Verifica dell'immagine della piattaforma Azure

Cloud Volumes ONTAP

NetApp
June 27, 2024

Sommario

Verifica dell'immagine della piattaforma Azure

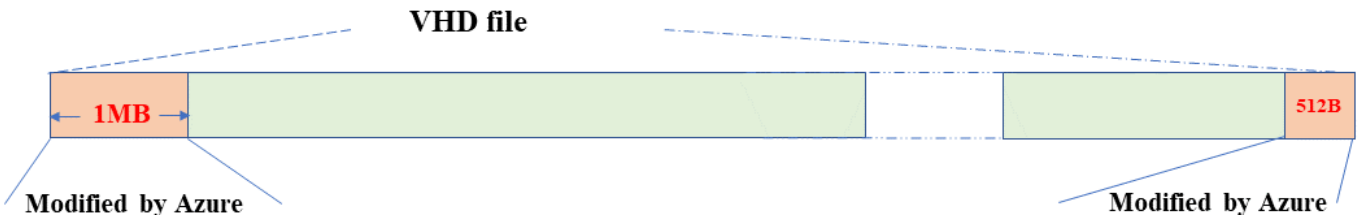
Panoramica di verifica delle immagini Azure

La verifica dell'immagine di Azure è conforme ai requisiti di sicurezza NetApp avanzati. Anche se la verifica di un file immagine è un processo semplice, la verifica della firma dell'immagine Azure non richiede speciali handling al noto file di immagine Azure VHD a causa di un'alternanza effettuata dal marketplace di Azure.

La verifica dell'immagine di Azure è supportata sul software Cloud Volumes ONTAP versione 9.15.0 o superiore.

Modifica di Azure dei file VHD pubblicati

I 1MB (1048576 byte) iniziali e i 512 byte finali del file VHD vengono modificati da Azure. La firma dell'immagine NetApp salta i 1MB byte iniziali e i 512 byte finali e firma la parte rimanente dell'immagine VHD.



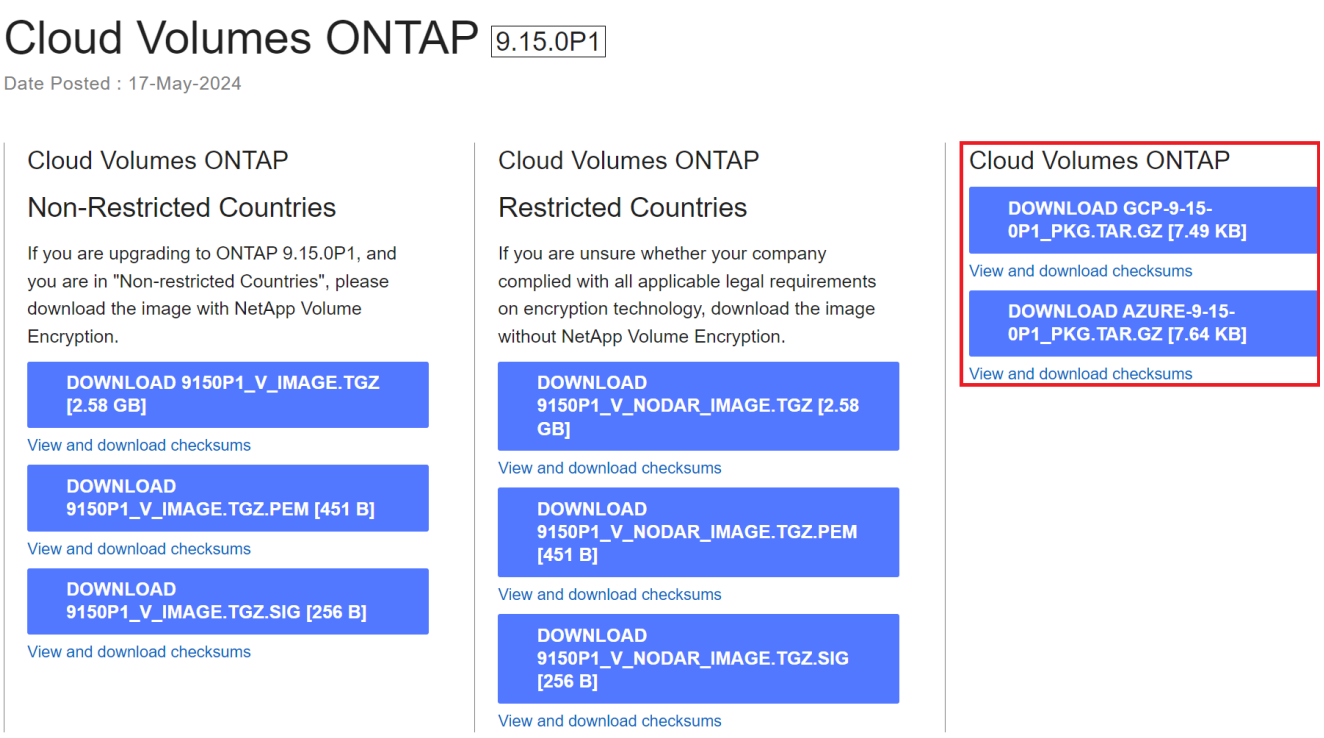
Come esempio, il diagramma precedente mostra un file VHD di dimensioni 10GB. Ma la parte con segno NetApp è contrassegnata in verde con dimensioni di 10GB - 1MB - 512B.

