



# 升級 **Health Checker** 文件

## Upgrade Health Checker

NetApp  
March 16, 2026

# 目錄

升級 Health Checker 文件	1
版本資訊	2
Upgrade Health Checker 新增功能	2
2026 年 2 月 13 日	2
開始使用	3
了解 Upgrade Health Checker	3
下載並設定 Upgrade Health Checker	3
使用 Upgrade Health Checker	7
使用 Upgrade Health Checker 產生升級計劃	7
使用 Upgrade Health Checker 自動產生升級計劃	9
了解 Upgrade Health Checker 的輸入參數	11
輸入方法優先順序	11
輸入參數	11
叢集 IP	11
叢集使用者名稱	12
叢集密碼	12
目標 ONTAP 版本	13
接受 EULA	14
設定檔路徑	14
執行輸出路徑	15
跳過相容性檢查	15
停用遙測	16
停用自動更新	16
使用每種輸入方法的範例	16
組合 CLI 參數	16
Config.yaml 檔案	17
互動模式	17
其他命令	17
升級健全狀況檢查程式常見問題	19
Upgrade Health Checker 與 Upgrade Advisor 有何不同？	19
升級健全狀況檢查程式報告包含哪些資訊？	19
Upgrade Health Checker 可以在沒有網際網路連線的情況下使用嗎？	19
Upgrade Health Checker 支援哪些 ONTAP 版本？	19
法律聲明	20
版權	20
商標	20
專利	20
隱私權政策	20
開放原始碼	20

# 升級 Health Checker 文件

# 版本資訊

## Upgrade Health Checker 新增功能

了解 Upgrade Health Checker 的新增功能。您可以透過導航至 ["NetApp Console 自動化中心"](#) 中的 Upgrade Health Checker 磁貼並查看最新的 Upgrade Health Checker 下載檔案，找到更多增強功能資訊。

**2026 年 2 月 13 日**

Upgrade Health Checker 提供了一種全新的解決方案，可產生全面的現場報告，幫助您成功完成 ONTAP 升級。它可以與現有的自動化和編排框架配合使用，從而在升級單一或多個叢集時提高效率。Upgrade Health Checker 支援升級到 ONTAP 9.11.1 及更高版本。

["深入瞭解 Upgrade Health Checker"](#)。

# 開始使用

## 了解 Upgrade Health Checker

Upgrade Health Checker 是一款升級諮詢服務工具，可提供詳細資訊和建議，協助您成功完成 ONTAP 升級。它會進行全面的現場健康檢查，識別您在執行升級之前必須解決的障礙和警告。

Upgrade Health Checker 可以整合到您現有的自動化和編排框架中，以協助您升級單一或多個叢集。它使用您最新的 AutoSupport 資料產生詳細、準確的報告，其中包含與叢集相關的風險資訊、您要升級的 ONTAP 版本中的新功能和增強功能，以及在嘗試 ONTAP 升級之前需要採取的任何措施。

若要深入瞭解 Upgrade Health Checker，您可以參考["升級健全狀況檢查程式常見問題"](#)或觀看以下介紹影片。

📺 | <https://img.youtube.com/vi/5mwmigXAB9c/maxresdefault.jpg>

## 下載並設定 Upgrade Health Checker

您可以下載 Upgrade Health Checker，在升級到更新版本的 ONTAP 之前產生現場綜合報告。

關於此任務

Upgrade Health Checker 支援內部部署 ONTAP 9.11.1 及更新版本的升級。如果您使用 Cloud Volumes ONTAP，請參閱["升級 Cloud Volumes ONTAP"](#)以取得系統升級資訊。

開始之前

使用以下規格為 Upgrade Health Checker 設定虛擬機器：

- 處理與記憶體：m5.large VM 或同等配置，配備 2 個 vCPU 和 8 GiB RAM。
- 建議的作業系統：任何具有 glibc 函式庫版本 2.28 或更高版本的 Linux 作業系統，以獲得最佳相容性。這包括：
  - Ubuntu 22.04
  - RHEL8
  - RHEL9
- 儲存：提供一個至少 100 GB 的根磁碟區和一個至少 100 GB 的額外 NFS 磁碟區，以確保在虛擬機器遭到入侵時資料能夠保留。
- 託管需求：將 VM 放置在具有叢集連線和網際網路存取權限的位置，以便實現工具的自動更新。該機器應可透過 HTTPS 存取以下端點以執行自動更新：
  - <https://api.uhc.netapp.com>
  - <https://gql.aiq.netapp.com>

