Konfigurieren des signierten Zertifikats der CA über die CLI im Cisco Voice Operating System (VOS)

Inhalt

Einführung

In diesem Dokument werden Konfigurationsschritte zum Hochladen eines Zertifikats der Zertifizierungsstelle (Certificate Authority, CA) eines Drittanbieters auf einen Collaboration-Server mit Cisco Voice Operating System (VOS) mithilfe der Befehlszeilenschnittstelle (CLI) beschrieben.

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- Grundlegende Kenntnisse der Public Key Infrastructure (PKI) und ihrer Implementierung auf Cisco VOS-Servern und Microsoft CA
- DNS-Infrastruktur ist vorkonfiguriert

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- VOS-Server: Cisco Unified Communications Manager (CUCM) Version 9.1.2
- CA: Windows 2012-Server
- Client-Browser: Mozilla Firefox, Version 47.0.1

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Hintergrundinformationen

Bei allen Cisco Unified Communications VOS-Produkten gibt es mindestens zwei Berechtigungsarten: Anwendungsart (ccmadmin, ccmservice, cuadmin, cfadmin, cuic) und VOS-Plattform (cmplattform, drf, cli).

In bestimmten Szenarien ist es sehr praktisch, Anwendungen über die Webseite zu verwalten und plattformbezogene Aktivitäten über die Befehlszeile auszuführen. Unten finden Sie eine Prozedur zum Importieren von Zertifikaten von Drittanbietern nur über CLI. In diesem Beispiel wird das Tomcat-Zertifikat hochgeladen. Für CallManager oder eine andere Anwendung sieht sie gleich aus.

Signiertes CA-Zertifikat generieren

Befehlsübersicht

Eine Liste der im Artikel verwendeten Befehle.

```
show cert list own
show cert own tomcat

set csr gen CallManager
show csr list own
show csr own CallManager

show cert list trust
set cert import trust CallManager
set cert import own CallManager CallManager-trust/allevich-DC12-CA.pem
```

Überprüfen der korrekten Zertifikatinformationen

Listen Sie alle hochgeladenen vertrauenswürdigen Zertifikate auf.

```
admin:show cert list own

tomcat/tomcat.pem: Self-signed certificate generated by system
ipsec/ipsec.pem: Self-signed certificate generated by system
CallManager/CallManager.pem: Certificate Signed by allevich-DC12-CA
```

```
CAPF/CAPF.pem: Self-signed certificate generated by system
TVS/TVS.pem: Self-signed certificate generated by system
```

Überprüfen Sie, wer das Zertifikat für den Dienst Tomcat ausgestellt hat.

```
admin:show cert own tomcat

[
  Version: V3
  Serial Number: 859978324705545211023663245198594366 90
  SignatureAlgorithm: SHA1withRSA (1.2.840.113549.1.1.5)
  Issuer Name: L=Krakow, ST=Malopolskie, CN=ucm1-1.allevich.local, OU=TAC, O=Cisco, C=PL
  Validity From: Sun Jul 31 11:37:17 CEST 2016
           To:   Fri Jul 30 11:37:16 CEST 2021
  Subject Name: L=Krakow, ST=Malopolskie, CN=ucm1-1.allevich.local, OU=TAC, O=Cisco, C=PL
  Key: RSA (1.2.840.113549.1.1.1)
    Key value: 3082010a0282010100a2
<output omited>
```

Dies ist ein selbstsigniertes Zertifikat, da der Emittent dem Betreff entspricht.

