



# Erstellen und Installieren eines CA-signierten Serverzertifikats

ONTAP 9

NetApp  
March 21, 2023

# Inhaltsverzeichnis

- Erstellen und Installieren eines CA-signierten Serverzertifikats ..... 1
  - Erstellen und installieren Sie eine Übersicht über ein CA-signiertes Serverzertifikat ..... 1
  - Generieren Sie eine Anforderung zum Signieren eines Zertifikats ..... 1
  - Installieren Sie ein CA-signiertes Serverzertifikat ..... 2

# Erstellen und Installieren eines CA-signierten Serverzertifikats

## Erstellen und installieren Sie eine Übersicht über ein CA-signiertes Serverzertifikat

Auf Produktionssystemen ist es eine Best Practice, ein von CA signiertes digitales Zertifikat zur Authentifizierung des Clusters oder der SVM als SSL-Server zu installieren. Sie können das verwenden `security certificate generate-csr` Befehl zum Generieren einer Zertifikatsignierungsanforderung (CSR) und des `security certificate install` Befehl zum Installieren des Zertifikats, das Sie von der Zertifizierungsstelle erhalten.

## Generieren Sie eine Anforderung zum Signieren eines Zertifikats

Sie können das verwenden `security certificate generate-csr` Befehl zum Generieren einer Zertifikatsignierungsanforderung (CSR). Nach Bearbeitung Ihrer Anfrage sendet Ihnen die Zertifizierungsstelle (CA) das signierte digitale Zertifikat.

### Was Sie benötigen

Sie müssen ein Cluster- oder SVM-Administrator sein, um diese Aufgabe durchzuführen.

### Schritte

1. CSR erstellen:

```
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
```

Mit dem folgenden Befehl wird eine CSR mit A erstellt 2048-Bit privater Schlüssel generiert durch die SHA256 Hashing-Funktion für den Einsatz durch Software Gruppe in der IT Abteilung eines Unternehmens, dessen eigener gemeinsamer Name ist `server1.companyname.com`, Befindet sich in Sunnyvale, California, USA. Die E-Mail-Adresse des SVM-Kontaktadministrators lautet `web@example.com`. Das System zeigt den CSR und den privaten Schlüssel 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-----
MIIBGjCBxQIBADBGMQwEgYDVQQDEwtleGFtcGx1LmNvbTElMAkGA1UEBhMCVVMx
CTAHBgNVBAgTADAEJMAcGA1UEBxMAMQkwBwYDVQQKEwAxCTAHBgNVBAStADEPMA0G
CSqGSIB3DQEJARYAMFwwDQYJKoZIhvcNAQEBBQADSwAwSAJBAPXFanNoJApTlnzS
xOcxixqImRRGZCR7tVmTYyqPSuTvfVtWdJbmXuj6U3a1woUsb13wfEvQnHVFNCi
2ninsJ8CAwEAAaAAMA0GCSqGSIB3DQEBCwUAA0EA6EagLfso5+4g+ejiRKKTUPQO
UqOUEoKuvxhOvPC2w7b//fNSFsFHvXloqEOhYECn/NX9h8mbphCoM5YZ4OfnKw==
-----END CERTIFICATE REQUEST-----
```

Private Key :

