



# **Verificar imagem da plataforma Azure**

## **Cloud Volumes ONTAP**

NetApp  
February 13, 2026

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

# Índice

- Verificar imagem da plataforma Azure . . . . . 1
  - Verificação de imagem do Azure Marketplace para Cloud Volumes ONTAP . . . . . 1
    - Alteração de arquivos VHD publicados pelo Azure . . . . . 1
  - Baixe o arquivo de imagem do Azure para o Cloud Volumes ONTAP . . . . . 1
  - Exportar imagens VHD para o Cloud Volumes ONTAP do marketplace do Azure . . . . . 3
    - Exportar arquivo VHD usando o Azure Cloud Shell no Linux . . . . . 4
    - Exportar arquivo VHD usando a CLI do Azure no Linux . . . . . 6
  - Verificar assinatura do arquivo . . . . . 9
    - Verificação de assinatura de imagem do Azure Marketplace para Cloud Volumes ONTAP . . . . . 9
    - Verificar assinatura de imagem do Azure Marketplace para Cloud Volumes ONTAP no Linux . . . . . 10
    - Verificar assinatura de imagem do Azure Marketplace para Cloud Volumes ONTAP no macOS . . . . . 11

# Verificar imagem da plataforma Azure

## Verificação de imagem do Azure Marketplace para Cloud Volumes ONTAP

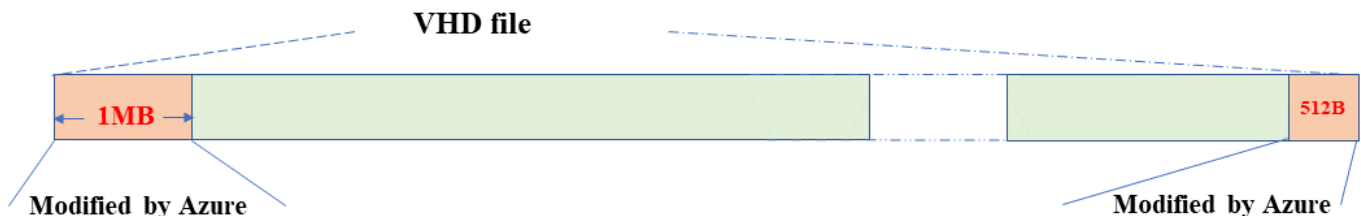
A verificação de imagem do Azure está em conformidade com os requisitos de segurança aprimorados da NetApp. Verificar um arquivo de imagem é um processo simples. No entanto, a verificação da assinatura da imagem do Azure requer considerações específicas para o arquivo de imagem VHD do Azure porque ele é alterado no marketplace do Azure.



A verificação de imagem do Azure é compatível com o Cloud Volumes ONTAP 9.15.0 e posteriores.

### Alteração de arquivos VHD publicados pelo Azure

O 1 MB (1048576 bytes) no início e 512 bytes no final do arquivo VHD são modificados pelo Azure. O NetApp assina o arquivo VHD restante.



No exemplo, o arquivo VHD tem 10 GB. A parte que a NetApp assinou está marcada em verde (10 GB - 1 MB - 512 bytes).

#### Links relacionados

- ["Blog de falhas de página: como assinar e verificar usando OpenSSL"](#)
- ["Use a imagem do Azure Marketplace para criar uma imagem de VM para sua GPU Azure Stack Edge Pro | Microsoft Learn"](#)
- ["Exportar/Copiar um disco gerenciado para uma conta de armazenamento usando a CLI do Azure | Microsoft Learn"](#)
- ["Início rápido do Azure Cloud Shell - Bash | Microsoft Learn"](#)
- ["Como instalar o Azure CLI | Microsoft Learn"](#)
- ["cópia do blob de armazenamento az | Microsoft Learn"](#)
- ["Sign in com a CLI do Azure — Login e Autenticação | Microsoft Learn"](#)

## Baixe o arquivo de imagem do Azure para o Cloud Volumes ONTAP

Você pode baixar o arquivo de imagem do Azure em ["Site de suporte da NetApp"](#).

