Autenticazione e autorizzazione utilizzando OAuth 2,0

ONTAP 9

NetApp
February 12, 2026

This PDF was generated from https://docs.netapp.com/it-it/ontap/authentication/overview-oauth2.html on February 12, 2026. Always check docs.netapp.com for the latest.

Sommario

Autenticazione e autorizzazione utilizzando OAuth 2,0 . . . 1
- Panoramica dell'implementazione di ONTAP OAuth 2,0 . . . 1
  - Caratteristiche e vantaggi . . . 1
  - Implementazione e configurazione . . . 2
  - Terminologia selezionata . . . 3
  - Risorse aggiuntive . . . 4
- Concetti . . . 4
  - Server di autorizzazione OAuth 2.0 e token di accesso in ONTAP . . . 4
  - Autorizzazione del client . . . 8
  - Scenari di distribuzione OAuth 2.0 con ONTAP . . . 16
  - Autenticazione client ONTAP tramite OAuth 2.0 Mutual TLS . . . 18
- Configurazione e implementazione . . . 20
  - Preparati a implementare OAuth 2,0 con ONTAP . . . 20
  - Implementa OAuth 2,0 in ONTAP . . . 22
  - Emettere una chiamata API REST ONTAP utilizzando OAuth 2.0 . . . 26

Autenticazione e autorizzazione utilizzando OAuth 2,0

Panoramica dell'implementazione di ONTAP OAuth 2,0

A partire da ONTAP 9,14, puoi controllare l'accesso ai tuoi cluster ONTAP utilizzando il framework Open Authorization (OAuth 2,0). Puoi configurare questa funzionalità utilizzando qualsiasi interfaccia amministrativa di ONTAP, inclusi l'interfaccia a riga di comando di ONTAP, System Manager e l'API REST. Tuttavia, le decisioni relative all'autorizzazione e al controllo dell'accesso OAuth 2,0 possono essere applicate solo quando un client accede a ONTAP utilizzando l'API REST.

Il supporto di OAuth 2,0 è stato introdotto per la prima volta con ONTAP 9.14.0, pertanto la sua disponibilità dipende dalla versione di ONTAP in uso. Vedere "Note di rilascio di ONTAP" per ulteriori informazioni.

Caratteristiche e vantaggi

Di seguito sono descritte le principali caratteristiche e i vantaggi dell'utilizzo di OAuth 2,0 con ONTAP.

Supporto per lo standard OAuth 2,0

OAuth 2,0 è il quadro di autorizzazione standard del settore. Viene utilizzato per limitare e controllare l'accesso alle risorse protette utilizzando token di accesso firmati. L'utilizzo di OAuth 2,0 offre diversi vantaggi:

- Molte opzioni per la configurazione dell'autorizzazione
- Non rivelare mai le credenziali del client, incluse le password
- I token possono essere impostati in modo che scadano in base alla configurazione
- Ideale per l'uso con API REST

Testato con i server di autorizzazione più diffusi

L'implementazione di ONTAP OAuth 2,0 è stata testata con diversi server o servizi comuni basati sulla versione ONTAP, come segue:

- ONTAP 9.16,1 (supporto per UUID di gruppo per la mappatura dei nomi e i ruoli esterni):
  - ID Microsoft Entra
- ONTAP 9.14,1 (supporto per le funzioni standard OAuth 2,0)
  - Auth0
  - Active Directory Federation Service (ADFS)
  - Keycloak

Per "Server di autorizzazione e token di accesso"ulteriori informazioni sulle caratteristiche e le funzionalità disponibili in ciascuna release di ONTAP, visitare il sito Web all'indirizzo

Supporto per più server di autorizzazione simultanei

È possibile definire fino a otto server di autorizzazione per un singolo cluster ONTAP. Ciò offre la flessibilità necessaria per soddisfare le esigenze dei diversi ambienti di sicurezza.

Integrazione con i ruoli REST

Le decisioni di autorizzazione ONTAP si basano in ultima analisi sui ruoli REST assegnati a utenti o gruppi. Questi ruoli vengono riportati nel token di accesso come ambiti indipendenti o in base alle definizioni ONTAP locali insieme ai gruppi Active Directory o LDAP.

Opzione per utilizzare token di accesso con restrizioni del mittente

È possibile configurare ONTAP e i server di autorizzazione per utilizzare Mutual Transport Layer Security (mTLS) che rafforza l'autenticazione client. Garantisce che i token di accesso OAuth 2,0 siano utilizzati solo dai client ai quali sono stati originariamente rilasciati. Questa funzionalità supporta e si allinea con diverse raccomandazioni di protezione note, incluse quelle stabilite da FAPI e MITER.

Implementazione e configurazione

A un livello elevato, ci sono diversi aspetti di un'implementazione e configurazione di OAuth 2,0 che è necessario considerare quando si inizia.

OAuth 2,0 entità all'interno di ONTAP

Il framework di autorizzazione OAuth 2,0 definisce diverse entità che possono essere mappate ad elementi reali o virtuali all'interno del data center o della rete. Le entità OAuth 2,0 e il loro adattamento a ONTAP sono presentati nella tabella seguente.

Entità OAuth 2,0	Descrizione
Risorsa	Gli endpoint delle API REST che forniscono accesso alle risorse ONTAP tramite comandi ONTAP interni.
Proprietario della risorsa	L'utente del cluster ONTAP che ha creato la risorsa protetta o la possiede per impostazione predefinita.
Server delle risorse	L'host per le risorse protette, ovvero il cluster ONTAP.
Client	Un'applicazione che richiede l'accesso a un endpoint API REST per conto o con l'autorizzazione del proprietario della risorsa.
Server di autorizzazione	In genere, un server dedicato responsabile dell'emissione dei token di accesso e dell'applicazione dei criteri amministrativi.

Configurazione core ONTAP

È necessario configurare il cluster ONTAP per abilitare e utilizzare OAuth 2,0. Ciò include la creazione di una connessione al server di autorizzazione e la definizione della configurazione di autorizzazione ONTAP richiesta. È possibile eseguire questa configurazione utilizzando una qualsiasi delle interfacce amministrative, tra cui:

- Interfaccia a riga di comando di ONTAP
- System Manager
- API REST di ONTAP

Ambiente e servizi di supporto

Oltre alle definizioni di ONTAP, è necessario configurare anche i server di autorizzazione. Se si utilizza la mappatura da gruppo a ruolo, è necessario configurare anche i gruppi Active Directory o l'equivalente LDAP.

Client ONTAP supportati

A partire da ONTAP 9,14, un client API REST può accedere a ONTAP utilizzando OAuth 2,0. Prima di eseguire una chiamata API REST, è necessario ottenere un token di accesso dal server di autorizzazione. Il client passa

quindi questo token al cluster ONTAP come *bearer token* utilizzando l'intestazione della richiesta di autorizzazione HTTP. A seconda del livello di protezione necessario, è anche possibile creare e installare un certificato nel client per utilizzare token con vincoli di mittente basati su mTLS.

Terminologia selezionata

Quando si inizia a esaminare la distribuzione di OAuth 2,0 con ONTAP, è utile acquisire familiarità con alcune parti della terminologia. Vedere "Risorse aggiuntive" Per collegamenti a ulteriori informazioni su OAuth 2,0.

Token di accesso

Token emesso da un server di autorizzazione e utilizzato da un'applicazione client OAuth 2,0 per effettuare richieste di accesso alle risorse protette.

Token Web JSON

Lo standard utilizzato per formattare i token di accesso. JSON viene utilizzato per rappresentare le rivendicazioni OAuth 2,0 in formato compatto con le rivendicazioni disposte in tre sezioni principali.

Token di accesso vincolato dal mittente

Funzione opzionale basata sul protocollo mTLS (Mutual Transport Layer Security). Utilizzando un'ulteriore richiesta di conferma nel token, questo garantisce che il token di accesso venga utilizzato solo dal client al quale è stato originariamente emesso.

Set di chiavi Web JSON

Un JWKS è un insieme di chiavi pubbliche utilizzate da ONTAP per verificare i token JWT presentati dai clienti. I set di chiavi sono generalmente disponibili sul server di autorizzazione tramite un URI dedicato.

