Configuration de CUCM pour LDAP sécurisé (LDAPS)

Table des matières

Introduction

Ce document décrit la procédure de mise à jour des connexions CUCM à AD à partir d'une connexion LDAP non sécurisée vers une connexion LDAP sécurisée.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

· Serveur AD LDAP
· Configuration LDAP CUCM

· CUCM IM & Presence Service (IM/P)

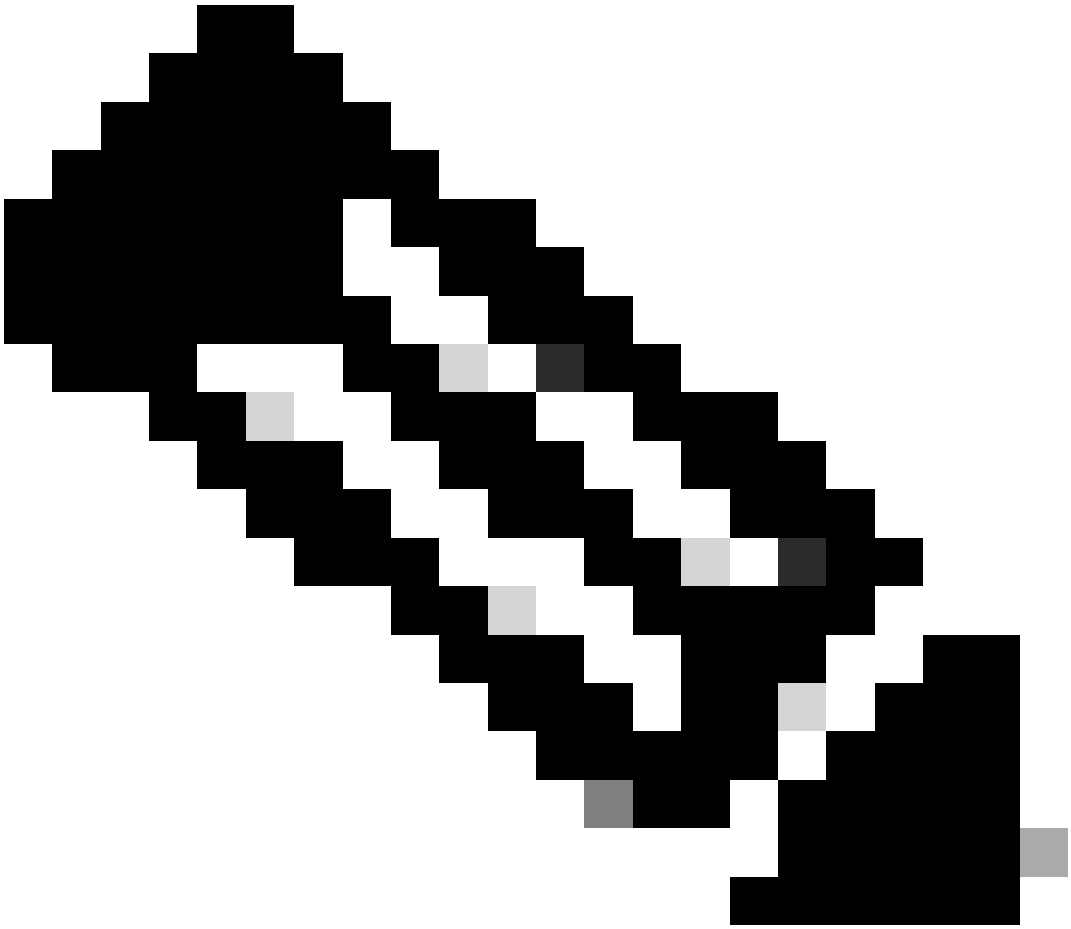
Composants utilisés

Les informations contenues dans ce document sont basées sur CUCM version 9.x et ultérieure.

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

Il est de la responsabilité de l'administrateur Active Directory (AD) de configurer le protocole LDAP (Lightweight Directory Access Protocol) AD pour le protocole LDAPS (Lightweight Directory Access Protocol) . Cela inclut l'installation de certificats signés par une autorité de certification qui répondent aux exigences d'un certificat LDAPS.



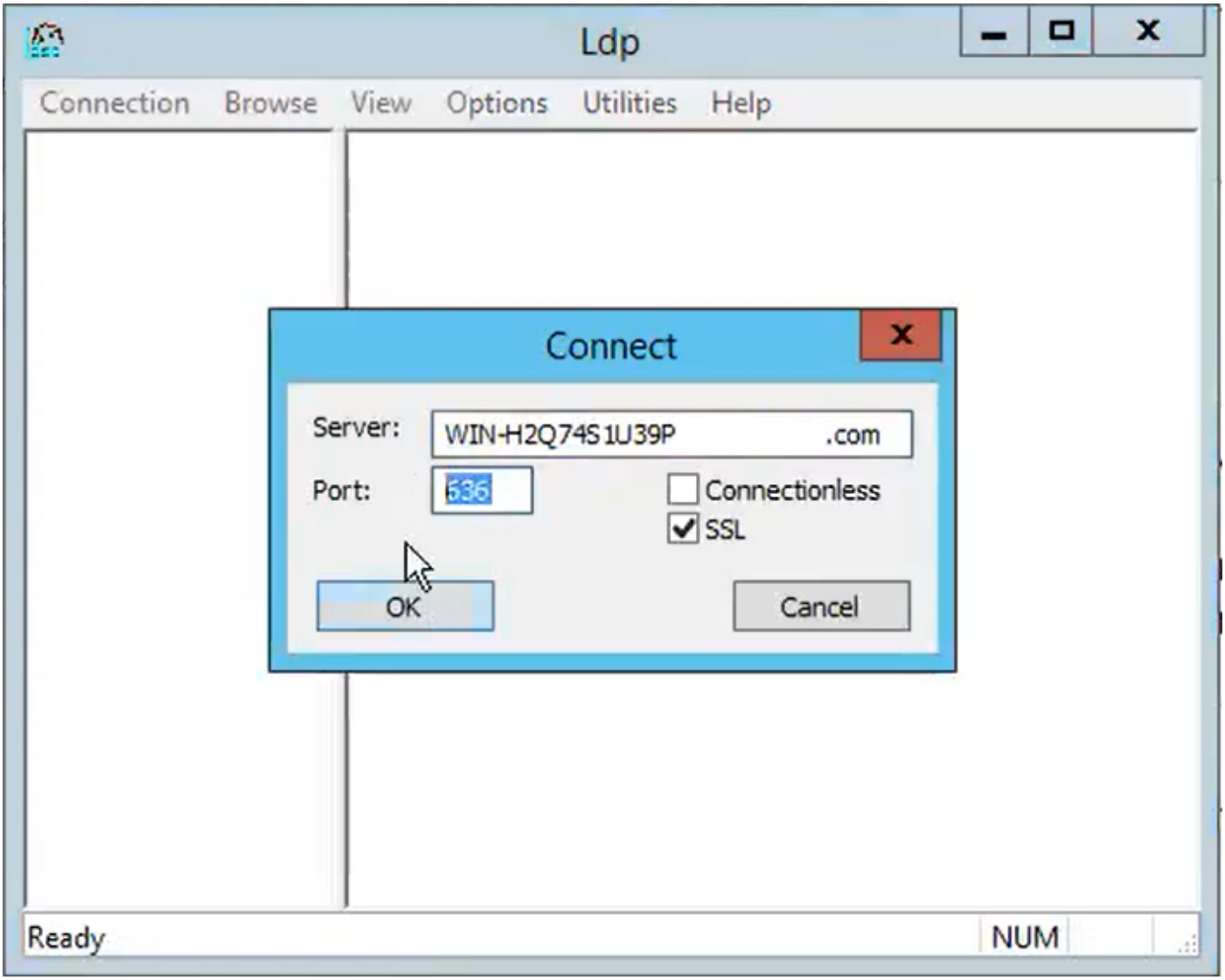
> Remarque : consultez ce lien pour obtenir des informations afin de mettre à jour les connexions LDAP non sécurisées vers les connexions LDAP sécurisées vers AD pour d'autres applications de collaboration Cisco : Software Advisory : Secure LDAP Mandatory for Active Directory Connections

