Configurar a autenticação externa e a autorização via LDAPS para acesso seguro ao Network Analytics Manager

Contents

Introduction **Prerequisites Requirements Componentes Utilizados** Configurar Etapa A. Efetue login no controlador de domínio do AD e exporte o certificado SSL usado para LDAP. Etapa B. Faça login no SNA Manager para adicionar o certificado do servidor LDAP e da cadeia raiz. Etapa C. Adicione a configuração do serviço externo LDAP. SNA versão 7.2 ou posterior SNA versão 7.1 Etapa D. Defina as configurações de autorização. Autorização local Autorização remota via LDAP Verificar Troubleshoot Informações Relacionadas

Introduction

Este documento descreve a configuração básica de um Secure Network Analytics Manager (antigo Stealthwatch Management Center) versão 7.1 ou posterior para usar a autenticação externa e, com a versão 7.2.1 ou posterior, para usar a autorização externa com LDAPS.

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Cisco Secure Network Analytics (antigo Stealthwatch)
- Operação geral LDAP e SSL
- Gerenciamento geral do Microsoft Ative Diretory

Componentes Utilizados

As informações neste documento são baseadas nestes componentes:

- Cisco Secure Network Analytics Manager (anteriormente SMC) versão 7.3.2
- Windows Server 2016 configurado como Controlador de Domínio do Ative Diretory

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Configurar

Etapa A. Efetue login no controlador de domínio do AD e exporte o certificado SSL usado para LDAP.

- 1. No Windows Server 2012 ou posterior, selecione **Executar** no menu Iniciar, digite **certIm.msc** e continue com a etapa **8**.
- 2. Para versões mais antigas do Windows Server, selecione **Executar** no menu Iniciar e digite **mmc**.

×

- 3. No menu Arquivo, selecione Adicionar/remover snap-in.
- 4. Na lista snap-ins disponíveis, selecione Certificados e clique em Adicionar.

Add or Remove Snap-ins

	Vander	^		Edit Extensions
hap-in	vendor			Euri Extensions
Active Directory Do	Microsoft Cor			Remove
Active Directory Site	Microsoft Cor			
Active Directory Use	Microsoft Cor			
ActiveX Control	Microsoft Cor			Move Up
ADSI Edit	Microsoft Cor			Maus Down
Authorization Manager	Microsoft Cor		<pre>< bbb</pre>	Move Down
Certificate Templates	Microsoft Cor		500 Z	
Certificates	Microsoft Cor			
Certification Authority	Microsoft Cor			
Component Services	Microsoft Cor			
Computer Managem	Microsoft Cor			
Device Manager	Microsoft Cor			
Disk Management	Microsoft and	~		Advanced
cription:				
e Certificates snan-in alle	ows you to browse	the	ntents of the certificate stores for yourself a serv	ice, or a computer.
ie Certificates snap-in allo	ows you to browse	the	ntents of the certificate stores for yourself, a serv	ice, or a computer.

- 5. Na janela snap-in Certificados, selecione Conta do computador e selecione Avançar.
- 6. Deixe o computador local selecionado e selecione Concluir.
- 7. Na janela Add or Remove Snap-in, selecione OK.

8. Navegue até Certificados (Computador Local) > Pessoal > Certificados

🚟 certlm - [Certificates - Local Con	nputer\Personal\Certificates]			-		\times
File Action View Help						
🗢 🔿 🙍 📅 🤞 🗙 🛛	1 🗟 🛛 🖬					
🗊 Certificates - Local Computer 🔺	Issued To	Issued By	Expiration Date	Intended Purposes		Frie
✓	angelort-a	angelort-RootCA2	11/25/2022	Client Authentication,	Server Auth.	<n< td=""></n<>
Certificates						
> Trusted Root Certification						
> Contemprise Trust						
> intermediate Certification						
> Trusted Publishers						
> Intrusted Certificates						
> iii Third-Party Root Certifica						
> iii Trusted People						
> Client Authentication Issu						
> Preview Build Roots						
> 🚞 Remote Desktop						
> 📔 Certificate Enrollment Rec						
> iii Smart Card Trusted Roots						
> Trusted Devices						
> 🧮 WebHosting						
Windows Live ID Token Ist						``
	•					
Personal store contains 2 certificates.						

