S3-Buckets verwalten

StorageGRID software

NetApp
October 21, 2025

Inhalt

S3-Buckets verwalten

Erstellen eines S3-Buckets

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

Bevor Sie beginnen

- Sie sind beim Tenant Manager angemeldet mit einem"unterstützter Webbrowser" .
- Sie gehören zu einer Benutzergruppe, die über Root-Zugriff oder die Möglichkeit verfügt, alle Buckets zu verwalten."Erlaubnis" . 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 S3 Object Lock für einen Bucket aktivieren möchten, 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 über 5.000 Buckets verfügt, verfügt jeder Speicherknoten im Grid über mindestens 64 GB RAM.

> Jedes Raster kann maximal 100.000 Buckets enthalten.

Zugriff auf den Assistenten

Schritte

1. Wählen Sie im Dashboard **Buckets anzeigen** oder wählen Sie **STORAGE (S3)** > **Buckets**.
2. Wählen Sie **Bucket erstellen**.

Details eingeben

Schritte

1. Geben Sie Details zum 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-kompatibel sein. • Muss mindestens 3 und darf nicht mehr als 63 Zeichen enthalten. • Jedes Etikett muss mit einem Kleinbuchstaben oder einer Zahl beginnen und enden und darf nur Kleinbuchstaben, Zahlen und Bindestriche enthalten. • Darf in Anfragen im virtuell gehosteten Stil keine Punkte enthalten. Punkte verursachen Probleme bei der Überprüfung des Platzhalterzertifikats des Servers. Weitere Informationen finden Sie im "Amazon Web Services (AWS)-Dokumentation zu Bucket-Benennungsregeln" . **Hinweis**: Sie können den Bucket-Namen nach dem Erstellen des Buckets nicht mehr ändern.
Region	Die Region des Buckets. 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. **Hinweis**: Sie können die Region nach dem Erstellen des Buckets nicht mehr ändern.

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 bei Bedarf frühere Versionen eines Objekts abrufen. Sie müssen die Objektversionierung aktivieren, wenn der Bucket für die gitterübergreifende Replikation verwendet wird.

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

   Aktivieren Sie die S3-Objektsperre für einen 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 diesem Bucket Objekte hinzufügen, die nicht geändert werden können. Möglicherweise können Sie diese Objekte oder den Bucket selbst nicht löschen.

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

3. Wenn Sie **S3-Objektsperre aktivieren** ausgewählt haben, aktivieren Sie optional **Standardaufbewahrung** für diesen 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 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 Bucket an.

Standardaufbewahrungsmodus	Beschreibung
Führung	• Benutzer mit der `s3:BypassGovernanceRetention` Berechtigung kann die `x-amz-bypass-governance-retention: true` Anforderungsheader zum Umgehen der Aufbewahrungseinstellungen. • Diese Benutzer können eine Objektversion löschen, bevor ihr 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 entfernt werden, wenn dieses Datum erreicht ist. **Hinweis**: Ihr Grid-Administrator muss Ihnen die Verwendung des Compliance-Modus gestatten.

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

      Die **Standardaufbewahrungsfrist** gibt an, wie lange neue Objekte, die diesem 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* Aufbewahrungsdauer, die zwischen 1 Tag und 100 Jahren liegen kann, wird festgelegt, wenn der Grid-Administrator den Mandanten erstellt. Wenn Sie eine *Standard*-Aufbewahrungsdauer festlegen, darf diese den für die maximale Aufbewahrungsdauer festgelegten Wert nicht überschreiten. Bitten Sie Ihren Grid-Administrator bei Bedarf, die maximale Aufbewahrungsdauer zu verlängern oder zu verkürzen.

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

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

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

5. Wählen Sie **Bucket erstellen**.

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

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

Bucket-Details anzeigen

Sie können die Buckets in Ihrem Mandantenkonto einsehen.

Bevor Sie beginnen

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

Schritte

1. Wählen Sie im Dashboard **Buckets anzeigen** oder wählen Sie **STORAGE (S3)** > **Buckets**.

   Die Seite „Buckets“ wird angezeigt.

2. Überprüfen Sie die Übersichtstabelle für jeden Bucket.

   Sie können die Informationen je nach Bedarf nach beliebigen Spalten sortieren oder in der Liste vor- und zurückblättern.

   > Die angezeigten Werte für Objektanzahl, belegten Speicherplatz und Nutzung sind Schätzungen. Diese Schätzungen werden durch den Zeitpunkt der Aufnahme, die Netzwerkkonnektivität und den Knotenstatus beeinflusst. Wenn für Buckets die Versionierung aktiviert ist, werden gelöschte Objektversionen in die Objektzählung einbezogen.

   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

Ob die S3-Objektsperre für den Bucket aktiviert ist.

Diese Spalte wird nur angezeigt, wenn die S3-Objektsperre für das Raster aktiviert ist. Diese Spalte zeigt auch Informationen zu allen älteren konformen 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 umfasst nicht den tatsächlichen Speicherplatz, der für replizierte oder löschcodierte Kopien oder für Objektmetadaten benötigt wird.

Die Aktualisierung dieses Werts kann bis zu 10 Minuten dauern.

Verwendung

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

Der Nutzungswert basiert auf internen Schätzungen und kann in Einzelfällen überschritten werden. Beispielsweise überprüft StorageGRID das Kapazitätslimit (sofern festgelegt), wenn ein Mandant mit dem Hochladen von Objekten beginnt, und lehnt neue Aufnahmen in diesen Bucket ab, wenn der Mandant das Kapazitätslimit überschritten hat. StorageGRID berücksichtigt jedoch nicht die Größe des aktuellen Uploads, wenn es feststellt, ob das Kapazitätslimit überschritten wurde. Wenn Objekte gelöscht werden, kann es einem Mandanten vorübergehend untersagt werden, neue Objekte in diesen Bucket hochzuladen, bis die Kapazitätslimitnutzung neu berechnet wird. 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 der Bucket-Erstellung. Diese Spalte ist standardmäßig ausgeblendet.