如果無法存取網際網路，請諮詢 NetApp 以取得指引。

- 建議套件：安裝 Web 伺服器以方便存取。

此外，請確保虛擬機器可以透過 HTTPS 連接到遙測端點(<https://support.netapp.com/>)，以便 NetApp 接收有關升級計劃的 AutoSupport 資訊。

#### 步驟

1. 下載 Upgrade Health Checker 二進位檔案，方法是 "導覽至 [NetApp Console Automation Hub](#)" 並找到 Upgrade Health Checker 圖示。
2. 設定 Upgrade Health Checker 虛擬機器，並使用 SSH 將二進位檔案放置在您選擇的位置。
3. 驗證 Upgrade Health Checker 的數位簽章。

Upgrade Health Checker 具有公共代碼簽署憑證 (UHC-Linux-codesigning-certificate-public.pem) 以及中間憑證和根憑證鏈 (UHC-Linux-chain-certificates-public.pem)。

- a. (選用) 根據鏈驗證程式碼簽署憑證：

```
openssl verify -CAfile UHC-Linux-chain-certificates-public.pem UHC-Linux-codesigning-certificate-public.pem
```

``OK`` 的輸出結果確認了有效的信任鏈。

- b. 從程式碼簽署憑證中提取公開金鑰：

```
openssl x509 -in UHC-Linux-codesigning-certificate-public.pem -pubkey -noout -out UHC-Linux-public.pub
```

- c. 使用公開金鑰驗證簽章檔案 ((`uhc.sig`) 與 Upgrade Health Checker 二進位檔案：

```
openssl dgst -sha256 -verify UHC-Linux-public.pub -signature uhc.sig uhc
```

``Verified OK`` 的輸出結果確認簽名有效。

4. 為 ONTAP 叢集存取配置服務帳戶和角色。對於透過 Upgrade Health Checker 存取叢集的情況，請將服務角色建立為 REST 角色。



您可以建立一個 Ansible playbook，以自動將角色和使用者部署到所有 ONTAP 叢集。

您必須為 HTTP 應用程式建立服務帳戶。請使用以下 CLI 指令設定必要的權限：

```

security login rest-role create -role uhctool -api /api -access readonly
-vserver

security login rest-role create -role uhctool -api
/api/support/autosupport -access read_create_modify -vserver

security login rest-role create -role uhctool -api
/api/support/autosupport/messages -access read_create_modify -vserver

vserver services web access create -name spi -role uhctool -vserver

security login create -user-or-group-name uhctool -role uhctool
-application http -authentication-method password

security login create -user-or-group-name uhctool -role uhctool
-application ssh -authentication-method password

```

5. (選用) 設定認證管理以保護對應用程式的存取。

例如，如果您有 CyberArk 和 Conjur，您可以設定您的環境，以避免透過 yamll 檔案或命令列傳遞認證資料。

a. 建立所需的 CyberArk 保險箱：

- i. 建立一個 Safe (Main-Conjur-Safe)，用於保存應用程式憑證和金鑰
- ii. 建立一個安全庫 (API 憑證安全庫)，用於存放 Conjur 主機 ID 和 API 金鑰
- iii. 建立一個存放必要憑證的保險箱 (Conjur-SSL-Certificate)

b. 為該應用程式建立設定檔 (Conjur.conf) 和身分檔 (Conjur.identity)：

i. Conjur.conf

```

account:
plugins: []
appliance_url: https://FQDN
cert_file: /etc/conjur.pem

```

ii. Conjur.identity

```

machine https://FQDN/authn
login host /prodvault/devops/<Main-Conjur-Safe>/host1
password XXXXXX

```

以下是如何在 Ansible playbook 中使用 CyberArk 和 Conjur 的範例：

- c. 在 Ansible 主機上安裝 Conjur Ansible Collection，其中包含 Conjur Ansible Lookup Plugin：

```
ansible-galaxy collection install cyberark.conjur
```

