Configurer la gestion des certificats de la solution UCCX

Table des matières

- Introduction
- Conditions préalables
  - Exigences
    - FQDN, DNS et domaines
  - Composants utilisés
- Informations générales
- Configurer
  - Schéma de configuration
  - Certificats signés
    - Installer les certificats d'application Tomcat signés
  - Certificats auto-signés
    - Installation Sur Des Serveurs Périphériques
    - Régénération des certificats auto-signés
  - Intégration et configuration client
    - UCCX vers SocialMiner
    - Certificat client AppAdmin UCCX
    - Certificat client de la plate-forme UCCX
    - Certificat client du service de notification
    - Certificat client Finesse
    - Certificat client SocialMiner/CCP
    - Certificat client CUIC
  - Applications tierces accessibles à partir de scripts
- Vérifier
- Dépannage
  - Problème - ID utilisateur/mot de passe non valide
    - Causes
    - Solution
  - Problème - Le SAN CSR et le SAN de certificat ne correspondent pas
    - Causes
    - Solution
  - Problème - NET::ERR_CERT_COMMON_NAME_INVALID
    - Causes
    - Solution
    - Plus d'informations
- Défauts du certificat
- Informations connexes

Introduction

Ce document décrit comment configurer Cisco Unified Contact Center Express (UCCX) pour l'utilisation de certificats auto-signés et signés.

Conditions préalables

Exigences

Avant de poursuivre les étapes de configuration décrites dans ce document, assurez-vous que vous avez accès à la page Administration du système d'exploitation (OS) pour ces applications :

- UCCX
- SocialMiner/CCP

Un administrateur peut également avoir accès au magasin de certificats sur les PC client de l'agent et du superviseur.

FQDN, DNS et domaines

Tous les serveurs de la configuration UCCX doivent être installés avec des serveurs DNS (Domain Name System) et des noms de domaine. Il est également nécessaire que les agents, les superviseurs et les administrateurs accèdent aux applications de configuration UCCX via le nom de domaine complet (FQDN).

Si le domaine change ou est renseigné pour la première fois, les certificats peuvent être régénérés. Après avoir ajouté le nom de domaine à la configuration du serveur, régénérez tous les certificats Tomcat avant de les installer sur les autres applications, dans les navigateurs clients ou lors de la génération de la demande de signature de certificat (CSR) pour la signature.

Composants utilisés

Les informations décrites dans ce document sont basées sur les composants matériels et logiciels suivants :

- Services Web UCCX
- Service de notification UCCX
- Plate-forme UCCX Tomcat
- Cisco Finesse Tomcat
- Cisco Unified Intelligence Center (CUIC) Tomcat
- SocialMiner/CCP Tomcat

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 générales

Avec l'introduction de Finesse et CUIC co-résidents, l'intégration entre UCCX et SocialMiner pour

les e-mails et les chats, et l'utilisation de MediaSense afin d'enregistrer, de comprendre et d'installer des certificats via Finesse, la capacité à dépanner les problèmes de certificats est maintenant extrêmement importante.

Ce document décrit l'utilisation des certificats auto-signés et signés dans l'environnement de configuration UCCX qui couvre :

- Services de notification UCCX
- Services Web UCCX
- Scripts UCCX
- Corésident Finesse
- CUIC co-résident (données en direct et rapports historiques)
- SocialMiner (chat)

Les certificats, signés ou auto-signés, doivent être installés à la fois sur les applications (serveurs) de la configuration UCCX, ainsi que sur les postes de travail client de l'agent et du superviseur.

