



S3 Buckets verwalten

StorageGRID software

NetApp
July 23, 2026

Inhalt

S3 Buckets verwalten	1
Erstellen Sie einen StorageGRID S3-Bucket	1
Assistenten aufrufen	1
Details eingeben	1
Einstellungen verwalten	2
S3-Bucket-Details in StorageGRID anzeigen	4
Erfahren Sie mehr über StorageGRID Branch-Buckets	6
Beispiele für die Verwendung von Branch Buckets	7
Operationen an Objekten in Branch Buckets	7
StorageGRID-Branch-Buckets verwalten	8
Branch Bucket erstellen	9
Details eingeben	9
Objekteinstellungen verwalten (optional)	10
Wenden Sie ein ILM-Policy-Tag auf einen StorageGRID Bucket an	12
StorageGRID Bucket-Richtlinie verwalten	13
Konsistenz von StorageGRID-Buckets verwalten	14
\${post_edited_translations.segment}	14
Bucket-Konsistenz ändern	14
\${post_edited_translations.segment}	15
Aktivieren oder deaktivieren Sie Aktualisierungen der letzten Zugriffszeit in StorageGRID	16
Objektversionierung für einen S3-Bucket in StorageGRID ändern	18
Verwenden Sie S3 Object Lock, um Objekte in StorageGRID aufzubewahren	19
Was ist S3 Object Lock?	19
S3 Object Lock Aufgaben	21
Anforderungen für Buckets mit aktiviertem S3 Object Lock	21
Anforderungen an Objekte in Buckets mit aktiviertem S3 Object Lock	22
Lebenszyklus von Objekten in Buckets mit aktiviertem S3 Object Lock	22
Kann ich weiterhin ältere Compliant Buckets verwalten?	22
Aktualisieren Sie die Standardaufbewahrung für S3 Object Lock in StorageGRID	23
Konfigurieren Sie CORS für S3-Buckets in StorageGRID	24
CORS für einen Bucket aktivieren	25
CORS-Einstellung ändern	25
CORS-Einstellung deaktivieren	26
Objekte aus einem StorageGRID S3-Bucket löschen	26
Löschen eines StorageGRID S3 bucket	29
Verwenden Sie die S3-Konsole in StorageGRID	30

S3 Buckets verwalten

Erstellen Sie einen StorageGRID S3-Bucket

Mit dem Tenant Manager können Sie S3 Buckets für Objektdaten erstellen.

Bevor Sie beginnen

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



Berechtigungen zum Festlegen oder Ändern von S3 Object Lock-Eigenschaften von Buckets oder Objekten können durch ["Bucket Policy oder Gruppenrichtlinie"](#) gewährt werden.

- Wenn Sie planen, S3 Object Lock für einen Bucket zu aktivieren, hat ein Grid-Administrator die globale S3 Object Lock-Einstellung für das StorageGRID System aktiviert und Sie haben die Anforderungen für S3 Object Lock Buckets und Objekte überprüft.
- Wenn jeder Mandant 5.000 Buckets hat, verfügt jeder Speicherknoten im Grid über mindestens 64 GB RAM.



Jedes Grid kann maximal 100.000 Buckets enthalten, einschließlich ["Branch Buckets"](#).

Assistenten aufrufen

Schritte

1. **View buckets** im Dashboard auswählen oder **STORAGE (S3) > Buckets**.
2. **Bucket erstellen** auswählen.

Details eingeben

Schritte

1. Geben Sie die Details für den Bucket ein.

Feld	Beschreibung
Bucket Name	Ein Name für den Bucket, der diesen Regeln entspricht: • Muss in jedem StorageGRID System eindeutig sein (nicht nur innerhalb des Mandantenkontos). • Muss DNS-konform sein. • Muss mindestens 3 und höchstens 63 Zeichen enthalten. • Jedes Etikett muss mit einem Kleinbuchstaben oder einer Zahl beginnen und enden und darf nur Kleinbuchstaben, Zahlen und Bindestriche enthalten. • Anfragen im virtuellen Hosting-Stil dürfen keine Punkte enthalten. Punkte verursachen Probleme bei der Überprüfung des Server-Wildcard-Zertifikats. Weitere Informationen finden Sie unter "Dokumentation von Amazon Web Services (AWS) zu den Regeln für die Bucket-Benennung". Hinweis: Der Bucket-Name kann nach der Erstellung des Buckets nicht mehr geändert werden.
Region	Die Region des Buckets. Ihr StorageGRID Administrator verwaltet die verfügbaren Regionen. Die Region eines Buckets kann die auf Objekte angewendete Datenschutzrichtlinie beeinflussen. Standardmäßig werden alle Buckets in der <code>us-east-1</code> Region erstellt. Wenn die Standardregion auf eine andere Region als <code>us-east-1</code> konfiguriert ist, wird diese andere Region zunächst im Dropdown-Menü ausgewählt. Hinweis: Die Region kann nach dem Erstellen des Buckets nicht mehr geändert werden.

2. Wählen Sie **Weiter**.

Einstellungen verwalten

Schritte

1. Optional kann die Objektversionierung für den Bucket aktiviert werden.

Die Objektversionierung kann aktiviert werden, wenn jede Version jedes Objekts in diesem Bucket gespeichert werden soll. Frühere Versionen eines Objekts können anschließend bei Bedarf abgerufen werden.

Sie müssen die Objektversionierung aktivieren, wenn:

- Der Bucket wird für die gridübergreifende Replikation verwendet.
- Sie möchten ein ["Branch-Bucket"](#) aus diesem Bucket erstellen.

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

Die S3 Object Lock-Funktion sollte für einen Bucket nur aktiviert werden, wenn Objekte für einen festgelegten Zeitraum aufbewahrt werden müssen, beispielsweise um bestimmte regulatorische Anforderungen zu erfüllen. S3 Object Lock ist eine permanente Einstellung, die verhindert, dass Objekte für einen festgelegten Zeitraum oder unbegrenzt gelöscht oder überschrieben werden.



Nachdem die S3 Object Lock-Einstellung für einen Bucket aktiviert wurde, kann sie nicht mehr deaktiviert werden. Jede Person mit den entsprechenden Berechtigungen kann diesem Bucket Objekte hinzufügen, die nicht geändert werden können. Möglicherweise können diese Objekte oder der Bucket selbst nicht gelöscht werden.

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

3. Wenn Sie **S3 Object Lock aktivieren** ausgewählt haben, kann optional **Standardaufbewahrung** für diesen Bucket aktiviert werden.



Ihr Grid-Administrator muss Ihnen die Berechtigung geben, "[spezifische Funktionen von S3 Object Lock](#)".

Wenn die **Standardaufbewahrung** aktiviert ist, werden neu hinzugefügte Objekte im Bucket automatisch vor dem Löschen oder Überschreiben geschützt. Die Einstellung **Standardaufbewahrung** gilt nicht für Objekte mit eigenen Aufbewahrungsfristen.

- a. Wenn die **Standardaufbewahrung** aktiviert ist, ist ein **Standardaufbewahrungsmodus** für den Bucket anzugeben.

Standard-Aufbewahrungsmodus	Beschreibung
Governance	• Benutzer mit der <code>s3:BypassGovernanceRetention</code> Berechtigung können den <code>x-amz-bypass-governance-retention: true</code> Anfrageheader verwenden, um die Aufbewahrungseinstellungen zu umgehen. • Diese Benutzer können eine Objektversion löschen, bevor deren Aufbewahrungsdatum erreicht ist. • Diese Benutzer können das Aufbewahrungsdatum eines Objekts erhöhen, verringern oder entfernen.
Einhaltung	• Das Objekt kann erst gelöscht werden, wenn sein Aufbewahrungsdatum erreicht ist. • Das Aufbewahrungsdatum des Objekts kann erhöht, aber nicht verringert werden. • Das Aufbewahrungsdatum des Objekts kann erst nach Erreichen dieses Datums entfernt werden. Hinweis: Ihr Grid-Administrator muss Ihnen die Verwendung des Compliance-Modus erlauben.

- b. Wenn die **Standardaufbewahrung** aktiviert ist, ist die **Standardaufbewahrungsdauer** für den Bucket anzugeben.

Die **Standardaufbewahrungsdauer** gibt an, wie lange neue Objekte, die diesem Bucket hinzugefügt werden, ab dem Zeitpunkt ihrer Aufnahme aufbewahrt werden sollen. Es ist ein Wert anzugeben, der kleiner oder gleich der maximalen Aufbewahrungsdauer für den Mandanten ist, wie sie vom Grid-Administrator festgelegt wurde.

Beim Anlegen des Mandanten durch den Grid-Administrator wird eine *maximale* Aufbewahrungsdauer festgelegt, die zwischen 1 Tag und 100 Jahren liegen kann. Wenn eine *standardmäßige* Aufbewahrungsdauer festgelegt wird, darf sie den für die maximale Aufbewahrungsdauer festgelegten Wert nicht überschreiten. Falls erforderlich, kann der Grid-Administrator gebeten werden, die maximale Aufbewahrungsdauer zu erhöhen oder zu verringern.

- Optional kann **Kapazitätslimit aktivieren** ausgewählt, ein Wert eingegeben und die Kapazitätseinheit ausgewählt werden.

Die Kapazitätsgrenze ist die maximal verfügbare Kapazität für die Objekte dieses Buckets. Dieser Wert stellt eine logische Größe (Objektgröße) und keine physische Größe (Größe auf der Festplatte) dar.

Wenn kein Limit festgelegt ist, ist die Kapazität dieses Buckets unbegrenzt. Weitere Informationen finden Sie unter "[Kapazitätslimitnutzung](#)".

- Optional kann **Objektanzahlbegrenzung aktivieren** ausgewählt werden.

Die Objektanzahlbegrenzung gibt die maximale Anzahl an Objekten an, die dieser Bucket enthalten kann. Dieser Wert stellt eine logische Anzahl (Objektanzahl) dar. Wenn keine Begrenzung festgelegt ist, ist die Objektanzahl unbegrenzt.

- Bucket erstellen** auswählen.

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

- Optional kann **Zur Bucket-Detailseite** ausgewählt werden, um "[Bucket-Details](#)" weitere Konfigurationen vorzunehmen.

Sie können auch "[Branch-Buckets erstellen](#)" nach Bedarf.

S3-Bucket-Details in StorageGRID anzeigen

Sie können die Buckets in Ihrem Mandantenkonto anzeigen.

