



Management von S3-Buckets

StorageGRID

NetApp

November 04, 2025

This PDF was generated from <https://docs.netapp.com/de-de/storagegrid-117/tenant/creating-s3-bucket.html> on November 04, 2025. Always check docs.netapp.com for the latest.

Inhalt

Management von S3-Buckets	1
Erstellen eines S3-Buckets	1
Greifen Sie auf den Assistenten zu	1
Geben Sie Details ein	1
Verwalten von Objekteinstellungen	2
Bucket-Details anzeigen	4
Ändern der Konsistenzstufe eines Buckets	5
Aktiviert bzw. deaktiviert Updates der letzten Zugriffszeit	6
Ändern Sie die Objektversionierung für einen Bucket	8
Verwenden Sie S3 Objektsperre, um Objekte beizubehalten	9
Was ist S3 Object Lock?	9
S3-Objektsperre-Workflow	11
Anforderungen für Buckets, bei denen die S3-Objektsperre aktiviert ist	12
Anforderungen für Objekte in Buckets, bei denen die S3-Objektsperre aktiviert ist	13
Lebenszyklus von Objekten in Buckets, wobei S3 Objektsperre aktiviert ist	13
Kann ich auch ältere konforme Buckets verwalten?	13
Aktualisieren Sie die S3 Object Lock-Standaufbewahrung	14
Konfiguration der Cross-Origin Resource Sharing (CORS)	15
CORS für einen Bucket aktivieren	15
CORS-Einstellung ändern	16
Deaktivieren Sie die CORS-Einstellung	16
Löschen von Objekten in Bucket	17
S3-Bucket löschen	20
Verwenden Sie die Experimental S3-Konsole	20

Management von S3-Buckets

Erstellen eines S3-Buckets

Sie können im Mandanten-Manager S3-Buckets für Objektdaten erstellen.

Bevor Sie beginnen

- Sie sind mit einem beim Mandantenmanager angemeldet "[Unterstützter Webbrowser](#)".
- Sie gehören einer Benutzergruppe an, die über den Root-Zugriff oder Alle Buckets verwalten verfügt "[Berechtigung](#)". Diese Berechtigungen überschreiben die Berechtigungseinstellungen in Gruppen- oder Bucket-Richtlinien.



Berechtigungen zum Festlegen oder Ändern der S3-Objektsperreigenschaften von Buckets oder Objekten können von erteilt werden "[Bucket-Richtlinie oder Gruppenrichtlinie](#)".

- Wenn Sie die S3-Objektsperrung für einen Bucket aktivieren möchten, hat ein Grid-Administrator die globale S3-Objektsperrung für das StorageGRID-System aktiviert, und Sie haben die Anforderungen für S3-Objektsperrbuckets und -Objekte geprüft. Siehe "[Verwenden Sie S3 Objektsperre, um Objekte beizubehalten](#)".

Greifen Sie auf den Assistenten zu

Schritte

1. Wählen Sie **View Buckets** aus dem Dashboard, oder wählen Sie **STORAGE (S3) > Buckets**.
2. Wählen Sie **Eimer erstellen**.

Geben Sie Details ein

Schritte

1. Geben Sie Details für den Bucket ein.

Feld	Beschreibung
Bucket-Name	<p>Ein Name für den Bucket, der die folgenden Regeln erfüllt:</p> <ul style="list-style-type: none"> • Jedes StorageGRID System muss eindeutig sein (nicht nur innerhalb des Mandantenkontos). • Muss DNS-konform sein. • Darf mindestens 3 und nicht mehr als 63 Zeichen enthalten. • Jedes Etikett muss mit einem Kleinbuchstaben oder einer Zahl beginnen und enden. Es können nur Kleinbuchstaben, Ziffern und Bindestriche verwendet werden. • Perioden sollten nicht in Anforderungen im virtuellen gehosteten Stil verwendet werden. Perioden verursachen Probleme bei der Überprüfung des Server-Platzhalterzertifikats. <p>Weitere Informationen finden Sie im ""Dokumentation der Amazon Web Services (AWS) zu den Bucket-Benennungsregeln".</p> <p>Hinweis: Sie können den Bucket-Namen nicht ändern, nachdem Sie den Bucket erstellt haben.</p>
Region	<p>Der Bereich des Eimers.</p> <p>Der StorageGRID-Administrator managt die verfügbaren Regionen. Die Regionen eines Buckets können die Datensicherungsrichtlinie, die auf Objekte angewendet wird, beeinflussen. Standardmäßig werden alle Buckets im erstellt us-east-1 Werden.</p> <p>Hinweis: Sie können die Region nicht ändern, nachdem Sie den Bucket erstellt haben.</p>

2. Wählen Sie **Weiter**.

Verwalten von Objekteinstellungen

Schritte

1. Aktivieren Sie optional die Objektversionierung für den Bucket.

Aktivieren Sie die Objektversionierung, wenn Sie jede Version jedes Objekts in diesem Bucket speichern möchten. Sie können dann nach Bedarf frühere Versionen eines Objekts abrufen. Sie müssen die Objektversionierung aktivieren, wenn der Bucket für die Grid-übergreifende Replizierung verwendet wird.

2. Wenn die globale S3 Object Lock-Einstellung aktiviert ist, können Sie optional S3 Object Lock für den Bucket aktivieren, um Objekte mithilfe eines WORM-Modells (Write-Once-Read-Many) zu speichern.

Aktivieren Sie die S3-Objektsperre für einen Bucket nur, wenn Objekte z. B. für eine bestimmte Zeit aufbewahrt werden müssen, um bestimmte gesetzliche Vorgaben zu erfüllen. S3 Object Lock ist eine permanente Einstellung, mit der Sie verhindern können, dass Objekte für einen festgelegten Zeitraum oder für einen unbegrenzten Zeitraum gelöscht oder überschrieben werden.



Nachdem die S3-Objektsperrung für einen Bucket aktiviert ist, kann sie nicht deaktiviert werden. Jeder mit den richtigen Berechtigungen kann diesem Bucket Objekte hinzufügen, die nicht geändert werden können. Sie können diese Objekte oder den Bucket selbst möglicherweise nicht löschen.

Wenn Sie S3 Object Lock für einen Bucket aktivieren, wird die Bucket-Versionierung automatisch aktiviert.

3. Wenn Sie **S3 Object Lock aktivieren** ausgewählt haben, aktivieren Sie optional **Default Retention** für diesen Bucket.

Wenn **Default Retention** aktiviert ist, werden neue Objekte, die dem Bucket hinzugefügt werden, automatisch vor dem Löschen oder Überschreiben geschützt. Die Einstellung **Default Retention** gilt nicht für Objekte mit eigenen Aufbewahrungsfristen.

- a. Wenn **Default Retention** aktiviert ist, geben Sie einen **Default Retention Mode** für den Bucket an.

Standardaufbewahrungsmode	Beschreibung
Compliance	<ul style="list-style-type: none">Das Objekt kann erst gelöscht werden, wenn das Aufbewahrungsdatum erreicht ist.Das Aufbewahrungsdatum des Objekts kann erhöht, aber nicht verringert werden.Das Aufbewahrungsdatum des Objekts kann erst entfernt werden, wenn dieses Datum erreicht ist.
Governance	<ul style="list-style-type: none">Benutzer mit s3:BypassGovernanceRetention Berechtigung kann den verwenden x-amz-bypass-governance-retention: true Kopfzeile anfordern, um Aufbewahrungseinstellungen zu umgehen.Diese Benutzer können eine Objektversion löschen, bevor das Aufbewahrungsdatum erreicht ist.Diese Benutzer können das Aufbewahrungsdatum eines Objekts erhöhen, verringern oder entfernen.

- b. Wenn **Default Retention** aktiviert ist, geben Sie die **Default Retention Period** für den Bucket an.

