Speicherkapazität zu einer S3-fähigen SVM hinzufügen

ONTAP 9

NetApp
November 14, 2026

This PDF was generated from https://docs.netapp.com/de-de/ontap/s3-config/create-bucket-task.html on November 14, 2026. Always check docs.netapp.com for the latest.

Inhalt

Speicherkapazität zu einer S3-fähigen SVM hinzufügen . . . 1
Einen ONTAP S3-Bucket erstellen . . . 1
S3-Buckets mit der ONTAP CLI erstellen . . . 2
S3-Buckets mit System Manager erstellen . . . 3
Die Größe des ONTAP S3-Buckets kann erhöht oder verringert werden. . . . 5
Ein ONTAP S3-Bucket auf einem gespiegelten oder nicht gespiegelten Aggregat in einer MetroCluster Konfiguration erstellen . . . 6
Prozess zum Erstellen von Buckets . . . 6
Erstellen einer ONTAP S3 Bucket-Lebenszyklusverwaltungsregel . . . 10
Lebenszyklusmanagementregeln mit der CLI verwalten . . . 11
Lebenszyklusmanagementregeln mit System Manager verwalten . . . 13
Löschen eines ONTAP S3 Bucket mit Objekten . . . 14
Löschen eines Buckets, der Objekte enthält . . . 15
Einen gelöschten Bucket wiederherstellen . . . 15
Einen ONTAP S3-Benutzer erstellen . . . 15
ONTAP S3 Benutzergruppen erstellen oder ändern, um den Zugriff auf Buckets zu steuern. . . . 17
ONTAP S3-Schlüssel neu generieren und deren Aufbewahrungsdauer ändern . . . 18
Einen S3-Zugriffsschlüssel neu generieren . . . 18
Generieren Sie einen zweiten S3-Zugriffsschlüssel . . . 19
S3-Zugriffsschlüssel anzeigen . . . 20
Einen S3-Zugriffsschlüssel entfernen . . . 20

Speicherkapazität zu einer S3-fähigen SVM hinzufügen

Einen ONTAP S3-Bucket erstellen

S3-Objekte werden in *Buckets* gespeichert. Sie sind nicht als Dateien in einem Verzeichnis innerhalb anderer Verzeichnisse verschachtelt.

Bevor Sie beginnen

Es muss bereits eine Storage-VM mit einem S3-Server existieren.

Über diese Aufgabe

- Ab ONTAP 9.14.1 ist die automatische Größenanpassung auf S3 FlexGroup Volumes aktiviert, wenn Buckets darauf erstellt werden. Dadurch wird eine übermäßige Kapazitätszuweisung während der Bucket-Erstellung auf bestehenden und neuen FlexGroup Volumes vermieden. FlexGroup Volumes werden anhand der folgenden Richtlinien auf die minimal erforderliche Größe skaliert. Die minimal erforderliche Größe entspricht der Gesamtgröße aller S3 Buckets in einem FlexGroup Volume.
  - Ab ONTAP 9.14.1 wird, wenn ein S3-FlexGroup-Volume im Rahmen der Erstellung eines neuen Buckets angelegt wird, das FlexGroup-Volume mit der minimal erforderlichen Größe erstellt.
  - Wurde ein S3 FlexGroup Volume vor ONTAP 9.14.1 erstellt, wird das erste Bucket, das nach ONTAP 9.14.1 erstellt oder gelöscht wird, das FlexGroup Volume auf die minimal erforderliche Größe anpassen.
  - Wenn ein S3 FlexGroup Volume vor ONTAP 9.14.1 erstellt wurde und bereits die erforderliche Mindestgröße hatte, bleibt bei der Erstellung oder Löschung eines Buckets nach ONTAP 9.14.1 die Größe des S3 FlexGroup Volumes erhalten.
- Speicherdienststufen sind vordefinierte adaptive Quality of Service (QoS)-Richtliniengruppen mit den Standardstufen *value*, *performance* und *extreme*. Statt einer der Standard-Speicherdienststufen kann auch eine benutzerdefinierte QoS-Richtliniengruppe definiert und auf einen Bucket angewendet werden. Weitere Informationen zu Speicherdienstdefinitionen finden sich unter "Definitionen von Speicherdiensten". Weitere Informationen zum Leistungsmanagement finden sich unter "Leistungsmanagement". Ab ONTAP 9.8 ist QoS bei der Speicherbereitstellung standardmäßig aktiviert. QoS kann während des Bereitstellungsprozesses oder zu einem späteren Zeitpunkt deaktiviert oder eine benutzerdefinierte QoS-Richtlinie ausgewählt werden.
- Wenn Sie lokales Capacity Tiering konfigurieren, werden Buckets und Benutzer in einer Datenspeicher-VM erstellt, nicht in der Systemspeicher-VM, in der sich der S3-Server befindet.
- Für den Remote-Clientzugriff müssen Buckets in einer S3-fähigen Storage-VM konfiguriert werden. Wenn ein Bucket in einer Storage-VM erstellt wird, die nicht S3-fähig ist, steht er nur für lokales Tiering zur Verfügung.
- Ab ONTAP 9.14.1 ist es möglich, "Erstellen eines Buckets auf einem gespiegelten oder nicht gespiegelten Aggregat in einer MetroCluster Konfiguration".
- Für die CLI stehen beim Erstellen eines Buckets zwei Bereitstellungsoptionen zur Verfügung:
  - ONTAP wählt die zugrunde liegenden Aggregate und FlexGroup-Komponenten aus (Standardeinstellung)
    - ONTAP erstellt und konfiguriert ein FlexGroup Volume für den ersten Bucket, indem die Aggregate automatisch ausgewählt werden. Dabei wird automatisch das höchste für Ihre Plattform verfügbare Servicelevel ausgewählt, oder das Speicherservicelevel kann angegeben werden. Alle weiteren

Buckets, die später in der Speicher-VM hinzugefügt werden, verwenden dasselbe zugrunde liegende FlexGroup Volume.

- Alternativ kann angegeben werden, ob der Bucket für Tiering verwendet wird, wobei ONTAP versucht, kostengünstige Medien mit optimaler Leistung für die gestaffelten Daten auszuwählen.

◦ Sie wählen die zugrunde liegenden Aggregate und FlexGroup Komponenten aus (erfordert Befehlsoptionen mit erweiterten Berechtigungen): Sie haben die Möglichkeit, die Aggregate, auf denen der Bucket und das zugehörige FlexGroup Volume erstellt werden müssen, manuell auszuwählen und anschließend die Anzahl der Bestandteile auf jedem Aggregat anzugeben. Beim Hinzufügen weiterer Buckets:

- Wenn Sie Aggregate und Bestandteile für einen neuen Bucket angeben, wird für den neuen Bucket eine neue FlexGroup erstellt.
- Wenn Sie für einen neuen Bucket keine Aggregate und Bestandteile angeben, wird der neue Bucket einem bestehenden FlexGroup hinzugefügt, jedoch nur, wenn die `retention-mode` Einstellung mit der `retention-mode` Einstellung bestehender Buckets und dem FlexGroup-Typ (`compliance`, `non-snaplock`, `enterprise` übereinstimmt. Weitere Informationen finden sich unter FlexGroup Volumenmanagement.

  Wenn Sie beim Erstellen eines Buckets Aggregate und Bestandteile angeben, werden keine QoS-Richtliniengruppen, weder Standard noch benutzerdefinierte, angewendet. Dies ist später mit dem `vserver object-store-server bucket modify` Befehl möglich.

Weitere Informationen zu `vserver object-store-server bucket modify` finden sich in der "ONTAP-Befehlsreferenz".

Hinweis: Wenn Sie Buckets von Cloud Volumes ONTAP bereitstellen, sollte die CLI-Prozedur verwendet werden. Es wird dringend empfohlen, die zugrunde liegenden Aggregate manuell auszuwählen, um sicherzustellen, dass nur ein Knoten verwendet wird. Die Verwendung von Aggregaten beider Knoten kann die Leistung beeinträchtigen, da sich die Knoten in geografisch getrennten Verfügbarkeitszonen befinden und daher anfällig für Latenzprobleme sind.

