Konfiguration und Implementierung

ONTAP 9

NetApp
April 24, 2024

Inhalt

Konfiguration und Implementierung

Bereiten Sie die Bereitstellung von OAuth 2.0 mit ONTAP vor

Bevor Sie OAuth 2.0 in einer ONTAP-Umgebung konfigurieren, sollten Sie die Bereitstellung vorbereiten. Im Folgenden finden Sie eine Zusammenfassung der wichtigsten Aufgaben und Entscheidungen. Die Anordnung der Abschnitte ist im Allgemeinen auf die Reihenfolge ausgerichtet, die Sie befolgen sollten. Dies gilt zwar für die meisten Implementierungen, Sie sollten es jedoch bei Bedarf an Ihre Umgebung anpassen. Sie sollten auch die Erstellung eines formellen Bereitstellungsplans in Betracht ziehen.

Je nach Umgebung können Sie die Konfiguration für die Autorisierungsserver auswählen, die für ONTAP definiert sind. Dazu gehören auch die Parameterwerte, die Sie für jeden Bereitstellungstyp spezifisch benötigen. Siehe "OAuth 2.0-Bereitstellungsszenarien" Finden Sie weitere Informationen.

Geschützte Ressourcen und Client-Applikationen

OAuth 2.0 ist ein Autorisierungs-Framework zur Kontrolle des Zugriffs auf geschützte Ressourcen. Aus diesem Grund besteht ein wichtiger erster Schritt bei jeder Bereitstellung darin zu bestimmen, welche Ressourcen verfügbar sind und welche Clients Zugriff darauf benötigen.

Identifizierung von Client-Applikationen

Sie müssen entscheiden, welche Clients OAuth 2.0 bei der Ausgabe von REST-API-Aufrufen verwenden und auf welche API-Endpunkte Zugriff benötigt wird.

Bestehende ONTAP REST-Rollen und lokale Benutzer prüfen

Sie sollten die vorhandenen ONTAP-Identitätsdefinitionen sowie die REST-Rollen und lokalen Benutzer überprüfen. Je nachdem, wie Sie OAuth 2.0 konfigurieren, können diese Definitionen für Zugriffsentscheidungen verwendet werden.

Globaler Übergang zu OAuth 2.0

Obwohl Sie die OAuth 2.0-Autorisierung schrittweise implementieren können, können Sie auch alle REST-API-Clients sofort nach OAuth 2.0 verschieben, indem Sie für jeden Autorisierungsserver ein globales Flag festlegen. Auf diese Weise können Sie basierend auf Ihrer bestehenden ONTAP-Konfiguration Zugriffsentscheidungen treffen, ohne dass Sie in sich geschlossene Bereiche erstellen müssen.

Autorisierungsserver

Die Autorisierungsserver spielen eine wichtige Rolle in Ihrer OAuth 2.0-Bereitstellung, indem sie Zugriffstoken ausgeben und die Verwaltungsrichtlinie durchsetzen.

Wählen Sie den Autorisierungsserver aus, und installieren Sie ihn

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 Geltungsbereichen.

Stellen Sie fest, ob das Zertifikat der Autorisierungsstammzertifizierungsstelle installiert werden muss

ONTAP verwendet das Zertifikat des Autorisierungsservers, um die von den Clients präsentierten signierten Zugriffstoken zu validieren. Dazu benötigt ONTAP das Stammzertifizierungsstellenzertifikat und alle Zwischenzertifikate. Diese sind möglicherweise mit ONTAP vorinstalliert. Wenn nicht, müssen Sie sie installieren.

Bewerten Sie den Netzwerkstandort und die -Konfiguration

Wenn sich der Autorisierungsserver hinter einer Firewall befindet, muss ONTAP für die Verwendung eines Proxy-Servers konfiguriert werden.

Client-Authentifizierung und -Autorisierung

Es gibt mehrere Aspekte der Client-Authentifizierung und -Autorisierung, die Sie berücksichtigen müssen.

Eigenständige Bereiche oder lokale ONTAP-Identitätsdefinitionen

Sie können entweder eigenständige Bereiche definieren, die auf dem Autorisierungsserver definiert sind, oder auf die vorhandenen lokalen ONTAP-Identitätsdefinitionen, einschließlich Rollen und Benutzer, zurückgreifen.

Optionen mit lokaler ONTAP-Verarbeitung

Wenn Sie die ONTAP-Identitätsdefinitionen verwenden, müssen Sie entscheiden, welche Anwendung zutrifft. Dazu gehören:

- Benannte REST-Rolle
- Ordnen Sie lokale Benutzer zu
- Active Directory oder LDAP-Gruppen

Lokale Validierung oder Remote-Introspektion

Sie müssen entscheiden, ob die Zugriffstoken lokal durch ONTAP oder auf dem Autorisierungsserver durch Introspektion validiert werden. Es gibt auch mehrere verwandte Werte zu berücksichtigen, wie zum Beispiel das Aktualisierungsintervall.