Bevor Sie beginnen

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

Schritte

- View buckets** im Dashboard auswählen oder **STORAGE (S3) > Buckets**.

Die Buckets-Seite wird angezeigt.

- Die Zusammenfassungstabelle für jeden Bucket kann eingesehen werden.

Bei Bedarf können Sie die Informationen nach jeder beliebigen Spalte sortieren oder in der Liste vor- und zurückblättern.



Die angezeigten Werte für Objektanzahl, Speicherplatznutzung und Auslastung sind Schätzwerte. Diese Schätzwerte werden durch den Zeitpunkt der Datenaufnahme, die Netzwerkverbindung und den Knotenstatus beeinflusst. Wenn für Buckets die Versionierung aktiviert ist, werden gelöschte Objektversionen in die Objektanzahl einbezogen.

Name

Der eindeutige Name des Buckets, der nicht geändert werden kann.

Aktivierte Funktionen

Die Liste der für den Bucket aktivierten Funktionen.

S3 Object Lock

Ob S3 Object Lock für den Bucket aktiviert ist.

Diese Spalte wird nur angezeigt, wenn S3 Object Lock für das Grid aktiviert ist. Diese Spalte zeigt außerdem Informationen zu allen älteren Compliant Buckets an.

Region

Die Region des Buckets, die nicht geändert werden kann. Diese Spalte ist standardmäßig ausgeblendet.

Objektanzahl

Die Anzahl der Objekte in diesem Bucket. Wenn für Buckets die Versionierung aktiviert ist, sind nicht aktuelle Objektversionen in diesem Wert enthalten.

Wenn Objekte hinzugefügt oder gelöscht werden, wird dieser Wert möglicherweise nicht sofort aktualisiert.

Verwendeter Speicherplatz

Die logische Größe aller Objekte im Bucket. Die logische Größe beinhaltet nicht den tatsächlich benötigten Speicherplatz für replizierte oder mit Löschkodierung versehene Kopien oder für Objektmetadaten.

Die Aktualisierung dieses Wertes kann bis zu 10 Minuten dauern.

Verwendung

Der Prozentsatz der genutzten Kapazitätsgrenze des Buckets, sofern eine solche festgelegt wurde.

Der Nutzungswert basiert auf internen Schätzungen und kann in manchen Fällen überschritten werden. StorageGRID prüft beispielsweise das Kapazitätslimit (sofern festgelegt), wenn ein Mandant mit dem Hochladen von Objekten beginnt, und lehnt neue Uploads in diesen Bucket ab, falls das Kapazitätslimit überschritten wurde. StorageGRID berücksichtigt jedoch die Größe des aktuellen Uploads bei der Ermittlung, ob das Kapazitätslimit überschritten wurde, nicht. Werden Objekte gelöscht, kann ein Mandant vorübergehend daran gehindert werden, neue Objekte in diesen Bucket hochzuladen, bis die Kapazitätsnutzung neu berechnet wurde. Die Berechnungen können 10 Minuten oder länger dauern.

Dieser Wert gibt die logische Größe an, nicht die physische Größe, die zum Speichern der Objekte und ihrer Metadaten erforderlich ist.

Kapazität

Falls festgelegt, die Kapazitätsgrenze für den Bucket.

Erstellungsdatum

Datum und Uhrzeit, zu der der Bucket erstellt wurde. Diese Spalte ist standardmäßig ausgeblendet.

3. Details zu einem bestimmten Bucket werden angezeigt, wenn der Bucket-Name aus der Tabelle ausgewählt wird.
 - a. Die zusammenfassenden Informationen oben auf der Webseite geben Aufschluss über die Details zum Bucket, wie Region und Objektanzahl.
 - b. Die Auslastungsbalken für Kapazitätsgrenze und Objektanzahlgrenze anzeigen. Liegt die Auslastung bei 100 % oder nahe 100 %, empfiehlt es sich, das Limit zu erhöhen oder einige Objekte zu löschen.
 - c. Bei Bedarf **Objekte im Bucket löschen** und **Bucket löschen** auswählen.



Achten Sie genau auf die Warnhinweise, die beim Auswählen der einzelnen Optionen angezeigt werden. Weitere Informationen sind unter folgendem Link zu finden:

- ["Alle Objekte in einem Bucket löschen"](#)
- ["Einen Bucket löschen"](#) (Der Bucket muss leer sein)

- d. Die Einstellungen für den Bucket lassen sich bei Bedarf in den einzelnen Registerkarten anzeigen oder ändern.
 - **S3-Konsole:** Die Objekte des Buckets anzeigen. Weitere Informationen finden sich unter ["S3-Konsole verwenden"](#).
 - **Bucket-Optionen:** Optionseinstellungen anzeigen oder ändern. Einige Einstellungen, wie zum Beispiel S3 Object Lock, können nach der Erstellung des Buckets nicht mehr geändert werden.
 - ["Konsistenz von Buckets verwalten"](#)
 - ["Letzte Zugriffszeit-Aktualisierungen"](#)
 - ["Kapazitätsgrenze"](#)
 - ["Objektanzahlbegrenzung"](#)
 - ["Objektversionierung"](#)
 - ["S3 Object Lock"](#)
 - ["Standardmäßige Bucket-Aufbewahrungsdauer"](#)
 - ["Verwaltung der gridübergreifenden Replikation"](#) (sofern dies dem Mieter gestattet ist)
 - **Plattformdienste:** ["Plattformdienste verwalten"](#) (sofern für den Mandanten zulässig)
 - **Bucket-Zugriff:** Optionseinstellungen anzeigen oder ändern. Spezielle Zugriffsberechtigungen sind erforderlich.
 - Konfigurieren Sie ["CORS für Buckets und Objekte"](#) so, dass der Bucket und die darin enthaltenen Objekte für Webanwendungen in anderen Domänen zugänglich sind.
 - ["Benutzerzugriff kontrollieren"](#) für einen S3-Bucket und Objekte in diesem Bucket.
 - **Branches:** Die Liste der Branch-Buckets für den Bucket anzeigen. ["Einen neuen Branch Bucket erstellen oder Branch Buckets verwalten"](#).

Erfahren Sie mehr über StorageGRID Branch-Buckets

Ein Branch Bucket ermöglicht den Zugriff auf Objekte in einem Bucket, wie sie zu einem bestimmten Zeitpunkt existierten.

Ein Branch-Bucket wird aus einem bestehenden Bucket erstellt. Nach dem Erstellen eines Branch-Buckets wird der ursprüngliche Bucket, aus dem er erstellt wurde, als *Base Bucket* bezeichnet. Zusätzlich kann ein Branch-Bucket aus einem anderen Branch-Bucket erstellt werden.

Ein Branch-Bucket bietet Zugriff auf geschützte Daten, dient aber nicht als Backup. Um Daten weiterhin zu schützen, stehen diese Funktionen für Basis-Buckets zur Verfügung:

- ["S3 Object Lock"](#)
- ["Gridübergreifende Replikation"](#) für Basiseimer
- ["Bucket Richtlinien"](#) für versionierte Buckets zum Bereinigen alter Objektversionen

Die folgenden Eigenschaften von Branch Buckets sind zu beachten:

- Sie können auf die Objekte in Branch Buckets mit ["S3 Konsole zum Herunterladen von Objekten"](#) zugreifen.
- Wenn Clients auf Objekte in einem Branch-Bucket zugreifen, bestimmen die ["Zugriffsrichtlinien"](#) Richtlinien des Branch-Buckets und nicht die des Basis-Buckets, ob der Zugriff gewährt oder verweigert wird.
- Objekte, die in einem Basis-Bucket erstellt werden, werden danach bewertet, wie ["ILM Regeln"](#) auf den Basis-Bucket anwendbar sind. Objekte, die in einem Zweig-Bucket erstellt werden, werden danach bewertet, wie ILM-Regeln auf den Zweig-Bucket anwendbar sind.
- Die netzübergreifende Replikation wird für Branch Buckets nicht unterstützt.
- Plattformdienste werden für Branch Buckets nicht unterstützt.

Beispiele für die Verwendung von Branch Buckets

- Sie können einen Branch-Bucket verwenden, um beschädigte Objekte zu entfernen, indem ein Branch-Bucket von einem Zeitpunkt vor dem Auftreten der Beschädigung erstellt wird und Anwendungen anschließend auf den Branch-Bucket statt auf den Basis-Bucket verwiesen werden, der die beschädigten Objekte enthält.
- Sie speichern Daten in einem versionierten Bucket. Es gab eine versehentliche Schwachstelle, durch die viele unerwünschte Objekte nach dem Zeitpunkt T aufgenommen wurden. Es kann ein Branch Bucket für den Zeitpunkt vor T erstellt und Client-Operationen auf diesen Branch Bucket umgeleitet werden. So werden den Clients nur Objekte bereitgestellt, die vor dem Zeitpunkt T aufgenommen wurden.

Operationen an Objekten in Branch Buckets

- Eine PUT-Objektoperation auf einem Branch-Bucket erstellt ein Objekt im Branch.
- Eine GET-Operation auf einem Branch-Bucket ruft ein Objekt aus dem Branch ab. Existiert das Objekt nicht im Branch-Bucket, wird es aus dem Basis-Bucket abgerufen.
- Das Löschen von Objekten aus Branch Buckets erfolgt wie folgt:

Betrieb	Ziel	Ergebnis	Objektsichtbarkeit im Basis-Bucket	Objektsichtbarkeit im Branch-Bucket
Löschen ohne Versions-ID	Basiseimer	Der Löschmarker wird nur für den Basis-Bucket erstellt	HEAD/GET gibt zurück, dass das Objekt nicht existiert, aber auf bestimmte Versionen kann weiterhin zugegriffen werden.	HEAD/GET gibt zurück, dass das Objekt existiert, und bestimmte Versionen können weiterhin aufgerufen werden. Die Löschmarkierung wäre nach dem Branch Bucket <code>beforeTime</code> erstellt worden.
Löschen mit Versions-ID	Basiseimer	Die spezifische Objektversion wird sowohl für den Basis- als auch für den Branch-Bucket gelöscht.	HEAD/GET gibt zurück, dass die Objektversion nicht existiert	HEAD/GET gibt zurück, dass die Objektversion nicht existiert
Löschen ohne Versions-ID	Branch-Bucket	Die Löschmarkierung wird nur für den Branch Bucket erstellt.	HEAD/GET gibt ein Objekt zurück (das Basis-Bucket-Objekt ist davon nicht betroffen)	HEAD/GET gibt zurück, dass das Objekt nicht existiert
Löschen mit Versions-ID	Branch-Bucket	Eine bestimmte Objektversion wird nur für den Branch Bucket gelöscht.	HEAD/GET gibt eine bestimmte Objektversion zurück (das Basis-Bucket-Objekt ist nicht betroffen)	HEAD/GET gibt zurück, dass die Objektversion nicht existiert

Siehe auch ["Wie versionierte S3-Objekte gelöscht werden"](#).

