



ILM und Objekt-Lebenszyklus

StorageGRID software

NetApp

February 12, 2026

Inhalt

ILM und Objekt-Lebenszyklus	1
Wie ILM im gesamten Leben eines Objekts funktioniert	1
Aufnahme von Objekten	2
Aufnahmeoptionen	2
Vorteile, Nachteile und Einschränkungen der Aufnahmeoptionen	4
Speicherung von Objekten (Replizierung oder Erasure Coding)	7
Was ist Replikation?	7
Warum sollten Sie keine Replizierung mit nur einer Kopie verwenden	8
Was ist Erasure Coding?	10
Was sind Erasure Coding-Systeme?	12
Vor- und Nachteile sowie Anforderungen für Erasure Coding	15
Wie die Aufbewahrung von Objekten bestimmt wird	17
Wie Mandantenbenutzer die Aufbewahrung von Objekten steuern	17
Grid-Administratoren steuern die Objektaufbewahrung	18
Interaktion von S3-Bucket-Lebenszyklus und ILM	18
Beispiele für die Aufbewahrung von Objekten	18
So werden Objekte gelöscht	19
Erforderliche Zeit zum Löschen von Objekten	21
Löschen von S3-versionierten Objekten	21

ILM und Objekt-Lebenszyklus

Wie ILM im gesamten Leben eines Objekts funktioniert

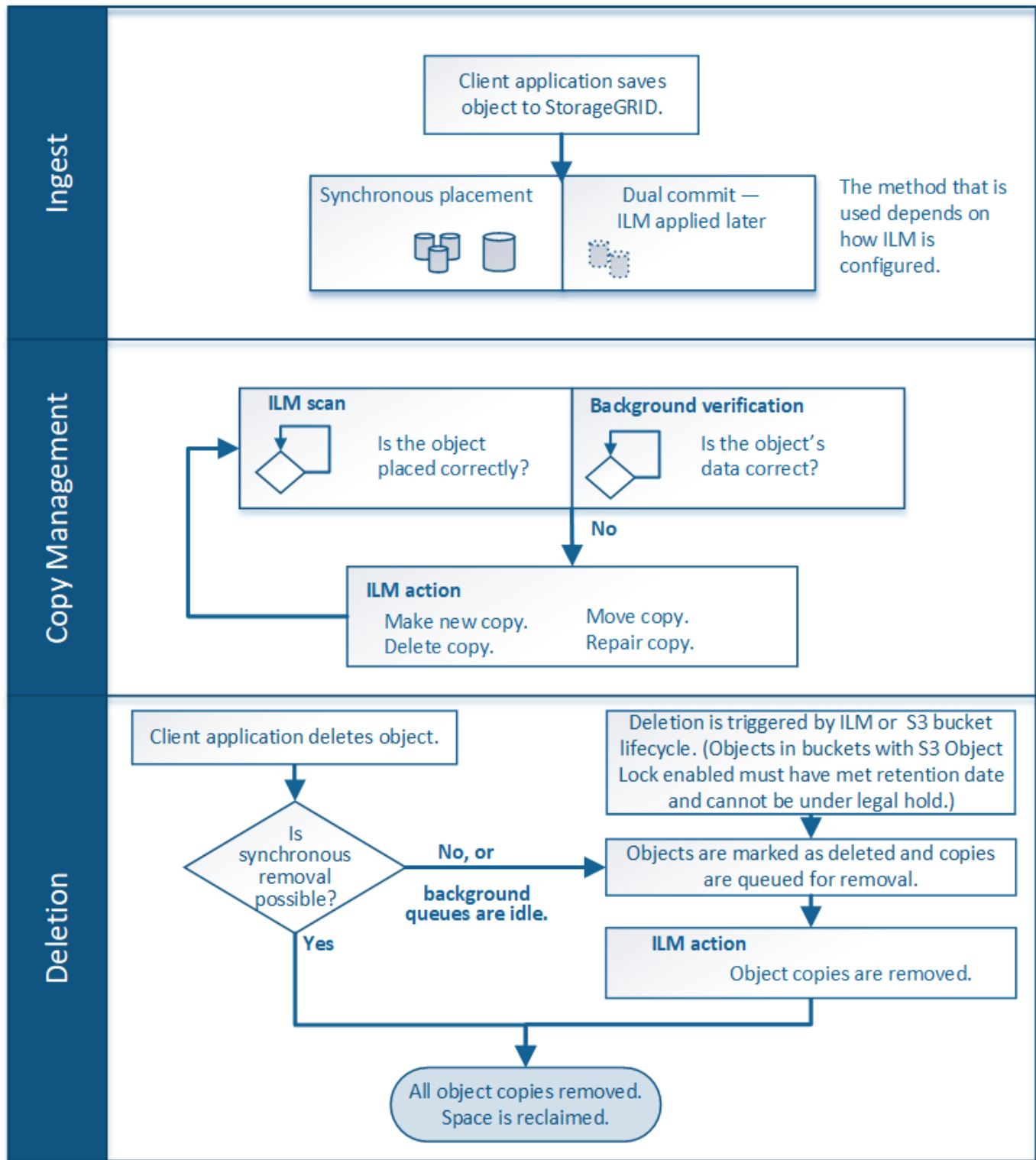
Wenn Sie verstehen, wie StorageGRID ILM für das Management von Objekten in jeder Lebensphase verwendet, können Sie eine effektivere Richtlinie entwickeln.

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



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

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



Aufnahme von Objekten

Aufnahmeoptionen

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

Je nach Ihrer Wahl erstellt StorageGRID später vorläufige Kopien und Warteschlangen für die ILM-Bewertung. Alternativ nutzt es die synchrone Platzierung und erstellt sofort Kopien zur Erfüllung der ILM-Anforderungen.

Flussdiagramm der Aufnahmeoptionen

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

Doppelte Provisionierung

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

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

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

Ausgeglichen (Standard)

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

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

Streng

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

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

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

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

Vorteile, Nachteile und Einschränkungen der Aufnahmeoptionen

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

Eine Übersicht über die Aufnahmeoptionen finden Sie unter ["Aufnahmeoptionen"](#).

