Aktivieren Sie Multi-Faktor-Authentifizierungskonten (MFA)

ONTAP 9

NetApp
April 16, 2024

This PDF was generated from https://docs.netapp.com/de-de/ontap/authentication/mfa-overview.html on April 16, 2024. Always check docs.netapp.com for the latest.

Inhalt

Aktivieren Sie Multi-Faktor-Authentifizierungskonten (MFA) . . . 1
Übersicht über Multi-Faktor-Authentifizierung . . . 1
Aktivieren Sie Multi-Faktor-Authentifizierung . . . 2
Konfigurieren Sie das lokale Benutzerkonto für MFA mit TOTP . . . 5
TOTP-Schlüssel zurücksetzen . . . 6
Deaktivieren Sie den geheimen TOTP-Schlüssel für das lokale Konto . . . 7

Aktivieren Sie Multi-Faktor-Authentifizierungskonten (MFA)

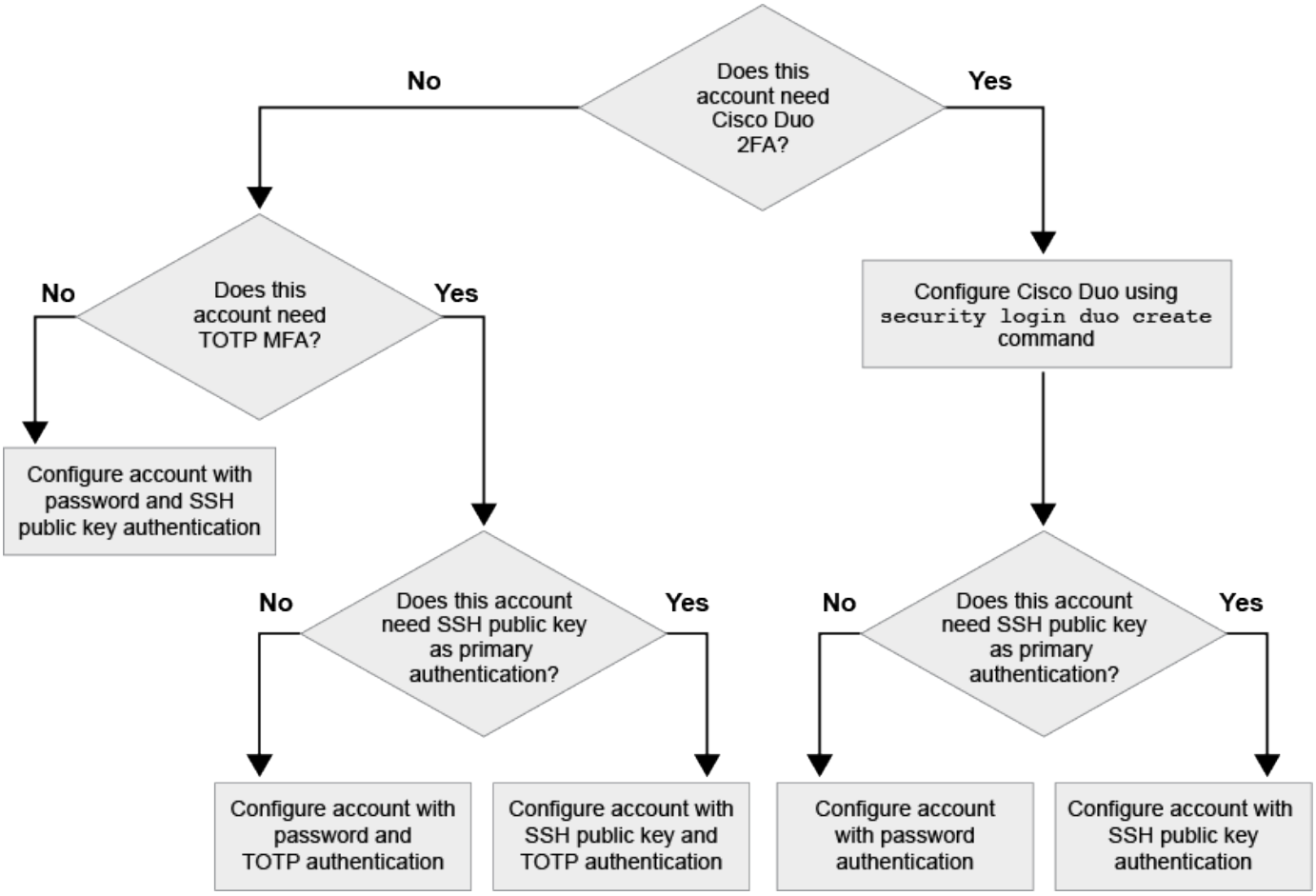
Übersicht über Multi-Faktor-Authentifizierung

Dank der Multi-Faktor-Authentifizierung (MFA) können Sie die Sicherheit erhöhen, da Benutzer zur Anmeldung bei einem Administrator oder einer Storage-VM zwei Authentifizierungsmethoden bereitstellen müssen.

