



Management von S3-Buckets

StorageGRID 11.5

NetApp
April 11, 2024

Inhalt

- Management von S3-Buckets 1
 - Verwenden der S3-Objektsperre 1
 - Erstellen eines S3-Buckets 5
 - Anzeigen von S3-Bucket-Details 8
 - Ändern der Konsistenzstufe 10
 - Aktivieren oder Deaktivieren von Updates der letzten Zugriffszeit 13
 - Konfigurieren der Cross-Origin Resource Sharing (CORS) 16
 - Löschen eines S3-Buckets 18

Management von S3-Buckets

Wenn Sie einen S3-Mandanten mit entsprechenden Berechtigungen verwenden, können Sie S3-Buckets erstellen, anzeigen und löschen, Einstellungen für Konsistenzstufen aktualisieren, Cross-Origin Resource Sharing (CORS) konfigurieren, Einstellungen für Updates der letzten Zugriffszeit aktivieren bzw. deaktivieren und S3-Platfformservices managen.

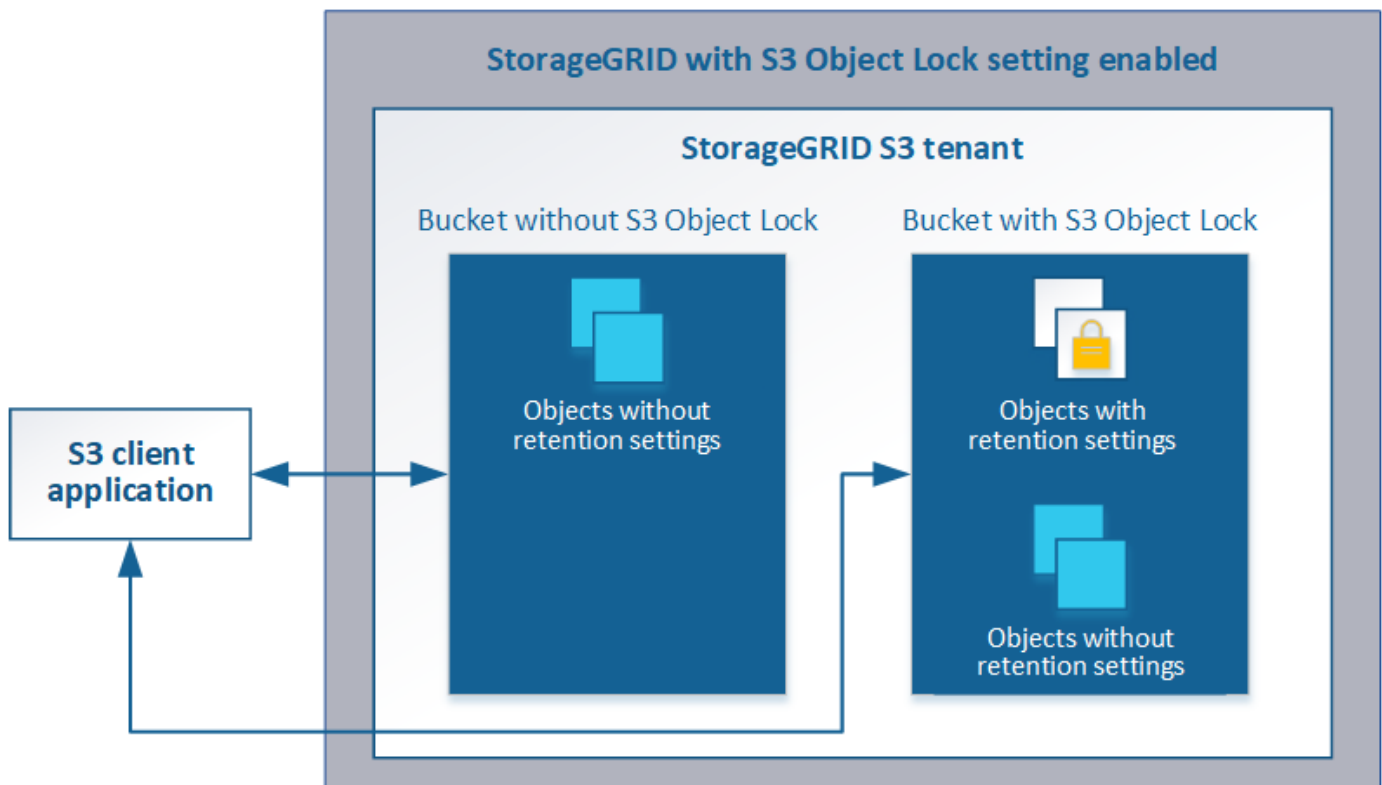
Verwenden der S3-Objektsperre

Sie können die S3-Objektsperrefunktion 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 Aufbewahrungspflicht hat kein Ablaufdatum, bleiben aber bis zur ausdrücklichen Entfernung erhalten. Die gesetzlichen Aufbewahrungspflichten sind unabhängig von der bisherigen Aufbewahrungsfrist.

Weitere Informationen zu diesen Einstellungen finden Sie unter „Using S3 object Lock“ in ["Unterstützte Vorgänge und Einschränkungen durch S3-REST-API"](#).

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.

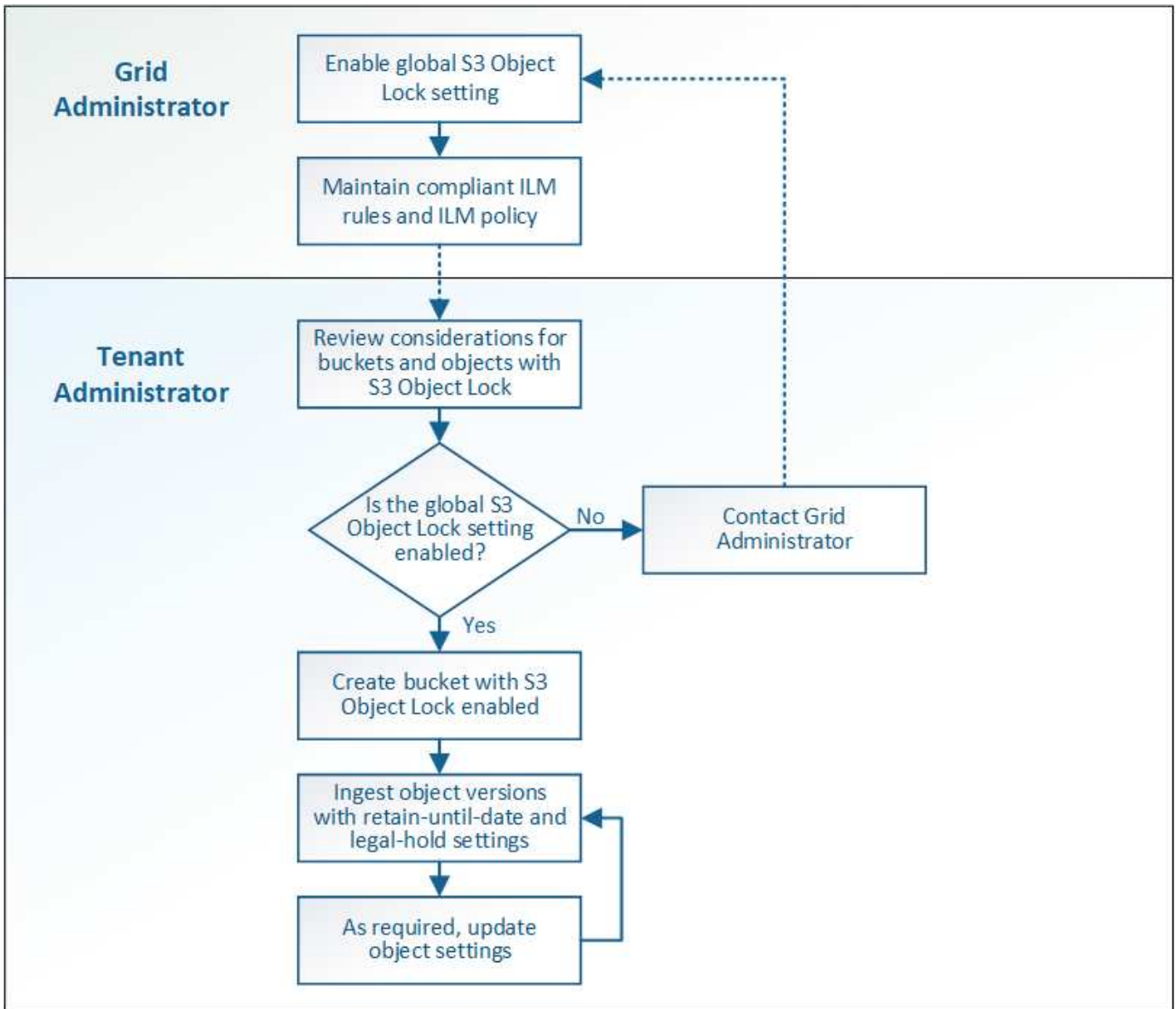
["NetApp Knowledge Base: Management älterer, konformer Buckets für StorageGRID 11.5"](#)

