Migrazione di telefoni tra cluster protetti

Sommario

Introduzione

In questo documento viene descritto come eseguire la migrazione di telefoni tra due cluster sicuri di Cisco Unified Communications Manager (CUCM).

Contributo di David Norman, Cisco TAC Engineer.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza di CUCM.

Componenti usati

Le informazioni di questo documento si basano sulle seguenti versioni software:

Cluster di origine: CUCM versione 10.5.2.1900-3
Cluster di destinazione: CUCM versione 11.0.1.10000-10
telefono 8861 con firmware sip88xx.10-3-1-20

I file dell'elenco di certificati attendibili (CTL) sono firmati con il certificato CallManager (non con token USB)

Sfondo

Durante il processo di migrazione, il telefono tenta di configurare una connessione sicura ai cluster di origine Cisco Trust Verification Service (TVS) per verificare il certificato CallManager dei cluster di destinazione. Se il file dell'elenco di certificati attendibili (CTL) e dell'elenco di certificati attendibili (ITL) del telefono non è valido, il telefono non può completare l'handshake protetto con la TV e la migrazione al cluster di destinazione non riuscirà. Prima di avviare il processo di migrazione, verificare che nei telefoni sia installato il file CTL/ITL corretto. Inoltre, nel cluster di origine, confermare che la funzionalità enterprise "Prepara cluster per rollback a versione

precedente alla 8.0" sia impostata su False.

Configurazione

Importare il certificato CallManager dei cluster di destinazione nell'archivio di attendibilità CallManager e Phone-SAST dei cluster di origine. Esistono due metodi per eseguire questa operazione.

Metodo 1.

Utilizzare Bulk Certificate Tool e completare questi passaggi sui cluster di origine e di destinazione.

Passaggio 1. Passare alla pagina **Cisco Unified OS Administration > Security > Bulk Certificate Management** sui cluster di origine e di destinazione.

Passaggio 2. Immettere i dettagli per il server SFTP (Secure File Transfer Protocol) e selezionare **Salva**.

Passaggio 3. Selezionare **Esporta** ed esportare il certificato TFTP (Trivial File Transfer Protocol).

Passaggio 4. Fare clic sul pulsante **Consolida** per eseguire il consolidamento dei certificati. Verrà creato un file PKCS12 che include sia il certificato di CallManager di origine che quello di destinazione.

Passaggio 5. Importare nuovamente i certificati consolidati in ogni cluster.

Durante il processo di consolidamento (passo 5), il il certificato CallManager dei cluster di origine viene caricato nel cluster di destinazione nell'archivio CallManager-trust e Phone-SAST-trust. Ciò consente ai telefoni di tornare al cluster di origine. Se viene seguito il metodo manuale, il certificato CallManager dei cluster di origine non essere caricato nel cluster di destinazione. Ciò significa che non è possibile eseguire la migrazione dei telefoni al cluster di origine. Se si desidera eseguire la migrazione dei telefoni nel cluster di origine, è possibile È necessario caricare il certificato CallManager dei cluster di origine nei cluster di destinazione CallManager-trust e Phone-SAST-trust.

> **Nota:** Entrambi i cluster devono esportare il certificato TFTP nello stesso server SFTP e nella stessa directory SFTP.

> **Nota:** Il passaggio 4 è obbligatorio solo in un cluster. Se si esegue la migrazione di telefoni da CUCM versione 8.x o 9.x a CUCM versione 10.5.2.13900-12 o successive, prendere nota dell'ID bug Cisco CSCuy43181 prima di consolidare i certificati.

Metodo 2.

Importare manualmente i certificati. Completare questi passaggi nel cluster di destinazione.

Passaggio 1. Passare alla pagina **Cisco Unified OS Administration > Sicurezza > Gestione certificati**.

Passaggio 2. Selezionare il certificato CallManager.pem e scaricarlo.

