Configurer LDAP dans l'appliance virtuelle Intersight

Table des matières

Introduction

Ce document décrit le processus de configuration de l'authentification LDAP dans un appareil virtuel privé Intersight (PVA).

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Protocole LDAP (Lightweight Directory Access Protocol).
- Appliance virtuelle privée Intersight.
- Serveur DNS (Domain Name Server).

Composants utilisés

- Appliance virtuelle privée Intersight.
- Microsoft Active Directory.
- Serveur DNS.

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

LDAP est un protocole utilisé pour accéder aux ressources d'un annuaire sur le réseau. Ces répertoires stockent des informations sur les utilisateurs, les organisations et les ressources. Le protocole LDAP fournit un moyen standard d'accès et de gestion de ces informations qui peuvent être utilisées pour les processus d'authentification et d'autorisation.

Ce document montre le processus de configuration pour ajouter l'authentification à distance via LDAP à un PVA Intersight.

Configurer

Configuration des paramètres de base LDAP

1. Accédez à System > Settings > AUTHENTICATION > LDAP/AD.
2. Cliquez sur Configurer LDAP.
3. Saisissez les informations requises. Examinez les recommandations suivantes :
    1. Le nom est défini arbitrairement et n'affecte pas la configuration.
    2. Pour BaseDN et BindDN, copiez et collez les valeurs correspondantes à partir de votre configuration Active Directory (AD).
    3. La valeur par défaut de l'attribut de groupe est member.

    > Remarque : Dans d'autres outils de gestion UCS tels que UCSM ou CIMC, l'attribut Group est défini sur memberOf. Dans Intersight, il est recommandé de le laisser comme membre.

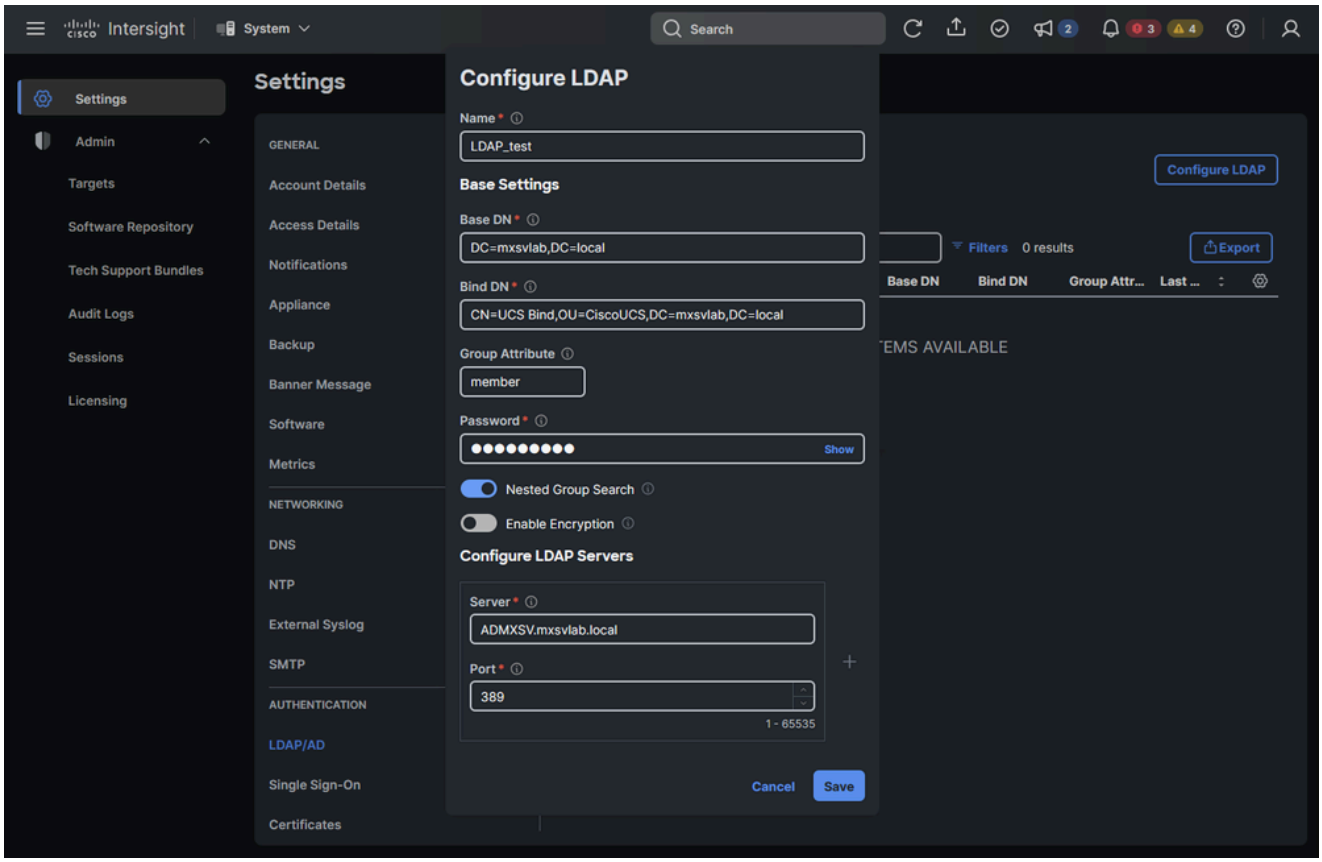
    4. Entrez le mot de passe de ce fournisseur LDAP.
    5. Activez l'option Nested Group Search si vous souhaitez autoriser une recherche récursive dans votre Active Directory pour tous les groupes à partir de la racine et leurs groupes contenus.
    6. Laissez Enable Encryption désactivé pour une configuration LDAP normale. Si un LDAP sécurisé est nécessaire, activez-le et assurez-vous de consulter la section Configuration de LDAP (LDAP sécurisé) pour connaître les étapes complémentaires à

configurer.

4. Ajoutez la configuration d'un serveur LDAP :
    1. Dans Serveur, introduisez l'adresse IP ou le nom d'hôte du serveur LDAP.

