Configurer le protocole LDAP sécurisé sur les serveurs UCS série C

Table des matières

Introduction

Ce document décrit comment configurer SecureLDAP sur les serveurs de la gamme C.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Compréhension de base de Cisco UCS et CIMC.

Composants utilisés

- Serveur Cisco UCS série C en mode autonome.

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

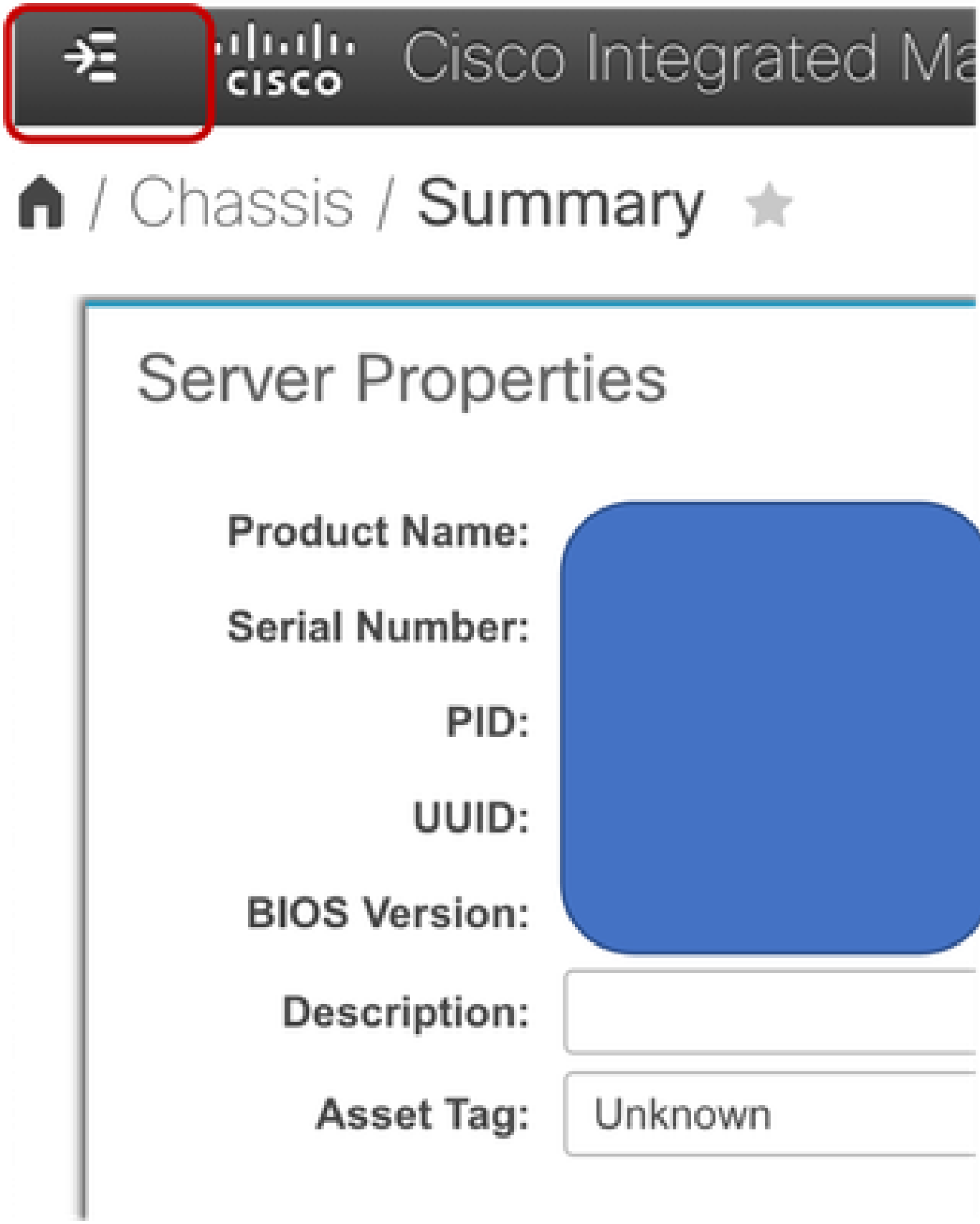
L'exemple de ce guide illustre la configuration LDAP sécurisée sur les serveurs UCS série C :