Erstellen einer Zertifikatssignaturanfrage (Certificate Sign Request, CSR)

CSR erstellen

```
admin:set csr gen tomcat
Successfully Generated CSR  for tomcat
```

Überprüfen Sie, ob die Anforderung für das Zertifikatszeichen erfolgreich erstellt wurde.

```
admin:show csr list own
tomcat/tomcat.csr
```

Öffnen Sie die Datei, und kopieren Sie den Inhalt in die Textdatei. Speichern Sie die Datei als Datei **tac_tomcat.csr**.

```
admin:show csr own tomcat

-----BEGIN CERTIFICATE REQUEST-----
MIIDSjCCAjICAQAwgb0xCzAJBgNVBAYTAlBMMRQwEgYDVQQIEwtNYWxvcG9sc2tp
ZTEPMA0GA1UEBxMGS3Jha293MQ4wDAYDVQQKEwVDaXNjbzEMMAoGA1UECxMDVEFD
MR4wHAYDVQQDExV1Y20xLTEuYWxsZXZpY2gubG9jYWwxSTBHBgNVBAUTQDlhMWJk
NDA5M2VjOGYxNjljODhmNGUyZTYwZTYzM2RjNjlhZmFkNDY1YTgzMDhkNjRhNGU1
MzExOGQ0YjZkZjcwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCVo5jh
lMqTUnYbHQUnYPt00PTflWbj7hi6PSYI7pVCbGUZBpIZ5PKwTD56OZ8SgpjYX5Pf
l9D09H2gtQJTMVv1Gm1eGdlJsbuABRKn6lWkO6b706MiGSgqel+41vnItjn3Y3kU
7h51nruJye3HpPQzvXXpOKJ/JeJc8InEvQcC/UQmFMKn0ulO0veFBHnG7TLDwDaQ
W1Al1rwrezN9Lwn2a/XZQR1P65sjmnkFFF2/FON4BmooeiiNJD0G+F4bKig1ymlR
84faF27plwHjcw8WAn2HwJT6O7TaE6EOJd0sgLU+HFAI3txKycS0NvLuMZYQH81s
/C74CIRWibEWT2qLAgMBAAGgRzBFBgkqhkiG9w0BCQ4xODA2MCcGA1UdJQQgMB4G
CCsGAQUFBwMBBggrBgEFBQcDAgYIKwYBBQUHAwUwCwYDVR0PBAQDAgO4MA0GCSqG
SIb3DQEBBQUAA4IBAQBUu1FhKuyQ1X58A6+7KPkYsWtioS0PoycltuQsVo0aav82
PiJkCvzWTeEo6v9qG0nnaI53e15+RPpWxpEgAIPPhtt6asDuW30SqSx4eClfgmKH
ak/tTuWmZbfyk2iqNFy0YgYTeBkG3AqPwWUCNoduPZ0/fo41QoJPwjE184U64WXB
gCzhIHfsV5DzYp3IR5C13hEa5fDgpD2ubQWja2LId85NGHEiqyiWqwmt07pTkBc+
7ZKa6fKnpACehrtVqEn02jOi+sanfQKGQqH8VYMFsW2uYFj9pf/Wn4aDGuJoqdOH
StV2Eh0afxPEq/1rQP3/rzq4NMYlJ7glyNFGPUVP
```