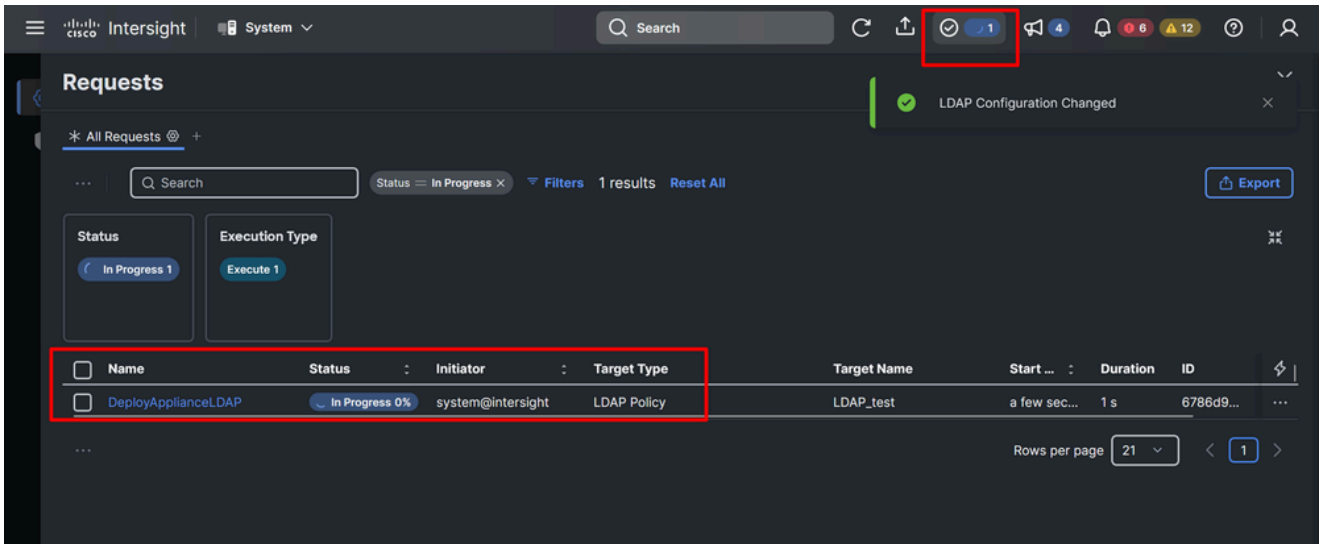
    > ⚠ Mise en garde : Si le nom d'hôte est utilisé, assurez-vous que le DNS est en mesure de mapper correctement ce nom d'hôte.

    2. Le port par défaut et recommandé pour LDAP est 389 .
5. Cliquez sur Save.



Exemple de configuration des paramètres LDAP de base

6. Surveillez le workflow DeployApplianceLDAP à partir des requêtes dans la barre supérieure.



Demande de déploiement

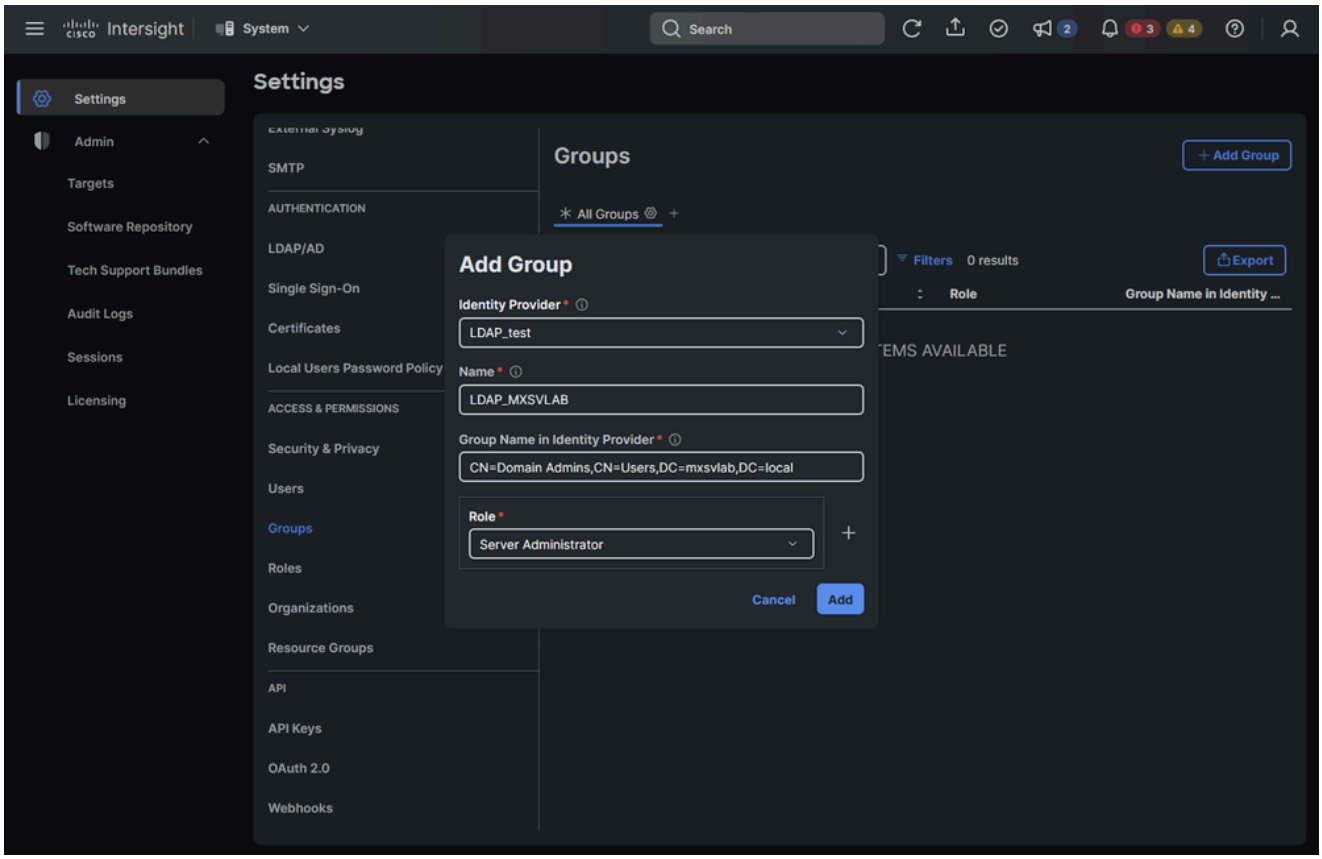
Configuration des utilisateurs et des groupes

Une fois le workflow DeployApplianceLDAP terminé, vous pouvez configurer des groupes ou des utilisateurs individuels.

Si vous décidez d'utiliser des groupes, l'autorisation est accordée à tous les utilisateurs qui appartiennent à ce groupe. Si vous utilisez des utilisateurs individuels, vous devez ajouter chaque utilisateur avec son propre rôle d'autorisation.

Configurer les groupes

1. Accédez à System > Settings > ACCESS & PERMISSION > Groups.
2. Cliquez sur Ajouter un groupe.
3. Sélectionnez le fournisseur d'identité. Il s'agit du nom que vous avez défini dans la section Configurer les paramètres de base LDAP.
4. Définissez un nom pour le groupe.
5. Entrez la valeur Nom du groupe dans Fournisseur d'identités. Il doit correspondre aux configurations du groupe dans votre serveur LDAP.
6. Sélectionnez le rôle en fonction du niveau d'accès que vous souhaitez fournir aux utilisateurs de ce groupe. Voir Rôles et privilèges dans Intersight.



