Authentifizierung und Autorisierung mit OAuth 2.0

ONTAP 9

NetApp
April 24, 2024

Inhalt

Authentifizierung und Autorisierung mit OAuth 2.0

Überblick über die Implementierung von ONTAP OAuth 2.0

Ab ONTAP 9.14 haben Sie die Möglichkeit, den Zugriff auf Ihre ONTAP-Cluster über das Open Authorization (OAuth 2.0)-Framework zu steuern. Sie können diese Funktion über jede der ONTAP-Administrationsschnittstellen konfigurieren, einschließlich der ONTAP-CLI, System Manager und REST-API. Die OAuth 2.0-Autorisierungs- und Zugriffskontrollentscheidungen können jedoch nur angewendet werden, wenn ein Client über die REST-API auf ONTAP zugreift.

> Die Unterstützung für OAuth 2.0 wurde erstmals mit ONTAP 9.14.0 eingeführt, sodass die Verfügbarkeit von der von Ihnen verwendeten ONTAP Version abhängt. Siehe "Versionshinweise zu ONTAP" Finden Sie weitere Informationen.

Funktionen und Vorteile

Die wichtigsten Merkmale und Vorteile der Verwendung von OAuth 2.0 mit ONTAP sind im Folgenden beschrieben.

Unterstützung für den Standard OAuth 2.0

OAuth 2.0 ist das Standard-Autorisierungsframework der Branche. Sie wird verwendet, um den Zugriff auf geschützte Ressourcen mit signierten Zugriffstoken zu beschränken und zu steuern. Die Verwendung von OAuth 2.0 bietet mehrere Vorteile:

- Viele Optionen für die Berechtigungskonfiguration
- Geben Sie niemals die Client-Anmeldeinformationen einschließlich Passwörter bekannt
- Token können basierend auf Ihrer Konfiguration auf „ablaufen lassen“ gesetzt werden
- Ideal geeignet für den Einsatz mit REST-APIs

Getestet mit mehreren gängigen Autorisierungsservern

Die ONTAP-Implementierung ist mit jedem OAuth 2.0-konformen Autorisierungsserver kompatibel. Es wurde mit den folgenden gängigen Servern oder Diensten getestet, darunter:

- Auth0
- Active Directory Federation Service (ADFS)
- Keycloak

Unterstützung für mehrere gleichzeitige Autorisierungsserver

Sie können bis zu acht Autorisierungsserver für einen einzelnen ONTAP-Cluster definieren. Dadurch erhalten Sie die Flexibilität, die Anforderungen Ihrer vielfältigen Sicherheitsumgebung zu erfüllen.

Integration in die REST-Rollen

Die ONTAP-Autorisierungsentscheidungen basieren letztlich auf den REST-Rollen, die Benutzern oder Gruppen zugewiesen sind. Diese Rollen werden entweder als eigenständige Bereiche im Zugriffstoken oder auf der Grundlage lokaler ONTAP-Definitionen zusammen mit Active Directory- oder LDAP-Gruppen

übertragen.

Option zur Verwendung von Zugriffstoken mit Senderbeschränkungen

Sie können ONTAP und die Autorisierungsserver so konfigurieren, dass die gegenseitige Transportschicht-Sicherheit (MTLS) verwendet wird, wodurch die Clientauthentifizierung gestärkt wird. Sie garantiert, dass die OAuth 2.0-Zugriffstoken nur von den Clients verwendet werden, auf die sie ursprünglich ausgestellt wurden. Diese Funktion unterstützt und harmonisiert mit mehreren gängigen Sicherheitsempfehlungen, einschließlich der von FAPI und MITER festgelegten.

Implementierung und Konfiguration

Auf hoher Ebene gibt es mehrere Aspekte einer OAuth 2.0-Implementierung und -Konfiguration, die Sie bei der Inbetriebnahme berücksichtigen sollten.

OAuth 2.0 Einheiten innerhalb von ONTAP

Das OAuth 2.0-Autorisierungs-Framework definiert mehrere Einheiten, die realen oder virtuellen Elementen in Ihrem Rechenzentrum oder Netzwerk zugeordnet werden können. Die OAuth 2.0 Einheiten und ihre Anpassung an ONTAP sind in der folgenden Tabelle dargestellt.

OAuth 2.0-Einheit	Beschreibung
Ressource	Die REST-API-Endpunkte, die über interne ONTAP-Befehle Zugriff auf die ONTAP-Ressourcen bieten.
Ressourceneigentümer	Der ONTAP-Cluster-Benutzer, der die geschützte Ressource erstellt hat oder der sie standardmäßig besitzt.
Ressourcenserver	Der Host für die geschützten Ressourcen, die der ONTAP-Cluster ist.
Client	Eine Applikation, die den Zugriff auf einen REST-API-Endpunkt im Namen oder mit Genehmigung des Ressourceneigentümers anfordert.
Autorisierungsserver	In der Regel ein dedizierter Server, der für die Ausgabe von Zugriffstoken und die Durchsetzung von Verwaltungsrichtlinien verantwortlich ist.

ONTAP-Kernkonfiguration

Sie müssen den ONTAP-Cluster konfigurieren, um OAuth 2.0 zu aktivieren und zu verwenden. Dazu gehört die Einrichtung einer Verbindung zum Autorisierungsserver und die Definition der erforderlichen ONTAP-Autorisierungskonfiguration. Sie können diese Konfiguration über eine der Administrationsschnittstellen durchführen, einschließlich:

- ONTAP Befehlszeilenschnittstelle
- System Manager
- ONTAP REST API

Umwelt und unterstützende Dienstleistungen

Zusätzlich zu den ONTAP-Definitionen müssen Sie auch die Autorisierungsserver konfigurieren. Wenn Sie eine Gruppen-zu-Rollen-Zuordnung verwenden, müssen Sie auch die Active Directory-Gruppen oder das LDAP-Äquivalent konfigurieren.

