Secure Network Analytics Managerアクセス用のLDAPSによる外部認証および許可の設定

内容

概要

このドキュメントでは、外部認証を使用するためにSecure Network Analytics Manager（旧Stealthwatch Management Center）バージョン7.1以降を設定し、LDAPSで外部認証を使用するためにバージョン7.2.1以降を設定する基本的な設定について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- Cisco Secure Network Analytics（旧Stealthwatch）
- 一般的なLDAPおよびSSLの動作
- 一般的なMicrosoft Active Directory管理

使用するコンポーネント

このドキュメントの情報は、次のコンポーネントに基づいています。

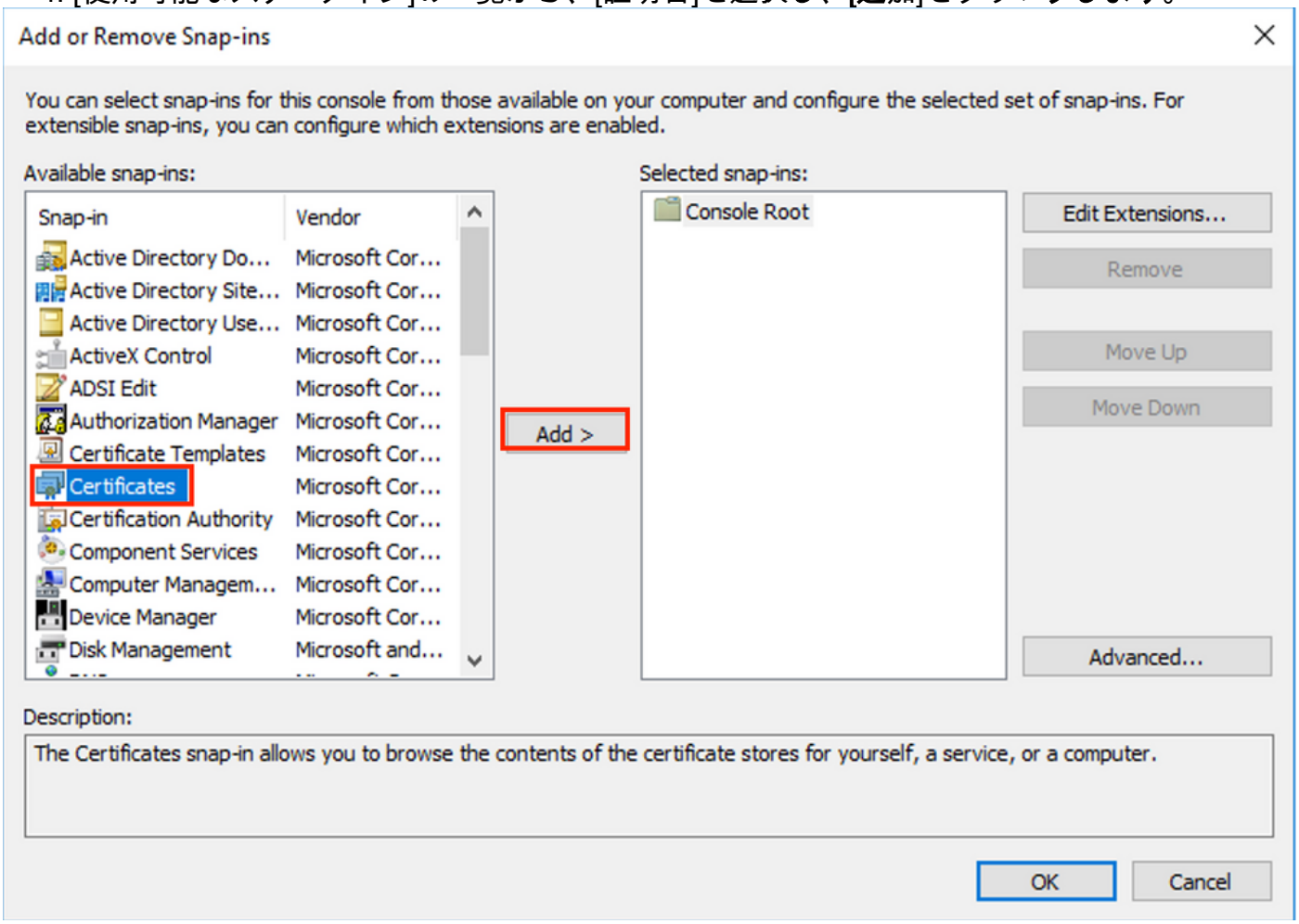
- Cisco Secure Network Analytics Manager（旧SMC）バージョン7.3.2
- Active Directoryドメインコントローラとして構成されたWindows Server 2016

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

設定

ステップA:ADドメインコントローラにログインし、LDAPに使用するSSL証明書をエクスポートします。

1. Windows Server 2012以降の場合は、[スタート]メニューから[実行]を選択し、certlm.mscと入力してステップ8に進みます。
2. 古いバージョンのWindows Serverの場合は、[スタートメニュー]から[ファイル名を指定して実行]を選択し、mmcと入力します。
3. [ファイル]メニューから、[スナップインを追加/削除]を選択します。
4. [使用可能なスナップイン]の一覧から、[証明書]を選択し、[追加]をクリックします。

