Azure 플랫폼 이미지 검증

Cloud Volumes ONTAP

NetApp
June 27, 2024

목차

Azure 플랫폼 이미지 검증

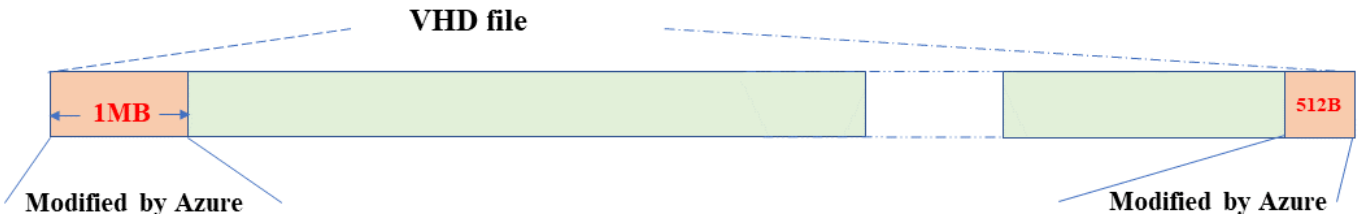
Azure 이미지 검증 개요

Azure 이미지 검증은 향상된 NetApp 보안 요구사항을 준수합니다. 이미지 파일을 검증하는 것은 간단한 프로세스이지만 Azure 마켓플레이스의 변경 사항으로 인해 Azure 이미지 서명 확인을 위해 잘 알려진 Azure VHD 이미지 파일에 특별한 필링이 필요합니다.

Azure 이미지 검증은 Cloud Volumes ONTAP 소프트웨어 버전 9.15.0 이상에서 지원됩니다.

게시된 VHD 파일에 대한 Azure의 변경

Azure에서 앞 1MB(1048576바이트)와 끝 512바이트의 VHD 파일을 수정합니다. NetApp 이미지 서명은 선행 1MB를 건너뛰고 512바이트를 종료하고 나머지 VHD 이미지 부분을 서명합니다.



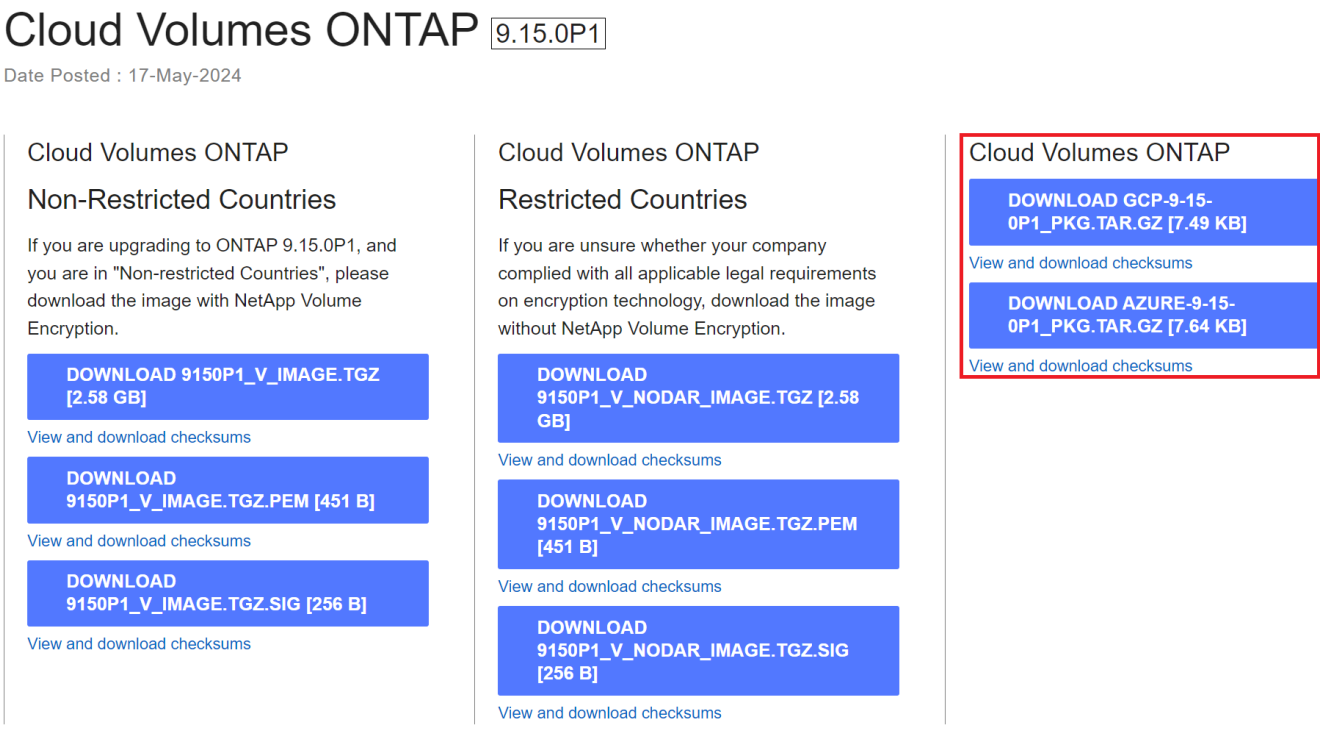
위의 다이어그램은 10GB의 VHD 파일을 보여 줍니다. 그러나 NetApp 서명 부분은 10GB-1MB-512B 크기로 녹색으로 표시됩니다.

