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**.

Add or Remove Snap-ins You can select snap-ins for t extensible snap-ins, you can	his console from the configure which e	nose xter	available on your computer and configure the selected s	et of snap-ins. For
Available snap-ins:			Selected snap-ins:	
Snap-in	Vendor	^	Console Root	Edit Extensions
Active Directory Do	Microsoft Cor Microsoft Cor			Remove
Active Directory Use	Microsoft Cor Microsoft Cor			Move Up
ADSI Edit	Microsoft Cor Microsoft Cor		Add >	Move Down
	Microsoft Cor Microsoft Cor			
Component Services	Microsoft Cor Microsoft Cor			
E Device Manager	Microsoft Cor			
T Disk Management	Microsoft and	¥		Advanced
Description: The Certificates snap-in allo	ows you to browse	the	contents of the certificate stores for yourself, a service	, or a computer.
				OK Cancel

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

藩 certlm - [Certificates - Local Cor	nputer\Personal\Certificates]			-		\times
File Action View Help						
🗢 🔿 🙍 📅 🐇 🖪 🗙 🛙	1 🔒 🛛 🖬					
Certificates - Local Computer 🔨	Issued To	Issued By	Expiration Date	Intended Purposes		Frie
Personal	🙀 angelort-a	angelort-RootCA2	11/25/2022	Client Authentication	, Server Auth.	<n< td=""></n<>
Certificates Trusted Root Certification	Second Se	approximation (1.000			
> 📔 Enterprise Trust						
> 🦳 Intermediate Certification						
> Trusted Publishers						
> Intrusted Certificates						
> intro-Party Root Certifica						
> Invited People						
> Client Authentication Issu						
> Preview Build Roots						
> 🦳 Remote Desktop						
> 🧮 Certificate Enrollment Rec						
> Construction Series Serie						
> Trusted Devices						
> 📔 WebHosting						
Windows Live ID Token Ise				_		
. ,						/
Personal store contains 2 certificates.						

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

💼 Certificate

General	Details	Certification	Path	
Show:	<all></all>		~	
Field Ser Sig Sig Sig Val	rsion nature al nature ha uer id from id to	er gorithm ash algorithm	Value	~
			Edit Properties	Copy to File
				ОК

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.

←	£.	Certificate	Export	Wizard
---	----	-------------	--------	--------

Export File Format

Certificates can be exported in a variety of file formats.

Base-64 encoded X.509 (.CER)	
Cryptographic Message Syntax Standard - PKCS	#7 Certificates (.P78)
Include all certificates in the certification path	if possible
Personal Information Exchange - PKCS #12 (.PFX	0
Include all certificates in the certification path	if possible
Delete the private key if the export is success	sful
Export all extended properties	
Enable certificate privacy	
Microsoft Serialized Certificate Store (.SST)	

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

Specify the na	ame of the file yo	ou want to exp	ort		
File name:					
1.000		LDAPSidcer	rtificate.cer	E	Browse

14. Klik op Voltooien, 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.

Certificate	\times
General Details Certification Path	
Certification path	
View Certificate Certificate status:	
This certificate is OK.	
OK	

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).

- 🖓 📙 🗸	LDAPS certificates						- 0	×
File Home	Share View							^ ?
Pin to Quick Copy access	Paste Paste shortcut	Move Copy to * Cot Delete Rename	New item • New folder	Properties	Select all Select none			
(lipboard	Organize	New	Open	Select			
$\leftrightarrow \rightarrow \cdot \uparrow$	a terret a terretari	LDAPS certificates				~ Ō	Search LDAPS certificates	P
	^ Name	^ Di	ate modified Type	Size				
1000	LDAPS_Root	tCA 11	/25/2021 11:46 Security	y Certificate 3	KB			
	LDAPSidcer	tificate 11	/24/2021 7:59 PM Security	y Certificate 3	KB			

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.

