Caricamento dei certificati radice e intermedi di Expressway-Core su CUCM

Sommario

Introduzione

In questo documento viene descritto come caricare i certificati radice e intermedi che hanno firmato il certificato Expessway-C per l'editore CUCM come "tomcat-trust" e "callmanager-trust".

A causa dei miglioramenti apportati al servizio server di traffico su Expressway in X14.0.2, Expressway-C invia il proprio certificato client ogni volta che un server (CUCM) lo richiede, per servizi in esecuzione su porte diverse da 8443 (ad esempio 6971,6972) anche se CUCM è in modalità non protetta. A causa di questa modifica, è necessario che l'Autorità di certificazione (CA) per la firma dei certificati Expressway-C venga aggiunta in CUCM come "tomcat-trust" e "callmanager-trust".

Il mancato caricamento della CA di firma Expressway-C su CUCM causa l'errore di accesso MRA dopo un aggiornamento di Expressways a X14.0.2 o versioni successive. Nell'acquisizione dei pacchetti tra Expressway-C e CUCM si vedrebbe che CUCM invia un errore TLS 'Unknown CA' a Expressway-C.

Prerequisiti

Premesse

Affinché CUCM consideri attendibile il certificato inviato da Expressway-C, è necessario che sia in grado di stabilire un collegamento da tale certificato a un'Autorità di certificazione (CA) di livello superiore (radice) considerata attendibile. Tale collegamento, ovvero una gerarchia di certificati che collega un certificato di entità a un certificato CA radice, è denominato catena di attendibilità. Per verificare tale catena di attendibilità, ogni certificato contiene due campi: Emittente (o 'Rilasciato da') e soggetto (o 'Rilasciato a').

I certificati server, ad esempio quello inviato da Expressway-C a CUCM, hanno in genere nel campo 'Oggetto' il nome di dominio completo (FQDN) della CN (Nome comune):

```
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
```

Esempio di certificato server per Expressway vcs-c1.vngtp.lab. Il nome di dominio completo (FQDN) è presente nell'attributo CN del campo Oggetto insieme ad altri attributi, quali Paese (C), Stato (ST), Posizione (L), ... Si noti inoltre che il certificato del server viene rilasciato da una CA denominata vngtp-ACTIVE-DIR-CA (vngtp-ACTIVE-DIR-CA.vngtp.lab).

Le CA di livello superiore (CA radice) possono inoltre rilasciare un certificato per identificarsi. In tale certificato CA radice, è possibile notare che l'autorità emittente e l'oggetto hanno lo stesso valore:

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

In questo certificato i campi Emittente e Oggetto hanno lo stesso valore. Si tratta di un certificato rilasciato da una CA radice per identificarsi.

In una situazione tipica, le CA radice non rilasciano direttamente certificati server. Al contrario, emettono certificati per altre CA. Tali altre CA vengono quindi definite CA intermedie. Le CA intermedie possono a loro volta emettere direttamente certificati server o certificati per altre CA intermedie. Si può verificare una situazione in cui un certificato server viene rilasciato dalla CA intermedia 1, che a sua volta ottiene un certificato dalla CA intermedia 2 e così via. Finché la CA intermedia non ottiene il proprio certificato direttamente dalla CA radice:

```
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
```

Ora, affinché CUCM consideri attendibile il certificato server inviato da Expressway-C, è necessario che sia in grado di creare la catena di attendibilità da tale certificato server fino a ottenere un certificato CA radice. A tale scopo, è necessario caricare il certificato CA radice e tutti i certificati CA intermedi (se presenti) nell'elenco di attendibilità di CUCM.

> **Nota: Sebbene i campi Issuer e Subject siano facili da creare e leggibili, Expressway-C e CUCM non utilizzano tali campi nel certificato. Utilizzano invece i campi 'Identificatore chiave autorità X509v3' e 'Identificatore chiave oggetto X509v3' per creare la catena di attendibilità. Tali chiavi contengono identificatori per i certificati più precisi rispetto all'utilizzo dei campi Oggetto/Emittente: possono essere presenti 2 certificati con gli stessi campi Oggetto/Autorità emittente, ma uno di essi è scaduto e uno è ancora valido. Entrambi avrebbero un identificatore di chiave del soggetto X509v3 diverso, in modo che Expressway/CUCM possa ancora determinare la corretta catena di attendibilità.**

Configurazione

Passaggio 1: Ottiene i certificati radice e intermedi che hanno firmato il certificato del server Expressway-C

Èbuona norma che quando inizialmente si ottiene il certificato server da una CA (CA radice o CA intermedia) che ha firmato il certificato server, si ottengono anche i certificati radice e intermedi per il certificato server e li si archivia in un luogo sicuro. In questo caso, è possibile ottenere i certificati radice e intermedi e passare al passaggio 2, dove è possibile trovare istruzioni su come caricarli in CUCM.

