Abilitare gli account MFA (Multiple Factor Authentication)

ONTAP 9

NetApp
April 24, 2024

Sommario

Abilitare gli account MFA (Multiple Factor Authentication)

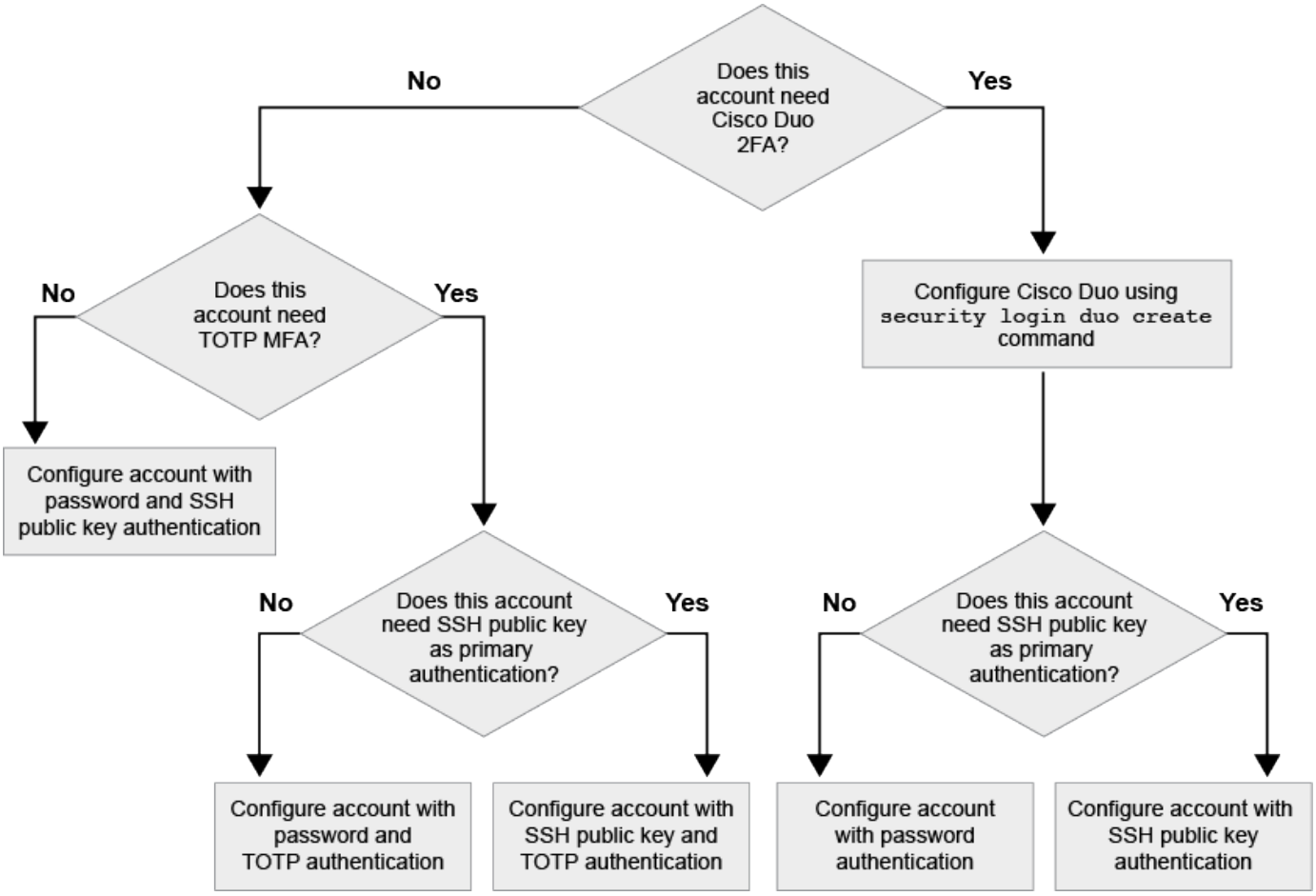
Panoramica dell’autenticazione a più fattori

La Multifactor Authentication (MFA) consente di migliorare la sicurezza richiedendo agli utenti di fornire due metodi di autenticazione per l’accesso a una VM di amministrazione o per lo storage dei dati.

