



Verifica la firma del file

Cloud Volumes ONTAP

NetApp

February 13, 2026

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

Sommario

Verifica la firma del file	1
Verifica della firma dell'immagine di Azure Marketplace per Cloud Volumes ONTAP	1
Riepilogo del flusso di lavoro di verifica della firma del file	1
Verifica la firma dell'immagine di Azure Marketplace per Cloud Volumes ONTAP su Linux	1
Verifica la firma dell'immagine di Azure Marketplace per Cloud Volumes ONTAP su macOS	2

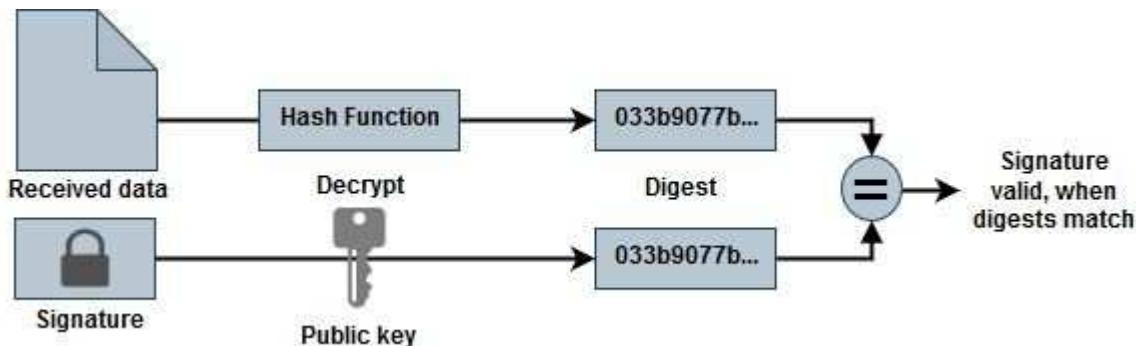
Verifica la firma del file

Verifica della firma dell'immagine di Azure Marketplace per Cloud Volumes ONTAP

Il processo di verifica dell'immagine di Azure genera un file digest dal file VHD eliminando 1 MB all'inizio e 512 byte alla fine, quindi applicando una funzione hash. Per abbinare la procedura di firma, per l'hashing viene utilizzato *sha256*.

Riepilogo del flusso di lavoro di verifica della firma del file

Di seguito è riportata una panoramica del processo di verifica della firma del file.



- Scaricamento dell'immagine di Azure da "[Sito di supporto NetApp](#)" ed estraendo il file digest (.sig), il file del certificato della chiave pubblica (.pem) e il file del certificato della catena (.pem). Fare riferimento a "[Scarica il file digest dell'immagine di Azure](#)" per maggiori informazioni.
- Verifica della catena di fiducia.
- Estrazione della chiave pubblica (.pub) dal certificato della chiave pubblica (.pem).
- Decifrare il file digest utilizzando la chiave pubblica estratta.
- Confronto del risultato con un digest appena generato di un file temporaneo creato dal file immagine dopo aver rimosso 1 MB all'inizio e 512 byte alla fine. Questo passaggio viene eseguito utilizzando lo strumento da riga di comando OpenSSL. Lo strumento OpenSSL CLI visualizza un messaggio appropriato in caso di successo o fallimento nella corrispondenza dei file.

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

Verifica la firma dell'immagine di Azure Marketplace per Cloud Volumes ONTAP su Linux

La verifica della firma di un file VHD esportato su Linux include la convalida della catena di attendibilità, la modifica del file e la verifica della firma.

Passi

- Scarica il file immagine di Azure da "[Sito di supporto NetApp](#)" ed estrarre il file digest (.sig), il file del certificato della chiave pubblica (.pem) e il file del certificato della catena (.pem).

Fare riferimento a "[Scarica il file digest dell'immagine di Azure](#)" per maggiori informazioni.

- Verificare la catena di fiducia.

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

- Rimuovere 1 MB (1.048.576 byte) all'inizio e 512 byte alla fine del file VHD. Quando si utilizza tail , IL -c +K L'opzione genera byte dal K-esimo byte del file. Pertanto, passa 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
```

- Utilizzare OpenSSL per estrarre la chiave pubblica dal certificato e verificare il file estratto (sign.tmp) con il file della firma e la chiave pubblica.

Il prompt dei comandi visualizza messaggi che indicano l'esito positivo o negativo della verifica.

```
% 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
```

- Pulisci l'area di lavoro.

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

Verifica la firma dell'immagine di Azure Marketplace per Cloud Volumes ONTAP su macOS

La verifica della firma di un file VHD esportato su Linux include la convalida della catena

di attendibilità, la modifica del file e la verifica della firma.

Passi

1. Scarica il file immagine di Azure da "[Sito di supporto NetApp](#)" ed estrarre il file digest (.sig), il file del certificato della chiave pubblica (.pem) e il file del certificato della catena (.pem).

Fare riferimento a "[Scarica il file digest dell'immagine di Azure](#)" per maggiori informazioni.

2. Verificare la catena di fiducia.

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

3. Rimuovere 1 MB (1.048.576 byte) all'inizio e 512 byte alla fine del file VHD. Quando si utilizza `tail -c +K` l'opzione genera byte dal K-esimo byte del file. Pertanto, passa 1048577 a `tail -c`. Tieni presente che su macOS il comando `tail` potrebbe richiedere circa dieci minuti per essere completato.

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

4. Utilizzare OpenSSL per estrarre la chiave pubblica dal certificato e verificare il file estratto (`sign.tmp`) con il file della firma e la chiave pubblica. Il prompt dei comandi visualizza messaggi che indicano l'esito positivo o negativo della verifica.