- Configurez un serveur DNS, permettant l'utilisation de noms de domaine pour le serveur LDAP au lieu d'une adresse IP sur le serveur UCS. Assurez-vous que les enregistrements A appropriés ont été configurés pour pointer vers les adresses IP du serveur LDAP et du serveur UCS série C.
- Configurez les services de certificats Windows sur le serveur LDAP, en activant la

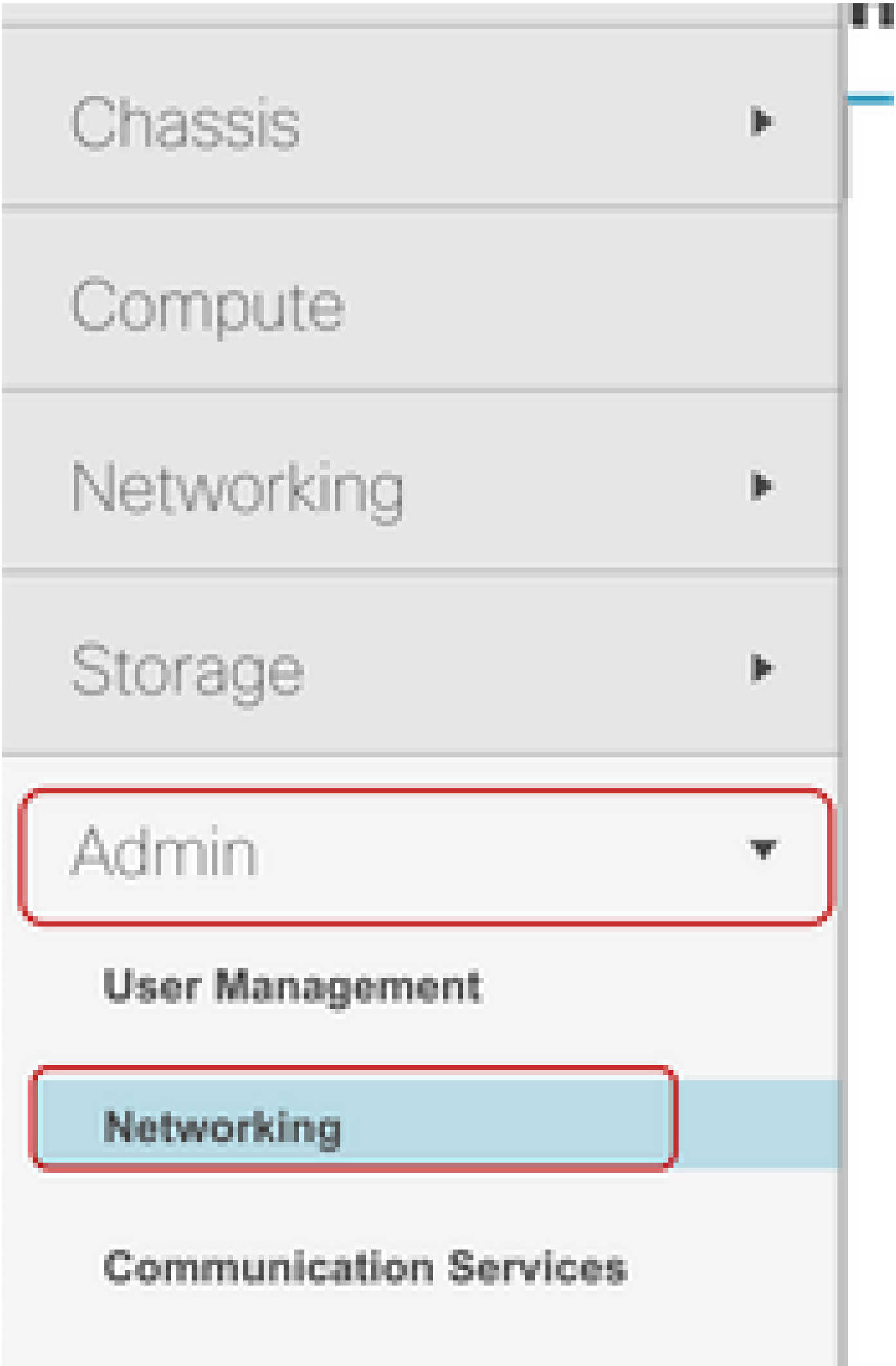
génération de certificats pour une communication LDAP sécurisée. Les certificats générés (racine et intermédiaire) sont téléchargés sur le serveur UCS série C.

