Konfigurieren der externen Authentifizierung und Autorisierung über LDAPS für den Zugriff auf Secure Network Analytics Manager

Inhalt

Einleitung Voraussetzungen Anforderungen Verwendete Komponenten Konfigurieren Schritt A: Melden Sie sich beim AD-Domänencontroller an, und exportieren Sie das für LDAP verwendete SSL-Zertifikat. Schritt B: Melden Sie sich beim SNA Manager an, um das Zertifikat des LDAP-Servers und der Stammkette hinzuzufügen. Schritt C: Hinzufügen der Konfiguration des externen LDAP-Diensts. SNA Version 7.2 oder höher SNA Version 7.1 Schritt D. Konfigurieren der Autorisierungseinstellungen Lokale Autorisierung Remote-Autorisierung über LDAP Überprüfung Fehlerbehebung Zugehörige Informationen

Einleitung

Dieses Dokument beschreibt die Basiskonfiguration eines Secure Network Analytics Manager (ehemals Stealthwatch Management Center) Version 7.1 oder höher, um eine externe Authentifizierung zu verwenden und, mit Version 7.2.1 oder höher, eine externe Autorisierung mit LDAPS zu verwenden.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Cisco Secure Network Analytics (ehemals Stealthwatch)
- Allgemeiner LDAP- und SSL-Betrieb
- Allgemeines Microsoft Active Directory-Management

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Komponenten:

- Cisco Secure Network Analytics Manager (ehemals SMC) Version 7.3.2
- Windows Server 2016 wird als Active Directory-Domänencontroller konfiguriert

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Konfigurieren

Schritt A: Melden Sie sich beim AD-Domänencontroller an, und exportieren Sie das für LDAP verwendete SSL-Zertifikat.

- 1. Wählen Sie für Windows Server 2012 oder höher im Startmenü die **Option Ausführen** aus, geben Sie dann **certlm.msc ein** und fahren Sie mit Schritt **8** fort.
- 2. Bei älteren Windows-Serverversionen wählen Sie **Ausführen** im Startmenü aus, und geben Sie dann **mmc** ein.
- 3. Wählen Sie im Menü Datei die Option Einscannen hinzufügen/entfernen.
- 4. Wählen Sie in der Liste Verfügbare Snap-Ins die Option **Zertifikate aus**, und klicken Sie dann auf **Hinzufügen**.

xtensible snap-ins, you can vailable snap-ins:	i configure which e	xter	s are enabled. 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			Move Down
	Microsoft Cor		Add >	
Certificates	Microsoft Cor			
Certification Authority	Microsoft Cor			
Component Services	Microsoft Cor			
E Computer Managem	Microsoft Cor			
Device Manager	Microsoft Cor			
📅 Disk Management	Microsoft and	~		Advanced
escription:				
The Certificates snap-in allo	ows you to browse	the	tents of the certificate stores for yourself, a servic	e, or a computer.

5. Wählen Sie im Snap-In für Zertifikate die Option Computerkonto und anschließend Weiter aus.

6. Lassen Sie Lokaler Computer ausgewählt, und wählen Sie Fertig stellen aus.

7. Wählen Sie im Fenster Snap-In hinzufügen oder entfernen die Option OK.

8. Navigieren Sie zu Zertifikate (Lokaler Computer) > Personal > Certificates (Personal > Zertifikate).

🚟 certlm - [Certificates - Local Cor	mputer\Personal\Certificates]			-		×
File Action View Help						
🗢 🔿 🖄 📅 🖌 🖬 🗙 🛙	1 📑 🛛 🖬					
🗇 Certificates - Local Computer 🔨	Issued To	Issued By	Expiration Date	Intended Purposes		Frie
V Personal	angelort-a	angelort-RootCA2	11/25/2022	Client Authentication	Server Auth	. <n< td=""></n<>
Certificates	Sector Sector	Application in the local sector		1.00		
> Trusted Root Certification						
> Enterprise Trust						
> Intermediate Certification						
> Trusted Publishers						
> Untrusted Certificates						
> Third-Party Root Certifica						
> In Trusted People						
> Client Authentication Issu						
> Preview Build Roots						
> 🧮 Remote Desktop						
> 🧮 Certificate Enrollment Rec						
> Smart Card Trusted Roots						
> Trusted Devices						
> 📔 WebHosting						
🔪 🤗 Windows Live ID Token Iss						
< >	<					>
Personal store contains 2 certificates.						

