Guide de Gestion de certificat de solution UCCX

Contenu

Introduction
Conditions préalables
Conditions requises
FQDN, DN, et domaines
Composants utilisés
Informations générales
Configurer
Diagramme de configuration
Certificats signés
Installez les Certificats signés d'application de Tomcat
Certificats Auto-signés
Installer sur les serveurs périphériques
Régénérer les Certificats Auto-signés
Intégration et configuration de client
UCCX-à-MediaSense
MediaSense-à-finesse
UCCX-à-SocialMiner
Certificat client UCCX AppAdmin
Certificat client de plate-forme UCCX
Certificat client de service de notification
Certificat client de finesse
Certificat client de SocialMiner
Certificat client CUIC
Applications tierces accessibles des scripts
Vérifier
Dépanner
Problème - User-id non valide/mot de passe
Causes
Solution
Problème - CSR SAN et certificat SAN ne s'assortit pas
Causes
Solution
Problème - NET : : ERR_CERT_COMMON_NAME_INVALID
Causes
Solution
Plus d'informations
Défauts de certificat
Informations connexes

Introduction

Ce document décrit comment configurer le Cisco Unified Contact Center Express (UCCX) pour l'usage des Certificats auto-signés et signés.

Conditions préalables

Exigences

Avant que vous poursuiviez les étapes de configuration qui sont décrites dans ce document, assurez-vous que vous avez accès à la page du système d'exploitation de gestion (de SYSTÈME D'EXPLOITATION) pour ces applications :

- UCCX
- SocialMiner
- MediaSense

Un administrateur devrait également avoir accès à la mémoire de certificat sur les PC de client d'agent et de superviseur.

FQDN, DN, et domaines

On l'exige que tous les serveurs dans la configuration UCCX soient installés avec des serveurs et des noms de domaine de Système de noms de domaine (DNS). On l'exige également que les agents, les superviseurs, et les administrateurs accèdent aux applications de configuration UCCX par l'intermédiaire du nom de domaine complet (FQDN).

La version 10.0+ UCCX exige que le nom de domaine et les serveurs DNS soient remplis lors de la pose. Les Certificats qui sont générés par l'installateur de la version 10.0+ UCCX contiennent le FQDN, comme approprié. Ajoutez les serveurs DNS et un domaine à la batterie UCCX avant que vous amélioriez à la version 10.0+ UCCX.

Si le domaine change ou est rempli pour la première fois, les Certificats devraient être régénérés. Après que vous ajoutiez le nom de domaine à la configuration du serveur, régénérez tous les Certificats de Tomcat avant que vous les installiez sur les autres applications, dans les navigateurs de client, ou lors de la génération de la demande de signature de certificat (CSR) de signature.

Composants utilisés

Les informations décrites dans ce document sont basées sur des ces matériel et composants logiciels :

- Services Web UCCX
- Service de notification UCCX
- Plate-forme Tomcat UCCX
- Cisco Finesse Tomcat
- Centre d'intelligence de Cisco Unified (CUIC) Tomcat
- SocialMiner Tomcat
- Services Web de MediaSense

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont

démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Informations générales

Avec l'introduction de la finesse de Co-résident et du CUIC, l'intégration entre UCCX et SocialMiner pour l'email et la conversation, et l'utilisation de MediaSense afin d'enregistrer, comprenez, et installez les Certificats par l'intermédiaire de la finesse, la capacité de dépanner des questions de certificat est maintenant en critique important.

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
- Finesse de Co-résident
- Co-résident CUIC (données et rapport historique vivants)
- MediaSense (enregistrement et étiquetage basés sur finesse)
- SocialMiner (conversation)