9. Selecione e clique com o botão direito do mouse no certificado SSL usado para autenticação LDAPS em seu controlador de domínio e clique em **Abrir**.

10. Navegue até a guia **Detalhes** > clique em **Copiar para arquivo** > **Avançar**

💼 Certificate

General	Details	Certification F	Path	
Show:	<al></al>		~	
Field See Sig Iss Va Va	rsion rial numbe nature al uer id from id from hiert	er gorithm ash algorithm	Value	
			Edit Properties	Copy to File
				ОК

11. Certifique-se de que Não, não exporte a chave privada está selecionada e clique em Avançar

12. Selecione o formato X.509 codificado em Base-64 e clique em Avançar.

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

Export File Format

Certificates can be exported in a variety of file formats.

ODER	encoded binary X.509 (.CER)
Base	e-64 encoded X.509 (.CER)
Crys	ptographic Message Syntax Standard - PKCS #7 Certificates (.P78)
	Include all certificates in the certification path if possible
Pers	ional Information Exchange - PKCS #12 (.PFX)
	Include all certificates in the certification path if possible
	Delete the private key if the export is successful
	Export all extended properties
	Enable certificate privacy
	osoft Serialized Certificate Store (.SST)

13. Selecione um local para armazenar o certificado, nomeie o arquivo e clique em Avançar.

🔗 Certificate Export V	lizard	
File to Export Specify the name	of the file you want to export	
File name:		
	LDAPSidcerthcate.co	Browse
		Next Cano

14. Clique em **Concluir**, você deve obter um "A exportação foi bem-sucedida". mensagem.

15. Volte para o certificado usado para LDAPS e selecione a guia Caminho de certificação.

16. Selecione o emissor da CA raiz sobre o caminho de certificação e clique em Exibir certificado.

 \sim

Certificate	\times
General Details Certification Path	
Certification path angelort-RootCA2	
View Certificate Certificate status: This certificate is OK.	
	ж

17. Repita as etapas 10-14 para exportar o certificado da CA raiz que assinou o certificado usado para autenticação LDAPS.

Note: Sua implantação pode ter uma hierarquia de CA multicamada, caso em que você precisa seguir o mesmo procedimento para exportar todos os certificados intermediários na cadeia de confiança.

18. Antes de continuar, certifique-se de que tem um ficheiro de certificado para o servidor LDAPS e para cada autoridade emitente no caminho de certificação: Certificado raiz e certificados intermediários (se aplicável).



Etapa B. Faça login no SNA Manager para adicionar o certificado do servidor LDAP e da cadeia raiz.

- 1. Navegue até Central Management > Inventory.
- 2. Localize o dispositivo SNA Manager e clique em Actions > Edit Appliance Configuration.
- 3. Na janela Appliance Configuration, navegue até **Configuration Menu > Trust Store > Add New**.
- 4. Digite o nome amigável, clique em **Escolher arquivo**, selecione o certificado do servidor LDAP e clique em **Adicionar certificado**.
- 5. Repita a etapa anterior para adicionar o certificado CA raiz e os certificados intermediários (se aplicável).
- 6. Verifique se os certificados carregados estão corretos e clique em Aplicar configurações.

Appliance Netwo	ork Services General	and the first state					Configuration Menu V
Trust Store Mod	dified						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			1000		Delete
10 Costificator							

7. Aguarde até que as alterações sejam aplicadas e o status do gerente seja ativado.

Etapa C. Adicione a configuração do serviço externo LDAP.

