在由FDM管理的FTD上为AnyConnect客户端配置 AD(LDAP)身份验证和用户身份

目录

简介 <u>先决条件</u> 要求 使用的组件 配置 网络图和场景 AD配置 确定LDAP基础DN 创建FTD帐户 创建AD组并将用户添加到AD组(可选) 复制LDAPS SSL证书根(仅LDAPS或STARTTLS需要) FDM配置 验证许可 设置AD身份源 配置AnyConnect以进行AD身份验证 启用身份策略并配置用户身份的安全策略 验证 最终配置 使用AnyConnect连接并验证访问控制策略规则 故障排除 调试 工作LDAP调试 无法与LDAP服务器建立连接 绑定登录DN和/或密码不正确 LDAP服务器找不到用户名 用户名的密码不正确 测试AAA 数据包捕获 Windows Server事件查看器日志

简介

本文档旨在详细说明如何为连接到由Firepower设备管理(FDM)管理的Cisco Firepower威胁防御 (FTD)的AnyConnect客户端配置Active Directory(AD)身份验证。 用户身份将用于访问策略,以便将 AnyConnect用户限制为特定IP地址和端口。

先决条件

要求

Cisco 建议您了解以下主题:

- FDM上RA VPN配置的基本知识
- FDM上LDAP服务器配置的基本知识
- AD的基本知识

使用的组件

本文档中的信息基于以下软件和硬件版本:

- Microsoft 2016服务器
- •运行6.5.0的FTDv

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原 始(默认)配置。如果您的网络处于活动状态,请确保您了解所有命令的潜在影响。

配置

网络图和场景



```
FTD
```

Windows服务器预配置了Internet信息服务(IIS)和远程桌面协议(RDP),以测试用户身份。在本配置 指南中,将创建三个用户帐户和两个组。

用户帐户:

- •FTD管理员:此帐户将用作目录帐户,以允许FTD绑定到AD服务器。
- IT管理员:用于演示用户身份的测试管理员帐户。
- •测试用户:用于演示用户身份的测试用户帐户。

组:

- AnyConnect管理员:IT管理员将添加到的测试组,用于演示用户身份。此组将只有对Windows Server的RDP访问权限
- AnyConnect用户:将添加测试用户的测试组以演示用户身份。此组将只有对Windows Server的HTTP访问权限

AD配置

为了在FTD上正确配置AD身份验证和用户身份,需要一些值。在FDM上完成配置之前,必须在 Microsoft服务器上创建或收集所有这些详细信息。主要值为:

- 域名:这是服务器的域名。在本配置指南中, example.com是域名。
- 服务器IP/FQDN地址:用于访问Microsoft服务器的IP地址或FQDN。如果使用FQDN,则必须 在FDM和FTD中配置DNS服务器以解析FQDN。在本配置指南中,这些值是 win2016.example.com,它解析为192.168.1.1。
- 服务器端口:LDAP服务使用的端口。默认情况下,LDAP和STARTTLS将TCP端口389用于 LDAP,而LDAPS(LDAPS)将使用TCP端口636。
- 根 CA:如果使用LDAPS或STARTTLS,则需要用于对LDAPS使用的SSL证书进行签名的根CA。
- 目录用户名和密码:这是FDM和FTD用于绑定到LDAP服务器并验证用户和搜索用户和组的帐户。将为此创建名为FTD Admin的帐户。
- •基本可分辨名称(DN):基本DN是FDM的起点,FTD将告知Active Directory在搜索用户时开始。 在本配置指南中,根域example.com将用作基本DN;但是,对于生产环境,在LDAP层次结构中 进一步使用基础DN可能会更好。例如,以此LDAP层次结构为例:



如果管理员希望营销组织单位内的用户能够对基本DN进行身份验证,则可以将其设置为根 (example.com),但这也允许财务组织单位下的用户1也登录,因为用户搜索将从根开始,并向下转 到财务、营销和研究部门。

基本DN设置为example.com。



为了仅限市场营销组织单位及以下用户登录,管理员可以将基本DN设置为市场营销。现在,只有 User2和User3能够进行身份验证,因为搜索将从营销部开始。

基本DN设置为"营销":



请注意,要在FTD内进行更精细的控制,允许用户根据其AD属性连接或分配不同的授权,需要配置 LDAP授权映射。

此简化的LDAP层次结构在本配置指南中使用,根example.com的DN将用于基本DN。



确定LDAP基础DN

1.打开AD用户和计算机。

=	Best match					
ŵ	Active Directory Users and Computers Desktop app					
	Settings					>
	Edit local	users a	and gro	ups		
	陀 Change U	lser Aco	count C	ontrol	setting	s
	🚨 User Acco	ounts				
	🗵 Select use	ers who	can us	e remo	te desl	ctop
۲	b	۵			₿	切
	users					
	ρœ	e	-	-	6	*

2.左键单击根域(以打开容器),右键单击根域,然后导航到"查看"并单**击"**高级**功能"**。



3.这将启用AD对象下其他属性的视图。例如,要查找根example.com的DN,请右键单击 example.com,然**后导航**到"属**性"**。



4.在"属性"下,单击"属性编辑器"选项卡。在"属性"下查找distinguishedName,然后单击"查看"。

example.com Properties		?	×
General Managed By Ot	bject Security Attribute Editor		
Attributes:			
Attribute	Value		^
dc	example		
defaultLocalPolicyObj	<not set=""></not>		
description	<not set=""></not>		
desktop Profile	<not set=""></not>		
displayName	<not set=""></not>		
displayNamePrintable	(not set)		
distinguishedName	DC-example.DC-com		
domainPolicyObject	<not set=""></not>		
domainReplica	<not set=""></not>		
dSASignature	{ V1: Flags = 0x0; LatencySecs =	0; DsaGuio	
dSCorePropagationD	0x0 = ()		
eFSPolicy	<not set=""></not>		
extensionName	<not set=""></not>		
flags	<not set=""></not>		~
<		>	_
View		Filter	
ОК	Cancel Apply	Hel	p

```
5.这将打开一个新窗口,在该窗口中,DN可以复制并粘贴到FDM中。在本例中,根DN为
```

DC=example, DC=com。复制值。单击**OK**以退出"字符串属性编辑器"窗口,然后再次单击**OK**以退 出"属性"。

String Attribute Editor ×	
Attribute: distinguishedName Value:	
DC-example,DC-com Clear OK Cancel	Undo Cut
	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	
cn <not set=""> controlAccessRights <not set=""> creationTime 4/29/2020 2:43:49 PM Eastern Daylight Tim dc example defaultLocalPolicyObj <not set=""> description <not set=""> desktopProfile <not set=""> displayName <not set=""> displayNamePrintable <not set=""></not></not></not></not></not></not></not>	
distinguishedName DC=example,DC=com domainPolicyObject <not set=""> domainReplica <not set=""> dSASignature { V1: Rags = 0x0; LatencySecs = 0; DsaGuic dSCorePropagationD 0x0 = () <</not></not>	
OK Cancel Apply Help	

这可以针对AD中的多个对象执行。例如,以下步骤用于查找用户容器的DN:



