Configuration de l'authentification et de l'autorisation externes via LDAPS pour l'accès SNA Manager

Table des matières

- Introduction
- Conditions préalables
  - Exigences
  - Composants utilisés
- Configurer
  - 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. Configuration des paramètres d'autorisation
    - Autorisation Locale
    - Autorisation à distance via LDAP
- Vérifier
- Dépannage
- Informations connexes

Introduction

Ce document décrit la configuration de base d'un Secure Network Analytics Manager avec le protocole LDAP (Lightweight Directory Access Protocol) sur SSL.

Conditions préalables

Exigences

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

Composants utilisés

Les informations contenues dans ce document sont basées sur les composants suivants :

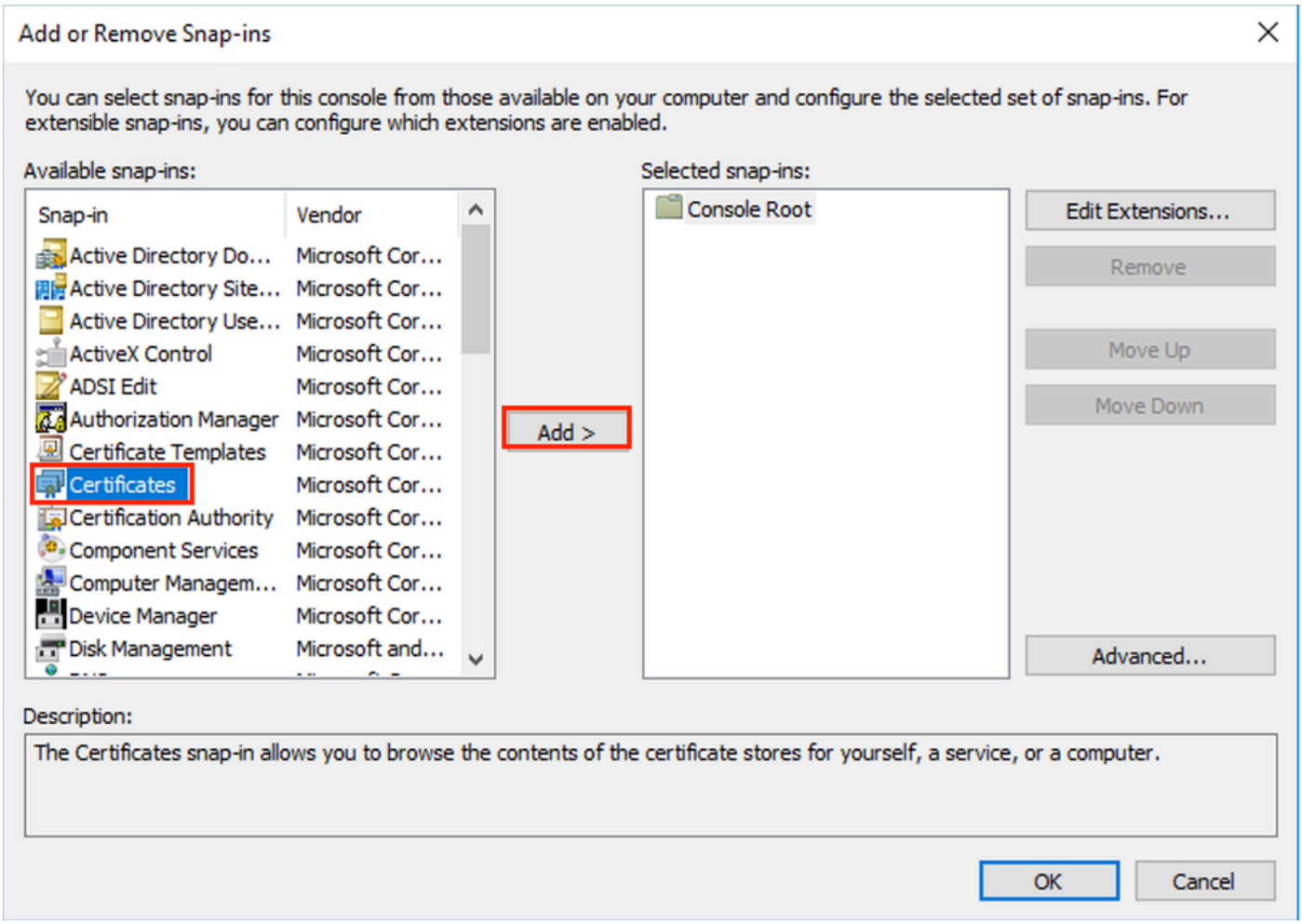
- Cisco Secure Network Analytics Manager (anciennement SMC) version 7.3.2
- Windows Server 2016 configuré comme contrôleur de domaine Active Directory

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.

Configurer

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 entrez 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.

