Autorizzazione del client

ONTAP 9

NetApp
February 12, 2026

Sommario

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.

Informazioni sul copyright

Informazioni sul marchio commerciale