Telefoons tussen beveiligde clusters migreren

Inhoud

Inleiding

Dit document beschrijft hoe u telefoons kunt migreren tussen twee beveiligde Cisco Unified Communications Manager (CUCM)-clusters.

Bijgedragen door David Norman, Cisco TAC Engineer.

Voorwaarden

Vereisten

Cisco raadt u aan kennis te hebben over CUCM.

Gebruikte componenten

De informatie in dit document is gebaseerd op deze softwareversies:

Broncluster: CUCM versie 10.5.2.1900-3
Bestemmingscluster: CUCM versie 11.0.1.1000-10
8861 telefoon met firmware Sp88xx.10-3-1-20

CTL-bestanden (certificaatlijst) worden getekend met het CallManager-certificaat (niet USB-token)

Achtergrond

Tijdens het migratieproces probeert de telefoon een beveiligde verbinding naar de bronclusters van Cisco Trust Verification Service (TVS) in te stellen om de doelclusters van CallManager-certificaat te verifiëren. Als het ITL-bestand van de certificaat lijst (CTL) en Identity Trust List (ITL) van de telefoon ongeldig zijn, kan de telefoon de beveiligde handdruk niet met de TVS voltooien en zal de migratie naar de doelcluster niet slagen. Voordat u het proces van de telefoonmigratie start, bevestig dat de telefoons het juiste CTL/ITL bestand geïnstalleerd hebben. Bevestig ook in het broncluster dat de ondernemingsoptie "Cluster voor terugdraaiing naar Pre 8.0 voorbereiden" op False is ingesteld.

Configureren

Importeer het certificaat van de doelclusters CallManager in de bronclusters CallManager-trust en de telefoon-SAST-trustwinkel. Er zijn twee methoden om dit te doen.

Methode 1.

Gebruik het Bulk certificaatgereedschap en vul deze stappen in op zowel de bron als de doelclusters.

Stap 1. Navigeer naar **Cisco Unified OS-**beheerpagina > **Beveiliging** > **Bulk certificaatbeheer** op zowel bron- als doelclusters.

Stap 2. Voer de gegevens in voor de Secure File Transfer Protocol (SFTP) server en selecteer **Opslaan**.

Stap 3. Selecteer **Exporteren** en exporteer het Trivial File Transfer Protocol (TFTP)-certificaat.

Stap 4. Klik op de knop **Consolidate** om de certificatenconsolidatie uit te voeren. Dit maakt een PKCS12-bestand dat zowel het bron- als het doelcertificaat CallManager bevat.

Stap 5. Importeer de geconsolideerde certificaten terug in elk cluster.

Tijdens het consolidatieproces (stap 5) Het certificaat van de bronclusters CallManager wordt geüpload naar de doelcluster in de winkel CallManager-trust en Phone-SAST-trust. Hiermee kunnen de telefoons terugmigreren naar het broncluster. Als de handmatige methode wordt gevolgd, wordt het certificaat van de bronclusters CallManager niet worden geüpload naar het doelcluster. Dit betekent dat u de telefoons niet naar het broncluster kunt migreren. Als u de optie wilt om de telefoons terug naar de broncluster te migreren, wilt u moet het certificaat van de bronclusters CallManager aan de bestemmingsclusters CallManager-Vertrouwen en de telefoon-SAST-trustwinkel uploaden.

> Opmerking: Beide clusters moeten het TFTP-certificaat naar dezelfde SFTP-server en dezelfde SFTP-folder exporteren.

> Opmerking: Stap 4 is alleen vereist voor één cluster. Als u telefoons tussen CUCM versie 8.x of 9.x naar CUCM versie 10.5.2.1390-12 of nieuwer migreert, neem dan nota van dit Cisco bug-ID CSCuy43181 voordat u de certificaten consolideert.

Methode 2.

Importeer de certificaten handmatig. Voltooi deze stappen in het doelcluster.

Stap 1. Navigeer naar **Cisco Unified OS-**pagina > **Security** > **certificaatbeheer**.

Stap 2. Selecteer het CallManager.pem-certificaat en download het.

Stap 3. Selecteer het certificaat van ITLrecovery.pem en download het

Stap 4 . Upload het certificaat CallManager aan de uitgever van de broncluster als CallManager-

trust en telefoon-SAST-trustcertificaat.