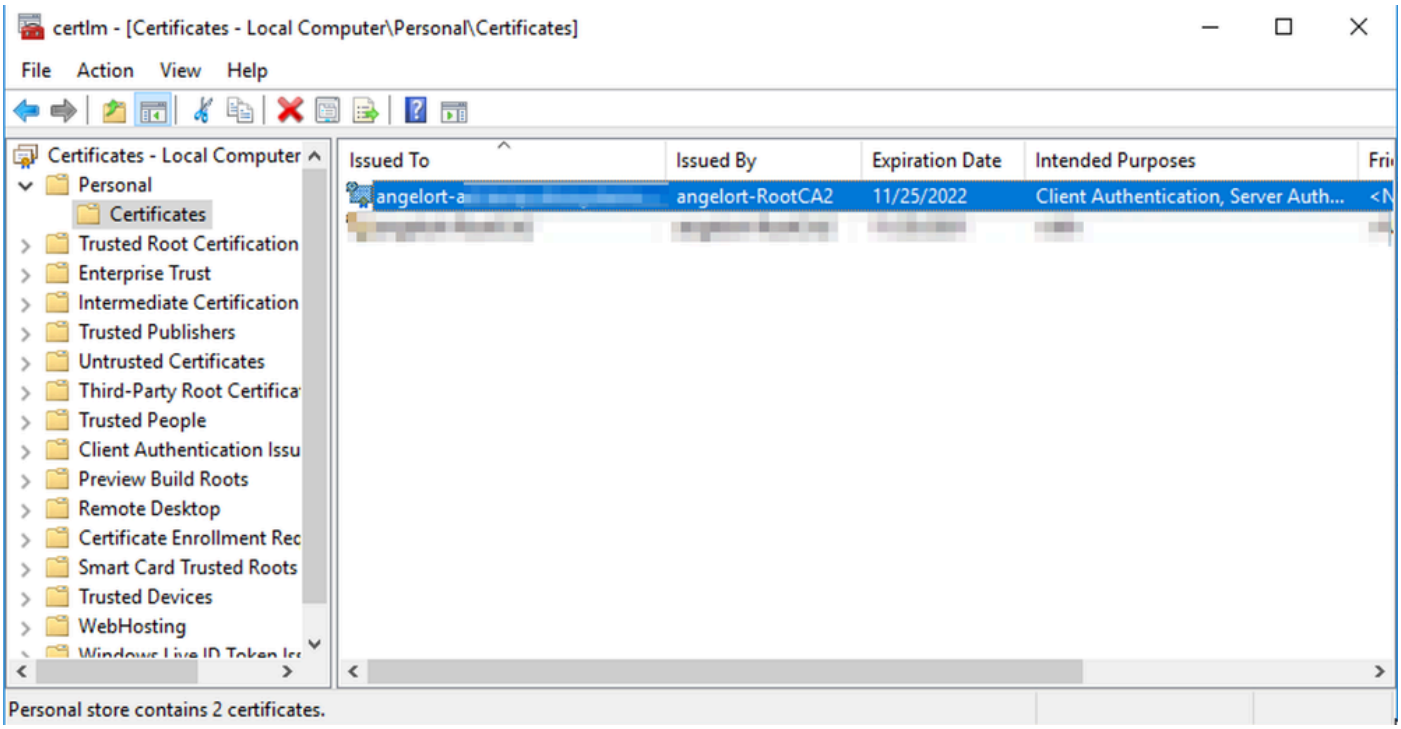


5. Dans la fenêtre du composant logiciel enfichable Certificats, sélectionnez Compte d'ordinateur, puis Suivant.

6. Laissez Ordinateur local sélectionné, puis sélectionnez Terminer.

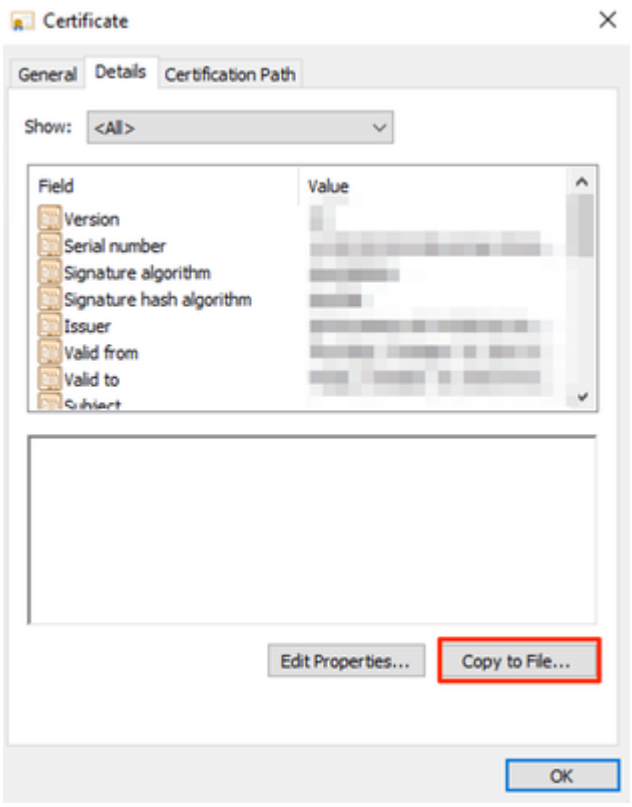
7. Dans la fenêtre Ajouter ou supprimer un composant logiciel enfichable, sélectionnez OK.

8. Accédez à Certificates (Local Computer) > Personal > Certificates



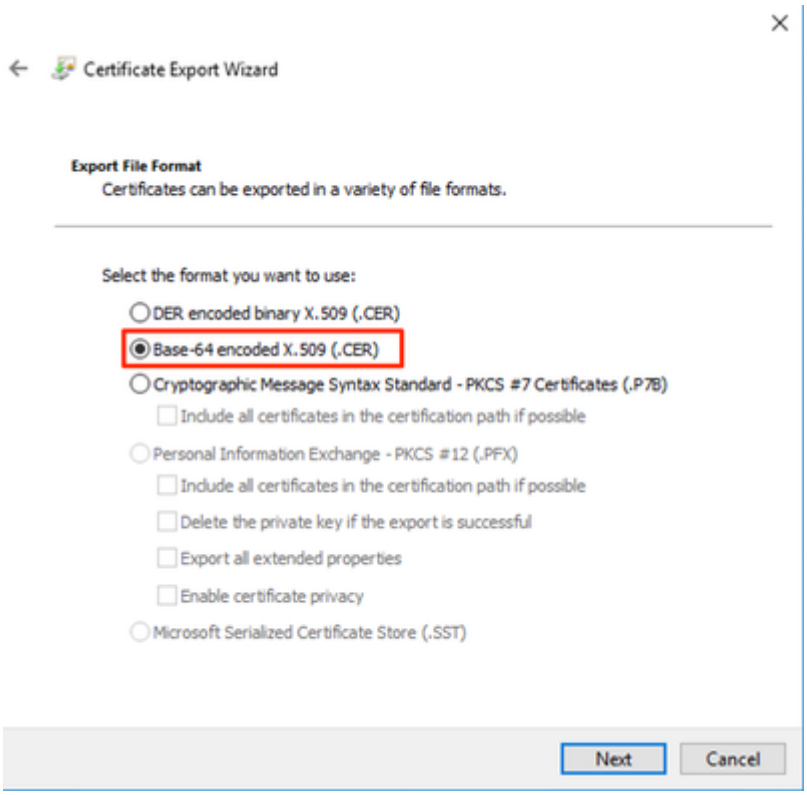
9. Sélectionnez et cliquez avec le bouton droit sur le certificat SSL utilisé pour l'authentification LDAPS sur votre contrôleur de domaine, puis cliquez sur Ouvrir.

