Exemple de configuration de services téléphoniques externes sécurisés

Contenu

Introduction

Ce document décrit comment configurer le service de téléphone externe sécurisé. Cette configuration peut fonctionner avec n'importe quel service tiers, mais à des fins de démonstration, ce document utilise un serveur Cisco Unified Communications Manager (CUCM) distant.

Contribution de Jose Villalobos, ingénieur TAC Cisco.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- CUCM
- Certificats CUCM
- Services téléphoniques

Components Used

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- CUCM 10.5.X/CUCM 11.X
- Les téléphones SCCP (Skinny Client Control Protocol) et SIP (Session Initiation Protocol) s'enregistrent auprès de CUCM
- Ces travaux pratiques utilisent des certificats SAN (Subject Alternative Name).
- Le répertoire externe se trouve sur les certificats SAN.
- Pour tous les systèmes de cet exemple, l'autorité de certification (AC) sera identique, tous les certificats utilisés sont des signes CA.
- Le serveur DNS (Domain Name Server) et le protocole NTP (Network Time Protocol) doivent être configurés et fonctionner.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est actif, assurez-vous de bien comprendre l'impact potentiel de tout changement.

Produits connexes

Ce document peut également être utilisé avec les versions de matériel et de logiciel suivantes :

- CUCM 9.X/10.X/11.X

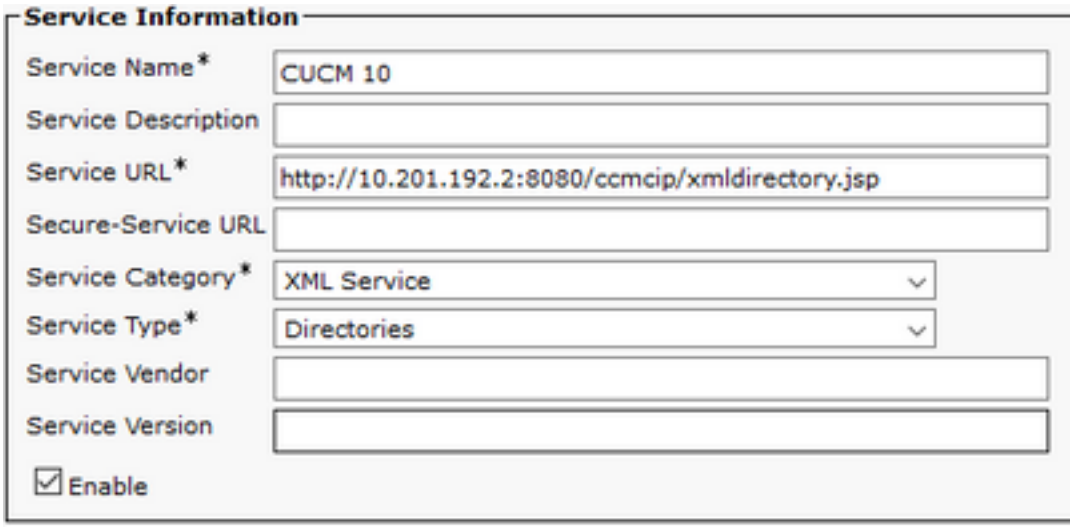
Configuration Steps

Étape 1. Configurez l'URL du service sur le système.

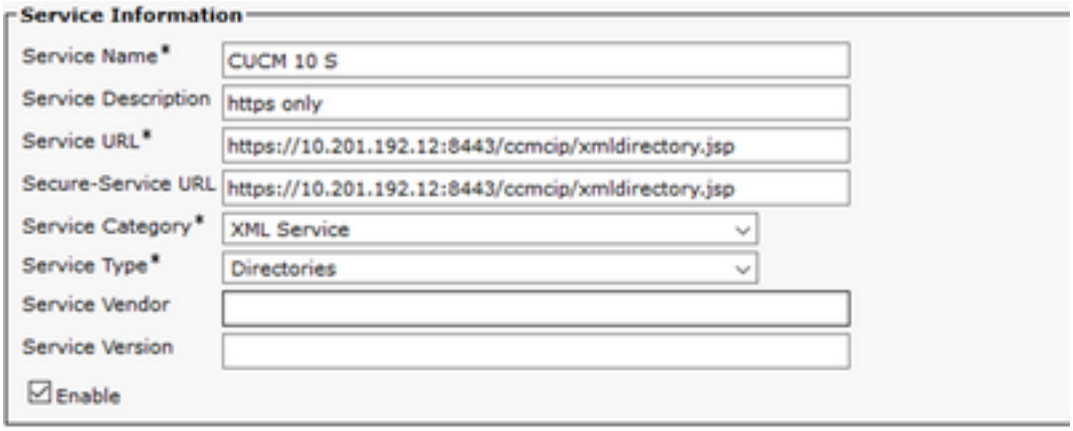
Configurez les protocoles HTTP (Hyper Text Transfer Protocol) et HTTPS (Hypertext Transfer Protocol Secure) comme preuve de concepts. L'idée finale est d'utiliser uniquement le trafic HTTP sécurisé.