Scopo

Gli ambiti forniscono un modo per limitare o controllare l'accesso di un'applicazione alle risorse protette come l'API REST ONTAP. Sono rappresentate come stringhe nel token di accesso.

Ruolo REST di ONTAP

I ruoli REST sono stati introdotti con ONTAP 9,6 e costituiscono una parte fondamentale del framework RBAC di ONTAP. Questi ruoli sono diversi dai ruoli tradizionali precedenti che sono ancora supportati da ONTAP. L'implementazione di OAuth 2,0 in ONTAP supporta solo i ruoli REST.

Intestazione autorizzazione HTTP

Intestazione inclusa nella richiesta HTTP per identificare il client e le autorizzazioni associate come parte di una chiamata API REST. Sono disponibili diverse varianti o implementazioni a seconda della modalità di autenticazione e autorizzazione. Quando si presenta un token di accesso OAuth 2,0 a ONTAP, il token viene identificato come *token bearer*.

Autenticazione di base HTTP

Una tecnica di autenticazione HTTP avanzata ancora supportata da ONTAP. Le credenziali in testo normale (nome utente e password) sono concatenate con due punti e codificate in base64. La stringa viene inserita nell'intestazione della richiesta di autorizzazione e inviata al server.

FAPI

Un gruppo di lavoro della OpenID Foundation che fornisce protocolli, schemi di dati e raccomandazioni sulla sicurezza per il settore finanziario. L'API era originariamente nota come API di livello finanziario.

MITRA

Un'azienda privata senza scopo di lucro che fornisce una guida tecnica e di sicurezza all'aeronautica militare degli Stati Uniti e al governo degli Stati Uniti.

Risorse aggiuntive

Di seguito sono riportate diverse risorse aggiuntive. Dovreste rivedere questi luoghi per ottenere più informazioni su OAuth 2,0 e sugli standard relativi.

Protocolli e standard

- "RFC 6749: Framework di autorizzazione OAuth 2,0"
- "RFC 7519: Token Web JSON (JWT)"
- "RFC 7523: Profilo JSON Web Token (JWT) per l'autenticazione client OAuth 2,0 e le concessioni di autorizzazione"
- "RFC 7662: Introspezione token OAuth 2,0"
- "RFC 7800: Chiave di prova del possesso per JWT"
- "RFC 8705: Autenticazione client OAuth 2,0 Mutual-TLS e token di accesso con associazione a certificati"

Governativi

- "Fondazione OpenID"
- "Gruppo di lavoro FAPI"
- "MITRA"
- "IANA - JWT"

Prodotti e servizi

- "Auth0"
- "ID entra"
- "Panoramica di ADFS"
- "Keycloak"

Strumenti e utilità aggiuntivi

- "JWT entro il Auth0"
- "OpenSSL"

Documentazione e risorse di NetApp

- "Documentazione sull'automazione di ONTAP"

Concetti

Server di autorizzazione OAuth 2.0 e token di accesso in ONTAP

I server di autorizzazione svolgono diverse funzioni importanti come componente centrale all'interno del framework OAuth 2,0 Authorization.

Server di autorizzazione OAuth 2,0

I server di autorizzazione sono principalmente responsabili della creazione e della firma dei token di accesso. Questi token contengono informazioni di identità e autorizzazione che consentono a un'applicazione client di accedere in modo selettivo alle risorse protette. I server sono generalmente isolati l'uno dall'altro e possono essere implementati in diversi modi, incluso come server dedicato standalone o come parte di un prodotto di

gestione delle identità e degli accessi più ampio.

> A volte è possibile utilizzare una terminologia diversa per un server di autorizzazione, specialmente quando la funzionalità OAuth 2,0 è inclusa in un prodotto o una soluzione di gestione delle identità e degli accessi più ampia. Ad esempio, il termine **provider di identità (IdP)** viene spesso utilizzato in modo intercambiabile con **server di autorizzazione**.

Amministrazione

Oltre all'emissione di token di accesso, i server di autorizzazione forniscono anche servizi amministrativi correlati, in genere tramite un'interfaccia utente Web. Ad esempio, è possibile definire e amministrare:

- Autenticazione degli utenti e degli utenti
- Ambiti
- Segregazione amministrativa attraverso locatari e regni
- Applicazione delle policy
- Collegamento a vari servizi esterni
- Supporto per altri protocolli di identità (come SAML)

ONTAP è compatibile con i server di autorizzazione conformi allo standard OAuth 2,0.

Definizione di ONTAP

È necessario definire uno o più server di autorizzazione in ONTAP. ONTAP comunica in modo sicuro con ciascun server per verificare i token ed eseguire altre attività correlate a supporto delle applicazioni client.

Di seguito sono illustrati gli aspetti principali della configurazione di ONTAP. Vedere anche "Scenari di distribuzione di OAuth 2,0" per ulteriori informazioni.

Come e dove vengono convalidati i token di accesso

Sono disponibili due opzioni per la convalida dei token di accesso.

- Convalida locale

  ONTAP può convalidare i token di accesso localmente in base alle informazioni fornite dal server di autorizzazione che ha emesso il token. Le informazioni recuperate dal server di autorizzazione vengono memorizzate nella cache da ONTAP e aggiornate a intervalli regolari.

- Introspezione remota

  È inoltre possibile utilizzare l'introspezione remota per convalidare i token nel server di autorizzazione. Introspezione è un protocollo che consente alle parti autorizzate di interrogare un server di autorizzazione su un token di accesso. Fornisce a ONTAP un modo per estrarre determinati metadati da un token di accesso e convalidare il token. ONTAP memorizza nella cache alcuni dati per motivi di prestazioni.

Posizione di rete

ONTAP potrebbe essere protetto da un firewall. In questo caso, è necessario identificare un proxy come parte della configurazione.

Come vengono definiti i server di autorizzazione

Puoi definire un server di autorizzazione per ONTAP utilizzando qualsiasi interfaccia amministrativa, inclusa

CLI, System Manager o API REST. Ad esempio, con l'interfaccia CLI si utilizza il comando `security oauth2 client create`.

Ulteriori informazioni su `security oauth2 client create` nella "Riferimento al comando ONTAP".

Numero di server di autorizzazione

È possibile definire fino a otto server di autorizzazione per un singolo cluster ONTAP. Lo stesso server di autorizzazione può essere definito più di una volta nello stesso cluster ONTAP, purché le attestazioni dell'emittente o dell'emittente/pubblico siano univoche. Per esempio, con Keycloak questo sarà sempre il caso quando si usano reami diversi.

Funzionalità OAuth 2,0 supportate in ONTAP

Il supporto per OAuth 2,0 era inizialmente disponibile con ONTAP 9.14,1 e continua ad essere migliorato con le versioni successive. Le funzioni di OAuth 2,0 supportate da ONTAP sono descritte di seguito.

Le funzionalità introdotte con una specifica release ONTAP sono riportate alle versioni future.

ONTAP 9.16.1

ONTAP 9.16,1 espande le funzionalità standard di OAuth 2,0 per includere estensioni specifiche di Entra ID per i gruppi di Entra ID nativi. Ciò implica l'utilizzo di GUID nel token di accesso anziché di nomi. Inoltre, la release aggiunge il supporto per la mappatura dei ruoli esterni per mappare i ruoli dei provider di identità nativi ai ruoli ONTAP utilizzando il campo "ruoli" nel token di accesso.

ONTAP 9.14.1

A partire da ONTAP 9.14,1, i server di autorizzazione sono supportati dalle seguenti funzionalità standard OAuth 2,0 per le applicazioni che utilizzano:

- OAuth 2,0 con i campi standard compresi "ISS", "aud" e "exp" come descritto in "RFC6749: Il framework di autorizzazione OAuth 2,0" e "RFC 7519: Token Web JSON (JWT)". Questo include anche il supporto per l'identificazione univoca degli utenti attraverso i campi nel token di accesso come "upn", "appid", "sub", "username" o "preferred_username".
- Estensioni specifiche del fornitore ADFS per i nomi dei gruppi con il campo "gruppo".
- Estensioni specifiche del fornitore di Azure per UUID gruppo con il campo "gruppo".
- Estensioni ONTAP per il supporto delle autorizzazioni che utilizzano ruoli autonomi e denominati nell'ambito del token di accesso OAuth 2,0. Sono inclusi i campi "Scope" e "SCP", nonché i nomi dei gruppi all'interno dell'ambito.

