S3-Client-Zugriff auf NAS-Daten

ONTAP 9

NetApp
March 22, 2023

Inhaltsverzeichnis

S3-Client-Zugriff auf NAS-Daten

S3-Multi-Protokoll-Übersicht

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 mithilfe herkömmlicher NAS-Clients (NFS oder SMB) erstellt wurden und sich in NAS Volumes (FlexVol oder FlexGroup Volumes) befinden, können Sie jetzt Analyse-Tools auf S3-Clients für den Zugriff auf diese Daten verwenden.

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

   Somit ist es möglich, integrierten Zugriff für Applikationen wie Spark und Kafka zu bieten, in denen dieselben Daten sowohl mit NAS- als auch mit S3-Protokollen gelesen und geschrieben werden können.

Funktionsweise von S3-Protokollen

Mit ONTAP Multi-Protokoll können Sie denselben Datensatz wie eine Dateihierarchie oder Objekte in einem Bucket präsentieren. Dazu erstellt ONTAP „S3-NAS-Buckets“, mit denen S3-Clients Dateien in NAS-Storage mit S3-Objektanforderungen erstellen, lesen, löschen und aufzählen können. Diese Zuordnung entspricht der NAS-Sicherheitskonfiguration, wobei die Zugriffsberechtigungen für Dateien und Verzeichnisse beachtet werden und ggf. in den Sicherheitsprüfungen geschrieben werden.

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.

Normale ONTAP-definierte S3 Benutzer können auf diesen Storage zugreifen, gemäß den für den Bucket definierten Bucket-Richtlinien, die das NAS-Verzeichnis zugeordnet sind. 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 einfach die Zuordnung von NAS-Daten für S3-Clients, sie sind keine S3-Standardcontainer. Daher ist die Sicherung von S3 NAS Buckets durch die NetApp S3 SnapMirror Funktion nicht erforderlich. Stattdessen können Sie Quell-SVMs mit S3 NAS Buckets mithilfe von SVM DR replizieren, einer standardmäßigen SnapMirror Datensicherungsbeziehung zu Ziel-SVMs. Die SVM-DR ist die einzige unterstützte SnapMirror Replizierungsmethode mit S3 Multi-Protokoll. SnapMirror Synchronous wird nicht unterstützt.

Erfahren Sie mehr über "SnapMirror SVM-Replizierung".

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. Weitere Informationen zu "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".

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

AWS Benutzer-Metadaten

- Als Teil der S3-Benutzer-Metadaten empfangene Key-Values-Paare werden nicht zusammen mit den Objektdaten in der aktuellen Version auf der Festplatte gespeichert.
- Anforderungsheader mit dem Präfix „x-amz-meta“ werden ignoriert.

AWS-Tags

- Bei PUT-Objekt- und Multipart-Initiierung von Anforderungen werden Kopfzeilen mit dem Präfix „x-amz-Tagging“ ignoriert.
- Anfragen zur Aktualisierung von Tags auf einer vorhandenen Datei (d.h. Put-, get- und Delete-Anfragen mit der ?Tagging-Abfragezeichenfolge) werden mit einem Fehler zurückgewiesen.

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.

Mehrteilige Vorgänge

Die folgenden Vorgänge werden nicht unterstützt:

- AbortMehrteilaUpload
- CompleteMultipartUpload
- CreateMultipartUpload
- ListenMehrpartUpload

NAS-Datenanforderungen für den S3-Client-Zugriff

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 von rechtmäßigen S3-Objektnamen können in der zugeordneten NAS-Verzeichnisstruktur nicht nebeneinander bestehen. So werden beispielsweise die gesetzlichen S3-Objektnamen „part1/part2“ und „part1/part2/part3“ Dateien zugeordnet, die nicht gleichzeitig im NAS-Verzeichnisbaum existieren können, da „part1/part2“ eine Datei im Vornamen und ein Verzeichnis im anderen 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 eine sehr große Anzahl von beliebigen Namen unterstützt, kann es bei einer NAS-Verzeichnisstruktur zu Performance-Problemen kommen, wenn eine sehr große Anzahl von Namen in einem Verzeichnis abgelegt wird. Insbesondere Namen ohne Schrägstrich (‘/’) Zeichen in ihnen werden alle in das Stammverzeichnis des NAS-Mapping gelegt. Anwendungen, die umfassende Verwendung von Namen, die nicht „NAS-freundlich“ sind, sind besser auf einem tatsächlichen Objektspeicher-Bucket statt auf einem NAS-Mapping gehostet werden.