9. Wählen Sie das SSL-Zertifikat aus, das für die LDAPS-Authentifizierung auf Ihrem Domänen-Controller verwendet wird, und klicken Sie mit der rechten Maustaste, und klicken Sie dann auf Öffnen.

10. Navigieren Sie zur Registerkarte Details > klicken Sie auf In Datei kopieren > Weiter

💼 Certificate

General Show:	Oetails	Certification F	Path V	
Field	rsion rial numb nature al nature h uer	er gorithm ash algorithm	Value	^
Va Va Roje	id from id to hiect		10.000	~
			Edit Properties	Copy to File
				ОК

11. Vergewissern Sie sich, dass Nein, privaten Schlüssel nicht exportieren ausgewählt ist, und klicken Sie auf Weiter.

12. Wählen Sie Base-64-kodiertes X.509-Format aus, und klicken Sie auf Weiter.

×

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

Export File Format

Certificates can be exported in a variety of file formats.

DER	encoded binary X.509 (.CER)
Base	-64 encoded X.509 (.CER)
Cryp	tographic Message Syntax Standard - PKCS #7 Certificates (.P78)
	nclude all certificates in the certification path if possible
Pers	onal Information Exchange - PKCS #12 (.PFX)
	nclude all certificates in the certification path if possible
	elete the private key if the export is successful
E	xport all extended properties
E	nable certificate privacy
Micro	soft Serialized Certificate Store (.SST)

13. Wählen Sie einen Speicherort für das Zertifikat aus, nennen Sie die Datei, und klicken Sie auf **Weiter**.

File to Export Specify the nam	e of the file you v	ant to export		
File name:				
1.000	-	LDAPSidcertifica	ite.cer	Browse

14. Klicken Sie auf **Fertig stellen**, um die Meldung "Der Export war erfolgreich." zu erhalten. Nachricht.

15. Kehren Sie zum für LDAPS verwendeten Zertifikat zurück, und wählen Sie die Registerkarte **Zertifizierungspfad** aus.

16. Wählen Sie oben im Zertifizierungspfad den Root CA-Emittenten aus, und klicken Sie auf **Zertifikat anzeigen**.

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

17. Wiederholen Sie die Schritte 10-14, um das Zertifikat der Root-Zertifizierungsstelle zu exportieren, die das für die LDAPS-Authentifizierung verwendete Zertifikat signiert hat.

Anmerkung: Ihre Bereitstellung kann über eine mehrschichtige CA-Hierarchie verfügen. In diesem Fall müssen Sie die gleiche Prozedur befolgen, um alle Zwischenzertifikate in der Vertrauenskette zu exportieren.

18. Bevor Sie fortfahren, stellen Sie sicher, dass Sie über eine Zertifikatsdatei für den LDAPS-Server und für jede Emittenten-Behörde im Zertifizierungspfad verfügen: Stammzertifikat und Zwischenzertifikate (falls zutreffend).

🖌 🗖	LDAPS certificates						- 0	×
File Home	Share View							^ (
Pin to Quick Copy access	Paste & Cut Paste Copy path Paste shortcut	Move to * Copy to *	New item •	Properties Open ~	Select all Select none			
(lipboard	Organize	New	Open	Select			
$\leftarrow \rightarrow \cdot \uparrow$	A DECK OF BRIDE	LDAPS certificates				~ Ō	Search LDAPS certificates	P
	^ Name	^	Date modified Type	Size				
	LDAPS_Roo	tCA	11/25/2021 11:46 Secu	ity Certificate 3	KB			
	LDAPSidcer	tificate	11/24/2021 7:59 PM Secu	ity Certificate 3	KB			

Schritt B: Melden Sie sich beim SNA Manager an, um das Zertifikat des LDAP-Servers und der Stammkette hinzuzufügen.

