Vérification des images de la plateforme Azure

Cloud Volumes ONTAP

NetApp
June 27, 2024

Sommaire

Vérification des images de la plateforme Azure

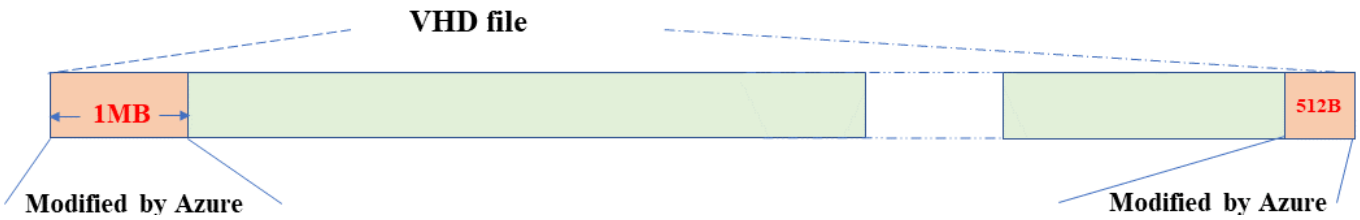
Présentation de la vérification des images Azure

La vérification des images Azure est conforme aux exigences de sécurité améliorées de NetApp. La vérification d'un fichier image est un processus simple, mais elle requiert également le transfert du fichier image VHD Azure, connu sous l'effet d'une alternance réalisée par Azure Marketplace.

> La vérification des images Azure est prise en charge par le logiciel Cloud Volumes ONTAP version 9.15.0 ou supérieure.

Modification par Azure des fichiers VHD publiés

Azure modifie le premier fichier VHD de 1 Mo (1048576 octets) à la fin de 512 octets. La signature d'image NetApp ignore le premier 1 Mo et se termine par 512 octets, et signe la partie restante de l'image VHD.



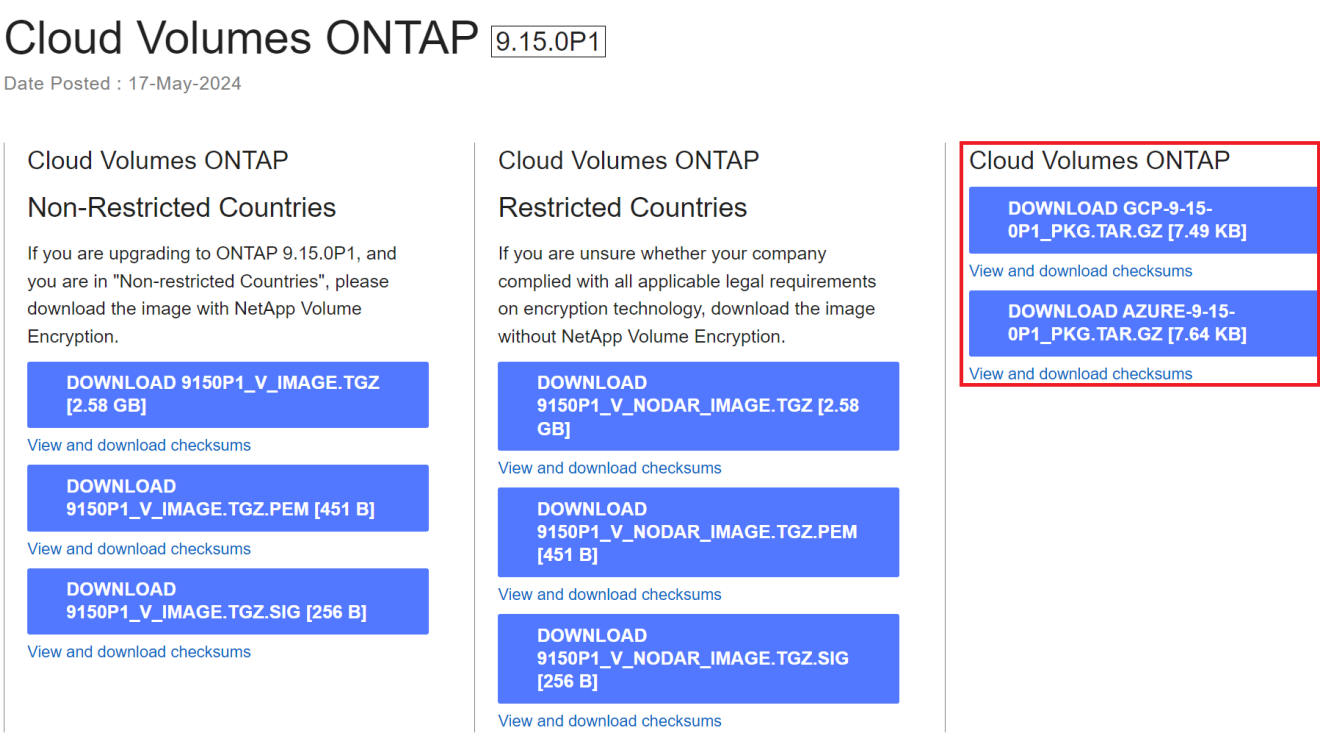
À titre d'exemple, le diagramme ci-dessus montre un fichier VHD de 10 Go. Mais la partie NetApp signée est marquée en vert avec une taille de 10GB - 1MB - 512B.