SNA versão 7.2 ou posterior

1. Abra o painel principal do Gerente e navegue para **Configurações globais > Gerenciamento do usuário**.

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
		te	UDP Director Configuration
			External Lookup Configuration
survey and the second s		and the second se	User Management
8.4			SecureX Configuration
			Select Language

- 2. Na janela Gerenciamento do usuário, selecione a guia Autenticação e autorização.
- 3. Clique em Create > Authentication Service.

cisco Stealthwatch	Dashboards • Monitor • Analyze • Jobs •	Configure • Deploy •		< ⊥ ☆ ±
User Management				
Users Data Roles Authentication and Authorization				Create
				User
				Data Role
Name	∧ Description	Authentication Type	Remote Authorization	Authentication Service
Ex. local	V Filter Authentication Service Description	Ex. LOCAL	~	
	There is n	o data to display		
10 v Items per page			1< <	1/1>>

- 4. No menu suspenso Authentication Service, selecione LDAP.
- 5. Preencha os campos obrigatórios.

Campo Nome amigável Descrição	Notas Digite um nome para oLDAPserver. Digite uma descrição para o servidor LDAP. Insira o nome de domínio totalmente qualificado
Endereço do servidor	 conforme especificado no campo Subject Alterna Name (SAN) (Nome alternativo do assunto) do certificado do servidor LDAP. Se o campo SAN contiver apenas o endereço IPv4, insira o endereço IPv4 no campo Serva Address (Endereço do servidor). Se o campo SAN contiver o nome DNS, insin nome DNS no campo Server Address (Ender do servidor). Se o campo SAN contiver valores de DNS entre do Servidor).
Porta	use o primeiro valor listado. Digite a porta designada para comunicação LDA segura (LDAP sobre TLS). A porta TCP conhecid para LDAPS é 636. Digite a ID de usuário usada para se conectar ao servidor LDAP. Por exemplo: CN=admin,OU=Us Corporativos,DC=exemplo,DC=com
Vincular usuário	Note: Se você adicionou seus usuários a ur contêiner AD integrado (por exemplo, "Usuários"), o DN de vinculação do usuário ter o nome canônico (CN) definido para a pa interna (por exemplo, CN=nome de usuário CN=Usuários, DC=domínio, DC=com). No entanto, se você adicionou seus usuários a novo contêiner, o DN de vinculação deve te unidade organizacional (OU) definida com o novo nome do contêiner (por exemplo, CN=username, OU=Corporate Users, DC=domain, DC=com).

vinculação do usuário de vinculação é consu o Ative Diretory em um Windows Server que tenha conectividade com o Ative Diretory Se Para obter essas informações, você pode at um prompt de comando do Windows e digita comando dsquery user dc= <distinto>,dc=<nome> -name <usuário> exemplo: dsquery user dc=example,dc=com name user1. O resultado parece "CN=user1,OU=Corporate Users,DC=example,DC=com"</usuário></nome></distinto>
Insira a senha do usuário vinculado usada para s conectar ao servidor LDAP. Insira o nome distinto (DN).
O DN se aplica à ramificação do diretório em que
Frequentemente, é o topo da árvore de diretórios domínio), mas você também pode especificar um subárvore dentro do diretório. O usuário vinculad usuários que devem ser autenticados devem esta acessíveis a partir de Contas base.

Por exemplo: DC=exemplo,DC=com

6. Click Save.

Contas básicas

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 Save			
* = 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=zitros ,DC=local			
Password *	Confirm Password *			

7. Se as configurações inseridas e os certificados adicionados ao repositório de confiança estiverem corretos, você deverá obter um banner "Você salvou as alterações com êxito".

8. O servidor configurado deve ser exibido em **User Management > Authentication and Authorization**.

Senha

cisco Stealthwatch	Dashboards • Monitor • Analyze • Jobs • Configure • Deploy •		< ⊥ ☆ ±
User Management			
Users Data Roles Authentication and Authorization			Create ~
Name	∧ Description	Authentication Type	Remote Authorization Actions
Ex. local	V 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 versão 7.1

- 1. Navegue até **Central Management >** Inventory.
- 2. Localize o dispositivo SMC e clique em Actions > Edit Appliance Configuration.
- 3. Na janela Appliance Configuration , navegue até **Configuration Menu > LDAP Setup > Add New**.
- 4. Preencha os campos obrigatórios conforme descrito na **SNA Versão 7.2 ou posterior** etapa 5.

