Vérification de la signature du fichier

Cloud Volumes ONTAP

NetApp
June 11, 2024

Sommaire

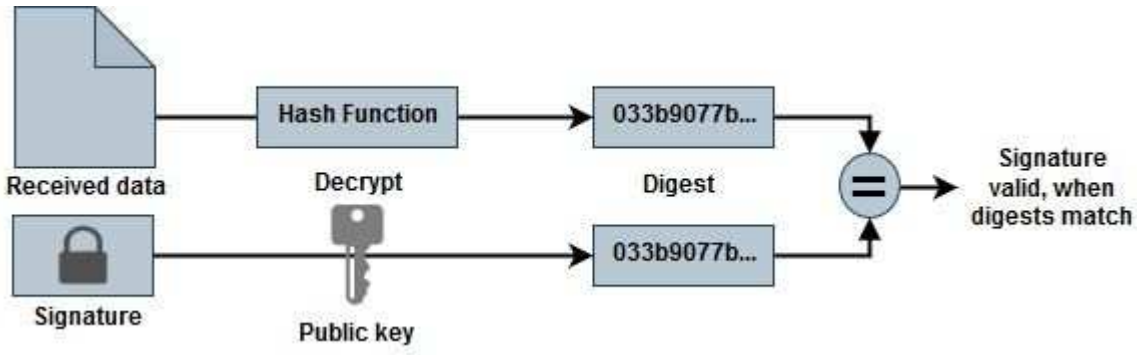
Vérification de la signature du fichier

Vérification de la signature du fichier

Le processus de vérification d'image Azure génère un résumé à partir du fichier VHD avec le principal bloc de 1 Mo et se terminant par un entrelacement de 512 octets à l'aide de la fonction de hachage. Pour correspondre à la procédure de signature, SHA256 est utilisé pour le hachage. Vous devez supprimer les 1 Mo et 512 Mo finaux du fichier VHD, puis vérifier la partie restante du fichier VHD.

Résumé du flux de travail de vérification de signature de fichier

Voici une présentation du processus de workflow de vérification de signature de fichier.



- Téléchargez le fichier Azure image Digest sur le "Site de support NetApp" et extrayez le fichier digest(.sig), le fichier de certificat de clé publique (.pem) et le fichier de certificat de chaîne (.pem).

  Reportez-vous à la "Téléchargez le fichier condensé d'images Azure" pour en savoir plus.

- Vérifier la chaîne de confiance.
- Extrayez la clé publique (.pub) du certificat de clé publique (.pem).
- La clé publique extraite est utilisée pour décrypter le fichier d'analyse. Le résultat est ensuite comparé à un nouveau résumé non chiffré du fichier temporaire créé à partir du fichier image avec 1 Mo de tête et 512 octets de fin supprimés.

  Cette étape est réalisée à l'aide de la commande openssl suivante.

  - L'instruction CLI générale s'affiche comme suit :

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

  - L'outil CLI OpenSSL affiche un message « vérifié OK » si les fichiers correspondent et « échec de vérification » s'ils ne correspondent pas.

Vérification de signature de fichier sous Linux

Vous pouvez vérifier une signature de fichier VHD exportée pour Linux en suivant les étapes ci-dessous.

Étapes

1. Téléchargez le fichier Azure image Digest sur le "Site de support NetApp" et extrayez le fichier digest(.sig), le fichier de certificat de clé publique (.pem) et le fichier de certificat de chaîne (.pem).

   Reportez-vous à la "Téléchargez le fichier condensé d'images Azure" pour en savoir plus.

2. Vérifier la chaîne de confiance.

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

3. Retirez le premier 1 Mo (1048576 octets) et terminez par 512 octets de fichier VHD.

   Si 'queue' est utilisé, l'option '-c +K' sort des octets commençant par les octets KTH du fichier spécifié. Par conséquent, 1048577 est passé à 'queue -c'.

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

4. Utilisez openssl pour extraire la clé publique du certificat et vérifier le fichier rayé(sign.tmp) avec le fichier de signature et la clé publique.

   Si le fichier d'entrée réussit la vérification, la commande s'affiche « Vérification OK ». Sinon, « échec de vérification » s'affiche.

```
% 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. Nettoyez l'espace de travail.

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

Vérification de signature de fichier sous Mac OS

Vous pouvez vérifier une signature de fichier VHD exportée pour Mac OS en suivant les étapes ci-dessous.

Étapes

1. Téléchargez le fichier Azure image Digest sur le "Site de support NetApp" et extrayez le fichier digest(.sig), le fichier de certificat de clé publique (.pem) et le fichier de certificat de chaîne (.pem).

   Reportez-vous à la "Téléchargez le fichier condensé d'images Azure" pour en savoir plus.

2. Vérifier la chaîne de confiance.

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

3. Supprimez le premier 1 Mo (1048576 octets) et terminez par 512 octets de fichier VHD.

   Si 'queue' est utilisé, l'option '-c +K' sort des octets commençant par les octets KTH du fichier spécifié. Par conséquent, 1048577 est passé à 'queue -c'. Il prend environ 13m Pour que la commande de queue se termine sous 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. Utilisez openssl pour extraire la clé publique du certificat et vérifier la bande file(sign.tmp) avec le fichier de signature et la clé publique.

   Si le fichier d'entrée réussit la vérification, la commande affiche « Vérification OK ». Sinon, « échec de vérification » s'affiche.

```
% 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. Nettoyez l’espace de travail.

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

Informations sur le copyright

Informations sur les marques commerciales