S3-Buckets mit der ONTAP CLI erstellen

1. Wenn Sie Aggregate und FlexGroup Komponenten selbst auswählen, ist die Berechtigungsstufe „Erweitert“ erforderlich (ansonsten ist die Administratorberechtigung ausreichend): `set -privilege advanced`
2. Einen Bucket erstellen:

   ```
   vserver object-store-server bucket create -vserver <svm_name> -bucket
   <bucket_name> -size [integer{KB|MB|GB|TB|PB}] [-comment text]
   [additional_options]
   ```

   Ab ONTAP 9.20.1 verwendet ONTAP beim Erstellen eines Buckets die auf dem S3-Server konfigurierte Standard-Bucketgröße, wenn die `-size` Option nicht angegeben wird. Wenn kein Standard konfiguriert ist, verwendet ONTAP die minimale Bucketgröße der Plattform. Dieses Verhalten gilt auch für Buckets, die ohne explizite Größenangabe über die S3-API oder ONTAP REST API erstellt werden.

   Der Name der Storage-VM kann entweder eine Datenspeicher-VM oder `Cluster` (der Name der Systemspeicher-VM) sein, wenn lokales Tiering konfiguriert wird.

   Wenn ONTAP einen Bucket basierend auf Leistung oder Nutzung erstellen soll, kann eine der folgenden Optionen verwendet werden:

   ◦ Service Level

Die `-storage-service-level` Option ist mit einem der folgenden Werte anzugeben: `value`, `performance` oder `extreme`.

- Tiering

  Die Option `-used-as-capacity-tier true` einschließen.

  Wenn Sie die Aggregate angeben möchten, auf denen das zugrunde liegende FlexGroup Volume erstellt werden soll, stehen die folgenden Optionen zur Verfügung:

- Der `-aggr-list`Parameter gibt die Liste der Aggregate an, die für FlexGroup Volume-Bestandteile verwendet werden.

  Jeder Eintrag in der Liste erstellt einen Bestandteil auf dem angegebenen Aggregat. Ein Aggregat kann mehrfach angegeben werden, sodass mehrere Bestandteile auf dem Aggregat erstellt werden.

Für eine gleichbleibende Leistung über das FlexGroup Volume hinweg müssen alle Aggregate den gleichen Festplattentyp und die gleiche RAID-Gruppenkonfiguration verwenden.

- Der `-aggr-list-multiplier`Parameter gibt an, wie oft die mit dem `-aggr-list`Parameter aufgeführten Aggregate beim Erstellen eines FlexGroup Volume durchlaufen werden.

  Der Standardwert des `-aggr-list-multiplier` Parameters ist 4.

3. Bei Bedarf kann eine QoS-Richtliniengruppe hinzugefügt werden:

   ```
   vserver object-store-server bucket modify -bucket bucket_name -qos-policy
   -group qos_policy_group
   ```

4. Bucket-Erstellung überprüfen:

   ```
   vserver object-store-server bucket show [-instance]
   ```

Beispiel

Das folgende Beispiel erstellt einen Bucket für Storage-VM `vs1` mit der Größe `1TB` und gibt das Aggregat an:

Weitere Informationen zu den in diesem Verfahren beschriebenen Befehlen befinden sich in der "ONTAP-Befehlsreferenz".

```
cluster-1::*> vserver object-store-server bucket create -vserver
svm1.example.com -bucket testbucket -aggr-list aggr1 -size 1TB
```

S3-Buckets mit System Manager erstellen

1. Einen neuen Bucket auf einer S3-fähigen Storage-VM hinzufügen.
   a. Klicken Sie auf **Speicher > Buckets** und anschließend auf **Hinzufügen**.
   b. Einen Namen eingeben, die Speicher-VM auswählen und eine Größe angeben.
      - Wenn Sie jetzt auf **Speichern** klicken, wird ein Bucket mit diesen Standardeinstellungen erstellt:
        - Benutzern wird kein Zugriff auf den Bucket gewährt, es sei denn, es sind bereits Gruppenrichtlinien aktiv.

Sie sollten den S3 Root-Benutzer nicht zur Verwaltung des ONTAP Objektspeichers und zur Freigabe seiner Berechtigungen verwenden, da dieser uneingeschränkten Zugriff auf den Objektspeicher hat. Stattdessen empfiehlt es sich, einen Benutzer oder eine Gruppe mit administrativen Berechtigungen zu erstellen, die Sie zuweisen.

- Ein Servicequalitätsniveau (Leistung), das für Ihr System das höchstmögliche verfügbare ist.
- Klicken Sie auf **Speichern**, um einen Bucket mit diesen Standardwerten zu erstellen.

Zusätzliche Berechtigungen und Einschränkungen konfigurieren

Sie können auf **Weitere Optionen** klicken, um Einstellungen für die Objektsperrung, Benutzerberechtigungen und Leistungsstufe bei der Konfiguration des Buckets festzulegen oder diese Einstellungen später ändern.

Wenn Sie den S3 Objektspeicher für FabricPool Tiering verwenden möchten, empfiehlt es sich, die Option **Für Tiering verwenden** (kostengünstige Medien mit optimaler Leistung für die gestaffelten Daten) statt eines Leistungs-Servicelevels auszuwählen.

Zur Aktivierung der Versionierung Ihrer Objekte für eine spätere Wiederherstellung dient **Enable Versioning**. Die Versionierung ist standardmäßig aktiviert, wenn Sie die Objektsperre für den Bucket aktivieren. Nachdem die Versionierung für einen Bucket aktiviert wurde, kann sie nicht mehr deaktiviert werden.

Die Versionierung kann aufgehoben werden, indem das Kontrollkästchen **Enable Versioning** in System Manager deaktiviert oder CLI verwendet wird.

```
vserver object-store-server bucket modify -vserver <svm_name> -bucket
<bucket_name> -versioning-state suspended
```

Wenn die Versionierung für einen Bucket aktiviert ist, kann die Aufbewahrungsdauer der Object Lock für bestimmte Versionen eines Objekts mithilfe von S3-Clients festgelegt werden. Das Sperren einer bestimmten Version eines Objekts verhindert nicht das Löschen anderer Versionen dieses Objekts.

Weitere Informationen zur Objektversionierung enthält "Verwendung der Versionierung in S3-Buckets für Amazon".

Ab Version 9.14.1 wird die Objektsperrung für S3-Buckets unterstützt. Die S3-Objektsperrung muss beim Erstellen eines Buckets aktiviert werden. Die Objektsperrung kann nicht für bereits vorhandene Buckets aktiviert werden. Die Objektsperrung kann nur in nativen S3-Anwendungsfällen verwendet werden. Multiprotokoll-NAS-Volumes, die für die Verwendung des S3-Protokolls konfiguriert sind, sollten SnapLock verwenden, um Daten im WORM-Speicher zu speichern. Die S3-Objektsperrung erfordert eine Standardlizenz für SnapLock. Diese Lizenz ist mit "ONTAP One" enthalten.

Vor ONTAP One war die SnapLock-Lizenz im Security and Compliance Bundle enthalten. Das Security and Compliance Bundle wird nicht mehr angeboten, ist aber weiterhin gültig. Obwohl es derzeit nicht erforderlich ist, können bestehende Kunden sich dafür entscheiden, "Upgrade auf ONTAP One". Wenn die Objektsperre für einen Bucket aktiviert wird, sollte "Es sollte überprüft werden, ob eine SnapLock-Lizenz installiert ist.". Wenn keine SnapLock-Lizenz installiert ist, muss "installieren" sie vor der Aktivierung der Objektsperre installiert werden.