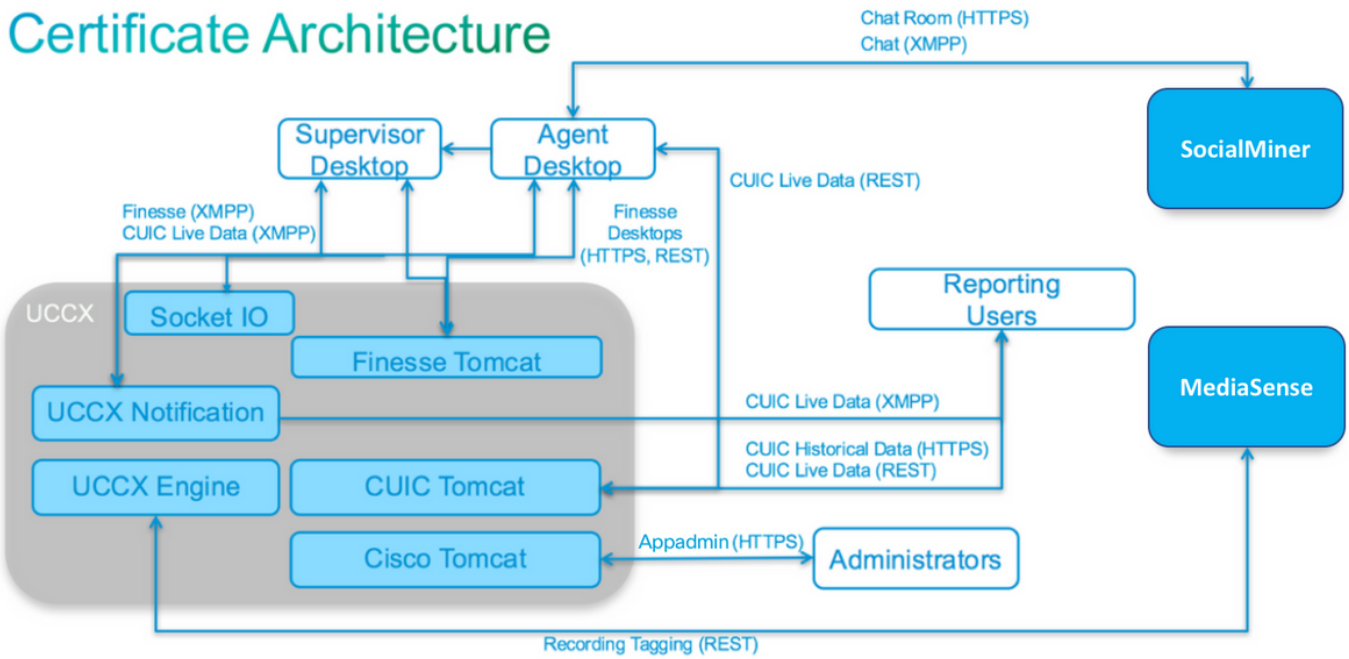
Des Certificats, signés ou auto-signés, doivent être installés sur les les deux les applications (serveurs) dans la configuration UCCX, aussi bien que les appareils de bureau de client d'agent et de superviseur.

Dans le système d'exploitation unifié de transmissions (UCOS) 10.5, des Certificats multiserveurs ont été ajoutés de sorte qu'un CSR simple ait pu être généré pour une batterie au lieu de devoir signer un certificat individuel pour chaque noeud dans la batterie. Ce type de certificat est explicitement sans support pour UCCX, MediaSense, et SocialMiner.

Configurer

Cette section décrit comment configurer l'UCCX pour l'usage des Certificats auto-signés et signés.

Diagramme de configuration



Architecture de solution UCCX valide en date d'UCCX 11.0. Diagramme de transmission HTTPS.

Certificats signés

La méthode recommandée de la Gestion de certificat pour la configuration UCCX est d'accroître les Certificats signés. Ces Certificats peuvent être signés par un Autorité de certification (CA) interne ou une tierce partie réputée CA.

En navigateurs importants, tels que Mozilla Firefox et l'Internet Explorer, des certificats racine pour la tierce partie réputée CAs sont installés par défaut. Les Certificats pour les applications de configuration UCCX qui sont signées par ces CAs sont de confiance par défaut, car leur chaîne de certificat finit dans un certificat racine qui est déjà installé dans le navigateur.

Le certificat racine d'un CA interne pourrait également être préinstallé dans le navigateur de client par une stratégie de groupe ou toute autre configuration en cours.

Vous pouvez choisir si faire signer les Certificats d'application de configuration UCCX par une tierce partie réputée CA ou par un CA interne basé sur la Disponibilité et la préinstallation du certificat racine pour le CAs dans le navigateur de client.

Installez les Certificats signés d'application de Tomcat

Terminez-vous ces étapes pour chaque noeud de l'UCCX Publisher et abonné, SocialMiner, et MediaSense Publisher et applications de gestion d'abonné :

1. Naviguez vers la page de **gestion de SYSTÈME D'EXPLOITATION** et choisissez la **Gestion de Sécurité > de certificat**.
2. Le clic **génèrent le CSR**.
3. De la liste déroulante de **liste de certificat**, choisissez le **chat** comme le nom et le clic de certificat **génèrent le CSR**.
4. Naviguez vers la **Gestion de Sécurité > de certificat** et choisissez le **CSR de téléchargement**.
5. De la fenêtre externe, choisissez le **chat de la** liste déroulante et cliquez sur Download le

CSR.

