파일 서명 확인

Cloud Volumes ONTAP

NetApp
November 25, 2025

목차

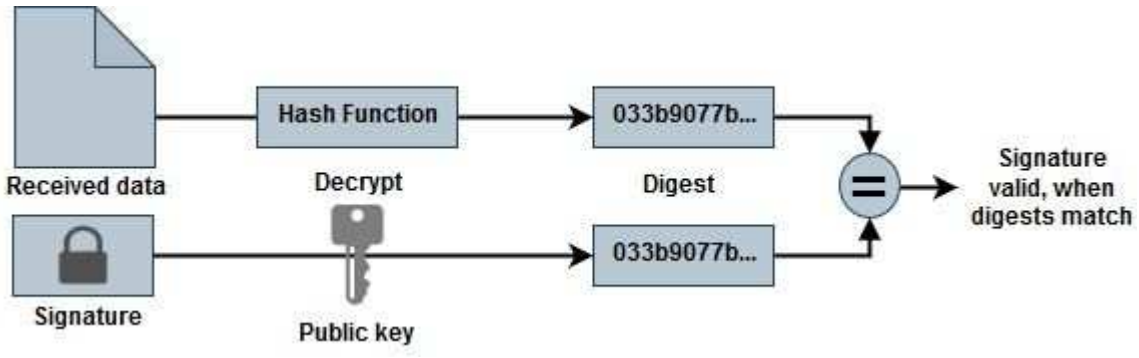
파일 서명 확인

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

상표 정보