



Verificar la imagen de la plataforma Azure

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-image-verification.html> on February 13, 2026. Always check docs.netapp.com for the latest.

Tabla de contenidos

- Verificar la imagen de la plataforma Azure. 1
 - Verificación de imágenes de Azure Marketplace para Cloud Volumes ONTAP. 1
 - Alteración de archivos VHD publicados por parte de Azure 1
 - Descargue el archivo de imagen de Azure para Cloud Volumes ONTAP 1
 - Exportar imágenes VHD para Cloud Volumes ONTAP desde Azure Marketplace 3
 - Exportar archivo VHD mediante Azure Cloud Shell en Linux 4
 - Exportar archivo VHD mediante la CLI de Azure en Linux 6
 - Verificar la firma del archivo 9
 - Verificación de la firma de imágenes de Azure Marketplace para Cloud Volumes ONTAP. 9
 - Verificar la firma de la imagen de Azure Marketplace para Cloud Volumes ONTAP en Linux. 10
 - Verificar la firma de la imagen de Azure Marketplace para Cloud Volumes ONTAP en macOS 11

Verificar la imagen de la plataforma Azure

Verificación de imágenes de Azure Marketplace para Cloud Volumes ONTAP

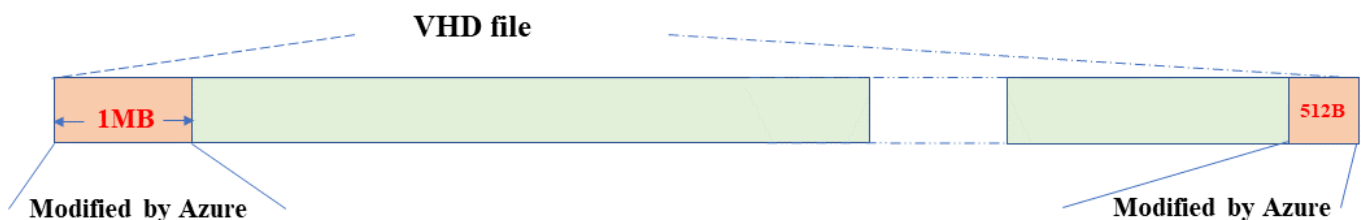
La verificación de imágenes de Azure cumple con los requisitos de seguridad mejorados de NetApp. Verificar un archivo de imagen es un proceso sencillo. Sin embargo, la verificación de la firma de la imagen de Azure requiere consideraciones específicas para el archivo de imagen VHD de Azure porque se modifica en Azure Marketplace.



La verificación de imágenes de Azure es compatible con Cloud Volumes ONTAP 9.15.0 y versiones posteriores.

Alteración de archivos VHD publicados por parte de Azure

Azure modifica los 1 MB (1048576 bytes) al principio y los 512 bytes al final del archivo VHD. NetApp firma el archivo VHD restante.



En el ejemplo, el archivo VHD es de 10 GB. La parte que firmó NetApp está marcada en verde (10 GB - 1 MB - 512 bytes).

Enlaces relacionados

- ["Blog de errores de página: Cómo firmar y verificar usando OpenSSL"](#)
- ["Usar la imagen de Azure Marketplace para crear una imagen de máquina virtual para su GPU de Azure Stack Edge Pro | Microsoft Learn"](#)
- ["Exportar o copiar un disco administrado a una cuenta de almacenamiento mediante la CLI de Azure | Microsoft Learn"](#)
- ["Guía de inicio rápido de Azure Cloud Shell: Bash | Microsoft Learn"](#)
- ["Cómo instalar la CLI de Azure | Microsoft Learn"](#)
- ["Copia de blobs de almacenamiento de Az | Microsoft Learn"](#)
- ["Sign in con la CLI de Azure: Inicio de sesión y autenticación | Microsoft Learn"](#)

Descargue el archivo de imagen de Azure para Cloud Volumes ONTAP

Puede descargar el archivo de imagen de Azure desde ["Sitio de soporte de NetApp"](#).