Envoyez le nouveau CSR à la tierce partie CA ou signez-le avec un CA interne, comme décrit précédemment. Ce processus devrait produire ces Certificats signés :

- Certificat racine pour le CA
- Certificat d'application UCCX Publisher
- Certificat d'application d'abonné UCCX
- Certificat d'application de SocialMiner
- Certificat d'application de MediaSense Publisher
- Certificat d'application d'abonné de MediaSense

Note: Quittez le champ de **distribution** dans le CSR comme FQDN du serveur.

Note: « (SAN) » le certificat multiserveur est pris en charge pour UCCX de la release 11.6 en avant. Cependant, le SAN devrait inclure UCCX Node-1 et Node-2 seulement. D'autres serveurs, tels que SocialMiner, ne devraient pas être inclus dans le SAN d'UCCX.

Note: Les supports UCCX seulement délivrent un certificat les longueurs principales de 1024 et 2048 bits.

Terminez-vous ces étapes sur chaque serveur d'applications afin de télécharger le certificat racine et le certificat d'application aux Noeuds :

Note: Si vous téléchargez les Certificats de racine et d'intermédiaire sur un éditeur (UCCX ou MediaSense), il devrait automatiquement être répliqué vers l'abonné. Il n'y a aucun besoin de télécharger les Certificats de racine ou d'intermédiaire sur l'autre, des serveurs de non-Publisher dans la configuration si tous les Certificats d'application sont signés par l'intermédiaire de la même chaîne de certificat.

1. Naviguez vers la page de **gestion de SYSTÈME D'EXPLOITATION** et choisissez la **Gestion de Sécurité > de certificat**.
2. Cliquez sur Upload le **certificat**.
3. Téléchargez le certificat racine et choisissez la Tomcat-**confiance** comme le type de certificat.
4. Cliquez sur Upload le **fichier**.
5. Cliquez sur Upload le **certificat**.
6. Téléchargez le certificat d'application et choisissez le **chat** comme le type de certificat.
7. Cliquez sur Upload le **fichier**. **Note**: Si un subalterne CA signe le certificat, téléchargez le certificat racine du subalterne CA comme certificat de Tomcat-*confiance* au lieu du certificat racine. Si un certificat intermédiaire est délivré, téléchargez ce certificat à la mémoire de Tomcat-*confiance* en plus du certificat d'application.
8. Une fois complet, redémarrez ces applications : Cisco MediaSense Publisher et abonnéCisco SocialMinerCisco UCCX Publisher et abonné

Note: Quand vous utilisez UCCX, MediaSense, et SocialMiner 11.5 et plus tard, il y a un nouveau certificat appelé Tomcat-ECDSA. Quand vous téléchargez un certificat signé de Tomcat-ECDSA au serveur, téléchargez le certificat d'application comme certificat de Tomcat-ECDSA--pas un certificat de chat. Pour plus d'informations sur ECDSA, référez-vous

à la section Informations connexes pour le lien pour comprendre et configurer des Certificats ECDSA.

Certificats Auto-signés

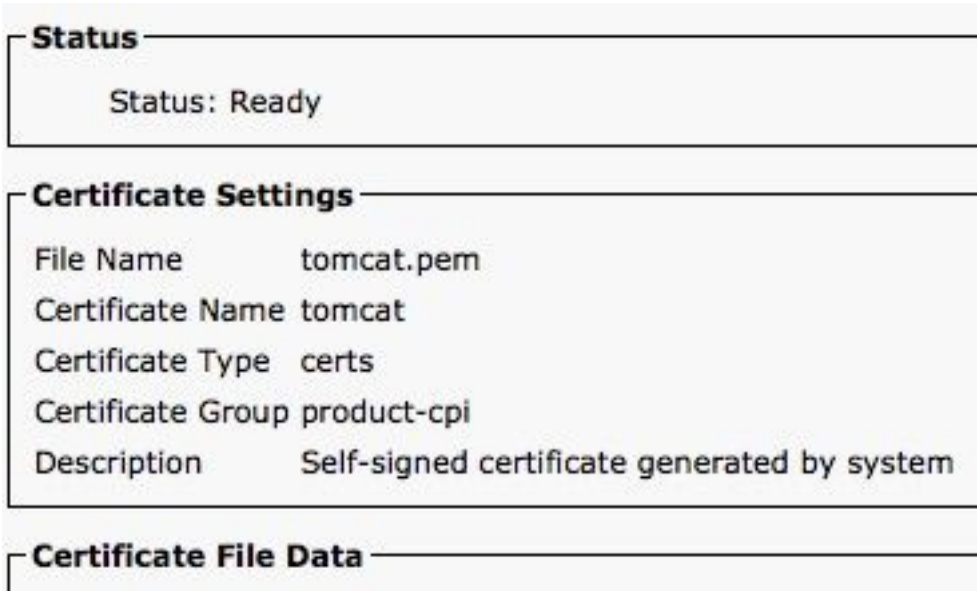
Installer sur les serveurs périphériques