StorageGRID-Branch-Buckets verwalten

Mit dem Tenant Manager lassen sich Branch-Buckets erstellen und Details dazu anzeigen.

Bevor Sie beginnen

- Sie haben sich beim Tenant Manager mit einem ["unterstützte Webbrowser"](#) angemeldet.
- Sie gehören einer Benutzergruppe an, die über Root-Zugriff oder ["Alle Buckets-Berechtigungen verwalten"](#) verfügt. Diese Berechtigungen überschreiben die Berechtigungseinstellungen in Gruppen- oder Bucket-Richtlinien.
- Der Basis-Bucket, von dem Sie einen Branch erstellen möchten, hat ["Versionierung aktiviert"](#).
- Sie sind der Besitzer des Basiseimers.

Über diese Aufgabe

Beachten Sie die folgenden Informationen zu Branch Buckets:

- Berechtigungen zum Festlegen von S3 Object Lock-Eigenschaften von Buckets oder Objekten können durch "[Bucket Policy](#) oder [Gruppenrichtlinie](#)" gewährt werden.
- Wenn die Versionierung des Basis-Buckets ausgesetzt wird, sind die Inhalte des Basis-Buckets in seinen Zweig-Buckets nicht mehr sichtbar.



Nachdem Sie einen Branch-Bucket konfiguriert und erstellt haben, kann die Konfiguration nicht mehr geändert werden.

Branch Bucket erstellen

Schritte

1. **View buckets** im Dashboard auswählen oder **STORAGE (S3) > Buckets**.
2. Wählen Sie den Bucket aus, von dem ein Branch erstellt werden soll (den „Base Bucket“).
3. Auf der Bucket-Detailseite **Branches > Create branch bucket** auswählen.

`${post_edited_translations.segment}`

Details eingeben

Schritte

1. `${post_edited_translations.segment}`

Feld	Beschreibung
Name des Branch-Buckets	<code>\${post_edited_translations.segment}</code> • Muss in jedem StorageGRID System eindeutig sein (nicht nur innerhalb des Mandantenkontos). • Muss DNS-konform sein. • Muss mindestens 3 und höchstens 63 Zeichen enthalten. • Jedes Etikett muss mit einem Kleinbuchstaben oder einer Zahl beginnen und enden und darf nur Kleinbuchstaben, Zahlen und Bindestriche enthalten. • Anfragen im virtuellen Hosting-Stil dürfen keine Punkte enthalten. Punkte verursachen Probleme bei der Überprüfung des Server-Wildcard-Zertifikats. Weitere Informationen finden Sie unter "Dokumentation von Amazon Web Services (AWS) zu den Regeln für die Bucket-Benennung". <code>\${post_edited_translations.segment}</code>
Region (kann für Branch Buckets nicht geändert werden)	<code>\${post_edited_translations.segment}</code> <code>\${post_edited_translations.segment}</code>

Feld	Beschreibung
<code>#{post_edited_translation.s.segment}</code>	Der Grenzzeitpunkt, bis zu dem im Base Bucket erstellte Objektversionen über das Branch Bucket zugänglich sind. Das Branch Bucket bietet Zugriff auf Objektversionen, die vor dem „Before“-Zeitpunkt erstellt wurden. Vorher muss ein Datum und eine Uhrzeit sein, die bereits vergangen sind. Es kann kein zukünftiges Datum sein.
Branch-Bucket-Typ	• Lese-/Schreibzugriff: Es besteht die Möglichkeit, Objekte oder Objektversionen im Branch Bucket hinzuzufügen oder zu löschen. • Schreibgeschützt: Sie können Objekte im Branch-Bucket nicht verändern. Hinweis: Sie können den Typ des Branch-Buckets nur dann auf „Read-Only“ festlegen, wenn der Branch-Bucket leer ist. Wenn der Typ für einen vorhandenen Branch-Bucket auf „Read-Write“ festgelegt ist und Sie noch keine Daten darauf geschrieben haben, können Sie den Typ in „Read-Only“ ändern.

2. Wählen Sie **Weiter**.

Objekteinstellungen verwalten (optional)

Die Objekteinstellungen für einen Branch Bucket haben keinen Einfluss auf die Objektversionen im Basis Bucket.

Schritte

1. Wenn die globale S3 Object Lock-Einstellung aktiviert ist, kann S3 Object Lock optional auch für den Branch Bucket aktiviert werden. Um S3 Object Lock zu aktivieren, muss der Branch Bucket ein Lese-/Schreib-Bucket sein.

Die S3 Object Lock-Funktion sollte für einen Branch-Bucket nur aktiviert werden, wenn Objekte für einen festgelegten Zeitraum aufbewahrt werden müssen, beispielsweise um bestimmte regulatorische Anforderungen zu erfüllen. S3 Object Lock ist eine permanente Einstellung, die verhindert, dass Objekte für einen festgelegten Zeitraum oder unbegrenzt gelöscht oder überschrieben werden.



Nachdem die S3 Object Lock Einstellung für einen Bucket aktiviert wurde, kann sie nicht mehr deaktiviert werden. Jeder mit den entsprechenden Berechtigungen kann dem Branch Bucket Objekte hinzufügen, die nicht geändert werden können. Sie können diese Objekte oder den Branch Bucket selbst unter Umständen nicht löschen.

2. `#{post_edited_translations.segment}`



Ihr Grid-Administrator muss Ihnen die Berechtigung geben, "[spezifische Funktionen von S3 Object Lock](#)".

Wenn **Default retention** aktiviert ist, werden neue Objekte, die dem Branch-Bucket hinzugefügt werden, automatisch vor dem Löschen oder Überschreiben geschützt. Die Einstellung **Default retention** gilt nicht für Objekte, die über eigene Aufbewahrungsfristen verfügen.

- a. Wenn die **Standardaufbewahrung** aktiviert ist, ist ein **Standardaufbewahrungsmodus** für den Branch-Bucket anzugeben.

Standard-Aufbewahrungsmodus	Beschreibung
Governance	• Benutzer mit der <code>s3:BypassGovernanceRetention</code> Berechtigung können den <code>x-amz-bypass-governance-retention: true</code> Anfrageheader verwenden, um die Aufbewahrungseinstellungen zu umgehen. • Diese Benutzer können eine Objektversion löschen, bevor deren Aufbewahrungsdatum erreicht ist. • Diese Benutzer können das Aufbewahrungsdatum eines Objekts erhöhen, verringern oder entfernen.
Einhaltung	• Das Objekt kann erst gelöscht werden, wenn sein Aufbewahrungsdatum erreicht ist. • Das Aufbewahrungsdatum des Objekts kann erhöht, aber nicht verringert werden. • Das Aufbewahrungsdatum des Objekts kann erst nach Erreichen dieses Datums entfernt werden. Hinweis: Ihr Grid-Administrator muss Ihnen die Verwendung des Compliance-Modus erlauben.

b. `${post_edited_translations.segment}`

Der **Standard-Aufbewahrungszeitraum** gibt an, wie lange neue Objekte, die dem Branch-Bucket hinzugefügt werden, ab dem Zeitpunkt ihrer Erfassung aufbewahrt werden sollen. Es ist ein Wert anzugeben, der kleiner oder gleich dem vom Grid-Administrator festgelegten maximalen Aufbewahrungszeitraum für den Mandanten ist.

Beim Anlegen des Mandanten durch den Grid-Administrator wird eine *maximale* Aufbewahrungsdauer festgelegt, die zwischen 1 Tag und 100 Jahren liegen kann. Wenn eine *standardmäßige* Aufbewahrungsdauer festgelegt wird, darf sie den für die maximale Aufbewahrungsdauer festgelegten Wert nicht überschreiten. Falls erforderlich, kann der Grid-Administrator gebeten werden, die maximale Aufbewahrungsdauer zu erhöhen oder zu verringern.

3. `${post_edited_translations.segment}`

Die Kapazitätsgrenze ist die maximal verfügbare Kapazität für den Branch Bucket. Dieser Wert stellt eine logische Größe (Objektgröße) und keine physische Größe (Speicherplatz auf der Festplatte) dar.

Wenn kein Limit festgelegt ist, ist die Kapazität für den Branch Bucket unbegrenzt. Weitere Informationen finden Sie unter "[Kapazitätslimitnutzung](#)".



Diese Einstellung gilt nur für Objekte, die direkt in den Branch-Bucket aufgenommen werden, und nicht für Objekte, die vom Basis-Bucket über den Branch-Bucket sichtbar sind.

4. `${post_edited_translations.segment}`

Das Limit für die Objektanzahl ist die maximale Anzahl von Objekten, die der Branch Bucket enthalten kann. Dieser Wert stellt eine logische Menge dar (Objektanzahl). Wenn kein Limit festgelegt ist, ist die Objektanzahl unbegrenzt.



Diese Einstellung gilt nur für Objekte, die direkt in den Branch-Bucket aufgenommen werden, und nicht für Objekte, die vom Basis-Bucket über den Branch-Bucket sichtbar sind.

5. **Bucket erstellen** auswählen.

`${post_edited_translations.segment}`

6. Optional kann **Zur Bucket-Detailseite** ausgewählt werden, um "[Details zum Branch Bucket](#)" weitere Konfigurationen vorzunehmen.

Auf der Bucket-Detailseite sind einige Konfigurationsoptionen im Zusammenhang mit der Änderung von Objekten für schreibgeschützte Buckets deaktiviert.

Wenden Sie ein ILM-Policy-Tag auf einen StorageGRID Bucket an

Wählen Sie ein ILM-Richtlinien-Tag aus, das auf einen Bucket entsprechend Ihren Objektspeicheranforderungen angewendet wird.

Die ILM-Richtlinie steuert, wo Objektdaten gespeichert werden und ob sie nach einer bestimmten Zeitspanne gelöscht werden. Ihr Grid-Administrator erstellt ILM-Richtlinien und weist sie ILM-Policy-Tags zu, wenn mehrere aktive Richtlinien verwendet werden.



