在FDM管理的FTD上為AnyConnect客戶端配置 AD(LDAP)身份驗證和使用者身份

目錄

簡介 必要條件 需求 採用元件 設定 網路圖表和案例 AD配置 確定LDAP基本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) FDM配置 驗證許可 設定AD身份源 配置AnyConnect進行AD身份驗證 啟用身份策略並為使用者身份配置安全策略 驗證 最終配置 使用AnyConnect連線並驗證訪問控制策略規則 疑難排解 調試 工作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

本文旨在詳細說明如何為連線到由Firepower裝置管理(FDM)管理的Cisco Firepower威脅防禦 (FTD)的AnyConnect客戶端配置Active Directory(AD)身份驗證。 使用者身份將用於訪問策略,以將 AnyConnect使用者限製為特定IP地址和埠。

必要條件

需求

思科建議您瞭解以下主題:

- FDM上RA VPN配置的基本知識
- 有關FDM上的LDAP伺服器配置的基本知識
- 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
- 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。

設定

網路圖表和案例



Windows伺服器已預配置Internet資訊服務(IIS)和遠端案頭協定(RDP),以便測試使用者身份。在此 配置指南中,將建立三個使用者帳戶和兩個組。

使用者帳戶:

- •FTD管理員:這將用作目錄帳戶,以允許FTD繫結到AD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:IT管理員將新增到以演示使用者身份的測試組。此組將僅具有對Windows Server的RDP訪問許可權
- AnyConnect使用者:测試使用者將新增到的一個測試組,用於演示使用者身份。此組將僅具有 對Windows Server的HTTP訪問許可權

AD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FDM上完成配置之前,必須在 Microsoft Server上建立或收集所有這些詳細資訊。主要值為:

- 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FDM和FTD中配置DNS伺服器才能解析FQDN。在本配置指南中,這些值為 win2016.example.com,解析為192.168.1.1。
- 伺服器埠:LDAP服務使用的埠。預設情況下,LDAP和STARTTLS將對LDAP使用TCP埠 389,而LDAP over SSL(LDAPS)將使用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FDM和FTD用於繫結到LDAP伺服器、驗證使用者以及搜尋使用 者和組的帳戶。將為此建立名為FTD Admin的帳戶。
- •基本可分辨名稱(DN):基礎DN是FDM的起點,FTD將通知Active Directory在搜尋使用者時開始 使用。在本配置指南中,根域example.com將用作基礎DN;但是,對於生產環境,在LDAP層次 結構中使用基本DN可能更好。例如,以此LDAP層次結構為例:



如果管理員希望市場行銷組織單位中的使用者能夠對基本DN進行身份驗證,則可以將基本DN設定 為根(example.com),但是,這也會允許財務組織單位下的User1也登入,因為使用者搜尋將從根開 始,並轉到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,因為搜尋將從市場行銷開始。

基本DN設定為Marketing:



請注意,為了在FTD內實現更精細的控制,允許使用者根據其AD屬性連線或分配不同的授權,需要 配置LDAP授權對映。

本配置指南中使用此簡化的LDAP層次結構,根example.com的DN將用於基礎DN。



確定LDAP基本DN

1.開啟AD使用者和電腦。

=	Best mate	ch							
ŵ	🥑 A D	ctive E esktop	Director app	y User	s and C	Comput	ers		
	Settings >								
	Edit	8 Edit local users and groups							
	陀 Cha	nge U	ser Acc	ount C	ontrol	settings	s		
	🍇 Use	r Acco	unts						
	Select users who can use remote desktop								
۲	11	۲	ß				វរា		
	users								
	ر مر		e	-	1	6	*0		

