



Überprüfen Sie die Identität der Remoteserver mit Zertifikaten

ONTAP 9

NetApp
February 12, 2026

Inhalt

- Überprüfen Sie die Identität der Remoteserver mit Zertifikaten 1
 - Erfahren Sie mehr über die Überprüfung der Identität von Remote-Servern mithilfe von Zertifikaten in ONTAP 1
 - Überprüfen Sie die Gültigkeit digitaler Zertifikate mit OCSP in ONTAP 1
 - Standardzertifikate für TLS-basierte Anwendungen in ONTAP anzeigen 3

Überprüfen Sie die Identität der Remoteserver mit Zertifikaten

Erfahren Sie mehr über die Überprüfung der Identität von Remote-Servern mithilfe von Zertifikaten in ONTAP

ONTAP unterstützt die Funktionen für Sicherheitszertifikate zur Überprüfung der Identität von Remote-Servern.

Die ONTAP Software ermöglicht sichere Verbindungen unter Verwendung dieser digitalen Zertifikatfunktionen und -Protokolle:

- Online Certificate Status Protocol (OCSP) validiert den Status von digitalen Zertifikatsanforderungen von ONTAP-Diensten mithilfe von SSL- und TLS-Verbindungen (Transport Layer Security). Diese Funktion ist standardmäßig deaktiviert.
- Die ONTAP-Software enthält standardmäßig vertrauenswürdige Stammzertifikate.
- KMIP-Zertifikate (Key Management Interoperability Protocol) ermöglichen die gegenseitige Authentifizierung eines Clusters und eines KMIP-Servers.

Überprüfen Sie die Gültigkeit digitaler Zertifikate mit OCSP in ONTAP

Mithilfe des Online Certificate Status Protocol (OCSP) können ONTAP -Anwendungen, die TLS-Kommunikation (Transport Layer Security) verwenden, den Status digitaler Zertifikate empfangen, wenn OCSP aktiviert ist. Sie können OCSP-Zertifikatsprüfungen für bestimmte Anwendungen jederzeit aktivieren oder deaktivieren. Standardmäßig ist die Überprüfung des OCSP-Zertifikatsstatus deaktiviert.

Bevor Sie beginnen

Sie benötigen einen erweiterten Zugriff auf die Berechtigungsebene, um diese Aufgabe ausführen zu können.

Über diese Aufgabe

OCSP unterstützt folgende Anwendungen:

- AutoSupport
- Event Management System (EMS)
- LDAP über TLS
- Key Management Interoperability Protocol (KMIP)
- Audit-Protokollierung
- FabricPool
- SSH (ab ONTAP 9.13.1)

Schritte

1. Stellen Sie die Berechtigungsebene auf erweitert: `set -privilege advanced.`

2. Um OCSP-Zertifikatsprüfungen für bestimmte ONTAP-Anwendungen zu aktivieren oder zu deaktivieren, verwenden Sie den entsprechenden Befehl.

Wenn Sie möchten, dass OCSP-Zertifikatsprüfungen für einige Anwendungen...	Verwenden Sie den Befehl...
Aktiviert	<code>security config ocsp enable -app app name</code>
Deaktiviert	<code>security config ocsp disable -app app name</code>

Mit dem folgenden Befehl wird OCSP-Unterstützung für AutoSupport und EMS aktiviert.

```
cluster::*> security config ocsp enable -app asup,ems
```

Wenn OCSP aktiviert ist, erhält die Anwendung eine der folgenden Antworten:

- Gut - das Zertifikat ist gültig und die Kommunikation wird fortgesetzt.
 - Widerrufen: Das Zertifikat wird von der ausstellenden Zertifizierungsstelle dauerhaft als nicht vertrauenswürdig eingestuft und die Kommunikation kann nicht fortgesetzt werden.
 - Unbekannt – der Server verfügt über keine Statusinformationen zum Zertifikat und die Kommunikation kann nicht fortgesetzt werden.
 - OCSP-Serverinformationen fehlen im Zertifikat - der Server fungiert als deaktiviert und fährt mit der TLS-Kommunikation fort, aber es erfolgt keine Statusüberprüfung.
 - Keine Antwort vom OCSP-Server - die Anwendung schlägt fehl.
3. Verwenden Sie den entsprechenden Befehl, um OCSP-Zertifikatsprüfungen für alle Anwendungen mithilfe von TLS-Kommunikation zu aktivieren oder zu deaktivieren.

Wenn Sie möchten, dass OCSP-Zertifikatsprüfungen für alle Anwendungen durchgeführt werden...	Verwenden Sie den Befehl...
Aktiviert	<code>security config ocsp enable</code> <code>-app all</code>
Deaktiviert	<code>security config ocsp disable</code> <code>-app all</code>

Wenn alle Applikationen aktiviert sind, wird eine signierte Antwort empfangen, die angibt, dass das angegebene Zertifikat in Ordnung, annulliert oder unbekannt ist. Im Fall eines annullierten Zertifikats kann die Anwendung nicht fortgesetzt werden. Wenn die Anwendung keine Antwort vom OCSP-Server erhält oder der Server nicht erreichbar ist, wird die Anwendung nicht fortgesetzt.

4. Verwenden Sie den `security config ocsp show` Befehl, um alle Anwendungen anzuzeigen, die

OCSP unterstützen, und ihren Supportstatus.

```
cluster::*> security config ocsp show
Application                                OCSP Enabled?
-----
autosupport                                false
audit_log                                  false
fabricpool                                 false
ems                                         false
kmip                                        false
ldap_ad                                    true
ldap_nis_namemap                           true
ssh                                         true

8 entries were displayed.
```

Verwandte Informationen

- ["Sicherheitskonfiguration OCSP aktivieren"](#)
- ["Sicherheitskonfiguration OCSP deaktivieren"](#)
- ["Sicherheitskonfiguration OCSP anzeigen"](#)

Standardzertifikate für TLS-basierte Anwendungen in ONTAP anzeigen

ONTAP bietet einen Standardsatz vertrauenswürdiger Stammzertifikate für ONTAP -Anwendungen mit Transport Layer Security (TLS).

Bevor Sie beginnen

Die Standardzertifikate werden nur während der Erstellung oder während eines Upgrades auf der Admin-SVM installiert.

Über diese Aufgabe

Die aktuellen Applikationen, die als Client fungieren und eine Zertifikatvalidierung erfordern, sind AutoSupport, EMS, LDAP, Audit Logging, FabricPool, Und KMIP.

Wenn Zertifikate ablaufen, wird eine EMS-Nachricht aufgerufen, die den Benutzer zum Löschen der Zertifikate auffordert. Die Standardzertifikate können nur auf der erweiterten Berechtigungsebene gelöscht werden.



Das Löschen der Standardzertifikate kann dazu führen, dass einige ONTAP-Anwendungen nicht wie erwartet funktionieren (z. B. AutoSupport- und Audit-Protokollierung).

Schritt

1. Sie können die Standardzertifikate, die auf der Admin-SVM installiert sind, anzeigen. Verwenden Sie dazu den Befehl „Security Certificate show“:

```
security certificate show -vserver -type server-ca
```

```
cluster1::> security certificate show
```

Vserver Type	Serial Number	Certificate Name
-----------------	---------------	------------------

-----	-----	-----

vs0	4F4E4D7B	www.example.com
server		

Certificate Authority: www.example.com

Expiration Date: Thu Feb 28 16:08:28 2013

Erfahren Sie mehr über `security certificate show` in der ["ONTAP-Befehlsreferenz"](#).

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.