CISCO Stealthwatch Central Management Appliance Manager Update Manager	App Manager	۲
Inventory Appliance Configuration - SMC Appliance Network Services General		Cancel Apply Settings Configuration Menu 🔻
LDAP Setup Add LDAP		Add New
FRENDLY NAME * angelort LDAP server	DESCRIPTION * Main AD server	
SERVIR ADDRESS * angelort-ad- CERTIFICATE REVOCATION • *	PORT * 636 BIND USER @ *	
Disabled PASSWORD *	CN==OU=SNA_OU=Cisco_DC=zitrcDC=local CONFIRM PASSWORD *	
BASE ACCOUNTS + DC+zitro DC+zitro DC+cial		
		Cancel Add

- 5. Clique em Add.
- 6. Clique em Aplicar configurações.

7. Quando as configurações inseridas e os certificados adicionados ao repositório de confiança estiverem corretos, as alterações no Gerenciador serão aplicadas e o estado do aplicativo deverá estar **Ativo**.

Etapa D. Defina as configurações de autorização.

O SNA suporta autorização local e remota via LDAP. Com essa configuração, os grupos LDAP do Servidor AD são mapeados para funções SNA internas ou personalizadas.

Os métodos de autenticação e autorização suportados para SNA via LDAP são:

- Autenticação remota e autorização local
- Autenticação remota e autorização remota (somente compatível com SNA versão 7.2.1 ou posterior)

Autorização local

Nesse caso, os usuários e suas funções precisam ser definidos localmente. Para isso, faça o seguinte:

1. Navegue para Gerenciamento de usuários novamente, clique na guia Usuários > Criar > Usuário.

2. Defina o nome de usuário para autenticar com o servidor LDAP e selecione o servidor configurado no menu suspenso **Authentication Service**.

3. Defina as permissões que o usuário deve ter sobre o Gerenciador depois que ele for autenticado pelo servidor LDAP e clique em **Salvar**.

CISCO Dashboards • Monitor • A	nalyze v Jobs v Configure v Deploy v	< ⊥ ¢ ±
User Management User		Cancel
User Name *	Authentication Service 🖌	
user20	angelort LDAP server v	
Full Name	Password 🕥	
		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		

Autorização remota via LDAP

A Autenticação e Autorização Remotas via LDAP foi suportada pela primeira vez no Secure Network Analytics versão 7.2.1.

Note: A autorização remota com LDAP não é suportada na versão 7.1.

Éimportante mencionar que, se um usuário for definido e ativado localmente (no Gerenciador), o usuário será autenticado remotamente, mas autorizado localmente. O processo de seleção do usuário é o seguinte:

1. Quando as credenciais são inseridas na página de boas-vindas do gerente, o gerente procura um usuário local com o nome especificado.

- Se um usuário local for encontrado e ativado, ele será autenticado remotamente (se a autenticação remota via LDAP com autorização local tiver sido configurada anteriormente), mas autorizado com as configurações locais.
- 3. Se a autorização remota estiver configurada e ativada e o usuário não for encontrado localmente (não configurado ou desativado), tanto a autenticação quanto a autorização serão executadas remotamente.

Por esse motivo, as etapas para configurar com êxito a autenticação remota são..

Etapa D-1. Desabilite ou exclua os usuários destinados a usar autorização remota, mas que são definidos localmente.

- 1. Abra o painel principal do Gerente e navegue até Configurações globais > Gerenciamento do usuário.
- 2. Desabilite ou exclua os usuários (se eles existirem) destinados a usar autenticação e autorização remotas via LDAP, mas configurados localmente.

Us	er Management								
U	sers Data Roles Authentication and	d 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]

Etapa D-2. Defina o cisco-stealthwatch Groups no servidor Microsoft AD.

Para Autenticação externa e autorização via usuários LDAP, as senhas e grupos *cisco-stealthwatch* são definidos remotamente no Microsoft Ative Diretory. Os grupos *cisco-stealthwatch* a serem definidos no servidor AD estão relacionados às diferentes funções que a SNA tem, eles devem ser definidos da seguinte forma.

