Konfiguration und Bereitstellung

ONTAP 9

NetApp
September 09, 2026

This PDF was generated from https://docs.netapp.com/de-de/ontap/authentication/oauth2-prepare.html on September 09, 2026. Always check docs.netapp.com for the latest.

Inhalt

Konfiguration und Bereitstellung . . . 1
- Vorbereitung der Bereitstellung von OAuth 2.0 mit ONTAP . . . 1
  - Geschützte Ressourcen und Client-Anwendungen . . . 1
  - Autorisierungsserver . . . 1
  - Client-Authentifizierung und -Autorisierung . . . 2
  - ONTAP konfigurieren . . . 3
- OAuth 2.0 in ONTAP bereitstellen . . . 3
  - Bevor Sie beginnen . . . 3
  - Schritt 1: Installation der Stammzertifikate der Autorisierungsserver-Zertifizierungsstelle . . . 3
  - Schritt 2: Autorisierungsserver konfigurieren . . . 4
  - Schritt 3: OAuth 2.0 aktivieren . . . 5
- Einen ONTAP REST API-Aufruf mit OAuth 2.0 ausführen . . . 6
  - Bevor Sie beginnen . . . 6
  - Schritt 1: Zugriffstoken abrufen . . . 6
  - Schritt 2: Den REST API-Aufruf ausführen . . . 7

Konfiguration und Bereitstellung

Vorbereitung der Bereitstellung von OAuth 2.0 mit ONTAP

Vor dem Konfigurieren von OAuth 2.0 in einer ONTAP Umgebung sollten Sie sich auf die Bereitstellung vorbereiten. Eine Zusammenfassung der wichtigsten Aufgaben und Entscheidungen ist unten aufgeführt. Die Anordnung der Abschnitte entspricht im Allgemeinen der Reihenfolge, der Sie folgen sollten. Obwohl dies für die meisten Bereitstellungen gilt, sollten Sie es bei Bedarf an Ihre Umgebung anpassen. Sie sollten auch die Erstellung eines formalen Bereitstellungsplans in Betracht ziehen.



Abhängig von Ihrer Umgebung kann die Konfiguration für die in ONTAP definierten Autorisierungsserver ausgewählt werden. Dies umfasst die Parameterwerte, die für jeden Bereitstellungstyp angegeben werden müssen. Siehe "OAuth 2.0 Bereitstellungsszenarien" für weitere Informationen.

Geschützte Ressourcen und Client-Anwendungen

OAuth 2.0 ist ein Autorisierungsframework zur Steuerung des Zugriffs auf geschützte Ressourcen. Daher ist ein wichtiger erster Schritt bei jeder Implementierung die Ermittlung der verfügbaren Ressourcen und der Clients, die Zugriff darauf benötigen.

Clientanwendungen identifizieren

Sie müssen entscheiden, welche Clients OAuth 2.0 bei REST API-Aufrufen verwenden und auf welche API-Endpunkte sie Zugriff benötigen.

Vorhandene ONTAP REST-Rollen und lokale Benutzer überprüfen

Die bestehenden ONTAP Identitätsdefinitionen, einschließlich der REST-Rollen und lokalen Benutzer, sollten überprüft werden. Abhängig von der Konfiguration von OAuth 2.0 können diese Definitionen für Zugriffsentscheidungen herangezogen werden.

Globaler Übergang zu OAuth 2.0

Sie können die OAuth 2.0-Autorisierung zwar schrittweise implementieren, aber auch alle REST API Clients sofort auf OAuth 2.0 umstellen, indem Sie für jeden Autorisierungsserver ein globales Flag setzen. Dadurch können Zugriffsentscheidungen basierend auf Ihrer bestehenden ONTAP Konfiguration getroffen werden, ohne dass selbstenthaltende Scopes erstellt werden müssen.

Autorisierungsserver

Die Autorisierungsserver spielen eine wichtige Rolle bei Ihrer OAuth 2.0 Implementierung, indem sie Zugriffstoken ausstellen und administrative Richtlinien durchsetzen.

Den Autorisierungsserver auswählen und installieren

Sie müssen einen oder mehrere Autorisierungsserver auswählen und installieren. Es ist wichtig, sich mit den Konfigurationsoptionen und Verfahren Ihrer Identitätsanbieter vertraut zu machen, einschließlich der Definition von Scopes. Zu beachten ist, dass einige Autorisierungsserver, darunter Microsoft Entra ID, Gruppen mithilfe von UUIDs anstelle von Namen darstellen.