A seconda della versione di ONTAP in uso, è possibile utilizzare una combinazione di chiave pubblica SSH, una password utente e una password monouso (TOTP) basata sul tempo per l’autenticazione multifattore. Quando si attiva e si configura Cisco Duo (ONTAP 9.14.1 e versioni successive), questo metodo funge da metodo di autenticazione aggiuntivo, che integra i metodi esistenti per tutti gli utenti.

Disponibile a partire da…	Primo metodo di autenticazione	Secondo metodo di autenticazione
ONTAP 9.14.1	Chiave pubblica SSH	TTP
	User Password (Password utente)	TTP
	Chiave pubblica SSH	Cisco Duo
	Password utente	Cisco Duo
ONTAP 9.13.1	Chiave pubblica SSH	TTP
	Password utente	TTP
ONTAP 9.3	Chiave pubblica SSH	Password utente

Se MFA è configurato, l’amministratore del cluster deve prima abilitare l’account utente locale, quindi l’account deve essere configurato dall’utente locale.



Abilitare l'autenticazione a più fattori

L'autenticazione a più fattori (MFA) consente di migliorare la sicurezza richiedendo agli utenti di fornire due metodi di autenticazione per accedere a un'SVM amministrativa o di dati.

A proposito di questa attività

- Per eseguire questa attività, è necessario essere un amministratore del cluster.
- Se non si è sicuri del ruolo di controllo degli accessi che si desidera assegnare all'account di accesso, è possibile utilizzare `security login modify` per aggiungere il ruolo in un secondo momento.

  "Modifica del ruolo assegnato a un amministratore"

- Se si utilizza una chiave pubblica per l'autenticazione, è necessario associare la chiave pubblica all'account prima che l'account possa accedere a SVM.

  "Associare una chiave pubblica a un account utente"

  È possibile eseguire questa attività prima o dopo aver attivato l'accesso all'account.

- A partire da ONTAP 9.12.1, è possibile utilizzare i dispositivi di autenticazione hardware di Yubikey per l'autenticazione MFA del client SSH utilizzando gli standard di autenticazione FIDO2 (Fast Identity Online) o Personal Identity Verification (PIV).

Abilitare MFA con chiave pubblica SSH e password utente

A partire da ONTAP 9.3, un amministratore del cluster può configurare account utente locali per l'accesso con MFA utilizzando una chiave pubblica SSH e una password utente.

1. Abilitare MFA sull'account utente locale con chiave pubblica SSH e password utente:

   ```
   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>
   ```

   Il seguente comando richiede l'account amministratore SVM `admin2` con il predefinito `admin` Ruolo di accesso a SVM`engData1` Con una chiave pubblica SSH e una password utente:

   ```
   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".
   ```

Abilitare MFA con TOTP

A partire da ONTAP 9.13.1, è possibile migliorare la sicurezza richiedendo agli utenti locali di accedere a un server di amministrazione o a una SVM di dati con una chiave pubblica SSH o una password utente e una password monouso (TOTP) basata sul tempo. Una volta abilitato l'account MFA con TOTP, l'utente locale deve effettuare l'accesso a. "completare la configurazione".

TOTP è un algoritmo per computer che utilizza l'ora corrente per generare una password monouso. Se si utilizza il protocollo TOTP, si tratta sempre della seconda forma di autenticazione dopo la chiave pubblica SSH o la password dell'utente.

Prima di iniziare

Per eseguire queste attività, è necessario essere un amministratore dello storage.

Fasi

È possibile impostare MFA su con una password utente o una chiave pubblica SSH come primo metodo di autenticazione e TOTP come secondo metodo di autenticazione.

