

Externe verificatie en autorisatie via LDAPS configureren voor beveiligde netwerkanalyse Manager-toegang

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Configureren](#)

[Stap A. Meld u aan bij de AD-domeincontroller en exporteert u het SSL-certificaat dat voor LDAP wordt gebruikt.](#)

[Stap B. Meld u aan bij SNA Manager om het certificaat van de LDAP-server en de basisketen toe te voegen.](#)

[Stap C. Voeg de LDAP-configuratie toe.](#)

[SNA versie 7.2 of hoger](#)

[SNA versie 7.1](#)

[Stap D. Configureer de instellingen voor de vergunning.](#)

[Lokale autorisatie](#)

[Afstandsvergunning via LDAP](#)

[Verifiëren](#)

[Problemen oplossen](#)

[Gerelateerde informatie](#)

Inleiding

In dit document wordt de basisconfiguratie beschreven van een Secure Network Analytics Manager (voorheen Stealthwatch Management Center) versie 7.1 of later om gebruik te maken van externe authenticatie en, met versie 7.2.1 of later, om gebruik te maken van externe autorisatie met LDAPS.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Cisco Secure Network Analytics (voorheen Stealthwatch)
- Algemeen gebruik van LDAP en SSL
- Algemeen Microsoft Active Directory-beheer

Gebruikte componenten

De informatie in dit document is gebaseerd op deze componenten:

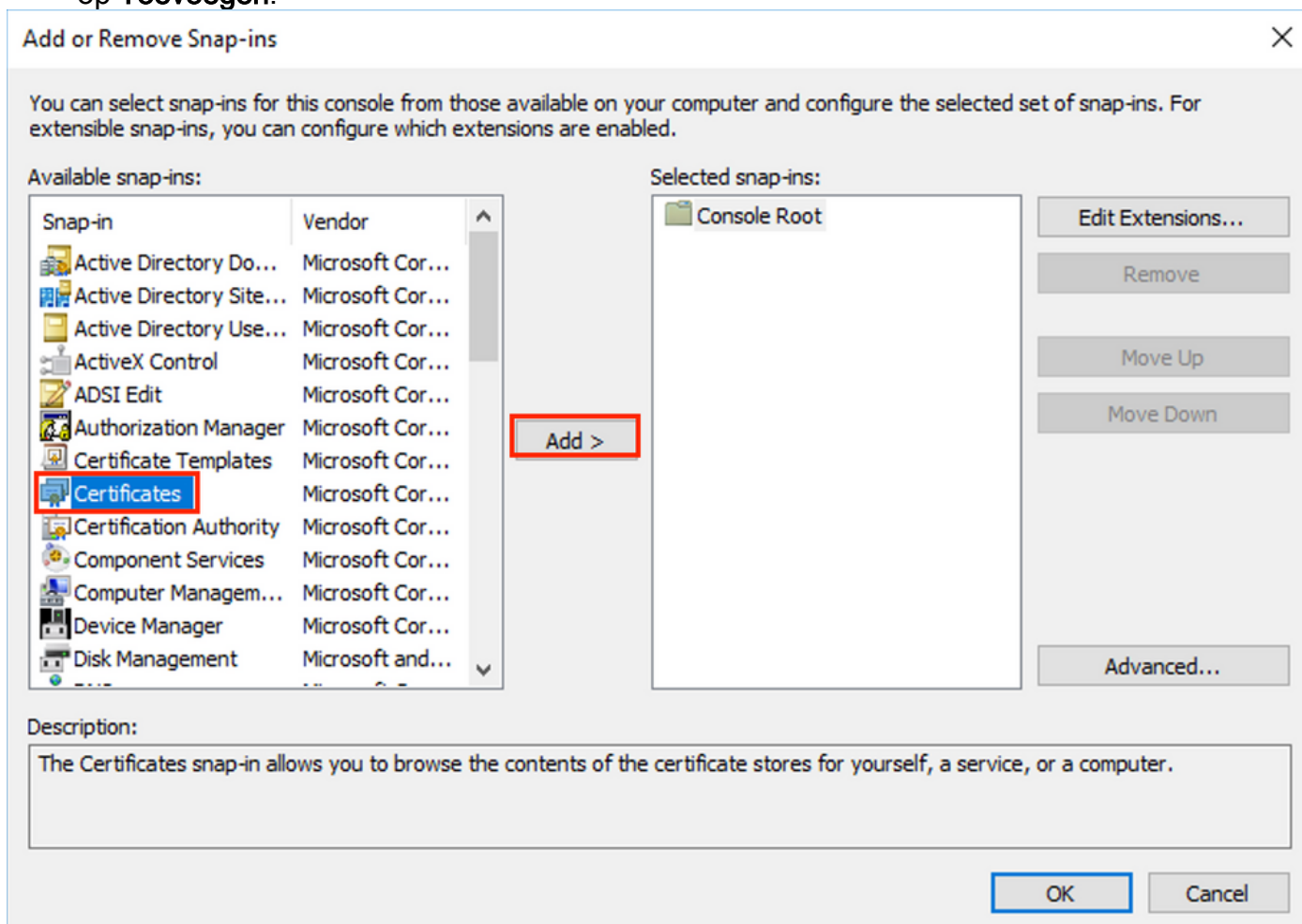
- Cisco Secure Network Analytics Manager (voorheen SMC) versie 7.3.2
- Windows Server 2016 ingesteld als Active Directory Domain Controller

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk levend is, zorg er dan voor dat u de mogelijke impact van om het even welke opdracht begrijpt.

Configureren

Stap A. Meld u aan bij de AD-domeincontroller en exporteert u het SSL-certificaat dat voor LDAP wordt gebruikt.

1. Selecteer voor Windows Server 2012 of selecteer **Run** in het menu Start en voer vervolgens **certlm.msc** in en ga verder met stap 8.
2. Voor oudere versies van Windows Server selecteert u **Run** in het menu Start en voer vervolgens **mmc** in.
3. Selecteer in het menu Bestand de optie **Magnetisch toevoegen/verwijderen**.
4. Selecteer in de lijst Beschikbare invoegtoepassingen de optie **Certificaten** en klik vervolgens op **Toevoegen**.

