Management von S3-Buckets

StorageGRID software

NetApp
January 15, 2026

Inhalt

Management von S3-Buckets

Erstellen eines S3-Buckets

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

Bevor Sie beginnen

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

> Berechtigungen zum Festlegen oder Ändern der S3 Object Lock-Eigenschaften von Buckets oder Objekten können erteilt werden durch"Bucket-Richtlinie oder Gruppenrichtlinie" .

- Wenn Sie die S3-Objektsperrung für einen Bucket aktivieren möchten, hat ein Grid-Administrator die globale S3-Objektsperrung für das StorageGRID-System aktiviert, und Sie haben die Anforderungen für S3-Objektsperrbuckets und -Objekte geprüft.
- Wenn jeder Mandant 5,000 Buckets hat, verfügt jeder Storage-Node im Grid über mindestens 64 GB RAM.

> Jedes Raster kann maximal 100.000 Buckets enthalten, darunter"Zweigeimer" .

Greifen Sie auf den Assistenten zu

Schritte

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

Geben Sie Details ein

Schritte

1. Geben Sie Details für den Bucket ein.

Feld	Beschreibung
Bucket-Name	Ein Name für den Bucket, der die folgenden Regeln erfüllt: • Jedes StorageGRID System muss eindeutig sein (nicht nur innerhalb des Mandantenkontos). • Muss DNS-konform sein. • Muss mindestens 3 und nicht mehr als 63 Zeichen enthalten. • Jedes Etikett muss mit einem Kleinbuchstaben oder einer Zahl beginnen und enden. Es können nur Kleinbuchstaben, Ziffern und Bindestriche verwendet werden. • Darf keine Punkte in Virtual-Hosted-Style-Anforderungen enthalten. Perioden verursachen Probleme bei der Überprüfung des Server-Platzhalterzertifikats. Weitere Informationen finden Sie im "Dokumentation der Amazon Web Services (AWS) zu den Bucket-Benennungsregeln". **Hinweis**: Sie können den Bucket-Namen nicht ändern, nachdem Sie den Bucket erstellt haben.
Region	Der Bereich des Eimers. Ihr StorageGRID Administrator verwaltet die verfügbaren Regionen. Die Region eines Buckets kann sich auf die auf Objekte angewendete Datenschutzrichtlinie auswirken. Standardmäßig werden alle Buckets im `us-east-1` Region. Wenn die Standardregion auf eine andere Region als `us-east-1` , diese andere Region ist zunächst im Dropdown-Menü ausgewählt. **Hinweis**: Sie können die Region nicht ändern, nachdem Sie den Bucket erstellt haben.

2. Wählen Sie **Weiter**.

Einstellungen verwalten

Schritte

1. Aktivieren Sie optional die Objektversionierung für den Bucket.

   Aktivieren Sie die Objektversionierung, wenn Sie jede Version jedes Objekts in diesem Bucket speichern möchten. Sie können dann nach Bedarf frühere Versionen eines Objekts abrufen.

   Sie müssen die Objektversionierung aktivieren, wenn:

   ◦ Der Bucket wird für die Cross-Grid-Replikation verwendet.
   ◦ Sie möchten eine"Asteimer" aus diesem Eimer.

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

   Aktivieren Sie die S3-Objektsperre für einen Bucket nur, wenn Objekte z. B. für eine bestimmte Zeit

aufbewahrt werden müssen, um bestimmte gesetzliche Vorgaben zu erfüllen. S3 Object Lock ist eine permanente Einstellung, mit der Sie verhindern können, dass Objekte für einen festgelegten Zeitraum oder für einen unbegrenzten Zeitraum gelöscht oder überschrieben werden.

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

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

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

> Ihr Grid-Administrator muss Ihnen die Berechtigung erteilen"Verwenden Sie bestimmte Funktionen von S3 Object Lock".

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

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

Standardaufbewahrungsmodus	Beschreibung
Governance	• Benutzer mit der `s3:BypassGovernanceRetention` Berechtigung können den Anforderungskopf verwenden `x-amz-bypass-governance-retention: true`, um die Aufbewahrungseinstellungen zu umgehen. • Diese Benutzer können eine Objektversion löschen, bevor das Aufbewahrungsdatum erreicht ist. • Diese Benutzer können das Aufbewahrungsdatum eines Objekts erhöhen, verringern oder entfernen.
Compliance	• Das Objekt kann erst gelöscht werden, wenn das Aufbewahrungsdatum erreicht ist. • Das Aufbewahrungsdatum des Objekts kann erhöht, aber nicht verringert werden. • Das Aufbewahrungsdatum des Objekts kann erst entfernt werden, wenn dieses Datum erreicht ist. **Hinweis**: Ihr Grid-Administrator muss Ihnen erlauben, den Compliance-Modus zu verwenden.

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

Die **Default Retention Period** gibt an, wie lange neue Objekte zu diesem Bucket hinzugefügt werden sollen, beginnend mit dem Zeitpunkt, zu dem sie aufgenommen werden. Geben Sie einen Wert an, der kleiner oder gleich der maximalen Aufbewahrungsfrist für den Mandanten ist, wie vom Grid-Administrator festgelegt.

Eine *maximale* Aufbewahrungsfrist, die ein Wert von 1 Tag bis 100 Jahre sein kann, wird festgelegt, wenn der Grid-Administrator den Mandanten erstellt. Wenn Sie eine *default* Aufbewahrungsfrist festlegen, darf sie den für die maximale Aufbewahrungsfrist festgelegten Wert nicht überschreiten. Bitten Sie bei Bedarf Ihren Grid-Administrator, die maximale Aufbewahrungsfrist zu verlängern oder zu verkürzen.

4. Wählen Sie optional **Kapazitätslimit aktivieren** aus, geben Sie einen Wert ein und wählen Sie die Kapazitätseinheit aus.

   Das Kapazitätslimit ist die maximale Kapazität, die für die Objekte dieses Buckets verfügbar ist. Dieser Wert stellt eine logische Menge (Objektgröße) und keine physische Menge (Größe auf Festplatte) dar.

   Wenn kein Limit festgelegt ist, ist die Kapazität für diesen Bucket unbegrenzt. Weitere Informationen finden Sie unter "Kapazitätsgrenze" .

5. Wählen Sie optional **Objektanzahllimit aktivieren**.

   Die Objektanzahlgrenze ist die maximale Anzahl von Objekten, die dieser Bucket enthalten kann. Dieser Wert stellt eine logische Menge (Objektanzahl) dar. Wenn kein Limit festgelegt ist, ist die Objektanzahl unbegrenzt.

6. Wählen Sie **Eimer erstellen**.

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

7. Wählen Sie optional **Gehe zu Bucket-Detailseite** zu "Bucket-Details anzeigen" und führen Sie zusätzliche Konfiguration durch.

Sie können auch"Erstellen Sie Zweig-Buckets" nach Bedarf.

Bucket-Details anzeigen

Sie können die Buckets in Ihrem Mandantenkonto anzeigen.

Bevor Sie beginnen

- Sie sind beim Tenant Manager mit einem angemeldet"Unterstützter Webbrowser".
- Sie gehören zu einer Benutzergruppe mit dem "Root-Zugriff, Alle Buckets verwalten oder Alle Buckets anzeigen". Diese Berechtigungen überschreiben die Berechtigungseinstellungen in Gruppen- oder Bucket-Richtlinien.

Schritte

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

   Die Seite „Buckets“ wird angezeigt.

2. Überprüfen Sie die Übersichtstabelle 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.

   Bei den angezeigten Werten für Objektanzahl, belegter Speicherplatz und Nutzung handelt es sich um Schätzwerte. Diese Schätzungen sind vom Zeitpunkt der Aufnahme, der Netzwerkverbindung und des Node-Status betroffen. Wenn Buckets die Versionierung aktiviert ist, sind gelöschte Objektversionen in der Objektanzahl enthalten.

Name

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

Aktivierte Funktionen

Die Liste der Funktionen, die für den Bucket aktiviert sind.

S3-Objektsperre

Gibt an, ob S3 Object Lock für den Bucket aktiviert ist.

Diese Spalte wird nur angezeigt, wenn die S3-Objektsperre für das Raster aktiviert ist. In dieser Spalte werden außerdem Informationen für alle Buckets angezeigt, die für die Konformität mit älteren Daten verwendet wurden.

