Créer de nouveaux certificats à partir de certificats CA signés

Table des matières

Introduction Conditions préalables Exigences Composants utilisés Informations de pré-vérification Configuration et régénération des certificats Certificat Tomcat Certificat CallManager Certificat IPSec Certificat CAPF Certificat TVS Dépanner les messages d'erreur de certificat téléchargés courants Le certificat CA n'est pas disponible dans le Trust-Store Le fichier /usr/local/platform/.security/tomcat/keys/tomcat.csr n'existe pas Clé publique CSR et clé publique de certificat ne correspondent pas Le nom alternatif de l'objet CSR (SAN) et le certificat SAN ne correspondent pas Les certificats de confiance avec le même CN ne sont pas remplacés

Introduction

Ce document décrit comment régénérer les certificats signés par une autorité de certification (CA) dans Cisco Unified Communications Manager (CUCM).

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- · Outil de surveillance en temps réel (RTMT)
- Certificats CUCM

Composants utilisés

• CUCM versions 10.x, 11.x et 12.x.

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 en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Informations de pré-vérification

Remarque : pour la régénération des certificats auto-signés, reportez-vous au <u>Guide</u> de régénération des certificats. Pour la régénération de certificat multi-SAN signé par l'autorité de certification, reportez-vous au <u>Guide de régénération de certificat multi-SAN</u>

Pour comprendre l'impact de chaque certificat et sa régénération, reportez-vous au <u>Guide de</u> <u>régénération auto-signé</u>.

Chaque type de demande de signature de certificat (CSR) a différentes utilisations de clé et celles-ci sont requises dans le certificat signé. Le <u>Guide de sécurité</u> inclut un tableau avec les utilisations de clés requises pour chaque type de certificat.

Pour modifier les paramètres d'objet (emplacement, état, unité d'organisation, etc.), exécutez cette commande :

• set web-security orgunit orgname locality state [country] [alternatehostname]

Le certificat Tomcat est régénéré automatiquement après l'exécution de la commande Tomcat_{set} web-security. Le nouveau certificat auto-signé n'est pas appliqué, sauf si le service Tomcat est redémarré. Reportez-vous à ces guides pour plus d'informations sur cette commande :

- Guide de référence de la ligne de commande
- Lien vers les étapes de la communauté Cisco
- <u>Vidéo</u>

Configuration et régénération des certificats

Les étapes de régénération des certificats de noeud unique dans un cluster CUCM signé par une autorité de certification sont répertoriées pour chaque type de certificat. Il n'est pas nécessaire de régénérer tous les certificats du cluster s'ils n'ont pas expiré.

Certificat Tomcat

Attention : vérifiez que l'authentification unique est désactivée dans le cluster (CM Administration > System > SAML Single Sign-On). Si l'authentification unique est activée, elle doit être désactivée, puis activée une fois le processus de régénération de certificat Tomcat terminé.

Sur tous les noeuds (CallManager et IM&P) du cluster :

Étape 1. Naviguez jusqu'à la date d'expiration du certificat Tomcat, Cisco Unified OS Administration > Security > Certificate Management > Find puis vérifiez-la.

Étape 2. Cliquez surGenerate CSR > Certificate Purpose: tomcat. Sélectionnez les paramètres souhaités pour le certificat, puis cliquez surGenerate. Attendez que le message de réussite s'affiche et cliquez surClose.

Generate Certificate Signing Request				
💽 Generate 🖳 Close				
Status	est Generated			
- Generate Certificate Signing Reque	st .			
Certificate Purpose**	tomcat			
Distribution *	115pub			
Common Name*	11Spub			
Subject Alternate Names (SANs) Parent Domain				
Key Type**	RSA			
Key Length*	2048 ~			
Hash Algorithm*	SHA256 ~			
Generate Close	anding with "-ECDSA' is selected, the certificate/key type is Elliptic Curve (EC). Otherwise, it is RSA.			

Étape 3. Téléchargez le CSR. Cliquez sur Download CSR, sélectionnez Certificate Purpose: tomcat, et cliquez sur Download.

Download Certificate Signing Request				
Download CSR Close				
Status				
Certificate names not listed below do not have a corresponding CSR				
Download Certificate Signing Request				
Certificate Purpose" torncat v				
Download CSR Close				

Étape 4. Envoyez le CSR à l'autorité de certification.