Stap 5. Upload het ITL-terugwinningscertificaat naar het broncluster als telefoon-SAST-Trust

Stap 6. Start TVS opnieuw in alle knooppunten van de broncluster.

Dan repliceren de certificaten naar de andere knooppunten in de cluster.

De stappen 3, 5, 6 zullen op scenario's van het migreren van telefoon van 8.x tot 12.x van toepassing zijn

> Opmerking: Het certificaat CallManager moet worden gedownload van alle knooppunten die de TFTP-service in de doelcluster uitvoeren.

Nadat de certificaten met een van de bovenstaande methoden zijn geüpload, wijzigt u de optie 150 van de Dynamic Host Configuration Protocol (DHCP) van de telefoons om naar het doelclusters TFTP-adres te wijzen.

> **Voorzichtig:** Eén methode om telefoons tussen niet-beveiligde clusters te migreren is om de "heersende cluster voor terugrol aan pre 8.0" op True op de broncluster in te stellen en de telefoons opnieuw op te starten. Dit is geen optie als je telefoons tussen veilige clusters migreert. Dit komt doordat het terugdraaien naar pre 8.0 optie alleen het ITL bestand onvolledig maakt (het heeft het CTL bestand niet leeg). Dit betekent dat wanneer de telefoon wordt gemigreerd en het CTL bestand uit de doelcluster wordt gedownload, het de nieuwe CTL met de bronclusters TVS moet verifiëren. Aangezien het ITL-bestand van de telefoon niet het TVS-certificaat van de bronclusters bevat, mislukt de handdruk wanneer de telefoon probeert een beveiligde verbinding naar de TVS-service in te stellen.

Verifiëren

Dit is een fragment uit de logboeken van de telefoonconsole en de TVS loggen (ingesteld op gedetailleerd) van de broncluster. De fragmenten tonen het proces van de telefoonregistratie aan de doelcluster.

1. De telefoon start en downloads van het CTL-bestand vanuit het doelcluster.

```
3232 NOT Nov 29 06:33:59.011270 downd-DDFORK - execing [/usr/sbin/dgetfile][-L620][ ]
3233 NOT Nov 29 06:33:59.033132 dgetfile(870)-GETXXTP
[GT870][src=CTLSEPB000B4BA0AEE.tlv][dest=/tmp/CTLFile.tlv][serv=][serv6=][sec=0]
```

