Autenticazione e autorizzazione utilizzando WebAuthn MFA

ONTAP 9

NetApp
January 08, 2025

Sommario

Autenticazione e autorizzazione utilizzando WebAuthn MFA

Panoramica dell'autenticazione a più fattori WebAuthn

A partire da ONTAP 9.16,1, gli amministratori possono attivare l'autenticazione multifattore WebAuthn per gli utenti che accedono a Gestione sistema. In questo modo si attivano gli accessi di System Manager utilizzando una chiave FIDO2 (ad esempio YubiKey) come seconda forma di autenticazione. Per impostazione predefinita, WebAuthn MFA è disattivato per gli utenti ONTAP nuovi ed esistenti.

WebAuthn MFA è supportato per utenti e gruppi che utilizzano i seguenti tipi di autenticazione per il primo metodo di autenticazione:

- Utenti: Password, dominio o nsswitch
- Gruppi: Dominio o nsswitch

Dopo aver attivato WebAuthn MFA come secondo metodo di autenticazione per un utente, all'utente viene richiesto di registrare un autenticatore hardware al momento dell'accesso a System Manager. Dopo la registrazione, la chiave privata viene memorizzata nell'autenticatore e la chiave pubblica viene memorizzata in ONTAP.

ONTAP supporta una credenziale WebAuthn per utente. Se un utente perde un autenticatore e deve sostituirlo, l'amministratore ONTAP deve eliminare la credenziale WebAuthn per l'utente in modo che l'utente possa registrare un nuovo autenticatore al successivo accesso.

Gli utenti che hanno attivato WebAuthn MFA come secondo metodo di autenticazione devono utilizzare l’FQDN (ad esempio, "https://myontap.example.com") invece dell’indirizzo IP (ad esempio, "https://192.168.100.200") per accedere a System Manager. Per gli utenti con WebAuthn MFA attivato, i tentativi di accesso a System Manager utilizzando l’indirizzo IP vengono rifiutati.

Abilitare WebAuthn MFA per utenti o gruppi di Gestione di sistema di ONTAP

In qualità di amministratore ONTAP, è possibile abilitare WebAuthn MFA per un utente o un gruppo di Gestione di sistema aggiungendo un nuovo utente o gruppo con l'opzione MFA WebAuthn attivata o attivando l'opzione per un utente o un gruppo esistente.

Dopo aver attivato WebAuthn MFA come secondo metodo di autenticazione per un utente o un gruppo, all'utente (o a tutti gli utenti di quel gruppo) verrà richiesto di registrare un dispositivo hardware FIDO2 al successivo accesso a System Manager. Questa registrazione viene gestita dal sistema operativo locale dell'utente e consiste generalmente nell'inserire la chiave di protezione, creare una chiave di accesso e toccare la chiave di protezione (se supportata).

Attivare WebAuthn MFA quando si crea un nuovo utente o gruppo

È possibile creare un nuovo utente o gruppo con WebAuthn MFA attivato utilizzando Gestione di sistema o la CLI di ONTAP.

System Manager

1. Selezionare **Cluster > Settings** (cluster > Impostazioni).
2. Selezionare l'icona a forma di freccia accanto a **utenti e ruoli**.
3. Selezionare **Aggiungi** in **utenti**.
4. Specificare un nome utente o gruppo e selezionare un ruolo nel menu a discesa **ruolo**.
5. Specificare un metodo di accesso e una password per l'utente o il gruppo.

   WebAuthn MFA supporta i metodi di accesso "password", "dominio" o "nsswitch" per gli utenti e "dominio" o "nsswitch" per i gruppi.

6. Nella colonna **MFA per HTTP**, selezionare **abilitato**.
7. Selezionare **Salva**.

CLI

1. Creare un nuovo utente o gruppo con WebAuthn MFA attivato.

   Nell'esempio seguente, WebAuthn MFA viene attivato scegliendo "publickey" per il secondo metodo di autenticazione:

```
security login create -user-or-group-name <user_or_group_name> \
                      -authentication-method domain \
                      -second-authentication-method publickey \
                      -application http \
                      -role admin
```

Abilitare WebAuthn MFA per un utente o un gruppo esistente

È possibile attivare WebAuthn MFA per un utente o un gruppo esistente.

System Manager

1. Selezionare **Cluster > Settings** (cluster > Impostazioni).
2. Selezionare l'icona a forma di freccia accanto a **utenti e ruoli**.
3. Nell'elenco degli utenti e dei gruppi, selezionare il menu delle opzioni per l'utente o il gruppo che si desidera modificare.

   WebAuthn MFA supporta i metodi di accesso "password", "dominio" o "nsswitch" per gli utenti e "dominio" o "nsswitch" per i gruppi.
4. Nella colonna **MFA per HTTP** per quell'utente, selezionare **attivato**.
5. Selezionare **Salva**.

CLI

1. Modificare un utente o un gruppo esistente per abilitare WebAuthn MFA per tale utente o gruppo.

   Nell'esempio seguente, WebAuthn MFA viene attivato scegliendo "publickey" per il secondo metodo di autenticazione:

```
security login modify -user-or-group-name <user_or_group_name> \
                      -authentication-method domain \
                      -second-authentication-method publickey \
                      -application http \
                      -role admin
```

Scopri di più

Visitare le pagine del manuale di ONTAP per i seguenti comandi:

- "creazione dell'accesso di sicurezza"
- "modifica dell'accesso di sicurezza"

Disattivare WebAuthn MFA per gli utenti di ONTAP System Manager

In qualità di amministratore di ONTAP, è possibile disattivare l'autenticazione MFA per un utente o un gruppo modificando l'utente o il gruppo con Gestione di sistema o l'interfaccia CLI di ONTAP.

