Guide de Comment-Faire complet de Jabber pour la validation de certificat

Contenu

Introduction

Ce document combine plusieurs ressources en Cisco dans un complet, unifié comment-au guide qui est utilisé afin d'implémenter toutes les conditions requises pour la validation de certificat dans le Cisco Jabber. C'est nécessaire parce que le Cisco Jabber exige maintenant de l'utilisation de la validation de certificat afin d'établir des connexions sécurisées avec des serveurs. Cette condition requise nécessite beaucoup de modifications qui pourraient être exigées pour des environnements de l'utilisateur.

> Remarque: Ce guide est pour des déploiements de sur-site seulement. Il n'y a actuellement aucune modification exigée pour des déploiements de service en nuage, parce qu'ils sont validés contre l'Autorité de certification (CA) public.

Quels clients de Jabber sont affectés par cette modification ?

Voici un tableau qui présente tous les clients qui implémentent la validation de certificat :

Tableau 1 :

Clients de bureau	Clients de mobile et de tablette
Jabber pour la version 9.2 (septembre 2013) de Macintosh Jabber pour la version 9.2.5 (septembre 2013) de Microsoft (MS) Windows	Jabber pour la version 9.5 (octobre 2013) d'iP Jacassez pour la version 9.6 (novembre 2013 d'iPhone et d'iPad Jabber pour la version 9.6 (décembre 2013) d'Android

Que fait ce moyen pour l'environnement de Jabber ?

Quand vous installez ou mise à jour sur n'importe quel client répertorié dans le **tableau 1**, la validation obligatoire de certificat avec des serveurs est utilisée pour des connexions sécurisées. Essentiellement, quand la tentative de clients de Jabber d'établir une connexion sécurisée maintenant, des serveurs présentent le Cisco Jabber avec des Certificats. Tentatives de Cisco Jabber puis de valider ces Certificats contre le stock de certificat du périphérique. Si le client ne peut pas valider le certificat, il vous incite à confirmer que vous voulez recevoir le certificat, et le placez dans sa mémoire de confiance d'entreprise.

Quels Certificats sont exigés ?

Voici une liste de serveurs de sur-site et les Certificats qu'elles présentent au Cisco Jabber afin d'établir une connexion sécurisée :

Tableau 2

Serveur	Certificat
Cisco Unified Presence	HTTP (Tomcat) XMPP
Cisco Unified Communications Manager IM et présence	HTTP (Tomcat) XMPP
Cisco Unified Communications Manager	HTTP (Tomcat)
Cisco Unity Connection	HTTP (Tomcat)
Serveur de téléconférences de Cisco WebEx	HTTP (Tomcat)

Voici quelques points importants à noter :

- Appliquez la mise à jour de service la plus récente (SU) pour le Cisco Unified Presence (TASSE) ou le Cisco Unified Communications Manager (CUCM) IM et présence avant que vous commenciez le processus de signature de certificat.
- Les Certificats exigés s'appliquent à toutes les versions serveur. Par exemple, version 8.x de TASSE et CUCM IM et présent de version 9.x et ultérieures de présence le client avec la Messagerie et la présence Protocol (XMPP) et les Certificats extensibles de HTTP.
- Chaque noeud dans une batterie, des abonnés et des éditeurs, dirige un service de Tomcat et peut présenter le client avec un certificat de HTTP. Prévoyez de signer les Certificats pour chaque noeud dans la batterie.
- Afin de sécuriser le Protocole SIP (Session Initiation Protocol) signalant entre le client et le CUCM, inscription de la fonction de proxy d'autorité de certification d'utilisation (CAPF).

Quelles méthodes sont disponibles pour la validation de certificat

?

Il y a actuellement plusieurs méthodes de validation de certification qui peuvent être utilisées.

Méthode 1 : Le clic d'utilisateurs simplement **reçoivent à** tous les popups de certificat. Ceci pourrait être la solution la plus idéale pour de plus petits environnements. Si vous clic **recevez**, des Certificats sont placés dans la mémoire de confiance d'entreprise sur le périphérique. Après que des Certificats soient placés dans la mémoire de confiance d'entreprise, des utilisateurs ne sont plus incités quand ils se connectent dans le client de Jabber sur ce périphérique local.

