Concetti

ONTAP 9

NetApp
April 24, 2024

Sommario

Concetti

Server di autorizzazione e token di accesso

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`.

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.

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.

Opzioni per l'autorizzazione client ONTAP

Sono disponibili diverse opzioni per personalizzare l'autorizzazione del client ONTAP. Le decisioni di autorizzazione si basano, in ultima analisi, sui ruoli REST ONTAP contenuti o derivati dai token di accesso.

> 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.

Introduzione

L'implementazione di OAuth 2,0 all'interno di ONTAP è progettata per essere flessibile e robusta, fornendo le opzioni necessarie per proteggere l'ambiente ONTAP. A un livello elevato, esistono tre categorie di

configurazione principali per la definizione dell'autorizzazione del client ONTAP. Queste opzioni di configurazione si escludono a vicenda.

ONTAP applica la singola opzione più appropriata in base alla configurazione scelta. Vedere "Modalità con cui ONTAP determina l'accesso" Per ulteriori informazioni su come ONTAP elabora le definizioni di configurazione per prendere decisioni sugli accessi.

Oscilloscopi indipendenti OAuth 2,0

Questi ambiti contengono uno o più ruoli REST personalizzati, ciascuno incapsulato in una singola stringa. Sono indipendenti dalle definizioni dei ruoli ONTAP. È necessario definire queste stringhe di ambito nel server di autorizzazione.

Ruoli e utenti REST locali specifici di ONTAP

In base alla configurazione, è possibile utilizzare le definizioni di identità ONTAP locali per prendere decisioni di accesso. Le opzioni includono:

- Singolo ruolo REST denominato
- Corrispondenza del nome utente con un utente ONTAP locale

La sintassi dell'ambito per un ruolo denominato è **ontap-role-**<URL-encoded-ONTAP-role-name>. Ad esempio, se il ruolo è "admin" la stringa dell'ambito sarà "ontap-role-admin".

Active Directory o gruppi LDAP

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).

Oscilloscopi OAuth 2,0 autonomi

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.

È possibile 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.

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.
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
```

Modalità con cui ONTAP determina l'accesso

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.

Fase 1: Oscilloscopi autonomi

Se il token di accesso contiene ambiti indipendenti, ONTAP esamina prima tali 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 valore del flag `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, 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 ONTAP locali

Estrarre il nome utente dal token di accesso e tentare di associarlo a un utente ONTAP locale.

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

Fase 5: Mappatura da gruppo a ruolo

Estrarre il gruppo dal token di accesso e tentare di associarlo a un gruppo. I gruppi vengono definiti utilizzando Active Directory o un server LDAP equivalente.

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 di OAuth 2,0

Quando si definisce un server di autorizzazione per ONTAP, sono disponibili diverse opzioni di configurazione. In base a queste opzioni, è possibile creare un server di autorizzazione appropriato per l'ambiente 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.

I nomi dei parametri possono variare leggermente a seconda dell'interfaccia amministrativa di ONTAP. Ad esempio, quando si configura l'introspezione remota, l'endpoint viene identificato utilizzando il parametro del comando CLI `-introspection-endpoint`. Con System Manager, il campo equivalente è *Authorization server token introspection URI*. Per soddisfare tutte le interfacce amministrative di ONTAP, viene fornita una descrizione generale dei parametri. Il parametro o il campo esatto 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.

Parametro	Descrizione
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.
Rimuovere la richiesta di rimborso dell'utente	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.

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.

Autenticazione client mediante TLS reciproco

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.

Parametro	Descrizione
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.