El archivo *tar.gz* contiene los archivos necesarios para la verificación de la firma de la imagen. Junto con el archivo *tar.gz*, también debe descargar el archivo *checksum* de la imagen. El archivo de suma de

comprobación contiene la md5 y sha256 sumas de comprobación del archivo *tar.gz*.

Pasos

1. Ir a la "[Página del producto Cloud Volumes ONTAP en el sitio de soporte de NetApp](#)" y descargue la versión de software requerida desde la sección **Descargas**.
2. En la página de descarga de Cloud Volumes ONTAP , haga clic en el archivo descargable de la imagen de Azure y descargue el archivo *tar.gz*.

Cloud Volumes ONTAP 9.15.0P1

Date Posted : 17-May-2024

Cloud Volumes ONTAP

Non-Restricted Countries

If you are upgrading to ONTAP 9.15.0P1, and you are in "Non-restricted Countries", please download the image with NetApp Volume Encryption.

DOWNLOAD 9150P1_V_IMAGE.TGZ [2.58 GB]

[View and download checksums](#)

DOWNLOAD 9150P1_V_IMAGE.TGZ.PEM [451 B]

[View and download checksums](#)

DOWNLOAD 9150P1_V_IMAGE.TGZ.SIG [256 B]

[View and download checksums](#)

Cloud Volumes ONTAP

Restricted Countries

If you are unsure whether your company complied with all applicable legal requirements on encryption technology, download the image without NetApp Volume Encryption.

DOWNLOAD 9150P1_V_NODAR_IMAGE.TGZ [2.58 GB]

[View and download checksums](#)

DOWNLOAD 9150P1_V_NODAR_IMAGE.TGZ.PEM [451 B]

[View and download checksums](#)

DOWNLOAD 9150P1_V_NODAR_IMAGE.TGZ.SIG [256 B]

[View and download checksums](#)

Cloud Volumes ONTAP

DOWNLOAD GCP-9-15-0P1_PKG.TAR.GZ [7.49 KB]

[View and download checksums](#)

DOWNLOAD AZURE-9-15-0P1_PKG.TAR.GZ [7.64 KB]

[View and download checksums](#)

3. En Linux, ejecute `md5sum AZURE-<version>_PKG.TAR.GZ` .

En macOS, ejecute `sha256sum AZURE-<version>_PKG.TAR.GZ` .

4. Verificar que el md5sum y sha256sum Los valores coinciden con los de la imagen de Azure descargada.
5. En Linux y macOS, extraiga el archivo *tar.gz* usando el `tar -xzf` dominio.

El archivo *tar.gz* extraído contiene el archivo de resumen (*.sig*), el archivo de certificado de clave pública (*.pem*) y el archivo de certificado de cadena (*.pem*).

Ejemplo de salida después de extraer el archivo tar.gz:

```
$ ls cert/ -l
-rw-r----- 1 netapp netapp 384 May 13 13:00 9.15.0P1_azure_digest.sig
-rw-r----- 1 netapp netapp 2365 May 13 13:00 Certificate-
9.15.0P1_azure.pem
-rw-r----- 1 netapp netapp 8537 May 13 13:00 Certificate-Chain-
9.15.0P1_azure.pem
-rw-r----- 1 netapp netapp 8537 May 13 13:00 version_readme
```

Exportar imágenes VHD para Cloud Volumes ONTAP desde Azure Marketplace

Una vez que la imagen VHD se publica en la nube de Azure, NetApp ya no la administra. En su lugar, la imagen publicada se coloca en el mercado de Azure. Cuando la imagen se prepara y se publica en Azure Marketplace, Azure modifica 1 MB al principio y 512 bytes al final del VHD. Para verificar la firma del archivo VHD, debe exportar la imagen VHD modificada por Azure desde Azure Marketplace.

Antes de empezar

Asegúrese de que la CLI de Azure esté instalada en su sistema o que Azure Cloud Shell esté disponible a través del portal de Azure. Para obtener más información sobre cómo instalar la CLI de Azure, consulte ["Documentación de Microsoft: Cómo instalar la CLI de Azure"](#).

Pasos

1. Asigne la versión de Cloud Volumes ONTAP en su sistema a la versión de la imagen de Azure Marketplace usando el contenido del archivo *version_readme*. La versión de Cloud Volumes ONTAP está representada por `buildname` y la versión de la imagen de Azure Marketplace está representada por `version` en las asignaciones de versiones.