Region

Der Bereich des Eimers, der nicht geändert werden kann. 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.

Belegten Speicherplatz

Die logische Größe aller Objekte im Bucket Die logische Größe umfasst nicht den tatsächlich benötigten Speicherplatz für replizierte oder Erasure Coding-Kopien oder für Objekt-Metadaten.

Die Aktualisierung dieses Werts kann bis zu 10 Minuten dauern.

Zu Verwenden

Der Prozentsatz, der vom Kapazitätslimit des Buckets verwendet wird, sofern ein Wert festgelegt wurde.

Der Nutzungswert basiert auf internen Schätzungen und kann in einigen Fällen überschritten werden. StorageGRID überprüft beispielsweise das Kapazitätslimit (sofern festgelegt), wenn ein Mandant beginnt, Objekte hochzuladen, und lehnt neue Ingest für diesen Bucket ab, wenn der Mandant das Kapazitätslimit überschritten hat. StorageGRID berücksichtigt jedoch nicht die Größe des aktuellen Uploads, wenn festgestellt wird, ob das Kapazitätslimit überschritten wurde. Wenn Objekte gelöscht werden, kann es vorkommen, dass ein Mandant vorübergehend verhindert wird, neue Objekte in diesen Bucket hochzuladen, bis die Auslastung der Kapazitätsgrenze neu berechnet wird. Die Berechnungen können 10 Minuten oder länger dauern.

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

Kapazität

Wenn festgelegt, wird das Kapazitätslimit des Buckets festgelegt.

Erstellungsdatum

Datum und Uhrzeit der Erstellung des Buckets. Diese Spalte ist standardmäßig ausgeblendet.

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

a. Zeigen Sie die zusammenfassenden Informationen oben auf der Webseite an, um die Details für den Bucket zu bestätigen, z. B. Region und Objektanzahl.

b. Zeigen Sie die Balken für die Kapazitätslimitnutzung und die Objektanzahllimitnutzung an. Wenn die Nutzung 100 % oder nahe 100 % beträgt, sollten Sie eine Erhöhung des Limits oder das Löschen einiger Objekte in Erwägung ziehen.

c. Wählen Sie bei Bedarf **Objekte im Bucket löschen** und **Bucket löschen** aus.

> Achten Sie bei der Auswahl dieser Optionen genau auf die Warnhinweise. Weitere Informationen finden Sie unter:
>
> - "Löschen aller Objekte in einem Bucket"
> - "Löschen eines Buckets" (Bucket muss leer sein)

d. Zeigen Sie die Einstellungen für den Bucket auf den einzelnen Registerkarten nach Bedarf an, oder ändern Sie sie.

- **S3 Console**: Zeigt die Objekte für den Bucket an. Weitere Informationen finden Sie unter "Verwenden Sie die S3-Konsole".
- **Bucket-Optionen**: Optionen anzeigen oder ändern. Einige Einstellungen, wie z. B. S3 Object Lock, können nach dem Erstellen des Buckets nicht geändert werden.
  - "Management der Bucket-Konsistenz"
  - "Aktualisierung der Uhrzeit des letzten Zugriffs"
  - "Kapazitätsgrenze"
  - "Objektanzahllimit"
  - "Objektversionierung"
  - "S3-Objektsperre"
  - "Standardmäßige Bucket-Aufbewahrung"
  - "Grid-übergreifende Replizierung managen" (Falls für den Mieter zulässig)
- **Plattform-Services**: "Management von Plattform-Services" (Wenn für den Mieter erlaubt)
- **Bucket Access**: Optionen anzeigen oder ändern. Sie müssen über spezifische Zugriffsberechtigungen verfügen.
  - Konfigurieren"CORS für Buckets und Objekte" sodass der Bucket und die Objekte im Bucket für Webanwendungen in anderen Domänen zugänglich sind.
  - "Kontrolle des Benutzerzugriffs" Für einen S3-Bucket und Objekte in diesem Bucket.
- **Branches**: Zeigen Sie die Liste der Branch-Buckets für den Bucket an. "Erstellen Sie einen neuen Branch-Bucket oder verwalten Sie Branch-Buckets" .

Was ist ein Asteimer?

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

Sie erstellen einen Branch-Bucket aus einem vorhandenen Bucket. Nachdem Sie einen Branch-Bucket erstellt haben, wird der ursprüngliche Bucket, aus dem er erstellt wurde, als *Basis-Bucket* bezeichnet. Darüber hinaus können Sie einen Branch-Bucket aus einem anderen Branch-Bucket erstellen.

Ein Branch-Bucket bietet Zugriff auf geschützte Daten, dient jedoch nicht als Backup. Um die Daten weiterhin zu schützen, verwenden Sie diese Funktionen für Basis-Buckets:

- "S3-Objektsperre"
- "Grid-übergreifende Replizierung"für Basiseimer
- "Bucket-Richtlinien"für versionierte Buckets zum Bereinigen alter Objektversionen

Beachten Sie die folgenden Merkmale von Zweig-Buckets:

- Sie können auf die Objekte in Zweig-Buckets zugreifen, indem Sie"S3-Konsole zum Herunterladen von Objekten" .
- Wenn Clients auf Objekte in einem Branch-Bucket zugreifen,"Zugriffsrichtlinien" und nicht die Richtlinien des Basis-Buckets bestimmen, ob der Zugriff gewährt oder verweigert wird.
- Objekte, die in einem Basis-Bucket erstellt werden, werden danach ausgewertet, wie"ILM-Regeln" auf den Basiseimer anwenden. In einem Branch-Bucket erstellte Objekte werden basierend darauf ausgewertet, wie ILM-Regeln auf den Branch-Bucket angewendet werden.
- Die Cross-Grid-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 Sie einen Branch-Bucket von einem Zeitpunkt vor dem Auftreten der Beschädigung erstellen und dann Anwendungen auf den Branch-Bucket statt auf den Basis-Bucket verweisen, der beschädigte Objekte enthält.
- Sie speichern Daten in einem versionierten Bucket. Es gab eine versehentliche Sicherheitslücke, die dazu führte, dass nach der Zeit *T* viele unerwünschte Objekte aufgenommen wurden. Sie können einen Branch-Bucket für den Vorher-Zeitwert *T* erstellen und Clientvorgänge an diesen Branch-Bucket umleiten. Dann werden den Clients nur Objekte angezeigt, die vor der Vorzeit *T* aufgenommen wurden.

Operationen an Objekten in Branch-Buckets

- Eine PUT-Objektoperation für einen Branch-Bucket erstellt ein Objekt im Branch.
- Eine GET-Objektoperation für einen Branch-Bucket ruft ein Objekt aus dem Branch ab. Wenn das Objekt im Zweig-Bucket nicht vorhanden ist, wird das Objekt 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 Versionskennung	Basiseimer	Löschmarkierung wird nur für den Basis-Bucket erstellt	HEAD/GET gibt zurück, dass das Objekt nicht existiert, auf bestimmte Versionen kann jedoch noch zugegriffen werden	HEAD/GET gibt zurück, dass das Objekt vorhanden ist und auf bestimmte Versionen noch zugegriffen werden kann Die Löschmarkierung wäre nach dem Branch-Bucket erstellt worden `beforeTime` .
Löschen mit Versions-ID	Basiseimer	Eine bestimmte Objektversion wird sowohl für den Basis- als auch für den Zweig-Bucket gelöscht	HEAD/GET gibt zurück, dass die Objektversion nicht existiert	HEAD/GET gibt zurück, dass die Objektversion nicht existiert
Löschen ohne Versionskennung	Asteimer	Löschmarkierung wird nur für den Branch-Bucket erstellt	HEAD/GET gibt Objekt zurück (Basis-Bucket-Objekt nicht betroffen)	HEAD/GET gibt zurück, dass das Objekt nicht existiert
Löschen mit Versions-ID	Asteimer	Bestimmte Objektversionen werden nur für den Zweig-Bucket gelöscht	HEAD/GET gibt eine bestimmte Objektversion zurück (Basis-Bucket-Objekt nicht betroffen)	HEAD/GET gibt zurück, dass die Objektversion nicht existiert

Siehe auch"Löschen von S3-versionierten Objekten" .

Verwalten von Branch-Buckets

Verwenden Sie den Mandanten-Manager, um Details für Zweigstellen-Buckets zu erstellen und anzuzeigen.