- 1. Navigieren Sie zu **Zentrale Verwaltung >** Bestand.
- 2. Suchen Sie die SNA Manager-Appliance, und klicken Sie auf Aktionen > Appliance Configuration (Einheitenkonfiguration bearbeiten).
- 3. Navigieren Sie im Fenster Appliance Configuration (Appliance-Konfiguration) zu Configuration Menu (Konfigurationsmenü) > Trust Store > Add New (Neu hinzufügen).
- 4. Geben Sie den Namen des Empfängers ein, klicken Sie auf **Datei auswählen**, und wählen Sie das Zertifikat des LDAP-Servers aus, und klicken Sie dann auf **Zertifikat hinzufügen**.
- 5. Wiederholen Sie den vorherigen Schritt, um das Zertifikat der Stammzertifizierungsstelle und ggf. Zwischenzertifikate hinzuzufügen.
- 6. Überprüfen Sie, ob die hochgeladenen Zertifikate die richtigen sind, und klicken Sie auf **Apply Settings**.

ory / Appliance	e Configuration Appliance Config	guration - SMC	0101 2000 PM 14 14				I	Cancel Apply Settings
	Appliance Netwo	rk Services General	_					Add New 🔍
	FRIENDLY NAME	ISSUED TO	ISSUED BY	VALID FROM	VALID TO	SERIAL NUMBER	KEY LENGTH	ACTIONS
	LDAP-Server	angelort-ad-	angelort-RootCA2			-		Delete
	LDAP-server-RootCA	angelort-RootCA2	angelort-RootCA2		-			Delete
	10 Certificates							
	Revert							

7. Warten Sie, bis die Änderungen übernommen wurden und der Manager-Status aktiv ist.

Schritt C: Hinzufügen der Konfiguration des externen LDAP-Diensts.

SNA Version 7.2 oder höher

1. Öffnen Sie das Haupt-Dashboard Manager, und navigieren Sie zu **Globale Einstellungen** > **Benutzerverwaltung**.

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
		and the second se	User Management
8.4			SecureX Configuration
			Select Language

2. Wählen Sie im Fenster Benutzerverwaltung die Registerkarte Authentifizierung und Autorisierung aus.

3. Klicken Sie auf Erstellen > Authentifizierungsdienst.

cisco Stealthwatch	Dashboards • Monitor • Analyze • Jobs •	Jonfigure * Deploy *			
User Management					
Users Data Roles Authentication and Authorization			Create ~		
			Data Role		
Name	∧ Description	Authentication Type	Remote Authorization Authentication Service		
Ex. local	✓ Filter Authentication Service Description	Ex. LOGAL	~		
There is no data to display					
10 v Items per page			$ \langle \langle 1 \rangle 1 \rangle \rangle = 1 \rangle 1 \rangle $		

4. Wählen Sie im Dropdown-Menü Authentication Service die Option LDAP aus.

5. Füllen Sie die erforderlichen Felder aus.

Feld	Hinweise
Name des Freundes	Geben Sie einen Namen für den LDAP-Server ei
Beschreibung	Geben Sie eine Beschreibung für den LDAP-Servein.
	Geben Sie den vollqualifizierten Domänennamen wie im Feld Subject Alternative Name (SAN) des LDAP-Serverzertifikats angegeben.
	 Wenn das SAN-Feld nur die IPv4-Adresse er geben Sie die IPv4-Adresse im Feld Server
Serveradresse	 Address (Serveradresse) ein. Wenn das Feld SAN den DNS-Namen enthäl geben Sie den DNS-Namen in das Feld Serv Address (Serveradresse) ein.
	 Wenn das SAN-Feld sowohl DNS- als auch I Werte enthält, verwenden Sie den ersten aufgeführten Wert.
Anschluss	Geben Sie den Port ein, der für die sichere LDAP Kommunikation (LDAP über TLS) festgelegt wurd Der bekannte TCP-Port für LDAPS ist 636. Geben Sie die Benutzer-ID ein, die für die Verbin- zum LDAP-Server verwendet wird. Beispiele: CN=admin,OU=Unternehmensbenutzer,DC=exar DC=com
Bind-Benutzer	Anmerkung: Wenn Sie Ihre Benutzer zu eine integrierten AD-Container hinzugefügt haber B. "Users"), muss der kanonische Name (CN die Bind-DN des Bind-Benutzers auf den integrierten Ordner (z. B. CN=username,
	CN=Users, DC=domain, DC=com) festgeleg sein. Wenn Sie Ihre Benutzer jedoch einem neuen Container hinzugefügt haben, muss d Organisationseinheit (OU) für die Bind-DN a den neuen Containernamen festgelegt sein CN=username, OU=Corporate Users,

DC=domain, DC=com).

