



Management von S3-Buckets

StorageGRID

NetApp

October 03, 2025

This PDF was generated from <https://docs.netapp.com/de-de/storagegrid-116/tenant/using-s3-object-lock.html> on October 03, 2025. Always check docs.netapp.com for the latest.

Inhalt

Management von S3-Buckets	1
Nutzen Sie die S3-Objektsperre für Mandanten	1
Was ist S3 Object Lock?	1
Management älterer, konformer Buckets	2
S3-Objektsperre-Workflow	2
Anforderungen für die S3-Objektsperre	3
S3-Bucket erstellen	5
Anzeigen von S3-Bucket-Details	7
Ändern der Konsistenzstufe	9
Aktiviert bzw. deaktiviert Updates der letzten Zugriffszeit	10
Ändern Sie die Objektversionierung für einen Bucket	13
Cross-Origin Resource Sharing (CORS) konfigurieren	15
S3-Bucket löschen	17
Verwenden Sie die Experimental S3-Konsole	19

Management von S3-Buckets

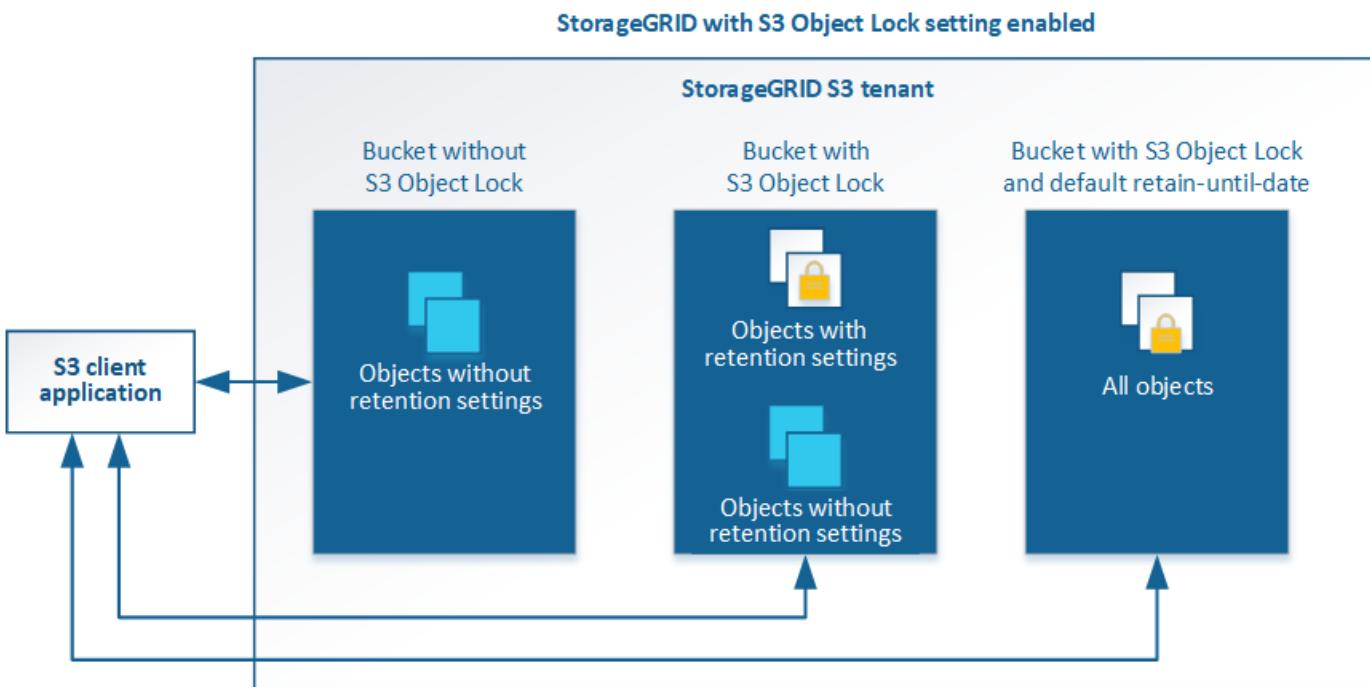
Nutzen Sie die S3-Objektsperre für Mandanten

Sie können die S3-Objektsperrfunktion in StorageGRID verwenden, wenn Ihre Objekte die gesetzlichen Aufbewahrungsvorgaben 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 in einem Bucket S3-Objektsperre aktiviert ist, können S3-Client-Applikationen optional Aufbewahrungseinstellungen für jede Objektversion in diesem Bucket angeben. Eine Objektversion muss über Aufbewahrungseinstellungen verfügen, die durch S3 Object Lock geschützt werden sollen.