Bevor Sie beginnen

- Sie haben sich beim Tenant Manager angemeldet mit einem"Unterstützter Webbrowser" .
- Sie gehören einer Benutzergruppe an, die über Root-Zugriff verfügt oder"Alle Berechtigungen für Buckets managen" . Diese Berechtigungen überschreiben die Berechtigungseinstellungen in Gruppen- oder Bucket-Richtlinien.
- Der Basis-Bucket, aus dem Sie einen Zweig erstellen möchten, hat"Versionierung aktiviert" .
- Sie sind der Eigentümer des Basis-Buckets.

Über diese Aufgabe

Beachten Sie die folgenden Informationen zu Branch-Buckets:

- Berechtigungen zum Festlegen von S3 Object Lock-Eigenschaften von Buckets oder Objekten können erteilt werden durch"Bucket-Richtlinie oder Gruppenrichtlinie" .
- Wenn Sie die Versionsverwaltung für den Basis-Bucket aussetzen, ist der Inhalt des Basis-Buckets in seinen Zweig-Buckets nicht mehr sichtbar.

Nachdem Sie einen Branch-Bucket konfiguriert und erstellt haben, können Sie die Konfiguration nicht mehr ändern.

Branch-Bucket erstellen

Schritte

1. Wählen Sie **View Buckets** aus dem Dashboard, oder wählen Sie **STORAGE (S3)** > **Buckets**.
2. Wählen Sie den Bucket aus, aus dem Sie einen Zweig erstellen möchten (den „Basis-Bucket“).
3. Wählen Sie auf der Bucket-Detailseite **Branches** > **Branch-Bucket erstellen**.

   Die Schaltfläche **Branch-Bucket erstellen** ist deaktiviert, wenn für den Basis-Bucket keine Versionierung aktiviert ist.

Geben Sie Details ein

Schritte

1. Geben Sie Details zum Zweig-Bucket ein.

Feld	Beschreibung
Name des Branch-Buckets	Ein Name für den Branch-Bucket, der diesen Regeln entspricht: • Jedes StorageGRID System muss eindeutig sein (nicht nur innerhalb des Mandantenkontos). • Muss DNS-konform sein. • Muss mindestens 3 und nicht mehr als 63 Zeichen enthalten. • Jedes Etikett muss mit einem Kleinbuchstaben oder einer Zahl beginnen und enden. Es können nur Kleinbuchstaben, Ziffern und Bindestriche verwendet werden. • Darf keine Punkte in Virtual-Hosted-Style-Anforderungen enthalten. Perioden verursachen Probleme bei der Überprüfung des Server-Platzhalterzertifikats. Weitere Informationen finden Sie im "Dokumentation der Amazon Web Services (AWS) zu den Bucket-Benennungsregeln". **Hinweis**: Sie können den Namen nach dem Erstellen des Branch-Buckets nicht mehr ändern.
Region (kann für Zweigstellen-Buckets nicht geändert werden)	Die Region des Zweig-Buckets. Die Region des Zweig-Buckets muss mit der Region des Basis-Buckets übereinstimmen, daher ist dieses Feld für Zweig-Buckets deaktiviert.

Feld	Beschreibung
Vor der Zeit	Die Frist für den Zugriff auf im Basis-Bucket erstellte Objektversionen vom Zweig-Bucket aus. Der Branch-Bucket bietet Zugriff auf Objektversionen, die vor dem Zeitpunkt „Before“ erstellt wurden. „Vor der Zeit“ muss ein Datum und eine Uhrzeit sein, die vergangen sind. Es kann kein zukünftiges Datum sein.
Zweigschaufeltyp	• **Lesen/Schreiben**: Sie können Objekte oder Objektversionen im Branch-Bucket hinzufügen oder löschen. • **Schreibgeschützt**: Sie können Objekte im Branch-Bucket nicht ändern. **Hinweis**: Sie können den Branch-Bucket-Typ nur dann auf schreibgeschützt setzen, wenn der Branch-Bucket leer ist. Wenn der Typ für einen vorhandenen Branch-Bucket auf Lesen/Schreiben eingestellt ist und Sie nicht darin geschrieben haben, können Sie den Typ auf schreibgeschützt ändern.

2. Wählen Sie **Weiter**.

Objekteinstellungen verwalten (optional)

Die Objekteinstellungen für einen Zweig-Bucket wirken sich nicht auf die Objektversionen im Basis-Bucket aus.

Schritte

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

   Aktivieren Sie S3 Object Lock für einen Branch-Bucket nur, wenn Sie Objekte für einen festgelegten Zeitraum aufbewahren müssen, beispielsweise um bestimmte gesetzliche Anforderungen zu erfüllen. S3 Object Lock ist eine permanente Einstellung, mit der Sie das Löschen oder Überschreiben von Objekten für einen festgelegten Zeitraum oder auf unbestimmte Zeit verhindern können.

   Nachdem die S3-Objektsperreinstellung 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. Möglicherweise können Sie diese Objekte oder den Branch-Bucket selbst nicht löschen.

2. Wenn Sie **S3-Objektsperre aktivieren** ausgewählt haben, aktivieren Sie optional **Standardaufbewahrung** für den Branch-Bucket.

   Ihr Grid-Administrator muss Ihnen die Berechtigung erteilen"Verwenden Sie bestimmte Funktionen von S3 Object Lock".

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

   a. Wenn **Standardaufbewahrung** aktiviert ist, geben Sie einen **Standardaufbewahrungsmodus** für den Branch-Bucket an.

Standardaufbewahrungsmodus	Beschreibung
Governance	• Benutzer mit der `s3:BypassGovernanceRetention` Berechtigung können den Anforderungskopf verwenden `x-amz-bypass-governance-retention: true`, um die Aufbewahrungseinstellungen zu umgehen. • Diese Benutzer können eine Objektversion löschen, bevor das Aufbewahrungsdatum erreicht ist. • Diese Benutzer können das Aufbewahrungsdatum eines Objekts erhöhen, verringern oder entfernen.
Compliance	• Das Objekt kann erst gelöscht werden, wenn das Aufbewahrungsdatum erreicht ist. • Das Aufbewahrungsdatum des Objekts kann erhöht, aber nicht verringert werden. • Das Aufbewahrungsdatum des Objekts kann erst entfernt werden, wenn dieses Datum erreicht ist. **Hinweis**: Ihr Grid-Administrator muss Ihnen erlauben, den Compliance-Modus zu verwenden.

b. Wenn die **Standardaufbewahrung** aktiviert ist, geben Sie die **Standardaufbewahrungsdauer** für den Zweig-Bucket an.

   Die **Standardaufbewahrungsfrist** gibt an, wie lange neue Objekte, die dem Branch-Bucket hinzugefügt werden, ab dem Zeitpunkt ihrer Aufnahme aufbewahrt werden sollen. Geben Sie einen Wert an, der kleiner oder gleich der vom Grid-Administrator festgelegten maximalen Aufbewahrungsdauer für den Mandanten ist.

Eine *maximale* Aufbewahrungsfrist, die ein Wert von 1 Tag bis 100 Jahre sein kann, wird festgelegt, wenn der Grid-Administrator den Mandanten erstellt. Wenn Sie eine *default* Aufbewahrungsfrist festlegen, darf sie den für die maximale Aufbewahrungsfrist festgelegten Wert nicht überschreiten. Bitten Sie bei Bedarf Ihren Grid-Administrator, die maximale Aufbewahrungsfrist zu verlängern oder zu verkürzen.

3. Wählen Sie optional **Kapazitätslimit aktivieren** aus.

   Die Kapazitätsgrenze ist die maximal verfügbare Kapazität für den Zweigstellen-Bucket. Dieser Wert stellt eine logische Menge (Objektgröße) dar, keine physische Menge (Größe auf der Festplatte).

   Wenn kein Limit festgelegt ist, ist die Kapazität für den Zweigstellen-Bucket unbegrenzt. Weitere Informationen finden Sie unter "Kapazitätsgrenze" für weitere Informationen.

   > 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. Wählen Sie optional **Objektanzahllimit aktivieren** aus.

   Die Objektanzahlgrenze ist die maximale Anzahl von Objekten, die der Zweig-Bucket enthalten kann. Dieser Wert stellt eine logische Menge (Objektanzahl) dar. 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. Wählen Sie **Eimer erstellen**.

