Configurer l'authentification et l'autorisation externes via LDAPS pour l'accès à Secure Network Analytics Manager

Contenu

Introduction
Conditions préalables
Conditions requises
Components Used
Configuration
Étape A. Connectez-vous au contrôleur de domaine AD et exportez le certificat SSL utilisé pour LDAP.
Étape B. Connectez-vous au gestionnaire SNA pour ajouter le certificat du serveur LDAP et la chaîne racine.
Étape C. Ajout de la configuration du service externe LDAP
SNA version 7.2 ou ultérieure
SNA version 7.1
Étape D. Configurez les paramètres d'autorisation.
Autorisation locale
Autorisation distante via LDAP
Vérification
Dépannage
Informations connexes

Introduction

Ce document décrit la configuration de base d'un gestionnaire Secure Network Analytics Manager (anciennement Stealthwatch Management Center) version 7.1 ou ultérieure pour utiliser l'authentification externe et, avec la version 7.2.1 ou ultérieure, pour utiliser l'autorisation externe avec LDAPS.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Cisco Secure Network Analytics (anciennement Stealthwatch)
- Fonctionnement général de LDAP et SSL
- Gestion générale de Microsoft Active Directory

Components Used

Les informations de ce document sont basées sur les composants suivants :

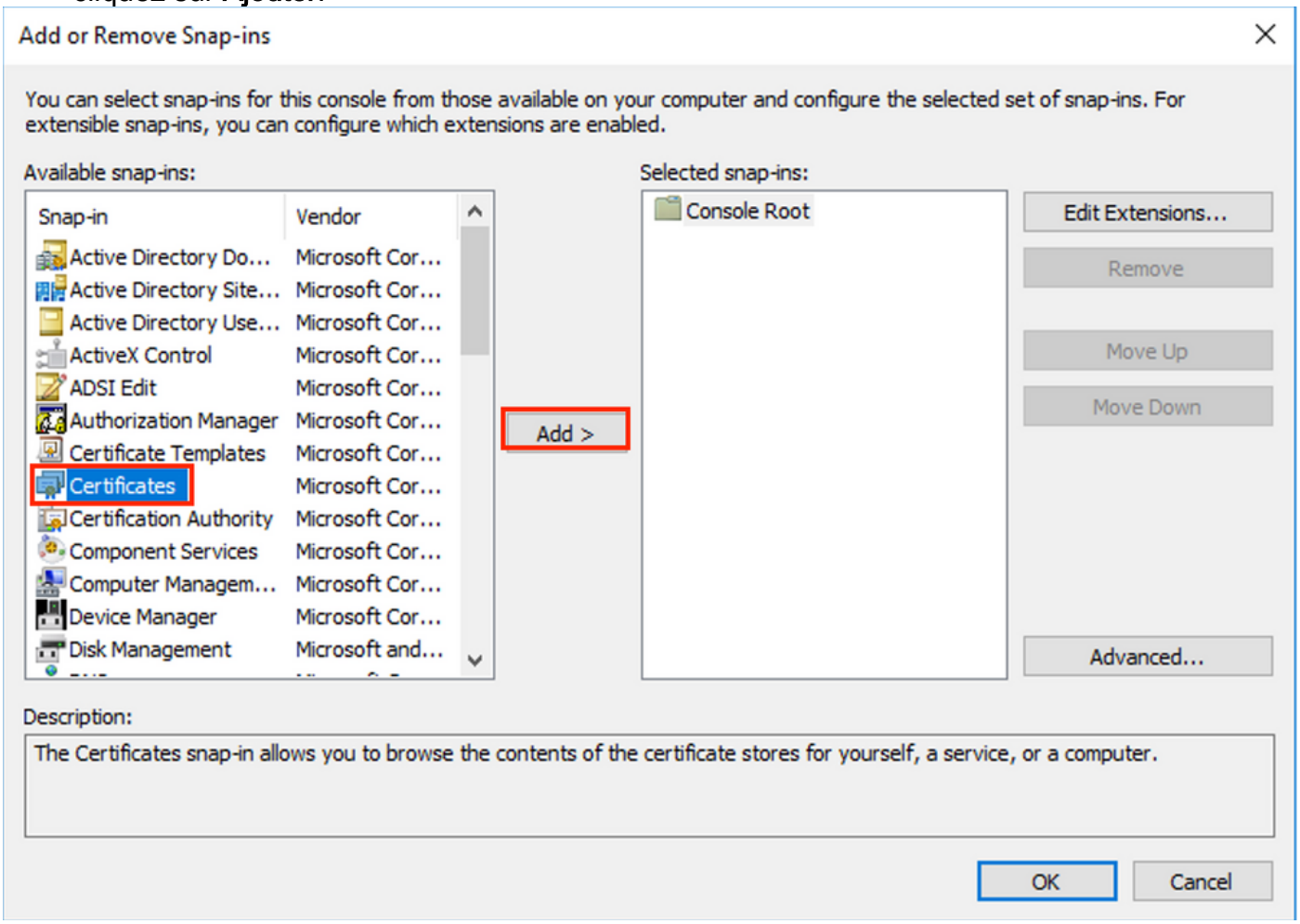
- Cisco Secure Network Analytics Manager (anciennement SMC) version 7.3.2
- Windows Server 2016 configuré en tant que contrôleur de domaine Active Directory

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.

Configuration

Étape A. Connectez-vous au contrôleur de domaine AD et exportez le certificat SSL utilisé pour LDAP.

1. Pour Windows Server 2012 ou version ultérieure, sélectionnez **Exécuter** dans le menu Démarrer, puis entrez **certlm.msc** et passez à l'étape **8**.
2. Pour les versions plus anciennes de Windows Server, sélectionnez **Exécuter** dans le menu Démarrer, puis saisissez **mmc**.
3. Dans le menu Fichier, sélectionnez **Ajouter/Supprimer un composant logiciel enfichable**.
4. Dans la liste Composants logiciels enfichables disponibles, sélectionnez **Certificats**, puis cliquez sur **Ajouter**.

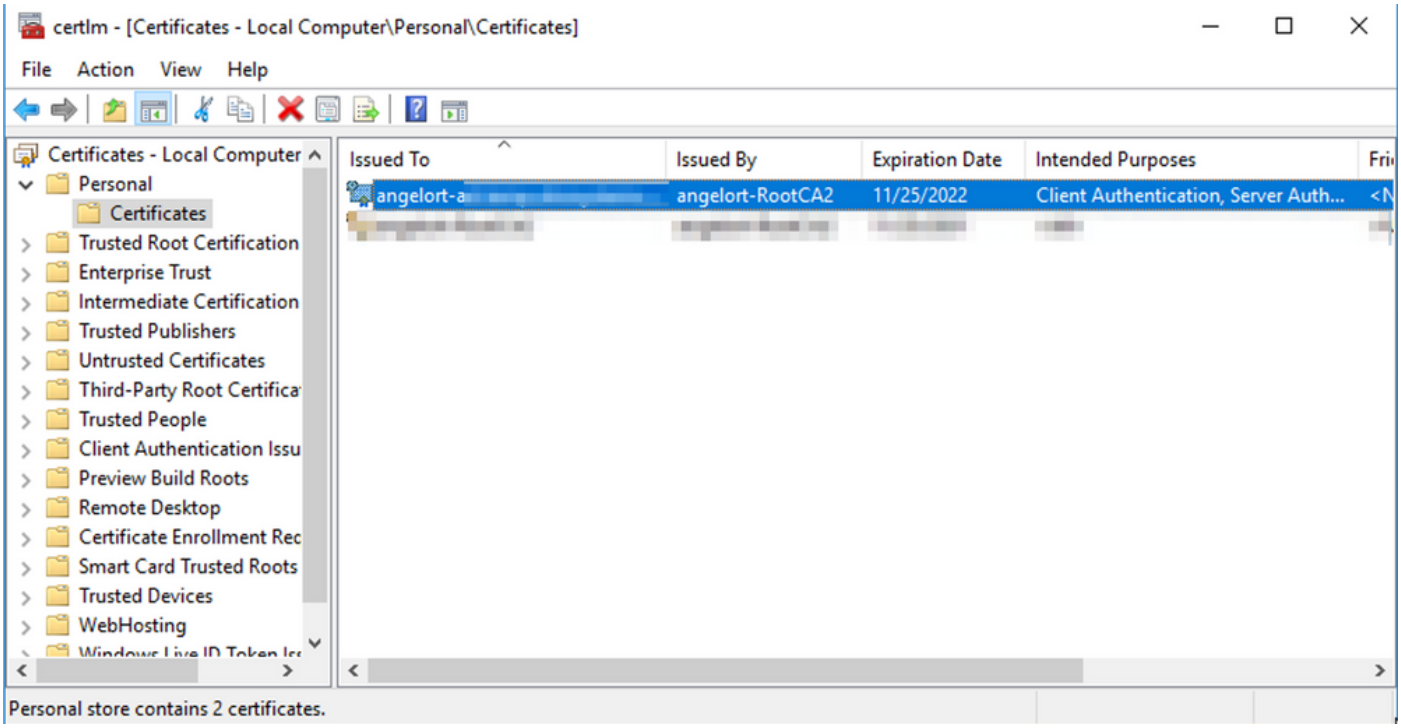


5. Dans la fenêtre **du composant logiciel enfichable Certificats**, sélectionnez **Compte ordinateur**, puis sélectionnez **Suivant**.