2.左鍵點選根域(以便開啟容器),右鍵點選根域,然後導航到**檢視**,然後按一下**高級功能**。



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,然後導航到**屬性**。



4.在**屬性**下,按一下**屬性編輯器**頁籤。在「屬性」下查詢distinguishedName,然後按一下**檢視**。

example.com Properties		?	×
General Managed By 0	bject Security Attribute Editor	-	
Attributes:			
Attribute	Value		^
dc	example		
derautLocalPolicyObj	(not set)		
desktopPorfile	(not set)		
displayName	(not set)		
displayNamePrintable	(not set)		
distinguishedName	DC=example_DC=com		
domainPolicyObject	<not set=""></not>		
domainReplica	<not set=""></not>		
dSASignature	{ V1: Rags = 0x0; LatencySecs	= 0; DsaGuic	
dSCorePropagationD	0x0 = ()		
eFSPolicy	<not set=""></not>		
extensionName	<not set=""></not>		
flags	<not set=""></not>		~
<		>	
Vew		Fiter	
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FDM中。在本示例中,根DN為
```

DC=example, DC=com。複製值。按一下**OK**以退出「字串屬性編輯器」視窗,然後再次按一下 **OK**以退出屬性。

String Attribute Editor ×	
Attribute: distinguishedName Value:	
DC=example,DC=com Clear OK Cancel	Undo
	Copy Paste
	Delete
	Select All
	Right to left Reading order
	Show Unicode control characters
	Insert Unicode control character
example.com Properties ? × General Managed By Object Security Attribute Editor Attributes: Attribute Value on ont set> controlAccessRights ont set> creationTime 4/29/2020 2:43:49 PM Eastern Daylight Tim dc example default.localPolicyObj ont set> desktopProfile ont set> displayName OC=example.DC=com domainPolicyObject ont set> displayItere (V1: Rags = 0x0; LatencySecs = 0; DsaGuit dSCorePropagationD 0x0 = ()	
< > New Fiter	
OK Cancel Apply Help	

可以對AD內的多個對象執行此操作。例如,以下步驟用於查詢使用者容器的DN:



6.可以刪除「高級功能」檢視。按一下右鍵根DN,導航到View,然後再次按一下Advanced Features。



建立FTD帳戶

此使用者帳戶將允許FDM和FTD與AD繫結,以搜尋使用者和組並對它們進行身份驗證。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範圍內。

1.在**Active Directory使用者和電腦**中,按一下右鍵FTD帳戶將新增到其中的容器/組織。在此組態中 ,FTD帳戶會新增到使用者名稱**ftd.admin@example.com**下的使用者容器下。按一下右鍵 **Users**,然後按一下**New > User**。

Active Directory Users and Con	-		х					
File Action View Help								
🗢 🄿 🙍 🔂 💰 📋 🗙	⊨ ⇒ 2 📷 4 🗉 🗙 🖾 9 🔒 🛛 🖬 🖏 🐄 🖄 🦅 🗵 🎘							
 Active Directory Users and Com Saved Queries Saved Queries Builtin Computers Domain Controllers ForeignSecurityPrincipal: Managed Service Accour Users Delegate Control Find 		Type User Security Group Security Group 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 All domain guests All domain users			^		
All Tasks View Refresh Export List Properties Help	> > WseAlertA & WseAllow WseAllow	Contact Group InetOrgPerson msDS-KeyCreder msDS-ResourceP msDS-ShadowPr msImaging-PSPs MSMQ Queue Al Printer User Shared Folder	ntial PropertyList incipalContainer ias			~		
Creates a new item in this container.		sharea rotael						

2.瀏覽「新建**對象 — 使用者向**導」。

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

New Object - User		×
🤱 Create in: exam	nple.com/Users	
Password:	•••••	
Confirm password:	•••••	
User must change passw	ord at next logon	
User cannot change pass	brown	
Password never expires		
Account is disabled		
	< Back Next >	Cancel
New Object - User		×
New Object - User	nple.com/Users	×
New Object - User Create in: exam When you click Finish, the for	nple.com/Users Nowing object will be created:	×
New Object - User Create in: exam When you click Finish, the for Full name: FTD Admin	nple.com/Users llowing object will be created:	×
New Object - User Create in: exam When you click Finish, the for Full name: FTD Admin User logon name: ftd.admin@	nple.com/Users Nowing object will be created: Bexample.com	×
New Object - User Create in: exam When you click Finish, the for Full name: FTD Admin User logon name: ftd.admin@ The password never expires	nple.com/Users Nowing object will be created: Bexample.com	×
New Object - User Create in: exam When you click Finish, the for Full name: FTD Admin User logon name: ftd.admin@ The password never expires	nple.com/Users llowing object will be created: @example.com	×
New Object - User Create in: exam When you click Finish, the for Full name: FTD Admin User logon name: ftd.admin@ The password never expires	nple.com/Users Nowing object will be created: Bexample.com	×
New Object - User Create in: exam When you click Finish, the for Full name: FTD Admin User logon name: ftd.admin@ The password never expires	nple.com/Users Nowing object will be created: Pexample.com	×
New Object - User Create in: exam When you click Finish, the for Full name: FTD Admin User logon name: ftd.admin@ The password never expires	nple.com/Users Nowing object will be created: Pexample.com	×
New Object - User Create in: exam When you click Finish, the for Full name: FTD Admin User logon name: ftd.admin@ The password never expires	nple.com/Users Nowing object will be created: Pexample.com	×

3.驗證是否已建立FTD帳戶。此外,還另外建立了兩個帳戶,**IT管理**員和**測試使用者**。

Active Directory Users and Computers						×	
File Action View Help							
🗢 🔿 🙍 📅 🔏 🗎 🗙 🛛	⊨ ⇒ 2 📅 🔏 🗈 🗶 🖾 🧟 🖬 📲 🖼 🧏 🤽 🕲 🦷 🧕 🍇						
 Active Directory Users and Com Saved Queries Saved Queries Saved Queries Builtin Computers Domain Controllers ForeignSecurityPrincipals Managed Service Accour Users 	Name DefaultAcco DefaultAcco Denied ROD DonsUpdateP Domain Ad Domain Ad Domain Co Domain Co Domain Gue Domain Gue Domain Users Enterprise A Enterprise A Enterprise R Enterprise R	Type User Security Group Security Group User User User User 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 All domain users Designated administrato Members of this group Members of this group Built-in account for gue Members of this group Members of this group			^	
	Read-only D	Security Group Security Group	Members of this group Designated administrato				
< >	Test User	User				÷	

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,以後將通過FDM中的使用者標識使用組來應用訪問控制策略設定。

1.在Active Directory**使用者和電腦**中,按一下右鍵新組將新增到其中的容器/組織。在本示例中 ,AnyConnect Admins組將新增到Users容器下。按一下右鍵Users,然後按一下New > Group。

Active Directory Users and Comp	puters			-		×		
File Action View Help								
🗢 🔿 🙍 📅 🔏 🗈 🗶 🛛	⊨⇒ 22 📷 & 🗈 🗙 🖾 @ 🖦 월 📷 🖏 📚 🖄 🦷 🧕 🗞							
Active Directory Users and Com Saved Queries Saved Queries Save	Name DefaultAcco Denied ROD DnsAdmins DnsUpdateP Domain Ad Domain Co trol ers	Type User Security Group 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 All domain guests All domain users			^		
All Tasks View Refresh Export List Properties Help	>	Contact Group InetOrgPerson msDS-KeyCreder msDS-ResourceP msDS-ShadowPr msImaging-PSPs MSMQ Queue Al	itial PropertyList incipalContainer ias					
Creates a new item in this container.	Schema A	Printer User Shared Folder				Ŷ		

2.瀏覽「新建**對象 — 組**」嚮導,如下圖所示。

New Object - Group	>
🥵 Create in: exam	nple.com/Users
Group name:	
AnyConnect Admins	
Group appeal for a Windows 20	202).
AnyConnect Admins	
Group scope	Group type
O Domain local	Security
Global	ODistribution
OUniversal	
	OK Cancel

3.驗證是否已建立組。還建立了AnyConnect Users組。

Active Directory Users and Computers						×		
File Action View Help								
🗢 🔿 🙍 📰 🔏 🗙 🖼 🛛	- + 2 📰 4 🗙 🖾 🗟 🖬 🖏 2 🖬 7 🗕 2							
Active Directory Users and Com Saved Queries Saved Queries Builtin Computers Solution ForeignSecurityPrincipals Managed Service Accour Users	Name AnyConnect Admins AnyConnect Users Calo Cert Publishers Cloneable Domain C DefaultAccount DefaultAccount DefaultAccount DonsAdmins DonsUpdateProxy DonsUpdateProxy 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 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 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					
` ` ` `	(ha					v		

4.按一下右鍵要新增至的使用者的組,然後選擇**屬性**。在此配置中,使用者IT Admin將新增到 AnyConnect Admins組,使用者Test User將新增到AnyConnect Users組。

Active Directory Users and Comp		-		×			
File Action View Help							
⊨ ⇒ 22 📅 🔏 🗈 🗙 🖼 @ 🖦 🛛 🖬 🖏 🍬 🏗 🍞 🔤 🍬							
Active Directory Users and Com	Name	Туре	Description			^	