Exemple de configuration d'un groupe

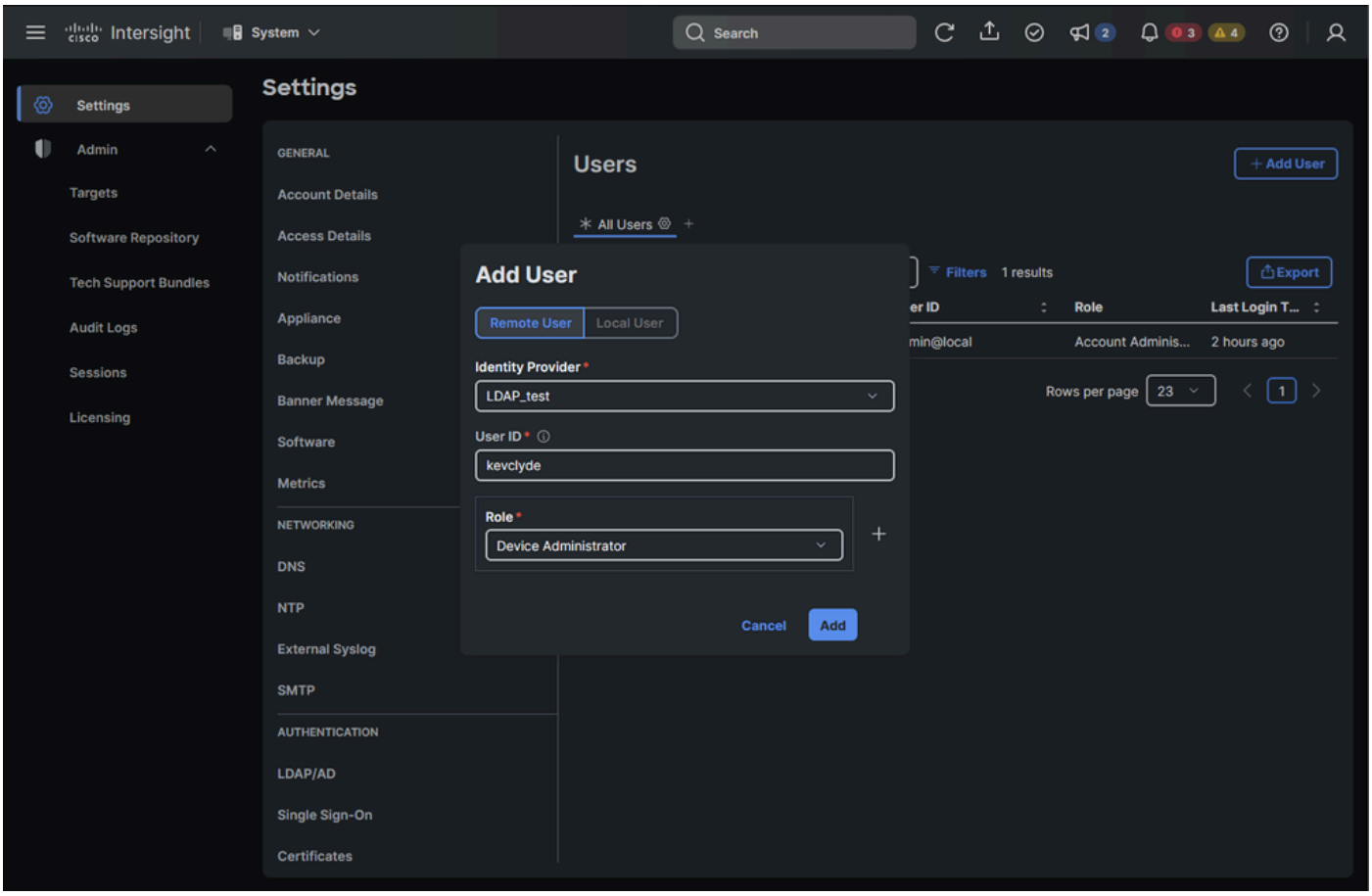
Configurer des utilisateurs

Si vous préférez configurer des utilisateurs individuels plutôt que des groupes, suivez les instructions suivantes :

1. Accédez à System > Settings > ACCESS & PERMISSION > Users.
2. Cliquez sur Ajouter un utilisateur.
3. Sélectionnez Utilisateur distant.
4. Sélectionnez le fournisseur d'identité. Il s'agit du nom que vous avez défini dans la section Configurer les paramètres de base LDAP.
5. Définissez un ID utilisateur.

> Conseil : Pour utiliser le nom d'utilisateur comme méthode de connexion, copiez dans le champ User ID, la valeur configurée en tant que sAMAccountName dans votre serveur LDAP.
> Si vous voulez utiliser l'e-mail, assurez-vous que vous définissez l'e-mail de l'utilisateur dans l'attribut mail dans le serveur LDAP.

6. Sélectionnez le rôle en fonction du niveau d'accès que vous souhaitez fournir à l'utilisateur. Voir Rôles et privilèges dans Intersight.