Die StorageGRID S3 Objektsperre bietet einen einheitlichen Aufbewahrungsmodus, der dem Amazon S3-Compliance-Modus entspricht. Standardmäßig kann eine geschützte Objektversion nicht von einem Benutzer überschrieben oder gelöscht werden. Die StorageGRID S3-Objektsperre unterstützt keinen Governance-Modus und erlaubt Benutzern mit speziellen Berechtigungen nicht, Aufbewahrungseinstellungen zu umgehen oder geschützte Objekte zu löschen.

Wenn in einem Bucket S3-Objektsperre aktiviert ist, kann die S3-Client-Applikation beim Erstellen oder Aktualisieren eines Objekts optional eine oder beide der folgenden Aufbewahrungseinstellungen auf Objektebene angeben:

- **Bis-Datum aufbewahren:** Wenn das Aufbewahrungsdatum einer Objektversion in der Zukunft liegt, kann das Objekt abgerufen, aber nicht geändert oder gelöscht werden. Bei Bedarf kann das Aufbewahrungsdatum eines Objekts erhöht werden, dieses Datum kann jedoch nicht verringert 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.

Das können Sie auch [Legen Sie einen Standardaufbewahrungsmodus und einen Standardaufbewahrungszeitraum für den Bucket fest](#). Diese werden auf jedes dem Bucket hinzugefügte Objekt angewendet, das keine eigenen Aufbewahrungseinstellungen vorgibt.

Weitere Informationen zu diesen Einstellungen finden Sie unter [Verwenden Sie die S3-Objektsperre](#).

Management älterer, konformer Buckets

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. Weitere Informationen finden Sie im NetApp Knowledge Base Artikel.

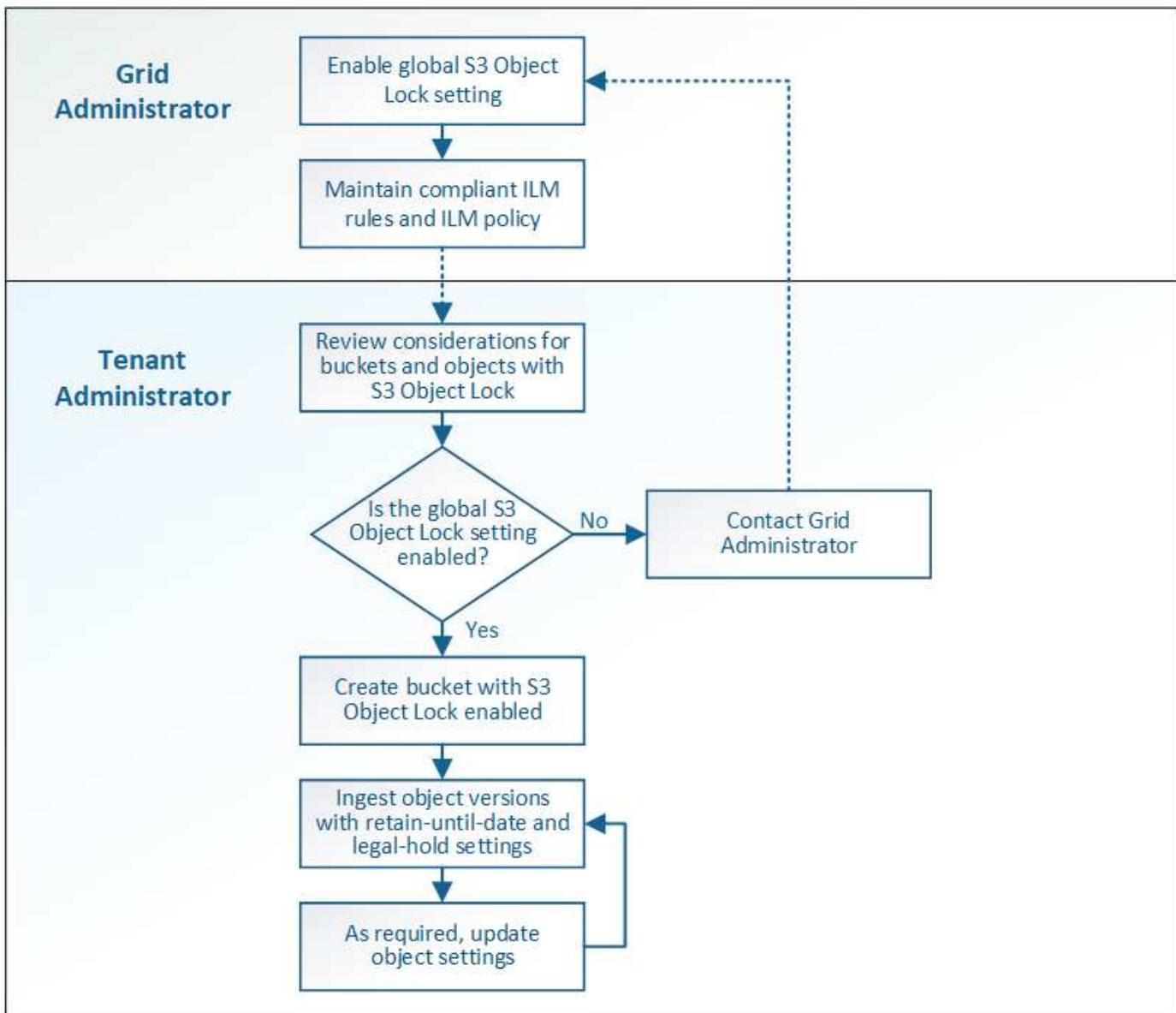
["NetApp Knowledge Base: Management älterer, konformer Buckets für StorageGRID 11.5"](#)

