S3 Objektspeicherverwaltung

ONTAP 9

NetApp
November 14, 2026

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

Inhalt

S3 Objektspeicherverwaltung . . . 1
- Informationen zur S3-Unterstützung in ONTAP 9 . . . 1
  - Informationen zur ONTAP S3 Konfiguration . . . 1
  - ONTAP S3 Architektur mit FlexGroup Volumes . . . 2
  - Primäre Anwendungsfälle von ONTAP S3 . . . 4
- Planen . . . 5
  - ONTAP Version und Plattformunterstützung für S3-Objektspeicher . . . 5
  - ONTAP S3 unterstützte Aktionen . . . 6
  - ONTAP S3 Interoperabilität . . . 15
  - Validierte Drittanbieterlösungen mit S3 in ONTAP . . . 17
- Konfigurieren . . . 18
  - Zum S3-Konfigurationsprozess . . . 18
  - S3-Zugriff auf eine SVM konfigurieren . . . 23
  - Speicherkapazität zu einer S3-fähigen SVM hinzufügen . . . 36
  - Zugriffsrichtlinien-Anweisungen erstellen oder ändern . . . 56
  - Clientzugriff auf S3-Objektspeicher ermöglichen . . . 69
  - ONTAP S3 Storage-Servicelevel . . . 72
  - Cross-Origin Resource Sharing (CORS) für ONTAP S3 Buckets konfigurieren . . . 73
- Buckets mit SnapMirror S3 schützen . . . 78
  - Informationen zu ONTAP SnapMirror S3 . . . 78
  - Spiegelungs- und Backup-Schutz auf einem entfernten Cluster . . . 81
  - Spiegelungs- und Backup-Schutz im lokalen Cluster . . . 92
  - Backup-Schutz mit Cloud-Zielen . . . 101
  - Eine ONTAP SnapMirror S3-Richtlinie ändern . . . 110
- S3-Daten mit Snapshots schützen . . . 110
  - Informationen zu ONTAP S3 Snapshots . . . 110
  - ONTAP S3 Snapshots erstellen . . . 112
  - ONTAP S3 Snapshots anzeigen und wiederherstellen . . . 114
  - ONTAP S3 Snapshots löschen . . . 117
- Audit S3-Ereignisse . . . 118
  - Informationen zur Überwachung von ONTAP S3-Ereignissen . . . 118
  - Planung einer ONTAP S3 Audit-Konfiguration . . . 121
  - Erstellen und Aktivieren einer ONTAP S3 Überwachungskonfiguration . . . 124
  - Buckets für ONTAP S3-Auditing auswählen . . . 125
  - Ändern einer ONTAP S3 Überwachungskonfiguration . . . 126
  - ONTAP S3-Überwachungskonfigurationen anzeigen . . . 127

S3 Objektspeicherverwaltung

Informationen zur S3-Unterstützung in ONTAP 9

Informationen zur ONTAP S3 Konfiguration

Ab ONTAP 9.8 kann ein ONTAP Simple Storage Service (S3) Objektspeicherserver in einem ONTAP Cluster aktiviert werden, wobei vertraute Verwaltungstools wie ONTAP System Manager verwendet werden, um leistungsstarken Objektspeicher für Entwicklung und Betrieb in ONTAP schnell bereitzustellen und die Speichereffizienz sowie Sicherheit von ONTAP zu nutzen.

Ab Juli 2024 sind Inhalte aus technischen Berichten, die zuvor als PDFs veröffentlicht wurden, in die ONTAP Produktdokumentation integriert. Die ONTAP S3 Dokumentation enthält nun Inhalte aus *TR-4814: S3 in ONTAP best practices*.

S3-Konfiguration mit System Manager und der ONTAP CLI

Sie können ONTAP S3 mit System Manager und der ONTAP CLI konfigurieren und verwalten. Wenn S3 aktiviert und Buckets mit System Manager erstellt werden, wählt ONTAP bewährte Standardwerte für eine vereinfachte Konfiguration aus. Falls Konfigurationsparameter angegeben werden müssen, kann die ONTAP CLI verwendet werden. Wenn der S3-Server und die Buckets über die CLI konfiguriert werden, ist eine Verwaltung mit System Manager weiterhin möglich, oder umgekehrt.

Wenn Sie mit dem System Manager einen S3-Bucket erstellen, konfiguriert ONTAP standardmäßig die höchste verfügbare Leistungsservice-Stufe Ihres Systems. Auf einem AFF System wäre die Standardeinstellung beispielsweise **Extreme**. Leistungsservice-Stufen sind vordefinierte adaptive Quality of Service (QoS) Richtliniengruppen. Statt einer der Standardservice-Stufen kann eine benutzerdefinierte QoS-Richtliniengruppe oder keine Richtliniengruppe angegeben werden.

Vordefinierte adaptive QoS-Richtliniengruppen sind:

- **Extrem**: Wird für Anwendungen genutzt, die die geringste Latenz und die höchste Leistung erwarten.
- **Leistung**: Wird für Anwendungen mit moderaten Leistungsanforderungen und Latenz verwendet.
- **Value**: Wird für Anwendungen verwendet, bei denen Durchsatz und Kapazität wichtiger sind als Latenz.
- **Benutzerdefiniert**: Eine benutzerdefinierte QoS-Richtlinie oder keine QoS-Richtlinie angeben.

Wenn Sie **Für Tiering verwenden** auswählen, werden keine Leistungs-Servicelevel ausgewählt, und das System versucht, kostengünstige Medien mit optimaler Leistung für die gestaffelten Daten auszuwählen.

Siehe auch: "Adaptive QoS-Richtliniengruppen".

ONTAP versucht, diesen Bucket auf lokalen Tiers mit den am besten geeigneten Festplatten bereitzustellen, um das gewählte Servicelevel zu erfüllen. Wenn jedoch angegeben werden muss, welche Festplatten im Bucket enthalten sein sollen, empfiehlt sich die Konfiguration des S3 Objektspeichers über die CLI, wobei die lokalen Tiers (Aggregate) spezifiziert werden. Wird der S3 Server über die CLI konfiguriert, ist eine Verwaltung weiterhin mit System Manager möglich, falls gewünscht.

Wenn die Möglichkeit bestehen soll, festzulegen, welche Aggregate für Buckets verwendet werden, ist dies nur über die CLI möglich.

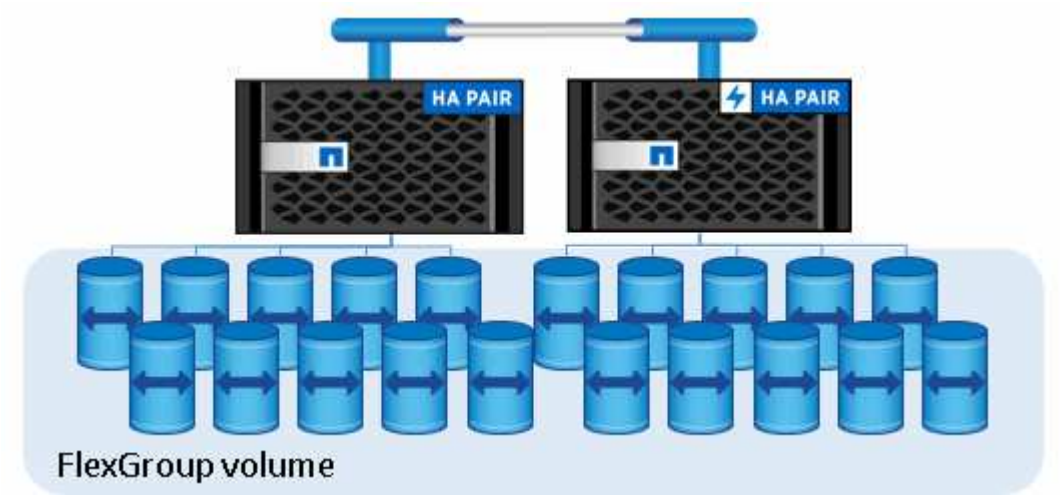
Konfiguration von S3-Buckets auf Cloud Volumes ONTAP

Wenn Sie Buckets von Cloud Volumes ONTAP bereitstellen möchten, wird dringend empfohlen, die zugrunde liegenden Aggregate manuell auszuwählen, um sicherzustellen, dass sie nur einen Knoten verwenden. 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. Daher sollte in Cloud Volumes ONTAP-Umgebungen S3 Buckets über die Befehlszeile konfigurieren.

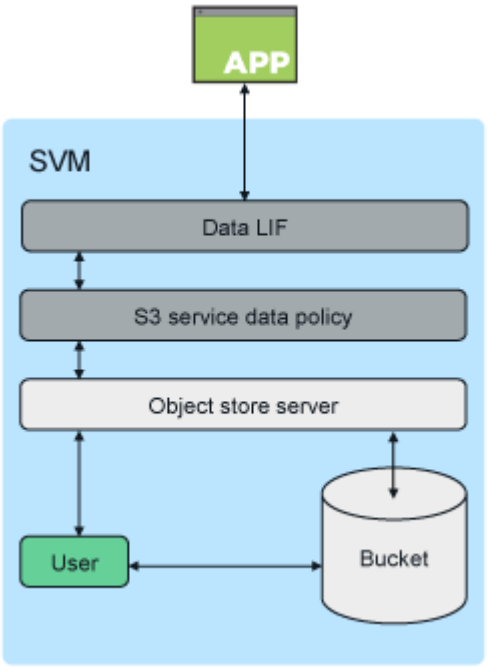
Ansonsten werden S3-Server auf Cloud Volumes ONTAP genauso konfiguriert und gewartet wie in lokalen Umgebungen.

ONTAP S3 Architektur mit FlexGroup Volumes

In ONTAP ist die zugrunde liegende Architektur für einen Bucket ein "FlexGroup-Volume", ein einzelner Namespace, der aus mehreren konstituierenden Mitgliedsvolumes besteht, aber als ein einzelnes Volume verwaltet wird.



Der Zugriff auf den Bucket erfolgt über autorisierte Benutzer und Client-Anwendungen.



Wird ein Bucket ausschließlich für S3-Anwendungen verwendet, einschließlich der Verwendung als FabricPool Endpunkt, unterstützt das zugrunde liegende FlexGroup Volume nur das S3-Protokoll.

Ab ONTAP 9.12.1 kann das S3-Protokoll auch in "Multiprotokoll NAS Volumes" aktiviert werden, die für die Verwendung von NAS-Protokollen vorkonfiguriert sind. Wenn das S3-Protokoll in Multiprotokoll-NAS-Volumes aktiviert ist, können Clientanwendungen Daten über NFS, SMB und S3 lesen und schreiben.

Bucket-Limits

Mindestkapazität

Die Mindestkapazität des Buckets wird durch die ONTAP Plattform bestimmt.

- 95GB für lokale Plattformen.
- 200 MB für ONTAP Select.

Maximale Größe

Die maximale Bucket-Kapazität ist auf die maximale FlexGroup-Größe von 60PB begrenzt.

Maximale Anzahl an Buckets

Die maximale Anzahl an Buckets beträgt 1000 pro FlexGroup Volume oder 12.000 Buckets pro Cluster (bei Verwendung von 12 FlexGroup Volumes).

Automatische FlexGroup Dimensionierung mit ONTAP 9.14.1 und höher

Ab ONTAP 9.14.1 basiert die Standardgröße des FlexGroup auf der Größe der enthaltenen Buckets. Das FlexGroup-Volume wächst oder schrumpft automatisch, wenn Buckets hinzugefügt oder entfernt werden.

Wenn beispielsweise ein anfänglicher Bucket_A mit 100GB bereitgestellt wird, wird das FlexGroup Thin-

Provisioned-Volume ebenfalls auf 100GB festgelegt. Wenn zwei zusätzliche Buckets erstellt werden, Bucket_B mit 300GB und Bucket_C mit 500GB, wächst das FlexGroup Volume auf 900GB.

(Bucket_A mit 100GB + Bucket_B mit 300GB + Bucket_C mit 500GB = 900GB.)

Wenn Bucket_A gelöscht wird, wird das zugrunde liegende FlexGroup Volume auf 800GB verkleinert.

Feste Standardgrößen für FlexGroup in ONTAP 9.13.1 und früher

Um die Kapazität für Bucket-Erweiterungen bereitzustellen, sollte die gesamte belegte Kapazität aller Buckets auf dem FlexGroup Volume weniger als 33 % der maximalen FlexGroup Volume-Kapazität betragen, basierend auf den verfügbaren Speicheraggregaten im Cluster. Falls dies nicht erfüllt werden kann, wird der neu erstellte Bucket auf einem neuen, automatisch erstellten FlexGroup Volume bereitgestellt.

Vor ONTAP 9.14.1 ist die Größe des FlexGroup standardmäßig abhängig von der jeweiligen Umgebung festgelegt:

- 1,6PB in ONTAP
- 100TB in ONTAP Select

Wenn ein Cluster nicht über genügend Kapazität verfügt, um ein FlexGroup Volume in der Standardgröße bereitzustellen, reduziert ONTAP die Standardgröße um die Hälfte, bis es in der bestehenden Umgebung bereitgestellt werden kann.

In einer 300-TB-Umgebung wird ein FlexGroup Volume beispielsweise automatisch mit 200 TB bereitgestellt (1,6-PB-, 800-TB- und 400-TB-FlexGroup Volumes wären zu groß für die Umgebung).

Primäre Anwendungsfälle von ONTAP S3

Dies sind die wichtigsten Anwendungsfälle für den Clientzugriff auf ONTAP S3 Services:

- Die Verwendung von FabricPool zum Tiering inaktiver Daten in einen Bucket in ONTAP ermöglicht ONTAP zu ONTAP Tiering. Das Tiering in einen Bucket innerhalb des "lokales Cluster" oder das Tiering in einen Bucket auf einem "Remote Cluster" wird jeweils unterstützt. Das Tiering zu ONTAP S3 ermöglicht die Nutzung kostengünstigerer ONTAP Systeme für inaktive Daten und Einsparungen bei neuer Flash-Kapazität, ohne dass zusätzliche FabricPool Lizenzen oder neue Technologien verwaltet werden müssen.
- Ab ONTAP 9.12.1 kann das S3-Protokoll auch in "Multiprotokoll NAS Volumes" aktiviert werden, die für die Verwendung von NAS-Protokollen vorkonfiguriert sind. Wenn das S3-Protokoll in Multiprotokoll-NAS-Volumes aktiviert ist, können Client-Anwendungen Daten über S3, NFS und SMB lesen und schreiben, was eine Vielzahl zusätzlicher Anwendungsfälle eröffnet. Einer der häufigsten Anwendungsfälle ist, dass NAS-Clients Daten auf ein Volume schreiben und S3-Clients dieselben Daten lesen und spezialisierte Aufgaben wie Analysen, Business Intelligence, maschinelles Lernen und optische Zeichenerkennung durchführen.

> ⓘ ONTAP S3 ist geeignet, wenn S3-Funktionen auf bestehenden ONTAP Clustern ohne zusätzliche Hardware und Verwaltung aktiviert werden sollen. NetApp StorageGRID ist die führende Lösung von NetApp für Objektspeicher. StorageGRID wird für native S3-Anwendungen empfohlen, die den vollständigen Funktionsumfang von S3, erweiterte ILM-Funktionen oder Kapazitäten benötigen, die in ONTAP-basierten Systemen nicht erreichbar sind. Weitere Informationen sind in der "StorageGRID Dokumentation" zu finden.

Verwandte Informationen

"FlexGroup Volumenmanagement"

Planen

ONTAP Version und Plattformunterstützung für S3-Objektspeicher

S3 Objektspeicher ist auf allen AFF, FAS und ONTAP Select Plattformen mit ONTAP 9.8 und höher verfügbar.

Wie bei anderen Protokollen wie FC, iSCSI, NFS, NVMe_oF und SMB ist für S3 die Installation einer Lizenz erforderlich, bevor es in ONTAP verwendet werden kann. Die S3-Lizenz ist eine kostenlose Lizenz, muss jedoch auf Systemen installiert werden, die auf ONTAP 9.8 aktualisiert werden. Die S3-Lizenz kann von der "Lizenzschlüssel-Seite" NetApp Support-Website heruntergeladen werden.

Bei neuen ONTAP 9.8 und höheren Systemen ist die S3-Lizenz vorinstalliert.

Cloud Volumes ONTAP

ONTAP S3 ist in Cloud Volumes ONTAP wie in lokalen Umgebungen konfiguriert und funktioniert genauso, mit einer Ausnahme:

- Beim Erstellen von Buckets in Cloud Volumes ONTAP sollte mithilfe der CLI-Prozedur sichergestellt werden, dass das zugrunde liegende FlexGroup Volume nur Aggregate von einem einzigen Knoten verwendet. Die Verwendung von Aggregaten aus mehreren Knoten wirkt sich auf die Performance aus, da sich die Knoten in geografisch getrennten Verfügbarkeitszonen befinden und anfällig für Latenzprobleme sind.

Cloud-Provider	ONTAP Version
Google Cloud	ONTAP 9.12.1 und höher
AWS	ONTAP 9.11.0 und höher
Azure	ONTAP 9.9.1 und höher

Amazon FSx for NetApp ONTAP

S3-Objektspeicher wird auf Amazon FSx für NetApp Dienste unterstützt, die ONTAP 9.11 und höher verwenden.

S3-Unterstützung mit MetroCluster

Ab ONTAP 9.20.1 werden die folgenden S3-Funktionen in MetroCluster Konfigurationen unterstützt:

- SnapMirror S3
- S3 Bucket Lebenszyklusmanagement

Ab ONTAP 9.14.1 ist es möglich, einen S3 Objektspeicherserver auf einer SVM in einem gespiegelten Aggregat in MetroCluster IP- und FC-Konfigurationen zu aktivieren.

Ab ONTAP 9.12.1 ist es möglich, einen S3-Objektspeicherserver auf einer SVM in einem nicht gespiegelten Aggregat in einer MetroCluster IP Konfiguration zu aktivieren. Weitere Informationen zu den Einschränkungen nicht gespiegelter Aggregate in MetroCluster IP Konfigurationen sind unter "Überlegungen zu nicht gespiegelten Aggregaten" zu finden.

Öffentliche Vorschau von S3 in ONTAP 9.7

In ONTAP 9.7 wurde S3 Objektspeicher als öffentliche Vorschau eingeführt. Diese Version war nicht für Produktionsumgebungen vorgesehen und wird ab ONTAP 9.8 nicht mehr aktualisiert. Nur ONTAP 9.8 und spätere Versionen unterstützen S3 Objektspeicher in Produktionsumgebungen.

Mit der öffentlichen Vorschauversion 9.7 erstellte S3-Buckets können in ONTAP 9.8 und höher verwendet werden, jedoch nicht von Funktionserweiterungen profitieren. Für Buckets, die mit der öffentlichen Vorschauversion 9.7 erstellt wurden, wird empfohlen, deren Inhalte in 9.8-Buckets zu migrieren, um Unterstützung für Funktionen, Sicherheit und Leistungsverbesserungen zu erhalten.

ONTAP S3 unterstützte Aktionen

ONTAP S3-Aktionen werden von den Standard-S3-REST-APIs unterstützt, sofern nachfolgend nichts anderes angegeben ist. Weitere Informationen enthält die "Amazon S3 API-Referenz".

> Diese S3-Aktionen werden speziell bei der Verwendung von nativen S3-Buckets in ONTAP unterstützt. Einige dieser Aktionen, wie beispielsweise solche im Zusammenhang mit Versionierung, Objektsperren und anderen Funktionen, werden bei der Verwendung von "S3 NAS Buckets (S3 in Multiprotokoll NAS Volumes)" nicht unterstützt.

Sofern für einen bestimmten Vorgang nichts anderes angegeben ist, werden ab ONTAP 9.8 die folgenden gängigen Anforderungsheader unterstützt:

- `Authorization`
- `Connection`
- `Content-Length`
- `Content-MD5`
- `Content-Type`
- `Date`
- `Expect`
- `Host`
- `x-amz-date`

Ab ONTAP 9.20.1 werden die folgenden Prüfsummen-Header für S3 NAS Buckets unterstützt:

- `x-amz-checksum-algorithm`
- `x-amz-checksum-crc64nvme`
- `x-amz-checksum-type`

Bucket-Operationen

Die folgenden Operationen werden in ONTAP mit AWS S3 APIs unterstützt:

Bucket-Operation	ONTAP Unterstützung ab
CreateBucket ONTAP S3 unterstützt diesen zusätzlichen Header: • `x-amz-bucket-object-lock-enabled`	ONTAP 9.11.1
DeleteBucket	ONTAP 9.11.1
DeleteBucketCors	ONTAP 9.8
DeleteBucketLifecycle	ONTAP 9.8
DeleteBucketPolicy	ONTAP 9.12.1
GetBucketAcl	ONTAP 9.8
GetBucketCors	ONTAP 9.8
GetBucketLifecycleConfiguration	ONTAP 9.13.1 *Es werden nur Ablaufaktionen unterstützt
GetBucketLocation	ONTAP 9.10.1
GetBucketPolicy	ONTAP 9.12.1
GetBucketVersioning	ONTAP 9.11.1
HeadBucket	ONTAP 9.8
ListAllMyBuckets	ONTAP 9.8
ListBuckets	ONTAP 9.8
ListBucketVersions	ONTAP 9.11.1
PutBucket	• ONTAP 9.11.1 • ONTAP 9.8 – wird nur mit ONTAP REST APIs unterstützt
PutBucketCors	ONTAP 9.8
PutBucketLifecycleConfiguration	ONTAP 9.13.1 * Nur Ablaufaktionen werden unterstützt
PutBucketPolicy	ONTAP 9.12.1
PutBucketVersioning	ONTAP 9.11.1

Objektoperationen

Ab ONTAP 9.19.1 unterstützt ONTAP S3 die Durchsetzung bedingter Schreibvorgänge beim Hochladen von Objekten und bedingter Löschvorgänge beim Löschen von Objekten. Bedingte Schreib- und Löschvorgänge bieten eine Möglichkeit, das Überschreiben oder unbeabsichtigte Löschen von Objekten zu verhindern. Bedingte Operationen funktionieren nur, wenn die Anfrage mit der AWS_V4-Signaturmethode über eine TLS-Verbindung gestellt wird. Die folgenden bedingten Header und Objektoperationen werden unterstützt:

Objektoperation	Bedingter Header
PutObject CopyObject CompleteMultipartUpload	If-None-Match If-Match
DeleteObject DeleteObjects	If-Match

Ab ONTAP 9.20.1 unterstützt ONTAP S3 flexible Prüfsummen für S3 NAS-Buckets.

- ONTAP validiert, speichert und gibt Prüfsummen zurück, wenn Clients Prüfsummen-Header in Anfragen einfügen.
- Es werden nur der CRC-64NVME-Algorithmus und der `FULL_OBJECT` Prüfsummentyp unterstützt.
- Die Unterstützung für flexible Prüfsummen gilt nur für S3 NAS-Buckets.

Ab ONTAP 9.9.1 unterstützt ONTAP S3 Objektmetadaten und Tagging.

- PutObject und CreateMultipartUpload enthalten Schlüssel-Wert-Paare mithilfe von `x-amz-meta-<key>`.

  Zum Beispiel: `x-amz-meta-project: ontap_s3`.

- GetObject und HeadObject geben benutzerdefinierte Metadaten zurück.
- Im Gegensatz zu Metadaten können Tags unabhängig von Objekten gelesen werden mit:
  - PutObjectTagging
  - GetObjectTagging
  - DeleteObjectTagging

Ab ONTAP 9.11.1 unterstützt ONTAP S3 die Objektversionierung und zugehörige Aktionen mit diesen ONTAP APIs:

- GetBucketVersioning
- ListBucketVersions
- PutBucketVersioning

Sofern für eine bestimmte Operation nicht anders angegeben, wird der folgende URI-Abfrageparameter unterstützt:

- `versionId` (wie für Objektoperationen ab ONTAP 9.12.1 erforderlich)

Objektoperation	ONTAP Unterstützung ab
AbortMultipartUpload ONTAP S3 unterstützt diesen zusätzlichen URI-Abfrageparameter: `uploadId`	ONTAP 9.8

Objektoperation	ONTAP Unterstützung ab
CompleteMultipartUpload ONTAP S3 unterstützt diesen zusätzlichen URI-Abfrageparameter: `uploadId`	ONTAP 9.8
CopyObject ONTAP S3 unterstützt diese zusätzlichen Header: • `x-amz-copy-source` • `x-amz-copy-source-if-match` • `x-amz-copy-source-if-modified-since` • `x-amz-copy-source-if-none-match` • `x-amz-copy-source-if-unmodified-since` • `x-amz-metadata-directive` • `x-amz-object-lock-mode` • `x-amz-object-lock-retain-until-date` • `x-amz-tagging` • `x-amz-tagging-directive` • `x-amz-meta-<metadata-name>`	ONTAP 9.12.1
CreateMultipartUpload ONTAP S3 unterstützt diese zusätzlichen Header: • `Cache-Control` • `Content-Disposition` • `Content-Encoding` • `Content-Language` • `Expires` • `x-amz-tagging` • `x-amz-object-lock-mode` • `x-amz-object-lock-retain-until-date` • `x-amz-meta-<metadata-name>`	ONTAP 9.8
DeleteObject ONTAP S3 unterstützt diesen zusätzlichen Header: • `x-amz-bypass-governance-retention`	ONTAP 9.8

Objektoperation	ONTAP Unterstützung ab
DeleteObjects ONTAP S3 unterstützt diesen zusätzlichen Header: * `x-amz-bypass-governance-retention`	ONTAP 9.11.1
DeleteObjectTagging	ONTAP 9.9.1
GetObject ONTAP S3 unterstützt diese zusätzlichen URI-Abfrageparameter: • `partNumber` • `response-cache-control` • `response-content-disposition` • `response-content-encoding` • `response-content-language` • `response-content-type` • `response-expires` Und diese zusätzlichen Anfrage-Header: • Bereich	ONTAP 9.8
GetObjectAcl	ONTAP 9.8
GetObjectAttributes ONTAP S3 unterstützt alle gängigen Parameter und Header für diese Anforderung, ONTAP S3 unterstützt außerdem diesen zusätzlichen Header: • `x-amz-object-attributes`	ONTAP 9.17.1
GetObjectRetention	ONTAP 9.14.1
GetObjectTagging	ONTAP 9.9.1
HeadObject ONTAP S3 unterstützt alle gängigen Parameter und Header für diese Anfrage.	ONTAP 9.8
ListMultipartUploads ONTAP S3 unterstützt diese zusätzlichen URI-Parameter: • `delimiter` • `key-marker` • `max-uploads` • `prefix` • `upload-id-marker`	ONTAP 9.8

Objektoperation	ONTAP Unterstützung ab
ListObjects ONTAP S3 unterstützt diese zusätzlichen URI-Parameter: • `delimiter` • `encoding-type` • `marker` • `max-keys` • `prefix`	ONTAP 9.8
ListObjectsV2 ONTAP S3 unterstützt diese zusätzlichen URI-Parameter: • `continuation-token` • `delimiter` • `encoding-type` • `fetch-owner` • `max-keys` • `prefix` • `start-after`	ONTAP 9.8
ListObjectVersions ONTAP S3 unterstützt diese zusätzlichen URI-Parameter: • `delimiter` • `encoding-type` • `key-marker` • `max-keys` • `prefix` • `version-id-marker`	ONTAP 9.11.1

Objektoperation	ONTAP Unterstützung ab
ListParts ONTAP S3 unterstützt diese zusätzlichen URI-Parameter: • `max-parts` • `part-number-marker` • `uploadId`	ONTAP 9.8
PutObject ONTAP S3 unterstützt diese zusätzlichen Header: • `Cache-Control` • `Content-Disposition` • `Content-Encoding` • `Content-Language` • `Expires` • `x-amz-tagging` • `x-amz-object-lock-mode` • `x-amz-object-lock-retain-until-date` • `x-amz-meta-<metadata-name>`	ONTAP 9.8
PutObjectLockConfiguration	ONTAP 9.14.1
PutObjectRetention ONTAP S3 unterstützt diesen zusätzlichen Header: • `x-amz-bypass-governance-retention`	ONTAP 9.14.1
PutObjectTagging	ONTAP 9.9.1
UploadPart ONTAP S3 unterstützt alle gängigen Parameter und Header für diese Anfrage.	ONTAP 9.8

Objektoperation	ONTAP Unterstützung ab
UploadPartCopy ONTAP S3 unterstützt diese zusätzlichen URI-Parameter: • `partNumber` • `uploadId` Und diese zusätzlichen Anfrage-Header: • `x-amz-copy-source` • `x-amz-copy-source-if-match` • `x-amz-copy-source-if-modified-since` • `x-amz-copy-source-if-none-match` • `x-amz-copy-source-if-unmodified-since` • `x-amz-copy-source-range`	ONTAP 9.12.1

Gruppenrichtlinien

Diese Operationen sind nicht S3-spezifisch und werden im Allgemeinen mit Identitäts- und Verwaltungsprozessen (IAM) in Verbindung gebracht. ONTAP unterstützt diese Befehle, verwendet jedoch nicht die IAM REST-APIs.

- Richtlinie erstellen
- AttachGroup Richtlinie

Benutzerverwaltung

Diese Operationen sind nicht spezifisch für S3 und stehen im Allgemeinen im Zusammenhang mit IAM-Prozessen.

- CreateUser
- DeleteUser
- CreateGroup
- DeleteGroup

S3-Aktionen nach Release

ONTAP 9.20.1

Ab ONTAP 9.20.1 unterstützen S3 NAS-Buckets auf FlexCache Volumes serverseitige Objektkopiervorgänge mithilfe der S3 `CopyObject` und `UploadPartCopy` APIs. Objekte lassen sich innerhalb desselben FlexCache NAS-Buckets oder von einem S3 NAS-Bucket, der auf einem FlexGroup Volume basiert, in einen FlexCache NAS-Bucket kopieren. Das Kopieren von einem S3 NAS-Bucket, der auf einem FlexVol Volume basiert, in einen FlexCache NAS-Bucket, zwischen zwei FlexCache NAS-Buckets oder von einem FlexCache NAS-Bucket in einen Nicht-FlexCache NAS-Bucket wird nicht unterstützt.

ONTAP 9.20.1 bietet Unterstützung für flexible Prüfsummen mithilfe des CRC-64NVME Algorithmus für S3

NAS-Buckets. ONTAP validiert, speichert und gibt Prüfsummen zurück, wenn Clients Prüfsummen-Header in Anfragen einfügen. Die folgenden Operationen unterstützen flexible Prüfsummen-Header:

- PutObject
- CreateMultipartUpload
- UploadPart
- CompleteMultipartUpload
- CopyObject
- UploadPartCopy
- GetObject
- HeadObject
- ListObjectsV2
- ListParts

Unterstützt werden nur der CRC-64NVME-Algorithmus und der Prüfsummentyp FULL_OBJECT. Flexible Prüfsummenunterstützung ist nur für S3 NAS Buckets verfügbar.

ONTAP 9.14.1

ONTAP 9.14.1 bietet Unterstützung für S3 Object Lock.

Legal hold-Operationen (Sperren ohne festgelegte Aufbewahrungszeiten) sind nicht unterstützt.

- GetObjectLockConfiguration
- GetObjectRetention
- PutObjectLockConfiguration
- PutObjectRetention

ONTAP 9.13.1

ONTAP 9.13.1 bietet Unterstützung für das Bucket Lifecycle Management.

- DeleteBucketLifecycleConfiguration
- GetBucketLifecycleConfiguration
- PutBucketLifecycleConfiguration

ONTAP 9.12.1

ONTAP 9.12.1 bietet Unterstützung für Bucket-Richtlinien und die Möglichkeit, Objekte zu kopieren.

- DeleteBucketPolicy
- GetBucketPolicy
- PutBucketPolicy
- CopyObject
- UploadPartCopy

ONTAP 9.11.1

ONTAP 9.11.1 bietet Unterstützung für Versionierung, vorab signierte URLs, Chunked Uploads und

Unterstützung für gängige S3-Aktionen wie das Erstellen und Löschen von Buckets mit S3-APIs.

- ONTAP S3 bietet Unterstützung für das Signieren von Anfragen für Chunked Uploads unter Verwendung von `x-amz-content-sha256: STREAMING-AWS4-HMAC-SHA256-PAYLOAD`
- ONTAP S3 unterstützt jetzt Clientanwendungen, die vorab signierte URLs verwenden, um Objekte freizugeben oder anderen Benutzern das Hochladen von Objekten zu ermöglichen, ohne dass Benutzeranmeldeinformationen erforderlich sind.
- CreateBucket
- DeleteBucket
- GetBucketVersioning
- ListBucketVersions
- PutBucket
- PutBucketVersioning
- DeleteObjects
- ListObjectVersions

> Da die zugrundeliegende FlexGroup erst erstellt wird, wenn der erste Bucket erstellt wird, muss zunächst ein Bucket in ONTAP erstellt werden, bevor ein externer Client mit CreateBucket einen Bucket erstellen kann.

ONTAP 9.10.1

ONTAP 9.10.1 bietet Unterstützung für SnapMirror S3 und GetBucketLocation.

- GetBucketLocation

ONTAP 9.9.1

ONTAP 9.9.1 erweitert ONTAP S3 um Unterstützung für Objektmetadaten und Tagging.

- PutObject und CreateMultipartUpload enthalten jetzt Schlüssel-Wert-Paare mit `x-amz-meta-<key>`. Zum Beispiel: `x-amz-meta-project: ontap_s3`.
- GetObject und HeadObject geben nun benutzerdefinierte Metadaten zurück.

Tags können auch mit Buckets verwendet werden. Im Gegensatz zu Metadaten können Tags unabhängig von Objekten gelesen werden mit:

- PutObjectTagging
- GetObjectTagging
- DeleteObjectTagging

ONTAP S3 Interoperabilität

Der ONTAP S3 Server interagiert normal mit anderen ONTAP Funktionen, außer wie in dieser Tabelle angegeben.

