



文件签名验证

Cloud Volumes ONTAP

NetApp
June 27, 2024

目录

文件签名验证	1
文件签名验证	1
Linux上的文件签名验证	1
Mac OS上的文件签名验证	3

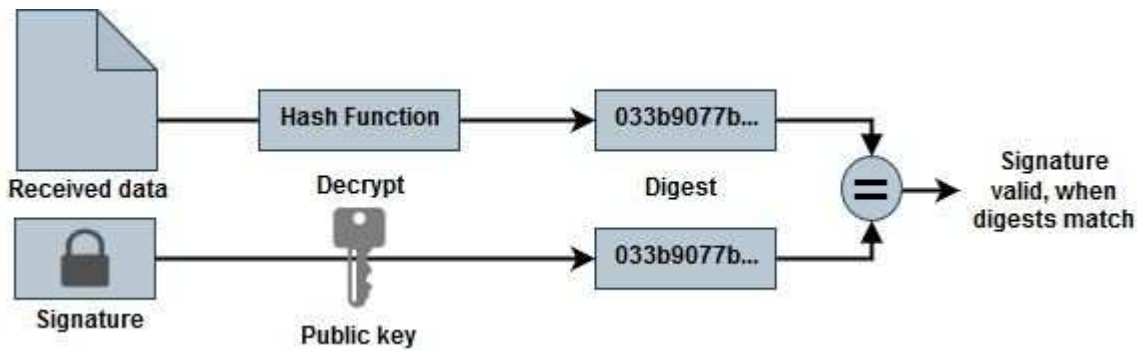
文件签名验证

文件签名验证

Azure映像验证过程将使用哈希函数从具有前导1 MB和末尾512 B条带化的vHD文件生成摘要。为了匹配签名操作步骤、使用SHA256进行哈希。您需要从该视频文件中删除前导1 MB和最终512 B、然后验证视频文件的其余部分。

文件签名验证 workflow 摘要

下面简要介绍了文件签名验证 workflow 过程。



- 从下载Azure Image Digest文件 "[NetApp 支持站点](#)" 并提取摘要文件(.sig)、公共密钥证书文件(.pem)和链证书文件(.pem)。

请参见 "[下载Azure映像摘要文件](#)" 有关详细信息 ...

- 验证信任链。
- 从公共密钥证书(.prom)提取公共密钥(.pub)。
- 提取的公共密钥用于对摘要文件进行解密。然后、将结果与从映像文件创建的临时文件的新未加密摘要进行比较、该文件删除了前导1 MB和结束512字节。

此步骤可通过以下openssl命令来实现。

- 常规CLI语句如下所示：

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

- 如果两个文件都匹配、OpenSSL命令行界面工具会显示"Verified Ok"消息、如果不匹配、则会显示"Verification Failure"消息。

Linux上的文件签名验证

您可以按照以下步骤验证已导出的Linux的VHD文件签名。

步骤

1. 从下载Azure Image Digest文件 "[NetApp 支持站点](#)" 并提取摘要文件(.sig)、公共密钥证书文件(.pem)和链证书文件(.pem)。

请参见 "[下载Azure映像摘要文件](#)" 有关详细信息 ...

2. 验证信任链。

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

3. 删除前1 MB (1048576字节)和后512字节的vhd文件。

如果使用"tail"、则选项"-c +K"将输出以指定文件的K有权 字节开头的字节。因此、1048交由"尾部-c"处理。

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

4. 使用openssl从证书中提取公共密钥、并使用签名文件和公共密钥验证条带化文件(ssign.tmp)。

如果输入文件通过验证、则会显示命令
"验证正常"。否则、将显示"Verification Failure"(验证失败)。

```
% 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. 清理工作空间。

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

Mac OS上的文件签名验证

您可以按照以下步骤验证已导出的Mac OS的vHD文件签名。

步骤

1. 从下载Azure Image Digest文件 "[NetApp 支持站点](#)" 并提取摘要文件(.sig)、公共密钥证书文件(.pem)和链证书文件(.pem)。

请参见 "[下载Azure映像摘要文件](#)" 有关详细信息 ...

2. 验证信任链。

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

3. 删除前1 MB (1048576字节)和后512字节的vHD文件。

如果使用"tail"、则选项"-c +K"输出以K有权 字节开头的字节指定文件的。因此、1048交由"尾部-c"处理。大约需要13米以便在Mac OS上完成尾部命令。

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

4. 使用openssl从证书中提取公共密钥并验证条带化带有签名文件和公共密钥的file(sign.tmp)。

如果输入文件通过验证、则该命令将显示"Verification Ok"(验证正常)。否则、将显示"Verification Failure"(验证失败)。

```
% 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. 清理工作空间。

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

版权信息

版权所有 © 2024 NetApp, Inc.。保留所有权利。中国印刷。未经版权所有者事先书面许可，本档中受版权保护的任何部分不得以任何形式或通过任何手段（图片、电子或机械方式，包括影印、录音、录像或存储在电子检索系统中）进行复制。

从受版权保护的 NetApp 资料派生的软件受以下许可和免责声明的约束：

本软件由 NetApp 按“原样”提供，不含任何明示或暗示担保，包括但不限于适销性以及针对特定用途的适用性的隐含担保，特此声明不承担任何责任。在任何情况下，对于因使用本软件而以任何方式造成的任何直接性、间接性、偶然性、特殊性、惩罚性或后果性损失（包括但不限于购买替代商品或服务；使用、数据或利润方面的损失；或者业务中断），无论原因如何以及基于何种责任理论，无论出于合同、严格责任或侵权行为（包括疏忽或其他行为），NetApp 均不承担责任，即使已被告知存在上述损失的可能性。

NetApp 保留在不另行通知的情况下随时对本文档所述的任何产品进行更改的权利。除非 NetApp 以书面形式明确同意，否则 NetApp 不承担因使用本文档所述产品而产生的任何责任或义务。使用或购买本产品不表示获得 NetApp 的任何专利权、商标权或任何其他知识产权许可。

本手册中描述的产品可能受一项或多项美国专利、外国专利或正在申请的专利的保护。

有限权利说明：政府使用、复制或公开本文档受 DFARS 252.227-7013（2014 年 2 月）和 FAR 52.227-19（2007 年 12 月）中“技术数据权利 — 非商用”条款第 (b)(3) 条规定的限制条件的约束。

本文档中所含数据与商业产品和/或商业服务（定义见 FAR 2.101）相关，属于 NetApp, Inc. 的专有信息。根据本协议提供的所有 NetApp 技术数据和计算机软件具有商业性质，并完全由私人出资开发。美国政府对这些数据的使用权具有非排他性、全球性、受限且不可撤销的许可，该许可既不可转让，也不可再许可，但仅限在与交付数据所依据的美国政府合同有关且受合同支持的情况下使用。除本文档规定的情形外，未经 NetApp, Inc. 事先书面批准，不得使用、披露、复制、修改、操作或显示这些数据。美国政府对国防部的授权仅限于 DFARS 的第 252.227-7015(b)（2014 年 2 月）条款中明确的权利。

商标信息

NetApp、NetApp 标识和 <http://www.netapp.com/TM> 上所列的商标是 NetApp, Inc. 的商标。其他公司和产品名称可能是其各自所有者的商标。