- d. 在 YAML 檔案中建立一個任務，用於從 CyberArk 取得使用者名稱和密碼：

```
conjur_username: "{{ lookup('cyberark.conjur.conjur_variable',  
'prodvault/devops/<Main-Conjur-Safe>/<Account name>/username',  
validate_certs=false) }}"  
conjur_password: "{{ lookup('cyberark.conjur.conjur_variable',  
'prodvault/devops/<Main-Conjur-Safe>/<Account name>/password',  
validate_certs=false) }}"
```

接下來呢？

您可以使用升級健康檢查器，透過["產生升級報告"](#)來協助您規劃 ONTAP 升級。

# 使用 Upgrade Health Checker

## 使用 Upgrade Health Checker 產生升級計畫

您可以使用 Upgrade Health Checker 為單一或多個 ONTAP 叢集產生升級計畫。

如果您擁有一個包含多個叢集的大型複雜環境，您還可以 ["自動產生升級報告"](#) 協助維護最新的升級計畫。

### 關於此任務

Upgrade Health Checker 支援內部部署 ONTAP 9.11.1 及更新版本的升級。如果您使用 Cloud Volumes ONTAP，請參閱 ["升級 Cloud Volumes ONTAP"](#) 以取得系統升級資訊。

### 開始之前

若要深入瞭解特定 Upgrade Health Checker 參數以及該工具接受輸入的優先順序，請參閱 ["了解 Upgrade Health Checker 的輸入參數"](#)。

### 步驟

1. 首次執行二進位檔案之前，請先設定執行權限：

```
chmod +x uhc
```



Upgrade Health Checker 是一個獨立的軟體包，需要先解壓縮才能執行。這可能需要幾秒鐘。

2. 在完成 Upgrade Health Checker 的完整運作之前，請執行全面檢查，以確保工具可以連接到叢集和所需的端點：

```
--test all
```

全面檢查可確保託管 Upgrade Health Checker 的虛擬機器具備以下功能：

- 透過 HTTPS 連線至 ONTAP 叢集 IP 位址
  - 透過 HTTPS 連接到遙測端點 (<https://support.netapp.com/>)
  - 透過 HTTPS 連接到自動更新端點(<https://api.uhc.netapp.com>和 <https://gql.aiq.netapp.com>)
  - 至少 4 GB 可用 `/tmp` 空間
3. (可選) 如果您想使用設定檔來儲存參數，請將 `config.yaml.example` 檔案 (位於您下載二進位檔案的相同位置) 重新命名為 `config.yaml`。

以下是一個 config.yaml 檔案範例：

```
# Application Configuration
APP:
  RUNS_PATH: "/opt/uhc/runs"

# Cluster Credentials
CLUSTER:
  IP: "x.x.x.x"
  USERNAME: "admin"
  PASSWORD: "xyz"
  TARGET_ONTAP_VERSION: "" # Optional: Specify target ONTAP version
  (e.g., "9.16.1" or "current" to keep existing version). Leave empty to
  prompt user.
  ACCEPT_EULA: false # Optional: Set to true to accept EULA through
  config. If false/empty, user will be prompted interactively.
```

- 執行 Upgrade Health Checker，輸入要升級到的 ONTAP 版本並接受 EULA，並根據需要添加其他參數。



EULA 是一份多頁文件。輸入 `all` 即可一次查看整份文件，然後輸入 `y` 接受。

下載叢集的 AutoSupport 日誌後，處理時間通常為一到兩分鐘，具體取決於叢集節點數量。由於不同 ONTAP 軟體版本處理 AutoSupport 收集的方式不同，每次 Upgrade Health Checker 執行都取決於叢集的目前負載和目前的 ONTAP 版本。

- 請參考 ["了解 Upgrade Health Checker 的輸入參數"](#)，熟悉可用的 Upgrade Health Checker 參數、輸入優先順序以及某些參數的預設值。

Input Parameters Guide 還提供了有關指定自訂設定檔路徑和執行路徑的資訊，以簡化您的工作流程。最佳實務做法是為每個叢集建立一個自訂輸出目錄，以便有效地組織您的報告和日誌。

- 接受最終使用者授權合約並輸入目標 ONTAP 版本和任何其他參數，以執行升級健全狀況檢查程式。

```
./uhc
```

- 升級健康檢查器完成檢查後，導航至 runs 資料夾以查看升級計劃和叢集報告。



程式的每次執行都是一次「獨立運行」，所有相關的資料、日誌和結果都將保存在相應的 runs 資料夾中。

- 在網頁瀏覽器中開啟報告檔案（名為 `uhc_<cluster-name>_<YYYYMMDDHHMMSS>.html`）以檢視報告。如果您在遠端主機上執行，請先將報告檔案下載到可以在網頁瀏覽器上檢視報告的機器。