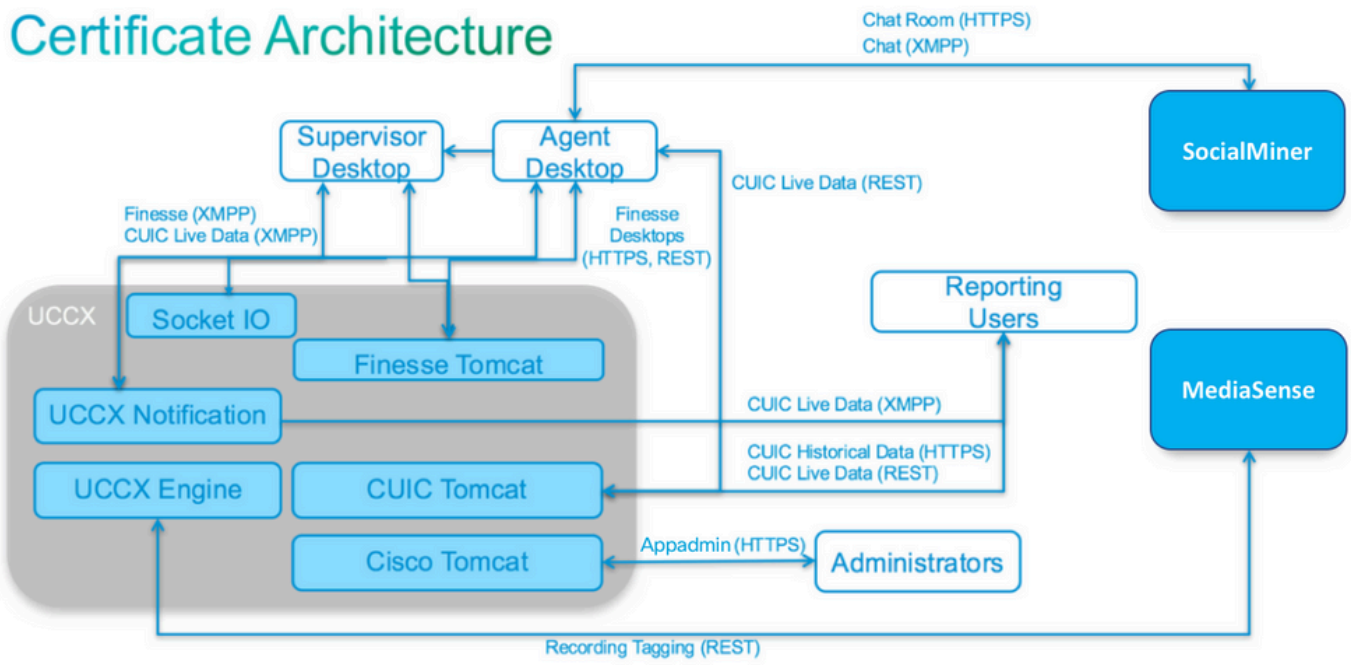
La prise en charge multi-SAN a été ajoutée dans UCCX à partir de la version 11.6.2.

Les certificats CA signés publiquement sur SomicalMiner/CCP sont requis pour que le chat externe fonctionne sur Internet.

Configurer

Cette section décrit comment configurer UCCX pour l'utilisation de certificats auto-signés et signés.

Schéma de configuration



Certificats signés

La méthode recommandée de gestion des certificats pour la configuration UCCX consiste à tirer parti des certificats signés. Ces certificats peuvent être signés par une autorité de certification interne ou par une autorité de certification tierce bien connue.

Dans les principaux navigateurs, tels que Mozilla Firefox et Microsoft Edge, les certificats racine des autorités de certification tierces bien connues sont installés par défaut. Les certificats des applications de configuration UCCX qui sont signés par ces autorités de certification sont approuvés par défaut, car leur chaîne de certificats se termine par un certificat racine qui est déjà installé dans le navigateur.

Le certificat racine d'une autorité de certification interne peut également être préinstallé dans le navigateur client par le biais d'une stratégie de groupe ou d'une autre configuration actuelle.

Vous pouvez choisir de faire signer les certificats de l'application de configuration UCCX par une autorité de certification tierce bien connue ou par une autorité de certification interne en fonction de la disponibilité et de la préinstallation du certificat racine pour les autorités de certification dans le navigateur client.

Installer les certificats d'application Tomcat signés

Effectuez ces étapes pour chaque noeud des applications UCCX Publisher and Subscriber, SocialMiner, MediaSense Publisher and Subscriber Administration :

1. Accédez à la page OS Administration et choisissez Security > Certificate Management.
2. Cliquez sur Generate CSR.
3. Dans la liste déroulante Certificate List, choisissez tomcat comme nom de certificat et cliquez sur Generate CSR.
4. Accédez à Security > Certificate Management et choisissez Download CSR.
5. Dans la fenêtre contextuelle, choisissez tomcat dans la liste déroulante et cliquez sur Download CSR.