Unterstützte ONTAP-Clients

Ab ONTAP 9.14 kann ein REST-API-Client über OAuth 2.0 auf ONTAP zugreifen. Bevor Sie einen REST-API-Aufruf ausgeben, müssen Sie ein Zugriffstoken vom Autorisierungsserver beziehen. Der Client leitet dieses Token dann über den Header der HTTP-Autorisierungsanforderung als *Bearer-Token* an den ONTAP-Cluster

weiter. Je nach Sicherheitsstufe können Sie auch ein Zertifikat auf dem Client erstellen und installieren, um auf MTLS basierende Token mit Senderbeschränkungen zu verwenden.

Ausgewählte Terminologie

Wenn Sie sich mit einer OAuth 2.0-Bereitstellung mit ONTAP vertraut machen, ist es hilfreich, sich mit einigen Begriffen vertraut zu machen. Siehe "Weitere Ressourcen" Für Links zu weiteren Informationen über OAuth 2.0.

Access Token

Ein Token, das von einem Autorisierungsserver ausgegeben und von einer OAuth 2.0-Clientanwendung verwendet wird, um Anfragen für den Zugriff auf die geschützten Ressourcen zu stellen.

JSON-Webtoken

Der Standard, der zum Formatieren der Zugriffstoken verwendet wird. JSON wird verwendet, um die OAuth 2.0 Claims in einem kompakten Format darzustellen, wobei die Claims in drei Hauptabschnitten angeordnet sind.

Zugriffstoken, die durch den Absender eingeschränkt sind

Eine optionale Funktion, die auf dem Protokoll Mutual Transport Layer Security (MTLS) basiert. Durch die Verwendung eines zusätzlichen Bestätigungsanspruchs im Token wird sichergestellt, dass das Zugriffstoken nur von dem Client verwendet wird, auf den es ursprünglich ausgestellt wurde.

JSON-Webschlüsselsatz

Ein JWKS ist eine Sammlung öffentlicher Schlüssel, die von ONTAP zur Überprüfung der von den Clients präsentierten JWT-Token verwendet werden. Die Schlüsselsätze sind normalerweise über einen dedizierten URI am Autorisierungsserver verfügbar.

Umfang

Scopes bieten eine Möglichkeit, den Zugriff einer Applikation auf geschützte Ressourcen wie die REST-API von ONTAP zu beschränken oder zu steuern. Sie werden im Zugriffstoken als Strings dargestellt.

ONTAP-REST-Rolle

REST-Rollen wurden mit ONTAP 9.6 eingeführt und sind ein wichtiger Bestandteil des RBAC Framework von ONTAP. Diese Rollen unterscheiden sich von den früheren herkömmlichen Rollen, die immer noch von ONTAP unterstützt werden. Die OAuth 2.0-Implementierung in ONTAP unterstützt nur REST-Rollen.

HTTP-Autorisierungskopf

Eine Kopfzeile, die in der HTTP-Anforderung enthalten ist, um den Client und die zugehörigen Berechtigungen als Teil eines REST-API-Aufrufs zu identifizieren. Je nachdem, wie Authentifizierung und Autorisierung durchgeführt werden, stehen verschiedene Varianten oder Implementierungen zur Verfügung. Wenn ein OAuth 2.0-Zugriffstoken an ONTAP übergeben wird, wird das Token als *Bearer Token* identifiziert.

HTTP-Basisauthentifizierung

Eine frühe HTTP-Authentifizierungstechnik, die noch von ONTAP unterstützt wird. Die Klartext-Anmeldeinformationen (Benutzername und Passwort) werden mit einem Doppelpunkt verkettet und in base64 kodiert. Die Zeichenfolge wird in den Header der Autorisierungsanforderung eingefügt und an den Server gesendet.

FAPI

Eine Arbeitsgruppe der OpenID Foundation, die Protokolle, Datenschemas und Sicherheitsempfehlungen für die Finanzbranche bereitstellt. Die API wurde ursprünglich als Financial Grade API bekannt.

GEHRUNG

Ein privates gemeinnütziges Unternehmen, das technische und sicherheitstechnische Leitlinien für die US-Luftwaffe und die US-Regierung bereitstellt.

Weitere Ressourcen

Im Folgenden finden Sie einige zusätzliche Ressourcen. Sie sollten diese Seiten durchsehen, um weitere Informationen über OAuth 2.0 und die zugehörigen Standards zu erhalten.

Protokolle und Standards

- "RFC 6749: Das OAuth 2.0 Authorization Framework"
- "RFC 7519: JSON Web Tokens (JWT)"
- "RFC 7523: JSON Web Token (JWT) Profile für OAuth 2.0 Client Authentication and Authorization Grants"
- "RFC 7662: OAuth 2.0 Token-Introspektion"
- "RFC 7800: Proof-of-Possession Key für JWTs"
- "RFC 8705: OAuth 2.0 Mutual-TLS Client Authentication und Certificate-bound Access Tokens"

Organisationen

- "OpenID Foundation"
- "FAPI-Arbeitsgruppe"
- "GEHRUNG"
- "IANA - JWT"

Produkte und Services

- "Auth0"
- "ADFS-Übersicht"
- "Keycloak"

Zusätzliche Tools und Dienstprogramme

- "JWT von Auth0"
- "OpenSSL"

NetApp Dokumentation und Ressourcen

- "ONTAP-Automatisierung" Dokumentation

Konzepte

Autorisierungsserver und Zugriffstoken

Autorisierungsserver führen als zentrale Komponente im OAuth 2.0-Autorisierungs-Framework mehrere wichtige Funktionen aus.