Merkmalsbereich	Unterstützt	Nicht unterstützt
Cloud Volumes ONTAP	• Azure Clients in ONTAP 9.9.1 und späteren Versionen • AWS Clients in ONTAP 9.11.0 und späteren Versionen • Google Cloud Clients in ONTAP 9.12.1 und späteren Versionen	• Cloud Volumes ONTAP für jeden Client in ONTAP 9.8 und früheren Versionen
Datenschutz	• Cloud Sync • Objektsperre; Governance und Compliance (beginnend mit ONTAP 9.14.1) • "Objektversionierung" (beginnend mit ONTAP 9.11.1) • "SnapMirror S3" (beginnend mit ONTAP 9.10.1) • SnapMirror (nur NAS-Volumes; ab ONTAP 9.12.1) • SnapLock (nur NAS-Volumes; ab ONTAP 9.14.1)	• Erasure Coding • NDMP • SMTape • SnapMirror (synchron und asynchron) • SnapMirror Cloud • SVM Disaster Recovery • SyncMirror (außer in MetroCluster Konfigurationen)
Verschlüsselung	• NetApp Aggregate Encryption (NAE) • NetApp Volume Encryption (NVE) • NetApp Storage Encryption (NSE) • TLS/SSL	• SLAG
MetroCluster Umgebungen	• Bucket-Lebenszyklusmanagement (ab ONTAP 9.20.1) • SnapMirror S3 (ab ONTAP 9.20.1) • SyncMirror (gespiegelte MetroCluster Aggregate ab ONTAP 9.14.1) • Ungespiegelte MetroCluster Aggregates (beginnend mit ONTAP 9.12.1)	-

Merkmalsbereich	Unterstützt	Nicht unterstützt
Speichereffizienz	• Deduplizierung • Komprimierung • Verdichtung	• Effizienzgewinne auf Aggregatebene (Mitglieder, die demselben Aggregat angehören, können die volumenübergreifende Deduplizierung nutzen, Mitglieder, die verschiedenen Aggregaten angehören, jedoch nicht) • Volume-Klon des FlexGroup Volume, das ONTAP S3-Buckets enthält • FlexClone technology (Volumes, Dateien und LUNs)
Quality of Service (QoS)	• QoS-Maximum (Obergrenze) • QoS-Mindestwerte (Untergrenzen) • Verschachtelte QoS-Richtlinien "Einschränkungen bei der Zuweisung von QoS-Richtliniengruppen"	
FabricPool	• FabricPool Cloud-Tier ("nur nativ S3") • FabricPool lokale Ebene ("Nur NAS-Volumes")	• FabricPool Cloud-Tier (nur NAS-Volumes) • FabricPool lokale Tier (nur natives S3)
Zusätzliche Funktionen	• Die Verschiebung von Volumes wird für einzelne Mitgliedsvolumes unterstützt, aus denen ein FlexGroup Volume besteht. • "Audit S3-Ereignisse" (beginnend mit ONTAP 9.10.1) • "Bucket Lifecycle-Management" (beginnend mit ONTAP 9.13.1) • "FlexCache Volumes" (beginnend mit ONTAP 9.18.1)	• FPolicy • Qtrees • Kontingente

Validierte Drittanbieterlösungen mit S3 in ONTAP

S3 ist ein universeller Standard und dies ist keine umfassende Liste der unterstützten Anwendungen, sondern nur eine Liste von Lösungen, die in Zusammenarbeit mit den jeweiligen Partnern validiert wurden. Falls die gesuchte Lösung nicht aufgeführt ist, kann Ihr NetApp Account Representative kontaktiert werden.

Drittanbieterlösungen, validiert mit nativen S3-Buckets

- Amazon SageMaker
- Apache Hadoop S3A Client
- Apache Kafka
- Apache Spark
- Commvault (V11)
- Confluent Kafka
- NetBackup
- Red Hat Quay
- Rubrik
- Snowflake
- Trino
- Veeam (V12)

Diese Lösungen sind speziell für die Verwendung von nativen S3-Buckets in ONTAP validiert. Einige dieser Lösungen, wie beispielsweise solche im Zusammenhang mit Versionierung, Objektsperren und anderen Funktionen, werden bei der Verwendung von "S3 NAS Buckets (S3 in Multiprotokoll NAS Volumes)" nicht unterstützt.

Konfigurieren

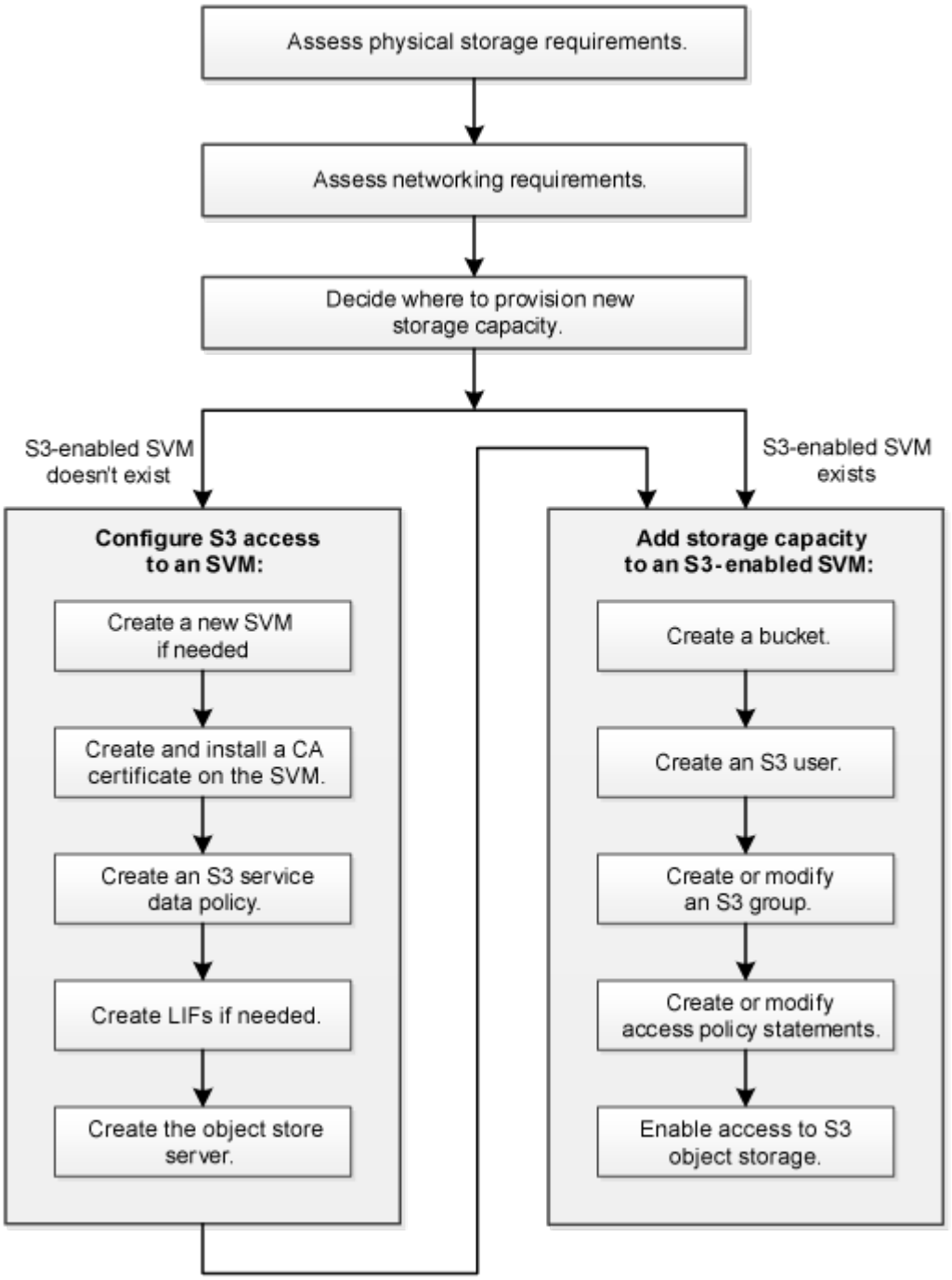
Zum S3-Konfigurationsprozess

ONTAP S3 Konfigurationsworkflow

Die Konfiguration von S3 beinhaltet die Beurteilung der physischen Speicher- und Netzwerkanforderungen sowie die Auswahl eines Workflows, der auf Ihr Ziel zugeschnitten ist: die Konfiguration des S3-Zugriffs auf eine neue oder bestehende SVM oder das Hinzufügen eines Buckets und von Benutzern zu einer bestehenden SVM, die bereits vollständig für den S3-Zugriff konfiguriert ist.

Die Konfiguration des Network Time Protocol (NTP) ist erforderlich, um die Zeitsynchronisierung zwischen Clustern und Clients sicherzustellen. Für den Clientzugriff ist häufig ein gültiger Zeitstempel mit einer Differenz von mindestens 15 Minuten zwischen dem ONTAP S3 Objektspeicher und dem Client erforderlich. "Informationen zur Konfiguration von NTP".

Wenn Sie den S3-Zugriff auf eine neue Storage-VM mithilfe des System Manager konfigurieren, werden Sie aufgefordert, Zertifikats- und Netzwerkinformationen einzugeben, und die Storage-VM sowie der S3-Objektspeicherserver werden in einem einzigen Vorgang erstellt.



Physische Speicheranforderungen für ONTAP S3 bewerten

Bevor S3-Speicher für Clients bereitgestellt wird, muss sichergestellt sein, dass in bestehenden Aggregaten ausreichend Speicherplatz für den neuen Objektspeicher vorhanden ist. Ist dies nicht der Fall, können Festplatten zu bestehenden Aggregaten hinzugefügt oder neue Aggregate des gewünschten Typs und Speicherorts erstellt werden.

Über diese Aufgabe

Wenn Sie in einer S3-fähigen SVM einen S3-Bucket erstellen, wird ein FlexGroup Volume "automatisch erstellt" zur Unterstützung des Buckets erstellt. Sie können ONTAP die zugrunde liegenden Aggregate und

FlexGroup Komponenten automatisch auswählen lassen (Standard) oder Sie können die zugrunde liegenden Aggregate und FlexGroup Komponenten selbst auswählen.

Wenn Sie die Aggregate und FlexGroup Komponenten festlegen – beispielsweise, wenn bestimmte Leistungsanforderungen an die zugrunde liegenden Datenträger bestehen –, sollte sichergestellt werden, dass die Aggregatkonfiguration den Best-Practice-Richtlinien für die Bereitstellung eines FlexGroup Volumes entspricht. Weitere Informationen:

- "FlexGroup Volumenmanagement"
- "NetApp Technical Report 4571-a: Die wichtigsten Best Practices für NetApp ONTAP FlexGroup Volumes"

Wenn Sie Buckets von Cloud Volumes ONTAP bereitstellen, wird dringend empfohlen, die zugrunde liegenden Aggregate manuell auszuwählen, um sicherzustellen, dass sie nur einen Knoten verwenden. 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. Informationen dazu "Erstellen von Buckets für Cloud Volumes ONTAP".

Sie können den ONTAP S3 Server verwenden, um eine lokale FabricPool Kapazitäts-Tier zu erstellen, das heißt im selben Cluster wie das Performance-Tier. Dies kann beispielsweise nützlich sein, wenn SSD-Festplatten an ein HA-Paar angeschlossen sind und *kalte* Daten auf HDD-Festplatten in einem anderen HA-Paar ausgelagert werden sollen. In diesem Anwendungsfall sollten sich der S3 Server und der Bucket mit dem lokalen Kapazitäts-Tier daher in einem anderen HA-Paar als das Performance-Tier befinden. Lokales Tiering wird auf Ein-Knoten- und Zwei-Knoten-Clustern nicht unterstützt.

Schritte

1. Anzeigen des verfügbaren Speicherplatzes in bestehenden Aggregaten:

   ```
   storage aggregate show
   ```

   Falls ein Aggregat mit ausreichend Speicherplatz oder der erforderlichen Knotenposition vorhanden ist, sollte dessen Name für die S3-Konfiguration festgehalten werden.

   ```
   cluster-1::> storage aggregate show
   Aggregate     Size Available Used% State   #Vols  Nodes  RAID Status
   --------- -------- --------- ----- ------- ------ ------ -----------
   aggr_0     239.0GB   11.13GB   95% online       1 node1  raid_dp,
                                                            normal
   aggr_1     239.0GB   11.13GB   95% online       1 node1  raid_dp,
                                                            normal
   aggr_2     239.0GB   11.13GB   95% online       1 node2  raid_dp,
                                                            normal
   aggr_3     239.0GB   11.13GB   95% online       1 node2  raid_dp,
                                                            normal
   aggr_4     239.0GB   238.9GB   95% online       5 node3  raid_dp,
                                                            normal
   aggr_5     239.0GB   239.0GB   95% online       4 node4  raid_dp,
                                                            normal
   6 entries were displayed.
   ```

2. Falls keine Aggregate mit ausreichend Speicherplatz oder der erforderlichen Knotenposition vorhanden sind, können Festplatten zu einem bestehenden Aggregat mit dem `storage aggregate add-disks` Befehl hinzugefügt werden oder ein neues Aggregat mit dem `storage aggregate create` Befehl erstellt werden.

Verwandte Informationen

- "storage aggregate add-disks"
- "Speicheraggregat erstellen"

ONTAP S3 Netzwerkanforderungen beurteilen

Bevor S3-Speicher für Clients bereitgestellt wird, ist zu überprüfen, dass die Netzwerkkonfiguration korrekt ist, sodass die S3-Bereitstellungsanforderungen erfüllt werden.

Bevor Sie beginnen

Die folgenden Cluster Netzwerkobjekte müssen konfiguriert werden:

- Physische und logische Ports
- Broadcast-Domains
- Subnetze (falls erforderlich)
- IPspaces (falls erforderlich, zusätzlich zum Standard IPspace)
- Failover-Gruppen (falls erforderlich, zusätzlich zur standardmäßigen Failover-Gruppe für jede Broadcast-Domäne)
- Externe Firewalls

Über diese Aufgabe

Für Remote FabricPool Kapazitätsstufen (Cloud) und Remote-S3-Clients ist eine Daten-SVM zu verwenden und Daten-LIFs sind zu konfigurieren. Für FabricPool Cloud-Tiers sind außerdem Intercluster-LIFs zu konfigurieren, Cluster-Peering ist nicht erforderlich.

Für lokale FabricPool Kapazitätsebenen muss die System-SVM (genannt “Cluster”) verwendet werden, aber es bestehen zwei Optionen für die LIF-Konfiguration:

- Sie können die Cluster-LIFs verwenden.

  Bei dieser Option ist keine weitere LIF-Konfiguration erforderlich, aber der Datenverkehr auf den Cluster-LIFs wird zunehmen. Außerdem ist die lokale Tier für andere Cluster nicht zugänglich.

- Sie können Daten- und Intercluster-LIFs verwenden.

  Diese Option erfordert zusätzliche Konfigurationen, einschließlich der Aktivierung der LIFs für das S3-Protokoll, aber die lokale Ebene ist auch als Remote FabricPool Cloud-Ebene für andere Cluster zugänglich.

Schritte

1. Die verfügbaren physischen und virtuellen Ports werden angezeigt:

   ```
   network port show
   ```

- Wenn möglich, ist der Port mit der höchsten Geschwindigkeit für das Datennetzwerk zu verwenden.
- Alle Komponenten im Datennetzwerk müssen für eine optimale Leistung die gleiche MTU-Einstellung haben.

2. Wenn die Verwendung eines Subnetznamens zur Zuweisung der IP-Adresse und des Netzwerkmaskenwerts für eine LIF vorgesehen ist, sollte überprüft werden, ob das Subnetz existiert und ausreichend Adressen verfügbar sind:

   `network subnet show`

   Subnetze enthalten einen Pool von IP-Adressen, die zum selben Layer-3-Subnetz gehören. Subnetze werden mit dem `network subnet create` Befehl erstellt.

   Weitere Informationen zu `network subnet show` finden sich in der "ONTAP-Befehlsreferenz".

3. Verfügbare IPspaces anzeigen:

   `network ipspace show`

   Sie können den Standard-IPspace oder einen benutzerdefinierten IPspace verwenden.

4. Wenn Sie IPv6-Adressen verwenden möchten, sollte überprüft werden, ob IPv6 auf dem Cluster aktiviert ist:

   `network options ipv6 show`

   Bei Bedarf kann IPv6 mit dem `network options ipv6 modify` Befehl aktiviert werden.

Verwandte Informationen

- "Netzwerkport anzeigen"
- "Netzwerkoptionen IPv6"
- "network ipspace show"
- "Netzwerk-Subnetz erstellen"

Festlegung des Standorts für die Bereitstellung neuer ONTAP S3-Speicherkapazität

Bevor Sie einen neuen S3-Bucket erstellen, muss entschieden werden, ob er in einer neuen oder in einer bestehenden SVM platziert wird. Diese Entscheidung bestimmt den Workflow.

Auswahlmöglichkeiten

- Wenn ein Bucket in einer neuen SVM oder einer SVM bereitgestellt werden soll, die nicht für S3 aktiviert ist, sind die Schritte in den folgenden Abschnitten zu befolgen.

  "Eine SVM für S3 erstellen"

  "Einen Bucket für S3 erstellen"

  Obwohl S3 in einer SVM zusammen mit NFS und SMB koexistieren kann, kann die Erstellung einer neuen SVM in Betracht gezogen werden, wenn eine der folgenden Bedingungen zutrifft:

  - S3 wird zum ersten Mal auf einem Cluster aktiviert.

- Sie haben bereits SVMs in einem Cluster, in dem Sie die S3-Unterstützung nicht aktivieren möchten.
- Sie haben eine oder mehrere S3-fähige SVMs in einem Cluster und möchten einen weiteren S3-Server mit anderen Leistungseigenschaften. Nach der Aktivierung von S3 auf der SVM erfolgt die Bereitstellung eines Buckets.

- Wenn der erste Bucket oder ein zusätzlicher Bucket auf einer bestehenden S3-fähigen SVM bereitgestellt werden soll, sind die Schritte im folgenden Thema zu befolgen.

  "Einen Bucket für S3 erstellen"

S3-Zugriff auf eine SVM konfigurieren

Eine SVM für ONTAP S3 erstellen

Obwohl S3 in einer SVM mit anderen Protokollen koexistieren kann, kann es sinnvoll sein, eine neue SVM zu erstellen, um den Namensraum und die Arbeitslast zu isolieren.

Über diese Aufgabe

Wenn Sie S3 Objektspeicher ausschließlich über eine SVM bereitstellen, benötigt der S3 Server keine DNS-Konfiguration. Wenn jedoch andere Protokolle verwendet werden, kann eine DNS-Konfiguration auf der SVM sinnvoll sein.

Wenn Sie den S3-Zugriff auf eine neue Storage-VM mithilfe des System Manager konfigurieren, werden Sie aufgefordert, Zertifikats- und Netzwerkinformationen einzugeben, und die Storage-VM sowie der S3-Objektspeicherserver werden in einem einzigen Vorgang erstellt.

Beispiel 1. Schritte

System Manager

Sie sollten darauf vorbereitet sein, den S3-Servernamen als vollqualifizierten Domänennamen (FQDN) einzugeben, den Clients für den S3-Zugriff verwenden. Der FQDN des S3-Servers darf nicht mit einem Bucket-Namen beginnen.

Sie sollten darauf vorbereitet sein, IP-Adressen für die Schnittstellenrolle Data einzugeben.

Wenn Sie ein von einer externen Zertifizierungsstelle signiertes Zertifikat verwenden, erfolgt während dieses Vorgangs eine Aufforderung zur Eingabe; alternativ besteht die Möglichkeit, ein systemgeneriertes Zertifikat zu verwenden.

1. S3 auf einer Storage-VM aktivieren.

   a. Eine neue Storage-VM hinzufügen: **Speicher > Storage-VMs** auswählen und dann auf **Hinzufügen** klicken.

      Falls es sich um ein neues System ohne vorhandene Storage-VMs handelt: **Dashboard > Protokolle konfigurieren** auswählen.

   Wenn Sie einen S3-Server zu einer bestehenden Storage-VM hinzufügen, auf **Speicher > Storage-VMs** klicken, eine Storage-VM auswählen, auf **Einstellungen** klicken und dann ⚙ unter **S3** klicken.

   a. **S3 aktivieren** auswählen und anschließend den S3-Servernamen eingeben.

   b. Wählen Sie den Zertifikatstyp aus.

Unabhängig davon, ob ein systemgeneriertes Zertifikat oder ein eigenes ausgewählt wird, ist es für den Clientzugriff erforderlich.

c. Die Netzwerkschnittstellen eingeben.

2. Wenn das systemgenerierte Zertifikat ausgewählt wurde, werden die Zertifikatsinformationen angezeigt, sobald die Erstellung der neuen Storage-VM bestätigt ist. **Herunterladen** kann ausgewählt und das Zertifikat für den Clientzugriff gespeichert werden.
   - Der geheime Schlüssel wird nicht erneut angezeigt.
   - Falls Sie die Zertifikatsinformationen erneut benötigen: **Speicher > Speicher-VMs** auswählen, die Speicher-VM auswählen und auf **Einstellungen** klicken.

CLI

1. Es sollte überprüft werden, ob S3 auf Ihrem Cluster lizenziert ist:

```
system license show -package s3
```

   Falls dies nicht der Fall ist, kontaktieren Sie Ihren Vertriebsmitarbeiter.

2. Eine SVM erstellen:

```
vserver create -vserver <svm_name> -subtype default -rootvolume
<root_volume_name> -aggregate <aggregate_name> -rootvolume-security
-style unix -language C.UTF-8 -data-services <data-s3-server>
-ipspace <ipspace_name>
```

   - Die UNIX-Einstellung für die `-rootvolume-security-style` Option verwenden.
   - Die Standardoption C.UTF-8 `-language` kann verwendet werden.
   - Die `ipspace` Einstellung ist optional.

3. Die Konfiguration und der Status der neu erstellten SVM können überprüft werden:

```
vserver show -vserver <svm_name>
```

   Das `Vserver Operational State`Feld muss den `running`Status anzeigen. Wenn es den `initializing`Status anzeigt, bedeutet dies, dass ein Zwischenvorgang wie die Erstellung des Root-Volumes fehlgeschlagen ist und die SVM gelöscht und neu erstellt werden muss.

Beispiele

Der folgende Befehl erstellt eine SVM für den Datenzugriff im IPspace ipspaceA:

```
cluster-1::> vserver create -vserver svm1.example.com -rootvolume
root_svm1 -aggregate aggr1 -rootvolume-security-style unix -language
C.UTF-8 -data-services data-s3-server -ipspace ipspaceA

[Job 2059] Job succeeded:
```

```
Vserver creation completed
```

Der folgende Befehl zeigt, dass eine SVM mit einem Root-Volume von 1 GB erstellt wurde, das automatisch gestartet wurde und sich im `running` Status befindet. Das Root-Volume verfügt über eine Standard-Export-Richtlinie, die keine Regeln enthält, sodass das Root-Volume bei der Erstellung nicht exportiert wird. Standardmäßig wird das vsadmin-Benutzerkonto erstellt und befindet sich im `locked` Status. Die vsadmin-Rolle ist dem Standard-vsadmin-Benutzerkonto zugewiesen.

```
cluster-1::> vserver show -vserver svm1.example.com
                                     Vserver: svm1.example.com
                                Vserver Type: data
                             Vserver Subtype: default
                                Vserver UUID: b8375669-19b0-11e5-b9d1-
00a0983d9736
                                 Root Volume: root_svm1
                                   Aggregate: aggr1
                                  NIS Domain: -
                  Root Volume Security Style: unix
                                 LDAP Client: -
               Default Volume Language Code: C.UTF-8
                             Snapshot Policy: default
                                     Comment:
                                Quota Policy: default
                  List of Aggregates Assigned: -
 Limit on Maximum Number of Volumes allowed: unlimited
                        Vserver Admin State: running
                  Vserver Operational State: running
   Vserver Operational State Stopped Reason: -
                           Allowed Protocols: nfs, cifs
                        Disallowed Protocols: -
                            QoS Policy Group: -
                                 Config Lock: false
                                IPspace Name: ipspaceA
```

Erstellen und Installieren eines CA-Zertifikats auf einer ONTAP S3-fähigen SVM

S3-Clients benötigen ein Zertifikat einer Zertifizierungsstelle (CA), um HTTPS-Datenverkehr an die S3-fähige SVM zu senden. CA-Zertifikate schaffen eine Vertrauensbeziehung zwischen Clientanwendungen und dem ONTAP Objektspeicher-Server. Ein CA-Zertifikat sollte auf ONTAP installiert werden, bevor es als Objektspeicher für Remote-Clients genutzt wird.

Über diese Aufgabe

Obwohl es möglich ist, einen S3-Server so zu konfigurieren, dass er nur HTTP verwendet, und obwohl es möglich ist, Clients ohne CA-Zertifikatsanforderung zu konfigurieren, gilt es als bewährte Methode, den

HTTPS-Datenverkehr zu ONTAP S3-Servern mit einem CA-Zertifikat abzusichern.

Ein CA-Zertifikat ist für einen lokalen Tiering-Anwendungsfall, bei dem der IP-Verkehr ausschließlich über Cluster-LIFs erfolgt, nicht erforderlich.

Die Anweisungen in diesem Verfahren erstellen und installieren ein selbstsigniertes ONTAP-Zertifikat. Obwohl ONTAP selbstsignierte Zertifikate generieren kann, wird die Verwendung signierter Zertifikate von einer Drittanbieter-Zertifizierungsstelle als empfohlene Best Practice angesehen; weitere Informationen enthält die Administrator-Authentifizierungsdokumentation.

"Administratorauthentifizierung und RBAC"

Weitere Informationen zu `security certificate` und zusätzlichen Konfigurationsoptionen finden sich in der "ONTAP-Befehlsreferenz".

Schritte

1. Ein selbstsigniertes digitales Zertifikat erstellen:

   `security certificate create -vserver` *`svm_name`* `-type root-ca -common-name` *`ca_cert_name`*

   Die `-type root-ca`Option erstellt und installiert ein selbstsigniertes digitales Zertifikat, das zum Signieren anderer Zertifikate dient, indem es als Zertifizierungsstelle (CA) fungiert.

   Die `-common-name`Option erstellt den Certificate Authority (CA)-Namen der SVM und wird beim Generieren des vollständigen Namens des Zertifikats verwendet.

   Die Standardzertifikatsgröße beträgt 2048 Bit.

   Beispiel

   ```
   cluster-1::> security certificate create -vserver svm1.example.com -type
   root-ca -common-name svm1_ca

   The certificate's generated name for reference:
   svm1_ca_159D1587CE21E9D4_svm1_ca
   ```

   Wenn der generierte Name des Zertifikats angezeigt wird, sollte dieser für spätere Schritte in diesem Verfahren gespeichert werden.

   Weitere Informationen zu `security certificate create` finden sich in der "ONTAP-Befehlsreferenz".

2. Eine Zertifikatsignierungsanforderung generieren:

   `security certificate generate-csr -common-name` *`s3_server_name`* `[additional_options]`

   Der `-common-name`Parameter für die Signierungsanforderung muss der S3-Servername (FQDN) sein.

   Sie können bei Bedarf den Standort und weitere detaillierte Informationen zur SVM angeben.

Der `-dns-name`Parameter wird häufig von Clients benötigt, um die Subject Alternate Name-Erweiterung anzugeben, die eine Liste von DNS-Namen bereitstellt.

Der `-ipaddr`Parameter wird häufig von Clients benötigt, um die Subject Alternate Name-Erweiterung anzugeben, die eine Liste von IP-Adressen bereitstellt.

Sie werden aufgefordert, eine Kopie Ihrer Zertifikatsanforderung und Ihres privaten Schlüssels für zukünftige Referenz aufzubewahren.

Weitere Informationen zu `security certificate generate-csr` finden sich in der "ONTAP-Befehlsreferenz".

3. Der CSR wird mit SVM_CA signiert, um das Zertifikat des S3 Servers zu generieren:

   `security certificate sign -vserver` *`svm_name`* `-ca` *`ca_cert_name`* `-ca-serial` *`ca_cert_serial_number`* `[additional_options]`

   Geben Sie die Befehlsoptionen ein, die Sie in den vorherigen Schritten verwendet haben:

   - `-ca` — der gebräuchliche Name der CA, den Sie in Schritt 1 eingegeben haben.
   - `-ca-serial` — die CA-Seriennummer aus Schritt 1. Wenn beispielsweise der Name des CA-Zertifikats svm1_ca_159D1587CE21E9D4_svm1_ca ist, ist die Seriennummer 159D1587CE21E9D4.

     Standardmäßig läuft das signierte Zertifikat nach 365 Tagen ab. Es kann ein anderer Wert ausgewählt und weitere Signaturdetails angegeben werden.

     Wenn Sie dazu aufgefordert werden, kopieren und geben Sie die in Schritt 2 gespeicherte Zertifikatsanforderungszeichenfolge ein.

   Ein signiertes Zertifikat wird angezeigt; dieses für die spätere Verwendung speichern.

4. Das signierte Zertifikat auf der S3-fähigen SVM installieren:

   `security certificate install -type server -vserver` *`svm_name`*

   Bei Aufforderung sind das Zertifikat und der private Schlüssel einzugeben.

   Sie haben die Möglichkeit, Zwischenzertifikate einzugeben, falls eine Zertifikatskette gewünscht ist.

   Wenn der private Schlüssel und das von der Zertifizierungsstelle signierte digitale Zertifikat angezeigt werden, sollten diese für eine spätere Referenz gespeichert werden.

5. Öffentliches Schlüsselzertifikat:

   `security certificate show -vserver` *`svm_name`* `-common-name` *`ca_cert_name`* `-type root-ca -instance`

   Das öffentliche Schlüsselzertifikat für die spätere Client-seitige Konfiguration speichern.

   Beispiel

   ```
   cluster-1::> security certificate show -vserver svm1.example.com -common
   -name svm1_ca -type root-ca  -instance
   ```

```
                    Name of Vserver: svm1.example.com
          FQDN or Custom Common Name: svm1_ca
        Serial Number of Certificate: 159D1587CE21E9D4
              Certificate Authority: svm1_ca
                Type of Certificate: root-ca
     (DEPRECATED)-Certificate Subtype: -
            Unique Certificate Name: svm1_ca_159D1587CE21E9D4_svm1_ca
Size of Requested Certificate in Bits: 2048
             Certificate Start Date: Thu May 09 10:58:39 2020
         Certificate Expiration Date: Fri May 08 10:58:39 2021
              Public Key Certificate: -----BEGIN CERTIFICATE-----
MIIDZ ...==
-----END CERTIFICATE-----
                        Country Name: US
             State or Province Name:
                       Locality Name:
                  Organization Name:
                  Organization Unit:
Contact Administrator's Email Address:
                           Protocol: SSL
                    Hashing Function: SHA256
            Self-Signed Certificate: true
      Is System Internal Certificate: false
```

Verwandte Informationen

- "Sicherheitszertifikat installieren"
- "Sicherheitszertifikat anzeigen"
- "Sicherheitszertifikat signieren"

Die ONTAP S3 Service-Datenrichtlinie erstellen

Sie können Dienstrichtlinien für S3-Daten- und Verwaltungsdienste erstellen. Eine S3-Daten-Dienstrichtlinie ist erforderlich, um den S3-Datenverkehr auf LIFs zu ermöglichen.

Über diese Aufgabe

Eine S3-Datenrichtlinie für Dienste ist erforderlich, wenn Sie Daten-LIFs und Intercluster-LIFs verwenden. Sie ist nicht erforderlich, wenn Sie Cluster-LIFs für den lokalen Tiering-Anwendungsfall verwenden.

Wenn für eine LIF eine Dienstrichtlinie festgelegt wird, wird diese Richtlinie verwendet, um eine Standardrolle, eine Failover-Richtlinie und eine Datenprotokollliste für die LIF zu erstellen.

Obwohl für SVMs und LIFs mehrere Protokolle konfiguriert werden können, ist es eine Best Practice, dass S3 das einzige Protokoll bei der Bereitstellung von Objektdaten ist.

Schritte

1. Die Berechtigungseinstellung auf „Erweitert“ ändern:

```
set -privilege advanced
```

2. Erstellen einer Dienstdatenrichtlinie:

   ```
   network interface service-policy create -vserver svm_name -policy policy_name
   -services data-core,data-s3-server
   ```

   Die `data-core`- und `data-s3-server`-Dienste sind die einzigen, die für die Aktivierung von ONTAP S3 erforderlich sind, obwohl bei Bedarf weitere Dienste eingeschlossen werden können.

   Weitere Informationen zu `network interface service-policy create` finden sich in der "ONTAP-Befehlsreferenz".

Daten-LIFs für ONTAP S3 erstellen

Wenn Sie eine neue SVM erstellt haben, sollten die dedizierten LIFs, die Sie für den S3-Zugriff erstellen, Daten-LIFs sein.

Bevor Sie beginnen

- Der zugrunde liegende physische oder logische Netzwerkport muss auf den administrativen `up` Status konfiguriert sein.
- Wenn geplant ist, einen Subnetznamen zu verwenden, um die IP-Adresse und den Netzwerkmaskenwert für ein LIF zuzuweisen, muss das Subnetz bereits existieren.

  Subnetze enthalten einen Pool von IP-Adressen, die zum selben Layer-3-Subnetz gehören. Sie werden mit dem `network subnet create` Befehl erstellt.

  Weitere Informationen zu `network subnet create` finden sich in der "ONTAP-Befehlsreferenz".

- Die LIF-Servicerichtlinie muss bereits existieren.
- Als Best Practice sollten LIFs, die für den Datenzugriff (data-s3-server) verwendet werden, und LIFs, die für Verwaltungsoperationen (management-https) verwendet werden, getrennt sein. Beide Dienste sollten nicht auf demselben LIF aktiviert sein.
- DNS-Einträge sollten nur die IP-Adressen der LIFs enthalten, denen ein data-s3-server zugeordnet ist. Wenn im DNS-Eintrag IP-Adressen anderer LIFs angegeben sind, können ONTAP S3-Anfragen von anderen Servern bearbeitet werden, was zu unerwarteten Antworten oder Datenverlust führen kann.

Über diese Aufgabe

- Sowohl IPv4- als auch IPv6-LIFs können auf demselben Netzwerkport erstellt werden.
- Wenn Sie eine große Anzahl von LIFs in Ihrem Cluster haben, kann die vom Cluster unterstützte LIF-Kapazität mit dem `network interface capacity show` Befehl und die von jedem Knoten unterstützte LIF-Kapazität mit dem `network interface capacity details show` Befehl (auf der erweiterten Berechtigungsstufe) überprüft werden.

  Weitere Informationen zu `network interface capacity show` und `network interface capacity details show` finden sich in der "ONTAP-Befehlsreferenz".

- Wenn Sie Remote-FabricPool-Kapazitäts-(Cloud)-Tiering aktivieren, müssen Sie auch Intercluster-LIFs konfigurieren.

Schritte

1. Eine LIF erstellen:

   `network interface create -vserver svm_name -lif lif_name -service-policy service_policy_names -home-node node_name -home-port port_name {-address IP_address -netmask IP_address | -subnet-name subnet_name} -firewall-policy data -auto-revert {true|false}`

   - `-home-node` ist der Knoten, zu dem die LIF zurückkehrt, wenn der `network interface revert` Befehl auf der LIF ausgeführt wird.

     Weitere Informationen zu `network interface revert` finden sich in der "ONTAP-Befehlsreferenz".

     Sie können auch angeben, ob die LIF mit der `-auto-revert` Option automatisch auf den Home-Node und Home-Port zurückkehren soll.

   - `-home-port` ist der physische oder logische Port, zu dem die LIF zurückkehrt, wenn der `network interface revert` Befehl auf der LIF ausgeführt wird.
   - Sie können eine IP-Adresse mit den `-address` und `-netmask` Optionen angeben oder die Zuweisung aus einem Subnetz mit der `-subnet_name` Option ermöglichen.
   - Wird ein Subnetz zur Bereitstellung der IP-Adresse und der Netzwerkmaske verwendet, wird, falls das Subnetz mit einem Gateway definiert wurde, beim Erstellen eines LIF mit diesem Subnetz automatisch eine Standardroute zu diesem Gateway zur SVM hinzugefügt.
   - Wenn Sie IP-Adressen manuell zuweisen (ohne Verwendung eines Subnetzes), müssen Sie möglicherweise eine Standardroute zu einem Gateway konfigurieren, falls sich Clients oder Domänencontroller in einem anderen IP-Subnetz befinden. Weitere Informationen zu `network route create` und zum Erstellen einer statischen Route innerhalb einer SVM finden sich im "ONTAP-Befehlsreferenz".
   - Für die `-firewall-policy` Option sollte derselbe Standardwert `data` wie für die LIF-Rolle verwendet werden.