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

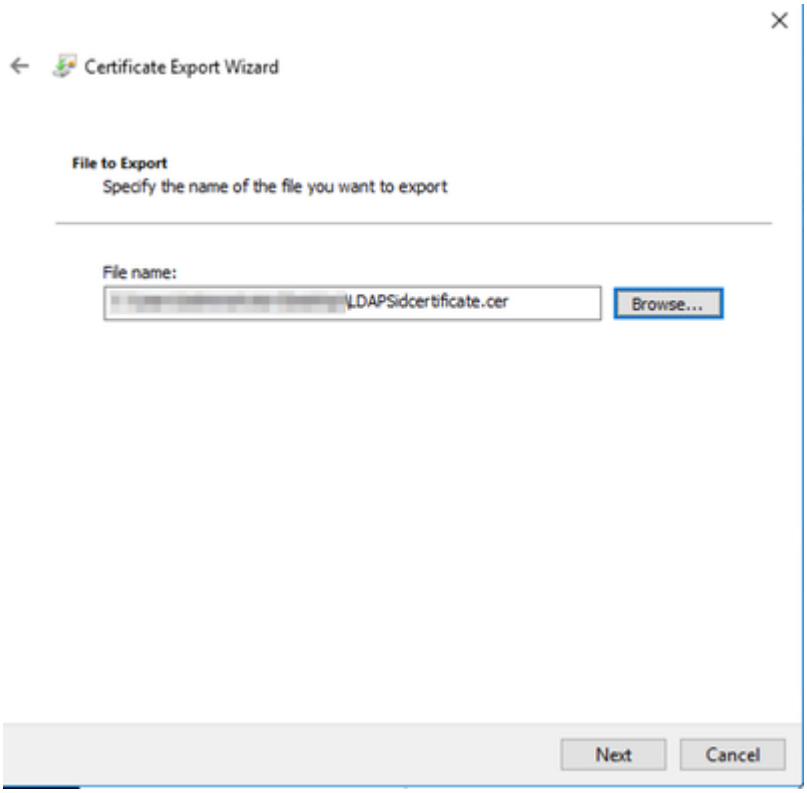


11. Assurez-vous que Non, ne pas exporter la clé privée est sélectionné et cliquez sur Suivant

12. Sélectionnez le format X.509 codé en base 64 et cliquez sur Next.



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



14. Cliquez sur Finish, vous devez obtenir un «L'exportation a réussi.» message.

15. Revenez au certificat utilisé pour LDAPS, puis sélectionnez l’onglet Chemin de certification.

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

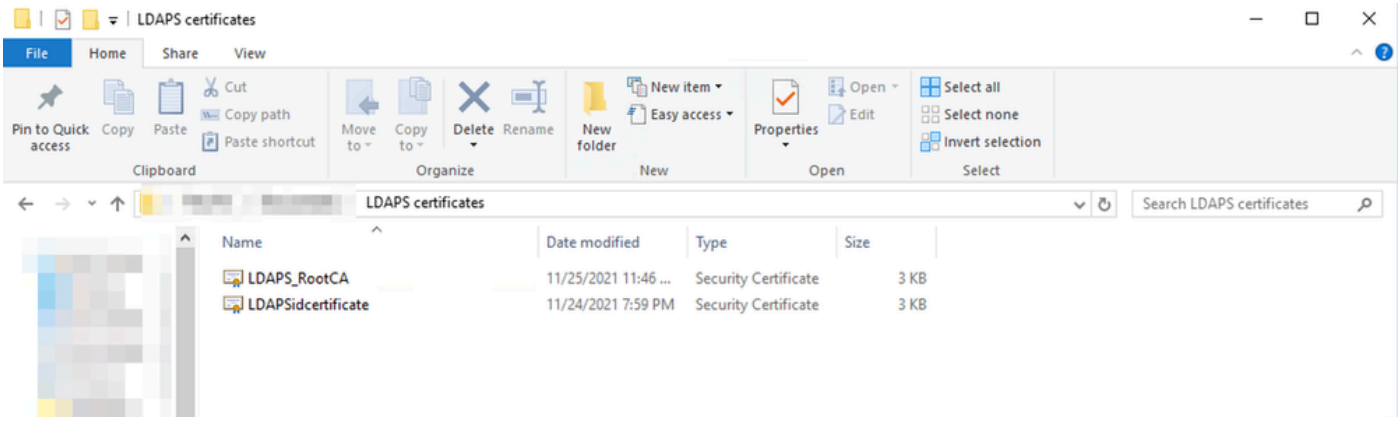


17. Répétez les étapes 10 à 14 pour exporter le certificat de l’autorité de certification racine qui a signé le certificat utilisé pour l’authentification LDAPS.

Remarque : Votre déploiement peut avoir une hiérarchie d'autorités de certification à plusieurs niveaux, auquel cas vous devez utiliser la même procédure pour exporter tous les certificats intermédiaires dans la chaîne d'approbation.

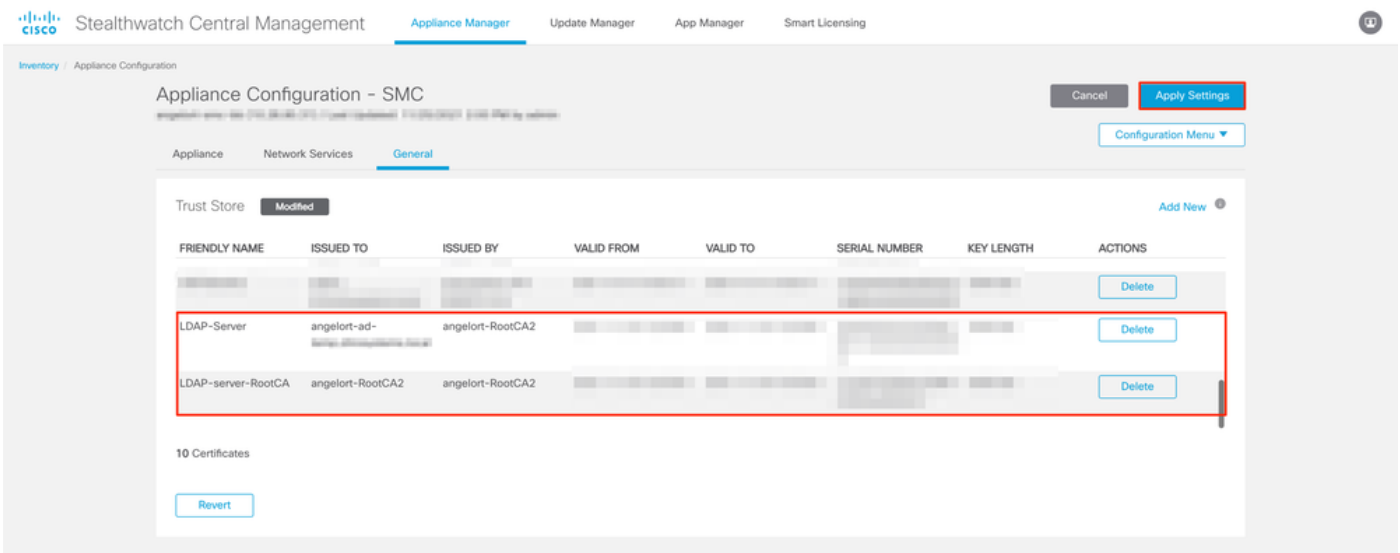
---

18. Avant de continuer, assurez-vous que vous disposez d’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. Localisez l'appliance SNA Manager et cliquez sur Actions > Edit Appliance Configuration.
3. Dans la fenêtre Appliance Configuration, accédez à Configuration Menu > Trust Store > Add New.
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 de l'autorité de certification racine et les certificats intermédiaires (le cas échéant).
6. Vérifiez que les certificats qui ont été téléchargés sont les bons et cliquez sur Apply Settings.

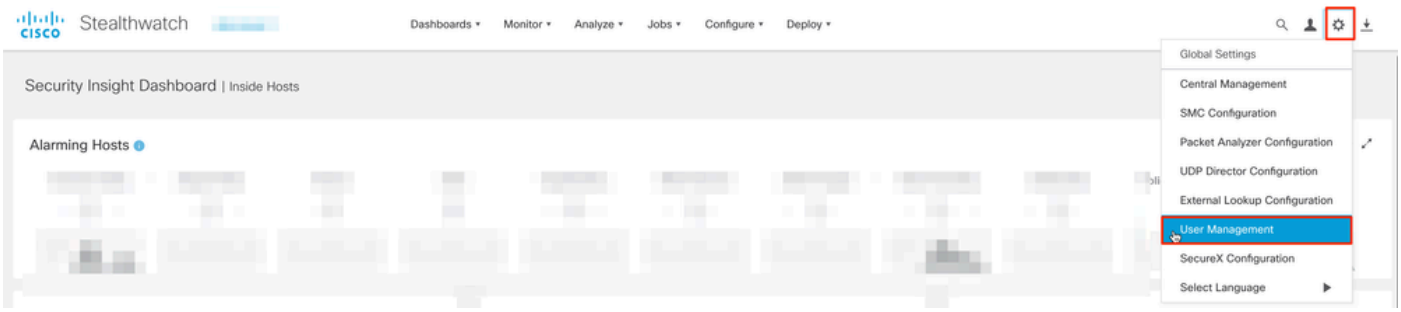


7. Attendez que les modifications soient appliquées et que l'état du manager soit Démarré.

Étape C. Ajout de la configuration du service externe LDAP

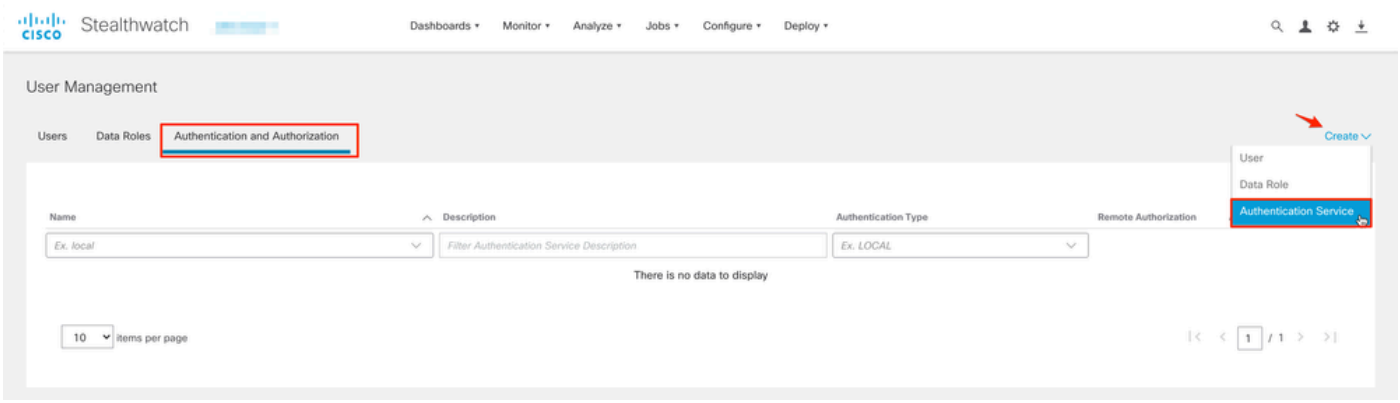
SNA version 7.2 ou ultérieure

1. Ouvrez le tableau de bord principal du gestionnaire et accédez à Paramètres généraux > Gestion des utilisateurs.



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.

