Vérifier l'image de la plateforme Azure

Cloud Volumes ONTAP

NetApp
February 13, 2026

Sommaire

Vérifier l’image de la plateforme Azure

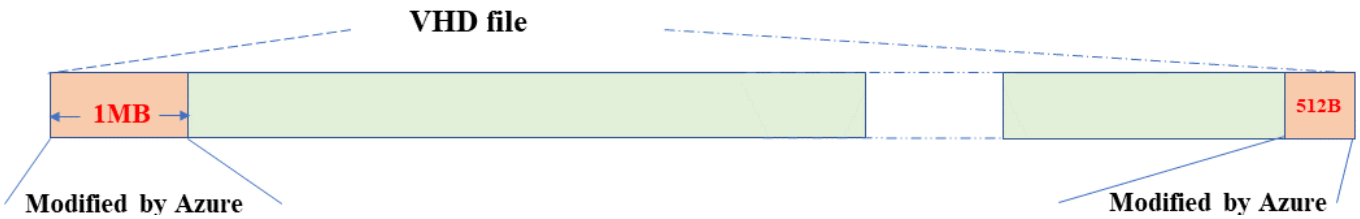
Vérification d’image de la place de marché Azure pour Cloud Volumes ONTAP

La vérification des images Azure est conforme aux exigences de sécurité renforcées de NetApp . La vérification d’un fichier image est un processus simple. Cependant, la vérification de la signature de l’image Azure nécessite des considérations spécifiques pour le fichier image Azure VHD, car il est modifié sur la place de marché Azure.

La vérification d’image Azure est prise en charge sur Cloud Volumes ONTAP 9.15.0 et versions ultérieures.

Modification des fichiers VHD publiés par Azure

Les 1 Mo (1048576 octets) au début et les 512 octets à la fin du fichier VHD sont modifiés par Azure. NetApp signe le fichier VHD restant.



Dans l’exemple, le fichier VHD est de 10 Go. La partie signée par NetApp est marquée en vert (10 Go - 1 Mo - 512 octets).

Liens connexes

- "Blog sur les erreurs de page : Comment signer et vérifier avec OpenSSL"
- "Utiliser l’image Azure Marketplace pour créer une image de machine virtuelle pour votre GPU Azure Stack Edge Pro | Microsoft Learn"
- "Exporter/copier un disque géré vers un compte de stockage via Azure CLI | Microsoft Learn"
- "Démarrage rapide d’Azure Cloud Shell - Bash | Microsoft Learn"
- "Comment installer Azure CLI | Microsoft Learn"
- "Copie de blob de stockage AZ | Microsoft Learn"
- "Sign in avec Azure CLI — Connexion et authentification | Microsoft Learn"

