S3-Objekt-Storage-Management

ONTAP 9

NetApp
February 01, 2026

Inhalt

S3-Objekt-Storage-Management

Erfahren Sie mehr über S3-Support in ONTAP 9

Erfahren Sie mehr über die ONTAP S3-Konfiguration

Ab ONTAP 9.8 können Sie einen ONTAP Simple Storage Service (S3)-Objekt-Storage-Server in einem ONTAP Cluster mithilfe vertrauter Managementtools wie ONTAP System Manager aktivieren, um schnell hochperformanten Objekt-Storage für Entwicklung und Betrieb in ONTAP bereitzustellen und von den ONTAP Storage-Effizienzfunktionen und -Sicherheit zu profitieren.

Ab Juli 2024 wurden die Inhalte aus zuvor als PDFs veröffentlichten technischen Berichten in die ONTAP Produktdokumentation integriert. Die Dokumentation zu ONTAP S3 enthält jetzt Inhalte aus *TR-4814: S3 in den Best Practices von ONTAP*.

S3-Konfiguration mit System Manager und der ONTAP-CLI

ONTAP S3 lässt sich mit System Manager und der ONTAP CLI konfigurieren und verwalten. Wenn Sie S3 aktivieren und Buckets mithilfe von System Manager erstellen, wählt ONTAP für eine vereinfachte Konfiguration Best Practice-Standards. Wenn Sie Konfigurationsparameter angeben müssen, möchten Sie sie möglicherweise die ONTAP-CLI verwenden. Wenn Sie den S3-Server und die Buckets aus der CLI konfigurieren, können Sie sie nach Bedarf auch mit System Manager managen oder umgekehrt.

Wenn Sie mit System Manager einen S3-Bucket erstellen, konfiguriert ONTAP ein Service-Level für die Standard-Performance, das auf Ihrem System am höchsten verfügbar ist. Bei einem AFF-System wäre beispielsweise die Standardeinstellung **Extreme**. Performance-Service-Level sind vordefinierte Richtliniengruppen (Quality of Service, QoS). Anstelle eines der Standard-Service-Level können Sie eine benutzerdefinierte QoS-Richtliniengruppe oder keine Richtliniengruppe angeben.

Folgende vordefinierten adaptiven QoS-Richtliniengruppen sind definiert:

- **Extreme**: Wird für Applikationen verwendet, die eine äußerst niedrige Latenz und höchste Performance erwarten.
- **Performance**: Wird für Applikationen mit geringen Performance-Anforderungen und Latenz verwendet.
- **Wert**: Wird für Applikationen verwendet, bei denen Durchsatz und Kapazität wichtiger sind als die Latenz.
- **Benutzerdefiniert**: Geben Sie eine benutzerdefinierte QoS-Richtlinie oder keine QoS-Richtlinie an.

Wenn Sie **für Tiering** verwenden auswählen, werden keine Leistungsservicelevel ausgewählt und das System versucht, kostengünstige Medien mit optimaler Leistung für die Tiered Data auszuwählen.

Siehe auch: "Verwendung von adaptiven QoS-Richtliniengruppen".

ONTAP versucht, diesen Bucket auf lokalen Tiers bereitzustellen, die über die am besten geeigneten Festplatten verfügen und dem ausgewählten Service-Level gerecht werden. Wenn Sie jedoch angeben müssen, welche Festplatten in den Bucket enthalten sind, sollten Sie S3-Objekt-Storage aus der CLI konfigurieren, indem Sie die lokalen Tiers (Aggregat) angeben. Wenn Sie den S3-Server über die CLI konfigurieren, können Sie ihn bei Bedarf weiterhin mit System Manager managen.

Wenn Sie angeben können, welche Aggregate für Buckets verwendet werden, können Sie dies nur über die

CLI tun.

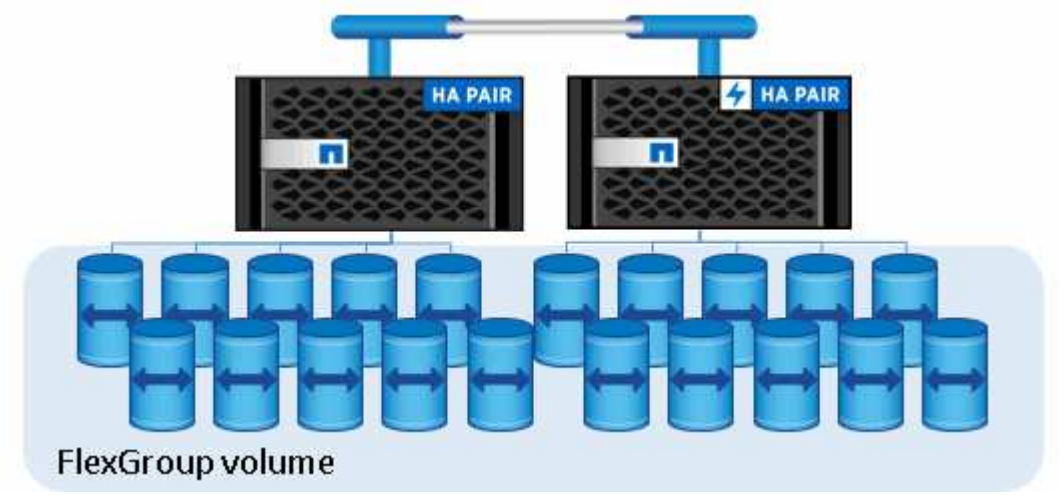
Konfigurieren von S3 Buckets für Cloud Volumes ONTAP

Wenn Sie Buckets von Cloud Volumes ONTAP dienen möchten, wird dringend empfohlen, dass Sie die zugrunde liegenden Aggregate manuell auswählen, um sicherzustellen, dass sie nur einen Node verwenden. Die Verwendung von Aggregaten beider Nodes kann sich auf die Performance auswirken, da die Nodes sich in geografisch getrennten Verfügbarkeitszonen befinden und daher anfällig für Latenzprobleme sind. Daher sollten Sie in Cloud Volumes ONTAP-Umgebungen Konfigurieren Sie S3 Buckets über die CLI.

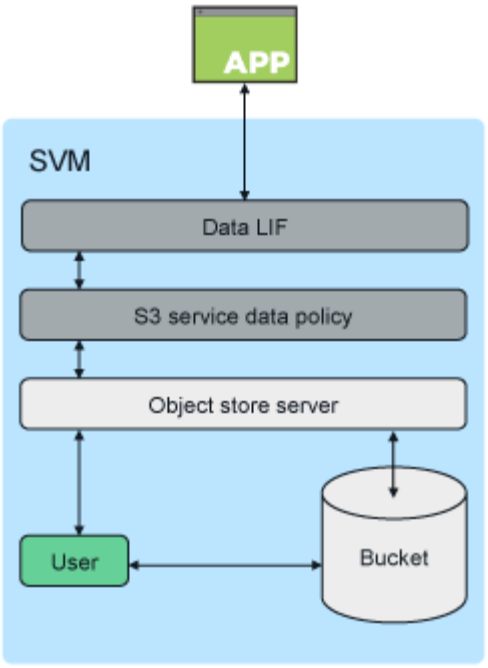
Ansonsten werden S3-Server in Cloud Volumes ONTAP in Cloud Volumes ONTAP wie in On-Premises-Umgebungen konfiguriert und gepflegt.

ONTAP S3 Architektur mit FlexGroup Volumes

In ONTAP ist die zugrunde liegende Architektur für einen Bucket ein , der ein einzelner Namespace ist "FlexGroup Volume", der aus mehreren zusammengehörigen Member Volumes besteht, aber als ein einziges Volume gemanagt wird.



Der Zugriff auf den Bucket wird durch autorisierte Benutzer und Client-Applikationen bereitgestellt.



Wenn ein Bucket ausschließlich für S3-Applikationen verwendet wird, einschließlich 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 vorkonfigurierten NAS-Protokollen aktiviert werden"Multiprotokoll-NAS-Volumes". Wenn das S3-Protokoll in Multiprotokoll-NAS-Volumes aktiviert ist, können Client-Applikationen Daten mithilfe von NFS, SMB und S3 lesen und schreiben.

Bucket-Grenzwerte

Mindestkapazität

Die Mindestkapazität des Behälters wird von der ONTAP Plattform bestimmt.

- 95 GB für lokale Plattformen.
- 1,6 GB für Lab on Demand.
- 200 MB für ONTAP Select.

Maximale Größe

Die maximale Schaufelkapazität ist auf die maximale FlexGroup Größe von 60PB begrenzt.

Maximale Anzahl an Eimern

Die maximale Anzahl an Buckets beträgt 1000 pro FlexGroup Volume bzw. 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 Standard-FlexGroup-Größe auf der Größe der darin enthaltenen Buckets. Das FlexGroup Volume lässt sich beim Hinzufügen oder Entfernen von Buckets automatisch vergrößern oder

verkleinern.

Wenn beispielsweise „Initial Bucket_A“ mit 100 GB bereitgestellt wird, wird die FlexGroup mit 100 GB über Thin Provisioning bereitgestellt. Wenn zwei zusätzliche Buckets erstellt werden, Bucket_B mit 300 GB und Bucket_C mit 500 GB, wächst das FlexGroup Volume auf 900 GB an.

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

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

Standardgrößen für FlexGroup in ONTAP 9.13.1 und früher wurden korrigiert

Um die Kapazität für die Bucket-Erweiterung zur Verfügung zu stellen, sollte die insgesamt genutzte Kapazität aller Buckets im FlexGroup Volume basierend auf verfügbaren Storage-Aggregaten auf weniger als 33 % der maximalen FlexGroup Volume-Kapazität betragen. Wenn diese Voraussetzungen nicht erfüllt werden können, wird der neu erstellte Bucket auf einem neuen, automatisch erstellten FlexGroup Volume bereitgestellt.

Vor ONTAP 9.14.1 ist die FlexGroup-Größe abhängig von der Umgebung auf Standardgröße festgelegt:

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

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

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

Primäre Anwendungsfälle für ONTAP S3

Dies sind die primären Anwendungsfälle für den Client-Zugriff auf ONTAP S3 Services:

- Mit FabricPool können inaktive Daten auf einen Bucket in ONTAP verschoben werden, um ONTAP auf ONTAP Tiering zu ermöglichen Tiering auf einen Bucket innerhalb von "Lokales Cluster"– oder Tiering auf einen Bucket auf einem "Remote-Cluster"– werden unterstützt. Durch Tiering in ONTAP S3 können Sie kostengünstigere ONTAP-Systeme für inaktive Daten verwenden und Kosten für neue Flash-Kapazität einsparen, ohne zusätzliche FabricPool Lizenzen oder neue Technologien zu managen.
- Ab ONTAP 9.12.1 kann das S3-Protokoll auch in vorkonfigurierten NAS-Protokollen aktiviert werden"Multiprotokoll-NAS-Volumes". Wenn das S3-Protokoll in Multiprotokoll-NAS-Volumes aktiviert ist, können Client-Applikationen Daten mithilfe von S3, NFS und SMB lesen und schreiben, was zu einer Vielzahl weiterer Anwendungsfälle führt. Eines der häufigsten Anwendungsfälle sind NAS-Clients, die Daten auf ein Volume schreiben, und S3-Clients, die dieselben Daten lesen und spezielle Aufgaben wie Analysen, Business Intelligence, maschinelles Lernen und optische Zeichenerkennung ausführen.

> ONTAP S3 ist geeignet, wenn Sie S3 Funktionen auf vorhandenen ONTAP-Clustern ohne zusätzliche Hardware und kein zusätzliches Management aktivieren möchten. NetApp StorageGRID ist die Vorzeigelösung von NetApp für Objekt-Storage. StorageGRID wird für native S3-Applikationen empfohlen, die alle S3-Aktionen, erweiterten ILM-Funktionen oder Kapazitäten nutzen müssen, die in ONTAP-basierten Systemen nicht erreichbar sind. Weitere Informationen finden Sie im "StorageGRID-Dokumentation".

Verwandte Informationen

"Management von FlexGroup Volumes"

Planen

ONTAP Version- und Plattformunterstützung für S3 Objekt-Storage

S3 Objekt-Storage wird auf allen AFF, FAS und ONTAP Select Plattformen unter Verwendung von ONTAP 9.8 und höher unterstützt.

Wie bei anderen Protokollen wie FC, iSCSI, NFS, NVMe_of und SMB, für S3 muss eine Lizenz installiert werden, bevor sie in ONTAP verwendet werden kann. Bei der S3-Lizenz handelt es sich um eine kostenlose Lizenz, die jedoch auf Systemen installiert werden muss, die auf ONTAP 9.8 aktualisiert werden. Die S3-Lizenz kann von auf der NetApp Support-Website heruntergeladen "Seite „Master License Keys“" werden.

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

Cloud Volumes ONTAP

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

- Beim Erstellen von Buckets in Cloud Volumes ONTAP sollten Sie mit der CLI sicherstellen, dass das zugrunde liegende FlexGroup Volume nur Aggregate eines einzigen Node verwendet. Die Verwendung von Aggregaten von mehreren Nodes wirkt sich negativ auf die Performance aus, da die Nodes sich 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 für NetApp ONTAP

S3-Objektspeicher wird auf Amazon FSX für NetApp-Services mit ONTAP 9.11 und höher unterstützt.

S3-Unterstützung mit MetroCluster

Ab ONTAP 9.14.1 können Sie einen S3-Objektspeicher-Server auf einer SVM in einem gespiegelten Aggregat in MetroCluster IP- und FC-Konfigurationen aktivieren.

Ab ONTAP 9.12.1 können Sie einen S3-Objekt-Storage-Server auf einer SVM in einem nicht gespiegelten Aggregat in einer MetroCluster IP-Konfiguration aktivieren. Weitere Informationen zu den Einschränkungen von nicht gespiegelten Aggregaten in MetroCluster IP-Konfigurationen finden Sie unter "Überlegungen bei nicht gespiegelten Aggregaten".

SnapMirror S3 wird in MetroCluster-Konfigurationen nicht unterstützt.

Öffentliche S3-Vorschau in ONTAP 9.7

Im ONTAP 9.7 wurde S3 Objekt-Storage als öffentliche Vorschau eingeführt. Diese Version wurde nicht für Produktionsumgebungen verwendet und wird ab ONTAP 9.8 nicht mehr aktualisiert. Nur ONTAP 9.8 und

neuere Versionen unterstützen S3 Objekt-Storage in Produktionsumgebungen.

Die mit der öffentlichen Vorschau 9.7 erstellten S3-Buckets können für ONTAP 9.8 und höher verwendet werden, können jedoch nicht von Funktionsverbesserungen profitieren. Wenn bei der öffentlichen Vorschau 9.7 Buckets erstellt wurden, sollten Sie die Inhalte dieser Buckets für Funktionsunterstützung, Sicherheit und Performance-Verbesserungen in 9.8 Buckets migrieren.

Von ONTAP S3 unterstützte Aktionen

ONTAP S3 Aktionen werden von S3-Standard-REST-APIs unterstützt, sofern nicht wie unten angegeben. Weitere Informationen finden Sie im "Amazon S3-API-Referenz".

> Diese S3-Aktionen werden speziell bei der Verwendung nativer S3-Buckets in ONTAP unterstützt. Einige dieser Aktionen, z. B. die mit der Versionierung, Objektsperren und anderen Funktionen verbundenen, werden bei Verwendung von nicht unterstützt"S3 NAS-Buckets (S3 in Multiprotokoll-NAS-Volumes)".

Sofern nicht für einen bestimmten Vorgang anders angegeben, werden ab ONTAP 9.8 die folgenden allgemeinen Anforderungsheader unterstützt:

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

Bucket-Vorgänge

Die folgenden Vorgänge werden in ONTAP über AWS S3-APIs unterstützt:

Bucket-Betrieb	Der ONTAP Support beginnt mit
CreateBucket ONTAP S3 unterstützt alle gängigen Parameter und Header für diese Anfrage sowie diesen zusätzlichen Header: • `x-amz-bucket-object-lock-enabled`	ONTAP 9.11.1

Bucket-Betrieb	Der ONTAP Support beginnt mit
DeleteBucket ONTAP S3 unterstützt alle gängigen Parameter und Header für diese Anfrage.	ONTAP 9.11.1
DeleteBucketCors ONTAP S3 unterstützt alle gängigen Parameter und Header für diese Anfrage.	ONTAP 9,8
DeleteBucketLifecycle ONTAP S3 unterstützt alle gängigen Parameter und Header für diese Anfrage.	ONTAP 9,8
DeleteBucketRichtlinien ONTAP S3 unterstützt alle gängigen Parameter und Header für diese Anfrage.	ONTAP 9.12.1
GetBucketAcl ONTAP S3 unterstützt alle gängigen Parameter und Header für diese Anfrage.	ONTAP 9,8
GetBucketCors ONTAP S3 unterstützt alle gängigen Parameter und Header für diese Anfrage.	ONTAP 9,8
GetBucketLifecycleKonfiguration ONTAP S3 unterstützt alle gängigen Parameter und Header für diese Anfrage.	ONTAP 9.13.1 *Es werden nur Ablaufaktionen unterstützt
GetBucketLocation ONTAP S3 unterstützt alle gängigen Parameter und Header für diese Anfrage.	ONTAP 9.10.1
GetBucketPolicy ONTAP S3 unterstützt alle gängigen Parameter und Header für diese Anfrage.	ONTAP 9.12.1
GetBucketVersioning ONTAP S3 unterstützt alle gängigen Parameter und Header für diese Anfrage.	ONTAP 9.11.1
HeadBucket ONTAP S3 unterstützt alle gängigen Parameter und Header für diese Anfrage.	ONTAP 9,8
ListAllMyBuckets ONTAP S3 unterstützt alle gängigen Parameter und Header für diese Anfrage.	ONTAP 9,8
ListBuckets ONTAP S3 unterstützt alle gängigen Parameter und Header für diese Anfrage.	ONTAP 9,8
ListBucketVersions ONTAP S3 unterstützt alle gängigen Parameter und Header für diese Anfrage.	ONTAP 9.11.1
PutBucket	• ONTAP 9.11.1 • ONTAP 9.8: Nur unterstützt mit ONTAP REST-APIs
PutBucketCors ONTAP S3 unterstützt alle gängigen Parameter und Header für diese Anfrage.	ONTAP 9,8

Bucket-Betrieb	Der ONTAP Support beginnt mit
PutBucketLifecycleConfiguration ONTAP S3 unterstützt alle gängigen Parameter und Header für diese Anfrage.	ONTAP 9.13.1 * Es werden nur Ablaufaktionen unterstützt
PutBucketPolicy ONTAP S3 unterstützt alle gängigen Parameter und Header für diese Anfrage.	ONTAP 9.12.1
PutBucketVersioning ONTAP S3 unterstützt alle gängigen Parameter und Header für diese Anfrage.	ONTAP 9.11.1

Objekt-Operationen

Ab ONTAP 9.9 unterstützt ONTAP S3 Objekt-Metadaten und -Tagging.

- PutObject und CreateMultipartUpload enthalten Schlüssel-Wert-Paare mit `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:
  - PutObjectTagging
  - GetObjectTagging
  - DeleteObjectTagging

Ab ONTAP 9.11.1 unterstützt ONTAP S3 Objektversionierung und damit verbundene Aktionen mit den folgenden ONTAP-APIs:

- GetBucketVersioning
- ListBucketVersions
- PutBucketVersioning

Sofern nicht für einen bestimmten Vorgang anders angegeben, werden die folgenden URI-Abfrageparameter unterstützt:

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

Objektvorgang	Der ONTAP Support beginnt mit
AbortMehrteilaUpload ONTAP S3 unterstützt alle gängigen Parameter und Header für diese Anfrage sowie diesen zusätzlichen URI-Abfrageparameter: `uploadId`	ONTAP 9,8

Objektvorgang	Der ONTAP Support beginnt mit
CompleteMultipartUpload ONTAP S3 unterstützt alle gängigen Parameter und Header für diese Anfrage sowie diesen zusätzlichen URI-Abfrageparameter: `uploadId`	ONTAP 9,8
CopyObject ONTAP S3 unterstützt alle gängigen Parameter und Header für diese Anfrage sowie 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

Objektvorgang	Der ONTAP Support beginnt mit
CreateMultipartUpload ONTAP S3 unterstützt alle gängigen Parameter und Header für diese Anfrage sowie 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 alle gängigen Parameter und Header für diese Anfrage sowie diesen zusätzlichen Header: • `x-amz-bypass-governance-retention`	ONTAP 9,8
DeleteObjects ONTAP S3 unterstützt alle gängigen Parameter und Header für diese Anfrage sowie diesen zusätzlichen Header: * `x-amz-bypass-governance-retention`	ONTAP 9.11.1
DeleteObjectTagging ONTAP S3 unterstützt alle gängigen Parameter und Header für diese Anfrage.	ONTAP 9.9.1

Objektvorgang	Der ONTAP Support beginnt mit
GetObject ONTAP S3 unterstützt alle gängigen Parameter und Header für diese Anfrage sowie diese zusätzlichen URI-Abfrageparameter: • `partNumber` • `response-cache-control` • `response-content-disposition` • `response-content-encoding` • `response-content-language` • `response-content-type` • `response-expires` Und dieser zusätzliche Anforderungsheader: • Bereich	ONTAP 9,8
GetObjectAcl ONTAP S3 unterstützt alle gängigen Parameter und Header für diese Anfrage.	ONTAP 9,8
GetObjectAttributes ONTAP S3 unterstützt alle gängigen Parameter und Header für diese Anfrage sowie diesen zusätzlichen Header: • `x-amz-object-attributes`	ONTAP 9.17.1
GetObjectRetention ONTAP S3 unterstützt alle gängigen Parameter und Header für diese Anfrage.	ONTAP 9.14.1
GetObjectTagging ONTAP S3 unterstützt alle gängigen Parameter und Header für diese Anfrage.	ONTAP 9.9.1
HeadObject ONTAP S3 unterstützt alle gängigen Parameter und Header für diese Anfrage.	ONTAP 9,8

Objektvorgang	Der ONTAP Support beginnt mit
ListenMehrpartUpload ONTAP S3 unterstützt alle gängigen Parameter und Header für diese Anfrage sowie diese zusätzlichen URI-Parameter: • `delimiter` • `key-marker` • `max-uploads` • `prefix` • `upload-id-marker`	ONTAP 9,8
ListObjekte ONTAP S3 unterstützt alle gängigen Parameter und Header für diese Anfrage sowie diese zusätzlichen URI-Parameter: • `delimiter` • `encoding-type` • `marker` • `max-keys` • `prefix`	ONTAP 9,8
ListObjekteV2 ONTAP S3 unterstützt alle gängigen Parameter und Header für diese Anfrage sowie diese zusätzlichen URI-Parameter: • `continuation-token` • `delimiter` • `encoding-type` • `fetch-owner` • `max-keys` • `prefix` • `start-after`	ONTAP 9,8

Objektvorgang	Der ONTAP Support beginnt mit
ListObjectVersions ONTAP S3 unterstützt alle gängigen Parameter und Header für diese Anfrage sowie diese zusätzlichen URI-Parameter: • `delimiter` • `encoding-type` • `key-marker` • `max-keys` • `prefix` • `version-id-marker`	ONTAP 9.11.1
ListenTeile ONTAP S3 unterstützt alle gängigen Parameter und Header für diese Anfrage sowie diese zusätzlichen URI-Parameter: • `max-parts` • `part-number-marker` • `uploadId`	ONTAP 9,8
PutObject ONTAP S3 unterstützt alle gängigen Parameter und Header für diese Anfrage sowie 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 S3 unterstützt alle gängigen Parameter und Header für diese Anfrage.	ONTAP 9.14.1

Objektvorgang	Der ONTAP Support beginnt mit
PutObjectRetention ONTAP S3 unterstützt alle gängigen Parameter und Header für diese Anfrage sowie diesen zusätzlichen Header: • `x-amz-bypass-governance-retention`	ONTAP 9.14.1
PutObjectTagging ONTAP S3 unterstützt alle gängigen Parameter und Header für diese Anfrage.	ONTAP 9.9.1
UploadTeil	ONTAP 9,8
UploadPartCopy ONTAP S3 unterstützt alle gängigen Parameter und Header für diese Anfrage sowie diese zusätzlichen URI-Parameter: • `partNumber` • `uploadId` Und diese zusätzlichen Anforderungsheader: • `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 Vorgänge sind nicht speziell für S3 vorgesehen und sind im Allgemeinen mit IAM-Prozessen verbunden. ONTAP unterstützt diese Befehle, verwendet jedoch keine IAM REST-APIs.

- Erstellen Sie Die Policy
- AttachGroup-Richtlinie

Benutzermanagement

Diese Vorgänge sind nicht spezifisch für S3 und im Allgemeinen mit IAM-Prozessen verknüpft.

- CreateUser
- DeleteUser
- CreateGroup

- DeleteGroup

S3-Aktionen nach Release

ONTAP 9.14.1

ONTAP 9.14.1 bietet Unterstützung für S3 Object Lock.

> Legal Hold Operationen (Sperren ohne definierte Aufbewahrungszeiten) werden nicht unterstützt.

- GetObjectLockConfiguration
- GetObjectRetention
- PutObjectLockKonfiguration
- PutObjectRetention

ONTAP 9.13.1

ONTAP 9.13.1 bietet zusätzliche Unterstützung für Bucket-Lifecycle-Management.

- DeleteBucketLifecycleKonfiguration
- GetBucketLifecycleKonfiguration
- PutBucketLifecycleKonfiguration

ONTAP 9.12.1

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

- DeleteBucketRichtlinien
- GetBucketPolicy
- PutBucketPolicy
- CopyObject
- UploadPartCopy

ONTAP 9.11.1

ONTAP 9.11.1 bietet Unterstützung für Versionierung, vorbestimmte URLs, Chunked-Uploads und Unterstützung für gängige S3-Aktionen wie das Erstellen und Löschen von Buckets mithilfe von S3-APIs.

- ONTAP S3 unterstützt jetzt Chunked Uploads Signierungsanfragen mit `x-amz-content-sha256: STREAMING-AWS4-HMAC-SHA256-PAYLOAD`
- ONTAP S3 unterstützt jetzt Client-Anwendungen mit vorgeschlichenen URLs, um Objekte freizugeben oder anderen Benutzern das Hochladen von Objekten zu ermöglichen, ohne dass Benutzeranmeldeinformationen erforderlich sind.
- CreateBucket
- DeleteBucket
- GetBucketVersioning
- ListBucketVersions
- PutBucket

- PutBucketVersioning
- Objekte deObjekteObjekte
- ListObjectVersions

> Da die zugrunde liegende FlexGroup erst dann erstellt wird, wenn der erste Bucket erstellt wurde, 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 bietet jetzt Unterstützung für Objekt-Metadaten und Tagging für ONTAP S3.

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

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

- PutObjectTagging
- GetObjectTagging
- DeleteObjectTagging

ONTAP S3 Interoperabilität

Der ONTAP S3-Server interagiert normalerweise mit anderen ONTAP-Funktionen, mit Ausnahme der in dieser Tabelle aufgeführten Funktion.

Feature-Bereich	Unterstützt	Nicht unterstützt
Cloud Volumes ONTAP	• Azure Clients in ONTAP 9.9.1 und neueren Versionen • AWS Clients in ONTAP 9.11.0 und neueren Versionen • Google Cloud Clients in ONTAP 9.12.1 und neueren Versionen	• Cloud Volumes ONTAP für jeden Client in ONTAP 9.8 und früheren Versionen

Feature-Bereich	Unterstützt	Nicht unterstützt
Datensicherung	• Cloud-Synchronisierung • Objektsperre; Governance und Compliance (ab ONTAP 9.14.1) • "Objektversionierung" (Ab ONTAP 9.11.1) • Nicht gespiegelte MetroCluster-Aggregate (ab ONTAP 9.12.1) • Gespiegelte MetroCluster-Aggregate (ab ONTAP 9.14.1) • "SnapMirror S3" (Ab 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 • Disaster Recovery für SVM • SyncMirror (SyncMirror-gespiegelte Aggregate werden in MetroCluster-Konfigurationen ab ONTAP 9.14.1 unterstützt. SyncMirror wird außerhalb von MetroCluster-Konfigurationen nicht unterstützt)
Verschlüsselung	• NetApp Aggregatverschlüsselung (NAE) • NetApp Volume Encryption (NVE) • NetApp Storage Encryption (NSE) • TLS/SSL	• SCHLACKE
MetroCluster Umgebungen beschrieben	-	SnapMirror S3
Storage-Effizienz	• Deduplizierung • Komprimierung • Datenverdichtung	• Effizienzgewinne auf Aggregatsebene (Mitglieder, die sich auf demselben Aggregat befinden, können die Vorteile der volumenübergreifenden Deduplizierung nutzen, Mitglieder, die sich auf verschiedenen Aggregaten befinden, jedoch nicht) • Volume-Klon des FlexGroup Volumes mit ONTAP S3 Buckets
Servicequalität (QoS)	• QoS-Maximalwerte (Decken) • QoS-Mindestwerte (Böden)	-

Feature-Bereich	Unterstützt	Nicht unterstützt
Zusätzliche Funktionen	• "Prüfung von S3-Ereignissen" (Ab ONTAP 9.10.1) • "Bucket-Lifecycle-Management" (Ab ONTAP 9.13.1) • FabricPool-Wolkenebene (nur natives S3) • FabricPool lokale Ebene (nur NAS-Volumes) • FlexCache volumes (beginnend mit ONTAP 9.18.1)	• FPolicy • Qtrees • Kontingente • FabricPool-Cloud-Tier (nur NAS-Volumes) • FabricPool lokale Ebene (nur natives S3)

Validierte Drittanbieterlösungen mit S3 in ONTAP

S3 ist ein universeller Standard und dies ist keine umfassende Liste unterstützter Anwendungen – lediglich eine Liste von Lösungen, die in Zusammenarbeit mit den jeweiligen Partnern validiert wurden. Wenn die von Ihnen gesuchte Lösung nicht aufgeführt ist, wenden Sie sich bitte an Ihren NetApp Ansprechpartner.

Mithilfe nativer S3-Buckets validierte Lösungen von Drittanbietern

- Amazon SageMaker
- Apache Hadoop S3A-Client
- Apache Kafka
- Apache Spark
- CommVault (V11)
- Konfluent Kafka
- NetBackup
- Red Hat Quay
- Rubrik
- Schneeflocke
- Trino
- Veeam (V12)

Diese Lösungen werden speziell für die Verwendung nativer S3-Buckets in ONTAP validiert. Einige dieser Lösungen, z. B. im Zusammenhang mit Versionierung, Objektsperren und anderen Funktionen, werden bei der Verwendung von "S3 NAS-Buckets (S3 in Multiprotokoll-NAS-Volumes)" .

Konfigurieren

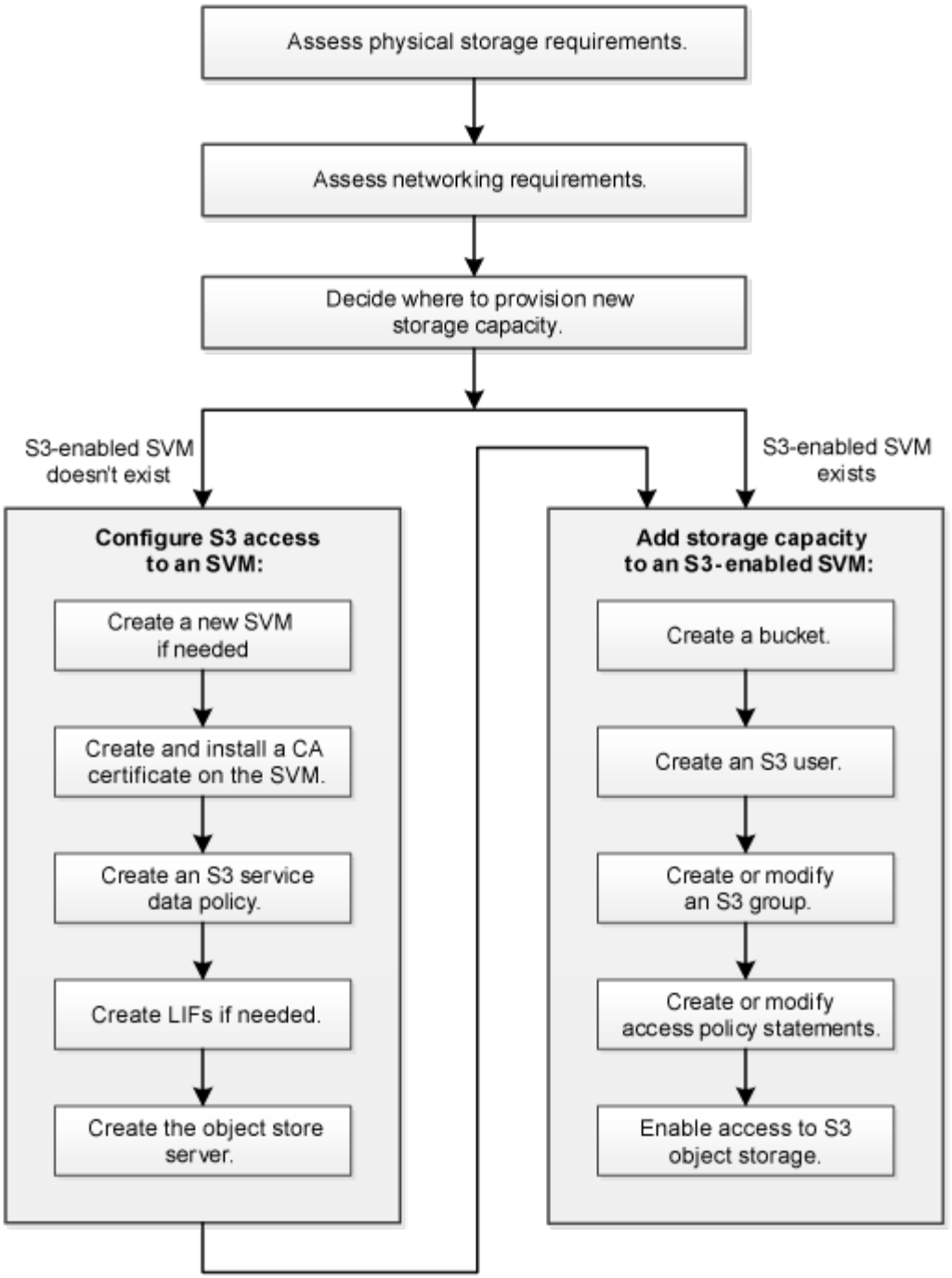
Allgemeines zur S3-Konfiguration

ONTAP S3 Konfigurations-Workflow

Bei der Konfiguration von S3 geht es darum, physische Storage- und Netzwerkanforderungen zu bewerten, und anschließend einen spezifischen Workflow auszuwählen: S3-Zugriff auf eine neue oder vorhandene SVM zu konfigurieren oder einen Bucket und Benutzer zu einer vorhandenen SVM hinzuzufügen, die bereits vollständig für S3-Zugriff konfiguriert ist.

