通過LDAPS為安全網路分析管理器訪問配置外部 身份驗證和授權

目錄

簡介 必要條件 需求 採用元件 設定 步驟A.登入到AD域控制器並匯出用於LDAP的SSL證書。 步驟B.登入到SNA Manager以新增LDAP伺服器的證書和根鏈。 步驟C.新增LDAP外部服務配置。 SNA 7.2或更高版本 SNA版本7.1 步驟D.配置授權設定。 本地授權 通過LDAP進行遠端授權 驗證 疑難排解 相關資訊

簡介

本檔案介紹安全網路分析管理員(前身為Stealthwatch管理中心)版本7.1或更高版本的基本設定 ,以使用外部驗證,並在7.2.1或更高版本中使用外部授權與LDAPS。

必要條件

需求

思科建議您瞭解以下主題:

- Cisco Secure Network Analytics (前身為Stealthwatch)
- 常規LDAP和SSL操作
- 常規Microsoft Active Directory管理

採用元件

本檔案中的資訊是根據以下元件:

- •思科安全網路分析管理員(前身為SMC)版本7.3.2
- 配置為Active Directory域控制器的Windows Server 2016

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除(預設

)的組態來啟動。如果您的網路運作中,請確保您瞭解任何指令可能造成的影響。

設定

Add as Demons Course

步驟A.登入到AD域控制器並匯出用於LDAP的SSL證書。

- 1. 對於Windows Server 2012或更高版本,從「開始」選單中選擇**運行**,然後輸入 certIm.msc,然後繼續執行步驟8。
- 2. 對於較舊的Windows Server版本,從「開始」選單中選擇「運行」,然後輸入mmc。

 \times

- 3. 從「檔案」(File)選單中,選擇「新增/刪除管理單元」(Add/Remove Snap In)。
- 4. 從可用管理單元清單中,選擇證書,然後按一下新增。

Add or Remove Shap-ins								
You can select snap-ins for extensible snap-ins, you car	this console from th n configure which e	iose xten	available on your computer and configure the selected solutions are enabled.	set of snap-ins. For				
Available snap-ins:			Selected snap-ins:					
Snap-in	Vendor	^	Console Root	Edit Extension				
		·						

Snap-in	Vendor	^		Console Root	Edit Extensions
Active Directory Do	Microsoft Cor				Demove
Active Directory Site	Microsoft Cor				Kellove
Active Directory Use	Microsoft Cor				
📹 ActiveX Control	Microsoft Cor				Move Up
📝 ADSI Edit	Microsoft Cor				Maria Davia
Authorization Manager	Microsoft Cor		Add		Move Down
Certificate Templates	Microsoft Cor		- Aug 2		
🙀 Certificates	Microsoft Cor				
Certification Authority	Microsoft Cor				
🙆 Component Services	Microsoft Cor				
Computer Managem	Microsoft Cor				
🖶 Device Manager	Microsoft Cor				
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	e, or a computer.
				_	
				L	OK Cancel

5.在「**證書」管理單元視窗**中,選擇「**電腦帳戶**」,然後選擇「下一步」。

6.保持選中Local computer,然後選擇Finish。

7.在「新增**或刪除管理單元」視窗中**,選擇「確定」。

8.導航到證書(本地電腦)>個人>證書



Personal store contains 2 certificates.

9.選擇並按一下右鍵域控制器上用於LDAPS身份驗證的SSL證書,然後按一下開啟。

10.定位至「詳細資訊」選**項卡>**按一下「複製**到檔案」>**「下一**步」**

General	ficate Details	Certification F	Path	×
Show:	<all></all>		~	
Field Se Sig Sig Sig Va Va	rsion rial numbe pnature al pnature ha suer lid from lid from hiert	er gorithm ash algorithm	Value	
			Edit Properties	Copy to File
				ОК

