在透過 FMC 管理的 FTD 上,針對 AnyConnect 用戶端設定 AD (LDAP) 驗證和使用者身分識別

目錄

簡介 必要條件 需求 採用元件 背景資訊 設定 網路圖表和案例 Active Directory配置 確定LDAP基本DN和組DN 建立FTD帳戶 建立AD組並將使用者新增到AD組(可選) 複製LDAPS SSL證書根(僅對於LDAPS或STARTTLS是必需的) FMC配置 驗證許可 設定領域 配置AnyConnect進行AD身份驗證 <u>啟用身份策略並</u>為使用者身份配置安全策略 配置NAT免除 部署 驗證 最終配置 AAA組態 AnvConnect配置 使用AnyConnect連線並驗證訪問控制策略規則 使用FMC連線事件進行驗證 疑難排解 調試 正在運行的LDAP調試 無法與LDAP伺服器建立連線 繫結登入DN和/或密碼不正確 LDAP伺服器找不到使用者名稱 使用者名稱密碼不正確 測試AAA 封包擷取 Windows Server事件檢視器日誌

簡介

本檔案介紹如何為連線至Cisco Firepower威脅防禦(FTD)的AnyConnect使用者端設定AD驗證。

必要條件

需求

思科建議您瞭解以下主題:

- FMC上的RA VPN配置基礎知識
- FMC上的LDAP伺服器配置基礎知識
- Active Directory(AD)基礎知識

採用元件

本文中的資訊係根據以下軟體和硬體版本:

- Microsoft 2016伺服器
- 運行6.5.0的FMCv
- 執行6.5.0的FTDv

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。

背景資訊

本檔案介紹如何為連線到Cisco Firepower**威脅防禦(FTD)**(由Firepower管理中心(FMC)管理)的 AnyConnect使用者端設定Active Directory(AD)驗證。

使用者身份用於訪問策略中,以將AnyConnect使用者限製為特定IP地址和埠。

設定

網路圖表和案例



Windows伺服器預配置了IIS和RDP以測試使用者身份。在此配置指南中,建立了三個使用者帳戶和 兩個組。

使用者帳戶:

- FTD管理員:它用作目錄帳戶,以允許FTD繫結到Active Directory伺服器。
- IT管理員:用於演示使用者身份的測試管理員帳戶。
- 測試使用者:用於演示使用者身份的測試使用者帳戶。

組:

- AnyConnect管理員:新增IT管理員以演示使用者身份的測試組。此組僅具有對Windows Server的RDP訪問許可權。
- AnyConnect使用者:新增測試使用者以演示使用者身份的測試組。此組僅具有對Windows Server的HTTP訪問許可權。

Active Directory配置

若要在FTD上正確設定AD驗證和使用者身分,需要幾個值。

在FMC上完成配置之前,必須在Microsoft伺服器上建立或收集所有這些詳細資訊。主要值包括:

• 域名:

這是伺服器的域名。在此配置指南中, example.com是域名。

• 伺服器IP/FQDN地址:

用於訪問Microsoft伺服器的IP地址或FQDN。如果使用FQDN,則必須在FMC和FTD中配置DNS伺服器以解析FQDN。

在本配置指南中,此值為win2016.example.com(解析為192.168.1.1)。

•伺服器端口:

LDAP服務使用的埠。預設情況下,LDAP和STARTTLS將TCP埠389用於LDAP,而LDAP over SSL(LDAPS)使用TCP埠636。

•根CA:

如果使用LDAPS或STARTTLS,則需要使用根CA來對LDAPS使用的SSL證書進行簽名。

•目錄使用者名稱和密碼:

這是FMC和FTD用於繫結到LDAP伺服器、對使用者進行身份驗證以及搜尋使用者和組的帳戶。

為此建立了一個名為FTD Admin的帳戶。

•基本和群組可分辨名稱(DN):

基礎DN是FMC的起點,FTD會告知Active Directory開始搜尋和驗證使用者。

同樣,組DN是起點,FMC會告知Active Directory從何處開始搜尋使用者身份組。

在本配置指南中,根域example.com用作基礎DN和組DN。

但是,對於生產環境,在LDAP層次結構中進一步使用Base DN和Group DN會更好。

例如,此LDAP層次結構:



如果管理員希望**Marketing**組織單位中的使用者能夠驗證基本DN,可以將基本DN設定為根 (example.com)。

但是,這也允許Finance組織單位下的User1登入,因為使用者搜尋從根使用者開始,然後轉到 Finance、Marketing和Research。

基本DN設定為example.com



為了將登入限製為Marketing組織單位及以下單位中的唯一使用者,管理員可以將Base DN設定為 Marketing。

現在只有User2和User3能夠進行身份驗證,因為搜尋從Marketing開始。

基本DN設定為Marketing



請注意,為了在FTD內進行更精細的控制(允許使用者連線或根據使用者的AD屬性為其分配不同的 授權),需要配置LDAP授權對映。

有關此操作的詳細資訊,請參閱<u>:在Firepower威脅防禦(FTD)上配置AnyConnect LDAP對映</u>。

此簡化的LDAP層次結構用於此配置指南,根example.com的DN用於基礎DN和組DN。



確定LDAP基本DN和組DN

1.開啟Active Directory使用者和電腦。



2.左鍵按一下根域(開啟容器),按一下右鍵根域,然後在View下按一下Advanced Features。



3.這將啟用AD對象下其他屬性的檢視。例如,要查詢根example.com的DN,請按一下右鍵 example.com,然後選擇**Properties**。



4.在**屬性**下,選擇**屬性編輯器**頁籤。在Attributes下查詢distinguishedName,然後按一下View。

example.com Properties		?	×
General Managed By O	bject Security Attribute Editor		
Attributes:			
Attribute	Value		^
dc defaultLocalPolicyObj description desktopProfile displayName displayNamePrintable displayNamePrintable distinguishedName	example <not set=""> <not set=""> <not set=""> <not set=""> <not set=""> DC=example,DC=com</not></not></not></not></not>		
domainPolicyObject	(not set)		
dSASignature dSCorePropagationD eFSPolicy extensionName Boos	{V1: Rags = 0x0; LatencySecs 0x0 = () <not set=""> <not set=""></not></not>	= 0; DsaGuio	
<	<not set=""></not>	>	
View		Filter	
OK	Cancel Apply	Hel	p

5.這將開啟一個新視窗,以後可以在其中複製並貼上到FMC中。在本示例中,根DN是

複製值儲存以備以後使用。按一下OK以退出「String Attribute Editor」視窗,然後再次按一下「OK」以退出「Properties」。

tring Attribute Editor		х	
ttribute: distingui	ishedName		
alue:		-L	
Clear	OK Cancel		Cut
			Сору
			Paste
			Delete
			Select All
			Right to left Reading order
			Show Unicode control characters
			Insert Unicode control character
General Managed By C Attributes:	bject Security Attribute Editor		
Attribute	Value ^		
cn	<not set=""></not>		
controlAccessRights	<pre><not set=""> 4/29/2020 2:42:49 PM Eastern Daulight Tim</not></pre>		
de	example		
defaultLocalPolicyObj	<not set=""></not>		
description	<not set=""></not>		
desktopProfile displayName	(not set)		
displayNamePrintable	(not set)		
distinguishedName	DC=example,DC=com		
domainPolicyObject	<not set=""></not>		
domainReplica	<not set=""></not>		
dSASignature	{ V1: Hags = 0x0; LatencySecs = 0; DsaGuic		
 dSCorePropagationD 	UXU = ()		
View	Fiter		
ОК	Cancel Apply Help		

這可以對**Active** Directory中的多個對象執**行此操作**。例如,以下步驟用於查詢**User** container的DN:



6.再次按一下右鍵根DN,然後在View下再次按一下Advanced Features,可以刪除Advanced Features檢視。



建立FTD帳戶

此使用者帳戶允許FMC和FTD與Active Directory繫結,以搜尋使用者和組並對使用者進行身份驗證。

建立單獨的FTD帳戶的目的是,在用於繫結的憑證遭到破壞時,防止網路中其他地方的未經授權存 取。

此帳戶無需在基本DN或組DN範圍內。

1.在Active Directory使用者和電腦中,按一下右鍵FTD帳戶新增到的容器/組織。

在此組態中,FTD帳戶會新增到使用者名稱ftd.admin@example.com下Users容器下方。

按一下右鍵Users,然後導航到New > User。

Active Directory Users and Computers							-	×
File Action Vi	File Action View Help							
🗢 🔿 🖂 🚾	⊨⇒ 2 🖬 4 🗉 🗙 🖫 @ 🕞 🛛 🖬 % № 🖄 🔻 🧕 %							
Active Director Saved Quer Saved Quer S	y Users and Com ries om iters o Controllers SecurityPrincipal: ed Service Accour Delegate Con Find	Name DefaultAcc Denied RO DonsAdmin DosUpdate Domain Ac Domain Ac Domain Co	:o D s :P d n e	Type User Security Group Security Group Security Group Security Group Security Group Security Group	Description A user account manage Members in this group c. DNS Administrators Gro DNS clients who are per Designated administrato. All workstations and ser All domain controllers i All domain guests	•		^
[New All Tasks View Refresh Export List	>	ers	Computer Contact Group InetOrgPerson msDS-KeyCreder msDS-ResourceP	ntial PropertyList			
< Creates a new item	Properties Help	WseAllertA WseAllow WseAllow		msDS-ShadowPr msImaging-PSPs MSMQ Queue Al Printer User Shared Folder	incipalContainer ias		_	~

2.完成「新建**對象 — 使用者」**嚮導。

New Object - User		х
🤱 Create in:	example.com/Users	
First name:	FTD Initials:	
Last name:	Admin	
Full name:	FTD Admin	
User logon name:		
ftd.admin	@example.com ~	
User logon name (pre		
EXAMPLE\	ftd.admin	
	< Back Next > Cance	4

New Object - User			×		
Create in: example.com/Users					
Password:	•••••				
Confirm password: User must change password at next logon User cannot change password Password never expires Account is disabled					
	< Back	Next >	Cancel		
New Object - User			×		
New Object - User Create in: exam When you click Finish, the fol Full name: FTD Admin	ple.com/Users lowing object will be c	reated:	×		
New Object - User Create in: exam When you click Finish, the fol Full name: FTD Admin User logon name: ftd.admin@ The exercise	ple.com/Users lowing object will be c Pexample.com	reated:	×		
New Object - User Create in: exam When you click Finish, the fol Full name: FTD Admin User logon name: ftd.admin@ The password never expires.	ple.com/Users lowing object will be c	reated:	×		

3.驗證是否已建**立FTD**帳戶。另外建立了兩個帳戶:IT管理員和測試用戶。

Active Directory Users and Com	-		×				
File Action View Help	File Action View Help						
🗢 🔿 🙋 🚾 🔏 🗈 🗶 🛛	i 🗟 🔒 🔽 🖬	1 🙎 🔌 🛍 🤋	r 🔟 🗽				
Active Directory Users and Com Saved Queries Saved Queries Save	Name DefaultAcco Denied ROD Denied ROD Domain Rod Domain Ad Domain Co Domain Co Domain Co Domain Co Domain Gue Domain Gue Domain Gue Domain Gue Domain Gue Domain Gue Comain Gue Enterprise A Enterprise R Enterprise R.	Type User Security Group Security Group User User User Security Group Security Group Security Group Security Group Security Group Security Group Security Group	Description A user account manage Members in this group c DNS Administrators Gro DNS clients who are per DNS clients who are per Designated administrato All workstations and ser All domain controllers i All domain guests All domain guests All domain users Designated administrato Members of this group Members of this group Designated administrato			^	
< >>		A 1 A				~	

建立AD組並將使用者新增到AD組(可選)

雖然身份驗證不需要使用組,但可以使用組來簡化將訪問策略應用至多個使用者以及LDAP授權的 過程。

在此配置指南中,組用於稍後通過FMC中的使用者標識應用訪問控制策略設定。

1.在Active Directory使用者和電腦中,按一下右鍵新組新增到其中的容器或組織單元。

在本示例中,組AnyConnect Admins被新增到**Users**容器下。按一下右鍵**Users**,然後導航到**New >** Group。

Active Directory Users and Com	puters			-		х	
File Action View Help	File Action View Help						
🗢 🔿 🙋 🚾 🔏 🗈 🛠 🛙	← ⇔ 2 📷 ¾ 🗈 💥 🗟 @ 💀 🛛 📷 🖏 📚 🛍 🍸 💆 ‰						
Active Directory Users and Com Saved Queries Saved Queries Save	Name DefaultAcco Denied ROD DisAdmins DisUpdateP Domain Ad Domain Ad Domain Co	Type User Security Group Security Group Security Group Security Group Security Group Security Group Security Group	Description A user account manage Members in this group c DNS Administrators Gro DNS clients who are per Designated administrato All workstations and ser All domain controllers i All domain guests			~	
New All Tasks View Refresh Export List Properties Help	> > > Read-only	Computer Contact Group InetOrgPerson msDS-KeyCreder msDS-ResourceP msDS-ShadowPr msImaging-PSPs MSMQ Queue Al	ntial PropertyList incipalContainer				
< >> Creates a new item in this container.	Schema A	Printer User Shared Folder				~	

2.完成「新建**對象 — 組」向**導。

ew Object - Group	×
🤽 Create in: example.	.com/Users
Group name:	
AnyConnect Admins	
Group name (nre-Windows 2000)	•
AnyConnect Admins	
Group scope	Group type
O Domain local	Security
Global	ODistribution
OUniversal	
	OK Cancel

