



Verificar la firma del archivo

Cloud Volumes ONTAP

NetApp

February 13, 2026

This PDF was generated from <https://docs.netapp.com/es-es/storage-management-cloud-volumes-ontap/concept-azure-file-sig-verify.html> on February 13, 2026. Always check docs.netapp.com for the latest.

Tabla de contenidos

- Verificar la firma del archivo 1
 - Verificación de la firma de imágenes de Azure Marketplace para Cloud Volumes ONTAP 1
 - Resumen del flujo de trabajo de verificación de firmas de archivos 1
 - Verificar la firma de la imagen de Azure Marketplace para Cloud Volumes ONTAP en Linux..... 1
 - Verificar la firma de la imagen de Azure Marketplace para Cloud Volumes ONTAP en macOS 3

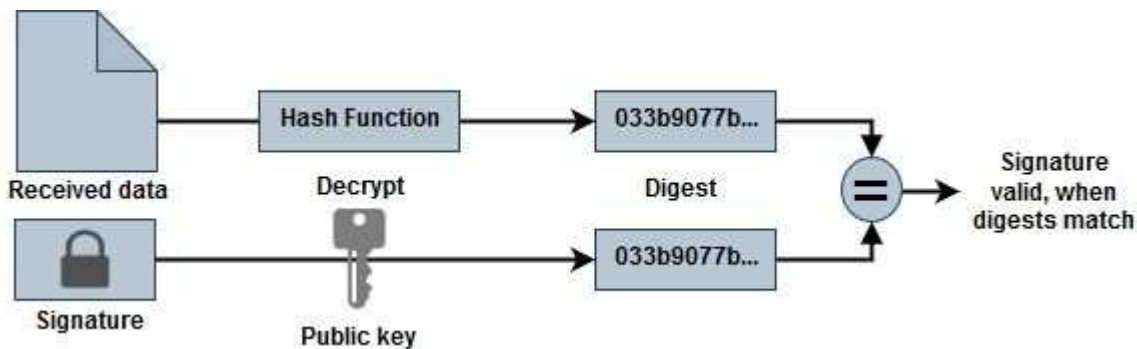
Verificar la firma del archivo

Verificación de la firma de imágenes de Azure Marketplace para Cloud Volumes ONTAP

El proceso de verificación de imágenes de Azure genera un archivo de resumen a partir del archivo VHD quitando 1 MB al principio y 512 bytes al final, y luego aplicando una función hash. Para que coincida con el procedimiento de firma, se utiliza *sha256* para el hash.

Resumen del flujo de trabajo de verificación de firmas de archivos

A continuación se presenta una descripción general del proceso de flujo de trabajo de verificación de firma de archivo.



- Descargar la imagen de Azure desde el ["Sitio de soporte de NetApp"](#) y extraer el archivo de resumen (.sig), el archivo de certificado de clave pública (.pem) y el archivo de certificado de cadena (.pem). Consulte ["Descargar el archivo de resumen de imagen de Azure"](#) Para más información.
- Verificación de la cadena de confianza.
- Extraer la clave pública (.pub) del certificado de clave pública (.pem).
- Descifrar el archivo de resumen utilizando la clave pública extraída.
- Comparando el resultado con un resumen recién generado de un archivo temporal creado a partir del archivo de imagen después de eliminar 1 MB al principio y 512 bytes al final. Este paso se realiza mediante la herramienta de línea de comandos OpenSSL. La herramienta CLI de OpenSSL muestra mensajes apropiados en caso de éxito o fracaso en la coincidencia de los archivos.

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

Verificar la firma de la imagen de Azure Marketplace para Cloud Volumes ONTAP en Linux

La verificación de la firma de un archivo VHD exportado en Linux incluye validar la cadena de confianza, editar el archivo y verificar la firma.

Pasos

1. Descargue el archivo de imagen de Azure desde ["Sitio de soporte de NetApp"](#) y extraiga el archivo de resumen (.sig), el archivo de certificado de clave pública (.pem) y el archivo de certificado de cadena (.pem).

Referirse a ["Descargar el archivo de resumen de imagen de Azure"](#) Para más información.

2. Verificar 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 1 MB (1.048.576 bytes) al principio y 512 bytes al final del archivo VHD. Al utilizar `tail`, el `-c +K` La opción genera bytes a partir del byte K del archivo. Por lo tanto, pasa 1048577 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 eliminado (sign.tmp) con el archivo de firma y la clave pública.

El símbolo del sistema muestra mensajes que indican el éxito o el fracaso según la 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. Limpiar el espacio de trabajo.

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

Verificar la firma de la imagen de Azure Marketplace para Cloud Volumes ONTAP en macOS

La verificación de la firma de un archivo VHD exportado en Linux incluye validar la cadena de confianza, editar el archivo y verificar la firma.

Pasos

1. Descargue el archivo de imagen de Azure desde "[Sitio de soporte de NetApp](#)" y extraiga el archivo de resumen (.sig), el archivo de certificado de clave pública (.pem) y el archivo de certificado de cadena (.pem).