```
-----BEGIN RSA PRIVATE KEY-----
MIIBOwIBAAJBAPXFanNoJApTlnzSxOcxixqImRRGZCR7tVmTYyqPSuTvfVtWdJb
mXuj6U3a1woUsb13wfEvQnHVFNCi2ninsJ8CAwEAAQJAWt2AO+bW3FKezEuIrQlu
KoMyRYK455wtMk8BrOyJfhYsB20B28eifjJvRWdTOBEav99M7cEzgpV+p5kaZTTM
gQIhAPsp+j1hrUXSRj979LIJJY0sNez397i7ViFXWQScx/ehAiEA+oDbOooWlVvu
xj4aitxVBu6ByVckYU8LbsfeRNsZwD8CIQCbZ1/ENvmlJ/P7N9Exj2NCtEYxd0Q5
cwBZ5NfZeMBpwQIhAPk0KWQSLadGfsKO077itF+h9FGFNHbtuNTrVq4vPW3nAiAA
peMBQgEv28y2r8D4dkYzxcXmjzJluUSZSZ9c/wS6fA==
-----END RSA PRIVATE KEY-----
```

Note: Please keep a copy of your certificate request and private key for future reference.

2. Kopieren Sie die Zertifikatsanforderung aus der CSR-Ausgabe, und senden Sie sie in elektronischer Form (z. B. E-Mail) an eine vertrauenswürdige Drittanbieter-CA zum Signieren.

Nach Bearbeitung Ihrer Anfrage sendet Ihnen die CA das signierte digitale Zertifikat. Sie sollten eine Kopie des privaten Schlüssels und des CA-signierten digitalen Zertifikats aufbewahren.

## Installieren Sie ein CA-signiertes Serverzertifikat

Sie können das verwenden `security certificate install` Befehl zum Installieren eines CA-signierten Serverzertifikats auf einer SVM. ONTAP fordert Sie auf, die Stammzertifikate und Zwischenzertifikate der Zertifizierungsstelle (CA) anzugeben, die die Zertifikatskette des Serverzertifikats bilden.

### Was Sie benötigen

Sie müssen ein Cluster- oder SVM-Administrator sein, um diese Aufgabe durchzuführen.

## Schritt

1. Installieren eines CA-signierten Serverzertifikats: `security certificate install -vserver SVM_name -type certificate_type`

Eine vollständige Befehlsyntax finden Sie im ["Arbeitsblatt"](#).



ONTAP fordert Sie zur Eingabe der CA-Stammzertifikate und der Zwischenzertifikate auf, die die Zertifikatskette des Serverzertifikats bilden. Die Kette beginnt mit dem Zertifikat der Zertifizierungsstelle, die das Serverzertifikat ausgestellt hat, und kann bis zum Stammzertifikat der Zertifizierungsstelle reichen. Fehlende Zwischenzertifikate führen zum Ausfall der Serverzertifikatinstallation.

Mit dem folgenden Befehl wird das CA-signierte installiert `server` Zertifikat und Zwischenzertifikate auf der `SVMengData2`.

```
cluster1::>security certificate install -vserver engData2 -type server
Please enter Certificate: Press <Enter> when done
-----BEGIN CERTIFICATE-----
MIIB8TCCAZugAwIBAwIBADANBgkqhkiG9w0BAQQFADBfMRMwEQYDVQQDEwpuZXRh
cHAuY29tMQswCQYDVQQGEwJVUzEJMAcGA1UECBMAMQkwBwYDVQQHEwAxCTAHBGNV
BAoTADAJMAcGA1UECzMAMQ8wDQYJKoZIhvcNAQkBFgAwHhcNMTAwNDI2MTk0OTI4
WhcNMTAwNTI2MTk0OTI4WjBfMRMwEQYDVQQDEwpuZXRhcHAuY29tMQswCQYDVQQG
EwJVUzEJMAcGA1UECBMAMQkwBwYDVQQHEwAxCTAHBGNVBAoTADAJMAcGA1UECzMA
MQ8wDQYJKoZIhvcNAQkBFgAwXDANBgkqhkiG9w0BAQEFAANLADBIAkEAyXrK2sry
-----END CERTIFICATE-----

