多要素認証（MFA）アカウントの有効化

ONTAP 9

NetApp
February 12, 2026

目次

多要素認証（MFA）アカウントの有効化

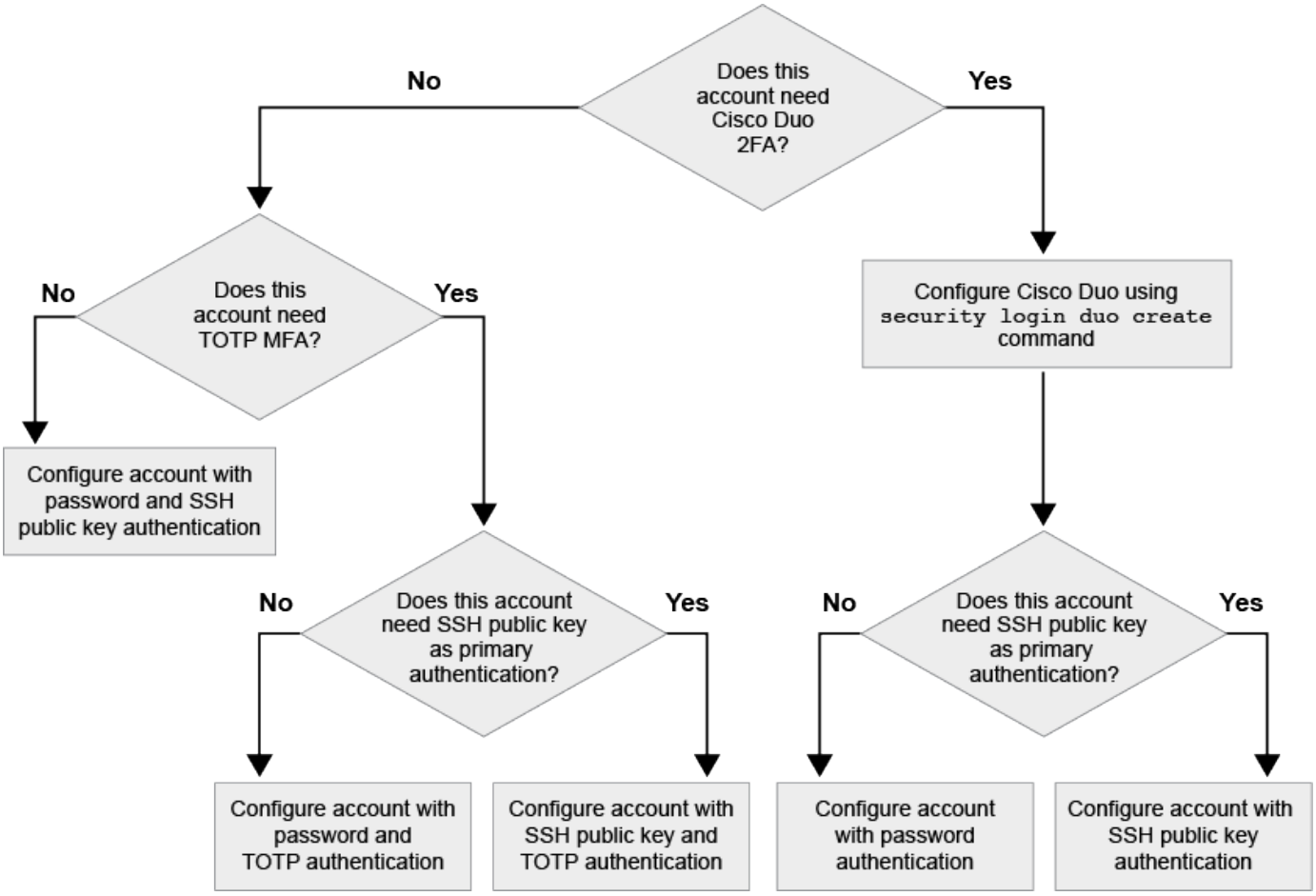
ONTAP多要素認証について学ぶ

多要素認証（MFA）では、管理VMやデータStorage VMにログインする際にユーザに2つの認証方式を要求することで、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、Time-based One-Time Password（TOTP）を組み合わせて多要素認証を行えます。Cisco Duoを有効にして設定すると（ONTAP 9.14.1以降）、すべてのユーザの既存の方式を補完する追加の認証方式として機能します。

追加されたリリース	第**1**の認証方式	第**2**の認証方式
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、最初にクラスタ管理者がローカル 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。