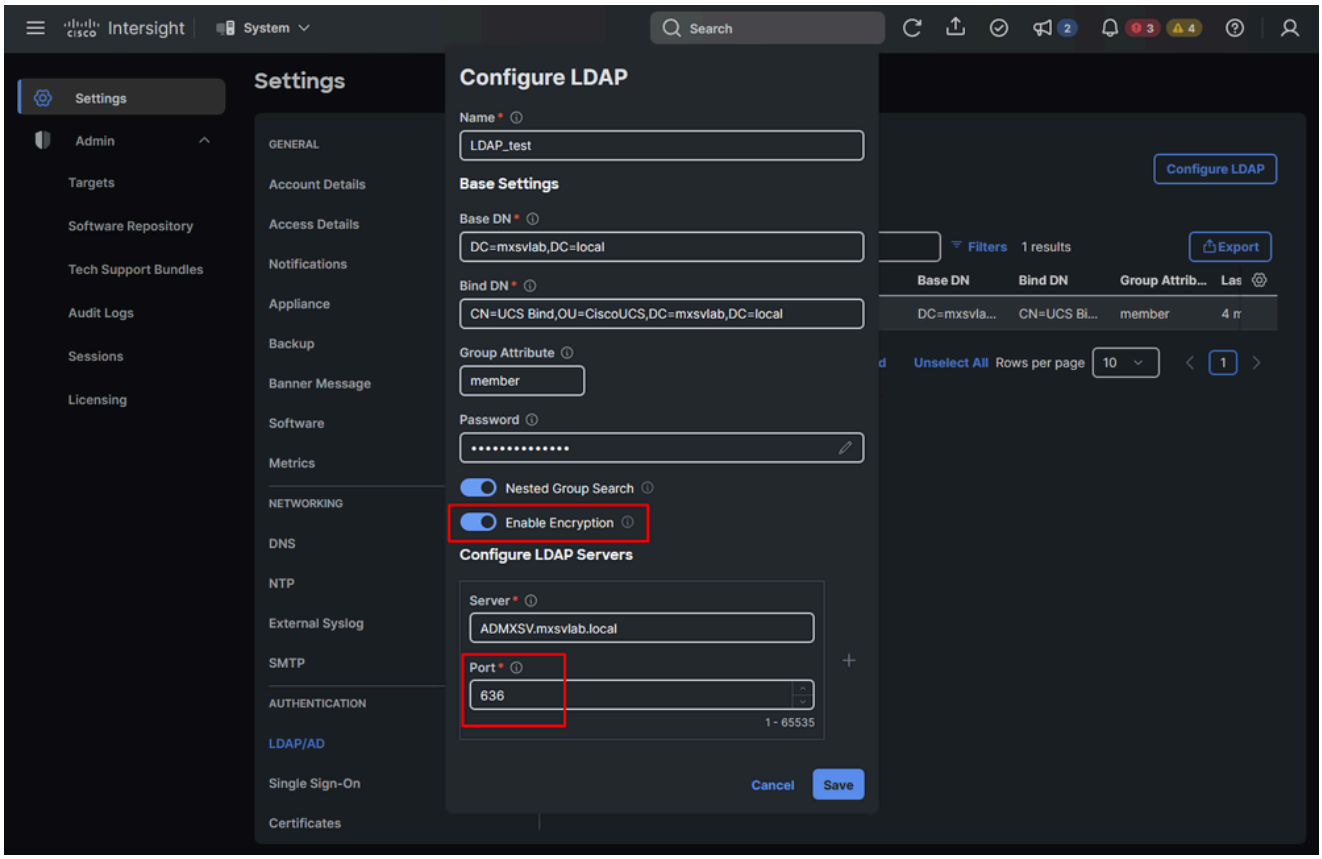


Exemple de configuration pour un utilisateur

Configuration de LDAP (Secure LDAP)

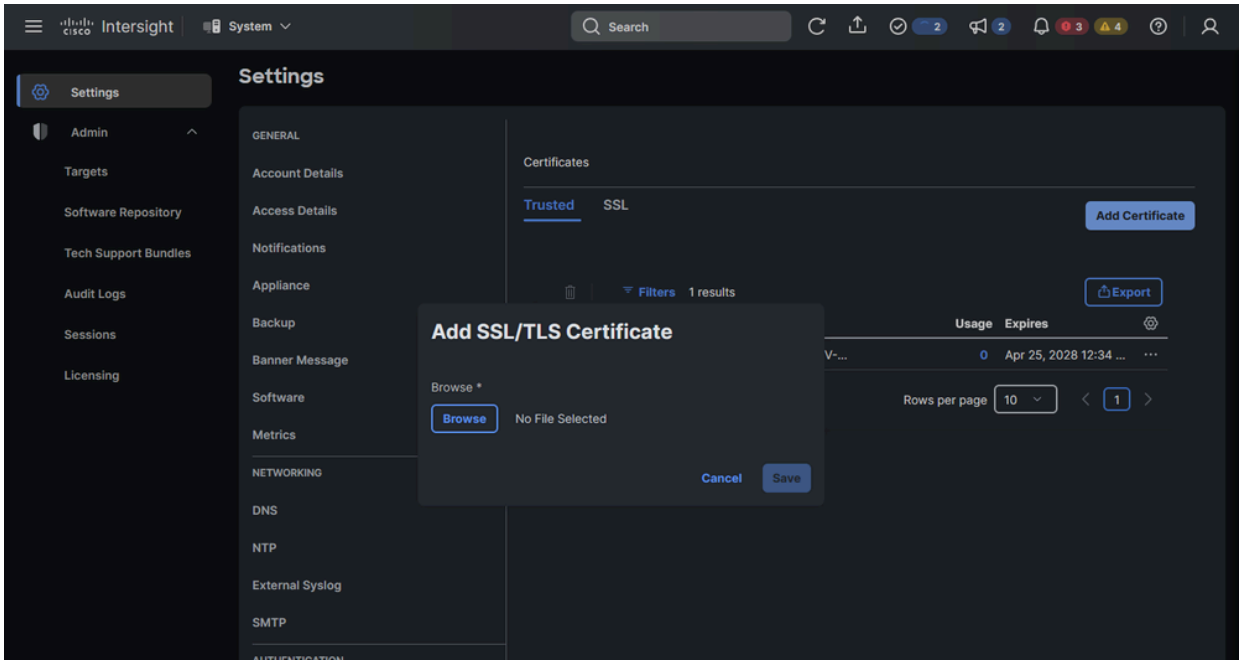
Si vous souhaitez que votre communication LDAP soit sécurisée par cryptage, vous devez disposer d'un certificat signé par votre autorité de certification. Assurez-vous d'appliquer ces modifications à la configuration :

1. Suivez les étapes de Configuration des paramètres de base LDAP mais assurez-vous de déplacer le curseur Enable Encryption vers la droite (Étape 3.g).
2. Assurez-vous que le port utilisé est 636 ou 3269 qui sont les ports qui prennent en charge LDAPS (sécurisé). Tous les autres ports prennent en charge LDAP sur TLS.