Anmerkung: Eine nützliche Möglichkeit, die I DN des Bind-Benutzers zu finden, besteht d das Active Directory auf einem Windows-Se abzufragen, der über eine Verbindung zum Active Directory-Server verfügt. Um diese Informationen abzurufen, können Sie eine Windows-Eingabeaufforderung öffnen und d Befehl dsquery user dc=<Distinguished>,dc=<name> -name <us eingeben. Beispiel: dsquery user dc=example,dc=com -name user1. Das Erge sieht aus wie "CN=user1,OU=Corporate Users,DC=example,DC=com"

Geben Sie das Bind-Benutzerkennwort ein, das fr Verbindung zum LDAP-Server verwendet wird. Geben Sie den Distinguished Name (DN) ein. Die DN gilt für die Verzweigung des Verzeichniss dem die Suche nach Benutzern beginnen muss. es der Anfang der Verzeichnisstruktur (Ihre Domä aber Sie können auch eine Unterstruktur innerhal Verzeichnisses angeben. Der Bind-Benutzer und zur Authentifizierung vorgesehenen Benutzer müs über Basiskonten erreichbar sein. Beispiele: DC=Beispiel, DC=com

Kennwort

Basiskonten

6. Klicken Sie auf Speichern.

CISCO Stealthwatch Dashboards Monitor Analyze Jobs	Configure * Deploy * 🔍 🛓 🌣 土
Add your SSL/TLS certificate to this appliance's Trust Store before you configure the LDAP Authentication service.	
User Management Authentication Service	Cancel
* = Required	
Friendly Name *	Authentication Service
angelort LDAP server	LDAP V
Description *	Port *
Main AD server	636
Server Address 😑 *	Bind User 🕕 *
angelort-ad-	CN=5OU=SNA,OU=Cisco,DC=zitrosDC=local
Certificate Revocation 😑 •	Base Accounts 📀 *
Disabled	DC=zitros,DC=local
Password *	Confirm Password *

7. Wenn die eingegebenen Einstellungen und die Zertifikate, die dem Vertrauensspeicher hinzugefügt wurden, korrekt sind, müssen Sie das Banner "Sie haben Ihre Änderungen erfolgreich gespeichert" öffnen.

8. Der konfigurierte Server muss unter **User Management > Authentication and Authorization** (Benutzerverwaltung **> Authentifizierung und Autorisierung)** angezeigt werden.

cisco Stealthwatch	Ashboards * Monitor * Analyze * Jobs * Configure * Deploy *		< ⊥ ☆ ±
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 Version 7.1

- 1. Navigieren Sie zu **Zentrale Verwaltung >** Bestand.
- 2. Suchen Sie die SMC-Appliance, und klicken Sie auf Aktionen > Appliance Configuration (Einheitenkonfiguration bearbeiten).
- 3. Navigieren Sie im Fenster "Appliance Configuration" zu **Configuration Menu > LDAP Setup >** Add New.
- 4. Füllen Sie die erforderlichen Felder wie in **SNA Version 7.2 oder höher** Schritt 5 beschrieben aus.

Stealthwatch Central Management Appliance Manager Update Manager	App Manager
Inventory Appliance Configuration – SMC Appliance Network Services General	Cancet Apply Settings Configuration Menu
LDAP Setup	Add New
Add LDAP	DESCRIPTION *
angeort.LDAP server SERVER ADDRESS * angelort-ad-	PORT + 636
CERTIFICATE REVOCATION * Disabled	BIND USER
PASSWORD *	CONFIRM PASSWORD *
BASE ACCOUNTS * DC=zitro ,DC=local	
	Cancel

5. Klicken Sie auf Hinzufügen.

6. Klicken Sie auf Einstellungen übernehmen.

7. Wenn die eingegebenen Einstellungen und die Zertifikate, die dem Vertrauensspeicher hinzugefügt wurden, korrekt sind, werden die Änderungen am Manager angewendet, und der Anwendungszustand muss **aktiv** sein.