6.可以删除"高级功能"视图。右键单击根DN,导航至"View(查看)"**,然**后再次**单击"Advanced** Features(高级功能)"。



创建FTD帐户

此用户帐户将允许FDM和FTD与AD绑定,以搜索用户和组并对其进行身份验证。创建单独的FTD帐 户的目的是防止在用于绑定的凭证受到侵害时未经授权访问网络中的其他位置。此帐户不必在基本 DN的范围内。

1.在Active Directory**用户和计算机**中,右键单击将添加FTD帐户的容器/组织。在此配置中,FTD帐 户将添加到用户名ftd.admin@example.com下的"用户"(Users)容**器下**。右键单击"**用户"**,然后单击 "**新建">"用户**"。

Active Directory Users and Computers	-	х
File Action View Help		
수 수) 🚈 😿 📋 🗙 🗒 @ 🖻 📓 🖬 🗏 🐄 🖄 🦅 💆 🗞		
Active Directory Users and Com Name Type Description Saved Queries Security Group A user account manage Builtin Denied ROD Security Group Members in this group c Domain Controllers Domain Controllers Security Group DNS Administrators Gro Managed Service Accoul Domain Co Security Group Designated administrato Managed Service Accoul Delegate Control Security Group All domain controllers i Members in this group c Designated administrato Security Group DNS Administrato Domain Co Security Group All workstations and ser Security Group All domain controllers i Managed Service Accoul n Security Group All domain users New Computer Contact Group InterOrgPerson Refresh Export List msDS-ResourcePropertyList msDS-ResourcePropertyList msDS-ShadowPrincipalContainer Help Help msImaging-PSPs Security Group Security Group Security Group		
MSMQ Queue Alias MSMQ Queue Alias Printer WseAllow WseAllow Shared Folder		~

2.浏览"新建对**象 — 用户向**导"。

lew Object - User		×
🧏 Create in:	example.com/Users	
Erst name:	FTD Initials:	
Last name:	Admin	
Full name:	FTD Admin	
User logon name:		
ftd.admin	@example.com ~	
User logon name (pre	- <u>Windows 2000</u>):	
EXAMPLE\	ftd.admin	
	< Back Next > Cancel	

New Object - User		×
🤱 Create in: exam	iple.com/Users	
Password:	•••••	
User must change password	ord at next logon	
Password never expires	word	
Account is disabled		
	< Back Next >	Cancel
New Object - User		×
New Object - User	nple.com/Users	×
New Object - User	iple.com/Users llowing object will be created:	×
New Object - User Create in: exam When you click Finish, the fo Full name: FTD Admin	iple.com/Users llowing object will be created:	×
New Object - User Create in: exam When you click Finish, the fo Full name: FTD Admin User logon name: ftd.admin@	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.确认已创建FTD帐户。此外,还创建了另外两个帐户,即IT管理员和测试用户。

Active Directory Users and Com	Active Directory Users and Computers					×
File Action View Help						
🗢 🔿 🖄 📆 🖌 🗎 🛠	🗉 🗟 📑 🚺 🖬	1 🗏 🐮 🕅 🦷	1 🔟 🗽			
 Active Directory Users and Com Saved Queries Saved Queries Builtin Computers Domain Controllers ForeignSecurityPrincipale Managed Service Account Users 	Name DefaultAcco DefaultAcco DefaultAcco Donain ROD DosUpdateP Domain Ad Domain Co Domain Co Domain Co Domain Gue Domain Gue Domain Gue Domain Gue Domain Gue Domain Gue Domain Gue Domain Gue Domain Gue Comain Co Comain Co Domain Co Comain C	Type User Security Group Security Group 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 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			^
	Read-only D	Security Group	Members of this group			
< >	Test User	User				÷

创建AD组并将用户添加到AD组(可选)

虽然身份验证不需要,但可以使用组来简化对多个用户应用访问策略以及LDAP授权的操作。在本 配置指南中,组将用于稍后通过FDM中的用户身份应用访问控制策略设置。

1.在Active Directory**用户和计算机**中,右键单击要添加新组的容器/组织。在本示例中,组 AnyConnect Admins将添加到"用户"容器下。右键单击"**用户"**,然后单击"**新建">"组"**。

Active Directory Users and Con	puters			-	х
File Action View Help					
🗢 🔿 🙍 🚾 🔏 🗈 🗙 🛛	🗉 🖬 📑 🖬	1 🗏 🐮 🛯	r 🗾 🍇		
Active Directory Users and Com Saved Queries Saved Queries Save	Name DefaultAcco Denied ROD DnsAdmins DnsUpdateP Domain Ad Domain Co ntrol 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 users		~
All Tasks View Refresh Export List Properties Help	> > A Read-only A Schema A	Computer Contact Group InetOrgPerson msDS-KeyCreder msDS-ResourceF msDS-ShadowPr msImaging-PSPs MSMQ Queue Al Printer User	itial ropertyList incipalContainer ias		
Creates a new item in this container.	(m	Shared Folder			v

2.浏览"新建对**象 — 组向导"**,如图所示。

lew Object - Group	>
🥵 Create in: exam	nple.com/Users
Group name:	
AnyConnect Admins	
Group name (ore-Windows 2	200)+
AnyConnect Admins	
Group scope	Group type
O Domain local	Security
Global	ODistribution
OUniversal	
	OK Cancel

3.检验组是否已创建。还**创建**了AnyConnect用户组。

Active Directory Users and Com	Active Directory Users and Computers				×
File Action View Help					
🗢 🔿 🙇 📰 🐇 🗶 🔛 🛙	a 🛛 🖬 🕲 🕹 🛍	🔻 🗾 🙇			
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 DefaultAccount DonsAdmins DosUpdateProxy DosUpdateProxy Domain Admins Domain Computers Domain Computers Domain Controllers Domain Guests Domain Guests Domain Users Enterprise Admins Enterprise Key Admins Enterprise Read-only FTD Admin Gouest Cuest Cuest 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		
· · · · · · · · · · · · · · · · · · ·	(m				v

4.右键单击要添加用户的组,然后选择"属**性"**。在此配置中,用户I**T管理员**将添加到组AnyConnect Admins,并且用户**测试用户**将添加到组AnyConnect Users中。

Active Directory Users and Comp	outers			-	х
File Action View Help					
🗢 🔿 🖄 📅 🔏 🗎 🗙 🛙	3 @ 🔒 🛛 🖬 🔧	ዾ 🛍 🔻 🗾 🎕	8		
Active Directory Users and Com > Saved Queries	Name	Type Security Group	Description		^
 Saved Queries example.com Builtin Computers Domain Controllers ForeignSecurityPrincipal: Managed Service Accour Users 	AnyConnect Admins AnyConnect Users Calo Cert Publishers Coneable Domain C DefaultAccount DefaultAccount Denied RODC Passw DonsUpdateProxy Domain Admins Domain Computers Domain Computers Domain Controllers Domain Guests Domain Guests Domain Guests Enterprise Admins Enterprise Read-only FTD Admin Group Policy Creator	Security Group User Security Group Security Group User Security Group Security Group	Add to a group Buil Move Mer Send Mail Mer All Tasks A u: Cut DNS Delete DNS Rename Des All All Tasks Properties All Help All communications Designated administrato Members of this group Members in this group c	>	
	🗞 Guest 🛃 IT Admin	User User	Built-in account for gue		
< >>	Key Admins	Security Group	Members of this group		 v

5.单击"成员**"选**项卡,然后单击**"添**加",如图所示。

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

在字段中输入用户,然后单击"Check Names(检查名称)"按钮以验证是否找到该用户。验证后,单击OK。

Select Users, Contacts, Computers, Service Accounts, or	Groups 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 (examples):	
IT Admin (it admin@example.com)	gheck Names
Advanced	OK Cancel

验证是否添加了正确的用户,然后单击"确定**"按**钮。用户测试用户也会使用相同的步骤添加到 AnyConnect用户组。

AnyConnect Admin	ns Properties		?	×
General Members	Member Of	Managed By		
Members:				_
Name	Active Dir example.c	rectory Domain Services Fold	er	
Add	Remove	OK Cancel	A	ply

复制LDAPS SSL证书根(仅LDAPS或STARTTLS需要)

1.按Win+R键并键入mmc.exe。Click OK.

