Verificación de imagen de la plataforma Azure

Cloud Volumes ONTAP

NetApp
October 07, 2024

Tabla de contenidos

Verificación de imagen de la plataforma Azure 1
Información general sobre la verificación de imágenes de Azure 1
Descargue Azure Image Digest File 1
Exportación de imágenes desde Azure Marketplace 2
Verificación de firma de archivo 9
Dónde encontrar información adicional sobre la verificación de imágenes de Azure 12

Verificación de imagen de la plataforma Azure

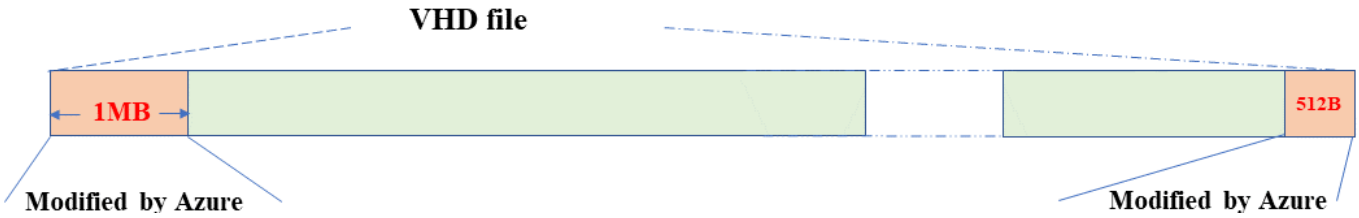
Información general sobre la verificación de imágenes de Azure

La verificación de imágenes de Azure cumple con los requisitos de seguridad de NetApp mejorada. Si bien la verificación de un archivo de imagen es un proceso sencillo, la verificación de la firma de imagen de Azure requiere una manipulación especial del conocido archivo de imagen de Azure VHD debido a una alternativa realizada por Azure Marketplace.

> La verificación de imágenes de Azure es compatible con la versión 9.15.0 del software Cloud Volumes ONTAP o posterior.

Modificación de Azure de los archivos VHD publicados

Los 1MB (1048576 bytes) iniciales y los 512 bytes finales del archivo VHD son modificados por Azure. La firma de imágenes NetApp omite los 1MB primeros y los 512 bytes finales y firma la parte de imagen VHD restante.



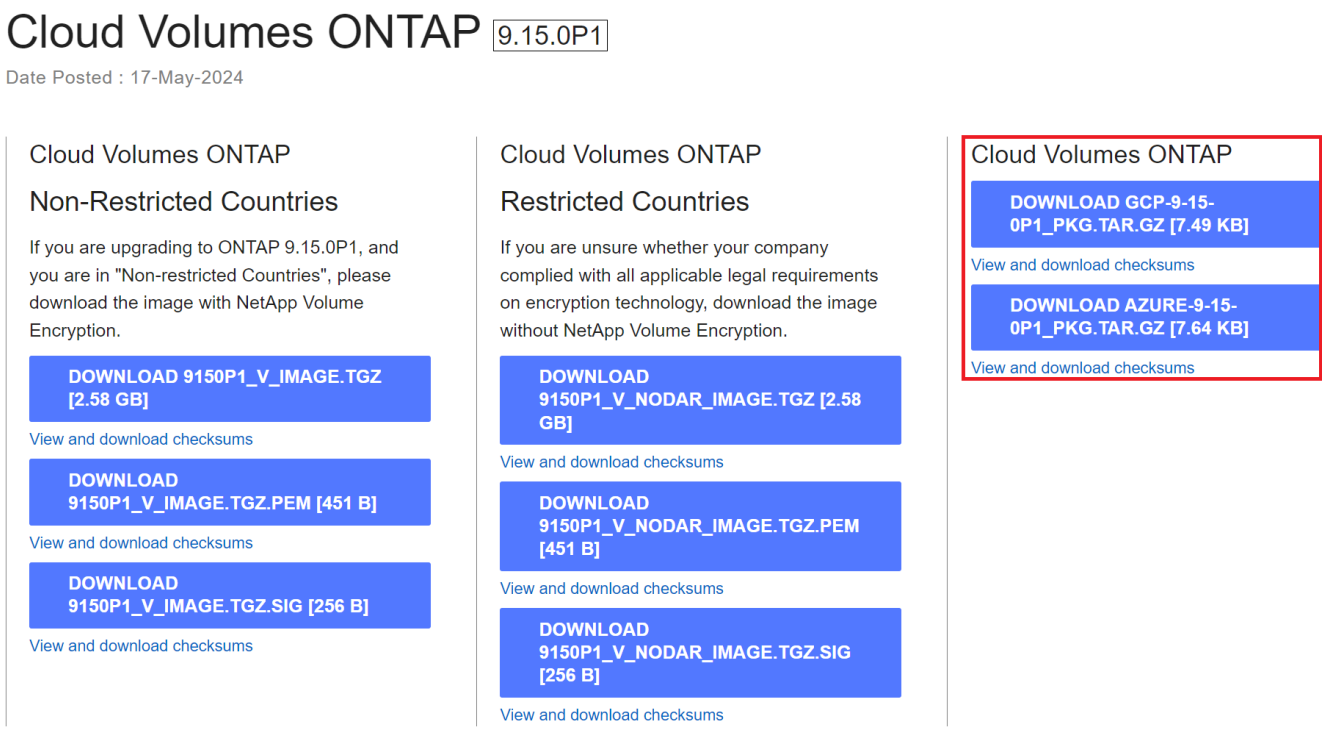
Como ejemplo, el diagrama anterior muestra un archivo VHD con un tamaño de 10GB MB. Pero la porción firmada de NetApp está marcada en verde con un tamaño de 10GB - 1MB - 512B.

