Multifaktor-Authentifizierung (MFA) Konten aktivieren

ONTAP 9

NetApp
September 09, 2026

This PDF was generated from https://docs.netapp.com/de-de/ontap/authentication/mfa-overview.html on September 09, 2026. Always check docs.netapp.com for the latest.

Inhalt

Multifaktor-Authentifizierung (MFA) Konten aktivieren . . . 1
- Informationen zur ONTAP Multifaktor Authentifizierung . . . 1
- ONTAP Multifaktor Authentifizierung mit SSH und TOTP aktivieren . . . 2
  - Multi-Faktor-Authentifizierung mit öffentlichem SSH-Schlüssel und Benutzerpasswort aktivieren . . . 3
  - MFA mit TOTP aktivieren . . . 3
- Lokale ONTAP Benutzerkonten für MFA mit TOTP konfigurieren . . . 5
- TOTP-Geheimschlüssel für ein ONTAP Benutzerkonto zurücksetzen . . . 6
  - TOTP zurücksetzen, falls Ihr Schlüssel kompromittiert wurde . . . 6
  - TOTP zurücksetzen, falls der Schlüssel verloren gegangen ist . . . 7
- Der TOTP-Geheimschlüssel für ein ONTAP Benutzerkonto wird deaktiviert. . . . 7

Multifaktor-Authentifizierung (MFA) Konten aktivieren

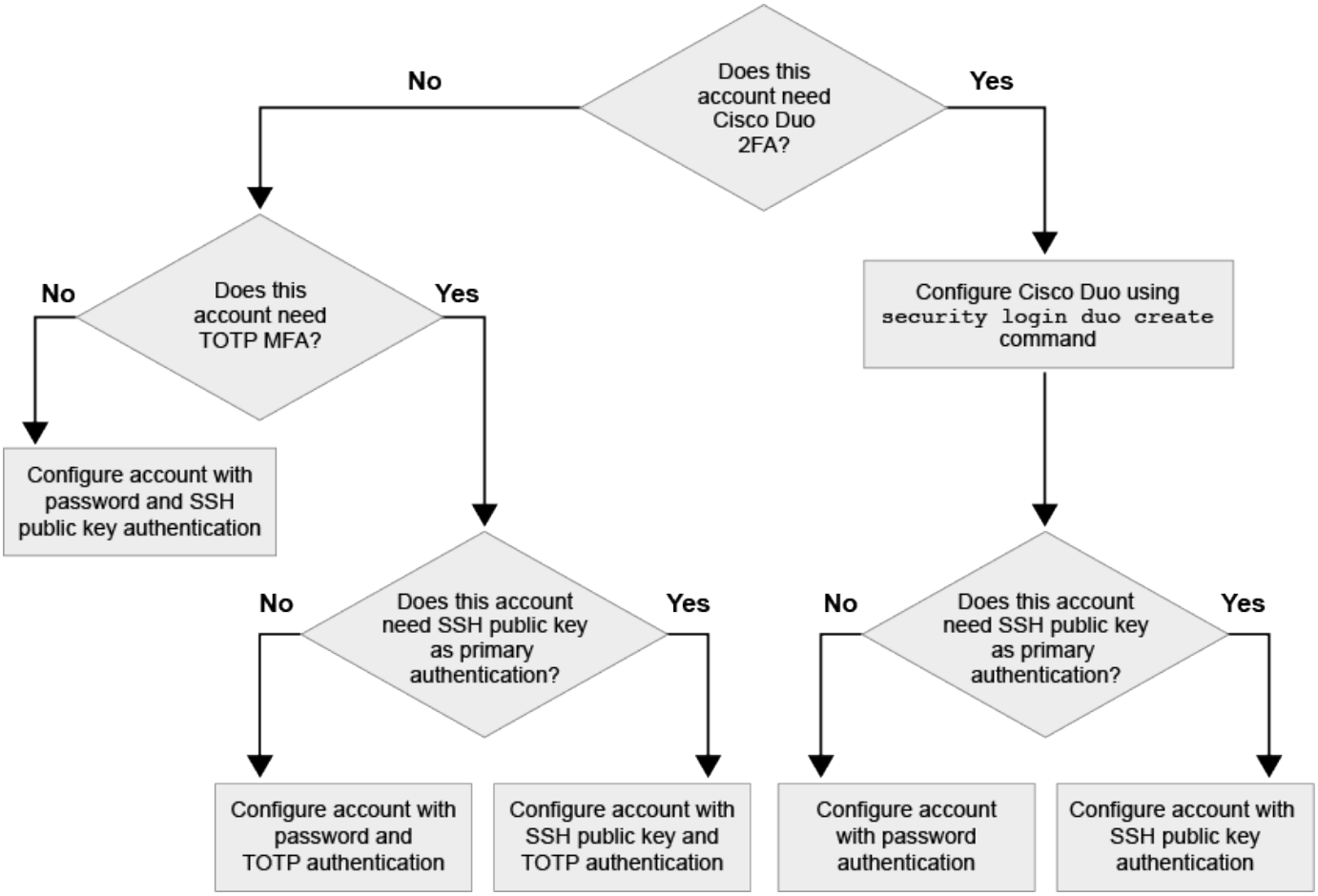
Informationen zur ONTAP Multifaktor Authentifizierung

