S3-Client-Zugriff auf NAS-Daten

ONTAP 9

NetApp
February 12, 2026

Inhalt

S3-Client-Zugriff auf NAS-Daten

Erfahren Sie mehr über die Multiprotokollunterstützung von ONTAP S3

Ab ONTAP 9.12.1 können Kunden, die das S3-Protokoll ausführen, auf dieselben Daten zugreifen, die Clients zur Verfügung stehen, die die Protokolle NFS und SMB verwenden, ohne dass sie neu formatiert werden müssen. Dank dieser Funktion können NAS-Daten weiterhin an NAS-Clients bereitgestellt werden, während S3-Clients, auf denen S3-Applikationen ausgeführt werden (z. B. Data Mining und künstliche Intelligenz), Objektdaten verfügbar sind.

S3-Multiprotokoll-Funktion unterstützt zwei Anwendungsfälle:

1. Zugriff auf vorhandene NAS-Daten über S3-Clients

   Wenn Ihre vorhandenen Daten mit herkömmlichen NAS-Clients (NFS oder SMB) erstellt wurden und sich auf NAS-Volumes (FlexVol oder FlexGroup Volumes) befinden, können Sie Analysetools auf S3-Clients verwenden, um auf diese Daten zuzugreifen.

2. Back-End-Storage für moderne Clients, die I/O mithilfe von NAS- und S3-Protokollen durchführen können

   Sie können integrierten Zugriff für Anwendungen wie Spark und Kafka bereitstellen, die mithilfe der NAS- und S3-Protokolle dieselben Daten lesen und schreiben können.

Funktionsweise der S3-Multi-Protokoll-Unterstützung

Dank der ONTAP Multiprotokollunterstützung können Sie denselben Datensatz als Dateihierarchie oder als Objekte in einem Bucket darstellen. Zu diesem Zweck erstellt ONTAP „S3 NAS-Buckets“, die es S3-Clients ermöglichen, mithilfe von S3-Objektanforderungen Dateien im NAS-Speicher zu erstellen, zu lesen, zu löschen und aufzuzählen. Diese Zuordnung entspricht der NAS-Sicherheitskonfiguration, beachtet die Zugriffsberechtigungen für Dateien und Verzeichnisse und schreibt bei Bedarf in den Sicherheitsprüfpfad.

Diese Zuordnung wird erreicht, indem eine angegebene NAS-Verzeichnishierarchie als S3-Bucket präsentiert wird. Jede Datei in der Verzeichnishierarchie wird als S3-Objekt dargestellt, dessen Name relativ vom zugeordneten Verzeichnis nach unten ist, wobei die Verzeichnisgrenzen durch das Schrägstrich-Zeichen ('/') dargestellt werden.

ONTAP-definierte S3-Benutzer können auf diesen Storage zugreifen, gemäß den Bucket-Richtlinien, die für den Bucket definiert sind, der dem NAS-Verzeichnis zugeordnet ist. Hierfür müssen zwischen den S3 Benutzern und SMB/NFS Benutzern Zuordnungen definiert werden. Die Zugangsdaten des SMB/NFS-Benutzers werden für die Überprüfung der NAS-Berechtigungen verwendet und in alle Audit-Datensätze aufgenommen, die sich aus diesen Zugriffen ergeben.

Durch SMB- oder NFS-Clients wird eine Datei sofort in einem Verzeichnis abgelegt und somit für Clients sichtbar, bevor sie darauf geschrieben wird. S3-Clients erwarten unterschiedliche Semantik, wobei das neue Objekt erst sichtbar ist, wenn alle Daten geschrieben wurden. Durch diese Zuordnung von S3 zu NAS-Storage werden Dateien mithilfe von S3-Semantik erstellt, sodass die Dateien extern unsichtbar bleiben, bis der S3-Erstellungsbefehl abgeschlossen ist.

Datensicherung für S3 NAS Buckets

S3 NAS-„Buckets“ sind lediglich Zuordnungen von NAS-Daten für S3-Clients, es handelt sich nicht um Standard-S3-Buckets. Daher besteht keine Notwendigkeit, S3-NAS-Buckets mit der NetApp SnapMirror S3-Funktionalität zu schützen. Stattdessen können Sie Volumes mit S3 NAS-Buckets mithilfe der asynchronen Volume-Replikation von SnapMirror schützen. Die synchrone SnapMirror und SVM-Notfallwiederherstellung wird nicht unterstützt.

