# Configurazione dell'autenticazione e dell'autorizzazione esterne tramite LDAPS per l'accesso sicuro a Network Analytics Manager

# Sommario

Introduzione Prerequisiti **Requisiti** Componenti usati Configurazione Passaggio A. Accedere al controller di dominio Active Directory ed esportare il certificato SSL utilizzato per LDAP. Passaggio B. Accedere a SNA Manager per aggiungere il certificato del server LDAP e la catena principale. Passaggio C. Aggiungere la configurazione del servizio esterno LDAP. SNA versione 7.2 o successive SNA versione 7.1 Passaggio D. Configurare le impostazioni di autorizzazione. Autorizzazione locale Autorizzazione remota tramite LDAP Verifica Risoluzione dei problemi Informazioni correlate

# Introduzione

Questo documento descrive la configurazione di base di Secure Network Analytics Manager (in precedenza Stealthwatch Management Center) versione 7.1 o successive per utilizzare l'autenticazione esterna e, con la versione 7.2.1 o successive, per utilizzare l'autorizzazione esterna con LDAPS.

# Prerequisiti

## Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Cisco Secure Network Analytics (in precedenza Stealthwatch)
- Operazione generale LDAP e SSL
- Gestione generale di Microsoft Active Directory

## Componenti usati

Le informazioni di questo documento si basano sui seguenti componenti:

- Cisco Secure Network Analytics Manager (in precedenza SMC) versione 7.3.2
- Windows Server 2016 configurato come controller di dominio Active Directory

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

# Configurazione

# Passaggio A. Accedere al controller di dominio Active Directory ed esportare il certificato SSL utilizzato per LDAP.

1. Per Windows Server 2012 o versioni successive selezionare **Esegui** dal menu Start, quindi immettere **certIm.msc** e continuare con il passaggio **8**.

1

- 2. Per le versioni precedenti di Windows Server, selezionare **Esegui** dal menu Start, quindi immettere **mmc**.
- 3. Dal menu File, selezionare Aggiungi/Rimuovi snap-in.
- 4. Nell'elenco Snap-in disponibili selezionare Certificati, quindi fare clic su Aggiungi.

Add or Remove Snap-ins				×
You can select snap-ins for this console from those available on your computer and configure the selected set of snap-ins. For extensible snap-ins, you can configure which extensions are enabled.				
Available snap-ins:			Selected snap-ins:	
Snap-in	Vendor	^	Console Root Edit Extens	ions
Active Directory Do	Microsoft Cor Microsoft Cor		Remov	/e
Active Directory Use	Microsoft Cor Microsoft Cor		Move	Up
ADSI Edit	Microsoft Cor Microsoft Cor		Add >	own
Certificate Templates	Microsoft Cor Microsoft Cor			
Certification Authority	Microsoft Cor Microsoft Cor			
Computer Managem	Microsoft Cor Microsoft Cor			
T Disk Management	Microsoft and	~	Advance	ed
Description:				
The Certificates snap-in allo	ws you to browse	the	contents of the certificate stores for yourself, a service, or a computer.	
			OK	Cancel

- 5. Nella finestra snap-in Certificati, selezionare Account computer, quindi selezionare Avanti.
- 6. Lasciare selezionato Computer locale, quindi selezionare Fine.

7. Nella finestra Aggiungi o rimuovi snap-in, selezionare OK.

## 8. Passare a Certificati (computer locale) > Personale > Certificati

🗃 certlm - [Certificates - Local Computer\Persona	l\Certificates]		-	
File Action View Help				
🗢 🔿 🙋 📷 🖌 🛍 🗙 🖼 🔒 🛛 🖬	1 1 2			
Certificates - Local Computer A Issued To	A Issued By	Expiration Date	Intended Purposes	Frie
V Personal	angelort-Ro	otCA2 11/25/2022	Client Authentication, Se	erver Auth <n< td=""></n<>
Certificates	takini mpiniki	ALC: 1 (2010)		
> Trusted Root Certification				
> Enterprise Irust				
> Intermediate Certification				
> Irusted Publishers				
> Untrusted Certificates				
> Inird-Party Root Certifica				
> Irusted People				
Client Authentication Issu				
> Preview Build Roots				
Remote Desktop				
Certificate Enrollment Rec				
> Smart Card Trusted Roots				
> Irusted Devices				
> WebHosting				
				>
Personal store contains 2 certificates.				