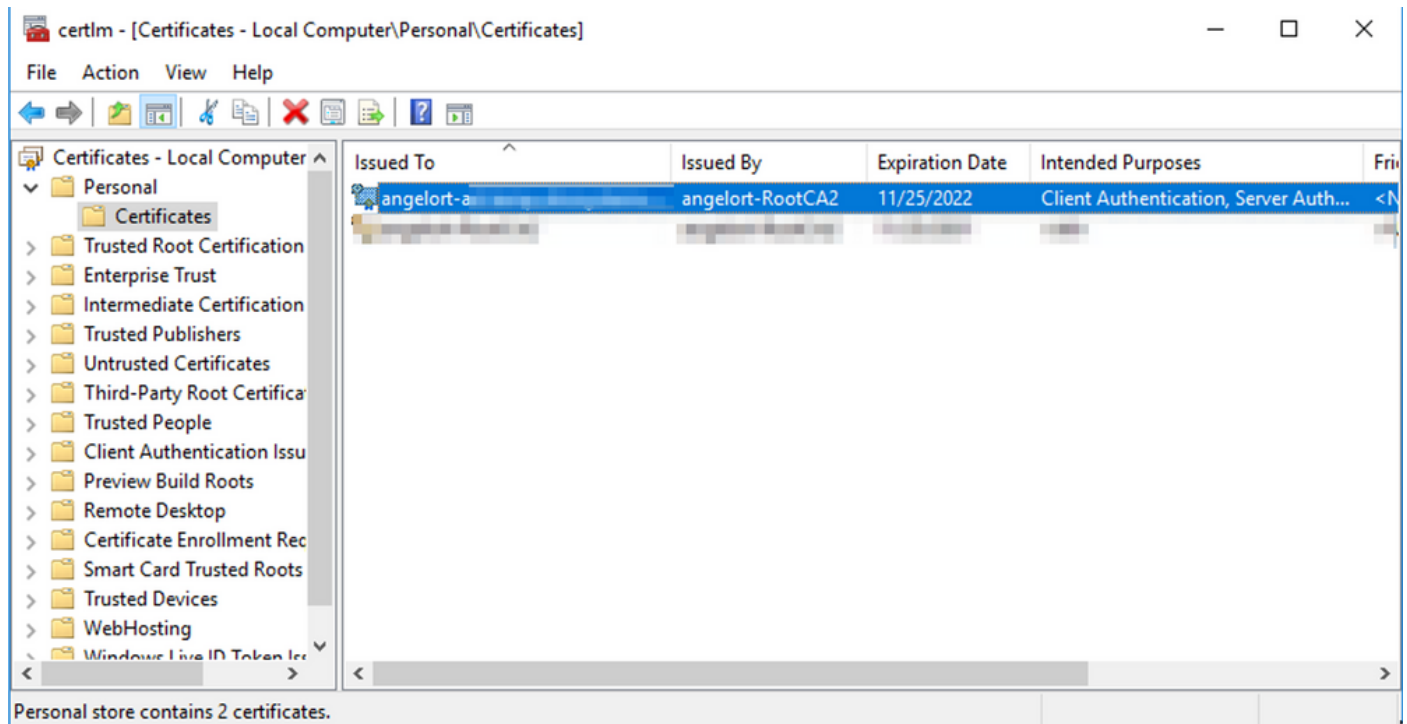


5. Selecteer in het venster **Certificaten** de optie **Computer-account** en selecteer vervolgens **Volgende**.

6. Laat de **lokale computer** geselecteerd zijn en selecteer **Voltooien**.

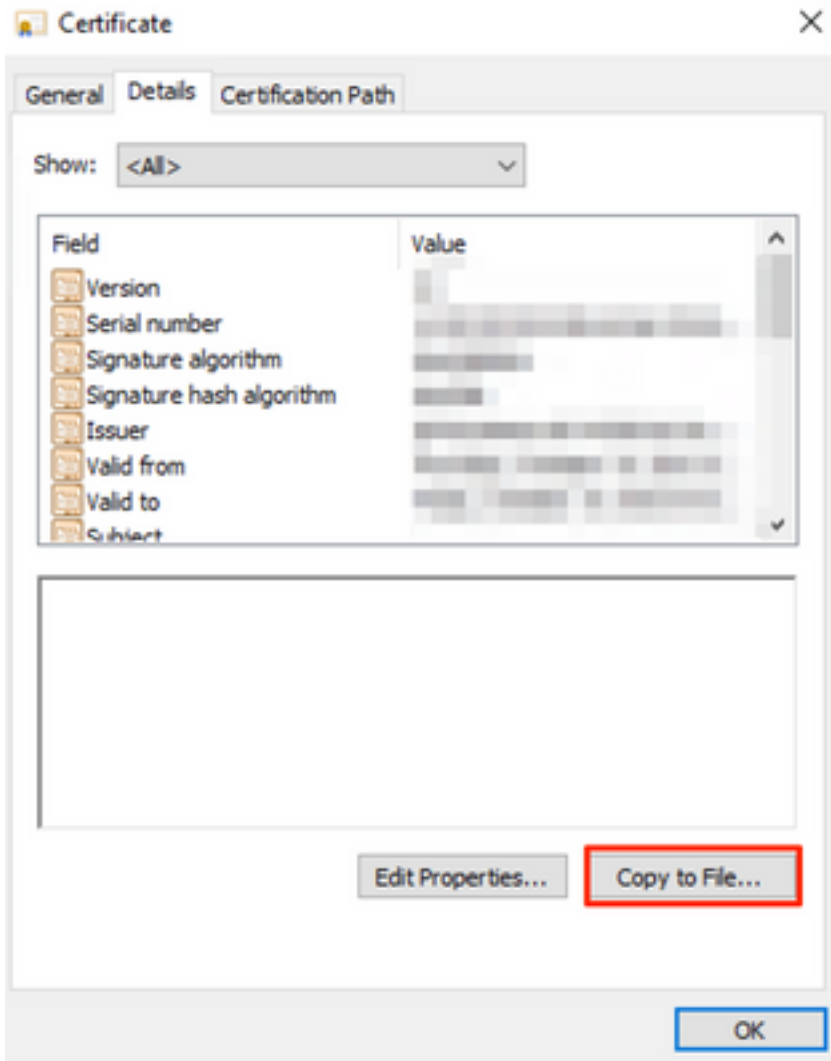
7. Selecteer **OK** in het venster **Magnetisch toevoegen of verwijderen**.

8. Navigatie naar **certificaten (lokale computer) > Persoonlijk > Certificaten**



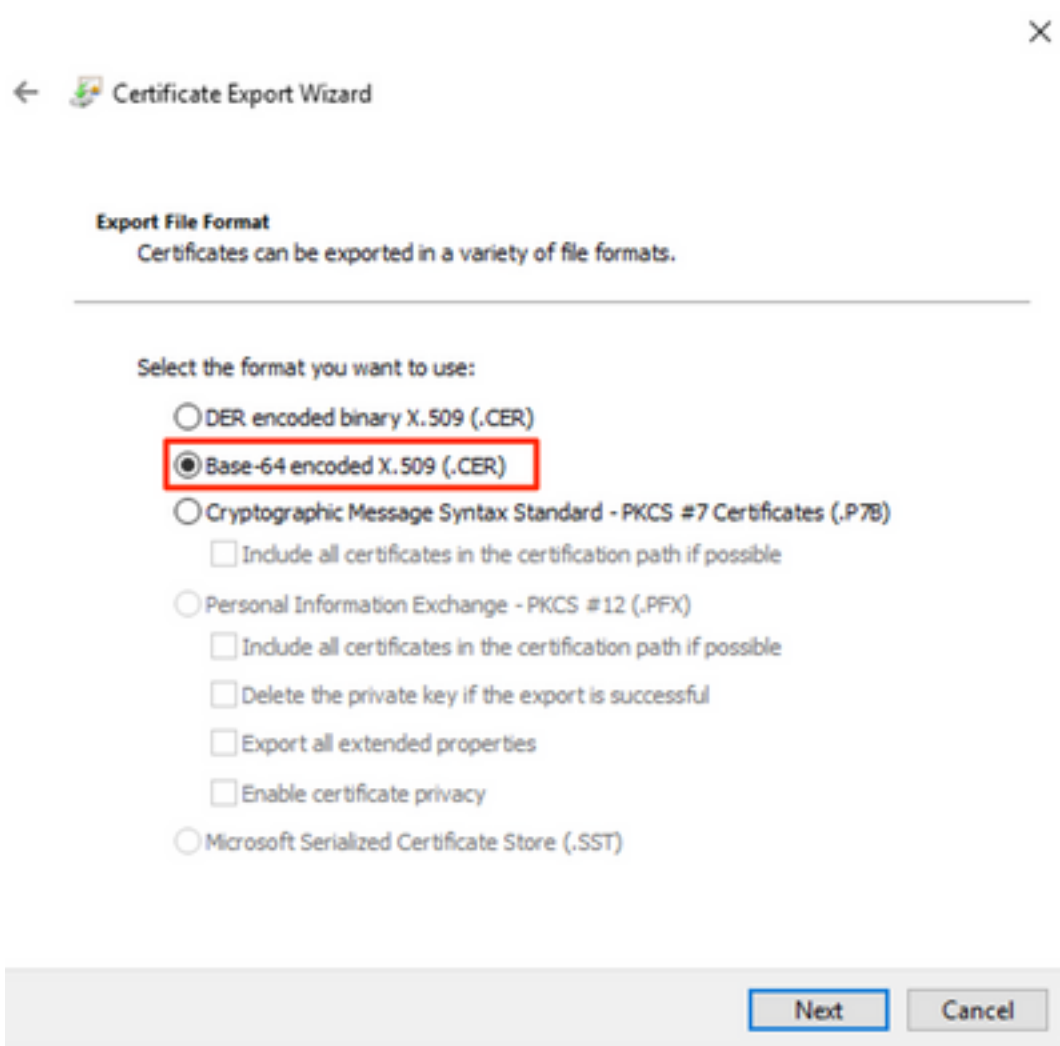
9. Selecteer en klik met de rechtermuisknop op het SSL-certificaat dat wordt gebruikt voor LGBPS-verificatie op uw domeincontroller en klik op **Openen**.