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

6. Wählen Sie optional **Zur Bucket-Detailseite**, um"Details zum Branch-Bucket anzeigen" und führen Sie zusätzliche Konfigurationen durch.

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

Anwenden eines ILM-Richtlinien-Tags auf einen Bucket

Wählen Sie ein ILM-Richtlinien-Tag aus, das auf einen Bucket angewendet werden soll, basierend auf den Anforderungen des Objekt-Storage.

Die ILM-Richtlinie steuert, wo die Objektdaten gespeichert werden und ob sie nach einem bestimmten Zeitraum gelöscht werden. Der Grid-Administrator erstellt ILM-Richtlinien und weist sie ILM-Richtlinien-Tags zu, wenn mehrere aktive Richtlinien verwendet werden.

Vermeiden Sie die häufige Neuzuweisung des Policy-Tags eines Buckets. Anderenfalls kann es zu Performance-Problemen kommen.

Bevor Sie beginnen

- Sie sind beim Tenant Manager mit einem angemeldet"Unterstützter Webbrowser".
- Sie gehören zu einer Benutzergruppe mit dem "Root-Zugriff, Alle Buckets verwalten oder Alle Buckets anzeigen". Diese Berechtigungen überschreiben die Berechtigungseinstellungen in Gruppen- oder Bucket-Richtlinien.

Schritte

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

   Die Seite „Buckets“ wird angezeigt. Bei Bedarf können Sie die Informationen nach einer beliebigen Spalte sortieren oder Sie können die Seite vorwärts und zurück durch die Liste blättern.

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

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

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

3. Erweitern Sie auf der Registerkarte Bucket-Optionen das ILM-Richtlinien-Tag Akkordeon. Dieses Akkordeon wird nur angezeigt, wenn Ihr Grid-Administrator die Verwendung von benutzerdefinierten Richtlinien-Tags aktiviert hat.

4. Lesen Sie die Beschreibung der einzelnen Richtlinien-Tags, um festzulegen, welches Tag auf den Bucket angewendet werden soll.

> Wenn Sie das ILM-Richtlinien-Tag für einen Bucket ändern, wird eine ILM-Neubewertung aller Objekte im Bucket ausgelöst. Wenn die neue Richtlinie Objekte für eine begrenzte Zeit aufbewahrt, werden ältere Objekte gelöscht.

5. Aktivieren Sie das Optionsfeld für das Tag, das Sie dem Bucket zuweisen möchten.
6. Wählen Sie **Änderungen speichern**. Auf dem Bucket wird ein neues S3-Bucket-Tag mit dem Schlüssel und dem Wert des ILM-Richtlinien-Tag-Namens festgelegt `NTAP-SG-ILM-BUCKET-TAG`.

> 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 nicht angegeben ist, werden Objekte in dem Bucket anhand der standardmäßigen ILM-Richtlinie wiederhergestellt.

> ILM-Richtlinien-Tags können nur mit der Tenant Manager- oder Tenant Manager-API festgelegt und geändert werden, wobei das ILM-Richtlinien-Tag validiert wird. Ändern Sie das ILM-Richtlinien-Tag nicht `NTAP-SG-ILM-BUCKET-TAG` über die S3 PutBucketTagging API oder die S3 DeleteBucketTagging API.

> Das Ändern der Richtlinie-Tag, die einem Bucket zugewiesen ist, wirkt sich vorübergehend auf die Performance aus, während Objekte mithilfe der neuen ILM-Richtlinie neu bewertet werden.

Management von Bucket-Richtlinien

Sie können den Benutzerzugriff für einen S3-Bucket und die Objekte in diesem Bucket steuern.

Bevor Sie beginnen

- Sie sind beim Tenant Manager mit einem angemeldet"Unterstützter Webbrowser".
- Sie gehören zu einer Benutzergruppe mit dem "Root-Zugriffsberechtigung". Die Berechtigungen Alle Buckets anzeigen und alle Buckets verwalten erlauben nur die Anzeige.
- Sie haben überprüft, ob die erforderliche Anzahl an Storage Nodes und Standorten verfügbar ist. 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.

Schritte

1. Wählen Sie **Buckets** aus, und wählen Sie dann den Bucket aus, den Sie verwalten möchten.
2. Wählen Sie auf der Seite mit den Bucket-Details **Bucket Access** > **Bucket Policy** aus.
3. Führen Sie einen der folgenden Schritte aus:
   - Geben Sie eine Bucket Policy ein, indem Sie das Kontrollkästchen **enable Policy** aktivieren. Geben Sie dann eine gültige JSON-formatierte Zeichenfolge ein.

     Jede Bucket-Richtlinie hat ein Größenlimit von 20,480 Byte.

- Ändern Sie eine vorhandene Richtlinie, indem Sie die Zeichenfolge bearbeiten.
- Deaktivieren Sie eine Richtlinie, indem Sie die Option **Richtlinie aktivieren** deaktivieren.

Ausführliche Informationen zu Bucket-Richtlinien, einschließlich Sprachtyntax und Beispielen, finden Sie unter "Beispiel für Bucket-Richtlinien".

Management der Bucket-Konsistenz

Mithilfe von Konsistenzwerten können Änderungen an den Bucket-Einstellungen festgelegt und ein Gleichgewicht zwischen der Verfügbarkeit der Objekte in einem Bucket und der Konsistenz dieser Objekte in verschiedenen Storage-Nodes und Standorten sichergestellt werden. Sie können die Konsistenzwerte so ändern, dass sie sich von den Standardwerten unterscheiden, damit Client-Anwendungen ihre betrieblichen Anforderungen erfüllen können.

Bevor Sie beginnen

- Sie sind beim Tenant Manager mit einem angemeldet"Unterstützter Webbrowser".
- Sie gehören zu einer Benutzergruppe mit dem "Managen aller Buckets oder Root-Zugriffsberechtigungen". Diese Berechtigungen überschreiben die Berechtigungseinstellungen in Gruppen- oder Bucket-Richtlinien.

Bucket-Konsistenzrichtlinien

Die Bucket-Konsistenz wird verwendet, um die Konsistenz von Client-Applikationen zu bestimmen, die sich auf Objekte in diesem S3 Bucket auswirken. Im Allgemeinen sollten Sie die Konsistenz **Read-after-New-write** für Ihre Buckets verwenden.

Bucket-Konsistenz ändern

Wenn die Konsistenz **Read-after-New-write** nicht den Anforderungen der Client-Anwendung entspricht, können Sie die Konsistenz ändern, indem Sie die Bucket-Konsistenz oder den Header festlegen `Consistency-Control`. Die `Consistency-Control` Kopfzeile überschreibt die Bucket-Konsistenz.

> Wenn Sie die Konsistenz eines Buckets ändern, erfüllen nur die Objekte, die nach der Änderung aufgenommen werden, die überarbeitete Einstellung.

Schritte

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

   Die Seite mit den Bucket-Details wird angezeigt.

3. Wählen Sie auf der Registerkarte **Bucket options** die Option ** accordion aus.
4. Wählen Sie eine Konsistenz für Vorgänge aus, die an den Objekten in diesem Bucket ausgeführt werden.
   - **All**: Bietet die höchste Konsistenz. Alle Nodes erhalten die Daten sofort, sonst schlägt die Anfrage fehl.
   - **Strong-global**: Garantiert Lese-nach-Schreiben-Konsistenz für alle Client-Anfragen über alle Standorte hinweg.
   - **Strong-site**: Garantiert Lese-nach-Schreiben Konsistenz für alle Client-Anfragen innerhalb einer Site.

- **Read-after-New-write** (default): Bietet Read-after-write-Konsistenz für neue Objekte und eventuelle Konsistenz für Objektaktualisierungen. Hochverfügbarkeit und garantierte Datensicherung Empfohlen für die meisten Fälle.
- **Verfügbar**: Bietet eventuelle Konsistenz für neue Objekte und Objekt-Updates. Verwenden Sie für S3-Buckets nur nach Bedarf (z. B. für einen Bucket mit Protokollwerten, die nur selten gelesen werden, oder für HEAD- oder GET-Vorgänge für nicht vorhandene Schlüssel). Nicht unterstützt für S3 FabricPool-Buckets.