Modifications de configuration pour LDAP sécurisé

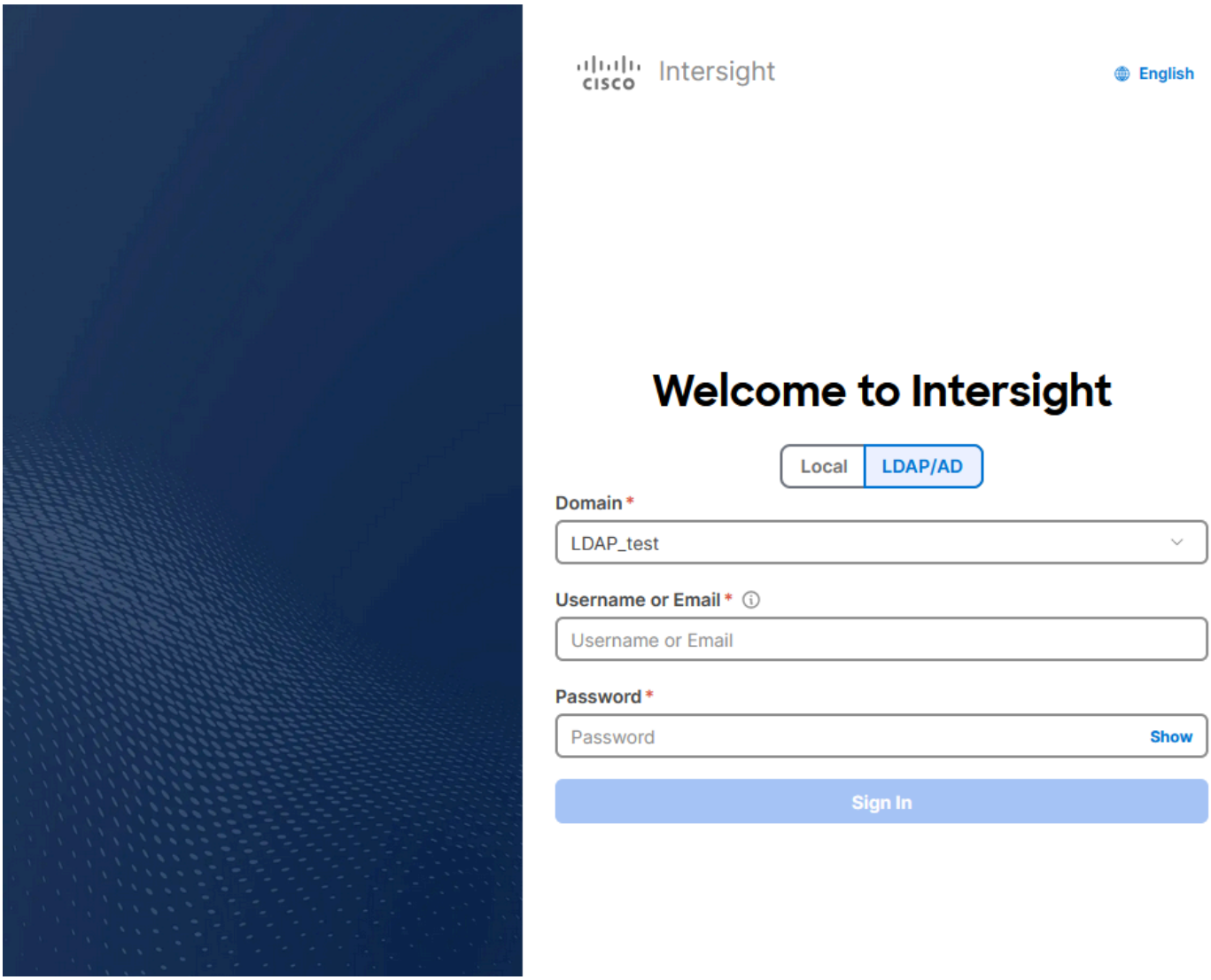
3. Enregistrez la configuration et attendez la fin du workflow DeployApplianceLDAP.
4. Ajoutez un certificat en procédant comme suit :
    1. Accédez à System > Settings > AUTHENTICATION > Certificats > Approuvés.
    2. Cliquez sur Ajouter un certificat.
    3. Cliquez sur Parcourir et sélectionnez un fichier .pem qui contient le certificat émis par votre autorité de certification.



Configuration pour ajouter un certificat

Vérifier

Dans votre navigateur, accédez à l'URL de votre appliance virtuelle Intersight. L'écran affiche désormais une option de connexion avec les informations d'identification LDAP :

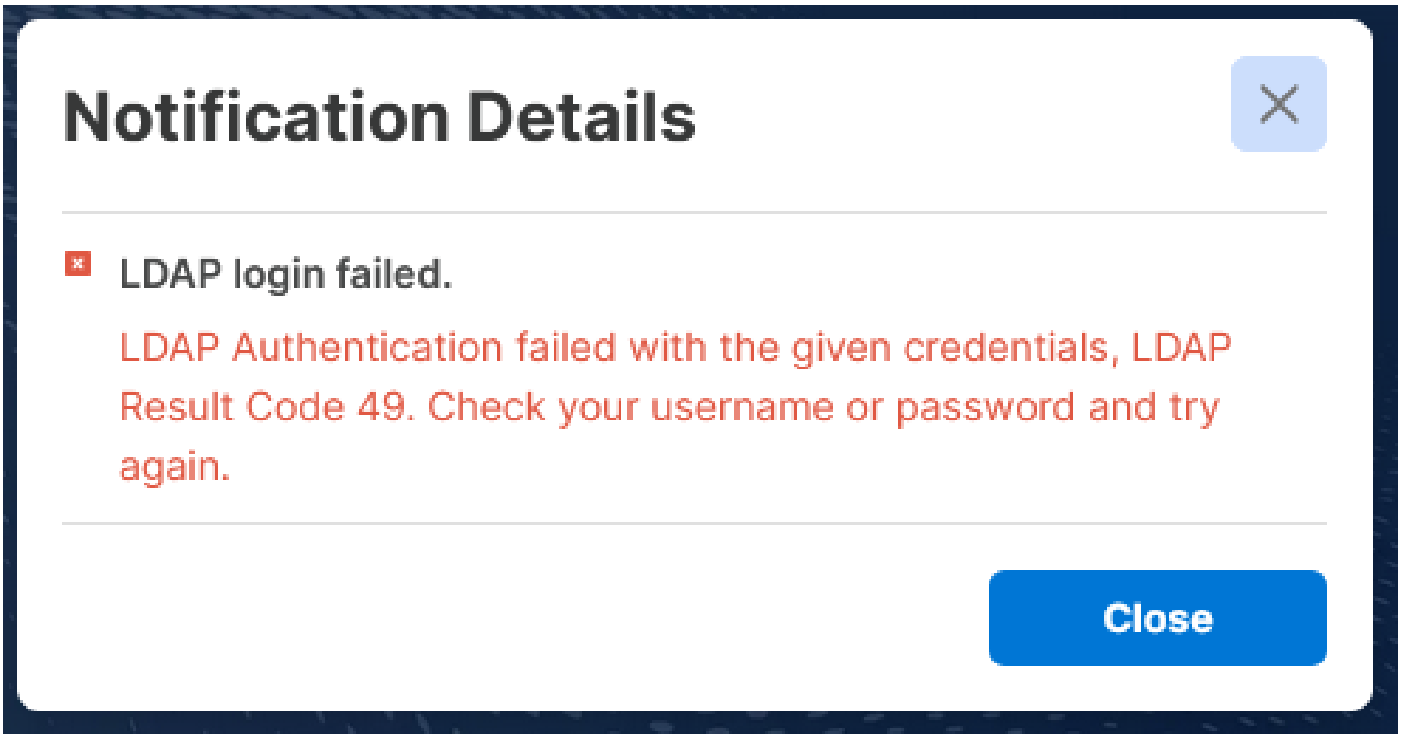


Configuration LDAP activée depuis l'écran de connexion

Dépannage

Si la connexion échoue, les messages d'erreur fournissent des indications sur ce qui pourrait être erroné.

