



Vérification de la signature du fichier

Cloud Volumes ONTAP

NetApp
June 11, 2024

Sommaire

- Vérification de la signature du fichier 1
- Vérification de la signature du fichier 1
- Vérification de signature de fichier sous Linux 2
- Vérification de signature de fichier sous Mac OS 3

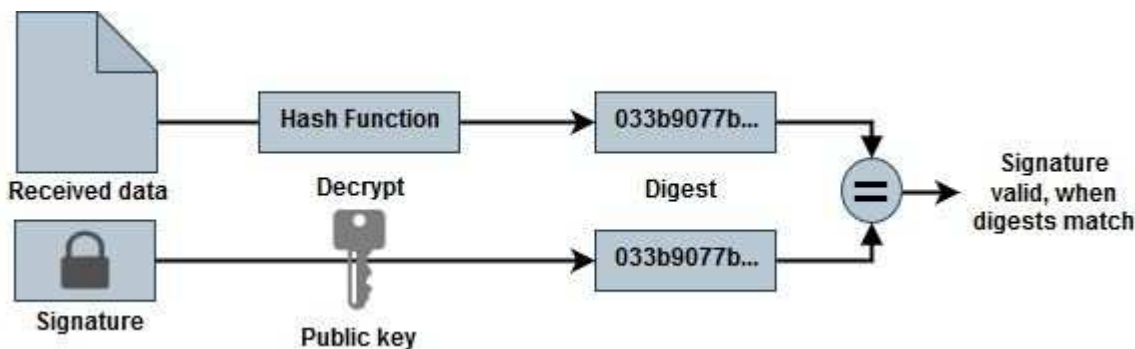
Vérification de la signature du fichier

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

Copyright © 2024 NetApp, Inc. Tous droits réservés. Imprimé aux États-Unis. Aucune partie de ce document protégé par copyright ne peut être reproduite sous quelque forme que ce soit ou selon quelque méthode que ce soit (graphique, électronique ou mécanique, notamment par photocopie, enregistrement ou stockage dans un système de récupération électronique) sans l'autorisation écrite préalable du détenteur du droit de copyright.

Les logiciels dérivés des éléments NetApp protégés par copyright sont soumis à la licence et à l'avis de non-responsabilité suivants :

CE LOGICIEL EST FOURNI PAR NETAPP « EN L'ÉTAT » ET SANS GARANTIES EXPRESSES OU TACITES, Y COMPRIS LES GARANTIES TACITES DE QUALITÉ MARCHANDE ET D'ADÉQUATION À UN USAGE PARTICULIER, QUI SONT EXCLUES PAR LES PRÉSENTES. EN AUCUN CAS NETAPP NE SERA TENU POUR RESPONSABLE DE DOMMAGES DIRECTS, INDIRECTS, ACCESSOIRES, PARTICULIERS OU EXEMPLAIRES (Y COMPRIS L'ACHAT DE BIENS ET DE SERVICES DE SUBSTITUTION, LA PERTE DE JOUISSANCE, DE DONNÉES OU DE PROFITS, OU L'INTERRUPTION D'ACTIVITÉ), QUELLES QU'EN SOIENT LA CAUSE ET LA DOCTRINE DE RESPONSABILITÉ, QU'IL S'AGISSE DE RESPONSABILITÉ CONTRACTUELLE, STRICTE OU DÉLICTEUELLE (Y COMPRIS LA NÉGLIGENCE OU AUTRE) DÉCOULANT DE L'UTILISATION DE CE LOGICIEL, MÊME SI LA SOCIÉTÉ A ÉTÉ INFORMÉE DE LA POSSIBILITÉ DE TELS DOMMAGES.

NetApp se réserve le droit de modifier les produits décrits dans le présent document à tout moment et sans préavis. NetApp décline toute responsabilité découlant de l'utilisation des produits décrits dans le présent document, sauf accord explicite écrit de NetApp. L'utilisation ou l'achat de ce produit ne concède pas de licence dans le cadre de droits de brevet, de droits de marque commerciale ou de tout autre droit de propriété intellectuelle de NetApp.

Le produit décrit dans ce manuel peut être protégé par un ou plusieurs brevets américains, étrangers ou par une demande en attente.

LÉGENDE DE RESTRICTION DES DROITS : L'utilisation, la duplication ou la divulgation par le gouvernement sont sujettes aux restrictions énoncées dans le sous-paragraphe (b)(3) de la clause Rights in Technical Data-Noncommercial Items du DFARS 252.227-7013 (février 2014) et du FAR 52.227-19 (décembre 2007).

Les données contenues dans les présentes se rapportent à un produit et/ou service commercial (tel que défini par la clause FAR 2.101). Il s'agit de données propriétaires de NetApp, Inc. Toutes les données techniques et tous les logiciels fournis par NetApp en vertu du présent Accord sont à caractère commercial et ont été exclusivement développés à l'aide de fonds privés. Le gouvernement des États-Unis dispose d'une licence limitée irrévocable, non exclusive, non cessible, non transférable et mondiale. Cette licence lui permet d'utiliser uniquement les données relatives au contrat du gouvernement des États-Unis d'après lequel les données lui ont été fournies ou celles qui sont nécessaires à son exécution. Sauf dispositions contraires énoncées dans les présentes, l'utilisation, la divulgation, la reproduction, la modification, l'exécution, l'affichage des données sont interdits sans avoir obtenu le consentement écrit préalable de NetApp, Inc. Les droits de licences du Département de la Défense du gouvernement des États-Unis se limitent aux droits identifiés par la clause 252.227-7015(b) du DFARS (février 2014).

Informations sur les marques commerciales

NETAPP, le logo NETAPP et les marques citées sur le site <http://www.netapp.com/TM> sont des marques déposées ou des marques commerciales de NetApp, Inc. Les autres noms de marques et de produits sont des marques commerciales de leurs propriétaires respectifs.