Scaricare il file di Azure Image Digest

Il file di inserimento immagini di Azure può essere scaricato da "Sito di supporto NetApp". Il download è in formato tar.gz e contiene file per la verifica della firma dell'immagine.

Fasi

1. Accedere alla "Pagina del prodotto Cloud Volumes ONTAP sul sito del supporto NetApp" E scaricare la versione software desiderata nella sezione Downloads.
2. Nella pagina di download di Cloud Volumes ONTAP, fare clic sul pulsante **download** per il file di inserimento immagini Azure per scaricare il file TAR. File GZ.



3. Per Linux e MacOS, è necessario effettuare le seguenti operazioni per ottenere i file md5sum e sha256sum per il file Azure Image Digest scaricato.
   a. Per md5sum, immettere il `md5sum` comando.
   b. Per sha256sum, immettere il `sha256sum` comando.
4. Verificare `md5sum` e. `sha256sum` I valori corrispondono al download del file di Azure Image Digest.
5. Su Linux e Mac OS, eseguire `tar -xzf` comando per estrarre il file tar.gz.

   Il CATRAME estratto. Il file GZ contiene il file digest(.sig), il file di certificato a chiave pubblica(.pem) e il file di certificato a catena(.pem).

   Elenco dei risultati del file 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
```

Esportazione di immagini da Azure Marketplace

Una volta che l'immagine VHD è pubblicata nel cloud Azure, l'immagine non è più gestita da NetApp. Al contrario, l'immagine pubblicata viene posizionata sul marketplace di Azure. La modifica di Azure al primo 1MB e alla fine del 512B del VHD si verifica quando

l'immagine viene messa in scena e pubblicata sul marketplace di Azure. Per verificare la firma del file VHD, l'immagine VHD modificata da Azure deve essere esportata prima dal marketplace di Azure.

Di cosa hai bisogno

È necessario installare i programmi richiesti sul sistema.

- È installata la CLI di Azure o è prontamente disponibile Azure Cloud Shell attraverso il portale di Azure.

> Per ulteriori informazioni su come installare l'interfaccia della riga di comando di Azure, vedere "Documentazione di Azure: Come installare l'interfaccia della riga di comando di Azure".

Fasi

1. Mappare la versione di ONTAP alla versione dell'immagine del marketplace di Azure utilizzando il contenuto del file version_readme.

   Per ogni mappatura di versione elencata nel file version_readme, la versione di ONTAP è rappresentata da "buildname" e la versione dell'immagine di mercato di Azure è rappresentata da "versione".

   Ad esempio, nel seguente file version_readme, la versione di ONTAP "9.15.0P1" è mappata alla versione "9150.01000024.05090105" dell'immagine del marketplace di Azure. Questa versione dell'immagine di Azure Marketplace viene utilizzata in seguito per impostare l'URN dell'immagine.

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

2. Identificare il nome della regione in cui si intende creare le macchine virtuali.

   Questo nome di zona viene utilizzato come valore per la variabile "locName" quando si imposta l'URN dell'immagine del mercato.

   a. Per ricevere un elenco delle regioni disponibili, immettere il `az account list-locations -o table` comando.

      Nella tabella seguente, il nome della regione viene indicato come campo "Nome".