Se non hai seguito la procedura consigliata per memorizzare i certificati radice/intermedi in un luogo sicuro, possiamo ottenerli da Expressway-C come li avresti caricati anche prima di caricare il certificato del server. Il primo passo consisterebbe nell'esaminare con esattezza il certificato di cui abbiamo bisogno. Per questo, in Expressway-C passare a Manutenzione > Sicurezza > Certificato server e fare clic o selezionare il pulsante 'Mostra (decodificato)' accanto a 'Certificato server'. Verrà aperta una nuova finestra/scheda con il contenuto del certificato del server Expressway-C. Cerchiamo il campo "Emittente":

```
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:
...
```

Il nostro certificato server Expressway è rilasciato da un'organizzazione DigiCert Inc con nome comune 'DigiCert Global CA-1'.

Passiamo ora a Manutenzione > Sicurezza > Certificato CA attendibile e cerchiamo nell'elenco se vi è un certificato con lo stesso identico valore (O=DigiCert Inc, CN=DigiCert Global CA-1) nel campo 'Oggetto'.

	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

Archivio attendibilità Expressway

Nell'archivio di attendibilità Expressway-C è infatti presente un certificato con un oggetto identico all'autorità emittente del certificato del server Expressway-C. Tale certificato, l'ultimo nell'elenco come illustrato nell'immagine, è rilasciato da O=DigiCert Inc, OU=www.digicert.com, CN=DigiCert Global Root CA. Si tratta di un certificato diverso dal relativo "Subject", pertanto questo non è un certificato CA radice ma un certificato CA intermedio.

> **Nota: Se nell'elenco non è presente un certificato con un oggetto corrispondente all'autorità emittente del certificato Expressway-C, controllare la colonna Autorità di certificazione nell'elenco e verificare se è possibile trovare una corrispondenza. In questo caso, se nella colonna 'Oggetto' viene visualizzato 'Corrisponde all'emittente' per il certificato, significa che è presente un certificato radice che ha firmato immediatamente il certificato del server Expressway-C, senza un'autorità di certificazione intermedia.**

Dopo aver trovato il certificato intermedio, non siamo ancora finiti. Dobbiamo arrivare fino al certificato radice. È quindi necessario trovare il certificato della CA che ha rilasciato il certificato CA intermedio con soggetto O=DigiCert Inc, CN=DigiCert Global CA-1. La CA che ha rilasciato il certificato è O=DigiCert Inc, OU=www.digicert.com, CN=DigiCert Global Root CA. Poiché nella colonna Oggetto non è presente alcuna corrispondenza per questa CA, nella colonna Emittente viene cercata la corrispondenza seguente: Il quarto certificato nell'elenco ha un'autorità emittente O=DigiCert Inc, OU=www.digicert.com, CN=DigiCert Global Root CA e, poiché il relativo "Oggetto" dice "Corrisponde all'autorità emittente", sappiamo che questo è il certificato della CA radice.

Conclusione : Il nostro certificato server Expressway-C è stato firmato dalla CA intermedia O=DigiCert Inc, CN=DigiCert Global CA-1 che a sua volta è stato firmato dalla CA radice O=DigiCert Inc, OU=www.digicert.com, CN=DigiCert Global Root CA.

Per ottenere il certificato radice e intermedio, selezionare o fare clic sul pulsante 'Mostra tutto (file PEM)' nell'elenco. Vengono visualizzati tutti i certificati principali e intermedi in formato PEM. Scorrere fino al quarto e ultimo certificato e copiare il contenuto. Il quarto certificato è il certificato CA radice:

```
...
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
...
```

