啟用多因素驗證（MFA）帳戶

ONTAP 9

NetApp

February 12, 2026

目錄

啟用多因素驗證（ **MFA** ）帳戶

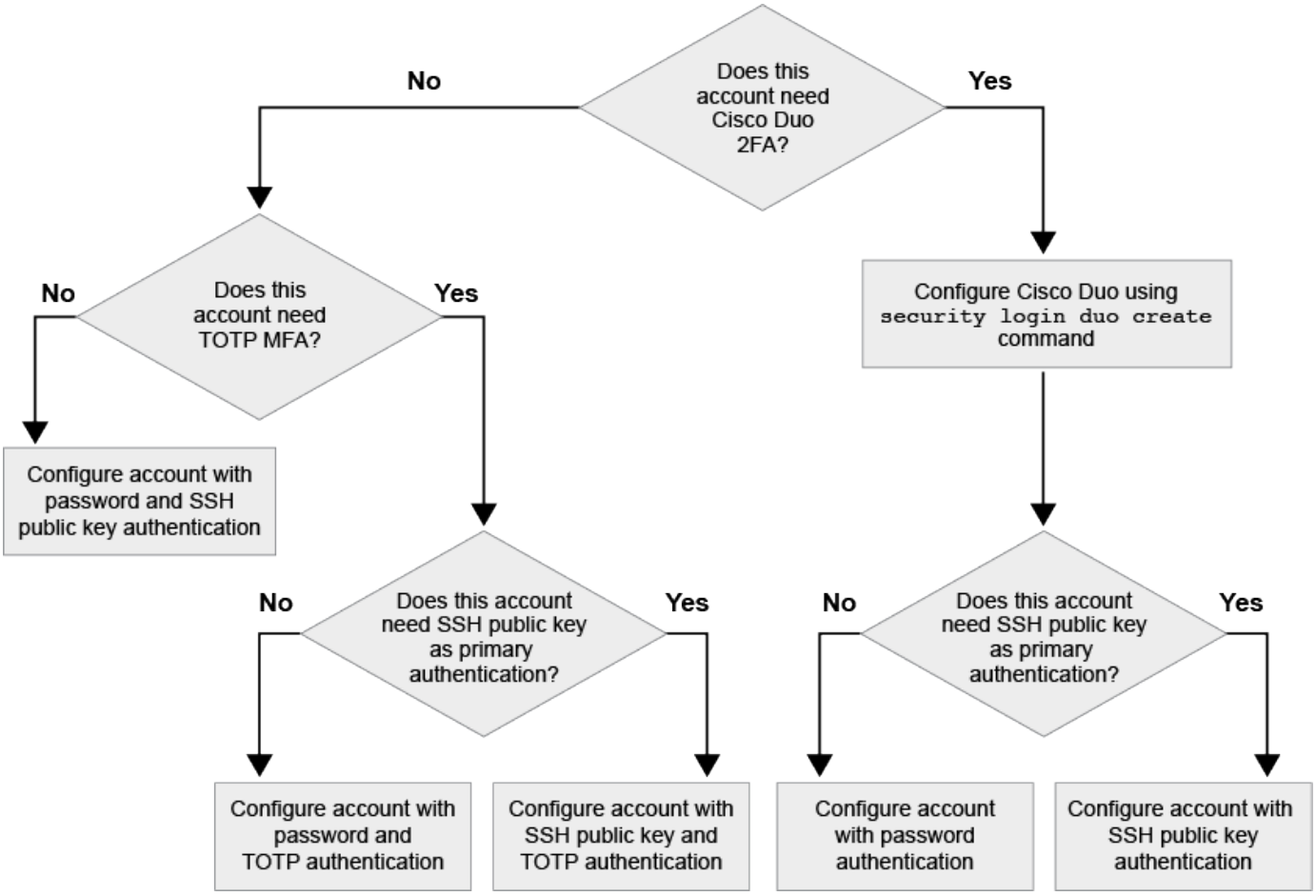
瞭解 **ONTAP** 多因素驗證

多因素驗證（ MFA ）可讓您要求使用者提供兩種驗證方法來登入管理或資料儲存 VM 、以增強安全性。

視您的 ONTAP 版本而定、您可以結合使用 SSH 公開金鑰、使用者密碼和時間型一次性密碼（ TOTP ）進行多因素驗證。當您啟用和設定 Cisco Duo （ ONTAP 9.14.1 及更新版本）時、它會作為額外的驗證方法、以補充所有使用者的現有方法。

