage Node.



Wenn eine ILM-Regel nur eine replizierte Kopie eines Objekts erstellt, ist das Objekt nicht mehr zugänglich, sobald der Storage Node nicht verfügbar ist. In diesem Beispiel geht der Zugriff auf das Objekt AAA vorübergehend verloren, wenn Storage Node 2 offline ist, beispielsweise während eines Upgrades oder einer anderen Wartungsmaßnahme. Das Objekt AAA geht vollständig verloren, wenn Storage Node 2 ausfällt.



Um Datenverlust zu vermeiden, sollten stets mindestens zwei Kopien aller Objekte erstellt werden, die durch Replikation geschützt werden sollen. Sind zwei oder mehr Kopien vorhanden, ist weiterhin Zugriff auf das Objekt möglich, falls ein Storage Node ausfällt oder offline geht.



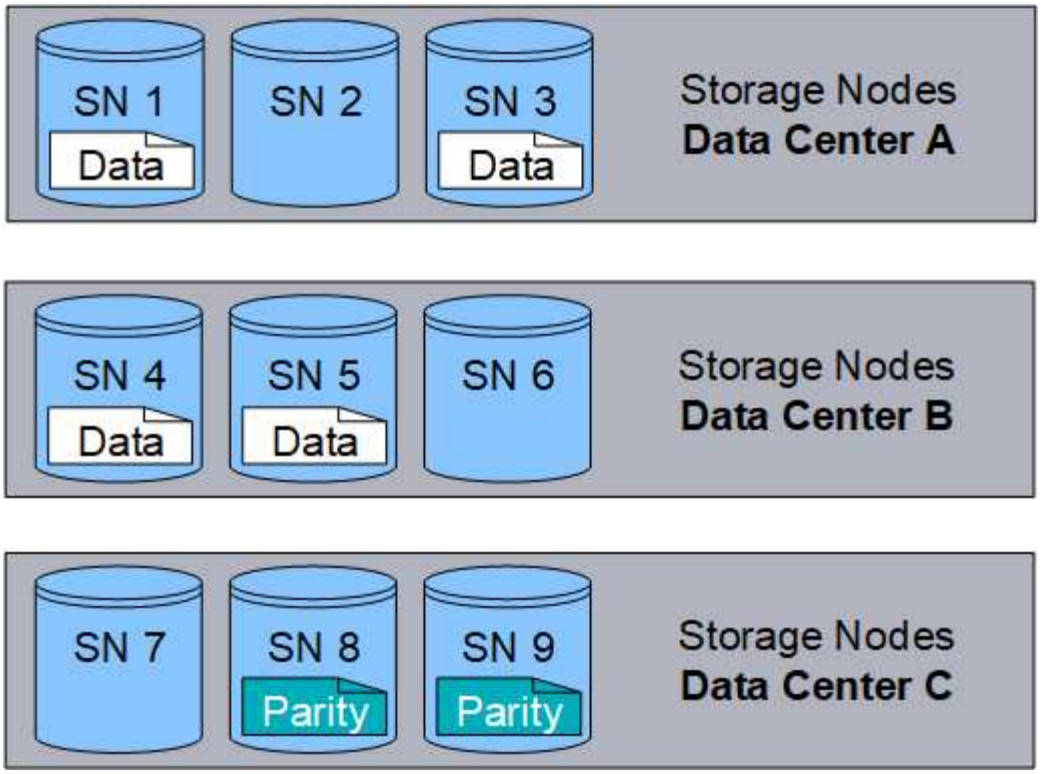
Erfahren Sie mehr über Erasure Coding in StorageGRID

Erasure Coding ist eine von zwei Methoden, die StorageGRID zur Speicherung von Objektdaten verwendet (die andere Methode ist die Replikation). Wenn Objekte einer ILM-Regel entsprechen, die Erasure Coding verwendet, werden diese Objekte in Datenfragmente zerlegt, zusätzliche Paritätsfragmente berechnet und jedes Fragment auf einem anderen Storage Node gespeichert.

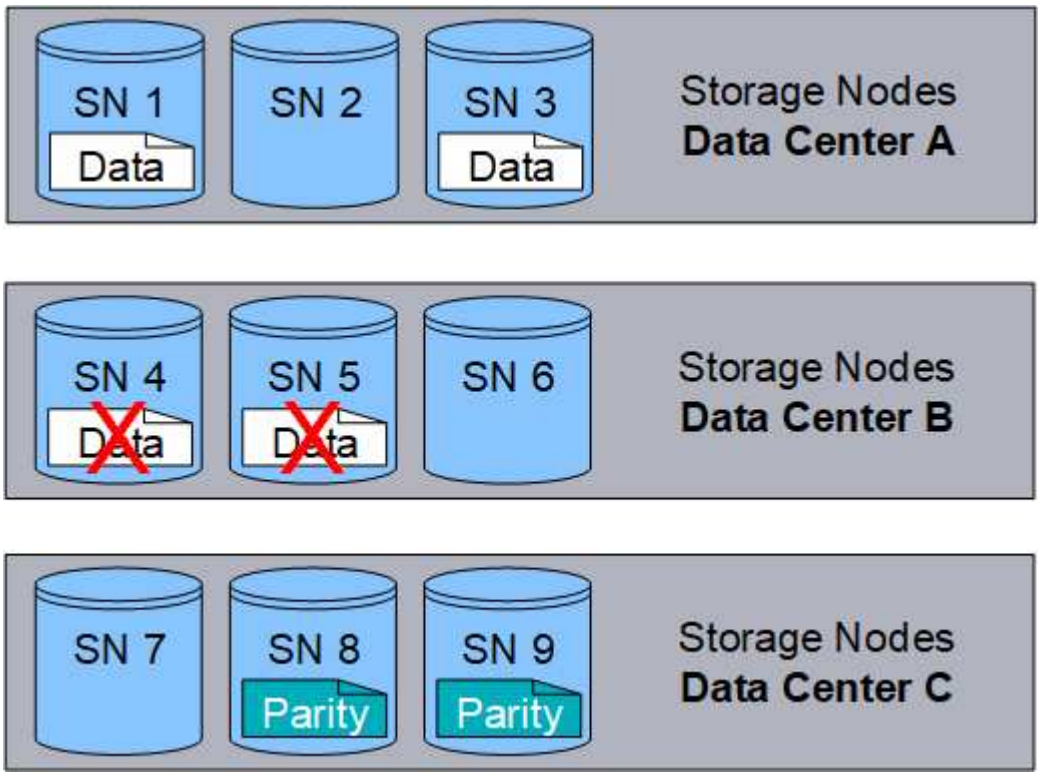
Beim Zugriff auf ein Objekt wird dieses mithilfe der gespeicherten Fragmente wiederhergestellt. Wenn ein Daten- oder Paritätsfragment beschädigt oder verloren geht, kann der Erasure-Coding-Algorithmus dieses Fragment mithilfe einer Teilmenge der verbleibenden Daten- und Paritätsfragmente wiederherstellen.

Beim Erstellen von ILM-Regeln erstellt StorageGRID Erasure-Coding-Profile, die diese Regeln unterstützen. Eine Liste der Erasure-Coding-Profile kann angezeigt, "ein Erasure-Coding-Profil umbenennen" oder "Ein Erasure-Coding-Profil kann deaktiviert werden, wenn es derzeit in keiner ILM-Regel verwendet wird." werden.

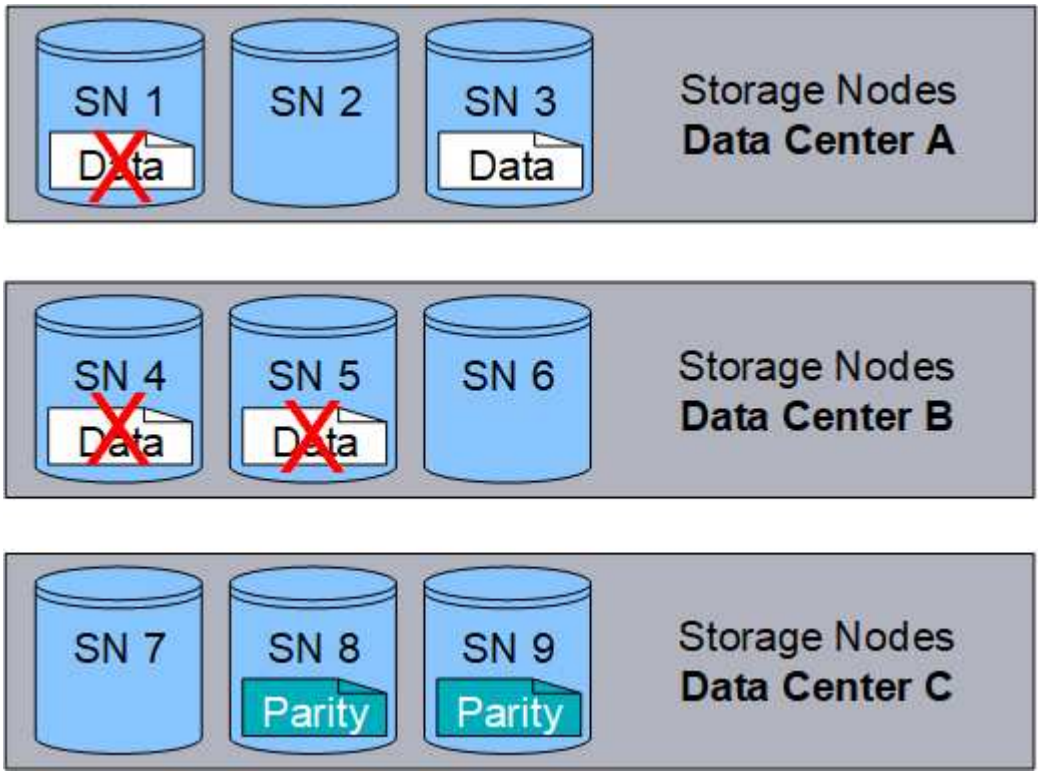
Das folgende Beispiel veranschaulicht die Anwendung eines Erasure-Coding Algorithmus auf die Daten eines Objekts. In diesem Beispiel verwendet die ILM-Regel ein 4+2 Erasure-Coding-Schema. Jedes Objekt wird in vier gleich große Datenfragmente aufgeteilt, und aus den Objektdaten werden zwei Paritätsfragmente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



Das 4+2-Erasure-Coding-Verfahren kann auf verschiedene Weise konfiguriert werden. Zum Beispiel kann ein Speicherpool mit einem einzelnen Standort eingerichtet werden, der sechs Storage Nodes enthält. Für "Standortverlustschutz" kann ein Speicherpool mit drei Standorten verwendet werden, wobei sich an jedem Standort drei Storage Nodes befinden. Ein Objekt kann abgerufen werden, solange vier der sechs Fragmente (Daten oder Parität) verfügbar sind. Bis zu zwei Fragmente können verloren gehen, ohne dass die Objektdaten verloren gehen. Wenn ein gesamter Standort ausfällt, kann das Objekt weiterhin abgerufen oder repariert werden, solange alle anderen Fragmente zugänglich bleiben.



Wenn mehr als zwei Storage Nodes verloren gehen, ist das Objekt nicht abrufbar.



Verwandte Informationen

- "Was ist Replikation"
- "Was ist ein Storage-Pool"
- "Was sind Löschcodierungsverfahren"
- "Ein Erasure-Coding-Profil umbenennen"
- "Ein Erasure-Coding-Profil deaktivieren"

Erfahren Sie mehr über Erasure-Coding-Schemata in StorageGRID

Erasure-Coding-Verfahren steuern, wie viele Datenfragmente und wie viele Paritätsfragmente für jedes Objekt erzeugt werden.

Beim Erstellen oder Bearbeiten einer ILM-Regel wird ein verfügbares Erasure-Codierungsschema ausgewählt. StorageGRID erstellt automatisch Erasure-Codierungsschemata basierend darauf, wie viele Storage Nodes und Standorte den Speicherpool bilden, den Sie verwenden möchten.

Datenschutz

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

Die `k + m = n`Fragmente werden auf `n`Storage Nodes verteilt, um den Datenschutz wie folgt zu gewährleisten:

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

höher ist die Fehlertoleranz.

Den besten Datenschutz bietet das Erasure-Codierungsverfahren mit der höchsten Fehlertoleranz gegenüber Knoten oder Volumes innerhalb eines Speicherpools.

Storage-Overhead

Der Speicherbedarf eines Erasure-Coding-Verfahrens wird berechnet, indem die Anzahl der Paritätsfragmente (`m` durch die Anzahl der Datenfragmente (`k` geteilt wird. Mit dem Speicherbedarf lässt sich berechnen, wie viel Speicherplatz jedes Erasure-Coding-Objekt benötigt:

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

Wenn Sie beispielsweise ein 10 MB großes Objekt im 4+2-Schema speichern (das einen Storage-Overhead von 50 % aufweist), belegt das Objekt 15 MB Grid-Storage. Wenn Sie dasselbe 10 MB große Objekt im 6+2-Schema speichern (das einen Storage-Overhead von 33 % aufweist), belegt es etwa 13,3 MB.

Wählen Sie das Löschcodierungsverfahren mit dem niedrigsten Gesamtwert von `k+m`, das Ihren Anforderungen entspricht. Löschcodierungsverfahren mit einer geringeren Anzahl von Fragmenten sind recheneffizienter, weil:

- Es werden weniger Fragmente pro Objekt erzeugt und verteilt (oder abgerufen)
- Sie zeigen eine bessere Leistung, weil die Fragmentgröße größer ist
- Sie können weniger Knoten in einem "Erweiterung, wenn mehr Speicherplatz benötigt wird" hinzufügen müssen

Richtlinien für Storage Pools

Bei der Auswahl des Speicherpools für eine Regel, die eine mit Erasure Coding erstellte Kopie erzeugt, gelten die folgenden Richtlinien für Speicherpools:

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

  > Erasure Coding kann nicht verwendet werden, wenn der Speicherpool zwei Standorte umfasst.

  - Löschcodierungsverfahren für Speicherpools mit drei oder mehr Standorten
  - Löschcodierungsverfahren für Speicherpools an einem Standort
- Keinen Speicherpool verwenden, der den Standort „All Sites“ enthält.
- Der Speicherpool sollte mindestens *k+m* `+1` Storage Nodes enthalten, die Objektdaten speichern können.

  > Speicherknoten können während der Installation so konfiguriert werden, dass sie Objektdaten und Metadaten („kombinierter“ Speicherknoten), nur Objektmetadaten oder nur Objektdaten enthalten. Weitere Informationen sind unter "Arten von Speicherknoten" zu finden.

  Die Mindestanzahl der erforderlichen Storage Nodes beträgt `k+m`. Allerdings kann mindestens ein zusätzlicher Storage Node dazu beitragen, Ingest-Fehler oder ILM-Rückstände zu vermeiden, falls ein erforderlicher Storage Node vorübergehend nicht verfügbar ist.

Löschcodierungsverfahren für Speicherpools mit drei oder mehr Standorten

Die folgende Tabelle beschreibt die von StorageGRID derzeit unterstützten Erasure-Coding-Verfahren für Speicherpools, die drei oder mehr Standorte umfassen. Alle diese Verfahren bieten Schutz vor Standortverlust. Ein Standort kann ausfallen, und das Objekt bleibt weiterhin zugänglich.

Bei Erasure-Codierungsverfahren, die einen Schutz vor Standortverlust bieten, ist die empfohlene Anzahl von Storage Nodes im Speicherpool größer `k+m +1`, da jeder Standort mindestens drei Storage Nodes benötigt.

Erasure-Coding-Schema (*k+m*)	Mindestanzahl der eingesetzten Standorte	Empfohlene Anzahl von Storage Nodes an jedem Standort	Empfohlene Gesamtzahl der Storage Nodes	Schutz vor Standortverlust?	Storage-Overhead
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 benötigt mindestens drei Storage-Nodes pro Standort. Für das 7+5-Schema sind mindestens vier Storage-Nodes pro Standort erforderlich. Die Verwendung von fünf Storage-Nodes pro Standort wird empfohlen.

Bei der Auswahl eines Löschcodierungsverfahrens, das den Schutz von Standorten bietet, ist die relative Bedeutung der folgenden Faktoren abzuwägen:

- **Anzahl der Fragmente**: Leistung und Erweiterungsflexibilität sind im Allgemeinen besser, wenn die Gesamtzahl der Fragmente geringer ist.
- **Fehlertoleranz**: Die Fehlertoleranz wird durch eine höhere Anzahl an Paritätssegmenten erhöht (das heißt, wenn `m` einen höheren Wert hat.)
- **Netzwerkverkehr**: Bei der Wiederherstellung nach Ausfällen führt die Verwendung eines Schemas mit mehr Fragmenten (d. h. einer höheren Gesamtzahl für `k+m`) zu mehr Netzwerkverkehr.
- **Speicheraufwand**: Schemata mit höherem Aufwand erfordern mehr Speicherplatz pro Objekt.

Bei der Entscheidung zwischen einem 4+2 Schema und einem 6+3 Schema (beide mit 50 % Speicher-

Overhead) sollte das 6+3 Schema gewählt werden, wenn zusätzliche Fehlertoleranz erforderlich ist. Das 4+2 Schema ist zu wählen, wenn Netzwerkressourcen eingeschränkt sind. Wenn alle anderen Faktoren gleich sind, ist das 4+2 Schema vorzuziehen, da es eine geringere Gesamtanzahl an Fragmenten aufweist.

Wenn nicht klar ist, welches Schema verwendet werden soll, empfiehlt sich die Auswahl von 4+2 oder 6+3 oder die Kontaktaufnahme mit dem technischen Support.

Löschcodierungsverfahren für Speicherpools an einem Standort

Ein Speicherpool an einem einzigen Standort unterstützt alle für drei oder mehr Standorte definierten Erasure-Codierungsverfahren, vorausgesetzt, der Standort verfügt über genügend Storage Nodes.

Die Mindestanzahl an Storage Nodes beträgt `k+m`, aber ein Storage-Pool mit `k+m +1` Storage Nodes wird empfohlen. Zum Beispiel erfordert das 2+1 Erasure-Coding-Schema einen Storage-Pool mit mindestens drei Storage Nodes, aber vier Storage Nodes werden empfohlen.

Erasure-Coding-Schema (*k+m*)	Mindestanzahl an Speicherknoten	Empfohlene Anzahl von Storage Nodes	Storage-Overhead
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 Anforderungen für Erasure Coding in StorageGRID

Bevor Sie sich entscheiden, ob Sie Replikation oder Erasure Coding zum Schutz von Objektdaten vor Datenverlust verwenden, sollten Sie die Vorteile, Nachteile und die Anforderungen für Erasure Coding kennen.

Vorteile der Erasure-Codierung

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

- **Zuverlässigkeit**: Gemessen an der Anzahl gleichzeitiger Ausfälle, die kontinuierlich ohne Datenverlust

verkraftet werden können.

  - Replikation: Mehrere identische Objektkopien werden auf verschiedenen Knoten und über Standorte hinweg gespeichert.
  - Erasure Coding: Ein Objekt wird in Daten- und Paritätsfragmente codiert und über viele Knoten und Standorte verteilt. Diese Verteilung bietet sowohl Schutz vor Standort- als auch vor Knotenausfällen.

- **Verfügbarkeit**: Die Fähigkeit, Objekte abzurufen, falls Storage Nodes ausfallen oder nicht mehr erreichbar sind. Im Vergleich zur Replikation bietet Erasure Coding eine höhere Verfügbarkeit bei vergleichbaren Speicherkosten.
- **Speichereffizienz**: Bei vergleichbarer Verfügbarkeit und Zuverlässigkeit benötigen mit Erasure Coding gesicherte Objekte weniger Speicherplatz als replizierte Objekte. Beispielsweise belegt ein 10 MB großes Objekt, das auf zwei Standorte repliziert wird, 20 MB Speicherplatz (zwei Kopien), während ein Objekt, das mit einem 6+3 Erasure-Coding-Schema über drei Standorte gesichert wird, nur 15 MB Speicherplatz benötigt.

> ⓘ Der Speicherplatz für erasure-codierte Objekte wird als Objektgröße zuzüglich des Speicher-Overheads berechnet. Der prozentuale Speicher-Overhead entspricht der Anzahl der Paritätsfragmente geteilt durch die Anzahl der Datenfragmente.

Nachteile der Löschcodierung

Im Vergleich zur Replikation weist das Erasure Coding folgende Nachteile auf:

- Je nach Erasure-Coding-Schema wird eine erhöhte Anzahl von Storage Nodes und Standorten empfohlen. Im Gegensatz dazu wird bei der Replikation von Objektdaten nur ein Storage Node pro Kopie benötigt. Siehe "Löschcodierungsverfahren für Speicherpools mit drei oder mehr Standorten" und "Löschcodierungsverfahren für Speicherpools an einem Standort".
- Erhöhte Kosten und Komplexität bei Speichererweiterungen. Um eine Bereitstellung mit Replikation zu erweitern, wird an jedem Standort, an dem Objektkopien erstellt werden, zusätzliche Speicherkapazität hinzugefügt. Bei der Erweiterung einer Bereitstellung mit Erasure Coding sind sowohl das verwendete Erasure-Coding-Verfahren als auch der Füllstand der vorhandenen Storage Nodes zu berücksichtigen. Wenn beispielsweise gewartet wird, bis die vorhandenen Knoten zu 100 % ausgelastet sind, müssen mindestens `k+m` Storage Nodes hinzugefügt werden, während bei einer Erweiterung, wenn die vorhandenen Knoten zu 70 % ausgelastet sind, zwei Knoten pro Standort hinzugefügt werden können und dennoch die nutzbare Speicherkapazität maximiert wird. Weitere Informationen finden sich unter "Speicherkapazität für mit Löschkodierung versehene Objekte hinzufügen".
- Bei der Verwendung von Erasure Coding über geografisch verteilte Standorte hinweg kommt es zu erhöhten Abruflatenzen. Die Objektfragmente eines mit Erasure Coding codierten und über entfernte Standorte verteilten Objekts benötigen über WAN-Verbindungen länger für den Abruf als ein Objekt, das repliziert und lokal verfügbar ist (am selben Standort, mit dem der Client verbunden ist).
- Bei der Verwendung von Erasure Coding an geografisch verteilten Standorten kommt es zu einer höheren Auslastung des WAN-Netzwerks für Abrufe und Reparaturen, insbesondere bei häufig abgerufenen Objekten oder bei Objektreparaturen über WAN-Netzwerkverbindungen.
- Bei der standortübergreifenden Verwendung von Erasure Coding sinkt der maximale Objektdurchsatz mit zunehmender Netzwerklatenz zwischen den Standorten deutlich. Dieser Rückgang ist das Ergebnis einer verringerten TCP-Netzwerkbandbreite, was die Geschwindigkeit beeinflusst, mit der das StorageGRID System Objektfragmente speichern und abrufen kann.
- Höhere Auslastung der Rechenressourcen.

Wann wird Erasure Coding verwendet?

Erasure Coding wird für die folgenden Anforderungen verwendet:

- Objekte größer als 1 MB.

> Erasure Coding eignet sich am besten für Objekte größer als 1 MB. Erasure Coding sollte für Objekte kleiner als 200 KB nicht verwendet werden, um den Aufwand für die Verwaltung sehr kleiner erasure-codierter Fragmente zu vermeiden.

- Langzeit- oder Kaltlagerung für selten abgerufene Inhalte.
- Hohe Datenverfügbarkeit und Zuverlässigkeit.
- Schutz vor vollständigen Standort- und Knotenausfällen.
- Speichereffizienz.
- Einzelstandort-Implementierungen, die 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.

Wie StorageGRID die Objektaufbewahrung bestimmt

StorageGRID bietet sowohl Grid-Administratoren als auch einzelnen Mandantenbenutzern Optionen zur Festlegung der Speicherdauer von Objekten. Im Allgemeinen haben die vom Mandantenbenutzer festgelegten Aufbewahrungsrichtlinien Vorrang vor den vom Grid-Administrator festgelegten Aufbewahrungsrichtlinien.

Wie Mandantenbenutzer die Objektaufbewahrung steuern

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

- Wenn die globale S3 Object Lock-Einstellung für das Grid aktiviert ist, können S3-Mandantenbenutzer Buckets mit aktivierter S3 Object Lock-Funktion erstellen und dann für jeden Bucket eine **Standardaufbewahrungsdauer** auswählen.
- Wenn die globale S3 Object Lock-Einstellung für das Grid aktiviert ist, können S3-Mandantenbenutzer Buckets mit aktivierter S3 Object Lock-Funktion erstellen und anschließend die S3 REST API verwenden, um für jede Objektversion, die diesem Bucket hinzugefügt wird, die Einstellungen für retain-until-date und legal hold festzulegen.
  - Eine unter rechtlicher Sperre stehende Objektversion 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 Object Lock werden von ILM „dauerhaft“ aufbewahrt. Nach Erreichen des Aufbewahrungsdatums kann eine Objektversion jedoch durch eine Client-Anfrage oder durch das Ablaufen des Bucket-Lebenszyklus gelöscht werden. Siehe "Objekte mit S3 Object Lock verwalten".
- S3-Mandantenbenutzer können ihren Buckets eine Lebenszykluskonfiguration hinzufügen, die eine Ablaufaktion festlegt. Wenn eine Bucket-Lebenszykluskonfiguration vorhanden ist, speichert StorageGRID ein Objekt bis zu dem in der Ablaufaktion angegebenen Datum oder der angegebenen Anzahl von Tagen, es sei denn, der Client löscht das Objekt vorher. Siehe "S3 Lifecycle-Konfiguration erstellen".

- Ein S3-Client kann eine Löschanforderung für ein Objekt stellen. StorageGRID priorisiert bei der Entscheidung, ob ein Objekt gelöscht oder beibehalten wird, stets Client-Löschanforderungen gegenüber S3-Bucket-Lifecycle oder ILM.

Wie Grid-Administratoren die Objektaufbewahrung steuern

Grid-Administratoren können diese Methoden verwenden, um die Aufbewahrung von Objekten zu steuern:

- Für jeden Mandanten kann eine maximale Aufbewahrungsdauer für S3 Object Lock festgelegt werden. Anschließend können Mandantenbenutzer für jeden ihrer Buckets eine Standardaufbewahrungsdauer festlegen. Die maximale Aufbewahrungsdauer wird auch auf alle neu in diesen Bucket aufgenommenen Objekte angewendet (retain-until-date des Objekts).
- ILM-Platzierungsanweisungen erstellen, 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 werden unbegrenzt aufbewahrt, wenn für die Platzierungsanweisungen „forever“ angegeben ist.
- Unabhängig davon, wer die Aufbewahrungsdauer von Objekten kontrolliert, legen die ILM-Einstellungen fest, welche Arten von Objektkopien (repliziert oder mit Erasure-Codierung) gespeichert werden und wo sich die Kopien befinden (Storage Nodes oder Cloud Storage Pools).

Wie S3-Bucket-Lebenszyklus und ILM zusammenwirken

Wenn ein S3-Bucket-Lifecycle konfiguriert ist, überschreiben die Ablaufaktionen des Lifecycles die ILM-Richtlinie für Objekte, die dem Lifecycle-Filter entsprechen. Daher kann ein Objekt im Grid verbleiben, selbst nachdem alle ILM-Anweisungen zum Platzieren des Objekts abgelaufen sind.

Beispiele für die Objektaufbewahrung

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

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

ILM

Zwei Kopien werden für 1 Jahr (365 Tage) gespeichert.

Bucket-Lebenszyklus

Objekte laufen nach 2 Jahren (730 Tagen) ab

Ergebnis

StorageGRID speichert das Objekt für 730 Tage. StorageGRID verwendet die Bucket-Lebenszykluseinstellungen, um zu bestimmen, ob ein Objekt gelöscht oder behalten wird.

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

Beispiel 2: Der Lebenszyklus eines S3-Buckets lässt Objekte vor dem ILM ablaufen.

ILM

Zwei Kopien werden für 2 Jahre (730 Tage) aufbewahrt.

Bucket-Lebenszyklus

Objekte laufen nach 1 Jahr (365 Tagen) ab

Ergebnis

StorageGRID löscht beide Kopien des Objekts nach Tag 365.

Beispiel 3: Client-Löschung überschreibt Bucket-Lifecycle und ILM

ILM

Zwei Kopien „für immer“ auf Storage Nodes speichern

Bucket-Lebenszyklus

Objekte laufen nach 2 Jahren (730 Tagen) ab

Client-Löschanforderung

Ausgestellt am Tag 400

Ergebnis

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

Beispiel 4: S3 Object Lock überschreibt Löschanforderung des Clients

S3 Object Lock

Das Retain-until-date für eine Objektversion ist der 31.03.2026. Eine Legal Hold ist nicht aktiv.

Konforme ILM-Regel

Zwei Kopien „für immer“ auf Storage Nodes speichern

Client-Löschanforderung

Ausgestellt am 2024-03-31

Ergebnis

StorageGRID wird die Objektversion nicht löschen, da das Aufbewahrungsdatum noch 2 Jahre in der Zukunft liegt.

Wie StorageGRID Objekte löscht

StorageGRID kann Objekte entweder direkt als Reaktion auf eine Clientanfrage oder automatisch infolge des Ablaufs eines S3-Bucket-Lebenszyklus oder aufgrund der Anforderungen der ILM-Richtlinie löschen. Ein Verständnis der verschiedenen Möglichkeiten, wie Objekte gelöscht werden können, und wie StorageGRID Löschanfragen verarbeitet, kann dabei helfen, Objekte effektiver zu verwalten.

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

- Synchrones Löschen: Wenn StorageGRID eine Löschanforderung eines Clients empfängt, werden alle Objektkopien sofort entfernt. Der Client wird nach dem Entfernen der Kopien über die erfolgreiche Löschung informiert.
- Objekte werden zur Löschung in die Warteschlange gestellt: Wenn StorageGRID eine Löschanforderung erhält, wird das Objekt zur Löschung in die Warteschlange gestellt und der Client wird umgehend darüber

informiert, dass die Löschung erfolgreich war. Objektkopien werden später durch die Hintergrundverarbeitung von ILM 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 zur Durchführung der Löschung	**Bei Verwendung**
Objekte werden zur Löschung 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 festgelegte Zeitraum ist abgelaufen. **Hinweis:** Objekte in einem Bucket, für den S3 Object Lock aktiviert ist, können nicht gelöscht werden, wenn sie einer rechtlichen Aufbewahrung 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 der Speicherort eines Objekts vorübergehend nicht verfügbar ist. ◦ Die Hintergrund-Löschwarteschlangen sind im Leerlauf.
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, fügt StorageGRID zunächst Objekte zur Löschwarteschlange hinzu. Anschließend erfolgt die synchron Löschung. Wenn sichergestellt ist, dass die Hintergrund-Löschwarteschlange Objekte zur Verarbeitung enthält, kann StorageGRID Löschvorgänge effizienter verarbeiten, insbesondere für Clients mit geringer Parallelität, und gleichzeitig Rückstaus bei Client-Löschvorgängen vermeiden.

Zeitaufwand für das Löschen von Objekten

Die Art und Weise, wie StorageGRID Objekte löscht, kann Auswirkungen darauf haben, wie die Systemleistung erscheint:

- Wenn StorageGRID eine synchron Löschung durchführt, kann es bis zu 30 Sekunden dauern, bis StorageGRID ein Ergebnis an den Client zurückgibt. Das bedeutet, dass die Löschung langsamer

erscheinen kann, obwohl Kopien tatsächlich schneller entfernt werden als wenn StorageGRID Objekte zur Löschung in die Warteschlange stellt.

- Wenn Sie die Löschleistung während eines Massenlöschvorgangs genau überwachen, stellen Sie möglicherweise fest, dass die Löschrate nach dem Löschen einer bestimmten Anzahl von Objekten langsamer erscheint. Diese Änderung tritt auf, wenn StorageGRID von der Warteschlangenfunktion zur synchronen Löschung übergeht. Die scheinbare Reduzierung der Löschrate bedeutet nicht, dass Objektkopien langsamer entfernt werden. Im Gegenteil, sie zeigt an, dass im Durchschnitt nun schneller Speicherplatz freigegeben wird.

Wenn Sie eine große Anzahl von Objekten löschen und Ihre Priorität darin besteht, Speicherplatz schnell freizugeben, empfiehlt sich das Löschen der Objekte per Client-Anfrage statt über ILM oder andere Methoden. Im Allgemeinen wird Speicherplatz schneller freigegeben, wenn die Löschung durch Clients erfolgt, da StorageGRID synchrones Löschen verwenden kann.

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

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

Wie versionierte S3-Objekte gelöscht werden

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

Bei versionierten Objekten löschen Löschanforderungen nicht die aktuelle Version des Objekts und geben keinen Speicherplatz frei. Stattdessen erstellt eine Löschanforderung eine Null-Byte-Löschmarkierung als aktuelle Version des Objekts, wodurch die vorherige Version des Objekts als „nicht aktuell“ gilt. Eine Objekt-Löschmarkierung wird zu einer abgelaufenen Objekt-Löschmarkierung, wenn sie die aktuelle Version ist und keine nicht aktuellen Versionen vorhanden sind.

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

Wenn ein Client eine Objektversion mit einer Versions-ID aus einem "Branch-Bucket" Branch-Bucket löscht, blendet StorageGRID die Existenz der Objektversion aus, erstellt jedoch keinen Löschmarker im Branch-Bucket. Wenn ein Client ein Objekt ohne Versions-ID aus einem Branch-Bucket löscht, erstellt StorageGRID gemäß dem Standardverhalten von S3 einen Löschmarker im Branch-Bucket.

Um beim Löschen versionierter Objekte Speicherplatz freizugeben oder Löschmarkierungen zu entfernen, kann eine der folgenden Methoden genutzt werden:

- **S3-Clientanfrage**: Die Objektversions-ID ist in der S3 DELETE Object-Anfrage anzugeben (`DELETE /object?versionId=ID`). Dabei ist zu beachten, dass mit dieser Anfrage nur Objektkopien der angegebenen Version entfernt werden (die anderen Versionen belegen weiterhin Speicherplatz).
- **Bucket Lifecycle**: Die `NoncurrentVersionExpiration` Aktion in der Bucket Lifecycle-Konfiguration wird verwendet. Sobald die angegebene Anzahl von NoncurrentDays erreicht ist, entfernt StorageGRID

dauerhaft alle Kopien nicht aktueller Objektversionen. Diese Objektversionen können nicht wiederhergestellt werden.

Die `NewerNoncurrentVersions` Aktion in der Bucket-Lebenszykluskonfiguration legt die Anzahl der in einem versionierten S3-Bucket aufbewahrten nicht aktuellen Versionen fest. Wenn mehr nicht aktuelle Versionen vorhanden sind, als `NewerNoncurrentVersions` angibt, entfernt StorageGRID die älteren Versionen, sobald der Wert von NoncurrentDays abgelaufen ist. Der `NewerNoncurrentVersions` Schwellenwert setzt die von ILM bereitgestellten Lebenszyklusregeln außer Kraft, das bedeutet, dass ein nicht aktuelles Objekt mit einer Version innerhalb des `NewerNoncurrentVersions` Schwellenwerts aufbewahrt wird, wenn ILM dessen Löschung anfordert.

Um abgelaufene Objektlöschmarkierungen zu entfernen, wird die `Expiration` Aktion mit einem der folgenden Tags verwendet: `ExpiredObjectDeleteMarker`, `Days` oder `Date`.