Nachdem Sie überprüft haben, dass die SnapLock-Lizenz installiert ist, kann zum Schutz von Objekten in Ihrem Bucket vor dem Löschen oder Überschreiben **Objektsperre aktivieren** ausgewählt werden. Die Sperrung kann entweder für alle oder für bestimmte Versionen von Objekten aktiviert werden, und nur, wenn

die SnapLock-Compliance-Uhr für die Clusterknoten initialisiert ist. Dabei sind folgende Schritte zu beachten:

1. Wenn die SnapLock Compliance-Uhr auf keinem Knoten des Clusters initialisiert ist, erscheint die Schaltfläche **SnapLock Compliance-Uhr initialisieren**. Mit **SnapLock Compliance-Uhr initialisieren** wird die SnapLock Compliance-Uhr auf den Cluster-Knoten initialisiert.
2. **Governance**-Modus auswählen, um eine zeitbasierte Sperre zu aktivieren, die *Write once, read many (WORM)*-Berechtigungen für die Objekte ermöglicht. Auch im *Governance*-Modus können die Objekte von Administratorbenutzern mit spezifischen Berechtigungen gelöscht werden.
3. **Compliance**-Modus auswählen, um strengere Regeln für das Löschen und Aktualisieren von Objekten festzulegen. In diesem Modus der Objektsperrung können die Objekte erst nach Ablauf der festgelegten Aufbewahrungsfrist ablaufen. Sofern keine Aufbewahrungsfrist angegeben ist, bleiben die Objekte unbegrenzt gesperrt.
4. Geben Sie die Aufbewahrungsdauer für die Sperre in Tagen oder Jahren an, wenn die Sperre für einen bestimmten Zeitraum wirksam sein soll.

> Sperren sind sowohl für versionierte als auch für nicht versionierte S3-Buckets möglich. Objektsperren sind für NAS-Objekte nicht möglich.

Sie können die Schutz- und Berechtigungseinstellungen sowie die Performance-Service-Stufe für den Bucket konfigurieren.

> Benutzer und Gruppen müssen bereits erstellt sein, bevor die Berechtigungen konfiguriert werden.

Weitere Informationen sind unter "Spiegel für neuen Bucket erstellen" zu finden.

Zugriff auf den Bucket überprüfen

Bei S3-Clientanwendungen (egal ob ONTAP S3 oder eine externe Drittanbieteranwendung) lässt sich der Zugriff auf den neu erstellten Bucket durch Eingabe des Folgenden überprüfen:

- Das S3-Server-CA-Zertifikat.
- Der Zugriffsschlüssel und der geheime Schlüssel des Benutzers.
- Der FQDN-Name des S3-Servers und der Bucket-Name.

Die Größe des ONTAP S3-Buckets kann erhöht oder verringert werden.

Bei Bedarf kann die Größe eines vorhandenen Buckets vergrößert oder verkleinert werden.

Schritte

Der System Manager oder die ONTAP CLI kann zur Verwaltung der Bucket-Größe verwendet werden.

System Manager

1. **Storage > Buckets** auswählen und den Bucket suchen, der geändert werden soll.
2. Klicken Sie ⋮ neben den Bucket-Namen und wählen Sie **Bearbeiten**.

3. Im Fenster **Bucket bearbeiten** die Kapazität des Buckets ändern.
4. **Speichern**.

CLI

1. Bucket-Kapazität ändern:

```
vserver object-store-server bucket modify -vserver <SVM_name>
-bucket <bucket_name> -size {<integer>[KB|MB|GB|TB|PB]}
```

Ein ONTAP S3-Bucket auf einem gespiegelten oder nicht gespiegelten Aggregat in einer MetroCluster Konfiguration erstellen

Ab ONTAP 9.14.1 ist es möglich, einen Bucket auf einem gespiegelten oder nicht gespiegelten Aggregat in MetroCluster FC- und IP-Konfigurationen bereitzustellen.

Über diese Aufgabe

- Standardmäßig werden Buckets auf gespiegelten Aggregaten bereitgestellt.
- Die gleichen Bereitstellungsrichtlinien, die in "Einen Bucket erstellen" beschrieben wurden, gelten auch für die Erstellung eines Buckets in einer MetroCluster Umgebung.
- Ab ONTAP 9.20.1 werden in MetroCluster Umgebungen die folgenden S3-Objektspeicherfunktionen unterstützt:
  - SnapMirror S3
  - S3 Bucket Lebenszyklusmanagement
- Die folgenden S3-Objektspeicherfunktionen werden in MetroCluster Umgebungen **nicht** unterstützt:
  - S3 Objektsperre im **Compliance** Modus

    Die S3 Objektsperre im **Governance** Modus wird unterstützt.

  - Lokales FabricPool Tiering

Bevor Sie beginnen

Eine SVM mit einem S3-Server muss bereits vorhanden sein.

Prozess zum Erstellen von Buckets

CLI

1. Wenn Sie Aggregate und FlexGroup Komponenten selbst auswählen, ist die Berechtigungsstufe „Erweitert“ erforderlich (ansonsten ist die Administratorberechtigung ausreichend): `set -privilege advanced`
2. Einen Bucket erstellen:

```
vserver object-store-server bucket create -vserver <svm_name> -bucket
```

`<bucket_name> [-size integer[KB|MB|GB|TB|PB]] [-use-mirrored-aggregates true/false]`

Die `-use-mirrored-aggregates` Option wird auf `true` oder `false` gesetzt, abhängig davon, ob ein gespiegeltes oder ein nicht gespiegeltes Aggregat verwendet werden soll.

Standardmäßig ist die `-use-mirrored-aggregates` Option auf `true` eingestellt.

- Der SVM-Name muss eine Daten-SVM sein.
- Wenn Sie keine Optionen angeben, erstellt ONTAP einen 800GB-Bucket, wobei die Serviceebene auf die höchste für Ihr System verfügbare Ebene eingestellt ist.
- Wenn ONTAP einen Bucket basierend auf Leistung oder Nutzung erstellen soll, kann eine der folgenden Optionen verwendet werden:
  - Service Level

    Die `-storage-service-level` Option ist mit einem der folgenden Werte anzugeben: `value`, `performance` oder `extreme`.

  - Tiering

    Die Option `-used-as-capacity-tier true` einschließen.
- Wenn Sie die Aggregate angeben möchten, auf denen das zugrunde liegende FlexGroup Volume erstellt werden soll, stehen die folgenden Optionen zur Verfügung:
  - Der `-aggr-list`Parameter gibt die Liste der Aggregate an, die für FlexGroup Volume-Bestandteile verwendet werden.

    Jeder Eintrag in der Liste erstellt einen Bestandteil auf dem angegebenen Aggregat. Ein Aggregat kann mehrfach angegeben werden, sodass mehrere Bestandteile auf dem Aggregat erstellt werden.

Für eine gleichbleibende Leistung über das FlexGroup Volume hinweg müssen alle Aggregate den gleichen Festplattentyp und die gleiche RAID-Gruppenkonfiguration verwenden.

- Der `-aggr-list-multiplier`Parameter gibt an, wie oft die mit dem `-aggr-list`Parameter aufgeführten Aggregate beim Erstellen eines FlexGroup Volume durchlaufen werden.

  Der Standardwert des `-aggr-list-multiplier` Parameters ist 4.

3. Bei Bedarf kann eine QoS-Richtliniengruppe hinzugefügt werden:

   `vserver object-store-server bucket modify -bucket` *`bucket_name`* `-qos-policy -group` *`qos_policy_group`*