Envoyez le nouveau CSR à l'autorité de certification tierce ou signez-le avec une autorité de certification interne, comme décrit précédemment. Ce processus peut produire les certificats signés suivants :

- Certificat racine pour l'autorité de certification
- Certificat d'application éditeur UCCX
- Certificat d'application d'abonné UCCX
- Certificat d'application SocialMiner/CCP

Remarque : Laissez le champ Distribution dans le CSR comme nom de domaine complet du serveur.

Remarque : Le certificat multiserveur (SAN) est pris en charge pour UCCX à partir de la

---

version 11.6. Cependant, le SAN peut inclure les noeuds UCCX 1 et 2 uniquement. D'autres serveurs, tels que SocialMiner, ne peuvent pas être inclus dans le SAN d'UCCX. Reportez-vous au bas de la page pour un exemple de SAN CUCM également valide pour UCCX.

Remarque : UCCX prend uniquement en charge les longueurs de clé de certificat de 1024 et 2048 bits.

Complétez ces étapes sur chaque serveur d'applications afin de télécharger le certificat racine et le certificat d'application vers les noeuds :

Remarque : Si vous téléchargez les certificats racine et intermédiaires sur un éditeur (UCCX ou MediaSense), ils peuvent être automatiquement répliqués sur l'abonné. Il n'est pas nécessaire de télécharger les certificats racine ou intermédiaires sur les autres serveurs non éditeurs de la configuration si tous les certificats d'application sont signés via la même chaîne de certificats.

1. Accédez à la page OS Administration et choisissez Security > Certificate Management.
2. Cliquez sur Upload Certificate.
3. Téléchargez le certificat racine et choisissez tomcat-trust comme type de certificat.
4. Cliquez sur Upload File.
5. Cliquez sur Upload Certificate.
6. Téléchargez le certificat d'application et choisissez tomcat comme type de certificat.
7. Cliquez sur Upload File.

   Remarque : Si une autorité de certification subordonnée signe le certificat, téléchargez le certificat racine de l'autorité de certification subordonnée en tant que certificat tomcat-trust au lieu du certificat racine. Si un certificat intermédiaire est émis, téléchargez ce certificat dans le magasin tomcat-trust en plus du certificat d'application.

8. Une fois terminé, redémarrez ces applications :
   - Éditeur et abonné Cisco MediaSense
   - Cisco SocialMiner
   - Éditeur et abonné Cisco UCCX

Remarque : Lorsque vous utilisez UCCX et SocialMiner 11.5, il existe un nouveau certificat appelé tomcat-ECDSA. Lorsque vous téléchargez un certificat tomcat-ECDSA signé sur le serveur, téléchargez le certificat d'application en tant que certificat tomcat-ECDSA et non en tant que certificat tomcat. Pour plus d'informations sur ECDSA, reportez-vous à la section Informations connexes pour obtenir le lien permettant de comprendre et de configurer les certificats ECDSA. Depuis la version 11.6, l'utilisation des certificats ECDSA a été complètement supprimée de la solution UCCX. Cela inclut UCCX, SM/CCP, CUIC et Finesse.