Étape 5. L'autorité de certification renvoie au moins deux fichiers pour la chaîne de certificats signés. Téléchargez les certificats dans l'ordre suivant :

- Certificat d'autorité de certification racine comme tomcat-trust. Naviguez jusqu'à Certificate Management > Upload certificate > Certificate Purpose: tomcat-trust. Définir la description du certificat et parcourez le fichier de certificat racine.
- Certificat intermédiaire comme tomcat-trust (facultatif). Accédez à Certificate Management > Upload certificate > Certificate Purpose: tomcat-trust. Définissez la description du certificat et parcourez le fichier de certificat intermédiaire.

Remarque : certaines autorités de certification ne fournissent pas de certificat intermédiaire. Si seul le certificat racine a été fourni, cette étape peut être omise.

- Certificat CA signé en tant que tomcat. Accédez àCertificate Management > Upload certificate > Certificate Purpose: tomcat. Définissez la description du certificat et parcourez le fichier de certificat signé par l'autorité de certification pour le noeud CUCM actuel.
- Remarque : à ce stade, CUCM compare le CSR et le certificat CA signé chargé. Si les informations correspondent, le CSR disparaît et le nouveau certificat signé par l'autorité de certification est téléchargé. Upload Certificate Common Error Messages Si vous recevez un message d'erreur après le téléchargement du certificat, reportez-vous à la section.

Étape 6. Pour que le nouveau certificat soit appliqué au serveur, le service Cisco Tomcat doit être redémarré via l'interface de ligne de commande (en commençant par Publisher, puis les abonnés, un par un), utilisez la commande utils service restart Cisco Tomcat.

Pour valider que le certificat Tomcat est maintenant utilisé par CUCM, accédez à la page Web du noeud et sélectionnez _{Site Information} (Icône de verrouillage) dans le navigateur. Cliquez sur cette _{certificate} option et vérifiez la date du nouveau certificat.



👔 Certific	ate	
General	Details	Cent

This c	ertificate i Ensures th	s intended e identity of	for the fe	computer	urpose(s):
1	ssued to:	115put			
1	ssued by:				
١	/alid from	9/16/2020	to 9/16/	2022	
					Issuer Statement

Certificat CallManager

Attention : ne régénérez pas les certificats CallManager et TVS en même temps. Cela entraîne une non-correspondance irrécupérable avec l'ITL installé sur les points d'extrémité, ce qui nécessite la suppression de l'ITL de TOUS les points d'extrémité du cluster. Terminez

×

Ie processus complet pour CallManager et, une fois les téléphones réenregistrés, démarrez le processus pour le TVS.

Remarque : pour déterminer si le cluster est en mode mixte, accédez à Cisco Unified CM Administration > System > Enterprise Parameters > Cluster Security Mode (0 == Non-Secure ; 1 == Mixed Mode).

Pour tous les noeuds CallManager du cluster :

Étape 1. Naviguez Cisco Unified OS Administration > Security > Certificate Management > Find jusqu'à la date d'expiration du certificat CallManager et vérifiez-la.

Étape 2. Cliquez surGenerate CSR > Certificate Purpose: CallManager. Sélectionnez les paramètres souhaités pour le certificat, puis cliquez surGenerate. Attendez que le message de réussite s'affiche et cliquez surClose.

Étape 3. Téléchargez le CSR. Cliquez sur Download CSR. Select Certificate Purpose: CallManager and click Download.

Étape 4. Envoyez le CSR à l' Certificate Authority .

Étape 5. L'autorité de certification renvoie au moins deux fichiers pour la chaîne de certificats signés. Téléchargez les certificats dans l'ordre suivant :

- Certificat d'autorité de certification racine comme CallManager-trust. Accédez àCertificate Management > Upload certificate > Certificate Purpose: CallManager-trust. Définissez la description du certificat et parcourez le fichier de certificat racine.
- Certificat intermédiaire en tant que CallManager-trust (facultatif). Accédez àCertificate Management > Upload certificate > Certificate Purpose: CallManager-trust. Définissez la description du certificat et parcourez le fichier de certificat intermédiaire.

Remarque : certaines autorités de certification ne fournissent pas de certificat intermédiaire. Si seul le certificat racine a été fourni, cette étape peut être omise.

