Télécharger les certificats racine et intermédiaire d'Expressway-Core sur CUCM

Contenu

Introduction

Ce document décrit comment télécharger les certificats racine et intermédiaire qui ont signé le certificat Expessway-C à l'éditeur CUCM en tant que " tomcat-trust " et en tant que " callmanager-trust ".

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 exécutés sur des ports autres que 8443 (par exemple 6971 6972) même si CUCM est en mode non sécurisé. En raison de ce changement, il est nécessaire que l'autorité de certification de signature de certificat (CA) 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 version ultérieure. Dans la capture de paquets entre Expressway-C et CUCM, CUCM envoie une erreur TLS 'Unknown CA' à Expressway-C.

Conditions préalables

Informations générales

Pour que CUCM puisse faire confiance au certificat qu'Expressway-C envoie, il doit être en mesure d'établir un lien entre ce certificat et une autorité de certification de niveau supérieur (racine) qu'elle a confiance. Une telle liaison, une hiérarchie de certificats qui relie un certificat d'entité à un certificat d'autorité de certification racine, est appelée chaîne de confiance. Pour pouvoir vérifier une telle chaîne de confiance, chaque certificat contient deux champs : Émetteur (ou 'Émis par') et Objet (ou 'Émis à').

Les certificats de serveur, tels que celui qu'Expressway-C envoie à CUCM, ont généralement dans le champ 'Subject' leur nom de domaine complet dans le CN (Common Name) :

```
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
```

Exemple de certificat de serveur pour Expressway vcs-c1.vngtp.lab. Il a le nom de domaine complet dans l'attribut CN du champ Objet ainsi que d'autres attributs tels que le pays (C), l'état (ST), l'emplacement (L), ... Nous pouvons également voir que le certificat de serveur est délivré (émis) par une autorité de certification appelée vngtp-ACTIVE-DIR-CA (vngtp-ACTIVE-DIR-CA.vngtp.lab).

Les autorités de certification de niveau supérieur (autorités de certification racine) peuvent également émettre un certificat pour s'identifier. Dans ce certificat d'autorité de certification racine, nous voyons que l'émetteur et l'objet ont la même valeur :

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

Dans ce certificat, les champs Émetteur et Objet ont la même valeur. Il s'agit d'un certificat délivré par une autorité de certification racine pour s'identifier.

Dans une situation typique, les autorités de certification racine ne délivrent pas directement de certificats de serveur. Au lieu de cela, ils délivrent des certificats pour d'autres autorités de certification. Ces autres autorités de certification sont ensuite appelées autorités de certification intermédiaires. Les autorités de certification intermédiaires peuvent à leur tour émettre directement des certificats de serveur ou des certificats pour d'autres autorités de certification intermédiaires. Nous pouvons avoir une situation où un certificat de serveur est émis par l'autorité de certification intermédiaire 1, qui à son tour obtient un certificat de l'autorité de certification intermédiaire 2 et ainsi de suite. Jusqu'à ce que finalement l'autorité de certification intermédiaire reçoive son certificat directement de l'autorité de certification racine :

```
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
```

Maintenant, pour que CUCM puisse faire confiance au certificat de serveur qu'Expressway-C envoie, il doit être capable de construire la chaîne de confiance à partir de ce certificat de serveur jusqu'à un certificat de CA racine. Pour ce faire, nous devons télécharger le certificat d'autorité de certification racine et tous les certificats d'autorité de certification intermédiaire (s'il y en a, ce qui n'est pas le cas si l'autorité de certification racine aurait directement émis le certificat de serveur d'Expressway-C) dans la liste de confiance de CUCM.

Note: Bien que les champs Émetteur et Sujet soient faciles à construire la chaîne de Confiance de manière lisible par l'homme, Expressway-C et CUCM n'utilisent pas ces champs dans le certificat. Ils utilisent plutôt les champs 'Identificateur de clé d'autorité

X509v3' et 'Identificateur de clé d'objet X509v3' pour créer la chaîne de confiance. Ces clés contiennent des identificateurs pour les certificats qui sont plus précis que pour utiliser les champs Objet/Émetteur : il peut y avoir 2 certificats avec les mêmes champs Objet/Émetteur, mais l'un d'eux a expiré et l'autre est toujours valide. Ils auraient tous deux un identificateur de clé d'objet X509v3 différent, de sorte qu'Expressway/CUCM puisse toujours déterminer la chaîne de confiance appropriée.