9. Selezionare e fare clic con il pulsante destro del mouse sul certificato SSL utilizzato per l'autenticazione LDAPS sul controller di dominio e fare clic su **Apri**.

10. Passare alla scheda Dettagli > fare clic su Copia su file > Avanti

#### 💼 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. Verificare che l'opzione No, non esportare la chiave privata sia selezionata e fare clic su Avanti

12. Selezionare il formato X.509 con codifica Base 64 e fare clic su Avanti.

←	£.	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 C	ertificates (.P78)
Include all certificates in the certification path if po	ssible
Personal Information Exchange - PKCS #12 (.PFX)	
Include all certificates in the certification path if po	ssible
Delete the private key if the export is successful	
Export all extended properties	
Enable certificate privacy	
Microsoft Serialized Certificate Store (.SST)	

13. Selezionare il percorso in cui memorizzare il certificato, assegnare un nome al file e fare clic su **Avanti**.

ile to Export Specify the name of the	file you want to export		
File name:			
· · · · · · · · · · · · · · · · · · ·	LDAPSidcertifi	cate.cer	Browse

14. Fare clic su **Finish** (Fine) per visualizzare il messaggio "Esportazione completata". messaggio.

15. Tornare al certificato utilizzato per LDAPS, quindi selezionare la scheda **Percorso** certificazione.

16. Selezionare l'autorità di certificazione radice sul percorso della certificazione e fare clic su **Visualizza certificato**.

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

17. Ripetere i passaggi da 10 a 14 per esportare il certificato della CA radice che ha firmato il certificato utilizzato per l'autenticazione LDAPS.

**Nota:** La distribuzione può avere una gerarchia di CA a più livelli. In questo caso, è necessario seguire la stessa procedura per esportare tutti i certificati intermedi nella catena di attendibilità.

18. Prima di continuare, assicurarsi di disporre di un file di certificato per il server LDAPS e per ogni autorità emittente nel percorso di certificazione: Certificato radice e certificati intermedi (se applicabile).

📕   🗹 📙 🖛   I	DAPS certificates						- 0	$\times$
File Home	Share View							^ <b>(</b>
Pin to Quick Copy access	Paste	Move Copy to * Copy	ne New folder	Properties	Select all Select none			
c	lipboard	Organize	New	Open	Select			
$\leftrightarrow$ $\rightarrow$ $\checkmark$ $\uparrow$	A REAL PROPERTY.	LDAPS certificates				~ Õ	Search LDAPS certificates	P
	^ Name	^	Date modified Type	Size				
	LDAPS_Root	CA	11/25/2021 11:46 Securi	ity Certificate 3	KB			
	LDAPSidcert	ificate	11/24/2021 7:59 PM Securi	ity Certificate 3	KB			

# Passaggio B. Accedere a SNA Manager per aggiungere il certificato del server LDAP e la catena principale.

- 1. Passare a **Gestione centrale** > Magazzino.
- 2. Individuare l'accessorio SNA Manager e fare clic su **Azioni > Modifica configurazione accessorio**.
- 3. Nella finestra Configurazione accessorio passare a **Menu Configurazione > Archivio** protezione > Aggiungi nuovo.
- 4. Digitare il Nome descrittivo, fare clic su **Scegli file** e selezionare il certificato del server LDAP, quindi fare clic su **Aggiungi certificato**.
- 5. Ripetere il passaggio precedente per aggiungere il certificato CA radice e i certificati intermedi (se applicabile).
- 6. Verificare che i certificati caricati siano corretti e fare clic su Applica impostazioni.