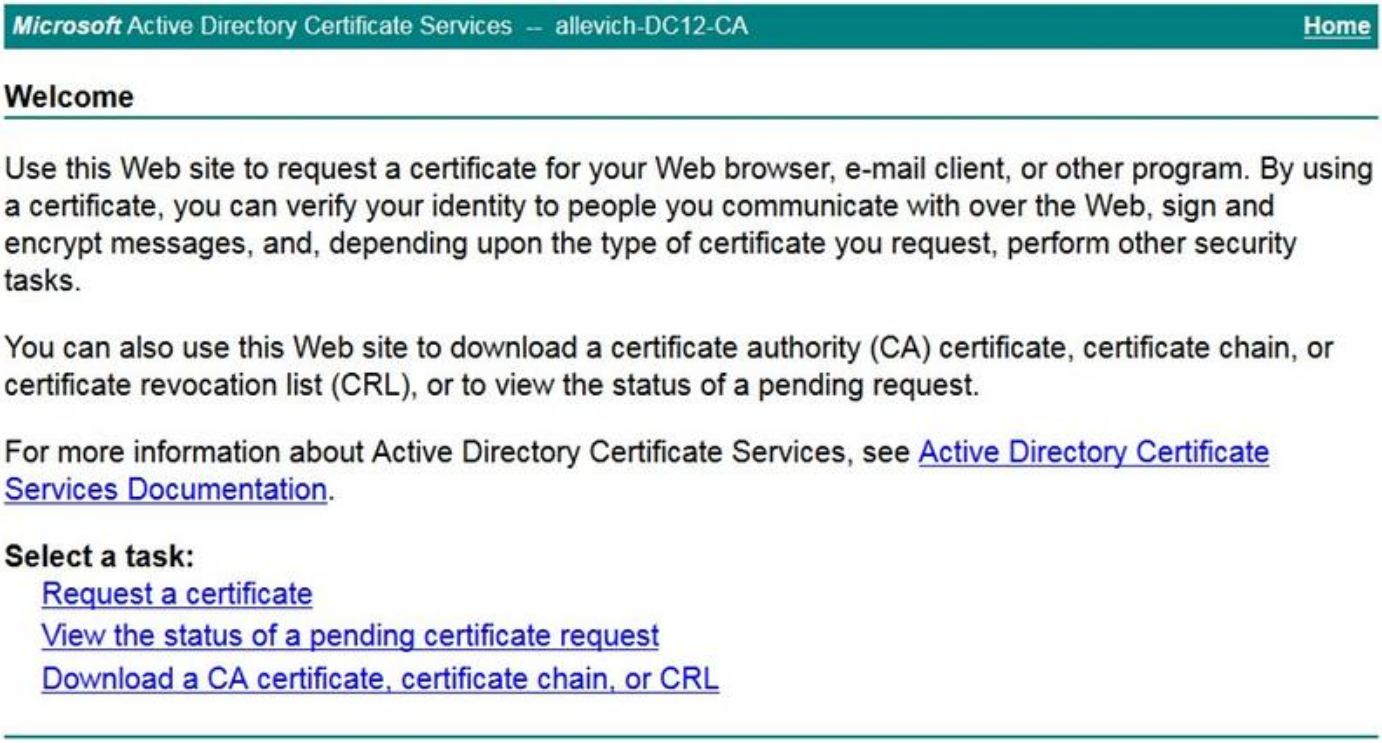
```
-----END CERTIFICATE REQUEST-----
```

Tomcat-Serverzertifikat erstellen

Generieren Sie ein Zertifikat für den Tomcat-Dienst auf der CA.