Descargue Azure Image Digest File

El archivo Azure Image Digest File se puede descargar de la "Sitio de soporte de NetApp". La descarga está en formato tar.gz y contiene archivos para la verificación de firma de imagen.

Pasos

1. Vaya a "Página del producto de Cloud Volumes ONTAP en el sitio de soporte de NetApp" y descargue la versión de software necesaria en la sección Descargas.
2. En la página de descarga de Cloud Volumes ONTAP, haga clic en el botón **download** para el archivo de resumen de imágenes de Azure para descargar el TAR. Archivo GZ.



3. Para Linux y macOS, debe realizar lo siguiente para obtener md5sum y sha256sum para el archivo Azure Image Digest descargado.
   a. Para md5sum, introduzca la `md5sum` comando.
   b. Para sha256sum, introduzca la `sha256sum` comando.
4. Compruebe el `md5sum` y.. `sha256sum` Los valores coinciden con la descarga de Azure Image Digest File.
5. En Linux y Mac OS, realice el `tar -xzf` comando para extraer el archivo tar.gz.

   El TAR extraído. El archivo GZ contiene el archivo digest(.sig), el archivo de certificado de clave pública(.pem) y el archivo de certificado de cadena(.pem).

   Lista de resultados de untar tar.gz archivo

```
$ 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
```

Exportación de imágenes desde Azure Marketplace

Una vez que la imagen del disco duro virtual se publica en la nube de Azure, la imagen deja de ser gestionada por NetApp. En su lugar, la imagen publicada se coloca en Azure Marketplace. La alteración de Azure a los 1MB líderes y 512B finales del VHD se

produce cuando la imagen se almacena en un lugar y se publica en Azure Marketplace. Para verificar la firma del archivo VHD, la imagen VHD modificada por Azure debe exportarse primero desde Azure Marketplace.

Lo que necesitará

Debe instalar los programas necesarios en su sistema.

- Azure CLI está instalado o Azure Cloud Shell a través del portal de Azure está disponible en todo momento.

> Para obtener más información sobre cómo instalar Azure CLI, consulte "Documentación de Azure: Cómo instalar la CLI de Azure" .

Pasos

1. Asigne la versión de ONTAP a la versión de la imagen de Azure Marketplace utilizando el contenido del archivo version_readme.

   Para cada asignación de versiones enumerada en el archivo version_readme, la versión de ONTAP se representa con «buildname» y la versión de la imagen de Azure Marketplace se representa con «version».