Die Multifaktor Authentifizierung (MFA) bietet die Möglichkeit, die Sicherheit zu erhöhen, indem von den Benutzern zwei Authentifizierungsverfahren verlangt werden, um sich bei einer Admin- oder Datenspeicher-VM anzumelden.

Abhängig von Ihrer ONTAP Version kann eine Kombination aus einem SSH Public Key, einem Benutzerpasswort und einem zeitbasierten Einmalpasswort (TOTP) für die Multifaktor Authentifizierung verwendet werden. Bei Aktivierung und Konfiguration von Cisco Duo (ONTAP 9.14.1 und höher) dient es als zusätzliches Authentifizierungsverfahren und ergänzt die bestehenden Methoden für alle Benutzer.

Verfügbar ab…	Erstes Authentifizierungsverfahren	Zweites Authentifizierungsverfahren
ONTAP 9.14.1	SSH öffentlicher Schlüssel	TOTP
	Benutzerpasswort	TOTP
	SSH öffentlicher Schlüssel	Cisco Duo
	Benutzerpasswort	Cisco Duo
ONTAP 9.13.1	SSH öffentlicher Schlüssel	TOTP
	Benutzerpasswort	TOTP
ONTAP 9.3	SSH öffentlicher Schlüssel	Benutzerpasswort

Wenn MFA konfiguriert ist, muss der Clusteradministrator zuerst das lokale Benutzerkonto aktivieren, anschließend wird das Konto vom lokalen Benutzer konfiguriert.



ONTAP Multifaktor Authentifizierung mit SSH und TOTP aktivieren

Die Multifaktor-Authentifizierung (MFA) bietet die Möglichkeit, die Sicherheit zu erhöhen, indem von Benutzern zwei Authentifizierungsverfahren verlangt werden, um sich bei einer Admin- oder Daten-SVM anzumelden.

Über diese Aufgabe

- Sie müssen Cluster-Administrator sein, um diese Aufgabe ausführen zu können.
- Wenn Sie sich nicht sicher sind, welche Zugriffskontrollrolle Sie dem Anmeldekonto zuweisen möchten, kann die Rolle später mit dem `security login modify` Befehl hinzugefügt werden.

  Weitere Informationen zu `security login modify` finden sich in der "ONTAP-Befehlsreferenz".

  "Ändern der einem Administrator zugewiesenen Rolle"

- Wenn ein öffentlicher Schlüssel zur Authentifizierung verwendet wird, muss der öffentliche Schlüssel mit dem Konto verknüpft werden, bevor das Konto auf die SVM zugreifen kann.

  "Einem Benutzerkonto wird ein öffentlicher Schlüssel zugeordnet."