Utilizzo dei token di accesso OAuth 2,0

I token di accesso OAuth 2,0 emessi dai server di autorizzazione vengono verificati da ONTAP e utilizzati per prendere decisioni di accesso basate sui ruoli per le richieste dei client API REST.

Acquisizione di un token di accesso

È necessario acquisire un token di accesso da un server di autorizzazione definito nel cluster ONTAP in cui si utilizza l'API REST. Per acquisire un token, è necessario contattare direttamente il server di autorizzazione.

ONTAP non rilascia token di accesso o reindirizza le richieste dai client ai server di autorizzazione.

Il modo in cui si richiede un token dipende da diversi fattori, tra cui:

- Server di autorizzazione e relative opzioni di configurazione
- Tipo di concessione OAuth 2,0
- Client o strumento software utilizzato per emettere la richiesta

Tipi di sovvenzione

Un *grant* è un processo ben definito, che include un insieme di flussi di rete, utilizzato per richiedere e ricevere un token di accesso OAuth 2,0. A seconda dei requisiti del client, dell'ambiente e della protezione, è possibile utilizzare diversi tipi di concessione. Un elenco dei tipi di sovvenzione più comuni è presentato nella tabella seguente.

Tipo di concessione	Descrizione
Credenziali client	Tipo di concessione comune basato sull'utilizzo di credenziali (come ID e segreto condiviso). Si presuppone che il client abbia una stretta relazione di trust con il proprietario della risorsa.
Password	È possibile utilizzare il tipo di concessione delle credenziali della password del proprietario della risorsa nei casi in cui il proprietario della risorsa abbia una relazione di trust stabilita con il client. Può essere utile anche per la migrazione di client HTTP legacy a OAuth 2,0.
Codice di autorizzazione	Si tratta di un tipo di sovvenzione ideale per i client riservati e si basa su un flusso basato sul reindirizzamento. Può essere utilizzato per ottenere sia un token di accesso che un token di aggiornamento.

Contenuti JWT

Un token di accesso OAuth 2,0 è formattato come JWT. Il contenuto viene creato dal server di autorizzazione in base alla configurazione. Tuttavia, i token sono opachi per le applicazioni client. Un cliente non ha motivo di ispezionare un token o di essere a conoscenza del contenuto.

Ogni token di accesso JWT contiene una serie di attestazioni. Le attestazioni descrivono le caratteristiche dell'emittente e l'autorizzazione basata sulle definizioni amministrative del server di autorizzazione. Alcuni dei reclami registrati con la norma sono descritti nella tabella seguente. Tutte le stringhe rilevano la distinzione tra maiuscole e minuscole.

Reclamo	Parola chiave	Descrizione
Emittente	iss	Identifica l'entità che ha emesso il token. L'elaborazione della richiesta di rimborso è specifica per l'applicazione.
Soggetto	sub	L'oggetto o l'utente del token. Il nome è considerato univoco a livello globale o locale.
Pubblico	aud	I destinatari a cui è destinato il token. Implementato come array di stringhe.
Scadenza	scad	Il tempo dopo il quale il token scade e deve essere rifiutato.

Vedere "RFC 7519: Token Web JSON" per ulteriori informazioni.

Autorizzazione del client

Panoramica e opzioni per l'autorizzazione del client ONTAP

L'implementazione di ONTAP OAuth 2,0 è progettata per essere flessibile e robusta, fornendo le funzionalità necessarie per proteggere l'ambiente ONTAP. Sono disponibili diverse opzioni di configurazione che si escludono a vicenda. Le decisioni di autorizzazione si basano in ultima analisi sui ruoli REST ONTAP contenuti o derivati dai token di accesso OAuth 2,0.

È possibile utilizzare solo "Ruoli REST di ONTAP" Quando si configura l'autorizzazione per OAuth 2,0. I ruoli tradizionali ONTAP precedenti non sono supportati.

ONTAP applica l'opzione di autorizzazione singola più appropriata in base alla configurazione. Per ulteriori informazioni su come ONTAP prende le decisioni relative all'accesso dei client, vedere "Modalità con cui ONTAP determina l'accesso".

Oscilloscopi indipendenti OAuth 2,0

Questi ambiti contengono uno o più ruoli REST personalizzati, ciascuno incapsulato in una singola stringa nel token di accesso. Sono indipendenti dalle definizioni dei ruoli ONTAP. È necessario configurare le stringhe di ambito nel server di autorizzazione. Per ulteriori informazioni, vedere "Oscilloscopi OAuth 2,0 autonomi" .

Ruoli REST ONTAP locali

È possibile utilizzare un singolo ruolo REST denominato, incorporato o personalizzato. La sintassi dell'ambito per un ruolo denominato è **ontap-role-**<URL-encoded-ONTAP-role-name>. Ad esempio, se il ruolo ONTAP è `admin` la stringa Scope sarà `ontap-role-admin`.

Utenti

È possibile utilizzare il nome utente nel token di accesso definito con accesso all'applicazione "http". Un utente viene testato nel seguente ordine in base al metodo di autenticazione definito: Password, dominio (Active Directory), nsswitch (LDAP).

Gruppi

I server di autorizzazione possono essere configurati in modo da utilizzare i gruppi ONTAP per l'autorizzazione. Se vengono esaminate le definizioni ONTAP locali ma non è possibile prendere alcuna decisione di accesso, vengono utilizzati i gruppi Active Directory ("dominio") o LDAP ("nsswitch"). Le informazioni sul gruppo possono essere specificate in due modi:

- Stringa OAuth 2,0 Scope

  Supporta le applicazioni riservate utilizzando il flusso di credenziali client in cui non vi è alcun utente con appartenenza a un gruppo. L'ambito deve essere denominato **ontap-group-**<URL-encoded-ONTAP-group-name>. Ad esempio, se il gruppo è "sviluppo" la stringa dell'ambito sarà "ontap-group-development".

- Nella richiesta di "gruppo"

  Questa funzione è destinata ai token di accesso emessi da ADFS utilizzando il flusso proprietario della risorsa (concessione password).

Vedere "Lavorare con gruppi IdP OAuth 2.0 o SAML in ONTAP" per maggiori informazioni.

Ambiti OAuth 2.0 autonomi in ONTAP

Gli scope autonomi sono stringhe trasportate nel token di accesso. Ognuno di essi costituisce una definizione completa e personalizzata del ruolo e include tutto ciò che ONTAP ha bisogno per prendere una decisione di accesso. L'ambito è separato e distinto dai ruoli REST definiti all'interno di ONTAP stesso.

Formato della stringa Scope

A livello base, l'ambito è rappresentato come una stringa contigua e composta da sei valori separati da due punti. I parametri utilizzati nella stringa Scope sono descritti di seguito.

Letterale di ONTAP

L'ambito deve iniziare con il valore letterale `ontap` in minuscolo. Questo identifica l'ambito come specifico di ONTAP.

Cluster

Definisce il cluster ONTAP a cui si applica l'ambito. I valori possono includere:

- UUID cluster

  Identificazione di un singolo cluster.

- Asterisco (*)

  Indica che l'ambito si applica a tutti i cluster.

Puoi utilizzare il comando CLI di ONTAP `cluster identity show` per visualizzare l'UUID del cluster. Se non specificato, l'ambito si applica a tutti i cluster. Ulteriori informazioni su `cluster identity show` nella "Riferimento al comando ONTAP".

Ruolo

Il nome del ruolo di RIPOSO contenuto nell'ambito autonomo. Questo valore non viene esaminato da ONTAP o abbinato a ruoli REST esistenti definiti in ONTAP. Il nome viene utilizzato per la registrazione.

Livello di accesso

Questo valore indica il livello di accesso applicato all'applicazione client quando si utilizza l'endpoint API nell'ambito. Sono disponibili sei valori, come descritto nella tabella seguente.