Méthode 2 : Les Certificats requis (le **tableau 2)** sont téléchargés des différents serveurs (par défaut, ce sont les Certificats auto-signés) et sont installés dans le stock de confiance d'entreprise du périphérique d'utilisateur. Ceci pourrait être la solution idéale si votre environnement n'a pas l'accès à un privé ou le public CA pour la signature de certificat.

Plusieurs méthodes peuvent être utilisées afin de pousser ces Certificats aux utilisateurs, mais une méthode rapide est d'utiliser l'utilisation du registre de Microsoft Windows :

1. D'un des ordinateurs, recevez tous les Certificats qui sont présentés pour jacasser dans la mémoire de confiance d'entreprise.
2. Afin de vérifier que les Certificats sont présents, sélectionnent la **commande Certmgr.msc** et naviguent vers EnterpriseTrust **> Certificats.**
3. Ouvrez **Regedit** avec une commande de **passage** et naviguez vers **HKCU > logiciel > Microsoft > SystemCertificates > confiance > Certificats**.
4. Cliquez avec le bouton droit et exportez le répertoire de Certifates dans le registre comme un fichier **.reg**.
5. Éliminez ce fichier par l'intermédiaire de l'objet de stratégie de groupe (GPO) à tous les utilisateurs (ou à toute autre méthode préférée).

Ceci se termine l'installer des Certificats de confiance d'entreprise pour le Jabber, et des utilisateurs ne sont plus incités.

Méthode 3 : Un public ou un CA privé (le **tableau 2)** signe tous les Certificats exigés. C'est la méthode recommandée de Cisco. Cette méthode exige qu'une demande de signature de certificat (CSR) est générée pour chacun des Certificats, est signée, re-téléchargée au serveur, et puis importée aux autorités de certificat racine de confiance la mémoire sur des périphériques d'utilisateur. Voyez le **générer un CSR** et **le comment j'obtiens des Certificats aux mémoires de certificat de périphériques d'utilisateur ?** sections de ce pour en savoir plus de document.

> Remarque: Dans le cas d'un public CA, le certificat racine devrait déjà être dans la mémoire de confiance de client.

Il est important de se souvenir que le public CAs exige typiquement de CSRs afin de se conformer aux formats spécifiques. Par exemple, un public CA pourrait seulement recevoir CSRs cela :

- Sont Base64-encoded
- Ne contenez pas certains caractères, tels que le @& ! , dans l'organisation, l'unité organisationnelle (OU), ou d'autres domaines
- Utilisez les longueurs de bit spécifiques dans la clé publique pour le serveur

De même, si vous soumettez CSRs des plusieurs noeuds, le public CAs pourrait avoir besoin de

que les informations sont cohérentes dans tout le CSRs.

Afin d'empêcher des questions avec votre CSRs, passez en revue les conditions requises de format du public CA auquel vous prévoyez de soumettre le CSRs. Assurez-vous alors que les informations que vous écrivez quand vous configurez votre serveur se conforme au format du lequel le public CA a besoin.

Voici une condition requise possible que vous pourriez rencontrer :

Un certificat par FQDN : Un certain signe CAs de public seulement un certificat par nom de domaine complet (FQDN).

Par exemple, afin de signer les Certificats de HTTP et XMPP pour un CUCM simple IM et le noeud de présence, vous pourriez devoir soumettre chaque CSR au public différent CAs.

Vérifiez si un certificat Auto-est signé ou Ca-signé

> Remarque: Cet exemple est pour la version 8.x CUCM. Le processus pourrait varier entre les serveurs.

1. Naviguez vers la **gestion de SYSTÈME D'EXPLOITATION de Cisco Unified**.
2. Choisissez la **Gestion de Sécurité > de certificat**.
3. Trouvez et cliquez sur le fichier du **certificat .pem de Tomcat-confiance**.
4. Cliquez sur Download, et **sauvegardez**.
5. Naviguez vers le fichier, et renommez-le avec l'extension de **.cer**.
6. Ouvrez et visualisez ce fichier (utilisateurs de MS Windows).
7. Vérifiez **émis par le** champ. S'il apparie **émis** pour mettre en place, alors le certificat Auto-est signé (voyez l'**exemple**).

Exemple : Auto-signé contre le certificat Ca-signé privé

Privé Auto-signé Ca-signé

Générez un CSR

> Remarque: Cet exemple est pour la version 8.x CUCM. Le processus pourrait varier entre les serveurs.