Vorteile der ausgewogenen und strengen Optionen

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

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

Nachteile der ausgewogenen und strengen Optionen

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

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

möglicherweise nicht den aktuellen ILM-Anforderungen, wenn der mehrteilige Upload abgeschlossen ist. In diesen Fällen schlägt die Aufnahme des Objekts nicht fehl. Stattdessen wird jedes Teil, das nicht korrekt platziert wird, in die Warteschlange für eine erneute ILM-Bewertung eingereiht und später an den richtigen Speicherort verschoben.

- **Wenn ILM-Regeln Filter auf Größe:** Bei der Bewertung von ILM für ein Teil filtert StorageGRID die Größe des Teils, nicht die Größe des Objekts. Das bedeutet, dass Teile eines Objekts an Orten gespeichert werden können, die die ILM-Anforderungen für das gesamte Objekt nicht erfüllen. Wenn z. B. eine Regel angibt, dass alle Objekte ab 10 GB auf DC1 gespeichert werden, während alle kleineren Objekte an DC2 gespeichert sind, wird bei Aufnahme jeder 1 GB-Teil eines 10-teiligen mehrteiligen Uploads auf DC2 gespeichert. Wenn ILM für das Objekt bewertet wird, werden alle Teile des Objekts auf DC1 verschoben.
- **(strict) Aufnahme scheitert nicht, wenn Objekt-Tags oder Metadaten aktualisiert werden und neu erforderliche Platzierungen nicht gemacht werden können:** Mit strikter, erwarten Sie, dass Objekte entweder wie in der ILM-Regel beschrieben platziert werden oder dass die Aufnahme fehlschlägt. Wenn Sie jedoch Metadaten oder Tags für ein Objekt aktualisieren, das bereits im Raster gespeichert ist, wird das Objekt nicht erneut aufgenommen. Das bedeutet, dass Änderungen an der Objektplatzierung, die durch die Aktualisierung ausgelöst werden, nicht sofort vorgenommen werden. Änderungen an der Platzierung werden vorgenommen, wenn ILM durch normale ILM-Prozesse im Hintergrund neu bewertet wird. Wenn erforderliche Platzierungsänderungen nicht vorgenommen werden können (z. B. weil ein neu erforderlicher Standort nicht verfügbar ist), behält das aktualisierte Objekt seine aktuelle Platzierung bei, bis die Platzierungsänderungen möglich sind.

Einschränkungen bei Objektplatzierungen mit den ausgewogenen und strengen Optionen

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

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

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

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

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

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

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

- **Alle:** Alle Knoten erhalten sofort Objektmetadaten, oder die Anfrage schlägt fehl.
- **Stark global:** Garantiert Lese-nach-Schreib-Konsistenz für alle Clientanforderungen auf allen Sites. Wenn Quorum-Semantiken konfiguriert sind, gelten die folgenden Verhaltensweisen:

- Ermöglicht Site-Fehlertoleranz für Clientanforderungen, wenn Grids drei oder mehr Sites haben. Zwei-Site-Grids verfügen über keine Site-Ausfalltoleranz.
- Die folgenden S3-Vorgänge sind nicht erfolgreich, wenn eine Site ausgefallen ist:
 - DeleteBucketEncryption
 - PutBucketBranch
 - PutBucketEncryption
 - PutBucketVersioning
 - PutObjectLegalHold
 - PutObjectLockKonfiguration
 - PutObjectRetention

Bei Bedarf können Sie ["Konfigurieren Sie die StorageGRID Quorum-Semantik für starke globale Konsistenz"](#) .

- **Strong-site:** Objektmetadaten werden sofort auf andere Knoten am Standort verteilt. Garantiert Konsistenz bei Lese-nach-Schreibvorgängen für alle Client-Anfragen innerhalb eines Standorts.
- **Read-after-New-write:** Bietet Read-after-write-Konsistenz für neue Objekte und eventuelle Konsistenz für Objektaktualisierungen. Hochverfügbarkeit und garantierte Datensicherung Empfohlen für die meisten Fälle.
- **Verfügbar:** Bietet eventuelle Konsistenz für neue Objekte und Objekt-Updates. Verwenden Sie für S3-Buckets nur nach Bedarf (z. B. für einen Bucket mit Protokollwerten, die nur selten gelesen werden, oder für HEAD- oder GET-Vorgänge für nicht vorhandene Schlüssel). Nicht unterstützt für S3 FabricPool-Buckets.



Bevor Sie einen Konsistenzwert auswählen, ["Lesen Sie die vollständige Beschreibung der Konsistenz"](#) . Sie sollten die Vorteile und Einschränkungen verstehen, bevor Sie den Standardwert ändern.

Beispiel für die Interaktion von Konsistenz- und ILM-Regeln

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

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

Wenn ein Client ein Objekt im Grid speichert, erstellt StorageGRID alle drei Objektkopien und verteilt Metadaten an mehrere Sites, bevor es dem Client die Erfolgsmeldung meldet.