Je nach Ihrer Version von ONTAP können Sie eine Kombination aus einem öffentlichen SSH-Schlüssel, einem Benutzerpasswort und einem zeitbasierten Einmalpasswort (TOTP) zur mehrstufigen Authentifizierung verwenden. Wenn Sie Cisco Duo (ONTAP 9.14.1 und höher) aktivieren und konfigurieren, dient es als zusätzliche Authentifizierungsmethode, die die bestehenden Methoden für alle Benutzer ergänzt.

Verfügbar ab…	Erste Authentifizierungsmethode	Zweite Authentifizierungsmethode
ONTAP 9.14.1	Öffentlicher SSH-Schlüssel	TOTP
	Benutzerkennwort	TOTP
	Öffentlicher SSH-Schlüssel	Cisco Duo
	Benutzerpasswort	Cisco Duo
ONTAP 9.13.1	Öffentlicher SSH-Schlüssel	TOTP
	Benutzerpasswort	TOTP
ONTAP 9.3	Öffentlicher SSH-Schlüssel	Benutzerpasswort

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



Aktivieren Sie Multi-Faktor-Authentifizierung

Dank der Multi-Faktor-Authentifizierung (MFA) können Sie die Sicherheit erhöhen, da Benutzer zur Anmeldung bei einem Administrator oder einer Daten-SVM zwei Authentifizierungsmethoden bereitstellen müssen.

Über diese Aufgabe

- Sie müssen ein Cluster-Administrator sein, um diese Aufgabe auszuführen.
- Wenn Sie sich nicht sicher sind, welche Rolle bei der Zugriffssteuerung Sie dem Login-Konto zuweisen möchten, können Sie das verwenden `security login modify` Befehl, um die Rolle später hinzuzufügen.

  "Ändern der Rolle, die einem Administrator zugewiesen ist"

- Wenn Sie einen öffentlichen Schlüssel für die Authentifizierung verwenden, müssen Sie den öffentlichen Schlüssel dem Konto zuordnen, bevor das Konto auf die SVM zugreifen kann.

  "Einem Benutzerkonto einen öffentlichen Schlüssel zuordnen"

  Sie können diese Aufgabe vor oder nach dem Aktivieren des Kontozugriffs ausführen.

- Ab ONTAP 9.12.1 können Sie Yubikey-Hardware-Authentifizierungsgeräte für SSH-Client MFA verwenden, indem Sie die Authentifizierungsstandards FIDO2 (Fast Identity Online) oder PIV (Personal Identity Verification) verwenden.

Aktivieren Sie MFA mit öffentlichem SSH-Schlüssel und Benutzerpasswort

Ab ONTAP 9.3 kann ein Cluster-Administrator lokale Benutzerkonten für die Anmeldung mit einem öffentlichen SSH-Schlüssel und einem Benutzerpasswort einrichten.

1. Aktivieren Sie MFA auf einem lokalen Benutzerkonto mit öffentlichem SSH-Schlüssel und Benutzerpasswort:

   ```
   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 dem vordefinierten `admin` Rolle zum Anmelden bei der SVM`engData1` Sowohl mit einem öffentlichen SSH-Schlüssel als auch mit einem Benutzerpasswort:

   ```
   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".
   ```

Aktivieren Sie MFA mit TOTP

Ab ONTAP 9.13.1 können Sie die Sicherheit erhöhen, indem Sie lokale Benutzer über einen öffentlichen SSH-Schlüssel oder ein Benutzerkennwort und ein zeitbasiertes Einmalpasswort (TOTP) bei einem Administrator oder einer Daten-SVM einloggen müssen. Nachdem das Konto für MFA mit TOTP aktiviert wurde, muss sich der lokale Benutzer bei anmelden "Schließen Sie die Konfiguration ab".

TOTP ist ein Computeralgorithmus, der die aktuelle Zeit verwendet, um ein Einmalpasswort zu generieren. Wenn TOTP verwendet wird, ist es immer die zweite Form der Authentifizierung nach dem öffentlichen SSH-Schlüssel oder dem Benutzerpasswort.

Bevor Sie beginnen

Sie müssen ein Storage-Administrator sein, um diese Aufgaben auszuführen.

Schritte

Sie können MFA für mit einem Benutzerpasswort oder einem öffentlichen SSH-Schlüssel als erste Authentifizierungsmethode und TOTP als zweite Authentifizierungsmethode einrichten.

Aktivieren Sie MFA mit Benutzerpasswort und TOTP

1. Aktivieren Sie ein Benutzerkonto für Multi-Faktor-Authentifizierung mit einem Benutzerpasswort und einem TOTP.

   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. Vergewissern Sie sich, dass MFA mit TOTP aktiviert ist:

   ```
   security login show
   ```

Aktivieren Sie MFA mit öffentlichem SSH-Schlüssel und TOTP

1. Aktivieren Sie ein Benutzerkonto für Multi-Faktor-Authentifizierung mit einem öffentlichen SSH-Schlüssel und TOTP.

   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>
   ```

