Image-Verifizierung Für Azure Plattform

Cloud Volumes ONTAP

NetApp
June 11, 2024

Inhalt

Image-Verifizierung Für Azure Plattform

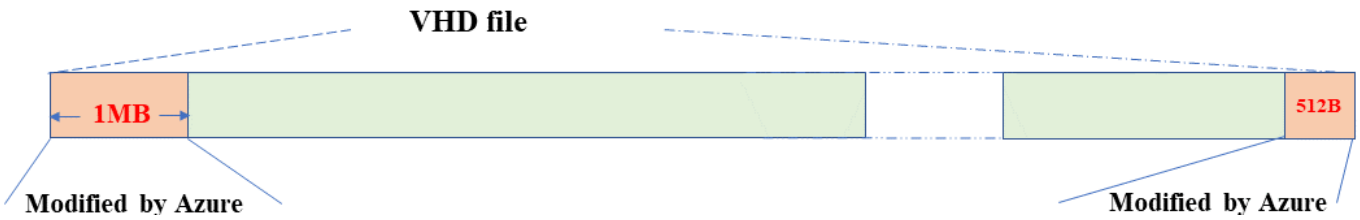
Azure Image Verifizierung – Übersicht

Die Azure-Image-Verifizierung erfüllt erweiterte Sicherheitsanforderungen von NetApp. Die Verifizierung einer Bilddatei ist zwar ein einfacher Vorgang, doch aufgrund eines Wechsels des Azure Marketplace erfordert die Überprüfung der Bildsignaturen bei Azure aufgrund einer speziellen Übergabe an die bekannte Azure VHD Bilddatei.

Die Azure-Image-Verifizierung wird von der Cloud Volumes ONTAP Softwareversion 9.15.0 oder höher unterstützt.

Änderung veröffentlichter VHD-Dateien in Azure

Die führende 1MB (1048576 Byte) und die letzte 512 Byte VHD-Datei wird von Azure geändert. NetApp Image Signing überspringt die ersten 1 MB und die letzten 512 Byte und signiert den verbleibenden VHD-Bildbereich.



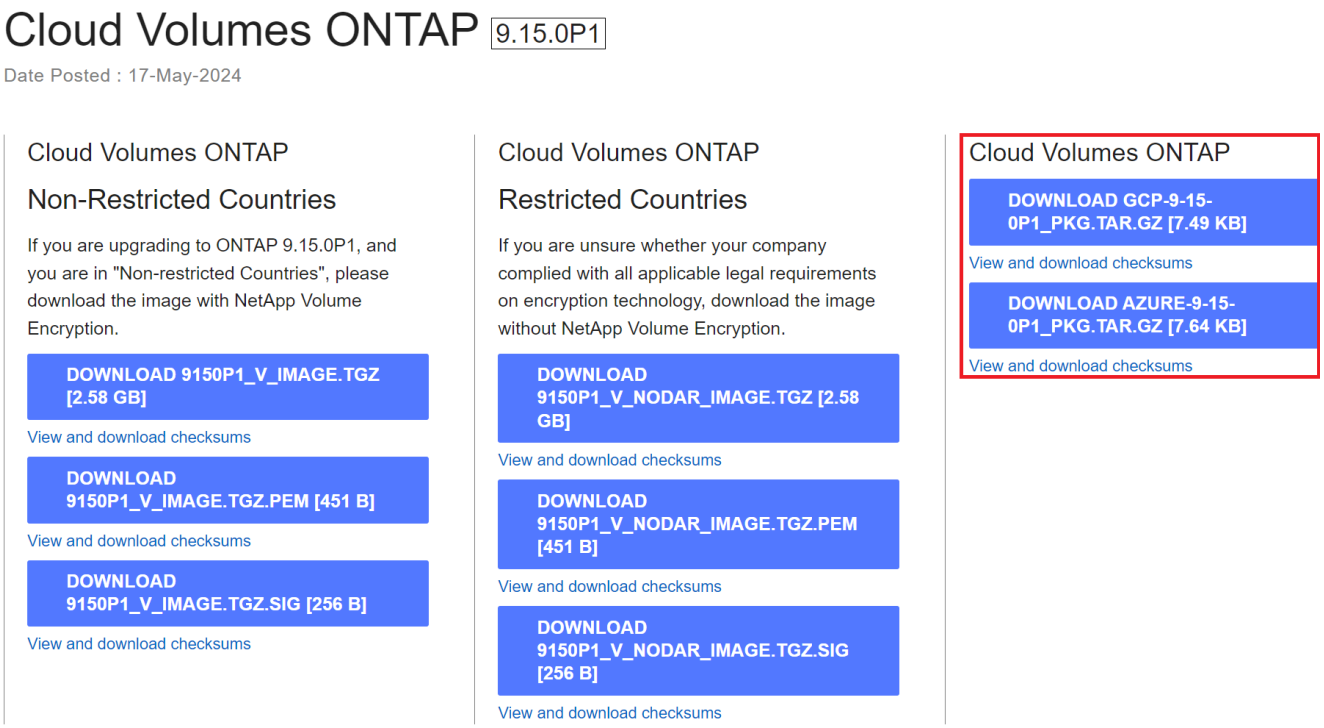
Das obige Diagramm zeigt als Beispiel eine VHD-Datei mit einer Größe von 10 GB. Aber der NetApp-signierte Teil ist grün mit einer Größe von 10GB - 1MB - 512B markiert.