3.驗證是否已建立組。AnyConnect Users組也將建立。

Active Directory Users and Com		-	×		
File Action View Help					
🗢 🔿 🙍 📷 🤞 🗙 🔛 🛛	è 🛛 🖬 🗏 🐮 🖬	🔻 🗾 🙇			
Active Directory Users and Com Saved Queries Saved Queries Builtin Sign Computers Sign Domain Controllers Sign ForeignSecurityPrincipals Sign Managed Service Accour Users	Name AnyConnect Admins AnyConnect Users Calo Cert Publishers Cloneable Domain C DefaultAccount DefaultAccount Domain RODC Passw DnsUpdateProxy Domain Admins Domain Computers Domain Computers Domain Computers Domain Guests Domain Guests Domain Guests Enterprise Admins Enterprise Key Admins Enterprise Read-only FTD Admin Group Policy Creator Guest IT Admin Key Admins	Type Security Group Security Group User Security Group User Security Group Security Group User User User Security Group	Description Built-in account for ad Members of this group Members of this group t A user account manage Members in this group c DNS Administrators Gro DNS clients who are per DNS clients who are per Designated administrato All workstations and ser All domain controllers i All domain guests All domain guests All domain users Designated administrato Members of this group Members of this group Built-in account for gue		
	Ch				

4.按一下右鍵使用者組,然後選擇**屬性**。在此配置中,使用者IT Admin新增到AnyConnect Admins組,使用者**Test User**新增到**AnyConnect Users組**。

Active Directory Users and Comp		-		×				
File Action View Help	File Action View Help							
🗢 🔿 🖄 📅 🔏 🖬 🗶 🛛	⇔ ⇒ 2 📰 🖌 🗈 🗙 🖾 🧔 🔜 🖬 🖘 🖏 🛍 🦁 📓 象							
Active Directory Users and Com	Name	Туре	Description			^		
 Saved Queries example.com Builtin Computers Domain Controllers ForeignSecurityPrincipals Managed Service Accour Users 	AnyConnect Admins AnyConnect Users Calo Cert Publishers Cloneable Domain C DefaultAccount DefaultAccount Domain RODC Passw DosAdmins DosUpdateProxy Domain Admins Domain Computers Domain Computers Domain Controllers Domain Guests Domain Guests Domain Users Enterprise Admins Enterprise Read-only FTD Admin Group Policy Creator Guest	Security Group User Security Group Security Group User Security Group Security Group User Security Group	Add to a group Buil Mer Mer Au: Mer Au: Mer Cut DNS Delete DNS Rename Properties All c Help All communications All domain users Designated administrato Members of this group Members in this group c Built-in account for gue	>				
< >>	Key Admins	Security Group	Members of this group			~		
Renames the current selection.								

5.在「**成員」**頁籤下,按一下**新增**。

AnyConnect Admins	Properties			?	×
General Members	Member Of	Managed By			
Members:					
Name	Active Dir	ectory Domain	Services Folder		
Add	Remove	ОК	Cancel	Appl	У

在欄位中輸入使用者,然後按一下Check Names以驗證找到該使用者。驗證後,按一下OK。

Select Users, Contacts, Computers, Service Accounts, or Gro	oups ×
Select this object type:	
Users, Service Accounts, Groups, or Other objects	Qbject Types
From this location:	
example.com	Locations
Enter the object names to select (examples):	
IT Admin (t.admin@example.com)	Gheck Names
ådvanced	OK Cancel

驗證是否新增了正確的使用者,然後按一下「OK(確定)」按鈕。使用者測試**使用者**也會使用相同 的步驟新增到AnyConnect使用者組。

AnyConnect Admins Properties	?	×
General Members Member Of Managed By		
Members:		
Name Active Directory Domain Services Folder		
Add Remove		
OK Cancel	Арр	ly .

複製LDAPS SSL證書根(僅對於LDAPS或STARTTLS是必需的)

1.按Win+R並輸入mmc.exe,然後按一下「確定」。

1000	Dura	
	nun	

0	Type the name of a progra resource, and Windows wi	m, folder, docum Il open it for you.	ent, or Internet
<u>O</u> pen:	mmc.exe		×
	ОК	Cancel	Browse

2.導航到**檔案>新增/刪除管理單元……**

File Action View Favorites Window Help New Ctrl+N Open Ctrl+S Save As Ctrl+S Add/Remove Snap-in Ctrl+M Options I 1 dnsmgmt 2 dsa Exit I	ᡖ Co	nsole1 - [Console Root]		-	σ×
New Ctrl+N Open Ctrl+O Save Ctrl+S Save As Add/Remove Snap-in Add/Remove Snap-in Ctrl+M Options 1 dnsmgmt 2 dsa Exit	🚪 File	Action View Favorites	Window	Help	- 8 ×
Open Ctrl+O Save Ctrl+S Save As Add/Remove Snap-in Add/Remove Snap-in Ctrl+M Options 1 dnsmgmt 2 dsa Exit	4	New	Ctrl+N		
Save Ctrl+S Save As Add/Remove Snap-in Add/Remove Snap-in Ctrl+M Options 1 1 dnsmgmt 2 2 dsa Exit		Open	Ctrl+0	Actions	
Save As More Actions Add/Remove Snap-in Ctrl+M Options 1 dnsmgmt 2 dsa Exit		Save	Ctrl+S	There are no items to show in this view.	
Add/Remove Snap-in Ctrl+M Options 1 dnsmgmt 2 dsa Exit		Save As		More Actions	+
Options 1 dnsmgmt 2 dsa Exit		Add/Remove Snap-in	Ctrl+M		
1 dnsmgmt 2 dsa Exit		Options			
Exit		1 dnsmgmt			
Exit		2 dsa			
		Exit			

3.在「可用管理單元」下,選擇Certificates,然後按一下Add。

Add or Remove Snap-ins				×
You can select snap-ins for t extensible snap-ins, you car	this console from th configure which e	iose xter	available on your computer and configure the selected set of snap-ins. For sions are enabled.	
Available snap-ins:			Selected snap-ins:	
Snap-in	Vendor	^	Console Root Edit Extensions	
Active Directory Do	Microsoft Cor Microsoft Cor		Bemove	
Active Directory Use	Microsoft Cor Microsoft Cor		Move <u>U</u> p	
Authorization Manager	Microsoft Cor Microsoft Cor		Add >	
Certificates	Microsoft Cor Microsoft Cor			
Component Services	Microsoft Cor Microsoft Cor			
Device Manager	Microsoft Cor Microsoft and	Ļ	Ad <u>v</u> anced	
Description:				
The Certificates snap-in all	ows you to browse	the	contents of the certificate stores for yourself, a service, or a computer.	
			OK Cancel	

4.選擇**電腦帳戶**,然後按一下**下一步**。

Certificates snap-in			×
This snap-in will always manage certificates for: <u>My</u> user account <u>Service account</u> <u>Computer account</u>			
	< <u>B</u> ack	<u>N</u> ext >	Cancel

Select Computer	х
Select the computer you want this snap-in to manage. This snap-in will always manage: Local computer: (the computer this console is running on) Another computer:	
< Back Finish Cancel	

5.現在按一下**OK**。

Add or Remove Snap-ins							×
You can select snap-ins for t extensible snap-ins, you can	his console from th configure which e	iose xter	available on you nsions are enable	r computer and configur d.	re the selected se	t of snap-ins. For	
Available snap-ins:			9	elected snap-ins:			
Snap-in	Vendor	^		Console Root		Edit Extensions	
Active Directory Do	Microsoft Cor			🖓 Certificates (Loc	al Computer)	Remove	
Active Directory Site	Microsoft Cor					Genere	_
Active Directory Use	Microsoft Cor					Marcalla	-
ActiveX Control	Microsoft Cor					Move Up	
AUSI Edit	Microsoft Cor					Move Down	
Certificate Templates	Microsoft Cor		<u>A</u> dd >				_
Certificates	Microsoft Cor						
Certification Authority	Microsoft Cor						
Component Services	Microsoft Cor						
Computer Managem	Microsoft Cor						
Device Manager	Microsoft Cor						
T Disk Management	Microsoft and	\checkmark				Advanced	
Development			, i				
Description:					16		_
The Certificates snap-in allo	ws you to browse	the	contents of the	certificate stores for you	urself, a service, o	or a computer.	
						OK Cancel	

6.展開**Personal**資料夾,然後按一下**Certificates**。LDAPS使用的證書頒發給Windows服**務器的完全 限定域**名(FQDN)。在此伺服器上列出了3個憑證。

[•] 頒發給example-WIN2016-CA的CA證書。

- 由example-WIN2016-CA頒發給WIN2016的身份證書。
- 由example-WIN2016-CA頒發給win2016.example.com的身份證書。

在此配置指南中,FQDN為win2016.example.com,因此前2個證書不能用作LDAPS SSL證書。頒 發給win2016.example.com的身份證書是由Windows Server CA服務自動頒發的證書。按兩下證書 檢查詳細資訊。

The Console	- [Console Root\Certific	ates (Local Computer)\Personal\Certi	ficates]			-	
🚟 File 🛛 Acti	on View Favorites	Window Help					- 8 ×
💠 🔿 🖄	🗖 🗎 🗖 🗟 🖡	? 🖬					
Console R	oot	Issued To	Issued By	Expiration Da	Actions		
V Certifi	ates (Local Computer)	🛱 example-WIN2016-CA	example-WIN2016-CA	4/19/2060	Certificates		
Y Per	Sonal	2 WIN2016	example-WIN2016-CA	4/27/2025	More Actions		+
	sted Root Certification	🕼 win2016.example.com	example-WIN2016-CA	4/28/2021			
> 🧾 Ent	erprise Trust						
> 🚞 Int	ermediate Certification						
> 🔛 Tru	sted Publishers						
> 🚞 Un	trusted Certificates						
> 🚞 Th	rd-Party Root Certificat						
> 📔 Tru	sted People						
> 🚞 Cli	ent Authentication Issue						
> Pre	view Build Roots						
> 0 00	al NonRemovable Cert						
> 🔤 Rei	note Desktop						
> Ce	tricate Enrollment Req						
> Sm	art Card Trusted Roots						
(🔤 w	h Hosting						
🤅 🖻 wi	adows Live ID Token Iss						
· · · · ·	Towns circ ib Toweriss						
<	>	<		>			
Personal store	contains 3 certificates.						

7.要用作LDAPS SSL證書,該證書必須滿足以下要求:

- 公用名或DNS使用者替代名稱與Windows Server的FQDN匹配。
- 在Enhanced Key Usage欄位下,證書具有Server Authentication。

在證書的**Details**頁籤下,選擇**Subject**和**Subject Alternative Name**,此時會顯示FQDN win2016.example.com。

🙀 Certif	ficate				×
General	Details	Certification Pa	1th		
Show:	<al></al>		~		
Field			Value		^
<u>詞</u> Sut	bject		win2016.examp	le.com	
📋 Put	blic key		RSA (2048 Bits)		
Put	blic key pa	arameters	05 00		
Ce	rtificate T	emplate Name	DomainControlle	r	
Enf	hanced Ke	ey Usage	Client Authentic	ation (1.3.6.1	
() () () () () () () () () () () () () (IME Capa	Dilities	[1]SMIME Capat	olity: Object I	
	bject Key Iboritu Ka	Identifier	30 D7 20 He H8 0	27 fb 11 16	¥
CN = w	in2016.e:	<pre>kample.com</pre>			
		[Edit Properties	Copy to File	
				O	¢

🙀 Certi	ficate			×
General	Details	Certification Path		
Show:	<al></al>		~	
Field () () () () () () () () () () () () ()	bject Key thority Ke I. Distribu thority In	Identifier y Identifier tion Points formation Access	Value 30 b7 2b 4e 48 0f 2f 17 17 e6 KeyID=3d 9f 26 37 fb 11 1f 4 [1]CRL Distribution Point: Distr [1]Authority Info Access: Acc	^
Ke Th Th	y Usage umbprint	slgorithm	Other Name:DS Object Guid = Digital Signature, Key Encipher sha1 ca 8e 11 3d eb bc 0f 6e 4a 00	*
Other M DS (18 DNS Na	Name: Object Gu Ime=win2	id=04 10 90 99 a9 016.example.com	a2 38 24 65 47 84 74 64 26 cd c6 8	D
		Ed	It Properties Copy to File	
			0	ĸ

在Enhanced Key Usage下,存在Server Authentication。

🙀 Certi	ficate			×
General	Details	Certification Path		
Show:	<al></al>		~	
Field			Value	^
E Sul	bject blic key		win2016.example.com RSA (2048 Bits)	
Pu	blic key pi cisticato T	arameters amplate Name	05 00 DomainController	
S SM	hanced Ki IME Capa	enplate Name bilities	Client Authentication (1.3.6.1 [1]SMIME Capability: Object I	
副 Sul 尼山	bject Key thority Ke	Identifier v Trlentifier	30 b7 2b 4e 48 0f 2f 17 17 e6 KevID=3d 9f 26 37 fb 11 1f 4	¥
Client / Server	Authentic	ation (1.3.6.1.5.5.) ation (1.3.6.1.5.5.	7.3.2) .7.3.1)	
		Ed	It Properties Copy to File	
			0	ĸ

8.確認後,在Certification Path頁籤下,選擇作為根CA證書的頂級證書,然後按一下View Certificate。

💽 Certificate	×
General Details Certification Path	
Certification path	
example-WIN2016-CA	
	View Certificate
Certificate status:	
This certificate is OK.	
	CY
	OK

9.這將開啟根CA證書的證書詳細資訊。

R Certificate	\times
General Details Certification Path	
Certificate Information	
This certificate is intended for the following purpose(s): • All issuance policies • All application policies	
Issued to: example-WIN2016-CA	-
Issued by: example-WIN2016-CA	
Valid from 4/27/2020 to 4/19/2060	
Issuer Statement	5
ок	

在Details頁籤下,按一下Copy to File...