Die **Default Retention Period** gibt an, wie lange neue Objekte zu diesem Bucket hinzugefügt werden sollen, beginnend mit dem Zeitpunkt, zu dem sie aufgenommen werden. Geben Sie einen Wert zwischen 1 und 36,500 Tagen oder zwischen 1 und 100 Jahren an, einschließlich.

4. Wählen Sie **Eimer erstellen**.

Der Bucket wird erstellt und der Tabelle auf der Seite Buckets hinzugefügt.

5. Wählen Sie optional **Gehe zur Seite mit den Bucket-Details** zu "[Bucket-Details anzeigen](#)" Und zusätzliche Konfiguration durchführen.

Bucket-Details anzeigen

Sie können die Buckets in Ihrem Mandantenkonto anzeigen.

Bevor Sie beginnen

- Sie sind mit einem beim Mandantenmanager angemeldet "[Unterstützter Webbrowser](#)".

Schritte

1. Wählen Sie **View Buckets** aus dem Dashboard, oder wählen Sie **STORAGE (S3) > Buckets**.

Die Seite „Buckets“ wird angezeigt.

2. Überprüfen Sie die Zusammenfassungsinformationen für jeden Bucket.

Bei Bedarf können Sie die Informationen nach einer beliebigen Spalte sortieren oder Sie können die Seite vorwärts und zurück durch die Liste blättern.



Die angezeigten Werte für Objektanzahl und verwendeter Speicherplatz sind Schätzungen.

Diese Schätzungen sind vom Zeitpunkt der Aufnahme, der Netzwerkverbindung und des Node-Status betroffen. Wenn Buckets die Versionierung aktiviert ist, sind gelöschte Objektversionen in der Objektanzahl enthalten.

Spalte	Beschreibung
Name	Der eindeutige Name des Buckets, der nicht geändert werden kann.
Aktivierte Funktionen	Die Liste der Funktionen, die für den Bucket aktiviert sind.
S3-Objektsperre	Gibt an, ob S3 Object Lock für den Bucket aktiviert ist. Diese Spalte wird nur angezeigt, wenn die S3-Objektsperre für das Raster aktiviert ist. In dieser Spalte werden außerdem Informationen für alle Buckets angezeigt, die für die Konformität mit älteren Daten verwendet wurden.
Region	Der Bereich des Eimers, der nicht geändert werden kann.
Objektanzahl	Die Anzahl der Objekte in diesem Bucket. Wenn Objekte hinzugefügt oder gelöscht werden, wird dieser Wert möglicherweise nicht sofort aktualisiert. Wenn für Buckets die Versionierung aktiviert ist, sind nicht aktuelle Objektversionen in diesem Wert enthalten.
Belegten Speicherplatz	Die logische Größe aller Objekte im Bucket. Die logische Größe umfasst nicht den tatsächlich benötigten Speicherplatz für replizierte oder Erasure Coding-Kopien oder für Objekt-Metadaten.
Erstellungsdatum	Datum und Uhrzeit der Erstellung des Buckets.

3. Um Details für einen bestimmten Bucket anzuzeigen, wählen Sie den Bucket-Namen aus der Tabelle aus.

Die Seite mit den Bucket-Details wird angezeigt. Auf dieser Seite können Sie die folgenden Aufgaben

ausführen:

- Konfigurieren und Managen von Bucket-Optionen wie z. B. "[Konsistenzstufe](#)", "[Aktualisierung der Uhrzeit des letzten Zugriffs](#)", "[Objektversionierung](#)", "[S3-Objektsperre](#)" Und "[Standardmäßige Bucket-Aufbewahrung](#)"
- Konfigurieren Sie den Bucket-Zugriff, z. B. "[Cross-Origin Resource Sharing \(CORS\)](#)"
- Managen "[Plattform-Services](#)" (Falls für den Mandanten erlaubt), einschließlich Replikation, Ereignisbenachrichtigungen und Suchintegration
- Aktivieren Sie und "[Grid-übergreifende Replizierung managen](#)" (Falls dies für den Mandanten zulässig ist) zum Replizieren von Objekten, die in diesen Bucket aufgenommen wurden, auf ein anderes StorageGRID-System
- Auf das zugreifen "[Experimentelle S3-Konsole](#)" Zum Verwalten der Objekte im Bucket
- "[Löschen aller Objekte in einem Bucket](#)"
- "[Löschen eines Buckets](#)" Das ist bereits leer

Ändern der Konsistenzstufe eines Buckets

Wenn Sie einen S3-Mandanten verwenden, können Sie die Konsistenzstufe für Vorgänge ändern, die für die Objekte in S3-Buckets ausgeführt werden.

Bevor Sie beginnen

- Sie sind mit einem beim Mandantenmanager angemeldet "[Unterstützter Webbrowser](#)".
- Sie gehören einer Benutzergruppe an, die über den verfügt "[Managen aller Buckets oder Root-Zugriffsberechtigungen](#)". Diese Berechtigungen überschreiben die Berechtigungseinstellungen in Gruppen- oder Bucket-Richtlinien.

Über diese Aufgabe

Konsistenzkontrollen bieten ein Gleichgewicht zwischen der Verfügbarkeit der Objekte und der Konsistenz dieser Objekte über verschiedene Storage Nodes und Standorte hinweg. Im Allgemeinen sollten Sie für Ihre Buckets die Konsistenzstufe **Read-after-New-write** verwenden.

Wenn die Konsistenzstufe **Read-after-New-write** nicht den Anforderungen der Client-Anwendung entspricht, können Sie die Konsistenzstufe ändern, indem Sie die Bucket-Konsistenzstufe oder die verwenden **Consistency-Control** Kopfzeile. Der **Consistency-Control** Kopfzeile setzt die Bucket-Konsistenzstufe außer Kraft.



Wenn Sie die Konsistenzstufe eines Buckets ändern, werden nur die Objekte, die nach der Änderung aufgenommen werden, garantiert, um die überarbeitete Ebene zu erfüllen.

Schritte

1. Wählen Sie **View Buckets** aus dem Dashboard, oder wählen Sie **STORAGE (S3) > Buckets**.
 2. Wählen Sie den Bucket-Namen aus der Tabelle aus.
- Die Seite mit den Bucket-Details wird angezeigt.
3. Wählen Sie auf der Registerkarte **Bucket options** das Akkordeon **Consistency Level** aus.
 4. Wählen Sie eine Konsistenzstufe für Operationen aus, die an den Objekten in diesem Bucket durchgeführt werden.

- **All:** Bietet die höchste Konsistenz. Alle Nodes erhalten die Daten sofort, sonst schlägt die Anfrage fehl.
- **Strong-global:** Garantiert Lese-nach-Schreiben-Konsistenz für alle Client-Anfragen über alle Standorte hinweg.
- **Strong-site:** Garantiert Lese-nach-Schreiben Konsistenz für alle Client-Anfragen innerhalb einer Site.
- **Read-after-New-write** (default): 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.

5. Wählen Sie **Änderungen speichern**.

Aktiviert bzw. deaktiviert Updates der letzten Zugriffszeit

Wenn Grid-Administratoren die Regeln für das Information Lifecycle Management (ILM) für ein StorageGRID-System erstellen, können sie optional angeben, dass die letzte Zugriffszeit eines Objekts verwendet wird, um zu bestimmen, ob das Objekt auf einen anderen Storage-Standort verschoben werden soll. Wenn Sie einen S3-Mandanten verwenden, können Sie diese Regeln nutzen, indem Sie Updates der letzten Zugriffszeit für die Objekte in einem S3-Bucket aktivieren.

Diese Anweisungen gelten nur für StorageGRID-Systeme, die mindestens eine ILM-Regel enthalten, die die Option **Letzte Zugriffszeit** als erweiterten Filter oder als Referenzzeit verwendet. Sie können diese Anweisungen ignorieren, wenn Ihr StorageGRID System eine solche Regel nicht enthält. Siehe "["Verwenden Sie die letzte Zugriffszeit in ILM-Regeln"](#) Entsprechende Details.