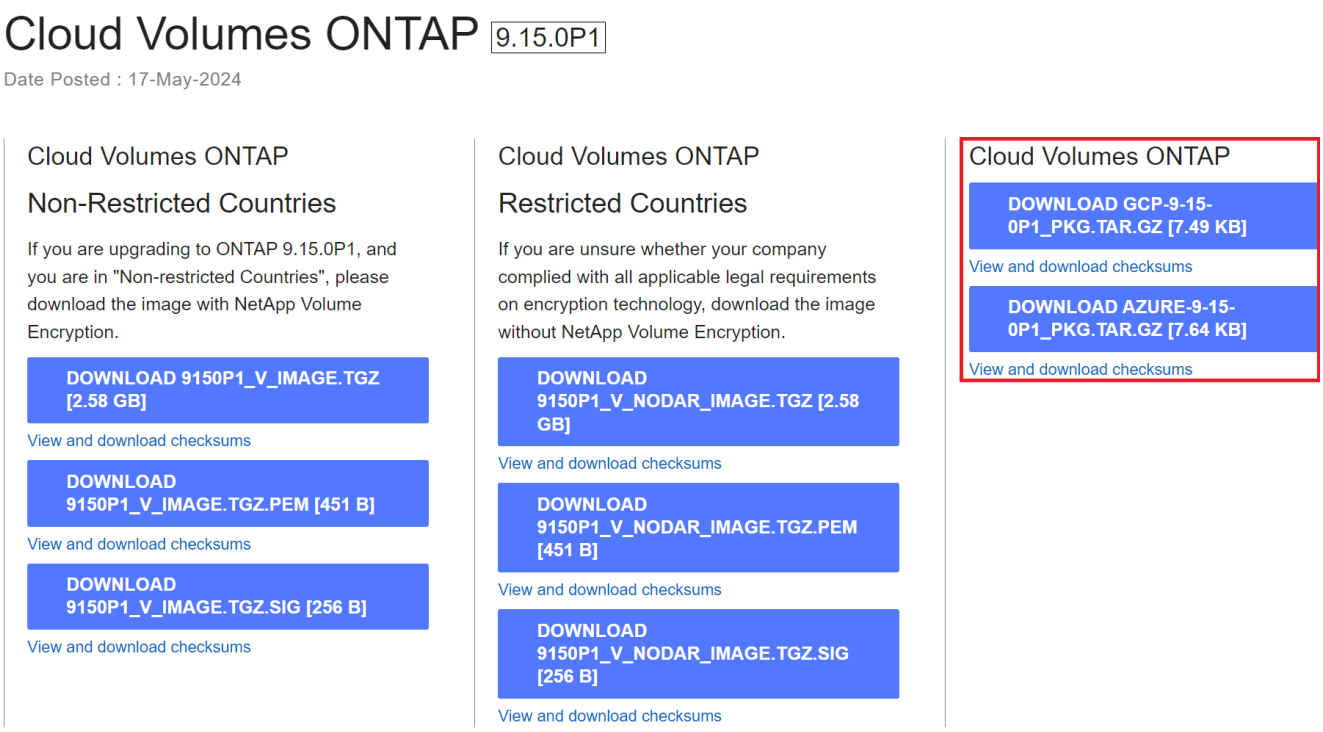
Téléchargez le fichier image Azure pour Cloud Volumes ONTAP

Vous pouvez télécharger le fichier image Azure à partir du "Site de support NetApp" .

Le fichier *tar.gz* contient les fichiers nécessaires à la vérification de la signature de l’image. En plus du fichier *tar.gz*, vous devez également télécharger le fichier *checksum* de l’image. Le fichier de somme de contrôle contient le `md5` et `sha256` sommes de contrôle du fichier *tar.gz*.

Étapes

1. Aller à la "Page produit Cloud Volumes ONTAP sur le site de support NetApp" et téléchargez la version du logiciel requise à partir de la section **Téléchargements**.
2. Sur la page de téléchargement de Cloud Volumes ONTAP , cliquez sur le fichier téléchargeable pour l'image Azure et téléchargez le fichier *tar.gz*.



3. Sous Linux, exécutez `md5sum AZURE-<version>_PKG.TAR.GZ` .

   Sur macOS, exécutez `sha256sum AZURE-<version>_PKG.TAR.GZ` .

4. Vérifiez que le `md5sum` et `sha256sum` les valeurs correspondent à celles de l'image Azure téléchargée.
5. Sous Linux et macOS, extrayez le fichier *tar.gz* à l'aide de la commande `tar -xzf` commande.

   Le fichier *tar.gz* extrait contient le fichier digest (*.sig*), le fichier de certificat de clé publique (*.pem*) et le fichier de certificat de chaîne (*.pem*).

   Exemple de sortie après extraction du fichier tar.gz :

```
$ ls cert/ -l
-rw-r----- 1 netapp netapp  384 May  13 13:00 9.15.0P1_azure_digest.sig
-rw-r----- 1 netapp netapp 2365 May  13 13:00 Certificate-
9.15.0P1_azure.pem
-rw-r----- 1 netapp netapp 8537 May  13 13:00 Certificate-Chain-
9.15.0P1_azure.pem
-rw-r----- 1 netapp netapp 8537 May  13 13:00 version_readme
```

Exporter des images VHD pour Cloud Volumes ONTAP depuis la place de marché Azure

Une fois l'image VHD publiée sur le cloud Azure, elle n'est plus gérée par NetApp. Au lieu de cela, l'image publiée est placée sur la place de marché Azure. Lorsque l'image est préparée et publiée sur la place de marché Azure, Azure modifie 1 Mo au début et 512 octets à la fin du VHD. Pour vérifier la signature du fichier VHD, vous devez exporter l'image VHD modifiée par Azure à partir de la place de marché Azure.

