Télécharger les certificats racine/intermédiaires d'Expressway-Core sur CUCM

Table des matières

Introduction

Informations générales

Configuration

- Étape 1. Obtenir les certificats racine et intermédiaire qui ont signé le certificat du serveur Expressway-C
- Étape 2. Télécharger les certificats racine et intermédiaires sur CUCM (le cas échéant)
- Étape 3. Redémarrez les services nécessaires sur CUCM

Informations connexes

Introduction

Ce document décrit comment télécharger les certificats racine et intermédiaires des CA qui ont signé des certificats Expressway-C vers l'éditeur CUCM.

Informations générales

En raison des améliorations apportées au service de serveur de trafic sur Expressway dans X14.0.2, Expressway-C envoie son certificat client chaque fois qu'un serveur (CUCM) le demande pour des services qui s'exécutent sur des ports autres que 8443 (par exemple, 6971,6972), même si CUCM est en mode non sécurisé. En raison de cette modification, il est nécessaire que l'autorité de certification (CA) de signature de certificat d'Expressway-C soit ajoutée dans CUCM en tant que tomcat-trust et callmanager-trust.

Si vous ne téléchargez pas l'autorité de certification de signature Expressway-C sur CUCM, la connexion MRA échouera après une mise à niveau d'Expressways vers X14.0.2 ou une version supérieure.

Pour que CUCM puisse faire confiance au certificat envoyé par Expressway-C, tomcat-trust et callmanager-trust doivent inclure l'autorité de certification racine et toutes les autorités de certification intermédiaires impliquées dans la signature du certificat Expressway-C.

Configuration

Étape 1. Obtenir les certificats racine et intermédiaire qui ont signé le certificat du serveur Expressway-C

Lorsque vous avez reçu le certificat de serveur d'une autorité de certification qui a signé ce certificat de serveur, vous disposez également des certificats racine et intermédiaire pour ce certificat de serveur et les avez stockés en lieu sûr. Si vous avez toujours ces fichiers ou si vous pouvez les télécharger à nouveau à partir de votre autorité de certification, vous pouvez passer à l'étape 2 où vous trouverez des instructions sur la façon de les télécharger sur CUCM.

Si vous n'avez plus ces fichiers, vous pouvez les télécharger à partir de l'interface Web d'Expressway-C. C'est un peu compliqué, il est donc fortement recommandé de contacter votre autorité de certification pour télécharger le magasin de confiance à partir d'eux, si possible.

Sur l'Expressway-C, accédez à Maintenance > Security > Server certificate, et cliquez sur le bouton Show (decoded) en regard de Server certificate. Une nouvelle fenêtre/un nouvel onglet s'ouvre avec le contenu du certificat du serveur Expressway-C. Vous y recherchez le champ Émetteur :

<#root>

```
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:
...
```

Dans cet exemple, le certificat du serveur Expressway-C est émis par une organisation, DigiCert Inc., avec le nom commun DigiCert Global CA-1.

À présent, accédez à Maintenance > Security > Trusted CA certificate, et regardez dans la liste pour voir si vous avez un certificat là-bas avec la même valeur exacte dans le champ Subject.

Dans cet exemple, O=DigiCert Inc, CN=DigiCert Global CA-1 dans le champ Subject (Objet). Si vous trouvez une correspondance, cela signifie qu'il s'agit d'une autorité de certification intermédiaire. Vous avez besoin de ce fichier et vous devez continuer à rechercher jusqu'à ce que vous trouviez l'autorité de certification racine.

Si vous ne trouvez pas de correspondance, recherchez un certificat avec cette valeur dans le champ Émetteur avec un objet correspondant à Émetteur. Si vous trouvez une correspondance, cela signifie qu'il s'agit du fichier CA racine et que c'est le seul fichier dont nous avons besoin.



	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

Magasin de confiance Expressway

Dans cet exemple, après avoir trouvé le certificat, vous remarquez que le champ Subject ne correspond pas au champ Issuer. Cela signifie qu'il s'agit d'un certificat CA intermédiaire. Vous avez besoin de ce certificat en plus du certificat racine. Si l'objet a indiqué Correspond à l'émetteur, vous savez qu'il s'agit de l'autorité de certification racine et du seul certificat auquel vous devez faire confiance.

Si vous avez un certificat intermédiaire, vous devez continuer jusqu'à ce que nous trouvions le certificat racine. Pour ce faire, consultez le champ Émetteur de votre certificat intermédiaire. Recherchez ensuite un certificat avec la même valeur dans le champ Subject (Objet). Dans notre cas, il s'agit de O=DigiCert Inc, OU=www.digicert.com, CN=DigiCert Global Root CA - Vous recherchez un certificat avec cette valeur dans le champ Subject. Si vous ne trouvez pas de certificat correspondant, recherchez cette valeur dans le champ Émetteur avec un objet correspondant à Émetteur.

Dans cet exemple, vous pouvez voir que notre certificat de serveur Expressway-C a été signé par l'intermédiaire CA O=DigiCert Inc, CN=DigiCert Global CA-1 qui a été signé par la racine CA O=DigiCert Inc. OU=www.digicert.com, CN=DigiCert Global Root CA. Puisque vous avez trouvé l'autorité de certification racine, vous avez terminé. Si, toutefois, vous avez trouvé une autre

autorité de certification intermédiaire, vous devez poursuivre ce processus jusqu'à ce que vous ayez identifié chaque autorité de certification intermédiaire et l'autorité de certification racine.