Ab ONTAP 9.14.1 werden S3 NAS-Buckets in gespiegelten und nicht gespiegelten Aggregaten für MetroCluster IP- und FC-Konfigurationen unterstützt.

Erfahren Sie mehr über "SnapMirror asynchron".

Prüfung für S3-NAS-Buckets

Da es sich bei S3-NAS-Buckets nicht um herkömmliche S3-Buckets handelt, kann das S3-Audit nicht für deren Zugriff konfiguriert werden. Erfahren Sie mehr über "S3-Audit".

Dennoch können die in S3-NAS-Buckets zugeordneten NAS-Dateien und Verzeichnisse mithilfe konventioneller ONTAP-Auditverfahren auf Zugriffsereignisse geprüft werden. S3-Vorgänge können daher NAS-Audit-Ereignisse mit folgenden Ausnahmen auslösen:

- Wenn der S3-Client-Zugriff über die S3-Richtlinienkonfiguration (Gruppen- oder Bucket-Richtlinie) verweigert wird, wird keine NAS-Prüfung für das Ereignis initiiert. Dies liegt daran, dass S3-Berechtigungen geprüft werden, bevor SVM-Audits durchgeführt werden können.
- Wenn die Zieldatei einer S3-get-Anforderung 0 Größe hat, wird der Inhalt 0 an die get-Anforderung zurückgegeben und der Lesezugriff wird nicht protokolliert.
- Wenn sich die Zieldatei einer S3-get-Anforderung in einem Ordner befindet, für den der Benutzer keine Traverse-Berechtigung hat, schlägt der Zugriffsversuch fehl und das Ereignis wird nicht protokolliert.

Erfahren Sie mehr über "Prüfung von NAS-Ereignissen auf SVMs".

Mehrteiliges Objekt-Upload

Ab ONTAP 9.16.1 wird Objekt-Multi-Part-Upload in S3 NAS Buckets unterstützt, wenn "Erweiterter Kapazitätsausgleich"diese für das zugrunde liegende FlexGroup Volume aktiviert sind.

Durch Objekt-Multi-Part-Upload auf NAS File Storage kann ein S3-Protokoll-Client große Objekte in kleineren Teilen hochladen. Das Hochladen von mehrteiligen Objekten bietet folgende Vorteile:

- Es ermöglicht das parallele Hochladen von Objekten.
- Bei einem Upload-Fehler oder einer Pause müssen nur die Teile hochgeladen werden, die noch nicht hochgeladen wurden. Der Upload des gesamten Objekts muss nicht neu gestartet werden.
- Wenn die Objektgröße nicht im Voraus bekannt ist (z. B. wenn ein großes Objekt noch geschrieben wird), können Clients sofort mit dem Hochladen von Teilen des Objekts beginnen und den Upload nach der Erstellung des gesamten Objekts abschließen.

Mehrteilige Objekte in S3 NAS-Buckets müssen in ganzen Größen und nicht in Teilgrößen ausgerichtet sein. Zum Beispiel kann ein Teil 4MB oder 4GB oder eine ähnliche Größe haben. Ein Teil kann keine Teil- oder Unter-MB-Größen wie 4.5MB oder 4000.5MB verwenden.

Multipart Upload unterstützt die folgenden S3-Aktionen:

- AbortMehrteilaUpload
- CompleteMultipartUpload
- CopyObject (ab ONTAP 9.17.1)
- CreateMultipartUpload

  Ab ONTAP 9.17.1 unterstützt CreateMultipartUpload Tagging und Schlüssel-/Wertpaare für Benutzermetadaten.

- ListenMehrpartUpload
- UploadTeil

DAS ABRUFEN nach Teilenummer („Teilenummer=xx“) wird in S3 NAS-Buckets nicht unterstützt. Stattdessen wird das vollständige Objekt zurückgegeben.

S3- und NAS-Interoperabilität

ONTAP S3 NAS Buckets unterstützen NAS- und S3-Standardfunktionen, ausgenommen die hier aufgeführt.

Die NAS-Funktionen werden derzeit von S3 NAS Buckets nicht unterstützt

FabricPool Kapazitäts-Tier

S3 NAS-Buckets können nicht als Kapazitäts-Tier für FabricPool konfiguriert werden.