- **ILM**: "Eine aktive Richtlinie klonen" und zwei ILM-Regeln zur neuen Richtlinie hinzufügen:
  - Erste Regel: Verwenden Sie „Nicht-aktuelle Zeit“ als Referenzzeit, um die nicht-aktuellen Versionen des Objekts abzugleichen. In "Schritt 1 (Details eingeben) des Assistenten zum Erstellen einer ILM-Regel" wählen Sie für die Frage „Diese Regel nur auf ältere Objektversionen anwenden (in S3-Buckets mit aktivierter Versionierung)?“ **Ja** aus.
  - Zweite Regel: **Aufnahmezeit** ist zu verwenden, um die aktuelle Version abzugleichen. Die Regel „Nicht-aktuelle Zeit“ muss in der Richtlinie oberhalb der Regel **Aufnahmezeit** erscheinen.

    Um abgelaufene Löschmarkierungen zu entfernen, wird eine **Aufnahmezeit**-Regel verwendet, die mit den aktuellen Löschmarkierungen übereinstimmt. 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**: Mit dem Tenant Manager können "Alle Objektversionen löschen"Objekte, einschließlich Löschmarkierungen, aus einem Bucket gelöscht werden.

Wenn ein versioniertes Objekt gelöscht wird, erstellt StorageGRID eine Löschmarkierung mit Nullbytes 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 durch S3-Client-Anfragen entfernt werden, sie werden nicht durch ILM, Bucket-Lifecycle-Regeln oder Löschvorgänge für Objekte im Bucket entfernt.
- Löschmarkierungen aus einem Bucket, der in StorageGRID 11.8 oder höher erstellt wurde, können durch ILM, Bucket-Lifecycle-Regeln, Löschvorgänge für Objekte im Bucket oder eine explizite Löschung durch einen S3-Client entfernt werden.

Verwandte Informationen

- "S3 REST-API verwenden"
- "Beispiel 4: ILM Regeln und Richtlinien für versionierte S3-Objekte"

Erstellen und Zuweisen von Speicherklassen in StorageGRID

Speicherklassen kennzeichnen den Speichertyp, der von einem Storage Node verwendet wird. Speicherklassen können erstellt werden, wenn ILM-Regeln bestimmte Objekte auf bestimmten Storage Nodes platzieren sollen.

Bevor Sie beginnen

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

Über diese Aufgabe

Bei der Erstinstallation von StorageGRID wird jedem Storage Node in Ihrem System automatisch die **Default** Storage Grade zugewiesen. Bei Bedarf können benutzerdefinierte Storage Grades definiert und verschiedenen Storage Nodes zugewiesen werden.

Durch die Verwendung benutzerdefinierter Speicherklassen können ILM-Speicherpools erstellt werden, die nur einen bestimmten Typ von Speicherknoten enthalten. Beispielsweise kann es gewünscht sein, dass bestimmte Objekte auf den schnellsten Speicherknoten, wie etwa StorageGRID All-Flash-Storage Appliances, gespeichert werden.

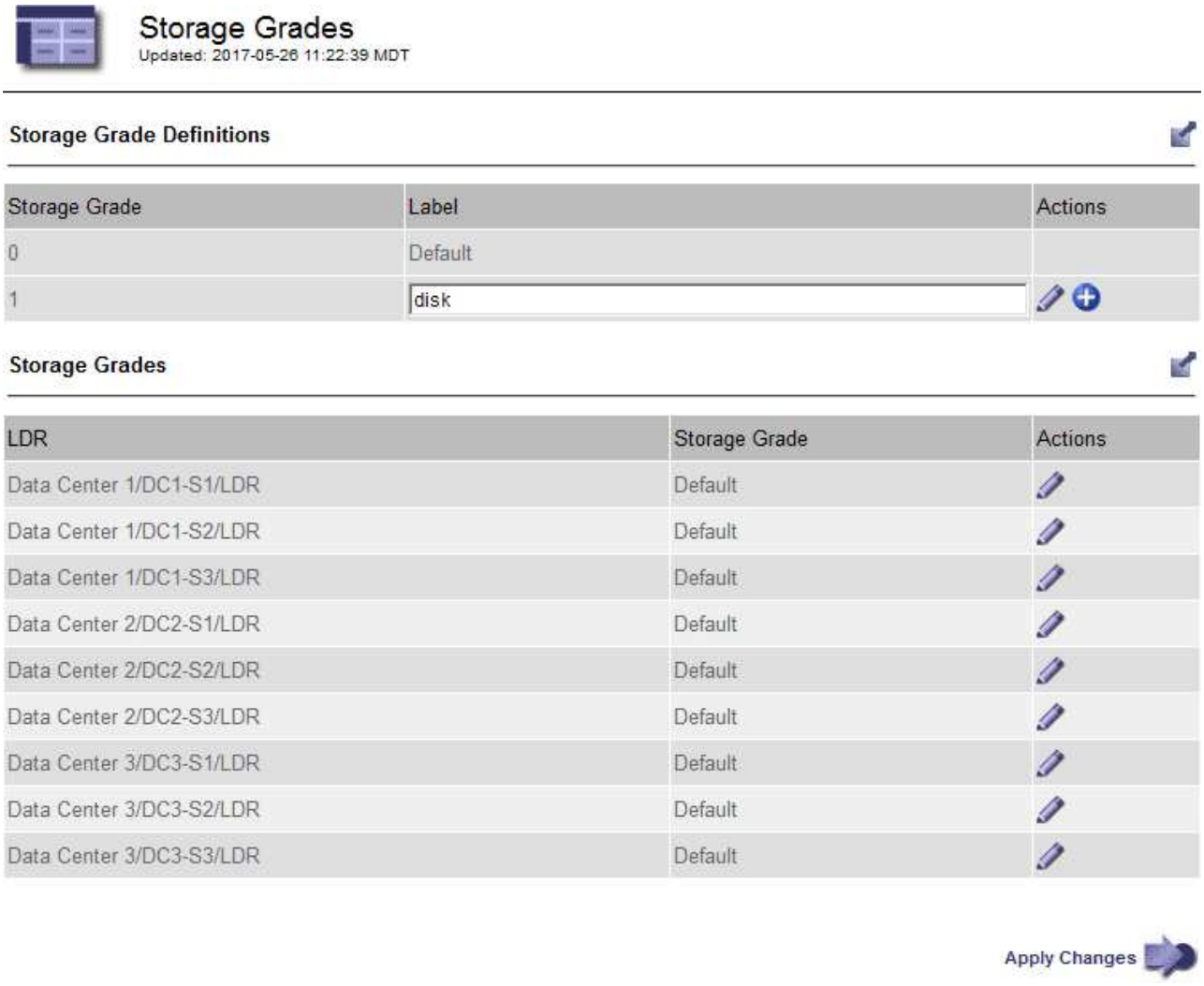
> Metadaten-only Storage Nodes können keiner Speicherklasse zugewiesen werden. Weitere Informationen finden sich unter "Arten von Speicherknoten".

Wenn die Speicherqualität keine Rolle spielt (zum Beispiel wenn alle Storage Nodes identisch sind), kann dieses Verfahren übersprungen werden und die Auswahl **includes all storage grades** für die Speicherqualität verwendet werden, wenn Sie "Speicherpools erstellen". Mit dieser Auswahl ist sichergestellt, dass der Speicherpool jeden Storage Node am Standort umfasst, unabhängig von seiner Speicherqualität.

> Erstellen Sie nicht mehr Speicherklassen als nötig. Beispielsweise sollte nicht für jeden Storage Node eine eigene Speicherklasse erstellt werden. Stattdessen empfiehlt es sich, jeder Speicherklasse zwei oder mehr Knoten zuzuweisen. Speicherklassen, die nur einem Knoten zugewiesen sind, können zu ILM-Rückständen führen, wenn dieser Knoten nicht verfügbar ist.

Schritte

1. Wählen Sie **ILM** > **Storage grades**.
2. Benutzerdefinierte Speicherklassen festlegen:
   a. Für jede benutzerdefinierte Speicherkategorie, die Sie hinzufügen möchten, **Einfügen** auswählen, um eine Zeile hinzuzufügen.
   b. Geben Sie eine beschreibende Bezeichnung ein.



c. **Änderungen anwenden** auswählen.

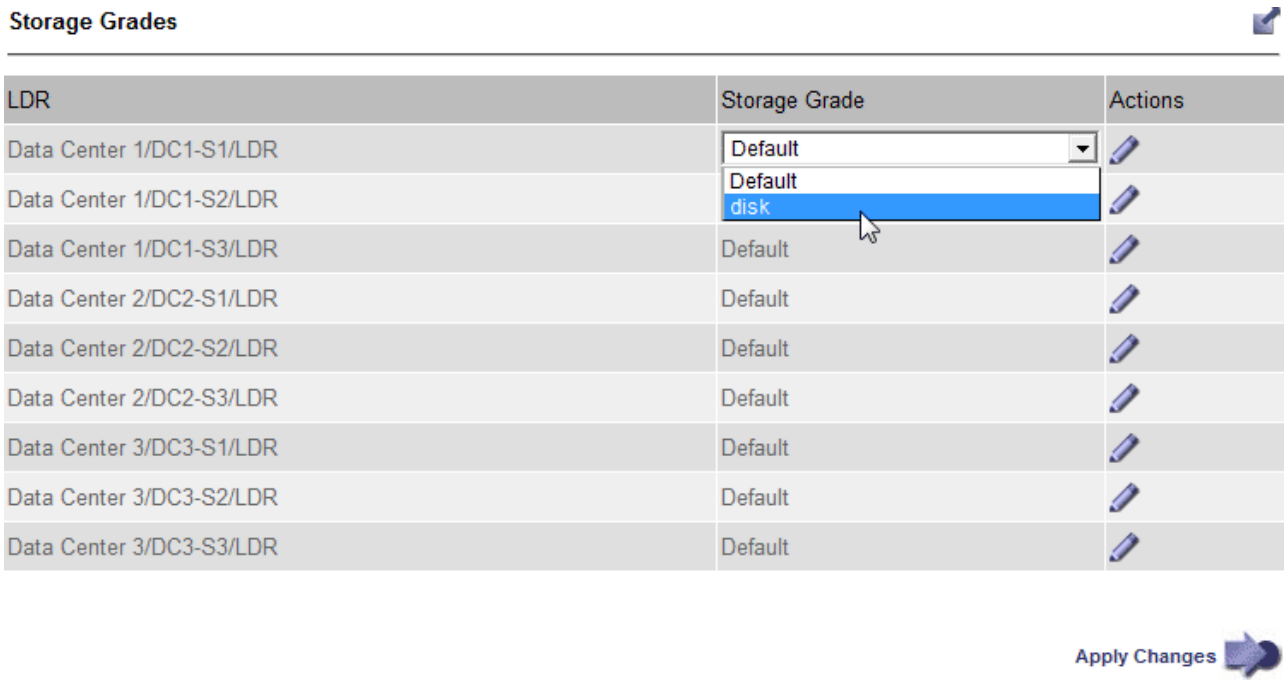
d. Optional: Falls eine gespeicherte Bezeichnung geändert werden muss, **Bearbeiten** auswählen und **Änderungen anwenden** wählen.

Speicherstufen können nicht gelöscht werden.

3. Neuen Speicherklassen werden den Storage Nodes zugewiesen:

a. Den Speicherknoten in der LDR-Liste suchen und dessen **Bearbeiten**-Symbol auswählen.

b. Die passende Storage-Klasse aus der Liste auswählen.



Einem Storage Node wird nur einmal eine Storage-Grade zugewiesen. Ein nach einem Ausfall wiederhergestellter Storage Node behält die zuvor zugewiesene Storage-Grade bei. Nach der Aktivierung der ILM-Richtlinie sollte diese Zuweisung nicht mehr geändert werden. Bei einer Änderung der Zuweisung erfolgt die Speicherung der Daten auf Basis der neuen Storage-Grade.

a. **Änderungen anwenden** auswählen.

Speicherpools verwenden

Erfahren Sie mehr über Speicherpools in StorageGRID

Ein Speicherpool ist eine logische Gruppierung von Storage Nodes.

Bei der Installation von StorageGRID wird automatisch ein Speicherpool pro Standort erstellt. Zusätzliche Speicherpools können je nach Speicheranforderungen konfiguriert werden.

Speicherknoten können während der Installation so konfiguriert werden, dass sie Objektdaten und Metadaten („kombinierter“ Speicherknoten), nur Objektmetadaten oder nur Objektdaten enthalten. Speicherknoten, die nur Metadaten enthalten, können nicht in Speicherpools verwendet werden. Weitere Informationen finden sich unter "Arten von Speicherknoten".

Speicherpools besitzen zwei Attribute:

- **Speicherklasse**: Für Storage Nodes die relative Leistung des zugrunde liegenden Speichers.
- **Standort**: Das Rechenzentrum, in dem die Objekte gespeichert werden.

Speicherpools werden in ILM-Regeln verwendet, um festzulegen, wo Objektdaten gespeichert werden und welcher Speichertyp verwendet wird. Bei der Konfiguration von ILM-Regeln für die Replikation wird ein oder werden mehrere Speicherpools ausgewählt.

Richtlinien zur Speicherpool-Konfiguration in StorageGRID

Speicherpools können so konfiguriert und genutzt werden, dass Datenverlust durch die Verteilung von Daten auf mehrere Standorte vermieden wird. Replizierte Kopien und Kopien mit Erasure-Codierung erfordern unterschiedliche Speicherpoolkonfigurationen.

Siehe "Beispiele für die Aktivierung des Schutzes vor Standortverlust durch Replikation und Erasure Coding".

Richtlinien für alle Storage Pools

- Die Konfigurationen der Speicherpools sollten so einfach wie möglich gehalten werden. Es sollten nicht mehr Speicherpools als nötig erstellt werden.
- Speicherpools sollten mit möglichst vielen Knoten erstellt werden. Jeder Speicherpool sollte zwei oder mehr Knoten enthalten. Ein Speicherpool mit einer unzureichenden Anzahl von Knoten kann zu ILM-Rückständen führen, wenn ein Knoten nicht verfügbar ist.
- Es sollte vermieden werden, Speicherpools zu erstellen oder zu verwenden, die sich überschneiden (einen oder mehrere gleiche Knoten enthalten). Wenn sich Speicherpools überschneiden, kann mehr als eine Kopie von Objektdaten auf demselben Knoten gespeichert werden.
- Im Allgemeinen sollte der Speicherpool All Storage Nodes (StorageGRID 11.6 und früher) oder der Standort All Sites nicht verwendet werden. Diese Elemente werden automatisch aktualisiert, um alle neuen Standorte einzuschließen, die bei einer Erweiterung hinzugefügt werden, was möglicherweise nicht das gewünschte Verhalten ist.

Richtlinien für Speicherpools, die für replizierte Kopien verwendet werden

- Für den Schutz vor Standortverlust mithilfe von "Replikation" sind ein oder mehrere standortspezifische Speicherpools im "Platzierungsanweisungen für jede ILM-Regel" anzugeben.

  Für jeden Standort wird während der Installation von StorageGRID automatisch ein Speicherpool erstellt.

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

- Wenn Sie im Rahmen einer Erweiterung einen Standort hinzufügen, erstellen Sie einen neuen Speicherpool, der nur den neuen Standort enthält. Anschließend "ILM-Regeln aktualisieren" lässt sich steuern, welche Objekte auf dem neuen Standort gespeichert werden.
- Ist die Anzahl der Kopien geringer als die Anzahl der Speicherpools, verteilt das System die Kopien, um die Festplattennutzung auf die Pools auszugleichen.
- Wenn sich die Speicherpools überschneiden (die gleichen Storage Nodes enthalten), könnten alle Kopien des Objekts nur an einem Standort gespeichert werden. Es ist sicherzustellen, dass die ausgewählten Speicherpools nicht die gleichen Storage Nodes enthalten.

Richtlinien für Speicherpools, die für löschcodierte Kopien verwendet werden

- Für den Schutz vor Standortverlusten mit "Erasure Coding" sollten Speicherpools erstellt werden, die aus mindestens drei Standorten bestehen. Wenn ein Speicherpool nur zwei Standorte umfasst, kann dieser Speicherpool nicht für Erasure Coding verwendet werden. Für einen Speicherpool mit zwei Standorten stehen keine Erasure-Coding-Verfahren zur Verfügung.
- Die Anzahl der im Storage-Pool enthaltenen Storage Nodes und Standorte bestimmt, welche "Löschcodierungsverfahren" verfügbar sind.

- Ein Speicherpool sollte nach Möglichkeit mehr Speicherknoten umfassen als die Mindestanzahl, die für das gewählte Erasure-Coding-Verfahren erforderlich ist. Bei Verwendung eines 6+3 Erasure-Coding-Verfahrens sind mindestens neun Speicherknoten erforderlich. Es wird jedoch empfohlen, pro Standort mindestens einen zusätzlichen Speicherknoten vorzusehen.
- Die Speicherknoten sollten so gleichmäßig wie möglich auf die Standorte verteilt werden. Zur Unterstützung eines 6+3-Erasure-Coding-Verfahrens empfiehlt sich die Konfiguration eines Speicherpools, der mindestens drei Speicherknoten an drei Standorten umfasst.
- Wenn Anforderungen an den Durchsatz hoch sind, wird die Verwendung eines Speicherpools, der mehrere Standorte umfasst, nicht empfohlen, wenn die Netzwerklatenz zwischen den Standorten mehr als 100 ms beträgt. Mit zunehmender Latenz verringert sich die Geschwindigkeit, mit der StorageGRID Objektfragmente erstellen, platzieren und abrufen kann, aufgrund des verringerten TCP-Netzwerkdurchsatzes deutlich.

  Die Verringerung des Durchsatzes beeinträchtigt die maximal erreichbaren Raten für die Objektaufnahme und -abfrage (wenn „Balanced“ oder „Strict“ als Aufnahmeverhalten ausgewählt sind) oder könnte zu Rückständen in der ILM-Warteschlange führen (wenn „Dual commit“ als Aufnahmeverhalten ausgewählt ist). Siehe "ILM-Regel-Ingest-Verhalten".

> Wenn Ihr Grid nur einen Standort umfasst, ist die Verwendung des Speicherpools „All Storage Nodes“ (StorageGRID 11.6 und früher) oder des Standorts „All Sites“ in einem Erasure-Coding-Profil nicht möglich. Dieses Verhalten verhindert, dass das Profil ungültig wird, wenn ein zweiter Standort hinzugefügt wird.

Schutz vor Standortverlust mit Speicherpools in StorageGRID

Wenn Ihre StorageGRID Bereitstellung mehr als einen Standort umfasst, können Replikation und Erasure Coding mit entsprechend konfigurierten Speicherpools verwendet werden, um den Schutz vor Standortverlust zu ermöglichen.

Replikation und Erasure Coding erfordern unterschiedliche Speicherpool-Konfigurationen:

- Für die Nutzung der Replikation zum Schutz vor Standortverlusten werden die standortspezifischen Speicherpools verwendet, die während der StorageGRID Installation automatisch erstellt werden. Anschließend werden ILM-Regeln mit "Platzierungsanweisungen" erstellt, die mehrere Speicherpools festlegen, sodass eine Kopie jedes Objekts an jedem Standort abgelegt wird.
- Um Erasure Coding zum Schutz vor Standortverlusten zu verwenden, "Speicherpools erstellen, die aus mehreren Standorten bestehen". Anschließend werden ILM-Regeln erstellt, die einen Speicherpool mit mehreren Standorten und einem beliebigen verfügbaren Erasure-Coding-Schema verwenden.

> Bei der Konfiguration Ihrer StorageGRID Bereitstellung zum Schutz vor Standortausfällen sind auch die Auswirkungen von "Aufnahmeoptionen" und "Konsistenz" zu berücksichtigen.

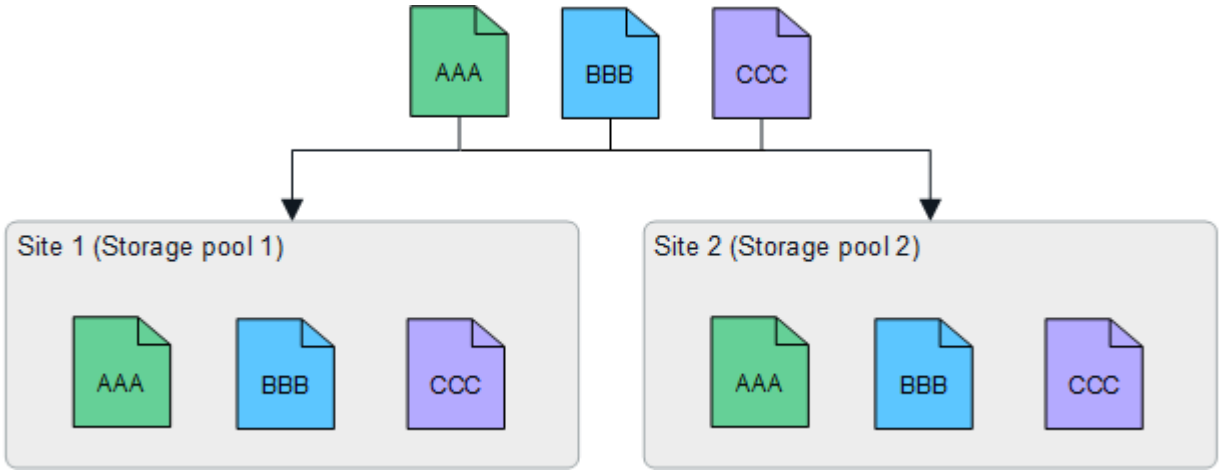
Replikationsbeispiel

Standardmäßig wird während der Installation von StorageGRID für jeden Standort ein Speicherpool erstellt. Speicherpools, die nur aus einem Standort bestehen, ermöglichen die Konfiguration von ILM-Regeln, die Replikation zum Schutz vor Standortverlust nutzen. In diesem Beispiel:

- Speicherpool 1 enthält Standort 1
- Speicherpool 2 enthält Standort 2

- Die ILM Regel enthält zwei Platzierungen:
  - Objekte durch Replizieren einer Kopie an Standort 1 speichern
  - Objekte durch Replizieren einer Kopie an Standort 2 speichern

ILM Regelplatzierungen:



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

Erasure Coding Beispiel

Durch die Verwendung von Speicherpools, die aus mehr als einem Standort pro Speicherpool bestehen, ist die Konfiguration von ILM-Regeln möglich, die Erasure Coding zum Schutz vor Standortverlusten nutzen. In diesem Beispiel:

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

ILM Regelplatzierungen:

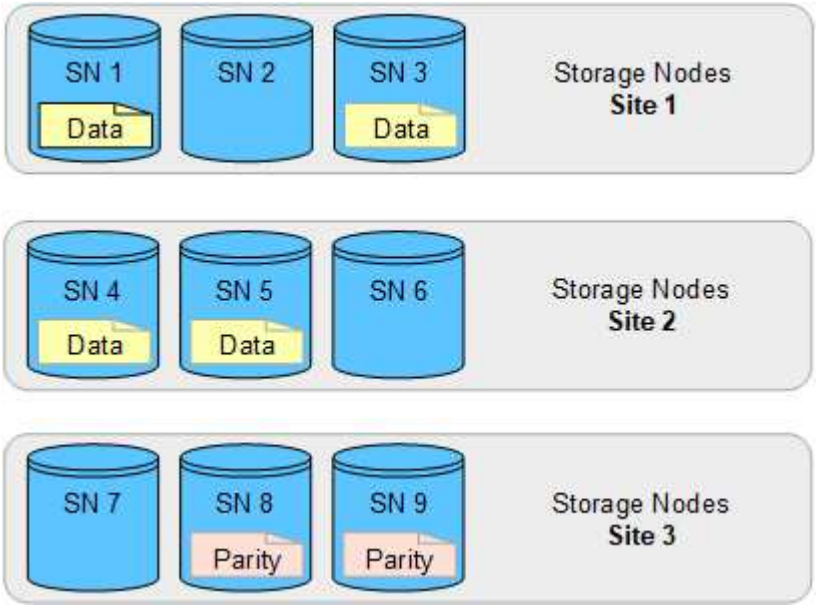
In diesem Beispiel:

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

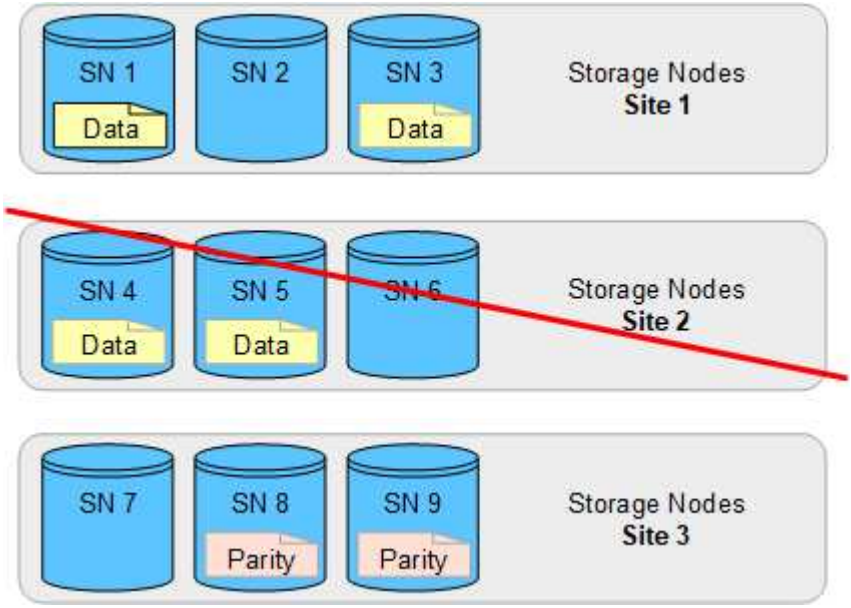
- Jedes der sechs Fragmente wird auf einem anderen Knoten an drei verschiedenen Rechenzentrumsstandorten gespeichert, um den Datenschutz bei Knotenausfällen oder Standortverlust zu gewährleisten.

> Erasure Coding ist in Speicherpools mit beliebig vielen Standorten zulässig, *außer* bei zwei Standorten.

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



Wenn ein Standort ausfällt, können die Daten dennoch wiederhergestellt werden:



Erstellen Sie einen Speicherpool in StorageGRID

Speicherpools werden erstellt, um festzulegen, wo das StorageGRID System Objektdaten speichert und welcher Speichertyp verwendet wird. Jeder Speicherpool umfasst einen oder mehrere Standorte und eine oder mehrere Speicherklassen.

Bei der Installation von StorageGRID 12.0 auf einem neuen Grid werden automatisch Speicherpools für jeden Standort erstellt. Wenn StorageGRID 11.6 oder eine frühere Version installiert wurde, werden Speicherpools nicht automatisch für jeden Standort erstellt.

Wenn Cloud-Speicherpools erstellt werden sollen, um Objektdaten außerhalb des StorageGRID Systems zu speichern, siehe "Informationen zur Nutzung von Cloud Storage Pools".

Bevor Sie beginnen

- Sie sind mit einem "unterstützte Webbrowser" beim Grid Manager angemeldet.
- Du hast "spezifische Zugriffsberechtigungen".
- Sie haben die Richtlinien für die Erstellung von Speicherpools überprüft.

Über diese Aufgabe

Speicherpools legen fest, wo Objektdaten gespeichert werden. Die Anzahl der benötigten Speicherpools hängt von der Anzahl der Standorte in Ihrem Grid und von den gewünschten Kopiertypen ab: repliziert oder mit Erasure-Coding.

- Für die Replikation und die standortspezifische Löschung von Daten einen Speicherpool für jeden Standort erstellen. Wenn beispielsweise replizierte Objektkopien an drei Standorten gespeichert werden sollen, drei Speicherpools erstellen.
- Für das Erasure Coding an drei oder mehr Standorten sollte ein Speicherpool erstellt werden, der für jeden Standort einen Eintrag enthält. Wenn beispielsweise Objekte über drei Standorte hinweg mit Erasure Coding versehen werden sollen, ist ein einzelner Speicherpool zu erstellen.

  Der Standort „All Sites“ sollte nicht in einen Speicherpool aufgenommen werden, der in einem Erasure-Coding-Profil verwendet wird. Stattdessen ist für jeden Standort, der erasure-codierte Daten speichert, ein separater Eintrag im Speicherpool hinzuzufügen. Siehe dieser Schritt für ein Beispiel.

- Wenn Sie über mehr als eine Speicherkategorie verfügen, sollte kein Speicherpool erstellt werden, der verschiedene Speicherkategorien an einem einzigen Standort umfasst. Siehe "Richtlinien für die Erstellung von Speicherpools".

Schritte

1. **ILM** > **Speicherpools** auswählen.

   Die Registerkarte „Storage pools“ listet alle definierten Storage pools auf.

   Bei Neuinstallationen von StorageGRID 11.6 oder älter wird der Speicherpool „All Storage Nodes“ automatisch aktualisiert, wenn neue Rechenzentrumsstandorte hinzugefügt werden. Dieser Pool sollte in ILM-Regeln nicht verwendet werden.

2. Zum Erstellen eines neuen Speicherpools **Erstellen** auswählen.
3. Geben Sie einen eindeutigen Namen für den Speicherpool ein. Ein Name, der bei der Konfiguration von Erasure-Codierungsprofilen und ILM-Regeln leicht zu identifizieren ist, ist empfehlenswert.
4. In der Dropdown-Liste **Standort** einen Standort für diesen Speicherpool auswählen.

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

Im Allgemeinen sollte der Speicherpool „All Sites“ in keinem Speicherpool verwendet werden. ILM-Regeln, die einen All Sites-Speicherpool verwenden, platzieren Objekte an jedem verfügbaren Standort, wodurch die Kontrolle über die Objektplatzierung verringert wird. Außerdem nutzt ein All Sites-Speicherpool die Storage Nodes an einem neuen Standort sofort, was möglicherweise nicht dem erwarteten Verhalten entspricht.

5. In der Dropdown-Liste **Speicherklasse** wird der Speichertyp ausgewählt, der verwendet wird, wenn eine ILM-Regel diesen Speicherpool nutzt.

   Die Speicherklasse, *umfasst alle Speicherklassen*, enthält alle Storage Nodes am ausgewählten Standort. Wenn Sie zusätzliche Speicherklassen für die Storage Nodes in Ihrem Grid erstellt haben, werden diese in der Drop-down-Liste aufgeführt.

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

   > Sie erhalten eine Warnung, wenn mehr als ein Eintrag mit unterschiedlichen Speicherklassen für einen Standort hinzugefügt wird.

   Um einen Eintrag zu entfernen, das Löschsymbol ✕ auswählen.

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

   Der neue Speicherpool ist zur Liste hinzugefügt.

Details zum Speicherpool in StorageGRID anzeigen

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

Bevor Sie beginnen

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

Schritte

1. **ILM** > **Speicherpools** auswählen.

   Die Tabelle „Speicherpools“ enthält für jeden Speicherpool, der Storage Nodes umfasst, die folgenden Informationen:

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

2. Details zu einem bestimmten Speicherpool werden angezeigt, wenn dessen Name ausgewählt wird.

Die Detailseite für den Speicherpool wird angezeigt.

3. Auf der Registerkarte **Knoten** werden Informationen zu den im Storage-Pool enthaltenen Storage-Nodes angezeigt.

   Die Tabelle enthält für jeden Knoten folgende Informationen:

   - Knotenname
   - Name der Website
   - Storage-Qualität
   - Speichernutzung: Der Prozentsatz des gesamten nutzbaren Speicherplatzes für Objektdaten, der für den Storage Node verwendet wurde.

   > Der gleiche Wert für die Speichernutzung (%) wird auch im Diagramm „Storage Used - Object Data“ für jeden Storage Node angezeigt (wählen Sie **Nodes** > ***Storage Node*** > **Storage**).

4. Die Registerkarte **ILM usage** zeigt an, ob der Storage-Pool aktuell in ILM-Regeln oder Erasure-Coding-Profilen verwendet wird.
5. Optional kann die **ILM-Regelseite** aufgerufen werden, um Informationen zu den Regeln zu erhalten und diese zu verwalten, die den Storage-Pool verwenden.

   Siehe "Anleitung zum Arbeiten mit ILM-Regeln".

Bearbeiten Sie einen Speicherpool in StorageGRID

Ein Speicherpool kann bearbeitet werden, um seinen Namen zu ändern oder Standorte und Speicherklassen zu aktualisieren.

Bevor Sie beginnen

- Sie sind mit einem "unterstützte Webbrowser" beim Grid Manager angemeldet.
- Du hast "spezifische Zugriffsberechtigungen".
- Sie haben die "Richtlinien für die Erstellung von Speicherpools" überprüft.
- Wenn Sie planen, einen Speicherpool zu bearbeiten, der von einer Regel in der aktiven ILM-Richtlinie verwendet wird, wurde berücksichtigt, wie sich Ihre Änderungen auf die Datenplatzierung von Objektdaten auswirken.

Über diese Aufgabe

Wenn Sie einem Speicherpool, der in der aktiven ILM-Richtlinie verwendet wird, einen neuen Standort oder eine neue Speicherkategorie hinzufügen, ist zu beachten, dass die Storage Nodes im neuen Standort oder der neuen Speicherkategorie nicht automatisch verwendet werden. Damit StorageGRID einen neuen Standort oder eine neue Speicherkategorie verwendet, muss nach dem Speichern des bearbeiteten Speicherpools eine neue ILM-Richtlinie aktiviert werden.

Schritte

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

   Der Speicherpool „All Storage Nodes“ kann nicht bearbeitet werden (StorageGRID 11.6 und früher).

3. **Bearbeiten** auswählen.
4. Der Name des Speicherpools kann bei Bedarf geändert werden.
5. Bei Bedarf können andere Standorte und Storage-Grades ausgewählt werden.

   Eine Änderung des Standorts oder der Speicherklasse ist nicht möglich, wenn der Speicherpool in einem Erasure-Coding-Profil verwendet wird und die Änderung das Erasure-Coding-Schema ungültig machen würde. Wenn beispielsweise ein in einem Erasure-Coding-Profil verwendeter Speicherpool derzeit eine Speicherklasse mit nur einem Standort enthält, ist die Verwendung einer Speicherklasse mit zwei Standorten nicht möglich, da dies das Erasure-Coding-Schema ungültig machen würde.

   > Das Hinzufügen oder Entfernen von Standorten aus einem bestehenden Speicherpool verschiebt keine vorhandenen, löschungscodierten Daten. Wenn die vorhandenen Daten vom Standort verschoben werden sollen, ist ein neuer Speicherpool und ein neues EC-Profil zu erstellen, um die Daten neu zu codieren.

6. **Speichern** auswählen.

Nachdem Sie fertig sind

Wenn ein neuer Standort oder eine neue Speicherkategorie zu einem Speicherpool hinzugefügt wurde, der in der aktiven ILM-Richtlinie verwendet wird, sollte eine neue ILM-Richtlinie aktiviert werden, damit StorageGRID den neuen Standort oder die neue Speicherkategorie verwendet. Zum Beispiel kann die bestehende ILM-Richtlinie geklont und anschließend der Klon aktiviert werden. Siehe "Mit ILM-Regeln und ILM-Richtlinien arbeiten".

Entfernen Sie einen Speicherpool in StorageGRID

Sie können einen nicht verwendeten Speicherpool entfernen.

Bevor Sie beginnen

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

Schritte

1. **ILM** > **Speicherpools** auswählen.
2. In der Tabelle die Spalte „ILM-Nutzung“ prüfen, um festzustellen, ob der Speicherpool entfernt werden kann.