```
$ 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. Esaminare il nome SKU per il tipo di implementazione VM corrispondente riportato nella tabella seguente.

   Il nome SKU viene utilizzato come valore per la variabile "skuName" quando si imposta l'URN dell'immagine del mercato.

   Ad esempio, le implementazioni a nodo singolo devono utilizzare il nome SKU "ontap_cloud_byol".

Tipo di implementazione VM	Nome SKU
Nodo singolo	cloud_ontap_byol
Alta disponibilità	ontap_cloud_byol_ha

4. Una volta mappate la versione di ONTAP e l'immagine di mercato di Azure, esportare il file VHD dal marketplace di Azure tramite Azure Cloud Shell o l'interfaccia a riga di comando di Azure.

Esporta file VHD tramite Azure Cloud Shell sul portale Azure

1. Da Azure Cloud Shell, esportare l'immagine del mercato in un vhd (image2, ad esempio 9150.01000024.05090105.vhd) e scaricarla sul computer locale (ad esempio, una macchina Linux o un PC Windows).

Fare clic per visualizzare

```
#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
```

Esporta file VHD tramite l'interfaccia CLI di Azure dalla macchina Linux locale

1. Esportare l'immagine del marketplace in un vhd tramite l'interfaccia CLI di Azure da una macchina Linux locale.

Fare clic per visualizzare

```
#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
```

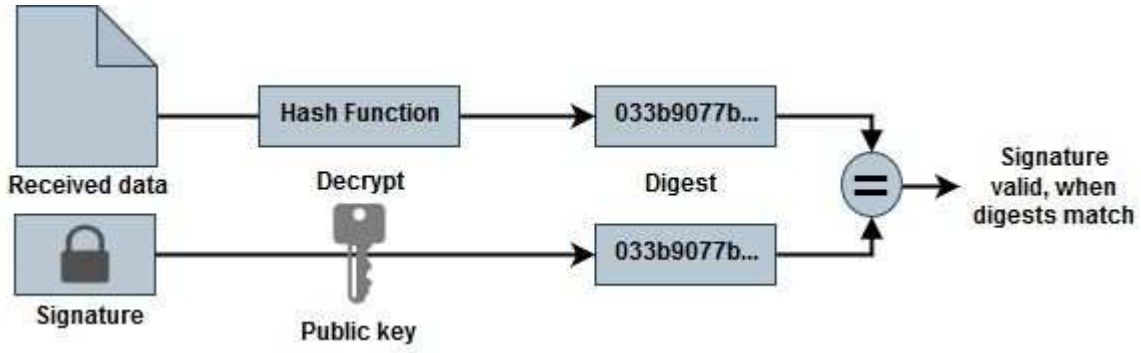
Verifica della firma del file

Verifica della firma del file

Il processo di verifica dell'immagine di Azure genera un digest dal file VHD con il primo 1MB e il termine del 512B striping mediante la funzione hash. Per far corrispondere la procedura di firma, SHA256 viene utilizzato per eseguire l'hash. È necessario rimuovere i file 1MB iniziali e 512B finali dal file VHD e verificare la parte rimanente del file VHD.

Riepilogo del flusso di lavoro di verifica della firma dei file

Di seguito viene fornita una panoramica del processo del flusso di lavoro di verifica della firma dei file.



- Scaricare il file Azure Image Digest dal "Sito di supporto NetApp" ed estrarre il file digest(.sig), il file di certificato a chiave pubblica(.pem) e il file di certificato a catena(.pem).

