Cargue los certificados raíz e intermedio de Expressway-Core en CUCM

Contenido

Introducción

Este documento describe cómo cargar los certificados raíz e intermedio que firmaron el certificado Expessway-C al editor de CUCM como "tomcat-trust" y como "callmanager-trust".

Debido a las mejoras en el servicio de servidor de tráfico en Expressway en X14.0.2, Expressway-C envía su certificado de cliente siempre que un servidor (CUCM) lo solicita, para los servicios que se ejecutan en puertos que no sean 8443 (por ejemplo, 6971,6972) incluso si CUCM está en modo no seguro. Debido a este cambio, se requiere que la autoridad de certificación (CA) de firma de certificados de Expressway-C se agregue en CUCM como "tomcat-trust" y "callmanager-trust".

Si no se carga la CA de firma de Expressway-C en CUCM, se producirá un error en el inicio de sesión de MRA después de una actualización de Expressway a X14.0.2 o superior. En la captura de paquetes entre Expressway-C y CUCM, verá que CUCM envía un error TLS de 'CA desconocida' a Expressway-C.

Prerequisites

Antecedentes

Para que CUCM confíe en el certificado que envía Expressway-C, debe ser capaz de establecer un enlace de ese certificado a una Autoridad de certificación (raíz) de nivel superior (CA) en la que confía. Tal link, una jerarquía de certificados que vinculan un certificado de entidad a un certificado de CA raíz, se denomina cadena de confianza. Para poder verificar dicha cadena de confianza, cada certificado contiene dos campos: Emisor (o "Emitido por") y Asunto (o "Emitido a").

Los certificados de servidor, como el que Expressway-C envía a CUCM, tienen en el campo 'Asunto' normalmente su FQDN en el CN (nombre común) :

```
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
```

Ejemplo de un certificado de servidor para Expressway vcs-c1.vngtp.lab. Tiene el FQDN en el atributo CN del campo Asunto junto con otros atributos como el País (C), Estado (ST), Ubicación (L), ... También podemos ver que el certificado del servidor es entregado (emitido) por una CA llamada vngtp-ACTIVE-DIR-CA (vngtp-ACTIVE-DIR-CA.vngtp.lab).

Las CA de nivel superior (CA raíz) también pueden emitir un certificado para identificarse. En este certificado de CA raíz, vemos que el emisor y el sujeto tienen el mismo valor :

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

En este certificado, los campos Emisor y Asunto tienen el mismo valor. Es un certificado que entrega una CA raíz para identificarse.

En una situación típica, las CA raíz no emiten directamente certificados de servidor. En su lugar, emiten certificados para otras CA. Estas otras CA se denominan luego CA intermedias. Las CA intermedias pueden a su vez emitir directamente certificados de servidor o certificados para otras CA intermedias. Podemos tener una situación en la que un certificado de servidor es emitido por la CA 1 intermedia, que a su vez obtiene un certificado de la CA 2 intermedia y así sucesivamente. Hasta que finalmente la CA intermedia obtiene su certificado directamente de la CA raíz :

```
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
```

Ahora, para que CUCM confíe en el certificado de servidor que envía Expressway-C, necesita poder construir la cadena de confianza desde ese certificado de servidor hasta un certificado de CA raíz. Para que esto suceda, necesitamos cargar el certificado de CA raíz y también todos los certificados de CA intermedia (si los hay, lo que no es el caso si la CA raíz hubiera emitido directamente el certificado de servidor de Expressway-C) en la lista de confianza de CUCM.

> **Nota: Aunque los campos Emisor y Asunto son fáciles de construir la cadena de confianza de una manera legible por las personas, Expressway-C y CUCM no utilizan estos campos en el certificado. En su lugar, utilizan los campos 'Identificador de clave de autoridad X509v3' e 'Identificador de clave de asunto X509v3' para crear la cadena de confianza. Estas claves contienen identificadores para los certificados que son más precisos que para utilizar los campos Asunto/Emisor : puede haber 2 certificados con los mismos campos Asunto/Emisor, pero uno de ellos ha caducado y otro sigue siendo válido. Ambos tendrían un identificador de clave de asunto X509v3 diferente, por lo que Expressway/CUCM aún puede determinar la cadena de confianza correcta.**

Configuración

Paso 1: Obtener la raíz y los certificados intermedios que firmaron el certificado de servidor de Expressway-C

Como buena práctica, cuando inicialmente obtuvo el certificado de servidor de una CA (CA raíz o CA intermedia) que firmó ese certificado de servidor, también obtuvo los certificados raíz e intermedio para ese certificado de servidor y los almacenó en algún lugar seguro. Si este es el caso, puede obtener esos certificados raíz e intermedios y pasar al paso 2, donde puede encontrar instrucciones para cargarlos en CUCM.