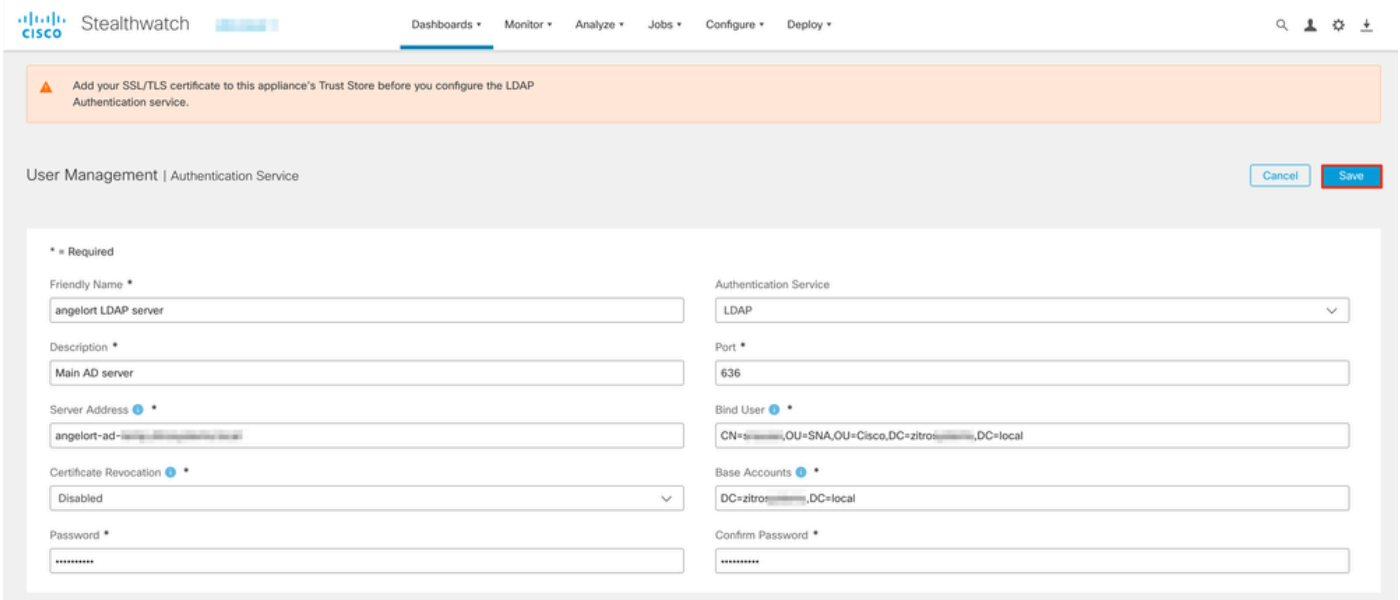
5. Renseignez les champs obligatoires.

Champ	Remarques
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 comme indiqué dans le champ Subject Alternative Name

	(SAN) du certificat du serveur LDAP. • Si le champ SAN ne contient que 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 à la fois des valeurs DNS et IPv4, utilisez la première valeur répertoriée.
Port	Saisissez le port désigné pour la communication LDAP sécurisée (LDAP sur TLS). Le port TCP le plus connu pour LDAPS est 636.
Lier un utilisateur	Saisissez l'ID utilisateur utilisé pour la connexion au serveur LDAP. Exemple : CN=admin,OU=Utilisateurs de l'entreprise,DC=exemple,DC=com Remarque : Si vous avez ajouté vos utilisateurs à un conteneur AD intégré (par exemple, « Utilisateurs »), le nom de domaine de liaison de l'utilisateur de liaison doit avoir le nom canonique (CN) défini sur le dossier intégré (par exemple, CN=username, CN=Users, DC=domain, DC=com). Toutefois, si vous avez ajouté vos utilisateurs à un nouveau conteneur, l'unité d'organisation (OU) du DN de liaison doit être définie sur le nouveau nom de conteneur (par exemple, CN=username, OU=Corporate Users, DC=domain, DC=com). Remarque : Pour trouver le DN de liaison de l'utilisateur de liaison, il est utile d'interroger Active Directory sur un serveur Windows Server connecté au serveur Active Directory. Pour obtenir ces informations, vous pouvez ouvrir une invite

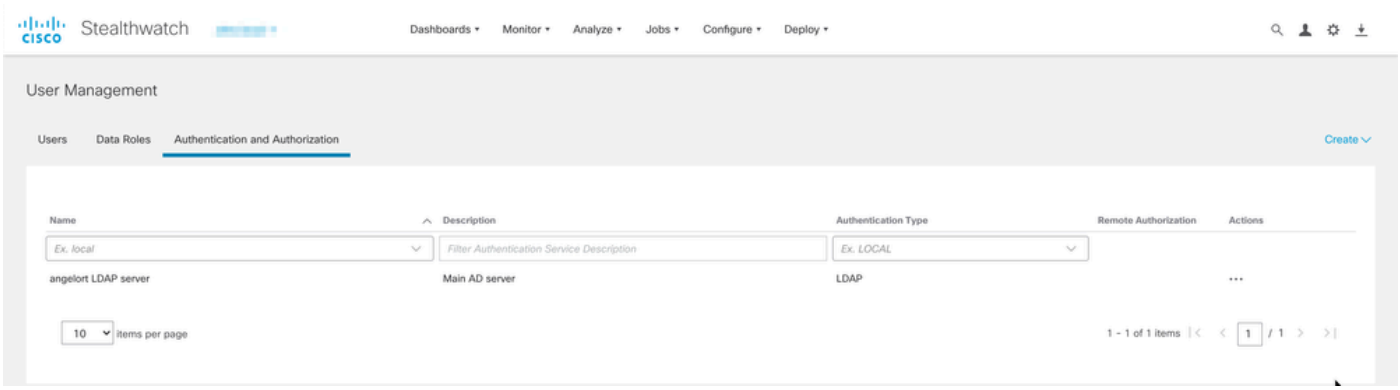
	de commandes Windows et taper la commande dsquery user dc=<distingué>,dc=<nom> -name <utilisateur>. Par exemple : dsquery user dc=example,dc=com -name user1. Le résultat ressemble à "CN=user1,OU=Corporate Users,DC=example,DC=com"
Mot de passe	Saisissez le mot de passe de liaison d'utilisateur utilisé pour la connexion au serveur LDAP.
Comptes de base	Saisissez le nom distinctif (DN). Le nom distinctif (DN) s'applique à la branche du répertoire dans laquelle les recherches d'utilisateurs doivent commencer. Il s'agit souvent de la partie supérieure de l'arborescence de répertoires (votre domaine), mais vous pouvez également spécifier une sous-arborescence dans le répertoire. L'utilisateur de liaison et les utilisateurs devant être authentifiés doivent être accessibles à partir des comptes de base. Exemple : DC=exemple,DC=com