S3-Aktionen und -Funktionen werden derzeit nicht von S3 NAS-Buckets unterstützt

Aktionen

- ByPassGovernanceRetention
- DeleteBucketLifecycleKonfiguration
- GetBucketLifecycleKonfiguration
- GetBucketObjectLockKonfiguration
- GetBucketVersioning
- GetObjectRetention
- ListBucketVersioning
- ListObjectVersions
- PutBucketLifecycleKonfiguration
- PutBucketVersioning
- PutObjectLockKonfiguration
- PutObjectRetention

Diese S3-Aktionen werden speziell bei der Verwendung von S3 in S3-NAS-Buckets nicht unterstützt. Bei Verwendung nativer S3-Buckets sind diese Aktionen "Wird normal unterstützt".

AWS Benutzer-Metadaten

- Ab ONTAP 9.17.1 Unterstützung für Metadaten mit mehrteiligen Objekten.
- Ab ONTAP 9.16.1 wird die Verwendung von Metadaten mit einteiligen Objekten unterstützt.

- Bei ONTAP 9.15.1 und älteren Versionen werden Schlüsselwerte-Paare, die als Teil der S3 Benutzer-Metadaten empfangen wurden, nicht zusammen mit Objektdaten auf Festplatte gespeichert.
- Bei ONTAP 9.15.1 und früher werden Anforderungsheader mit dem Präfix "x-amz-meta" ignoriert.

AWS-Tags

- Ab ONTAP 9.17.1 Unterstützung für Tags mit mehrteiligen Objekten.
- Ab ONTAP 9.16.1 wird die Verwendung von Tags mit einteiligen Objekten unterstützt.
- Bei PUT-Objekt- und Multipart-Initialanforderungen ab ONTAP 9.15.1 werden Header mit dem Präfix „x-amz-Tagging“ ignoriert.
- Bei ONTAP 9.15.1 und früheren Versionen werden Anfragen zum Aktualisieren von Tags auf einer vorhandenen Datei (Put, get und Delete Requests with the ?Tagging query-string) mit einem Fehler abgelehnt.

Versionierung

Es ist nicht möglich, die Versionierung in der Bucket-Mapping-Konfiguration anzugeben.

- Anfragen, die nicht-Null-Versionsangaben (die versionId=xyz query-string) enthalten, erhalten Fehlerantworten.
- Anfragen, die sich auf den Versionierungsstatus eines Buckets auswirken, werden mit Fehlern abgelehnt.

Informieren Sie sich über die NAS-Datenanforderungen für den ONTAP S3-Clientzugriff

Es ist wichtig zu verstehen, dass es einige inhärente Inkompatibilitäten beim Zuordnen von NAS-Dateien und Verzeichnissen für S3-Zugriff gibt. Unter Umständen müssen NAS-Dateihierarchien angepasst werden, bevor sie über S3 NAS Buckets bereitgestellt werden.

Ein S3-NAS-Bucket bietet S3-Zugriff auf ein NAS-Verzeichnis, indem dieses Verzeichnis mithilfe der S3-Bucket-Syntax zugeordnet wird. Die Dateien in der Verzeichnisstruktur werden als Objekte angezeigt. Die Objektnamen sind die durch Schrägstriche getrennten Pfadnamen der Dateien relativ zum in der S3-Bucket-Konfiguration angegebenen Verzeichnis.

Diese Zuordnung enthält einige Anforderungen, wenn Dateien und Verzeichnisse über S3 NAS Buckets bereitgestellt werden:

- S3-Namen sind auf 1024 Byte beschränkt, daher ist der Zugriff auf Dateien mit längeren Pfadnamen über S3 nicht möglich.
- Die Datei- und Verzeichnisnamen sind auf 255 Zeichen beschränkt, sodass ein Objektname nicht mehr als 255 aufeinanderfolgende Zeichen ohne Schrägstrich (‘/’) enthalten kann
- Ein SMB-Pfadname, der durch Backslash (‘\’)-Zeichen getrennt wird, erscheint S3 als Objektname mit Vorwärtsschrägstrich (‘/’) Zeichen.
- Einige Paare gültiger S3-Objektnamen können im zugeordneten NAS-Verzeichnisbaum nicht koexistieren. Beispielsweise werden die gültigen S3-Objektnamen „part1/part2“ und „part1/part2/part3“ Dateien zugeordnet, die nicht gleichzeitig im NAS-Verzeichnisbaum vorhanden sein können, da „part1/part2“ im ersten Namen eine Datei und im anderen ein Verzeichnis ist.
  - Wenn „part1/part2“ eine vorhandene Datei ist, schlägt eine S3-Erstellung von „part1/part2/part3“ fehl.