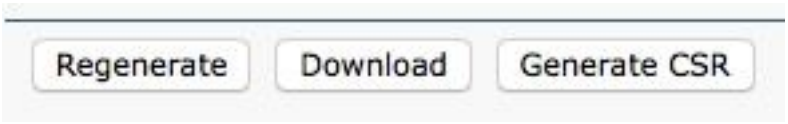
Tous les Certificats qui sont utilisés dans la configuration UCCX sont livré préinstallé sur les applications de configuration et auto-sont signés. Ces Certificats auto-signés ne sont pas implicitement faits confiance une fois présentés à un navigateur de client ou à une application différente de configuration. Bien qu'il soit recommandé pour signer tous les Certificats dans la configuration UCCX, vous pouvez utiliser les Certificats auto-signés préinstallés.

Pour chaque relations d'application, vous devez télécharger le certificat approprié et le télécharger à l'application. Terminez-vous ces étapes afin d'obtenir et télécharger les Certificats :

1. Accédez à la page de **gestion de SYSTÈME D'EXPLOITATION d'**application et choisissez la **Gestion de Sécurité > de certificat**.

2. Cliquez sur le fichier approprié du certificat **.pem** et choisissez le **téléchargement** :





3. Afin de télécharger un certificat sur l'application appropriée, naviguez vers la page de **gestion de SYSTÈME D'EXPLOITATION** et choisissez la **Gestion de Sécurité > de certificat**.
4. Cliquez sur Upload le **certificat/chaîne de certificat :**

5. Une fois complet, redémarrez ces serveurs :

Cisco MediaSense Publisher et abonnéCisco SocialMinerCisco UCCX Publisher et abonné
Afin d'installer auto-a signé des Certificats sur la machine cliente, utilise un gestionnaire de stratégie de groupe ou de module, ou les installe individuellement dans le navigateur de chaque PC d'agent.

Pour l'Internet Explorer, installez le côté client les Certificats auto-signés dans la mémoire d'**Autorités de certification racine approuvée**.

Pour Mozilla Firefox, terminez-vous ces étapes :

1. Naviguez vers des **outils > des options**.
2. Cliquez sur l'onglet **Advanced**.
3. **Certificats de vue de** clic.
4. Naviguez vers l'onglet de **serveurs**.
5. Cliquez sur Add l'**exception**.

Régénérer les Certificats Auto-signés

Dans le cas que les Certificats auto-signés expirent, ils devront être régénérés, et les étapes de configuration d'**installer sur les serveurs périphériques** devront être exécutées de nouveau.

1. Accédez à la page de **gestion de SYSTÈME D'EXPLOITATION d'**application et choisissez la **Gestion de Sécurité > de certificat**.
2. Cliquez sur le certificat approprié et choisissez le **régénéré**.
3. Le serveur dont le certificat a été régénéré doit être redémarré.
4. Pour chaque relations d'application, vous devez télécharger le certificat approprié et le télécharger à l'application après les étapes de configuration d'**installer sur les serveurs périphériques.**

Intégration et configuration de client

UCCX-à-MediaSense

L'UCCX consomme l'interface de programmation de REPOS de services Web de MediaSense (API) pour deux buts :

- Afin de s'abonner aux notifications des nouveaux enregistrements qui sont appelés sur Cisco Unified Communications Manager (CUCM).
- Afin d'étiqueter des enregistrements des agents UCCX avec l'agent et les informations de la file d'attente du service de contact (CSQ).

