在由 FMC 管理的面向 AnyConnect 客户端的 FTD 上配置 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 背景信息 配置 网络图和场景 Active Directory配置 确定LDAP基本DN和组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(仅对于LDAPS或STARTTLS是必需的) FMC配置 验证许可 设置领域 配置AnyConnect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 配置NAT免除 部署 验证 最终配置 AAA配置 AnvConnect配置 使用AnyConnect连接并验证访问控制策略规则 使用FMC连接事件进行验证 故障排除 调试 正在运行的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

本文档介绍如何为连接到思科Firepower威胁防御(FTD)的AnyConnect客户端配置AD身份验证。

先决条件

要求

Cisco 建议您了解以下主题:

- •基本了解FMC上的RA VPN配置
- •基本了解FMC上的LDAP服务器配置
- Active Directory(AD)基础知识

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FMCv
- •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。

背景信息

本文档介绍如何为连接到Cisco Firepower**威胁防御(FTD)**(由Firepower管理中心(FMC)管理)的 AnyConnect客户端配置Active Directory(AD)身份验证。

用户身份用于访问策略,以将AnyConnect用户限制为特定IP地址和端口。

配置

网络图和场景



Windows服务器预配置了IIS和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:用作目录帐户,以允许FTD绑定到Active Directory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 Admins:添加IT管理员以演示用户身份的测试组。此组仅对Windows Server具有 RDP访问权限。
- AnyConnect用户:添加测试用户以展示用户身份的测试组。此组仅对Windows Server具有 HTTP访问权限。

Active Directory配置

要在FTD上正确配置AD身份验证和用户身份,需要几个值。

在FMC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。主要值包括:

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FMC和FTD中配置DNS服 务器以解析FQDN。

在本配置指南中,此值为win2016.example.com(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使用TCP端口389进行LDAP,LDAP over SSL(LDAPS)使用TCP端口636。

•根 CA:

如果使用LDAPS或STARTTLS,则需要用于签署LDAPS所用SSL证书的根CA。

•目录用户名和密码:

这是FMC和FTD用于绑定到LDAP服务器、对用户进行身份验证以及搜索用户和组的帐户。

为此创建了一个名为FTD Admin的帐户。

•基本和组可分辨名称(DN):

基础DN是FMC的起点,FTD告知Active Directory开始搜索和验证用户。

同样,组DN是起点,FMC告知Active Directory从何处开始搜索用户身份组。

在本配置指南中,根域example.com用作基础DN和组DN。

但是,对于生产环境,在LDAP层次结构中进一步使用Base DN和Group DN会更好。

例如,此LDAP层次结构:



如果管理员希望**Marketing**组织单位内的用户能够验证基本DN,可以将基本DN设置为根 (example.com)。

但是,这也允许**Finance**组织单元下的User1登录,因为用户搜索从根目录开始,然后转到 **Finance、Marketing**和**Research**。

基本DN设置为example.com



要将登录限制为Marketing组织单位及以下单位中的唯一用户,管理员可以将Base DN设置为 Marketing。

现在只有User2和User3能够进行身份验证,因为搜索从Marketing开始。

基本DN设置为Marketing



请注意,为了在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。

有关这方面的详细信息,请参阅<u>:在Firepower威胁防御(FTD)上配置AnyConnect LDAP映射</u>。

此配置指南中使用此简化的LDAP层次结构,根example.com的DN用于基础DN和组DN。



确定LDAP基本DN和组DN

1.打开Active Directory用户和计算机。



2.左键点击根域(打开容器),右键点击根域,然后在视图下单击高级功能。



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,然后选择**Properties**。



4.在Properties下,选择Attribute Editor选项卡。在Attributes下查找distinguishedName,然后单击 View。

example.com Properties		?	×
General Managed By 0	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)		
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	
OK	Cancel Apply	Hel	þ