Configuration côté serveur de la gamme UCS C

Pour configurer le serveur UCS série C afin qu'il interagisse avec un serveur DNS préconfiguré, accédez à l'interface CIMC du serveur UCS, puis cliquez sur l'icône de navigation située dans le coin supérieur gauche.

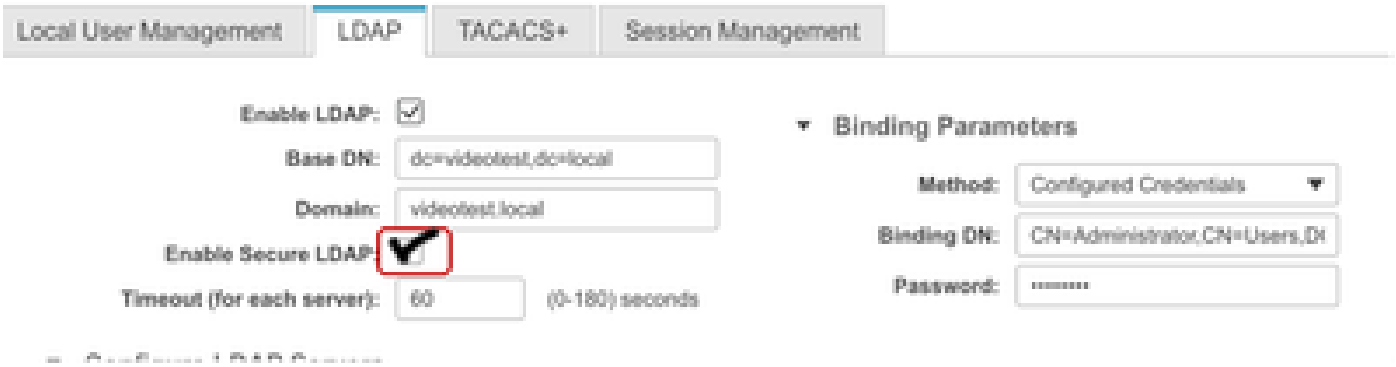


Accédez à Admin et choisissez Networking.


Chassis
Compute
Networking
Storage
Admin
User Management
Networking
Communication Services

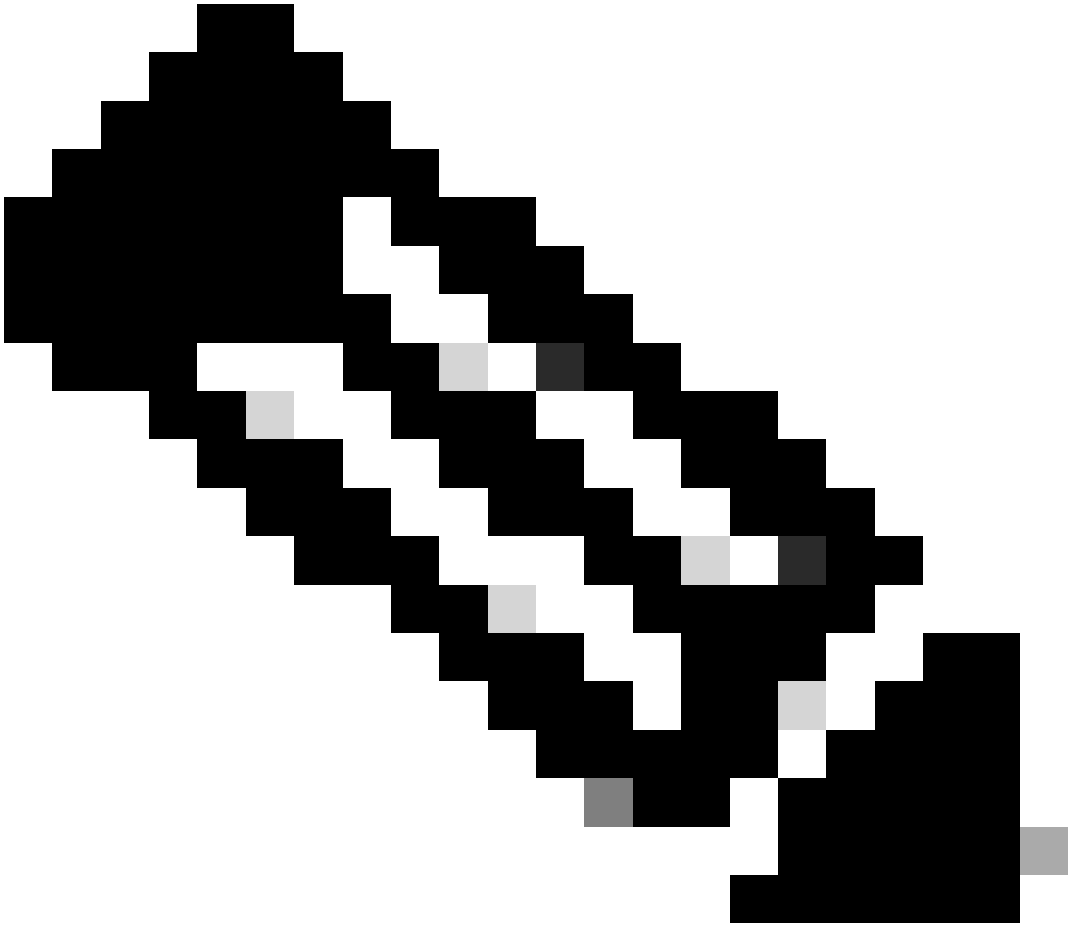
, configurez les paramètres BaseDN, Domain, Timeout et Bind en conformité avec les pratiques de configuration LDAP standard.