Certificat signé par l'autorité de certification comme CallManager. Accédez àCertificate Management
 > Upload certificate > Certificate Purpose: CallManager. Définissez la description du certificat et parcourez le fichier de certificat signé par l'autorité de certification pour le noeud CUCM actuel.

Remarque : à ce stade, CUCM compare le CSR et le certificat CA signé chargé. Si les informations correspondent, le CSR disparaît et le nouveau certificat signé par l'autorité de certification est téléchargé. Si vous recevez un message d'erreur après le téléchargement du certificat, reportez-vous à la section Messages d'erreur courants du téléchargement du certificat.

Étape 6. Si le cluster est en mode mixte, mettez à jour la CTL avant le redémarrage des services :

<u>Token</u> ou <u>Tokenless</u>. Si le cluster est en mode non sécurisé, ignorez cette étape et redémarrez les services.

Étape 7. Pour que le nouveau certificat soit appliqué au serveur, les services requis doivent être redémarrés (uniquement si le service s'exécute et est actif). Naviguez jusqu'à l'adresse :

- Cisco Unified Serviceability > Tools > Control Center Network Services > Cisco Trust Verification Service
- Cisco Unified Serviceability > Tools > Control Center Feature Services > Cisco TFTP
- Cisco Unified Serviceability > Tools > Control Center Feature Services > Cisco CallManager
- Cisco Unified Serviceability > Tools > Control Center Feature Services > Cisco CTIManager

Étape 8. Réinitialisez tous les téléphones :

Accédez àCisco Unified CM Administration > System > Enterprise Parameters > Reset. Une fenêtre contextuelle s'affiche avec l'instruction « Vous êtes sur le point de réinitialiser tous les périphériques du système ». Cette action ne peut pas être annulée. Continuer ? sélectionnez OK, puis cliquez sur Reset.

Remarque : surveillez l'enregistrement des périphériques via RTMT. Une fois que tous les téléphones se sont réinscrits, vous pouvez passer au type de certificat suivant.

Certificat IPSec

Attention : une tâche de sauvegarde ou de restauration ne doit pas être active lors de la régénération du certificat IPSec.

Pour tous les noeuds (CallManager et IM&P) du cluster :

Étape 1. Accédez à Cisco Unified OS Administration > Security > Certificate Management > Findet vérifiez la date d'expiration du certificat ipsec.

Étape 2. Cliquez sur Generate CSR > Certificate Purpose : ipsec. Sélectionnez les paramètres souhaités pour le certificat, puis cliquez sur Générer. Attendez que le message de réussite s'affiche, puis cliquez sur Fermer.

Étape 3. Téléchargez le CSR. Cliquez sur Download CSR. Sélectionnez Certificate Purpose ipsec et cliquez sur Download.

Étape 4. Envoyez le CSR à l'autorité de certification.

Étape 5. L'autorité de certification renvoie au moins deux fichiers pour la chaîne de certificats signés. Téléchargez les certificats dans l'ordre suivant :

- Certificat d'autorité de certification racine comme ipsec-trust. Accédez à Certificate Management > Upload certificate > Certificate Purpose : ipsec-trust. Définissez la description du certificat et parcourez le fichier de certificat racine.
- Certificat intermédiaire comme ipsec-trust (facultatif). Accédez à Certificate Management >

Upload certificate > Certificate Purpose : tomcat-trust. Définissez la description du certificat et parcourez le fichier de certificat intermédiaire.



 Certificat signé par l'autorité de certification en tant qu'ipsec. Accédez à Certificate Management > Upload certificate > Certificate Purpose : ipsec. Définissez la description du certificat et parcourez le fichier de certificat signé par l'autorité de certification pour le noeud CUCM actuel.

Remarque : à ce stade, CUCM compare le CSR et le certificat CA signé chargé. Si les informations correspondent, le CSR disparaît et le nouveau certificat signé par l'autorité de certification est téléchargé. Si vous recevez un message d'erreur après le téléchargement du certificat, reportez-vous à la section Messages d'erreur communs de téléchargement du certificat

Étape 6. Pour que le nouveau certificat soit appliqué au serveur, les services requis doivent être redémarrés (uniquement si le service s'exécute et est actif). Naviguez jusqu'à l'adresse :

- Cisco Unified Serviceability > Outils > Control Center Services réseau > Cisco DRF Master(Publisher)
- Cisco Unified Serviceability > Outils > Control Center Services réseau > Cisco DRF Local (Éditeur et Abonnés)

Certificat CAPF

Remarque : pour déterminer si le cluster est en mode mixte, accédez à Cisco Unified CM Administration > System > Enterprise Parameters > Cluster Security Mode (0 == Non-Secure ; 1 == Mixed Mode).

