



## 啟用本機帳戶存取 ONTAP 9

NetApp  
April 24, 2024

# 目錄

啟用本機帳戶存取.....	1
啟用本機帳戶存取總覽.....	1
啟用密碼帳戶存取 .....	1
啟用SSH公開金鑰帳戶.....	1
啟用多因素驗證（MFA）帳戶 .....	3
啟用SSL憑證帳戶.....	9

# 啟用本機帳戶存取

## 啟用本機帳戶存取總覽

本機帳戶是指帳戶資訊、公開金鑰或安全性憑證位於儲存系統上的帳戶。您可以使用 `security login create` 命令以啟用本機帳戶存取管理或資料 SVM。

## 啟用密碼帳戶存取

您可以使用 `security login create` 命令可讓系統管理員帳戶使用密碼存取管理或資料 SVM。輸入命令後、系統會提示您輸入密碼。

關於這項工作

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` 命令以稍後新增角色。

開始之前

您必須是叢集管理員才能執行此工作。

步驟

1. 讓本機系統管理員帳戶使用密碼存取SVM：

```
security login create -vserver SVM_name -user-or-group-name user_or_group_name  
-application application -authmethod authentication_method -role role -comment  
comment
```

如需完整的命令語法、請參閱 ["工作表"](#)。

下列命令可啟用叢集管理員帳戶 `admin1` 使用預先定義的 `backup` 存取管理 SVM 的角色 `engCluster` 使用密碼。輸入命令後、系統會提示您輸入密碼。

```
cluster1::>security login create -vserver engCluster -user-or-group-name  
admin1 -application ssh -authmethod password -role backup
```

## 啟用SSH公開金鑰帳戶

您可以使用 `security login create` 命令可讓系統管理員帳戶使用 SSH 公開金鑰存取管理或資料 SVM。

關於這項工作

- 您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。

- 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` 命令以稍後新增角色。

如果您想在叢集上啟用FIPS模式、則必須使用支援的金鑰類型來重新設定現有SSH公開金鑰帳戶、而不需要支援的金鑰演算法。在您啟用FIPS之前、應先重新設定帳戶、否則系統管理員驗證將會失敗。

下表指出ONTAP 支援哪些主機金鑰類型演算法來進行支援以利執行支援的SSH連線。這些金鑰類型不適用於設定SSH公用驗證。

發行版ONTAP	FIPS模式支援的金鑰類型	非FIPS模式支援的金鑰類型
9.11.1 及更新版本	ECDSA-SHA2-nistp256	ECDSA-SHA2-nistp256 RSA-SHA2-512 RSA-SHA2-256 SSH-ed25519 SSH-DSS SSH-RSA
9.10.1及更早版本	ECDSA-SHA2-nistp256 SSH-ed25519.	ECDSA-SHA2-nistp256 SSH-ed25519 SSH-DSS SSH-RSA



從 ONTAP 9.11.1 開始、移除對 ssh-ed25519 主機金鑰演算法的支援。

如需詳細資訊、請參閱 ["使用FIPS設定網路安全性"](#)。

#### 開始之前

您必須是叢集管理員才能執行此工作。

#### 步驟

1. 允許本機系統管理員帳戶使用SSH公開金鑰存取SVM：

```
security login create -vserver SVM_name -user-or-group-name user_or_group_name  
-application application -authmethod authentication_method -role role -comment  
comment
```

如需完整的命令語法、請參閱 ["工作表"](#)。

下列命令可啟用 SVM 管理員帳戶 `svmadmin1` 使用預先定義的 `vsadmin-volume` 存取 SVM 的角色 `engData1` 使用 SSH 公開金鑰：

```
cluster1::>security login create -vserver engData1 -user-or-group-name  
svmadmin1 -application ssh -authmethod publickey -role vsadmin-volume
```