O arquivo *tar.gz* contém os arquivos necessários para verificação da assinatura da imagem. Junto com o

arquivo *tar.gz*, você também deve baixar o arquivo *checksum* da imagem. O arquivo de soma de verificação contém o md5 e sha256 somas de verificação do arquivo *tar.gz*.

## Passos

1. Vá para o "[Página do produto Cloud Volumes ONTAP no site de suporte da NetApp](#)" e baixe a versão do software necessária na seção **Downloads**.
2. Na página de download do Cloud Volumes ONTAP , clique no arquivo para download da imagem do Azure e baixe o arquivo *tar.gz*.

## Cloud Volumes ONTAP 9.15.0P1

Date Posted : 17-May-2024

Cloud Volumes ONTAP	Cloud Volumes ONTAP	Cloud Volumes ONTAP
<b>Non-Restricted Countries</b>  If you are upgrading to ONTAP 9.15.0P1, and you are in "Non-restricted Countries", please download the image with NetApp Volume Encryption.  <a href="#">DOWNLOAD 9150P1_V_IMAGE.TGZ [2.58 GB]</a> <a href="#">View and download checksums</a>  <a href="#">DOWNLOAD 9150P1_V_IMAGE.TGZ.PEM [451 B]</a> <a href="#">View and download checksums</a>  <a href="#">DOWNLOAD 9150P1_V_IMAGE.TGZ.SIG [256 B]</a> <a href="#">View and download checksums</a>	<b>Restricted Countries</b>  If you are unsure whether your company complied with all applicable legal requirements on encryption technology, download the image without NetApp Volume Encryption.  <a href="#">DOWNLOAD 9150P1_V_NODAR_IMAGE.TGZ [2.58 GB]</a> <a href="#">View and download checksums</a>  <a href="#">DOWNLOAD 9150P1_V_NODAR_IMAGE.TGZ.PEM [451 B]</a> <a href="#">View and download checksums</a>  <a href="#">DOWNLOAD 9150P1_V_NODAR_IMAGE.TGZ.SIG [256 B]</a> <a href="#">View and download checksums</a>	<b>Cloud Volumes ONTAP</b>  <a href="#">DOWNLOAD GCP-9-15-0P1_PKG.TAR.GZ [7.49 KB]</a> <a href="#">View and download checksums</a>  <a href="#">DOWNLOAD AZURE-9-15-0P1_PKG.TAR.GZ [7.64 KB]</a> <a href="#">View and download checksums</a>

3. No Linux, execute `md5sum AZURE-<version>_PKG.TAR.GZ .`

No macOS, execute `sha256sum AZURE-<version>_PKG.TAR.GZ .`

4. Verifique se o `md5sum` e `sha256sum` os valores correspondem aos da imagem do Azure baixada.
5. No Linux e macOS, extraia o arquivo *tar.gz* usando o `tar -xzf` comando.

O arquivo *tar.gz* extraído contém o arquivo de resumo (*.sig*), o arquivo de certificado de chave pública (*.pem*) e o arquivo de certificado de cadeia (*.pem*).

### Exemplo de saída após extrair o arquivo *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 imagens VHD para o Cloud Volumes ONTAP do marketplace do Azure

Depois que a imagem VHD é publicada na nuvem do Azure, ela não é mais gerenciada pelo NetApp. Em vez disso, a imagem publicada é colocada no marketplace do Azure. Quando a imagem é preparada e publicada no marketplace do Azure, o Azure modifica 1 MB no início e 512 bytes no final do VHD. Para verificar a assinatura do arquivo VHD, você precisa exportar a imagem VHD modificada pelo Azure do marketplace do Azure.

## Antes de começar

Certifique-se de que a CLI do Azure esteja instalada no seu sistema ou que o Azure Cloud Shell esteja disponível no portal do Azure. Para obter mais informações sobre como instalar o Azure CLI, consulte o ["Documentação da Microsoft: Como instalar o Azure CLI"](#).