Um sicherzustellen, dass die Zeit zwischen Clustern und Clients synchronisiert wird, ist eine NTP-Konfiguration (Network Time Protocol) erforderlich. Für den Clientzugriff ist häufig ein gültiger Zeitstempel mit mindestens 15 Minuten Unterschied zwischen dem ONTAP S3-Objektspeicher und dem Client erforderlich. "Erfahren Sie, wie Sie NTP konfigurieren" .

Wenn Sie mit System Manager S3-Zugriff auf eine neue Storage-VM konfigurieren, müssen Sie Zertifikat- und Netzwerkinformationen eingeben. Die Storage-VM und der S3-Objekt-Storage-Server werden in einem Vorgang erstellt.



Physische Storage-Anforderungen von ONTAP S3 bewerten

Bevor Sie S3-Storage für die Clients bereitstellen, müssen Sie sicherstellen, dass in vorhandenen Aggregaten für den neuen Objektspeicher ausreichend Speicherplatz vorhanden ist. Wird dies nicht der Fall sein, können Sie den gewünschten Typ und den gewünschten Speicherort mit Festplatten zu vorhandenen Aggregaten hinzufügen oder neue Aggregate erstellen.

Über diese Aufgabe

Wenn Sie einen S3-Bucket in einer S3-fähigen SVM erstellen, unterstützt ein FlexGroup-Volume "Automatisch erstellt" den Bucket. Sie können ONTAP Select die zugrunde liegenden Aggregate und FlexGroup

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

Wenn Sie sich entscheiden, die Aggregate und FlexGroup-Komponenten anzugeben, z. B. wenn Sie bestimmte Performance-Anforderungen für die zugrunde liegenden Festplatten haben — sollten Sie sicherstellen, dass die Aggregatkonfiguration den Best Practice-Richtlinien für die Bereitstellung eines FlexGroup Volume entspricht. Weitere Informationen:

- "Management von FlexGroup Volumes"
- "Technischer Bericht 4571-a: NetApp ONTAP FlexGroup Volume Top Best Practices"

Wenn Sie Buckets von Cloud Volumes ONTAP bereitstellen, wird dringend empfohlen, die zugrunde liegenden Aggregate manuell auszuwählen, um sicherzustellen, dass sie nur einen Node verwenden. Die Verwendung von Aggregaten beider Nodes kann sich auf die Performance auswirken, da die Nodes sich in geografisch getrennten Verfügbarkeitszonen befinden und daher anfällig für Latenzprobleme sind. Erfahren Sie mehr über "Erstellen von Buckets für Cloud Volumes ONTAP".

Sie können den ONTAP S3-Server verwenden, um eine lokale FabricPool-Kapazitäts-Tier zu erstellen, d. h. im selben Cluster wie die Performance-Tier. Dies kann beispielsweise nützlich sein, wenn Sie SSD-Festplatten an ein HA-Paar angeschlossen haben und Sie *Cold* Daten auf HDD-Festplatten in einem anderen HA-Paar verschieben möchten. In diesem Anwendungsfall sollten sich der S3-Server und der Bucket, der die lokale Kapazitäts-Tier enthält, daher in einem anderen HA-Paar als das Performance-Tier befinden. Lokales Tiering wird nicht auf Clustern mit einem oder zwei Nodes unterstützt.

Schritte

1. Anzeige des verfügbaren Speicherplatzes in vorhandenen Aggregaten:

   ```
   storage aggregate show
   ```

   Wenn genügend Speicherplatz oder der erforderliche Speicherort für ein Aggregat vorhanden ist, notieren Sie seinen Namen für die S3-Konfiguration.

   ```
   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 einem erforderlichen Node vorhanden sind, fügen Sie mithilfe des `storage aggregate add-disks` Befehls Festplatten zu einem vorhandenen Aggregat hinzu oder erstellen Sie mithilfe des `storage aggregate create` Befehls ein neues Aggregat.

Verwandte Informationen

- "Speicheraggregat-Add-Disks"
- "Speicheraggregat erstellen"

Netzwerkanforderungen von ONTAP S3 bewerten

Bevor Sie Clients S3 Storage bereitstellen, müssen Sie überprüfen, ob Netzwerke korrekt konfiguriert sind, um die S3-Bereitstellungsanforderungen zu erfüllen.

Bevor Sie beginnen

Die folgenden Cluster-Netzwerkobjekte müssen konfiguriert werden:

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

Über diese Aufgabe

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

Für lokale FabricPool-Kapazitäts-Tiers müssen Sie die System-SVM (namens „`Cluster`“) verwenden, aber es gibt zwei Optionen für die LIF-Konfiguration:

- Sie können die Cluster-LIFs verwenden.

  Bei dieser Option ist keine weitere LIF-Konfiguration erforderlich, doch der Datenverkehr auf Cluster-LIFs wird erhöht. Außerdem kann andere Cluster nicht auf die lokale Tier zugreifen.

- Sie können Daten verwenden und LIFs Intercluster verwenden.

  Diese Option erfordert eine zusätzliche Konfiguration, einschließlich der Aktivierung der LIFs für das S3-Protokoll, aber auf die lokale Tier kann auch für andere Cluster als Remote-FabricPool-Cloud-Tier zugegriffen werden.

Schritte

1. Anzeigen der verfügbaren physischen und virtuellen Ports:

   ```
   network port show
   ```

   - Wenn möglich, sollten Sie den Port mit der höchsten Geschwindigkeit für das Datennetzwerk verwenden.

    - Für optimale Performance müssen alle Komponenten im Datennetzwerk dieselbe MTU-Einstellung aufweisen.
2. Wenn Sie planen, einen Subnetznamen zu verwenden, um die IP-Adresse und den Netzwerkmaskenwert für eine LIF zuzuweisen, überprüfen Sie, ob das Subnetz existiert und über ausreichende Adressen verfügbar ist:

   `network subnet show`

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

   Erfahren Sie mehr über `network subnet show` 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, überprüfen Sie, ob IPv6 auf dem Cluster aktiviert ist:

   `network options ipv6 show`

   Falls erforderlich, können Sie IPv6 mit dem `network options ipv6 modify` Befehl aktivieren.

Verwandte Informationen

- "Netzwerkport zeigen"
- "Netzwerkoptionen ipv6"
- "Netzwerk-ipspace wird angezeigt"
- "Netzwerk-Subnetz erstellen"

Entscheiden Sie, wo Sie neue ONTAP S3 Storage-Kapazität bereitstellen

Bevor Sie einen neuen S3-Bucket erstellen, müssen Sie entscheiden, ob er in eine neue oder vorhandene SVM platziert werden soll. Diese Entscheidung bestimmt Ihren Workflow.

Wahlmöglichkeiten

- Wenn Sie einen Bucket in einer neuen SVM oder einer SVM bereitstellen möchten, der für S3 nicht aktiviert ist, führen Sie die Schritte in den folgenden Themen aus.

  "Erstellung einer SVM für S3"

  "Erstellen eines Buckets für S3"

  Obwohl S3 parallel in einer SVM mit NFS und SMB eingesetzt werden kann, können Sie möglicherweise eine neue SVM erstellen, sofern eine der folgenden Optionen zutrifft:

    - Sie aktivieren erstmals S3 auf einem Cluster.
    - Sie verfügen über vorhandene SVMs in einem Cluster, in dem die S3-Unterstützung nicht aktiviert

werden soll.

    - Sie verfügen über eine oder mehrere S3-fähige-SVMs in einem Cluster und möchten einen weiteren S3-Server mit unterschiedlichen Performance-Merkmalen nutzen. Nachdem Sie S3 auf der SVM aktiviert haben, fahren Sie mit der Bereitstellung eines Buckets fort.

- Wenn Sie den anfänglichen Bucket oder einen zusätzlichen Bucket auf einer vorhandenen S3-fähigen SVM bereitstellen möchten, führen Sie die Schritte im folgenden Thema aus.

  "Erstellen eines Buckets für S3"

Konfigurieren des S3-Zugriffs auf eine SVM

SVM für ONTAP S3 erstellen

Obwohl S3 parallel zu anderen Protokollen in einer SVM unterstützt werden kann, sollten Sie möglicherweise eine neue SVM erstellen, um Namespace und Workload zu isolieren.

Über diese Aufgabe

Wenn Sie lediglich S3-Objekt-Storage über eine SVM bereitstellen, ist für den S3-Server keine DNS-Konfiguration erforderlich. Allerdings möchten Sie DNS möglicherweise auf der SVM konfigurieren, wenn andere Protokolle verwendet werden.

Wenn Sie mit System Manager S3-Zugriff auf eine neue Storage-VM konfigurieren, müssen Sie Zertifikat- und Netzwerkinformationen eingeben. Die Storage-VM und der S3-Objekt-Storage-Server werden in einem Vorgang erstellt.

Beispiel 1. Schritte

System Manager

Sie sollten darauf vorbereitet sein, den S3-Servernamen als vollständig qualifizierter Domain-Name (FQDN) einzugeben, den die 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 Schnittstellenrollendaten einzugeben.

Wenn Sie ein von einer externen Zertifizierungsstelle signiertes Zertifikat verwenden, werden Sie aufgefordert, es während dieses Verfahrens einzugeben. Sie haben auch die Möglichkeit, ein vom System generiertes Zertifikat zu verwenden.

1. Aktivieren Sie S3 auf einer Storage-VM.

   a. Fügen Sie eine neue Speicher-VM hinzu: Klicken Sie auf **Storage > Storage VMs** und dann auf **Hinzufügen**.

      Falls es sich um ein neues System ohne bereits vorhandene Storage-VMs handelt, klicken Sie auf **Dashboard > Protokolle konfigurieren**.

   Wenn Sie einen S3-Server zu einer vorhandenen Speicher-VM hinzufügen: Klicken Sie auf **Speicher > Speicher-VMs**, wählen Sie eine Speicher-VM aus, klicken Sie auf **Einstellungen** und klicken Sie dann ⚙ unter **S3**.

   a. Klicken Sie auf **S3** aktivieren und geben Sie dann den S3-Servernamen ein.

   b. Wählen Sie den Zertifikatstyp aus.

      Unabhängig davon, ob Sie ein vom System generiertes Zertifikat oder ein eigenes Zertifikat auswählen, wird es für den Client-Zugriff erforderlich sein.

   c. Geben Sie die Netzwerkschnittstellen ein.

2. Wenn Sie das vom System generierte Zertifikat ausgewählt haben, werden Ihnen die Zertifikatsinformationen angezeigt, wenn die Erstellung der neuen Storage-VM bestätigt wurde. Klicken Sie auf **Download** und speichern Sie es für den Client-Zugriff.
   - Der Geheimschlüssel wird nicht mehr angezeigt.
   - Wenn Sie die Zertifikatinformation erneut benötigen: Klicken Sie auf **Storage > Storage VMs**, wählen Sie die Speicher-VM aus und klicken Sie auf **Einstellungen**.

CLI

1. Vergewissern Sie sich, dass S3 für Ihr Cluster lizenziert ist:

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

   Falls nicht, wenden Sie sich an Ihren Vertriebsmitarbeiter.

2. 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>
```

- Verwenden Sie die UNIX-Einstellung für die `-rootvolume-security-style` Option.
- Verwenden Sie die Standardoption C.UTF-8 `-language`.
- Die `ipspace` Einstellung ist optional.

3. Konfiguration und Status der neu erstellten SVM überprüfen:

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

Das `Vserver Operational State` Feld muss den `running` Status anzeigen. Wenn auf der Statusanzeige der `initializing` Status angezeigt wird, ist ein Zwischenvorgang wie das Erstellen des Root-Volumes fehlgeschlagen, und Sie müssen die SVM löschen und neu erstellen.

Beispiele

Mit dem folgenden Befehl wird eine SVM für den Datenzugriff im IPspace ipspace A erstellt:

```
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
```

Mit dem folgenden Befehl wird angezeigt, dass eine SVM mit einem 1-GB-Root-Volume erstellt wurde und dieses automatisch gestartet wurde und sich im `running` Status befindet. Das Root-Volume verfügt über eine standardmäßige Exportrichtlinie, 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 vsadmin-Standardbenutzerkonto 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 S3-fähigen ONTAP SVM

S3-Clients benötigen ein CA-Zertifikat (Certificate Authority), um HTTPS-Verkehr an die S3-fähige SVM zu senden. CA-Zertifikate stellen eine vertrauenswürdige Beziehung zwischen Clientanwendungen und dem ONTAP Objektspeicherserver her. Sie sollten ein CA-Zertifikat auf ONTAP installieren, bevor Sie es als für Remote-Clients zugänglichen Objektspeicher verwenden.

Über diese Aufgabe

Zwar ist es möglich, einen S3-Server so zu konfigurieren, dass nur HTTP verwendet wird. Clients können zwar auch ohne CA-Zertifikat konfiguriert werden, es empfiehlt sich jedoch, den HTTPS-Datenverkehr auf ONTAP S3-Servern mit einem CA-Zertifikat zu sichern.

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

Die Anweisungen in diesem Verfahren erstellen und installieren ein selbstsigniertes ONTAP-Zertifikat. Obwohl ONTAP selbstsignierte Zertifikate generieren kann, empfiehlt es sich, signierte Zertifikate von einer Zertifizierungsstelle eines Drittanbieters zu verwenden. Weitere Informationen finden Sie in der Dokumentation zur Administratorauthentifizierung.

"Administratorauthentifizierung und RBAC"

Weitere Informationen zu `security certificate` und zusätzlichen Konfigurationsoptionen finden Sie im "ONTAP-Befehlsreferenz".

Schritte

1. Erstellen eines selbstsignierten digitalen Zertifikats:

   `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, um andere Zertifikate durch die Funktion einer Zertifizierungsstelle zu signieren.

   Die `-common-name` Option erstellt den Namen der Zertifizierungsstelle (CA) der SVM und wird verwendet, wenn der vollständige Name des Zertifikats generiert wird.

   Die standardmäßige Zertifikatsgröße 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, speichern Sie ihn für die nachfolgenden Schritte.

   Erfahren Sie mehr über `security certificate create` in der "ONTAP-Befehlsreferenz".

2. Erzeugen einer Anfrage zum Signieren eines Zertifikats:

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

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

   Gegebenenfalls können Sie den Speicherort und weitere detaillierte Informationen zur SVM angeben.

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

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

   Sie werden aufgefordert, eine Kopie Ihrer Zertifikatsanfrage und einen privaten Schlüssel für zukünftige Referenz aufzubewahren.

   Erfahren Sie mehr über `security certificate generate-csr` in der "ONTAP-Befehlsreferenz".

3. Signieren Sie die CSR mit SVM_CA, um das S3-Server-Zertifikat 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 früheren Schritten verwendet haben:

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

     Standardmäßig läuft das signierte Zertifikat in 365 Tagen ab. Sie können einen anderen Wert auswählen und weitere Signierungsdetails angeben.

     Wenn Sie dazu aufgefordert werden, kopieren Sie die Zeichenfolge für die Zertifikatanforderung, die Sie in Schritt 2 gespeichert haben, und geben Sie sie ein.

   Es wird ein signiertes Zertifikat angezeigt und zur späteren Verwendung gespeichert.

4. Installieren Sie das signierte Zertifikat auf der S3-fähigen SVM:

   `security certificate install -type server -vserver svm_name`

   Geben Sie bei Aufforderung das Zertifikat und den privaten Schlüssel ein.

   Sie haben die Möglichkeit, Zwischenzertifikate einzugeben, wenn eine Zertifikatkette gewünscht wird.

   Wenn der private Schlüssel und das CA-signierte digitale Zertifikat angezeigt werden, speichern Sie sie für zukünftige Referenz.

5. Holen Sie sich das Zertifikat für den öffentlichen Schlüssel:

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

   Speichern Sie das Zertifikat für den öffentlichen Schlüssel für eine spätere Client-seitige Konfiguration.

   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"
- "Sicherheitszertifikatzeichen"

ONTAP S3 Servicedatenrichtlinie erstellen

Es können Service-Richtlinien für S3-Daten und Managementservices erstellt werden. Für die Aktivierung des S3-Datenverkehrs auf LIFs ist eine S3-Service-Datenrichtlinie erforderlich.

Über diese Aufgabe

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

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

Obwohl mehrere Protokolle für SVMs und LIFs konfiguriert werden können, empfiehlt es sich, S3 als einziges

Protokoll für die Bereitstellung von Objektdaten zu verwenden.

Schritte

1. Ändern Sie die Berechtigungseinstellung in erweitert:

   ```
   set -privilege advanced
   ```

2. Service-Datenrichtlinie erstellen:

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

   Die `data-core` `data-s3-server` Services und sind die einzigen, die zur Aktivierung von ONTAP S3 erforderlich sind, auch wenn bei Bedarf andere Services enthalten sein können.

   Erfahren Sie mehr über `network interface service-policy create` in der "ONTAP-Befehlsreferenz".

Erstellen Sie Daten-LIFs für ONTAP S3

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

Bevor Sie beginnen

- Der zugrunde liegende physische oder logische Netzwerkport muss im Administratorstatus konfiguriert worden `up` sein. Erfahren Sie mehr über `up` in der "ONTAP-Befehlsreferenz".
- Wenn Sie planen, einen Subnetznamen zu verwenden, um die IP-Adresse und den Netzwerkmaskenwert für eine LIF zuzuweisen, muss das Subnetz bereits vorhanden sein.

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

  Erfahren Sie mehr über `network subnet create` in der "ONTAP-Befehlsreferenz".

- Die Richtlinie für den LIF-Dienst muss bereits vorhanden sein.
- Als Best Practice sollten LIFs, die für den Datenzugriff verwendet werden (Daten-s3-Server), und für Managementaufgaben verwendete LIFs (Management-https) getrennt sein. Beide Services sollten nicht auf derselben logischen Schnittstelle aktiviert werden.
- DNS-Einträge sollten nur IP-Adressen der LIFs haben, denen der Daten-s3-Server zugeordnet ist. Wenn IP-Adressen anderer LIFs im DNS-Datensatz angegeben werden, können ONTAP S3-Anfragen von anderen Servern bedient werden, was zu unerwarteten Antworten oder Datenverlusten führt.

Über diese Aufgabe

- Sie können am gleichen Netzwerkport IPv4- und IPv6-LIFs erstellen.
- Wenn Sie im Cluster eine große Anzahl von LIFs enthalten sind, können Sie die auf dem Cluster unterstützte LIF- `network interface capacity show`Kapazität überprüfen. Verwenden Sie dazu den Befehl und die auf jedem Node unterstützte LIF-Kapazität. Hierzu können Sie mit dem `network interface capacity details show` Befehl (auf der erweiterten Berechtigungsebene) nachprüfen.

  Erfahren Sie mehr über `network interface capacity show` und `network interface capacity`

`details show` in der "ONTAP-Befehlsreferenz".

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

Schritte

1. 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 Node, zu dem das LIF zurückgibt, wenn der `network interface revert` Befehl auf der LIF ausgeführt wird.

     Erfahren Sie mehr über `network interface revert` in der "ONTAP-Befehlsreferenz".

     Sie können außerdem angeben, ob die LIF mithilfe der `-auto-revert` Option automatisch zum Home Node und Home Port zurückgesetzt werden soll.

   - `-home-port` Ist der physische oder logische Port, zu dem die LIF zurückgibt, wenn der `network interface revert` Befehl auf der LIF ausgeführt wird.
   - Sie können eine IP-Adresse mit den `-address -netmask` Optionen und angeben oder die Zuweisung aus einem Subnetz mit der `-subnet_name` Option aktivieren.
   - Wenn Sie zur Versorgung der IP-Adresse und Netzwerkmaske ein Subnetz verwenden, wird bei einem Gateway automatisch eine Standardroute zu diesem Gateway zur SVM hinzugefügt, wenn mithilfe dieses Subnetzes eine LIF erstellt wird.
   - Wenn Sie IP-Adressen manuell zuweisen (ohne ein Subnetz zu verwenden), müssen Sie möglicherweise eine Standardroute zu einem Gateway konfigurieren, wenn Clients oder Domänen-Controller in einem anderen IP-Subnetz vorhanden sind. Weitere Informationen zum `network route create` Erstellen einer statischen Route innerhalb einer SVM finden Sie im "ONTAP-Befehlsreferenz".
   - `-firewall-policy`Verwenden Sie für die Option denselben Standard `data` wie die LIF-Rolle.

     Sie können bei Bedarf später eine benutzerdefinierte Firewallrichtlinie erstellen und hinzufügen.

     > Ab ONTAP 9.10.1 sind Firewall-Richtlinien veraltet und werden vollständig durch LIF-Servicerichtlinien ersetzt. Weitere Informationen finden Sie unter "Konfigurieren Sie Firewallrichtlinien für LIFs".

   - `-auto-revert` Ermöglicht Ihnen die Angabe, ob eine Daten-LIF automatisch auf ihren Home Node zurückgesetzt wird, wenn beispielsweise ein Start erfolgt, Änderungen am Status der Managementdatenbank oder die Netzwerkverbindung hergestellt wird. Die Standardeinstellung ist `false`, Sie können sie jedoch `false` abhängig von den Netzwerkverwaltungsrichtlinien in Ihrer Umgebung auf festlegen.
   - Die `-service-policy` Option gibt die Richtlinie für Daten- und Managementservices an, die Sie erstellt haben, sowie weitere Richtlinien, die Sie benötigen.

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

a. Verwenden Sie den `network ndp prefix show` Befehl, um die Liste der RA-Präfixe anzuzeigen, die an verschiedenen Schnittstellen gelernt wurden.

   Der `network ndp prefix show` Befehl ist auf der erweiterten Berechtigungsebene verfügbar.

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

   `prefix` Wird das Präfix an verschiedenen Schnittstellen gelernt.

   ```
   `id`Wählen Sie zum Ableiten der eine zufällige 64-Bit-Hexadezimalzahl aus.
   ```

3. Überprüfen Sie mit dem `network interface show` Befehl, ob das LIF erfolgreich erstellt wurde.
4. Vergewissern Sie sich, dass die konfigurierte IP-Adresse erreichbar ist:

Überprüfen einer…	**Verwenden…**
IPv4-Adresse	`network ping`
IPv6-Adresse	`network ping6`

Beispiele

Im folgenden Befehl wird gezeigt, wie eine S3-Daten-LIF erstellt wird, die mit der `my-S3-policy` Service-Richtlinie zugewiesen ist:

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

Mit dem folgenden Befehl werden alle LIFs in Cluster-1 angezeigt. Datenschnittstellen Datenschnittstellen Datenverbund Daten3 werden mit IPv4-Adressen konfiguriert und Daten3 wird 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"
- "Netzwerk-ndp-Präfix anzeigen"

Erstellen Sie Intercluster LIFs für Remote-FabricPool-Tiering mit ONTAP S3

Wenn Sie Cloud-Tiering (Remote FabricPool Capacity) mit ONTAP S3 aktivieren, müssen Sie Intercluster LIFs konfigurieren. Sie können Intercluster-LIFs an Ports konfigurieren, die gemeinsam mit dem Datennetzwerk verwendet werden. Auf diese Weise wird die Anzahl der Ports reduziert, die Sie für Intercluster-Netzwerke benötigen.

Bevor Sie beginnen

- Der zugrunde liegende physische oder logische Netzwerkport muss im Administratorstatus konfiguriert worden `up` sein. Erfahren Sie mehr über `up` in der "ONTAP-Befehlsreferenz".
- Die Richtlinie für den LIF-Dienst muss bereits vorhanden sein.

Über diese Aufgabe

Intercluster LIFs sind für das lokale Fabric Pool Tiering oder für die Bereitstellung externer S3-Applikationen nicht erforderlich.

Schritte

1. Liste der Ports im Cluster:

   ```
   network port show
   ```

   Das folgende Beispiel zeigt die Netzwerkports 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
   ```

   Erfahren Sie mehr über `network port show` in der "ONTAP-Befehlsreferenz".

2. Intercluster-LIFs auf der 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
   ```

   Im folgenden Beispiel werden Intercluster LIFs `cluster01_icl01` und erstellt `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
```

Erfahren Sie mehr über `network interface create` in der "ONTAP-Befehlsreferenz".

3. Überprüfen Sie, 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. Vergewissern Sie sich, dass die Intercluster-LIFs redundant sind:

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

   Im folgenden Beispiel wird gezeigt, dass Intercluster LIFs `cluster01_icl01` und `cluster01_icl02` auf dem `e0c` Port `e0d` ein Failover zum Port ausführen.

```
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
```

Erfahren Sie mehr über `network interface show` in der "ONTAP-Befehlsreferenz".

Erstellen Sie den ONTAP S3-Objektspeicher-Server

Der ONTAP Objektspeicher-Server managt Daten als S3-Objekte, anstatt von Datei- oder Block-Storage, der von ONTAP NAS- und SAN-Servern bereitgestellt wird.

Bevor Sie beginnen

Sie sollten darauf vorbereitet sein, den S3-Servernamen als vollständig qualifizierter Domain-Name (FQDN) einzugeben, den die Clients für den S3-Zugriff verwenden. Der FQDN darf nicht mit einem Bucket-Namen beginnen. Beim Zugriff auf Buckets im Virtual-Hosted-Stil wird der Servername als verwendet `mydomain.com`. `bucketname.mydomain.com`Beispiel: .

Sie sollten über ein selbstsigniertes CA-Zertifikat (erstellt in vorherigen Schritten) oder ein Zertifikat, das von einem externen CA-Anbieter signiert wurde. Ein CA-Zertifikat ist nicht erforderlich für einen lokalen Tiering-Anwendungsfall, bei dem der IP-Traffic nur über die Cluster LIFs erfolgt.

Über diese Aufgabe

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

> Verwenden Sie als NetApp Best Practice diesen Root-Benutzer nicht. Alle Client-Anwendungen, die den Zugriffsschlüssel oder den geheimen Schlüssel des Root-Benutzers verwenden, haben vollständigen Zugriff auf alle Buckets und Objekte im Objektspeicher.

Erfahren Sie mehr über `vserver object-store-server` in der "ONTAP-Befehlsreferenz".

Beispiel 2. Schritte

System Manager

Gehen Sie folgendermaßen vor, wenn Sie einer vorhandenen Storage-VM einen S3-Server hinzufügen. Informationen zum Hinzufügen eines S3-Servers zu einer neuen Storage-VM finden Sie unter "Erstellung einer Storage-SVM für S3".

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

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

      Unabhängig davon, ob Sie ein vom System generiertes Zertifikat oder ein eigenes Zertifikat auswählen, wird es für den Client-Zugriff erforderlich sein.

   d. Geben Sie die Netzwerkschnittstellen ein.
2. Wenn Sie das vom System generierte Zertifikat ausgewählt haben, werden Ihnen die Zertifikatsinformationen angezeigt, wenn die Erstellung der neuen Storage-VM bestätigt wurde. Klicken Sie auf **Download** und speichern Sie es für den Client-Zugriff.
   - Der Geheimschlüssel wird nicht mehr angezeigt.
   - Wenn Sie die Zertifikatinformation erneut benötigen: Klicken Sie auf **Storage > Storage VMs**, wählen Sie die Speicher-VM aus und klicken Sie auf **Einstellungen**.

CLI

1. Erstellen des S3-Servers:

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

   Sie können weitere Optionen beim Erstellen des S3-Servers oder zu einem späteren Zeitpunkt festlegen.

   - Beim Konfigurieren von lokalem Tiering kann der SVM-Name entweder ein Daten-SVM- oder ein System-SVM-(Cluster-)Name sein.
   - Der Zertifikatname sollte der Name des Serverzertifikats (Endbenutzer- oder Leaf-Zertifikat) und nicht das Server-CA-Zertifikat (Zwischen- oder Stammzertifizierungsstellenzertifikat) sein.
   - HTTPS ist standardmäßig an Port 443 aktiviert. Sie können die Portnummer mit der `-secure -listener-port` Option ändern.

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

   - HTTP ist standardmäßig deaktiviert. Wenn diese Option aktiviert ist, wartet der Server an Port 80. Sie können sie mit der `-is-http-enabled` Option aktivieren oder die Portnummer mit der `-listener-port` Option ändern.

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

2. Vergewissern Sie sich, dass S3 konfiguriert ist:

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

Beispiel

Mit diesem Befehl werden die Konfigurationswerte aller Objektspeicher-Server überprüft:

```
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
```

Fügen Sie einer S3-fähigen SVM Storage-Kapazität hinzu

Erstellen eines ONTAP S3-Buckets

S3 Objekte werden in *Buckets* aufbewahrt. Sie sind nicht als Dateien innerhalb eines Verzeichnisses in anderen Verzeichnissen verschachtelt.

Bevor Sie beginnen

Eine Storage-VM mit einem S3-Server muss bereits vorhanden sein.

Über diese Aufgabe

- Ab ONTAP 9.14.1 wurde die automatische Größenanpassung bei S3 FlexGroup Volumes beim Erstellen von Buckets aktiviert. So wird bei der Bucket-Erstellung auf vorhandenen und neuen FlexGroup Volumes keine übermäßige Kapazitätszuweisung mehr erreicht. Die Größe von FlexGroup Volumes wird anhand der folgenden Richtlinien auf die erforderliche Mindestgröße angepasst. Die erforderliche Mindestgröße ist die Gesamtgröße aller S3-Buckets in einem FlexGroup Volume.
  - Ab ONTAP 9.14.1 wird das FlexGroup Volume mit der minimal erforderlichen Größe erstellt, wenn ein S3-FlexGroup-Volume als Teil einer neuen Bucket-Erstellung erstellt wird.
  - Wenn ein S3-FlexGroup-Volume vor ONTAP 9.14.1 erstellt wurde, wird beim ersten, nach ONTAP 9.14.1 erstellten oder gelöschten Bucket das FlexGroup-Volume auf die minimal erforderliche Größe angepasst.
  - Wenn ein S3-FlexGroup-Volume vor ONTAP 9.14.1 erstellt wurde und bereits über die erforderliche Mindestgröße verfügt, bleibt beim Erstellen oder Löschen eines Buckets nach ONTAP 9.14.1 die Größe des S3-FlexGroup-Volumes erhalten.

- Storage-Service-Level sind vordefinierte Richtliniengruppen mit adaptiver Quality of Service (QoS) mit Standardeinstellungen wie *Value*, Performance_ und *extreme*. Anstelle eines der standardmäßigen Storage-Service-Level können Sie auch eine individuelle QoS-Richtliniengruppe definieren und auf einen Bucket anwenden. Weitere Informationen zu Speicherdienstdefinitionen finden Sie unter "Definitionen von Storage-Services". Weitere Informationen zum Leistungsmanagement finden Sie unter "Performance Management". Ab ONTAP 9.8 ist bei der Bereitstellung von Storage QoS standardmäßig aktiviert. Sie können die QoS während der Bereitstellung oder zu einem späteren Zeitpunkt deaktivieren oder eine benutzerdefinierte QoS-Richtlinie auswählen.
- Wenn Sie lokales Kapazitäts-Tiering konfigurieren, erstellen Sie Buckets und Benutzer in einer Daten-Storage-VM und nicht in der System-Storage-VM, auf der sich der S3 Server befindet.
- Für den Remote-Client-Zugriff müssen Sie Buckets in einer S3-fähigen Storage-VM konfigurieren. Wenn Sie einen Bucket in einer Storage-VM erstellen, die nicht S3-aktiviert ist, ist dieser nur für lokales Tiering verfügbar.
- Beginnend mit ONTAP 9.14.1, können Sie "Erstellung eines Buckets auf einem gespiegelten oder nicht gespiegelten Aggregat in einer MetroCluster Konfiguration".
- Wenn Sie für die CLI einen Bucket erstellen, haben Sie zwei Bereitstellungsoptionen:
  - Lassen Sie ONTAP Select die zugrunde liegenden Aggregate und FlexGroup Komponenten (Standard)
    - ONTAP erstellt und konfiguriert ein FlexGroup-Volume für den ersten Bucket durch die automatische Auswahl der Aggregate. Er wählt automatisch das höchste Service-Level aus, das für Ihre Plattform verfügbar ist, oder Sie können das Storage-Service-Level angeben. Alle zusätzlichen Buckets, die Sie später in der Storage-VM hinzufügen, verfügen über dasselbe zugrunde liegende FlexGroup Volume.
    - Alternativ können Sie angeben, ob der Bucket für das Tiering verwendet wird. In diesem Fall versucht ONTAP, kostengünstige Medien mit optimaler Performance für die Tiered-Daten auszuwählen.
  - Zudem wählen Sie die zugrunde liegenden Aggregate und FlexGroup-Komponenten aus (Optionen mit Advanced Privilege-Befehlen erforderlich): Sie können die Aggregate, auf denen der Bucket und das zugehörige FlexGroup Volume erstellt werden sollen, manuell auswählen und dann die Anzahl der Komponenten in jedem Aggregat angeben. Beim Hinzufügen weiterer Buckets:
    - Wenn Sie Aggregate und Komponenten für einen neuen Bucket angeben, wird für den neuen Bucket eine neue FlexGroup erstellt.
    - Wenn Sie keine Aggregate und Komponenten für einen neuen Bucket angeben, wird der neue Bucket zu einem vorhandenen FlexGroup hinzugefügt. Weitere Informationen finden Sie unter Management von FlexGroup Volumes .

      Wenn bei der Erstellung eines Buckets Aggregate und Komponenten angegeben werden, werden keine QoS-Richtliniengruppen oder Benutzerdefiniert angewendet. Sie können `vserver object-store-server bucket modify` dies später mit dem Befehl tun.

  Erfahren Sie mehr über `vserver object-store-server bucket modify` in der "ONTAP-Befehlsreferenz".

Hinweis: Wenn Sie Eimer von Cloud Volumes ONTAP bedienen, sollten Sie das CLI-Verfahren verwenden. Es wird dringend empfohlen, die zugrunde liegenden Aggregate manuell auszuwählen, um sicherzustellen, dass sie nur einen Node verwenden. Die Verwendung von Aggregaten beider Nodes kann sich auf die Performance auswirken, da die Nodes sich in geografisch getrennten Verfügbarkeitszonen befinden und daher anfällig für Latenzprobleme sind.

Erstellen von S3 Buckets mit der ONTAP-CLI

1. Wenn Sie Aggregate und FlexGroup-Komponenten selbst auswählen möchten, legen Sie die Berechtigungsebene auf „Advanced“ fest (anderenfalls ist die Administratorberechtigungsebene ausreichend): `set -privilege advanced`
2. Erstellen eines Buckets:

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

   Der Name der Storage-VM kann entweder eine Daten-Storage-VM oder `Cluster` (der Name der System-Storage-VM) sein, wenn Sie lokales Tiering konfigurieren.

   Wenn ONTAP einen Bucket auf Basis der Performance oder Auslastung erstellen soll, verwenden Sie eine der folgenden Optionen:

   - Service-Level

     Schließen Sie die `-storage-service-level` Option mit einem der folgenden Werte ein: `value`, `performance` Oder `extreme`.

   - tiering

     Schließen Sie die `-used-as-capacity-tier true` Option ein.

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

   - Der `-aggr-list` Parameter gibt die Liste mit Aggregaten an, die für FlexGroup Volume-Komponenten verwendet werden sollen.

     Jeder Eintrag in der Liste erstellt eine Komponente im angegebenen Aggregat. Sie können ein Aggregat mehrmals angeben, damit mehrere Komponenten auf dem Aggregat erstellt werden.

   Für eine konsistente Performance im FlexGroup Volume müssen alle Aggregate denselben Festplattentyp und dieselbe Konfiguration der RAID-Gruppen verwenden.

   - Der `-aggr-list-multiplier` Parameter gibt die Anzahl der Wiederholungen über die Aggregate an, die `-aggr-list` beim Erstellen eines FlexGroup Volume mit dem Parameter aufgelistet sind.

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

3. Fügen Sie bei Bedarf eine QoS-Richtliniengruppe hinzu:

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

4. Überprüfen der Bucket-Erstellung:

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

Beispiel

Im folgenden Beispiel wird ein Bucket für die Storage-VM `vs1` mit der Größe erstellt `1TB` und das Aggregat angegeben:

Erfahren Sie mehr über die in diesem Verfahren beschriebenen Befehle im "ONTAP-Befehlsreferenz".

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

Erstellung von S3 Buckets mit System Manager

1. Fügen Sie auf einer S3-fähigen Storage-VM einen neuen Bucket hinzu.
   a. Klicken Sie auf **Storage > Buckets** und dann auf **Hinzufügen**.
   b. Geben Sie einen Namen ein, wählen Sie die Storage-VM aus und geben Sie eine Größe ein.
      - Wenn Sie an dieser Stelle auf **Speichern** klicken, wird ein Bucket mit den folgenden Standardeinstellungen erstellt:
        - Benutzern wird kein Zugriff auf den Bucket gewährt, es sei denn, bereits Gruppenrichtlinien sind gültig.

          Sie sollten den S3-Root-Benutzer nicht zum Managen von ONTAP-Objekt-Storage und zur gemeinsamen Nutzung seiner Berechtigungen verwenden, da er unbegrenzten Zugriff auf den Objektspeicher hat. Erstellen Sie stattdessen einen Benutzer oder eine Gruppe mit Administratorrechten, die Sie zuweisen.

        - Das Niveau der Servicequalität (Performance) ist das höchste für Ihr System verfügbare Niveau.
      - Klicken Sie auf **Speichern**, um einen Bucket mit diesen Standardwerten zu erstellen.

Konfigurieren Sie zusätzliche Berechtigungen und Einschränkungen

Sie können auf **Weitere Optionen** klicken, um Einstellungen für Objektsperrung, Benutzerberechtigungen und Leistungslevel zu konfigurieren, wenn Sie den Bucket konfigurieren, oder Sie können diese Einstellungen später ändern.

Wenn Sie beabsichtigen, den S3-Objektspeicher für FabricPool Tiering zu nutzen, sollten Sie die Wahl erwägen **für Tiering** zu verwenden (kostengünstige Medien mit optimaler Performance für die Tiered Data verwenden) anstatt ein Performance-Service-Level.

Wenn die Versionierung für einen Bucket aktiviert ist, kann die Aufbewahrungszeit für Objektsperren auf bestimmte Versionen eines Objekts über S3 Clients platziert werden. Das Sperren einer bestimmten Version eines Objekts verhindert nicht, dass andere Versionen des Objekts gelöscht werden. Wenn Sie die Versionierung für Ihre Objekte für eine spätere Wiederherstellung aktivieren möchten, wählen Sie **Versionierung aktivieren**. Die Versionierung ist standardmäßig aktiviert, wenn Sie die Objektsperrung auf dem Bucket aktivieren. Informationen zur Objektversionierung finden Sie im "Verwenden von Versionierung in S3 Buckets für Amazon".

Ab Version 9.14.1 wird die Objektsperrung in S3 Buckets unterstützt. Die S3-Objektsperre muss aktiviert sein, wenn ein Bucket erstellt wird. Objektsperre kann für bereits vorhandene Buckets nicht aktiviert werden. Object Lock kann nur in nativen S3-Anwendungsfällen verwendet werden. Multiprotokoll-NAS-Volumes, die für die Verwendung des S3-Protokolls konfiguriert werden, sollten SnapLock zum Übertragen von Daten in WORM-Storage verwenden. Für die S3 Objektsperrung ist eine standardmäßige SnapLock-Lizenz erforderlich. Diese

Lizenz ist in enthalten"ONTAP One".

Vor ONTAP One war die SnapLock-Lizenz im Paket für Sicherheit und Compliance enthalten. Das Paket „Sicherheit und Compliance“ wird nicht mehr angeboten, ist aber weiterhin gültig. Obwohl derzeit nicht erforderlich, können Bestandskunden wählen"Upgrade auf ONTAP One". Wenn Sie die Objektsperre für einen Bucket aktivieren, sollten Sie "Vergewissern Sie sich, dass eine SnapLock-Lizenz installiert ist" . Wenn keine SnapLock -Lizenz installiert ist, müssen Sie "Installieren" bevor Sie die Objektsperre aktivieren können.

Wenn Sie die Installation der SnapLock-Lizenz überprüft haben, wählen Sie **enable object locking** aus, um Objekte in Ihrem Bucket vor dem Löschen oder Überschreiben zu schützen. Die Sperrung kann entweder für alle oder für bestimmte Objektversionen aktiviert werden und nur dann, wenn die SnapLock-Compliance-Uhr für die Cluster-Nodes initialisiert wird. Führen Sie hierzu folgende Schritte aus:

1. Wenn die SnapLock-Compliance-Uhr auf keinem Knoten des Clusters initialisiert wird, wird die Schaltfläche **SnapLock-Compliance-Uhr initialisieren** angezeigt. Klicken Sie auf **SnapLock-Compliance-Uhr initialisieren**, um die SnapLock-Compliance-Uhr auf den Clusterknoten zu initialisieren.
2. Wählen Sie den Modus **Governance**, um eine zeitbasierte Sperre zu aktivieren, die *Write Once, Read Many (WORM)* Berechtigungen für die Objekte erlaubt. Selbst im *Governance*-Modus können die Objekte von Administratorbenutzern mit bestimmten Berechtigungen gelöscht werden.
3. Wählen Sie **Compliance**-Modus, wenn Sie strengere Regeln für die Löschung und Aktualisierung der Objekte zuweisen möchten. In diesem Modus der Objektsperrung können die Objekte nur nach Abschluss der angegebenen Aufbewahrungsfrist abgelaufen sein. Sofern keine Aufbewahrungsfrist festgelegt ist, bleiben die Objekte unbegrenzt gesperrt.
4. Geben Sie die Aufbewahrungsfrist für die Sperre in Tagen oder Jahren an, wenn die Verriegelung für einen bestimmten Zeitraum wirksam sein soll.

> Das Sperren gilt für S3-Buckets mit Versionsangabe und ohne Versionsangabe. Objektsperrung gilt nicht für NAS-Objekte.

Sie können Sicherungs- und Berechtigungseinstellungen sowie Performance Service Level für den Bucket konfigurieren.

> Sie müssen bereits Benutzer und Gruppen erstellt haben, bevor Sie die Berechtigungen konfigurieren.

Weitere Informationen finden Sie unter "Spiegelung für neuen Bucket erstellen".

Überprüfen Sie den Zugriff auf den Bucket

Für S3-Client-Applikationen (ob ONTAP S3 oder eine externe Drittanbieterapplikation) können Sie Ihren Zugriff auf den neu erstellten Bucket überprüfen, indem Sie Folgendes eingeben:

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

Vergrößern oder Verkleinern der ONTAP S3-Bucket-Größe

Bei Bedarf können Sie die Größe eines vorhandenen Buckets vergrößern oder verkleinern.

Schritte

Sie können System Manager oder die ONTAP-CLI zum Verwalten der Bucket-Größe verwenden.

System Manager

1. Wählen Sie **Speicher > Buckets** und suchen Sie den Bucket, den Sie ändern möchten.
2. Klicken Sie ⋮ neben dem Bucket-Namen und wählen Sie **Bearbeiten**.
3. Ändern Sie im Fenster **Edit bucket** die Kapazität für den Bucket.
4. **Speichern**.

CLI

1. Ändern der Bucket-Kapazität:

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

Erstellung eines ONTAP S3 Buckets auf einem gespiegelten oder nicht gespiegelten Aggregat in einer MetroCluster Konfiguration

Ab ONTAP 9.14.1 können Sie einen Bucket auf einem gespiegelten oder nicht gespiegelten Aggregat in MetroCluster FC- und IP-Konfigurationen bereitstellen.

Über diese Aufgabe

- Standardmäßig werden Buckets für gespiegelte Aggregate bereitgestellt.
- Die in beschriebenen Bereitstellungsrichtlinien "Erstellen eines Buckets"gelten für das Erstellen eines Buckets in einer MetroCluster Umgebung.
- Die folgenden S3-Objekt-Storage-Funktionen werden in MetroCluster Umgebungen **nicht** unterstützt:
  - SnapMirror S3
  - S3 Bucket-Lifecycle-Management
  - S3-Objektsperre im **Compliance**-Modus

    ⓘ S3-Objektsperre im **Governance**-Modus wird unterstützt.

  - Lokales FabricPool Tiering

Bevor Sie beginnen

Eine SVM, die einen S3-Server enthält, muss bereits vorhanden sein.

Erstellung von Buckets wird verarbeitet

CLI

1. Wenn Sie Aggregate und FlexGroup-Komponenten selbst auswählen möchten, legen Sie die Berechtigungsebene auf „Advanced“ fest (anderenfalls ist die Administratorberechtigungsebene ausreichend): `set -privilege advanced`
2. Erstellen eines Buckets:

   ```
   vserver object-store-server bucket create -vserver <svm_name> -bucket
   <bucket_name> [-size integer[KB|MB|GB|TB|PB]] [-use-mirrored-aggregates
   true/false]
   ```

   Legen Sie die `-use-mirrored-aggregates` Option auf `true` oder fest `false`, je nachdem, ob Sie ein gespiegeltes oder nicht gespiegeltes Aggregat verwenden möchten.

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

   - Der SVM-Name muss eine Daten-SVM sein.
   - Wenn Sie keine Optionen angeben, erstellt ONTAP einen Bucket mit 800 GB mit dem Service Level auf das höchste für das System verfügbare Level.
   - Wenn ONTAP einen Bucket auf Basis der Performance oder Auslastung erstellen soll, verwenden Sie eine der folgenden Optionen:
     - Service-Level

       Schließen Sie die `-storage-service-level` Option mit einem der folgenden Werte ein: `value`, `performance` Oder `extreme`.

     - tiering

       Schließen Sie die `-used-as-capacity-tier true` Option ein.
   - Wenn Sie die Aggregate angeben möchten, auf denen das zugrunde liegende FlexGroup Volume erstellt werden soll, verwenden Sie die folgenden Optionen:
     - Der `-aggr-list` Parameter gibt die Liste mit Aggregaten an, die für FlexGroup Volume-Komponenten verwendet werden sollen.

       Jeder Eintrag in der Liste erstellt eine Komponente im angegebenen Aggregat. Sie können ein Aggregat mehrmals angeben, damit mehrere Komponenten auf dem Aggregat erstellt werden.

   Für eine konsistente Performance im FlexGroup Volume müssen alle Aggregate denselben Festplattentyp und dieselbe Konfiguration der RAID-Gruppen verwenden.

   - Der `-aggr-list-multiplier` Parameter gibt die Anzahl der Wiederholungen über die Aggregate an, die `-aggr-list` beim Erstellen eines FlexGroup Volume mit dem Parameter aufgelistet sind.

     Der Standardwert des `-aggr-list-multiplier` Parameters ist 4.
3. Fügen Sie bei Bedarf eine QoS-Richtliniengruppe hinzu:

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

4. Überprüfen der Bucket-Erstellung:

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

Beispiel

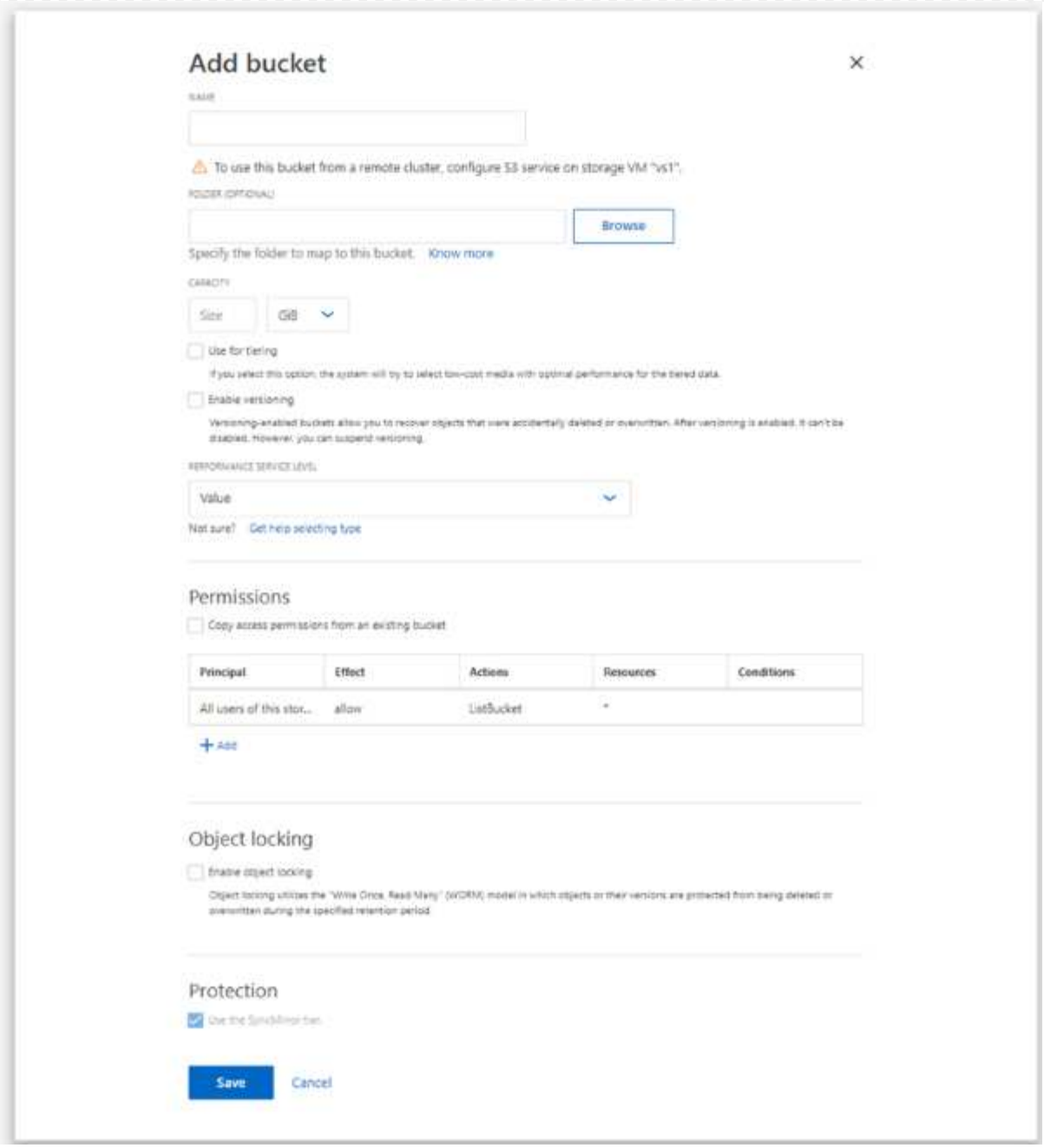
Im folgenden Beispiel wird ein Bucket für SVM vs1 mit der Größe 1 TB auf einem gespiegelten Aggregat erstellt:

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

System Manager

1. Fügen Sie auf einer S3-fähigen Storage-VM einen neuen Bucket hinzu.
   a. Klicken Sie auf **Storage > Buckets** und dann auf **Hinzufügen**.
   b. Geben Sie einen Namen ein, wählen Sie die Storage-VM aus und geben Sie eine Größe ein.

      Standardmäßig wird der Bucket auf einem gespiegelten Aggregat bereitgestellt. Wenn Sie einen Bucket auf einem nicht gespiegelten Aggregat erstellen möchten, wählen Sie **Weitere Optionen** und deaktivieren Sie das Kontrollkästchen **Use the SyncMirror Tier** unter **Schutz** wie im folgenden Bild gezeigt:



- Wenn Sie an dieser Stelle auf **Speichern** klicken, wird ein Bucket mit den folgenden Standardeinstellungen erstellt:
  - Benutzern wird kein Zugriff auf den Bucket gewährt, es sei denn, bereits Gruppenrichtlinien sind gültig.

    Sie sollten den S3-Root-Benutzer nicht zum Managen von ONTAP-Objekt-Storage und zur gemeinsamen Nutzung seiner Berechtigungen verwenden, da er unbegrenzten Zugriff auf den Objektspeicher hat. Erstellen Sie stattdessen einen Benutzer oder eine Gruppe mit Administratorrechten, die Sie zuweisen.

  - Das Niveau der Servicequalität (Performance) ist das höchste für Ihr System verfügbare Niveau.

- Sie können auf **Weitere Optionen** klicken, um Benutzerberechtigungen und Leistungslevel zu konfigurieren, wenn Sie den Bucket konfigurieren, oder Sie können diese Einstellungen später ändern.
  - Sie müssen bereits Benutzer und Gruppen erstellt haben, bevor Sie **Weitere Optionen** verwenden, um ihre Berechtigungen zu konfigurieren.
  - Wenn Sie beabsichtigen, den S3-Objektspeicher für FabricPool Tiering zu nutzen, sollten Sie die Wahl erwägen **für Tiering** zu verwenden (kostengünstige Medien mit optimaler Performance für die Tiered Data verwenden) anstatt ein Performance-Service-Level.

2. Überprüfen Sie bei S3-Client-Applikationen (einem anderen ONTAP-System oder einer externen Drittanbieterapplikation) den Zugriff auf den neuen Bucket, indem Sie Folgendes eingeben:
   - Das S3-Server-CA-Zertifikat.
   - Der Zugriffsschlüssel und der geheime Schlüssel des Benutzers.
   - Der FQDN-Name des S3-Servers und der Bucket-Name.

ONTAP S3-Bucket-Lifecycle-Management-Regel erstellen

Ab ONTAP 9.13.1 können Sie Lifecycle-Managementregeln erstellen, um Objekt-Lebenszyklen in Ihren S3 Buckets zu managen. Sie können Löschregeln für bestimmte Objekte in einem Bucket definieren und diese Bucket-Objekte durch diese Regeln ablaufen lassen. So können Sie Datenhaltungsanforderungen erfüllen und den gesamten S3 Objekt-Storage effizient managen.

Wenn die Objektsperrung für Ihre Bucket-Objekte aktiviert ist, werden die Lifecycle-Management-Regeln für die Objektablauffrist nicht auf gesperrte Objekte angewendet. Informationen zum Sperren von Objekten finden Sie unter "Erstellen eines Buckets".

Bevor Sie beginnen

- Eine S3-fähige SVM mit einem S3-Server und einem Bucket muss bereits vorhanden sein. Weitere Informationen finden Sie unter "Erstellung einer SVM für S3" .
- Die Regeln für das Bucket-Lifecycle-Management werden nicht unterstützt, wenn S3 in Multiprotokoll-NAS-Volumes oder S3 in MetroCluster-Konfigurationen verwendet werden.

Über diese Aufgabe

Beim Erstellen von Lifecycle-Management-Regeln können Sie die folgenden Löschaktionen auf Ihre Bucket-Objekte anwenden:

- Löschen aktueller Versionen – Diese Aktion läuft Objekte ab, die durch die Regel identifiziert werden. Wenn die Versionierung auf dem Bucket aktiviert ist, sind alle abgelaufenen Objekte in S3 nicht verfügbar. Wenn die Versionierung nicht aktiviert ist, werden die Objekte durch diese Regel dauerhaft gelöscht. Die CLI-Aktion lautet `Expiration`.
- Löschen nicht aktueller Versionen – Diese Aktion gibt an, wann S3 nicht aktuelle Objekte dauerhaft entfernen kann. Die CLI-Aktion lautet `NoncurrentVersionExpiration`.

Eine nicht aktuelle Version basiert auf der Erstellungszeit oder Änderungszeit der aktuellen Version. Das verzögerte Entfernen nicht aktueller Objekte kann hilfreich sein, wenn Sie versehentlich ein Objekt löschen oder überschreiben. Sie können beispielsweise eine Ablaufregel konfigurieren, um nicht aktuelle Versionen fünf Tage nach ihrer Nichtaktueller zu löschen. Nehmen wir beispielsweise an, dass Sie am 1/2014 um 10:30 UHR UTC ein Objekt mit dem Namen (Versions-ID `111111`) erstellen `photo.gif`. Am 2/2014 um 11:30 Uhr UTC löschen Sie versehentlich `photo.gif` (Versions-ID `111111`), wodurch eine Löschmarkierung mit einer neuen Versions-ID (z.B. Versions-ID) erstellt `4857693` wird. Sie haben nun fünf Tage Zeit, um die ursprüngliche Version von (Versions-ID `111111`) wiederherzustellen `photo.gif`, bevor die Löschung dauerhaft ist. Am 8/2014 um 00:00 UTC wird die Lebenszyklusregel für den Ablauf ausgeführt und dauerhaft gelöscht `photo.gif` (Versions-ID `111111`), fünf Tage nachdem sie zu einer nicht aktuellen Version wurde.

- Löschen abgelaufener Löschmarkierungen - Diese Aktion löscht abgelaufene Löschmarkierungen von Objekten. In versionierungsfähigen Buckets werden Objekte mit Löschmarkierungen zu den aktuellen Versionen der Objekte. Die Objekte werden nicht gelöscht, und es kann keine Aktion für sie ausgeführt werden. Diese Objekte sind abgelaufen, wenn ihnen keine aktuellen Versionen zugeordnet sind. Die CLI-Aktion lautet `Expiration`.
- Löschen von unvollständigen mehrteiligen Uploads: Mit dieser Aktion wird die maximale Zeit (in Tagen) festgelegt, die Sie zulassen möchten, dass mehrteilige Uploads noch ausgeführt werden. Danach werden sie gelöscht. Die CLI-Aktion lautet `AbortIncompleteMultipartUpload`.

Die Vorgehensweise, die Sie befolgen, hängt von der verwendeten Schnittstelle ab. Bei ONTAP 9.13,1 müssen Sie die CLI verwenden. Ab ONTAP 9.14.1 können Sie auch System Manager verwenden.

Verwalten Sie Lifecycle Management-Regeln mit der CLI

Ab ONTAP 9.13.1 können Sie über die ONTAP CLI Lifecycle-Managementregeln erstellen, um Objekte in Ihren S3 Buckets ablaufen zu lassen.

Bevor Sie beginnen

Für die CLI müssen Sie die erforderlichen Felder für jeden Ablaufaktionstyp definieren, wenn Sie eine Bucket-Lebenszyklusverwaltungsregel erstellen. Diese Felder können nach der ersten Erstellung geändert werden. In der folgenden Tabelle werden die eindeutigen Felder für jeden Aktionstyp angezeigt.

Aktionstyp	Eindeutige Felder
NichtCurrentVersionAblauf	• `-non-curr-days` - Anzahl der Tage, nach denen nicht aktuelle Versionen gelöscht werden • `-new-non-curr-versions` - Anzahl der neuesten nicht-aktuellen Versionen, die beibehalten werden sollen
Ablauf	• `-obj-age-days` - Anzahl der Tage seit der Erstellung, nach denen die aktuelle Version der Objekte gelöscht werden kann • `-obj-exp-date` - Bestimmtes Datum, wann die Objekte ablaufen sollen • `-expired-obj-del-markers` - Löschen von Objektmarkierungen

AbortInsetteMultipartUpload	• `-after-initiation-days` - Anzahl der Tage der Initiierung, nach denen der Upload abgebrochen werden kann

Damit die Bucket-Lifecycle-Management-Regel nur auf eine bestimmte Untergruppe von Objekten angewendet werden kann, 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 innerhalb des Buckets angewendet.

Alle Filter können nach der ersten Erstellung geändert werden *außer* für Folgendes: +

- `-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 Lifecycle Management-Regel zu erstellen.

Beispiel

Mit dem folgenden Befehl wird eine Lebenszyklusverwaltungsregel für den Bucket „NonCurrentVersionExpiration“ erstellt:

```
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

Mit dem folgenden Befehl wird eine Management-Regel für AblaufBucket-Lebenszyklus erstellt:

```
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

Mit dem folgenden Befehl wird eine AbortIncompleMultipartUpload Bucket Lifecycle Management-Regel erstellt:

```
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>
```

Managen Sie Lifecycle Management-Regeln mit System Manager

Ab ONTAP 9.14.1 können Sie S3 Objekte mit System Manager ablaufen lassen. Sie können Lifecycle-Management-Regeln für Ihre S3-Objekte hinzufügen, bearbeiten und löschen. Darüber hinaus können Sie eine für einen Bucket erstellte Lebenszyklusregel importieren und für Objekte in einem anderen Bucket verwenden. Sie können eine aktive Regel deaktivieren und später aktivieren.

Fügen Sie eine Lebenszyklusverwaltungsregel hinzu

1. Klicken Sie Auf **Speicher > Buckets**.
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. Klicken Sie auf **Hinzufügen > Lebenszyklusregel**.
5. Fügen Sie auf der Seite Lebenszyklusregel hinzufügen den Namen der Regel hinzu.
6. Definieren Sie den Geltungsbereich der Regel, unabhängig davon, ob sie auf alle Objekte im Bucket oder auf bestimmte Objekte angewendet werden soll. Wenn Sie Objekte angeben möchten, fügen Sie mindestens eines der folgenden Filterkriterien hinzu:
   a. Präfix: Geben Sie ein Präfix der Objektschlüsselnamen an, auf die die Regel angewendet werden soll. Normalerweise handelt es sich um den Pfad oder Ordner des Objekts. Sie können pro Regel ein Präfix eingeben. Sofern kein gültiges Präfix angegeben wird, gilt die Regel für alle Objekte in einem Bucket.
   b. Tags: Geben Sie bis zu drei Schlüssel- und Wertpaare (Tags) für die Objekte an, auf die die Regel angewendet werden soll. Zum Filtern werden nur gültige Schlüssel verwendet. Der Wert ist optional. Wenn Sie jedoch Werte hinzufügen, stellen Sie sicher, dass Sie nur gültige Werte für die entsprechenden Schlüssel hinzufügen.
   c. Größe: Sie können den Umfang zwischen der minimalen und maximalen Größe der Objekte begrenzen. Sie können einen oder beide Werte eingeben. Die Standardeinheit ist MiB.
7. Geben Sie die Aktion an:
   a. **Die aktuelle Version von Objekten ablaufen lassen**: Legen Sie eine Regel fest, um alle aktuellen Objekte nach einer bestimmten Anzahl von Tagen seit ihrer Erstellung oder an einem bestimmten Datum dauerhaft nicht mehr verfügbar zu machen. Diese Option ist nicht verfügbar, wenn die Option **Delete Expired object delete Markers** ausgewählt ist.
   b. **Nicht aktuelle Versionen dauerhaft löschen**: Geben Sie die Anzahl der Tage an, nach denen die nicht aktuelle Version gelöscht wird, und die Anzahl der zu haltenden Versionen.
   c. **Löschen abgelaufener Objektlösch-Marker**: Wählen Sie diese Aktion, um Objekte mit abgelaufenen Löschmarkierungen zu löschen, d.h. Marker ohne zugeordnetes aktuelles Objekt zu löschen.

Diese Option ist nicht mehr verfügbar, wenn Sie die Option **die aktuelle Version von Objekten ablaufen lassen** auswählen, die automatisch alle Objekte nach der Aufbewahrungsfrist löscht. Diese Option ist auch nicht mehr verfügbar, wenn Objekt-Tags zum Filtern verwendet werden.

d. **Unvollständige mehrteilige Uploads löschen**: Legen Sie die Anzahl der Tage fest, nach denen unvollständige mehrteilige Uploads gelöscht werden sollen. Wenn die mehrteiligen Uploads, die gerade ausgeführt werden, innerhalb der angegebenen Aufbewahrungsfrist fehlschlagen, können Sie die unvollständigen mehrteiligen Uploads löschen. Diese Option ist nicht mehr verfügbar, wenn Objekt-Tags zum Filtern verwendet werden.

e. Klicken Sie Auf **Speichern**.

Lebenszyklusregel importieren

1. Klicken Sie Auf **Speicher > Buckets**.
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. Klicken Sie auf **Hinzufügen > Regel importieren**.
5. Wählen Sie den Bucket aus, aus dem Sie die Regel importieren möchten. Die für den ausgewählten Bucket definierten Lifecycle-Management-Regeln werden angezeigt.
6. Wählen Sie die Regel aus, die Sie importieren möchten. Sie haben die Möglichkeit, jeweils eine Regel auszuwählen, wobei die Standardauswahl die erste Regel ist.
7. Klicken Sie Auf **Import**.

Bearbeiten, löschen oder deaktivieren Sie eine Regel

Sie können nur die Lifecycle-Management-Aktionen bearbeiten, die der Regel zugeordnet sind. Wenn die Regel mit Objekt-Tags gefiltert wurde, stehen die Optionen **abgelaufene Objekte löschen Marker** und **unvollständige mehrteilige Uploads löschen** nicht zur Verfügung.

Wenn Sie eine Regel löschen, gilt diese Regel nicht mehr für zuvor zugeordnete Objekte.

1. Klicken Sie Auf **Speicher > Buckets**.
2. Wählen Sie den Bucket aus, für den Sie die Lifecycle-Management-Regel bearbeiten, löschen oder deaktivieren möchten.
3. Klicken Sie auf das ⋮ Symbol und wählen Sie **Lebenszyklusregeln verwalten**.
4. Wählen Sie die gewünschte Regel aus. Sie können jeweils eine Regel bearbeiten und deaktivieren. Sie können mehrere Regeln auf einmal löschen.
5. Wählen Sie **Bearbeiten**, **Löschen** oder **Deaktivieren**, und schließen Sie das Verfahren ab.

Erstellen Sie einen ONTAP S3-Benutzer

Erstellen eines S3-Benutzers mit bestimmten Berechtigungen. Für alle ONTAP-Objektspeicher ist eine Benutzerautorisierung erforderlich, um die Konnektivität zu autorisierten Clients einzuschränken.

Bevor Sie beginnen.

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

Über diese Aufgabe

Ein S3-Benutzer kann Zugriff auf jeden Bucket in einer Storage-VM erhalten. Wenn Sie einen S3-Benutzer erstellen, werden auch ein Zugriffsschlüssel und ein geheimer Schlüssel für den Benutzer generiert. Sie sollten zusammen mit dem FQDN des Objektspeichers und dem Bucket-Namen für den Benutzer freigegeben werden.

Aus Sicherheitsgründen werden ab ONTAP 9.15.1 Zugriffsschlüssel und geheime Schlüssel nur zum Zeitpunkt der Erstellung des S3-Benutzers angezeigt und können nicht mehr angezeigt werden. Wenn die Schlüssel verloren gehen, "Neue Schlüssel müssen neu generiert werden".

Sie können S3 Benutzern in einer Bucket-Richtlinie oder einer Objekt-Server-Richtlinie spezifische Zugriffsberechtigungen zuweisen.

Wenn Sie einen neuen Objektspeicher-Server erstellen, erstellt ONTAP einen Root-Benutzer (UID 0), ein privilegierter Benutzer mit Zugriff auf alle Buckets. Anstatt ONTAP S3 als Root-Benutzer zu verwalten, empfiehlt NetApp, eine Admin-Benutzerrolle mit bestimmten Berechtigungen zu erstellen.

CLI

1. 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 können Sie den Zeitraum definieren `-key-time-to-live`, für den der Schlüssel im Parameter gültig sein soll. Sie können die Aufbewahrungsfrist in diesem Format hinzufügen, um den Zeitraum anzugeben, nach dem der Zugriffsschlüssel abläuft: `P[<integer>D]T[<integer>H][<integer>M][<integer>S] | P<integer>W` Wenn Sie beispielsweise eine Aufbewahrungsfrist von einem Tag, zwei Stunden, drei Minuten und vier Sekunden eingeben möchten, geben Sie den Wert als ein `P1DT2H3M4S`. Sofern nicht angegeben, ist der Schlüssel für einen unbestimmten Zeitraum gültig.

     Das folgende Beispiel erstellt einen Benutzer mit Namen `sm_user1` auf Storage VM `vs0`, mit einem Schlüssel Aufbewahrungszeitraum von einer Woche.

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

2. Achten Sie darauf, den Zugriffsschlüssel und den geheimen Schlüssel zu speichern. Sie werden für den Zugriff von S3-Clients benötigt.

System Manager

1. Klicken Sie auf **Storage > Storage VMs**. Wählen Sie die Speicher-VM aus, zu der Sie einen Benutzer hinzufügen möchten, wählen Sie **Einstellungen** und klicken Sie dann ✎ unter S3.
2. Um einen Benutzer hinzuzufügen, klicken Sie auf **Benutzer > Hinzufügen**.
3. Geben Sie einen Namen für den Benutzer ein.
4. Ab ONTAP 9.14.1 können Sie den Aufbewahrungszeitraum der Zugriffsschlüssel festlegen, die für den Benutzer erstellt werden. Sie können den Aufbewahrungszeitraum in Tagen, Stunden, Minuten oder Sekunden angeben, nach denen die Schlüssel automatisch ablaufen. Standardmäßig wird der Wert auf festgelegt `0`, der angibt, dass der Schlüssel unbegrenzt gültig ist.
5. Klicken Sie Auf **Speichern**. Der Benutzer wird erstellt, und ein Zugriffsschlüssel und ein geheimer Schlüssel werden für den Benutzer generiert.
6. Laden Sie den Zugriffsschlüssel und den geheimen Schlüssel herunter, oder speichern Sie ihn. Sie werden für den Zugriff von S3-Clients benötigt.

Nächste Schritte

- Erstellen oder Ändern von S3-Gruppen

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

Sie können den Bucket-Zugriff vereinfachen, indem Sie Benutzergruppen mit entsprechenden Zugriffsberechtigungen erstellen.

Bevor Sie beginnen

S3-Benutzer in einer S3-fähigen SVM müssen bereits vorhanden sein.

Über diese Aufgabe

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

- Auf Bucket-Ebene

  Nachdem Sie eine Gruppe von S3-Benutzern erstellt haben, geben Sie in den Bucket-Richtlinienerklärungen Gruppenberechtigungen an, die nur auf diesen Bucket angewendet werden.

- Auf SVM-Ebene

  Nach dem Erstellen einer Gruppe von S3-Benutzern geben Sie in der Gruppendefinition die Namen der Objektserverrichtlinien an. Diese Richtlinien bestimmen die Buckets und den Zugriff für die Gruppenmitglieder.

System Manager

1. Bearbeiten Sie die Speicher-VM: Klicken Sie auf **Speicher > Speicher-VMs**, klicken Sie auf die Speicher-VM, klicken Sie auf **Einstellungen** und dann ✎ unter S3.
2. Fügen Sie eine Gruppe hinzu: Wählen Sie **Gruppen** und dann **Hinzufügen**.
3. Geben Sie einen Gruppennamen ein, und wählen Sie aus einer Benutzerliste aus.
4. Sie können eine vorhandene Gruppenrichtlinie auswählen oder eine jetzt hinzufügen oder später eine Richtlinie hinzufügen.

CLI

1. Erstellen einer 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 Richtlinien für Objekt-Storage-Server erstellt wurden.

Regenerieren Sie ONTAP S3-Schlüssel und ändern Sie deren Aufbewahrungsdauer

Zugriffsschlüssel und geheime Schlüssel werden automatisch während der Erstellung von Benutzern generiert, um den S3-Client-Zugriff zu ermöglichen. Sie können Schlüssel für einen Benutzer neu generieren, wenn ein Schlüssel abgelaufen ist oder kompromittiert wurde.

Informationen zur Generierung von Zugriffsschlüsseln finden Sie unter "Erstellen eines S3-Benutzers".

System Manager

1. Klicken Sie auf **Storage > Storage VMs** und wählen Sie dann die Speicher-VM aus.
2. Klicken Sie im Register **Einstellungen** auf die Kachel **S3**.
3. Überprüfen Sie auf der Registerkarte **Users**, ob kein Zugriffsschlüssel vorhanden ist oder der Schlüssel für den Benutzer abgelaufen ist.
4. Wenn Sie den Schlüssel neu generieren müssen, klicken Sie neben dem Benutzer auf **Schlüssel neu generieren**.
5. Generierte Schlüssel sind standardmäßig für eine unbestimmte Zeit gültig. Ab 9.14.1 können Sie die Aufbewahrungsfrist ändern, nach der die Schlüssel automatisch ablaufen. Geben Sie den Aufbewahrungszeitraum in Tagen, Stunden, Minuten oder Sekunden ein.
6. Klicken Sie Auf **Speichern**. Der Schlüssel wird neu generiert. Jede Änderung der Schlüsselaufbewahrungsfrist tritt unmittelbar in Kraft.
7. Laden Sie den Zugriffsschlüssel und den geheimen Schlüssel herunter, oder speichern Sie ihn. Sie werden für den Zugriff von S3-Clients benötigt.

CLI

1. Regenerieren Sie Zugriff und geheime Schlüssel für einen Benutzer `vserver object-store-server user regenerate-keys`, indem Sie den Befehl ausführen.
2. Generierte Schlüssel sind standardmäßig für unbegrenzte Zeit gültig. Ab 9.14.1 können Sie die Aufbewahrungsfrist ändern, nach der die Schlüssel automatisch ablaufen. Sie können den Aufbewahrungszeitraum in diesem Format hinzufügen: `P[<integer>D]T[<integer>H][<integer>M][<integer>S] | P<integer>W` Wenn Sie beispielsweise einen Aufbewahrungszeitraum von einem Tag, zwei Stunden, drei Minuten und vier Sekunden eingeben möchten, geben Sie den Wert als ein `P1DT2H3M4S`.

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

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

Erstellen oder Ändern von Zugriffsrichtlinien-Anweisungen

Informieren Sie sich über ONTAP S3 Bucket und Objektspeicher-Server-Richtlinien

Benutzer- und Gruppenzugriff auf S3-Ressourcen wird über Bucket- und Objektspeicher-Serverrichtlinien gesteuert. Wenn Sie eine kleine Anzahl von Benutzern oder Gruppen haben, ist die Kontrolle des Zugriffs auf Bucket-Ebene wahrscheinlich ausreichend, aber wenn Sie viele Benutzer und Gruppen haben, ist es einfacher, den Zugriff auf der Objektspeicherserverebene zu steuern.

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

Zugriffsregeln können zur Standard-Bucket-Richtlinie hinzugefügt werden. Der Umfang seiner Zugriffssteuerung umfasst den Bucket, der im EinzelBucket enthalten ist, daher ist

er am besten geeignet.

Bevor Sie beginnen

Eine S3-fähige Storage-VM muss bereits vorhanden sein, die einen S3-Server und einen Bucket enthält.

Sie müssen bereits Benutzer oder Gruppen erstellt haben, bevor Sie Berechtigungen erteilen.

Über diese Aufgabe

Sie können neue Anweisungen für neue Benutzer und Gruppen hinzufügen oder die Attribute vorhandener Anweisungen ändern. Erfahren Sie mehr über `vserver object-store-server bucket policy` in der "ONTAP-Befehlsreferenz".

Benutzer- und Gruppenberechtigungen können bei Erstellung des Buckets oder nach Bedarf später zugewiesen werden. Sie können auch die Bucket-Kapazität und die QoS-Richtliniengruppenzuweisung ändern.

Wenn Sie ab ONTAP 9.9.1 die Objekt-Tagging-Funktionalität des AWS-Clients mit dem ONTAP S3-Server unterstützen möchten, `GetObjectTagging` `PutObjectTagging` `DeleteObjectTagging` müssen die Aktionen, und über die Bucket- oder Gruppenrichtlinien erlaubt sein.

Die folgende Vorgehensweise ist abhängig von der Schnittstelle, die Sie --System Manager oder die CLI verwenden:

System Manager

Schritte

1. Bearbeiten Sie den Bucket: Klicken Sie auf **Storage > Buckets**, klicken Sie auf den gewünschten Bucket und klicken Sie dann auf **Bearbeiten**. Beim Hinzufügen oder Ändern von Berechtigungen können Sie die folgenden Parameter angeben:
   - **Auftraggeber**: Der Benutzer oder die Gruppe, auf die der Zugriff gewährt wird.
   - **Effekt**: Erlaubt oder verweigert den Zugriff auf einen Benutzer oder eine Gruppe.
   - **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. Sie können auch Zugriff auf einzelne Objekte gewähren, z. B. ***buchketname/*_readme.txt**.
   - **Bedingungen** (optional): Ausdrücke, die beim Versuch des Zugriffs ausgewertet werden. Sie können beispielsweise eine Liste mit IP-Adressen angeben, für die der Zugriff zulässig oder verweigert wird.

> Ab ONTAP 9.14.1 können Sie Variablen für die Bucket-Richtlinie im Feld **Ressourcen** angeben. Diese Variablen sind Platzhalter, die bei der Bewertung der Richtlinie durch kontextbezogene Werte ersetzt werden. Beispiel: Wenn `${aws:username}` als Variable für eine Richtlinie angegeben ist, wird diese Variable durch den Benutzernamen für den Anforderungskontext ersetzt, und die Richtlinienaktion kann wie für diesen Benutzer konfiguriert ausgeführt werden.

CLI

Schritte

1. Hinzufügen einer Anweisung zu einer Bucket-Richtlinie:

```
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 Zugriffsberechtigungen:

`-effect`	Die Anweisung kann den Zugriff erlauben oder verweigern
`-action`	Sie können festlegen `*`, dass alle Aktionen oder eine Liste mit einer oder mehreren der folgenden Aktionen gemeint sind: `GetObject, PutObject, DeleteObject, ListBucket, GetBucketAcl,GetObjectAcl, ListBucketMultipartUploads,` Und `ListMultipartUploadParts`.

`-principal`	Eine Liste mit einem oder mehreren S3-Benutzern oder -Gruppen. • Es können maximal 10 Benutzer oder Gruppen angegeben werden. • Wenn eine S3-Gruppe angegeben wird, muss sie sich im Formular befinden `group/group_name`. • `*` Kann angegeben werden, um öffentlichen Zugriff zu bedeuten, d. h. Zugriff ohne Zugriffsschlüssel und geheimen Schlüssel. • Wenn kein Principal angegeben wird, werden allen S3-Benutzern in der Storage-VM Zugriff gewährt.
`-resource`	Den Bucket und jedes darin enthaltene Objekt. Die Platzhalterzeichen `*` und `?` können verwendet werden, um einen regulären Ausdruck für die Angabe einer Ressource zu bilden. Für eine Ressource können Sie Variablen in einer Richtlinie angeben. Bei diesen Richtlinienvariablen handelt es sich um Platzhalter, die bei der Bewertung der Richtlinie durch die Kontextwerte ersetzt werden.

Mit der `-sid` Option können Sie optional einen Text-String als Kommentar angeben.

Beispiele

Im folgenden Beispiel wird eine Bucket-Policy-Anweisung für den Objektspeicher-Server für die Storage-VM svm1.example.com und bucket1 erstellt, die den zulässigen Zugriff auf einen Readme-Ordner für den Objektspeicher-Server-Benutzer Benutzer1 angibt.

```
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"
```

Im folgenden Beispiel wird eine Bucket-Policy-Anweisung für den Objektspeicher-Server für die Storage-VM svm1.example.com und bucket1 erstellt, die den erlaubten Zugriff auf alle Objekte für die Objektspeicher-Servergruppe1 angibt.

```
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 9.14.1 können Sie Variablen für eine Bucket-Richtlinie angeben. Im folgenden Beispiel wird eine Policy-Anweisung für Server-Buckets für die Storage-VM `svm1` und `bucket1` erstellt und `${aws:username}` als Variable für eine Policy-Ressource angegeben. Wenn die Richtlinie ausgewertet wird, wird die Richtlinienvariable durch den Benutzernamen für den Anforderungskontext ersetzt, und die Richtlinienaktion kann wie für diesen Benutzer konfiguriert ausgeführt werden. Wenn beispielsweise die folgende Richtlinienanweisung bewertet wird, `${aws:username}` wird sie durch den Benutzer ersetzt, der den S3-Vorgang ausführt. Wenn ein Benutzer `user1` den Vorgang durchführt, erhält dieser Benutzer

Zugriff auf `bucket1` AS `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 sich auf einen oder mehrere Buckets in einem Objektspeicher anwenden lassen. Serverrichtlinien für Objektspeicher können an Gruppen von Benutzern angehängt werden, wodurch das Management des Datenzugriffs über mehrere Buckets hinweg vereinfacht wird.

Bevor Sie beginnen

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

Über diese Aufgabe

Sie können die Zugriffsrichtlinien auf der SVM-Ebene aktivieren, indem Sie eine standardmäßige oder benutzerdefinierte Richtlinie in einer Objekt-Storage-Servergruppe angeben. Die Richtlinien werden erst wirksam, wenn sie in der Gruppendefinition angegeben sind.

> Wenn Sie die Objekt-Storage-Server-Richtlinien verwenden, geben Sie Principals (d. h. Benutzer und Gruppen) in der Gruppendefinition und nicht in der Richtlinie selbst an.

Es gibt drei schreibgeschützte Standardrichtlinien für den Zugriff auf ONTAP S3-Ressourcen:

- Vollzugriff
- NoS3Access
- ReadOnlyAccess

Sie können auch neue benutzerdefinierte Richtlinien erstellen, neue Anweisungen für neue Benutzer und Gruppen hinzufügen oder die Attribute vorhandener Anweisungen ändern. Erfahren Sie mehr über `vserver object-store-server policy` in der "ONTAP-Befehlsreferenz".

Wenn Sie ab ONTAP 9.9.1 die Objekt-Tagging-Funktionalität des AWS-Clients mit dem ONTAP S3-Server unterstützen möchten, `GetObjectTagging` `PutObjectTagging` `DeleteObjectTagging` müssen die Aktionen, und über die Bucket- oder Gruppenrichtlinien erlaubt sein.

Die folgende Vorgehensweise ist abhängig von der Schnittstelle, die Sie --System Manager oder die CLI verwenden:

System Manager

Verwenden Sie System Manager zum Erstellen oder Ändern einer Objektspeicherserverrichtlinie

Schritte

1. Bearbeiten Sie die Speicher-VM: Klicken Sie auf **Speicher > Speicher-VMs**, klicken Sie auf die Speicher-VM, klicken Sie auf **Einstellungen** und dann ✎ unter S3.
2. Fügen Sie einen Benutzer hinzu: Klicken Sie auf **Richtlinien** und dann auf **Hinzufügen**.
   a. Geben Sie einen Richtliniennamen ein, und wählen Sie ihn aus einer Gruppenliste aus.
   b. Wählen Sie eine vorhandene Standardrichtlinie aus, oder fügen Sie eine neue hinzu.

      Beim Hinzufügen oder Ändern einer Gruppenrichtlinie können Sie die folgenden Parameter angeben:

      - Gruppe: Die Gruppen, denen der Zugriff gewährt wird.
      - Effekt: Ermöglicht 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 Zugang zu allen Objekten in einem bestimmten Bucket.
        - **Bucketname/readme.txt** gewährt Zugriff auf ein Objekt in einem bestimmten Bucket.
   c. Fügen Sie gegebenenfalls Anweisungen zu bestehenden Richtlinien hinzu.

CLI

Verwenden Sie die CLI, um eine Objekt-Store-Serverrichtlinie zu erstellen oder zu ändern

Schritte

1. Objekt-Storage-Server-Richtlinie erstellen:

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

2. Erstellen einer Anweisung für die Richtlinie:

   ```
   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 Zugriffsberechtigungen:

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

`-action`	Sie können festlegen `*`, dass alle Aktionen oder eine Liste mit einer oder mehreren der folgenden Aktionen gemeint sind: `GetObject, PutObject, DeleteObject, ListBucket,GetBucketAcl, GetObjectAcl, ListAllMyBuckets, ListBucketMultipartUploads`, Und `ListMultipartUploadParts`.
`-resource`	Den Bucket und jedes darin enthaltene Objekt. Die Platzhalterzeichen `*` und `?` können verwendet werden, um einen regulären Ausdruck für die Angabe einer Ressource zu bilden.

Mit der `-sid` Option können Sie optional einen Text-String als Kommentar angeben.

Standardmäßig werden am Ende der Liste der Anweisungen neue Anweisungen hinzugefügt, die in der Reihenfolge bearbeitet werden. Wenn Sie später Anweisungen hinzufügen oder ändern, haben Sie die Möglichkeit, die `-index` Einstellung der Anweisung zu ändern, um die Verarbeitungsreihenfolge zu ändern.

Erfahren Sie mehr über die in diesem Verfahren beschriebenen Befehle im "ONTAP-Befehlsreferenz".

Konfigurieren Sie externe Verzeichnisdienste für ONTAP S3-Zugriff

Ab ONTAP 9.14.1 sind Services für externe Verzeichnisse in ONTAP S3 Objekt-Storage integriert. Diese Integration vereinfacht die Benutzer- und Zugriffsverwaltung durch externe Verzeichnisdienste.

Sie können Benutzergruppen, die zu einem externen Verzeichnisdienst gehören, mit Zugriff auf Ihre ONTAP Objekt-Storage-Umgebung versehen. 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. Für den Zugriff müssen Sie LDAP-Gruppen in Ihrer ONTAP S3-Umgebung konfigurieren. Nachdem Sie den Zugriff konfiguriert haben, haben die Gruppenmitglieder Berechtigungen für ONTAP S3 Buckets. Informationen zu LDAP finden Sie unter "Erfahren Sie mehr über die Verwendung von LDAP-Namensdiensten auf ONTAP NFS SVMs".

Sie können auch Active Directory-Benutzergruppen für den schnellen Bindungsmodus konfigurieren, sodass die Anmeldeinformationen von Benutzern validiert und S3-Anwendungen von Drittanbietern und Open-Source-Anwendungen über LDAP-Verbindungen authentifiziert werden können.

Bevor Sie beginnen

Stellen Sie vor der Konfiguration von LDAP-Gruppen und der Aktivierung des fast-Bind-Modus für den Gruppenzugriff Folgendes sicher:

1. Es wurde eine S3-fähige Storage-VM erstellt, die einen S3-Server enthält. Siehe "Erstellung einer SVM für S3".
2. In dieser Storage-VM wurde ein Bucket erstellt. Siehe "Erstellen eines Buckets".
3. DNS ist auf der Storage-VM konfiguriert. Siehe "Konfigurieren Sie DNS-Dienste".

4. Auf der Storage-VM wird ein selbstsigniertes CA-Zertifikat (Root Certification Authority) des LDAP-Servers installiert. Siehe "Installieren Sie selbstsignierte Stamm-CA-Zertifikate auf der SVM".
5. Ein LDAP-Client wird mit TLS auf der SVM konfiguriert. Siehe "Erstellen Sie LDAP-Clientkonfigurationen für den ONTAP NFS-Zugriff" und "Verknüpfen Sie LDAP-Clientkonfigurationen mit ONTAP NFS SVMs für Informationen".

Konfigurieren Sie den S3-Zugriff für LDAP

1. Geben Sie LDAP als *Name Service-Datenbank* der SVM für die Gruppe und Passwort für LDAP an:

```
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 Link:https://docs.NetApp.com/US-en/ONTAP-cli/vserver-services-name-service-ns-switch-modify.html^] finden[`vserver services name-service ns-switch modify` Sie in der ONTAP-Befehlsreferenz.

2. Erstellen Sie eine Objektspeicher-Bucket-Policy-Anweisung mit der `principal` Einstellung auf die LDAP-Gruppe, der Sie Zugriff gewähren möchten:

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

Beispiel: Im folgenden Beispiel wird eine Bucket Policy-Anweisung für erstellt `buck1`. Die Richtlinie ermöglicht den Zugriff der LDAP-Gruppe `group1` auf die Ressource (Bucket und deren 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. Vergewissern Sie sich, dass ein Benutzer der LDAP-Gruppe `group1` S3-Vorgänge vom S3-Client ausführen kann.

Verwenden Sie für die Authentifizierung den LDAP-F.A.S.T. Bind-Modus

1. Geben Sie LDAP als *Name Service-Datenbank* der SVM für die Gruppe und Passwort für LDAP an:

```
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 Link:https://docs.NetApp.com/US-en/ONTAP-cli/vserver-services-name-service-ns-switch-modify.html^] finden[`vserver services name-service ns-switch modify` Sie in der ONTAP-Befehlsreferenz.

2. Stellen Sie sicher, dass für einen LDAP-Benutzer, der auf den S3-Bucket zugreift, in den Bucket-Richtlinien definierte Berechtigungen gelten. Weitere Informationen finden Sie unter "Ändern einer Bucket-Richtlinie".
3. Überprüfen Sie, ob ein Benutzer aus der LDAP-Gruppe die folgenden Vorgänge ausführen kann:
   a. Konfigurieren Sie den Zugriffsschlüssel auf dem S3-Client in diesem Format: `"NTAPFASTBIND" + base64-encode(user-name:password)` Beispiel: `"NTAPFASTBIND"` + base64-encode(ldapuser:password), was dazu führt `NTAPFASTBINDbGRhcHVzZXI6cGFzc3dvcmQ=`

      > Der S3-Client fordert möglicherweise einen geheimen Schlüssel an. In Ermangelung eines geheimen Schlüssels kann ein Passwort mit mindestens 16 Zeichen eingegeben werden.

   b. Führen Sie grundlegende S3-Vorgänge über den S3-Client durch, für den der Benutzer Berechtigungen besitzt.

Base64-Anmeldeinformationen

Die Standardkonfiguration von ONTAP S3 schließt HTTP aus und verwendet ausschließlich HTTPS und eine TLS-Verbindung (Transport Layer Security). ONTAP kann selbstsignierte Zertifikate generieren, als Best Practice wird jedoch empfohlen, Zertifikate von einer Drittanbieter-Zertifizierungsstelle zu verwenden. Wenn Sie CA-Zertifikate verwenden, erstellen Sie eine vertrauenswürdige Beziehung zwischen Client-Anwendungen und dem ONTAP-Objektspeicher-Server.

Beachten Sie, dass Anmeldeinformationen, die mit Base64 kodiert werden, leicht decodiert werden. Mit HTTPS werden verschlüsselte Anmeldeinformationen von man-in-the-Middle-Paketabfragern nicht erfasst.

Verwenden Sie beim Erstellen vorsignierter URLs keinen LDAP-Fast-Bind-Modus zur Authentifizierung. Die Authentifizierung basiert ausschließlich auf dem Base64-Zugriffsschlüssel, der in der vorsignierten URL enthalten ist. Der Benutzername und das Passwort werden jedem angezeigt, der den Base64-Zugriffsschlüssel decodiert.

Authentifizierungsmethode 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"}
```

Leiten Sie die API an die Cluster-Management-LIF weiter, nicht an die Daten-LIF der SVM. Wenn Sie Benutzern erlauben möchten, eigene Schlüssel zu generieren, müssen Sie ihrer Rolle HTTP-Berechtigungen hinzufügen, um Curl zu verwenden. Diese Berechtigung wird zusätzlich zu den S3-API-Berechtigungen gewährt.

Konfigurieren des S3-Zugriffs für Active Directory- oder SMB-Server

Wenn die in der Bucket-Policy-Anweisung angegebene nasgroup oder die Benutzer, die Teil der nasgroup sind, keine UID und keine GID festgelegt haben, schlagen die Suchen fehl, wenn diese Attribute nicht gefunden werden. Active Directory verwendet SID, nicht UID. Wenn SID-Einträge nicht der UID zugeordnet werden können, müssen die erforderlichen Daten an ONTAP übertragen werden.

Verwenden Sie dazu, "Erstellung von vserver Active Directory"damit sich die SVM bei Active Directory authentifizieren kann und die erforderlichen Benutzer- und Gruppeninformationen abrufen kann.

Alternativ können Sie verwenden"cifs vserver erstellen", um einen SMB-Server in einer Active Directory-Domäne zu erstellen.

Wenn Sie unterschiedliche Domänennamen für Nameserver und Objektspeicher verwenden, kann es zu Suchfehlern kommen. Um Suchfehler zu vermeiden, empfiehlt NetApp die Verwendung vertrauenswürdiger Domänen für die Ressourcenautorisierung im UPN-Format: `nasgroup/group@trusted_domain.com` Vertrauenswürdige Domänen sind diejenigen, die der Liste der vertrauenswürdigen Domänen des SMB-Servers hinzugefügt wurden. Erfahren Sie, wie Sie "bevorzugte vertrauenswürdige Domänen hinzufügen, entfernen und ändern" in der SMB-Serverliste.

Generieren Sie Schlüssel, wenn die Authentifizierungsmethode Domain ist und vertrauenswürdige Domänen in Active Directory konfiguriert sind

Verwenden Sie den `s3/services/<svm_uuid>/users` Endpunkt mit Benutzern, die im UPN-Format angegeben sind. 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"}
```

Leiten Sie die API an die Cluster-Management-LIF weiter, nicht an die Daten-LIF der SVM. Wenn Sie Benutzern erlauben möchten, eigene Schlüssel zu generieren, müssen Sie ihrer Rolle HTTP-Berechtigungen hinzufügen, um Curl zu verwenden. Diese Berechtigung wird zusätzlich zu den S3-API-Berechtigungen gewährt.

Generieren Sie Schlüssel, wenn die Authentifizierungsmethode Domain ist und keine vertrauenswürdigen Domänen vorhanden sind

Diese Aktion ist möglich, wenn LDAP deaktiviert ist oder 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"}
```

Leiten Sie die API an die Cluster-Management-LIF weiter, nicht an die Daten-LIF der SVM. Wenn Sie Benutzern erlauben möchten, eigene Schlüssel zu generieren, müssen Sie ihrer Rolle HTTP-Berechtigungen hinzufügen, um Curl zu verwenden. Diese Berechtigung wird zusätzlich zu den S3-API-Berechtigungen gewährt. Sie müssen einem Benutzernamen nur den optionalen Domänenwert (@fqdn) hinzufügen, wenn keine vertrauenswürdigen Domänen vorhanden sind.

Ermöglichen Sie LDAP- oder Domänenbenutzern, ihre eigenen ONTAP S3-Zugriffsschlüssel zu generieren

Ab ONTAP 9.14.1 können Sie als ONTAP-Administrator benutzerdefinierte Rollen erstellen und sie lokalen oder Domänengruppen oder LDAP-Gruppen (Lightweight Directory Access Protocol) zuweisen, sodass die Benutzer dieser Gruppen ihren eigenen Zugriff und geheime Schlüssel für den S3-Clientzugriff generieren können.

Sie müssen für die Storage-VM einige Konfigurationsschritte durchführen, um die benutzerdefinierte Rolle zu erstellen und dem Benutzer zuzuweisen, der die API zur Schlüsselgenerierung nach dem Zugriff aktiviert.

Wenn LDAP deaktiviert ist, können Sie "Konfigurieren externer Verzeichnisdienste für den ONTAP S3-Zugriff" um Benutzern das Generieren von Zugriffsschlüsseln zu ermöglichen.

Bevor Sie beginnen

Stellen Sie Folgendes sicher:

1. Es wurde eine S3-fähige Storage-VM erstellt, die einen S3-Server enthält. Siehe "Erstellung einer SVM für S3".
2. In dieser Storage-VM wurde ein Bucket erstellt. Siehe "Erstellen eines Buckets".
3. DNS ist auf der Storage-VM konfiguriert. Siehe "Konfigurieren Sie DNS-Dienste".
4. Auf der Storage-VM wird ein selbstsigniertes CA-Zertifikat (Root Certification Authority) des LDAP-Servers installiert. Siehe "Installieren Sie selbstsignierte Stamm-CA-Zertifikate auf der SVM".
5. Ein LDAP-Client wird auf der Storage-VM mit aktiviertem TLS konfiguriert. Siehe "Erstellen Sie LDAP-Clientkonfigurationen für den ONTAP NFS-Zugriff".
6. Verknüpfen Sie die Client-Konfiguration mit dem Vserver. Siehe "LDAP-Clientkonfigurationen mit ONTAP NFS SVMs verknüpfen". Erfahren Sie mehr über `vserver services name-service ldap create` in der "ONTAP-Befehlsreferenz".
7. Wenn Sie eine Storage-VM verwenden, erstellen Sie eine Management-Netzwerkschnittstelle (LIF) und auf der VM, und außerdem eine Service-Richtlinie für die LIF. Erfahren Sie mehr über `network interface create` und `network interface service-policy create` in der "ONTAP-Befehlsreferenz".

Konfigurieren Sie Benutzer für die Generierung des Zugriffsschlüssels

Beispiel 3. Schritte

LDAP-Benutzer

1. Geben Sie LDAP als *Name Service Database* der Speicher-VM für die Gruppe und Passwort für LDAP an:

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

   Erfahren Sie mehr über `vserver services name-service ns-switch modify` in der "ONTAP-Befehlsreferenz".

2. Benutzerdefinierte Rolle mit Zugriff auf den REST-API-Endpunkt des S3-Benutzers 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 `s3-role` wird die Rolle für Benutzer auf der Storage-VM generiert `svm-1`, 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
```

   Erfahren Sie mehr über `security login rest-role create` in der "ONTAP-Befehlsreferenz".

3. Erstellen Sie eine LDAP-Benutzergruppe mit dem `security login` und fügen Sie die neue benutzerdefinierte Rolle für den Zugriff auf den REST-API-Endpunkt des S3-Benutzers hinzu. Erfahren Sie mehr über `security login create` im "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 `ldap-group-1` wird die LDAP-Gruppe in erstellt `svm-1`, und die benutzerdefinierte Rolle `s3role` wird ihr für den Zugriff auf den API-Endpunkt hinzugefügt, zusammen mit der Aktivierung des LDAP-Zugriffs im Modus „Fast BIND“.

```
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 Sie unter "Verwenden Sie LDAP Fast Bind für die NSswitch-Authentifizierung für ONTAP NFS SVMs".

Erfahren Sie mehr über `security login create` in der "ONTAP-Befehlsreferenz".

Das Hinzufügen der benutzerdefinierten Rolle zur LDAP-Gruppe ermöglicht Benutzern in dieser Gruppe einen eingeschränkten Zugriff auf die ONTAP `/api/protocols/s3/services/{svm.uuid}/users` Endpunkt. Durch Aufrufen der API können die LDAP-Gruppenbenutzer ihre eigenen Zugriffs- und Geheimschlüssel für den Zugriff auf den S3-Client generieren. Sie können die Schlüssel nur für sich selbst und nicht für andere Benutzer generieren.

Domänenbenutzer

1. Erstellen Sie eine benutzerdefinierte 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 `s3-role` Rolle wird für Benutzer auf der Speicher-VM generiert `svm-1` , dem 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
```

Erfahren Sie mehr über `security login rest-role create` in der "ONTAP-Befehlsreferenz".