Accédez à **Device > Device Settings > Phone service > Add new**

HTTP uniquement



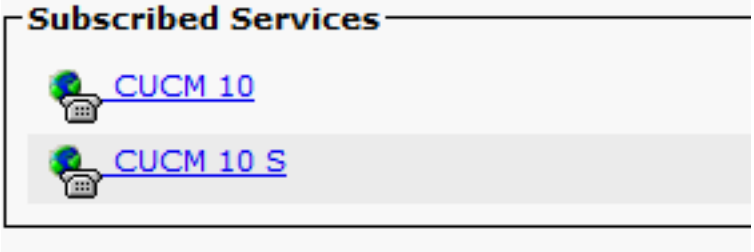
HTTPS uniquement



Avertissement : si vous ajoutez la vérification pour l'**abonnement Entreprise,** l'étape 2 peut être ignorée. Cependant, cette modification réinitialise tous les téléphones, assurez-vous de bien comprendre l'impact potentiel.

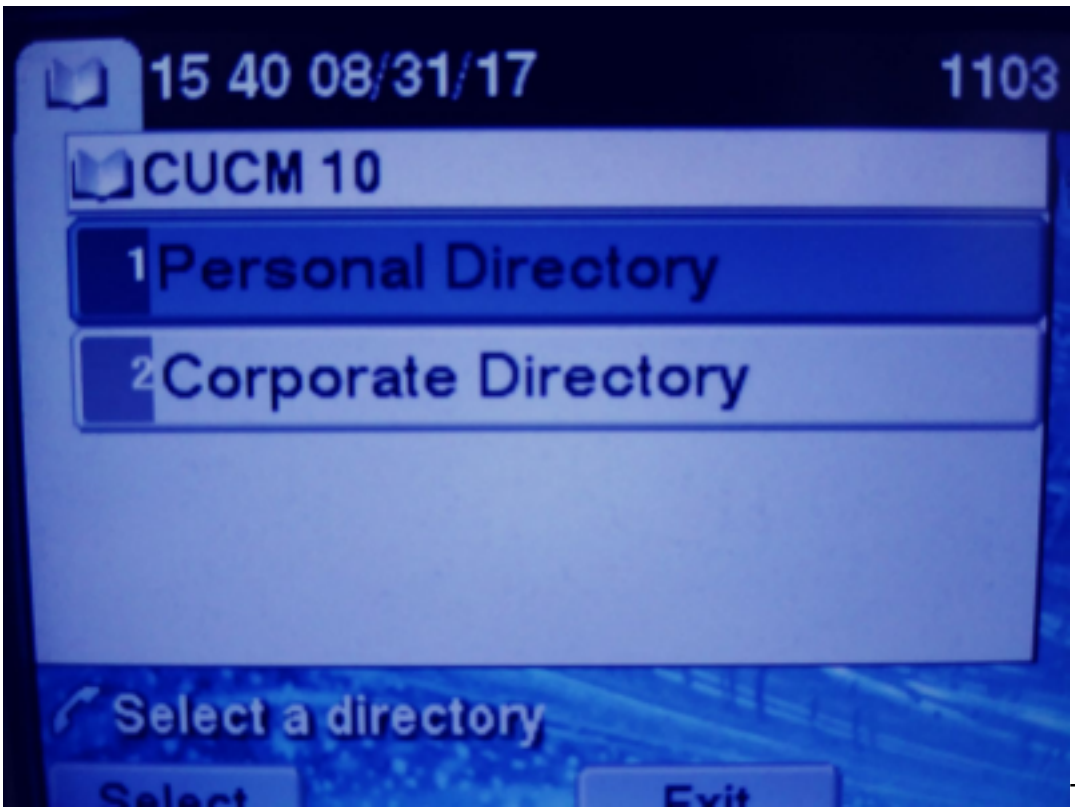
Étape 2. Abonnez les téléphones aux services.