Téléchargez le fichier condensé d'images Azure

Le fichier de résumé d'image Azure peut être téléchargé à partir du "Site de support NetApp". Le téléchargement est au format tar.gz et contient des fichiers pour la vérification de la signature d'image.

Étapes

1. Accédez au "Page produit Cloud Volumes ONTAP sur le site de support NetApp" Et téléchargez la version du logiciel souhaitée dans la section Téléchargements.
2. Dans la page de téléchargement de Cloud Volumes ONTAP, cliquez sur le bouton **download** du fichier de résumé d'images Azure pour télécharger le TAR. Fichier GZ.



3. Pour Linux et MacOS, vous devez effectuer les opérations suivantes pour obtenir les fichiers md5sum et sha256sum pour le fichier Azure image Digest téléchargé.
   a. Pour md5sum, entrez le `md5sum` commande.
   b. Pour sha256sum, entrez le `sha256sum` commande.
4. Vérifiez le `md5sum` et `sha256sum` Les valeurs correspondent au téléchargement du fichier de résumé d'image Azure.
5. Sous Linux et Mac OS, exécutez `tar -xzf` pour extraire le fichier tar.gz.

   Le TAR extrait. Le fichier GZ contient le fichier digest(.SIG), le fichier de certificat de clé publique (.pem) et le fichier de certificat de chaîne (.pem).

   Liste des résultats du fichier untar 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
```

Exportation d'images depuis Azure Marketplace

Une fois l'image VHD publiée dans le cloud Azure, celle-ci n'est plus gérée par NetApp. L'image publiée est placée sur Azure Marketplace. La modification d'Azure au 1 Mo

principal et se terminant à 512 Mo du VHD se produit lorsque l'image est échelonnée et publiée sur Azure Marketplace. Pour vérifier la signature du fichier VHD, l'image VHD modifiée par Azure doit d'abord être exportée depuis Azure Marketplace.

Ce dont vous avez besoin

Vous devez installer les programmes requis sur votre système.

- L'interface de ligne de commande Azure est installée ou Azure Cloud Shell est disponible via le portail Azure.

> Pour plus d'informations sur l'installation d'Azure CLI, voir "Documentation Azure : installation de l'interface de ligne de commandes Azure".

Étapes

1. Mappez la version ONTAP à la version d'image d'Azure Marketplace en utilisant le contenu du fichier readme version_readme.

   Pour chaque mappage de version répertorié dans le fichier readme version, la version de ONTAP est représentée par « nom_build » et la version d'image d'Azure Marketplace est représentée par « version ».

   Par exemple, dans le fichier readme version suivant, la version de ONTAP « 9.15.0P1 » est mappée sur l'image Azure Marketplace version « 9150.01000024.05090105 ». Cette version d'image Azure Marketplace est ensuite utilisée pour définir l'URN de l'image.

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

2. Identifiez le nom de la région où vous souhaitez créer des machines virtuelles.

   Ce nom de région est utilisé comme valeur pour la variable "locName" lors de la définition de l'URN de l'image Marketplace.

   a. Pour recevoir une liste des régions disponibles, entrez le `az account list-locations -o table` commande.

      Dans le tableau ci-dessous, le nom de la région est appelé le champ « Nom ».