可從 ... 開始使用。	第一種驗證方法	第二種驗證方法
ONTAP 9.14.1.	SSH公開金鑰	TOTP
	使用者密碼	TOTP
	SSH公開金鑰	Cisco DuoTM
	使用者密碼	Cisco DuoTM
ONTAP 9.13.1.12.9.11.9.11.	SSH公開金鑰	TOTP
	使用者密碼	TOTP
ONTAP 9.3	SSH公開金鑰	使用者密碼

如果已設定 MFA 、叢集管理員必須先啟用本機使用者帳戶、則該帳戶必須由本機使用者設定。



使用 SSH 和 TOTP 啟用 ONTAP 多因素驗證

多因素驗證（ MFA ）可讓您要求使用者提供兩種驗證方法來登入管理或資料 SVM 、以增強安全性。

關於這項工作

- 您必須是叢集管理員才能執行此工作。
- 如果您不確定要指派給登入帳戶的存取控制角色，可以使用 `security login modify`命令稍後再新增該角色。

  如"指令參考資料ONTAP"需詳細 `security login modify`資訊，請參閱。

  "修改指派給系統管理員的角色"

- 如果您使用公開金鑰進行驗證、則必須先將公開金鑰與帳戶建立關聯、帳戶才能存取 SVM 。

  "將公開金鑰與使用者帳戶建立關聯"

  您可以在啟用帳戶存取之前或之後執行此工作。

- 從S廳9.12.1開始ONTAP 、您可以使用FIDO2（Fast Identity Online）或個人身分驗證（PIV）驗證標準、將Yobikey硬體驗證裝置用於SSH用戶端MFA。

使用 SSH 公開金鑰和使用者密碼來啟用 MFA

從 ONTAP 9.3 開始、叢集管理員可以設定本機使用者帳戶、使用 SSH 公開金鑰和使用者密碼登入 MFA 。

1. 使用 SSH 公開金鑰和使用者密碼、在本機使用者帳戶上啟用 MFA ：

```
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>
```

下列命令需要 SVM 系統管理員帳戶 `admin2` 使用預先定義的 `admin` 登入 SVM 的角色`engData1` 使用 SSH 公開金鑰和使用者密碼：

```
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".
```

如"指令參考資料ONTAP"需詳細 `security login create`資訊，請參閱。

使用 TOTP 啟用 MFA

從 ONTAP 9.13.1 開始、您可以要求本機使用者同時使用 SSH 公開金鑰或使用者密碼和時間型一次性密碼（ TOTP ）登入管理或資料 SVM 、以增強安全性。啟用 MFA 與 TOTP 的帳戶後、本機使用者必須登入 "完成組態設定"。

TOTP 是一種電腦演算法、使用目前時間來產生一次性密碼。 如果使用 TOTP 、它永遠是 SSH 公開金鑰或使用者密碼之後的第二種驗證形式。

開始之前

您必須是儲存管理員才能執行這些工作。

步驟

您可以將 MFA 設為使用者密碼或 SSH 公開金鑰做為第一種驗證方法、並將 TOTP 設為第二種驗證方法。

使用使用者密碼和 **TOTP** 啟用 **MFA**

1. 使用使用者密碼和 TOTP 啟用多因素驗證的使用者帳戶。

   ◦ 適用於新使用者帳戶 *

   ```
   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>
   ```

   ◦ 適用於現有使用者帳戶 *

   ```
   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. 確認 MFA 已啟用 TOTP ：

   ```
   security login show
   ```

使用 **SSH** 公開金鑰和 **TOTP** 啟用 **MFA**

1. 使用 SSH 公開金鑰和 TOTP 啟用多因素驗證的使用者帳戶。

   ◦ 適用於新使用者帳戶 *

   ```
   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>
   ```

   ◦ 適用於現有使用者帳戶 *

   ```
   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>
   ```

   + 如"指令參考資料ONTAP"需詳細 `security login modify`資訊，請參閱。

2. 確認 MFA 已啟用 TOTP ：