Bevor Sie beginnen

- Sie sind mit einem beim Mandantenmanager angemeldet "["Unterstützter Webbrowser"](#)".
- Sie gehören einer Benutzergruppe an, die über den verfügt "["Managen aller Buckets oder Root-Zugriffsberechtigungen"](#)". Diese Berechtigungen überschreiben die Berechtigungseinstellungen in Gruppen- oder Bucket-Richtlinien.

Über diese Aufgabe

Letzte Zugriffszeit ist eine der Optionen für die **Referenzzeit**-Platzierungsanweisung für eine ILM-Regel. Durch Festlegen der Referenzzeit für eine Regel auf Letzte Zugriffszeit können Grid-Administratoren festlegen, dass Objekte an bestimmten Speicherorten platziert werden, basierend auf dem Zeitpunkt, zu dem diese Objekte zuletzt abgerufen (gelesen oder angezeigt) wurden.

Um z. B. sicherzustellen, dass kürzlich angezeigte Objekte im schnelleren Storage verbleiben, kann ein Grid-Administrator eine ILM-Regel erstellen, die Folgendes angibt:

- Objekte, die im letzten Monat abgerufen wurden, sollten auf lokalen Speicherknoten verbleiben.
- Objekte, die im letzten Monat nicht abgerufen wurden, sollten an einen externen Standort verschoben werden.

Standardmäßig werden Updates zur letzten Zugriffszeit deaktiviert. Wenn Ihr StorageGRID System eine ILM-Regel enthält, die die Option **Uhrzeit des letzten Zugriffs** verwendet, und Sie möchten, dass diese Option auf Objekte in diesem Bucket angewendet wird, müssen Sie für die in dieser Regel angegebenen S3-Buckets

Updates für den letzten Zugriff aktivieren.



Durch das Aktualisieren der letzten Zugriffszeit, zu der ein Objekt abgerufen wird, kann sich die StorageGRID-Performance insbesondere für kleine Objekte reduzieren.

Eine Performance-Beeinträchtigung wird durch die letzten Updates der Zugriffszeit beeinflusst, da StorageGRID jedes Mal, wenn Objekte abgerufen werden, die folgenden zusätzlichen Schritte durchführen muss:

- Aktualisieren Sie die Objekte mit neuen Zeitstempel
- Fügen Sie die Objekte zur ILM-Warteschlange hinzu, damit sie anhand aktueller ILM-Regeln und Richtlinien neu bewertet werden können

Die Tabelle fasst das Verhalten zusammen, das auf alle Objekte im Bucket angewendet wird, wenn die letzte Zugriffszeit deaktiviert oder aktiviert ist.

Art der Anfrage	Verhalten, wenn die letzte Zugriffszeit deaktiviert ist (Standard)		Verhalten, wenn die letzte Zugriffszeit aktiviert ist	
	Zeitpunkt des letzten Zugriffs aktualisiert?	Das Objekt wurde zur ILM-Auswertungswarteschlange hinzugefügt?	Zeitpunkt des letzten Zugriffs aktualisiert?	Das Objekt wurde zur ILM-Auswertungswarteschlange hinzugefügt?
Anforderung zum Abrufen eines Objekts, seiner Zugriffssteuerungsliste oder seiner Metadaten	Nein	Nein	Ja.	Ja.
Anforderung zum Aktualisieren der Metadaten eines Objekts	Ja.	Ja.	Ja.	Ja.
Anforderung zum Kopieren eines Objekts von einem Bucket in einen anderen	<ul style="list-style-type: none">• Nein, für die Quellkopie• Ja, für die Zielkopie	<ul style="list-style-type: none">• Nein, für die Quellkopie• Ja, für die Zielkopie	<ul style="list-style-type: none">• Ja, für die Quellkopie• Ja, für die Zielkopie	<ul style="list-style-type: none">• Ja, für die Quellkopie• Ja, für die Zielkopie
Anforderung zum Abschließen eines mehrteiligen Uploads	Ja, für das zusammengesetzte Objekt	Ja, für das zusammengesetzte Objekt	Ja, für das zusammengesetzte Objekt	Ja, für das zusammengesetzte Objekt

Schritte

1. Wählen Sie **View Buckets** aus dem Dashboard, oder wählen Sie **STORAGE (S3) > Buckets**.
2. Wählen Sie den Bucket-Namen aus der Tabelle aus.

Die Seite mit den Bucket-Details wird angezeigt.

3. Wählen Sie auf der Registerkarte **Bucket options** das Akkordeon **Letzte Zugriffszeit-Updates** aus.
4. Aktivieren oder deaktivieren Sie die Zeitaktualisierungen für den letzten Zugriff.
5. Wählen Sie **Änderungen speichern**.

Ändern Sie die Objektversionierung für einen Bucket

Wenn Sie einen S3-Mandanten verwenden, können Sie den Versionsstatus für S3-Buckets ändern.

Bevor Sie beginnen

- Sie sind mit einem beim Mandantenmanager angemeldet "[Unterstützter Webbrowser](#)".
- Sie gehören einer Benutzergruppe an, die über den verfügt "[Managen aller Buckets oder Root-Zugriffsberechtigungen](#)". Diese Berechtigungen überschreiben die Berechtigungseinstellungen in Gruppen- oder Bucket-Richtlinien.

Über diese Aufgabe

Sie können die Objektversionierung für einen Bucket aktivieren oder aussetzen. Nachdem Sie die Versionierung für einen Bucket aktiviert haben, kann dieser nicht in den Status „unversioniert“ zurückkehren. Sie können die Versionierung für den Bucket jedoch unterbrechen.

- Deaktiviert: Versionierung wurde noch nie aktiviert
- Aktiviert: Versionierung ist aktiviert
- Suspendiert: Die Versionierung war zuvor aktiviert und wird ausgesetzt

Weitere Informationen finden Sie im Folgenden:

- "[Objektversionierung](#)"
- "[ILM-Regeln und Richtlinien für versionierte S3-Objekte \(Beispiel 4\)](#)"
- "[So werden Objekte gelöscht](#)"

Schritte

1. Wählen Sie **View Buckets** aus dem Dashboard, oder wählen Sie **STORAGE (S3) > Buckets**.
2. Wählen Sie den Bucket-Namen aus der Tabelle aus.

Die Seite mit den Bucket-Details wird angezeigt.

3. Wählen Sie auf der Registerkarte **Bucket options** das Akkordeon **Object Versioning** aus.
4. Wählen Sie einen Versionierungsstatus für die Objekte in diesem Bucket aus.

Die Objektversionierung muss für einen Bucket aktiviert bleiben, der für die Grid-übergreifende Replizierung verwendet wurde. Wenn die S3-Objektsperre oder die ältere Compliance aktiviert ist, sind die Optionen **Objektversionierung** deaktiviert.

Option	Beschreibung
Aktivieren Sie die Versionierung	<p>Aktivieren Sie die Objektversionierung, wenn Sie jede Version jedes Objekts in diesem Bucket speichern möchten. Sie können dann nach Bedarf frühere Versionen eines Objekts abrufen.</p> <p>Objekte, die sich bereits im Bucket befanden, werden versioniert, wenn sie von einem Benutzer geändert werden.</p>
Die Versionierung unterbrechen	<p>Unterbrechen Sie die Objektversionierung, wenn Sie keine neuen Objektversionen mehr erstellen möchten. Sie können weiterhin alle vorhandenen Objektversionen abrufen.</p>

5. Wählen Sie **Änderungen speichern**.

Verwenden Sie S3 Objektsperre, um Objekte beizubehalten

Sie können S3 Object Lock verwenden, wenn Buckets und Objekte die gesetzlichen Aufbewahrungsanforderungen erfüllen müssen.

Was ist S3 Object Lock?