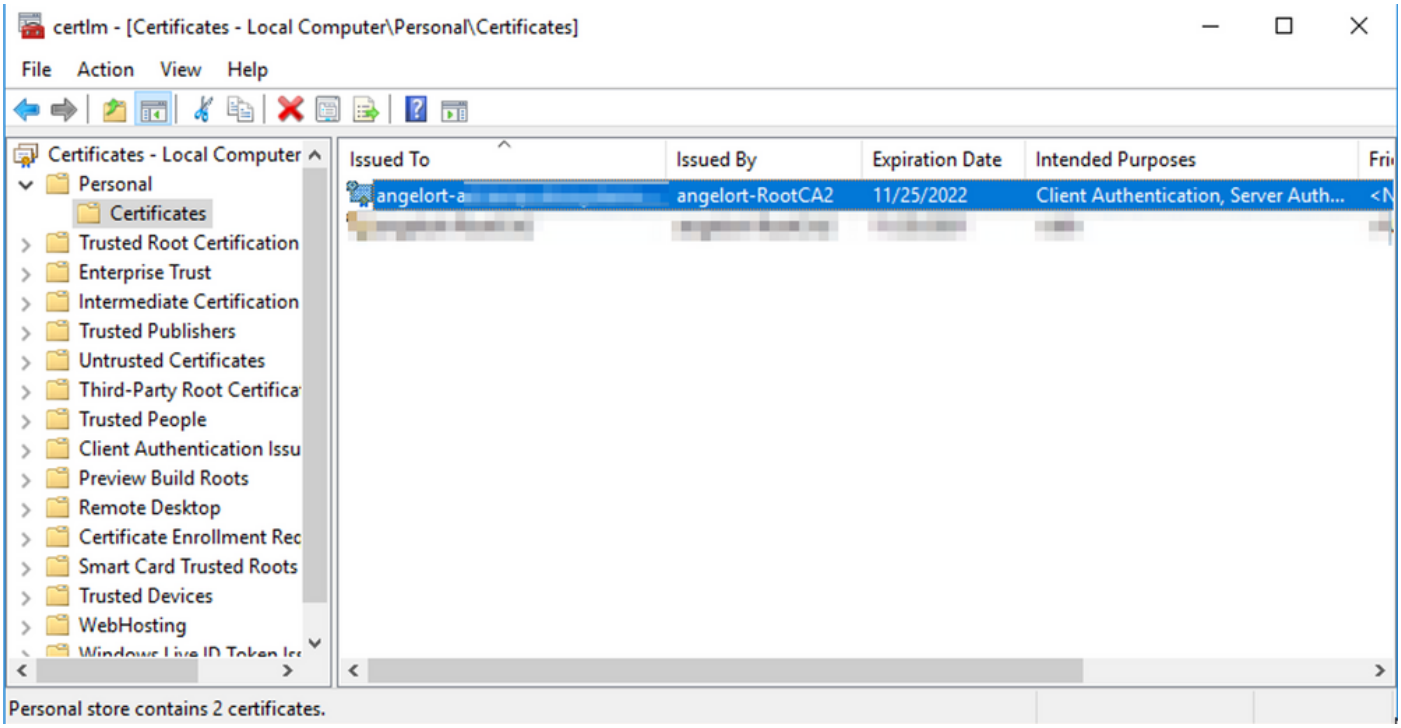


5. [証明書スナップイン]ウィンドウで、[コンピュータアカウント]を選択して、[次へ]を選択します。

6. [ローカルコンピュータ]を選択したままにし、[完了]を選択します。

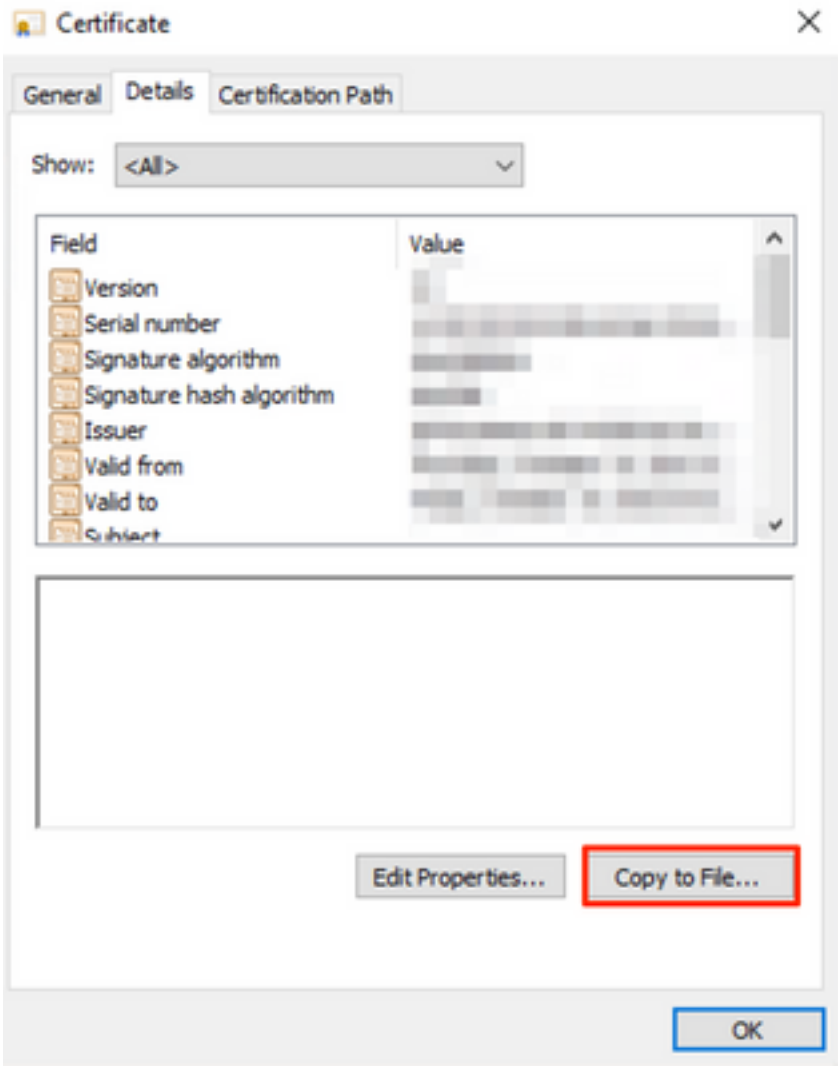
7. 「スナップインの追加または削除」ウィンドウで、「OK」を選択します。

8. [**Certificates (**Local Computer)] > [Personal] > [Certificates]に移動します



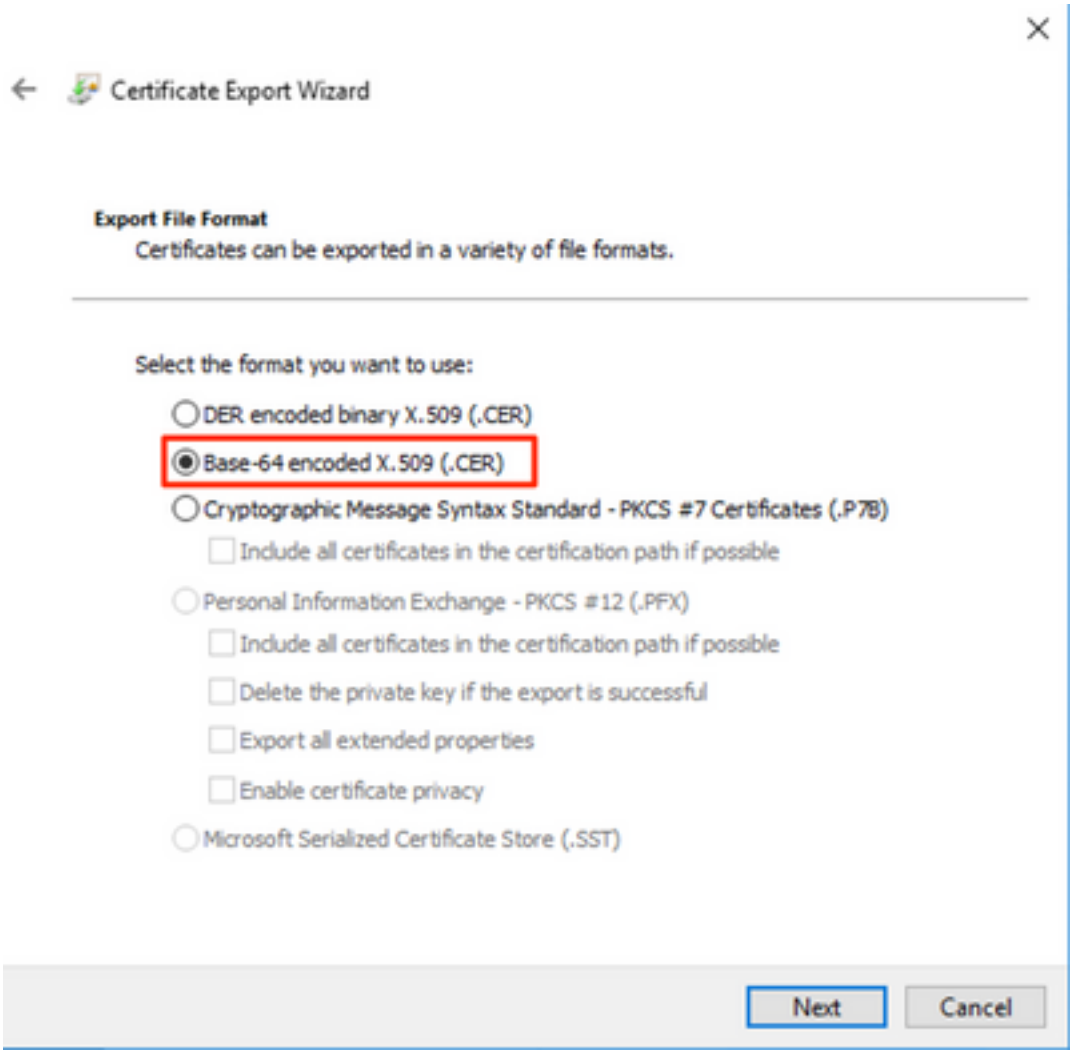
9.ドメインコントローラのLDAPS認証に使用するSSL証明書を選択して右クリックし、[開く]をクリックします。

