



# 驗證文件簽名

## Cloud Volumes ONTAP

NetApp  
February 13, 2026

# 目錄

驗證文件簽名 .....	1
針對Cloud Volumes ONTAP 的Azure 市場映像簽章驗證 .....	1
文件簽章驗證工作流程摘要 .....	1
驗證 Linux 上Cloud Volumes ONTAP的 Azure 市場映像簽名 .....	1
驗證 macOS 上Cloud Volumes ONTAP的 Azure 市場映像簽名 .....	2

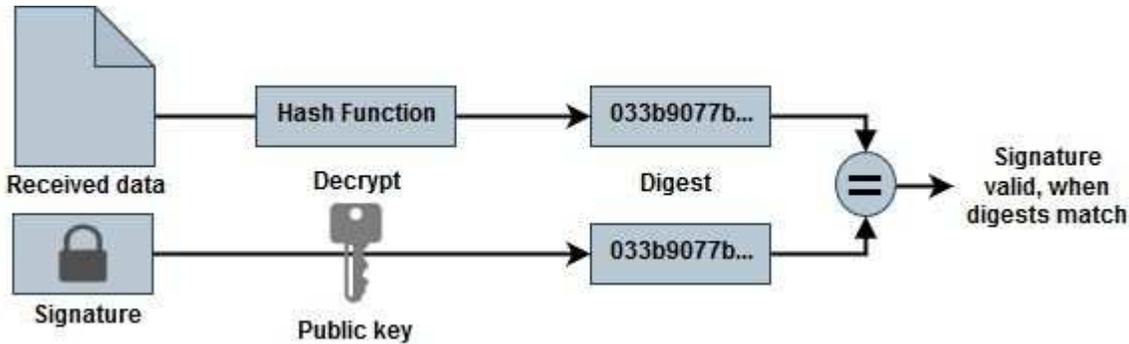
# 驗證文件簽名

## 針對Cloud Volumes ONTAP 的Azure 市場映像簽章驗證

Azure 映像驗證過程透過剝離 VHD 檔案的開頭 1 MB 和結尾 512 位元組，然後套用雜湊函數來產生摘要檔案。為了匹配簽章程序，使用\_sha256\_進行雜湊。

### 文件簽章驗證工作流程摘要

以下是文件簽章驗證工作流程的概述。



- 從 ["NetApp支援站點"](#) 並提取摘要 (.sig) 文件、公鑰證書 (.pem) 文件和鍵證書 (.pem) 文件。請參閱["下載 Azure 映像摘要文件"](#) 了解更多。
- 信任鍵的驗證。
- 從公鑰憑證 (.pem) 中提取公鑰 (.pub) 。
- 使用提取的公鑰解密摘要檔案。
- 將結果與從圖像檔案中刪除開頭 1 MB 和結尾 512 位元組後建立的臨時檔案的新生成的摘要進行比較。此步驟透過使用 OpenSSL 命令列工具執行。OpenSSL CLI 工具會在檔案比對成功或失敗時顯示對應的訊息。

```
openssl dgst -verify <public_key> -keyform <form> <hash_function>  
-signature <digest_file> -binary <temporary_file>
```

## 驗證 Linux 上Cloud Volumes ONTAP的 Azure 市場映像簽名

在 Linux 上驗證匯出的 VHD 檔案簽章包括驗證信任鏈、編輯檔案和驗證簽章。

### 步驟

1. 從下載 Azure 映像檔 ["NetApp支援站點"](#) 並提取摘要 (.sig) 文件、公鑰證書 (.pem) 文件和鍵證書 (.pem) 文件。

參考 ["下載 Azure 映像摘要文件"](#) 了解更多。

2. 驗證信任鏈。

```
% openssl verify -CAfile Certificate-Chain-9.15.0P1_azure.pem
Certificate-9.15.0P1_azure.pem
Certificate-9.15.0P1_azure.pem: OK
```

3. 刪除 VHD 檔案開頭的 1 MB (1,048,576 位元組) 和結尾的 512 位元組。使用時 `tail`，這 `-c +K` 選項從檔案的第 `K` 個位元組產生位元組。因此，它將 `1048577` 傳遞給 `tail -c`。

```
% tail -c +1048577 ./9150.01000024.05090105.vhd > ./sign.tmp.tail
% head -c -512 ./sign.tmp.tail > sign.tmp
% rm ./sign.tmp.tail
```

4. 使用 OpenSSL 從憑證中提取公鑰，並使用簽署檔案和公鑰驗證剝離的檔案 (`sign.tmp`)。

命令提示字元根據驗證顯示指示成功或失敗的訊息。

```
% openssl x509 -pubkey -noout -in ./Certificate-9.15.0P1_azure.pem >
./Code-Sign-Cert-Public-key.pub

% openssl dgst -verify Code-Sign-Cert-Public-key.pub -keyform PEM
-sha256 -signature digest.sig -binary ./sign.tmp
Verification OK

% openssl dgst -verify Code-Sign-Cert-Public-key.pub -keyform PEM
-sha256 -signature digest.sig -binary ./another_file_from_nowhere.tmp
Verification Failure
```

5. 清理工作區。

```
% rm ./9150.01000024.05090105.vhd ./sign.tmp
% rm *.sig *.pub *.pem
```

## 驗證 macOS 上 Cloud Volumes ONTAP 的 Azure 市場映像簽名

在 Linux 上驗證匯出的 VHD 檔案簽章包括驗證信任鏈、編輯檔案和驗證簽章。

### 步驟

1. 從下載 Azure 映像檔 "[NetApp 支援站點](#)" 並提取摘要 (.sig) 文件、公鑰證書 (.pem) 文件和鏈證書 (.pem) 文件。

參考 "[下載 Azure 映像摘要文件](#)" 了解更多。

2. 驗證信任鏈。

```
% openssl verify -CAfile Certificate-Chain-9.15.0P1_azure.pem
Certificate-9.15.0P1_azure.pem
Certificate-9.15.0P1_azure.pem: OK
```

3. 刪除 VHD 檔案開頭的 1MB (1,048,576 位元組) 和結尾的 512 位元組。使用時 `tail`，這 `-c +K` 選項從檔案的第 `K` 個位元組產生位元組。因此，它將 `1048577` 傳遞給 `tail -c`。請注意，在 macOS 上，`tail` 指令可能需要大約十分鐘才能完成。

```
% tail -c +1048577 ./9150.01000024.05090105.vhd > ./sign.tmp.tail
% head -c -512 ./sign.tmp.tail > sign.tmp
% rm ./sign.tmp.tail
```

4. 使用 OpenSSL 從憑證中提取公鑰，並使用簽署檔案和公鑰驗證剝離的檔案 (`sign.tmp`)。命令提示字元根據驗證顯示指示成功或失敗的訊息。

```
% openssl x509 -pubkey -noout -in ./Certificate-9.15.0P1_azure.pem >
./Code-Sign-Cert-Public-key.pub

% openssl dgst -verify Code-Sign-Cert-Public-key.pub -keyform PEM
-sha256 -signature digest.sig -binary ./sign.tmp
Verified OK

% openssl dgst -verify Code-Sign-Cert-Public-key.pub -keyform PEM
-sha256 -signature digest.sig -binary ./another_file_from_nowhere.tmp
Verification Failure
```

5. 清理工作區。

```
% rm ./9150.01000024.05090105.vhd ./sign.tmp
% rm *.sig *.pub *.pem
```

## 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。