Erstellen oder Ändern von Zugriffsrichtlinien-Anweisungen

ONTAP 9

NetApp
February 12, 2026

This PDF was generated from https://docs.netapp.com/de-de/ontap/s3-config/create-modify-bucket-policy-statements-task.html on February 12, 2026. Always check docs.netapp.com for the latest.

Inhalt

Erstellen oder Ändern von Zugriffsrichtlinien-Anweisungen . . . 1
- Informieren Sie sich über ONTAP S3 Bucket und Objektspeicher-Server-Richtlinien . . . 1
- Fügen Sie Zugriffsregeln zur standardmäßigen ONTAP S3-Bucket-Richtlinie hinzu . . . 1
- Erstellen oder Ändern einer ONTAP S3-Objektspeicherserverrichtlinie . . . 4
- Konfigurieren Sie externe Verzeichnisdienste für ONTAP S3-Zugriff . . . 6
  - Konfigurieren Sie den S3-Zugriff für LDAP . . . 7
  - Verwenden Sie für die Authentifizierung den LDAP-F.A.S.T. Bind-Modus . . . 7
  - Konfigurieren des S3-Zugriffs für Active Directory- oder SMB-Server . . . 9
- Ermöglichen Sie LDAP- oder Domänenbenutzern, ihre eigenen ONTAP S3-Zugriffsschlüssel zu generieren . . . 10
  - Konfigurieren Sie Benutzer für die Generierung des Zugriffsschlüssels . . . 11
  - Generieren Sie als S3- oder LDAP-Benutzer eigene Zugriffsschlüssel . . . 14

Erstellen oder Ändern von Zugriffsrichtlinien-Anweisungen

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

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

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

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

Bevor Sie beginnen

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

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

Über diese Aufgabe

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

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

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

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

System Manager

Schritte

1. Bearbeiten Sie den Bucket: Klicken Sie auf **Storage > Buckets**, klicken Sie auf den gewünschten Bucket und klicken Sie dann auf **Bearbeiten**. Beim Hinzufügen oder Ändern von Berechtigungen können Sie die folgenden Parameter angeben:
   - **Auftraggeber**: Der Benutzer oder die Gruppe, auf die der Zugriff gewährt wird.
   - **Effekt**: Erlaubt oder verweigert den Zugriff auf einen Benutzer oder eine Gruppe.
   - **Aktionen**: Zulässige Aktionen im Bucket für einen bestimmten Benutzer oder eine bestimmte Gruppe.
   - **Ressourcen**: Pfade und Namen von Objekten innerhalb des Buckets, für die der Zugriff gewährt oder verweigert wird.

     Die Standardeinstellungen ***bucketname*** und ***bucketname/**** gewähren Zugriff auf alle Objekte im Bucket. Sie können auch Zugriff auf einzelne Objekte gewähren, z. B. ***buchketname/*_readme.txt**.
   - **Bedingungen** (optional): Ausdrücke, die beim Versuch des Zugriffs ausgewertet werden. Sie können beispielsweise eine Liste mit IP-Adressen angeben, für die der Zugriff zulässig oder verweigert wird.

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

CLI

Schritte

1. Hinzufügen einer Anweisung zu einer Bucket-Richtlinie:

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

Die folgenden Parameter definieren Zugriffsberechtigungen:

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

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

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

Beispiele

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

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

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

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

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

Zugriff auf `bucket1` AS `bucket1/user1/*`.

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

Erstellen oder Ändern einer ONTAP S3-Objektspeicherserverrichtlinie

Sie können Richtlinien erstellen, die sich auf einen oder mehrere Buckets in einem Objektspeicher anwenden lassen. Serverrichtlinien für Objektspeicher können an Gruppen von Benutzern angehängt werden, wodurch das Management des Datenzugriffs über mehrere Buckets hinweg vereinfacht wird.

Bevor Sie beginnen

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

Über diese Aufgabe

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

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

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

- Vollzugriff
- NoS3Access
- ReadOnlyAccess

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

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

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

System Manager

Verwenden Sie System Manager zum Erstellen oder Ändern einer Objektspeicherserverrichtlinie

Schritte

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

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

      - Gruppe: Die Gruppen, denen der Zugriff gewährt wird.
      - Effekt: Ermöglicht oder verweigert den Zugriff auf eine oder mehrere Gruppen.
      - Aktionen: Zulässige Aktionen in einem oder mehreren Buckets für eine bestimmte Gruppe.
      - Ressourcen: Pfade und Namen von Objekten innerhalb eines oder mehrerer Buckets, für die der Zugriff gewährt oder verweigert wird. Beispiel:
        - * Gewährt Zugriff auf alle Buckets in der Storage-VM.
        - **Bucketname** und **bucketname/*** gewähren Zugang zu allen Objekten in einem bestimmten Bucket.
        - **Bucketname/readme.txt** gewährt Zugriff auf ein Objekt in einem bestimmten Bucket.
   c. Fügen Sie gegebenenfalls Anweisungen zu bestehenden Richtlinien hinzu.