Certificats auto-signés

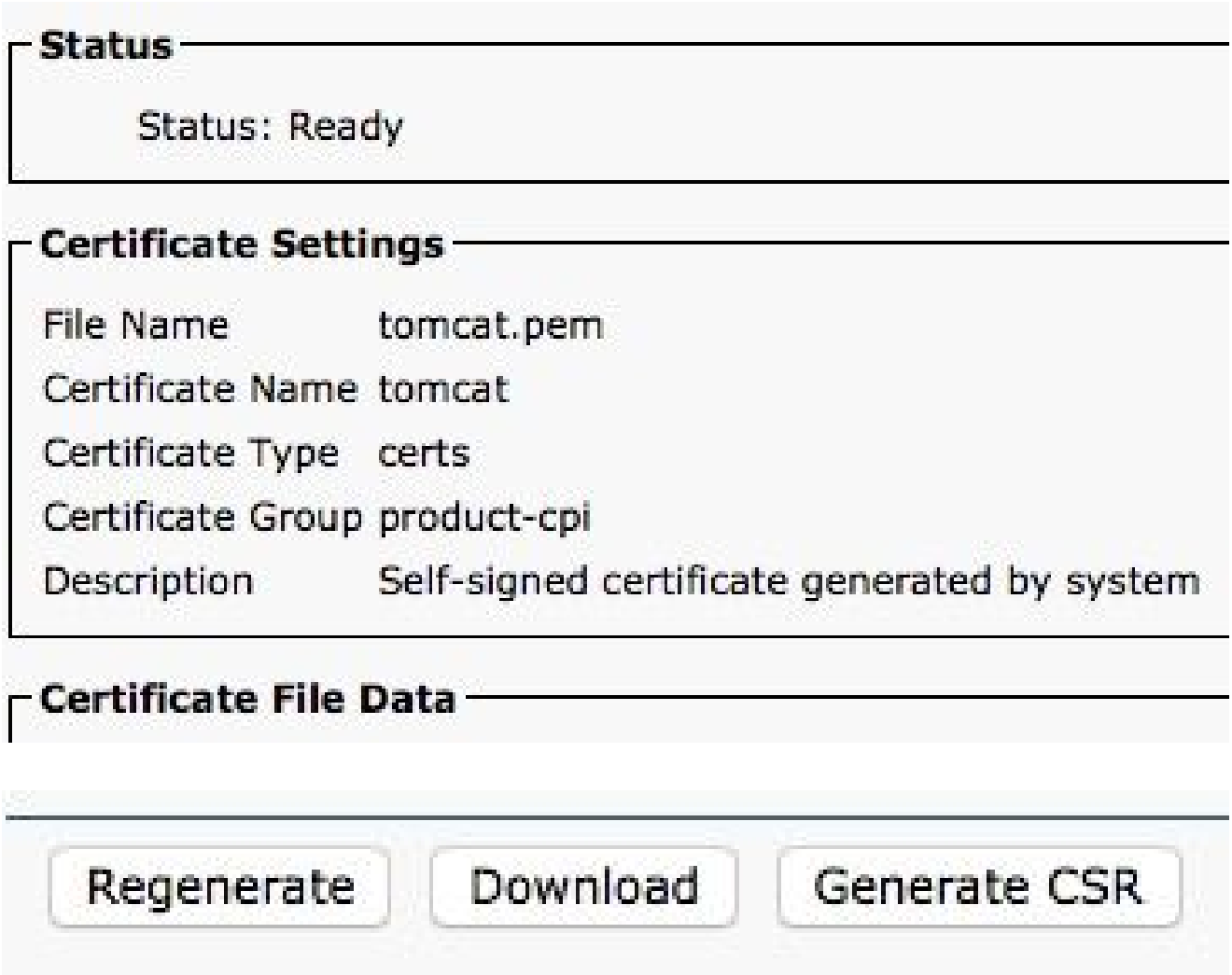
Installation Sur Des Serveurs Périphériques

Tous les certificats utilisés dans la configuration UCCX sont préinstallés sur les applications de configuration et sont auto-signés. Ces certificats auto-signés ne sont pas implicitement approuvés lorsqu'ils sont présentés à un navigateur client ou à une autre application de configuration. Bien qu'il soit recommandé de signer tous les certificats dans la configuration UCCX, vous pouvez utiliser les certificats auto-signés préinstallés.

Pour chaque relation d'application, vous devez télécharger le certificat approprié et le charger dans l'application. Complétez ces étapes afin d'obtenir et de télécharger les certificats :

1. Accédez à la page Application OS Administration et choisissez Security > Certificate Management.

2. Cliquez sur le fichier certificate.pem approprié et choisissez Download :



3. Afin de télécharger un certificat sur l'application appropriée, accédez à la page OS Administration et choisissez Security > Certificate Management.
4. Cliquez sur Télécharger le certificat / Chaîne de certificats :



5. Une fois terminé, redémarrez ces serveurs :

    - Cisco SocialMiner
    - Éditeur et abonné Cisco UCCX

Afin d'installer des certificats auto-signés sur l'ordinateur client, utilisez une stratégie de groupe ou un gestionnaire de package, ou installez-les individuellement dans le navigateur de chaque PC agent.

