Erstellen oder Ändern von Zugriffsrichtlinien-Anweisungen

ONTAP 9

NetApp
April 24, 2024

This PDF was generated from https://docs.netapp.com/de-de/ontap/s3-config/create-modify-bucket-policy-statements-task.html on April 24, 2024. Always check docs.netapp.com for the latest.

Inhalt

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. ***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}` 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`	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 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`	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.

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::> 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 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
svm1 -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(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.

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` endpunkt: 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-Endpunkt verwenden.

HTTP-Methode und -Endpunkt

Dieser REST-API-Aufruf verwendet die folgende Methode und den folgenden Endpunkt. 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"
}
```

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 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.