OAuth 2.0-Autorisierungsserver

Autorisierungsserver sind in erster Linie für das Erstellen und Signieren von Zugriffstoken verantwortlich. Diese Token enthalten Identitäts- und Autorisationsinformationen, die es einer Clientanwendung ermöglichen,

selektiv auf geschützte Ressourcen zuzugreifen. Die Server sind in der Regel voneinander isoliert und können auf verschiedene Weise implementiert werden, beispielsweise als eigenständiger dedizierter Server oder als Teil eines größeren Identitäts- und Zugriffsverwaltungsprodukts.

> Für einen Autorisierungsserver kann manchmal eine andere Terminologie verwendet werden, insbesondere wenn die OAuth 2.0-Funktionalität in einem größeren Produkt oder einer größeren Lösung zur Identitäts- und Zugriffsverwaltung enthalten ist. Der Begriff **Identity Provider (IdP)** wird beispielsweise häufig mit **Authorization Server** synonym verwendet.

Administration

Zusätzlich zur Ausgabe von Zugriffstoken bieten Autorisierungsserver auch zugehörige Verwaltungsdienste, in der Regel über eine Web-Benutzeroberfläche. Sie können beispielsweise Folgendes definieren und verwalten:

- Benutzer- und Benutzerauthentifizierung
- Bereich
- Administrative Trennung durch Mandanten und Bereiche
- Richtlinienumsetzung
- Anbindung an verschiedene externe Dienste
- Unterstützung für andere Identitätsprotokolle (z. B. SAML)

ONTAP ist mit Autorisierungsservern kompatibel, die dem OAuth 2.0-Standard entsprechen.

Definieren auf ONTAP

Sie müssen einen oder mehrere Autorisierungsserver für ONTAP definieren. ONTAP kommuniziert sicher mit jedem Server, um Token zu überprüfen und andere damit verbundene Aufgaben zur Unterstützung der Client-Anwendungen auszuführen.

Die wichtigsten Aspekte der ONTAP-Konfiguration sind im Folgenden aufgeführt. Siehe auch "OAuth 2.0-Bereitstellungsszenarien" Finden Sie weitere Informationen.

Wie und wo die Zugriffstoken validiert werden

Es gibt zwei Optionen für die Validierung von Zugriffstoken.

- Lokale Validierung

  ONTAP kann Zugriffstoken lokal anhand der Informationen validieren, die vom Autorisierungsserver bereitgestellt werden, der das Token ausgestellt hat. Die vom Autorisierungsserver abgerufenen Informationen werden von ONTAP zwischengespeichert und in regelmäßigen Abständen aktualisiert.

- Fernintrospektion

  Sie können auch Remote-Introspektion verwenden, um Token auf dem Autorisierungsserver zu validieren. Introspektion ist ein Protokoll, das es autorisierten Parteien ermöglicht, einen Autorisierungsserver nach einem Zugriffstoken abzufragen. Es bietet ONTAP eine Möglichkeit, bestimmte Metadaten aus einem Zugriffstoken zu extrahieren und das Token zu validieren. ONTAP speichert einige Daten aus Gründen der Performance im Cache.

Netzwerkspeicherort

ONTAP befindet sich möglicherweise hinter einer Firewall. In diesem Fall müssen Sie einen Proxy als Teil der Konfiguration identifizieren.

Wie die Autorisierungsserver definiert werden

Sie können einen Autorisierungsserver für ONTAP über eine der Administrationsschnittstellen definieren, einschließlich CLI, System Manager oder REST-API. Beispielsweise verwenden Sie in der CLI den Befehl `security oauth2 client create`.

Anzahl der Autorisierungsserver

Sie können bis zu acht Autorisierungsserver für einen einzelnen ONTAP-Cluster definieren. Der gleiche Autorisierungsserver kann für denselben ONTAP-Cluster mehr als einmal definiert werden, solange die Ansprüche des Emittenten oder des Emittenten/der Zielgruppe eindeutig sind. Zum Beispiel, mit Keycloak wird dies immer der Fall sein, wenn verschiedene Bereiche.

Verwenden von OAuth 2.0-Zugriffstoken

Die von den Autorisierungsservern ausgegebenen OAuth 2.0-Zugriffstoken werden von ONTAP überprüft und für rollenbasierte Zugriffsentscheidungen für die REST-API-Clientanforderungen verwendet.

Abrufen eines Zugriffstoken

Sie müssen ein Zugriffstoken von einem Autorisierungsserver erwerben, der für das ONTAP-Cluster definiert ist, wo Sie die REST-API verwenden. Um ein Token zu erwerben, müssen Sie sich direkt an den Autorisierungsserver wenden.

> ONTAP gibt keine Zugriffstoken aus und leitet Anforderungen von Clients nicht an die Autorisierungsserver weiter.

Wie Sie ein Token anfordern, hängt von mehreren Faktoren ab, darunter:

- Autorisierungsserver und seine Konfigurationsoptionen
- OAuth 2.0 Zuschussart
- Client oder Softwaretool zur Ausgabe der Anforderung

Grant-Typen

Ein *Grant* ist ein gut definierter Prozess, einschließlich einer Reihe von Netzwerkflüssen, die zum anfordern und Empfangen eines OAuth 2.0-Zugriffstoken verwendet werden. Je nach Client-, Umgebungs- und Sicherheitsanforderungen können verschiedene Zuteilungsarten verwendet werden. Eine Liste der gängigen Fördertypen finden Sie in der folgenden Tabelle.