Schritt D. Konfigurieren der Autorisierungseinstellungen

SNA unterstützt die lokale und Remote-Autorisierung über LDAP. Bei dieser Konfiguration werden die LDAP-Gruppen des AD-Servers integrierten oder benutzerdefinierten SNA-Rollen zugeordnet.

Folgende Authentifizierungs- und Autorisierungsmethoden werden für SNA über LDAP unterstützt:

- Remote-Authentifizierung und lokale Autorisierung
- Remote-Authentifizierung und Remote-Autorisierung (wird nur für SNA Version 7.2.1 oder höher unterstützt)

Lokale Autorisierung

In diesem Fall müssen die Benutzer und ihre Rollen lokal definiert werden. Gehen Sie wie folgt vor, um dies zu erreichen.

1. Navigieren Sie erneut zur **Benutzerverwaltung**, und klicken Sie auf die Registerkarte **Benutzer** > **Erstellen > Benutzer**.

2. Legen Sie den Benutzernamen für die Authentifizierung mit dem LDAP-Server fest, und wählen Sie den konfigurierten Server aus dem Dropdown-Menü **Authentifizierungsdienst aus**.

3. Legen Sie fest, welche Berechtigungen der Benutzer über den Manager verfügen muss, nachdem er vom LDAP-Server authentifiziert wurde, und klicken Sie auf **Speichern**.

CISCO Stealthwatch Dashboards • Monitor • Av	nalyze • Jobs • Configure • Deploy •	9 🛓 🌣 🛨
User Management User		Cancel Save
User Name *	Authentication Service	
user20	angelort LDAP server V	
Full Name	Password O	
		Generate Password
Email	Confirm Password	
×	Show Password	
Role Settings		
Primary Admin		
Data Role		
All Data (Read & Write)		
Web Desktop		
Web Roles Compare		
Configuration Manager Analyst Power Analyst		

Remote-Autorisierung über LDAP

Die Remote-Authentifizierung und -Autorisierung über LDAP wurde erstmals von Secure Network Analytics Version 7.2.1 unterstützt.

Anmerkung: Remote Authorization mit LDAP wird in Version 7.1 nicht unterstützt.

Wenn ein Benutzer lokal (im Manager) definiert und aktiviert ist, muss erwähnt werden, dass der Benutzer remote authentifiziert, aber lokal autorisiert wird. Die Benutzerauswahl wird wie folgt durchgeführt:

1. Sobald die Anmeldeinformationen auf der Begrüßungsseite des Managers eingegeben wurden, sucht der Manager nach einem lokalen Benutzer mit dem angegebenen Namen.

- 2. Wenn ein lokaler Benutzer gefunden wird und aktiviert ist, wird er remote authentifiziert (wenn die Remote-Authentifizierung über LDAP mit lokaler Autorisierung zuvor konfiguriert wurde), aber mit den lokalen Einstellungen autorisiert.
- 3. Wenn die Remote-Autorisierung konfiguriert und aktiviert ist und der Benutzer nicht lokal (nicht konfiguriert oder deaktiviert) gefunden wird, werden Authentifizierung und Autorisierung per Remote-Zugriff durchgeführt.

Aus diesem Grund sind die Schritte zur erfolgreichen Konfiguration der Remote-Authentifizierung nicht.

Schritt D-1: Deaktivieren oder löschen Sie die Benutzer, die Remote-Autorisierung verwenden sollen, aber lokal definiert sind.

- Öffnen Sie das Haupt-Dashboard des Managers, und navigieren Sie zu Global Settings > User Management (Globale Einstellungen > Benutzerverwaltung).
- 2. Deaktivieren oder löschen Sie die Benutzer (sofern vorhanden), die Remote-Authentifizierung und -Autorisierung über LDAP verwenden möchten, aber lokal konfiguriert werden.

Us	er Management								
L	Isers Data Roles Authentication and	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)	O n	
	angelort	Angel Ortiz	~				All Data (Read & Write)	On	
	user20			~	~		All Data (Read & Write)	O off	

Schritt D-2: Definieren Sie cisco-stealthWatch-Gruppen im Microsoft AD-Server.