1. Naviguez vers la **gestion de SYSTÈME D'EXPLOITATION de Cisco Unified**.
2. Choisissez la **Gestion de Sécurité > de certificat**.
3. Cliquez sur **génèrent le CSR**, et choisissent **Tomcat de la** liste déroulante.
4. Le clic **génèrent le CSR**, et cliquent sur **étroitement**.
5. Cliquez sur Download le **CSR**, et choisissez **Tomcat de la** liste déroulante.
6. Cliquez sur Download le **CSR**, et sauvegardez le fichier.
7. Envoyez le fichier **.csr** à signer par votre serveur privé ou un public CA CA.
   Remarque: Une fois que vous avez ce fichier CSR, le processus varie basé sur votre environnement.

8. Cliquez sur Upload le **certificat/chaîne de certificat** sous le re-téléchargement de **Gestion de Sécurité > de certificat les** nouveaux Certificats signés qui ont été fournis à votre serveur.

Comment vont-ils les Certificats d'importation I dans des mémoires de certificat de périphérique d'utilisateur ?

Chaque certificat de serveur devrait avoir un certificat racine associé actuel dans la mémoire de confiance sur le périphérique d'utilisateur. Le Cisco Jabber valide les Certificats que les serveurs présents contre les certificats racine en confiance enregistrent.

Certificats racine d'importation dans la mémoire de certificat de MS Windows si :

- Les Certificats sont signés par un CA qui n'existe pas déjà dans la mémoire de confiance, telle qu'un CA privé. Si oui, vous devez importer le certificat de CA privé à la mémoire d'Autorités de certification racine approuvée.
- Les Certificats auto-sont signés. Si oui, vous devez importer les Certificats auto-signés à la mémoire de confiance d'entreprise.

Vous pouvez utiliser tous les Certificats d'importation appropriés de méthode dans la mémoire de certificat de MS Windows, comme :

- Utilisez les Certificats d'importation d'assistant d'importation de certificat individuellement.
- Déployez les Certificats vers des utilisateurs avec l'outil ligne de commande CertMgr.exe sur le serveur de MS Windows. (Cette option exige de vous d'utiliser l'outil de gestionnaire de certificat, CertMgr.exe, pas la console de gestion de MS de Certificats, CertMgr.msc.)
- Déployez les Certificats vers des utilisateurs avec un GPO sur le serveur de MS Windows.

  Remarque: Pour le mode d'emploi détaillé sur la façon dont aux Certificats d'importation, référez-vous à la documentation appropriée de MS.

Identité de serveur dans les Certificats

En tant qu'élément du processus de signature, le CA spécifie l'identité de serveur dans le certificat. Quand le client valide ce certificat, il vérifie cela :

- Une autorité de confiance a délivré le certificat.
- L'identité du serveur qui présente le certificat apparie l'identité du serveur spécifié dans le certificat.

  Remarque: Le public CAs a besoin généralement d'un FQDN comme identité de serveur, pas une adresse IP.

Champs d'identification

Le client vérifie ces champs d'identification dans les Certificats de serveur pour une correspondance d'identité :

Certificats XMPP

- SubjectAltName \ OtherName \ xmppAddr
- SubjectAltName \ OtherName \ srvName
- SubjectAltName \ dnsNames
- NC de sujet

Certificats de HTTP

- SubjectAltName \ dnsNames
- NC de sujet

  Remarque: Le champ NC de sujet peut contenir un masque (*) comme caractère extrême gauche ; par exemple, *.cisco.com. Votre CUCM, TASSE, et serveurs de Cisco Unity Connection ne pourraient pas prendre en charge des Certificats de masque. (Référez-vous à l'ID de bogue Cisco CSCta14114 d'amélioration).

Empêchez la non-concordance d'identité

Quand les tentatives d'un client de Jabber de se connecter à un serveur à une adresse IP, et le certificat de serveur identifie le serveur avec un FQDN, le client ne peut pas identifier le serveur comme fait confiance et incite l'utilisateur. Ainsi, si vos Certificats de serveur identifient les serveurs avec des FQDN, vous devez spécifier le nom du serveur comme FQDN dans beaucoup d'endroits sur vos serveurs.