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

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

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

Verwandte Informationen

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

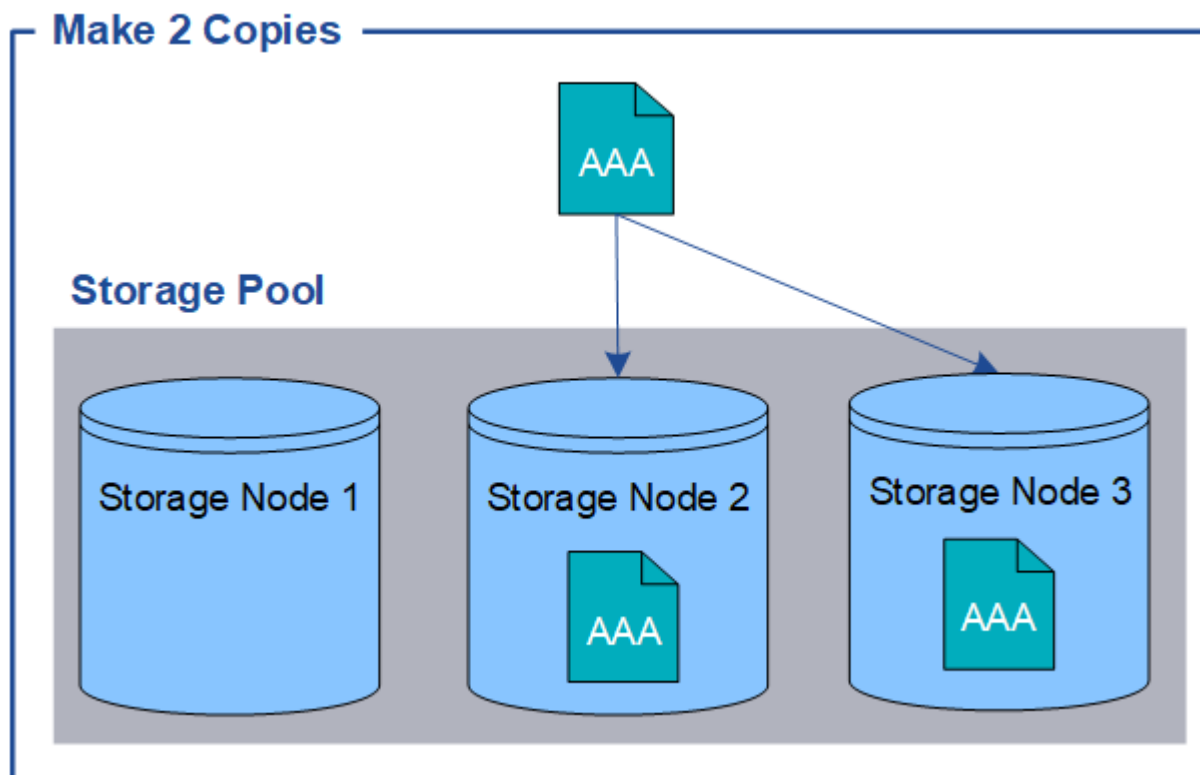
Speicherung von Objekten (Replizierung oder Erasure Coding)

Was ist Replikation?

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

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

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



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

der Nodes im Speicherpool ausfällt.



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

Verwandte Informationen

- ["Was ist Erasure Coding"](#)
- ["Was ist ein Speicherpool"](#)
- ["Schutz vor Standortausfällen durch Replizierung und Erasure Coding"](#)

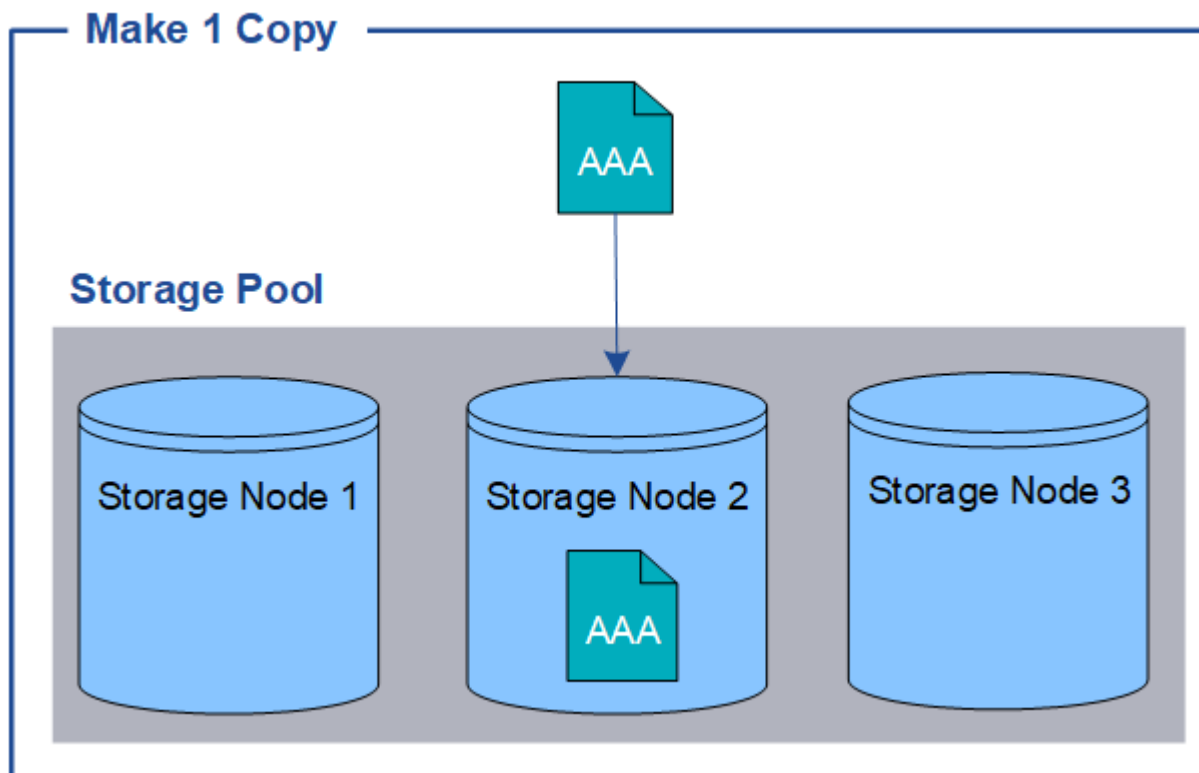
Warum sollten Sie keine Replizierung mit nur einer Kopie verwenden