1000	C
1.00	Kum
_	evul i

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.导航至"**文件">"添加/删除管理单元……"** 如图所示.

File Action View Favorites Window Help	- 8 ×
A New Ctrl+N	
Open Ctrl+O Actions	
Save Ctrl+S There are no items to show in this view. Console Root	-
Save As More Actions	×
Add/Remove Snap-in Ctrl+M	
Options	
1 dnsmgmt	
2 dsa	
Exit	

3.在可用管理单元下,单击"证**书"**,然后单击"**添加"**。

Add or Remove Snap-ins				×
You can select snap-ins for t extensible snap-ins, you car	this console from th a configure which e	nose 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	~	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.选择"计**算机帐**户",然后单击**"下**一步",如图所示。

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

单击 **完成**。

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: 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.单击"确**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 Microsoft Cor			Certificates (Local Computer)				
Active Directory Use	Microsoft Cor Microsoft Cor			Move <u>U</u> o				
ADSI Edit	Microsoft Cor Microsoft Cor		Add >	Move <u>D</u> own				
Certificate Templates	Microsoft Cor Microsoft Cor		handling					
Certification Authority	Microsoft Cor Microsoft Cor							
Computer Managem	Microsoft Cor Microsoft Cor							
Disk Management	Microsoft and	~		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				

6.展开"个人"**文件夹**,然后单击"证**书"**。LDAPS使用的证书应颁发给Windows服务器的完全限定域名 (FQDN)。在此服务器上,列出了3个证书。

[•]颁发给WIN2016-CA的CA证书和由WIN2016-CA颁发的CA证书。

- 由example-WIN2016-CA颁发给WIN2016的身份证书。
- 由example-WIN2016-CA颁发给win2016.example.com的身份证书。

在本配置指南中,FQDN为win2016.example.com,因此前2个证书无效,无法用作LDAPS SSL证 书。颁发给win2016.example.com的身份证书是Windows Server CA服务自动颁发的证书。双击证 书以检查详细信息。

	Console1 - [Console Root\Certific	ates (Local Computer)\Personal\Certif	licates]			-	\Box \times
-	File Action View Favorites	Window Help					- 8 ×
٠	👄 🖄 🚾 📋 🙆 📦						
	Console Root	Issued To	Issued By	Expiration Da	Actions		
~	Certificates (Local Computer)	🕼 example-WIN2016-CA	example-WIN2016-CA	4/19/2060	Certificates		
	Personal Certificates	2 WIN2016	example-WIN2016-CA	4/27/2025	More Actions		+
	> Trusted Root Certification .	win2016.example.com	example-WIN2016-CA	4/28/2021			
	> 📔 Enterprise Trust						
	> intermediate Certification.						
	> Trusted Publishers						
	> Untrusted Certificates						
	> Third-Party Root Certificat						
	> Trusted People						
	Client Authentication Issue						
	> Preview Build Koots						
	Secolar Nonkemovable Cert Remote Deskton						
	Certificate Enrollment Ren						
	Smart Card Trusted Roots						
	> Trusted Devices						
	> 🎬 Web Hosting						
	> 📫 Windows Live ID Token Iss						
<	>	<		>			
Per	sonal store contains 3 certificates.						

7.要用作LDAPS SSL证书,证书必须满足以下要求:

• 公用名或DNS使用者备用名与Windows Server的FQDN匹配。

• 证书在Enhanced Key Usage字段下具有Server Authentication。

在证书的Details选项卡下,在**Subject和Subject Alternative Name**下,FQDN **win2016.example.com**出现。

🙀 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 Ent	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	y Usage umbprint	algorithm	Digital Signature, Key Encipher sha1 ca 8e 11 3d eb bc 0f 6e 4a 00	*
Other I DS (18 DNS No	Name: Object Gu ame=win2	id=04 10 90 99 a9 016.example.com	a2 38 24 65 47 84 74 64 26 cd c6 8	0
		Ed	It Properties Copy to File	
			0	ĸ

在"增**强的密钥使**用"下**,出现"服**务器身份验证"。

🙀 Certi	ficate			×
General	Details	Certification Path		
Show:	<al></al>		\sim	
Field			Value	^
E Su E Pu Pu	bject blic key blic key pa	arameters	win2016.example.com RSA (2048 Bits) 05 00	
Ce SE SM SM	rtificate T hanced Ki IIME Capa	emplate Name ey Usage bilities	DomainController Client Authentication (1.3.6.1 [1]SMIME Capability: Object I 20.b7.2b.4e.48.0f.2f.17.17.ef.	
(金) SU 用 Au	thority Ke	uenuner v Identifier	30 07 20 He Ho UT 2T 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.确认后,导航至"认证路径"**选项**卡。单击应是根CA证书的顶级证书,然后单击"查看证**书"**按钮。

💼 Certificate	×
General Details Certification Path	
Certification path	
	View Certificate
Certificate status:	
This certificate is OK.	
1	
	ОК

9.这将打开根CA证书的证书详细信息。

Certificate	×					
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						
ок						

10.打开"详细信**息"**选项卡,然**后单击"复制到文件……"** 如图所示.