S3-Protokollzugriff auf NAS-Daten aktivieren

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 – werden 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 **Storage > Storage VMs**, wählen Sie eine NAS-fähige Storage-VM, klicken Sie auf Einstellungen und klicken Sie dann auf ⚙ 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 der 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 erforderlich ist, lesen Sie "Erstellen und installieren Sie ein CA-Zertifikat auf der SVM".
3. Die Service-Datenrichtlinie aktualisieren
   a. Zeigt die Service-Datenrichtlinie für die SVM + an `network interface service-policy show -vserver svm_name`
   b. Fügen Sie die hinzu `data-core` Und `data-s3-server services` Wenn sie nicht vorhanden sind.
   `network interface service-policy add-service -vserver svm_name -policy policy_name -services data-core,data-s3-server`
4. Stellen Sie sicher, dass die Daten-LIFs auf der SVM Ihre Anforderungen erfüllen:
   `network interface show -vserver svm_name`
5. Den S3-Server erstellen:
   `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.
- 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 nach Bedarf konfiguriert ist:
     `vserver object-store-server show`

Beispiel + mit dem folgenden Befehl werden die Konfigurationswerte aller Objekt-Speicherserver 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
```

S3-NAS-Bucket erstellen

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

Bevor Sie beginnen

- Ein S3-Objektserver wird in einer SVM mit NAS-Daten konfiguriert.
- Die NAS-Daten entsprechen dem "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 könnten Sie separate Bucket-Richtlinien verwenden, die schreibgeschützten Datenzugriff für eine große Gruppe von Benutzern gewähren, und eine weitere Gruppe, die es erlaubt, Operationen für eine Untermenge dieser Daten durchzuführen.

Da S3-NAS „Buckets“ Zuordnungen sind und keine S3-Buckets, gelten die folgenden Eigenschaften von S3-Standard-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 -protected \ is -protected-on-ontap \ is -protected-On-Cloud** + S3 NAS Buckets werden mit S3 SnapMirror nicht geschützt oder gespiegelt, sondern nutzen stattdessen den regulären SnapMirror

Schutz, der mit der Granularität des Volumes zur Verfügung steht.

- **Versionierung-State** + NAS Volumes haben in der Regel Snapshot Technologie zur Verfügung, um verschiedene Versionen zu speichern. 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.

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

Erstellen eines S3-NAS-Buckets in einer SVM mit NAS-Dateisystemen.

```
vserver object-store-server bucket create -vserver svm_name -bucket
bucket_name -type nas -nas-path junction_path [-comment text]
```

Beispiel:

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

S3-Client-Benutzer aktivieren

Damit S3-Client-Benutzer auf NAS-Daten zugreifen können, müssen Sie den entsprechenden NAS-Benutzern S3-Benutzernamen zuordnen und ihnen anschließend die Berechtigung erteilen, über die Bucket-Service-Richtlinien auf die NAS-Daten zuzugreifen.

Bevor Sie beginnen

Benutzernamen für Client-Zugriff – LINUX/UNIX-, Windows- und S3-Client-Benutzer – müssen bereits vorhanden sein.

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 ändern `vserver object-store-server modify` Befehl.

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 auf → Unter **Name Mapping** (unter **Host-Benutzer und -Gruppen**).
   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 **Storage > Buckets**, und klicken Sie auf ⋮ Klicken Sie neben dem gewünschten S3-Bucket 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 Zuordnungsbewertung; 1 oder 2 eingeben.
   - `-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 zulässig oder verweigert wird, wenn ein Benutzer eine Aktion anfordert.
   - `-action <Action>, …` - Gibt Ressourcenvorgänge an, die zulässig oder verweigert werden. 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.

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