5.这将打开一个新窗口,以后可以在其中复制并粘贴到FMC中。在本示例中,根DN为 DC=example,DC=com。

复制值,保存以备后用。单击OK退出String Attribute Editor窗口,然后再次单击OK退出 Properties。



这可以对Active Directory中的多个对象执行此操作。例如,这些步骤用于查找User容器的DN:



6.再次右键单击根DN,然后在View下再次单击Advanced Features,可以删除Advanced Features视图。



创建FTD帐户

此用户帐户允许FMC和FTD与Active Directory绑定,以搜索用户和组并对用户进行身份验证。

创建单独的FTD帐户的目的是,在用于绑定的凭证遭到入侵时,防止未经授权访问网络内的其他位 置。

此帐户无需在基础DN或组DN范围内。

1.在Active Directory用户和计算机中,右键单击FTD帐户添加到的容器/组织。

在此配置中,FTD帐户将添加到用户名ftd.admin@example.com下的Users容器下。

右键单击Users,然后导航到New > User。

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		Ŷ

2.完成"新建**对象 — 用户向**导"。

Create in: ex Erst name: FTC Last name: Adn	ample.com/Users
<u>B</u> irst name: FTC Last name: Adm	D Initials:
Last name: Adn	win
Full name: FTD	D Admin
User logon name:	
ftd.admin	@example.com ~
User logon name (pre-Wind	dows 2000):
EXAMPLE\	ftd.admin
	< Back Next > Cancel

New Object - User		×
🤱 Create in: exam	nple.com/Users	
Password:	•••••	
Confirm password:	•••••	
User must change passw	ord at next logon	
User cannot change pass	brows	
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 Nowing 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: @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: @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: @example.com	×
New Object - User Create in: exam When you click Finish, the for Full name: FTD Admin User logon name: ftd.admine The password never expires	nple.com/Users Nowing 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: @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: @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: @example.com	×

3.验证是否已创**建FTD**帐户。另外创建了两个帐户:IT管理员和测试用户。

Active Directory Users and Com	-	×			
File Action View Help					
🗢 🔿 🖄 📷 🖌 🗈 🗙 🛙	🛛 🗟 📑 🔽 🖬	1 🙎 🔌 🛍 🦷	7 🗾 🗽		
 Active Directory Users and Com Saved Queries Saved Queries Builtin Computers Domain Controllers ForeignSecurityPrincipals Managed Service Accourting Users 	Name DefaultAcco DefaultAcco DefaultAcco DonsUpdateP Domain Ad Domain Ad Domain Co Domain Co Domain Gue Domain Gue Domain Gue Domain Gue Domain Gue Domain Gue Domain Gue Domain Gue Domain Gue Comain Gue.	Type User Security Group Security Group User User 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 Designated administrato Members of this group Members of this group c Built-in account for gue Members of this group Designated administrato		^
< >>	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将访问策略应用至多个用户以及LDAP授权的过程。

在本配置指南中,组稍后用于通过FMC内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,右键单击新组添加到的容器或组织单位。

在本示例中,AnyConnect Admins组被添加到**Users**容器下。右键单击**Users**,然后导航到**New >** Group。

Active Directory Users and Com	puters			-	х
File Action View Help					
🗢 🔿 🙍 🚾 🔏 💷 🗶 🛙	n 🖸 🔒 👔 🖬	1 🗏 🐮 🕅 🦷	r 🗾 🤽		
Active Directory Users and Com Saved Queries Saved Queries Delegate Com Find	Name DefaultAcco Denied ROD DnsAdmins DnsUpdateP Domain Ad Domain Ad Domain Co ntrol ers	Type User Security Group Security Group Security Group Security Group Security Group Security Group Security Group	Description A user account manage Members in this group c DNS Administrators Gro DNS clients who are per Designated administrato All workstations and ser All domain controllers i All domain guests All domain users		^
All Tasks View Refresh Export List Properties Help	> > A Read-only & Schema A & Test User	Computer Contact Group InetOrgPerson msDS-KeyCreder msDS-ResourceP msDS-ShadowPr msImaging-PSPs MSMQ Queue Al Printer User	ntial PropertyList incipalContainer ias		
Creates a new item in this container.	(79)	Shared Folder			