Avant de commencer

Assurez-vous que l'interface de ligne de commande Azure est installée sur votre système ou qu'Azure Cloud Shell est disponible via le portail Azure. Pour plus d'informations sur l'installation de l'interface de ligne de commande Azure, reportez-vous à la "Documentation Microsoft : Comment installer Azure CLI" .

Étapes

1. Mappez la version Cloud Volumes ONTAP sur votre système à la version de l'image de la place de marché Azure à l'aide du contenu du fichier *version_readme*. La version Cloud Volumes ONTAP est représentée par `buildname` et la version de l'image de la place de marché Azure est représentée par `version` dans les mappages de versions.

   Dans l'exemple suivant, la version Cloud Volumes ONTAP `9.15.0P1` est mappé à la version de l'image de la place de marché Azure `9150.01000024.05090105` . Cette version d'image de la place de marché Azure est utilisée ultérieurement pour définir l'URN de l'image.

   ```
   [
    "buildname": "9.15.0P1",
       "publisher": "netapp",
        "version": "9150.01000024.05090105"

   ]
   ```

2. Identifiez la région dans laquelle vous souhaitez créer les machines virtuelles. Le nom de la région est utilisé comme valeur pour le `locName` variable lors de la définition de l'URN de l'image du marché. Pour lister les régions disponibles, exécutez cette commande :

   ```
   az account list-locations -o table
   ```

   Dans ce tableau, le nom de la région apparaît dans le `Name` champ.

```
$ az account list-locations -o table
DisplayName               Name                 RegionalDisplayName
------------------------  -------------------
-----------------------------------
East US                   eastus               (US) East US
East US 2                 eastus2              (US) East US 2
South Central US          southcentralus       (US) South Central US
...
```

3. Consultez les noms de référence (SKU) pour les versions Cloud Volumes ONTAP correspondantes et les types de déploiement de machine virtuelle dans le tableau ci-dessous. Le nom du SKU est utilisé comme valeur pour le `skuName` variable lors de la définition de l'URN de l'image du marché.

   Par exemple, tous les déploiements à nœud unique avec Cloud Volumes ONTAP 9.15.0 doivent utiliser `ontap_cloud_byol` comme nom de référence.

* Version Cloud Volumes ONTAP *	**Déploiement de VM via**	**Nom du SKU**
9.17.1 et versions ultérieures	La place de marché Azure	ontap_cloud_direct_gen2
9.17.1 et versions ultérieures	La NetApp Console	ontap_cloud_gen2
9.16.1	La place de marché Azure	ontap_cloud_direct
9.16.1	La console	ontap_cloud
9.15.1	La console	ontap_cloud
9.15.0	La console, déploiements à nœud unique	ontap_cloud_byol
9.15.0	La console, déploiements haute disponibilité (HA)	ontap_cloud_byol_ha

4. Après avoir mappé la version ONTAP et l'image de la place de marché Azure, exportez le fichier VHD à partir de la place de marché Azure à l'aide d'Azure Cloud Shell ou d'Azure CLI.

Exporter un fichier VHD à l'aide d'Azure Cloud Shell sous Linux

À partir d'Azure Cloud Shell, exportez l'image de la place de marché vers le fichier VHD (par exemple, *9150.01000024.05090105.vhd*) et téléchargez-la sur votre système Linux local. Effectuez ces étapes pour obtenir l'image VHD à partir de la place de marché Azure.

Étapes

1. Définissez l'URN et d'autres paramètres de l'image du marché. Le format URN est `<publisher>:<offer>:<sku>:<version>` . Vous pouvez également répertorier les images du marché NetApp pour confirmer la version d'image correcte.

```
PS /home/user1> $urn="netapp:netapp-ontap-
cloud:ontap_cloud_byol:9150.01000024.05090105"
PS /home/user1> $locName="eastus2"
PS /home/user1> $pubName="netapp"
PS /home/user1> $offerName="netapp-ontap-cloud"
PS /home/user1> $skuName="ontap_cloud_byol"
PS /home/user1> Get-AzVMImage -Location $locName -PublisherName $pubName
-Offer $offerName -Sku $skuName |select version
...
141.20231128
9.141.20240131
9.150.20240213
9150.01000024.05090105
...
```