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 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 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.



Verwandte Informationen

["Objektmanagement mit ILM"](#)

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 aktivierter 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.

1 bucket

Create bucket

Actions ▾

<input type="checkbox"/>	Name ▾	S3 Object Lock  ▾	Region ▾	Object Count  ▾	Space Used  ▾	Date Created ▾
<input type="checkbox"/>	bank-records	✓	us-east-1	0	0 bytes	2021-01-06 16:53:19 MST

← Previous 1 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 aktivierter S3-Objektsperre erstellt haben, können Sie die S3-Objektsperre oder die Versionierung für diesen Bucket nicht deaktivieren.
- Ein StorageGRID-Bucket mit aktivierter S3-Objektsperre hat keinen standardmäßigen Aufbewahrungszeitraum. Stattdessen kann die S3-Client-Applikation optional für jede Objektversion, die zu diesem Bucket hinzugefügt wird, ein Aufbewahrungsdatum und eine Einstellung für die Aufbewahrung gemäß den gesetzlichen Aufbewahrungspflichten festlegen.
- 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

- Die S3-Client-Applikation muss Aufbewahrungseinstellungen für jedes Objekt angeben, das durch die S3-Objektsperre geschützt werden muss.
- 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 aktivierter S3-Objektsperre gespeichert wird, durchläuft drei Phasen:

1. Objektaufnahme

- Beim Hinzufügen einer Objektversion zu einem Bucket mit aktivierter 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.

Erstellen eines S3-Buckets

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

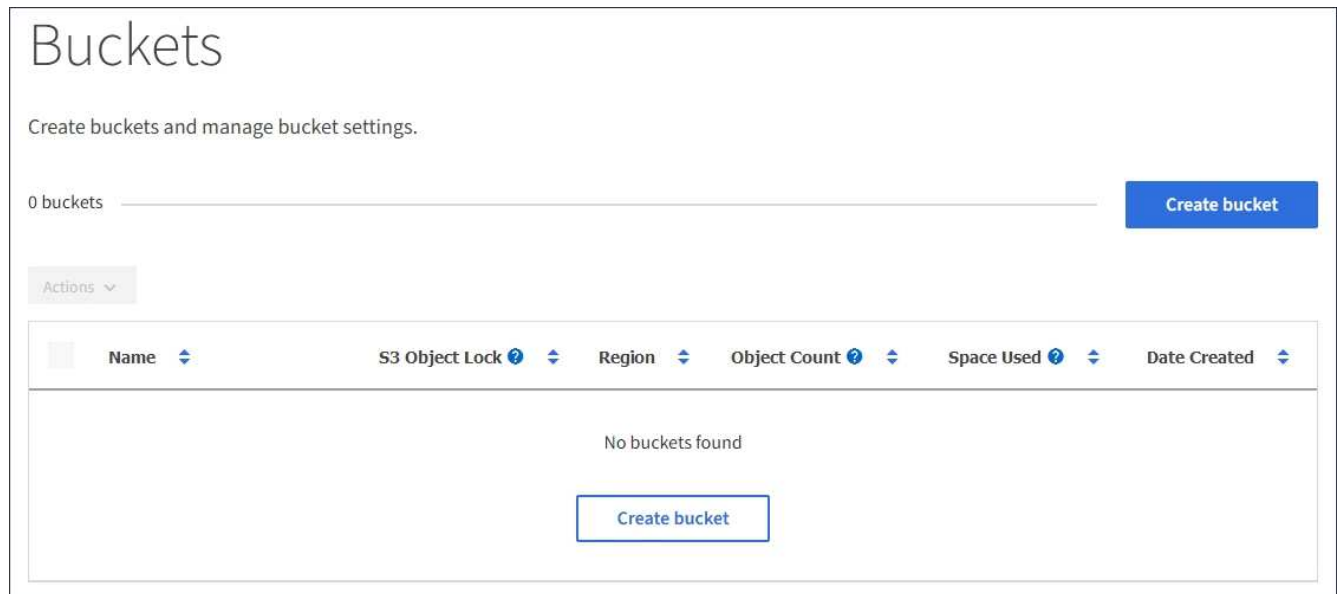
- Sie müssen über einen unterstützten Browser beim Tenant Manager angemeldet sein.
- Sie müssen einer Benutzergruppe angehören, die über die Berechtigung Alle Buckets verwalten oder Root Access verfügt. Diese Berechtigungen überschreiben die Berechtigungseinstellungen in Gruppen- oder Bucket-Richtlinien.
- Wenn Sie einen Bucket mit S3-Objektsperre erstellen möchten, muss die globale S3-Objektsperre für das StorageGRID-System aktiviert worden sein und Sie müssen die Anforderungen für S3-Objektsperren-Buckets und -Objekte überprüft haben.