  Diese Aufgabe kann vor oder nach der Aktivierung des Kontozugriffs durchgeführt werden.

- Ab ONTAP 9.12.1 ist die Verwendung von Yubikey Hardware-Authentifizierungsgeräten für die SSH-Client-MFA mit den Authentifizierungsstandards FIDO2 (Fast IDentity Online) oder Personal Identity Verification (PIV) möglich.

Multi-Faktor-Authentifizierung mit öffentlichem SSH-Schlüssel und Benutzerpasswort aktivieren

Ab ONTAP 9.3 kann ein Cluster-Administrator lokale Benutzerkonten einrichten, um sich mit MFA unter Verwendung eines öffentlichen SSH-Schlüssels und eines Benutzerpassworts anzumelden.

1. Multi-Faktor-Authentifizierung für das lokale Benutzerkonto mit öffentlichem SSH-Schlüssel und Benutzerpasswort aktivieren:

   ```
   security login create -vserver <svm_name> -user-or-group-name
   <user_name> -application ssh -authentication-method <password|publickey>
   -role admin -second-authentication-method <password|publickey>
   ```

   Der folgende Befehl erfordert das SVM-Administratorkonto `admin2` mit der vordefinierten `admin` Rolle, um sich bei der SVM`engData1` sowohl mit einem öffentlichen SSH-Schlüssel als auch mit einem Benutzerpasswort anzumelden:

   ```
   cluster-1::> security login create -vserver engData1 -user-or-group-name
   admin2 -application ssh -authentication-method publickey -role admin
   -second-authentication-method password

   Please enter a password for user 'admin2':
   Please enter it again:
   Warning: To use public-key authentication, you must create a public key
   for user "admin2".
   ```

   Weitere Informationen zu `security login create` finden sich in der "ONTAP-Befehlsreferenz".

MFA mit TOTP aktivieren

Ab ONTAP 9.13.1 lässt sich die Sicherheit erhöhen, indem lokale Benutzer verpflichtet werden, sich sowohl mit einem öffentlichen SSH-Schlüssel oder Benutzerpasswort als auch mit einem zeitbasierten Einmalpasswort (TOTP) an einer Admin- oder Daten-SVM anzumelden. Nachdem das Konto für die Multi-Faktor-Authentifizierung (MFA) mit TOTP aktiviert wurde, muss sich der lokale Benutzer bei "Konfiguration abschließen" anmelden.

TOTP ist ein Algorithmus, der anhand der aktuellen Zeit ein Einmalpasswort generiert. Wenn TOTP verwendet wird, ist es immer die zweite Form der Authentifizierung nach dem SSH Public Key oder dem Benutzerpasswort.

Bevor Sie beginnen

Um diese Aufgaben auszuführen, ist die Rolle eines Speicheradministrators erforderlich.

Schritte

MFA kann so eingerichtet werden, dass als erstes Authentifizierungsverfahren entweder ein Benutzerpasswort oder ein SSH Public Key und als zweites Authentifizierungsverfahren TOTP verwendet wird.

MFA mit Benutzerpasswort und TOTP aktivieren

1. Ein Benutzerkonto kann für die Multifaktor Authentifizierung mit Benutzerpasswort und TOTP verwendet werden.

   Für neue Benutzerkonten

   ```
   security login create -vserver <svm_name> -user-or-group-name
   <user_or_group_name> -application ssh -authentication-method
   password -second-authentication-method totp -role <role> -comment
   <comment>
   ```

   Für bestehende Benutzerkonten

   ```
   security login modify -vserver <svm_name> -user-or-group-name
   <user_or_group_name> -application ssh -authentication-method
   password -second-authentication-method totp -role <role> -comment
   <comment>
   ```

