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

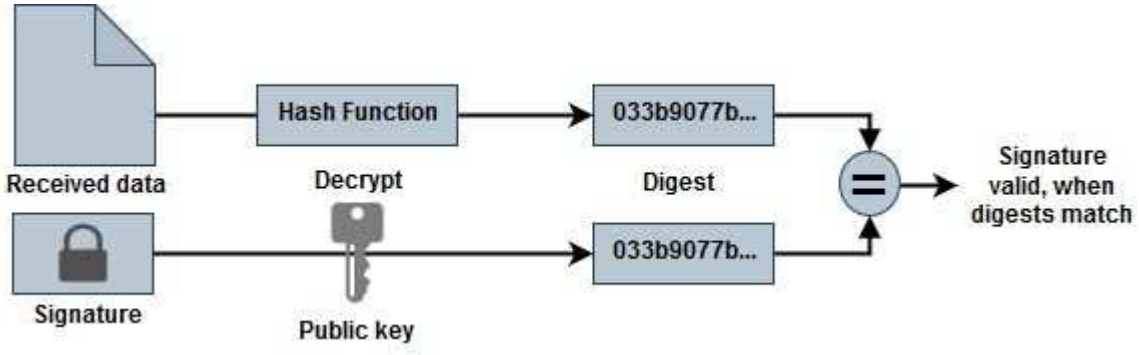
驗證文件簽名

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）文件和鏈證書（.pem）文件。請參閱"下載 Azure 映像摘要文件"了解更多。
- 信任鏈的驗證。
- 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 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
```