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

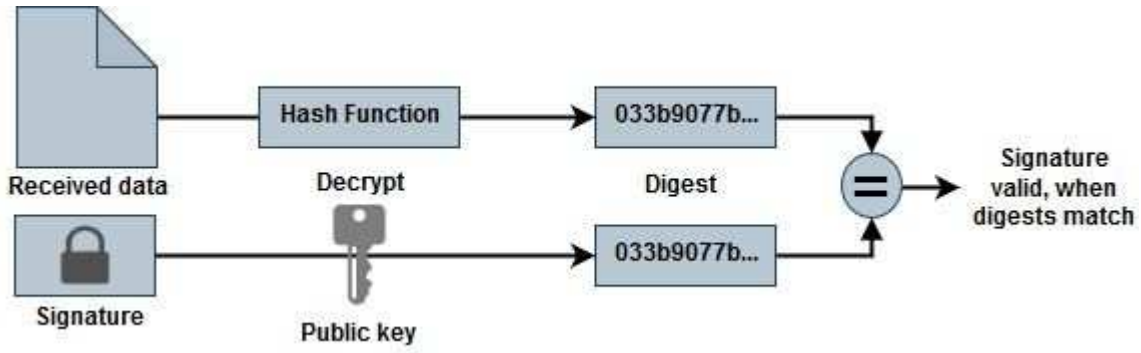
文件签名验证

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。

文件签名验证工作流摘要

下面简要介绍了文件签名验证工作流过程。



- 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opensl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

商标信息