6. Cliquez sur Enregistrer.



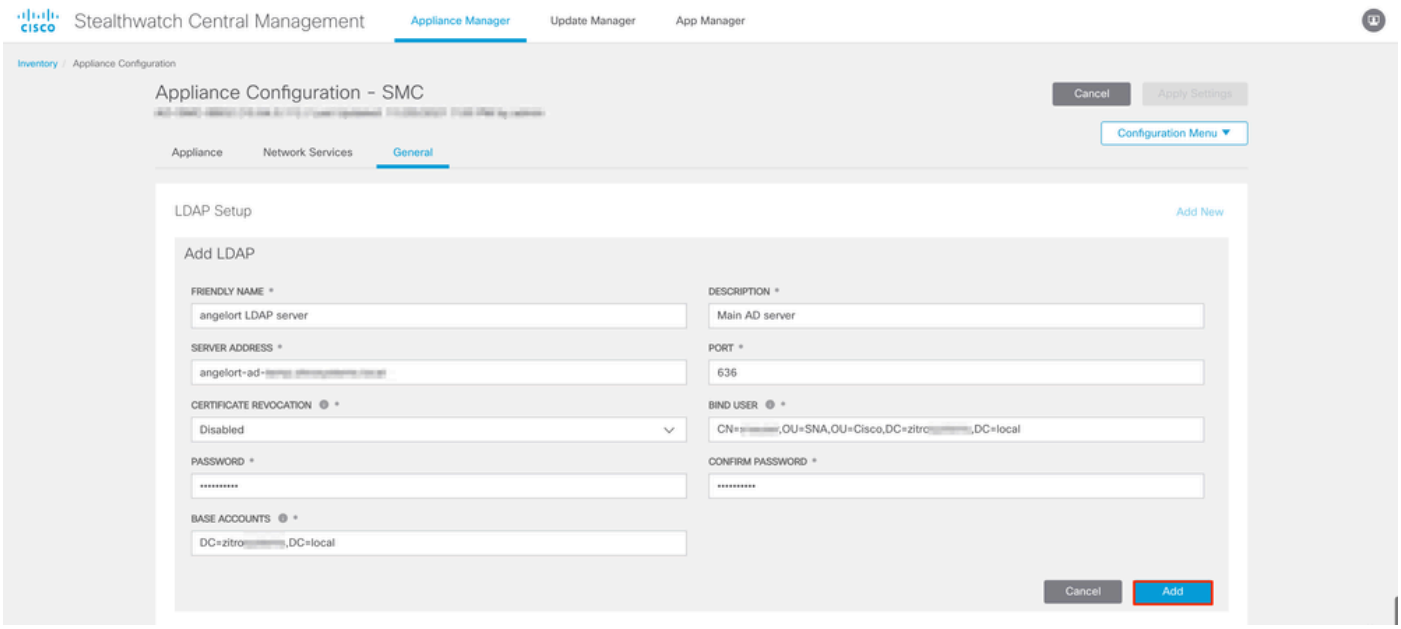
7. Si les paramètres entrés et les certificats ajoutés au magasin d'approbation sont corrects, vous recevez une You've successfully saved your changes bannière.

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



SNA version 7.1

1. Accédez à Central Management > Inventory.
2. Localisez l'appliance SMC et cliquez sur Actions > Edit Appliance Configuration.
3. Dans la fenêtre Appliance Configuration, accédez à Configuration Menu > LDAP Setup > Add New.
4. Renseignez les champs obligatoires comme décrit dans SNA Version 7.2 ou ultérieure Étape 5.



5. Cliquez sur Ajouter.

6. Cliquez sur Apply Settings.

7. Une fois que les paramètres entrés et les certificats ajoutés au magasin d'approbation sont corrects, les modifications sur le Gestionnaire sont appliquées et l'état de l'appliance doit être Up.

Étape D. Configuration des 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 et autorisation à distance (prises en charge uniquement pour SNA version 7.2.1 ou ultérieure)

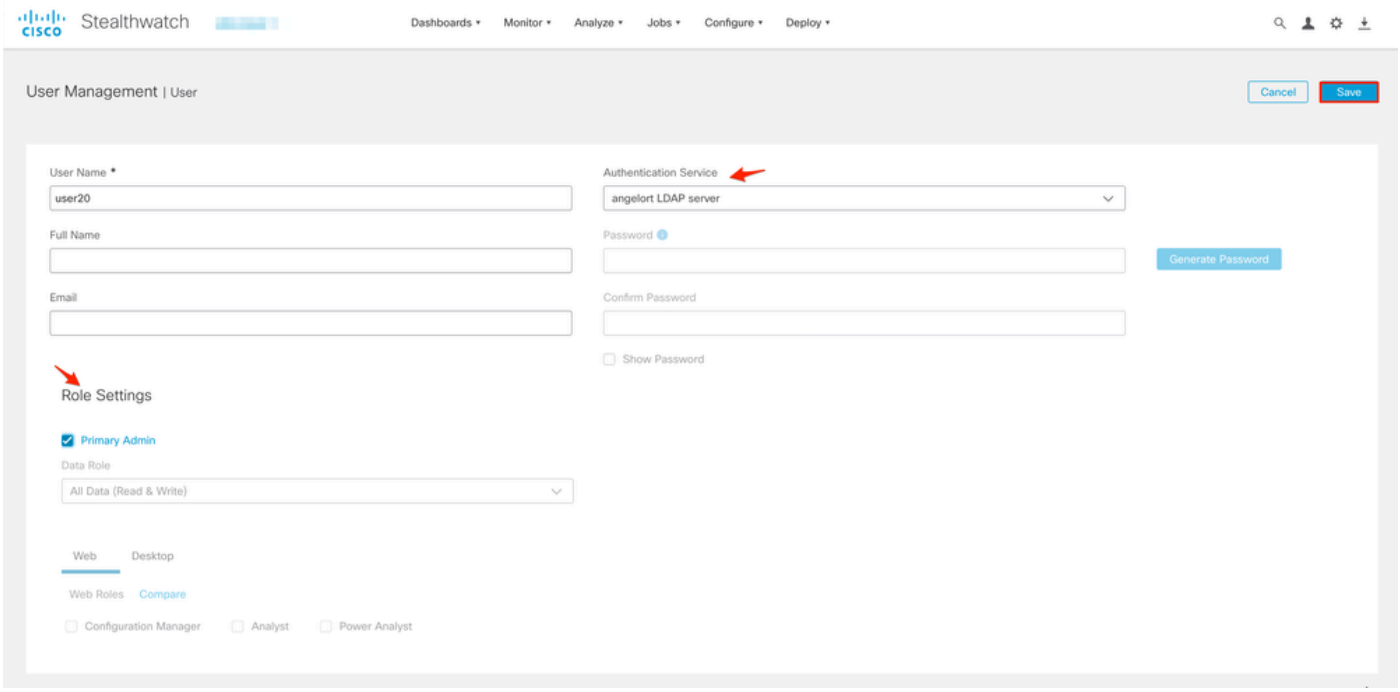
Autorisation Locale

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

1. Accédez à nouveau à Gestion des utilisateurs, 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 qu'il est authentifié par le serveur LDAP et cliquez sur Enregistrer.



Autorisation à distance via LDAP

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

Remarque : L'autorisation à distance avec LDAP n'est pas prise en charge dans la version 7.1.

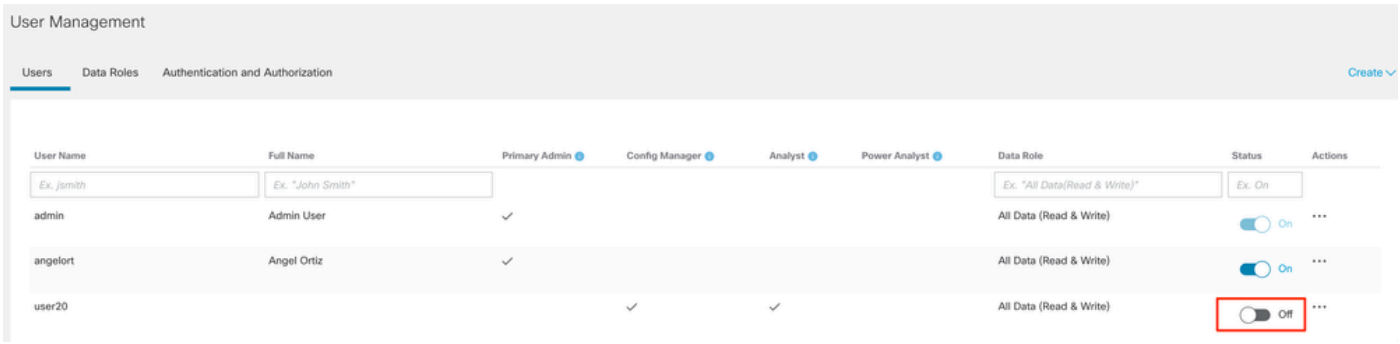
Il est important de mentionner que si un utilisateur est défini et activé localement (dans le Manager), alors l'utilisateur est authentifié à distance, mais autorisé localement. Le processus de sélection de l'utilisateur est le suivant :

1. Une fois les informations d'identification saisies sur la page d'accueil, le gestionnaire 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 configurée précédemment) 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 effectuées à distance.

