파일 서명 확인

Cloud Volumes ONTAP

NetApp
June 27, 2024

목차

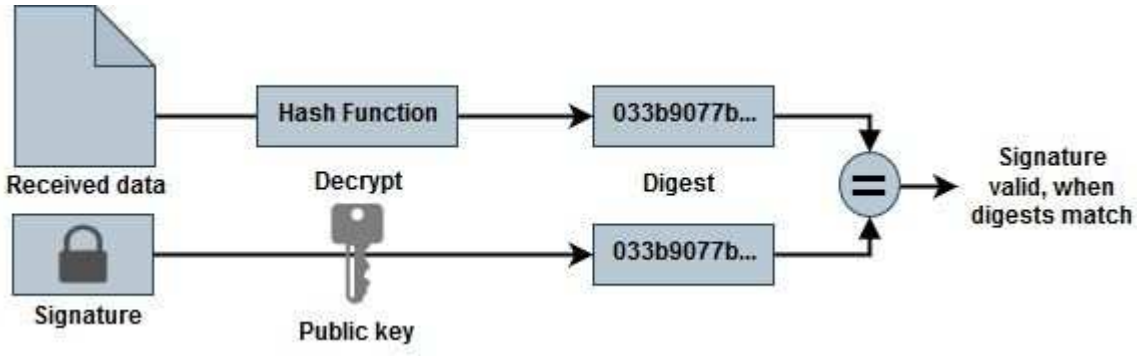
파일 서명 확인

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
```

저작권 정보

상표 정보