Erreur 1. Détails d'accès incorrects

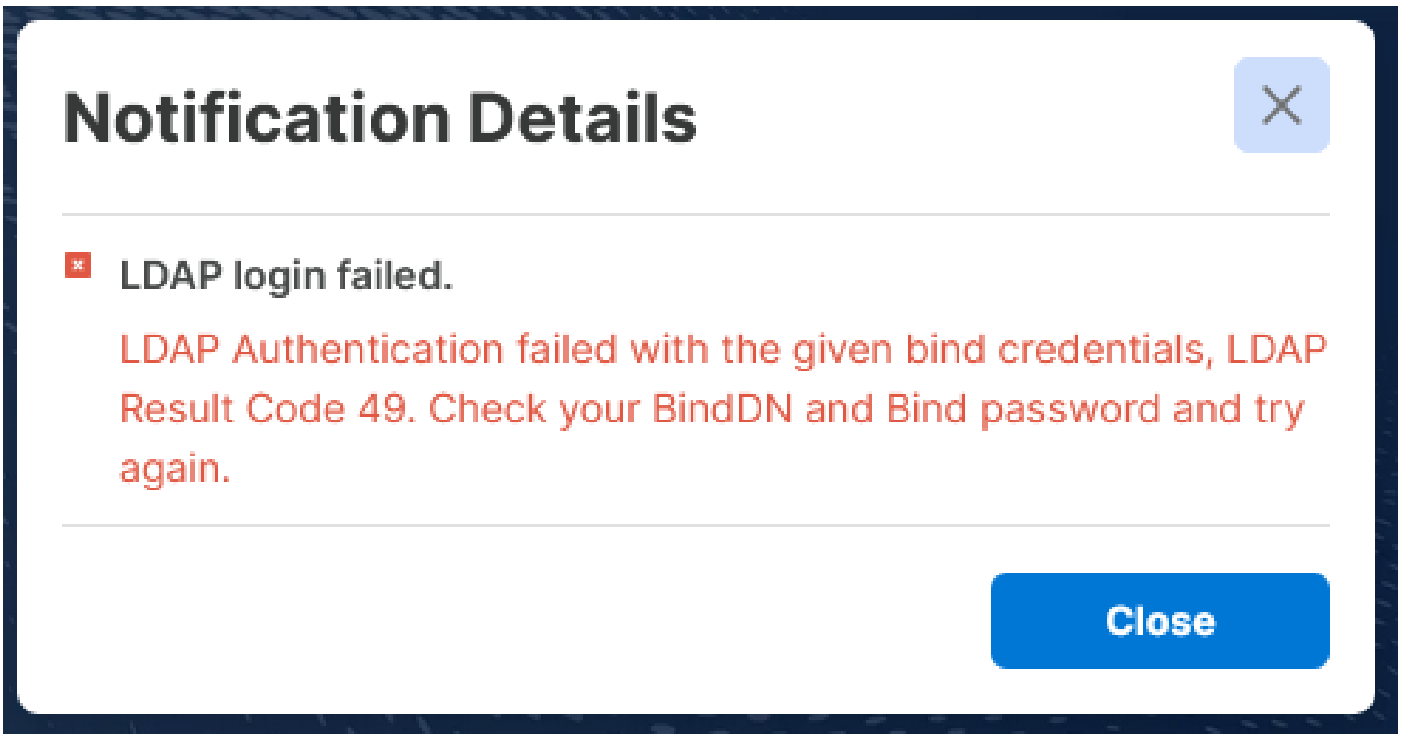


Message d'erreur pour erreur de mot de passe

Cette erreur signifie que les données d'accès sont incorrectes.

1. Vérifiez que le nom d'utilisateur et le mot de passe sont corrects.

Erreur 2. Mauvaise liaison des données

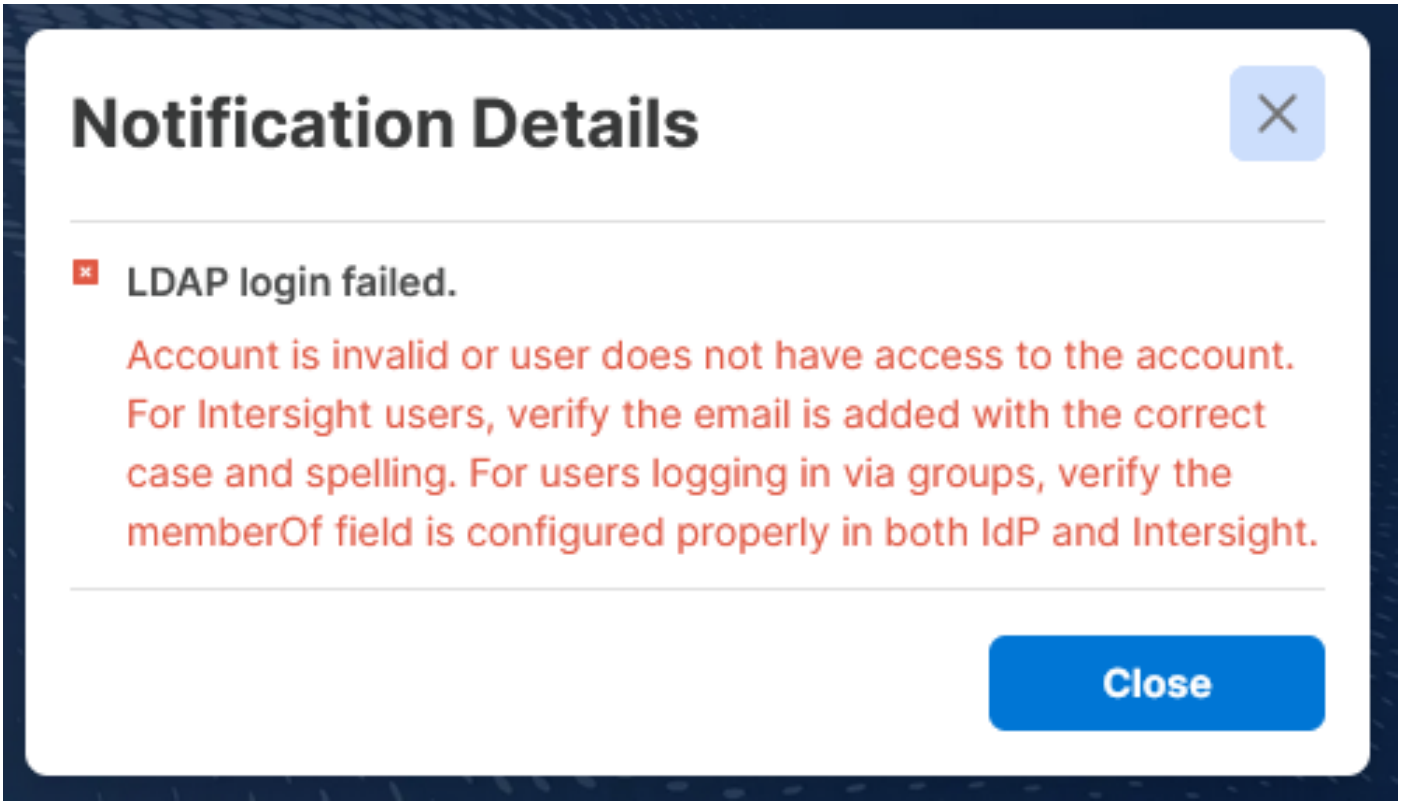


Message d'erreur pour des données de liaison incorrectes

Cette erreur signifie que les données de liaison sont incorrectes.