4. Bucket-Erstellung überprüfen:

   `vserver object-store-server bucket show [-instance]`

Beispiel

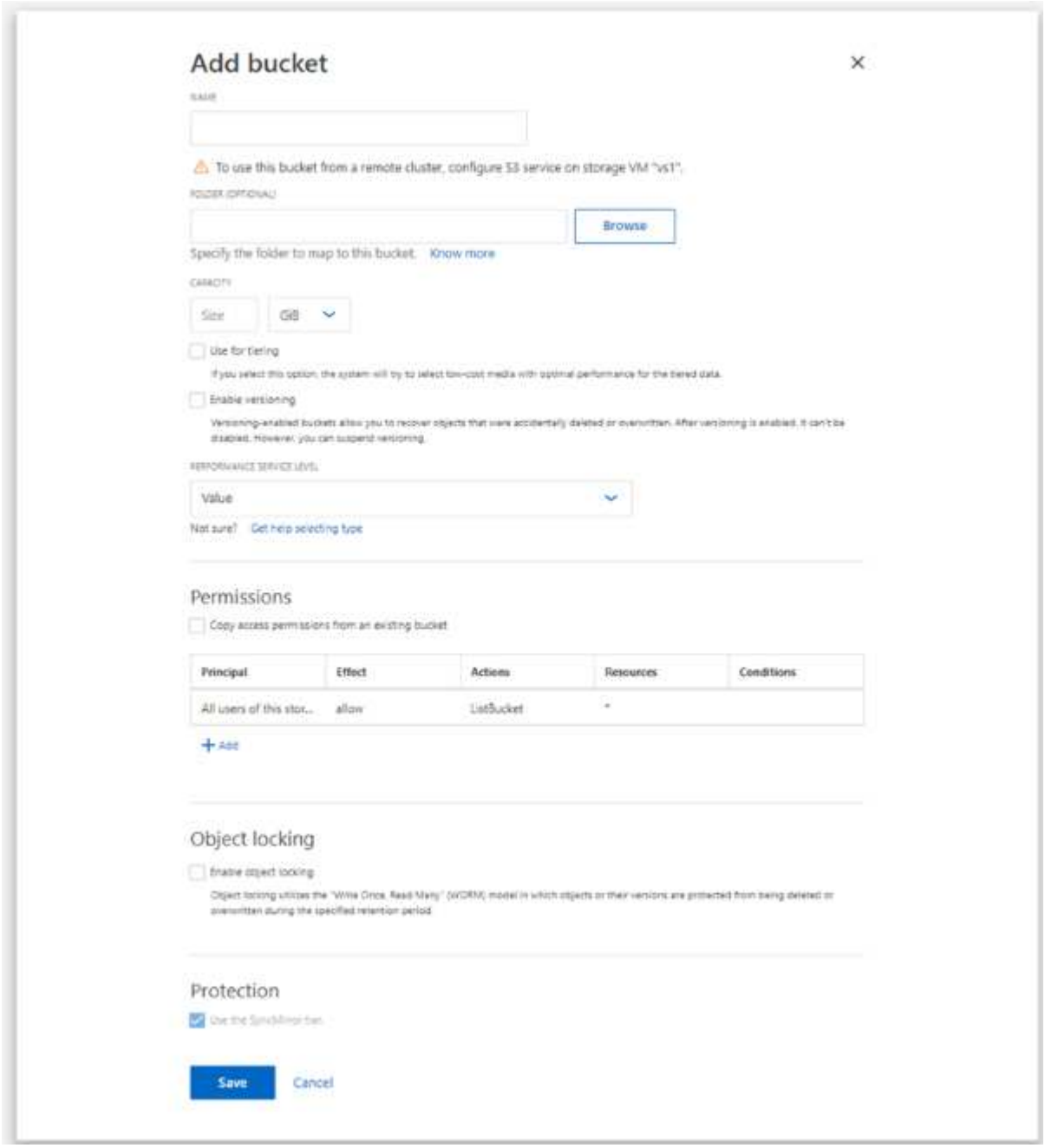
Das folgende Beispiel erstellt einen Bucket für SVM vs1 mit einer Größe von 1 TB auf einem gespiegelten Aggregat:

```
cluster-1::*> vserver object-store-server bucket create -vserver
svm1.example.com -bucket testbucket  -size 1TB -use-mirrored-aggregates
true
```

System Manager

1. Einen neuen Bucket auf einer S3-fähigen Storage-VM hinzufügen.
   a. Klicken Sie auf **Speicher > Buckets** und anschließend auf **Hinzufügen**.
   b. Einen Namen eingeben, die Speicher-VM auswählen und eine Größe angeben.

      Standardmäßig wird der Bucket auf einem gespiegelten Aggregat bereitgestellt. Wenn ein Bucket auf einem nicht gespiegelten Aggregat erstellt werden soll, sind unter **Weitere Optionen** das Kontrollkästchen **SyncMirror-Ebene verwenden** unter **Schutz** zu deaktivieren, wie in der folgenden Abbildung gezeigt:



- Wenn Sie jetzt auf **Speichern** klicken, wird ein Bucket mit diesen Standardeinstellungen erstellt:
  - Benutzern wird kein Zugriff auf den Bucket gewährt, es sei denn, es sind bereits Gruppenrichtlinien aktiv.

    Sie sollten den S3 Root-Benutzer nicht zur Verwaltung des ONTAP Objektspeichers und zur Freigabe seiner Berechtigungen verwenden, da dieser uneingeschränkten Zugriff auf den Objektspeicher hat. Stattdessen empfiehlt es sich, einen Benutzer oder eine Gruppe mit administrativen Berechtigungen zu erstellen, die Sie zuweisen.

  - Ein Servicequalitätsniveau (Leistung), das für Ihr System das höchstmögliche verfügbare ist.

- Sie können auf **Weitere Optionen** klicken, um Benutzerberechtigungen und Leistungsniveau beim Konfigurieren des Buckets festzulegen, oder diese Einstellungen später ändern.
  - Benutzer und Gruppen müssen bereits erstellt worden sein, bevor über **Weitere Optionen** deren Berechtigungen konfiguriert werden können.
  - Wenn Sie den S3 Objektspeicher für FabricPool Tiering verwenden möchten, empfiehlt es sich, die Option **Für Tiering verwenden** (kostengünstige Medien mit optimaler Leistung für die gestaffelten Daten) statt eines Leistungs-Servicelevels auszuwählen.

2. In S3-Client-Apps (einem anderen ONTAP-System oder einer externen Drittanbieter-App) kann der Zugriff auf den neuen Bucket durch Eingabe des Folgenden überprüft werden:
   - Das S3-Server-CA-Zertifikat.
   - Der Zugriffsschlüssel und der geheime Schlüssel des Benutzers.
   - Der FQDN-Name des S3-Servers und der Bucket-Name.

Erstellen einer ONTAP S3 Bucket-Lebenszyklusverwaltungsregel

Ab ONTAP 9.13.1 können Lebenszyklusmanagementregeln erstellt werden, um die Lebenszyklen von Objekten in Ihren S3-Buckets zu verwalten. Löschregeln für bestimmte Objekte in einem Bucket lassen sich definieren, und durch diese Regeln können diese Bucket-Objekte ablaufen. So werden Aufbewahrungsanforderungen erfüllt und der gesamte S3-Objektspeicher effizient verwaltet.

Wenn die Objektsperrung für Ihre Bucket-Objekte aktiviert ist, werden die Lebenszyklusverwaltungsregeln für den Objektablauf nicht auf gesperrte Objekte angewendet. Informationen zur Objektsperrung finden sich unter "Einen Bucket erstellen".

Bevor Sie beginnen

- Eine S3-fähige SVM mit einem S3-Server und einem Bucket muss bereits existieren. Siehe "Eine SVM für S3 erstellen" für weitere Informationen.
- Ab ONTAP 9.20.1 werden Regeln für das Bucket-Lifecycle-Management für native S3-Buckets in einer MetroCluster Umgebung unterstützt.
- S3 in Multiprotokoll-NAS-Volumes unterstützt keine Bucket-Lebenszyklusverwaltungsregeln.

Über diese Aufgabe

Beim Erstellen Ihrer Lebenszyklusverwaltungsregeln können Sie die folgenden Löschaktionen auf Ihre Bucket-Objekte anwenden:

- Löschen aktueller Versionen, diese Aktion führt zum Ablauf von Objekten, die durch die Regel identifiziert werden. Wenn die Versionierung für den Bucket aktiviert ist, macht S3 alle abgelaufenen Objekte nicht mehr verfügbar. Wenn die Versionierung nicht aktiviert ist, löscht diese Regel die Objekte dauerhaft. Die CLI-Aktion ist `Expiration`.
- Löschung nicht aktueller Versionen – Diese Aktion legt fest, wann S3 nicht aktuelle Objekte endgültig entfernen kann. Die CLI-Aktion ist `NoncurrentVersionExpiration`.