3. Um Details zu einem bestimmten Bucket anzuzeigen, wählen Sie den Bucket-Namen aus der Tabelle aus.
   a. Sehen Sie sich 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 Kapazitätslimit-Nutzungsleiste 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**.

Achten Sie genau auf die Warnhinweise, die bei der Auswahl der einzelnen Optionen angezeigt werden. Weitere Informationen finden Sie unter:

- "Alle Objekte in einem Bucket löschen"
- "Löschen eines Buckets"(Eimer muss leer sein)

d. Zeigen Sie die Einstellungen für den Bucket in den einzelnen Registerkarten nach Bedarf an oder ändern Sie sie.
   - **S3-Konsole**: Zeigen Sie die Objekte für den Bucket an. Weitere Informationen finden Sie unter "Verwenden Sie die S3-Konsole" .
   - **Bucket-Optionen**: Optionseinstellungen anzeigen oder ändern. Einige Einstellungen, wie z. B. S3 Object Lock, können nach der Erstellung des Buckets nicht mehr geändert werden.
     - "Verwalten der Bucket-Konsistenz"
     - "Aktualisierungen der letzten Zugriffszeit"
     - "Kapazitätsgrenze"
     - "Objektversionierung"
     - "S3-Objektsperre"
     - "Standardmäßige Bucket-Aufbewahrung"
     - "Verwalten der Cross-Grid-Replikation"(sofern für den Mieter zulässig)
   - **Plattformdienste**:"Plattformdienste verwalten" (sofern für den Mieter zulässig)
   - **Bucket-Zugriff**: Optionseinstellungen anzeigen oder ändern. Sie müssen über bestimmte Zugriffsberechtigungen verfügen.
     - Konfigurieren"Cross-Origin-Ressourcenfreigabe (CORS)" sodass der Bucket und die Objekte im Bucket für Webanwendungen in anderen Domänen zugänglich sind.
     - "Benutzerzugriff steuern"für einen S3-Bucket und Objekte in diesem Bucket.

Anwenden eines ILM-Richtlinientags auf einen Bucket

Wählen Sie basierend auf Ihren Objektspeicheranforderungen ein ILM-Richtlinien-Tag aus, das auf einen Bucket angewendet werden soll.

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

Vermeiden Sie die häufige Neuzuweisung des Richtlinien-Tags eines Buckets. Andernfalls können Leistungsprobleme auftreten.

Bevor Sie beginnen

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

Schritte

1. Wählen Sie im Dashboard **Buckets anzeigen** oder wählen Sie **STORAGE (S3)** > **Buckets**.

   Die Seite „Buckets“ wird angezeigt. Sie können die Informationen je nach Bedarf nach beliebigen Spalten sortieren oder in der Liste vor- und zurückblättern.

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

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

   Die angezeigten Werte für „Objektanzahl“ und „Benutzter Speicherplatz“ sind Schätzungen. Diese Schätzungen werden durch den Zeitpunkt der Aufnahme, die Netzwerkkonnektivität und den Knotenstatus beeinflusst. Wenn für Buckets die Versionierung aktiviert ist, werden gelöschte Objektversionen in die Objektzählung einbezogen.

3. Erweitern Sie auf der Registerkarte „Bucket-Optionen“ das Akkordeon „ILM-Richtlinientag“. Dieses Akkordeon wird nur angezeigt, wenn Ihr Grid-Administrator die Verwendung benutzerdefinierter Richtlinien-Tags aktiviert hat.
4. Lesen Sie die Beschreibung jedes Richtlinien-Tags, um zu bestimmen, welches Tag auf den Bucket angewendet werden soll.

   Das Ändern des ILM-Richtlinientags für einen Bucket löst eine ILM-Neubewertung aller Objekte im Bucket aus. Wenn die neue Richtlinie Objekte für eine begrenzte Zeit aufbewahrt, werden ältere Objekte gelöscht.

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

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

   Legen Sie ILM-Richtlinien-Tags fest und ändern Sie sie nur mithilfe des Tenant Managers oder der Tenant Manager-API, wo das ILM-Richtlinien-Tag validiert wird. Ändern Sie nicht die `NTAP-SG-ILM-BUCKET-TAG` ILM-Richtlinientag mithilfe der S3 PutBucketTagging-API oder der S3 DeleteBucketTagging-API.

   Das Ändern des einem Bucket zugewiesenen Richtlinientags hat vorübergehende Auswirkungen auf die Leistung, während Objekte mithilfe der neuen ILM-Richtlinie neu ausgewertet werden.

Bucket-Richtlinie verwalten

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

Bevor Sie beginnen

- Sie sind beim Tenant Manager angemeldet mit einem"unterstützter Webbrowser" .
- Sie gehören einer Benutzergruppe an, die über die"Root-Zugriffsberechtigung" . Die Berechtigungen „Alle Buckets anzeigen“ und „Alle Buckets verwalten“ erlauben nur das Anzeigen.
- Sie haben überprüft, dass die erforderliche Anzahl an Speicherknoten und Sites verfügbar ist. Wenn an einem Standort zwei oder mehr Speicherknoten nicht verfügbar sind oder ein Standort nicht verfügbar ist, können diese Einstellungen möglicherweise nicht geändert werden.

Schritte

1. Wählen Sie **Buckets** und dann den Bucket aus, den Sie verwalten möchten.
2. Wählen Sie auf der Bucket-Detailseite **Bucket-Zugriff** > **Bucket-Richtlinie** aus.
3. Führen Sie einen der folgenden Schritte aus:
   - Geben Sie eine Bucket-Richtlinie ein, indem Sie das Kontrollkästchen **Richtlinie aktivieren** aktivieren. Geben Sie dann eine gültige Zeichenfolge im JSON-Format ein.