2. Vergewissern Sie sich, dass MFA mit TOTP aktiviert ist:

```
security login show
```

Nachdem Sie fertig sind

- Falls Sie dem Administratorkonto keinen öffentlichen Schlüssel zugeordnet haben, müssen Sie dies tun, bevor das Konto auf die SVM zugreifen kann.

  "Verknüpfen eines öffentlichen Schlüssels mit einem Benutzerkonto"

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

  "Konfigurieren Sie das lokale Benutzerkonto für MFA mit TOTP"

Verwandte Informationen

Weitere Informationen zu "Mehrstufige Authentifizierung in ONTAP 9 (TR-4647)".

Konfigurieren Sie das lokale Benutzerkonto für MFA mit TOTP

Ab ONTAP 9.13.1 können Benutzerkonten mit Multi-Faktor-Authentifizierung (MFA) unter Verwendung eines zeitbasierten Einmalpasswords (TOTP) konfiguriert werden.

Bevor Sie beginnen

- Der Storage-Administrator muss "Aktivieren Sie MFA mit TOTP" Als zweite Authentifizierungsmethode für Ihr Benutzerkonto.
- Die primäre Authentifizierungsmethode für das Benutzerkonto 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-Schlüssel erstellt.

  TOTP wird von verschiedenen Authentifikator-Apps wie Google Authenticator unterstützt.

Schritte

1. Melden Sie sich mit Ihrer aktuellen Authentifizierungsmethode bei Ihrem Benutzerkonto an.

   Die aktuelle Authentifizierungsmethode sollte ein Benutzerpasswort oder ein öffentlicher SSH-Schlüssel sein.

2. Erstellen Sie die TOTP-Konfiguration für Ihr Konto:

   ```
   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>"
```

TOTP-Schlüssel zurücksetzen

Um die Sicherheit deines Kontos zu schützen, solltest du den TOTP-Schlüssel deaktivieren und einen neuen erstellen, wenn er kompromittiert oder verloren ist.

Setzen Sie TOTP zurück, wenn Ihr Schlüssel kompromittiert ist

Wenn Ihr TOTP-Schlüssel kompromittiert ist, Sie aber trotzdem Zugriff darauf haben, können Sie den kompromittierten Schlüssel entfernen und einen neuen erstellen.

1. Melden Sie sich mit Ihrem Benutzerkennwort oder dem öffentlichen SSH-Schlüssel und Ihrem kompromittierten TOTP-Schlüssel bei Ihrem Benutzerkonto an.
2. Entfernen Sie den kompromittierten TOTP-Schlüssel:

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

3. Neuen TOTP-Schlüssel 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>
   ```

Setzen Sie TOTP zurück, wenn Ihr Schlüssel verloren geht

Wenn Ihr TOTP-Geheimschlüssel verloren geht, wenden Sie sich an Ihren Speicheradministrator "Lassen Sie den Schlüssel deaktiviert". Nachdem der Schlüssel deaktiviert wurde, können Sie sich mit Ihrer ersten Authentifizierungsmethode anmelden und ein neues TOTP konfigurieren.

Bevor Sie beginnen

Der TOTP-Schlüssel muss von einem Speicheradministrator deaktiviert werden. Wenn Sie kein Storage-Administratorkonto haben, wenden Sie sich an Ihren Storage-Administrator, um den Schlüssel zu deaktivieren.

Schritte

1. Nachdem der TOTP-Schlüssel von einem Speicheradministrator deaktiviert wurde, melden Sie sich mit Ihrer primären Authentifizierungsmethode bei Ihrem lokalen Konto an.

2. Neuen TOTP-Schlüssel 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>
```

Deaktivieren Sie den geheimen TOTP-Schlüssel für das lokale Konto

Wenn der zeitbasierte TOTP-Schlüssel (One-Time Password) eines lokalen Benutzers verloren geht, 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 über ein Cluster-Administratorkonto ausgeführt werden.

Schritt

1. Deaktivieren Sie den geheimen TOTP-Schlüssel:

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

Copyright-Informationen

Copyright © 2024 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.