L'UCCX consomme le REPOS API sur les Noeuds de gestion de MediaSense. Il y a un maximum de deux dans n'importe quelle batterie de MediaSense. L'UCCX ne se connecte pas par l'intermédiaire du REPOS API aux Noeuds d'extension de MediaSense. Les deux Noeuds UCCX doivent consommer le REPOS API de MediaSense, ainsi installez les deux Certificats de MediaSense Tomcat sur chacun des deux Noeuds UCCX.

Téléchargez la chaîne de certificat signée ou auto-signée des serveurs de MediaSense au keystore de Tomcat-*confiance* UCCX.

MediaSense-à-finesse

MediaSense consomme le REPOS API de services Web de finesse afin d'authentifier des agents pour la recherche de MediaSense et lire l'instrument sur la finesse.

Le serveur de MediaSense configuré sur l'affichage de la finesse XML pour l'instrument de recherche et de jeu doit consommer le REPOS API de finesse, ainsi installez les deux Certificats UCCX Tomcat sur ce noeud de MediaSense.

Téléchargez la chaîne de certificat signée ou auto-signée des serveurs UCCX au keystore de Tomcat-*confiance de* MediaSense.

UCCX-à-SocialMiner

L'UCCX consomme le REPOS et la notification API de SocialMiner afin de gérer des contacts et la configuration d'email. Chacun des deux Noeuds UCCX doivent consommer le REPOS API de SocialMiner et être annoncés par le service de notification de SocialMiner, ainsi installez le certificat de SocialMiner Tomcat sur chacun des deux Noeuds UCCX.

Téléchargez la chaîne de certificat signée ou auto-signée du serveur de SocialMiner au keystore de Tomcat-*confiance* UCCX.

Certificat client UCCX AppAdmin

Le certificat client UCCX AppAdmin est utilisé pour la gestion du système UCCX. Afin d'installer le certificat UCCX AppAdmin pour des administrateurs UCCX, sur le PC client, naviguer vers **https:// <UCCX FQDN>/appadmin/main** pour chacun des Noeuds UCCX et installer le certificat par le navigateur.

Certificat client de plate-forme UCCX

Les services Web UCCX sont utilisés pour la livraison des contacts de conversation aux navigateurs de client. Afin d'installer le certificat de plate-forme UCCX pour des agents et des superviseurs UCCX, sur le PC client, naviguer vers **https:// <UCCX FQDN>/appadmin/main** pour chacun des Noeuds UCCX et installer le certificat par le navigateur.

Certificat client de service de notification

Le service de la notification CCX est utilisé par finesse, UCCX, et CUIC afin d'envoyer l'information en temps réel à l'appareil de bureau de client par l'intermédiaire de la Messagerie et de la présence extensibles Protocol (XMPP). Ceci est utilisé pour la transmission en temps réel de finesse aussi bien que CUIC vivent des données.

Afin d'installer la notification entretenez le certificat client sur le PC des agents et des superviseurs ou des utilisateurs d'enregistrement qui utilisent des données vivantes, naviguent vers **https:// <UCCX FQDN>:7443/** pour chacun des Noeuds UCCX et installent le certificat par le navigateur.

Certificat client de finesse

Le certificat client de finesse est utilisé par les appareils de bureau de finesse afin de connecter à

Tomcat de finesse l'exemple aux fins de la transmission du REPOS API entre le serveur de bureau et de Co-résident de finesse.

Afin d'installer le certificat de finesse pour des agents et des superviseurs, sur le PC client, naviguer vers **https:// <UCCX FQDN>:8445/** pour chacun des Noeuds UCCX et installer le certificat par les demandes de navigateur.

Afin d'installer le certificat de finesse pour des administrateurs de finesse, sur le PC client, naviguer vers **https:// <UCCX FQDN>:8445/cfadmin** pour chacun des Noeuds UCCX et installer le certificat par les demandes de navigateur.

Certificat client de SocialMiner

Le certificat de SocialMiner Tomcat doit être installé sur la machine cliente. Une fois qu'un agent reçoit une demande de conversation, l'instrument de conversation est réorienté à un URL qui représente le chatroom. Ce chatroom est hébergé par le serveur de SocialMiner et contient le contact de client ou de conversation.

Afin d'installer le certificat de SocialMiner dans le navigateur, sur le PC client, naviguer vers le **<SocialMiner FQDN>/de https://** et installer le certificat par les demandes de navigateur.