En el siguiente ejemplo, la versión de Cloud Volumes ONTAP 9.15.0P1 se asigna a la versión de la imagen de Azure Marketplace 9150.01000024.05090105. Esta versión de la imagen de Azure Marketplace se utiliza posteriormente para establecer la URN de la imagen.

```
[
  "buildname": "9.15.0P1",
  "publisher": "netapp",
  "version": "9150.01000024.05090105"
]
```

2. Identifique la región donde desea crear las máquinas virtuales. El nombre de la región se utiliza como valor para el `locName` variable al configurar la URN de la imagen del marketplace. Para enumerar las regiones disponibles, ejecute este comando:

```
az account list-locations -o table
```

En esta tabla, el nombre de la región aparece en el `Name` campo.

```
$ az account list-locations -o table
DisplayName          Name          RegionalDisplayName
-----
East US              eastus        (US) East US
East US 2            eastus2       (US) East US 2
South Central US     southcentralus (US) South Central US
...
```

3. Revise los nombres de SKU para las versiones de Cloud Volumes ONTAP y los tipos de implementación de VM correspondientes en la siguiente tabla. El nombre del SKU se utiliza como valor para el `skuName` variable al configurar la URN de la imagen del marketplace.

Por ejemplo, todas las implementaciones de un solo nodo con Cloud Volumes ONTAP 9.15.0 deben usar `ontap_cloud_byol` como el nombre del SKU.

*Versión de Cloud Volumes ONTAP *	Implementación de VM a través de	Nombre del SKU
9.17.1 y posteriores	El mercado de Azure	ontap_cloud_direct_gen2
9.17.1 y posteriores	La NetApp Console	ontap_cloud_gen2
9.16.1	El mercado de Azure	ontap_cloud_direct
9.16.1	La consola	ontap_cloud
9.15.1	La consola	ontap_cloud
9.15.0	La consola, implementaciones de nodo único	ontap_cloud_byol
9.15.0	La consola, implementaciones de alta disponibilidad (HA)	ontap_cloud_byol_ha

4. Después de asignar la versión de ONTAP y la imagen de Azure Marketplace, exporte el archivo VHD desde Azure Marketplace mediante Azure Cloud Shell o la CLI de Azure.

Exportar archivo VHD mediante Azure Cloud Shell en Linux

Desde Azure Cloud Shell, exporte la imagen de Marketplace al archivo VHD (por ejemplo, `9150.01000024.05090105.vhd`) y descárguelo en su sistema Linux local. Realice estos pasos para obtener la imagen VHD del mercado de Azure.

Pasos

1. Establezca la URN y otros parámetros de la imagen del mercado. El formato URN es `<publisher>:<offer>:<sku>:<version>`. Opcionalmente, puede enumerar las imágenes del mercado de NetApp para confirmar la versión correcta de la imagen.

```

PS /home/user1> $urn="netapp:netapp-ontap-
cloud:ontap_cloud_byol:9150.01000024.05090105"
PS /home/user1> $locName="eastus2"
PS /home/user1> $pubName="netapp"
PS /home/user1> $offerName="netapp-ontap-cloud"
PS /home/user1> $skuName="ontap_cloud_byol"
PS /home/user1> Get-AzVMImage -Location $locName -PublisherName $pubName
-Offer $offerName -Sku $skuName |select version
...
141.20231128
9.141.20240131
9.150.20240213
9150.01000024.05090105
...