💼 Certificate	×
General Details Certification Path	
Show: <all></all>	\checkmark
Field	Value ^
Version Serial number Signature algorithm	V3 13 86 46 e5 9d 70 4f a9 4e 35 sha256RSA
Signature hash algorithm Signature hash algorithm Signature hash algorithm Signature hash algorithm	sha256 example-WIN2016-CA Monday, April 27, 2020 10:50:
Valid to	Monday, April 19, 2060 10:50: v
E	it Properties Copy to File
	ОК

10.通過證書導**出嚮導**,以PEM格式匯出根CA。

÷	🚰 Certificate Export Wizard	×
	Welcome to the Certificate Export Wizard	
	This wizard helps you copy certificates, certificate trust lists and certificate revocation lists from a certificate store to your disk.	
	A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.	
	To continue, click Next.	
	Next	1
	Next Cance	1

選擇Base-64 encoded X.509

Certificat	rmat es can be exported in a variety of file formats.
Select the	e format you want to use:
ODE	R encoded binary X.509 (.CER)
🖲 Ba	se-64 encoded X.509 (.CER)
Ocr	yptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)
	Include all certificates in the certification path if possible
⊖ Pe	rsonal 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
ОМі	crosoft Serialized Certificate Store (.SST)

選擇檔案的名稱以及匯出檔案的位置。

Everificate Export Wizard File to Export Specify the name of the file you want to export File name:	Browse	
	Next Cancel	
save As		×
← → ~ ↑ ■ > This PC > Desktop	∨ Ö Si	arch Desktop 🔎
Organize 🔻 New folder		III 🕶 😮
Image: Point of the second	Date modified Type No items match your search.	Size
File name: root		~
Save as type: Base64 Encoded X.509 (*.cer)		v
∧ Hide Folders	[Save Cancel

÷	🚰 Certificate Export Wizard	×
	File to Export Specify the name of the file you want to export	
	File name:	_
	C:\Users\admin\Desktop\root.cer Browse	
	Next Cancel	

現在按一下**完成**。

÷	🐉 Certificate Export Wizard												
		Completing the Certificate Exp	port Wizard										
		You have successfully completed the Certificate	Export wizard.										
		You have specified the following settings:											
		File Name	C:\Users\admin\Desktop\root.cer										
		Export Keys	No										
		Include all certificates in the certification path	No										
		File Format	Base64 Encoded X.509 (*.cer)										
			Finish Canc	el									

11.現在轉到該位置,並使用記事本或其他文本編輯器開啟證書。這顯示PEM格式證書。儲存以備以 後使用。

----BEGIN CERTIFICATE----

```
MIIDCDCCAfCgAwIBAgIQE4ZG5Z1wT6lONTjooEQyMTANBgkqhkiG9w0BAQsFADAd
MRswGQYDVQQDExjleGFtcGxlLVdJTjIwMTYtQ0EwIBcNMjAwNDI3MTQ1MDU5WhgP
MjA2MDA0MTkxNDUwNTlaMB0xGzAZBgNVBAMTEmV4YW1wbGUtV010MjAxNi1DQTCC
ASIwDQYJKoZIhvcNAQEBBQADqqEPADCCAQoCqqEBAI8qhT719NzSQpoQPh0YT67b
Ya+PnqsxMyvkewP33QLTAWw1HW1Tb9Mk5BDW0ItTaVsqHwPBfd++M+bLn3AiZnHV
OO+k6dVVY/E5qVkEKSGoY+v940S2316lzdwReMOFhgbc2qMertIoficrRhihonuU
Cjyeub3CO+meJUuKom2R47C0D35TUvo/FEHGgXJFaJS1se2UrpN07KEMkfAlLPuM
aob4XE/OzxYQpPa18djsNnskfcFqD/HOTFQN4+SrOhHWlRnUIQBUaLdQaabhipD/
sVs5PneYJX8YKma821uYI6j90YuytmsHBtCieyC062a8BKqOL7N86HFPFkMA3u8C
\texttt{AwEAAaNCMEAwDgYDVR0PAQH/BAQDAgGGMA8GA1UdEwEB/wQFMAMBAf8wHQYDVR0O}
BBYEFD2fjjf7ER9EM/HCxCVFN5QzqEdvMA0GCSqGSIb3DQEBCwUAA4IBAQB31ZJo
vzwVD3c5Q1nrNP+6Mq62OFpYH91k4Ch9S5g/CEOemhcwg8MDIoxW2dTsjenAEt7r
phFIHZoCoSyjBjMgK3xybmoSeg8vBjCXseYNGEmOc9KW1oFmTOvdNVIb7Xpl1IVa
6tALTt3ANRNgREtxPA6yQbthKGavW0Anfsojk9IcDr2vp0MTjlBCxsTscbubRl+D
dLEFKQqmMeYvkVf+a7a64mqPZsG3Uxo0rd6cZxAPkq/ylcdwNSJFfQV3DqZq+R96
9WLCR3Obig6xyo9Zu+lixcWpdrbADO6zMhbEYEhkhOOjBrUEBBI6Cy83iTZ9ejsk
KgwBJXEu33PplW6E
```

----END CERTIFICATE-----

12.(可選)如果LDAPS可使用多個身份證書,且使用哪個身份證書存在不確定性,或者無法訪問 LDAPS伺服器,則可以從在Windows伺服器或FTD之後完成的資料包捕獲中提取根ca。

FMC配置

為了部署AnyConnect配置,FTD需要在智慧許可伺服器中註冊,並且必須向裝置應用有效的Plus、 Apex或VPN僅許可證。

1.導航至**系統>許可證>智慧許可**。

Overview	Analysis	Policies	Devices	Objects	AMP	Intelligence					Deplo	y 💽 🥵 🖻	System	Help 🔻	admin 🔻
						Configuration	Users	Domains	Integration	Updates	Licenses 🔻	Health 🔻	Mon	itoring 🔻	Tools *
										Sm	art Licenses ssic Licenses				

2.驗證裝置是否合規並成功註冊。確保裝置已註冊到AnyConnect Apex、Plus或VPN Only許可證。

verview Analysis Policies	De	vices Objec	ts AMP	Intelligence						Deploy 05	System H	ielp v admin
			Configuratio	on Users	Domains	Integration	Updates	Licenses	Smart Licen	ises Health	• Monito	ring • Tool
Smart License Status					<u>Cisco S</u>	mart Software M						
Usage Authorization:	۲	Authorized (Las	t Synchronized	On Nay 03 2020	0							
Product Registration:	0	Registered (Last	t Renewed On #	Mar 03 2020)								
Assigned Virtual Account:		SEC TAC										
Export-Controlled Features:		Enabled										
Cisco Success Network:		Disabled 🕕										
Cisco Support Diagnostics:		Disabled										
Smart Licenses									Filter Devices		×	Edit Licenses
License Type/Device Name					License St	atus	Device Type			Domain	Grou	ıp
Firepower Management e	Cent	er Virtual (2)			0							
🖻 📁 Base (2)					0							
🖻 🟳 Mahware (1)					٥							
🖻 🟳 Threat (2)					0							
🖻 🟳 URL Filtering (2)					0							
🖌 🧭 AnyConnect Apex (1)					0							
FTD-2 192.168.1.17 · Cisco Firepo	wer T	Threat Defense fo	r VMWare - v6	.3.0	0		Cisco Firepower	Threat Defen	se for VMWare	Global	N/A	
AnyConnect Plus (0)												
AnyConnect VPN Only (0)												

設定領域

1.定位至**系統>整合**。

Overview	Analysis	Policies	Devices	Objects	AMP	Intelligence					Deploy	- e,	System	Help 🔻	admin 🔻
						Configuration	Users	Domains	Integration	Updates	Licenses *	Health	 Mon 	itoring 🔻	Tools *

2.在**領域**下,按一下**新建領域**。

Overview Analysis Policie	s Devices Objects	S AMP I	ntelligence					Deploy	O Sy:	stem Help +	admin 🔻
			Configuration	Users	Domains	Integration	Updates	Licenses 🔻	Health 🔻	Monitoring •	Tools *
Cloud Services Realms	Identity Sources	eStreamer	Host Input Client	Smart	t Software S	atellite					
									K Comp	are realms	New realm
Name	Description	Domain	Туре	t	Sase DN	Group	p DN	Group Att	ribute	State	

3.根據從Microsoft伺服器收集的資訊填寫相應的欄位。完成後,按一下OK。

ame *	LAB-AD		
escription			
ype *	AD	~	
D Primary Domain *	example.com		ex: domain.com
D Join Username			ex: user@domain
D Join Password			Test AD Join
Directory Username *	ftd.admin@example.com		ex: user@domain
Directory Password *	•••••		
Base DN *	DC=example,DC=com		ex: ou=user,dc=cisco,dc=com
Group DN *	DC=example,DC=com		ex: ou=group,dc=cisco,dc=com
Scoup Attribute	Member	~	

4.在新視窗中,選擇Directory(如果尚未選擇),然後按一下Add directory。

Overview	Analysis	Policies	Devices	Objects	AMP	Intellige	nce			Deploy	🕘 🔍 Sys	stem Help 🔻	admin v
				Configura	tion	Users	Domains	Integration	Updates	Licenses 🔻	Health 🔻	Monitoring •	Tools •
LAB-AD Enter Descript	ion											Save	Cancel
Directory	Realm Con	figuration	User Down	beole									
												0 A	Idd directory

填寫AD伺服器的詳細資訊。請注意,如果使用FQDN,則除非將DNS配置為解析FQDN,否則 FMC和FTD無法成功繫結。

要設定FMC的DNS,請導航至System > Configuration,然後選擇Management Interfaces。

若要為FTD設定DNS,請導覽至**Devices > Platform Settings**,建立一個新原則,或編輯目前的原則 ,然後前往DNS。

Add directory		? ×
Hostname / IP Address	win2016.example.com	
Port	389	
Encryption	○ STARTTLS ○ LDAPS ④ None	
SSL Certificate	 O 	
	ОК Те	st Cancel

如果使用LDAPS或STARTTLS,請按一下綠色+符號,為證書指定一個名稱,然後複製PEM格式的 根CA證書。完成後按一下**Save**。

Import Trusted Certificate Authority	? ×
Name: LDAPS_ROOT	
Certificate Data or, choose a file: Browse	
 BEGIN CERTIFICATE MIIDCDCCAFCgAwIBAgIQE4ZG5Z1wT6lONTjooEQyMTANBgkqhkiG9w0BAQsFADAd MRswGQYDVQQDExJleGFtcGxlLVdJTjIwMTYtQ0EwIBcNMjAwNDI3MTQ1MDU5WhgP MjA2MDA0MTkxNDUwNTlaMB0xGzAZBgNVBAMTEmV4YW1wbGUtV0lOMjAxNi1DQTCC ASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAI8ghT719NzSQpoQPh0YT67b Ya+PngsxMyvkewP33QLTAWw1HW1Tb9Mk5BDWOItTaVsgHwPBfd++M+bLn3AiZnHV OO+k6dVVY/E5qVkEKSGoY+v940S2316lzdwReMOFhgbc2qMertIoficrRhihonuU Cjyeub3C0+meJUuKom2R47C0D35TUvo/FEHGgXJFaJS1se2UrpN07KEMkfA1LPuM aob4XE/OzxYQpPa18djsNnskfcFqD/HOTFQN4+SrOhHWIRnUIQBUaLdQaabhipD/ sV55PneYJX8YKma821uY16j90YuytmsHBtCieyC062a8BKq0L7N86HFPFkMA3u8C AwEAAaNCMEAwDgYDVR0PAQH/BAQDAgGGMA8GA1UdEwEB/wQFMAMBAf8wHQYDVR00 BBYEFD2fJjf7ER9EM/HCxCVFN5QzqEdvMA0GCSqGSIB3DQEBCwUAA4IBAQB31ZJo vzwVD3c5Q1nrNP+6Mq62OFpYH91k4Ch9S5g/CEOemhcwg8MDIoxW2dTsjenAEt7r phFIHZoCoSyjBjMgK3xybmoSeg8vBjCXseYNGEmOc9KW1oFmTOvdNVIb7Xpl1IVa 6tALTt3ANRNgREtxPA6yQbthKGavW0Anfsojk91cDr2vp0MTjlBCxsTscbubRI+D dLEFKQqmMeYvkVf+a7a64mqPZsG3Uxo0rd6cZxAPkq/ylcdwNSJFfQV3DgZg+R96 9WLCR3Obig6xyo9Zu+lixcWpdrbADO6zMhbEYEhkhOOjBrUEBBI6Cy83iTZ9ejsk KgwBJXEu33PpIW6E END CERTIFICATE 	
Encrypted, and the password is:	
Save	Cancel

從SSL Certificate旁邊的下拉選單中選擇新增的根CA,然後按一下STARTTLS或LDAPS。

Edit directory		?	×
Hostname / IP Address	win2016.example.com		
Port	636		
Encryption	○ STARTTLS		
SSL Certificate	LDAPS_ROOT 💙 📀		
	OK Test Canc	el	

按一下測試以確保FMC能夠使用上一步中提供的目錄使用者名稱和密碼成功繫結。

由於這些測試是從FMC啟動的,而不是通過FTD上配置的某個可路由介面(如內部、外部、 dmz),因此成功(或失敗)的連線不能保證AnyConnect身份驗證的相同結果,因為AnyConnect LDAP身份驗證請求是從FTD可路由介面之一啟動的。 有關從FTD測試LDAP連線的更多資訊,請檢視「故障排除」區域中的「測試AAA」和「資料包捕獲」部分。



5.在User Download下,在後續步驟中下載用於使用者身份的組。

選中**Download users and groups**覈取方塊,Available Groups列將填充在Active Directory中配置的 組。

組可以包括(Included)或排除(Excluded),但預設情況下包括組DN下找到的所有組。

也可以包括或排除特定使用者。任何包含的組和使用者都可供以後選擇用於使用者身份。

完成後,按一下「Save」。

Overview Analysis Policies Devices Objects	AMP Intel	lligence				Deplo	🕘 🕘 Sys	Help 🔻	admin 🔻
		Configuration User	s Domains	Integration	Upda	ates Licenses •	Health *	Monitoring •	Tools *
LAB-AD						You have un	saved changes	🔚 Save	🙁 Cancel
Enter Description									
Directory Realm Configuration User Download									
Download users and groups									
Begin automatic download at 8 Y PM Y America/New Y	fork Repeat Every	24 V Hours							
L Download Now									
Available Groups		Groups to Include (2)			Groups to Exclude (01		
C Search by name		AnyConnect Admi	na		9	None			
AnyConnect Admins		🝰 AnyConnect Users	;		8				
A DnsUpdateProxy									
A WseRemoteAccessUsers									
A WseInvisibleToDashboard									
Allowed RODC Password Replication Group	Add to								
🝰 Enterprise Key Admins	Include								
🍰 Domain Admins	Add to								
A WseAlertAdministrators	Exclude								
🝰 Event Log Readers									
A Replicator									
🝰 Domain Guests									
A Windows Authorization Access Group									
Account Operators									
A Hyper-V Administrators	~								_
👶 System Managed Accounts Group		Enter User Inclusion			Add	Enter User Exclusion			Add

