Der Cluster und ein KMIP-Server werden gegenseitig authentifiziert.

ONTAP 9

NetApp
November 16, 2026

This PDF was generated from https://docs.netapp.com/de-de/ontap/system-admin/mutually-authenticating-cluster-kmip-server-concept.html on November 16, 2026. Always check docs.netapp.com for the latest.

Inhalt

Der Cluster und ein KMIP-Server werden gegenseitig authentifiziert. 1
Übersicht zur gegenseitigen Authentifizierung des ONTAP Clusters und eines KMIP Servers 1
Eine Zertifikatsignierungsanforderung für den Cluster in ONTAP generieren 1
Ein von einer Zertifizierungsstelle signiertes Serverzertifikat für den ONTAP Cluster installieren 2
Ein von einer Zertifizierungsstelle signiertes Clientzertifikat für den KMIP Server in ONTAP installieren 3

Der Cluster und ein KMIP-Server werden gegenseitig authentifiziert.

Übersicht zur gegenseitigen Authentifizierung des ONTAP Clusters und eines KMIP Servers

Die gegenseitige Authentifizierung des Clusters und eines externen Schlüsselmanagers wie eines Key Management Interoperability Protocol (KMIP) Servers ermöglicht es dem Schlüsselmanager, mit dem Cluster über KMIP via SSL zu kommunizieren. Dies erfolgt, wenn eine Anwendung oder bestimmte Funktionalität (zum Beispiel die Storage Encryption Funktionalität) sichere Schlüssel benötigt, um sicheren Datenzugriff bereitzustellen.

Eine Zertifikatsignierungsanforderung für den Cluster in ONTAP generieren

Sie können den Befehl `generate-csr`security certificate verwenden, um eine Zertifikatsignierungsanforderung (CSR) zu generieren. Nach der Bearbeitung Ihrer Anforderung sendet die Zertifizierungsstelle (CA) das signierte digitale Zertifikat.

Bevor Sie beginnen

Um diese Aufgabe auszuführen, ist die Rolle als Cluster-Administrator oder SVM-Administrator erforderlich.

Schritte

1. Eine CSR generieren:

```
security certificate generate-csr -common-name <FQDN_or_common_name>
-size 512|1024|1536|2048 -country <country> -state <state> -locality
<locality> -organization <organization> -unit <unit> -email-addr
<email_of_contact> -hash-function SHA1|SHA256|MD5
```

Weitere Informationen zu `security certificate generate-csr` finden sich in der "ONTAP-Befehlsreferenz".

Der folgende Befehl erstellt eine CSR für die Softwaregruppe in der IT-Abteilung eines Unternehmens in Sunnyvale, California, USA. Die CSR hat den benutzerdefinierten Common Name server1.companyname.com und einen 2.048-Bit-Privatschlüssel, der von der SHA256 Hash-Funktion generiert wird. Die E-Mail-Adresse des SVM-Kontaktadministrators lautet web@example.com. Das System zeigt die CSR und den Privatschlüssel in der Ausgabe an.

```
cluster1::>security certificate generate-csr -common-name
server1.companyname.com -size 2048 -country US -state California -
locality Sunnyvale -organization IT -unit Software -email-addr
web@example.com -hash-function SHA256
```

```
Certificate Signing Request :
-----BEGIN CERTIFICATE REQUEST-----
<certificate_value>
-----END CERTIFICATE REQUEST-----
Private Key :
24 | Administrator Authentication and RBAC
-----BEGIN RSA PRIVATE KEY-----
<key_value>
-----END RSA PRIVATE KEY-----
Note: Please keep a copy of your certificate request and private key
for future reference.
```

2. Die Zertifikatsanforderung aus der CSR-Ausgabe wird kopiert und anschließend in elektronischer Form (z. B. per E-Mail) zur Signierung an eine vertrauenswürdige Drittzertifizierungsstelle gesendet.

   Die Zertifizierungsstelle muss das signierte Zertifikat im Base64-kodierten PEM- oder PKCS12-Format zurückgeben.

   Nach Bearbeitung Ihres Antrags sendet Ihnen die Zertifizierungsstelle das signierte digitale Zertifikat. Eine Kopie des privaten Schlüssels und des von der Zertifizierungsstelle signierten digitalen Zertifikats sollte aufbewahrt werden.

Ein von einer Zertifizierungsstelle signiertes Serverzertifikat für den ONTAP Cluster installieren

Damit ein SSL-Server das Cluster oder die Storage Virtual Machine (SVM) als SSL-Client authentifizieren kann, wird ein digitales Zertifikat mit dem Client-Typ auf dem Cluster oder der SVM installiert. Anschließend wird das Client-CA-Zertifikat dem SSL-Serveradministrator zur Installation auf dem Server bereitgestellt.