## Passos

1. Mapeie a versão do Cloud Volumes ONTAP no seu sistema para a versão da imagem do Azure Marketplace usando o conteúdo do arquivo *version\_readme*. A versão Cloud Volumes ONTAP é representada por `buildname` e a versão da imagem do marketplace do Azure é representada por `version` nos mapeamentos de versão.

No exemplo a seguir, a versão do Cloud Volumes ONTAP 9.15.0P1 é mapeado para a versão da imagem do Azure Marketplace 9150.01000024.05090105. Esta versão da imagem do Azure Marketplace é usada posteriormente para definir o URN da imagem.

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

2. Identifique a região onde você deseja criar as VMs. O nome da região é usado como valor para o `locName` variável ao definir a URN da imagem do marketplace. Para listar as regiões disponíveis, execute este comando:

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

Nesta tabela, o nome da região aparece no `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 os nomes de SKU para as versões correspondentes do Cloud Volumes ONTAP e os tipos de implantação de VM na tabela abaixo. O nome do SKU é usado como valor para o `skuName` variável ao definir o URN da imagem do marketplace.

Por exemplo, todas as implantações de nó único com Cloud Volumes ONTAP 9.15.0 devem usar `ontap_cloud_byol` como o nome do SKU.

* Versão Cloud Volumes ONTAP *	Implantação de VM por meio de	Nome do SKU
9.17.1 e posterior	O mercado do Azure	ontap_cloud_direct_gen2
9.17.1 e posterior	O NetApp Console	ontap_cloud_gen2
9.16.1	O mercado do Azure	ontap_cloud_direct
9.16.1	O Console	ontap_cloud
9.15.1	O Console	ontap_cloud
9.15.0	O Console, implantações de nó único	ontap_cloud_byol
9.15.0	O Console, implantações de alta disponibilidade (HA)	ontap_cloud_byol_ha

4. Após mapear a versão do ONTAP e a imagem do Azure Marketplace, exporte o arquivo VHD do Azure Marketplace usando o Azure Cloud Shell ou o Azure CLI.

## Exportar arquivo VHD usando o Azure Cloud Shell no Linux

No Azure Cloud Shell, exporte a imagem do marketplace para o arquivo VHD (por exemplo, `9150.01000024.05090105.vhd`) e baixe-a para o seu sistema Linux local. Execute estas etapas para obter a imagem VHD do marketplace do Azure.

### Passos

1. Defina o URN e outros parâmetros da imagem do marketplace. O formato URN é `<publisher>:<offer>:<sku>:<version>`. Opcionalmente, você pode listar imagens do NetApp Marketplace para confirmar a versão correta da imagem.

```

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. Crie um novo disco gerenciado a partir da imagem do marketplace com a versão da imagem correspondente:

```

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 o arquivo VHD do disco gerenciado para o Armazenamento do Azure. Crie um contêiner com o nível de acesso apropriado. Neste exemplo, usamos um contêiner chamado `vm-images` com `Container` nível de acesso. Obtenha a chave de acesso da conta de armazenamento no portal do Azure: **Contas de armazenamento > *examplesaname* > Chave de acesso > *key1* > key > Mostrar > <cópia>**

```

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. Baixe a imagem gerada para o seu sistema Linux. Use o `wget` comando para baixar o arquivo VHD:

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

O URL segue um formato padrão. Para automação, você pode derivar a sequência de URL conforme mostrado abaixo. Como alternativa, você pode usar o Azure CLI `az` comando para obter a URL. URL de exemplo: `https://examplesaname.bluelxpinfraprod.eastus2.data.azurecr.io/vm-images/9150.01000024.05090105.vhd[]`

5. Limpe o disco gerenciado

```

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

```

## Exportar arquivo VHD usando a CLI do Azure no Linux

Exporte a imagem do marketplace para um arquivo VHD usando a CLI do Azure de um sistema Linux local.

### Passos

1. Efetue login na CLI do Azure e liste as imagens do marketplace:

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

2. Para fazer login, use um navegador da web para abrir a página <https://microsoft.com/devicelogin> e digite o código de autenticação.