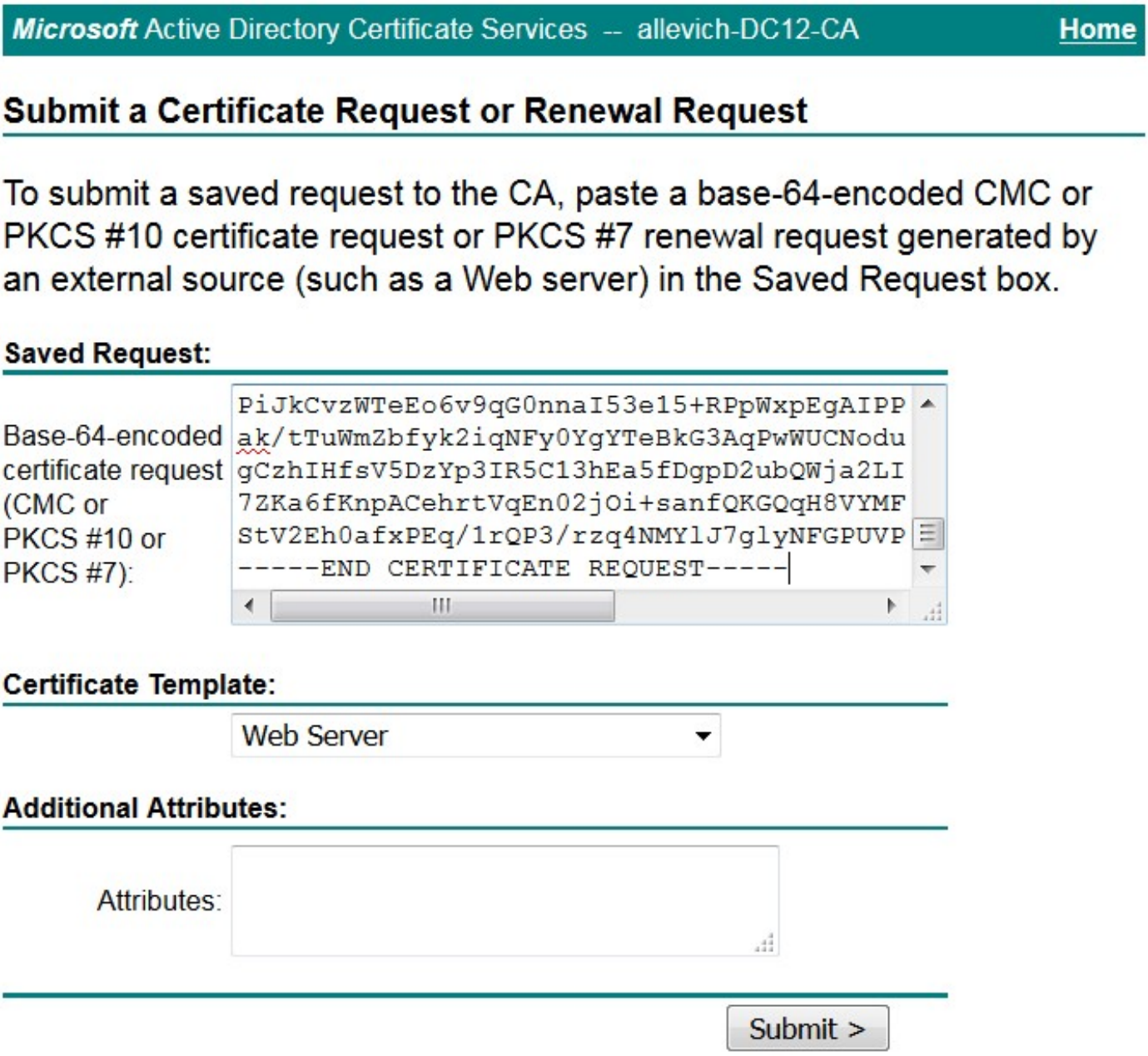
Öffnen Sie die Webseite für die Zertifizierungsstelle in einem Browser. Geben Sie die richtigen Anmeldeinformationen in die Authentifizierungsanzeige ein.

http://dc12.allevich.local/certsrv/



Laden Sie das CA-Stammzertifikat herunter. Wählen Sie **Zertifikat, Zertifikatskette oder CRL-**Menü **herunterladen aus**. Wählen Sie im nächsten Menü die richtige CA aus der Liste aus. Die Verschlüsselungsmethode sollte **Base 64** sein. Laden Sie das Zertifizierungsstellenzertifikat herunter, und speichern Sie es im Betriebssystem mit dem Namen **ca.cer**.

Drücken Sie **Zertifikat anfordern** und anschließend **Erweiterte Zertifikatsanforderung**. Legen Sie **Zertifikatsvorlage** auf Webserver fest, und fügen Sie den CSR-Inhalt aus der Textdatei **tac_tomcat.csr** wie gezeigt ein.



> **Tipp**: Wenn der Vorgang im Labor (oder im Cisco VOS-Server und der CA unter derselben administrativen Domäne) durchgeführt wird, sparen Sie Zeit, kopieren Sie den CSR und fügen Sie ihn aus dem Speicherpuffer ein.

Drücken Sie **Senden**. Wählen Sie **Base 64-verschlüsselte** Option aus, und laden Sie das Zertifikat für den Tomcat-Dienst herunter.

> **Hinweis**: Wenn die Zertifikatgenerierung in loser Schüttung durchgeführt wird, stellen Sie sicher, dass der Name des Zertifikats in einen sinnvollen Namen geändert wird.