Eine nicht aktuelle Version basiert auf dem Erstellungs- oder Änderungszeitpunkt der aktuellen Version. Die verzögerte Entfernung nicht aktueller Objekte kann hilfreich sein,

wenn ein Objekt versehentlich gelöscht oder überschrieben wird. Beispielsweise kann eine Ablaufregel so konfiguriert werden, dass nicht aktuelle Versionen fünf Tage nach dem Wechsel in den nicht aktuellen Status gelöscht werden. Angenommen, am 1.1.2014 um 10:30 Uhr UTC wird ein Objekt namens `photo.gif` (Versions-ID `111111`) erstellt. Am 2.1.2014 um 11:30 Uhr UTC wird `photo.gif` (Versions-ID `111111`) versehentlich gelöscht, wodurch eine Löschmarkierung mit einer neuen Versions-ID (wie Versions-ID `4857693`) erstellt wird. Nun stehen fünf Tage zur Verfügung, um die ursprüngliche Version von `photo.gif` (Versions-ID `111111`) wiederherzustellen, bevor die Löschung endgültig ist. Am 8.1.2014 um 00:00 Uhr UTC wird die Ablaufregel für die Löschung ausgeführt und löscht `photo.gif` (Versions-ID `111111`) endgültig, fünf Tage nachdem sie zu einer nicht aktuellen Version wurde.

- Löschen abgelaufener Löschmarkierungen - Diese Aktion löscht abgelaufene Löschmarkierungen von Objekten. In Buckets mit aktivierter Versionierung werden Objekte mit einer Löschmarkierung zu den aktuellen Versionen der Objekte. Die Objekte werden nicht gelöscht, und es kann keine Aktion an ihnen durchgeführt werden. Diese Objekte sind abgelaufen, wenn keine aktuellen Versionen mehr mit ihnen verknüpft sind. Die CLI-Aktion ist `Expiration`.
- Löschen unvollständiger Multipart-Uploads – Diese Aktion legt eine maximale Zeit (in Tagen) fest, die Multipart-Uploads im Status „laufend“ verbleiben dürfen. Danach werden sie gelöscht. Die CLI-Aktion ist `AbortIncompleteMultipartUpload`.

Die Vorgehensweise hängt von der verwendeten Schnittstelle ab. Mit ONTAP 9.13.1 ist die Nutzung der CLI erforderlich. Ab ONTAP 9.14.1 ist auch die Verwendung von System Manager möglich.

Lebenszyklusmanagementregeln mit der CLI verwalten

Ab ONTAP 9.13.1 kann die ONTAP CLI verwendet werden, um Lebenszyklusverwaltungsregeln zu erstellen, mit denen Objekte in S3-Buckets ablaufen.

Bevor Sie beginnen

Für die CLI sind beim Erstellen einer Bucket-Lebenszyklusverwaltungsregel die erforderlichen Felder für jeden Ablaufaktionstyp zu definieren. Diese Felder können nach der erstmaligen Erstellung geändert werden. Die folgende Tabelle zeigt die eindeutigen Felder für jeden Aktionstyp.

Aktionstyp	Einzigartige Felder
NonCurrentVersionExpiration	• `-non-curr-days` - Anzahl der Tage, nach denen nicht mehr aktuelle Versionen gelöscht werden • `-new-non-curr-versions` - Anzahl der zuletzt beibehaltenen nicht aktuellen Versionen
Ablauf	• `-obj-age-days` - Anzahl der Tage seit der Erstellung, nach denen die aktuelle Version der Objekte gelöscht werden kann • `-obj-exp-date` - Genaues Datum, an dem die Objekte ablaufen sollen • `-expired-obj-del-markers` - Objektlöschmarkierungen bereinigen
AbortIncompleteMultipartUpload	• `-after-initiation-days` - Anzahl der Tage nach der Initiierung, nach denen der Upload abgebrochen werden kann

Damit die Bucket-Lebenszyklusverwaltungsregel nur auf eine bestimmte Teilmenge von Objekten angewendet wird, müssen Administratoren beim Erstellen der Regel jeden Filter festlegen. Wenn diese Filter beim Erstellen

der Regel nicht festgelegt werden, wird die Regel auf alle Objekte im Bucket angewendet.

Alle Filter können nach ihrer Erstellung geändert werden, *mit Ausnahme* der folgenden:

- `-prefix`
- `-tags`
- `-obj-size-greater-than`
- `-obj-size-less-than`

Schritte

1. Verwenden Sie den `vserver object-store-server bucket lifecycle-management-rule create` Befehl mit den erforderlichen Feldern für Ihren Ablaufaktionstyp, um Ihre Bucket-Lebenszyklusverwaltungsregel zu erstellen.

Beispiel

Der folgende Befehl erstellt eine NonCurrentVersionExpiration Bucket-Lebenszyklusverwaltungsregel:

```
vserver object-store-server bucket lifecycle-management-rule create
-vserver <svm_name> -bucket <bucket_name> -rule-id <rule_name> -action
NonCurrentVersionExpiration -index <lifecycle_rule_index_integer> -is
-enabled {true|false} -prefix <object_name> -tags <text> -obj-size-greater
-than {<integer>[KB|MB|GB|TB|PB]} -obj-size-less-than
{<integer>[KB|MB|GB|TB|PB]} -new-non-curr-versions <integer> -non-curr
-days <integer>
```

Beispiel

Der folgende Befehl erstellt eine Lebenszyklusverwaltungsregel für den Expiration-Bucket:

```
vserver object-store-server bucket lifecycle-management-rule create
-vserver <svm_name> -bucket <bucket_name> -rule-id <rule_name> -action
Expiration -index <lifecycle_rule_index_integer> -is-enabled {true|false}
-prefix <object_name> -tags <text> -obj-size-greater-than
{<integer>[KB|MB|GB|TB|PB]} -obj-size-less-than
{<integer>[KB|MB|GB|TB|PB]} -obj-age-days <integer> -obj-exp-date
<"MM/DD/YYYY HH:MM:SS"> -expired-obj-del-marker {true|false}
```

Beispiel

Der folgende Befehl erstellt eine AbortIncompleteMultipartUpload Bucket-Lebenszyklusverwaltungsregel:

```
vserver object-store-server bucket lifecycle-management-rule create
-vserver <svm_name> -bucket <bucket_name> -rule-id <rule_name> -action
AbortIncompleteMultipartUpload -index <lifecycle_rule_index_integer> -is
-enabled {true|false} -prefix <object_name> -tags <text> -obj-size-greater
-than {<integer>[KB|MB|GB|TB|PB]} -obj-size-less-than
```

```
{<integer>[KB|MB|GB|TB|PB]} -after-initiation-days <integer>
```

Lebenszyklusmanagementregeln mit System Manager verwalten

Ab ONTAP 9.14.1 ist es möglich, S3-Objekte mithilfe von System Manager ablaufen zu lassen. Es besteht die Möglichkeit, Lebenszyklusverwaltungsregeln für S3-Objekte hinzuzufügen, zu bearbeiten und zu löschen. Zusätzlich kann eine für einen Bucket erstellte Lebenszyklusregel importiert und für die Objekte in einem anderen Bucket verwendet werden. Eine aktive Regel kann deaktiviert und später wieder aktiviert werden.