     Bei Bedarf kann später eine benutzerdefinierte Firewall-Richtlinie erstellt und hinzugefügt werden.

     > ⓘ Ab ONTAP 9.10.1 sind Firewall-Richtlinien veraltet und vollständig durch LIF-Dienstrichtlinien ersetzt. Weitere Informationen finden sich unter "Firewall-Richtlinien für LIFs konfigurieren".

   - `-auto-revert`Hiermit kann festgelegt werden, ob ein Daten-LIF unter Umständen wie Systemstart, Änderungen am Status der Management-Datenbank oder beim Herstellen einer Netzwerkverbindung automatisch auf seinen Heimatknoten zurückkehrt. Die Standardeinstellung ist `false, sie kann jedoch je nach Netzwerkverwaltungsrichtlinien in Ihrer Umgebung auf `false` gesetzt werden.
   - Die `-service-policy` Option legt die von Ihnen erstellte Daten- und Verwaltungsdienstrichtlinie sowie alle weiteren benötigten Richtlinien fest.

2. Wenn Sie eine IPv6-Adresse in der `-address` Option zuweisen möchten:

   a. Mit dem `network ndp prefix show` Befehl lässt sich die Liste der auf verschiedenen Schnittstellen gelernten RA-Präfixe anzeigen.

      Der `network ndp prefix show` Befehl ist auf der Stufe „Erweiterte Berechtigungen“ verfügbar.

b. Verwenden Sie das Format `prefix:id`, um die IPv6-Adresse manuell zu erstellen.

`prefix` ist das Präfix, das auf verschiedenen Schnittstellen gelernt wird.

Zur Ableitung des `id`wird eine zufällige 64-Bit-Hexadezimalzahl gewählt.

3. Es kann mit dem `network interface show` Befehl überprüft werden, ob die LIF erfolgreich erstellt wurde.
4. Es sollte überprüft werden, ob die konfigurierte IP-Adresse erreichbar ist:

Zur Überprüfung einer…	Verwenden…
IPv4-Adresse	`network ping`
IPv6-Adresse	`network ping6`

Beispiele

Der folgende Befehl zeigt, wie ein S3-Daten-LIF erstellt wird, dem die `my-S3-policy` Dienstrichtlinie zugewiesen ist:

```
network interface create -vserver svm1.example.com -lif lif2 -home-node
node2 -homeport e0d -service-policy my-S3-policy -subnet-name ipspace1
```

Der folgende Befehl zeigt alle LIFs in cluster-1 an. Die Data LIFs datalif1 und datalif3 sind mit IPv4-Adressen konfiguriert, und datalif4 ist mit einer IPv6-Adresse konfiguriert:

```
cluster-1::> network interface show

            Logical    Status     Network          Current      Current Is
Vserver     Interface  Admin/Oper Address/Mask     Node         Port
Home
----------- ---------- ---------- ---------------- ------------ -------
----
cluster-1
            cluster_mgmt up/up    192.0.2.3/24     node-1       e1a
true
node-1
            clus1        up/up    192.0.2.12/24    node-1       e0a
true
            clus2        up/up    192.0.2.13/24    node-1       e0b
true
            mgmt1        up/up    192.0.2.68/24    node-1       e1a
true
node-2
            clus1        up/up    192.0.2.14/24    node-2       e0a
true
            clus2        up/up    192.0.2.15/24    node-2       e0b
```

```
true
            mgmt1        up/up    192.0.2.69/24    node-2       e1a
true
vs1.example.com
            datalif1     up/down  192.0.2.145/30   node-1       e1c
true
vs3.example.com
            datalif3     up/up    192.0.2.146/30   node-2       e0c
true
            datalif4     up/up    2001::2/64       node-2       e0c
true
5 entries were displayed.
```

Verwandte Informationen

- "Netzwerk-Ping"
- "Netzwerkschnittstelle"
- "network ndp prefix show"

Intercluster-LIFs für Remote FabricPool Tiering mit ONTAP S3 erstellen

Wenn Sie die Remote FabricPool Kapazitäts-Tiering (Cloud) mit ONTAP S3 aktivieren, müssen Intercluster-LIFs konfiguriert werden. Intercluster-LIFs können auf Ports konfiguriert werden, die mit dem Datennetzwerk gemeinsam genutzt werden. Dadurch wird die Anzahl der für die Intercluster-Vernetzung benötigten Ports reduziert.

Bevor Sie beginnen

- Der zugrunde liegende physische oder logische Netzwerkport muss auf den administrativen `up` Status konfiguriert sein.
- Die LIF-Servicerichtlinie muss bereits existieren.

Über diese Aufgabe

Intercluster LIFs sind weder für das lokale FabricPool Tiering noch für die Bereitstellung externer S3-Anwendungen erforderlich.

Schritte

1. Die Ports im Cluster werden aufgelistet:

   `network port show`

   Das folgende Beispiel zeigt die Netzwerkanschlüsse in `cluster01`:

   ```
   cluster01::> network port show
                                                                  Speed
   (Mbps)
   Node   Port      IPspace      Broadcast Domain Link   MTU    Admin/Oper
   ------ --------- ------------ ---------------- ----- -------
   ```

```
------------
cluster01-01
       e0a       Cluster      Cluster          up     1500   auto/1000
       e0b       Cluster      Cluster          up     1500   auto/1000
       e0c       Default      Default          up     1500   auto/1000
       e0d       Default      Default          up     1500   auto/1000
cluster01-02
       e0a       Cluster      Cluster          up     1500   auto/1000
       e0b       Cluster      Cluster          up     1500   auto/1000
       e0c       Default      Default          up     1500   auto/1000
       e0d       Default      Default          up     1500   auto/1000
```

Weitere Informationen zu `network port show` finden sich in der "ONTAP-Befehlsreferenz".

2. Intercluster-LIFs auf dem System-SVM erstellen:

   `network interface create -vserver Cluster -lif` *`LIF_name`* `-service-policy default-intercluster -home-node` *`node`* `-home-port` *`port`* `-address` *`port_IP`* `-netmask` *`netmask`*

   Das folgende Beispiel erstellt Intercluster-LIFs `cluster01_icl01` und `cluster01_icl02`:

```
cluster01::> network interface create -vserver Cluster -lif
cluster01_icl01 -service-
policy default-intercluster -home-node cluster01-01 -home-port e0c
-address 192.168.1.201
-netmask 255.255.255.0

cluster01::> network interface create -vserver Cluster -lif
cluster01_icl02 -service-
policy default-intercluster -home-node cluster01-02 -home-port e0c
-address 192.168.1.202
-netmask 255.255.255.0
```

   Weitere Informationen zu `network interface create` finden sich in der "ONTAP-Befehlsreferenz".

3. Es sollte überprüft werden, ob die Intercluster-LIFs erstellt wurden:

   `network interface show -service-policy default-intercluster`

```
cluster01::> network interface show -service-policy default-intercluster
            Logical    Status     Network            Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node          Port
Home
----------- ---------- ---------- ------------------ -------------
```

```
------- ----
cluster01
            cluster01_icl01
                       up/up      192.168.1.201/24   cluster01-01  e0c
true
            cluster01_icl02
                       up/up      192.168.1.202/24   cluster01-02  e0c
true
```

4. Es sollte sichergestellt werden, dass die Intercluster-LIFs redundant sind:

   `network interface show -service-policy default-intercluster -failover`

   Das folgende Beispiel zeigt, dass die Intercluster-LIFs `cluster01_icl01` und `cluster01_icl02` auf dem `e0c` Port auf den `e0d` Port übergehen.

```
cluster01::> network interface show -service-policy default-intercluster
-failover
         Logical         Home                  Failover        Failover
Vserver  Interface       Node:Port             Policy          Group
-------- --------------- --------------------- --------------- --------
cluster01
         cluster01_icl01 cluster01-01:e0c   local-only
192.168.1.201/24
                            Failover Targets: cluster01-01:e0c,
                                              cluster01-01:e0d
         cluster01_icl02 cluster01-02:e0c   local-only
192.168.1.201/24
                            Failover Targets: cluster01-02:e0c,
                                              cluster01-02:e0d
```

   Weitere Informationen zu `network interface show` finden sich in der "ONTAP-Befehlsreferenz".

ONTAP S3 Objektspeicher-Server erstellen

Der ONTAP Objektspeicher-Server verwaltet Daten als S3-Objekte, im Gegensatz zum Datei- oder Blockspeicher, der von ONTAP NAS- und SAN-Servern bereitgestellt wird.

Bevor Sie beginnen

Sie sollten darauf vorbereitet sein, den S3-Servernamen als vollqualifizierten Domänennamen (FQDN) anzugeben, den Clients für den S3-Zugriff verwenden. Der FQDN ist ab ONTAP 9.18.1 erforderlich. Der FQDN darf nicht mit einem Bucket-Namen beginnen. Beim Zugriff auf Buckets mit virtual-hosted-style wird der Servername als `mydomain.com` verwendet. Zum Beispiel `bucketname.mydomain.com`.

Sie benötigen ein selbstsigniertes CA-Zertifikat (das in den vorherigen Schritten erstellt wurde) oder ein von einem externen CA-Anbieter signiertes Zertifikat. Ein CA-Zertifikat ist für einen lokalen Tiering-Anwendungsfall, bei dem der IP-Verkehr ausschließlich über Cluster-LIFs erfolgt, nicht erforderlich.

Über diese Aufgabe

Wenn ein Objektspeicherserver erstellt wird, wird ein Root-Benutzer mit der UID 0 angelegt. Für diesen Root-Benutzer werden kein Zugriffsschlüssel und kein geheimer Schlüssel generiert. Der ONTAP Administrator muss den `object-store-server user regenerate-keys` Befehl ausführen, um den Zugriffsschlüssel und den geheimen Schlüssel für diesen Benutzer festzulegen.

> Als NetApp Best Practice sollte dieser Root-Benutzer nicht verwendet werden. Jede Clientanwendung, die den Zugriffsschlüssel oder den geheimen Schlüssel des Root-Benutzers verwendet, hat vollen Zugriff auf alle Buckets und Objekte im Objektspeicher.

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

Beispiel 2. Schritte

System Manager

Verwenden Sie dieses Verfahren, wenn Sie einen S3-Server zu einer bestehenden Storage-VM hinzufügen. Um einen S3-Server zu einer neuen Storage-VM hinzuzufügen, siehe "Eine Storage-SVM für S3 erstellen".

Sie sollten darauf vorbereitet sein, IP-Adressen für die Schnittstellenrolle Data einzugeben.

1. S3 auf einer vorhandenen Storage-VM aktivieren.
   a. Wählen Sie die Storage-VM aus: Klicken Sie auf **Storage > Storage VMs**, wählen Sie eine Storage-VM aus, klicken Sie auf **Einstellungen** und dann auf ⚙ unter **S3**.
   b. **S3 aktivieren** auswählen und anschließend den S3-Servernamen eingeben.
   c. Wählen Sie den Zertifikatstyp aus.

      Unabhängig davon, ob ein systemgeneriertes Zertifikat oder ein eigenes ausgewählt wird, ist es für den Clientzugriff erforderlich.

   d. Die Netzwerkschnittstellen eingeben.
2. Wenn das systemgenerierte Zertifikat ausgewählt wurde, werden die Zertifikatsinformationen angezeigt, sobald die Erstellung der neuen Storage-VM bestätigt ist. **Herunterladen** kann ausgewählt und das Zertifikat für den Clientzugriff gespeichert werden.
   - Der geheime Schlüssel wird nicht erneut angezeigt.
   - Falls Sie die Zertifikatsinformationen erneut benötigen: **Speicher > Speicher-VMs** auswählen, die Speicher-VM auswählen und auf **Einstellungen** klicken.

CLI

1. Den S3-Server erstellen:

   ```
   vserver object-store-server create -vserver svm_name -object-store-server
   s3_server_fqdn -certificate-name server_certificate_name -comment text
   [additional_options]
   ```

   Zusätzliche Optionen können beim Erstellen des S3-Servers oder jederzeit später angegeben werden.

   - Ab ONTAP 9.20.1 können Sie mit der Option `-default-bucket-size` die Größe von S3-Buckets festlegen, die ohne die Option `-size` erstellt werden. Diese Einstellung gilt für Buckets,

die mit der ONTAP CLI, der ONTAP REST API oder der S3 API erstellt werden. Vorhandene Buckets werden dadurch nicht geändert.

Nach dem Erstellen des S3-Servers lässt sich mit dem `vserver object-store-server modify`Befehl über die `-default-bucket-size`Option die Standardgröße für neue Buckets ändern.

- Wenn lokales Tiering konfiguriert wird, kann der SVM-Name entweder ein Daten-SVM-Name oder ein System-SVM-Name (Cluster-Name) sein.
- Der Zertifikatsname sollte der Name des Serverzertifikats (Endbenutzer- oder Blattzertifikat) sein und nicht der Name des Server-CA-Zertifikats (Zwischen- oder Stammzertifizierungsstellenzertifikat).
- HTTPS ist standardmäßig auf Port 443 aktiviert. Die Portnummer kann mit der `-secure -listener-port` Option geändert werden.

  Wenn HTTPS aktiviert ist, sind CA-Zertifikate für die korrekte Integration mit SSL/TLS erforderlich. Ab ONTAP 9.15.1 wird TLS 1.3 mit S3 Objektspeicher unterstützt.

- HTTP ist standardmäßig deaktiviert. Wenn aktiviert, hört der Server auf Port 80. HTTP kann mit der `-is-http-enabled` Option aktiviert oder die Portnummer mit der `-listener-port` Option geändert werden.

  Wenn HTTP aktiviert ist, werden Anfragen und Antworten im Klartext über das Netzwerk gesendet.

2. Es sollte überprüft werden, ob S3 konfiguriert ist:

```
vserver object-store-server show
```

Beispiel

Dieser Befehl überprüft die Konfigurationswerte aller Objektspeicherserver:

```
cluster1::> vserver object-store-server show

            Vserver: vs1

                      Object Store Server Name: s3.example.com
                          Administrative State: up
                        Listener Port For HTTP: 80
                   Secure Listener Port For HTTPS: 443
                                     HTTP Enabled: false
                                    HTTPS Enabled: true
             Certificate for HTTPS Connections: svm1_ca
                                       Comment: Server comment
```

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:

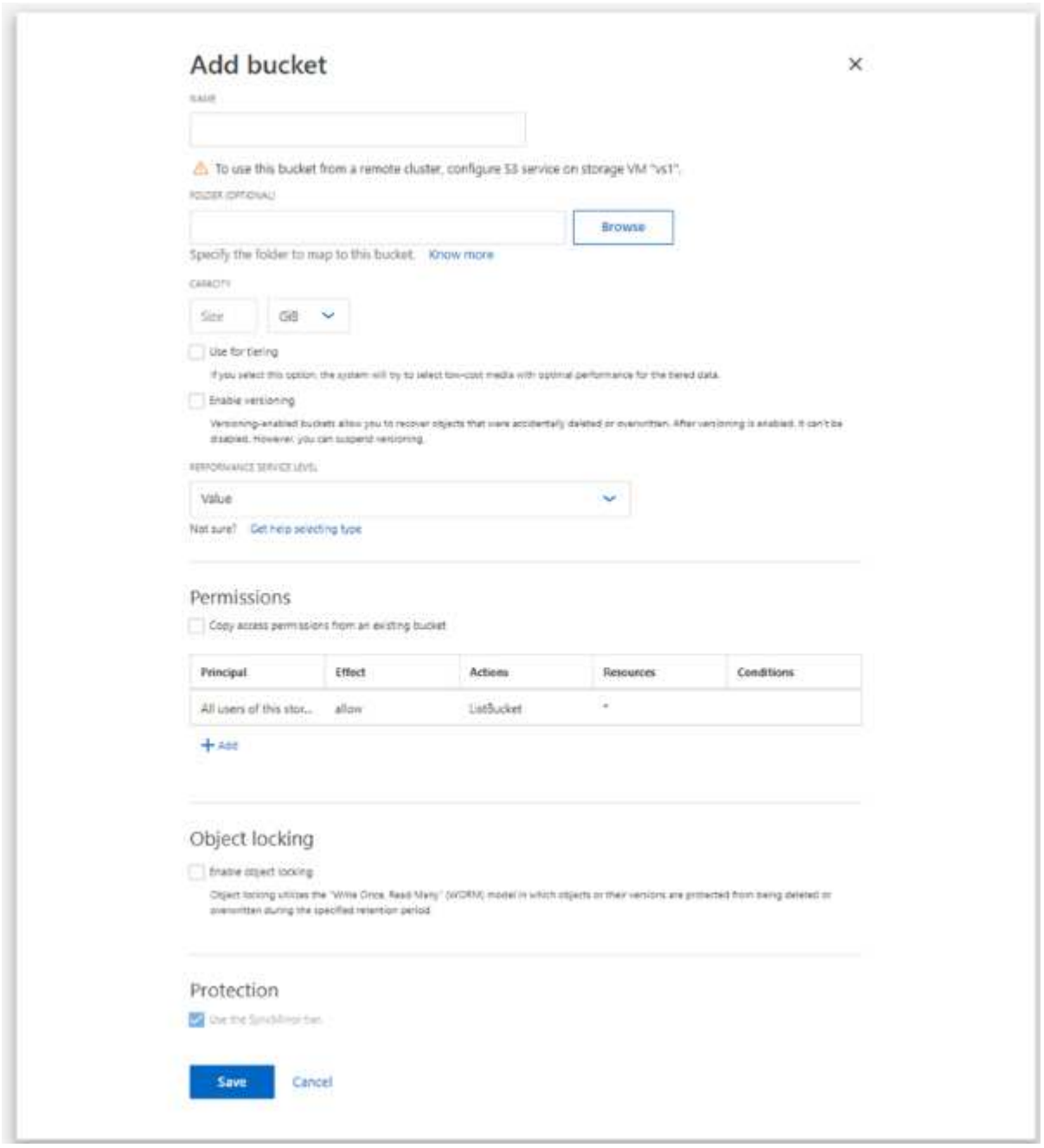
```
cluster-1::*> vserver object-store-server bucket create -vserver
svm1.example.com -bucket testbucket  -size 1TB -use-mirrored-aggregates
true
```

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
```

Zugriffsrichtlinien-Anweisungen erstellen oder ändern

Informationen zu ONTAP S3-Bucket- und Objektspeicher-Serverrichtlinien

Der Zugriff von Benutzern und Gruppen auf S3-Ressourcen wird durch Bucket- und Objektspeicher-Serverrichtlinien gesteuert. Bei einer geringen Anzahl von Benutzern oder Gruppen ist die Zugriffskontrolle auf Bucket-Ebene wahrscheinlich ausreichend, aber bei vielen Benutzern und Gruppen ist es einfacher, den Zugriff auf der Objektspeicher-Server-Ebene zu steuern.

Fügen Sie der standardmäßigen ONTAP S3-Bucket-Richtlinie Zugriffsregeln hinzu

Sie können der Standard-Bucket-Richtlinie Zugriffsregeln hinzufügen. Der Geltungsbereich der Zugriffskontrolle ist der enthaltende Bucket, daher ist sie am besten geeignet, wenn es nur einen Bucket gibt.

Bevor Sie beginnen

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

Benutzer oder Gruppen müssen bereits erstellt worden sein, bevor Berechtigungen vergeben werden können.

Über diese Aufgabe

Sie können neue Anweisungen für neue Benutzer und Gruppen hinzufügen oder die Attribute bestehender Anweisungen ändern. Weitere Informationen zu `vserver object-store-server bucket policy` finden sich in der "ONTAP-Befehlsreferenz".

Benutzer- und Gruppenberechtigungen können bei der Erstellung des Buckets oder bei Bedarf später erteilt werden. Auch die Bucket-Kapazität und die Zuordnung der QoS-Policy-Gruppe können angepasst werden.

Ab ONTAP 9.19.1 können Sie Bedingungen verwenden, um bedingte Schreibvorgänge für Objekt-Uploads und bedingte Löschvorgänge für Objekt-Löschungen zu erzwingen. Bedingte Schreib- und Löschvorgänge bieten eine Möglichkeit, das Überschreiben oder unbeabsichtigte Löschen von Objekten zu verhindern.

Ab ONTAP 9.9.1, wenn die AWS-Client-Objekt-Tagging-Funktionalität mit dem ONTAP S3-Server unterstützt werden soll, müssen die Aktionen `GetObjectTagging`, `PutObjectTagging` und `DeleteObjectTagging`

mithilfe der Bucket- oder Gruppenrichtlinien zugelassen werden.

Die Vorgehensweise hängt von der verwendeten Schnittstelle ab, System Manager oder CLI:

System Manager

Schritte

1. Den Bucket bearbeiten: Auf **Speicher > Buckets** klicken, den gewünschten Bucket auswählen und anschließend auf **Bearbeiten** klicken. Beim Hinzufügen oder Ändern von Berechtigungen können die folgenden Parameter angegeben werden:
   - **Principal**: der Benutzer oder die Gruppe, denen der Zugriff gewährt wird.
   - **Wirkung**: Erlaubt oder verweigert einem Benutzer oder einer Gruppe den Zugriff.
   - **Aktionen**: Zulässige Aktionen im Bucket für einen bestimmten Benutzer oder eine bestimmte Gruppe.
   - **Ressourcen**: Pfade und Namen von Objekten innerhalb des Buckets, für die der Zugriff gewährt oder verweigert wird.

     Die Standardeinstellungen ***bucketname*** und ***bucketname/**** gewähren Zugriff auf alle Objekte im Bucket. Zugriff kann auch auf einzelne Objekte gewährt werden, zum Beispiel ***bucketname/*_readme.txt**.

   - **Bedingungen** (optional): Ausdrücke, die bei einem Zugriffsversuch ausgewertet werden. Beispielsweise kann eine Liste von IP-Adressen angegeben werden, für die der Zugriff erlaubt oder verweigert wird.

> Ab ONTAP 9.14.1 können Variablen für die Bucket-Richtlinie im Feld **Ressourcen** angegeben werden. Diese Variablen sind Platzhalter, die beim Auswerten der Richtlinie durch Kontextwerte ersetzt werden. Wenn zum Beispiel `${aws:username}` als Variable für eine Richtlinie angegeben ist, wird diese Variable durch den Benutzernamen des Anforderungskontexts ersetzt, und die Richtlinienaktion kann wie für diesen Benutzer konfiguriert ausgeführt werden.

CLI

Schritte

1. Einer Bucket-Richtlinie eine Anweisung hinzufügen:

```
vserver object-store-server bucket policy add-statement -vserver svm_name
-bucket bucket_name -effect {allow|deny} -action object_store_actions
-principal user_and_group_names -resource object_store_resources [-sid
text] [-index integer]
```

   Die folgenden Parameter definieren die Zugriffsberechtigungen:

`-effect`	Die Anweisung kann den Zugriff erlauben oder verweigern.
`-action`	Sie können `*` angeben, um alle Aktionen zu meinen, oder eine Liste mit einer oder mehreren der folgenden: `GetObject, PutObject, DeleteObject, ListBucket, GetBucketAcl,GetObjectAcl, ListBucketMultipartUploads`, und `ListMultipartUploadParts`.

`-principal`	Eine Liste von einem oder mehreren S3-Benutzern oder Gruppen. • Es können maximal 10 Benutzer oder Gruppen angegeben werden. • Wenn eine S3-Gruppe angegeben wird, muss sie das Format `group/group_name`. haben • `*`kann so spezifiziert werden, dass damit öffentlicher Zugriff gemeint ist, das heißt Zugriff ohne Zugriffsschlüssel und geheimen Schlüssel. • Wenn kein Principal angegeben ist, erhalten alle S3-Benutzer in der Storage-VM Zugriff.
`-resource`	Der Bucket und alle darin enthaltenen Objekte. Die Platzhalterzeichen `*` und `?` können verwendet werden, um einen regulären Ausdruck zur Angabe einer Ressource zu erstellen. Für eine Ressource können Variablen in einer Richtlinie festgelegt werden. Diese Richtlinienvariablen sind Platzhalter, die bei der Auswertung der Richtlinie durch die Kontextwerte ersetzt werden.

Optional kann ein Text-String als Kommentar mit der `-sid`Option angegeben werden.

Beispiele

Das folgende Beispiel erstellt eine Objektspeicher-Server-Bucket-Richtlinienanweisung für die Storage-VM svm1.example.com und bucket1, die den erlaubten Zugriff auf einen readme-Ordner für den Objektspeicher-Server-Benutzer user1 festlegt.

```
cluster1::> vserver object-store-server bucket policy statement create
-vserver svm1.example.com -bucket bucket1 -effect allow -action
GetObject,PutObject,DeleteObject,ListBucket -principal user1 -resource
bucket1/readme/* -sid "fullAccessToReadmeForUser1"
```

Das folgende Beispiel erstellt eine Objektspeicherserver-Bucket-Richtlinienanweisung für die Storage-VM svm1.example.com und bucket1, die den zulässigen Zugriff auf alle Objekte für die Objektspeicherservergruppe group1 festlegt.

```
cluster1::> vserver object-store-server bucket policy statement create
-vserver svm1.example.com -bucket bucket1 -effect allow -action
GetObject,PutObject,DeleteObject,ListBucket -principal group/group1
-resource bucket1/* -sid "fullAccessForGroup1"
```

Ab ONTAP 9.19.1 können Sie Bedingungen verwenden, um bedingte Schreibvorgänge für Objekt-Uploads und bedingte Löschvorgänge für Objekt-Löschungen zu erzwingen. Das folgende Beispiel erstellt eine Bucket-Richtlinienbedingung, um bedingte Schreibvorgänge für bucket1 zu erzwingen:

```
cluster::> vserver object-store-server bucket policy-statement-
condition create -vserver vs0 -bucket buck1 -index 1 -operator Null -s3
-if-match true
```

Ab ONTAP 9.14.1 können Variablen für eine Bucket-Richtlinie festgelegt werden. Das folgende Beispiel erstellt eine Server-Bucket-Richtlinienanweisung für die Storage-VM `svm1` und `bucket1` und gibt `${aws:username}` als Variable für eine Richtlinienressource an. Bei der Auswertung der Richtlinie wird die Richtlinienvariable durch den Benutzernamen des Anforderungskontexts ersetzt, und die Richtlinienaktion kann wie für diesen Benutzer konfiguriert ausgeführt werden. Wenn beispielsweise die folgende Richtlinienanweisung ausgewertet wird, wird `${aws:username}` durch den Benutzer ersetzt, der die S3-Operation ausführt. Wenn ein Benutzer `user1` die Operation ausführt, erhält dieser Benutzer Zugriff auf `bucket1` als `bucket1/user1/*`.

```
cluster1::> object-store-server bucket policy statement create -vserver
svm1 -bucket bucket1 -effect allow -action * -principal - -resource
bucket1,bucket1/${aws:username}/*##
```

Erstellen oder Ändern einer ONTAP S3 Objektspeicherserverrichtlinie

Sie können Richtlinien erstellen, die für einen oder mehrere Buckets in einem Objektspeicher gelten. Objektspeicher-Serverrichtlinien können Benutzergruppen zugeordnet werden, wodurch die Verwaltung des Ressourcenzugriffs über mehrere Buckets hinweg vereinfacht wird.

Bevor Sie beginnen

Eine S3-fähige SVM mit einem S3-Server und einem Bucket muss bereits existieren.

Über diese Aufgabe

Sie können Zugriffsrichtlinien auf SVM-Ebene aktivieren, indem Sie eine Standard- oder benutzerdefinierte Richtlinie in einer Objektspeicherservergruppe angeben. Die Richtlinien werden erst wirksam, nachdem sie in der Gruppendefinition festgelegt wurden.

Bei der Verwendung von Objektspeicherserverrichtlinien werden die Prinzipale (das heißt, Benutzer und Gruppen) in der Gruppendefinition und nicht in der Richtlinie selbst angegeben.

Für den Zugriff auf ONTAP S3 Ressourcen gibt es drei standardmäßige Lese-Richtlinien:

- FullAccess
- NoS3Access
- ReadOnlyAccess

Sie können auch neue benutzerdefinierte Richtlinien erstellen, anschließend neue Anweisungen für neue Benutzer und Gruppen hinzufügen oder die Attribute bestehender Anweisungen ändern. Weitere Informationen zu `vserver object-store-server policy` finden sich in der "ONTAP-Befehlsreferenz".

Ab ONTAP 9.9.1, wenn die AWS-Client-Objekt-Tagging-Funktionalität mit dem ONTAP S3-Server unterstützt werden soll, müssen die Aktionen `GetObjectTagging`, `PutObjectTagging` und `DeleteObjectTagging` mithilfe der Bucket- oder Gruppenrichtlinien zugelassen werden.

Die Vorgehensweise hängt von der verwendeten Schnittstelle ab, System Manager oder CLI:

System Manager

Mit System Manager eine Objektspeicher-Serverrichtlinie erstellen oder ändern

Schritte

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. Einen Benutzer hinzufügen: **Richtlinien** auswählen und dann auf **Hinzufügen** klicken.
   a. Geben Sie einen Richtliniennamen ein und wählen Sie aus einer Liste von Gruppen.
   b. Wählen Sie eine vorhandene Standardrichtlinie aus oder fügen Sie eine neue hinzu.

      Beim Hinzufügen oder Ändern einer Gruppenrichtlinie können die folgenden Parameter angegeben werden:

      - Gruppe: die Gruppen, denen Zugriff gewährt wird.
      - Wirkung: Erlaubt oder verweigert den Zugriff auf eine oder mehrere Gruppen.
      - Aktionen: Zulässige Aktionen in einem oder mehreren Buckets für eine bestimmte Gruppe.
      - Ressourcen: Pfade und Namen von Objekten innerhalb eines oder mehrerer Buckets, für die der Zugriff gewährt oder verweigert wird. Beispiel:
        - ***** gewährt Zugriff auf alle Buckets in der Storage-VM.
        - **bucketname** und **bucketname/*** gewähren Zugriff auf alle Objekte in einem bestimmten Bucket.
        - **bucketname/readme.txt** gewährt Zugriff auf ein Objekt in einem bestimmten Bucket.
   c. Bei Bedarf lassen sich bestehenden Richtlinien weitere Aussagen hinzufügen.

CLI

Mit der CLI eine Objektspeicher Serverrichtlinie erstellen oder ändern

Schritte

1. Erstellen einer Objektspeicher-Serverrichtlinie:

   ```
   vserver object-store-server policy create -vserver svm_name -policy
   policy_name [-comment text]
   ```

2. Eine Anweisung für die Richtlinie erstellen:

   ```
   vserver object-store-server policy statement create -vserver svm_name
   -policy policy_name -effect {allow|deny} -action object_store_actions
   -resource object_store_resources [-sid text]
   ```

   Die folgenden Parameter definieren die Zugriffsberechtigungen:

`-effect`	Die Anweisung kann den Zugriff erlauben oder verweigern.

`-action`	Sie können `*` angeben, um alle Aktionen zu meinen, oder eine Liste mit einer oder mehreren der folgenden: `GetObject, PutObject, DeleteObject, ListBucket,GetBucketAcl, GetObjectAcl, ListAllMyBuckets, ListBucketMultipartUploads`, und `ListMultipartUploadParts`.
`-resource`	Der Bucket und alle darin enthaltenen Objekte. Die Platzhalterzeichen `*` und `?` können verwendet werden, um einen regulären Ausdruck zur Angabe einer Ressource zu erstellen.

Optional kann ein Text-String als Kommentar mit der `-sid`Option angegeben werden.

Standardmäßig werden neue Anweisungen am Ende der Anweisungsliste hinzugefügt und der Reihe nach verarbeitet. Wenn später Anweisungen hinzugefügt oder geändert werden, besteht die Möglichkeit, die `-index` Einstellung der Anweisung zu ändern, um die Verarbeitungsreihenfolge anzupassen.

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

Externe Verzeichnisdienste für den ONTAP S3-Zugriff konfigurieren

Ab ONTAP 9.14.1 sind Dienste für externe Verzeichnisse in ONTAP S3 Objektspeicher integriert. Diese Integration vereinfacht die Benutzer- und Zugriffsverwaltung über externe Verzeichnisdienste.

Sie können Benutzergruppen eines externen Verzeichnisdienstes Zugriff auf Ihre ONTAP Objektspeicherumgebung gewähren. Das Lightweight Directory Access Protocol (LDAP) ist eine Schnittstelle zur Kommunikation mit Verzeichnisdiensten wie Active Directory, die eine Datenbank und Dienste für Identitäts- und Zugriffsmanagement (IAM) bereitstellen. Um Zugriff bereitzustellen, ist die Konfiguration von LDAP-Gruppen in Ihrer ONTAP S3-Umgebung erforderlich. Nach der Konfiguration verfügen die Gruppenmitglieder über Berechtigungen für ONTAP S3 Buckets. Informationen zu LDAP finden sich unter "Informationen zur Verwendung von LDAP-Name-Services auf ONTAP NFS SVMs".

Sie können auch Active Directory-Benutzergruppen für den Fast-Bind-Modus konfigurieren, sodass Benutzeranmeldeinformationen validiert und S3-Anwendungen von Drittanbietern sowie Open-Source-S3-Anwendungen über LDAP-Verbindungen authentifiziert werden können.

Bevor Sie beginnen

Vor der Konfiguration von LDAP-Gruppen und der Aktivierung des Schnellbindungsmodus für den Gruppenzugriff sind die folgenden Punkte zu beachten:

1. Es wurde eine S3-fähige Storage-VM mit einem S3-Server erstellt. Siehe "Eine SVM für S3 erstellen".
2. In dieser Storage-VM wurde ein Bucket erstellt. Siehe "Einen Bucket erstellen".
3. DNS ist auf der Speicher-VM konfiguriert. Siehe "DNS-Dienste konfigurieren".
4. Ein selbstsigniertes Stammzertifizierungsstellenzertifikat (CA-Zertifikat) des LDAP-Servers ist auf der Storage-VM installiert. Siehe "Selbstsignierte Root-CA-Zertifikate auf der SVM installieren".

5. Ein LDAP-Client ist mit aktiviertem TLS auf der SVM konfiguriert. Siehe "LDAP-Client-Konfigurationen für ONTAP NFS-Zugriff erstellen" und "Zu Informationszwecken können LDAP-Client-Konfigurationen mit ONTAP NFS SVMs verknüpft werden.".

S3-Zugriff für LDAP konfigurieren

1. LDAP als *Namensdienstdatenbank* der SVM für die Gruppe und das Passwort für LDAP angeben:

```
ns-switch modify -vserver <vserver-name> -database group -sources
files,ldap
ns-switch modify -vserver <vserver-name> -database passwd -sources
files,ldap
```

   Weitere Informationen zum Befehl `vserver services name-service ns-switch modify` finden Sie in der ONTAP Befehlsreferenz.

2. Erstellen Sie eine Objektspeicher-Bucket-Richtlinienanweisung, bei der `principal` auf die LDAP-Gruppe gesetzt ist, der Zugriff gewährt werden soll:

```
object-store-server bucket policy statement create -bucket <bucket-name>
-effect allow -principal nasgroup/<ldap-group-name> -resource <bucket-
name>, <bucket-name>/*
```

   Beispiel: Das folgende Beispiel erstellt eine Bucket-Richtlinienanweisung für `buck1`. Die Richtlinie erlaubt der LDAP-Gruppe `group1` den Zugriff auf die Ressource (Bucket und seine Objekte) `buck1`.