2. Es sollte überprüft werden, ob die Multi-Faktor-Authentifizierung mit TOTP aktiviert ist:

   ```
   security login show
   ```

MFA mit SSH Public Key und TOTP aktivieren

1. Ein Benutzerkonto für die Multifaktor-Authentifizierung mit einem öffentlichen SSH-Schlüssel und TOTP aktivieren.

   Für neue Benutzerkonten

   ```
   security login create -vserver <svm_name> -user-or-group-name
   <user_or_group_name> -application ssh -authentication-method
   publickey -second-authentication-method totp -role <role> -comment
   <comment>
   ```

   Für bestehende Benutzerkonten

   ```
   security login modify -vserver <svm_name> -user-or-group-name
   <user_or_group_name> -application ssh -authentication-method
   publickey -second-authentication-method totp -role <role> -comment
   <comment>
   ```

Weitere Informationen zu `security login modify` finden sich in der "ONTAP-Befehlsreferenz".

2. Es sollte überprüft werden, ob die Multi-Faktor-Authentifizierung mit TOTP aktiviert ist:

```
security login show
```

Weitere Informationen zu `security login show` finden sich in der "ONTAP-Befehlsreferenz".

Nachdem Sie fertig sind

- Wenn einem Administratorkonto noch kein öffentlicher Schlüssel zugeordnet ist, muss dies erfolgen, bevor das Konto auf die SVM zugreifen kann.

  "Verknüpfung eines öffentlichen Schlüssels mit einem Benutzerkonto"

- Der lokale Benutzer muss sich anmelden, um die MFA-Konfiguration mit TOTP abzuschließen.

  "Lokales Benutzerkonto für MFA mit TOTP konfigurieren"

Verwandte Informationen

- "Multifaktor-Authentifizierung in ONTAP 9 (TR-4647)"
- "ONTAP-Befehlsreferenz"

Lokale ONTAP Benutzerkonten für MFA mit TOTP konfigurieren

Ab ONTAP 9.13.1 können Benutzerkonten mit Multifaktor-Authentifizierung (MFA) unter Verwendung eines zeitbasierten Einmalpassworts (TOTP) konfiguriert werden.

Bevor Sie beginnen

- Der Speicheradministrator muss "MFA mit TOTP verwenden" als zweites Authentifizierungsverfahren für Ihr Benutzerkonto festlegen.
- Das Authentifizierungsverfahren für das primäre Nutzerkonto sollte ein Benutzerpasswort oder ein öffentlicher SSH-Schlüssel sein.
- Sie müssen Ihre TOTP-App so konfigurieren, dass sie mit Ihrem Smartphone funktioniert und Ihren TOTP-Geheimschlüssel erstellen.

  Microsoft Authenticator, Google Authenticator, Authy und alle anderen TOTP-kompatiblen Authentifizierungsprogramme werden unterstützt.

Schritte

1. Melden Sie sich mit Ihrem aktuellen Authentifizierungsverfahren bei Ihrem Nutzerkonto an.

   Das aktuelle Authentifizierungsverfahren sollte ein Benutzerpasswort oder ein öffentlicher SSH-Schlüssel sein.

2. Die TOTP-Konfiguration für Ihr Konto erstellen:

```
security login totp create -vserver "<svm_name>" -username
"<account_username >"
```

3. Überprüfen Sie, ob die TOTP Konfiguration für Ihr Konto aktiviert ist:

```
security login totp show -vserver "<svm_name>" -username
"<account_username>"
```

Verwandte Informationen

- "security login totp create"
- "security login totp show"

TOTP-Geheimschlüssel für ein ONTAP Benutzerkonto zurücksetzen

Zum Schutz der Kontosicherheit sollte der TOTP-Geheimschlüssel deaktiviert und ein neuer erstellt werden, falls dieser kompromittiert oder verloren geht.

TOTP zurücksetzen, falls Ihr Schlüssel kompromittiert wurde

Wenn Ihr TOTP-Geheimschlüssel kompromittiert wurde, Sie aber noch Zugriff darauf haben, kann der kompromittierte Schlüssel entfernt und ein neuer erstellt werden.