2.执行"新建**对象 — 组"向**导。

ew Object - Group	×
🥵 Create in: exam	nple.com/Users
Group name:	
AnyConnect Admins	
Group name (ore-Windows 2)	000):
AnyConnect Admins	
Group scope	Group type
O Domain local	Security
Global	ODistribution
OUniversal	
	OK Canad

3.确认已创建组。AnyConnect Users组也将创建。

Active Directory Users and Computers					×
File Action View Help					
🗢 🔿 🙍 📰 🔏 🗙 🖼 🛛	è 🛛 🖬 🐍 🗽 🛍 '	7 🗾 🐍			
Active Directory Users and Com Saved Queries Saved Queries Builtin Builtin Computers Solution ForeignSecurityPrincipals Managed Service Accour Users	Name AnyConnect Admins AnyConnect Users Calo Cert Publishers Cloneable Domain C DefaultAccount DefaultAccount Domain RODC Passw DnsUpdateProxy Domain Admins DosUpdateProxy Domain Computers Domain Computers Domain Controllers Domain Guests Domain Guests Domain Guests Enterprise Key Admins Enterprise Key Admins Enterprise Read-only FTD Admin Group Policy Creator Guest IT Admin Key Admins	Type Security Group Security Group User Security Group User Security Group Security Group User User User Security Group	Description Built-in account for ad Members of this group Members of this group t A user account manage Members in this group c DNS Administrators Gro DNS clients who are per Designated administrato All workstations and ser All domain controllers i All domain guests All domain guests All domain users Designated administrato Members of this group Members of this group Built-in account for gue		
, ,	(h.s				¥

4.右键单击用户组,然后选择**属性**。在此配置中,用户IT Admin被添加到AnyConnect Admins组 ,用户**Test User**被添加到**AnyConnect Users组**。

Active Directory Users and Computers	-	×
File Action View Help		
수 수 2 📷 사 🗈 🗙 🖼 🕢 🔂 🖬 🛛 🖬 🖏 🖄 🧐 🏹 🗟 🗞		
Active Directory Users and Com Name Type Description		^
> Saved Queries AnyConnect Admins Security Group Add to a group > Builtin Computers Security Group Buil Move > Domain Controllers CorreginSecurityPrincipat Coneable Domain C Security Group Mer And to a group > Managed Service Accour Managed Service Accour DefaultAccount User Mer And > Users Managed Service Accour DefaultAccount User Mer Cut Display Domain Computers Security Group Mer Cut Delete Display Domain Computers Security Group Mer Cut Delete Display Domain Computers Security Group DN: Delete Domain Computers Security Group DN: Rename Domain Computers Security Group All Help Domain Guests Security Group All Help Domain Guests Security Group All domain users Designated administrato Enterprise Read-only Security Group Members of this group Mer Enterprise Read-only Secur		
< > Key Admins Security Group Members of this group		~

5.在"成员**"选**项卡下,单击**添加**。

AnyConnect Admins Properties	?	×
General Members Member Of Managed By		
Members:		
Name Active Directory Domain Services Folder		
		- 1
Add Remove		
OK Cancel	Appl	ý

在字段中输入用户,然后单击Check Names以验证是否已找到该用户。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

确认已添加正确的用户,然后点击OK按钮。用户的Test User也会使用相同的步骤添加到 AnyConnect Users组。

AnyConnect A	dmins	Properties			?	х
General Merr	bers	Member Of	Managed By			
Members:						_
Name	1	Active Directory	ectory Domain om/Users	Services Folder		
Add		Remove				
			ОК	Cancel	Арр	ły

复制LDAPS SSL证书根(仅对于LDAPS或STARTTLS是必需的)

