Azure 플랫폼 이미지 확인

Cloud Volumes ONTAP

NetApp
November 25, 2025

This PDF was generated from https://docs.netapp.com/ko-kr/storage-management-cloud-volumes-ontap/concept-azure-image-verification.html on November 25, 2025. Always check docs.netapp.com for the latest.

목차

Azure 플랫폼 이미지 확인

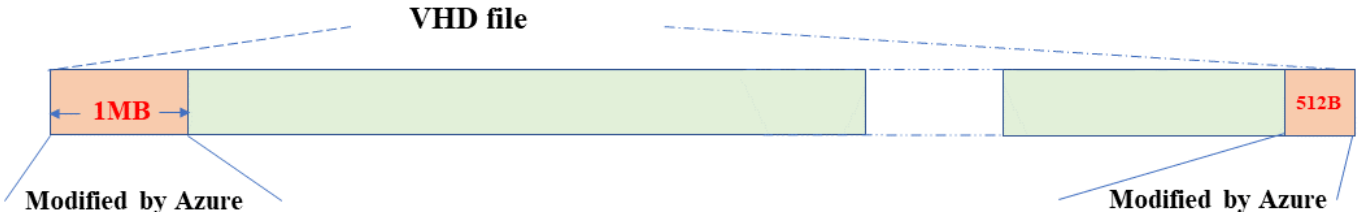
Cloud Volumes ONTAP 에 대한 Azure 마켓플레이스 이미지 검증

Azure 이미지 검증은 향상된 NetApp 보안 요구 사항을 준수합니다. 이미지 파일을 검증하는 것은 간단한 과정입니다. 그러나 Azure 이미지 서명 검증에는 Azure VHD 이미지 파일에 대한 특정 고려 사항이 필요합니다. Azure VHD 이미지 파일은 Azure Marketplace에서 변경되기 때문입니다.

Azure 이미지 검증은 Cloud Volumes ONTAP 9.15.0 이상에서 지원됩니다.

Azure에서 게시된 VHD 파일 변경

VHD 파일의 시작 부분인 1MB(1048576바이트)와 끝 부분인 512바이트는 Azure에 의해 수정됩니다. NetApp 나머지 VHD 파일에 서명합니다.



이 예에서 VHD 파일의 크기는 10GB입니다. NetApp 에서 서명한 부분은 녹색으로 표시되어 있습니다(10GB - 1MB - 512바이트).

관련 링크

- "페이지 폴트 블로그: OpenSSL을 사용하여 서명하고 확인하는 방법"
- "Azure Marketplace 이미지를 사용하여 Azure Stack Edge Pro GPU용 VM 이미지 만들기 | Microsoft Learn"
- "Azure CLI를 사용하여 관리 디스크를 저장소 계정으로 내보내기/복사 | Microsoft Learn"
- "Azure Cloud Shell 빠른 시작 - Bash | Microsoft Learn"
- "Azure CLI 설치 방법 | Microsoft Learn"
- "az 스토리지 BLOB 복사 | Microsoft Learn"
- "Azure CLI로 Sign in - 로그인 및 인증 | Microsoft Learn"

Cloud Volumes ONTAP 용 Azure 이미지 파일 다운로드

Azure 이미지 파일은 다음에서 다운로드할 수 있습니다. "NetApp 지원 사이트" .