Abilitare MFA con password utente e TOTP

1. Abilitare un account utente per l'autenticazione a più fattori con una password utente e TOTP.

   Per nuovi account utente

   ```
   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>
   ```

   Per gli account utente esistenti

   ```
   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. Verificare che MFA con TOTP sia attivato:

   ```
   security login show
   ```

Abilitare MFA con chiave pubblica SSH e TOTP

1. Abilitare un account utente per l'autenticazione a più fattori con una chiave pubblica SSH e TOTP.

   Per nuovi account utente

   ```
   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>
   ```

   Per gli account utente esistenti

   ```
   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. Verificare che MFA con TOTP sia attivato:

```
security login show
```

Al termine

- Se non è stata associata una chiave pubblica all'account amministratore, è necessario farlo prima che l'account possa accedere a SVM.

  "Associazione di una chiave pubblica a un account utente"

- L'utente locale deve effettuare l'accesso per completare la configurazione MFA con TOTP.

  "Configurare l'account utente locale per MFA con TOTP"

Informazioni correlate

Scopri di più "Autenticazione multifattore in ONTAP 9 (TR-4647)".

Configurare l'account utente locale per MFA con TOTP

A partire da ONTAP 9.13.1, gli account utente possono essere configurati con autenticazione multifattore (MFA) utilizzando una password monouso (TTP) basata sul tempo.

Prima di iniziare

- L'amministratore dello storage deve "Abilitare MFA con TOTP" come secondo metodo di autenticazione per l'account utente.
- Il metodo di autenticazione dell'account utente principale deve essere una password utente o una chiave SSH pubblica.
- È necessario configurare l'applicazione TOTP per il funzionamento con lo smartphone e creare la chiave segreta TOTP.

  TOTP è supportato da diverse applicazioni di autenticazione come Google Authenticator.

Fasi

1. Accedere all'account utente con il metodo di autenticazione corrente.

   Il metodo di autenticazione corrente deve essere una password utente o una chiave pubblica SSH.

2. Creare la configurazione TOTP sull'account:

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

3. Verificare che la configurazione TOTP sia attivata sull'account:

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

Reimpostare la chiave segreta TOTP

Per proteggere la sicurezza del tuo account, se la tua chiave segreta TOTP viene compromessa o persa, devi disattivarla e crearne una nuova.

Reimpostare il TOTP se la chiave viene compromessa

Se la chiave segreta TOTP è compromessa, ma si dispone ancora dell'accesso, è possibile rimuovere la chiave compromessa e crearne una nuova.

1. Accedere all'account utente con la password utente o la chiave pubblica SSH e la chiave segreta TOTP compromessa.
2. Rimuovere la chiave segreta TOTP compromessa:

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

3. Creare una nuova chiave segreta TOTP:

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

4. Verificare che la configurazione TOTP sia attivata sull'account:

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

Ripristinare il TOTP se la chiave viene persa

Se la chiave segreta TOTP viene persa, contattare l'amministratore dello storage per "disattivare la chiave". Una volta disattivata la chiave, è possibile utilizzare il primo metodo di autenticazione per accedere e configurare un nuovo TOTP.

Prima di iniziare

La chiave segreta TOTP deve essere disattivata da un amministratore dello storage. Se non si dispone di un account amministratore dello storage, contattare l'amministratore dello storage per disattivare la chiave.

Fasi

1. Una volta disattivato il segreto TOTP da un amministratore dello storage, utilizzare il metodo di autenticazione principale per accedere all'account locale.

2. Creare una nuova chiave segreta TOTP:

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

3. Verificare che la configurazione TOTP sia attivata sull'account:

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

Disattiva la chiave segreta TOTP per l'account locale

Se la chiave segreta TOTP (Time-Based One-Time Password) di un utente locale viene persa, la chiave persa deve essere disattivata da un amministratore dello storage prima che l'utente possa creare una nuova chiave segreta TOTP.

A proposito di questa attività

Questa attività può essere eseguita solo da un account amministratore del cluster.

Fase

1. Disattivare la chiave segreta TOTP:

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