Zuteilungsart	Beschreibung
Client-Anmeldedaten	Ein beliebter Zuschusstyp, der nur auf der Verwendung von Anmeldeinformationen basiert (z. B. eine ID und ein gemeinsam genutzter Schlüssel). Es wird davon ausgegangen, dass der Client eine enge Vertrauensbeziehung zum Ressourcenbesitzer hat.
Passwort	Der Zuteilungstyp für die Kennwortanmeldeinformationen des Ressourceneigentümers kann in Fällen verwendet werden, in denen der Ressourceneigentümer über eine Vertrauensbeziehung zum Client verfügt. Sie kann auch bei der Migration älterer HTTP-Clients zu OAuth 2.0 nützlich sein.
Autorisierungscode	Dies ist eine ideale Zuteilungsart für vertrauliche Clients und basiert auf einem auf Umleitung basierenden Fluss. Es kann verwendet werden, um sowohl ein Zugriffstoken als auch ein Aktualisierungs-Token zu erhalten.

JWT-Inhalt

Ein OAuth 2.0-Zugriffstoken ist als JWT formatiert. Der Inhalt wird basierend auf Ihrer Konfiguration vom Autorisierungsserver erstellt. Die Token sind jedoch für die Client-Anwendungen undurchsichtig. Ein Kunde hat keinen Grund, ein Token zu prüfen oder sich des Inhalts bewusst zu sein.

Jedes JWT-Zugriffstoken enthält eine Reihe von Ansprüchen. Die Ansprüche beschreiben die Merkmale des Emittenten und die Autorisierung basierend auf administrativen Definitionen am Autorisierungsserver. Einige der mit dem Standard registrierten Ansprüche sind in der folgenden Tabelle beschrieben. Bei allen Strings wird zwischen Groß- und Kleinschreibung unterschieden.

Forderung	Stichwort	Beschreibung
Aussteller	ISS	Identifiziert den Prinzipal, der das Token ausgegeben hat. Die Antragsbearbeitung ist anwendungsspezifisch.
Betreff	Unterbereich	Der Betreff oder Benutzer des Tokens. Der Name ist global oder lokal eindeutig.
Zielgruppe	AUD	Die Empfänger, für die das Token bestimmt ist. Als Array von Strings implementiert.
Ablauf	exsp	Die Zeit, nach der das Token abläuft und zurückgewiesen werden muss.

Siehe "RFC 7519: JSON Web Tokens" Finden Sie weitere Informationen.

Optionen für die ONTAP-Clientautorisierung

Für die Anpassung Ihrer ONTAP-Clientautorisierung stehen verschiedene Optionen zur Verfügung. Die Autorisierungsentscheidungen basieren letztlich auf den ONTAP-REST-Rollen, die entweder in den Zugriffstoken enthalten sind oder von diesen abgeleitet wurden.

> Sie können nur verwenden "ONTAP REST-Rollen" Bei der Konfiguration der Autorisierung für OAuth 2.0. Die früheren herkömmlichen ONTAP Rollen werden nicht unterstützt.

Einführung

Die OAuth 2.0 Implementierung in ONTAP ist flexibel und robust und bietet Ihnen die Optionen, die Sie für die Sicherung der ONTAP Umgebung benötigen. Im Wesentlichen gibt es drei Hauptkonfigurationskategorien zur Definition der ONTAP-Clientautorisierung. Diese Konfigurationsoptionen schließen sich gegenseitig aus.

ONTAP wendet je nach Konfiguration die am besten geeignete Option an. Siehe "Wie ONTAP den Zugriff bestimmt" Finden Sie heraus, wie ONTAP Ihre Konfigurationsdefinitionen für Zugriffsentscheidungen verarbeitet.

OAuth 2.0 eigenständige Oszilloskope

Diese Bereiche enthalten eine oder mehrere benutzerdefinierte REST-Rollen, die jeweils in einer einzigen Zeichenfolge gekapselt sind. Sie sind unabhängig von den Rollendefinitionen von ONTAP. Sie müssen diese Bereichszeichenfolgen auf Ihrem Autorisierungsserver definieren.

Lokale ONTAP-spezifische REST-Rollen und Benutzer

Je nach Konfiguration können die lokalen ONTAP-Identitätsdefinitionen für Zugriffsentscheidungen verwendet

werden. Folgende Optionen stehen zur Verfügung:

- Einzelne benannte REST-Rolle
- Übereinstimmung des Benutzernamens mit einem lokalen ONTAP-Benutzer

Die scope Syntax für eine benannte Rolle ist **ontap-role-**<URL-encoded-ONTAP-role-name>. Wenn die Rolle beispielsweise „admin“ lautet, lautet der Scope-String „ontap-role-admin“.

Active Directory oder LDAP-Gruppen

Wenn die lokalen ONTAP-Definitionen überprüft werden, aber keine Zugriffsentscheidung getroffen werden kann, werden die Active Directory („Domain“)- oder LDAP („nsswitch“)-Gruppen verwendet. Gruppeninformationen können auf zwei Arten angegeben werden:

- OAuth 2.0-Scope-String

  Unterstützt vertrauliche Anwendungen, die den Ablauf der Clientanmeldeinformationen verwenden, wenn kein Benutzer mit einer Gruppenmitgliedschaft vorhanden ist. Der Umfang sollte benannt werden **ontap-Group-**<URL-encoded-ONTAP-group-name>. Wenn die Gruppe beispielsweise „Entwicklung“ ist, lautet der Scope String „ontap-Group-Development“.

- In der „Gruppe“-Forderung

  Dies ist für Zugriffstoken vorgesehen, die von ADFS unter Verwendung des Ablaufs Resource Owner (Password Grant) ausgegeben werden.

Eigenständige Oszilloskope von OAuth 2.0

In sich geschlossene Bereiche sind Strings, die im Zugriffstoken enthalten sind. Jede dieser Rollen ist vollständig definiert und beinhaltet alles, was ONTAP für eine Zugriffsentscheidung benötigt. Der Umfang unterscheidet sich von jeder der REST-Rollen, die in ONTAP selbst definiert sind.