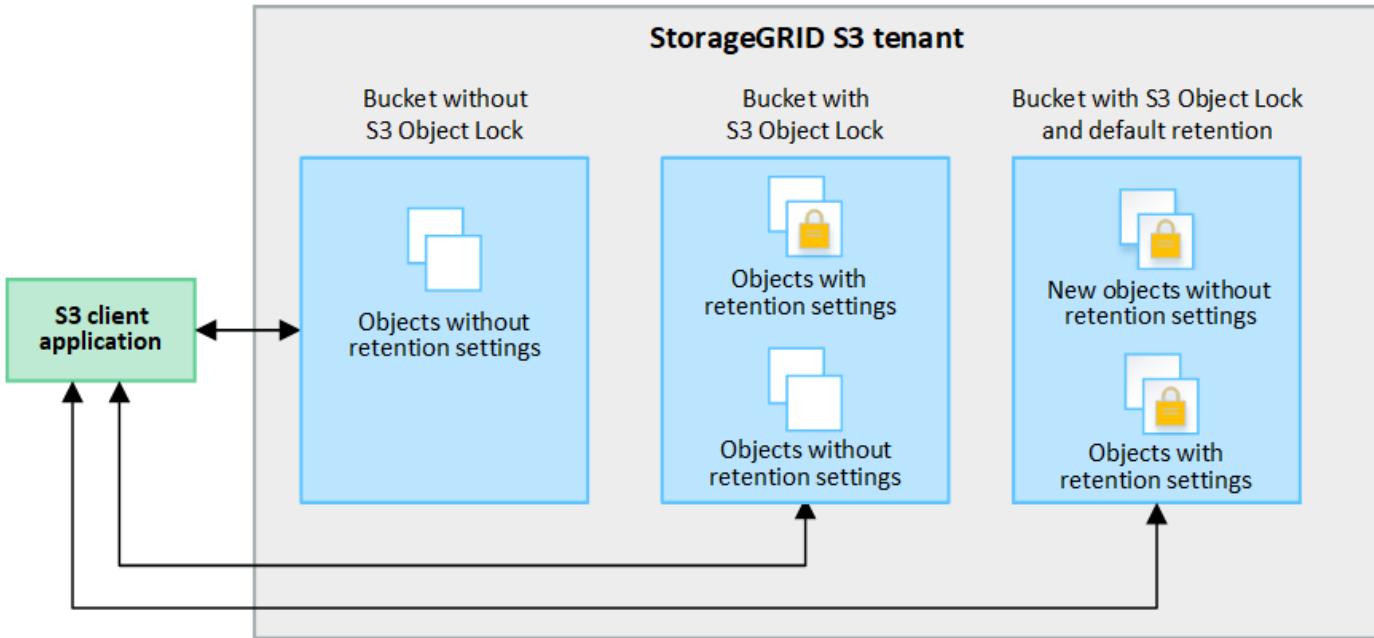
Die Funktion StorageGRID S3 Object Lock ist eine Objektschutzlösung, die der S3 Object Lock in Amazon Simple Storage Service (Amazon S3) entspricht.

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

Wenn für einen Bucket die S3 Object Lock aktiviert ist, können S3-Client-Applikationen optional Aufbewahrungseinstellungen für jede Objektversion angeben, die in diesem Bucket gespeichert ist.

Darüber hinaus kann für einen Bucket, auf dem die S3 Object Lock aktiviert ist, optional ein Standardaufbewahrungsmodus und ein Aufbewahrungszeitraum verwendet werden. Die Standardeinstellungen gelten nur für Objekte, die ohne eigene Aufbewahrungseinstellungen zum Bucket hinzugefügt werden.

StorageGRID with S3 Object Lock setting enabled



Aufbewahrungsmodi

Die Objektsperrfunktion StorageGRID S3 unterstützt zwei Aufbewahrungsmodi, um verschiedene Schutzstufen auf Objekte anzuwenden. Diese Modi entsprechen den Amazon S3 Aufbewahrungsmodi.

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

Aufbewahrungseinstellungen für Objektversionen

Wenn ein Bucket mit aktiverter S3-Objektsperrung erstellt wird, können Benutzer mithilfe der S3-Client-Applikation optional die folgenden Aufbewahrungseinstellungen für jedes Objekt angeben, das dem Bucket hinzugefügt wird:

- **Retention Mode:** Entweder Compliance oder Governance.
- **Rebeat-until-date:** Wenn das Aufbewahrungsdatum einer Objektversion in der Zukunft liegt, kann das Objekt abgerufen, aber nicht gelöscht werden.
- **Legal Hold:** Die Anwendung eines gesetzlichen Hold auf eine Objektversion sperrt diesen Gegenstand sofort. Beispielsweise müssen Sie ein Objekt, das mit einer Untersuchung oder einem Rechtsstreit zusammenhängt, rechtlich festhalten. Eine gesetzliche Aufbewahrungspflichten haben kein Ablaufdatum, bleiben aber bis zur ausdrücklichen Entfernung erhalten. Die gesetzlichen Aufbewahrungspflichten sind unabhängig von der bisherigen Aufbewahrungsfrist.



Befindet sich ein Objekt unter einer Legal Hold-Funktion, kann das Objekt unabhängig vom Aufbewahrungsmodus nicht gelöscht werden.

Weitere Informationen zu den Objekteinstellungen finden Sie unter ["Konfigurieren Sie die S3-Objektsperre über die S3-REST-API"](#).

Standardeinstellung für die Aufbewahrung von Buckets

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

- **Default Retention Mode:** Entweder Compliance oder Governance.
- **Default Retention Period:** Wie lange neue Objektversionen, die zu diesem Bucket hinzugefügt wurden, beibehalten werden sollen, beginnend mit dem Tag, an dem sie hinzugefügt werden.

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

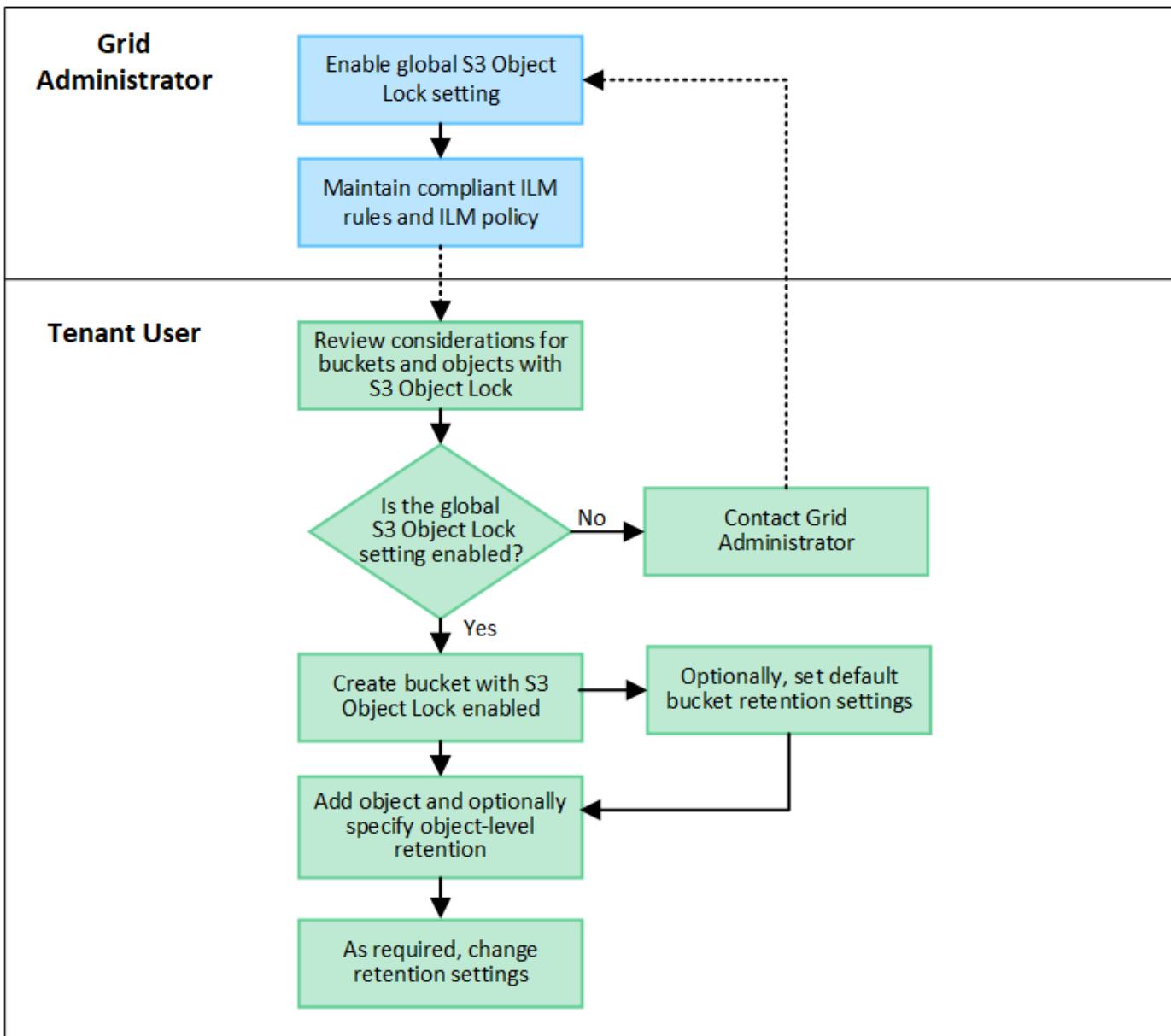
Siehe ["Erstellen eines S3-Buckets"](#) Und ["Aktualisieren Sie die S3 Object Lock-Standardaufbewahrung"](#).