Für die externe Authentifizierung und Autorisierung über LDAP-Benutzer werden Kennwörter und *cisco-stealthwatch-*Gruppen in Microsoft Active Directory remote definiert. Die im AD-Server definierten *Cisco Stealthwatch-*Gruppen beziehen sich auf die verschiedenen Rollen, die die SNA innehat. Sie müssen wie folgt definiert werden.

SNA-Rolle Gruppe(n) Name cisco-stealthwatch-master-admin Hauptadministrator cisco-stealthWatch-all-Lese- und Schreibzug cisco-stealthwatch-all-data-read-only cisco-stealthwatch-<custom> (optional) Datenrolle Anmerkung: Stellen Sie sicher, dass benutzerdefinierte Data-Rollengruppen mit "cisco-stealthwatch-" beginnen. cisco-stealthWatch-configuration-manager Webfunktionale Rolle cisco-stealthwatch-power-analyst cisco-stealthwatch-analyst cisco-stealthwatch-desktop-stealthwatch-pow user Desktop-Funktionsrolle cisco-stealthwatch-desktop-configuration-ma cisco-stealthwatch-desktop-network-enginee

- cisco-stealthwatch-desktop-security-analyst
- cisco-stealthwatch-desktop-<custom> (optior

Anmerkung: Stellen Sie sicher, dass benutzerdefinierte Desktop-Funktionsgruppe "cisco-stealthwatch-desktop-" beginnen.

Active Directory Users and Computers										
File Action View Help										
⇔ ⇒ 2 📷 ¼ 🗉 🗙 🖾 @ 🕞 🛛 🖬 🐍 🔌 🖆 🍸 💆 🍇										
Active Directory Users and C	Name	Туре	Descriptior '	^						
> 🦰 Saved Queries	🗟 cisco-stealthwatch-all-data-read-and-write	Security Group								
s 😭 Adusia	acisco-stealthwatch-all-data-read-only	Security Group								
> 🖸 Admin	💐 cisco-stealthwatch-analyst	Security Group								
	acisco-stealthwatch-configuration-manager	Security Group								
¢ i cisco	acisco-stealthwatch-custom1	Security Group								
the second se	💐 cisco-stealthwatch-desktop-configuration-manager	Security Group								
	💐 cisco-stealthwatch-desktop-custom1	Security Group								
SNA	💐 cisco-stealthwatch-desktop-network-engineer	Security Group								
> 🧮 Computers	💐 cisco-stealthwatch-desktop-security-analyst	Security Group								
> 📓 Domain Controllers	💐 cisco-stealthwatch-desktop-stealthwatch-power-user	Security Group								
> 📔 ForeignSecurityPrinci	acisco-stealthwatch-master-admin	Security Group								
> 📔 Managed Service Acc 🗸	acisco-stealthwatch-power-analyst	Security Group		~						
< >	<		>							

Anmerkung: Wie bereits beschrieben, werden benutzerdefinierte Gruppen für "Datenrolle" und "Desktop-Funktionsrolle" unterstützt, solange dem Gruppennamen die entsprechende Zeichenfolge vorangestellt wird. Diese benutzerdefinierten Rollen und Gruppen müssen sowohl im SNA Manager als auch im Active Directory-Server definiert werden. Wenn Sie z. B. im SNA Manager eine benutzerdefinierte Rolle "custom1" für eine Desktop-Client-Rolle definieren, muss sie cisco-stealthwatch-desktop-custom1 in Active Directory zugeordnet werden.

Schritt D-3: Definieren Sie LDAP-Autorisierungsgruppenzuordnungen für die Benutzer.

Nachdem die *cisco-stealthwatch-*Gruppen im AD-Server definiert wurden, können wir die Benutzer, die Zugriff auf den SNA Manager haben sollen, den erforderlichen Gruppen zuordnen. Dies muss wie folgt geschehen.