["Verwenden der S3-Objektsperre"](#)

Schritte

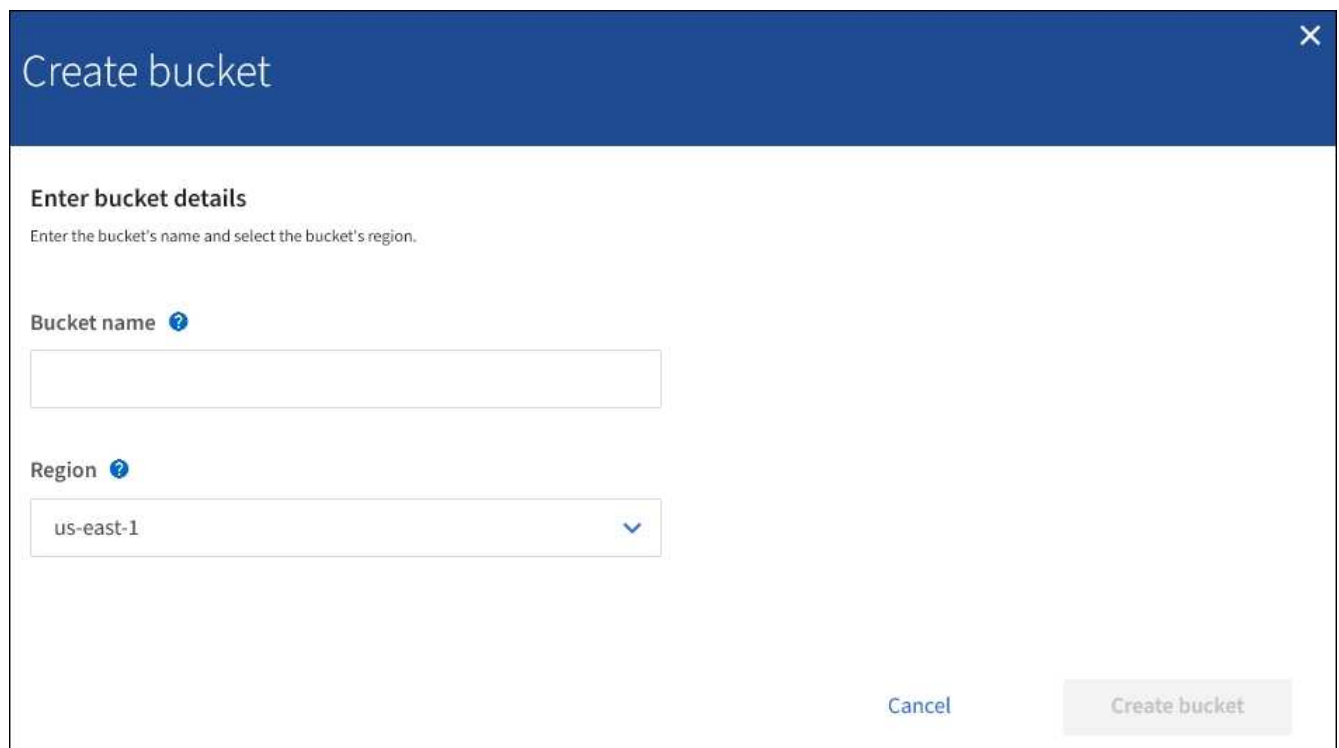
1. Wählen Sie **STORAGE (S3) > Buckets** aus.