S3-Objektsperre-Workflow

Das Workflow-Diagramm zeigt die grundlegenden Schritte zur Verwendung der S3-Objektsperre in StorageGRID.

Bevor Sie Buckets mit aktivierter S3-Objektsperre erstellen können, muss der Grid-Administrator die globale S3-Objektsperreinstellung für das gesamte StorageGRID-System aktivieren. Der Grid-Administrator muss außerdem sicherstellen, dass die Richtlinie für das Information Lifecycle Management (ILM) „konform“ ist; sie muss die Anforderungen von Buckets erfüllen, wenn S3 Object Lock aktiviert ist. Weitere Informationen erhalten Sie von Ihrem Grid-Administrator oder in den Anweisungen für ["Managen von Objekten mit S3 Object Lock"](#).

Nachdem die globale S3 Object Lock-Einstellung aktiviert wurde, können Sie Buckets erstellen, für die S3 Object Lock aktiviert ist, und optional für jeden Bucket Standardaufbewahrungseinstellungen festlegen. Darüber hinaus können Sie mit der S3-Client-Anwendung optional Aufbewahrungseinstellungen für jede Objektversion angeben.



Anforderungen für Buckets, bei denen die S3-Objektsperre aktiviert ist

- Wenn die globale S3-Objektsperre für das StorageGRID System aktiviert ist, können Sie die Buckets mit aktiver S3-Objektsperre über den Mandantenmanager, die Mandantenmanagement-API oder die S3-REST-API erstellen.
- Wenn Sie die S3-Objektsperre verwenden möchten, müssen Sie beim Erstellen des Buckets die S3-Objektsperre aktivieren. Sie können die S3-Objektsperre für einen vorhandenen Bucket nicht aktivieren.
- Wenn die S3-Objektsperre für einen Bucket aktiviert ist, ermöglicht StorageGRID automatisch die Versionierung für diesen Bucket. Sie können S3 Object Lock nicht deaktivieren oder die Versionierung für den Bucket nicht unterbrechen.
- Optional können Sie mithilfe von Tenant Manager, der Mandanten-Management-API oder der S3-REST-API für jeden Bucket einen Standardaufbewahrungsmodus und einen Aufbewahrungszeitraum angeben. Die Standardaufbewahrungseinstellungen des Buckets gelten nur für neue Objekte, die dem Bucket hinzugefügt wurden und keine eigenen Aufbewahrungseinstellungen haben. Sie können diese Standardeinstellungen außer Kraft setzen, indem Sie einen Aufbewahrungsmodus und das Aufbewahrungsdatum für jede Objektversion festlegen, wenn sie hochgeladen wird.

- Die Konfiguration des Bucket-Lebenszyklus wird für Buckets unterstützt, für die S3 Object Lock aktiviert ist.
- Die CloudMirror-Replizierung wird für Buckets nicht unterstützt, wenn S3-Objektsperre aktiviert ist.

Anforderungen für Objekte in Buckets, bei denen die S3-Objektsperre aktiviert ist

- Zum Schutz einer Objektversion können Sie Standardaufbewahrungseinstellungen für den Bucket angeben oder Aufbewahrungseinstellungen für jede Objektversion angeben. Aufbewahrungseinstellungen auf Objektebene können mit der S3-Client-Applikation oder der S3-REST-API angegeben werden.
- Aufbewahrungseinstellungen gelten für einzelne Objektversionen. Eine Objektversion kann sowohl eine Aufbewahrungsfrist als auch eine gesetzliche Haltungseinstellung haben, eine jedoch nicht die andere oder keine. Wenn Sie eine Aufbewahrungsfrist oder eine gesetzliche Aufbewahrungseinstellung für ein Objekt angeben, wird nur die in der Anforderung angegebene Version geschützt. Sie können neue Versionen des Objekts erstellen, während die vorherige Version des Objekts gesperrt bleibt.

Lebenszyklus von Objekten in Buckets, wobei S3 Objektsperre aktiviert ist

Jedes in einem Bucket gespeicherte Objekt mit aktivierter S3 Object Lock durchlaufen die folgenden Phasen:

1. Objektaufnahme

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

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

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

2. Objektaufbewahrung und -Lösung

Von jedem geschützten Objekt werden innerhalb StorageGRID des angegebenen Aufbewahrungszeitraums mehrere Kopien gespeichert. Die genaue Anzahl und Art der Objektkopien sowie der Speicherort werden durch die konformen Regeln der aktiven ILM-Richtlinie bestimmt. Ob ein geschütztes Objekt gelöscht werden kann, bevor das Aufbewahrungsdatum erreicht ist, hängt vom Aufbewahrungsmodus ab.

- Befindet sich ein Objekt unter einer Legal Hold-Funktion, kann das Objekt unabhängig vom Aufbewahrungsmodus nicht gelöscht werden.

Kann ich auch ältere konforme Buckets verwalten?

Die S3-Objektsperre ersetzt die in früheren StorageGRID-Versionen verfügbare Compliance-Funktion. Wenn Sie mithilfe einer früheren Version von StorageGRID konforme Buckets erstellt haben, können Sie die Einstellungen dieser Buckets weiterhin verwalten. Sie können jedoch keine neuen, konformen Buckets mehr erstellen. Anweisungen hierzu finden Sie unter https://kb.netapp.com/Advice_and_Troubleshooting/Hybrid_Cloud_Infrastructure/StorageGRID/How_to_manage_legacy_Compliant_buckets_in_StorageGRID_11.5 [NetApp Knowledge Base: Management älterer, konformer Buckets für StorageGRID 11.5^].

Aktualisieren Sie die S3 Object Lock-Standardaufbewahrung

Wenn Sie beim Erstellen des Buckets die S3-Objektsperre aktiviert haben, können Sie den Bucket bearbeiten, um die Standardeinstellungen für die Aufbewahrung zu ändern. Sie können die Standardaufbewahrung aktivieren (oder deaktivieren) und einen Standardaufbewahrungsmodus und eine Standardaufbewahrungsdauer festlegen.

Bevor Sie beginnen

- Sie sind mit einem beim Mandantenmanager angemeldet ["Unterstützter Webbrowser"](#).
- Sie gehören einer Benutzergruppe an, die über den verfügt ["Managen aller Buckets oder Root-Zugriffsberechtigungen"](#). Diese Berechtigungen überschreiben die Berechtigungseinstellungen in Gruppen- oder Bucket-Richtlinien.
- S3 Objektsperre ist global für Ihr StorageGRID-System aktiviert; Sie haben S3 Objektsperre bei Erstellung des Buckets aktiviert. Siehe ["Verwenden Sie S3 Objektsperre, um Objekte beizubehalten"](#).

