



S3-Objekt-Storage-Management

ONTAP 9

NetApp
April 24, 2024

Inhalt

- S3-Objekt-Storage-Management 1
 - Erfahren Sie mehr über S3-Support in ONTAP 9 1
 - Planen 4
 - Konfigurieren 8
 - Buckets werden mit S3 SnapMirror geschützt 58
 - Prüfung von S3-Ereignissen 93

S3-Objekt-Storage-Management

Erfahren Sie mehr über S3-Support in ONTAP 9

S3-Konfigurationsübersicht

Ab ONTAP 9.8 können Sie einen S3-Objekt-Storage-Server (ONTAP Simple Storage Service) in einem ONTAP-Cluster aktivieren.

ONTAP unterstützt zwei lokale Anwendungsszenarien für die Bereitstellung von S3-Objekt-Storage:

- FabricPool Tiering zu einem Bucket auf lokalem Cluster (Tiering zu einem lokalen Bucket) oder Remote-Cluster (Cloud-Tier)
- Zugriff auf einen S3-Client-App auf einen Bucket auf dem lokalen Cluster oder auf einem Remote-Cluster

Ab ONTAP 9.14.1 können Sie einen S3 Objekt-Storage-Server auf einer SVM in einem gespiegelten oder nicht 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 nicht gespiegelter Aggregate in MetroCluster IP-Konfigurationen finden Sie unter "[Überlegungen bei nicht gespiegelten Aggregaten](#)".

Sie sollten die folgenden Verfahren verwenden, wenn Sie S3-Objektspeicher wie folgt konfigurieren möchten:

- Sie möchten S3 Objekt-Storage von einem vorhandenen Cluster mit ONTAP bereitstellen.

ONTAP S3 ist die richtige Lösung, wenn Sie S3-Funktionen auf vorhandenen Clustern ohne zusätzliche Hardware und Management wünschen. NetApp StorageGRID Software ist jedoch weiterhin die Vorzeigelösung von NetApp für Objekt-Storage. Weitere Informationen finden Sie im "[StorageGRID-Dokumentation](#)".

- Sie verfügen über Cluster-Administratorrechte, keine SVM-Administratorrechte.

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. In Cloud Volumes ONTAP-Umgebungen sollten Sie dies daher tun [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.

Der Netapp Architektur Sind

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

Buckets werden nur durch die physischen Maximalwerte der zugrunde liegenden Hardware begrenzt, deren maximale Anzahl an Architekturen höher sein könnte. Buckets können von der flexiblen FlexGroup Größenanpassung profitieren, um automatisch eine Komponente eines FlexGroup Volume zu vergrößern, wenn der Speicherplatz knapp wird. Es gibt ein Limit von 1000 Buckets pro FlexGroup Volume oder 1/3 der Kapazität des FlexGroup Volume (um das Datenwachstum in Buckets zu berücksichtigen).



Dem FlexGroup Volume mit S3 Buckets ist kein NAS- oder SAN-Protokollzugriff gestattet.

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



Anwendungsfälle

Es gibt drei primäre Anwendungsfälle für den Client-Zugriff auf ONTAP S3-Services:

- Bei ONTAP Systemen, die ONTAP S3 als Remote-Tier für FabricPool-Kapazität (Cloud) verwenden

Der S3-Server und der Bucket mit der Kapazitäts-Tier (für *Cold* Daten) befinden sich in einem anderen Cluster als der Performance-Tier (für *Hot* Daten).

- Bei ONTAP Systemen, die ONTAP S3 als lokalen FabricPool Tier verwenden

Der S3-Server und der Bucket mit Kapazitäts-Tier befinden sich auf demselben Cluster, jedoch auf einem anderen HA-Paar, als Performance-Tier.

- Für externe S3 Client-Applikationen

ONTAP S3 liefert S3-Client-Applikationen, die auf Systemen anderer Anbieter ausgeführt werden.

Als Best Practice wird empfohlen, über HTTPS den Zugriff auf ONTAP S3-Buckets zu ermöglichen. Wenn HTTPS aktiviert ist, sind Sicherheitszertifikate für die ordnungsgemäße Integration mit SSL/TLS erforderlich. Um den Benutzer` ONTAP S3 zu authentifizieren und gleichzeitig die Zugriffsberechtigungen der Benutzer` ONTAP S3 zu autorisieren, müssen Client-Benutzer Zugriff und geheime Schlüssel verwenden. Die Client-Anwendung sollte auch Zugriff auf das Root-CA-Zertifikat (das signierte Zertifikat des ONTAP S3-Servers) haben, um den Server authentifizieren und eine sichere Verbindung zwischen Client und Server erstellen zu können.

Benutzer werden innerhalb der S3-fähigen SVM erstellt und ihre Zugriffsberechtigungen können auf Bucket- oder SVM-Ebene gesteuert werden; das heißt, sie können Zugriff auf einen oder mehrere Buckets innerhalb der SVM erhalten.

HTTPS ist auf ONTAP S3 Servern standardmäßig aktiviert. Es ist möglich, HTTPS zu deaktivieren und HTTP für den Client-Zugriff zu aktivieren. In diesem Fall ist keine Authentifizierung mit CA-Zertifikaten erforderlich. Wenn jedoch HTTP aktiviert ist und HTTPS deaktiviert ist, wird die gesamte Kommunikation mit dem ONTAP

S3-Server über das Netzwerk in Klartext gesendet.

Weitere Informationen finden Sie unter ["Technischer Bericht S3 in ONTAP Best Practices"](#)

Verwandte Informationen

["Management von FlexGroup Volumes"](#)

Planen

ONTAP-Versionsunterstützung für S3 Objekt-Storage

ONTAP unterstützt S3 Objekt-Storage für On-Premises-Umgebungen ab ONTAP 9.8. Cloud Volumes ONTAP unterstützt S3-Objekt-Storage für Cloud-Umgebungen ab ONTAP 9.9.1.

S3-Unterstützung mit Cloud Volumes ONTAP

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

- Die zugrunde liegenden Aggregate sollten sich nur von einem Node stammen. Weitere Informationen zu ["Bucket-Erstellung in CVO-Umgebungen"](#).

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

Öffentliche S3-Vorschau in ONTAP 9.7

Im ONTAP 9.7 wurde S3 Objekt-Storage als öffentliche Vorschau eingeführt. Diese Version war nicht für Produktionsumgebungen vorgesehen und wird ab ONTAP 9.8 nicht mehr aktualisiert. Nur ONTAP 9.8 und 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"](#).

Bucket-Vorgänge

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

Bucket-Betrieb	Der ONTAP Support beginnt mit
CreateBucket	ONTAP 9.11.1
DeleteBucket	ONTAP 9.11.1
DeleteBucketRichtlinien	ONTAP 9.12.1
GetBucketAcl	ONTAP 9.8
GetBucketLifecycleKonfiguration	ONTAP 9.13.1 + * nur Ablaufaktionen werden unterstützt
GetBucketLocation	ONTAP 9.10.1
GetBucketPolicy	ONTAP 9.12.1
HeadBucket	ONTAP 9.8
ListBuchs	ONTAP 9.8
ListBucketVersioning	ONTAP 9.11.1
ListObjectVersions	ONTAP 9.11.1
PutBucket	<ul style="list-style-type: none"> • ONTAP 9.11.1 • ONTAP 9.8: Nur unterstützt mit ONTAP REST-APIs
PutBucketLifecycleKonfiguration	ONTAP 9.13.1 + * nur Ablaufaktionen werden unterstützt
PutBucketPolicy	ONTAP 9.12.1

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>`.

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

Objektvorgang	Der ONTAP Support beginnt mit
AbortMehnteilaUpload	ONTAP 9.8
CompleteMultipartUpload	ONTAP 9.8
CopyObject	ONTAP 9.12.1
CreateMultipartUpload	ONTAP 9.8
DeleteObject	ONTAP 9.8
Objekte deObjekteObjekte	ONTAP 9.11.1
DeleteObjectTagging	ONTAP 9.9.1
GetBucketVersioning	ONTAP 9.11.1
GetObject	ONTAP 9.8
GetObjectAcl	ONTAP 9.8
GetObjectRetention	ONTAP 9.14.1
GetObjectTagging	ONTAP 9.9.1
HeadObject	ONTAP 9.8
ListenMehrpertUpload	ONTAP 9.8
ListObjekte	ONTAP 9.8
ListObjekteV2	ONTAP 9.8
ListBucketVersions	ONTAP 9.11.1
ListenTeile	ONTAP 9.8
PutBucketVersioning	ONTAP 9.11.1
PutObject	ONTAP 9.8
PutObjectLockKonfiguration	ONTAP 9.14.1
PutObjectRetention	ONTAP 9.14.1
PutObjectTagging	ONTAP 9.9.1
UploadTeil	ONTAP 9.8
UploadPartCopy	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

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	<ul style="list-style-type: none"> • 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 	<ul style="list-style-type: none"> • Cloud Volumes ONTAP für jeden Client in ONTAP 9.8 und früheren Versionen
Datensicherung	<ul style="list-style-type: none"> • Cloud-Synchronisierung • "Objektversionierung" (Ab ONTAP 9.11.1) • "S3 SnapMirror" (Ab ONTAP 9.10.1) • MetroCluster IP-Konfigurationen (ab ONTAP 9.12.1) • SnapLock (ab ONTAP 9.14.1) • WORM (ab ONTAP 9.14.1) 	<ul style="list-style-type: none"> • Erasure Coding • Informationslebenszyklus-Management • NDMP • SMTape • SnapMirror Cloud • Disaster Recovery für SVM • SyncMirror • Von Benutzern erstellte Snapshot Kopien
Verschlüsselung	<ul style="list-style-type: none"> • NetApp Aggregatverschlüsselung (NAE) • NetApp Volume Encryption (NVE) • NetApp Storage Encryption (NSE) • TLS/SSL 	<ul style="list-style-type: none"> • SCHLACKE
Storage-Effizienz	<ul style="list-style-type: none"> • Deduplizierung • Komprimierung • Datenverdichtung 	<ul style="list-style-type: none"> • Effizienz auf Aggregatebene • Volume-Klon des FlexGroup Volumes mit ONTAP S3 Buckets

Feature-Bereich	Unterstützt	Nicht unterstützt
Storage-Virtualisierung	-	NetApp FlexArray-Virtualisierung
Servicequalität (QoS)	<ul style="list-style-type: none"> • QoS-Maximalwerte (Decken) • QoS-Mindestwerte (Böden) 	-
Zusätzliche Funktionen	<ul style="list-style-type: none"> • "Prüfung von S3-Ereignissen" (Ab ONTAP 9.10.1) 	<ul style="list-style-type: none"> • FlexCache Volumes • FPolicy • Qtrees • Kontingente

Validierte ONTAP S3 Lösungen von Drittanbietern

NetApp hat die folgenden Drittanbieterlösungen für die Verwendung mit ONTAP S3 validiert.