```
vserver object-store-server bucket policy add-statement -bucket buck1
-effect allow -action
GetObject,PutObject,DeleteObject,ListBucket,GetBucketAcl,GetObjectAcl,Li
stBucketMultipartUploads,ListMultipartUploadParts,
ListBucketVersions,GetObjectTagging,PutObjectTagging,DeleteObjectTagging
,GetBucketVersioning,PutBucketVersioning -principal nasgroup/group1
-resource buck1, buck1/*
```

3. Es wird überprüft, ob ein Benutzer aus der LDAP-Gruppe `group1` in der Lage ist, S3-Operationen vom S3-Client aus durchzuführen.

LDAP-Fast-Bind-Modus für die Authentifizierung verwenden

1. LDAP als *Namensdienstdatenbank* der SVM für die Gruppe und das Passwort für LDAP angeben:

```
ns-switch modify -vserver <vserver-name> -database group -sources
files,ldap
ns-switch modify -vserver <vserver-name> -database passwd -sources
files,ldap
```

Weitere Informationen zum Befehl `vserver services name-service ns-switch modify` finden Sie in der ONTAP Befehlsreferenz.

2. Stellen Sie sicher, dass ein LDAP-User, der auf den S3-Bucket zugreift, über die in den Bucket-Policies definierten Berechtigungen verfügt. Weitere Informationen finden sich unter "Ändern einer Bucket-Richtlinie".
3. Es sollte überprüft werden, ob ein Benutzer der LDAP-Gruppe die folgenden Operationen ausführen kann:
   a. Der Zugriffsschlüssel wird auf dem S3-Client in diesem Format konfiguriert: `"NTAPFASTBIND" + base64-encode(user-name:password)` Beispiel: `"NTAPFASTBIND"` + base64-encode(ldapuser:password), was zu `NTAPFASTBINDbGRhcHVzZXI6cGFzc3dvcmQ=` führt

      > Der S3-Client fordert möglicherweise einen geheimen Schlüssel an. Falls kein geheimer Schlüssel vorhanden ist, kann ein beliebiges Passwort mit mindestens 16 Zeichen eingegeben werden.

   b. Grundlegende S3-Operationen können über den S3-Client ausgeführt werden, für die der Benutzer die entsprechenden Berechtigungen besitzt.

Base64-Anmeldeinformationen

Die Standardkonfiguration von ONTAP S3 schließt HTTP aus und verwendet ausschließlich HTTPS und eine Transport Layer Security (TLS)-Verbindung. ONTAP kann selbstsignierte Zertifikate generieren, aber die empfohlene Best Practice ist die Verwendung von Zertifikaten einer Drittanbieter-Zertifizierungsstelle (CA). Bei der Verwendung von CA-Zertifikaten entsteht eine Vertrauensbeziehung zwischen Client-Anwendungen und dem ONTAP Objektspeicher-Server.

Beachten Sie, dass mit Base64 codierte Anmeldeinformationen leicht entschlüsselt werden können. Die Verwendung von HTTPS verhindert, dass codierte Anmeldeinformationen von Man-in-the-Middle-Paketsniffern abgefangen werden.

Der LDAP-Fast-Bind-Modus sollte beim Erstellen vorab signierter URLs nicht für die Authentifizierung verwendet werden. Die Authentifizierung basiert ausschließlich auf dem Base64-Zugriffsschlüssel, der in der vorab signierten URL enthalten ist. Benutzername und Passwort werden jedem offengelegt, der den Base64-Zugriffsschlüssel entschlüsselt.

Authentifizierungsverfahren ist nsswitch und LDAP ist aktiviert Beispiel

```
$curl -siku <user>:<user_password> -X POST
https://<LIF_IP_Address>/api/protocols/s3/services/<SVM_UUID>/users -d
{"comment":"<S3_user_name>", "name":<user>,"key_time_to_live":"PT6H3M"}
```

> Die API ist an das Cluster-Management-LIF und nicht an das Daten-LIF der SVM zu richten. Um Benutzern das Generieren eigener Schlüssel zu ermöglichen, sind ihrer Rolle HTTP-Berechtigungen für die Nutzung von curl hinzuzufügen. Diese Berechtigung kommt zu den S3-API-Berechtigungen hinzu.

S3-Zugriff für Active Directory oder SMB-Server konfigurieren

Wenn für die in der Bucket-Richtlinie angegebene nasgroup oder die Benutzer, die dieser nasgroup

angehören, keine UID und GID festgelegt sind, schlagen Suchvorgänge fehl, wenn diese Attribute nicht gefunden werden. Active Directory verwendet SID, nicht UID. Können SID-Einträge nicht UID zugeordnet werden, müssen die erforderlichen Daten zu ONTAP gebracht werden.

Dazu "vserver active-directory create" verwenden, damit sich die SVM bei Active Directory authentifizieren und die erforderlichen Benutzer- und Gruppeninformationen abrufen kann.

Alternativ kann "vserver cifs create" verwendet werden, um einen SMB-Server in einer Active Directory-Domäne zu erstellen.

Wenn Sie unterschiedliche Domänennamen für Nameserver und Objektspeicher verwenden, kann es zu Namensauflösungsfehlern kommen. Um Namensauflösungsfehler zu vermeiden, empfiehlt NetApp, für die Ressourcenautorisierung vertrauenswürdige Domänen im UPN-Format zu verwenden: `nasgroup/group@trusted_domain.com` Vertrauenswürdige Domänen sind solche, die der Liste der vertrauenswürdigen Domänen des SMB-Servers hinzugefügt wurden. Es wird erläutert, wie "Bevorzugte vertrauenswürdige Domänen hinzufügen, entfernen und ändern" in der SMB-Serverliste vorzugehen ist.

Schlüssel werden generiert, wenn das Authentifizierungsverfahren „Domäne“ ist und vertrauenswürdige Domänen in Active Directory konfiguriert sind.

Der `s3/services/<svm_uuid>/users`Endpoint wird mit Benutzern im UPN-Format verwendet. Beispiel:

```
$curl -siku FQDN\\user:<user_password> -X POST
https://<LIF_IP_Address>/api/protocols/s3/services/<SVM_UUID>/users -d
{"comment":"<S3_user_name>",
"name":<user@fqdn>,"key_time_to_live":"PT6H3M"}
```

Die API ist an das Cluster-Management-LIF und nicht an das Daten-LIF der SVM zu richten. Um Benutzern das Generieren eigener Schlüssel zu ermöglichen, sind ihrer Rolle HTTP-Berechtigungen für die Nutzung von curl hinzuzufügen. Diese Berechtigung kommt zu den S3-API-Berechtigungen hinzu.

Schlüssel generieren, wenn das Authentifizierungsverfahren „Domäne“ ist und keine vertrauenswürdigen Domänen vorhanden sind

Diese Aktion ist möglich, wenn LDAP deaktiviert ist oder wenn Nicht-POSIX-Benutzer keine UID und GID konfiguriert haben. Beispiel:

```
$curl -siku FQDN\\user:<user_password> -X POST
https://<LIF_IP_Address>/api/protocols/s3/services/<SVM_UUID>/users -d
{"comment":"<S3_user_name>",
"name":<user[@fqdn]>,"key_time_to_live":"PT6H3M"}
```

Die API ist an das Cluster-Management-LIF und nicht an das Daten-LIF der SVM zu richten. Um Benutzern das Generieren eigener Schlüssel zu ermöglichen, sind ihrer Rolle HTTP-Berechtigungen für die Nutzung von curl hinzuzufügen. Diese Berechtigung kommt zu den S3-API-Berechtigungen hinzu. Der optionale Domänenwert (@fqdn) ist einem Benutzernamen nur hinzuzufügen, wenn keine vertrauenswürdigen Domänen vorhanden sind.

LDAP- oder Domänenbenutzern wird ermöglicht, eigene ONTAP S3-Zugriffsschlüssel zu generieren.

Ab ONTAP 9.14.1 können ONTAP-Administratoren benutzerdefinierte Rollen erstellen und diese lokalen oder Domänengruppen oder Lightweight Directory Access Protocol (LDAP)-Gruppen zuweisen, sodass die Benutzer, die zu diesen Gruppen gehören, ihre eigenen Zugriffs- und geheimen Schlüssel für den S3-Clientzugriff generieren können.

Auf Ihrer Storage-VM sind einige Konfigurationsschritte erforderlich, damit die benutzerdefinierte Rolle erstellt und dem Benutzer zugewiesen werden kann, der die API zur Generierung des Zugriffsschlüssels aufruft.

Wenn LDAP deaktiviert ist, besteht die Möglichkeit, "Externe Verzeichnisdienste für den ONTAP S3-Zugriff konfigurieren"Benutzern das Generieren von Zugriffsschlüsseln zu ermöglichen.

Bevor Sie beginnen

Stellen Sie Folgendes sicher:

1. Es wurde eine S3-fähige Storage-VM mit einem S3-Server erstellt. Siehe "Eine SVM für S3 erstellen".
2. In dieser Storage-VM wurde ein Bucket erstellt. Siehe "Einen Bucket erstellen".
3. DNS ist auf der Speicher-VM konfiguriert. Siehe "DNS-Dienste konfigurieren".
4. Ein selbstsigniertes Stammzertifizierungsstellenzertifikat (CA-Zertifikat) des LDAP-Servers ist auf der Storage-VM installiert. Siehe "Selbstsignierte Root-CA-Zertifikate auf der SVM installieren".
5. Auf der Storage-VM ist ein LDAP-Client mit aktiviertem TLS konfiguriert. Siehe "LDAP-Client-Konfigurationen für ONTAP NFS-Zugriff erstellen".
6. Die Client-Konfiguration dem Vserver zuordnen. Siehe "LDAP-Client-Konfigurationen mit ONTAP NFS SVMs verknüpfen". Weitere Informationen zu `vserver services name-service ldap create` finden sich in der "ONTAP-Befehlsreferenz".
7. Wenn Sie eine Datenspeicher-VM verwenden, eine Management-Netzwerkschnittstelle (LIF) auf der VM sowie eine Dienstrichtlinie für die LIF erstellen. Weitere Informationen zu `network interface create` und `network interface service-policy create` finden sich in der "ONTAP-Befehlsreferenz".

Benutzer für die Generierung von Zugriffsschlüsseln konfigurieren

Beispiel 3. Schritte

LDAP-Benutzer

1. LDAP als *Namensdienstdatenbank* der Storage-VM für die Gruppe und das Passwort zu LDAP angeben:

```
ns-switch modify -vserver <vserver-name> -database group -sources
files,ldap
ns-switch modify -vserver <vserver-name> -database passwd -sources
files,ldap
```

   Weitere Informationen zu `vserver services name-service ns-switch modify` finden sich in der "ONTAP-Befehlsreferenz".

2. Eine benutzerdefinierte Rolle mit Zugriff auf den S3-Benutzer-REST-API-Endpunkt erstellen:

`security login rest-role create -vserver <vserver-name> -role <custom-role-name> -api "/api/protocols/s3/services/*/users" -access <access-type>` In diesem Beispiel wird die `s3-role` Rolle für Benutzer auf der Storage-VM `svm-1` generiert, denen alle Zugriffsrechte, Lesen, Erstellen und Aktualisieren, gewährt werden.

```
security login rest-role create -vserver svm-1 -role s3role -api
"/api/protocols/s3/services/*/users" -access all
```

Weitere Informationen zu `security login rest-role create` finden sich in der "ONTAP-Befehlsreferenz".

3. Eine LDAP-Benutzergruppe wird mit dem `security login` Befehl erstellt, und die neue benutzerdefinierte Rolle für den Zugriff auf den S3-User-REST-API-Endpunkt wird hinzugefügt. Weitere Informationen zu `security login create` finden sich in der "ONTAP-Befehlsreferenz".

```
security login create -user-or-group-name <ldap-group-name>
-application http -authentication-method nsswitch -role <custom-
role-name> -is-ns-switch-group yes
```

In diesem Beispiel wird die LDAP-Gruppe `ldap-group-1` in `svm-1` erstellt, und die benutzerdefinierte Rolle `s3role` wird ihr für den Zugriff auf den API-Endpunkt hinzugefügt. Zusätzlich wird der LDAP-Zugriff im Fast-Bind-Modus aktiviert.

```
security login create -user-or-group-name ldap-group-1 -application
http -authentication-method nsswitch -role s3role -is-ns-switch
-group yes -second-authentication-method none -vserver svm-1 -is
-ldap-fastbind yes
```

Weitere Informationen finden sich unter "LDAP Fast Bind für die nsswitch-Authentifizierung für ONTAP NFS SVMs verwenden".

Weitere Informationen zu `security login create` finden sich in der "ONTAP-Befehlsreferenz".

Durch Hinzufügen der benutzerdefinierten Rolle zur LDAP-Gruppe erhalten Benutzer dieser Gruppe eingeschränkten Zugriff auf den ONTAP `/api/protocols/s3/services/{svm.uuid}/users` Endpoint. Durch Aufruf der API können die Benutzer der LDAP-Gruppe ihre eigenen Zugriffs- und geheimen Schlüssel zum Zugriff auf den S3-Client generieren. Sie können die Schlüssel nur für sich selbst und nicht für andere Benutzer generieren.

Domänenbenutzer

1. Erstellen einer benutzerdefinierten Rolle mit Zugriff auf den S3-Benutzer-REST-API-Endpunkt:

```
security login rest-role create -vserver <vserver-name> -role <custom-
role-name> -api "/api/protocols/s3/services/*/users" -access <access-
type>
```

In diesem Beispiel wird die `s3-role` Rolle für Benutzer auf der Storage-VM `svm-1` generiert, denen alle Zugriffsrechte (Lesen, Erstellen und Aktualisieren) gewährt werden.

```
security login rest-role create -vserver svm-1 -role s3role -api
"/api/protocols/s3/services/*/users" -access all
```

Weitere Informationen zu `security login rest-role create` finden sich in der "ONTAP-Befehlsreferenz".

1. Eine Domänenbenutzergruppe wird mit dem `security login`-Befehl erstellt, und die neue benutzerdefinierte Rolle für den Zugriff auf den S3 User REST API Endpoint wird hinzugefügt. Weitere Informationen zu `security login create` finden sich in der "ONTAP-Befehlsreferenz".

   ```
   security login create -vserver <vserver-name> -user-or-group-name
   domain\<group-name> -application http -authentication-method domain
   -role <custom-role-name>
   ```

   In diesem Beispiel wird die Domänengruppe `domain\group1` in `svm-1` erstellt, und die benutzerdefinierte Rolle `s3role` wird ihr für den Zugriff auf den API-Endpunkt hinzugefügt.

   ```
   security login create -user-or-group-name domain\group1 -application
   http -authentication-method domain -role s3role -vserver svm-1
   ```

   Weitere Informationen zu `security login create` finden sich in der "ONTAP-Befehlsreferenz".

Durch Hinzufügen der benutzerdefinierten Rolle zur Domänengruppe erhalten Benutzer dieser Gruppe eingeschränkten Zugriff auf den ONTAP `/api/protocols/s3/services/{svm.uuid}/users` Endpoint. Durch Aufruf der API können die Benutzer der Domänengruppe ihre eigenen Zugriffs- und geheimen Schlüssel zum Zugriff auf den S3-Client generieren. Sie können die Schlüssel nur für sich selbst und nicht für andere Benutzer generieren.

Als S3- oder LDAP-Benutzer eigene Zugriffsschlüssel generieren

Ab ONTAP 9.14.1 können Sie eigene Zugriffs- und geheime Schlüssel für den Zugriff auf S3-Clients generieren, sofern Ihr Administrator Ihnen die Rolle zum Generieren eigener Schlüssel zugewiesen hat. Schlüssel können ausschließlich für Sie selbst über den folgenden ONTAP REST API-Endpunkt generiert werden.

Einen S3-Benutzer erstellen und Schlüssel generieren

Dieser REST-API-Aufruf verwendet die folgende Methode und den folgenden Endpunkt. Weitere Informationen zu diesem Endpunkt sind in der Referenz "API-Dokumentation" zu finden.

HTTP-Methode	Pfad
POST	/api/protocols/s3/services/{svm.uuid}/users

Für Domänenbenutzer wird folgendes Format für den S3-Benutzernamen verwendet: `user@fqdn`, wobei

`fqdn` die vollqualifizierte Domain der Domäne ist.

Curl Beispiel

```
curl
--request POST \
--location "https://$FQDN_IP /api/protocols/s3/services/{svm.uuid}/users "
\
--include \
--header "Accept: */*" \
--header "Authorization: Basic $BASIC_AUTH"
--data '{"name":"user1@example.com"}'
```

JSON-Ausgabebeispiel

```
{
  "records": [
    {
      "access_key": "4KX07KF7ML8YNWY01JWG",
      "_links": {
        "next": {
          "href": "/api/resourcelink"
        },
        "self": {
          "href": "/api/resourcelink"
        }
      },
      "name": "user1@example.com",
      "secret_key": "<secret_key_value>"
    }
  ],
  "num_records": "1"
}
```

Schlüssel für einen S3-Benutzer neu generieren

Wenn ein S3-Benutzer bereits existiert, können dessen Zugriffs- und geheimen Schlüssel neu generiert werden. Dieser REST-API-Aufruf verwendet die folgende Methode und den folgenden Endpunkt.

HTTP-Methode	Pfad
PATCH	/api/protocols/s3/services/{svm.uuid}/users/{name}

Curl Beispiel

```
curl
--request PATCH \
--location "https://$FQDN_IP
```

```
/api/protocols/s3/services/{svm.uuid}/users/{name} " \
--include \
--header "Authorization: Basic $BASIC_AUTH" \
--data '{"regenerate_keys":"True"}'
```

JSON-Ausgabebeispiel

```
{
  "records": [
    {
      "access_key": "DX12U609DMRVD8U30Z1M",
      "_links": {
        "self": {
          "href": "/api/resourcelink"
        }
      },
      "name": "user1@example.com",
      "secret_key": "<secret_key_value>"
    }
  ],
  "num_records": "1"
}
```

Clientzugriff auf S3-Objektspeicher ermöglichen

ONTAP S3-Zugriff für Remote FabricPool Tiering aktivieren

Damit ONTAP S3 als Remote FabricPool Kapazitäts- (Cloud-) Ebene verwendet werden kann, muss der ONTAP S3-Administrator dem Remote ONTAP Cluster-Administrator Informationen zur S3-Serverkonfiguration bereitstellen.

Über diese Aufgabe

Die folgenden S3-Serverinformationen sind erforderlich, um FabricPool Cloud-Tiers zu konfigurieren:

- Servername (FQDN)
- Bucket Name
- CA-Zertifikat
- Zugangsschlüssel
- Passwort (geheimer Zugriffsschlüssel)

Darüber hinaus ist folgende Netzwerkkonfiguration erforderlich:

- Im für die Admin-SVM konfigurierten DNS-Server muss ein Eintrag für den Hostnamen des Remote-ONTAP-S3-Servers vorhanden sein, einschließlich des FQDN-Namens des S3-Servers und der IP-Adressen seiner LIFs.
- Intercluster LIFs müssen auf dem lokalen Cluster konfiguriert werden, obwohl Cluster-Peering nicht

erforderlich ist.

In der FabricPool-Dokumentation gibt es Informationen zur Konfiguration von ONTAP S3 als Cloud-Tier.

"Verwaltung von Speicherebenen mithilfe von FabricPool"

ONTAP S3-Zugriff für lokales FabricPool Tiering aktivieren

Damit ONTAP S3 als lokale FabricPool Kapazitätsebene verwendet werden kann, muss ein Objektspeicher auf Basis des erstellten Buckets definiert und dieser Objektspeicher einem Performance-Tier-Aggregat zugeordnet werden, um eine FabricPool zu erstellen.

Bevor Sie beginnen

Sie benötigen den ONTAP S3 Servernamen und einen Bucket-Namen, und der S3-Server muss mithilfe von Cluster-LIFs (mit dem `-vserver Cluster` Parameter) erstellt worden sein.

Über diese Aufgabe

Die Objektspeicherkonfiguration enthält Informationen über die lokale Kapazitätsebene, einschließlich der Namen des S3-Servers und des Buckets sowie der Authentifizierungsanforderungen.

Eine einmal erstellte Objektspeicherkonfiguration darf nicht mit einem anderen Objektspeicher oder Bucket verknüpft werden. Es können mehrere Buckets für lokale Tiers erstellt werden, jedoch nicht mehrere Objektspeicher in einem einzelnen Bucket.

Für eine lokale Kapazitätsstufe ist keine FabricPool-Lizenz erforderlich.

Schritte

1. Den Objektspeicher für die lokale Kapazitätsebene erstellen:

   ```
   storage aggregate object-store config create -object-store-name store_name
   -ipspace Cluster -provider-type ONTAP_S3 -server S3_server_name -container
   -name bucket_name -access-key access_key -secret-password password
   ```

   - Der `-container-name` ist der von Ihnen erstellte S3-Bucket.
   - Der `-access-key`Parameter autorisiert Anfragen an den ONTAP S3 Server.
   - Der `-secret-password`Parameter (geheimer Zugriffsschlüssel) authentifiziert Anfragen an den ONTAP S3 Server.
   - Sie können den `-is-certificate-validation-enabled` Parameter auf `false` setzen, um die Zertifikatsprüfung für ONTAP S3 zu deaktivieren.

   ```
   cluster1::> storage aggregate object-store config create
   -object-store-name MyLocalObjStore -ipspace Cluster -provider-type
   ONTAP_S3 -server s3.example.com
   -container-name bucket1 -access-key myS3key -secret-password myS3pass
   ```

2. Anzeige und Überprüfung der Objektspeicher-Konfigurationsinformationen:

   ```
   storage aggregate object-store config show
   ```

3. Optional: "Ermitteln, wie viele Daten in einem Volume inaktiv sind, indem die Berichterstellung für inaktive Daten verwendet wird.".

   Die Kenntnis darüber, wie viele Daten in einem Volume inaktiv sind, kann bei der Entscheidung unterstützen, welches Aggregat für FabricPool Local Tiering verwendet wird.

4. Den Objektspeicher an ein Aggregat anbinden:

   `storage aggregate object-store attach -aggregate` *`aggr_name`* `-object-store-name` *`store_name`*

   Sie können die `allow-flexgroup` **`true`** Option verwenden, um Aggregate anzuhängen, die FlexGroup-Volumenbestandteile enthalten.

   ```
   cluster1::> storage aggregate object-store attach
   -aggregate aggr1 -object-store-name MyLocalObjStore
   ```

5. Die Objektspeicherinformationen werden angezeigt und es wird überprüft, ob der angeschlossene Objektspeicher verfügbar ist:

   `storage aggregate object-store show`

   ```
   cluster1::> storage aggregate object-store show

   Aggregate    Object Store Name    Availability State
   ---------    -----------------    ------------------
   aggr1        MyLocalObjStore      available
   ```

Verwandte Informationen

- "storage aggregate Objektspeicher anhängen"
- "storage aggregate Objektspeicher config create"
- "storage aggregate Objektspeicher-Konfiguration anzeigen"
- "storage aggregate object-store show"

S3-Clientanwendungen erhalten Zugriff auf einen ONTAP S3-Server.

Damit S3-Client-Apps auf den ONTAP S3-Server zugreifen können, muss der ONTAP S3-Administrator dem S3-Benutzer Konfigurationsinformationen bereitstellen.

Bevor Sie beginnen

Die S3-Client-App muss in der Lage sein, sich beim ONTAP S3 Server mit den folgenden AWS-Signaturversionen zu authentifizieren:

- Signature Version 4, ONTAP 9.8 und höher
- Signaturversion 2, ONTAP 9.11.1 und höher

Andere Signaturversionen werden von ONTAP S3 nicht unterstützt.

Der ONTAP S3-Administrator muss S3-Benutzer angelegt und ihnen Zugriffsberechtigungen erteilt haben, entweder als Einzelbenutzer oder als Gruppenmitglied, in der Bucket-Richtlinie oder in der Objektspeicherserver-Richtlinie.

Die S3-Client-App muss in der Lage sein, den ONTAP S3-Servernamen aufzulösen, was erfordert, dass der ONTAP S3-Administrator den S3-Servernamen (FQDN) und die IP-Adressen für die LIFs des S3-Servers bereitstellt.

Über diese Aufgabe

Um auf einen ONTAP S3-Bucket zuzugreifen, gibt ein Benutzer in der S3-Client-App Informationen ein, die vom ONTAP S3-Administrator bereitgestellt wurden.

Ab ONTAP 9.9.1 unterstützt der ONTAP S3 Server die folgende AWS-Clientfunktionalität:

- benutzerdefinierte Objektmetadaten

  Beim Erstellen von Objekten mit PUT (oder POST) können ihnen Schlüssel-Wert-Paare als Metadaten zugewiesen werden. Wenn eine GET-/HEAD-Operation für das Objekt durchgeführt wird, werden die benutzerdefinierten Metadaten zusammen mit den Systemmetadaten zurückgegeben.

- Objektkennzeichnung

  Zur Kategorisierung von Objekten kann ein separates Set von Schlüssel-Wert-Paaren als Tags zugewiesen werden. Im Gegensatz zu Metadaten werden Tags unabhängig vom Objekt mithilfe von REST-APIs erstellt und gelesen, und sie werden bei der Erstellung von Objekten oder jederzeit danach implementiert.

  Damit Clients Tagging-Informationen abrufen und einfügen können, müssen die Aktionen `GetObjectTagging`, `PutObjectTagging` und `DeleteObjectTagging` mithilfe der Bucket- oder Gruppenrichtlinien zugelassen werden.

Weitere Informationen sind in der AWS S3 Dokumentation verfügbar.

Schritte

1. Die S3-Client-App wird beim ONTAP S3-Server authentifiziert, indem der S3-Servername und das CA-Zertifikat eingegeben werden.
2. Ein Benutzer wird in der S3 Client-App authentifiziert, wenn die folgenden Informationen eingegeben werden:
   - S3-Servername (FQDN) und Bucket-Name
   - Zugriffs-Schlüssel und geheimer Schlüssel des Benutzers

ONTAP S3 Storage-Servicelevel

ONTAP beinhaltet vordefinierte Speicherdienste, die entsprechenden minimalen Leistungsfaktoren zugeordnet sind.

Die tatsächlich verfügbaren Speicherdienste in einem Cluster oder einer SVM werden durch die Art des Speichers bestimmt, aus dem ein Aggregat in der SVM besteht.

Die folgende Tabelle zeigt, wie die minimalen Leistungsfaktoren den vordefinierten Speicherdiensten zugeordnet sind:

Speicherservice	Erwartete IOPS (SLA)	Maximale IOPS (SLO)	Minimale Volume-IOPS	Geschätzte Latenz	Werden die erwarteten IOPS eingehalten?
Wert	128 pro TB	512 pro TB	75	17 ms	Auf AFF: Ja Ansonsten: Nein
Leistung	2048 pro TB	4096 pro TB	500	2 ms	Ja
extrem	6144 pro TB	12288 pro TB	1000	1 ms	Ja

Die folgende Tabelle definiert die verfügbare Storage-Service-Ebene für jeden Medientyp oder Knoten:

Medien oder Knoten	Verfügbare Speicherserviceebene
Festplatte	Wert
Festplatte der virtuellen Maschine	Wert
Hybrid	Wert
Kapazitätsoptimierter Flash	Wert
Solid-state drive (SSD) nicht AFF	Wert
Leistungsoptimierter Flash - SSD (AFF)	Extreme, Leistung, Wert

Cross-Origin Resource Sharing (CORS) für ONTAP S3 Buckets konfigurieren

Ab ONTAP 9.16.1 ist es möglich, Cross-Origin Resource Sharing (CORS) zu konfigurieren, sodass Client-Webanwendungen aus verschiedenen Domänen auf Ihre ONTAP Buckets zugreifen können. Dadurch wird ein sicherer Zugriff auf die Bucket-Objekte über einen Webbrowser ermöglicht.

CORS ist ein auf HTTP basierendes Framework, das es Skripten auf einer Webseite ermöglicht, auf Ressourcen eines Servers in einer anderen Domain zuzugreifen. Das Framework wird verwendet, um die *Same-Origin-Policy* sicher zu umgehen, die eine frühe Grundlage der Websicherheit bildet. Die wichtigsten Konzepte und die Terminologie werden nachfolgend beschrieben.

Herkunft

Der Ursprung definiert präzise den Ort und die Identität einer Ressource. Er wird als Kombination der folgenden Werte dargestellt:

- URI-Schema (Protokoll)
- Hostname (Domänenname oder IP-Adresse)
- Portnummer

Hier ist ein einfaches Beispiel für einen Ursprung: `https://www.mycompany.com:8001`. Wenn ein Ursprung mit CORS verwendet wird, identifiziert er den Client, der die Anfrage stellt.

Same-origin-Richtlinie

Die Same-Origin-Policy (SOP) ist ein Sicherheitskonzept und eine Beschränkung für browserbasierte Skripte. Die Richtlinie erlaubt Skripten, die ursprünglich von einer Webseite geladen wurden, auf Daten einer anderen Seite zuzugreifen, sofern beide Seiten denselben Ursprung haben. Diese Einschränkung verhindert, dass

schädliche Skripte auf Daten von Seiten mit anderem Ursprung zugreifen.

Häufige Anwendungsfälle für CORS

CORS hat mehrere allgemeine Anwendungsfälle. Die meisten betreffen klar definierte Fälle von domänenübergreifendem Zugriff, wie AJAX-Anfragen, das Laden von Schriftarten, Stylesheets und Skripten sowie die domänenübergreifende Authentifizierung. CORS kann auch als Teil einer Single-Page-Anwendung (SPA) implementiert werden.

HTTP-Header

CORS wird mithilfe von Headern implementiert, die in die HTTP-Anfragen und -Antworten eingefügt werden. Beispielsweise gibt es mehrere Antwort-Header, die eine Zugriffskontrolle implementieren und angeben, welche Operationen, einschließlich Methoden und Header, zulässig sind. Das Vorhandensein des *Origin* -Headers in einer HTTP-Anfrage definiert diese als domänenübergreifende Anfrage. Der Origin-Wert wird vom CORS-Server verwendet, um eine gültige CORS-Konfiguration zu finden.

HTTP Preflight-Anfrage

Dies ist eine optionale Anfrage, um zunächst zu prüfen, ob ein Server CORS unterstützt, einschließlich der spezifischen Methoden und Header. Basierend auf der Antwort kann die CORS-Anfrage abgeschlossen oder nicht abgeschlossen werden.

ONTAP Buckets

Ein Bucket ist ein Container für Objekte, die anhand eines klar definierten Namensraums gespeichert und abgerufen werden. Es gibt zwei Arten von ONTAP Buckets:

- NAS Buckets, die über die NAS- und S3-Protokolle zugänglich sind
- S3 Buckets, die ausschließlich über das S3-Protokoll zugänglich sind

CORS-Implementierung in ONTAP

CORS ist in ONTAP 9.16.1 und späteren Versionen standardmäßig aktiviert. CORS muss auf jeder SVM konfiguriert werden, auf der es aktiv sein soll.

> Es gibt keine administrative Option, CORS für einen ONTAP Cluster zu deaktivieren. Allerdings kann CORS effektiv deaktiviert werden, indem keine Regeln definiert oder alle vorhandenen Regeln gelöscht werden.

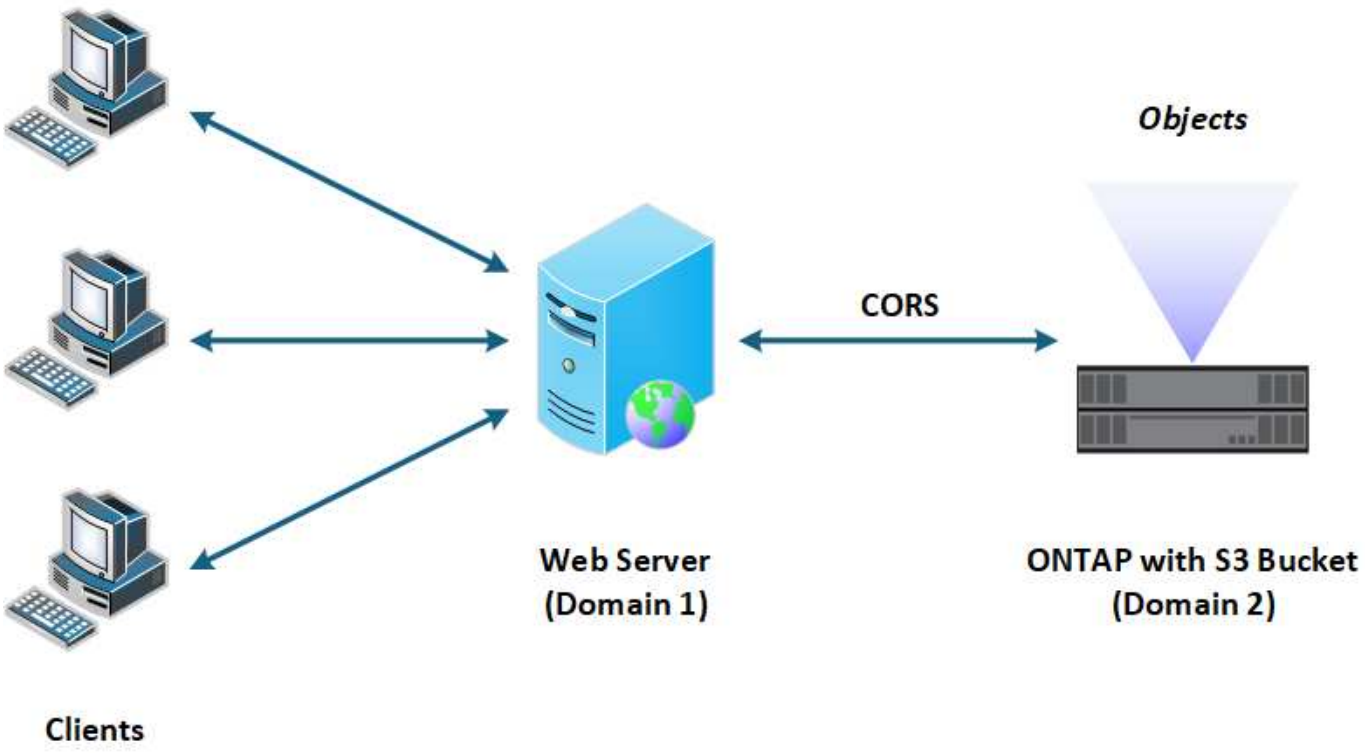
Mögliche Anwendungsfälle

Die ONTAP CORS-Implementierung ermöglicht verschiedene Topologien für den domänenübergreifenden Ressourcenzugriff, darunter:

- ONTAP S3 Buckets (innerhalb desselben oder eines anderen SVM oder Clusters)
- ONTAP NAS Buckets (innerhalb derselben oder verschiedener SVM oder Cluster)
- ONTAP S3 und NAS Buckets (innerhalb derselben oder verschiedener SVM oder Cluster)
- ONTAP Buckets und Buckets externer Anbieter
- Buckets in verschiedenen Zeitzonen

Überblick

Nachfolgend wird auf hoher Ebene veranschaulicht, wie CORS den Zugriff auf die ONTAP S3 Buckets ermöglicht.



Definition von CORS-Regeln

CORS-Regeln müssen in ONTAP definiert werden, um die Funktion zu aktivieren und zu nutzen.

Konfigurationsaktionen

In ONTAP werden drei primäre Konfigurationsregel-Aktionen unterstützt:

- Zeigen
- Erstellen
- Löschen

Eine in ONTAP definierte CORS-Regel besitzt mehrere Eigenschaften, darunter die SVM und den Bucket sowie die zulässigen Ursprünge, Methoden und Header.

Verwaltungsoptionen

Bei der Administration von CORS in Ihrem ONTAP Cluster stehen mehrere Optionen zur Verfügung.

ONTAP Befehlszeilenschnittstelle

CORS kann über die Befehlszeile konfiguriert werden. Siehe CORS-Verwaltung mit der CLI für weitere

Informationen.

ONTAP REST API

Sie können CORS über die ONTAP REST API konfigurieren. Es wurden keine neuen Endpunkte zur Unterstützung der CORS-Funktion hinzugefügt. Stattdessen kann der folgende vorhandene Endpunkt verwendet werden:

```
/api/protocols/s3/services/{svm.uuid}/buckets/{bucket.uuid}
```

Weitere Informationen finden Sie im "ONTAP Automatisierungsdokumentation".

S3 API

Sie können die S3-API verwenden, um eine CORS-Konfiguration auf einem ONTAP Bucket zu erstellen und zu löschen. Ein S3-Clientadministrator benötigt ausreichende Berechtigungen, darunter:

- Zugangs- oder geheime Schlüssel-Anmeldeinformationen
- Für den Bucket wurde eine Richtlinie konfiguriert, die den Zugriff über s3api ermöglicht.

Aktualisierung und Zurücksetzung

Wenn Sie CORS für den Zugriff auf die ONTAP S3 Buckets verwenden möchten, sollten Sie sich einiger administrativer Aspekte bewusst sein.

Upgrade

Die CORS-Funktion wird unterstützt, wenn alle Knoten auf 9.16.1 aktualisiert wurden. In Clustern im gemischten Modus ist die Funktion nur verfügbar, wenn die effektive Clusterversion (ECV) 9.16.1 oder höher ist.

Wiederherstellung

Aus Benutzersicht müssen alle CORS-Konfigurationen entfernt werden, bevor die Clusterwiederherstellung durchgeführt werden kann. Intern werden dabei alle CORS-Datenbanken gelöscht. Es erfolgt eine Aufforderung, einen Befehl auszuführen, um diese Datenstrukturen zu löschen und zurückzusetzen.

CORS-Verwaltung mit der CLI

Die ONTAP CLI kann zur Verwaltung von CORS-Regeln verwendet werden. Die wichtigsten Vorgänge sind nachfolgend beschrieben. Für die Ausführung der CORS-Befehle ist die ONTAP **admin**-Berechtigungsstufe erforderlich.

Erstellen

Eine CORS-Regel kann mit dem `vserver object-store-server bucket cors-rule create` Befehl definiert werden. Weitere Informationen zu `vserver object-store-server bucket cors-rule create` finden sich in der "ONTAP-Befehlsreferenz".

Parameter

Die zur Erstellung einer Regel verwendeten Parameter sind nachfolgend beschrieben.

Parameter	Beschreibung
`vserver`	Gibt den Namen der SVM (vserver) an, die den Objektspeicher Server-Bucket hostet, in dem die Regel erstellt wird.

Parameter	Beschreibung
`bucket`	Der Name des Buckets auf dem Objektspeicher-Server, für den die Regel erstellt wurde.
`index`	Ein optionaler Parameter, der den Index des Objektspeicher-Server-Buckets angibt, in dem die Regel erstellt wird.
`rule id`	Eine eindeutige Kennung für die Bucket-Regel des Objektspeicherservers.
`allowed-origins`	Eine Liste der Ursprünge, von denen Cross-Origin-Anfragen zulässig sind.
`allowed-methods`	Eine Liste der in einer ursprungsübergreifenden Anfrage zulässigen HTTP-Methoden.
`allowed-headers`	Eine Liste der in Cross-Origin-Anfragen zulässigen HTTP-Header.
`expose-headers`	Eine Liste der zusätzlichen Header, die in den CORS-Antworten gesendet werden und auf die Kunden von ihren Anwendungen aus zugreifen können.
`max-age-in-seconds`	Ein optionaler Parameter, der die Zeitdauer angibt, für die Ihr Browser eine Preflight-Antwort für eine bestimmte Ressource zwischenspeichern soll.

Beispiel

```
vserver object-store-server bucket cors-rule create -vserver vs1 -bucket
bucket1 -allowed-origins www.myexample.com -allowed-methods GET,DELETE
```

Zeigen

Sie können den Befehl `vserver object-store-server bucket cors-rule show` verwenden, um eine Liste der aktuellen Regeln und deren Inhalte anzuzeigen. Weitere Informationen zu `vserver object-store-server bucket cors-rule show` finden sich in der "ONTAP-Befehlsreferenz".

Durch die Einbeziehung des Parameters `-instance` werden die für jede Regel angezeigten Daten erweitert. Es kann außerdem festgelegt werden, welche Felder gewünscht sind.

Beispiel

```
server object-store-server bucket cors-rule show -instance
```

Löschen

Mit dem Befehl „delete“ kann eine Instanz einer CORS-Regel entfernt werden. Der `index` Wert der Regel wird benötigt, daher erfolgt dieser Vorgang in zwei Schritten:

1. Ein `show`Befehl gibt die Regel aus und ruft deren Index ab.
2. Der Löschvorgang wird anhand des Indexwerts ausgeführt.

Beispiel

```
vserver object-store-server bucket cors-rule delete -vserver vs1 -bucket
bucket1 -index 1
```

Ändern

Es gibt keinen CLI-Befehl zum Ändern einer bestehenden CORS-Regel. Zum Ändern einer Regel sind die folgenden Schritte erforderlich:

1. Die bestehende Regel wird gelöscht.
2. Eine neue Regel mit den gewünschten Optionen erstellen.

Buckets mit SnapMirror S3 schützen

Informationen zu ONTAP SnapMirror S3

Ab ONTAP 9.10.1 ist der Schutz von Buckets in ONTAP S3 Objektspeichern mithilfe der SnapMirror Spiegelungs- und Sicherungsfunktionen möglich. Im Gegensatz zum Standard SnapMirror ermöglicht SnapMirror S3 die Spiegelung und Sicherung zu Nicht-NetApp-Zielen wie AWS S3.

SnapMirror S3 unterstützt aktive Spiegelungen und Backup-Ebenen von ONTAP S3-Buckets zu den folgenden Zielen:

Ziel	Unterstützt aktive Spiegel und Übernahme?	Unterstützt Backup und Wiederherstellung?
ONTAP S3 • Buckets in derselben SVM • Buckets in verschiedenen SVMs auf demselben Cluster • Buckets in SVMs auf verschiedenen Clustern	Ja	Ja
StorageGRID	Nein	Ja
AWS S3	Nein	Ja
Cloud Volumes ONTAP für Azure	Ja	Ja
Cloud Volumes ONTAP für AWS	Ja	Ja
Cloud Volumes ONTAP für Google Cloud	Ja	Ja

Sie können bestehende Buckets auf ONTAP S3 Servern schützen oder neue Buckets erstellen, bei denen die Datensicherung sofort aktiviert ist.

SnapMirror S3-Anforderungen

- ONTAP Version

  Auf dem Quell- und dem Zielcluster muss ONTAP 9.10.1 oder höher ausgeführt werden.

  In einer MetroCluster Konfiguration muss ONTAP 9.20.1 oder höher auf den Quell- und Ziel-Clustern ausgeführt werden.

- Lizenzierung

Die folgenden Lizenzen sind in der "ONTAP One" Software-Suite verfügbar und werden auf ONTAP Quell- und Zielsystemen benötigt, um Zugriff zu ermöglichen:

  - ONTAP S3 Protokoll und Speicher
  - SnapMirror S3 zur Ansprache anderer NetApp Objektspeicher (ONTAP S3, StorageGRID und Cloud Volumes ONTAP)
  - SnapMirror S3 zur Ansprache von Objektspeichern von Drittanbietern, einschließlich AWS S3 (verfügbar in der "ONTAP One Kompatibilitätspaket")
  - Wenn auf Ihrem Cluster ONTAP 9.10.1 ausgeführt wird, ist ein "FabricPool Lizenz" erforderlich.
  - In einer MetroCluster Konfiguration muss die SnapMirror S3-Lizenz auf beiden Clustern installiert sein.
- ONTAP S3
  - ONTAP S3-Server müssen auf Quell- und Ziel-SVMs ausgeführt werden.
  - Es wird empfohlen, aber nicht vorausgesetzt, dass CA-Zertifikate für den TLS-Zugriff auf Systemen installiert sind, die S3-Server hosten.
    - Die CA-Zertifikate, die zum Signieren der Zertifikate der S3-Server verwendet werden, müssen auf der Admin-Speicher-VM der Cluster installiert sein, die die S3-Server hosten.
    - Sie können ein selbstsigniertes CA-Zertifikat oder ein von einem externen CA-Anbieter signiertes Zertifikat verwenden.
    - Wenn die Quell- oder Ziel-Storage-VMs nicht auf HTTPS lauschen, ist die Installation von CA-Zertifikaten nicht erforderlich.
- Peering (für ONTAP S3-Ziele)
  - Intercluster-LIFs müssen konfiguriert werden (für entfernte ONTAP Ziele), und die Intercluster-LIFs des Quell- und Ziel-Cluster können eine Verbindung zu den Daten-LIFs des Quell- und Ziel-S3-Server herstellen.
  - Quell- und Ziel-Cluster sind per Peering verbunden (für entfernte ONTAP Ziele).
  - Quell- und Ziel-Storage-VMs sind per Peering verbunden (für alle ONTAP Ziele).
- SnapMirror Richtlinie
  - Eine S3-spezifische SnapMirror Richtlinie ist für alle SnapMirror S3-Beziehungen erforderlich, jedoch kann dieselbe Richtlinie für mehrere Beziehungen verwendet werden.
  - Sie können eine eigene Richtlinie erstellen oder die Standardrichtlinie **Continuous** akzeptieren, die die folgenden Werte enthält:
    - Drosselung (Obergrenze für Durchsatz/Bandbreite), unbegrenzt.
    - Zeit für Recovery Point Objective: 1 Stunde (3600 Sekunden).

> Es ist zu beachten, dass wenn zwei S3-Buckets in einer SnapMirror Beziehung stehen und Lebenszyklusrichtlinien so konfiguriert sind, dass die aktuelle Version eines Objekts abläuft (gelöscht wird), die gleiche Aktion auf den Partner-Bucket repliziert wird. Dies gilt auch, wenn der Partner-Bucket schreibgeschützt oder passiv ist.

- Root-Benutzerzugriffsschlüssel für Storage-VMs sind für SnapMirror S3-Beziehungen erforderlich; ONTAP weist diese nicht standardmäßig zu. Beim erstmaligen Erstellen einer SnapMirror S3-Beziehung ist zu überprüfen, ob die Schlüssel sowohl auf der Quell- als auch auf der Ziel-Storage-VM vorhanden sind, und sie sind neu zu generieren, falls sie fehlen. Falls eine Neugenerierung erforderlich ist, muss sichergestellt werden, dass alle Clients und alle SnapMirror Objektspeicherkonfigurationen, die das Zugriffsschlüssel- und geheime Schlüsselpaar verwenden, mit den neuen Schlüsseln aktualisiert werden.

- MetroCluster Ab ONTAP 9.20.1 wird SnapMirror S3 in MetroCluster Konfigurationen unterstützt. Die MetroCluster Konfiguration muss die folgenden Anforderungen erfüllen:
  - Die MetroCluster Konfiguration befindet sich in einem einwandfreien Zustand.
  - Auf beiden Clustern läuft ONTAP 9.20.1 oder höher.
  - Die SnapMirror S3 Lizenz ist auf beiden Clustern installiert.

Informationen zur S3-Serverkonfiguration sind in den folgenden Abschnitten verfügbar:

- "Einen S3-Server auf einer Storage-VM aktivieren"
- "Informationen zum ONTAP S3 Konfigurationsprozess"

Informationen zu Cluster- und Storage-VM-Peering sind im folgenden Thema verfügbar:

- "Vorbereitung auf Spiegelung und Archivierung (System Manager, Schritte 1-6)"
- "Cluster- und SVM-Peering (CLI)"

Unterstützte SnapMirror Beziehungen

SnapMirror S3 unterstützt Fan-Out- und Kaskadenbeziehungen. Eine Übersicht ist unter "Verzweigte und kaskadierte Datensicherungsbereitstellungen" zu finden.

SnapMirror S3 unterstützt keine Fan-In-Bereitstellungen (Datensicherungsbeziehungen zwischen mehreren Quell-Buckets und einem einzelnen Ziel-Bucket). SnapMirror S3 kann mehrere Bucket-Spiegelungen von mehreren Clustern auf einen einzelnen sekundären Cluster unterstützen, jedoch muss jeder Quell-Bucket einen eigenen Ziel-Bucket auf dem sekundären Cluster haben.

Zugriff auf S3-Buckets steuern

Beim Erstellen neuer Buckets können Sie den Zugriff durch das Erstellen von Benutzern und Gruppen steuern.

Obwohl SnapMirror S3 Objekte vom Quell-Bucket in einen Ziel-Bucket repliziert, werden Benutzer, Gruppen und Richtlinien nicht vom Quell-Objektspeicher in den Ziel-Objektspeicher repliziert.

Benutzer, Gruppenrichtlinien, Berechtigungen und ähnliche Komponenten müssen im Ziel-Objektspeicher konfiguriert werden, damit Clients während eines Failover-Ereignisses auf den Ziel-Bucket zugreifen können.

Quell- und Zielbenutzer können dieselben Zugriffs- und geheimen Schlüssel verwenden, sofern die Quellschlüssel bei der Erstellung des Benutzers im Ziel-Cluster manuell angegeben werden. Beispiel:

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

Weitere Informationen sind in den folgenden Abschnitten zu finden:

- "S3-Benutzer und Gruppen hinzufügen (System Manager)"
- "Erstellen eines S3-Benutzers (CLI)"
- "S3-Gruppen erstellen oder ändern (CLI)"

S3 Object Lock und Versionierung mit SnapMirror S3

Sie können SnapMirror S3 auf ONTAP Buckets mit aktivierter Objektsperre und Versionsverwaltung verwenden, wobei einige Punkte zu beachten sind:

- Um einen Quell-Bucket mit aktivierter Objektsperre zu replizieren, muss die Objektsperre auch im Ziel-Bucket aktiviert sein. Zusätzlich muss sowohl im Quell- als auch im Ziel-Bucket die Versionierung aktiviert sein. So werden Probleme beim Spiegeln von Löschvorgängen auf den Ziel-Bucket vermieden, wenn beide Buckets unterschiedliche Standard-Aufbewahrungsrichtlinien haben.
- S3 SnapMirror repliziert keine historischen Versionen von Objekten. Nur die aktuelle Version eines Objekts wird repliziert.

Wenn Object Locked-Objekte in einen Ziel-Bucket gespiegelt werden, behalten sie ihre ursprüngliche Aufbewahrungsdauer bei. Wenn entsperrte Objekte repliziert werden, übernehmen sie die Standardaufbewahrungsdauer des Ziel-Buckets. Beispiel:

- Bucket A hat eine Standardaufbewahrungsdauer von 30 Tagen und Bucket B hat eine Standardaufbewahrungsdauer von 60 Tagen. Objekte, die von Bucket A nach Bucket B repliziert werden, behalten ihre 30-tägige Aufbewahrungsdauer bei, auch wenn diese kürzer ist als die Standardaufbewahrungsdauer von Bucket B.
- Bucket A hat keine Standardaufbewahrungsfrist und Bucket B hat eine Standardaufbewahrungsfrist von 60 Tagen. Wenn nicht gesperrte Objekte von Bucket A nach Bucket B repliziert werden, übernehmen sie die 60-tägige Aufbewahrungsfrist. Wenn ein Objekt in Bucket A manuell gesperrt wird, behält es beim Replizieren nach Bucket B seine ursprüngliche Aufbewahrungsfrist bei.
- Bucket A hat eine standardmäßige Aufbewahrungsfrist von 30 Tagen und Bucket B hat keine standardmäßige Aufbewahrungsfrist. Objekte, die von Bucket A nach Bucket B repliziert werden, behalten ihre 30-tägige Aufbewahrungsfrist bei.

Spiegelungs- und Backup-Schutz auf einem entfernten Cluster

Eine Spiegelbeziehung für einen neuen ONTAP S3 Bucket auf dem Remote-Cluster erstellen

Wenn neue S3-Buckets erstellt werden, ist ein sofortiger Schutz auf einem SnapMirror S3-Ziel auf einem Remote-Cluster möglich.

Über diese Aufgabe

Aufgaben sind sowohl auf dem Quell- als auch auf dem Zielsystem durchzuführen.

Bevor Sie beginnen

- Die Anforderungen an ONTAP Versionen, Lizenzen und die S3-Serverkonfiguration wurden erfüllt.
- Zwischen Quell- und Ziel-Cluster besteht eine Peering-Beziehung, und zwischen Quell- und Ziel-Storage-VMs besteht eine Peering-Beziehung.
- Für die Quell- und Ziel-VMs werden CA-Zertifikate benötigt. Es können selbstsignierte CA-Zertifikate oder Zertifikate eines externen CA-Anbieters verwendet werden.

System Manager

1. Falls dies die erste SnapMirror S3-Beziehung für diese Storage-VM ist, sollte überprüft werden, ob Root-Benutzerschlüssel für sowohl die Quell- als auch die Ziel-Storage-VM vorhanden sind, und sie sollten neu generiert werden, falls dies nicht der Fall ist:

a. Klicken Sie auf **Speicher > Speicher-VMs** und wählen Sie dann die Speicher-VM aus.
b. Im Tab **Einstellungen** auf in der Kachel **S3** klicken.
c. Auf der Registerkarte **Benutzer** ist zu überprüfen, ob ein Zugriffsschlüssel für den Root-Benutzer vorhanden ist.
d. Falls kein Schlüssel vorhanden ist, auf neben **root** und anschließend auf **Schlüssel neu generieren** klicken. Der Schlüssel sollte nicht neu generiert werden, falls bereits einer existiert.

2. Die Storage-VM wird bearbeitet, um Benutzer hinzuzufügen und Benutzer Gruppen zuzuordnen, sowohl in der Quell- als auch in der Ziel-Storage-VM:

   Klicken Sie auf **Speicher > Speicher-VMs**, klicken Sie auf die Speicher-VM, klicken Sie auf **Einstellungen** und dann auf unter S3.

   Siehe "S3-Benutzer und Gruppen hinzufügen" für weitere Informationen.

3. Erstellen Sie auf dem Quell-Cluster eine SnapMirror S3-Richtlinie, falls noch keine vorhanden ist und Sie nicht die Standardrichtlinie verwenden möchten:
   a. **Schutz > Übersicht** und danach **Lokale Richtlinieneinstellungen** auswählen.
   b. Klicken Sie neben **Schutzrichtlinien** und dann auf **Hinzufügen**.
      - Geben Sie den Namen und die Beschreibung der Richtlinie ein.
      - Den Richtlinienbereich, den Cluster oder die SVM auswählen
      - **Kontinuierlich** für SnapMirror S3-Beziehungen auswählen.
      - Geben Sie Ihre **Throttle**- und **Recovery Point Objective**-Werte ein.
4. Einen Bucket mit SnapMirror-Schutz erstellen:
   a. Klicken Sie auf **Speicher > Buckets** und anschließend auf **Hinzufügen**. Die Überprüfung der Berechtigungen ist optional, aber empfehlenswert.
   b. Geben Sie einen Namen ein, wählen Sie die Storage-VM aus, geben Sie eine Größe ein und klicken Sie dann auf **Weitere Optionen**.
   c. Unter **Berechtigungen** auf **Hinzufügen** klicken.
      - **Principal** und **Effect** – Werte auswählen, die den Einstellungen Ihrer Benutzergruppe entsprechen, oder die Standardwerte übernehmen.
      - **Aktionen** – die folgenden Werte werden angezeigt:

        ```
        GetObject,PutObject,DeleteObject,ListBucket,GetBucketAcl,GetObjectAcl,ListBucketMultipartUploads,ListMultipartUploadParts
        ```

      - **Ressourcen** – Standardwerte (*bucketname, bucketname/**) oder andere benötigte Werte verwenden.

        Weitere Informationen zu diesen Bereichen sind unter "Benutzerzugriff auf Buckets verwalten" zu finden.

   d. Unter **Schutz** die Option **Enable SnapMirror (ONTAP oder Cloud)** aktivieren. Anschließend die folgenden Werte eingeben:
      - Ziel

        - **ZIEL: ONTAP System**
        - **CLUSTER**: Der Remote-Cluster wird ausgewählt.
        - **STORAGE VM**: Eine Storage-VM auf dem Remote-Cluster auswählen.
        - **S3 SERVER CA-ZERTIFIKAT**: Den Inhalt des *Quell*-Zertifikats kopieren und einfügen.
    - Quelle
        - **S3 SERVER CA-ZERTIFIKAT:** Den Inhalt des *Ziel*-Zertifikats kopieren und einfügen.
5. **Dasselbe Zertifikat auf dem Zielsystem verwenden** auswählen, wenn ein von einem externen CA-Anbieter signiertes Zertifikat verwendet wird.
6. Wenn Sie auf **Zieleinstellungen** klicken, können Sie anstelle der Standardwerte für Bucket-Name, Kapazität und Performance-Servicelevel auch eigene Werte eingeben.
7. Auf **Speichern** klicken. Ein neuer Bucket wird in der Quell-Speicher-VM erstellt und in einen neuen Bucket gespiegelt, der in der Ziel-Speicher-VM erstellt wird.

Verschlossene Buckets sichern

Ab ONTAP 9.14.1 ist es möglich, gesperrte S3-Buckets zu sichern und bei Bedarf wiederherzustellen.

Beim Festlegen der Schutzeinstellungen für einen neuen oder bestehenden Bucket kann die Objektsperrung für Ziel-Buckets aktiviert werden, sofern Quell- und Ziel-Cluster ONTAP 9.14.1 oder höher ausführen und die Objektsperrung im Quell-Bucket aktiviert ist. Der Objektsperrmodus und die Aufbewahrungsdauer der Sperre des Quell-Buckets gelten für die replizierten Objekte im Ziel-Bucket. Im Abschnitt **Zieleinstellungen** kann auch eine abweichende Aufbewahrungsdauer für den Ziel-Bucket definiert werden. Diese Aufbewahrungsdauer wird ebenfalls auf alle nicht gesperrten Objekte angewendet, die vom Quell-Bucket und über S3-Schnittstellen repliziert werden.

Informationen darüber, wie die Objektsperre für einen Bucket aktiviert wird, finden sich unter "Einen Bucket erstellen".

CLI

1. Falls dies die erste SnapMirror S3-Beziehung für diese SVM ist, sollte überprüft werden, ob Root-Benutzerschlüssel für sowohl die Quell- als auch die Ziel-SVM vorhanden sind, und diese gegebenenfalls neu generiert werden:

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

   Überprüfen Sie, ob ein Zugriffsschlüssel für den Root-Benutzer vorhanden ist. Falls nicht, Folgendes eingeben:

   ```
   vserver object-store-server user regenerate-keys -vserver svm_name -user root
   ```

   Der Schlüssel sollte nicht neu generiert werden, falls bereits einer existiert.

2. Buckets sowohl in der Quell- als auch in der Ziel-SVM erstellen:

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

3. Zugriffsregeln zu den Standard-Bucket-Richtlinien sowohl in der Quell-SVM als auch in der Ziel-SVM hinzufügen:

```
vserver object-store-server bucket policy add-statement -vserver svm_name
-bucket bucket_name -effect {allow|deny} -action object_store_actions
-principal user_and_group_names -resource object_store_resources [-sid
text] [-index integer]
```

Beispiel

```
src_cluster::> vserver object-store-server bucket policy add-
statement -bucket test-bucket -effect allow -action
GetObject,PutObject,DeleteObject,ListBucket,GetBucketAcl,GetObjectAc
l,ListBucketMultipartUploads,ListMultipartUploadParts -principal -
-resource test-bucket, test-bucket /*
```

4. Auf der Quell-SVM eine SnapMirror S3-Richtlinie erstellen, falls noch keine vorhanden ist und die Standardrichtlinie nicht verwendet werden soll:
`snapmirror policy create -vserver svm_name -policy policy_name -type continuous [-rpo integer] [-throttle throttle_type] [-comment text] [additional_options]`

   Parameter:

   - Typ `continuous` - der einzige Richtlinientyp für SnapMirror S3-Beziehungen (erforderlich).
   - `-rpo` - gibt die Zeit für das Recovery Point Objective in Sekunden an (optional).
   - `-throttle` - gibt die Obergrenze für Durchsatz/Bandbreite in Kilobyte/Sekunde an (optional).

   Beispiel

   ```
   src_cluster::> snapmirror policy create -vserver vs0 -type
   continuous -rpo 0 -policy test-policy
   ```

5. CA-Serverzertifikate auf den Admin-SVMs der Quell- und Ziel-Cluster installieren:

   a. Installieren Sie auf dem Quell-Cluster das CA-Zertifikat, das das *Ziel*-S3-Serverzertifikat signiert hat:
   `security certificate install -type server-ca -vserver src_admin_svm -cert-name dest_server_certificate`

   b. Installieren Sie auf dem Ziel-Cluster das CA-Zertifikat, das das *Quell*-S3-Serverzertifikat signiert hat:
   `security certificate install -type server-ca -vserver dest_admin_svm -cert-name src_server_certificate`

   Wenn ein von einem externen CA-Anbieter signiertes Zertifikat verwendet wird, ist dasselbe Zertifikat auf der Quell- und Ziel-Admin-SVM zu installieren.

   Weitere Informationen zu `security certificate install` finden sich in der "ONTAP-Befehlsreferenz".

6. Auf dem Quell-SVM eine SnapMirror S3-Beziehung erstellen:

```
snapmirror create -source-path src_svm_name:/bucket/bucket_name
-destination-path dest_peer_svm_name:/bucket/bucket_name, …} [-policy
policy_name]
```

Sie können eine von Ihnen erstellte Richtlinie verwenden oder die Standardrichtlinie akzeptieren.

Beispiel

```
src_cluster::> snapmirror create -source-path vs0-src:/bucket/test-
bucket -destination-path vs1-dest:bucket/test-bucket-mirror -policy
test-policy
```

7. Es sollte überprüft werden, ob die Spiegelung aktiv ist:
`snapmirror show -policy-type continuous -fields status`

Verwandte Informationen

- "snapmirror create"
- "snapmirror policy create"
- "snapmirror show"

Eine Spiegelbeziehung für einen vorhandenen ONTAP S3 Bucket auf dem Remote-Cluster erstellen

Sie können jederzeit mit dem Schutz bestehender S3-Buckets beginnen, beispielsweise wenn eine S3-Konfiguration von einer Version vor ONTAP 9.10.1 aktualisiert wurde.

Über diese Aufgabe

Aufgaben sind sowohl auf dem Quell-Cluster als auch auf dem Ziel-Cluster durchzuführen.

Bevor Sie beginnen

- Die Anforderungen an ONTAP Versionen, Lizenzen und die S3-Serverkonfiguration wurden erfüllt.
- Zwischen Quell- und Ziel-Cluster besteht eine Peering-Beziehung, und zwischen Quell- und Ziel-Storage-VMs besteht eine Peering-Beziehung.
- Für die Quell- und Ziel-VMs werden CA-Zertifikate benötigt. Es können selbstsignierte CA-Zertifikate oder Zertifikate eines externen CA-Anbieters verwendet werden.

Schritte

Eine Spiegelbeziehung kann mithilfe des System Manager oder der ONTAP CLI erstellt werden.

System Manager

1. Falls dies die erste SnapMirror S3-Beziehung für diese Storage-VM ist, sollte überprüft werden, ob Root-Benutzerschlüssel für sowohl die Quell- als auch die Ziel-Storage-VM vorhanden sind, und sie sollten neu generiert werden, falls dies nicht der Fall ist:
   a. Wählen Sie **Speicher > Speicher-VMs** und anschließend die gewünschte Speicher-VM aus.
   b. Im Tab **Einstellungen** auf in der Kachel **S3** klicken.
   c. Auf der Registerkarte **Benutzer** ist zu überprüfen, ob ein Zugriffsschlüssel für den Root-Benutzer vorhanden ist.

d. Falls kein Schlüssel vorhanden ist, auf ⋮ neben **root** und anschließend auf **Schlüssel neu generieren** klicken. Der Schlüssel sollte nicht neu generiert werden, falls bereits einer existiert.

2. Es sollte überprüft werden, ob die vorhandenen Benutzer und Gruppen sowohl in der Quell- als auch in der Ziel-Speicher-VM vorhanden sind und über die korrekten Zugriffsrechte verfügen: **Storage > Storage VMs** auswählen, dann die entsprechende Storage VM und anschließend die Registerkarte **Settings**. Abschließend die Kachel **S3** suchen, ✎ auswählen und dann die Registerkarte **Users** sowie anschließend die Registerkarte **Groups** auswählen, um die Zugriffsberechtigungen für Benutzer und Gruppen anzuzeigen.

   Siehe "S3-Benutzer und Gruppen hinzufügen" für weitere Informationen.

3. Erstellen Sie auf dem Quell-Cluster eine SnapMirror S3-Richtlinie, falls noch keine vorhanden ist und Sie nicht die Standardrichtlinie verwenden möchten:
   a. **Schutz > Übersicht** auswählen und anschließend auf **Lokale Richtlinieneinstellungen** klicken.
   b. Wählen Sie → neben **Schutzrichtlinien** aus und klicken Sie dann auf **Hinzufügen**.
   c. Geben Sie den Namen und die Beschreibung der Richtlinie ein.
   d. Den Richtlinienbereich auswählen, entweder Cluster oder SVM.
   e. **Kontinuierlich** für SnapMirror S3-Beziehungen auswählen.
   f. Geben Sie Ihre **Throttle**- und **Recovery Point Objective**-Werte ein.
4. Es sollte geprüft werden, ob die Zugriffsrichtlinie des bestehenden Buckets weiterhin den eigenen Anforderungen entspricht:
   a. Klicken Sie auf **Storage > Buckets** und wählen Sie dann den Bucket aus, den Sie schützen möchten.
   b. Im Tab **Berechtigungen** auf ✎ **Bearbeiten** klicken, dann unter **Berechtigungen** auf **Hinzufügen** klicken.
      - **Prinzip und Wirkung**: Werte auswählen, die den Einstellungen Ihrer Benutzergruppe entsprechen, oder die Standardwerte übernehmen.
      - **Aktionen**: Die folgenden Werte sollten angezeigt werden:

        ```
        GetObject,PutObject,DeleteObject,ListBucket,GetBucketAcl,GetObjectAcl,ListBucketMultipartUploads,ListMultipartUploadParts
        ```

      - **Ressourcen**: Standardwerte (*bucketname, bucketname/**) oder andere benötigte Werte verwenden.

        Weitere Informationen zu diesen Bereichen sind unter "Benutzerzugriff auf Buckets verwalten" zu finden.

5. Einen bestehenden Bucket mit SnapMirror S3-Schutz schützen:
   a. Klicken Sie auf **Speicher** > **Buckets** und wählen Sie dann den Bucket aus, den Sie schützen möchten.
   b. Auf **Schützen** klicken und die folgenden Werte eingeben:
      - Ziel
        - **ZIEL**: ONTAP System

        - **CLUSTER**: Der Remote-Cluster wird ausgewählt.
        - **STORAGE VM**: Eine Storage-VM auf dem Remote-Cluster auswählen.
        - **S3 SERVER CA-ZERTIFIKAT**: Den Inhalt des *Quell*-Zertifikats kopieren und einfügen.
    - Quelle
        - **S3 SERVER CA-ZERTIFIKAT**: Den Inhalt des *Ziel*-Zertifikats kopieren und einfügen.
6. **Dasselbe Zertifikat auf dem Zielsystem verwenden** auswählen, wenn ein von einem externen CA-Anbieter signiertes Zertifikat verwendet wird.
7. Wenn Sie auf **Zieleinstellungen** klicken, können Sie anstelle der Standardwerte für Bucket-Name, Kapazität und Performance-Servicelevel auch eigene Werte eingeben.
8. Auf **Speichern** klicken. Der vorhandene Bucket wird in einen neuen Bucket auf der Ziel-Speicher-VM gespiegelt.

Verschlossene Buckets sichern

Ab ONTAP 9.14.1 ist es möglich, gesperrte S3-Buckets zu sichern und bei Bedarf wiederherzustellen.

Beim Festlegen der Schutzeinstellungen für einen neuen oder bestehenden Bucket kann die Objektsperrung für Ziel-Buckets aktiviert werden, sofern Quell- und Ziel-Cluster ONTAP 9.14.1 oder höher ausführen und die Objektsperrung im Quell-Bucket aktiviert ist. Der Objektsperrmodus und die Aufbewahrungsdauer der Sperre des Quell-Buckets gelten für die replizierten Objekte im Ziel-Bucket. Im Abschnitt **Zieleinstellungen** kann auch eine abweichende Aufbewahrungsdauer für den Ziel-Bucket definiert werden. Diese Aufbewahrungsdauer wird ebenfalls auf alle nicht gesperrten Objekte angewendet, die vom Quell-Bucket und über S3-Schnittstellen repliziert werden.

Informationen darüber, wie die Objektsperre für einen Bucket aktiviert wird, finden sich unter "Einen Bucket erstellen".

CLI

1. Wenn dies die erste SnapMirror S3-Beziehung für diese SVM ist, ist zu überprüfen, ob Root-Benutzer-Schlüssel für sowohl Quell- als auch Ziel-SVMs existieren, und diese gegebenenfalls neu zu generieren:
   `vserver object-store-server user show` + Es ist zu überprüfen, ob ein Zugriffsschlüssel für den Root-Benutzer vorhanden ist. Falls keiner vorhanden ist, ist Folgendes einzugeben:
   `vserver object-store-server user regenerate-keys -vserver svm_name -user root` + Der Schlüssel darf nicht neu generiert werden, wenn bereits einer existiert.
2. Einen Bucket auf der Ziel-SVM als Spiegelungsziel erstellen:

   ```
   vserver object-store-server bucket create -vserver svm_name -bucket
   dest_bucket_name [-size integer[KB|MB|GB|TB|PB]] [-comment text]
   [additional_options]
   ```

3. Es sollte sichergestellt werden, dass die Zugriffsregeln der Standard Bucket-Richtlinien sowohl in der Quell-SVM als auch in der Ziel-SVM korrekt sind:

   ```
   vserver object-store-server bucket policy add-statement -vserver svm_name
   -bucket bucket_name -effect {allow|deny} -action object_store_actions
   -principal user_and_group_names -resource object_store_resources [-sid
   text] [-index integer]
   ```

Beispiel