Certificate		×
General Details Certification Path		
Show: <all></all>	~	
Field	Value ^	•
Version Serial number Signature algorithm Signature hash algorithm Issuer Valid from Valid to Subject	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	,
E	lit Properties Copy to File	1
	ОК	

11.浏览以PEM格式导出根CA的证书导出向导。

÷	🚰 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 Canc	el

12.选择**Base-64编码的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.选择文件的名称及其导出位置。

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.单击"完**成"**。

÷	ş	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 Can	cel

15.现在,导航到该位置,使用记事本或其他文本编辑器打开证书。这将显示PEM格式证书。保存此 内容以备以后使用。

----BEGIN CERTIFICATE----

```
MIIDCDCCAfCgAwIBAgIQE4ZG5Z1wT6lONTjooEQyMTANBgkqhkiG9w0BAQsFADAd
MRswGQYDVQQDExjleGFtcGxlLVdJTjIwMTYtQ0EwIBcNMjAwNDI3MTQ1MDU5WhgP
MjA2MDA0MTkxNDUwNTlaMB0xGzAZBgNVBAMTEmV4YW1wbGUtV010MjAxNi1DQTCC
ASIwDQYJKoZIhvcNAQEBBQADqqEPADCCAQoCqqEBAI8qhT719NzSQpoQPh0YT67b
Ya+PngsxMyvkewP33QLTAWw1HW1Tb9Mk5BDW0ItTaVsgHwPBfd++M+bLn3AiZnHV
OO+k6dVVY/E5qVkEKSGoY+v940S2316lzdwReMOFhgbc2qMertIoficrRhihonuU
Cjyeub3CO+meJUuKom2R47C0D35TUvo/FEHGgXJFaJS1se2UrpN07KEMkfAlLPuM
aob4XE/OzxYQpPa18djsNnskfcFqD/HOTFQN4+SrOhHWlRnUIQBUaLdQaabhipD/
sVs5PneYJX8YKma821uYI6j90YuytmsHBtCieyC062a8BKqOL7N86HFPFkMA3u8C
BBYEFD2fjjf7ER9EM/HCxCVFN5QzqEdvMA0GCSqGSIb3DQEBCwUAA4IBAQB31ZJo
vzwVD3c5Q1nrNP+6Mq62OFpYH91k4Ch9S5g/CEOemhcwg8MDIoxW2dTsjenAEt7r
phFIHZoCoSyjBjMgK3xybmoSeg8vBjCXseYNGEmOc9KW1oFmTOvdNVIb7Xpl1IVa
6tALTt3ANRNgREtxPA6yQbthKGavW0Anfsojk9IcDr2vp0MTjlBCxsTscbubRl+D
dLEFKQqmMeYvkVf+a7a64mqPZsG3Uxo0rd6cZxAPkq/ylcdwNSJFfQV3DqZq+R96
9WLCR3Obig6xyo9Zu+lixcWpdrbADO6zMhbEYEhkhOOjBrUEBBI6Cy83iTZ9ejsk
KgwBJXEu33PplW6E
```

----END CERTIFICATE----

FDM配置

验证许可

要在FDM上配置AnyConnect,FTD需要向智能许可服务器注册,并且必须向设备应用有效的Plus、 Apex或VPN专用许可证。

1.导航至"设**备">"智能许**可证",如图所示。

CISCO. Firepower Devic	ce Manager	Monitoring Policies	:문도 Objects	Device: FTD-3	(Σ)	۲	?:	admin Adm/nistrator
	traide Netwo	Cisco Firspower Threat De 0/0 2	0/1 0/2 0/2	NGMT COMSOLE	ISP/WAN/Gateway	Internet DNS Server ONTP Server	a	
Interfaces Connected Enabled 3 of 4 View All Interfaces	>	Routing 2 routes View Configuration	>	Updates Geolocation, Rule, VDE Security Intelligence Fo View Configuration	3, System Upgrade, eeds >	Syste Manag Loggin DHCP DNS S	erm Settings ement Access g Settings Server erver	ŀ
Smart License Registered View Configuration	>	Backup and Restore	>	Troubleshoot No files created yet REQUEST FILE TO BE	E CREATED	Manag Hostne NTP Cloud Reboo Traffic	ement Interfac me Services t/Shutdown Settings Itering Preferer	2

2.验证FTD是否已注册到智能许可服务器,并且AnyConnect Plux、Apex或仅VPN许可证已启用。

CISCO. Firepower Device Manager Monitoring Policies Objects	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 ENABLE Disabled by user	Malware Example Disabled by user
This License allows you to perform intrusion detection and prevention and file control. You must have this license to apply intrusion policies in access rules. You also must have this license to apply file policies that control files based on file type.	This License allows you to perform Cisco Advanced Malware Protection (AMP) with AMP for 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 DISABLE	RA VPN License Type PLUS V DISABLE
C Enabled	C Enabled
This license allows you to control web access based on URL categories and reputations, rather than by individual URL alone. You must have this license to deploy access rules that filter web traffic based on category and reputation.	Please select the license type that you purchased to enable remote access VPN. Note that Firepower Device Manager does not support any of the advanced features covered by the Apex license.
Includes: URL Reputation	Includes: RA-VPN

设置AD身份源

1.导航至"对**象">"身份**源",然后单击**+符**号并选择AD,如图所示。

cisco. Firepower Devic	e Manager Monitoring Pr	Objects Device: FTD-3	S 🔮 🕘 ? 🗄	admin Administrator
Object Types ← ^	Identity Sources			
C Networks	1 object		Q Search	+ ~
😫 Ports	* NAKE	THE	VALUE	RADIUS Server
🔒 Security Zones	1 LocalIdentitySource	LOCAL		RADIUS Server Group
🐔 Application Filters				AD
Ø URLS				Identity Services Engine
Geolocations				
Syslog Servers				
🔏 IKE Policies				
🐴 IPSec Proposals				
AnyConnect Client				
S Identity Sources				
1 Users				
R Certificates				
🔒 Secret Keys				
DNS Groups				
Ye Event List Filters				

2.使用之前收集的信息填写Active Directory服务器的适当设置。如果主机名(FQDN)用于Microsoft服 务器而不是IP地址,请确保在"对象"(Objects)>"DNS组"(DNS Group)下**创建适当的DNS组**。然后 ,导航到**Device > System Settings > DNS Server**,在**Management Interface** 和**Data Interface** 下 应用DNS组,然后为DNS查询指定适当的出口接口,将该DNS组应用到FTD。单击**Test**按钮以验证 是否成功配置并从FTD的管理接口访问。由于这些测试是从FTD的管理接口而不是通过在FTD上配 置的可路由接口(如内部、外部、dmz)启动的,因此成功(或失败)连接不能保证AnyConnect身 份验证的结果相同,因为AnyConnect LDAP身份验证请求将从FTD的可路由接口之一启动。有关从 FTD测试LDAP连接的详细信息,请查看故障排除区域中的测试AAA和数据包捕获部分。 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
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	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	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 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
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 CANCEL OK

如果使用LDAPS或STARTTLS,请选择适当的加密,然后选择受信任CA证书。如果尚未添加根 CA,请点击Create New Trusted CA Certificate。为根CA证书提供名称,然后粘贴之前收集的 PEM格式根CA证书。

0 ×

Add Trusted CA Certificate

	Ĩ.	
Name LDAPS_ROOT		
Paste certificate, or choose file: UPLOAD CERTIFICATE The supported formats are: PEM, DER.		
BEGIN CERTIFICATE MIIDCDCCAfCgAwIBAgIQE4ZG5Z1wT6IONTjooEQyMTANBgkqhkiG9w0BAQsFADAd		^
MRswGQYDVQQDExJleGFtcGxlLVdJTjlwMTYtQ0EwlBcNMjAwNDl3MTQ1MDU5WhgP MjA2MDA0MTkxNDUwNTlaMB0xGzAZBgNVBAMTEmV4YW1wbGUtV0IOMjAxNi1DQTCC ASIwDOY_IKoZlbycNAOERROADooEPADCCAOoCcoERAI8obT719NzSOooOPb0YT67b		~
CANCEL	ОК	
Directory Server Configuration		