Ensuite, cochez la case Enable Secure LDAP.



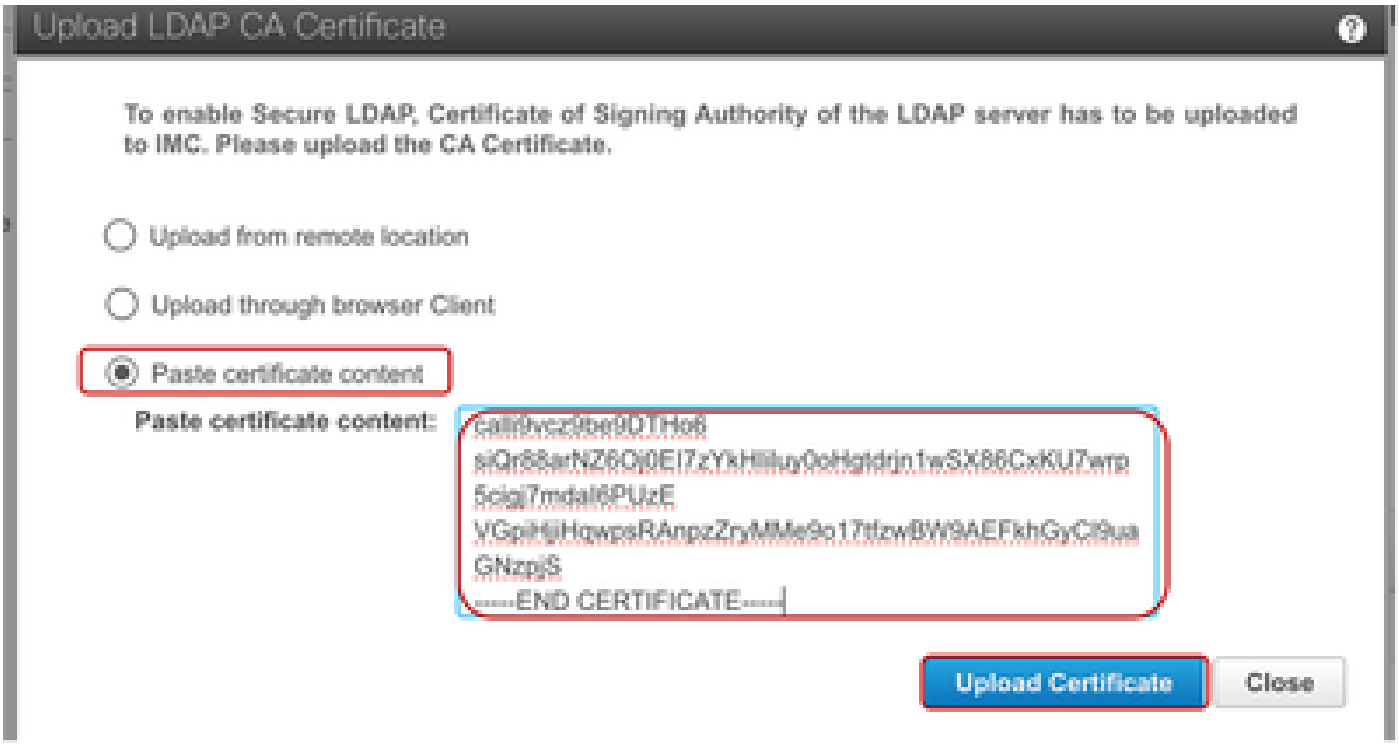
Dans la fenêtre contextuelle, sélectionnez l'option Coller le contenu du certificat.