10. 「詳細」タブにナビゲートし、「ファイルにコピー」をクリックし、「次へ」

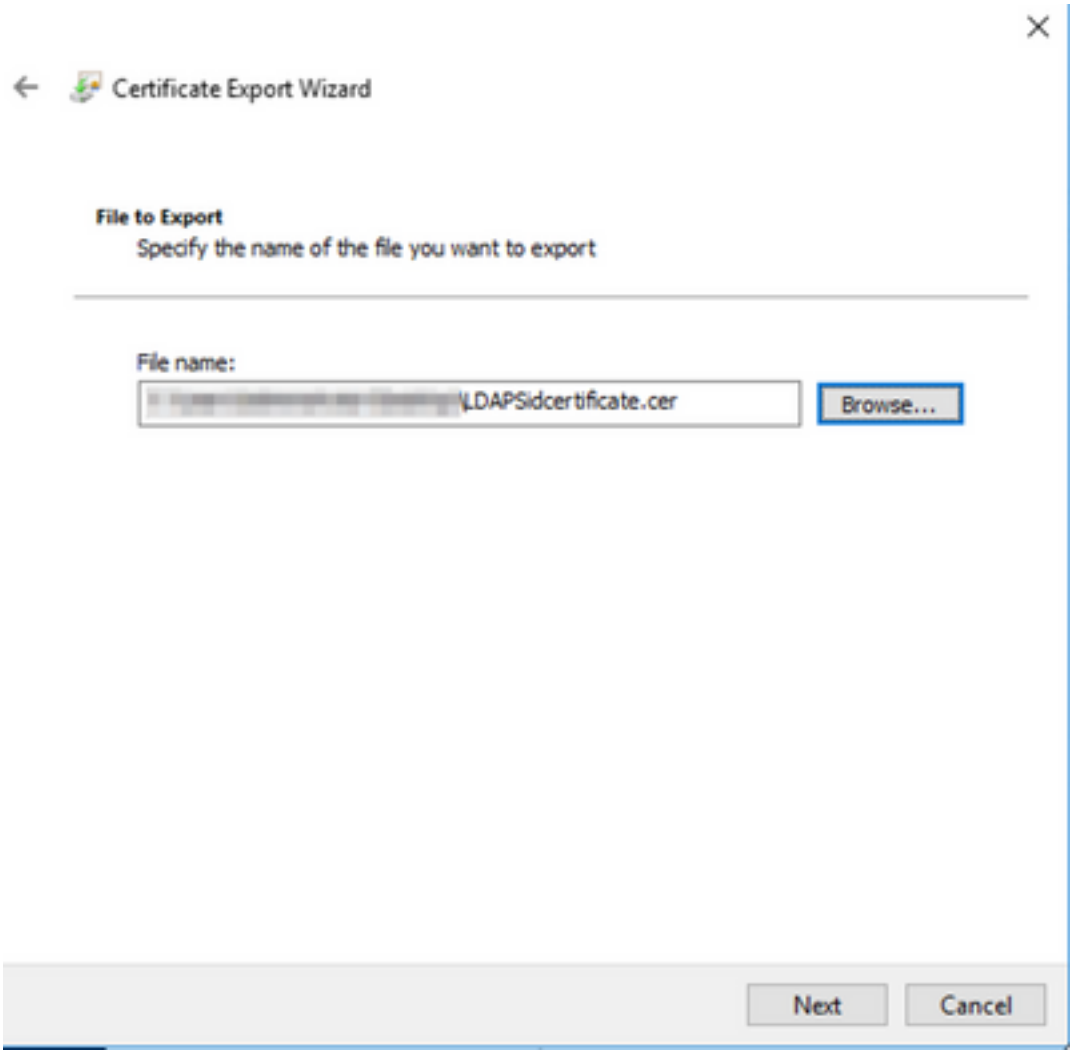


11. [いいえ、秘密キーを**エクスポートしない]が選択されていることを確認**し、[次へ]をクリック**します**

12. **Base**-64 encoded **X.509 formatを選択し、**Nextをクリック**します。**



13.証明書を保存する場所を選択し、ファイルに名前を付けて、[次へ]をクリックします。



14. [**Finish**]をクリックします。「The export was successful」が表示されます。 メッセージに応答します。

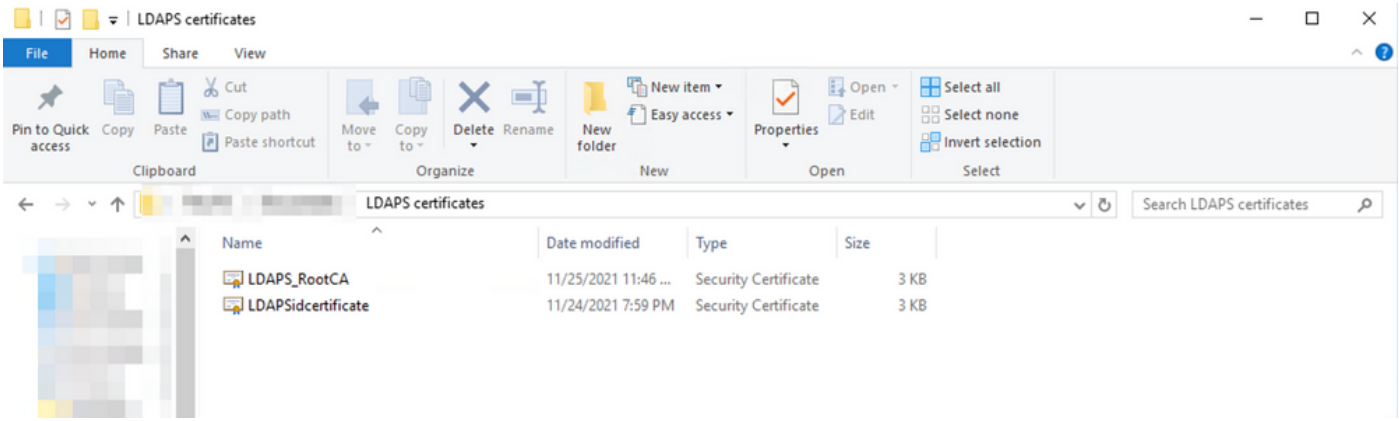
15. LDAPSに使用する証明書に戻り、[Certification Path]タブを**選択します。**

16.認証パスの上部にあるルートCA発行者を選択し、[**View Certificate**]をクリ**ックします。**

17. LDAPS認証に使用される証明書に署名したルートCAの証明書をエクスポートするには、手順10 ~ 14を繰り返します。

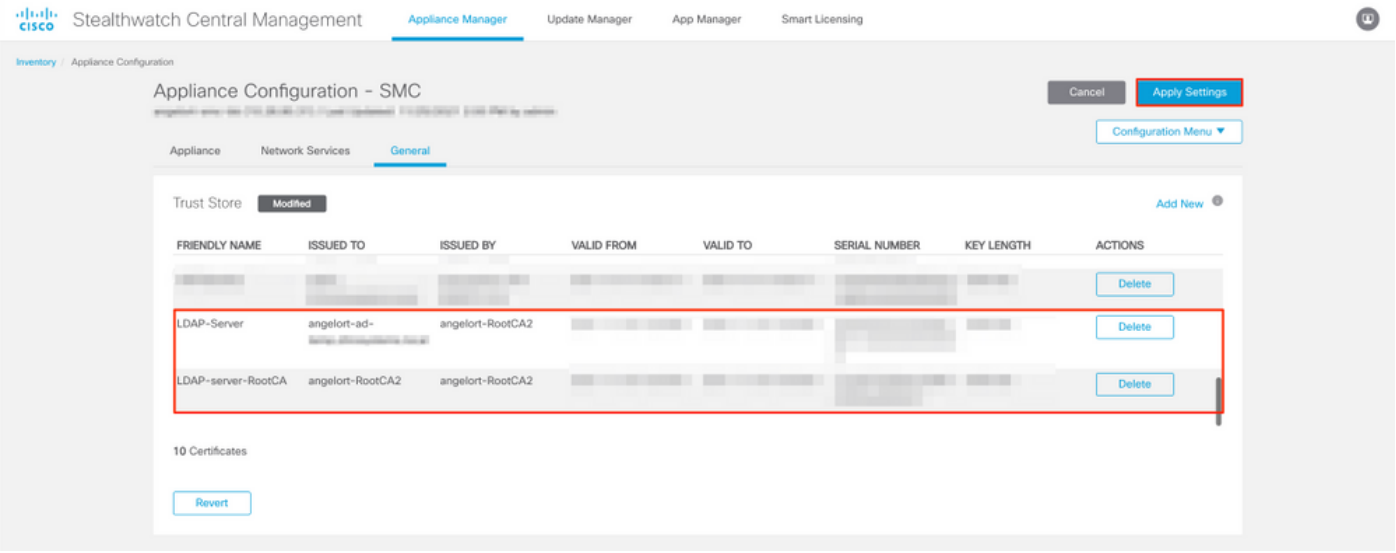
> **注**：導入には複数階層のCA階層を使用できます。この場合、同じ手順に従って、信頼チェーン内のすべての中間証明書をエクスポートする必要があります。

18.続行する前に、LDAPSサーバ用の証明書ファイルと、証明書パス内の各発行局の証明書ファイルが1つあることを確認してください。ルート証明書と中間証明書（該当する場合）。



ステップB:SNAマネージャにログインし、LDAPサーバとルートチェーンの証明書を追加します。

1. [Central Management] > [Inventory]に移動します。
2. SNA Managerアプライアンスを見つけ、[アクション(Actions)] > [アプライアンス設定の編集(Edit Appliance Configuration)]をクリックします。
3. [アプライアンスの設定(Appliance Configuration)]ウィンドウで、[設定(Configuration)]メニュー> [信頼ストア(Trust Store)] > [新規追加(Add New)]に移動します。
4. フレンドリ名を入力し、[ファイルの選択]をクリックしてLDAPサーバーの証明書を選択し、[証明書の追加]をクリックします。
5. 前の手順を繰り返して、ルートCA証明書と中間証明書（該当する場合）を追加します。
6. アップロードされた証明書が正しいことを確認し、[Apply Settings]をクリックします。