   Ein Speicherpool kann nicht entfernt werden, wenn er in einer ILM-Regel oder in einem Erasure-Coding-Profil verwendet wird. Gegebenenfalls kann ***Speicherpoolname*** > **ILM-Nutzung** ausgewählt werden, um zu ermitteln, wo der Speicherpool verwendet wird.

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

Cloud Storage Pools verwenden

Erfahren Sie mehr über Cloud Storage Pools in StorageGRID

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

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

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

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

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

Lebenszyklus eines Cloud Storage Pool-Objekts in StorageGRID

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

S3: Lebenszyklus eines Cloud Storage Pool-Objekts

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

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

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

1. **Objekt in StorageGRID gespeichert**

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

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

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

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

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

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

5. **Objekt abgerufen**

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

Azure: Lebenszyklus eines Cloud Storage Pool Objekts

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

1. **Objekt in StorageGRID gespeichert**

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

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

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

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

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

4. **Objekt aus der Archivebene wiederhergestellt**

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

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

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

5. **Objekt abgerufen**

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

Verwandte Informationen

"S3 REST-API verwenden"

Anwendungsfälle für Cloud Storage Pool in StorageGRID

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

StorageGRID Daten an einem externen Speicherort sichern

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

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

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

Zur Implementierung einer Backup-Lösung:

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

Tier-Daten von StorageGRID an externen Speicherort

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

Zur Implementierung einer Tiering-Lösung:

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

Mehrere Cloud-Endpunkte verwalten

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

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

Zur Implementierung mehrerer Cloud-Endpunkte:

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

Anforderungen und Beschränkungen für Cloud Storage Pool in StorageGRID

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

Allgemeine Überlegungen

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

Überlegungen zu den für Cloud Storage Pools verwendeten Ports

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

Standardmäßig verwenden Cloud Storage Pools die folgenden Ports:

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

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

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

Kostenüberlegungen

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

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

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

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

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

S3: Erforderliche Berechtigungen für den Cloud Storage Pool-Bucket

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

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

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

S3: Überlegungen zum Lebenszyklus des externen Buckets

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

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

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

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

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

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

Wenn Sie Objekte im Cloud Storage Pool in S3 Glacier Deep Archive (anstatt in Amazon S3 Glacier) überführen möchten, geben Sie `<StorageClass>DEEP_ARCHIVE</StorageClass>` im Bucket-Lebenszyklus an. Es ist jedoch zu beachten, dass die `Expedited`-Speicherebene nicht zur Wiederherstellung von Objekten aus S3 Glacier Deep Archive verwendet werden kann.

Azure: Überlegungen zur Zugriffsebene

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

Azure: Lebenszyklusverwaltung wird nicht unterstützt

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

Verwandte Informationen

"Einen Cloud Storage Pool erstellen"

Cloud-Speicherpools und CloudMirror Replikation in StorageGRID

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

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

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

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

Erstellen Sie einen Cloud Storage Pool in StorageGRID

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

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

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

Bevor Sie beginnen

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

Schritte

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

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

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

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

Amazon S3/GCP

a. Für das Protokoll entweder HTTPS oder HTTP auswählen.

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

b. Geben Sie den Hostnamen ein. Beispiel:

`s3-aws-region.amazonaws.com`

c. Wählen Sie den URL-Stil aus:

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

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

Azure Blob Storage

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

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

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

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

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

Zugangsschlüssel

Für Amazon S3/GCP oder andere S3-kompatible Anbieter

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

IAM Roles Anywhere

Für den AWS IAM Roles Anywhere Dienst

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

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

CAP (C2S-Zugangsportal)

Für Commercial Cloud Services (C2S) S3-Service

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

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

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

Azure Blob Storage

Nur für Azure Blob Storage, nur Shared Key

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

Diese Werte sind im Azure-Portal zu finden.

Anonym

Es werden keine weiteren Informationen benötigt.

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

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

6. **Speichern** auswählen.

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

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

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

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

Details zum Cloud Storage Pool in StorageGRID anzeigen

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

Bevor Sie beginnen

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

Schritte

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

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

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

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

   Die Detailseite für den Pool wird angezeigt.

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

Bearbeiten Sie einen Cloud Storage Pool in StorageGRID

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

Bevor Sie beginnen

- Sie sind mit einem "unterstützte Webbrowser" beim Grid Manager angemeldet.
- Du hast "spezifische Zugriffsberechtigungen".
- Sie haben die "Überlegungen zu Cloud Storage Pools" überprüft.

Schritte

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

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

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

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

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

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

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

4. **Speichern** auswählen.

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

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

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

Entfernen Sie einen Cloud-Speicherpool in StorageGRID

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

Bevor Sie beginnen

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

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

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

Schritte

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

   Ein Cloud Storage Pool kann nicht entfernt werden, wenn er in einer ILM-Regel oder in einem Erasure-

Coding-Profil verwendet wird.

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

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

6. Bearbeiten Sie jede der geklonten Regeln.

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

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

Cloud Storage Pool löschen

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

Bevor Sie beginnen

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

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

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

Schritte

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

Fehlerbehebung bei Cloud Storage Pools in StorageGRID

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

Feststellen, ob ein Fehler aufgetreten ist

StorageGRID führt für jeden Cloud Storage Pool eine einfache Integritätsprüfung durch, indem das bekannte

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

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

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

Überprüfung, ob ein Fehler behoben wurde

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

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

Fehler: Integritätsprüfung fehlgeschlagen. Fehler vom Endpunkt

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

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

Fehler: Dieser Cloud Storage Pool enthält unerwartete Inhalte

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

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

Einer dieser Schritte kann zur Behebung des Problems beitragen:

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

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

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

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

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

Dieser Fehler kann unter folgenden Umständen auftreten:

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

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

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

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

Fehler: CA-Zertifikat konnte nicht analysiert werden

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

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

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

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

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

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

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

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

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

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

Fehler: In diesem Bucket wurden bereits Objekte platziert

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

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

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

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

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

Dieser Fehler kann auftreten, wenn ein nicht transparenter Speicherproxy zwischen den Storage Nodes und dem externen S3-Endpunkt verwendet wird, der für den Cloud Storage Pool genutzt wird. Dieser Fehler tritt auf, wenn der externe Proxyserver den Cloud Storage Pool-Endpunkt nicht erreichen kann. Beispielsweise kann der DNS-Server den Hostnamen möglicherweise nicht auflösen oder es liegt ein externes Netzwerkproblem vor.

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

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

- Die Netzwerkkonfiguration des Proxyservers prüfen.

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

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

Folgende Schritte können zur Behebung des Problems unternommen werden:

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

Verwandte Informationen

"Lebenszyklus eines Cloud Storage Pool-Objekts"

Verwalten Sie Erasure-Coding-Profile in StorageGRID

Sie können die Details eines Erasure-Coding-Profils einsehen und das Profil bei Bedarf umbenennen. Ein Erasure-Coding-Profil kann deaktiviert werden, wenn es aktuell in keiner ILM-Regel verwendet wird.

Bevor Sie beginnen

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

Details zum Erasure Coding Profil

Sie können die Details eines Erasure-Coding-Profils einsehen, um dessen Status, das verwendete Erasure-Coding-Verfahren und weitere Informationen zu ermitteln.

Schritte

1. **Konfiguration** > **System** > **Erasure Coding** auswählen.
2. Wählen Sie das Profil aus. Die Detailseite für das Profil erscheint.
3. Optional kann auf der Registerkarte „ILM-Regeln“ eine Liste der ILM-Regeln angezeigt werden, die das Profil verwenden, sowie der ILM-Richtlinien, die diese Regeln verwenden.
4. Optional kann die Registerkarte „Storage Nodes“ angezeigt werden, um Details zu jedem Storage Node im Storage-Pool des Profils zu sehen, wie zum Beispiel den Standort und die Speichernutzung.

Ein Erasure-Coding-Profil umbenennen

Es kann sinnvoll sein, ein Erasure-Coding-Profil umzubenennen, um deutlicher zu machen, wofür das Profil dient.

Schritte

1. **Konfiguration** > **System** > **Erasure Coding** auswählen.
2. Wählen Sie das Profil aus, das umbenannt werden soll.

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

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

   > Die Namen von Erasure-Coding-Profilen müssen eindeutig sein. Ein Validierungsfehler tritt auf, wenn der Name eines vorhandenen Profils verwendet wird, selbst wenn dieses Profil deaktiviert wurde.

5. **Speichern** auswählen.

Ein Erasure-Coding-Profil deaktivieren

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

> Bestätigen Sie, dass keine Reparaturvorgänge für erasure-codierte Daten oder Decommission-Verfahren im Gange sind. Eine Fehlermeldung wird zurückgegeben, wenn versucht wird, ein Erasure-Coding-Profil zu deaktivieren, während einer dieser Vorgänge läuft.

Über diese Aufgabe

StorageGRID verhindert die Deaktivierung eines Erasure-Coding-Profils, wenn eine der folgenden Bedingungen zutrifft:

- Das Erasure-Coding-Profil wird aktuell in einer ILM-Regel verwendet.
- Das Erasure-Coding-Profil wird in keiner ILM-Regel mehr verwendet, aber Objektdaten und Paritätsfragmente für das Profil existieren weiterhin.

Schritte

1. **Konfiguration** > **System** > **Erasure Coding** auswählen.
2. Auf der Registerkarte „Aktiv“ in der Spalte **Status** kann überprüft werden, ob das Erasure-Coding-Profil, das deaktiviert werden soll, in keiner ILM-Regel verwendet wird.

   Ein Erasure-Coding-Profil kann nicht deaktiviert werden, 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, sind die folgenden Schritte auszuführen:
   a. Wählen Sie **ILM** > **Regeln**.
   b. Jede Regel auswählen und das Aufbewahrungsdiagramm überprüfen, um festzustellen, ob die Regel das gewünschte Löschcodierungsprofil verwendet, das deaktiviert werden soll.

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. Schließen Sie die zusätzlichen Schritte in der Tabelle ab, abhängig davon, wo das Löschcodierungsprofil verwendet wird.

Wo wurde das Profil verwendet?	**Zusätzliche Schritte, die vor der Deaktivierung des Profils auszuführen sind**	**Weitere Anweisungen sind zu beachten.**
Niemals in einer ILM-Regel verwendet	Es sind keine weiteren Schritte erforderlich. Mit diesem Verfahren kann fortgefahren werden.	*Keine*
In einer ILM Regel, die noch nie in einer ILM Richtlinie verwendet wurde	i. Bearbeiten oder löschen Sie alle betroffenen ILM-Regeln. Wenn die Regel bearbeitet wird, sind alle Platzierungen zu entfernen, die das Erasure-Coding-Profil verwenden. ii. Fahren Sie mit diesem Verfahren fort.	"Mit ILM-Regeln und ILM-Richtlinien arbeiten"
In einer ILM-Regel, die sich derzeit in einer aktiven ILM-Richtlinie befindet	i. Die Richtlinie klonen. ii. Die ILM-Regel, die das Erasure-Coding-Profil verwendet, entfernen. iii. Eine oder mehrere neue ILM-Regeln hinzufügen, damit Objekte geschützt sind. iv. Die neue Richtlinie kann gespeichert, simuliert und aktiviert werden. v. Warten Sie, bis die neue Richtlinie angewendet wird und bestehende Objekte basierend auf den hinzugefügten neuen Regeln an neue Standorte verschoben werden. **Hinweis:** Je nach Anzahl der Objekte und der Größe Ihres StorageGRID Systems kann es Wochen oder sogar Monate dauern, bis die ILM Vorgänge die Objekte gemäß den neuen ILM Regeln an neue Speicherorte verschieben. Sie können zwar versuchen, ein Erasure-Codierungsprofil zu deaktivieren, solange es noch mit Daten verknüpft ist, jedoch schlägt die Deaktivierung fehl. Eine Fehlermeldung informiert Sie, falls das Profil noch nicht zur Deaktivierung bereit ist. vi. Bearbeiten oder löschen Sie die Regel, die Sie aus der Richtlinie entfernt haben. Wenn die Regel bearbeitet wird, sind alle Platzierungen zu entfernen, die das Erasure-Coding-Profil verwenden. vii. Fahren Sie mit diesem Verfahren fort.	"Eine ILM-Richtlinie erstellen" "Mit ILM-Regeln und ILM-Richtlinien arbeiten"

Wo wurde das Profil verwendet?	Zusätzliche Schritte, die vor der Deaktivierung des Profils auszuführen sind	Weitere Anweisungen sind zu beachten.
In einer ILM-Regel, die sich derzeit in einer ILM-Richtlinie befindet	i. Die Richtlinie bearbeiten. ii. Die ILM-Regel, die das Erasure-Coding-Profil verwendet, entfernen. iii. Eine oder mehrere neue ILM-Regeln hinzufügen, damit alle Objekte geschützt sind. iv. Die Richtlinie wird gespeichert. v. Bearbeiten oder löschen Sie die Regel, die Sie aus der Richtlinie entfernt haben. Wenn die Regel bearbeitet wird, sind alle Platzierungen zu entfernen, die das Erasure-Coding-Profil verwenden. vi. Fahren Sie mit diesem Verfahren fort.	"Eine ILM-Richtlinie erstellen" "Mit ILM-Regeln und ILM-Richtlinien arbeiten"

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

4. Wird das Profil in keiner ILM-Regel verwendet, wählen Sie das Optionsfeld und anschließend **Deaktivieren**. Das Dialogfeld „Erasure-Coding-Profil deaktivieren“ wird angezeigt.

> Sie können mehrere Profile gleichzeitig deaktivieren, sofern jedes Profil in keiner Regel verwendet wird.

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

Ergebnisse

- Wenn StorageGRID das Erasure-Coding-Profil deaktivieren kann, lautet dessen Status „Deaktiviert“. Dieses Profil kann für keine ILM-Regel mehr ausgewählt werden. Ein deaktiviertes Profil kann nicht reaktiviert werden.
- Wenn StorageGRID das Profil nicht deaktivieren kann, wird eine Fehlermeldung angezeigt. Eine Fehlermeldung wird beispielsweise angezeigt, wenn Objektdaten noch mit diesem Profil verknüpft sind. Es kann erforderlich sein, mehrere Wochen zu warten, bevor der Deaktivierungsvorgang erneut versucht wird.

S3-Regionen für StorageGRID konfigurieren

ILM-Regeln können Objekte anhand der optionalen Regionen filtern, in denen S3-Buckets erstellt werden, sodass Objekte aus verschiedenen Regionen an verschiedenen Speicherorten abgelegt werden können.

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

> Die Region eines Buckets kann nach der Erstellung des Buckets nicht mehr geändert werden.

Bevor Sie beginnen

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

Über diese Aufgabe

Beim Erstellen eines S3-Buckets kann angegeben werden, dass der Bucket in einer bestimmten Region erstellt wird. Die Angabe einer Region ermöglicht es, den Bucket geografisch in der Nähe der Nutzer zu platzieren, was die Latenz optimieren, Kosten minimieren und regulatorische Anforderungen erfüllen kann.

Beim Erstellen einer ILM-Regel kann es sinnvoll sein, die einem S3-Bucket zugeordnete Region als erweiterten Filter zu verwenden. Beispielsweise lässt sich eine Regel erstellen, die nur für Objekte in S3-Buckets gilt, die in der `us-west-2` Region erstellt wurden. Anschließend kann festgelegt werden, dass Kopien dieser Objekte auf Storage Nodes an einem Rechenzentrumsstandort innerhalb dieser Region platziert werden, um die Latenz zu optimieren.

Bei der Konfiguration von Regionen sind folgende Richtlinien zu beachten:

- Standardmäßig werden alle Buckets als zur `us-east-1`Region zugehörig betrachtet.
- Sie müssen die Regionen mithilfe des Grid Managers erstellen, bevor eine nicht standardmäßige Region beim Erstellen von Buckets mit dem Tenant Manager, der Tenant Management API oder mit dem LocationConstraint-Anforderungselement für S3 PUT Bucket API-Anfragen angegeben werden kann. Ein Fehler tritt auf, wenn eine PUT Bucket-Anfrage eine Region verwendet, die nicht in StorageGRID definiert ist.
- Beim Erstellen des S3-Buckets muss der exakte Regionsname verwendet werden. Regionsnamen sind Groß-/Kleinschreibung. Zulässige Zeichen sind Zahlen, Buchstaben und Bindestriche.

  EU gilt nicht als Alias für eu-west-1. Für die Nutzung der Region EU oder eu-west-1 ist die genaue Bezeichnung erforderlich.

- Eine Region kann nicht gelöscht oder geändert werden, wenn sie in einer Regel verwendet wird, die einer Richtlinie (aktiv oder inaktiv) zugewiesen ist.
- Wenn in einer ILM-Regel eine ungültige Region als erweiterter Filter verwendet wird, kann diese Regel nicht zu einer Richtlinie hinzugefügt werden.

  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 verwenden, um eine Regel zu erstellen und eine Region angeben, die Sie nicht definiert haben.

- Wenn eine Region gelöscht wurde, nachdem sie zum Erstellen eines S3-Buckets verwendet wurde, ist es erforderlich, die Region erneut hinzuzufügen, falls der erweiterte Filter „Standortbeschränkung“ genutzt werden soll, um Objekte in diesem Bucket zu finden.

Schritte

1. **ILM** > **Regionen** auswählen.

   Die Seite „Regionen“ wird angezeigt.

2. Die Registerkarte **Alle Regionen** oder **Standardregion** auswählen.

Alle Regionen

Die Registerkarte **Alle Regionen** listet die aktuell definierten Regionen auf, einschließlich der definierten Standardregion.

> Im Tab „Alle Regionen“ kann die Standardregion weder entfernt noch geändert werden. Im Tab „Standardregion“ lässt sich die Standardregion ändern.

a. Zum Hinzufügen einer Region **Weitere Region hinzufügen** auswählen.
b. Geben Sie den Namen einer Region ein, die beim Erstellen von S3 Buckets verwendet werden soll.

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

c. Um einen ungenutzten Bereich zu entfernen, das Löschsymbol ✕ auswählen.

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

d. Wenn Sie alle Änderungen vorgenommen haben, wählen Sie **Speichern**.

   Sie können diese Regionen nun im Abschnitt „Erweiterte Filter“ in Schritt 1 des Assistenten zum Erstellen von ILM-Regeln auswählen. Siehe "Erweiterte Filter in ILM-Regeln verwenden".

Standardregion

Auf der Registerkarte **Standardregion** wird die aktuell definierte Standardregion angezeigt, die geändert werden kann.

a. Um die Standardregion zu ändern, den Regionsnamen aus den verfügbaren Optionen in der Dropdown-Liste **Standardregion** auswählen.
b. **Speichern** auswählen.

${post_edited_translations.segment}

Erfahren Sie mehr über ILM-Regeln in StorageGRID

Zur Verwaltung von Objekten wird eine Reihe von Regeln für das Informationslebenszyklusmanagement (ILM) erstellt und in einer ILM-Richtlinie organisiert.

Jedes in das System aufgenommene Objekt wird anhand der aktiven Richtlinie geprüft. Wenn eine Regel 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. An jedem Standort werden automatisch drei Kopien der Objektmetadaten vorgehalten, um die Daten vor Verlust zu schützen.

Elemente einer ILM Regel

Eine ILM Regel besteht aus drei Elementen:

- **Filterkriterien**: Die Basis- und erweiterten Filter einer Regel definieren, 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, Art und Position der Objektkopien. Jede Regel kann eine Folge von Platzierungsanweisungen enthalten, um die Anzahl, Art und Position der Objektkopien im Laufe der Zeit zu ändern. Wenn der Zeitraum einer Platzierung abläuft, werden die Anweisungen der nächsten Platzierung automatisch durch die nächste ILM-Auswertung angewendet.
- **Aufnahmeverhalten**: Das Aufnahmeverhalten einer Regel ermöglicht die Auswahl, wie die von der Regel gefilterten Objekte beim Aufnehmen geschützt werden (wenn ein S3-Client ein Objekt im Grid speichert).

ILM Regelfilterung

Beim Erstellen einer ILM-Regel geben Sie Filter an, um festzulegen, auf welche Objekte die Regel angewendet wird.

Im einfachsten Fall verwendet eine Regel 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 enthält Speicheranweisungen für Objekte, die nicht den Filtern einer anderen Regel entsprechen.

- Mit Basisfiltern können Sie verschiedene Regeln auf große, voneinander abgegrenzte Objektgruppen anwenden. Diese Filter ermöglichen es, eine Regel auf bestimmte Mandantenkonten, bestimmte S3 Buckets oder beides anzuwenden.

  Mit einfachen Filtern können Sie unkompliziert verschiedene Regeln auf eine große Anzahl von Objekten anwenden. Beispielsweise müssen die Finanzdaten Ihres Unternehmens möglicherweise aus regulatorischen Gründen gespeichert werden, während Daten der Marketingabteilung für den reibungslosen Geschäftsbetrieb benötigt werden. Nachdem Sie separate Mandantenkonten für jede Abteilung erstellt oder die Daten der verschiedenen Abteilungen in separate S3-Buckets aufgeteilt haben, kann ganz einfach eine Regel erstellt werden, die für alle Finanzdatensätze gilt, und eine zweite Regel, die für alle Marketingdaten gilt.

- Erweiterte Filter bieten Ihnen detaillierte Kontrolle. Sie können Filter erstellen, um Objekte anhand der folgenden Objekteigenschaften auszuwählen:
  - Ingest-Zeitpunkt
  - Letzter Zugriff
  - Der gesamte oder ein Teil des Objektnamens (Key)
  - Standortbeschränkung (nur S3)
  - Objektgröße
  - Benutzermetadaten
  - Object Tag (nur S3)

Sie können Objekte nach sehr spezifischen Kriterien filtern. Beispielsweise werden Objekte, die von der radiologischen Abteilung eines Krankenhauses gespeichert werden, möglicherweise häufig verwendet, solange sie weniger als 30 Tage alt sind und danach nur noch selten, während Objekte, die Patientenbesuchsinformationen enthalten, möglicherweise an die Abrechnungsabteilung der Zentrale des Gesundheitsnetzwerks kopiert werden müssen. Es können Filter erstellt werden, die jeden Objekttyp anhand

von Objektname, Größe, S3-Objekttags oder anderen relevanten Kriterien identifizieren, und anschließend separate Regeln definiert werden, um jede Objektgruppe 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 Personalakten in einer bestimmten Region und Richtlinieninformationen zentral speichern muss. In diesem Fall lassen sich Regeln erstellen, die nach Mandantenkonto filtern, um die Datensätze der einzelnen Abteilungen zu trennen, wobei in jeder Regel Filter verwendet werden, um den jeweiligen Objekttyp zu identifizieren, auf den die Regel zutrifft.

ILM Regelplatzierungsanweisungen

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

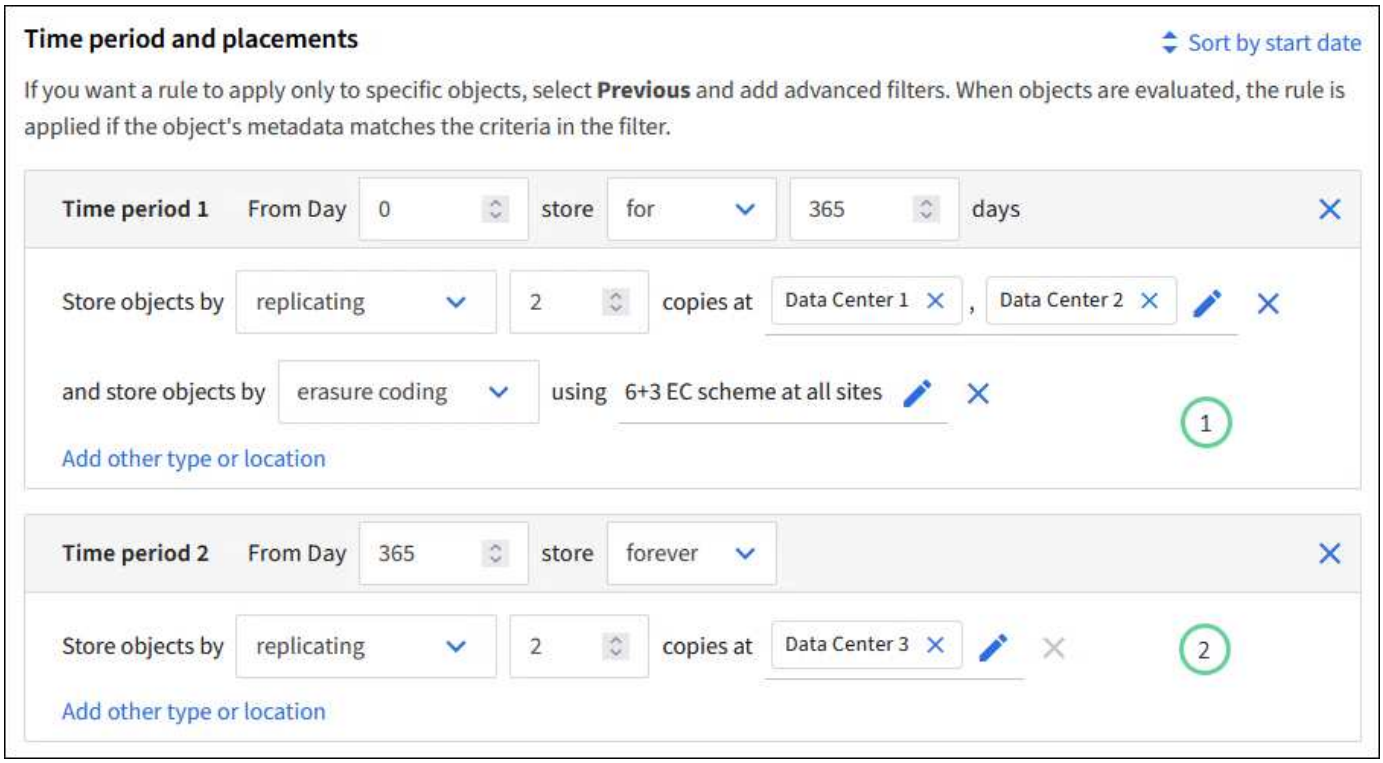
Beim Erstellen von Platzierungsanweisungen:

- Zunächst wird der Referenzzeitpunkt festgelegt, der bestimmt, wann die Platzierungsanweisungen beginnen. Der Referenzzeitpunkt kann der Zeitpunkt sein, zu dem ein Objekt aufgenommen wird, zu dem auf ein Objekt zugegriffen wird, zu dem ein versioniertes Objekt nicht mehr aktuell ist, oder ein benutzerdefinierter Zeitpunkt.
- Anschließend wird festgelegt, wann die Platzierung relativ zum Referenzzeitpunkt gilt. Beispielsweise kann eine Platzierung am Tag 0 beginnen und 365 Tage andauern, bezogen auf den Zeitpunkt der Objektaufnahme.
- Abschließend wird die Art der Kopien (Replikation oder Erasure Coding) und der Speicherort der Kopien festgelegt. Zum Beispiel kann es sinnvoll sein, zwei replizierte Kopien an zwei verschiedenen Standorten zu speichern.

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

- Um Objekte an mehreren Orten innerhalb eines Zeitraums zu platzieren, **Anderen Typ oder Ort hinzufügen** auswählen, um für diesen Zeitraum mehr als eine Zeile hinzuzufügen.
- Um Objekte in verschiedenen Zeiträumen an unterschiedlichen Orten zu platzieren, kann mit **Weiteren Zeitraum hinzufügen** der nächste Zeitraum hinzugefügt werden. Anschließend sind eine oder mehrere Zeilen innerhalb des Zeitraums anzugeben.

Das Beispiel zeigt zwei Platzierungsanweisungen auf der Seite „Platzierungen definieren“ des Assistenten zum Erstellen von ILM-Regeln.



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

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

Die zweite Platzierungsanweisung (2) erstellt nach einem Jahr zwei Kopien und bewahrt diese Kopien dauerhaft auf.

Wenn Sie die Platzierungsanweisungen für eine Regel definieren, muss sichergestellt sein, dass mindestens eine Platzierungsanweisung am Tag 0 beginnt, dass keine Lücken zwischen den von Ihnen definierten Zeiträumen bestehen und dass die letzte Platzierungsanweisung entweder unbegrenzt oder so lange fortgesetzt wird, bis keine Objektkopien mehr benötigt werden.

Sobald ein Zeitraum innerhalb der Regel abläuft, werden die Anweisungen zur Inhaltsplatzierung für den nächsten Zeitraum angewendet. Neue Objektkopien werden erstellt und nicht mehr benötigte Kopien gelöscht.

ILM-Regel-Ingest-Verhalten

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

- **Ausgewogen**: StorageGRID versucht, beim Datenimport alle in der ILM-Regel festgelegten Kopien zu erstellen. Ist dies nicht möglich, werden Zwischenkopien erstellt und dem Client eine Erfolgsmeldung zurückgegeben. Die in der ILM-Regel festgelegten Kopien werden erstellt, sobald dies möglich ist.
- **Streng**: Alle in der ILM-Regel angegebenen Kopien müssen erstellt werden, bevor dem Client Erfolg gemeldet wird.
- **Dual commit**: StorageGRID erstellt sofort temporäre Kopien des Objekts und gibt dem Client eine Erfolgsmeldung zurück. Kopien, die in der ILM-Regel angegeben sind, werden nach Möglichkeit erstellt.

Verwandte Informationen

- "Aufnahmeoptionen"
- "Vorteile, Nachteile und Einschränkungen der Aufnahmemöglichkeiten"
- "Wie Konsistenz- und ILM-Regeln zusammenwirken, um den Datenschutz zu beeinflussen"

Beispiel einer ILM-Regel

Eine ILM Regel könnte beispielsweise Folgendes festlegen:

- Gilt nur für Objekte, die zu Tenant A gehören.
- Zwei replizierte Kopien dieser Objekte werden erstellt und jede Kopie an einem anderen Standort gespeichert.
- Die beiden Kopien werden dauerhaft gespeichert, das bedeutet, dass StorageGRID sie nicht automatisch löscht. Stattdessen bewahrt StorageGRID diese Objekte auf, bis sie entweder durch eine Löschanforderung eines Clients oder durch das Ablaufen eines Bucket-Lebenszyklus gelöscht werden.
- Die Option „Ausgewogen“ für das Aufnahmeverhalten bewirkt, dass die Anweisung zur Platzierung an zwei Standorten angewendet wird, sobald Mandant A ein Objekt in StorageGRID speichert, es sei denn, es ist nicht möglich, beide erforderlichen Kopien sofort zu erstellen.

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

Verwandte Informationen

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

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

ILM-Regeln ermöglichen die Verwaltung der Platzierung von Objektdaten im Zeitverlauf. Zum Erstellen einer ILM-Regel wird der Assistent „ILM-Regel erstellen“ verwendet.

Wenn die Standard-ILM-Regel für eine Richtlinie erstellt werden soll, ist stattdessen der "Anleitung zum Erstellen einer Standard ILM-Regel" zu befolgen.

Bevor Sie beginnen

- Sie sind mit einem "unterstützte Webbrowser" beim Grid Manager angemeldet.
- Du hast "spezifische Zugriffsberechtigungen".
- Wenn Sie festlegen möchten, für welche Mandantenkonten diese Regel gilt, haben Sie die "Berechtigung für Mieterkonten" 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 sein.
- Sie haben alle Cloud-Speicherpools konfiguriert, die Sie verwenden möchten. Siehe "Cloud Storage Pool erstellen".
- Sie sind mit dem "Aufnahmeoptionen" vertraut.
- Wenn Sie eine konforme Regel für die Verwendung mit S3 Object Lock erstellen müssen, sind Sie mit der "Anforderungen für S3 Object Lock" vertraut.

- Optional haben Sie sich das Video angesehen:

  Überblick über ILM-Regeln

Über diese Aufgabe

Beim Erstellen von ILM-Regeln:

- Die Topologie und die Speicherkonfigurationen des StorageGRID Systems sind zu berücksichtigen.
- Berücksichtigen Sie, welche Arten von Objektkopien (repliziert oder mit Löschcodierung) und wie viele Kopien jedes Objekts erforderlich sind.
- Bestimmt werden die Arten von Objektmetadaten, die in den Anwendungen verwendet werden, die mit dem StorageGRID System verbunden sind. ILM-Regeln filtern Objekte anhand ihrer Metadaten.
- Berücksichtigen Sie, wo Objektkopien im Laufe der Zeit platziert werden sollen.
- Es wird festgelegt, welche Aufnahmeoption verwendet wird (Balanced, Strict oder Dual commit).

Schritte

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

Geben Sie Details und Filter für eine StorageGRID ILM-Regel ein

Im Schritt **Details eingeben** des Assistenten zum Erstellen einer ILM-Regel ist es möglich, einen Namen und eine Beschreibung für die Regel einzugeben sowie Filter für die Regel zu definieren.

Das Eingeben einer Beschreibung und das Definieren von Filtern für die Regel sind optional.

Über diese Aufgabe

Bei der Auswertung eines Objekts anhand einer "ILM Regel" Regel vergleicht StorageGRID die Objektmetadaten mit den Filtern der Regel. Wenn die Objektmetadaten mit allen Filtern übereinstimmen, verwendet StorageGRID die Regel, um das Objekt zu platzieren. Eine Regel kann so gestaltet werden, dass sie für alle Objekte gilt, oder es können grundlegende Filter wie ein oder mehrere Mandantenkonten oder Bucket-Namen sowie erweiterte Filter wie die Objektgröße oder Benutzermetadaten angegeben werden.

Schritte

1. Geben Sie im Feld **Name** einen eindeutigen Namen für die Regel ein.
2. Optional kann im Feld **Beschreibung** eine kurze Beschreibung der Regel eingegeben werden.

   Der Zweck oder die Funktion der Regel sollte beschrieben werden, damit die Regel später wiedererkannt werden kann.

3. Optional kann ein oder mehrere S3-Mandantenkonten ausgewählt werden, für die diese Regel gilt. Wenn diese Regel für alle Mandanten gilt, bleibt dieses Feld leer.

   Wenn Sie weder über die Root-Zugriffsberechtigung noch über die Berechtigung für Tenant accounts verfügen, können Sie keine Tenants aus der Liste auswählen. Stattdessen die Tenant-ID oder mehrere IDs als durch Kommas getrennte Zeichenfolge eingeben.

4. Optional können die S3-Buckets angegeben werden, für die diese Regel gilt.

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

5. Für S3-Mandanten kann optional **Ja** ausgewählt werden, um die Regel nur auf ältere Objektversionen in S3 Buckets anzuwenden, für die die Versionierung aktiviert ist.

   Wenn Sie **Ja** auswählen, wird "Nicht-aktuelle Zeit" automatisch als Referenzzeit in "Schritt 2 des Assistenten zum Erstellen einer ILM-Regel" ausgewählt.

   > Nicht-aktuelle Zeit gilt nur für S3-Objekte in Buckets mit aktivierter Versionsverwaltung. Siehe "Operationen an Buckets, PutBucketVersioning" und "Objekte mit S3 Object Lock verwalten".

   Sie können diese Option nutzen, um den Speicherbedarf versionierter Objekte zu reduzieren, indem Sie nach nicht aktuellen Objektversionen filtern. Siehe "Beispiel 4: ILM Regeln und Richtlinien für versionierte S3-Objekte".

6. Optional kann **Erweiterten Filter hinzufügen** ausgewählt werden, um zusätzliche Filter anzugeben.

   Wenn Sie keine erweiterte Filterung konfigurieren, gilt die Regel für alle Objekte, die den Basisfiltern entsprechen. Weitere Informationen zur erweiterten Filterung finden sich unter Erweiterte Filter in ILM-Regeln verwenden und Mehrere Metadatentypen und -werte angeben.

