# Configurazione e implementazione

ONTAP 9

NetApp
April 24, 2024

# Sommario

# 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.

#### 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.

#### 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.

#### 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.

## Passaggio 1: Installazione del certificato del server di autenticazione

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-----

   -----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
   ```

## 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
   ```

# Eseguire una chiamata API REST 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"
```