---

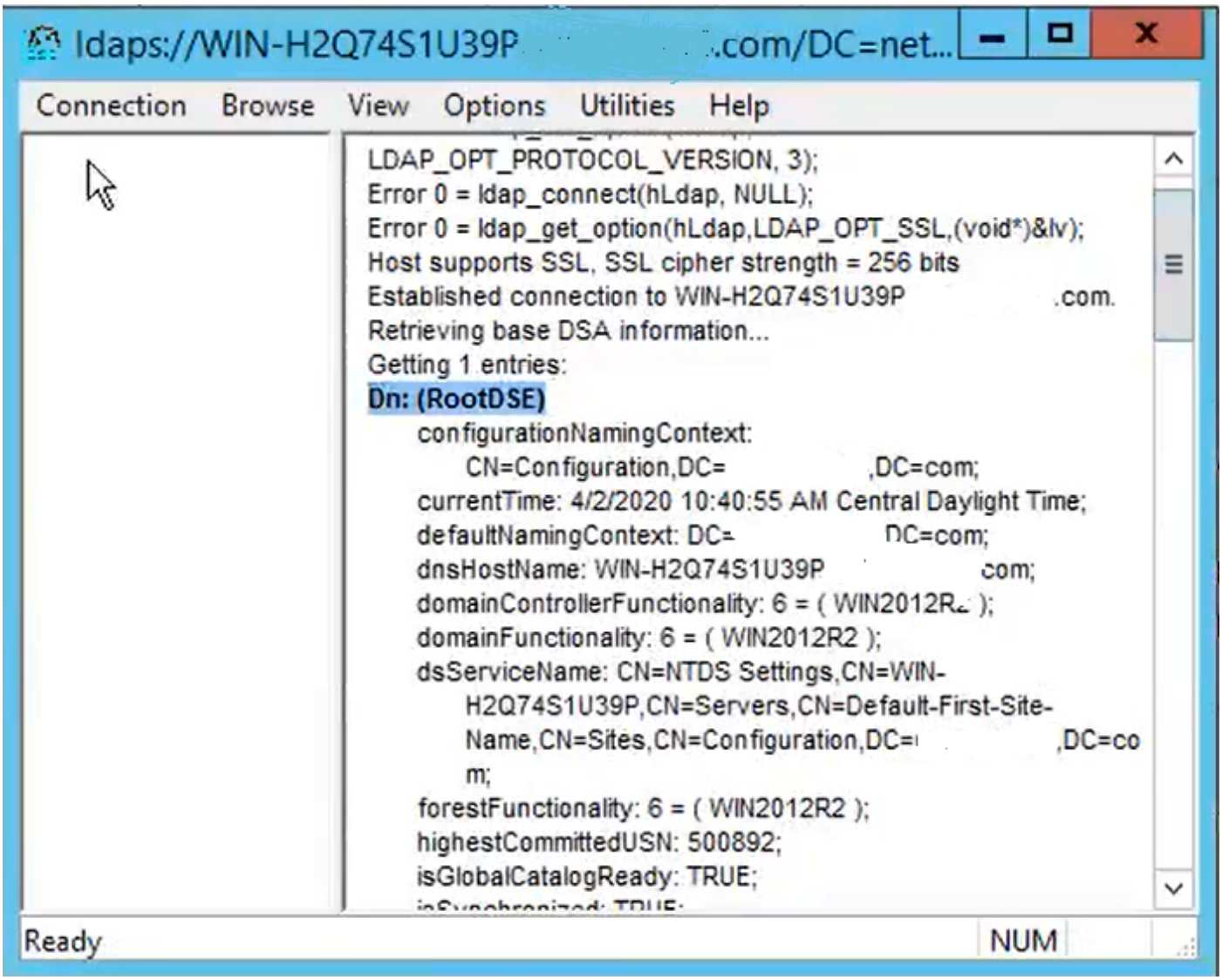
Vérification et installation des certificats LDAPS

Étape 1. Une fois que le certificat LDAPS a été téléchargé sur le serveur AD, vérifiez que LDAPS est activé sur le serveur AD avec l'outil ldp.exe.

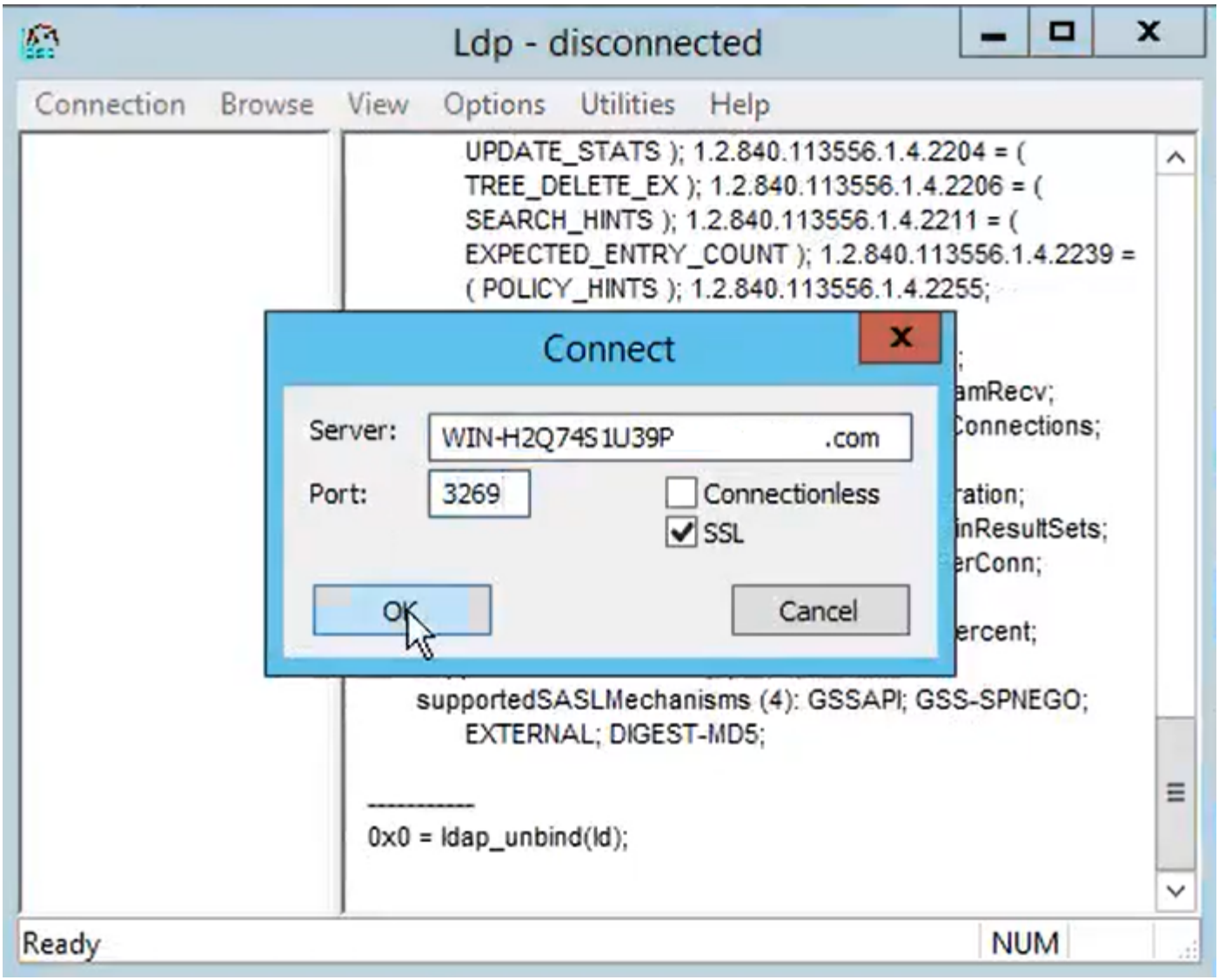
1. Démarrez l'outil d'administration AD (Ldp.exe) sur le serveur AD.
2. Dans le menu Connection, sélectionnez Connect.
3. Saisissez le nom de domaine complet (FQDN) du serveur LDAP en tant que serveur.
4. Entrez 636 comme numéro de port.
5. Cliquez sur OK, comme illustré dans l'image