```
$ 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 le nom de référence du type de déploiement VM correspondant dans le tableau ci-dessous.

   Le nom de SKU est utilisé comme valeur pour la variable "skuName" lors de la définition de l'URN de l'image Marketplace.

   Par exemple, les déploiements à un seul nœud doivent utiliser le nom de référence « ontap_cloud_byol ».

Type de déploiement VM	Nom SKU
Nœud unique	ontap_cloud_byol
Haute disponibilité	ontap_cloud_byol_ha

4. Une fois la version ONTAP et l'image Azure Marketplace mappées, exportez le fichier VHD depuis Azure Marketplace via Azure Cloud Shell ou l'interface de ligne de commande Azure.

Exportez le fichier VHD via Azure Cloud Shell sur le portail Azure

1. À partir d'Azure Cloud Shell, exportez l'image Marketplace vers une vhd (image 2, par exemple 9150.01000024.05090105.vhd) et téléchargez-la sur votre machine locale (par exemple, une machine Linux ou un PC Windows).

Cliquez pour afficher

```
#Azure Cloud Shell on Azure portal to get VHD image from Azure
Marketplace
a) Set the URN and other parameters of the marketplace image. URN is
with format "<publisher>:<offer>:<sku>:<version>". Optionally, a
user can list NetApp marketplace images to confirm the proper image
version.
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
...

b) Create a new managed disk from the Marketplace image with the
matching image version
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

c) Export a VHD from the managed disk to Azure Storage
Create a container with proper access level. As an example, a
container named 'vm-images' with 'Container' access level is used
here.
Get storage account access key, on Azure portal, 'Storage
Accounts'/'examplesaname'/'Access Key'/'key1'/'key'/'show'/<copy>.
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

d) Download the generated image to your server, e.g., a Linux
machine.
Use "wget <URL of file examplesaname/Containers/vm-
images/9150.01000024.05090105.vhd>".
The URL is organized in a formatted way. For automation tasks, the
following example could be used to derive the URL string. Otherwise,
Azure CLI 'az' command could be issued to get the URL, which is not
covered in this guide. URL Example:
https://examplesaname.blob.core.windows.net/vm-
images/9150.01000024.05090105.vhd

e) Clean up the managed disk
PS /home/user1> Revoke-AzDiskAccess -ResourceGroupName $diskRG
-DiskName $diskName
PS /home/user1> Remove-AzDisk -ResourceGroupName $diskRG -DiskName
$diskName
```

Exportez le fichier VHD via l’interface de ligne de commande Azure à partir d’une machine Linux locale

1. Exportez l’image Marketplace vers une vhd via l’interface de ligne de commande Azure à partir d’une machine Linux locale.