Eine Lebenszyklusverwaltungsregel hinzufügen

1. **Speicher > Buckets** auswählen.
2. Wählen Sie den Bucket aus, für den Sie die Ablaufregel festlegen möchten.
3. Klicken Sie auf das ⋮ Symbol und wählen Sie **Lebenszyklusregeln verwalten**.
4. **Hinzufügen > Lebenszyklusregel** auswählen.
5. Auf der Seite „Lebenszyklusregel hinzufügen“ den Namen der Regel hinzufügen.
6. Definieren Sie den Geltungsbereich der Regel, ob sie für alle Objekte im Bucket oder nur für bestimmte Objekte gelten soll. Wenn Sie Objekte angeben möchten, fügen Sie mindestens eines der folgenden Filterkriterien hinzu:
   a. Präfix: Geben Sie ein Präfix für die Objektschlüsselnamen an, auf die die Regel angewendet werden soll. In der Regel ist dies der Pfad oder Ordner des Objekts. Pro Regel kann ein Präfix eingegeben werden. Sofern kein gültiges Präfix angegeben wird, gilt die Regel für alle Objekte in einem Bucket.
   b. Tags: Es können bis zu drei Schlüssel-Wert-Paare (Tags) für die Objekte angegeben werden, auf die die Regel angewendet werden soll. Nur gültige Schlüssel werden zum Filtern verwendet. Der Wert ist optional. Falls Werte hinzugefügt werden, sollten nur gültige Werte für die entsprechenden Schlüssel angegeben werden.
   c. Größe: Sie können den Bereich zwischen minimaler und maximaler Objektgröße einschränken. Sie können einen oder beide Werte eingeben. Die Standardeinheit ist MiB.
7. Aktion angeben:
   a. **Aktuelle Objektversionen ablaufen lassen**: Es kann eine Regel festgelegt werden, nach der alle aktuellen Objekte nach einer bestimmten Anzahl von Tagen seit ihrer Erstellung oder an einem bestimmten Datum dauerhaft nicht mehr verfügbar sind. Diese Option ist nicht verfügbar, wenn die Option **Löschmarkierungen abgelaufener Objekte löschen** ausgewählt ist.
   b. **Nicht mehr aktuelle Versionen endgültig löschen**: Geben Sie die Anzahl der Tage an, nach denen die nicht mehr aktuelle Version gelöscht wird, und die Anzahl der zu behaltenden Versionen.
   c. **Abgelaufene Objektlöschmarkierungen löschen**: Diese Aktion löscht Objekte mit abgelaufenen Löschmarkierungen, also Löschmarkierungen ohne zugehöriges aktuelles Objekt.

      ⓘ Diese Option ist nicht verfügbar, wenn die Option **Aktuelle Version von Objekten ablaufen lassen** ausgewählt wird, die alle Objekte nach Ablauf der Aufbewahrungsfrist automatisch löscht. Diese Option ist ebenfalls nicht verfügbar, wenn Objekttags zum Filtern verwendet werden.

   d. **Unvollständige Multipart-Uploads löschen**: Legen Sie die Anzahl der Tage fest, nach denen unvollständige Multipart-Uploads gelöscht werden. Wenn laufende Multipart-Uploads innerhalb des angegebenen Aufbewahrungszeitraums fehlschlagen, können die unvollständigen Multipart-Uploads gelöscht werden. Diese Option ist nicht verfügbar, wenn Objekt-Tags zum Filtern verwendet werden.

e. Auf **Speichern** klicken.

Import einer Lebenszyklusregel

1. **Speicher > Buckets** auswählen.
2. Wählen Sie den Bucket aus, für den Sie die Ablaufregel importieren möchten.
3. Klicken Sie auf das ⋮ Symbol und wählen Sie **Lebenszyklusregeln verwalten**.
4. **Hinzufügen > Regel importieren** auswählen.
5. Wählen Sie den Bucket aus, aus dem Sie die Regel importieren möchten. Die für den ausgewählten Bucket definierten Lebenszyklusverwaltungsregeln werden angezeigt.
6. Wählen Sie die Regel aus, die Sie importieren möchten. Es besteht die Möglichkeit, jeweils eine Regel auszuwählen, wobei standardmäßig die erste Regel ausgewählt ist.
7. Klicken Sie auf **Import**.

Eine Regel bearbeiten, löschen oder deaktivieren

Sie können nur die mit der Regel verknüpften Lebenszyklusverwaltungsaktionen bearbeiten. Wenn die Regel mit Objekt-Tags gefiltert wurde, sind die Optionen **Abgelaufene Objektlöschmarkierungen löschen** und **Unvollständige Multipart-Uploads löschen** nicht verfügbar.

Wenn eine Regel gelöscht wird, gilt diese Regel nicht mehr für zuvor verknüpfte Objekte.

1. **Speicher > Buckets** auswählen.
2. Wählen Sie den Bucket aus, für den Sie die Lebenszyklusverwaltungsregel bearbeiten, löschen oder deaktivieren möchten.
3. Klicken Sie auf das ⋮ Symbol und wählen Sie **Lebenszyklusregeln verwalten**.
4. Wählen Sie die gewünschte Regel aus. Es ist möglich, jeweils eine Regel zu bearbeiten und zu deaktivieren. Mehrere Regeln können gleichzeitig gelöscht werden.
5. **Bearbeiten**, **Löschen** oder **Deaktivieren** auswählen und den Vorgang abschließen.

Löschen eines ONTAP S3 Bucket mit Objekten

Ab ONTAP 9.20.1 können Sie Löschvorgänge für Buckets auf Objektspeicher-Servern planen, um Buckets zu entfernen, ohne sie zuvor zu leeren. Dies geschieht mithilfe eines konfigurierbaren, auf Aufbewahrung basierenden Wiederherstellungsfensters, das die Bucket-Wiederherstellung vor Ablauf des Aufbewahrungsintervalls ermöglicht.

Die Möglichkeit, nicht leere Buckets zu löschen, vereinfacht die Außerbetriebnahme von Buckets, da eine manuelle Bereinigung Objekt für Objekt vor dem Entfernen eines Buckets vermieden wird, der Ablaufrückstand reduziert wird und die Kapazität schneller wiederverwendbar ist.

Bevor Sie beginnen

- Sie müssen Cluster-Administrator oder SVM-Administrator sein.
- Sie müssen sich auf der erweiterten Berechtigungsstufe befinden.

Löschen eines Buckets, der Objekte enthält

Sie können einen Bucket zur Löschung planen, ohne ihn vorher zu leeren, indem Sie ein Aufbewahrungsintervall festlegen. Standardmäßig beträgt die Aufbewahrungsdauer 12 Stunden.

Schritte

Diese Aufgabe kann über den System Manager oder die ONTAP CLI ausgeführt werden.

System Manager

1. Unter **Storage > Buckets** ist der Bucket zu finden, der gelöscht werden soll.
2. Neben dem Bucket-Namen können Sie **Delete** auswählen.
3. Wenn der Bucket nicht leer ist, ist im Fenster **Delete Bucket** die Option zum Löschen der Daten und zum Leeren des Buckets auszuwählen, und anschließend ist **Delete** auszuwählen.

CLI

1. Das Aufbewahrungsintervall angeben, nach dessen Ablauf der Bucket endgültig gelöscht wird:

   ```
   object-store-server create -vserver <SVM name> -bucket-delete-retention
   -hours <integer>
   ```

2. Einleitung des Zeitplans für die Bucket-Löschung:

   `object-store-server bucket delete -bucket <bucket name> -delete-objects tru`e

Einen gelöschten Bucket wiederherstellen

Wenn ein Bucket versehentlich gelöscht wird, können Sie ihn während der von Ihnen festgelegten Aufbewahrungsfrist mithilfe der ONTAP CLI wiederherstellen.

1. Ein gelöschter Bucket lässt sich mit dem folgenden Befehl wiederherstellen:

   ```
   object-store-server bucket recover-deleted-bucket -bucket <bucket name>
   ```

Einen ONTAP S3-Benutzer erstellen

Ein S3-Benutzer mit spezifischen Berechtigungen wird erstellt. Für alle ONTAP Objektspeicher ist eine Benutzerautorisierung erforderlich, um die Konnektivität auf autorisierte Clients zu beschränken.

Bevor Sie beginnen.

Eine S3-fähige Storage-VM muss bereits vorhanden sein.

Über diese Aufgabe

Einem S3-Benutzer kann Zugriff auf jeden Bucket in einer Storage-VM gewährt werden. Wenn ein S3-Benutzer erstellt wird, werden für den Benutzer auch ein Zugriffsschlüssel und ein geheimer Schlüssel generiert. Diese sollten dem Benutzer zusammen mit dem FQDN des Objektspeichers und dem Bucket-Namen mitgeteilt werden.

Für zusätzliche Sicherheit werden ab ONTAP 9.15.1 Zugriffsschlüssel und geheime Schlüssel nur zum

Zeitpunkt der Erstellung des S3-Benutzers angezeigt und können danach nicht erneut angezeigt werden. Wenn die Schlüssel verloren gehen, "Neue Schlüssel müssen neu generiert werden".