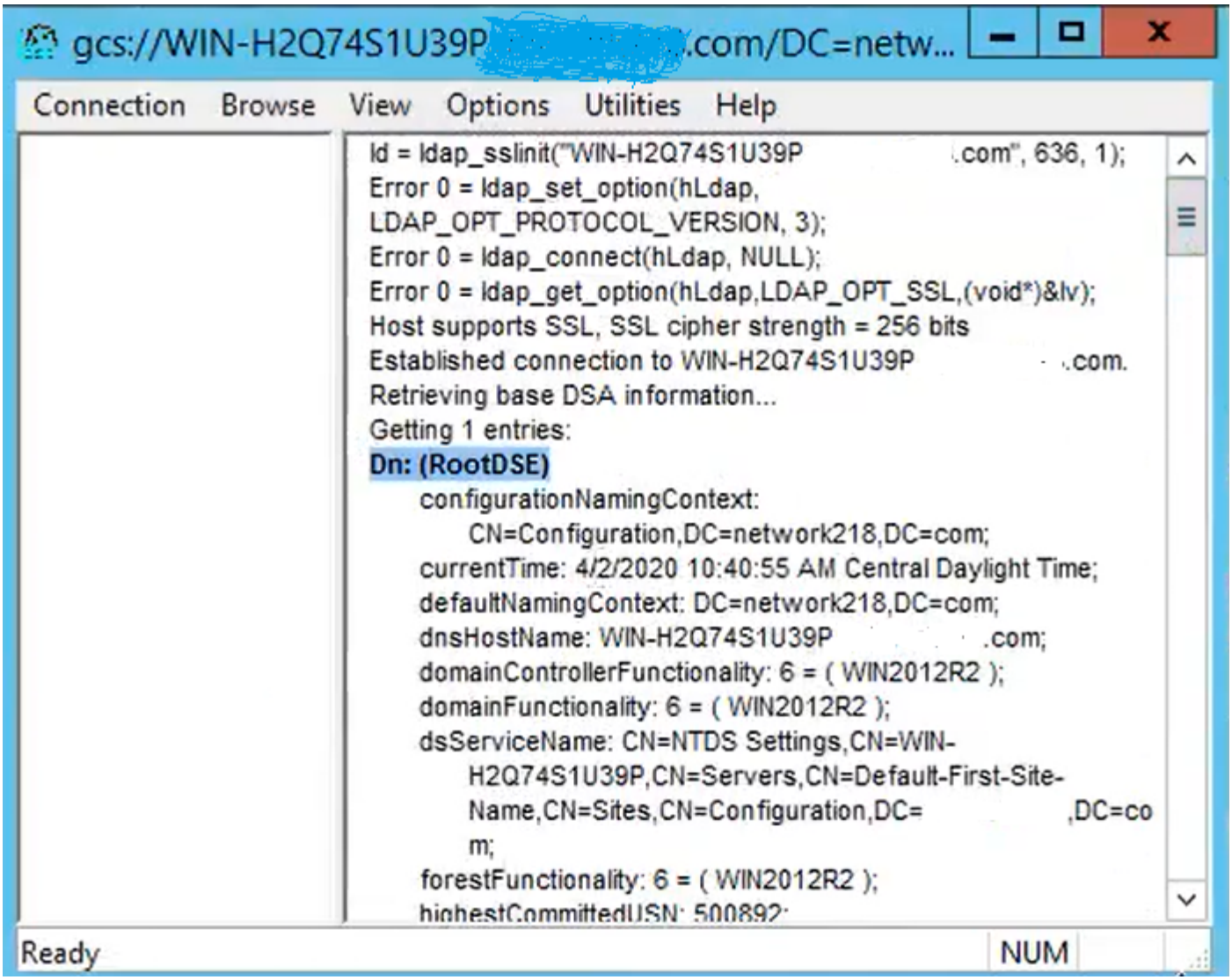
Pour une connexion réussie sur le port 636, les informations RootDSE s'impriment dans le volet droit, comme illustré dans l'image :



Répétez la procédure pour le port 3269, comme indiqué dans l'image :

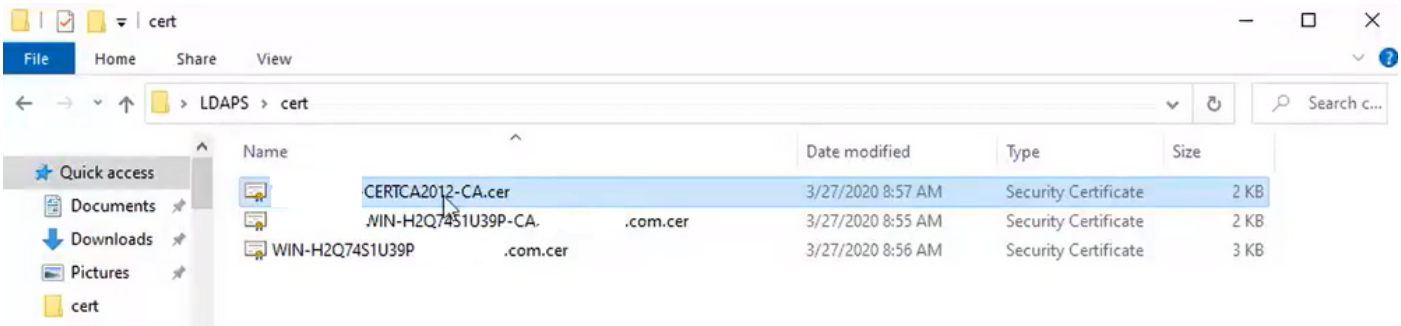


Pour une connexion réussie sur le port 3269, les informations RootDSE s'impriment dans le volet droit, comme illustré dans l'image :

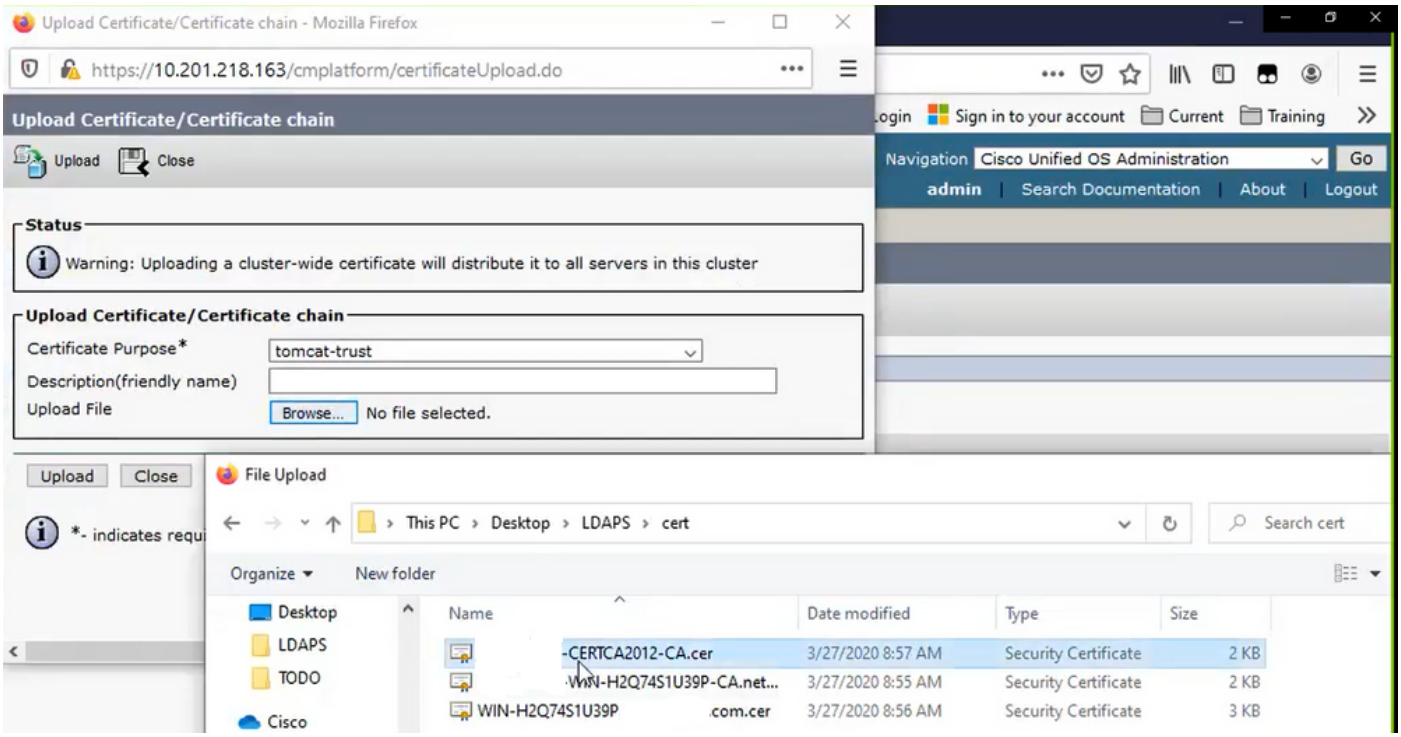


Étape 2. Procurez-vous le certificat racine et tout certificat intermédiaire faisant partie du certificat du serveur LDAPS et installez-les en tant que certificats de confiance de chat sur chacun des noeuds CUCM et de l'éditeur IM/P et en tant que CallManager-trust sur l'éditeur CUCM.