Azure Image Digest Datei herunterladen

Die Azure Image Digest-Datei kann von der heruntergeladen werden "NetApp Support Website". Der Download wurde im Format tar.gz heruntergeladen und enthält Dateien zur Überprüfung der Bildsignatur.

Schritte

1. Wechseln Sie zum "Cloud Volumes ONTAP Produktseite auf der NetApp Support-Website" Und laden Sie die gewünschte Softwareversion im Abschnitt Downloads herunter.
2. Klicken Sie auf der Cloud Volumes ONTAP-Download-Seite auf den **Download-Button** für die Azure-Image-Digest-Datei, um den TAR herunterzuladen. GZ-Datei.



3. Für Linux und MacOS müssen Sie Folgendes ausführen, um md5sum und sha256sum für die heruntergeladene Azure Image Digest-Datei zu erhalten.
   a. Geben Sie für md5sum den ein `md5sum` Befehl.
   b. Geben Sie für sha256sum den ein `sha256sum` Befehl.
4. Überprüfen Sie die `md5sum` Und `sha256sum` Die Werte stimmen mit dem Download der Azure Image Digest Datei überein.
5. Führen Sie unter Linux und Mac OS die aus `tar -xzf` Befehl, um die Datei tar.gz zu extrahieren.

   Das extrahierte TAR. Die GZ-Datei enthält die Digest-Datei(.SIG), die Zertifikatdatei mit öffentlichem Schlüssel (.pem) und die Zertifikatdatei mit Kettenzertifikat (.pem).

   Ergebnis der untar tar.gz-Datei auflisten

```
$ 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
```

Bildexport aus Azure Marketplace

Nachdem das VHD-Image in der Azure Cloud veröffentlicht wurde, wird das Image nicht mehr von NetApp gemanagt. Stattdessen wird das veröffentlichte Bild auf dem Azure

Marketplace platziert. Die Änderung der führenden 1 MB und der letzten 512 B der VHD durch Azure tritt auf, wenn das Image bereitgestellt und auf dem Azure Marketplace veröffentlicht wird. Um die Signatur der VHD-Datei zu überprüfen, muss das von Azure geänderte VHD-Image zuerst aus dem Azure Marketplace exportiert werden.

Was Sie benötigen

Sie müssen die erforderlichen Programme auf Ihrem System installieren.

- Azure CLI ist installiert oder Azure Cloud Shell ist über das Azure-Portal jederzeit verfügbar.

> Weitere Informationen zum Installieren der Azure-CLI finden Sie unter "Azure-Dokumentation: Installieren von Azure CLI".

Schritte

1. Ordnen Sie die ONTAP-Version mithilfe des Inhalts der Datei „Version_readme“ der Azure Marketplace-Bildversion zu.

   Für jede Versionszuordnung, die in der Datei Version_readme aufgeführt ist, wird die ONTAP-Version durch „buildname“ und die Azure Marketplace Image-Version durch „Version“ dargestellt.

   In der folgenden Datei „Version_readme“ ist beispielsweise die ONTAP-Version „915.0P1“ der Azure Marketplace-Image-Version „9150.01000024.05090105“ zugeordnet. Diese Azure Marketplace-Image-Version wird später verwendet, um die Image-URN festzulegen.

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

2. Geben Sie den Namen der Region an, in der Sie VMs erstellen möchten.

   Dieser Name der Region wird als Wert für die Variable „locName“ verwendet, wenn die URN des Marktplatzbildes festgelegt wird.

   a. Um eine Liste der verfügbaren Regionen zu erhalten, geben Sie den ein `az account list-locations -o table` Befehl.