Configuration Appliance Config	guration - SMC						Cancel Apply Settings
Appliance Netwo	rk Services General	COLUMN 2 COLUMN 2 CARDIN					Configuration Menu 🔻
Trust Store Mod	fed						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							T
Revert							

7. Attendere che le modifiche vengano applicate e che lo stato del responsabile sia Attivo.

## Passaggio C. Aggiungere la configurazione del servizio esterno LDAP.

### SNA versione 7.2 o successive

1. Aprire il pannello di controllo principale Responsabile e passare a **Impostazioni globali > Gestione utente**.

cisco Stealthwatch	Dashboards • Monitor • Analyze • Jobs • Configure • Dep	ploy *	ب 🛓 🗢 🛨
Security Insight Dashboard   Inside Hosts		G	Ilobal Settings
Alarming Hosts		P D D D D D D D D D D D D D D D D D D D	Acket Analyzer Configuration     JDP Director Configuration     Set Management     SecureX Configuration     Select Language

- 2. Nella finestra Gestione utenti, selezionare la scheda Autenticazione e autorizzazione.
- 3. Fare clic su Crea > Servizio di autenticazione.

cisco Stealthwatch	Dashboards * Monitor * Analyze * Jobs * Configure * 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. LOCAL V	
	There is no data to display		
10 v items per page			$ \langle \langle 1   / 1 \rangle \rangle $

- 4. Dal menu a discesa Servizio di autenticazione selezionare LDAP.
- 5. Completare i campi obbligatori.

Campo	Note
Nome	Immettere un nome per il server LDAP.
Descrizione	Immettere una descrizione per il server LDAP. Immettere il nome di dominio completo specificat campo Nome alternativo soggetto (SAN) del certi server LDAP.
Indirizzo server	<ul> <li>Se il campo SAN contiene solo findirizzo IPv immettere l'indirizzo IPv4 nel campo Indirizzo server.</li> <li>Se il campo SAN contiene il nome DNS, imm il nome DNS nel campo Indirizzo server.</li> <li>Se il campo SAN contiene sia valori DNS che IDv4 utilizzoro il primo valoro elonosto.</li> </ul>
Port	Immettere la porta designata per la comunicazion LDAP protetta (LDAP su TLS). La porta TCP nota LDAPS è la 636. Immettere l'ID utente utilizzato per la connessione server LDAP. Ad esempio: CN=admin,OU=utenti aziendali,DC=esempio,DC=com
Associa utente	Nota: Se gli utenti sono stati aggiunti a un contenitore AD incorporato (ad esempio, "Utenti"), il DN di associazione dell'utente di associazione deve avere il nome canonico ( impostato sulla cartella predefinita (ad esem CN=nomeutente, CN=Utenti, DC=dominio, DC=com). Se tuttavia sono stati aggiunti gli a un nuovo contenitore, l'unità organizzativa del DN di associazione deve essere imposta sul nuovo nome del contenitore, ad esempio CN=nomeutente, OU=Utenti aziendali, DC=dominio, DC=com.
	<b>Nota:</b> Un modo utile per trovare il DN di bind dell'utente di binding consiste nell'eseguire u query su Active Directory in un server Windo

	connesso al server Active Directory. Per otte queste informazioni, è possibile aprire un pro dei comandi di Windows e digitare il comano dsquery user dc= <distinguished>,dc=<name name <user>. Ad esempio: dsquery user dc=example,dc=com -name user1. Il risultato sarà "CN=user1,OU=Corporate Users,DC=example,DC=com"</user></name </distinguished>
Password	Immettere la password utente di binding utilizzata la connessione al server LDAP. Immettere il nome distinto (DN)
	II DN si applica alla sezione della directory in cui devono iniziare le ricerche degli utenti. Spesso si nella parte superiore della struttura di directory
Conti base	(dominio), ma è possibile specificare anche una sottostruttura all'interno della directory. L'utente d binding e gli utenti da autenticare devono essere accessibili dagli account di base. Ad esempio: DC=esempio,DC=com

## 6. Fare clic su Salva.

CISCO Stealthwatch 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
* = Required	
Friendly Name *	Authentication Service
angelort LDAP server	LDAP V
Description *	Port *
Main AD server	636
Server Address 🕖 *	Bind User 😗 *
angelort-ad-	CN+s=OU+SNA,OU+Cisco,DC+zitros=DC+local
Certificate Revocation 🗿 *	Base Accounts 🕕 *
Disabled V	DC=zitro: ,DC=local
Password *	Confirm Password *

7. Se le impostazioni immesse e i certificati aggiunti all'archivio di attendibilità sono corretti, è necessario visualizzare il banner "Salvataggio delle modifiche completato".

