多要素認証（MFA）アカウントを有効にする
ONTAP 9

NetApp
December 20, 2024

This PDF was generated from https://docs.netapp.com/ja-jp/ontap/authentication/mfa-overview.html on December 20, 2024. Always check docs.netapp.com for the latest.

目次

多要素認証（MFA）アカウントを有効にする

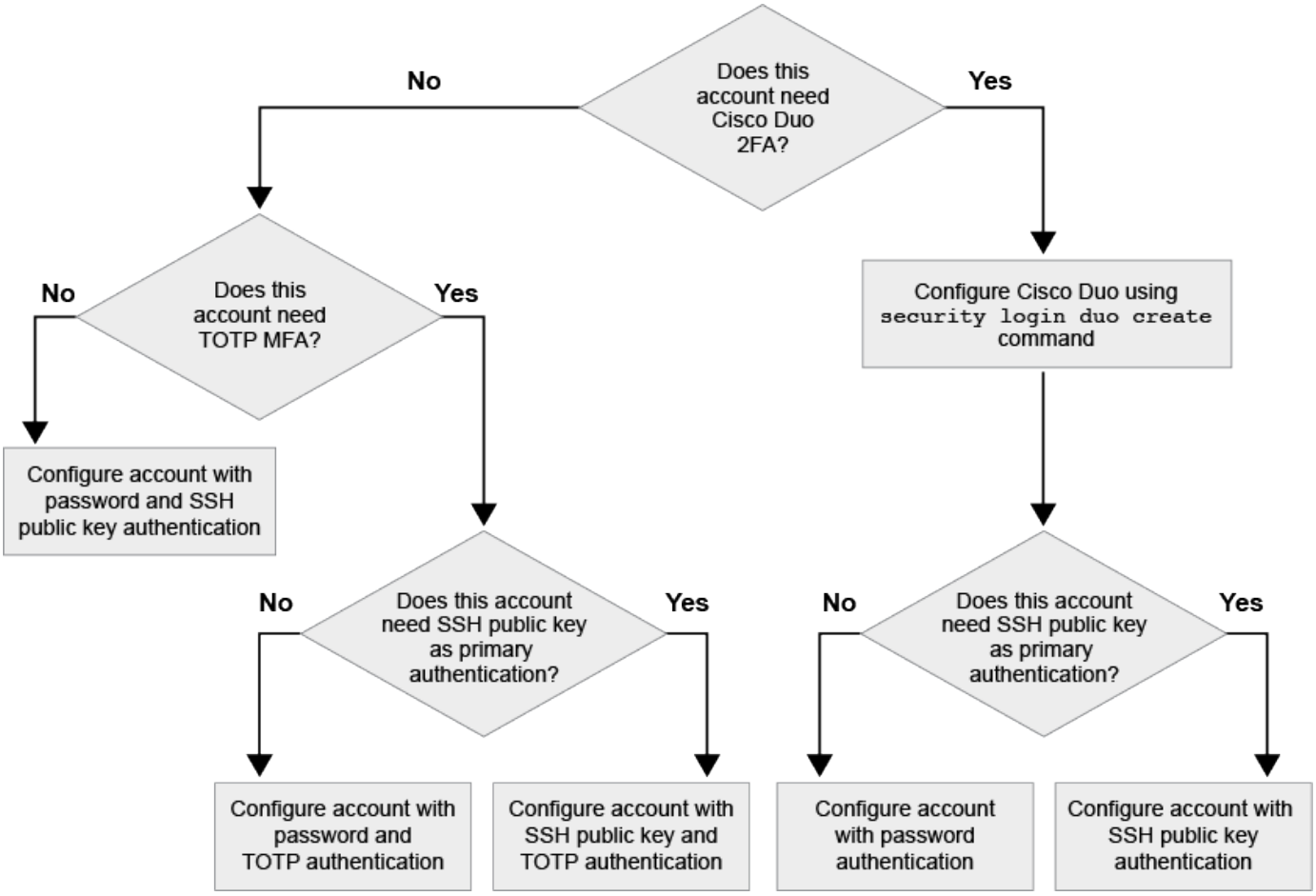
多要素認証の概要

多要素認証（MFA）を使用すると、ユーザが管理Storage VMまたはデータStorage VMにログインする際に2つの認証方式を指定する必要があるため、セキュリティを強化できます。

ONTAPのバージョンに応じて、SSH公開鍵、ユーザパスワード、および時間ベースのワンタイムパスワード（TOTP）を組み合わせて多要素認証に使用できます。Cisco Duo（ONTAP 9 14.1以降）を有効にして設定すると、追加の認証方式として機能し、すべてのユーザの既存の方式を補完します。

使用可能なバージョン	最初の認証方法	**2**番目の認証方法
ONTAP 9 .14.1	SSH公開鍵	TOTP
	ユーザパスワード	TOTP
	SSH公開鍵	Cisco Duo
	ユーザパスワード	Cisco Duo
ONTAP 9 .13.1	SSH公開鍵	TOTP
	ユーザパスワード	TOTP
ONTAP 9.3	SSH公開鍵	ユーザパスワード