Pour cette raison, les étapes permettant de configurer correctement l'authentification à distance sont décrites ci-dessous.

Étape D-1. Désactiver ou supprimer 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 à distance via LDAP, mais qui sont configurés localement.

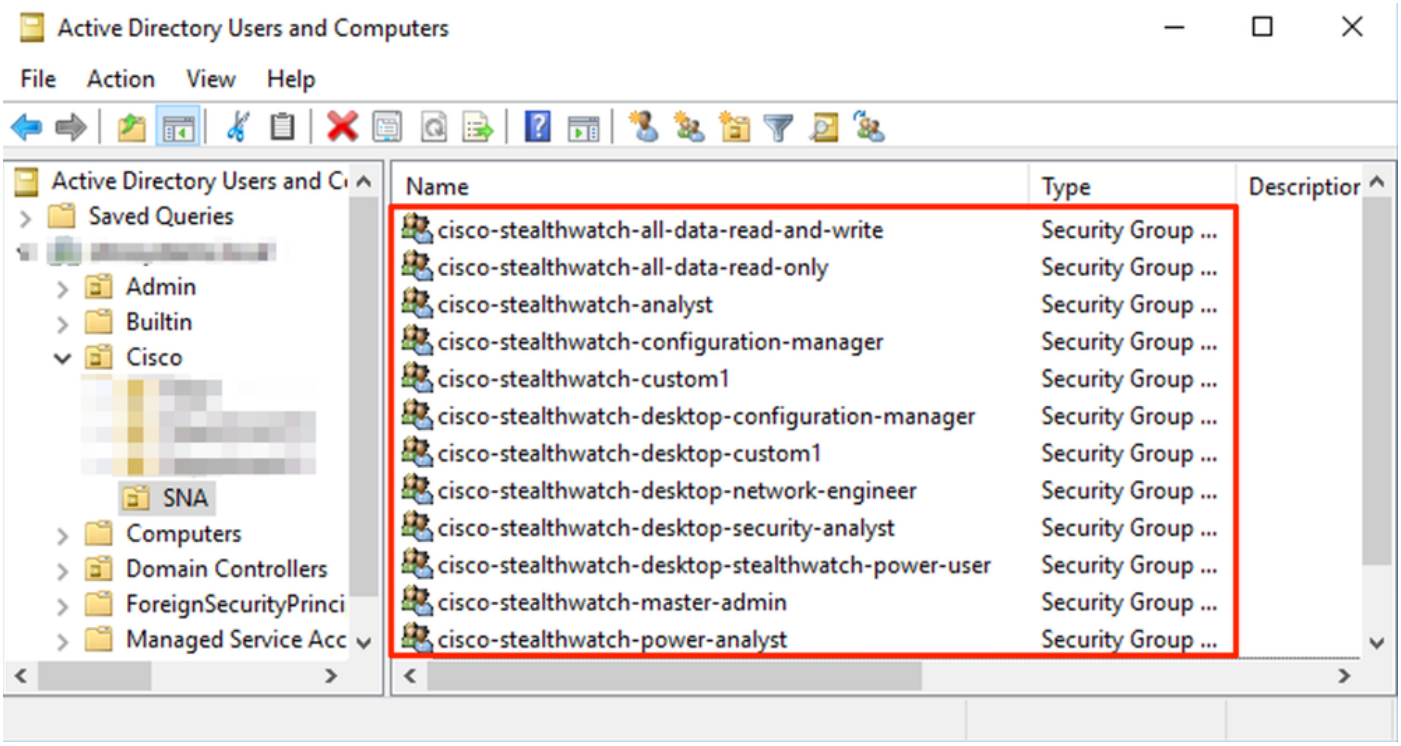


Étape D-2. Définition des groupes cisco-stealthwatch sur le serveur Microsoft AD

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 que SNA a, ils doivent être définis comme suit.

Rôle SNA	Nom du ou des groupes
Administrateur principal	• cisco-stealthwatch-master-admin
Rôle des données	• cisco-stealthwatch-all-data-read-and-write • cisco-stealthwatch-all-data-read-only • cisco-stealthwatch-<custom> (facultatif) Remarque : Assurez-vous que les groupes de rôles de données personnalisés commencent par « cisco-stealthwatch- ».
Rôle fonctionnel Web	• cisco-stealthwatch-configuration-manager • Cisco StealthWatch Power Analyst • cisco-stealthwatch-analyst

Rôle fonctionnel du bureau	• cisco-stealthwatch-desktop-stealthwatch-power-user • cisco-stealthwatch-desktop-configuration-manager • cisco-stealthwatch-desktop-network-engineering • cisco-stealthwatch-desktop-security-analyst • cisco-stealthwatch-desktop-<personnalisé> (facultatif) Remarque : Assurez-vous que les groupes de rôles fonctionnels personnalisés commencent par « cisco-stealthwatch-desktop-desktop- ».



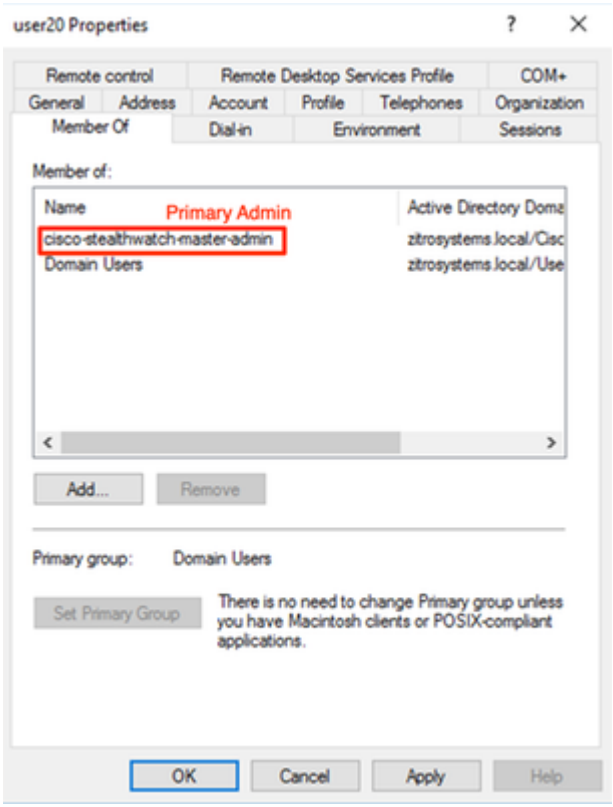
Remarque : Comme décrit précédemment, les groupes personnalisés sont pris en charge pour « Rôle de données » et « Rôle fonctionnel de bureau » tant que le nom du groupe est précédé de la chaîne appropriée. Ces rôles et groupes personnalisés doivent être définis à la fois dans le gestionnaire SNA et dans le serveur Active Directory. Par exemple, si vous définissez un rôle personnalisé « personnalisé » dans le SNA Manager pour un rôle de client de bureau, il doit être mappé à cisco-stealthwatch-desktop-custom dans Active Directory. Notez que bien qu'il soit possible de créer des rôles et des groupes avec des valeurs numériques présentes dans ce, cela casse le journal LDAP/TACACS avec une (IllegalRolesException). Ce défaut est documenté sous l'ID de bogue Cisco CSCww00167

. 🔍. Pour cette raison, nous vous recommandons de NE PAS utiliser de valeurs numériques lors de la création de ces rôles/groupes.