5. Wählen Sie **Änderungen speichern**.

Was passiert, wenn Sie Bucket-Einstellungen ändern

Buckets verfügen über mehrere Einstellungen, die sich auf das Verhalten der Buckets und der Objekte in diesen Buckets auswirken.

Die folgenden Bucket-Einstellungen verwenden standardmäßig **strong**-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 von leeren Buckets im Hintergrund"
- "Zeitpunkt Des Letzten Zugriffs"
- "Bucket-Lebenszyklus"
- "Bucket-Richtlinie"
- "Bucket-Tagging"
- "Bucket-Versionierung"
- "S3-Objektsperre"
- "Bucket-Verschlüsselung"

Der Konsistenzwert für Bucket-Versionierung, S3 Object Lock- und Bucket-Verschlüsselung kann nicht auf einen Wert festgelegt 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 können einige Zeit dauern, bevor sie wirksam werden.

- "Konfiguration von Plattform-Services: Benachrichtigung, Replikation oder Suchintegration"
- "Konfigurieren Sie StorageGRID CORS für Buckets und Objekte"
- Änderung der Bucket-Konsistenz

Wenn die Standardkonsistenz, die beim Ändern von Bucket-Einstellungen verwendet wird, nicht den Anforderungen der Client-Anwendung entspricht, können Sie die Konsistenz ändern, indem Sie den `Consistency-Control` Header für "S3-REST-API"oder verwenden, indem Sie die Optionen oder `force` im verwenden `reducedConsistency`"Mandantenmanagement-API".

Aktiviert bzw. deaktiviert Updates der letzten Zugriffszeit

Wenn Grid-Administratoren die Regeln für das Information Lifecycle Management (ILM) für ein StorageGRID-System erstellen, können sie optional angeben, dass die letzte

Zugriffszeit eines Objekts verwendet wird, um zu bestimmen, ob das Objekt auf einen anderen Storage-Standort verschoben werden soll. Wenn Sie einen S3-Mandanten verwenden, können Sie diese Regeln nutzen, indem Sie Updates der letzten Zugriffszeit für die Objekte in einem S3-Bucket aktivieren.

Diese Anweisungen gelten nur für StorageGRID-Systeme, die mindestens eine ILM-Regel enthalten, die die Option **Letzte Zugriffszeit** als erweiterten Filter oder als Referenzzeit verwendet. Sie können diese Anweisungen ignorieren, wenn Ihr StorageGRID System eine solche Regel nicht enthält. Weitere Informationen finden Sie unter "Verwenden Sie die letzte Zugriffszeit in ILM-Regeln" .

Bevor Sie beginnen

- Sie sind beim Tenant Manager mit einem angemeldet"Unterstützter Webbrowser".
- Sie gehören zu einer Benutzergruppe mit dem "Managen aller Buckets oder Root-Zugriffsberechtigungen". Diese Berechtigungen überschreiben die Berechtigungseinstellungen in Gruppen- oder Bucket-Richtlinien.

Über diese Aufgabe

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

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

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

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

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

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

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

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

Art der Anfrage

	Verhalten, wenn die letzte Zugriffszeit deaktiviert ist (Standard)		Verhalten, wenn die letzte Zugriffszeit aktiviert ist	
	Zeitpunkt des letzten Zugriffs aktualisiert?	Das Objekt wurde zur ILM-Auswertungswarteschlange hinzugefügt?	Zeitpunkt des letzten Zugriffs aktualisiert?	Das Objekt wurde zur ILM-Auswertungswarteschlange hinzugefügt?
Anforderung zum Abrufen der Metadaten eines Objekts, wenn eine HEAD-Operation ausgeführt wird	Nein	Nein	Nein	Nein
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 Auflisten von Objekten oder Objektversionen	Nein	Nein	Nein	Nein
Anforderung 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
Anforderung zum Abschließen eines mehrteiligen Uploads	Ja, für das zusammengesetzte Objekt	Ja, für das zusammengesetzte Objekt	Ja, für das zusammengesetzte Objekt	Ja, für das zusammengesetzte Objekt

Schritte

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

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

Ändern Sie die Objektversionierung für einen Bucket

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

Bevor Sie beginnen

- Sie sind beim Tenant Manager mit einem angemeldet"Unterstützter Webbrowser".
- Sie gehören zu einer Benutzergruppe mit dem "Managen aller Buckets oder Root-Zugriffsberechtigungen". Diese Berechtigungen überschreiben die Berechtigungseinstellungen in Gruppen- oder Bucket-Richtlinien.
- Sie haben überprüft, ob die erforderliche Anzahl an Storage Nodes und Standorten verfügbar ist. 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.

Über diese Aufgabe

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

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

Weitere Informationen finden Sie im Folgenden:

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

Schritte

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

   Die Seite mit den Bucket-Details wird angezeigt.

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

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

Option	Beschreibung
Aktivieren Sie die Versionierung	Aktivieren Sie die Objektversionierung, wenn Sie jede Version jedes Objekts in diesem Bucket speichern möchten. Sie können dann nach Bedarf frühere Versionen eines Objekts abrufen. Objekte, die sich bereits im Bucket befanden, werden versioniert, wenn sie von einem Benutzer geändert werden.

Option	Beschreibung
Die Versionierung unterbrechen	Unterbrechen Sie die Objektversionierung, wenn Sie keine neuen Objektversionen mehr erstellen möchten. Sie können weiterhin alle vorhandenen Objektversionen abrufen.

5. Wählen Sie **Änderungen speichern**.

Verwenden Sie S3 Objektsperre, um Objekte beizubehalten

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

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

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

Ein Bucket ohne S3 Object Lock kann nur Objekte ohne Aufbewahrungseinstellungen haben. Keine aufgenommenen Objekte verfügen über Aufbewahrungseinstellungen.

Ein Bucket mit S3 Object Lock kann Objekte mit und ohne Aufbewahrungseinstellungen haben, die von S3-Client-Applikationen angegeben wurden. Einige aufgenommene Objekte haben Aufbewahrungseinstellungen.

Ein Bucket mit S3 Object Lock und konfigurierter Standardaufbewahrung kann Objekte mit angegebenen Aufbewahrungseinstellungen und neue Objekte ohne Aufbewahrungseinstellungen hochgeladen haben. Die neuen Objekte verwenden die Standardeinstellung, da die Aufbewahrungseinstellung nicht auf Objektebene konfiguriert wurde.

Tatsächlich verfügen alle neu aufgenommenen Objekte über Aufbewahrungseinstellungen, wenn die Standardaufbewahrung konfiguriert ist. Vorhandene Objekte ohne Objektaufbewahrungseinstellungen bleiben hiervon unberührt.

Aufbewahrungsmodi

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

- Im Compliance-Modus:
  - Das Objekt kann erst gelöscht werden, wenn das Aufbewahrungsdatum erreicht ist.
  - Das Aufbewahrungsdatum des Objekts kann erhöht, aber nicht verringert werden.
  - Das Aufbewahrungsdatum des Objekts kann erst entfernt werden, wenn dieses Datum erreicht ist.
- Im Governance-Modus:

- Benutzer mit besonderer Berechtigung können in Anfragen einen Überbrückungskopf verwenden, um bestimmte Aufbewahrungseinstellungen zu ändern.
- Diese Benutzer können eine Objektversion löschen, bevor das Aufbewahrungsdatum erreicht ist.
- Diese Benutzer können das Aufbewahrungsdatum eines Objekts erhöhen, verringern oder entfernen.

Aufbewahrungseinstellungen für Objektversionen

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

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

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

  Details zu den Objekteinstellungen finden Sie unter "Konfigurieren Sie die S3-Objektsperre über die S3-REST-API".

Standardeinstellung für die Aufbewahrung von Buckets

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

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

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

Siehe "Erstellen eines S3-Buckets" und "Aktualisieren Sie die S3 Object Lock-Standardaufbewahrung".

S3 Objektsperraufgaben

Die folgenden Listen für Grid-Administratoren und Mandantenbenutzer enthalten die allgemeinen Aufgaben für die Verwendung der S3 Objektsperrfunktion.

Grid-Administrator

- Globale S3-Objektsperrung für das gesamte StorageGRID-System aktivieren.
- Stellen Sie sicher, dass die Richtlinien für Information Lifecycle Management (ILM) den *Compliance-Anforderungen entsprechen*, "Anforderungen für Buckets mit aktivierter S3-Objektsperrung"d. h. dass

sie die erfüllen.