```
% 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. Crie um novo disco gerenciado a partir da imagem do marketplace com a versão da imagem correspondente.

```
% 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/xxxxxx/abcd?sv=2018-03-
28&sr=b&si=xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxx&sigxxxxxxxxxxxxxxxxxxxxxxxxxxxx"
}
% export diskAccessSAS="https://md-
xxxxxx.bluepinfraprod.eastus2.data.azurecr.io/xxxxxx/abcd?sv=2018-03-
28&sr=b&si=xxxxxxxx-xxxx-xx-xx-xx&sigxxxxxxxxxxxxxxxxxxxxxxxxxxxx"
```

Para automatizar o processo, o SAS precisa ser extraído da saída padrão. Consulte os documentos apropriados para obter orientação.

4. Exporte o arquivo VHD do disco gerenciado.
  - a. Crie um contêiner com o nível de acesso apropriado. Neste exemplo, um contêiner chamado `vm-images` com Container nível de acesso é usado.
  - b. Obtenha a chave de acesso da conta de armazenamento no portal do Azure: **Contas de armazenamento > *examplesaname* > Chave de acesso > *key1* > *key* > Mostrar > <cópia>**

Você também pode usar o `az` comando para esta etapa.

```
% 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 o status da cópia do 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/xxxxx/abcd?sv=2018-03-
28&sr=b&si=xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx",
    "status": "success",
    "statusDescription": null
  },
....
```

##### 6. Baixe a imagem gerada para o seu servidor Linux.

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

O URL segue um formato padrão. Para automação, você pode derivar a sequência de URL conforme mostrado abaixo. Como alternativa, você pode usar o Azure CLI `az` comando para obter a URL. URL de exemplo: `https://examplesaname.bluelxpinfraprod.eastus2.data.azurecr.io/vm-images/9150.01000024.05090105.vhd`

## 7. Limpe o disco gerenciado

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

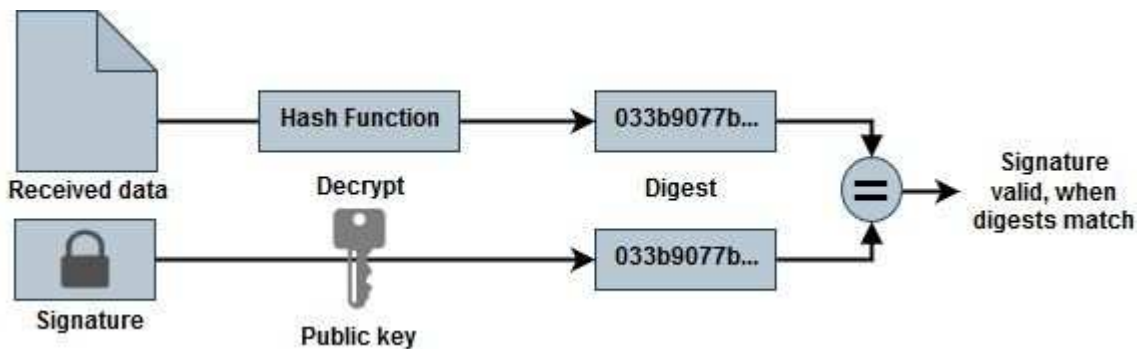
# Verificar assinatura do arquivo

## Verificação de assinatura de imagem do Azure Marketplace para Cloud Volumes ONTAP

O processo de verificação de imagem do Azure gera um arquivo de resumo a partir do arquivo VHD, retirando 1 MB no início e 512 bytes no final e, em seguida, aplicando uma função de hash. Para corresponder ao procedimento de assinatura, *sha256* é usado para hash.

