Überprüfung der Dateisignatur

Cloud Volumes ONTAP

NetApp
June 27, 2024

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

Inhalt

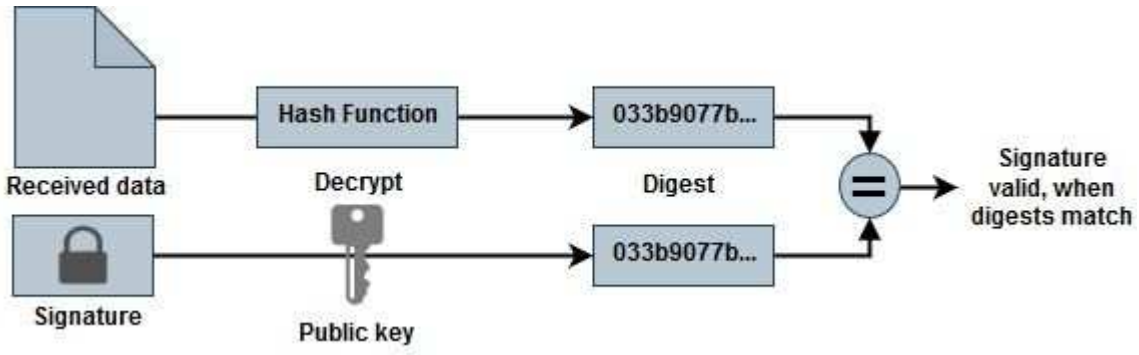
Überprüfung der Dateisignatur

Überprüfung der Dateisignatur

Bei der Azure-Image-Verifizierung wird mithilfe der Hash-Funktion ein Digest aus der VHD-Datei mit den führenden 1 MB und dem endenden 512B-Striping generiert. Um die Signaturverfahren anzupassen, wird SHA256 zum Hash verwendet. Sie müssen die führenden 1MB und die letzten 512B aus der VHD-Datei entfernen und dann den verbleibenden Teil der VHD-Datei überprüfen.

Zusammenfassung des Dateisignaturüberprüfungs-Workflows

Im Folgenden finden Sie eine Übersicht über den Prozess zur Überprüfung der Dateisignatur.



- Laden Sie die Datei Azure Image Digest von der herunter "NetApp Support Website" Und extrahieren Sie die Digest-Datei(.SIG), die Zertifikatdatei des öffentlichen Schlüssels(.pem) und die Zertifikatdatei der Kette(.pem).

  Siehe "Azure Image Digest Datei herunterladen" Finden Sie weitere Informationen.

- Überprüfen Sie die Vertrauenskette.
- Extrahieren Sie den öffentlichen Schlüssel(.Pub) aus dem öffentlichen Schlüsselzertifikat(.pem).
- Der extrahierte öffentliche Schlüssel wird verwendet, um die Digest-Datei zu entschlüsseln. Das Ergebnis wird dann mit einem neuen unverschlüsselten Digest der aus der Image-Datei erstellten temporären Datei mit führenden 1MB und enden 512 Bytes entfernt verglichen.

  Dieser Schritt wird durch den folgenden Befehl openssl erreicht.

  - Die allgemeine CLI-Anweisung wird wie folgt angezeigt:

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

  - OpenSSL CLI-Tool gibt eine "Verified OK"-Meldung, wenn beide Dateien übereinstimmen und "Verification Failure", wenn sie nicht übereinstimmen.

Überprüfung der Dateisignatur unter Linux

Sie können eine exportierte VHD-Dateisignatur für Linux überprüfen, indem Sie die folgenden Schritte ausführen.

Schritte

1. Laden Sie die Datei Azure Image Digest von der herunter "NetApp Support Website" Und extrahieren Sie die Digest-Datei(.SIG), die Zertifikatdatei des öffentlichen Schlüssels(.pem) und die Zertifikatdatei der Kette(.pem).

   Siehe "Azure Image Digest Datei herunterladen" Finden Sie weitere Informationen.

2. Überprüfen Sie die Vertrauenskette.

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

3. Entfernen Sie die führenden 1 MB (1048576 Byte) und die letzten 512 Byte VHD-Datei.

   Wenn 'Tail' verwendet wird, gibt die Option '-c +K' Bytes ab den KTH Bytes der angegebenen Datei aus. Daher wird 1048577 an 'tail -c' übergeben.

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

4. Verwenden Sie openssl, um den öffentlichen Schlüssel aus dem Zertifikat zu extrahieren und die gestreifte Datei (sign.tmp) mit der Signaturdatei und dem öffentlichen Schlüssel zu überprüfen.

   Wenn die Eingabedatei die Überprüfung bestanden hat, wird der Befehl angezeigt „Verifizierung OK“. Andernfalls wird „Überprüfungsfehler“ angezeigt.

```
% 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. Den Arbeitsbereich bereinigen.

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

Überprüfung der Dateisignatur auf Mac OS

Sie können eine exportierte VHD-Dateisignatur für Mac OS überprüfen, indem Sie die folgenden Schritte ausführen.

Schritte

1. Laden Sie die Datei Azure Image Digest von der herunter "NetApp Support Website" Und extrahieren Sie die Digest-Datei(.SIG), die Zertifikatdatei des öffentlichen Schlüssels(.pem) und die Zertifikatdatei der Kette(.pem).

   Siehe "Azure Image Digest Datei herunterladen" Finden Sie weitere Informationen.

2. Überprüfen Sie die Vertrauenskette.

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

3. Entfernen Sie die führende 1 MB (1048576 Byte) und die letzte 512 Byte VHD-Datei.

   Wenn 'Tail' verwendet wird, gibt die Option '-c +K' Bytes beginnend mit den KTH Bytes aus
   Der angegebenen Datei. Daher wird 1048577 an 'tail -c' übergeben. Es dauert ca. 13m
   Damit der tail-Befehl unter Mac OS abgeschlossen wird.

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

4. Verwenden Sie openssl, um den öffentlichen Schlüssel aus dem Zertifikat zu extrahieren und den gestreiften Schlüssel zu überprüfen
   Datei(sign.tmp) mit Signaturdatei und öffentlichem Schlüssel.

   Wenn die Eingabedatei die Überprüfung besteht, wird im Befehl „Überprüfung OK“ angezeigt.
   Andernfalls wird „Überprüfungsfehler“ angezeigt.