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

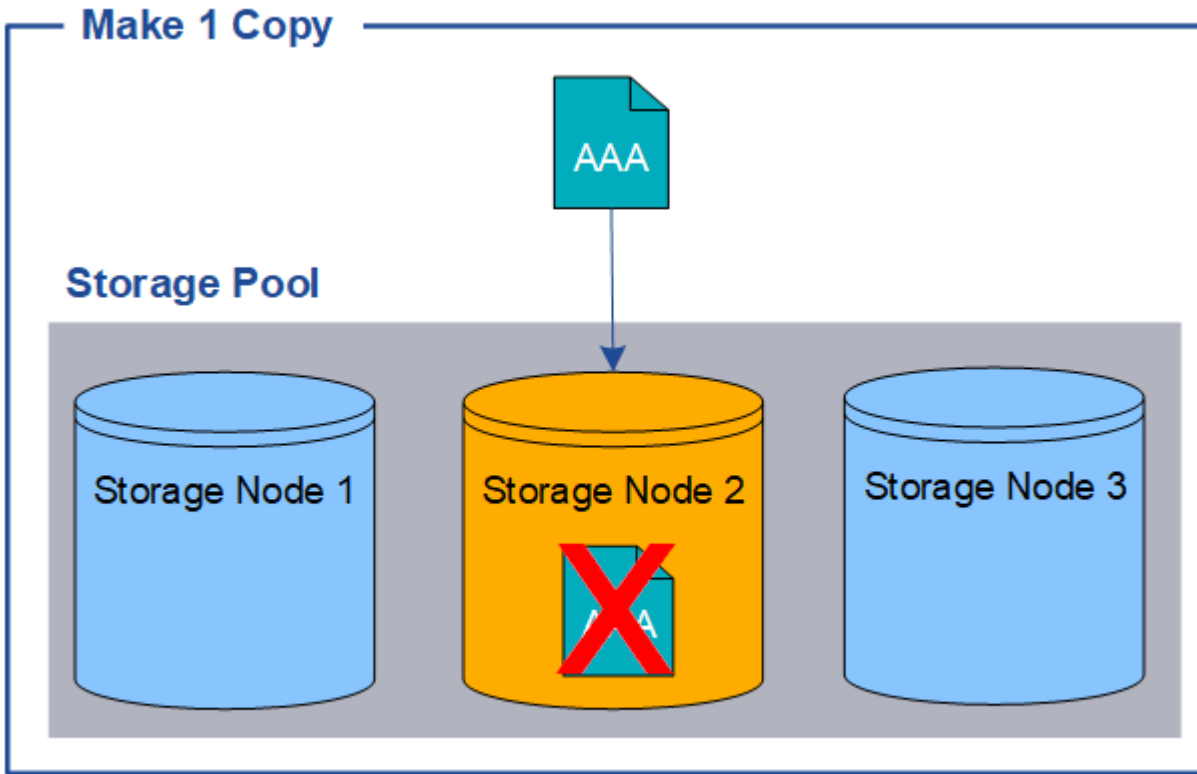


Verwenden Sie keine ILM-Regel, die nur eine replizierte Kopie für einen beliebigen Zeitraum erstellt. Wenn nur eine replizierte Kopie eines Objekts vorhanden ist, geht dieses Objekt verloren, wenn ein Speicherknoten ausfällt oder einen beträchtlichen Fehler hat. Während Wartungsarbeiten wie Upgrades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

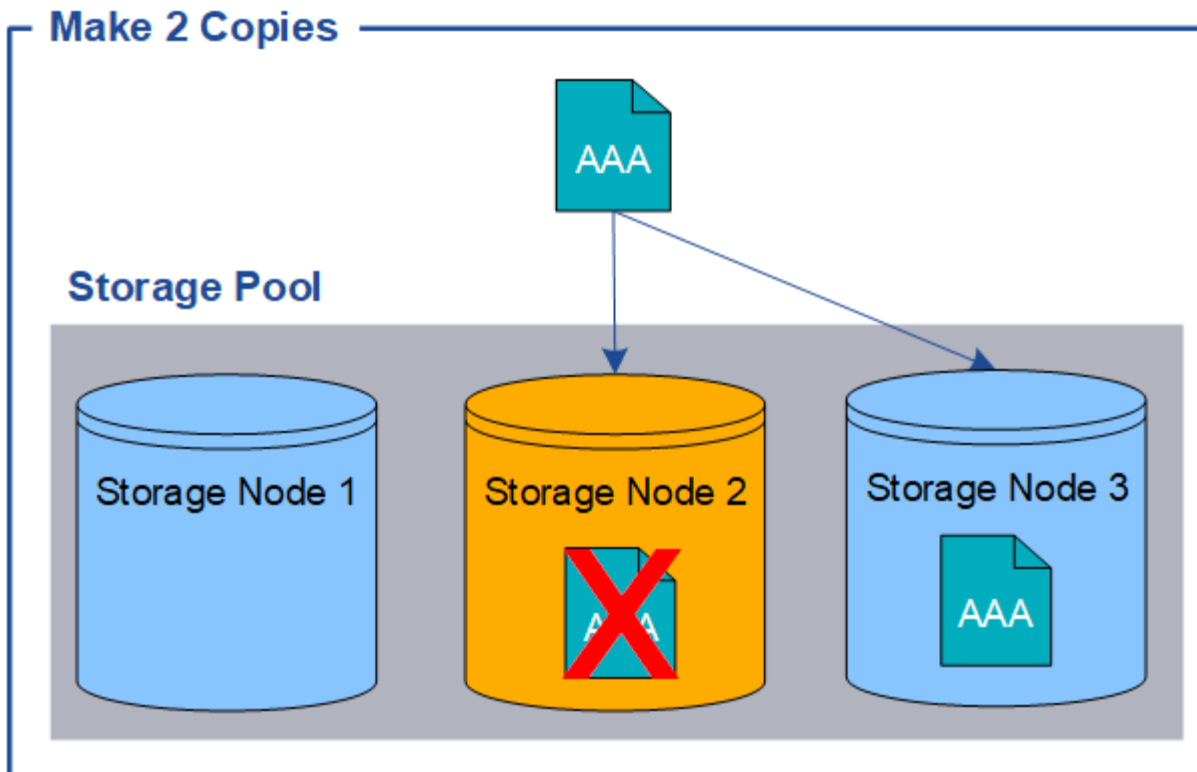
Im folgenden Beispiel gibt die ILM-Regel „1 Kopie erstellen“ an, dass eine replizierte Kopie eines Objekts in einem Speicherpool platziert wird, der drei Storage-Nodes enthält. Wenn ein Objekt aufgenommen wird, das dieser Regel entspricht, platziert StorageGRID eine einzelne Kopie auf nur einem Storage-Node.