10. Navigeer naar het tabblad **Details** > klik op **Kopie naar bestand** > **Volgende**

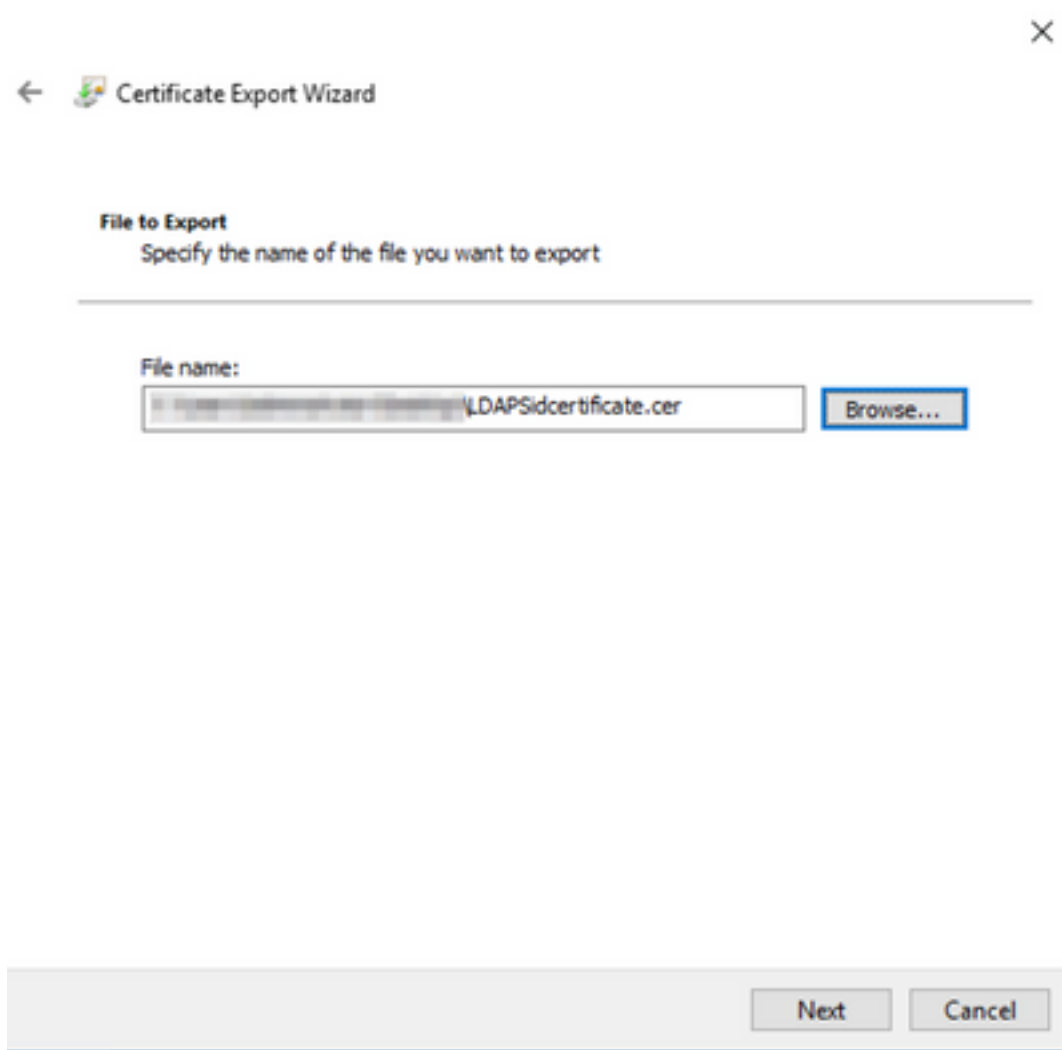


11. Zorg ervoor dat **Nee, geen privé-toets exporteren** is geselecteerd en klik op **Volgende**

12. Selecteer **Base-64 gecodeerde X.509-indeling** en klik op **Volgende**.



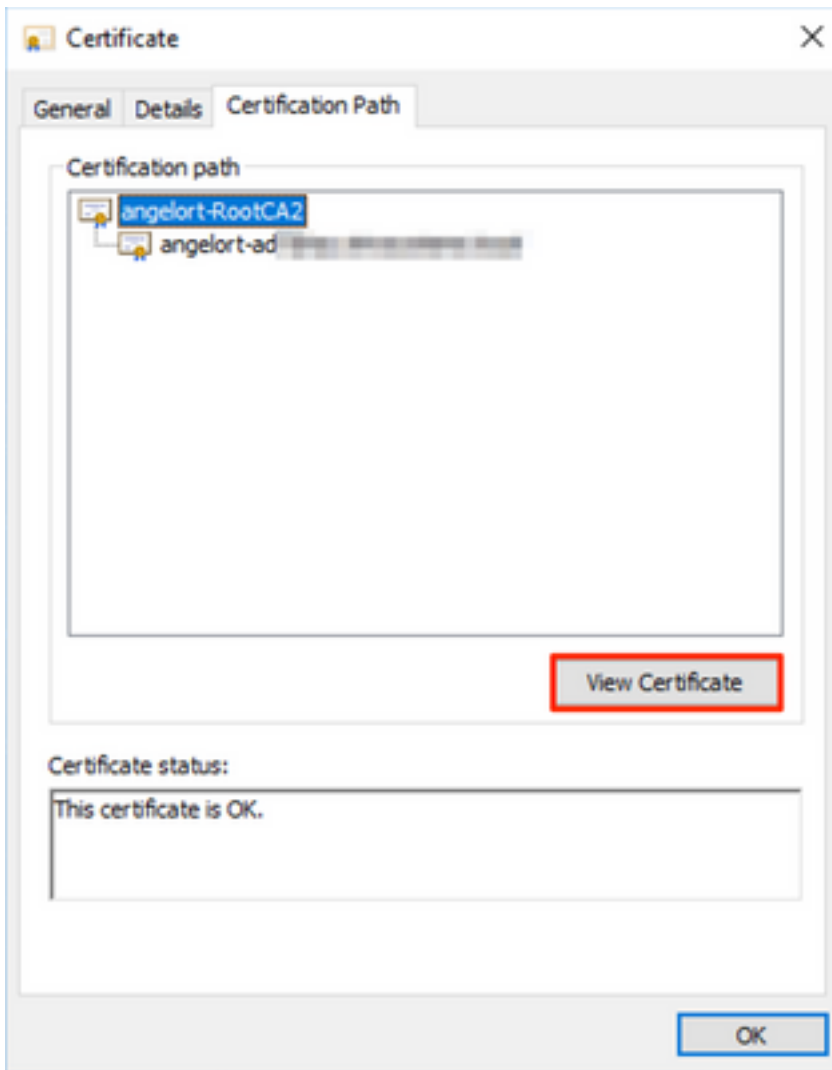
13. Selecteer een locatie waar u het certificaat op wilt slaan, geef het bestand een naam en klik op **Volgende**.



14. Klik op **Voltoeien**, dan krijgt u een 'De export is geslaagd'. bericht.

15. Ga terug naar het certificaat dat gebruikt wordt voor LDAPS en selecteer vervolgens het tabblad **certificeringspad**.

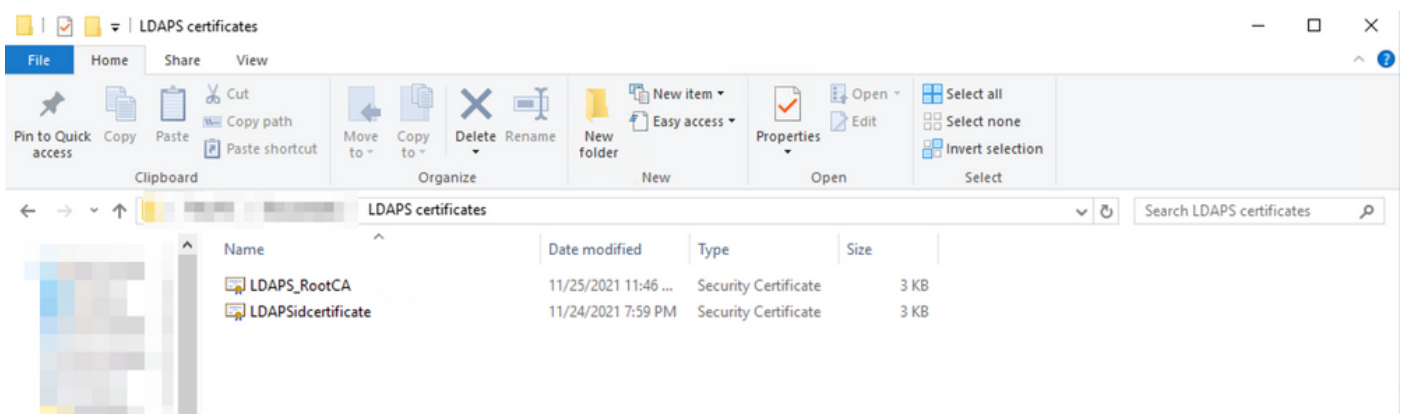
16. Selecteer de Root CA-emittent boven het certificeringspad en klik op **View certificaatdocument**.



17. Herhaal stappen 10-14 om het certificaat van de basiscode CA te exporteren dat het voor de validatie van de LDAPS gebruikte certificaat heeft ondertekend.

Opmerking: Uw plaatsing kan een multicast CA Hierarchy hebben, in welk geval u de zelfde procedure moet volgen om alle intermediaire certificaten in de trustketen uit te voeren.

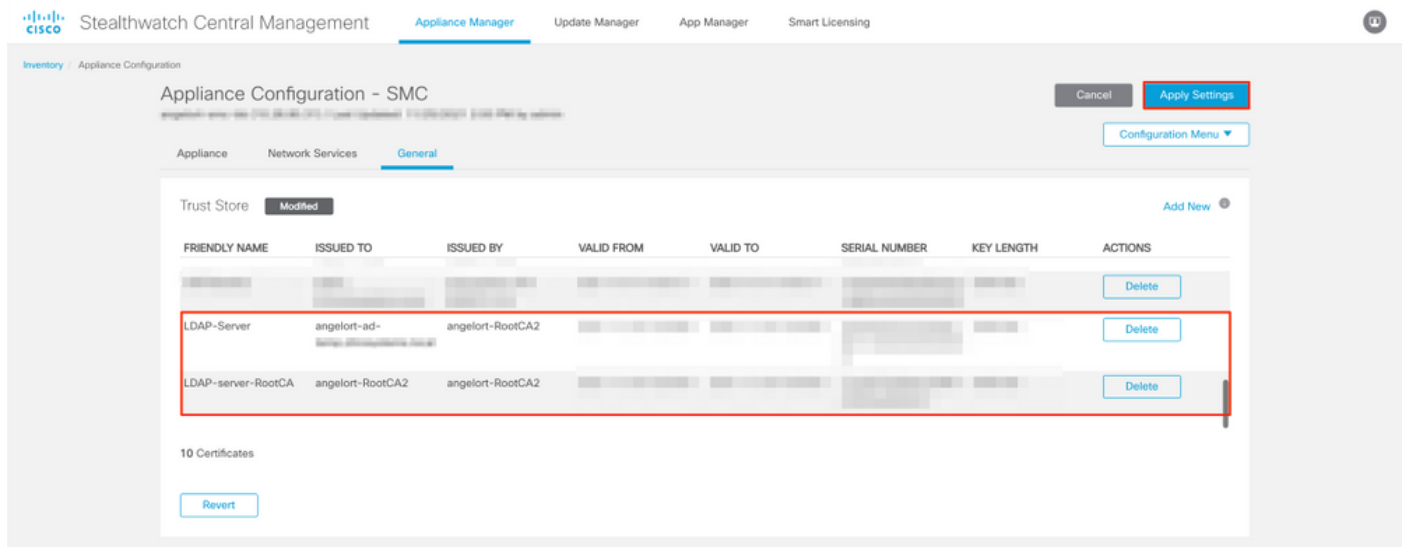
18. Zorg ervoor dat u, voordat u verdergaat, één certificatiebestand hebt voor de LDAPS-server en voor elke emittent in het certificeringspad: wortelcertificaat en tussentijdse certificaten (indien van toepassing).



Stap B. Meld u aan bij SNA Manager om het certificaat van de LDAP-server en de

basisketen toe te voegen.

1. Navigeer naar **Central Management** > inventaris.
2. Zoek het apparaat van SNA Manager en klik op **Handelingen** > **Toepassingsconfiguratie bewerken**.
3. Blader in het venster Application Configuration naar het menu **Configuration** > **Trust Store** > **Add New**.
4. Typ de vriendschappelijke naam, klik op **Bestand kiezen** en selecteer het certificaat van de LDAP server en klik op **Certificaat toevoegen**.
5. Herhaal de vorige stap om het CA-certificaat en de tussentijdse certificaten (indien van toepassing) aan de voet toe te voegen.
6. Controleer of de geüploade certificaten de juiste zijn en klik op **Instellingen toepassen**.