1. Erstellen Sie eine Domänenbenutzergruppe mit dem `security login` und fügen Sie die neue benutzerdefinierte Rolle für den Zugriff auf den REST-API-Endpunkt des S3-Benutzers hinzu. Erfahren Sie mehr über `security login create` im "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 die Domänengruppe `domain\group1` entsteht in `svm-1` und die benutzerdefinierte Rolle `s3role` wird 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
   ```

   Erfahren Sie mehr über `security login create` in der "ONTAP-Befehlsreferenz".

Das Hinzufügen der benutzerdefinierten Rolle zur Domänengruppe ermöglicht Benutzern in dieser Gruppe einen eingeschränkten Zugriff auf die ONTAP `/api/protocols/s3/services/{svm.uuid}/users` Endpunkt. Durch Aufrufen der API können die Domänengruppenbenutzer ihre eigenen Zugriffs- und Geheimschlüssel für den Zugriff auf den S3-Client generieren. Sie können die Schlüssel nur für sich selbst und nicht für andere Benutzer generieren.

Generieren Sie als S3- oder LDAP-Benutzer eigene Zugriffsschlüssel

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 eingeräumt hat. Sie können Schlüssel nur für sich selbst generieren, indem Sie den folgenden ONTAP REST-API-Endpunkt verwenden.

Erstellen Sie einen S3-Benutzer und generieren Sie Schlüssel

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

HTTP-Methode	Pfad
POST	/API/Protokolle/s3/Services/{svm.uuid}/Benutzer

Verwenden Sie für Domänenbenutzer das folgende Format für den S3-Benutzernamen: `user@fqdn` , Wo `fqdn` ist der vollqualifizierte Domänenname der Domäne.

Beispiel für die Wellung

```
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"}'
```

Beispiel für eine JSON-Ausgabe

```
{
  "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 bereits ein S3-Benutzer vorhanden ist, können Sie dessen Zugriffs- und Geheimschlüssel neu generieren. Dieser REST-API-Aufruf verwendet die folgende Methode und den folgenden Endpunkt.

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

Beispiel für die Wellung

```
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"}'
```

Beispiel für eine JSON-Ausgabe

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

Client-Zugriff auf S3-Objekt-Storage aktivieren

Aktivieren Sie ONTAP S3 Zugriff für Remote FabricPool Tiering

Damit ONTAP S3 als Cloud-Tier (Remote FabricPool Capacity) verwendet werden kann, muss der ONTAP S3-Administrator dem Remote-ONTAP-Cluster-Administrator Informationen über die S3-Serverkonfiguration bereitstellen.

Über diese Aufgabe

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

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

Darüber hinaus ist die folgende Netzwerkkonfiguration erforderlich:

- Der Hostname des Remote-ONTAP S3-Servers muss im für die Admin-SVM konfigurierten DNS-Server einen Eintrag enthalten, einschließlich des FQDN-Namens des S3-Servers und der IP-Adressen auf seinen LIFs.
- Intercluster LIFs müssen auf dem lokalen Cluster konfiguriert werden, obwohl Cluster-Peering nicht erforderlich ist.

In der FabricPool Dokumentation finden Sie Informationen zur Konfiguration von ONTAP S3 als Cloud-Tier.

"Managen von Storage-Tiers mit FabricPool"

Aktivieren Sie ONTAP S3-Zugriff für lokales FabricPool Tiering

Damit ONTAP S3 als lokale FabricPool-Kapazitäts-Tier verwendet werden kann, müssen Sie einen Objektspeicher basierend auf dem von Ihnen erstellten Bucket definieren und dann den Objektspeicher an ein Performance-Tier-Aggregat anhängen, um eine FabricPool zu erstellen.

Bevor Sie beginnen

Sie müssen über den ONTAP S3-Servernamen und einen Bucket-Namen verfügen und der S3-Server muss mit Cluster-LIFs (mit dem `-vserver Cluster` Parameter) erstellt worden sein.

Über diese Aufgabe

Die Objektspeicher-Konfiguration enthält Informationen zur lokalen Kapazitäts-Tier, einschließlich der S3-Server, Bucket-Namen und Authentifizierungsanforderungen.

Eine einmal erstellte Objekt-Storage-Konfiguration darf keinem anderen Objektspeicher oder Bucket zugeordnet werden. Sie können mehrere Buckets für lokale Tiers erstellen, jedoch nicht mehrere Objektspeichern in einem einzelnen Bucket erstellen.

Für eine lokale Kapazitäts-Tier ist keine FabricPool-Lizenz erforderlich.

Schritte

1. Objektspeicher für die lokale Kapazitäts-Tier 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
   ```

   - Das `-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 festlegen `false`, um die Zertifikatüberprüfung 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. Anzeigen und Überprüfen der Konfigurationsinformationen des Objektspeichers:

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

3. Optional: "Legen Sie fest, wie viele Daten in einem Volume inaktiv sind, indem Sie die inaktive Datenberichterstellung verwenden".

   Wenn Sie feststellen möchten, wie viele Daten in einem Volume inaktiv sind, können Sie entscheiden, welches Aggregat für lokales FabricPool Tiering verwendet werden soll.

4. Verbinden Sie den Objektspeicher mit einem Aggregat:

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

   Sie können `allow-flexgroup` **`true`** Aggregate mit FlexGroup Volume-Komponenten jederzeit anhängen.

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

5. Zeigen Sie die Objektspeicherinformationen an, und überprüfen Sie, 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

- "Speicheraggregat-Objektspeicher anhängen"
- "Speicheraggregat Objektspeicher Konfiguration erstellen"
- "Speicheraggregat Objektspeicher Konfiguration anzeigen"
- "Speicheraggregat-Objektspeicher anzeigen"

Aktivieren Sie S3-Client-Applikationen für den Zugriff auf einen ONTAP S3-Server

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

Bevor Sie beginnen

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

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

Andere Signaturversionen werden von ONTAP S3 nicht unterstützt.

Der ONTAP S3 Administrator muss S3 Benutzer erstellt und ihnen Zugriffsberechtigungen als einzelne Benutzer oder als Gruppenmitglied, in der Bucket-Richtlinie oder der Objekt-Storage-Server-Richtlinie gewährt haben.

Die S3-Client-App muss in der Lage sein, den ONTAP S3-Servernamen zu beheben. Dazu muss der ONTAP

S3-Administrator den S3-Servernamen (FQDN) und die IP-Adressen für die LIFs des S3-Servers angeben.

Über diese Aufgabe

Um auf einen ONTAP S3-Bucket zuzugreifen, geben Benutzer in der S3-Client-Applikation Informationen ein, die der ONTAP S3-Administrator zur Verfügung stellt.

Ab ONTAP 9.9 unterstützt der ONTAP S3 Server die folgenden AWS-Client-Funktionen:

- Benutzerdefinierte Objekt-Metadaten

  Ein Satz von Schlüsselwert-Paaren kann Objekten als Metadaten zugewiesen werden, wenn sie mit PUT (oder POST) erstellt werden. Wenn ein GET/HEAD-Vorgang am Objekt ausgeführt wird, werden die benutzerdefinierten Metadaten zusammen mit den Systemmetadaten zurückgegeben.

- Objekt-Tagging

  Ein separater Satz von Schlüsselwert-Paaren kann als Tags für die Kategorisierung von Objekten zugewiesen werden. Im Gegensatz zu Metadaten werden Tags unabhängig vom Objekt mit REST-APIs erstellt und gelesen. Sie werden auch dann implementiert, wenn Objekte erstellt oder zu einem beliebigen Zeitpunkt danach erstellt werden.

> Damit Kunden Tagging-Informationen abrufen und einfügen `GetObjectTagging` `PutObjectTagging` `DeleteObjectTagging` können, müssen die Aktionen, und über die Bucket- oder Gruppenrichtlinien erlaubt sein.

Weitere Informationen finden Sie in der AWS S3-Dokumentation.

Schritte

1. Authentifizieren Sie die S3-Client-App mit dem ONTAP S3-Server, indem Sie den S3-Servernamen und das CA-Zertifikat eingeben.
2. Authentifizieren Sie einen Benutzer in der S3-Client-App, indem Sie die folgenden Informationen eingeben:
   - S3-Servername (FQDN) und Bucket-Name
   - Zugriffsschlüssel und geheimer Schlüssel des Benutzers

ONTAP S3 Storage-Service-Level

ONTAP umfasst vordefinierte Storage-Services, die den entsprechenden minimalen Performance-Faktoren zugeordnet sind.

Die tatsächliche Menge an Storage-Services, die in einem Cluster oder einer SVM verfügbar sind, hängt von der Storage-Art ab, aus der ein Aggregat in der SVM besteht.

Die folgende Tabelle zeigt, wie die minimalen Performance-Faktoren den vordefinierten Storage-Services zugeordnet werden:

Storage-Service	Erwartete IOPS (SLA)	IOPS-Spitzenwerte (SLO)	Minimale Volume-IOPS	Geschätzte Latenz	Werden IOPS erzwungen?
Wert	128 pro TB	512 pro TB	75	17 ms	Bei AFF: Ja Ansonsten: Nein
Performance	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 das verfügbare Storage-Service-Level für jeden Medien- oder Node-Typ:

Medien oder Node	Verfügbares Storage Service Level
Festplatte	Wert
Festplatte einer virtuellen Maschine	Wert
Hybrid	Wert
Flash mit optimierter Kapazität	Wert
Solid State Drive (SSD) - kein All Flash FAS System	Wert
Performance-optimierter Flash – SSD (AFF)	Höchste Leistung, Mehrwert

Konfiguration der standortübergreifenden Ressourcenfreigabe (CORS) für ONTAP S3 Buckets

Ab ONTAP 9.16.1 können Sie die standortübergreifende Ressourcenfreigabe (Cross-Origin Resource Sharing, CORS) konfigurieren, damit Client-Webanwendungen aus verschiedenen Domänen auf Ihre ONTAP-Buckets zugreifen können. Dies ermöglicht einen sicheren Zugriff auf die Bucket-Objekte über einen Webbrowser.

CORS ist ein auf HTTP gebautes Framework, mit dem Skripts, die auf einer Webseite definiert sind, auf Ressourcen eines Servers in einer anderen Domäne zugreifen können. Das Framework wird verwendet, um sicher die *Same-Origin Policy* zu umgehen, die eine frühe Grundlage für die Web-Sicherheit darstellt. Die wichtigsten Konzepte und Terminologie werden im Folgenden beschrieben.

Ursprung

Ein Ursprung definiert genau den Standort und die Identität einer Ressource. Er wird als Kombination der folgenden Werte dargestellt:

- URI-Schema (Protokoll)
- Host-Name (Domain-Name oder IP-Adresse)

- Port-Nummer

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

Richtlinie für den gleichen Ursprung

Die Same-Origin Policy (SOP) ist ein Sicherheitskonzept und eine Einschränkung, die auf browserbasierte Skripte angewendet wird. Die Richtlinie ermöglicht es Skripts, die ursprünglich von einer Webseite geladen wurden, auf Daten auf einer anderen Seite zuzugreifen, solange beide Seiten denselben Ursprung haben. Diese Einschränkung verhindert, dass schädliche Skripte auf Daten auf den Seiten anderer Herkunft zugreifen.

Gängige CORS-Anwendungsfälle

Es gibt mehrere allgemeine Anwendungsfälle für CORS. Die meisten erfordern genau definierte Instanzen domänenübergreifenden Zugriffs, wie AJAX-Anforderungen, Laden von Schriftarten, Stylesheets und Skripts sowie domänenübergreifende Authentifizierung. CORS können auch als Teil einer einseiigen Anwendung (SPA) implementiert werden.

HTTP-Header

CORS wird mithilfe von Headern implementiert, die in die HTTP-Anforderungen und -Antworten eingefügt werden. Zum Beispiel gibt es mehrere Antwortheader, die die Zugriffskontrolle implementieren und angeben, welche Vorgänge, einschließlich Methoden und Header, zulässig sind. Das Vorhandensein des *Origin* Headers in einer HTTP-Anforderung definiert ihn als domänenübergreifende Anforderung. Der Ursprungswert wird vom CORS-Server verwendet, um eine gültige CORS-Konfiguration zu finden.

HTTP-Preflight-Anforderung

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

ONTAP-Buckets

Ein Bucket ist ein Container von Objekten, die anhand eines klar definierten Namespace gespeichert und abgerufen wurden. Es gibt zwei Arten von ONTAP Buckets:

- NAS-Buckets, auf die über die NAS- und S3-Protokolle zugegriffen werden kann
- S3-Buckets, auf die nur über das S3-Protokoll zugegriffen werden kann

Implementierung von CIS in ONTAP

CORS ist standardmäßig in ONTAP 9.16.1 und höheren Versionen aktiviert. Sie müssen CORS auf jeder SVM konfigurieren, wo sie aktiv ist.

> Es gibt keine administrative Option zum Deaktivieren von CORS für einen ONTAP-Cluster. Sie können sie jedoch effektiv deaktivieren, indem Sie keine Regeln definieren oder alle vorhandenen Regeln löschen.

Mögliche Anwendungsfälle

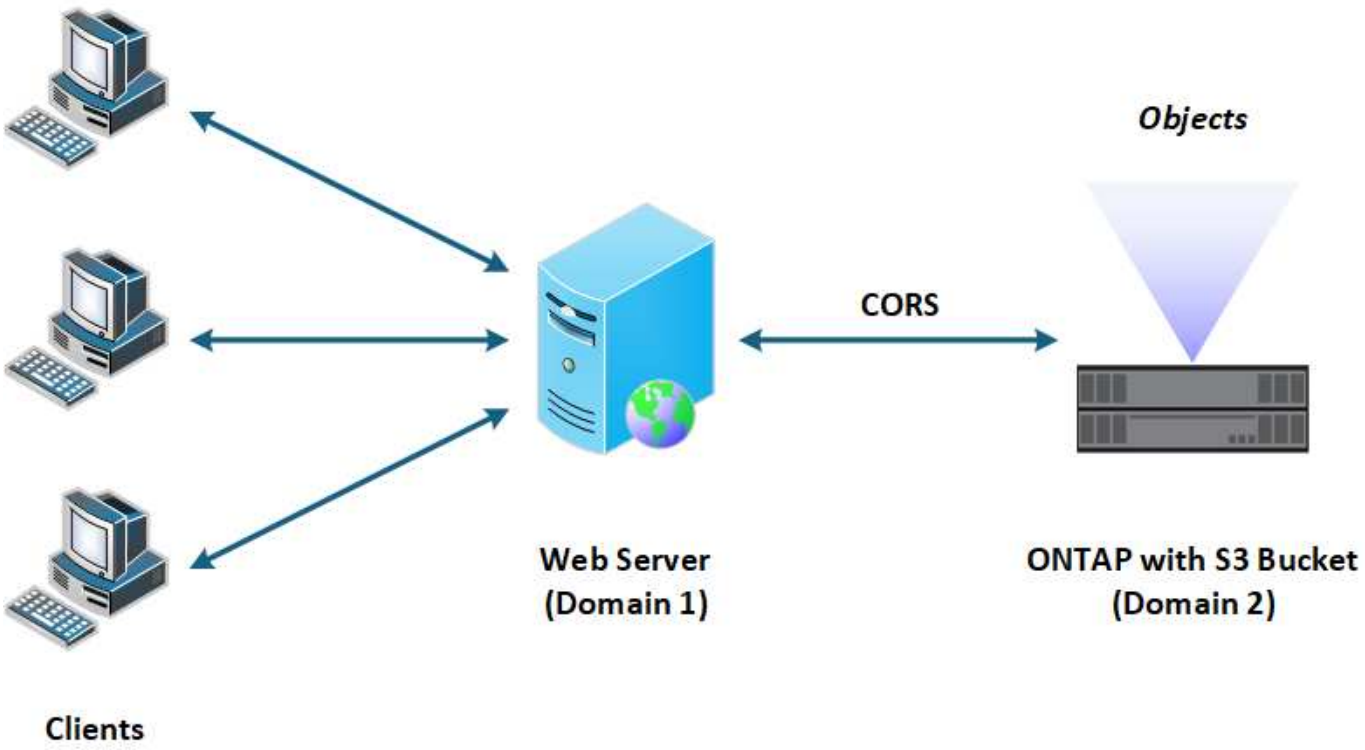
Die ONTAP CORS-Implementierung ermöglicht mehrere mögliche Topologien für den domänenübergreifenden Ressourcenzugriff, einschließlich:

- ONTAP S3 Buckets (innerhalb derselben oder einer anderen SVM bzw. Cluster)
- ONTAP NAS-Buckets (innerhalb derselben oder einer anderen SVM bzw. Cluster)

- ONTAP S3 und NAS-Buckets (innerhalb derselben oder anderer SVM bzw. Cluster)
- ONTAP-Buckets und Buckets externer Anbieter
- Buckets in verschiedenen Zeitzonen

Allgemeine Ansicht

Die folgende Abbildung zeigt auf einer allgemeinen Ebene, wie CORS den Zugriff auf die ONTAP S3 Buckets ermöglicht.



CORS-Regeln definieren

Sie müssen in ONTAP CORS-Regeln definieren, um die Funktion zu aktivieren und zu verwenden.

Konfigurationsaktionen

In ONTAP werden drei primäre Aktionen für Konfigurationsregeln unterstützt:

- Anzeigen
- Erstellen
- Löschen

Eine in ONTAP definierte CORS-Regel verfügt über mehrere Eigenschaften, einschließlich der SVM und des Buckets sowie über die zulässigen Ursprünge, Methoden und Header.

Administrationsoptionen

Für die Verwaltung von CORS auf Ihrem ONTAP-Cluster stehen Ihnen verschiedene Optionen zur Verfügung.

ONTAP Befehlszeilenschnittstelle

Sie können CORS über die Befehlszeilenschnittstelle konfigurieren. Weitere Informationen finden Sie unter Verwalten von CORS über die CLI .

ONTAP REST API

Sie können CORS mit der ONTAP REST API konfigurieren. Zur Unterstützung der CORS-Funktion wurden keine neuen Endpunkte hinzugefügt. Stattdessen können Sie den folgenden vorhandenen Endpunkt verwenden:

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

Erfahren Sie mehr in der "Dokumentation zur ONTAP Automatisierung".

S3 API

Sie können die S3-API verwenden, um eine CORS-Konfiguration auf einem ONTAP-Bucket zu erstellen und zu löschen. Ein S3-Client-Administrator benötigt ausreichende Privileges, einschließlich:

- Zugangsdaten für den Zugriff oder den geheimen Schlüssel
- Für den Bucket konfigurierte Richtlinie zum Zulassen des Zugriffs über s3API

Upgrade und Zurücksetzen

Wenn Sie CORS für den Zugriff auf die ONTAP S3 Buckets verwenden möchten, sollten Sie sich über mehrere administrative Probleme im Klaren sein.

Aktualisierung

Die CORS-Funktion wird unterstützt, wenn alle Knoten auf 9.16.1 aktualisiert werden. In Clustern mit gemischtem Modus ist die Funktion nur verfügbar, wenn die effektive Cluster-Version (ECV) 9.16.1 oder höher ist.

Zurücksetzen

Aus der Benutzerperspektive sollte die gesamte CORS-Konfiguration entfernt werden, bevor die Cluster-Wiederherstellung fortgesetzt werden kann. Intern werden alle CORS-Datenbanken gelöscht. Sie werden aufgefordert, einen Befehl auszuführen, um diese Datenstrukturen zu löschen und zurückzusetzen.

Verwalten von CORS über die CLI

Sie können die ONTAP-CLI verwenden, um CORS-Regeln zu verwalten. Die primären Vorgänge werden im Folgenden beschrieben. Sie müssen sich auf der Berechtigungsebene ONTAP **admin** befinden, um die CORS-Befehle ausgeben zu können.

Erstellen

Mit dem Befehl können Sie eine CORS-Regel definieren `vserver object-store-server bucket cors-rule create`. Erfahren Sie mehr über `vserver object-store-server bucket cors-rule create` in der "ONTAP-Befehlsreferenz".

Parameter

Die zum Erstellen einer Regel verwendeten Parameter werden nachfolgend beschrieben.

Parameter	Beschreibung
`vserver`	Gibt den Namen der SVM (vServer) an, die den Objektspeicher-Server-Bucket hostet, auf dem die Regel erstellt wird.
`bucket`	Der Name des Buckets auf dem Objektspeicher-Server, für den die Regel erstellt wird.
`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 Objektspeichers-Servers.
`allowed-origins`	Eine Liste der Ursprünge, von denen Anfragen über den Ursprung hinweg stammen dürfen.
`allowed-methods`	Eine Liste der HTTP-Methoden, die in einer Anforderung vom Typ „Cross-Origin“ zulässig sind.
`allowed-headers`	Eine Liste der in den Cross-Origin-Anfragen zulässigen HTTP-Header.
`expose-headers`	Eine Liste der zusätzlichen Kopfzeilen, die in den CORS-Antworten gesendet werden, auf die Kunden über ihre Anwendungen zugreifen können.
`max-age-in-seconds`	Ein optionaler Parameter, der angibt, wie lange Ihr Browser eine Pre-Flight-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
```

Anzeigen

Mit dem Befehl können `vserver object-store-server bucket cors-rule show` Sie eine Liste der aktuellen Regeln und deren Inhalt anzeigen. Erfahren Sie mehr über `vserver object-store-server bucket cors-rule show` in der "ONTAP-Befehlsreferenz".

Mit dem Parameter `-instance` werden die für jede der Regeln dargestellten Daten erweitert. Sie können auch angeben, welche Felder Sie möchten.

Beispiel

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

Löschen

Mit dem Befehl delete können Sie eine Instanz einer CORS-Regel entfernen. Sie benötigen den `index` Wert der Regel und so wird diese Operation in zwei Schritten ausgeführt:

1. Geben Sie einen Befehl ein `show`, um die Regel anzuzeigen und ihren Index abzurufen.
2. Geben Sie das Löschen mit dem Indexwert aus.

Beispiel

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

Ändern

Es ist kein CLI-Befehl verfügbar, um eine vorhandene CORS-Regel zu ändern. Um eine Regel zu ändern, müssen Sie Folgendes tun:

1. Löschen Sie die vorhandene Regel.
2. Erstellen Sie eine neue Regel mit den gewünschten Optionen.

Sicherung von Buckets mit SnapMirror S3

Informationen zu ONTAP SnapMirror S3

Ab ONTAP 9.10.1 können Buckets in ONTAP S3 Objektspeichern mithilfe von SnapMirror Spiegelungs- und Backup-Funktion gesichert werden. Im Gegensatz zu Standard-SnapMirror ermöglicht SnapMirror S3 Spiegelung und Backups an nicht-NetApp-Ziele wie AWS S3.

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

Ziel	Unterstützt aktive Spiegelungen und Takeover?	Unterstützung für Backup und Restore?
ONTAP S3 • Buckets in derselben SVM • Buckets in verschiedenen SVMs im selben Cluster • Buckets in SVMs auf verschiedenen Clustern	Ja.	Ja.

Ziel	Unterstützt aktive Spiegelungen und Takeover?	Unterstützung für Backup und Restore?
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 vorhandene Buckets auf ONTAP S3 Servern sichern oder neue Buckets erstellen, wobei die Datensicherung sofort aktiviert ist.

Anforderungen für SnapMirror S3

- ONTAP-Version

  ONTAP 9.10.1 oder höher muss auf Quell- und Ziel-Clustern ausgeführt werden.

  SnapMirror S3 wird in MetroCluster-Konfigurationen nicht unterstützt.

- Lizenzierung

  Die folgenden Lizenzen sind in der "ONTAP One" Softwaresuite verfügbar, die auf den Quell- und Zielsystemen von ONTAP erforderlich sind, um Zugriff auf:

  - ONTAP S3 Protokoll und Storage
  - SnapMirror S3 als Ziel für andere NetApp Objektspeicher-Ziele (ONTAP S3, StorageGRID und Cloud Volumes ONTAP)
  - SnapMirror S3 für Objektspeicher von Drittanbietern, einschließlich AWS S3 (verfügbar im "ONTAP One Kompatibilitätspaket")
  - Wenn auf Ihrem Cluster ONTAP 9.10.1 ausgeführt wird, ist ein "FabricPool Lizenz"erforderlich.

- ONTAP S3
  - ONTAP S3 Server müssen Quell- und Ziel-SVMs ausführen.
  - Es wird empfohlen, aber nicht erforderlich, dass CA-Zertifikate für TLS-Zugriff auf Systemen installiert werden, die S3-Server hosten.
    - Die Zertifizierungsstellenzertifikate, die zum Signieren der S3-Serverzertifikate verwendet werden, müssen auf der Admin-Speicher-VM der Cluster installiert werden, die S3-Server hosten.
    - Sie können ein selbstsigniertes CA-Zertifikat oder ein Zertifikat verwenden, das von einem externen CA-Anbieter signiert wurde.
    - Wenn die Quell- oder Ziel-Storage-VMs nicht HTTPS zuhören, ist es nicht erforderlich, CA-Zertifikate zu installieren.
- Peering (für ONTAP S3 Ziele)
  - Intercluster LIFs müssen konfiguriert werden (für Remote ONTAP Ziele). Die Intercluster LIFs des Quell- und Ziel-Clusters können mit den S3-Daten-LIFs des Quell- und Ziel-Servers verbunden werden.
  - Quell- und Ziel-Cluster werden (für Remote-ONTAP-Ziele) per Peering durchgeführt.

    - Quell- und Ziel-Storage VMs werden (für alle ONTAP Ziele) Peered.
- SnapMirror-Richtlinie
    - Eine S3-spezifische SnapMirror-Richtlinie ist für alle SnapMirror S3-Beziehungen erforderlich, Sie können jedoch für mehrere Beziehungen dieselbe Richtlinie verwenden.
    - Sie können Ihre eigene Richtlinie erstellen oder die standardmäßige **Continuous**-Richtlinie akzeptieren, die die folgenden Werte enthält:
        - Drosselklappe (oberer Grenzwert für Durchsatz/Bandbreite) – unbegrenzt.
        - Zeit für Recovery-Zeitpunkt: 1 Stunde (3600 Sekunden).

> Sie sollten beachten, dass wenn sich zwei S3-Buckets in einer SnapMirror Beziehung befinden und Lifecycle-Richtlinien so konfiguriert sind, dass die aktuelle Version eines Objekts abläuft (gelöscht wird), wird dieselbe Aktion auch in den Partner-Bucket repliziert. Dies gilt selbst dann, wenn der Partner-Bucket schreibgeschützt oder passiv ist.

- Root-Benutzerschlüssel Storage VM Root-Benutzerzugriffsschlüssel sind für SnapMirror S3-Beziehungen erforderlich; ONTAP weist diese standardmäßig nicht zu. Wenn Sie zum ersten Mal eine SnapMirror S3-Beziehung erstellen, müssen Sie überprüfen, ob die Schlüssel sowohl auf der Quell- als auch auf der Ziel-Speicher-VM vorhanden sind, und sie neu generieren, wenn dies nicht der Fall ist. Wenn Sie sie neu generieren müssen, müssen Sie sicherstellen, dass alle Clients und alle SnapMirror Objektspeicher-Konfigurationen unter Verwendung des Zugriffs- und geheimen Schlüsselpaars mit den neuen Schlüsseln aktualisiert werden.

Informationen zur S3-Serverkonfiguration finden Sie unter den folgenden Themen:

- "Aktivieren eines S3-Servers auf einer Storage-VM"
- "Allgemeines zum ONTAP S3-Konfigurationsprozess"

Informationen über Cluster und Storage VM Peering finden Sie unter folgendem Thema:

- "Vorbereiten auf Spiegelung und Vaulting (System Manager, Schritte 1–6)"
- "Cluster- und SVM-Peering (CLI)"

Unterstützte SnapMirror Beziehungen

SnapMirror S3 unterstützt Fan-Out- und Kaskadenbeziehungen. Eine Übersicht finden Sie unter "Fan-out- und kaskadierende Datensicherungsimplementierungen" .

SnapMirror S3 unterstützt keine Fan-in-Implementierungen (Datensicherungsbeziehungen zwischen mehreren Quell-Buckets und einem einzelnen Ziel-Bucket). SnapMirror S3 kann mehrere Bucket-Spiegelungen von mehreren Clustern auf ein einzelnes sekundäres Cluster unterstützen, aber jeder Quell-Bucket muss auf dem sekundären Cluster über einen eigenen Ziel-Bucket verfügen.

SnapMirror S3 wird in MetroCluster-Umgebungen nicht unterstützt.

Steuerung des Zugriffs auf S3 Buckets

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

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

Benutzer, Gruppenrichtlinien, Berechtigungen und ähnliche Komponenten müssen auf dem Ziel-Objektspeicher konfiguriert werden, damit Clients bei einem Failover auf den Ziel-Bucket zugreifen können.

Quell- und Zielbenutzer können denselben Zugriff und dieselben geheimen Schlüssel verwenden, sofern die Quellschlüssel manuell bereitgestellt werden, wenn der Benutzer auf dem Ziel-Cluster erstellt wird. Beispiel:

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

Weitere Informationen finden Sie in den folgenden Themen:

- "Hinzufügen von S3-Benutzern und -Gruppen (System Manager)"
- "Erstellen eines S3-Benutzers (CLI)"
- "S3-Gruppen erstellen oder ändern (CLI)"

S3 Objektsperre und Versionierung mit SnapMirror S3 verwenden

Sie können SnapMirror S3 für Objektsperre und Versionierung von aktivierten ONTAP Buckets verwenden. Es gibt einige Überlegungen:

- Um einen Quell-Bucket mit aktivierter Objektsperre zu replizieren, muss für den Ziel-Bucket auch die Objektsperre aktiviert sein. Darüber hinaus muss sowohl für die Quelle als auch für das Ziel die Versionierung aktiviert sein. Dadurch werden Probleme beim Spiegeln von Löschungen zum Ziel-Bucket vermieden, wenn beide Buckets über unterschiedliche standardmäßige Aufbewahrungsrichtlinien verfügen.
- S3 SnapMirror repliziert keine historischen Versionen von Objekten. Nur die aktuelle Version eines Objekts wird repliziert.

Werden Objekte, für die ein Objekt gesperrt ist, auf einen Ziel-Bucket gespiegelt, bleibt die ursprüngliche Aufbewahrungszeit erhalten. Wenn entsperrte Objekte repliziert werden, übernehmen sie den Standardaufbewahrungszeitraum 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 auf Bucket B repliziert wurden, behalten ihre 30-tägige Aufbewahrungsfrist bei, obwohl sie kleiner als die Standardaufbewahrungsfrist von Bucket B ist
- Bucket A verfügt nicht über eine Standardaufbewahrungsdauer und Bucket B hat eine Standardaufbewahrungsdauer von 60 Tagen. Wenn entsperrte Objekte von Bucket A auf Bucket B repliziert werden, übernehmen sie die 60-Tage-Aufbewahrungsfrist. Wenn ein Objekt manuell in Bucket A gesperrt wird, behält es beim Replizieren in Bucket B seinen ursprünglichen Aufbewahrungszeitraum bei
- Bucket A hat eine Standardaufbewahrungsdauer von 30 Tagen und Bucket B hat keine Standardaufbewahrungsdauer. Von Bucket A nach Bucket B replizierte Objekte behalten die Aufbewahrungsfrist von 30 Tagen bei.

Spiegelung und Backup-Schutz auf einem Remote-Cluster

Erstellen einer Spiegelbeziehung für einen neuen ONTAP S3-Bucket auf dem Remote-Cluster

Wenn Sie neue S3-Buckets erstellen, können Sie diese sofort in einem SnapMirror S3-Ziel auf einem Remote-Cluster schützen.

Über diese Aufgabe

Sie müssen Aufgaben sowohl auf Quell- als auch auf Zielsystemen ausführen.

Bevor Sie beginnen

- Die Anforderungen für ONTAP-Versionen, Lizenzierung und S3-Serverkonfiguration wurden erfüllt.
- Zwischen Quell- und Ziel-Clustern ist eine Peering-Beziehung vorhanden, während zwischen Quell- und Ziel-Storage VMs eine Peering-Beziehung besteht.
- FÜR die Quell- und Ziel-VMs SIND CA-Zertifikate erforderlich. Sie können selbstsignierte CA-Zertifikate oder -Zertifikate verwenden, die von einem externen CA-Anbieter signiert wurden.