Remarque : le service CAPF s'exécute uniquement dans le serveur de publication et c'est le seul certificat utilisé. Il n'est pas nécessaire d'obtenir les noeuds d'abonné signés par une autorité de certification, car ils ne sont pas utilisés. Si le certificat a expiré dans les Abonnés et que vous souhaitez éviter les alertes de certificats expirés, vous pouvez régénérer les certificats CAPF des abonnés en tant que certificats auto-signés. Pour plus d'informations, consultez <u>Certificat CAPF auto-signé</u>.

Dans l'éditeur :

Étape 1. Accédez à Cisco Unified OS Administration > Security > Certificate Management > Find and verify the expiration date of the CAPF certificate.

Étape 2. Cliquez sur Generate CSR > Certificate Purpose : CAPF. Sélectionnez les paramètres

souhaités pour le certificat, puis cliquez sur Generate. Attendez que le message de réussite s'affiche et cliquez sur Close.

Étape 3. Téléchargez le CSR. Cliquez sur Download CSR. Sélectionnez Certificate Purpose CAPF et cliquez sur Download.

Étape 4. Envoyez le CSR à l'autorité de certification.

Étape 5. L'autorité de certification renvoie au moins deux fichiers pour la chaîne de certificats signés. Téléchargez les certificats dans l'ordre suivant :

- Certificat d'autorité de certification racine comme CAPF-trust. Accédez à Certificate Management > Upload certificate > Certificate Purpose : CAPF-trust. Définissez la description du certificat et parcourez le fichier de certificat racine.
- Certificat intermédiaire en tant que CAPF-trust (facultatif). Accédez à Certificate Management > Upload certificate > Certificate Purpose : CAPF-trust. Définissez la description du certificat et parcourez le fichier de certificat intermédiaire.

Remarque : certaines autorités de certification ne fournissent pas de certificat intermédiaire. Si seul le certificat racine a été fourni, cette étape peut être omise.

 Certificat CA signé en tant que CAPF. Accédez à Certificate Management > Upload certificate > Certificate Purpose : CAPF. Définissez la description du certificat et parcourez le fichier de certificat signé par l'autorité de certification pour le noeud CUCM actuel.

Remarque : à ce stade, CUCM compare le CSR et le certificat CA signé chargé. Si les informations correspondent, le CSR disparaît et le nouveau certificat signé par l'autorité de certification est téléchargé. Si vous recevez un message d'erreur après le téléchargement du certificat, reportez-vous à la section Messages d'erreur communs de téléchargement du certificat.

Étape 6. Si le cluster est en mode mixte, mettez à jour la CTL avant le redémarrage des services : <u>Token</u> ou <u>Tokenless</u>. Si le cluster est en mode non sécurisé, ignorez cette étape et redémarrez le service.

Étape 7. Pour que le nouveau certificat soit appliqué au serveur, les services requis doivent être redémarrés (uniquement si le service s'exécute et est actif). Naviguez jusqu'à l'adresse :

- Cisco Unified Serviceability > Tools > Control Center Network Services > Cisco Trust Verification Service (Tous les noeuds où le service s'exécute.)
- Cisco Unified Serviceability > Tools > Control Center Feature Services > Cisco TFTP (Tous les noeuds où le service s'exécute.)
- Cisco Unified Serviceability > Outils > Control Center Services de fonctionnalités > Fonction Cisco Certificate Authority Proxy (Publisher)

Étape 8. Réinitialisez tous les téléphones :

 Accédez à Cisco Unified CM Administration > System > Enterprise Parameters > Reset. Une fenêtre contextuelle s'affiche avec l'instruction « Vous êtes sur le point de réinitialiser tous les périphériques du système ». Cette action ne peut pas être annulée. Continuer ? sélectionnez OK, puis cliquez sur Réinitialiser.

Remarque : surveillez l'enregistrement des périphériques via RTMT. Une fois que tous les téléphones se sont réinscrits, vous pouvez passer au type de certificat suivant.