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



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



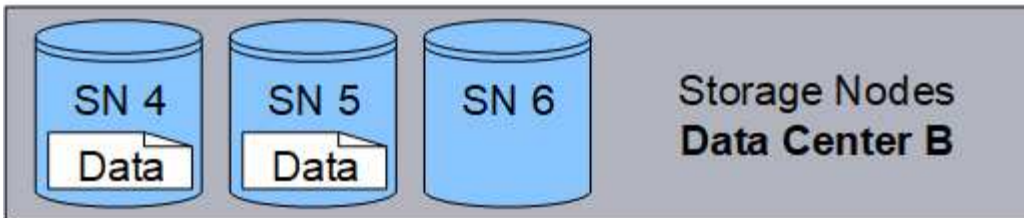
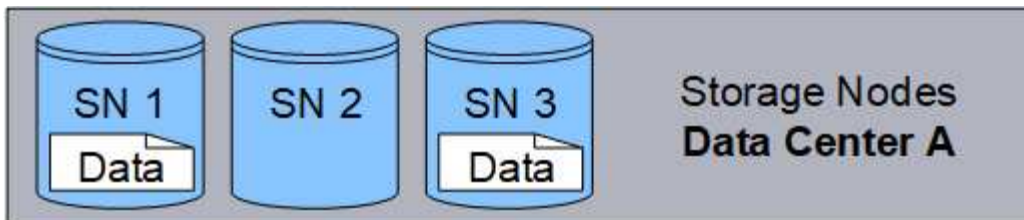
Was ist Erasure Coding?

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

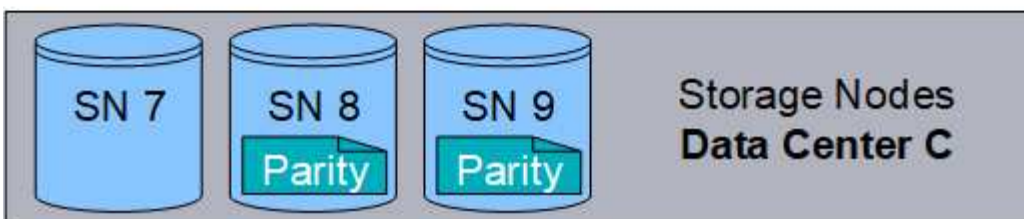
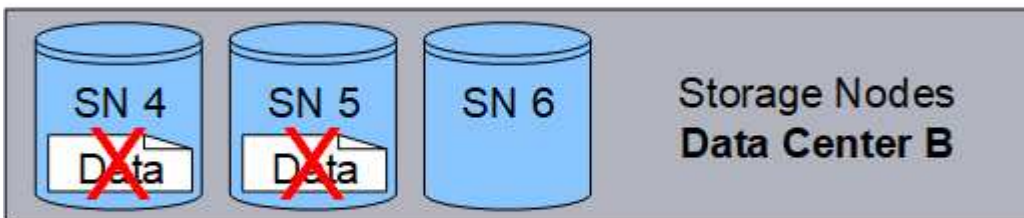
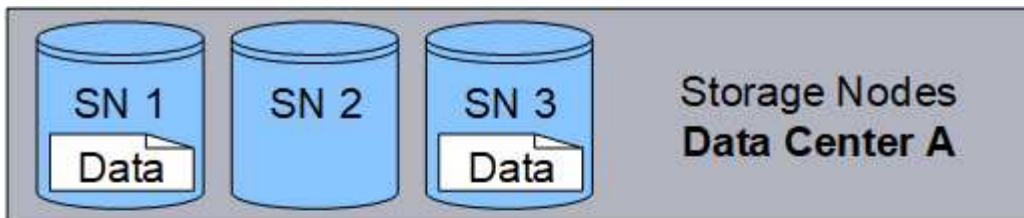
Wenn auf ein Objekt zugegriffen wird, wird es anhand der gespeicherten Fragmente neu zusammengesetzt. Wenn ein Daten- oder ein Paritätsfragment beschädigt wird oder verloren geht, kann der Algorithmus zur Fehlerkorrektur dieses Fragment mit einer Teilmenge der verbleibenden Daten und Paritätsfragmente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