Die Seite Buckets wird angezeigt und listet alle Buckets auf, die bereits erstellt wurden.



2. Wählen Sie **Eimer erstellen**.

Der Bucket-Assistent Erstellen wird angezeigt.



Wenn die globale S3-Objektsperre aktiviert ist, enthält Create Bucket einen zweiten Schritt zum Managen der S3-Objektsperre für den Bucket.

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.
- Kann eine Reihe von einer oder mehreren Etiketten sein, wobei angrenzende Etiketten durch einen Zeitraum getrennt sind. Jedes Etikett muss mit einem Kleinbuchstaben oder einer Zahl beginnen und enden. Es können nur Kleinbuchstaben, Ziffern und Bindestriche verwendet werden.
- Darf nicht wie eine Text-formatierte IP-Adresse aussehen.
- Perioden sollten nicht in Anforderungen im virtuellen gehosteten Stil verwendet werden. Perioden verursachen Probleme bei der Überprüfung des Server-Platzhalterzertifikats.



Weitere Informationen finden Sie in der Dokumentation zu Amazon Web Services (AWS).

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 erstellten `us-east-1` erstellt.



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

5. Wählen Sie **Eimer erstellen** oder **Weiter**.

- Wenn die globale S3-Objektsperre nicht aktiviert ist, wählen Sie **Bucket erstellen** aus. Der Bucket wird erstellt und der Tabelle auf der Seite Buckets hinzugefügt.
- Wenn die globale S3-Objektsperre aktiviert ist, wählen Sie **Weiter**. Schritt 2, S3-Objektsperre verwalten, wird angezeigt.

×

Create bucket

✓ Enter details
 2 Manage S3 Object Lock
Optional

Manage S3 Object Lock (This step is optional)

S3 Object Lock allows you to specify retention and legal hold settings for the objects ingested into a bucket. If you want to use S3 Object Lock, you must enable this setting when you create the bucket. You cannot add or disable S3 Object Lock after a bucket is created.

If S3 Object Lock is enabled, bucket versioning is required and will be enabled automatically.

Enable S3 Object Lock

Previous
Create bucket

6. Aktivieren Sie optional das Kontrollkästchen, um die S3-Objektsperre für diesen Bucket zu aktivieren.

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.



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



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

7. Wählen Sie **Eimer erstellen**.

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

Verwandte Informationen

["Objektmanagement mit ILM"](#)

["Das Mandantenmanagement-API von NetApp"](#)

["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 über einen unterstützten Browser beim Tenant Manager angemeldet sein.

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.

2 buckets Create bucket

Actions ▾

<input type="checkbox"/>	Name ▾	S3 Object Lock  ▾	Region ▾	Object Count  ▾	Space Used  ▾	Date Created ▾
<input type="checkbox"/>	bucket-01	✓	us-east-1	0	0 bytes	2020-11-04 14:16:59 MST
<input type="checkbox"/>	bucket-02		us-east-1	0	0 bytes	2020-11-04 14:17:14 MST

← Previous **1** Next →

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 verwendeter Speicherplatz sind Schätzungen. Diese Schätzungen sind vom Zeitpunkt der Aufnahme, der Netzwerkverbindung und des Node-Status betroffen.

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

Die Seite mit den Bucket-Details wird angezeigt.

Auf dieser Seite können Sie die Einstellungen für Bucket-Optionen, Bucket-Zugriff und Plattform-Services anzeigen und bearbeiten.

Weitere Informationen zur Konfiguration der einzelnen Einstellungen oder des Plattform-Service finden Sie in den Anweisungen.