Certificat TVS

Attention : ne régénérez pas les certificats CallManager et TVS en même temps. Cela entraîne une non-correspondance irrécupérable avec l'ITL installé sur les points d'extrémité, ce qui nécessite la suppression de l'ITL de TOUS les points d'extrémité du cluster. Terminez le processus complet pour CallManager et, une fois les téléphones réenregistrés, démarrez le processus pour le TVS.

Pour tous les noeuds TVS du cluster :

Étape 1. Accédez à Cisco Unified OS Administration > Security > Certificate Management > Find et vérifiez la date d'expiration du certificat TVS.

Étape 2. Cliquez sur Generate CSR > Certificate Purpose : TVS. Sélectionnez les paramètres souhaités pour le certificat, puis cliquez sur Generate. Attendez que le message de réussite s'affiche et cliquez sur Close.

Étape 3. Téléchargez le CSR. Cliquez sur Download CSR. Sélectionnez Certificate Purpose TVS et cliquez sur Download.

Étape 4. Envoyez le CSR à l'autorité de certification.

Étape 5. L'autorité de certification renvoie au moins deux fichiers pour la chaîne de certificats signés. Téléchargez les certificats dans l'ordre suivant :

- Certificat d'autorité de certification racine comme TVS-trust. Accédez à Certificate Management > Upload certificate > Certificate Purpose : TVS-trust. Définissez la description du certificat et parcourez le fichier de certificat racine.
- Certificat intermédiaire de confiance TVS (facultatif). Accédez à Certificate Management > Upload certificate > Certificate Purpose : TVS-trust. Définissez la description du certificat et parcourez le fichier de certificat intermédiaire.

Remarque : certaines autorités de certification ne fournissent pas de certificat intermédiaire. Si seul le certificat racine a été fourni, cette étape peut être omise.

 Certificat CA signé comme TVS. Accédez à Certificate Management > Upload certificate > Certificate Purpose : TVS. Définissez la description du certificat et parcourez le fichier de certificat signé par l'autorité de certification pour le noeud CUCM actuel.

Remarque : à ce stade, CUCM compare le CSR et le certificat CA signé chargé. Si les informations correspondent, le CSR disparaît et le nouveau certificat signé par l'autorité de certification est téléchargé. Si vous recevez un message d'erreur après le téléchargement du certificat, reportez-vous à la section Messages d'erreur courants du téléchargement du certificat.

Étape 6. Pour que le nouveau certificat soit appliqué au serveur, les services requis doivent être redémarrés (uniquement si le service s'exécute et est actif). Naviguez jusqu'à l'adresse :

- Cisco Unified Serviceability > Tools > Control Center Feature Services > Cisco TFTP (Tous les noeuds où le service s'exécute.)
- Cisco Unified Serviceability > Tools > Control Center Network Services > Cisco Trust Verification Service (Tous les noeuds où le service s'exécute.)

Étape 7. Réinitialisez tous les téléphones :

 Accédez à Cisco Unified CM Administration > System > Enterprise Parameters > Reset. Une fenêtre contextuelle s'affiche avec l'instruction « Vous êtes sur le point de réinitialiser tous les périphériques du système ». Cette action ne peut pas être annulée. Continuer ? sélectionnez OK, puis cliquez sur Réinitialiser.

Remarque : surveillez l'enregistrement des périphériques via RTMT. Une fois que tous les téléphones se sont réinscrits, vous pouvez passer au type de certificat suivant.

Dépanner les messages d'erreur de certificat téléchargés courants

Cette section répertorie certains des messages d'erreur les plus courants lors du téléchargement d'un certificat signé par une autorité de certification.

Le certificat CA n'est pas disponible dans le Trust-Store

Cette erreur signifie que le certificat racine ou intermédiaire n'a pas été téléchargé sur le CUCM. Vérifiez que ces deux certificats ont été téléchargés en tant que trust-store avant le téléchargement du certificat de service.

Le fichier /usr/local/platform/.security/tomcat/keys/tomcat.csr n'existe pas

Cette erreur apparaît lorsqu'il n'existe pas de CSR pour le certificat (tomcat, callmanager, ipsec, capf, tvs). Vérifiez que le CSR a été créé avant et que le certificat a été créé en fonction de ce CSR. Points importants à garder à l'esprit :

• Un seul CSR par serveur et type de certificat peut exister. Cela signifie que si une nouvelle

RSE est créée, l'ancienne est remplacée.