Livello di accesso	Descrizione
nessuno	Nega tutti gli accessi all'endpoint specificato.
readonly	Consente solo l'accesso in lettura utilizzando GET.
read_create	Consente l'accesso in lettura e la creazione di nuove istanze di risorse utilizzando POST.
read_modify	Consente l'accesso in lettura e la possibilità di aggiornare le risorse esistenti utilizzando PATCH.

Livello di accesso	Descrizione
read_create_modify	Consente tutti gli accessi ad eccezione dell'eliminazione. Le operazioni consentite includono GET (lettura), POST (creazione) e PATCH (aggiornamento).
tutto	Consente l'accesso completo.

SVM

Nome della SVM all'interno del cluster a cui si applica l'ambito. Utilizzare il valore * (asterisco) per indicare tutte le SVM.

Questa funzione non è completamente supportata con ONTAP 9.14.1. È possibile ignorare il parametro SVM e utilizzare un asterisco come segnaposto. Esaminare "Note di rilascio di ONTAP" Per verificare il supporto SVM futuro.

URI API REST

Percorso completo o parziale di una risorsa o di una serie di risorse correlate. La stringa deve iniziare con `/api`. Se non si specifica un valore, l'ambito si applica a tutti gli endpoint API nel cluster ONTAP.

Esempi di ambito

Di seguito sono riportati alcuni esempi di ambiti auto-contenuti.

ontap:*:joes-role:read_create_modify:*:/api/cluster

Fornisce all'utente assegnato a questo ruolo l'accesso di lettura, creazione e modifica al `/cluster` endpoint.

Strumento di amministrazione CLI

Per rendere più semplice e meno incline agli errori l'amministrazione degli ambiti autonomi, ONTAP fornisce il comando CLI `security oauth2 scope` per generare stringhe di ambito in base ai parametri di input.

Il comando `security oauth2 scope` ha due casi d'utilizzo sulla base delle tue indicazioni:

- Parametri CLI per la stringa di ambito

  È possibile utilizzare questa versione del comando per generare una stringa di ambito in base ai parametri di input.

- Stringa di ambito per i parametri CLI

  È possibile utilizzare questa versione del comando per generare i parametri del comando in base alla stringa dell'ambito di input.

Esempio

Nell'esempio seguente viene generata una stringa di scope con l'output incluso dopo l'esempio di comando riportato di seguito. La definizione si applica a tutti i cluster.

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

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

Ulteriori informazioni su `security oauth2 scope` nella "Riferimento al comando ONTAP".

Mapping dei ruoli esterni OAuth 2.0 in ONTAP

Un ruolo esterno viene definito in un provider di identificazione configurato per l'utilizzo da parte di ONTAP. È possibile creare e amministrare relazioni di mappatura tra questi ruoli esterni e i ruoli ONTAP utilizzando l'interfaccia CLI di ONTAP.

È inoltre possibile configurare la funzione di mapping dei ruoli esterni utilizzando l'API REST di ONTAP. Per ulteriori informazioni, vedere "Documentazione sull'automazione di ONTAP" .

Ruoli esterni in un token di accesso

Ecco un frammento di un token di accesso JSON contenente due ruoli esterni.

```
...
"appidacr": "1",
"family_name": "User",
"name": "Test User 1",
"oid": "4c2215c7-6d52-40a7-ce71-096fa41379ba",
"roles": [
  "Global Administrator",
  "Application Administrator"
],
"ver": "1.0",
...
```

Configurazione

È possibile utilizzare l'interfaccia della riga di comando di ONTAP per amministrare la funzione di mappatura dei ruoli esterna.

Creare

È possibile definire una configurazione di mappatura dei ruoli con il `security login external-role-mapping create` comando. Per eseguire questo comando e le relative opzioni, è necessario essere al livello di privilegio **admin** di ONTAP.

Parametri

I parametri utilizzati per creare una mappatura di gruppo sono descritti di seguito.

Parametro	Descrizione
`external-role`	Il nome del ruolo definito nel provider di identità esterno.
`provider`	Il nome del provider di identità. Questo deve essere l'identificatore del sistema.
`ontap-role`	Indica il ruolo ONTAP esistente a cui è mappato il ruolo esterno.

Esempio

```
security login external-role-mapping create -external-role "Global
Administrator" -provider entra -ontap-role admin
```

Ulteriori informazioni su `security login external-role-mapping create` nella "Riferimento al comando ONTAP".

Operazioni CLI aggiuntive

Il comando supporta diverse operazioni aggiuntive, tra cui:

- Mostra
- Modificare
- Eliminare

Informazioni correlate

- "Riferimento al comando ONTAP"

Modalità con cui ONTAP determina l'accesso dei client

Per progettare e implementare correttamente OAuth 2,0, è necessario comprendere in che modo la configurazione delle autorizzazioni viene utilizzata da ONTAP per prendere decisioni di accesso per i client. I passaggi principali utilizzati per determinare l'accesso sono presentati di seguito in base alla versione ONTAP.

Non sono stati effettuati aggiornamenti significativi di OAuth 2,0 con ONTAP 9.15,1. Se si utilizza la versione 9.15.1, fare riferimento alla descrizione di ONTAP 9.14,1.

Informazioni correlate

- "Funzionalità OAuth 2,0 supportate in ONTAP"

ONTAP 9.16.1

ONTAP 9.16,1 espande il supporto standard OAuth 2,0 per includere estensioni specifiche di Microsoft Entra ID per i gruppi Entra ID nativi e la mappatura di ruoli esterni.

Determinare l'accesso client per ONTAP 9.16,1

Fase 1: Oscilloscopi autonomi

Se il token di accesso contiene ambiti indipendenti, ONTAP esamina prima questi ambiti. Se non sono presenti oscilloscopi autonomi, passare al punto 2.

Con uno o più ambiti auto-contenuti presenti, ONTAP applica ogni ambito fino a quando non può essere presa una decisione esplicita **ALLOW** o **DENY**. Se viene presa una decisione esplicita, l'elaborazione termina.

Se ONTAP non è in grado di prendere una decisione di accesso esplicita, continuare con il passaggio 2.

Passaggio 2: Controllare il flag dei ruoli locali

ONTAP esamina il parametro booleano `use-local-roles-if-present` . Il valore di questo indicatore viene impostato separatamente per ogni server di autorizzazione definito su ONTAP.

- Se il valore è `true` passare alla fase 3.
- Se il valore è `false` l'elaborazione termina e l'accesso è negato.

Passaggio 3: Ruolo REST di Named ONTAP

Se il token di accesso contiene un ruolo REST denominato nel `scope` campo o `scp`, o come attestazione, ONTAP utilizza il ruolo per prendere la decisione di accesso. Ciò comporta sempre una decisione **ALLOW** o **DENY** e l'elaborazione termina.

Se non è presente alcun ruolo REST denominato o se il ruolo non è stato trovato, passare al punto 4.

Fase 4: Utenti

Estrarre il nome utente dal token di accesso e tentare di associarlo agli utenti che hanno accesso all'applicazione "http". Gli utenti vengono esaminati in base al metodo di autenticazione nel seguente ordine:

- password
- Dominio (Active Directory)
- Nsswitch (LDAP)

Se viene trovato un utente corrispondente, ONTAP utilizza il ruolo definito per l'utente per prendere una decisione di accesso. Ciò comporta sempre una decisione **ALLOW** o **DENY** e l'elaborazione termina.

Se un utente non corrisponde o se non è presente alcun nome utente nel token di accesso, passare al punto 5.

Fase 5: Gruppi

Se sono inclusi uno o più gruppi, il formato viene esaminato. Se i gruppi sono rappresentati come UUID, viene eseguita una ricerca in una tabella di mappatura dei gruppi interna. Se esiste una corrispondenza di gruppo e un ruolo associato, ONTAP utilizza il ruolo definito per il gruppo per prendere una decisione di accesso. Ciò comporta sempre una decisione **CONSENTI** o **NEGGIA** e l'elaborazione termina. Per ulteriori informazioni, consultare "Lavorare con gruppi IdP OAuth 2.0 o SAML in ONTAP" .