Wenn die von Ihnen gesuchte Lösung nicht aufgeführt ist, wenden Sie sich bitte an Ihren NetApp Ansprechpartner.

Für ONTAP S3 validierte Lösungen von Drittanbietern

NetApp hat diese Lösungen in Zusammenarbeit mit den jeweiligen Partnern getestet.

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

Konfigurieren

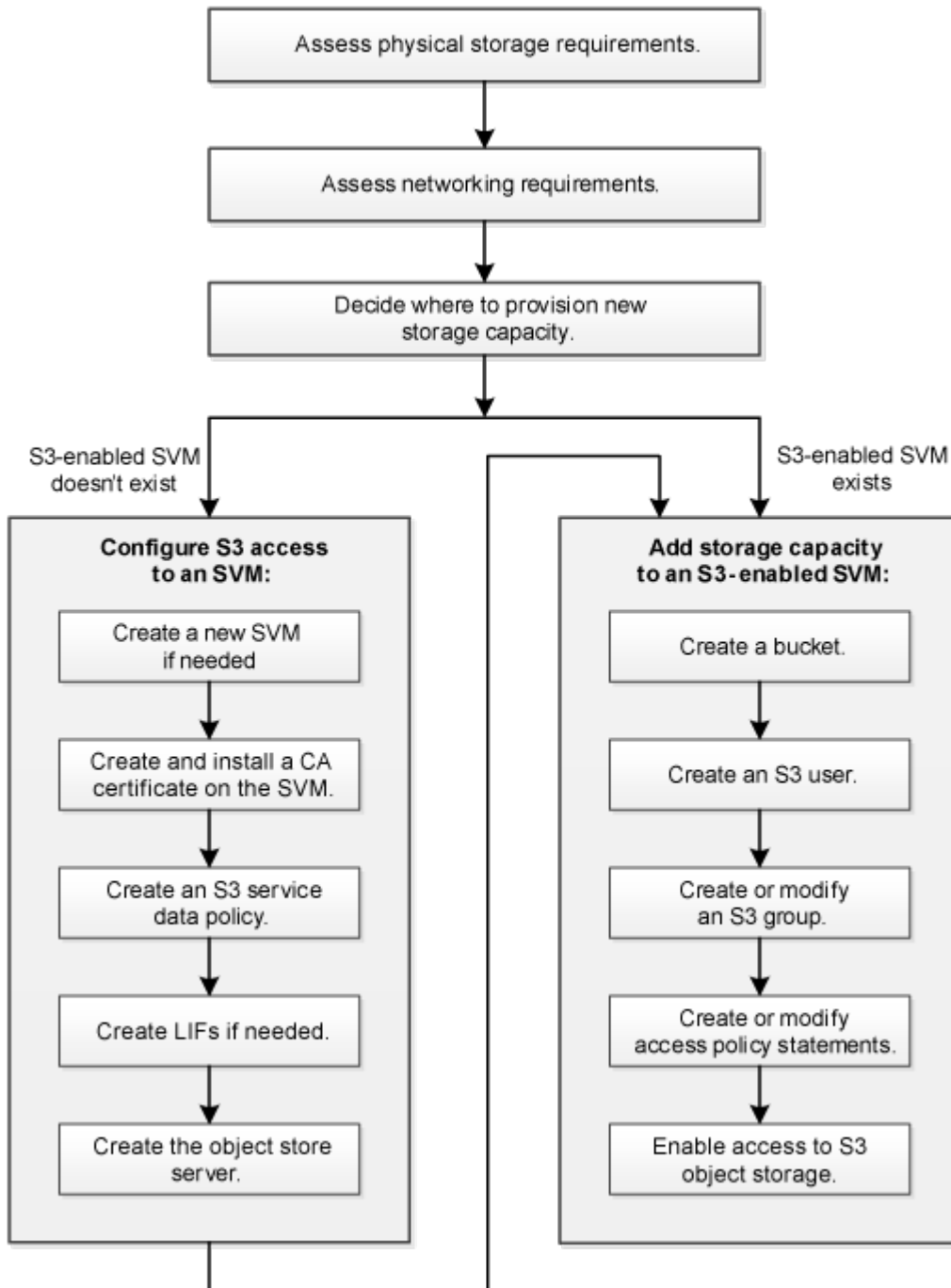
Allgemeines zur S3-Konfiguration

S3-Konfigurationsworkflow

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.

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.



Physischer Storage-Bedarf 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, wird automatisch ein FlexGroup-Volume erstellt, um den Bucket zu unterstützen. 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 genügend Speicherplatz oder den erforderlichen Node-Standort vorhanden sind, fügen Sie mithilfe der Festplatten zu einem vorhandenen Aggregat hinzu `storage aggregate add-disks` Befehl, oder erstellen Sie mit dem ein neues Aggregat `storage aggregate create` Befehl.

Netzwerkanforderungen 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 mithilfe des `network subnet create` Befehl.

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
```

Bei Bedarf können Sie IPv6 mithilfe des `network options ipv6 modify` Befehl.

Legen Sie fest, wo neue S3-Storage-Kapazität bereitgestellt werden soll

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

Erstellung einer SVM für S3

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 **Storage > Storage VMs**, wählen Sie eine Speicher-VM aus, klicken Sie auf **Einstellungen** und klicken Sie dann auf  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 Zertifikatsinformation 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 den `-rootvolume-security-style` Option.
- Verwenden Sie die Standard-C.UTF-8 `-language` Option.
- Der `ipSPACE` Die Einstellung ist optional.

3. Konfiguration und Status der neu erstellten SVM überprüfen:

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

Der Vserver Operational State Das Feld muss angezeigt werden `running` Bundesland. Wenn der angezeigt wird `initializing` Zustand: Einiger Zwischenvorgang wie z. B. die Erstellung des Root-Volumes ist fehlgeschlagen. Außerdem müssen Sie die SVM löschen und erneut 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
```

Der folgende Befehl zeigt, dass eine SVM mit einem Root-Volume von 1 GB erstellt wurde und dass sie automatisch gestartet wurde und sich in befindet `running` Bundesland. 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 in `locked` Bundesland. 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 Sie ein CA-Zertifikat auf der SVM

Um den HTTPS-Datenverkehr von S3-Clients auf die S3-fähige SVM zu aktivieren, ist ein CA-Zertifikat erforderlich.

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. CA-Zertifikate von Drittanbietern werden ebenfalls unterstützt. Weitere Informationen finden Sie in der Dokumentation zur Administratorauthentifizierung.

"Administratorauthentifizierung und RBAC"

Siehe `security certificate` Man-Pages für weitere Konfigurationsoptionen.

Schritte

1. Erstellen eines selbstsignierten digitalen Zertifikats:

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

Der `-type root-ca` Option erstellt und installiert ein selbstsigniertes digitales Zertifikat, um andere Zertifikate zu signieren, indem es als Zertifizierungsstelle fungiert.

Der `-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.

2. Erzeugen einer Anfrage zum Signieren eines Zertifikats:

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

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

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

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

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, die Sie in Schritt 1 eingegeben haben.
- `-ca-serial` — die CA-Seriennummer von 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

```

Erstellen einer S3-Service-Datenrichtlinie

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
```

Der data-core Und data-s3-server Services sind die einzigen erforderlich, die für die Aktivierung von ONTAP S3 erforderlich sind, andere Services können jedoch bei Bedarf eingebunden werden.

Erstellung von Daten-LIFs

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 Netzwerk-Port muss für den Administrator konfiguriert worden sein up Status:
- 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 erstellt `network subnet create` Befehl.

- Die Richtlinie für den LIF-Dienst muss bereits vorhanden sein.

Über diese Aufgabe

- Sie können am gleichen Netzwerkport IPv4- und IPv6-LIFs erstellen.
- Wenn Sie eine große Anzahl von LIFs im Cluster besitzen, können Sie die im Cluster unterstützte LIF-Kapazität mithilfe der überprüfen `network interface capacity show` Befehl und die LIF-Kapazität, die auf jedem Node mithilfe von unterstützt wird `network interface capacity details show` Befehl (auf der erweiterten Berechtigungsebene).
- 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, den das LIF zurückgibt, wenn das `network interface revert` Befehl wird auf dem LIF ausgeführt.

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

- -home-port Ist der physische oder logische Port, an den das LIF zurückgibt, wenn das `network interface revert` Befehl wird auf dem LIF ausgeführt.
- Sie können eine IP-Adresse mit dem angeben `-address` Und `-netmask` Optionen, oder Sie

aktivieren die Zuweisung von einem Subnetz mit dem `-subnet_name` Option.