Format der Bereichszeichenfolge

Auf einer Basisebene wird der Umfang als zusammenhängende Zeichenfolge dargestellt und besteht aus sechs durch Doppelpunkte getrennten Werten. Die im Scope String verwendeten Parameter werden im Folgenden beschrieben.

ONTAP-Literal

Der Bereich muss mit dem Literalwert beginnen `ontap` In Kleinbuchstaben. Der ONTAP-spezifische Umfang wird angegeben.

Cluster

Dies definiert, auf welchen ONTAP Cluster sich der Umfang bezieht. Die Werte können Folgendes umfassen:

- Cluster-UUID

  Identifiziert ein einzelnes Cluster.

- Sternchen (*)

  Gibt an, dass der Umfang auf alle Cluster angewendet wird.

Sie können den ONTAP-CLI-Befehl verwenden `cluster identity show` Um die UUID des Clusters anzuzeigen. Falls nicht angegeben, gilt der Umfang für alle Cluster.

Rolle

Der Name der im eigenständigen Bereich enthaltenen REST-Rolle. Dieser Wert wird von ONTAP nicht untersucht oder auf vorhandene REST-Rollen abgestimmt, die für ONTAP definiert sind. Der Name wird für die Protokollierung verwendet.

Zugangsstufe

Dieser Wert gibt die Zugriffsebene an, die auf die Clientanwendung angewendet wird, wenn der API-Endpunkt im Umfang verwendet wird. Es gibt sechs mögliche Werte, wie in der Tabelle unten beschrieben.

Zugangsstufe	Beschreibung
Keine	Verweigert allen Zugriff auf den angegebenen Endpunkt.
readonly	Nur Lesezugriff mit GET ist möglich.
Read_create	Ermöglicht den Lesezugriff sowie die Erstellung neuer Ressourceninstanzen über POST.
Lesen_ändern	Ermöglicht den Lesezugriff sowie die Möglichkeit, vorhandene Ressourcen mithilfe von PATCHES zu aktualisieren.
Lesen_create_modify	Ermöglicht alle Zugriffe außer Löschen. Zu den zulässigen Operationen gehören GET (read), POST (create) und PATCH (Update).
Alle	Ermöglicht vollständigen Zugriff.

SVM

Der Name der SVM innerhalb des Clusters, für den der Umfang gilt. Verwenden Sie den *-Wert (Sternchen), um alle SVMs anzuzeigen.

> Diese Funktion wird von ONTAP 9.14.1 nicht vollständig unterstützt. Sie können den SVM-Parameter ignorieren und ein Sternchen als Platzhalter verwenden. Überprüfen Sie die "Versionshinweise zu ONTAP" Um auf zukünftige SVM-Unterstützung zu prüfen.

REST-API-URI

Der vollständige oder teilweise Pfad zu einer Ressource oder einem Satz zugehöriger Ressourcen. Der String muss mit beginnen `/api`. Wenn Sie keinen Wert angeben, gilt der Umfang für alle API-Endpunkte im ONTAP-Cluster.

Beispiele für den Umfang

Im Folgenden werden einige Beispiele für eigenständige Oszilloskope vorgestellt.

ontap:*:joes-role:read_create_modify:*:/API/Cluster

Bietet dem Benutzer, dem diese Rolle zugewiesen ist, den Zugriff auf das zu lesen, zu erstellen und zu ändern `/cluster` endpunkt:

CLI-Verwaltungstool

Um die Administration der eigenständigen Bereiche einfacher und weniger fehleranfällig zu machen, bietet ONTAP den CLI-Befehl `security oauth2 scope` So generieren Sie auf der Grundlage Ihrer Eingabeparameter Oszilloskop-Strings.

Der Befehl `security oauth2 scope` Basierend auf Ihren Angaben gibt es zwei Anwendungsfälle:

- CLI-Parameter für den Umfang einer Zeichenfolge

  Mit dieser Version des Befehls können Sie auf Grundlage der Eingabeparameter eine Bereichszeichenfolge generieren.

- Scope-String zu CLI-Parametern

  Sie können diese Version des Befehls verwenden, um die Befehlsparameter basierend auf der Zeichenfolge für den Eingabebereich zu generieren.

Beispiel

Im folgenden Beispiel wird eine Scope-String mit der Ausgabe generiert, die nach dem unten stehenden Befehlsbeispiel enthalten ist. Die Definition gilt für alle Cluster.

```
security oauth2 scope cli-to-scope -role joes-role -access readonly -api
/api/cluster
```

```
ontap:*:joes-role:readonly:*:/api/cluster
```

Wie ONTAP den Zugriff bestimmt

Um OAuth 2.0 richtig zu entwickeln und zu implementieren, müssen Sie verstehen, wie Ihre Autorisierungskonfiguration von ONTAP verwendet wird, um Zugriffsentscheidungen für die Clients zu treffen.

Schritt 1: Eigenständige Bereiche

Wenn das Zugriffstoken eigenständige Bereiche enthält, untersucht ONTAP diese Bereiche zuerst. Wenn keine eigenständigen Bereiche vorhanden sind, mit Schritt 2 fortfahren.

Wenn ein oder mehrere eigenständige Bereiche vorhanden sind, wendet ONTAP jeden Bereich an, bis eine explizite **ALLOW**- oder **DENY**-Entscheidung getroffen werden kann. Wenn eine explizite Entscheidung getroffen wird, endet die Verarbeitung.

Wenn ONTAP keine explizite Zugriffsentscheidung treffen kann, fahren Sie mit Schritt 2 fort.