 Saved Queries example.com Builtin Computers Domain Controllers ForeignSecurityPrincipal: Managed Service Accour Users 	AnyConnect Admins AnyConnect Users Calo Cert Publishers Cloneable Domain C DefaultAccount Denied RODC Passw Donain RODC Passw DosAdmins DosUpdateProxy Domain Admins Domain Computers Domain Computers Domain Guests Domain Guests Domain Guests Domain Users Enterprise Admins Enterprise Read-only FTD Admin Group Policy Creator Guest	Security Group Security Group User Security Group Security Group User	Add to a group Buil Move Mer Send Mail Mer All Tasks Mer Cut DNS Delete DNS Rename Des All Cut Help All communications All domain users Designated administrato Members of this group Members of this group Members in this group c Built-in account for que	>			
	Key Admin	User Security Group	Members of this group				
< >> >	(h					×	

5.按一下**Members**標籤,然後按一下**Add**,如下圖所示。

AnyConnect Admins	Properties			?	×
General Members	Member Of	Managed By			
Members:					
Name	Active Dire	ectory Domain	Services Folder		
Add	Remove	ОК	Cancel	App	Ŋy

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

Select Users, Contacts, Computers, Service Accounts, or Grou	ips X
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 (axamples):	
IT Admin (It.admin@example.com)	Check Names
Advanced	K Cancel

驗證是否新增了正確的使用者,然後按一下**OK**按鈕。使用者測試使用者也使用相同的步驟新增到組 AnyConnect使用者。

AnyConn	ect Admin	s Properties			?	×
General	Members	Member Of	Managed By			
Membe	rs:					_
Name	Admin	Active Din example.c	ectory Domain om/Users	Services Folder		
Ad	d	Remove	ОК	Cancel	Ap	ply

複製LDAPS SSL證書根(僅對於LDAPS或STARTTLS是必需的)

1.按Win+R並鍵入mmc.exe。按一下「OK」(確定)。

	-	
1000	0	
	100	
_		

0	Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.						
<u>O</u> pen:	mmc.exe		~				
	ОК	Cancel	Browse				

2.導航到**檔案>新增/刪除管理單元……**如下圖所示。

ᡖ Co	nsole1 - [C	onsole F	loot]								_	×
🚡 File	Action	View	Favorites	Window	Help							. 8 ×
4	New			Ctrl+N								
	Open			Ctrl+0					A	ctions		
	Save			Ctrl+S	There are	no items t	o show in this v	iew.	C	onsole Root		
	Save As				More Actions				More Actions		+	
	Add/Rem	nove Sna	p-in	Ctrl+M								
	options	•										
	1 dnsmgi	mt										
	2 asa											
	Exit											
Enables	you to add	snap-in	s to or remo	ove them fro	m the snap-in cons	ole.						

3.在可用管理單元下,按一下Certificates,然後按一下Add。

Add or Remove Snap-ins				×				
You can select snap-ins for this console from those available on your computer and configure the selected set of snap-ins. For extensible snap-ins, you can configure which extensions are enabled.								
Available snap-ins:			Selected snap-ins:					
Snap-in	Vendor	^	Console Root Edit Extensions					
Active Directory Do	Microsoft Cor Microsoft Cor		Bemove					
Active Directory Use	Microsoft Cor Microsoft Cor		Move Up	1				
Authorization Manager	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	Ad <u>v</u> anced					
Description: The Certificates snap-in allows you to browse the contents of the certificate stores for yourself, a service, or a computer.								
			OK Cancel					

4.選擇「Computer account」,然後按一下「Next」,如下圖所示。

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

按一下「Finish」(結束)。

Select Computer	×
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: Browse Another computer: Browse Allow the selected computer to be changed when launching from the command line. This only applies if you save the console.	
< Back Finish Cancel	

5.按一下**確定**。

Add or Remove Snap-ins					×			
You can select snap-ins for this console from those available on your computer and configure the selected set of snap-ins. For extensible snap-ins, you can configure which extensions are enabled.								
Available snap-ins:				Selected snap-ins:				
Snap-in	Vendor	^		Console Root Edit Extensions				
Active Directory Do	Microsoft Cor			Certificates (Local Computer)				
Active Directory Site	Microsoft Cor			Benere	- 1			
Active Directory Use	Microsoft Cor							
ActiveX Control	Microsoft Cor			Move <u>U</u> p				
ADSI Edit	Microsoft Cor			Move Down				
Authorization Manager	Microsoft Cor		<u>A</u> dd >					
Certificates	Microsoft Cor							
Certification Authority	Microsoft Cor							
Component Services	Microsoft Cor							
A Computer Managem	Microsoft Cor							
Device Manager	Microsoft Cor							
📅 Disk Management	Microsoft and	~		Ad <u>v</u> anced				
			1		_			
Description:					_			
The Certificates snap-in allo	ws you to browse	the	contents of the	certificate stores for yourself, a service, or a computer.				
				OK Cancel				

6.展開**Personal**資料夾,然後按一下**Certificates**。LDAPS使用的證書應頒發給Windows伺服器的完 全限定域名(FQDN)。在此伺服器上列出了3個證書。

• 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。

ᡖ o	onsole1 - [Console Root\Certific	ates (Local Computer)\Personal\Certi	ficates]			-	\Box \times
ᡖ Fi	le Action View Favorites	Window Help					- 8 ×
(• •) 🖄 📆 🛱 🗖 🖓	? 🖬					
📔 C	onsole Root	Issued To	Issued By	Expiration Da	Actions		
× 📮	Certificates (Local Computer)	🛱 example-WIN2016-CA	example-WIN2016-CA	4/19/2060	Certificates		
ľ	Personal Contificator	2 WIN2016	example-WIN2016-CA	4/27/2025	More Actions		+
Ļ	Trusted Root Certification	🖏 win2016.example.com	example-WIN2016-CA	4/28/2021			
5	Enterprise Trust						
>	Intermediate Certification.						
>	Trusted Publishers						
>	Untrusted Certificates						
>	Third-Party Root Certificat						
>	Trusted People						
>	Client Authentication Issue						
2	Preview Build Koots						
2	Eocal NonKemovable Cert Remote Deckton						
	Certificate Enrollment Ren						
5	Smart Card Trusted Roots						
Ś	Trusted Devices						
5	Web Hosting						
>	Windows Live ID Token Iss						
<	>	×		>			
Persor	al store contains 3 certificates.						

7.要用作LDAPS SSL證書,證書必須符合以下要求:

• 公用名稱或DNS使用者替代名稱與Windows Server的FQDN匹配。

• 證書在Enhanced Key Usage欄位下具有伺服器身份驗證。

在證書的「詳細資訊」頁籤下的Subject和Subject替代名稱下,存在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	
Ent Contraction	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	¢

🙀 Certif	ficate			×
General	Details	Certification Path		
Show:	<al></al>		~	
Field Sult Au CR Au	bject Key thority Ke L 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	^
Key The The	y Usage umbprint a umborint	native Name	Other Name:DS Object Guid= Digital Signature, Key Encipher sha1 ca 8e 11 3d eb bc 0f 6e 4a 00	*
Other N DS C 18 DNS Na	lame: Object Gu me=win2	d=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,出現Server Authentication。

🙀 Certi	ficate			×
General	Details	Certification Path		
Show:	<al></al>		\sim	
Field			Value	^
E Su E Pu	bject blic key	samatare	win2016.example.com RSA (2048 Bits)	
Ce Ce	rtificate T	emplate Name	DomainController	
Client / Server	hanced K IIME Capa bject Key thority Ka thority Ka Authenticz Authenticz	ey Usage bilities Identifier or Identifier ation (1.3.6.1.5.5. ation (1.3.6.1.5.5.	Client Authentication (1.3.6.1 [1]SMIME Capability: Object I 30 b7 2b 4e 48 0f 2f 17 17 e6 KevID=3d 9f 26 37 fb 11 1f 4 7.3.2) 7.3.1)	>
		Ed	It Properties Copy to File	
			0	(

8.確認後,請導航至**認證路徑**標籤。按一下應該為根CA證書的頂級證書,然後按一下View Certificate按鈕。

💽 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。

Certificate	Х
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	1
ОК	

10.開啟Details頁籤,然後單擊Copy to File... 如下圖所示。

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

11.瀏覽將以PEM格式匯出根CA的證書匯出嚮導。

÷	🛃 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, dick Next.	
	Net Const	
	<u>N</u> ext Cancel	

12.選擇Base-64 encoded X.509。

÷	🐓 Certificate Export Wizard	×
	Export 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)	
	Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)	
	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) 	
	Next Ca	ncel

13.選擇檔案的名稱和匯出位置。

Erile 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	

14.按一下**完成**。

÷	Ş	Certificate Export Wizard		×
		Completing the Certificate Exp	oort 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 Cano	el :

15.現在,導航到該位置,並使用記事本或其他文本編輯器開啟證書。這將顯示PEM格式證書。儲存 以備以後使用。

----BEGIN CERTIFICATE----