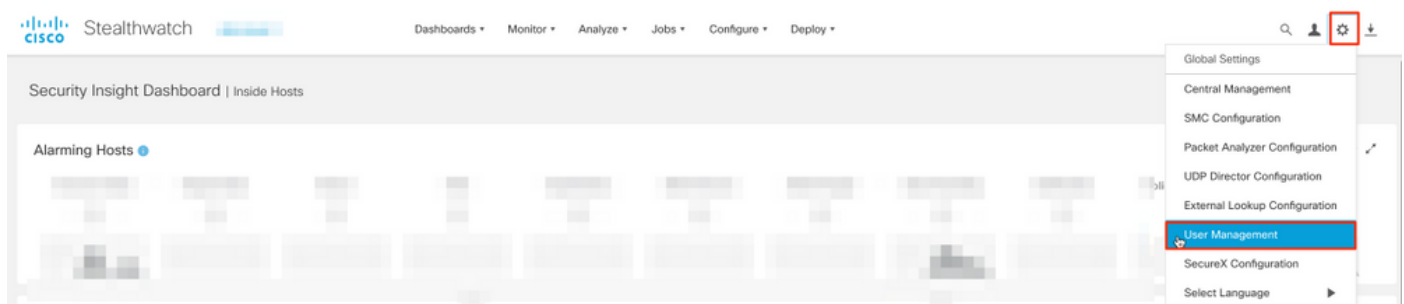


7. Wacht tot de wijzigingen worden toegepast en wacht tot de Manager-status **omhoog** is.

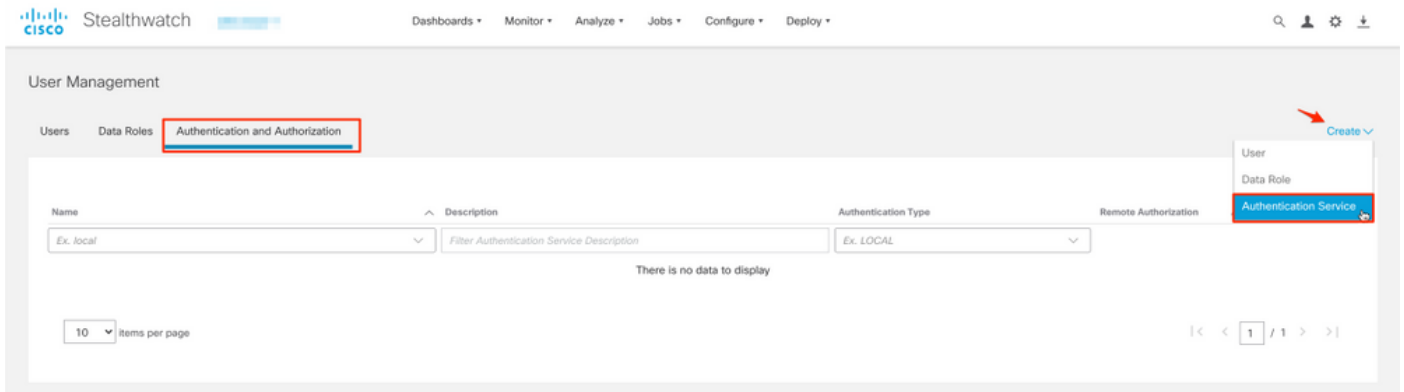
Stap C. Voeg de LDAP-configuratie toe.

SNA versie 7.2 of hoger

1. Open het hoofddashboard van Manager en navigeer naar **Global Settings** > **User Management**.



2. Selecteer in het venster Gebruikersbeheer het tabblad **Verificatie en autorisatie**.
3. Klik op **Maken** > **Verificatieservice**.



4. Selecteer in het vervolgkeuzemenu **Verificatieservice LDAP**.

5. Vul de gewenste velden in.

Veld

Friendly Name

Beschrijving

Serveradres

Port

Bind gebruiker

Opmerkingen

Voer een naam in voor de LDAPserver.

Voer een beschrijving in voor de LDAP server.

Voer de volledig gekwalificeerde domeinnaam in gespecificeerd in het veld Onderwerp Alternative Name (SAN) van het LDAP-servercertificaat.

- Als het SAN-veld alleen het IPv4-adres bevat voert u het IPv4-adres in het veld Adres server in.
- Als het SAN-veld de DNS-naam bevat, voert u de DNS-naam in het veld Adres server in.
- Als het SAN-veld zowel DNS- als IPv4-waarden bevat, gebruikt u de eerste vermelde waarde.

Geef de haven op die is aangewezen voor veilige LGO-communicatie (LDAP via TLS). De bekende poort voor LDAPS is 636.

Geef de gebruiker-ID op die gebruikt wordt om verbinding te maken met de LDAP-server.

Bijvoorbeeld: CN=admin, OU=Corporate Gebruikers, DC=voorbeeld, DC=com

Opmerking: Als u uw gebruikers aan een ingebouwde AD-container hebt toegevoegd (bijvoorbeeld "Gebruikers"), dan moet de bind DN van de eindgebruiker de canonische naam (CN) hebben ingesteld op de ingebouwde naam (bijvoorbeeld CN=gebruikersnaam, CN=Gebruikers, DC=domein, DC=com). Als gebruikers echter aan een nieuwe container toegevoegd, dan moet de Bind DN de organisatorische eenheid (OU) hebben ingesteld op de nieuwe containernaam (bijvoorbeeld CN=gebruikersnaam, OU=Corporate Gebruikers, DC=domein, DC=com).

Opmerking: Een bruikbare manier om de Bind DN van de gebruiker van de Bind te vinden is

de Actieve Map op een Server van Windows vragen die connectiviteit op de Actieve Server van de Map heeft. Om deze informatie te krijgen kunt u een Windows-opdrachtprompt openen met de opdrachtsyntaxis van **gebruiker dc=<geachte>, dc=<naam> -naam <gebruiker>** typen. Bijvoorbeeld: **Dc=voorbeeldgebruiker dc=voorbeeld, dc=com -name gebruiker1**. Het resultaat lijkt op "CN=user1,OU=Corporate Gebruikers, DC=voorbeeld, DC=com"

Wachtwoord

Voer het gebruikerswachtwoord in dat gebruikt wordt om verbinding te maken met de LDAP server.

Voer de opgegeven naam in (DN).

De DN is van toepassing op de tak van de folder waarin het zoeken naar gebruikers moet beginnen.

is vaak de top van folder boom (uw domein), maar kunt ook een subboom binnen de folder specificeren.

De eindgebruiker en de gebruikers die voor authenticatie in aanmerking komen, moeten van basisrekeningen kunnen profiteren.

Bijvoorbeeld: DC=voorbeeld, DC=com

Basisrekeningen

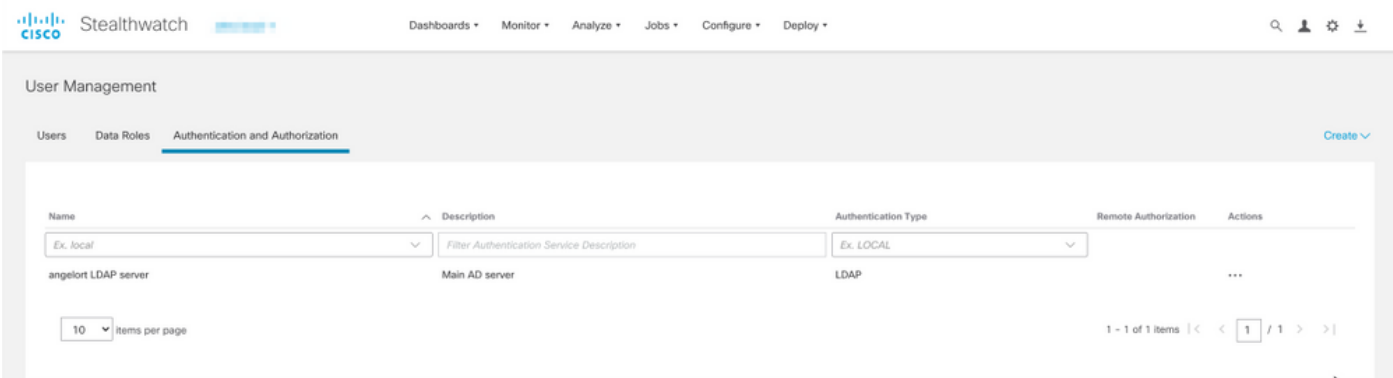
6. Klik op Opslaan.