- Wenn „part1/part2/part3“ eine vorhandene Datei ist, schlägt eine S3-Erstellung oder -Löschung von „part1/part2“ fehl.
- Bei einer S3-Objekterstellung, die mit dem Namen eines vorhandenen Objekts übereinstimmt, werden das vorhandene Objekt (in nicht versionierten Buckets) ersetzt. Das Objekt befindet sich in NAS, benötigt jedoch einen genauen Abgleich. Die obigen Beispiele führen nicht zum Entfernen des vorhandenen Objekts, da die Namen nicht übereinstimmen, während die Namen kollidieren.

Während ein Objektspeicher für die Unterstützung einer sehr großen Anzahl beliebiger Namen ausgelegt ist, können bei einer NAS-Verzeichnisstruktur Leistungsprobleme auftreten, wenn eine sehr große Anzahl von Namen in einem Verzeichnis abgelegt wird. Insbesondere werden alle Namen ohne Schrägstrich ('/') im Stammverzeichnis der NAS-Zuordnung abgelegt. Anwendungen, die häufig Namen verwenden, die nicht „NAS-freundlich“ sind, sollten besser in einem tatsächlichen Objektspeicher-Bucket als in einer NAS-Zuordnung gehostet werden.

Aktivieren Sie den S3-Protokollzugriff auf NAS-Daten auf einem ONTAP SVM

Durch die Aktivierung des S3-Protokollzugriffs wird sichergestellt, dass eine NAS-fähige SVM dieselben Anforderungen erfüllt wie ein S3-fähiger Server. Dazu gehört auch das Hinzufügen eines Objektspeicher-Servers sowie die Überprüfung von Netzwerk- und Authentifizierungsanforderungen.

Bei neuen Installationen von ONTAP sollten Sie den S3-Protokollzugriff auf eine SVM aktivieren, nachdem Sie sie für die Bereitstellung von NAS-Daten für die Clients konfiguriert haben. Weitere Informationen zur Konfiguration von NAS-Protokollen finden Sie unter:

- "NFS-Konfiguration"
- "SMB-Konfiguration"

Bevor Sie beginnen

Vor Aktivierung des S3-Protokolls muss Folgendes konfiguriert werden:

- Das S3-Protokoll und die gewünschten NAS-Protokolle – NFS, SMB oder beides – sind lizenziert.
- Eine SVM wird für die gewünschten NAS-Protokolle konfiguriert.
- Es existieren NFS- und/oder SMB-Server.
- DNS und alle anderen erforderlichen Dienste werden konfiguriert.
- NAS-Daten werden exportiert oder an Client-Systeme freigegeben.

Über diese Aufgabe

Um den HTTPS-Datenverkehr von S3-Clients auf die S3-fähige SVM zu aktivieren, ist ein CA-Zertifikat erforderlich. CA-Zertifikate aus drei Quellen können verwendet werden:

- Ein neues eigensigniertes ONTAP-Zertifikat auf der SVM.
- Ein vorhandenes ONTAP selbstsigniertes Zertifikat auf der SVM.
- Ein Zertifikat eines Drittanbieters.

Sie können dieselben Daten-LIFs für den S3/NAS-Bucket verwenden, die Sie für die Bereitstellung von NAS-Daten verwenden. Wenn bestimmte IP-Adressen erforderlich sind, siehe "Erstellung von Daten-LIFs". Um den S3-Datenverkehr auf LIFs zu aktivieren, ist eine Datenrichtlinie für den S3-Service erforderlich. Sie können die

vorhandene Servicerichtlinie der SVM auf S3 ändern.

Wenn Sie den S3-Objektserver erstellen, sollten Sie darauf vorbereitet sein, den S3-Servernamen als vollständig qualifizierter Domain-Name (FQDN) einzugeben, den Clients für den S3-Zugriff verwenden. Der FQDN des S3-Servers darf nicht mit einem Bucket-Namen beginnen.