Vermeiden Sie es, das Policy-Tag eines Buckets häufig neu zuzuweisen. Andernfalls können Leistungsprobleme auftreten.

Bevor Sie beginnen

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

Schritte

1. **View buckets** im Dashboard auswählen oder **STORAGE (S3) > Buckets**.

Die Seite „Buckets“ wird angezeigt. Nach Bedarf kann die Information nach jeder Spalte sortiert werden oder es ist möglich, in der Liste vor- und zurückzublättern.

2. Wählen Sie den Namen des Buckets aus, dem Sie ein ILM-Policy-Tag zuweisen möchten.

Sie können auch die ILM-Policy-Tag-Zuweisung für einen Bucket ändern, dem bereits ein Tag zugewiesen ist.



Die angezeigten Werte für Objektanzahl und Speicherplatzbelegung sind Schätzwerte. Diese Schätzwerte werden durch den Zeitpunkt der Datenaufnahme, die Netzwerkverbindung und den Knotenstatus beeinflusst. Wenn für Buckets die Versionierung aktiviert ist, werden gelöschte Objektversionen in die Objektanzahl einbezogen.

3. Im Tab „Bucket-Optionen“ den Bereich „ILM-Richtlinien-Tag“ erweitern. Dieser Bereich erscheint nur, wenn der Grid-Administrator die Verwendung benutzerdefinierter Richtlinien-Tags aktiviert hat.

4. Anhand der Beschreibung jedes Policy-Tags lässt sich bestimmen, welches Tag auf den Bucket angewendet werden sollte.



Durch die Änderung des ILM-Richtlinientags für einen Bucket wird eine erneute ILM-Bewertung aller Objekte im Bucket ausgelöst. Wenn die neue Richtlinie Objekte für eine begrenzte Zeit beibehält, werden ältere Objekte gelöscht.

5. Wählen Sie das Optionsfeld für das Tag aus, das Sie dem Bucket zuweisen möchten.
6. **Änderungen speichern** auswählen. Ein neues S3-Bucket-Tag wird auf dem Bucket mit dem Schlüssel `NTAP-SG-ILM-BUCKET-TAG` und dem Wert des ILM-Policy-Tag-Namens gesetzt.



Stellen Sie sicher, dass Ihre S3-Anwendungen das neue Bucket-Tag nicht versehentlich überschreiben oder löschen. Wenn dieses Tag beim Anwenden eines neuen TagSet auf den Bucket weggelassen wird, werden die Objekte im Bucket wieder anhand der Standard-ILM-Richtlinie ausgewertet.



ILM-Richtlinientags können ausschließlich über den Tenant Manager oder die Tenant Manager API festgelegt und geändert werden, sofern der ILM-Richtlinientag dort validiert wird. Der `NTAP-SG-ILM-BUCKET-TAG` ILM-Richtlinientag sollte nicht mit der S3 PutBucketTagging API oder der S3 DeleteBucketTagging API geändert werden.



Das Ändern des einem Bucket zugewiesenen Policy-Tags hat vorübergehende Auswirkungen auf die Performance, während die Objekte anhand der neuen ILM-Policy neu ausgewertet werden.

StorageGRID Bucket-Richtlinie verwalten

Sie können den Benutzerzugriff auf einen S3-Bucket und die darin enthaltenen Objekte steuern.

Bevor Sie beginnen

- Sie sind beim Tenant Manager mit einem ["unterstützte Webbrowser"](#) angemeldet.
- Sie gehören einer Benutzergruppe an, die über die Berechtigung ["Root-Zugriffsberechtigung"](#) verfügt. Die Berechtigungen „Alle Buckets anzeigen“ und „Alle Buckets verwalten“ erlauben nur das Anzeigen.
- Sie haben überprüft, dass die erforderliche Anzahl von Storage Nodes und Standorten verfügbar ist. Wenn zwei oder mehr Storage Nodes an einem Standort nicht verfügbar sind oder ein Standort nicht verfügbar ist, sind Änderungen an diesen Einstellungen möglicherweise nicht möglich.

Schritte

1. `${post_edited_translations.segment}`
2. Auf der Bucket-Detailseite **Bucket access** > **Bucket policy** auswählen.
3. Führen Sie einen der folgenden Schritte aus:
 - Geben Sie eine Bucket-Richtlinie ein, indem Sie das Kontrollkästchen **Richtlinie aktivieren** auswählen. Anschließend eine gültige, im JSON-Format vorliegende Zeichenfolge eingeben.

Jede Bucket-Richtlinie hat eine Größenbeschränkung von 20.480 Bytes.

- Eine bestehende Richtlinie wird durch Bearbeiten der Zeichenfolge geändert.
- Deaktivieren Sie eine Richtlinie, indem Sie **Richtlinie aktivieren** abwählen.

Detaillierte Informationen zu Bucket-Richtlinien, einschließlich Sprachsyntax und Beispielen, sind unter ["Beispiel-Bucket-Richtlinien"](#) zu finden.

Konsistenz von StorageGRID-Buckets verwalten

Konsistenzwerte können verwendet werden, um die Verfügbarkeit von Bucket-Einstellungsänderungen festzulegen sowie ein Gleichgewicht zwischen der Verfügbarkeit der Objekte innerhalb eines Buckets und der Konsistenz dieser Objekte über verschiedene Storage Nodes und Standorte hinweg bereitzustellen. Die Konsistenzwerte können von den Standardwerten abweichen, sodass Clientanwendungen ihre betrieblichen Anforderungen erfüllen können.

Bevor Sie beginnen

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

`${post_edited_translations.segment}`

Die Bucket-Konsistenz wird verwendet, um die Konsistenz für Clientanwendungen zu bestimmen, die Objekte innerhalb dieses S3-Buckets beeinflussen. Im Allgemeinen empfiehlt sich für Ihre Buckets die Konsistenz **Read-after-new-write**.

Bucket-Konsistenz ändern

Wenn die **Read-after-new-write**-Konsistenz nicht den Anforderungen der Clientanwendung entspricht, kann die Konsistenz geändert werden, indem entweder die Bucket-Konsistenz festgelegt oder der `Consistency-Control` Header verwendet wird. Der `Consistency-Control` Header setzt die Bucket-Konsistenz außer Kraft.



Wenn die Konsistenz eines Buckets geändert wird, ist nur bei Objekten, die nach der Änderung importiert werden, gewährleistet, dass sie die geänderte Einstellung erfüllen.

Schritte

1. Im Dashboard steht **View buckets** zur Auswahl, alternativ **STORAGE (S3) > Buckets**.
2. Den Bucket-Namen aus der Tabelle auswählen.

Die Seite mit den Bucket-Details wird angezeigt.

3. Auf der Registerkarte **Bucket options** das ****** accordion auswählen.
4. Eine Konsistenz für Vorgänge auswählen, die an den Objekten in diesem Bucket ausgeführt werden.
 - **Alle:** Bietet das höchste Maß an Konsistenz. Alle Knoten empfangen die Daten sofort, oder die Anfrage schlägt fehl.
 - **Stark-global:** Gewährleistet Lese-nach-Schreib-Konsistenz für alle Client-Anfragen über alle Standorte

hinweg.

- **Strong-site:** Gewährleistet Lese-nach-Schreib-Konsistenz für alle Client-Anfragen innerhalb eines Standorts.
- **Read-after-new-write** (Standard): Bietet Read-after-Write-Konsistenz für neue Objekte und Eventual Consistency für Objektaktualisierungen. Bietet hohe Verfügbarkeit und Datenschutzgarantien. Wird für die meisten Fälle empfohlen.
- **Verfügbar:** Gewährleistet letztendliche Konsistenz sowohl für neue Objekte als auch für Objektaktualisierungen. Für S3-Buckets nur bei Bedarf verwenden (zum Beispiel für einen Bucket, der Log-Werte enthält, die selten gelesen werden, oder für HEAD- oder GET-Operationen auf Schlüsseln, die nicht existieren). Nicht unterstützt für S3 FabricPool Buckets.

5. Wählen Sie **Save changes**.

`${post_edited_translations.segment}`

`${post_edited_translations.segment}`

Die folgenden Bucket-Einstellungen verwenden standardmäßig **starke** Konsistenz. Wenn zwei oder mehr Storage Nodes innerhalb eines Standorts nicht verfügbar sind oder ein Standort nicht verfügbar ist, sind Änderungen an diesen Einstellungen möglicherweise nicht verfügbar.

- "Löschen leerer Buckets im Hintergrund"
- "Letzte Zugriffszeit"
- "Bucket-Lebenszyklus"
- "Bucket Richtlinie"
- `"${post_edited_translations.segment}"`
- "Bucket Versionierung"
- "S3 Object Lock"
- "Bucket Verschlüsselung"



Der Konsistenzwert für Bucket-Versionierung, S3 Object Lock und Bucket-Verschlüsselung darf nicht auf einen Wert gesetzt werden, der nicht stark konsistent ist.

Die folgenden Bucket-Einstellungen verwenden keine starke Konsistenz und weisen eine höhere Verfügbarkeit für Änderungen auf. Änderungen an diesen Einstellungen werden unter Umständen erst nach einiger Zeit wirksam.

- "Konfiguration der Plattformdienste: Benachrichtigung, Replikation oder Suchintegration"
- "StorageGRID CORS für Buckets und Objekte konfigurieren"
- Bucket-Konsistenz ändern



Wenn die standardmäßige Konsistenz, die beim Ändern der Bucket-Einstellungen verwendet wird, nicht den Anforderungen der Client-Anwendung entspricht, kann die Konsistenz durch Verwendung des Consistency-Control Headers für die "S3 REST API" oder durch die `reducedConsistency` oder `force` Optionen im "Mandantenverwaltungs-API" geändert werden.

Aktivieren oder deaktivieren Sie Aktualisierungen der letzten Zugriffszeit in StorageGRID

Wenn Grid-Administratoren die Information Lifecycle Management (ILM)-Regeln für ein StorageGRID System erstellen, kann optional festgelegt werden, dass die letzte Zugriffszeit eines Objekts zur Bestimmung, ob dieses Objekt an einen anderen Speicherort verschoben wird, verwendet wird. Bei Verwendung eines S3-Tenants besteht die Möglichkeit, solche Regeln zu nutzen, indem die Aktualisierung der letzten Zugriffszeit für die Objekte in einem S3-Bucket aktiviert wird.