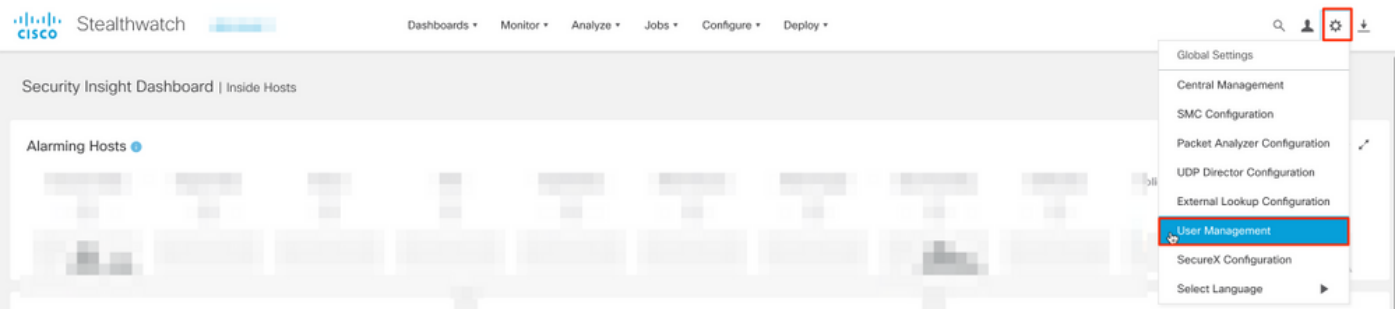


7.変更が適用され、マネージャのステータスが[Up]になるまで待ちます。

ステップC:LDAP外部サービス設定を追加します。

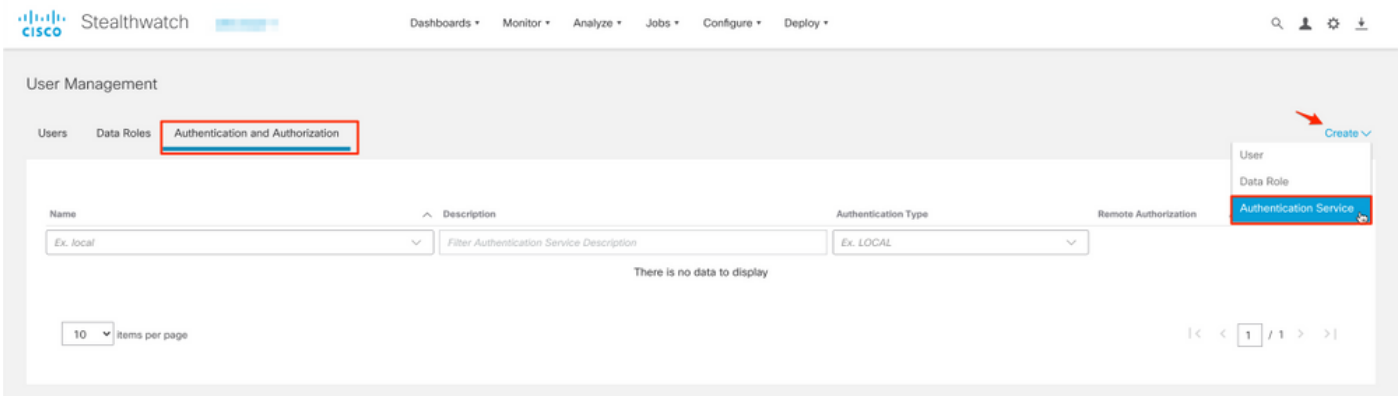
SNAバージョン7.2以降

1. Managerのメイン・ダッシュボードを開き、「グローバル設定」>「ユーザー管理」に移動します。



2. 「ユーザー管理」ウィンドウで、「認証」タブを選択します。

3. [Create] > [Authentication Service]をクリックします。



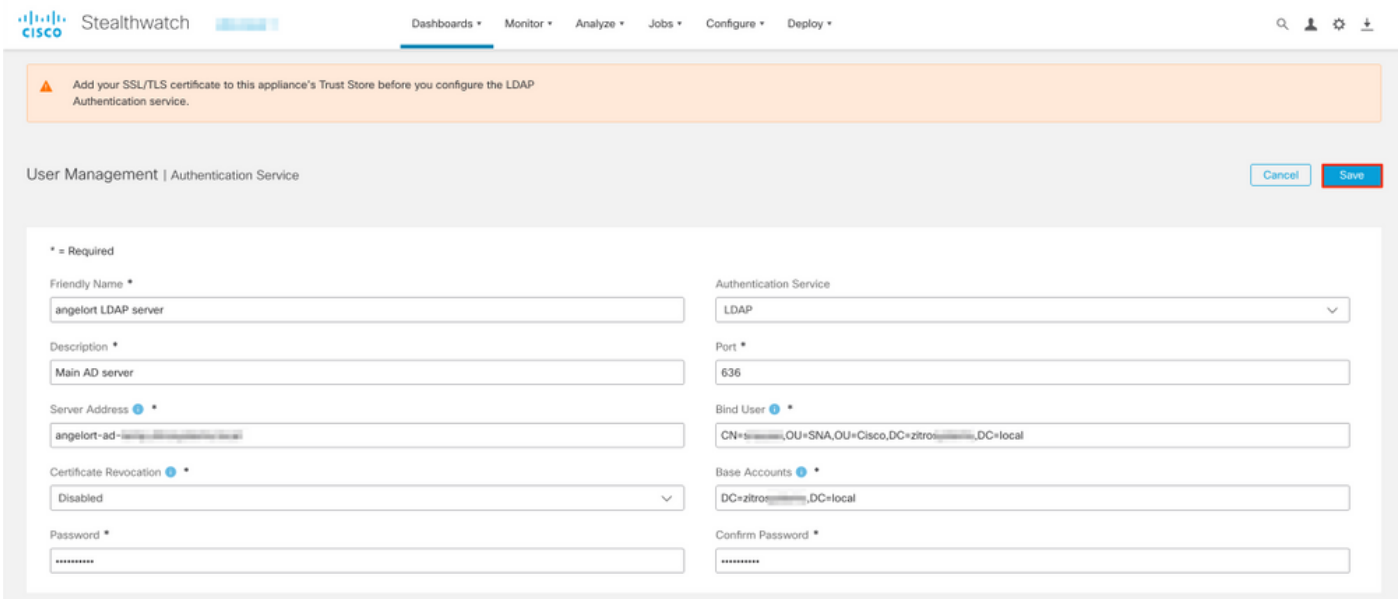
4. [Authentication Service]ドロップダ**ウンメニュー**から[LDAP]を**選択します。**

5.必須フィールドに入力します。

フィールド	**注意事項**
フレンドリ名	LDAPserverの名前を入力します。
説明	LDAPサーバの説明を入力します。
Server address	**LDAPサーバ証明書の[Subject Alternative Name (SAN)]フィールドで指定された完全修飾ドメイン入力します。** • [SAN]フィールドにIPv4アドレスだけが含まいる場合は、[Server Address]フィールドにIドレスを入力します。 • [SAN]フィールドにDNS名が含まれている場、[Server Address]フィールドにDNS名を入ます。 • [SAN]フィールドにDNSとIPv4の両方の値がれている場合は、リストされている最初の値用します。
ポート	セキュアLDAP通信(LDAP over TLS)用に指定されートを入力します。 LDAPSの既知のTCPポート636です。
ユーザのバインド	LDAPサーバへの接続に使用するユーザIDを入力す。以下に、いくつかの例を示します。 CN=admin,OU=Corporate Users,DC=example,DC=com **注**：ユーザを組み込みADコンテナ（「Userなど）に追加した場合、バインドユーザのバンドDNには、組み込みフォルダ（たとえばCN=username、CN=Users、DC=domain、DC=com）に設定した正規名(CN)が必要でただし、新しいコンテナにユーザを追加した合、バインドDNには、新しいコンテナ名（CN=username、OU=Corporate Users、DC=domain、DC=comなど）に組織単位(OU設定されている必要があります。 **注**：バインドユーザのバインドDNを見つけ利な方法は、Active Directoryサーバに接続て

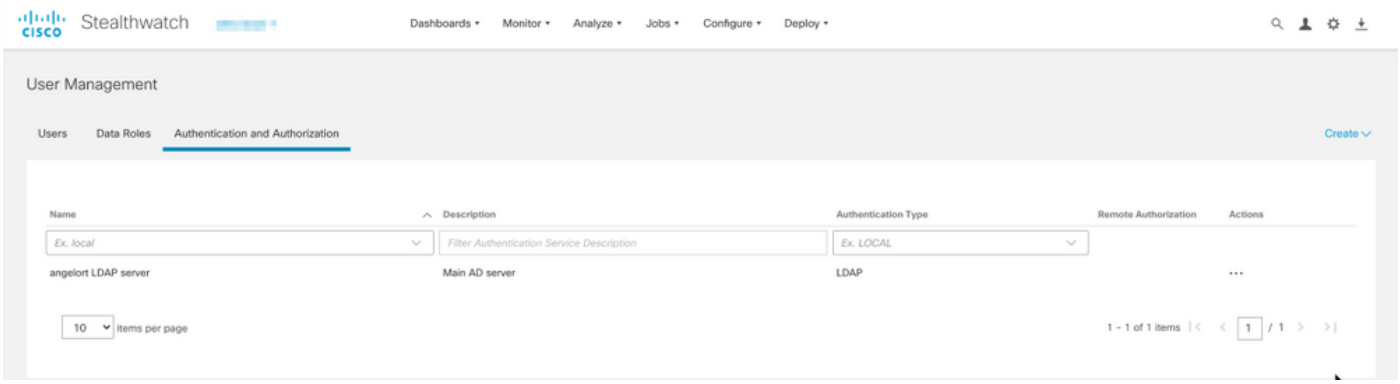
	るWindows Server上のActive Directoryを照会
ることです。この情報を取得するには、
Windowsコマンドプロンプトを開き、コマン
dsquery user dc=<distinguished>,dc=<name
name <user>を入力します。例：**dsquery us**
dc=example,dc=com -name user1。結果は
"CN=user1,OU=Corporate
Users,DC=example,DC=com"のようになりま
。
Password	LDAPサーバへの接続に使用するバインドユーザ
ワードを入力します。
基本アカウント	識別名(DN)を入力します。
DNは、ユーザの検索を開始する必要があるディ
トリのブランチに適用されます。多くの場合、テ
クトリツリー（ドメイン）の一番上にありますが
ィレクトリ内でサブツリーを指定することもでき
。バインドユーザおよび認証を受けるユーザは、
スアカウントからアクセスできる必要があります
以下に、いくつかの例を示します。
dc=example,dc=com