1. Vérifiez le BindDN.
2. Vérifiez le mot de passe de liaison configuré dans les paramètres LDAP.

Erreur 3. Impossible de trouver l'utilisateur

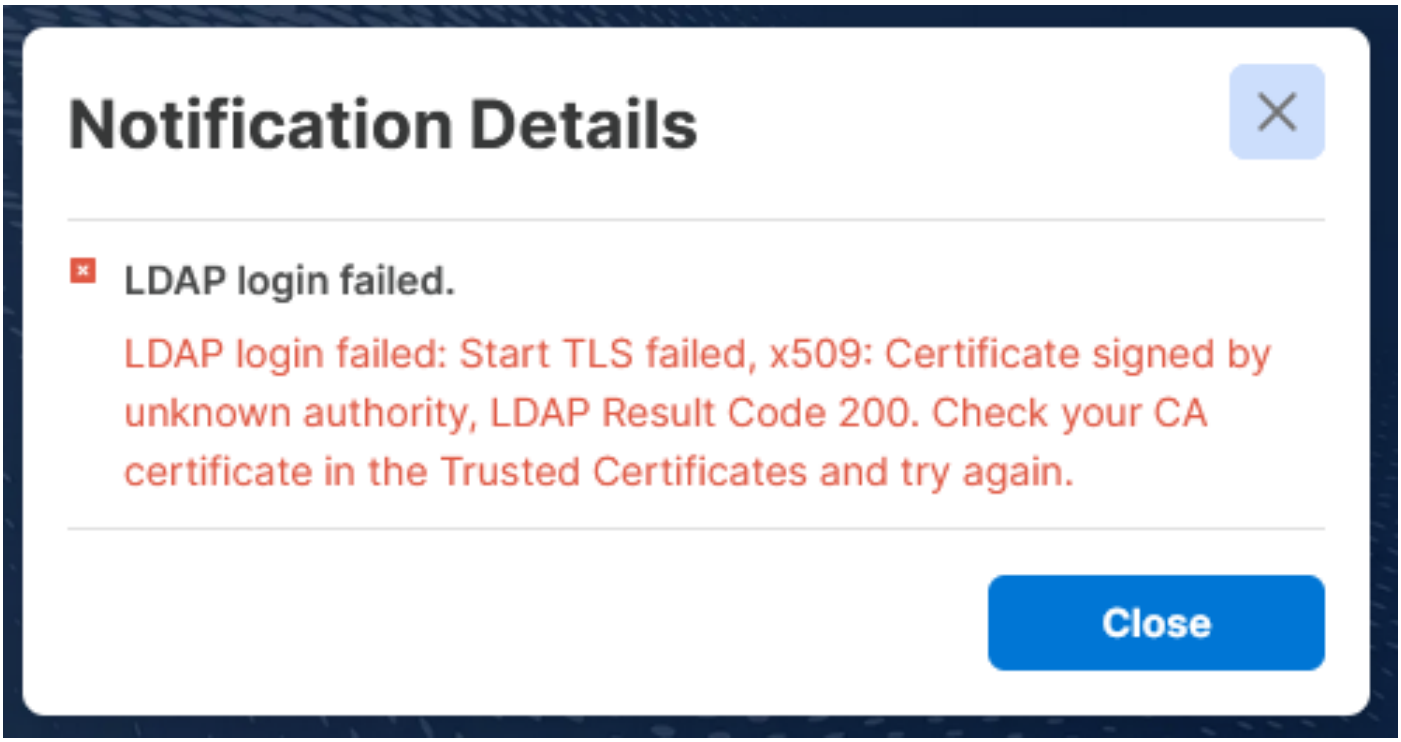


Message d'erreur pour l'utilisateur introuvable

Ceci est déclenché lorsque la recherche dans le serveur LDAP ne renvoie aucun utilisateur autorisé. Vérifiez que les paramètres suivants sont corrects :

1. Cochez BaseDN. Les paramètres utilisés pour rechercher l'utilisateur sont incorrects.
2. Assurez-vous que l'attribut de groupe est défini sur member au lieu de memberOf.
3. Vérifiez que le nom du groupe dans le fournisseur d'identités dans la configuration Groups est correct. Ceci s'applique uniquement lorsque l'autorisation est fournie via des groupes.
4. Vérifiez que l'adresse e-mail de l'utilisateur est définie correctement dans le champ mail de la configuration Active Directory de l'utilisateur. Cela s'applique uniquement lorsque l'autorisation est accordée à des utilisateurs individuels.