System Manager

1. Aktivieren Sie S3 auf einer Storage-VM mit konfigurierten NAS-Protokollen.
   a. Klicken Sie auf **Speicher > Speicher-VMs**, wählen Sie eine NAS-fähige Speicher-VM aus, klicken Sie auf Einstellungen, und klicken Sie dann ⚙ unter S3.
   b. Wählen Sie den Zertifikatstyp aus. Unabhängig davon, ob Sie ein vom System generiertes Zertifikat oder ein eigenes Zertifikat auswählen, wird es für den Client-Zugriff erforderlich sein.
   c. Geben Sie die Netzwerkschnittstellen ein.
2. Wenn Sie das vom System generierte Zertifikat ausgewählt haben, werden Ihnen die Zertifikatsinformationen angezeigt, wenn die Erstellung der neuen Storage-VM bestätigt wurde. Klicken Sie auf **Download** und speichern Sie es für den Client-Zugriff.
   ◦ Der Geheimschlüssel wird nicht mehr angezeigt.
   ◦ Wenn Sie die Zertifikatinformation erneut benötigen: Klicken Sie auf **Storage > Storage VMs**, wählen Sie die Speicher-VM aus und klicken Sie auf **Einstellungen**.

CLI

1. Vergewissern Sie sich, dass das S3-Protokoll auf SVM: + zulässig ist `vserver show -fields allowed-protocols`
2. Notieren Sie das Zertifikat für den öffentlichen Schlüssel dieser SVM. + Wenn ein neues selbstsigniertes ONTAP-Zertifikat benötigt wird, siehe "Erstellen und installieren Sie ein CA-Zertifikat auf der SVM".
3. Die Service-Datenrichtlinie aktualisieren
   a. Zeigt die Service-Datenrichtlinie für SVM + an `network interface service-policy show -vserver` *`svm_name`*

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

   b. Fügen Sie `data-core` und hinzu `data-s3-server services`, wenn sie nicht vorhanden sind. `network interface service-policy add-service -vserver` *`svm_name`* `-policy` *`policy_name`* `-service data-core,data-s3-server`
4. Überprüfen Sie, ob die Daten-LIFs auf der SVM Ihre Anforderungen erfüllen: `network interface show -vserver` *`svm_name`*

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

5. Erstellen Sie den S3-Server: `vserver object-store-server create -vserver` *`svm_name`* `-object-store-server` *`s3_server_fqdn`* `-certificate-name` *`ca_cert_name`* `-comment text [additional_options]`

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

- HTTPS ist standardmäßig an Port 443 aktiviert. Sie können die Portnummer mit der Option -Secure -Listener-Port ändern. + Wenn HTTPS aktiviert ist, sind CA-Zertifikate für die ordnungsgemäße Integration mit SSL/TLS erforderlich. Ab ONTAP 9.15.1 wird TLS 1.3 auch für S3-Objektspeicher unterstützt.
- HTTP ist standardmäßig deaktiviert; wenn diese Option aktiviert ist, wartet der Server auf Port 80. Sie

können sie mit der Option -is-http-enabled aktivieren oder die Portnummer mit der Option -Listener -Port ändern. + Wenn HTTP aktiviert ist, werden alle Anfragen und Antworten in Klartext über das Netzwerk gesendet.

1. Vergewissern Sie sich, dass S3 wie gewünscht konfiguriert ist:
   `vserver object-store-server show`

Beispiel + der folgende Befehl überprüft die Konfigurationswerte aller Objektspeicher-Server:

```
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
```

Verwandte Informationen

- "Service-Policy-Add-Service für die Netzwerkschnittstelle"

Erstellen Sie einen ONTAP S3 NAS-Bucket

Ein S3-NAS-Bucket ist eine Zuordnung zwischen einem S3-Bucket-Namen und einem NAS-Pfad. S3-NAS-Buckets ermöglichen Ihnen den S3-Zugriff auf jeden Teil eines SVM-Namespace mit vorhandenen Volumes und Verzeichnisstrukturen.

Bevor Sie beginnen

- Ein S3-Objektserver wird in einer SVM mit NAS-Daten konfiguriert.
- Die NAS-Daten entsprechen der "Anforderungen für S3-Client-Zugriff".

Über diese Aufgabe

Sie können S3-NAS-Buckets konfigurieren, um einen beliebigen Satz von Dateien und Verzeichnissen im Stammverzeichnis der SVM festzulegen.

