Verifica la firma del file

Cloud Volumes ONTAP

NetApp
February 13, 2026

Sommario

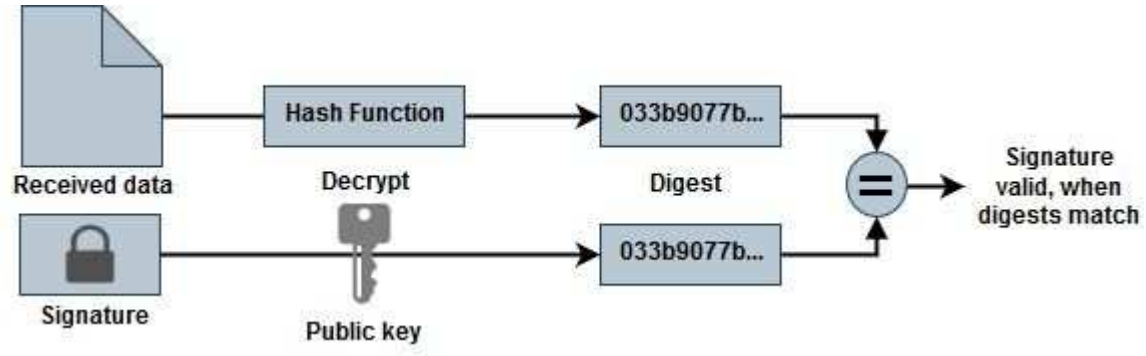
Verifica la firma del file

Verifica della firma dell'immagine di Azure Marketplace per Cloud Volumes ONTAP

Il processo di verifica dell'immagine di Azure genera un file digest dal file VHD eliminando 1 MB all'inizio e 512 byte alla fine, quindi applicando una funzione hash. Per abbinare la procedura di firma, per l'hashing viene utilizzato *sha256*.

Riepilogo del flusso di lavoro di verifica della firma del file

Di seguito è riportata una panoramica del processo di verifica della firma del file.



- Scaricamento dell'immagine di Azure da "Sito di supporto NetApp" ed estraendo il file digest (.sig), il file del certificato della chiave pubblica (.pem) e il file del certificato della catena (.pem). Fare riferimento a "Scarica il file digest dell'immagine di Azure" per maggiori informazioni.
- Verifica della catena di fiducia.
- Estrazione della chiave pubblica (.pub) dal certificato della chiave pubblica (.pem).
- Decifrare il file digest utilizzando la chiave pubblica estratta.
- Confronto del risultato con un digest appena generato di un file temporaneo creato dal file immagine dopo aver rimosso 1 MB all'inizio e 512 byte alla fine. Questo passaggio viene eseguito utilizzando lo strumento da riga di comando OpenSSL. Lo strumento OpenSSL CLI visualizza un messaggio appropriato in caso di successo o fallimento nella corrispondenza dei file.

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

Verifica la firma dell'immagine di Azure Marketplace per Cloud Volumes ONTAP su Linux

La verifica della firma di un file VHD esportato su Linux include la convalida della catena di attendibilità, la modifica del file e la verifica della firma.

Passi

1. Scarica il file immagine di Azure da "Sito di supporto NetApp" ed estrarre il file digest (.sig), il file del certificato della chiave pubblica (.pem) e il file del certificato della catena (.pem).

   Fare riferimento a "Scarica il file digest dell'immagine di Azure" per maggiori informazioni.

2. Verificare la catena di fiducia.

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

3. Rimuovere 1 MB (1.048.576 byte) all'inizio e 512 byte alla fine del file VHD. Quando si utilizza `tail` , IL `-c +K` L'opzione genera byte dal K-esimo byte del file. Pertanto, passa 1048577 a `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. Utilizzare OpenSSL per estrarre la chiave pubblica dal certificato e verificare il file estratto (sign.tmp) con il file della firma e la chiave pubblica.

   Il prompt dei comandi visualizza messaggi che indicano l'esito positivo o negativo della verifica.

```
% 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. Pulisci l'area di lavoro.

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

Verifica la firma dell'immagine di Azure Marketplace per Cloud Volumes ONTAP su macOS

La verifica della firma di un file VHD esportato su Linux include la convalida della catena

di attendibilità, la modifica del file e la verifica della firma.

Passi

1. Scarica il file immagine di Azure da "Sito di supporto NetApp" ed estrarre il file digest (.sig), il file del certificato della chiave pubblica (.pem) e il file del certificato della catena (.pem).

   Fare riferimento a "Scarica il file digest dell'immagine di Azure" per maggiori informazioni.

2. Verificare la catena di fiducia.

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

3. Rimuovere 1 MB (1.048.576 byte) all'inizio e 512 byte alla fine del file VHD. Quando si utilizza `tail` , IL `-c +K` L'opzione genera byte dal K-esimo byte del file. Pertanto, passa 1048577 a `tail -c` . Tieni presente che su macOS il comando tail potrebbe richiedere circa dieci minuti per essere completato.

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

4. Utilizzare OpenSSL per estrarre la chiave pubblica dal certificato e verificare il file estratto (sign.tmp) con il file della firma e la chiave pubblica. Il prompt dei comandi visualizza messaggi che indicano l'esito positivo o negativo della verifica.

```
% 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. Pulisci l'area di lavoro.

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

Informazioni sul copyright

Informazioni sul marchio commerciale