6. [保存]をクリックします。



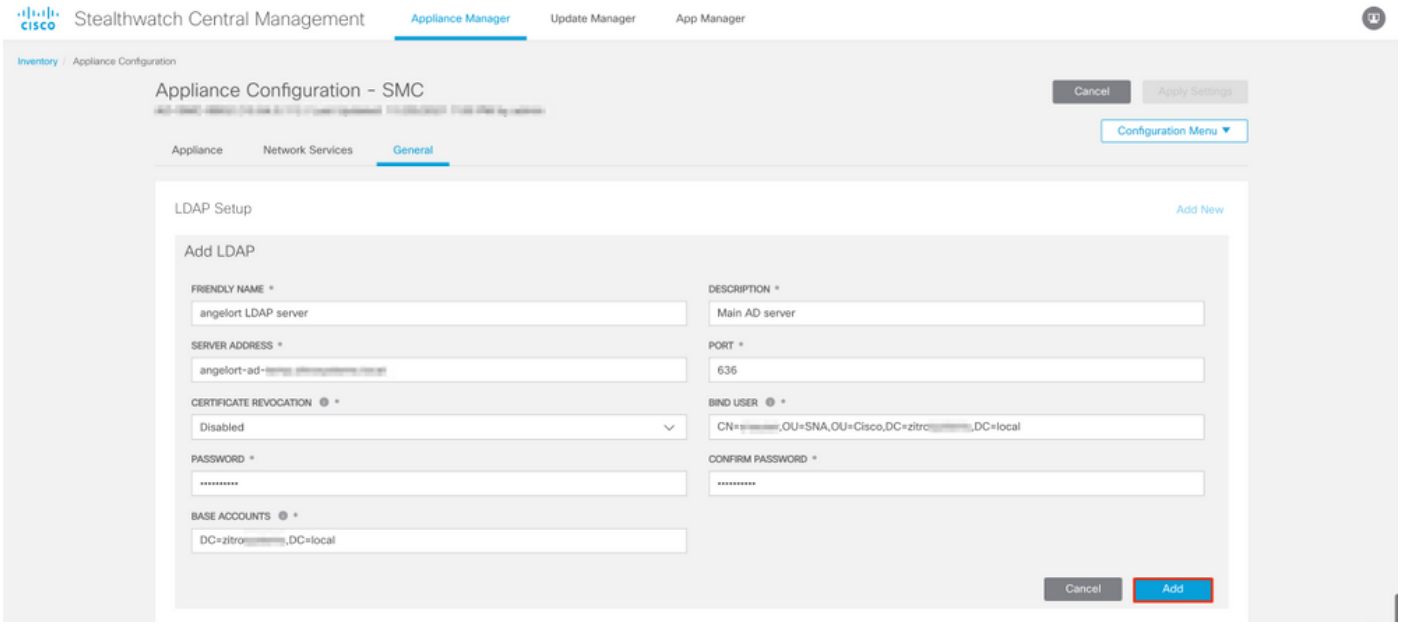
7.入力した設定と信頼ストアに追加した証明書が正しい場合は、「You'have successfully saved your changes」バナーを取得する必要があります。

8.設定されたサーバは、[User **Management] > [Authentication and Authorization]**の下に表示される必要があります。



SNAバージョン7.1

1. [Central Management] > [Inventory]に移動します。
2. SMCアプライアンスを見つけ、[Actions] > [Edit Appliance Configuration]をクリックします。
3. [アプライアンスの設定(Appliance Configuration)]ウィンドウで、[設定メニュー(Configuration Menu)] > [LDAP設定(LDAP Setup)] > [新規追加(Add New)]に移動します。
4. SNAバージョン7.2以降のステップ5の説明に従って、必須フィールドに入力します。



5. 「追加」をクリックします。

6. [設定の適用]をクリックします。

7.入力した設定と信頼ストアに追加した証明書が正しければ、マネージャの変更が適用され、アプライアンスの状態がアップである必要があります。

ステップD：許可設定を設定します。

SNAは、LDAP経由のローカル認証とリモート認証の両方をサポートします。この設定では、ADサーバのLDAPグループが組み込みロールまたはカスタムSNAロールにマッピングされます。

LDAPを介したSNAでサポートされる認証および許可方式は次のとおりです。

- リモート認証とローカル認証

- リモート認証とリモート認証(SNAバージョン7.2.1以降でのみサポート)

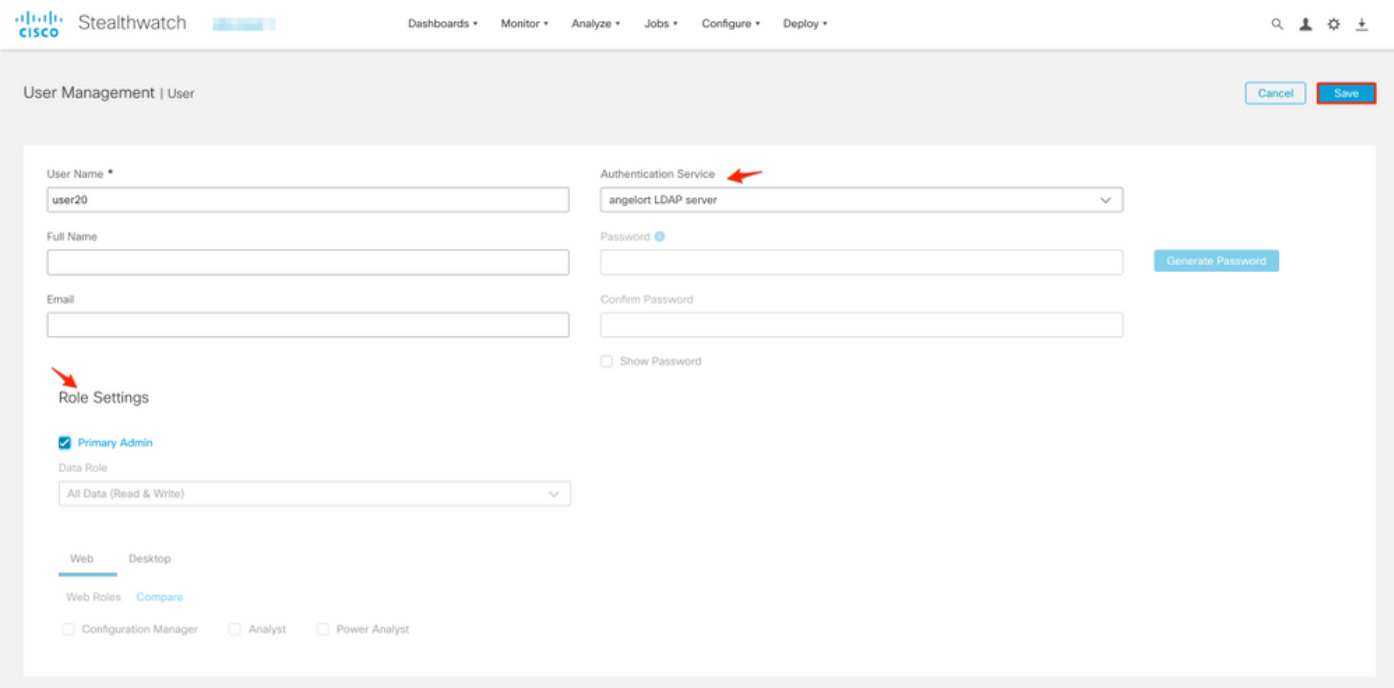
ローカル認証

この場合、ユーザとそのロールをローカルに定義する必要があります。これを実現するには、次の手順に従います。

1. [User Management]に再び移動し、[Users]タブ> [Create] > [User]の順にクリックします。

2. LDAPサーバーで認証するユーザー名を定義し、「認証サービス」ドロップダウン・メニューから構成されたサーバーを選択します。

3. LDAPサーバーで認証されたユーザーがマネージャーに対して持っている必要があるアクセス許可を定義し、[Save]をクリックします。



LDAPによるリモート認証

LDAP経由のリモート認証と許可は、Secure Network Analyticsバージョン7.2.1で最初にサポートされました。

> **注**：バージョン7.1では、LDAPによるリモート認証はサポートされていません。

関連する点として、ユーザが（マネージャで）ローカルに定義され、有効になっている場合、そのユーザはリモートで認証されますが、ローカルで認証されます。ユーザ選択プロセスは次のとおりです。

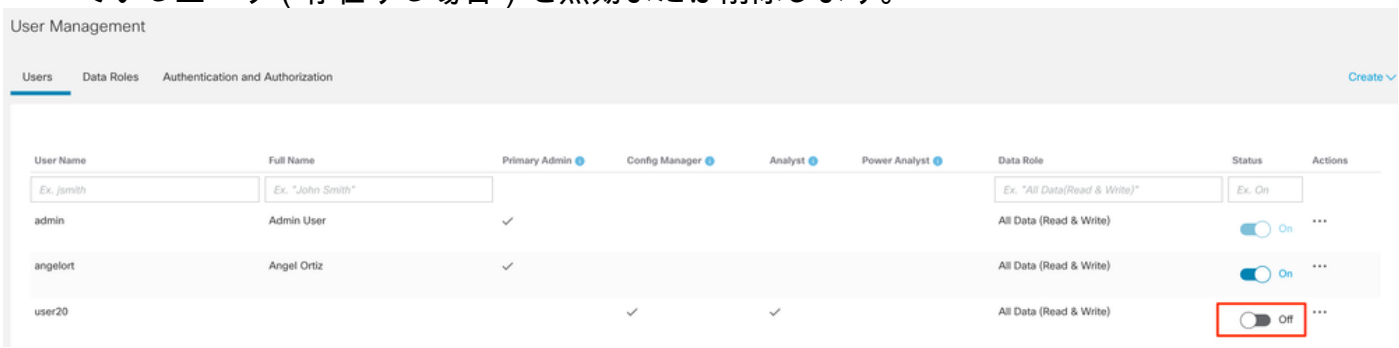
1. マネージャのウェルカムページでクレデンシャルを入力すると、マネージャは指定した名前のローカルユーザを検索します。
2. ローカルユーザが見つかり、有効になっている場合は、リモートで認証されますが（ローカル認証を使用したLDAP経由のリモート認証が事前に設定されている場合）、ローカル設定で認証されます。