Accédez à **Device>Phone »Subscriber/Unsubscribe service.**



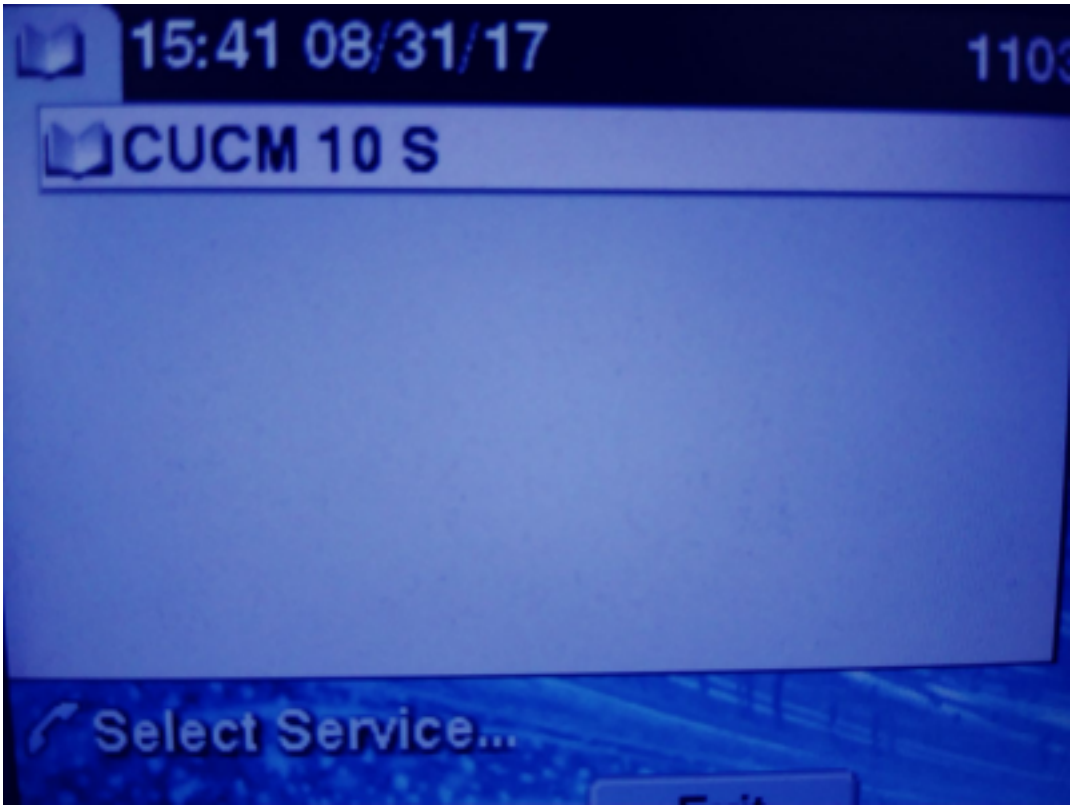
Àce stade, si l'application offre HTTP, vous devez être en mesure d'atteindre le service, mais https n'est toujours pas actif.

HTTP



TTP

HTTPS



HTTPS affichera un hôte " introuvable " erreur en raison du fait que le service TVS ne peut pas authentifier ceci pour le téléphone.

Étape 3. Téléchargez les certificats de service externe vers CUCM.

Téléchargez le service externe en tant que **approbation Tomcat uniquement**. Vérifiez que les services sont réinitialisés sur tous les noeuds.