Bevor Sie beginnen

Das Stammzertifikat des SSL-Servers mit dem `server-ca` Zertifikatstyp muss bereits auf dem Cluster oder der SVM installiert sein.

Schritte

1. Um ein selbstsigniertes digitales Zertifikat für die Client-Authentifizierung zu verwenden, wird der `security certificate create` Befehl mit dem `type client` Parameter genutzt.

   Weitere Informationen zu `security certificate create` finden sich in der "ONTAP-Befehlsreferenz".

2. Zur Verwendung eines von einer Zertifizierungsstelle signierten digitalen Zertifikats für die Client-Authentifizierung sind die folgenden Schritte erforderlich:

   a. Eine digitale Zertifikatsignierungsanforderung (CSR) kann mit dem Befehl security certificate `generate-csr` generiert werden.

      ONTAP zeigt die CSR-Ausgabe an, die eine Zertifikatsanforderung und einen privaten Schlüssel enthält, und weist darauf hin, die Ausgabe zur späteren Referenz in eine Datei zu kopieren.

b. Die Zertifikatsanforderung aus der CSR-Ausgabe in elektronischer Form (z. B. per E-Mail) wird zur Signierung an eine vertrauenswürdige Zertifizierungsstelle gesendet.

   Eine Kopie des privaten Schlüssels und des von der Zertifizierungsstelle signierten Zertifikats sollte für zukünftige Zwecke aufbewahrt werden.

Nach Bearbeitung Ihres Antrags sendet Ihnen die Zertifizierungsstelle das signierte digitale Zertifikat.

a. Das CA-signierte Zertifikat wird mit dem `security certificate install` Befehl und dem `-type client` Parameter installiert.
b. Geben Sie das Zertifikat und den privaten Schlüssel ein, wenn Sie dazu aufgefordert werden, und drücken Sie anschließend die **Eingabetaste**.
c. Geben Sie bei Aufforderung alle weiteren Root- oder Zwischenzertifikate ein und drücken Sie anschließend die **Eingabetaste**.

   Sie installieren ein Zwischenzertifikat auf dem Cluster oder der SVM, wenn in der Zertifikatskette, die bei der vertrauenswürdigen Stammzertifizierungsstelle beginnt und mit dem Ihnen ausgestellten SSL-Zertifikat endet, die Zwischenzertifikate fehlen. Ein Zwischenzertifikat ist ein untergeordnetes Zertifikat, das von der vertrauenswürdigen Stammzertifizierungsstelle speziell zur Ausstellung von End-Entity-Serverzertifikaten ausgestellt wird. Das Ergebnis ist eine Zertifikatskette, die bei der vertrauenswürdigen Stammzertifizierungsstelle beginnt, über das Zwischenzertifikat verläuft und mit dem Ihnen ausgestellten SSL-Zertifikat endet.

3. Das `client-ca`Zertifikat des Clusters oder der SVM ist dem Administrator des SSL-Servers zur Installation auf dem Server bereitzustellen.

   Der Befehl „security certificate show“ mit den `-instance` und `-type client-ca` Parametern zeigt die `client-ca` Zertifikatsinformationen an.

Verwandte Informationen

- "Sicherheitszertifikat installieren"
- "Sicherheitszertifikat anzeigen"

Ein von einer Zertifizierungsstelle signiertes Clientzertifikat für den KMIP Server in ONTAP installieren

Die Typen Client-CA und Server-CA legen fest, dass das Zertifikat zur gegenseitigen Authentifizierung des Clusters und eines externen Schlüsselmanagers, wie beispielsweise eines KMIP-Servers, verwendet wird.

Über diese Aufgabe

Installieren Sie ein Zertifikat, um einen KMIP-Server als SSL-Server gegenüber dem Cluster zu authentifizieren.

Schritte

1. Verwenden Sie den `security certificate install` Befehl mit dem `-type server-ca` Parameter, um ein Zertifikat für den KMIP-Server zu installieren.
2. Wenn Sie dazu aufgefordert werden, das Zertifikat eingeben und anschließend die Eingabetaste drücken.

   ONTAP erinnert Sie daran, eine Kopie des Zertifikats für zukünftige Referenz aufzubewahren.

```
cluster1::> security certificate install -type server-ca -vserver
cluster1

Please enter Certificate: Press <Enter> when done
-----BEGIN CERTIFICATE-----
<certificate_value>
-----END CERTIFICATE-----


You should keep a copy of the CA-signed digital certificate for future
reference.

cluster1::>
```

Verwandte Informationen

- "Sicherheitszertifikat installieren"

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 IRGENDEINER 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.