• Ein **primärer Admin-**Benutzer **muss** der *Cisco-stealthwatch-master-admin*-Gruppe zugewiesen und **darf keiner anderen** *cisco-stealthwatch*-Gruppe **angehören**.

user20 Properties				?	×
Remote control General Address Member Of	Ontrol Remote Desktop Services Profile Address Account Profile Telephones Of Dial-in Environment				tion
Member of: Name Pri Cisco-stealthwatch-m Domain Users	mary Admin aster-admin		Active Din zitrosysten zitrosysten	ectory Domi ns Jocal/Use	
K Add R	lemove			>	
Primary group: Do	main Users There is n you have application	o need to o Macintosh 1s.	change Primary g clients or POSIX	roup unless (-compliant	I
01	(C	ancel	Apply	Help	

- Jeder Benutzer, der keine primären Admin-Benutzer ist, muss einer Gruppe jeder Rolle mit den folgenden Bedingungen zugewiesen werden.
- 1. Datenrolle: Der Benutzer muss nur einer Gruppe zugewiesen sein.
- 2. Webfunktionale Rolle: Der Benutzer muss mindestens einer Gruppe zugewiesen sein.
- 3. Funktion des Desktops: Der Benutzer muss mindestens einer Gruppe zugewiesen sein.

snauser10 Properties					?	×		
Remote control	te control Remote Desktop Services Profile			file	CO	M+		
Member Of	Member Of Dial-in Environment							
Member of:								
Name				Active I	Directory	D		
cisco-stealthwatch-a	l-data-read-an	d-write		-				
cisco-steathwatch-co	onfiguration m	anager						
cisco-steatnwatch-de	esktop-configu	uration-mar	lager					
Data Ro Web Fur Desktop	le nctional Rol Functional	e Role						
<						>		
Add R	emove							
Primary group: Do	main Users There is n you have application	o need to o Macintosh ns.	change Pr clients or	imary gr POSIX-	roup unle compliar	tss t		
OF	((Cancel	Арр	ly .	He	elp		

Schritt D-4: Aktivieren Sie die Remote-Autorisierung über LDAP im SNA Manager.

- 1. Öffnen Sie das Haupt-Dashboard Manager, und navigieren Sie zu **Globale Einstellungen** > **Benutzerverwaltung**.
- 2. Wählen Sie im Fenster **Benutzerverwaltung** die Registerkarte **Authentifizierung und Autorisierung aus**.
- 3. Suchen Sie den LDAP-Authentifizierungsdienst, der in Schritt C konfiguriert wurde.
- 4. Klicken Sie auf Aktionen > Remote Authorization aktivieren.

Anmerkung: Es kann jeweils nur ein externer Autorisierungsdienst verwendet werden. Wenn bereits ein anderer Autorisierungsdienst verwendet wird, wird dieser automatisch deaktiviert und der neue Dienst aktiviert. Alle Benutzer, die mit dem vorherigen externen Dienst autorisiert wurden, werden jedoch abgemeldet. Eine Bestätigungsmeldung wird angezeigt, bevor eine Aktion ausgeführt wird.

Use	er Mana	gement					
Us	ers D	ata Roles	Authentication and Authorization				
1	Name		^	Description	Authentication Type	Remote Authorization	Actions
	Ex. local		~	Filter Authentication Service Description	Ex. LOCAL V		
-	angelort LD	AP server		Main AD server	LDAP	~	

Überprüfung

Die Benutzer können sich mit den auf dem AD-Server definierten Anmeldeinformationen anmelden.



Der zweite Überprüfungsschritt betrifft die Autorisierung. In diesem Beispiel wurde der Benutzer "user20" zum Mitglied der Gruppe *cisco-stealthwatch-master-admin* im AD-Server gemacht, und wir können bestätigen, dass der Benutzer über primäre Administratorberechtigungen verfügt. Der Benutzer ist in den lokalen Benutzern nicht definiert, daher können wir bestätigen, dass die Autorisierungsattribute vom AD-Server gesendet wurden.