```
src_cluster::> vserver object-store-server bucket policy add-
statement -bucket test-bucket -effect allow -action
GetObject,PutObject,DeleteObject,ListBucket,GetBucketAcl,GetObjectAc
l,ListBucketMultipartUploads,ListMultipartUploadParts -principal -
-resource test-bucket, test-bucket /*
```

4. Auf der Quell-SVM eine SnapMirror S3-Richtlinie erstellen, falls noch keine vorhanden ist und die Standardrichtlinie nicht verwendet werden soll:

   `snapmirror policy create -vserver svm_name -policy policy_name -type continuous [-rpo integer] [-throttle throttle_type] [-comment text] [additional_options]`

   Parameter:

   - `continuous` – die einzige Richtlinienart für SnapMirror S3-Beziehungen (erforderlich).
   - `-rpo` gibt die Zeit für das Recovery Point Objective in Sekunden an (optional).
   - `-throttle` gibt die Obergrenze für Durchsatz/Bandbreite in Kilobyte/Sekunde an (optional).

   Beispiel

   ```
   src_cluster::> snapmirror policy create -vserver vs0 -type
   continuous -rpo 0 -policy test-policy
   ```

5. CA-Zertifikate auf den Admin-SVMs der Quell- und Ziel-Cluster installieren:
   a. Installieren Sie auf dem Quell-Cluster das CA-Zertifikat, das das *Ziel*-S3-Serverzertifikat signiert hat:
   `security certificate install -type server-ca -vserver src_admin_svm -cert-name dest_server_certificate`
   b. Auf dem Ziel-Cluster das CA-Zertifikat installieren, das das *Quell*-S3-Serverzertifikat signiert hat:
   `security certificate install -type server-ca -vserver dest_admin_svm -cert-name src_server_certificate` + Bei Verwendung eines von einem externen CA-Anbieter signierten Zertifikats ist dasselbe Zertifikat auf der Quell- und Ziel-Admin-SVM zu installieren.

   Weitere Informationen zu `security certificate install` finden sich in der "ONTAP-Befehlsreferenz".

6. Auf dem Quell-SVM eine SnapMirror S3-Beziehung erstellen:

   `snapmirror create -source-path src_svm_name:/bucket/bucket_name -destination-path dest_peer_svm_name:/bucket/bucket_name, …} [-policy policy_name]`

   Sie können eine von Ihnen erstellte Richtlinie verwenden oder die Standardrichtlinie akzeptieren.

Beispiel

```
src_cluster::> snapmirror create -source-path vs0:/bucket/test-
bucket -destination-path vs1:/bucket/test-bucket-mirror -policy
test-policy
```

7. Es sollte überprüft werden, ob die Spiegelung aktiv ist:
`snapmirror show -policy-type continuous -fields status`

Verwandte Informationen

- "snapmirror create"
- "snapmirror policy create"
- "snapmirror show"

Übernahme vom Ziel ONTAP S3-Bucket auf dem Remote-Cluster

Wenn die Daten in einem Quell-Bucket nicht mehr verfügbar sind, kann die SnapMirror Beziehung unterbrochen werden, sodass der Ziel-Bucket beschreibbar ist und Daten bereitgestellt werden können.

Über diese Aufgabe

Bei einer Übernahmeoperation wird der Quell-Bucket in einen schreibgeschützten Bucket umgewandelt und der ursprüngliche Ziel-Bucket in einen Lese-/Schreib-Bucket, wodurch die SnapMirror S3-Beziehung umgekehrt wird.

Wenn der deaktivierte Quell-Bucket wieder verfügbar ist, resynchronisiert SnapMirror S3 die Inhalte der beiden Buckets automatisch. Eine explizite Resynchronisierung der Beziehung ist nicht erforderlich, wie sie bei Volume SnapMirror Deployments notwendig ist.

Die Übernahme muss vom Remote-Cluster aus initiiert werden.

Obwohl SnapMirror S3 Objekte vom Quell-Bucket in einen Ziel-Bucket repliziert, werden Benutzer, Gruppen und Richtlinien nicht vom Quell-Objektspeicher in den Ziel-Objektspeicher repliziert.

Benutzer, Gruppenrichtlinien, Berechtigungen und ähnliche Komponenten müssen im Ziel-Objektspeicher konfiguriert werden, damit Clients während eines Failover-Ereignisses auf den Ziel-Bucket zugreifen können.

Quell- und Zielbenutzer können dieselben Zugriffs- und geheimen Schlüssel verwenden, sofern die Quellschlüssel bei der Erstellung des Benutzers im Ziel-Cluster manuell angegeben werden. Beispiel:

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

System Manager

Failover vom nicht verfügbaren Bucket und Beginn der Datenbereitstellung:

1. **Schutz > Beziehungen** auswählen und dann **SnapMirror S3** wählen.

2. Klicken Sie auf ⋮, wählen Sie **Failover** und dann **Failover**.

CLI

1. Einen Failover-Vorgang für den Ziel-Bucket initiieren:
   `snapmirror failover start -destination-path svm_name:/bucket/bucket_name`
2. Der Status des Failover-Vorgangs kann überprüft werden:
   `snapmirror show -fields status`

   Beispiel

```
dest_cluster::> snapmirror failover start -destination-path
dest_svm1:/bucket/test-bucket-mirror
```

Verwandte Informationen

- "S3-Benutzer und Gruppen hinzufügen (System Manager)"
- "Erstellen eines S3-Benutzers (CLI)"
- "S3-Gruppen erstellen oder ändern (CLI)"
- "SnapMirror Failover Start"
- "snapmirror show"

Ein ONTAP S3-Bucket kann von der Ziel-SVM auf dem Remote-Cluster wiederhergestellt werden.

Wenn Daten in einem Quell-Bucket verloren gehen oder beschädigt werden, kann eine Wiederherstellung der Daten erfolgen, indem Objekte aus einem Ziel-Bucket wiederhergestellt werden.

Über diese Aufgabe

Sie können den Ziel-Bucket in einem vorhandenen Bucket oder in einem neuen Bucket wiederherstellen. Der Ziel-Bucket für die Wiederherstellung muss größer sein als der logisch genutzte Speicherplatz des Ziel-Buckets.

Wenn Sie einen vorhandenen Bucket verwenden, muss dieser beim Start einer Wiederherstellungsoperation leer sein. Die Wiederherstellung führt kein „Rollback“ eines Buckets in der Zeit durch, sondern füllt einen leeren Bucket mit seinem vorherigen Inhalt.

Der Wiederherstellungsvorgang muss vom Remote-Cluster aus gestartet werden.

System Manager

Die gesicherten Daten wiederherstellen:

1. **Schutz > Beziehungen** auswählen und dann **SnapMirror S3** wählen.
2. Klicken Sie ⋮ und wählen Sie dann **Wiederherstellen**.
3. Unter **Quelle Vorhandener Bucket** (Standardeinstellung) oder **Neuer Bucket** auswählen.
   - Um auf einen **vorhandenen Bucket** (Standardeinstellung) wiederherzustellen, sind folgende Schritte erforderlich:

        - Den Cluster und die Storage-VM auswählen, um nach dem vorhandenen Bucket zu suchen.
        - Wählen Sie den vorhandenen Bucket aus.
        - Kopieren und fügen Sie den Inhalt des *destination* S3-Server-CA-Zertifikats ein.
    - Für die Wiederherstellung in einem **neuen Bucket** sind die folgenden Werte anzugeben:
        - Der Cluster und die Storage-VM zum Hosten des neuen Buckets.
        - Name, Kapazität und Leistungsniveau des neuen Buckets. Siehe "Storage-Servicelevel" für weitere Informationen.
        - Der Inhalt des *destination* S3 Server CA-Zertifikats.
4. Unter **Ziel** den Inhalt des CA-Zertifikats des *source* S3-Servers kopieren und einfügen.
5. **Schutz > Beziehungen** kann zur Überwachung des Wiederherstellungsfortschritts verwendet werden.

Gesperrte Buckets wiederherstellen

Ab ONTAP 9.14.1 ist es möglich, gesperrte Buckets zu sichern und bei Bedarf wiederherzustellen.

Sie können einen objektgesperrten Bucket in einem neuen oder vorhandenen Bucket wiederherstellen. Sie können einen objektgesperrten Bucket in den folgenden Szenarien als Ziel auswählen:

- **Wiederherstellung in einem neuen Bucket**: Wenn die Objektsperrung aktiviert ist, kann ein Bucket wiederhergestellt werden, indem ein Bucket erstellt wird, in dem die Objektsperrung ebenfalls aktiviert ist. Beim Wiederherstellen eines gesperrten Buckets werden der Objektsperrmodus und die Aufbewahrungsdauer des ursprünglichen Buckets übernommen. Es kann auch eine andere Aufbewahrungsdauer für die Sperre im neuen Bucket definiert werden. Diese Aufbewahrungsdauer gilt für nicht gesperrte Objekte aus anderen Quellen.
- **Wiederherstellung in einem bestehenden Bucket**: Ein objektgesperrter Bucket kann in einem bestehenden Bucket wiederhergestellt werden, sofern für den bestehenden Bucket Versionierung und ein ähnlicher Objektsperrmodus aktiviert sind. Die Aufbewahrungsdauer des ursprünglichen Buckets bleibt erhalten.
- **Nicht gesperrten Bucket wiederherstellen**: Selbst wenn die Objektsperrung für einen Bucket nicht aktiviert ist, kann er in einem Bucket wiederhergestellt werden, in dem die Objektsperrung aktiviert ist und der sich im Quell-Cluster befindet. Beim Wiederherstellen des Buckets werden alle nicht gesperrten Objekte gesperrt, und der Aufbewahrungsmodus sowie die Aufbewahrungsdauer des Ziel-Buckets gelten für diese Objekte.

CLI

1. Den neuen Ziel-Bucket für die Wiederherstellung erstellen. Weitere Informationen finden sich unter "Eine Cloud-Backup-Beziehung für einen neuen ONTAP S3 Bucket erstellen".
2. Einen Wiederherstellungsvorgang für den Ziel-Bucket initiieren:
   `snapmirror restore -source-path svm_name:/bucket/bucket_name -destination-path svm_name:/bucket/bucket_name`

   Beispiel

   ```
   dest_cluster::> snapmirror restore -source-path
   src_vs1:/bucket/test-bucket -destination-path dest_vs1:/bucket/test-
   bucket-mirror
   ```

Weitere Informationen zu `snapmirror restore` finden sich in der "ONTAP-Befehlsreferenz".

Spiegelungs- und Backup-Schutz im lokalen Cluster

Eine Spiegelbeziehung für einen neuen ONTAP S3 Bucket auf dem lokalen Cluster erstellen

Wenn neue S3-Buckets erstellt werden, ist deren sofortiger Schutz auf ein SnapMirror S3-Ziel im selben Cluster möglich. Gespiegelte Daten können in einen Bucket in einer anderen Storage-VM oder in derselben Storage-VM wie das Quell-System übertragen werden.

Bevor Sie beginnen

- Die Anforderungen an ONTAP Versionen, Lizenzen und die S3-Serverkonfiguration wurden erfüllt.
- Eine Peering-Beziehung besteht zwischen den Quell- und Ziel-Storage-VMs.
- Für die Quell- und Ziel-VMs werden CA-Zertifikate benötigt. Es können selbstsignierte CA-Zertifikate oder Zertifikate eines externen CA-Anbieters verwendet werden.

System Manager

1. Falls dies die erste SnapMirror S3-Beziehung für diese Storage-VM ist, sollte überprüft werden, ob Root-Benutzerschlüssel für sowohl die Quell- als auch die Ziel-Storage-VM vorhanden sind, und sie sollten neu generiert werden, falls dies nicht der Fall ist:
   a. Klicken Sie auf **Speicher > Speicher-VMs** und wählen Sie dann die Speicher-VM aus.
   b. Im Tab **Einstellungen** auf ✎ in der S3-Kachel klicken.
   c. Auf der Registerkarte **Benutzer** ist zu überprüfen, ob ein Zugriffsschlüssel für den Root-Benutzer vorhanden ist
   d. Falls kein Schlüssel vorhanden ist, auf ⋮ neben **root** und anschließend auf **Schlüssel neu generieren** klicken. Der Schlüssel sollte nicht neu generiert werden, falls bereits einer existiert.
2. Die Storage-VM kann bearbeitet werden, um Benutzer hinzuzufügen und Benutzer zu Gruppen hinzuzufügen, sowohl in der Quell- als auch in der Ziel-Storage-VM: **Speicher > Storage-VMs** auswählen, die Storage-VM auswählen, **Einstellungen** auswählen und dann ✎ unter S3 auswählen.

   Siehe "S3-Benutzer und Gruppen hinzufügen" für weitere Informationen.
3. Eine SnapMirror S3-Richtlinie kann erstellt werden, wenn noch keine vorhanden ist und die Standardrichtlinie nicht verwendet werden soll:
   a. Klicken Sie auf **Schutz > Übersicht** und dann auf **Lokale Richtlinieneinstellungen**.
   b. Klicken Sie → neben **Schutzrichtlinien** und dann auf **Hinzufügen**.
      - Geben Sie den Namen und die Beschreibung der Richtlinie ein.
      - Den Richtlinienbereich, den Cluster oder die SVM auswählen
      - **Kontinuierlich** für SnapMirror S3-Beziehungen auswählen.
      - Geben Sie Ihre **Throttle**- und **Recovery Point Objective**-Werte ein.
4. Einen Bucket mit SnapMirror-Schutz erstellen:
   a. Wählen Sie **Speicher > Buckets** und dann **Hinzufügen** aus.

b. Geben Sie einen Namen ein, wählen Sie die Storage-VM aus, geben Sie eine Größe ein und klicken Sie dann auf **Weitere Optionen**.

c. Unter **Berechtigungen** auf **Hinzufügen** klicken. Die Überprüfung der Berechtigungen ist optional, aber empfehlenswert.

- **Principal** und **Effect** – Werte auswählen, die den Einstellungen Ihrer Benutzergruppe entsprechen, oder die Standardwerte übernehmen.
- **Aktionen** – die folgenden Werte werden angezeigt:

```
GetObject,PutObject,DeleteObject,ListBucket,GetBucketAcl,GetObjectAcl,ListBucketMultipartUploads,ListMultipartUploadParts
```

- **Ressourcen** – Standardwerte `(bucketname, bucketname/*)` oder andere benötigte Werte verwenden

  Weitere Informationen zu diesen Bereichen sind unter "Benutzerzugriff auf Buckets verwalten" zu finden.

d. Unter **Schutz** die Option **Enable SnapMirror (ONTAP oder Cloud)** aktivieren. Anschließend die folgenden Werte eingeben:

- Ziel
  - **ZIEL**: ONTAP System
  - **CLUSTER**: Der lokale Cluster wird ausgewählt.
  - **STORAGE VM**: Eine Storage-VM im lokalen Cluster auswählen.
  - **S3 SERVER CA-ZERTIFIKAT**: Den Inhalt des Quellzertifikats kopieren und einfügen.
- Quelle
  - **S3 SERVER CA-ZERTIFIKAT**: Den Inhalt des Zielzertifikats kopieren und einfügen.

5. **Dasselbe Zertifikat auf dem Zielsystem verwenden** auswählen, wenn ein von einem externen CA-Anbieter signiertes Zertifikat verwendet wird.
6. Wenn Sie auf **Zieleinstellungen** klicken, können Sie anstelle der Standardwerte für Bucket-Name, Kapazität und Performance-Servicelevel auch eigene Werte eingeben.
7. Auf **Speichern** klicken. Ein neuer Bucket wird in der Quell-Speicher-VM erstellt und in einen neuen Bucket gespiegelt, der in der Ziel-Speicher-VM erstellt wird.

Verschlossene Buckets sichern

Ab ONTAP 9.14.1 ist es möglich, gesperrte S3-Buckets zu sichern und bei Bedarf wiederherzustellen.

Beim Festlegen der Schutzeinstellungen für einen neuen oder bestehenden Bucket kann die Objektsperrung für Ziel-Buckets aktiviert werden, sofern Quell- und Ziel-Cluster ONTAP 9.14.1 oder höher ausführen und die Objektsperrung im Quell-Bucket aktiviert ist. Der Objektsperrmodus und die Aufbewahrungsdauer der Sperre des Quell-Buckets gelten für die replizierten Objekte im Ziel-Bucket. Im Abschnitt **Zieleinstellungen** kann auch eine abweichende Aufbewahrungsdauer für den Ziel-Bucket definiert werden. Diese Aufbewahrungsdauer wird ebenfalls auf alle nicht gesperrten Objekte angewendet, die vom Quell-Bucket und über S3-Schnittstellen repliziert werden.

Informationen darüber, wie die Objektsperre für einen Bucket aktiviert wird, finden sich unter "Einen Bucket erstellen".

CLI

1. Falls dies die erste SnapMirror S3-Beziehung für diese SVM ist, sollte überprüft werden, ob Root-Benutzerschlüssel für sowohl Quell- als auch Ziel-SVMs vorhanden sind, und sie sollten neu generiert werden, falls sie nicht existieren:
   `vserver object-store-server user show`

   Überprüfen Sie, ob ein Zugriffsschlüssel für den Root-Benutzer vorhanden ist. Falls nicht, Folgendes eingeben:
   `vserver object-store-server user regenerate-keys -vserver svm_name -user root`

   Der Schlüssel sollte nicht neu generiert werden, falls bereits einer existiert.

2. Buckets sowohl in der Quell- als auch in der Ziel-SVM erstellen:

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

3. Zugriffsregeln zu den Standard-Bucket-Richtlinien sowohl in der Quell-SVM als auch in der Ziel-SVM hinzufügen:

   ```
   vserver object-store-server bucket policy add-statement -vserver svm_name
   -bucket bucket_name -effect {allow|deny} -action object_store_actions
   -principal user_and_group_names -resource object_store_resources [-sid
   text] [-index integer]
   ```

   ```
   src_cluster::> vserver object-store-server bucket policy add-
   statement -bucket test-bucket -effect allow -action
   GetObject,PutObject,DeleteObject,ListBucket,GetBucketAcl,GetObjectAc
   l,ListBucketMultipartUploads,ListMultipartUploadParts -principal -
   -resource test-bucket, test-bucket /*
   ```

4. Erstellen Sie eine SnapMirror S3-Richtlinie, falls Sie noch keine haben und nicht die Standardrichtlinie verwenden möchten:
   `snapmirror policy create -vserver svm_name -policy policy_name -type continuous [-rpo integer] [-throttle throttle_type] [-comment text] [additional_options]`

   Parameter:

   - `continuous` – die einzige Richtlinienart für SnapMirror S3-Beziehungen (erforderlich).
   - `-rpo` gibt die Zeit für das Recovery Point Objective in Sekunden an (optional).
   - `-throttle` gibt die Obergrenze für Durchsatz/Bandbreite in Kilobyte/Sekunde an (optional).

   Beispiel

   ```
   src_cluster::> snapmirror policy create -vserver vs0 -type
   continuous -rpo 0 -policy test-policy
   ```

5. CA-Serverzertifikate auf der Admin-SVM installieren:
   a. Das CA-Zertifikat, das das Zertifikat des *source* S3-Servers signiert hat, auf der Admin-SVM installieren:
   `security certificate install -type server-ca -vserver admin_svm -cert -name src_server_certificate`
   b. Das CA-Zertifikat, das das Zertifikat des *Ziel*-S3-Servers signiert hat, auf der Admin-SVM installieren
   `security certificate install -type server-ca -vserver admin_svm -cert -name dest_server_certificate`. Wenn ein von einem externen CA-Anbieter signiertes Zertifikat verwendet wird, ist nur die Installation dieses Zertifikats auf der Admin-SVM erforderlich.

      Weitere Informationen zu `security certificate install` finden sich in der "ONTAP-Befehlsreferenz".

6. Erstellen einer SnapMirror S3-Beziehung:
   `snapmirror create -source-path src_svm_name:/bucket/bucket_name -destination-path dest_peer_svm_name:/bucket/bucket_name, …} [-policy policy_name]`

   Sie können eine von Ihnen erstellte Richtlinie verwenden oder die Standardrichtlinie akzeptieren.

   ```
   src_cluster::> snapmirror create -source-path vs0-src:/bucket/test-bucket -destination-path vs1-dest:/vs1/bucket/test-bucket-mirror -policy test-policy
   ```

7. Es sollte überprüft werden, ob die Spiegelung aktiv ist:
   `snapmirror show -policy-type continuous -fields status`

Verwandte Informationen

- "snapmirror create"
- "snapmirror policy create"
- "snapmirror show"

Eine Spiegelbeziehung für einen vorhandenen ONTAP S3 Bucket auf dem lokalen Cluster erstellen

Sie können jederzeit mit dem Schutz bestehender S3-Buckets auf demselben Cluster beginnen, beispielsweise wenn eine S3-Konfiguration von einer Version vor ONTAP 9.10.1 aktualisiert wurde. Gespiegelte Daten können in einen Bucket in einer anderen Storage-VM oder in derselben Storage-VM wie das Quell-System übertragen werden.

Bevor Sie beginnen

- Die Anforderungen an ONTAP Versionen, Lizenzen und die S3-Serverkonfiguration wurden erfüllt.
- Eine Peering-Beziehung besteht zwischen den Quell- und Ziel-Storage-VMs.
- Für die Quell- und Ziel-VMs werden CA-Zertifikate benötigt. Es können selbstsignierte CA-Zertifikate oder Zertifikate eines externen CA-Anbieters verwendet werden.

System Manager

1. Falls dies die erste SnapMirror S3-Beziehung für diese Storage-VM ist, sollte überprüft werden, ob Root-Benutzerschlüssel für sowohl die Quell- als auch die Ziel-Storage-VM vorhanden sind, und sie sollten neu generiert werden, falls dies nicht der Fall ist:
   a. Klicken Sie auf **Speicher > Speicher-VMs** und wählen Sie dann die Speicher-VM aus.
   b. Im Tab **Einstellungen** auf in der Kachel **S3** klicken.
   c. Auf der Registerkarte **Benutzer** ist zu überprüfen, ob ein Zugriffsschlüssel für den Root-Benutzer vorhanden ist.
   d. Falls kein Schlüssel vorhanden ist, auf neben **root** und anschließend auf **Schlüssel neu generieren** klicken. Der Schlüssel sollte nicht neu generiert werden, falls bereits einer existiert.
2. Es sollte überprüft werden, ob die vorhandenen Benutzer und Gruppen sowohl auf der Quell- als auch auf der Ziel-Speicher-VM vorhanden sind und über die korrekten Zugriffsrechte verfügen: **Speicher > Speicher-VMs** auswählen, dann die gewünschte Speicher-VM und anschließend die Registerkarte **Einstellungen**. Abschließend die Kachel **S3** suchen, auswählen und dann die Registerkarte **Users** sowie anschließend die Registerkarte **Groups** auswählen, um die Zugriffsberechtigungen für Benutzer und Gruppen anzuzeigen.

   Siehe "S3-Benutzer und Gruppen hinzufügen" für weitere Informationen.
3. Eine SnapMirror S3-Richtlinie kann erstellt werden, wenn noch keine vorhanden ist und die Standardrichtlinie nicht verwendet werden soll:
   a. **Schutz > Übersicht** auswählen und anschließend **Lokale Richtlinieneinstellungen** öffnen.
   b. Klicken Sie neben **Schutzrichtlinien** und dann auf **Hinzufügen**.
      - Geben Sie den Namen und die Beschreibung der Richtlinie ein.
      - Den Richtlinienbereich, den Cluster oder die SVM auswählen
      - **Kontinuierlich** für SnapMirror S3-Beziehungen auswählen.
      - Geben Sie Ihre **Throttle**- und **Recovery Point Objective**-Werte ein.
4. Es sollte geprüft werden, ob die Zugriffsrichtlinie des bestehenden Buckets weiterhin den Anforderungen entspricht:
   a. Klicken Sie auf **Storage > Buckets** und wählen Sie dann den Bucket aus, den Sie schützen möchten.
   b. Im Tab **Berechtigungen** auf **Bearbeiten** klicken, dann unter **Berechtigungen** auf **Hinzufügen** klicken.
      - **Principal** und **Effect** – Werte auswählen, die den Einstellungen Ihrer Benutzergruppe entsprechen, oder die Standardwerte übernehmen.
      - **Aktionen** – die folgenden Werte werden angezeigt:

        ```
        GetObject,PutObject,DeleteObject,ListBucket,GetBucketAcl,GetObjectAcl,ListBucketMultipartUploads,ListMultipartUploadParts
        ```

      - **Ressourcen** – Standardwerte *(bucketname, bucketname/*)* oder andere benötigte Werte verwenden.

        Weitere Informationen zu diesen Bereichen sind unter "Benutzerzugriff auf Buckets verwalten"

zu finden.

5. Einen bestehenden Bucket mit SnapMirror S3 schützen:
   a. Klicken Sie auf **Speicher** > **Buckets** und wählen Sie dann den Bucket aus, den Sie schützen möchten.
   b. Auf **Schützen** klicken und die folgenden Werte eingeben:
      - Ziel
        - **ZIEL**: ONTAP System
        - **CLUSTER**: Der lokale Cluster wird ausgewählt.
        - **STORAGE VM**: Dieselbe oder eine andere Storage-VM kann ausgewählt werden.
        - **S3 SERVER CA-ZERTIFIKAT**: Den Inhalt des *Quell*-Zertifikats kopieren und einfügen.
      - Quelle
        - **S3 SERVER CA-ZERTIFIKAT**: Den Inhalt des *Ziel*-Zertifikats kopieren und einfügen.
6. **Dasselbe Zertifikat auf dem Zielsystem verwenden** auswählen, wenn ein von einem externen CA-Anbieter signiertes Zertifikat verwendet wird.
7. Wenn Sie auf **Zieleinstellungen** klicken, können Sie anstelle der Standardwerte für Bucket-Name, Kapazität und Performance-Servicelevel auch eigene Werte eingeben.
8. Auf **Speichern** klicken. Der vorhandene Bucket wird in einen neuen Bucket auf der Ziel-Speicher-VM gespiegelt.

Verschlossene Buckets sichern

Ab ONTAP 9.14.1 ist es möglich, gesperrte S3-Buckets zu sichern und bei Bedarf wiederherzustellen.

Beim Festlegen der Schutzeinstellungen für einen neuen oder bestehenden Bucket kann die Objektsperrung für Ziel-Buckets aktiviert werden, sofern Quell- und Ziel-Cluster ONTAP 9.14.1 oder höher ausführen und die Objektsperrung im Quell-Bucket aktiviert ist. Der Objektsperrmodus und die Aufbewahrungsdauer der Sperre des Quell-Buckets gelten für die replizierten Objekte im Ziel-Bucket. Im Abschnitt **Zieleinstellungen** kann auch eine abweichende Aufbewahrungsdauer für den Ziel-Bucket definiert werden. Diese Aufbewahrungsdauer wird ebenfalls auf alle nicht gesperrten Objekte angewendet, die vom Quell-Bucket und über S3-Schnittstellen repliziert werden.

Informationen darüber, wie die Objektsperre für einen Bucket aktiviert wird, finden sich unter "Einen Bucket erstellen".

CLI

1. Falls dies die erste SnapMirror S3-Beziehung für diese SVM ist, sollte überprüft werden, ob Root-Benutzerschlüssel für sowohl Quell- als auch Ziel-SVMs vorhanden sind, und sie sollten neu generiert werden, falls sie nicht existieren:
   `vserver object-store-server user show`

   Überprüfen Sie, ob ein Zugriffsschlüssel für den Root-Benutzer vorhanden ist. Falls nicht, Folgendes eingeben:
   `vserver object-store-server user regenerate-keys -vserver svm_name -user root`

   Der Schlüssel sollte nicht neu generiert werden, falls bereits einer existiert.

2. Einen Bucket auf der Ziel-SVM als Spiegelungsziel erstellen:

```
vserver object-store-server bucket create -vserver svm_name -bucket
dest_bucket_name [-size integer[KB|MB|GB|TB|PB]] [-comment text]
[additional_options]
```

3. Es sollte sichergestellt sein, dass die Zugriffsregeln für die Standard-Bucket-Richtlinien sowohl in der Quell-SVM als auch in der Ziel-SVM korrekt sind:

   ```
   vserver object-store-server bucket policy add-statement -vserver svm_name
   -bucket bucket_name -effect {allow|deny} -action object_store_actions
   -principal user_and_group_names -resource object_store_resources [-sid
   text] [-index integer]`
   ```

   Beispiel

   ```
   clusterA::> vserver object-store-server bucket policy add-statement
   -bucket test-bucket -effect allow -action
   GetObject,PutObject,DeleteObject,ListBucket,GetBucketAcl,GetObjectAc
   l,ListBucketMultipartUploads,ListMultipartUploadParts -principal -
   -resource test-bucket, test-bucket /*
   ```

4. Eine SnapMirror S3-Richtlinie kann erstellt werden, wenn noch keine vorhanden ist und die Standardrichtlinie nicht verwendet werden soll:

   ```
   snapmirror policy create -vserver svm_name -policy policy_name -type
   continuous [-rpo _integer] [-throttle throttle_type] [-comment text]
   [additional_options]
   ```

   Parameter:

   - `continuous` – die einzige Richtlinienart für SnapMirror S3-Beziehungen (erforderlich).
   - `-rpo` gibt die Zeit für das Recovery Point Objective in Sekunden an (optional).
   - `-throttle` gibt die Obergrenze für Durchsatz/Bandbreite in Kilobyte/Sekunde an (optional).

     Beispiel

     ```
     clusterA::> snapmirror policy create -vserver vs0 -type
     continuous -rpo 0 -policy test-policy
     ```

5. CA-Serverzertifikate auf der Admin-SVM installieren:

   a. Das CA-Zertifikat, das das Zertifikat des *source* S3-Servers signiert hat, auf der Admin-SVM installieren:
   `security certificate install -type server-ca -vserver admin_svm -cert -name src_server_certificate`

   b. Das CA-Zertifikat, das das Zertifikat des *Ziel*-S3-Servers signiert hat, auf der Admin-SVM installieren
   `security certificate install -type server-ca -vserver admin_svm -cert -name dest_server_certificate`. Wenn ein von einem externen CA-Anbieter signiertes Zertifikat verwendet wird, ist nur die Installation dieses Zertifikats auf der Admin-SVM erforderlich.

Weitere Informationen zu `security certificate install` finden sich in der "ONTAP-Befehlsreferenz".

6. Erstellen einer SnapMirror S3-Beziehung:
`snapmirror create -source-path src_svm_name:/bucket/bucket_name -destination-path dest_peer_svm_name:/bucket/bucket_name, …} [-policy policy_name]`

   Sie können eine von Ihnen erstellte Richtlinie verwenden oder die Standardrichtlinie akzeptieren.

   Beispiel

   ```
   src_cluster::> snapmirror create -source-path vs0-src:/bucket/test-bucket -destination-path vs1-dest:/bucket/test-bucket-mirror -policy test-policy
   ```

7. Es sollte überprüft werden, ob die Spiegelung aktiv ist:
`snapmirror show -policy-type continuous -fields status`

Verwandte Informationen

- "snapmirror create"
- "snapmirror policy create"
- "snapmirror show"

Übernahme vom Ziel-ONTAP S3 Bucket auf dem lokalen Cluster

Wenn die Daten in einem Quell-Bucket nicht mehr verfügbar sind, kann die SnapMirror Beziehung unterbrochen werden, sodass der Ziel-Bucket beschreibbar ist und Daten bereitgestellt werden können.

Über diese Aufgabe

Bei einer Übernahmeoperation wird der Quell-Bucket in einen schreibgeschützten Bucket umgewandelt und der ursprüngliche Ziel-Bucket in einen Lese-/Schreib-Bucket, wodurch die SnapMirror S3-Beziehung umgekehrt wird.

Wenn der deaktivierte Quell-Bucket wieder verfügbar ist, resynchronisiert SnapMirror S3 die Inhalte der beiden Buckets automatisch. Eine explizite Resynchronisierung der Beziehung ist nicht erforderlich, wie es bei herkömmlichen Volume SnapMirror Deployments notwendig ist.

Befindet sich der Ziel-Bucket auf einem Remote-Cluster, muss die Übernahme vom Remote-Cluster aus initiiert werden.

System Manager

Failover vom nicht verfügbaren Bucket und Beginn der Datenbereitstellung:

1. **Schutz > Beziehungen** auswählen und dann **SnapMirror S3** wählen.
2. Klicken Sie auf ⋮, wählen Sie **Failover** und dann **Failover**.

CLI

1. Einen Failover-Vorgang für den Ziel-Bucket initiieren:
   `snapmirror failover start -destination-path svm_name:/bucket/bucket_name`
2. Der Status des Failover-Vorgangs kann überprüft werden:
   `snapmirror show -fields status`

Beispiel