     Jede Bucket-Richtlinie hat eine Größenbeschränkung von 20.480 Bytes.
   - Ändern Sie eine vorhandene Richtlinie, indem Sie die Zeichenfolge bearbeiten.
   - Deaktivieren Sie eine Richtlinie, indem Sie die Option **Richtlinie aktivieren** abwählen.

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

Verwalten der Bucket-Konsistenz

Konsistenzwerte können verwendet werden, um die Verfügbarkeit von Bucket-Einstellungsänderungen anzugeben und um ein Gleichgewicht zwischen der Verfügbarkeit der Objekte innerhalb eines Buckets und der Konsistenz dieser Objekte über verschiedene Speicherknoten und Sites hinweg herzustellen. Sie können die Konsistenzwerte so ändern, dass sie von den Standardwerten abweichen, damit Clientanwendungen ihre Betriebsanforderungen erfüllen können.

Bevor Sie beginnen

- Sie sind beim Tenant Manager angemeldet mit einem"unterstützter Webbrowser" .
- Sie gehören einer Benutzergruppe an, die über die"Verwalten Sie alle Buckets oder Root-Zugriffsberechtigungen" . Diese Berechtigungen überschreiben die Berechtigungseinstellungen in Gruppen- oder Bucket-Richtlinien.

Richtlinien zur Eimerkonsistenz

Die Bucket-Konsistenz wird verwendet, um die Konsistenz für Clientanwendungen zu bestimmen, die sich auf Objekte innerhalb dieses S3-Buckets auswirken. Im Allgemeinen sollten Sie für Ihre Buckets die Konsistenz **Lesen nach neuem Schreiben** verwenden.

Konsistenz des Änderungs-Buckets

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

Konsistenz.

> Wenn Sie die Konsistenz eines Buckets ändern, wird nur für die Objekte, die nach der Änderung aufgenommen werden, garantiert, dass sie der überarbeiteten Einstellung entsprechen.

Schritte

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

   Die Bucket-Detailseite wird angezeigt.

3. Wählen Sie auf der Registerkarte **Bucket-Optionen** das ** Akkordeon aus.
4. Wählen Sie eine Konsistenz für Vorgänge aus, die an den Objekten in diesem Bucket ausgeführt werden.
   - **Alle**: Bietet das höchste Maß an Konsistenz. Alle Knoten empfangen die Daten sofort, andernfalls schlägt die Anforderung fehl.
   - **Stark global**: Garantiert Lese-nach-Schreib-Konsistenz für alle Clientanforderungen auf allen Sites.
   - **Strong-Site**: Garantiert die Lese-nach-Schreib-Konsistenz für alle Clientanforderungen innerhalb einer Site.
   - **Lesen nach neuem Schreiben** (Standard): Bietet Lese-nach-Schreib-Konsistenz für neue Objekte und letztendliche Konsistenz für Objektaktualisierungen. Bietet hohe Verfügbarkeit und Datenschutzgarantien. Für die meisten Fälle empfohlen.
   - **Verfügbar**: Bietet letztendliche Konsistenz sowohl für neue Objekte als auch für Objektaktualisierungen. Verwenden Sie es für S3-Buckets nur nach Bedarf (z. B. für einen Bucket, der Protokollwerte enthält, die selten gelesen werden, oder für HEAD- oder GET-Operationen für nicht vorhandene Schlüssel). Wird für S3 FabricPool Buckets nicht unterstützt.
5. Wählen Sie **Änderungen speichern**.

Was passiert, wenn Sie die Bucket-Einstellungen ändern?

Buckets verfügen über mehrere Einstellungen, die das Verhalten der Buckets und der Objekte in diesen Buckets beeinflussen.

Die folgenden Bucket-Einstellungen verwenden standardmäßig **starke** Konsistenz. Wenn an einem Standort zwei oder mehr Speicherknoten nicht verfügbar sind oder wenn ein Standort nicht verfügbar ist, sind Änderungen an diesen Einstellungen möglicherweise nicht möglich.

- "Löschen eines leeren Buckets im Hintergrund"
- "Letzter Zugriffszeitpunkt"
- "Bucket-Lebenszyklus"
- "Bucket-Richtlinie"
- "Bucket-Tagging"
- "Bucket-Versionierung"
- "S3-Objektsperre"
- "Bucket-Verschlüsselung"

Der Konsistenzwert für Bucket-Versionierung, S3-Objektsperre und Bucket-Verschlüsselung kann nicht auf einen Wert eingestellt werden, der nicht stark konsistent ist.

Die folgenden Bucket-Einstellungen verwenden keine starke Konsistenz und weisen eine höhere Verfügbarkeit für Änderungen auf. Es kann einige Zeit dauern, bis Änderungen an diesen Einstellungen wirksam werden.

- "Konfiguration der Plattformdienste: Benachrichtigung, Replikation oder Suchintegration"
- "CORS-Konfiguration"
- Eimerkonsistenz ändern

Wenn die beim Ändern der Bucket-Einstellungen verwendete Standardkonsistenz nicht den Anforderungen der Client-Anwendung entspricht, können Sie die Konsistenz mithilfe der `Consistency-Control` Kopfzeile für die"S3 REST API" oder mithilfe der `reducedConsistency` oder `force` Optionen in der"Mandantenverwaltungs-API" .

Aktivieren oder Deaktivieren der Aktualisierung der letzten Zugriffszeit

Wenn Grid-Administratoren die Regeln für das Information Lifecycle Management (ILM) für ein StorageGRID System erstellen, können sie optional angeben, dass der Zeitpunkt des letzten Zugriffs auf ein Objekt verwendet werden soll, um zu bestimmen, ob dieses Objekt an einen anderen Speicherort verschoben werden soll. Wenn Sie einen S3-Mandanten verwenden, können Sie solche Regeln nutzen, indem Sie Aktualisierungen 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 **Letzter Zugriffszeitpunkt** als erweiterten Filter oder als Referenzzeit verwendet. Sie können diese Anweisungen ignorieren, wenn Ihr StorageGRID System keine solche Regel enthält. Sehen"Verwenden der letzten Zugriffszeit in ILM-Regeln" für Details.