11.確保選中No, do not export private key, 然後單擊Next

12.選擇Base-64 encoded X.509 format,然後按一下Next。

Expo	rt File Format Certificates can be exported in a variety of file formats.
	Select the format you want to use:
	O DER encoded binary X.509 (.CER)
	Base-64 encoded X.509 (.CER)
	O Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P78)
	Include all certificates in the certification path if possible
	Personal 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
	Microsoft Serialized Certificate Store (.SST)

13.選擇儲存證書的位置,命名檔案,然後按一下**下一步**。

Sertificate Export Wizard	
File to Export Specify the name of the file you want to export	
	_
Eie come	
LDAPSidcertificate.cer Browse	
Next Canc	el

14.按一下**Finish**,必須獲得「The export was successful」(匯出成功)。 消息。

15.返回用於LDAPS的證書,然後選擇Certification Path頁籤。

16.選擇證書路徑頂部的根CA頒發者,然後按一下View Certificate。

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

17.重複步驟10-14以匯出對用於LDAPS身份驗證的證書進行簽名的根CA的證書。

附註:您的部署可以具有多層CA層次結構,在這種情況下,您需要遵循相同的過程匯出信任 鏈中的所有中間證書。

18.繼續之前,請確保LDAPS伺服器和證書路徑中的每個頒發機構都有一個證書檔案:根憑證和中間憑證(如果適用)。

📕 🗹 📕 🖛 I L	DAPS certificates						- 0	×
File Home	Share View							^ 🕐
Pin to Quick Copy access	Paste	Move Copy to * Cot	New item ▼ New folder	Properties	Select all Select none			
c	lipboard	Organize	New	Open	Select			
← → ~ ↑]	A REAL PROPERTY.	LDAPS certificates				~ Ō	Search LDAPS certificates	P
Name Date modified Type Size								
	LDAPS_Root	1/25/2021 11:46 Security	Certificate 3	KB				
	LDAPSidcert	ificate 1	/24/2021 7:59 PM Security	Certificate 3	KB			

步驟B.登入到SNA Manager以新增LDAP伺服器的證書和根鏈。

1. 導航到Central Management > Inventory。

- 2. 找到SNA Manager裝置,然後按一下操作>編輯裝置配置。
- 3. 在Appliance Configuration視窗中, 導航至Configuration Menu > Trust Store > Add New。
- 4. 鍵入友好名稱,按一下選擇檔案並選擇LDAP伺服器的證書,然後按一下新增證書。
- 5. 重複上一步新增根CA證書和中間證書(如果適用)。
- 6. 確認上傳的憑證是否正確,然後按一下「Apply Settings」。

Trust Store Modified Actions FRIENDLY NAME ISSUED TO ISSUED BY VALID FROM VALID TO SERIAL NUMBER KEY LENGTH ACTIONS LDAP-Server appellort-ad- appellort-RootCA2 Delete Delete
FRIENDLY NAME ISSUED TO ISSUED BY VALID FROM VALID TO SERIAL NUMBER KEY LENGTH ACTIONS LDAP-Server angelort-RootCA2 Delete
LDAP-Server angelort-RootCA2
LDAP-Server angelort-ad- angelort-RootCA2
LDAP-server-RootCA angelort-RootCA2 angelort-RootCA2 Delete

7.等待應用更改,並等待Manager狀態變為Up。

步驟C.新增LDAP外部服務配置。

SNA 7.2或更高版本

1.開啟Manager主控制面板,然後導航至全域性設定 > 使用者管理。

cisco Stealthwatch	Dashboards • Monitor • Analyze • Jobs • Configure •	 Deploy • 	د 💶 🗢 ±
			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 s		sections are set as a section of the	User Management
8.4			SecureX Configuration
			Select Language

2.在「使用者管理」視窗中,選擇Authentication and Authorization選項卡。

3.按一下建立 > 身份驗證服務。

cisco Stealthwatch	Dashboard:	 Monitor • 	Analyze *	Jobs *	Configure *	Deploy *				९ 🛓 🌣 ±
User Management										
Users Data Roles Authentication and Authorization										Create ~
										Data Role
Name	∧ Desc	iption					Authentication Type		Remote Authorization	Authentication Service
Ex. local	 ✓ Filte 	Authentication Se	rvice Descriptio	n			Ex. LOGAL	~		
There is no data to display										
10 v Items per page										
10 v items per page									1< <	1/1>>