Pour Microsoft Edge, installez les certificats auto-signés côté client dans le magasin d'autorités de certification racine de confiance.

Pour Mozilla Firefox, procédez comme suit :

1. Accédez à Outils > Options.
2. Cliquez sur l'onglet Advanced.
3. Cliquez sur Afficher les certificats.
4. Accédez à l'onglet Serveurs.
5. Cliquez sur Ajouter une exception.

Régénération des certificats auto-signés

Si les certificats auto-signés expirent, ils doivent être régénérés et les étapes de configuration de l'installation sur les serveurs périphériques doivent être réexécutées.

1. Accédez à la page Application OS Administration et choisissez Security > Certificate Management.
2. Cliquez sur le certificat approprié et choisissez Régénérer.
3. Le serveur dont le certificat a été régénéré doit être redémarré.
4. Pour chaque relation d'application, vous devez télécharger le certificat approprié et le télécharger vers l'application à partir des étapes de configuration de la page Installation sur des serveurs périphériques.

Intégration et configuration client

UCCX vers SocialMiner

UCCX utilise les API REST et Notification de SocialMiner afin de gérer les contacts et la configuration des e-mails. Les deux noeuds UCCX doivent utiliser l'API REST de SocialMiner et être notifiés par le service de notification de SocialMiner. Installez donc le certificat SocialMiner Tomcat sur les deux noeuds UCCX.

Téléchargez la chaîne de certificats signée ou auto-signée du serveur SocialMiner vers le keystore UCCX tomcat-trust.

Téléchargez le certificat UCCX tomcat des noeuds Publisher et Subscriber sur le serveur SocialMiner en tant que keystore tomcat-trust.

Certificat client AppAdmin UCCX

Le certificat client AppAdmin UCCX est utilisé pour l'administration du système UCCX. Afin d'installer le certificat UCCX AppAdmin pour les administrateurs UCCX, sur le PC client, accédez à https://<UCCX FQDN>/appadmin/main pour chacun des noeuds UCCX et installez le certificat via le navigateur.

Certificat client de la plate-forme UCCX

Les services Web UCCX sont utilisés pour la transmission de contacts de discussion aux navigateurs clients. Afin d'installer le certificat de la plate-forme UCCX pour les agents et les superviseurs UCCX, sur le PC client, accédez à https://<UCCX FQDN>/appadmin/main pour chacun des noeuds UCCX et installez le certificat via le navigateur.

Certificat client du service de notification

Le service de notification CCX est utilisé par Finesse, UCCX et CUIC afin d'envoyer des informations en temps réel au bureau du client via le protocole XMPP (Extensible Messaging and Presence Protocol). Il est utilisé pour la communication Finesse en temps réel ainsi que pour les données CUIC Live.

Afin d'installer le certificat client du service de notification sur le PC des agents et superviseurs ou des utilisateurs de rapports qui utilisent Live Data, accédez à https://<UCCX FQDN>:7443/ pour chacun des noeuds UCCX et installez le certificat via le navigateur.

Certificat client Finesse

Le certificat client Finesse est utilisé par les bureaux Finesse afin de se connecter à l'instance Finesse Tomcat pour les besoins de la communication de l'API REST entre le bureau et le serveur Finesse co-résident.

Afin d'installer le certificat Finesse pour :

- Les agents et les superviseurs, sur le PC client, accédez à https://<UCCX FQDN>:8445/ pour chacun des noeuds UCCX et installez le certificat via les invites du navigateur.
- Les administrateurs Finesse, sur le PC client, accédez à https://<UCCX FQDN>:8445/cfadmin pour chacun des noeuds UCCX et installez le certificat via les invites du navigateur.

Certificat client SocialMiner/CCP

Le certificat SocialMiner Tomcat doit être installé sur l'ordinateur client. Une fois qu'un agent accepte une demande de discussion, le gadget de discussion est redirigé vers une URL qui représente la salle de discussion. Cette salle de discussion est hébergée par le serveur SocialMiner et contient l'utilisateur ou le contact de discussion.

Afin d'installer le certificat SocialMiner dans le navigateur, sur le PC client, naviguez vers https://<FQDN SocialMiner>/ et installez le certificat à travers les invites du navigateur.