Azure Image Digest 파일을 다운로드합니다

Azure Image Digest 파일은 에서 다운로드할 수 있습니다 "NetApp Support 사이트". 다운로드는 tar.gz 형식으로 이미지 서명 확인을 위한 파일이 포함되어 있습니다.

단계

1. 로 이동합니다 "NetApp Support 사이트의 Cloud Volumes ONTAP 제품 페이지 를 참조하십시오" 다운로드 섹션에서 원하는 소프트웨어 버전을 다운로드합니다.
2. Cloud Volumes ONTAP 다운로드 페이지에서 Azure 이미지 다이제스트 파일에 대한 * 다운로드 버튼 * 을 클릭하여 TAR을 다운로드합니다. GZ 파일.



3. Linux 및 MacOS의 경우 다운로드한 Azure Image Digest 파일에 대한 md5sum 및 sha256sum을 얻으려면 다음을 수행해야 합니다.
   a. md5sum 의 경우 을 입력합니다 `md5sum` 명령.
   b. sha256sum 의 경우 을 입력합니다 `sha256sum` 명령.
4. 를 확인합니다 `md5sum` 및 `sha256sum` 값은 Azure Image Digest File 다운로드와 일치합니다.
5. Linux 및 Mac OS에서 를 수행합니다 `tar -xzf` tar.gz 파일의 압축을 푸는 명령입니다.

   추출된 TAR입니다. GZ 파일에는 다이제스트 파일(.sig), 공개 키 인증서 파일(.pem) 및 체인 인증서 파일(.pem)이 포함되어 있습니다.

   *untar tar.gz 파일의 결과를 나열합니다

```
$ 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
```

Azure Marketplace에서 이미지 내보내기

VHD 이미지가 Azure 클라우드에 게시되면 NetApp에서 이미지를 더 이상 관리할 수 없습니다. 대신 게시된 이미지가 Azure 마켓플레이스에 배치됩니다. Azure가 최고 1MB로 변경되고

512B의 VHD가 종료되는 것은 이미지가 Azure 마켓플레이스에서 스테이징되고 게시될 때 발생합니다. VHD 파일의 서명을 확인하려면 Azure에서 수정한 VHD 이미지를 먼저 Azure 마켓플레이스에서 내보내야 합니다.

필요한 것

시스템에 필요한 프로그램을 설치해야 합니다.

- Azure CLI가 설치되어 있거나 Azure 포털을 통해 Azure Cloud Shell을 바로 사용할 수 있습니다.

> Azure CLI 설치 방법에 대한 자세한 내용은 를 참조하십시오 "Azure 설명서: Azure CLI 설치 방법".

단계

1. version_readme 파일의 내용을 사용하여 ONTAP 버전을 Azure 마켓플레이스 이미지 버전에 매핑합니다.

   version_readme 파일에 나열된 각 버전 매핑에 대해 ONTAP 버전은 "buildname"으로 표시되고 Azure 마켓플레이스 이미지 버전은 "version"으로 표시됩니다.

   예를 들어 다음 version_readme 파일에서 ONTAP 버전 "9.15.0P1"은 Azure 마켓플레이스 이미지 버전 "9150.01000024.05090105"에 매핑되어 있습니다. 이 Azure 마켓플레이스 이미지 버전은 나중에 이미지 URN을 설정하는 데 사용됩니다.