1.按Win+R并输入mmc.exe,然后单击"确定"。

	-	
1000	0	
	100	
_		

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

2.导航到**文件>添加/删除管理单元……**

ᡖ Co	onsole1 - [C	onsole	Root]										-		×
🚡 File	a Action	View	Favorites	Window	Help									-	8 ×
4	New			Ctrl+N											
	Open			Ctrl+0							Action	5			
	Save			Ctrl+S	There are	no iter	ms to sh	now in this v	iew.		Conso	le Root			
	Save As										M	lore Actions			×
	Add/Ren	nove Sna	ap-in	Ctrl+M											
	Options.														
	1 dnsmg	mt													
	2 dsa														
	Exit														
Enables	you to add	l snap-ir	ns to or rem	ove them fro	om the snap-in cons	ole.									

3.在"可用管理单元"下,选择**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。

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 2	×
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 Alow the selected computer to be changed when launching from the command line. This only applies if you save the console.	
< Back Finish Cancel	

5.现在单击**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:				elected snap-ins:			
Snap-in	Vendor	^		Console Root	Edit Extensions		
Active Directory Do	Microsoft Cor Microsoft Cor			데이슈(Local Computer)	Remove		
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						
Scomputer Managem	Microsoft Cor						
Device Manager	Microsoft Cor						
T 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.							
				C	OK Cancel		

6.展开**Personal**文件夹,然后单击**Certificates**。LDAPS使用的证书颁发给**Windows服务器的完全限 定域名(FQDN**)。此服务器上列出了3个证书。

[•] 颁发给example-WIN2016-CA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个证书不能用作LDAPS SSL证书。颁 发给win2016.example.com的身份证书是由Windows Server CA服务自动颁发的证书。双击证书检 查详细信息。

🜇 Console1 - [Console Root\Certifi	cates (Local Computer)\Personal\C	ertificates]			-	
🖀 File Action View Favorites	Window Help					- 8 ×
🗢 🏟 🗖 📅 🛍 🗖 🕞 🖡	? 💼					
Console Root	Issued To	Issued By	Expiration Da	Actions		
 Certificates (Local Computer) 	🛱 example-WIN2016-CA	example-WIN2016-CA	4/19/2060	Certificates		
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						
> iii Trusted Publishers						
> Untrusted Certificates						
> Third-Party Root Certificat						
> Trusted People						
Client Authentication Issue Denticue Ruild Reads	6					
> Preview build Roots						
Semote Deskton						
Certificate Enrollment Reg						
> Smart Card Trusted Roots						
> 📫 Trusted Devices						
> 🔛 Web Hosting						
> I Windows Live ID Token Iss						
			>			
Personal 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主体备用名称(DNS Subject Alternate Name)与Windows Server的FQDN匹配。

• 证书在Enhanced Key Usage字段下有Server Authentication。

在证书的**Details**选项卡下,选择**Subject**和**Subject Alternative Name**,此时会显示FQDN win2016.example.com。

🙀 Certif	ficate				×
General	Details	Certification Pa	1th		
Show:	<al></al>		~		
Field			Value		^
<u>詞</u> Sut	bject		win2016.examp	le.com	
📋 Put	blic key		RSA (2048 Bits)		
Put	blic key pa	arameters	05 00		
Ce	rtificate T	emplate Name	DomainControlle	r	
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	¢

🙀 Certi	ficate			×		
General	Details	Certification Path				
Show:	<al></al>		~			
Field Sul Au Au Au Au Au Au Au	bject Key thority Ke I. Distribu thority In	Identifier y Identifier tion Points formation Access	Value 30 b7 2b 4e 48 0f 2f 17 17 e6 KeyID=3d 9f 26 37 fb 11 1f 4 [1]CRL Distribution Point: Distr [1]Authority Info Access: Acc	^		
Ke Th Th	y Usage umbprint	slgorithm	Other Name:DS Object Guid = Digital Signature, Key Encipher sha1 ca.8e 11 3d eb bc 0f 6e 4a.00	*		
Other M DS (18 DNS Na	Other Name: DS Object Guid=04 10 90 99 a9 a2 38 24 65 47 84 74 64 26 cd c6 80 18 ONS Name =win2016.example.com					
		Ed	It Properties Copy to File			
			0	ĸ		