4.從Authentication Service下拉選單中選擇LDAP。

5.填寫必填欄位。

欄位

友好名稱 說明

伺服器位址

連接埠

繫結使用者

密碼

基本帳戶

6.按一下儲存。

備註

輸入LDAP伺服器的名稱。

輸入LDAP伺服器的說明。

輸入在LDAP伺服器證書的Subject Alternative Name(SAN)欄位中指定的完全限定的域名。

- 如果SAN欄位僅包含IPv4地址,請在Server Address欄位中輸入IPv4地址。
- 如果SAN欄位包含DNS名稱,請在Server Address欄位中輸入DNS名稱。
- 如果SAN欄位同時包含DNS和IPv4值,請使用 的第一個值。

輸入為安全LDAP通訊(通過TLS的LDAP)指定的 LDAPS的公認TCP埠是636。

輸入用於連線到LDAP伺服器的使用者ID。例如 : CN=admin, OU=Corporate Users, DC=example, DC=com

> **附註**:如果將使用者新增到內建AD容器(例 「使用者」),則繫結使用者的繫結DN必 規範名稱(CN)設定為內建資料夾(例如 , CN=username, CN=Users, DC=domai DC=com)。 但是,如果已將使用者新增到新 器,則繫結DN必須將組織單位(OU)設定為新 名稱(例如, CN=username, OU=Corpora Users, DC=domain, DC=com)。

> **附註**:查詢繫結使用者的繫結DN的一個有用 是查詢與Active Directory伺服器連線的Windo Server上的Active Directory。若要獲取此資訊 ,您可以開啟Windows命令提示符並鍵入命令 dsquery user dc=<distinguished>,dc=<name name <user>。例如: dsquery user dc=example,dc=com-name user1。結果類 CN=user1,OU=Corporate Users, DC=example, DC=com_

輸入用於連線到LDAP伺服器的繫結使用者密碼。 輸入唯一判別名(DN)。 DN適用於必須開始搜尋使用者的目錄分支。它通知 於目錄樹(您的域)的頂部,但是您也可以在目銷 定子樹。「繫結使用者」和要進行身份驗證的使用 須可從基本帳戶訪問。

例如:DC=example,DC=com

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=sOU=SNA,OU=Cisco,DC=zitrosDC=local
Certificate Revocation 🔘 •	Base Accounts 📀 *
Disabled V	DC=zitros ,DC=local
Password *	Confirm Password *

7.如果輸入的設定和新增到信任儲存的證書正確,您必須收到「您已成功儲存更改」的橫幅。

8.已配置的伺服器必須顯示在User Management > Authentication and Authorization下。

cisco Stealthwatch	Dashboards • Monitor • Analyze • Jobs • Configure • Deploy	•	Q 💶 🌣 ±
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 ~	
angelort LDAP server	Main AD server	LDAP	
10 v Items per page			1 - 1 of 1 items < < 1 / 1 > >

SNA版本7.1

- 1. 導航到Central Management > Inventory。
- 2. 找到SMC裝置,然後按一下**操作 > 編輯裝置配置**。
- 3. 在Appliance Configuration視窗中, 導航到Configuration Menu > LDAP Setup > Add New。
- 4. 按照SNA 7.2版或更高版本中的說明完成必填欄位,步驟5。

cisco Stealthwatch Central Ma	anagement Appliance Manager	Update Manager A	ipp Manager		۲
Inventery / Appliance Configuration Appliance Configuration Appliance N	nfiguration - SMC etwork Services General			Cancel Apply Settings Configuration Menu 🕈	
LDAP Setup				Add New	
FRENDLY NAME * angelort LDAP	server		DESCRIPTION * Main AD server		
SERVER ADDRESS angelort-ad-	•		PORT * 636		
CERTIFICATE REVO Disabled	XCATION @ *	~	BIND USER • * CN==,OU=SNA,OU=Cisco,DC=zitrc,DC=local		
PASSWORD *			CONFIRM PASSWORD *		
BASE ACCOUNTS DC=zitro	DC=local				
				Cancel Add	