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

2. VM을 생성할 지역 이름을 식별합니다.

   이 지역 이름은 마켓플레이스 이미지의 URN을 설정할 때 "locName" 변수의 값으로 사용됩니다.

   a. 사용 가능한 지역 목록을 받으려면 를 입력합니다 `az account list-locations -o table` 명령.

      아래 표에서 지역 이름을 "이름" 필드라고 합니다.

```
$ 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. 아래 표에서 해당 VM 배포 유형에 대한 SKU 이름을 검토합니다.

   SKU 이름은 마켓플레이스 이미지의 URN을 설정할 때 "skuName" 변수의 값으로 사용됩니다.

   예를 들어, 단일 노드 구축에서는 "ONTAP_CLOUD_BYOL" SKU 이름을 사용해야 합니다.

VM 배포 유형	**SKU** 이름
단일 노드	ONTAP_CLOUD_BYOL
고가용성	ONTAP_CLOUD_BYOL_ha

4. ONTAP 버전과 Azure 마켓플레이스 이미지가 매핑되면 Azure Cloud Shell 또는 Azure CLI를 통해 Azure 마켓플레이스의 VHD 파일을 내보냅니다.

Azure 포털의 Azure Cloud Shell을 통해 VHD 파일을 내보냅니다

1. Azure 클라우드 셸에서 마켓플레이스 이미지를 VHD(image2, 예: 9150.01000024.05090105.vhd)로 내보내고 로컬 컴퓨터(예: Linux 시스템 또는 Windows PC)로 다운로드합니다.

클릭하여 표시합니다

```
#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
```

로컬 **Linux** 시스템에서 **Azure CLI**를 통해 **VHD** 파일을 내보냅니다

1. 로컬 Linux 시스템에서 Azure CLI를 통해 마켓플레이스 이미지를 VHD로 내보냅니다.

클릭하여 표시합니다

```
#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
```

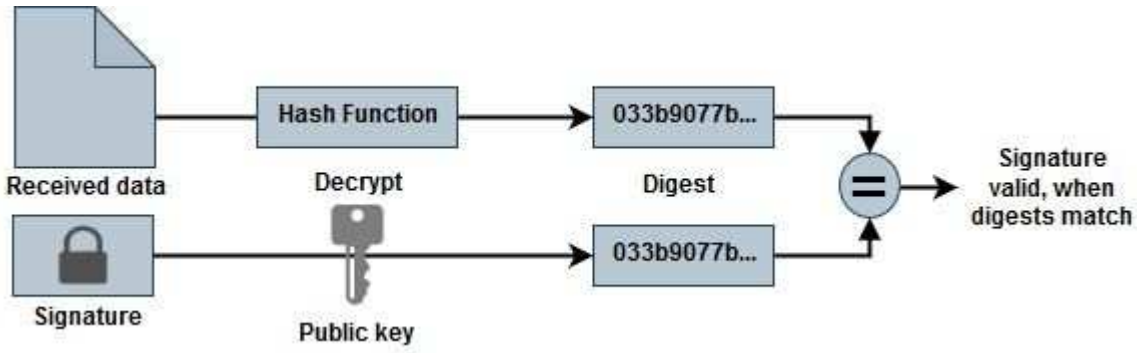
파일 서명 확인

파일 서명 확인

Azure 이미지 확인 프로세스는 해시 기능을 사용하여 선행 1MB로 VHD 파일에서 다이제스트를 생성하고 512B 스트라이프를 종료합니다. 서명 프로시저와 일치시키기 위해 SHA256을 해시에 사용합니다. VHD 파일에서 선행 1MB 및 최종 512B를 제거한 다음 VHD 파일의 나머지 부분을 확인해야 합니다.

파일 서명 확인 워크플로 요약

다음은 파일 서명 확인 워크플로 프로세스의 개요입니다.



- 에서 Azure Image Digest 파일을 다운로드합니다 "NetApp Support 사이트" 다이제스트 파일(.sig), 공개 키 인증서 파일(.pem) 및 체인 인증서 파일(.pem)의 압축을 풉니다.

  을 참조하십시오 "Azure Image Digest 파일을 다운로드합니다" 를 참조하십시오.

- 신뢰 체인을 확인합니다.
- 공개 키 인증서(.pem)에서 공개 키(.pub)를 추출합니다.
- 추출된 공개 키는 다이제스트 파일을 해독하는 데 사용됩니다. 그런 다음 이미지 파일에서 생성된 임시 파일의 암호화되지 않은 새 다이제스트와 선행 1MB를 제거하고 512바이트가 제거된 새 다이제스트를 비교합니다.

  이 단계는 다음 openssl 명령을 통해 수행됩니다.

  - 일반 CLI 문은 다음과 같이 나타납니다.

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

  - OpenSSL CLI 도구는 두 파일이 일치하면 "확인 완료" 메시지와 일치하지 않을 경우 "확인 실패"를 표시합니다.

Linux에서 파일 서명 확인

다음 단계에 따라 내보낸 Linux용 VHD 파일 서명을 확인할 수 있습니다.

단계

1. 에서 Azure Image Digest 파일을 다운로드합니다 "NetApp Support 사이트" 다이제스트 파일(.sig), 공개 키 인증서 파일(.pem) 및 체인 인증서 파일(.pem)의 압축을 풉니다.

   을 참조하십시오 "Azure Image Digest 파일을 다운로드합니다" 를 참조하십시오.

2. 신뢰 체인을 확인합니다.

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

3. 앞의 1MB(1048576바이트)와 끝 512바이트의 VHD 파일을 제거합니다.

   'tail'을 사용하는 경우 '-c+K' 옵션은 지정된 파일의 Kth 바이트로 시작하는 바이트를 출력합니다. 따라서 1048577은 'tail -c'로 전달됩니다.

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

4. openssl을 사용하여 인증서에서 공개 키를 추출하고 서명 파일과 공개 키로 스트라이프 파일(sign.tmp)을 확인합니다.

   입력 파일이 확인을 통과하면 명령이 표시됩니다
   "확인 정상". 그렇지 않으면 "Verification Failure(확인 실패)"가 표시됩니다.