The screenshot shows the Cisco Stealthwatch interface for configuring an LDAP authentication service. The page title is "User Management | Authentication Service". A warning message at the top states: "Add your SSL/TLS certificate to this appliance's Trust Store before you configure the LDAP Authentication service." The form includes the following fields:

- Friendly Name: angelort LDAP server
- Description: Main AD server
- Server Address: angelort-ad-10.10.10.10
- Certificate Revocation: Disabled
- Password: [Redacted]
- Authentication Service: LDAP
- Port: 636
- Bind User: CN=s...,OU=SNA,OU=Cisco,DC=zitros...,DC=local
- Base Accounts: DC=zitros...,DC=local
- Confirm Password: [Redacted]

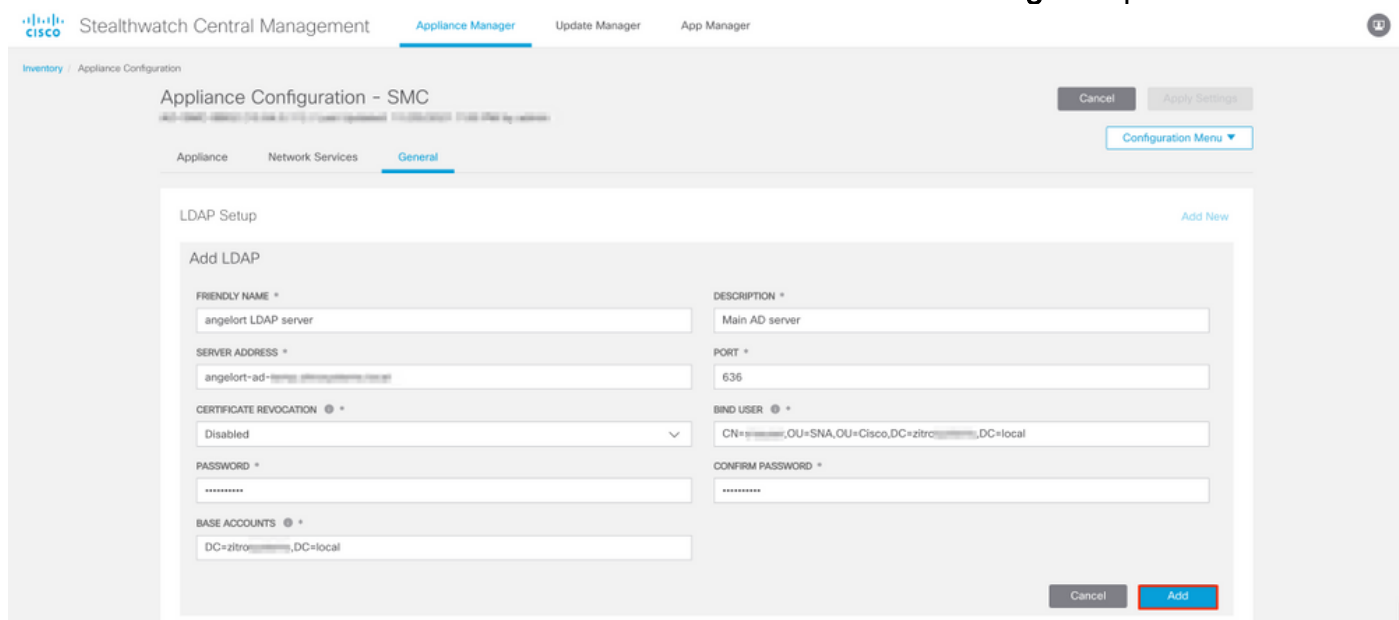
7. Als de instellingen die zijn ingevoerd en de certificaten die aan de trust store zijn toegevoegd, juist zijn, moet u een spandoek "U hebt uw wijzigingen met succes opgeslagen" krijgen.

8. De geconfigureerde server moet worden weergegeven onder **User Management > Verificatie en autorisatie**.



SNA versie 7.1

1. Navigeer naar **Central Management** > inventaris.
2. Pak de stekker uit het stopcontact en klik op **Handelingen** > **Toepassingsconfiguratie bewerken**.
3. Blader in het venster Application Configuration naar het menu **Configuration** > **LDAP Setup** > **Add New**.
4. Vul de vereiste velden in zoals beschreven in **SNA versie 7.2 of hoger** stap 5.



5. Klik op **Toevoegen**.
6. Klik op **Instellingen toepassen**.
7. Zodra de ingevoerde instellingen en de aan de trustwinkel toegevoegde certificaten juist zijn, worden de wijzigingen in het beheer toegepast en moet de status van het apparaat **Up** zijn.

Stap D. Configureer de instellingen voor de vergunning.

SNA ondersteunt zowel lokale als externe autorisatie via LDAP. Met deze configuratie worden de LDAP groepen van de AD Server in kaart gebracht aan ingebouwde of aangepaste SNA rollen.

De ondersteunde authenticatie- en autorisatiemethoden voor SNA via LDAP zijn:

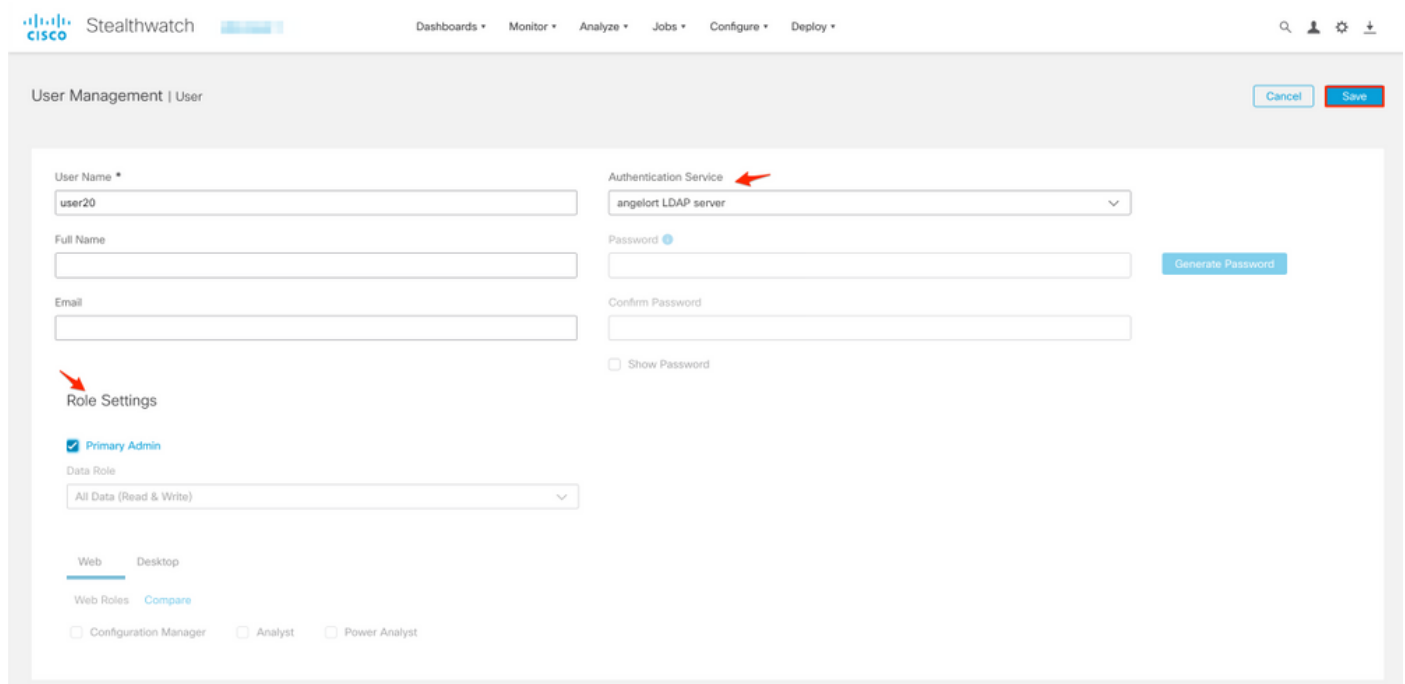
- Remote-verificatie en lokale autorisatie

- Remote-verificatie en -autorisatie (alleen ondersteund door SNA versie 7.2.1 of hoger)

Lokale autorisatie

In dit geval moeten de gebruikers en hun rollen lokaal worden gedefinieerd. Om dit te bereiken, gaat u als volgt te werk.

1. navigeren naar **gebruikersbeheer** opnieuw, klik op het **tabblad Gebruikers > Maken > Gebruiker**.
2. Definieer de gebruikersnaam voor authenticatie met de LDAP server en selecteer de geconfigureerde server in het vervolgkeuzemenu **Verificatieservice**.
3. Bepaal de rechten die de gebruiker over de Manager moet hebben zodra deze door de LDAP server is geauthentiseerd en klik op **Opslaan**.



The screenshot shows the 'User Management | User' configuration page in the Cisco Stealthwatch interface. The page includes a navigation bar with 'Stealthwatch' and various menu items like 'Dashboards', 'Monitor', 'Analyze', 'Jobs', 'Configure', and 'Deploy'. The main form is titled 'User Management | User' and has 'Cancel' and 'Save' buttons. The form fields are: 'User Name *' (containing 'user20'), 'Full Name', 'Email', 'Authentication Service' (a dropdown menu with 'angelort LDAP server' selected, indicated by a red arrow), 'Password' (with a 'Generate Password' button), 'Confirm Password', and 'Show Password' (checkbox). Below the form is the 'Role Settings' section, which has a red arrow pointing to it. It includes a checked 'Primary Admin' checkbox, a 'Data Role' dropdown menu (set to 'All Data (Read & Write)'), and a 'Web' tab. At the bottom, there are 'Web Roles' and 'Compare' options, with checkboxes for 'Configuration Manager', 'Analyst', and 'Power Analyst'.

Afstandsvergunning via LDAP

Verificatie en autorisatie op afstand via LDAP werd eerst ondersteund door Secure Network Analytics versie 7.2.1.

Opmerking: De afstandsbediening met LDAP wordt niet ondersteund in versie 7.1.