Função SNA	Nome do(s) grupo(s)
Administrador principal	 cisco-stealthwatch-master-admin
	 cisco-stealthwatch-all-data-read-and-write
	 cisco-stealthwatch-all-data-read-only
	 cisco-stealthwatch-<custom> (opcional)</custom>
Função de dados	Note : Certifique-se de que os grupos de fund de dados personalizados comecem com o "cisco-stealthwatch-".
	 cisco-stealthwatch-configuration-manager
Função funcional da Web	 cisco-stealthwatch-power-analyst
	 cisco-stealthwatch-analyst
	 cisco-stealthwatch-desktop-stealthwatch-pow
	user
Função funcional da área de trabalho	 cisco-stealthwatch-desktop-configuration-ma
· · · · · · · · · · · · · · · · · · ·	 cisco-stealthwatch-desktop-network-engenhe
	 cisco-stealthwatch-desktop-security-analyst
	 cisco-stealthwatch-desktop-<custom> (opcion</custom>

Note: Certifique-se de que os grupos de fund de desktop personalizados comecem com o "cisco-stealthwatch-desktop-".

Active Directory Users and Computers —								
File Action View Help								
🗢 🔿 🙍 📊 🤞 🛤] Q 📑 🛛 🖬 🗏 📚 🛅 🍸 🗾 🍇							
Active Directory Users and C	Name	Туре	Descriptior ^					
> Saved Queries	🎘 cisco-stealthwatch-all-data-read-and-write	Security Group						
Admin	🎘 cisco-stealthwatch-all-data-read-only	Security Group						
> Admin	🎘 cisco-stealthwatch-analyst	Security Group						
	🎘 cisco-stealthwatch-configuration-manager	Security Group						
CISCO	💐 cisco-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	🎘 cisco-stealthwatch-master-admin	Security Group						
> 📔 Managed Service Acc 🗸	acisco-stealthwatch-power-analyst	Security Group	~					
< >	<		>					

Note: Conforme descrito anteriormente, grupos personalizados são suportados para "Função de dados" e "Função funcional da área de trabalho", desde que o nome do grupo seja anexado à sequência correta. Essas funções e grupos personalizados devem ser definidos no SNA Manager e no servidor do Ative Diretory. Por exemplo, se você definir uma função personalizada "custom1" no SNA Manager para uma função de cliente de desktop, ela deverá ser mapeada para cisco-stealthwatch-desktop-custom1 no Ative Diretory.

Etapa D-3. Defina Mapeamentos de grupos de autorização LDAP para os usuários.

Depois que os grupos *cisco-stealthwatch* forem definidos no servidor AD, poderemos mapear os usuários destinados a ter acesso ao SNA Manager para os grupos necessários. Isso deve ser feito da seguinte forma.

• Um usuário administrador principal deve ser atribuído ao grupo *cisco-stealthwatch-master-admin* e não deve ser membro de nenhum outro grupo do *cisco-stealthwatch*.

user20 Properties				? ×	
Remote control	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>		
<				>	
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	

- Cada usuário, além dos usuários do Administrador principal, deve ser atribuído a um grupo de cada função com as próximas condições.
- 1. Função de dados: O usuário deve ser atribuído a apenas um grupo.
- 2. Função funcional da Web: O usuário deve ser atribuído a pelo menos um grupo.
- 3. Função funcional da área de trabalho: O usuário deve ser atribuído a pelo menos um grupo.

snauser10 Properties					?	×	
Remote control	Remote D	esktop Se	rvices Profile		COM+		
General Address Member Of	65	Organiz Session	ns				
Member of: Name Active Directory D cisco-stealthwatch-all-data-read-and-write							
Web Fu Desktop	nctional Ro Functional	e Role				>	
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.							
0	K C	Cancel	Apply		He	dp	

Etapa D-4. Ative a autorização remota via LDAP no SNA Manager.

