Authentifizierung und Autorisierung mit WebAuthn MFA

ONTAP 9

NetApp
January 17, 2025

Inhalt

Authentifizierung und Autorisierung mit WebAuthn MFA

WebAuthn Multi-Faktor-Authentifizierung – Übersicht

Ab ONTAP 9.16.1 können Administratoren die Multifaktor-Authentifizierung (MFA) von WebAuthn für Benutzer aktivieren, die sich bei System Manager anmelden. Somit können sich System Manager Anmeldungen über einen FIDO2 Schlüssel (z. B. einen YubiKey) als zweite Form der Authentifizierung anmelden. WebAuthn MFA ist standardmäßig für neue und bestehende ONTAP-Benutzer deaktiviert.

WebAuthn MFA wird für Benutzer und Gruppen unterstützt, die die folgenden Authentifizierungstypen für die erste Authentifizierungsmethode verwenden:

- Benutzer: Passwort, Domain oder nsswitch
- Gruppen: Domain oder nsswitch

Nachdem Sie WebAuthn MFA als zweite Authentifizierungsmethode für einen Benutzer aktiviert haben, wird der Benutzer nach der Anmeldung bei System Manager aufgefordert, einen Hardware-Authentifikator zu registrieren. Nach der Registrierung wird der private Schlüssel im Authentifikator gespeichert und der öffentliche Schlüssel im ONTAP gespeichert.

ONTAP unterstützt eine WebAuthn-Anmeldeinformation pro Benutzer. Wenn ein Benutzer einen Authentifikator verliert und ersetzt werden muss, muss der ONTAP-Administrator die WebAuthn-Anmeldeinformationen für den Benutzer löschen, damit der Benutzer bei der nächsten Anmeldung einen neuen Authentifikator registrieren kann.

Benutzer, für die WebAuthn MFA als zweite Authentifizierungsmethode aktiviert ist, müssen den FQDN (z. B. "https://myontap.example.com") anstelle der IP-Adresse (z. B. "https://192.168.100.200") verwenden, um auf System Manager zuzugreifen. Bei Benutzern mit aktiviertem WebAuthn MFA werden Versuche, sich unter Verwendung der IP-Adresse beim System Manager anzumelden, abgelehnt.

Aktivieren Sie WebAuthn MFA für Benutzer oder Gruppen von ONTAP System Manager

Als ONTAP-Administrator können Sie WebAuthn MFA für einen Benutzer oder eine Gruppe des System Managers aktivieren, indem Sie entweder einen neuen Benutzer oder eine neue Gruppe hinzufügen, wobei die Option WebAuthn MFA aktiviert ist, oder die Option für einen vorhandenen Benutzer oder eine vorhandene Gruppe aktivieren.

Nachdem Sie WebAuthn MFA als zweite Authentifizierungsmethode für einen Benutzer oder eine Gruppe aktiviert haben, wird der Benutzer (oder alle Benutzer dieser Gruppe) bei der nächsten Anmeldung bei System Manager aufgefordert, ein Hardware-FIDO2-Gerät zu registrieren. Diese Registrierung wird vom lokalen Betriebssystem des Benutzers durchgeführt und besteht in der Regel aus dem Einfügen des Sicherheitsschlüssels, dem Erstellen eines Passschlüssels und dem Berühren des Sicherheitsschlüssels (sofern unterstützt).

Aktivieren Sie WebAuthn MFA beim Erstellen eines neuen Benutzers oder einer neuen Gruppe

Sie können einen neuen Benutzer oder eine neue Gruppe mit aktiviertem WebAuthn MFA entweder mit dem System-Manager oder der ONTAP-CLI erstellen.

System Manager

1. Wählen Sie **Cluster > Einstellungen**.
2. Wählen Sie das Pfeilsymbol neben **Users and Roles**.
3. Wählen Sie unter **Benutzer Hinzufügen** aus.
4. Geben Sie einen Benutzer- oder Gruppennamen an und wählen Sie im Dropdown-Menü für **Rolle** eine Rolle aus.
5. Geben Sie eine Anmeldemethode und ein Kennwort für den Benutzer oder die Gruppe an.