6.啟用新領域。

Overview Analysis Polici	es Devices Object	IS AMP I	ntelligence					Deploy	0 Sys	stem Help	• ▼ admin ▼
			Configura	tion Use	ers Domains	Integration	Updates	Licenses 🔻	Health *	Monitorin	g ▼ Tools ▼
Cloud Services Realms	Identity Sources	eStreamer	Host Input	t Client	Smart Software	Satellite					
									Comp	are realms	New realm
									1		-
Name	Description	Domain	1	Туре	Base DN	Group	p DN	Group Attri	bute	State	
LAB-AD		Global	,	AD	DC=example,Di	-com DC-es	xample,DC=com	member			🕁 🥒 🐚 🖯

7.如果使用LDAPS或STARTTLS,則根CA也需要由FTD信任。為此,請首先導覽至**Devices> Certificates**。

Overview	Analysis	Policies	Device	s Objec	ts AMP	I	ntelligence			Deploy	0,	System	Help 🔻	admin 🔻
Device Mana	gement	NAT N	/PN 🔻 🛛	QoS Pla	tform Settir	ngs	FlexConfig	Certificates						
按一下右	日上角的	的Add。	b											

Overview Analysis	Polici	ies Dev	ices	Objects AMP In	telligence		Deploy	Q,	System	Help 🔻	admin 🔻	
Device Management	NAT	VPN -	QoS	Platform Settings	FlexConfig	Certificates						
										0	Add	

選擇FTD,將LDAP配置新增到中,然後點選綠色+符號。

Add New Certificat	te	? ×
Add a new certificate to identify certificate.	the device using cert enrollment object whi	ich is used to generate CA and
Device":	FTD-2	¥
Cert Enrollment*:	Select a certificate entrollment object	¥ 🙆
		Add Cancel

為信任點指定**名稱**,然後從**註冊型別**下拉選單中選擇**手動註冊**。將PEM根ca證書貼上到此處,然後 按一下**Save**。

Add Cert Enrollment

Name*	LDAPS_ROOT	
Description		
CA Information	Certificate Parameters Key Revocation	
Enrollment Type:	Manual	^
CA Certificate:*	 MIIDCDCCAfCgAwIBAgIQE42G5Z1wT6lONTjooEQyMTANBgkqhki G9w0BAQsFADAd MRswGQYDVQQDExJleGFtcGxlLVdJTjIwMTYtQ0EwIBcNMjAwNDI 3MTQ1MDU5WhgP MjA2MDA0MTkxNDUwNTlaMB0xGzAZBgNVBAMTEmV4YW1wbGU tv0lOMjAxNi1DQTCC ASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAI8ghT719N zSQpoQPh0YT67b Ya+PngsxMyvkewP33QLTAWw1HW1Tb9Mk5BDWOItTaVsgHwPBf d++M+bLn3AiZnHV OO+k6dVVY/E5qVkEKSGoY+v940S2316lzdwReMOFhgbc2qMertIo ficrRhihonuU CJyeub3CO+meJUuKom2R47C0D35TUvo/FEHGgXJFaJS1se2UrpN O7KEMkfA1LPuM aob4XE/OzxYQpPa18djsNnskfcFqD/HOTFQN4+SrOhHWlRnUIQBU aLQaabhipD/ 	~
Allow Overrides		
	Save	Cancel

驗證已選擇建立的信任點,然後按一下Add。

Add New Certificate		? ×	
Add a new certificate to the identify certificate.	e device using cert enrollment object which	h is used to generate CA and	
Device*:	FTD-2	~	
Cert Enrollment*:	LDAPS_ROOT	~ ©	
Cert Enrollment Details:			
Name:	LDAPS_ROOT		
Enrollment Type:	Manual		
SCEP URL:	NA		
		Add Cancel	

? X

新信任點將出現在FTD下。雖然其中提到需要匯入身份證書,但對於FTD而言,並不要求能夠對 LDAPS伺服器傳送的SSL證書進行身份驗證,因此可以忽略此消息。

Overview Analysis	Policies Devices Of	ojects AMP Intel	lligence	Deploy 🔍 System	Help 🔻 admin 🔻
Device Management	NAT VPN VOS	Platform Settings	FlexConfig Certificates		
					🔕 Add
Name	Domain	Enrollment Type	Status		
4 🗐 FTD-1					
FTD-1-PKCS12	Global	PKCS12 file	CA OLD		£¢ 🗄
4 🗐 FTD-2					
FTD-2-PKCS12	Global	PKCS12 file	CA CA		£¢ 🗉
FTD-2-Selfsigned	Global	Self-Signed	S CA LD		i?¢ 🛙
LDAPS_ROOT	Global	Manual	🔍 CA 🔺 ID 🛓 Ide	ntity certificate import required	P 🗘 🗎

配置AnyConnect進行AD身份驗證

1.這些步驟假定尚未建立遠端訪問vpn策略。如果已建立策略,請點選該策略的edit按鈕,並跳至步 驟3。

導覽至Devices > VPN > Remote Access。



按一下Add建立新的遠端訪問VPN策略

Overview Analysis	Policies D	Devices	Objects	AMP	Intelligence				Deploy	0	System	Help 🔻	admin v
Device Management	NAT VPN	N + Remote	e Access	Qo5	Platform Settings	FlexConfig	Certificates						
												0	Add
Name					Status		L.	est Modified					

No configuration available Add a new configuration

2.完成**遠端訪問VPN策略嚮導**。在Policy Assignment下,指定策略名稱和應用該策略的裝置。

Overview Analysis	Policies De	vices Objects	AMP Intelligence			Deploy 🔩 Syste	em Help ⊤ admin ⊤
Device Management	NAT VPN •	Remote Access	QoS Platform Setting	FlexConfig	Certificates		
Remote Access V	PN Policy V	Vizard					
1 Policy Assignment	nt 🔵 Co	onnection Profile	> 3 AnyConnect >	Access &	Certificate	S Summary	
Ta Th	argeted Device is wizard will guid new user-defined (es and Protocols le you through the requir connection profile.	red minimal steps to configur	e the Remote Acces	s VPN policy with	8 Before You Start	^
Na	ime:*	FTD-2-RA-Policy				Before you start, ensure the following configuration elements to be in place to complete Remote Access VPM Policy. Authentication Server	
De VP	escription: PN Protocols:	🗹 SSL 🗹 IPsec-IKi	Ev2		0	Configure <u>Realm</u> or <u>RADIUS Server Group</u> to authenticate VPN dients. AnyConnect Client Package	
т	rgeted Devices:	Available Devices	Add	Selected Device	2	Make sure you have AnyConnect package for VPN Clent downloaded or you have the relevant Clacc credentials to download it during the wixard. Device Interface Interfaces should be already configured on targeted <u>devices</u> so that they can be used as a security zone or interface group to enable VPN access.	
							~
						Back	t Cancel

在**Connection Profile**下,指定**Connection Profile**的名稱,該名稱也用作AnyConnect使用者在連線 時看到的組別名。

指定以前在Authentication Server下建立的**領域。**

指定為AnyConnect客戶端分配IP地址的方法。

指定用於此連線配置檔案的預設組策略。

Overview	Analysis	Policies	Devices	Objects	AMP	Intelligence						Deploy	e ,	System	Help 🔻	admin v	
Device Mana	agement	NAT	VPN • Remot	te Access	QoS	Platform Settings	FlexConfig	C	ertificates								
Remote	Access	VPN Pol	icy Wizar	d													
1 Policy	Assignme	ent 🔪 🤅	Connecti	on Profile	3	AnyConnect > (Access 	& Cer	tificate $>$ (5 Summary	У						
			Connection Pr accomplished	n Profile: ofiles specify (and how addr	the tunnel esses are	group policies for a VPN assigned. They also inclu	connection. Th ide user attribu	ese pol tes, wh	cies pertain to or ich are defined in	eating the tunne group policies.	el itself, how	AAA is					^
			Conne	ction Profile N	lame:*	General											
						This name is configured a	a a connection a	lan, it c	an be used to con-	nect to the VTN g	apavak						
			Authenticati Specify the m	on, Authoriza ethod of autho	stion & A intication	ccounting (AAA): (AAA, certificates or both	h), and the AAA	server	s that will be used	d for VPN connec	ctions.						
			Authe	ntication Meth	od:	AAA Only		•									
			Auther	ntication Serv	er:*	LAB-AD		0-	(Realm or RADIU	15)							
			Author	rization Serve	r:			0	(RADIUS)								
			Accou	nting Server:				0	(RADIUS)								
			Client Addre Client IP addre assignment is	ss Assignme ess can be ass tried in the o	nt: igned from rder of AA	m AAA server, DHCP serv A server, DHCP server ar	ver and IP addr nd IP address p	iss poo	ls. When multiple	options are sele	ected, 1P ade	dress					
				e AAA Server (e DHCP Server	RADDUS o	nly) 🕕											
			M Use	e IP Address P	pols												
				IPv4 Address	s Pools:	AnyConnect-Pool		6									
				IPv6 Address	s Pools:			ø									
			Group Policy														
			A group policy or create a Gr	y is a collection oup Policy obj	n of user-a ect.	priented session attribute	is which are as	igned t	o client when a V	PN connection is	s established	i. Select					
			Group	Policy:*		DfltGrpPolicy Edit Group Policy		0									
						······											ľ
												Back	חר	Next	C	ancel	

在AnyConnect下,上傳並指定使用的AnyConnect軟體包。



在Access & Certificate下,指定AnyConnect使用者訪問AnyConnect的介面。

建立和/或指定FTD在SSL交握期間使用的憑證。

確保取消選中解密流量(sysopt permit-vpn)的**旁路訪問控制策略**覈取方塊,以便以後建立的使用者標 識對RAVPN連線生效。

Overview Analysis Policies Devices Objects AMP Intelligence		Deploy 🔍	System	Help 🔻	admin 🔻
Device Management NAT VPN • Remote Access QoS Platform Settings FlexConfig	Certificates				
Remote Access VPN Policy Wizard					
Policy Assignment 2 Connection Profile 3 AnyConnect 4 Access &	Certificate 5 Summary				
Network Interface for Incoming VPN Access Select or create an Interface Group or a Security Zone that contains t connections.	he network interfaces users will access for VPN				~
Interface group/Security Zone:* outside-zone	× 0-				
Enable DTLS on member inte	infaces				
Device Certificates					
Device certificate (also called Identity certificate) identifies the VPN gr certificate which is used to authenticate the VPN reference.	atemay to the remote access clients. Select a				
Certificate Enrollment:* FTD-2-Selfsioned	× 0				
Peoplithe selected estificate	shiert on the ternet devices				
	suger of the target bences				
Access Control for VPN Traffic					
All decrypted traffic in the VPN burnel is subjected to the Access Cont bypass decrypted traffic from the Access Control Policy.	rol Policy by default. Select this option to				
Bypass Access Control policy for decrypted traffic (sysopt permit- This option bypasses the Access Centrol Policy Inspection, but VPN RE AAA server are still applied to VPN traffic.	pn) er ACL and authorization ACL downloaded from				~
		Back	Next	Ca	incel

在Summary下,按一下Finish檢視配置。



3.在Remote Access VPN Policy下,按一下相應的Connection Profile的edit。

Overview Analysis Policies Devices Objects	AMP Intelligence	Deploy 😝 System Help 🔻 admin 🔻
Device Management NAT VPN • Remote Access	QoS Platform Settings FlexConfig Certificates	
FTD-2-RA-Policy Enter Description		Save Cancel
Connection Buddle Access Interfaces Advanced		Policy Assignments (1)
Connection Prome Access Interfaces Advanced		
		a
Name	AAA Group Policy	
DefaultWEBVPNGroup	Authentication: None DfkGrpPolicy Authorization: None Accounting: None	/ 0
General	Authentication: LAB-AD (AD) E DftGrpPolicy Authorization: down Accounting: down	28

確保將身份驗證伺服器設定為之前建立的領域。

在Advanced Settings下,可以選中Enable Password Management,以允許使用者在其密碼到期時 或之前更改其密碼。

但是,此設定要求領域使用LDAPS。如果進行了任何更改,請按一下Save。

Edit Connection Profile		? ×
Connection Profile:* Gene Group Policy:* DfltG Edit G Client Address Assignment	al pPolicy CO oup Policy AAA Aliases	
Authentication		
Authentication Method:	AAA Only	
Authentication Server:	LAB-AD (AD)	
Use secondary authent	cation	
Authorization		
Authorization Server:	Allow connection only if year exists in authorization database	
Accounting	Allow connection only in user exists in authorization database	
Accounting Server:	v	
Call & damaged California		
Strip Realm from usern	ime	
Strip Group from usern	ime	
Enable Password Mana	ement	
O Notify User 14 day	ys prior to password expiration f password expiration	
	Save Cancel	

完成後,按一下右上角的Save。



啟用身份策略並為使用者身份配置安全策略

1.定位至策略>訪問控制>標識。

Overview An	alysis Policies	Devices	; Objects	AMP	Intelligence				Deploy	е,	System	Help 🔻	admin v
Access Control •	Network Disco	very	Application D	etectors	Correlation	Actions 🔻							
Access Control													
Intrusion													
Malware & File													
DNS													
Identity													
SSL													
Prefilter													

建立新的身份策略。

Overview Analysis Policies Devices Objects A	MP Intelligence	Deploy 🔍 Sy	stem Help v admin v
Access Control + Identity Network Discovery Application	on Detectors Correlation Actions •		
		Object	Management Access Control
		🕑 Compa	re Policies 🔍 New Policy
Identity Policy	Domain	Status	Last Modified