Le tableau 3 répertorie tous les endroits qui doivent spécifier le nom du serveur pendant qu'il apparaît dans le certificat, si c'est une adresse IP ou un FQDN.

Tableau 3

Serveur	Emplacement (la configuration doit apparier le certificat)
Clients de Cisco Jabber	Adresse du serveur de procédure de connexion (diffère pour des clients, normalement sous des **paramètres de connexion)** ** Tous les noms du noeud (**système > topologie de batterie)** ** **Attention** : Assurez-vous que si vous changez ceci au FQDN, vous pouvez résoudre ceci par l'intermédiaire des DN ou les serveurs restent dans l'état démarrant !
TASSE (version 8.x et antérieures)	Serveurs TFTP (**application > Cisco Jabber > configurations)** Téléphone IP primaire et secondaire de Cisco de Cisco Call manager (CCMCIP (**application > Cisco Jabber > profil CCMCIP)** Nom d'hôte de messagerie vocale (**serveur d'application > de Cisco Jabber > d messagerie vocale)** Nom de Mailstore **(application > Cisco Jabber > Mailstore)** Nom d'hôte de Conférences (**serveur d'application > de Cisco Jabber > de Conférences)** (lieu de rencontre seulement) Domaine XMPP (voyez le **domaine de la fourniture XMPP à la** section de **client**
CUCM IM et présence (version 9.x et ultérieures)	** Tous les noms du noeud **(système > topologie de batterie**) ** **Attention** : Assurez-vous que si vous changez ceci au FQDN, vous pouvez résoudre ceci par l'intermédiaire des DN ou les serveurs restent dans l'état démarrant !

CUCM (version 8.x et antérieures)	Serveurs TFTP (**application > clients existants > configurations)** CCMCIP primaire et secondaire **(application > clients existants > profil CCMCIF** Domaine XMPP (voyez le **domaine de la fourniture XMPP à la** section de **client** Nom du serveur (**System > Server)**
CUCM (version 9.x et ultérieures)	Nom du serveur **(System > Server)** IM et Presence Server (**gestion des utilisateurs > paramètres utilisateurs > serv UC > IM et présence)** Nom d'hôte de messagerie vocale **(gestion des utilisateurs > paramètres utilisat > service > messagerie vocale UC)** Nom de Mailstore **(gestion des utilisateurs > paramètres utilisateurs > service > Mailstore UC)** Nom d'hôte de Conférences (**(gestion des utilisateurs > paramètres utilisateurs service UC > Conférences)** (lieu de rencontre seulement)
Cisco Unity Connection (toutes les versions)	**Aucune modification requise**

Fournissez le domaine XMPP aux clients

Le client identifie des Certificats XMPP avec le domaine XMPP, plutôt qu'avec le FQDN. Les Certificats XMPP doivent contenir le domaine XMPP dans un champ d'identification.

Quand les tentatives de client de se connecter au serveur de présence, le serveur de présence fournit le domaine XMPP au client. Le client peut alors valider l'identité du serveur de présence contre le certificat XMPP.

Terminez-vous ces étapes afin de s'assurer que le serveur de présence fournit le domaine XMPP au client :

1. Ouvrez l'interface de gestion pour votre serveur de présence, le **Cisco Unified CM IM et interface de gestion de présence** ou l'**interface de gestion de Cisco Unified Presence**.
2. Naviguez vers le **système > la Sécurité > les configurations**.
3. Localisez la section de **configurations de certificat XMPP**.
4. Spécifiez le domaine de serveur de présence dans le **nom de domaine pour la** zone d'**identification alternative de sujet de certificat de Serveur-à-serveur XMPP**.
5. Cochez le **nom de domaine d'utilisation pour la** case **alternative de nom de sujet de certificat XMPP**.
6. Cliquez sur **Save**.
7. Après que vous sauvegardiez cette modification, vous devez régénérer le certificat de **tasse-xmpp** sur le serveur.
8. Redémarrez le **routeur XCP** pour que la modification la prenne effet.

Attention : Une reprise du routeur XCP affecte le service.

La validation de certificat est maintenant complète !

Informations connexes

- Cisco Jabber 9.2.5 notes de mise à jour

- Cisco Jabber : Validation obligatoire TechNote de certificat de serveur
- Support et documentation techniques - Cisco Systems