### Resumo do fluxo de trabalho de verificação de assinatura de arquivo

A seguir, uma visão geral do processo de fluxo de trabalho de verificação de assinatura de arquivo.



- Baixando a imagem do Azure do ["Site de suporte da NetApp"](#) e extrair o arquivo digest (.sig), o arquivo de certificado de chave pública (.pem) e o arquivo de certificado de cadeia (.pem). Consulte ["Baixe o arquivo de resumo da imagem do Azure"](#) para maiores informações.
- Verificação da cadeia de confiança.
- Extraindo a chave pública (.pub) do certificado de chave pública (.pem).
- Descriptografando o arquivo de resumo usando a chave pública extraída.
- Comparando o resultado com um resumo recém-gerado de um arquivo temporário criado a partir do arquivo de imagem após remover 1 MB no início e 512 bytes no final. Esta etapa é realizada usando a

ferramenta de linha de comando OpenSSL. A ferramenta OpenSSL CLI exibe mensagens apropriadas sobre sucesso ou falha na correspondência dos arquivos.

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

## Verificar assinatura de imagem do Azure Marketplace para Cloud Volumes ONTAP no Linux

A verificação da assinatura de um arquivo VHD exportado no Linux inclui a validação da cadeia de confiança, a edição do arquivo e a verificação da assinatura.

### Passos

1. Baixe o arquivo de imagem do Azure em "[Site de suporte da NetApp](#)" e extraia o arquivo digest (.sig), o arquivo de certificado de chave pública (.pem) e o arquivo de certificado de cadeia (.pem).

Consulte "[Baixe o arquivo de resumo da imagem do Azure](#)" para maiores informações.

2. Verifique a cadeia de confiança.

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

3. Remova 1 MB (1.048.576 bytes) no início e 512 bytes no final do arquivo VHD. Ao usar `tail`, o `-c +K` opção gera bytes a partir do K-ésimo byte do arquivo. Portanto, ele passa 1048577 para `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. Use o OpenSSL para extrair a chave pública do certificado e verificar o arquivo removido (sign.tmp) com o arquivo de assinatura e a chave pública.

O prompt de comando exibe mensagens indicando sucesso ou falha com base na verificação.

```
% 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. Limpe o espaço de trabalho.

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

## Verificar assinatura de imagem do Azure Marketplace para Cloud Volumes ONTAP no macOS

A verificação da assinatura de um arquivo VHD exportado no Linux inclui a validação da cadeia de confiança, a edição do arquivo e a verificação da assinatura.

### Passos

1. Baixe o arquivo de imagem do Azure em ["Site de suporte da NetApp"](#) e extraia o arquivo digest (.sig), o arquivo de certificado de chave pública (.pem) e o arquivo de certificado de cadeia (.pem).

Consulte ["Baixe o arquivo de resumo da imagem do Azure"](#) para maiores informações.

2. Verifique a cadeia de confiança.

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

3. Remova 1 MB (1.048.576 bytes) no início e 512 bytes no final do arquivo VHD. Ao usar `tail`, o `-c +K` opção gera bytes a partir do K-ésimo byte do arquivo. Portanto, ele passa 1048577 para `tail -c`. Observe que no macOS, o comando `tail` pode levar cerca de dez minutos para ser concluído.

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

4. Use o OpenSSL para extrair a chave pública do certificado e verificar o arquivo removido (sign.tmp) com o

arquivo de assinatura e a chave pública. O prompt de comando exibe mensagens indicando sucesso ou falha com base na verificação.

```
% 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. Limpe o espaço de trabalho.

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

## **Informações sobre direitos autorais**

Copyright © 2026 NetApp, Inc. Todos os direitos reservados. Impresso nos EUA. Nenhuma parte deste documento protegida por direitos autorais pode ser reproduzida de qualquer forma ou por qualquer meio — gráfico, eletrônico ou mecânico, incluindo fotocópia, gravação, gravação em fita ou storage em um sistema de recuperação eletrônica — sem permissão prévia, por escrito, do proprietário dos direitos autorais.