```
% 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. 작업 영역을 정리합니다.

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

Mac OS에서 파일 서명 확인

다음 단계에 따라 Mac OS에 대해 내보낸 VHD 파일 서명을 확인할 수 있습니다.

단계

1. 에서 Azure Image Digest 파일을 다운로드합니다 "NetApp Support 사이트" 다이제스트 파일(.sig), 공개 키 인증서 파일(.pem) 및 체인 인증서 파일(.pem)의 압축을 풉니다.

   을 참조하십시오 "Azure Image Digest 파일을 다운로드합니다" 를 참조하십시오.

2. 신뢰 체인을 확인합니다.

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

3. 앞의 1MB(1048576바이트)와 끝 512바이트의 VHD 파일을 제거합니다.

   'tail'을 사용하는 경우 '-c+K' 옵션은 Kth 바이트로 시작하는 바이트를 출력합니다
   지정된 파일의 이름을 변경합니다. 따라서 1048577은 'tail -c'로 전달됩니다. 약 13m 정도 걸립니다
   Mac OS에서 tail 명령을 완료합니다.

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

4. openssl을 사용하여 인증서에서 공개 키를 추출하고 스트라이핑된 키를 확인합니다
서명 파일과 공개 키가 있는 파일(sign.tmp)입니다.

   입력 파일이 확인을 통과하면 명령이 "Verification OK(확인 확인 확인)"를 표시합니다.
그렇지 않으면 "Verification Failure(확인 실패)"가 표시됩니다.

```
% 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. 작업 영역을 정리합니다.

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

Azure 이미지 검증에 대한 추가 정보를 확인할 수 있는 위치

Azure 이미지 검증에 대한 자세한 내용은 아래 링크를 참조하십시오. 아래 링크를 클릭하면 비 NetApp 사이트로 이동합니다.

참조

- "페이지 오류 블로그 : 어떻게 서명하고 OpenSSL을 사용하여 확인"
- "Azure Marketplace 이미지를 사용하여 Azure Stack Edge Pro GPU | Microsoft Learn용 VM 이미지를 만드십시오"
- "Azure CLI | Microsoft Learn 을 사용하여 관리되는 디스크를 저장소 계정으로 내보내기/복사합니다"
- "Azure Cloud Shell Quickstart - Bash | Microsoft Learn"
- "Azure CLI 설치 방법 | Microsoft 알아보기"
- "AZ 저장 blob 사본 | Microsoft learn"
- "Azure CLI로 로그인 - 로그인 및 인증 | Microsoft Learn 을 참조하십시오"