- CUCM ne prend pas en charge les certificats génériques.
- Il n'est pas possible de remplacer un certificat de service actuellement en place sans un nouveau CSR.
- Une autre erreur possible pour le même problème est « Le fichier /usr/local/platform/upload/certs//tomcat.der n'a pas pu être chargé. » Cela dépend de la version de CUCM.

Clé publique CSR et clé publique de certificat ne correspondent pas

Cette erreur apparaît lorsque le certificat fourni par l'autorité de certification a une clé publique différente de celle envoyée dans le fichier CSR. Les raisons possibles sont :

- Le certificat incorrect (provenant peut-être d'un autre noeud) est chargé.
- Le certificat CA a été généré avec un CSR différent.
- Le CSR a été régénéré et a remplacé l'ancien CSR utilisé pour obtenir le certificat signé.

Pour vérifier la correspondance entre le CSR et la clé publique de certificat, plusieurs outils sont disponibles en ligne, tels que <u>SSL</u>.

O Check if a Certificate and a Private Key match

Check if a CSR and a Certificate match

Enter your Certificate:

TJ13aW4xMixDTJ1DRFAcQ049UHVIbGIJTIWS2V5JTWU2VydmIJ2XMsQ049U2Vy dmIJ2XMsQ049Q29uZmindXJhdGivbixEQ21Jb2xsYWIsREM96Xg/Y2VydGimaWNh dGVSZX2VY2F0aW9uTGI2dD9YYXNIP29IamVjdENsYXN2PWNSTERpc3RyaWJ1d6/v bi8vaW50MiG78ggrBgEFBQcBAQ58rjCBqrCBqAYIKwY8BQUHMAXGg2ts2GFw08v L0NOPUNv6GxhYUJyMENBLENOPUFJQ5xDTJ1QdWjsaWMiMjBL2XkIMJBT2XJ2WNI cyxDTJ1T2Xj2aWNicyxDTJ1D625maWd1cmF0aW9uLERDPWNv6GxHY0xEQ21teD9j QUNIcnRp2mIjYXRIP2Jhc2U/b2jq2WN0Q2xhc3M9Y2VydGimaWNhdGivbkF1d6/hv cmi0eTAh8gkrBgEEAY13FAIEFB4SAFcA2QBIAFMA2QByAHYA2QByMA0GC5QGSIb3 DQEBCwUAA4IBAQCfq2Bc28CMxkunQavdYaUi6DrfDpML5A/TYhisqW55x/bEQs 9LyqftmiddCmkoMPt0K4I2vMie4oTpKBYAQvbrApG001mWV5u+f1lo9PvYygWEyi. D+ve7rMp8sirVo1Tmhe/26in3lbm+0fwe5NuvCx3wN/dLRR3904KcaPCxsVLQ6Aw PtrivAz/Kk2GRhzqacd9fvLJUoWTKDj2QsladcgsI5cvFMz3B8f0MJGBNX16JGIQ yZ2br6Gm4pa4yIQfsUrcXxHYsIomecYeRheKu5kuPus0oEIVIWszJ0QMT7P4/Ww 28pT2TkrQd0DA2HJGuJP+yBa75QGGTZWVVg1 ----END CERTIFICATE----- The certificate and CSR do NOT match!

🕜 Certificate Hash:

684ad486131856ce0015d4b3e615e1ed 3b3bef6b8f590a493921661a4c4f62e9

🕜 CSR Hash:

635f45c1ebcd876526a3133d1ee73d9a8 4544876fdbc8dc3a4d8fed377dcc635

Enter your CSR:

q+hjgokSx+ogqVavFSNRdqTh0Giris1ga0pjSsGxOOLCqAzQhEARnEcGyanZzrK gSjTQhfBjStD2vDYyD3wgSiyhwNiqkMUI3tRD5qcSD7trfLGLs8hB9ySHqtaDA3 11wLjSQ4RKt2188EScILIB3DA02eg2o5Vw4rh5tP8r09er/CTWsXZtBfLOytvcDGk OGrdWZxLuaUV2u25jWTmLD70tCN/XCMI5XYpLJb6utyMLIf0DFh+s0P1Mr7gal3b hX8S4ZjoFIMKXYBWSPDwexH7XtD+HQaPeM4YS0N4YqhxAgMBAAGgbzBtBgkqhkiG 9w08CQ4xYDBeMB0GA1UdjQQWMBQGCCsGAQUFBwMBBggrBgEFBQcDAjALBgNVHQ8E BAMCBLAwMAYDVR0RBCkinj4iOY3Vjb55jb2xsYWIubXtCFTExNKB1Yt5jdWNtLmNv bGxhYt5teDANBgkqhkiG9w0BAQsFAA0CAQEAAhbgli76T59rWXtOFJsg7hsj36vf ubcW7HGPrNYt6/pI9UydunRtXkDxQTtz2WWc9tOA3xFpcjYz+8LdHtR1FnrwBWCV YcA9soNWZsmU1+clbTH1HSg8FFoHAdg+FR3+1AE7GNfGK0CA0RtpRih2PGzQ6dO 62TRSfQ4SLbCwxe4EZOSxjEQW7ZrkjfWby1GQKYg3CuXcEtrY3UunMCZrWymNxKg0 n7B1nNdx7rbgFz1teY+ZozPHWgbu2HwCHuH1bOAMUpkwtPebQ2n9H+R7drsjBAZR leXEYWL739M7BTveNmHoOnR6SkwVHYbb7jq0jntXxSy9R0S0S2vUhkj7Hw== ----END CERTIFICATE REQUEST----

Une autre erreur possible pour le même problème est « Le fichier

/usr/local/platform/upload/certs//tomcat.der n'a pas pu être chargé. » Cela dépend de la version de CUCM.

Le nom alternatif de l'objet CSR (SAN) et le certificat SAN ne correspondent pas

Les SAN entre le CSR et le certificat doivent être identiques. Cela empêche la certification pour les domaines qui ne sont pas autorisés. Pour vérifier la non-concordance du SAN, procédez comme suit :

1. Décoder le CSR et le certificat (base 64). Différents décodeurs sont disponibles en ligne, tels que le <u>Decoder</u>.

2. Comparez les entrées SAN et vérifiez qu'elles correspondent toutes. L'ordre n'est pas important, mais toutes les entrées du CSR doivent être identiques dans le certificat.

Par exemple, le certificat signé par une autorité de certification comporte deux entrées SAN supplémentaires, le nom commun du certificat et une adresse IP supplémentaire.

CSR Summary		Certificate Summary			
Subject domain.com			Subject		
RDN	Value		RDN	Value	
Common Name (CN)	pub-ms.domain.com		Common Name (CN)	pub-res.domain.com	
Organizational Unit (OU)	Collaboration		Organizational Unit (OU)	Collaboration	
Organization (O)	Cisco		Organization (0)	Cisco	
Locality (L)	CUCM		Locality (L)	CUCM	
State (ST)	CDMX		State (ST)	CDMX	
Country (C)	MX		Country (C)	MX	
Properties domain.com		Properties			
Property	Value		Property	Value	
Subject	CN = pub-ms.domsin.com,OU = Collaboration,O = Cisco,L = CUCM,ST = CDMX,C = MX		Issuer	CN = Collab CA,DC = collab,DC = mx	
Key Size	2048 bits		Subject	CN = pub-ms.domain.com,OU = Collaboration,O = Cisco,L = CUCM,ST = CDMX,C = MX	
Fingerprint (SHA-1)	C3 87 05 C8 79 F8 88 4A 86 96 77 0A C5 88 63 27 55 3C A4 84		Valid From	17 Sep 2020, 1:24 a.m.	
Fingerprint (MDS)	CE:5C:90:59:1F8EE1:26:C5:21:90:A2:F1:CA:68:86		Valid To	17 Sep 2022, 1:24 a.m.	
SANS	domain.com, sub.domain.com, pub.domain.com, imp.domain.com	L	Serial Number	69.00.00.20.5A.92.08.EA.9A.85.65.C4.00.00.00.00.20 (2341578246081205845683969935281333940237893677)	
		L	CA Cert	No	
			Key Size	2048 bits	
			Fingerprint (SHA-1)	4E:15 /7 / 3 :9C:37 A9:8D:52:1A (C:6D:4D:70:AF / E:08:88:80:07	
			Fingerprint (MDS)	08/22/33/92/50/F7.70/2A/05/28/00/2D/57/C0/F7/8C	
			SANS	pub-ms.domain.com, domain.com, sub.domain.com, pub.domain.com, imp.domain.com, 10.xx.xx.xx	

3. Une fois que vous avez identifié que le réseau SAN ne correspond pas, vous avez deux options pour résoudre ce problème :

- 1. Demandez à votre administrateur CA d'émettre un certificat avec les mêmes entrées SAN que celles envoyées dans le CSR.
- 2. Créez un CSR dans CUCM qui correspond aux exigences de l'autorité de certification.