   Por ejemplo, en el siguiente archivo version_readme, la versión de ONTAP «9.15.0P1» está asignada a la versión de la imagen de Azure Marketplace «9150.01000024.05090105». Esta versión de imagen de Azure Marketplace se utiliza más adelante para establecer la imagen URN.

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

2. Identifique el nombre de la región en la que pretende crear máquinas virtuales.

   Este nombre de región se utiliza como valor para la variable “locName” al definir el URN de la imagen de mercado.

   a. Para recibir una lista de regiones disponibles, introduzca la `az account list-locations -o table` comando.

      En la siguiente tabla, el nombre de la región se denomina campo Nombre.

```
$ 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. Revise el nombre de SKU para el tipo de puesta en marcha de VM correspondiente en la tabla siguiente.

   El nombre de SKU se utiliza como valor para la variable skuName al establecer el URN de la imagen de mercado.

   Por ejemplo, las puestas en marcha de un solo nodo deben utilizar el nombre SKU «ontap_cloud_byol».

Tipo de despliegue de máquinas virtuales	Nombre de SKU
Nodo único	ontap_cloud_byol
Alta disponibilidad	ontap_cloud_byol_ha

4. Una vez que se hayan asignado la versión de ONTAP y la imagen de Azure Marketplace, exporte el archivo VHD desde Azure Marketplace a través de Azure Cloud Shell o la interfaz de línea de comandos de Azure.

Exporte el archivo VHD a través de Azure Cloud Shell en el portal de Azure

1. Desde Azure Cloud Shell, exporte la imagen del mercado a un vhd (image2, por ejemplo, 9150.01000024.05090105.vhd) y descárguela en su equipo local (por ejemplo, una máquina Linux o un PC con Windows).

Haga clic para mostrar

```
#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
```

Exporte el archivo VHD a través de la CLI de Azure desde el equipo Linux local

1. Exporte la imagen de mercado a un vhd a través de la CLI de Azure desde una máquina Linux local.

Haga clic para mostrar

```
#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&sigxxxxxxxxxxxxxxxxxxxxxxxx"
}

% export diskAccessSAS="https://md-
xxxxxx.blob.core.windows.net/xxxxxxx/abcd?sv=2018-03-
28&sr=b&si=xxxxxxxx-xxxx-xx-xx-xx&sigxxxxxxxxxxxxxxxxxxxxxxxx"
#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
```

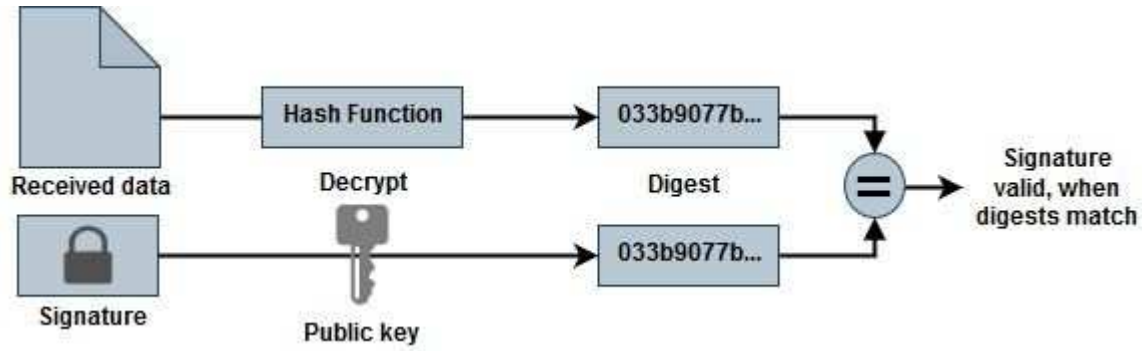
Verificación de firma de archivo

Verificación de firma de archivo

El proceso de verificación de imágenes de Azure generará un resumen del archivo VHD con el 1MB principal y el 512B final segmentado mediante la función hash. Para que coincida con el procedimiento de firma, SHA256 se utiliza para hash. Debe eliminar los 1MB principales y los 512B finales del archivo VHD y, a continuación, verificar la parte restante del archivo VHD.

Resumen del flujo de trabajo de verificación de firmas de archivos

A continuación se ofrece una descripción general del proceso de flujo de trabajo de verificación de firmas de archivos.



- Descargue el archivo Azure Image Digest de la "Sitio de soporte de NetApp" y extraiga el archivo digest(.sig), el archivo de certificado de clave pública(.pem) y el archivo de certificado de cadena(.pem).

Consulte "Descargue Azure Image Digest File" si desea obtener más información.

- Verifique la cadena de confianza.
- Extraiga la clave pública(.pub) del certificado de clave pública(.pem).
- La clave pública extraída se utiliza para descifrar el archivo de resumen. El resultado se compara con un nuevo resumen no cifrado del archivo temporal creado a partir del archivo de imagen con 1MB inicial y 512 bytes finales eliminados.

  Este paso se logra a través del siguiente comando openssl.

  - La sentencia CLI general aparece de la siguiente manera:

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

  - La herramienta CLI de OpenSSL muestra un mensaje de confirmación verificada si ambos archivos coinciden y si no coinciden.

Verificación de firma de archivo en Linux

Puede verificar una firma de archivo VHD exportada para Linux siguiendo los pasos que se indican a continuación.

Pasos

1. Descargue el archivo Azure Image Digest de la "Sitio de soporte de NetApp" y extraiga el archivo digest(.sig), el archivo de certificado de clave pública(.pem) y el archivo de certificado de cadena(.pem).

   Consulte la "Descargue Azure Image Digest File" si quiere más información.

2. Verifique la cadena de confianza.

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

3. Elimine los 1MB primeros (1048576 bytes) y los 512 bytes finales del archivo VHD.

   Si se utiliza 'tail', la opción '-c +K' genera bytes que comienzan con los bytes KTH del archivo especificado. Por lo tanto, 1048577 se pasa a '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. Utilice openssl para extraer la clave pública del certificado y verificar el archivo segmentado (sign.tmp) con el archivo de firma y la clave pública.

Si el archivo de entrada pasa la verificación, se mostrará el comando Verificación correcta. De lo contrario, aparecerá el mensaje Fallo de verificación.