3. リモート認証が設定され、有効になっており、ユーザがローカルに見つからない（設定されていない、または無効になっている）場合、認証と認可の両方がリモートで実行されます。

このため、リモート認証を正常に設定する手順は、

ステップD-1：リモート認証を使用するユーザのうち、ローカルで定義されているユーザを無効または削除します。

1. マネージャのメインダッシュボードを開き、[Global Settings] > [User Management]に移動します。
2. LDAP経由のリモート認証と許可を使用することを目的としているが、ローカルに設定されているユーザ（存在する場合）を無効または削除します。

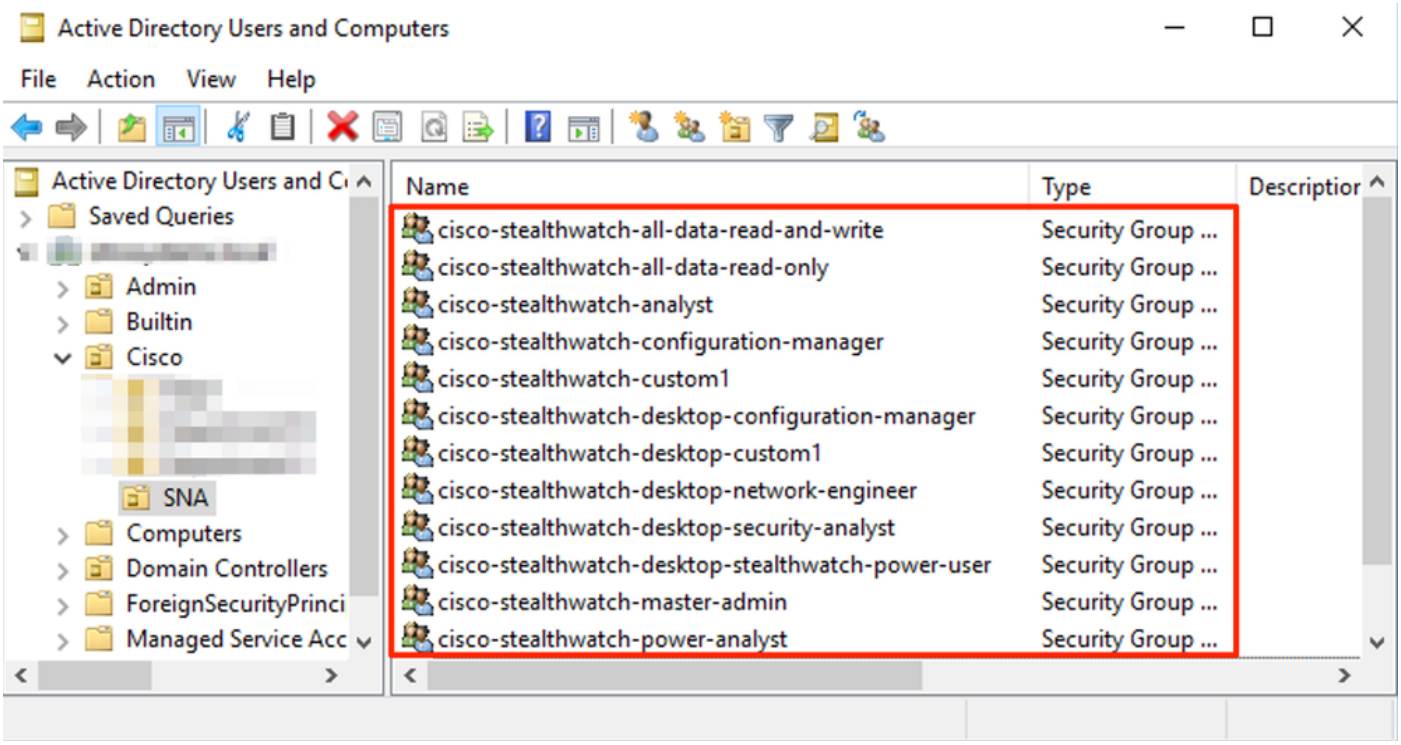


ステップD-2:Microsoft ADサーバでcisco-stealthwatchグループを定義します。

LDAPユーザによる外部認証および許可の場合、パスワードと*cisco-stealthwatchグループ*は、Microsoft Active Directoryでリモートに定義されます。ADサーバで*定義する*cisco-stealthwatchグループは、SNAが持つ異なるロールに関連付けられており、次のように定義する必要があります。

SNAロール	グループ名
プライマリ管理者	• cisco-stealthwatch-master-admin • cisco-stealthwatch-all-data-read-and-write • cisco-stealthwatch-all-data-read-only • cisco-stealthwatch-<カスタム>（オプション **注：**カスタムデータロールグループが「cisc stealthwatch – 」で始まっていることを確認す。
データロール	
Web機能ロール	• cisco-stealthwatch-configuration-manager • cisco-stealthwatch-power-analyst • cisco-stealthwatch-analyst • cisco-stealthwatch-desktop-stealthwatch-pow user • cisco-stealthwatch-desktop-configuration-ma • cisco-stealthwatch-desktop-network-enginee
デスクトップ機能の役割	• cisco-stealthwatch-desktop-security-analyst • cisco-stealthwatch-desktop-<カスタム>（オプン） **注：**カスタムデスクトップの機能ロールグループが「cisco-stealthwatch-desktop – 」で始ま

ていることを確認します。

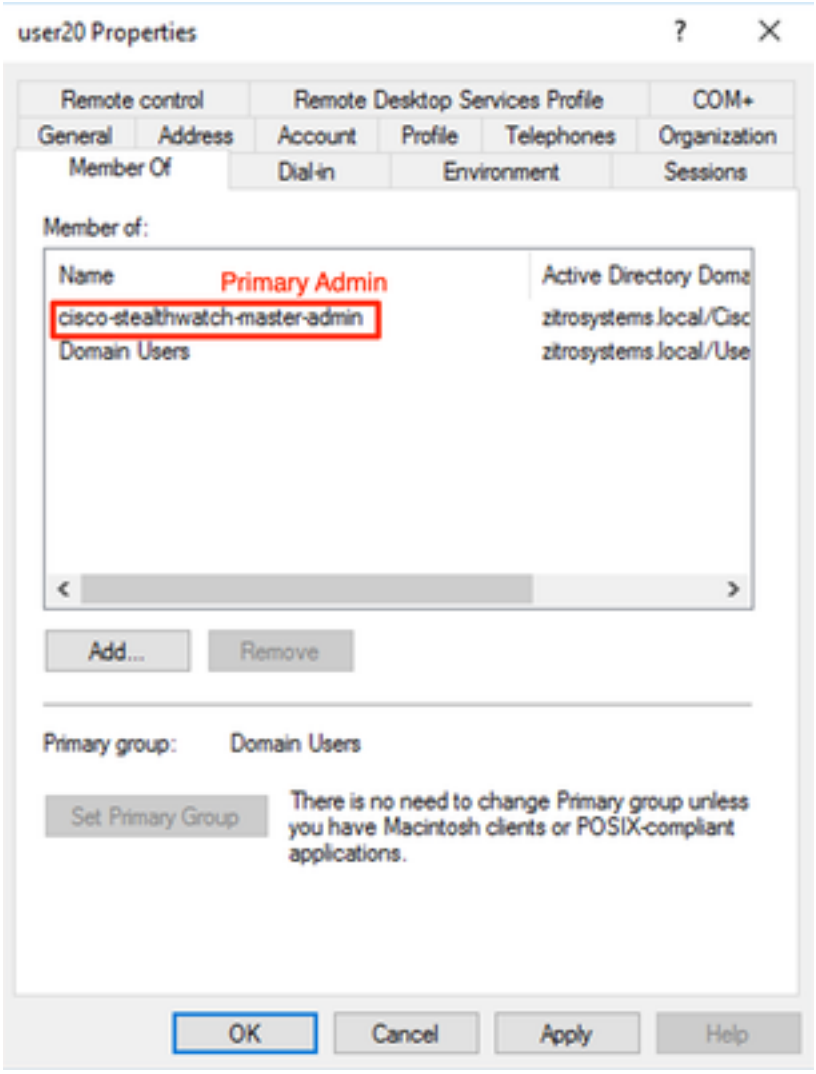


注：前述のように、グループ名の前に適切な文字列が付加されている限り、「データロール」および「デスクトップ機能ロール」に対してカスタムグループがサポートされます。これらのカスタムの役割とグループは、SNAマネージャとActive Directoryサーバの両方で定義する必要があります。たとえば、SNAマネージャでデスクトップクライアントロールのカスタムロール「custom1」を定義する場合、Active Directoryのcisco-stealthwatch-desktop-custom1にマッピングする必要があります。