There are no policies created. Add a new policy

指定新**身份**策略的**名稱**。

lew Identit	y policy	? X
Name	FTD-2 Identity Policy	
Description		
	Save Ca	ncel

2.按一下**新增規則**。

	Overview Analysis Poli	icies Device	s Objects	AMP Intellig	ence				De	play 🔒 Sys	tem Help v	admin v
1	ccess Control > Identity	Network Disc	overy Appl	ication Detectors	Correlation	Actions *						
F	TD-2 Identity Poli Inter Description	icy									E Save	3 Cancel
R	Active Authentication											
								Add Category	/ 🔾 Add Ruk	Search Rules		×
	Name	Source Zo	Dest Zones	Source Net	Dest Netw	VLAN Tags	Source Ports	Dest Ports	Realm	Action	Auth Prote	col

3.為新規則指定**名稱**。請確保已啟用該功能,並將操作設定為Passive Authentication。

按一下Realm & Settings頁籤,然後選擇之前建立的領域。完成後按一下Add。

ame R	AVPN			🗹 Enable	d Insert	into Category	×	Standard Rules	1
tion P	assive Authentic	sation		Realm: LAB-AD (AD)	Authentication Protocol:	HTTP Basic Exclude	HTTP User-	Agents: None	
Re	mote access VP	N sessions are a	actively authent	cated by VPN. Other session	is use the rule Action.				
Zones	Networks	VLAN Tags	Ports					Realm & S	ietting
					-				
ealm *		LAB-AD (AI	D)		¥ 🦉				
Use a	ctive authentical	tion if passive o	r VPN identity o	annot be established					
,									
Require	ed Field								
Require	ed Field								

4.按一下Save。

Overview Analysis Poli	icies Device	es Objects	AMP Intelli	gence				Dep	xloy 🧛 System	Help 🔻 adr	nin •
Access Control > Identity	Network Disc	covery Apple	cation Detectors	Correlation	Actions *						
FTD-2 Identity Pol	icy							You have	unsaved changes [Save 🔀 C	ancel
Rules Active Authentication											
							Add Categor	y 🛛 🔘 Add Rule	Search Rules		×
# Name	Source Zo	Dest Zones	Source Net	Dest Netw	VLAN Tags	Source Ports	Dest Ports	Realm	Action	Auth Protocol	
Administrator Rules											
This category is empty											
Standard Rules											
1 RAVPN	any	any	any	any	any	any	any	LAB-AD	Passive Authentication	none	/8
Root Rules											
This category is empty											

Displaying 1 - 1 of 1 rules |< < Page 1 of 1 > >| C

5.定位至**策略>訪問控制>訪問控制**。

Overview Analysis Policies Devices Objects AMP Intelligence	Deploy	🧛 System	Help 🔻	admin v
Access Control + Identity Network Discovery Application Detectors Correlation Actions				
Access Control				
Intrusion				
Malware & File				
DNS				
Identity				
SSL				
Prefilter				

6.編輯FTD**配置所**在的訪問控制策略。

Overview Analysis Policies	Devices Objects	AMP Intelligence					Deplo	y 🧕	System	Help 🔻	admin v
Access Control > Access Control	Network Discovery	Application Detectors	Correlation	Actions *							
					Objec	ct Management	Intrusion No	stwork Ana	lysis Policy	DNS Im	port/Export
										O Nev	Policy
Access Control Policy		Status			Last	Modified					
Default-Policy		Targeting 1 de Up-to-date on	evices all targeted devic	es	2020 Modif	-05-04 09:15:56 ied by "admin"				B B	26

7.按一下Identity Policy旁邊的值。



Identity Policy		
FTD-2 Identity Policy		¥ 🖉
Revert to Defaults	OK	Cancel

8.按一下Add Rule以建立新的ACP規則。這些步驟建立規則以允許AnyConnect Admins組中的使用 者使用RDP連線到內部網路中的裝置。

Overview Analysis Policies	Devices Objects AMP	Intelligence		Deplo	y 🧕 System Help 🔻 admin 🔻
Access Control > Access Control	Network Discovery Applic	ation Detectors Correlation	Actions •		
Default-Policy Enter Description				You have unsaved changes Analy	ze Hit Counts 🛛 🔚 Save 🛛 🔞 Cancel
Prefilter Policy: Default Prefilter Policy		SSL Policy: Non		Identity	Policy: FTD-2 Identity Policy
				Te Inher	ritance Settings 🧮 Policy Assignments (1)
Rules Security Intelligence HTT	TP Responses Logging Adv	vanced			
曲 Filter by Device		🗆 st	ow Rule Conflicts 😣 🛛 🔘	Add Category 🛛 🔾 Add Rule	🚔 Search Rules 🛛 💥
# Name Sourc Dest	t Z Sourc Dest N VI	LAN Users Applic	Sourc Dest P UF	RLs Sourc Dest S /	Action 😈 🏷 🔏 😓 🗢 ම
👻 Mandatory - Default-Policy (-)					
There are no rules in this section. Add Rul	le or Add Category				
🗢 Default - Default-Policy (-)					
There are no rules in this section. Add Rul	le or Add Category				
Default Action				Access Control: Block All Traffic	¥ 📕

Displaying 0 - 0 of 0 rules $|\langle \langle Page | 1 \rangle$ of 1 > > C | Rules per page: 100 -

指定規則的名稱。確保規則已啟用並具有相應的操作。

在Zones頁籤下,為相關流量指定適當的區域。

使用者所起始的RDP流量會進入源自外部區域介面的FTD,然後輸出內部區域。

Name AC RDP Access Action Allow Zones Networks VLAN Tags Users Applications Ports URLs SGT/ISE Attributes Inspection Logging Comments Available Zones Image: Comments Add to Add to Add to Image: Comments Imag	Add Rule									? ×
Action Action Allow Action Allow Allow Allow Allow Comments Zones Networks VLAN Tags Users Applications Ports URLs SGT/ISE Attributes Inspection Logging Comments Available Zones C Source Zones (1) Destination Zones (1) Source Zone Add to Source Add to	Name AC RDP Access			Enabled	Insert	into Mandato	ary Y]		
Zones Networks VLAN Tags Users Applications Ports URLs SGT/ISE Attributes Inspection Logging Comments Available Zones C Source Zones (1) Destination Zones (1) Image: Comments Image: Comments Image: Comments Image: Comments Image: Comments Image: Comments Available Zones Image: Comments Image: Comments Image: Comments Image: Comments Image: Comments Image: Comments Image: Comments Image: Comments Image: Comments Image: Comments Image: Comments Image: Comments Image: Comments Image: Comments Image: Comments Image: Comments Image: Comments Image: Comments Image: Comments Image: Comments Image: Comments Image: Comments Image: Comments Image: Comments Image: Comments Image: Comments Image: Comments Image: Comments Image: Comments Image: Comments Image: Comments Image: Comments Image: Comments Image: Comments Image: Comments Image: Comments Image: Comments Image: Comments Image: Comments Image: Comments Image: Comments Image: Comments Image: Comments Image: Comments Image: Comments Image: Comments Ima	Action Allow		V 0 28 6	2 U						
Available Zones C Source Zones (1) Destination Zones (1) Add to Add to Add to	Zones Networks	VLAN Tags Users	Applications P	Ports URLs	SGT/ISE Attributes			Inspection	Logging	Comments
side inside-zone inside-zone Add to Add to	Available Zones 🛭 🗯			Source Zones	(1)		Destinatio	on Zones (1)		
At inside-zone At outside-zone Add to Source	🔍 side	×		📩 outside-zor	ne	6	🚠 inside	-zone		6
Destination	슈 inside-zone 슈 outside-zone		Add to Source Add to Destination							

在Networks下,定義源網路和目標網路。

對象AnyConnect_Pool包括分配給AnyConnect客戶端的IP地址。

對象Inside_Net包括內部網路子網。

Name A Action	C RDP Access			• • • • 8] ⊻ ∈ 1:1	abled		Insert	into Manda	tory		~
Zones	Networks	VLAN Tags	Users	Applications	Ports	URLs	SGT/ISE	Attributes		Inspec	tion Logging	Comments
Available	Networks C		0		Sourc	e Netwo	rks (1)			Destination Netv	rorks (1)	
Search	h by name or value					Source	e -	Original (Client	📰 Inside_Net		6
No	ctworks	Geolocati	on		A	nyConned	t_Pool		6			
Inside IPv4-E IPv4-E IPv4-F IPv4-F IPv4-F IPv4-F IPv4-F	Net Benchmark-Tests Link-Local Multicast Private-10.0.0.0-8 Private-172.16.0.0 Private-192.168.0.0 Private-All-RFC1918	-12 D-16 8	•	Add To Source Networks Add to Destination			faces.					
IPv6-1	Pv4-Mapped				Enter	an IP add	dress		Add	Enter an IP addre	55	Add
											Add	Cancel

在Users下,按一下Available Realms下之前建立的領域,在Available Users下按一下相應的組/使用者,然後按一下Add to Rule。

如果Available Users部分下沒有可用的使用者或組,請確保FMC能夠下載realm部分下的Users和 Groups,並且包含適當的Groups/User。

從源角度檢查此處指定的**使用者/組**。

Add Rule

例如,根據此規則到目前為止所定義的內容,FTD會評估以下情況:流量來源為外部區域,且目的 地為內部區域,來源為AnyConnect_Pools對象中的網路,且目的地為Inside_Net對象中的網路,而 流量來源為AnyConnect Admins組中的使用者。

Add Rule		? ×
Name AC RDP Access	🖌 Enabled	Insert into Mandatory
Action 🖌 Allow	▼ 0 D A th D	
Zones Networks VLAN Tags Users	Applications Ports URLs SGT/ISE Attri	butes Inspection Logging Comments
Available Realms	Available Users 🖸	Selected Users (1)
Search by name or value	Search by name or value	🛃 LAB-AD/AnyConnect Admins 📋
🌐 Special Identities	() LAB-AD/*	
🌐 LAB-AD	🛃 AnyConnect Admins	
	AnyConnect Users	
	a it.admin	Add to Rule
	a test.user	
		Add Cancel

在Ports下,建立並新增自定義RDP對象以允許TCP和UDP埠3389。請注意,本可以在 Applications部分下新增RDP,但為簡單起見,只檢查埠。

Name AC RDP Access		Enabled	Insert into Mandatory	*	
Action & Allow	▼ 0.0	A to U			
Zones Networks VLAN Tags	Users Applications	Ports URLs SGT/ISE	E Attributes	Inspection Logging	Comments
Available Ports C	0	Selected Source Ports (0) Select	ed Destination Ports (2)	
Search by name or value		any	PRC RD	P-TCP	6
AOL AOL AC Bittorrent Bittorrent DNS_over_TCP DNS_over_UDP FNC-HTTPS FNC-SSH FTD-3-FDM FTD-3-SSH FTD-3-SSH FTD	Add to Source Add to Destination		ø RD	JP-UDP	6
🥕 НТТР	~		Port Enter Add Protoco	ol TCP (6) Y Port Er	iter a Add
				Add	Cancel

Add Rule

最後,在Logging下,稍後會檢查Log at End of Connection以進行其他驗證。完成後按一下Add。

Add Ru	le											? ×
Name	AC RDP Access				V 6	Enabled		Insert	into Mandatory	•		
Action	🖌 Allow			• • • • •	8 🗠 📕							
Zone	s Networks V	LAN Tags	Users	Applications	Ports	URLs	SGT/ISE Attrib	butes		Inspection	Logging	Comments
Log Log File Even Log Send Co V Even	at Beginning of Conn at End of Connection ts: Files nnection Events to: t Viewer	ection										
Syst	og Server (Using defi	ault syslog co	nfiguration	in Access Contr	ol Logging)) Show O	verrides					
SNM	P Trap Select an SN	MP Alert Conf	figuration			~	G					
											Add	Cancel

9.為HTTP訪問建立了一個附加規則,以允許組**AnyConnect** User**中的用**戶訪問**Windows Server** IIS網站。按一下「Save」。

Overview Analysis Policies	Devices Objects	AMP Intelligence				Dep	loy 🔍 System	Help 🔹 admin 🔻		
Access Control > Access Control	Network Discovery	Application Detectors	Correlation Actions •							
Default-Policy Enter Description					You have unsave	ed changes Ana	lyze Hit Counts	Save 🖸 Cancel		
Prefilter Policy: Default Prefilter Policy		551	Policy: None		Identity	Policy: PTD-2.1de	ntity Policy			
						T= Inb	eritance Settings 🧾 Po	licy Assignments (1)		
Rules Security Intelligence H	TTP Responses Loggin	ng Advanced								
🛱 Fitter by Device Show Rule Conflicts 🕖 🕥 Add Category 🕥 Add Rule 🚅 Search Rules										
# Name Source Zo	Dest Zones Sour	rce Networks Dest Netw	vo V Users	A S	Dest Ports U	J S D A	iction 🤠 🐚 🔏	to 🗢 🔍		
➡ Mandatory - Default-Policy (1-2)										
1 AC RDP Access A outside-zo	ne 🚓 inside-zone 🛛 👼 /	AnyConnect_Pool 🛛 📾 Inside,	Net 🛛 🖧 💣 LAB-AD/AnyConnect Adr	mins Any An	RDP-TCP	Any Any Any	Allow U D .8	ta 🛛 🔹 🥒 G		
2 AC HTTP Access do outside-zo	ne 👍 inside-zone 🛛 🚃 A	AnyConnect_Pool 🛛 👼 Inside	Net 🛛 🗛 🧬 LAB-AD/AnyConnect Use	ers Any An	у 🥜 НТТР	Any Any Any	Allow 0 D. 8	🖄 🖃 o 🔛 🖯 🖯		
▼ Default - Default-Policy (-)										
There are no rules in this section. Add R	ule or Add Category									
Default Action					Access Contro	I: Block All Traffic		× 🔳		

? ×

Displaying 1 - 2 of 2 rules $|\langle \langle Page | 1 \rangle$ of 1 $\rangle > | C |$ Rules per page: 100 -