Diese Anweisungen gelten nur für StorageGRID Systeme, die mindestens eine ILM-Regel enthalten, die die Option **Letzter Zugriffszeitpunkt** als erweiterten Filter oder als Referenzzeitpunkt verwendet. Diese Anweisungen sind nicht relevant, wenn Ihr StorageGRID System keine solche Regel enthält. Siehe "[Letzte Zugriffszeit in ILM-Regeln verwenden](#)" für Details.

Bevor Sie beginnen

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

Über diese Aufgabe

Letzter Zugriff ist eine der verfügbaren Optionen für die Platzierungsanweisung **Referenzzeit** einer ILM-Regel. Wenn die Referenzzeit für eine Regel auf **Letzter Zugriff** gesetzt wird, können Grid-Administratoren festlegen, dass Objekte an bestimmten Speicherorten abgelegt werden, basierend darauf, wann diese Objekte zuletzt abgerufen (gelesen oder angezeigt) wurden.

Um beispielsweise sicherzustellen, dass kürzlich angezeigte Objekte auf schnellerem Speicher verbleiben, kann ein Grid-Administrator eine ILM-Regel erstellen, die Folgendes festlegt:

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

Standardmäßig sind Aktualisierungen der letzten Zugriffszeit deaktiviert. Wenn Ihr StorageGRID System eine ILM-Regel enthält, die die Option **Letzte Zugriffszeit** verwendet und diese Option auf Objekte in diesem Bucket angewendet werden soll, müssen Aktualisierungen der letzten Zugriffszeit für die in dieser Regel angegebenen S3 Buckets aktiviert werden.



Das Aktualisieren der letzten Zugriffszeit beim Abruf eines Objekts kann die Leistung von StorageGRID beeinträchtigen, insbesondere bei kleinen Objekten.

Bei Aktualisierungen der letzten Zugriffszeit kommt es zu Leistungseinbußen, da StorageGRID diese zusätzlichen Schritte jedes Mal ausführen muss, wenn Objekte abgerufen werden:

- Aktualisieren Sie die Objekte mit neuen Zeitstempeln
- Die Objekte werden der ILM-Warteschlange hinzugefügt, sodass sie anhand der aktuellen ILM-Regeln und Richtlinien erneut geprüft 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 (Standardeinstellung)		Verhalten, wenn die letzte Zugriffszeit aktiviert ist	
	Letzte Zugriffszeit aktualisiert?	Objekt zur ILM-Auswertungswarteschlange hinzugefügt?	Letzte Zugriffszeit aktualisiert?	Objekt zur ILM-Auswertungswarteschlange hinzugefügt?
Anfrage zum Abrufen der Metadaten eines Objekts, wenn eine HEAD-Operation ausgeführt wird	Nein	Nein	Nein	Nein
Anfrage zum Abrufen eines Objekts, seiner Zugriffssteuerungsliste oder seiner Metadaten	Nein	Nein	Ja	Ja
Anfrage zur Aktualisierung der Metadaten eines Objekts	Ja	Ja	Ja	Ja
Anfrage zum Auflisten von Objekten oder Objektversionen	Nein	Nein	Nein	Nein
Anfrage zum Kopieren eines Objekts von einem Bucket in einen anderen	• Nein, für die Quellkopie • Ja, für die Zielkopie	• Nein, für die Quellkopie • Ja, für die Zielkopie	• Ja, für die Quellkopie • Ja, für die Zielkopie	• Ja, für die Quellkopie • Ja, für die Zielkopie
Anfrage zum Abschließen eines mehrteiligen Uploads	Ja, für das zusammengebaute Objekt	Ja, für das zusammengebaute Objekt	Ja, für das zusammengebaute Objekt	Ja, für das zusammengebaute Objekt

Schritte

1. **View buckets** im Dashboard auswählen oder **STORAGE (S3) > Buckets**.
2. Den Bucket-Namen aus der Tabelle auswählen.

Die Seite mit den Bucket-Details wird angezeigt.

3. Auf der Registerkarte **Bucket Optionen** das Akkordeon **Letzte Zugriffszeitaktualisierungen** auswählen.
4. Aktualisierungen der letzten Zugriffszeit aktivieren oder deaktivieren.
5. Wählen Sie **Save changes**.

Objektversionierung für einen S3-Bucket in StorageGRID ändern

Wenn Sie einen S3-Tenant verwenden, kann der Versionsstatus für S3 Buckets geändert werden.

Bevor Sie beginnen

- Sie sind beim Tenant Manager mit einem ["unterstützte Webbrowser"](#) angemeldet.
- Sie gehören einer Benutzergruppe an, die über die ["Alle Buckets oder Root-Zugriffsberechtigung verwalten"](#) verfügt. Diese Berechtigungen überschreiben die Berechtigungseinstellungen in Gruppen- oder Bucket-Richtlinien.
- Sie haben überprüft, dass die erforderliche Anzahl von Storage Nodes und Standorten verfügbar ist. Wenn zwei oder mehr Storage Nodes an einem Standort nicht verfügbar sind oder ein Standort nicht verfügbar ist, sind Änderungen an diesen Einstellungen möglicherweise nicht möglich.

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 mehr in einen nicht versionierten Zustand zurückversetzt werden. Die Versionierung für den Bucket kann jedoch ausgesetzt werden.

- Deaktiviert: Die Versionierung wurde nie aktiviert
- Aktiviert: Versionsverwaltung ist aktiviert
- Ausgesetzt: Die Versionierung war zuvor aktiviert und ist ausgesetzt

Weitere Informationen sind in Folgendem zu finden:

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

Schritte

1. **View buckets** im Dashboard auswählen oder **STORAGE (S3) > Buckets**.
2. Den Bucket-Namen aus der Tabelle auswählen.

Die Seite mit den Bucket-Details wird angezeigt.

3. Auf der Registerkarte **Bucket-Optionen** das Akkordeon **Objektversionierung** auswählen.
4. Wählen Sie einen Versionsstatus für die Objekte in diesem Bucket.

Die Objektversionierung muss für einen Bucket, der für die grid-übergreifende Replikation verwendet wird, aktiviert bleiben. Wenn S3 Object Lock oder Legacy Compliance aktiviert ist, sind die Optionen für die **Objektversionierung** deaktiviert.

Option	Beschreibung
Versionierung aktivieren	Die Objektversionierung kann aktiviert werden, wenn jede Version jedes Objekts in diesem Bucket gespeichert werden soll. Frühere Versionen eines Objekts können anschließend bei Bedarf abgerufen werden. Objekte, die sich bereits im Bucket befanden, werden versioniert, wenn sie von einem Benutzer geändert werden.
Versionierung aussetzen	Setzen Sie die Objektversionierung aus, wenn keine neuen Objektversionen mehr erstellt werden sollen. Vorhandene Objektversionen können weiterhin abgerufen werden.

5. Wählen Sie **Save changes**.

Verwenden Sie S3 Object Lock, um Objekte in StorageGRID aufzubewahren

Sie können S3 Object Lock verwenden, wenn Buckets und Objekte regulatorischen Aufbewahrungsvorschriften entsprechen müssen.



Ihr Grid-Administrator muss Ihnen die Berechtigung erteilen, bestimmte Funktionen von S3 Object Lock zu verwenden.

Was ist S3 Object Lock?

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

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

Ein Bucket ohne S3 Object Lock kann nur Objekte ohne festgelegte Aufbewahrungseinstellungen enthalten. Für importierte Objekte werden keine Aufbewahrungseinstellungen festgelegt.

Ein Bucket mit S3 Object Lock kann Objekte mit und ohne von S3-Clientanwendungen festgelegte Aufbewahrungseinstellungen enthalten. Einige der importierten Objekte weisen Aufbewahrungseinstellungen auf.

Ein Bucket mit S3 Object Lock und konfigurierter Standardaufbewahrung kann sowohl hochgeladene Objekte mit festgelegten Aufbewahrungseinstellungen als auch neue Objekte ohne Aufbewahrungseinstellungen enthalten. Die neuen Objekte verwenden die Standardeinstellung, da die Aufbewahrungseinstellung nicht auf Objektebene konfiguriert wurde.

Effektiv haben alle neu importierten Objekte Aufbewahrungseinstellungen, wenn die Standardaufbewahrung konfiguriert ist. Vorhandene Objekte ohne Objektspezifische Aufbewahrungseinstellungen bleiben unberührt.

Aufbewahrungsmodi

Die StorageGRID S3 Object Lock-Funktion unterstützt zwei Aufbewahrungsmodi, um unterschiedliche

Schutzstufen für Objekte anzuwenden. Diese Modi entsprechen den Amazon S3 Aufbewahrungsmodi.

- Im Konformitätsmodus:
 - Das Objekt kann erst gelöscht werden, wenn sein Aufbewahrungsdatum erreicht ist.
 - Das Aufbewahrungsdatum des Objekts kann erhöht, aber nicht verringert werden.
 - Das Aufbewahrungsdatum des Objekts kann erst nach Erreichen dieses Datums entfernt werden.
- Im Governance-Modus:
 - Benutzer mit speziellen Berechtigungen können einen Bypass-Header in Anfragen verwenden, um bestimmte Aufbewahrungseinstellungen zu ändern.
 - Diese Benutzer können eine Objektversion löschen, bevor deren Aufbewahrungsdatum erreicht ist.
 - Diese Benutzer können das Aufbewahrungsdatum eines Objekts erhöhen, verringern oder entfernen.

Aufbewahrungseinstellungen für Objektversionen

Wenn ein Bucket mit aktiviertem S3 Object Lock erstellt wird, können Benutzer die S3-Clientanwendung verwenden, um optional die folgenden Aufbewahrungseinstellungen für jedes Objekt festzulegen, das dem Bucket hinzugefügt wird:

- **Aufbewahrungsmodus:** Entweder Compliance oder Governance.
- **Retain-until-date:** Wenn das Retain-until-date einer Objektversion in der Zukunft liegt, kann das Objekt abgerufen, aber nicht gelöscht werden.
- **Rechtliche Sperre:** Durch das Anwenden einer rechtlichen Sperre auf eine Objektversion wird dieses Objekt sofort gesperrt. Beispielsweise kann es erforderlich sein, eine rechtliche Sperre auf ein Objekt anzuwenden, das mit einer Untersuchung oder einem Rechtsstreit in Zusammenhang steht. Eine rechtliche Sperre hat kein Ablaufdatum, sondern bleibt bestehen, bis sie explizit entfernt wird. Rechtliche Sperren sind unabhängig vom Aufbewahrungsdatum.