5.按一下Add。

6.按一下**應用設定**。

7.一旦輸入的設定和新增到信任儲存的證書正確無誤,就會應用Manager上的更改,並且裝置狀態 必須為**Up**。

步驟D.配置授權設定。

SNA同時支援通過LDAP進行的本地和遠端授權。通過此配置,AD伺服器的LDAP組對映到內建或 自定義SNA角色。

通過LDAP支援SNA的身份驗證和授權方法有:

- 遠端身份驗證和本地授權
- 遠端身份驗證和遠端授權(僅支援SNA 7.2.1版或更高版本)

本地授權

在這種情況下,需要在本地定義使用者及其角色。為此,請按照以下步驟操作。

1.再次定位至使用者管理,按一下使用者標籤>建立>使用者。

2.定義要使用LDAP伺服器進行身份驗證的使用者名稱,並從Authentication Service下拉選單中選擇 配置的伺服器。

3.定義經LDAP伺服器驗證後,使用者對Manager必須擁有的許可權,然後按一下Save。

Dashboards • Monitor • Av	nalyze * Jobs * Configure * Deploy *	< ⊥ ⇔ ±
User Management User		Cancel Save
User Name * user20 Full Name	Authentication Service angelort LDAP server Password	Generate Password
Email	Confirm Password	
Role Settings Primary Admin Data Role All Data (Road & Write)		
Web Desktop Web Roles Compare		
Configuration Manager Analyst Power Analyst		

通過LDAP進行遠端授權

Secure Network Analytics 7.2.1版首次支援通過LDAP進行遠端身份驗證和授權。

附註:7.1版不支援使用LDAP進行遠端授權。

- 需要提及的是,如果使用者是在本地(在Manager中)定義和啟用的,則使用者是遠端身份驗證的 ,但在本地授權。使用者選擇過程如下:
 - 1. 在Manager的歡迎頁上輸入憑據後,Manager將查詢具有指定名稱的本地使用者。
 - 如果找到本地使用者並啟用該使用者,則遠端驗證該使用者(如果之前配置了具有本地授權的 LDAP遠端驗證),但使用本地設定進行授權。
 - 如果已配置和啟用遠端授權,且未在本地找到使用者(未配置或禁用),則遠端執行身份驗證 和授權。

因此,成功配置遠端身份驗證的步驟是:

步驟D-1.禁用或刪除打算使用遠端授權但在本地定義的使用者。

- 1. 開啟Manager主儀表板並導航到Global Settings > User Management。
- 2. 禁用或刪除通過LDAP使用遠端身份驗證和授權的使用者(如果存在),但是這些使用者是在 本地配置的。

Us	er Management									
U	sers Data Roles Authentication and	Roles Authentication and Authorization								
	User Name	Full Name	Primary Admin 🌖	Config Manager 😑	Analyst 😗	Power Analyst 🕚	Data Role	Status	Actions	
	Ex. jsmith	Ex. "John Smith"					Ex. "All Date(Read & Write)"	Ex. On		
	admin	Admin User	~				All Data (Read & Write)	C On		
	angelort	Angel Ortiz	~				All Data (Read & Write)	C On		
	user20			~	~		All Data (Read & Write)	O off		

步驟D-2.在Microsoft AD伺服器中定義cisco-stealthwatch組。

對於通過LDAP使用者的外部身份驗證和授權,密碼和*cisco-stealthwatch*組在Microsoft Active Directory中遠端定義。要在AD伺服器中定義的*cisco-stealthwatch*組與SNA具有的不同角色相關 ,它們必須定義如下。