System Manager

1. Wenn dies die erste SnapMirror S3-Beziehung für diese Storage-VM ist, überprüfen Sie, ob Root-Benutzerschlüssel sowohl für Quell- als auch für Ziel-Storage-VMs vorhanden sind, und regenerieren Sie Sie sie erneut, wenn dies nicht der Fall ist:
   a. Klicken Sie auf **Storage > Storage VMs** und wählen Sie dann die Speicher-VM aus.
   b. Klicken Sie im Register **Einstellungen** auf die Kachel **S3**.
   c. Überprüfen Sie auf der Registerkarte **Benutzer**, ob für den Root-Benutzer ein Zugriffsschlüssel vorhanden ist.
   d. Wenn nicht, klicken Sie neben **root** und dann auf **regenerieren-Schlüssel**. Generieren Sie den Schlüssel nicht neu, wenn er bereits vorhanden ist.
2. Bearbeiten Sie die Storage VM, um Benutzer hinzuzufügen und Benutzern zu Gruppen hinzuzufügen, sowohl im Quell- als auch im Ziel-Storage der VMs:

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

   Weitere Informationen finden Sie unter "Fügen Sie S3-Benutzer und -Gruppen hinzu" .
3. Erstellen Sie im Quellcluster eine SnapMirror S3-Richtlinie, wenn Sie noch keine haben und nicht die Standardrichtlinie verwenden möchten:
   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.
      - Wählen Sie den Richtlinienumfang, das Cluster oder die SVM aus
      - Wählen Sie **kontinuierlich** für SnapMirror S3-Beziehungen aus.
      - Geben Sie Ihre **Throttle**- und **Recovery Point Objective**-Werte ein.
4. Erstellung eines Buckets mit SnapMirror Sicherung:
   a. Klicken Sie auf **Storage > Buckets** und dann auf **Hinzufügen**. Die Überprüfung der Berechtigungen ist optional, wird aber empfohlen.
   b. Geben Sie einen Namen ein, wählen Sie die Speicher-VM aus, geben Sie eine Größe ein und klicken Sie dann auf **Weitere Optionen**.
   c. Klicken Sie unter **Berechtigungen** auf **Hinzufügen**.
      - **Principal** und **Effect** - Wählen Sie Werte aus, die Ihren Benutzergruppeneinstellungen entsprechen, oder übernehmen Sie die Standardeinstellungen.
      - **Aktionen**- stellen Sie sicher, dass die folgenden Werte angezeigt werden:

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

      - **Ressourcen** - Verwenden Sie die Standardeinstellungen (*bucketname, bucketname/**) oder andere Werte, die Sie benötigen.

        "Management des Benutzerzugriffs auf Buckets"Weitere Informationen zu diesen Feldern finden Sie unter.

d. Aktivieren Sie unter **Schutz Enable SnapMirror (ONTAP oder Cloud)**. Geben Sie anschließend die folgenden Werte ein:

- Ziel
  - **ZIEL: ONTAP-System**
  - **CLUSTER**: Wählen Sie den Remote-Cluster aus.
  - **STORAGE VM**: Wählen Sie eine Speicher-VM auf dem Remote-Cluster aus.
  - **S3-SERVER-CA-ZERTIFIKAT**: Kopieren Sie den Inhalt des *source*-Zertifikats.
- Quelle
  - **S3-SERVER-CA-ZERTIFIKAT:** Kopieren und Einfügen des Inhalts des *Destination* -Zertifikats.

5. Überprüfen Sie **Verwenden Sie dasselbe Zertifikat auf dem Ziel**, wenn Sie ein Zertifikat verwenden, das von einem externen CA-Anbieter signiert wurde.
6. Wenn Sie auf **Zieleinstellungen** klicken, können Sie Ihre eigenen Werte anstelle der Standardeinstellungen für Bucket-Name, -Kapazität und -Service-Level eingeben.
7. Klicken Sie Auf **Speichern**. Ein neuer Bucket wird in der Quell-Storage-VM erstellt und in einem neuen Bucket gespiegelt, der die Ziel-Storage-VM erstellt wurde.

Sichern Sie gesperrte Buckets

Ab ONTAP 9.14.1 können Sie gesperrte S3-Buckets sichern und nach Bedarf wiederherstellen.

Wenn Sie die Schutzeinstellungen für einen neuen oder vorhandenen Bucket definieren, können Sie die Objektsperrung für Ziel-Buckets aktivieren, sofern auf den Quell- und Ziel-Clustern ONTAP 9.14.1 oder höher ausgeführt wird und die Objektsperrung auf dem Quell-Bucket aktiviert ist. Der Sperrmodus für Objekte und die Aufbewahrungsdauer der Quell-Buckets werden für die replizierten Objekte auf dem Ziel-Bucket angewendet. Sie können auch eine andere Sperrfrist für den Ziel-Bucket im Abschnitt **Zieleinstellungen** definieren. Dieser Aufbewahrungszeitraum wird auch auf alle nicht gesperrten Objekte angewendet, die aus den Quell-Bucket und S3-Schnittstellen repliziert werden.

Informationen zum Aktivieren der Objektsperrung auf einem Bucket finden Sie unter "Erstellen eines Buckets".

CLI

1. Wenn es sich hierbei um die erste SnapMirror S3-Beziehung für diese SVM handelt, überprüfen Sie, ob Root-Benutzerschlüssel für Quell- und Ziel-SVMs vorhanden sind, und regenerieren Sie sie erneut, wenn dies nicht der Fall ist:

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

   Vergewissern Sie sich, dass für den Root-Benutzer ein Zugriffsschlüssel vorhanden ist. Falls nicht, geben Sie Folgendes ein:

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

   Generieren Sie den Schlüssel nicht neu, wenn er bereits vorhanden ist.

2. Buckets für die Quell- und Ziel-SVMs 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. Fügen Sie Zugriffsregeln den Standard-Bucket-Richtlinien sowohl in den Quell- als auch in Ziel-SVMs hinzu:

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

   Parameter:

   - Typ `continuous`: Die einzige Richtlinienart für SnapMirror S3-Beziehungen (erforderlich).
   - `-rpo` - Gibt die Zeit für die Recovery Point Objective in Sekunden an (optional).
   - `-throttle` - Gibt die obere Grenze für Durchsatz/Bandbreite in Kilobyte/Sekunden an (optional).

     Beispiel

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

5. Installieren von CA-Server-Zertifikaten auf den Administrator-SVMs der Quell- und Ziel-Cluster:

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

      Wenn Sie ein von einem externen CA-Anbieter signiertes Zertifikat verwenden, installieren Sie dasselbe Zertifikat auf der Quell- und Ziel-Administrator-SVM.

Erfahren Sie mehr über `security certificate install` in der "ONTAP-Befehlsreferenz".

6. Erstellen Sie auf der Quell-SVM eine 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 Standardeinstellung übernehmen.

   Beispiel

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

7. Vergewissern Sie sich, dass die Spiegelung aktiv ist:
   `snapmirror show -policy-type continuous -fields status`

Verwandte Informationen

- "snapmirror erstellen"
- "Snapmirror-Richtlinie erstellen"
- "Snapmirror-Show"

Erstellen einer Spiegelbeziehung für einen vorhandenen ONTAP S3-Bucket auf dem Remote-Cluster

Sie können jederzeit damit beginnen, vorhandene S3-Buckets zu schützen. Wenn Sie beispielsweise eine S3-Konfiguration von einer älteren Version als ONTAP 9.10.1 aktualisiert haben.

Über diese Aufgabe

Sie müssen Aufgaben sowohl auf den Quell- als auch auf den Ziel-Clustern ausführen.

Bevor Sie beginnen

- Die Anforderungen für ONTAP-Versionen, Lizenzierung und S3-Serverkonfiguration wurden erfüllt.
- Zwischen Quell- und Ziel-Clustern ist eine Peering-Beziehung vorhanden, während zwischen Quell- und Ziel-Storage VMs eine Peering-Beziehung besteht.
- FÜR die Quell- und Ziel-VMs SIND CA-Zertifikate erforderlich. Sie können selbstsignierte CA-Zertifikate oder -Zertifikate verwenden, die von einem externen CA-Anbieter signiert wurden.

Schritte

Sie können eine Spiegelbeziehung mit System Manager oder der ONTAP CLI erstellen.

System Manager

1. Wenn dies die erste SnapMirror S3-Beziehung für diese Storage-VM ist, überprüfen Sie, ob Root-Benutzerschlüssel sowohl für Quell- als auch für Ziel-Storage-VMs vorhanden sind, und regenerieren Sie Sie sie erneut, wenn dies nicht der Fall ist:
   a. Wählen Sie **Storage > Storage VMs** aus und wählen Sie dann die Storage VM aus.
   b. Klicken Sie im Register **Einstellungen** auf die Kachel **S3**.
   c. Überprüfen Sie auf der Registerkarte **Benutzer**, ob für den Root-Benutzer ein Zugriffsschlüssel vorhanden ist.
   d. Wenn nicht, klicken Sie neben **root** und dann auf **regenerieren-Schlüssel.** Generieren Sie den Schlüssel nicht neu, wenn er bereits vorhanden ist.
2. Überprüfen Sie, ob vorhandene Benutzer und Gruppen vorhanden sind und den richtigen Zugriff auf die Quell- und Zielspeicher-VMs haben: Wählen Sie **Speicher > Speicher-VMs**, wählen Sie dann die Speicher-VM und dann **Einstellungen** Tab. Suchen Sie schließlich die Kachel **S3**, wählen Sie , und wählen Sie die Registerkarte **Benutzer** und dann die Registerkarte **Gruppen**, um die Benutzer- und Gruppenzugriffseinstellungen anzuzeigen.

   Weitere Informationen finden Sie unter "Fügen Sie S3-Benutzer und -Gruppen hinzu" .
3. Erstellen Sie im Quellcluster eine SnapMirror S3-Richtlinie, wenn Sie noch keine haben und nicht die Standardrichtlinie verwenden möchten:
   a. Wählen Sie **Schutz > Übersicht** und klicken Sie dann auf **Einstellungen für lokale Richtlinien**.
   b. Wählen Sie neben **Schutzrichtlinien** aus , und klicken Sie dann auf **Hinzufügen**.
   c. Geben Sie den Namen und die Beschreibung der Richtlinie ein.
   d. Wählen Sie den Richtlinienumfang aus – entweder Cluster oder SVM.
   e. Wählen Sie **kontinuierlich** für SnapMirror S3-Beziehungen aus.
   f. Geben Sie Ihre **Throttle**- und **Recovery Point Objective**-Werte ein.
4. Vergewissern Sie sich, dass die Bucket-Zugriffsrichtlinie des vorhandenen Buckets nach wie vor die Anforderungen erfüllt:
   a. Klicken Sie auf **Speicher > Eimer** und wählen Sie dann den Eimer aus, den Sie schützen möchten.
   b. Klicken Sie im Register **Berechtigungen** auf **Bearbeiten** und dann unter **Berechtigungen** auf **Hinzufügen**.
      - **Principal und Effect**: Wählen Sie die Werte, die Ihren Benutzergruppeneinstellungen entsprechen, oder übernehmen Sie die Standardeinstellungen.
      - **Aktionen**: Stellen Sie sicher, dass folgende Werte angezeigt werden:

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

      - **Ressourcen**: Verwenden Sie die Standardwerte (*bucketname, bucketname/**) oder andere Werte, die Sie benötigen.

        "Management des Benutzerzugriffs auf Buckets"Weitere Informationen zu diesen Feldern finden Sie unter.

5. Schützen Sie einen vorhandenen Bucket mit SnapMirror S3-Sicherung:
   a. Klicken Sie auf **Storage** > **Buckets** und wählen Sie dann den Eimer aus, den Sie schützen möchten.
   b. Klicken Sie auf **Protect** und geben Sie die folgenden Werte ein:
      - Ziel
        - **ZIEL**: ONTAP-System
        - **CLUSTER**: Wählen Sie den Remote-Cluster aus.
        - **STORAGE VM**: Wählen Sie eine Speicher-VM auf dem Remote-Cluster aus.
        - **S3-SERVER-CA-ZERTIFIKAT**: Kopieren Sie den Inhalt des *source*-Zertifikats.
      - Quelle
        - **S3-SERVER-CA-ZERTIFIKAT**: Kopieren Sie den Inhalt des *Destination*-Zertifikats.
6. Überprüfen Sie **Verwenden Sie dasselbe Zertifikat auf dem Ziel**, wenn Sie ein Zertifikat verwenden, das von einem externen CA-Anbieter signiert wurde.
7. Wenn Sie auf **Zieleinstellungen** klicken, können Sie Ihre eigenen Werte anstelle der Standardeinstellungen für Bucket-Name, -Kapazität und -Service-Level eingeben.
8. Klicken Sie Auf **Speichern**. Der vorhandene Bucket wird zu einem neuen Bucket in der Ziel-Storage-VM gespiegelt.

Sichern Sie gesperrte Buckets

Ab ONTAP 9.14.1 können Sie gesperrte S3-Buckets sichern und nach Bedarf wiederherstellen.

Wenn Sie die Schutzeinstellungen für einen neuen oder vorhandenen Bucket definieren, können Sie die Objektsperrung für Ziel-Buckets aktivieren, sofern auf den Quell- und Ziel-Clustern ONTAP 9.14.1 oder höher ausgeführt wird und die Objektsperrung auf dem Quell-Bucket aktiviert ist. Der Sperrmodus für Objekte und die Aufbewahrungsdauer der Quell-Buckets werden für die replizierten Objekte auf dem Ziel-Bucket angewendet. Sie können auch eine andere Sperrfrist für den Ziel-Bucket im Abschnitt **Zieleinstellungen** definieren. Dieser Aufbewahrungszeitraum wird auch auf alle nicht gesperrten Objekte angewendet, die aus den Quell-Bucket und S3-Schnittstellen repliziert werden.

Informationen zum Aktivieren der Objektsperrung auf einem Bucket finden Sie unter "Erstellen eines Buckets".

CLI

1. Wenn dies die erste SnapMirror S3-Beziehung für diese SVM ist, überprüfen Sie, ob Root-Benutzerschlüssel für Quell- und Ziel-SVMs vorhanden sind, und regenerieren Sie sie, wenn sie `vserver object-store-server user show` dies nicht tun: + Überprüfen Sie, ob es einen Zugriffsschlüssel für den Root-Benutzer gibt. Wenn nicht, geben Sie ein: `vserver object-store-server user regenerate-keys -vserver svm_name -user root` + Den Schlüssel nicht neu generieren, wenn er bereits vorhanden ist.
2. Erstellen eines Buckets für die Ziel-SVM als Ziel-Ziel:

   ```
   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. Überprüfen Sie, ob die Zugriffsregeln der Standard-Bucket-Richtlinien sowohl in den Quell- als auch in den Ziel-SVMs 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. Erstellen Sie auf der Quell-SVM eine SnapMirror S3-Richtlinie, wenn Sie noch keine haben und die Standardrichtlinie nicht 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 Recovery Point Objective in Sekunden an (optional).
   - `-throttle` – Gibt die obere Grenze für Durchsatz/Bandbreite in Kilobyte/Sekunden an (optional).

     Beispiel

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

5. Installieren von CA-Zertifikaten auf den Administrator-SVMs von Quell- und Ziel-Clustern:

   a. Installieren Sie auf dem Quell-Cluster das CA-Zertifikat, das das *Destination* 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 *source* S3-Serverzertifikat signiert `security certificate install -type server-ca -vserver dest_admin_svm -cert-name src_server_certificate` hat: + Wenn Sie ein von einem externen CA-Anbieter signiertes Zertifikat verwenden, installieren Sie dasselbe Zertifikat auf der Quell- und Ziel-Admin-SVM.

      Erfahren Sie mehr über `security certificate install` in der "ONTAP-Befehlsreferenz".

6. Erstellen Sie auf der Quell-SVM eine 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 Standardeinstellung übernehmen.

Beispiel

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

7. Vergewissern Sie sich, dass die Spiegelung aktiv ist:
`snapmirror show -policy-type continuous -fields status`

Verwandte Informationen

- "snapmirror erstellen"
- "Snapmirror-Richtlinie erstellen"
- "Snapmirror-Show"

Übernehmen Sie die Übernahme vom ONTAP S3-Zielbucket auf dem Remote-Cluster

Wenn die Daten in einem Quell-Bucket nicht mehr verfügbar sind, können Sie die SnapMirror Beziehung unterbrechen, um den Ziel-Bucket beschreibbar zu machen und mit der Bereitstellung von Daten zu beginnen.

Über diese Aufgabe

Wenn ein Takeover-Vorgang durchgeführt wird, wird Quell-Bucket in schreibgeschützt konvertiert und der ursprüngliche Ziel-Bucket in Lese-/Schreibzugriff konvertiert, um die SnapMirror S3-Beziehung rückgängig zu machen.

Wenn der deaktivierte Quell-Bucket wieder verfügbar ist, synchronisiert SnapMirror S3 den Inhalt der beiden Buckets automatisch neu. Es ist nicht erforderlich, die Beziehung explizit neu zu synchronisieren, wie es für Volume SnapMirror Implementierungen erforderlich ist.

Der Takeover-Vorgang muss vom Remote Cluster aus initiiert werden.

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

Benutzer, Gruppenrichtlinien, Berechtigungen und ähnliche Komponenten müssen auf dem Ziel-Objektspeicher konfiguriert werden, damit Clients bei einem Failover auf den Ziel-Bucket zugreifen können.

Quell- und Zielbenutzer können denselben Zugriff und dieselben geheimen Schlüssel verwenden, sofern die Quellschlüssel manuell bereitgestellt werden, wenn der Benutzer auf dem Ziel-Cluster erstellt wird. Beispiel:

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

System Manager

Failover aus dem nicht verfügbaren Bucket und Beginn der Datenbereitstellung:

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

CLI

1. Initiieren Sie einen Failover-Vorgang für den Ziel-Bucket:
   `snapmirror failover start -destination-path` *`svm_name`*`:/bucket/`*`bucket_name`*
2. Überprüfen Sie den Status des Failover-Vorgangs:
   `snapmirror show -fields status`

   Beispiel

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

Verwandte Informationen

- "Hinzufügen von S3-Benutzern und -Gruppen (System Manager)"
- "Erstellen eines S3-Benutzers (CLI)"
- "S3-Gruppen erstellen oder ändern (CLI)"
- "Snapmirror-Failover-Start"
- "Snapmirror-Show"

Stellen Sie einen ONTAP S3-Bucket von der Ziel-SVM auf dem Remote-Cluster wieder her

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

Über diese Aufgabe

Sie können den Ziel-Bucket auf einem vorhandenen oder einem neuen Bucket wiederherstellen. Der Ziel-Bucket für den Wiederherstellungsvorgang muss größer sein als der logische genutzte Speicherplatz des Ziel-Buckets.

Wenn Sie einen vorhandenen Bucket verwenden, muss er beim Starten eines Wiederherstellungsvorgangs leer sein. Beim Restore wird ein Bucket nicht rechtzeitig „zurück“, sondern es füllt einen leeren Bucket mit den vorherigen Inhalten aus.

Der Wiederherstellungsvorgang muss vom Remote-Cluster initiiert werden.

System Manager

Gesicherte Daten wiederherstellen:

1. Klicken Sie auf **Schutz > Beziehungen**, und wählen Sie dann **SnapMirror S3** aus.
2. Klicken Sie auf ⋮ und wählen Sie dann **Wiederherstellen**.
3. Wählen Sie unter **Quelle vorhandener Bucket** (Standard) oder **Neuer Bucket** aus.
   - Um einen **vorhandenen Bucket** (die Standardeinstellung) wiederherzustellen, führen Sie die folgenden Aktionen aus:
     - Wählen Sie das Cluster und die Storage-VM aus, um nach dem vorhandenen Bucket zu suchen.
     - Wählen Sie den vorhandenen Bucket aus.
     - Kopieren Sie den Inhalt des CA-Zertifikats des *Destination* S3-Servers und fügen Sie ihn ein.
   - Um einen **neuen Bucket** wiederherzustellen, geben Sie die folgenden Werte ein:
     - Der Cluster und die Storage-VM zum Hosten des neuen Buckets.
     - Name, Kapazität und Performance des neuen Bucket Weitere Informationen finden Sie unter "Storage Service Level" .
     - Der Inhalt des CA-Zertifikats des *Destination* S3-Servers.
4. Kopieren Sie unter **Destination** den Inhalt des CA-Zertifikats *source* S3-Server.
5. Klicken Sie auf **Schutz > Beziehungen**, um den Wiederherstellungsfortschritt zu überwachen.

Gesperrte Buckets wiederherstellen

Ab ONTAP 9.14.1 können Sie gesperrte Buckets sichern und nach Bedarf wiederherstellen.

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

- **Wiederherstellung auf einen neuen Bucket**: Wenn die Objektsperrung aktiviert ist, kann ein Bucket wiederhergestellt werden, indem ein Bucket erstellt wird, für den auch die Objektsperrung aktiviert ist. Wenn Sie einen gesperrten Bucket wiederherstellen, werden der Objektsperrmodus und der Aufbewahrungszeitraum des ursprünglichen Buckets repliziert. Sie können auch eine andere Sperrfrist für den neuen Bucket definieren. Diese Aufbewahrungsfrist wird auf nicht gesperrte Objekte aus anderen Quellen angewendet.
- **Wiederherstellung auf einen vorhandenen Bucket**: Ein Object-Locked Bucket kann in einen bestehenden Bucket wiederhergestellt werden, sofern auf dem bestehenden Bucket Versionierung und ein ähnlicher Object-Locking-Modus aktiviert sind. Die Aufbewahrungsdauer des ursprünglichen Eimers wird beibehalten.
- **Nicht gesperrte Buckets wiederherstellen**: Selbst wenn die Objektsperrung auf einem Bucket nicht aktiviert ist, können Sie sie in einem Bucket wiederherstellen, der die Objektsperrung aktiviert hat und sich auf dem Quellcluster befindet. Wenn Sie den Bucket wiederherstellen, werden alle nicht gesperrten Objekte gesperrt, und der Aufbewahrungszeitraum und die Dauer des Ziel-Buckets werden für sie anwendbar.

CLI

1. Erstellen Sie den neuen Ziel-Bucket für die Wiederherstellung. Weitere Informationen finden Sie unter "Eine Cloud-Backup-Beziehung für einen neuen ONTAP S3 Bucket erstellen".
2. Initiieren Sie einen Wiederherstellungsvorgang für den Ziel-Bucket:

```
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
```

Erfahren Sie mehr über `snapmirror restore` in der "ONTAP-Befehlsreferenz".

Spiegelung und Backup-Schutz auf dem lokalen Cluster

Erstellen einer Spiegelbeziehung für einen neuen ONTAP S3-Bucket auf dem lokalen Cluster

Wenn Sie neue S3-Buckets erstellen, können Sie diese sofort in einem SnapMirror S3-Ziel im selben Cluster schützen. Sie können Daten auf einen Bucket in einer anderen Storage-VM oder auf derselben Storage-VM wie die Quelle spiegeln.

Bevor Sie beginnen

- Die Anforderungen für ONTAP-Versionen, Lizenzierung und S3-Serverkonfiguration wurden erfüllt.
- Zwischen Quell- und Ziel-Storage-VMs besteht eine Peering-Beziehung.
- FÜR die Quell- und Ziel-VMs SIND CA-Zertifikate erforderlich. Sie können selbstsignierte CA-Zertifikate oder -Zertifikate verwenden, die von einem externen CA-Anbieter signiert wurden.

System Manager

1. Wenn dies die erste SnapMirror S3-Beziehung für diese Storage-VM ist, überprüfen Sie, ob Root-Benutzerschlüssel sowohl für Quell- als auch für Ziel-Storage-VMs vorhanden sind, und regenerieren Sie Sie sie erneut, wenn dies nicht der Fall ist:
   a. Klicken Sie auf **Storage > Storage VMs** und wählen Sie dann die Speicher-VM aus.
   b. Klicken Sie im Register **Einstellungen** auf die Kachel S3.
   c. Überprüfen Sie auf der Registerkarte **Benutzer**, ob für den Root-Benutzer ein Zugriffsschlüssel vorhanden ist
   d. Wenn nicht, klicken Sie neben **root** und dann auf **regenerieren-Schlüssel**. Generieren Sie den Schlüssel nicht neu, wenn er bereits vorhanden ist.
2. Bearbeiten Sie die Speicher-VM zum Hinzufügen von Benutzern und zum Hinzufügen von Benutzern zu Gruppen in den Quell- und Zielspeicher-VMs: Klicken Sie auf **Speicher > Speicher-VMs**, klicken Sie auf die Speicher-VM, klicken Sie auf **Einstellungen** und klicken Sie dann unter S3.

   Weitere Informationen finden Sie unter "Fügen Sie S3-Benutzer und -Gruppen hinzu" .
3. Erstellen Sie eine SnapMirror S3-Richtlinie, wenn Sie noch keine haben und die Standardrichtlinie nicht verwenden möchten:
   a. Klicken Sie auf **Schutz > Übersicht** und dann auf **Einstellungen für lokale Richtlinien**.
   b. Klicken Sie neben **Schutzrichtlinien** und dann auf **Hinzufügen**.
      - Geben Sie den Namen und die Beschreibung der Richtlinie ein.
      - Wählen Sie den Richtlinienumfang, das Cluster oder die SVM aus
      - Wählen Sie **kontinuierlich** für SnapMirror S3-Beziehungen aus.
      - Geben Sie Ihre **Throttle**- und **Recovery Point Objective**-Werte ein.
4. Erstellung eines Buckets mit SnapMirror Sicherung:
   a. Klicken Sie auf **Storage > Buckets** und dann auf **Hinzufügen**.
   b. Geben Sie einen Namen ein, wählen Sie die Speicher-VM aus, geben Sie eine Größe ein und klicken Sie dann auf **Weitere Optionen**.
   c. Klicken Sie unter **Berechtigungen** auf **Hinzufügen**. Die Überprüfung der Berechtigungen ist optional, wird aber empfohlen.
      - **Principal** und **Effect** - Wählen Sie Werte aus, die Ihren Benutzergruppeneinstellungen entsprechen, oder übernehmen Sie die Standardeinstellungen.
      - **Aktionen** - stellen Sie sicher, dass die folgenden Werte angezeigt werden:

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

      - **Ressourcen** - Verwenden Sie die Standardeinstellungen `(bucketname, bucketname/*)` oder andere Werte, die Sie benötigen

        "Management des Benutzerzugriffs auf Buckets"Weitere Informationen zu diesen Feldern finden Sie unter.

d. Aktivieren Sie unter **Schutz Enable SnapMirror (ONTAP oder Cloud)**. Geben Sie anschließend die folgenden Werte ein:

- Ziel
  - **ZIEL**: ONTAP-System
  - **CLUSTER**: Wählen Sie den lokalen Cluster aus.
  - **STORAGE VM**: Wählen Sie eine Storage VM auf dem lokalen Cluster aus.
  - **S3 SERVER CA-ZERTIFIKAT**: Kopieren Sie den Inhalt des Quellzertifikats und fügen Sie ihn ein.
- Quelle
  - **S3 SERVER CA-ZERTIFIKAT**: Kopieren Sie den Inhalt des Zielzertifikats und fügen Sie ihn ein.

5. Überprüfen Sie **Verwenden Sie dasselbe Zertifikat auf dem Ziel**, wenn Sie ein Zertifikat verwenden, das von einem externen CA-Anbieter signiert wurde.
6. Wenn Sie auf **Zieleinstellungen** klicken, können Sie Ihre eigenen Werte anstelle der Standardeinstellungen für Bucket-Name, -Kapazität und -Service-Level eingeben.
7. Klicken Sie Auf **Speichern**. Ein neuer Bucket wird in der Quell-Storage-VM erstellt und in einem neuen Bucket gespiegelt, der die Ziel-Storage-VM erstellt wurde.

Sichern Sie gesperrte Buckets

Ab ONTAP 9.14.1 können Sie gesperrte S3-Buckets sichern und nach Bedarf wiederherstellen.

Wenn Sie die Schutzeinstellungen für einen neuen oder vorhandenen Bucket definieren, können Sie die Objektsperrung für Ziel-Buckets aktivieren, sofern auf den Quell- und Ziel-Clustern ONTAP 9.14.1 oder höher ausgeführt wird und die Objektsperrung auf dem Quell-Bucket aktiviert ist. Der Sperrmodus für Objekte und die Aufbewahrungsdauer der Quell-Buckets werden für die replizierten Objekte auf dem Ziel-Bucket angewendet. Sie können auch eine andere Sperrfrist für den Ziel-Bucket im Abschnitt **Zieleinstellungen** definieren. Dieser Aufbewahrungszeitraum wird auch auf alle nicht gesperrten Objekte angewendet, die aus den Quell-Bucket und S3-Schnittstellen repliziert werden.

Informationen zum Aktivieren der Objektsperrung auf einem Bucket finden Sie unter "Erstellen eines Buckets".

CLI

1. Wenn es sich hierbei um die erste SnapMirror S3-Beziehung für diese SVM handelt, überprüfen Sie, ob Root-Benutzerschlüssel für Quell- und Ziel-SVMs vorhanden sind, und regenerieren Sie sie erneut, wenn dies nicht der Fall ist:
   `vserver object-store-server user show`

   Vergewissern Sie sich, dass für den Root-Benutzer ein Zugriffsschlüssel vorhanden ist. Wenn dies nicht der Fall ist, geben Sie Folgendes ein:
   `vserver object-store-server user regenerate-keys -vserver svm_name -user root`

   Generieren Sie den Schlüssel nicht neu, wenn er bereits vorhanden ist.

2. Buckets für die Quell- und Ziel-SVMs 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. Fügen Sie Zugriffsregeln den Standard-Bucket-Richtlinien sowohl in den Quell- als auch in Ziel-SVMs hinzu:

   `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, wenn Sie noch keine haben und die Standardrichtlinie nicht 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 Recovery Point Objective in Sekunden an (optional).
   - `-throttle` – Gibt die obere Grenze für Durchsatz/Bandbreite in Kilobyte/Sekunden an (optional).

   Beispiel

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

5. Installieren Sie CA-Serverzertifikate auf der Admin-SVM:

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

   b. Installieren Sie das CA
      `security certificate install -type server-ca -vserver admin_svm -cert -name dest_server_certificate`-Zertifikat, das das *Destination* S3-Serverzertifikat auf der Admin-SVM signiert hat: + Wenn Sie ein Zertifikat verwenden, das von einem externen CA-Anbieter signiert wurde, müssen Sie dieses Zertifikat nur auf der Admin-SVM installieren.

      Erfahren Sie mehr über `security certificate install` in der "ONTAP-Befehlsreferenz".

6. Erstellen Sie eine 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 Standardeinstellung übernehmen.

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

7. Vergewissern Sie sich, dass die Spiegelung aktiv ist:
`snapmirror show -policy-type continuous -fields status`

Verwandte Informationen

- "snapmirror erstellen"
- "Snapmirror-Richtlinie erstellen"
- "Snapmirror-Show"

Erstellen einer Spiegelbeziehung für einen vorhandenen ONTAP S3-Bucket auf dem lokalen Cluster

Sie können vorhandene S3-Buckets für das gleiche Cluster jederzeit schützen, wenn Sie beispielsweise eine S3-Konfiguration von einer Version vor ONTAP 9.10.1 aktualisiert haben. Sie können Daten auf einen Bucket in einer anderen Storage-VM oder auf derselben Storage-VM wie die Quelle spiegeln.

Bevor Sie beginnen

- Die Anforderungen für ONTAP-Versionen, Lizenzierung und S3-Serverkonfiguration wurden erfüllt.
- Zwischen Quell- und Ziel-Storage-VMs besteht eine Peering-Beziehung.
- FÜR die Quell- und Ziel-VMs SIND CA-Zertifikate erforderlich. Sie können selbstsignierte CA-Zertifikate oder -Zertifikate verwenden, die von einem externen CA-Anbieter signiert wurden.

System Manager

1. Wenn dies die erste SnapMirror S3-Beziehung für diese Storage-VM ist, überprüfen Sie, ob Root-Benutzerschlüssel sowohl für Quell- als auch für Ziel-Storage-VMs vorhanden sind, und regenerieren Sie Sie sie erneut, wenn dies nicht der Fall ist:
   a. Klicken Sie auf **Storage > Storage VMs** und wählen Sie dann die Speicher-VM aus.
   b. Klicken Sie im Register **Einstellungen** auf die Kachel **S3**.
   c. Überprüfen Sie auf der Registerkarte **Benutzer**, ob für den Root-Benutzer ein Zugriffsschlüssel vorhanden ist.
   d. Wenn nicht, klicken Sie neben **root** und dann auf **regenerieren-Schlüssel**. Generieren Sie den Schlüssel nicht neu, wenn er bereits vorhanden ist
2. Überprüfen Sie, ob vorhandene Benutzer und Gruppen vorhanden sind und den richtigen Zugriff auf die Quell- und ZielspeicherVMs haben: Wählen Sie **Speicher > Speicher-VMs**, wählen Sie dann die Speicher-VM und dann **Einstellungen** Tab. Suchen Sie schließlich die Kachel **S3**, wählen Sie , und wählen Sie die Registerkarte **Benutzer** und dann die Registerkarte **Gruppen**, um die Benutzer- und Gruppenzugriffseinstellungen anzuzeigen.

   Weitere Informationen finden Sie unter "Fügen Sie S3-Benutzer und -Gruppen hinzu" .
3. Erstellen Sie eine SnapMirror S3-Richtlinie, wenn Sie noch keine haben und die Standardrichtlinie nicht verwenden möchten:
   a. Klicken Sie auf **Schutz > Übersicht** und dann auf **Lokale Richtlinieneinstellung**.
   b. Klicken Sie neben **Schutzrichtlinien** und dann auf **Hinzufügen**.
      - Geben Sie den Namen und die Beschreibung der Richtlinie ein.
      - Wählen Sie den Richtlinienumfang, das Cluster oder die SVM aus
      - Wählen Sie **kontinuierlich** für SnapMirror S3-Beziehungen aus.
      - Geben Sie Ihre **Throttle**- und **Recovery Point Objective**-Werte ein.
4. Vergewissern Sie sich, dass die Bucket-Zugriffsrichtlinie des vorhandenen Buckets nach wie vor die Anforderungen erfüllt:
   a. Klicken Sie auf **Speicher > Eimer** und wählen Sie dann den Eimer aus, den Sie schützen möchten.
   b. Klicken Sie im Register **Berechtigungen** auf **Bearbeiten** und dann unter **Berechtigungen** auf **Hinzufügen**.
      - **Principal** und **Effect** - Wählen Sie Werte aus, die Ihren Benutzergruppeneinstellungen entsprechen, oder übernehmen Sie die Standardeinstellungen.
      - **Aktionen** - stellen Sie sicher, dass die folgenden Werte angezeigt werden:

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

      - **Ressourcen** - Verwenden Sie die Standardeinstellungen *(bucketname, bucketname/*)* oder andere Werte, die Sie benötigen.

        "Management des Benutzerzugriffs auf Buckets"Weitere Informationen zu diesen Feldern finden Sie unter.

5. Schützen Sie einen vorhandenen Bucket mit SnapMirror S3:
   a. Klicken Sie auf **Storage** > **Buckets** und wählen Sie dann den Eimer aus, den Sie schützen möchten.
   b. Klicken Sie auf **Protect** und geben Sie die folgenden Werte ein:
      - Ziel
        - **ZIEL**: ONTAP-System
        - **CLUSTER**: Wählen Sie den lokalen Cluster aus.
        - **STORAGE VM**: Wählen Sie dieselbe oder eine andere Storage VM.
        - **S3-SERVER-CA-ZERTIFIKAT**: Kopieren Sie den Inhalt des *source*-Zertifikats.
      - Quelle
        - **S3-SERVER-CA-ZERTIFIKAT**: Kopieren Sie den Inhalt des *Destination*-Zertifikats.
6. Überprüfen Sie **Verwenden Sie dasselbe Zertifikat auf dem Ziel**, wenn Sie ein Zertifikat verwenden, das von einem externen CA-Anbieter signiert wurde.
7. Wenn Sie auf **Zieleinstellungen** klicken, können Sie Ihre eigenen Werte anstelle der Standardeinstellungen für Bucket-Name, -Kapazität und -Service-Level eingeben.
8. Klicken Sie Auf **Speichern**. Der vorhandene Bucket wird zu einem neuen Bucket in der Ziel-Storage-VM gespiegelt.

Sichern Sie gesperrte Buckets

Ab ONTAP 9.14.1 können Sie gesperrte S3-Buckets sichern und nach Bedarf wiederherstellen.

Wenn Sie die Schutzeinstellungen für einen neuen oder vorhandenen Bucket definieren, können Sie die Objektsperrung für Ziel-Buckets aktivieren, sofern auf den Quell- und Ziel-Clustern ONTAP 9.14.1 oder höher ausgeführt wird und die Objektsperrung auf dem Quell-Bucket aktiviert ist. Der Sperrmodus für Objekte und die Aufbewahrungsdauer der Quell-Buckets werden für die replizierten Objekte auf dem Ziel-Bucket angewendet. Sie können auch eine andere Sperrfrist für den Ziel-Bucket im Abschnitt **Zieleinstellungen** definieren. Dieser Aufbewahrungszeitraum wird auch auf alle nicht gesperrten Objekte angewendet, die aus den Quell-Bucket und S3-Schnittstellen repliziert werden.

Informationen zum Aktivieren der Objektsperrung auf einem Bucket finden Sie unter "Erstellen eines Buckets".

CLI

1. Wenn es sich hierbei um die erste SnapMirror S3-Beziehung für diese SVM handelt, überprüfen Sie, ob Root-Benutzerschlüssel für Quell- und Ziel-SVMs vorhanden sind, und regenerieren Sie sie erneut, wenn dies nicht der Fall ist:
   `vserver object-store-server user show`

   Vergewissern Sie sich, dass für den Root-Benutzer ein Zugriffsschlüssel vorhanden ist. Wenn dies nicht der Fall ist, geben Sie Folgendes ein:
   `vserver object-store-server user regenerate-keys -vserver svm_name -user root`

   Generieren Sie den Schlüssel nicht neu, wenn er bereits vorhanden ist.

2. Erstellen eines Buckets für die Ziel-SVM als Ziel-Ziel:

   `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. Vergewissern Sie sich, dass die Zugriffsregeln für die Standard-Bucket-Richtlinien sowohl in den Quell- als auch in den Ziel-SVMs 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. Erstellen Sie eine SnapMirror S3-Richtlinie, wenn Sie noch keine haben und die Standardrichtlinie nicht 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 Recovery Point Objective in Sekunden an (optional).
   - `-throttle` – Gibt die obere Grenze für Durchsatz/Bandbreite in Kilobyte/Sekunden an (optional).

     Beispiel

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

5. Installieren Sie CA-Serverzertifikate auf der Admin-SVM:

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

   b. Installieren Sie das CA
   `security certificate install -type server-ca -vserver admin_svm -cert -name dest_server_certificate`-Zertifikat, das das *Destination* S3-Serverzertifikat auf der Admin-SVM signiert hat: + Wenn Sie ein Zertifikat verwenden, das von einem externen CA-Anbieter signiert wurde, müssen Sie dieses Zertifikat nur auf der Admin-SVM installieren.

Erfahren Sie mehr über `security certificate install` in der "ONTAP-Befehlsreferenz".

6. Erstellen Sie eine 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 Standardeinstellung übernehmen.

   Beispiel

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

7. Vergewissern Sie sich, dass die Spiegelung aktiv ist:
`snapmirror show -policy-type continuous -fields status`

Verwandte Informationen

- "snapmirror erstellen"
- "Snapmirror-Richtlinie erstellen"
- "Snapmirror-Show"

Übernehmen Sie die Übernahme aus dem ONTAP S3-Zielbucket auf dem lokalen Cluster

Wenn die Daten in einem Quell-Bucket nicht mehr verfügbar sind, können Sie die SnapMirror Beziehung unterbrechen, um den Ziel-Bucket beschreibbar zu machen und mit der Bereitstellung von Daten zu beginnen.

Über diese Aufgabe

Wenn ein Takeover-Vorgang durchgeführt wird, wird Quell-Bucket in schreibgeschützt konvertiert und der ursprüngliche Ziel-Bucket in Lese-/Schreibzugriff konvertiert, um die SnapMirror S3-Beziehung rückgängig zu machen.

Wenn der deaktivierte Quell-Bucket wieder verfügbar ist, synchronisiert SnapMirror S3 den Inhalt der beiden Buckets automatisch neu. Sie müssen die Beziehung nicht explizit neu synchronisieren, wie es für standardmäßige Volume SnapMirror Implementierungen erforderlich ist.

Wenn der Ziel-Bucket auf einem Remote-Cluster liegt, muss der Takeover-Vorgang vom Remote-Cluster aus initiiert werden.

System Manager

Failover aus dem nicht verfügbaren Bucket und Beginn der Datenbereitstellung:

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

CLI

1. Initiieren Sie einen Failover-Vorgang für den Ziel-Bucket:
   `snapmirror failover start -destination-path` *`svm_name`*`:/bucket/`*`bucket_name`*
2. Überprüfen Sie den Status des Failover-Vorgangs:
   `snapmirror show -fields status`

Beispiel

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

Verwandte Informationen

- "Snapmirror-Failover-Start"
- "Snapmirror-Show"

Stellen Sie einen ONTAP S3-Bucket von der Ziel-SVM auf dem lokalen Cluster wieder her

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

Über diese Aufgabe

Sie können den Ziel-Bucket auf einem vorhandenen oder einem neuen Bucket wiederherstellen. Der Ziel-Bucket für den Wiederherstellungsvorgang muss größer sein als der logische genutzte Speicherplatz des Ziel-Buckets.

Wenn Sie einen vorhandenen Bucket verwenden, muss er beim Starten eines Wiederherstellungsvorgangs leer sein. Beim Restore wird ein Bucket nicht rechtzeitig „zurück“, sondern es füllt einen leeren Bucket mit den vorherigen Inhalten aus.

Der Wiederherstellungsvorgang muss vom lokalen Cluster aus gestartet werden.

System Manager

Wiederherstellen der Backup-Daten:

1. Klicken Sie auf **Schutz > Beziehungen** und wählen Sie dann den Bucket aus.
2. Klicken Sie auf ⋮ und wählen Sie dann **Wiederherstellen**.
3. Wählen Sie unter **Quelle vorhandener Bucket** (Standard) oder **Neuer Bucket** aus.
   - Um einen **vorhandenen Bucket** (die Standardeinstellung) wiederherzustellen, führen Sie die folgenden Aktionen aus:
     - Wählen Sie das Cluster und die Storage-VM aus, um nach dem vorhandenen Bucket zu suchen.
     - Wählen Sie den vorhandenen Bucket aus.
4. Kopieren Sie den Inhalt des S3-Zielserver-CA-Zertifikats und fügen Sie ihn ein.
   - Um einen **neuen Bucket** wiederherzustellen, geben Sie die folgenden Werte ein:
     - Der Cluster und die Storage-VM zum Hosten des neuen Buckets.
     - Name, Kapazität und Performance des neuen Bucket Weitere Informationen finden Sie unter "Storage Service Level" .
     - Der Inhalt des CA-Zertifikats des Ziel-S3-Servers.
5. Kopieren Sie unter **Destination** den Inhalt des Quell-S3-Server-CA-Zertifikats und fügen Sie ihn ein.
6. Klicken Sie auf **Schutz** > Beziehungen, um den Wiederherstellungsfortschritt zu überwachen.

Gesperrte Buckets wiederherstellen

Ab ONTAP 9.14.1 können Sie gesperrte Buckets sichern und nach Bedarf wiederherstellen.

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

- **Wiederherstellung auf einen neuen Bucket**: Wenn die Objektsperrung aktiviert ist, kann ein Bucket wiederhergestellt werden, indem ein Bucket erstellt wird, für den auch die Objektsperrung aktiviert ist. Wenn Sie einen gesperrten Bucket wiederherstellen, werden der Objektsperrmodus und der Aufbewahrungszeitraum des ursprünglichen Buckets repliziert. Sie können auch eine andere Sperrfrist für den neuen Bucket definieren. Diese Aufbewahrungsfrist wird auf nicht gesperrte Objekte aus anderen Quellen angewendet.
- **Wiederherstellung auf einen vorhandenen Bucket**: Ein Object-Locked Bucket kann in einen bestehenden Bucket wiederhergestellt werden, sofern auf dem bestehenden Bucket Versionierung und ein ähnlicher Object-Locking-Modus aktiviert sind. Die Aufbewahrungsdauer des ursprünglichen Eimers wird beibehalten.
- **Nicht gesperrte Buckets wiederherstellen**: Selbst wenn die Objektsperrung auf einem Bucket nicht aktiviert ist, können Sie sie in einem Bucket wiederherstellen, der die Objektsperrung aktiviert hat und sich auf dem Quellcluster befindet. Wenn Sie den Bucket wiederherstellen, werden alle nicht gesperrten Objekte gesperrt, und der Aufbewahrungszeitraum und die Dauer des Ziel-Buckets werden für sie anwendbar.

CLI

1. Wenn Sie Objekte in einem neuen Bucket wiederherstellen, erstellen Sie den neuen Bucket. Weitere Informationen finden Sie unter "Eine Cloud-Backup-Beziehung für einen neuen ONTAP S3 Bucket erstellen".

2. Initiieren Sie einen Wiederherstellungsvorgang für den Ziel-Bucket:
`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
```