Si no siguió la buena práctica para almacenar los certificados raíz/intermedate en algún lugar seguro, podemos obtenerlos de Expressway-C como si los hubiera cargado allí también antes de cargar el certificado del servidor. El primer paso sería ver qué certificado necesitamos exactamente. Para ello, en Expressway-C navegue hasta Mantenimiento > Seguridad > Certificado de servidor y haga clic o seleccione el botón 'Mostrar (decodificado)' situado junto a 'Certificado de servidor'. Esto abre una nueva ventana/ficha con el contenido del certificado de servidor de Expressway-C. Buscamos el campo 'Emisor' ahí:

```
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:
...
```

Nuestro certificado de servidor de Expressway lo emite una Empresa DigiCert Inc con el nombre común 'DigiCert Global CA-1'.

Ahora vamos a Maintenance > Security > Trusted CA certificate y buscamos en la lista si tenemos un certificado con el mismo valor exacto (O=DigiCert Inc, CN=DigiCert Global CA-1) en el campo 'Subject'.

	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

Almacén de confianza de Expressway

De hecho, vemos que hay un certificado en el almacén de confianza de Expressway-C que tiene un asunto que es idéntico al 'emisor' del certificado de servidor de Expressway-C. Ese certificado (el último de la lista como se muestra en la imagen) es emitido por O=DigiCert Inc, OU=www.digicert.com, CN=DigiCert Global Root CA. Esto es diferente a su 'Asunto', por lo que sabemos que no es un certificado de CA raíz sino un certificado de CA intermedia.

> **Nota: Si no ve ningún certificado en esa lista con un "Asunto" que coincida con el "emisor" de nuestro certificado de Expressway-C, consulte la columna "Emisor" de la lista y vea si puede encontrar una coincidencia allí. Si ese es el caso y la columna 'Asunto' muestra 'Coincide con el emisor' para ese certificado, significa que hay un certificado raíz que firmó nuestro certificado de servidor de Expressway-C inmediatamente, sin una CA intermedia entre sí.**

Después de encontrar el certificado intermedio, aún no hemos terminado. Tenemos que ir hasta el certificado raíz. Por lo tanto, necesitamos encontrar el certificado de la CA que emitió el certificado de CA intermedio con el asunto O=DigiCert Inc, CN=DigiCert Global CA-1. Sabemos que la CA que emitió este certificado es O=DigiCert Inc, OU=www.digicert.com, CN=DigiCert Global Root CA. Como no vemos una coincidencia para esta CA en la columna Asunto, vemos en la columna Emisor y sí vemos una coincidencia: el cuarto certificado de la lista tiene un emisor O=DigiCert Inc, OU=www.digicert.com, CN=DigiCert Global Root CA y como su 'Asunto' dice 'Coincide con el emisor' sabemos que este es el certificado raíz CA.

Conclusión: nuestro certificado de servidor de Expressway-C fue firmado por CA intermedia O=DigiCert Inc, CN=DigiCert Global CA-1 que a su vez fue firmado por CA raíz O=DigiCert Inc, OU=www.digicert.com, CN=DigiCert Global Root CA CA.

Para obtener el certificado raíz e intermedate, haga clic o seleccione el botón 'Mostrar todo (archivo PEM)' en la lista. Muestra todos los certificados raíz e intermedio en formato PEM. Desplácese hacia abajo hasta el cuarto y último certificado y copie el contenido. El cuarto certificado es nuestro certificado de CA raíz :