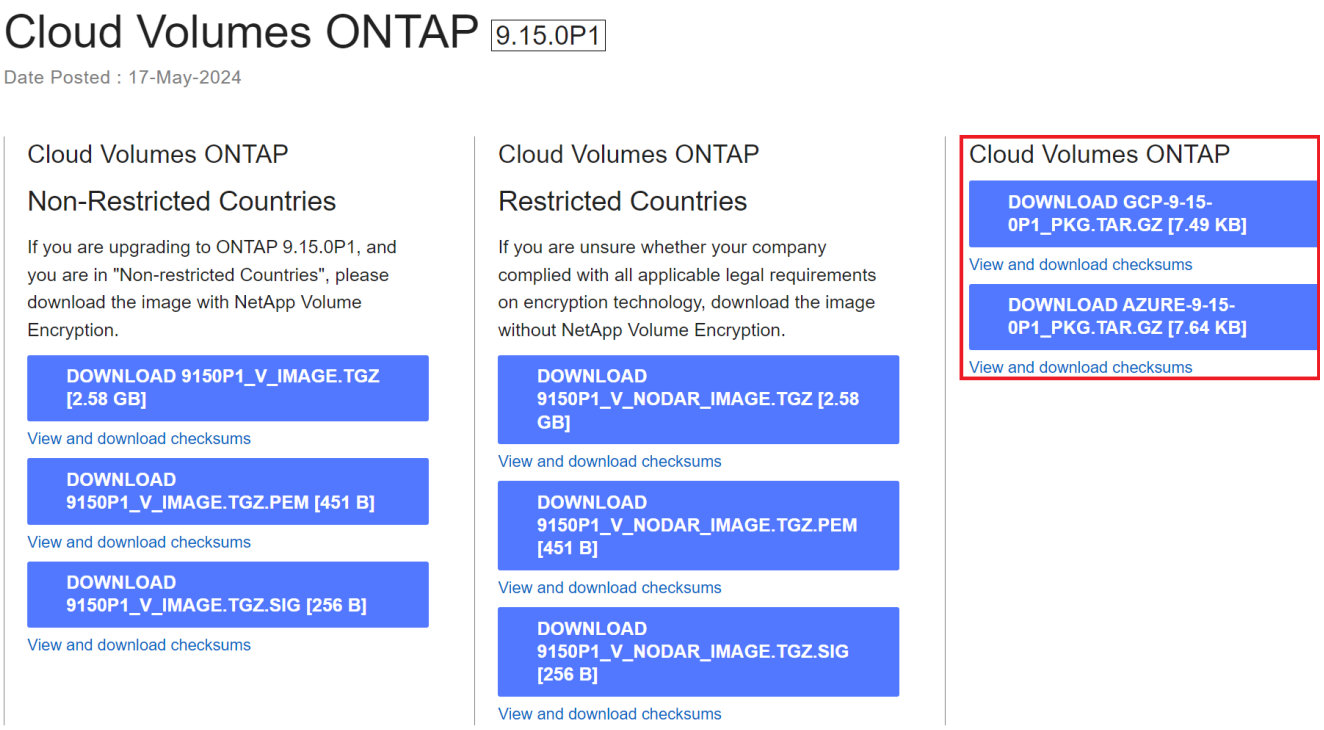
tar.gz 파일에는 이미지 서명 검증에 필요한 파일이 포함되어 있습니다. *tar.gz* 파일과 함께 이미지에 대한 *checksum* 파일도 다운로드해야 합니다. 체크섬 파일에는 다음이 포함됩니다. `md5` 그리고 `sha256` *tar.gz* 파일의 체크섬.

단계

1. 로 가다 "NetApp 지원 사이트의 Cloud Volumes ONTAP 제품 페이지" 다운로드 섹션에서 필요한 소프트웨어

버전을 다운로드하세요.

2. Cloud Volumes ONTAP 다운로드 페이지에서 Azure 이미지에 대한 다운로드 가능한 파일을 클릭하고 *tar.gz* 파일을 다운로드합니다.



3. Linux에서 실행 `md5sum AZURE-<version>_PKG.TAR.GZ` .

   macOS에서는 다음을 실행합니다. `sha256sum AZURE-<version>_PKG.TAR.GZ` .

4. 다음을 확인하십시오. `md5sum` 그리고 `sha256sum` 값이 다운로드한 Azure 이미지의 값과 일치합니다.

5. Linux 및 macOS에서는 다음을 사용하여 *tar.gz* 파일을 추출합니다. `tar -xzf` 명령.

   추출된 *tar.gz* 파일에는 다이제스트(*.sig*) 파일, 공개 키 인증서(*.pem*) 파일, 체인 인증서(*.pem*) 파일이 포함되어 있습니다.