6. Laissez **l'ordinateur local** sélectionné, puis sélectionnez **Terminer**.

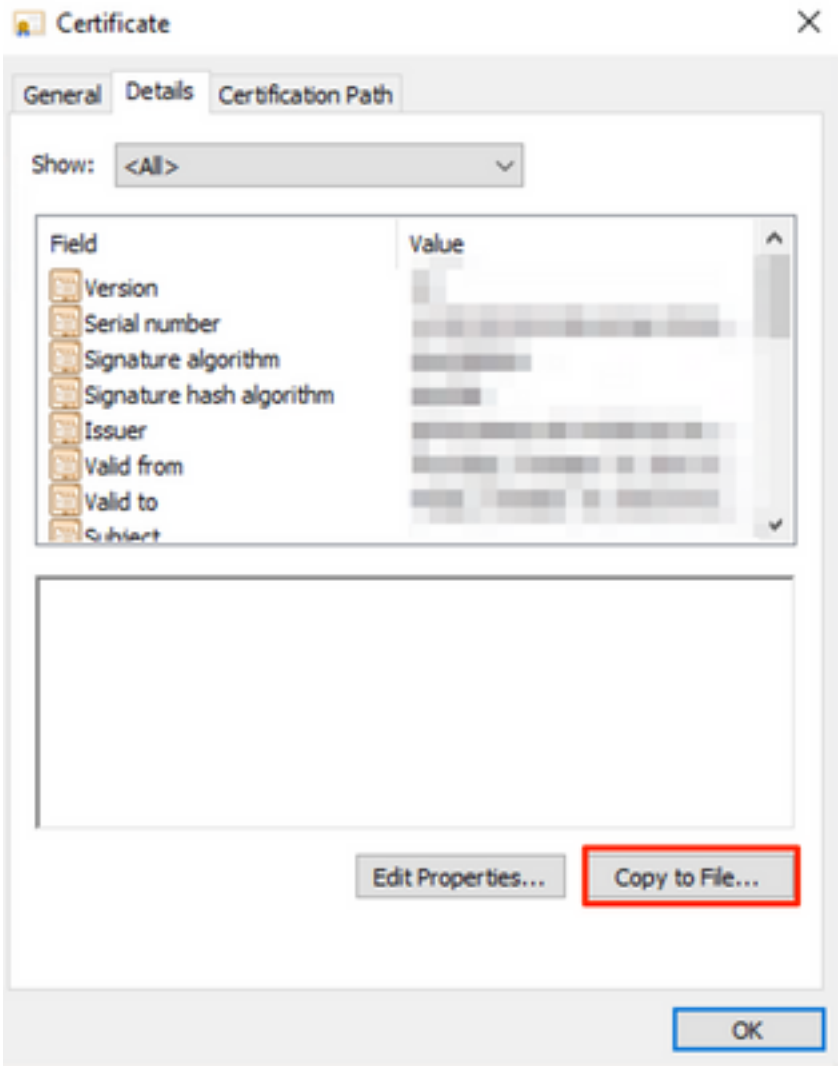
7. Dans la fenêtre **Ajouter ou supprimer un composant logiciel enfichable**, sélectionnez **OK**.

8. Accédez à **Certificats (Ordinateur local) > Personnel > Certificats**



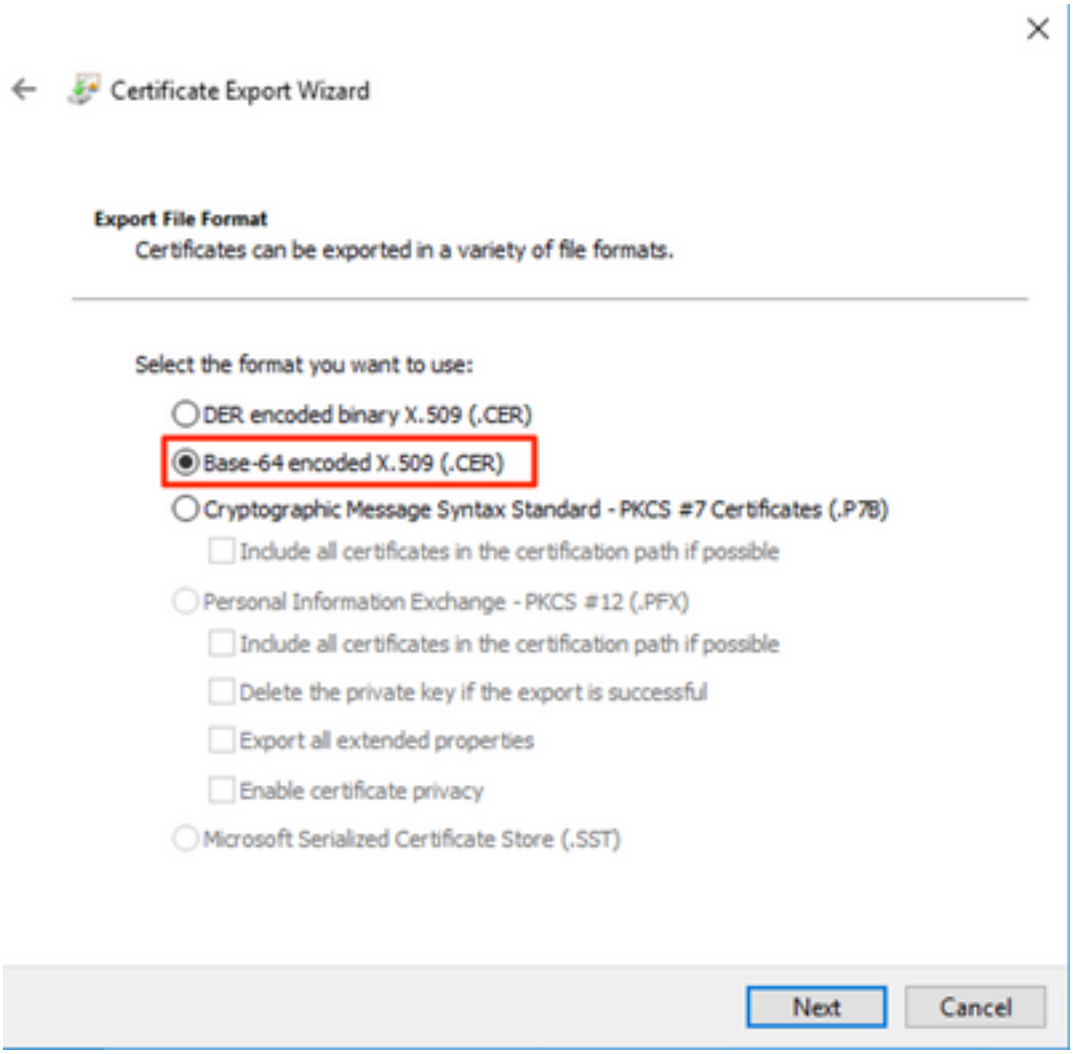
9. Sélectionnez et cliquez avec le bouton droit sur le certificat SSL utilisé pour l'authentification LDAPS sur votre contrôleur de domaine, puis cliquez sur **Ouvrir**.