      In der folgenden Tabelle wird der Name der Region als Feld „Name“ bezeichnet.

```
$ 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. Überprüfen Sie den SKU-Namen für den entsprechenden VM-Bereitstellungstyp aus der folgenden Tabelle.

   Der SKU-Name wird als Wert für die Variable „skuName“ verwendet, wenn die URN des Marketplace-Images festgelegt wird.

   Beispielsweise sollten für Single-Node-Implementierungen der SKU-Name „ontap_Cloud_byol“ verwendet werden.

VM-Bereitstellungstyp	SKU-Name
Single Node	ontap_Cloud_byol
Hochverfügbarkeit	ontap_Cloud_byol_ha

4. Sobald die ONTAP Version und das Azure Marketplace Image zugeordnet sind, exportieren Sie die VHD-Datei aus dem Azure Marketplace über die Azure Cloud Shell oder die Azure CLI.

Exportieren Sie die VHD-Datei über Azure Cloud Shell im Azure-Portal

1. Exportieren Sie das Marketplace-Image von Azure Cloud Shell in ein vhd (image2, z. B. 9150.01000024.05090105.vhd), und laden Sie es auf Ihren lokalen Rechner (z. B. einen Linux-Rechner oder einen Windows-PC) herunter.

Klicken Sie zum Anzeigen auf

```
#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
```

Exportieren Sie die VHD-Datei über die Azure CLI von einem lokalen Linux-Computer

1. Exportieren Sie das Marketplace-Image über die Azure CLI von einem lokalen Linux-Rechner in ein VHD.

Klicken Sie zum Anzeigen auf

```
#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
```

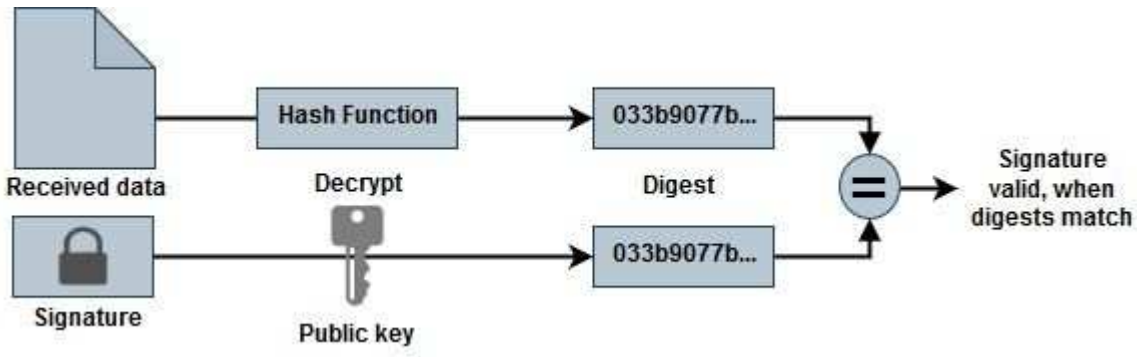
Überprüfung der Dateisignatur

Überprüfung der Dateisignatur

Bei der Azure-Image-Verifizierung wird mithilfe der Hash-Funktion ein Digest aus der VHD-Datei mit den führenden 1 MB und dem endenden 512B-Striping generiert. Um die Signaturverfahren anzupassen, wird SHA256 zum Hash verwendet. Sie müssen die führenden 1MB und die letzten 512B aus der VHD-Datei entfernen und dann den verbleibenden Teil der VHD-Datei überprüfen.

Zusammenfassung des Dateisignaturüberprüfungs-Workflows

Im Folgenden finden Sie eine Übersicht über den Prozess zur Überprüfung der Dateisignatur.



- Laden Sie die Datei Azure Image Digest von der herunter "NetApp Support Website" Und extrahieren Sie die Digest-Datei(.SIG), die Zertifikatdatei des öffentlichen Schlüssels(.pem) und die Zertifikatdatei der Kette(.pem).

Siehe "Azure Image Digest Datei herunterladen" Finden Sie weitere Informationen.

- Überprüfen Sie die Vertrauenskette.
- Extrahieren Sie den öffentlichen Schlüssel(.Pub) aus dem öffentlichen Schlüsselzertifikat(.pem).
- Der extrahierte öffentliche Schlüssel wird verwendet, um die Digest-Datei zu entschlüsseln. Das Ergebnis wird dann mit einem neuen unverschlüsselten Digest der aus der Image-Datei erstellten temporären Datei mit führenden 1MB und enden 512 Bytes entfernt verglichen.

  Dieser Schritt wird durch den folgenden Befehl openssl erreicht.

  - Die allgemeine CLI-Anweisung wird wie folgt angezeigt:

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

  - OpenSSL CLI-Tool gibt eine "Verified OK"-Meldung, wenn beide Dateien übereinstimmen und "Verification Failure", wenn sie nicht übereinstimmen.

Überprüfung der Dateisignatur unter Linux

Sie können eine exportierte VHD-Dateisignatur für Linux überprüfen, indem Sie die folgenden Schritte ausführen.

Schritte

1. Laden Sie die Datei Azure Image Digest von der herunter "NetApp Support Website" Und extrahieren Sie die Digest-Datei(.SIG), die Zertifikatdatei des öffentlichen Schlüssels(.pem) und die Zertifikatdatei der Kette(.pem).

   Siehe "Azure Image Digest Datei herunterladen" Finden Sie weitere Informationen.

2. Überprüfen Sie die Vertrauenskette.

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

3. Entfernen Sie die führenden 1 MB (1048576 Byte) und die letzten 512 Byte VHD-Datei.

   Wenn 'Tail' verwendet wird, gibt die Option '-c +K' Bytes ab den KTH Bytes der angegebenen Datei aus. Daher wird 1048577 an 'tail -c' übergeben.

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

4. Verwenden Sie openssl, um den öffentlichen Schlüssel aus dem Zertifikat zu extrahieren und die gestreifte Datei (sign.tmp) mit der Signaturdatei und dem öffentlichen Schlüssel zu überprüfen.

Wenn die Eingabedatei die Überprüfung bestanden hat, wird der Befehl angezeigt „Verifizierung OK“. Andernfalls wird „Überprüfungsfehler“ angezeigt.