cisco Stealthwa	itch Central Mana	igement App	iance Manager	Update Manager Ap	op Manager Smart	Licensing		
ventory / Appliance Configur	Appliance Config Appliance Networ	guration - SMC * Services General	000 100 Persona					Cancel Apply Settings Configuration Menu V
	Trust Store Mod	hed						Add New 🔎
	FRIENDLY NAME	ISSUED TO	ISSUED BY	VALID FROM	VALID TO	SERIAL NUMBER	KEY LENGTH	ACTIONS
	-	The second	-					Delete
	LDAP-Server	angelort-ad-	angelort-RootCA2			-		Delete
	LDAP-server-RootCA	angelort-RootCA2	angelort-RootCA2			10000		Delete
	10 Certificates							
	Revert							

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.

cisco Stealthwatch	Dashboards * Monitor * Analyze * Jobs * Configure *	Deploy -	۹ 💵 🌣 ±
			Global Settings
Security Insight Dashboard Inside Hosts			Central Management
			SMC Configuration
Alarming Hosts 💿			Packet Analyzer Configuration
			UDP Director Configuration
			External Lookup Configuration
territory continue continue		and the second se	User Management
8.4			SecureX Configuration
			Select Language

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

cisco	Stealthwatch	Dashboards	Monitor •	Analyze *	Jobs *	Configure *	Deploy *				९ 💶 🌣 ±
User	Management										
Users	Data Roles Authentication and Authorization										Create
											User
											Data Role
Nar	ne	∧ Descrip	otion					Authentication Type		Remote Authorization	Authentication Service
Ex	. local	✓ Filter	Authentication Se	rvice Descriptic	va.			Ex. LOGAL	\sim		
					There is no	data to display					
	10										E LUX X
	10 ttems per page									14 4	1 /1 2 21

4. Selecteer in het vervolgkeuzemenu Verificatieservice LDAP.

5. Vul de gewenste velden in.

Veld	Opmerkingen
Friendly Name	Voer een naam in voor de LDAPserver.
Beschrijving	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 beva
Serveradres	voert u het IPv4-adres in het veld Adres serv
	 Als het SAN-veld de DNS-naam bevat, voert DNS-naam in het veld Adres server in. Als het SAN-veld zowel DNS- als IPv4-waard bevat, gebruikt u de eerste vermelde waarde Geef de haven op die is aangewezen voor veilige
Port	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 Gebruik DC=voorbeeld, DC=com
Bind gebruiker	Opmerking: Als u uw gebruikers aan een ingebouwde AD-container hebt toegevoegd (bijvoorbeeld "Gebruikers"), dan moet de bir DN van de eindgebruiker de canonische naa (CN) hebben ingesteld op de ingebouwde m (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 inge op de nieuwe containernaam (bijvoorbeeld CN=gebruikersnaam, OU=Corporate Gebrui DC=domein, DC=com).

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

	de Actieve Map op een Server van Windows vragen die connectiviteit op de Actieve Serve van de Map heeft. Om deze informatie te krij kunt u een Windows-opdrachtprompt opener de opdrachtsyntaxis van gebruiker dc= <geachte>, dc=<naam> -naam <gebruiker dc=voorbeeld; Dc=voorbeeldgebruiker dc=voorbeeld, dc=com -name gebruiker1. H resultaat lijkt op "CN=user1,OU=Corporate Gebruikers, DC=voorbeeld, DC=com"</gebruiker </naam></geachte>
Wachtwoord	Voer het gebruikerswachtwoord in dat gebruikt wo 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 beginne
Basisrekeningen	is vaak de top van folder boom (uw domein), maa kunt ook een subboom binnen de folder specifice De eindgebruiker en de gebruikers die voor authenticatie in aanmerking komen, moeten van basisrekeningen kunnen profiteren. Bijvoorbeeld: DC=voorbeeld, DC=com