```

2. Cree un nuevo disco administrado a partir de la imagen de Marketplace con la versión de imagen correspondiente:

```

PS /home/user1> $diskName = "9150.01000024.05090105-managed-disk"
PS /home/user1> $diskRG = "fnf1"
PS /home/user1> az disk create -g $diskRG -n $diskName --image-reference
$urn
PS /home/user1> $sas = az disk grant-access --duration-in-seconds 3600
--access-level Read --name $diskName --resource-group $diskRG
PS /home/user1> $diskAccessSAS = ($sas | ConvertFrom-Json)[0].accessSas

```

3. Exporte el archivo VHD desde el disco administrado a Azure Storage. Cree un contenedor con el nivel de acceso adecuado. En este ejemplo, hemos utilizado un contenedor llamado `vm-images` con `Container` nivel de acceso. Obtenga la clave de acceso de la cuenta de almacenamiento desde el portal de Azure: **Cuentas de almacenamiento > *examplesaname* > Clave de acceso > *key1* > *key* > Mostrar > <copy>**

```

PS /home/user1> $storageAccountName = "examplesaname"
PS /home/user1> $containerName = "vm-images"
PS /home/user1> $storageAccountKey = "<replace with the above access
key>"
PS /home/user1> $destBlobName = "9150.01000024.05090105.vhd"
PS /home/user1> $destContext = New-AzureStorageContext
-StorageAccountName $storageAccountName -StorageAccountKey
$storageAccountKey
PS /home/user1> Start-AzureStorageBlobCopy -AbsoluteUri $diskAccessSAS
-DestContainer $containerName -DestContext $destContext -DestBlob
$destBlobName
PS /home/user1> Get-AzureStorageBlobCopyState -Container $containerName
-Context $destContext -Blob $destBlobName

```

4. Descargue la imagen generada a su sistema Linux. Utilice el `wget` Comando para descargar el archivo VHD:

```
wget <URL of filename/Containers/vm-images/9150.01000024.05090105.vhd>
```

La URL sigue un formato estándar. Para la automatización, puede derivar la cadena URL como se muestra a continuación. Alternativamente, puede utilizar la CLI de Azure `az` Comando para obtener la URL. URL de ejemplo: `https://examplesaname.bluelxpinfraprod.eastus2.data.azurecr.io/vm-images/9150.01000024.05090105.vhd[]`

5. Limpiar el disco administrado

```

PS /home/user1> Revoke-AzDiskAccess -ResourceGroupName $diskRG -DiskName
$diskName
PS /home/user1> Remove-AzDisk -ResourceGroupName $diskRG -DiskName
$diskName

```

Exportar archivo VHD mediante la CLI de Azure en Linux

Exporte la imagen del mercado a un archivo VHD mediante la CLI de Azure desde un sistema Linux local.

Pasos

1. Inicie sesión en la CLI de Azure y enumere las imágenes del Marketplace:

```
% az login --use-device-code
```

2. Para iniciar sesión, utilice un navegador web para abrir la página. <https://microsoft.com/devicelogin> e ingrese el código de autenticación.

```
% az vm image list --all --publisher netapp --offer netapp-ontap-cloud
--sku ontap_cloud_byol
...
{
  "architecture": "x64",
  "offer": "netapp-ontap-cloud",
  "publisher": "netapp",
  "sku": "ontap_cloud_byol",
  "urn": "netapp:netapp-ontap-
cloud:ontap_cloud_byol:9150.01000024.05090105",
  "version": "9150.01000024.05090105"
},
...
```

3. Cree un nuevo disco administrado a partir de la imagen del mercado con la versión de imagen correspondiente.

```
% export urn="netapp:netapp-ontap-
cloud:ontap_cloud_byol:9150.01000024.05090105"
% export diskName="9150.01000024.05090105-managed-disk"
% export diskRG="new_rg_your_rg"
% az disk create -g $diskRG -n $diskName --image-reference $urn
% az disk grant-access --duration-in-seconds 3600 --access-level Read
--name $diskName --resource-group $diskRG
{
  "accessSas": "https://md-
xxxxxx.bluepinfraprod.eastus2.data.azurecr.io/xxxxxxx/abcd?sv=2018-03-
28&sr=b&si=xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxx&sigxxxxxxxxxxxxxxxxxxxxxxxxxxxx"
}
% export diskAccessSAS="https://md-
xxxxxx.bluepinfraprod.eastus2.data.azurecr.io/xxxxxxx/abcd?sv=2018-03-
28&sr=b&si=xxxxxxxx-xxxx-xx-xx-xx&sigxxxxxxxxxxxxxxxxxxxxxxxxxxxx"
```

Para automatizar el proceso, es necesario extraer el SAS de la salida estándar. Consulte los documentos apropiados para obtener orientación.