- Erlauben Sie einem Mandanten nach Bedarf, Compliance als Aufbewahrungsmodus zu verwenden. Andernfalls ist nur der Governance-Modus zulässig.
- Legen Sie bei Bedarf eine maximale Aufbewahrungsfrist für einen Mandanten fest.

Mandantenbenutzer

- Überlegungen für Buckets und Objekte mit S3 Object Lock prüfen.
- Wenden Sie sich bei Bedarf an den Grid-Administrator, um die globale S3 Object Lock-Einstellung zu aktivieren und Berechtigungen festzulegen.
- Erstellen von Buckets mit aktivierter S3-Objektsperre
- Optional können Sie Standardaufbewahrungseinstellungen für einen Bucket konfigurieren:
  - Standardaufbewahrungsmodus: Governance oder Compliance, falls vom Grid-Administrator zugelassen.
  - Standardaufbewahrungszeitraum: Muss kleiner oder gleich der maximalen Aufbewahrungsfrist sein, die vom Grid-Administrator festgelegt wurde.
- Fügen Sie mithilfe der S3-Client-Applikation Objekte hinzu und legen Sie optional die objektspezifische Aufbewahrung fest:
  - Aufbewahrungsmodus. Governance oder Compliance, falls vom Grid-Administrator zugelassen.
  - Bis-Datum beibehalten: Muss kleiner oder gleich dem sein, was durch die vom Grid-Administrator festgelegte maximale Aufbewahrungsfrist zulässig 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.
- Wenn Sie die S3-Objektsperre verwenden möchten, müssen Sie beim Erstellen des Buckets die S3-Objektsperre aktivieren. Sie können die S3-Objektsperre für einen vorhandenen Bucket nicht aktivieren.
- Wenn die S3-Objektsperre für einen Bucket aktiviert ist, ermöglicht StorageGRID automatisch die Versionierung für diesen Bucket. Sie können S3 Object Lock nicht deaktivieren oder die Versionierung für den Bucket nicht unterbrechen.
- Optional können Sie mithilfe von Tenant Manager, der Mandanten-Management-API oder der S3-REST-API für jeden Bucket einen Standardaufbewahrungsmodus und einen Aufbewahrungszeitraum angeben. Die Standardaufbewahrungseinstellungen des Buckets gelten nur für neue Objekte, die dem Bucket hinzugefügt wurden und keine eigenen Aufbewahrungseinstellungen haben. Sie können diese Standardeinstellungen außer Kraft setzen, indem Sie einen Aufbewahrungsmodus und das Aufbewahrungsdatum für jede Objektversion festlegen, wenn sie hochgeladen wird.
- Die Konfiguration des Bucket-Lebenszyklus wird für Buckets unterstützt, für die S3 Object Lock aktiviert ist.
- Die CloudMirror-Replizierung wird für Buckets nicht unterstützt, wenn S3-Objektsperre aktiviert ist.

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

- Zum Schutz einer Objektversion können Sie Standardaufbewahrungseinstellungen für den Bucket angeben oder Aufbewahrungseinstellungen für jede Objektversion angeben. Aufbewahrungseinstellungen auf Objektebene können mit der S3-Client-Applikation oder der S3-REST-API angegeben werden.
- Aufbewahrungseinstellungen gelten für einzelne Objektversionen. Eine Objektversion kann sowohl eine

Aufbewahrungsfrist als auch eine gesetzliche Haltungseinstellung haben, eine jedoch nicht die andere oder keine. Wenn Sie eine Aufbewahrungsfrist oder eine gesetzliche Aufbewahrungseinstellung für ein Objekt angeben, wird nur die in der Anforderung angegebene Version geschützt. Sie können neue Versionen des Objekts erstellen, während die vorherige Version des Objekts gesperrt bleibt.

Lebenszyklus von Objekten in Buckets, wobei S3 Objektsperre aktiviert ist

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

1. **Objektaufnahme**

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

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

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

2. **Objektaufbewahrung und -Löschung**

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

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

Kann ich auch ältere konforme Buckets verwalten?

Die S3-Objektsperre ersetzt die in früheren StorageGRID-Versionen verfügbare Compliance-Funktion. Wenn Sie mithilfe einer früheren Version von StorageGRID konforme Buckets erstellt haben, können Sie die Einstellungen dieser Buckets weiterhin verwalten. Sie können jedoch keine neuen, konformen Buckets mehr erstellen. Anweisungen hierzu finden Sie unter "NetApp Knowledge Base: Management älterer, konformer Buckets für StorageGRID 11.5".

Aktualisieren Sie die S3 Object Lock-Standardaufbewahrung

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

Bevor Sie beginnen

- Sie sind beim Tenant Manager mit einem angemeldet"Unterstützter Webbrowser".
- Sie gehören zu einer Benutzergruppe mit dem "Managen aller Buckets oder Root-Zugriffsberechtigungen". Diese Berechtigungen überschreiben die Berechtigungseinstellungen in Gruppen- oder Bucket-Richtlinien.
- S3 Objektsperre ist global für Ihr StorageGRID-System aktiviert; Sie haben S3 Objektsperre bei Erstellung des Buckets aktiviert. Siehe "Verwenden Sie S3 Objektsperre, um Objekte beizubehalten".

Schritte

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

   Die Seite mit den Bucket-Details wird angezeigt.

3. Wählen Sie auf der Registerkarte **Bucket options** das Akkordeon **S3 Object Lock** aus.
4. Aktivieren oder deaktivieren Sie optional **Default Retention** für diesen Bucket.

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

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

Standardaufbewahrungsmodus	Beschreibung
Governance	• Benutzer mit der `s3:BypassGovernanceRetention` Berechtigung können den Anforderungskopf verwenden `x-amz-bypass-governance-retention: true`, um die Aufbewahrungseinstellungen zu umgehen. • Diese Benutzer können eine Objektversion löschen, bevor das Aufbewahrungsdatum erreicht ist. • Diese Benutzer können das Aufbewahrungsdatum eines Objekts erhöhen, verringern oder entfernen.
Compliance	• Das Objekt kann erst gelöscht werden, wenn das Aufbewahrungsdatum erreicht ist. • Das Aufbewahrungsdatum des Objekts kann erhöht, aber nicht verringert werden. • Das Aufbewahrungsdatum des Objekts kann erst entfernt werden, wenn dieses Datum erreicht ist. **Hinweis**: Ihr Grid-Administrator muss Ihnen erlauben, den Compliance-Modus zu verwenden.

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

   Die **Default Retention Period** gibt an, wie lange neue Objekte zu diesem Bucket hinzugefügt werden sollen, beginnend mit dem Zeitpunkt, zu dem sie aufgenommen werden. Geben Sie einen Wert an, der kleiner oder gleich der maximalen Aufbewahrungsfrist für den Mandanten ist, wie vom Grid-Administrator festgelegt.

   Eine *maximale* Aufbewahrungsfrist, die ein Wert von 1 Tag bis 100 Jahre sein kann, wird festgelegt, wenn der Grid-Administrator den Mandanten erstellt. Wenn Sie eine *default* Aufbewahrungsfrist festlegen, darf

sie den für die maximale Aufbewahrungsfrist festgelegten Wert nicht überschreiten. Bitten Sie bei Bedarf Ihren Grid-Administrator, die maximale Aufbewahrungsfrist zu verlängern oder zu verkürzen.

7. Wählen Sie **Änderungen speichern**.

Konfigurieren Sie StorageGRID CORS für Buckets und Objekte

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

Bevor Sie beginnen

- Sie sind beim Tenant Manager mit einem angemeldet"Unterstützter Webbrowser".
- Für GET CORS-Konfigurationsanforderungen gehören Sie einer Benutzergruppe an, die den hat"Managen aller Buckets oder Anzeigen aller Buckets Berechtigung". Diese Berechtigungen überschreiben die Berechtigungseinstellungen in Gruppen- oder Bucket-Richtlinien.
- Für PUT CORS-Konfigurationsanforderungen gehören Sie einer Benutzergruppe "Alle Berechtigungen für Buckets managen"an, die den hat. Diese Berechtigung überschreibt die Berechtigungseinstellungen in Gruppen- oder Bucket-Richtlinien.
- Der "Root-Zugriffsberechtigung" bietet Zugriff auf alle CORS-Konfigurationsanforderungen.