```
security login show
```

如"指令參考資料ONTAP"需詳細 `security login show`資訊，請參閱。

完成後

- 如果您尚未將公開金鑰與系統管理員帳戶建立關聯、則必須先建立公開金鑰、帳戶才能存取SVM。

  "將公開金鑰與使用者帳戶建立關聯"

- 本機使用者必須登入才能使用 TOTP 完成 MFA 組態。

  "使用 TOTP 設定 MFA 的本機使用者帳戶"

相關資訊

- "支援多因素驗證ONTAP 功能（TR-4647）"
- "指令參考資料ONTAP"

使用 TOTP 設定 MFA 的本機 ONTAP 使用者帳戶

從 ONTAP 9.13.1 開始，使用者帳戶可以使用時間型一次性密碼（ TOTP ）來設定多因素驗證（ MFA ）。

開始之前

- 儲存管理員必須 "使用 TOTP 啟用 MFA" 作為使用者帳戶的第二種驗證方法。
- 您的主要使用者帳戶驗證方法應為使用者密碼或公開 SSH 金鑰。
- 您必須將 TOTP 應用程式設定為與智慧型手機搭配使用、並建立 TOTP 秘密金鑰。

  支援 Microsoft Authenticator 、 Google Authenticator 、 Authy 及任何其他 TOTP 相容驗證器。

步驟

1. 使用目前的驗證方法登入您的使用者帳戶。

   您目前的驗證方法應該是使用者密碼或 SSH 公開金鑰。

2. 在您的帳戶上建立 TOTP 組態：

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

3. 確認您的帳戶已啟用 TOTP 組態：

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

相關資訊

- "安全登入 totp 創建"
- "安全登入 totp 顯示"

重設 ONTAP 使用者帳戶的 TOTP 秘密金鑰

為了保護您的帳戶安全、如果 TOTP 秘密金鑰遭到洩漏或遺失、您應該停用該金鑰並建立新的金鑰。

如果金鑰遭到入侵、請重設 TOTP

如果您的 TOTP 秘密金鑰已洩漏、但您仍有權存取、您可以移除洩漏的金鑰並建立新的金鑰。

1. 使用您的使用者密碼或 SSH 公開金鑰、以及您遭入侵的 TOTP 秘密金鑰、登入您的使用者帳戶。
2. 移除遭入侵的 TOTP 秘密金鑰：

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

3. 建立新的 TOTP 秘密金鑰：

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

4. 確認您的帳戶已啟用 TOTP 組態：

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

如果金鑰遺失、請重設 TOTP

如果 TOTP 秘密金鑰遺失、請聯絡您的儲存管理員 "停用金鑰"。停用金鑰後、您可以使用第一種驗證方法登入並設定新的 TOTP 。

開始之前

TOTP 秘密金鑰必須由儲存管理員停用。 如果您沒有儲存管理員帳戶、請聯絡您的儲存管理員以停用金鑰。

步驟

1. 儲存管理員停用 TOTP 密碼後、請使用主要驗證方法登入您的本機帳戶。
2. 建立新的 TOTP 秘密金鑰：

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

3. 確認您的帳戶已啟用 TOTP 組態：

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

相關資訊

- "安全登入 totp 創建"
- "安全登入 totp 刪除"
- "安全登入 totp 顯示"

停用 ONTAP 使用者帳戶的 TOTP 秘密金鑰

如果本機使用者的時間型一次性密碼（ TOTP ）秘密金鑰遺失、則儲存管理員必須先停用遺失的金鑰、使用者才能建立新的 TOTP 秘密金鑰。

關於這項工作

此工作只能從叢集管理員帳戶執行。

步驟

1. 停用 TOTP 秘密金鑰：

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

如"指令參考資料ONTAP"需詳細 `security login totp modify`資訊，請參閱。