10. Accédez à l'onglet **Détails** > cliquez sur **Copier dans un fichier > Suivant**

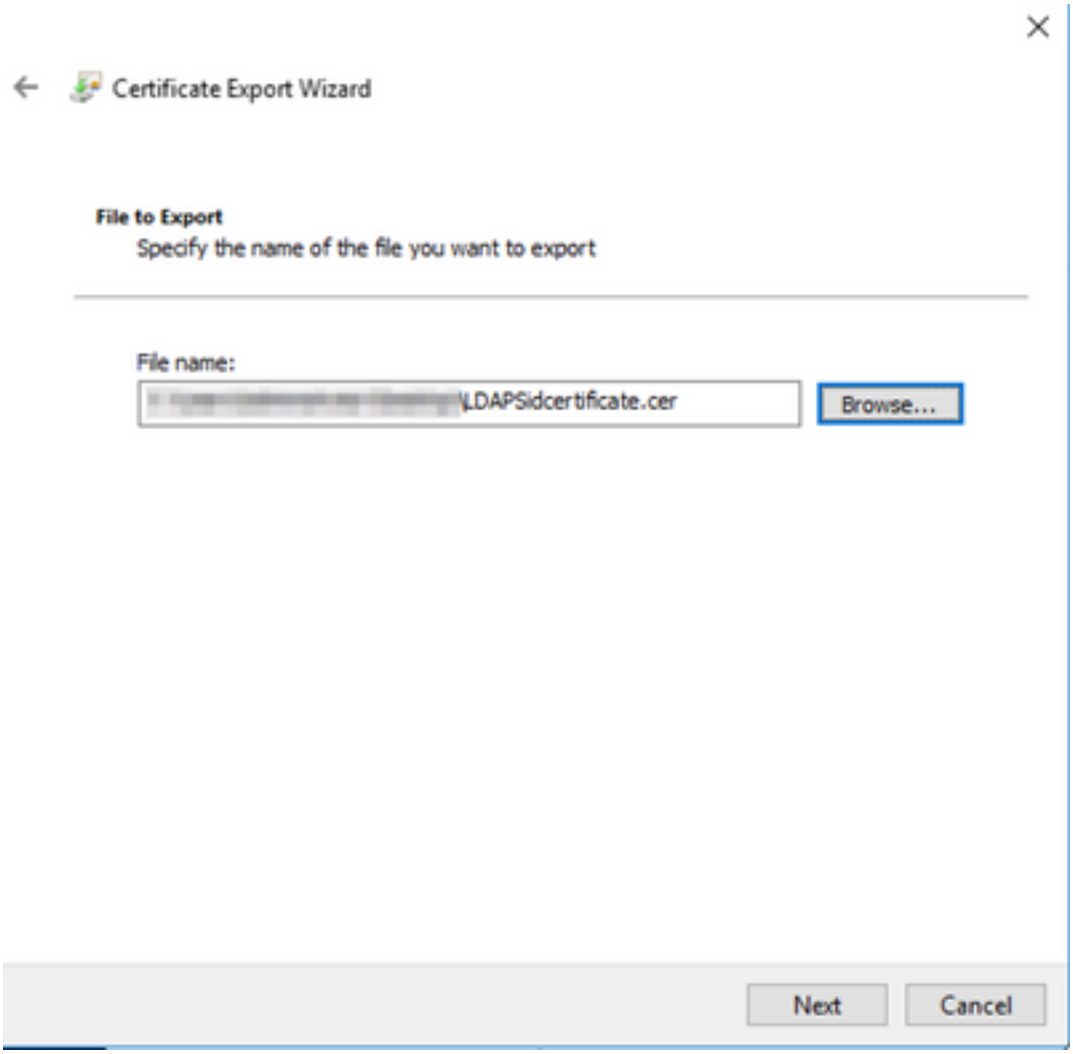


11. Assurez-vous que **Non, ne pas exporter la clé privée** est sélectionné et cliquez sur **Suivant**

12. Sélectionnez le format **X.509 codé en base-64** et cliquez sur **Suivant**.



13. Sélectionnez un emplacement pour stocker le certificat, nommez le fichier et cliquez sur **Suivant**.



14. Cliquez sur **Terminer**, vous devez obtenir une “ L'exportation a réussi. ” message.

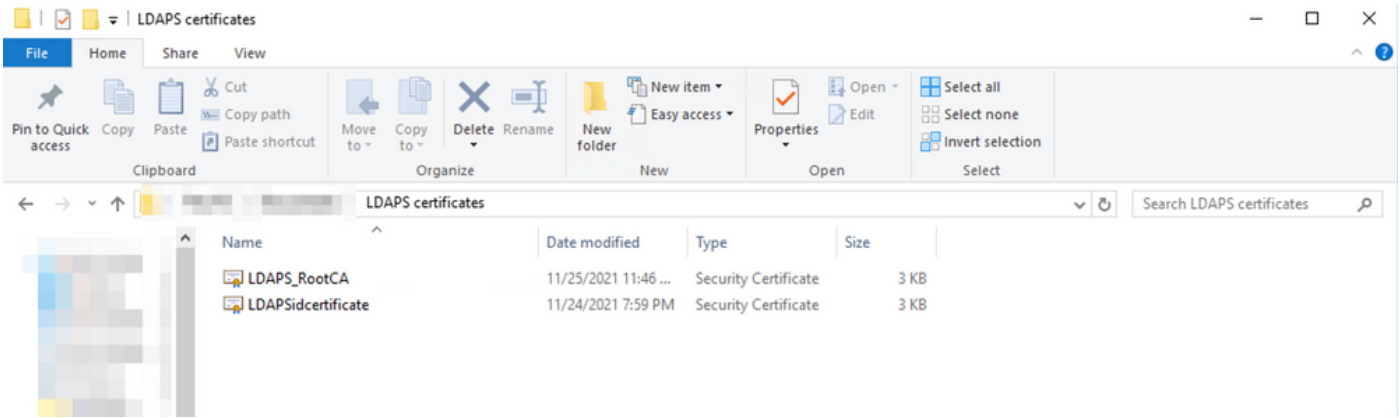
15. Revenez au certificat utilisé pour LDAPS, puis sélectionnez l'onglet **Chemin d'accès de certification**.

16. Sélectionnez l'émetteur de l'autorité de certification racine en haut du chemin de certification et cliquez sur **Afficher le certificat**.

17. Répétez les étapes 10 à 14 pour exporter le certificat de l'autorité de certification racine qui a signé le certificat utilisé pour l'authentification LDAPS.

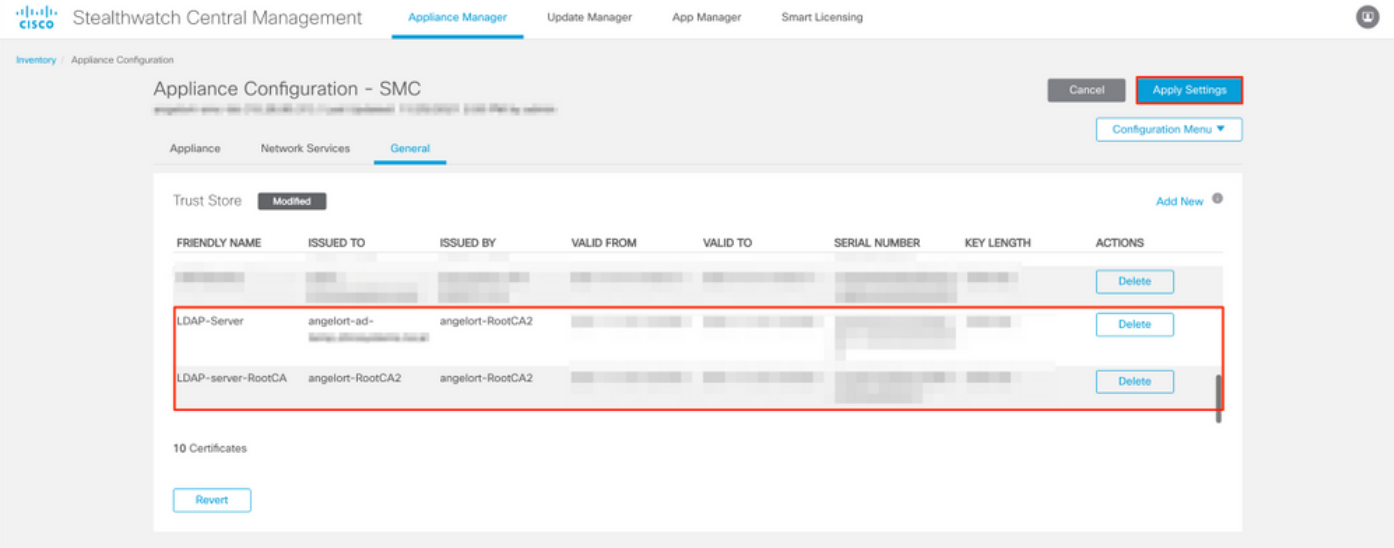
> **Note**: Votre déploiement peut avoir une hiérarchie CA multiniveau, auquel cas vous devez suivre la même procédure pour exporter tous les certificats intermédiaires dans la chaîne d'approbation.

18. Avant de continuer, assurez-vous d'avoir un fichier de certificat pour le serveur LDAPS et pour chaque autorité émettrice dans le chemin de certification : Certificat racine et certificats intermédiaires (le cas échéant).



Étape B. Connectez-vous au gestionnaire SNA pour ajouter le certificat du serveur LDAP et la chaîne racine.

1. Accédez à **Central Management** > Inventory.
2. Recherchez l'appliance SNA Manager et cliquez sur **Actions** > **Modifier la configuration de l'appliance**.
3. Dans la fenêtre Configuration de l'appareil, accédez au **menu Configuration** > **Magasin de confiance** > **Ajouter nouveau**.
4. Tapez le nom convivial, cliquez sur **Choisir un fichier** et sélectionnez le certificat du serveur LDAP, puis cliquez sur **Ajouter un certificat**.
5. Répétez l'étape précédente pour ajouter le certificat d'autorité de certification racine et les certificats intermédiaires (le cas échéant).
6. Vérifiez que les certificats chargés sont corrects et cliquez sur **Appliquer les paramètres**.