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

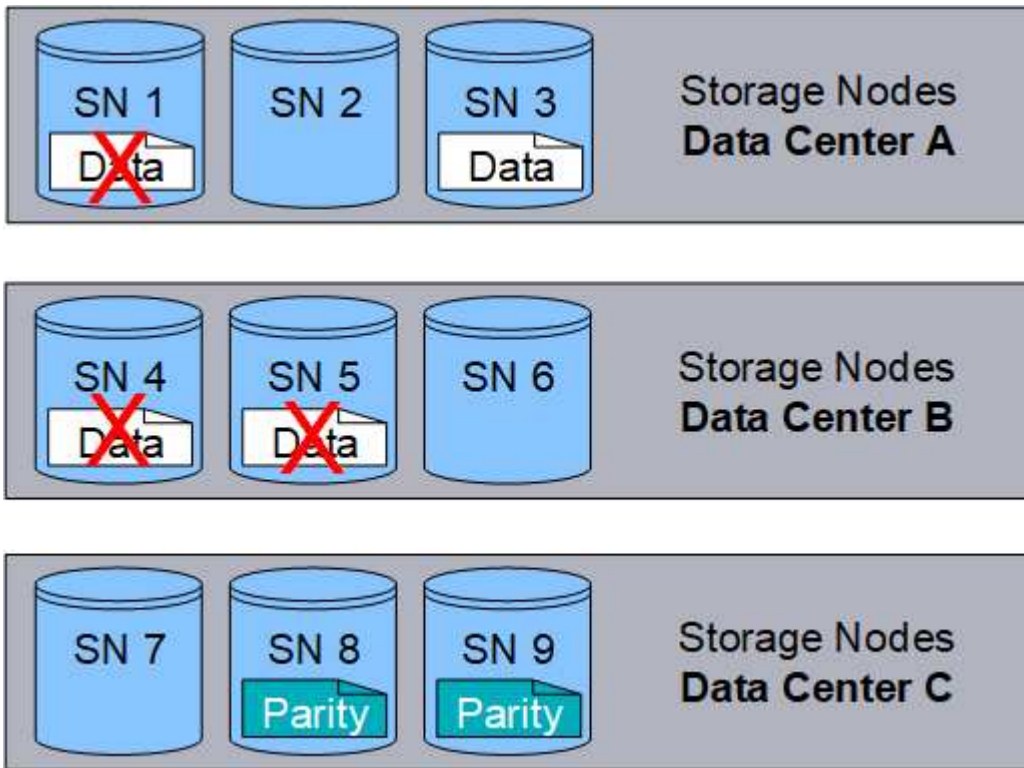
Im folgenden Beispiel wird der Algorithmus zur Einhaltung von Datenkonsistenz (Erasure Coding) für Objektdaten dargestellt. In diesem Beispiel verwendet die ILM-Regel ein 4+2-Schema zur Einhaltung von Datenkonsistenz. Jedes Objekt wird in vier gleiche Datenfragmente geteilt und aus den Objektdaten werden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



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



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



Verwandte Informationen

- ["Was ist Replikation"](#)
- ["Was ist ein Speicherpool"](#)
- ["Was sind Erasure Coding-Systeme"](#)
- ["Umbenennen eines Profils für die Erasure Coding"](#)
- ["Deaktivieren Sie ein Erasure Coding-Profil"](#)

Was sind Erasure Coding-Systeme?

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

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

Datensicherung

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

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

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

die Ausfalltoleranz.

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

Storage Overhead

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

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

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

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

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

Richtlinien für Speicherpools

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

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



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

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



Speicherknoten können während der Installation so konfiguriert werden, dass sie Objektdaten und Metadaten („kombinierter“ Speicherknoten), nur Objektmetadaten oder nur Objektdaten enthalten. Weitere Informationen finden Sie unter ["Typen von Storage-Nodes"](#).

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

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

Die folgende Tabelle beschreibt die von StorageGRID derzeit unterstützten Erasure Coding-Schemata für Storage-Pools, die drei oder mehr Standorte umfassen. Alle diese Maßnahmen bieten einen Standortausfallschutz. Ein Standort kann verloren gehen, und das Objekt ist weiterhin verfügbar.

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

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



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

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

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

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



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

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

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

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

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

Vor- und Nachteile sowie Anforderungen für Erasure Coding

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

Vorteile von Erasure Coding

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

- **Zuverlässigkeit:** Gemessen an der Anzahl gleichzeitiger Ausfälle, die ohne Datenverlust überstanden werden können.
 - Replikation: Mehrere identische Objektkopien werden auf verschiedenen Knoten und an verschiedenen Standorten gespeichert.
 - Erasure Coding: Ein Objekt wird in Daten- und Paritätsfragmente kodiert und auf viele Knoten und Standorte verteilt. Diese Verteilung bietet sowohl Site- als auch Knotenausfallschutz.
- **Verfügbarkeit:** Die Möglichkeit, Objekte abzurufen, wenn Speicherknoten ausfallen oder nicht mehr zugänglich sind. Im Vergleich zur Replikation bietet Erasure Coding eine höhere Verfügbarkeit bei vergleichbaren Speicherkosten.
- **Speichereffizienz:** Bei ähnlicher Verfügbarkeit und Zuverlässigkeit benötigen Erasure-Coded-Objekte weniger Speicherplatz als replizierte Objekte. Beispielsweise verbraucht ein 10 MB großes Objekt, das an zwei Standorten repliziert wird, 20 MB Speicherplatz (zwei Kopien), während ein Objekt, das an drei Standorten mit einem 6+3-Erasure-Coding-Schema löschcodiert wird, nur 15 MB Speicherplatz verbraucht.



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

Nachteile des Erasure Coding

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

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

-System Objektfragmente speichern und abrufen kann.

- Höhere Auslastung von Computing-Ressourcen:

Wann sollte das Erasure Coding verwendet werden

Verwenden Sie Erasure Coding für die folgenden Anforderungen:

- Objekte größer als 1 MB.



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

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

Wie die Aufbewahrung von Objekten bestimmt wird

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

Wie Mandantenbenutzer die Aufbewahrung von Objekten steuern

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

- Wenn die globale S3-Objektsperre für das Grid aktiviert ist, können Benutzer von S3-Mandanten Buckets erstellen, für die S3-Objektsperre aktiviert ist, und dann für jeden Bucket einen **Standardaufbewahrungszeitraum** auswählen.
- Wenn die globale S3-Objektsperreinstellung für das Grid aktiviert ist, können Nutzer von S3-Mandanten Buckets erstellen, deren S3-Objektsperre aktiviert ist. Anschließend können sie über die S3-REST-API Aufbewahrungseinstellungen für jede zu diesem Bucket hinzugefügte Objektversion festlegen.
 - Eine Objektversion, die sich unter einem Legal Hold befindet, kann mit keiner Methode gelöscht werden.
 - Bevor das Aufbewahrungsdatum einer Objektversion erreicht ist, kann diese Version nicht mit einer Methode gelöscht werden.
 - Objekte in Buckets mit aktivierter S3 Object Lock werden von ILM „Forever“ aufbewahrt. Nachdem jedoch eine Aufbewahrungsfrist erreicht ist, kann eine Objektversion durch eine Client-Anfrage oder

den Ablauf des Bucket-Lebenszyklus gelöscht werden. Siehe ["Objekte managen mit S3 Object Lock"](#).