```
clusterA::> snapmirror failover start -destination-path vs1:/bucket/test-
bucket-mirror
```

Verwandte Informationen

- "SnapMirror Failover Start"
- "snapmirror show"

Ein ONTAP S3 Bucket kann von der Ziel-SVM auf dem lokalen Cluster wiederhergestellt werden.

Wenn Daten in einem Quell-Bucket verloren gehen oder beschädigt werden, können Sie Ihre Daten wiederherstellen, indem Sie Objekte aus einem Ziel-Bucket wiederherstellen.

Über diese Aufgabe

Sie können den Ziel-Bucket in einem vorhandenen Bucket oder in einem neuen Bucket wiederherstellen. Der Ziel-Bucket für die Wiederherstellung muss größer sein als der logisch genutzte Speicherplatz des Ziel-Buckets.

Wenn Sie einen vorhandenen Bucket verwenden, muss dieser beim Start einer Wiederherstellungsoperation leer sein. Die Wiederherstellung führt kein „Rollback“ eines Buckets in der Zeit durch, sondern füllt einen leeren Bucket mit seinem vorherigen Inhalt.

Der Wiederherstellungsvorgang muss vom lokalen Cluster aus gestartet werden.

System Manager

Die Sicherungsdaten wiederherstellen:

1. Klicken Sie auf **Schutz > Beziehungen** und wählen Sie dann den Bucket aus.
2. Klicken Sie ⋮ und wählen Sie dann **Wiederherstellen**.
3. Unter **Quelle Vorhandener Bucket** (Standardeinstellung) oder **Neuer Bucket** auswählen.
   - Um auf einen **vorhandenen Bucket** (Standardeinstellung) wiederherzustellen, sind folgende Schritte erforderlich:
     - Den Cluster und die Storage-VM auswählen, um nach dem vorhandenen Bucket zu suchen.
     - Wählen Sie den vorhandenen Bucket aus.
4. Kopieren und fügen Sie den Inhalt des CA-Zertifikats des Ziel-S3-Servers ein.
   - Für die Wiederherstellung in einem **neuen Bucket** sind die folgenden Werte anzugeben:
     - Der Cluster und die Storage-VM zum Hosten des neuen Buckets.
     - Name, Kapazität und Leistungsniveau des neuen Buckets. Siehe "Storage-Servicelevel" für weitere Informationen.

- Der Inhalt des CA-Zertifikats des Ziel-S3-Servers.

5. Unter **Ziel** den Inhalt des CA-Zertifikats des Quell-S3-Servers kopieren und einfügen.
6. Klicken Sie auf **Schutz** > Beziehungen, um den Fortschritt der Wiederherstellung zu überwachen.

Gesperrte Buckets wiederherstellen

Ab ONTAP 9.14.1 ist es möglich, gesperrte Buckets zu sichern und bei Bedarf wiederherzustellen.

Sie können einen objektgesperrten Bucket in einem neuen oder vorhandenen Bucket wiederherstellen. Sie können einen objektgesperrten Bucket in den folgenden Szenarien als Ziel auswählen:

- **Wiederherstellung in einem neuen Bucket**: Wenn die Objektsperrung aktiviert ist, kann ein Bucket wiederhergestellt werden, indem ein Bucket erstellt wird, in dem die Objektsperrung ebenfalls aktiviert ist. Beim Wiederherstellen eines gesperrten Buckets werden der Objektsperrmodus und die Aufbewahrungsdauer des ursprünglichen Buckets übernommen. Es kann auch eine andere Aufbewahrungsdauer für die Sperre im neuen Bucket definiert werden. Diese Aufbewahrungsdauer gilt für nicht gesperrte Objekte aus anderen Quellen.
- **Wiederherstellung in einem bestehenden Bucket**: Ein objektgesperrter Bucket kann in einem bestehenden Bucket wiederhergestellt werden, sofern für den bestehenden Bucket Versionierung und ein ähnlicher Objektsperrmodus aktiviert sind. Die Aufbewahrungsdauer des ursprünglichen Buckets bleibt erhalten.
- **Nicht gesperrten Bucket wiederherstellen**: Selbst wenn die Objektsperrung für einen Bucket nicht aktiviert ist, kann er in einem Bucket wiederhergestellt werden, in dem die Objektsperrung aktiviert ist und der sich im Quell-Cluster befindet. Beim Wiederherstellen des Buckets werden alle nicht gesperrten Objekte gesperrt, und der Aufbewahrungsmodus sowie die Aufbewahrungsdauer des Ziel-Buckets gelten für diese Objekte.

CLI

1. Wenn Sie Objekte in einem neuen Bucket wiederherstellen, muss der neue Bucket erstellt werden. Weitere Informationen finden sich unter "Eine Cloud-Backup-Beziehung für einen neuen ONTAP S3 Bucket erstellen".
2. Einen Wiederherstellungsvorgang für den Ziel-Bucket initiieren:
   `snapmirror restore -source-path` *`svm_name`*`:/bucket/`*`bucket_name`* `-destination-path` *`svm_name`*`:/bucket/`*`bucket_name`*

   Beispiel

   ```
   clusterA::> snapmirror restore -source-path vs0:/bucket/test-bucket
   -destination-path vs1:/bucket/test-bucket-mirror
   ```

   Weitere Informationen zu `snapmirror restore` finden sich in der "ONTAP-Befehlsreferenz".

Backup-Schutz mit Cloud-Zielen

Anforderungen für ONTAP SnapMirror S3 Cloud-Zielbeziehungen

Stellen Sie sicher, dass Ihre Quell- und Zielumgebungen die Anforderungen für SnapMirror S3-Backup-Schutz in Cloud-Zielen erfüllen.

Sie benötigen gültige Zugangsdaten beim Objektspeicheranbieter, um auf den Daten-Bucket zugreifen zu

können.

Intercluster LIFs und ein IPspace sollten auf dem Cluster konfiguriert werden, bevor der Cluster eine Verbindung zu einem Cloud Objektspeicher herstellen kann. Intercluster LIFs sollten auf jedem Knoten erstellt werden, um Daten nahtlos vom lokalen Speicher in den Cloud Objektspeicher zu übertragen.

Für StorageGRID Ziele sind folgende Informationen erforderlich:

- Servername, angegeben als vollqualifizierter Domänenname (FQDN) oder IP-Adresse
- Bucket Name; der Bucket muss bereits existieren
- Zugangsschlüssel
- geheimer Schlüssel

Zusätzlich muss das CA-Zertifikat, mit dem das StorageGRID Serverzertifikat signiert wurde, auf der Admin-Storage-VM des ONTAP S3-Clusters mithilfe des `security certificate install` Befehls installiert werden. Weitere Informationen finden sich unter "Installation eines CA-Zertifikats", wenn StorageGRID verwendet wird.

Für AWS S3-Ziele benötigen Sie die folgenden Informationen:

- Servername, angegeben als vollqualifizierter Domänenname (FQDN) oder IP-Adresse
- Bucket Name; der Bucket muss bereits existieren
- Zugangsschlüssel
- geheimer Schlüssel

Der DNS-Server für die Admin-Speicher-VM des ONTAP-Clusters muss in der Lage sein, FQDNs (falls verwendet) in IP-Adressen aufzulösen.

Verwandte Informationen

- "Sicherheitszertifikat installieren"

Eine Cloud-Backup-Beziehung für einen neuen ONTAP S3 Bucket erstellen

Wenn neue S3-Buckets erstellt werden, können diese sofort in einem SnapMirror S3-Ziel-Bucket bei einem Objektspeicher-Anbieter gesichert werden, wobei es sich um ein StorageGRID System oder eine Amazon S3-Bereitstellung handeln kann.

Bevor Sie beginnen

- Sie verfügen über gültige Kontoanmeldeinformationen und Konfigurationsinformationen für den Objektspeicheranbieter.
- Intercluster-Netzwerkschnittstellen und ein IPspace wurden auf dem Quellsystem konfiguriert.
- Die DNS-Konfiguration für die Quell-Speicher-VM muss den FQDN des Ziels auflösen können.

System Manager

1. Die Storage-VM wird bearbeitet, um Benutzer hinzuzufügen und Benutzer Gruppen zuzuordnen:
   a. Klicken Sie auf **Speicher > Speicher-VMs**, klicken Sie auf die Speicher-VM, klicken Sie auf **Einstellungen** und dann auf  unter **S3**.

Siehe "S3-Benutzer und Gruppen hinzufügen" für weitere Informationen.

2. Einen Cloud-Objektspeicher zum Quellsystem hinzufügen:
   a. **Schutz > Übersicht** auswählen und anschließend **Cloud Object Stores** wählen.
   b. Klicken Sie auf **Hinzufügen** und wählen Sie dann **Amazon S3** oder **StorageGRID** aus.
   c. Geben Sie die folgenden Werte ein:
      - Name des Cloud-Objektspeichers
      - URL-Stil (Pfad oder virtual-hosted)
      - Storage VM (für S3 aktiviert)
      - Name des Objektspeicher-Servers (FQDN)
      - Objektspeicherzertifikat
      - Zugangsschlüssel
      - Geheimer Schlüssel
      - Containername (Bucket)
3. Eine SnapMirror S3-Richtlinie kann erstellt werden, falls keine vorhanden ist und die Standardrichtlinie nicht verwendet werden soll:
   a. Klicken Sie auf **Schutz > Übersicht** und dann auf **Lokale Richtlinieneinstellungen**.
   b. Klicken Sie → neben **Schutzrichtlinien** und dann auf **Hinzufügen**.
      - Geben Sie den Namen und die Beschreibung der Richtlinie ein.
      - Den Richtlinienbereich, den Cluster oder die SVM auswählen
      - **Kontinuierlich** für SnapMirror S3-Beziehungen auswählen.
      - Geben Sie Ihre **Throttle**- und **Recovery Point Objective**-Werte ein.
4. Einen Bucket mit SnapMirror-Schutz erstellen:
   a. Klicken Sie auf **Speicher > Buckets** und anschließend auf **Hinzufügen**.
   b. Geben Sie einen Namen ein, wählen Sie die Storage-VM aus, geben Sie eine Größe ein und klicken Sie dann auf **Weitere Optionen**.
   c. Unter **Berechtigungen** auf **Hinzufügen** klicken. Die Überprüfung der Berechtigungen ist optional, aber empfehlenswert.
      - **Principal** und **Effect**: Werte auswählen, die den Einstellungen der Benutzergruppe entsprechen, oder die Standardwerte übernehmen.
      - **Aktionen**: Die folgenden Werte sollten angezeigt werden:

        ```
        GetObject,PutObject,DeleteObject,ListBucket,GetBucketAcl,GetObjectAcl,ListBucketMultipartUploads,ListMultipartUploadParts
        ```

      - **Ressourcen**: Die Standardwerte `_(bucketname, bucketname/*)` oder andere benötigte Werte verwenden.

        Weitere Informationen zu diesen Bereichen sind unter "Benutzerzugriff auf Buckets verwalten" zu finden.

d. Unter **Schutz** die Option **Enable SnapMirror (ONTAP oder Cloud)** aktivieren, **Cloud Storage** auswählen und dann den **Cloud Object Store** auswählen.

Wenn Sie auf **Speichern** klicken, wird ein neuer Bucket in der Quell-Speicher-VM erstellt und im Cloud-Objektspeicher gesichert.

CLI

1. Wenn dies die erste SnapMirror S3-Beziehung für diese SVM ist, muss überprüft werden, ob Root-Benutzerschlüssel für sowohl Quell- als auch Ziel-SVMs vorhanden sind, und sie müssen neu generiert werden, falls sie nicht existieren:
`vserver object-store-server user show` Es sollte bestätigt werden, dass ein Zugriffsschlüssel für den Root-Benutzer vorhanden ist. Falls keiner vorhanden ist, ist Folgendes einzugeben:
`vserver object-store-server user regenerate-keys -vserver svm_name -user root` + Der Schlüssel darf nicht neu generiert werden, wenn bereits einer existiert.
2. Erstellen eines Buckets in der Quell-SVM:
`vserver object-store-server bucket create -vserver svm_name -bucket bucket_name [-size integer[KB|MB|GB|TB|PB]] [-comment text] [additional_options]`
3. Zugriffsregeln zur Standard-Bucket-Richtlinie hinzufügen:
`vserver object-store-server bucket policy add-statement -vserver svm_name -bucket bucket_name -effect {allow|deny} -action object_store_actions -principal user_and_group_names -resource object_store_resources [-sid text] [-index integer]`

   Beispiel

   ```
   clusterA::> vserver object-store-server bucket policy add-statement
   -bucket test-bucket -effect allow -action
   GetObject,PutObject,DeleteObject,ListBucket,GetBucketAcl,GetObjectAc
   l,ListBucketMultipartUploads,ListMultipartUploadParts -principal -
   -resource test-bucket, test-bucket /*
   ```

4. Erstellen Sie eine SnapMirror S3-Richtlinie, falls Sie noch keine haben und nicht die Standardrichtlinie verwenden möchten:
`snapmirror policy create -vserver svm_name -policy policy_name -type continuous [-rpo integer] [-throttle throttle_type] [-comment text] [additional_options]`

   Parameter: * `type continuous` – der einzige Richtlinientyp für SnapMirror S3-Beziehungen (erforderlich). * `-rpo` – gibt die Zeit bis zum Wiederherstellungspunkt in Sekunden an (optional). * `-throttle` – gibt die Obergrenze für Durchsatz/Bandbreite in Kilobyte/Sekunde an (optional).

   Beispiel

   ```
   clusterA::> snapmirror policy create -vserver vs0 -type continuous
   -rpo 0 -policy test-policy
   ```

5. Wenn das Ziel ein StorageGRID System ist, das StorageGRID CA Serverzertifikat auf der Admin-

SVM des Quell-Cluster installieren:
`security certificate install -type server-ca -vserver src_admin_svm -cert -name storage_grid_server_certificate`

Weitere Informationen zu `security certificate install` finden sich in der "ONTAP-Befehlsreferenz".

6. Den SnapMirror S3 Objektspeicher als Ziel definieren:
`snapmirror object-store config create -vserver svm_name -object-store-name target_store_name -usage data -provider-type {AWS_S3|SGWS} -server target_FQDN -container-name remote_bucket_name -is-ssl-enabled true -port port_number -access-key target_access_key -secret-password target_secret_key`

Parameter: * `-object-store-name` – der Name des Objektspeicherziels auf dem lokalen ONTAP System. * `-usage` – `data` für diesen Workflow verwenden. * `-provider-type` – `AWS_S3` und `SGWS` (StorageGRID) Ziele werden unterstützt. * `-server` – der FQDN oder die IP-Adresse des Zielservers. * `-is-ssl-enabled` – die Aktivierung von SSL ist optional, aber empfohlen. + Weitere Informationen zu `snapmirror object-store config create` in der "ONTAP-Befehlsreferenz".

Beispiel

```
src_cluster::> snapmirror object-store config create -vserver vs0
-object-store-name sgws-store -usage data -provider-type SGWS
-server sgws.example.com -container-name target-test-bucket -is-ssl
-enabled true -port 443 -access-key abc123 -secret-password xyz890
```

7. Erstellen einer SnapMirror S3-Beziehung:
`snapmirror create -source-path svm_name:/bucket/bucket_name -destination -path object_store_name:/objstore -policy policy_name`

Parameter: * `-destination-path` – der im vorherigen Schritt erstellte Objektspeichername und der feste Wert `objstore`. + Es kann eine selbst erstellte Richtlinie verwendet oder die Standardrichtlinie übernommen werden.

Beispiel

```
src_cluster::> snapmirror create -source-path vs0:/bucket/test-
bucket -destination-path sgws-store:/objstore -policy test-policy
```

8. Es sollte überprüft werden, ob die Spiegelung aktiv ist:
`snapmirror show -policy-type continuous -fields status`

Verwandte Informationen

- "snapmirror create"
- "snapmirror policy create"
- "snapmirror show"

Eine Cloud-Backup-Beziehung für einen vorhandenen ONTAP S3 Bucket erstellen

Sie können jederzeit mit der Sicherung bestehender S3 Buckets beginnen, beispielsweise wenn eine S3 Konfiguration von einer Version vor ONTAP 9.10.1 aktualisiert wurde.

Bevor Sie beginnen

- Sie verfügen über gültige Kontoanmeldeinformationen und Konfigurationsinformationen für den Objektspeicheranbieter.
- Intercluster-Netzwerkschnittstellen und ein IPspace wurden auf dem Quellsystem konfiguriert.
- Die DNS-Konfiguration für die Quell-Speicher-VM muss den FQDN des Ziels auflösen können.

System Manager

1. Überprüfen Sie, ob die Benutzer und Gruppen korrekt definiert sind: Klicken Sie auf **Speicher > Speicher-VMs**, klicken Sie auf die Speicher-VM, klicken Sie auf **Einstellungen** und dann auf unter S3.

   Siehe "S3-Benutzer und Gruppen hinzufügen" für weitere Informationen.

2. Eine SnapMirror S3-Richtlinie kann erstellt werden, wenn noch keine vorhanden ist und die Standardrichtlinie nicht verwendet werden soll:
   a. **Schutz > Übersicht** und danach **Lokale Richtlinieneinstellungen** auswählen.
   b. Klicken Sie → neben **Schutzrichtlinien** und dann auf **Hinzufügen**.
   c. Geben Sie den Namen und die Beschreibung der Richtlinie ein.
   d. Den Richtlinienbereich, den Cluster oder die SVM auswählen
   e. **Kontinuierlich** für SnapMirror S3-Beziehungen auswählen.
   f. Geben Sie Ihre **Throttle**- und **Recovery Point Objective**-Werte ein.
3. Einen Cloud-Objektspeicher zum Quellsystem hinzufügen:
   a. **Schutz > Übersicht** auswählen und anschließend **Cloud Object Store** wählen.
   b. Wählen Sie **Hinzufügen** und dann **Amazon S3** oder **Andere** für StorageGRID Webscale aus.
   c. Geben Sie die folgenden Werte ein:
      - Name des Cloud-Objektspeichers
      - URL-Stil (Pfad oder virtual-hosted)
      - Storage VM (für S3 aktiviert)
      - Name des Objektspeicher-Servers (FQDN)
      - Objektspeicherzertifikat
      - Zugangsschlüssel
      - Geheimer Schlüssel
      - Containername (Bucket)
4. Es sollte geprüft werden, ob die Zugriffsrichtlinie des bestehenden Buckets weiterhin den eigenen Anforderungen entspricht:
   a. Klicken Sie auf **Speicher** > **Buckets** und wählen Sie dann den Bucket aus, den Sie schützen möchten.

b. Im Tab **Berechtigungen** auf **Bearbeiten** klicken, dann unter **Berechtigungen** auf **Hinzufügen** klicken.

- **Principal** und **Effect** – Werte auswählen, die den Einstellungen Ihrer Benutzergruppe entsprechen, oder die Standardwerte übernehmen.
- **Aktionen** – es wird sichergestellt, dass die folgenden Werte angezeigt werden: `GetObject,PutObject,DeleteObject,ListBucket,GetBucketAcl,GetObjectAcl,ListBucketMultipartUploads,ListMultipartUploadParts`
- **Ressourcen** – Standardwerte *(bucketname, bucketname/*)* oder andere benötigte Werte verwenden.

  Weitere Informationen zu diesen Bereichen sind unter "Benutzerzugriff auf Buckets verwalten" zu finden.

5. Den Bucket mit SnapMirror S3 sichern:
   a. Klicken Sie auf **Speicher** > **Buckets** und wählen Sie dann den Bucket aus, den Sie sichern möchten.
   b. Klicken Sie auf **Schützen**, wählen Sie unter **Ziel Cloud-Speicher** und anschließend den **Cloud Object Store** aus.

Wenn Sie auf **Speichern** klicken, wird der bestehende Bucket im Cloud-Objektspeicher gesichert.

CLI

1. Es sollte überprüft werden, ob die Zugriffsregeln in der Standard Bucket-Richtlinie korrekt sind:
   `vserver object-store-server bucket policy add-statement -vserver svm_name -bucket bucket_name -effect {allow|deny} -action object_store_actions -principal user_and_group_names -resource object_store_resources [-sid text] [-index integer]`

   Beispiel

   ```
   clusterA::> vserver object-store-server bucket policy add-statement
   -bucket test-bucket -effect allow -action
   GetObject,PutObject,DeleteObject,ListBucket,GetBucketAcl,GetObjectAc
   l,ListBucketMultipartUploads,ListMultipartUploadParts -principal -
   -resource test-bucket, test-bucket /*
   ```

2. Erstellen Sie eine SnapMirror S3-Richtlinie, falls Sie noch keine haben und nicht die Standardrichtlinie verwenden möchten:
   `snapmirror policy create -vserver svm_name -policy policy_name -type continuous [-rpo integer] [-throttle throttle_type] [-comment text] [additional_options]`

   Parameter: * `type continuous` – der einzige Richtlinientyp für SnapMirror S3-Beziehungen (erforderlich). * `-rpo` – gibt die Zeit bis zum Wiederherstellungspunkt in Sekunden an (optional). * `-throttle` – gibt die Obergrenze für Durchsatz/Bandbreite in Kilobyte/Sekunde an (optional).

   Beispiel

   ```
   clusterA::> snapmirror policy create -vserver vs0 -type continuous
   ```

```
-rpo 0 -policy test-policy
```

3. Wenn das Ziel ein StorageGRID System ist, das StorageGRID CA-Zertifikat auf der Admin-SVM des Quell-Cluster installieren:
`security certificate install -type server-ca -vserver src_admin_svm -cert -name storage_grid_server_certificate`

   Weitere Informationen zu `security certificate install` finden sich in der "ONTAP-Befehlsreferenz".

4. Den SnapMirror S3 Objektspeicher als Ziel definieren:
`snapmirror object-store config create -vserver svm_name -object-store-name target_store_name -usage data -provider-type {AWS_S3|SGWS} -server target_FQDN -container-name remote_bucket_name -is-ssl-enabled true -port port_number -access-key target_access_key -secret-password target_secret_key`

   Parameter: * `-object-store-name` – der Name des Objektspeicherziels auf dem lokalen ONTAP System. * `-usage` – `data` für diesen Workflow verwenden. * `-provider-type` – `AWS_S3` und `SGWS` (StorageGRID) Ziele werden unterstützt. * `-server` – der FQDN oder die IP-Adresse des Zielservers. * `-is-ssl-enabled` – die Aktivierung von SSL ist optional, aber empfohlen. + Weitere Informationen zu `snapmirror object-store config create` in der "ONTAP-Befehlsreferenz".

   Beispiel

   ```
   src_cluster::> snapmirror object-store config create -vserver vs0
   -object-store-name sgws-store -usage data -provider-type SGWS
   -server sgws.example.com -container-name target-test-bucket -is-ssl
   -enabled true -port 443 -access-key abc123 -secret-password xyz890
   ```

5. Erstellen einer SnapMirror S3-Beziehung:
`snapmirror create -source-path svm_name:/bucket/bucket_name -destination -path object_store_name:/objstore -policy policy_name`

   Parameter: * `-destination-path` – der im vorherigen Schritt erstellte Objektspeichername und der feste Wert `objstore`. + Es kann eine selbst erstellte Richtlinie verwendet oder die Standardrichtlinie übernommen werden.

   ```
   src_cluster::> snapmirror create -source-path vs0:/bucket/buck-evp
   -destination-path sgws-store:/objstore -policy test-policy
   ```

6. Es sollte überprüft werden, ob die Spiegelung aktiv ist:
`snapmirror show -policy-type continuous -fields status`

Verwandte Informationen

- "snapmirror create"
- "snapmirror policy create"

- "snapmirror show"

Wiederherstellung eines ONTAP S3-Buckets aus einem Cloud-Ziel

Wenn Daten in einem Quell-Bucket verloren gehen oder beschädigt werden, lässt sich der Datenbestand durch Wiederherstellung aus einem Ziel-Bucket wieder auffüllen.

Über diese Aufgabe

Sie können den Ziel-Bucket in einem vorhandenen Bucket oder in einem neuen Bucket wiederherstellen. Der Ziel-Bucket für die Wiederherstellung muss größer sein als der logisch genutzte Speicherplatz des Ziel-Buckets.

Wenn Sie einen vorhandenen Bucket verwenden, muss dieser beim Start einer Wiederherstellungsoperation leer sein. Die Wiederherstellung führt kein „Rollback“ eines Buckets in der Zeit durch, sondern füllt einen leeren Bucket mit seinem vorherigen Inhalt.

System Manager

Die Sicherungsdaten wiederherstellen:

1. **Schutz > Beziehungen** auswählen und dann **SnapMirror S3** wählen.
2. Klicken Sie ⋮ und wählen Sie dann **Wiederherstellen**.
3. Unter **Quelle Vorhandener Bucket** (Standardeinstellung) oder **Neuer Bucket** auswählen.
   - Um auf einen **vorhandenen Bucket** (Standardeinstellung) wiederherzustellen, sind folgende Schritte erforderlich:
     - Den Cluster und die Storage-VM auswählen, um nach dem vorhandenen Bucket zu suchen.
     - Wählen Sie den vorhandenen Bucket aus.
     - Kopieren und fügen Sie den Inhalt des *destination* S3-Server-CA-Zertifikats ein.
   - Für die Wiederherstellung in einem **neuen Bucket** sind die folgenden Werte anzugeben:
     - Der Cluster und die Storage-VM zum Hosten des neuen Buckets.
     - Name, Kapazität und Leistungsservicelevel des neuen Buckets. Siehe "Storage-Servicelevel" für weitere Informationen.
     - Der Inhalt des CA-Zertifikats des Ziel-S3-Servers.
4. Unter **Ziel** den Inhalt des CA-Zertifikats des *source* S3-Servers kopieren und einfügen.
5. **Schutz > Beziehungen** kann zur Überwachung des Wiederherstellungsfortschritts verwendet werden.

CLI Prozedur

1. Den neuen Ziel-Bucket für die Wiederherstellung erstellen. Weitere Informationen finden sich unter "Erstellen einer Backup-Beziehung für einen Bucket (Cloud-Ziel)".
2. Einen Wiederherstellungsvorgang für den Ziel-Bucket initiieren:
   `snapmirror restore -source-path` *`object_store_name`*`:/objstore -destination -path` *`svm_name`*`:/bucket/`*`bucket_name`*

   Beispiel

   Das folgende Beispiel stellt einen Ziel-Bucket in einem bestehenden Bucket wieder her.

```
clusterA::> snapmirror restore -source-path sgws.store:/objstore
```

```
-destination-path vs0:/bucket/test-bucket
```

Weitere Informationen zu `snapmirror restore` finden sich in der "ONTAP-Befehlsreferenz".

Eine ONTAP SnapMirror S3-Richtlinie ändern

Möglicherweise wird eine S3 SnapMirror Richtlinie geändert, wenn eine Anpassung der RPO- und Drosselungswerte erforderlich ist.

System Manager

1. Klicken Sie auf **Schutz > Beziehungen** und wählen Sie dann die Datensicherungsstrategie für die Beziehung aus, die Sie ändern möchten.
2. Klicken Sie ⋮ neben dem Namen der Policy und dann auf **Bearbeiten**.

CLI

Eine SnapMirror S3-Richtlinie ändern:
`snapmirror policy modify -vserver <svm_name> -policy <policy_name> [-rpo <integer>] [-throttle <throttle_type>] [-comment <text>]`

Parameter:

- `-rpo`: Gibt die Zeit für das Recovery Point Objective in Sekunden an.
- `-throttle`: Gibt die Obergrenze für Durchsatz/Bandbreite in Kilobyte/Sekunde an.

```
clusterA::> snapmirror policy modify -vserver vs0 -policy test-policy
-rpo 60
```

Verwandte Informationen

- "snapmirror policy modify"

S3-Daten mit Snapshots schützen

Informationen zu ONTAP S3 Snapshots

Ab ONTAP 9.16.1 kann die ONTAP Snapshot-Technologie verwendet werden, um schreibgeschützte, zeitpunktgenaue Images der ONTAP S3 Buckets zu erzeugen.

Mit der S3 Snapshots Funktion lassen sich Snapshots manuell erstellen oder automatisch über Snapshot Richtlinien generieren. S3 Snapshots werden S3 Clients als S3 Buckets präsentiert. Das Durchsuchen und Wiederherstellen der Inhalte aus den Snapshots ist über S3 Clients möglich.

S3-Snapshots erfassen nur die aktuellen Versionen der Objekte in S3-Buckets. Die nicht aktuellen Versionen versionierter Buckets werden in den S3-Snapshots nicht erfasst. Außerdem werden die zeitpunktgenauen Objekt-Tags in den Snapshots nicht erfasst, wenn die Objekt-Tags nach der Erstellung der Snapshots geändert werden.

S3 Snapshots sind von der Clusterzeit abhängig. Der NTP-Server sollte im Cluster konfiguriert werden, um die Zeit zu synchronisieren. Weitere Informationen finden sich unter "Clusterzeit verwalten".

Quota- und Platznutzung

Quotas erfassen die Anzahl der Objekte und die logische Größe, die in einem S3-Bucket verwendet werden. Wenn S3-Snapshots erstellt werden, werden die in den S3-Snapshots erfassten Objekte auf die Anzahl der Objekte und die verwendete Größe des Buckets angerechnet, bis die Snapshots aus dem Dateisystem gelöscht werden.

Mehrteilige Objekte

Bei mehrteiligen Objekten werden nur die finalen Objekte in Snapshots erfasst. Teilweise Uploads mehrteiliger Objekte werden nicht in Snapshots erfasst.

Snapshots von versionierten und nicht versionierten Buckets

Sie können Snapshots sowohl für versionierte als auch für nicht versionierte Buckets erstellen. Der Snapshot enthält nur die aktuellen Objektversionen zum Zeitpunkt der Snapshot-Erstellung.

Versionierte Buckets und Snapshots

In Buckets mit aktivierter Objektversionierung speichert ein Snapshot den Inhalt der aktuellsten Objektversion, nach der der Snapshot erstellt wurde. Nicht-aktuelle Versionen im Bucket werden ausgeschlossen.

Betrachten Sie dieses Beispiel: In einem Bucket, in dem die Objektversionierung aktiviert ist, hat das Objekt `obj1` die Versionen v1, v2, v3, v4, v5. Ein Snapshot `snap1` wurde von `obj1` v3 (der zum Zeitpunkt der Aufnahme aktuellsten Version) erstellt. Beim Durchsuchen `snap1`, `obj1` erscheint das Objekt mit dem Inhalt, der bei v3 erstellt wurde. Inhalte der vorherigen Versionen werden nicht zurückgegeben.

Die nicht aktuellen Versionen bleiben im Dateisystem erhalten, bis die Snapshots gelöscht werden.

Nicht versionierte Buckets und Snapshots

In nicht versionierten Buckets bewahren S3-Snapshots den Inhalt der letzten Commits vor der Erstellung des Snapshots.

Betrachten Sie dieses Beispiel: In einem Bucket, in dem keine Objektversionierung verfügbar ist, wurde das Objekt `obj1`mehrmals überschrieben (zu den Zeitpunkten t1, t2, t3, t4 und t5). Ein S3-Snapshot `snap1`wurde irgendwann zwischen t3 und t4 erstellt. Beim Durchsuchen `snap1`, `obj1`erscheint das Objekt mit dem Inhalt, der zu t3 erstellt wurde.

Objektablauf und Snapshots

Die Funktionen ONTAP S3 Object Expiration und S3 Snapshots arbeiten unabhängig voneinander. Die ONTAP Object Expiration Funktion lässt Objektversionen gemäß den für den S3-Bucket definierten Lifecycle-Management-Regeln ablaufen. S3 Snapshots sind statische Kopien der Bucket-Objekte zu einem Zeitpunkt, an dem der Snapshot erstellt wird.

Wenn die Objektversionierung in einem Bucket aktiviert ist, bleibt beim Löschen einer bestimmten Version eines Objekts aufgrund einer für diesen Bucket definierten Ablaufregel der Inhalt der abgelaufenen Objektversion weiterhin im Dateisystem erhalten, sofern diese Version als aktuelle Version in einem oder mehreren S3-Snapshots erfasst wurde. Diese Objektversion existiert im Dateisystem erst dann nicht mehr, wenn der entsprechende Snapshot gelöscht wird.

In einem Bucket, in dem die Versionierung deaktiviert ist, bleibt ein Objekt, das aufgrund einer Ablaufregel gelöscht wird, aber noch in vorhandenen S3-Snapshots erfasst ist, im Dateisystem erhalten. Das Objekt wird dauerhaft aus dem Dateisystem entfernt, wenn die Snapshots, die es erfassen, gelöscht werden.

Informationen zum Ablauf von S3-Objekten und zum Lebenszyklusmanagement finden sich unter "Erstellen einer Bucket Lifecycle Management-Regel".

Einschränkungen bei S3 Snapshots

Sie sollten sich der folgenden Funktionsausschlüsse und Szenarien bewusst sein:

- Sie können bis zu 1023 Snapshots für einen S3-Bucket generieren.
- Alle S3-Snapshots und Metadaten müssen aus allen Buckets in einem Cluster gelöscht werden, bevor der Cluster auf eine ONTAP Version vor ONTAP 9.16.1 zurückgesetzt wird.
- Wenn Sie einen S3-Bucket löschen müssen, der Objekte mit Snapshots enthält, muss sichergestellt sein, dass alle entsprechenden Snapshots aller Objekte in diesem Bucket gelöscht wurden.
- S3 Snapshots werden in diesen Konfigurationen nicht unterstützt:
  - Zu Buckets in einer SnapMirror Beziehung
  - Bei Buckets, in denen die Objektsperrung aktiviert ist
  - In der NetApp Console
  - Im System Manager
  - In ONTAP MetroCluster Konfigurationen
- S3-Snapshots werden für Buckets, die als lokale oder Remote FabricPool Kapazitätsebene verwendet werden, nicht empfohlen.

ONTAP S3 Snapshots erstellen

Sie können S3-Snapshots entweder manuell erstellen oder Snapshot-Richtlinien einrichten, die automatisch S3-Snapshots für Sie erstellen. Snapshots dienen als statische Kopien von Objekten, die für Backup und Recovery verwendet werden. Zur Bestimmung der Aufbewahrungsdauer von Snapshots können Snapshot-Richtlinien erstellt werden, die die automatische Erstellung von Snapshots in festgelegten Intervallen ermöglichen.

S3 Snapshots helfen dabei, Objektdaten in S3 Buckets mit oder ohne aktivierte Objektversionierung zu schützen.



Snapshots können besonders nützlich sein, um den Datenschutz zu gewährleisten, wenn die Objektversionierung in einem S3-Bucket nicht aktiviert ist, da sie als zeitpunktgenaue Aufzeichnungen dienen, die für Wiederherstellungsvorgänge verwendet werden können, wenn keine frühere Objektversion verfügbar ist.

Über diese Aufgabe

- Für Snapshots gelten folgende Namenskonventionen (sowohl für manuelle als auch für automatische Snapshots):
  - S3 Snapshot Namen können bis zu 30 Zeichen lang sein
  - S3 Snapshot Namen dürfen nur aus Kleinbuchstaben, Zahlen, Punkten (.) und Bindestrichen (-)

bestehen.

  - S3 Snapshot Namen müssen mit einem Buchstaben oder einer Zahl enden.
  - S3 Snapshot Namen dürfen keine Teilzeichenfolgen enthalten `s3snap`

- Im Kontext des S3-Protokolls ist der Bucket-Name auf 63 Zeichen beschränkt. Da ONTAP S3 Snapshots über das S3-Protokoll als Buckets präsentiert werden, gelten ähnliche Beschränkungen auch für die Namen der Snapshot-Buckets. Standardmäßig wird der ursprüngliche Bucket-Name als Basis-Bucket-Name verwendet.
- Um die Zuordnung von Snapshots zu Buckets zu vereinfachen, besteht der Name des Snapshot-Buckets aus dem Namen des Basis-Buckets und einer speziellen Zeichenfolge, `-s3snap-`, die dem Snapshot-Namen vorangestellt wird. Die Namen der Snapshot-Buckets haben das Format `<base_bucket_name>-s3snap-<snapshot_name>`.

  Wenn zum Beispiel der folgende Befehl ausgeführt wird, um `snap1` auf `bucket-a` einen Snapshot-Bucket mit dem Namen `bucket-a-s3snap-snap1` zu erstellen, ist dieser über S3-Clients zugänglich, sofern Sie die Berechtigung zum Zugriff auf den Basis-Bucket haben.