Bevor Sie beginnen

- Sie sind beim Tenant Manager angemeldet mit einem"unterstützter Webbrowser" .
- Sie gehören einer Benutzergruppe an, die über die"Verwalten Sie alle Buckets oder Root-Zugriffsberechtigungen" . Diese Berechtigungen überschreiben die Berechtigungseinstellungen in Gruppen- oder Bucket-Richtlinien.

Informationen zu diesem Vorgang

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

Um beispielsweise sicherzustellen, dass kürzlich angezeigte Objekte auf einem schnelleren Speicher 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 abgeholt wurden, sollten an einen externen Standort gebracht werden.

Standardmäßig sind Aktualisierungen der letzten Zugriffszeit deaktiviert. Wenn Ihr StorageGRID System eine ILM-Regel enthält, die die Option **Letzter Zugriffszeitpunkt** verwendet, und Sie möchten, dass diese Option auf Objekte in diesem Bucket angewendet wird, müssen Sie Aktualisierungen des letzten Zugriffszeitpunkts für die in dieser Regel angegebenen S3-Buckets aktivieren.

> ⚠ Das Aktualisieren der letzten Zugriffszeit beim Abrufen eines Objekts kann die StorageGRID Leistung verringern, insbesondere bei kleinen Objekten.

Bei Aktualisierungen der letzten Zugriffszeit kommt es zu Leistungseinbußen, da StorageGRID bei jedem Abrufen von Objekten die folgenden zusätzlichen Schritte ausführen muss:

- Aktualisieren Sie die Objekte mit neuen Zeitstempeln
- Fügen Sie die Objekte zur ILM-Warteschlange hinzu, damit sie anhand der aktuellen 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 bei aktivierter letzter Zugriffszeit	
	Letzte Zugriffszeit aktualisiert?	Objekt zur ILM-Auswertungswarteschlange hinzugefügt?	Letzte Zugriffszeit aktualisiert?	Objekt zur ILM-Auswertungswarteschlange hinzugefügt?
Anforderung zum Abrufen eines Objekts, seiner Zugriffskontrollliste oder seiner Metadaten	Nein	Nein	Ja	Ja
Anforderung zum Aktualisieren der Metadaten eines Objekts	Ja	Ja	Ja	Ja
Anfrage 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

Anfrage zum Abschließen eines mehrteiligen Uploads	Ja, für das montierte Objekt	Ja, für das montierte Objekt	Ja, für das montierte Objekt	Ja, für das montierte Objekt

Schritte

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

   Die Bucket-Detailseite wird angezeigt.
3. Wählen Sie auf der Registerkarte **Bucket-Optionen** das Akkordeon **Aktualisierungen der letzten Zugriffszeit** aus.
4. Aktivieren oder deaktivieren Sie Aktualisierungen der letzten Zugriffszeit.
5. Wählen Sie **Änderungen speichern**.

Ändern der 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 angemeldet mit einem"unterstützter Webbrowser" .
- Sie gehören einer Benutzergruppe an, die über die"Verwalten Sie alle Buckets oder Root-Zugriffsberechtigungen" . Diese Berechtigungen überschreiben die Berechtigungseinstellungen in Gruppen- oder Bucket-Richtlinien.
- Sie haben überprüft, dass die erforderliche Anzahl an Speicherknoten und Sites verfügbar ist. Wenn an einem Standort zwei oder mehr Speicherknoten nicht verfügbar sind oder ein Standort nicht verfügbar ist, können diese Einstellungen möglicherweise nicht geändert werden.

Informationen zu diesem Vorgang

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. Sie können die Versionierung für den Bucket jedoch aussetzen.

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

Weitere Informationen finden Sie unter:

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

Schritte

1. Wählen Sie im Dashboard **Buckets anzeigen** oder wählen Sie **STORAGE (S3)** > **Buckets**.

2. Wählen Sie den Bucket-Namen aus der Tabelle aus.

   Die Bucket-Detailseite wird angezeigt.

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

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

Option	Beschreibung
Aktivieren der Versionsverwaltung	Aktivieren Sie die Objektversionierung, wenn Sie jede Version jedes Objekts in diesem Bucket speichern möchten. Sie können dann bei Bedarf frühere Versionen eines Objekts abrufen. Objekte, die sich bereits im Bucket befanden, werden versioniert, wenn sie von einem Benutzer geändert werden.
Versionsverwaltung aussetzen	Unterbrechen Sie die Objektversionierung, wenn Sie nicht mehr möchten, dass neue Objektversionen erstellt werden. Sie können weiterhin alle vorhandenen Objektversionen abrufen.

5. Wählen Sie **Änderungen speichern**.

Verwenden Sie S3 Object Lock, um Objekte beizubehalten

Sie können S3 Object Lock verwenden, wenn Buckets und Objekte den gesetzlichen Aufbewahrungsanforderungen entsprechen müssen.

Ihr Grid-Administrator muss Ihnen die Berechtigung zur Verwendung bestimmter Funktionen von S3 Object Lock erteilen.

Was ist S3 Object Lock?

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

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

Ein Bucket ohne S3-Objektsperre kann nur Objekte ohne angegebene Aufbewahrungseinstellungen enthalten. Für aufgenommene Objekte werden keine Aufbewahrungseinstellungen festgelegt.

Ein Bucket mit S3 Object Lock kann Objekte mit und ohne Aufbewahrungseinstellungen enthalten, die von S3-Clientanwendungen angegeben werden. Für einige aufgenommene Objekte gelten Aufbewahrungseinstellungen.