Certificat client CUIC

Le certificat CUIC Tomcat devrait être installé sur la machine cliente pour des agents, des superviseurs, et les utilisateurs d'enregistrement qui utilisent l'interface web CUIC pour des états historiques ou des données vivantes signale dans la page Web CUIC ou dans les instruments dans l'appareil de bureau.

Afin d'installer le certificat CUIC Tomcat dans le navigateur, sur le PC client, naviguer vers **https:// <UCCX FQDN>:8444/** et installer le certificat par les demandes de navigateur.

CUIC vivent le certificat de données (depuis 11.x)

Le CUIC utilise le service du socket E/S pour centralise des données vivantes. Ce certificat devrait être installé sur la machine cliente pour des agents, des superviseurs et des utilisateurs d'enregistrement qui utilisent l'interface web CUIC pour des données Live ou qui utilisent les instruments vivants de données dans la finesse.

Afin d'installer le certificat du socket E/S dans le navigateur, sur le PC client, naviguer vers **https:// <UCCX FQDN>:12015/** et installer le certificat par les demandes de navigateur.

Applications tierces accessibles des scripts

Si un script UCCX est conçu afin d'accéder à un emplacement sécurisé sur un tiers serveur (par exemple, *obtenez l'*étape de *document URL à un* URL HTTPS ou *faites l'appel de repos à un* URL de REPOS HTTPS), téléchargez la chaîne de certificat signée ou auto-signée du service tiers au keystore de Tomcat-*confiance* UCCX. Afin d'obtenir ce certificat, accéder à la page de **gestion de SYSTÈME D'EXPLOITATION** UCCX et choisir le **certificat de téléchargement**.

L'engine UCCX est configurée afin de rechercher le keystore de Tomcat de plate-forme pour de tiers chaînes de certificat une fois présentée avec ces Certificats par des applications tierces

quand ils accèdent à des emplacements sécurisés par l'intermédiaire des étapes de script.

La chaîne de certificat entière doit être téléchargée au keystore de Tomcat de plate-forme, accessible par l'intermédiaire de la page de **gestion de SYSTÈME D'EXPLOITATION**, car le keystore de Tomcat ne contient aucun certificat racine par défaut.

Après que vous vous terminiez ces actions, redémarrez l'engine de Cisco UCCX.

Vérifiez

Afin de vérifier que tous les Certificats sont installés correctement, vous pouvez tester les caractéristiques qui sont décrites dans cette section. Si erreur de certificat n'apparaît pas et toutes les caractéristiques fonctionnent correctement, les Certificats sont installés correctement.

- Configurez la finesse de sorte qu'elle enregistre automatiquement un agent par l'intermédiaire du processus. Après qu'un appel soit traité par l'agent, utilisez la recherche de MediaSense et lisez l'application afin de trouver l'appel. Vérifiez que l'appel a l'agent, un CSQ, et des balises d'équipe reliées aux métadonnées d'enregistrement dans MediaSense.
- Configurez la conversation de Web d'agent par SocialMiner. Injectez un contact de conversation par l'intermédiaire du formulaire web. Vérifiez que l'agent reçoit la bannière pour recevoir le contact de conversation et pour le vérifier également qu'une fois le contact de conversation est reçu, les chargements de forme de conversation correctement et l'agent peut recevoir et envoyer des messages instantanés.
- Tentez d'ouvrir une session un agent par l'intermédiaire de la finesse. Vérifiez qu'avertissement de certificat n'apparaît pas et que la page Web n'incite pas pour l'installation des Certificats dans le navigateur. Vérifiez que l'agent peut changer des états correctement et un nouvel appel dans UCCX est correctement présenté à l'agent.
- Après que vous configuriez les instruments vivants de données dans l'affichage de bureau de finesse d'agent et de superviseur, ouvrez une session un agent, un superviseur, et un utilisateur d'enregistrement. Vérifiez que les instruments vivants de données chargent correctement, que les données initiales sont remplies dans l'instrument, et que les données régénèrent quand les données sous-jacentes changent.
- Tentative de se connecter d'un navigateur à l'URL d'AppAdmin sur les deux Noeuds UCCX. Vérifiez qu'avertissement de certificat n'apparaît pas une fois incité avec la page de connexion.

Dépanner

Problème - User-id non valide/mot de passe

Les agents de finesse UCCX ne peuvent pas ouvrir une session avec l'erreur « **user-id non valide/mot de passe** ».