- 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. Der `network route create` Die man-Page enthält Informationen zum Erstellen einer statischen Route in einer SVM.
- Für das `-firewall-policy` Wählen Sie die gleiche Standardeinstellung aus data 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-Service-Richtlinien ersetzt. Weitere Informationen finden Sie unter ["Konfigurieren Sie Firewallrichtlinien für LIFs"](#).

- `-auto-revert` Ermöglicht Ihnen, anzugeben, ob eine Daten-LIF automatisch auf den Home-Node zurückgesetzt wird. Dies kann unter Umständen wie „Startvorgang“, ändert den Status der Management-Datenbank oder wenn die Netzwerkverbindung hergestellt wird. Die Standardeinstellung ist `false`, Aber Sie können es auf `true` einstellen `false` Abhängig von Netzwerkmanagement-Richtlinien in Ihrer Umgebung.
- Der `-service-policy` Option gibt die von Ihnen erstellte Daten- und Management-Services-Richtlinie sowie alle weiteren Richtlinien an, die Sie benötigen.

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

- a. Verwenden Sie die `network ndp prefix show` Befehl zum Anzeigen der Liste der RA-Präfixe, die auf 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` Ist das Präfix auf verschiedenen Schnittstellen gelernt.

Für die Ableitung der `id`, Wählen Sie eine zufällige 64-Bit-Hexadezimalzahl aus.

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

Überprüfen einer...	Verwenden...
IPv4-Adresse	<code>network ping</code>
IPv6-Adresse	<code>network ping6</code>

Beispiele

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

```
network interface create -vserver svml.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
```

Vserver	Logical Interface	Status Admin/Oper	Network Address/Mask	Current Node	Current Is 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.

Erstellen von Intercluster LIFs für Remote FabricPool Tiering

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 Netzwerk-Port muss für den Administrator konfiguriert worden sein up Status:
- 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
```

Im folgenden Beispiel werden die Netzwerkports in angezeigt 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

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 erstellt cluster01_icl01 Und cluster01_icl02:

```

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

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

```

3. Überprüfen Sie, ob die Intercluster-LIFs erstellt wurden:

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

```

cluster01::> network interface show -service-policy default-intercluster

```

Current Is	Logical	Status	Network	Current
Vserver	Interface	Admin/Oper	Address/Mask	Node
Home				Port
-----	-----	-----	-----	-----
-----	-----	-----	-----	-----
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
```

Das folgende Beispiel zeigt, dass die Intercluster-LIFs sind cluster01_icl01 Und cluster01_icl02 Auf dem e0c Ein Failover des Ports zum erfolgt e0d Port:

```
cluster01::> network interface show -service-policy default-intercluster
-failover
```

Vserver	Logical Interface	Home Node:Port	Failover Policy	Failover 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	

Erstellen Sie den 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.

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 ausführen `object-store-server users regenerate-keys` Befehl zum Festlegen des Zugriffsschlüssels und des Geheimschlüssels für diesen Benutzer.



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.

Siehe `vserver object-store-server` Man-Pages für zusätzliche Konfigurations- und Anzeigoptionen.


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

- Wählen Sie die Speicher-VM aus: Klicken Sie auf **Storage > Storage VMs**, wählen Sie eine Speicher-VM aus, klicken Sie auf **Einstellungen** und klicken Sie dann auf  Unter **S3**.
- Klicken Sie auf **S3 aktivieren** und geben Sie dann den S3-Servernamen ein.
- 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.

- 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 Zertifikatsinformation 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 Zertifikatsname 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 dem ändern `-secure-listener-port` Option.

Wenn HTTPS aktiviert ist, sind CA-Zertifikate für die korrekte Integration mit SSL/TLS erforderlich.

- HTTP ist standardmäßig deaktiviert. Wenn diese Option aktiviert ist, wartet der Server an Port 80. Aktivieren Sie die Aktivierung mit dem `-is-http-enabled` Oder ändern Sie die Portnummer mit `-listener-port` Option.

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 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 Speicherservicedefinitionen 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 deaktivieren oder während des Bereitstellungsprozesses oder zu einem späteren Zeitpunkt eine individuelle 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.
- Ab ONTAP 9.14.1 ist dies möglich "[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. Siehe [Management von FlexGroup Volumes](#) Finden Sie weitere Informationen.

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

Siehe "[vserver Objekt-Store-Server Bucket ändern](#)" Finden Sie weitere Informationen.

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, setzen Sie die Berechtigungsebene auf „Advanced“ (ansonsten reicht die Admin-Berechtigungsebene aus): `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 sein Cluster (Der Name der System-Storage-VM), wenn Sie lokales Tiering konfigurieren.

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

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

- tiering

Nehmen Sie die auf `-used-as-capacity-tier true` Option.

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

- Der `-aggr-list` Der Parameter gibt die Liste der Aggregate 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 mit dem aufgeführt sind `-aggr-list` Parameter beim Erstellen eines FlexGroup-Volumes.

Der Standardwert des `-aggr-list-multiplier` Der Parameter 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 Storage-VM erstellt `vs1` Der Größe 1TB Und Angabe des Aggregats:

```
cluster-1::*> vserver object-store-server bucket create -vserver  
svml.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 Objektspernung, 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 Sie die Versionierung für Ihre Objekte für eine spätere Wiederherstellung aktivieren möchten, wählen Sie **Versionierung aktivieren**. Die Versionierung ist standardmäßig aktiviert, wenn Sie die Objektspernung 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 Objektspernung in S3 Buckets unterstützt. Für die S3 Objektspernung 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. Bestehende Kunden können diese Option wählen, obwohl sie derzeit nicht benötigt werden ["Upgrade auf ONTAP One"](#).

Wenn Sie die Objektspernung für einen Bucket aktivieren, sollten Sie dies tun ["Vergewissern Sie sich, dass eine SnapLock-Lizenz installiert ist"](#). Wenn keine SnapLock-Lizenz installiert ist, müssen Sie dies tun ["Installieren"](#) Bevor Sie die Objektspernung 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 Objektsperre 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. Objektsperre 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.

Erstellung eines 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.
- Dieselben Bereitstellungsrichtlinien wie in beschrieben ["Erstellen eines Buckets"](#) Anwenden bei der Erstellung eines Buckets in einer MetroCluster-Umgebung.
- Die folgenden S3-Objekt-Storage-Funktionen werden in MetroCluster Umgebungen **nicht** unterstützt:
 - S3 SnapMirror

- 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, setzen Sie die Berechtigungsebene auf „Advanced“ (ansonsten reicht die Admin-Berechtigungsebene aus): `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]
```

Stellen Sie die `-use-mirrored-aggregates` Option auf `true` Oder `false` Je nachdem, ob Sie ein gespiegeltes oder nicht gespiegeltes Aggregat verwenden möchten.



Standardmäßig wird der verwendet `-use-mirrored-aggregates` Die Option ist auf festgelegt `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**

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

- **tiering**

Nehmen Sie die auf `-used-as-capacity-tier true` Option.

- Wenn Sie die Aggregate angeben möchten, auf denen das zugrunde liegende FlexGroup Volume erstellt werden soll, verwenden Sie die folgenden Optionen:
 - Der `-aggr-list` Der Parameter gibt die Liste der Aggregate 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 mit dem aufgeführt sind `-aggr-list` Parameter beim Erstellen eines FlexGroup-Volumes.

Der Standardwert des `-aggr-list-multiplier` Der Parameter 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  
svml.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:

Add bucket

NAME

To use this bucket from a remote cluster, configure S3 service on storage VM "vs1".

FOLDER (OPTIONAL)

Specify the folder to map to this bucket. [Know more](#)

CAPACITY

Size

GB

☐ Use tiering
If you select this option, the system will try to select low-cost media with optimal performance for the tiered data.
☐ Enable versioning
Versioning-enabled buckets allow you to recover objects that were accidentally deleted or overwritten. After versioning is enabled, it can't be disabled. However, you can suspend versioning.

PERFORMANCE SERVICE LEVEL

Value

Not sure? [Get help selecting type](#)

Permissions

☐ Copy access permissions from an existing bucket

Principal	Effect	Actions	Resources	Conditions
All users of this stor...	allow	ListBucket	*	

+ Add

Object locking

☐ Enable object locking
Object locking utilizes the "Write Once, Read Many" (WORM) model in which objects or their versions are protected from being deleted or overwritten during the specified retention period.

Protection

☒ Use the S3x3l0n0r1t10n

- 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 App von Drittanbietern – den Zugriff auf den neuen Bucket, indem Sie Folgendes eingeben:
 - Das S3-Server-CA-Zertifikat.
 - Der Zugriffsschlüssel und der Geheimschlüssel des Benutzers.
 - Der FQDN-Name des S3-Servers und der Bucket-Name.

Erstellen einer Bucket-Lifecycle-Management-Regel

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 Objektsperre für Ihre Bucket-Objekte aktiviert ist, werden die Lifecycle-Management-Regeln für die Objektablauffrist nicht auf gesperrte Objekte angewendet. Informationen zur Objektsperre finden Sie unter ["Erstellen eines Buckets"](#).

Bevor Sie beginnen

Eine S3-fähige SVM mit einem S3-Server und einem Bucket muss bereits vorhanden sein. Siehe ["Erstellung einer SVM für S3"](#) Finden Sie weitere Informationen.