```
% 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. Pulisci l'area di lavoro.

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

Informazioni sul copyright

Copyright © 2026 NetApp, Inc. Tutti i diritti riservati. Stampato negli Stati Uniti d'America. Nessuna porzione di questo documento soggetta a copyright può essere riprodotta in qualsiasi formato o mezzo (grafico, elettronico o meccanico, inclusi fotocopie, registrazione, nastri o storage in un sistema elettronico) senza previo consenso scritto da parte del detentore del copyright.

Il software derivato dal materiale sottoposto a copyright di NetApp è soggetto alla seguente licenza e dichiarazione di non responsabilità:

IL PRESENTE SOFTWARE VIENE FORNITO DA NETAPP "COSÌ COM'È" E SENZA QUALSIVOGLIA TIPO DI GARANZIA IMPLICITA O ESPRESSA FRA CUI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, GARANZIE IMPLICITE DI COMMERCIALITÀ E IDONEITÀ PER UNO SCOPO SPECIFICO, CHE VENGONO DECLINATE DAL PRESENTE DOCUMENTO. NETAPP NON VERRÀ CONSIDERATA RESPONSABILE IN ALCUN CASO PER QUALSIVOGLIA DANNO DIRETTO, INDIRETTO, ACCIDENTALE, SPECIALE, ESEMPLARE E CONSEGUENZIALE (COMPRESI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, PROCUREMENT O SOSTITUZIONE DI MERCI O SERVIZI, IMPOSSIBILITÀ DI UTILIZZO O PERDITA DI DATI O PROFITTI OPPURE INTERRUZIONE DELL'ATTIVITÀ AZIENDALE) CAUSATO IN QUALSIVOGLIA MODO O IN RELAZIONE A QUALUNQUE TEORIA DI RESPONSABILITÀ, SIA ESSA CONTRATTUALE, RIGOROSA O DOVUTA A INSOLVENZA (COMPRESA LA NEGLIGENZA O ALTRO) INSORTA IN QUALSIASI MODO ATTRAVERSO L'UTILIZZO DEL PRESENTE SOFTWARE ANCHE IN PRESENZA DI UN PREAVVISO CIRCA L'EVENTUALITÀ DI QUESTO TIPO DI DANNI.

NetApp si riserva il diritto di modificare in qualsiasi momento qualunque prodotto descritto nel presente documento senza fornire alcun preavviso. NetApp non si assume alcuna responsabilità circa l'utilizzo dei prodotti o materiali descritti nel presente documento, con l'eccezione di quanto concordato espressamente e per iscritto da NetApp. L'utilizzo o l'acquisto del presente prodotto non comporta il rilascio di una licenza nell'ambito di un qualche diritto di brevetto, marchio commerciale o altro diritto di proprietà intellettuale di NetApp.

Il prodotto descritto in questa guida può essere protetto da uno o più brevetti degli Stati Uniti, esteri o in attesa di approvazione.

LEGENDA PER I DIRITTI SOTTOPOSTI A LIMITAZIONE: l'utilizzo, la duplicazione o la divulgazione da parte degli enti governativi sono soggetti alle limitazioni indicate nel sottoparagrafo (b)(3) della clausola Rights in Technical Data and Computer Software del DFARS 252.227-7013 (FEB 2014) e FAR 52.227-19 (DIC 2007).

I dati contenuti nel presente documento riguardano un articolo commerciale (secondo la definizione data in FAR 2.101) e sono di proprietà di NetApp, Inc. Tutti i dati tecnici e il software NetApp forniti secondo i termini del presente Contratto sono articoli aventi natura commerciale, sviluppati con finanziamenti esclusivamente privati. Il governo statunitense ha una licenza irrevocabile limitata, non esclusiva, non trasferibile, non cedibile, mondiale, per l'utilizzo dei Dati esclusivamente in connessione con e a supporto di un contratto governativo statunitense in base al quale i Dati sono distribuiti. Con la sola esclusione di quanto indicato nel presente documento, i Dati non possono essere utilizzati, divulgati, riprodotti, modificati, visualizzati o mostrati senza la previa approvazione scritta di NetApp, Inc. I diritti di licenza del governo degli Stati Uniti per il Dipartimento della Difesa sono limitati ai diritti identificati nella clausola DFARS 252.227-7015(b) (FEB 2014).

Informazioni sul marchio commerciale

NETAPP, il logo NETAPP e i marchi elencati alla pagina <http://www.netapp.com/TM> sono marchi di NetApp, Inc. Gli altri nomi di aziende e prodotti potrebbero essere marchi dei rispettivi proprietari.