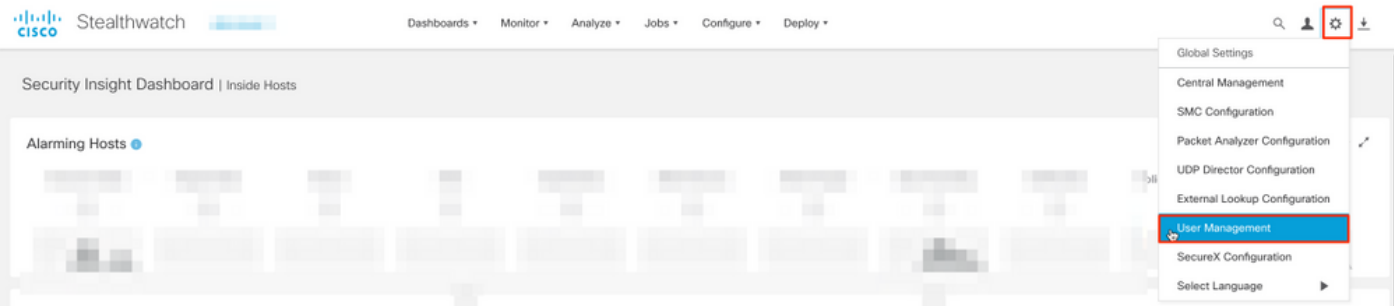


7. Attendez que les modifications soient appliquées et que le statut du manager soit **Actif**.

Étape C. Ajout de la configuration du service externe LDAP

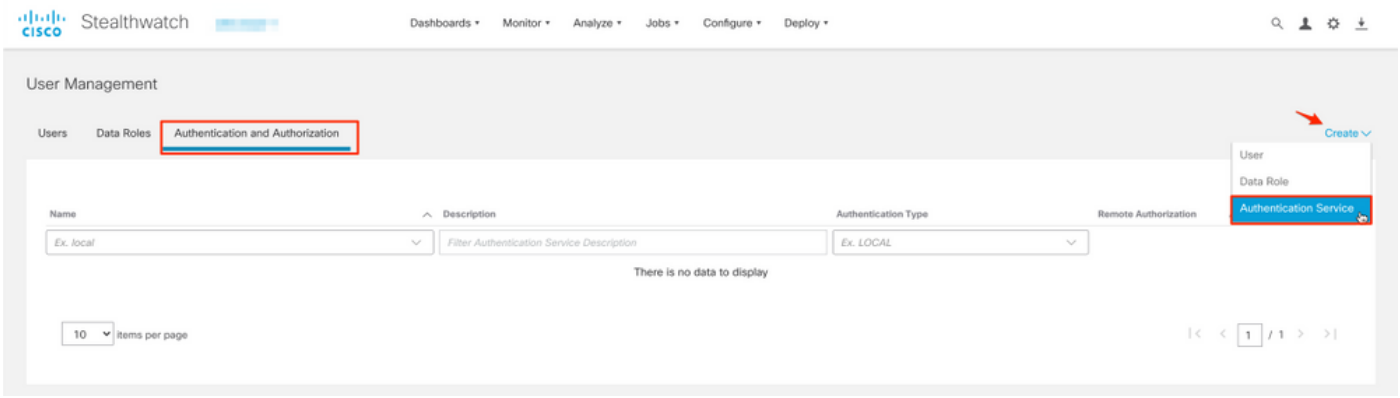
SNA version 7.2 ou ultérieure

1. Ouvrez le tableau de bord principal du manager et accédez à **Global Settings** > **User Management**.



2. Dans la fenêtre Gestion des utilisateurs, sélectionnez l'onglet **Authentification et autorisation**.

3. Cliquez sur **Create** > **Authentication Service**.



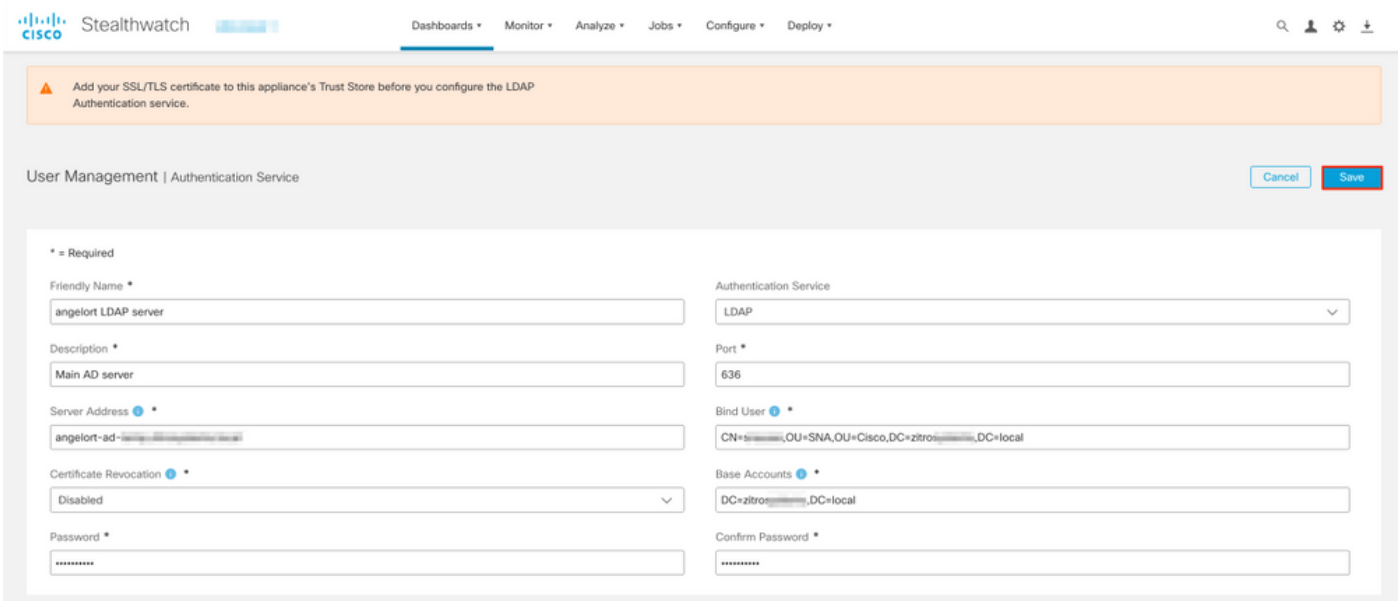
4. Dans le menu déroulant **Authentication Service**, sélectionnez **LDAP**.

5. Renseignez les champs obligatoires.

Champ	Notes
Nom convivial	Entrez un nom pour le serveur LDAP.
Description	Entrez une description pour le serveur LDAP.
Adresse du serveur	**Entrez le nom de domaine complet spécifié dans champ Subject Alternative Name (SAN) du certifi serveur LDAP.** • Si le champ SAN contient uniquement l'adres IPv4, saisissez l'adresse IPv4 dans le champ Server Address. • Si le champ SAN contient le nom DNS, saisis le nom DNS dans le champ Server Address. • Si le champ SAN contient des valeurs DNS e IPv4, utilisez la première valeur indiquée.
Port	Entrez le port désigné pour la communication LDA sécurisée (LDAP sur TLS). Le port TCP bien conn pour LDAPS est 636.
Lier l'utilisateur	Saisissez l'ID utilisateur utilisé pour la connexion serveur LDAP. Exemple : CN=admin, OU=Utilisat de l'entreprise, DC=exemple, DC=com **Note**: Si vous avez ajouté vos utilisateurs à u conteneur AD intégré (par exemple, « Utilisa »), le nom unique de liaison de l'utilisateur d liaison doit avoir le nom canonique (CN) défi sur le dossier intégré (par exemple, CN=username, CN=Users, DC=domain, DC=com). Cependant, si vous avez ajouté v utilisateurs à un nouveau conteneur, le nom unique de liaison doit avoir l'unité d'organisa (OU) définie sur le nouveau nom de contene (par exemple, CN=username, OU=Corporate Users, DC=domain, DC=com). **Note**: Une méthode utile pour trouver le nom unique de liaison de l'utilisateur de liaison consiste à interroger Active Directory sur un

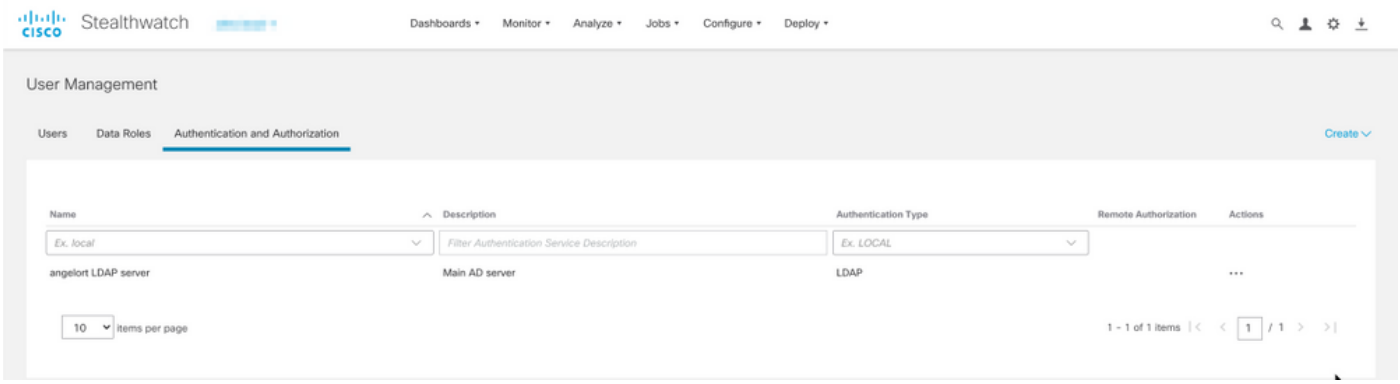
	serveur Windows qui dispose d'une connecti au serveur Active Directory. Pour obtenir ces informations, vous pouvez ouvrir une invite d commandes Windows et taper la commande **dsquery user dc=<distingué>, dc=<nom> -na <utilisateur>**. Par exemple : **dsquery user dc=exemple, dc=com -name user1**. Le résul ressemble à « CN=user1,OU=Corporate Users,DC=example,DC=com »
Mot de passe	Saisissez le mot de passe utilisateur de liaison ut pour la connexion au serveur LDAP.
Comptes de base	Saisissez le nom distinctif (DN). Le DN s'applique à la branche du répertoire dans laquelle les recherches d'utilisateurs doivent commencer. Il s'agit souvent de la partie supérieu l'arborescence des répertoires (votre domaine), m vous pouvez également spécifier une sous-arborescence dans le répertoire. L'utilisateur de li et les utilisateurs destinés à être authentifiés doiv être accessibles à partir des comptes de base. Exemple : DC=exemple, DC=com