Disattivare WebAuthn MFA per un utente o un gruppo esistente

È possibile disattivare WebAuthn MFA per un utente o un gruppo esistente in qualsiasi momento.

> Se si disabilitano le credenziali registrate, le credenziali vengono conservate. Se si riabilitano le credenziali in futuro, vengono utilizzate le stesse credenziali, quindi l'utente non deve effettuare nuovamente la registrazione al momento dell'accesso.

System Manager

1. Selezionare **Cluster > Settings** (cluster > Impostazioni).
2. Selezionare l'icona a forma di freccia accanto a **utenti e ruoli**.
3. Nell'elenco degli utenti e dei gruppi, selezionare l'utente o il gruppo che si desidera modificare.
4. Nella colonna **MFA per HTTP** per quell'utente, selezionare **Disabilitato**.
5. Selezionare **Salva**.

CLI

1. Modificare un utente o un gruppo esistente per disattivare WebAuthn MFA per tale utente o gruppo.

   Nell'esempio seguente, WebAuthn MFA viene disattivato scegliendo "nessuno" per il secondo metodo di autenticazione.

   ```
   security login modify -user-or-group-name <user_or_group_name> \
                         -authentication-method domain \
                         -second-authentication-method none \
                         -application http \
                         -role admin
   ```

Scopri di più

Visitare le pagine del manuale di ONTAP per questo comando:

- "modifica dell'accesso di sicurezza"

Visualizzare le impostazioni MFA di ONTAP WebAuthn e gestire le credenziali

In qualità di amministratore ONTAP, è possibile visualizzare le impostazioni MFA di WebAuthn a livello di cluster e gestire le credenziali di utenti e gruppi per MFA di WebAuthn.

Visualizzare le impostazioni del cluster per WebAuthn MFA

È possibile visualizzare le impostazioni del cluster per WebAuthn MFA utilizzando l'interfaccia CLI di ONTAP.

Fasi

1. Visualizzare le impostazioni del cluster per WebAuthn MFA. È possibile facoltativamente specificare una macchina virtuale di storage utilizzando l' `vserver`argomento:

   ```
   security webauthn show -vserver <storage_vm_name>
   ```

Visualizzare gli algoritmi WebAuthn MFA a chiave pubblica supportati

È possibile visualizzare gli algoritmi a chiave pubblica supportati per WebAuthn MFA per una VM di storage o per un cluster.

Fasi

1. Elencare gli algoritmi MFA WebAuthn a chiave pubblica supportati. È possibile facoltativamente specificare una macchina virtuale di storage utilizzando l' `vserver`argomento:

```
security webauthn supported-algorithms show -vserver <storage_vm_name>
```

Visualizzare le credenziali MFA di WebAuthn registrate

In qualità di amministratore ONTAP, è possibile visualizzare le credenziali WebAuthn registrate per tutti gli utenti. Gli utenti non amministratori che utilizzano questa procedura possono visualizzare solo le proprie credenziali WebAuthn registrate.

Fasi

1. Visualizzare le credenziali MFA di WebAuthn registrate:

```
security webauthn credentials show
```

Rimuovere una credenziale MFA WebAuthn registrata

È possibile rimuovere una credenziale MFA WebAuthn registrata. Ciò è utile quando la chiave hardware di un utente è stata persa, rubata o non è più in uso. È anche possibile rimuovere una credenziale registrata quando l'utente dispone ancora dell'autenticatore hardware originale, ma desidera sostituirla con una nuova. Dopo aver rimosso la credenziale, all'utente verrà richiesto di registrare l'autenticatore sostitutivo.

> La rimozione di una credenziale registrata per un utente non disattiva WebAuthn MFA per l'utente. Se un utente perde un autenticatore hardware e deve accedere prima di sostituirlo, è necessario rimuovere la credenziale utilizzando questi passaggi e anche "Disattivare WebAuthn MFA" per l'utente.

System Manager

1. Selezionare **Cluster > Settings** (cluster > Impostazioni).
2. Selezionare l'icona a forma di freccia accanto a **utenti e ruoli**.
3. Nell'elenco degli utenti e dei gruppi, selezionare il menu delle opzioni per l'utente o il gruppo di cui si desidera rimuovere le credenziali.
4. Selezionare **Rimuovi MFA per credenziali HTTP**.
5. Selezionare **Rimuovi**.

CLI

1. Eliminare le credenziali registrate. Tenere presente quanto segue:
   - È possibile facoltativamente specificare una macchina virtuale di storage dell'utente. Se omessa, la credenziale viene rimossa a livello di cluster.
   - È possibile specificare facoltativamente un nome utente dell'utente per il quale si desidera eliminare la credenziale. Se omessa, la credenziale viene rimossa per l'utente corrente.

```
security webauthn credentials delete -vserver <storage_vm_name>
-username <username>
```

Scopri di più

Visitare le pagine del manuale di ONTAP per i seguenti comandi:

- "sicurezza webauthn show"
- "security webauthn supportati-algoritmi show"
- "mostra le credenziali webauthn di sicurezza"
- "eliminazione delle credenziali webauthn di sicurezza"

Informazioni sul copyright

Informazioni sul marchio commerciale