```
MIIDCDCCAfCgAwIBAgIQE4ZG5Z1wT6lONTjooEQyMTANBgkqhkiG9w0BAQsFADAd
MRswGQYDVQQDExjleGFtcGxlLVdJTjIwMTYtQ0EwIBcNMjAwNDI3MTQ1MDU5WhgP
MjA2MDA0MTkxNDUwNTlaMB0xGzAZBgNVBAMTEmV4YW1wbGUtV010MjAxNi1DQTCC
ASIwDQYJKoZIhvcNAQEBBQADqqEPADCCAQoCqqEBAI8qhT719NzSQpoQPh0YT67b
Ya+PngsxMyvkewP33QLTAWw1HW1Tb9Mk5BDW0ItTaVsgHwPBfd++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----

FDM配置

驗證許可

要在FDM上配置AnyConnect,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許可證。

1.導覽至**Device > Smart License**,如下圖所示。

CISCO. Firepower Devic	ce Manager	Monitoring Policies	:문도 Objects	Device: FTD-3	\odot	۵ ۵	?:	admin Adm/nistrator
	raide Netwo	Cisco Firepower Thread I	07 Dufense for V ● 0 0/1 0/2 2 2 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	MGAFT COMPOSE	ISP/WAN/Gatowey	Internet Internet DNS Server ONTP Server Smart License		
Interfaces Connected Enabled 3 of 4 View All Interfaces	>	Routing 2 routes View Configuration	>	Updates Geolocation, Rul Security Intellige View Configurat	e, VDB, System Upgrade, nce Feeds	Syste Manag Loggin DHCP 5 DNS 50	em Setting: ement Access g Settings Server inver	\$
Smart License Registered View Configuration	>	Backup and Restore	•	Troubleshoo No files created REQUEST FILE	t vet TO BE CREATED	Manag Hostna NTP Cloud : Reboot Traffic	ement Interfac me Services /Shutdown Settings terino Prefere	20 DCES

2.驗證FTD是否已註冊到智慧許可伺服器,以及是否已啟用AnyConnect Plux、Apex或VPN Only許可證。

CISCO. Firepower Device Manager Monitoring Policies Ob	ects Device: FTD-3
Device Summary Smart License	
CONNECTED Last sync: 16 Apr 2020 08:27 AM SUFFICIENT LICENSE Next sync: 16 Apr 2020 08:37 AM	Go to Cloud Services 🛛 🗘 🗸
SUBSCRIPTION LICENSES INCLUDED	
Threat ENA	Malware Disabled by user
This License allows you to perform intrusion detection and prevention and file control. Y must have this license to apply intrusion policies in access rules. You also must have the license to apply file policies that control files based on file type.	ou This License allows you to perform Cisco Advanced Malware Protection (AMP) with AMP for s Firepower and AMP Threat Grid. You must have this license to apply file policies that detect and block malware in files transmitted over your network.
Includes: 🖏 Intrusion Policy	Includes: \mathbb{C}_{Θ} File Policy
URL License DISA	RLE RA VPN License Type PLUS - DISABLE
S Enabled	S Enabled
This license allows you to control web access based on URL categories and reputations than by individual URL alone. You must have this license to deploy access rules that filte traffic based on category and reputation.	, rather Please select the license type that you purchased to enable remote access VPN. Note that Firepower Device Manager closs not support any of the advanced features covered by the Apex license.
Includes: URL Reputation	Includes: RA-VPN

設定AD身份源

1.導覽至**對象>身份源**,然後按一下+符號並選擇AD,如下圖所示。

cisco. Firepower Device	Manager Monitoring Poli	Cies Objects Device: FTD-3	: 0 🕲 👌 د	admin Administrator
Object Types 🔶 ^	Identity Sources			
C Networks	1 object		Q Search	+~
\$ Ports	* NAME	THE	VALUE	RADIUS Server
8 Security Zones	1 LocalidentitySource	LOCAL		RADIUS Server Group
🐔 Application Filters				AD
Ø URLs				Identity Services Engine
Geolocations				
Syslog Servers				
& ICE Policies				
IPSec Propests				
AnyConnect Client				
E Identity Sources				
1 Users				
R Certificates				
🔒 Secret Keys				
DNS Groups				
Vert List Filters				

2.使用之前收集的資訊填充Active Directory伺服器的相應設定。如果為Microsoft伺服器使用主機名 (FQDN)而不是IP地址,請確保在**對象> DNS組**下建立適當的DNS組。然後導航到**Device > System Settings > DNS Server**,然後在**Management Interface**和**Data Interface**下應用DNS組,即可將該 DNS組應用到FTD,然後為DNS查詢指定適當的輸出介面。按一下**Test**按鈕以驗證是否成功設定以 及是否可從FTD的管理介面連線。由於這些測試是從FTD的管理介面啟動,而不是通過FTD上設定 的其中一個可路由介面(例如內部、外部、dmz)來啟動,因此成功(或失敗)的連線並不能保證 AnyConnect驗證有相同的結果,因為AnyConnect LDAP驗證要求會從FTD的一個可路由介面啟動 。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。 Add Identity Realm

Ŀ.

Identity Realm is used for Identity Policies and Remote Access VPN. Any changes impact all features that use this realm.

Name	Туре
LAB-AD	Active Directory (AD)
Directory Username	Directory Password
ftd.admin@example.com	••••••
e.g. user@example.com	
Base DN	AD Primary Domain
DC=example,DC=com	example.com
e.g. ou=user, dc=example, dc=com	e.g. example.com
Directory Server Configuration	
win2016.example.com:389	▲
Hostname / IP Address	Port
Hostname / IP Address win2016.example.com	90rt 389
Hostname / IP Address win2016.example.com e.g. ad.example.com	Port 389
Hostname / IP Address win2016.example.com e.g. ad.example.com Encryption	Port 389 Trusted CA certificate
Hostname / IP Address win2016.example.com e.g. ad.example.com Encryption NONE	Port 389 Trusted CA certificate Please select a certificate
Hostname / IP Address win2016.example.com e.g. ad.example.com Encryption NONE ✓ TEST ✓ Connection to realm is successful	Port 389 Trusted CA certificate Please select a certificate
Hostname / IP Address win2016.example.com e.g. ad.example.com Encryption NONE ✓ TEST ✓ Connection to realm is successful Add another configuration	Port 389 Trusted CA certificate Please select a certificate
Hostname / IP Address win2016.example.com e.g. ad.example.com Encryption NONE ✓ TEST ✓ Connection to realm is successful Add another configuration	Port 389 Trusted CA certificate Please select a certificate

如果使用LDAPS或STARTTLS,請選擇適當的Encryption,然後選擇Trusted CA證書。如果尚未新 增根CA,請按一下**Create New Trusted CA Certificate**。提供根CA證書的名稱,然後貼上之前收集 的PEM格式根CA證書。

Add Trusted CA Certificate

		Ŭ	
Name LDAPS_ROOT			
Paste certificate, or choose file: UPLOAD CERTIFICATE The supported formats are: PEM, DEF	È.		
BEGIN CERTIFICATE MIIDCDCCAfCgAwIBAgIQE4ZG5Z1wT6IONTjooEQyMTANBgkqhkiG9w0BAQsFADAd MRswGQYDVQQDExJleGFtcGxlLVdJTjlwMTYtQ0EwIBcNMjAwNDI3MTQ1MDU5WhgP MjA2MDA0MTkxNDUwNTIaMB0xGzAZBgNVBAMTEmV4YW1wbGUtV0IOMjAxNi1DQTCC ASIwDOX IKoZlbwcNAQERBQADooEPADCCAQoCcoeFRAI8chT719NzSQooQPb0YT67b			
	CANCEL	ОК	
Directory Server Configuration			

win2016.example.com:636		▲
Hostname / IP Address		Port
win2016.example.com		636
e.g. ad.example.com		
Encryption		Trusted CA certificate
LDAPS	~	LDAPS_ROOT
TEST ✓ Connection to realm is su	ccessful	

在此配置中,使用以下值:

- 名稱:LAB-AD
- 目錄使用者名稱: ftd.admin@example.com
- 基本DN:DC=example,DC=com
- AD主域: example.com
- 主機名/IP地址: win2016.example.com
- 連接埠:389
- 3.按一下右上**角的「**待定更改」按鈕,如下圖所示。

cisco. Firepower De	vice Manager Monitoring Policies	Dijects Device: FTD-3	admin Administrator
Object Types 🔶	Identity Sources		
C Networks	2 objects	Q Snarrh	+ ~
S Ports	H NAME	TYPE VALUE	ACTIONS
8 Security Zones	1 LocalIdentitySource	LOCAL	
🐔 Application Filters	2 LAB-AD	AD win2016.example.com	