SNA角色 主管理員	組名稱 • cisco-stealthwatch-master-admin • cisco-stealthwatch-all-data-read-and-write
資料角色	• cisco-stealthwatch-all-data-read-only • cisco-stealthwatch- <custom>(可選) 附註:確保自定義資料角色組以「cisco- stealthwatch — 」開頭。</custom>
Web功能角色	 cisco-stealthwatch-configuration-manager cisco-stealthwatch-power-analyst cisco-stealthwatch-analyst cisco-stealthwatch-desktop-stealthwatch-powuser
案頭功能角色	 cisco-stealthwatch-desktop-configuration-ma cisco-stealthwatch-desktop-network-enginee cisco-stealthwatch-desktop-security-analyst cisco-stealthwatch-desktop-<custom>(可選)</custom>
	附註 :確保自定義案頭功能角色組以「cisco- stealthwatch-desktop — 」開頭。

Active Directory Users and Computers - [
File Action View Help										
← ⇒ 2 📷 ¼ 📋 🗙 🗒 @ 🐟 🛛 📷 🐍 📚 🛅 🍸 🧕 象										
Active Directory Users and Cr A	Name	Туре	Descriptior ^							
> Saved Queries	🕮 cisco-stealthwatch-all-data-read-and-write	Security Group								
A davia	🕮 cisco-stealthwatch-all-data-read-only	Security Group								
> Admin	🎕 cisco-stealthwatch-analyst	Security Group								
> Builtin	💐 cisco-stealthwatch-configuration-manager	Security Group								
CISCO	🕮 cisco-stealthwatch-custom1	Security Group								
and 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	acisco-stealthwatch-desktop-security-analyst	Security Group								
> 📓 Domain Controllers	acisco-stealthwatch-desktop-stealthwatch-power-user	Security Group								
> 📔 ForeignSecurityPrinci	🎘 cisco-stealthwatch-master-admin	Security Group								
> 📔 Managed Service Acc 🗸	acisco-stealthwatch-power-analyst	Security Group	~							
< >	<		>							

附註:如前所述,只要組名前面有正確的字串,則支援「資料角色」和「案頭功能角色」自定 義組。必須在SNA Manager和Active Directory伺服器中定義這些自定義角色和組。例如,如 果您在SNA Manager中為案頭客戶端角色定義自定義角色「custom1」,則必須將其對映到 Active Directory中的cisco-stealthwatch-desktop-custom1。

步驟D-3.定義使用者的LDAP授權組對映。

在AD伺服器中定義*cisco-stealthwatch*組後,我們可以將想要訪問SNA Manager的使用者對映到必要的組。必須按以下步驟操作。

• Primary Admin使用者必須分配給*cisco-stealthwatch-master-admin*組,且不能是任何其他 *cisco-stealthwatch*組的成員。

user20 Properties				?	\times					
Remote control General Address Member Of	Remote control Remote Desktop Services Profile General Address Account Profile Telephones Member Of Dial-in Environment									
Member of: Name Pri cisco-stealthwatch-m	mary Admin aster-admin		Active Dir ztrosyster	ectory Do ns.local/C	ma Jisc					
Domain Users			zitrosyster	ns Jocal/U	lse					
٢					>					
Add R	emove				_					
Primary group: Domain Users Set Primary Group There is no need to change Primary group unless you have Macintosh clients or POSIX-compliant applications.										
OF	(C	ancel	Apply	H	elp					

•除主管理員使用者以外的每個使用者都必須分配到具有下一個條件的每個角色組。

- 1. 資料角色:使用者必須僅分配到一個組。
- 2. Web功能角色:必須將使用者分配至至少一個組。
- 3. 案頭功能角色:必須將使用者分配至至少一個組。

nauser10 Properties					?	×
Remote control General Address	Remote D Account	Remote Desktop Services Pro Account Profile Telepho			CO Organia	M+ tation
Member of:	Dial-In	Envi	ronment		Sessio	ns
Name cisco-steathwatch-a cisco-steathwatch-c cisco-steathwatch-d Data Ro Web Fu	I-data-read-an ontiguration-m esktop-configu esktop-configu le nctional Ro	d-write anager uration-mar) nager	Active (Directory	D
Cesktop	Functional	Role				>
Add F	amain Users There is n you have application	o need to o Macintosh ns.	change Prir clients or F	many gr POSIX-	oup unle complian	155 t
0	((Cancel	Apply	y	He	slp