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-Objektsperreneinstellung für das gesamte StorageGRID-System aktivieren. Der Grid-Administrator muss außerdem sicherstellen, dass der [Information Lifecycle Management-Richtlinie \(ILM\)](#) Ist „konform“; er muss die Anforderungen von Buckets erfüllen, wenn S3 Objektsperre aktiviert ist. Weitere Informationen erhalten Sie von Ihrem Grid-Administrator oder in den Anweisungen zum Verwalten von Objekten mit Information Lifecycle Management.

Nachdem die globale S3-Objektsperre aktiviert wurde, können Sie Buckets mit aktivierter S3-Objektsperre erstellen. Anschließend können Sie mithilfe der S3-Client-Applikation optional Aufbewahrungseinstellungen für jede Objektversion angeben.



Anforderungen für die S3-Objektsperre

Bevor Sie die S3-Objektsperre für einen Bucket aktivieren, überprüfen Sie die Anforderungen für S3-Objektsperren-Buckets und -Objekte sowie den Lebenszyklus von Objekten in Buckets, wobei S3-Objektsperre aktiviert ist.

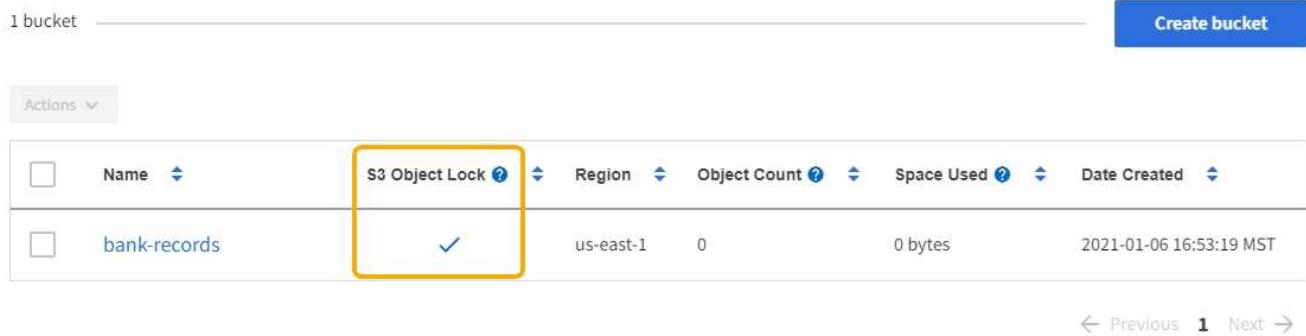
Anforderungen für Buckets, bei denen die S3-Objektsperre aktiviert ist

- Wenn die globale S3-Objektsperre für das StorageGRID System aktiviert ist, können Sie die Buckets mit aktiverter S3-Objektsperre über den Mandantenmanager, die Mandantenmanagement-API oder die S3-REST-API erstellen.

In diesem Beispiel aus dem Tenant Manager wird ein Bucket angezeigt, in dem S3 Object Lock aktiviert ist.

Buckets

Create buckets and manage bucket settings.



The screenshot shows the AWS S3 Buckets list. At the top, it says "1 bucket". On the right, there is a blue "Create bucket" button. Below the header is a "Actions" dropdown menu. The main table has columns: Name, S3 Object Lock, Region, Object Count, Space Used, and Date Created. The "Name" column lists "bank-records". The "S3 Object Lock" column for "bank-records" contains a blue checkmark, which is highlighted with a yellow border. The "Region" column shows "us-east-1", "Object Count" shows "0", "Space Used" shows "0 bytes", and "Date Created" shows "2021-01-06 16:53:19 MST". At the bottom right of the table, there are navigation links: "Previous", "1", and "Next".