6. Click **Save**.



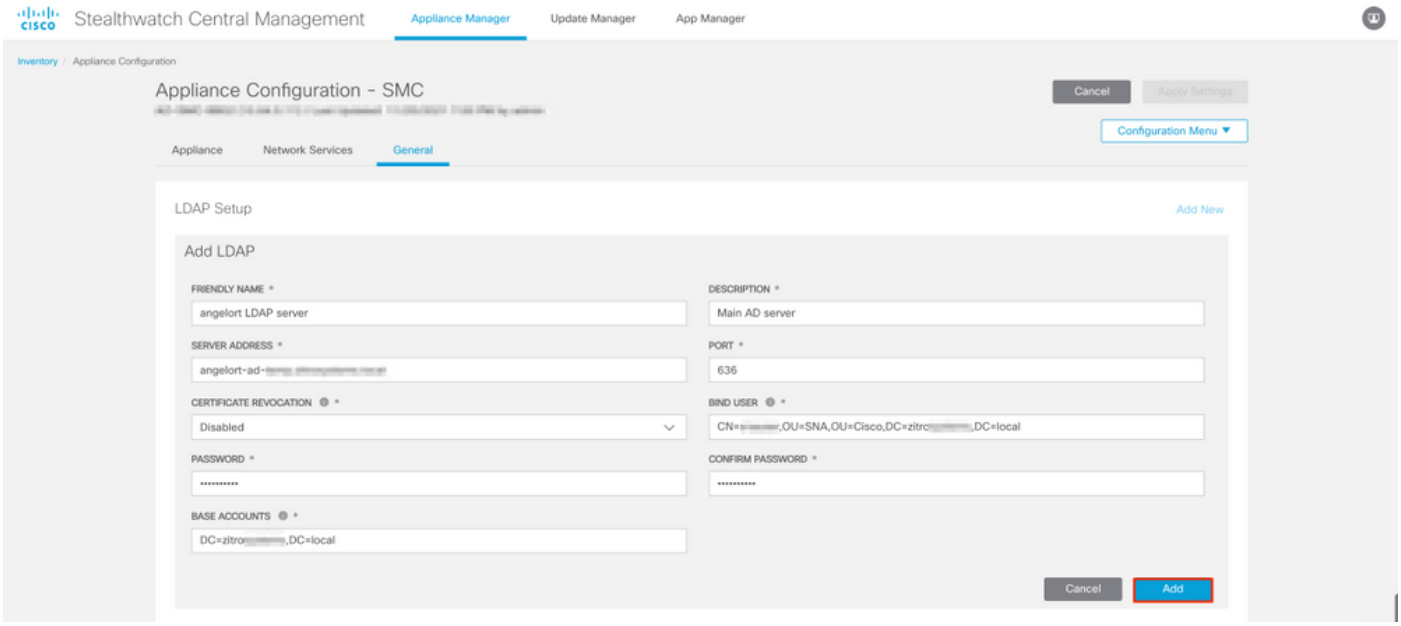
7. Si les paramètres saisis et les certificats ajoutés au magasin d'approbation sont corrects, vous devez obtenir une bannière « Vous avez enregistré vos modifications ».

8. Le serveur configuré doit être affiché sous **User Management > Authentication and Authorization**.



SNA version 7.1

1. Accédez à **Central Management** > Inventory.
2. Recherchez l'appliance SMC et cliquez sur **Actions** > **Modifier la configuration de l'appliance**.
3. Dans la fenêtre Configuration de l'appareil, accédez au **menu Configuration** > **Configuration LDAP** > **Ajouter nouveau**.
4. Renseignez les champs requis comme décrit dans **SNA version 7.2 ou version ultérieure** étape 5.



5. Cliquez sur **Add**.

6. Cliquez sur **Appliquer les paramètres**.

7. Une fois les paramètres saisis et les certificats ajoutés au magasin d'approbation corrects, les modifications du gestionnaire sont appliquées et l'état de l'appliance doit être **Actif**.

Étape D. Configurez les paramètres d'autorisation.

SNA prend en charge l'autorisation locale et distante via LDAP. Avec cette configuration, les groupes LDAP du serveur AD sont mappés à des rôles SNA intégrés ou personnalisés.

Les méthodes d'authentification et d'autorisation prises en charge pour SNA via LDAP sont les suivantes :

- Authentification à distance et autorisation locale
- Authentification à distance et autorisation à distance (prise en charge uniquement pour SNA version 7.2.1 ou ultérieure)

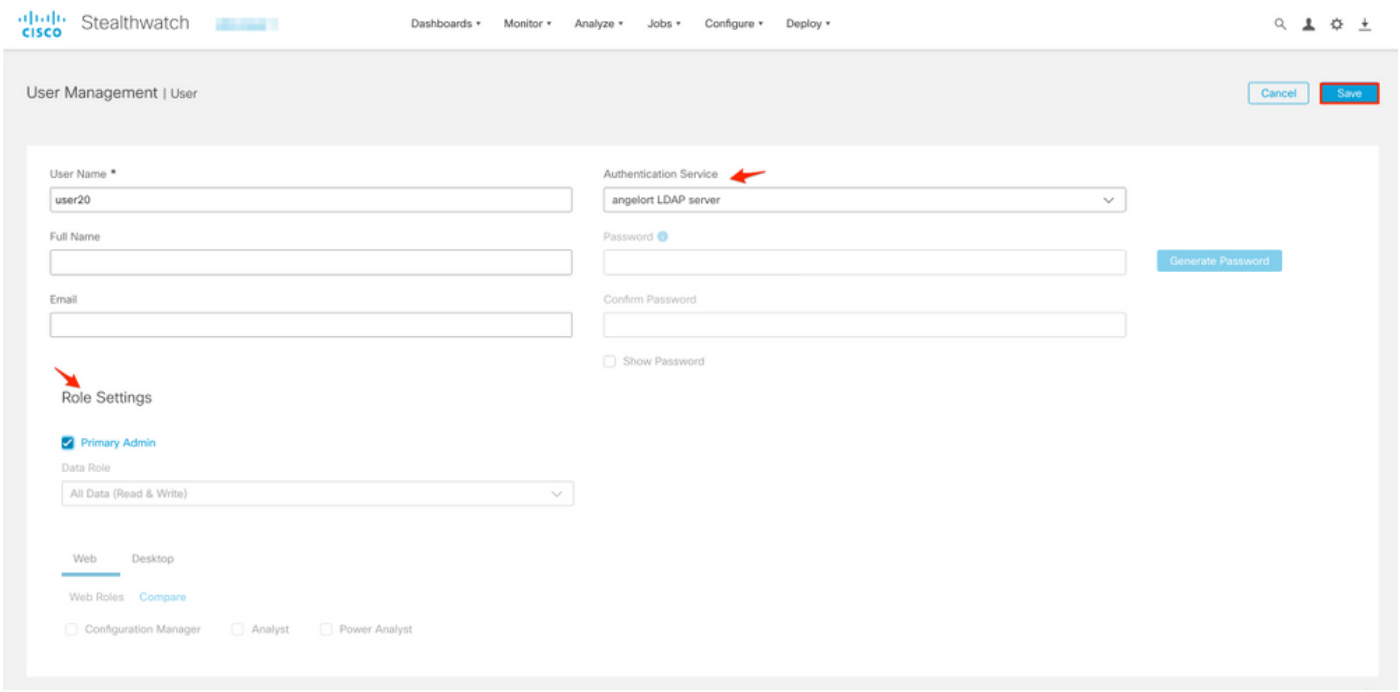
Autorisation locale

Dans ce cas, les utilisateurs et leurs rôles doivent être définis localement. Pour y parvenir, procédez comme suit.

1. Accédez à **Gestion des utilisateurs** à nouveau, cliquez sur l'onglet **Utilisateurs** > **Créer** > **Utilisateur**.

2. Définissez le nom d'utilisateur à authentifier auprès du serveur LDAP et sélectionnez le serveur configuré dans le menu déroulant **Authentication Service**.

3. Définissez les autorisations que l'utilisateur doit avoir sur le gestionnaire une fois authentifié par le serveur LDAP et cliquez sur **Enregistrer**.



Autorisation distante via LDAP

L'authentification et l'autorisation à distance via LDAP ont été prises en charge pour la première fois dans Secure Network Analytics version 7.2.1.

> **Note**: L'autorisation distante avec LDAP n'est pas prise en charge dans la version 7.1.

Il est important de mentionner que si un utilisateur est défini et activé localement (dans le gestionnaire), l'utilisateur est authentifié à distance, mais autorisé localement. Le processus de sélection des utilisateurs est le suivant :

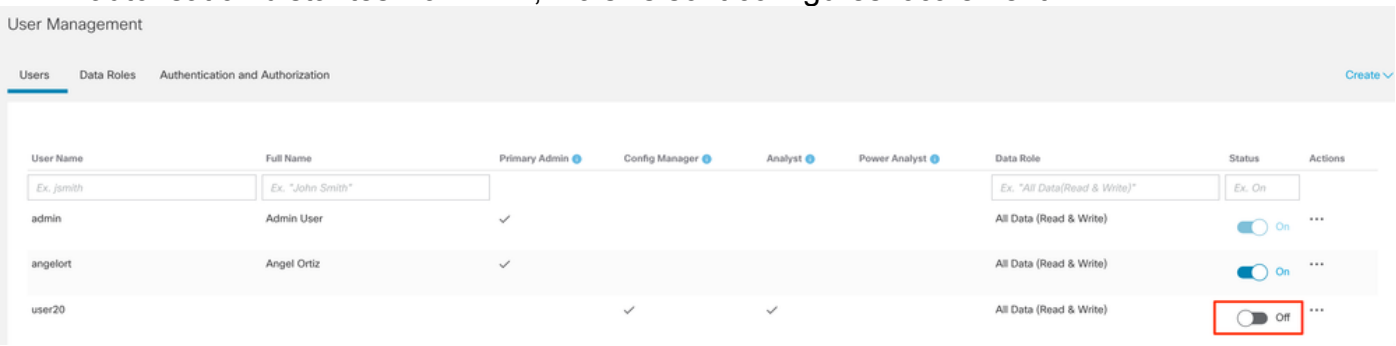
1. Une fois les informations d'identification entrées sur la page d'accueil du manager, le manager recherche un utilisateur local portant le nom spécifié.