8. Il server configurato deve essere visualizzato in **Gestione utenti > Autenticazione e autorizzazione**.

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 $ \langle -\langle 1 \rangle / 1 \rangle \rightarrow  $

### SNA versione 7.1

- 1. Passare a **Gestione centrale >** Magazzino.
- 2. Individuare l'accessorio SMC e fare clic su Azioni > Modifica configurazione accessorio.
- 3. Nella finestra Configurazione accessorio passare a Menu Configurazione > Impostazione LDAP > Aggiungi nuovo.
- 4. Completare i campi obbligatori come descritto nel passaggio 5 della SNA versione 7.2 o successive.

CISCO Stealthwatch Central Management Appliance Manager Update Manager	App Manager	e
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-	DESCRIPTION * Main AD server PORT * 636	
CERTIFICATE REVOCATION	BIND USER	
BASE ACCOUNTS   * DC=zitro DC=local	Cancel Add	

#### 5. Fare clic su Aggiungi.

6. Fare clic su Applica impostazioni.

7. Quando le impostazioni immesse e i certificati aggiunti all'archivio di attendibilità sono corretti, le modifiche apportate al Manager vengono applicate e lo stato dell'accessorio deve essere **Attivo**.

## Passaggio D. Configurare le impostazioni di autorizzazione.

La SNA supporta l'autorizzazione locale e remota tramite LDAP. Con questa configurazione, i gruppi LDAP del server AD vengono mappati a ruoli SNA predefiniti o personalizzati.

I metodi di autenticazione e autorizzazione supportati per SNA tramite LDAP sono:

Autenticazione remota e autorizzazione locale

 Autenticazione e autorizzazione remote (supportate solo per SNA versione 7.2.1 o successive)

#### Autorizzazione locale

In questo caso, gli utenti e i relativi ruoli devono essere definiti localmente. A tale scopo, procedere come segue.

1. Passare di nuovo a Gestione utente, fare clic sulla scheda Utenti > Crea > Utente.

2. Definire il nome utente da autenticare con il server LDAP e selezionare il server configurato dal menu a discesa **Servizio di autenticazione**.

3. Definire le autorizzazioni che l'utente deve avere sul Manager una volta autenticato dal server LDAP e fare clic su **Salva**.

CISCO Stealthwatch Dashboards - Monitor - A	nalyze • Jobs • Configure • Deploy •	Q <b>⊥ ☆ ±</b>
User Management   User		Cancel Save
User Name •  user20 Full Name  mail  Role Settings  Primary Admin Data Role  MI Data (Read & Write)  Web Roles Compare	Authentication Service	Cenerate Password
С топа напук		

#### Autorizzazione remota tramite LDAP

L'autenticazione e l'autorizzazione in remoto tramite LDAP sono state inizialmente supportate in Secure Network Analytics versione 7.2.1.

Nota: L'autorizzazione remota con LDAP non è supportata nella versione 7.1.

Èimportante ricordare che se un utente è definito e abilitato localmente (in Manager), viene autenticato in remoto, ma autorizzato localmente. Il processo di selezione degli utenti è il seguente:

- 1. Una volta immesse le credenziali nella pagina di benvenuto del Manager, quest'ultimo cerca un utente locale con il nome specificato.
- 2. Se un utente locale viene individuato e abilitato, viene autenticato in remoto (se l'autenticazione remota tramite LDAP con autorizzazione locale è stata configurata in

precedenza) ma autorizzato con le impostazioni locali.

3. Se l'autorizzazione remota è configurata e abilitata e l'utente non viene trovato localmente (non configurato o disabilitato), sia l'autenticazione che l'autorizzazione vengono eseguite in remoto.

Per questo motivo, per configurare correttamente l'autenticazione remota, è necessario eseguire la procedura seguente.

# Passaggio D-1. Disabilitare o eliminare gli utenti che intendono utilizzare l'autorizzazione remota ma che sono definiti localmente.

- 1. Aprire il dashboard principale di Manager e selezionare Impostazioni globali > Gestione utente.
- 2. Disabilitare o eliminare gli utenti (se esistenti) destinati a utilizzare l'autenticazione e l'autorizzazione remote tramite LDAP, ma configurati localmente.