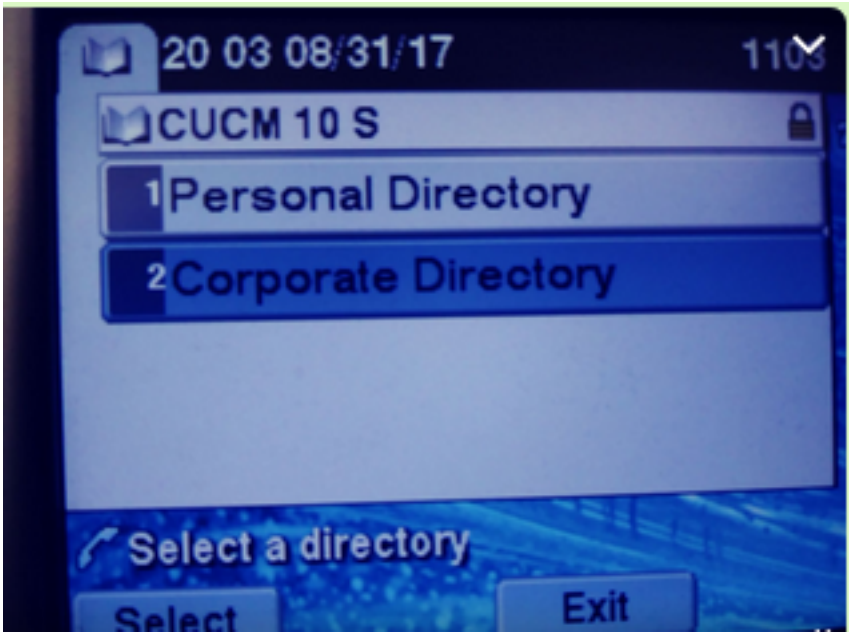
Ce type de certificat n'est pas stocké sur le téléphone, mais le téléphone doit vérifier auprès du service TVS pour voir s'il établit la connexion HTTPS.

Accédez à **OS admin> Certificate> Certificate upload.**

Àpartir de SSH, réinitialisez le service CUCM Tomcat sur tous les noeuds.

```
admin:utils service restart Cisco Tomcat
Do not press Ctrl+C while the service is restarting. If the service has not rest
arted properly, execute the same command again.
Service Manager is running
```

Après ces étapes, les téléphones doivent pouvoir accéder au service HTTPS sans problème



Foire aux questions (FAQ)

Une fois les certificats échangés, HTTPS échoue toujours avec « hôte introuvable ».

- Vérifiez le noeud sur lequel le téléphone est enregistré et assurez-vous que le certificat tiers apparaît sur le noeud.

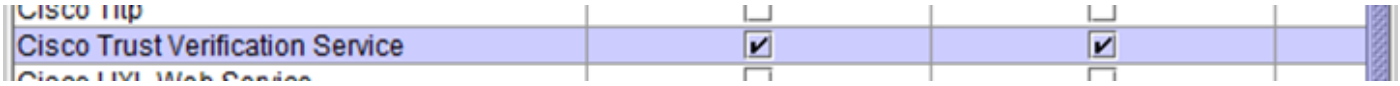
- Réinitialisez le tomcat sur le noeud spécifique.

- Vérifiez DNS, assurez-vous que le nom commun (CN) du certificat peut être résolu.

Dépannage

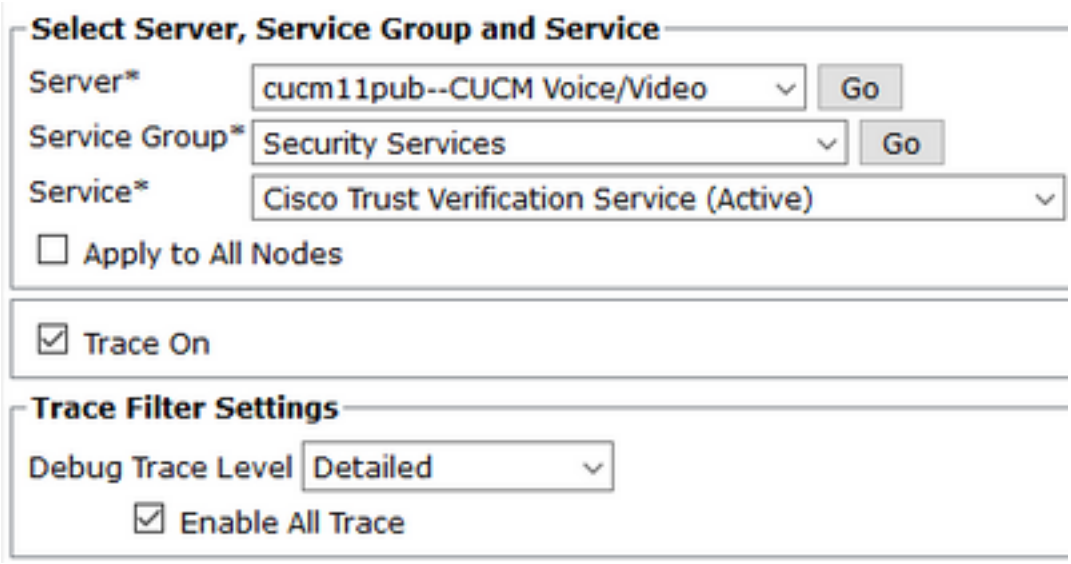
Collecter les journaux CUCM TVS doit vous fournir de bonnes informations