日誌路徑和報告路徑如下：

- 日誌路徑： `<output-path>/<unique-run-dir>/<cluster-name>/logs`
- 報告路徑： `<output-path>/<unique-run-dir>/<cluster-name>/results/uhc_<cluster-name>_<YYYYMMDDHHMMSS>.html`

# 使用 Upgrade Health Checker 自動產生升級計劃

在大型、複雜的環境中規劃 ONTAP 升級時，您可以自動產生升級健全狀況檢查程式報告，以減少手動工作量。

關於此任務

Upgrade Health Checker 支援內部部署 ONTAP 9.11.1 及更新版本的升級。如果您使用 Cloud Volumes ONTAP，請參閱 ["升級 Cloud Volumes ONTAP"](#) 以取得系統升級資訊。

步驟

1. 為確保成功建立升級報告，請完成 ["產生 ONTAP 升級報告"](#) 中概述的任何必要設定步驟和一次性任務。
2. 建立一個腳本，使用適合您環境的參數執行 Upgrade Health Checker。

```
./uhc \  
  --cluster-ip=<cluster-ip> \  
  --cluster-username=<cluster-username> \  
  --cluster-password=<cluster-password> \  
  --target-ontap-version=<target-ontap-version> \  
  --accept-eula=true
```

以下是一個 cronjob 的範例，該 cronjob 會在週一至週五凌晨 4 點執行該工具。二進位檔案和 config.yaml 檔案已安裝到 /opt/uhc/tool/ 中。

Bash 腳本：

```
#!/bin/bash  
cd /opt/uhc/tool  
/opt/uhc/tool/uhc --accept-eula true --cluster-ip cluster-  
mgmt1.example.com --target-ontap-version current --cluster-username  
uhctool --cluster-password passw0rd  
/opt/uhc/tool/uhc --accept-eula true --cluster-ip cluster-  
mgmt2.example.com --target-ontap-version 9.14.1 --cluster-username  
uhctool --cluster-password passw0rd
```

Cron 工作：

```
0 4 * * 1-5 /usr/local/bin/uhccron.sh
```

3. 升級健康檢查器完成檢查後，導航至 runs 資料夾以查看升級計劃和叢集報告。



每次執行程式都是獨立的運行，所有相關的資料、日誌和結果都將保存在相應的 runs 資料夾中。

4. 在網頁瀏覽器中開啟報告檔案（名稱為 `uhc_<cluster-name>_<YYYYMMDDHHMMSS>.html`）以檢視報告。如果您在遠端主機上執行 Upgrade Health Checker，請先將報告檔案下載到可以使用網頁瀏覽器檢視的電腦。

日誌路徑和報告路徑如下：

- 日誌路徑：`<output-path>/<unique-run-dir>/<cluster-name>/logs`
- 報告路徑：`<output-path>/<unique-run-dir>/<cluster-name>/results/uhc_<cluster-name>_<YYYYMMDDHHMMSS>.html`

# 了解 Upgrade Health Checker 的輸入參數

您可以了解更多關於 Upgrade Health Checker 的輸入參數以及如何透過 CLI 參數、設定檔或互動式提示提供這些參數的資訊，以協助您產生 ONTAP 叢集的升級報告。

