Upload de Root and Intermediate Certificates of Expressway-Core op CUCM

Inhoud

Inleiding

Dit document beschrijft hoe de root- en tussentijdse certificaten die het Expessway-C-certificaat hebben ondertekend aan de CUCM-uitgever kunnen worden geüpload als 'link-trust' en als 'callmanager-trust'.

Vanwege verbeteringen in de verkeersserverservice op expressway in X14.0.2 stuurt Expressway-C het client-certificaat wanneer een server (CUCM) ernaar vraagt, voor diensten die op andere poorten dan 8443 lopen (bijvoorbeeld 6971.6972), zelfs als CUCM zich in een niet-veilige modus bevindt. Vanwege deze verandering is vereist dat het certificaat dat de expressway-C ondertekende certificaatautoriteit (CA) in CUCM wordt toegevoegd, zowel als als "link-trust" en "callmanager-trust".

Het niet uploaden van CA, dat expressway-C tekent op CUCM, veroorzaakt MRA-inloggen om te falen na een upgrade van expressways naar X14.0.2 of hoger. In de pakketvastlegging tussen Expressway-C en CUCM ziet u CUCM een 'Onbekende CA' TLS-fout naar Expressway-C verzenden.

Voorwaarden

Achtergrondinformatie

Om CUCM het certificaat te kunnen vertrouwen dat Expressway-C verstuurt, moet het in staat zijn om een link te leggen van dat certificaat naar een hoogste certificeringsinstantie (root) waarop het vertrouwen heeft. Zo een link, een hiërarchie van certificaten die een certificaat van een entiteit aan een certificaat van de wortel van CA verbinden, wordt een keten van vertrouwen genoemd. Om een dergelijke vertrouwensketen te kunnen verifiëren, bevat elk certificaat twee velden : afgevende instantie (of "afgegeven door") en onderwerp (of "afgegeven door").

servercertificaten, zoals degene die Expressway-C naar CUCM stuurt, hebben in het veld "Onderwerp" doorgaans hun FQDN in de GN (gezamenlijke naam):

```
Issuer: DC=lab, DC=vngtp, CN=vngtp-ACTIVE-DIR-CA
Subject: C=BE, ST=Flamish-Brabant, L=Diegem, O=Cisco, OU=TAC, CN=vcs-c1.vngtp.lab
```

Voorbeeld van een servercertificaat voor Expressway vcs-c1.vngtp.lab. Het heeft de FQDN in de GN-eigenschap van het onderwerpveld samen met andere kenmerken zoals het land (C), staat (ST), locatie (L), ... We kunnen ook zien dat het servercertificaat wordt afgegeven (afgegeven) door een CA genaamd vngtp-ACTIVE-DIR-CA (vngtp-ACTIVE-DIR-CA.vngtp.lab).

CA's op topniveau (root CA's) kunnen ook een certificaat afgeven om zichzelf te identificeren. In een dergelijk basiscertificaat van CA zien we dat de uitgevende instelling en het onderwerp dezelfde waarde hebben:

```
Issuer:  DC=lab, DC=vngtp, CN=vngtp-ACTIVE-DIR-CA
Subject: DC=lab, DC=vngtp, CN=vngtp-ACTIVE-DIR-CA
```

In dit certificaat hebben de uitgevende instelling en de onderwerpvelden dezelfde waarde. Het is een certificaat dat wordt afgegeven door een bron-CA om zichzelf te identificeren.