Schritt 2: Überprüfen Sie die lokale Rollenmarkierung

ONTAP überprüft den Wert des Flags `use-local-roles-if-present`. Der Wert dieses Flags wird für jeden Autorisierungsserver, der für ONTAP definiert ist, separat festgelegt.

- Wenn der Wert ist `true` Fahren Sie mit Schritt 3 fort.
- Wenn der Wert ist `false` Die Verarbeitung endet und der Zugriff wird verweigert.

Schritt 3: Benannte ONTAP REST-Rolle

Wenn das Zugriffstoken eine benannte REST-Rolle enthält, verwendet ONTAP die Rolle, um die

Zugriffsentscheidung zu treffen. Dies führt immer zu einer **ALLOW** oder **DENY** Entscheidung und Verarbeitungsende.

Wenn keine benannte REST-Rolle vorhanden ist oder die Rolle nicht gefunden wurde, fahren Sie mit Schritt 4 fort.

Schritt 4: Lokale ONTAP-Benutzer

Extrahieren Sie den Benutzernamen aus dem Zugriffstoken und versuchen Sie, ihn einem lokalen ONTAP-Benutzer zuzuordnen.

Wenn ein lokaler ONTAP-Benutzer abgeglichen wird, verwendet ONTAP die für den Benutzer definierte Rolle, um eine Zugriffsentscheidung zu treffen. Dies führt immer zu einer **ALLOW** oder **DENY** Entscheidung und Verarbeitungsende.

Wenn ein lokaler ONTAP-Benutzer nicht stimmt oder kein Benutzername im Zugriffstoken vorhanden ist, fahren Sie mit Schritt 5 fort.

Schritt 5: Gruppen-zu-Rollen-Zuordnung

Extrahieren Sie die Gruppe aus dem Zugriffstoken, und versuchen Sie, sie einer Gruppe zuzuordnen. Die Gruppen werden über Active Directory oder einen gleichwertigen LDAP-Server definiert.

Wenn eine Gruppenübereinstimme vorhanden ist, verwendet ONTAP die für die Gruppe definierte Rolle, um eine Zugriffsentscheidung zu treffen. Dies führt immer zu einer **ALLOW** oder **DENY** Entscheidung und Verarbeitungsende.

Wenn keine Gruppenübereinstimme vorhanden ist oder keine Gruppe im Zugriffstoken vorhanden ist, wird der Zugriff verweigert und die Verarbeitung wird beendet.

OAuth 2.0-Bereitstellungsszenarien

Beim Definieren eines Autorisierungsservers für ONTAP stehen verschiedene Konfigurationsoptionen zur Verfügung. Basierend auf diesen Optionen können Sie einen Autorisierungsserver erstellen, der für Ihre Bereitstellungsumgebung geeignet ist.

Zusammenfassung der Konfigurationsparameter

Beim Definieren eines Autorisierungsservers für ONTAP stehen mehrere Konfigurationsparameter zur Verfügung. Diese Parameter werden in der Regel in allen administrativen Schnittstellen unterstützt.

Die Parameternamen können je nach ONTAP-Administratorschnittstelle leicht variieren. Bei der Konfiguration der Remote-Introspektion wird der Endpunkt beispielsweise mit dem CLI-Befehlsparameter identifiziert `-introspection-endpoint`. Aber mit dem System Manager ist das äquivalente Feld *Authorization Server Token Introspection URI*. Um alle ONTAP-Verwaltungsschnittstellen aufzunehmen, wird eine allgemeine Beschreibung der Parameter bereitgestellt. Der genaue Parameter oder das Feld sollte je nach Kontext offensichtlich sein.

Parameter	Beschreibung
Name	Der Name des Autorisierungsservers, der ONTAP bekannt ist.
Applikation	Die ONTAP-interne Anwendung, für die die Definition gilt. Dies muss **http** sein.
Aussteller-URI	Der FQDN mit Pfad, der den Standort oder die Organisation identifiziert, der die Token ausgibt.

Parameter	Beschreibung
Provider-JWKS-URI	Der FQDN mit Pfad und Dateiname, bei dem ONTAP die JSON-Webschlüsselsätze erhält, die zur Validierung der Zugriffstoken verwendet werden.
JWKS-Aktualisierungsintervall	Das Zeitintervall, in dem festgelegt wird, wie oft ONTAP Zertifikatsinformationen vom Provider JWKS URI aktualisiert. Der Wert wird im ISO-8601-Format angegeben.
Introspektion Endpunkt	Der FQDN mit Pfad, den ONTAP zur Remote-Token-Validierung durch Introspektion verwendet.
Client-ID	Der Name des Clients, wie er auf dem Autorisierungsserver definiert ist. Wenn dieser Wert enthalten ist, müssen Sie auch den zugehörigen Client-Schlüssel basierend auf der Schnittstelle angeben.
Ausgehender Proxy	Damit wird der Zugriff auf den Autorisierungsserver ermöglicht, wenn sich ONTAP hinter einer Firewall befindet. Der URI muss im Curl-Format vorliegen.
Verwenden Sie ggf. lokale Rollen	Ein boolesches Flag, das bestimmt, ob die lokalen ONTAP-Definitionen verwendet werden, einschließlich einer benannten REST-Rolle und lokalen Benutzern.
Benutzeranspruch entfernen	Ein alternativer Name, den ONTAP für lokale Benutzer verwendet. Verwenden Sie die `sub` Feld im Zugriffstoken, das mit dem lokalen Benutzernamen übereinstimmt.

Bereitstellungsszenarien

Im Folgenden werden verschiedene gängige Bereitstellungsszenarien vorgestellt. Sie sind abhängig davon organisiert, ob die Token-Validierung lokal durch ONTAP oder Remote durch den Autorisierungsserver durchgeführt wird. Jedes Szenario enthält eine Liste der erforderlichen Konfigurationsoptionen. Siehe "Implementieren Sie OAuth 2.0 in ONTAP" Beispiele für Konfigurationsbefehle.