Es wird festgestellt, ob das Autorisierungs-Root-CA-Zertifikat installiert werden muss.

ONTAP verwendet das Zertifikat des Autorisierungsservers, um die von den Clients präsentierten signierten

Zugriffstoken zu validieren. Dazu benötigt ONTAP das Root-CA-Zertifikat und alle Zwischenzertifikate. Diese könnten bereits mit ONTAP vorinstalliert sein. Falls dies nicht der Fall ist, ist eine Installation erforderlich.

Netzwerkstandort und -konfiguration beurteilen

Wenn sich der Autorisierungsserver hinter einer Firewall befindet, muss ONTAP so konfiguriert werden, dass ein Proxyserver verwendet wird.

Client-Authentifizierung und -Autorisierung

Bei der Client-Authentifizierung und Autorisierung sind mehrere Aspekte zu berücksichtigen.

In sich abgeschlossene Bereiche oder lokale ONTAP Identitätsdefinitionen

Im Wesentlichen können entweder in sich abgeschlossene Bereiche auf dem Autorisierungsserver definiert werden oder es kann auf die vorhandenen lokalen ONTAP Identitätsdefinitionen einschließlich Rollen und Benutzern zurückgegriffen werden.

Optionen mit lokaler ONTAP Verarbeitung

Wenn Sie die ONTAP Identitätsdefinitionen verwenden, muss entschieden werden, welche angewendet werden sollen, einschließlich:

- Benannte REST-Rolle
- Lokale Benutzer abgleichen
- Active Directory oder LDAP-Gruppen

Lokale Validierung oder Fernintrospektion

Es ist zu entscheiden, ob die Zugriffstoken lokal von ONTAP oder auf dem Autorisierungsserver durch Introspektion validiert werden. Es sind außerdem mehrere damit zusammenhängende Werte zu berücksichtigen, wie das Aktualisierungsintervall.

Absenderbeschränkte Zugriffstoken

Für Umgebungen mit hohen Sicherheitsanforderungen können auf mTLS basierende, zugriffsbeschränkte Token verwendet werden. Hierfür ist ein Zertifikat für jeden Client erforderlich.

Gruppen als UUIDs und Identitätszuordnung

Wenn ein Autorisierungsserver verwendet wird, der Gruppen mithilfe von UUIDs darstellt, ist zu planen, wie diese auf Gruppennamen und gegebenenfalls auf zugehörige Rollen abgebildet werden.

Administrative Schnittstelle

Die Administration von OAuth 2.0 ist über jede der ONTAP Schnittstellen möglich, einschließlich:

- Befehlszeilenschnittstelle
- System Manager
- REST API

Wie Clients Zugriffstoken anfordern

Die Clientanwendungen müssen Zugriffstoken direkt vom Autorisierungsserver anfordern. Es ist zu entscheiden, wie dies erfolgen soll, einschließlich des Berechtigungstyps.

ONTAP konfigurieren

Es sind mehrere ONTAP Konfigurationsaufgaben erforderlich.

REST-Rollen und lokale Benutzer definieren

Basierend auf Ihrer Autorisierungskonfiguration kann die lokale ONTAP Identify-Verarbeitung verwendet werden. In diesem Fall sind die REST-Rollen und Benutzerdefinitionen zu überprüfen und zu definieren. Abhängig von Ihrem Autorisierungsserver kann dies auch die Verwaltung von Gruppen auf Basis von UUID-Werten einschließen.

Kernkonfiguration

Für die grundlegende ONTAP Konfiguration sind drei Hauptschritte erforderlich:

- Optional kann das Stammzertifikat (und alle Zwischenzertifikate) für die Zertifizierungsstelle installiert werden, die das Zertifikat des Autorisierungsservers signiert hat.
- Definieren Sie den Autorisierungsserver.
- Die OAuth 2.0-Verarbeitung für den Cluster aktivieren.

OAuth 2.0 in ONTAP bereitstellen

Die Bereitstellung der Kernfunktionalität von OAuth 2.0 umfasst drei Hauptschritte.

Bevor Sie beginnen

Vor der Konfiguration von ONTAP ist eine Vorbereitung für die OAuth 2.0 Bereitstellung erforderlich. Beispielsweise sollte der Autorisierungsserver bewertet werden, einschließlich der Signierung seines Zertifikats und ob er sich hinter einer Firewall befindet. Siehe "Vorbereitung der Bereitstellung von OAuth 2.0 mit ONTAP" für weitere Informationen.