#### 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](#)

# 啟用多因素驗證（MFA）帳戶

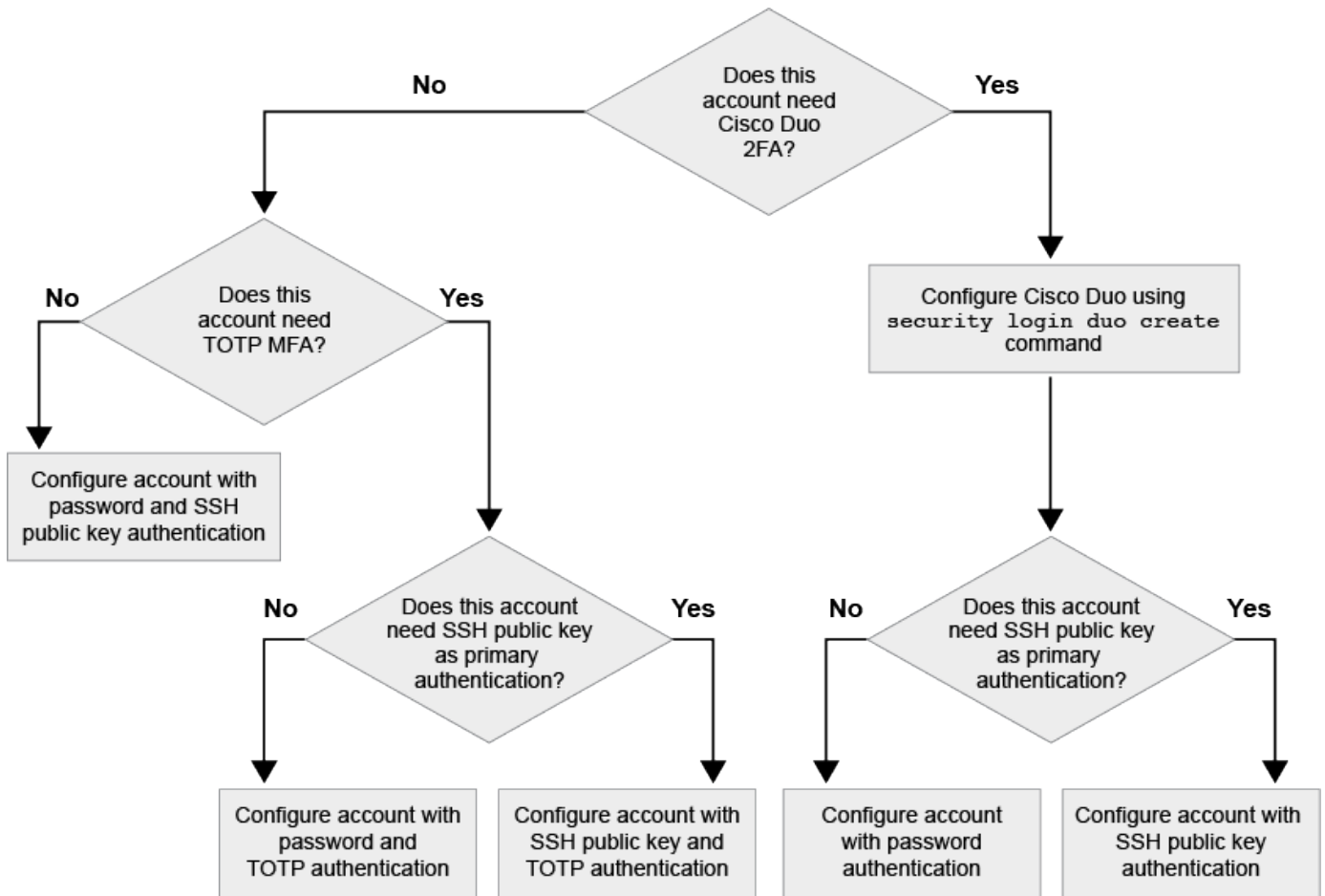
## 多因素驗證總覽

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。



## 啟用多因素驗證

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` 命令以稍後新增角色。

["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Yubikey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".
```

### 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>
```

### 2. 確認 MFA 已啟用 TOTP：



```
security login show
```

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

深入瞭解 ["支援多因素驗證ONTAP 功能（TR-4647）"](#)。

## 使用 TOTP 設定 MFA 的本機使用者帳戶

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。

TOTP 受到各種驗證者應用程式的支援、例如 Google Authenticator。

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>"
```

## 重設 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>
```