Ein Bucket mit S3 Object Lock und konfigurierter Standardaufbewahrung kann hochgeladene Objekte mit

angegebenen Aufbewahrungseinstellungen und neue Objekte ohne Aufbewahrungseinstellungen enthalten. 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 davon unberührt.

Aufbewahrungsmodi

Die StorageGRID S3 Object Lock-Funktion unterstützt zwei Aufbewahrungsmodi, um unterschiedliche Schutzstufen auf Objekte anzuwenden. Diese Modi entsprechen den Aufbewahrungsmodi von Amazon S3.

- Im Compliance-Modus:
  - 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 entfernt werden, wenn dieses Datum erreicht ist.
- Im Governance-Modus:
  - Benutzer mit Sonderberechtigung können in Anfragen einen Bypass-Header verwenden, um bestimmte Aufbewahrungseinstellungen zu ändern.
  - Diese Benutzer können eine Objektversion löschen, bevor ihr Aufbewahrungsdatum erreicht ist.
  - Diese Benutzer können das Aufbewahrungsdatum eines Objekts erhöhen, verringern oder entfernen.

Aufbewahrungseinstellungen für Objektversionen

Wenn ein Bucket mit aktivierter S3-Objektsperre erstellt wird, können Benutzer mit der S3-Clientanwendung optional die folgenden Aufbewahrungseinstellungen für jedes dem Bucket hinzugefügte Objekt angeben:

- **Aufbewahrungsmodus**: Entweder Compliance oder Governance.
- **Aufbewahrungsdatum**: Wenn das Aufbewahrungsdatum einer Objektversion in der Zukunft liegt, kann das Objekt abgerufen, aber nicht gelöscht werden.
- **Rechtliche Sperre**: Durch Anwenden einer rechtlichen Sperre auf eine Objektversion wird dieses Objekt sofort gesperrt. Beispielsweise müssen Sie möglicherweise ein Objekt, das mit einer Untersuchung oder einem Rechtsstreit in Zusammenhang steht, rechtlich sperren. Eine rechtliche Sperre hat kein Ablaufdatum, sondern bleibt bestehen, bis sie ausdrücklich aufgehoben wird. Rechtliche Sperren sind unabhängig vom Aufbewahrungsdatum.

  > ⓘ Wenn ein Objekt einer rechtlichen Sperre unterliegt, kann niemand das Objekt löschen, unabhängig von seinem Aufbewahrungsmodus.

  Details zu den Objekteinstellungen finden Sie unter"Verwenden Sie die S3 REST API, um S3 Object Lock zu konfigurieren" .

Standardaufbewahrungseinstellung für Buckets

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

- **Standardaufbewahrungsmodus**: Entweder Compliance oder Governance.

- **Standardaufbewahrungszeitraum**: Wie lange neue Objektversionen, die diesem Bucket hinzugefügt werden, ab dem Tag ihrer Hinzufügung aufbewahrt werden sollen.

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

Sehen"Erstellen eines S3-Buckets" Und"Standardaufbewahrung für S3 Object Lock aktualisieren" .

S3 Object Lock-Aufgaben

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

Grid-Administrator

- Aktivieren Sie die globale S3-Objektsperreinstellung für das gesamte StorageGRID System.
- Stellen Sie sicher, dass die Richtlinien für das Information Lifecycle Management (ILM) *konform* sind; das heißt, sie erfüllen die"Anforderungen an Buckets mit aktivierter S3-Objektsperre" .
- Erlauben Sie einem Mandanten bei Bedarf, Compliance als Aufbewahrungsmodus zu verwenden. Andernfalls ist nur der Governance-Modus zulässig.
- Legen Sie bei Bedarf eine maximale Aufbewahrungsdauer für einen Mandanten fest.

Mandantenbenutzer

- Überprüfen Sie die Überlegungen zu Buckets und Objekten mit S3 Object Lock.
- Wenden Sie sich bei Bedarf an den Grid-Administrator, um die globale S3-Objektsperreinstellung zu aktivieren und Berechtigungen festzulegen.
- Erstellen Sie Buckets mit aktivierter S3-Objektsperre.
- Konfigurieren Sie optional die Standardaufbewahrungseinstellungen für einen Bucket:
  - Standardaufbewahrungsmodus: Governance oder Compliance, sofern vom Grid-Administrator zugelassen.
  - Standardaufbewahrungszeitraum: Muss kleiner oder gleich dem vom Grid-Administrator festgelegten maximalen Aufbewahrungszeitraum sein.
- Verwenden Sie die S3-Clientanwendung, um Objekte hinzuzufügen und optional eine objektspezifische Aufbewahrung festzulegen:
  - Aufbewahrungsmodus. Governance oder Compliance, sofern vom Grid-Administrator zugelassen.
  - Aufbewahrungsdatum: Muss kleiner oder gleich dem vom Grid-Administrator festgelegten maximalen Aufbewahrungszeitraum sein.

Anforderungen für Buckets mit aktivierter S3-Objektsperre

- Wenn die globale S3-Objektsperre-Einstellung für das StorageGRID -System aktiviert ist, können Sie den Tenant Manager, die Tenant Management API oder die S3 REST API verwenden, um Buckets mit aktivierter S3-Objektsperre zu erstellen.
- Wenn Sie S3 Object Lock verwenden möchten, müssen Sie S3 Object Lock beim Erstellen des Buckets aktivieren. Sie können S3 Object Lock nicht für einen vorhandenen Bucket aktivieren.
- Wenn S3 Object Lock für einen Bucket aktiviert ist, aktiviert StorageGRID automatisch die Versionierung für diesen Bucket. Sie können die S3-Objektsperre nicht deaktivieren oder die Versionsverwaltung für den Bucket aussetzen.