```
% 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. Den Arbeitsbereich bereinigen.

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

Copyright-Informationen

Copyright © 2024 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtsinhabers in keiner Form und durch keine Mittel – weder grafische noch elektronische oder mechanische, einschließlich Fotokopieren, Aufnehmen oder Speichern in einem elektronischen Abrufsystem – auch nicht in Teilen, vervielfältigt werden.

Software, die von urheberrechtlich geschütztem NetApp Material abgeleitet wird, unterliegt der folgenden Lizenz und dem folgenden Haftungsausschluss:

DIE VORLIEGENDE SOFTWARE WIRD IN DER VORLIEGENDEN FORM VON NETAPP ZUR VERFÜGUNG GESTELLT, D. H. OHNE JEGLICHE EXPLIZITE ODER IMPLIZITE GEWÄHRLEISTUNG, EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE STILLSCHWEIGENDE GEWÄHRLEISTUNG DER MARKTGÄNGIGKEIT UND EIGNUNG FÜR EINEN BESTIMMTEN ZWECK, DIE HIERMIT AUSGESCHLOSSEN WERDEN. NETAPP ÜBERNIMMT KEINERLEI HAFTUNG FÜR DIREKTE, INDIREKTE, ZUFÄLLIGE, BESONDERE, BEISPIELHAFTE SCHÄDEN ODER FOLGESCHÄDEN (EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE BESCHAFFUNG VON ERSATZWAREN ODER -DIENSTLEISTUNGEN, NUTZUNGS-, DATEN- ODER GEWINNVERLUSTE ODER UNTERBRECHUNG DES GESCHÄFTSBETRIEBS), UNABHÄNGIG DAVON, WIE SIE VERURSACHT WURDEN UND AUF WELCHER HAFTUNGSTHEORIE SIE BERUHEN, OB AUS VERTRAGLICH FESTGELEGTER HAFTUNG, VERSCHULDENSUNABHÄNGIGER HAFTUNG ODER DELIKTSHAFTUNG (EINSCHLIESSLICH FAHRLÄSSIGKEIT ODER AUF ANDEREM WEGE), DIE IN IRGENDEINER WEISE AUS DER NUTZUNG DIESER SOFTWARE RESULTIEREN, SELBST WENN AUF DIE MÖGLICHKEIT DERARTIGER SCHÄDEN HINGEWIESEN WURDE.

NetApp behält sich das Recht vor, die hierin beschriebenen Produkte jederzeit und ohne Vorankündigung zu ändern. NetApp übernimmt keine Verantwortung oder Haftung, die sich aus der Verwendung der hier beschriebenen Produkte ergibt, es sei denn, NetApp hat dem ausdrücklich in schriftlicher Form zugestimmt. Die Verwendung oder der Erwerb dieses Produkts stellt keine Lizenzierung im Rahmen eines Patentrechts, Markenrechts oder eines anderen Rechts an geistigem Eigentum von NetApp dar.

Das in diesem Dokument beschriebene Produkt kann durch ein oder mehrere US-amerikanische Patente, ausländische Patente oder anhängige Patentanmeldungen geschützt sein.

ERLÄUTERUNG ZU „RESTRICTED RIGHTS“: Nutzung, Vervielfältigung oder Offenlegung durch die US-Regierung unterliegt den Einschränkungen gemäß Unterabschnitt (b)(3) der Klausel „Rights in Technical Data – Noncommercial Items“ in DFARS 252.227-7013 (Februar 2014) und FAR 52.227-19 (Dezember 2007).

Die hierin enthaltenen Daten beziehen sich auf ein kommerzielles Produkt und/oder einen kommerziellen Service (wie in FAR 2.101 definiert) und sind Eigentum von NetApp, Inc. Alle technischen Daten und die Computersoftware von NetApp, die unter diesem Vertrag bereitgestellt werden, sind gewerblicher Natur und wurden ausschließlich unter Verwendung privater Mittel entwickelt. Die US-Regierung besitzt eine nicht ausschließliche, nicht übertragbare, nicht unterlizenzierbare, weltweite, limitierte unwiderrufliche Lizenz zur Nutzung der Daten nur in Verbindung mit und zur Unterstützung des Vertrags der US-Regierung, unter dem die Daten bereitgestellt wurden. Sofern in den vorliegenden Bedingungen nicht anders angegeben, dürfen die Daten ohne vorherige schriftliche Genehmigung von NetApp, Inc. nicht verwendet, offengelegt, vervielfältigt, geändert, aufgeführt oder angezeigt werden. Die Lizenzrechte der US-Regierung für das US-Verteidigungsministerium sind auf die in DFARS-Klausel 252.227-7015(b) (Februar 2014) genannten Rechte beschränkt.

Markeninformationen

NETAPP, das NETAPP Logo und die unter http://www.netapp.com/TM aufgeführten Marken sind Marken von NetApp, Inc. Andere Firmen und Produktnamen können Marken der jeweiligen Eigentümer sein.