6. Klik op **Opslaan**.

Dashboards • Monitor • Analyze • Jobs •	Configure * Deploy * Q 🛓 🌣 🛨
Add your SSL/TLS certificate to this appliance's Trust Store before you configure the LDAP Authentication service.	
User Management Authentication Service	Cancel Save
* = Required	
Friendly Name *	Authentication Service
angelort LDAP server	LDAP V
Description *	Port *
Main AD server	636
Server Address 0 *	Bind User 6 *
angelort-ad-	CN=s ,OU=SNA,OU=Cisco,DC=zitros ,DC=local
Certificate Revocation 9 *	Base Accounts 0 *
Disabled	DC=zitro: ,DC=local
Daseword *	Confirm Dassuared *

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**.

cisco Stealthwatch	Dashboards • Monitor • Analyze • Jobs • Configure • Deploy •		9 ք 🌣 🛨
User Management			
Users Data Roles Authentication and Authorization			Create ~
Name	∧ Description	Authentication Type	Remote Authorization Actions
Ex. local	Filter Authentication Service Description	Ex. LOCAL V	
angelort LDAP server	Main AD server	LDAP	
10 v Items per page			1 - 1 of 1 items < _ < _ 1 / 1 > _ >

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.

cisco Stealthwatch Central Management Appliance Manager Update Manager	App Manager)
Inventory / Appliance Configuration - SMC Appliance Network Services General	Cancel Apply Settings Configuration Menu 💌	
LDAP Setup	Add New	
Add LDAP FRENDLY NAME * angelort LDAP server server ADDRESS * angelort-ad- CERTIFICATE REVOCATION • * Disabled	DESCRIPTION * Main AD server PORT * 636 BIND USER @ * CN==OU=SNA,OU=Cisco,DC=zitroDC=local CONFIRM PASSWORD *	
BASE ACCOUNTS * DC=zitro DC=local	Cancel Add	

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. Defineer 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**.

Isco Stealthwatch Dashboards • Monitor • Ar	alyze * Jobs * Configure * Deploy *	Q 🛓 🌣 🛨
User Management User		Cancel
User Name *	Authentication Service	
Full Name	Password	
Email	Confirm Password	Generate Password
	Show Password	
Role Settings		
Primary Admin Data Role		
All Data (Read & Write) V		
Web Desktop		
Web Roles Compare Configuration Manager Analyst 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 welkomstpagina 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.

3. 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.

- 1. Open het hoofddashboard van Manager en navigeer naar Global Settings > User Management.
- 2. 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.

User	Management
------	------------

~

Users Data Roles Authentication and	I Authorization							Create ↓
User Name	Full Name	Primary Admin 😑	Config Manager 😑	Analyst 😑	Power Analyst 🌖	Data Role	Status	Actions
Ex, jsmith	Ex. "John Smith"					Ex. "All Data(Read & Write)"	Ex. On	
admin	Admin User	~				All Data (Read & Write)	C On	
angelort	Angel Ortiz	~				All Data (Read & Write)	On	
user20			~	~		All Data (Read & Write)	Off Off	

Stap D-2. Defineer 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-roi	Naam van de groep(en)
Primaire beheerder	cisco-stealthwatch-master-admincisco-stealthwatch-all-data-read-and-schrijf
	 Cisco Stealthwatch-all-data-only
	 Cisco-Stealthwatch-OS-9<cube> (optioneel</cube>
Gegevensrol	Opmerking: Zorg ervoor dat de groepen van aangepaste gegevensrol met "cisco-stealthwatch-" beginnen.
Functionele rol voor het web	Cisco Stealthwatch-app voor configuratieanalist voor cisco-stealthwatch-power
	 Cisco-Stealthwatch-analist grootgebruiker van cisco-stealthwatch-deskto Stealthwatch-stroom
	 Cisco Stealthwatch-desktop-configuratie-mar
	 cisco-stealthwatch-desktop-netwerk-ingenieu
Functionele rol voor desktop	 Cisco Stealthwatch-desktop-security analist
	 Cisco-Stealthwatch-desktop-<cube> (option</cube>
	Opmerking: Zorg ervoor dat aangepaste des functionele rolgroepen beginnen met "cisco-

...

stealthwatch-desktop-desktop".