Configuration

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

Par mesure de précaution, lorsque vous avez obtenu le certificat de serveur d'une autorité de certification (autorité de certification racine ou autorité de certification intermédiaire) qui a signé ce certificat de serveur, vous avez également obtenu les certificats racine et intermédiaire pour ce certificat de serveur et les avez stockés quelque part dans un endroit sûr. Si c'est le cas, vous pouvez obtenir ces certificats racine et intermédiaire et passer à l'étape 2 où vous pouvez trouver des instructions pour les télécharger sur CUCM.

Si vous n'avez pas suivi la bonne pratique pour stocker vos certificats root/intermedate quelque part en toute sécurité, nous pouvons les obtenir de l'Expressway-C comme vous les auriez téléchargés là aussi avant de télécharger le certificat du serveur. La première étape serait de chercher le certificat dont nous avons besoin exactement. Pour cela, sur l'Expressway-C, naviguez jusqu'à Maintenance > Security > Server certificate et cliquez ou sélectionnez le bouton Show (décodé) en regard de Server certificate. Ceci ouvre une nouvelle fenêtre/onglet avec le contenu du certificat du serveur Expressway-C. Nous recherchons le champ 'Émetteur' ici :

```
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:
...
```

Notre certificat de serveur Expressway est délivré par une société DigiCert Inc. de nom commun 'DigiCert Global CA-1'.

Nous allons maintenant à Maintenance > Security > Trusted CA certificate et recherchons dans la liste si nous y avons un certificat avec la même valeur exacte (O=DigiCert Inc, CN=DigiCert Global CA-1) dans le champ '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

Magasin d'approbation Expressway

Nous constatons en effet qu'il existe dans le magasin de fiducie Expressway-C un certificat dont le sujet est identique à celui de l'émetteur du certificat de serveur Expressway-C. Ce certificat (le dernier de la liste comme indiqué sur l'image) est émis par O=DigiCert Inc, OU=www.digicert.com, CN=DigiCert Global Root CA. Ceci est différent de son 'Subject', nous savons donc qu'il ne s'agit pas d'un certificat d'autorité de certification racine mais d'un certificat d'autorité de certification intermédiaire.

> **Remarque: Si vous ne voyez pas de certificat dans cette liste avec un objet qui correspond à l'émetteur de notre certificat Expressway-C, regardez la colonne de l'émetteur dans la liste et voyez si vous pouvez trouver une correspondance. Si c'est le cas et que la colonne 'Subject' indique 'Matches Issue' pour ce certificat, cela signifie qu'il y a un certificat racine qui a signé notre certificat de serveur Expressway-C immédiatement, sans CA intermédiaire entre les deux.**

Après avoir trouvé le certificat intermédiaire, nous n'avons pas encore terminé. Nous devons aller jusqu'au certificat racine. Nous devons donc trouver le certificat de l'AC qui a délivré le certificat de l'AC intermédiaire avec le sujet O=DigiCert Inc, CN=DigiCert Global CA-1. Nous savons que l'AC qui a délivré ce certificat est O=DigiCert Inc, OU=www.digicert.com, CN=DigiCert Global Root CA. Comme nous ne voyons pas de correspondance pour cette autorité de certification dans la colonne Objet, nous regardons dans la colonne Émetteur et voyons qu'il y a effectivement une correspondance : le 4e certificat de la liste a un émetteur O=DigiCert Inc, OU=www.digicert.com, CN=DigiCert Global Root CA et parce que son 'Subject' dit 'Matches Issue' (Correspond à l'émetteur), nous savons que c'est le certificat de l'autorité de certification racine.

Conclusion: notre certificat de serveur Expressway-C a été signé par l'intermédiaire CA O=DigiCert Inc, CN=DigiCert Global CA-1 qui à son tour a été signé par l'intermédiaire CA O=DigiCert Inc, OU=www.digicert.com, CN=DigiCert Global Root CA.

Afin d'obtenir le certificat racine et intermédiaire, cliquez ou sélectionnez le bouton Afficher tout (fichier PEM) sous la liste. Vous voyez tous les certificats racine et intermédiaire au format PEM. Faites défiler jusqu'au quatrième et dernier certificat et copiez le contenu. Le 4ème certificat est notre certificat CA racine :