User Management								
Users 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)	On	
angelort	Angel Ortiz	$\checkmark$				All Data (Read & Write)	On	
user20			~	~		All Data (Read & Write)	Off Off	]

Passaggio D-2. Definire i gruppi cisco-stealthwatch nel server AD Microsoft.

Per l'autenticazione e l'autorizzazione esterne tramite utenti LDAP, le password e i gruppi *cisco-stealthwatch* vengono definiti in remoto in Microsoft Active Directory. I gruppi *cisco-stealthwatch* da definire nel server AD sono correlati ai diversi ruoli svolti dalla SNA e devono essere definiti come segue.

Ruolo SNA	Nome gruppo/i
Amministratore primario	<ul> <li>cisco-stealthwatch-master-admin</li> </ul>
	<ul> <li>cisco-stealthwatch-all-data-read-and-write</li> </ul>
	<ul> <li>cisco-stealthwatch-all-data-read-only</li> </ul>
	<ul> <li>cisco-stealthwatch-<personalizzato> (opzion</personalizzato></li> </ul>
Ruolo dati	
	Nota: Verificare che i gruppi di ruoli dati personalizzati inizino con "cisco-stealthwatc
	<ul> <li>cisco-stealthwatch-configuration-manager</li> </ul>
Ruolo funzionale Web	<ul> <li>cisco-stealthwatch-power-analyst</li> </ul>
	<ul> <li>cisco-stealthwatch-analyst</li> </ul>
	<ul> <li>cisco-stealthwatch-desktop-stealthwatch-pov user</li> </ul>
	<ul> <li>cisco-stealthwatch-desktop-configuration-ma</li> </ul>
Puelo funzionalo del deskton	<ul> <li>cisco-stealthwatch-desktop-network-enginee</li> </ul>
Rubio fullzionale del desktop	<ul> <li>cisco-stealthwatch-desktop-security-analyst</li> </ul>
	<ul> <li>cisco-stealthwatch-desktop-<personalizzato> (opzionale)</personalizzato></li> </ul>
	<ul> <li>cisco-stealthwatch-desktop-<personalizzato (opzionale)</personalizzato </li> </ul>

**Nota:** Verificare che i gruppi di ruoli funziona desktop personalizzati inizino con "cisco-stealthwatch-desktop-".

Active Directory Users and Complexity	puters	-	$\Box$ ×
File Action View Help			
🗢 🔿 🙍 📅 🖌 📋 🗙 🛛	] Q 📑 🛛 🖬 🗏 📚 🛅 🍸 🗾 🐍		
Active Directory Users and C	Name	Туре	Descriptior ^
> 🦳 Saved Queries	acisco-stealthwatch-all-data-read-and-write	Security Group	
1 Admin	🂐 cisco-stealthwatch-all-data-read-only	Security Group	
> Admin	🂐 cisco-stealthwatch-analyst	Security Group	
	acisco-stealthwatch-configuration-manager	Security Group	
CISCO	acisco-stealthwatch-custom1	Security Group	
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	acisco-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	~
< >	<		>

**Nota:** Come descritto in precedenza, i gruppi personalizzati sono supportati per "Ruolo dati" e "Ruolo funzionale desktop" a condizione che al nome del gruppo sia anteposta la stringa corretta. I ruoli e i gruppi personalizzati devono essere definiti sia in Gestione SNA che nel server Active Directory. Ad esempio, se si definisce un ruolo personalizzato "custom1" in Gestione SNA per un ruolo client desktop, è necessario mapparlo a cisco-stealthwatch-desktop-custom1 in Active Directory.

### Passaggio D-3. Definire i mapping dei gruppi di autorizzazione LDAP per gli utenti.

Una volta definiti i gruppi *cisco-stealthwatch* nel server AD, è possibile mappare gli utenti che devono accedere a SNA Manager sui gruppi necessari. Ciò deve avvenire nel modo seguente.