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 ist `Expiration`.
- Löschen nicht aktueller Versionen – Diese Aktion gibt an, wann S3 nicht aktuelle Objekte dauerhaft entfernen kann. Die CLI-Aktion ist `NoncurrentVersionExpiration`.
- 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 ist `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 ist `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	<ul style="list-style-type: none">• <code>-non-curr-days</code> - Anzahl der Tage, nach denen nicht aktuelle Versionen gelöscht werden• <code>-new-non-curr-versions</code> - Anzahl der neuesten nicht-aktuellen Versionen, die beibehalten werden sollen
Ablauf	<ul style="list-style-type: none">• <code>-obj-age-days</code> - Anzahl der Tage seit der Erstellung, nach denen die aktuelle Version der Objekte gelöscht werden kann• <code>-obj-exp-date</code> - Bestimmtes Datum, wann die Objekte ablaufen sollen• <code>-expired-obj-del-markers</code> - Löschen von Objektmarkierungen
AbortInsetteMultipartUpload	<ul style="list-style-type: none">• <code>-after-initiation-days</code> - 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 die `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 AbortIncompleteMultipartUpload 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 die Objekte in einem anderen Bucket nutzen. 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  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 Version nicht aktuell wird, und danach kann gelöscht werden, 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  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  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 eines S3-Benutzers

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. Die Schlüssel eines S3-Benutzers können mit dem angezeigt werden `vserver object-store-server user show` Befehl.

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 festlegen, für den der Schlüssel gültig sein wird -key-time-to-live Parameter. Sie können den Aufbewahrungszeitraum 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 P1DT2H3M4S. Sofern nicht angegeben, ist der Schlüssel für einen unbestimmten Zeitraum gültig.

Im folgenden Beispiel wird ein Benutzer mit dem Namen erstellt `sm_user1` Auf Storage-VM `vs0`, Mit einer Schlüsselaufbewahrungsfrist 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 auf  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 ist der Wert auf festgelegt 0 Das bedeutet, 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](#)

Erstellen oder Ändern von S3-Gruppen

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 Objektspeicherrichtlinien an. Diese Richtlinien bestimmen die Buckets und den Zugriff für die Gruppenmitglieder.

System Manager

1. Bearbeiten Sie den Speicher-VM: Klicken Sie auf **Storage > Storage VMs**, klicken Sie auf die Speicher-VM, klicken Sie auf **Einstellungen** und klicken Sie dann auf  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\]\`Der \`-  
policies Option kann in Konfigurationen mit nur einem Bucket in einem Objektspeicher  
weggelassen werden; der Gruppenname kann der Bucket-Richtlinie hinzugefügt werden. Der  
-policies Option kann später mit der hinzugefügt werden vserver object-store-server  
group modify Befehl nach Erstellung der Objekt-Storage-Server-Richtlinien
```

Schlüssel neu generieren und Aufbewahrungsfrist ändern

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"](#).

CLI

1. Regenerieren Sie Zugriff und geheime Schlüssel für einen Benutzer, indem Sie den ausführen
`vserver object-store-server user regenerate-keys` Befehl.
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 eine Aufbewahrungsfrist 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.

System Manager

1. Klicken Sie auf **Storage > Storage VMs** und wählen Sie dann die Speicher-VM aus.
2. Klicken Sie auf der Registerkarte **Einstellungen** auf  In der 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 möchten, klicken Sie auf  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.

Erstellen oder Ändern von Zugriffsrichtlinien-Anweisungen

Allgemeines zu Bucket- und Objektspeicherserverrichtlinien

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.

Ändern einer Bucket-Richtlinie

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. Weitere Optionen finden Sie im `vserver object-store-server bucket policy` Man-Pages.

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.

Ab ONTAP 9.9 unterstützen Sie die Objekt-Tagging-Funktionen von AWS für Clients mit dem ONTAP S3-Server `GetObjectTagging`, `PutObjectTagging`, und `DeleteObjectTagging`. Es müssen die Bucket- oder Gruppenrichtlinien verwendet werden.

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.

bucketname/*_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}` Wird als Variable für eine Richtlinie angegeben, dann 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 angeben * Um alle Aktionen oder eine Liste mit einer oder mehreren der folgenden Aktionen zu bedeuten: GetObject, PutObject, DeleteObject, ListBucket, GetBucketAcl, GetObjectAcl, ListBucketMultipartUploads, Und ListMultipartUploadParts.

-principal	<p>Eine Liste mit einem oder mehreren S3-Benutzern oder -Gruppen.</p> <ul style="list-style-type: none"> • Es können maximal 10 Benutzer oder Gruppen angegeben werden. • Wenn eine S3-Gruppe angegeben wird, muss sie sich im Formular befinden <code>group/group_name</code>. • * Kann als öffentlicher Zugriff angegeben werden, d. h. ohne Zugriffsschlüssel und Geheimschlüssel. • Wenn kein Principal angegeben wird, werden allen S3-Benutzern in der Storage-VM Zugriff gewährt.
-resource	<p>Den Bucket und jedes darin enthaltene Objekt. Die Platzhalterzeichen * Und ? Kann verwendet werden, um einen regulären Ausdruck zum Angeben 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.</p>

Sie können optional einen Textstring als Kommentar mit dem angeben `-sid` Option.

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::> vservers 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::> vservers 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 Server-Bucket-Richtlinienanweisung für die Storage-VM erstellt `svm1` Und `bucket1`, Und gibt an `${aws:username}` Als Variable für eine Policy-Ressource. Wenn die Richtlinie ausgewertet wird, wird die RichtlinienvARIABLE durch den Benutzernamen für den Anforderungskontext ersetzt, und die Richtlinienaktion kann wie für diesen Benutzer konfiguriert ausgeführt werden. Wenn beispielsweise die folgende Richtlinienanweisung bewertet wird, `${aws:username}` Wird durch den Benutzer ersetzt, der den S3-Vorgang durchführt. Wenn ein Benutzer `user1` Führt den Vorgang durch, auf den der Benutzer

Zugriff hat bucket1 Als bucket1/user1/*.

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

Erstellen oder Ändern einer 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. Weitere Optionen finden Sie im `vserver object-store-server policy` ["Befehlsreferenz"](#).


Ab ONTAP 9.9 unterstützen Sie die Objekt-Tagging-Funktionen von AWS für Clients mit dem ONTAP S3-Server `GetObjectTagging`, `PutObjectTagging`, und `DeleteObjectTagging`. Es müssen die Bucket- oder Gruppenrichtlinien verwendet werden.

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 den Speicher-VM: Klicken Sie auf **Storage > Storage VMs**, klicken Sie auf die Speicher-VM, klicken Sie auf **Einstellungen** und klicken Sie dann auf  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 angeben * Um alle Aktionen oder eine Liste mit einer oder mehreren der folgenden Aktionen zu bedeuten: GetObject, PutObject, DeleteObject, ListBucket, GetBucketAcl, GetObjectAcl, ListAllMyBuckets, ListBucketMultipartUploads, Und ListMultipartUploadParts.
-resource	Den Bucket und jedes darin enthaltene Objekt. Die Platzhalterzeichen * Und ? Kann verwendet werden, um einen regulären Ausdruck zum Angeben einer Ressource zu bilden.

Sie können optional einen Textstring als Kommentar mit dem angeben -sid Option.

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

Konfigurieren Sie den S3-Zugriff für externe Verzeichnisdienste

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 ["Überblick über die Verwendung von LDAP"](#).

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 das selbstsignierte Root-CA-Zertifikat auf der SVM"](#).

5. Ein LDAP-Client wird mit TLS auf der SVM konfiguriert. Siehe "[Erstellen Sie eine LDAP-Client-Konfiguration](#)" Und "[Verknüpfen Sie die LDAP-Client-Konfiguration mit SVMs, um Informationen zu erhalten](#)".

Konfigurieren Sie den S3-Zugriff für externe Verzeichnisdienste

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 zu diesem Befehl finden Sie im "[vserver Services Name-Service ns-Switch modify](#)" Befehl.

2. Erstellen einer Bucket-Richtlinienanweisung für Objektspeicher mit dem `principal` Legen Sie die LDAP-Gruppe fest, 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 auf die LDAP-Gruppe `group1` Für 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. Überprüfen Sie, ob ein Benutzer aus der LDAP-Gruppe stammt `group1` Kann S3-Vorgänge vom S3-Client ausführen.

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 zu diesem Befehl finden Sie im ["vserver Services Name-Service ns-Switch modify"](#) Befehl.

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 folgendem Format:
"NTAPFASTBIND" + base64-encode(user-name:password)
Beispiel: "NTAPFASTBIND" + base64-encode(ladapuser: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.

Ermöglichen Sie LDAP- oder Domänenbenutzern, eigene 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 Ihre Storage-VM ein paar Konfigurationsschritte durchführen, um die benutzerdefinierte Rolle zu erstellen und dem Benutzer zuzuweisen, der die API zur Schlüsselgenerierung nach dem Zugriff aufruft.

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 das selbstsignierte Root-CA-Zertifikat auf der SVM"](#).
5. Ein LDAP-Client wird auf der Storage-VM mit aktiviertem TLS konfiguriert. Siehe ["Erstellen Sie eine LDAP-Client-Konfiguration"](#) Und .
6. Verknüpfen Sie die Client-Konfiguration mit dem Vserver. Siehe ["Zuordnen der LDAP-Client-Konfiguration zu SVMs"](#) Und ["vserver Services Name-Service ldap-Erstellung"](#).

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. Siehe ["Netzwerkschnittstelle erstellen"](#) Und ["Erstellen der Service-Policy für die Netzwerkschnittstelle"](#) Befehle.

Konfigurieren Sie Benutzer für die Generierung des Zugriffsschlüssels

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
```

Weitere Informationen zu diesem Befehl finden Sie im ["vserver Services Name-Service ns-Switch modify"](#) Befehl.