Active Directory Users and Complexity	puters	_	
File Action View Help			
🗢 🔿 🙋 📷 🖌 📋 🗙 🛛] @ 🕞 🛛 📅 🗏 🔽 🛅 🍸 🗾 🍇		
Active Directory Users and C	Name	Туре	Descriptior ^
> 🧮 Saved Queries	acisco-stealthwatch-all-data-read-and-write	Security Group	
Admin	acisco-stealthwatch-all-data-read-only	Security Group	
> Admin	acisco-stealthwatch-analyst	Security Group	
	acisco-stealthwatch-configuration-manager	Security Group	
CISCO	acisco-stealthwatch-custom1	Security Group	
and the second se	🂐 cisco-stealthwatch-desktop-configuration-manager	Security Group	
	acisco-stealthwatch-desktop-custom1	Security Group	
SNA	acisco-stealthwatch-desktop-network-engineer	Security Group	
> 🛗 Computers	🂐 cisco-stealthwatch-desktop-security-analyst	Security Group	
> 📓 Domain Controllers	acisco-stealthwatch-desktop-stealthwatch-power-user	Security Group	
> 📔 ForeignSecurityPrinci	acisco-stealthwatch-master-admin	Security Group	
> 🚞 Managed Service Acc 🗸	acisco-stealthwatch-power-analyst	Security Group	~
< >	<		>

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 Mappingen 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-masteradmin* groep en **mag geen lid zijn van een andere** *cisco-stealthwatch*-groep.

user20 Properties				?	×		
Remote control General Address Member Of	Remote Desktop Services Profile Account Profile Telephones			COM+ Organization			
Member of: Name Pri cisco-stealthwatch-m	mary Admin	Envi	Active Dire	sectory Doma			
Comain Users			zitrosystem	ns Jocal/Use	•		
Add Remove Add Remove Primary group: Domain Users Set Primary Group There is no need to change Primary group unless you have Macintosh clients or POSIX-compliant applications.							
01	(C	ancel	Apply	Help	,		

- 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.

snauser10 Properties					?	×
Remote control General Address Member Of	Remote control Remote Desktop Services Profile General Address Account Profile Telephones Member Of Dialing Environment			COM+ Organization		
Member of:						
Name cisco-steathwatch-o cisco-steathwatch-o cisco-steathwatch-o Data Ro Web Fu Desktop	Idata read-an onliguration m esktop-config esktop-config notional Rol Functional	d-write anager uration-man e Role	ager	Active (Directory	D
<						>
Add R Primary group: Do Set Primary Group	emove main Users There is n you have	o need to o Macintosh	change Prir	many gr POSIX-	oup unle	iss t
01		Cancel	Appl	У	He	elp

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.

Us	er Management					
U	Isers Data Roles	Authentication and Authorization				
	Name	^	Description	Authentication Type	Remote Authorization	Actions
	Ex. local	~	Filter Authentication Service Description	Ex. LOCAL ~		
	angelort LDAP server		Main AD server	LDAP	~	

Verifiëren

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

1	יוןייוןי כוsco))	1
Welcom	e user20 K		
This is you There wer	r first time logging in. 0 failed attempt(s) since the account	t was created.	
		ОК	• 11
	Sign In		

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.

cisco Stealthwatch	Dashboards •	Monitor • Analyze	• • Jobs • Configure	 Deploy * 			۹	.	≎ ±
User Management							Online Help	-	
Users Data Roles Authentication and	Authorization						Resources		create 🗸
							Logout		
User Name	Full Name	Primary Admin 😗	Config Manager 😗	Analyst 😑	Power Analyst 😗	Data Role	Status A	ictions	
Ex. jsmith	Ex. "John Smith"					Ex. "All Data(Read & Write)"	Ex. On		
admin	Admin User	~				All Data (Read & Write)	🕥 On -		
10 v Items per page						1 - 1 of 1 items $\parallel <$	< 1 / 1	> >	

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.

1
1

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: <u>Cisco's wereldwijde contactgegevens voor ondersteuning.</u>