在Enhanced Key Usage下,存在Server Authentication。

🙀 Certi	ficate			×
General	Details	Certification Path		
Show:	<al></al>		\sim	
Field			Value	^
E Su E Pu Pu	bject blic key blic key pa	arameters	win2016.example.com RSA (2048 Bits) 05 00	
En Ce	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,在Certification Path选项卡下,选择作为根CA证书的顶级证书,然后单击View Certificate。

💼 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。

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

在**详细信息**选项卡下,单击**复制到文件……**

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	

10.通过以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 Cance	

选择Base-64**编码**X.509

Export File Certif	Format icates can be exported in a variety of file formats.
Select	t the format you want to use:
0	DER encoded binary X.509 (.CER)
C	Base-64 encoded X.509 (.CER)
C) Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)
	Include all certificates in the certification path if possible
0	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
0) Microsoft Serialized Certificate Store (.SST)

选择文件的名称以及导出文件的位置。

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	

现在单击Finish。

÷	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 Cano	el:

11.现在转到该位置并使用记事本或其他文本编辑器打开证书。这显示PEM格式证书。请保存以备后 用。

----BEGIN CERTIFICATE----

```
MIIDCDCCAfCgAwIBAgIQE4ZG5Z1wT6lONTjooEQyMTANBgkqhkiG9w0BAQsFADAd
MRswGQYDVQQDExjleGFtcGxlLVdJTjIwMTYtQ0EwIBcNMjAwNDI3MTQ1MDU5WhgP
MjA2MDA0MTkxNDUwNTlaMB0xGzAZBgNVBAMTEmV4YW1wbGUtV010MjAxNi1DQTCC
ASIwDQYJKoZIhvcNAQEBBQADqqEPADCCAQoCqqEBAI8qhT719NzSQpoQPh0YT67b
Ya+PnqsxMyvkewP33QLTAWw1HW1Tb9Mk5BDW0ItTaVsqHwPBfd++M+bLn3AiZnHV
OO+k6dVVY/E5qVkEKSGoY+v940S2316lzdwReMOFhgbc2qMertIoficrRhihonuU
Cjyeub3CO+meJUuKom2R47C0D35TUvo/FEHGgXJFaJS1se2UrpNO7KEMkfAlLPuM
aob4XE/OzxYQpPa18djsNnskfcFqD/HOTFQN4+SrOhHWlRnUIQBUaLdQaabhipD/
sVs5PneYJX8YKma821uYI6j90YuytmsHBtCieyC062a8BKqOL7N86HFPFkMA3u8C
\texttt{AwEAAaNCMEAwDgYDVR0PAQH/BAQDAgGGMA8GA1UdEwEB/wQFMAMBAf8wHQYDVR0O}
BBYEFD2fjjf7ER9EM/HCxCVFN5QzqEdvMA0GCSqGSIb3DQEBCwUAA4IBAQB31ZJo
vzwVD3c5Q1nrNP+6Mq62OFpYH91k4Ch9S5g/CEOemhcwg8MDIoxW2dTsjenAEt7r
phFIHZoCoSyjBjMgK3xybmoSeg8vBjCXseYNGEmOc9KW1oFmTOvdNVIb7Xpl1IVa
6tALTt3ANRNgREtxPA6yQbthKGavW0Anfsojk9IcDr2vp0MTjlBCxsTscbubRl+D
dLEFKQqmMeYvkVf+a7a64mqPZsG3Uxo0rd6cZxAPkq/ylcdwNSJFfQV3DqZq+R96
9WLCR3Obig6xyo9Zu+lixcWpdrbADO6zMhbEYEhkhOOjBrUEBBI6Cy83iTZ9ejsk
KgwBJXEu33PplW6E
```