配置NAT免除

如果存在影響AnyConnect流量的NAT規則(如網際網路PAT規則),則必須配置NAT免除規則,以 使AnyConnect流量不會受NAT影響。

1.導航到Devices > NAT。

Overview Analysis	s Polici	es Dev	ices	Objects	AMP	Intelligence		Deploy	0,	System	Help 🔻	admin v
Device Management	NAT	VPN •	QoS	Platfor	m Setting	s FlexConfig	Certificates					

選擇應用於FTD的NAT策略。

Overview Analys	is Polic	ies Devi	ices 0	bjects A	MP Inf	telligence		(Deploy	e ,	System	Help 🔻	admin 🔻
Device Management	NAT	VPN *	QoS	Platform Se	ettings	FlexConfig	Certificates						
												🔾 New	Policy
NAT Policy					Dev	rice Type		Status					
FTD-2-NAT-Polic	Ŷ				Thre	at Defense		Targeting 1 devices Up-to-date on all target	ed devices			D E	28

2.在該NAT策略中,終端有一個動態PAT,該PAT會影響從外部介面到外部介面的所有流量(包括 AnyConnect流量)。

要防止AnyConnect流量受NAT影響,請按一下右上角的Add Rule。

Overview A	nalysis	Policies 0	evices	Objects	AMP	Intelliger	nce					Deploy	0,	System	Help 🔻	admin 🔻
Device Manage	ment	NAT VPN	• Q	S Platfor	m Setting	gs Flex	Config	Certificat	es							
FTD-2-NA Enter Description	AT-Poli	cy										🛕 Shov	v Warning	8	Save	😫 Cancel
Rules														5	Policy A	ssignments (1)
B Filter by Device															0	Add Rule
						Orig	pinal Packe	t			Translated Pac	cket				
# Direction	Туре	Source Interface 0	Des bje Inte	tination erface Object	Original Sources	0	Driginal Destination	ls i	Orig Services	Translated Sources	Translated Destination	s 1	Frans Services	Options	:	
 NAT Rules Befo 	re															
 Auto NAT Rules 	5															
= +	Dynamic	🥞 any	- 44	outside-zone	👼 obj-a	ny				🥵 Interface				🥞 Dns:	false	28
▼ NAT Rules Afte	r															
								0	Splaying	1-1 of 1 rows	IC C Page 1	of 1	> >	Ć R	ows per p	age: 100 •

3.配置NAT免除規則,確保該規則是型別為Static的手動NAT規則。這是適用於AnyConnect流量的 雙向NAT規則。

透過這些設定,當FTD偵測來源為Inside_Net且目的地為AnyConnect IP位址(由 AnyConnect_Pool定義)的流量時,來源會轉換為相同的值(Inside_Net),而目的地會在流量進入 inside_zone且離開outside_zone時轉換為相同的值(AnyConnect_Pool)。在滿足這些條件時,這基 本上會繞過NAT。

NAT Rule:	Manual NAT Rul	e 👻	Insert:	In Category	V NAT Rules Before	
Type:	Static	~	✓ Enable			
Description:		1				<u>^</u>
Interface Objects	Translation	DAT Bool	Advanced			~
Available Interface O	hierts C	PAT POOL	Source Inter	face Objects (1)	Destination Interface Objects (1)	
a, zone	.,	×	inside-zo	ne 🕅	and outside-zone	F
		_				
and outside-zone		Ad	d to			
			urce			
		Ad Desti	d to nation			
					OK	Cancel
					OK	CONVOI
					UK .	Concer
dd NAT Rule					UK	?
Add NAT Rule	Manual NAT Rul	e v	Insert:	In Category	▼ NAT Rules Before ▼	?
Add NAT Rule NAT Rule:	Manual NAT Rul	e v	Insert:	In Category	NAT Rules Before	?
Add NAT Rule NAT Rule: Type:	Manual NAT Rul Static	e v v	Insert: Enable	In Category	▼ NAT Rules Before ▼	?
Add NAT Rule NAT Rule: Type: Description:	Manual NAT Rul Static	e v	Insert: Insert:	In Category	V NAT Rules Before	?
Add NAT Rule NAT Rule: Type: Description:	Manual NAT Rul Static Translation	e V V	Insert: Enable Advanced	In Category	▼ NAT Rules Before ▼	?
dd NAT Rule NAT Rule: Type: Description: Interface Objects Original Packet	Manual NAT Rul Static Translation	e v v PAT Pool	Insert: Enable Advanced	In Category Translated Packet	NAT Rules Before	?
Add NAT Rule NAT Rule: Type: Description: Interface Objects Original Packet Original Source:*	Manual NAT Rul Static Translation Inside_Net	e V V PAT Pool	Insert: Enable Advanced	In Category Translated Packet Translated Source:	NAT Rules Before	?
Add NAT Rule NAT Rule: Type: Description: Interface Objects Original Packet Original Source:*	Manual NAT Rul Static Translation	e V V PAT Pool	Insert: Enable Advanced	In Category Translated Packet Translated Source:	Address	? ?
dd NAT Rule: NAT Rule: Type: Description: Interface Objects Original Packet Original Source:* Original Destination:	Manual NAT Rul Static Translation Inside_Net Address	e v v	Insert: Enable Advanced	In Category Translated Packet Translated Source:	Address Inside_Net	? ?
Add NAT Rule NAT Rule: Type: Description: Interface Objects Original Packet Original Source:* Original Destination:	Manual NAT Rul Static Translation Inside_Net Address AnyConnet	e v PAT Pool	Insert: Enable Advanced	In Category In Category Translated Packet Translated Source: Translated Destination:	Address Inside_Net AnyConnect_Pool	? ? V V 0
Add NAT Rule NAT Rule: Type: Description: Interface Objects Original Packet Original Source:* Original Destination:	Manual NAT Rul Static Translation Inside_Net Address AnyConne	e v PAT Pool	Insert: Enable Advanced Control Advanced Control Contro Control Control Con	In Category Translated Packet Translated Source: Translated Destination: Translated Source Port:	Address Inside_Net AnyConnect_Pool	? ? V 0
Add NAT Rule NAT Rule: Type: Description: Interface Objects Original Packet Original Source:* Original Destination: Original Source Port:	Manual NAT Rul Static Translation Inside_Net Address AnyConnet	e v PAT Pool	Insert: Enable Advanced Control Con	In Category In Category Translated Packet Translated Source: Translated Destination: Translated Source Port:	Address Inside_Net AnyConnect_Pool	
Add NAT Rule NAT Rule: Type: Description: Interface Objects Original Packet Original Source:* Original Destination: Original Source Port: Original Destination P	Manual NAT Rul Static Translation Inside_Net Address AnyConnet	e v PAT Pool	Insert: Enable Advanced Control Contro Control Control Control Control Control Control Control Cont	In Category In Category Translated Packet Translated Source: Translated Destination: Translated Source Port: Translated Destination Port:	Address Inside_Net AnyConnect_Pool	 ? ?<
Add NAT Rule NAT Rule: Type: Description: Interface Objects Original Packet Original Source:* Original Destination: Original Source Port: Original Destination P	Manual NAT Rul Static Translation Inside_Net Address AnyConne	e v PAT Pool	Insert: Enable Advanced Control Contro Control Control Control Control Control Control Control Cont	In Category In Category Translated Packet Translated Source: Translated Destination: Translated Source Port: Translated Destination Port:	Address Inside_Net AnyConnect_Pool	· · · · · · · · · · · · · · · · · · ·
Add NAT Rule NAT Rule: Type: Description: Interface Objects Original Packet Original Source:* Original Destination: Original Source Port: Original Destination P	Manual NAT Rul Static Translation Inside_Net Address AnyConnet	e v PAT Pool t ct_Pool	Insert: Enable Advanced	In Category Translated Packet Translated Destination: Translated Source Port: Translated Destination Port:	Image: NAT Rules Before Address Inside_Net AnyConnect_Pool	 マ マ マ マ マ ○ マ ○ マ ○ マ ○ ○

此外,FTD設定為對此流量執行路由查詢,而不是代理ARP。完成後按一下**OK**。

Add NAT Rule						? X
NAT Rule:	Manual NAT Rule	Insert:	In Category	VAT Rules Be	fore 💙	
Type:	Static 🗸	Enable				
Description:						0
Interface Objects	Translation PAT Pool	Advanced				
Translate DNS repli	es that match this rule					
Fallthrough to Inter	face PAT(Destination Interface)					
IPv6						
Net to Net Mapping						
🗹 Do not proxy ARP o	n Destination Interface					
Perform Route Look	up for Destination Interface					
Unidirectional						
					ок с	ancel

4.按一下Save。

c	verview /	Analysis	Policies Devi	ces Objects	AMP Inte	elligence				Depl	y 🌖	System Help	r admin v
0	evice Manag	ement	NAT VPN *	QoS Platfor	m Settings	FlexConfig	Certificates	1					
F	TD-2-N	AT-Poli	cy						You have un	saved changes 🔬 S	how Warning	ps 🔚 Save	Cancel
R	ules											Policy.	Assignments (1
æ	Filter by Device											0	Add Rule
						Original Pack	et			Franslated Packet			
*	Direction	Туре	Source Interface Object	Destination Interface Object	Original Sources	Original Destination	ns Se	rig trvices	Translated Sources	Translated Destinations	Trans Services	Options	
٠	NAT Rules Bef	ore											
1	*	Static	å inside-zone	🚠 outside-zone	👼 Inside_Net	t 📻 AnyCon	nect_Pool		📻 Inside_Net	👼 AnyConnect_Pool		ଞ୍ଚେ Dns:false ଞ୍ରେ route-lookup ଞ୍ରେ no-proxy-an	/ 1
٠	Auto NAT Rule	5											
z	+	Dynamic	🥵 any	🚠 outside-zone	🚌 obj-any				🍓 Interface			🝓 Dns:false	/ 6
٠	NAT Rules Afte	er											

Displaying 1-2 of 2 rows $|\langle \langle Page | 1 \rangle$ of 1 $\rangle \rangle | C | Rows per page: 100 -$

部署

1.配置完成後,按一下右上角的Deploy按鈕。



2.按一下FTD旁的覈取方塊,然後按一下「**Deploy**」。

Depl	Deploy Policies Version: 2020-05-04 09:40 AM X							
V	Device	Inspect Interruption	Туре	Group	Current Version	٢		
₹ 3	■ FTD-2	No	FTD		2020-05-04 09:16 AM			

Deploy

Cancel

```
Selected devices: 1
```

```
驗證
```

最終配置

AAA組態

```
> show running-configuration aaa-server
aaa-server LAB-AD protocol ldap
max-failed-attempts 4
realm-id 5
aaa-server LAB-AD host win2016.example.com
server-port 389
ldap-base-dn DC=example,DC=com
ldap-group-base-dn DC=example,DC=com
ldap-scope subtree
ldap-naming-attribute samaccountname
ldap-login-password *****
ldap-login-dn ftd.admin@example.com
server-type microsoft
```

AnyConnect配置

```
> show running-config webvpn
webvpn
enable Outside
anyconnect image disk0:/csm/anyconnect-linux64-4.7.03052-webdeploy-k9.pkg 1 regex "Linux"
anyconnect image disk0:/csm/anyconnect-win-4.7.00136-webdeploy-k9.pkg 2 regex "Windows"
anyconnect profiles Lab disk0:/csm/lab.xml
```

```
anyconnect enable
tunnel-group-list enable
cache
no disable
error-recovery disable
```

file-entry disable file-browsing disable url-entry disable deny-message none

> show running-config ssl

```
> show running-config tunnel-group
tunnel-group General type remote-access
tunnel-group General general-attributes
address-pool AnyConnect-Pool
authentication-server-group LAB-AD
tunnel-group General webvpn-attributes
group-alias General enable
> show running-config group-policy
group-policy DfltGrpPolicy attributes
vpn-simultaneous-logins 10
vpn-tunnel-protocol ikev2 ssl-client
split-tunnel-policy tunnelspecified
split-tunnel-network-list value Lab
user-authentication-idle-timeout none
webvpn
 anyconnect keep-installer none
 anyconnect modules value dart
 anyconnect ask none default anyconnect
 http-comp none
 activex-relay disable
```

anyconnect ssl df-bit-ignore enable

ssl trust-point FTD-2-SelfSigned outside

使用AnyConnect連線並驗證訪問控制策略規則

🚳 Cisco AnyCo	onnect Secu	ıre Mobili	ty Client	_		×	
	VPN: Contacting ftd2.exam	ftd2.exam ple.com	ple.com.	~	Connect		
		🕙 Cisc	o AnyConne	ect ftd2.e	xample.c	:om	×
\$ ()							
		_	Group:	General			~
			Username:	it.admin			
			Password:	******	*		
					ОК		Cancel
🔇 Cisco AnyCo	onnect Secu	ıre Mobili	ty Client	÷		×	
	VPN: Connected ftd2.exam	to ftd2.ex ple.com	ample.com.	~ D	isconnect		
00:00:12					1	IPv4	
Ö ()							

使用者IT Admin位於對Windows Server具有RDP訪問許可權的AnyConnect Admins組中,但是沒有 對HTTP的訪問許可權。

開啟與此伺服器的RDP和Firefox會話將驗證此使用者只能通過RDP訪問伺服器。



如果使用AnyConnect使用者組(作為HTTP訪問但不是RDP訪問)中的使用者測試使用者登入,我 們可以驗證訪問控制策略規則是否生效。



使用FMC連線事件進行驗證

由於在訪問控制策略規則中啟用了日誌記錄,因此可以檢查連線事件中是否存在與這些規則匹配的 任何流量

導航到分析>連線>事件。

Overview Analys	sis Policies D	evices Objec	ts AMF	P Intellige	ence	D	eploy 🔒 🤮	System Help	🔻 admin 🔻
Context Explorer	Connections v	Intrusions 🔻	Files 🔻	Hosts 🔻	Users v	Correlation v	Advanced v	Search	
	Events								
	Security Intellig	ence Events							