In een typische situatie, geven de wortel CAs niet direct servercertificaten uit. In plaats daarvan geven zij certificaten af voor andere CA's. Zulke andere CA's worden dan intermediaire CA's genoemd. Intermediate CA's kunnen op hun beurt direct servercertificaten of certificaten voor andere intermediaire CA's uitgeven. We kunnen een situatie hebben waarin een servercertificaat wordt afgegeven door tussenpersoon CA 1, die op zijn beurt een certificaat krijgt van tussenpersoon CA 2 enzovoort. Tot eindelijk CA haar certificaat rechtstreeks uit CA krijgt:

```
Server certificate :
Issuer: DC=lab, DC=vngtp, CN=vngtp-intermediate-CA-1 Subject: C=BE, ST=Flamish-Brabant,
L=Diegem, O=Cisco, OU=TAC, CN=vcs-c1.vngtp.lab
Intermediate CA 1 certificate :
Issuer: DC=lab, DC=vngtp, CN=vngtp-intermediate-CA-2
Subject: DC=lab, DC=vngtp, CN=vngtp-intermediate-CA-1
Intermediate CA 2 certificate :
Issuer: DC=lab, DC=vngtp, CN=vngtp-intermediate-CA-3
Subject: DC=lab, DC=vngtp, CN=vngtp-intermediate-CA-2
...
Intermediate CA n certificate :
Issuer: DC=lab, DC=vngtp, CN=vngtp-ACTIVE-DIR-CA
Subject: DC=lab, DC=vngtp, CN=vngtp-intermediate-CA-n
Root CA certificate :
Issuer: DC=lab, DC=vngtp, CN=vngtp-ACTIVE-DIR-CA
Subject: DC=lab, DC=vngtp, CN=vngtp-ACTIVE-DIR-C
```

Nu, om CUCM het servercertificaat te kunnen vertrouwen dat Expressway-C verstuurt, moet het in staat zijn om de vertrouwensketen van dat servercertificaat op te bouwen tot een basis-CA-certificaat. Daarvoor moeten we het CA-basiscertificaat uploaden, en ook alle tussenliggende CA-certificaten (indien er een is, wat niet het geval is als de CA-wortel direct het server-certificaat van Expressway-C zou hebben afgegeven) in de vertrouwenslijst van CUCM.

> **Opmerking: Hoewel de kwesties van de uitgevende instelling en de onderwerpvelden gemakkelijk de vertrouwensketen op een voor de mens leesbare manier kunnen opbouwen, gebruiken Expressway-C en CUCM deze velden niet in het certificaat. In plaats daarvan gebruiken ze de velden 'X509v3 Authority Key Identifier' en 'X509v3 subject Key Identifier' om de vertrouwensketen op te bouwen. Deze sleutels bevatten identificatiegegevens voor de certificaten die nauwkeuriger zijn dan het gebruik van de velden Onderwerp/uitgevende instelling: er kunnen twee certificaten worden afgegeven met hetzelfde vak van Onderwerp/uitgevende instelling, maar één daarvan is verlopen en één van de certificaten is**

nog geldig. Ze zouden beide een andere X509v3 subject Key identifier hebben, zodat Expressway/CUCM nog steeds de juiste vertrouwensketen kan bepalen.

Configuratie

Stap 1: Ontvang de wortel en de tussenhandelcertificaten die het certificaat van de autosnelweg-C server ondertekenden

Als goed gebruik, toen u het servercertificaat aanvankelijk van een CA (root CA of intermediaire CA) kreeg die dat servercertificaat ondertekende, kreeg u ook de root en intermediaire certificaten voor dat servercertificaat en bewaarde ze ergens op een veilige plaats. Als dit probleem zich voordoet, kunt u deze wortel- en intermediaire certificaten verkrijgen en naar stap 2 gaan waar u instructies kunt vinden hoe u deze op CUCM kunt uploaden.

Als u de goede praktijk niet volgde om uw wortel/intermedate certs ergens veilig op te slaan, kunnen we ze van de Expressway-C krijgen omdat u ze daar ook geüpload had voordat u het servercertificaat uploadde. De eerste stap is om te kijken wat we precies nodig hebben. Hiervoor navigeer in de sneltoets Expressway-C naar Onderhoud > Security > Server certificaat en klik of selecteer de knop 'Show (gedecodeerd)' naast 'Server certificaat'. Dit opent een nieuw venster/tabblad met de inhoud van het sneltoets-C servercertificaat. We zoeken het veld 'Problemen' daar:

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            55:00:00:02:21:bb:2d:41:60:55:d7:b2:27:00:01:00:00:02:21
    Signature Algorithm: sha256WithRSAEncryption
        Issuer: O=DigiCert Inc, CN=DigiCert Global CA-1
        Validity
            Not Before: Dec  8 10:36:57 2021 GMT
            Not After : Dec  8 10:36:57 2023 GMT
        Subject: C=BE, ST=Flamish-Brabant, L=Diegem, O=Cisco, OU=TAC, CN=vcs-c1.vngtp.lab
        Subject Public Key Info:
...
```

Ons snelservercertificaat wordt afgegeven door een Organisatie DigiCert Inc met de gebruikelijke naam 'DigiCert Global CA-1'.

We gaan nu naar Onderhoud > Beveiliging > Vertrouwde CA-certificaat en kijken in de lijst als we daar een certificaat hebben met exact dezelfde waarde (O=DigiCert Inc., CN=DigiCert Global CA-1) in het veld Onderwerp.

	Type	Issuer	Subject
☐	Certificate	CN=vngtp-ACTIVE-DIR-CA	Matches Issuer
☐	Certificate	O=IdenTrust, CN=IdenTrust Commercial Root CA 1	Matches Issuer
☐	Certificate	O=Baltimore, OU=CyberTrust, CN=Baltimore CyberTrust Root	Matches Issuer
☐	Certificate	O=DigiCert Inc, OU=www.digicert.com, CN=DigiCert Global Root CA	Matches Issuer
☐	Certificate	O=The Go Daddy Group, Inc., OU=Go Daddy Class 2 Certification Authority	Matches Issuer
☐	Certificate	O=GoDaddy.com, Inc., CN=Go Daddy Root Certificate Authority - G2	Matches Issuer
☐	Certificate	O=QuoVadis Limited, CN=QuoVadis Root CA 2	Matches Issuer
☐	Certificate	O=thawte, Inc., OU=Certification Services Division, OU=(c) 2006 thawte, Inc. - For authorized use only, CN=thawte Primary Root CA	Matches Issuer
☐	Certificate	O=VeriSign, Inc., OU=VeriSign Trust Network, OU=(c) 2006 VeriSign, Inc. - For authorized use only, CN=VeriSign Class 3 Public Primary Certification Authority - G5	Matches Issuer
☐	Certificate	O=DigiCert Inc, OU=www.digicert.com, CN=DigiCert Global Root CA	O=DigiCert Inc, CN=DigiCert Global CA-1

Show all (decoded) | Show all (PEM file) | Delete | Select all | Unselect all

Express Trust Store

We zien inderdaad dat er een certificaat is in de express-C trust store met een onderwerp dat identiek is aan de 'uitgever' van het expressway-C-servercertificaat. Dat certificaat (de laatste in de lijst zoals in de afbeelding getoond) wordt afgegeven door O=DigiCert Inc., OU=www.digicert.com, CN=DigiCert Global Root CA. Dit is anders dan het "Onderwerp", dus we weten dat dit geen basiscertificaat is, maar een tussencertificaat van CA.

> **Opmerking: Als u geen certificaat in die lijst ziet met een 'Onderwerp' dat overeenkomt met de 'Uitgever' van ons certificaat van snelweg C, kijk dan naar de kolom 'Uitgever' in de lijst en kijk of u daar een match kunt vinden. Als dat het geval is en in de kolom "Onderwerp" staat "Matches Issuer" voor dat certificaat, betekent dit dat er een basiscertificaat is dat ons certificaat van de expressway-C server meteen heeft ondertekend, zonder tussenliggende CA.**

Nadat we het tussentijdse certificaat hebben gevonden, zijn we nog niet klaar. We moeten helemaal naar het wortelcertificaat. We moeten dus het certificaat van de CA vinden dat het intermediaire CA-certificaat heeft afgegeven met onderwerp O=DigiCert Inc, CN=DigiCert Global CA-1. We weten dat de CA die dit certificaat heeft afgegeven O=DigiCert Inc. OU=www.digicert.com, CN=DigiCert Global Root CA is. Aangezien we geen match zien voor deze CA in de Onderwerp kolom, kijken we in de kolom van de uitgevende instelling en zien we inderdaad een match: het vierde certificaat in de lijst heeft een uitgever O=DigiCert Inc., OU=www.digicert.com, CN=DigiCert Global Root CA en omdat het "Onderwerp" zegt "Matches Issuer" weten we dat dit het basiscertificaat van CA is.

Conclusie: ons certificaat van de Expressway-C server is ondertekend door CA=DigiCert Inc., CN=DigiCert Global CA-1 dat op zijn beurt werd ondertekend door root CA=DigiCert Inc., OU=www.digicert.com, CN=DigiCert Global Root CA.

Klik op of selecteer de knop 'Alles weergeven (PEM-bestand)' onder de lijst om het basiscertificaat en het intermedate certificaat te verkrijgen. Dit toont u alle wortel en intermediaire certificaten in PEM formaat. Scrolt naar het 4de en laatste certificaat en kopieer de inhoud. Het 4de certificaat is onze basis-CA cert:

```
...
Epn3o0WC4zxe9Z2etiefC7IpJ5OCBRLbf1wbWsaY71k5h+3zvDyny67G7fyUIhz
```

```
ksLi4xaNmjICq44Y3ekQEe5+NauQrz4wlHrQMz2nZQ/1/I6eYs9HRCwBXbsdtTLS
R9I4LtD+gdwyah617jzV/OeBHRnDJELqYzmp -----END CERTIFICATE----- O=DigiCert Inc, CN=DigiCert
Global Root CA -----BEGIN CERTIFICATE-----
MIIDrzCCApegAwIBAgIQCDvgVpBCRrGhdWrJWZHHSjANBgkqhkiG9w0BAQUFADBh
MQswCQYDVQQGEwJVUzEVMBMGA1UEChMMRGlnaUNlcnQgSW5jMRkwFwYDVQQLExB3
d3cuZGlnaWNlcnQuY29tMSAwHgYDVQQDExdEaWdpQ2VydCBHbG9iYWwgUm9vdCBD
QTAeFw0wNjExMTAwMDAwMDBaFw0zMTExMTAwMDAwMDBaMGExCzAJBgNVBAYTAlVT
MRUwEwYDVQQKEwxEaWdpQ2VydCBJbmMxGTAXBgNVBAsTEHd3dy5kaWdpY2VydC5j
b20xIDAeBgNVBAMTF0RpZ2lDZXJ0IEdsb2JhbCBSb290IENBMIIBIjANBgkqhkiG
9w0BAQEFAAOCAQ8AMIIBCgKCAQEA4jvhEXLeqKTTo1eqUKKPC3eQyaKl7hLOllsB
CSDMAZOnTjC3U/dDxGkAV53ijSLdhwZAAIEJzs4bg7/fzTtxRuLWZscFs3YnFo97
nh6Vfe63SKMI2tavegw5BmV/Sl0fvBf4q77uKNd0f3p4mVmFaG5cIzJLv07A6Fpt
43C/dxC//AH2hdmoRBBYMql1GNXRor5H4idq9Joz+EkIYIvUX7Q6hL+hqkpMfT7P
T19sdl6gSzeRntwi5m3OFBqOasv+zbMUZBfHWymeMr/y7vrTC0LUq7dBMtoM1O/4
gdW7jVg/tRvoSSiicNoxBN33shbyTApOB6jtSj1etX+jkMOvJwIDAQABo2MwYTAO
BgNVHQ8BAf8EBAMCAYYwDwYDVR0TAQH/BAUwAwEB/zAdBgNVHQ4EFgQUA95QNVbR
TLtm8KPiGxvDl7I90VUwHwYDVR0jBBgwFoAUA95QNVbRTLtm8KPiGxvDl7I90VUw
