



# 檔案簽章驗證

## Cloud Volumes ONTAP

NetApp  
June 11, 2024

# 目錄

檔案簽章驗證 .....	1
檔案簽章驗證 .....	1
Linux 上的檔案簽章驗證 .....	1
Mac OS 上的檔案簽章驗證 .....	3

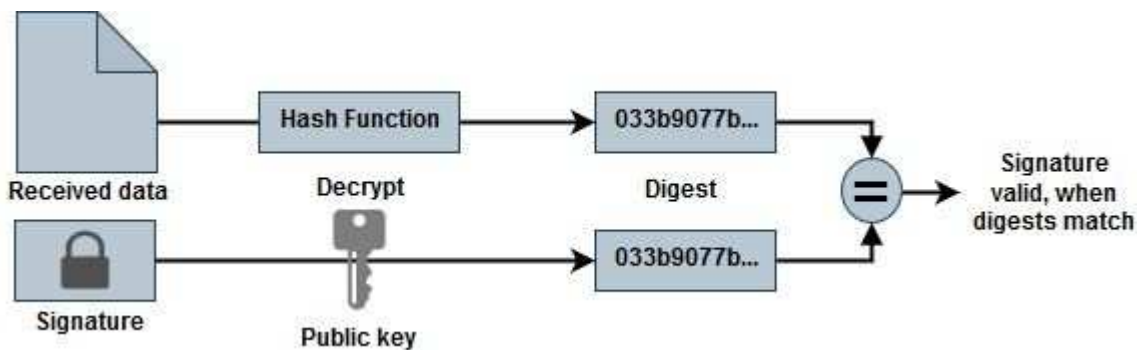
# 檔案簽章驗證

## 檔案簽章驗證

Azure 影像驗證程序將使用雜湊功能、從 VHD 檔案產生內含前導式 1MB 等量區塊的摘要、並結束 512B 等量區塊。為了符合簽署程序、使用 SHA256 進行雜湊。您需要從 VHD 檔案移除前導式 1MB 和最終版 512B、然後驗證 VHD 檔案的其餘部分。

### 檔案簽章驗證工作流程摘要

以下是檔案簽章驗證工作流程程序的概觀。



- 從下載 Azure Image Digest 檔案 "[NetApp 支援網站](#)" 然後擷取摘要檔案 (.SIG)、公開金鑰憑證檔案 (.pem) 和鏈結憑證檔案 (.pem)。

請參閱 "[下載 Azure Image Digest File](#)" 以取得更多資訊。

- 驗證信任鏈結。
- 從公開金鑰憑證 (.pem) 擷取公開金鑰 (.pub)。
- 解壓縮的公開金鑰用於解密摘要檔案。然後將結果與從映像檔案建立的新未加密暫存檔案摘要進行比較、並移除前導式 1MB 與結尾 512 位元組的檔案。

此步驟可透過下列 openssl 命令來達成。

- 一般 CLI 聲明如下所示：

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

- 如果檔案相符、則 Openssl CLI 工具會顯示「驗證成功」訊息、如果檔案不符、則會顯示「驗證失敗」訊息。

## Linux 上的檔案簽章驗證

您可以依照下列步驟驗證匯出的 VHD 檔案簽章適用於 Linux。

## 步驟

1. 從下載 Azure Image Digest 檔案 "[NetApp 支援網站](#)" 然後擷取摘要檔案 (.SIG) 、公開金鑰憑證檔案 (.pem) 和鏈結憑證檔案 (.pem) 。

請參閱 "[下載 Azure Image Digest File](#)" 以取得更多資訊。

2. 驗證信任鏈結。

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

3. 移除前導的 1MB ( 1048576 位元組) 、並結束 512 位元組的 VHD 檔案。

如果使用「tail」、選項「-c +K」會以指定檔案的 KTH 位元組開始輸出位元組。因此、1048577 會傳送至 '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 從憑證擷取公開金鑰、並使用簽章檔案和公開金鑰驗證等量分佈的檔案 ( sign.tmp ) 。

如果輸入檔通過驗證、則會顯示命令  
" 驗證正常 " 。否則將顯示「驗證失敗」。

```
% 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
```

# Mac OS 上的檔案簽章驗證

您可以依照下列步驟、驗證 Mac OS 匯出的 VHD 檔案簽章。

## 步驟

1. 從下載 Azure Image Digest 檔案 "[NetApp 支援網站](#)" 然後擷取摘要檔案 (.SIG) 、公開金鑰憑證檔案 (.pem) 和鏈結憑證檔案 (.pem) 。

請參閱 "[下載 Azure Image Digest File](#)" 以取得更多資訊。

2. 驗證信任鏈結。

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

3. 移除前導的 1MB ( 1048576 位元組) 、並結束 512 位元組的 VHD 檔案。

如果使用「tail」、選項「-c +K」會以 KTH 位元組開始輸出位元組指定檔案的。因此、1048577 會傳送至 'tail -c'。大約需要 13 分鐘以在 Mac OS 上完成 tail 命令。

```
% 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 從憑證擷取公開金鑰、並驗證等量分割檔案 ( sign.tmp ) 、含簽章檔案和公開金鑰。

如果輸入檔案通過驗證、命令會顯示「驗證正常」。  
否則將顯示「驗證失敗」。

```
% 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 © 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。