  Fare riferimento a. "Scaricare il file di Azure Image Digest" per ulteriori informazioni.

- Verificare la catena di trust.
- Estrarre la chiave pubblica(.pub) dal certificato a chiave pubblica(.pem).
- La chiave pubblica estratta viene utilizzata per decrittografare il file digest. Il risultato viene quindi confrontato con un nuovo digest non crittografato del file temporaneo creato dal file di immagine con 1MB iniziale e 512 byte finale rimossi.

  Questo passo viene ottenuto mediante il seguente comando openssl.

  - L'istruzione CLI generale viene visualizzata come segue:

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

  - Lo strumento CLI OpenSSL visualizza un messaggio "verificato OK" se entrambi i file corrispondono e "errore di verifica" se non corrispondono.

Verifica della firma dei file su Linux

È possibile verificare la firma di un file VHD esportato per Linux seguendo la procedura riportata di seguito.

Fasi

1. Scaricare il file Azure Image Digest dal "Sito di supporto NetApp" ed estrarre il file digest(.sig), il file di certificato a chiave pubblica(.pem) e il file di certificato a catena(.pem).

   Fare riferimento a. "Scaricare il file di Azure Image Digest" per ulteriori informazioni.

2. Verificare la catena di trust.

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

3. Rimuovere i 1MB iniziali (1048576 byte) e i 512 byte finali del file VHD.

   Se si usa 'tail', l'opzione '-c +K' genera byte che iniziano con i kth byte del file specificato. Quindi, 1048577 viene passato alla coda -c'.

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

4. Utilizzare openssl per estrarre la chiave pubblica dal certificato e verificare il file con striping (sign.tmp) con il file della firma e la chiave pubblica.

   Se il file di input supera la verifica, viene visualizzato il comando "Verifica OK". In caso contrario, viene visualizzato "errore di verifica".

```
% 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. Pulire lo spazio di lavoro.

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

Verifica della firma del file su Mac OS

Per verificare la firma di un file VHD esportato per Mac OS, procedere come segue.

Fasi

1. Scaricare il file Azure Image Digest dal "Sito di supporto NetApp" ed estrarre il file digest(.sig), il file di certificato a chiave pubblica(.pem) e il file di certificato a catena(.pem).

   Fare riferimento a. "Scaricare il file di Azure Image Digest" per ulteriori informazioni.

2. Verificare la catena di trust.

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

3. Rimuovere i 1MB (1048576 byte) iniziali e i 512 byte finali del file VHD.

   Se si usa 'tail', l'opzione '-c +K' emette byte a partire dai kth byte
   del file specificato. Quindi, 1048577 viene passato alla coda -c'. Ci vogliono circa 13m minuti
   Per completare il comando tail su 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. Utilizzare openssl per estrarre la chiave pubblica dal certificato e verificare lo striping
   file(sign.tmp) con il file della firma e la chiave pubblica.

Se il file di input supera la verifica, il comando visualizza "verifica OK".
In caso contrario, viene visualizzato "errore di verifica".

```
% 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. Pulire lo spazio di lavoro.

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

Dove trovare ulteriori informazioni sulla verifica dell'immagine Azure

Consulta i link seguenti per ulteriori informazioni su Azure Image Verification. I link seguenti consentono di accedere a siti non NetApp.

Riferimenti

- "Page Fault Blog: Come firmare e verificare usando OpenSSL"
- "USA l'immagine di Azure Marketplace per creare l'immagine VM per la tua GPU Azure Stack Edge Pro | Microsoft Learn"
- "Esportare/copiare un disco gestito in un account di storage utilizzando l'interfaccia CLI di Azure | Microsoft Learn"
- "Azure Cloud Shell Quickstart - Bash | Microsoft Learn"
- "Come installare la CLI di Azure | Microsoft Learn"
- "Copia BLOB storage az | Microsoft Learn"
- "Accedi con Azure CLI — Login e autenticazione | Microsoft Learn"

Informazioni sul copyright

Informazioni sul marchio commerciale