## 輸入方法優先順序

升級健康檢查器為所有參數提供了多種輸入選項。其接受輸入的優先順序如下：

1. CLI 參數 (優先順序最高)
2. 組態檔 (config.yaml)
3. 互動式提示 (優先順序最低)

當一個參數透過多種方式提供時，該工具將使用優先順序最高的來源的值。

## 輸入參數

### 叢集 IP

此 `--cluster-ip` 參數指定要連接的 ONTAP 叢集的 IP 位址或主機名稱。

提供此參數的優先順序為：

1. CLI 參數：`--cluster-ip`
2. 組態檔：`CLUSTER.IP`
3. 互動式提示

### 範例

- CLI 參數：

```
./uhc --cluster-ip 192.168.1.100
```

- Config.yaml：

```
CLUSTER:  
  IP: "192.168.1.100"
```

- 互動模式 (如果以上未提供)：

工具將提示：`Enter cluster IP address:`

## 叢集使用者名稱

`--cluster-username` 參數指定用於向 ONTAP 叢集進行身份驗證的使用者名稱。

提供此參數的優先順序為：

1. CLI 參數：`--cluster-username`
2. 組態檔：`CLUSTER.USERNAME`
3. 互動式提示

### 範例

- CLI 參數：

```
./uhc --cluster-username admin
```

- Config.yaml：

```
CLUSTER:  
  USERNAME: "admin"
```

- 互動模式（如果以上未提供）：

```
工具將提示：Enter cluster username:
```

## 叢集密碼

`--cluster-password` 參數指定用於向 ONTAP 叢集進行身份驗證的密碼。

提供此參數的優先順序為：

1. CLI 參數：`--cluster-password`
2. 組態檔：`CLUSTER.PASSWORD`
3. 互動式提示（安全輸入）

## 範例

- CLI 參數（基於安全考量不建議使用）：

```
./uhc --cluster-password mypassword
```

- Config.yaml（確保檔案權限受到限制）：

```
CLUSTER:  
  PASSWORD: "mypassword"
```

- 互動模式（建議 - 密碼已隱藏）：

工具將提示：Enter cluster password:

## 目標 ONTAP 版本

此 `--target-ontap-version` 參數指定您要升級到的 ONTAP 版本以進行分析。使用 "current" 可保留現有叢集 ONTAP 版本。

提供此參數的優先順序為：

1. CLI 參數：--target-ontap-version
2. 組態檔：CLUSTER.TARGET\_ONTAP\_VERSION
3. 互動式選擇選單

## 範例

- CLI 參數：

ONTAP 的更新版本：./uhc --target-ontap-version 9.15.1

保持目前版本的 ONTAP：./uhc --target-ontap-version current

- Config.yaml：

```
CLUSTER:  
  TARGET_ONTAP_VERSION: "9.15.1"
```

- 互動模式（如果以上未提供）：

工具將顯示可用版本並提示選擇

## 接受 EULA

`--accept-eula` 參數指定是否接受最終使用者授權合約。必須設為 `true` 才能繼續。

提供此參數的優先順序為：

1. CLI 參數：`--accept-eula`
2. 組態檔：`CLUSTER.ACCEPT_EULA`
3. 互動式提示

範例

- CLI 參數：

```
./uhc --accept-eula true
```

- Config.yaml：

```
CLUSTER:  
  ACCEPT_EULA: true
```

- 互動模式（如果以上未提供）：

該工具將顯示 EULA 並提示接受

## 設定檔路徑

`--config-path` 參數指定自訂配置 YAML 檔案的路徑。

提供此參數的優先順序為：

1. CLI 參數：`--config-path`
2. 預設：`config.yaml`

## 範例

- CLI 參數：

```
./uhc --config-path /path/to/custom_config.yaml
```

- 預設值（如果未提供）：

工具將在目前目錄中尋找 config.yaml

## 執行輸出路徑

`--runs-path` 參數指定用於儲存執行輸出和報告的自訂目錄。

提供此參數的優先順序為：

1. CLI 參數：--runs-path
2. 組態檔：APP.RUNS\_PATH
3. 預設：./runs

## 範例

- CLI 參數：

```
./uhc --runs-path /custom/output/path
```

- Config.yaml：

```
APP:  
  RUNS_PATH: "/custom/output/path"
```

- 預設值（如果未提供）：

工具將使用 ./runs 目錄

## 跳過相容性檢查

此 `--skip-compatibility-check` 參數會繞過硬體相容性檢查，並使用您要升級到的指定 ONTAP 版本。



僅當您確定目標 ONTAP 版本與您的硬體相容時才使用此選項。

提供此參數的優先順序為：

1. CLI 參數： `--skip-compatibility-check`
2. 組態檔： `CLUSTER.SKIP_COMPATIBILITY_CHECK`
3. 預設： `false`

## 範例

- CLI 參數：

```
./uhc --skip-compatibility-check true
```

- Config.yaml：

```
CLUSTER:  
  SKIP_COMPATIBILITY_CHECK: true
```

## 停用遙測

若要停用遙測功能，請將以下內容新增至您的 `config.yaml` 檔案：

```
TELEMETRY:  
  ENABLED: false
```

## 停用自動更新

若要停用升級健康檢查器的自動更新，請將以下內容新增至您的 `config.yaml` 檔案：

```
AUTO_UPDATE:  
  ENABLED: false
```

