Verifica della firma del file

Cloud Volumes ONTAP

NetApp
June 27, 2024

This PDF was generated from https://docs.netapp.com/it-it/bluexp-cloud-volumes-ontap/concept-azure-file-sig-verify.html on June 27, 2024. Always check docs.netapp.com for the latest.

Sommario

Verifica della firma del file 1
Verifica della firma del file 1
Verifica della firma dei file su Linux 1
Verifica della firma del file su Mac OS 3

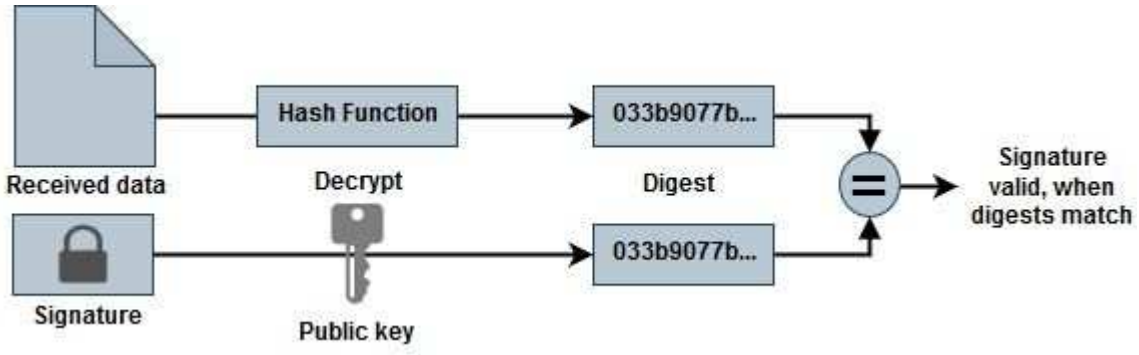
Verifica della firma del file

Verifica della firma del file

Il processo di verifica dell'immagine di Azure genera un digest dal file VHD con il primo 1MB e il termine del 512B striping mediante la funzione hash. Per far corrispondere la procedura di firma, SHA256 viene utilizzato per eseguire l'hash. È necessario rimuovere i file 1MB iniziali e 512B finali dal file VHD e verificare la parte rimanente del file VHD.

Riepilogo del flusso di lavoro di verifica della firma dei file

Di seguito viene fornita una panoramica del processo del flusso di lavoro di verifica della firma dei file.



- Scaricare il file Azure Image Digest dal "Sito di supporto NetApp" ed estrarre il file digest(.sig), il file di certificato a chiave pubblica(.pem) e il file di certificato a catena(.pem).

  Fare riferimento a. "Scaricare il file di Azure Image Digest" per ulteriori informazioni.

- Verificare la catena di trust.
- Estrarre la chiave pubblica(.pub) dal certificato a chiave pubblica(.pem).
- La chiave pubblica estratta viene utilizzata per decrittografare il file digest. Il risultato viene quindi confrontato con un nuovo digest non crittografato del file temporaneo creato dal file di immagine con 1MB iniziale e 512 byte finale rimossi.

  Questo passo viene ottenuto mediante il seguente comando openssl.

  - L'istruzione CLI generale viene visualizzata come segue:

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

  - Lo strumento CLI OpenSSL visualizza un messaggio "verificato OK" se entrambi i file corrispondono e "errore di verifica" se non corrispondono.

Verifica della firma dei file su Linux

È possibile verificare la firma di un file VHD esportato per Linux seguendo la procedura

riportata di seguito.

Fasi

1. Scaricare il file Azure Image Digest dal "Sito di supporto NetApp" ed estrarre il file digest(.sig), il file di certificato a chiave pubblica(.pem) e il file di certificato a catena(.pem).

   Fare riferimento a. "Scaricare il file di Azure Image Digest" per ulteriori informazioni.

2. Verificare la catena di trust.

```
% 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 i 1MB iniziali (1048576 byte) e i 512 byte finali del file VHD.

   Se si usa 'tail', l'opzione '-c +K' genera byte che iniziano con i kth byte del file specificato. Quindi, 1048577 viene passato alla coda -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 con striping (sign.tmp) con il file della firma e la chiave pubblica.

   Se il file di input supera la verifica, viene visualizzato il comando "Verifica OK". In caso contrario, viene visualizzato "errore di 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. Pulire lo spazio di lavoro.

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

Verifica della firma del file su Mac OS

Per verificare la firma di un file VHD esportato per Mac OS, procedere come segue.

Fasi

1. Scaricare il file Azure Image Digest dal "Sito di supporto NetApp" ed estrarre il file digest(.sig), il file di certificato a chiave pubblica(.pem) e il file di certificato a catena(.pem).

   Fare riferimento a. "Scaricare il file di Azure Image Digest" per ulteriori informazioni.

2. Verificare la catena di trust.

```
% 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 i 1MB (1048576 byte) iniziali e i 512 byte finali del file VHD.