## 停用本機帳戶的 **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 delete -vserver "<svm_name>" -username  
"<account_username>"
```

## 啟用**SSL**憑證帳戶

您可以使用 `security login create` 命令可讓系統管理員帳戶使用 SSL 憑證存取管理或資料 SVM。

關於這項工作

- 您必須先安裝CA簽署的伺服器數位憑證、帳戶才能存取SVM。

[產生及安裝CA簽署的伺服器憑證](#)

您可以在啟用帳戶存取之前或之後執行此工作。

- 如果您不確定要指派給登入帳戶的存取控制角色、可以稍後再使用新增該角色 `security login modify` 命令。

[修改指派給系統管理員的角色](#)



對於叢集管理員帳戶、支援憑證驗證 `http`、`ontapi` 和 `rest` 應用程式；對於 SVM 系統管理員帳戶、僅支援憑證驗證 `ontapi` 和 `rest` 應用程式：

步驟

1. 啟用本機系統管理員帳戶、以使用SSL憑證存取SVM：

```
security login create -vserver SVM_name -user-or-group-name user_or_group_name  
-application application -authmethod authentication_method -role role -comment  
comment
```

如需完整的命令語法、請參閱 ["發佈的手冊頁ONTAP"](#)。

下列命令可啟用 SVM 管理員帳戶 `svmin2` 使用預設值 `vsadmin` 存取 SVM 的角色 `engData2` 使用 SSL 數位憑證。

```
cluster1::>security login create -vserver engData2 -user-or-group-name  
svmin2 -application ontapi -authmethod cert
```

完成後

如果您尚未安裝CA簽署的伺服器數位憑證、則必須先安裝該憑證、帳戶才能存取SVM。

[產生及安裝CA簽署的伺服器憑證](#)

## 版權資訊

Copyright © 2024 NetApp, Inc. 版權所有。台灣印製。非經版權所有人事先書面同意，不得將本受版權保護文件的任何部分以任何形式或任何方法（圖形、電子或機械）重製，包括影印、錄影、錄音或儲存至電子檢索系統中。

由 NetApp 版權資料衍伸之軟體必須遵守下列授權和免責聲明：

此軟體以 NETAPP「原樣」提供，不含任何明示或暗示的擔保，包括但不限於有關適售性或特定目的適用性之擔保，特此聲明。於任何情況下，就任何已造成或基於任何理論上責任之直接性、間接性、附隨性、特殊性、懲罰性或衍生性損害（包括但不限於替代商品或服務之採購；使用、資料或利潤上的損失；或企業營運中斷），無論是在使用此軟體時以任何方式所產生的契約、嚴格責任或侵權行為（包括疏忽或其他）等方面，NetApp 概不負責，即使已被告知有前述損害存在之可能性亦然。

NetApp 保留隨時變本文所述之任何產品的權利，恕不另行通知。NetApp 不承擔因使用本文所述之產品而產生的責任或義務，除非明確經過 NetApp 書面同意。使用或購買此產品並不會在依據任何專利權、商標權或任何其他 NetApp 智慧財產權的情況下轉讓授權。

本手冊所述之產品受到一項（含）以上的美國專利、國外專利或申請中專利所保障。

有限權利說明：政府機關的使用、複製或公開揭露須受 DFARS 252.227-7013（2014 年 2 月）和 FAR 52.227-19（2007 年 12 月）中的「技術資料權利 - 非商業項目」條款 (b)(3) 小段所述之限制。

此處所含屬於商業產品和 / 或商業服務（如 FAR 2.101 所定義）的資料均為 NetApp, Inc. 所有。根據本協議提供的所有 NetApp 技術資料和電腦軟體皆屬於商業性質，並且完全由私人出資開發。美國政府對於該資料具有非專屬、非轉讓、非轉授權、全球性、有限且不可撤銷的使用權限，僅限於美國政府為傳輸此資料所訂合約所允許之範圍，並基於履行該合約之目的方可使用。除非本文另有規定，否則未經 NetApp Inc. 事前書面許可，不得逕行使用、揭露、重製、修改、履行或展示該資料。美國政府授予國防部之許可權利，僅適用於 DFARS 條款 252.227-7015(b)（2014 年 2 月）所述權利。

## 商標資訊

NETAPP、NETAPP 標誌及 <http://www.netapp.com/TM> 所列之標章均為 NetApp, Inc. 的商標。文中所涉及的所有其他公司或產品名稱，均為其各自所有者的商標，不得侵犯。