



파일 서명 확인

Cloud Volumes ONTAP

NetApp
June 27, 2024

목차

파일 서명 확인	1
파일 서명 확인	1
Linux에서 파일 서명 확인	1
Mac OS에서 파일 서명 확인	3

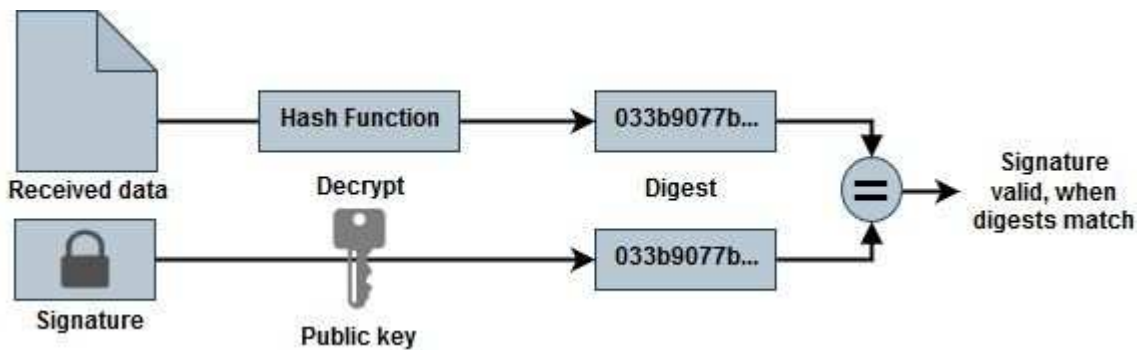
파일 서명 확인

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

Copyright © 2024 NetApp, Inc. All Rights Reserved. 미국에서 인쇄된 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 라이선스와 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 라이선스도 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 라이선스를 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 라이선스는 DFARS 조항 252.227-7015(b)(2014년 2월)에 명시된 권한으로 제한됩니다.

상표 정보

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