- Optional können Sie mithilfe des Tenant Managers, der Tenant Management API oder der S3 REST API einen Standardaufbewahrungsmodus und eine Standardaufbewahrungsdauer für jeden Bucket angeben. Die Standardaufbewahrungseinstellungen des Buckets gelten nur für neue Objekte, die dem Bucket hinzugefügt werden und keine eigenen Aufbewahrungseinstellungen haben. Sie können diese Standardeinstellungen überschreiben, indem Sie beim Hochladen für jede Objektversion einen Aufbewahrungsmodus und ein Aufbewahrungsdatum angeben.
- Die Bucket-Lebenszykluskonfiguration wird für Buckets mit aktivierter S3-Objektsperre unterstützt.
- Die CloudMirror-Replikation wird für Buckets mit aktivierter S3-Objektsperre nicht unterstützt.

Anforderungen für Objekte in Buckets mit aktivierter S3-Objektsperre

- Um eine Objektversion zu schützen, können Sie Standardaufbewahrungseinstellungen für den Bucket oder Aufbewahrungseinstellungen für jede Objektversion angeben. Aufbewahrungseinstellungen auf Objektebene können mithilfe der S3-Clientanwendung oder der S3-REST-API angegeben werden.
- Aufbewahrungseinstellungen gelten für einzelne Objektversionen. Eine Objektversion kann sowohl über eine Aufbewahrungsfrist als auch über eine gesetzliche Aufbewahrungsfrist verfügen, über eine der beiden Einstellungen, aber nicht über die andere, oder über keine von beiden. Durch die Angabe eines Aufbewahrungsdatums oder einer Einstellung für die rechtliche Aufbewahrung eines Objekts 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 mit aktivierter S3-Objektsperre

Jedes Objekt, das in einem Bucket mit aktivierter S3-Objektsperre gespeichert wird, durchläuft die folgenden Phasen:

1. **Objektaufnahme**

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

   - Wenn für das Objekt Aufbewahrungseinstellungen angegeben 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 vorhanden sind.
   - 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 benutzerdefinierten S3-Metadaten geschützt.

2. **Objektaufbewahrung und -löschung**

   Von jedem geschützten Objekt werden von StorageGRID mehrere Kopien für den angegebenen Aufbewahrungszeitraum 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 einer rechtlichen Sperre unterliegt, kann niemand das Objekt löschen, unabhängig von seinem Aufbewahrungsmodus.

Kann ich weiterhin ältere konforme Buckets verwalten?

Die S3 Object Lock-Funktion ersetzt die Compliance-Funktion, die in früheren StorageGRID Versionen verfügbar war. Wenn Sie konforme Buckets mit einer früheren Version von StorageGRID erstellt haben, können Sie die Einstellungen dieser Buckets weiterhin verwalten. Sie können jedoch keine neuen konformen Buckets mehr erstellen. Anweisungen hierzu finden Sie unterhttps://kb.netapp.com/Advice_and_Troubleshooting/Hybrid_Cloud_Infrastructure/StorageGRID/How_to_manage_legacy_Compliant_buckets_in_StorageGRID_11.5["NetApp Knowledge Base: So verwalten Sie ältere konforme Buckets in StorageGRID 11.5"^] .

Standardaufbewahrung für S3 Object Lock aktualisieren

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

Bevor Sie beginnen

- Sie sind beim Tenant Manager angemeldet mit einem"unterstützter Webbrowser" .
- Sie gehören einer Benutzergruppe an, die über die"Verwalten Sie alle Buckets oder Root-Zugriffsberechtigungen" . Diese Berechtigungen überschreiben die Berechtigungseinstellungen in Gruppen- oder Bucket-Richtlinien.
- S3 Object Lock ist global für Ihr StorageGRID -System aktiviert und Sie haben S3 Object Lock beim Erstellen des Buckets aktiviert. Sehen "Verwenden Sie S3 Object Lock, um Objekte beizubehalten" .

Schritte

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

   Die Bucket-Detailseite wird angezeigt.

3. Wählen Sie auf der Registerkarte **Bucket-Optionen** das Akkordeon **S3-Objektsperre** aus.
4. Aktivieren oder deaktivieren Sie optional die **Standardaufbewahrung** für diesen Bucket.

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

5. Wenn **Standardaufbewahrung** aktiviert ist, geben Sie einen **Standardaufbewahrungsmodus** für den Bucket an.

Standardaufbewahrungsmodus	Beschreibung
Führung	• Benutzer mit der `s3:BypassGovernanceRetention` Berechtigung kann die `x-amz-bypass-governance-retention: true` Anforderungsheader zum Umgehen der Aufbewahrungseinstellungen. • Diese Benutzer können eine Objektversion löschen, bevor ihr 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 entfernt werden, wenn dieses Datum erreicht ist. **Hinweis**: Ihr Grid-Administrator muss Ihnen die Verwendung des Compliance-Modus gestatten.

6. Wenn die **Standardaufbewahrung** aktiviert ist, geben Sie die **Standardaufbewahrungsdauer** für den Bucket an.

   Die **Standardaufbewahrungsfrist** gibt an, wie lange neue Objekte, die diesem 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* Aufbewahrungsdauer, die zwischen 1 Tag und 100 Jahren liegen kann, wird festgelegt, wenn der Grid-Administrator den Mandanten erstellt. Wenn Sie eine *Standard*-Aufbewahrungsdauer festlegen, darf diese den für die maximale Aufbewahrungsdauer festgelegten Wert nicht überschreiten. Bitten Sie Ihren Grid-Administrator bei Bedarf, die maximale Aufbewahrungsdauer zu verlängern oder zu verkürzen.

