



Dateisignatur überprüfen

Cloud Volumes ONTAP

NetApp
February 13, 2026

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

Inhalt

- Dateisignatur überprüfen 1
 - Azure Marketplace-Imagesignaturüberprüfung für Cloud Volumes ONTAP 1
 - Zusammenfassung des Workflows zur Dateisignaturüberprüfung 1
 - Überprüfen der Azure Marketplace-Imagesignatur für Cloud Volumes ONTAP unter Linux 1
 - Überprüfen der Azure Marketplace-Imagesignatur für Cloud Volumes ONTAP unter macOS 3

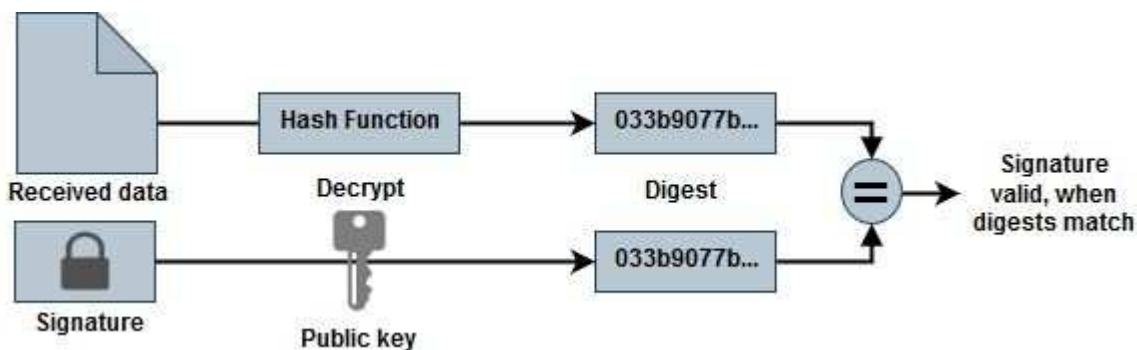
Dateisignatur überprüfen

Azure Marketplace-Imagesignaturüberprüfung für Cloud Volumes ONTAP

Der Azure-Imageüberprüfungsprozess generiert eine Digest-Datei aus der VHD-Datei, indem er am Anfang 1 MB und am Ende 512 Byte entfernt und dann eine Hash-Funktion anwendet. Um dem Signaturverfahren zu entsprechen, wird *sha256* zum Hashing verwendet.

Zusammenfassung des Workflows zur Dateisignaturüberprüfung

Nachfolgend finden Sie eine Übersicht über den Workflow-Prozess zur Dateisignaturüberprüfung.



- Herunterladen des Azure-Images von der ["NetApp Support Site"](#) und Extrahieren der Digest-Datei (.sig), der Public-Key-Zertifikatdatei (.pem) und der Kettenzertifikatdatei (.pem). Weitere Informationen finden Sie unter ["Herunterladen der Azure-Image-Digest-Datei"](#) für weitere Informationen.
- Überprüfung der Vertrauenskette.
- Extrahieren des öffentlichen Schlüssels (.pub) aus dem öffentlichen Schlüsselzertifikat (.pem).
- Entschlüsseln der Digest-Datei mithilfe des extrahierten öffentlichen Schlüssels.
- Vergleichen Sie das Ergebnis mit einem neu generierten Digest einer temporären Datei, die aus der Bilddatei erstellt wurde, nachdem 1 MB am Anfang und 512 Byte am Ende entfernt wurden. Dieser Schritt wird mithilfe des OpenSSL-Befehlszeilentools ausgeführt. Das OpenSSL-CLI-Tool zeigt eine entsprechende Meldung an, wenn die Zuordnung der Dateien erfolgreich war oder fehlgeschlagen ist.

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

Überprüfen der Azure Marketplace-Imagesignatur für Cloud Volumes ONTAP unter Linux

Die Überprüfung der Signatur einer exportierten VHD-Datei unter Linux umfasst die Validierung der Vertrauenskette, die Bearbeitung der Datei und die Überprüfung der Signatur.