2. Créez un nouveau disque géré à partir de l'image du marketplace avec la version d'image correspondante :

```
PS /home/user1> $diskName = "9150.01000024.05090105-managed-disk"
PS /home/user1> $diskRG = "fnf1"
PS /home/user1> az disk create -g $diskRG -n $diskName --image-reference
$urn
PS /home/user1> $sas = az disk grant-access --duration-in-seconds 3600
--access-level Read --name $diskName --resource-group $diskRG
PS /home/user1> $diskAccessSAS = ($sas | ConvertFrom-Json)[0].accessSas
```

3. Exportez le fichier VHD du disque géré vers le stockage Azure. Créez un conteneur avec le niveau d'accès approprié. Dans cet exemple, nous avons utilisé un conteneur nommé `vm-images` avec `Container` niveau d'accès. Obtenez la clé d'accès au compte de stockage à partir du portail Azure : **Comptes de stockage > *examplesaname* > Clé d'accès > *key1* > *key* > Afficher > <*copie*>**

```
PS /home/user1> $storageAccountName = “examplesaname”
PS /home/user1> $containerName = “vm-images”
PS /home/user1> $storageAccountKey = "<replace with the above access
key>"
PS /home/user1> $destBlobName = “9150.01000024.05090105.vhd”
PS /home/user1> $destContext = New-AzureStorageContext
-StorageAccountName $storageAccountName -StorageAccountKey
$storageAccountKey
PS /home/user1> Start-AzureStorageBlobCopy -AbsoluteUri $diskAccessSAS
-DestContainer $containerName -DestContext $destContext -DestBlob
$destBlobName
PS /home/user1> Get-AzureStorageBlobCopyState –Container $containerName
–Context $destContext -Blob $destBlobName
```

4. Téléchargez l’image générée sur votre système Linux. Utilisez le `wget` commande pour télécharger le fichier VHD :

```
wget <URL of filename/Containers/vm-images/9150.01000024.05090105.vhd>
```

L’URL suit un format standard. Pour l’automatisation, vous pouvez dériver la chaîne URL comme indiqué ci-dessous. Vous pouvez également utiliser l’interface de ligne de commande Azure. `az` commande pour obtenir l’URL. Exemple d’URL :https://examplesaname.bluexpinfraprod.eastus2.data.azurecr.io/vm-images/9150.01000024.05090105.vhd[]

5. Nettoyer le disque géré

```
PS /home/user1> Revoke-AzDiskAccess -ResourceGroupName $diskRG -DiskName
$diskName
PS /home/user1> Remove-AzDisk -ResourceGroupName $diskRG -DiskName
$diskName
```

Exporter un fichier VHD à l’aide d’Azure CLI sous Linux

Exportez l’image de la place de marché vers un fichier VHD à l’aide de l’interface de ligne de commande Azure à partir d’un système Linux local.

Étapes

1. Connectez-vous à l’interface de ligne de commande Azure et répertoriez les images de la place de marché :

```
% az login --use-device-code
```

2. Pour vous connecter, utilisez un navigateur Web pour ouvrir la page https://microsoft.com/devicelogin et entrez le code d’authentification.

```
% az vm image list --all --publisher netapp --offer netapp-ontap-cloud
--sku ontap_cloud_byol
...
{
"architecture": "x64",
"offer": "netapp-ontap-cloud",
"publisher": "netapp",
"sku": "ontap_cloud_byol",
"urn": "netapp:netapp-ontap-
cloud:ontap_cloud_byol:9150.01000024.05090105",
"version": "9150.01000024.05090105"
},
...
```

3. Créez un nouveau disque géré à partir de l'image du marché avec la version d'image correspondante.

```
% export urn="netapp:netapp-ontap-
cloud:ontap_cloud_byol:9150.01000024.05090105"
% export diskName="9150.01000024.05090105-managed-disk"
% export diskRG="new_rg_your_rg"
% az disk create -g $diskRG -n $diskName --image-reference $urn
% az disk grant-access --duration-in-seconds 3600 --access-level Read
--name $diskName --resource-group $diskRG
{
  "accessSas": "https://md-
xxxxxx.bluexpinfraprod.eastus2.data.azurecr.io/xxxxxxx/abcd?sv=2018-03-
28&sr=b&si=xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxx&sigxxxxxxxxxxxxxxxxxxxxxxxx"
}
% export diskAccessSAS="https://md-
xxxxxx.bluexpinfraprod.eastus2.data.azurecr.io/xxxxxxx/abcd?sv=2018-03-
28&sr=b&si=xxxxxxxx-xxxx-xx-xx-xx&sigxxxxxxxxxxxxxxxxxxxxxxxx"
```

Pour automatiser le processus, le SAS doit être extrait de la sortie standard. Consultez les documents appropriés pour obtenir des conseils.