4. Exportar el archivo VHD desde el disco administrado.
 - a. Cree un contenedor con el nivel de acceso adecuado. En este ejemplo, un contenedor llamado `vm-images` con `Container` Se utiliza el nivel de acceso.
 - b. Obtenga la clave de acceso de la cuenta de almacenamiento desde el portal de Azure: **Cuentas de almacenamiento > *examplesaname* > Clave de acceso > *key1* > *key* > Mostrar > <copy>**

También puedes utilizar el `az` Comando para este paso.

```
% export storageAccountName="examplesaname"
% export containerName="vm-images"
% export storageAccountKey="xxxxxxxxxxx"
% export destBlobName="9150.01000024.05090105.vhd"

% az storage blob copy start --source-uri $diskAccessSAS --destination
--container $containerName --account-name $storageAccountName --account
--key $storageAccountKey --destination-blob $destBlobName

{
  "client_request_id": "xxxx-xxxx-xxxx-xxxx-xxxx",
  "copy_id": "xxxx-xxxx-xxxx-xxxx-xxxx",
  "copy_status": "pending",
  "date": "2022-11-02T22:02:38+00:00",
  "etag": "\"0xxxxxxxxxxxxxxxxxxxx\"",
  "last_modified": "2022-11-02T22:02:39+00:00",
  "request_id": "xxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx",
  "version": "2020-06-12",
  "version_id": null
}
```

5. Verifique el estado de la copia del blob.

```
% az storage blob show --name $destBlobName --container-name
$containerName --account-name $storageAccountName

....
  "copy": {
    "completionTime": null,
    "destinationSnapshot": null,
    "id": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxx",
    "incrementalCopy": null,
    "progress": "10737418752/10737418752",
    "source": "https://md-
xxxxxx.bluexpinfraprod.eastus2.data.azurecr.io/xxxxxx/abcd?sv=2018-03-
28&sr=b&si=xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx",
    "status": "success",
    "statusDescription": null
  },
....
```

6. Descargue la imagen generada a su servidor Linux.

```
wget <URL of file examplesaname/Containers/vm-  
images/9150.01000024.05090105.vhd>
```

La URL sigue un formato estándar. Para la automatización, puede derivar la cadena URL como se muestra a continuación. Alternativamente, puede utilizar la CLI de Azure `az` Comando para obtener la URL. URL de ejemplo: `https://examplesaname.bluelxpinfraprod.eastus2.data.azurecr.io/vm-images/9150.01000024.05090105.vhd`

7. Limpiar el disco administrado

```
az disk revoke-access --name $diskName --resource-group $diskRG  
az disk delete --name $diskName --resource-group $diskRG --yes
```

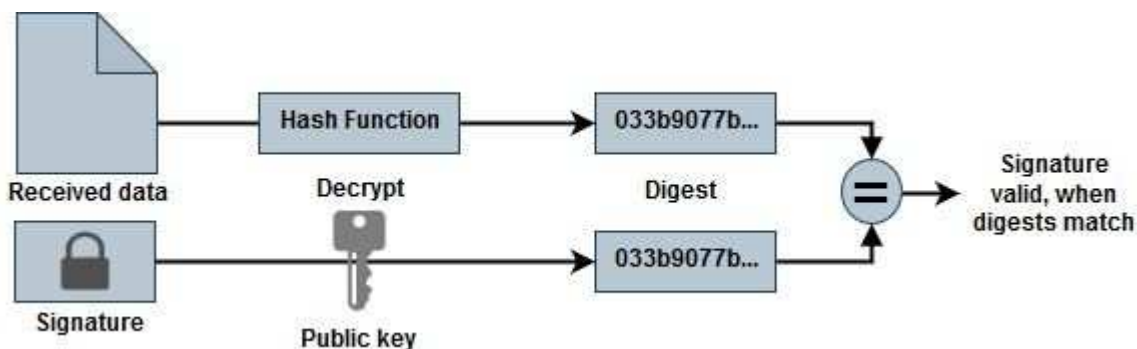
Verificar la firma del archivo

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.