2. Het CTL-bestand wordt getekend door het bestemmingspluikerscertificaat dat niet in het bestaande CTL- of ITL-bestand staat. Dit betekent dat de telefoon zijn TVS-dienst moet bereiken om het certificaat te controleren. Op dit punt heeft de telefoon nog zijn oude configuratie die het IP adres van de bron cluster TVS-service bevat (de TVS die in de configuratie van de telefoons worden gespecificeerd is hetzelfde als de groep van de telefoonaanroep). De telefoon stelt een SSL verbinding met de TVS dienst in. Wanneer de TVS-dienst zijn certificaat aan de telefoon presenteert, verifieert de telefoon het certificaat aan de hand van het certificaat in zijn ITL-bestand. Als ze hetzelfde zijn, wordt de handdruk voltooid.

```
3287 INF Nov 29 06:33:59.395199 SECUREAPP-Attempting connect to TVS server addr [192.168.11.32],
mode [IPv4]
3288 INF Nov 29 06:33:59.395294 SECUREAPP-TOS set to [96] on sock, [192.168.11.32][11]
3289 INF Nov 29 06:33:59.396011 SECUREAPP-TCP connect() successful, [192.168.11.32] [11]
3290 DEB Nov 29 06:33:59.396111 SECUREAPP-BIO created with: addr:192.168.11.32, port:2445,
mode:IPv4
3291 INF Nov 29 06:33:59.396231 SECUREAPP-Sec SSL Connection - TVS.
3292 INF Nov 29 06:33:59.396379 SECUREAPP-SSL session setup - Requesting Cert
3293 DEB Nov 29 06:33:59.396402 SECUREAPP-Obtaining certificate.
3294 INF Nov 29 06:33:59.396444 SECUREAPP-SSL session setup - Get Active cert ok
3295 DEB Nov 29 06:33:59.396464 SECUREAPP-SSL session setup - cert len=785, type=LSC
3296 DEB Nov 29 06:33:59.396854 SECUREAPP-Certificate subject name = /serialNumber=PID:CP-8861
SN:FCH18198CNQ/C=AU/O=stormin/OU=IST/CN=CP-8861-SEPB000B4BA0AEE
3297 DEB Nov 29 06:33:59.396917 SECUREAPP-SSL session setup - Certificate issuer name =
/C=AU/O=stormin/OU=IST/CN=CAPF-a7fb32bf/ST=NSQ/L=Sydney
3298 INF Nov 29 06:33:59.396947 SECUREAPP-SSL session setup - Requesting Pkey
3299 INF Nov 29 06:33:59.397024 SECUREAPP-SSL session setup - Get private key ok
3300 DEB Nov 29 06:33:59.397045 SECUREAPP-SSL session setup - key len=1191
3301 INF Nov 29 06:33:59.399181 SECUREAPP-Setup SSL session - SSL use certificate okay
3302 INF Nov 29 06:33:59.399477 SECUREAPP-Setup SSL session - SSL use private key okay
3303 DEB Nov 29 06:33:59.399974 SECUREAPP-Sec SSL Connection - Added SSL connection handle
0x40e01270, connDesc 11 to table.
3304 DEB Nov 29 06:33:59.400225 SECUREAPP-Sec SSL Connection - check status & perform handshake.
3305 DEB Nov 29 06:33:59.401086 SECUREAPP-Blocked TVS Secure Connection - Waiting (0) ....
3306 DEB Nov 29 06:33:59.401796 SECUREAPP-Sec SSL Connection - check status & perform handshake.
3307 DEB Nov 29 06:33:59.403321 SECUREAPP-SSL session setup Cert Verification - Role is = 21
3308 INF Nov 29 06:33:59.403412 SECUREAPP-SSL session setup Cert Verification - Invoking
certificate validation helper plugin.
3309 INF Nov 29 06:33:59.403662 SECUREAPP-SSL session setup Cert Verification - Certificate
validation helper plugin returned.
3310 INF Nov 29 06:33:59.403731 SECUREAPP-SSL session setup Cert Verification - Certificate is
valid.
3311 DEB Nov 29 06:33:59.403784 SECUREAPP-SSL session setup Cert Verification - returning
validation result = 1
3312 ERR Nov 29 06:33:59.428892 downd-SOCKET accept errno=4 "Interrupted system call"
3313 DEB Nov 29 06:33:59.907337 SECUREAPP-Blocked TVS Secure Connection - Waiting (1) ....
3314 DEB Nov 29 06:33:59.907393 SECUREAPP-Sec SSL Connection - check status & perform handshake.
3315 NOT Nov 29 06:33:59.908586 SECUREAPP-Sec SSL Connection - Handshake successful.
3316 INF Nov 29 06:33:59.908696 SECUREAPP-Sec SSL Connection - caching disabled, session not
saved
3317 DEB Nov 29 06:33:59.908752 SECUREAPP-Connection to server succeeded
```

3. Het TVS-logbestand laat de inkomende verbinding via de telefoon zien en de handdruk was geslaagd.

```
18:01:05.333 | debug Accepted TCP connection from socket 0x00000012, fd = 8
18:01:05.333 | debug Total Session attempted = 7 accepted = 7
18:01:05.334 | debug tvsGetNextThread
18:01:05.334 | debug Recd event
18:01:05.334 | debug new ph on fd 8
18:01:05.334 | debug 7:UNKNOWN:Got a new SCB from RBTree
18:01:05.334 | debug ipAddrStr (Phone) 192.168.11.100
18:01:05.334 | debug 8:UNKNOWN:Got a new ph conn 192.168.11.100 on 8, Total Acc = 7..
18:01:05.334 | debug addded 8 to readset
18:01:05.338 | debug after select, 8 was set
18:01:05.338 | debug ipAddrStr (Phone) 192.168.11.100
18:01:05.855 | debug tvsSSLHandShakeNotify
18:01:05.855 | debug 192.168.11.100: tvsSSLHandShake Session ciphers - AES256-SHA
18:01:05.855 | debug addded 8 to readset
```

```
18:01:05.855 | debug Recd event
18:01:05.855 | debug TLS HS Done for ph_conn
```