```
% 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. Limpie el espacio de trabajo.

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

Verificación de firma de archivo en Mac OS

Puede verificar una firma de archivo VHD exportada para Mac OS siguiendo los pasos que se indican a continuación.

Pasos

1. Descargue el archivo Azure Image Digest de la "Sitio de soporte de NetApp" y extraiga el archivo digest(.sig), el archivo de certificado de clave pública(.pem) y el archivo de certificado de cadena(.pem).

   Consulte la "Descargue Azure Image Digest File" si quiere más información.

2. Verifique la cadena de confianza.

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

3. Elimine los 1MB primeros (1048576 bytes) y los 512 bytes finales del archivo VHD.

   Si se utiliza 'tail', la opción '-c +K' genera bytes que comienzan con los bytes KTH del archivo especificado. Por lo tanto, 1048577 se pasa a 'tail -c'. Toma alrededor de 13m Para que el comando tail se complete en 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. Utilice openssl para extraer la clave pública del certificado y verificar la rayada archivo (sign.tmp) con el archivo de firma y la clave pública.

   Si el archivo de entrada pasa la verificación, el comando mostrará “Verificación correcta”. De lo contrario, aparecerá el mensaje Fallo de verificación.

```
% 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. Limpie el espacio de trabajo.

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

Dónde encontrar información adicional sobre la verificación de imágenes de Azure

Consulte los siguientes enlaces para obtener información adicional sobre la verificación de imágenes de Azure. Los siguientes enlaces le llevan a sitios ajenos a NetApp.

Referencias

- "Page Fault Blog: Cómo firmar y verificar usando OpenSSL"
- "Utilice la imagen de Azure Marketplace para crear una imagen de VM para su GPU Azure Stack Edge Pro | Microsoft Learn"
- "Exportar/Copiar un disco gestionado a una cuenta de almacenamiento mediante la CLI de Azure | Microsoft Learn"
- "Inicio rápido de Azure Cloud Shell - Bash | Microsoft Learn"
- "Cómo instalar la CLI de Azure | Microsoft Learn"
- "Copia blob de almacenamiento az | Microsoft Learn"

- "Iniciar sesión con Azure CLI — Inicio de sesión y autenticación | Microsoft Learn"