SSHとTOTPを使用してONTAP多要素認証を有効にする

多要素認証（MFA）では、管理SVMやデータSVMにログインする際にユーザに2つの認証方式を要求することで、セキュリティを強化できます。

タスク概要

- 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、 `security login modify` コマンドを使用して後でロールを追加できます。

  `security login modify`の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/security-login-modify.html["ONTAPコマンド リファレンス"^]を参照してください。

  "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、アカウントがSVMにアクセスするためには、アカウントに公開鍵を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"

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 パスワードを使用するMFAの有効化

ONTAP 9.3以降、クラスタ管理者は、SSH公開鍵とユーザ パスワードを使用してMFAでログインするようにローカル ユーザ アカウントを設定できます。

1. ローカル ユーザ アカウントに対して、SSH公開鍵とユーザパスワードを使用するMFAを有効化します。

```
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`ロールを持つ SVM 管理者アカウント `admin2`が SSH 公開キーとユーザーパスワードの両方を使用して SVMengData1にログインする必要があります：

```
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".
```

`security login create`の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/security-login-create.html["ONTAPコマンド リファレンス"^]をご覧ください。

TOTPを使用するMFAの有効化

ONTAP 9.13.1以降では、ローカルユーザにSSH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）の両方を使用して管理SVMまたはデータSVMにログインすることを要求することで、セキュリティを強化できます。アカウントでTOTPを使用したMFAが有効になった後、ローカルユーザは"設定を完了する"にログインする必要があります。

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は、必ずSSH公開鍵またはユーザ パスワードに続く第2の認証方式として使用します。

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

第1の認証方式にユーザ パスワードまたはSSH公開鍵を使用し、第2の認証方式にTOTPを使用するようにMFAを設定できます。

ユーザ パスワードと**TOTP**を使用する**MFA**の有効化

1. ユーザ アカウントに対して、ユーザ パスワードとTOTPを使用する多要素認証を有効化します。

   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を使用する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**を使用する**MFA**の有効化

1. SSH公開鍵とTOTPを使用する多要素認証を有効化します。

   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>
   ```

`security login modify`
の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/security-login-modify.html["ONTAPコマンド リファレンス"^]を参照してください。

2. TOTPを使用するMFAが有効になっていることを確認します。

```
security login show
```

`security login show`の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/security-login-show.html["ONTAPコマンド リファレンス"^]を参照してください。

終了後の操作

- 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、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"

- ローカル ユーザがログインし、TOTPを使用するMFAの設定を完了する必要があります。

  "ローカル ユーザ アカウントでのTOTPを使用するMFAの設定"

関連情報

- "ONTAP 9 における多要素認証（TR-4647）"
- "ONTAPコマンド リファレンス"

TOTPを使用したMFA用のローカルONTAPユーザーアカウントを構成する

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）を使用した多要素認証（MFA）でユーザーアカウントを設定できます。

開始する前に

- ストレージ管理者は、ユーザーアカウントの2番目の認証方法として"TOTPでMFAを有効にする"を設定する必要があります。
- ユーザ アカウントの第1の認証方式が、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。
- スマートフォンにTOTPアプリを設定し、TOTPシークレット キーを作成しておく必要があります。

  Microsoft Authenticator、Google Authenticator / Google認証システム、AuthyなどのTOTP互換認証コード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 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. アカウントに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>"
```

関連情報

- "セキュリティログイン TOTP 作成"
- "security login totp show"

ONTAPユーザーアカウントのTOTP秘密キーをリセットします

アカウントのセキュリティを確保するために、TOTPシークレット キーが侵害されたり、キーを紛失した場合、既存のキー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。

キー侵害時のTOTPのリセット

TOTPシークレット キーが侵害されたが引き続き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>
```

キー紛失時のTOTPのリセット

TOTP 秘密キーを紛失した場合は、ストレージ管理者に連絡して"キーが無効になっている"してください。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。ストレージ管理者でない場合は、ストレージ管理者にキーの無効化を依頼してください。

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、第1の認証方式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>
```

関連情報

- "セキュリティログイン TOTP 作成"
- "セキュリティログイン TOTP 削除"
- "security login totp show"

ONTAPユーザーアカウントのTOTPシークレットキーを無効にする

ローカル ユーザのTime-based One-Time Password（TOTP）シークレット キーが失われた場合は、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。

タスク概要

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。

手順

1. TOTPシークレット キーを無効にします。

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

`security login totp modify`
の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/security-login-totp-modify.html["ONTAPコマンド リファレンス"^]を参照してください。