## 使用每種輸入方法的範例

### 組合 CLI 參數

```
./uhc \  
  --cluster-ip 192.168.1.100 \  
  --cluster-username admin \  
  --cluster-password mypassword \  
  --target-ontap-version 9.15.1 \  
  --accept-eula true \  
  --config-path /path/to/custom_config.yaml \  
  --runs-path /custom/output \  
  --skip-compatibility-check false
```

## Config.yaml 檔案

```
CLUSTER:  
  IP: "192.168.1.100"  
  USERNAME: "admin"  
  PASSWORD: "mypassword"  
  TARGET_ONTAP_VERSION: "9.15.1"  
  ACCEPT_EULA: true  
  SKIP_COMPATIBILITY_CHECK: false  
  
APP:  
  RUNS_PATH: "/custom/output"
```

## 互動模式

若要以互動方式提示輸入所有必要的輸入參數，請不帶任何參數執行 Upgrade Health Checker：

```
./uhc
```

## 其他命令

這些命令提供了一些工具完整執行以外的額外功能：

- 顯示說明

```
./uhc --help
```

- 顯示版本

```
./uhc --version
```

- 測試叢集連線能力

```
./uhc --test-connectivity cluster
```

- 測試遙測連線能力

```
./uhc --test-connectivity telemetry
```

- 測試自動更新連線能力

```
./uhc --test-connectivity autoupdate
```

- 執行所有測試

```
./uhc --test all
```

# 升級健全狀況檢查程式常見問題

Upgrade Health Checker 常見問題 (FAQ)。

## Upgrade Health Checker 與 Upgrade Advisor 有何不同？

Upgrade Health Checker 是一款本地部署工具，適用於環境規模龐大或複雜、網路存取受限或已部署自動化和編排框架的使用者。Upgrade Advisor 則適用於環境規模較小、偏好基於雲端、以使用者介面為中心的使用者體驗的使用者。

您可以深入瞭解 "[升級健全狀況檢查程式](#)" 和 "[升級顧問](#)"，以確定哪種工具最適合您的需求。

## 升級健全狀況檢查程式報告包含哪些資訊？

Upgrade Health Checker 報告提供有關升級 ONTAP 叢集之前需要解決的潛在障礙和警告的詳細資訊、與叢集相關的風險，以及有關您要升級到的 ONTAP 版本中的新功能和增強功能的資訊。

## Upgrade Health Checker 可以在沒有網際網路連線的情況下使用嗎？

您不需要網際網路連線即可執行 Upgrade Health Checker。它會使用您的 ONTAP 叢集目前的組態資料在現場產生升級計劃和報告。

但是，自動工具更新需要網際網路存取。如果您的環境缺乏網際網路連線，您可以從 "[NetApp Console 自動化中心](#)" 上的 Upgrade Health Checker 磚手動下載工具的最新版本。

## Upgrade Health Checker 支援哪些 ONTAP 版本？

升級健全狀況檢查程式支援內部部署 ONTAP 9.11.1 及更新版本的升級。

# 法律聲明

法律聲明提供版權聲明、商標、專利等資訊的存取權限。

## 版權

["https://www.netapp.com/company/legal/copyright/"](https://www.netapp.com/company/legal/copyright/)

## 商標

NETAPP、NETAPP 標誌以及 NetApp 商標頁面上所列的標記均為 NetApp, Inc. 的商標。其他公司和產品名稱可能是其各自所有者的商標。

["https://www.netapp.com/company/legal/trademarks/"](https://www.netapp.com/company/legal/trademarks/)

## 專利

目前 NetApp 擁有的專利清單可在以下網址找到：

<https://www.netapp.com/pdf.html?item=/media/11887-patentspage.pdf>

## 隱私權政策

["https://www.netapp.com/company/legal/privacy-policy/"](https://www.netapp.com/company/legal/privacy-policy/)

## 開放原始碼

通知文件提供有關 NetApp 軟體中使用的第三方版權和授權的資訊。

## 版權資訊

Copyright © 2026 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 保留隨時變更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。