7. Wählen Sie **Änderungen speichern**.

Konfigurieren Sie Cross-Origin Resource Sharing (CORS)

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 angemeldet mit einem"unterstützter Webbrowser" .
- Für GET CORS-Konfigurationsanfragen gehören Sie zu einer Benutzergruppe, die über die"Berechtigung „Alle Buckets verwalten“ oder „Alle Buckets anzeigen“" . Diese Berechtigungen überschreiben die Berechtigungseinstellungen in Gruppen- oder Bucket-Richtlinien.
- Für PUT CORS-Konfigurationsanfragen gehören Sie zu einer Benutzergruppe, die über die"Berechtigung

„Alle Buckets verwalten“" . Diese Berechtigung überschreibt die Berechtigungseinstellungen in Gruppen- oder Bucket-Richtlinien.

- Der"Root-Zugriffsberechtigung" bietet Zugriff auf alle CORS-Konfigurationsanforderungen.

Informationen zu diesem Vorgang

Cross-Origin Resource Sharing (CORS) ist ein Sicherheitsmechanismus, der es Client-Webanwendungen in einer Domäne ermöglicht, auf Ressourcen in einer anderen Domäne zuzugreifen. Angenommen, Sie verwenden einen S3-Bucket namens `Images` zum Speichern von Grafiken. Durch die Konfiguration von CORS für die `Images` Bucket, können Sie die Anzeige der Bilder in diesem Bucket auf der Website zulassen `http://www.example.com` .

CORS für einen Bucket aktivieren

Schritte

1. Verwenden Sie einen Texteditor, um das erforderliche XML zu erstellen. Dieses Beispiel zeigt das XML, das zum Aktivieren von CORS für einen S3-Bucket verwendet wird. Speziell:
   - Ermöglicht jeder Domäne, GET-Anfragen an den Bucket zu senden
   - Erlaubt nur die `http://www.example.com` Domäne zum Senden von GET-, POST- und DELETE-Anfragen
   - Alle Anforderungsheader 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-Benutzerhandbuch" .

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

   Die Bucket-Detailseite wird angezeigt.

4. Wählen Sie auf der Registerkarte **Bucket-Zugriff** 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 **Löschen** aus, um von vorne zu beginnen.
2. Wählen Sie **Änderungen speichern**.

CORS-Einstellung deaktivieren

Schritte

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

Objekte im Bucket löschen

Mit dem Tenant Manager können Sie die Objekte in einem oder mehreren Buckets löschen.

Überlegungen und Anforderungen

Beachten Sie vor der Durchführung dieser Schritte Folgendes:

- Wenn Sie die Objekte in einem Bucket löschen, entfernt StorageGRID dauerhaft alle Objekte und alle Objektversionen in jedem ausgewählten Bucket von allen Knoten und Sites in Ihrem StorageGRID System. StorageGRID entfernt auch alle zugehörigen Objektmetadaten. Sie können diese Informationen nicht wiederherstellen.
- Das Löschen aller Objekte in einem Bucket kann je nach Anzahl der Objekte, Objektkopien und gleichzeitigen Vorgängen Minuten, Tage oder sogar Wochen dauern.
- Wenn ein Eimer"S3-Objektsperre aktiviert" , kann es *Jahre* lang im Status **Objekte werden gelöscht: schreibgeschützt** verbleiben.

  Ein Bucket, der S3 Object Lock verwendet, verbleibt im Status **Objekte werden gelöscht: schreibgeschützt**, bis das Aufbewahrungsdatum für alle Objekte erreicht ist und alle rechtlichen Sperren aufgehoben wurden.

- Während Objekte gelöscht werden, lautet der Status des Buckets **Objekte werden gelöscht: schreibgeschützt**. In diesem Zustand können Sie dem Bucket keine neuen Objekte hinzufügen.
- Wenn alle Objekte gelöscht wurden, bleibt der Bucket im schreibgeschützten Zustand. Sie können einen der folgenden Schritte ausführen:
  - Setzen Sie den Bucket wieder in den Schreibmodus und verwenden Sie ihn erneut für neue Objekte
  - Löschen Sie den Bucket
  - Behalten Sie den Bucket im schreibgeschützten Modus, 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 Vorgänge „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 finden Sie in"So werden versionierte S3-Objekte gelöscht" .
- Wenn Sie"Cross-Grid-Replikation" , beachten Sie Folgendes:
  - Durch die Verwendung dieser Option werden keine Objekte aus dem Bucket im anderen Raster gelöscht.
  - Wenn Sie diese Option für den Quell-Bucket auswählen, wird die Warnung **Fehler bei der Grid-übergreifenden Replikation** ausgelöst, wenn Sie dem Ziel-Bucket im anderen Grid Objekte hinzufügen. Wenn Sie nicht garantieren können, dass niemand Objekte zum Bucket auf dem anderen Raster hinzufügt,"Deaktivieren Sie die Cross-Grid-Replikation" für diesen Bucket, bevor alle Bucket-Objekte gelöscht werden.

Bevor Sie beginnen

- Sie sind beim Tenant Manager angemeldet mit einem"unterstützter Webbrowser" .
- Sie gehören einer Benutzergruppe an, die über die"Root-Zugriffsberechtigung" . Diese Berechtigung überschreibt die Berechtigungseinstellungen in Gruppen- oder Bucket-Richtlinien.

Schritte

1. Wählen Sie im Dashboard **Buckets anzeigen** oder wählen Sie **STORAGE (S3)** > **Buckets**.

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

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 **Aktionen** > **Objekte im Bucket löschen**.

   Detailseite

   a. Wählen Sie einen Bucket-Namen aus, um dessen 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 einigen Minuten:

   - Auf der Bucket-Detailseite wird ein gelbes Statusbanner angezeigt. Der Fortschrittsbalken zeigt an, wie viel Prozent der Objekte gelöscht wurden.
   - **(schreibgeschützt)** wird nach dem Bucket-Namen auf der Bucket-Detailseite angezeigt.
   - **(Objekte löschen: schreibgeschützt)** wird neben dem Namen des Buckets auf der Seite „Buckets“ angezeigt.