Zugriffstoken, die durch den Absender eingeschränkt sind

Für Umgebungen, die ein hohes Maß an Sicherheit erfordern, können Sie auf Basis von MTLS sendende Zugriffstoken verwenden. Dies erfordert ein Zertifikat für jeden Client.

Administrationsschnittstelle

Sie können die Verwaltung von OAuth 2.0 über eine der ONTAP-Schnittstellen durchführen, einschließlich:

- Befehlszeilenschnittstelle
- System Manager
- REST API

Wie Clients Zugriffstoken anfordern

Die Client-Anwendungen müssen Zugriffstoken direkt vom Autorisierungsserver anfordern. Sie müssen entscheiden, wie dies geschehen wird, einschließlich der Zuschussart.

Konfigurieren Sie ONTAP

Es gibt mehrere ONTAP-Konfigurationsaufgaben, die Sie durchführen müssen.

Definieren Sie REST-Rollen und lokale Benutzer

Basierend auf Ihrer Autorisierungskonfiguration kann die lokale ONTAP-Identifizieren-Verarbeitung verwendet werden. In diesem Fall müssen Sie die REST-Rollen und Benutzerdefinitionen überprüfen und definieren.

Kernkonfiguration

Zur Durchführung der zentralen ONTAP-Konfiguration sind drei wichtige Schritte erforderlich:

- Installieren Sie optional das Stammzertifikat (und alle Zwischenzertifikate) für die Zertifizierungsstelle, die das Zertifikat des Autorisierungsservers signiert hat.
- Definieren Sie den Autorisierungsserver.
- Aktivieren Sie die OAuth 2.0-Verarbeitung für den Cluster.

Implementieren Sie OAuth 2.0 in ONTAP

Die Bereitstellung der zentralen OAuth 2.0-Funktionalität umfasst drei Hauptschritte.

Bevor Sie beginnen

Sie müssen die Bereitstellung von OAuth 2.0 vorbereiten, bevor Sie ONTAP konfigurieren. Sie müssen beispielsweise den Autorisierungsserver beurteilen, einschließlich der Art und Weise, wie das Zertifikat signiert wurde und ob es sich hinter einer Firewall befindet. Siehe "Bereiten Sie die Bereitstellung von OAuth 2.0 mit ONTAP vor" Finden Sie weitere Informationen.

Schritt 1: Installieren Sie das Zertifikat für den Authentifizierungsserver

ONTAP enthält eine große Anzahl vorinstallierter Stammzertifizierungsstellen-Zertifikate. So wird in vielen Fällen das Zertifikat für Ihren Autorisierungsserver von ONTAP ohne zusätzliche Konfiguration sofort erkannt. Je nachdem, wie das Zertifikat des Autorisierungsservers signiert wurde, müssen Sie möglicherweise ein Stammzertifizierungszertifikat und alle Zwischenzertifikate installieren.

Befolgen Sie die Anweisungen unten, um das Zertifikat zu installieren, falls es benötigt wird. Installieren Sie alle erforderlichen Zertifikate auf Cluster-Ebene.

Wählen Sie das richtige Verfahren, je nachdem, wie Sie auf ONTAP zugreifen.

Beispiel 1. Schritte

System Manager

1. Wählen Sie im System Manager **Cluster** > **Einstellungen** aus.
2. Scrollen Sie nach unten zum Abschnitt **Sicherheit**.
3. Klicken Sie neben **Certificates** auf →.
4. Klicken Sie auf der Registerkarte **Vertrauenswürdige Zertifizierungsstellen** auf **Hinzufügen**.
5. Klicken Sie auf **Import** und wählen Sie die Zertifikatdatei aus.
6. Vervollständigen Sie die Konfigurationsparameter für Ihre Umgebung.
7. Klicken Sie Auf **Hinzufügen**.

CLI

1. Starten Sie die Installation:

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

2. Suchen Sie nach der folgenden Konsolenmeldung:

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

3. Öffnen Sie die Zertifikatdatei mit einem Texteditor.
4. Kopieren Sie das gesamte Zertifikat einschließlich der folgenden Zeilen:

   ```
   -----BEGIN CERTIFICATE-----

   -----END CERTIFICATE-----
   ```

5. Fügen Sie das Zertifikat nach der Eingabeaufforderung in das Terminal ein.
6. Drücken Sie **Enter**, um die Installation abzuschließen.
7. Vergewissern Sie sich, dass das Zertifikat installiert ist, indem Sie eine der folgenden Methoden verwenden:

   ```
   security certificate show-user-installed

   security certificate show
   ```

Schritt 2: Konfigurieren des Autorisierungsservers

Sie müssen mindestens einen Autorisierungsserver für ONTAP definieren. Sie sollten die Parameterwerte auf Grundlage Ihres Konfigurations- und Bereitstellungsplans auswählen. Prüfen "OAuth2-Bereitstellungsszenarien" Um die genauen Parameter zu bestimmen, die für Ihre Konfiguration erforderlich sind.