Pour cette démonstration, un certificat auto-signé est utilisé, généré à partir de l'instance Windows Server exécutant Active Directory et enregistré dans un fichier texte. Ce certificat auto-signé a également été concaténé avec le certificat racine du même serveur pour former une chaîne de certificats.

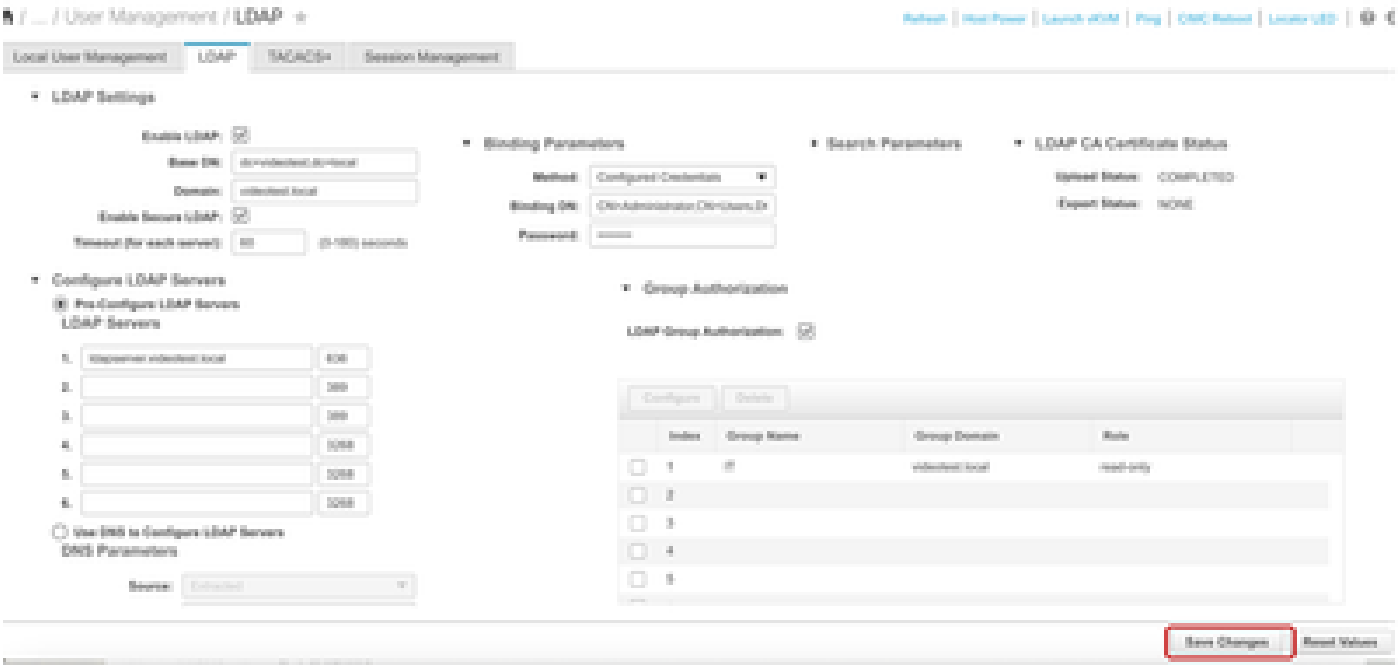


Remarque : Notez que l'intégralité du contenu du fichier X.509 (CER) codé en Base64, du -----BEGIN CERTIFICATE----- au -----END CERTIFICATE-----, doit être copiée, puis immédiatement à la ligne suivante, doit être le certificat suivant, du -----BEGIN CERTIFICATE----- au -----END CERTIFICATE-----, dans les cas où plusieurs certificats sont utilisés.