Erreur 4. Certificat incorrect

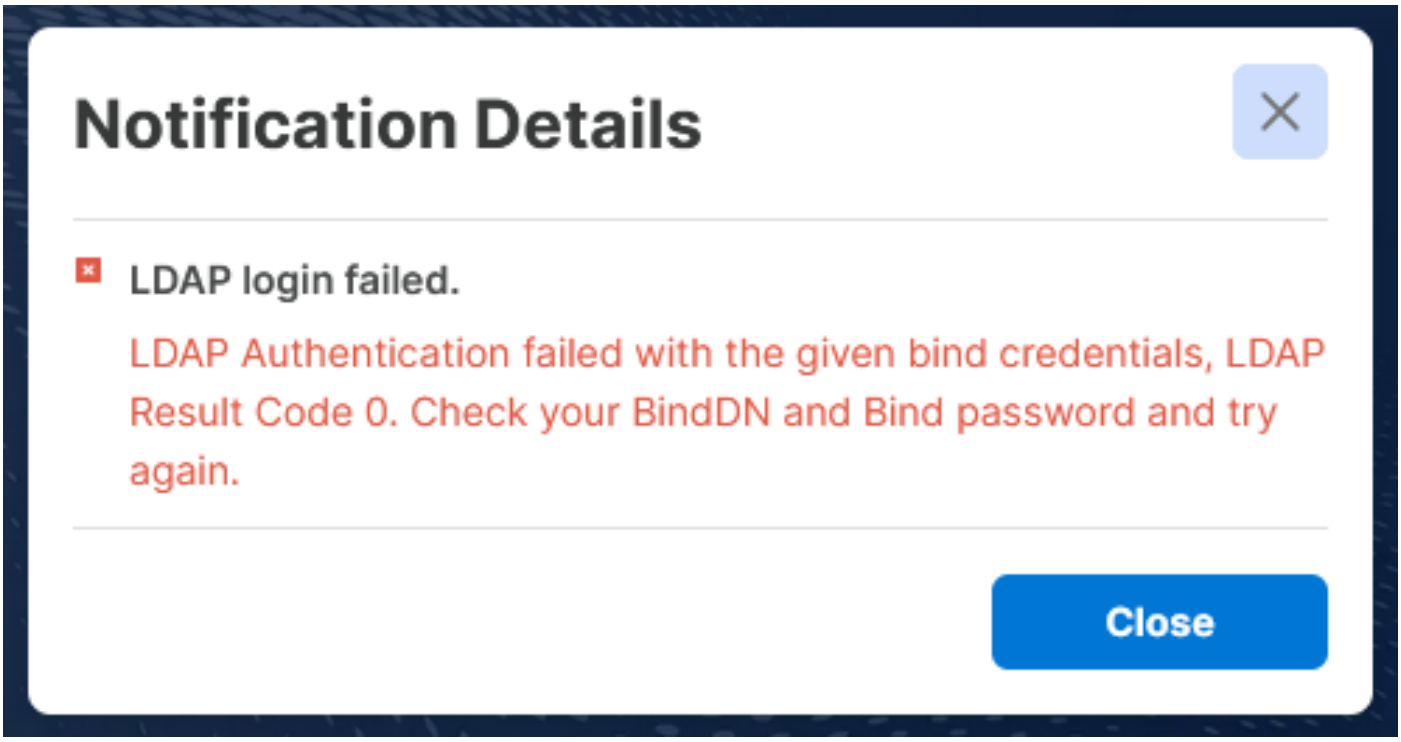


Message d'erreur pour certificat incorrect

Si le protocole LDAP chiffré est activé :

1. Vérifiez que le certificat est configuré et qu'il inclut le certificat complet correct.

Erreur 5. Activer le chiffrement est utilisé avec un port sécurisé



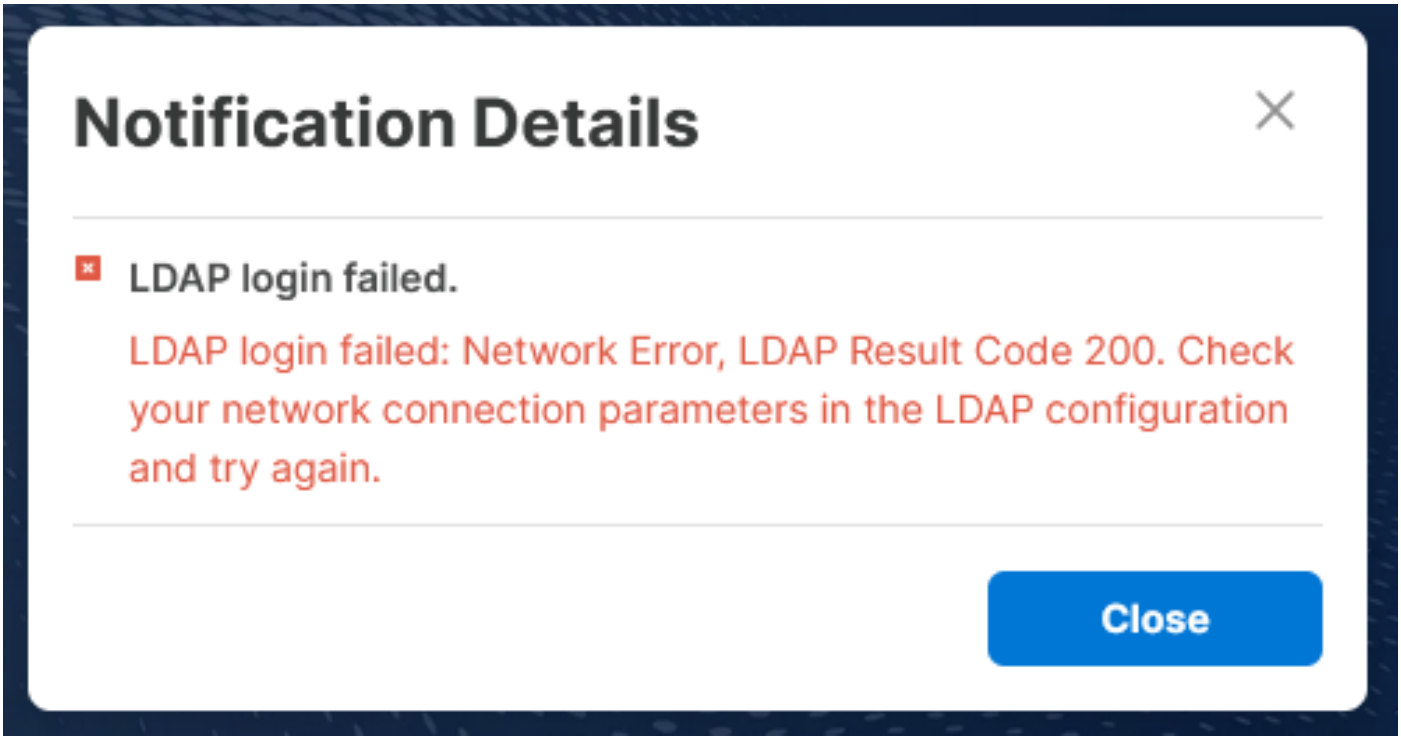
Le message d'erreur Activer le chiffrement est désactivé

Cette erreur apparaît quand Enable Encryption n'est pas activé mais qu'un port pour LDAP

sécurisé est configuré.

1. Assurez-vous d'utiliser le port 389 si le cryptage n'est pas activé.

Erreur 6. Paramètres de connexion incorrects



Message d'erreur pour le port incorrect

Cette erreur signifie qu'il n'a pas été possible d'établir une connexion réussie au serveur LDAP. Veuillez vérifier :

1. Le serveur DNS doit résoudre le nom d'hôte du serveur LDAP sur l'adresse IP correcte.
2. L'appliance Intersight peut atteindre le serveur LDAP.
3. Assurez-vous que le port 389 est utilisé pour LDAP non chiffré, 636 ou 3269 pour LDAP sécurisé (LDAPS) et tout autre port pour TLS (activez le chiffrement et configurez un certificat).

Informations connexes

- Intégration de Cisco Intersight Virtual Appliance avec LDAP (vidéo)
- Configurer les paramètres LDAP dans l'appliance Intersight
- Rôles et privilèges dans Intersight
- Exemple de configuration de LDAP dans UCSM

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.