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

Erweiterte Filter in ILM-Regeln verwenden

Die erweiterte Filterung ermöglicht die Erstellung von ILM-Regeln, die nur auf bestimmte Objekte basierend auf deren Metadaten angewendet werden. Beim Einrichten der erweiterten Filterung für eine Regel werden der gewünschte Metadatentyp, ein Operator und ein Metadatenwert ausgewählt. Bei der Auswertung von Objekten wird die ILM-Regel nur auf diejenigen 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
Ingest-Zeitpunkt	• ist • ist nicht • ist vorher • ist am oder vor • ist nach • ist an oder nach	Zeit und Datum, zu denen das Objekt aufgenommen wurde. **Hinweis:** Um Ressourcenprobleme bei der Aktivierung einer neuen ILM-Richtlinie zu vermeiden, kann der erweiterte Filter „Ingest time“ in allen Regeln verwendet werden, die den Speicherort einer großen Anzahl vorhandener Objekte ändern könnten. Die Ingest time sollte auf einen Wert größer oder gleich dem ungefähren Zeitpunkt gesetzt werden, zu dem die neue Richtlinie in Kraft tritt, damit vorhandene Objekte nicht unnötig verschoben werden.

Metadatentyp	Unterstützte Operatoren	Metadatenwert
Schlüssel	• gleich • ist nicht gleich • enthält • enthält nicht • beginnt mit • beginnt nicht mit • endet mit • endet nicht mit	Ganz oder teilweise ein eindeutiger S3-Objektschlüssel. Beispielsweise kann es erforderlich sein, Objekte abzugleichen, die mit `.txt` enden oder mit `test-object/` beginnen.
Letzter Zugriff	• ist • ist nicht • ist vorher • ist am oder vor • ist nach • ist an oder nach	Zeit und Datum, zu denen das Objekt zuletzt abgerufen (gelesen oder angezeigt) wurde. **Hinweis:** Wenn "Letzte Zugriffszeit verwenden" als erweiterter Filter verwendet werden soll, müssen Aktualisierungen der letzten Zugriffszeit für den S3-Bucket aktiviert sein.
Standortbeschränkung (nur S3)	• gleich • ist nicht gleich	Die Region, in der ein S3-Bucket erstellt wurde. **ILM** > **Regionen** dient zur Definition der anzuzeigenden Regionen. **Hinweis:** Der Wert „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. Siehe "S3-Regionen konfigurieren".
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 größer als 1 MB. Erasure Coding sollte für Objekte kleiner als 200 KB nicht verwendet werden, um den Aufwand für die Verwaltung sehr kleiner erasure-codierter Fragmente zu vermeiden.

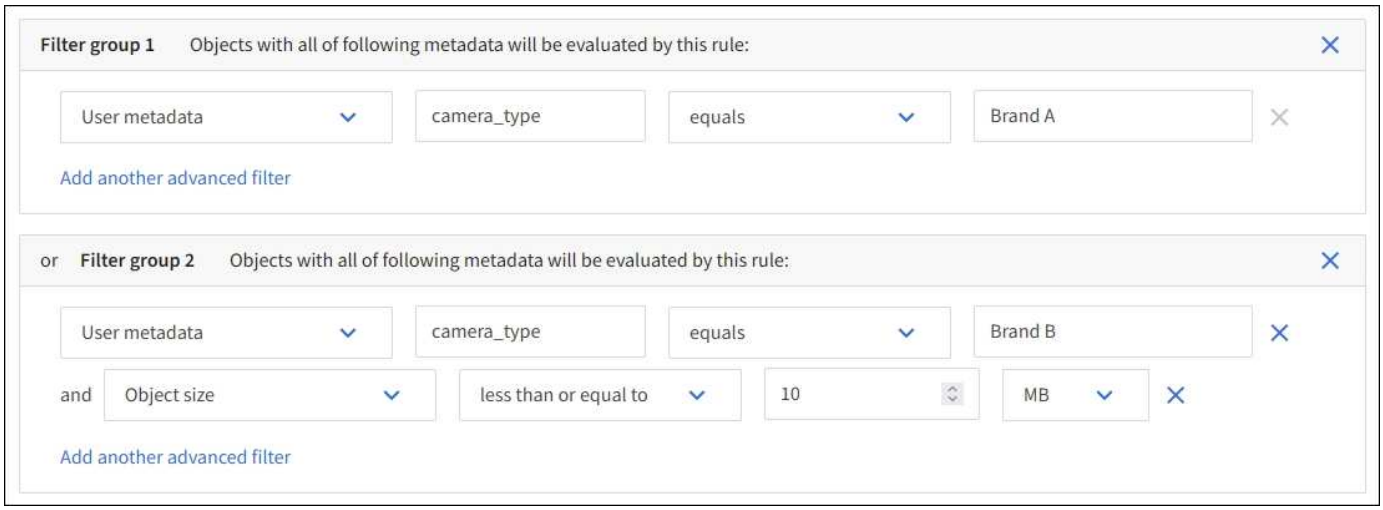
Metadatentyp	Unterstützte Operatoren	Metadatenwert
Benutzermetadaten	• enthält • endet mit • gleich • existiert • beginnt mit • enthält nicht • endet nicht mit • ist nicht gleich • Existiert nicht • beginnt nicht mit	Schlüssel-Wert-Paar, wobei **Benutzermetadatenname** der Schlüssel und **Metadatenwert** der Wert ist. Um beispielsweise nach Objekten zu filtern, die Benutzermetadaten von `color=blue` haben, `color` für **Benutzermetadatenname**, `equals` für den Operator und `blue` für **Metadatenwert** angeben. **Hinweis:** Benutzermetadatennamen sind nicht Groß-/Kleinschreibung, Benutzermetadatenwerte sind Groß-/Kleinschreibung.
Object 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. Beispielsweise kann für die Filterung von Objekten mit einem Objekt-Tag von `Image=True Image` für **Object tag name**, `equals` für den Operator und `True` für **Object tag value** angegeben werden. **Hinweis:** Objekt-Tag-Namen und Objekt-Tag-Werte sind Groß-/Kleinschreibung. Diese Angaben müssen exakt so eingegeben werden, wie sie für das Objekt definiert wurden.

Mehrere Metadatentypen und -werte angeben

Bei der Definition erweiterter Filter können Sie mehrere Metadatentypen und mehrere Metadatenwerte festlegen. Wenn beispielsweise eine Regel Objekte mit einer Größe zwischen 10 MB und 100 MB erfassen soll, wird der Metadatentyp **Object size** ausgewählt und zwei Metadatenwerte angegeben.

- Der erste Metadatenwert gibt Objekte mit einer Größe von mindestens 10 MB an.
- Der zweite Metadatenwert gibt Objekte mit einer Größe von maximal 100 MB an.

Durch die Verwendung mehrerer Einträge lässt sich präzise steuern, welche Objekte abgeglichen werden. Im folgenden Beispiel gilt die Regel für Objekte, bei denen der Wert der Benutzer-Metadaten camera_type „Brand A“ oder „Brand B“ ist. Die Regel gilt jedoch nur für jene Brand B Objekte, die kleiner als 10 MB sind.



Platzierungsanweisungen für eine StorageGRID ILM-Regel definieren

Im Schritt **Platzierungen definieren** des Assistenten zum Erstellen von ILM-Regeln lassen sich die Platzierungsanweisungen festlegen, die bestimmen, wie lange Objekte gespeichert werden, welche Art von Kopien (repliziert oder mit Erasure-Coding), der Speicherort und die Anzahl der Kopien.

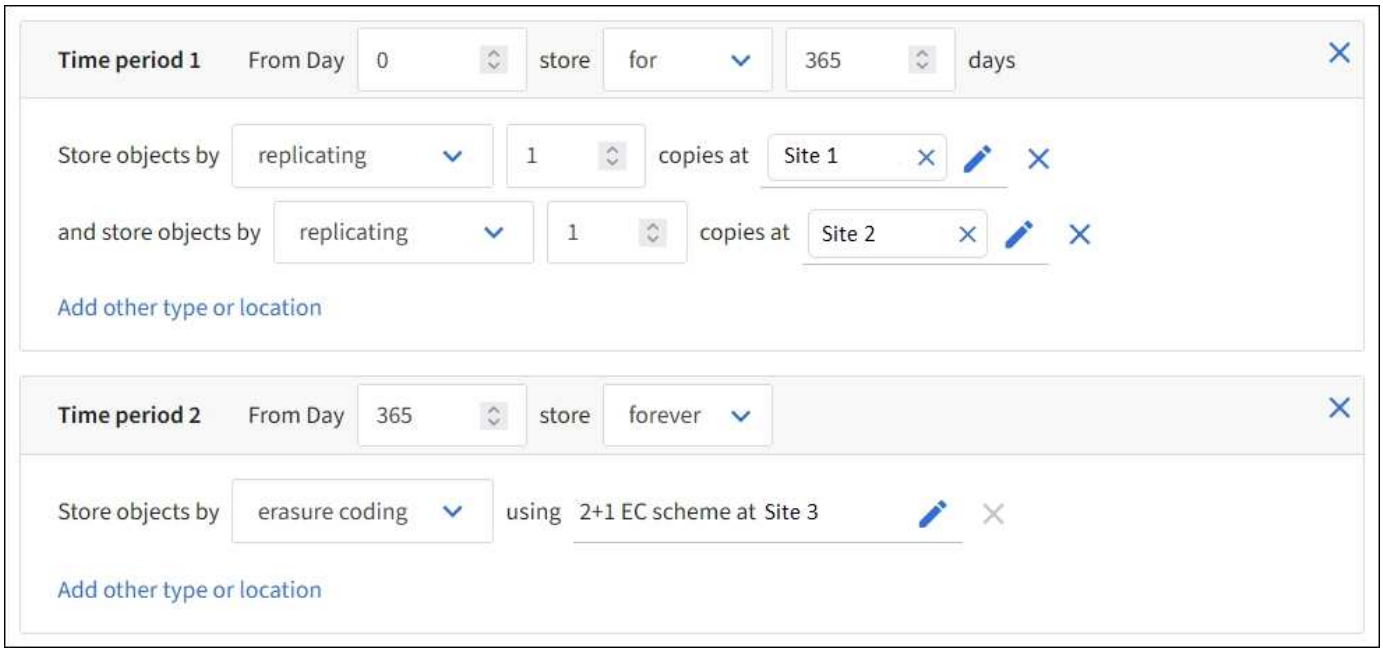
> Die gezeigten Screenshots sind Beispiele. Ihre Ergebnisse können je nach StorageGRID Version abweichen.

Über diese Aufgabe

Eine ILM-Regel kann eine oder mehrere Platzierungsanweisungen enthalten. Jede Platzierungsanweisung gilt für einen einzelnen Zeitraum. Wenn mehr als eine Anweisung verwendet wird, müssen die Zeiträume angrenzend sein, und mindestens eine Anweisung muss am Tag 0 beginnen. Die Anweisungen können entweder unbegrenzt fortgesetzt werden oder bis keine Objektkopien mehr benötigt werden.

Jede Platzierungsanweisung kann mehrere Zeilen umfassen, wenn verschiedene Arten von Kopien erstellt oder während dieses Zeitraums verschiedene Orte genutzt werden sollen.

In diesem Beispiel speichert die ILM-Regel im ersten Jahr je eine replizierte Kopie an Standort 1 und an Standort 2. Nach einem Jahr wird eine 2+1 erasure-coded Kopie erstellt und nur an einem Standort gespeichert.



Schritte

1. Für **Referenzzeit** den Zeittyp auswählen, der bei der Berechnung der Startzeit für eine Platzierungsanweisung verwendet wird.

Option	Beschreibung
Ingest-Zeitpunkt	Der Zeitpunkt, zu dem das Objekt aufgenommen wurde.
Letzter Zugriff	Der Zeitpunkt, zu dem das Objekt zuletzt abgerufen (gelesen oder angezeigt) wurde. Um diese Option nutzen zu können, müssen Aktualisierungen der letzten Zugriffszeit für den S3-Bucket aktiviert sein. Siehe "Letzte Zugriffszeit in ILM-Regeln verwenden".
Benutzerdefinierte Erstellungszeit	Ein in benutzerdefinierten Metadaten festgelegter Zeitpunkt.
Nichtaktuelle Zeit	„Nicht-aktuelle Zeit“ wird automatisch ausgewählt, wenn **Ja** für die Frage „Diese Regel nur auf ältere Objektversionen anwenden (in S3-Buckets mit aktivierter Versionierung)?“ in "Schritt 1 des Assistenten zum Erstellen einer ILM Regel" ausgewählt wurde.

   Wenn Sie eine *konforme* Regel erstellen möchten, muss **Aufnahmezeit** ausgewählt werden. Weitere Informationen finden Sie unter "Objekte mit S3 Object Lock verwalten".

2. Im Abschnitt **Zeitraum und Platzierungen** eine Startzeit und eine Dauer für den ersten Zeitraum eingeben.

   Beispielsweise kann festgelegt werden, wo Objekte im ersten Jahr gespeichert werden (Ab Tag 0 für 365 Tage speichern). Mindestens eine Anweisung muss bei Tag 0 beginnen.

3. Wenn Sie replizierte Kopien erstellen möchten:

a. In der Dropdown-Liste **Objekte speichern nach** ist **Replikation** auszuwählen.

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

   Eine Warnung wird angezeigt, wenn die Anzahl der Kopien auf 1 geändert wird. Eine ILM-Regel, die für einen beliebigen Zeitraum nur eine replizierte Kopie erstellt, setzt Daten dem Risiko eines dauerhaften Verlusts aus. Weitere Informationen unter "Warum die Einzelkopie-Replikation nicht verwendet werden sollte".

   Um das Risiko zu vermeiden, kann eine oder mehrere der folgenden Maßnahmen durchgeführt werden:

   - Die Anzahl der Kopien für den Zeitraum erhöhen.
   - Kopien können zu anderen Speicherpools oder zu einem Cloud Storage Pool hinzugefügt werden.
   - **Erasure Coding** statt **Replicating** auswählen.

     Diese Warnung kann ignoriert werden, wenn diese Regel bereits mehrere Kopien für alle Zeiträume erstellt.

c. Im Feld **Kopien bei** die Speicherpools auswählen, die hinzugefügt werden sollen.

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

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

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

   - Die Anzahl der Kopien darf 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.
   - Ist die Anzahl der Kopien geringer als die Anzahl der Speicherpools, wird eine Kopie am Aufnahmestandort gespeichert, und das System verteilt anschließend die verbleibenden Kopien, um die Festplattennutzung auf die Pools auszugleichen, wobei sichergestellt wird, dass kein Standort mehr als eine Kopie eines Objekts erhält.
   - Wenn sich die Speicherpools überschneiden (die gleichen Storage Nodes enthalten), könnten alle Kopien des Objekts nur an einem Standort gespeichert werden. Aus diesem Grund sollte weder der All Storage Nodes Speicherpool (StorageGRID 11.6 und früher) noch ein weiterer Speicherpool angegeben werden.

4. Wenn Sie eine löschcodierte Kopie erstellen möchten:

   a. In der Dropdown-Liste **Objekte speichern nach** ist **Erasure Coding** auszuwählen.

      Erasure Coding eignet sich am besten für Objekte größer als 1 MB. Erasure Coding sollte für Objekte kleiner als 200 KB nicht verwendet werden, um den Aufwand für die Verwaltung sehr kleiner erasure-codierter 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 anschließend **Erweiterten Filter hinzufügen**

und legen Sie einen **Objektgrößen**-Filter auf einen beliebigen 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 löschcodierte Kopie enthält den Namen des Löschcodierungsverfahrens, gefolgt vom Namen des Speicherpools.

Die verfügbaren Erasure-Coding-Verfahren sind durch die Anzahl der Storage Nodes im ausgewählten Speicherpool begrenzt. Ein `Recommended`-Abzeichen erscheint neben den Verfahren, die entweder die "bester Schutz oder geringster Speicherplatzbedarf" bereitstellen.

5. Optional:

   a. **Anderen Typ oder Standort hinzufügen** auswählen, um zusätzliche Kopien an verschiedenen Standorten zu erstellen.

   b. **Weiteren Zeitraum hinzufügen** auswählen, um verschiedene Zeiträume hinzuzufügen.

> Objektlöschungen erfolgen auf Grundlage der folgenden Einstellungen:
>
> - Objekte werden am Ende des letzten Zeitraums automatisch gelöscht, es sei denn, ein anderer Zeitraum endet mit **forever**.
> - Je nach "Einstellungen für Bucket- und Mandanten-Aufbewahrungsfristen"Konfiguration werden Objekte möglicherweise auch dann nicht gelöscht, wenn die ILM-Aufbewahrungsfrist abläuft.

6. Wenn Sie Objekte in einem Cloud Storage Pool speichern möchten:

   a. In der Dropdown-Liste **Objekte speichern nach** die Option **Replikation** auswählen.

   b. Wählen Sie das Feld **Kopien bei** aus und wählen Sie anschließend einen Cloud Storage Pool aus.

      Bei der Verwendung von Cloud Storage Pools sind die folgenden Regeln zu beachten:

      - In einer einzelnen Platzierungsanweisung kann nicht mehr als ein Cloud Storage Pool ausgewählt werden. Ebenso kann in derselben Platzierungsanweisung nicht sowohl ein Cloud Storage Pool als auch ein Speicherpool ausgewählt werden.
      - In einem Cloud-Speicherpool kann nur eine Kopie eines Objekts gespeichert werden. Eine Fehlermeldung erscheint, wenn **Kopien** auf 2 oder mehr gesetzt wird.
      - Es können nicht mehrere Objektkopien gleichzeitig in einem Cloud Storage Pool gespeichert werden. Eine Fehlermeldung erscheint, wenn mehrere Platzierungen, die einen Cloud Storage Pool verwenden, sich überschneidende Datumsangaben aufweisen oder wenn mehrere Zeilen in derselben Platzierung einen Cloud Storage Pool verwenden.
      - Sie können ein Objekt gleichzeitig in einem Cloud Storage Pool speichern, während dieses Objekt als replizierte oder mit Erasure-Codierung versehene Kopien in StorageGRID gespeichert wird. Allerdings muss die Platzierungsanweisung für den Zeitraum mehr als eine Zeile enthalten, sodass die Anzahl und die Typen der Kopien für jeden Speicherort angegeben werden können.

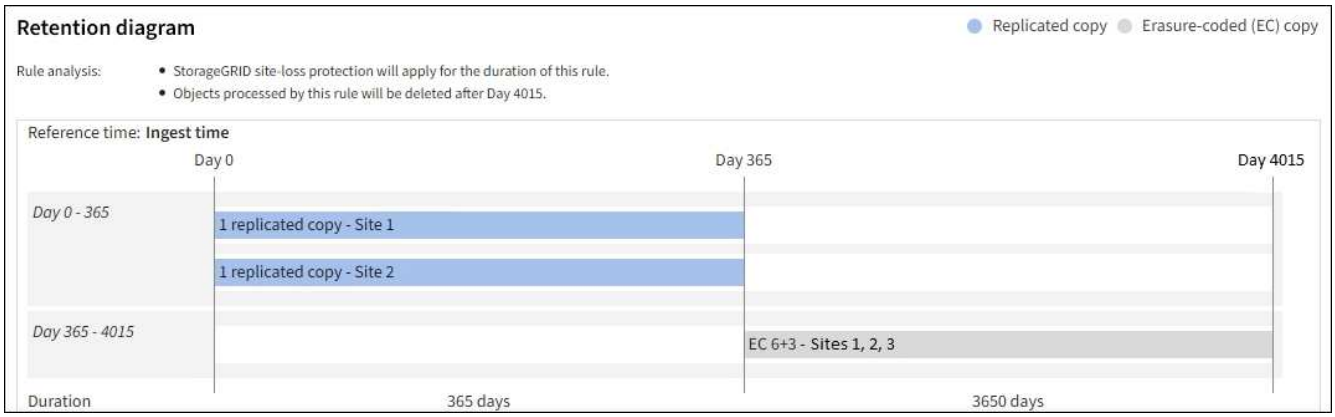
7. Im Retentionsdiagramm die Platzierungsanweisungen bestätigen.

   In diesem Beispiel speichert die ILM-Regel im ersten Jahr je 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-erasure-coded Kopie an drei Standorten gespeichert. Nach insgesamt 11 Jahren werden die Objekte aus StorageGRID gelöscht.

Im Abschnitt „Regelanalyse“ des Aufbewahrungsdiagramms heißt es:

- StorageGRID Site-Loss-Schutz gilt für die Dauer dieser Regel.
- Objekte, die von dieser Regel verarbeitet wurden, werden nach Tag 4015 gelöscht.

  Siehe "Schutz vor Standortausfall aktivieren."



8. Wählen Sie **Weiter**. "Schritt 3 (Ingest-Verhalten auswählen)" Der Assistent zum Erstellen einer ILM-Regel wird angezeigt.

Letzte Zugriffszeit in StorageGRID ILM-Regeln verwenden

Sie können den Zeitpunkt des letzten Zugriffs als Referenzzeitpunkt in einer ILM-Regel verwenden. Zum Beispiel kann es gewünscht sein, Objekte, die in den letzten drei Monaten angezeigt wurden, auf lokalen Storage Nodes zu belassen, während Objekte, die nicht so kürzlich angezeigt wurden, an einen externen Standort verschoben werden. Der Zeitpunkt des letzten Zugriffs kann auch als erweiterter Filter verwendet werden, wenn eine ILM-Regel nur auf Objekte angewendet werden soll, auf die zuletzt an einem bestimmten Datum zugegriffen wurde.

Über diese Aufgabe

Vor der Verwendung der letzten Zugriffszeit in einer ILM-Regel sind die folgenden Punkte zu berücksichtigen:

- Wenn die letzte Zugriffszeit als Referenzzeit verwendet wird, ist zu beachten, dass eine Änderung der letzten Zugriffszeit für ein Objekt keine sofortige ILM-Auswertung auslöst. Stattdessen werden die Platzierungen des Objekts überprüft und das Objekt wird bei der Hintergrund-ILM-Auswertung entsprechend verschoben. Dies kann zwei Wochen oder länger nach dem Zugriff auf das Objekt dauern.

  Diese Latenz ist bei der Erstellung von ILM Regeln auf Basis der letzten Zugriffszeit zu berücksichtigen, und Platzierungen, die kurze Zeiträume (weniger als einen Monat) verwenden, sind zu vermeiden.

- Wenn die letzte Zugriffszeit als erweiterter Filter oder als Referenzzeit verwendet wird, muss die Aktualisierung der letzten Zugriffszeit für S3-Buckets aktiviert werden. Es kann entweder die "Tenant Manager" oder die "Mandantenverwaltungs-API" verwendet werden.

  Die Aktualisierung der letzten Zugriffszeit ist für S3 Buckets standardmäßig deaktiviert.

Beachten Sie, dass die Aktivierung von Aktualisierungen der letzten Zugriffszeit die Leistung beeinträchtigen kann, insbesondere in Systemen mit kleinen Objekten. Die Leistungseinbußen entstehen, weil StorageGRID die Objekte bei jedem Abruf mit neuen Zeitstempeln versehen muss.

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

Art der Anfrage	Ob die letzte Zugriffszeit aktualisiert wird, wenn Aktualisierungen der letzten Zugriffszeit deaktiviert sind	Ob die letzte Zugriffszeit aktualisiert wird, wenn Aktualisierungen der letzten Zugriffszeit aktiviert sind
Anfrage zum Abrufen eines Objekts, seiner Zugriffssteuerungsliste oder seiner Metadaten	Nein	Ja
Anfrage zur Aktualisierung der Metadaten eines Objekts	Ja	Ja
Anfrage 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 zusammengebaute Objekt	Ja, für das zusammengebaute Objekt

Wählen Sie das Aufnahmeverhalten für eine StorageGRID ILM-Regel aus

Im Schritt **Aufnahmeverhalten auswählen** des Assistenten zum Erstellen einer ILM-Regel lässt sich festlegen, wie die durch diese Regel gefilterten Objekte beim Aufnehmen geschützt werden.

Über diese Aufgabe

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

Schritte

1. Die "Ingest-Verhalten" zur Verwendung auswählen.

   Weitere Informationen finden sich unter "Vorteile, Nachteile und Einschränkungen der Aufnahmemöglichkeiten".

Die Optionen „Ausgewogen“ oder „Streng“ können nicht verwendet werden, wenn die Regel eine dieser Platzierungen verwendet:

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

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

2. Wählen Sie **Create**.

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

   Die Details der Regel sind auf der ILM-Regelseite durch Auswahl des Namens der Regel einsehbar.

Erstellen Sie eine Standard-ILM-Regel in StorageGRID

Bevor eine ILM-Richtlinie erstellt wird, muss eine Standardregel definiert werden, die alle Objekte, die keiner anderen Regel in der Richtlinie zugeordnet sind, aufnimmt. Die Standardregel darf keine Filter verwenden. Sie muss für alle Mandanten, alle Buckets und alle Objektversionen gelten.

Bevor Sie beginnen

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

Über diese Aufgabe

Die Standardregel wird in einer ILM-Richtlinie als letzte Regel ausgewertet und kann daher keine Filter verwenden. Die Platzierungsanweisungen der Standardregel werden auf alle Objekte angewendet, die keiner anderen Regel in der Richtlinie zugeordnet sind.

In dieser Beispielrichtlinie gilt die erste Regel nur für Objekte, die zum Mandanten test-tenant-1 gehören. Die Standardregel, die zuletzt steht, gilt für Objekte, die zu allen anderen Mandantenkonten gehören.

Beim Erstellen der Standardregel sind folgende Anforderungen zu beachten:

- Die Standardregel wird beim Hinzufügen zu einer Richtlinie automatisch als letzte Regel platziert.
- Die Standardregel kann keine einfachen oder erweiterten Filter verwenden.
- Die Standardregel muss für alle Objektversionen gelten.
- Die Standardregel sollte replizierte Kopien erstellen.

> Verwenden Sie keine Regel, die löschcodierte Kopien erstellt, als Standardregel für eine Richtlinie. Löschcodierungsregeln sollten einen erweiterten Filter verwenden, um zu verhindern, dass kleinere Objekte löschcodiert werden.

- Im Allgemeinen sollte die Standardregel Objekte dauerhaft aufbewahren.
- Wenn Sie die globale S3 Object Lock-Einstellung verwenden (oder deren Aktivierung planen), muss die Standardregel konform sein.

Schritte

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

   Schritt 1 (Details eingeben) des Assistenten zum Erstellen einer ILM-Regel wird angezeigt.

3. Geben Sie im Feld **Rule name** einen eindeutigen Namen für die Regel ein.
4. Optional kann im Feld **Beschreibung** eine kurze Beschreibung der Regel eingegeben werden.
5. Das Feld **Mieterkonten** bleibt leer.

   Die Standardregel muss für alle Mandantenkonten gelten.

6. Die Auswahl im Dropdown-Menü „Bucket-Name“ bleibt auf **gilt für alle Buckets** eingestellt.

   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. Keine erweiterten Filter hinzufügen.

   Die Standardregel kann keine Filter angeben.

9. **Weiter** auswählen.

   Schritt 2 (Platzierungen definieren) wird angezeigt.

10. Für die Referenzzeit kann jede Option ausgewählt werden.

    Wenn Sie die Standardantwort „Nein“ bei der Frage „Diese Regel nur auf ältere Objektversionen anwenden?“ beibehalten haben, wird die nicht aktuelle Zeit nicht in der Auswahlliste angezeigt. Die Standardregel muss für alle Objektversionen gelten.

11. Geben Sie die Platzierungsanweisungen für die Standardregel an.
    - Die Standardregel sollte Objekte dauerhaft speichern. Beim Aktivieren einer neuen Richtlinie erscheint eine Warnung, wenn die Standardregel Objekte nicht dauerhaft speichert. Es muss bestätigt werden, dass dies das erwartete Verhalten ist.
    - Die Standardregel sollte replizierte Kopien erstellen.

      > Es sollte keine Regel, die löschcodierte Kopien erstellt, als Standardregel für eine Richtlinie verwendet werden. Löschcodierungsregeln sollten den erweiterten Filter **Objektgröße (MB) größer als 200 KB** enthalten, um zu verhindern, dass kleinere Objekte löschcodiert werden.

    - Wenn Sie die globale S3 Object Lock-Einstellung verwenden (oder deren Aktivierung planen), muss die Standardregel konform sein:
      - Mindestens zwei replizierte Objektkopien oder eine löschcodierte Kopie müssen erstellt werden.
      - Diese Kopien müssen für die gesamte Dauer jeder Zeile in den Platzierungsanweisungen auf den Storage Nodes vorhanden sein.
      - Objektkopien können nicht in einem Cloud Storage Pool gespeichert werden.
      - Mindestens eine Zeile der Platzierungsanweisungen muss am Tag 0 beginnen, wobei die Ingest-Zeit als Referenzzeit dient.
      - Mindestens eine Zeile der Platzierungsanweisungen muss „forever“ lauten.
12. Das Retentionsdiagramm gibt Aufschluss darüber, ob die Platzierungsanweisungen korrekt sind.
13. Wählen Sie **Weiter**.

    Schritt 3 (Aufnahmeverhalten auswählen) erscheint.

14. Die gewünschte Aufnahmeoption auswählen und **Erstellen** auswählen.

ILM Richtlinien verwalten

Erfahren Sie mehr über ILM-Richtlinien in StorageGRID

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

> Eine fehlerhaft konfigurierte ILM-Richtlinie kann zu unwiederbringlichem Datenverlust führen. Vor der Aktivierung einer ILM-Richtlinie empfiehlt sich eine sorgfältige Überprüfung der ILM-Richtlinie und ihrer ILM-Regeln, anschließend sollte die ILM-Richtlinie simuliert werden. Es sollte stets bestätigt werden, dass die ILM-Richtlinie wie beabsichtigt funktioniert.

Standard ILM-Richtlinie

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

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

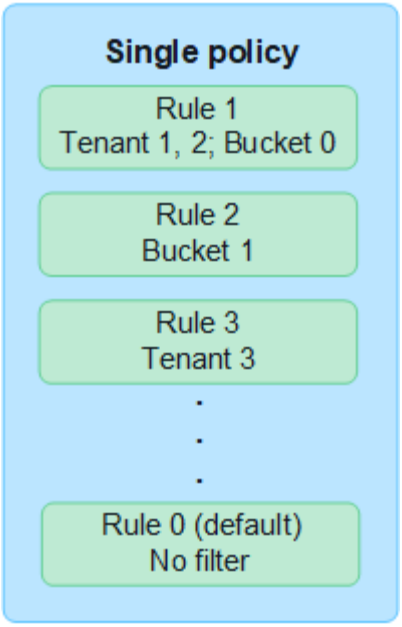
Falls die Standardrichtlinie Ihre Speicheranforderungen nicht erfüllt, können Sie eigene Regeln und Richtlinien erstellen. Siehe "Eine ILM-Regel erstellen" und "Eine ILM-Richtlinie erstellen".

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, genügt eine einzige aktive ILM-Richtlinie. Die ILM-Regeln können Filter zur Verwaltung verschiedener Buckets oder Mandanten enthalten.



Wenn nur eine Richtlinie vorhanden ist und sich die Anforderungen eines Mandanten ändern, ist eine neue ILM-Richtlinie zu erstellen oder die bestehende Richtlinie zu klonen, um Änderungen anzuwenden, zu simulieren und anschließend die neue ILM-Richtlinie zu aktivieren. Änderungen an der ILM-Richtlinie können zu Objektverschiebungen führen, die mehrere Tage in Anspruch nehmen und Systemlatenz verursachen können.

Mehrere Richtlinien

Um Mandanten unterschiedliche Servicequalitätsoptionen anzubieten, können mehrere aktive Richtlinien gleichzeitig verwendet werden. Jede Richtlinie kann bestimmte Mandanten, S3-Buckets und Objekte verwalten. Wenn eine Richtlinie für eine bestimmte Gruppe von Mandanten oder Objekten angewendet oder geändert wird, bleiben die für andere Mandanten und Objekte geltenden Richtlinien davon unberührt.

ILM Policy-Tags

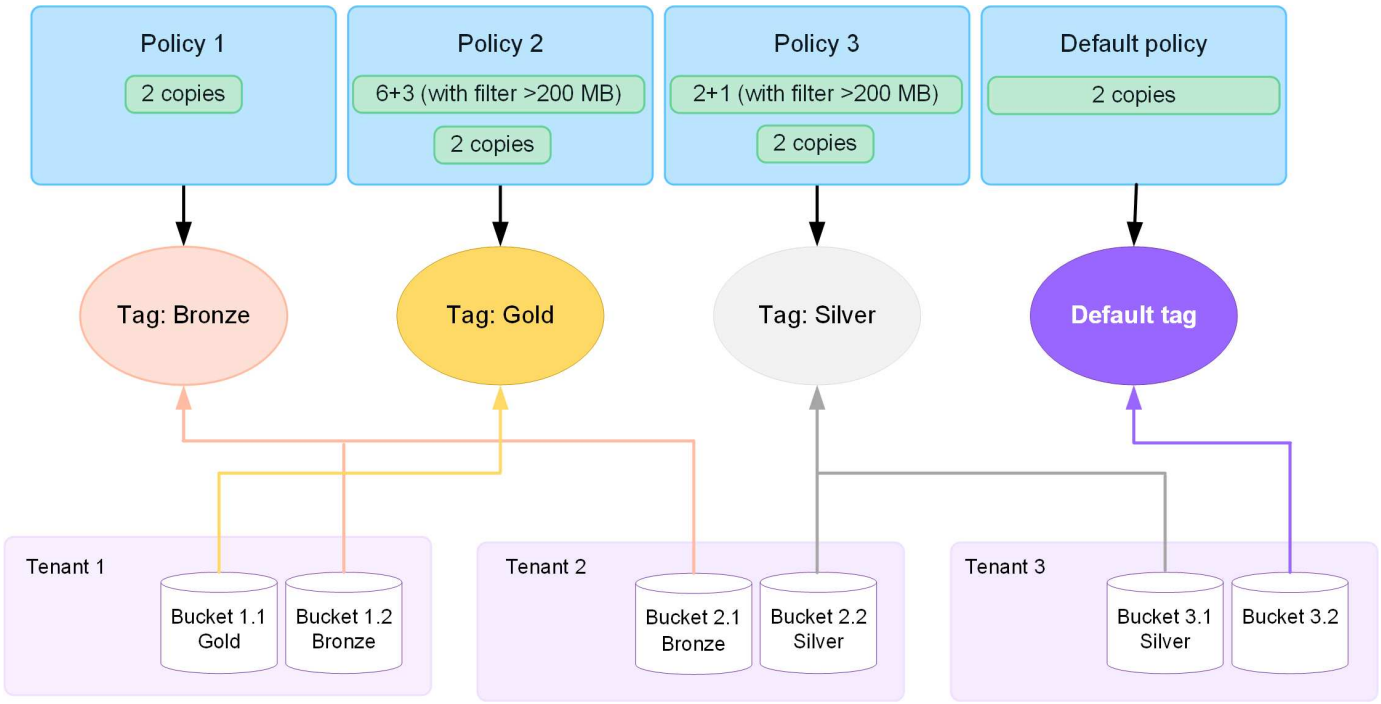
Wenn Mandanten die Möglichkeit erhalten sollen, einfach zwischen mehreren Datenschutzrichtlinien auf Bucket-Basis zu wechseln, werden mehrere ILM-Richtlinien mit *ILM policy tags* verwendet. Jeder ILM-Richtlinie wird ein Tag zugewiesen, anschließend versehen Mandanten einen Bucket mit einem Tag, um die Richtlinie auf diesen Bucket anzuwenden. ILM policy tags können nur für S3 Buckets festgelegt werden.