Erfahren Sie mehr über `snapmirror restore` in der "ONTAP-Befehlsreferenz".

Backup-Sicherung mit Cloud-Zielen

Anforderungen für Cloud-Zielbeziehungen mit ONTAP SnapMirror S3

Stellen Sie sicher, dass Ihre Quell- und Zielumgebungen die Anforderungen für die SnapMirror S3-Backup-Sicherung auf Cloud-Ziele erfüllen.

Um auf den Daten-Bucket zuzugreifen, müssen Sie über gültige Kontoanmeldeinformationen beim Objektspeicher-Provider verfügen.

Intercluster LIFs und ein IPspace sollten auf dem Cluster konfiguriert werden, bevor das Cluster eine Verbindung zu einem Cloud-Objektspeicher herstellen kann. Es sollten Intercluster LIFs auf jedem Node erstellt werden, um Daten nahtlos vom lokalen Storage zum Cloud-Objektspeicher zu übertragen.

Für StorageGRID-Ziele müssen Sie die folgenden Informationen kennen:

- Servername, ausgedrückt als vollständig qualifizierter Domain-Name (FQDN) oder IP-Adresse
- Bucket-Name: Der Bucket muss bereits vorhanden sein
- Zugriffsschlüssel
- Geheimer Schlüssel

Darüber hinaus muss das CA-Zertifikat, das zum Signieren des StorageGRID-Serverzertifikats verwendet wird, auf der Admin-Storage-VM des ONTAP S3-Clusters installiert werden. Dazu wird der `security certificate install` Befehl. Weitere Informationen finden Sie unter"Installieren eines CA-Zertifikats", wenn Sie StorageGRID verwenden.

Für AWS S3 Ziele sind die folgenden Informationen erforderlich:

- Servername, ausgedrückt als vollständig qualifizierter Domain-Name (FQDN) oder IP-Adresse
- Bucket-Name: Der Bucket muss bereits vorhanden sein
- Zugriffsschlüssel
- Geheimer Schlüssel

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

Verwandte Informationen

- "Sicherheitszertifikat installieren"

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

Wenn Sie neue S3-Buckets erstellen, können Sie diese sofort in einem SnapMirror S3-Ziel-Bucket bei einem Objektspeicheranbieter sichern. Dabei kann es sich um ein StorageGRID-System oder eine Amazon S3-Bereitstellung handeln.

Bevor Sie beginnen

- Sie haben gültige Anmeldeinformationen und Konfigurationsinformationen für den Objektspeicher-Provider.
- Intercluster-Netzwerkschnittstellen und ein IPspace wurden auf dem Quellsystem konfiguriert.
- • Die DNS-Konfiguration für die Quell-Speicher-VM muss in der Lage sein, den FQDN des Ziels aufzulösen.

System Manager

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

      Weitere Informationen finden Sie unter "Fügen Sie S3-Benutzer und -Gruppen hinzu" .
2. Cloud Object Store auf dem Quellsystem hinzufügen:
   a. Klicken Sie auf **Schutz > Übersicht** und wählen Sie dann **Cloud Object Stores**.
   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 virtuell gehostet)
      - Storage-VM (aktiviert für S3)
      - Objektspeicherservername (FQDN)
      - Objektspeicherzertifikat
      - Zugriffsschlüssel
      - Geheimer Schlüssel
      - Container-Name (Bucket
3. Erstellen Sie eine SnapMirror S3-Richtlinie, wenn Sie noch keine haben und die Standardrichtlinie nicht verwenden möchten:
   a. Klicken Sie auf **Schutz > Übersicht** und dann auf **Einstellungen für lokale Richtlinien**.
   b. Klicken Sie → neben **Schutzrichtlinien** und dann auf **Hinzufügen**.
      - Geben Sie den Namen und die Beschreibung der Richtlinie ein.
      - Wählen Sie den Richtlinienumfang, das Cluster oder die SVM aus
      - Wählen Sie **kontinuierlich** für SnapMirror S3-Beziehungen aus.
      - Geben Sie Ihre **Throttle**- und **Recovery Point Objective**-Werte ein.
4. Erstellung eines Buckets mit SnapMirror Sicherung:
   a. Klicken Sie auf **Storage > Buckets** und dann auf **Hinzufügen**.
   b. Geben Sie einen Namen ein, wählen Sie die Speicher-VM aus, geben Sie eine Größe ein und klicken Sie dann auf **Weitere Optionen**.
   c. Klicken Sie unter **Berechtigungen** auf **Hinzufügen**. Die Überprüfung der Berechtigungen ist optional, wird aber empfohlen.
      - **Principal** und **effect**: Wählen Sie die Werte aus, die Ihren Benutzergruppeneinstellungen entsprechen, oder akzeptieren Sie die Standardeinstellungen.
      - **Aktionen**: Stellen Sie sicher, dass folgende Werte angezeigt werden:

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

- **Ressourcen**: Verwenden Sie die Standardwerte oder andere Werte, die `_(bucketname, bucketname/*)` Sie benötigen.

  "Management des Benutzerzugriffs auf Buckets"Weitere Informationen zu diesen Feldern finden Sie unter.

d. Aktivieren Sie unter **Schutz SnapMirror aktivieren (ONTAP oder Cloud)** die Option **Cloud-Speicher** und wählen Sie dann den **Cloud-Objektspeicher** aus.

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

CLI

1. Wenn dies die erste SnapMirror S3-Beziehung für diese SVM ist, überprüfen Sie, ob Root-Benutzerschlüssel für Quell- und Ziel-SVMs vorhanden sind, und regenerieren Sie sie, wenn sie `vserver object-store-server user show` dies nicht tun: + Bestätigen Sie, dass es einen Zugriffsschlüssel für den Root-Benutzer gibt. Wenn nicht, geben Sie ein: `vserver object-store-server user regenerate-keys -vserver svm_name -user root` + Den Schlüssel nicht neu generieren, wenn er bereits vorhanden ist.
2. Bucket in der Quell-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. Fügen Sie Zugriffsregeln zur Standard-Bucket-Richtlinie hinzu:
   `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, wenn Sie noch keine haben und die Standardrichtlinie nicht 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 für die Recovery Point Objective in Sekunden an (optional). * `-throttle` – Gibt die obere Grenze für Durchsatz/Bandbreite in Kilobyte/Sekunden an (optional).

Beispiel

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

5. Wenn es sich bei dem Ziel um ein StorageGRID-System handelt, installieren Sie das StorageGRID CA-Serverzertifikat auf der Admin-SVM des Quell-Clusters:
`security certificate install -type server-ca -vserver src_admin_svm -cert -name storage_grid_server_certificate`

   Erfahren Sie mehr über `security certificate install` in der "ONTAP-Befehlsreferenz".

6. SnapMirror S3-Zielobjektspeicher 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` -SSL zu aktivieren ist optional, aber empfohlen. + Erfahren Sie mehr über `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 Sie eine 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 Name des Objektspeichers, den Sie im vorherigen Schritt erstellt `objstore` haben, und der feste Wert. + Sie können eine Richtlinie verwenden, die Sie erstellt haben, oder die Standardvorgabe akzeptieren.

   Beispiel

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

8. Vergewissern Sie sich, dass die Spiegelung aktiv ist:
`snapmirror show -policy-type continuous -fields status`

Verwandte Informationen

- "snapmirror erstellen"
- "Snapmirror-Richtlinie erstellen"
- "Snapmirror-Show"

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

Sie können jederzeit damit beginnen, vorhandene S3-Buckets zu sichern. Wenn Sie beispielsweise eine S3-Konfiguration aus einer älteren Version als ONTAP 9.10.1 aktualisiert haben,

Bevor Sie beginnen

- Sie haben gültige Anmeldeinformationen und Konfigurationsinformationen für den Objektspeicher-Provider.
- Intercluster-Netzwerkschnittstellen und ein IPspace wurden auf dem Quellsystem konfiguriert.
- Die DNS-Konfiguration für die Quell-Speicher-VM muss in der Lage sein, den FQDN des Ziels aufzulösen.

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 klicken Sie dann unter S3.

   Weitere Informationen finden Sie unter "Fügen Sie S3-Benutzer und -Gruppen hinzu" .

2. Erstellen Sie eine SnapMirror S3-Richtlinie, wenn Sie noch keine haben und die Standardrichtlinie nicht verwenden möchten:
   a. Klicken Sie auf **Schutz > Übersicht** und dann auf **Lokale Richtlinieneinstellungen**.
   b. Klicken Sie neben **Schutzrichtlinien** und dann auf **Hinzufügen**.
   c. Geben Sie den Namen und die Beschreibung der Richtlinie ein.
   d. Wählen Sie den Richtlinienumfang, das Cluster oder die SVM aus
   e. Wählen Sie **kontinuierlich** für SnapMirror S3-Beziehungen aus.
   f. Geben Sie Ihre **Throttle**- und **Recovery Point-Zielwerte** ein.
3. Cloud Object Store auf dem Quellsystem hinzufügen:
   a. Klicken Sie auf **Schutz > Übersicht** und wählen Sie dann **Cloud Object Store**.
   b. Klicken Sie auf **Hinzufügen** und wählen Sie **Amazon S3** oder **andere** für StorageGRID Webscale.
   c. Geben Sie die folgenden Werte ein:
      - Name des Cloud-Objektspeichers
      - URL-Stil (Pfad oder virtuell gehostet)
      - Storage-VM (aktiviert für S3)
      - Objektspeicherservername (FQDN)
      - Objektspeicherzertifikat
      - Zugriffsschlüssel
      - Geheimer Schlüssel
      - Container-Name (Bucket
4. Vergewissern Sie sich, dass die Bucket-Zugriffsrichtlinie des vorhandenen Buckets nach wie vor die Anforderungen erfüllt:
   a. Klicken Sie auf **Storage** > **Buckets** und wählen Sie dann den Eimer aus, den Sie schützen möchten.
   b. Klicken Sie im Register **Berechtigungen** auf **Bearbeiten** und dann unter **Berechtigungen** auf **Hinzufügen**.
      - **Principal** und **Effect** - Wählen Sie Werte aus, die Ihren Benutzergruppeneinstellungen entsprechen, oder übernehmen Sie die Standardeinstellungen.
      - **Actions** - Stellen Sie sicher, dass die folgenden Werte angezeigt werden: `GetObject,PutObject,DeleteObject,ListBucket,GetBucketAcl,GetObjectAcl,ListBucketMultipartUploads,ListMultipartUploadParts`
      - **Ressourcen** - Verwenden Sie die Standardeinstellungen *(bucketname, bucketname/*)* oder andere Werte, die Sie benötigen.

"Management des Benutzerzugriffs auf Buckets"Weitere Informationen zu diesen Feldern finden Sie unter.

5. Backup des Buckets mit SnapMirror S3:
   a. Klicken Sie auf **Storage** > **Buckets** und wählen Sie dann den Eimer aus, den Sie sichern möchten.
   b. Klicken Sie auf **Protect**, wählen Sie **Cloud Storage** unter **Target** und wählen Sie dann den **Cloud Object Store** aus.

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

CLI

1. Überprüfen Sie, 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, wenn Sie noch keine haben und die Standardrichtlinie nicht 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 für die Recovery Point Objective in Sekunden an (optional). * `-throttle` – Gibt die obere Grenze für Durchsatz/Bandbreite in Kilobyte/Sekunden an (optional).

   Beispiel

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

3. Wenn es sich bei dem Ziel um ein StorageGRID-System handelt, installieren Sie das StorageGRID CA-Zertifikat auf der Admin-SVM des Quell-Clusters:
   `security certificate install -type server-ca -vserver src_admin_svm -cert -name storage_grid_server_certificate`

   Erfahren Sie mehr über `security certificate install` in der "ONTAP-Befehlsreferenz".

4. SnapMirror S3-Zielobjektspeicher 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` -SSL zu aktivieren ist optional, aber empfohlen. + Erfahren Sie mehr über `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 Sie eine 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 Name des Objektspeichers, den Sie im vorherigen Schritt erstellt `objstore` haben, und der feste Wert. + Sie können eine Richtlinie verwenden, die Sie erstellt haben, oder die Standardvorgabe akzeptieren.

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

6. Vergewissern Sie sich, dass die Spiegelung aktiv ist:
`snapmirror show -policy-type continuous -fields status`

Verwandte Informationen

- "snapmirror erstellen"
- "Snapmirror-Richtlinie erstellen"
- "Snapmirror-Show"

Wiederherstellung eines ONTAP S3-Buckets aus einem Cloud-Ziel

Wenn Daten in einem Quell-Bucket verloren gehen oder beschädigt sind, können Sie Ihre Daten neu befüllen, indem Sie sie von einem Ziel-Bucket wiederherstellen.

Über diese Aufgabe

Sie können den Ziel-Bucket auf einem vorhandenen oder einem neuen Bucket wiederherstellen. Der Ziel-Bucket für den Wiederherstellungsvorgang muss größer sein als der logische verwendete Speicherplatz des Ziels.

Wenn Sie einen vorhandenen Bucket verwenden, muss er beim Starten eines Wiederherstellungsvorgangs leer sein. Beim Restore wird ein Bucket nicht rechtzeitig „zurück“, sondern es füllt einen leeren Bucket mit den vorherigen Inhalten aus.

System Manager

Wiederherstellen der Backup-Daten:

1. Klicken Sie auf **Schutz > Beziehungen**, und wählen Sie dann **SnapMirror S3** aus.
2. Klicken Sie auf ⋮ und wählen Sie dann **Wiederherstellen**.
3. Wählen Sie unter **Quelle vorhandener Bucket** (Standard) oder **Neuer Bucket** aus.
   - Um einen **vorhandenen Bucket** (die Standardeinstellung) wiederherzustellen, führen Sie die folgenden Aktionen aus:
     - Wählen Sie das Cluster und die Storage-VM aus, um nach dem vorhandenen Bucket zu suchen.
     - Wählen Sie den vorhandenen Bucket aus.
     - Kopieren Sie den Inhalt des CA-Zertifikats des *Destination* S3-Servers und fügen Sie ihn ein.
   - Um einen **neuen Bucket** wiederherzustellen, geben Sie die folgenden Werte ein:
     - Der Cluster und die Storage-VM zum Hosten des neuen Buckets.
     - Der Name, die Kapazität und das Performance-Service-Level des neuen Buckets. Weitere Informationen finden Sie unter "Storage Service Level" .
     - Der Inhalt des CA-Zertifikats des Ziel-S3-Servers.
4. Kopieren Sie unter **Destination** den Inhalt des CA-Zertifikats *source* S3-Server.
5. Klicken Sie auf **Schutz > Beziehungen**, um den Wiederherstellungsfortschritt zu überwachen.

CLI-Verfahren

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

   Beispiel

   Im folgenden Beispiel wird ein Ziel-Bucket in einem vorhandenen Bucket wiederhergestellt.

   ```
   clusterA::> snapmirror restore -source-path sgws.store:/objstore
   -destination-path vs0:/bucket/test-bucket
   ```

   Erfahren Sie mehr über `snapmirror restore` in der "ONTAP-Befehlsreferenz".

ONTAP SnapMirror S3-Richtlinie ändern

Sie können eine S3-SnapMirror-Richtlinie ändern, wenn Sie RPO und Drosselungswerte anpassen möchten.

System Manager

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

CLI

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

Parameter:

- `-rpo`: Gibt die Zeit für den Wiederherstellungspunkt in Sekunden an.
- `-throttle`: Gibt die obere Grenze für Durchsatz/Bandbreite in Kilobyte/Sekunden an.

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

Verwandte Informationen

- "Snapmirror-Richtlinie ändern"

Sicherung von S3 Daten mit Snapshots

Erfahren Sie mehr über ONTAP S3 Snapshots

Ab der Version ONTAP 9.16.1 können Sie ONTAP Snapshot Technologie verwenden, um schreibgeschützte, zeitpunktgenaue Images Ihrer ONTAP S3 Buckets zu generieren.

Mit der S3-Snapshot-Funktion können Sie Snapshots manuell erstellen oder automatisch durch Snapshot-Richtlinien generieren. S3-Snapshots werden S3-Clients als S3-Buckets bereitgestellt. Sie können den Inhalt aus den Snapshots über S3-Clients durchsuchen und wiederherstellen.

In ONTAP 9.16.1 erfassen S3 Snapshots 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 Point-in-Time-Objekttags in den Snapshots nicht erfasst, wenn die Objekt-Tags nach der Erstellung der Snapshots geändert werden.

S3 Snapshots basieren auf der Cluster-Zeit. Sie sollten den NTP-Server im Cluster so konfigurieren, dass die Zeit synchronisiert wird. Weitere Informationen finden Sie unter "Verwalten der Cluster-Zeit".

Kontingente und Speicherplatznutzung

Quoten verfolgen die Anzahl der Objekte und die logische Größe, die in einem S3-Bucket verwendet werden. Bei der Erstellung von S3-Snapshots werden die in den S3-Snapshots erfassten Objekte auf die Anzahl und Größe der verwendeten Bucket-Objekte angerechnet, bis die Snapshots aus dem Filesystem gelöscht werden.

Mehrteilige Objekte

Bei mehrteiligen Objekten werden nur die endgültigen Objekte in Snapshots erfasst. Teilweise Uploads von mehrteiligen Objekten werden nicht in Snapshots erfasst.

Snapshots in versionierten und nichtversionierten Buckets

Sie können Snapshots sowohl für versionierte als auch für nichtversionierte Buckets erstellen. Der Snapshot enthält nur die aktuellen Objektversionen zu einem Zeitpunkt, zu dem der Snapshot erfasst wird.

Versionierte Buckets und Snapshots

In Buckets mit aktivierter Objektversionierung behält ein Snapshot den Inhalt der letzten Objektversion bei, nach der der Snapshot erstellt wurde. Nicht aktuelle Versionen im Bucket werden ausgeschlossen.

Betrachten wir dieses Beispiel: In einem Bucket, auf dem die Objektversionierung aktiviert ist, weist das Objekt `obj1` die Versionen v1, v2, v3, v4 und v5 auf. Sie haben einen Snapshot von `obj1` v3 (der neuesten Version am Erfassungspunkt) erstellt `snap1`. Beim Browsen `snap1` erscheint , `obj1` als Objekt mit Inhalt, der bei v3 erstellt wurde. Der Inhalt der vorherigen Versionen wird 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 Snapshot-Erstellung bei.

Betrachten Sie dieses Beispiel: In einem Bucket, bei dem die Objektversionierung nicht verfügbar ist, wurde das Objekt `obj1` mehrfach überschrieben (t1, t2, t3, t4 und t5). Sie haben irgendwann zwischen t3 und t4 einen S3-Snapshot erstellt `snap1`. Beim Browsen `snap1` `obj1` wird mit dem bei t3 erstellten Inhalt angezeigt.

Objektablauf und Snapshots

ONTAP S3 Objektablauf und S3 Snapshots funktionieren unabhängig voneinander. Die ONTAP Objektverfallsfunktion läuft Objektversionen gemäß den für den S3-Bucket definierten Lifecycle-Managementregeln ab. S3 Snapshots sind statische Kopien von Bucket-Objekten zu einem Zeitpunkt, zu dem der Snapshot erstellt wurde.

Wenn die Objektversionierung in einem Bucket aktiviert ist und eine bestimmte Version eines Objekts aufgrund einer für diesen Bucket definierten Ablaufregel gelöscht wird, bleibt der Inhalt der abgelaufenen Objektversion weiterhin im Dateisystem, wenn die Version in einem oder mehreren S3-Snapshots als aktuelle Version erfasst wurde. Diese Objektversion wird im Dateisystem nur dann nicht mehr existieren, wenn dieser Snapshot gelöscht wird.

Gleichermaßen wird das Objekt in einem Bucket, in dem die Versionierung deaktiviert ist, auf der Grundlage einer Ablaufregel gelöscht, aber in einigen vorhandenen S3-Snapshots noch erfasst, im Dateisystem beibehalten. Das Objekt wird dauerhaft aus dem Dateisystem entfernt, wenn die Snapshots, die es erfassen, gelöscht werden.

Weitere Informationen über S3-Objektablauf und Lifecycle-Management finden Sie unter "Erstellen einer Bucket-Lifecycle-Management-Regel".

Beschränkungen bei S3 Snapshots

Beachten Sie die folgenden Funktionsausschlüsse und -Szenarien in ONTAP 9.16.1:

- Sie können bis zu 1023 Snapshots für einen S3-Bucket generieren.
- Es ist erforderlich, alle S3-Snapshots und -Metadaten aus allen Buckets eines Clusters zu löschen, bevor das Cluster auf eine ONTAP-Version vor ONTAP 9 zurückgesetzt wird.16.1.
- Wenn Sie einen S3-Bucket löschen müssen, der Objekte mit Snapshots enthält, stellen Sie sicher, dass Sie alle entsprechenden Snapshots aller Objekte in diesem Bucket gelöscht haben.
- S3-Snapshots werden in diesen Konfigurationen nicht unterstützt:
  - Für Buckets in einer SnapMirror-Beziehung
  - In Buckets, für die die Objektsperrung aktiviert ist
  - Auf der NetApp Konsole
  - Auf System Manager
  - In ONTAP MetroCluster-Konfigurationen zu verschieben
- Für Buckets, die als lokale oder Remote FabricPool Kapazitätsebene verwendet werden, werden S3-Snapshots nicht empfohlen.

Erstellen Sie ONTAP S3 Snapshots

Sie können S3-Snapshots manuell generieren oder Snapshot-Richtlinien zur automatischen Erstellung von S3-Snapshots einrichten. Snapshots dienen als statische Kopien von Objekten, die Sie für Daten-Backup und -Recovery verwenden. Zur Bestimmung der Dauer der Snapshot-Aufbewahrung können Sie Snapshot-Richtlinien erstellen, die die automatische Snapshot-Erstellung in festgelegten Intervallen erleichtern.

S3 Snapshots unterstützen Sie beim Schutz Ihrer Objektdaten in S3 Buckets, bei denen die Objektversionierung aktiviert ist oder nicht.

Snapshots können besonders beim Einrichten der Datensicherung nützlich sein, wenn die Objektversionierung in einem S3-Bucket nicht aktiviert ist, da sie als zeitpunktgenaue Datensätze fungieren, die Sie für Restore-Vorgänge verwenden können, wenn keine vorherige Objektversion verfügbar ist.