		^
	Port	
	636	
	Trusted CA certificate	
~	LDAPS_ROOT	~
uccessful		
	✓	Port 636 Trusted CA certificate LDAPS_ROOT

在此配置中,使用了以下值:

- 名称:LAB-AD
- 目录用户名: ftd.admin@example.com
- 基准 DN:DC=example,DC=com
- AD主域: example.com
- 主机名/IP地址: win2016.example.com
- 端口:389
- 3.单击右上**角的"**待更改"按钮,如图所示。

cisco. Firepower De	avice Manager 👼 🦸 Monitoring Policies	Objects Device: FTD-3	admin Administrator
Object Types 🔶	 Identity Sources 		
C Networks	2 objects	Q. Snawh	+ ~
S Ports	H NAME	TYPE VALLE	ACTIONS
Security Zones	1 LocalIdentitySource	LOCAL	
Application Filters	2 LAB-AD	AD win2016.example.com	

4.单击"立即部**署"**按钮。

Pe	ending Changes	0 ×
0	Last Deployment Completed Successfully 01 May 2020 12:54 PM. <u>See Deployment History</u>	
	Deployed Version (01 May 2020 12:54 PM)	Pending Version C LEGEND 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	ORE ACTIONS Y	CANCEL DEPLOY NOW

配置AnyConnect以进行AD身份验证

要使用已配置的AD身份源,需要将其应用到AnyConnect配置。

1.导航到Device > Remote Access VPN,如图所示。

cisco. Firepower Device Manager	题 创 益 Monitoring Policies Objects	Device: FTD-3	admin Administrator
	000 [
Interfaces Connected Enabled 3 of 4 View All Interfaces	Routing 2 routes View Configuration >	Updates Geolocation, Rule, VDB, System Upgrade, Security IntelSgence 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.单击+**符号**或"创**建连接配**置文件"按钮,如图所示。



3.在"连接和客户端配置"部分下,选择之前创建的AD身份源。为其他部分设置适当的值,包括连接 配置文件名称和客户端地址池分配。完成后**单击"提**交查询"。

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 can 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	ion	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

4.在"远程用户体验"部分下,选择适当的组策略。默认情况下,**将使**用DfltGrpPolicy;但是,可以创 建另一个。

```
View Group Policy
```

DfltGrpPolicy

Policy Group Brief Details

DNS + BANNER	
DNS Server	None
Banner Text for Authenticated Clients	None
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"全局设置"(Global Settings)部分下,至少指定SSL证书、外部接口和AnyConnect软件包。如果 之前未创建证书,则可以选择默认自签名证书(<u>DefaultInternalCertificate</u>),但会看到不受信任的服 务器证书消息。应取消选中已解密流量(sysopt permit-vpn)的绕行访问控制策略,以便用户身份访问 策略规则稍后生效。NAT免除也可在此处配置。在此配置中,从内部接口到AnyConnect客户端IP地 址的所有ipv4流量除来自NAT外。对于更复杂的设置(如外部到外部迂回),需要在NAT策略下创 建其他NAT规则。AnyConnect软件包可在思科支持站点找到:

<u>https://software.cisco.com/download/home</u>。要下载AnyConnect软件包,需要有效的Plus或Apex许 可证。

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 Interf	ace		
ftd3.example.com			
e.g. ravpn.example.com			
Access Control for VPN Traffic Decrypted VPN traffic is subjected to access control policy inspection by default. Enabling the Bypass Access Control policy for decrypted traffic option bypasses the access control policy, but for remote access VPN, the VPN Filter Ac and the authorization ACL downloaded from the AAA server are still applied to VPN traffic Bypass Access Control policy for decrypted traffic (sysopt permit-vpn)			
NAT Exempt			
Inside Interfaces The interfaces through which remote access VPN users can connect to the Internal networks	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. D anv-inv4		
	.⊡ any-ipve		
AnyConnect Package			
If a user does not already have the right AnyConnect packa 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.cls You must have the necessary AnyConnect software license	ico.com.		



6.在"摘要"部分下,验证AnyConnect是否已正确设置,然后单击"提**交查询"**。

Summary

Review the summary of the Remote Access VPN configuration.

General		
FTER 4. CONNECTION AND CLIENT CONFIGURATI	CM	
STEP I: CONNECTION AND CLEAT CONFIGURATI		
Primary Identity Source		
Authentication Type	AAA Only	
Primary Identity Source	赴 LAB-AD	
Fallback Local Identity Source	-	
Strip Identity Source server from username	No	
Strip Group from Username	No	
Connedan Identity Course		
Secondary identity Source		
Secondary Identity Source for User Authenticatio	n –	
Fallback Local Identity Source	-	
Advanced Advanceed Advanceed Advanceed Advanceed Advanceed Adva		
<u> </u>		
Authorization Server		
Accounting Server		
Client Address Pool Assignment		
	anne anne	
	BACK SUBMIT QUERY	

7.单击右上**角的"**待更改"按钮,如图所示。

cisco. Firepower De	avice Manager 🕅 👘 🗮 Monitoring Policies Objects	Device: FTD-3	(5) 🛃 🗐 (?) 🕴 admin Administrator		
RA VPN +	Device Summary Remote Access VPN Connection Pro	Device Summery Remote Access VPN Connection Profiles			
Connection Profiles	1 object	Q	tearch +		
	# NAME	***	GROUP POLICY ACTIONS		
	1 General	Authentication: AAA Only Authorization: None Accounting: None	DfttGrpPolicy		

8.单击"立即**部署"**。

Pe	nding Changes	0 ×	Clos
 ♥ L 1 	ast Deployment Completed Successfully 6 Apr 2020 12:41 PM. See Deployment History		
	Deployed Version (16 Apr 2020 12:41 PM)	Pending Version C LEGEND Removed Added Edite	d
0	Network Object Added: AnyConnect-Pool		^
	-	<pre>subType: Network value: 10.10.10.0/24 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>	Ì
	anyconnectPackageFiles:	neurosenast - de 4 7 03050 - setateniau 10 etc.	
	<pre>- vpmGatewaySettings[0].serverCertificate;</pre>	anyconnect-win-4.7.00052-webbepioy-k9.pkg	
	-	FTD-3-Manual	
	<pre>vpnGatewaySettings[0].outsideInterface:</pre>		
	- uncatevauSattines[0] insideInterfaces.	outside	
	-	inside	
	vpnGatewaySettings[0].insideNetworks:		~
мо	RE ACTIONS Y	CANCEL DEPLOY NOW	

启用身份策略并配置用户身份的安全策略

此时,AnyConnect用户应该能够成功连接,但可能无法访问特定资源。此步骤将启用用户身份,以 便只有AnyConnect管理员中的用户可以使用RDP连接到内部资源,并且只有组AnyConnect用户中 的用户可以使用HTTP连接到内部资源。