Het is relevant om op te merken dat als een gebruiker lokaal is gedefinieerd en ingeschakeld (in de Manager), de gebruiker op afstand is geauthentiseerd, maar lokaal is geautoriseerd. De gebruikersselectie verloopt als volgt:

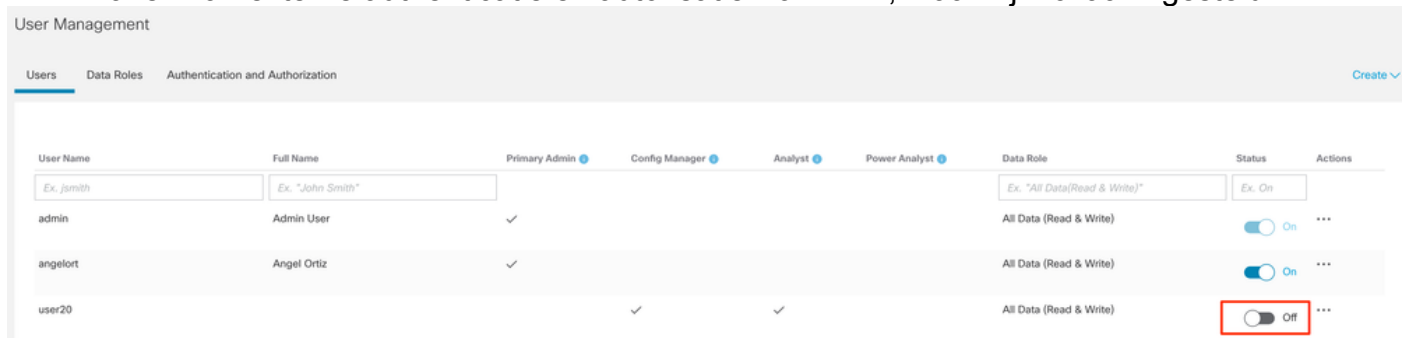
1. Zodra de aanmeldingsgegevens op de welkomspagina van de Manager zijn ingevoerd, zoekt de Manager een lokale gebruiker met de opgegeven naam.
2. Als een lokale gebruiker wordt gevonden en deze optie is ingeschakeld, wordt deze op afstand echt gemaakt (als verificatie op afstand via LDAP met lokale vergunning eerder is ingesteld) maar is deze op basis van de lokale instellingen geautoriseerd.

- Als een externe autorisatie is ingesteld en ingeschakeld en de gebruiker niet lokaal wordt gevonden (niet ingesteld of uitgeschakeld), worden zowel de verificatie als de autorisatie op afstand uitgevoerd.

Om deze reden zijn de stappen om externe verificatie met succes te configureren niet...

Stap D-1. Schakel de gebruikers uit die bedoeld zijn om een vergunning op afstand te gebruiken, maar die lokaal zijn gedefinieerd.

- Open het hoofddashboard van Manager en navigeer naar Global Settings > User Management.
- Schakel de gebruikers uit of verwijder (indien ze bestaan) die bedoeld zijn om gebruik te maken van externe authenticatie en autorisatie via LDAP, maar zijn lokaal ingesteld.



Stap D-2. Definieer cisco-stealthwatch-groepen in de Microsoft AD-server.

Voor externe verificatie en autorisatie via LDAP-gebruikers worden wachtwoorden en *cisco-stealthwatch*-groepen extern gedefinieerd in Microsoft Active Directory. De *cisco-stealthwatch*-groepen die moeten worden gedefinieerd in de AD-server zijn gerelateerd aan de verschillende rollen die SNA heeft, en moeten als volgt worden gedefinieerd.

SNA-rol

Primaire beheerder

Naam van de groep(en)

- cisco-stealthwatch-master-admin
- cisco-stealthwatch-all-data-read-and-schrijf
- Cisco Stealthwatch-all-data-only
- Cisco-Stealthwatch-OS-9<CUBE> (optioneel)

Gegevensrol

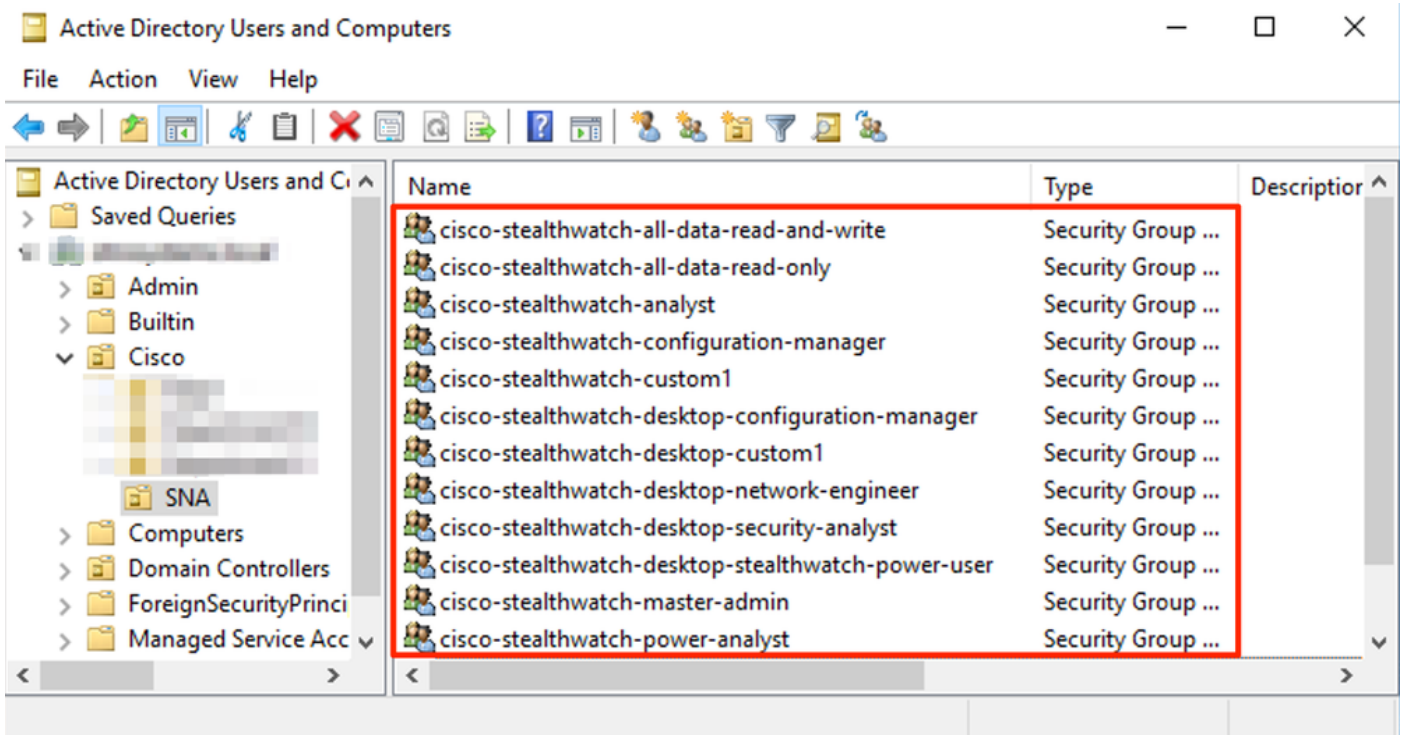
Opmerking: Zorg ervoor dat de groepen van aangepaste gegevensrol met "cisco-stealthwatch-" beginnen.

Functionele rol voor het web

- Cisco Stealthwatch-app voor configuratie
- analist voor cisco-stealthwatch-power
- Cisco-Stealthwatch-analist
- grootgebruiker van cisco-stealthwatch-desktop Stealthwatch-stroom
- Cisco Stealthwatch-desktop-configuratie-man
- cisco-stealthwatch-desktop-netwerk-ingenieur
- Cisco Stealthwatch-desktop-security analyst
- Cisco-Stealthwatch-desktop-<CUBE> (optioneel)

Functionele rol voor desktop

Opmerking: Zorg ervoor dat aangepaste des functionele rolgroepen beginnen met "cisco-

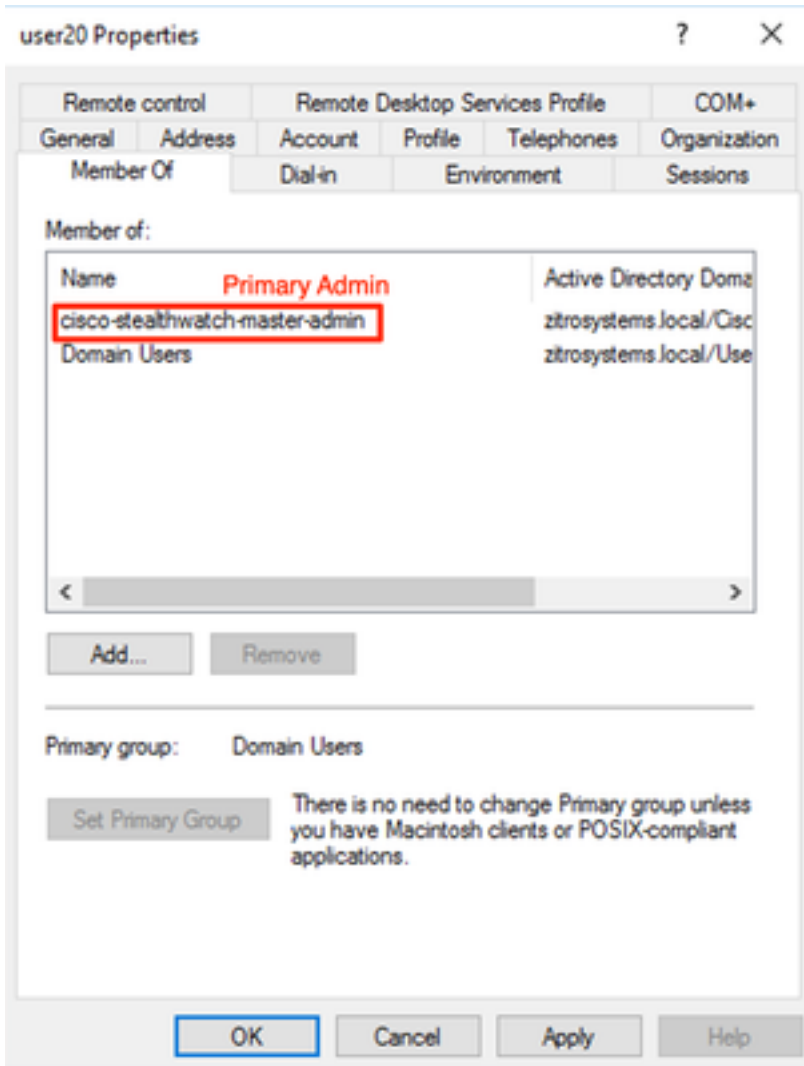


Opmerking: Zoals eerder beschreven, worden aangepaste groepen ondersteund voor "Data Rol" en "Desktop Functional Rol" zolang de groepsnaam wordt geprepend met de juiste string. Deze aangepaste rollen en groepen moeten in zowel de SNA Manager als de Active Directory server worden gedefinieerd. Als u bijvoorbeeld een aangepaste rol "custom1" in de SNA Manager definieert voor een desktop client rol, moet deze in kaart worden gebracht in `cisco-stealthwatch-desktop-aangepaste1` in Active Directory.