MFAが設定されている場合は、クラスタ管理者が最初にローカルユーザアカウントを有効にしてから、ローカルユーザがアカウントを設定する必要があります。



多要素認証を有効にする

多要素認証（MFA）を使用すると、管理SVMまたはデータSVMにログインする際にユーザに2つの認証方式の指定を要求することで、セキュリティを強化できます。

タスクの内容

- このタスクを実行するには、クラスタ管理者である必要があります。
- ログインアカウントに割り当てるアクセス制御ロールが不明な場合は、あとでコマンドを使用してロールを追加できます `security login modify`。

  "管理者に割り当てられているロールの変更"

- 認証に公開鍵を使用している場合は、アカウントがSVMにアクセスする前にアカウントに公開鍵を関連付ける必要があります。

  "ユーザアカウントに公開鍵を関連付ける"

  このタスクは、アカウントアクセスを有効にする前後どちらでも実行できます。

- ONTAP 9.12.1以降では、FIDO2（Fast Identity Online）またはPIV（Personal Identity Verification）認証標準を使用して、SSHクライアントMFAにYubikeyハードウェア認証デバイスを使用できます。

SSH公開鍵とユーザパスワードを使用してMFAを有効にする

3以降では、クラスタ管理者がONTAP 9公開鍵とユーザパスワードを使用して、MFAを使用してログインするためのローカルユーザアカウントを設定できます。

1. ローカルユーザアカウントでSSH公開鍵とユーザパスワードを使用してMFAを有効にします。

```
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>
```

次のコマンドでは、事前定義された `admin`ロールのSVM管理者アカウントで、SSH公開鍵とユーザパスワードの両方を使用してSVMにログインするengData1必要があり `admin2`ます。

```
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".
```

TOTPでMFAを有効にする

SSH.13.1以降では、ONTAP 9公開鍵またはユーザパスワードと時間ベースのワンタイムパスワード（TOTP）の両方を使用してローカルユーザに管理SVMまたはデータSVMへのログインを要求することで、セキュリティを強化できます。TOTPを使用してMFAのアカウントを有効にしたあと、ローカルユーザはにログインする必要があります"設定を完了します"。

TOTPは、現在の時刻を使用してワンタイムパスワードを生成するコンピュータアルゴリズムです。TOTPを使用する場合は、常にSSH公開鍵またはユーザパスワードに続く2番目の認証形式になります。

開始する前に

これらのタスクを実行するには、ストレージ管理者である必要があります。

手順

最初の認証方法としてユーザパスワードまたはSSH公開鍵を使用し、2番目の認証方法としてTOTPを使用してMFAを設定できます。

ユーザパスワードと**TOTP**で**MFA**を有効にする

1. ユーザパスワードとTOTPを使用して、ユーザアカウントで多要素認証を有効にします。

   新規ユーザーアカウントの場合

   ```
   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>
   ```

   既存のユーザーアカウントの場合

   ```
   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. TOTPを使用したMFAが有効になっていることを確認します。

   ```
   security login show
   ```

SSH公開鍵と**TOTP**を使用して**MFA**を有効にする

1. SSH公開鍵とTOTPを使用した多要素認証のユーザアカウントを有効にします。

   新規ユーザーアカウントの場合

   ```
   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>
   ```

   既存のユーザーアカウントの場合

   ```
   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. TOTPを使用したMFAが有効になっていることを確認します。

```
security login show
```

終了後

- 管理者アカウントに公開鍵が関連付けられていない場合は、アカウントがSVMにアクセスする前に関連付けておく必要があります。

  "ユーザアカウントへの公開鍵の関連付け"

- TOTPを使用したMFAの設定を完了するには、ローカルユーザがログインする必要があります。

  "TOTPを使用したMFA用のローカルユーザアカウントの設定"

関連情報

詳細については、をご覧ください "ONTAP 9での多要素認証（TR-4647）"。

TOTPを使用したMFA用のローカルユーザアカウントの設定

ONTAP 9 .13.1以降では、時間ベースのワンタイムパスワード（TOTP）を使用して多要素認証（MFA）でユーザアカウントを設定できます。

開始する前に

- ユーザアカウントの第2の認証方法として、ストレージ管理者が必要です"TOTPでMFAを有効にする"。
- プライマリユーザアカウントの認証方法は、ユーザパスワードまたは公開SSHキーである必要があります。
- スマートフォンと連携するようにTOTPアプリを設定し、TOTPシークレットキーを作成する必要があります。

  Microsoft Authenticator、Google Authenticator、Authy、およびその他のTOTP互換オーセンティケータがサポートされています。

手順

1. 現在の認証方法でユーザーアカウントにログインします。

   現在の認証方法は、ユーザパスワードまたはSSH公開鍵である必要があります。

2. アカウントでTOTP設定を作成します。

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

3. アカウントでTOTP設定が有効になっていることを確認します。

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

TOTPシークレットキーのリセット

アカウントのセキュリティを保護するために、TOTPシークレットキーが侵害されたり紛失したりした場合は、それを無効にして新しいシークレットキーを作成する必要があります。