Referirse a "[Descargar el archivo de resumen de imagen de Azure](#)" Para más información.

2. Verificar 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 1 MB (1.048.576 bytes) al principio y 512 bytes al final del archivo VHD. Al utilizar `tail`, el `-c +K` La opción genera bytes a partir del byte K del archivo. Por lo tanto, pasa 1048577 a `tail -c`. Tenga en cuenta que en macOS, el comando `tail` puede tardar unos diez minutos en completarse.

```
% 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 eliminado (sign.tmp) con el archivo de firma y la clave pública. El símbolo del sistema muestra mensajes que indican el éxito o el fracaso según la 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. Limpiar el espacio de trabajo.

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

Información de copyright

Copyright © 2026 NetApp, Inc. Todos los derechos reservados. Imprimido en EE. UU. No se puede reproducir este documento protegido por copyright ni parte del mismo de ninguna forma ni por ningún medio (gráfico, electrónico o mecánico, incluidas fotocopias, grabaciones o almacenamiento en un sistema de recuperación electrónico) sin la autorización previa y por escrito del propietario del copyright.

El software derivado del material de NetApp con copyright está sujeto a la siguiente licencia y exención de responsabilidad:

ESTE SOFTWARE LO PROPORCIONA NETAPP «TAL CUAL» Y SIN NINGUNA GARANTÍA EXPRESA O IMPLÍCITA, INCLUYENDO, SIN LIMITAR, LAS GARANTÍAS IMPLÍCITAS DE COMERCIALIZACIÓN O IDONEIDAD PARA UN FIN CONCRETO, CUYA RESPONSABILIDAD QUEDA EXIMIDA POR EL PRESENTE DOCUMENTO. EN NINGÚN CASO NETAPP SERÁ RESPONSABLE DE NINGÚN DAÑO DIRECTO, INDIRECTO, ESPECIAL, EJEMPLAR O RESULTANTE (INCLUYENDO, ENTRE OTROS, LA OBTENCIÓN DE BIENES O SERVICIOS SUSTITUTIVOS, PÉRDIDA DE USO, DE DATOS O DE BENEFICIOS, O INTERRUPCIÓN DE LA ACTIVIDAD EMPRESARIAL) CUALQUIERA SEA EL MODO EN EL QUE SE PRODUJERON Y LA TEORÍA DE RESPONSABILIDAD QUE SE APLIQUE, YA SEA EN CONTRATO, RESPONSABILIDAD OBJETIVA O AGRAVIO (INCLUIDA LA NEGLIGENCIA U OTRO TIPO), QUE SURJAN DE ALGÚN MODO DEL USO DE ESTE SOFTWARE, INCLUSO SI HUBIEREN SIDO ADVERTIDOS DE LA POSIBILIDAD DE TALES DAÑOS.

NetApp se reserva el derecho de modificar cualquiera de los productos aquí descritos en cualquier momento y sin aviso previo. NetApp no asume ningún tipo de responsabilidad que surja del uso de los productos aquí descritos, excepto aquello expresamente acordado por escrito por parte de NetApp. El uso o adquisición de este producto no lleva implícita ninguna licencia con derechos de patente, de marcas comerciales o cualquier otro derecho de propiedad intelectual de NetApp.

Es posible que el producto que se describe en este manual esté protegido por una o más patentes de EE. UU., patentes extranjeras o solicitudes pendientes.

LEYENDA DE DERECHOS LIMITADOS: el uso, la copia o la divulgación por parte del gobierno están sujetos a las restricciones establecidas en el subpárrafo (b)(3) de los derechos de datos técnicos y productos no comerciales de DFARS 252.227-7013 (FEB de 2014) y FAR 52.227-19 (DIC de 2007).

Los datos aquí contenidos pertenecen a un producto comercial o servicio comercial (como se define en FAR 2.101) y son propiedad de NetApp, Inc. Todos los datos técnicos y el software informático de NetApp que se proporcionan en este Acuerdo tienen una naturaleza comercial y se han desarrollado exclusivamente con fondos privados. El Gobierno de EE. UU. tiene una licencia limitada, irrevocable, no exclusiva, no transferible, no sublicenciable y de alcance mundial para utilizar los Datos en relación con el contrato del Gobierno de los Estados Unidos bajo el cual se proporcionaron los Datos. Excepto que aquí se disponga lo contrario, los Datos no se pueden utilizar, desvelar, reproducir, modificar, interpretar o mostrar sin la previa aprobación por escrito de NetApp, Inc. Los derechos de licencia del Gobierno de los Estados Unidos de América y su Departamento de Defensa se limitan a los derechos identificados en la cláusula 252.227-7015(b) de la sección DFARS (FEB de 2014).

Información de la marca comercial

NETAPP, el logotipo de NETAPP y las marcas que constan en <http://www.netapp.com/TM> son marcas comerciales de NetApp, Inc. El resto de nombres de empresa y de producto pueden ser marcas comerciales de sus respectivos propietarios.