Um den Zugriff auf S3-Ressourcen aufrechtzuerhalten, wenn der ursprüngliche Zugriffsschlüssel abläuft, können Sie ab ONTAP 9.19.1 "einen zweiten Zugriffsschlüssel generieren" für jeden S3-Benutzer vorgehen.

Sie können S3-Benutzern in einer Bucket-Richtlinie oder einer Objektserver-Richtlinie spezifische Zugriffsberechtigungen erteilen.

> Beim Erstellen eines neuen Objektspeicherservers erstellt ONTAP einen Root-Benutzer (UID 0), einen privilegierten Benutzer mit Zugriff auf alle Buckets. Statt ONTAP S3 als Root-Benutzer zu verwalten, empfiehlt NetApp, eine Admin-Benutzerrolle mit spezifischen Berechtigungen zu erstellen.

CLI

1. Einen S3-Benutzer erstellen:
   `vserver object-store-server user create -vserver svm_name -user user_name -comment [-comment text] -key-time-to-live time`

   - Das Hinzufügen eines Kommentars ist optional.
   - Ab ONTAP 9.14.1 kann der Zeitraum, für den der Schlüssel gültig ist, im `-key-time-to-live` Parameter definiert werden. Die Aufbewahrungsdauer kann in diesem Format hinzugefügt werden, um den Zeitraum anzugeben, nach dem der Zugriffsschlüssel abläuft: `P[<integer>D]T[<integer>H][<integer>M][<integer>S] | P<integer>W` Zum Beispiel, wenn eine Aufbewahrungsdauer von einem Tag, zwei Stunden, drei Minuten und vier Sekunden eingegeben werden soll, wird der Wert als `P1DT2H3M4S` eingegeben. Sofern nicht anders angegeben, ist der Schlüssel für einen unbegrenzten Zeitraum gültig.

     Im folgenden Beispiel wird ein Benutzer mit dem Namen `sm_user1` auf der Storage-VM `vs0` mit einer Schlüsselaufbewahrungsfrist von einer Woche erstellt.

     ```
     vserver object-store-server user create -vserver vs0 -user
     sm_user1 -key-time-to-live P1W
     ```

     Sie können beim Erstellen eines Benutzers in den `-access-key` und `-secret-key` Parametern auch manuell Ihren eigenen Zugriffsschlüssel und geheimen Schlüssel definieren. Beispiel:

   ```
   vserver object-store-server user create -vserver svm1 -user user1
   -access-key "20-characters" -secret-key "40-characters"
   ```

2. Der Zugriffsschlüssel und der geheime Schlüssel sollten gespeichert werden. Diese werden für den Zugriff von S3-Clients benötigt.

System Manager

1. Wählen Sie **Speicher > Speicher-VMs**. Wählen Sie die Speicher-VM aus, der Sie einen Benutzer hinzufügen möchten, wählen Sie **Einstellungen** und wählen Sie dann ✎ unter S3.
2. Um einen Benutzer hinzuzufügen, wählen Sie **Benutzer > Hinzufügen**.

3. Einen Namen für den Benutzer eingeben.
4. Ab ONTAP 9.14.1 können Sie die Aufbewahrungsdauer der für den Benutzer erstellten Zugriffsschlüssel festlegen. Sie können die Aufbewahrungsdauer in Tagen, Stunden, Minuten oder Sekunden angeben, nach deren Ablauf die Schlüssel automatisch ablaufen. Standardmäßig ist der Wert auf `0` festgelegt, was bedeutet, dass der Schlüssel unbegrenzt gültig ist.
5. **Speichern** auswählen. Der Benutzer wird erstellt, und ein Zugriffsschlüssel sowie ein geheimer Schlüssel werden für den Benutzer generiert.
6. Den Zugriffsschlüssel und den geheimen Schlüssel herunterladen oder speichern. Diese werden für den Zugriff von S3-Clients benötigt.

Nächste Schritte

- S3 Gruppen erstellen oder ändern

ONTAP S3 Benutzergruppen erstellen oder ändern, um den Zugriff auf Buckets zu steuern.

Der Zugriff auf Buckets lässt sich vereinfachen, indem Gruppen von Benutzern mit entsprechenden Zugriffsberechtigungen erstellt werden.

Bevor Sie beginnen

S3-Benutzer in einer S3-fähigen SVM müssen bereits existieren.

Über diese Aufgabe

Benutzern einer S3-Gruppe kann Zugriff auf jeden Bucket in einer SVM gewährt werden, jedoch nicht auf mehrere SVMs. Gruppenzugriffsberechtigungen können auf zwei Arten konfiguriert werden:

- Auf der Bucket-Ebene

  Nachdem eine Gruppe von S3-Benutzern erstellt wurde, werden die Gruppenberechtigungen in Bucket-Richtlinien festgelegt und gelten nur für diesen Bucket.

- Auf SVM-Ebene

  Nach dem Erstellen einer Gruppe von S3-Benutzern werden in der Gruppendefinition die Namen der Objektserverrichtlinien angegeben. Diese Richtlinien legen die Buckets und den Zugriff für die Gruppenmitglieder fest.

System Manager

1. Die Storage-VM kann bearbeitet werden: Auf **Speicher > Speicher-VMs** klicken, die Storage-VM auswählen, auf **Einstellungen** klicken und dann auf unter S3 klicken.
2. Gruppe hinzufügen: **Gruppen** auswählen und dann **Hinzufügen** wählen.
3. Einen Gruppennamen eingeben und aus einer Liste von Benutzern auswählen.
4. Es kann eine vorhandene Gruppenrichtlinie ausgewählt oder jetzt eine hinzugefügt werden, oder eine Richtlinie kann später hinzugefügt werden.

CLI

1. Erstellen Sie eine S3-Gruppe:

`vserver object-store-server group create -vserver svm_name -name group_name -users user_name\(s\) [-policies policy_names] [-comment text\]` Die `-policies` Option kann in Konfigurationen mit nur einem Bucket in einem Objektspeicher weggelassen werden; der Gruppenname kann der Bucket-Richtlinie hinzugefügt werden. Die `-policies` Option kann später mit dem `vserver object-store-server group modify` Befehl hinzugefügt werden, nachdem die Objektspeicherserverrichtlinien erstellt wurden.

ONTAP S3-Schlüssel neu generieren und deren Aufbewahrungsdauer ändern

Zugriffsschlüssel und geheime Schlüssel werden bei der Benutzererstellung automatisch generiert, um den S3-Clientzugriff zu ermöglichen. Sie können Schlüssel für einen Benutzer neu generieren, falls ein Schlüssel abgelaufen oder kompromittiert wurde. Ab ONTAP 9.19.1 können Sie außerdem einen zweiten Zugriffsschlüssel für einen S3-Benutzer generieren oder entfernen, damit dieser auf S3-Ressourcen zugreifen kann, wenn sein ursprünglicher Zugriffsschlüssel abläuft.

Informationen zur Generierung von Zugriffsschlüsseln sind unter "Einen S3-Benutzer erstellen" zu finden.

Einen S3-Zugriffsschlüssel neu generieren

System Manager

1. Wählen Sie **Speicher > Speicher-VMs** und anschließend die gewünschte Speicher-VM aus.
2. Wählen Sie im Reiter **Einstellungen** in der Kachel **S3** aus.
3. Auf der Registerkarte **Benutzer** ist zu überprüfen, ob kein Zugriffsschlüssel vorhanden ist oder der Schlüssel für den Benutzer abgelaufen ist.
4. Falls Sie den Schlüssel neu generieren müssen, wählen Sie neben dem Benutzer und klicken Sie anschließend auf **Schlüssel neu generieren**.
5. Generierte Schlüssel haben standardmäßig den Gültigkeitswert 0 und laufen nie ab. Ab ONTAP 9.14.1 können Sie deren Aufbewahrungsdauer ändern, nach deren Ablauf die Schlüssel automatisch verfallen. Geben Sie die Aufbewahrungsdauer in Tagen, Stunden, Minuten oder Sekunden ein.
6. Ab ONTAP 9.19.1 können Benutzer einen zweiten Zugriffsschlüssel besitzen. Falls der Benutzer über einen zweiten Zugriffsschlüssel verfügt, wählen Sie den Zugriffsschlüssel zur Regenerierung aus. Sie können beide Zugriffsschlüssel zur Regenerierung auswählen.
7. Wählen Sie **Speicher > Speicher-VMs** und anschließend die gewünschte Speicher-VM aus. **Speichern**. Der Schlüssel wird neu generiert. Alle Änderungen an der Schlüsselaufbewahrungsdauer werden sofort wirksam.
8. Den Zugriffsschlüssel und den geheimen Schlüssel herunterladen oder speichern. Diese werden für den Zugriff von S3-Clients benötigt.