Sie können außerdem Bucket-Richtlinien festlegen, die den Zugriff auf NAS-Daten ermöglichen oder aus der Kombination dieser Parameter entlassen:

- Dateien und Verzeichnisse
- Benutzer- und Gruppenberechtigungen
- S3-Betrieb

Beispielsweise möchten Sie möglicherweise eine Bucket-Richtlinie einrichten, die einer großen Gruppe von Benutzern nur Lesezugriff auf Daten gewährt, und eine andere Bucket-Richtlinie, die es einer begrenzten

Gruppe erlaubt, Operationen an einer Teilmenge dieser Daten durchzuführen.

Ab ONTAP 9.18.1 können Sie NAS-Buckets erstellen, die es Anwendungen ermöglichen, auf Daten auf FlexCache-Volumes über das S3-Protokoll zuzugreifen. Alle Knoten im Cluster müssen ONTAP 9.18.1 oder neuer ausführen. Bevor Sie mit dem S3-Protokoll auf ein FlexCache-Volume zugreifen können, müssen Sie die `-is-s3-enabled` Option auf `true` "auf dem FlexCache Volume" setzen. Der Parameter ist standardmäßig auf `false` gesetzt.

Ab ONTAP 9.17.1 können Sie einen S3-NAS-Bucket direkt mit einem Volume verknüpfen, anstatt den Junction-Pfad zu verwenden. Standardmäßig ist ein S3-Bucket auf einem NAS-Volume einem Junction-Pfad zugeordnet, der von einem ONTAP Administrator jederzeit geändert werden kann. Diese Änderungen können den Betrieb des S3-Buckets beeinträchtigen. Ab ONTAP 9.17.1 können Sie die `-is-nas-path-mutable false` Option mit der `vserver object-store-server bucket create` Befehl in der ONTAP CLI, um die Verknüpfung des S3 NAS-Buckets mit einem Volume zu aktivieren. Standardmäßig `-is-nas-path -mutable` ist eingestellt auf `true` .

Da es sich bei S3 NAS-„Buckets“ um Zuordnungen und nicht um S3-Buckets handelt, gelten die folgenden Eigenschaften von Standard-S3-Buckets nicht für S3 NAS-Buckets.

- **Aggr-list \ aggr-list-Multiplikator \ Storage-Service-Level \ Volume \ size \ exclude-aggr-list \ qos-Policy-Group** + bei der Konfiguration von S3 NAS Buckets werden keine Volumes oder qtree erstellt.
- **Rolle \ ist -geschützt \ ist -auf-OnTap-geschützt \ ist -in-Cloud-geschützt** + S3-NAS-Buckets werden nicht mit SnapMirror S3 geschützt oder gespiegelt, sondern verwenden stattdessen den regulären SnapMirror Schutz, der auf Volume-Granularitätsebene verfügbar ist.
- **Versioning-State** + NAS-Volumes verfügen in der Regel über Snapshot-Technologie zum Speichern verschiedener Versionen. Derzeit ist die Versionierung jedoch nicht in S3 NAS Buckets verfügbar.
- **Logisch-benutzte \ objektcount** + Äquivalente Statistiken stehen für NAS-Volumes über die Volume-Befehle zur Verfügung.
- **Multipart-Objekte** + Ab ONTAP 9.16.1 werden Multipart-Objekte in S3 NAS-Buckets unterstützt, wenn "Erweiterter Kapazitätsausgleich" ist auf dem zugrunde liegenden FlexGroup -Volume aktiviert. Der erweiterte Kapazitätsausgleich kann nur auf FlexGroup -Volumes aktiviert werden. Er kann nicht auf FlexVol -Volumes aktiviert werden.

Schritte

Sie können System Manager oder die ONTAP CLI verwenden, um einen NAS-Bucket zu erstellen.

System Manager

Fügen Sie einen neuen S3 NAS-Bucket auf einer NAS-fähigen Storage-VM hinzu.

1. Klicken Sie auf **Storage > Buckets** und dann auf **Hinzufügen**.
2. Geben Sie einen Namen für den S3-NAS-Bucket ein und wählen Sie die Speicher-VM aus, geben Sie keine Größe ein und klicken Sie dann auf **Weitere Optionen**.
3. Geben Sie einen gültigen Pfadnamen ein, oder klicken Sie auf Durchsuchen, um eine Liste mit gültigen Pfadnamen auszuwählen. + Wenn Sie einen gültigen Pfadnamen eingeben, werden die Optionen, die für die S3-NAS-Konfiguration nicht relevant sind, ausgeblendet.
4. Wenn Sie NAS-Benutzern und erstellten Gruppen bereits S3-Benutzer zugeordnet haben, können Sie deren Berechtigungen konfigurieren und dann auf **Speichern** klicken. + Sie müssen NAS-Benutzern bereits S3-Benutzer zugeordnet haben, bevor Sie in diesem Schritt Berechtigungen konfigurieren.

