



Verificar assinatura do arquivo

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-file-sig-verify.html> on February 13, 2026. Always check docs.netapp.com for the latest.

Índice

- Verificar assinatura do arquivo 1
 - Verificação de assinatura de imagem do Azure Marketplace para Cloud Volumes ONTAP 1
 - Resumo do fluxo de trabalho de verificação de assinatura de arquivo 1
 - Verificar assinatura de imagem do Azure Marketplace para Cloud Volumes ONTAP no Linux..... 1
 - Verificar assinatura de imagem do Azure Marketplace para Cloud Volumes ONTAP no macOS 3

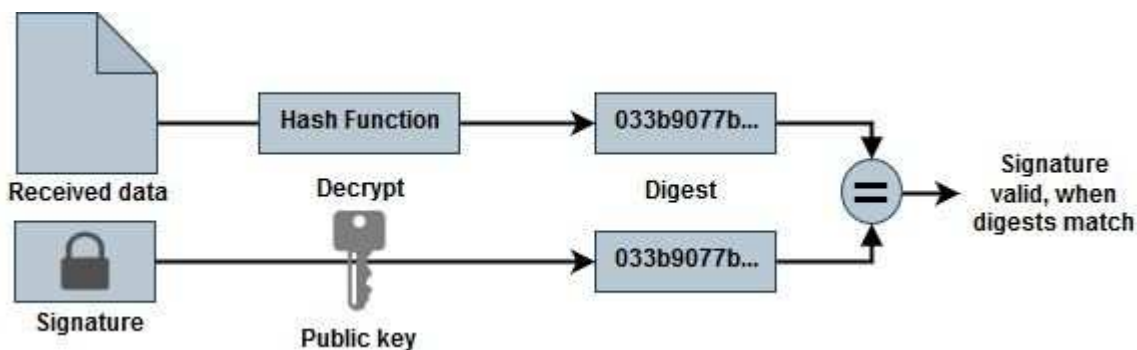
Verificar assinatura do arquivo

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 SOBRESSALIENTES; 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.