Pour modifier le CSR créé par CUCM :

- 1. Si l'autorité de certification supprime le domaine, un CSR dans CUCM peut être créé sans le domaine. Lors de la création de CSR, supprimez le domaine qui est renseigné par défaut.
- 2. Si un <u>certificat Multi-SAN</u> est créé, il y a des CA qui n'acceptent pas les -ms dans le nom commun. L'option -ms peut être supprimée de la CSR lors de sa création.

Generate Certificate Signing Request				
Generate T Close				
Status				
Warning: Generating a new CSR for a specific certifi	cate type will overwrite the existing CSR for that type			
Generate Certificate Signing Request				
Certificate Purpose**	tomcat v			
Distribution*	Multi-server(SAN)			
Common Name*	11Spub-ms.			
Subject Alternate Names (SANs)				
Auto-populated Domains	115imp. 115pub. 115sub.			
Parent Domain				
Other Domains				
Key Type ** Key Length	RSA V			
Generate Close	SHA250			

- 3. Pour ajouter un autre nom en plus de ceux remplis automatiquement par CUCM :
 - 1. Si le certificat Multi-SAN est utilisé, d'autres noms de domaine complets peuvent être ajoutés. (Les adresses IP ne sont pas acceptées.)

enerate Certificate Signing F	lequest			
Generate 🖳 Close				
Status				
A Warning: Generating a new	CSR for a specific certificate type will ove	erwrite the existing CSR for that	type	
Generate Certificate Signing F	Request			
Certificate Purpose**	tomcat	v		
Distribution*	Multi-server(SAN)	~		
Common Name*	11Soub-ms			
Subject Alternate Names (SA	Ns)			
Auto-populated Domains	115imp. 115pub 115sub			
Descar Descala				
Parent Domain				
Other Domains	extraHostname.domain.com		Choose File For more info	
			🗄 Add	
Key Type**	RSA			
Key Length*	2048	×		
Hash Algorithm*	SHA256	~		

set web-securityb. Si le certificat est un noeud unique, utilisez la commande . Cette commande
 s'applique même aux certificats multi-SAN. (Tout type de domaine peut être ajouté, les adresses
 IP sont également autorisées.)

Pour plus d'informations, consultez le Guide de référence de la ligne de commande.

Les certificats de confiance avec le même CN ne sont pas remplacés

CUCM a été conçu pour stocker un seul certificat avec le même nom commun et le même type de certificat. Cela signifie que si un certificat tomcat-trust existe déjà dans la base de données et doit être remplacé par un certificat récent avec le même CN, CUCM supprime l'ancien certificat et le remplace par le nouveau.

Dans certains cas, CUCM ne remplace pas l'ancien certificat :

- 1. Le certificat téléchargé a expiré : CUCM ne vous permet pas de télécharger un certificat expiré.
- 2. L'ancien certificat a une date FROM plus récente que le nouveau certificat. CUCM conserve le certificat le plus récent, et la date FROM plus ancienne est cataloguée comme plus ancienne. Pour ce scénario, il est nécessaire de supprimer le certificat indésirable, puis de télécharger le nouveau.

Certificate	Certificate X
General Details Certification Path	General Details Certification Path
Certificate Information This certificate is intended for the following purpose(s):	Certificate Information This certificate is intended for the following purpose(s):
All issuance policies All application policies	Al issuance policies Al application policies
Old Certificate	New Certificate
Issued to: Colab CA	Issued to: Collab CA
Issued by: Colab CA	Issued by: Coliab CA
Valid from 7/23/2019 to 7/23/2024	Valid from 5/23/2019 to 12/23/2030
Issuer Statement	Issuer Statement
OK.	OK

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.