4.按一下**Deploy Now**按鈕。

Pe	ending Changes	0 ×
I	Last Deployment Completed Successfully 01 May 2020 12:54 PM. See Deployment History	
	Deployed Version (01 May 2020 12:54 PM)	Pending Version CLEGEND Removed Added Edited
0	Active Directory Realm Added: LAB-AD	~
	- - - - - - - - -	<pre>dirPassword.masked: false dirPassword.encryptedString: *** directoryConfigurations[0].port: 389 directoryConfigurations[0].hostname: win2016.example.com directoryConfigurations[0].encryptionProtocol: NONE adPrimaryDomain: example.com dirUsername: ftd.admin@example.com baseDN: DC=example,DC=com enabled: true realmId: 9 name: LAB-AD</pre>
м	DRE ACTIONS Y	CANCEL DEPLOY NOW

配置AnyConnect進行AD身份驗證

要使用配置的AD身份源,需要將其應用到AnyConnect配置。

1.導覽至Device > Remote Access VPN,如下圖所示。

Gisco. Firepower Device Manage	Monitoring Policies Objects	Device: FTD-3	admin Administrator
	[00] [
Interfaces Connected Enabled 3 of 4 View All Interfaces	Routing 2 routes View Configuration	Updates Geolocation, Rule, VDB, System Upgrade, Security Intelligence Feeds View Configuration	System Settings Management Access Logging Settings DHCP Server DNS Server
Smart License Registered View Configuration	Backup and Restore View Configuration	Troubleshoot No files created yet REQUEST FILE TO BE CREATED	Management Interface Hostname NTP Cloud Services Reboot/Shutdown Traffic Settings URL Filtering Preferences
Site-to-Site VPN There are no connections yet View Configuration	Remote Access VPN Configured 1 connection 2 Group Policies View Configuration	Advanced Configuration Includes: FlexConfig, Smart CLI View Configuration	Device Administration Audit Events, Deployment History, Download Configuration View Configuration

2.按一下+符號或Create Connection Profile按鈕,如下圖所示。



3.在「連線和客戶端配置」部分下,選擇之前建立的AD身份源。為包括連線配置檔名稱和客戶端地 址池分配在內的其他部分設定適當的值。完成後按一下**Submit Query**。

Connection and Client Configuration

Specify how to authenticate remote users and the AnyConnect clients they can use to connect to the inside network.

Connection Profile Name This name is configured as a connection alias, it ca	n be used	to connect to the VPN gateway	
General			
Group Alias		Group URL	
General			
Add Group Alias		Add Group URL	
Primary Identity Source			
Authentication Type			
AAA Only Client Certificate Only	AAA a	nd Client Certificate	
Primary Identity Source for User Authenticat	tion	Fallback Local Identity Source 🛕	
Filter	~	Please Select Local Identity Source	~
1 LocalIdentitySource		^	
<u>北</u> LAB-AD	0		
1 Special-Identities-Realm		~	
Create new 🗠			

Client Address Pool Assignment

IPv4 Address Pool Endpoints are provided an address from this pool	IPv6 Address Pool Endpoints are provided an address from this pool
C AnyConnect-Pool]
+	
CANCEL	SUBMIT QUERY

4.在「遠端使用者體驗」部分下,選擇適當的組策略。預設情況下,將使用**DfltGrpPolicy**;但是,可 以建立另一個模板。

```
View Group Policy
```

DfltGrpPolicy

Policy Group Brief Details

DNS + BANNER	Edi
DNS Server	Nooe
Dito Server	140100
Banner Text for Authenticated Clients	Nane
CERCION RETRINCE	
SESSION SETTINGS	
Maximum Connection Time / Alert Interval	Unlimited / 1 Minutes
Idle Time / Alert Interval	30 / 1 Minutes
Simultaneous Login per User	3
SPLIT TUNNELING	
IPv4 Split Tunneling	Allow all traffic over tunnel
IPv6 Split Tunneling	Allow all traffic over tunnel
ANYCONNECT CLIENT	
AnyConnect Client Profiles	None

5.在「全域性設定」部分下,至少指定SSL證書、外部介面和AnyConnect包。如果之前未建立證書 ,可以選擇預設自簽名證書(<u>DefaultInternalCertificate</u>),但是會看到不受信任的伺服器證書消息。 應取消選中解密流量的旁路訪問控制策略(sysopt permit-vpn),以便使用者身份訪問策略規則稍後生 效。此處也可以配置NAT豁免。在此配置中,從內部介面到AnyConnect客戶端IP地址的所有ipv4流 量均來自NAT。對於更複雜的設定(例如外部到外部髮夾),需要根據NAT策略建立其他NAT規則 。AnyConnect軟體包可在思科支援站點找到: <u>https://software.cisco.com/download/home</u>。需要 有效的Plus或Apex許可證才能下載AnyConnect軟體包。

Global Settings

These settings control the basic functioning of the connection. Changes to any of these options apply to all connection profiles; you cannot configure different settings in different profiles.

Certificate of Device Identity	Outside Interface
FTD-3-Manual V	outside (GigabitEthernet0/0)
Fully-qualified Domain Name for the Outside Inter	face
ftd3.example.com	
e.g. ravpn.example.com	
Access Control for VPN Traffic Decrypted VPN traffic is subjected to access control policy policy for decrypted traffic option bypasses the access co and the authorization ACL downloaded from the AAA serv Bypass Access Control policy for decrypted to	y inspection by default. Enabling the Bypass Access Control ntrol policy, but for remote access VPN, the VPN Filter ACL er are still applied to VPN traffic traffic (sysopt permit-vpn)
NAT Exempt	
Inside Interfaces The interfaces through which remote access VPN users can connect to the Internal networks + Inside (GigabitEthemet0/1)	Inside Networks The internal networks remote access VPN users are allowed to use. The IP versions of the internal networks and address pools must match, either IPv4, IPv6, or both.
	G any-ipv4
AnyConnect Package	
If a user does not already have the right AnyConnect packs installer when the client authenticates for the first time. The	ge installed, the system will launch the AnyConnect user can then install the package from the system.
You can download AnyConnect packages from software.ck You must have the necessary AnyConnect software license	sco.com.



6.在「摘要」部分下,驗證AnyConnect是否設定正確,然後按一下**提交查詢**。

Summary

Review the summary of the Remote Access VPN configuration.

STEP 1: CONNECTION AND CLIENT CONFIGURA	non	
Primary Identity Source		
Authentication Type	AAA Only	
Primary Identity Source	北 LAB-AD	
Fallback Local Identity Source	-	
Strip Identity Source server from username	No	
Strip Group from Username	No	
Secondary Identity Source		
Secondary Identity Source for User Authenticat	on –	
Fallback Local Identity Source	-	
O Advanced		
Authorization Server		
Accounting Server		
Client Address Deal Assignment		

7.按一下右上**角的**「待決更改」按鈕,如下圖所示。

cisco. Firepower Devi	ce Manager 👼 🐨 🛱 Monitoring Policies Objects	Device: FTD-3	∑ 🗑 ? : admin Administrator
RA VPN +	Device Summary Remote Access VPN Connection Profil	es	
Connection Profiles	1 object	Q ~	+
	· NAME	***	GROUP POLICY ACTIONS
	1 General	Authentication: AAA Only Authorization: None Accounting: None	DftGrpPolicy