CLI

1. Zugriffs- und geheime Schlüssel für einen Benutzer können durch Ausführen des `vserver object-store-server user regenerate-keys` Befehls neu generiert werden.
2. Standardmäßig sind generierte Schlüssel unbegrenzt gültig. Ab ONTAP 9.14.1 können Sie deren Aufbewahrungsdauer ändern, nach deren Ablauf die Schlüssel automatisch verfallen. Sie können die

Aufbewahrungsdauer in folgendem Format hinzufügen: `P[<integer>D]T[<integer>H][<integer>M][<integer>S] | P<integer>W` Wenn Sie beispielsweise eine Aufbewahrungsdauer von einem Tag, zwei Stunden, drei Minuten und vier Sekunden festlegen möchten, geben Sie den Wert wie folgt ein `P1DT2H3M4S`.

3. Ab ONTAP 9.19.1 können Sie, falls der Benutzer über mehrere Zugriffsschlüssel verfügt, auswählen, welcher Schlüssel neu generiert werden soll. Die Angabe des Schlüssels erfolgt in folgendem Format: `[-key-id {1..2}]`
   - Wenn keine Schlüssel-ID angegeben werden muss, wird Schlüssel 1 neu generiert.
   - Um Schlüssel 1 anzugeben, geben Sie den Wert als `-key-id 1` ein.
   - Um Schlüssel 2 anzugeben, geben Sie den Wert als `-key-id 2` ein.
   - Um die Schlüssel 1 und 2 anzugeben, geben Sie den Wert wie folgt ein `-key-id 1 2`. Um beispielsweise Schlüssel 1 neu zu generieren:

     ```
     vserver object-store-server user regenerate-keys -vserver
     svm_name -user user -key-id 1 -key-time-to-live 0
     ```

4. Speichern Sie die Zugriffs- und geheimen Schlüssel. Diese werden für den Zugriff von S3-Clients benötigt.

Generieren Sie einen zweiten S3-Zugriffsschlüssel

Ab ONTAP 9.19.1 können Sie einen zweiten Zugriffsschlüssel für einen Benutzer generieren.

System Manager

1. Wählen Sie **Speicher > Speicher-VMs** und anschließend die gewünschte Speicher-VM aus.
2. Wählen Sie **Speicher > Speicher-VMs** und anschließend die gewünschte Speicher-VM aus. **Storage > Storage VMs** und anschließend die Storage-VM auswählen.
3. Wählen Sie im Reiter **Einstellungen** in der Kachel **S3** aus.
4. Im Reiter **Benutzer** wählen Sie neben dem Benutzer die Option **Weiteren Schlüssel hinzufügen**.
5. Generierte Schlüssel haben standardmäßig den Gültigkeitswert 0 und laufen nie ab. Ab ONTAP 9.14.1 können Sie deren Aufbewahrungsdauer ändern, nach deren Ablauf die Schlüssel automatisch verfallen. Geben Sie die Aufbewahrungsdauer in Tagen, Stunden, Minuten oder Sekunden ein.
6. Wählen Sie **Speicher > Speicher-VMs** und anschließend die gewünschte Speicher-VM aus. **Hinzufügen**. Der zweite Schlüssel wird generiert. Die angegebene Aufbewahrungsfrist für den Schlüssel tritt sofort in Kraft.
7. Den Zugriffsschlüssel und den geheimen Schlüssel herunterladen oder speichern. Diese werden für den Zugriff von S3-Clients benötigt.

CLI

1. Generieren Sie zweite Zugriffs- und geheime Schlüssel für einen Benutzer, indem Sie den `vserver object-store-server user regenerate-keys` Befehl ausführen.
2. Standardmäßig sind generierte Schlüssel unbegrenzt gültig. Ab ONTAP 9.14.1 können Sie deren Aufbewahrungsdauer ändern, nach deren Ablauf die Schlüssel automatisch verfallen. Sie können die Aufbewahrungsdauer in folgendem Format hinzufügen:

`P[<integer>D]T[<integer>H][<integer>M][<integer>S] | P<integer>W` Wenn Sie beispielsweise eine Aufbewahrungsdauer von einem Tag, zwei Stunden, drei Minuten und vier Sekunden festlegen möchten, geben Sie den Wert wie folgt ein `P1DT2H3M4S`.

3. Ab ONTAP 9.19.1 können Sie einen zweiten Zugriffsschlüssel in diesem Format generieren: `[-key-id 2]`

   Beispiel:

   ```
   vserver object-store-server user regenerate-keys -vserver svm_name
   -user user -key-id 2 -key-time-to-live 0
   ```

4. Speichern Sie die Zugriffs- und geheimen Schlüssel. Diese werden für den Zugriff von S3-Clients benötigt.

S3-Zugriffsschlüssel anzeigen

System Manager

1. Wählen Sie **Speicher > Speicher-VMs** und anschließend die gewünschte Speicher-VM aus.
2. Wählen Sie im Reiter **Einstellungen** in der Kachel **S3** aus.
3. Überprüfen Sie auf der Registerkarte **Benutzer**, ob es keine zweiten Zugriffsschlüssel für die S3-Benutzer gibt.

CLI

Zugriffs- und geheime Schlüssel eines Benutzers können durch Ausführen des `vserver object-store-server user show` Befehls angezeigt werden.

Beispiel:

```
vserver object-store-server user show -vserver svm_name -user user
```

Einen S3-Zugriffsschlüssel entfernen

Ab ONTAP 9.19.1 können Sie einen der Zugriffsschlüssel eines Benutzers entfernen. Um beide Schlüssel eines Benutzers zu löschen, muss der Benutzer gelöscht werden.

System Manager

1. Wählen Sie **Speicher > Speicher-VMs** und anschließend die gewünschte Speicher-VM aus.
2. Wählen Sie im Reiter **Einstellungen** in der Kachel **S3** aus.
3. Im Reiter **Benutzer** wählen Sie neben dem Benutzer die Option **Weiteren Schlüssel hinzufügen**.
4. Wählen Sie **Schlüssel 1 entfernen** oder **Schlüssel 2 entfernen** aus.
5. **Speichern** auswählen. Der ausgewählte Schlüssel wird entfernt.

6. Den Zugriffsschlüssel und den geheimen Schlüssel herunterladen oder speichern. Diese werden für den Zugriff von S3-Clients benötigt.

CLI

1. Entfernen Sie die Zugriffs- und geheimen Schlüssel eines Benutzers, indem Sie den `vserver object-store-server user delete-keys` Befehl ausführen.
2. Sie können den zu entfernenden Schlüssel auswählen, indem Sie den Schlüssel in diesem Format angeben: `[-key-id {1..2}]`
   - Besitzt der Benutzer nur einen Schlüssel, muss keine Schlüssel-ID angegeben werden.
   - Um Schlüssel 1 anzugeben, geben Sie den Wert als `-key-id 1` ein.
   - Um Schlüssel 2 anzugeben, geben Sie den Wert als `-key-id 2` ein.
   - Wird keine Schlüssel-ID angegeben, löscht der Befehl standardmäßig Schlüssel 2.
   - Um beide Schlüssel zu löschen, löschen Sie den Benutzer. Beispiel:

```
vserver object-store-server user delete-keys -vserver svm_name
-user user -key-id 2
```

Copyright-Informationen

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

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

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

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

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

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

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

Markeninformationen

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