• Un utente Admin primario deve essere assegnato al gruppo *cisco-stealthwatch-master-admin* e non deve essere membro di alcun altro *gruppo cisco-stealthwatch*.

user20 Properties				? ×	
Remote control	Remote D	esktop Se	rvices Profile	COM+	
General Address	Account	Profile	Telephones	Organization	
Member Of	Dial-in	Envi	ronment	Sessions	
Member of:					
Name Pri	mary Admin		Active Dire	ectory Doma	
cisco-stealthwatch-m	aster-admin		zinsvelen	s local/Cisc	
Domaio Lisers	dater darini		simevelor	e local/Lise	
			<i>La coporcia</i>		
Member Of     Dial-in     Environment     Sessions       Member of:	>				
Add	lemnue				
700	icinove				
Primary group: Do	omain Users				
	There is n	o need to d	hance Primary o	roup unless	
Set Primary Group	you have	Macintosh	clients or POSIX	compliant	
	application	15.			
01	C C	ancel	Apply	Help	

- Ogni utente, diverso dagli utenti Amministratore primario, deve essere assegnato a un gruppo di ogni ruolo con le condizioni successive.
- 1. Ruolo dati: L'utente deve essere assegnato a un solo gruppo.
- 2. Ruolo funzionale Web: L'utente deve essere assegnato ad almeno un gruppo.
- 3. Ruolo funzionale del desktop: L'utente deve essere assegnato ad almeno un gruppo.

snauser10 Properties					?	×
Remote control General Address Member Of	Remote D Account Dial-in	esktop Se Profile Envi	rvices Pro Telepho ronment	ones	CO Organi Sessio	M+ zation
Member of:						
Name cisco-steathwatch-a cisco-steathwatch-o cisco-steathwatch-o Data Ro Web Fut Desktop	I-data-read-an onfiguration-m esktop-configu- esktop-configu- nctional Rol Functional	d-write anager rration-mar le Role	ager	Active	Directory	D
<						>
Add R Primary group: Do Set Primary Group	main Users There is n you have application	o need to o Macintosh 1s.	change Pr clients or	imary g POSIX	roup unle compliar	ess t
OF	( C	ancel	Αρς	sły	Н	elp

#### Passaggio D-4. Abilitare l'autorizzazione remota tramite LDAP su SNA Manager.

- 1. Aprire il dashboard principale di Manager e passare a **Impostazioni globali > Gestione utente**.
- 2. Nella finestra Gestione utenti selezionare la scheda Autenticazione e autorizzazione.
- 3. Individuare il servizio di autenticazione LDAP configurato nel passo C.
- 4. Fare clic su Azioni > Abilita autorizzazione remota.

Nota: È possibile utilizzare un solo servizio di autorizzazione esterno alla volta. Se un altro servizio di autorizzazione è già in uso, viene automaticamente disabilitato e il nuovo servizio viene abilitato, tuttavia tutti gli utenti autorizzati con il servizio esterno precedente verranno disconnessi. Prima di eseguire qualsiasi azione viene visualizzato un messaggio di conferma.

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

# Verifica

Gli utenti possono accedere con le credenziali definite nel server AD.

1	cisco		1	
Wel	ome user20 🗡			
This is	your first time logging in.	created.		
			ОК	
	Sign In			

La seconda fase di verifica riguarda l'autorizzazione. Nell'esempio, l'utente "user20" è stato aggiunto al gruppo *cisco-stealthwatch-master-admin* nel server AD e possiamo confermare che l'utente ha le autorizzazioni di amministratore primario. L'utente non è definito negli utenti locali, pertanto è possibile verificare che gli attributi di autorizzazione siano stati inviati dal server AD.

Stealthwatch	Dashboards *	Monitor • Analyze	e • Jobs • Configure	<ul> <li>Deploy •</li> </ul>			۹	1	◊ ±	
User Management								_		
							Resources			
Users Data Roles Authentication an	Users Data Roles Authentication and Authorization						About		Create ~	
							Logout			
User Name	Full Name	Primary Admin 👩	Config Manager 🔕	Analyst 😑	Power Analyst 👩	Data Role	Status	Actions		
Ex. jsmlth	Ex. "John Smith"					Ex. "All Data(Read & Write)"	Ex. On			
admin	Admin User	~				All Data (Read & Write)	C On			
10 v Items per page						1 - 1 of 1 items	< 1/1	>		

La stessa verifica viene effettuata per l'altro utente in questo esempio "serpente10". È possibile confermare la riuscita dell'autenticazione con le credenziali configurate nel server AD.