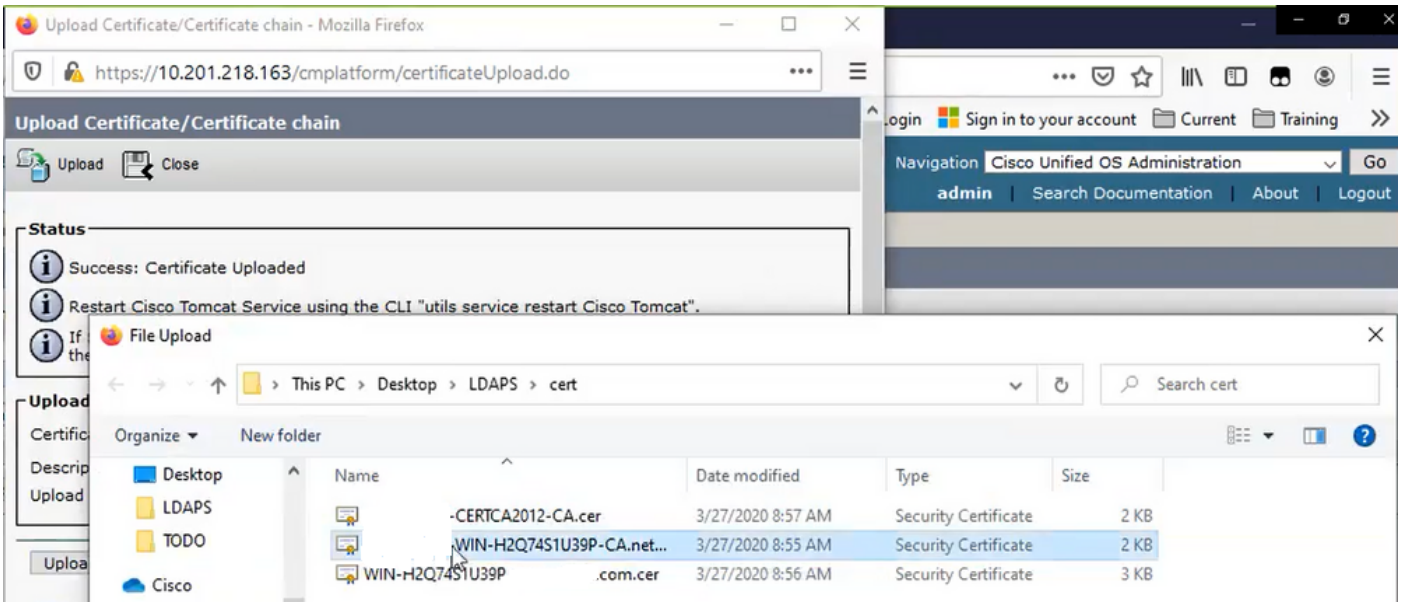
Les certificats racine et intermédiaires qui font partie d'un certificat de serveur LDAP, <hostname>.<Domain>.cer, sont indiqués dans l'image :



Accédez à CUCM publisher Cisco Unified OS Administration > Security > Certificate Management. Téléchargez la racine comme tomcat-trust (comme illustré dans l'image) et comme CallManager-trust (non illustré) :



Téléchargez l'intermédiaire comme tomcat-trust (comme illustré dans l'image) et comme CallManager-trust (non illustré) :

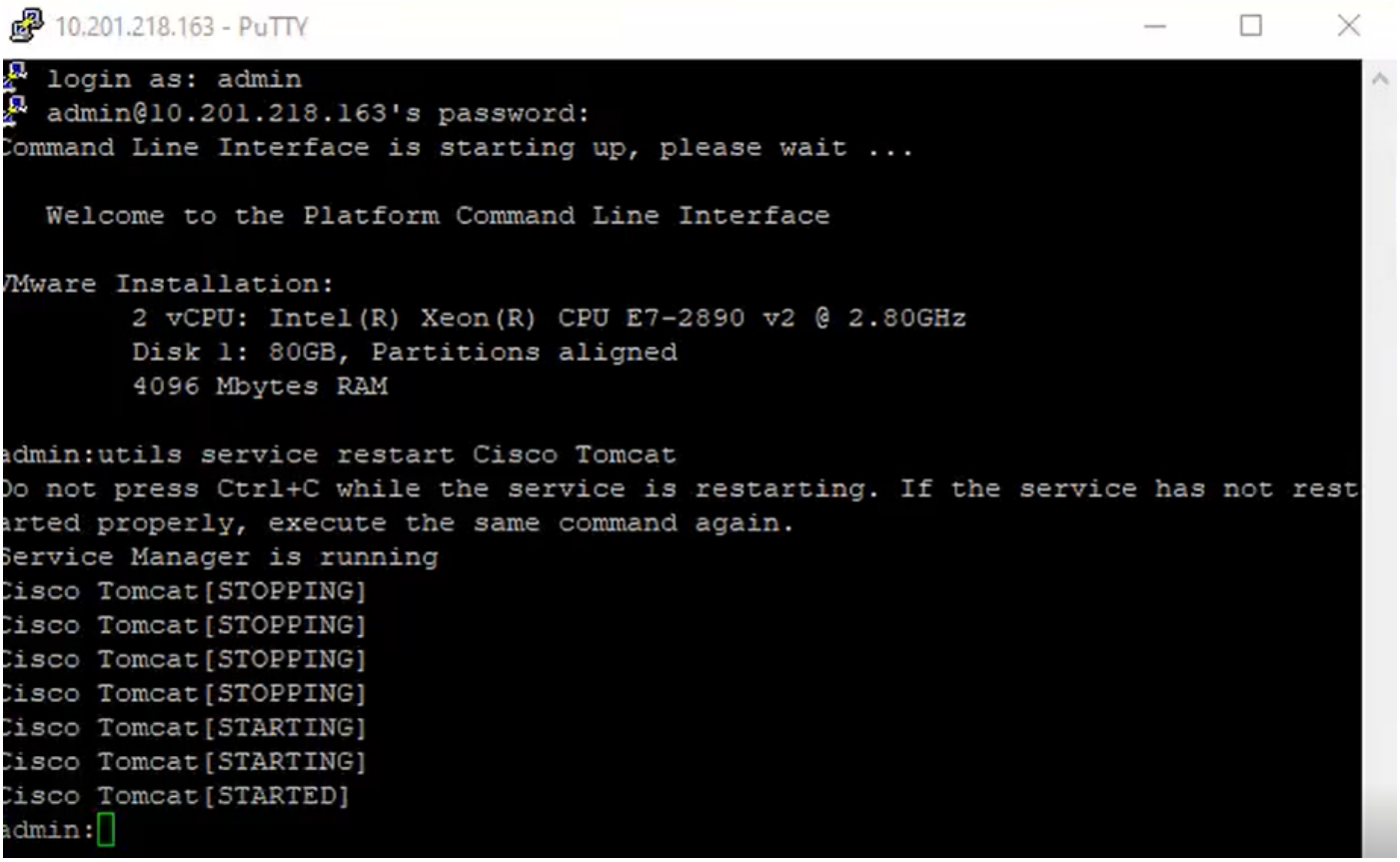


Remarque : si des serveurs IM/P font partie du cluster CUCM, vous devez également télécharger ces certificats vers ces serveurs IM/P.