1.导航至Policies > Identity, 然后单击Enable Identity Policy。



对于此配置,无需进一步配置,默认操作就足够了。

cisco. Firep	ower Device Manag	er Mo	itoring Polici	os Objects	Device: FTD-3		o 🚑 Ø	? : å	ámin dministrator	~		
🛷 Security I	Policies											
$\Box \rightarrow \bigcirc SSL Decryption \rightarrow \textcircled{SSL Decryption} \rightarrow \bigcirc Security Intelligence \rightarrow \textcircled{NAT} \rightarrow \textcircled{Access Control} \rightarrow \textcircled{Intrusion}$												
Identity Policy	D					Q Search			¢ <u>a</u>	+		
# NAME	AUTHENTICATION	AUTH, TYPE	SOURCE	NETWORKS	PORTS	DESTINATION	NETWORKS	PORTS/PROTO	ACTIO	45		
				_								
				Start by creating	r identity rules yet. 9 the first identity rule.							
				CREATE	IDENTITY RULE							
Default Action	🙆 Passive Auth 🛛 A	ny Identity Source	· 0									

2.导航至**Policies > NAT**,确保NAT配置正确。如果在AnyConnect设置中配置的NAT异常已足够 ,则无需在此处进行其他配置。

cisco. Firepor	ver Device	Manager	Monitoring	Policies	i≑≣ Objects	Device: FTD-3		۵. 🚑	۵ ()	admin Adminis	trator
🛷 Security P	olicies										
□ → ○ s	5L Decryption	-> 🕑 kd	entity \rightarrow () is	ecurity Intelligence	• -> 🕑 NAT	- 📀 Acces	ss Control \rightarrow	S Intrusion			
1 rule								Q Search			+
OPPORVAL PACKET THIS											
			OFFICINAL PACKET				TRANSLATED PACK	17			
a NAME	TYPE	INTERFACES	OFFICENAL PACKET	DESTINATIO	SOURCE PORT	DESTINATIO	TRANSLATED PACK	DESTINATIO	SOURCE PORT	DESTINATIO	ACTIONS
a NAMI Auto NAT Rules	TYPE	INTERFACES	OFFICINAL PACKET	DESTINATIO	SOUNCE POINT	DESTINATIO_	TRANSLATED PACK	DESTINATIO	SOURCE PORT	DESTINATIO	ACTIONS

3.导航至"策**略">"访问控制**"。在本节中,Default Action(默认操作)设置为Block(阻止),并且未 创建访问规则,因此,一旦AnyConnect用户连接,他们将无法访问任何内容。单击+**符号或**创建访 问规则以添加新规则。

cisco. Fire	epower Device Manager	题 Monitoring	Ø Policies	ii⊒ Objects	Device: FTD-3		6.	0 ()	adi Ad	min v ministrator	
🛷 Security	y Policies										
$\Box \rightarrow \bigcirc SSL Decryption \rightarrow \oslash Identity \rightarrow \bigcirc Security Intelligence \rightarrow \oslash NAT \rightarrow \bigodot Access Control \rightarrow \And Intrusion$											
						Q Search				®. +	
	sounce			DESTINATION							
8 NAME	ACTION ZONES	NETWORKS	PORTS	ZONES	NETWORKS	PORTS/PROTO	APPLICATIONS	UPLS	USERS	ACTIONS	
			St	There are no i art by creating (access rules yet. the first access rule.						
				CREATE A	ACCESS RULE						
Default Action	Access Control 😑 Block	9, E, V									

4.用适当的值填写字段。在此配置中,AnyConnect Admins组内的用户应具有对内部网络中 Windows服务器的RDP访问权限。对于源,区域配置为outside_zone,该外部接口是AnyConnect用 户将要连接到的外部接口,而网络配置为AnyConnect-Pool对象,此对象之前配置为向 AnyConnect客户端分配IP地址。对于FDM中的用户身份,源必须是用户从发起连接的区域和网络。 对于目标,区域配置为Windows Server所在的内部接口inside_zone,网络配置为定义Windows Server所在子网的Inside_Net对象,端口/协议设置为两个自定义端口对象以允许通过TCP 3389和 UDP 3389进行RDP访问。

Edit Access Rul	e					×
Order Title 1 Y AC RDP Ac Source/Destination Ap	pplications URLs Use	Action Allow	File policy ⁹ Logging			
SOURCE Zones +	Networks +	Ports +	DESTINATION Zones +	Networks +	Ports/Protocols	+

Show Diagram	0. 0	CANCEL	04
	Not hit yet	CANCEL	UK .

在"用户"部分下,将添加组AnyConnect管理员,以便允许此组以外的用户通过RDP访问Windows服 务器。单击+**符号**,单击"组"选项卡,单击适当的组,然后单击"**确定"**。请注意,也可以选择单个用 户和身份源。

Add Access Rule		×
Order Title Action 1 AC RDP Access Image: Allow model Source/Destination Applications URLs Users Intrusion Policy® File policy® Logging		
AVAILABLE USERS It CONTROLLING ACCESS FOR USERS AND USER GROUPS It filter Identity Sources Groups LAB-AD \ Account Operators It LAB-AD \ Administrators It LAB-AD \ AnyConnect Users Create new Identity Realm CANCEL	ource IP oply the or obtain hip, use moving	S a f
Show Diagram CANCEL	OK	

选择适当的选项后,单击"确**定"**。

Add Access Rule	0 ×
Order Title 1 V AC RDP Access	Action Allow
Source/Destination Applications URLs Users AVAILABLE USERS LAB-AD \ AnyConnect Admins	Intrusion Policy File policy Logging Image: 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.根据需要创建更多访问规则。在此配置中,会创建另一个访问规则以允许AnyConnect用户组内的 用户通过HTTP访问Windows服务器。

Edit Access F	Rule	e									×
Order Title 2 AC HT Source/Destination	TTP A	plications URLs	Use	Action Allor rs Intrusion Policy	w ~ 0	File policy [©] Loggi	ng				
SOURCE Zones	+	Networks	+	Ports	+	DESTINATION	+	Networks	+	Ports/Protocols	+
Outside_zone		T AnyConnect-Pool		ANY		inside_zone		C Inside_Net		₩TTP	

Show Diagram	0	0 Not hit yet	CANCEL	ок

Edit Access Rule	0 ×	
Order Title	Action	
2 Y AC HTTP Access	Allow ∨	
Source/Destination Applications URLs Users Inf	trusion Policy ⁹ File policy ⁹ Logging	
AVAILABLE USERS	+ 11 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 membership. By controlling access based on user identity, you can apply the	

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

CANCEL

 Not hit yet
 Not hi Show Diagram

6.验证访问规则配置,然后单击右上角的Pending Changes按钮,如图所示。

cisco. Firepowe	er Devic	e Manager	Monitoring	OF Policies	Cobjects D	evice: FTD-3		0	0?) : (;	ədmin Administrat	tor
Ø Security Policies												
$\square \rightarrow \bigcirc$ SSL	Decryptio	o 🔶 🥑 Iden	tity \rightarrow \bigcirc Se	curity Intelligence	ightarrow 📀 NAT	→ 🖌 Access	Control 🔿 🦉	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_Not	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.	
Default Action Acco	ess Control	O Block	E. I v									