Afin de télécharger les fichiers de certificat racine et intermédiaire, cliquez sur le bouton Show all (PEM file) sous la liste. Vous voyez ainsi tous les certificats racine et intermédiaires au format PEM. Faites défiler vers le bas jusqu'à ce que vous trouviez un certificat correspondant à l'un de vos certificats intermédiaires ou au certificat racine. Dans cet exemple, le premier que vous trouvez est O=DigiCert Inc, CN=DigiCert Global Root CA - vous allez copier ce certificat dans un fichier et l'enregistrer localement.

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

Pour chacun des certificats racine et éventuellement intermédiaires, copiez tout ce qui commence par (inclus) -----BEGIN CERTIFICATE----- et se termine par (inclus) -----END CERTIFICATE-----. Placez chacun d'eux dans un fichier texte séparé et ajoutez 1 ligne vide supplémentaire au bas (après la ligne avec -----END CERTIFICATE-----). Enregistrez ces fichiers avec l'extension .pem : racine.pem, intermédiaire1.pem, intermédiaire2.pem, ... Vous avez besoin d'un fichier distinct pour chaque certificat racine/intermédiaire. Pour l'exemple précédent, notre fichier root.pem

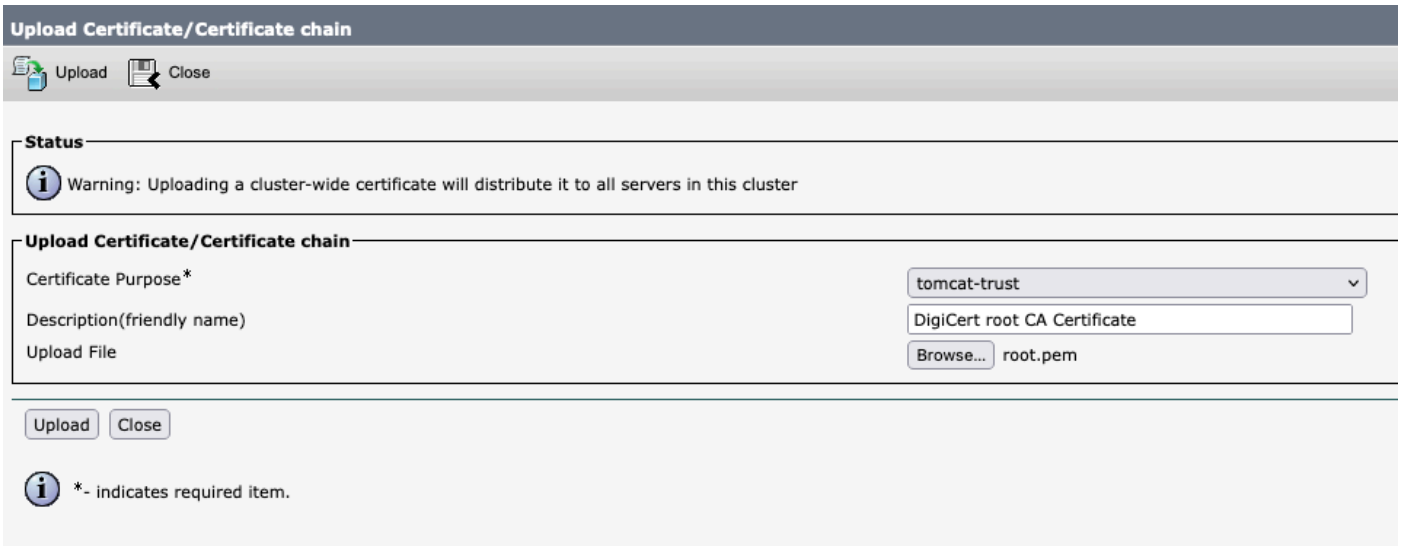
contiendrait :

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

Remarque : Il doit y avoir une seule ligne vide en bas.

Étape 2. Télécharger les certificats racine et intermédiaires sur CUCM (le cas échéant)

- Connectez-vous à la page Cisco Unified OS Administration de votre serveur de publication CUCM.
- Accédez à Security > Certificate Management.
- Cliquez sur le bouton Upload Certificate/Certificate chain.
- Dans la nouvelle fenêtre, commencez à télécharger le certificat racine à partir de l'étape 1. Téléchargez-le sur tomcat-trust.



- Cliquez sur le bouton Upload, et ensuite vous devez voir Success : Certificat téléchargé. Ignorez le message vous demandant de redémarrer Tomcat pour l'instant.
- Téléchargez le même fichier racine maintenant avec CallManager-trust pour le rôle du certificat.
- Répétez les étapes précédentes (téléchargement vers tomcat-trust et CallManager-trust) pour tous les certificats intermédiaires utilisés sur l'Expressway-C.

Étape 3. Redémarrez les services nécessaires sur CUCM

Ces services doivent être redémarrés sur chaque noeud CUCM de votre cluster CUCM :

- Cisco CallManager
- TFTP Cisco
- Cisco Tomcat
- Cisco HAProxy

Cisco CallManager et Cisco TFTP peuvent être redémarrés à partir des pages Cisco Unified Serviceability de CUCM :

- Connectez-vous à la page Cisco Unified Serviceability de votre serveur de publication CUCM.
- Accédez à Outils > Centre de contrôle - Services de fonctionnalités.
- Sélectionnez votre serveur Publisher comme serveur.
- Choisissez Cisco CallManager service, puis cliquez sur le bouton Restart.
- Après le redémarrage du service Cisco CallManager, choisissez Cisco TFTP service, puis cliquez sur le bouton Restart.

Cisco Tomcat et HAProxy peuvent uniquement être redémarrés à partir de l'interface de ligne de commande :

- Ouvrez une connexion de ligne de commande à votre serveur de publication CUCM.
- Utilisez la commande utils service restart Cisco Tomcat.
- Utilisez la commande utils service restart Cisco HAProxy

Informations connexes

Support technique et documentation – Cisco Systems

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.