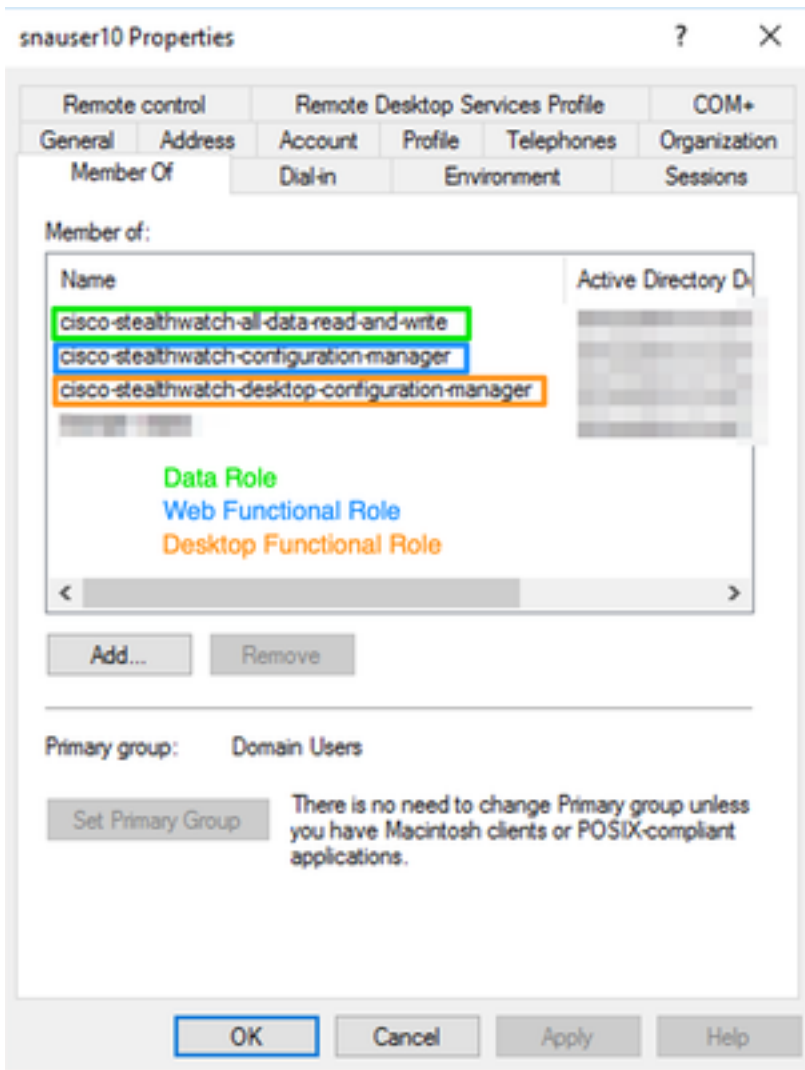
Stap D-3. Bepaal de Mappings van de LGO-machtigingsgroep voor de gebruikers.

Zodra de groepen *cisco-stealthwatch* in de AD server zijn gedefinieerd, kunnen we de gebruikers die bedoeld zijn om toegang tot de SNA Manager te hebben in kaart brengen naar de benodigde groepen. Dit moet als volgt gebeuren.

- Een **Primaire Admin**-gebruiker moet worden toegewezen aan de *cisco-stealthwatch-master-admin* groep en mag geen lid zijn van een andere *cisco-stealthwatch*-groep.



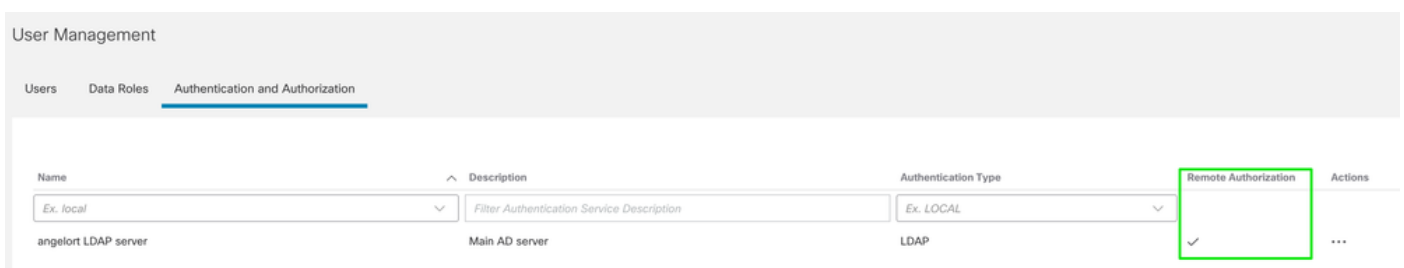
- Elke gebruiker, anders dan gebruikers van Primaire Admin, moet aan een groep van elke rol met de volgende voorwaarden worden toegewezen.
 1. **Gegevensrol:** De gebruiker moet aan **slechts één groep** zijn toegewezen.
 2. **Functionele rol van het web:** De gebruiker moet aan **ten minste één groep** zijn toegewezen.
 3. **Functionele rol voor desktop:** De gebruiker moet aan **ten minste één groep** zijn toegewezen.



Stap D-4. Schakel autorisatie op afstand via LDAP in op SNA Manager.

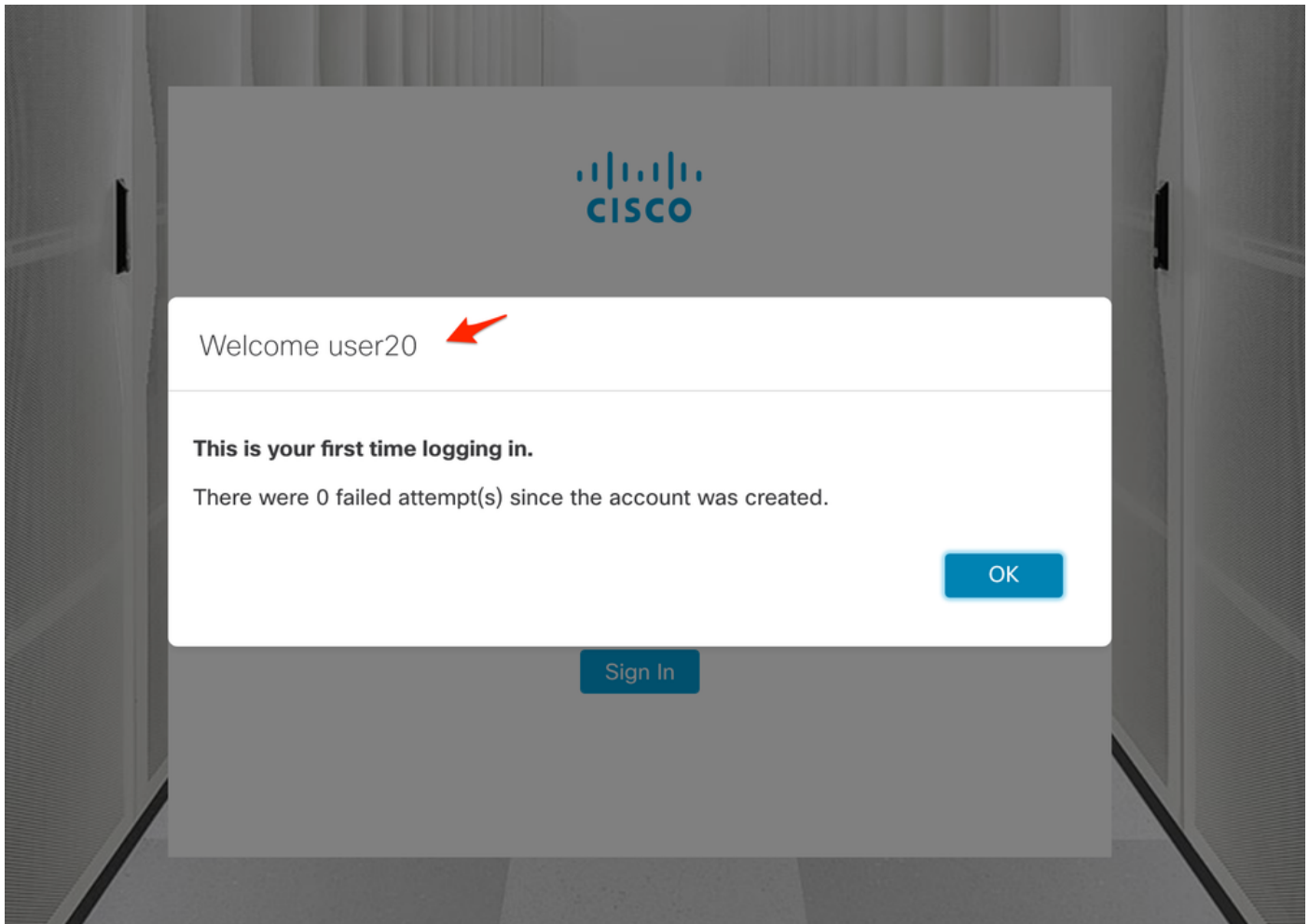
1. Open het hoofddashboard van Manager en navigeer naar **Global Settings > User Management**.
2. Selecteer in het venster **User Management** het tabblad **Verificatie en autorisatie**.
3. Zoek de LDAP-verificatiedienst die in **Stap C** is ingesteld.
4. Klik op **Handelingen > Toegang voor externe autorisatie**.