Se i gruppi sono rappresentati come nomi e configurati con autorizzazione dominio o nsswitch, ONTAP tenta di associarli rispettivamente a un gruppo Active Directory o LDAP. Se esiste una corrispondenza di gruppo, ONTAP utilizza il ruolo definito per il gruppo per prendere una decisione di accesso. Ciò comporta sempre una decisione **ALLOW** o **DENY** e l'elaborazione termina.

Se non è presente alcuna corrispondenza di gruppo o se non è presente alcun gruppo nel token di accesso, l'accesso viene negato e l'elaborazione termina.

ONTAP 9.14.1

OAuth 2,0 iniziale supportato viene introdotto con ONTAP 9.14,1 in base alle funzionalità standard di OAuth 2,0.

Determinare l’accesso client per ONTAP 9.14,1

Fase 1: Oscilloscopi autonomi

Se il token di accesso contiene ambiti indipendenti, ONTAP esamina prima questi ambiti. Se non sono presenti oscilloscopi autonomi, passare al punto 2.

Con uno o più ambiti auto-contenuti presenti, ONTAP applica ogni ambito fino a quando non può essere presa una decisione esplicita **ALLOW** o **DENY**. Se viene presa una decisione esplicita, l’elaborazione termina.

Se ONTAP non è in grado di prendere una decisione di accesso esplicita, continuare con il passaggio 2.

Passaggio 2: Controllare il flag dei ruoli locali

ONTAP esamina il parametro booleano `use-local-roles-if-present` . Il valore di questo indicatore viene impostato separatamente per ogni server di autorizzazione definito su ONTAP.

- Se il valore è `true` passare alla fase 3.
- Se il valore è `false` l’elaborazione termina e l’accesso è negato.

Passaggio 3: Ruolo REST di Named ONTAP

Se il token di accesso contiene un ruolo REST denominato nel `scope` campo o `scp` , ONTAP utilizza il ruolo per prendere la decisione di accesso. Ciò comporta sempre una decisione **ALLOW** o **DENY** e l’elaborazione termina.

Se non è presente alcun ruolo REST denominato o se il ruolo non è stato trovato, passare al punto 4.

Fase 4: Utenti

Estrarre il nome utente dal token di accesso e tentare di associarlo agli utenti che hanno accesso all’applicazione "http". Gli utenti vengono esaminati in base al metodo di autenticazione nel seguente ordine:

- password
- Dominio (Active Directory)
- Nsswitch (LDAP)

Se viene trovato un utente corrispondente, ONTAP utilizza il ruolo definito per l’utente per prendere una decisione di accesso. Ciò comporta sempre una decisione **ALLOW** o **DENY** e l’elaborazione termina.

Se un utente non corrisponde o se non è presente alcun nome utente nel token di accesso, passare al punto 5.

Fase 5: Gruppi

Se uno o più gruppi sono inclusi e configurati con autorizzazione dominio o nsswitch, ONTAP tenta di associarli rispettivamente a un gruppo Active Directory o LDAP.

Se esiste una corrispondenza di gruppo, ONTAP utilizza il ruolo definito per il gruppo per prendere una decisione di accesso. Ciò comporta sempre una decisione **ALLOW** o **DENY** e l’elaborazione termina.

Se non è presente alcuna corrispondenza di gruppo o se non è presente alcun gruppo nel token di accesso, l’accesso viene negato e l’elaborazione termina.

Scenari di distribuzione OAuth 2.0 con ONTAP

Quando si definisce un server di autorizzazione per ONTAP, sono disponibili diverse opzioni di configurazione. In base a queste opzioni, è possibile definire un server di autorizzazione appropriato per l'ambiente in uso utilizzando uno dei diversi scenari di distribuzione.

Riepilogo dei parametri di configurazione

Quando si definisce un server di autorizzazione per ONTAP, sono disponibili diversi parametri di configurazione. Questi parametri sono generalmente supportati in tutte le interfacce amministrative.

> Il nome utilizzato per un singolo parametro o campo può variare a seconda dell'interfaccia amministrativa di ONTAP. Per adattarsi alle differenze nelle interfacce amministrative, viene utilizzato un unico nome generico per ciascun parametro della tabella. Il nome esatto utilizzato con un'interfaccia specifica dovrebbe essere ovvio in base al contesto.

Parametro	Descrizione
Nome	Il nome del server di autorizzazione così come è noto a ONTAP.
Applicazione	L'applicazione interna ONTAP a cui si applica la definizione. Deve essere **http**.
URI emittente	FQDN con percorso che identifica il sito o l'organizzazione che emette i token.
Provider JWKS URI	L'FQDN con percorso e nome file in cui ONTAP ottiene i set di chiavi Web JSON utilizzati per convalidare i token di accesso.
Intervallo di aggiornamento JWKS	L'intervallo di tempo che determina la frequenza con cui ONTAP aggiorna le informazioni del certificato dall'URI JWKS del provider. Il valore è specificato in formato ISO-8601.
Endpoint introspezione	L'FQDN con percorso utilizzato da ONTAP per eseguire la convalida dei token remoti tramite introspezione.
ID client	Il nome del client come definito nel server di autorizzazione. Quando questo valore è incluso, è necessario anche fornire il segreto client associato in base all'interfaccia.
Proxy in uscita	In questo modo viene fornito l'accesso al server di autorizzazione quando ONTAP è protetto da un firewall. L'URI deve essere in formato Curl.
Utilizzare i ruoli locali, se presenti	Un flag booleano che determina se vengono utilizzate le definizioni ONTAP locali, inclusi un ruolo REST denominato e gli utenti locali.
Richiesta di rimborso per utenti remoti	Un nome alternativo utilizzato da ONTAP per associare gli utenti locali. Utilizzare `sub` nel token di accesso in modo che corrisponda al nome utente locale.
Pubblico	Questo campo definisce gli endpoint in cui è possibile utilizzare il token di accesso.

Scenari di distribuzione

Di seguito vengono presentati diversi scenari di distribuzione comuni. Sono organizzati in base al fatto che la convalida dei token venga eseguita localmente da ONTAP o in remoto dal server di autorizzazione. Ogni scenario include un elenco delle opzioni di configurazione richieste. Vedere "Implementa OAuth 2,0 in ONTAP" per esempi dei comandi di configurazione.

Dopo aver definito un server di autorizzazione, è possibile visualizzarne la configurazione tramite l'interfaccia amministrativa di ONTAP. Ad esempio, utilizzare il comando `security oauth2 client show` Con l'interfaccia a riga di comando di ONTAP.

Convalida locale

I seguenti scenari di distribuzione si basano su ONTAP che esegue la convalida dei token localmente.

Utilizzare gli oscilloscopi autonomi senza proxy

Questa è l'implementazione più semplice che utilizza solo gli oscilloscopi indipendenti OAuth 2,0. Nessuna delle definizioni di identità ONTAP locali viene utilizzata. È necessario includere i seguenti parametri:

- Nome
- Applicazione (http)
- Provider JWKS URI
- URI emittente

È inoltre necessario aggiungere gli ambiti al server di autorizzazione.

Utilizzare gli oscilloscopi autonomi con un proxy

Questo scenario di distribuzione utilizza gli oscilloscopi indipendenti OAuth 2,0. Nessuna delle definizioni di identità ONTAP locali viene utilizzata. Ma il server di autorizzazione è protetto da un firewall e quindi è necessario configurare un proxy. È necessario includere i seguenti parametri:

- Nome
- Applicazione (http)
- Provider JWKS URI
- Proxy in uscita
- URI emittente
- Pubblico

È inoltre necessario aggiungere gli ambiti al server di autorizzazione.

Utilizzare ruoli utente locali e associazione nome utente predefinita con un proxy

Questo scenario di distribuzione utilizza ruoli utente locali con mappatura dei nomi predefinita. La richiesta di rimborso dell'utente remoto utilizza il valore predefinito di `sub` quindi questo campo nel token di accesso viene utilizzato per corrispondere al nome utente locale. Il nome utente deve contenere al massimo 40 caratteri. Il server di autorizzazione è protetto da un firewall, quindi è necessario configurare anche un proxy. È necessario includere i seguenti parametri:

- Nome
- Applicazione (http)
- Provider JWKS URI
- Utilizzare i ruoli locali, se presenti (`true`)
- Proxy in uscita
- Emittente

È necessario assicurarsi che l'utente locale sia definito su ONTAP.