Étape D-3. Définition des mappages de groupes d’autorisations LDAP pour les utilisateurs

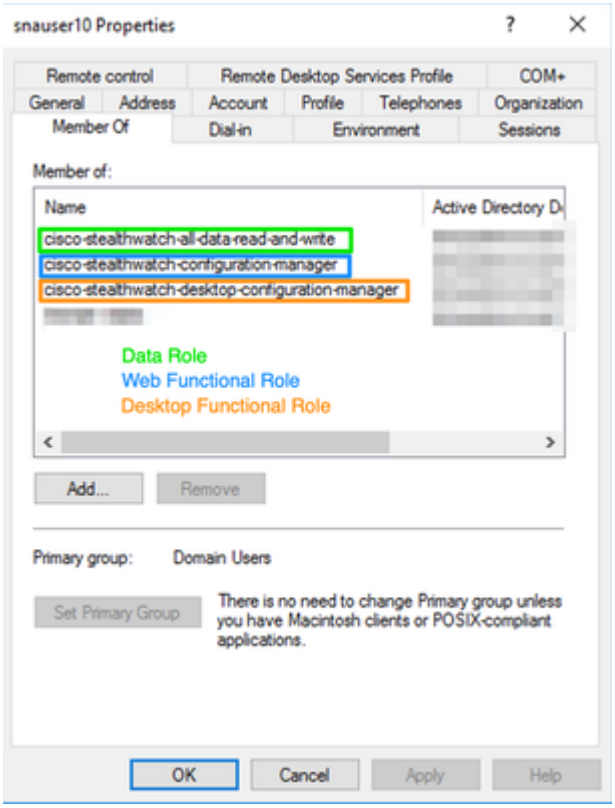
Une fois que les groupes cisco-stealthwatch ont été définis dans le serveur AD, nous pouvons mapper les utilisateurs destinés à avoir accès au SNA Manager aux groupes nécessaires. Cela doit se faire comme suit.

- Un utilisateur Administrateur 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 d'administration principale, doit être affecté à un groupe de chaque rôle avec les conditions suivantes.

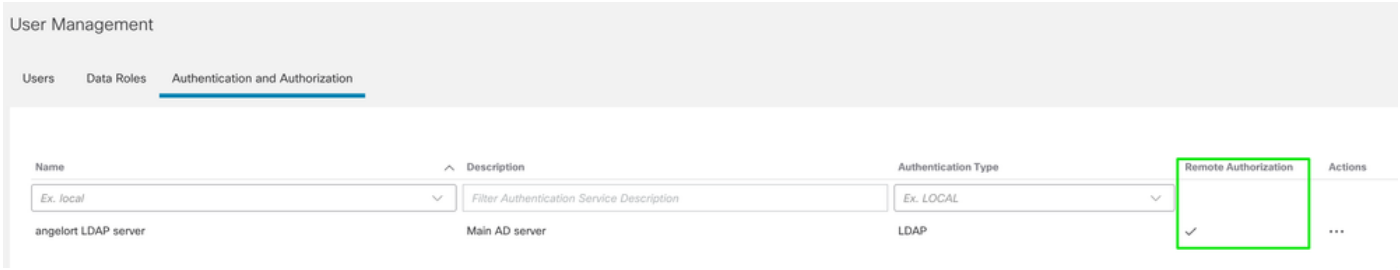
a. Rôle de données : L'utilisateur doit être affecté à un seul groupe.
b. Rôle fonctionnel Web : L'utilisateur doit être affecté à au moins un groupe.
c. Rôle fonctionnel du bureau : L'utilisateur doit être affecté à au moins un groupe.



Étape D-4. Activer l'autorisation à distance via LDAP sur le gestionnaire SNA.

1. Ouvrez le tableau de bord principal du gestionnaire et accédez à Paramètres généraux > Gestion des utilisateurs.
2. Dans la fenêtre Gestion des utilisateurs, sélectionnez l'onglet Authentification et autorisation.
3. Localisez le service d'authentification LDAP qui a été configuré à l'étape C.
4. Cliquez sur Actions > Enable Remote Authorization.

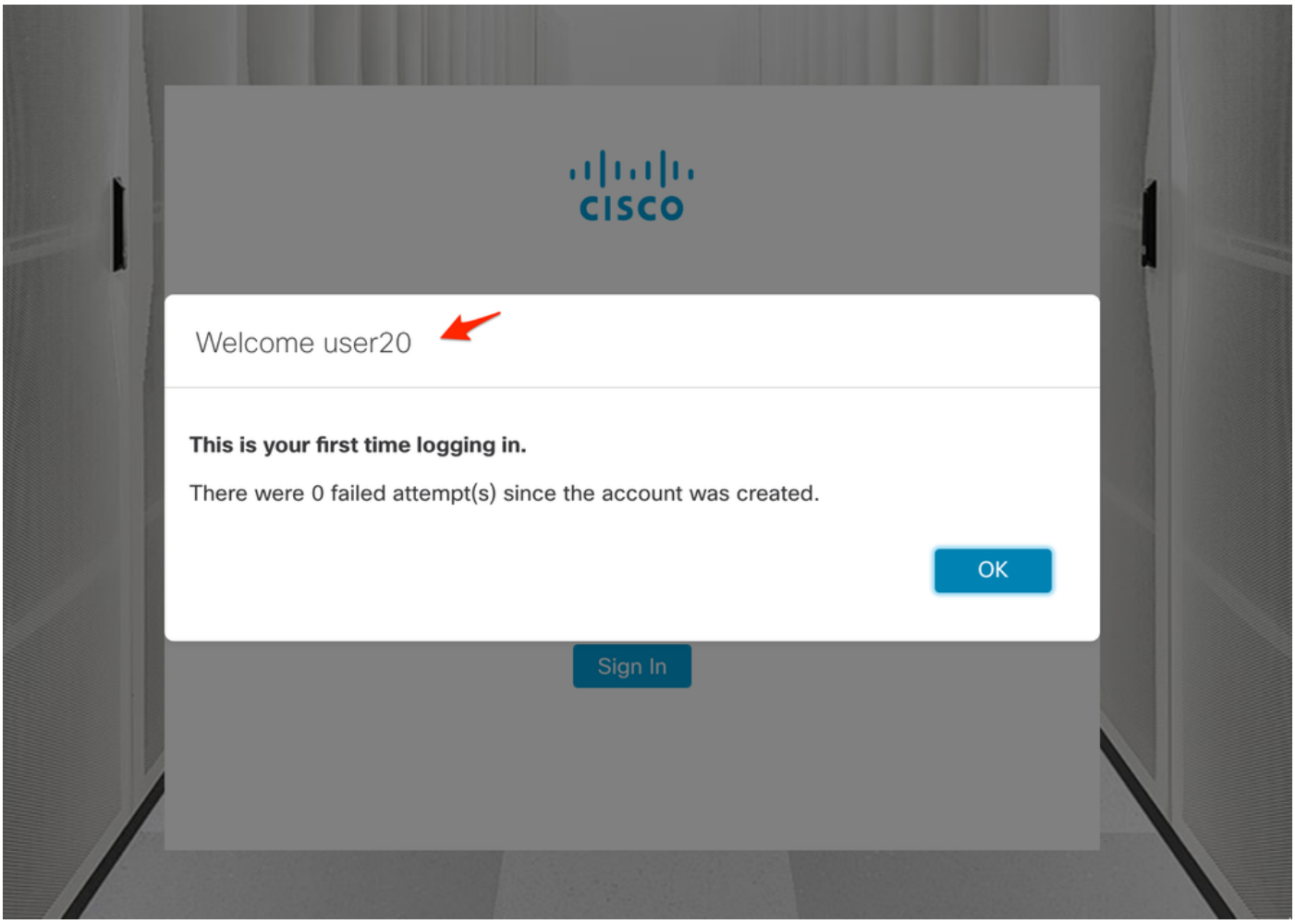
Remarque : Un seul service d'autorisation externe peut être utilisé à la fois. Si un autre service d'autorisation est déjà en cours d'utilisation, il est automatiquement désactivé et le nouveau est activé. Cependant, tous les utilisateurs qui étaient autorisés avec le service externe précédent sont déconnectés.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