- Benutzer von S3-Mandanten können ihren Buckets eine Lifecycle-Konfiguration hinzufügen, für die eine Ablaufaktion festgelegt ist. Wenn ein Bucket-Lebenszyklus vorhanden ist, speichert StorageGRID ein Objekt, bis das Datum oder die Anzahl der Tage, die im Verfallsvorgang angegeben sind, erreicht ist, es sei denn, der Client löscht das Objekt zuerst. Siehe ["S3-Lebenszykluskonfiguration erstellen"](#).
- Ein S3-Client kann eine Anfrage zum Löschen von Objekten ausgeben. StorageGRID priorisiert Löschanfragen von Clients immer über den S3-Bucket-Lebenszyklus oder ILM, wenn sie bestimmen, ob ein Objekt gelöscht oder aufbewahrt werden soll.

Grid-Administratoren steuern die Objektaufbewahrung

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

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

Interaktion von S3-Bucket-Lebenszyklus und ILM

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

Beispiele für die Aufbewahrung von Objekten

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

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

ILM

Speichern von zwei Kopien für 1 Jahr (365 Tage)

Bucket-Lebenszyklus

Verfalle Objekte in 2 Jahren (730 Tage)

Ergebnis

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



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

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

ILM

Speichern von zwei Kopien für 2 Jahre (730 Tage)

Bucket-Lebenszyklus

Verfalle Objekte in 1 Jahr (365 Tage)

Ergebnis

StorageGRID löscht beide Kopien des Objekts nach Tag 365.

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

ILM

„Ewig“ Speicherung von zwei Kopien auf Storage-Nodes

Bucket-Lebenszyklus

Verfalle Objekte in 2 Jahren (730 Tage)

Anforderung zum Löschen des Clients

Ausgestellt am 400. Tag

Ergebnis

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

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

S3-Objektsperre

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

Kompatible ILM-Regel

„Ewig“ Speicherung von zwei Kopien auf Storage-Nodes

Anforderung zum Löschen des Clients

Herausgegeben am 2024-03-31

Ergebnis

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

So werden Objekte gelöscht

StorageGRID kann Objekte entweder als direkte Antwort auf eine Client-Anfrage oder automatisch aufgrund des Ablaufs eines S3-Bucket-Lebenszyklus oder der

Anforderungen der ILM-Richtlinie löschen. Wenn Sie verstehen, auf welche Weise Objekte gelöscht werden können und wie StorageGRID Löschanfragen verarbeitet, können Sie Objekte effizienter managen.

StorageGRID kann Objekte auf eine von zwei Methoden löschen:

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

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

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

Löschmethode	Wenn verwendet
Objekte werden zum Löschen in eine Warteschlange eingereiht	<p>Wenn eine der folgenden Bedingungen zutrifft:</p> <ul style="list-style-type: none"> • Das automatische Löschen von Objekten wurde von einem der folgenden Ereignisse ausgelöst: <ul style="list-style-type: none"> ◦ Das Ablaufdatum oder die Anzahl der Tage in der Lebenszykluskonfiguration für einen S3-Bucket erreicht ist. ◦ Der letzte in einer ILM-Regel angegebene Zeitraum ist abgelaufen. <p>Hinweis: Objekte in einem Bucket, für den S3 Object Lock aktiviert ist, können nicht gelöscht werden, wenn sie sich unter einem Legal Hold befinden oder wenn ein Aufbewahrungsdatum angegeben, aber noch nicht erfüllt wurde.</p> <ul style="list-style-type: none"> • Ein S3-Client fordert die Löschung an, und eine oder mehrere dieser Bedingungen sind zutreffend: <ul style="list-style-type: none"> ◦ Kopien können nicht innerhalb von 30 Sekunden gelöscht werden, da z. B. ein Objektspeicherort vorübergehend nicht verfügbar ist. ◦ Löschwarteschlangen im Hintergrund sind inaktiv.
Objekte werden sofort entfernt (synchrones Löschen)	<p>Wenn ein S3-Client eine Löschanfrage abgibt und alle der folgenden Bedingungen erfüllt sind:</p> <ul style="list-style-type: none"> • Alle Kopien können innerhalb von 30 Sekunden entfernt werden. • Warteschlangen zum Löschen im Hintergrund enthalten Objekte, die verarbeitet werden sollen.

Wenn S3-Clients Löschanforderungen durchführen, beginnt StorageGRID mit dem Hinzufügen von Objekten zur Löschwarteschlange. Anschließend wechselt er zur Durchführung des synchronen Löschvorgangs. Wenn sichergestellt wird, dass in der Warteschlange zum Löschen im Hintergrund Objekte verarbeitet werden, kann

StorageGRID das Löschen von Löschungen effizienter verarbeiten, insbesondere bei Clients mit geringer Parallelität. Gleichzeitig wird verhindert, dass die Backlogs von Clients gelöscht werden.

Erforderliche Zeit zum Löschen von Objekten

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

- Wenn StorageGRID das synchrone Löschen durchführt, kann StorageGRID bis zu 30 Sekunden dauern, bis ein Ergebnis an den Client zurückgegeben wird. Das heißt, das Löschen kann scheinbar langsamer erfolgen, auch wenn Kopien tatsächlich schneller entfernt werden als wenn StorageGRID Objekte zum Löschen Warteschlangen.
- Wenn Sie die Löschleistung beim Löschen eines Großteils genau überwachen, wird möglicherweise nach dem Löschen einer bestimmten Anzahl von Objekten die Löschrates zu langsam angezeigt. Diese Änderung tritt auf, wenn StorageGRID von Objekten aus der Warteschlange zum Löschen auf das synchrone Löschen verschiebt. Die offensichtliche Reduzierung der Löschrates bedeutet nicht, dass Objektkopien langsamer entfernt werden. Im Gegenteil: Er zeigt an, dass durchschnittlich Speicherplatz schneller freigegeben wird.