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 ist der s3-role Die Rolle wird für Benutzer auf der Storage-VM generiert svm-1, Auf die alle Zugriffsrechte, Lesen, Erstellen und Aktualisieren gewährt werden.

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

Weitere Informationen zu diesem Befehl finden Sie im ["Erstellen der Rest-Rolle für die Sicherheitsanmeldung"](#) Befehl.

3. Erstellen Sie eine LDAP-Benutzergruppe mit dem Befehl für die Sicherheitsanmeldung, und fügen Sie die neue benutzerdefinierte Rolle für den Zugriff auf den REST-API-Endpunkt des S3-Benutzers hinzu. Weitere Informationen zu diesem Befehl finden Sie im ["Sicherheits-Login erstellen"](#) Befehl.

```
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 die LDAP-Gruppe ldap-group-1 Wird in erstellt svm-1`Und die benutzerdefinierte Rolle `s3role Wird hinzugefügt, um auf den API-Endpunkt zuzugreifen, zusammen mit der Aktivierung von LDAP-Zugriff 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 nswitch-Authentifizierung"](#).

Durch das Hinzufügen der benutzerdefinierten Rolle zur Domäne oder LDAP-Gruppe erhalten Benutzer in dieser Gruppe eingeschränkten Zugriff auf die ONTAP

/api/protocols/s3/services/{svm.uuid}/users endpoint: Durch Aufruf der API können die Benutzer der Domäne oder LDAP-Gruppe eigene Zugriffs- und geheime Schlüssel 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-Endpoint verwenden.

HTTP-Methode und -Endpoint

Dieser REST-API-Aufruf verwendet die folgende Methode und den folgenden Endpoint. Informationen zu den anderen Methoden dieses Endpunkts finden Sie in der Referenz ["API-Dokumentation"](#).

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

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": "_name_"}'
```

Beispiel für eine JSON-Ausgabe

```
{
  "records": [
    {
      "access_key":
"Pz3SB54G2B_6dsXQPrA5HrTPcf478qoAW6_Xx6qyqZ948AgZ_7YfCf_9nO87YoZmskxx3cq41
U2JAH2M3_fs321B4rkzS3a_oC5_8u7D8j_45N8OsBCBPWGD_1d_ccfq",
      "_links": {
        "next": {
          "href": "/api/resourcelink"
        },
        "self": {
          "href": "/api/resourcelink"
        }
      },
      "name": "user-1",
      "secret_key":
"A20_tDhC_cux2C2BmtL45bXB_a_Q65c_96FsAcOdo14Az8V31jBKDTc0uCL62Bh559gPB8s9r
rn0868QrF38_1dsV2u1_9H2tSf3qQ5xp9NT259C6z_GiZQ883Qn63X1"
    }
  ],
  "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 mithilfe von Cluster-LIFs (mit der erstellt wurden `-vserver Cluster Parameter`).

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
-ipospace Cluster -provider-type ONTAP_S3 -server S3_server_name -container
-name bucket_name -access-key access_key -secret-password password
```

- Der `-container-name` Ist der von Ihnen erstellte S3-Bucket.
- Der `-access-key` Parameter autorisiert Anfragen an den ONTAP S3-Server.
- Der `-secret-password` Parameter (Secret Access Key) authentifiziert Anforderungen an den ONTAP S3-Server.
- Sie können die einstellen `-is-certificate-validation-enabled` Parameter an `false` So deaktivieren Sie die Zertifikatprüfung für ONTAP S3.

```
cluster1::> storage aggregate object-store config create
-object-store-name MyLocalObjStore -ipospace 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: Um zu sehen, wie viele Daten in einem Volume inaktiv sind, führen Sie die Schritte unter aus ["Bestimmen der Menge an Daten in einem Volume, die inaktiv sind, mithilfe der inaktiven Datenberichterstellung"](#).

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 das verwenden `allow-flexgroup true` Sie können Aggregate hinzufügen, die FlexGroup Volume-Komponenten enthalten.

```
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

Aktivieren des Client-Zugriffs über eine S3-Applikation

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 Clients Informationen zum Tagging abrufen und einfügen können, werden die Aktionen durchgeführt `GetObjectTagging`, `PutObjectTagging`, und `DeleteObjectTagging`. Es müssen die Bucket- oder Gruppenrichtlinien verwendet werden.

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

Definitionen von Storage-Services

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
FlexArray-LUN	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

Buckets werden mit S3 SnapMirror geschützt

Übersicht über S3 SnapMirror

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 S3 SnapMirror Spiegelung und Backups an Ziele anderer Anbieter wie AWS S3.

S3 SnapMirror unterstützt aktive Spiegelungen und Backup Tiers von ONTAP S3 Buckets für die folgenden Ziele:

Ziel	Unterstützt aktive Spiegelungen und Takeover?	Unterstützung für Backup und Restore?
ONTAP S3 <ul style="list-style-type: none"> • Buckets in derselben SVM • Buckets in verschiedenen SVMs im selben Cluster • Buckets in SVMs auf verschiedenen Clustern 	✓	✓
StorageGRID		✓
AWS S3		✓
Cloud Volumes ONTAP für Azure	✓	✓
Cloud Volumes ONTAP für AWS	✓	✓
Cloud Volumes ONTAP für Google Cloud	✓	✓

Sie können vorhandene Buckets auf ONTAP S3 Servern sichern oder neue Buckets erstellen, wobei die Datensicherung sofort aktiviert ist.

Anforderungen für S3 SnapMirror

- ONTAP-Version
ONTAP 9.10.1 oder höher muss auf Quell- und Ziel-Clustern ausgeführt werden.
- Lizenzierung die folgenden Lizenzpakete sind auf ONTAP Quell- und Zielsystemen erforderlich:
 - Core Bundle für ONTAP S3-Protokoll und Storage
 - Datensicherungs-Bundle für S3 SnapMirror zur Zielvorgabe für andere NetApp Objektspeicher-Ziele (ONTAP S3, StorageGRID und Cloud Volumes ONTAP)
 - Data Protection Bundle und Hybrid Cloud Bundle
Für S3 SnapMirror als Ziel für Objektspeicher von Drittanbietern, einschließlich AWS S3.
- 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 CA-Zertifikate, die zum Signieren der S3-Server-Zertifikate verwendet werden, müssen auf der Admin Storage-VM der Cluster installiert sein, 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).
 - 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
 - Für alle S3 SnapMirror Beziehungen ist eine S3-spezifische Richtlinie erforderlich. Diese Richtlinie kann jedoch für diverse Beziehungen verwendet werden.
 - 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).
- Root-Benutzerschlüssel Storage-VM-Root-Benutzerzugriffsschlüssel sind für S3-SnapMirror-Beziehungen erforderlich; ONTAP weist sie nicht standardmäßig zu. Wenn Sie zum ersten Mal eine S3 SnapMirror Beziehung erstellen, müssen Sie überprüfen, ob die Schlüssel sowohl auf den Quell- als auch auf dem Ziel-Storage VMs vorhanden sind, und diese neu generieren, wenn sie nicht. 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 zur S3-Konfiguration"](#)

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

S3 SnapMirror unterstützt Fan-out- und Kaskadenbeziehungen. Eine Übersicht finden Sie unter ["Fan-out- und kaskadierende Datensicherungsimplementierungen"](#).

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

Steuerung des Zugriffs auf S3 Buckets

Beim Erstellen neuer Buckets können Sie den Zugriff durch Erstellen von Benutzern und Gruppen steuern. 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 \(CLI\)"](#)

Spiegelung und Backup-Schutz auf einem Remote-Cluster

Erstellen einer Spiegelbeziehung für einen neuen Bucket (Remote-Cluster)

Wenn Sie neue S3-Buckets erstellen, können Sie sie unmittelbar in einem S3-SnapMirror-Ziel in einem Remote-Cluster sichern.


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 S3 SnapMirror Beziehung für diese Storage-VM ist, überprüfen Sie, ob die Root-Benutzerschlüssel für Quell- und Ziel-Storage VMs vorhanden sind, und generieren Sie sie erneut, wenn sie nicht:
 - a. Klicken Sie auf **Storage > Storage VMs** und wählen Sie dann die Speicher-VM aus.
 - b. Klicken Sie auf der Registerkarte **Einstellungen** auf  In der Kachel **S3**.
 - c. Überprüfen Sie auf der Registerkarte **Benutzer**, ob für den Root-Benutzer ein Zugriffsschlüssel vorhanden ist.
 - d. Falls nicht, klicken Sie auf  Klicken Sie neben **root** auf **Schlüssel neu generieren**. 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 **Storage > Storage VMs**, klicken Sie auf die Speicher-VM, klicken Sie auf **Einstellungen** und dann auf  Unter S3.

Siehe "[Fügen Sie S3-Benutzer und -Gruppen hinzu](#)" Finden Sie weitere Informationen.

3. Auf dem Quell-Cluster, erstellen Sie eine S3 SnapMirror Politik wenn Sie nicht haben eine bestehende und Sie wollen nicht die Standard-Policy verwenden:
 - a. Klicken Sie auf **Schutz > Übersicht** und dann auf **Lokale Richtlinienereinstellungen**.
 - b. Klicken Sie Auf  Klicken Sie neben **Schutzrichtlinien** auf **Hinzufügen**.
 - Geben Sie den Namen und die Beschreibung der Richtlinie ein.
 - Wählen Sie den Richtlinienumfang, das Cluster oder die SVM aus
 - Wählen Sie * Continuous* für S3 SnapMirror Beziehungen.
 - 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.

Siehe "[Management des Benutzerzugriffs auf Buckets](#)" Weitere Informationen zu diesen Feldern.