> Nachdem Sie einen Autorisierungsserver definiert haben, können Sie seine Konfiguration über die ONTAP-Verwaltungsschnittstelle anzeigen. Verwenden Sie beispielsweise den Befehl `security oauth2 client show` Mit der ONTAP CLI.

Lokale Validierung

Die folgenden Bereitstellungsszenarien basieren auf der lokalen Tokenvalidierung durch ONTAP.

Verwenden Sie eigenständige Bereiche ohne Proxy

Dies ist die einfachste Bereitstellung, bei der nur OAuth 2.0 eigenständige Bereiche verwendet werden. Keine der lokalen ONTAP-Identitätsdefinitionen werden verwendet. Sie müssen die folgenden Parameter angeben:

- Name
- Anwendung (http)
- Provider-JWKS-URI
- Aussteller-URI

Sie müssen die Gültigkeitsbereiche auch auf dem Autorisierungsserver hinzufügen.

Verwenden Sie eigenständige Bereiche mit einem Proxy

In diesem Bereitstellungsszenario werden die eigenständigen Oszilloskope von OAuth 2.0 verwendet. Keine der lokalen ONTAP-Identitätsdefinitionen werden verwendet. Aber der Autorisierungsserver befindet sich hinter einer Firewall und Sie müssen daher einen Proxy konfigurieren. Sie müssen die folgenden Parameter angeben:

- Name
- Anwendung (http)
- Provider-JWKS-URI
- Ausgehender Proxy
- Aussteller-URI
- Zielgruppe

Sie müssen die Gültigkeitsbereiche auch auf dem Autorisierungsserver hinzufügen.

Verwenden Sie lokale Benutzerrollen und die standardmäßige Zuweisung von Benutzernamen mit einem Proxy

Dieses Bereitstellungsszenario verwendet lokale Benutzerrollen mit Standardnamenszuordnung. Der Anspruch des Remotebenutzers verwendet den Standardwert `sub` Daher wird dieses Feld im Zugriffstoken verwendet, um mit dem lokalen Benutzernamen zu übereinstimmen. Der Benutzername darf maximal 40 Zeichen lang sein. Der Autorisierungsserver befindet sich hinter einer Firewall, Sie müssen also auch einen Proxy konfigurieren. Sie müssen die folgenden Parameter angeben:

- Name
- Anwendung (http)
- Provider-JWKS-URI
- Verwenden Sie ggf. lokale Rollen (`true`)
- Ausgehender Proxy
- Aussteller

Sie müssen sicherstellen, dass der lokale Benutzer für ONTAP definiert ist.

Verwenden Sie lokale Benutzerrollen und alternative Benutzernamen-Zuordnungen mit einem Proxy

Dieses Bereitstellungsszenario verwendet lokale Benutzerrollen mit einem alternativen Benutzernamen, der für einen lokalen ONTAP-Benutzer verwendet wird. Der Autorisierungsserver befindet sich hinter einer Firewall, Sie müssen also einen Proxy konfigurieren. Sie müssen die folgenden Parameter angeben:

- Name
- Anwendung (http)
- Provider-JWKS-URI
- Verwenden Sie ggf. lokale Rollen (`true`)
- Anspruch des Remote-Benutzers
- Ausgehender Proxy
- Aussteller-URI
- Zielgruppe

Sie müssen sicherstellen, dass der lokale Benutzer für ONTAP definiert ist.

Fernintrospektion

Die folgenden Bereitstellungskonfigurationen basieren auf ONTAP, die Token per Remote-Prüfung durch Introspektion validieren.

Verwenden Sie eigenständige Bereiche ohne Proxy

Dies ist eine einfache Bereitstellung, die auf der Verwendung der eigenständigen Oszilloskope von OAuth 2.0 basiert. Keine der ONTAP-Identitätsdefinitionen wird verwendet. Sie müssen die folgenden Parameter einschließen:

- Name
- Anwendung (http)
- Introspektion Endpunkt
- Client-ID
- Aussteller-URI

Sie müssen die Bereiche sowie den Client- und Client-Schlüssel auf dem Autorisierungsserver definieren.

Client-Authentifizierung mit gegenseitigem TLS

Je nach Ihren Sicherheitsanforderungen können Sie optional Mutual TLS (MTLS) zur Implementierung einer starken Clientauthentifizierung konfigurieren. Bei Verwendung mit ONTAP als Teil einer OAuth 2.0-Bereitstellung garantiert MTLS, dass die Zugriffstoken nur von den Clients verwendet werden, für die sie ursprünglich ausgegeben wurden.

Gegenseitiges TLS mit OAuth 2.0

Transport Layer Security (TLS) wird verwendet, um einen sicheren Kommunikationskanal zwischen zwei Anwendungen herzustellen, in der Regel zwischen einem Client-Browser und einem Webserver. Mutual TLS erweitert dies durch eine starke Identifizierung des Clients über ein Client-Zertifikat. Bei Verwendung in einem ONTAP-Cluster mit OAuth 2.0 wird die Basis-MTLS-Funktionalität durch das Erstellen und Verwenden von Sender-beschränkten Zugriffstoken erweitert.

Ein vom Absender beschränktem Zugriffstoken kann nur vom Client verwendet werden, an den es ursprünglich ausgegeben wurde. Um diese Funktion zu unterstützen, muss ein neuer Bestätigungsantrag gestellt werden (`cnf`) Wird in das Token eingefügt. Das Feld enthält die Eigenschaft `x5t#S256` Enthält einen Digest des Clientzertifikats, das bei der Anforderung des Zugriffstoken verwendet wird. Dieser Wert wird von ONTAP im Rahmen der Überprüfung des Tokens überprüft. Von Autorisierungsservern ausgegebene Zugriffstoken, die nicht durch den Absender eingeschränkt sind, enthalten keinen zusätzlichen Bestätigungsanspruch.