7.验证更改,然后单击"立即**部署"**。

Pending Changes

0 ×

Last Deployment Completed Successfully

使用本部分可确认配置能否正常运行。

show running-configuration aaa-server

dn ftd.admin@example.com server-type auto-detect

28 Apr 2020 01:35 PM. See Deployment History

	Deployed Version (28 Apr 2020 01:35 PM)	Pending Version 3 LEGEND Removed Added Edited	
Θ	Access Rule Added: AC HTTP Access	-	•
	- - - - sourceZones:	users[0].name: AnyConnect Users logFiles: false eventLogAction: LOG_NONE ruleId: 268435467 name: AC HTTP Access	
	- destinationZones:	outside_zone	
	- sourceNetworks:	inside_zone	
	- destinationNetworks:	AnyConnect-Pool	
	- destinationPorts:	Inside_Net	
	users[0].identitySource:	LAB-AD	
0	Access Rule Added: AC RDP Access		,
M	ORE ACTIONS Y	CANCEL DEPLOY NOW	

验证

最终配置

AAA配置

webvpn

配置AnyConnect

enable outside http-headers hsts-server enable

no preload

max-age 31536000 include-sub-domains

> show running-config webvpn

	destinationNetworks:	
	-	Inside_Net
	destinationPorts:	
	-	HTTP
	users[0].identitySource:	
	-	LAB-AD
0	Access Rule Added: AC RDP Access	~
мо	REACTIONS Y	CANCEL DEPLOY NOW V

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-login-

```
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连接并验证访问控制策略规则

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

🕙 Cisco AnyC		-		×	
	VPN: Connected to ftd3.example.com. ftd3.example.com	~		Disconnect	
00:00:14				I	Pv4
Ö (i)					

用户IT管理员位于组AnyConnect管理员中,该管理员具有对Windows Server的RDP访问权限,但 无权访问HTTP。打开到此服务器的RDP和Firefox会话,验证此用户是否只能通过RDP访问服务器 。

	Windows Security ×					
	Enter your credentials These credentials will be used to connect to win2016.example.com.					
Note Desktop Connection – 🗆 🗙						
Remote Desktop Connection	User name Password					
Computer: win2016.example.com	Domain:					
User name: None specified You will be asked for credentials when you connect.	Remember my credentials					
Show Optio Cognect Help	OK Cancel					
A Problem loading page × +	– – ×					
\leftrightarrow \rightarrow C ^d (a) (b) (c) win2016.example.com	♡☆ Ⅲ\ ① ③ ≪ Ξ					
The	server at win2016.example.com is taking too long to respond. The site could be temporarily unavailable or too busy. Try again in a					
L. X. S	few moments.					
If you are unable to load any pages, check your computer's network connection.						
says.	If your computer or network is protected by a firewall or proxy, make sure that Firefox is permitted to access the Web.					
Timed Out	Try Again					

如果使用AnyConnect用户组中具有HTTP访问权限但没有RDP访问权限的测试用户登录,则可以验 证访问控制策略规则是否生效。



故障排除

使用本部分可确认配置能否正常运行。

调试

此调试可在诊断CLI中运行,以排除与LDAP身份验证相关的问题:debug Idap 255。

为了排除用户身份访问控制策略问题,**系统支持firewall-engine-debug**,以便确定流量被意外允许或 阻止的原因。

工作LDAP调试

```
[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
```

无法与LDAP服务器建立连接

[-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

潜在解决方案:

• 检查路由并确保FTD收到来自LDAP服务器的响应。

- 如果使用LDAPS或STARTTLS,请确保正确的根CA证书受信任,以便SSL握手可以成功完成。
- 检验使用的IP地址和端口是否正确。如果使用主机名,请验证DNS是否能将其解析为正确的 IP地址

绑定登录DN和/或密码不正确

```
[-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
```

潜在解决方案:验证登录DN和登录密码是否已正确配置。这可以在AD服务器上使用ldp.exe**进行验 证**。要验证帐户是否可以成功绑定使用ldp,请浏览以下步骤:

 Image: Run internet intere

1.在AD服务器上,按Win+R并搜索ldp.exe。

2.单击"**连接">"连接……"** 如图所示.

🔝 Ldp	_		×
Connection Browse View Options Utilities Help			
Connect			
Bind Ctrl+B			
Disconnect			
New Ctrl+N			
Save			
5.4			
Exit			
		NUM	

3.为服务器和相应的端口指定localhost,然后单击**OK**。

Connect		×
<u>S</u> erver:	localhost	
Port:	389	Connectionless
<u>O</u> K		<u>C</u> ancel

4.右列显示指示连接成功的文本。单击Connection > Bind... 如图所示.



5.选择"简单绑定",然后指定"目录帐户用户名和密码"。Click OK.

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

如果绑定成功,则ldp将显示Authenticated为DOMAIN\username。

🔝 Idap://w	🔝 Idap://win2016.example.com/DC=example,DC=com — 🗆 🗙									
Connection	Browse	View	Options	Utilities	Help					
				1.2. 1.2. supporte Max Max Max Max Max Max Max Supporte supporte SPN	840.113556 840.113556 840.113556 edLDAPPoli PercentDir ReceiveBu Connection BatchRetur DirSyncDu ResultSets ResultSets ValRange; edMemory edLDAPVer edSASLMe IEGO; EXTE	5.1.4.2255; 5.1.4.2256; 5.1.4.2309; cies (20): Ma SyncReques ffer; InitRectors; MaxConn rnMessages ration; MaxT ize; MinRestor PerConn; Ma MaxValRang Limit; Syster rsion (2): 3; 3 chanisms (4 RNAL; DIGE	axPooIThr sts; MaxDa vTimeout; IdleTime; I idleTime; I	eads; atagramR MaxPage ryDuratio Size; tionPerCo ve; .imitPerce I; GSS-	ecv; Size; n; onn; ent;	^
				es = Idap_s unavailable wthenticate	imple_bind e>); // v.3 ed as: 'EXA	_s(ld, 'ftd.ad MPLE\ftd.ad	lmin@exai min'.	mple.com	<i>l.</i>	~
Ready										

如果尝试使用无效的用户名或密码进行绑定,将导致此类失败。

Idap://win2016.example.com/DC=example,DC=com - D								×	
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 erver error omment: Ac rror 0x8005	ResultSetSi (ResultSetsF (ValRange; I eadMemoryL edLDAPVers edSASLMed IEGO; EXTEF simple_bind_ e>); // v.3 ed as: 'EXAM simple_bind_ e>); // v.3 Idap_simple_ cceptSecuri 90308 The to	ze; MinResu PerConn; Ma MaxValRang imit; Systen sion (2): 3; 2 hanisms (4) RNAL; DIGE s(Id, 'ftd.adr s(Id, 'ftd.adr s(Id, 'wrong bind_s() fa LdapErr: D tyContext er oken supplie	utSets; ixNotificat geTransitiv nMemoryL 2;): GSSAPI ST-MD5; min@examp nin".)@examp iled: Invali SID-0C090 rror, data ed to the fi	ionPerConn /e; .imitPercent; ; GSS- nple.com', le.com', d Credentia 042A, 52e, v3839 unction is	is is
Ready									

LDAP服务器找不到用户名