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 Objektsperre für Ziel-Buckets aktivieren, sofern auf den Quell- und Ziel-Clustern ONTAP 9.14.1 oder höher ausgeführt wird und die Objektsperre 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 Objektsperre auf einem Bucket finden Sie unter ["Erstellen eines Buckets"](#).

CLI

1. Wenn dies die erste S3 SnapMirror Beziehung für diese SVM ist, überprüfen Sie, ob die Root-Benutzerschlüssel für Quell- und Ziel-SVMs vorhanden sind, und generieren Sie sie erneut, wenn sie dies nicht tun:

```
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 S3-SnapMirror-Richtlinie, wenn keine vorhandene Richtlinie vorhanden ist und Sie 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 Policy-Art für S3 SnapMirror-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 Quellcluster das CA-Zertifikat, das das *Destination* S3-Serverzertifikat unterzeichnet 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.

Siehe `security certificate install` Man-Page für Details.

6. Erstellen Sie auf der Quell-SVM eine S3-SnapMirror 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. Überprüfen Sie, ob die Spiegelung aktiv ist:

```
snapmirror show -policy-type continuous -fields status
```

Erstellen einer Spiegelbeziehung für einen vorhandenen Bucket (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 S3 SnapMirror Beziehung für diese Storage-VM ist, überprüfen Sie, ob die Root-Benutzerschlüssel für Quell- und Ziel-Storage VMs vorhanden sind, und generieren Sie sie erneut, wenn sie nicht:
 - a. Wählen Sie **Storage > Storage VMs** aus und wählen Sie dann die Storage VM aus.
 - b. Klicken Sie auf der Registerkarte **Einstellungen** auf  In der Kachel **S3**.
 - c. Überprüfen Sie auf der Registerkarte **Benutzer**, ob für den Root-Benutzer ein Zugriffsschlüssel vorhanden ist.
 - d. Falls nicht, klicken Sie auf  Klicken Sie neben **root** dann auf **Schlüssel erneut generieren**. Generieren Sie den Schlüssel nicht neu, wenn er bereits existiert.
2. Vergewissern Sie sich, dass der Benutzer- und Gruppenzugriff sowohl auf den Quell- als auch auf den Ziel-Storage-VMs korrekt ist:
Wählen Sie **Storage > Storage VMs**, und wählen Sie dann die Storage VM und dann **Settings** aus. Wählen Sie abschließend aus  Unter **S3**.

Siehe "[Fügen Sie S3-Benutzer und -Gruppen hinzu](#)" Finden Sie weitere Informationen.

3. Auf dem Quell-Cluster, erstellen Sie eine S3 SnapMirror Politik wenn Sie nicht haben eine bestehende und Sie wollen nicht die Standard-Policy verwenden:
 - a. Wählen Sie **Schutz > Übersicht** und klicken Sie dann auf **Einstellungen für lokale Richtlinien**.
 - b. Wählen Sie  Klicken Sie neben **Schutzrichtlinien** 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 * Continuous* für S3 SnapMirror Beziehungen.
 - 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 auf der Registerkarte **Berechtigungen** auf  **Bearbeiten**, dann klicken Sie 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 Standardeinstellungen (*bucketname*, *bucketname/**) Oder andere Werte, die Sie benötigen.

Siehe "[Management des Benutzerzugriffs auf Buckets](#)" Weitere Informationen zu diesen Feldern.

5. Schutz eines vorhandenen Buckets durch S3 SnapMirror 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 Objektsperre für Ziel-Buckets aktivieren, sofern auf den Quell- und Ziel-Clustern ONTAP 9.14.1 oder höher ausgeführt wird und die Objektsperre 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 Objektsperre auf einem Bucket finden Sie unter ["Erstellen eines Buckets"](#).

CLI

1. Wenn dies die erste S3 SnapMirror Beziehung für diese SVM ist, überprüfen Sie, ob die Root-Benutzerschlüssel für Quell- und Ziel-SVMs vorhanden sind, und generieren Sie sie erneut, wenn sie dies nicht tun:

`vserver object-store-server user show`+ Überprüfen Sie, 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. 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. Auf der Quell-SVM, erstellen Sie eine S3 SnapMirror- Politik wenn Sie keine bestehende haben und Sie nicht die Default-Richtlinie verwenden möchten:

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

Parameter:

- continuous – Der einzige Richtlinientyp für S3 SnapMirror Beziehungen (erforderlich).
- -rpo – Gibt die Zeit für den Wiederherstellungspunkt 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 Quellcluster das CA-Zertifikat, das das *Destination* S3-Serverzertifikat unterzeichnet 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 Zertifikat verwenden, das von einem externen CA-Anbieter signiert wurde, installieren Sie dasselbe Zertifikat auf der Quell- und Ziel-Administrator-SVM.

Siehe `security certificate install` Man-Page für Details.

6. Erstellen Sie auf der Quell-SVM eine S3-SnapMirror 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. Überprüfen Sie, ob die Spiegelung aktiv ist:

```
snapmirror show -policy-type continuous -fields status
```

Übernahme und Bereitstellung von Daten vom Ziel-Bucket (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 der Quell-Bucket in schreibgeschützt umgewandelt und der ursprüngliche Ziel-Bucket in Lese-/Schreibzugriff umgewandelt, sodass die S3 SnapMirror Beziehung rückgängig gemacht wird.

Wenn der deaktivierte Quell-Bucket wieder verfügbar ist, werden die Inhalte der beiden Buckets von S3 SnapMirror automatisch neu synchronisiert. 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.

System Manager

Failover aus dem nicht verfügbaren Bucket und Beginn der Datenbereitstellung:

1. Klicken Sie auf **Schutz > Beziehungen** und wählen Sie dann **S3 SnapMirror**.
2. Klicken Sie Auf  Wählen Sie **Failover** und klicken Sie dann auf **Failover**.

CLI

1. Initiieren eines Failover-Vorgangs 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
```

Wiederherstellung eines Buckets aus der Ziel-Storage-VM (Remote-Cluster)

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 **S3 SnapMirror**.
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
Siehe "[Storage Service Level](#)" Finden Sie weitere Informationen.
 - 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 Objektsperre aktiviert ist, kann ein Bucket wiederhergestellt werden, indem ein Bucket erstellt wird, für den auch die Objektsperre aktiviert ist. Wenn Sie einen gesperrten Bucket wiederherstellen, werden der Objektsperremodus 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 Objektsperre auf einem Bucket nicht aktiviert ist, können Sie sie in einem Bucket wiederherstellen, der die Objektsperre 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 "[Backup-Beziehung für einen neuen Bucket erstellen \(Cloud-Ziel\)](#)".
2. Initiieren eines Restore-Vorgangs 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
```

Spiegelung und Backup-Schutz auf dem lokalen Cluster




Erstellen einer Spiegelbeziehung für einen neuen Bucket (lokales Cluster)

Wenn Sie neue S3-Buckets erstellen, können Sie sie unmittelbar in einem S3-SnapMirror-Ziel im selben Cluster sichern. 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 S3 SnapMirror Beziehung für diese Storage-VM ist, überprüfen Sie, ob die Root-Benutzerschlüssel für Quell- und Ziel-Storage VMs vorhanden sind, und generieren Sie sie erneut, wenn sie nicht:
 - a. Klicken Sie auf **Storage > Storage VMs** und wählen Sie dann die Speicher-VM aus.
 - b. Klicken Sie auf der Registerkarte **Einstellungen** auf  Im S3-Tile.
 - c. Überprüfen Sie auf der Registerkarte **Benutzer**, ob für den Root-Benutzer ein Zugriffsschlüssel vorhanden ist
 - d. Falls nicht, klicken Sie auf  Klicken Sie neben **root** auf **Schlüssel neu generieren**. Generieren Sie den Schlüssel nicht neu, wenn er bereits vorhanden ist.
2. Bearbeiten Sie die Speicher-VM, um Benutzer hinzuzufügen und um Benutzer zu Gruppen hinzuzufügen, sowohl in den Quell- und Ziel-Speicher-VMs: Klicken Sie auf **Storage > Speicher-VMs**, klicken Sie auf die Speicher-VM, klicken Sie auf **Einstellungen** und klicken Sie dann auf  Unter S3.

Siehe "[Fügen Sie S3-Benutzer und -Gruppen hinzu](#)" Finden Sie weitere Informationen.

3. Erstellen Sie eine S3 SnapMirror Politik wenn Sie keine bestehende haben und Sie die Standardrichtlinie nicht verwenden möchten:
 - a. Klicken Sie auf **Schutz > Übersicht** und dann auf **Einstellungen für lokale Richtlinien**.
 - b. Klicken Sie Auf  Klicken Sie neben **Schutzrichtlinien** auf **Hinzufügen**.
 - Geben Sie den Namen und die Beschreibung der Richtlinie ein.
 - Wählen Sie den Richtlinienumfang, das Cluster oder die SVM aus
 - Wählen Sie * Continuous* für S3 SnapMirror Beziehungen.
 - 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

Siehe "[Management des Benutzerzugriffs auf Buckets](#)" Weitere Informationen zu diesen Feldern.

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 Objektsperre für Ziel-Buckets aktivieren, sofern auf den Quell- und Ziel-Clustern ONTAP 9.14.1 oder höher ausgeführt wird und die Objektsperre 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 Objektsperre auf einem Bucket finden Sie unter ["Erstellen eines Buckets"](#).

CLI

1. Wenn dies die erste S3 SnapMirror Beziehung für diese SVM ist, überprüfen Sie, ob die Root-Benutzerschlüssel für Quell- und Ziel-SVMs vorhanden sind, und generieren Sie sie erneut, wenn sie dies nicht tun:

```
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]
```

```
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 S3 SnapMirror Politik wenn Sie keine bestehende haben und Sie 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* – Der einzige Richtlinientyp für S3 SnapMirror Beziehungen (erforderlich).
- *-rpo* – Gibt die Zeit für den Wiederherstellungspunkt 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-Zertifikat, das das Zertifikat des *Destination* S3-Servers auf der Admin-SVM signiert hat:

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

Siehe `security certificate install` Man-Page für Details.