キーが侵害された場合にTOTPをリセット

TOTPシークレットキーが侵害されたにもかかわらずアクセスできる場合は、侵害されたキーを削除して新しいキーを作成できます。

1. ユーザパスワードまたはSSH公開鍵と侵害されたTOTPシークレットキーを使用してユーザアカウントにログインします。
2. 侵害されたTOTPシークレットキーを削除します。

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

3. 新しいTOTPシークレットキーを作成します。

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

4. アカウントでTOTP設定が有効になっていることを確認します。

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

キーを紛失した場合にTOTPをリセット

TOTPシークレットキーが失われた場合は、ストレージ管理者にに問い合わせてください"キーを無効にします"。キーが無効になったら、最初の認証方法を使用してログインし、新しいTOTPを設定できます。

開始する前に

ストレージ管理者がTOTPシークレットキーを無効にする必要があります。ストレージ管理者アカウントがない場合は、ストレージ管理者に連絡してキーを無効にしてください。

手順

1. ストレージ管理者がTOTPシークレットを無効にしたら、プライマリの認証方法を使用してローカルアカウントにログインします。
2. 新しいTOTPシークレットキーを作成します。

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

3. アカウントでTOTP設定が有効になっていることを確認します。

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

ローカルアカウントの**TOTP**シークレットキーを無効にする

ローカルユーザの時間ベースのワンタイムパスワード（TOTP）シークレットキーが失われた場合、失われたキーをストレージ管理者が無効にしてからユーザが新しいTOTPシークレットキーを作成する必要があります。

タスクの内容

このタスクは、クラスタ管理者アカウントからのみ実行できます。

ステップ

1. TOTPシークレットキーを無効にします。

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

著作権に関する情報

Copyright © 2024 NetApp, Inc. All Rights Reserved. Printed in the U.S.このドキュメントは著作権によって保護されています。著作権所有者の書面による事前承諾がある場合を除き、画像媒体、電子媒体、および写真複写、記録媒体、テープ媒体、電子検索システムへの組み込みを含む機械媒体など、いかなる形式および方法による複製も禁止します。

ネットアップの著作物から派生したソフトウェアは、次に示す使用許諾条項および免責条項の対象となります。

このソフトウェアは、ネットアップによって「現状のまま」提供されています。ネットアップは明示的な保証、または商品性および特定目的に対する適合性の暗示的保証を含み、かつこれに限定されないいかなる暗示的な保証も行いません。ネットアップは、代替品または代替サービスの調達、使用不能、データ損失、利益損失、業務中断を含み、かつこれに限定されない、このソフトウェアの使用により生じたすべての直接的損害、間接的損害、偶発的損害、特別損害、懲罰的損害、必然的損害の発生に対して、損失の発生の可能性が通知されていたとしても、その発生理由、根拠とする責任論、契約の有無、厳格責任、不法行為（過失またはそうでない場合を含む）にかかわらず、一切の責任を負いません。

ネットアップは、ここに記載されているすべての製品に対する変更を随時、予告なく行う権利を保有します。ネットアップによる明示的な書面による合意がある場合を除き、ここに記載されている製品の使用により生じる責任および義務に対して、ネットアップは責任を負いません。この製品の使用または購入は、ネットアップの特許権、商標権、または他の知的所有権に基づくライセンスの供与とはみなされません。

このマニュアルに記載されている製品は、1つ以上の米国特許、その他の国の特許、および出願中の特許によって保護されている場合があります。

権利の制限について：政府による使用、複製、開示は、DFARS 252.227-7013（2014年2月）およびFAR 5252.227-19（2007年12月）のRights in Technical Data -Noncommercial Items（技術データ - 非商用品目に関する諸権利）条項の(b)(3)項、に規定された制限が適用されます。

本書に含まれるデータは商用製品および / または商用サービス（FAR 2.101の定義に基づく）に関係し、データの所有権はNetApp, Inc.にあります。本契約に基づき提供されるすべてのネットアップの技術データおよびコンピュータ ソフトウェアは、商用目的であり、私費のみで開発されたものです。米国政府は本データに対し、非独占的かつ移転およびサブライセンス不可で、全世界を対象とする取り消し不能の制限付き使用権を有し、本データの提供の根拠となった米国政府契約に関連し、当該契約の裏付けとする場合にのみ本データを使用できます。前述の場合を除き、NetApp, Inc.の書面による許可を事前に得ることなく、本データを使用、開示、転載、改変するほか、上演または展示することはできません。国防総省にかかる米国政府のデータ使用権については、DFARS 252.227-7015(b)項（2014年2月）で定められた権利のみが認められます。

商標に関する情報

NetApp、NetAppのロゴ、http://www.netapp.com/TMに記載されているマークは、NetApp, Inc.の商標です。その他の会社名と製品名は、それを所有する各社の商標である場合があります。