Wenn ein Objekt unter einer rechtlichen Aufbewahrungspflicht steht, kann niemand das Objekt löschen, unabhängig vom Aufbewahrungsmodus.

Weitere Informationen zu den Objekteinstellungen finden Sie unter ["S3 REST API zur Konfiguration von S3 Object Lock verwenden"](#).

Standardmäßige Aufbewahrungseinstellung für Buckets

Wenn ein Bucket mit aktiviertem S3 Object Lock erstellt wird, können Benutzer optional die folgenden Standardeinstellungen für den Bucket angeben:

- **Standardmäßiger Aufbewahrungsmodus:** Entweder Compliance oder Governance.
- **Standardmäßige Aufbewahrungsdauer:** Wie lange neue Objektversionen, die diesem Bucket hinzugefügt werden, ab dem Tag ihrer Hinzufügung aufbewahrt werden.

Die Standardeinstellungen für Buckets gelten nur für neue Objekte, die keine eigenen Aufbewahrungseinstellungen haben. Bestehende Bucket-Objekte sind nicht betroffen, wenn Sie diese Standardeinstellungen hinzufügen oder ändern.

Siehe ["Einen S3-Bucket erstellen"](#) und ["Standardaufbewahrungsdauer für S3 Object Lock aktualisieren"](#).

S3 Object Lock Aufgaben

Die folgenden Listen für Grid-Administratoren und Mandantenbenutzer enthalten die wichtigsten Aufgaben zur Verwendung der S3 Object Lock Funktion.

Grid Administrator

- Globale S3-Objektsperreinstellung für das gesamte StorageGRID System aktivieren.
- Stellen Sie sicher, dass die Richtlinien für das Informationslebenszyklusmanagement (ILM) *konform* sind; das heißt, dass sie die "[Anforderungen von Buckets mit aktiviertem S3 Object Lock](#)" erfüllen.
- Gegebenenfalls kann ein Mandant Compliance als Aufbewahrungsmodus verwenden. Andernfalls ist nur Governance als Modus zulässig.
- Bei Bedarf kann eine maximale Aufbewahrungsdauer für einen Mandanten festgelegt werden.

Mandantenbenutzer

- Hinweise zu Buckets und Objekten mit S3 Object Lock.
- Gegebenenfalls den Grid-Administrator kontaktieren, damit die globale S3 Object Lock-Einstellung aktiviert und die Berechtigungen festgelegt werden.
- Buckets mit aktivierter S3-Objektsperre erstellen.
- Optional lassen sich die Standard-Aufbewahrungseinstellungen für einen Bucket konfigurieren:
 - Standardmäßiger Aufbewahrungsmodus: Governance oder Compliance, sofern vom Grid-Administrator zugelassen.
 - Standardmäßige Aufbewahrungsfrist: Muss kleiner oder gleich der vom Grid-Administrator festgelegten maximalen Aufbewahrungsfrist sein.
- Verwenden Sie die S3-Clientanwendung, um Objekte hinzuzufügen und optional objektspezifische Aufbewahrungsfristen festzulegen:
 - Aufbewahrungsmodus. Governance oder Compliance, sofern vom Grid-Administrator zugelassen.
 - Aufbewahrungsdatum: Muss kürzer oder gleich der vom Grid-Administrator festgelegten maximalen Aufbewahrungsfrist sein.

Anforderungen für Buckets mit aktiviertem S3 Object Lock

- Wenn die globale S3 Object Lock-Einstellung für das StorageGRID System aktiviert ist, kann der Tenant Manager, die Tenant Management API oder die S3 REST API verwendet werden, um Buckets mit aktivierter S3 Object Lock-Funktion zu erstellen.
- Wenn Sie S3 Object Lock verwenden möchten, müssen Sie S3 Object Lock beim Erstellen des Buckets aktivieren. S3 Object Lock kann für einen bestehenden Bucket nicht aktiviert werden.
- Wenn S3 Object Lock für einen Bucket aktiviert ist, aktiviert StorageGRID automatisch die Versionierung für diesen Bucket. S3 Object Lock kann nicht deaktiviert oder die Versionierung für den Bucket ausgesetzt werden.
- Optional können Sie mithilfe des Tenant Managers, der Tenant Management API oder der S3 REST API einen Standard-Aufbewahrungsmodus und eine Standard-Aufbewahrungsdauer für jeden Bucket festlegen. Die Standardeinstellungen für die Aufbewahrung gelten nur für neue Objekte, die dem Bucket hinzugefügt werden und keine eigenen Aufbewahrungseinstellungen haben. Diese Standardeinstellungen lassen sich überschreiben, indem für jede Objektversion beim Hochladen ein Aufbewahrungsmodus und ein Aufbewahrungsdatum festgelegt werden.
- Die Bucket-Lebenszykluskonfiguration wird für Buckets mit aktiviertem S3 Object Lock unterstützt.

- CloudMirror Replikation wird für Buckets mit aktiviertem S3 Object Lock nicht unterstützt.

Anforderungen an Objekte in Buckets mit aktiviertem S3 Object Lock

- Um eine Objektversion zu schützen, können Sie Standardaufbewahrungseinstellungen für den Bucket festlegen oder Aufbewahrungseinstellungen für jede Objektversion angeben. Aufbewahrungseinstellungen auf Objektebene können mithilfe der S3-Clientanwendung oder der S3 REST API angegeben werden.
- Die Aufbewahrungseinstellungen gelten für einzelne Objektversionen. Eine Objektversion kann sowohl ein Aufbewahrungsdatum als auch eine rechtliche Aufbewahrungseinstellung haben, nur eine von beiden oder keine. Die Angabe eines Aufbewahrungsdatums oder einer rechtlichen Aufbewahrungseinstellung für ein Objekt schützt nur die in der Anfrage angegebene Version. Es können neue Versionen des Objekts erstellt werden, während die vorherige Version des Objekts gesperrt bleibt.

Lebenszyklus von Objekten in Buckets mit aktiviertem S3 Object Lock

Jedes Objekt, das in einem Bucket mit aktiviertem S3 Object Lock gespeichert wird, durchläuft folgende Phasen:

1. Objektaufnahme

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

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

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

2. Objektaufbewahrung und -Löschung

Mehrere Kopien jedes geschützten Objekts werden von StorageGRID für die festgelegte Aufbewahrungsfrist gespeichert. Die genaue Anzahl und Art der Objektkopien sowie die Speicherorte werden durch die konformen Regeln in den aktiven ILM-Richtlinien bestimmt. Ob ein geschütztes Objekt vor Erreichen seines Aufbewahrungsdatums gelöscht werden kann, hängt von seinem Aufbewahrungsmodus ab.

- Wenn ein Objekt unter einer rechtlichen Aufbewahrungspflicht steht, kann niemand das Objekt löschen, unabhängig vom Aufbewahrungsmodus.

Kann ich weiterhin ältere Compliant Buckets verwalten?

Die Funktion S3 Object Lock ersetzt die Compliance-Funktion, die in früheren StorageGRID Versionen verfügbar war. Wenn mit einer früheren Version von StorageGRID konforme Buckets erstellt wurden, lassen sich die Einstellungen dieser Buckets weiterhin verwalten; es können jedoch keine neuen konformen Buckets mehr erstellt werden. Anleitungen finden sich unter "[NetApp Knowledge Base: Verwaltung älterer konformer Buckets in StorageGRID 11.5](#)".

Aktualisieren Sie die Standardaufbewahrung für S3 Object Lock in StorageGRID

Wenn Sie beim Erstellen des Buckets die S3 Object Lock aktiviert haben, können Sie den Bucket bearbeiten, um die Standardaufbewahrungseinstellungen zu ändern. Sie können die Standardaufbewahrung aktivieren (oder deaktivieren) und einen Standardaufbewahrungsmodus sowie eine Standardaufbewahrungsdauer festlegen.

Bevor Sie beginnen

- Sie sind beim Tenant Manager mit einem ["unterstützte Webbrowser"](#) angemeldet.
- Sie gehören einer Benutzergruppe an, die über die ["Alle Buckets oder Root-Zugriffsberechtigung verwalten"](#) verfügt. Diese Berechtigungen überschreiben die Berechtigungseinstellungen in Gruppen- oder Bucket-Richtlinien.
- S3 Object Lock ist global für Ihr StorageGRID System aktiviert, und S3 Object Lock wurde beim Erstellen des Buckets aktiviert. Siehe ["S3 Object Lock zur Aufbewahrung von Objekten verwenden"](#).

Schritte

1. **View buckets** im Dashboard auswählen oder **STORAGE (S3) > Buckets**.
2. Den Bucket-Namen aus der Tabelle auswählen.

Die Seite mit den Bucket-Details wird angezeigt.

3. `#{post_edited_translations.segment}`
4. Optional kann die **Standardaufbewahrung** für diesen Bucket aktiviert oder deaktiviert werden.

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

5. Wenn die **Standardaufbewahrung** aktiviert ist, ist ein **Standardaufbewahrungsmodus** für den Bucket anzugeben.

Standard-Aufbewahrungsmodus	Beschreibung
Governance	• Benutzer mit der <code>s3:BypassGovernanceRetention</code> Berechtigung können den <code>x-amz-bypass-governance-retention: true</code> Anfrageheader verwenden, um die Aufbewahrungseinstellungen zu umgehen. • Diese Benutzer können eine Objektversion löschen, bevor deren Aufbewahrungsdatum erreicht ist. • Diese Benutzer können das Aufbewahrungsdatum eines Objekts erhöhen, verringern oder entfernen.

Standard-Aufbewahrungsmodus	Beschreibung
Einhaltung	• Das Objekt kann erst gelöscht werden, wenn sein Aufbewahrungsdatum erreicht ist. • Das Aufbewahrungsdatum des Objekts kann erhöht, aber nicht verringert werden. • Das Aufbewahrungsdatum des Objekts kann erst nach Erreichen dieses Datums entfernt werden. Hinweis: Ihr Grid-Administrator muss Ihnen die Verwendung des Compliance-Modus erlauben.