   WebAuthn MFA unterstützt Anmeldemethoden von "Password", "Domain" oder "nsswitch" für Benutzer und "Domain" oder "nsswitch" für Gruppen.
6. Wählen Sie in der Spalte **MFA für HTTP enabled** aus.
7. Wählen Sie **Speichern**.

CLI

1. Erstellen Sie einen neuen Benutzer oder eine neue Gruppe mit aktiviertem WebAuthn MFA.

   Im folgenden Beispiel wird WebAuthn MFA durch Auswahl von „publickey“ für die zweite Authentifizierungsmethode aktiviert:

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

Aktivieren Sie WebAuthn MFA für einen vorhandenen Benutzer oder eine vorhandene Gruppe

Sie können WebAuthn MFA für einen vorhandenen Benutzer oder eine vorhandene Gruppe aktivieren.

System Manager

1. Wählen Sie **Cluster > Einstellungen**.
2. Wählen Sie das Pfeilsymbol neben **Users and Roles**.
3. Wählen Sie in der Liste der Benutzer und Gruppen das Optionsmenü für den Benutzer oder die Gruppe aus, den Sie bearbeiten möchten.

   WebAuthn MFA unterstützt Anmeldemethoden von "Password", "Domain" oder "nsswitch" für Benutzer und "Domain" oder "nsswitch" für Gruppen.
4. Wählen Sie in der Spalte **MFA für HTTP** für diesen Benutzer **Enabled** aus.
5. Wählen Sie **Speichern**.

CLI

1. Ändern Sie einen vorhandenen Benutzer oder eine vorhandene Gruppe, um WebAuthn MFA für diesen Benutzer oder diese Gruppe zu aktivieren.

   Im folgenden Beispiel wird WebAuthn MFA durch Auswahl von „publickey“ für die zweite Authentifizierungsmethode aktiviert:

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

Weitere Informationen .

Im ONTAP-Handbuch finden Sie die folgenden Befehle:

- "Sicherheits-Login erstellen"
- "Sicherheitsanmeldung ändern"

Deaktivieren Sie WebAuthn MFA für ONTAP System Manager-Benutzer

Als ONTAP-Administrator können Sie WebAuthn MFA für einen Benutzer oder eine Gruppe deaktivieren, indem Sie den Benutzer oder die Gruppe mit dem Systemmanager oder der ONTAP-CLI bearbeiten.

Deaktivieren Sie WebAuthn MFA für einen vorhandenen Benutzer oder eine vorhandene Gruppe

Sie können WebAuthn MFA für einen vorhandenen Benutzer oder eine vorhandene Gruppe jederzeit deaktivieren.

Wenn Sie registrierte Anmeldeinformationen deaktivieren, bleiben die Anmeldeinformationen erhalten. Wenn Sie die Anmeldeinformationen in Zukunft erneut aktivieren, werden dieselben Anmeldeinformationen verwendet, sodass der Benutzer sich bei der Anmeldung nicht erneut registrieren muss.

System Manager

1. Wählen Sie **Cluster > Einstellungen**.
2. Wählen Sie das Pfeilsymbol neben **Users and Roles**.
3. Wählen Sie in der Liste der Benutzer und Gruppen den Benutzer oder die Gruppe aus, den Sie bearbeiten möchten.
4. Wählen Sie in der Spalte **MFA für HTTP** für diesen Benutzer **disabled** aus.
5. Wählen Sie **Speichern**.

CLI

1. Ändern Sie einen vorhandenen Benutzer oder eine vorhandene Gruppe, um WebAuthn MFA für diesen Benutzer oder diese Gruppe zu deaktivieren.

   Im folgenden Beispiel wird WebAuthn MFA deaktiviert, indem für die zweite Authentifizierungsmethode „none“ ausgewählt wird.

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

Weitere Informationen .