Über diese Aufgabe

CORS (Cross-Origin Resource Sharing) ist ein Sicherheitsmechanismus, mit dem Client-Webanwendungen in einer Domäne auf Ressourcen in einer anderen Domäne zugreifen können. Angenommen, Sie verwenden einen S3-Bucket mit dem Namen `Images` zum Speichern von Grafiken. Durch die Konfiguration von CORS für den `Images` Bucket können Sie die Bilder in diesem Bucket auf der Website anzeigen lassen `http://www.example.com`.

CORS für einen Bucket aktivieren

Schritte

1. Verwenden Sie einen Texteditor, um die erforderliche XML zu erstellen. Dieses Beispiel zeigt die XML, die zur Aktivierung von CORS für einen S3-Bucket verwendet wird. Im Detail:
   - Ermöglicht jeder Domäne, GET-Anforderungen an den Bucket zu senden
   - Ermöglicht der Domäne nur `http://www.example.com` das Senden von GET-, POST- und LÖSCHANFRAGEN
   - Alle Anforderungskopfzeilen 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 User Guide".

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

   Die Seite mit den Bucket-Details wird angezeigt.

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

CORS-Einstellung ändern

Schritte

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

Deaktivieren Sie die CORS-Einstellung

Schritte

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

Verwandte Informationen

"Konfigurieren Sie StorageGRID CORS für eine Verwaltungsschnittstelle"

Löschen von Objekten in Bucket

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

Überlegungen und Anforderungen

Bevor Sie diese Schritte durchführen, beachten Sie Folgendes:

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

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

- Während Objekte gelöscht werden, ist der Zustand des Buckets **delete objects: Read-only**. In diesem Status können Sie dem Bucket keine neuen Objekte hinzufügen.
- Nachdem alle Objekte gelöscht wurden, verbleibt der Bucket im schreibgeschützten Status. Sie haben folgende Möglichkeiten:
  - Versetzen Sie den Bucket in den Schreibmodus und verwenden Sie ihn für neue Objekte wieder
  - Löschen Sie den Bucket
  - Belassen Sie den Bucket im schreibgeschützten Modus, um seinen Namen für eine zukünftige Verwendung zu reservieren
- Wenn für einen Bucket die Objektversionierung aktiviert ist, können Löschmarkierungen, die in StorageGRID 11.8 oder höher erstellt wurden, mithilfe der Option Objekte löschen in Bucket-Operationen entfernt werden.
- Wenn für einen Bucket die Objektversionierung aktiviert ist, entfernt der Vorgang „Objekte löschen“ keine Löschmarkierungen, die in StorageGRID 11.7 oder früher erstellt wurden. Siehe Informationen zum Löschen von Objekten in einem Bucket in "Löschen von S3-versionierten Objekten".
- Wenn Sie verwenden"Grid-übergreifende Replizierung", beachten Sie Folgendes:
  - Mit dieser Option werden keine Objekte aus dem Bucket auf dem anderen Raster gelöscht.
  - Wenn Sie diese Option für den Quell-Bucket auswählen, wird die Warnung **gitterübergreifender Replikationsfehler** ausgelöst, wenn Sie dem Ziel-Bucket auf dem anderen Grid Objekte hinzufügen. Wenn Sie nicht garantieren können, dass niemand dem Bucket auf dem anderen Raster Objekte für diesen Bucket hinzufügt, "Deaktivieren Sie die Grid-übergreifende Replizierung"bevor alle Bucket-Objekte gelöscht werden.

Bevor Sie beginnen

- Sie sind beim Tenant Manager mit einem angemeldet"Unterstützter Webbrowser".
- Sie gehören zu einer Benutzergruppe mit dem "Root-Zugriffsberechtigung". Diese Berechtigung überschreibt die Berechtigungseinstellungen in Gruppen- oder Bucket-Richtlinien.

Schritte

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

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

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

   Menü „Aktionen“

   a. Aktivieren Sie das Kontrollkästchen für jeden Bucket, aus dem Sie Objekte löschen möchten.

   b. Wählen Sie **actions** > **Delete objects in bucket**.

   Detailseite

   a. Wählen Sie einen Bucket-Namen aus, um die Details anzuzeigen.

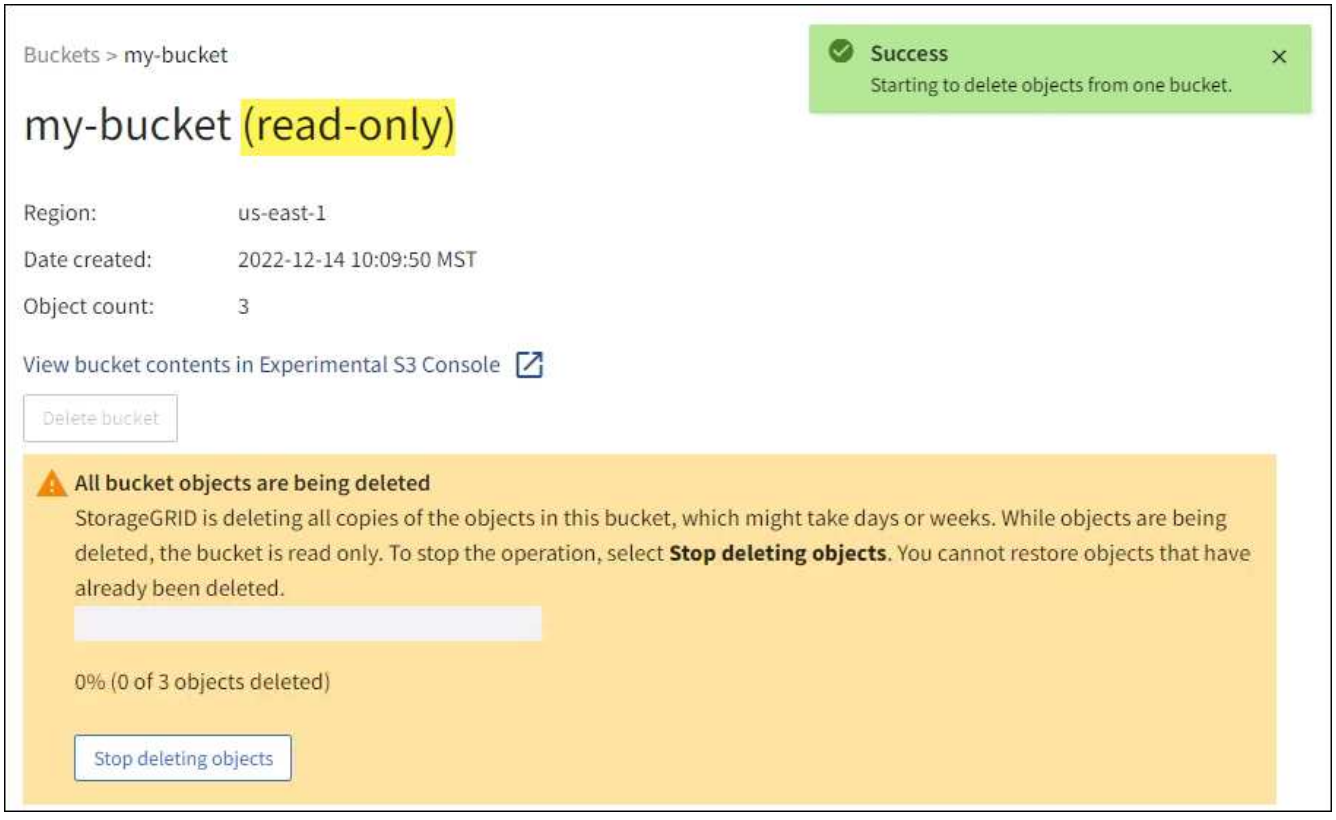
   b. Wählen Sie **Objekte im Bucket löschen**.