2. Si un utilisateur local est trouvé et qu'il est activé, il est authentifié à distance (si l'authentification à distance via LDAP avec autorisation locale a été précédemment configurée) mais autorisé avec les paramètres locaux.
3. Si l'autorisation à distance est configurée et activée et que l'utilisateur est introuvable localement (non configuré ou désactivé), l'authentification et l'autorisation sont toutes deux effectuées à distance.

Pour cette raison, les étapes permettant de configurer correctement l'authentification distante sont les suivantes :

Étape D-1. Désactivez ou supprimez les utilisateurs destinés à utiliser l'autorisation à distance mais qui sont définis localement.

1. Ouvrez le tableau de bord principal du gestionnaire et accédez à Paramètres globaux > Gestion des utilisateurs.
2. Désactivez ou supprimez les utilisateurs (s'ils existent) destinés à utiliser l'authentification et l'autorisation distantes via LDAP, mais ils sont configurés localement.



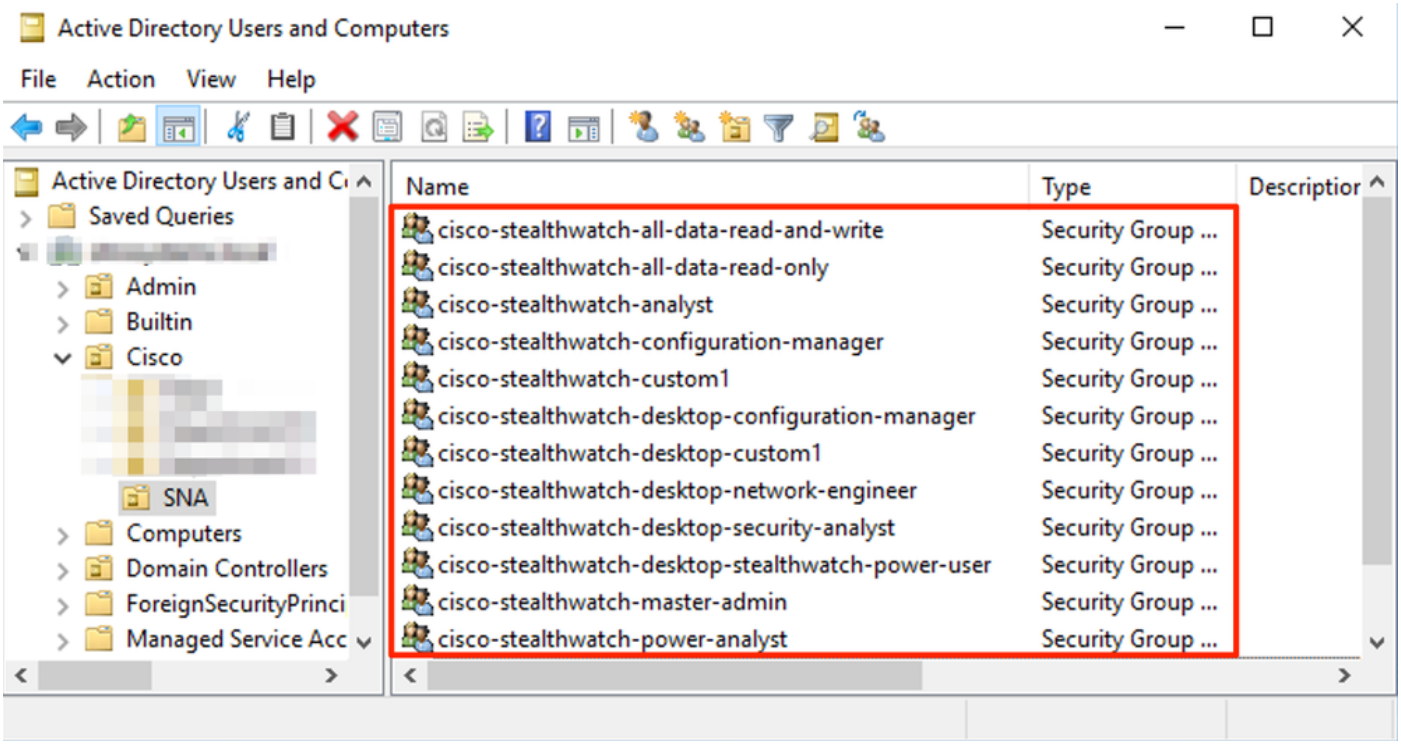
Étape D-2. Définissez les groupes cisco-stealthwatch dans le serveur Microsoft AD.

Pour l'authentification et l'autorisation externes via les utilisateurs LDAP, les mots de passe et les groupes *cisco-stealthwatch* sont définis à distance dans Microsoft Active Directory. Les groupes *cisco-stealthwatch* à définir dans le serveur AD sont liés aux différents rôles de SNA, ils doivent être définis comme suit.

Rôle SNA	Nom du ou des groupes
Administrateur principal	• cisco-stealthwatch-master-admin • cisco-stealthwatch-all-data-read-and-write • cisco-stealthwatch-all-data-read-only • cisco-stealthwatch-<custom> (facultatif)
Rôle des données	**Note**: Assurez-vous que les groupes de rôles données personnalisés commencent par “ ci stealthwatch-“.
Rôle fonctionnel Web	• Cisco-Stealthwatch-Configuration-Manager • Cisco-stealthwatch-power-analyst • analyste cisco-stealthwatch • cisco-stealthwatch-desktop-stealthwatch-pow user
Rôle fonctionnel du bureau	• Cisco-Stealthwatch-desktop-configuration-manager • cisco-stealthwatch-desktop-network-ingénieu

- Cisco-Stealthwatch-desktop-security-analyst
- cisco-stealthwatch-desktop-<custom> (faculta

Note: Assurez-vous que les groupes de rôles fonctionnels personnalisés commencent par cisco-stealthwatch-desktop-“.

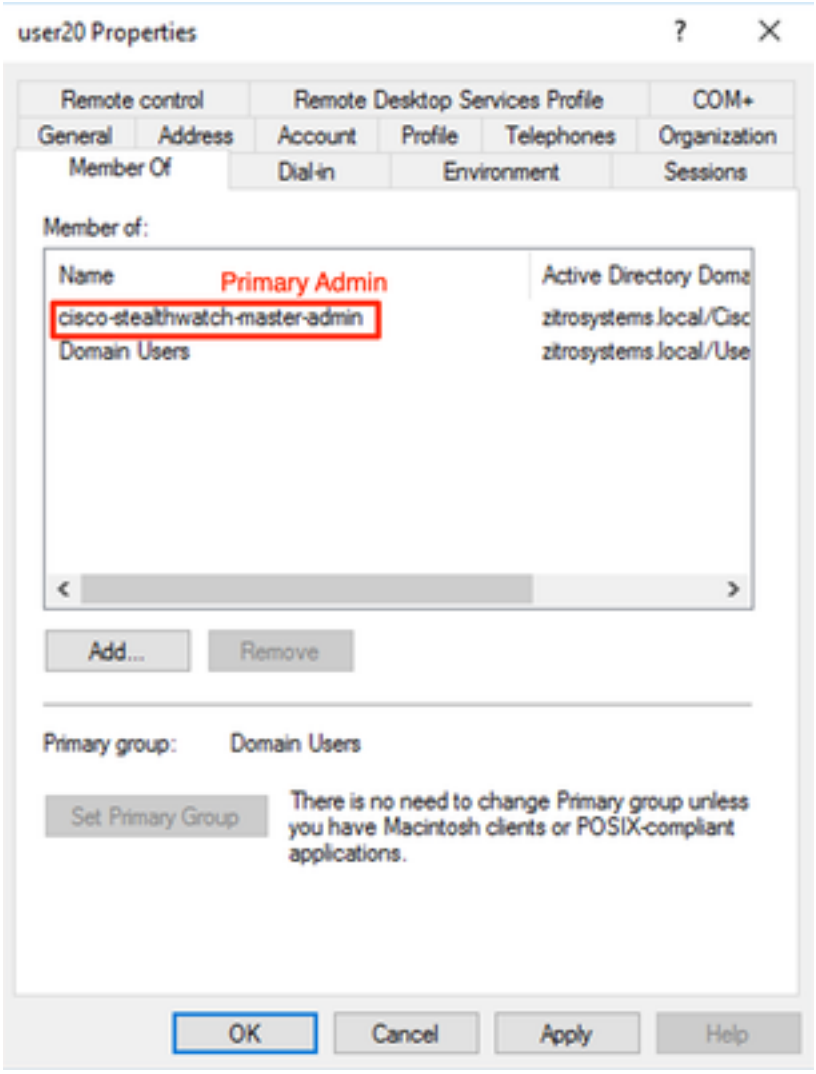


Note: Comme décrit précédemment, les groupes personnalisés sont pris en charge pour “ rôle de données ” et “ rôle fonctionnel de bureau ” tant que le nom du groupe est précédé de la chaîne appropriée. Ces rôles et groupes personnalisés doivent être définis dans le gestionnaire SNA et le serveur Active Directory. Par exemple, si vous définissez un rôle personnalisé “ un ” personnalisé1 dans le SNA Manager pour un rôle client de bureau, il doit être mappé à cisco-stealthwatch-desktop-custom1 dans Active Directory.