在Table View of Connection Events下,日誌被過濾為僅顯示IT管理員的連線事件。

在這裡,您可以驗證到伺服器的RDP流量(TCP和UDP 3389)是否被允許,但是埠80流量被阻止。

Ove	rview	Analysi	s Policies I	Devices	Objects	AMP I	ntelligence			Deplo	γ 🤒	System	Help 🔻	admin 🔻
Cont	text Ex	oplorer C	onnections + E	ivents	Intrusions	 Files 	 Hosts * 	Users v	Correlation *	Advanced ¥	Search			
								Во	okmark This Pa	ge Report Designer	Dashboar	d View B	ookmarks	Search 🔻
Conr Conr	Interction Events (switch workflow) Interction Switch workflow) Expanding Ex													
► Se	Search Constraints (<u>Edit Search Save Search</u>) Disabled Columns													
Ju	mp to													
		Action ×	Initiator × IP	Initiator	<u>r User</u> ×		Responder × IP	Ingress Security	Zone S	ecurity Zone	Source Po ICMP Typ	e <u>rt/</u> ×	Destinat ICMP Co	ion Port / × de
4		Allow	10.10.10.1	🖳 it adm	nin (LAB-AD\it	admin. LDA	P) 102 168 1	outride-a	in in	rida. zona	63.673 (he		2222 Ja	
							192.100.1	gotside a		side-zone	624737 ttp	2	3389 / to	2
4		Block	<u>i 10.10.10.1</u>	📇 it adm	nin (LAB-AD\it	admin, LDA	P) # 192.168.1	outside-z	tone in	side-zone	62474 / tep	2	80 (http)	2 / tcp
4		Block Block	10.10.10.1 10.10.10.1	lit adm	nin (LAB-AD\it nin (LAB-AD\it	admin, LDA	P) # 192.168.1	<u>outside-z</u> <u>outside-z</u>	one in one in	side-zone side-zone	62473 / tq 62474 / tq 62475 / tq	2	80 (http)	2 <u>/ tcp</u> / tcp

對於使用者**測試使用者**,可以驗證到伺服器的RDP流量是否被阻止,以及埠80流量是否被允許。

c	verview	Analysi	s Policies I	Devices	Objects	AMP	Intelligence				Deplo	y 🔒	System	Help v	admin 🔻
C	ontext Ex	plorer C	onnections • E	Events	Intrusions	 File 	es 🔻 🛛 Hosts 🔻	Users v	Correlati	on 🔻	Advanced •	Search			
									Bookmark Th	iis Page	Report Designer	Dashboar	d View Bo	okmarks	Search 🔻
	Connections onnections Search Co Jump to	ction Ev with Application with applications (Edition	Vents (switch ion Details > <u>Tab</u> t Search Save Sea	workflow) de View of arch)	f Connection	Events					II <u>2020</u>	-05-05 14:	14:17 - 20	20-05-05 Disab	<u>16:26:39</u> ⊘ Expanding oled Columns
		Action ×	Initiator × IP	Initiato	r User ×		Respond IP	er × Ins Sec	iress > urity Zone	Eq Se	ress ×	Source P ICMP Ty	<u>kont/</u> ×	Destin ICMP (ation Port / >
	1	Block	10.10.10.1	📑 <u>test u</u>	iser (LAB-AD\t	est.user, L	DAP) = 192.16	i8.1.1 out	ide-zone	insi	ide-zone	<u>62493 / ta</u>	22	3389 / 1	tap
	1	Allow	10.10.10.1	📇 <u>test u</u>	iser (LAB-AD\t	est.user, L	.DAP) 🧾 192.16	8.1.1 out	ide-zone	insi	ide-zone	<u>62494 / tr</u>	20	80 (http	b) / top

疑難排解

調試

此調試可以在診斷CLI中運行,以對LDAP身份驗證相關問題進行故障排除: debug ldap 255

要排除使用者身份訪問控制策略問題,可以私下運行system support firewall-engine-debug以確定 流量被允許或意外阻止的原因。

正在運行的LDAP調試

```
[53] Session Start
[53] New request Session, context 0x00002bld13f4bbf0, reqType = Authentication
[53] Fiber started
[53] Creating LDAP context with uri=ldap://192.168.1.1:389
[53] Connect to LDAP server: ldap://192.168.1.1:389, status = Successful
[53] supportedLDAPVersion: value = 3
[53] supportedLDAPVersion: value = 2
[53] LDAP server 192.168.1.1 is Active directory
[53] Binding as ftd.admin@example.com
[53] Performing Simple authentication for ftd.admin@example.com to 192.168.1.1
[53] LDAP Search:
       Base DN = [DC=example,DC=com]
       Filter = [sAMAccountName=it.admin]
       Scope = [SUBTREE]
[53] User DN = [CN=IT Admin, CN=Users, DC=example, DC=com]
[53] Talking to Active Directory server 192.168.1.1
[53] Reading password policy for it.admin, dn:CN=IT Admin,CN=Users,DC=example,DC=com
[53] Read bad password count 6
[53] Binding as it.admin
[53] Performing Simple authentication for it.admin to 192.168.1.1
[53] Processing LDAP response for user it.admin
[53] Message (it.admin):
[53] Authentication successful for it.admin to 192.168.1.1
[53] Retrieved User Attributes:
[53] objectClass: value = top
       objectClass: value = person
[53]
[53]
       objectClass: value = organizationalPerson
       objectClass: value = user
[53]
[53]
      cn: value = IT Admin
[53] sn: value = Admin
[53]
      givenName: value = IT
       distinguishedName: value = CN=IT Admin, CN=Users, DC=example, DC=com
[53]
       instanceType: value = 4
[53]
       whenCreated: value = 20200421025811.0Z
[53]
[53]
       whenChanged: value = 20200421204622.0Z
[53]
       displayName: value = IT Admin
[53]
       uSNCreated: value = 25896
[53]
      memberOf: value = CN=AnyConnect Admins,CN=Users,DC=example,DC=com
      uSNChanged: value = 26119
[53]
[53]
      name: value = IT Admin
       objectGUID: value = &...J..O..2w...c
[53]
       userAccountControl: value = 512
[53]
[53]
       badPwdCount: value = 6
[53]
      codePage: value = 0
[53]
       countryCode: value = 0
[53]
       badPasswordTime: value = 132320354378176394
[53]
       lastLogoff: value = 0
       lastLogon: value = 0
[53]
       pwdLastSet: value = 132319114917186142
[53]
       primaryGroupID: value = 513
[53]
[53]
       objectSid: value = ......{I...;....j...
       accountExpires: value = 9223372036854775807
[53]
[53]
      logonCount: value = 0
[53]
       sAMAccountName: value = it.admin
       sAMAccountType: value = 805306368
[53]
[53]
       userPrincipalName: value = it.admin@example.com
[53]
       objectCategory: value = CN=Person, CN=Schema, CN=Configuration, DC=example, DC=com
[53]
       dSCorePropagationData: value = 16010101000000.0Z
[53]
       lastLogonTimestamp: value = 132319755825875876
```

[53] Fiber exit Tx=515 bytes Rx=2659 bytes, status=1
[53] Session End

無法與LDAP伺服器建立連線

[-2147483611] Session Start [-2147483611] New request Session, context 0x00007f9e65ccdc40, reqType = Authentication [-2147483611] Fiber started [-2147483611] Creating LDAP context with uri=ldap://171.16.1.1:389 [-2147483611] Connect to LDAP server: ldap://172.16.1.1:389, status = Failed [-2147483611] Unable to read rootDSE. Can't contact LDAP server. [-2147483611] Fiber exit Tx=0 bytes Rx=0 bytes, status=-2 [-2147483611] Session End

潛在解決方案:

- 檢查路由並確保FTD收到來自LDAP伺服器的響應。
- 如果使用LDAPS或STARTTLS,請確保信任的根CA證書正確無誤,以成功完成SSL握手。
- •驗證使用了正確的IP地址和埠。如果使用主機名,請確認DNS能夠將其解析為正確的IP地址。

繫結登入DN和/或密碼不正確

```
[-2147483615] Session Start
[-2147483615] New request Session, context 0x00007f9e65ccdc40, reqType = Authentication
[-2147483615] Fiber started
[-2147483615] Creating LDAP context with uri=ldap://192.168.1.1:389
[-2147483615] Connect to LDAP server: ldap://192.168.1.1:389, status = Successful
[-2147483615] defaultNamingContext: value = DC=example,DC=com
[-2147483615] supportedLDAPVersion: value = 3
[-2147483615] supportedLDAPVersion: value = 2
[-2147483615] LDAP server 192.168.1.1 is Active directory
[-2147483615] supportedSASLMechanisms: value = GSSAPI
[-2147483615] supportedSASLMechanisms: value = GSS-SPNEGO
[-2147483615] supportedSASLMechanisms: value = EXTERNAL
[-2147483615] supportedSASLMechanisms: value = DIGEST-MD5
[-2147483615] Binding as ftd.admin@example.com
[-2147483615] Performing Simple authentication for ftd.admin@example.com to 192.168.1.1
[-2147483615] Simple authentication for ftd.admin@example.com returned code (49) Invalid
credentials
[-2147483615] Failed to bind as administrator returned code (-1) Can't contact LDAP server
[-2147483615] Fiber exit Tx=186 bytes Rx=744 bytes, status=-2
[-2147483615] Session End
```

潜在解決方案:驗證登入DN和登入密碼是否正確配置。這可以在使用**ldp.exe**的AD伺服器上驗證。 要驗證帳戶是否可以使用ldp成功繫結,請完成以下步驟:

1.在AD伺服器上,按Win+R並搜尋ldp.exe

🖅 Run	×
	Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.
<u>O</u> pen:	ldp.exe 🗸
	OK Cancel <u>B</u> rowse

2.在Connection下,選擇Connect...



3.指定伺服器的本地主機和相應的埠,然後按一下**確定**。

Connect		×
<u>S</u> erver:	localhost	
Port:	389	Co <u>n</u> nectionless
<u>0</u> K		<u>C</u> ancel

4. 「右」列顯示指示連線成功的文本。導航到Connection > Bind...

🔝 Idap://w	in2016.exa	ample.co	om/DC	= example, DC	=com		—		×
Connection	Browse	View	Optio	ns Utilities	Help				
Connec Bind Disconr	.t nect	Ctrl+B		ld = ldap_op Established Retrieving b Getting 1 en Dn: (RootD	en("localho connection ase DSA in tries: SE)	st", 389); to localhost. formation			^
New Save Save As Exit	;	Ctrl+N		configu CN: current Tim defaulth dnsHos domain(domain	rationNamin =Configurati Time: 5/1/20 e; VamingConte tName: win/ ControllerFu Functionality iceName: CN tings,CN=W it-Site- ne,CN=Sites n; unctionality: CommittedU CatalogRea tronized: TR viceName: C	gContext: on,DC=examp 20 4:16:55 PM ext: DC=exam 2016.example nctionality: 7 = v: 7 = (WIN20 N=NTDS IN2016,CN=Se s,CN=Configur 7 = (WIN2010 SN: 13410; dy: TRUE; RUE; example.com	lle,DC=c I Eastern ple,DC=c .com; = (WIN2 16); ervers,C ation,DC 6); win2016	om; n Daylight com; 016); N=Default- :=example,D)C=

5.選擇Simple Bind,然後指定Directory Account Username和Password。按一下「OK」(確定)。

Bind	×
<u>U</u> ser: <u>P</u> assword:	ftd.admin@example.com
Domain: Bind type Bind as cur Bind with c Simple bind	rrently logged on user redentials (DIGEST)
Encrypt tra	affic after bind Cancel OK

如果繫結成功,則ldp顯示驗證為:DOMAIN\username

🔝 Idap://w	in2016.exa	mple.co	om/DC=ex	ample,DC	=com		_		×	<
Connection	Browse	View	Options	Utilities	Help					
				1.2. 1.2. 1.2. support Max Max Max Max Max Max Max Max	840.113556 840.113556 840.113556 edLDAPPoli (PercentDir (ReceiveBu (Connection (BatchRetur (DirSyncDu (ResultSetS (ResultSetS (ValRange; eadMemory edLDAPVer edSASLMe IEGO; EXTE	5.1.4.2255; 5.1.4.2256; 5.1.4.2309; cies (20): M SyncReques ffer; InitRec is; MaxConr rnMessages ration; MaxT ize; MinRes PerConn; Max MaxValRan Limit; Syster rsion (2): 3; chanisms (4 RNAL; DIGE _s(Id, 'ftd.ad	axPoolThr sts; MaxDa vTimeout; IdleTime; I s; MaxQue fempTable ultSets; axNotificat geTransiti mMemoryL 2; 4): GSSAP ST-MD5; dmin@exal min.	eads; atagramR MaxPage ryDuratio Size; tionPerCo ve; .imitPerce l; GSS-	lecv; Size; m; onn; ent;	~
Ready										

嘗試使用無效的使用者名稱或密碼進行繫結會導致失敗,如此處所示的兩個錯誤。

🔝 Idap://w	in2016.exa	mple.co	om/DC=ex	ample,DC	=com		_		×
Connection	Browse	View	Options	Utilities	Help				
			r A E S C E ir	Max Max Max Three supporte supporte SPN es = Idap_s unavailable cuthenticate es = Idap_s unavailable rror <49>: I cerver error comment: Ac rror 0x8000	ResultSetSiz (ResultSetSiz (ValRange; MeadMemoryLedLDAPVersedSASLMection) (ValRange; MeadMemoryLedLDAPVersedSASLMection) (IEGO; EXTER (IEGO; IEGO; IEGO	ze; MinResu erConn; Ma MaxValRang imit; System sion (2): 3; 2 hanisms (4) NAL; DIGES s(Id, 'ftd.adr PLE\ftd.adr s(Id, 'wrong bind_s() fai LdapErr: DS yContext er oken supplie	ItSets; xNotificat eTransitiv MemoryL :: GSSAPI :: GSSAPI ST-MD5; min@exar nin'. @exampl iled: Invali SID-0C090 ror, data d to the fi	ionPerConn /e; imitPercent; ; GSS- nple.com', le.com', d Credentia 042A, 52e, v3839 unction is	is V
Ready									