O software derivado do material da NetApp protegido por direitos autorais está sujeito à seguinte licença e isenção de responsabilidade:

ESTE SOFTWARE É FORNECIDO PELA NETAPP "NO PRESENTE ESTADO" E SEM QUAISQUER GARANTIAS EXPRESSAS OU IMPLÍCITAS, INCLUINDO, SEM LIMITAÇÕES, GARANTIAS IMPLÍCITAS DE COMERCIALIZAÇÃO E ADEQUAÇÃO A UM DETERMINADO PROPÓSITO, CONFORME A ISENÇÃO DE RESPONSABILIDADE DESTES DOCUMENTOS. EM HIPÓTESE ALGUMA A NETAPP SERÁ RESPONSÁVEL POR QUALQUER DANO DIRETO, INDIRETO, INCIDENTAL, ESPECIAL, EXEMPLAR OU CONSEQUENCIAL (INCLUINDO, SEM LIMITAÇÕES, AQUISIÇÃO DE PRODUTOS OU SERVIÇOS SOBRESSALENTE; PERDA DE USO, DADOS OU LUCROS; OU INTERRUPÇÃO DOS NEGÓCIOS), INDEPENDENTEMENTE DA CAUSA E DO PRINCÍPIO DE RESPONSABILIDADE, SEJA EM CONTRATO, POR RESPONSABILIDADE OBJETIVA OU PREJUÍZO (INCLUINDO NEGLIGÊNCIA OU DE OUTRO MODO), RESULTANTE DO USO DESTES DOCUMENTOS, MESMO SE ADVERTIDA DA RESPONSABILIDADE DE TAL DANO.

A NetApp reserva-se o direito de alterar quaisquer produtos descritos neste documento, a qualquer momento e sem aviso. A NetApp não assume nenhuma responsabilidade nem obrigação decorrentes do uso dos produtos descritos neste documento, exceto conforme expressamente acordado por escrito pela NetApp. O uso ou a compra deste produto não representam uma licença sob quaisquer direitos de patente, direitos de marca comercial ou quaisquer outros direitos de propriedade intelectual da NetApp.

O produto descrito neste manual pode estar protegido por uma ou mais patentes dos EUA, patentes estrangeiras ou pedidos pendentes.

LEGENDA DE DIREITOS LIMITADOS: o uso, a duplicação ou a divulgação pelo governo estão sujeitos a restrições conforme estabelecido no subparágrafo (b)(3) dos Direitos em Dados Técnicos - Itens Não Comerciais no DFARS 252.227-7013 (fevereiro de 2014) e no FAR 52.227- 19 (dezembro de 2007).

Os dados aqui contidos pertencem a um produto comercial e/ou serviço comercial (conforme definido no FAR 2.101) e são de propriedade da NetApp, Inc. Todos os dados técnicos e software de computador da NetApp fornecidos sob este Contrato são de natureza comercial e desenvolvidos exclusivamente com despesas privadas. O Governo dos EUA tem uma licença mundial limitada, irrevogável, não exclusiva, intransferível e não sublicenciável para usar os Dados que estão relacionados apenas com o suporte e para cumprir os contratos governamentais desse país que determinam o fornecimento de tais Dados. Salvo disposição em contrário no presente documento, não é permitido usar, divulgar, reproduzir, modificar, executar ou exibir os dados sem a aprovação prévia por escrito da NetApp, Inc. Os direitos de licença pertencentes ao governo dos Estados Unidos para o Departamento de Defesa estão limitados aos direitos identificados na cláusula 252.227-7015(b) (fevereiro de 2014) do DFARS.

## **Informações sobre marcas comerciais**

NETAPP, o logotipo NETAPP e as marcas listadas em <http://www.netapp.com/TM> são marcas comerciais da NetApp, Inc. Outros nomes de produtos e empresas podem ser marcas comerciais de seus respectivos proprietários.