8.按一下**立即部署**。

Pe	ending Changes	0 X	
O I	Last Deployment Completed Successfully 16 Apr 2020 12:41 PM. See Deployment History		Clos
	Deployed Version (16 Apr 2020 12:41 PM)	Pending Version CLEGEND Removed Added Edit	ed
0	Network Object Added: AnyConnect-Pool		^
		<pre>subType: Network value: 10.10.00/24 isSystemDefined: false dnsResolution: IPV4_AND_IPV6 name: AnyConnect-Pool</pre>	
0	RA VPN Added: NGFW-Remote-Access-VPN		
		<pre>vpnGatewaySettings[0].exemptNatRule: true vpnGatewaySettings[0].outsideFqdn: ftd3.example.com vpnGatewaySettings[0].bypassAccessControlForVPNTraffic: t name: NGFW-Remote-Access-VPN</pre>	ľ
	anyconnectPackageFiles:		
	-	anyconnect-win-4.7.03052-webdeploy-k9.pkg	
	<pre>vpnGatewaySettings[0].serverCertificate: -</pre>	FTD-3-Manual	
	<pre>vpnGatewaySettings[0].outsideInterface:</pre>		
	-	outside	
	<pre>vpnGatewaySettings[0].insideInterfaces:</pre>		
	-	inside	~
	<pre>vpmacewaySettings[0].insidenetworks;</pre>		
мо	DRE ACTIONS Y	CANCEL DEPLOY NOW V	

啟用身份策略並為使用者身份配置安全策略

此時,AnyConnect使用者應該能夠成功連線,但可能無法訪問特定資源。此步驟將啟用使用者身份 ,以便只有AnyConnect管理員中的使用者才能使用RDP連線到內部資源,並且只有組 AnyConnect使用者中的使用者才能使用HTTP連線到內部資源。

1.導航到Policies > Identity, 然後點選Enable Identity Policy。



對於此配置,不需要進一步的配置,並且預設操作就足夠了。

cisco. Firepo	wer Device Manage	er Moni	itoring Policies	譜面 Objects	Device: FTD-3		D 🔒 🛛	? : Å	dmin Idministrator	×
Security Policies										
$\Box \rightarrow \bigcirc$ SSL Decryption \rightarrow \bigcirc Identity \rightarrow \bigcirc Security Intelligence \rightarrow \oslash NAT \rightarrow \bigotimes Access Control \rightarrow Intrusion										
Identity Policy Q Search									¢ _A	+
			SOURCE			DESTINATION				
H NAME	AUTHONTICATION	AUTH, TYPE	ZONES	NETWORKS	PORTS	ZONES	NETWORKS	PORTS/PROTO	ACTION	5
				There are no lo	lentity rules yet.					
				Start by creating th	he first identity rule.					
				CREATE IDE	ENTITY RULE					
Default Action	Passive Auth Am	y Identity Source	~ 0							

2.導航到**Policies > NAT**,確保正確配置NAT。如果AnyConnect設定中配置的NAT異常足夠,則無 需在此進行其他配置。

cisco. Firepow	er Device	Manager	Monitoring	Policies	詳正 Objects	Device: FTD-3		0.	0 ?	admin Admini	strator	
⊡ → O ss	Decryption	-> 🕑 Id	entity \rightarrow ()	Security Intelligen	ce 🔶 🥑 NA	T -> 📀 Acc	ess Control \rightarrow	S Intrusion				
1 rule								Q Search			+	
			OFFICINAL PACKET				TRANSLATED PAGKET					
a NAME	TYPE	INTERFACES	SOURCE AD	DESTINATIO	SOURCE PORT	DESTINATIO	SOURCE AD	DESTINATIO	SOURCE PORT	DESTINATIO	ACTIONS	
Auto NAT Rules												
> # Internet_PAT	DYNAMIC	ANY	any-ipv4	ARY	ANY	ANY	Interface	ANY	ANY	ANY		

3.定位至**策略>訪問控制**。在本節中, Default Action設定為Block ,並且未建立任何訪問規則,因 此一旦AnyConnect使用者連線,他們將無法訪問任何內容。按一下+符號或Create Access Rule新 增新規則。

CISCO. Firepower Device Manager											
$\Box \rightarrow \bigcirc$ SSL Decryption $\rightarrow \oslash$ Identity $\rightarrow \bigcirc$ Security Intelligence $\rightarrow \oslash$ NAT $\rightarrow \oslash$ Access Control $\rightarrow \circledast$ Intrusion											
						Q Search				®. +	
	SOURCE			DESTINATION							
* NAME	ACTION ZONES	NETWORKS	PORTS	ZONES	NETWORKS	PORTS/PROTO	APPLICATIONS	URLS	USERS	ACTIONS	
There are no access rules yet. Start by creating the first access rule. CREATE ACCESS RULE											
Default Action	Access Control 😑 Block	9, E, I v									

4.使用適當的值填寫欄位。在此配置中,AnyConnect Admins組內的使用者應該對內部網路中的 Windows Server具有RDP訪問許可權。對於源,區域配置為outside_zone,這是AnyConnect使用 者將要連線的外部介面,網路配置為AnyConnect-Pool對象,該對象之前配置為將IP地址分配給 AnyConnect客戶端。對於FDM中的使用者身份,源必須是使用者將從中啟動連線的區域和網路。 對於目標,區域配置為inside_zone(即Windows Server所在的內部介面),網路配置為 Inside_Net對象(即定義Windows Server所在子網的對象),埠/協定設定為兩個自定義埠對象,以 允許通過TCP 3389和UDP 3389進行RDP訪問。

Edit Access Rule		0 ×
Order Title 1 ✓ AC RDP Access Source/Destination Applications URLs	Action Allow ars Intrusion Policy File policy Logging	
SOURCE Zones Networks AnyConnect-Pool	DESTINATION Ports Cones ANY Inside_zone	Networks Ports/Protocols Networks Ports/Protocols Ports/Protocols Ports/Ports/Protocols Ports/Por

Show Diagram	Not hit yet	CANCEL	ок

在Users部分下,將新增組AnyConnect Admins,以便允許此組以外的使用者對Windows Server進 行RDP訪問。按一下+符號,按一下「組」(Groups)頁籤,按一下相應的組,然後按一下**「確定」** (**OK)**。請注意,也可以選擇單個使用者和身份源。

Add Access Rule	0 ×
Order Title 1 AC RDP Access Source/Destination Applications URLs Users Inte	Action Allow Image: Allow Allow rusion Policy File policy Logging
AVAILABLE USERS	CONTROLLING ACCESS FOR USERS AND USER GROUPS If you configure identity policies to establish user identity based on source IP address, you can control access based on user identity, you can apply the appropriate access controls whether the user changes workstations or obtains a different address through DHCP. If you base rules on group membership, user network access changes as users change roles in your organization, moving from one group to another.
Show Diagram	CANCEL

選擇適當的選項後,按一下**確定**。

Add Access Rule	• ×
Order Title 1 V AC RDP Access	Action Action Allow
Source/Destination Applications URLs U	ers Intrusion Policy ⁹ File policy ⁹ Logging
AVAILABLE USERS	CONTROLLING ACCESS FOR USERS AND USER GROUPS If you configure identity policies to establish user identity based on source IP address, you can control access based on user name or user group membership. By controlling access based on user identity, you can apply the appropriate access controls whether the user changes workstations or obtains a different address through DHCP. If you base rules on group membership, user network access changes as users change roles in your organization, moving from one group to another.