Opmerking: Er kan slechts één externe vergunningsdienst tegelijk worden gebruikt. Als een andere vergunningsdienst al in gebruik is, wordt deze automatisch uitgeschakeld en wordt de nieuwe uitgeschakeld. Alle gebruikers die een vergunning hadden gekregen voor de vorige externe dienst worden echter uitgelogd. Er verschijnt een bevestigingsbericht voordat er actie wordt ondernomen.

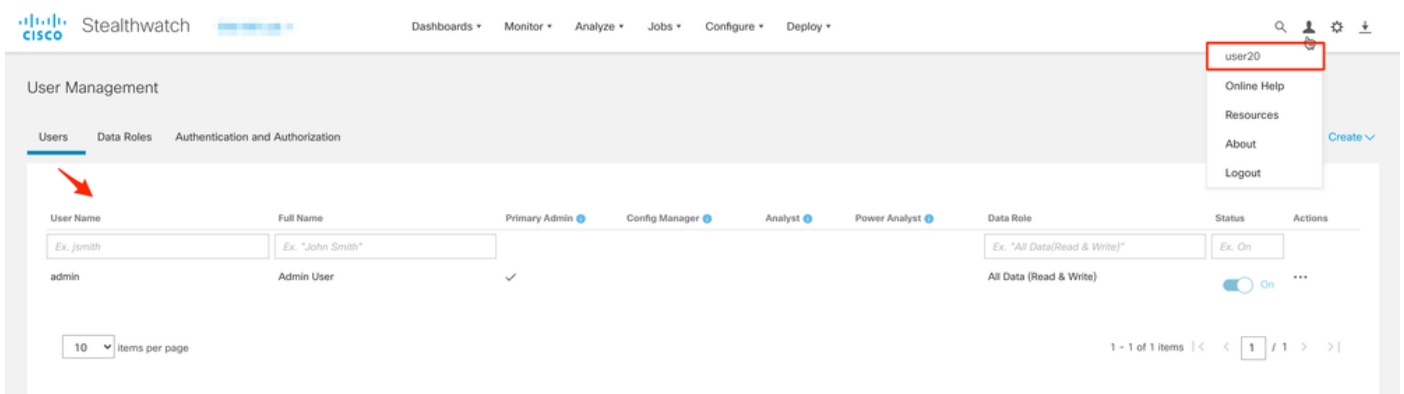


Verifiëren

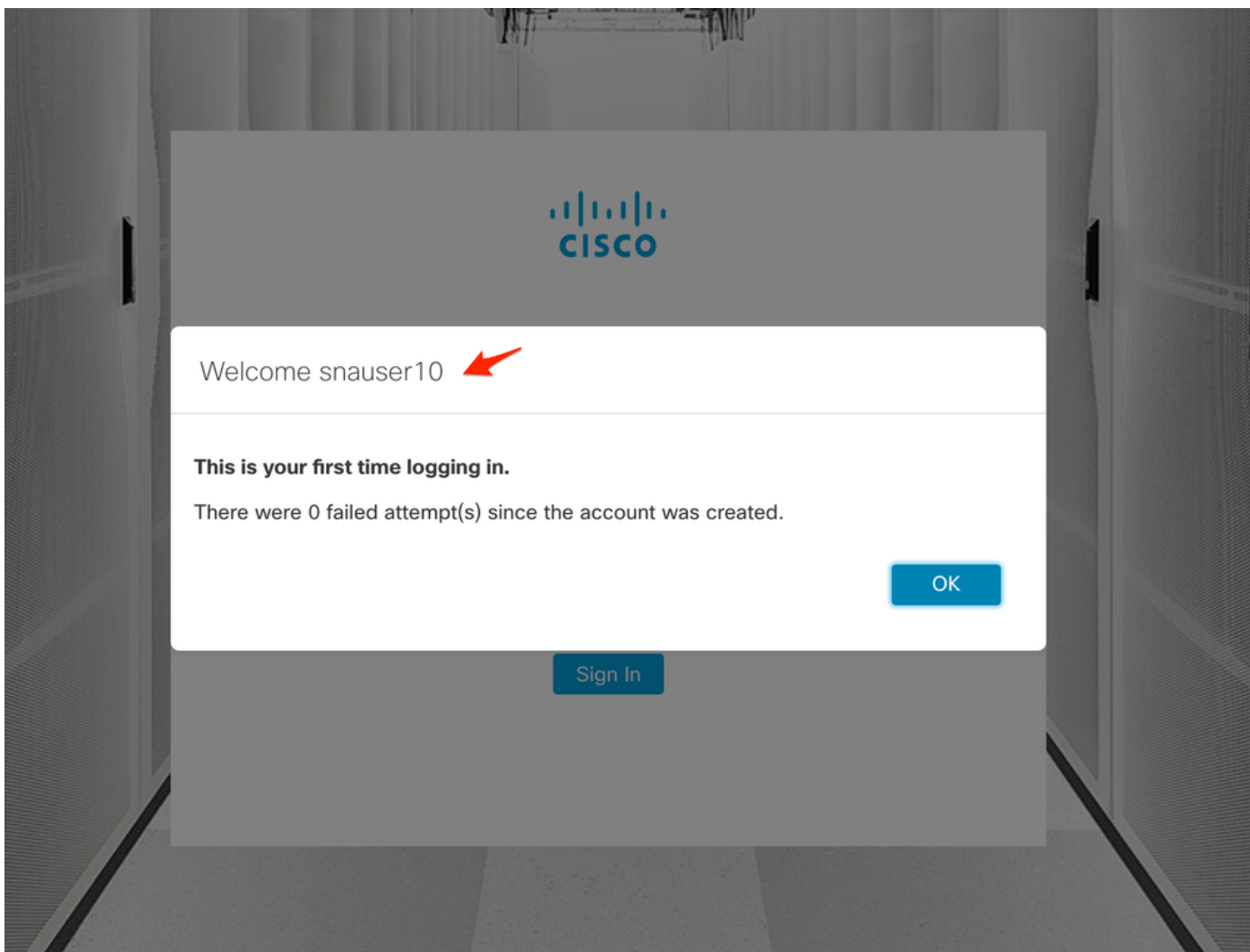
De gebruikers kunnen inloggen met de referenties die op de AD server zijn gedefinieerd.



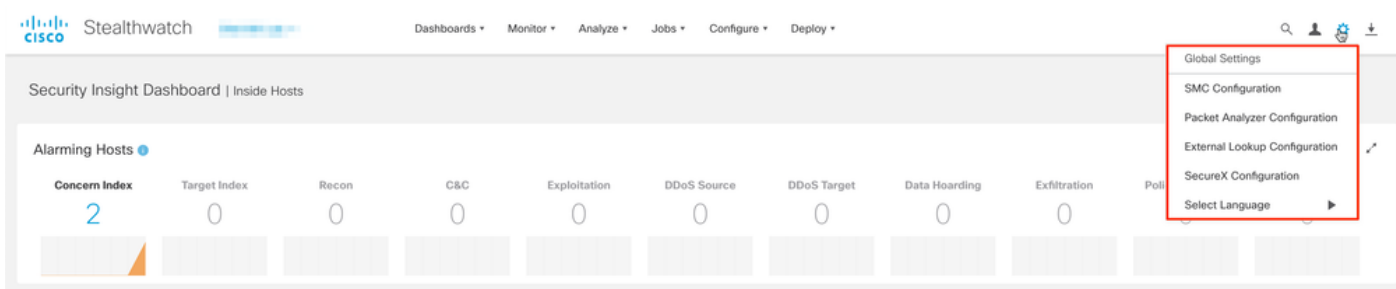
De tweede stap is de vergunning. In dit voorbeeld werd gebruiker "user20" gemaakt tot lid van de groep *cisco-stealthwatch-master-admin* in de AD-server en we kunnen bevestigen dat de gebruiker primaire Admin-toegangsrechten heeft. De gebruiker is niet gedefinieerd in de lokale gebruikers, zodat we kunnen bevestigen dat de autorisatie eigenschappen werden verzonden door de AD server.



Dezelfde verificatie wordt uitgevoerd voor de andere gebruiker in dit voorbeeld "snauser10". We kunnen succesvolle authenticatie bevestigen met de aanmeldingsgegevens die op de AD server zijn ingesteld.



Aangezien deze gebruiker niet tot de Primaire Admin-groep behoort, zijn bepaalde functies voor de verificatie van de autorisatie niet beschikbaar.



Problemen oplossen

Als de configuratie van de verificatieservice niet met succes kan worden opgeslagen, dient u te controleren of:

1. U hebt de juiste certificaten van de LDAP server toegevoegd aan de trustwinkel van de Manager.
2. Het geconfigureerd **serveradres** is zoals gespecificeerd in het veld Onderwerp Alternative Name (SAN) van het LDAP-servercertificaat. Als het SAN-veld alleen het IPv4-adres bevat, voert u het IPv4-adres in het veld Adres server in. Als het SAN-veld de DNS-naam bevat, voert u de DNS-naam in het veld Adres server in. Als het SAN-veld zowel DNS- als IPv4-

waarden bevat, gebruikt u de eerste vermelde waarde.

3. De geconfigureerde **Bind User**- en **Base Account**-velden zijn correct, zoals gespecificeerd door de AD Domain Controller.

Gerelateerde informatie

Neem voor extra assistentie contact op met Cisco Technical Assistance Center (TAC). Een geldig ondersteuningscontract is vereist: [Cisco's wereldwijde contactgegevens voor ondersteuning](#).