ステップD-3：ユーザのLDAP許可グループマッピングを定義します。

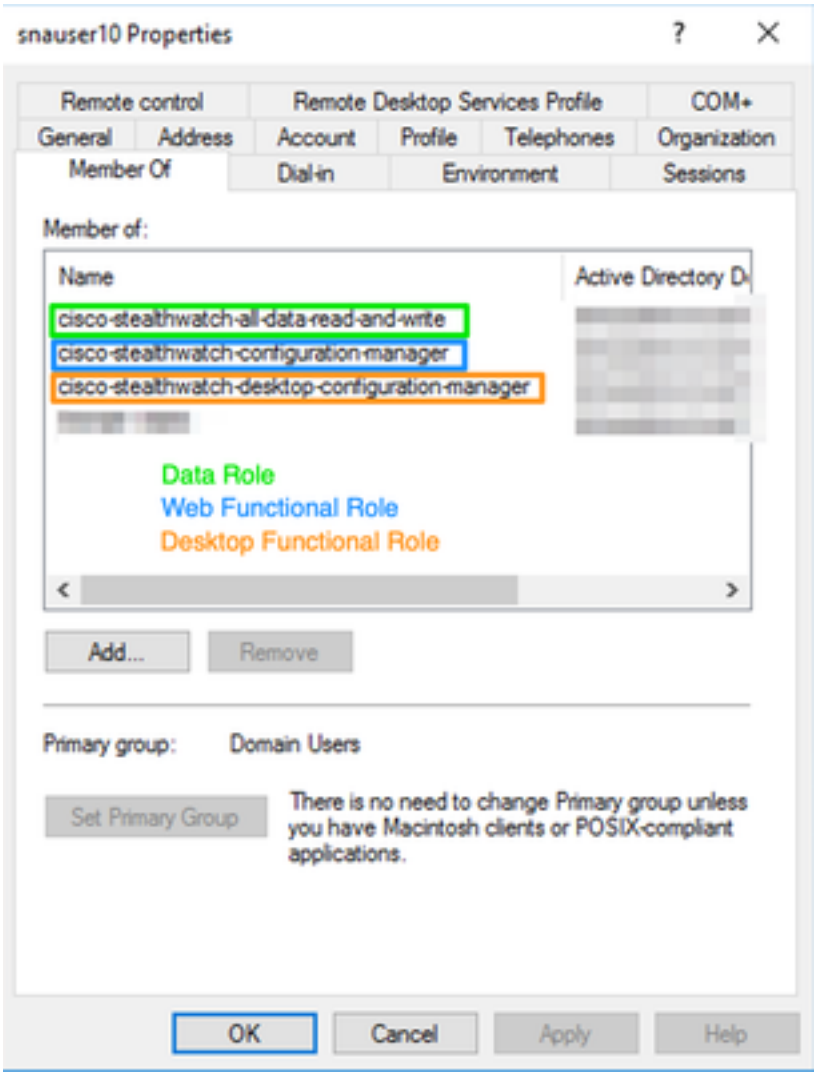
*cisco-stealthwatchグループがADサーバで定義*されたら、SNAマネージャにアクセスするユーザを必要なグループにマッピングできます。これは次のように行う必要があります。

- プライマリ**管理ユーザは、***cisco-stealthwatch-master-adminグループに割り当*てる必要があり、**他の***cisco-stealthwatchグループのメンバーでなければなり*ません。



- プライマリ管理者ユーザ以外の各ユーザは、次の条件で各ロールのグループに割り当てる必要があります。

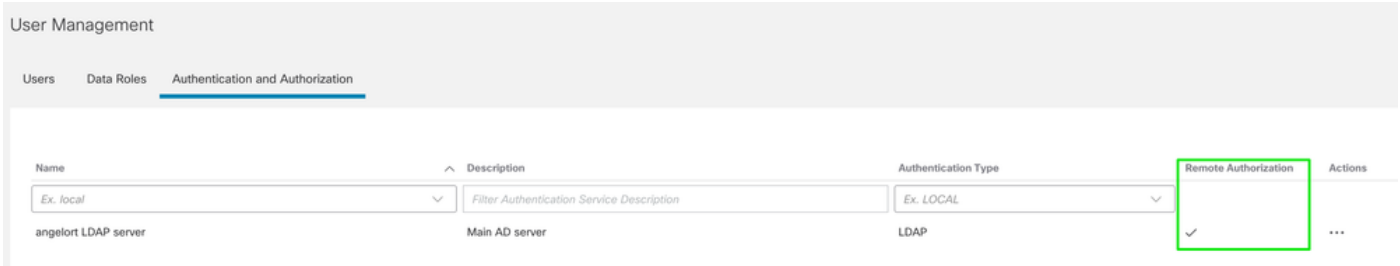
1. **データロール**:ユーザーは1つのグループにのみ割り当**てられている必要があります。**
2. **Web機能ロール**:ユーザーは少なくとも1つのグループに割り当**てられている必要があります**。
3. **デスクトップ機能の役割**:ユーザーは少なくとも1つのグループに割り当**てられている必要があります。**



手順D-4:SNAマネージャでLDAP経由のリモート認証を有効にします。

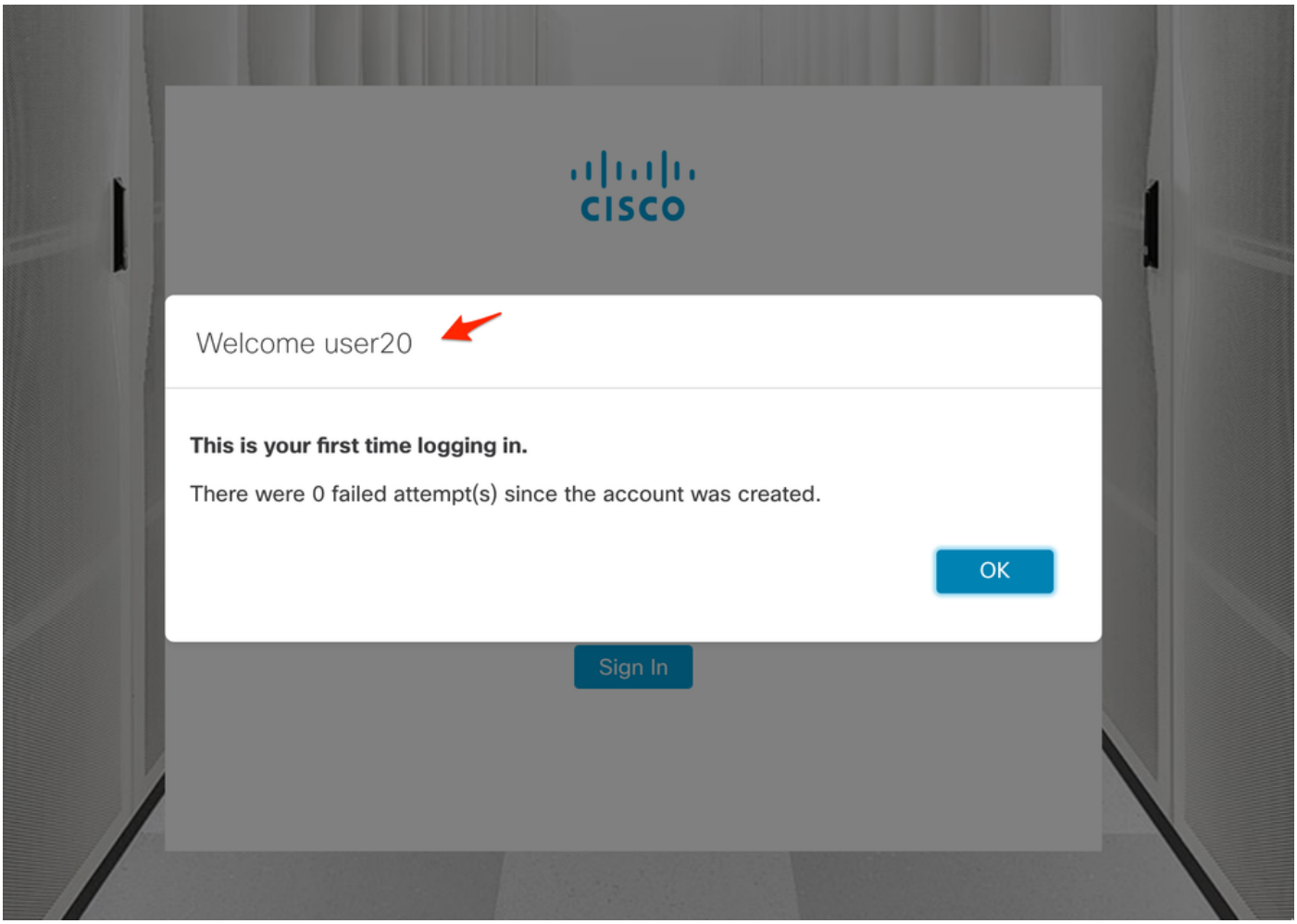
1. マネージャのメインダッシュボードを開き、[グローバル設定] > [ユーザー管理]に移動します。
2. [ユーザー管理]ウィンドウで、[認証と許可]タブを選択します。
3. ステップCで設定したLDAP認証サービスを見つけます。
4. [Actions] > [Enable Remote Authorization]をクリックします。