Beispielsweise könnten Sie drei Tags mit den Namen Gold, Silber und Bronze haben. Jedem Tag kann eine ILM-Richtlinie zugewiesen werden, basierend darauf, wie lange und wo diese Richtlinie Objekte speichert. Mandanten können auswählen, welche Richtlinie verwendet wird, indem sie ihre Buckets taggen. Ein Bucket mit dem Tag Gold wird durch die Gold-Richtlinie verwaltet und erhält das Gold-Niveau an Datenschutz und Leistung.

Sie können "Es können maximal 10 Policy-Tags erstellt werden." für Ihr Grid verwenden.

Standardmäßiges ILM Richtlinien-Tag

Ein Standard-ILM-Policy-Tag wird automatisch erstellt, wenn Sie StorageGRID installieren. Jedes Grid muss über eine aktive Richtlinie verfügen, die dem Default-Tag zugewiesen ist. Die Standardrichtlinie gilt für alle nicht getaggten S3-Buckets.



Wie bewertet eine ILM Richtlinie Objekte?

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

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

1. Wenn die Filter der ersten 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 der ersten Regel nicht mit dem Objekt übereinstimmen, wird das Objekt mit jeder nachfolgenden Regel in der Richtlinie verglichen, bis eine Übereinstimmung gefunden wird.
3. Wenn keine Regel auf ein Objekt zutrifft, werden das Aufnahmeverhalten und die Platzierungsanweisungen der Standardregel in der Richtlinie angewendet. Die Standardregel ist die letzte Regel in einer Richtlinie. Die Standardregel muss für alle Mandanten, alle S3-Buckets und alle Objektversionen gelten und darf keine erweiterten Filter verwenden.

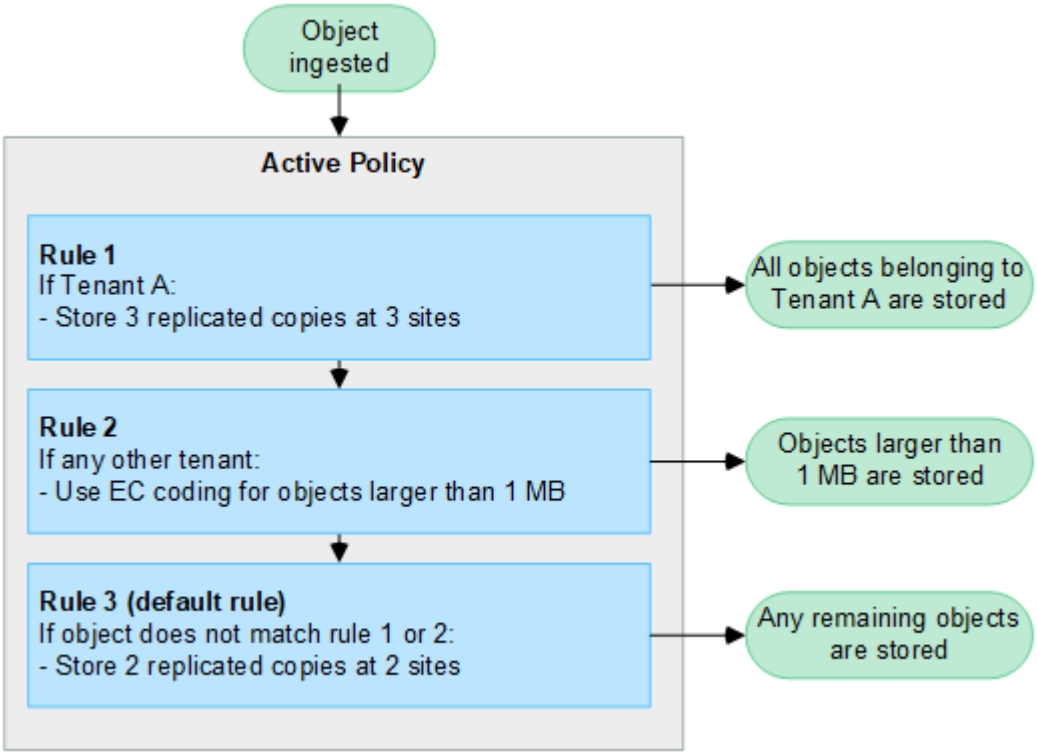
Beispiel einer ILM-Richtlinie

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

- **Regel 1: Replizierte Kopien für Mandant A**
  - Alle Objekte, die zu Tenant A gehören, abgleichen.
  - Diese Objekte werden als drei replizierte Kopien an drei Standorten gespeichert.
  - Objekte, die anderen Mandanten gehören, werden von Regel 1 nicht erfasst, daher erfolgt die Auswertung anhand von Regel 2.
- **Regel 2: Erasure Coding für Objekte größer als 1 MB**
  - Alle Objekte anderer Mandanten werden abgeglichen, jedoch nur, wenn sie größer als 1 MB sind. Diese größeren Objekte werden mithilfe von 6+3 Erasure Coding an drei Standorten gespeichert.

- Entspricht nicht Objekten mit einer Größe von 1 MB oder kleiner, daher werden diese Objekte anhand von Regel 3 ausgewertet.

- **Regel 3: 2 Kopien 2 Rechenzentren** (Standard)
  - Dies ist die letzte und Standardregel in der Richtlinie. Verwendet keine Filter.
  - Zwei replizierte Kopien aller Objekte, die nicht von Regel 1 oder Regel 2 erfasst werden (Objekte, die nicht zu Tenant A gehören und 1 MB oder kleiner sind), werden erstellt.



Was sind aktive und inaktive Richtlinien?

Jedes StorageGRID System muss mindestens eine aktive ILM-Richtlinie haben. Wenn mehr als eine aktive ILM-Richtlinie vorhanden sein soll, werden ILM-Richtlinien-Tags erstellt und jeder Tag erhält eine Richtlinie zugewiesen. Mandanten wenden dann Tags auf S3-Buckets an. Die Standardrichtlinie gilt für alle Objekte in Buckets, denen kein Richtlinien-Tag zugewiesen ist.

Wenn eine ILM-Richtlinie erstmals erstellt wird, werden eine oder mehrere ILM-Regeln ausgewählt und in eine bestimmte Reihenfolge gebracht. Nachdem die Richtlinie simuliert wurde, um ihr Verhalten zu bestätigen, wird sie aktiviert.

Wenn eine ILM-Richtlinie aktiviert wird, verwendet StorageGRID diese Richtlinie zur Verwaltung aller Objekte, einschließlich vorhandener und neu aufgenommener Objekte. Vorhandene Objekte können an neue Speicherorte verschoben werden, wenn die ILM-Regeln der neuen Richtlinie umgesetzt werden.

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

Ein StorageGRID System verfolgt die Historie der Richtlinien, die aktiviert oder deaktiviert wurden.

Überlegungen zur Erstellung einer ILM-Richtlinie

- In Testsystemen ausschließlich die systemseitig bereitgestellte Richtlinie Baseline 2 copies policy

verwenden. Bei StorageGRID 11.6 und früher verwendet die Regel Make 2 Copies in dieser Richtlinie den Speicherpool All Storage Nodes, der alle Sites enthält. Wenn das StorageGRID System über mehr als einen Standort verfügt, könnten zwei Kopien eines Objekts am selben Standort abgelegt werden.

> Der Speicherpool „All Storage Nodes“ wird während der Installation von StorageGRID 11.6 und früher automatisch erstellt. Wenn Sie auf eine spätere Version von StorageGRID aktualisieren, bleibt der Pool „All Storage Nodes“ weiterhin bestehen. Wenn StorageGRID 11.7 oder neuer als Neuinstallation installiert wird, wird der Pool „All Storage Nodes“ nicht erstellt.

- Bei der Entwicklung einer neuen Richtlinie sind alle verschiedenen Objekttypen zu berücksichtigen, die in Ihr Grid aufgenommen werden könnten. Die Richtlinie sollte Regeln enthalten, um diese Objekte zuzuordnen und entsprechend zu platzieren.
- Die ILM-Richtlinie sollte so einfach wie möglich gehalten werden. Dadurch werden potenziell gefährliche Situationen vermieden, in denen Objektdaten bei Änderungen am StorageGRID System im Laufe der Zeit nicht wie vorgesehen geschützt sind.
- Stellen Sie sicher, dass die Regeln in der Richtlinie in der richtigen Reihenfolge vorliegen. Nach der Aktivierung der Richtlinie werden neue und bestehende Objekte anhand der Regeln in der angegebenen Reihenfolge, beginnend oben, ausgewertet. Wenn beispielsweise die erste Regel in einer Richtlinie auf ein Objekt zutrifft, wird dieses Objekt von keiner weiteren 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 zugeordnet wurde, legt die Standardregel fest, wo dieses Objekt abgelegt wird und wie lange es aufbewahrt wird.
- Bevor eine neue Richtlinie aktiviert wird, sollten alle Änderungen überprüft werden, die diese Richtlinie an der Platzierung vorhandener Objekte vornimmt. Eine Änderung des Standorts eines vorhandenen Objekts kann zu vorübergehenden Ressourcenproblemen führen, wenn die neuen Platzierungen ausgewertet und implementiert werden.

Erstellen Sie ILM-Richtlinien in StorageGRID

Eine oder mehrere ILM Richtlinien können erstellt werden, um die Anforderungen an die Servicequalität zu erfüllen.

Eine einzige aktive ILM-Richtlinie ermöglicht die Anwendung derselben ILM-Regeln auf alle Mandanten und Buckets.

Mehrere aktive ILM-Richtlinien ermöglichen die Anwendung der passenden ILM-Regeln auf bestimmte Mandanten und Buckets, sodass verschiedene Quality-of-Service-Anforderungen erfüllt werden können.

Eine ILM-Richtlinie erstellen

Über diese Aufgabe

Bevor Sie Ihre eigene Richtlinie erstellen, vergewissern Sie sich, dass die "Standard ILM-Richtlinie" nicht Ihren Speicheranforderungen entspricht.

> In Testsystemen sollten ausschließlich die systemseitig bereitgestellten Richtlinien 2 copies Policy (für Ein-Standort-Grids) oder 1 Copy per Site (für Multi-Site-Grids) verwendet werden. Für StorageGRID 11.6 und früher verwendet die Standardregel in dieser Richtlinie den All Storage Nodes Speicherpool, der alle Standorte enthält. Wenn Ihr StorageGRID System mehr als einen Standort hat, können zwei Kopien eines Objekts am selben Standort abgelegt werden.

Falls "Die globale S3 Object Lock Einstellung wurde aktiviert." müssen Sie sicherstellen, dass die ILM-Richtlinie den Anforderungen von Buckets mit aktiviertem S3 Object Lock entspricht. In diesem Abschnitt sind die Anweisungen zu beachten, die die Aktivierung von S3 Object Lock erwähnen.

Bevor Sie beginnen

- Sie sind mit einem "unterstützte Webbrowser" beim Grid Manager angemeldet.
- Sie haben die "Erforderliche Zugriffsberechtigungen".
- Sie haben "erstellte ILM Regeln" abhängig davon, ob S3 Object Lock aktiviert ist.

  S3 Object Lock nicht aktiviert

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

  S3 Object Lock aktiviert

  - Das "Globale S3 Object Lock-Einstellung ist bereits aktiviert" für das StorageGRID System.
  - Sie haben "die konformen und nicht konformen ILM-Regeln erstellt" die Sie der Richtlinie hinzufügen möchten. Bei Bedarf können Sie eine Richtlinie speichern, zusätzliche Regeln erstellen und die Richtlinie anschließend bearbeiten, um die neuen Regeln hinzuzufügen.
  - Sie haben "Eine Standard-ILM-Regel wurde erstellt" für die Richtlinie, die konform ist.

- Optional haben Sie sich das Video angesehen:

Überblick über ILM-Richtlinien

Siehe auch "ILM Richtlinien verwenden".

Schritte

1. **ILM** > **Richtlinien** auswählen.

   Wenn die globale S3 Object Lock-Einstellung aktiviert ist, zeigt die ILM-Richtlinienseite an, welche ILM-Regeln konform sind.

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

   Neue Richtlinie erstellen

   a. **Richtlinie erstellen** auswählen.

   Vorhandene Richtlinie klonen

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

   Bestehende Richtlinie bearbeiten

   a. Wenn eine Richtlinie inaktiv ist, kann sie bearbeitet werden. Das Kontrollkästchen der inaktiven Richtlinie, mit der begonnen werden soll, auswählen und anschließend **Bearbeiten** wählen.

3. Im Feld **Richtlinienname** einen eindeutigen Namen für die Richtlinie eingeben.
4. Optional kann im Feld **Grund für die Änderung** der Grund für die Erstellung einer neuen Richtlinie eingetragen werden.
5. Um der Richtlinie Regeln hinzuzufügen, **Regeln auswählen** auswählen. Einen Regelnamen auswählen, um die Einstellungen für diese Regel anzuzeigen.

   Wenn Sie eine Richtlinie klonen:

   - Die Regeln, die von der Richtlinie, die Sie klonen, verwendet werden, sind ausgewählt.
   - Falls die Richtlinie, die Sie klonen, Regeln ohne Filter verwendet hat, die nicht die Standardregel waren, erfolgt eine Aufforderung, alle bis auf eine dieser Regeln zu entfernen.
   - Wenn die Standardregel einen Filter verwendet hat, erscheint eine Aufforderung, eine neue Standardregel auszuwählen.
   - Wenn die Standardregel nicht die letzte Regel war, kann die Regel an das Ende der neuen Richtlinie verschoben werden.

S3 Object Lock nicht aktiviert

a. Wählen Sie eine Standardregel für die Richtlinie aus. Zum Erstellen einer neuen Standardregel die **ILM rules page** auswählen.

   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.

   > Die Regel „Zwei Kopien erstellen“ sollte nicht als Standardregel für eine Richtlinie verwendet werden. Die Regel „Zwei Kopien erstellen“ verwendet einen einzelnen Speicherpool, „Alle Speicherknoten“, der alle Standorte enthält. Wenn Ihr StorageGRID System mehr als einen Standort hat, könnten zwei Kopien eines Objekts am selben Standort abgelegt werden.

S3 Object Lock aktiviert

a. Wählen Sie eine Standardregel für die Richtlinie aus. Zum Erstellen einer neuen Standardregel die **ILM rules page** auswählen.

   Die Liste der Regeln enthält nur die konformen Regeln und verwendet keine Filter.

   > Verwenden Sie die Regel „Make 2 Copies“ nicht als Standardregel für eine Richtlinie. Die Regel „Make 2 Copies“ verwendet einen einzigen Speicherpool, All Storage Nodes, der alle Standorte enthält. Wenn Sie diese Regel verwenden, können mehrere Kopien eines Objekts am selben Standort abgelegt werden.

b. Wenn eine andere "Standard"-Regel für Objekte in nicht konformen S3-Buckets erforderlich ist, **Regel ohne Filter für nicht konforme S3-Buckets einbeziehen** auswählen und eine nicht konforme Regel auswählen, die keinen Filter verwendet.

   Beispielsweise könnte ein Cloud Storage Pool verwendet werden, um Objekte in Buckets zu speichern, bei denen 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. Nachdem Sie die Standardregel ausgewählt haben, auf **Weiter** klicken.
7. Im Schritt „Weitere Regeln“ können alle weiteren Regeln ausgewählt werden, die der Richtlinie hinzugefügt werden sollen. Diese Regeln verwenden mindestens einen Filter (Mandantenkonto, Bucket Name, erweiterter Filter oder Noncurrent Referenzzeitpunkt). Anschließend **Auswählen** auswählen.

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

   Wenn S3 Object Lock aktiviert ist und außerdem eine nicht konforme „default“-Regel ausgewählt wurde, wird diese Regel als vorletzte Regel in die Richtlinie aufgenommen.

Eine Warnung wird angezeigt, wenn eine Regel Objekte nicht dauerhaft speichert. Beim Aktivieren dieser Richtlinie ist zu bestätigen, dass StorageGRID Objekte löscht, wenn die Platzierungsanweisungen der Standardregel abgelaufen sind (es sei denn, ein Bucket-Lebenszyklus bewahrt die Objekte für einen längeren Zeitraum auf).

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

   Die Standardregel kann nicht verschoben werden. Wenn S3 Object Lock aktiviert ist, kann auch die nicht konforme „default“-Regel nicht verschoben werden, falls eine ausgewählt wurde.

   Sie müssen bestätigen, dass die ILM-Regeln in der richtigen Reihenfolge sind. Bei der Aktivierung der Richtlinie werden neue und bestehende Objekte von oben beginnend in der aufgelisteten Reihenfolge durch die Regeln ausgewertet.

9. Bei Bedarf kann **Regeln auswählen** ausgewählt werden, um Regeln hinzuzufügen oder zu entfernen.
10. Wenn Sie fertig sind, **Speichern** auswählen.
11. Diese Schritte werden wiederholt, um zusätzliche ILM-Richtlinien zu erstellen.
12. Eine ILM-Richtlinie simulieren. Eine Richtlinie sollte immer simuliert werden, bevor sie aktiviert wird, um sicherzustellen, dass sie wie erwartet funktioniert.

Eine Richtlinie simulieren

Eine Richtlinie kann an Testobjekten simuliert werden, bevor sie aktiviert und auf Ihre Produktionsdaten angewendet wird.

Bevor Sie beginnen

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

Schritte

1. Mit einem S3-Client oder dem "S3 Konsole" können die für den Test jeder Regel erforderlichen Objekte ingestiert werden.
2. Auf der Seite „ILM-Richtlinien“ das Kontrollkästchen für die Richtlinie auswählen und dann **Simulieren** auswählen.
3. Im Feld **Objekt** die S3 `bucket/object-key` für ein Testobjekt eingeben. Zum Beispiel `bucket-01/filename.png`.
4. Wenn die S3-Versionierung aktiviert ist, kann optional eine Versions-ID für das Objekt im Feld **Versions-ID** eingegeben werden.
5. **Simulieren** auswählen.
6. Im Abschnitt „Simulationsergebnisse“ ist zu bestätigen, dass jedes Objekt der richtigen Regel zugeordnet wurde.
7. Zur Feststellung, welcher Speicherpool oder welches Erasure-Coding-Profil aktiv ist, den Namen der übereinstimmenden Regel auswählen, um zur Seite mit den Regeldetails zu gelangen.

Alle Änderungen an der Platzierung bestehender replizierter und per Erasure-Coding gesicherter Objekte überprüfen. Eine Änderung des Speicherorts eines bestehenden Objekts kann zu vorübergehenden Ressourcenproblemen führen, wenn die neuen Platzierungen bewertet und implementiert werden.

Ergebnisse

Änderungen an den Richtlinienregeln werden in den Simulationsergebnissen angezeigt und zeigen die neue und die vorherige Übereinstimmung an. Das Fenster „Richtlinie simulieren“ behält die getesteten Objekte bei, bis entweder **Alle löschen** oder das Entfernungssymbol ✕ für jedes Objekt in der Liste der Simulationsergebnisse ausgewählt wird.

Verwandte Informationen

"Beispielhafte ILM-Policy-Simulationen"

Eine Richtlinie aktivieren

Wenn eine einzelne neue ILM-Richtlinie aktiviert wird, werden sowohl vorhandene als auch neu importierte Objekte von dieser Richtlinie verwaltet. Wenn mehrere Richtlinien aktiviert werden, bestimmen die den Buckets zugewiesenen ILM-Policy-Tags, welche Objekte verwaltet werden.

Bevor Sie eine neue Richtlinie aktivieren:

1. Die Richtlinie kann simuliert werden, um zu bestätigen, dass sie sich wie erwartet verhält.
2. Alle Änderungen an der Platzierung bestehender replizierter und per Erasure-Coding gesicherter Objekte überprüfen. Eine Änderung des Speicherorts eines bestehenden Objekts kann zu vorübergehenden Ressourcenproblemen führen, wenn die neuen Platzierungen bewertet und implementiert werden.

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

Über diese Aufgabe

Wenn eine ILM-Richtlinie aktiviert wird, verteilt das System die neue Richtlinie an alle Knoten. Die neue aktive Richtlinie tritt jedoch möglicherweise erst in Kraft, wenn alle Grid-Knoten verfügbar sind, um die neue Richtlinie zu empfangen. In einigen Fällen wartet das System mit der Umsetzung einer neuen aktiven Richtlinie, um sicherzustellen, dass Grid-Objekte nicht versehentlich entfernt werden. Konkret:

- Wenn Richtlinienänderungen vorgenommen werden, die die Datenredundanz oder -haltbarkeit erhöhen, werden diese Änderungen sofort umgesetzt. Wenn beispielsweise eine neue Richtlinie aktiviert wird, die eine Drei-Kopien-Regel anstelle einer Zwei-Kopien-Regel enthält, wird diese Richtlinie sofort umgesetzt, da sie die Datenredundanz erhöht.
- Wenn Richtlinienänderungen vorgenommen werden, die die Datenredundanz oder Haltbarkeit verringern könnten, werden diese Änderungen erst umgesetzt, wenn alle Grid-Knoten verfügbar sind. Beispielsweise erscheint eine neue Richtlinie, die eine Zwei-Kopien-Regel anstelle einer Drei-Kopien-Regel verwendet, zwar auf der Registerkarte Active policy, tritt jedoch erst in Kraft, wenn alle Knoten online und verfügbar sind.

Schritte

Die folgenden Schritte dienen zur Aktivierung einer oder mehrerer Richtlinien:

Eine Richtlinie aktivieren

Führen Sie diese Schritte aus, wenn nur eine aktive Richtlinie vorhanden ist. Wenn bereits eine oder mehrere aktive Richtlinien vorhanden sind und zusätzliche Richtlinien aktiviert werden, gelten die Schritte zur Aktivierung mehrerer Richtlinien.

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

   Alternativ lässt sich eine einzelne Richtlinie auf der Seite **ILM** > **Policy tags** aktivieren.

2. Auf der Registerkarte „Richtlinien“ das Kontrollkästchen für die Richtlinie auswählen, die aktiviert werden soll, dann **Aktivieren** auswählen.
3. Führen Sie den entsprechenden Schritt aus:
   - Wenn eine Warnmeldung zur Bestätigung der Aktivierung der Richtlinie angezeigt wird, **OK** auswählen.
   - Wenn eine Warnmeldung mit Details zur Richtlinie angezeigt wird:
     i. Die Details geben Aufschluss darüber, ob die Richtlinie die Daten wie erwartet verwaltet.
     ii. Wenn die Standardregel Objekte nur für eine begrenzte Anzahl von Tagen speichert, das Aufbewahrungsdiagramm prüfen und anschließend diese Anzahl von Tagen in das Textfeld eingeben.
     iii. Wenn die Standardregel Objekte für immer speichert, aber eine oder mehrere andere Regeln eine begrenzte Aufbewahrungsdauer haben, **ja** in das Textfeld eingeben.
     iv. **Richtlinie aktivieren** auswählen.

Mehrere Richtlinien aktivieren

Um mehrere Richtlinien zu aktivieren, müssen Sie Richtlinien-Tags erstellen und jedem Tag eine Richtlinie zuweisen. Es können maximal 10 Richtlinien-Tags für Ihr Grid erstellt werden.

> Wenn mehrere Richtlinientags verwendet werden, kann die Grid-Performance beeinträchtigt werden, wenn Mandanten Richtlinientags häufig Buckets neu zuweisen. Bei nicht vertrauenswürdigen Mandanten sollte in Erwägung gezogen werden, ausschließlich den Default-Richtlinientag zu verwenden.

1. Wählen Sie **ILM** > **Policy-Tags**.
2. Wählen Sie **Create**.
3. Im Dialogfeld „Richtlinientag erstellen“ einen Tag-Namen und optional eine Beschreibung für den Tag eingeben.

   > Tag-Namen und Beschreibungen sind für Mandanten sichtbar. Werte, die Mandanten helfen, eine fundierte Entscheidung bei der Auswahl von Richtlinien-Tags für ihre Buckets zu treffen, sind auszuwählen. Wenn die zugewiesene Richtlinie beispielsweise Objekte nach einer bestimmten Zeit löscht, kann dies in der Beschreibung kommuniziert werden. In diesen Feldern sollten keine sensiblen Informationen enthalten sein.

4. **Tag erstellen** auswählen.
5. In der ILM-Richtlinien-Tag-Tabelle kann mithilfe des Dropdown-Menüs eine Richtlinie ausgewählt werden, die dem Tag zugewiesen wird.

6. Wenn in der Spalte „Richtlinienbeschränkungen“ Warnungen angezeigt werden, kann **Richtliniendetails anzeigen** ausgewählt werden, um die Richtlinie zu überprüfen.
7. Es wird sichergestellt, dass jede Richtlinie die Daten wie erwartet verwaltet.
8. **Zugewiesene Richtlinien aktivieren** auswählen. Alternativ kann **Änderungen löschen** ausgewählt werden, um die Richtlinienzuordnung zu entfernen.
9. Im Dialogfeld „Richtlinien mit neuen Tags aktivieren“ werden die Beschreibungen angezeigt, wie die einzelnen Tags, Richtlinien und Regeln Objekte verwalten. Änderungen können vorgenommen werden, um sicherzustellen, dass die Richtlinien 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**.

Verwandte Informationen

"Beispiel 6: Ändern einer ILM-Richtlinie"

Beispiel-ILM-Policy-Simulationen in StorageGRID

Die Beispiele für ILM Policy-Simulationen liefern Richtlinien für die Strukturierung und Modifizierung von Simulationen für Ihre Umgebung.

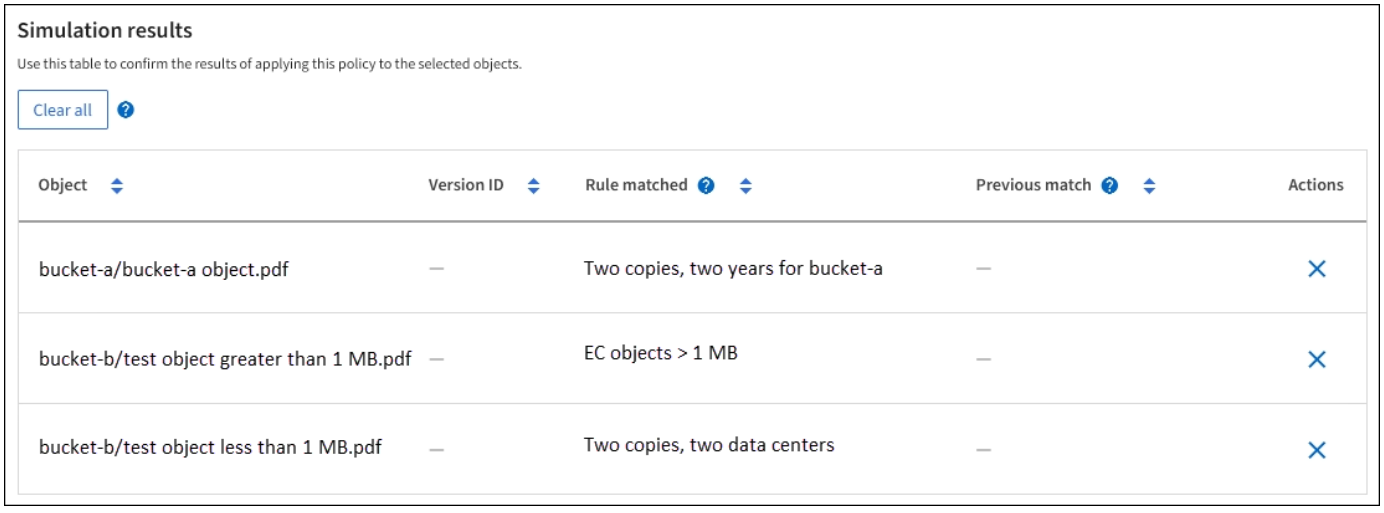
Beispiel 1: Regeln beim Simulieren einer ILM-Richtlinie überprüfen

Dieses Beispiel beschreibt, wie Regeln beim Simulieren einer Richtlinie überprüft werden können.

In diesem Beispiel wird die **Beispiel-ILM-Richtlinie** anhand der in zwei Buckets aufgenommenen Objekte simuliert. Die Richtlinie umfasst 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. Sie enthält keine Filter und verwendet nicht die Noncurrent-Referenzzeit.

Nach der Simulation der Richtlinie sollte bestätigt werden, dass jedes Objekt der richtigen Regel zugeordnet wurde.



In diesem Beispiel:

- `bucket-a/bucket-a object.pdf`hat die erste Regel, die auf Objekte in `bucket-a`filtert, korrekt erfüllt.
- `bucket-b/test object greater than 1 MB.pdf` befindet sich in `bucket-b`, daher traf die erste Regel nicht zu. Stattdessen wurde es korrekt von der zweiten Regel erfasst, die Objekte mit einer Größe von mehr als 1 MB filtert.
- `bucket-b/test object less than 1 MB.pdf` entsprach nicht den Filtern in den ersten beiden Regeln, daher erfolgt die Platzierung durch die Standardregel, die keine Filter enthält.

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

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

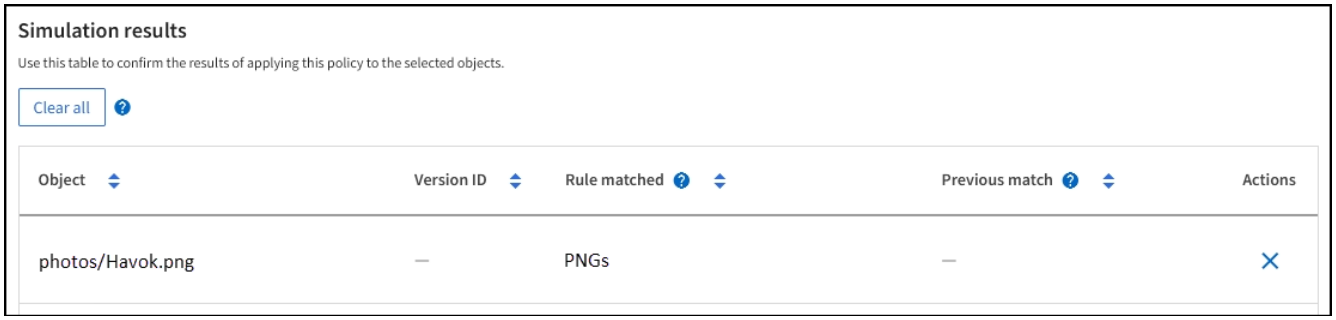
In diesem Beispiel wird die **Demo**-Richtlinie simuliert. Diese Richtlinie, die dazu dient, Objekte mit den Benutzermetadaten series=x-men zu finden, umfasst drei Regeln:

- Die erste Regel, **PNGs**, filtert nach Schlüsselnamen, die mit `.png` enden.
- Die zweite Regel, **X-men**, gilt nur für Objekte für Mandant A und Filter für `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 die Regeln hinzugefügt und die Richtlinie gespeichert wurden, **Simulieren** auswählen.
2. Im Feld **Objekt** den S3-Bucket/Objektschlüssel für ein Testobjekt eingeben und **Simulieren** auswählen.

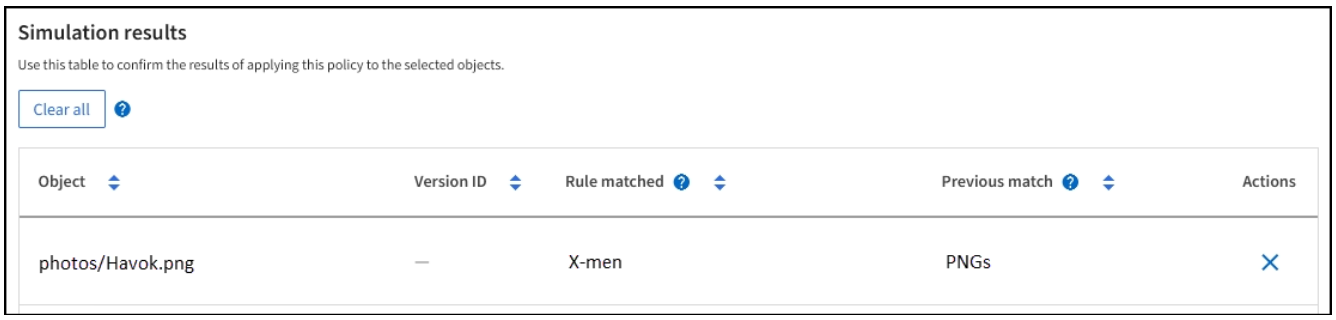
   Die Simulationsergebnisse werden angezeigt und zeigen, dass das `Havok.png` Objekt der **PNGs**-Regel zugeordnet wurde.



   Jedoch, `Havok.png` sollte die **X-men**-Regel getestet werden.

3. Zur Behebung des Problems empfiehlt sich eine Neuordnung der Regeln.
   a. **Fertigstellen** auswählen, um das Fenster „ILM-Richtlinie simulieren“ zu schließen.
   b. **Bearbeiten** auswählen, um die Richtlinie zu bearbeiten.
   c. Die **X-men**-Regel befindet sich nun ganz oben in der Liste.
   d. **Speichern** auswählen.
4. **Simulieren** auswählen.

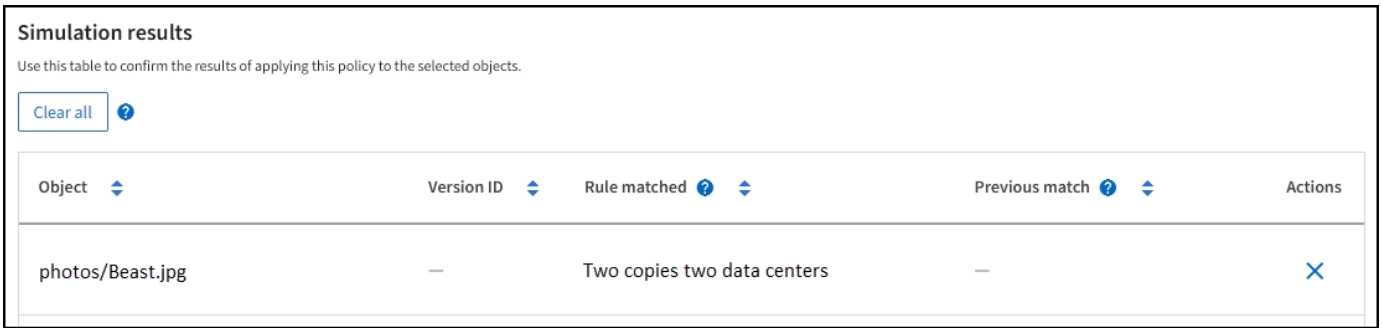
Die zuvor getesteten Objekte werden anhand der aktualisierten Richtlinie erneut ausgewertet, und die neuen Simulationsergebnisse werden angezeigt. Im Beispiel zeigt die Spalte „Regelübereinstimmung“, dass das `Havok.png` Objekt nun wie erwartet der X-men Metadatenregel entspricht. Die Spalte „Vorherige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



Beispiel 3: Eine Regel bei der Simulation einer ILM-Richtlinie korrigieren

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

In diesem Beispiel wird die **Demo**-Richtlinie simuliert. Diese Richtlinie soll Objekte finden, die `series=x-men` Benutzermetadaten haben. Unerwartete Ergebnisse traten jedoch auf, als diese Richtlinie gegen das `Beast.jpg` Objekt simuliert wurde. Statt der X-men-Metadatenregel entsprach das Objekt der Standardregel Zwei Kopien zwei Rechenzentren.