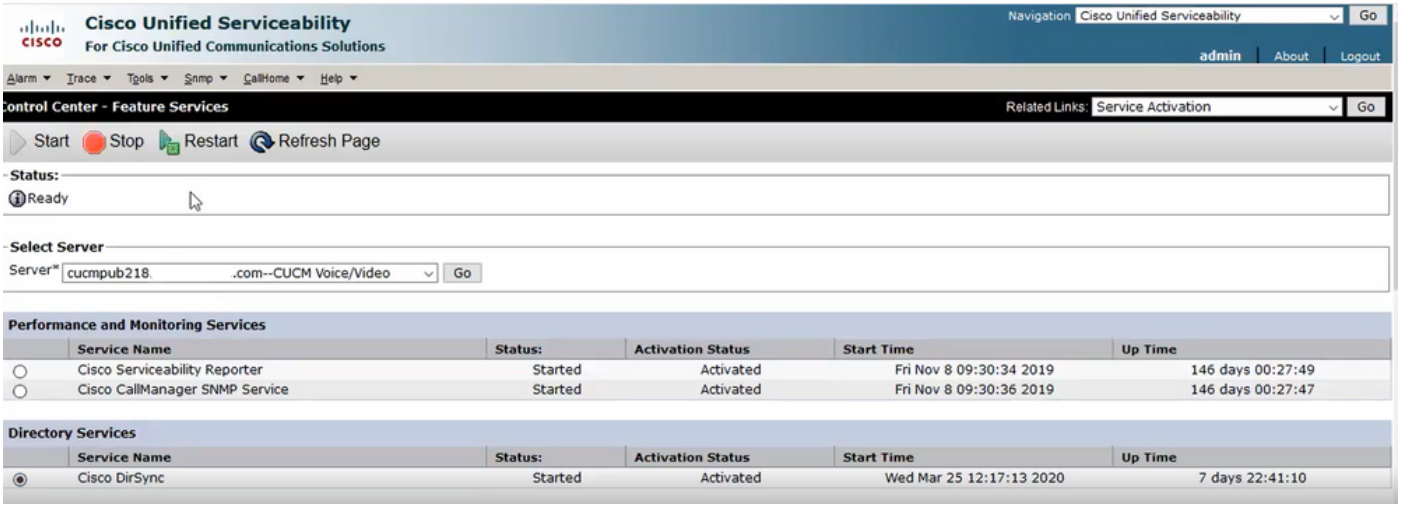
Remarque : vous pouvez également installer le certificat du serveur LDAPS en tant que tomcat-trust.

Étape 3. Redémarrez Cisco Tomcat à partir de l'interface de ligne de commande de chaque noeud (CUCM et IM/P) dans les clusters. En outre, pour le cluster CUCM, vérifiez que le service Cisco DirSync sur le noeud éditeur est démarré.

Pour redémarrer le service Tomcat, vous devez ouvrir une session CLI pour chaque noeud et exécuter la commande utils service restart Cisco Tomcat, comme indiqué dans l'image :



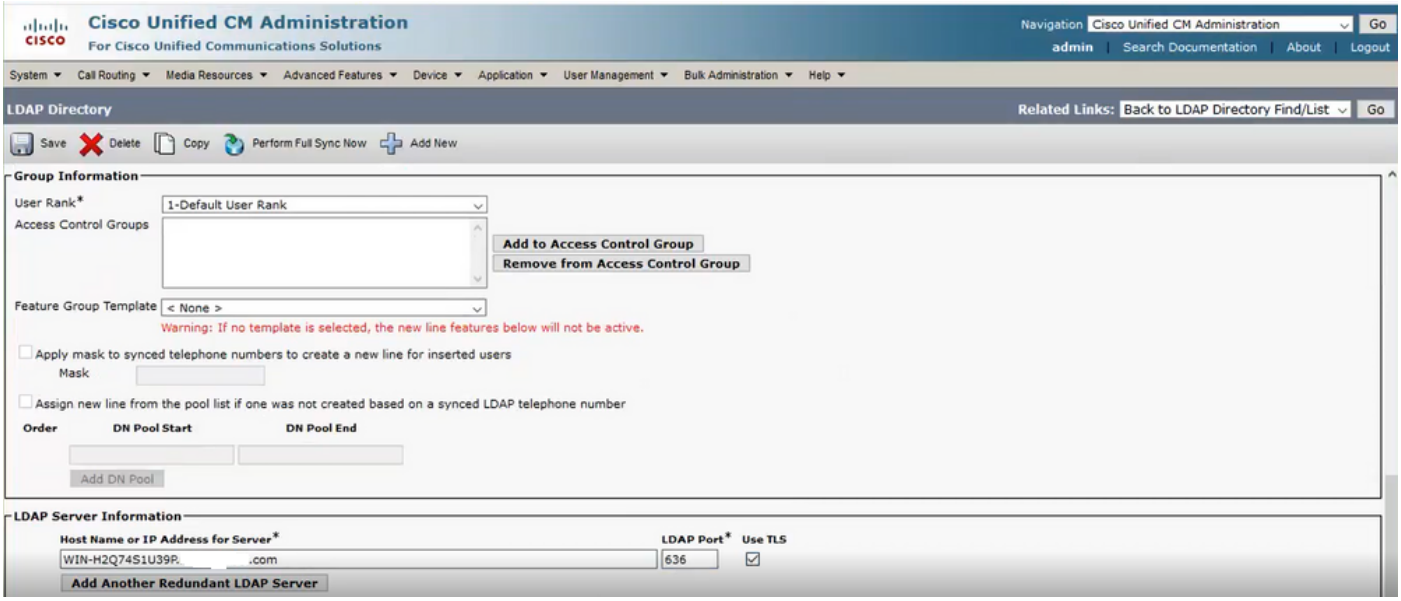
Étape 4. Accédez à CUCM publisher Cisco Unified Serviceability > Tools > Control Center - Feature Services, vérifiez que le service Cisco DirSync est activé et démarré (comme illustré dans l'image), et redémarrez le service Cisco CTIManager sur chaque noeud si ce dernier est utilisé (non illustré) :

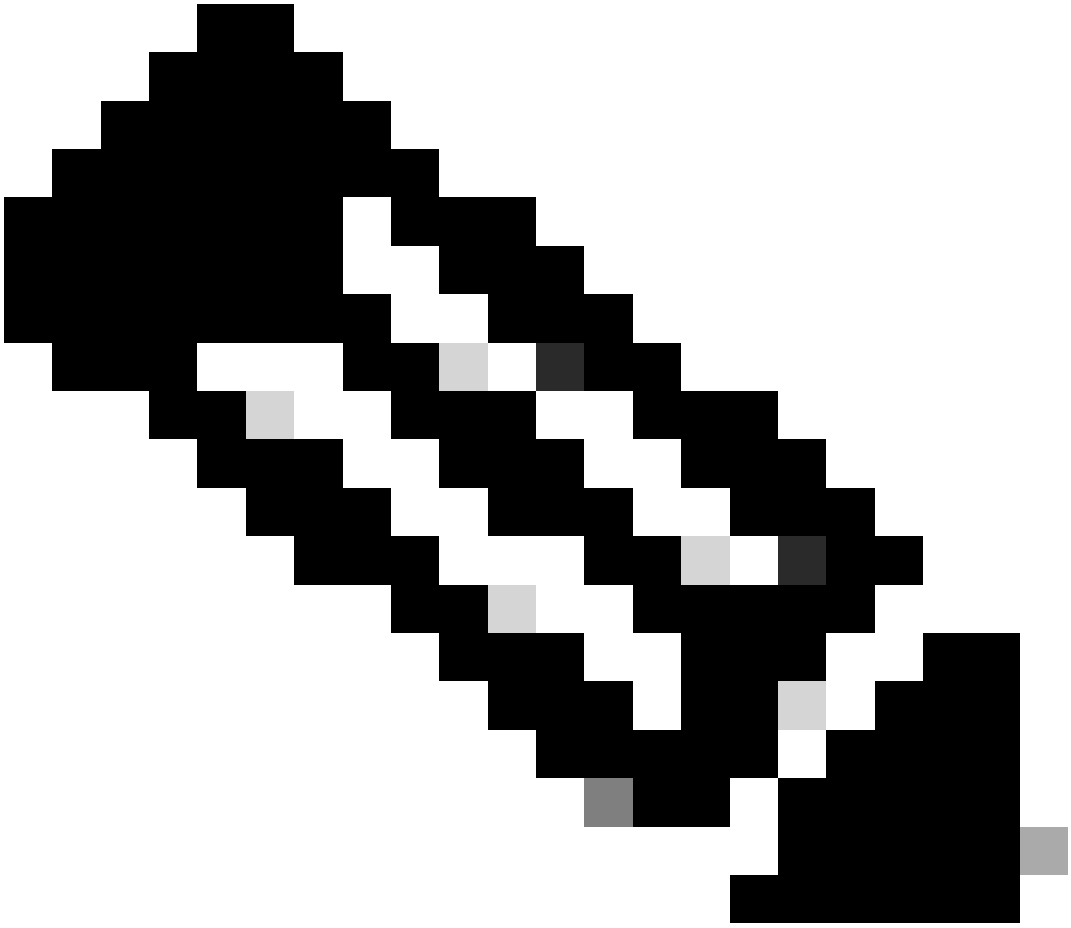


Configurer l'annuaire LDAP sécurisé

Étape 1. Configurez l'annuaire LDAP CUCM afin d'utiliser la connexion TLS LDAP à AD sur le port 636.