Sie müssen ONTAP so konfigurieren, dass MTLS für jeden Autorisierungsserver separat verwendet wird. Beispiel: Der CLI-Befehl `security oauth2 client` Enthält den Parameter `use-mutual-tls` Zur Steuerung der MTLS-Verarbeitung anhand von drei Werten, wie in der folgenden Tabelle dargestellt.

> In jeder Konfiguration hängen das Ergebnis und die von ONTAP ergriffenen Maßnahmen vom Wert des Konfigurationsparameters sowie vom Inhalt des Zugriffstoken und des Clientzertifikats ab. Die Parameter in der Tabelle sind vom kleinsten bis zum restriktivsten organisiert.

Parameter	Beschreibung
Keine	Die gegenseitige TLS-Authentifizierung OAuth 2.0 ist für den Autorisierungsserver vollständig deaktiviert. ONTAP führt keine MTLS-Clientzertifikatauthentifizierung durch, selbst wenn der Bestätigungsanspruch im Token vorhanden ist oder ein Clientzertifikat mit der TLS-Verbindung geliefert wird.
Anforderung	Die gegenseitige TLS-Authentifizierung von OAuth 2.0 wird erzwungen, wenn ein vom Absender beschränktes Zugriffstoken vom Client angezeigt wird. Das heißt, MTLS wird nur erzwungen, wenn die Bestätigung Anspruch (mit Eigentum `x5t#S256`) Ist im Access-Token vorhanden. Dies ist die Standardeinstellung.
Erforderlich	Die gegenseitige TLS-Authentifizierung OAuth 2.0 wird für alle Zugriffstoken durchgesetzt, die vom Autorisierungsserver ausgegeben werden. Daher müssen alle Zugriffstoken durch den Absender eingeschränkt sein. Die Authentifizierung und die REST-API-Anforderung schlagen fehl, wenn der Bestätigungsanspruch nicht im Zugriffstoken vorhanden ist oder wenn ein ungültiges Clientzertifikat vorliegt.

Grundlegende Implementierungsablaufs

Die typischen Schritte bei der Verwendung von MTLS mit OAuth 2.0 in einer ONTAP-Umgebung sind nachfolgend dargestellt. Siehe "RFC 8705: OAuth 2.0 Mutual-TLS Client Authentication und Certificate-bound Access Tokens" Entnehmen.

Schritt 1: Erstellen und installieren Sie ein Client-Zertifikat

Die Ermittlung der Kundenidentität basiert auf dem Nachweis der Kenntnis eines privaten Kundenschlüssels. Der entsprechende öffentliche Schlüssel wird in ein signiertes X.509-Zertifikat gelegt, das vom Client vorgelegt wird. Auf einer übergeordneten Ebene umfassen die Schritte zur Erstellung des Clientzertifikats Folgendes:

1. Erzeugen Sie ein öffentliches und privates Schlüsselpaar
2. Erstellen Sie eine Zertifikatsignierungsanforderung
3. Senden Sie die CSR-Datei an eine bekannte Zertifizierungsstelle
4. CA überprüft die Anforderung und stellt das signierte Zertifikat aus

Sie können das Clientzertifikat normalerweise in Ihrem lokalen Betriebssystem installieren oder direkt mit einem gängigen Dienstprogramm wie Curl verwenden.

Schritt 2: Konfigurieren Sie ONTAP für die Verwendung von MTLS

Sie müssen ONTAP für die Verwendung von MTLS konfigurieren. Diese Konfiguration erfolgt für jeden Autorisierungsserver separat. Beispielsweise mit dem CLI-Befehl `security oauth2 client` Wird mit dem optionalen Parameter verwendet `use-mutual-tls`. Siehe "Implementieren Sie OAuth 2.0 in ONTAP" Finden Sie weitere Informationen.

Schritt 3: Client fordert ein Zugriffstoken an

Der Client muss ein Zugriffstoken vom Autorisierungsserver anfordern, der für ONTAP konfiguriert ist. Die Client-Anwendung muss MTLS mit dem in Schritt 1 erstellten und installierten Zertifikat verwenden.

Schritt 4: Der Autorisierungsserver generiert das Zugriffstoken

Der Autorisierungsserver überprüft die Clientanforderung und erstellt ein Zugriffstoken. Dazu wird ein Nachrichtendigest des Client-Zertifikats erstellt, das als Bestätigungsforderung im Token enthalten ist (Feld `cnf`).

Schritt 5: Client-Anwendung präsentiert das Zugriffstoken an ONTAP

Die Client-Anwendung führt einen REST-API-Aufruf zum ONTAP-Cluster durch und schließt das Zugriffstoken in den Header der Autorisierungsanforderung als **Bearer Token** ein. Der Client muss MTLS mit demselben Zertifikat verwenden, das für die Anforderung des Zugriffstoken verwendet wird.

Schritt 6: ONTAP überprüft Client und Token.

ONTAP erhält das Zugriffstoken in einer HTTP-Anfrage sowie das Clientzertifikat, das als Teil der MTLS-Verarbeitung verwendet wird. ONTAP validiert zuerst die Signatur im Zugriffstoken. Basierend auf der Konfiguration generiert ONTAP einen Nachrichtendigest des Client-Zertifikats und vergleicht ihn mit dem Bestätigungsanspruch **cnf** im Token. Wenn die beiden Werte übereinstimmen, hat ONTAP bestätigt, dass der Client, der die API-Anforderung erstellt, derselbe Client ist, für den das Zugriffstoken ursprünglich ausgegeben wurde.

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"
```