...

```
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
...
```

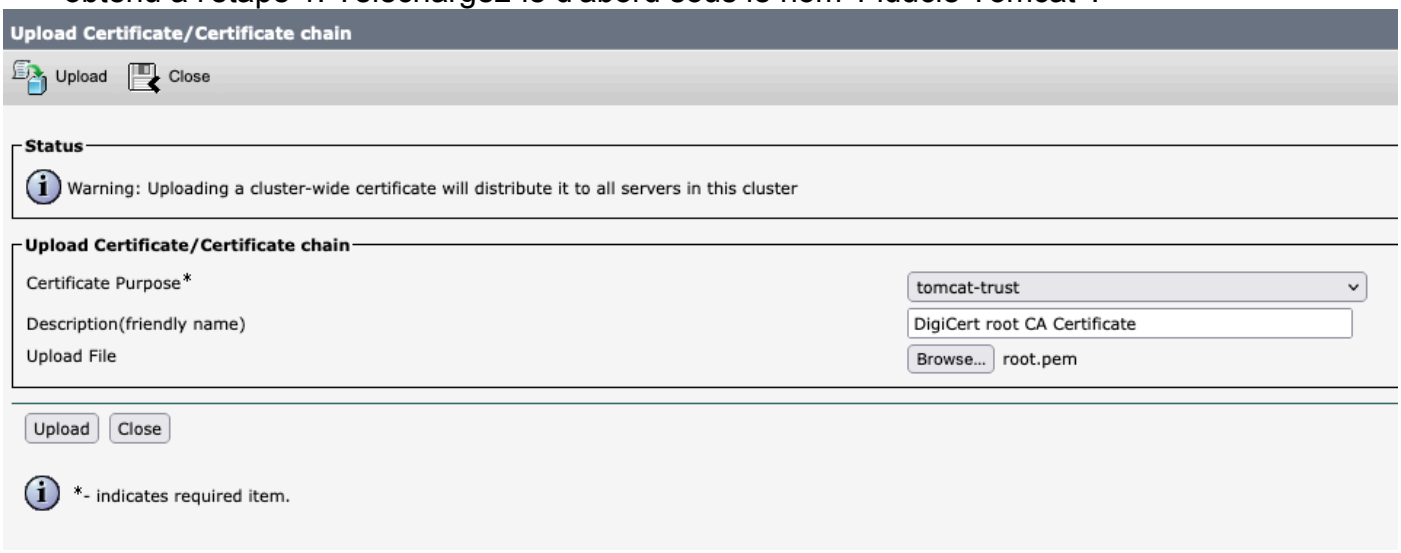
Pour chacun des certificats intermédiaires racine et éventuel, vous copiez tout ce qui commence par '—BEGIN CERTIFICATE—' et se termine par '—END CERTIFICATE—'. Placez chacun dans un fichier texte séparé et ajoutez 1 ligne vide supplémentaire en bas (après la ligne avec —END CERTIFICATE—). Enregistrez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

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

(notez qu'il y a 1 ligne vide en bas)

Étape 2 : Télécharger les certificats racine et intermédiaire (s'il y en a) sur CUCM

- Connectez-vous à la page Cisco Unified OS Administration de votre serveur de publication CUCM
- Naviguez jusqu'à Security > Certificate Management
- Cliquez ou sélectionnez le bouton Télécharger le certificat/la chaîne de certificats.
- Dans la nouvelle fenêtre, commencez à télécharger le certificat root.pem que vous avez obtenu à l'étape 1. Téléchargez-le d'abord sous le nom 'Fiducie Tomcat' :



- Cliquez ou sélectionnez le bouton 'Télécharger' et vous devez voir « Réussite : Certificat téléchargé ». Ignorez le message sur le redémarrage de Tomcat pour l'instant.
- Téléchargez le même fichier root.pem maintenant que 'CallManager-trust' pour l'objet du certificat.
- Répétez les étapes précédentes (téléchargez en tant que 'tomcat-trust' et 'CallManager-trust') pour tous les certificats intermédiaires dont vous disposez.

Étape 3 : Redémarrer les services nécessaires sur CUCM

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

- Cisco CallManager
- Cisco TFTP
- Cisco Tomcat

Les 2 premières pages de CUCM sur Cisco Unified Servicability :

- Connectez-vous à la page de maintenance Cisco Unified de votre serveur de publication CUCM
- Naviguez jusqu'à Tools > Control Center - Feature Services (Outils > Centre de contrôle - Services de fonctionnalité
- Sélectionnez votre serveur de publication en tant que serveur
- Sélectionnez le service Cisco CallManager et cliquez sur le bouton Redémarrer.
- Une fois le service Cisco CallManager redémarré, sélectionnez Service Cisco TFTP et cliquez sur le bouton Redémarrer.
- Attendez le redémarrage du service TFTP Cisco
- Répétez les étapes précédentes pour chacun de vos éditeurs

Cisco Tomcat ne peut être redémarré qu'à partir de l'interface de ligne de commande :

- Ouvrir une connexion de ligne de commande à votre serveur de publication CUCM
- Utilisez la commande: **utils service restart Cisco Tomcat**
- Répétez les étapes précédentes sur chacun des noeuds de votre abonné