- 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.
- Bucket-Versionierung ist mit S3 Object Lock erforderlich. Wenn die S3-Objektsperre für einen Bucket aktiviert ist, ermöglicht StorageGRID automatisch die Versionierung für diesen Bucket.
- Nachdem Sie einen Bucket mit aktiverter S3-Objektsperre erstellt haben, können Sie die S3-Objektsperre oder die Versionierung für diesen Bucket nicht deaktivieren.
- Optional können Sie die Standardaufbewahrung für einen Bucket konfigurieren. Wenn eine Objektversion hochgeladen wird, wird die standardmäßige Aufbewahrung auf die Objektversion angewendet. Sie können den Bucket-Standard überschreiben, indem Sie einen Aufbewahrungsmodus angeben und in der Anforderung zum Hochladen einer Objektversion bis dato aufzubewahren.
- Bucket-Lifecycle-Konfiguration wird für S3-Objekt-Lifecycle-Buckets unterstützt.
- 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 muss die S3-Client-Applikation entweder die Bucket-Standardaufbewahrung konfigurieren oder Aufbewahrungseinstellungen in jeder Upload-Anfrage angeben.
- Sie können das Aufbewahrungsdatum für eine Objektversion erhöhen, diesen Wert jedoch nie reduzieren.
- Wenn Sie über eine ausstehende rechtliche oder behördliche Untersuchung informiert werden, können Sie relevante Informationen erhalten, indem Sie eine gesetzliche Aufbewahrungspflichten auf eine Objektversion setzen. Wenn eine Objektversion unter einer gesetzlichen Aufbewahrungspflichten liegt, kann das Objekt nicht aus StorageGRID gelöscht werden, auch wenn es seine Aufbewahrungsfrist bis zum letzten Tag erreicht hat. Sobald die gesetzliche Aufbewahrungspflichten aufgehoben sind, kann die Objektversion gelöscht werden, wenn das Aufbewahrungsdatum erreicht ist.
- Für die S3-Objektsperre ist die Verwendung versionierter Buckets erforderlich. 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 Objekt, das in einem Bucket mit aktiverter S3-Objektsperre gespeichert wird, durchläuft drei Phasen:

1. Objektaufnahme

- Beim Hinzufügen einer Objektversion zu einem Bucket mit aktiver S3-Objektsperre kann die S3-Client-Applikation optional Aufbewahrungseinstellungen für das Objekt festlegen (bis dato, gesetzliche Aufbewahrungspflichten oder beides). StorageGRID generiert dann Metadaten für dieses Objekt, einschließlich einer eindeutigen Objekt-ID (UUID) sowie Datum und Uhrzeit der Aufnahme.
- Nach der Aufnahme einer Objektversion mit Aufbewahrungseinstellungen können seine Daten und benutzerdefinierten S3-Metadaten nicht mehr geändert werden.
- StorageGRID speichert die Objektmetadaten unabhängig von den Objektdaten. Es behält drei Kopien aller Objektmetadaten an jedem Standort.

2. Aufbewahrung von Objekten

- StorageGRID speichert mehrere Kopien des Objekts. Die genaue Anzahl und Art der Kopien und der Speicherorte werden durch die konformen Regeln in der aktiven ILM-Richtlinie festgelegt.

3. Löschen von Objekten

- Ein Objekt kann gelöscht werden, wenn sein Aufbewahrungsdatum erreicht ist.
- Ein Objekt, das sich unter einer gesetzlichen Aufbewahrungspflichten befindet, kann nicht gelöscht werden.

S3-Bucket erstellen

Sie können im Mandanten-Manager S3-Buckets für Objektdaten erstellen. Wenn Sie einen Bucket erstellen, müssen Sie Namen und Region des Bucket angeben. Wenn die globale S3-Objektsperre für das StorageGRID-System aktiviert ist, können Sie optional die S3-Objektsperre für den Bucket aktivieren.

Was Sie benötigen

- Sie sind mit einem beim Mandantenmanager angemeldet [Unterstützter Webbrowser](#).
- Sie gehören zu einer Benutzergruppe mit den Berechtigungen Alle Buckets verwalten oder Root Access. 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 einen Bucket mit S3-Objektsperre erstellen möchten, haben Sie die globale S3-Objektsperreneinstellung für das StorageGRID-System aktiviert und die Anforderungen für S3-Objektsperren-Buckets und -Objekte überprüft.

Verwenden Sie die S3-Objektsperre

Schritte

1. Wählen Sie **STORAGE (S3) Buckets** aus.
2. Wählen Sie **Eimer erstellen**.

Create bucket

1 Enter details 2 Manage object settings
Optional

Enter bucket details
Enter the bucket's name and select the bucket's region.

Bucket name ?

Region ?

us-east-1

[Cancel](#) [Continue](#)

3. Geben Sie einen eindeutigen Namen für den Bucket ein.



Sie können den Bucket-Namen nach dem Erstellen des Buckets nicht ändern.