   tar.gz 파일을 추출한 후의 출력 예**:**

```
$ 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 Cloud Volumes ONTAP 용 VHD 이미지 내보내기

VHD 이미지가 Azure 클라우드에 게시되면 더 이상 NetApp 에서 관리되지 않습니다. 대신, 게시된 이미지는 Azure Marketplace에 배치됩니다. 이미지가 Azure 마켓플레이스에 스테이징되어 게시되면 Azure는 VHD의 시작 부분에서 1MB, 끝 부분에서 512바이트를 수정합니다. VHD 파일의 서명을 확인하려면 Azure 마켓플레이스에서 Azure가 수정한 VHD 이미지를 내보내야 합니다.

시작하기 전에

시스템에 Azure CLI가 설치되어 있는지, 아니면 Azure Portal을 통해 Azure Cloud Shell을 사용할 수 있는지 확인하세요. Azure CLI를 설치하는 방법에 대한 자세한 내용은 다음을 참조하세요. "Microsoft 설명서: Azure CLI 설치 방법" .

단계

1. *version_readme* 파일의 내용을 사용하여 시스템의 Cloud Volumes ONTAP 버전을 Azure Marketplace 이미지 버전에 매핑합니다. Cloud Volumes ONTAP 버전은 다음과 같이 표현됩니다. `buildname` Azure Marketplace 이미지 버전은 다음과 같이 표현됩니다. `version` 버전 매핑에서.

   다음 예에서는 Cloud Volumes ONTAP 버전 `9.15.0P1` Azure Marketplace 이미지 버전에 매핑됨 `9150.01000024.05090105` . 이 Azure 마켓플레이스 이미지 버전은 나중에 이미지 URN을 설정하는 데 사용됩니다.

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

   ]
   ```

2. VM을 만들려는 지역을 식별합니다. 지역 이름은 값으로 사용됩니다. `locName` 마켓플레이스 이미지의 URN을 설정할 때 변수입니다. 사용 가능한 지역을 나열하려면 다음 명령을 실행하세요.

   ```
   az account list-locations -o table
   ```

   이 표에서는 지역 이름이 다음과 같이 나타납니다. `Name` 필드.

```
$ 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 Cloud Volumes ONTAP 버전과 VM 배포 유형에 대한 SKU 이름을 검토하세요. SKU 이름은 값으로 사용됩니다. `skuName` 마켓플레이스 이미지의 URN을 설정할 때 변수입니다.

   예를 들어, Cloud Volumes ONTAP 9.15.0을 사용한 모든 단일 노드 배포는 다음을 사용해야 합니다. `ontap_cloud_byol` SKU 이름으로.

* Cloud Volumes ONTAP 버전*	**VM** 배포를 통해	**SKU** 이름
9.17.1 이상	Azure 마켓플레이스	ontap_cloud_direct_gen2
9.17.1 이상	NetApp Console	ontap_cloud_gen2
9.16.1	Azure 마켓플레이스	온탭_클라우드_다이렉트
9.16.1	콘솔	온탭_클라우드
9.15.1	콘솔	온탭_클라우드
9.15.0	콘솔, 단일 노드 배포	온탭_클라우드_바이올
9.15.0	콘솔, 고가용성(HA) 배포	온탑_클라우드_비올_하

4. ONTAP 버전과 Azure 마켓플레이스 이미지를 매핑한 후 Azure Cloud Shell 또는 Azure CLI를 사용하여 Azure 마켓플레이스에서 VHD 파일을 내보냅니다.

Linux에서 **Azure Cloud Shell**을 사용하여 **VHD** 파일 내보내기

Azure Cloud Shell에서 마켓플레이스 이미지를 VHD 파일(예: *9150.01000024.05090105.vhd*)로 내보내고 로컬 Linux 시스템에 다운로드합니다. Azure Marketplace에서 VHD 이미지를 가져오려면 다음 단계를 수행하세요.

단계

1. 마켓플레이스 이미지의 URN 및 기타 매개변수를 설정합니다. URN 형식은 다음과 같습니다. `<publisher>:<offer>:<sku>:<version>` . 선택적으로 NetApp 마켓플레이스 이미지를 나열하여 올바른 이미지 버전을 확인할 수 있습니다.

```
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
...
```

2. 일치하는 이미지 버전으로 마켓플레이스 이미지에서 새 관리 디스크를 만듭니다.

```
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
```

3. 관리 디스크에서 Azure Storage로 VHD 파일을 내보냅니다. 적절한 액세스 수준으로 컨테이너를 만듭니다. 이 예에서 우리는 다음과 같은 이름의 컨테이너를 사용했습니다. `vm-images` ~와 함께 `Container` 접근 수준. Azure Portal에서 저장소 계정 액세스 키를 가져옵니다. 저장소 계정 **> *examplesaname* >** 액세스 키 **> *key1* > *key* >** 표시 **> <복사>**

```
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
```

4. 생성된 이미지를 Linux 시스템에 다운로드합니다. 사용하다 `wget` VHD 파일을 다운로드하는 명령:

```
wget <URL of filename/Containers/vm-images/9150.01000024.05090105.vhd>
```

URL은 표준 형식을 따릅니다. 자동화를 위해 아래와 같이 URL 문자열을 파생시킬 수 있습니다. 또는 Azure CLI를 사용할 수 있습니다. `az` URL을 가져오는 명령입니다. URL 예시:https://examplesaname.bluexpinfraprod.eastus2.data.azurecr.io/vm-images/9150.01000024.05090105.vhd[]

5. 관리되는 디스크 정리

```
PS /home/user1> Revoke-AzDiskAccess -ResourceGroupName $diskRG -DiskName
$diskName
PS /home/user1> Remove-AzDisk -ResourceGroupName $diskRG -DiskName
$diskName
```

Linux에서 Azure CLI를 사용하여 VHD 파일 내보내기

로컬 Linux 시스템에서 Azure CLI를 사용하여 마켓플레이스 이미지를 VHD 파일로 내보냅니다.

단계

1. Azure CLI에 로그인하고 마켓플레이스 이미지를 나열합니다.

```
% az login --use-device-code
```

2. 로그인하려면 웹 브라우저를 사용하여 페이지를 엽니다. https://microsoft.com/devicelogin 인증코드를 입력하세요.

```
% 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"
},
...
```

3. 마켓플레이스 이미지에서 일치하는 이미지 버전으로 새로운 관리 디스크를 만듭니다.

```
% 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.bluexpinfraprod.eastus2.data.azurecr.io/xxxxxxx/abcd?sv=2018-03-
28&sr=b&si=xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxx&sigxxxxxxxxxxxxxxxxxxxxxxxx"
}
% export diskAccessSAS="https://md-
xxxxxx.bluexpinfraprod.eastus2.data.azurecr.io/xxxxxxx/abcd?sv=2018-03-
28&sr=b&si=xxxxxxxx-xxxx-xx-xx-xx&sigxxxxxxxxxxxxxxxxxxxxxxxx"
```

프로세스를 자동화하려면 표준 출력에서 SAS를 추출해야 합니다. 자세한 내용은 해당 문서를 참조하세요.

4. 관리 디스크에서 VHD 파일을 내보냅니다.

   a. 적절한 액세스 수준으로 컨테이너를 만듭니다. 이 예에서는 컨테이너라는 이름이 있습니다. `vm-images` ~와 함께 `Container` 접근 수준이 사용됩니다.

   b. Azure Portal에서 저장소 계정 액세스 키를 가져옵니다. 저장소 계정 **> *examplesaname* >** 액세스 키 **> *key1* > *key* >** 표시 **> <복사>**

      또한 다음을 사용할 수도 있습니다. `az` 이 단계에 대한 명령입니다.

```
% 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": "\"0xXXXXXXXXXXXXXXXX\"",
  "last_modified": "2022-11-02T22:02:39+00:00",
  "request_id": "xxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxx",
  "version": "2020-06-12",
  "version_id": null
}
```

5. Blob 복사본의 상태를 확인하세요.

```
% 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.bluexpinfraprod.eastus2.data.azurecr.io/xxxxx/abcd?sv=2018-03-
28&sr=b&si=xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxx",
      "status": "success",
      "statusDescription": null
    },
....
```

6. 생성된 이미지를 Linux 서버로 다운로드합니다.

```
wget <URL of file examplesaname/Containers/vm-
images/9150.01000024.05090105.vhd>
```

URL은 표준 형식을 따릅니다. 자동화를 위해 아래와 같이 URL 문자열을 파생시킬 수 있습니다. 또는 Azure CLI를 사용할 수 있습니다. `az` URL을 가져오는 명령입니다. URL 예시:https://examplesaname.bluexpinfraprod.eastus2.data.azurecr.io/vm-images/9150.01000024.05090105.vhd[]

7. 관리되는 디스크 정리