```
% 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. Den Arbeitsbereich bereinigen.

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

Überprüfung der Dateisignatur auf Mac OS

Sie können eine exportierte VHD-Dateisignatur für Mac OS überprüfen, indem Sie die folgenden Schritte ausführen.

Schritte

1. Laden Sie die Datei Azure Image Digest von der herunter "NetApp Support Website" Und extrahieren Sie die Digest-Datei(.SIG), die Zertifikatdatei des öffentlichen Schlüssels(.pem) und die Zertifikatdatei der Kette(.pem).

   Siehe "Azure Image Digest Datei herunterladen" Finden Sie weitere Informationen.

2. Überprüfen Sie die Vertrauenskette.

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

3. Entfernen Sie die führende 1 MB (1048576 Byte) und die letzte 512 Byte VHD-Datei.

   Wenn 'Tail' verwendet wird, gibt die Option '-c +K' Bytes beginnend mit den KTH Bytes aus Der angegebenen Datei. Daher wird 1048577 an 'tail -c' übergeben. Es dauert ca. 13m Damit der tail-Befehl unter Mac OS abgeschlossen wird.

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

4. Verwenden Sie openssl, um den öffentlichen Schlüssel aus dem Zertifikat zu extrahieren und den gestreiften Schlüssel zu überprüfen
Datei(sign.tmp) mit Signaturdatei und öffentlichem Schlüssel.

   Wenn die Eingabedatei die Überprüfung besteht, wird im Befehl „Überprüfung OK“ angezeigt. Andernfalls wird „Überprüfungsfehler“ angezeigt.

```
% 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. Den Arbeitsbereich bereinigen.

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

Weitere Informationen zur Azure-Image-Verifizierung

Weitere Informationen zur Azure-Image-Verifizierung finden Sie unter den folgenden Links. Die unten stehenden Links führen Sie zu Websites, die nicht von NetApp stammen.

Quellen

- "Page Fault Blog: Wie signieren und überprüfen Sie mit OpenSSL"
- "Erstellen Sie mit Azure Marketplace Image ein VM-Image für Ihre Azure Stack Edge Pro GPU im Microsoft Learn"
- "Exportieren/Kopieren einer verwalteten Festplatte in ein Storage-Konto mithilfe der Azure CLI in Microsoft Learn"
- "Azure Cloud Shell Quickstart – Bash Microsoft Learn"
- "So installieren Sie die Azure CLI von Microsoft Learn"

- "az Storage Blob copy – Microsoft Learn"
- "Anmelden mit Azure CLI – Anmeldung und Authentifizierung – Microsoft Learn"