Klicken Sie andernfalls auf **Speichern**, um die S3-NAS-Bucket-Konfiguration abzuschließen.

CLI

1. Erstellen Sie einen S3 NAS-Bucket in einer SVM, die NAS-Dateisysteme enthält.
   ```
   vserver object-store-server bucket create -vserver <svm_name> -bucket
   <bucket_name> -type nas -nas-path <junction_path> -is-nas-path-mutable
   true|false [-comment <text>]
   ```

   Beispiel 1: Erstellen eines S3 NAS-Buckets

   ```
   cluster1::> vserver object-store-server bucket create -bucket testbucket
   -type nas -path /vol1
   ```

   Beispiel 2: Erstellen eines S3 NAS-Buckets und Verknüpfen des Buckets mit einem Volume

   ```
   vserver object-store-server bucket create -vserver vs1 -bucket nasbucket1
   -type nas -nas-path /pathA/dir1 -is-nas-path-mutable false
   ```

Aktivieren Sie ONTAP S3-Clientbenutzer

Um S3-Client-Benutzern den Zugriff auf NAS-Daten zu ermöglichen, müssen Sie S3-Benutzernamen den entsprechenden NAS-Benutzern zuordnen und ihnen dann mithilfe von Bucket-Service-Richtlinien die Berechtigung zum Zugriff auf die NAS-Daten erteilen.

Bevor Sie beginnen

Benutzernamen für den Clientzugriff (LINUX/UNIX-, Windows- und S3-Clientbenutzer) müssen bereits vorhanden sein.

Sie sollten beachten, dass einige S3-Funktionalität ist "Nicht von S3 NAS-Buckets unterstützt".

Über diese Aufgabe

Die Zuordnung eines S3-Benutzernamens zu einem entsprechenden LINUX/UNIX- oder Windows-Benutzer ermöglicht die Überprüfung der Berechtigungen auf die NAS-Dateien, wenn auf diese Dateien von S3-Clients zugegriffen wird. S3-zu-NAS-Zuordnungen werden durch die Angabe eines S3-Benutzernamens *Pattern*, der als einzelner Name oder POSIX-regulärer Ausdruck ausgedrückt werden kann, und eines LINUX/UNIX- oder

Windows-Benutzernamens *Replacement* angegeben.

Falls keine Namenszuweisung vorhanden ist, wird das Standard-Namenszuordnungen verwendet, wobei der S3-Benutzername selbst als UNIX-Benutzername und Windows-Benutzername verwendet wird. Sie können die UNIX- und Windows-Standardbenutzernamenzuordnungen mit dem `vserver object-store-server modify` Befehl ändern.

Es wird nur die lokale Konfiguration der Namenszuordnungen unterstützt; LDAP wird nicht unterstützt.

Nachdem S3-Benutzer NAS-Benutzern zugeordnet wurden, können Sie Benutzern Berechtigungen erteilen, um die Ressourcen (Verzeichnisse und Dateien) anzugeben, auf die sie zugreifen können, und die Aktionen, die sie dort ausführen dürfen oder die sie nicht ausführen dürfen.