Schritte

1. Wählen Sie **View Buckets** aus dem Dashboard, oder wählen Sie **STORAGE (S3) > Buckets**.
 2. Wählen Sie den Bucket-Namen aus der Tabelle aus.
- Die Seite mit den Bucket-Details wird angezeigt.
3. Wählen Sie auf der Registerkarte **Bucket options** das Akkordeon **S3 Object Lock** aus.
 4. Aktivieren oder deaktivieren Sie optional **Default Retention** für diesen Bucket.

Änderungen an dieser Einstellung gelten nicht für Objekte, die bereits im Bucket vorhanden sind, oder für Objekte, die möglicherweise eigene Aufbewahrungsfristen haben.

5. Wenn **Default Retention** aktiviert ist, geben Sie einen **Default Retention Mode** für den Bucket an.

Standardaufbewahrungsmodus	Beschreibung
Compliance	<ul style="list-style-type: none">• Das Objekt kann erst gelöscht werden, wenn das Aufbewahrungsdatum erreicht ist.• Das Aufbewahrungsdatum des Objekts kann erhöht, aber nicht verringert werden.• Das Aufbewahrungsdatum des Objekts kann erst entfernt werden, wenn dieses Datum erreicht ist.
Governance	<ul style="list-style-type: none">• Benutzer mit <code>s3:BypassGovernanceRetention</code> Berechtigung kann den verwenden <code>x-amz-bypass-governance-retention: true</code> Kopfzeile anfordern, um Aufbewahrungseinstellungen zu umgehen.• Diese Benutzer können eine Objektversion löschen, bevor das Aufbewahrungsdatum erreicht ist.• Diese Benutzer können das Aufbewahrungsdatum eines Objekts erhöhen, verringern oder entfernen.

6. Wenn **Default Retention** aktiviert ist, geben Sie die **Default Retention Period** für den Bucket an.

Die **Default Retention Period** gibt an, wie lange neue Objekte zu diesem Bucket hinzugefügt werden sollen, beginnend mit dem Zeitpunkt, zu dem sie aufgenommen werden. Geben Sie einen Wert zwischen 1 und 36,500 Tagen oder zwischen 1 und 100 Jahren an, einschließlich.

7. Wählen Sie **Änderungen speichern**.

Konfiguration der Cross-Origin Resource Sharing (CORS)

Sie können CORS (Cross-Origin Resource Sharing) für einen S3-Bucket konfigurieren, wenn Webapplikationen in anderen Domänen auf diesen Bucket und die Objekte in diesem Bucket zugreifen sollen.

Bevor Sie beginnen

- Sie sind mit einem beim Mandantenmanager angemeldet "[Unterstützter Webbrowser](#)".
- Sie gehören einer Benutzergruppe an, die über den verfügt "[Managen aller Buckets oder Root-Zugriffsberechtigungen](#)". Diese Berechtigungen überschreiben die Berechtigungseinstellungen in Gruppen- oder Bucket-Richtlinien.

Über diese Aufgabe

CORS (Cross-Origin Resource Sharing) ist ein Sicherheitsmechanismus, mit dem Client-Webanwendungen in einer Domäne auf Ressourcen in einer anderen Domäne zugreifen können. Angenommen, Sie verwenden einen S3-Bucket mit dem Namen `Images` Zum Speichern von Grafiken. Durch Konfigurieren von CORS für das `Images` Bucket: Sie können zulassen, dass die Bilder in diesem Bucket auf der Website angezeigt werden <http://www.example.com>.

CORS für einen Bucket aktivieren

Schritte

1. Verwenden Sie einen Texteditor, um die erforderliche XML zu erstellen.

Dieses Beispiel zeigt die XML, die zur Aktivierung von CORS für einen S3-Bucket verwendet wird. Mit dieser XML-Datei kann jede Domäne GET-Anforderungen an den Bucket senden, es erlaubt jedoch nur das <http://www.example.com> Domain zum Senden VON POST- und LÖSCHEN von Anfragen. Alle Anfragezeilen sind zulässig.

```

<corsConfiguration
  xmlns="http://s3.amazonaws.com/doc/2020-10-22/">
  <corsRule>
    <allowedOrigin>*</allowedOrigin>
    <allowedMethod>GET</allowedMethod>
    <allowedHeader>*</allowedHeader>
  </corsRule>
  <corsRule>
    <allowedOrigin>http://www.example.com</allowedOrigin>
    <allowedMethod>GET</allowedMethod>
    <allowedMethod>POST</allowedMethod>
    <allowedMethod>DELETE</allowedMethod>
    <allowedHeader>*</allowedHeader>
  </corsRule>
</corsConfiguration>

```

Weitere Informationen zur CORS-Konfigurations-XML finden Sie unter ["Amazon Web Services \(AWS\) Dokumentation: Amazon Simple Storage Service Developer Guide"](#).

2. Wählen Sie **View Buckets** aus dem Dashboard, oder wählen Sie **STORAGE (S3) > Buckets**.
3. Wählen Sie den Bucket-Namen aus der Tabelle aus.

Die Seite mit den Bucket-Details wird angezeigt.

4. Wählen Sie auf der Registerkarte **Bucket Access** das Akkordeon **Cross-Origin Resource Sharing (CORS)** aus.
5. Aktivieren Sie das Kontrollkästchen **CORS aktivieren**.
6. Fügen Sie die CORS-Konfigurations-XML in das Textfeld ein.
7. Wählen Sie **Änderungen speichern**.

CORS-Einstellung ändern

Schritte

1. Aktualisieren Sie die CORS-Konfigurations-XML im Textfeld, oder wählen Sie **Clear**, um von vorne zu beginnen.
2. Wählen Sie **Änderungen speichern**.

Deaktivieren Sie die CORS-Einstellung

Schritte

1. Deaktivieren Sie das Kontrollkästchen **CORS aktivieren**.
2. Wählen Sie **Änderungen speichern**.

Löschen von Objekten in Bucket

Sie können den Tenant Manager verwenden, um die Objekte in einem oder mehreren Buckets zu löschen.

Überlegungen und Anforderungen

Bevor Sie diese Schritte durchführen, beachten Sie Folgendes:

- Wenn Sie die Objekte in einem Bucket löschen, entfernt StorageGRID endgültig alle Objekte und alle Objektversionen in jedem ausgewählten Bucket von allen Nodes und Standorten im StorageGRID System. StorageGRID entfernt auch alle zugehörigen Objekt-Metadaten. Sie können diese Informationen nicht wiederherstellen.
- Das Löschen aller Objekte in einem Bucket kann je nach Anzahl der Objekte, Objektkopien und gleichzeitigen Vorgängen Minuten, Tage oder sogar Wochen dauern.
- Wenn ein Eimer hat "[S3-Objektsperre aktiviert](#)", Kann es im Zustand **delete objects: Read-only** für years bleiben.



Ein Bucket, der S3 Object Lock verwendet, bleibt im Zustand **delete Objects: Read-only**, bis das Aufbewahrungsdatum für alle Objekte erreicht ist und alle Legal Holds entfernt werden.