Per la verifica dell'autorizzazione, alcune funzionalità non sono disponibili perché l'utente non appartiene al gruppo Amministratore primario.

Stealthwat	tch		Dashboards • N	fonitor • Analyze •	Jobs • Configure	<ul> <li>Deploy *</li> </ul>				a 🕇 👸	+
										Global Settings	
Security Insight Dashboard   Inside Hosts								SMC Configuration			
										Packet Analyzer Configuration	
g Hosts 📀										External Lookup Configuration	1
ern Index	Target Index	Recon	C&C	Exploitation	DDoS Source	DDoS Target	Data Hoarding	Exfiltration	Poli	SecureX Configuration	
2	0	0	0	0	0	0	0	0		Select Language	
~	0	U	0	U	0	U	Ŭ	U		0	
	Stealthwar y Insight Das g Hosts • em Index 2	Stealthwatch y Insight Dashboard   Inside P g Hosts • em Index Target Index 2 0	Stealthwatch y Insight Dashboard   Inside Hosts g Hosts • em Index Target Index Recon 2 0 0	Stealthwatch Dashboard > M y Insight Dashboard   Inside Hosts g Hosts • em Index Target Index Recon C&C 2 0 0 0	Stealthwatch Dashboards Monitor Analyze  y Insight Dashboard   Inside Hosts g Hosts em Index Target Index Recon C&C Exploitation 2 0 0 0	Stealthwatch     Dashboards · Monitor · Analyze · Jobs · Configure       y Insight Dashboard   Inside Hosts       ig Hosts •       em Index     Target Index       2     0       0     0	Stealthwatch     Dashboards · Monitor · Analyze · Jobs · Configure · Deploy ·       y Insight Dashboard   Inside Hosts     g Hosts •       em Index     Target Index     Recon     C&C     Exploitation     DDoS Source     DDoS Target       2     0     0     0     0     0	Stealthwatch     Dashboards + Monitor + Analyze + Jobs + Configure + Deploy +       y Insight Dashboard   Inside Hosts       rg Hosts •       em Index     Target Index       2     0       0     0       0     0	Stealthwatch     Dashboards + Monitor + Analyze + Jobs + Configure + Deploy +       y Insight Dashboard   Inside Hosts       rg Hosts •       em Index     Target Index       2     0       0     0       0     0       0     0       0     0	Stealthwatch     Dashboards + Monitor + Analyze + Jobs + Configure + Deploy +       y Insight Dashboard   Inside Hosts       ig Hosts •       em Index     Target Index       2     0       0     0       0     0       0     0	Stealthwatch Dashboards · Monitor · Analyze · Jobs · Configure · Deploy ·     Q Q Q     Global Settings     SMC Configuration     Packet Analyze / Configuration     Packet Analyze / Configuration     Packet Analyze / Configuration     External Lookup Configuration     Secure X Configuration     Packet Analyze / Configuration     Packet Analyze / Configuration     Secure X Configuration

# Risoluzione dei problemi

Se non è possibile salvare la configurazione del servizio di autenticazione, verificare che:

- 1. I certificati appropriati del server LDAP sono stati aggiunti all'archivio di attendibilità di Manager.
- 2. L'indirizzo del server configurato è quello specificato nel campo Nome alternativo soggetto (SAN) del certificato del server LDAP. Se il campo SAN contiene solo l'indirizzo IPv4, immettere l'indirizzo IPv4 nel campo Indirizzo server.Se il campo SAN contiene il nome DNS, immettere il nome DNS nel campo Indirizzo server.Se il campo SAN contiene sia valori DNS che IPv4, utilizzare il primo valore elencato.

3. I campi **Associa utente** e **Account di base** configurati sono corretti, come specificato dal controller di dominio Active Directory.

# Informazioni correlate

Per ulteriore assistenza, contattare il Cisco Technical Assistance Center (TAC). È necessario un contratto di supporto valido: <u>Contatti del supporto Cisco internazionali.</u>