Schritt 1: Installation der Stammzertifikate der Autorisierungsserver-Zertifizierungsstelle

ONTAP enthält eine Vielzahl vorinstallierter Stamm-CA-Zertifikate. In vielen Fällen wird das Zertifikat Ihres Autorisierungsservers daher von ONTAP ohne zusätzliche Konfiguration sofort erkannt. Je nachdem, wie das Zertifikat des Autorisierungsservers signiert wurde, kann es jedoch erforderlich sein, ein Stamm-CA-Zertifikat und gegebenenfalls Zwischenzertifikate zu installieren.

Befolgen Sie die unten stehenden Anweisungen, um das Zertifikat gegebenenfalls zu installieren. Alle erforderlichen Zertifikate sollten auf Clusterebene installiert werden.

Das richtige Verfahren ist abhängig davon, wie Sie auf ONTAP zugreifen.

Beispiel 1. Schritte

System Manager

1. Im System Manager **Cluster** > **Einstellungen** auswählen.
2. Zum Abschnitt **Sicherheit** nach unten scrollen.
3. Klicken Sie auf → neben **Zertifikate**.
4. Unter der Registerkarte **Vertrauenswürdige Zertifizierungsstellen** auf **Hinzufügen** klicken.

5. Klicken Sie auf **Import** und wählen Sie die Zertifikatsdatei aus.
6. Vervollständigen Sie die Konfigurationsparameter für Ihre Umgebung.
7. Klicken Sie auf **Add**.

CLI

1. Installation starten:

```
security certificate install -type server-ca
```

2. Die folgende Konsolenmeldung erscheint:

```
Please enter Certificate: Press <Enter> when done
```

3. Die Zertifikatsdatei mit einem Texteditor öffnen.
4. Das gesamte Zertifikat einschließlich der folgenden Zeilen kopieren:

```
-----BEGIN CERTIFICATE-----
<certificate_value>
-----END CERTIFICATE-----
```

5. Fügen Sie das Zertifikat nach der Eingabeaufforderung in das Terminal ein.
6. Drücken Sie **Enter**, um die Installation abzuschließen.
7. Das Zertifikat kann mit einer der folgenden Methoden als installiert bestätigt werden:

```
security certificate show-user-installed
```

```
security certificate show
```

Schritt 2: Autorisierungsserver konfigurieren

Mindestens ein Autorisierungsserver muss für ONTAP definiert werden. Die Auswahl der Parameterwerte richtet sich nach der jeweiligen Konfiguration und dem Bereitstellungsplan. Die Überprüfung von "OAuth2 Bereitstellungsszenarien" ermöglicht die Ermittlung der genauen für die Konfiguration erforderlichen Parameter.



Um eine Autorisierungsserverdefinition zu ändern, können Sie die bestehende Definition löschen und eine neue erstellen.

Das untenstehende Beispiel basiert auf dem ersten einfachen Bereitstellungsszenario unter "Lokale Validierung". Es werden in sich abgeschlossene Bereiche ohne Proxy verwendet.

Das richtige Verfahren ist abhängig davon, wie Sie auf ONTAP zugreifen. Das CLI-Verfahren verwendet symbolische Variablen, die vor der Ausführung des Befehls ersetzt werden müssen.

Beispiel 2. Schritte

System Manager

1. Im System Manager **Cluster** > **Einstellungen** auswählen.
2. Zum Abschnitt **Sicherheit** nach unten scrollen.
3. Klicken Sie auf **+** neben **OAuth 2.0 authorization**.
4. **Weitere Optionen** auswählen.
5. Geben Sie die für Ihre Bereitstellung erforderlichen Werte an, wie zum Beispiel:
   - Name
   - Anwendung (http)
   - Provider-JWKS-URI
   - Issuer-URI
6. Klicken Sie auf **Add**.

CLI

1. Die Definition erneut erstellen:

   ```
   security oauth2 client create -config-name <NAME> -provider-jwks-uri
   <URI_JWKS> -application http -issuer <URI_ISSUER>
   ```

   Beispiel:

   ```
   security oauth2 client create \
   -config-name auth0 \
   -provider-jwks-uri https://superzap.dev.netapp.com:8443/realms/my-
   realm/protocol/openid-connect/certs \
   -application http \
   -issuer https://superzap.dev.netapp.com:8443/realms/my-realm
   ```

   Weitere Informationen zu `security oauth2 client create` finden sich in der "ONTAP-Befehlsreferenz".