4. Exportez le fichier VHD à partir du disque géré.

   a. Créez un conteneur avec le niveau d'accès approprié. Dans cet exemple, un conteneur nommé `vm-images` avec `Container` le niveau d'accès est utilisé.

   b. Obtenez la clé d'accès au compte de stockage à partir du portail Azure : **Comptes de stockage > *examplesaname* > Clé d'accès > *key1* > *key* > Afficher > <*copie*>**

      Vous pouvez également utiliser le `az` commande pour cette étape.

```
% export storageAccountName="examplesaname"
% export containerName="vm-images"
% export storageAccountKey="xxxxxxxxxx"
% export destBlobName="9150.01000024.05090105.vhd"

% az storage blob copy start --source-uri $diskAccessSAS --destination
-container $containerName --account-name $storageAccountName --account
-key $storageAccountKey --destination-blob $destBlobName

{
  "client_request_id": "xxxx-xxxx-xxxx-xxxx-xxxx",
  "copy_id": "xxxx-xxxx-xxxx-xxxx-xxxx",
  "copy_status": "pending",
  "date": "2022-11-02T22:02:38+00:00",
  "etag": "\"0xXXXXXXXXXXXXXXXX\"",
  "last_modified": "2022-11-02T22:02:39+00:00",
  "request_id": "xxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxx",
  "version": "2020-06-12",
  "version_id": null
}
```

5. Vérifiez l'état de la copie du blob.

```
% az storage blob show --name $destBlobName --container-name
$containerName --account-name $storageAccountName

....
    "copy": {
      "completionTime": null,
      "destinationSnapshot": null,
      "id": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxx",
      "incrementalCopy": null,
      "progress": "10737418752/10737418752",
      "source": "https://md-
xxxxxx.bluexpinfraprod.eastus2.data.azurecr.io/xxxxx/abcd?sv=2018-03-
28&sr=b&si=xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx",
      "status": "success",
      "statusDescription": null
    },
....
```

6. Téléchargez l'image générée sur votre serveur Linux.

```
wget <URL of file examplesaname/Containers/vm-
images/9150.01000024.05090105.vhd>
```

L'URL suit un format standard. Pour l'automatisation, vous pouvez dériver la chaîne URL comme indiqué ci-dessous. Vous pouvez également utiliser l'interface de ligne de commande Azure. `az` commande pour obtenir l'URL. Exemple d'URL :https://examplesaname.bluexpinfraprod.eastus2.data.azurecr.io/vm-images/9150.01000024.05090105.vhd[]

7. Nettoyer le disque géré

```
az disk revoke-access --name $diskName --resource-group $diskRG
az disk delete --name $diskName --resource-group $diskRG --yes
```

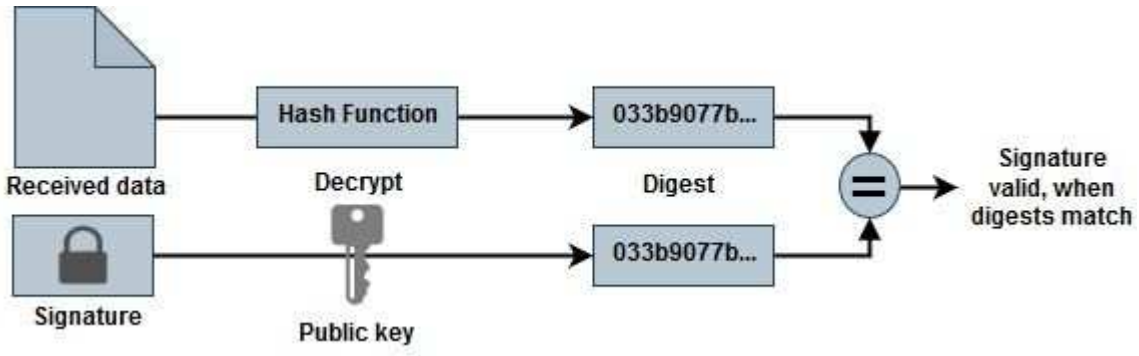
Vérifier la signature du fichier

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

Informations sur les marques commerciales