Certificat client CUIC

Le certificat Tomcat CUIC peut être installé sur l'ordinateur client pour les agents, les superviseurs et les utilisateurs de rapports qui utilisent l'interface Web CUIC pour les rapports historiques ou les rapports de données en direct, soit dans la page Web CUIC, soit dans les gadgets du bureau.

Afin d'installer le certificat CUIC Tomcat dans le navigateur, sur le PC client, naviguez vers https://<UCCX FQDN>:8444/ et installez le certificat via les invites du navigateur.

Certificat de données en direct CUIC (depuis 11.x)

Le CUIC utilise le service d'E/S de socket pour les données en direct du back-end. Ce certificat peut être installé sur l'ordinateur client pour les agents, les superviseurs et les utilisateurs de rapports qui utilisent l'interface Web CUIC pour Live Data, ou qui utilisent les gadgets Live Data dans Finesse.

Afin d'installer le certificat d'E/S de socket dans le navigateur, sur le PC client, accédez à https://<UCCX FQDN>:12015/ et installez le certificat via les invites du navigateur.

Applications tierces accessibles à partir de scripts

Si un script UCCX est conçu pour accéder à un emplacement sécurisé sur un serveur tiers (par exemple, l'étape Get URL Document to an HTTPS URL ou Make Rest Call to an HTTPS REST URL), téléchargez la chaîne de certificats signée ou auto-signée du service tiers vers le magasin de clés UCCX tomcat-trust. Afin d'obtenir ce certificat, accédez à la page Administration du système d'exploitation UCCX et choisissez Upload Certificate.

Le moteur UCCX est configuré afin de rechercher les chaînes de certificats tierces dans le keystore Tomcat de la plate-forme lorsqu'elles sont présentées avec ces certificats par des applications tierces lorsqu'elles accèdent à des emplacements sécurisés via des étapes de script.

La chaîne de certificats complète doit être téléchargée vers le keystore Tomcat de la plate-forme, accessible via la page Administration du système d'exploitation, car le keystore Tomcat ne contient aucun certificat racine par défaut.

Une fois ces actions effectuées, redémarrez le moteur Cisco UCCX.

Vérifier

Afin de vérifier que tous les certificats sont installés correctement, vous pouvez tester les

fonctionnalités qui sont décrites dans cette section. Si aucune erreur de certificat n'apparaît et que toutes les fonctionnalités fonctionnent correctement, les certificats sont installés correctement.

1. Configurez Agent Web Chat via SocialMiner/CCP. Injecter un contact de discussion via le formulaire Web. Vérifiez que l'agent reçoit la bannière pour accepter le contact de discussion et qu'une fois le contact de discussion accepté, le formulaire de discussion se charge correctement et l'agent peut à la fois recevoir et envoyer des messages de discussion.
2. Essayez de vous connecter à un agent via Finesse. Vérifiez qu'aucun avertissement de certificat n'apparaît et que la page Web ne vous invite pas à installer des certificats dans le navigateur. Vérifiez que l'agent peut changer d'état correctement et qu'un nouvel appel dans UCCX lui est correctement présenté.
3. Après avoir configuré les gadgets Live Data dans la présentation du bureau Finesse de l'agent et du superviseur, connectez-vous à un agent, un superviseur et un utilisateur de rapports. Vérifiez que les gadgets Live Data se chargent correctement, que les données initiales sont renseignées dans le gadget et que les données sont actualisées lorsque les données sous-jacentes changent.
4. Essayez de vous connecter à partir d'un navigateur à l'URL AppAdmin sur les deux noeuds UCCX. Vérifiez qu'aucun avertissement de certificat ne s'affiche lorsque vous y êtes invité sur la page de connexion.

Dépannage

Problème - ID utilisateur/mot de passe non valide

Les agents UCCX Finesse ne peuvent pas se connecter avec l'erreur « ID utilisateur/mot de passe non valide ».

Causes

Unified CCX lève une exception « SSLHandshakeException » et ne parvient pas à établir une connexion avec Unified CM.

Solution

- Vérifiez que le certificat Unified CM Tomcat n'a pas expiré.
- Assurez-vous que l'une des extensions de certificat que vous avez téléchargées dans Unified CM est marquée comme critique :
  Utilisation de la clé X509v3 (OID - 2.5.29.15)
  Contraintes de base X509v3 (OID - 2.5.29.19)
  Si vous marquez d'autres postes comme critiques, la communication échoue entre Unified CCX et Unified CM en raison de l'échec de la vérification du certificat Unified CM.