Utilizzare ruoli utente locali e mapping nome utente alternativo con un proxy

Questo scenario di distribuzione utilizza ruoli utente locali con un nome utente alternativo utilizzato per associare un utente ONTAP locale. Il server di autorizzazione è protetto da un firewall, quindi è necessario configurare un proxy. È necessario includere i seguenti parametri:

- Nome
- Applicazione (http)
- Provider JWKS URI
- Utilizzare i ruoli locali, se presenti (`true`)
- Richiesta di rimborso per utenti remoti
- Proxy in uscita
- URI emittente
- Pubblico

È necessario assicurarsi che l'utente locale sia definito su ONTAP.

Introspezione remota

Le seguenti configurazioni di distribuzione si basano su ONTAP che esegue la convalida dei token in modalità remota tramite introspezione.

Utilizzare gli oscilloscopi autonomi senza proxy

Si tratta di una semplice implementazione basata sull'utilizzo degli oscilloscopi indipendenti OAuth 2,0. Nessuna delle definizioni di identità ONTAP viene utilizzata. È necessario includere i seguenti parametri:

- Nome
- Applicazione (http)
- Endpoint introspezione
- ID client
- URI emittente

È necessario definire gli ambiti, nonché il segreto client e client nel server di autorizzazione.

Informazioni correlate

- "spettacolo client oauth2 di sicurezza"

Autenticazione client ONTAP tramite OAuth 2.0 Mutual TLS

A seconda delle esigenze di protezione, è possibile configurare il protocollo mTLS (Mutual TLS) per implementare l'autenticazione client avanzata. Quando viene utilizzato con ONTAP come parte di una distribuzione OAuth 2,0, mTLS garantisce che i token di accesso vengano utilizzati solo dai client ai quali sono stati originariamente emessi.

TLS reciproco con OAuth 2,0

Transport Layer Security (TLS) viene utilizzato per stabilire un canale di comunicazione sicuro tra due applicazioni, in genere un browser client e un server Web. Il TLS reciproco estende questa funzione fornendo una solida identificazione del client tramite un certificato client. Quando viene utilizzata in un cluster ONTAP con OAuth 2,0, la funzionalità mTLS di base viene estesa creando e utilizzando token di accesso con vincoli di mittente.

Un token di accesso vincolato dal mittente può essere utilizzato solo dal client al quale è stato originariamente emesso. Per supportare questa funzione, è necessario presentare una nuova richiesta di conferma (`cnf`) è inserito nel token. Il campo contiene proprietà `x5t#S256` che contiene un digest del certificato client utilizzato quando si richiede il token di accesso. Questo valore viene verificato da ONTAP come parte della convalida del token. I token di accesso emessi dai server di autorizzazione che non sono vincolati dal mittente non includono la richiesta di conferma aggiuntiva.

È necessario configurare ONTAP in modo che utilizzi mTLS separatamente per ogni server di autorizzazione. Ad esempio, il comando CLI `security oauth2 client` include il parametro `use-mutual-tls` Per controllare l'elaborazione mTLS in base a tre valori, come mostrato nella tabella seguente.

In ogni configurazione, il risultato e l'azione intrapresi da ONTAP dipendono dal valore del parametro di configurazione, dal contenuto del token di accesso e dal certificato client. I parametri nella tabella sono organizzati dal minimo al più restrittivo.

Parametro	Descrizione
nessuno	L'autenticazione TLS reciproca OAuth 2,0 è completamente disattivata per il server di autorizzazione. ONTAP non eseguirà l'autenticazione del certificato client mTLS anche se la richiesta di conferma è presente nel token o se viene fornito un certificato client con la connessione TLS.
richiesta	L'autenticazione reciproca TLS OAuth 2,0 viene applicata se il client presenta un token di accesso con restrizioni del mittente. Vale a dire, mTLS viene applicato solo se la richiesta di conferma (con proprietà `x5t#S256`) è presente nel token di accesso. Questa è l'impostazione predefinita.
obbligatorio	L'autenticazione TLS reciproca OAuth 2,0 viene applicata per tutti i token di accesso emessi dal server di autorizzazione. Pertanto, tutti i token di accesso devono essere vincolati dal mittente. L'autenticazione e la richiesta dell'API REST non riescono se la richiesta di conferma non è presente nel token di accesso o se è presente un certificato client non valido.

Flusso di implementazione di alto livello

Di seguito vengono illustrati i passaggi tipici richiesti quando si utilizza mTLS con OAuth 2,0 in un ambiente ONTAP. Vedere "RFC 8705: Autenticazione client OAuth 2,0 Mutual-TLS e token di accesso con associazione a certificati" per ulteriori dettagli.

Passaggio 1: Creare e installare un certificato client

La definizione dell'identità del client si basa sulla prova della conoscenza di una chiave privata del client. La chiave pubblica corrispondente viene inserita in un certificato X,509 firmato presentato dal cliente. A un livello elevato, i passaggi necessari per la creazione del certificato client includono:

1. Generare una coppia di chiavi pubbliche e private
2. Creare una richiesta di firma del certificato

3. Inviare il file CSR a una CA nota
4. CA verifica la richiesta ed emette il certificato firmato

In genere è possibile installare il certificato client nel sistema operativo locale o utilizzarlo direttamente con un'utilità comune, ad esempio curl.

Passaggio 2: Configurare ONTAP per l'utilizzo di mTLS

È necessario configurare ONTAP per utilizzare mTLS. Questa configurazione viene eseguita separatamente per ogni server di autorizzazione. Ad esempio, con il CLI il comando `security oauth2 client` viene utilizzato con il parametro opzionale `use-mutual-tls`. Vedere "Implementa OAuth 2,0 in ONTAP" per ulteriori informazioni.

Passaggio 3: Il client richiede un token di accesso

Il client deve richiedere un token di accesso dal server di autorizzazione configurato su ONTAP. L'applicazione client deve utilizzare mTLS con il certificato creato e installato nel passaggio 1.

Passaggio 4: Il server di autorizzazione genera il token di accesso

Il server di autorizzazione verifica la richiesta del client e genera un token di accesso. Come parte di ciò, crea un riepilogo del messaggio del certificato client che è incluso nel token come richiesta di conferma (campo `cnf`).

Passaggio 5: L'applicazione client presenta il token di accesso a ONTAP

L'applicazione client effettua una chiamata API REST al cluster ONTAP e include il token di accesso nell'intestazione della richiesta di autorizzazione come token **bearer**. Il client deve utilizzare mTLS con lo stesso certificato utilizzato per richiedere il token di accesso.

Passaggio 6: ONTAP verifica client e token.

ONTAP riceve il token di accesso in una richiesta HTTP e il certificato client utilizzato come parte dell'elaborazione mTLS. ONTAP prima convalida la firma nel token di accesso. In base alla configurazione, ONTAP genera un riepilogo dei messaggi del certificato client e lo confronta con l'attestazione di conferma **cnf** nel token. Se i due valori corrispondono, ONTAP ha confermato che il client che effettua la richiesta API è lo stesso client a cui è stato originariamente emesso il token di accesso.

Informazioni correlate

- "client di sicurezza oauth2"

Configurazione e implementazione

Preparati a implementare OAuth 2,0 con ONTAP

Prima di configurare OAuth 2,0 in un ambiente ONTAP, è necessario prepararsi per la distribuzione. Di seguito è riportato un riepilogo delle principali attività e decisioni. La disposizione delle sezioni è generalmente allineata con l'ordine da seguire. Tuttavia, sebbene sia applicabile per la maggior parte delle implementazioni, è consigliabile adattarlo all'ambiente in base alle esigenze. È inoltre opportuno prendere in considerazione la creazione di un piano di distribuzione formale.