Importieren des Tomcat-Zertifikats in den Cisco VOS-Server

CA-Zertifikat importieren

Öffnen Sie das Zertifizierungsstellenzertifikat, das mit dem Namen **ca.cer** gespeichert wurde. Sie

muss zuerst importiert werden.

Kopieren Sie den Inhalt in den Puffer, und geben Sie den folgenden Befehl in die CUCM-CLI ein:

```
admin:set cert import trust tomcat

Paste the Certificate and Hit Enter
```

Eine Aufforderung zum Einfügen des Zertifizierungsstellenzertifikats wird angezeigt. Fügen Sie es wie unten gezeigt ein.

```
-----BEGIN CERTIFICATE-----
MIIDczCCAlugAwIBAgIQEZg1rT9fAL9B6HYkXMikITANBgkqhkiG9w0BAQUFADBM
MRUwEwYKCZImiZPyLGQBGRYFbG9jYWwxGDAWBgoJkiaJk/IsZAEZFghhbGxldmlj
aDEZMBcGA1UEAxMQYWxsZXZpY2gtREMxMi1DQTAeFw0xNjA1MDExNzUxNTlaFw0y
MTA1MDExODAxNTlaMEwxFTATBgoJkiaJk/IsZAEZFgVsb2NhbDEYMBYGCgmSJomT
8ixkARkWCGFsbGV2aWNoMRkwFwYDVQQDExBhbGxldmljaC1EQzEyLUNBMIIBIjAN
BgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAoL2ubJJOgyTX2X4zhmZs+fOZz7SF
O3GReUavF916UZ/CSP49EgHcuYw58846uxZw6bcjgwsaE+oMQD2EYHKZmQAALwxv
ERVfyc5kS6EM7oR6cwOnK5piZOUORzq/Y7teinF91wtOSJOR6ap8aEC3Bfr23SIN
bDJXMB5KYw68MtoebhiDYxExvY+XYREoqSFC4KeRrpTmuy7VfGPjv0clwmfm0/Ir
MzYtkAILcfvEVduz+KqZdehuwYWAIQBhvDszQGW5aUEXj+07GKRiIT9vaPOt6TBZ
g78IKQoXe6a8Uge/1+F9VlFvQiG3AeqkIvD/UHrZACfASp8t+csGnr3vQIDAQAB
o1EwTzALBgNVHQ8EBAMCAYYwDwYDVR0TAQH/BAUwAwEB/zAdBgNVHQ4EFgQUr1sv
r5HPbDhDGoSN5EeU7upV9iQwEAYJKwYBBAGCNxUBBAMCAQAwDQYJKoZIhvcNAQEF
BQADggEBABfguqa6swmmXpStXdg0mPuqE9mnWQTPnWx91SSKyyY3+icHaUlXgW/9
WppSfMajzKOueWelzDOwsBk17CYEAiT6SGnak8/+Yz5NCY4fOowl7OvRz9jP1iOO
Zd9eowH6fgYw6+M5zsLvBB3SFGatKgUrpB9rExaWOtsZHCF5mrd13vl+BmpBxDCz
FuzSFfyxuMzOXkJPmH0LByBUw90h4s6wJgJHp9B0f6J5d9ES7PkzHuKVtIxvioHa
Uf1g9jqOqoe1UXQh+09uZKOi62gfkBcZiWkHaP0OmjOQCbSQcSLLMTJoRvLxZKNX
jzqAOylrPEYgvQFrkH1Yvo8fotXYw5A=
-----END CERTIFICATE-----
```

Wenn der Upload eines Vertrauenszertifikats erfolgreich ist, wird diese Ausgabe angezeigt.

```
Import of trust certificate is successful
```

Überprüfen Sie, ob das Zertifizierungsstellenzertifikat erfolgreich als Tomcat-trust1 importiert wurde.

```
admin:show cert list trust

tomcat-trust/ucm1-1.pem: Trust Certificate
tomcat-trust/allevich-win-CA.pem: w2008r2 139
<output omited for brevity>
```

Tomcat-Zertifikat importieren

Der nächste Schritt besteht darin, ein signiertes Tomcat CA-Zertifikat zu importieren. Die Operation sieht genauso aus wie bei tomcat-trust cert, nur der Befehl ist anders.

```
set cert import own tomcat tomcat-trust/allevich-DC12-CA.pem
```

Starten Sie den Dienst neu

Und zuletzt starten Sie den Tomcat-Dienst neu.

```
utils service restart Cisco Tomcat
```

> **Vorsicht**: Beachten Sie, dass dies den Betrieb von webserverabhängigen Diensten wie Extension Mobility, Verpasste Anrufe, Corporate Directory und anderen stört.