Collez le contenu copié dans le champ Paste Certificate Content et cliquez sur Upload Certificate.



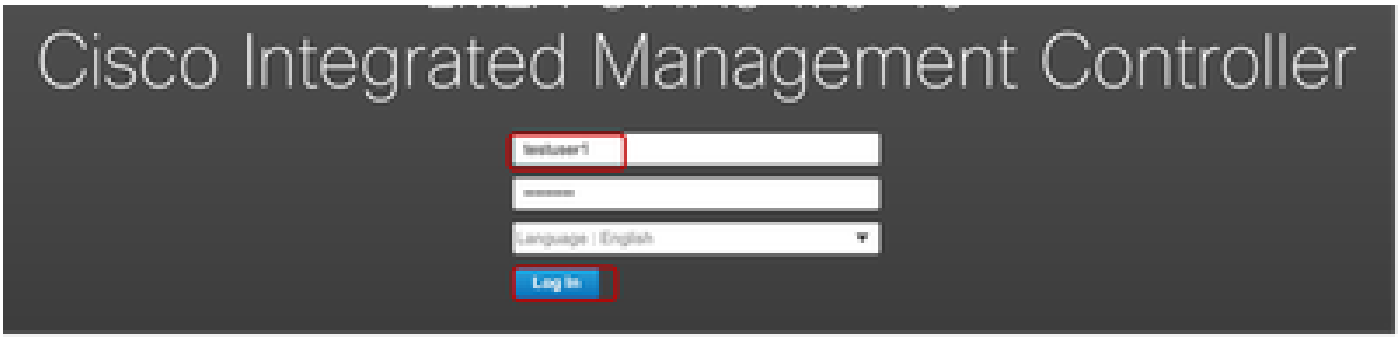
Tous les autres paramètres de Secure LDAP restent identiques à la configuration LDAP standard pour les serveurs C Series. Par conséquent, cliquez sur Save Changes sur la page de configuration LDAP globale.



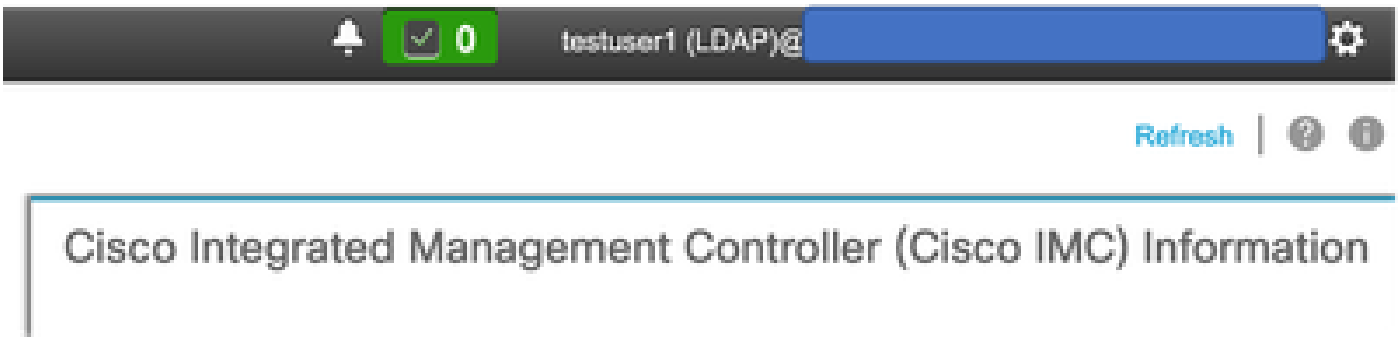
Le protocole LDAP sécurisé a été correctement configuré sur le serveur UCS série C.

Vérification

Pour le vérifier, essayez de vous connecter au serveur UCS série C à l'aide de l'un des comptes d'utilisateurs configurés dans Active Directory. Sélectionnez votre domaine et continuez à vous connecter.



La connexion de l'utilisateur de test 1 a réussi sur LDAP sécurisé



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.