Problème - Le SAN CSR et le SAN de certificat ne correspondent pas

Le téléchargement d'un certificat signé par une autorité de certification affiche l'erreur « CSR SAN and Certificate SAN does not match ».

Causes

L'autorité de certification peut avoir ajouté un autre domaine parent dans le champ de certificat Noms alternatifs de l'objet (SAN). Par défaut, le CSR peut avoir les SAN suivants :

SubjectAltName [
  example.com (dNSName)
  hostname.example.com (dNSName)
]

Les autorités de certification peuvent renvoyer un certificat avec un autre SAN ajouté au certificat : Exemple de nom d'hôte. Le certificat peut avoir un SAN supplémentaire dans ce cas :

SubjectAltName [
  example.com (dNSName)
  hostname.example.com (dNSName)

  www.hostname.example.com (dNSName)
]

Cela entraîne l'erreur de non-concordance SAN.

Solution

Dans la section Subject Alternate Name (SANs) de la page UCCX Generate Certificate Signing Request, générez le CSR avec un champ Parent Domain vide. De cette manière, le CSR n'est pas généré avec un attribut SAN, l'autorité de certification peut formater les SAN et il ne peut pas y avoir de non-correspondance d'attribut SAN lorsque vous téléchargez le certificat vers UCCX. Notez que le champ Parent Domain est défini par défaut sur le domaine du serveur UCCX, de sorte que la valeur doit être explicitement supprimée lorsque les paramètres du CSR sont configurés.

Problème - NET::ERR_CERT_COMMON_NAME_INVALID

Lorsque vous accédez à une page Web UCCX, MediaSense ou SocialMiner, un message d'erreur s'affiche.

"Votre connexion n'est pas privée. Des pirates peuvent tenter de voler vos informations à <Server_FQDN> (par exemple, des mots de passe, des messages ou des cartes de crédit). NET::ERR_CERT_COMMON_NAME_INVALID. Ce serveur n'a pas pu prouver qu'il s'agit de <Server_FQDN>; son certificat de sécurité provient de [missing_subjectAltName]. Cela peut être dû à une mauvaise configuration ou à un pirate qui intercepte votre connexion. »

Causes

Chrome version 58 introduit une nouvelle fonctionnalité de sécurité où il signale qu'un certificat de

site Web n'est pas sécurisé si son nom commun (CN) n'est pas également inclus comme un SAN.

Solution

- Vous pouvez naviguer vers Advanced > Proceed to <Server_FQDN> (unsafe) afin de continuer vers le site et d'accepter l'erreur de certificat.
- Vous pouvez éviter l'erreur ainsi que les certificats signés par l'autorité de certification. Lorsque vous générez un CSR, le nom de domaine complet du serveur est inclus en tant que SAN. L'autorité de certification peut signer le CSR et, après avoir téléchargé le certificat signé sur le serveur, le certificat du serveur contient le nom de domaine complet dans le champ SAN, de sorte que l'erreur ne peut pas être présentée.

Plus d'informations

Voir la section Supprimer la prise en charge de la correspondance commonName dans les certificats dans Dépréciations et suppressions dans Chrome 58.

Défauts du certificat

- ID de bogue Cisco CSCvb46250 - UCCX : Impact du certificat ECDSA Tomcat sur Finesse Live Data
- ID de bogue Cisco CSCvb5850 - Impossible de se connecter à SocialMiner avec tomcat et tomcat-ECDSA signés par l'autorité de certification RSA
- ID de bogue Cisco CSCvd56174 - UCCX : Échec de connexion de l'agent Finesse en raison de SSLHandshakeException
- ID de bogue Cisco CSCuv89545 - Vulnérabilité Finesse Logjam

Informations connexes

- Comprendre les certificats ECDSA dans une solution UCCX
- Prise en charge SHA 256 pour UCCX
- Exemple de configuration d'une configuration de cluster de communications unifiées avec un nom alternatif d'objet multiserveur signé CA
- Assistance et documentation techniques - 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.

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.