Wenn ein Testobjekt nicht mit der erwarteten Regel in der Richtlinie übereinstimmt, ist es erforderlich, jede Regel in der Richtlinie zu überprüfen und eventuelle Fehler zu korrigieren.

Schritte

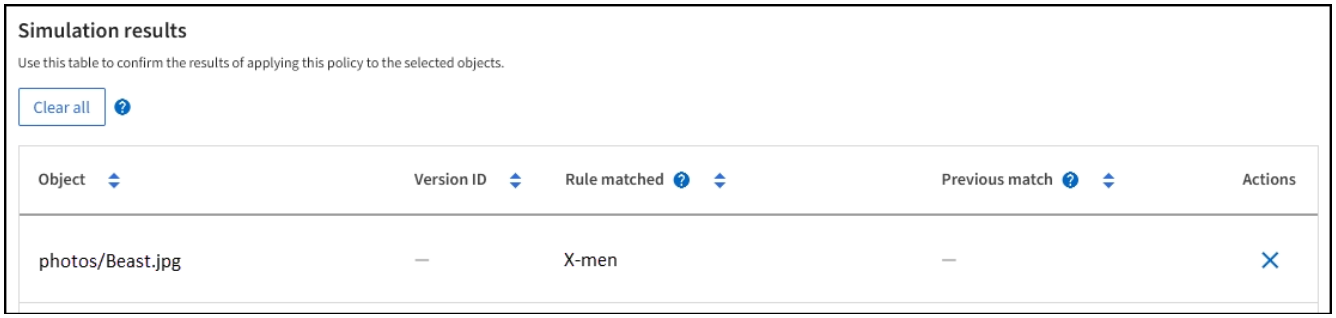
1. **Fertigstellen** auswählen, um das Dialogfeld „Simulate policy“ zu schließen. Auf der Detailseite der Richtlinie **Retention diagram** auswählen. Dann für jede Regel nach Bedarf **Expand all** oder **View details** auswählen.
2. Das Mandantenkonto, der Bezugszeitpunkt und die Filterkriterien der Regel werden angezeigt.

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

3. Zur Behebung des Fehlers sollte die Regel wie folgt korrigiert werden:
   - Wenn die Regel Teil der Richtlinie ist, kann die Regel entweder geklont oder aus der Richtlinie entfernt und anschließend bearbeitet werden.
   - Wenn die Regel Teil der aktiven Richtlinie ist, müssen Sie die Regel klonen. Sie können eine Regel nicht bearbeiten oder entfernen, wenn sie Teil der aktiven Richtlinie ist.

4. Die Simulation wird erneut durchgeführt.

   In diesem Beispiel stimmt die korrigierte X-men-Regel nun mit dem `Beast.jpg` Objekt anhand der `series=x-men` Benutzermetadaten wie erwartet überein.



ILM-Richtlinientags in StorageGRID verwalten

Sie können die Details des ILM-Policy-Tags anzeigen, ein Tag bearbeiten oder ein Tag entfernen.

Bevor Sie beginnen

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

Details des ILM-Policy-Tags anzeigen

Details eines Tags anzeigen:

1. Wählen Sie **ILM** > **Policy-Tags**.
2. Wählen Sie den Namen der Richtlinie aus der Tabelle aus. Die Detailseite für das Tag wird angezeigt.
3. Auf der Detailseite ist die bisherige Historie der zugewiesenen Policen sichtbar.
4. Eine Richtlinie wird durch Auswahl angezeigt.

ILM-Richtlinientag bearbeiten

> Tag-Namen und Beschreibungen sind für Mandanten sichtbar. Werte, die Mandanten helfen, eine fundierte Entscheidung bei der Auswahl von Richtlinien-Tags für ihre Buckets zu treffen, sind auszuwählen. Wenn die zugewiesene Richtlinie beispielsweise Objekte nach einer bestimmten Zeit löscht, kann dies in der Beschreibung kommuniziert werden. In diesen Feldern sollten keine sensiblen Informationen enthalten sein.

Die Beschreibung eines bestehenden Tags kann wie folgt bearbeitet werden:

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

   Alternativ kann der Name des Tags ausgewählt werden. Die Detailseite des Tags wird angezeigt, und dort kann **Bearbeiten** ausgewählt werden.

3. Die Tag-Beschreibung kann bei Bedarf angepasst werden.

4. **Speichern** auswählen.

ILM-Policy-Tag entfernen

Wenn ein Richtlinien-Tag entfernt wird, wird auf alle Buckets, denen dieses Tag zugewiesen ist, die Default-Richtlinie angewendet.

Ein Tag entfernen:

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

   Alternativ kann der Name des Tags ausgewählt werden. Die Detailseite des Tags wird angezeigt, und dort kann **Entfernen** ausgewählt werden.

3. **Ja** auswählen, um das Tag zu löschen.

Verwandte Informationen

"Informationen zur Erstellung von ILM Policy-Tags"

Überprüfen Sie eine ILM-Richtlinie mit Objektmetadatenabfrage in StorageGRID

Nachdem eine ILM-Richtlinie aktiviert wurde, werden repräsentative Testobjekte in das StorageGRID System importiert, anschließend erfolgt eine Objektmetadatenabfrage, um zu bestätigen, dass Kopien wie vorgesehen 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 (Universally Unique Identifier).
- **CBID**: Die eindeutige Kennung des Objekts in StorageGRID. Die CBID eines Objekts kann dem Revisionsprotokoll entnommen werden. Die CBID ist vollständig in Großbuchstaben einzugeben.
- **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. Ist der S3-Bucket versioniert und soll eine bestimmte Version eines S3-Objekts mithilfe des Bucket und Objektschlüssels nachgeschlagen werden, steht die **Version ID** zur Verfügung.

Schritte

1. Das Objekt aufnehmen.
2. **ILM** > **Objektmetadatensuche** auswählen.
3. Geben Sie die Kennung des Objekts im Feld **Kennung** ein. Es kann eine UUID, eine CBID oder ein S3-Bucket/Objektschlüssel eingegeben werden.
4. Optional kann eine Versions-ID für das Objekt eingegeben werden (nur S3).
5. **Nach oben suchen** auswählen.

   Die Ergebnisse der Objektmetadatenabfrage werden angezeigt. Diese Seite listet die folgenden Informationstypen auf:

- Systemmetadaten wie Objekt-ID (UUID), Ergebnistyp (Objekt, Löschmarkierung, S3-Bucket) und logische Größe des Objekts. Im folgenden Beispiel-Screenshot sind weitere Details ersichtlich.
- Alle benutzerdefinierten Metadaten-Schlüssel-Wert-Paare, die dem Objekt zugeordnet sind.
- Bei S3-Objekten alle Objekt-Tag-Schlüssel-Wert-Paare, die dem Objekt zugeordnet sind.
- Für replizierte Objektkopien der aktuelle Speicherort jeder Kopie.
- Für mit Erasure-Codierung versehene Objektkopien ist der aktuelle Speicherort jedes Fragments.
- Bei Objektkopien in einem Cloud-Speicherpool ist der Speicherort des Objekts, einschließlich des Namens des externen Buckets und der eindeutigen Kennung des Objekts.
- Für segmentierte Objekte und Multipart-Objekte eine Liste der Objektsegmente einschließlich Segmentkennungen und Datengrößen. Für Objekte mit mehr als 100 Segmenten werden nur die ersten 100 Segmente angezeigt.
- Alle Objektmetadaten im unverarbeiteten, internen Speicherformat. Diese Rohmetadaten enthalten interne Systemmetadaten, deren Persistenz von Version zu Version nicht garantiert werden kann.

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

   Wenn die Audit-Option aktiviert ist, kann das Revisionsprotokoll auch auf die Meldung „ORLM Object Rules Met“ überwacht werden. Die ORLM-Audit-Meldung liefert weitere Informationen zum Status des ILM-Auswertungsprozesses, jedoch keine Informationen über die Korrektheit der Platzierung der Objektdaten oder die Vollständigkeit der ILM-Richtlinie. Dies muss selbst bewertet werden. Einzelheiten finden sich unter "Audit-Protokolle prüfen".

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

> Der folgende Screenshot dient als Beispiel. Die Ergebnisse können je nach StorageGRID Version variieren.

System Metadata

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

Replicated Copies

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

Raw Metadata


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


Verwandte Informationen

"S3 REST-API verwenden"

Arbeiten mit ILM-Richtlinien und ILM-Regeln in StorageGRID

Wenn sich Ihre Speicheranforderungen ändern, kann es erforderlich sein, zusätzliche Richtlinien zu implementieren oder die mit einer Richtlinie verknüpften ILM-Regeln zu ändern. ILM-Metriken können angezeigt werden, um die Systemleistung zu bestimmen.

Bevor Sie beginnen

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

ILM-Richtlinien anzeigen

Aktive und inaktive ILM-Richtlinien sowie den Aktivierungsverlauf der Richtlinien anzeigen:

1. **ILM** > **Richtlinien** auswählen.
2. **Richtlinien** anzeigen, um eine Liste der aktiven und inaktiven Richtlinien zu sehen. Die Tabelle listet den Namen jeder Richtlinie, die Tags, denen die Richtlinie zugewiesen ist, sowie den Status (aktiv oder inaktiv) auf.
3. **Aktivierungsverlauf** zeigt eine Liste der Start- und Enddaten der Aktivierung für Richtlinien an.
4. Wählen Sie einen Policennamen aus, um die Details der Policy anzuzeigen.

> Wenn Sie die Details einer Richtlinie anzeigen, deren Status „Bearbeitet“ oder „Gelöscht“ ist, erscheint eine Meldung, die erklärt, dass Sie die Version der Richtlinie sehen, 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 eine aktive Richtlinie bearbeitet werden soll, muss sie deaktiviert oder ein Klon erstellt und dieser bearbeitet werden.

Eine Richtlinie kann wie folgt bearbeitet werden:

1. **ILM** > **Richtlinien** auswählen.
2. Wählen Sie das Kontrollkästchen für die Richtlinie aus, die Sie bearbeiten möchten, und wählen Sie dann **Bearbeiten**.
3. Die Richtlinie kann bearbeitet werden, indem den Anweisungen in "ILM-Richtlinien erstellen" gefolgt wird.
4. Die Richtlinie sollte vor der erneuten Aktivierung simuliert werden.

> Eine fehlerhaft konfigurierte ILM-Richtlinie kann zu unwiederbringlichem Datenverlust führen. Vor der Aktivierung einer ILM-Richtlinie empfiehlt sich eine sorgfältige Überprüfung der ILM-Richtlinie und ihrer ILM-Regeln, anschließend sollte die ILM-Richtlinie simuliert werden. Es sollte stets bestätigt werden, dass die ILM-Richtlinie wie beabsichtigt funktioniert.

Klonen einer ILM Richtlinie

Eine ILM-Richtlinie klonen:

1. **ILM** > **Richtlinien** auswählen.
2. Das Kontrollkästchen für die Richtlinie, die geklont werden soll, auswählen und anschließend **Klonen** wählen.
3. Erstellen Sie eine neue Richtlinie, beginnend mit der geklonten Richtlinie, indem Sie den Anweisungen in "ILM-Richtlinien erstellen" folgen.

> Eine fehlerhaft konfigurierte ILM-Richtlinie kann zu unwiederbringlichem Datenverlust führen. Vor der Aktivierung einer ILM-Richtlinie empfiehlt sich eine sorgfältige Überprüfung der ILM-Richtlinie und ihrer ILM-Regeln, anschließend sollte die ILM-Richtlinie simuliert werden. Es sollte stets bestätigt werden, dass die ILM-Richtlinie wie beabsichtigt funktioniert.

Entfernen einer ILM-Richtlinie

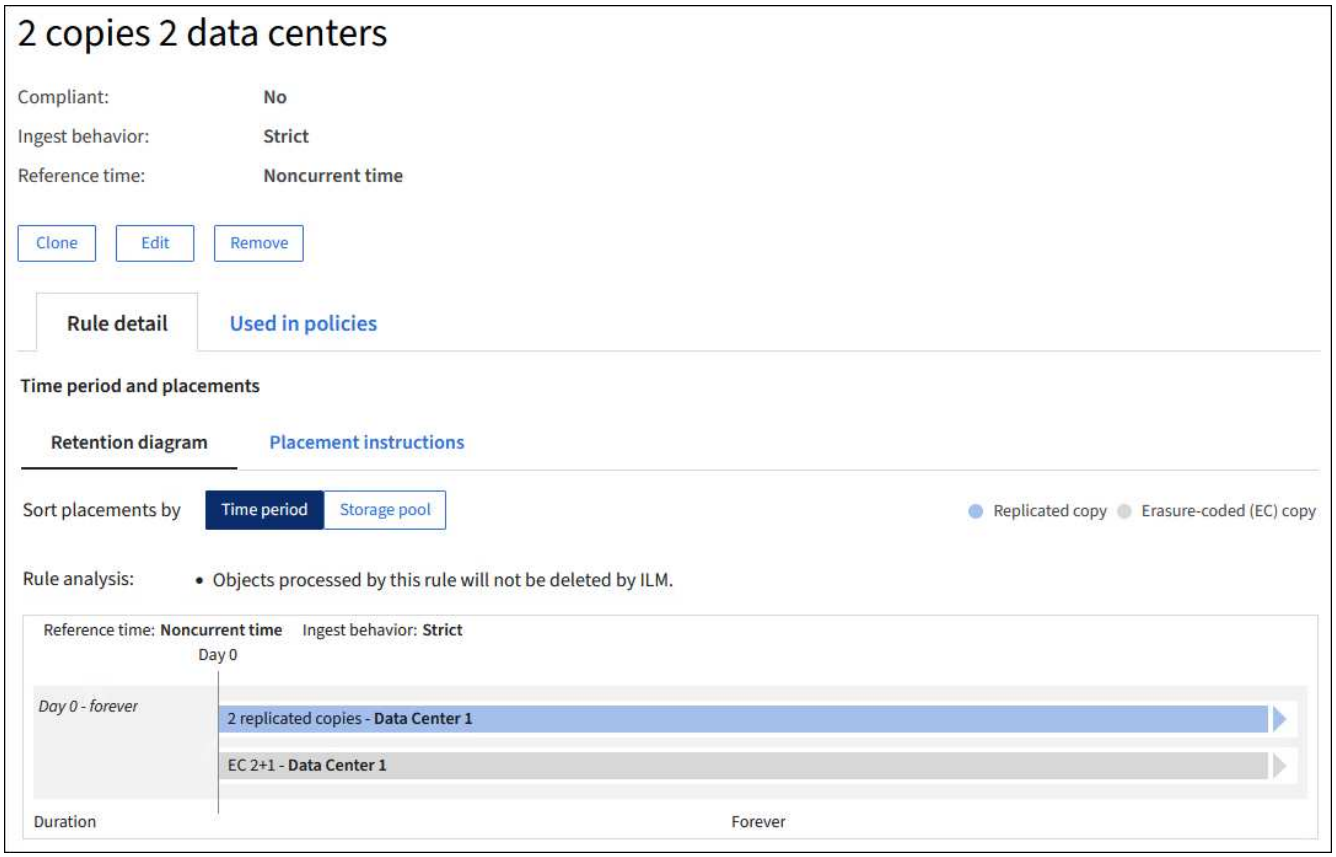
Eine ILM-Richtlinie kann nur entfernt werden, wenn sie inaktiv ist. Zum Entfernen einer Richtlinie:

1. **ILM** > **Richtlinien** auswählen.
2. Aktivieren Sie das Kontrollkästchen für die inaktive Richtlinie, die entfernt werden soll.
3. Wählen Sie **Remove**.

ILM-Regeldetails

Details einer ILM-Regel, einschließlich des Aufbewahrungsdiagramms und der Platzierungsanweisungen für die Regel, können angezeigt werden:

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



Zusätzlich kann die Detailseite verwendet werden, um eine Regel zu klonen, zu bearbeiten oder zu entfernen. Eine Regel kann nicht bearbeitet oder entfernt werden, wenn sie in einer Richtlinie verwendet wird.

Klonen einer ILM-Regel

Sie können eine bestehende Regel klonen, wenn eine neue Regel erstellt werden soll, die einige Einstellungen der bestehenden Regel verwendet. Falls eine Regel bearbeitet werden muss, die in einer Richtlinie verwendet wird, wird stattdessen die Regel geklont und Änderungen am Klon vorgenommen. Nachdem Änderungen am Klon vorgenommen wurden, kann die ursprüngliche Regel aus der Richtlinie entfernt und bei Bedarf durch die geänderte Version ersetzt werden.

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

Schritte

1. Wählen Sie **ILM** > **Regeln**.
2. Aktivieren Sie das Kontrollkästchen für die Regel, die Sie klonen möchten, und wählen Sie anschließend **Klonen** aus. Alternativ kann der Regelnamen ausgewählt und anschließend **Klonen** auf der Seite mit den Regeldetails gewählt werden.
3. Die geklonte Regel wird aktualisiert, indem die Schritte für Bearbeiten einer ILM-Regel und "Verwendung erweiterter Filter in ILM-Regeln" befolgt werden.

   Beim Klonen einer ILM Regel muss ein neuer Name eingegeben werden.

Bearbeiten einer ILM Regel

Es kann erforderlich sein, eine ILM-Regel zu bearbeiten, um einen Filter oder eine Platzierungsanweisung zu ändern.

Eine Regel kann nicht bearbeitet werden, wenn sie in einer ILM-Richtlinie verwendet wird. Stattdessen besteht die Möglichkeit, Die Regel klonen und alle erforderlichen Änderungen an der geklonten Kopie vorzunehmen.

Eine fehlerhaft konfigurierte ILM-Richtlinie kann zu unwiederbringlichem Datenverlust führen. Vor der Aktivierung einer ILM-Richtlinie empfiehlt sich eine sorgfältige Überprüfung der ILM-Richtlinie und ihrer ILM-Regeln, anschließend sollte die ILM-Richtlinie simuliert werden. Es sollte stets bestätigt werden, dass die ILM-Richtlinie wie beabsichtigt funktioniert.

Schritte

1. Wählen Sie **ILM** > **Regeln**.
2. Bestätigen Sie, dass die Regel, die Sie bearbeiten möchten, in keiner ILM-Richtlinie verwendet wird.
3. Wenn die zu bearbeitende Regel nicht verwendet wird, das Kontrollkästchen der Regel auswählen und **Aktionen** > **Bearbeiten** wählen. Alternativ den Namen der Regel auswählen und dann auf der Detailseite der Regel **Bearbeiten** wählen.
4. Führen Sie die Schritte des Assistenten zum Bearbeiten der ILM-Regel vollständig aus. Gegebenenfalls sind die Schritte für "Erstellen einer ILM Regel" und "Verwendung erweiterter Filter in ILM-Regeln" zu beachten.

   Beim Bearbeiten einer ILM-Regel kann deren Name nicht geändert werden.

Eine ILM-Regel entfernen

Um die Liste der aktuellen ILM-Regeln übersichtlich zu halten, sollten ILM-Regeln entfernt werden, die voraussichtlich nicht verwendet werden.

Schritte

Eine ILM-Regel, die aktuell in einer aktiven Richtlinie verwendet wird, kann wie folgt entfernt werden:

1. Die Richtlinie klonen.
2. Die ILM-Regel aus dem Richtlinienklon entfernen.

3. Die neue Richtlinie kann gespeichert, simuliert und aktiviert werden, sodass Objekte wie erwartet geschützt sind.
4. Wechseln Sie zu den Schritten zum Entfernen einer ILM-Regel, die derzeit in einer inaktiven Richtlinie verwendet wird.

Eine ILM-Regel, die derzeit in einer inaktiven Richtlinie verwendet wird, kann wie folgt entfernt werden:

1. Wählen Sie die inaktive Richtlinie aus.
2. Entfernen Sie die ILM-Regel aus der Richtlinie oder die Richtlinie entfernen.
3. Zu den Schritten für das Entfernen einer ILM-Regel, die derzeit nicht verwendet wird.

Eine ILM-Regel, die derzeit nicht verwendet wird, kann entfernt werden:

1. Wählen Sie **ILM** > **Regeln**.
2. Bestätigen Sie, dass die Regel, die Sie entfernen möchten, in keiner Richtlinie verwendet wird.
3. Wenn die zu entfernende Regel nicht verwendet wird, kann die Regel ausgewählt und über **Aktionen** > **Entfernen** entfernt werden. Es ist möglich, mehrere Regeln auszuwählen und alle gleichzeitig zu entfernen.
4. **Ja** auswählen, um zu bestätigen, dass die ILM-Regel entfernt werden soll.

ILM-Metriken anzeigen

Sie können Kennzahlen für ILM einsehen, z. B. die Anzahl der Objekte in der Warteschlange und die Auswertungsrate. Anhand dieser Kennzahlen lässt sich die Systemleistung ermitteln. Eine große Warteschlange oder eine hohe Auswertungsrate kann darauf hinweisen, dass das System mit der Aufnahmerate nicht Schritt halten kann, die Last durch die Clientanwendungen zu hoch ist oder eine ungewöhnliche Bedingung vorliegt.

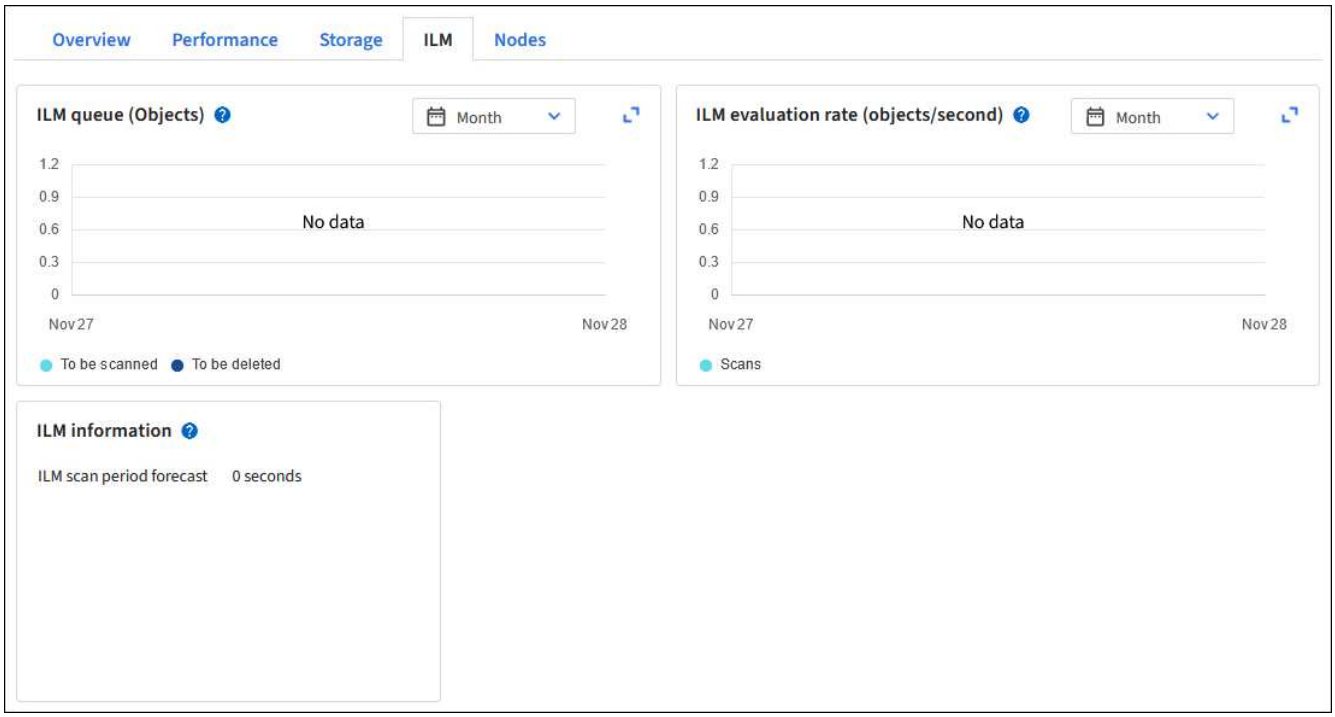
Schritte

1. **Dashboard** > **ILM** auswählen.

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

2. Die Kennzahlen auf der Registerkarte ILM lassen sich überwachen.

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



S3 Object Lock verwenden

Wie S3 Object Lock Objekte in StorageGRID schützt

Als Grid-Administrator können Sie die S3 Object Lock für Ihr StorageGRID System aktivieren und eine konforme ILM-Richtlinie implementieren, sodass Objekte in bestimmten S3 Buckets für eine festgelegte Zeitspanne weder gelöscht noch überschrieben werden.

Was ist S3 Object Lock?

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

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

Ein Bucket ohne S3 Object Lock kann nur Objekte ohne festgelegte Aufbewahrungseinstellungen enthalten. Für importierte Objekte werden keine Aufbewahrungseinstellungen festgelegt.

Ein Bucket mit S3 Object Lock kann Objekte mit und ohne von S3-Clientanwendungen festgelegte Aufbewahrungseinstellungen enthalten. Einige der importierten Objekte weisen Aufbewahrungseinstellungen auf.

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

Effektiv haben alle neu importierten Objekte Aufbewahrungseinstellungen, wenn die Standardaufbewahrung

konfiguriert ist. Vorhandene Objekte ohne Objektspezifische Aufbewahrungseinstellungen bleiben unberührt.

Aufbewahrungsmodi

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

- Im Konformitätsmodus:
  - 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 nach Erreichen dieses Datums entfernt werden.
- Im Governance-Modus:
  - Benutzer mit speziellen Berechtigungen können einen Bypass-Header in Anfragen verwenden, um bestimmte Aufbewahrungseinstellungen zu ändern.
  - Diese Benutzer können eine Objektversion löschen, bevor deren Aufbewahrungsdatum erreicht ist.
  - Diese Benutzer können das Aufbewahrungsdatum eines Objekts erhöhen, verringern oder entfernen.

Aufbewahrungseinstellungen für Objektversionen

Wenn ein Bucket mit aktiviertem S3 Object Lock erstellt wird, können Benutzer die S3-Clientanwendung verwenden, um optional die folgenden Aufbewahrungseinstellungen für jedes Objekt festzulegen, das dem Bucket hinzugefügt wird:

- **Aufbewahrungsmodus**: Entweder Compliance oder Governance.
- **Retain-until-date**: Wenn das Retain-until-date einer Objektversion in der Zukunft liegt, kann das Objekt abgerufen, aber nicht gelöscht werden.
- **Rechtliche Sperre**: Durch das Anwenden einer rechtlichen Sperre auf eine Objektversion wird dieses Objekt sofort gesperrt. Beispielsweise kann es erforderlich sein, eine rechtliche Sperre auf ein Objekt anzuwenden, das mit einer Untersuchung oder einem Rechtsstreit in Zusammenhang steht. Eine rechtliche Sperre hat kein Ablaufdatum, sondern bleibt bestehen, bis sie explizit entfernt wird. Rechtliche Sperren sind unabhängig vom Aufbewahrungsdatum.

  > Wenn ein Objekt unter einer rechtlichen Aufbewahrungspflicht steht, kann niemand das Objekt löschen, unabhängig vom Aufbewahrungsmodus.

  Weitere Informationen zu den Objekteinstellungen finden Sie unter "S3 REST API zur Konfiguration von S3 Object Lock verwenden".

Standardmäßige Aufbewahrungseinstellung für Buckets

Wenn ein Bucket mit aktiviertem S3 Object Lock erstellt wird, können Benutzer optional die folgenden Standardeinstellungen für den Bucket angeben:

- **Standardmäßiger Aufbewahrungsmodus**: Entweder Compliance oder Governance.
- **Standardmäßige Aufbewahrungsdauer**: Wie lange neue Objektversionen, die diesem Bucket hinzugefügt werden, ab dem Tag ihrer Hinzufügung aufbewahrt werden.

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

Siehe "Einen S3-Bucket erstellen" und "Standardaufbewahrungsdauer für S3 Object Lock aktualisieren".

Vergleich der S3 Object Lock mit der herkömmlichen Compliance

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

> ⓘ Die globale Compliance-Einstellung ist veraltet. Wenn diese Einstellung in einer früheren Version von StorageGRID aktiviert wurde, wird die S3 Object Lock-Einstellung automatisch aktiviert. Die Verwaltung der Einstellungen vorhandener konformer Buckets mit StorageGRID ist weiterhin möglich; das Erstellen neuer konformer Buckets ist jedoch nicht möglich. Weitere Informationen finden sich unter "NetApp Knowledge Base: Verwaltung älterer konformer Buckets in StorageGRID 11.5".

Wenn Sie in einer früheren Version von StorageGRID die herkömmliche Compliance-Funktion verwendet haben, zeigt die folgende Tabelle den Vergleich mit der S3-Objektsperrfunktion in StorageGRID.

	S3 Object Lock	**Compliance (Legacy)**
Wie wird die Funktion global aktiviert?	Im Grid Manager **Konfiguration** > **System** > **S3 Object Lock** auswählen.	Wird nicht mehr unterstützt.
Wie wird die Funktion für einen Bucket aktiviert?	Benutzer müssen die S3 Object Lock-Funktion aktivieren, wenn sie einen neuen Bucket mit dem Tenant Manager, der Tenant Management API oder der S3 REST API erstellen.	Wird nicht mehr unterstützt.
Wird die Bucket-Versionierung unterstützt?	Ja. Die Bucket-Versionierung ist erforderlich und wird automatisch aktiviert, wenn S3 Object Lock für den Bucket aktiviert ist.	Nr.
Wie wird die Aufbewahrungsdauer von Objekten festgelegt?	Benutzer können für jede Objektversion ein Aufbewahrungsdatum festlegen oder eine Standardaufbewahrungsdauer für jeden Bucket festlegen.	Benutzer müssen eine Aufbewahrungsfrist für den gesamten Bucket festlegen. Die Aufbewahrungsfrist gilt für alle Objekte im Bucket.

	S3 Object Lock	Compliance (Legacy)
Kann die Aufbewahrungsfrist geändert werden?	• Im Compliance-Modus kann das Aufbewahrungsdatum für eine Objektversion erhöht, aber niemals verringert werden. • Im Governance-Modus können Benutzer mit speziellen Berechtigungen die Aufbewahrungseinstellungen eines Objekts verringern oder sogar entfernen.	Die Aufbewahrungsdauer eines Buckets kann verlängert, aber niemals verkürzt werden.
Wo wird die Legal Hold-Funktion gesteuert?	Benutzer können für jede Objektversion im Bucket eine rechtliche Sperre einrichten oder aufheben.	Eine rechtliche Sperre wird auf den Bucket angewendet und betrifft alle Objekte im Bucket.
Wann können Objekte gelöscht werden?	• Im Compliance-Modus kann eine Objektversion nach Ablauf des Aufbewahrungsdatums gelöscht werden, vorausgesetzt, das Objekt befindet sich nicht unter Legal Hold. • Im Governance-Modus können Benutzer mit speziellen Berechtigungen ein Objekt löschen, bevor dessen Aufbewahrungsfrist erreicht ist, vorausgesetzt, das Objekt unterliegt keiner rechtlichen Aufbewahrungspflicht.	Ein Objekt kann nach Ablauf der Aufbewahrungsfrist gelöscht werden, sofern der Bucket nicht unter rechtlicher Sperrung steht. Objekte können automatisch oder manuell gelöscht werden.
Wird die Bucket-Lifecycle-Konfiguration unterstützt?	Ja	Nein

S3 Object Lock-Workflow in StorageGRID

Als Grid-Administrator ist eine enge Abstimmung mit den Mandantenbenutzern erforderlich, damit die Objekte so geschützt werden, dass ihre Aufbewahrungsanforderungen erfüllt sind.

> Das Anwenden der Mandanteneinstellungen im gesamten Grid kann abhängig von der Netzwerkverbindung, dem Knotenstatus und den Cassandra-Operationen 15 Minuten oder länger in Anspruch nehmen.

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

Grid Administrator

- Globale S3-Objektsperreinstellung für das gesamte StorageGRID System aktivieren.
- Stellen Sie sicher, dass die Richtlinien für das Informationslebenszyklusmanagement (ILM) *konform* sind; das heißt, dass sie die "Anforderungen von Buckets mit aktiviertem S3 Object Lock" erfüllen.
- Gegebenenfalls kann ein Mandant Compliance als Aufbewahrungsmodus verwenden. Andernfalls ist nur Governance als Modus zulässig.
- Bei Bedarf kann eine maximale Aufbewahrungsdauer für einen Mandanten festgelegt werden.

Mandantenbenutzer

- Hinweise zu Buckets und Objekten mit S3 Object Lock.
- Gegebenenfalls den Grid-Administrator kontaktieren, damit die globale S3 Object Lock-Einstellung aktiviert und die Berechtigungen festgelegt werden.
- Buckets mit aktivierter S3-Objektsperre erstellen.
- Optional lassen sich die Standard-Aufbewahrungseinstellungen für einen Bucket konfigurieren:
  - Standardmäßiger Aufbewahrungsmodus: Governance oder Compliance, sofern vom Grid-Administrator zugelassen.
  - Standardmäßige Aufbewahrungsfrist: Muss kleiner oder gleich der vom Grid-Administrator festgelegten maximalen Aufbewahrungsfrist sein.
- Verwenden Sie die S3-Clientanwendung, um Objekte hinzuzufügen und optional objektspezifische Aufbewahrungsfristen festzulegen:
  - Aufbewahrungsmodus. Governance oder Compliance, sofern vom Grid-Administrator zugelassen.
  - Aufbewahrungsdatum: Muss kürzer oder gleich der vom Grid-Administrator festgelegten maximalen Aufbewahrungsfrist sein.

S3 Object Lock-Anforderungen in StorageGRID

Die Voraussetzungen für die Aktivierung der globalen S3-Objektsperre, die Anforderungen an die Erstellung konformer ILM-Regeln und ILM-Richtlinien sowie die von StorageGRID auferlegten Einschränkungen für Buckets und Objekte, die S3-Objektsperre verwenden, sind zu beachten.

Voraussetzungen für die Verwendung der globalen S3 Object Lock-Einstellung

- Die globale S3 Object Lock-Einstellung muss über den Grid Manager oder die Grid Management API aktiviert werden, bevor ein S3-Mandant einen Bucket mit aktivierter S3 Object Lock-Funktion erstellen kann.
- Durch Aktivieren der globalen S3 Object Lock-Einstellung können alle S3-Mandantenkonten Buckets mit aktivierter S3 Object Lock-Funktion erstellen.
- Nachdem Sie die globale S3 Object Lock-Einstellung aktiviert haben, kann die Einstellung nicht mehr deaktiviert werden.
- Die globale S3 Object Lock kann erst aktiviert werden, wenn die Standardregel in allen aktiven ILM-Richtlinien *konform* ist (das heißt, die Standardregel muss den Anforderungen von Buckets mit aktivierter S3 Object Lock entsprechen).
- Wenn die globale S3 Object Lock-Einstellung aktiviert ist, kann keine neue ILM-Richtlinie erstellt oder eine bestehende ILM-Richtlinie aktiviert werden, es sei denn, die Standardregel in der Richtlinie ist konform. Nachdem die globale S3 Object Lock-Einstellung aktiviert wurde, wird auf den Seiten „ILM-Regeln“ und

„ILM-Richtlinien“ angezeigt, welche ILM-Regeln konform sind.