- Während Objekte gelöscht werden, ist der Zustand des Buckets **delete objects: Read-only**. In diesem Status können Sie dem Bucket keine neuen Objekte hinzufügen.
- Nachdem alle Objekte gelöscht wurden, verbleibt der Bucket im schreibgeschützten Status. Sie haben folgende Möglichkeiten:
 - Versetzen Sie den Bucket in den Schreibmodus und verwenden Sie ihn für neue Objekte wieder
 - Löschen Sie den Bucket
 - Belassen Sie den Bucket im schreibgeschützten Modus, um seinen Namen für eine zukünftige Verwendung zu reservieren
- Wenn für einen Bucket die Objektversionierung aktiviert ist, werden alle Löschmarkierungen, die sich beim Starten dieser Schritte im Bucket befinden, nicht durch den Vorgang „Objekte löschen“ entfernt. Wenn Sie einen versionierten Bucket löschen möchten, nachdem alle Objekte gelöscht wurden, müssen Sie alle bereits vorhandenen Löschmarkierungen entfernen.
- Wenn Sie verwenden "[Grid-übergreifende Replizierung](#)", Beachten Sie Folgendes:
 - Mit dieser Option werden keine Objekte aus dem Bucket auf dem anderen Raster gelöscht.
 - Wenn Sie diese Option für den Quell-Bucket auswählen, wird die Warnung **gitterübergreifender Replikationsfehler** ausgelöst, wenn Sie dem Ziel-Bucket auf dem anderen Grid Objekte hinzufügen. Wenn Sie nicht garantieren können, dass niemand dem Bucket auf dem anderen Raster Objekte hinzufügen wird, "[Deaktivieren Sie die Grid-übergreifende Replizierung](#)" Für diesen Bucket, bevor alle Bucket-Objekte gelöscht werden.

Bevor Sie beginnen

- Sie sind mit einem beim Mandantenmanager angemeldet "[Unterstützter Webbrowser](#)".
- Sie gehören einer Benutzergruppe an, die über den verfügt "[Root-Zugriffsberechtigung](#)". Diese Berechtigung überschreibt die Berechtigungseinstellungen in Gruppen- oder Bucket-Richtlinien.

Schritte

1. Wählen Sie **View Buckets** aus dem Dashboard, oder wählen Sie **STORAGE (S3) > Buckets**.

Die Seite Buckets wird angezeigt und zeigt alle vorhandenen S3-Buckets an.

2. Verwenden Sie das Menü **Aktionen** oder die Detailseite für einen bestimmten Bucket.

Menü „Aktionen“

- Aktivieren Sie das Kontrollkästchen für jeden Bucket, aus dem Sie Objekte löschen möchten.
- Wählen Sie **actions > Delete objects in bucket**.

Detailseite

- Wählen Sie einen Bucket-Namen aus, um die Details anzuzeigen.
- Wählen Sie **Objekte im Bucket löschen**.

3. Wenn das Bestätigungsdialogfeld angezeigt wird, überprüfen Sie die Details, geben Sie **Ja** ein und wählen Sie **OK**.

4. Warten Sie, bis der Löschvorgang beginnt.

Nach ein paar Minuten:

- Auf der Seite mit den Bucket-Details wird ein gelbes Statusbanner angezeigt. Der Fortschrittsbalken gibt an, wie viel Prozent der Objekte gelöscht wurden.
- (read-only)** erscheint nach dem Namen des Buckets auf der Seite mit den Bucket-Details.
- (Objekte löschen: Schreibgeschützt)** erscheint neben dem Namen des Buckets auf der Buckets-Seite.

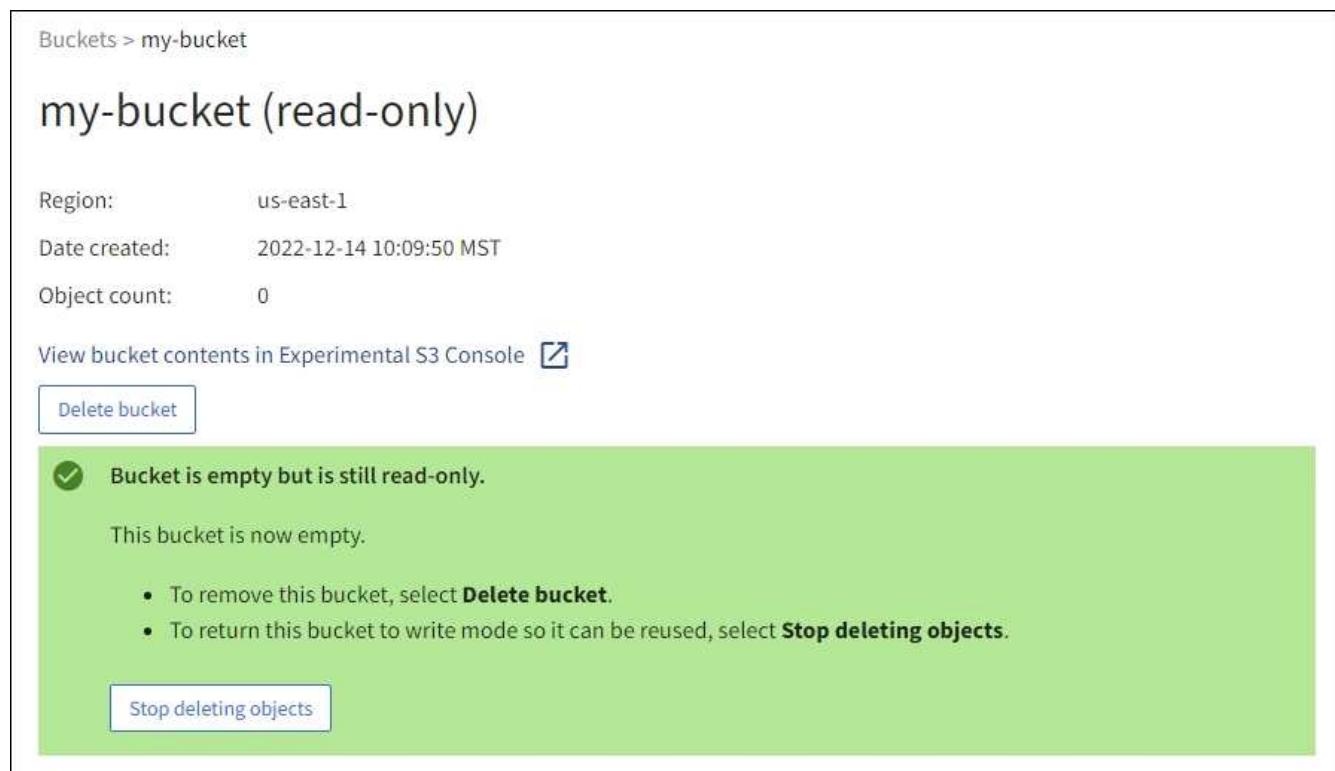
The screenshot shows the AWS S3 Bucket details page for 'my-bucket'. The bucket name 'my-bucket' is highlighted in yellow. The page displays basic information: Region (us-east-1), Date created (2022-12-14 10:09:50 MST), and Object count (3). A 'Delete bucket' button is visible. A green success banner at the top right says 'Success' and 'Starting to delete objects from one bucket.' A yellow warning box at the bottom left states: 'All bucket objects are being deleted. StorageGRID is deleting all copies of the objects in this bucket, which might take days or weeks. While objects are being deleted, the bucket is read only. To stop the operation, select Stop deleting objects. You cannot restore objects that have already been deleted.' A progress bar shows 0% completion. The status bar at the bottom of the browser window shows '0% (0 of 3 objects deleted)' and a 'Stop deleting objects' button.

5. Wählen Sie, wie erforderlich, während der Vorgang ausgeführt wird, **Löschen von Objekten stoppen**, um den Prozess anzuhalten. Wählen Sie dann optional **Objekte im Bucket löschen** aus, um den Prozess fortzusetzen.

Wenn Sie **Löschen von Objekten stoppen** auswählen, wird der Bucket in den Schreibmodus zurückversetzt. Sie können jedoch nicht auf Objekte zugreifen oder diese wiederherstellen.

6. Warten Sie, bis der Vorgang abgeschlossen ist.

Wenn der Bucket leer ist, wird das Statusbanner aktualisiert, der Bucket bleibt jedoch weiterhin schreibgeschützt.