步驟D-4.在SNA管理器上通過LDAP啟用遠端授權。

- 1. 開啟Manager主控制面板,然後導航至全域性設定 > 使用者管理。
- 2. 在User Management視窗中,選擇Authentication and Authorization頁籤。
- 3. 找到在步驟C中配置的LDAP身份驗證服務。
- 4. 按一下Actions > Enable Remote Authorization。

附註:一次只能使用一個外部授權服務。如果另一個授權服務已在使用中,則會自動禁用該授 權服務並啟用新的授權服務,但所有通過以前的外部服務獲得授權的使用者都將註銷。在任何 操作發生之前都會顯示確認消息。

Use	er Man	agement					
Us	iers	Data Roles	Authentication and Authorization				
	Name			Description	Authentication Type	Remote Authorization	Actions
	Ex. local	I	~	Filter Authentication Service Description	Ex. LOCAL V		
	angelort l	LDAP server		Main AD server	LDAP	~	

驗證

使用者可以使用在AD伺服器上定義的憑據登入。



第二個驗證步驟與授權有關。在本例中,使用者「user20」成為AD伺服器中*cisco-stealthwatch-master-admin*組的成員,我們可以確認該使用者具有Primary Admin許可權。本地使用者中未定義 使用者,因此我們可以確認Authorization屬性是由AD伺服器傳送的。

cisco	Stealthwatch	Dashboards *	Monitor * Analyze	• Jobs • Configure	Deploy			۹	1	\$ ±
								user20		
User Ma	anagement							Online Help		
								Resources		
Users	Data Roles Authentication and	I Authorization						About	1	Create 🗸
×								Logout		
User N	lame	Full Name	Primary Admin ()	Config Manager 🔵	Analyst 😗	Power Analyst 💿	Data Role	Status A	ctions	
Ex. js	smith	Ex. "John Smith"					Ex. "All Data(Read & Write)"	Ex. On		
admin	1	Admin User	~				All Data (Read & Write)	🕥 On		
1	10 v items per page						1 - 1 of 1 items	< 1 / 1	> :	

在本示例「snauser10」中對其他使用者執行相同的驗證。 我們可以使用AD伺服器上配置的憑據確 認身份驗證成功。



對於授權驗證,由於此使用者不屬於主要管理員組,因此某些功能不可用。

cisco	Stealthwa	atch		Dashboards • M	fonitor • Analyze •	Jobs • Configure	 Deploy * 				 ▲ ĝ 	+
											Global Settings	
Sec	urity Insight Da	shboard Inside H	losts								SMC Configuration	
											Packet Analyzer Configuration	
Alar	ming Hosts 0										External Lookup Configuration	1
	Concern 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	

疑難排解

如果無法成功儲存身份驗證服務的配置,請驗證:

- 1. 您已將LDAP伺服器的正確證書新增到Manager的信任儲存中。
- 2. 配置的Server Address在LDAP伺服器證書的Subject Alternative Name(SAN)欄位中指定。如果SAN欄位僅包含IPv4地址,請在Server Address欄位中輸入IPv4地址。如果SAN欄位包含DNS名稱,請在Server Address欄位中輸入DNS名稱。如果SAN欄位同時包含DNS和IPv4值,請使用列出的第一個值。
- 3. 配置的Bind User和Base Account欄位正確,如AD域控制器所指定。

相關資訊

如需其他協助,請聯絡思科技術協助中心(TAC)。需要有效的支援合約: <u>思科全球支援聯絡人.</u>