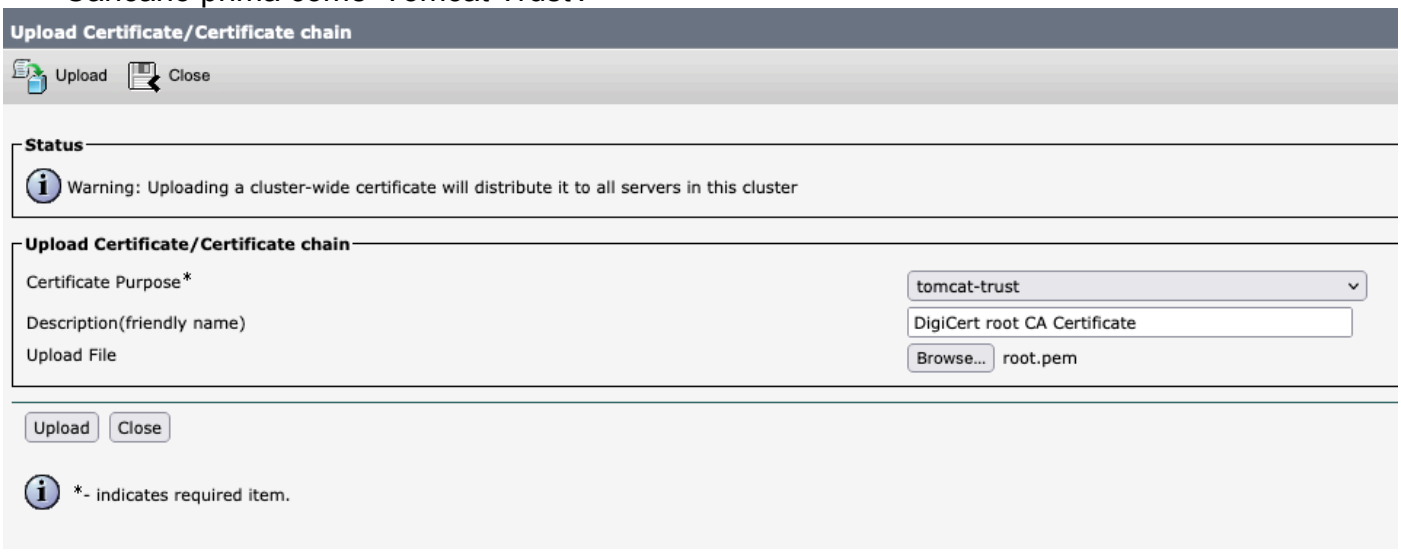
Per ogni certificato radice ed eventuale certificato intermedio, copiare tutto ciò che inizia con '—BEGIN CERTIFICATE—' e termina con '—END CERTIFICATE—' (incluso). Inserire ognuno di essi in un file di testo separato e aggiungere una riga vuota in basso (dopo la riga con —END CERTIFICATE—). Salva i file con estensione .pem: root.pem, intermediate1.pem, intermediate2.pem, ... È necessario un file separato per ogni certificato radice/intermedio. Nell'esempio precedente, il file root.pem contiene:

```
-----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-----
```

(notare che nella parte inferiore è presente una riga vuota)

Passaggio 2: Carica i certificati radice e intermedi (se presenti) in CUCM

- Accedere alla pagina Cisco Unified OS Administration di CUCM Publisher
- Selezionare Protezione > Gestione certificati
- Selezionare o fare clic sul pulsante "Carica catena certificati/certificati"
- Nella nuova finestra, iniziare a caricare il certificato root.pem ottenuto dal passaggio 1. Caricarlo prima come 'Tomcat Trust':



- Fare clic o selezionare il pulsante 'Upload' e quindi vedere "Success: Certificate Uploaded" (Caricato certificato). Ignora il messaggio sul riavvio di Tomcat per il momento.
- Caricare lo stesso file root.pem di 'CallManager-trust' per 'Certificate Purpose'.
- Ripetere i passaggi precedenti (caricare come 'tomcat-trust' e 'CallManager-trust') per tutti i certificati intermedi disponibili.

Passaggio 3: Riavviare i servizi necessari in CUCM

Ènecessario riavviare questi servizi in ogni nodo CUCM del cluster CUCM:

- Cisco CallManager
- Cisco TFTP
- Cisco Tomcat

I primi due possono essere riavviati dalle pagine Cisco Unified Serviceability di CUCM:

- Accedere alla pagina Cisco Unified Serviceability di CUCM Publisher
- Selezionare Strumenti > Control Center - Servizi funzionalità
- Selezionare il server di pubblicazione
- Selezionare il servizio 'Cisco CallManager' e fare clic sul pulsante 'Riavvia'
- Dopo aver riavviato il servizio Cisco CallManager, selezionare 'Cisco TFTP' e fare clic sul pulsante 'Riavvia'.
- Attendere il riavvio del servizio Cisco TFTP
- Ripetere i passaggi precedenti per ogni editore

Cisco Tomcat può essere riavviato solo dalla CLI:

- Aprire una connessione della riga di comando al server di pubblicazione CUCM
- Utilizzare il comando: **utilizza il servizio per riavviare Cisco Tomcat**
- Ripetere i passaggi precedenti su ogni nodo del destinatario predefinito