Anforderungen an konforme ILM Regeln

Wenn Sie die globale S3 Object Lock-Einstellung aktivieren möchten, muss sichergestellt sein, dass die Standardregel in allen aktiven ILM-Richtlinien konform ist. Eine konforme Regel erfüllt die Anforderungen sowohl von Buckets mit aktivierter S3 Object Lock-Funktion als auch von allen vorhandenen Buckets, für die die Legacy Compliance aktiviert ist:

- Mindestens zwei replizierte Objektkopien oder eine löschcodierte Kopie müssen erstellt werden.
- Diese Kopien müssen für die gesamte Dauer jeder Zeile in den Platzierungsanweisungen auf den Storage Nodes vorhanden sein.
- Objektkopien können nicht in einem Cloud Storage Pool 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 „forever“ lauten.

Anforderungen an ILM Richtlinien

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

- Die Standardregel in einer aktiven oder inaktiven ILM-Richtlinie muss konform sein.
- Nicht konforme Regeln gelten nur für Objekte in Buckets, bei denen S3 Object Lock nicht aktiviert ist oder bei denen die Legacy 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 sein.

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

Anforderungen für Buckets mit aktiviertem S3 Object Lock

- Wenn die globale S3 Object Lock-Einstellung für das StorageGRID System aktiviert ist, kann der Tenant Manager, die Tenant Management API oder die S3 REST API verwendet werden, um Buckets mit aktivierter S3 Object Lock-Funktion zu erstellen.
- Wenn Sie S3 Object Lock verwenden möchten, müssen Sie S3 Object Lock beim Erstellen des Buckets aktivieren. S3 Object Lock kann für einen bestehenden Bucket nicht aktiviert werden.
- Wenn S3 Object Lock für einen Bucket aktiviert ist, aktiviert StorageGRID automatisch die Versionierung für diesen Bucket. S3 Object Lock kann nicht deaktiviert oder die Versionierung für den Bucket ausgesetzt werden.
- Optional können Sie mithilfe des Tenant Managers, der Tenant Management API oder der S3 REST API einen Standard-Aufbewahrungsmodus und eine Standard-Aufbewahrungsdauer für jeden Bucket festlegen. Die Standardeinstellungen für die Aufbewahrung gelten nur für neue Objekte, die dem Bucket hinzugefügt werden und keine eigenen Aufbewahrungseinstellungen haben. Diese Standardeinstellungen lassen sich überschreiben, indem für jede Objektversion beim Hochladen ein Aufbewahrungsmodus und ein Aufbewahrungsdatum festgelegt werden.
- Die Bucket-Lebenszykluskonfiguration wird für Buckets mit aktiviertem S3 Object Lock unterstützt.
- CloudMirror Replikation wird für Buckets mit aktiviertem S3 Object Lock nicht unterstützt.

Anforderungen an Objekte in Buckets mit aktiviertem S3 Object Lock

- Um eine Objektversion zu schützen, können Sie Standardaufbewahrungseinstellungen für den Bucket festlegen oder Aufbewahrungseinstellungen für jede Objektversion angeben. Aufbewahrungseinstellungen auf Objektebene können mithilfe der S3-Clientanwendung oder der S3 REST API angegeben werden.
- Die Aufbewahrungseinstellungen gelten für einzelne Objektversionen. Eine Objektversion kann sowohl ein Aufbewahrungsdatum als auch eine rechtliche Aufbewahrungseinstellung haben, nur eine von beiden oder keine. Die Angabe eines Aufbewahrungsdatums oder einer rechtlichen Aufbewahrungseinstellung für ein Objekt schützt nur die in der Anfrage angegebene Version. Es können neue Versionen des Objekts erstellt werden, während die vorherige Version des Objekts gesperrt bleibt.

Lebenszyklus von Objekten in Buckets mit aktiviertem S3 Object Lock

Jedes Objekt, das in einem Bucket mit aktiviertem S3 Object Lock gespeichert wird, durchläuft folgende Phasen:

1. **Objektaufnahme**

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

   - Wenn Aufbewahrungseinstellungen für das Objekt festgelegt 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 existieren.
   - 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 S3-benutzerdefinierten Metadaten geschützt.

2. **Objektaufbewahrung und -Löschung**

   Mehrere Kopien jedes geschützten Objekts werden von StorageGRID für die festgelegte Aufbewahrungsfrist 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 unter einer rechtlichen Aufbewahrungspflicht steht, kann niemand das Objekt löschen, unabhängig vom Aufbewahrungsmodus.

Verwandte Informationen

- "Einen S3-Bucket erstellen"
- "Standardaufbewahrung für S3 Object Lock aktualisieren"
- "S3 REST API zur Konfiguration von S3 Object Lock verwenden"
- "Beispiel 7: Konforme ILM-Richtlinie für S3 Object Lock"

Aktivieren Sie die S3 Object Lock global in StorageGRID

Wenn ein S3-Mandantenkonto beim Speichern von Objektdaten regulatorische Anforderungen erfüllen muss, muss die S3 Object Lock-Funktion für das gesamte

StorageGRID System aktiviert werden. Die Aktivierung der globalen S3 Object Lock-Einstellung ermöglicht es jedem S3-Mandantenbenutzer, Buckets und Objekte mit S3 Object Lock zu erstellen und zu verwalten.

Bevor Sie beginnen

- Sie haben die "Root-Zugriffsberechtigung".
- Sie sind mit einem "unterstützte Webbrowser" beim Grid Manager angemeldet.
- Sie haben den Workflow für die S3 Object Lock geprüft und verstehen die zu beachtenden Punkte.
- Sie haben bestätigt, dass die Standardregel in der aktiven ILM-Richtlinie konform ist. Siehe "Erstellen einer Standard-ILM-Regel" für Details.

Über diese Aufgabe

Ein Grid-Administrator muss die globale S3 Object Lock-Einstellung aktivieren, damit Mandantenbenutzer neue Buckets mit aktivierter S3 Object Lock-Funktion erstellen können. Nachdem diese Einstellung aktiviert wurde, kann sie nicht mehr deaktiviert werden.

Die Compliance-Einstellungen bestehender Mandanten sollten nach der Aktivierung der globalen S3 Object Lock-Einstellung überprüft werden. Nach der Aktivierung dieser Einstellung hängen die S3 Object Lock-Einstellungen pro Mandant von der StorageGRID Version ab, die zum Zeitpunkt der Erstellung des Mandanten verwendet wurde.

> ⓘ Die globale Compliance-Einstellung ist veraltet. Wenn diese Einstellung in einer früheren Version von StorageGRID aktiviert wurde, wird die S3 Object Lock-Einstellung automatisch aktiviert. Die Verwaltung der Einstellungen vorhandener konformer Buckets mit StorageGRID ist weiterhin möglich; das Erstellen neuer konformer Buckets ist jedoch nicht möglich. Weitere Informationen finden sich unter "NetApp Knowledge Base: Verwaltung älterer konformer Buckets in StorageGRID 11.5".

Schritte

1. **Konfiguration** > **System** > **S3 Object Lock** auswählen.

   Die Seite „S3 Object Lock Einstellungen“ wird angezeigt.

2. **S3 Object Lock aktivieren** auswählen.
3. **Anwenden** auswählen.

   Es erscheint ein Bestätigungsdialogfeld, das Sie daran erinnert, dass die S3-Objektsperre nach der Aktivierung nicht mehr deaktiviert werden kann.

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

   Wenn **OK** ausgewählt wird:

   - Wenn die Standardregel in der aktiven ILM-Richtlinie konform ist, ist die S3 Object Lock nun für das gesamte Grid aktiviert und kann nicht deaktiviert werden.
   - Wenn die Standardregel nicht konform ist, wird ein Fehler angezeigt. Es ist erforderlich, eine neue ILM-Richtlinie zu erstellen und zu aktivieren, die eine konforme Regel als Standardregel enthält. **OK** auswählen. Anschließend eine neue Richtlinie erstellen, sie simulieren und aktivieren. Siehe "ILM-Richtlinie erstellen" für Anweisungen.

Beheben Sie Konsistenzfehler beim Aktualisieren von S3 Object Lock oder älteren Compliance-Einstellungen in StorageGRID

Wenn ein Rechenzentrumsstandort oder mehrere Storage Nodes an einem Standort nicht verfügbar sind, könnte es erforderlich sein, S3-Tenant-Benutzern bei der Anwendung von Änderungen an der S3 Object Lock oder der Legacy Compliance-Konfiguration zu unterstützen.

Mandantenbenutzer, die Buckets mit aktiviertem S3 Object Lock (oder der älteren Compliance-Funktion) haben, können bestimmte Einstellungen ändern. Beispielsweise kann ein Mandantenbenutzer, der S3 Object Lock verwendet, eine Objektversion unter Legal Hold stellen.

Wenn ein Benutzer eines Mandanten die Einstellungen für einen S3-Bucket oder eine Objektversion aktualisiert, versucht StorageGRID, die Metadaten des Buckets oder Objekts im gesamten Grid umgehend zu aktualisieren. Wenn das System die Metadaten nicht aktualisieren kann, weil ein Rechenzentrumsstandort oder mehrere Storage Nodes nicht verfügbar sind, wird ein Fehler zurückgegeben:

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

Um diesen Fehler zu beheben, sind die folgenden Schritte erforderlich:

1. Alle Storage Nodes oder Standorte sollten so schnell wie möglich wieder verfügbar sein.
2. Falls Sie nicht genügend Speicherknoten an jedem Standort zur Verfügung stellen können, wenden Sie sich an den technischen Support, der Sie bei der Wiederherstellung der Knoten unterstützen und sicherstellen kann, dass die Änderungen im gesamten Grid einheitlich angewendet werden.
3. Sobald das zugrundeliegende Problem behoben ist, sollte der Mandantenbenutzer daran erinnert werden, die Konfigurationsänderungen erneut zu versuchen.

Verwandte Informationen

- "Ein Mandantenkonto verwenden"_
- "S3 REST-API verwenden"
- "Wiederherstellen und pflegen"

Beispielhafte ILM Regeln und Richtlinien

ILM-Regeln und -Richtlinien für den grundlegenden Objektschutz und die Aufbewahrung in StorageGRID

Die folgenden Beispielregeln und die folgende Richtlinie können als Ausgangspunkt bei der Definition einer ILM-Richtlinie dienen, um Anforderungen an den Objektschutz und die Aufbewahrung zu erfüllen.

Die folgenden ILM-Regeln und Richtlinien sind lediglich Beispiele. Es gibt viele Möglichkeiten, ILM-Regeln zu konfigurieren. Vor der Aktivierung einer neuen Richtlinie empfiehlt es sich, diese zu simulieren, um zu bestätigen, dass sie wie beabsichtigt funktioniert und Inhalte vor Verlust schützt.

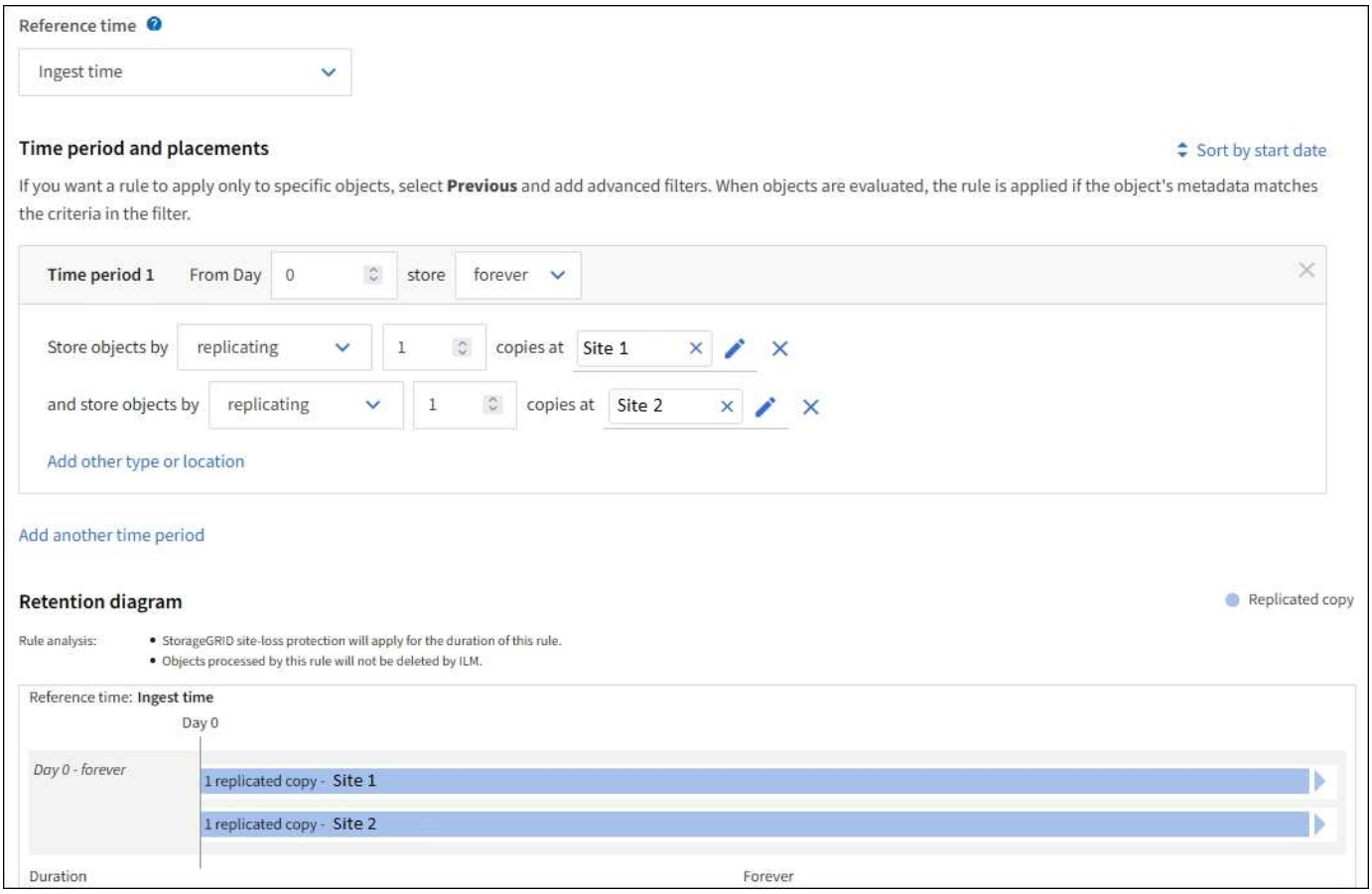
ILM-Regel 1 für Beispiel 1: Objektdaten an zwei Standorte kopieren

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

Regeldefinition	Beispielwert
Speicherpools an einem Standort	Zwei Speicherpools, die jeweils unterschiedliche Standorte enthalten, mit den Namen Site 1 und Site 2.
Regelname	Zwei Kopien zwei Standorte
Referenzzeit	Ingest-Zeitpunkt
Platzierungen	Vom Tag 0 an bis in alle Ewigkeit befindet sich eine replizierte Kopie an Standort 1 und eine replizierte Kopie an Standort 2.

Im Abschnitt „Regelanalyse“ des Aufbewahrungsdiagramms heißt es:

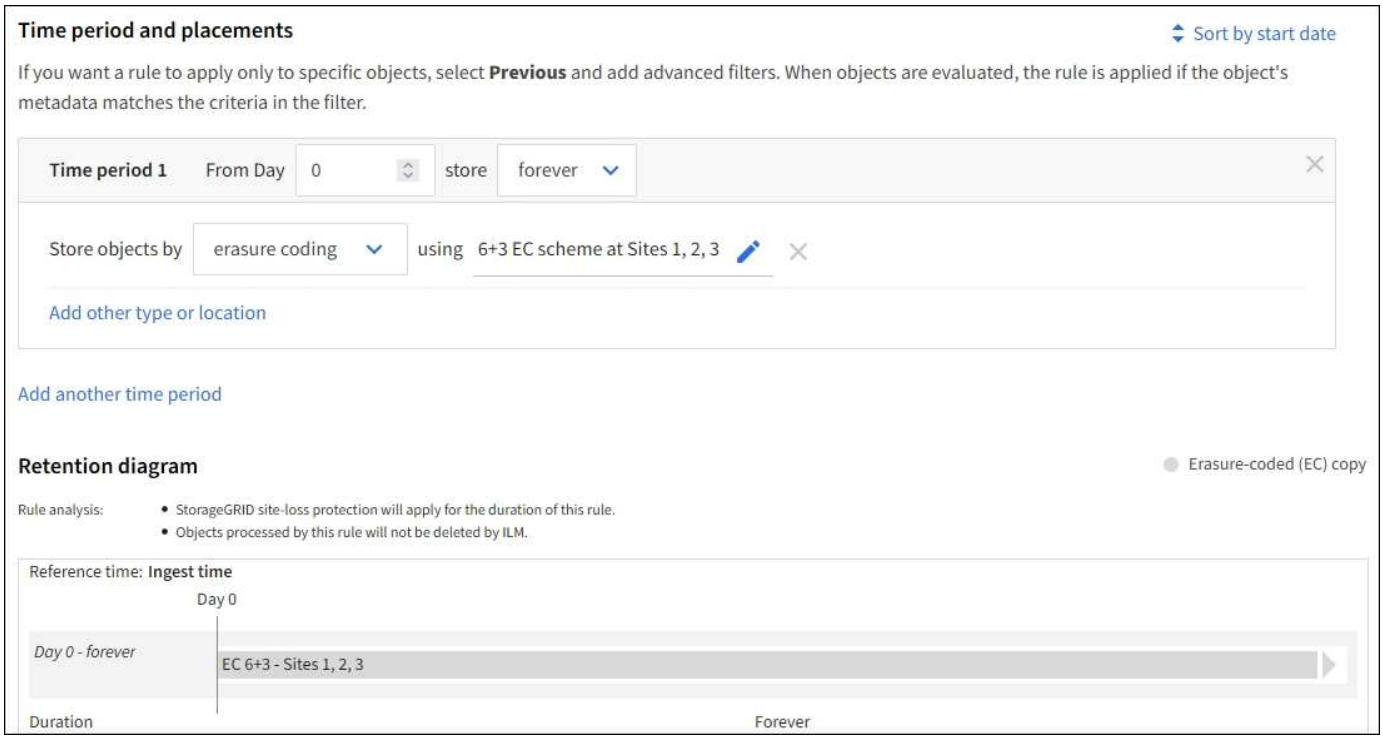
- StorageGRID Site-Loss-Schutz gilt für die Dauer dieser Regel.
- Objekte, die von dieser Regel verarbeitet werden, werden von ILM nicht gelöscht.



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
Storage-Pool mit mehreren Standorten	• Ein gemeinsamer Speicherpool an drei Standorten (Standorte 1, 2, 3) • 6+3-Löschcodierungsverfahren verwenden
Regelname	S3-Bucket finance-records
Referenzzeit	Ingest-Zeitpunkt
Platzierungen	Für Objekte im S3-Bucket „finance-records“ eine mit Erasure-Codierung versehene Kopie im durch das Erasure-Codierungsprofil angegebenen Pool erstellen. Diese Kopie bleibt dauerhaft erhalten.

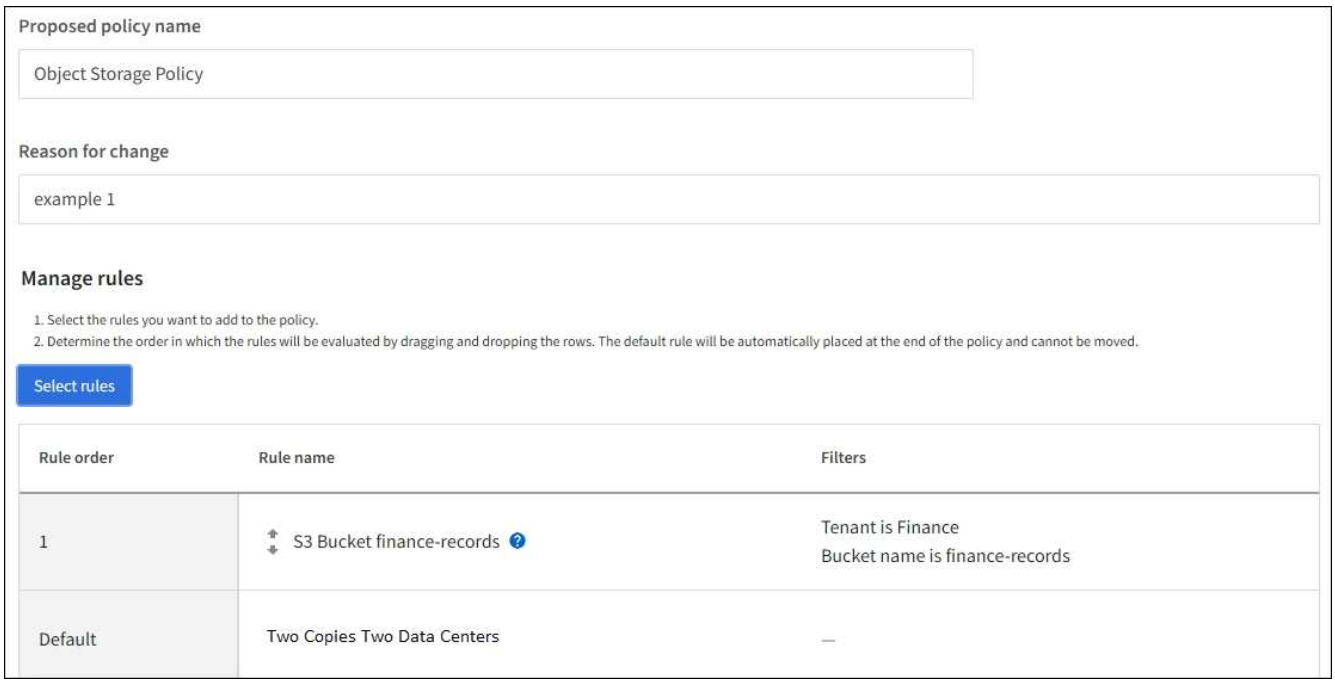


ILM-Richtlinie für Beispiel 1

In der Praxis sind die meisten ILM-Richtlinien einfach, auch wenn das StorageGRID System die Entwicklung anspruchsvoller und komplexer ILM-Richtlinien ermöglicht.

Eine typische ILM Richtlinie für ein Multi Site Grid könnte ILM Regeln wie die folgenden umfassen:

- Beim Import werden alle Objekte, die zum S3-Bucket mit dem Namen `finance-records` gehören, in einem Speicherpool gespeichert, der drei Standorte umfasst. 6+3 Erasure Coding wird verwendet.
- Wenn ein Objekt nicht mit der ersten ILM-Regel übereinstimmt, wird die Standard-ILM-Regel der Richtlinie, Two Copies Two Data Centers, verwendet, um eine Kopie dieses Objekts an Standort 1 und eine Kopie an Standort 2 zu speichern.



Verwandte Informationen

- "ILM Richtlinien verwenden"
- "ILM-Richtlinien erstellen"

ILM-Regeln und Richtlinien für die Filterung der EC-Objektgröße in StorageGRID

Die folgenden Beispielregeln und -richtlinien dienen als Ausgangspunkt für die Definition einer ILM-Richtlinie, die nach Objektgröße filtert, um die empfohlenen EC-Anforderungen zu erfüllen.

Die folgenden ILM-Regeln und Richtlinien sind lediglich Beispiele. Es gibt viele Möglichkeiten, ILM-Regeln zu konfigurieren. Vor der Aktivierung einer neuen Richtlinie empfiehlt es sich, diese zu simulieren, um zu bestätigen, dass sie wie beabsichtigt funktioniert und Inhalte vor Verlust schützt.

ILM-Regel 1 für Beispiel 2: EC für Objekte verwenden, die größer als 1 MB sind

Dieses Beispiel einer ILM-Regel verwendet Erasure Coding für Objekte, die größer als 1 MB sind.

Erasure Coding eignet sich am besten für Objekte größer als 1 MB. Erasure Coding sollte für Objekte kleiner als 200 KB nicht verwendet werden, um den Aufwand für die Verwaltung sehr kleiner erasure-codierter Fragmente zu vermeiden.

Regeldefinition	Beispielwert
Regelname	Nur EC Objekte > 1 MB
Referenzzeit	Ingest-Zeitpunkt

Regeldefinition	Beispielwert
Erweiterter Filter für Objektgröße	Objektgröße größer als 1 MB
Platzierungen	Eine 2+1-Löschcodierungskopie mit drei Standorten erstellen

ILM-Regel 2 für Beispiel 2: Zwei replizierte Kopien

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

Regeldefinition	Beispielwert
Regelname	Zwei replizierte Kopien
Referenzzeit	Ingest-Zeitpunkt
Erweiterter Filter für Objektgröße	Keine
Platzierungen	Vom Tag 0 an bis in alle Ewigkeit befindet sich eine replizierte Kopie an Standort 1 und eine replizierte Kopie an Standort 2.

ILM-Richtlinie für Beispiel 2: EC für Objekte größer als 1 MB

Diese beispielhafte ILM-Richtlinie enthält zwei ILM-Regeln:

- Die erste Regel verwendet Erasure Codes für 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.

ILM-Regeln und -Richtlinien zum Schutz von Image-Dateien in StorageGRID

Mit den folgenden Beispielregeln und der Beispielrichtlinie lässt sich sicherstellen, dass Bilder, die größer als 1 MB sind, mit einem Löschcodierverfahren geschützt werden und dass von kleineren Bildern zwei Kopien erstellt werden.

> Die folgenden ILM-Regeln und Richtlinien sind lediglich Beispiele. Es gibt viele Möglichkeiten, ILM-Regeln zu konfigurieren. Vor der Aktivierung einer neuen Richtlinie empfiehlt es sich, diese zu simulieren, um zu bestätigen, dass sie wie beabsichtigt funktioniert und Inhalte vor Verlust schützt.

ILM-Regel 1 für Beispiel 3: EC für Bilddateien verwenden, die größer als 1 MB sind

Diese Beispiel-ILM-Regel verwendet erweiterte Filterung, um alle Bilddateien größer als 1 MB mit Erasure Coding zu versehen.

> Erasure Coding eignet sich am besten für Objekte größer als 1 MB. Erasure Coding sollte für Objekte kleiner als 200 KB nicht verwendet werden, um den Aufwand für die Verwaltung sehr kleiner erasure-codierter Fragmente zu vermeiden.

Regeldefinition	Beispielwert
Regelname	EC Image-Dateien > 1 MB
Referenzzeit	Ingest-Zeitpunkt
Erweiterter Filter für Objektgröße	Objektgröße größer als 1 MB
Erweiterte Filter für Schlüssel	• Endet mit .jpg • Endet mit .png
Platzierungen	Eine 2+1-Löschcodierungskopie mit drei Standorten erstellen

Da diese Regel als erste Regel in der Richtlinie konfiguriert ist, gilt die Anweisung zur Platzierung der Erasure-Codierung nur für .jpg und .png Dateien, die größer als 1 MB sind.

ILM Regel 2 für Beispiel 3: Zwei replizierte Kopien für alle verbleibenden Image-Dateien erstellen

Diese Beispielregel für ILM verwendet erweiterte Filter, um festzulegen, dass kleinere Bilddateien repliziert werden. Da die erste Regel in der Richtlinie bereits Bilddateien größer als 1 MB erfasst hat, gilt diese Regel für Bilddateien mit einer Größe von 1 MB oder weniger.

Regeldefinition	Beispielwert
Regelname	2 Kopien für Image-Dateien

Regeldefinition	Beispielwert
Referenzzeit	Ingest-Zeitpunkt
Erweiterte Filter für Schlüssel	• Endet mit .jpg • Endet mit .png
Platzierungen	2 replizierte Kopien in zwei Speicherpools erstellen

ILM-Richtlinie für Beispiel 3: Besserer Schutz für Bilddateien

Dieses Beispiel für eine ILM Richtlinie enthält drei Regeln:

- Die erste Regel wendet Erasure Codes auf alle Bilddateien an, die größer als 1 MB sind.
- Die zweite Regel erstellt zwei Kopien aller verbleibenden Bilddateien (das heißt, Bilder, die 1 MB oder kleiner sind).
- Die Standardregel gilt für alle übrigen 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	—

ILM-Regeln und -Richtlinien für nicht aktuelle S3-Objektversionen in StorageGRID

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

> Wenn Sie eine begrenzte Aufbewahrungsdauer für Objekte festlegen, werden diese Objekte nach Ablauf der Frist endgültig gelöscht. Es sollte nachvollzogen werden, wie lange die Objekte aufbewahrt werden.

Wie dieses Beispiel zeigt, kann die Menge des von versionierten Objekten verwendeten Speicherplatzes gesteuert werden, indem unterschiedliche Platzierungsanweisungen für nicht aktuelle Objektversionen verwendet werden.

Die folgenden ILM-Regeln und Richtlinien sind lediglich Beispiele. Es gibt viele Möglichkeiten, ILM-Regeln zu konfigurieren. Vor der Aktivierung einer neuen Richtlinie empfiehlt es sich, diese zu simulieren, um zu bestätigen, dass sie wie beabsichtigt 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 ermitteln, verwenden Sie "Objektmetadaten-Lookup" während das Objekt noch aktuell ist.

Verwandte Informationen

"Wie Objekte gelöscht werden"

ILM-Regel 1 für Beispiel 4: Drei Kopien für 10 Jahre speichern

Diese Beispiel-ILM-Regel speichert eine Kopie jedes Objekts an drei Standorten für 10 Jahre.

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

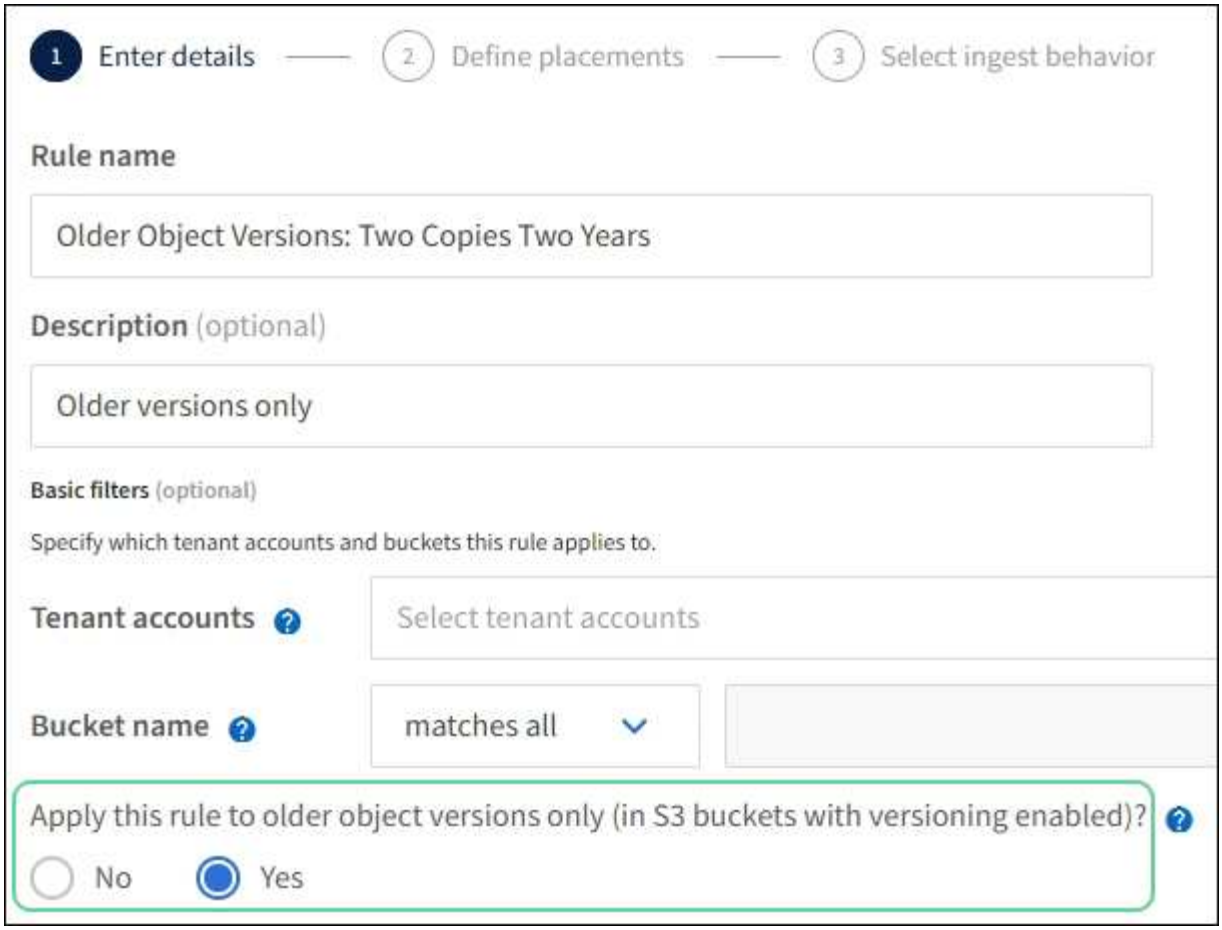
Regeldefinition	Beispielwert
Storage Pools	Drei Speicherpools, die jeweils aus verschiedenen Rechenzentren bestehen, mit den Namen Site 1, Site 2 und Site 3.
Regelname	Drei Kopien zehn Jahre
Referenzzeit	Ingest-Zeitpunkt
Platzierungen	Am Tag 0 werden drei replizierte Kopien für 10 Jahre (3.652 Tage) aufbewahrt, eine in Standort 1, eine in Standort 2 und eine in Standort 3. Am Ende der 10 Jahre werden alle Kopien des Objekts gelöscht.

ILM-Regel 2 für Beispiel 4: Zwei Kopien nicht aktueller Versionen werden für 2 Jahre gespeichert.

Dieses Beispiel einer ILM-Regel speichert zwei Kopien der nicht aktuellen Versionen eines versionierten S3-Objekts für 2 Jahre.

Da die ILM-Regel 1 für alle Versionen des Objekts gilt, muss eine weitere Regel erstellt werden, um nicht aktuelle Versionen herauszufiltern.

Um eine Regel zu erstellen, die „Nicht-aktuelle Zeit“ als Referenzzeit verwendet, wird im ersten Schritt (Details eingeben) des Assistenten zum Erstellen einer ILM-Regel für die Frage „Diese Regel nur auf ältere Objektversionen anwenden (in S3-Buckets mit aktivierter Versionierung)?“ die Option „Ja“ ausgewählt. Bei Auswahl von „Ja“ wird automatisch „Nicht-aktuelle Zeit“ als Referenzzeit festgelegt, und eine andere Referenzzeit kann nicht ausgewählt werden.



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

Regeldefinition	Beispielwert
Speicherpools	Zwei Speicherpools, jeweils in unterschiedlichen Rechenzentren, Site 1 und Site 2.
Regelname	Nicht aktuelle Versionen: Zwei Kopien zwei Jahre
Referenzzeit	Nichtaktuelle Zeit Wird automatisch ausgewählt, wenn im Assistenten zum Erstellen einer ILM-Regel für die Frage „Diese Regel nur auf ältere Objektversionen anwenden (in S3-Buckets mit aktivierter Versionierung)?“ **Ja** ausgewählt wird.
Platzierungen	Am Tag 0 relativ zum nichtaktuellen Zeitpunkt (d. h. beginnend mit dem Tag, an dem die Objektversion zur nichtaktuellen Version wird), werden zwei replizierte Kopien der nichtaktuellen Objektversionen für 2 Jahre (730 Tage) aufbewahrt, eine an Standort 1 und eine an Standort 2. Nach Ablauf von 2 Jahren werden die nichtaktuellen Versionen gelöscht.