In base all'ambiente in uso, è possibile selezionare la configurazione per i server di autorizzazione definiti in ONTAP. Sono inclusi i valori dei parametri da specificare per ogni tipo di distribuzione. Vedere "Scenari di distribuzione di OAuth 2,0" per ulteriori informazioni.

Risorse protette e applicazioni client

OAuth 2,0 è un framework di autorizzazione per controllare l'accesso alle risorse protette. In questo caso, un primo passo importante per qualsiasi distribuzione consiste nel determinare quali sono le risorse disponibili e quali client devono accedervi.

Identificare le applicazioni client

È necessario decidere quali client utilizzeranno OAuth 2,0 per l'emissione di chiamate API REST e a quali endpoint API devono accedere.

Esaminare i ruoli REST ONTAP esistenti e gli utenti locali

È necessario esaminare le definizioni di identità ONTAP esistenti, inclusi i ruoli REST e gli utenti locali. A seconda della configurazione di OAuth 2,0, queste definizioni possono essere utilizzate per prendere decisioni sugli accessi.

Transizione globale a OAuth 2,0

Sebbene sia possibile implementare l'autorizzazione OAuth 2,0 gradualmente, è anche possibile spostare immediatamente tutti i client API REST in OAuth 2,0 impostando un flag globale per ogni server di autorizzazione. In questo modo, è possibile prendere decisioni di accesso in base alla configurazione ONTAP esistente senza dover creare ambiti autonomi.

Server di autorizzazione

I server di autorizzazione svolgono un ruolo importante nella distribuzione di OAuth 2,0 rilasciando token di accesso e applicando criteri amministrativi.

Selezionare e installare il server di autorizzazione

È necessario selezionare e installare uno o più server di autorizzazione. È importante acquisire familiarità con le opzioni di configurazione e le procedure dei provider di identità, incluse le modalità di definizione degli ambiti. Si noti che alcuni server di autorizzazione, incluso Microsoft Entra ID, rappresentano gruppi che utilizzano UUID anziché nomi.

Determinare se è necessario installare il certificato CA principale di autorizzazione

ONTAP utilizza il certificato del server di autorizzazione per convalidare i token di accesso firmati presentati dai client. A tale scopo, ONTAP necessita del certificato della CA principale e di eventuali certificati intermedi. Questi potrebbero essere preinstallati con ONTAP. In caso contrario, è necessario installarli.

Valutare la posizione e la configurazione della rete

Se il server di autorizzazione è protetto da un firewall, ONTAP deve essere configurato per utilizzare un server proxy.

Autenticazione e autorizzazione del client

È necessario prendere in considerazione diversi aspetti dell'autenticazione e dell'autorizzazione dei client.

Ambiti indipendenti o definizioni di identità ONTAP locali

A un livello elevato, è possibile definire ambiti indipendenti definiti nel server di autorizzazione o fare affidamento sulle definizioni di identità ONTAP locali esistenti, inclusi ruoli e utenti.

Opzioni con elaborazione ONTAP locale

Se si utilizzano le definizioni di identità ONTAP, è necessario decidere quale applicare, tra cui:

- Ruolo REST denominato

- Far corrispondere gli utenti locali
- Active Directory o gruppi LDAP

Convalida locale o introspezione remota

È necessario decidere se i token di accesso verranno convalidati localmente da ONTAP o dal server di autorizzazione tramite introspezione. Ci sono anche diversi valori correlati da prendere in considerazione, come l'intervallo di aggiornamento.

Token di accesso con restrizioni del mittente

Per gli ambienti che richiedono un alto livello di protezione, è possibile utilizzare token di accesso con limitazioni di invio basati su mTLS. Questo richiede un certificato per ciascun client.

Gruppi come UUID e mappatura identità

Se si utilizza un server di autorizzazione che rappresenta gruppi che utilizzano UUID, è necessario pianificare come associarli ai nomi dei gruppi ed eventualmente ai ruoli associati.

Interfaccia amministrativa

È possibile eseguire l'amministrazione di OAuth 2,0 tramite una qualsiasi delle interfacce ONTAP, tra cui:

- Interfaccia della riga di comando
- System Manager
- API REST

Modalità con cui i client richiedono i token di accesso

Le applicazioni client devono richiedere i token di accesso direttamente dal server di autorizzazione. È necessario decidere in che modo eseguire questa operazione, incluso il tipo di concessione.

Configure ONTAP (Configura SNMP)

È necessario eseguire diverse attività di configurazione di ONTAP.

Definire i ruoli REST e gli utenti locali

In base alla configurazione dell'autorizzazione, è possibile utilizzare l'elaborazione dell'identificazione ONTAP locale. In questo caso, è necessario rivedere e definire i ruoli REST e le definizioni utente. A seconda del server di autorizzazione, questo può includere anche l'amministrazione dei gruppi in base ai valori UUID.

Configurazione di base

Per eseguire la configurazione di base di ONTAP sono necessari tre passaggi principali, tra cui:

- Se si desidera, installare il certificato di origine (e qualsiasi certificato intermedio) per la CA che ha firmato il certificato del server di autorizzazione.
- Definire il server di autorizzazione.
- Abilitare l'elaborazione OAuth 2,0 per il cluster.

Implementa OAuth 2,0 in ONTAP

L'implementazione della funzionalità principale di OAuth 2,0 richiede tre fasi principali.

Prima di iniziare

È necessario prepararsi per la distribuzione di OAuth 2,0 prima di configurare ONTAP. Ad esempio, è necessario valutare il server di autorizzazione, incluso il modo in cui il certificato è stato firmato e se è protetto da un firewall. Vedere "Preparati a implementare OAuth 2,0 con ONTAP" per ulteriori informazioni.

Passo 1: Installazione dei certificati CA principali del server di autorizzazione

ONTAP include un gran numero di certificati CA principali preinstallati. Pertanto, in molti casi, il certificato per il server di autorizzazione verrà immediatamente riconosciuto da ONTAP senza ulteriori configurazioni. Tuttavia, a seconda di come è stato firmato il certificato del server di autorizzazione, potrebbe essere necessario installare un certificato della CA principale e qualsiasi certificato intermedio.

Seguire le istruzioni fornite di seguito per installare il certificato, se necessario. È necessario installare tutti i certificati richiesti a livello di cluster.

Scegliere la procedura corretta in base alla modalità di accesso a ONTAP.

Esempio 1. Fasi

System Manager

1. In System Manager, selezionare **Cluster** > **Impostazioni**.
2. Scorrere fino alla sezione **protezione**.
3. Fare clic su → accanto a **certificati**.
4. Nella scheda **autorità di certificazione attendibili** fare clic su **Aggiungi**.
5. Fare clic su **Importa** e selezionare il file del certificato.
6. Completare i parametri di configurazione dell'ambiente.
7. Fare clic su **Aggiungi**.

CLI

1. Avviare l'installazione:

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

2. Cercare il seguente messaggio della console:

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

3. Aprire il file del certificato con un editor di testo.
4. Copiare l'intero certificato, incluse le seguenti righe:

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

5. Incollare il certificato nel terminale dopo il prompt dei comandi.
6. Premere **Invio** per completare l'installazione.
7. Verificare che il certificato sia installato utilizzando una delle seguenti opzioni:

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

   ```
   security certificate show
   ```

Passaggio 2: Configurare il server di autorizzazione

È necessario definire almeno un server di autorizzazione per ONTAP. È necessario scegliere i valori dei parametri in base alla configurazione e al piano di distribuzione. Revisione "OAuth2 scenari di distribuzione" per determinare i parametri esatti necessari per la configurazione.

Per modificare la definizione di un server di autorizzazione, è possibile eliminare la definizione esistente e crearne una nuova.

L'esempio fornito di seguito si basa sul primo semplice scenario di distribuzione all'indirizzo "Convalida locale".

Gli oscilloscopi autonomi vengono utilizzati senza proxy.

Scegliere la procedura corretta in base alla modalità di accesso a ONTAP. La procedura CLI utilizza variabili simboliche che è necessario sostituire prima di eseguire il comando.