Buckets > bucket-02

Overview

Name:	bucket-02
Region:	us-east-1
S3 Object Lock:	Disabled
Date created:	2020-11-04 14:51:59 MST

Bucket options Bucket access Platform services

Consistency level	Read-after-new-write	▼
Last access time updates	Disabled	▼

Verwandte Informationen

["Ändern der Konsistenzstufe"](#)

["Aktivieren oder Deaktivieren von Updates der letzten Zugriffszeit"](#)

["Konfigurieren der Cross-Origin Resource Sharing \(CORS\)"](#)

["CloudMirror-Replizierung wird konfiguriert"](#)

["Ereignisbenachrichtigungen werden konfiguriert"](#)

["Konfigurieren des Suchintegrationsservice"](#)

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 über einen unterstützten Browser beim Tenant Manager angemeldet sein.
- 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

Die Konsistenzstufe sorgt für einen Kompromiss zwischen der Verfügbarkeit der Objekte und der Konsistenz dieser Objekte über verschiedene Speicherknoten 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.

Bucket options
Bucket access
Platform services

Consistency level
Read-after-new-write (default)
⤴

Change the consistency control for operations performed on the objects in the bucket. Consistency level makes a trade-off between the availability of the objects and the consistency of those objects across different Storage Nodes and sites.

In general, use the **Read-after-new-write** consistency level for your buckets. Then, if objects do not meet availability or consistency requirements, change the client application's behavior, or set the Consistency-Control header for an individual API request, which overrides the bucket setting.

- All**
Provides the highest guarantee of consistency. All nodes receive the data immediately, or the request will fail.
- Strong-global**
Guarantees read-after-write consistency for all client requests across all sites.
- Strong-site**
Guarantees read-after-write consistency for all client requests within a site.
- Read-after-new-write (default)**
Provides read-after-write consistency for new objects and eventual consistency for object updates. Offers high availability, and data protection guarantees.

Note: If your application attempts HEAD operations on keys that do not exist, set the Consistency Level to **Available**, unless you require AWS S3 consistency guarantees. Otherwise, a high number of 500 Internal Server errors can result if one or more Storage Nodes are unavailable.

- Available**
Behaves the same as the **Read-after-new-write** consistency level, but only provides eventual consistency for HEAD operations. Offers higher availability for HEAD operations than **Read-after-new-write** if Storage Nodes are unavailable. Differs from AWS S3 consistency guarantees for HEAD operations only.

Save changes

4. Wählen Sie eine Konsistenzstufe für Operationen aus, die an den Objekten in diesem Bucket durchgeführt werden.

Konsistenzstufe	Beschreibung
Alle	Alle Nodes erhalten die Daten sofort, sonst schlägt die Anfrage fehl.

Konsistenzstufe	Beschreibung
Stark global	Garantierte Konsistenz bei Lese-nach-Schreibvorgängen für alle Client-Anfragen an allen Standorten.
Stark vor Ort	Garantiert Konsistenz bei Lese-nach-Schreibvorgängen für alle Client-Anfragen innerhalb eines Standorts.
Read-after-New-Write (Standard)	<p>Ermöglicht Konsistenz von Lese- nach Schreibvorgängen für neue Objekte und die eventuelle Konsistenz von Objekt-Updates. Hochverfügbarkeit und garantierte Datensicherung Entspricht den Amazon S3 -Konsistenzgarantien.</p> <p>Hinweis: Wenn Ihre Anwendung versucht, HEAD-Operationen auf Schlüssel, die nicht vorhanden sind, setzen Sie die Consistency Level auf available, es sei denn, Sie benötigen Amazon S3 Consistency Guarantees. Andernfalls kann eine hohe Anzahl von 500 internen Serverfehlern führen, wenn ein oder mehrere Speicherknoten nicht verfügbar sind.</p>
Verfügbar (eventuelle Konsistenz für DEN HAUPTBETRIEB)	Verhält sich wie die Konsistenz Read-after-New-write , bietet aber nur eventuelle Konsistenz für DEN KOPFBETRIEB. Bietet höhere Verfügbarkeit für DEN HAUPTBETRIEB als Read-after-New-write , wenn Speicherknoten nicht verfügbar sind. Unterschied zu Amazon S3 Konsistenzgarantien nur für HEAD-Operationen.

5. Wählen Sie **Änderungen speichern**.

Verwandte Informationen

["Mandantenmanagement-Berechtigungen"](#)

Aktivieren oder Deaktivieren von 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 über einen unterstützten Browser beim Tenant Manager angemeldet sein.
- 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.

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.

Bucket options
Bucket access
Platform services

Consistency level Read-after-new-write ▼

Last access time updates Disabled ▲

Enable or disable last access time updates for the objects in this bucket.

