



Vérifier la signature du fichier

Cloud Volumes ONTAP

NetApp
February 13, 2026

This PDF was generated from <https://docs.netapp.com/fr-fr/storage-management-cloud-volumes-ontap/concept-azure-file-sig-verify.html> on February 13, 2026. Always check docs.netapp.com for the latest.

Sommaire

- Vérifier la signature du fichier 1
 - Vérification de la signature d'image de la place de marché Azure pour Cloud Volumes ONTAP 1
 - Résumé du flux de travail de vérification de la signature du fichier 1
 - Vérifier la signature de l'image de la place de marché Azure pour Cloud Volumes ONTAP sur Linux 1
 - Vérifier la signature de l'image de la place de marché Azure pour Cloud Volumes ONTAP sur macOS 3

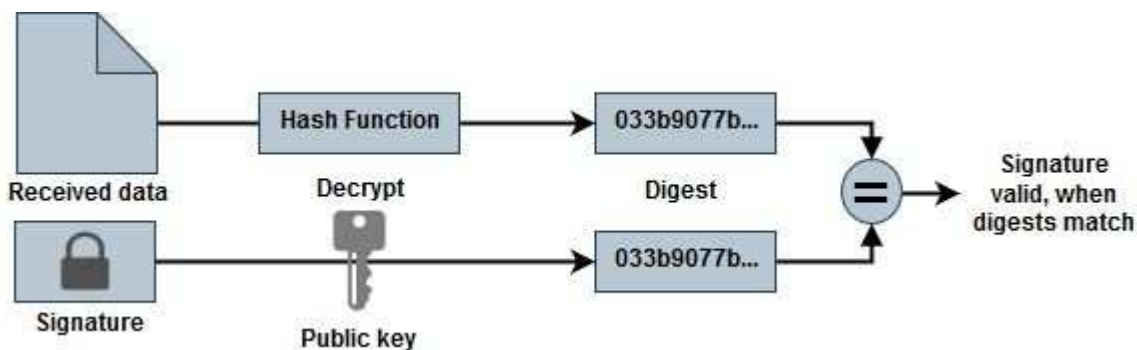
Vérifier la signature du fichier

Vérification de la signature d'image de la place de marché Azure pour Cloud Volumes ONTAP

Le processus de vérification d'image Azure génère un fichier de résumé à partir du fichier VHD en supprimant 1 Mo au début et 512 octets à la fin, puis en appliquant une fonction de hachage. Pour correspondre à la procédure de signature, *sha256* est utilisé pour le hachage.

Résumé du flux de travail de vérification de la signature du fichier

Voici un aperçu du processus de vérification de la signature du fichier.



- Téléchargement de l'image Azure à partir du ["Site de support NetApp"](#) et extraire le fichier digest (.sig), le fichier de certificat de clé publique (.pem) et le fichier de certificat de chaîne (.pem). Consultez ["Téléchargez le fichier de résumé de l'image Azure"](#) pour plus d'informations.
- Vérification de la chaîne de confiance.
- Extraction de la clé publique (.pub) du certificat de clé publique (.pem).
- Décryptage du fichier digest en utilisant la clé publique extraite.
- Comparaison du résultat avec un condensé nouvellement généré d'un fichier temporaire créé à partir du fichier image après avoir supprimé 1 Mo au début et 512 octets à la fin. Cette étape est réalisée à l'aide de l'outil de ligne de commande OpenSSL. L'outil OpenSSL CLI affiche un message approprié en cas de réussite ou d'échec de la correspondance des fichiers.

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

Vérifier la signature de l'image de la place de marché Azure pour Cloud Volumes ONTAP sur Linux

La vérification d'une signature de fichier VHD exportée sous Linux comprend la validation de la chaîne de confiance, la modification du fichier et la vérification de la signature.

Étapes

1. Téléchargez le fichier image Azure à partir du ["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).

Se référer à ["Téléchargez le fichier de résumé de l'image Azure"](#) pour plus d'informations.

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 1 Mo (1 048 576 octets) au début et 512 octets à la fin du fichier VHD. Lors de l'utilisation `tail`, le `-c +K` l'option génère des octets à partir du K-ième octet du fichier. Par conséquent, il passe 1048577 à `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. Utilisez OpenSSL pour extraire la clé publique du certificat et vérifiez le fichier dépouillé (sign.tmp) avec le fichier de signature et la clé publique.

L'invite de commande affiche des messages indiquant la réussite ou l'échec en fonction de la vérification.

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

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

Vérifier la signature de l'image de la place de marché Azure pour Cloud Volumes ONTAP sur macOS

La vérification d'une signature de fichier VHD exportée sous Linux comprend la validation de la chaîne de confiance, la modification du fichier et la vérification de la signature.

Étapes

1. Téléchargez le fichier image Azure à partir du ["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).

Se référer à ["Téléchargez le fichier de résumé de l'image Azure"](#) pour plus d'informations.

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 1 Mo (1 048 576 octets) au début et 512 octets à la fin du fichier VHD. Lors de l'utilisation `tail`, le `-c +K` l'option génère des octets à partir du K-ième octet du fichier. Par conséquent, il passe 1048577 à `tail -c`. Notez que sur macOS, l'exécution de la commande `tail` peut prendre environ dix minutes.

```
% 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 vérifiez le fichier dépouillé (sign.tmp) avec le fichier de signature et la clé publique. L'invite de commande affiche des messages indiquant la réussite ou l'échec en fonction de la vérification.

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

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

Informations sur le copyright

Copyright © 2026 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 DÉLICTELLE (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.