6. Wenn die **Standardaufbewahrung** aktiviert ist, ist die **Standardaufbewahrungsdauer** für den Bucket anzugeben.

Die **Standardaufbewahrungsdauer** gibt an, wie lange neue Objekte, die diesem Bucket hinzugefügt werden, ab dem Zeitpunkt ihrer Aufnahme aufbewahrt werden sollen. Es ist ein Wert anzugeben, der kleiner oder gleich der maximalen Aufbewahrungsdauer für den Mandanten ist, wie sie vom Grid-Administrator festgelegt wurde.

Beim Anlegen des Mandanten durch den Grid-Administrator wird eine *maximale* Aufbewahrungsdauer festgelegt, die zwischen 1 Tag und 100 Jahren liegen kann. Wenn eine *standardmäßige* Aufbewahrungsdauer festgelegt wird, darf sie den für die maximale Aufbewahrungsdauer festgelegten Wert nicht überschreiten. Falls erforderlich, kann der Grid-Administrator gebeten werden, die maximale Aufbewahrungsdauer zu erhöhen oder zu verringern.

7. Wählen Sie **Save changes**.

Konfigurieren Sie CORS für S3-Buckets in StorageGRID

Sie können Cross-Origin Resource Sharing (CORS) für einen S3-Bucket konfigurieren, wenn dieser Bucket und die darin enthaltenen Objekte für Webanwendungen in anderen Domänen zugänglich sein sollen.

Bevor Sie beginnen

- Sie sind beim Tenant Manager mit einem ["unterstützte Webbrowser"](#) angemeldet.
- Für GET CORS-Konfigurationsanfragen gehören Sie einer Benutzergruppe an, die über die ["Berechtigung „Alle Buckets verwalten“](#) oder ["Alle Buckets anzeigen"](#) verfügt. Diese Berechtigungen überschreiben die Berechtigungseinstellungen in Gruppen- oder Bucket-Richtlinien.
- Für PUT-CORS-Konfigurationsanfragen gehören Sie einer Benutzergruppe an, die über die ["Alle Buckets-Berechtigungen verwalten"](#) verfügt. Diese Berechtigung überschreibt die Berechtigungseinstellungen in Gruppen- oder Bucket-Richtlinien.
- Das ["Root-Zugriffsberechtigung"](#) bietet Zugriff auf alle CORS-Konfigurationsanfragen.

Über diese Aufgabe

Cross-Origin Resource Sharing (CORS) ist ein Sicherheitsmechanismus, der es Client-Webanwendungen in einer Domäne ermöglicht, auf Ressourcen in einer anderen Domäne zuzugreifen. Angenommen, es wird ein S3-Bucket namens `Images` verwendet, um Grafiken zu speichern. Durch die Konfiguration von CORS für das `Images` Bucket kann die Anzeige der Bilder aus diesem Bucket auf der Website `http://www.example.com`

ermöglicht werden.

CORS für einen Bucket aktivieren

Schritte

1. Verwenden Sie einen Texteditor, um das erforderliche XML zu erstellen. Dieses Beispiel zeigt das XML, das verwendet wird, um CORS für einen S3 Bucket zu aktivieren. Im Einzelnen:
 - Ermöglicht jeder Domain, GET-Anfragen an den Bucket zu senden
 - Erlaubt nur der `http://www.example.com` Domain, GET-, POST- und DELETE-Anfragen zu senden
 - Alle Anfrage-Header 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 sind unter ["Amazon Web Services \(AWS\) Dokumentation: Amazon Simple Storage Service Benutzerhandbuch"](#) zu finden.

2. Im Dashboard steht **View buckets** zur Auswahl, alternativ **STORAGE (S3) > Buckets**.
3. Den Bucket-Namen aus der Tabelle auswählen.

Die Seite mit den Bucket-Details wird angezeigt.

4. Auf der Registerkarte **Bucket access** die Akkordeon-Option **Cross-Origin Resource Sharing (CORS)** auswählen.
5. Das Kontrollkästchen **Enable CORS** auswählen.
6. Fügen Sie die CORS Konfigurations-XML in das Textfeld ein.
7. Wählen Sie **Save changes**.

CORS-Einstellung ändern

Schritte

1. Die CORS-Konfigurations-XML im Textfeld kann aktualisiert werden, oder mit **Löschen** wird neu begonnen.

2. Wählen Sie **Save changes**.

CORS-Einstellung deaktivieren

Schritte

1. Das Kontrollkästchen **CORS aktivieren** wird deaktiviert.
2. Wählen Sie **Save changes**.

Verwandte Informationen

["StorageGRID CORS für eine Managementoberfläche konfigurieren"](#)

Objekte aus einem StorageGRID S3-Bucket löschen

Mit dem Tenant Manager ist das Löschen der Objekte in einem oder mehreren Buckets möglich.

Überlegungen und Anforderungen

Vor der Durchführung dieser Schritte ist Folgendes zu beachten:

- Wenn Sie Objekte in einem Bucket löschen, entfernt StorageGRID dauerhaft alle Objekte und alle Objektversionen in jedem ausgewählten Bucket von allen Knoten und Standorten in Ihrem StorageGRID System. StorageGRID entfernt außerdem alle zugehörigen Objektmetadaten. Diese Informationen können nicht wiederhergestellt werden.
- Das Löschen aller Objekte in einem Bucket kann je nach Anzahl der Objekte, Objektkopien und gleichzeitigen Operationen Minuten, Tage oder sogar Wochen dauern.
- Wenn ein Bucket ["S3 Object Lock aktiviert"](#) hat, kann er sich *Jahre* lang im Zustand **Objekte werden gelöscht: Nur lesend** befinden.



Ein Bucket, der S3 Object Lock verwendet, bleibt im Status **Objekte werden gelöscht: Nur lesend**, bis das Aufbewahrungsdatum für alle Objekte erreicht ist und alle rechtlichen Sperren entfernt wurden.

- Während Objekte gelöscht werden, hat der Bucket den Status **Objekte werden gelöscht: read-only**. In diesem Zustand können Sie dem Bucket keine neuen Objekte hinzufügen.
- Nachdem alle Objekte gelöscht wurden, bleibt der Bucket im schreibgeschützten Zustand. Es besteht eine der folgenden Möglichkeiten:
 - Den Bucket wieder in den Schreibmodus versetzen und für neue Objekte wiederverwenden
 - Den Bucket löschen
 - Den Bucket im schreibgeschützten Modus belassen, um seinen Namen für die zukünftige Verwendung zu reservieren
- Wenn für einen Bucket die Objektversionierung aktiviert ist, können Löschmarkierungen, die in StorageGRID 11.8 oder höher erstellt wurden, mithilfe der Operationen „Objekte im Bucket löschen“ entfernt werden.
- Wenn für einen Bucket die Objektversionierung aktiviert ist, werden beim Löschen von Objekten keine Löschmarkierungen entfernt, die in StorageGRID 11.7 oder früher erstellt wurden. Informationen zum Löschen von Objekten in einem Bucket befinden sich in ["Wie versionierte S3-Objekte gelöscht werden"](#).
- Wenn Sie ["gridübergreifende Replikation"](#) verwenden, ist Folgendes zu beachten:

- Durch die Verwendung dieser Option werden keine Objekte aus dem Bucket im anderen Grid gelöscht.
- Wenn Sie diese Option für den Quell-Bucket auswählen, wird die Warnung **Cross-grid replication failure** ausgelöst, wenn Sie Objekte zum Ziel-Bucket auf dem anderen Grid hinzufügen. Falls Sie nicht garantieren können, dass niemand Objekte zum Bucket auf dem anderen Grid hinzufügt, "[Grid-übergreifende Replikation deaktivieren](#)" für diesen Bucket, bevor alle Bucket-Objekte gelöscht werden.

Bevor Sie beginnen

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

Schritte

1. **View buckets** im Dashboard auswählen oder **STORAGE (S3) > Buckets**.

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

2. Das Menü **Aktionen** oder die Detailseite für einen bestimmten Bucket kann verwendet werden.

Aktionsmenü

- a. Aktivieren Sie das Kontrollkästchen für jeden Bucket, aus dem Objekte gelöscht werden sollen.
- b. Wählen Sie **Aktionen > Objekte im Bucket löschen**.

Detailseite

- a. Wählen Sie einen Bucket-Namen aus, um dessen Details anzuzeigen.
- b. **Objekte im Bucket löschen** auswählen.

3. Wenn das Bestätigungsdiaologfeld erscheint, die Angaben prüfen, **Ja** eingeben und **OK** auswählen.
4. Warten Sie, bis der Löschvorgang beginnt.

Nach einigen Minuten:

- Auf der Seite mit den Bucket-Details wird ein gelbes Statusbanner angezeigt. Der Fortschrittsbalken zeigt an, welcher Prozentsatz der Objekte gelöscht wurde.
- **(schreibgeschützt)** erscheint nach dem Namen des Buckets auf der Bucket-Detailseite.
- **(Objekte löschen: Nur lesen)** erscheint neben dem Namen des Buckets auf der Seite „Buckets“.

Buckets > my-bucket

my-bucket (read-only)

Region: us-east-1

Date created: 2022-12-14 10:09:50 MST

Object count: 3

View bucket contents in Experimental S3 Console

Delete bucket

Success

Starting to delete objects from one bucket.

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.