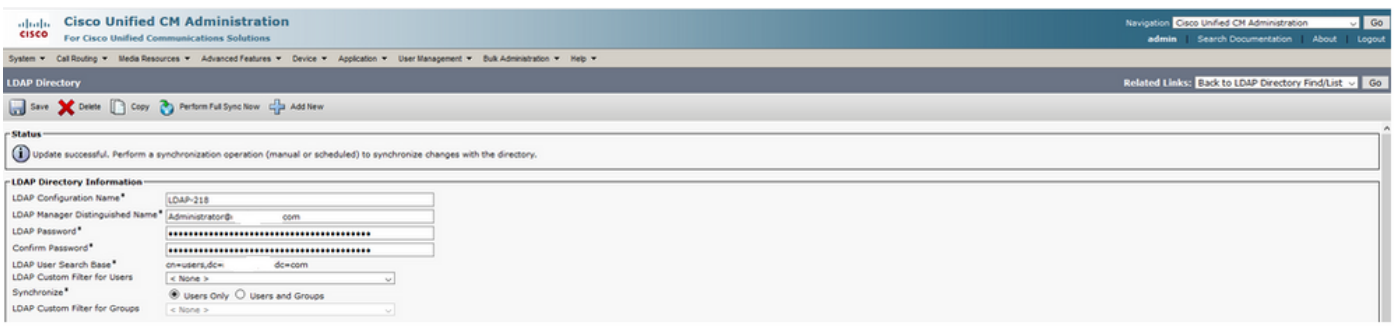
Accédez à CUCM Administration > System > LDAP Directory. Tapez le nom de domaine complet ou l'adresse IP du serveur LDAP pour obtenir des informations sur le serveur LDAP. Spécifiez le port LDAPS 636 et cochez la case Use TLS, comme indiqué dans l'image :



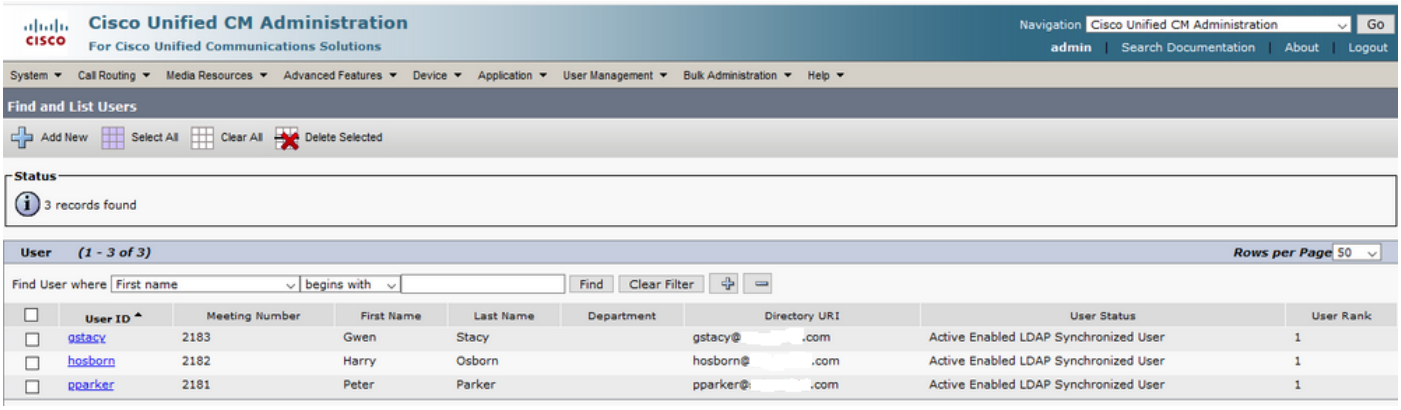


Remarque : par défaut, après vérification du nom de domaine complet (FQDN) des versions 10.5(2)SU2 et 9.1(2)SU3 configurées dans les informations du serveur LDAP par rapport au nom commun du certificat, dans le cas où l'adresse IP est utilisée à la place du nom de domaine complet (FQDN), la commande utils ldap config ipaddr est émise pour arrêter l'application du nom de domaine complet (FQDN) à la vérification CN.

Étape 2. Afin de terminer la modification de configuration en LDAPS, cliquez sur Perform Full Sync Now, comme indiqué dans l'image :

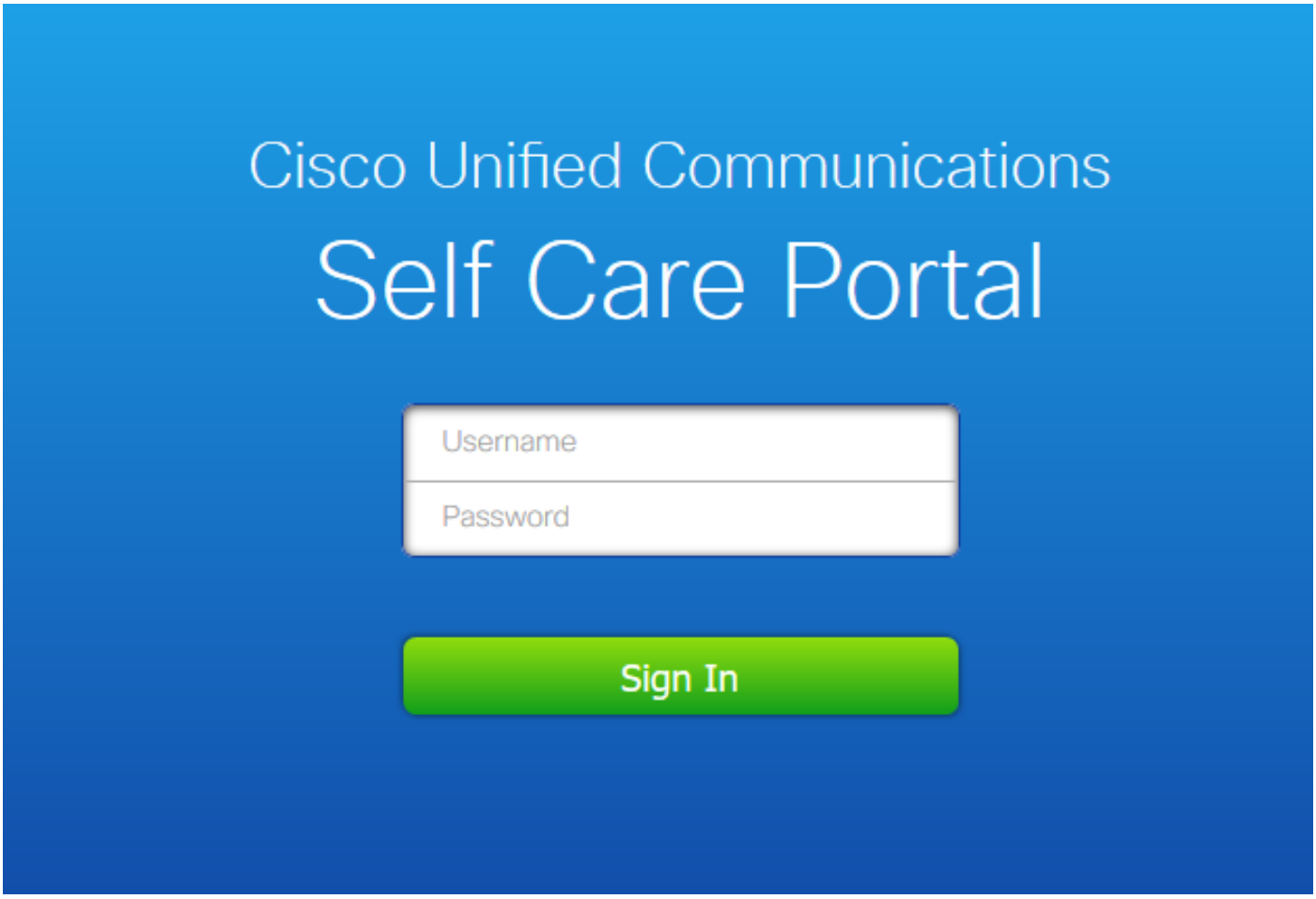


Étape 3. Accédez à CUCM Administration > User Management > End User et vérifiez que les utilisateurs finaux sont présents, comme illustré dans l'image :