ILM-Richtlinie für Beispiel 4: Versionierte S3-Objekte

Wenn ältere Versionen eines Objekts anders als die aktuelle Version verwaltet werden sollen, müssen Regeln, die „Nicht-aktuelle Zeit“ als Referenzzeit verwenden, in der ILM-Richtlinie vor Regeln stehen, die für die aktuelle Objektversion gelten.

Eine ILM-Richtlinie für versionierte S3-Objekte könnte ILM-Regeln wie die folgenden enthalten:

- Alle älteren (nicht aktuellen) Versionen jedes Objekts werden 2 Jahre lang aufbewahrt, beginnend mit dem Tag, an dem die Version nicht mehr aktuell ist.

> Die Regeln für „Nicht-aktuelle Zeit“ müssen in der Richtlinie vor den Regeln aufgeführt werden, die für die aktuelle Objektversion gelten. Andernfalls werden die nicht-aktuellen Objektversionen niemals von der Regel für „Nicht-aktuelle Zeit“ erfasst.

- Beim Import werden drei Replikate erstellt und jeweils eines an drei Standorten gespeichert. Kopien der aktuellen Objektversion werden 10 Jahre lang aufbewahrt.

Wenn die Beispielrichtlinie simuliert wird, ist zu erwarten, dass Testobjekte wie folgt ausgewertet werden:

- Alle nicht mehr aktuellen Objektversionen würden der ersten Regel entsprechen. Ist eine nicht mehr aktuelle Objektversion älter als 2 Jahre, wird sie von ILM endgültig gelöscht (alle Kopien der nicht mehr aktuellen Version werden aus dem Grid entfernt).
- Die aktuelle Objektversion wird von der zweiten Regel abgeglichen. 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 „nicht aktuell“. Bei der nächsten ILM-Auswertung wird diese nicht aktuelle Version von der ersten Regel abgeglichen. Dadurch wird die Kopie an Standort 3 gelöscht und die beiden Kopien an Standort 1 und Standort 2 werden für weitere 2 Jahre gespeichert.

ILM rules und Richtlinien für Strict ingest behavior in StorageGRID

Ein Standortfilter und das Strict-Ingest-Verhalten in einer Regel ermöglichen es, zu verhindern, dass Objekte an einem bestimmten Rechenzentrumsstandort gespeichert werden.

In diesem Beispiel möchte ein in Paris ansässiger Mieter aufgrund regulatorischer Bedenken bestimmte Objekte nicht außerhalb der EU speichern. Andere Objekte, einschließlich aller Objekte aus anderen Mieterkonten, können entweder im Pariser Rechenzentrum oder im US-amerikanischen Rechenzentrum gespeichert werden.

> Die folgenden ILM-Regeln und Richtlinien sind lediglich Beispiele. Es gibt viele Möglichkeiten, ILM-Regeln zu konfigurieren. Vor der Aktivierung einer neuen Richtlinie empfiehlt es sich, diese zu simulieren, um zu bestätigen, dass sie wie beabsichtigt funktioniert und Inhalte vor Verlust schützt.

Verwandte Informationen

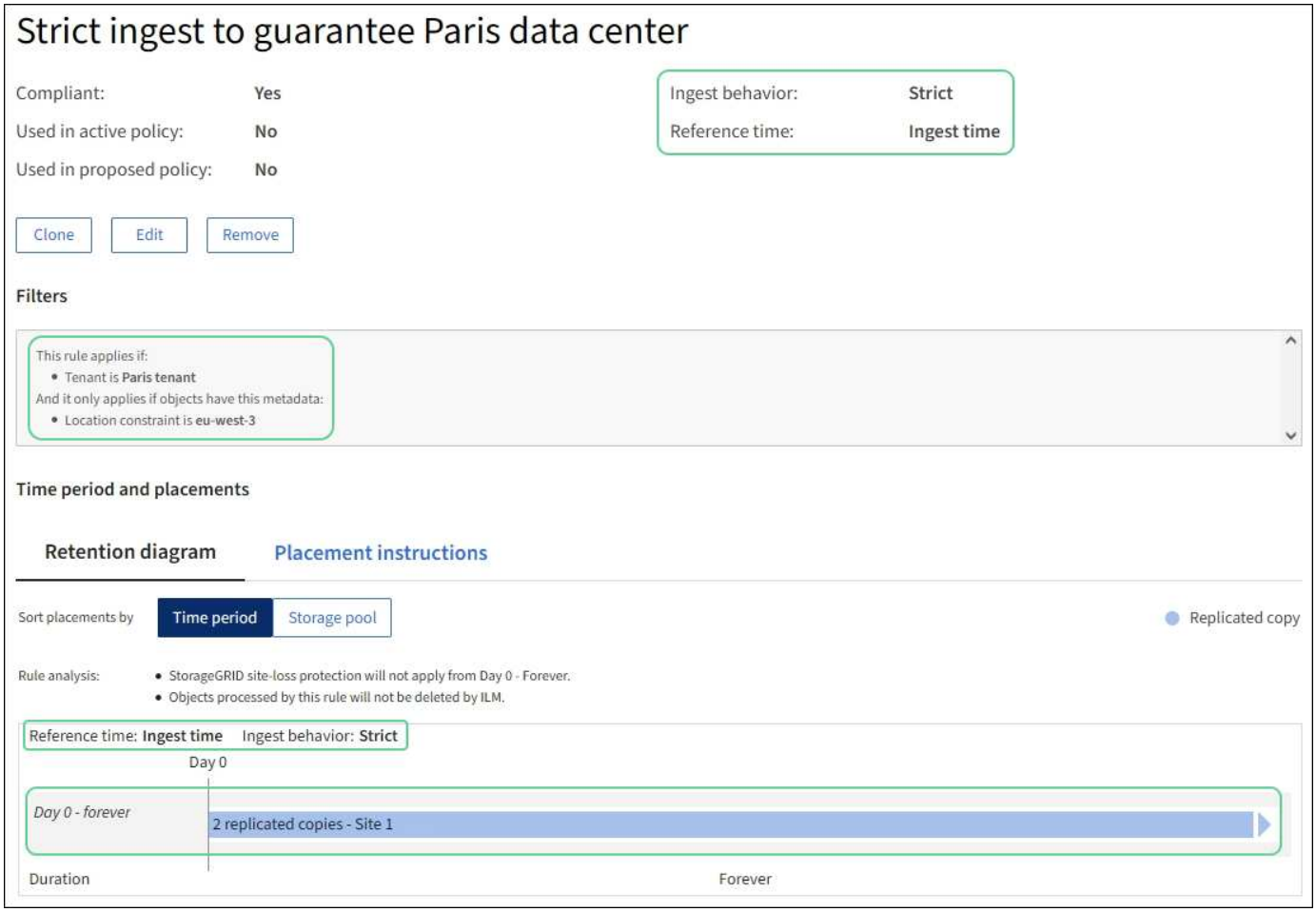
- "Aufnahmeoptionen"
- "ILM-Regel erstellen: Aufnahmeverhalten auswählen"

ILM-Regel 1 für Beispiel 5: Strikte Datenaufnahme 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 Region eu-west-3 Region (Paris) gespeichert werden, niemals im US-Rechenzentrum gespeichert werden.

Diese Regel gilt für Objekte, die zum Mandanten Paris gehören und deren S3-Bucket-Region auf eu-west-3 (Paris) gesetzt ist.

Regeldefinition	Beispielwert
Mandantenkonto	Paris-Mandant
Erweiterter Filter	Standortbeschränkung entspricht eu-west-3
Storage Pools	Standort 1 (Paris)
Regelname	Strenge Datenaufnahme zur Gewährleistung des Paris Rechenzentrums
Referenzzeit	Ingest-Zeitpunkt
Platzierungen	Am Tag 0 bleiben zwei replizierte Kopien dauerhaft in Standort 1 (Paris) erhalten.
Ingest-Verhalten	Streng. Die Platzierungen dieser Regel werden beim Import immer verwendet. Der Import schlägt fehl, wenn es nicht möglich ist, zwei Kopien des Objekts im Pariser Rechenzentrum zu speichern.



ILM-Regel 2 für Beispiel 5: Ausgewogene Datenerfassung für andere Objekte

Diese Beispiel-ILM-Regel nutzt das ausgewogene Aufnahmeverhalten, um eine optimale ILM-Effizienz für alle Objekte zu bieten, die nicht von der ersten Regel erfasst werden. 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 Standort gespeichert.

Diese Regel gilt für Objekte, die zu einem beliebigen Mandanten und einer beliebigen Region gehören.

Regeldefinition	Beispielwert
Mandantenkonto	Ignorieren
Erweiterter Filter	*Nicht angegeben*
Storage Pools	Standort 1 (Paris) und Standort 2 (US)
Regelname	2 Kopien 2 Rechenzentren
Referenzzeit	Ingest-Zeitpunkt

Regeldefinition	Beispielwert
Platzierungen	Am Tag 0 bleiben zwei replizierte Kopien dauerhaft in zwei Rechenzentren erhalten.
Ingest-Verhalten	Ausgewogen. Objekte, die dieser Regel entsprechen, werden nach Möglichkeit gemäß den Platzierungsanweisungen der Regel platziert. Andernfalls werden Zwischenkopien an beliebigen verfügbaren Orten erstellt.

ILM-Richtlinie für Beispiel 5: Kombinieren von Aufnahmeverhalten

Die Beispiel-ILM-Richtlinie enthält zwei Regeln mit unterschiedlichem Aufnahmeverhalten.

Eine ILM-Richtlinie, die zwei unterschiedliche Aufnahmeverhaltensweisen verwendet, könnte ILM-Regeln wie die folgenden enthalten:

- Objekte, die zum Mandanten „Paris“ gehören und deren S3-Bucket-Region auf „eu-west-3“ (Paris) festgelegt ist, werden ausschließlich im Rechenzentrum Paris gespeichert. Die Datenaufnahme schlägt fehl, wenn das Rechenzentrum Paris nicht verfügbar ist.
- Alle übrigen Objekte (einschließlich derer, die zum Paris-Mandanten gehören, aber einer anderen Bucket-Region zugeordnet sind), sowohl im US-Rechenzentrum als auch im Paris-Rechenzentrum speichern. Zwischenkopien können an jedem verfügbaren Standort erstellt werden, falls die Platzierungsanweisung nicht erfüllt werden kann.

Beim Simulieren der Beispielrichtlinie ist zu erwarten, dass Testobjekte wie folgt ausgewertet werden:

- Alle Objekte, die zum Mandanten Paris gehören und deren S3-Bucket-Region auf eu-west-3 gesetzt ist, werden von der ersten Regel erfasst und im Pariser Rechenzentrum gespeichert. Da die erste Regel Strict ingest verwendet, werden diese Objekte niemals im US-Rechenzentrum gespeichert. Wenn die Storage Nodes im Pariser Rechenzentrum nicht verfügbar sind, schlägt die Aufnahme fehl.
- Alle übrigen Objekte werden durch die zweite Regel abgeglichen, einschließlich der Objekte, die zum Mandanten Paris gehören und deren S3-Bucket-Region nicht auf eu-west-3 festgelegt ist. Von jedem Objekt wird in jedem Rechenzentrum eine Kopie gespeichert. Da die zweite Regel jedoch Balanced ingest verwendet, werden bei Ausfall eines Rechenzentrums zwei temporäre Kopien an einem beliebigen verfügbaren Standort gespeichert.

Wie sich die Änderung einer ILM-Richtlinie auf die Leistung von StorageGRID auswirkt

Wenn sich Ihre Anforderungen an den Datenschutz ändern oder Sie neue Standorte hinzufügen, kann eine neue ILM-Richtlinie erstellt und aktiviert werden.

Bevor Sie eine Richtlinie ändern, muss nachvollzogen werden, wie sich Änderungen an der ILM-Platzierung 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, zunächst "eine Richtlinie erstellen". Anschließend "simulieren" und dann "aktivieren" die neue Richtlinie.

Die folgenden ILM-Regeln und Richtlinien sind lediglich Beispiele. Es gibt viele Möglichkeiten, ILM-Regeln zu konfigurieren. Vor der Aktivierung einer neuen Richtlinie empfiehlt es sich, diese zu simulieren, um zu bestätigen, dass sie wie beabsichtigt funktioniert und Inhalte vor Verlust schützt.

Wie sich die Änderung einer ILM-Richtlinie auf die Leistung auswirkt

Bei der Aktivierung einer neuen ILM-Richtlinie 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.

Bei Aktivierung einer neuen ILM-Richtlinie verwendet StorageGRID diese zur Verwaltung aller Objekte, einschließlich vorhandener und neu ingestierter Objekte. Vor der Aktivierung einer neuen ILM-Richtlinie sollten alle Änderungen an der Platzierung vorhandener replizierter und mit Erasure Coding versehener Objekte überprüft werden. Eine Änderung des Speicherorts eines vorhandenen Objekts kann zu vorübergehenden Ressourcenproblemen führen, wenn die neuen Platzierungen bewertet und implementiert werden.

Um sicherzustellen, dass eine neue ILM-Richtlinie die Platzierung bereits replizierter und mit Erasure-Coding versehener Objekte nicht beeinträchtigt, kann "Eine ILM-Regel mit einem Aufnahmezeitfilter erstellen" simuliert werden. Beispielsweise **Aufnahmezeit *ist am oder nach <date and time>***, 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:

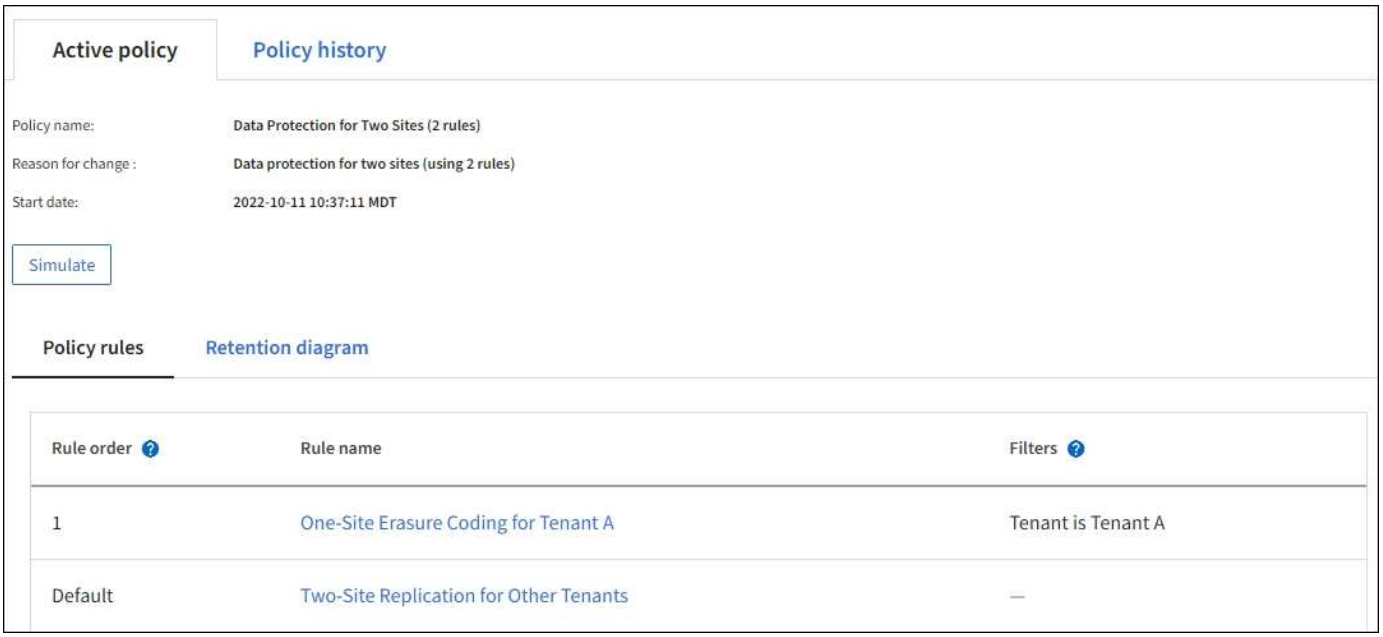
- Anwenden eines anderen Erasure-Coding-Profils auf vorhandene erasure-codierte Objekte.

  StorageGRID betrachtet jedes Erasure-Coding-Profil als einzigartig und verwendet Erasure-Coding-Fragmente nicht wieder, wenn ein neues Profil verwendet wird.

- Änderung der Art der für bestehende Objekte erforderlichen Kopien, beispielsweise die Umwandlung eines großen Prozentsatzes replizierter Objekte in Objekte mit Löschcodierung.
- Kopien bestehender Objekte an einen völlig anderen Ort verschieben, beispielsweise eine große Anzahl von Objekten zu oder von einem Cloud Storage Pool oder zu oder von einem entfernten Standort.

Aktive ILM Richtlinie, Beispiel 6: Datenschutz an zwei Standorten

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



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

Regel 1: Ein-Standort-Löschungscodierung für Tenant A

Regeldefinition	Beispielwert
Regelname	One-Site-Löschcodierung für Mandant A
Mandantenkonto	Mandant A
Speicherpool	Standort 1
Platzierungen	2+1 Erasure Coding in Standort 1 von Tag 0 bis für immer

Regel 2: Zwei-Standorte-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 Site 1 und eine Kopie an Site 2.

ILM-Richtlinie für Beispiel 6: Datenschutz an drei Standorten

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

Nach der Erweiterung um den neuen Standort erstellte der Grid-Administrator zwei neue Speicherpools: einen Speicherpool für Standort 3 und einen Speicherpool, der alle drei Standorte umfasst (nicht zu verwechseln mit dem Standard-Speicherpool „All Storage Nodes“). Anschließend wurden zwei neue ILM-Regeln und eine neue ILM-Richtlinie erstellt, die den Schutz der Daten an allen drei Standorten gewährleisten soll.

Wenn diese neue ILM-Richtlinie aktiviert wird, werden Objekte, die zu Tenant A gehören, durch 2+1 Erasure Coding an drei Standorten geschützt, während Objekte, die zu anderen Tenants gehören (und kleinere Objekte, die zu Tenant A gehören), über drei Standorte hinweg mittels 3-Kopien-Replikation geschützt werden.

Regel 1: Drei-Standort-Löschcodierung für Tenant A

Regeldefinition	Beispielwert
Regelname	Drei-Standort Erasure Coding für Mieter A
Mandantenkonto	Mandant A
Speicherpool	Alle 3 Standorte (einschließlich Standort 1, Standort 2 und Standort 3)
Platzierungen	2+1 Erasure Coding an allen 3 Standorten von Tag 0 an für immer

Regel 2: Drei-Standort-Replikation für andere Mandanten

Regeldefinition	Beispielwert
Regelname	Drei-Standort-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.

Aktivierung der ILM-Richtlinie für Beispiel 6

Wenn eine neue ILM-Richtlinie aktiviert wird, können vorhandene Objekte an neue Speicherorte verschoben oder neue Objektkopien für vorhandene Objekte erstellt werden, abhängig von den Platzierungsanweisungen in neuen oder aktualisierten Regeln.

Fehler in einer ILM-Richtlinie können zu unwiederbringlichem Datenverlust führen. Die Richtlinie sollte sorgfältig überprüft und simuliert werden, bevor sie aktiviert wird, um sicherzustellen, dass sie wie vorgesehen funktioniert.

Bei Aktivierung einer neuen ILM-Richtlinie verwendet StorageGRID diese zur Verwaltung aller Objekte, einschließlich vorhandener und neu ingestierter Objekte. Vor der Aktivierung einer neuen ILM-Richtlinie sollten alle Änderungen an der Platzierung vorhandener replizierter und mit Erasure Coding versehener Objekte überprüft werden. Eine Änderung des Speicherorts eines vorhandenen Objekts kann zu vorübergehenden Ressourcenproblemen führen, wenn die neuen Platzierungen bewertet und implementiert werden.

Was passiert, wenn sich die Anweisungen zur Erasure-Codierung ändern

In der aktuell aktiven ILM-Richtlinie für dieses Beispiel werden Objekte, die zu Tenant A gehören, mit 2+1 Erasure Coding an Standort 1 geschützt. In der neuen ILM-Richtlinie werden Objekte, die zu Tenant A gehören, mit 2+1 Erasure Coding an den Standorten 1, 2 und 3 geschützt.

Wenn die neue ILM-Richtlinie aktiviert wird, treten die folgenden ILM-Operationen auf:

- Neue Objekte, die von Mandant A erfasst werden, werden in zwei Datenfragmente aufgeteilt und ein Paritätsfragment wird hinzugefügt. Anschließend wird jedes der drei Fragmente an einem separaten Standort gespeichert.
- Die vorhandenen Objekte von Tenant A werden im Rahmen des laufenden ILM-Scanvorgangs neu bewertet. Da die ILM-Platzierungsanweisungen ein neues Erasure-Coding-Profil verwenden, werden vollständig neue erasure-codierte Fragmente erstellt und auf 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 keine Erasure-Coding-Fragmente wieder, wenn ein neues Profil verwendet wird.

Was passiert, wenn sich die Replikationsanweisungen ändern

In der aktuell aktiven ILM-Richtlinie für dieses Beispiel werden Objekte anderer Mandanten durch zwei replizierte Kopien in Speicherpools an den Standorten 1 und 2 geschützt. In der neuen ILM-Richtlinie werden Objekte anderer Mandanten durch drei replizierte Kopien in Speicherpools an den Standorten 1, 2 und 3 geschützt.

Wenn die neue ILM-Richtlinie aktiviert wird, treten die folgenden ILM-Operationen auf:

- Wenn ein anderer Mandant als Mandant A ein neues Objekt aufnimmt, erstellt StorageGRID drei Kopien und speichert jeweils eine Kopie an jedem Standort.
- 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. Höhere als normale Mengen an Grid-Ressourcen werden benötigt, um neue mit Erasure-Coding versehene Fragmente für die vorhandenen Objekte von Tenant A und neue replizierte Kopien am Standort 3 für die vorhandenen Objekte anderer Tenants zu erstellen.

Aufgrund der Änderung der ILM-Richtlinie können Lese- und Schreibanfragen von Clients vorübergehend höhere als normale Latenzzeiten aufweisen. Die Latenzzeiten kehren auf normale Werte zurück, nachdem die Platzierungsanweisungen vollständig im gesamten Grid umgesetzt wurden.

Um Ressourcenprobleme bei der Aktivierung einer neuen ILM-Richtlinie zu vermeiden, kann der erweiterte Filter „Ingest time“ in jeder Regel verwendet werden, die den Speicherort einer großen Anzahl vorhandener Objekte ändern könnte. Die Ingest time sollte auf einen Wert größer oder gleich dem ungefähren Zeitpunkt gesetzt werden, zu dem die neue Richtlinie in Kraft tritt, um sicherzustellen, dass vorhandene Objekte nicht unnötig verschoben werden.

Wenden Sie sich an den technischen Support, falls die Geschwindigkeit, mit der Objekte nach einer ILM-Richtlinienänderung verarbeitet werden, verlangsamt oder erhöht werden soll.

Konforme ILM-Richtlinie für S3 Object Lock in StorageGRID

Der S3-Bucket, die ILM-Regeln und die ILM-Richtlinie in diesem Beispiel können als Ausgangspunkt dienen, wenn eine ILM-Richtlinie definiert wird, um die Anforderungen an den Objektschutz und die Aufbewahrung für Objekte in Buckets mit aktiviertem S3 Object Lock zu erfüllen.

Wenn in früheren StorageGRID Versionen die Legacy Compliance Funktion verwendet wurde, kann dieses Beispiel auch zur Verwaltung vorhandener Buckets dienen, bei denen die Legacy Compliance Funktion aktiviert ist.

Die folgenden ILM-Regeln und Richtlinien sind lediglich Beispiele. Es gibt viele Möglichkeiten, ILM-Regeln zu konfigurieren. Vor der Aktivierung einer neuen Richtlinie empfiehlt es sich, diese zu simulieren, um zu bestätigen, dass sie wie beabsichtigt funktioniert und Inhalte vor Verlust schützt.

Verwandte Informationen

- "Objekte mit S3 Object Lock verwalten"
- "Eine ILM-Richtlinie erstellen"

Bucket und Objekte für das S3 Object Lock-Beispiel

In diesem Beispiel hat ein S3-Mandantenkonto mit dem Namen Bank of ABC den Tenant Manager verwendet, um einen Bucket mit aktiviertem S3 Object Lock zu erstellen, um kritische Bankdatensätze zu speichern.

Bucket Definition	Beispielwert
Name des Mandantenkontos	Bank of ABC
Bucket-Name	Bankunterlagen
Bucket-Region	us-east-1 (Standard)

Jedes Objekt und jede Objektversion, die dem Bucket „bank-records“ 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 in Kraft) Eine rechtliche Sperre kann für jede Objektversion jederzeit während der Aufbewahrungsfrist eingerichtet oder aufgehoben werden. Wenn ein Objekt unter einer rechtlichen Sperre steht, kann das Objekt nicht gelöscht werden, selbst wenn der `retain-until-date` erreicht wurde.

ILM-Regel 1 für das S3 Object Lock-Beispiel: Erasure-coding-Profil mit Bucket-Abgleich

Dieses Beispiel für eine ILM-Regel gilt nur für das S3-Mandantenkonto namens Bank of ABC. Sie trifft auf jedes Objekt im `bank-records` Bucket zu und verwendet dann Erasure Coding, um das Objekt auf Storage Nodes an drei Rechenzentrumsstandorten mit einem 6+3-Erasure-Coding-Profil zu speichern. Diese Regel erfüllt die Anforderungen von Buckets mit aktivierter S3 Object Lock: Eine Kopie wird ab Tag 0 dauerhaft auf Storage Nodes aufbewahrt, wobei die Ingest-Zeit als Referenzzeit dient.

Regeldefinition	Beispielwert
Regelname	Konforme Regel: EC-Objekte im Bucket „Bankdatensätze“ - Bank of ABC
Mandantenkonto	Bank of ABC
Bucket-Name	`bank-records`
Erweiterter Filter	Objektgröße (MB) größer als 1 **Hinweis:** Dieser Filter stellt sicher, dass für Objekte mit einer Größe von 1 MB oder kleiner keine Erasure Coding verwendet wird.

Regeldefinition	Beispielwert
Referenzzeit	Ingest-Zeitpunkt
Platzierungen	Ab Tag 0 für immer speichern
Erasure Coding Profil	• Eine löschcodierte Kopie auf Storage Nodes an drei Rechenzentrumsstandorten erstellen • Verwendet ein 6+3 Löschcodierungsverfahren

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

Dieses Beispiel für eine ILM-Regel speichert zunächst zwei replizierte Objektkopien auf Storage Nodes. Nach einem Jahr wird eine Kopie dauerhaft in einem Cloud Storage Pool gespeichert. Da diese Regel einen Cloud Storage Pool verwendet, ist sie nicht konform und gilt nicht für Objekte in Buckets mit aktivierter S3 Object Lock.

Regeldefinition	Beispielwert
Regelname	Nicht konforme Regel: Cloud Storage Pool verwenden
Mieterkonten	Nicht angegeben
Bucket Name	Nicht spezifiziert, gilt aber nur für Buckets, bei denen S3 Object Lock (oder die Legacy-Compliance-Funktion) nicht aktiviert ist.
Erweiterter Filter	Nicht angegeben

Regeldefinition	Beispielwert
Referenzzeit	Ingest-Zeitpunkt
Platzierungen	• An Tag 0 verbleiben zwei replizierte Kopien auf Storage Nodes in Data Center 1 und Data Center 2 für 365 Tage. • Nach einem Jahr bleibt eine replizierte Kopie dauerhaft in einem Cloud-Speicherpool erhalten.

ILM-Regel 3 für S3 Object Lock Beispiel: Standardregel

Diese Beispiel-ILM-Regel kopiert Objektdaten in Speicherpools in zwei Rechenzentren. Diese konforme Regel ist als Standardregel in der ILM-Richtlinie vorgesehen. Sie enthält keine Filter, verwendet nicht die Referenzzeit „Nicht aktuell“ und erfüllt die Anforderungen von Buckets mit aktivierter S3 Object Lock: Zwei Objektkopien werden ab Tag 0 bis unbegrenzt auf Storage Nodes gespeichert, wobei Ingest als Referenzzeitpunkt dient.

Regeldefinition	Beispielwert
Regelname	Standardkonforme Regel: Zwei Kopien, zwei Rechenzentren
Mandantenkonto	Nicht angegeben
Bucket Name	Nicht angegeben
Erweiterter Filter	Nicht angegeben

Regeldefinition	Beispielwert
Referenzzeit	Ingest-Zeitpunkt

Regeldefinition	Beispielwert
Platzierungen	Vom ersten Tag an bis in alle Ewigkeit werden zwei replizierte Kopien aufbewahrt, eine auf Storage Nodes in Data Center 1 und eine auf Storage Nodes in Data Center 2.

Beispiel für eine konforme ILM-Richtlinie für S3 Object Lock

Um eine ILM-Richtlinie zu erstellen, die alle Objekte in Ihrem System effektiv schützt, einschließlich derer in Buckets mit aktiviertem S3 Object Lock, müssen ILM-Regeln ausgewählt werden, die die Speicheranforderungen für alle Objekte erfüllen. Anschließend ist die Richtlinie zu simulieren und zu aktivieren.

Regeln zur Richtlinie hinzufügen

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

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

Die Richtlinie simulieren

Nachdem Sie Ihrer Richtlinie Regeln hinzugefügt, eine standardmäßige konforme Regel ausgewählt und die übrigen Regeln angeordnet haben, sollte die Richtlinie simuliert werden, indem Objekte aus dem Bucket mit aktiviertem S3 Object Lock und aus anderen Buckets getestet werden. Wenn die Beispielrichtlinie simuliert wird, ist zu erwarten, dass Testobjekte wie folgt ausgewertet werden:

- Die erste Regel trifft nur auf Testobjekte zu, die größer als 1 MB sind und sich im Bucket bank-records für den Mandanten Bank of ABC befinden.
- Die zweite Regel stimmt mit allen Objekten in allen nicht konformen Buckets für alle anderen Mandantenkonten überein.
- Die Standardregel gilt für diese Objekte:
  - Objekte mit einer Größe von 1 MB oder kleiner im Bucket bank-records für den Mandanten Bank of ABC.
  - Objekte in jedem anderen Bucket, für den die S3-Objektsperre für alle anderen Mandantenkonten aktiviert ist.

Die Richtlinie aktivieren

Wenn Sie vollständig sicher sind, dass die neue Richtlinie die Objektdaten wie erwartet schützt, kann sie aktiviert werden.

Wie der S3-Bucket-Lebenszyklus und die ILM-Richtlinie in StorageGRID zusammenwirken

Je nach Ihrer Lebenszykluskonfiguration folgen die Objekte den Aufbewahrungseinstellungen entweder des S3-Bucket-Lebenszyklus oder einer ILM-Richtlinie.

Beispiel dafür, dass der Bucket-Lebenszyklus Vorrang vor der ILM-Richtlinie hat

ILM Richtlinie

- Regel basierend auf einem nicht aktuellen Zeitbezug: Am Tag 0 X Kopien für 20 Tage aufbewahren
- Regel basierend auf dem Aufnahmezeitpunkt (Standard): Am Tag 0 X Kopien für 50 Tage 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-Lifecycle-Filter mit dem Präfix „docs/“.
  - Nach 100 Tagen wird eine Löschmarkierung erstellt und „docs/text“ wird nicht mehr aktuell.
  - Nach 5 Tagen, insgesamt 105 Tagen seit der Aufnahme, wird „docs/text“ gelöscht.
  - Nach 95 Tagen, insgesamt 200 Tagen seit der Datenaufnahme und 100 Tagen seit der Erstellung des Löschmarkers, wird der abgelaufene Löschmarker gelöscht.
- Ein Objekt mit dem Namen „video/movie“ wird importiert. Es entspricht nicht dem Filter und verwendet die ILM Aufbewahrungsrichtlinie.
  - Nach 50 Tagen wird eine Löschmarkierung erstellt und „video/movie“ wird nicht mehr aktuell.
  - Nach 20 Tagen, also insgesamt 70 Tagen seit der Aufnahme, wird „video/movie“ gelöscht.
  - Nach 30 Tagen, insgesamt 100 Tagen seit der Datenaufnahme und 50 Tagen seit der Erstellung des Löschmarkers, wird der abgelaufene Löschmarker gelöscht.

Beispiel für einen Bucket Lifecycle, der implizit unbegrenzt beibehält

ILM Richtlinie

- Regel basierend auf einem nicht aktuellen Zeitbezug: Am Tag 0 X Kopien für 20 Tage aufbewahren
- Regel basierend auf dem Aufnahmezeitpunkt (Standard): Am Tag 0 X Kopien für 50 Tage aufbewahren

Bucket-Lebenszyklus

```
"Filter": {"Prefix": "docs/"}, "Expiration": {"ExpiredObjectDeleteMarker":
true}
```

Ergebnis

- Ein Objekt mit dem Namen „docs/text“ wird aufgenommen. Es entspricht dem Bucket-Lifecycle-Filter mit dem Präfix „docs/“.

  Die `Expiration`Aktion gilt nur für abgelaufene Löschmarkierungen, was bedeutet, dass alles andere für immer erhalten bleibt (beginnend mit "docs/").

Löschmarkierungen, die mit "docs/" beginnen, werden entfernt, wenn sie abgelaufen sind.

- Ein Objekt mit dem Namen „video/movie“ wird importiert. Es entspricht nicht dem Filter und verwendet die ILM Aufbewahrungsrichtlinie.
  - Nach 50 Tagen wird eine Löschmarkierung erstellt und „video/movie“ wird nicht mehr aktuell.
  - Nach 20 Tagen, also insgesamt 70 Tagen seit der Aufnahme, wird „video/movie“ gelöscht.
  - Nach 30 Tagen, insgesamt 100 Tagen seit der Datenaufnahme 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 zum Bereinigen abgelaufener Löschmarkierungen

ILM Richtlinie

- Regel basierend auf einem nicht aktuellen Zeitbezug: Am Tag 0 X Kopien für 20 Tage aufbewahren
- Regel basierend auf dem Aufnahmezeitpunkt (Standard): Am Tag 0 X Kopien werden dauerhaft aufbewahrt

Bucket-Lebenszyklus

```
"Filter": {}, "Expiration": {"ExpiredObjectDeleteMarker": true},
"NoncurrentVersionExpiration": {"NoncurrentDays": 20}
```

Ergebnis

- Die ILM-Richtlinie wird im Bucket-Lifecycle dupliziert.
  - Die Forever-Regel der ILM-Richtlinie ist dafür vorgesehen, Objekte manuell zu entfernen und nicht mehr aktuelle Versionen nach 20 Tagen zu bereinigen. Folglich wird die Regel für die Aufnahmezeit abgelaufene Löschmarkierungen dauerhaft behalten.
  - Der Bucket-Lebenszyklus dupliziert das Verhalten der ILM-Richtlinie und fügt `"ExpiredObjectDeleteMarker": true`hinzu, wodurch Löschmarkierungen nach Ablauf ihrer Gültigkeit entfernt werden.
- Ein Objekt wird importiert. Kein Filter bedeutet, dass der Bucket-Lebenszyklus für alle Objekte gilt und die ILM-Aufbewahrungsrichtlinie überschreibt.
  - Wenn ein Mandant eine Objektlöschungsanforderung stellt, wird ein Löschmarker erstellt und das Objekt wird nicht mehr aktuell.
  - Nach 20 Tagen wird das nicht mehr aktuelle Objekt gelöscht und die Löschmarkierung läuft ab.
  - Kurz darauf wird die abgelaufene Löschmarkierung gelöscht.