4. De logbestanden van de telefoonconsole tonen dat de telefoon een verzoek naar de TVS-service stuurt om het certificaat van de CallManager uit de doelgroep te controleren.

```
3318 DEB Nov 29 06:33:59.908800 SECUREAPP-TVS provider Init - connect returned TVS srvr sock: 11
3319 DEB Nov 29 06:33:59.908848 SECUREAPP-TVS process request - processing TVS Query Certificate
request.
3320 NOT Nov 29 06:33:59.909322 SECUREAPP-TVS process request - Successfully sent the TVS
request to TVS server, bytes written : 153
3321 DEB Nov 29 06:33:59.909364 SECUREAPP-==== TVS process request - request byte dump ====, len
= 153
3322 DEB Nov 29 06:33:59.913075 SECUREAPP-TVS Service receives 1480 bytes of data
3323 DEB Nov 29 06:33:59.913270 SECUREAPP-==== TVS process response - response byte dump ====,
len = 1480
3324 DEB Nov 29 06:33:59.914466 SECUREAPP-Found the work order from pending req list element at
index 0
```

5. De TVS-stamboeken tonen aan dat het verzoek is ontvangen.

```
18:01:06.345 | debug 8:UNKNOWN:Incoming Phone Msg:
HEX_DUMP: Len = 153:
18:01:06.345 | debug 57 01 03 00 00 00 03 e9
18:01:06.345 | debug 00 8f 01 00 18 01 43 50
18:01:06.345 | debug 2d 38 38 36 31 2d 53 45
18:01:06.345 | debug 50 42 30 30 30 42 34 42
18:01:06.345 | debug 41 30 41 45 45 03 00 42
18:01:06.345 | debug 43 4e 3d 75 63 6d 31 31
18:01:06.345 | debug 70 75
18:01:06.345 | debug tvsPhoneDecodeMsg -
Decoded Phone Msg:
18:01:06.345 | debug Protocol Discriminator: 57
18:01:06.345 | debug MsgType : TVS_MSG_QUERY_CERT_REQ
18:01:06.345 | debug Session Id : 0
18:01:06.345 | debug Length : 143
18:01:06.345 | debug 8:UNKNOWN:TVS CORE: Rcvd Event: TVS_EV_QUERY_CERT_REQ in State:
TVS_STATE_AWAIT_REQ
18:01:06.345 | debug tvsHandleQueryCertReq
18:01:06.345 | debug tvsHandleQueryCertReq : Subject Name is:
CN=ucm11pub.stormin.local;OU=IST;O=Stormin;L=Brisbane;ST=QLD;C=AU
18:01:06.345 | debug tvsHandleQueryCertReq : Issuer Name is: CN=stormin-WIN2012-CA
18:01:06.345 | debug tvsHandleQueryCertReq : Serial Number is:
24000000179479B8F124AC3F3B000000000017
18:01:06.345 | debug CertificateDBCache::getCertificateInformation - Looking up the certificate
cache using Unique MAP ID : 24000000179479B8F124AC3F3B000000000017CN=stormin-WIN2012-CA
18:01:06.345 | debug CertificateDBCache::getCertificateInformation - Found entry {rolecount : 2}
18:01:06.345 | debug CertificateDBCache::getCertificateInformation - {role : 0}
18:01:06.346 | debug CertificateDBCache::getCertificateInformation - {role : 3}
18:01:06.346 | debug convertX509ToDER -x509cert : 0xbb696e0
```