Accédez à **RTMT>System>Trace & log Central > Collecter les fichiers journaux**



> **Note**: Collectez les journaux de tous les noeuds et assurez-vous que les journaux TVS sont définis sur détaillés.

Journaux TVS définis en détail



Exemple de suivi

```
11:17:38.291 |   debug CTVSChangeNotifyServer::ProcessChangeNotification () -
CDBString=<msg><type>DBL</type><table>certificate</table><tableid>46</tableid><action>I</action>
<user>repl</user><time>1504203458</time><new><cdrserver>2</cdrserver><cdrtime>1504203457</cdrtim
e><pkid>e6148ee3-3eb5-e955-fa56-
2baa538a88fb</pkid><servername>cucm11pub</servername><subjectname>CN=10.201.192.12,OU=RCH,O=Cisc
o,L=RCH,ST=Tx,C=US</subjectname><issuername>CN=pablogon-
CA,DC=rcdncollab,DC=com</issuername><serialnumber>3d00000008230ded92f687ec03000000000008</serial
number><certificate></certificate><ipv4address>10.201.192.13</ipv4address><ipv6address></ipv6add
ress><timetolive>NULL</timetolive><tkcertificatedistribution>1</tkcertificatedistribution><ifx_r
eplcheck>6460504654345273346</ifx_replcheck></new></msg>
11:17:38.291 |   debug CTVSChangeNotifyServer::ProcessChangeNotification () - Database table
"certificate" has been changed
11:17:38.291 |   debug CTVSChangeNotifyServer::ProcessChangeNotification () - Looking up the
roles for
11:17:38.291 |   debug Pkid : fead9987-66b5-498f-4e41-c695c54fac98
11:17:38.291 |   debug CTVSChangeNotifyServer::ProcessThreadProc () - Waiting for DBChange
Notification
11:17:38.300 |   debug CTVSChangeNotifyServer::ProcessThreadProc () - DBChange Notification
received
11:17:38.300 |   debug CTVSChangeNotifyServer::ProcessChangeNotification () -
CDBString=<msg><type>DBL</type><table>certificatetrustrolemap</table><tableid>50</tableid><actio
n>I</action><user>repl</user><time>1504203458</time><new><cdrserver>2</cdrserver><cdrtime>150420
3457</cdrtime><pkid>5ae6e1d2-63a2-4590-bf40-1954bfa79a2d</pkid><fkcertificate>e6148ee3-3eb5-
e955-fa56-
2baa538a88fb</fkcertificate><tktrustrole>7</tktrustrole><ifx_replcheck>6460504654345273346</ifx_
replcheck></new></msg>
11:17:38.300 |   debug CTVSChangeNotifyServer::ProcessChangeNotification () - Database table
"certificatetrustrolemap" has been changed
11:17:38.300 |   debug CTVSChangeNotifyServer::ProcessThreadProc () - Waiting for DBChange
Notification
11:17:46.811 |   debug updateLocalDBCache : Refreshing the local DB certificate cache
11:34:00.131 |   debug Return value after polling is 1
11:34:00.131 |   debug FD_ISSET i=0, SockServ=14

11:34:00.131 |   debug Accepted TCP connection from socket 0x00000014
```