```
vserver object-store-server bucket snapshot create -bucket bucket-a
-snapshot snap1
```

- Es ist nicht möglich, einen Snapshot zu erstellen, dessen Snapshot-Bucket-Name mehr als 63 Zeichen enthält.
- Der Name des automatischen Snapshots enthält den Namen des Richtlinienzeitplans und den Zeitstempel, was der Namenskonvention für herkömmliche Volume Snapshots entspricht. Beispielsweise können die Namen der geplanten Snapshots `daily-2024-01-01-0015` und `hourly-2024-05-22-1105` sein.

S3-Snapshots manuell erstellen

Sie können einen S3-Snapshot manuell mithilfe der ONTAP CLI erstellen. Das Verfahren erstellt einen Snapshot nur auf dem lokalen Cluster.

Schritte

1. Einen S3-Snapshot erstellen:

```
vserver object-store-server bucket snapshot create -vserver <svm_name>
-bucket <bucket_name> -snapshot <snapshot_name>
```

   Das folgende Beispiel erstellt einen Snapshot mit dem Namen `pre-update` auf der `vs0` Storage-VM und dem `website-data` Bucket:

```
vserver object-store-server bucket snapshot create -vserver vs0 -bucket
website-data -snapshot pre-update
```

Einem Bucket eine S3 Snapshot-Richtlinie zuweisen

Wenn Sie Snapshot-Richtlinien auf S3-Bucket-Ebene konfigurieren, erstellt ONTAP automatisch geplante S3-

Snapshots für Sie. Wie bei herkömmlichen Snapshot-Richtlinien können bis zu fünf Zeitpläne für S3-Snapshots konfiguriert werden.

Eine Snapshot-Richtlinie legt typischerweise die Zeitpläne für die Erstellung von Snapshots, die Anzahl der für jeden Zeitplan aufzubewahrenden Kopien und das Zeitplanpräfix fest. Beispielsweise kann eine Richtlinie täglich um 0:10 Uhr einen S3 Snapshot erstellen, die beiden aktuellsten Kopien aufbewahren und diese `daily-<timestamp>` benennen.

Die standardmäßige Snapshot-Richtlinie bewahrt Folgendes auf:

- Sechs stündliche Snapshots
- Zwei tägliche Snapshots
- Zwei wöchentliche Snapshots

Bevor Sie beginnen

- Vor der Zuweisung zum S3-Bucket muss eine Snapshot-Richtlinie erstellt worden sein.

> Für S3 Snapshots gelten dieselben Regeln wie für andere ONTAP Snapshot Richtlinien. Eine Snapshot Richtlinie, deren Aufbewahrungsfrist in einem der Snapshot Zeitpläne konfiguriert ist, kann jedoch keinem S3 Bucket zugewiesen werden.

Weitere Informationen zum Erstellen von Snapshot-Richtlinien für die automatische Generierung von Snapshots sind unter "Übersicht zur Konfiguration benutzerdefinierter Snapshot-Richtlinien" zu finden.

Schritte

1. Die Snapshot-Richtlinie wird Ihrem Bucket zugewiesen:

```
vserver object-store-server bucket create -vserver <svm_name> -bucket
<bucket_name> -snapshot-policy <policy_name>
```

oder

```
vserver object-store-server bucket modify -vserver <svm_name> -bucket
<bucket_name> -snapshot-policy <policy_name>
```

> Falls ein Cluster auf eine ONTAP Version vor ONTAP 9.16.1 zurückgesetzt werden muss, ist sicherzustellen, dass der Wert für `snapshot-policy` für alle Buckets auf `none` (oder `-`) gesetzt ist.

Verwandte Informationen

"Informationen zu ONTAP S3 Snapshots"

ONTAP S3 Snapshots anzeigen und wiederherstellen

Ab ONTAP 9.16.1 können Sie S3 Snapshot-Daten Ihrer Buckets von S3 Clients aus anzeigen und durchsuchen. Ab ONTAP 9.18.1 ist der S3 Snapshot Bucket nativ über die ONTAP CLI zugänglich. Zusätzlich besteht die Möglichkeit, auf einem S3 Client ein

einzelnes Objekt, eine Gruppe von Objekten oder einen gesamten Bucket aus einem S3 Snapshot wiederherzustellen.

Bevor Sie beginnen

- Alle Knoten im Cluster müssen ONTAP 9.18.1 oder höher ausführen, bevor die Bucket-Snapshot-Wiederherstellung nativ in der ONTAP CLI durchgeführt werden kann. Ab ONTAP 9.18.1 ist der S3 Browser nicht mehr erforderlich, die Operationen werden aber weiterhin unterstützt.
- Für einen bestimmten Bucket ist jeweils nur eine Snapshot-Wiederherstellung zulässig.

Über diese Aufgabe

Ab ONTAP 9.16.1 bietet die ONTAP S3 Snapshots-Funktion grundlegende Snapshot-Funktionalität für ONTAP S3 Buckets, einschließlich manueller und geplanter Snapshot-Erstellung und -Löschung, Snapshot-Richtlinien für S3 Buckets sowie S3-Client-basiertem Durchsuchen von Snapshots.

Ab ONTAP 9.18.1 wird die native ONTAP Snapshot-Wiederherstellung unterstützt, wodurch ONTAP-Administratoren eine zeitpunktgenaue Restore-Funktionalität ohne die Verwendung eines S3-Browsers zur Verfügung steht. Im Snapshot wird nur die aktuelle Bucket-Version erfasst. Der Versionsverlauf wird nicht erfasst und wird durch die S3 Snapshot Restore-Operation nicht wiederhergestellt.

S3 Snapshots auflisten und anzeigen

Sie können die Details der S3-Snapshots anzeigen, vergleichen und Fehler identifizieren. Mit der ONTAP CLI können alle auf Ihren S3-Buckets erstellten Snapshots aufgelistet werden.

Schritte

1. S3-Snapshots auflisten:

   ```
   vserver object-store-server bucket snapshot show
   ```

   Sie können die Snapshot-Namen, Storage-VMs, Buckets, Erstellungszeiten und Instance-UUIDs der für alle Ihre Buckets im Cluster erstellten S3-Snapshots anzeigen.

2. Sie können auch einen Bucket-Namen angeben, um die Namen, Erstellungszeiten und Instanz-UUIDs aller für diesen spezifischen Bucket erstellten S3-Snapshots anzuzeigen.

   ```
   vserver object-store-server bucket snapshot show -vserver <svm_name>
   -bucket <bucket_name>
   ```

S3 Snapshot-Inhalte durchsuchen

Wenn Sie in Ihrer Umgebung Fehler oder Probleme feststellen, können Sie die Inhalte der S3-Bucket-Snapshots durchsuchen, um die Fehler zu identifizieren. Sie können die S3-Snapshots auch durchsuchen, um die fehlerfreien Inhalte zu ermitteln, die wiederhergestellt werden können.

S3-Snapshots werden S3-Clients als Snapshot-Buckets präsentiert. Der Name des Snapshot-Buckets hat das Format `<base_bucket_name>-s3snap-<snapshot_name>`. Alle Snapshot-Buckets in einer Storage-VM sind über die `ListBuckets` S3-API-Operation sichtbar.

Der S3-Snapshot-Bucket erbt die Zugriffsrichtlinien des Basis-Buckets und unterstützt ausschließlich

Leseoperationen. Lösch- und schreibbasierte Vorgänge sind untersagt. Wenn Sie Berechtigungen für den Zugriff auf den Basis-Bucket haben, können Sie auch Leseoperationen der S3-API auf dem S3-Snapshot-Bucket ausführen, wie zum Beispiel `HeadObject`, `GetObject`, `GetObjectTagging`, `ListObjects`, `ListObjectVersions`, `GetObjectAcl` und `CopyObject`.

> Die `CopyObject`Operation wird für einen S3-Snapshot-Bucket nur unterstützt, wenn es sich um einen Snapshot des Quell-Buckets handelt, nicht wenn es sich um das Speicherziel des Snapshots handelt.

Weitere Informationen zu diesen Vorgängen sind unter "ONTAP S3 unterstützte Aktionen" zu finden.

Einen Bucket aus S3-Snapshots mit ONTAP wiederherstellen

Ab ONTAP 9.18.1 kann die ONTAP CLI verwendet werden, um einen gesamten Bucket mithilfe eines ONTAP S3 Snapshots wiederherzustellen. Es kann nur die Version des Buckets wiederhergestellt werden, die zum Zeitpunkt der Erstellung des ausgewählten Snapshots existierte.

Schritte

1. Identifizieren Sie den Snapshot, den Sie zum Wiederherstellen des Buckets verwenden möchten:

```
vserver object-store-server bucket snapshot show
```

2. Stellen Sie den Bucket wieder her:

```
vserver object-store-server bucket snapshot restore start -vserver
<storage VM name> -bucket <bucket name> -snapshot <snapshot name>
```

Daten aus S3-Bucket-Snapshots mit einem S3-Client wiederherstellen

Zusätzlich zur Wiederherstellung eines gesamten Buckets in ONTAP ist es auch möglich, ein einzelnes Objekt, eine Gruppe von Objekten oder einen gesamten Bucket aus einem S3-Snapshot mithilfe eines S3-Clients wie S3cmd oder S3 Browser wiederherzustellen.

"Weitere Informationen zu versionierten und nicht versionierten Snapshots."

Sie können den gesamten Bucket, Objekte mit einem bestimmten Präfix oder ein einzelnes Objekt mit dem `aws s3 cp` Befehl wiederherstellen.

Schritte

1. Einen Snapshot des Basis-S3-Buckets erstellen.

```
vserver object-store-server bucket snapshot create -vserver <svm_name>
-bucket <base_bucket_name> -snapshot <snapshot_name>
```

2. Das Basis-Bucket wird mithilfe des Snapshots wiederhergestellt:
   - Einen gesamten Bucket wiederherstellen. Den Snapshot-Bucket-Namen im Format `<base_bucket_name>-s3snap-<snapshot_name>` verwenden.

```
aws --endpoint http://<IP> s3 cp s3://<snapshot-bucket-name>
s3://<base-bucket>  --recursive
```

- Objekte in einem Verzeichnis mit dem Präfix `dir1` wiederherstellen:

```
aws --endpoint http://<IP> s3 cp s3://<snapshot-bucket-name>/dir1
s3://<base_bucket_name>/dir1 --recursive
```

- Ein einzelnes Objekt mit dem Namen `web.py` wiederherstellen:

```
aws --endpoint http://<IP> s3 cp s3:// <snapshot-bucket-name>/web.py
s3://<base_bucket_name>/web.py
```

ONTAP S3 Snapshots löschen

Sie können nicht mehr benötigte S3 Snapshots löschen und so Speicherplatz in Ihren Buckets freigeben. Sie können S3 Snapshots manuell entfernen oder die den S3 Buckets zugeordneten Snapshot Richtlinien ändern, um die Anzahl der aufzubewahrenden Snapshots für einen Zeitplan zu ändern.

Snapshot-Richtlinien für S3-Buckets folgen denselben Löschregeln wie die herkömmlichen ONTAP Snapshot-Richtlinien. Weitere Informationen zum Erstellen von Snapshot-Richtlinien sind unter "Erstellen einer Snapshot-Richtlinie" zu finden.

Über diese Aufgabe

- Wenn eine Objektversion (in einem versionierten Bucket) oder ein Objekt (in einem nicht versionierten Bucket) in mehreren Snapshots erfasst wird, wird das Objekt erst aus dem Dateisystem entfernt, nachdem der letzte Snapshot, der es schützt, gelöscht wurde.
- Wenn Sie einen S3-Bucket löschen müssen, der Objekte mit Snapshots enthält, stellen Sie sicher, dass Sie alle Snapshots aller Objekte in diesem Bucket gelöscht haben.
- Wenn ein Cluster auf eine ONTAP Version vor ONTAP 9.16.1 zurückgesetzt werden muss, ist sicherzustellen, dass alle S3 Snapshots für alle Buckets gelöscht wurden. Es kann außerdem erforderlich sein, den `vserver object-store-server bucket clear-snapshot-metadata` Befehl auszuführen, um die Snapshot-Metadaten für einen S3 Bucket zu entfernen. Informationen dazu finden sich unter "S3-Snapshots-Metadaten löschen".
- Beim Löschen von Snapshots in Stapeln kann eine große Anzahl von Objekten entfernt werden, die in mehreren Snapshots erfasst wurden, wodurch effektiv mehr Speicherplatz freigegeben wird, als es beim Löschen einzelner Snapshots der Fall wäre. Dadurch kann mehr Speicherplatz für Ihre Speicherobjekte zurückgewonnen werden.

Schritte

1. Um einen bestimmten S3 Snapshot zu löschen, diesen Befehl ausführen:

```
vserver object-store-server bucket snapshot delete -vserver <svm_name>
```

```
-bucket <bucket_name> -snapshot <snapshot_name>
```

2. Um alle S3-Snapshots in einem Bucket zu entfernen, diesen Befehl ausführen:

```
vserver object-store-server bucket snapshot delete -vserver <svm_name>
-bucket <bucket_name> -snapshot *
```

S3-Snapshots-Metadaten löschen

Bei S3-Snapshots werden auch Snapshot-Metadaten in einem Bucket generiert. Die Snapshot-Metadaten bleiben im Bucket erhalten, selbst wenn alle Snapshots daraus entfernt werden. Das Vorhandensein von Snapshot-Metadaten blockiert die folgenden Operationen:

- Cluster auf eine ONTAP Version vor ONTAP 9.16.1 zurücksetzen
- Konfiguration von SnapMirror S3 auf dem Bucket

Vor der Durchführung dieser Operationen sollten alle Snapshot-Metadaten aus dem Bucket gelöscht werden.

Bevor Sie beginnen

Stellen Sie sicher, dass Sie alle S3-Snapshots aus einem Bucket entfernt haben, bevor Sie mit dem Löschen der Metadaten beginnen.

Schritte

1. Um die Snapshot-Metadaten aus einem Bucket zu löschen, diesen Befehl ausführen:

```
vserver object-store-server bucket clear-snapshot-metadata -vserver
<svm_name> -bucket <bucket_name>
```

Audit S3-Ereignisse

Informationen zur Überwachung von ONTAP S3-Ereignissen

Ab ONTAP 9.10.1 ist die Protokollierung von Daten- und Verwaltungsereignissen in ONTAP S3 Umgebungen möglich. Die S3-Protokollierungsfunktionalität ist mit den bestehenden NAS-Protokollierungsfunktionen vergleichbar, und S3- sowie NAS-Protokollierung können in einem Cluster parallel bestehen.

Wenn Sie eine S3-Überwachungskonfiguration auf einer SVM erstellen und aktivieren, werden S3-Ereignisse in einer Protokolldatei aufgezeichnet. Sie können die folgenden Ereignisse angeben, die protokolliert werden sollen:

Objektzugriff (Daten) Ereignisse nach Release

9.11.1:

- ListBucketVersions

- ListBucket (ListObjects von 9.10.1 wurde in diesen umbenannt)
- ListAllMyBuckets (ListBuckets von 9.10.1 wurde in diesen umbenannt)

9.10.1:

- HeadObject
- GetObject
- PutObject
- DeleteObject
- ListBuckets
- ListObjects
- MPUpload
- MPUploadPart
- MPComplete
- MPAbort
- GetObjectTagging
- DeleteObjectTagging
- PutObjectTagging
- ListUploads
- ListParts

Managementereignisse nach Release

9.15.1:

- GetBucketCORS
- PutBucketCORS
- DeleteBucketCORS

9.14.1:

- GetObjectRetention
- PutObjectRetention
- PutBucketObjectLockConfiguration
- GetBucketObjectLockConfiguration

9.13.1:

- PutBucketLifecycle
- DeleteBucketLifecycle
- GetBucketLifecycle

9.12.1:

- GetBucketPolicy
- CopyObject
- UploadPartCopy
- PutBucketPolicy
- DeleteBucketPolicy

9.11.1:

- GetBucketVersioning
- PutBucketVersioning

9.10.1:

- HeadBucket
- GetBucketAcl
- GetObjectAcl
- PutBucket
- DeleteBucket
- ModifyObjectTagging
- GetBucketLocation

Das Protokollformat ist JavaScript Object Notation (JSON).

Die kombinierte Obergrenze für S3- und NFS-Revisionsprotokollkonfigurationen beträgt 400 SVMs pro Cluster.

Folgende Lizenz ist erforderlich:

- ONTAP One, ehemals Teil des Core Bundle, für das ONTAP S3 Protokoll und Storage

Weitere Informationen finden sich unter "Wie der ONTAP Revisionsprozess funktioniert".

Garantierte Prüfung

Standardmäßig ist die Überwachung von S3 und NAS gewährleistet. ONTAP garantiert, dass alle prüfbaren Bucket-Zugriffsereignisse protokolliert werden, selbst wenn ein Knoten nicht verfügbar ist. Ein angeforderter Bucket-Vorgang kann erst abgeschlossen werden, wenn der Prüfdatensatz für diesen Vorgang im Staging-Volume auf dem persistenten Speicher gespeichert wurde. Können Prüfdatensätze nicht in den Staging-Dateien gespeichert werden, entweder aufgrund von unzureichendem Speicherplatz oder wegen anderer Probleme, werden Client-Operationen abgelehnt.

Platzbedarf für die Prüfung

Im ONTAP Auditing-System werden Audit-Datensätze zunächst in binären Zwischenspeicherdateien auf den einzelnen Knoten gespeichert. Periodisch werden sie konsolidiert und in benutzerlesbare Ereignisprotokolle umgewandelt, die im Verzeichnis für Revisionsprotokolle des SVM gespeichert werden.

Die Staging-Dateien werden in einem dedizierten Staging-Volume gespeichert, das von ONTAP bei der Erstellung der Revisionsprotokoll-Konfiguration erstellt wird. Pro Aggregat existiert ein Staging-Volume.

In der Audit-Konfiguration ist ausreichend verfügbarer Speicherplatz einzuplanen:

- Für die Staging Volumes in Aggregaten, die geprüfte Buckets enthalten.
- Für das Volume, das das Verzeichnis enthält, in dem konvertierte Ereignisprotokolle gespeichert sind.

Sie können die Anzahl der Ereignisprotokolle und damit den verfügbaren Speicherplatz im Volume mit einer von zwei Methoden beim Erstellen der S3 Auditing-Konfiguration steuern:

- Ein numerischer Grenzwert; der `-rotate-limit` Parameter steuert die Mindestanzahl der zu speichernden Revisionsprotokolldateien.
- Ein Zeitlimit; der `-retention-duration` Parameter steuert die maximale Zeitspanne, für die Dateien aufbewahrt werden können.

Bei beiden Parametern können ältere Revisionsprotokolldateien gelöscht werden, sobald der konfigurierte Wert überschritten ist, um Platz für neuere zu schaffen. Für beide Parameter beträgt der Wert 0, was bedeutet, dass alle Dateien erhalten bleiben müssen. Um ausreichend Speicherplatz sicherzustellen, ist es daher eine bewährte Methode, einen der Parameter auf einen Wert ungleich null zu setzen.

Aufgrund der garantierten Revisionsprotokollierung können keine neuen Revisionsprotokolldaten erstellt werden, wenn der verfügbare Speicherplatz für Revisionsprotokolldaten vor dem Rotationslimit erschöpft ist, was dazu führt, dass Clients nicht auf Daten zugreifen können. Daher sollten der Wert für die Revisionsprotokollierung und der für die Revisionsprotokollierung reservierte Speicherplatz sorgfältig gewählt werden, und auf Warnungen des Revisionsprotokollierungssystems bezüglich des verfügbaren Speicherplatzes ist zu reagieren.

Weitere Informationen finden sich unter "Grundlegende Auditierungskonzepte".

Planung einer ONTAP S3 Audit-Konfiguration

Sie müssen für die S3-Auditing-Konfiguration eine Reihe von Parametern festlegen oder die Standardeinstellungen übernehmen. Insbesondere sollte berücksichtigt werden, welche Parameter für die Protokollrotation dazu beitragen, ausreichend freien Speicherplatz sicherzustellen.

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

Allgemeine Parameter

Beim Erstellen der Audit-Konfiguration müssen zwei obligatorische Parameter angegeben werden. Es gibt außerdem drei optionale Parameter, die angegeben werden können.

Art der Information	Option	Erforderlich
SVM Name Name der SVM, auf der die Revisionsprotokoll-Konfiguration erstellt werden soll. Die SVM muss bereits existieren und für S3 aktiviert sein.	`-vserver` *`svm_name`*	Ja

Protokollzielpfad Gibt an, wo die konvertierten Revisionsprotokolle gespeichert werden. Der Pfad muss auf der SVM bereits vorhanden sein. Der Pfad darf maximal 864 Zeichen lang sein und muss über Lese-/Schreibberechtigung verfügen. Ist der Pfad ungültig, schlägt der Revisionsdatei-Konfigurationsbefehl fehl.	`-destination text`	Ja
Kategorien von zu prüfenden Ereignissen Die folgenden Ereigniskategorien können im Revisionsprotokoll erfasst werden: • Daten GetObject, PutObject und DeleteObject-Ereignisse • Management PutBucket und DeleteBucket Ereignisse Standardmäßig werden nur Datenereignisse geprüft.	`-events {data|management}, …`	Nein

Sie können einen der folgenden Parameter eingeben, um die Anzahl der Revisionsprotokoll Logdateien zu steuern. Wenn kein Wert eingegeben wird, werden alle Logdateien beibehalten.

Art der Information	Option	Erforderlich
Rotationslimit für Protokolldateien Legt fest, wie viele Revisionsprotokoll-Logdateien aufbewahrt werden, bevor die älteste Logdatei entfernt wird. Bei einem Wert von 5 werden beispielsweise die letzten fünf Logdateien aufbewahrt. Der Wert 0 bedeutet, dass alle Protokolldateien beibehalten werden. Der Standardwert ist 0.	`-rotate-limit integer`	Nein
Dauerbegrenzung für Protokolldateien Legt fest, wie lange eine Protokolldatei aufbewahrt werden kann, bevor sie gelöscht wird. Wenn ein Wert von 5d0h0m eingegeben wird, werden Protokolle, die älter als 5 Tage sind, gelöscht. Der Wert 0 bedeutet, dass alle Protokolldateien beibehalten werden. Der Standardwert ist 0.	`-retention duration integer_time`	Nein

Parameter für die Rotation des Revisionsprotokolls

Sie können Revisionsprotokolle basierend auf Größe oder Zeitplan rotieren lassen. Standardmäßig werden Revisionsprotokolle basierend auf Größe rotiert.

Protokolle basierend auf der Protokollgröße rotieren

Wenn Sie die Standardmethode für die Protokollrotation und die Standardprotokollgröße verwenden, ist keine spezifische Konfiguration von Parametern für die Protokollrotation erforderlich. Die Standardprotokollgröße

beträgt 100 MB.

Wenn Sie nicht die Standardprotokollgröße verwenden möchten, kann der `-rotate-size` Parameter so konfiguriert werden, dass eine benutzerdefinierte Protokollgröße festgelegt wird.

Wenn Sie die Rotation nur anhand der Loggröße zurücksetzen möchten, verwenden Sie den folgenden Befehl, um den `-rotate-schedule-minute` Parameter zu entfernen:

```
vserver audit modify -vserver svm_name -destination / -rotate-schedule-minute -
```

Protokolle gemäß einem Zeitplan rotieren

Wenn Sie sich dafür entscheiden, die Revisionsprotokolle nach einem Zeitplan zu rotieren, kann die Protokollrotation mithilfe der zeitbasierten Rotationsparameter in beliebiger Kombination geplant werden.

- Bei Verwendung einer zeitbasierten Rotation ist der `-rotate-schedule-minute` Parameter obligatorisch.
- Alle anderen zeitbasierten Rotationsparameter sind optional.
  - `-rotate-schedule-month`
  - `-rotate-schedule-dayofweek`
  - `-rotate-schedule-day`
  - `-rotate-schedule-hour`
- Der Rotationsplan wird anhand aller zeitbezogenen Werte berechnet. Wenn nur der `-rotate-schedule-minute` Parameter angegeben wird, werden die Revisionsprotokoll-Dateien an allen Wochentagen, zu allen Stunden und in allen Monaten des Jahres entsprechend der angegebenen Minuten rotiert.
- Wenn Sie nur einen oder zwei zeitbasierten Rotationsparameter angeben (zum Beispiel `-rotate-schedule-month` und `-rotate-schedule-minutes`), erfolgt die Rotation der Protokolldateien an allen Wochentagen und zu allen Stunden auf Grundlage der angegebenen Minutenwerte, jedoch nur während der festgelegten Monate.

  Beispielsweise kann festgelegt werden, dass das Revisionsprotokoll in den Monaten Januar, März und August jeweils montags, mittwochs und samstags um 10:30 Uhr rotiert wird.

- Wenn Sie Werte für sowohl `-rotate-schedule-dayofweek` als auch `-rotate-schedule-day` angeben, werden diese unabhängig voneinander betrachtet.

  Wenn beispielsweise `-rotate-schedule-dayofweek` als Freitag und `-rotate-schedule-day` als 13 angegeben werden, werden die Revisionsprotokolle an jedem Freitag und am 13. Tag des angegebenen Monats rotiert, nicht nur an jedem Freitag, der auf den 13. fällt.

- Wenn Sie die Rotation nur anhand eines Zeitplans zurücksetzen möchten, verwenden Sie den folgenden Befehl, um die `-rotate-size parameter` aufzuheben:

  ```
  vserver audit modify -vserver svm_name -destination / -rotate-size -
  ```

Protokolldateien basierend auf ihrer Größe und dem Zeitplan rotieren

Sie können die Rotation der Protokolldateien anhand der Protokolldateigröße und eines Zeitplans steuern, indem sowohl der Parameter -rotate-size als auch die zeitbasierten Rotationsparameter in beliebiger Kombination gesetzt werden. Beispielsweise: Wenn `-rotate-size` auf 10 MB und `-rotate-schedule`

`-minute` auf 15 gesetzt ist, werden die Protokolldateien rotiert, sobald die Protokolldateigröße 10 MB erreicht oder in der 15. Minute jeder Stunde (je nachdem, welches Ereignis zuerst eintritt).

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

Erstellen und Aktivieren einer ONTAP S3 Überwachungskonfiguration

Zur Implementierung von S3 Auditing wird zunächst eine persistente Objektspeicher Auditing-Konfiguration auf einer S3-fähigen SVM erstellt und anschließend die Konfiguration aktiviert.

Bevor Sie beginnen

- Sie verfügen über eine S3-fähige SVM.
- Bestätigen Sie, dass ausreichend Speicherplatz für Staging-Volumes in der lokalen Tier vorhanden ist.

Über diese Aufgabe

Für jede SVM, die S3-Buckets enthält, die Sie überwachen möchten, ist eine Überwachungskonfiguration erforderlich. Die S3-Überwachung kann auf neuen oder bestehenden S3-Servern aktiviert werden. Überwachungskonfigurationen bleiben in einer S3-Umgebung erhalten, bis sie mit dem Befehl **vserver object-store-server audit delete** entfernt werden.

Die S3-Audit-Konfiguration gilt für alle Buckets in der SVM, die für die Überwachung ausgewählt werden. Eine SVM mit aktivierter Überwachung kann sowohl überwachte als auch nicht überwachte Buckets enthalten.

Es wird empfohlen, die S3-Überwachung für die automatische Protokollrotation zu konfigurieren, die anhand der Protokollgröße oder eines Zeitplans erfolgt. Wenn die automatische Protokollrotation nicht konfiguriert wird, werden standardmäßig alle Protokolldateien beibehalten. Die S3-Protokolldateien können auch manuell mit dem Befehl **vserver object-store-server audit rotate-log** rotiert werden.

Wenn die SVM eine SVM Disaster Recovery-Quelle ist, kann sich der Zielpfad nicht auf dem Root-Volume befinden.

Schritte

1. Die Überwachungskonfiguration ermöglicht das Rotieren von Überwachungsprotokollen basierend auf der Protokollgröße oder einem Zeitplan.

Wenn Sie die Revisionsprotokolle rotieren möchten…	Eingeben…
Loggröße	`vserver object-store-server audit create -vserver` *`svm_name`* `-destination` *`path`* `[[-events] {data|management}, …] {[-rotate-limit` *`integer`*`] | [-retention-duration [`*`integer_d`*`][`*`integer_h`*`][`*`integer_m`*`][`*`integers`*`]]} [-rotate-size {`*`integer`*`[KB|MB|GB|TB|PB]}]`

Wenn Sie die Revisionsprotokolle rotieren möchten…	Eingeben…
Ein Zeitplan	`vserver object-store-server audit create -vserver` *svm_name* `-destination path [[-events] {data|management}, …] {[-rotate-limit` *integer*`] | [-retention-duration [`*integerd*`][`*integerh*`] [`*integerm*`][`*integers*`]] } [-rotate-schedule-month` *chron_month*`] [-rotate-schedule-dayofweek` *chron_dayofweek*`] [-rotate-schedule-day` *chron_dayofmonth*`] [-rotate-schedule-hour` *chron_hour*`] -rotate-schedule-minute` *chron_minute* Der `-rotate-schedule-minute`Parameter ist erforderlich, wenn eine zeitbasierte Revisionsprotokollrotation konfiguriert wird.

2. S3-Überwachung aktivieren:

   `vserver object-store-server audit enable -vserver` *svm_name*

Beispiele

Das folgende Beispiel erstellt eine Überwachungskonfiguration, die alle S3-Ereignisse (Standard) mithilfe einer größenbasierten Rotation überwacht. Die Protokolle werden im Verzeichnis /audit_log gespeichert. Die maximale Protokolldateigröße beträgt 200 MB. Die Protokolle werden rotiert, sobald sie 200 MB groß sind.

```
cluster1::> vserver audit create -vserver vs1 -destination /audit_log -rotate
-size 200MB
```

Das folgende Beispiel erstellt eine Überwachungskonfiguration, die alle S3-Ereignisse (Standard) mithilfe einer größenbasierten Rotation überwacht. Die maximale Protokolldateigröße beträgt 100 MB (Standard), und die Protokolle werden 5 Tage lang aufbewahrt, bevor sie gelöscht werden.

```
cluster1::> vserver audit create -vserver vs1 -destination /audit_log -retention
-duration 5d0h0m
```

Das folgende Beispiel erstellt eine Audit-Konfiguration, die S3-Management-Ereignisse und Ereignisse der zentralen Zugriffsrichtlinien-Staging mithilfe zeitbasierter Rotation auditiert. Die Audit-Protokolle werden monatlich um 12:30 Uhr an allen Wochentagen rotiert. Das Protokoll-Rotationslimit beträgt 5.

```
cluster1::> vserver audit create -vserver vs1 -destination /audit_log -events
management -rotate-schedule-month all -rotate-schedule-dayofweek all -rotate
-schedule-hour 12 -rotate-schedule-minute 30 -rotate-limit 5
```

Buckets für ONTAP S3-Auditing auswählen

Es ist anzugeben, welche Buckets in einer Audit-aktivierten SVM überwacht werden.

Bevor Sie beginnen

- Sie haben eine SVM für die S3-Überwachung aktiviert.

Über diese Aufgabe

S3-Audit-Konfigurationen werden pro SVM aktiviert, jedoch müssen Sie in den SVMs die Buckets auswählen,

die für das Audit aktiviert sind. Wenn Buckets zur SVM hinzugefügt werden und diese neuen Buckets auditiert werden sollen, müssen sie mit diesem Verfahren ausgewählt werden. Es können auch nicht auditierte Buckets in einer SVM für S3-Auditing aktiviert sein.

Die Überwachungskonfigurationen bleiben für Buckets bestehen, bis sie durch den `vserver object-store-server audit event-selector delete` Befehl entfernt werden.

Schritte

1. Wählen Sie einen Bucket für die S3-Überwachung aus:

```
vserver object-store-server audit event-selector create -vserver
<svm_name> -bucket <bucket_name> [[-access] {read-only|write-only|all}]
[[-permission] {allow-only|deny-only|all}]
```

   - `-access`: Gibt die Art des zu überwachenden Ereigniszugriffs an: `read-only`, `write-only` oder `all` (Standardwert ist `all`).
   - `-permission`: Gibt den Typ der zu überwachenden Ereignisberechtigung an: `allow-only`, `deny-only` oder `all` (Standardwert ist `all`).

Beispiel

Das folgende Beispiel erstellt eine Bucket-Audit-Konfiguration, die nur zulässige Ereignisse mit Lesezugriff protokolliert:

```
cluster1::> vserver object-store-server audit event-selector create -vserver vs1
-bucket test-bucket -access read-only -permission allow-only
```

Ändern einer ONTAP S3 Überwachungskonfiguration

Sie können die Revisionsparameter einzelner Buckets oder die Revisionskonfiguration aller zur Revision ausgewählten Buckets im SVM anpassen.

Wenn Sie die Revisionsprotokollkonfiguration für… anpassen möchten	Eingeben…
Einzelne Buckets	`vserver object-store-server audit event-selector modify -vserver` *`svm_name`* `[-bucket` *`bucket_name`*`] [`*`parameters to modify`*`]`
Alle Buckets in der SVM	`vserver object-store-server audit modify -vserver` *`svm_name`* `[`*`parameters to modify`*`]`

Beispiele

Das folgende Beispiel ändert eine einzelne Bucket-Audit-Konfiguration, um nur Schreibzugriffsereignisse zu protokollieren:

```
cluster1::> vserver object-store-server audit event-selector modify
-vserver vs1 -bucket test-bucket -access write-only
```

Das folgende Beispiel ändert die Revisionsprotokollkonfiguration aller Buckets in der SVM, um die Protokollgrößenbeschränkung auf 10 MB zu ändern und 3 Protokolldateien vor der Rotation aufzubewahren.

```
cluster1::> vserver object-store-server audit modify -vserver vs1 -rotate
-size 10MB -rotate-limit 3
```

ONTAP S3-Überwachungskonfigurationen anzeigen

Nach Abschluss der Revisionsprotokollkonfiguration kann überprüft werden, ob das Revisionsprotokoll ordnungsgemäß konfiguriert und aktiviert ist. Es lassen sich außerdem Informationen zu allen Objektspeicher-Revisionsprotokollkonfigurationen im Cluster anzeigen.

Über diese Aufgabe

Informationen zu Bucket- und SVM-Audit-Konfigurationen lassen sich anzeigen.

- Buckets: Der `vserver object-store-server audit event-selector show`Befehl kann verwendet werden

  Ohne Angabe von Parametern zeigt der Befehl die folgenden Informationen über Buckets in allen SVMs im Cluster mit Objektspeicher-Audit-Konfigurationen an:

  - SVM-Name
  - Bucket Name
  - Zugriffs- und Berechtigungswerte
- SVMs: Mit dem `vserver object-store-server audit show` Befehl

  Ohne Angabe von Parametern zeigt der Befehl die folgenden Informationen zu allen SVMs im Cluster mit Objektspeicher-Revisionsprotokollkonfigurationen an:

  - SVM-Name
  - Revisionsstatus
  - Zielverzeichnis

Sie können den `-fields` Parameter angeben, um festzulegen, welche Revisionsprotokoll-Konfigurationsinformationen angezeigt werden.

Schritte

Informationen zu S3-Audit-Konfigurationen:

Wenn Sie die Konfiguration für … ändern möchten	Eingeben…
Buckets	`vserver object-store-server audit event-selector show [-vserver` *svm_name*`] [`*parameters*`]`
SVMs	`vserver object-store-server audit show [-vserver` *svm_name*`] [`*parameters*`]`

Beispiele

Das folgende Beispiel zeigt Informationen für einen einzelnen Bucket:

```
cluster1::> vserver object-store-server audit event-selector show -vserver
vs1 -bucket test-bucket
     Vserver     Bucket     Access          Permission
     ----------- ---------- --------------- ----------
     vs1         bucket1    read-only       allow-only
```

Das folgende Beispiel zeigt Informationen für alle Buckets auf einer SVM:

```
cluster1::> vserver object-store-server audit event-selector show -vserver
vs1

     Vserver           :vs1
     Bucket            :test-bucket
     Access            :all
     Permission        :all
```

Das folgende Beispiel zeigt den Namen, den Revisionsprotokollstatus, die Ereignistypen, das Protokollformat und das Zielverzeichnis für alle SVMs.

```
cluster1::> vserver object-store-server audit show

Vserver     State  Event Types Log Format Target Directory
----------- ------ ----------- ---------- --------------------
vs1         false  data        json       /audit_log
```

Das folgende Beispiel zeigt die SVM-Namen und Details zum Revisionsprotokoll für alle SVMs.

```
cluster1::> vserver object-store-server audit show -log-save-details

                 Rotation                              Rotation
      Vserver    File Size Rotation Schedule          Limit
      ---------- --------- ------------------------- --------
      vs1        100MB     -                         0
```

Das folgende Beispiel zeigt in Listenform alle Revisionsprotokoll-Konfigurationsinformationen zu allen SVMs.

```
cluster1::> vserver object-store-server audit show -instance

                           Vserver: vs1
                  Auditing state: true
```

```
               Log Destination Path: /audit_log
     Categories of Events to Audit: data
                         Log Format: json
                Log File Size Limit: 100MB
      Log Rotation Schedule: Month: -
Log Rotation Schedule: Day of Week: -
        Log Rotation Schedule: Day: -
       Log Rotation Schedule: Hour: -
     Log Rotation Schedule: Minute: -
                Rotation Schedules: -
          Log Files Rotation Limit: 0
                Log Retention Time: 0s
```

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.