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

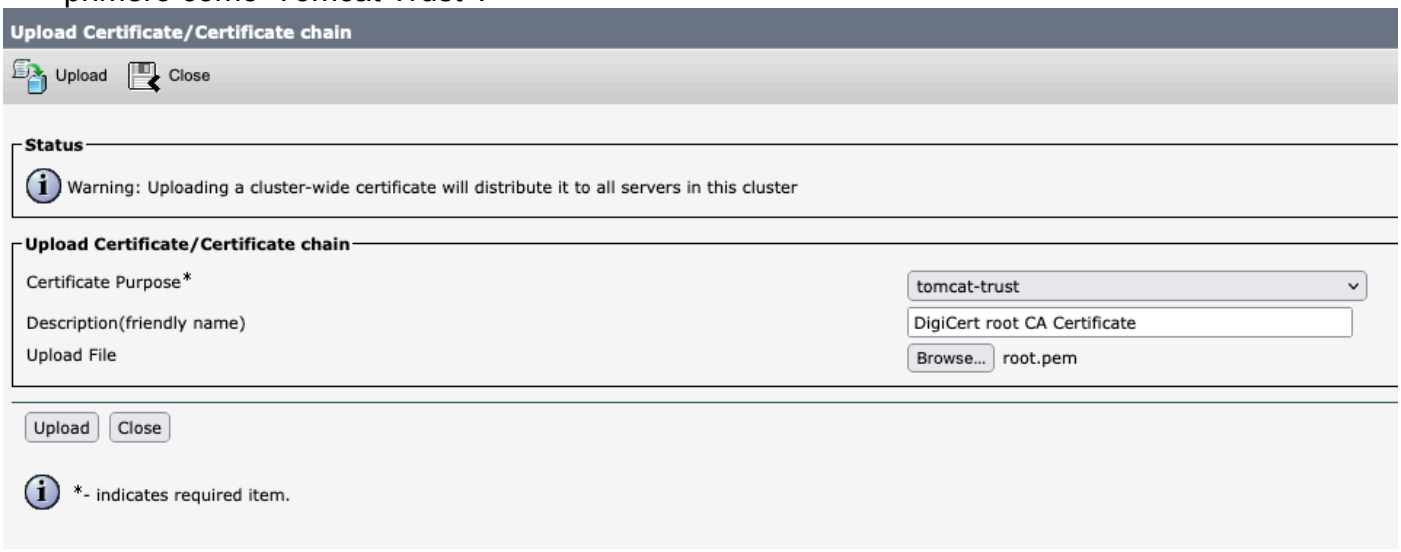
Para cada uno de los certificados raíz y eventual intermedio, copiará todo lo que comienza con '—BEGIN CERTIFICATE—' y termina con (incluido) '—END CERTIFICATE—'. Coloque cada uno de ellos en un archivo de texto independiente y agregue una línea vacía adicional en la parte inferior (después de la línea con —END CERTIFICATE—). Guarde estos archivos con la extensión .pem : root.pem, intermediario1.pem, intermedio2.pem, ... Necesita un archivo independiente para cada certificado raíz/intermedio. Para el ejemplo anterior, nuestro archivo root.pem contendría:

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

(observe que hay 1 línea vacía en la parte inferior)

Paso 2: Cargue los certificados raíz e intermedio (si los hay) en CUCM

- Inicie sesión en la página de administración de Cisco Unified OS de su editor de CUCM
- Vaya a Security > Certificate Management .
- Haga clic o seleccione el botón "Cargar certificado/cadena de certificado".
- En la nueva ventana, comience a cargar el certificado root.pem que obtuvo del Paso 1. Sube primero como 'Tomcat Trust' :



- Haga clic o seleccione el botón "Cargar" y, a continuación, verá "Éxito: Certificado cargado". Ignore el mensaje sobre reiniciar Tomcat por ahora.
- Cargue el mismo archivo root.pem ahora que 'CallManager-trust' para 'Certificate Purpose'.
- Repita los pasos anteriores (cargue como 'tomcat-trust' y 'CallManager-trust') para todos los certificados intermedios que tenga.

Paso 3: Reinicie los servicios necesarios en CUCM

Estos servicios deben reiniciarse en cada nodo de CUCM del clúster de CUCM :

- CallManager de Cisco
- Cisco TFTP
- Tomcat de Cisco

Los primeros 2 podemos reiniciar desde las páginas de Serviciabilidad de Cisco Unified de CUCM:

- Inicie sesión en la página Cisco Unified serviceability de su editor de CUCM
- Vaya a Tools > Control Center - Feature Services (Herramientas > Centro de control > servicios de funciones).
- Seleccione el editor como servidor
- Seleccione el servicio 'Cisco CallManager' y haga clic en el botón 'Reiniciar'
- Después de reiniciar el servicio Cisco CallManager, seleccione el servicio 'Cisco TFTP' y haga clic en el botón 'Restart' (Reiniciar).
- Espere a que se reinicie el servicio Cisco TFTP
- Repita los pasos anteriores para cada uno de sus editores

Solo se puede reiniciar Cisco Tomcat desde CLI:

- Abrir una conexión de línea de comandos a su editor de CUCM
- Use el comando: **utils service restart Cisco Tomcat**

- Repita los pasos anteriores en cada uno de sus nodos suscriptores