Verificación de firma de archivo

Cloud Volumes ONTAP

NetApp
June 27, 2024

Tabla de contenidos

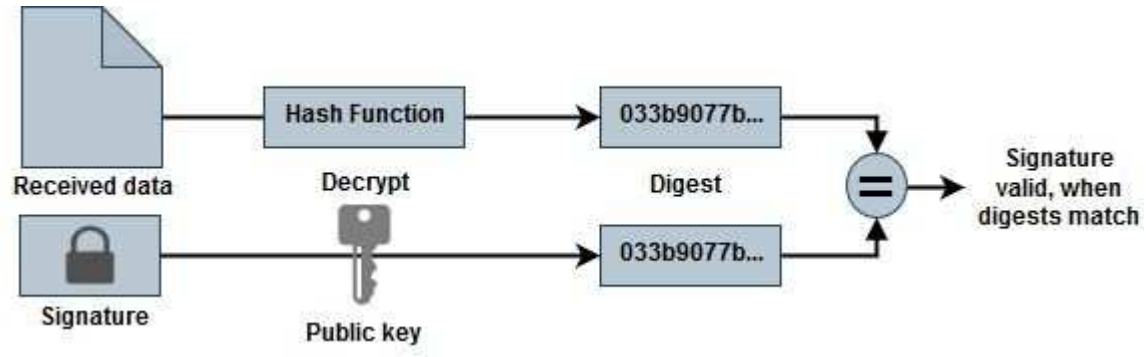
Verificación de firma de archivo

Verificación de firma de archivo

El proceso de verificación de imágenes de Azure generará un resumen del archivo VHD con el 1MB principal y el 512B final segmentado mediante la función hash. Para que coincida con el procedimiento de firma, SHA256 se utiliza para hash. Debe eliminar los 1MB principales y los 512B finales del archivo VHD y, a continuación, verificar la parte restante del archivo VHD.

Resumen del flujo de trabajo de verificación de firmas de archivos

A continuación se ofrece una descripción general del proceso de flujo de trabajo de verificación de firmas de archivos.



- Descargue el archivo Azure Image Digest de la "Sitio de soporte de NetApp" y extraiga el archivo digest(.sig), el archivo de certificado de clave pública(.pem) y el archivo de certificado de cadena(.pem).

  Consulte la "Descargue Azure Image Digest File" si quiere más información.

- Verifique la cadena de confianza.
- Extraiga la clave pública(.pub) del certificado de clave pública(.pem).
- La clave pública extraída se utiliza para descifrar el archivo de resumen. El resultado se compara con un nuevo resumen no cifrado del archivo temporal creado a partir del archivo de imagen con 1MB inicial y 512 bytes finales eliminados.

  Este paso se logra a través del siguiente comando openssl.

  - La sentencia CLI general aparece de la siguiente manera:

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

  - La herramienta CLI de OpenSSL muestra un mensaje de confirmación verificada si ambos archivos coinciden y si no coinciden.

Verificación de firma de archivo en Linux

Puede verificar una firma de archivo VHD exportada para Linux siguiendo los pasos que se indican a continuación.

Pasos

1. Descargue el archivo Azure Image Digest de la "Sitio de soporte de NetApp" y extraiga el archivo digest(.sig), el archivo de certificado de clave pública(.pem) y el archivo de certificado de cadena(.pem).

   Consulte la "Descargue Azure Image Digest File" si quiere más información.

2. Verifique la cadena de confianza.

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

3. Elimine los 1MB primeros (1048576 bytes) y los 512 bytes finales del archivo VHD.

   Si se utiliza 'tail', la opción '-c +K' genera bytes que comienzan con los bytes KTH del archivo especificado. Por lo tanto, 1048577 se pasa a '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. Utilice openssl para extraer la clave pública del certificado y verificar el archivo segmentado (sign.tmp) con el archivo de firma y la clave pública.

   Si el archivo de entrada pasa la verificación, se mostrará el comando
   Verificación correcta. De lo contrario, aparecerá el mensaje Fallo de verificación.

```
% 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. Limpie el espacio de trabajo.

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

Verificación de firma de archivo en Mac OS

Puede verificar una firma de archivo VHD exportada para Mac OS siguiendo los pasos que se indican a continuación.

Pasos

1. Descargue el archivo Azure Image Digest de la "Sitio de soporte de NetApp" y extraiga el archivo digest(.sig), el archivo de certificado de clave pública(.pem) y el archivo de certificado de cadena(.pem).

   Consulte la "Descargue Azure Image Digest File" si quiere más información.

2. Verifique la cadena de confianza.

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

3. Elimine los 1MB primeros (1048576 bytes) y los 512 bytes finales del archivo VHD.

   Si se utiliza 'tail', la opción '-c +K' genera bytes que comienzan con los bytes KTH del archivo especificado. Por lo tanto, 1048577 se pasa a 'tail -c'. Toma alrededor de 13m Para que el comando tail se complete en Mac OS.

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

4. Utilice openssl para extraer la clave pública del certificado y verificar la rayada archivo (sign.tmp) con el archivo de firma y la clave pública.

   Si el archivo de entrada pasa la verificación, el comando mostrará “Verificación correcta”. De lo contrario, aparecerá el mensaje Fallo de verificación.

```
% 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. Limpie el espacio de trabajo.

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

Información de copyright

Información de la marca comercial