When last access time updates are disabled, the following behavior applies to objects in the bucket:

- Requests to retrieve an object, its access control list, or its metadata do not update the object's last access time. The object is not added to ILM evaluation queues.
- Requests to update an object's metadata update the object's last access time. The object is added to ILM evaluation queues.
- Requests to copy an object from one bucket to another do not update the last access time for the source copy and do not add the source object to the ILM evaluation queue. However, the last access time is updated for the destination copy, and the destination object is added to ILM evaluation queues.
- A request to complete a multipart upload causes the last access time for the assembled object to be updated. The new object is added to ILM evaluation queues.

i Updating the last access time when an object is retrieved can reduce performance, especially for small objects.

Enable last access time updates when retrieving an object
 Disable last access time updates when retrieving an object

Save changes

5. Wählen Sie **Änderungen speichern**.

Verwandte Informationen

["Mandantenmanagement-Berechtigungen"](#)

["Objektmanagement mit ILM"](#)

Konfigurieren der Cross-Origin Resource Sharing (CORS)

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 über einen unterstützten Browser beim Tenant Manager angemeldet sein.
- 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-Zugriff > 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**.

Bucket options
Bucket access
Platform services

Cross-Origin Resource Sharing (CORS)

Disabled

▲

Configure Cross-Origin Resource Sharing (CORS) for an S3 bucket if you want that bucket and objects in that bucket to be accessible to web applications in other domains.

Enable CORS

Clear

```

<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>

```

Save changes

7. Um die CORS-Einstellung für den Bucket zu ändern, aktualisieren Sie die CORS-Konfigurations-XML in 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.

Löschen eines S3-Buckets

Sie können den Mandanten-Manager verwenden, um einen leeren S3-Bucket zu löschen.

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Tenant Manager angemeldet sein.
- 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

Diese Anweisungen beschreiben das Löschen eines S3-Buckets mithilfe von Tenant Manager. Sie können auch S3-Buckets mithilfe der Mandantenmanagement-API oder der S3-REST-API löschen.

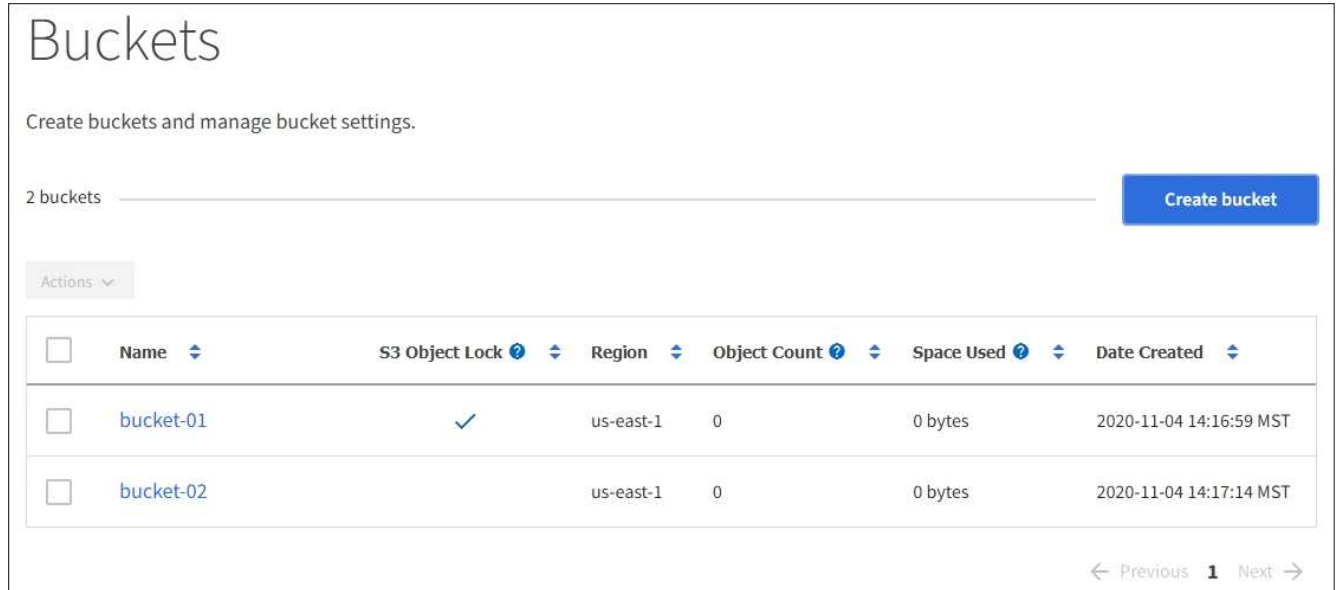
Ein S3-Bucket kann nicht gelöscht werden, wenn er Objekte oder nicht aktuelle Objektversionen enthält.