Show Diagram	CANCEL	ок	

5.根據需要建立更多訪問規則。在此配置中,將建立另一個訪問規則,以允許AnyConnect使用者組 中的使用者通過HTTP訪問Windows Server。

Edit Access	Rul	e										×
Order Title 2 AC HI Source/Destination	TTP A	occess	Use	rs Intrus	Action Allow	File policy ⁹ Log	ging					
SOURCE Zones	+	Networks	+	Ports	+	DESTINATION Zones	+	Networks	+	Ports/Protocols		+
outside_zone		AnyConnect-Pool		ANY		inside_zone		Inside_Net		ЧТТΗ € ²		
Show Diagram	\supset	e Not hit yet							CA	INCEL	ОК	

Edit Access Rule	@ >	<
Order Title	Action	
2 Y AC HTTP Access	Allow Y	
Source/Destination Applications URLs Users	Intrusion Policy ⁹ File policy ⁹ Logging	
AVAILABLE USERS	+ the controlling access for users and user groups	
LAB-AD \ AnyConnect Users	If you configure identity policies to establish user identity based on source IP address, you can control access based on user name or user group	

from one group to another.

appropriate access controls whether the user changes workstations or obtains a different address through DHCP. If you base rules on group membership, user network access changes as users change roles in your organization, moving

Show Diagram
CANCEL
OK
CANCEL
OK

6.驗證訪問規則配置,然後按一下右上角的Pending Changes按鈕,如下圖所示。

cisco. Firepowe	r Devic	e Manager	Monitoring	Policies	i≑E Objects D	evice: FTD-3		0	0 ?) : (;	idmin Idministrat	or
Ø Security Policies												
$\square \rightarrow \bigcirc$ SSL Decryption $\rightarrow \oslash$ Identity $\rightarrow \bigcirc$ Security Intelligence $\rightarrow \oslash$ NAT $\rightarrow \bigtriangledown$ Access Control $\rightarrow $ \heartsuit Intrusion												
2 rules						Q Search				0	+	
		SOURCE			DESTINATION							
# NAME	ACTION	ZONES	NETWORKS	PORTS	ZONES	NETWORKS	PORTS/PROTO_	APPLICATIONS	UNLS	USERS		ACTIONS
> 1 AC RDP Access	→ Allow	outside_zone	AnyConnect-Pool	ANY	inside_zone	Inside_Net	RDP-TCP RDP-UDP	ANY	ANY	AnyConne	Ф.С.	
> 2 AC HTTP Access	Allow	outside_zone	AnyConnect-Pool	ANY	inside_zone	Inside_Net	HTTP	ANY	ANY	AnyConne	ф.С ₄	
Default Action Acco	Default Action Access Control 😑 Block 🖏 📴 🗸											

7.驗證更改,然後按一下Deploy Now。

```
MORE ACTIONS Y
```

C LEGEND Removed Added Edited Deployed Version (28 Apr 2020 01:35 PM) Pending Version Access Rule Added: AC HTTP Access users[0].name: AnyConnect Users _ logFiles: false eventLogAction: LOG_NONE ruleId: 268435467 name: AC HTTP Access sourceZones: outside_zone destinationZones: inside_zone sourceNetworks: _ AnyConnect-Pool destinationNetworks: Inside_Net _ destinationPorts: _ HTTP users[0].identitySource: LAB-AD Access Rule Added: AC RDP Access CANCEL DEPLOY NOW

AAA組態

最終配置

使用本節內容,確認您的組態是否正常運作。

驗證

> show running-config webvpn webvpn enable outside http-headers hsts-server enable max-age 31536000 include-sub-domains

配置AnyConnect

no preload

show running-configuration aaa-server aaa-server LAB-AD protocol ldap realm-id 7 aaa-server LAB-AD host win2016.example.com serverport 389 ldap-base-dn DC=example, DC=com ldap-scope subtree ldap-login-password ***** ldap-logindn ftd.admin@example.com server-type auto-detect

Pending Changes

Last Deployment Completed Successfully 28 Apr 2020 01:35 PM. See Deployment History

```
hsts-client
  enable
 x-content-type-options
 x-xss-protection
 content-security-policy
 anyconnect image disk0:/anyconnpkgs/anyconnect-linux64-4.7.03052-webdeploy-k9.pkg 1
 anyconnect image disk0:/anyconnpkgs/anyconnect-win-4.7.03052-webdeploy-k9.pkg 2
anyconnect enable
tunnel-group-list enable
cache
 disable
error-recovery disable
> 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-tunnel-protocol ssl-client
split-tunnel-policy tunnelspecified
split-tunnel-network-list value DfltGrpPolicy|splitAcl
webvpn
 anyconnect ssl dtls none
> show running-config ssl
```

ssl trust-point FTD-3-Manual outside 使用AnyConnect連線並驗證訪問控制策略規則

🚳 Cisco AnyC	onnect Secure N	lobility Cli	ent -	-	×	
	VPN: Contacting ftd3.	example.co	om.			
_	ftd3.example.c	om	~	Connect		
	_	🕙 Cisc	o AnyConne	ct ftd3.exam	ple.com	×
\$ (i)						
			Group:	General		~
			Username:	it.admin		
			Password:	******		
					ОК	Cancel



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。



如果以組中的AnyConnect使用者(該使用者具有HTTP訪問許可權但沒有RDP訪問許可權)中的測 試使用者登入,則可以驗證訪問控制策略規則是否生效。



疑難排解

使用本節內容,確認您的組態是否正常運作。

調試

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

為了排查使用者身份訪問控制策略問題,可以秘密運行system support firewall-engine-debug,以 確定流量被允許或意外阻止的原因。

工作LDAP調試

```
[53] Session Start
[53] New request Session, context 0x00002b1d13f4bbf0, 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]
              = [SUBTREE]
        Scope
[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
[53]
      objectClass: value = person
      objectClass: value = organizationalPerson
[53]
[53]
      objectClass: value = user
[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]
[53]
      instanceType: value = 4
[53]
      whenCreated: value = 20200421025811.0Z
      whenChanged: value = 20200421204622.0Z
[53]
[53]
      displayName: value = IT Admin
       uSNCreated: value = 25896
[53]
       memberOf: value = CN=AnyConnect Admins, CN=Users, DC=example, DC=com
[53]
      uSNChanged: value = 26119
[53]
      name: value = IT Admin
[53]
[53]
      objectGUID: value = &...J..O..2w...c
      userAccountControl: value = 512
[53]
      badPwdCount: value = 6
[53]
[53]
      codePage: value = 0
[53]
       countryCode: value = 0
[53]
       badPasswordTime: value = 132320354378176394
[53]
      lastLogoff: value = 0
[53]
      lastLogon: value = 0
      pwdLastSet: value = 132319114917186142
[53]
      primaryGroupID: value = 513
[53]
[53]
      objectSid: value = .....{I...;....j...
       accountExpires: value = 9223372036854775807
[53]
      logonCount: value = 0
[53]
      sAMAccountName: value = it.admin
[53]
[53]
      sAMAccountType: value = 805306368
[53]
      userPrincipalName: value = it.admin@example.com
[53]
       objectCategory: value = CN=Person, CN=Schema, CN=Configuration, DC=example, DC=com
       dSCorePropagationData: value = 16010101000000.0Z
[53]
[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

潜在解決方案:

• 檢查路由並確保FTD收到來自LDAP伺服器的回應。

- 如果使用LDAPS或STARTTLS,請確保信任正確的根CA證書,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,請驗證DNS是否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:確認登入DN和登入密碼是否正確設定。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,請瀏覽以下步驟:

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.按一下**連線>連線……**如下圖所示。

🔝 Ldp					_		×
Connection Browse	View Op	otions	Utilities	Help			
Connect	C1 1 0						
Disconnect	Ctrl+B						
New	Ctrl+N						
Save							
Save As							
Exit							
						NUM	

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	
<u>P</u> ort:	389	Connectionless
<u>0</u> K		<u>C</u> ancel

4. 「右」列顯示表示連線成功的文本。按一下Connection > Bind... 如下圖所示。



5.選擇Simple Bind,然後指定目錄帳戶使用者名稱和密碼。按一下「OK」(確定)。

Bind	×
<u>U</u> ser:	ftd.admin@example.com
Password:	•••••
Domain:	
Bind type Bind as <u>c</u> ur Bind with c Simple bind Advanced	rrently logged on user redentials (DIGEST) affic after bind Cancel OK

成功繫結後,ldp將顯示驗證為DOMAIN\username。

🟠 Idap://w	in2016.exa	mple.co	=com		—		×					
Connection	Browse	View	Options	Utilities	Help							
				<pre>DC=example,DC=com</pre>								
			< < A	unavailable	ed as: 'EXA	MPLE\ftd.ad	min'.		,			
			-						_	¥		
, Ready												

如果嘗試使用無效的使用者名稱或密碼進行繫結,將會導致類似這樣的失敗。

🔝 Idap://w	in2016.exa	mple.co	om/DC=ex	=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 server error comment: Ac rror 0x8009 tvalid	ResultSets ResultSets ValRange; eadMemory edLDAPVer edSASLMed EGO; EXTE imple_bind_ e>); // v.3 ed as: 'EXAl imple_bind_ e>); // v.3 idap_simple cceptSecur 90308 The f	ize; MinRes PerConn; Ma MaxValRan Limit; Syster sion (2): 3; chanisms (4 RNAL; DIGE _s(Id, 'ftd.ad MPLE\ftd.ad _s(Id, 'wron _bind_s() fa : LdapErr: D ityContext e token suppli	ultSets; axNotificat geTransitiv mMemoryL 2;): GSSAPI :ST-MD5; Imin@exar min'. g@examp ailed: Invali)SID-0C09 error, data ed to the f	tionPerConn ve; .imitPercent l; GSS- mple.com', le.com', id Credentia 042A, 52e, v3839 function is	i; ;
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:確認AD可以通過FTD完成的搜尋找到使用者。這也可以使用ldp.exe來完成。
```