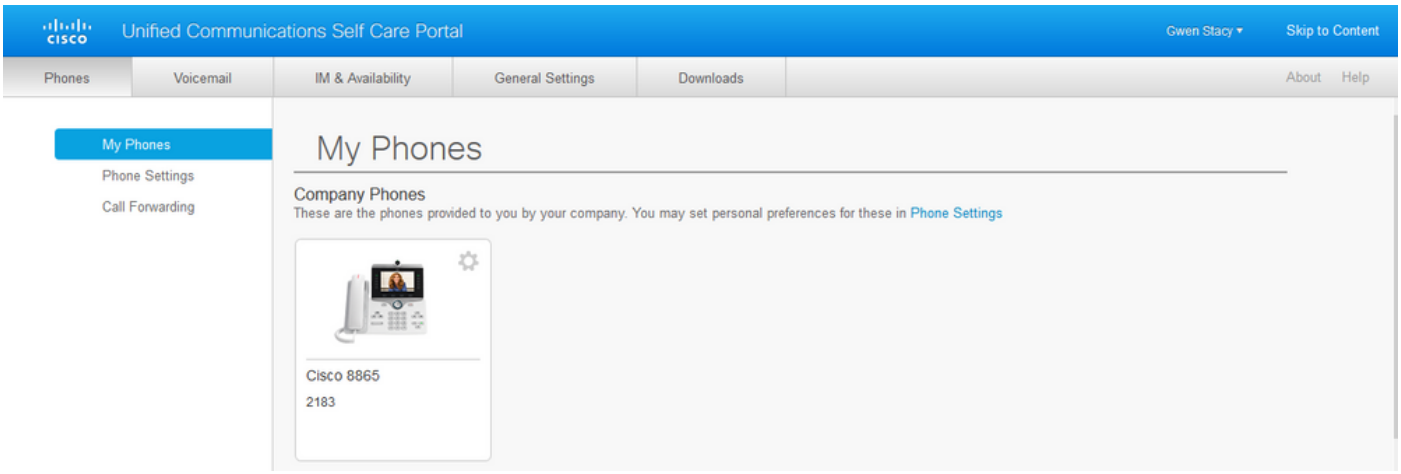


Étape 4. Accédez à la page ccmuser (https://<ip address of cucm pub>/ccmuser) afin de vérifier que la connexion de l'utilisateur a réussi.

La page ccmuser pour CUCM version 12.0.1 ressemble à ceci :



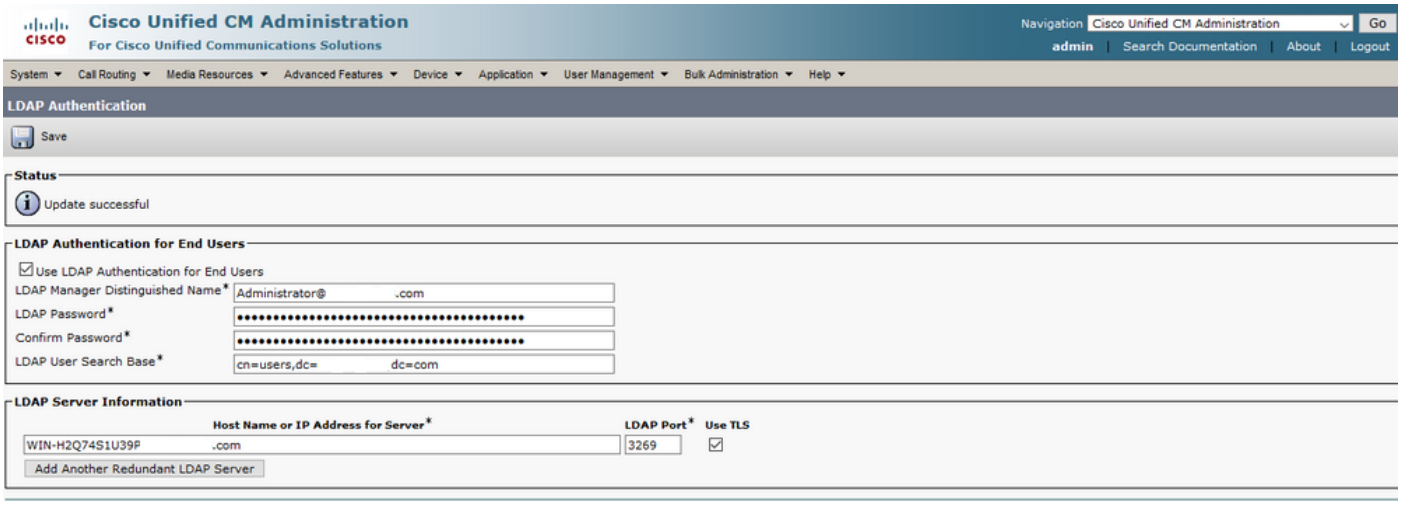
L'utilisateur peut se connecter une fois les informations d'identification LDAP saisies, comme indiqué dans l'image :

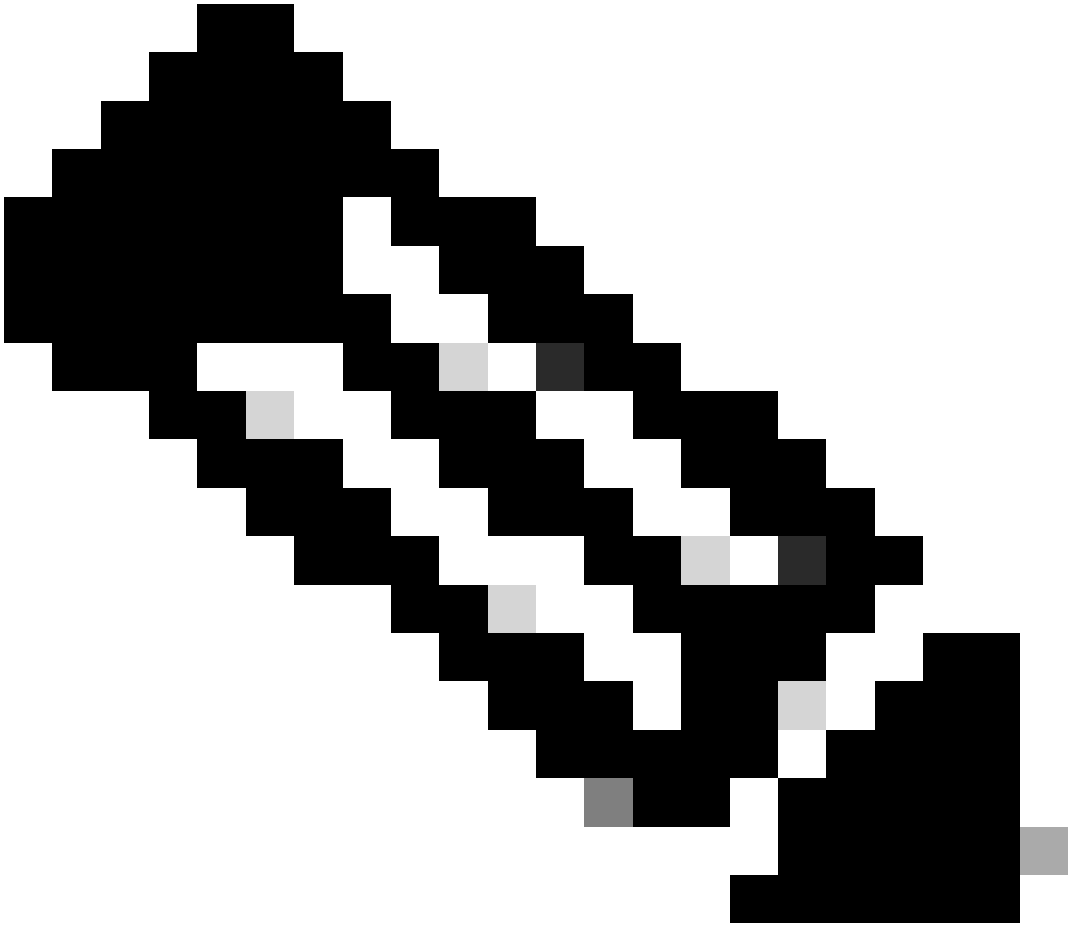


Configurer l'authentification LDAP sécurisée

Configurez l'authentification LDAP CUCM afin d'utiliser la connexion TLS LDAP à AD sur le port 3269.