6. Erstellung einer S3 SnapMirror 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. Überprüfen Sie, ob die Spiegelung aktiv ist:

```
snapmirror show -policy-type continuous -fields status
```

Erstellen einer Spiegelbeziehung für einen vorhandenen Bucket (lokales 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 S3 SnapMirror Beziehung für diese Storage-VM ist, überprüfen Sie, ob die Root-Benutzerschlüssel für Quell- und Ziel-Storage VMs vorhanden sind, und generieren Sie sie erneut, wenn sie nicht:
 - a. Klicken Sie auf **Storage > Storage VMs** und wählen Sie dann die Speicher-VM aus.
 - b. Klicken Sie auf der Registerkarte **Einstellungen** auf  In der Kachel **S3**.
 - c. Überprüfen Sie auf der Registerkarte **Benutzer**, ob für den Root-Benutzer ein Zugriffsschlüssel vorhanden ist.
 - d. Falls nicht, klicken Sie auf  Klicken Sie neben **root** auf **Schlüssel neu generieren**. Generieren Sie den Schlüssel nicht neu, wenn er bereits vorhanden ist
2. Vergewissern Sie sich, dass der Benutzer- und Gruppenzugriff sowohl auf den Quell- als auch auf den Ziel-Storage-VMs korrekt ist:
 - Klicken Sie auf **Storage > Storage VMs**, klicken Sie auf die Speicher-VM, klicken Sie auf **Einstellungen** und dann auf  Unter S3.

Siehe "[Fügen Sie S3-Benutzer und -Gruppen hinzu](#)" Finden Sie weitere Informationen.

3. Erstellen Sie eine S3 SnapMirror Politik wenn Sie keine bestehende haben und Sie die Standardrichtlinie nicht verwenden möchten:
 - a. Klicken Sie auf **Schutz > Übersicht** und dann auf **Lokale Richtlinieneinstellung**.
 - b. Klicken Sie Auf  Klicken Sie neben **Schutzrichtlinien** auf **Hinzufügen**.
 - Geben Sie den Namen und die Beschreibung der Richtlinie ein.
 - Wählen Sie den Richtlinienumfang, das Cluster oder die SVM aus
 - Wählen Sie * Continuous* für S3 SnapMirror Beziehungen.
 - 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 auf der Registerkarte **Berechtigungen** auf  **Bearbeiten**, dann 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.

Siehe "[Management des Benutzerzugriffs auf Buckets](#)" Weitere Informationen zu diesen Feldern.

5. Schutz eines vorhandenen Buckets durch S3 SnapMirror:

- 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 Objektsperre für Ziel-Buckets aktivieren, sofern auf den Quell- und Ziel-Clustern ONTAP 9.14.1 oder höher ausgeführt wird und die Objektsperre 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 Objektsperre auf einem Bucket finden Sie unter ["Erstellen eines Buckets"](#).

CLI

1. Wenn dies die erste S3 SnapMirror Beziehung für diese SVM ist, überprüfen Sie, ob die Root-Benutzerschlüssel für Quell- und Ziel-SVMs vorhanden sind, und generieren Sie sie erneut, wenn sie dies nicht tun:

```
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. 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 S3 SnapMirror Politik wenn Sie keine bestehende haben und Sie 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 – Der einzige Richtlinientyp für S3 SnapMirror Beziehungen (erforderlich).
- -rpo – Gibt die Zeit für den Wiederherstellungspunkt 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-Zertifikat, das das Zertifikat des *Destination* S3-Servers auf der Admin-SVM signiert hat:

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

Siehe `security certificate install` Man-Page für Details.

6. Erstellung einer S3 SnapMirror 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. Überprüfen Sie, ob die Spiegelung aktiv ist:

```
snapmirror show -policy-type continuous -fields status
```

Übernahme und Bereitstellung von Daten aus dem Ziel-Bucket (lokaler 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 der Quell-Bucket in schreibgeschützt umgewandelt und der ursprüngliche Ziel-Bucket in Lese-/Schreibzugriff umgewandelt, sodass die S3 SnapMirror Beziehung rückgängig gemacht wird.

Wenn der deaktivierte Quell-Bucket wieder verfügbar ist, werden die Inhalte der beiden Buckets von S3 SnapMirror automatisch neu synchronisiert. 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 **S3 SnapMirror**.
2. Klicken Sie Auf  Wählen Sie **Failover** und klicken Sie dann auf **Failover**.

CLI

1. Initiieren eines Failover-Vorgangs 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
```

Wiederherstellen eines Buckets aus der Ziel-Storage-VM (lokales Cluster)

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 Zielspeicherplatz.

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-Zielservers-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
Siehe "[Storage Service Level](#)" Finden Sie weitere Informationen.
 - 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 Objektsperre aktiviert ist, kann ein Bucket wiederhergestellt werden, indem ein Bucket erstellt wird, für den auch die Objektsperre aktiviert ist. Wenn Sie einen gesperrten Bucket wiederherstellen, werden der Objektsperremodus 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 Objektsperre auf einem Bucket nicht aktiviert ist, können Sie sie in einem Bucket wiederherstellen, der die Objektsperre 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 "[Backup-Beziehung für einen neuen Bucket erstellen \(Cloud-Ziel\)](#)".
2. Initiieren eines Restore-Vorgangs 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
```

Backup-Sicherung mit Cloud-Zielen

Anforderungen für Cloud-Zielbeziehungen

Vergewissern Sie sich, dass Ihre Quell- und Zielumgebungen die Anforderungen für S3 SnapMirror Backup-Sicherung in der Cloud erfüllen.

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

Auf dem Cluster sollten Intercluster-Netzwerkschnittstellen und ein IPspace konfiguriert werden, bevor das Cluster eine Verbindung zu einem Cloud-Objektspeicher herstellen kann. Sie sollten auf jedem Node Cluster-Netzwerkschnittstellen erstellen, um Daten nahtlos vom lokalen Storage in den 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-Speicher-VM des ONTAP S3-Clusters mit installiert werden `security certificate install` command. 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 (falls verwendet) auf IP-Adressen aufzulösen.

Backup-Beziehung für einen neuen Bucket erstellen (Cloud-Ziel)


Wenn neue S3-Buckets erstellt werden, können diese sofort in einem S3 SnapMirror Ziel-Bucket auf einem Objektspeicher-Provider gesichert werden. Dabei kann es sich um ein

StorageGRID-System oder eine Amazon S3-Implementierung 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 **Storage > Storage VMs**, klicken Sie auf die Speicher-VM, klicken Sie auf **Einstellungen** und dann auf  Unter **S3**.

Siehe "Fügen Sie S3-Benutzer und -Gruppen hinzu" Finden Sie weitere Informationen.

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 S3 SnapMirror Politik wenn Sie keine bestehende haben und Sie die Standardrichtlinie nicht verwenden möchten:
 - a. Klicken Sie auf **Schutz > Übersicht** und dann auf **Lokale Richtlinieneinstellungen**.
 - b. Klicken Sie Auf  Klicken Sie neben **Schutzrichtlinien** auf **Hinzufügen**.
 - Geben Sie den Namen und die Beschreibung der Richtlinie ein.
 - Wählen Sie den Richtlinienumfang, das Cluster oder die SVM aus
 - Wählen Sie * Continuous* für S3 SnapMirror Beziehungen.
 - 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.

Siehe "[Management des Benutzerzugriffs auf Buckets](#)" Weitere Informationen zu diesen Feldern.

- 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 S3 SnapMirror Beziehung für diese SVM ist, überprüfen Sie, ob die Root-Benutzerschlüssel für Quell- und Ziel-SVMs vorhanden sind, und generieren Sie sie erneut, wenn sie dies nicht tun:

`vserver object-store-server user show`+ Bestätigen Sie, 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. Erstellung eines Buckets in der Quell-SVM:

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

3. 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 S3 SnapMirror Politik wenn Sie keine bestehende haben und Sie 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 S3 SnapMirror Beziehungen (erforderlich). * `-rpo` – Gibt die Zeit für den Wiederherstellungspunkt 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 Zertifikat für den StorageGRID CA-Server auf der Admin-SVM des Quell-Clusters:

```
security certificate install -type server-ca -vserver src_admin_svm -cert  
-name storage_grid_server_certificate
```

Siehe `security certificate install` Man-Page für Details.

6. S3 SnapMirror Ziel-Objektspeicher 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` – Gebrauch `data` Für diesen Workflow. * `-provider-type` – `AWS_S3` Und `SGWS` (StorageGRID) Ziele werden unterstützt. * `-server` – Der FQDN des Zielservers oder die IP-Adresse. * `-is-ssl-enabled` – Die Aktivierung von SSL ist optional, wird jedoch empfohlen. + Siehe `snapmirror object-store config create` Man-Page für Details.

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. Erstellung einer S3 SnapMirror 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 haben, und der feste Wert `objstore`.

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 sgws-store:/objstore -policy test-policy
```

8. Überprüfen Sie, ob die Spiegelung aktiv ist:

```
snapmirror show -policy-type continuous -fields status
```


Backup-Beziehung für einen vorhandenen Bucket erstellen (Cloud-Ziel)

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 richtig definiert sind: Klicken Sie auf **Storage > Storage VMs**, klicken Sie auf die Speicher-VM, klicken Sie auf **Einstellungen** und klicken Sie dann auf  Unter S3.

Siehe "[Fügen Sie S3-Benutzer und -Gruppen hinzu](#)" Finden Sie weitere Informationen.