Passaggio 3. Selezionare il certificato ITLrecovery.pem e scaricarlo

Passaggio 4. Caricare il certificato di CallManager nel server di pubblicazione del cluster di origine come certificato di trust CallManager e di trust Phone-SAST.

Passaggio 5. Caricare il certificato di ripristino ITL nel cluster di origine come Phone-SAST-Trust

Passaggio 6. Riavviare TVS in tutti i nodi dal cluster di origine.

I certificati vengono quindi replicati negli altri nodi del cluster.

I passi 3, 5, 6 si applicano agli scenari di migrazione del telefono da 8.x a 12.x

> **Nota:** Il certificato di CallManager deve essere scaricato da tutti i nodi che eseguono il servizio TFTP nel cluster di destinazione.

Dopo aver caricato i certificati con uno dei metodi descritti in precedenza, modificare l'opzione 150 del protocollo DHCP (Dynamic Host Configuration Protocol) dei telefoni in modo che puntino all'indirizzo TFTP dei cluster di destinazione.

> **Attenzione:** Un metodo per eseguire la migrazione dei telefoni tra cluster non protetti consiste nell'impostare "Prepara cluster per rollback a versione precedente alla 8.0" su True nel cluster di origine e riavviare i telefoni. Questa opzione non è disponibile quando si esegue la migrazione di telefoni tra cluster protetti. Questo perché la funzione di rollback per le versioni precedenti alla 8.0 cancella solo il file ITL (non cancella il file CTL). Ciò significa che quando il telefono viene migrato e scarica il file CTL dal cluster di destinazione, deve verificare il nuovo CTL con le TV dei cluster di origine. Poiché il file ITL del telefono non contiene il certificato TVS dei cluster di origine, l'handshake non riesce quando il telefono tenta di stabilire una connessione sicura al servizio TVS.

Verifica

Questo è un estratto dei log della console telefonica e dei log TVS (impostati in dettaglio) del cluster di origine. Gli snippet mostrano il processo di registrazione dei telefoni nel cluster di destinazione.

1. Il telefono avvia e scarica il file CTL dal cluster di destinazione.

```
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. Il file CTL è firmato dal certificato del gestore chiamate dei cluster di destinazione che non si trova nel file CTL o ITL dei telefoni esistenti. Ciò significa che il telefono deve contattare il servizio TV per verificare il certificato. A questo punto il telefono ha ancora la sua configurazione precedente che contiene l'indirizzo IP del servizio TVS cluster di origine (il TVS specificato nella

configurazione dei telefoni è lo stesso del gruppo phone call manager). Il telefono configura una connessione SSL al servizio TVS. Quando il servizio TVS presenta il proprio certificato al telefono, il telefono verifica il certificato confrontandolo con il certificato nel relativo file ITL. Se sono uguali, l'handshake viene completato correttamente.

```
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. I registri TVS mostrano la connessione in entrata dal telefono e l'handshake è riuscito.

```
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. I registri della console telefonica mostrano che il telefono invia una richiesta al servizio TVS per verificare il certificato del gestore chiamate dal cluster di destinazione.

```
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. I registri TVS indicano che la richiesta è stata ricevuta.

```
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. I registri TVS mostrano il certificato nel proprio punto vendita e il TVS invia una risposta al telefono.

```
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. I registri della console telefonica indicano che il certificato è stato verificato correttamente e che il file CTL è stato aggiornato.

```
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. I registri della console telefonica vengono visualizzati quando il telefono scarica il file ITL.

```
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. Il file ITL viene verificato rispetto al file CTL. Il file CTL contiene il certificato CallManager dei cluster di destinazione. Questo significa che il telefono può verificare il certificato senza contattare il servizio TV dei cluster di origine.

```
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.
```

Risoluzione dei problemi

Prima del processo di migrazione, verificare il CTL/ITL sui telefoni. Per ulteriori informazioni su come verificare il CTL/ITL, fare clic qui: https://www.cisco.com/c/en/us/support/docs/voice-unified-communications/unified-communications-manager-callmanager/116232-technote-sbd-00.html#anc9