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

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

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

Löschen von S3-versionierten Objekten

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

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

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

Löscht ein Client eine Objektversion mit einer Versions-ID aus einem "Asteimer", StorageGRID verbirgt die Existenz der Objektversion, erstellt jedoch keine Löschmarkierung im Branch-Bucket. Wenn ein Client ein Objekt ohne Versions-ID aus einem Branch-Bucket löscht, erstellt StorageGRID gemäß dem Standardverhalten von S3 eine Löschmarkierung im Branch-Bucket.

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

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

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

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

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

Um abgelaufene Objektlöschmarkierungen zu entfernen, verwenden Sie eine **Ingest Time**-Regel, um den aktuellen Löschmarkierungen zu entsprechen. Löschmarkierungen werden nur entfernt, wenn ein **Zeitraum** von **Tagen** abgelaufen ist und der aktuelle Löschmarker abgelaufen ist (es gibt keine nicht-aktuellen Versionen).

- **Objekte im Bucket löschen:** Verwenden Sie den Tenant Manager "[Löschen Sie alle Objektversionen](#)", um Marker aus einem Bucket zu löschen.

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

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

Verwandte Informationen

- "[S3-REST-API VERWENDEN](#)"

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

Copyright-Informationen

Copyright © 2026 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtsinhabers in keiner Form und durch keine Mittel – weder grafische noch elektronische oder mechanische, einschließlich Fotokopieren, Aufnehmen oder Speichern in einem elektronischen Abrufsystem – auch nicht in Teilen, vervielfältigt werden.

Software, die von urheberrechtlich geschütztem NetApp Material abgeleitet wird, unterliegt der folgenden Lizenz und dem folgenden Haftungsausschluss:

DIE VORLIEGENDE SOFTWARE WIRD IN DER VORLIEGENDEN FORM VON NETAPP ZUR VERFÜGUNG GESTELLT, D. H. OHNE JEGLICHE EXPLIZITE ODER IMPLIZITE GEWÄHRLEISTUNG, EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE STILLSCHWEIGENDE GEWÄHRLEISTUNG DER MARKTGÄNGIGKEIT UND EIGNUNG FÜR EINEN BESTIMMTEN ZWECK, DIE HIERMIT AUSGESCHLOSSEN WERDEN. NETAPP ÜBERNIMMT KEINERLEI HAFTUNG FÜR DIREKTE, INDIREKTE, ZUFÄLLIGE, BESONDERE, BEISPIELHAFT SCHÄDEN ODER FOLGESCHÄDEN (EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE BESCHAFFUNG VON ERSATZWAREN ODER -DIENSTLEISTUNGEN, NUTZUNGS-, DATEN- ODER GEWINNVERLUSTE ODER UNTERBRECHUNG DES GESCHÄFTSBETRIEBS), UNABHÄNGIG DAVON, WIE SIE VERURSACHT WURDEN UND AUF WELCHER HAFTUNGSTHEORIE SIE BERUHEN, OB AUS VERTRAGLICH FESTGELEGTER HAFTUNG, VERSCHULDENSUNABHÄNGIGER HAFTUNG ODER DELIKTSHAFTUNG (EINSCHLIESSLICH FAHRLÄSSIGKEIT ODER AUF ANDEREM WEGE), DIE IN IRGEND EINER WEISE AUS DER NUTZUNG DIESER SOFTWARE RESULTIEREN, SELBST WENN AUF DIE MÖGLICHKEIT DERARTIGER SCHÄDEN HINGEWIESEN WURDE.

NetApp behält sich das Recht vor, die hierin beschriebenen Produkte jederzeit und ohne Vorankündigung zu ändern. NetApp übernimmt keine Verantwortung oder Haftung, die sich aus der Verwendung der hier beschriebenen Produkte ergibt, es sei denn, NetApp hat dem ausdrücklich in schriftlicher Form zugestimmt. Die Verwendung oder der Erwerb dieses Produkts stellt keine Lizenzierung im Rahmen eines Patentrechts, Markenrechts oder eines anderen Rechts an geistigem Eigentum von NetApp dar.

Das in diesem Dokument beschriebene Produkt kann durch ein oder mehrere US-amerikanische Patente, ausländische Patente oder anhängige Patentanmeldungen geschützt sein.

ERLÄUTERUNG ZU „RESTRICTED RIGHTS“: Nutzung, Vervielfältigung oder Offenlegung durch die US-Regierung unterliegt den Einschränkungen gemäß Unterabschnitt (b)(3) der Klausel „Rights in Technical Data – Noncommercial Items“ in DFARS 252.227-7013 (Februar 2014) und FAR 52.227-19 (Dezember 2007).

Die hierin enthaltenen Daten beziehen sich auf ein kommerzielles Produkt und/oder einen kommerziellen Service (wie in FAR 2.101 definiert) und sind Eigentum von NetApp, Inc. Alle technischen Daten und die Computersoftware von NetApp, die unter diesem Vertrag bereitgestellt werden, sind gewerblicher Natur und wurden ausschließlich unter Verwendung privater Mittel entwickelt. Die US-Regierung besitzt eine nicht ausschließliche, nicht übertragbare, nicht unterlizenzierbare, weltweite, limitierte unwiderrufliche Lizenz zur Nutzung der Daten nur in Verbindung mit und zur Unterstützung des Vertrags der US-Regierung, unter dem die Daten bereitgestellt wurden. Sofern in den vorliegenden Bedingungen nicht anders angegeben, dürfen die Daten ohne vorherige schriftliche Genehmigung von NetApp, Inc. nicht verwendet, offengelegt, vervielfältigt, geändert, aufgeführt oder angezeigt werden. Die Lizenzrechte der US-Regierung für das US-Verteidigungsministerium sind auf die in DFARS-Klausel 252.227-7015(b) (Februar 2014) genannten Rechte beschränkt.

Markeninformationen

NETAPP, das NETAPP Logo und die unter <http://www.netapp.com/TM> aufgeführten Marken sind Marken von NetApp, Inc. Andere Firmen und Produktnamen können Marken der jeweiligen Eigentümer sein.