Überprüfen

Überprüfen Sie das erstellte Zertifikat.

```
admin:show cert own tomcat

[
  Version: V3
  Serial Number: 276529240473076562022540660071542142548731496 5
  SignatureAlgorithm: SHA1withRSA (1.2.840.113549.1.1.5)
  Issuer Name: CN=allevich-DC12-CA, DC=allevich, DC=local
  Validity From: Sun Jul 31 12:17:46 CEST 2016
           To:   Tue Jul 31 12:17:46 CEST 2018
  Subject Name: CN=ucm1-1.allevich.local, OU=TAC, O=Cisco, L=Krakow, ST=Malopolskie, C=PL
  Key: RSA (1.2.840.113549.1.1.1)
    Key value: 3082010a028201010095a
```

Stellen Sie sicher, dass der Name des Emittenten der Zertifizierungsstelle angehört, die das Zertifikat erstellt hat.

Melden Sie sich bei der Webseite an, indem Sie FQDN des Servers in einem Browser eingeben. Es wird keine Zertifikatswarnung angezeigt.

Fehlerbehebung

Ziel dieses Artikels ist es, eine Prozedur mit Befehlssyntax zum Hochladen des Zertifikats über die CLI zu geben, nicht die Logik der Public Key Infrastructure (PKI) hervorzuheben. SAN-Zertifikat, nachrangige CA, Länge des Zertifikats 4096 und viele andere Szenarien werden nicht abgedeckt.

In seltenen Fällen schlägt der Vorgang beim Hochladen eines Webserverzertifikats über die CLI fehl und es wird die Fehlermeldung "CA-Zertifikat kann nicht gelesen werden" angezeigt. Eine Problemumgehung hierfür ist die Installation des Zertifikats über die Webseite.

Eine nicht standardmäßige Konfiguration der Zertifizierungsstelle kann zu einem Problem bei der Zertifikatinstallation führen. Versuchen Sie, das Zertifikat von einer anderen Zertifizierungsstelle mit einer Standardkonfiguration zu generieren und zu installieren.

Zurück-Plan

Falls ein selbst signiertes Zertifikat generiert werden muss, kann dies auch in der CLI erfolgen.

Geben Sie den folgenden Befehl ein, und das Tomcat-Zertifikat wird auf das selbstsignierte Zertifikat regeneriert.

```
admin:set cert regen tomcat

WARNING: This operation will overwrite any CA signed certificate previously imported for  tomcat

Proceed with regeneration (yes|no)? yes
Successfully Regenerated Certificate for tomcat.

You must restart services related to tomcat for the regenerated certificates to become active.
```

Um ein neues Zertifikat anzuwenden, muss der Tomcat-Dienst neu gestartet werden.

```
admin:utils service restart Cisco Tomcat

 Don't press Ctrl-c while the service is getting RESTARTED.If Service has not Restarted
Properly, execute the same Command Again

Service Manager is running
Cisco Tomcat[STOPPING]
Cisco Tomcat[STOPPING]
Commanded Out of Service
Cisco Tomcat[NOTRUNNING]
Service Manager is running
Cisco Tomcat[STARTING]
Cisco Tomcat[STARTING]
Cisco Tomcat[STARTED]
```

Verwandte Artikel

Zertifikat über Webseite hochladen

Verfahren zum Abrufen und Hochladen von selbstsignierten Windows-Servern oder Zertifizierungsstelle (Certificate Authority, CA) ...