S3 Object Lock verwenden

StorageGRID software

NetApp
July 23, 2026

Inhalt

S3 Object Lock verwenden . . . 1
- Wie S3 Object Lock Objekte in StorageGRID schützt . . . 1
  - Was ist S3 Object Lock? . . . 1
  - Vergleich der S3 Object Lock mit der herkömmlichen Compliance . . . 2
- S3 Object Lock-Workflow in StorageGRID . . . 4
- S3 Object Lock-Anforderungen in StorageGRID . . . 5
  - Voraussetzungen für die Verwendung der globalen S3 Object Lock-Einstellung . . . 5
  - Anforderungen an konforme ILM Regeln . . . 5
  - Anforderungen an ILM Richtlinien . . . 6
  - Anforderungen für Buckets mit aktiviertem S3 Object Lock . . . 6
  - Anforderungen an Objekte in Buckets mit aktiviertem S3 Object Lock . . . 6
  - Lebenszyklus von Objekten in Buckets mit aktiviertem S3 Object Lock . . . 6
- Aktivieren Sie die S3 Object Lock global in StorageGRID . . . 7
- Beheben Sie Konsistenzfehler beim Aktualisieren von S3 Object Lock oder älteren Compliance-Einstellungen in StorageGRID . . . 8

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.
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.

	S3 Object Lock	Compliance (Legacy)
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"