DQYJKoZIhvcNAQEFBQADggEBAMucN6pIExIK+t1EnE9SsPTfrgT1eXkIoyQY/Esr
hMAtudXH/vTBH1jLuG2cenTnmCmrEbXjcKChzUyImZOMkXDiqw8cvpOp/2PV5Adg
06O/nVsJ8dWO41P0jmP6P6fbtGbfYmbW0W5BjfIttep3Sp+dWOIrWcBAI+0tKIJF
PnlUkiaY4IBIqDfv8NZ5YBberOgOzW6sRBc4L0na4UU+Krk2U886UAb3LujEV0ls
YSEY1QSteDwsOoBrp+uvFRTp2InBuThs4pFsiv9kuXclVzDAGySj4dzp30d8tbQk
CAUw7C29C79Fv1C5qfPrmAESrciIxpg0X40KPMbp1ZWVbd4= -----END CERTIFICATE----- O=The Go Daddy Group,
Inc. -----BEGIN CERTIFICATE-----
MIIEADCCAuigAwIBAgIBADANBgkqhkiG9w0BAQUFADBjMQswCQYDVQQGEwJVUzEh
MB8GA1UEChMYVGhlIEdvIERhZGR5IEdyb3VwLCBJbmMuMTEwLwYDVQQLEyhHbyBE
...
```

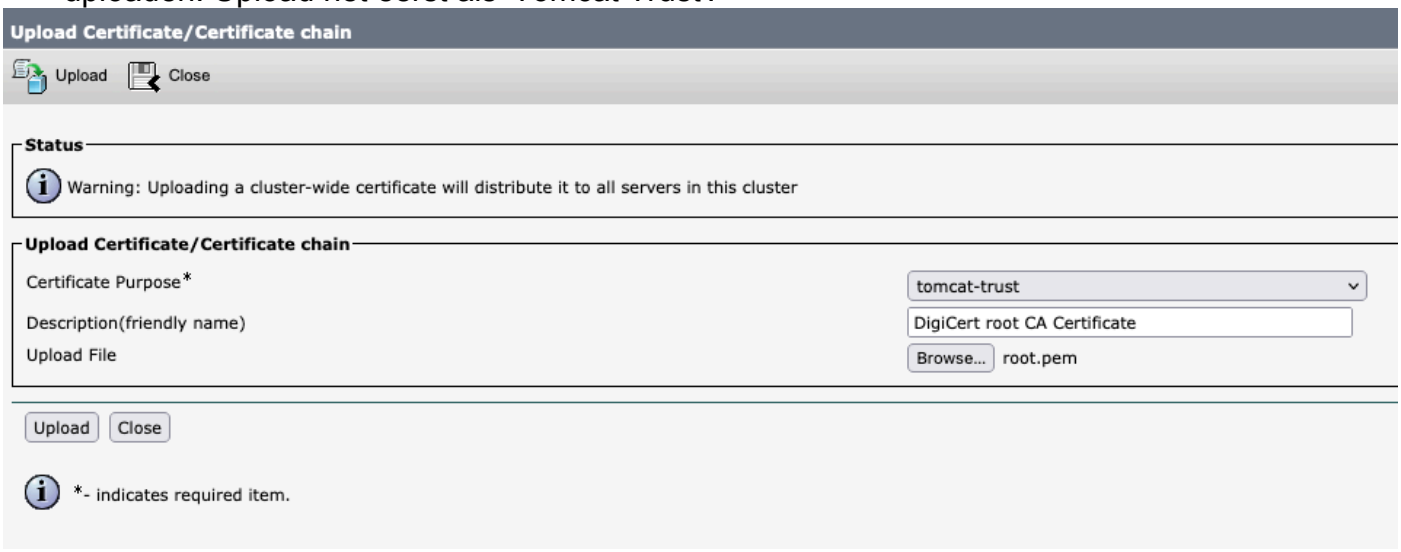
Voor elk van de wortel en de uiteindelijke intermediaire certificaten kopieert u alles dat begint met '—BEGIN CERTIFICAAT—' en eindigt met (inbegrepen) '—EINDCERTIFICAAT—'. Plaats elk ervan in een afzonderlijk tekstbestand en voeg 1 extra lege regel onderaan toe (na de regel met —EINDCERTIFICAAT—). Sla deze bestanden op met de bestandsextensie .pem: root.pem, intermediair1.pem, intermediair2.pem, ... U hebt een afzonderlijk bestand nodig voor elk wortel-/tussencertificaat. Bijvoorbeeld, ons root.pem bestand zou bevatten:

```
-----BEGIN CERTIFICATE-----
MIIDrzCCApegAwIBAgIQCDvgVpBCRrGhdWrJWZHHSjANBgkqhkiG9w0BAQUFADBh
MQswCQYDVQQGEwJVUzEVMBMGA1UEChMMRGlnaUNlcnQgSW5jMRkwFwYDVQQLExB3
d3cuZGlnaWNlcnQuY29tMSAwHgYDVQQDExdEaWdpQ2VydCBHbG9iYWwgUm9vdCBD
QTAeFw0wNjExMTAwMDAwMDBaFw0zMTExMTAwMDAwMDBaMGExCzAJBgNVBAYTAlVT
MRUwEwYDVQQKEwxEaWdpQ2VydCBJbmMxGTAXBgNVBAsTEHd3dy5kaWdpY2VydC5j
b20xIDAeBgNVBAMTF0RpZ2lDZXJ0IEdsb2JhbCBSb290IENBMIIBIjANBgkqhkiG
9w0BAQEFAAOCAQ8AMIIBCgKCAQEA4jvhEXLeqKTTo1eqUKKPC3eQyaKl7hLOllsB
CSDMAZOnTjC3U/dDxGkAV53ijSLdhwZAAIEJzs4bg7/fzTtxRuLWZscFs3YnFo97
nh6Vfe63SKMI2tavegw5BmV/Sl0fvBf4q77uKNd0f3p4mVmFaG5cIzJLv07A6Fpt
43C/dxC//AH2hdmoRBBYMql1GNXRor5H4idq9Joz+EkIYIvUX7Q6hL+hqkpMfT7P
T19sdl6gSzeRntwi5m3OFBqOasv+zbMUZBfHWymeMr/y7vrTC0LUq7dBMtoM1O/4
gdW7jVg/tRvoSSiicNoxBN33shbyTApOB6jtSj1etX+jkMOvJwIDAQABo2MwYTAO
BgNVHQ8BAf8EBAMCAYYwDwYDVR0TAQH/BAUwAwEB/zAdBgNVHQ4EFgQUA95QNVbR
TLtm8KPiGxvDl7I90VUwHwYDVR0jBBgwFoAUA95QNVbRTLtm8KPiGxvDl7I90VUw
DQYJKoZIhvcNAQEFBQADggEBAMucN6pIExIK+t1EnE9SsPTfrgT1eXkIoyQY/Esr
hMAtudXH/vTBH1jLuG2cenTnmCmrEbXjcKChzUyImZOMkXDiqw8cvpOp/2PV5Adg
06O/nVsJ8dWO41P0jmP6P6fbtGbfYmbW0W5BjfIttep3Sp+dWOIrWcBAI+0tKIJF
PnlUkiaY4IBIqDfv8NZ5YBberOgOzW6sRBc4L0na4UU+Krk2U886UAb3LujEV0ls
YSEY1QSteDwsOoBrp+uvFRTp2InBuThs4pFsiv9kuXclVzDAGySj4dzp30d8tbQk
CAUw7C29C79Fv1C5qfPrmAESrciIxpg0X40KPMbp1ZWVbd4=
-----END CERTIFICATE-----
```

(Merk op dat er 1 lege regel onderaan staat)

Stap 2: Upload de bron en tussenliggende (indien aanwezig) certificaten op CUCM

- Meld u aan op de Cisco Unified OS-beheerpagina van uw CUCM Publisher
- Navigeren in naar beveiliging > certificaatbeheer
- Klik of selecteer de knop "Upload certificaatketting/certificaat".
- Start in het nieuwe venster het root.pem-certificaat dat u uit Stap 1 hebt ontvangen te uploaden. Upload het eerst als 'Tomcat Trust':



- Klik op of selecteer de knop 'Upload' en vervolgens moet u 'Success' zien: Certificaat geüpload". Negeer de boodschap over het opnieuw opstarten van Tomcat voor nu.
- Upload hetzelfde root.pem-bestand nu als 'CallManager-trust' voor het 'certificaatdoel'.
- Herhaal eerdere stappen (uploaden als 'vertrouwen-in' en 'CallManager-Vertrouwen') voor alle intermediaire certificaten die u hebt.

Stap 3: De gewenste services op CUCM herstarten

Deze services moeten opnieuw worden gestart op elk CUCM-knooppunt in uw CUCM-cluster:

- Cisco CallManager
- Cisco TFTP
- Cisco Tomcat

De eerste 2 we kunnen opnieuw starten vanaf de Cisco Unified Services-pagina's van CUCM:

- Inloggen op de Cisco Unified Service pagina van uw CUCM Publisher
- Navigeren in naar Gereedschappen > Control Center - Functieservices
- Selecteer uw uitgever als server
- Selecteer de optie 'Cisco CallManager' en klik op de knop 'Herstart'
- Nadat de Cisco CallManager-service opnieuw is gestart, selecteert u de optie 'Cisco TFTP'-service en klikt u op de knop 'Herstart'.
- Wacht tot de Cisco TFTP-service opnieuw is gestart
- Herhaal eerdere stappen voor elk van uw uitgevers

Cisco Tomcat kan alleen vanaf CLI opnieuw starten:

- Open een opdrachtregel-verbinding met uw CUCM-uitgever
- Gebruik de opdracht: **utist-service opnieuw opstarten, Cisco Tomcat**
- Herhaal eerdere stappen op elk van uw abonneeknooppunten