5. Wählen Sie bei Bedarf während der Ausführung des Vorgangs **Löschen von Objekten stoppen** aus, um den Prozess anzuhalten. Wählen Sie dann optional **Objekte im Bucket löschen** aus, um den Vorgang fortzusetzen.

   Wenn Sie „Löschen von Objekten beenden“ auswählen, wird der Bucket wieder in den Schreibmodus versetzt. Sie können jedoch 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, der Bucket bleibt jedoch schreibgeschützt.

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

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

   - Bringen Sie den Bucket zurück in den Schreibmodus und verwenden Sie ihn optional für neue Objekte erneut. Sie können **Löschen von Objekten stoppen** für einen einzelnen Bucket auswählen oder zur Buckets-Seite zurückkehren und **Aktion** > **Löschen von Objekten stoppen** für mehr als einen Bucket auswählen.

S3-Bucket löschen

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

Bevor Sie beginnen

- Sie sind beim Tenant Manager angemeldet mit einem"unterstützter Webbrowser" .
- Sie gehören einer Benutzergruppe an, die über die"Verwalten Sie alle Buckets oder Root-Zugriffsberechtigungen" . Diese Berechtigungen überschreiben die Berechtigungseinstellungen in Gruppen- oder Bucket-Richtlinien.
- Die Buckets, die Sie löschen möchten, sind leer. Wenn die Buckets, die Sie löschen möchten, *nicht* leer sind,"Objekte aus dem Bucket löschen" .

Informationen zu diesem Vorgang

Diese Anweisungen beschreiben, wie Sie einen S3-Bucket mit dem Tenant Manager löschen. Sie können S3-Buckets auch löschen, indem Sie"Mandantenverwaltungs-API" oder die"S3 REST API" .

Sie können einen S3-Bucket nicht löschen, wenn er Objekte, nicht aktuelle Objektversionen oder Löschmarkierungen enthält. Informationen zum Löschen versionierter S3-Objekte finden Sie unter"So werden Objekte gelöscht" .

Schritte

1. Wählen Sie im Dashboard **Buckets anzeigen** oder wählen Sie **STORAGE (S3)** > **Buckets**.

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

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 **Aktionen** > **Buckets löschen**.

   Detailseite

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

   b. Wählen Sie **Bucket 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, erscheint eine Fehlermeldung. Sie müssen"alle Objekte und alle Löschmarkierungen im Bucket löschen" bevor Sie den Bucket löschen können.

Verwenden Sie die S3-Konsole

Sie können die S3-Konsole verwenden, um die Objekte in einem S3-Bucket anzuzeigen und zu verwalten.

Mit der S3-Konsole können Sie:

- Objekte hochladen, herunterladen, umbenennen, kopieren, verschieben und löschen
- Objektversionen anzeigen, zurücksetzen, herunterladen und löschen
- Suche nach Objekten anhand des Präfixes
- Objekt-Tags verwalten
- Objektmetadaten anzeigen
- Ordner anzeigen, erstellen, umbenennen, kopieren, verschieben und löschen

> Die S3-Konsole bietet in den gängigsten Fällen eine verbesserte Benutzererfahrung. Es ist nicht dafür gedacht, CLI- oder API-Operationen in allen Situationen zu ersetzen.
>
> Wenn die Verwendung der S3-Konsole dazu führt, dass Vorgänge zu lange dauern (z. B. Minuten oder Stunden), sollten Sie Folgendes in Betracht ziehen:
>
> - Reduzieren der Anzahl ausgewählter Objekte
> - Verwenden nicht-grafischer Methoden (API oder CLI) für den Zugriff auf Ihre Daten

Bevor Sie beginnen

- Sie sind beim Tenant Manager angemeldet mit einem"unterstützter Webbrowser" .
- Wenn Sie Objekte verwalten möchten, gehören Sie zu einer Benutzergruppe, die über die Root-

Zugriffsberechtigung verfügt. Alternativ gehören Sie zu einer Benutzergruppe, die über die Berechtigung „Registerkarte „S3-Konsole verwenden“ und entweder die Berechtigung „Alle Buckets anzeigen“ oder „Alle Buckets verwalten“ verfügt. Sehen "Berechtigungen zur Mandantenverwaltung" .

- Für den Benutzer wurde eine S3-Gruppen- oder Bucket-Richtlinie konfiguriert. Sehen "Verwenden Sie 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 die"Anleitung 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.
4. Wählen Sie * Sign in*.
5. Die Tabelle mit den Bucket-Objekten wird angezeigt. Sie können Objekte nach Bedarf verwalten.

Weitere Informationen

- **Suche nach Präfix**: Die Präfix-Suchfunktion sucht nur nach Objekten, die relativ zum aktuellen Ordner mit einem bestimmten Wort beginnen. Die Suche umfasst keine Objekte, die das Wort an anderer Stelle enthalten. Diese Regel gilt auch für Objekte innerhalb von Ordnern. Beispielsweise eine Suche nach `folder1/folder2/somefile-` würde Objekte zurückgeben, die innerhalb der `folder1/folder2/` Ordner und beginnen Sie mit dem Wort `somefile-` .
- **Drag & Drop**: Sie können Dateien per Drag & Drop aus dem Dateimanager Ihres Computers in die S3-Konsole ziehen. Sie können jedoch keine Ordner hochladen.
- **Operationen an Ordnern**: Wenn Sie einen Ordner verschieben, kopieren oder umbenennen, werden alle Objekte im Ordner einzeln aktualisiert, was einige Zeit dauern kann.
- **Dauerhaftes Löschen bei deaktivierter Bucket-Versionierung**: Wenn Sie ein Objekt in einem Bucket mit deaktivierter Versionierung überschreiben oder löschen, ist der Vorgang dauerhaft. Sehen "Ändern der Objektversionierung für einen Bucket" .