----END CERTIFICATE-----

12.(可选)如果LDAPS可以使用多个身份证书,并且使用哪个身份证书存在不确定性,或者无法 访问LDAPS服务器,则可以从在Windows服务器或FTD之后完成的数据包捕获中提取根ca。

FMC配置

要部署AnyConnect配置,FTD需要注册到智能许可服务器,并且必须将有效的Plus、Apex或仅 VPN许可证应用到设备。

1.导航到**系统>许可证>智能许可**。

Overview	Analysis	Policies	Devices	Objects	AMP	Intelligence					Deplo	y 🛛 🔒 🧧	system	Help 🔻	admin 🔻
						Configuration	Users	Domains	Integration	Updates	Licenses *	Health 🔻	Mon	itoring 🔻	Tools v
										Sm	art Licenses				

2.确认设备符合要求并成功注册。确保设备已注册到AnyConnect Apex、Plus或仅VPN许可证。

verview Analysis Policies	De	vices Objects	AMP	Intelligence					(Deploy 0	System	ielp v admin
			Configuration	n Users	Domain	s Integratio	on Updates	Lk	censes + Smart Lice	nses Heal	th • Monit	oring • Too
Smart License Status					Ciaco	Smart Software	Manager 🛛 🔴	9				
Usage Authorization:	۲	Authorized (Last S	ynchronized O	0n May 03 2020)							
Product Registration:	0	Registered (Last R	enewed On Ma	ar 03 2020)								
Assigned Virtual Account:		SEC TAC										
Export-Controlled Features:		Enabled										
Cisco Success Network:		Disabled										
Cisco Support Diagnostics:		Disabled 🕕										
Smart Licenses									Filter Devices		×	Edit Licenses
License Type/Device Name					License	Status	Device Type	•		Domain	Gro	up
Firepower Management 0	Cent	ter Virtual (2)			0							
🖻 📁 Base (2)					0							
🖻 🟳 Mahware (1)					0							
🖻 📁 Threat (2)					0							
🖻 🟳 URL Filtering (2)					0							
🖌 🥬 AnyConnect Apex (1)					0							
FTD-2 192.168.1.17 · Cisco Firepo	wer '	Threat Defense for \	/MWare - v6.3		0		Cisco Firepov	ver Three	at Defense for VMWare	Global	N/A	
AnyConnect Plus (0)												
AnyConnect VPN Only (0)												

设置领域

1.定位至**系统>集成**。

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

2.在**领域**下,单击**新建领域**。

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

3.根据从Microsoft服务器收集的信息填写相应字段。完成后,单击OK。

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

4.在新窗口中,选择Directory(如果尚未选择),然后单击Add directory。

Overview	Analysis	Policies	Devices	Objects	AMP	Intellige	nce			Deploy	🖉 🔍 Sys	tem Help 🔻	admin v
				Configu	ration	Users	Domains	Integration	Updates	Licenses 🔻	Health 🔻	Monitoring •	Tools •
LAB-AD Enter Descript	ion											Save 🛛	Cancel
Directory	Realm Con	figuration	User Down	hload									
												0 A	idd directory

填写AD服务器的详细信息。请注意,如果使用FQDN,则除非将DNS配置为解析FQDN,否则 FMC和FTD无法成功绑定。

要设置FMC的DNS,请导航到System > Configuration,然后选择Management Interfaces。

要设置FTD的DNS,请导航到**Devices > Platform Settings**,创建新策略,或编辑当前策略,然后转 到DNS。

Add directory		? ×
Hostname / IP Address	win2016.example.com	
Port	389	
Encryption	○ STARTTLS ○ LDAPS	
SSL Certificate	 O 	
	OK Test	Cancel