System Manager

1. Erstellen Sie lokale Namenszuordnungen für UNIX oder Windows Clients (oder beide).
   a. Klicken Sie auf **Storage > Buckets** und wählen Sie dann die S3/NAS-fähige Storage-VM aus.
   b. Wählen Sie **Einstellungen** und klicken Sie dann → in **Name Mapping** (unter **Host Users and Groups**).
   c. Klicken Sie in den Kacheln **S3 zu Windows** oder **S3 zu UNIX** (oder beide) auf **Hinzufügen** und geben Sie dann die gewünschten **Pattern** (S3) und **Ersatz** (NAS) an.
2. Erstellen einer Bucket-Richtlinie für Client-Zugriff
   a. Klicken Sie auf **Speicher > Buckets**, klicken Sie ⋮ neben dem gewünschten S3-Bucket und dann auf **Bearbeiten**.
   b. Klicken Sie auf **Hinzufügen** und geben Sie die gewünschten Werte ein.
      - **Principal** - Bereitstellen von S3-Benutzernamen oder Verwenden der Standardeinstellung (alle Benutzer).
      - **Effekt** - Wählen Sie **Zulassen** oder **verweigern**.
      - **Aktionen** - Geben Sie Aktionen für diese Benutzer und Ressourcen ein. Die Ressourcenvorgänge, die der Objektspeicher-Server derzeit für S3-NAS-Buckets unterstützt, sind: GetObject, PutObject, DeleteObject, ListBucket, GetBucketAcl, GetObjectAcl, GetObjectTagging, PuttObjectTagging, DeleteObjektTagging, GetBucketLocation, GetBucketVersioning, PutBucketVersioning und ListBucketVersions. Platzhalter werden für diesen Parameter akzeptiert.
      - **Ressourcen** - Geben Sie Ordner- oder Dateipfade ein, in denen die Aktionen erlaubt oder verweigert werden, oder verwenden Sie die Standardwerte (Stammverzeichnis des Buckets).

CLI

1. Erstellen Sie lokale Namenszuordnungen für UNIX oder Windows Clients (oder beide).
   `vserver name-mapping create -vserver svm_name> -direction {s3-win|s3-unix} -position` *`integer`* `-pattern` *`s3_user_name`* `-replacement` *`nas_user_name`*
   - `-position` - Prioritätsnummer für die Bewertung der Zuordnung; geben Sie 1 oder 2 ein.
   - `-pattern` - Ein S3-Benutzername oder ein regulärer Ausdruck
   - `-replacement` - Ein Windows- oder unix-Benutzername

Beispiele

```
vserver name-mapping create -direction s3-win -position 1 -pattern s3_user_1
-replacement win_user_1 vserver name-mapping create -direction s3-unix
-position 2 -pattern s3_user_1 -replacement unix_user_1
```

1. Erstellen einer Bucket-Richtlinie für Client-Zugriff
   `vserver object-store-server bucket policy add-statement -vserver svm_name -bucket bucket_name -effect {deny|allow} -action list_of_actions -principal list_of_users_or_groups -resource [-sid alphanumeric_text]`
   - `-effect {deny|allow}` - Gibt an, ob der Zugriff erlaubt oder verweigert wird, wenn ein Benutzer eine Aktion anfordert.
   - `-action <Action>, …` - Gibt Ressourcenvorgänge an, die erlaubt oder verweigert werden. Der Satz von Ressourcenoperationen, die der Objektspeicher-Server derzeit für S3-NAS-Buckets unterstützt, ist GetObject, PutObject, DeleteObject, ListBucket, GetBucket Acl, GetObjectAcl und

GetBucket Location. Platzhalter werden für diesen Parameter akzeptiert.

- `-principal <Objectstore Principal>, …` - Überprüft den Benutzer, der Zugriff auf die in diesem Parameter angegebenen Benutzer oder Gruppen des Objektspeichers anfordert.
  - Eine Objektspeicherservergruppe wird durch Hinzufügen einer Präfixgruppe/ zum Gruppennamen angegeben.
  - `-principal` - (Bindestrich) gewährt allen Benutzern Zugriff.
- `-resource <text>, …` - Gibt den Bucket, Ordner oder das Objekt an, für das die Zulassen/Ablehnen-Berechtigungen festgelegt sind. Platzhalter werden für diesen Parameter akzeptiert.
- `[-sid <SID>]` - Gibt einen optionalen Textkommentar für die Bucket Policy-Anweisung des Objektspeichers an.

Beispiele

```
cluster1::> vserver object-store-server bucket policy add-statement -bucket
testbucket -effect allow -action
GetObject,PutObject,DeleteObject,ListBucket,GetBucketAcl,GetObjectAcl,
GetBucketLocation,GetBucketPolicy,PutBucketPolicy,DeleteBucketPolicy
-principal user1 -resource testbucket,testbucket/* sid "FullAccessForUser1"

cluster1::> vserver object-store-server bucket policy statement create
-vserver vs1 -bucket bucket1 -effect allow -action GetObject -principal -
-resource bucket1/readme/* -sid "ReadAccessToReadmeForAllUsers"
```