Über diese Aufgabe

- Für Snapshots gelten die folgenden Benennungsregeln (sowohl für manuelle als auch automatische Snapshots):
  - S3-Snapshot-Namen können bis zu 30 Zeichen lang sein
  - S3 Snapshot-Namen können nur aus Kleinbuchstaben, Zahlen, Punkten (.) und Bindestrichen (-) bestehen.
  - S3-Snapshot-Namen müssen mit einem Buchstaben oder einer Zahl enden
  - S3-Snapshot-Namen dürfen keine Teilzeichenfolge enthalten `s3snap`
- Im Kontext des S3-Protokolls beschränken die Namensbeschränkungen für Bucket-Namen einen Bucket-Namen auf 63 Zeichen. Da ONTAP S3-Snapshots über das S3-Protokoll als Buckets dargestellt werden, gelten für die Snapshot-Bucket-Namen ähnliche Einschränkungen. Standardmäßig wird der ursprüngliche Bucket-Name als Basis-Bucket-Name verwendet.
- Um einfacher zu identifizieren, welcher Snapshot zu welchem Bucket gehört, besteht der Snapshot-Bucket-Name aus dem Basis-Bucket-Namen, zusammen mit einem speziellen String, `-s3snap-` der dem

Snapshot-Namen vorangestellt ist. Die Snapshot-Bucket-Namen sind als formatiert `<base_bucket_name>-s3snap-<snapshot_name>`.

Wenn Sie zum Erstellen auf `bucket-a` beispielsweise den folgenden Befehl ausführen `snap1`, wird ein Snapshot-Bucket mit dem Namen erstellt `bucket-a-s3snap-snap1`, der Ihnen über S3-Clients zugänglich ist, wenn Sie über die Berechtigungen zum Zugriff auf den Basis-Bucket verfügen.

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

- Sie können keinen Snapshot erstellen, der zu einem Snapshot-Bucket-Namen mit mehr als 63 Zeichen führt.
- Der automatische Snapshot-Name enthält den Richtlinienplannamen und den Zeitstempel, der der Namenskonvention für die herkömmlichen Volume-Snapshots ähnlich ist. Die geplanten Snapshot-Namen können beispielsweise und `hourly-2024-05-22-1105` sein `daily-2024-01-01-0015`.

S3-Snapshots manuell erstellen

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

Schritte

1. Erstellen eines S3-Snapshots:

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

Im folgenden Beispiel wird ein Snapshot mit dem Namen auf der `vs0` Storage-VM und `website-data` dem Bucket erstellt `pre-update`:

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

Weisen Sie eine S3-Snapshot-Richtlinie einem Bucket zu

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 in der Regel die Zeitpläne zum Erstellen von Snapshots, die Anzahl der Kopien, die für jeden Zeitplan aufbewahrt werden sollen, und das Präfix für den Zeitplan fest. Eine Richtlinie kann beispielsweise jeden Tag um 12:10 UHR einen S3-Snapshot erstellen, die beiden neuesten Kopien beibehalten und mit benennen. `daily-<timestamp>`

Mit der Snapshot-Standardrichtlinie wird Folgendes beibehalten:

- 6 stündliche Snapshots

- Zwei tägliche Snapshots
- Zwei wöchentliche Schnappschüsse

Bevor Sie beginnen

- Bevor Sie sie dem S3-Bucket zuweisen, muss eine Snapshot-Richtlinie erstellt worden sein.

> Für S3-Snapshots gelten dieselben Regeln wie für andere ONTAP-Snapshot-Richtlinien. Allerdings kann eine Snapshot-Richtlinie mit einer in einem der Snapshot-Zeitpläne konfigurierten Aufbewahrungsfrist einem S3-Bucket nicht zugewiesen werden.

Weitere Informationen zum Erstellen von Snapshot-Richtlinien zum automatischen Erstellen von Snapshots finden Sie unter "Konfigurieren Sie eine Übersicht über benutzerdefinierte Snapshot-Richtlinien".

Schritte

1. Weisen Sie die Snapshot-Richtlinie für Ihren Bucket zu:

```
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>
```

> Wenn Sie ein Cluster auf eine ONTAP-Version vor ONTAP 9.16.1 zurücksetzen müssen, stellen Sie sicher, dass der Wert für `snapshot-policy` alle Buckets auf (oder `-`) gesetzt ist `none`.

Verwandte Informationen

"Erfahren Sie mehr über ONTAP S3 Snapshots"

Anzeigen und Wiederherstellen von ONTAP S3 Snapshots

Ab ONTAP 9.16.1 können Sie S3-Snapshot-Daten für Ihre Buckets von S3-Clients aus anzeigen und durchsuchen. Ab ONTAP 9.18.1 ist der S3-Snapshot-Bucket nativ über die ONTAP CLI zugänglich. Darüber hinaus können Sie auf einem S3-Client aus einem S3-Snapshot ein einzelnes Objekt, eine Gruppe von Objekten oder einen ganzen Bucket wiederherstellen.

Bevor Sie beginnen

- Alle Knoten im Cluster müssen ONTAP 9.18.1 oder höher ausführen, bevor Sie die Wiederherstellung des Bucket-Snapshots nativ in der ONTAP -CLI durchführen können. 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-Snapshot-Funktion grundlegende Snapshot-Funktionalität für ONTAP

S3-Buckets, einschließlich der manuellen und geplanten Erstellung und Löschung von Snapshots, Snapshot-Richtlinien für S3-Buckets und des clientseitigen Durchsuchens von S3-Snapshots.

Ab ONTAP 9.18.1 wird die native Wiederherstellung von ONTAP -Snapshots unterstützt, wodurch ONTAP Administratoren eine Point-in-Time-Wiederherstellungsfunktion erhalten, ohne einen S3-Browser verwenden zu müssen. Im Snapshot wird nur die aktuelle Bucket-Version erfasst. Der Versionsverlauf wird nicht erfasst und kann auch durch die Wiederherstellung des S3-Snapshots nicht wiederhergestellt werden.

Listen Sie S3 Snapshots auf und zeigen Sie sie an

Sie können die S3-Snapshot-Details anzeigen, vergleichen und Fehler identifizieren. Über die ONTAP-CLI können Sie alle Snapshots auflisten, die auf den S3-Buckets erstellt wurden.

Schritte

1. S3-Snapshots auflisten:

   ```
   vserver object-store-server bucket snapshot show
   ```

   Sie können die Snapshot-Namen, Speicher-VMs, Buckets, Erstellungszeiten und Instanz-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>
   ```

Durchsuchen von S3-Snapshots

Falls Ausfälle oder Probleme in Ihrer Umgebung auftreten, können Sie die Inhalte der S3-Bucket-Snapshots durchsuchen, um die Fehler zu identifizieren. Sie können auch die S3 Snapshots durchsuchen, um zu ermitteln, welche fehlerfreien Inhalte wiederhergestellt werden sollen.

S3-Snapshots werden S3-Clients als Snapshot-Buckets präsentiert. Der Name des Snapshot-Buckets hat folgendes Format: `<base_bucket_name>-s3snap-<snapshot_name>` Die Sie können alle Snapshot-Buckets in einer Speicher-VM mithilfe von `ListBuckets` S3-API-Operation.

Der S3-Snapshot-Bucket erbt die Zugriffsrichtlinien des Basis-Buckets und unterstützt ausschließlich Leseoperationen. Lösch- und Schreibvorgänge sind verboten. Wenn Sie über Berechtigungen für den Zugriff auf den Basis-Bucket verfügen, können Sie auch schreibgeschützte S3-API-Operationen auf dem S3-Snapshot-Bucket durchführen, wie zum Beispiel `HeadObject` , `GetObject` , `GetObjectTagging` , `ListObjects` , `ListObjectVersions` , `GetObjectAcl` , Und `CopyObject` Die

> Der `CopyObject` Vorgang wird auf einem S3-Snapshot-Bucket unterstützt, nur wenn es sich um einen Snapshot des Quell-Buckets handelt, und nicht, wenn es sich um das Storage-Ziel des Snapshots handelt.

Weitere Informationen zu diesen Vorgängen finden Sie unter "Von ONTAP S3 unterstützte Aktionen".

Einen Bucket aus S3-Snapshots mit ONTAP wiederherstellen

Ab ONTAP 9.18.1 können Sie mit der ONTAP CLI einen gesamten Bucket mithilfe eines ONTAP S3-Snapshots wiederherstellen. Sie können nur die Version des Buckets wiederherstellen, die zum Zeitpunkt der Erstellung des ausgewählten Snapshots existierte.

Schritte

1. Wählen Sie den Snapshot aus, den Sie zum Wiederherstellen des Buckets verwenden möchten:

```
vserver object-store-server bucket snapshot show
```

2. Bucket wiederherstellen:

```
vserver object-store-server bucket snapshot restore start -vserver
<storage VM name> -bucket <bucket name> -snapshot <snapshot name>
```

Daten aus S3-Bucket-Snapshots mithilfe eines S3-Clients wiederherstellen

Zusätzlich zur Wiederherstellung eines kompletten Buckets in ONTAP können Sie auch ein einzelnes Objekt, eine Gruppe von Objekten oder einen kompletten Bucket aus einem S3-Snapshot mithilfe eines S3-Clients wie S3cmd oder S3 Browser wiederherstellen.

"Erfahren Sie mehr über versionierte und nicht versionierte Snapshots."

Sie können den gesamten Bucket, Objekte mit einem bestimmten Präfix oder ein einzelnes Objekt mithilfe der Funktion wiederherstellen. `aws s3 cp` Befehl.

Schritte

1. Erstellen Sie einen Snapshot des Basis-S3-Buckets.

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

2. Stellen Sie den Basis-Bucket mithilfe des folgenden Snapshots wieder her:
   - Stellen Sie einen gesamten Bucket wieder her. Verwenden Sie den Snapshot Bucket-Namen im Format `<base_bucket_name>-s3snap-<snapshot_name>`.

```
aws --endpoint http://<IP> s3 cp s3://<snapshot-bucket-name>
s3://<base-bucket>  --recursive
```

   - Wiederherstellen von Objekten in einem Verzeichnis mit dem Präfix `dir1`:

```
aws --endpoint http://<IP> s3 cp s3://<snapshot-bucket-name>/dir1
s3://<base_bucket_name>/dir1 --recursive
```

- Ein einzelnes Objekt mit dem Namen wiederherstellen `web.py`:

```
aws --endpoint http://<IP> s3 cp s3:// <snapshot-bucket-name>/web.py
s3://<base_bucket_name>/web.py
```

Löschen Sie ONTAP S3 Snapshots

Sie können nicht mehr benötigte S3-Snapshots löschen und Speicherplatz in Ihren Buckets freigeben. Sie können S3-Snapshots manuell entfernen oder die Snapshot-Richtlinien, die den S3-Buckets zugeordnet sind, ändern, um die Anzahl der für einen Zeitplan einzubehaltenden Snapshots zu ändern.

Snapshot-Richtlinien für S3-Buckets folgen denselben Löschregeln wie die herkömmlichen Snapshot-Richtlinien für ONTAP. Weitere Informationen zum Erstellen von Snapshot-Richtlinien finden Sie unter "Erstellen einer Snapshot-Richtlinie".

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 nach dem Löschen des letzten Snapshot, der es schützt, aus dem Dateisystem entfernt.
- 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 Sie ein Cluster auf eine ONTAP-Version vor ONTAP 9.16.1 zurücksetzen müssen, stellen Sie sicher, dass Sie alle S3-Snapshots für alle Buckets gelöscht haben. Unter Umständen müssen Sie den Befehl auch ausführen `vserver object-store-server bucket clear-snapshot-metadata`, um die Snapshot-Metadaten für einen S3 Bucket zu entfernen. Weitere Informationen finden Sie unter "Löschen Sie die S3 Snapshots-Metadaten".
- Wenn Sie Snapshots in Stapeln löschen, können Sie eine große Anzahl von Objekten entfernen, die in mehreren Snapshots erfasst wurden. Dadurch wird effektiv mehr Speicherplatz freigegeben, als durch eine einzelne Snapshot-Löschung verursacht werden würde. Dadurch können Sie mehr Speicherplatz für Ihre Storage-Objekte zurückgewinnen.

Schritte

1. Führen Sie den folgenden Befehl aus, um einen bestimmten S3-Snapshot zu löschen:

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

2. Führen Sie den folgenden Befehl aus, um alle S3-Snapshots in einem Bucket zu entfernen:

```
vserver object-store-server bucket snapshot delete -vserver <svm_name>
-bucket <bucket_name> -snapshot *
```

Löschen Sie die S3 Snapshots-Metadaten

Mit S3 Snapshots werden auch Snapshot-Metadaten in einem Bucket generiert. Die Snapshot-Metadaten befinden sich weiterhin im Bucket, selbst wenn alle Snapshots entfernt wurden. Das Vorhandensein von Snapshot-Metadaten blockiert die folgenden Vorgänge:

- Setzen Sie das Cluster auf eine ältere ONTAP-Version als ONTAP 9.16.1 zurück
- Konfiguration von SnapMirror S3 auf dem Bucket

Bevor Sie diese Vorgänge ausführen, sollten Sie alle Snapshot-Metadaten aus dem Bucket löschen.

Bevor Sie beginnen

Vergewissern Sie sich, dass Sie alle S3-Snapshots aus einem Bucket entfernt haben, bevor Sie mit dem Löschen der Metadaten beginnen.

Schritte

1. Führen Sie den folgenden Befehl aus, um die Snapshot-Metadaten aus einem Bucket zu löschen:

```
vserver object-store-server bucket clear-snapshot-metadata -vserver
<svm_name> -bucket <bucket_name>
```

Prüfung von S3-Ereignissen

Hier erhalten Sie Informationen über das Auditing von ONTAP S3 Ereignissen

Ab ONTAP 9.10.1 können Daten- und Managementereignisse in ONTAP S3 Umgebungen geprüft werden. Die S3-Audit-Funktion ähnelt den vorhandenen NAS-Audit-Funktionen. Zudem können S3- und NAS-Audits in einem Cluster nebeneinander bestehen.

Wenn Sie eine S3-Audit-Konfiguration auf einer SVM erstellen und aktivieren, werden S3-Ereignisse in einer Protokolldatei aufgezeichnet. Sie können die folgenden Ereignisse angeben, die protokolliert werden sollen:

Objektzugriffsereignisse (Daten) nach Freigabe

9.11.1:

- ListBucketVersions
- ListBucket (ListObjects von 9.10.1 wurde in dieses umbenannt)
- ListAllMyBuckets (ListBuckets von 9.10.1 wurde in diese umbenannt)

9.10.1:

- HeadObject
- GetObject
- PutObject
- DeleteObject
- ListBuchs
- ListObjekte
- MPUpload
- MPUploadPart
- MPComplete
- MPAbort
- GetObjectTagging
- DeleteObjectTagging
- PutObjectTagging
- ListUploads
- ListenTeile

Management-Ereignisse nach Freigabe

9.15.1:

- GetBucketCORS
- PutBucketCORS
- DeleteBucketCORS

9.14.1:

- GetObjectRetention
- PutObjectRetention
- PutBucketObjectLockKonfiguration
- GetBucketObjectLockKonfiguration

9.13.1:

- PutBucketLifecycle
- DeleteBucketLifecycle
- GetBucketLifecycle

9.12.1:

- GetBucketPolicy
- CopyObject
- UploadPartCopy
- PutBucketPolicy

- DeleteBucketRichtlinien

9.11.1:

- GetBucketVersioning
- PutBucketVersioning

9.10.1:

- HeadBucket
- GetBucketAcl
- GetObjectAcl
- PutBucket
- DeleteBucket
- ModifyObjectTagging
- GetBucketLocation

Das Protokollformat ist JavaScript Object Notation (JSON).

Der kombinierte Grenzwert für S3- und NFS-Audit-Konfigurationen beträgt 400 SVMs pro Cluster.

Die folgende Lizenz ist erforderlich:

- ONTAP One – ehemals Teil des Kernpakets – für ONTAP S3 Protokoll und Storage

Weitere Informationen finden Sie unter "Funktionsweise des ONTAP-Prüfprozesses".

Garantierte Audits

S3- und NAS-Audits sind standardmäßig gewährleistet. ONTAP garantiert, dass alle prüffähigen Bucket-Zugriffsereignisse aufgezeichnet werden, selbst wenn ein Node nicht verfügbar ist. Ein angeforderter Bucket-Vorgang kann erst abgeschlossen werden, wenn der Prüfdatensatz für diesen Vorgang im Staging-Volume auf persistentem Storage gespeichert wird. Wenn Audit-Datensätze nicht in den Staging-Dateien übergeben werden können, entweder aufgrund von unzureichendem Speicherplatz oder wegen anderer Probleme, werden Client-Vorgänge verweigert.

Speicherplatzanforderungen für Auditing

Im ONTAP-Auditersystem werden die Audit-Datensätze zunächst in binären Staging-Dateien auf einzelnen Knoten gespeichert. Sie werden in regelmäßigen Abständen konsolidiert und in benutzerlesbare Ereignisprotokolle umgewandelt, die im Verzeichnis der Auditereignisse für die SVM gespeichert sind.

Die Staging-Dateien werden in einem dedizierten Staging-Volume gespeichert, das von ONTAP beim Erstellen der Audit-Konfiguration erstellt wird. Es gibt ein Staging-Volume pro Aggregat.

In der Überwachungskonfiguration müssen ausreichend Platz vorhanden sein:

- Für die Staging-Volumes in Aggregaten, die geprüfte Buckets enthalten
- Für das Volume, das das Verzeichnis enthält, in dem konvertierte Ereignisprotokolle gespeichert werden.

Sie können die Anzahl der Ereignisprotokolle und damit den verfügbaren Speicherplatz im Volume mit einer von zwei Methoden zum Erstellen der S3-Überwachungskonfiguration steuern:

- Ein numerischer Grenzwert; der `-rotate-limit` Parameter steuert die Mindestanzahl an Audit-Dateien, die beibehalten werden müssen.
- Ein Zeitlimit; der `-retention-duration` Parameter steuert den maximalen Zeitraum, in dem Dateien aufbewahrt werden können.

In beiden Parametern können nach dem Überschreiten der Konfiguration ältere Audit-Dateien gelöscht werden, um Platz für neuere zu schaffen. Für beide Parameter ist der Wert 0, was bedeutet, dass alle Dateien gepflegt werden müssen. Um ausreichend Platz zu gewährleisten, empfiehlt es sich daher, einen der Parameter auf einen Wert ohne Null zu setzen.

Aus Gründen der garantierten Prüfung kann es nicht möglich sein, neue Audit-Daten zu erstellen, wenn der für Audit-Daten verfügbare Speicherplatz vor dem jeweiligen Rotationslimit überschritten wird, was zu einem Ausfall des Clients, der auf Daten zugreift, führt. Daher muss die Auswahl dieses Werts und des Platzes, der für die Prüfung zugewiesen wird, sorgfältig ausgewählt werden, und Sie müssen auf Warnungen über den verfügbaren Speicherplatz des Auditsystems reagieren.

Weitere Informationen finden Sie unter "Grundlegende Prüfungskonzepte".

Planen Sie eine ONTAP S3 Auditing-Konfiguration

Sie müssen eine Reihe von Parametern für die S3-Überwachungskonfiguration angeben oder die Standardeinstellungen akzeptieren. Insbesondere sollten Sie berücksichtigen, welche Protokollrotationsparameter dazu beitragen, ausreichend freien Speicherplatz zu gewährleisten.

Erfahren Sie mehr über `vserver object-store-server audit create` in der "ONTAP-Befehlsreferenz".

Allgemeine Parameter

Es gibt zwei erforderliche Parameter, die Sie beim Erstellen der Überwachungskonfiguration angeben müssen. Es gibt außerdem drei optionale Parameter, die Sie angeben können.

Informationstyp	Option	Erforderlich
SVM Name Name der SVM, auf der die Audit-Konfiguration erstellt werden soll. Die SVM muss bereits vorhanden und für S3 aktiviert sein.	`-vserver` *`svm_name`*	Ja.
Zielpfad protokollieren Gibt an, wo die konvertierten Audit-Protokolle gespeichert werden. Der Pfad muss auf der SVM bereits vorhanden sein. Der Pfad kann bis zu 864 Zeichen lang sein und muss über Lese-/Schreibberechtigungen verfügen. Wenn der Pfad nicht gültig ist, schlägt der Befehl für die Prüfungskonfiguration fehl.	`-destination` *`text`*	Ja.

Kategorien von Ereignissen zur Prüfung Folgende Ereigniskategorien können geprüft werden: • Data GetObject, PutObject und DeleteObject Ereignisse • Management-Events „PutBucket“ und „DeleteBucket“ Standardmäßig werden nur Datenereignisse geprüft.	`-events {data|management}, …`	Nein

Sie können einen der folgenden Parameter eingeben, um die Anzahl der Audit-Log-Dateien zu steuern. Wenn kein Wert eingegeben wird, bleiben alle Protokolldateien erhalten.

Informationstyp	Option	Erforderlich
Log-Dateien Rotationsgrenze Legt fest, wie viele Audit-Log-Dateien gespeichert werden sollen, bevor die älteste Protokolldatei ausgedreht wird. Wenn Sie beispielsweise einen Wert von 5 eingeben, werden die letzten fünf Protokolldateien beibehalten. Der Wert 0 gibt an, dass alle Protokolldateien aufbewahrt werden. Der Standardwert ist 0.	`-rotate-limit` *`integer`*	Nein
Dauer der Protokolldateien Legt fest, wie lange eine Protokolldatei aufbewahrt werden kann, bevor sie gelöscht wird. Wenn Sie beispielsweise einen Wert von 5d0h0m eingeben, werden Protokolle gelöscht, die älter als 5 Tage sind. Der Wert 0 gibt an, dass alle Protokolldateien aufbewahrt werden. Der Standardwert ist 0.	`-retention duration` *`integer_time`*	Nein

Parameter für die Drehung des Prüfprotokolls

Sie können Prüfprotokolle basierend auf Größe oder Zeitplan drehen. Standardmäßig werden Auditprotokolle auf der Grundlage der Größe gedreht.

Drehen Sie Protokolle basierend auf der Protokollgröße

Wenn Sie die Standard-Protokollrotation-Methode und die Standard-Protokollgröße verwenden möchten, müssen Sie keine spezifischen Parameter für die Protokollrotation konfigurieren. Die Standard-Protokollgröße beträgt 100 MB.

Wenn Sie die Standard-Protokollgröße nicht verwenden möchten, können Sie den `-rotate-size` Parameter so konfigurieren, dass eine benutzerdefinierte Protokollgröße angegeben wird.

Wenn Sie die Rotation allein anhand einer Protokollgröße zurücksetzen möchten, verwenden Sie den folgenden Befehl, um die Einstellung des `-rotate-schedule-minute` Parameters aufzuheben:

```
vserver audit modify -vserver svm_name -destination / -rotate-schedule-minute -
```

Protokolle nach einem Zeitplan drehen

Wenn Sie die Prüfprotokolle nach einem Zeitplan drehen möchten, können Sie die Protokollrotation mithilfe der zeitbasierten Rotationsparameter in beliebiger Kombination planen.

- Wenn Sie `-rotate-schedule-minute` eine zeitbasierte Rotation verwenden, ist der Parameter obligatorisch.
- Alle anderen zeitbasierten Rotationsparameter sind optional.
  - `-rotate-schedule-month`
  - `-rotate-schedule-dayofweek`
  - `-rotate-schedule-day`
  - `-rotate-schedule-hour`
- Der Rotationsplan wird unter Verwendung aller zeitbezogenen Werte berechnet. Wenn Sie beispielsweise nur den `-rotate-schedule-minute` Parameter angeben, werden die Audit-Log-Dateien basierend auf den an allen Wochentagen festgelegten Minuten gedreht, während aller Stunden an allen Monaten des Jahres.
- Wenn Sie nur einen oder zwei zeitbasierte Rotationsparameter angeben (z. B. `-rotate-schedule -month` und `-rotate-schedule-minutes`), werden die Protokolldateien basierend auf den Minutenwerten gedreht, die Sie an allen Wochentagen, zu allen Stunden, aber nur während der angegebenen Monate angegeben haben.

  Sie können z. B. angeben, dass das Audit-Protokoll in den Monaten Januar, März und August alle Montag, Mittwoch und Samstag um 10:30 Uhr gedreht werden soll
- Wenn Sie Werte für `-rotate-schedule-dayofweek` und angeben `-rotate-schedule-day`, werden diese unabhängig voneinander betrachtet.

  Wenn Sie beispielsweise `-rotate-schedule-dayofweek` Freitag und `-rotate-schedule-day` 13 angeben, werden die Prüfprotokolle an jedem Freitag und am 13. Tag des angegebenen Monats gedreht, nicht nur an jedem Freitag, dem 13…
- Wenn Sie die Rotation auf Basis eines Zeitplans zurücksetzen möchten, verwenden Sie den folgenden Befehl, um die Einstellung aufzuheben `-rotate-size parameter`:

  ```
  vserver audit modify -vserver svm_name -destination / -rotate-size -
  ```

Drehen Sie Protokolle basierend auf der Protokollgröße und dem Zeitplan

Sie können wählen, ob Sie die Protokolldateien basierend auf der Protokollgröße und einem Zeitplan drehen möchten, indem Sie den Parameter -rotieren-size und die zeitbasierten Rotationsparameter in einer beliebigen Kombination einstellen. Beispiel: Wenn `-rotate-size` auf 10 MB gesetzt ist und `-rotate-schedule -minute` auf 15 eingestellt ist, drehen sich die Protokolldateien, wenn die Größe der Protokolldatei 10 MB oder auf die 15. Minute jeder Stunde (je nachdem, welches Ereignis zuerst eintritt) erreicht.

Erfahren Sie mehr über die in diesem Verfahren beschriebenen Befehle im "ONTAP-Befehlsreferenz".

Erstellen und Aktivieren einer ONTAP S3 Auditing-Konfiguration

Für die Implementierung der S3-Prüfung wird zuerst eine persistente Objektspeicherauditierung auf einer S3-fähigen SVM erstellt, dann die Konfiguration

aktiviert.

Bevor Sie beginnen

- Sie haben eine S3-fähige SVM.
- Vergewissern Sie sich, dass ausreichend Speicherplatz für das Staging von Volumes in der lokalen Ebene vorhanden ist.

Über diese Aufgabe

Für jede SVM, die S3-Buckets enthält, die Sie prüfen möchten, ist eine Audit-Konfiguration erforderlich. Sie können S3-Prüfungen auf neuen oder vorhandenen S3-Servern aktivieren. Das Auditing von Konfigurationen bleibt 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 der SVM, die Sie für das Auditing auswählen. Eine SVM, die für Audits aktiviert ist, kann geprüfte und nicht geprüfte Buckets enthalten.

Es wird empfohlen, die S3-Prüfung für automatische Protokollrotation anhand von Protokollgröße oder Zeitplan zu konfigurieren. Wenn Sie die automatische Protokollrotation nicht konfigurieren, bleiben alle Protokolldateien standardmäßig erhalten. Sie können S3-Protokolldateien auch manuell mit dem Befehl **vserver object-Store-Server Audit rotieren-log** drehen.

Wenn die SVM eine SVM Disaster-Recovery-Quelle ist, kann sich der Zielpfad nicht auf dem Root-Volume befinden.

Schritte

1. Erstellen Sie die Überwachungskonfiguration, um Prüfprotokolle basierend auf Protokollgröße oder einem Zeitplan zu drehen.

Wenn Sie die Prüfprotokolle drehen möchten, um…	Eingeben…
Protokollgröße	`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]}]`
Einen 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 Sie die zeitbasierte Rotation des Überwachungsprotokolls konfigurieren.

2. S3-Auditing aktivieren:

   `vserver object-store-server audit enable -vserver svm_name`

Beispiele

Im folgenden Beispiel wird eine Audit-Konfiguration erstellt, die alle S3-Ereignisse (die Standardeinstellung) anhand von größenbasierter Rotation prüft. Die Protokolle werden im Verzeichnis /Audit_log gespeichert. Die maximale Größe der Protokolldatei beträgt 200 MB. Die Protokolle werden gedreht, wenn sie 200 MB groß.

```
cluster1::> vserver audit create -vserver vs1 -destination /audit_log -rotate
-size 200MB
```

Im folgenden Beispiel wird eine Audit-Konfiguration erstellt, die alle S3-Ereignisse (die Standardeinstellung) anhand von größenbasierter Rotation prüft. 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
```

Im folgenden Beispiel wird eine Audit-Konfiguration erstellt, die S3-Managementereignisse und zentrale Zugriffs- und Staging-Ereignisse mithilfe zeitbasierter Rotation prüft. Die Prüfprotokolle werden monatlich um 12:30 Uhr an allen Wochentagen gedreht. Die Protokollrotationsgrenze ist 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
```

Wählen Sie Buckets für ONTAP S3 Auditing aus

Sie müssen angeben, welche Buckets in einer SVM mit Audit-Aktivierung geprüft werden sollen.

Bevor Sie beginnen

- Sie haben eine SVM für die S3-Prüfung aktiviert.

Über diese Aufgabe

S3-Audit-Konfigurationen sind auf SVM-Basis aktiviert, jedoch müssen Sie die Buckets für SVMS auswählen, die für die Prüfung aktiviert sind. Wenn der SVM Buckets hinzugefügt werden sollen und die neuen Buckets geprüft werden sollen, müssen Sie diese bei diesem Verfahren auswählen. Es können auch nicht geprüfte Buckets in einer SVM für die S3-Prüfung aktiviert sein.

Die Überwachungskonfigurationen bleiben für Buckets bestehen, bis `vserver object-store-server audit event-selector delete` sie mit dem Befehl entfernt werden.

Schritte

1. Wählen Sie einen Bucket für die S3-Prüfung 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` (Standard ist `all`).
- `-permission`: Gibt die Art der zu prüfenden Ereignisberechtigung an: `allow-only`, `deny-only` Oder `all` (Standard ist `all`).

Beispiel

Im folgenden Beispiel wird eine Bucket-Audit-Konfiguration erstellt, die nur erlaubte Ereignisse mit schreibgeschütztem Zugriff protokolliert:

```
cluster1::> vserver object-store-server audit event-selector create -vserver vs1
-bucket test-bucket -access read-only -permission allow-only
```

Ändern Sie eine ONTAP S3 Überwachungskonfiguration

Sie können die Audit-Parameter einzelner Buckets oder die Auditing-Konfiguration aller für das Audit in der SVM ausgewählten Buckets ändern.

Wenn Sie die Audit-Konfiguration ändern möchten für…	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

Im folgenden Beispiel wird eine individuelle Bucket-Audit-Konfiguration geändert, um nur schreibgeschützten Zugriffsereignisse zu überwachen:

```
cluster1::> vserver object-store-server audit event-selector modify
-vserver vs1 -bucket test-bucket -access write-only
```

Im folgenden Beispiel wird die Audit-Konfiguration aller Buckets in der SVM geändert, um die Protokollgröße auf 10 MB zu ändern und 3 Protokolldateien vor der Drehung aufzubewahren.

```
cluster1::> vserver object-store-server audit modify -vserver vs1 -rotate
-size 10MB -rotate-limit 3
```

Zeigen Sie die ONTAP S3 Audit-Konfigurationen an

Nach Abschluss der Überwachungskonfiguration können Sie überprüfen, ob die Prüfung ordnungsgemäß konfiguriert und aktiviert ist. Sie können auch Informationen zu allen Objektspeicherprüfungen im Cluster anzeigen.

Über diese Aufgabe

Sie können Informationen zu Bucket- und SVM-Audit-Konfigurationen anzeigen.

- Buckets: Verwenden Sie den `vserver object-store-server audit event-selector show` Befehl

  Ohne Parameter zeigt der Befehl die folgenden Informationen über Buckets in allen SVMs im Cluster mit Objektspeicherprüfungen-Konfigurationen an:

  - SVM-Name
  - Bucket-Name
  - Zugriffs- und Berechtigungswerte

- SVMs: Verwenden Sie den `vserver object-store-server audit show` Befehl

  Ohne Parameter zeigt der Befehl die folgenden Informationen über alle SVMs im Cluster mit Objektspeicherprüfungen-Konfigurationen an:

  - SVM-Name
  - Audit-Status
  - Zielverzeichnis

Sie können den `-fields` Parameter angeben, um festzulegen, welche Audit-Konfigurationsinformationen angezeigt werden sollen.

Schritte

Informationen zu S3-Audit-Konfigurationen anzeigen:

Wenn Sie die Konfiguration ändern möchten für…	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

Im folgenden Beispiel werden Informationen für einen einzelnen Bucket angezeigt:

```
cluster1::> vserver object-store-server audit event-selector show -vserver
vs1 -bucket test-bucket
     Vserver     Bucket     Access          Permission
     ----------- ---------- --------------- ----------
     vs1         bucket1    read-only       allow-only
```

Im folgenden Beispiel werden Informationen für alle Buckets einer SVM angezeigt:

```
cluster1::> vserver object-store-server audit event-selector show -vserver
vs1

     Vserver           :vs1
     Bucket            :test-bucket
     Access            :all
     Permission        :all
```

Im folgenden Beispiel werden Name, Audit-Status, Ereignistypen, Protokollformat und Zielverzeichnis für alle SVMs angezeigt.

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

Vserver     State  Event Types Log Format Target Directory
----------- ------ ----------- ---------- --------------------
vs1         false  data        json       /audit_log
```

Im folgenden Beispiel werden die Namen und Details zu den SVM-Protokollen für alle SVMs angezeigt.

```
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 alle Informationen zur Audit-Konfiguration über alle SVMs in Listenform.

```
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
```