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

Das folgende Beispiel basiert auf dem ersten einfachen Implementierungsszenario unter "Lokale Validierung".

Eigenständige Bereiche werden ohne Proxy verwendet.

Wählen Sie das richtige Verfahren, je nachdem, wie Sie auf ONTAP zugreifen. Das CLI-Verfahren verwendet symbolische Variablen, die Sie vor der Ausgabe des Befehls ersetzen müssen.

Beispiel 2. Schritte

System Manager

1. Wählen Sie im System Manager **Cluster** > **Einstellungen** aus.
2. Scrollen Sie nach unten zum Abschnitt **Sicherheit**.
3. Klicken Sie neben **OAuth 2.0 Authorization** auf **+**.
4. Wählen Sie **Weitere Optionen**.
5. Geben Sie die erforderlichen Werte für Ihre Bereitstellung an, z. B.:
   - Name
   - Anwendung (http)
   - Provider-JWKS-URI
   - Aussteller-URI
6. Klicken Sie Auf **Hinzufügen**.

CLI

1. Erstellen Sie die Definition erneut:

   ```
   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
   ```

Schritt 3: Aktivieren Sie OAuth 2.0

Der letzte Schritt ist die Aktivierung von OAuth 2.0. Dies ist eine globale Einstellung für das ONTAP Cluster.

> Aktivieren Sie die OAuth 2.0-Verarbeitung erst, wenn Sie bestätigen, dass ONTAP, die Autorisierungsserver und alle unterstützenden Dienste ordnungsgemäß konfiguriert wurden.

Wählen Sie das richtige Verfahren, je nachdem, wie Sie auf ONTAP zugreifen.

Beispiel 3. Schritte

System Manager

1. Wählen Sie im System Manager **Cluster** > **Einstellungen** aus.
2. Scrollen Sie nach unten zum Abschnitt **Sicherheit**.
3. Klicken Sie neben **OAuth 2.0 Authorization** auf →.
4. Aktivieren Sie **OAuth 2.0-Autorisierung**.

CLI

1. OAuth 2.0 aktivieren:

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

2. Bestätigen Sie, dass OAuth 2.0 aktiviert ist:

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

Geben Sie einen REST-API-Aufruf mit OAuth 2.0 aus

Die OAuth 2.0-Implementierung in ONTAP unterstützt REST-API-Client-Applikationen. Sie können einen einfachen REST API-Aufruf mit Curl ausgeben, um mit OAuth 2.0 zu beginnen. Im folgenden Beispiel wird die ONTAP Cluster-Version abgerufen.

Bevor Sie beginnen

Sie müssen die Funktion OAuth 2.0 für Ihren ONTAP-Cluster konfigurieren und aktivieren. Dazu gehört auch die Definition eines Autorisierungsservers.

Schritt 1: Erwerben Sie ein Zugriffstoken

Sie müssen ein Zugriffstoken erwerben, um es mit dem REST-API-Aufruf zu verwenden. Die Token-Anforderung wird außerhalb von ONTAP ausgeführt, und die genaue Vorgehensweise hängt vom Autorisierungsserver und seiner Konfiguration ab. Sie können das Token über einen Webbrowser, mit einem Curl-Befehl oder mit einer Programmiersprache anfordern.

Zur Veranschaulichung wird unten ein Beispiel gezeigt, wie ein Zugriffstoken von Keycloak mit 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'
```

Sie sollten das zurückgegebene Token kopieren und speichern.

Schritt 2: Geben Sie den REST API-Aufruf aus

Nachdem Sie über ein gültiges Zugriffstoken verfügen, können Sie einen Curl-Befehl mit dem Zugriffstoken verwenden, um einen REST-API-Aufruf auszustellen.

Parameter und Variablen

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

Variabel	Beschreibung
FQDN_IP-DOLLAR	Der vollständig qualifizierte Domain-Name oder die IP-Adresse der ONTAP Management LIF.
ACCESS_TOKEN IN HÖHE VON USD	Das vom Autorisierungsserver ausgegebene Zugriffstoken OAuth 2.0.

Sie sollten diese Variablen zuerst in der Bash Shell-Umgebung festlegen, bevor Sie das Curl-Beispiel ausgeben. Geben Sie beispielsweise in der Linux CLI den folgenden Befehl ein, um die FQDN-Variable festzulegen und anzuzeigen:

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

Nachdem beide Variablen in Ihrer lokalen Bash Shell definiert wurden, können Sie den Curl-Befehl kopieren und in die CLI einfügen. Drücken Sie **Enter**, um die Variablen zu ersetzen und den Befehl auszugeben.

Beispiel für die Wellung

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