Informationen zum Löschen von S3-versionierten Objekten finden Sie in den Anweisungen zum Managen 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 console. At the top, it says "Buckets" and "Create buckets and manage bucket settings." Below that, it indicates "2 buckets" and has a "Create bucket" button. A table lists the buckets:

<input type="checkbox"/>	Name	S3 Object Lock	Region	Object Count	Space Used	Date Created
<input type="checkbox"/>	bucket-01	✓	us-east-1	0	0 bytes	2020-11-04 14:16:59 MST
<input type="checkbox"/>	bucket-02		us-east-1	0	0 bytes	2020-11-04 14:17:14 MST

At the bottom right, there are navigation arrows: "← Previous 1 Next →".

2. Aktivieren Sie das Kontrollkästchen für den leeren Bucket, den Sie löschen möchten.

Das Menü Aktionen ist aktiviert.

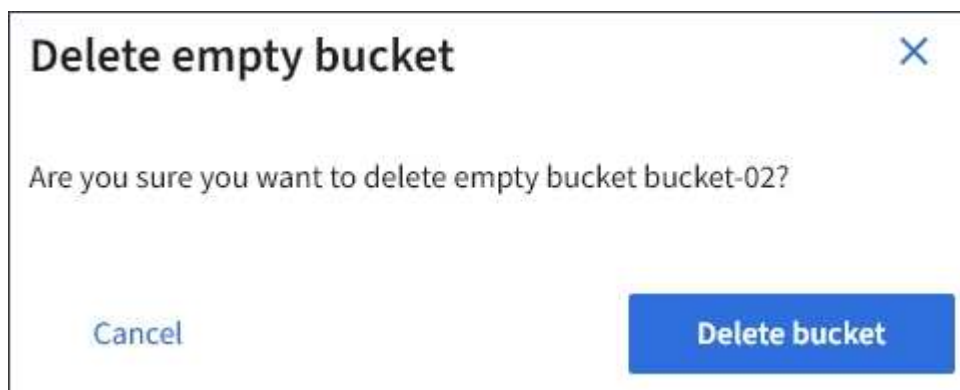
3. Wählen Sie im Menü Aktionen die Option **leerer Eimer löschen** aus.



The screenshot shows the same AWS S3 Buckets console, but with the "Actions" menu open. The "Delete empty bucket" option is selected. The table below shows that the checkbox for "bucket-02" is now checked:

<input type="checkbox"/>	Name	S3 Object Lock	Region	Object Count	Space Used	Date Created
<input type="checkbox"/>	bucket-01	✓	us-east-1	0	0 bytes	2020-11-04 14:16:59 MST
<input checked="" type="checkbox"/>	bucket-02		us-east-1	0	0 bytes	2020-11-04 14:17:14 MST

Eine Bestätigungsmeldung wird angezeigt.



The screenshot shows a confirmation dialog box titled "Delete empty bucket". The text inside asks: "Are you sure you want to delete empty bucket bucket-02?". At the bottom, there are two buttons: "Cancel" and "Delete bucket".

4. Wenn Sie sicher sind, dass Sie den Bucket löschen möchten, wählen Sie **Bucket löschen**.

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

Wenn der Bucket nicht leer ist, wird eine Fehlermeldung angezeigt. Sie müssen alle Objekte löschen, bevor Sie den Bucket löschen können.



Unable to delete the bucket because it is not empty. You must delete all objects before you can delete this bucket.

Verwandte Informationen

["Objektmanagement mit ILM"](#)

Copyright-Informationen

Copyright © 2024 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtinhabers in keiner Form und durch keine Mittel – weder grafische noch elektronische oder mechanische, einschließlich Fotokopieren, Aufnehmen oder Speichern in einem elektronischen Abrufsystem – auch nicht in Teilen, vervielfältigt werden.

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

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

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

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

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

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

Markeninformationen

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