CLI

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

Schritte

1. Objekt-Storage-Server-Richtlinie erstellen:

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

2. Erstellen einer Anweisung für die Richtlinie:

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

   Die folgenden Parameter definieren Zugriffsberechtigungen:

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

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

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

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

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

Konfigurieren Sie externe Verzeichnisdienste für ONTAP S3-Zugriff

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

Sie können Benutzergruppen, die zu einem externen Verzeichnisdienst gehören, mit Zugriff auf Ihre ONTAP Objekt-Storage-Umgebung versehen. Lightweight Directory Access Protocol (LDAP) ist eine Schnittstelle zur Kommunikation mit Verzeichnisdiensten wie Active Directory, die eine Datenbank und Dienste für Identitäts- und Zugriffsmanagement (IAM) bereitstellen. Für den Zugriff müssen Sie LDAP-Gruppen in Ihrer ONTAP S3-Umgebung konfigurieren. Nachdem Sie den Zugriff konfiguriert haben, haben die Gruppenmitglieder Berechtigungen für ONTAP S3 Buckets. Informationen zu LDAP finden Sie unter "Erfahren Sie mehr über die Verwendung von LDAP-Namensdiensten auf ONTAP NFS SVMs".

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

Bevor Sie beginnen

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

1. Es wurde eine S3-fähige Storage-VM erstellt, die einen S3-Server enthält. Siehe "Erstellung einer SVM für S3".

2. In dieser Storage-VM wurde ein Bucket erstellt. Siehe "Erstellen eines Buckets".
3. DNS ist auf der Storage-VM konfiguriert. Siehe "Konfigurieren Sie DNS-Dienste".
4. Auf der Storage-VM wird ein selbstsigniertes CA-Zertifikat (Root Certification Authority) des LDAP-Servers installiert. Siehe "Installieren Sie selbstsignierte Stamm-CA-Zertifikate auf der SVM".
5. Ein LDAP-Client wird mit TLS auf der SVM konfiguriert. Siehe "Erstellen Sie LDAP-Clientkonfigurationen für den ONTAP NFS-Zugriff" und "Verknüpfen Sie LDAP-Clientkonfigurationen mit ONTAP NFS SVMs für Informationen".

Konfigurieren Sie den S3-Zugriff für LDAP

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

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

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

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

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

Beispiel: Im folgenden Beispiel wird eine Bucket Policy-Anweisung für erstellt `buck1`. Die Richtlinie ermöglicht den Zugriff der LDAP-Gruppe `group1` auf die Ressource (Bucket und deren Objekte) `buck1`.

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

3. Vergewissern Sie sich, dass ein Benutzer der LDAP-Gruppe `group1` S3-Vorgänge vom S3-Client ausführen kann.

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

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

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

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

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

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

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

Base64-Anmeldeinformationen

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

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

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

Authentifizierungsmethode ist nsswitch und LDAP ist aktiviert Beispiel

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Bevor Sie beginnen

Stellen Sie Folgendes sicher:

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

Konfigurieren Sie Benutzer für die Generierung des Zugriffsschlüssels

Beispiel 1. Schritte

LDAP-Benutzer

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

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

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

2. Benutzerdefinierte Rolle mit Zugriff auf den REST-API-Endpunkt des S3-Benutzers erstellen: `security login rest-role create -vserver <vserver-name> -role <custom-role-name> -api "/api/protocols/s3/services/*/users" -access <access-type>` In diesem Beispiel `s3-role` wird die Rolle für Benutzer auf der Storage-VM generiert `svm-1`, denen alle Zugriffsrechte, Lesen, Erstellen und Aktualisieren gewährt werden.

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

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

3. Erstellen Sie eine LDAP-Benutzergruppe mit dem `security login` und fügen Sie die neue benutzerdefinierte Rolle für den Zugriff auf den REST-API-Endpunkt des S3-Benutzers hinzu. Erfahren Sie mehr über `security login create` im "ONTAP-Befehlsreferenz" .

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

In diesem Beispiel `ldap-group-1` wird die LDAP-Gruppe in erstellt `svm-1`, und die benutzerdefinierte Rolle `s3role` wird ihr für den Zugriff auf den API-Endpunkt hinzugefügt, zusammen mit der Aktivierung des LDAP-Zugriffs im Modus „Fast BIND“.

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

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

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

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

Domänenbenutzer

1. Erstellen Sie eine benutzerdefinierte Rolle mit Zugriff auf den S3-Benutzer-REST-API-Endpunkt:

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

In diesem Beispiel `s3-role` Rolle wird für Benutzer auf der Speicher-VM generiert `svm-1` , dem alle Zugriffsrechte Lesen, Erstellen und Aktualisieren gewährt werden.

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

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

1. Erstellen Sie eine Domänenbenutzergruppe mit dem `security login` und fügen Sie die neue benutzerdefinierte Rolle für den Zugriff auf den REST-API-Endpunkt des S3-Benutzers hinzu. Erfahren Sie mehr über `security login create` im "ONTAP-Befehlsreferenz" .

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

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

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

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

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

Generieren Sie als S3- oder LDAP-Benutzer eigene Zugriffsschlüssel

Ab ONTAP 9.14.1 können Sie eigene Zugriffs- und geheime Schlüssel für den Zugriff auf S3-Clients generieren, sofern Ihr Administrator Ihnen die Rolle zum Generieren eigener Schlüssel eingeräumt hat. Sie können Schlüssel nur für sich selbst generieren, indem Sie den folgenden ONTAP REST-API-Endpunkt verwenden.

Erstellen Sie einen S3-Benutzer und generieren Sie Schlüssel

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

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

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

Beispiel für die Wellung

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

Beispiel für eine JSON-Ausgabe

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

Schlüssel für einen S3-Benutzer neu generieren

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

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

Beispiel für die Wellung

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

Beispiel für eine JSON-Ausgabe

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

Copyright-Informationen

Copyright © 2026 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtsinhabers in keiner Form und durch keine Mittel – weder grafische noch elektronische oder mechanische, einschließlich Fotokopieren, Aufnehmen oder Speichern in einem elektronischen Abrufsystem – auch nicht in Teilen, vervielfältigt werden.

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

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

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

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

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

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

Markeninformationen

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