Bucket-Namen müssen folgende Regeln einhalten:

- 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.



Weitere Informationen finden Sie im "[Dokumentation der Amazon Web Services \(AWS\) zu den Bucket-Benennungsregeln](#)".

4. Wählen Sie die Region für diesen Bucket aus.

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.



Nach dem Erstellen des Buckets können Sie die Region nicht ändern.

5. Wählen Sie **Weiter**.

6. 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.

7. Wenn der Abschnitt S3-Objektsperre angezeigt wird, aktivieren Sie optional die S3-Objektsperre für den Bucket.



Sie können die S3-Objektsperre nach dem Erstellen des Buckets nicht aktivieren oder deaktivieren.

Der Abschnitt S3-Objektsperre wird nur angezeigt, wenn die globale S3-Objektsperre aktiviert ist.

S3-Objektsperre muss für den Bucket aktiviert sein, bevor eine S3-Client-Applikation für die dem Bucket hinzugefügten Objekte Haltungs- bis datums- und gesetzliche Aufbewahrungs-Einstellungen festlegen kann.

Wenn Sie S3 Object Lock für einen Bucket aktivieren, wird die Bucket-Versionierung automatisch aktiviert. Das können Sie auch [Legen Sie einen Standardaufbewahrungsmodus und einen Standardaufbewahrungszeitraum für den Bucket fest](#). Die auf jedes in den Bucket aufgenommene Objekt angewendet werden, das keine eigenen Aufbewahrungseinstellungen spezifiziert.

8. Wählen Sie **Eimer erstellen**.

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

Verwandte Informationen

[Objektmanagement mit ILM](#)

[Mandantenmanagement-API verstehen](#)

[S3 verwenden](#)

Anzeigen von S3-Bucket-Details

Sie können eine Liste der Buckets und Bucket-Einstellungen in Ihrem Mandantenkonto anzeigen.

Was Sie benötigen

- Sie müssen mit einem beim Mandantenmanager angemeldet sein [Unterstützter Webbrowser](#).

Schritte

1. Wählen Sie **STORAGE (S3) Buckets** aus.

Die Seite Buckets wird angezeigt und enthält alle Buckets für das Mandantenkonto.

Buckets

Create buckets and manage bucket settings.

3 buckets							Create bucket
Actions		Experimental S3 Console					
Name	S3 Object Lock	Region	Object Count	Space Used	Date Created		
bucket-01a	✓	us-east-1	0	0 bytes	2022-01-06 13:48:08 MST		
bucket-02a	✓	us-east-1	0	0 bytes	2022-01-06 13:48:26 MST		
bucket-03a		us-east-1	0	0 bytes	2022-01-06 13:48:38 MST		

2. Überprüfen Sie die Informationen 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.

- Name: Der eindeutige Name des Buckets, der nicht geändert werden kann.
- S3 Object Lock: Ob S3 Object Lock für diesen Bucket aktiviert ist.

Diese Spalte wird nicht angezeigt, wenn die globale S3-Objektsperre deaktiviert ist. In dieser Spalte werden außerdem Informationen für alle Buckets angezeigt, die für die Konformität mit älteren Daten verwendet wurden.

- Region: Die Eimer-Region, die nicht geändert werden kann.
- Objektanzahl: Die Anzahl der Objekte in diesem Bucket.
- Verwendeter Speicherplatz: Die logische Größe aller Objekte in diesem Bucket. Die logische Größe umfasst nicht den tatsächlich benötigten Speicherplatz für replizierte oder Erasure Coding-Kopien oder für Objekt-Metadaten.
- Erstellungsdatum: Das Datum und die Uhrzeit, zu der der Bucket erstellt wurde.



Die angezeigten Werte für Objektanzahl und verwandelter 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.

3. Um die Einstellungen für einen Bucket anzuzeigen und zu managen, wählen Sie den Bucket-Namen aus.

Auf der Seite mit den Bucket-Details können Sie Einstellungen für Bucket-Optionen, Bucket-Zugriff und -Einstellungen anzeigen und bearbeiten [Plattform-Services](#).

Buckets > bucket-01

Overview

Name:	bucket-01
Region:	us-east-1
Date created:	2021-11-30 09:55:55 MST

[View bucket contents in Experimental S3 Console](#)

Bucket options **Bucket access** **Platform services**

Consistency level	Read-after-new-write (default)
Last access time updates	Disabled
Object versioning	Enabled
S3 Object Lock	Disabled

Ändern der Konsistenzstufe

Wenn Sie einen S3-Mandanten verwenden, können Sie mithilfe des Mandanten Manager oder der Mandanten-Management-API die Konsistenzkontrolle für Vorgänge ändern, die in den Objekten in S3 Buckets ausgeführt werden.