Please enter Private Key: Press <Enter> when done
-----BEGIN RSA PRIVATE KEY-----
MIIBPAIBAAJBAM16ytrK8nQj82UsWeHOeT8gk0BPX+Y5MLyCsUdXA7hXhumHNpvF
C61X2G32Sx8VEa1th94tx+vOEzq+UaqH1t0CAwEAAQJBAMZjDWlgmlm3qIr/n8VT
PFnnZnbVcXVM70tbUsgPKw+QCCh9dF1jmuQKeDr+wUMWkn1DeGrfhILpzfJGHRlJ
z7UCIQDr8d3gOG71UyX+BbFmo/N0uAKjS2cvUU+Y8a8pDxGLLwIhANqa99SuS18U
DiPvdaKTj6+EcGuXfCXz+G0rfgTZK8uzAiEArlmnrFYC8KwE9k7A0y1RzBLdUwK9
AvuJDn+/z+H1Bd0CIQDD93P/xpaJETNz53Au49VE5Jba/Jugckrbosd/lSd7nQIq
aEMAZt6qHHT4mndi8Bo8sDGedG2SKx6Qbn2IpuNZ7rc=
-----END RSA PRIVATE KEY-----

Do you want to continue entering root and/or intermediate certificates
{y|n}: y

Please enter Intermediate Certificate: Press <Enter> when done
-----BEGIN CERTIFICATE-----
MIIE+zCCBGsgAwIBAgICAQ0wDQYJKoZIhvcNAQEFBQAwwgsxJDAiBgNVBACGTG1Zh
bG1DZXJ0IFZhbG1kYXRpb24gTmV0d29yazEXMBUGA1UEChMOVmFsaUNlcnQsIElu
Yy4xNTAzBgNVBAsTTFZhbG1DZXJ0IENsYXNzIDIGUG9saWN5IFZhbG1kYXRpb24g
QXV0aG9yaXR5MSEwHwYDVQQDEwExodHRwOi8vd3d3LnZhbG1jZXJ0LmNvbS8xIDAe
```

```
BgkqhkiG9w0BCQEWluZm9AdmFsaWNlcnQuY29tMB4XDTA0MDYyOTE3MDYyMFoX
DTI0MDYyOTE3MDYyMFowYzELMAkGA1UEBhMCVVMxITAfBgNVBAoTGFROZSBHbyBE
YWRkeSBHcm91cCwgSW5jLjExMC8GA1UECXMOR28gRGFkZHKgQ2xhc3MgMiBDZXJ0
-----END CERTIFICATE-----
```

Do you want to continue entering root and/or intermediate certificates  
{y|n}: y

Please enter Intermediate Certificate: Press <Enter> when done

```
-----BEGIN CERTIFICATE-----
MIIC5zCCAlACAQEwDQYJKoZIhvcNAQEFBQAwbgsxJDAiBgNVBACtG1ZhbG1DZXJ0
IFZhbG1kYXRpb24gTmV0d29yazEXMBUGA1UEChMOVmFsaUNlcnQsIEluYy4xNTAz
BgNVBAsTTFZhbG1DZXJ0IENsYXNzIDIGUG9saWN5IFZhbG1kYXRpb24gQXV0aG9y
aXR5MSEwHwYDVQQDEzhodHRwOi8vd3d3LnZhbG1jZXJ0LmNvbS8xIDAeBgkqhkiG
9w0BCQEWluZm9AdmFsaWNlcnQuY29tMB4XDk5MDYyNjAwMTk1NFoXDTE5MDYy
NjAwMTk1NFowgsxJDAiBgNVBACtG1ZhbG1DZXJ0IFZhbG1kYXRpb24gTmV0d29y
azEXMBUGA1UEChMOVmFsaUNlcnQsIEluYy4xNTAzBgNVBAsTTFZhbG1DZXJ0IENs
YXNzIDIGUG9saWN5IFZhbG1kYXRpb24gQXV0aG9yaXR5MSEwHwYDVQQDEzhodHRw
-----END CERTIFICATE-----
```

Do you want to continue entering root and/or intermediate certificates  
{y|n}: n

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

## Copyright-Informationen

Copyright © 2023 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtinhabers 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, BEISPIELHAFT 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.