如果使用LDAPS或STARTTLS,请单击绿色+符号,为证书指定一个名称,然后复制PEM格式的根 CA证书。完成后单击**Save**。

Import Trusted Certificate Authority	? ×
Name: LDAPS_ROOT	
Certificate Data or, choose a file: Browse	
 BEGIN CERTIFICATE MIIDCDCCAfCgAwIBAgIQE4ZG5Z1wT6lONTjooEQyMTANBgkqhkiG9w0BAQsFADAd MRswGQYDVQQDEXJleGFtcGxlLVdJTjIwMTYtQ0EwIBcNMjAwNDI3MTQ1MDU5WhgP MjA2MDA0MTkxNDUwNTlaMB0xGzAZBgNVBAMTEmV4YW1wbGUtV0lOMjAxNi1DQTCC ASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAI8ghT719NzSQpoQPh0YT67b Ya+PngsxMyvkewP33QLTAWw1HW1Tb9Mk5BDWOITTaVsgHwPBfd++M+bLn3AiZnHV OO+k6dVVY/E5qVkEKSGoY+v940S2316lzdwReMOFhgbc2qMertIoficrRhihonuU Cjyeub3CO+meJUuKom2R47C0D35TUvo/FEHGgXJFaJS1se2UrpNO7KEMkfA1LPuM aob4XE/OzxYQpPa18djsNnskfcFqD/HOTFQN4+SrOhHWIRnUIQBUaLdQaabhipD/ sVs5PneYJX8YKma821uYI6j90YuytmsHBtCieyC062a8BKqOL7N86HFPFkMA3u8C AwEAAaNCMEAwDgYDVR0PAQH/BAQDAgGGMA8GA1UdEwEB/wQFMAMBAf8wHQYDVR0O BBYEFD2f1jf7ER9EM/HCxCVFNSQzqEdvMA0GCSqGSID3DQEBCwUAA4IBAQB31ZJo vzwVD3c5Q1nrNP+6Mq62OFpYH91k4Ch9S5g/CEOemhcwg8MDIoxW2dTsjenAEt7r phFIHZoCoSyjBjMgK3xybmoSeg8vBjCXseYNGEmOc9KW10FmTOvdNVIb7Xpl1IVa 6tALTt3ANRNgREbxPA6yQbthKGavW0Anfsojk91CDr2vp0MTjlBCxSTscbuBRI+D dLEFKQqmMeYvkVf+a7a64mqPZsG3Uxo0rd6cZxAPkq/ylcdwNSJFfQV3DgZg+R96 9WLCR3Obig6xyo9Zu+lixcWpdrbADO6zMhbEYEhkhOOjBrUEBBI6Cy83iTZ9ejsk KgwBJXEu33PpIW6E END CERTIFICATE 	
Save	Cancel

从SSL Certificate旁边的下拉列表中选择新添加的根CA,然后点击STARTTLS或LDAPS。

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

点击Test以确保FMC能够成功绑定上一步中提供的目录用户名和密码。

由于这些测试是从FMC启动的,而不是通过FTD上配置的某个可路由接口(例如内部、外部和 dmz)启动,因此成功(或失败)的连接不能保证AnyConnect身份验证的相同结果,因为 AnyConnect LDAP身份验证请求是从FTD可路由接口之一启动的。 有关从FTD测试LDAP连接的详细信息,请查看Troubleshooting区域中的Test AAA and Packet Capture部分。



5.在User Download下,下载后续步骤中用于用户身份的组。

选中**Download users and groups**复选框,Available Groups列将使用Active Directory中配置的组进 行填充。