Was Sie benötigen

- Sie müssen mit einem beim Mandantenmanager angemeldet sein [Unterstützter Webbrowser](#).
- Sie müssen einer Benutzergruppe angehören, die über die Berechtigung Alle Buckets verwalten oder Root Access verfügt. Diese Berechtigungen überschreiben die Berechtigungseinstellungen in Gruppen- oder Bucket-Richtlinien. Siehe [Mandantenmanagement-Berechtigungen](#).

Über diese Aufgabe

Die Konsistenzstufe bietet 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 **STORAGE (S3) Buckets** aus.
2. Wählen Sie den Bucket-Namen aus der Liste aus.

Die Seite mit den Bucket-Details wird angezeigt.
3. Wählen Sie **Bucket-Optionen Konsistenzstufe** 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 **Last Access Time** in ihrer Platzierungsanleitung verwendet. Sie können diese Anweisungen ignorieren, wenn Ihr StorageGRID System eine solche Regel nicht enthält.

Was Sie benötigen

- Sie müssen mit einem beim Mandantenmanager angemeldet sein [Unterstützter Webbrowser](#).
- Sie müssen einer Benutzergruppe angehören, die über die Berechtigung Alle Buckets verwalten oder Root Access verfügt. Diese Berechtigungen überschreiben die Berechtigungseinstellungen in Gruppen- oder Bucket-Richtlinien. Siehe [Mandantenmanagement-Berechtigungen](#).

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

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.



Weitere Informationen finden Sie in den Anweisungen zum Verwalten von Objekten mit Information Lifecycle Management.

Standardmäßig werden Updates zur letzten Zugriffszeit deaktiviert. Wenn Ihr StorageGRID-System eine ILM-Regel enthält, die die Option **Last Access Time** verwendet und diese Option auf Objekte in diesem Bucket angewendet werden soll, müssen Sie Aktualisierungen für die letzte Zugriffszeit für die in dieser Regel festgelegten S3-Buckets 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 **STORAGE (S3) Buckets** aus.
2. Wählen Sie den Bucket-Namen aus der Liste aus.

Die Seite mit den Bucket-Details wird angezeigt.

3. Wählen Sie **Bucket-Optionen Letzte Aktualisierung der Zugriffszeit** aus.
4. Wählen Sie das entsprechende Optionsfeld aus, um Aktualisierungen der letzten Zugriffszeit zu aktivieren oder zu deaktivieren.

The screenshot shows the 'Bucket access' tab selected in the top navigation bar. Under the 'Consistency level' section, 'Read-after-new-write (default)' is chosen. In the 'Last access time updates' section, 'Disabled' is selected. A note below explains that when disabled, objects are not added to ILM evaluation queues. A detailed list of behaviors follows, including requests for object metadata, updates to copy objects, and multipart uploads. A note states that updating last access times can reduce performance for small objects. Two radio button options are shown: 'Enable last access time updates when retrieving an object' (unchecked) and 'Disable last access time updates when retrieving an object' (checked). A 'Save changes' button is at the bottom right.

5. Wählen Sie Änderungen speichern.

Verwandte Informationen

[Mandantenmanagement-Berechtigungen](#)

[Objektmanagement mit ILM](#)

Ändern Sie die Objektversionierung für einen Bucket

Wenn Sie einen S3-Mandanten verwenden, können Sie den Mandanten-Manager oder die Mandanten-Management-API verwenden, um den Versionierungsstatus für S3 Buckets zu ändern.

Was Sie benötigen

- Sie sind mit einem beim Mandantenmanager angemeldet [Unterstützter Webbrowser](#).
- Sie gehören zu einer Benutzergruppe mit den Berechtigungen Alle Buckets verwalten oder Root Access. Diese Berechtigungen überschreiben die Berechtigungseinstellungen in Gruppen- oder Bucket-Richtlinien.

[Mandantenmanagement-Berechtigungen](#)

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 wieder in einen nichtversionierten Zustand zurückkehrt. Sie können die Versionierung für den Bucket jedoch unterbrechen.