   Se si usa 'tail', l'opzione '-c +K' emette byte a partire dai kth byte
   del file specificato. Quindi, 1048577 viene passato alla coda -c'. Ci vogliono circa 13m minuti
   Per completare il comando tail su Mac OS.

```
% 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 lo striping
   file(sign.tmp) con il file della firma e la chiave pubblica.

   Se il file di input supera la verifica, il comando visualizza "verifica OK".
   In caso contrario, viene visualizzato "errore di 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. Pulire lo spazio di lavoro.

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

Informazioni sul copyright

Copyright © 2024 NetApp, Inc. Tutti i diritti riservati. Stampato negli Stati Uniti d'America. Nessuna porzione di questo documento soggetta a copyright può essere riprodotta in qualsiasi formato o mezzo (grafico, elettronico o meccanico, inclusi fotocopie, registrazione, nastri o storage in un sistema elettronico) senza previo consenso scritto da parte del detentore del copyright.

Il software derivato dal materiale sottoposto a copyright di NetApp è soggetto alla seguente licenza e dichiarazione di non responsabilità:

IL PRESENTE SOFTWARE VIENE FORNITO DA NETAPP "COSÌ COM'È" E SENZA QUALSIVOGLIA TIPO DI GARANZIA IMPLICITA O ESPRESSA FRA CUI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, GARANZIE IMPLICITE DI COMMERCIABILITÀ E IDONEITÀ PER UNO SCOPO SPECIFICO, CHE VENGONO DECLINATE DAL PRESENTE DOCUMENTO. NETAPP NON VERRÀ CONSIDERATA RESPONSABILE IN ALCUN CASO PER QUALSIVOGLIA DANNO DIRETTO, INDIRETTO, ACCIDENTALE, SPECIALE, ESEMPLARE E CONSEQUENZIALE (COMPRESI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, PROCUREMENT O SOSTITUZIONE DI MERCI O SERVIZI, IMPOSSIBILITÀ DI UTILIZZO O PERDITA DI DATI O PROFITTI OPPURE INTERRUZIONE DELL'ATTIVITÀ AZIENDALE) CAUSATO IN QUALSIVOGLIA MODO O IN RELAZIONE A QUALUNQUE TEORIA DI RESPONSABILITÀ, SIA ESSA CONTRATTUALE, RIGOROSA O DOVUTA A INSOLVENZA (COMPRESA LA NEGLIGENZA O ALTRO) INSORTA IN QUALSIASI MODO ATTRAVERSO L'UTILIZZO DEL PRESENTE SOFTWARE ANCHE IN PRESENZA DI UN PREAVVISO CIRCA L'EVENTUALITÀ DI QUESTO TIPO DI DANNI.

NetApp si riserva il diritto di modificare in qualsiasi momento qualunque prodotto descritto nel presente documento senza fornire alcun preavviso. NetApp non si assume alcuna responsabilità circa l'utilizzo dei prodotti o materiali descritti nel presente documento, con l'eccezione di quanto concordato espressamente e per iscritto da NetApp. L'utilizzo o l'acquisto del presente prodotto non comporta il rilascio di una licenza nell'ambito di un qualche diritto di brevetto, marchio commerciale o altro diritto di proprietà intellettuale di NetApp.

Il prodotto descritto in questa guida può essere protetto da uno o più brevetti degli Stati Uniti, esteri o in attesa di approvazione.

LEGENDA PER I DIRITTI SOTTOPOSTI A LIMITAZIONE: l'utilizzo, la duplicazione o la divulgazione da parte degli enti governativi sono soggetti alle limitazioni indicate nel sottoparagrafo (b)(3) della clausola Rights in Technical Data and Computer Software del DFARS 252.227-7013 (FEB 2014) e FAR 52.227-19 (DIC 2007).

I dati contenuti nel presente documento riguardano un articolo commerciale (secondo la definizione data in FAR 2.101) e sono di proprietà di NetApp, Inc. Tutti i dati tecnici e il software NetApp forniti secondo i termini del presente Contratto sono articoli aventi natura commerciale, sviluppati con finanziamenti esclusivamente privati. Il governo statunitense ha una licenza irrevocabile limitata, non esclusiva, non trasferibile, non cedibile, mondiale, per l'utilizzo dei Dati esclusivamente in connessione con e a supporto di un contratto governativo statunitense in base al quale i Dati sono distribuiti. Con la sola esclusione di quanto indicato nel presente documento, i Dati non possono essere utilizzati, divulgati, riprodotti, modificati, visualizzati o mostrati senza la previa approvazione scritta di NetApp, Inc. I diritti di licenza del governo degli Stati Uniti per il Dipartimento della Difesa sono limitati ai diritti identificati nella clausola DFARS 252.227-7015(b) (FEB 2014).

Informazioni sul marchio commerciale

NETAPP, il logo NETAPP e i marchi elencati alla pagina http://www.netapp.com/TM sono marchi di NetApp, Inc. Gli altri nomi di aziende e prodotti potrebbero essere marchi dei rispettivi proprietari.