Étape D-3. Définissez les mappages de groupe d'autorisations LDAP pour les utilisateurs.

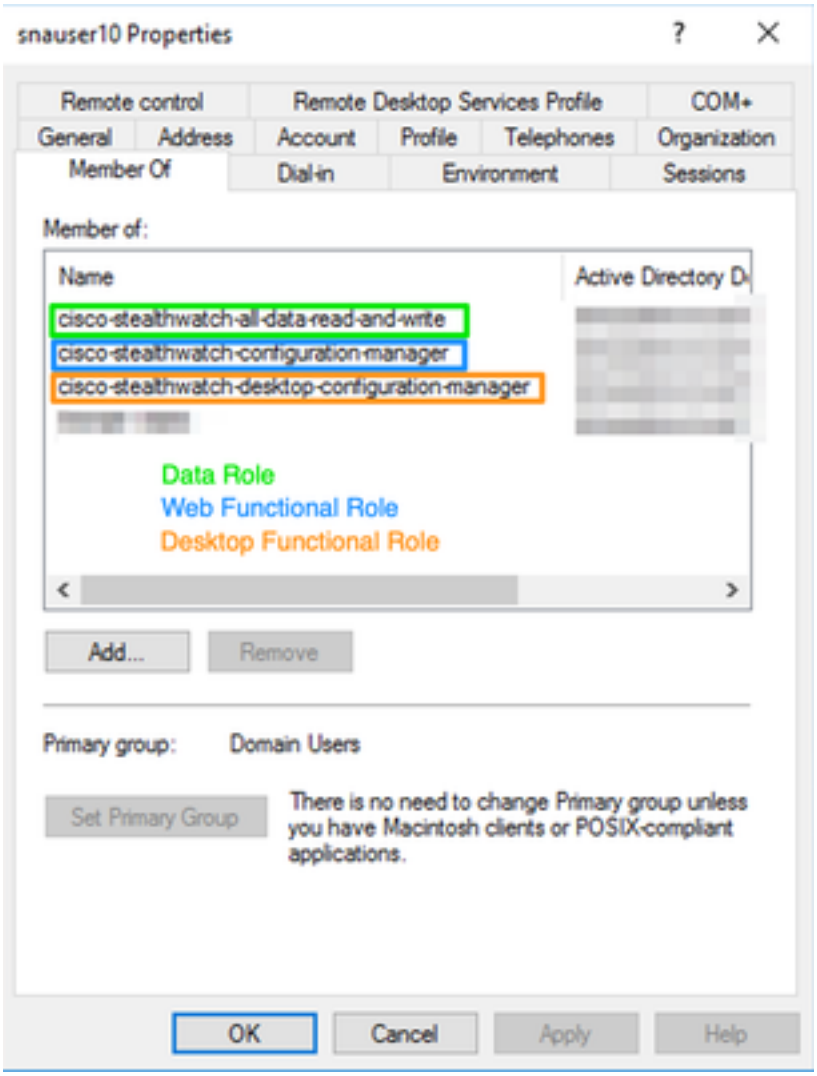
Une fois que les groupes *cisco-stealthwatch* ont été définis dans le serveur AD, nous pouvons mapper les utilisateurs destinés à avoir accès au SNA Manager aux groupes nécessaires. Cela doit se faire comme suit.

- Un utilisateur **Admin principal doit** être affecté au groupe *cisco-stealthwatch-master-admin* et **ne doit pas être membre d'autres** groupes *cisco-stealthwatch*.



- Chaque utilisateur, autre que les utilisateurs Admin principaux, doit être affecté à un groupe de chaque rôle avec les conditions suivantes.

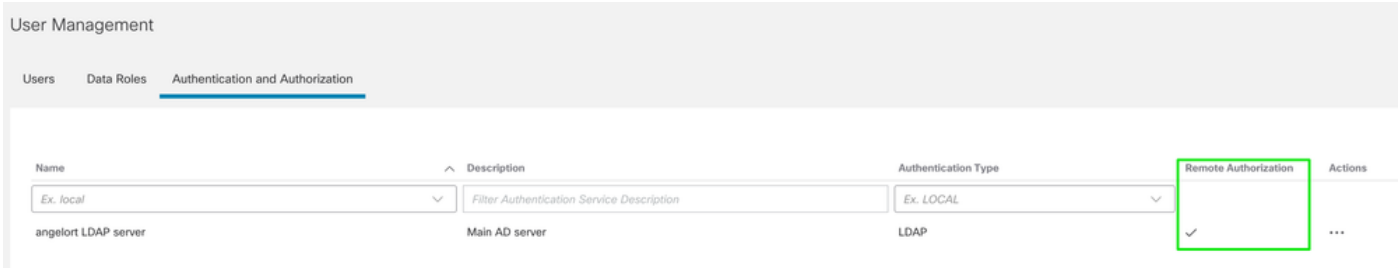
1. **Rôle de données** : L'utilisateur doit être affecté à **un seul groupe**.
2. **Rôle fonctionnel Web** : L'utilisateur doit être affecté à **au moins un groupe**.
3. **Rôle fonctionnel du bureau** : L'utilisateur doit être affecté à **au moins un groupe**.



Étape D-4. Activez l'autorisation à distance via LDAP sur le SNA Manager.

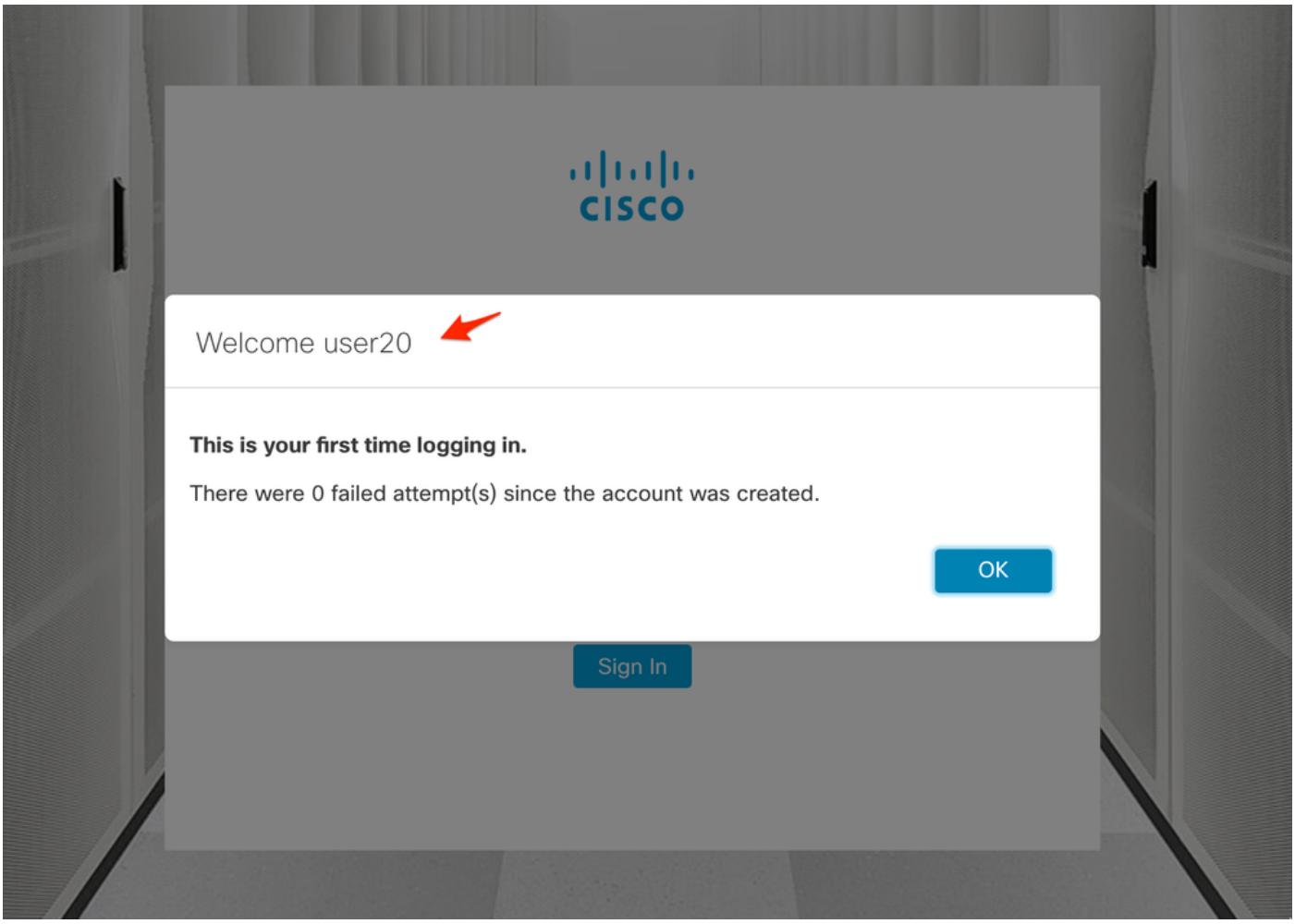
1. Ouvrez le tableau de bord principal du manager et accédez à **Global Settings > User Management**.
2. Dans la fenêtre **Gestion des utilisateurs**, sélectionnez l'onglet **Authentification et autorisation**.
3. Recherchez le service d'authentification LDAP configuré à l'**étape C**.
4. Cliquez sur **Actions > Activer l'autorisation distante**.