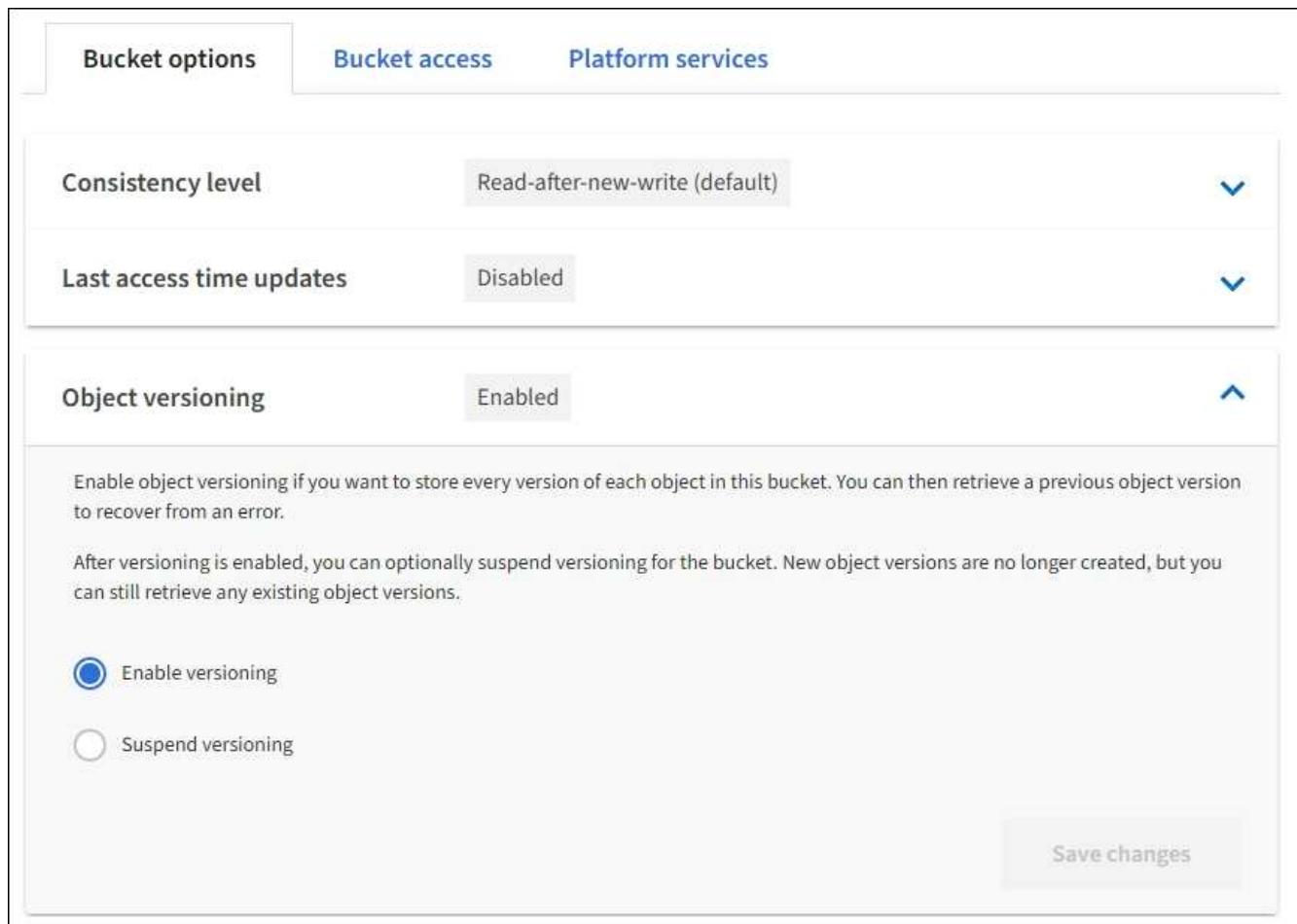
- Deaktiviert: Versionierung wurde noch nie aktiviert
- Aktiviert: Versionierung ist aktiviert
- Suspendiert: Die Versionierung war zuvor aktiviert und wird ausgesetzt

S3 Objektversionierung

ILM-Regeln und Richtlinien für versionierte S3-Objekte (Beispiel 4)

Schritte

1. Wählen Sie **STORAGE (S3) Buckets** aus.
2. Wählen Sie den Bucket-Namen aus der Liste aus.
3. Wählen Sie **Bucket-Optionen Objektversionierung** aus.



4. Wählen Sie einen Versionierungsstatus für die Objekte in diesem Bucket aus.



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**.

Cross-Origin Resource Sharing (CORS) konfigurieren

Die Cross-Origin Resource Sharing (CORS) kann für einen S3-Bucket konfiguriert werden, wenn für Web-Applikationen in anderen Domänen auf diesen Bucket und Objekte in diesem Bucket zugegriffen werden soll.

Was Sie benötigen

- Sie müssen mit einem beim Mandantenmanager angemeldet sein [Unterstützter Webbrowser](#).
- Sie müssen einer Benutzergruppe angehören, die über die Berechtigung Alle Buckets verwalten oder Root Access verfügt. Diese Berechtigungen überschreiben die Berechtigungseinstellungen in Gruppen- oder Bucket-Richtlinien.

Über diese Aufgabe

Cross-Origin Resource Sharing (CORS) 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>.