6. De TVS-documenten bevatten het certificaat in de winkel en TVS stuurt een reactie op de telefoon.

```
18:01:06.346 | debug 8:UNKNOWN:Sending QUERY_CERT_RES msg
18:01:06.346 | debug tvsPhoneDecodeMsg -
Decoded Phone Msg:
18:01:06.346 | debug Protocol Discriminator: 57
18:01:06.346 | debug MsgType : TVS_MSG_QUERY_CERT_RES
18:01:06.346 | debug Session Id : 0
18:01:06.346 | debug Length : 1470
18:01:06.346 | debug ReasonInfo : 00$
18:01:06.346 | debug Number of Certs : 1
18:01:06.346 | debug Cert[0] :
18:01:06.346 | debug Cert Type : 0
HEX_DUMP: Len = 1451:
18:01:06.346 | debug 30 82 05 a7 30 82 04 8f
18:01:06.346 | debug a0 03 02 01 02 02 13 24
18:01:06.346 | debug 00 00 00 17 94 79 b8 f1
18:01:06.346 | debug 24 ac 3f 3b 00 00 00 00
18:01:06.346 | debug 00 17 30 0d 06 09 2a 86
18:01:06.346 | debug 48 86 f7 0d 01 01 0b 05
18:01:06.346 | debug 00 30
18:01:06.346 | debug Version : 0
18:01:06.346 | debug PublicKey :
HEX_DUMP: Len = 4:
18:01:06.347 | debug 00 01 51 80
18:01:06.347 | debug Sending TLS Msg ..
HEX_DUMP: Len = 1480:
18:01:06.347 | debug 57 01 04 f7 00 00 03 e9
18:01:06.347 | debug 05 be 07 00 01 00 02 05
18:01:06.347 | debug ab 30 82 05 a7 30 82 04
18:01:06.347 | debug 8f a0 03 02 01 02 02 13
18:01:06.347 | debug 24 00 00 00 17 94 79 b8
18:01:06.347 | debug f1 24 ac 3f 3b 00 00 00
18:01:06.347 | debug 00 00
18:01:06.347 | debug ipAddrStr (Phone) 192.168.11.100
```

7. De logbestanden van de telefoonconsole tonen aan dat het certificaat met succes is geverifieerd en dat het CTL-bestand is bijgewerkt.

```
3325 INF Nov 29 06:33:59.915121 SECUREAPP-TVS added cert to TVS cache - expires in 24 hours
3333 NOT Nov 29 06:34:00.411671 SECUREAPP-Hashes match... authentication successful.
3334 WRN Nov 29 06:34:00.412849 SECUREAPP-AUTH: early exit from parser loop; old version header?
3335 WRN Nov 29 06:34:00.412945 SECUREAPP-AUTH: hdr ver 1.2 (knows only upto 1.1)
3336 NOT Nov 29 06:34:00.413031 SECUREAPP-updateFromFile: TL parse to table: CTL_SUCCESS
3337 NOT Nov 29 06:34:00.413088 SECUREAPP-updateFromFile: Updating master TL table
3338 DEB Nov 29 06:34:00.413442 SECUREAPP-TL file verified successfully.
3339 INF Nov 29 06:34:00.413512 SECUREAPP-TL file updated.
```

8. De telefoonconsole toont wanneer de telefoon zijn ITL-bestand downloads.

```
3344 NOT Nov 29 06:34:00.458890 dgetfile(877)-GETXXTP
[GT877][src=ITLSEPB000B4BA0AEE.tlv][dest=/tmp/ITLFile.tlv][serv=][serv6=][sec=0]
3345 NOT Nov 29 06:34:00.459122 dgetfile(877)-In normal mode, call - > makeXXTPrequest (V6...)

3281 NOT Dec 14 06:34:00.488697 dgetfile(851)-XXTP complete - status = 100
3282 NOT Dec 14 06:34:00.488984 dgetfile(851)-XXTP actualserver [192.168.11.51]
```

9. Het ITL-bestand wordt tegen het CTL-bestand geverifieerd. Het CTL-bestand bevat het doelclusters CallManager-certificaat. Dit betekent dat de telefoon het certificaat kan verifiëren zonder contact op te nemen met de bron clusters TVS service.

```
3287 NOT Nov 29  06:34:00.499372 SECUREAPP-Hashes match... authentication successful.
3288 WRN Nov 29  06:34:00.500821 SECUREAPP-AUTH: early exit from parser loop; old version
header?
3289 WRN Nov 29 06:34:00.500987 SECUREAPP-AUTH: hdr ver 1.2 (knows only upto 1.1)
3290 NOT Nov 29  06:34:00.501083 SECUREAPP-updateFromFile: TL parse to table: CTL_SUCCESS
3291 NOT Nov 29  06:34:00.501147 SECUREAPP-updateFromFile: Updating master TL table
3292 DEB Nov 29  06:34:00.501584 SECUREAPP-TL file verified successfully.
3293 INF Nov 29  06:34:00.501699 SECUREAPP-TL file updated.
```

Problemen oplossen

Controleer voor het migratieproces het CTL/ITL op de telefoons. Klik hier voor meer informatie over het controleren van de CTL/ITL: https://www.cisco.com/c/en/us/support/docs/voice-unified-communications/unified-communications-manager-callmanager/116232-technote-sbd-00.html#anc9