Note: **Un seul service d'autorisation externe peut être utilisé à la fois.** Si un autre service d'autorisation est déjà utilisé, il est automatiquement désactivé et le nouveau est activé. Toutefois, tous les utilisateurs autorisés avec le service externe précédent sont déconnectés. Un message de confirmation s'affiche avant toute action.

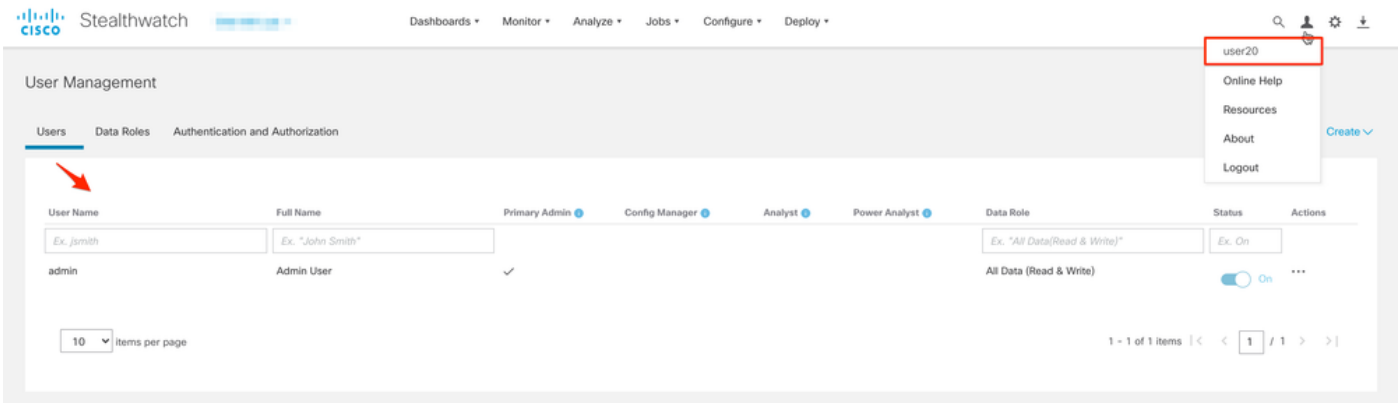


Vérification

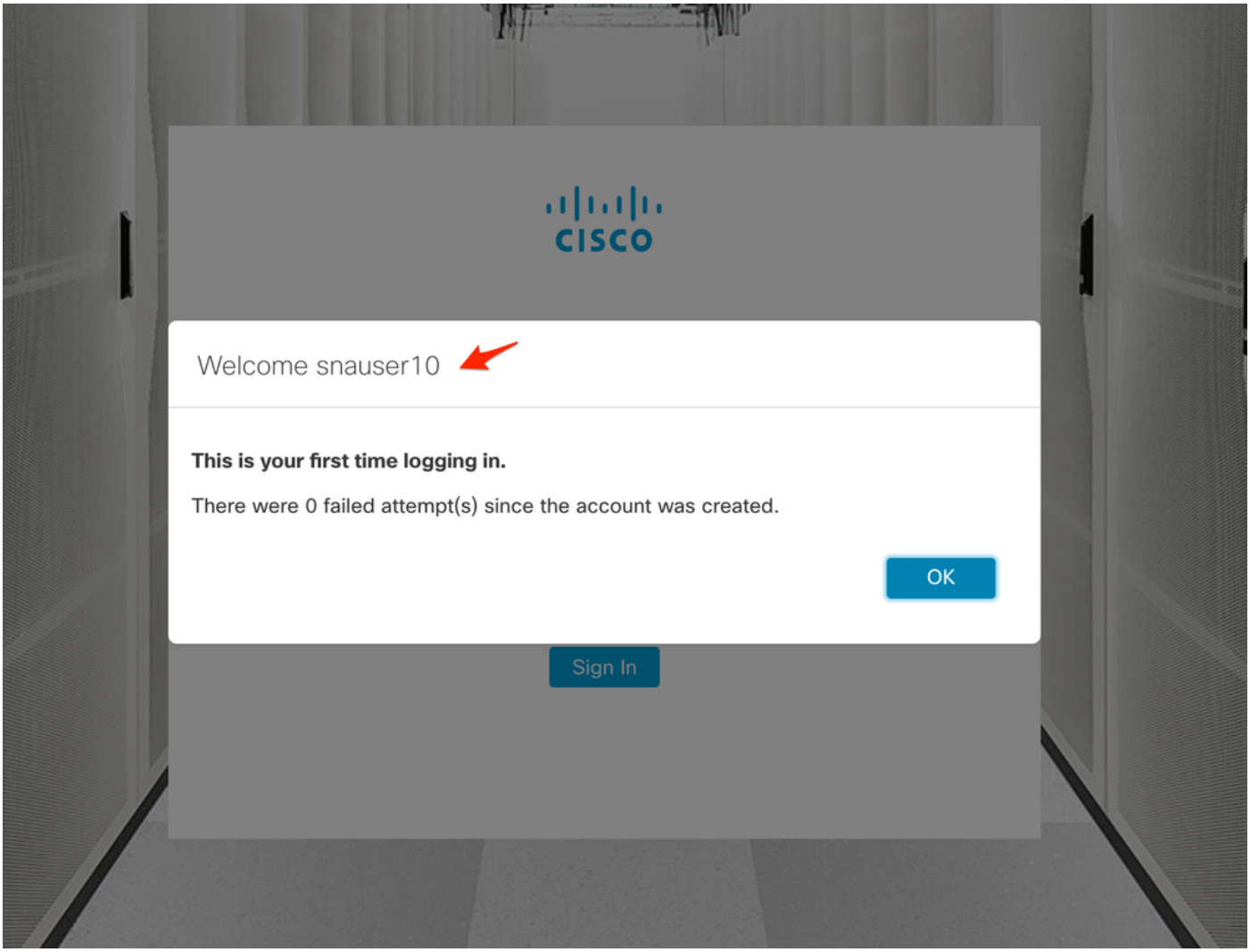
Les utilisateurs peuvent se connecter avec les informations d'identification définies sur le serveur AD.



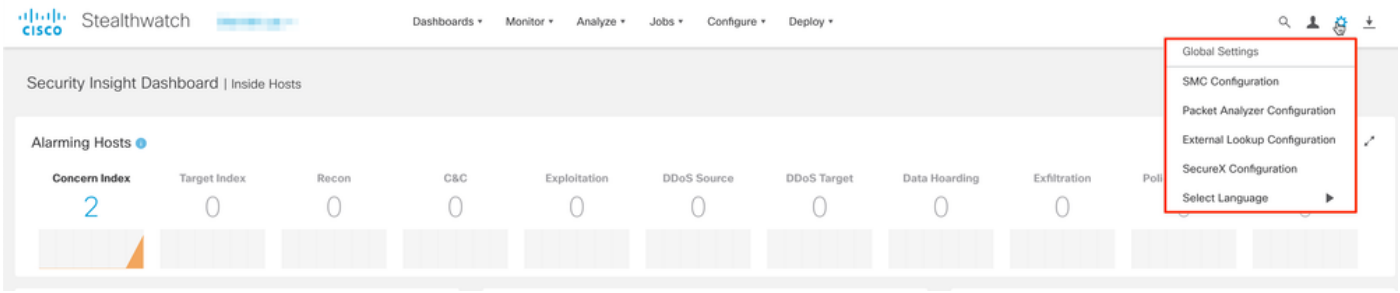
La deuxième étape de vérification concerne l'autorisation. Dans cet exemple, l'utilisateur « user20 » a été fait membre du groupe *cisco-stealthwatch-master-admin* dans le serveur AD, et nous pouvons confirmer que l'utilisateur dispose des autorisations d'administrateur principal. L'utilisateur n'est pas défini dans les utilisateurs locaux, nous pouvons donc confirmer que les attributs d'autorisation ont été envoyés par le serveur AD.



La même vérification est effectuée pour l'autre utilisateur dans cet exemple « snauser10 ». Nous pouvons confirmer l'authentification réussie avec les informations d'identification configurées sur le serveur AD.



Pour la vérification de l'autorisation, comme cet utilisateur n'appartient pas au groupe d'administration principal, certaines fonctionnalités ne sont pas disponibles.



Dépannage

Si la configuration du service d'authentification ne peut pas être enregistrée, vérifiez que :

1. Vous avez ajouté les certificats appropriés du serveur LDAP au magasin d'approbation du gestionnaire.
2. L'**adresse du serveur** configuré est celle spécifiée dans le champ Subject Alternative Name (SAN) du certificat du serveur LDAP. Si le champ SAN contient uniquement l'adresse IPv4, saisissez l'adresse IPv4 dans le champ Server Address.Si le champ SAN contient le nom DNS, saisissez le nom DNS dans le champ Server Address.Si le champ SAN contient des valeurs DNS et IPv4, utilisez la première valeur indiquée.

3. Les champs **Bind User** et **Base Account** configurés sont corrects, comme spécifié par le contrôleur de domaine AD.

Informations connexes

Pour obtenir de l'aide supplémentaire, contactez le centre d'assistance technique Cisco (TAC). Un contrat d'assistance valide est requis : Coordonnées du service d’assistance Cisco à l’échelle mondiale.