Schritte

1. Verwenden Sie einen Texteditor, um die XML-Datei zu erstellen, die für die Aktivierung von CORS erforderlich ist.

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 im Tenant Manager **STORAGE (S3) Buckets** aus.
3. Wählen Sie den Bucket-Namen aus der Liste aus.

Die Seite mit den Bucket-Details wird angezeigt.

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

The screenshot shows the 'Bucket access' tab selected in the AWS S3 console. Under the 'Cross-Origin Resource Sharing (CORS)' section, it is currently 'Disabled'. A descriptive text explains how to configure CORS for an S3 bucket to allow access from other domains. Below this, there is a checkbox labeled 'Enable CORS' which is checked. To the right of the checkbox is a 'Clear' button. A large text area displays the XML configuration code:

```
<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>
  </corsRule>
</corsConfiguration>
```

At the bottom right of the configuration area is a blue 'Save changes' button.

7. Um die CORS-Einstellung für den Bucket zu ändern, aktualisieren Sie die CORS-Konfigurations-XML im Textfeld oder wählen Sie **Löschen**, um neu zu starten. Wählen Sie dann **Änderungen speichern**.
8. Um CORS für den Bucket zu deaktivieren, deaktivieren Sie das Kontrollkästchen **CORS aktivieren*** und wählen dann **Änderungen speichern** aus.

S3-Bucket löschen

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

Was Sie benötigen

- Sie müssen mit einem beim Mandantenmanager angemeldet sein [Unterstützter Webbrowser](#).
- Sie müssen einer Benutzergruppe angehören, die über die Berechtigung Alle Buckets verwalten oder Root Access verfügt. Diese Berechtigungen überschreiben die Berechtigungseinstellungen in Gruppen- oder Bucket-Richtlinien. Siehe [Mandantenmanagement-Berechtigungen](#).
- 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](#).

Ein S3-Bucket kann nicht gelöscht werden, wenn er Objekte oder nicht aktuelle Objektversionen enthält. Informationen zum Löschen von S3-versionierten Objekten finden Sie im [Anweisungen zum Verwalten von Objekten mit Information Lifecycle Management](#).

Schritte

1. Wählen Sie **STORAGE (S3) Buckets** aus.

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

The screenshot shows the AWS S3 Buckets management interface. At the top, it says "Create buckets and manage bucket settings." Below that, there's a "Create bucket" button. The main area is titled "Buckets" and displays a table of existing buckets. The columns are: Name, S3 Object Lock, Region, Object Count, Space Used, and Date Created. The table contains three rows:

Name	S3 Object Lock	Region	Object Count	Space Used	Date Created
bucket-01a	✓	us-east-1	0	0 bytes	2022-01-06 13:48:08 MST
bucket-02a	✓	us-east-1	0	0 bytes	2022-01-06 13:48:26 MST
bucket-03a		us-east-1	0	0 bytes	2022-01-06 13:48:38 MST

2. Aktivieren Sie das Kontrollkästchen für den leeren Bucket, den Sie löschen möchten. Sie können mehrere Bucket gleichzeitig auswählen.

Das Menü Aktionen ist aktiviert.

3. Wählen Sie im Menü Aktionen die Option **Bucket löschen** (oder **Buckets löschen**, wenn Sie mehrere ausgewählt haben).

The screenshot shows the same AWS S3 Buckets page, but now the "Actions" menu is open over the first row. The "Delete bucket" option is highlighted. The table below shows the same three buckets, with the first one having its checkbox checked.

Name	S3 Object Lock	Region	Object Count	Space Used	Date Created
bucket-01	✓	us-east-1	0	0 bytes	2021-12-02 11:14:26 MST
bucket-02		us-east-1	0	0 bytes	2021-12-02 11:14:49 MST

4. Wenn das Bestätigungsdialogfeld angezeigt wird, wählen Sie **Ja** aus, um alle ausgewählten Buckets zu löschen.

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. Sie müssen alle Objekte löschen, bevor Sie einen Bucket löschen können.

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

 S3 Console wurde nicht vollständig getestet und ist als „experimentell“ gekennzeichnet. Sie ist nicht für die Massenverwaltung von Objekten oder für die Verwendung in einer Produktionsumgebung bestimmt. 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.

Was Sie benötigen

- Sie sind mit einem beim Mandantenmanager angemeldet [Unterstützter Webbrowser](#).
- Sie verfügen über die Berechtigung zum Verwalten Ihrer eigenen S3-Anmeldedaten.
- Sie haben einen Bucket erstellt.
- 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 BESCHRÄNKKT 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, BEISPIELHAFFE SCHÄDEN ODER FOLGESCHÄDEN (EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKKT 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 IRGENDERWEINER 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.