```
[-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
潜在解决方案:验证AD是否可以通过FTD完成搜索找到用户。这也可以通过ldp.exe完成。
```

1.成功绑定后,导航至"视图">"树",如图所示。

Connection Browse View Options Utilities Help Tree Ctrl+T Interprise Configuration //axPoolThreads; sts; MaxDatagramRecv; Status Bar Status Bar Strimeout; ndleTime; MaxPageSize; s; MaxQueryDuration; Status Bar Status Bar Status Bar Status Bar Status Bar Status Bar MaxDirSyncDuration; MaxTempTableSize; MaxQueryDuration; maxResultSetSize; MinResultSets; MaxNarResultSetSize; MinResultSetSize; MinResultSetSize; MinResultSetSize; MinResultSetSize; MinResultSetSize; MaxNalRange; MaxValRangeTransitive; ThreedMemoryLimit; SystemMemoryLimitPercent; supportedSASLMechanisms (4): GSSAPI; GSS- SPNEGO; EXTERNAL; DIGEST-MD5; res = Idap_simple_bind_s(Id, 'ftd.admin@example.com', /// v.3 Authenticated as: 'EXAMPLE\ftd.admin'.	Idap://win2016.example.com/DC=example,DC=com									\times		
Tree Ctrl+T Enterprise Configuration //axPoolThreads; sts; MaxDatagramRecv; vTimeout; nldleTime; MaxPageSize; s; MaxQueryDuration; Set Font MaxDirSyncDuration; MaxTempTableSize; MaxResultSetSize; MinResultSets; MaxResultSetSize; MinResultSets; MaxResultSetsPerConn; MaxNotificationPerConn; MaxValRange; MaxValRangeTransitive; ThreadMemoryLimit; SystemMemoryLimitPercent; supportedLDAPVersion (2): 3; 2; supportedSASLMechanisms (4): GSSAPI; GSS- SPNEGO; EXTERNAL; DIGEST-MD5;	Connection	Browse	View	v Options	Utilities	Help						
Set Font s; MaxQueryDuration; MaxDirSyncDuration; MaxTempTableSize; MaxResultSetSize; MinResultSets; MaxResultSetSPerConn; MaxNotificationPerConn; MaxValRange; MaxValRangeTransitive; ThreadMemoryLimit; SystemMemoryLimitPercent; supportedLDAPVersion (2): 3; 2; supportedSASLMechanisms (4): GSSAPI; GSS- SPNEGO; EXTERNAL; DIGEST-MD5;			~	Tree Enterprise Status Bar	Configurat	ion	Ctrl+T	AaxPoolThreads; sts; MaxDatagramRecv; cvTimeout; nldleTime: MaxPageSize				
res = ldap_simple_bind_s(ld, 'ftd.admin@example.com', <unavailable>); // v.3 Authenticated as: 'EXAMPLE\ftd.admin'.</unavailable>	Set Font Indel Time; MaxPageSize; s; MaxQueryDuration; s; MaxQueryDuration; maxResultSetSize; MinResultSetSize; MaxResultSetSize; MinResultSets; MaxResultSetsPerConn; MaxNotificationPerConn MaxValRange; MaxValRangeTransitive; ThreadMemoryLimit; SystemMemoryLimitPercent supportedLDAPVersion (2): 3; 2; supportedSASLMechanisms (4): GSSAPI; GSS- SPNEGO; EXTERNAL; DIGEST-MD5;								on; onn; ent;			
		r,										

2.指定在FTD上配置的基本DN,然后单击**OK**。

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

3.右键点击Base DN,然后点击Search,如图所示。

🔝 Idap://win2016.example.com/DC=example,DC=com — 🗆 🗙							(
Connection	Browse	View	Options	Utilities	Help		
⊕ DC=examp	DC= example, DC= com		Search Virtual List View Delete Modify Modify DN Add child Compare		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 document							

- 4.指定调试中看到的相同的Base DB、Filter和Scope值。在本例中,以下是:
 - 基准 DN:dc=example,dc=com
 - 过滤器:samaccountname=it.admi
 - •范围:子树

🟠 Idap://w	n2016.example.com/DC=example,DC=com	– 🗆 ×					
Connection	Browse View Options Utilities Help						
Search	×	C=example,DC=com; S8811D1ADED00C04FD8D5CD:C					
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 <	68811D1ADED00C04FD8D5CD:C nple,DC=com;					
Options	Run Close	2020 3:43:59 PM Eastern Daylight					
***Searching //////////////////////////////////							
Ready							

ldp查找0个条目,因为在Base DN dc=example,dc=com下**没有具有samaccountname=it.admi**的用 户帐户。

再次尝试使用正确的**samaccountname=it.admin显示**的结果不同。ldp在Base DN dc=example,dc=com下查找1个条目并打印该用户的DN。

🔝 Idap://wi	n2016.example.com/DC=exar	mple,DC=	=com		– 🗆 ×		
Connection	Browse View Options	Utilities	Help				
Search				×	58811D1ADED00C04FD8D5CD:C DC=example,DC=com; 58811D1ADED00C04FD8D5CD:C	^	
Base <u>D</u> N:	DC=example,DC=com			\sim	ample,DC=com;		
<u>F</u> ilter:	sAMAccountName=it.admin			\sim	lers,DC=example,DC=com;		
Scope	○ <u>O</u> ne Level <u> S</u> ubtree				58811D1ADED00C04FD8D5CD:C example,DC=com; 68811D1ADED00C04FD8D5CD:C mple_DC=com;		
<u>A</u> ttributes:	objectClass;name;description;c	anonicalN	lame	\sim	020 3:43:59 PM Eastern Daylight		
Options	<u>R</u> un		<u>C</u> lose)20 2:41:57 PM Eastern Daylight		
***Searching Idap_search_s(Id, "DC=example,DC=com", 2, "sAMAccountName=it.admin", attrList, 0, &msg) Getting 1 entries: Dn: CN=IT Admin,CN=Users,DC=example,DC=com canonicalName: example.com/Users/IT Admin; name: IT Admin; objectClass (4): top; person; organizationalPerson; user;							
Ready	9						

用户名的密码不正确

```
[-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
```

潜在解决方案:验证用户的密码是否配置正确且未过期。与登录DN类似,FTD将使用用户凭证对 AD进行绑定。此绑定也可以在ldp中完成,以验证AD是否能够识别相同的用户名和密码凭证。ldp中 的步骤显示在绑定登录DN和**/或密码不正确部分中**。此外,还可以出于可能的原因查看Microsoft服 务器事件查看器日志。

测试AAA

test aaa-server命令可用于使用特定用户名和密码模拟来自FTD的身份验证尝试。这可用于测试连 接或身份验证失败。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
```

数据包捕获

数据包捕获可用于验证到AD服务器的可达性。如果LDAP数据包离开FTD,但没有响应,这可能表 示路由问题。

以下是显示双向LDAP流量的捕获完成:

> 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事件查看器日志

AD服务器范上的事件查看器日志提供了有关失败原因的更多详细信息。

1.搜索并打开事件查看器。

=	Best match							
ŵ	Event Viewer Desktop app							
	Settings >							
	🖄 Vi	🐵 View event logs						
۲	10	۲	ß		63	□	រុក	
	event							
-	Q	([])	e	-	2		8	

2.展开"Windows**日志"**并单击"**安全"**。使用用**户的帐**户名搜索"审核失败",并查看"失败信息",如图所 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