Accédez à CUCM Administration > System > LDAP Authentication. Tapez le nom de domaine complet du serveur LDAP pour obtenir des informations sur le serveur LDAP. Spécifiez le port LDAPS 3269 et cochez la case Use TLS, comme indiqué dans l'image :



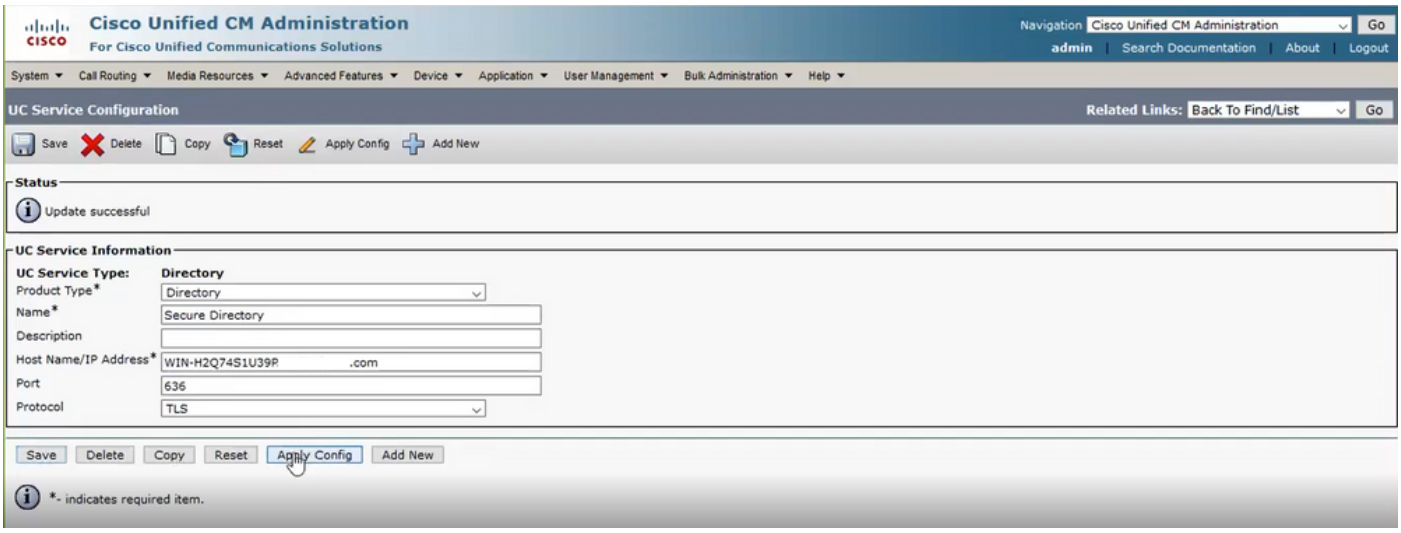


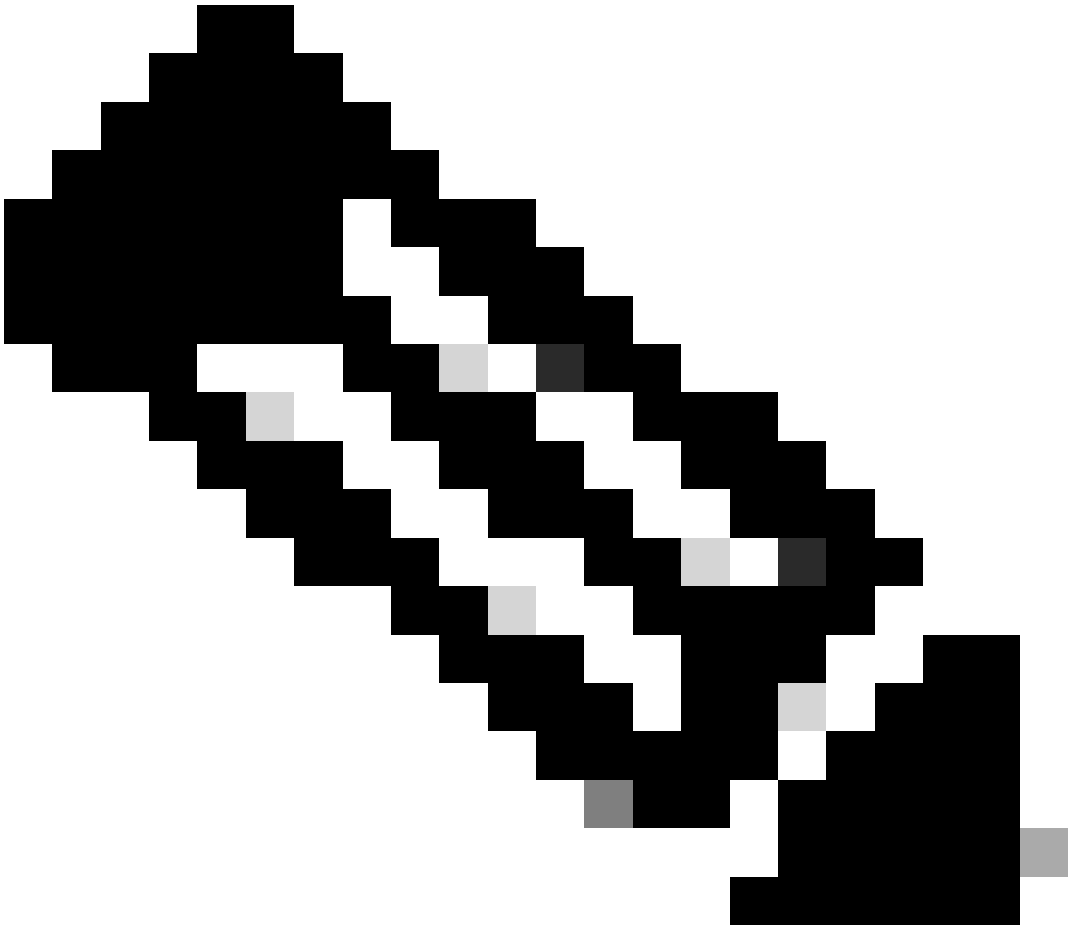
Remarque : si vous avez des clients Jabber, il est recommandé d'utiliser le port 3269 pour l'authentification LDAPS, car le délai d'attente Jabber pour la connexion peut se produire si aucune connexion sécurisée au serveur de catalogue global n'est spécifiée.

Configurer des connexions sécurisées à Active Directory pour les services de communications unifiées

Si vous avez besoin de sécuriser des services de communications unifiées qui utilisent LDAP, configurez ces services de communications unifiées pour utiliser le port 636 ou 3269 avec TLS.

Accédez à CUCM administration > User Management > User Settings > UC Service. Recherchez le service d'annuaire qui pointe vers AD. Saisissez le nom de domaine complet (FQDN) du serveur LDAP comme nom d'hôte/adresse IP. Spécifiez le port 636 ou 3269 et le protocole TLS, comme indiqué dans l'image :





Remarque : les ordinateurs clients Jabber doivent également disposer des certificats LDAPS de confiance tomcat qui ont été installés sur CUCM dans le magasin de confiance de gestion des certificats de l'ordinateur client Jabber afin de permettre au client Jabber d'établir une connexion LDAPS à AD.

Vérifier

Référez-vous à cette section pour vous assurer du bon fonctionnement de votre configuration.

Afin de vérifier la chaîne de certificats LDAPS réelle envoyée du serveur LDAP à CUCM pour la connexion TLS, exportez le certificat LDAPS TLS à partir d'une capture de paquets CUCM. Ce lien fournit des informations sur la façon d'exporter un certificat TLS à partir d'une capture de paquets CUCM : Comment exporter un certificat TLS à partir de la capture de paquets CUCM

Dépannage

Il n’y a actuellement aucune information spécifique disponible pour dépanner cette configuration.

Informations connexes

- Ce lien permet d'accéder à une vidéo présentant les configurations LDAP : Vidéo de présentation de l'annuaire LDAP sécurisé et de l'authentification
- 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.