1.成功繫結後,導航到檢視>樹,如下圖所示。

Idap://win2016.example.com/DC=example,DC=com								—		×	<	
Connection	Browse	View	v Options	Utilities	Help							
			Tree			Ctrl+T					^	
			Enterprise	Configurat	ion		A	/axPoolThreads;				
		~	Status Bar				:5	 sts; MaxDatagramRecv; vTimeout; 				
			Set Font				n s	ildleTime; : MaxQue	MaxPage ervDuratio	Size;		
				MaxDirSyncDuration; MaxTempTableSize; MaxResultSetSize; MinResultSets; MaxResultSetsPerConn; MaxNotificationPerConn; MaxValRange; MaxValRangeTransitive; ThreadMemoryLimit; SystemMemoryLimitPercent; supportedLDAPVersion (2): 3; 2; supportedSASLMechanisms (4): GSSAPI; GSS- SPNEGO; EXTERNAL; DIGEST-MD5;						onn; ent;		
				res = Idap_s <unavailable Authenticate</unavailable 	imple_bi ⊳); // v.3 ed as: 'E)	ind_s(ld, 'fto } XAMPLE\ftd	d.ad I.adı	imin@exa min'.	imple.com	ť,	l	
											~	

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「搜尋」,如下圖所示。

🔝 Idap://wi	n2016.exa	- 🗆 ×	(
Connection	Browse	View	Options	Utilities	Help		
<mark>⊕</mark> . <mark>DC= exam</mark>	ple,DC=c	om	Search Virtual L Delete Modify Modify Add chil Compar Advance	ist View DN Id e	Ctrl+S Ctrl+D Ctrl+M Ctrl+R Ctrl+A	cipals,DC=example,DC=com; 11D2B9AA00C04F79F805:CN =example,DC=com; 11D297C400C04FD8D5CD:C =example,DC=com; 11D1ADED00C04FD8D5CD:C =example,DC=com; 11D1ADED00C04FD8D5CD:C ble,DC=com; 11D1AA4B00C04FD7D83A:O s,DC=example,DC=com; 11D1ADED00C04FD8D5CD:C ample,DC=com;	^
			Copy Copy Select al Clear ou	N I Itput	Ctrl+C Ctrl+N	311D1ADED00C04FD8D5CD:C e,DC=com; 0 3:43:59 PM Eastern Daylight 2:41:57 PM Eastern Daylight	*
Create a new d	locument						

4.指定與debug中相同的基本DB、篩選器和範圍值。在此範例中,這些如下:

- 基本DN:dc=example,dc=com
- Filter: (篩選條件:)samaccountname=it.admi
- 範圍:子樹

🟠 Idap://w	n2016.example.com/DC=example,DC=com	– 🗆 ×
Connection	Browse View Options Utilities Help	
Search	×	C=example,DC=com; S8811D1ADED00C04FD8D5CD:C DC=example DC=com;
Base DN:	DC=example,DC=com ~	58811D1ADED00C04FD8D5CD:C
Filter:	sAMAccountName=it.admi ~	ample,DC=com; D211D1AA4B00C04FD7D83A:O
Scope O Base	One Level Subtree	lers,DC=example,DC=com; 58811D1ADED00C04FD8D5CD:C example,DC=com;
Attributes:	objectClass;name;description;canonicalName \sim	68811D1ADED00C04FD8D5CD:C nple,DC=com;
Options	Run Close	2020 3:43:59 PM Eastern Daylight
	***Searching Idap_search_s(Id, "DC= "sAMAccountName=it.a Getting 0 entries:	example,DC=com", 2, idmi", attrList, 0, &msg)
Ready		

由於Base DN dc=example,dc=com下沒有具有**samaccountname=it.admi**的使用者帳戶,LDP會找 到0個條目。

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

🔝 Idap://wi	n2016.example.com	n/DC=exa	mple,DC:	=com		>	<
Connection	Browse View O	Options	Utilities	Help			
Search					×	58811D1ADED00C04FD8D5CD:C DC=example,DC=com; 58811D1ADED00C04FD8D5CD:C	^
Base <u>D</u> N:	DC=example,DC=cc	om			\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;d	escription;	canonicalN	lame	\sim	020 3:43:59 PM Eastern Dayligh	t
Options		<u>R</u> un		<u>C</u> lose)20 2:41:57 PM Eastern Daylight	
		*** Ida "s. Ge Dr	Searching ap_search AMAccour etting 1 ent CN=IT A canonica name: IT objectCla user	 _s(ld, "I ntName: ries: .d min,(alName: Admin; ass (4): ;	DC=e =it.ad CN=U exar top;	example,DC=com", 2, Imin", attrList, 0, &msg) Jsers,DC=example,DC=com mple.com/Users/IT Admin; person; organizationalPerson;	
Ready							

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:驗證使用者的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 對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 檢視器日誌的潛在原因。

測試AAA

test aaa-server命令可用於使用特定使用者名稱和密碼模擬來自FTD的驗證嘗試。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。

以下是顯示雙向LDAP流量的捕獲:

> 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 1dap > 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 1: 23:02:16.770712 192.168.1.17.61960 > 192.168.1.1.389: S 3681912834:3681912834(0) win 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> 3: 23:02:16.772039 192.168.1.17.61960 > 192.168.1.1.389: . ack 491521507 win 32768 <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> 192.168.1.17.61960 > 192.168.1.1.389: . ack 491522163 win 32768 9: 23:02:16.775075 <nop,nop,timestamp 1061373061 762393887> [...] 54 packets shown

Windows Server事件檢視器日誌

AD伺服器Van上的事件檢視器日誌提供了更多有關失敗原因的詳細資訊。

1.搜尋並開啟事件**檢視器**。

=	Best match					
ŵ	Event Viewer Desktop app					
	Settings >					
	Here we we we we we we way to be well as the second					
æ		P		E.	~	la.
89	ы 89	Ц	Ц		L4	41
	event					
-	D D	e	-	-	1	8

2.展開**Windows Logs**,然後按一下**Security**。使用使用者的Account Name搜尋**Audit Failure**,然後 檢視Failure Information,如下圖所示。



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