1. Melden Sie sich mit Ihrem Benutzerpasswort oder Ihrem öffentlichen SSH-Schlüssel und Ihrem kompromittierten TOTP-Geheimschlüssel bei Ihrem Benutzerkonto an.
2. Den kompromittierten TOTP-Geheimschlüssel entfernen:

```
security login totp delete -vserver <svm_name> -username
<account_username>
```

> Ab ONTAP 9.19.1 muss ein gültiger TOTP-Code oder Scratch-Code eingegeben werden, um den TOTP-Geheimschlüssel mithilfe der ONTAP CLI zu löschen. Das Löschen des TOTP-Geheimschlüssels über die ONTAP REST API ist nicht möglich.

3. Einen neuen TOTP-Geheimschlüssel erstellen:

```
security login totp create -vserver <svm_name> -username
<account_username>
```

4. Überprüfen Sie, ob die TOTP Konfiguration für Ihr Konto aktiviert ist:

```
security login totp show -vserver <svm_name> -username
```

```
<account_username>
```

TOTP zurücksetzen, falls der Schlüssel verloren gegangen ist

Wenn Ihr TOTP-Geheimschlüssel verloren geht, sollte Ihr Speicheradministrator "Der Schlüssel ist deaktiviert" kontaktiert werden. Nachdem Ihr Schlüssel deaktiviert wurde, kann das erste Authentifizierungsverfahren zur Anmeldung und zur Konfiguration eines neuen TOTP verwendet werden.

Bevor Sie beginnen

Der TOTP-Geheimschlüssel muss von einem Storage-Administrator deaktiviert werden. Wenn kein Storage-Administratorkonto vorhanden ist, sollte der Storage-Administrator kontaktiert werden, damit der Schlüssel deaktiviert wird.

Schritte

1. Nachdem das TOTP-Geheimnis von einem Speicheradministrator deaktiviert wurde, kann das primäre Authentifizierungsverfahren genutzt werden, um sich beim lokalen Konto anzumelden.
2. Einen neuen TOTP-Geheimschlüssel erstellen:

```
security login totp create -vserver <svm_name> -username
<account_username >
```

3. Überprüfen Sie, ob die TOTP Konfiguration für Ihr Konto aktiviert ist:

```
security login totp show -vserver <svm_name> -username
<account_username>
```

Verwandte Informationen

- "security login totp create"
- "security login totp löschen"
- "security login totp show"

Der TOTP-Geheimschlüssel für ein ONTAP Benutzerkonto wird deaktiviert.

Geht der geheime Schlüssel für das zeitbasierte Einmalpasswort (TOTP) eines lokalen Benutzers verloren, muss der verlorene Schlüssel von einem Speicheradministrator deaktiviert werden, bevor der Benutzer einen neuen TOTP-Schlüssel erstellen kann.

Über diese Aufgabe

Diese Aufgabe kann nur von einem Cluster-Administratorkonto aus durchgeführt werden.

Schritt

1. TOTP-Geheimschlüssel deaktivieren:

```
security login totp modify -vserver <svm_name> -username
<account_username> -enabled false
```

Weitere Informationen zu `security login totp modify` finden sich in der "ONTAP-Befehlsreferenz".

Copyright-Informationen

Copyright © 2026 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtsinhabers in keiner Form und durch keine Mittel – weder grafische noch elektronische oder mechanische, einschließlich Fotokopieren, Aufnehmen oder Speichern in einem elektronischen Abrufsystem – auch nicht in Teilen, vervielfältigt werden.

Software, die von urheberrechtlich geschütztem NetApp Material abgeleitet wird, unterliegt der folgenden Lizenz und dem folgenden Haftungsausschluss:

DIE VORLIEGENDE SOFTWARE WIRD IN DER VORLIEGENDEN FORM VON NETAPP ZUR VERFÜGUNG GESTELLT, D. H. OHNE JEGLICHE EXPLIZITE ODER IMPLIZITE GEWÄHRLEISTUNG, EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE STILLSCHWEIGENDE GEWÄHRLEISTUNG DER MARKTGÄNGIGKEIT UND EIGNUNG FÜR EINEN BESTIMMTEN ZWECK, DIE HIERMIT AUSGESCHLOSSEN WERDEN. NETAPP ÜBERNIMMT KEINERLEI HAFTUNG FÜR DIREKTE, INDIREKTE, ZUFÄLLIGE, BESONDERE, BEISPIELHAFTE SCHÄDEN ODER FOLGESCHÄDEN (EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE BESCHAFFUNG VON ERSATZWAREN ODER -DIENSTLEISTUNGEN, NUTZUNGS-, DATEN- ODER GEWINNVERLUSTE ODER UNTERBRECHUNG DES GESCHÄFTSBETRIEBS), UNABHÄNGIG DAVON, WIE SIE VERURSACHT WURDEN UND AUF WELCHER HAFTUNGSTHEORIE SIE BERUHEN, OB AUS VERTRAGLICH FESTGELEGTER HAFTUNG, VERSCHULDENSUNABHÄNGIGER HAFTUNG ODER DELIKTSHAFTUNG (EINSCHLIESSLICH FAHRLÄSSIGKEIT ODER AUF ANDEREM WEGE), DIE IN IRGENDEINER WEISE AUS DER NUTZUNG DIESER SOFTWARE RESULTIEREN, SELBST WENN AUF DIE MÖGLICHKEIT DERARTIGER SCHÄDEN HINGEWIESEN WURDE.

NetApp behält sich das Recht vor, die hierin beschriebenen Produkte jederzeit und ohne Vorankündigung zu ändern. NetApp übernimmt keine Verantwortung oder Haftung, die sich aus der Verwendung der hier beschriebenen Produkte ergibt, es sei denn, NetApp hat dem ausdrücklich in schriftlicher Form zugestimmt. Die Verwendung oder der Erwerb dieses Produkts stellt keine Lizenzierung im Rahmen eines Patentrechts, Markenrechts oder eines anderen Rechts an geistigem Eigentum von NetApp dar.

Das in diesem Dokument beschriebene Produkt kann durch ein oder mehrere US-amerikanische Patente, ausländische Patente oder anhängige Patentanmeldungen geschützt sein.

ERLÄUTERUNG ZU „RESTRICTED RIGHTS“: Nutzung, Vervielfältigung oder Offenlegung durch die US-Regierung unterliegt den Einschränkungen gemäß Unterabschnitt (b)(3) der Klausel „Rights in Technical Data – Noncommercial Items“ in DFARS 252.227-7013 (Februar 2014) und FAR 52.227-19 (Dezember 2007).

Die hierin enthaltenen Daten beziehen sich auf ein kommerzielles Produkt und/oder einen kommerziellen Service (wie in FAR 2.101 definiert) und sind Eigentum von NetApp, Inc. Alle technischen Daten und die Computersoftware von NetApp, die unter diesem Vertrag bereitgestellt werden, sind gewerblicher Natur und wurden ausschließlich unter Verwendung privater Mittel entwickelt. Die US-Regierung besitzt eine nicht ausschließliche, nicht übertragbare, nicht unterlizenzierbare, weltweite, limitierte unwiderrufliche Lizenz zur Nutzung der Daten nur in Verbindung mit und zur Unterstützung des Vertrags der US-Regierung, unter dem die Daten bereitgestellt wurden. Sofern in den vorliegenden Bedingungen nicht anders angegeben, dürfen die Daten ohne vorherige schriftliche Genehmigung von NetApp, Inc. nicht verwendet, offengelegt, vervielfältigt, geändert, aufgeführt oder angezeigt werden. Die Lizenzrechte der US-Regierung für das US-Verteidigungsministerium sind auf die in DFARS-Klausel 252.227-7015(b) (Februar 2014) genannten Rechte beschränkt.

Markeninformationen

NETAPP, das NETAPP Logo und die unter http://www.netapp.com/TM aufgeführten Marken sind Marken von NetApp, Inc. Andere Firmen und Produktnamen können Marken der jeweiligen Eigentümer sein.