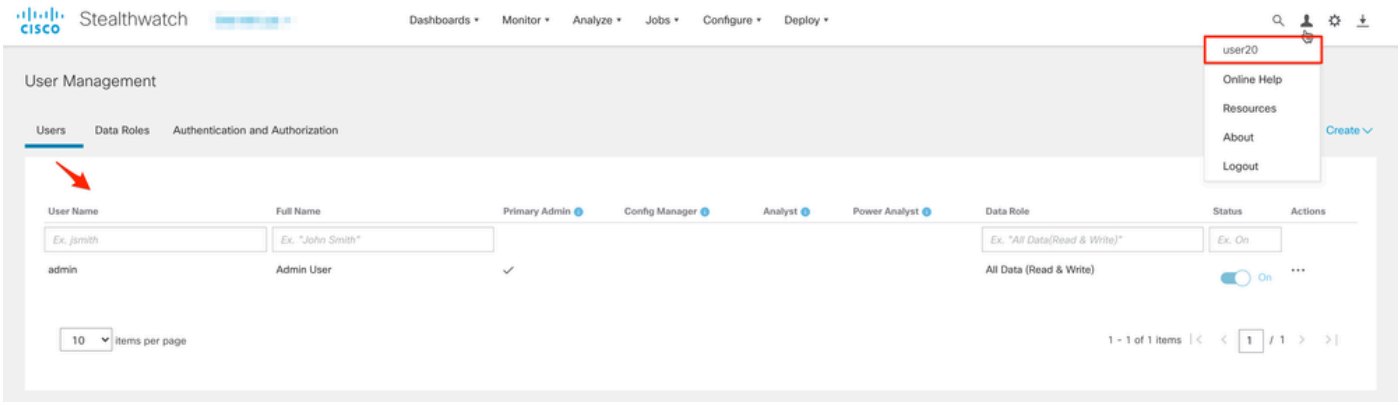
Vérifier

Utilisez cette section pour confirmer que votre configuration fonctionne correctement.

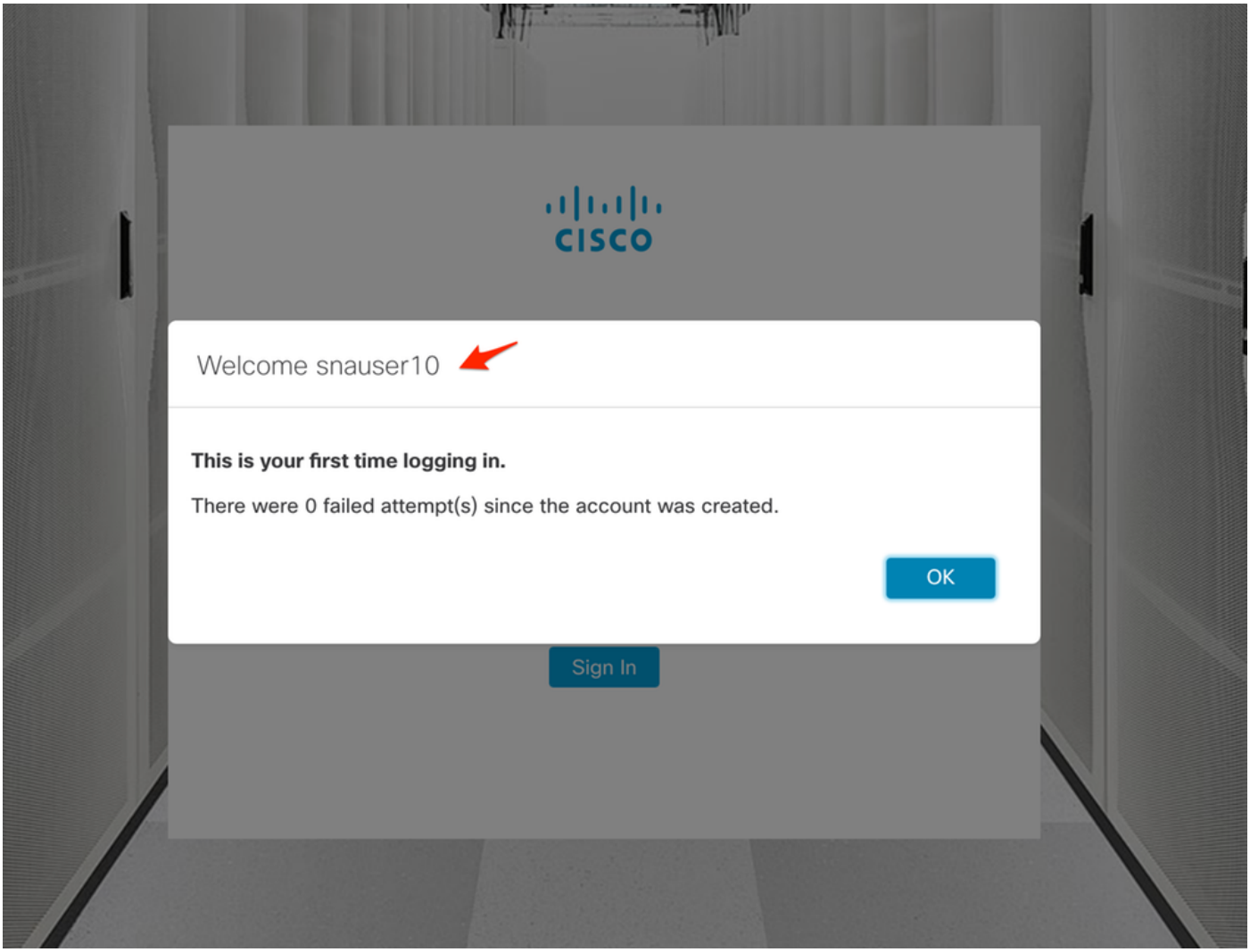
Les utilisateurs peuvent se connecter avec les informations d'identification définies sur le serveur AD.



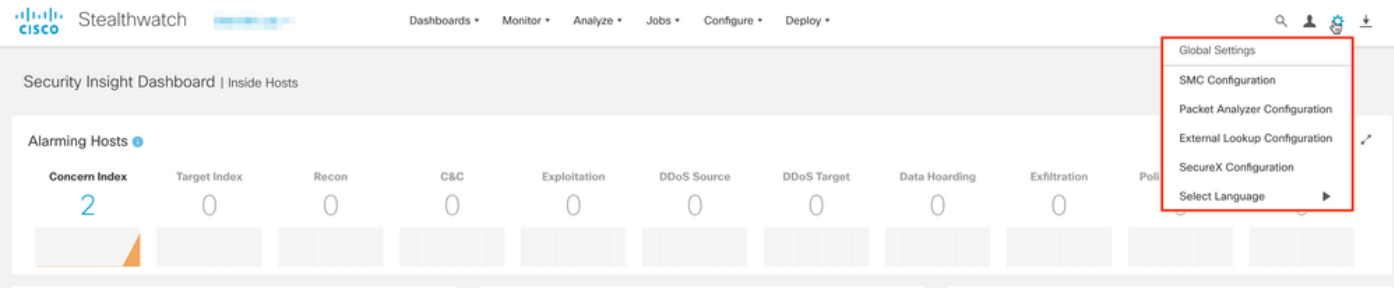
La deuxième étape de vérification concerne l'autorisation. Dans cet exemple, l'utilisateur « user20 » a été fait membre du groupe cisco-stealthwatch-master-admin dans le serveur AD, et vous pouvez confirmer que l'utilisateur a des autorisations d'administrateur principal. L'utilisateur n'étant pas défini dans les utilisateurs locaux, vous pouvez 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". Vous pouvez confirmer l'authentification avec les informations d'identification configurées sur le serveur AD.



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



Dépannage

Cette section fournit des informations que vous pouvez utiliser pour dépanner votre configuration.

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 ne contient que 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 à la fois des valeurs DNS et IPv4, utilisez la première valeur répertoriée.
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 de Cisco. Un contrat d'assistance valide est requis : Cisco Worldwide Support Contacts.
- 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.