Esempio 2. Fasi

System Manager

1. In System Manager, selezionare **Cluster** > **Impostazioni**.
2. Scorrere fino alla sezione **protezione**.
3. Fare clic su **+** accanto a **autorizzazione OAuth 2,0**.
4. Selezionare **altre opzioni**.
5. Fornire i valori richiesti per la distribuzione, ad esempio:
   - Nome
   - Applicazione (http)
   - Provider JWKS URI
   - URI emittente
6. Fare clic su **Aggiungi**.

CLI

1. Creare nuovamente la definizione:

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

   Ad esempio:

   ```
   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
   ```

   Ulteriori informazioni su `security oauth2 client create` nella "Riferimento al comando ONTAP".

Fase 3: Abilitare OAuth 2,0

Il passaggio finale consiste nell'abilitare OAuth 2,0. Si tratta di un'impostazione globale per il cluster ONTAP.

> Non attivare l'elaborazione OAuth 2,0 finché non si conferma che ONTAP, i server di autorizzazione e gli eventuali servizi di supporto sono stati configurati correttamente.

Scegliere la procedura corretta in base alla modalità di accesso a ONTAP.

Esempio 3. Fasi

System Manager

1. In System Manager, selezionare **Cluster** > **Impostazioni**.
2. Scorrere fino alla sezione **protezione**.
3. Fare clic su → accanto a **autorizzazione OAuth 2,0**.
4. Abilita **autorizzazione OAuth 2,0**.

CLI

1. Abilita OAuth 2,0:

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

2. Confermare che OAuth 2,0 sia abilitato:

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

Informazioni correlate

- "installazione del certificato di sicurezza"
- "mostra certificato di sicurezza"
- "modifica sicurezza oauth2"
- "sicurezza oauth2 mostra"

Emettere una chiamata API REST ONTAP utilizzando OAuth 2.0

L'implementazione di OAuth 2,0 in ONTAP supporta le applicazioni client API REST. È possibile eseguire una semplice chiamata API REST utilizzando curl per iniziare a utilizzare OAuth 2,0. L'esempio presentato di seguito recupera la versione del cluster ONTAP.

Prima di iniziare

È necessario configurare e abilitare la funzione OAuth 2,0 per il cluster ONTAP. Ciò include la definizione di un server di autorizzazione.

Fase 1: Acquisire un token di accesso

È necessario acquisire un token di accesso da utilizzare con la chiamata API REST. La richiesta token viene eseguita al di fuori di ONTAP e la procedura esatta dipende dal server di autorizzazione e dalla relativa configurazione. È possibile richiedere il token tramite un browser Web, con un comando curl o utilizzando un linguaggio di programmazione.

A scopo illustrativo, di seguito viene presentato un esempio di come un token di accesso può essere richiesto

da Keycloak usando curl.

Esempio Keycloak

```
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'
```

Copiare e salvare il token restituito.

Passaggio 2: Eseguire la chiamata API REST

Dopo avere un token di accesso valido, è possibile utilizzare un comando curl con il token di accesso per eseguire una chiamata API REST.

Parametri e variabili

Le due variabili nell'esempio dell'arricciatura sono descritte nella tabella seguente.

Variabile	Descrizione
$FQDN_IP	Il nome di dominio o l'indirizzo IP pienamente qualificato della LIF di gestione ONTAP.
$ACCESS_TOKEN	Token di accesso OAuth 2,0 emesso dal server di autorizzazione.

Prima di eseguire l'esempio Curl, è necessario impostare queste variabili nell'ambiente della shell Bash. Ad esempio, nella CLI di Linux digitare il seguente comando per impostare e visualizzare la variabile FQDN:

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

Dopo aver definito entrambe le variabili nella shell Bash locale, è possibile copiare il comando curl e incollarlo nella CLI. Premere **Invio** per sostituire le variabili ed eseguire il comando.

Esempio di arricciamento

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

Informazioni sul copyright

Copyright © 2026 NetApp, Inc. Tutti i diritti riservati. Stampato negli Stati Uniti d'America. Nessuna porzione di questo documento soggetta a copyright può essere riprodotta in qualsiasi formato o mezzo (grafico, elettronico o meccanico, inclusi fotocopie, registrazione, nastri o storage in un sistema elettronico) senza previo consenso scritto da parte del detentore del copyright.

Il software derivato dal materiale sottoposto a copyright di NetApp è soggetto alla seguente licenza e dichiarazione di non responsabilità:

IL PRESENTE SOFTWARE VIENE FORNITO DA NETAPP "COSÌ COM'È" E SENZA QUALSIVOGLIA TIPO DI GARANZIA IMPLICITA O ESPRESSA FRA CUI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, GARANZIE IMPLICITE DI COMMERCIABILITÀ E IDONEITÀ PER UNO SCOPO SPECIFICO, CHE VENGONO DECLINATE DAL PRESENTE DOCUMENTO. NETAPP NON VERRÀ CONSIDERATA RESPONSABILE IN ALCUN CASO PER QUALSIVOGLIA DANNO DIRETTO, INDIRETTO, ACCIDENTALE, SPECIALE, ESEMPLARE E CONSEQUENZIALE (COMPRESI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, PROCUREMENT O SOSTITUZIONE DI MERCI O SERVIZI, IMPOSSIBILITÀ DI UTILIZZO O PERDITA DI DATI O PROFITTI OPPURE INTERRUZIONE DELL'ATTIVITÀ AZIENDALE) CAUSATO IN QUALSIVOGLIA MODO O IN RELAZIONE A QUALUNQUE TEORIA DI RESPONSABILITÀ, SIA ESSA CONTRATTUALE, RIGOROSA O DOVUTA A INSOLVENZA (COMPRESA LA NEGLIGENZA O ALTRO) INSORTA IN QUALSIASI MODO ATTRAVERSO L'UTILIZZO DEL PRESENTE SOFTWARE ANCHE IN PRESENZA DI UN PREAVVISO CIRCA L'EVENTUALITÀ DI QUESTO TIPO DI DANNI.

NetApp si riserva il diritto di modificare in qualsiasi momento qualunque prodotto descritto nel presente documento senza fornire alcun preavviso. NetApp non si assume alcuna responsabilità circa l'utilizzo dei prodotti o materiali descritti nel presente documento, con l'eccezione di quanto concordato espressamente e per iscritto da NetApp. L'utilizzo o l'acquisto del presente prodotto non comporta il rilascio di una licenza nell'ambito di un qualche diritto di brevetto, marchio commerciale o altro diritto di proprietà intellettuale di NetApp.

Il prodotto descritto in questa guida può essere protetto da uno o più brevetti degli Stati Uniti, esteri o in attesa di approvazione.

LEGENDA PER I DIRITTI SOTTOPOSTI A LIMITAZIONE: l'utilizzo, la duplicazione o la divulgazione da parte degli enti governativi sono soggetti alle limitazioni indicate nel sottoparagrafo (b)(3) della clausola Rights in Technical Data and Computer Software del DFARS 252.227-7013 (FEB 2014) e FAR 52.227-19 (DIC 2007).

I dati contenuti nel presente documento riguardano un articolo commerciale (secondo la definizione data in FAR 2.101) e sono di proprietà di NetApp, Inc. Tutti i dati tecnici e il software NetApp forniti secondo i termini del presente Contratto sono articoli aventi natura commerciale, sviluppati con finanziamenti esclusivamente privati. Il governo statunitense ha una licenza irrevocabile limitata, non esclusiva, non trasferibile, non cedibile, mondiale, per l'utilizzo dei Dati esclusivamente in connessione con e a supporto di un contratto governativo statunitense in base al quale i Dati sono distribuiti. Con la sola esclusione di quanto indicato nel presente documento, i Dati non possono essere utilizzati, divulgati, riprodotti, modificati, visualizzati o mostrati senza la previa approvazione scritta di NetApp, Inc. I diritti di licenza del governo degli Stati Uniti per il Dipartimento della Difesa sono limitati ai diritti identificati nella clausola DFARS 252.227-7015(b) (FEB 2014).

Informazioni sul marchio commerciale

NETAPP, il logo NETAPP e i marchi elencati alla pagina http://www.netapp.com/TM sono marchi di NetApp, Inc. Gli altri nomi di aziende e prodotti potrebbero essere marchi dei rispettivi proprietari.