2. Erstellen Sie eine S3 SnapMirror Politik wenn Sie keine bestehende haben und Sie die Standardrichtlinie nicht verwenden möchten:
 - a. Klicken Sie auf **Schutz > Übersicht** und dann auf **Lokale Richtlinieneinstellungen**.
 - b. Klicken Sie Auf  Klicken Sie neben **Schutzrichtlinien** 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 * Continuous* für S3 SnapMirror Beziehungen.
 - 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 auf der Registerkarte **Berechtigungen** auf  **Bearbeiten**, dann 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.

Siehe "[Management des Benutzerzugriffs auf Buckets](#)" Weitere Informationen zu diesen Feldern.

5. Backup des Buckets mithilfe von S3 SnapMirror:

- 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. Vergewissern Sie sich, dass 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,GetObjectAcl,
ListBucketMultipartUploads,ListMultipartUploadParts -principal -
-resource test-bucket, test-bucket /*
```

2. Erstellen Sie eine S3 SnapMirror Politik wenn Sie keine bestehende haben und Sie 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 S3 SnapMirror Beziehungen (erforderlich). * *-rpo* – Gibt die Zeit für den Wiederherstellungspunkt 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
```

Siehe `security certificate install` Man-Page für Details.

4. S3 SnapMirror Ziel-Objektspeicher 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 – Gebrauch data Für diesen Workflow. * -provider-type – AWS_S3 Und SGWS (StorageGRID) Ziele werden unterstützt. * -server – Der FQDN des Zielservers oder die IP-Adresse. * -is-ssl-enabled –Die Aktivierung von SSL ist optional, wird jedoch empfohlen. + Siehe snapmirror object-store config create Man-Page für Details.

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. Erstellung einer S3 SnapMirror 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 haben, und der feste Wert objstore.

Sie können eine von Ihnen erstellte Richtlinie verwenden oder die Standardeinstellung übernehmen.

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

6. Überprüfen Sie, ob die Spiegelung aktiv ist:

```
snapmirror show -policy-type continuous -fields status
```

Wiederherstellung eines 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 **S3 SnapMirror**.
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. Siehe ["Storage Service Level"](#) Finden Sie weitere Informationen.
 - 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 eines Restore-Vorgangs 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
```

Ändern einer Spiegelrichtlinie

Vielleicht möchten Sie eine S3-Spiegelrichtlinie ändern, beispielsweise wenn Sie die RPO- und Drosselwerte anpassen möchten.

System Manager

Wenn Sie diese Werte anpassen möchten, können Sie eine vorhandene Schutzrichtlinie bearbeiten.

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

CLI

Ändern einer S3-SnapMirror-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
```

Prüfung von S3-Ereignissen

Prüfung von 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. Die Sie können die folgenden zu protokollierenden Ereignisse angeben:

- Objektzugriff (Daten) Ereignisse
GetObject, PutObject und DeleteObject
- Management-Ereignisse
PutBucket und DeleteBucket

Das Protokollformat ist JavaScript Object Notation (JSON).

Der kombinierte Grenzwert für S3- und NFS-Audit-Konfigurationen beträgt 50 SVMs pro Cluster.

Das folgende Lizenzpaket ist erforderlich:

- Core Bundle 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-Auditorsystem 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:

- Eine numerische Begrenzung; die `-rotate-limit` Parameter steuert die minimale Anzahl von Überwachungsdateien, die beibehalten werden müssen.
- Ein Zeitlimit; das `-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 einer S3-Audit-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.

Siehe **vserver object-store-server audit create** Man page für Syntax Details.

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.	<code>-verserver svm_name</code>	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.	<code>-destination text</code>	Ja.
Kategorien von Ereignissen zur Prüfung Folgende Ereigniskategorien können geprüft werden: <ul style="list-style-type: none">• Data GetObject, PutObject und DeleteObject Ereignisse• Management-Events „PutBucket“ und „DeleteBucket“ Standardmäßig werden nur Datenereignisse geprüft.	<code>-events {data management}, ...</code>	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.	<code>-rotate-limit integer</code>	Nein

<p>Dauer der Protokolldateien</p> <p>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.</p> <p>Der Wert 0 gibt an, dass alle Protokolldateien aufbewahrt werden. Der Standardwert ist 0.</p>	<p><code>-retention duration</code> <code>integer_time</code></p>	<p>Nein</p>
---	---	-------------

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 Standardprotokollgröße nicht verwenden möchten, können Sie das konfigurieren `-rotate -size` Parameter zum Festlegen einer benutzerdefinierten Protokollgröße.

Wenn Sie die Drehung auf Basis einer Protokollgröße zurücksetzen möchten, können Sie die Einstellung mit dem folgenden Befehl aufheben `-rotate-schedule-minute` Parameter:

```
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 zeitbasierte Rotation verwenden, wird das angezeigt `-rotate-schedule-minute` Parameter muss angegeben werden.
- 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 die angeben `-rotate-schedule-minute` Parameter, die Audit-Log-Dateien werden auf der Grundlage der Minuten gedreht, die an allen Wochentagen, während aller Stunden an allen Monaten des Jahres angegeben sind.
- Wenn Sie nur einen oder zwei zeitbasierte Rotationsparameter angeben (z. B. `-rotate-schedule-month` Und `-rotate-schedule-minutes`), die Log-Dateien werden basierend auf den Minutenwerten, die Sie an allen Wochentagen, während aller Stunden, aber nur während der angegebenen Monate angegeben.

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 beide angeben `-rotate-schedule-dayofweek` Und `-rotate-schedule-day`, Sie werden unabhängig betrachtet.

Beispiel: Wenn Sie angeben `-rotate-schedule-dayofweek` Als Freitag und `-rotate-schedule-day` Als 13, dann werden die Audit-Protokolle an jedem Freitag und am 13. Tag des angegebenen Monats gedreht werden, nicht nur an jedem Freitag der 13...

- Wenn Sie die Rotation basierend auf einem Zeitplan allein zurücksetzen möchten, verwenden Sie den folgenden Befehl, um die Einstellung einzustellen `-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` Ist auf 10 MB und eingestellt `-rotate-schedule-minute` Ist auf 15 gesetzt, drehen sich die Protokolldateien, wenn die Protokolldateigröße 10 MB oder in der 15. Minute jeder Stunde (je nachdem, welches Ereignis zuerst eintritt) erreicht.

Erstellung und Aktivierung einer S3-Audit-Konfiguration

Für die Implementierung der S3-Prüfung wird zuerst eine persistente Objektspeicherauditierung auf einer S3-fähigen SVM erstellt, dann die Konfiguration aktiviert.

Was Sie benötigen

- Eine S3-fähige SVM
- Ausreichend Platz für das Staging von Volumes im Aggregat.

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 keine automatische Protokollrotation konfigurieren, werden alle Protokolldateien standardmäßig beibehalten. 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.

Verfahren

1. Erstellen Sie die Überwachungskonfiguration, um Prüfprotokolle basierend auf Protokollgröße oder einem

Zeitplan zu drehen.

Wenn Sie die Prüfprotokolle drehen möchten, um...	Eingeben...
Protokollgröße	<pre>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]}]</pre>
Einen Zeitplan	<pre>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</pre> <p>Der -rotate-schedule-minute Der Parameter ist erforderlich, wenn Sie die zeitbasierte Rotation des Prüfprotokolls konfigurieren.</p>

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 gedreht An allen Wochentagen. 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
```

Buckets für S3-Auditing auswählen

Sie müssen angeben, welche Buckets in einer SVM mit Audit-Aktivierung geprüft werden sollen.

Was Sie benötigen

- Eine SVM für S3-Prüfungen 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.

Das Auditing von Konfigurationen bleibt für Buckets erhalten, bis sie von entfernt werden `vserver object-store-server audit object-select delete` Befehl.

Verfahren

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 den Typ des zu prüfenden Ereigniszugangs an: `read-only`, `write-only` Oder `all` (Standardeinstellung ist `all`).
- `-permission` - Gibt die Art der zu prüfenden Ereignisberechtigung an: `allow-only`, `deny-only` Oder `all` (Standardeinstellung 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 einer S3-Audit-Konfiguration

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	<pre>vserver object-store-server audit event-selector modify -vserver svm_name [-bucket bucket_name] [parameters to modify]</pre>

Wenn Sie die Audit-Konfiguration ändern möchten für...	Eingeben...
Alle Buckets in der SVM	<code>vserver object-store-server audit modify -vserver svm_name [parameters to modify]</code>

Beispiele

Im folgenden Beispiel wird eine individuelle Bucket-Audit-Konfiguration geändert, um nur schreibgeschützten Zugriffseignisse 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
```

Zeigt 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 das `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 die `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 angeben `-fields` Parameter, um anzugeben, welche Audit-Konfigurationsinformationen angezeigt werden sollen.

Verfahren

Informationen zu S3-Audit-Konfigurationen anzeigen:

Wenn Sie die Konfiguration ändern möchten für...	Eingeben...
Buckets	<code>vserver object-store-server audit event-selector show [-vserver <i>svm_name</i>] [<i>parameters</i>]</code>
SVMs	<code>vserver object-store-server audit show [-vserver <i>svm_name</i>] [<i>parameters</i>]</code>

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
```

Vserver	Rotation File Size	Rotation Schedule	Rotation 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
```


Copyright-Informationen

Copyright © 2024 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtsinhabers in keiner Form und durch keine Mittel – weder grafische noch elektronische oder mechanische, einschließlich Fotokopieren, Aufnehmen oder Speichern in einem elektronischen Abrufsystem – auch nicht in Teilen, vervielfältigt werden.

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

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

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

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

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

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

Markeninformationen

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