```
az disk revoke-access --name $diskName --resource-group $diskRG
az disk delete --name $diskName --resource-group $diskRG --yes
```

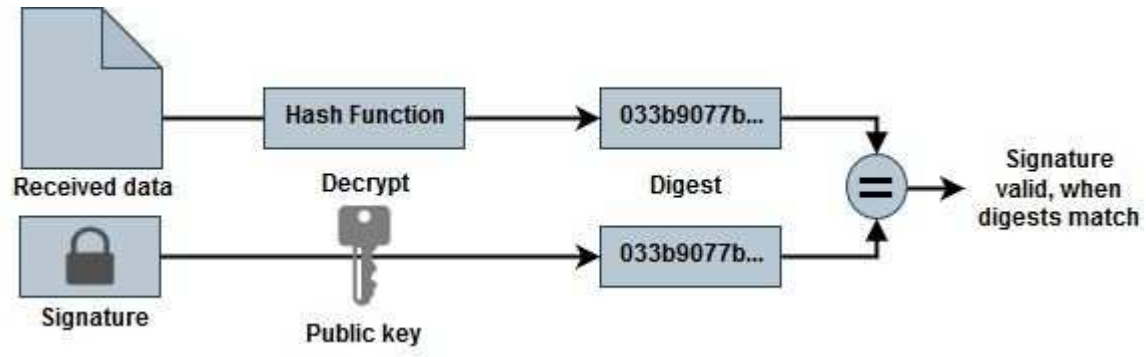
파일 서명 확인

Cloud Volumes ONTAP 에 대한 Azure 마켓플레이스 이미지 서명 확인

Azure 이미지 검증 프로세스는 VHD 파일의 시작 부분에서 1MB, 끝 부분에서 512바이트를 제거한 다음 해시 함수를 적용하여 다이제스트 파일을 생성합니다. 서명 절차를 일치시키기 위해 해싱에는 _sha256_이 사용됩니다.

파일 서명 검증 워크플로 요약

다음은 파일 서명 검증 워크플로 프로세스에 대한 개요입니다.



- Azure 이미지를 다운로드합니다. "NetApp 지원 사이트" 그리고 다이제스트(.sig) 파일, 공개 키 인증서(.pem) 파일, 체인 인증서(.pem) 파일을 추출합니다. . "Azure 이미지 다이제스트 파일 다운로드" 자세한 내용은.
- 신뢰 사슬의 검증.
- 공개 키 인증서(.pem)에서 공개 키(.pub)를 추출합니다.
- 추출된 공개 키를 사용하여 다이제스트 파일을 해독합니다.
- 이미지 파일에서 시작 부분 1MB와 끝 부분 512바이트를 제거한 후 생성된 임시 파일의 새로 생성된 다이제스트와 결과를 비교합니다. 이 단계는 OpenSSL 명령줄 도구를 사용하여 수행됩니다. OpenSSL CLI 도구는 파일 일치에 성공하거나 실패할 경우 적절한 메시지를 표시합니다.

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

Linux에서 Cloud Volumes ONTAP 에 대한 Azure 마켓플레이스 이미지 서명 확인

Linux에서 내보낸 VHD 파일 서명을 검증하는 작업에는 신뢰 체인 검증, 파일 편집, 서명 검증이 포함됩니다.

단계

1. Azure 이미지 파일을 다운로드하세요. "NetApp 지원 사이트" 그리고 다이제스트(.sig) 파일, 공개 키 인증서(.pem) 파일, 체인 인증서(.pem) 파일을 추출합니다.

   참조하다 "Azure 이미지 다이제스트 파일 다운로드" 자세한 내용은.

2. 신뢰 사슬을 확인하세요.

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

3. VHD 파일의 시작 부분에서 1MB(1,048,576바이트)를 제거하고 끝 부분에서 512바이트를 제거합니다. 사용시 `tail` , 그 `-c +K` 이 옵션은 파일의 K번째 바이트에서 바이트를 생성합니다. 따라서 1048577을 전달합니다. `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. OpenSSL을 사용하여 인증서에서 공개 키를 추출하고, 스트립된 파일(sign.tmp)을 서명 파일과 공개 키로 검증합니다.

   명령 프롬프트는 검증 결과에 따라 성공 또는 실패를 나타내는 메시지를 표시합니다.

```
% 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 공간을 정리하세요.

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

macOS에서 Cloud Volumes ONTAP 대한 Azure 마켓플레이스 이미지 서명 확인

Linux에서 내보낸 VHD 파일 서명을 검증하는 작업에는 신뢰 체인 검증, 파일 편집, 서명 검증이 포함됩니다.

단계

1. Azure 이미지 파일을 다운로드하세요. "NetApp 지원 사이트" 그리고 다이제스트(.sig) 파일, 공개 키 인증서(.pem) 파일, 체인 인증서(.pem) 파일을 추출합니다.

   참조하다 "Azure 이미지 다이제스트 파일 다운로드" 자세한 내용은.

2. 신뢰 사슬을 확인하세요.