cisco Stealthwatch	Dashboards *	Monitor • Analyze	e • Jobs • Configure	 Deploy * 			۹ 🛔	\$ ±
User Management							Online Help	
Licera Data Dales Authenticatio	and Authorization						Resources	Constant
Users Data Koles Authenticatio	and Authonization						About	Create V
							Logout	
User Name	Full Name	Primary Admin 🔵	Config Manager 🌖	Analyst 💿	Power Analyst 😗	Data Role	Status Action	5
Ex. jsmith	Full Name Ex. "John Smith"	Primary Admin 🌖	Config Manager 🌖	Analyst 😑	Power Analyst 😑	Data Role Ex. "All Data(Read & Write)"	Status Action	5
User Name Ex. jsmith admin	Full Name Ex. "John Smith" Admin User	Primary Admin 💿	Config Manager 🚷	Analyst 🕤	Power Analyst 🌖	Data Role Ex. "All Data(Read & Write)" All Data (Read & Write)	Status Action	5

Dieselbe Überprüfung wird für den anderen Benutzer in diesem Beispiel "snauser10" durchgeführt. Die erfolgreiche Authentifizierung kann mit den Anmeldeinformationen bestätigt werden, die auf dem AD-Server konfiguriert wurden.



Da dieser Benutzer nicht zur primären Administratorgruppe gehört, sind zur Autorisierungsüberprüfung einige Funktionen nicht verfügbar.

watch		Dashboards * M	Monitor • Analyze •	Jobs * Configure	 Deploy * 				a 🛓 🁸	+
									Global Settings	
Dashboard Inside H	losts								SMC Configuration	
									Packet Analyzer Configuration	
									External Lookup Configuration	1
Target Index	Recon	C&C	Exploitation	DDoS Source	DDoS Target	Data Hoarding	Exfiltration	Poli	SecureX Configuration	
0	0	0	0	0	0	0	0		Select Language	
Ū	Ŭ	Ū	Ū	Ŭ	Ŭ	Ū	Ŭ			
	Watch Dashboard Inside H Target Index	Vatch Dashboard Inside Hosts Target Index Recon O O O	Watch Dashboards - M Dashboard Inside Hosts Target Index Recon C&C O O O	Watch Dashboards Monitor Analyze - Dashboard Inside Hosts Target Index Recon C&C Exploitation 0 0 0 0	Watch Dashboards * Monitor * Analyze * Jobs * Configure Dashboard Inside Hosts Target Index Recon C&C Exploitation DDoS Source O O	Watch Dashboards Monitor Analyze Jobs Configure Deploy Dashboard Inside Hosts Target Index Recon C&C Exploitation DDoS Source DDoS Target O O O O O O O O O O O O O O O O O O O	Watch Dashboards · Monitor · Analyze · Jobs · Configure · Deploy · Dashboard Inside Hosts Target Index Recon C&C Exploitation DDoS Source DDoS Target Data Hoarding O O	Watch Dashboards Monitor Analyze Jobs Configure Deploy +	Watch Dashboards Monitor Analyze Jobs Configure Deploy + Dashboard Inside Hosts Target Index Recon CBC Exploitation DDoS Source DDoS Target Data Hoarding Exfitration Poll OOOOO	Watch Dashboards Monitor Analyze Jobs Configure Deploy Qeloy Gold Settings

Fehlerbehebung

Wenn die Konfiguration des Authentifizierungsdienstes nicht erfolgreich gespeichert werden kann, überprüfen Sie Folgendes:

- 1. Sie haben dem Vertrauensspeicher des Managers die entsprechenden Zertifikate des LDAP-Servers hinzugefügt.
- 2. Die konfigurierte Serveradresse entspricht den Angaben im Feld Subject Alternative Name (SAN) des LDAP-Serverzertifikats. Wenn das SAN-Feld nur die IPv4-Adresse enthält, geben Sie die IPv4-Adresse im Feld Server Address (Serveradresse) ein.Wenn das Feld SAN den DNS-Namen enthält, geben Sie den DNS-Namen in das Feld Server Address

(Serveradresse) ein.Wenn das SAN-Feld sowohl DNS- als auch IPv4-Werte enthält, verwenden Sie den ersten aufgeführten Wert.

3. Die konfigurierten Felder **Bind User** und **Base Account** sind korrekt, wie vom AD Domain Controller angegeben.

Zugehörige Informationen

Weitere Unterstützung erhalten Sie vom Cisco Technical Assistance Center (TAC). Ein gültiger Support-Vertrag ist erforderlich: <u>Weltweiter Kontakt zum Cisco Support.</u>