Schritte

1. Laden Sie die Azure-Imagedatei von der ["NetApp Support Site"](#) und extrahieren Sie die Digest-Datei (.sig), die Public-Key-Zertifikatdatei (.pem) und die Kettenzertifikatdatei (.pem).

Siehe ["Herunterladen der Azure-Image-Digest-Datei"](#) für weitere Informationen.

2. Überprüfen Sie die Vertrauenskette.

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

3. Entfernen Sie 1 MB (1.048.576 Bytes) am Anfang und 512 Bytes am Ende der VHD-Datei. Bei der Verwendung `tail`, Die `-c +K` Option generiert Bytes aus dem K-ten Byte der Datei. Daher geht es 1048577 an `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. Verwenden Sie OpenSSL, um den öffentlichen Schlüssel aus dem Zertifikat zu extrahieren und die extrahierte Datei (sign.tmp) mit der Signaturdatei und dem öffentlichen Schlüssel zu überprüfen.

Die Eingabeaufforderung zeigt Meldungen an, die den Erfolg oder Misserfolg der Überprüfung basierend auf deren Erfolg anzeigen.

```
% 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. Räumen Sie den Arbeitsbereich auf.

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

Überprüfen der Azure Marketplace-Imagesignatur für Cloud Volumes ONTAP unter macOS

Die Überprüfung der Signatur einer exportierten VHD-Datei unter Linux umfasst die Validierung der Vertrauenskette, die Bearbeitung der Datei und die Überprüfung der Signatur.

Schritte

1. Laden Sie die Azure-Imagedatei von der [NetApp Support Site](#) und extrahieren Sie die Digest-Datei (.sig), die Public-Key-Zertifikatdatei (.pem) und die Kettenzertifikatdatei (.pem).

Siehe ["Herunterladen der Azure-Image-Digest-Datei"](#) für weitere Informationen.

2. Überprüfen Sie die Vertrauenskette.

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

3. Entfernen Sie 1 MB (1.048.576 Bytes) am Anfang und 512 Bytes am Ende der VHD-Datei. Bei der Verwendung `tail`, Die `-c +K` Option generiert Bytes aus dem K-ten Byte der Datei. Daher geht es 1048577 an `tail -c`. Beachten Sie, dass die Ausführung des Tail-Befehls unter macOS etwa zehn Minuten dauern kann.

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

4. Verwenden Sie OpenSSL, um den öffentlichen Schlüssel aus dem Zertifikat zu extrahieren und die extrahierte Datei (sign.tmp) mit der Signaturdatei und dem öffentlichen Schlüssel zu überprüfen. Die Eingabeaufforderung zeigt Meldungen an, die den Erfolg oder Misserfolg der Überprüfung basierend auf deren Erfolg anzeigen.

```
% 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. Räumen Sie den Arbeitsbereich auf.

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

Copyright-Informationen

Copyright © 2026 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtsinhabers in keiner Form und durch keine Mittel – weder grafische noch elektronische oder mechanische, einschließlich Fotokopieren, Aufnehmen oder Speichern in einem elektronischen Abrufsystem – auch nicht in Teilen, vervielfältigt werden.

Software, die von urheberrechtlich geschütztem NetApp Material abgeleitet wird, unterliegt der folgenden Lizenz und dem folgenden Haftungsausschluss:

DIE VORLIEGENDE SOFTWARE WIRD IN DER VORLIEGENDEN FORM VON NETAPP ZUR VERFÜGUNG GESTELLT, D. H. OHNE JEGLICHE EXPLIZITE ODER IMPLIZITE GEWÄHRLEISTUNG, EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE STILLSCHWEIGENDE GEWÄHRLEISTUNG DER MARKTGÄNGIGKEIT UND EIGNUNG FÜR EINEN BESTIMMTEN ZWECK, DIE HIERMIT AUSGESCHLOSSEN WERDEN. NETAPP ÜBERNIMMT KEINERLEI HAFTUNG FÜR DIREKTE, INDIREKTE, ZUFÄLLIGE, BESONDERE, BEISPIELHAFTE SCHÄDEN ODER FOLGESCHÄDEN (EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE BESCHAFFUNG VON ERSATZWAREN ODER -DIENSTLEISTUNGEN, NUTZUNGS-, DATEN- ODER GEWINNVERLUSTE ODER UNTERBRECHUNG DES GESCHÄFTSBETRIEBS), UNABHÄNGIG DAVON, WIE SIE VERURSACHT WURDEN UND AUF WELCHER HAFTUNGSTHEORIE SIE BERUHEN, OB AUS VERTRAGLICH FESTGELEGTER HAFTUNG, VERSCHULDENSUNABHÄNGIGER HAFTUNG ODER DELIKTSHAFTUNG (EINSCHLIESSLICH FAHRLÄSSIGKEIT ODER AUF ANDEREM WEGE), DIE IN IRGEND EINER WEISE AUS DER NUTZUNG DIESER SOFTWARE RESULTIEREN, SELBST WENN AUF DIE MÖGLICHKEIT DERARTIGER SCHÄDEN HINGEWIESEN WURDE.

NetApp behält sich das Recht vor, die hierin beschriebenen Produkte jederzeit und ohne Vorankündigung zu ändern. NetApp übernimmt keine Verantwortung oder Haftung, die sich aus der Verwendung der hier beschriebenen Produkte ergibt, es sei denn, NetApp hat dem ausdrücklich in schriftlicher Form zugestimmt. Die Verwendung oder der Erwerb dieses Produkts stellt keine Lizenzierung im Rahmen eines Patentrechts, Markenrechts oder eines anderen Rechts an geistigem Eigentum von NetApp dar.

Das in diesem Dokument beschriebene Produkt kann durch ein oder mehrere US-amerikanische Patente, ausländische Patente oder anhängige Patentanmeldungen geschützt sein.

ERLÄUTERUNG ZU „RESTRICTED RIGHTS“: Nutzung, Vervielfältigung oder Offenlegung durch die US-Regierung unterliegt den Einschränkungen gemäß Unterabschnitt (b)(3) der Klausel „Rights in Technical Data – Noncommercial Items“ in DFARS 252.227-7013 (Februar 2014) und FAR 52.227-19 (Dezember 2007).

Die hierin enthaltenen Daten beziehen sich auf ein kommerzielles Produkt und/oder einen kommerziellen Service (wie in FAR 2.101 definiert) und sind Eigentum von NetApp, Inc. Alle technischen Daten und die Computersoftware von NetApp, die unter diesem Vertrag bereitgestellt werden, sind gewerblicher Natur und wurden ausschließlich unter Verwendung privater Mittel entwickelt. Die US-Regierung besitzt eine nicht ausschließliche, nicht übertragbare, nicht unterlizenzierbare, weltweite, limitierte unwiderrufliche Lizenz zur Nutzung der Daten nur in Verbindung mit und zur Unterstützung des Vertrags der US-Regierung, unter dem die Daten bereitgestellt wurden. Sofern in den vorliegenden Bedingungen nicht anders angegeben, dürfen die Daten ohne vorherige schriftliche Genehmigung von NetApp, Inc. nicht verwendet, offengelegt, vervielfältigt, geändert, aufgeführt oder angezeigt werden. Die Lizenzrechte der US-Regierung für das US-Verteidigungsministerium sind auf die in DFARS-Klausel 252.227-7015(b) (Februar 2014) genannten Rechte beschränkt.

Markeninformationen

NETAPP, das NETAPP Logo und die unter <http://www.netapp.com/TM> aufgeführten Marken sind Marken von NetApp, Inc. Andere Firmen und Produktnamen können Marken der jeweiligen Eigentümer sein.