Den folgenden Befehl finden Sie in den Handbuchseiten von ONTAP:

- "Sicherheitsanmeldung ändern"

Zeigen Sie die MFA-Einstellungen für ONTAP WebAuthn an und verwalten Sie die Anmeldeinformationen

Als ONTAP-Administrator können Sie Cluster-weite WebAuthn-MFA-Einstellungen anzeigen und Benutzer- und Gruppenanmeldeinformationen für WebAuthn MFA verwalten.

Cluster-Einstellungen für WebAuthn MFA anzeigen

Sie können die Clustereinstellungen für WebAuthn MFA mithilfe der ONTAP-CLI anzeigen.

Schritte

1. Zeigen Sie die Clustereinstellungen für WebAuthn MFA an. Sie können optional eine Storage-VM mit dem Argument angeben `vserver`:

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

Unterstützte öffentliche WebAuthn-MFA-Algorithmen anzeigen

Sie können die unterstützten Public-Key-Algorithmen für WebAuthn MFA für eine Speicher-VM oder für einen Cluster anzeigen.

Schritte

1. Listen Sie die unterstützten öffentlichen WebAuthn MFA-Algorithmen auf. Sie können optional eine Storage-VM mit dem Argument angeben `vserver`:

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

Registrierte WebAuthn-MFA-Anmeldedaten anzeigen

Als ONTAP-Administrator können Sie die registrierten WebAuthn-Anmeldeinformationen für alle Benutzer anzeigen. Benutzer, die dieses Verfahren nicht von Administratoren verwenden, können nur ihre eigenen registrierten WebAuthn-Anmeldedaten anzeigen.

Schritte

1. Registrierte WebAuthn-MFA-Anmeldedaten anzeigen:

```
security webauthn credentials show
```

Entfernen Sie eine registrierte WebAuthn-MFA-Anmeldeinformation

Sie können registrierte WebAuthn-MFA-Anmeldeinformationen entfernen. Dies ist nützlich, wenn der Hardwareschlüssel eines Benutzers verloren gegangen ist, gestohlen wurde oder nicht mehr verwendet wird. Sie können auch registrierte Anmeldeinformationen entfernen, wenn der Benutzer noch über den ursprünglichen Hardwareauthentifizator verfügt, ihn aber durch einen neuen ersetzen möchte. Nach dem Entfernen der Anmeldeinformationen wird der Benutzer aufgefordert, den Ersatz-Authentifikator zu registrieren.

Durch das Entfernen von registrierten Anmeldeinformationen für einen Benutzer wird WebAuthn MFA für den Benutzer nicht deaktiviert. Wenn ein Benutzer einen Hardware-Authentifikator verliert und sich vor dem Ersetzen anmelden muss, müssen Sie die Anmeldeinformationen mithilfe dieser Schritte und auch für den Benutzer entfernen"Deaktivieren Sie WebAuthn MFA".

System Manager

1. Wählen Sie **Cluster > Einstellungen**.
2. Wählen Sie das Pfeilsymbol neben **Users and Roles**.
3. Wählen Sie in der Liste der Benutzer und Gruppen das Optionsmenü für den Benutzer oder die Gruppe aus, dessen Anmeldeinformationen Sie entfernen möchten.
4. Wählen Sie **MFA für HTTP-Anmeldeinformationen entfernen**.
5. Wählen Sie **Entfernen**.

CLI

1. Löschen Sie die registrierten Anmeldedaten. Beachten Sie Folgendes:
   - Sie können optional eine Storage-VM des Benutzers angeben. Wenn sie nicht angegeben sind, werden die Zugangsdaten auf Cluster-Ebene entfernt.
   - Sie können optional einen Benutzernamen des Benutzers angeben, für den Sie die Anmeldeinformationen löschen möchten. Wenn sie nicht angegeben ist, werden die Anmeldeinformationen für den aktuellen Benutzer entfernt.

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

Weitere Informationen .

Im ONTAP-Handbuch finden Sie die folgenden Befehle:

- "Sicherheit webauthn zeigen"
- "Sicherheit webauthn Unterstützte Algorithmen zeigen"
- "Sicherheits-webauthn-Anmeldeinformationen werden angezeigt"
- "Sicherheit webauthn Anmeldeinformationen löschen"