0% (0 of 3 objects deleted)

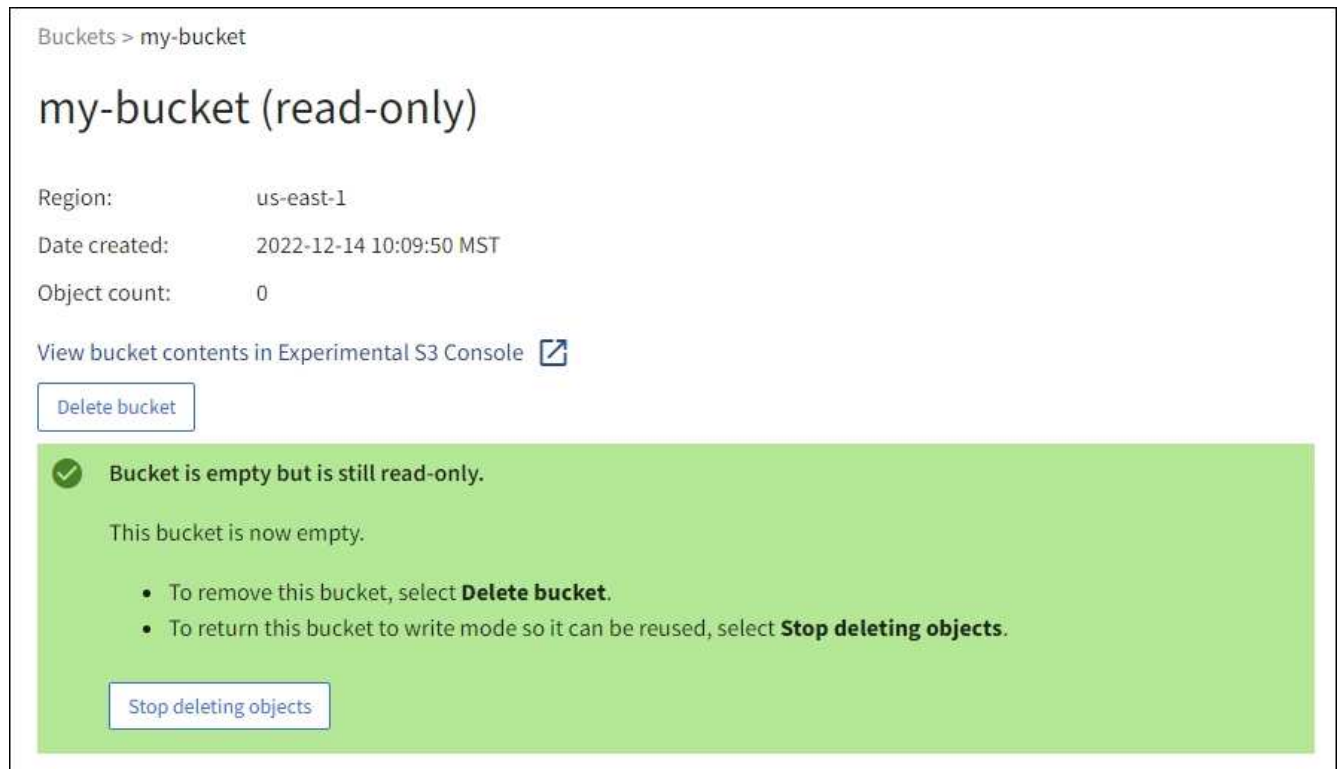
Stop deleting objects

5. Falls erforderlich, während der Vorgang läuft, **Objekte löschen stoppen** auswählen, um den Prozess anzuhalten. Anschließend optional **Objekte im Bucket löschen** auswählen, um den Prozess fortzusetzen.

Wenn Sie **Objekte nicht mehr löschen** auswählen, wird der Bucket wieder in den Schreibmodus versetzt; jedoch können Sie nicht auf gelöschte Objekte zugreifen oder diese wiederherstellen.

6. Warten Sie, bis der Vorgang abgeschlossen ist.

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



7. Führen Sie einen der folgenden Schritte aus:

- Verlassen Sie die Seite, um den Bucket im schreibgeschützten Modus zu belassen. Beispielsweise kann ein leerer Bucket im schreibgeschützten Modus belassen werden, um den Bucket-Namen für die zukünftige Verwendung zu reservieren.
- Den Bucket löschen. Es besteht die Möglichkeit, **Bucket löschen** auszuwählen, um einen einzelnen Bucket zu löschen, oder zur Seite „Buckets“ zurückzukehren und **Aktionen > Buckets löschen** auszuwählen, um mehrere Buckets zu entfernen.



Wenn Sie einen versionierten Bucket nach dem Löschen aller Objekte nicht löschen können, könnten Löschmarkierungen verbleiben. Zum Löschen des Buckets müssen alle verbleibenden Löschmarkierungen entfernt werden.

- Den Bucket wieder in den Schreibmodus versetzen und optional für neue Objekte wiederverwenden. Es besteht die Möglichkeit, **Löschen von Objekten stoppen** für einen einzelnen Bucket auszuwählen oder zur Seite „Buckets“ zurückzukehren und **Aktion > Löschen von Objekten stoppen** für mehrere Buckets auszuwählen.

Löschen eines StorageGRID S3 bucket

Mit dem Tenant Manager ist das Löschen eines oder mehrerer leerer S3-Buckets möglich.

Bevor Sie beginnen

- Sie sind beim Tenant Manager mit einem "unterstützte Webbrowser" angemeldet.
- Sie gehören einer Benutzergruppe an, die über die "Alle Buckets oder Root-Zugriffsberechtigung verwalten" verfügt. Diese Berechtigungen überschreiben die Berechtigungseinstellungen in Gruppen- oder Bucket-Richtlinien.

- Die zu löschenden Buckets sind leer. Wenn die zu löschenden Buckets *nicht* leer sind, "[Objekte aus dem Bucket löschen](#)".

Über diese Aufgabe

Diese Anleitung beschreibt, wie ein S3-Bucket mithilfe des Tenant Managers gelöscht wird. S3-Buckets können auch mithilfe der "[Mandantenverwaltungs-API](#)" oder der "[S3 REST API](#)" gelöscht werden.

Ein S3-Bucket kann nicht gelöscht werden, wenn er Objekte, nicht aktuelle Objektversionen oder Löschmarkierungen enthält. Informationen darüber, wie S3-versionierte Objekte gelöscht werden, finden sich unter "[Wie Objekte gelöscht werden](#)".

Schritte

1. **View buckets** im Dashboard auswählen oder **STORAGE (S3) > Buckets**.

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

2. Das Menü **Aktionen** oder die Detailseite für einen bestimmten Bucket kann verwendet werden.

Aktionsmenü

- a. Wählen Sie das Kontrollkästchen für jeden Bucket, den Sie löschen möchten.
- b. **Aktionen > Buckets löschen** auswählen.

Detailseite

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

3. Wenn das Bestätigungsdiaologfeld erscheint, **Ja** auswählen.

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

Wenn ein Bucket nicht leer ist, wird eine Fehlermeldung angezeigt. Sie müssen "[Alle Objekte und alle Löschmarkierungen im Bucket löschen](#)" ihn leeren, bevor Sie den Bucket löschen können.

Verwenden Sie die S3-Konsole in StorageGRID

`{post_edited_translations.segment}`

Die S3-Konsole ermöglicht Folgendes:

- Objekte hochladen, herunterladen, umbenennen, kopieren, verschieben und löschen
- `{post_edited_translations.segment}`
- Suche nach Objekten anhand des Präfixes
- Objekttags verwalten
- Objektmetadaten anzeigen
- Ordner anzeigen, erstellen, umbenennen, kopieren, verschieben und löschen

S3 Console bietet eine verbesserte Benutzererfahrung für die häufigsten Anwendungsfälle. Sie ist nicht dafür ausgelegt, CLI- oder API-Operationen in allen Situationen zu ersetzen.



Falls die Verwendung der S3-Konsole dazu führt, dass Vorgänge zu lange dauern (zum Beispiel Minuten oder Stunden), kann Folgendes in Betracht gezogen werden:

- Reduzierung der Anzahl ausgewählter Objekte
- Verwendung nicht-grafischer Methoden (API oder CLI) für den Zugriff auf Ihre Daten

Bevor Sie beginnen

- Sie sind beim Tenant Manager mit einem ["unterstützte Webbrowser"](#) angemeldet.
- Wenn Sie Objekte verwalten möchten, gehören Sie einer Benutzergruppe an, die über die Root-Zugriffsberechtigung verfügt. Alternativ gehören Sie einer Benutzergruppe an, die über die Berechtigung „S3-Konsole verwenden“ sowie entweder die Berechtigung „Alle Buckets anzeigen“ oder „Alle Buckets verwalten“ verfügt. Siehe ["Berechtigungen zur Mieterverwaltung"](#).
- Für den Benutzer wurde eine S3 Group- oder Bucket-Richtlinie konfiguriert. Siehe ["Bucket- und Gruppenzugriffsrichtlinien"](#).
- Sie kennen die Zugriffsschlüssel-ID und den geheimen Zugriffsschlüssel des Benutzers. Optional steht eine `.csv` Datei mit diesen Informationen zur Verfügung. Siehe ["Anleitung zum Erstellen von Zugriffsschlüsseln"](#).

Schritte

1. Wählen Sie **Storage > Buckets > *bucket name***.
2. Die Registerkarte S3 Console auswählen.
3. Fügen Sie die Zugriffsschlüssel-ID und den geheimen Zugriffsschlüssel in die Felder ein. Andernfalls **Zugriffsschlüssel hochladen** auswählen und die `.csv` Datei auswählen.
4. **Anmelden** auswählen.
5. Die Tabelle mit den Bucket-Objekten wird angezeigt. Objekte können nach Bedarf verwaltet werden.

Weitere Informationen

- **Suche nach Präfix:** Die Präfixsuche findet nur Objekte, die mit einem bestimmten Wort relativ zum aktuellen Ordner beginnen. Die Suche schließt Objekte aus, die das Wort an anderer Stelle enthalten. Diese Regel gilt auch für Objekte innerhalb von Ordnern. Beispielsweise würde eine Suche nach `folder1/folder2/somefile-` Objekte zurückgeben, die sich im `folder1/folder2/` Ordner befinden und mit dem Wort `somefile-` beginnen.
- **Drag and drop:** Sie können Dateien per Drag and drop aus dem Dateimanager Ihres Computers in die S3 Console ziehen. Das Hochladen von Ordnern ist jedoch nicht möglich.
- `${post_edited_translations.segment}`
- **Endgültiges Löschen bei deaktivierter Bucket-Versionierung:** Wenn ein Objekt in einem Bucket mit deaktivierter Versionierung überschrieben oder gelöscht wird, ist der Vorgang endgültig. Siehe ["`\${post\_edited\_translations.segment}`"](#).

Copyright-Informationen

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

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

DIE VORLIEGENDE SOFTWARE WIRD IN DER VORLIEGENDEN FORM VON NETAPP ZUR VERFÜGUNG GESTELLT, D. H. OHNE JEGliche EXPLIZITE ODER IMPLIZITE GEWÄHRLEISTUNG, EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE STILLSCHWEIGENDE GEWÄHRLEISTUNG DER MARKTGÄNGIGKEIT UND EIGNUNG FÜR EINEN BESTIMMTEN ZWECK, DIE HIERMIT AUSGESCHLOSSEN WERDEN. NETAPP ÜBERNIMMT KEINERLEI HAFTUNG FÜR DIREKTE, INDIREKTE, ZUFÄLLIGE, BESONDERE, 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 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.