- 1. Abra o painel principal do Gerente e navegue para **Configurações globais > Gerenciamento do usuário**.
- 2. Na janela User Management, selecione a guia Authentication and Authorization (Autenticação e autorização).
- 3. Localize o serviço de autenticação LDAP configurado na Etapa C.
- 4. Clique em **Ações > Ativar autorização remota**.

Note: Apenas um serviço de Autorização externa pode estar em uso de cada vez. Se outro serviço de autorização já estiver em uso, ele será automaticamente desabilitado e o novo será habilitado, no entanto, todos os usuários autorizados com o serviço externo anterior serão desconectados. Uma mensagem de confirmação é exibida antes que qualquer ação ocorra.

Use	r Manag	gement							
Use	ars Da	ita Roles	Authentication and Authorization						
1	lame			\sim	Description	Authentication Type	1	Remote Authorization	Actions
	Ex. local		· · · · · · · · · · · · · · · · · · ·	-	Filter Authentication Service Description	Ex. LOCAL	2		
a	ngelort LDA	P server			Main AD server	LDAP		~	

Verificar

Os usuários podem fazer logon com as credenciais definidas no servidor do AD.

1	cisco	1
	Welcome user20 K	
	This is your first time logging in.	
	OK	
	Sign In	

A segunda etapa de verificação diz respeito à autorização. Neste exemplo, o usuário "user20" se tornou um membro do grupo *cisco-stealthwatch-master-admin* no servidor AD e podemos confirmar se o usuário tem permissões de Administrador Primário. O usuário não está definido nos usuários locais, portanto podemos confirmar se os atributos de autorização foram enviados pelo servidor do AD.

cisco Stealthwatch	Dashboards •	Monitor * Analyze	 Jobs Configure 	 Deploy * 			۹.	± ≎ ±
User Management							User20 Online Help	_
Users Data Roles Authentication and	Authorization						About	Create 🗸
×							Logout	
User Name	Full Name	Primary Admin 🌖	Config Manager 🔵	Analyst 👩	Power Analyst 😗	Data Role	Status Ac	tions
Ex. jsmlth	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	< 1 / 1 - 2	⊢ >I

A mesma verificação é feita para o outro usuário neste exemplo "snauser10". Podemos confirmar a autenticação com êxito com as credenciais configuradas no servidor AD.



Para a verificação de autorização, como este usuário não pertence ao grupo Administrador primário, alguns recursos não estão disponíveis.

cisco Stealthw	vatch		Dashboards • N	fonitor • Analyze •	Jobs • Configure	 Deploy * 				a 🛓 🎖	*
										Global Settings	
Security Insight Dashboard Inside Hosts									SMC Configuration		
									Packet Analyzer Configuration		
Alarming Hosts									External Lookup Configuration	1	
Concern Index	Target Index	Recon	080	Exploitation	DDoS Source	DDoS Target	Data Hoarding	Exfiltration	Poli	SecureX Configuration	
0		0	0		0			0	1.011	Select Language	
2	0	0	0	0	0	0	0	0		0	-

Troubleshoot

Se a configuração do Serviço de Autenticação não puder ser salva, verifique se:

- 1. Você adicionou os certificados apropriados do servidor LDAP ao armazenamento confiável do gerente.
- 2. O Endereço do Servidor configurado é conforme especificado no campo Nome Alternativo do Assunto (SAN) do certificado do servidor LDAP. Se o campo SAN contiver apenas o endereço IPv4, insira o endereço IPv4 no campo Server Address (Endereço do servidor).Se o campo SAN contiver o nome DNS, insira o nome DNS no campo Server Address (Endereço do servidor).Se o campo SAN contiver valores de DNS e IPv4, use o primeiro

valor listado.

3. Os campos **Vincular usuário** e **Conta base** configurados estão corretos, conforme especificado pelo Controlador de domínio do AD.

Informações Relacionadas

Para obter assistência adicional, entre em contato com o Cisco Technical Assistance Center (TAC). É necessário um contrato de suporte válido: <u>Contatos de suporte da Cisco no mundo inteiro.</u>