Causes

L'Unified CCX jette une exception « SSLHandshakeException « et n'établit pas une connexion avec l'Unified CM.

Solution

- Vérifiez que le certificat de Tomcat d'Unified CM n'est pas expiré.
- Assurez-vous que n'importe quel certificat que vous avez téléchargé dans l'Unified CM a des n'importe quelles de ces extensions marquées en tant qu'essentiel :
  Utilisation principale X509v3 (OID - 2.5.29.15)
  Contraintes X509v3 de base (OID - 2.5.29.19)
  Si vous marquez n'importe quelles autres extensions comme essentielles, la transmission échoue entre l'Unified CCX et l'Unified CM dus à la panne de la vérification de certificat d'Unified CM.

Problème - CSR SAN et certificat SAN ne s'assortit pas

Le téléchargement d'une erreur « CSR SAN d'affichages de certificat signé CA et du certificat SAN ne s'assortit pas ».

Causes

Le CA pourrait avoir ajouté un autre domaine de parent dans le domaine alternatif des noms de sujet de certificat (SAN). Par défaut, le CSR aura ces derniers sans :

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

Le CAs pourrait renvoyer un certificat avec un autre SAN ajouté au certificat : www.hostname.example.com. Le certificat aura un SAN supplémentaire dans ce cas :

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

  www.hostname.example.com (dNSName)
]

Ceci entraîne l'erreur de non-concordance SAN.

Solution

Dans la section « de nom secondaire soumis (sans) » de la page « générez de certificat UCCX de signature demande », génèrent le CSR avec un champ Domain vide de parent. De cette façon le CSR n'est pas générée avec un attribut SAN, le CA peut formater sans, et il n'y aura pas une non-concordance d'attribut SAN quand vous téléchargez le certificat à UCCX. Notez que le champ Domain de parent se transfère sur le domaine du serveur UCCX, ainsi la valeur doit explicitement être enlevée tandis que les configurations pour le CSR sont configurées.

Problème - NET : : ERR_CERT_COMMON_NAME_INVALID

Quand vous accédez à n'importe quelle page Web UCCX, de MediaSense, ou de SocialMiner,

vous recevez un message d'erreur.

« Votre connexion n'est pas privée.

Les attaquants pourraient essayer de dérober vos informations de <Server_FQDN> (par exemple, des mots de passe, des messages, ou des cartes de crédit). NET : : ERR_CERT_COMMON_NAME_INVALID

Ce serveur ne pourrait pas montrer que c'est <Server_FQDN> ; son Security Certificate est de [missing_subjectAltName]. Ceci peut sont provoqué par par une mauvaise configuration ou un attaquant interceptant votre connexion. »

Causes

La version 58 de Chrome a introduit une nouvelle fonctionnalité de sécurité où elle signale que le certificat d'un site Web n'est pas sécurisé si son nom commun (NC) n'est pas également inclus comme SAN.

Solution

- Vous pouvez naviguer vers **avancé > poursuivez au <Server_FQDN> (peu sûr)** afin de continuer au site et recevoir l'erreur de certificat.
- Vous pouvez éviter l'erreur totalement avec les Certificats signés CA. Quand vous générez un CSR, le FQDN du serveur est inclus comme SAN. Le CA peut signer le CSR, et après que vous téléchargiez le certificat signé de nouveau au serveur, le certificat de serveur aura le FQDN dans le domaine SAN de sorte que l'erreur ne soit pas présentée.

Plus d'informations

Voyez la section « enlever le soutien du commonName s'assortissant dans les Certificats » dans les condamnations et les suppressions dans Chrome 58.

Défauts de certificat

- ID de bogue Cisco CSCvb46250 - UCCX : Incidence de certificat de Tomcat ECDSA sur des données vivantes de finesse
- ID de bogue Cisco CSCvb58580 - Incapable d'ouvrir une session à SocialMiner avec le chat et le Tomcat-ECDSA a signé par RSA CA
- ID de bogue Cisco CSCvd56174 - UCCX : Panne de connexion de l'agent de finesse due à SSLHandshakeException
- ID de bogue Cisco CSCuv89545 - Vulnérabilité d'embouteillage de finesse

Informations connexes

- Comprenez les Certificats ECDSA dans une solution UCCX
- Soutien du SHA 256 d'UCCX

- Exemple signé et Auto-signé UCCX de Certificats de configuration
- Support et documentation techniques - Cisco Systems