注：一度に使用できる外部認証サービスは1つだけです。別の承認サービスがすでに使用中の場合、自動的に無効になり、新しい承認サービスが有効になりますが、以前の外部サービスで承認されたすべてのユーザがログアウトします。アクションが実行される前に、確認メッセージが表示されます。

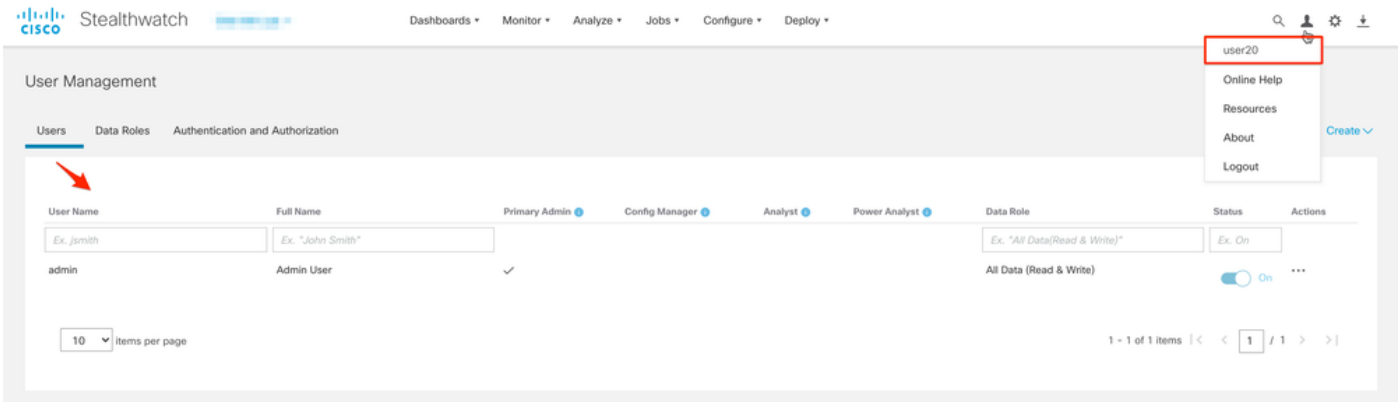


確認

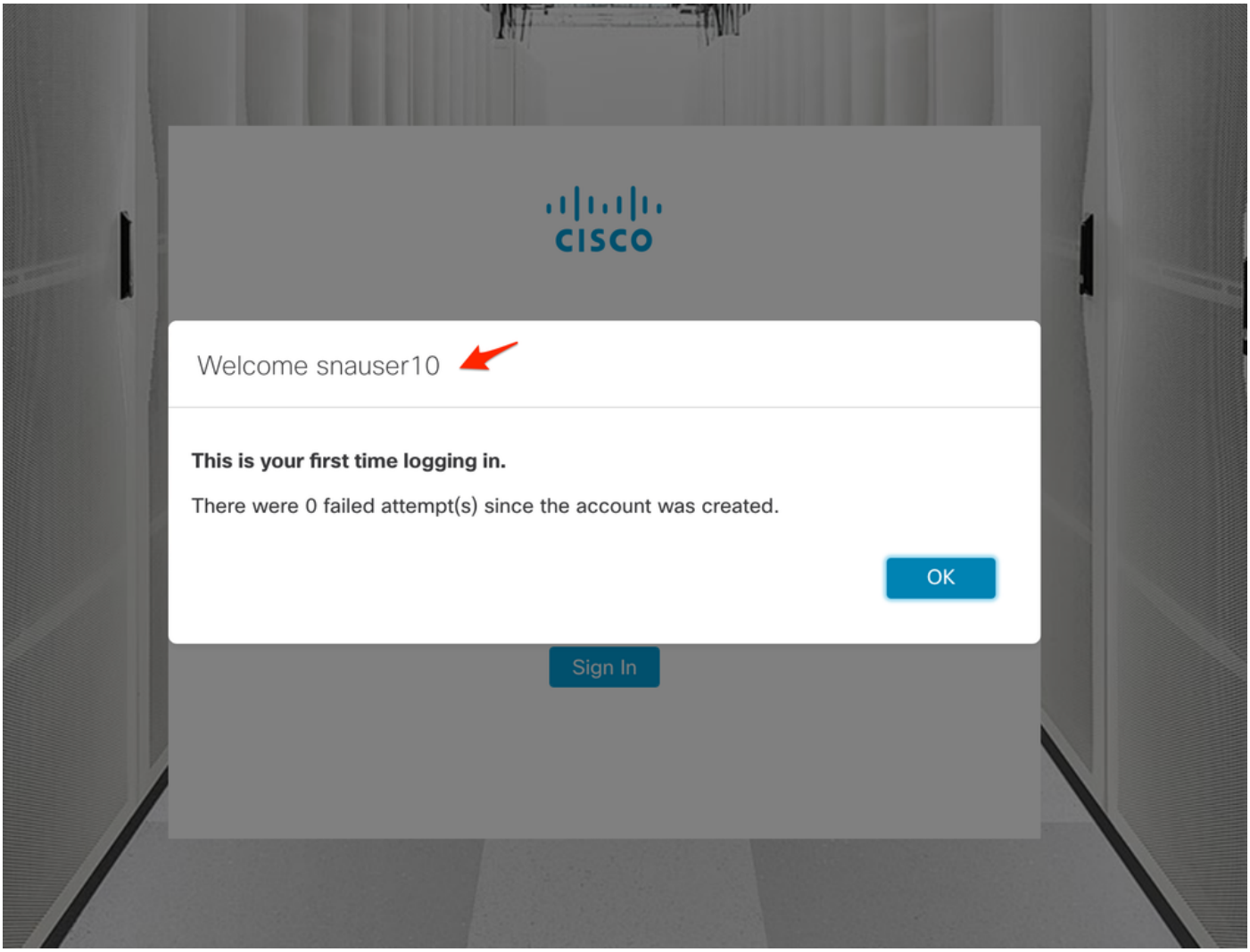
ユーザは、ADサーバで定義されたクレデンシャルを使用してログインできます。



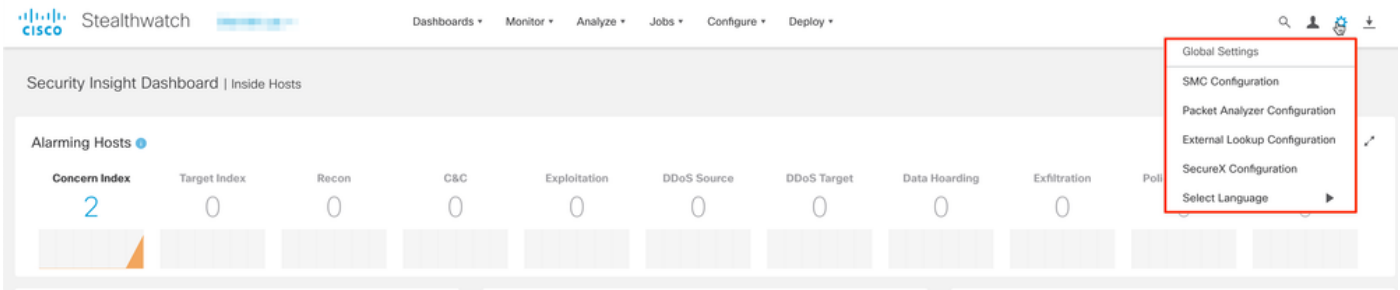
2番目の確認手順は、認可に関するものです。この例では、ユーザ「user20」がADサーバの*cisco-stealthwatch-master-admin*グループのメンバーに設定され、ユーザにプライマリ管理者権限があることを確認できます。ユーザがローカルユーザに定義されていないため、認可属性がADサーバから送信されたことを確認できます。



この例の「snauser10」では、他のユーザについても同じ検証が行われます。 ADサーバで設定されたクレデンシャルを使用して、認証の成功を確認できます。



認証の検証では、このユーザはプライマリ管理者グループに属していないため、一部の機能は使用できません。



トラブルシュート

認証サービスの設定を正常に保存できない場合は、次のことを確認します。

1. LDAPサーバの適切な証明書をマネージャの信頼ストアに追加しました。
2. 設定されたサーバーアドレスは、LDAPサーバ証明書のサブジェクト代替名(SAN)フィールドで指定されているとおりです。 [SAN]フィールドにIPv4アドレスだけが含まれている場合は、[Server Address]フィールドにIPv4アドレスを入力します。[SAN]フィールドにDNS名が含まれている場合は、[Server Address]フィールドにDNS名を入力します。[SAN]フィールドにDNSとIPv4の両方の値が含まれている場合は、リストされている最初の値を使用します。
3. ADドメインコントローラで指定された設定された[Bind User]フィールドと[Base Account]フ

ィールドが正しいです。

関連情報

その他のサポートについては、Cisco Technical Assistance Center(TAC)にお問い合わせください。有効なサポート契約が必要です。 各国のシスコ サポートの連絡先.