The screenshot shows the AWS S3 Bucket details page for 'my-bucket'. The bucket is listed as '(read-only)'. Key details shown are Region: us-east-1, Date created: 2022-12-14 10:09:50 MST, and Object count: 0. A link to 'View bucket contents in Experimental S3 Console' is present. A prominent green banner at the bottom states: 'Bucket is empty but is still read-only.' It also says 'This bucket is now empty.' and provides two options: 'To remove this bucket, select Delete bucket.' and 'To return this bucket to write mode so it can be reused, select Stop deleting objects.' A 'Delete bucket' button is also visible.

7. Führen Sie einen der folgenden Schritte aus:

- Schließen Sie die Seite, um den Bucket im schreibgeschützten Modus zu belassen. Beispielsweise können Sie einen leeren Bucket im schreibgeschützten Modus belassen, um den Bucket-Namen für die zukünftige Verwendung zu reservieren.
- Löschen Sie den Bucket. Sie können **Eimer löschen** auswählen, um einen einzelnen Eimer zu löschen, oder die Buckets-Seite zurücksenden und **Aktionen** > *Eimer löschen auswählen, um mehr als einen Eimer zu entfernen.



Wenn Sie einen versionierten Bucket nicht löschen können, nachdem alle Objekte gelöscht wurden, bleiben möglicherweise Löschmarkierungen erhalten. Um den Bucket zu löschen, müssen Sie alle verbleibenden Löschmarkierungen entfernen.

- Versetzen Sie den Bucket in den Schreibmodus und verwenden Sie ihn optional für neue Objekte wieder. Sie können für einen einzelnen Bucket **Stop delete objects** auswählen oder zur Buckets-Seite zurückkehren und für mehr als einen Bucket **Action** > **Stop delete objects** auswählen.

S3-Bucket löschen

Mit dem Tenant Manager können Sie eine oder mehrere leere S3-Buckets löschen.

Bevor Sie beginnen

- Sie sind mit einem beim Mandantenmanager angemeldet "[Unterstützter Webbrower](#)".
- Sie gehören einer Benutzergruppe an, die über den verfügt "[Managen aller Buckets oder Root-Zugriffsberechtigungen](#)". Diese Berechtigungen überschreiben die Berechtigungseinstellungen in Gruppen- oder Bucket-Richtlinien.
- Die Buckets, die Sie löschen möchten, sind leer.

Über diese Aufgabe

Diese Anweisungen beschreiben das Löschen eines S3-Buckets mithilfe von Tenant Manager. Sie können auch S3-Buckets über löschen "[Mandantenmanagement-API](#)" Oder im "[S3-REST-API](#)".

Sie können einen S3-Bucket nicht löschen, wenn er Objekte, nicht aktuelle Objektversionen enthält oder Markierungen löscht. Informationen zum Löschen von S3-versionierten Objekten finden Sie unter "[So werden Objekte gelöscht](#)".

Schritte

1. Wählen Sie **View Buckets** aus dem Dashboard, oder wählen Sie **STORAGE (S3) > Buckets**.

Die Seite Buckets wird angezeigt und zeigt alle vorhandenen S3-Buckets an.

2. Verwenden Sie das Menü **Aktionen** oder die Detailseite für einen bestimmten Bucket.

Menü „Aktionen“

- a. Aktivieren Sie das Kontrollkästchen für jeden Bucket, den Sie löschen möchten.
- b. Wählen Sie **Actions > Eimer löschen**.

Detailseite

- a. Wählen Sie einen Bucket-Namen aus, um die Details anzuzeigen.
- b. Wählen Sie **Eimer löschen**.

3. Wenn das Bestätigungsdialogfeld angezeigt wird, wählen Sie **Ja**.

StorageGRID bestätigt, dass jeder Bucket leer ist und löscht dann jeden Bucket. Dieser Vorgang kann einige Minuten dauern.

Wenn ein Bucket nicht leer ist, wird eine Fehlermeldung angezeigt. Bevor Sie den Bucket löschen können, müssen Sie alle Objekte und alle Löschmarkierungen im Bucket löschen.

Verwenden Sie die Experimental S3-Konsole

Sie können die Objekte über die S3-Konsole in einem S3-Bucket anzeigen.

Sie können auch S3 Console verwenden, um folgende Aufgaben zu erledigen:

- Hinzufügen und Löschen von Objekten, Objektversionen und Ordnern
- Benennen Sie Objekte um
- Verschieben und Kopieren von Objekten zwischen Buckets und Ordnern
- Verwalten von Objekt-Tags
- Zeigen Sie Objektmetadaten an
- Objekte herunterladen

 Die S3-Konsole ist als „experimentell“ gekennzeichnet, da sie noch nicht vollständig oder für die Verwendung in einer Produktionsumgebung freigegeben ist. Mandanten sollten die S3-Konsole nur verwenden, wenn sie Funktionen für eine kleine Anzahl von Objekten ausführen, z. B. beim Hochladen von Objekten zur Simulation einer neuen ILM-Richtlinie, bei der Fehlerbehebung von Ingest-Problemen oder bei der Verwendung von Proof-of-Concept- oder nicht-Production-Grids.

Bevor Sie beginnen

- Sie sind mit einem beim Mandantenmanager angemeldet "[Unterstützter Webbrowser](#)".
- Sie gehören einer Benutzergruppe an, die über die Root-Zugriffsberechtigung verfügt oder die sowohl die Verwaltung aller Buckets als auch die Verwaltung von Objekten mit der S3-Konsole verfügt "[Berechtigungen](#)".



Benutzer, die über die Berechtigung zum Verwalten von Objekten mit S3-Konsole verfügen, aber nicht über die Berechtigung zum Verwalten aller Buckets verfügen, können dennoch direkt zur Experimental S3-Konsole navigieren.

- Sie haben einen Bucket erstellt.
- Für den Benutzer wurde eine S3-Gruppen- oder Bucket-Richtlinie konfiguriert.
- Sie kennen die Zugriffsschlüssel-ID und den geheimen Zugriffsschlüssel des Benutzers. Optional haben Sie eine .csv Datei mit diesen Informationen. Siehe "[Anweisungen zum Erstellen von Zugriffsschlüsseln](#)".

Schritte

1. Wählen Sie **Buckets**.
2. Wählen Sie [Experimental S3 Console](#)  . Sie können auch über die Seite mit den Bucket-Details auf diesen Link zugreifen.
3. Fügen Sie auf der Anmeldeseite Experimental S3 Console die Zugriffsschlüssel-ID und den geheimen Zugriffsschlüssel in die Felder ein. Wählen Sie andernfalls * Zugriffsschlüssel hochladen* aus, und wählen Sie Ihr aus .csv Datei:
4. Wählen Sie **Anmelden**.
5. Objektmanagement nach Bedarf

Buckets > bucket-01

bucket-01

[Upload](#)[New folder](#)[Refresh](#)[Actions](#) Search by prefix

<input type="checkbox"/>	Name	Logical space used	Last modified on
<input type="checkbox"/>	03_Grid_Primer_11.5.pdf	2.73 MB	2021-12-03 09:43:26 MST
<input type="checkbox"/>	04_Tenant_Users_Guide_11.5.pdf	1.07 MB	2021-12-03 09:44:24 MST
<input type="checkbox"/>	06_Tenant_Users_Guide_11.5.pdf	1.25 MB	2021-12-03 09:44:27 MST
<input type="checkbox"/>	08_Tenant_Users_Guide_11.5.pdf	1.25 MB	2021-12-03 09:44:27 MST
<input type="checkbox"/>	09_Tenant_Users_Guide_11.5.pdf	1.25 MB	2021-12-03 09:44:26 MST
<input type="checkbox"/>	10_Grid_Primer_11.5.pdf	2.8 MB	2021-12-03 09:43:27 MST

Select an object or folder to view its details.

Displaying 16 objects
Selected 0 objects

| < Previous 1 Next > |

Copyright-Informationen

Copyright © 2025 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtsinhabers in keiner Form und durch keine Mittel – weder grafische noch elektronische oder mechanische, einschließlich Fotokopieren, Aufnehmen oder Speichern in einem elektronischen Abrufsystem – auch nicht in Teilen, vervielfältigt werden.

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

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