Schritt 3: OAuth 2.0 aktivieren

Der letzte Schritt besteht darin, OAuth 2.0 zu aktivieren. Dies ist eine globale Einstellung für den ONTAP Cluster.



Die OAuth 2.0 Verarbeitung sollte erst aktiviert werden, nachdem bestätigt wurde, dass ONTAP, die Autorisierungsserver und alle unterstützenden Dienste ordnungsgemäß konfiguriert sind.

Das richtige Verfahren ist abhängig davon, wie Sie auf ONTAP zugreifen.

Beispiel 3. Schritte

System Manager

1. Im System Manager **Cluster** > **Einstellungen** auswählen.
2. Zum Abschnitt **Sicherheit** nach unten scrollen.
3. Klicken Sie auf → neben **OAuth 2.0 authorization**.
4. **OAuth 2.0-Autorisierung** aktivieren.

CLI

1. OAuth 2.0 aktivieren:

   ```
   security oauth2 modify -enabled true
   ```

2. Bestätigen, dass OAuth 2.0 aktiviert ist:

   ```
   security oauth2 show
   Is OAuth 2.0 Enabled: true
   ```

Verwandte Informationen

- "Sicherheitszertifikat installieren"
- "Sicherheitszertifikat anzeigen"
- "security oauth2 modify"
- "security oauth2 show"

Einen ONTAP REST API-Aufruf mit OAuth 2.0 ausführen

Die OAuth 2.0 Implementierung in ONTAP unterstützt REST API Clientanwendungen. Ein einfacher REST API Aufruf mit curl kann verwendet werden, um mit OAuth 2.0 zu beginnen. Das folgende Beispiel ruft die ONTAP Cluster-Version ab.

Bevor Sie beginnen

Sie müssen die OAuth 2.0 Funktion für Ihren ONTAP Cluster konfigurieren und aktivieren. Dies umfasst die Definition eines Autorisierungsservers.

Schritt 1: Zugriffstoken abrufen

Sie benötigen ein Zugriffstoken, um es mit dem ONTAP REST API-Aufruf zu verwenden. Die Token-Anforderung erfolgt außerhalb von ONTAP und die genaue Vorgehensweise hängt vom Autorisierungsserver und dessen Konfiguration ab. Das Token kann über einen Webbrowser, mit einem curl-Befehl oder mithilfe einer Programmiersprache angefordert werden.

Zur Veranschaulichung ist nachfolgend ein Beispiel dafür dargestellt, wie ein Zugriffstoken von Keycloak mithilfe von curl angefordert werden kann.

Keycloak Beispiel

```
curl --request POST \
--location
'https://superzap.dev.netapp.com:8443/realms/peterson/protocol/openid-
connect/token' \
--header 'Content-Type: application/x-www-form-urlencoded' \
--data-urlencode 'client_id=dp-client-1' \
--data-urlencode 'grant_type=client_credentials' \
--data-urlencode 'client_secret=5iTUf9QKLGxAoYa1iR33vlD5A2xq09V7'
```

Das zurückgegebene Token sollte kopiert und gespeichert werden.

Schritt 2: Den REST API-Aufruf ausführen

Nachdem Sie über ein gültiges Zugriffstoken verfügen, kann mit dem Zugriffstoken und dem curl Befehl ein REST API Aufruf ausgeführt werden.

Parameter und Variablen

Die beiden Variablen im curl-Beispiel sind in der folgenden Tabelle beschrieben.

Variable	Beschreibung
$FQDN_IP	Der vollqualifizierte Domainname oder die IP-Adresse des ONTAP Management-LIF.
$ACCESS_TOKEN	Das vom Autorisierungsserver ausgestellte OAuth 2.0 Zugriffstoken.

Diese Variablen sind zuerst in der Bash-Shell-Umgebung festzulegen, bevor das curl-Beispiel ausgeführt wird. Im Linux-CLI kann zum Festlegen und Anzeigen der FQDN-Variable folgender Befehl eingegeben werden:

```
FQDN_IP=172.14.31.224
echo $FQDN_IP
172.14.31.224
```

Nachdem beide Variablen in Ihrer lokalen Bash-Shell definiert sind, kann der curl-Befehl kopiert und in die CLI eingefügt werden. Mit **Enter** werden die Variablen ersetzt und der Befehl ausgeführt.

Curl Beispiel

```
curl --request GET \
--location "https://$FQDN_IP/api/cluster?fields=version" \
--include \
--header "Accept: */*" \
--header "Authorization: Bearer $ACCESS_TOKEN"
```

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.