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

4. Warten Sie, bis der Löschvorgang beginnt.

   Nach ein paar Minuten:

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

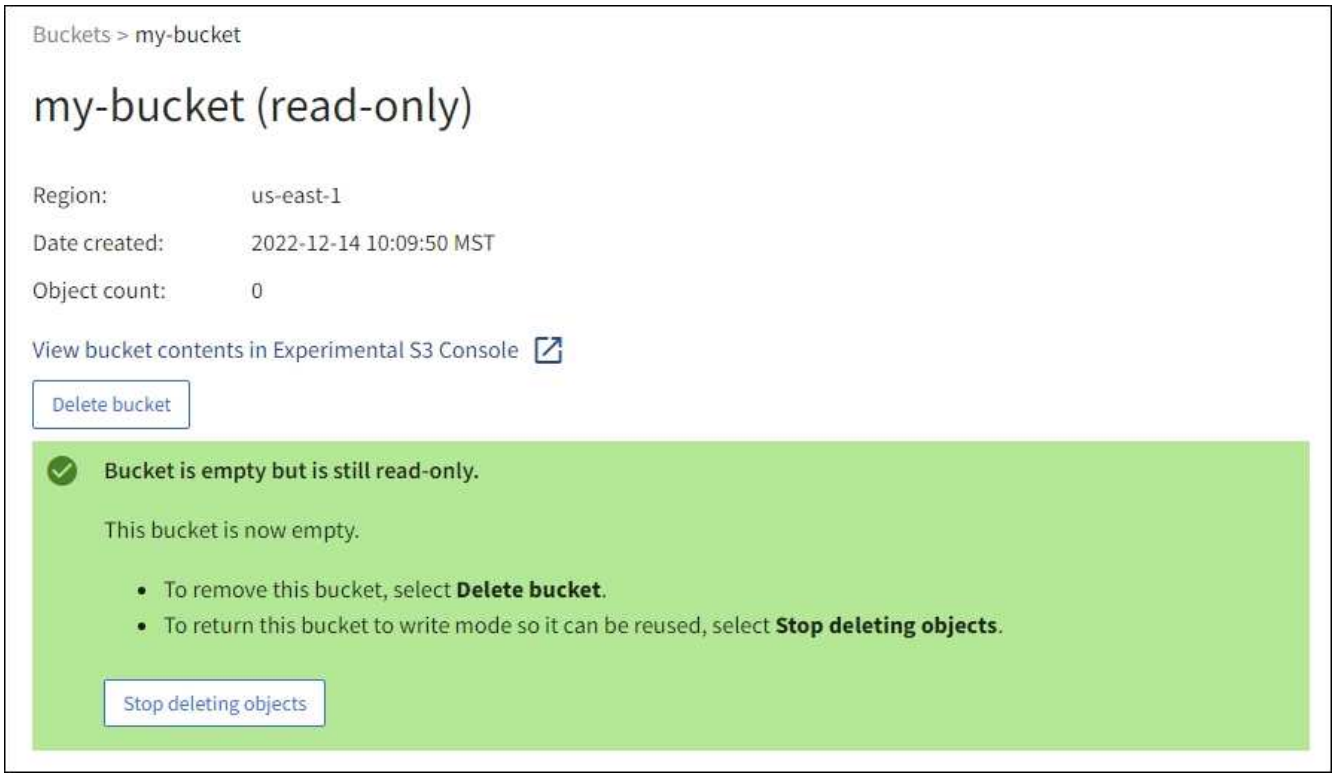


5. Wählen Sie, wie erforderlich, während der Vorgang ausgeführt wird, **Löschen von Objekten stoppen**, um den Prozess anzuhalten. Wählen Sie dann optional **Objekte im Bucket löschen** aus, um den Prozess fortzusetzen.

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

6. Warten Sie, bis der Vorgang abgeschlossen ist.

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



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

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

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

S3-Bucket löschen

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

Bevor Sie beginnen

- Sie sind beim Tenant Manager mit einem angemeldet"Unterstützter Webbrowser".
- Sie gehören zu einer Benutzergruppe mit dem "Managen aller Buckets oder Root-Zugriffsberechtigungen". Diese Berechtigungen überschreiben die Berechtigungseinstellungen in Gruppen- oder Bucket-Richtlinien.
- Die Buckets, die Sie löschen möchten, sind leer. Wenn Buckets, die Sie löschen möchten, *Not* leer sind, "Löschen von Objekten aus dem Bucket".

Über diese Aufgabe

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

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

Schritte

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

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

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

   Menü „Aktionen“

   a. Aktivieren Sie das Kontrollkästchen für jeden Bucket, den Sie löschen möchten.

   b. Wählen Sie **Actions** > **Eimer löschen**.

   Detailseite

   a. Wählen Sie einen Bucket-Namen aus, um die Details anzuzeigen.

   b. Wählen Sie **Eimer löschen**.

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

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

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

Verwenden Sie die S3-Konsole

Mit der S3-Konsole können Sie die Objekte in einem S3-Bucket anzeigen und managen.

Mithilfe der S3-Konsole können Sie

- Hochladen, herunterladen, umbenennen, kopieren, verschieben, und Objekte löschen
- Objektversionen anzeigen, zurücksetzen, herunterladen und löschen
- Suchen Sie nach Objekten nach Präfix
- Verwalten von Objekt-Tags
- Zeigen Sie Objektmetadaten an
- Anzeigen, Erstellen, Umbenennen, Kopieren, Verschieben, und Ordner löschen

> Die S3-Konsole bietet in den gängigsten Fällen eine höhere Benutzerfreundlichkeit. Es ist nicht dafür ausgelegt, CLI- oder API-Vorgänge in allen Situationen zu ersetzen.
>
> Wenn Vorgänge durch die Verwendung von S3-Konsole zu lange dauern (z. B. Minuten oder Stunden), sollten Sie Folgendes berücksichtigen:
>
> - Reduzieren der Anzahl ausgewählter Objekte
> - Verwenden von nicht-grafischen (API oder CLI) Methoden für den Zugriff auf Ihre Daten

Bevor Sie beginnen

- Sie sind beim Tenant Manager mit einem angemeldet"Unterstützter Webbrowser".
- Wenn Sie Objekte verwalten möchten, gehören Sie einer Benutzergruppe an, die über die Root-Zugriffsberechtigung verfügt. Alternativ gehören Sie zu einer Benutzergruppe, die über die Berechtigung zur Registerkarte „S3-Konsole verwenden“ und entweder die Berechtigung „Alle Buckets anzeigen“ oder „Alle Buckets verwalten“ verfügt. Siehe "Mandantenmanagement-Berechtigungen".
- Für den Benutzer wurde eine S3-Gruppen- oder Bucket-Richtlinie konfiguriert. Sehen "Verwendung von Bucket- und Gruppenzugriffsrichtlinien" .
- Sie kennen die Zugriffsschlüssel-ID und den geheimen Zugriffsschlüssel des Benutzers. Optional haben Sie eine `.csv` Datei, die diese Informationen enthält. Siehe "Anweisungen zum Erstellen von Zugriffsschlüsseln".

Schritte

1. Wählen Sie **Speicher** > **Buckets** > ***Bucketname***.
2. Wählen Sie die Registerkarte S3-Konsole aus.
3. Fügen Sie die Zugriffsschlüssel-ID und den geheimen Zugriffsschlüssel in die Felder ein. Andernfalls wählen Sie **Zugriffsschlüssel hochladen** und wählen Sie Ihre `.csv` Datei aus.
4. Wählen Sie **Anmelden**.
5. Die Tabelle der Bucket-Objekte wird angezeigt. Sie können Objekte nach Bedarf verwalten.

Weitere Informationen

- **Suche nach Präfix**: Die Präfix-Suche sucht nur nach Objekten, die mit einem bestimmten Wort relativ zum aktuellen Ordner beginnen. Die Suche umfasst keine Objekte, die das Wort an anderer Stelle enthalten. Diese Regel gilt auch für Objekte in Ordnern. Zum Beispiel würde eine Suche nach `folder1/folder2/somefile-` Objekte zurückgeben, die sich innerhalb des Ordners befinden `folder1/folder2/` und mit dem Wort beginnen `somefile-`.
- **Drag & Drop**: Sie können Dateien aus dem Dateimanager Ihres Computers in die S3-Konsole ziehen und ablegen. Sie können jedoch keine Ordner hochladen.
- **Operationen für Ordner**: Wenn Sie einen Ordner verschieben, kopieren oder umbenennen, werden alle Objekte im Ordner einzeln aktualisiert, was Zeit in Anspruch nehmen kann.

- **Permanent Deletion wenn Bucket-Versionierung deaktiviert ist**: Wenn Sie ein Objekt in einem Bucket mit deaktivierter Versionierung überschreiben oder löschen, ist der Vorgang permanent. Siehe "Ändern Sie die Objektversionierung für einen Bucket".