Cliquez pour afficher

```
#Azure CLI on local Linux machine to get VHD image from Azure
Marketplace
a) Login Azure CLI and list marketplace images
% az login --use-device-code
To sign in, use a web browser to open the page
https://microsoft.com/devicelogin and enter the code XXXXXXXXX to
authenticate.

% 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"
},
...

b) Create a new managed disk from the Marketplace image with the
matching image version
% 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.blob.core.windows.net/xxxxxxx/abcd?sv=2018-03-
28&sr=b&si=xxxxxxxx-xxxx-xxxx-xxxx-
xxxxxxx&sigxxxxxxxxxxxxxxxxxxxxxxx"
}

% export diskAccessSAS="https://md-
xxxxxx.blob.core.windows.net/xxxxxxx/abcd?sv=2018-03-
28&sr=b&si=xxxxxxxx-xxxx-xx-xx-xx&sigxxxxxxxxxxxxxxxxxxxxxxx"
#To automate the process, the SAS needs to be extracted from the
standard output. This is not included in this guide.
```

```
c) export vhd from managed disk
Create a container with proper access level. As an example, a
container named 'vm-images' with 'Container' access level is used
here.
Get storage account access key, on Azure portal, 'Storage
Accounts'/'examplesaname'/'Access Key'/'key1'/'key'/'show'/<copy>.
There should be az command that can achieve the same, but this is
not included in this guide.
% 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": "\"0xXXXXXXXXXXXXXXXXX\"",
  "last_modified": "2022-11-02T22:02:39+00:00",
  "request_id": "xxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxx",
  "version": "2020-06-12",
  "version_id": null
}

#to check the status of the blob copying
% 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.blob.core.windows.net/xxxxx/abcd?sv=2018-03-
28&sr=b&si=xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxx",
      "status": "success",
      "statusDescription": null
```

```
    },
....

d) Download the generated image to your server, e.g., a Linux
machine.
Use "wget <URL of file examplesaname/Containers/vm-
images/9150.01000024.05090105.vhd>".
The URL is organized in a formatted way. For automation tasks, the
following example could be used to derive the URL string. Otherwise,
Azure CLI 'az' command could be issued to get the URL, which is not
covered in this guide. URL Example:
https://examplesaname.blob.core.windows.net/vm-
images/9150.01000024.05090105.vhd

e) Clean up the managed disk
az disk revoke-access --name $diskName --resource-group $diskRG
az disk delete --name $diskName --resource-group $diskRG --yes
```

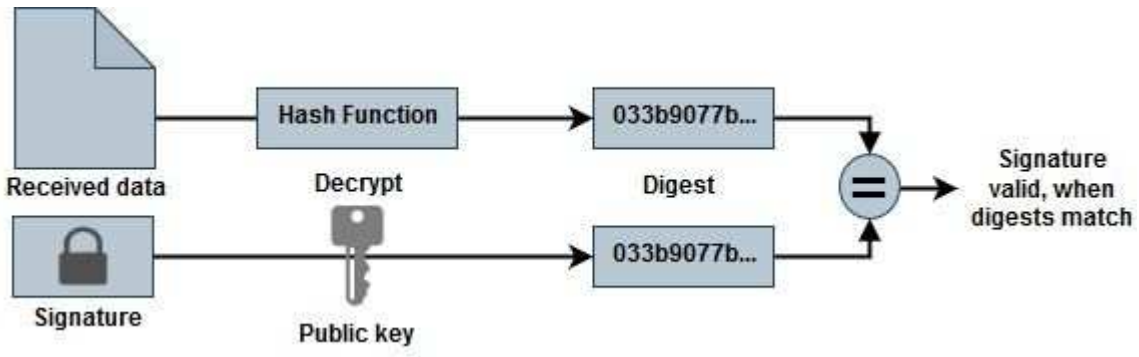
Vérification de la signature du fichier

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
```

Où trouver des informations supplémentaires sur la vérification des images Azure

Pour plus d'informations sur Azure image Verification, cliquez sur les liens ci-dessous. Les liens ci-dessous vous permettent d'accéder à des sites qui ne sont pas des sites NetApp.

Références

- "Page Fault Blog : comment signer et vérifier à l'aide d'OpenSSL"
- "Utilisez l'image Azure Marketplace pour créer l'image de machine virtuelle pour votre processeur graphique Azure Stack Edge Pro | Microsoft Learn"
- "Exportez/copiez un disque géré vers un compte de stockage à l'aide de l'interface de ligne de commande Azure | Microsoft Learn"
- "Démarrage rapide d'Azure Cloud Shell - Bash | Microsoft Learn"
- "Installation de l'interface de ligne de commande Azure | Microsoft Learn"
- "Copie d'objets blob de stockage az | Microsoft Learn"
- "Connectez-vous à l'aide de l'interface de ligne de commande Azure : connexion et authentification | Microsoft Learn"

Informations sur le copyright

Informations sur les marques commerciales