LDAP伺服器找不到使用者名稱

```
[-2147483612] Session Start
[-2147483612] New request Session, context 0x00007f9e65ccdc40, reqType = Authentication
[-2147483612] Fiber started
[-2147483612] Creating LDAP context with uri=ldap://192.168.1.1:389
[-2147483612] Connect to LDAP server: ldap://192.168.1.1:389, status = Successful
[-2147483612] supportedLDAPVersion: value = 3
[-2147483612] supportedLDAPVersion: value = 2
[-2147483612] LDAP server 192.168.1.1 is Active directory
[-2147483612] Binding as ftd.admin@example.com
[-2147483612] Performing Simple authentication for ftd.admin@example.com to 192.168.1.1
[-2147483612] LDAP Search:
       Base DN = [dc=example,dc=com]
       Filter = [samaccountname=it.admi]
       Scope
               = [SUBTREE]
[-2147483612] Search result parsing returned failure status
[-2147483612] Talking to Active Directory server 192.168.1.1
[-2147483612] Reading password policy for it.admi, dn:
[-2147483612] Binding as ftd.admin@example.com
[-2147483612] Performing Simple authentication for ftd.admin@example.com to 192.168.1.1
[-2147483612] Fiber exit Tx=456 bytes Rx=1082 bytes, status=-1
[-2147483612] Session End
潜在解決方案:驗證AD能否使用FTD完成的搜尋找到使用者。這也可使用Idp.exe完成。
```

1.成功繫結後(如上所示),導航到**檢視>樹**。

🔝 Idap://w	in2016.exa	mple.	.com/DC=e	xample,DC	=com			_		×	
Connection	Browse	View	/ Options	Utilities	Help						
		~	Tree Enterprise Status Bar	Configurat	ion	Ctrl+T	/axP sts; cvTir	PoolThr MaxDa meout:	eads; atagramR	ecv;	^
			Set Font				nidle s: Mi	eTime; I axQue	MaxPage: rvDuratio	Size; n:	
				Max Max Max Supporte Supporte SPN	DirSyncl ResultSe ResultSe ValRang adMemo edLDAP edSASLI EGO; EX	Duration; Ma etSize; MinF etsPerConn je; MaxValF oryLimit; Sys /ersion (2): Mechanisms (TERNAL; D	axTem ResultS ; MaxN RangeT stemMe : 3; 2; s (4): G IGEST-	pTable Sets; Iotificat Transitiv emoryL GSSAPI -MD5;	Size; tionPerCo ve; .imitPerce I; GSS-	ent;	
				res = Idap_s <unavailable Authenticate</unavailable 	imple_bi ⊳); // v.3 ed as: 'E>	nd_s(ld, 'ftd (AMPLE\ftd	I.admin .admin'	i@exai '.	mple.com	ι,	
			J								×

2.指定在FTD上設定的基本DN,然後按一下「OK」

Tree View	×
BaseDN: DC=example,DC=com	~
Cancel	ОК

3.按一下右鍵基本DN,然後按一下**Search**。

🔝 Idap://wi	n2016.exa	mple.co	om/DC=ex	ample,DC	=com	- 🗆 X	
Connection	Browse	View	Options	Utilities	Help		
<u> •</u> · <u> DC=exam</u>	iple,DC=c	om	Search Virtual L Delete Modify Modify Add chil Compar Advance Copy DN Copy Select al Clear ou	ist View DN Id e ed N	Ctrl+S Ctrl+D Ctrl+M Ctrl+R Ctrl+A Ctrl+A	cipals,DC=example,DC=com; 11D2B9AA00C04F79F805:CN =example,DC=com; 11D297C400C04FD8D5CD:C =example,DC=com; 11D1ADED00C04FD8D5CD:C =example,DC=com; 11D1ADED00C04FD8D5CD:C ple,DC=com; 11D1AA4B00C04FD7D83A:O s,DC=example,DC=com; 11D1ADED00C04FD8D5CD:C ample,DC=com; 311D1ADED00C04FD8D5CD:C e,DC=com; 0 3:43:59 PM Eastern Daylight 2:41:57 PM Eastern Daylight	~
Create a new o	locument						

4.指定與debug中相同的Base DB、Filter和Scope值。

在此範例中,這些如下:

- 基本DN:dc=example,dc=com
- •篩選器:samaccountname=it.admi
- 範圍:子樹

🟠 Idap://w	n2016.example.com/DC=example,DC=com		— C) X	
Connection	Browse View Options Utilities Help				
Search		\times	C=example,DC=com; 8811D1ADED00C04FD DC=example DC=com;	8D5CD:C	^
Base DN:	DC=example,DC=com	\sim	8811D1ADED00C04FD	8D5CD:C	
Filter:	sAMAccountName=it.admi	~ =	mple,DC=com; D211D1AA4B00C04FD	07D83A:0	
Scope O Base	One Level Subtree	B F	ers,DC=example,DC=co 8811D1ADED00C04FD example,DC=com;	om;)8D5CD:C	
Attributes:	objectClass;name;description;canonicalName		8811D1ADED00C04FE ple,DC=com;)20 3:43:59 DM Easter	08D5CD:C	
Options	Run Close		20 2:41:57 PM Eastern	Daylight	
	***Searching ldap_search_s(ld, "Du "sAMAccountName=i Getting 0 entries:)C=exa it.admi	ample,DC=com", 2, ", attrList, 0, &msg)		~
Ready					

ldp發現0個條目,因為在Base DN dc=example,dc=com下沒有具有samaccountname **it.admi**的使 用者帳戶

使用正確的samaccountname **it.admin**的另一嘗試顯示不同的結果。ldp在Base DN dc=example,dc=com下找到1個條目,並列印該使用者DN。

🔝 Idap://wi	n2016.example.com	n/DC=exar	mple,DC:	=com		>	<
Connection	Browse View C	Options	Utilities	Help			
Search					×	58811D1ADED00C04FD8D5CD:C DC=example,DC=com; 58811D1ADED00C04FD8D5CD:C	^
Base <u>D</u> N:	DC=example,DC=co	m			\sim	ample,DC=com;	
<u>F</u> ilter:	sAMAccountName=i	t.admin			\sim	lers,DC=example,DC=com;	,
Scope O <u>B</u> ase	O <u>O</u> ne Level) <u>S</u> ubtree				58811D1ADED00C04FD8D5CD:C example,DC=com; 68811D1ADED00C04FD8D5CD:C mple.DC=com;	2
<u>A</u> ttributes:	objectClass;name;de	escription;c	anonicalN	lame	\sim	020 3:43:59 PM Eastern Daylight	t
Options		<u>R</u> un		<u>C</u> lose)20 2:41:57 PM Eastern Daylight	
		***S Idaj "sA Get Dn:	Searching p_search MAccour tting 1 ent CN=IT A canonica name: IT objectCla user	 _s(ld, "I ntName: ries: . dmin,(alName: Admin; ass (4): ;	DC=e: =it.ad CN=U exar top;	xample,DC=com", 2, lmin", attrList, 0, &msg) Isers,DC=example,DC=com mple.com/Users/IT Admin; person; organizationalPerson;	
Ready		1					

使用者名稱密碼不正確

```
[-2147483613] Session Start
[-2147483613] New request Session, context 0x00007f9e65ccdc40, reqType = Authentication
[-2147483613] Fiber started
[-2147483613] Creating LDAP context with uri=ldap://192.168.1.1:389
[-2147483613] Connect to LDAP server: ldap://192.168.1.1:389, status = Successful
[-2147483613] supportedLDAPVersion: value = 3
[-2147483613] supportedLDAPVersion: value = 2
[-2147483613] LDAP server 192.168.1.1 is Active directory
[-2147483613] Binding as ftd.admin@example.com
[-2147483613] Performing Simple authentication for ftd.admin@example.com to 192.168.1.1
[-2147483613] LDAP Search:
       Base DN = [dc=example,dc=com]
       Filter = [samaccountname=it.admin]
               = [SUBTREE]
       Scope
[-2147483613] User DN = [CN=IT Admin, CN=Users, DC=example, DC=com]
[-2147483613] Talking to Active Directory server 192.168.1.1
[-2147483613] Reading password policy for it.admin, dn:CN=IT Admin,CN=Users,DC=example,DC=com
[-2147483613] Read bad password count 0
[-2147483613] Binding as it.admin
[-2147483613] Performing Simple authentication for it.admin to 192.168.1.1
```

```
[-2147483613] Simple authentication for it.admin returned code (49) Invalid credentials
[-2147483613] Message (it.admin): 80090308: LdapErr: DSID-0C09042A, comment:
AcceptSecurityContext error, data 52e, v3839
[-2147483613] Invalid password for it.admin
[-2147483613] Fiber exit Tx=514 bytes Rx=2764 bytes, status=-1
[-2147483613] Session End
潜在解決方案:驗證使用者密碼是否正確配置且未過期。與登入DN類似,FTD會使用使用者憑證與
```

AD進行繫結。

此繫結也可以在ldp中完成,以驗證AD是否能夠識別相同的使用者名稱和密碼憑據。ldp中的步驟顯 示在**繫結登入DN和/或密碼不正確**一節中。

此外,還可以檢視Microsoft**伺服器事**件檢視器日誌,以瞭解可能的原因。

測試AAA

test aaa-server命令可用於使用特定使用者名稱和密碼來模擬從FTD進行的身份驗證嘗試。這可用 於測試連線或身份驗證失敗。命令是test aaa-server authentication [AAA-server] host [AD IP/hostname]

> show running-configuration aaa-server aaa-server LAB-AD protocol ldap realm-id 7 aaa-server LAB-AD host win2016.example.com server-port 389 ldap-base-dn DC=example,DC=com ldap-scope subtree ldap-login-password ***** ldap-login-dn ftd.admin@example.com server-type auto-detect > test aaa-server authentication LAB-AD host win2016.example.com Username: it.admin Password: ******* INFO: Attempting Authentication test to IP address (192.168.1.1) (timeout: 12 seconds) INFO: Authentication Successful

封包擷取

封包擷取可用於驗證與AD伺服器的連線能力。如果LDAP封包離開FTD,但沒有回應,這可能表示 路由問題。

Capture顯示雙向LDAP流量。

> show route 192.168.1.1

Routing entry for 192.168.1.0 255.255.255.0
Known via "connected", distance 0, metric 0 (connected, via interface)
Routing Descriptor Blocks:
* directly connected, via inside
 Route metric is 0, traffic share count is 1

> capture AD interface inside match tcp any host 192.168.1.1 eq 389

> show capture

capture AD type raw-data interface inside [Capturing - 0 bytes] match tcp any host 192.168.1.1 eq ldap > test aaa-server authentication LAB-AD host win2016.example.com username it.admin password ***** INFO: Attempting Authentication test to IP address (192.168.1.1) (timeout: 12 seconds) INFO: Authentication Successful > show capture capture AD type raw-data interface inside [Capturing - 10905 bytes] match tcp any host 192.168.1.1 eq ldap > show capture AD 54 packets captured 192.168.1.17.61960 > 192.168.1.1.389: S 3681912834:3681912834(0) win 1: 23:02:16.770712 32768 <mss 1460,nop,nop,timestamp 1061373057 0> 192.168.1.1.389 > 192.168.1.17.61960: S 491521506:491521506(0) ack 2: 23:02:16.772009 3681912835 win 8192 <mss 1460,nop,nop,timestamp 762393884 1061373057> 192.168.1.17.61960 > 192.168.1.1.389: . ack 491521507 win 32768 3: 23:02:16.772039 <nop,nop,timestamp 1061373058 762393884> 4: 23:02:16.772482 192.168.1.17.61960 > 192.168.1.1.389: P 3681912835:3681912980(145) ack 491521507 win 32768 <nop,nop,timestamp 1061373059 0> 5: 23:02:16.772924 192.168.1.1.389 > 192.168.1.17.61960: P 491521507:491522141(634) ack 3681912980 win 65160 <nop,nop,timestamp 762393885 1061373059> 6: 23:02:16.772955 192.168.1.17.61960 > 192.168.1.1.389: . ack 491522141 win 32768 <nop,nop,timestamp 1061373059 762393885> 7: 23:02:16.773428 192.168.1.17.61960 > 192.168.1.1.389: P 3681912980:3681913024(44) ack 491522141 win 32768 <nop,nop,timestamp 1061373060 0> 192.168.1.1.389 > 192.168.1.17.61960: P 491522141:491522163(22) ack 8: 23:02:16.775030 3681913024 win 65116 <nop,nop,timestamp 762393887 1061373060> 9: 23:02:16.775075 192.168.1.17.61960 > 192.168.1.1.389: . ack 491522163 win 32768 <nop,nop,timestamp 1061373061 762393887> [...] 54 packets shown

Windows Server事件檢視器日誌

AD伺服器上的**事件檢視器**日誌可以提供有關失敗原因的更詳細資訊。

1.搜尋並開啟「事件查看器」。

=	Best match									
ŵ	E D	vent V esktop	f iewer app							
	Settings						>			
	🖄 Viev	v even	t logs							
٢	10	۲	ß		53	□	la.			
	event									
	ו כ	[]]	e	-	2	2	8			

2.展開Windows Logs,然後按一下Security。使用使用者帳戶名稱搜尋稽核失敗並檢視失敗資訊。



An account failed to log on.

Subject: Security ID:SYSTEM Account Name:WIN2016\$ Account Domain:EXAMPLE Logon ID:0x3E7

Logon Type:3

Account For Which Logon Failed: Security ID:NULL SID Account Name:it.admin Account Domain:EXAMPLE

Failure Information:

Failure Reason: The specified user account has expired. Status: 0xC0000193 Sub Status: 0x0

Process Information: Caller Process ID:0x25c Caller Process Name:C:\Windows\System32\lsass.exe

Network Information: Workstation Name:WIN2016 Source Network Address:192.168.1.17 Source Port:56321

關於此翻譯

思科已使用電腦和人工技術翻譯本文件,讓全世界的使用者能夠以自己的語言理解支援內容。請注 意,即使是最佳機器翻譯,也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準 確度概不負責,並建議一律查看原始英文文件(提供連結)。