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

3. VHD 파일의 시작 부분에서 1MB(1,048,576바이트)를 제거하고 끝 부분에서 512바이트를 제거합니다. 사용시 `tail` , 그 `-c +K` 이 옵션은 파일의 K번째 바이트에서 바이트를 생성합니다. 따라서 1048577을 전달합니다. `tail -c` . macOS에서는 tail 명령을 완료하는 데 약 10분이 걸릴 수 있습니다.

```
% 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, 스트립된 파일(sign.tmp)을 서명 파일과 공개 키로

검증합니다. 명령 프롬프트는 검증 결과에 따라 성공 또는 실패를 나타내는 메시지를 표시합니다.

```
% 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 공간을 정리하세요.

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

저작권 정보

Copyright © 2025 NetApp, Inc. All Rights Reserved. 미국에서 인쇄됨 본 문서의 어떠한 부분도 저작권 소유자의 사전 서면 승인 없이는 어떠한 형식이나 수단(복사, 녹음, 녹화 또는 전자 검색 시스템에 저장하는 것을 비롯한 그래픽, 전자적 또는 기계적 방법)으로도 복제될 수 없습니다.

NetApp이 저작권을 가진 자료에 있는 소프트웨어에는 아래의 라이센스와 고지사항이 적용됩니다.

본 소프트웨어는 NetApp에 의해 '있는 그대로' 제공되며 상품성 및 특정 목적에의 적합성에 대한 명시적 또는 묵시적 보증을 포함하여(이에 제한되지 않음) 어떠한 보증도 하지 않습니다. NetApp은 대체품 또는 대체 서비스의 조달, 사용 불능, 데이터 손실, 이익 손실, 영업 중단을 포함하여(이에 국한되지 않음), 이 소프트웨어의 사용으로 인해 발생하는 모든 직접 및 간접 손해, 우발적 손해, 특별 손해, 징벌적 손해, 결과적 손해의 발생에 대하여 그 발생 이유, 책임론, 계약 여부, 엄격한 책임, 불법 행위(과실 또는 그렇지 않은 경우)와 관계없이 어떠한 책임도 지지 않으며, 이와 같은 손실의 발생 가능성이 통지되었다 하더라도 마찬가지입니다.

NetApp은 본 문서에 설명된 제품을 언제든지 예고 없이 변경할 권리를 보유합니다. NetApp은 NetApp의 명시적인 서면 동의를 받은 경우를 제외하고 본 문서에 설명된 제품을 사용하여 발생하는 어떠한 문제에도 책임을 지지 않습니다. 본 제품의 사용 또는 구매의 경우 NetApp에서는 어떠한 특허권, 상표권 또는 기타 지적 재산권이 적용되는 라이센스도 제공하지 않습니다.

본 설명서에 설명된 제품은 하나 이상의 미국 특허, 해외 특허 또는 출원 중인 특허로 보호됩니다.

제한적 권리 표시: 정부에 의한 사용, 복제 또는 공개에는 DFARS 252.227-7013(2014년 2월) 및 FAR 52.227-19(2007년 12월)의 기술 데이터-비상업적 품목에 대한 권리(Rights in Technical Data -Noncommercial Items) 조항의 하위 조항 (b)(3)에 설명된 제한사항이 적용됩니다.

여기에 포함된 데이터는 상업용 제품 및/또는 상업용 서비스(FAR 2.101에 정의)에 해당하며 NetApp, Inc.의 독점 자산입니다. 본 계약에 따라 제공되는 모든 NetApp 기술 데이터 및 컴퓨터 소프트웨어는 본질적으로 상업용이며 개인 비용만으로 개발되었습니다. 미국 정부는 데이터가 제공된 미국 계약과 관련하여 해당 계약을 지원하는 데에만 데이터에 대한 전 세계적으로 비독점적이고 양도할 수 없으며 재사용이 불가능하며 취소 불가능한 라이센스를 제한적으로 가집니다. 여기에 제공된 경우를 제외하고 NetApp, Inc.의 사전 서면 승인 없이는 이 데이터를 사용, 공개, 재생산, 수정, 수행 또는 표시할 수 없습니다. 미국 국방부에 대한 정부 라이센스는 DFARS 조항 252.227-7015(b)(2014년 2월)에 명시된 권한으로 제한됩니다.

상표 정보

NETAPP, NETAPP 로고 및 http://www.netapp.com/TM에 나열된 마크는 NetApp, Inc.의 상표입니다. 기타 회사 및 제품 이름은 해당 소유자의 상표일 수 있습니다.