组可以包括(Included)或排除(Excluded),但默认情况下包括组DN下找到的所有组。

也可以包括或排除特定用户。任何包含的组和用户都可以在以后选择用于用户身份。

完成后,单击 Save (保存)。

Overview Analysis Policies Devices Object	s AMP In	telligence					Deplo	🕘 🕘 Sy	stem Help 🔻	admin 🔻
		Configuration	Users	Domains	Integration	Upda	ates Licenses •	Health *	Monitoring •	Tools *
LAB-AD Enter Description							You have un	saved change	s 🔚 Save	Cancel
Directory Realm Configuration User Download										
Download users and groups Begin automatic download at 8 PM America/New Lownload New	York Repeat Ev	ery 24 Y Hours								
Available Groups 😋		Groups to In	idude (2)				Groups to Exclude (0)		
Search by name		💣 AnyConn	ect Admina			8	None			
AnyConnect Admins DnsUpdateProxy WsekemoteAccessUsers WselawisbleTeDashboard Allowed RODC Password Replication Group Enterprise Key Admins Domain Admins WseAlertAdministrators WseAlertAdministrators Replicator Domain Guests Windows Authorization Access Group Account Operators	Add to Include Add to Exclude	<i>∯</i> AnyCorn	ect Users			8				
Phyper-V Administrators System Managed Accounts Group	~	Enter User In	dusion			Add	Enter User Exclusion			Add

6.启用新领域。

Overview Analysis Policie	es Devices Object	S AMP In	itelligence						Deploy	0 ₄ Sys	tem Hel	p v admin v
			Configura	ation Us	sers D	Domains	Integratio	n Updates L	icenses 🔻	Health *	Monitoria	ng ▼ Tools ▼
Cloud Services Realms	Identity Sources	eStreamer	Host Inpu	rt Client	Smart S	Software Se	stellite					
										Comp	are realms	🔕 New realm
Name	Description	Domain		Туре	Base	e DN	Gro	oup DN	Group Attri	bute	State	
LAB-AD		Global		AD	DC-4	example,DC=	com DC-	-example,DC-com	member			ታ 🥒 🕤 🖯

7.如果使用LDAPS或STARTTLS,则根CA也需要由FTD信任。为此,请首先导航到**设备>证书**。

Overview Analysis	Polic	ies Dev	ices	Objects	AMP	Intelligence		Deploy	e ₅	System	Help 🔻	admin 🔻
Device Management	NAT	VPN V	QoS	Platform	m Settings	s FlexConfig	Certificates					

点击右上角的Add。

Overview Anal	ysis	Policies	Dev	ices	Objects	AMP	Intellige	ence			Deploy	e,	System	Help 🔻	admin v
Device Manageme	nt	NAT	VPN •	QoS	Platform	Settings	s Flex	xConfig	Certificates						
														0	Add

选择FTD,将LDAP配置添加到中,然后点击绿色+符号。

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

为信任点指定**Name**,然后从**Enrollment Type**下拉列表中选择**Manual enrollment**。将PEM根ca证书 粘贴到此处,然后单击**Save**。

Add Cert Enrollment

Name*	LDAPS_ROOT	
Description		
CA Information	Certificate Parameters Key Revocation	
Enrollment Type:	Manual	^
CA Certificate:*	MIIDCDCCAfCgAwIBAgIQE4ZG5Z1wT6lONTjooEQyMTANBgkqhki G9w0BAQsFADAd MRswGQYDVQQDExJleGFtcGxlLVdJTjIwMTYtQ0EwIBcNMjAwNDI 3MTQ1MDU5WhgP MJA2MDA0MTkxNDUwNTlaMB0xGzAZBgNVBAMTEmV4YW1wbGU tV0lOMjAxNi1DQTCC ASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAI8ghT719N zSQpoQPh0YT67b Ya+PngsxMyvkewP33QLTAWw1HW1Tb9Mk5BDWOItTaVsgHwPBf d++M+bLn3AiZnHV OO+k6dVVY/E5qVkEKSGoY+v940S2316lzdwReMOFhgbc2qMertIo ficrRhihonuU Cjyeub3CO+meJUuKom2R47C0D35TUvo/FEHGgXJFaJS1se2UrpN O7KEMkfA1LPuM aoh4YE/QzyYOnPa18disNoskfcEnD/HOTEON4+SrOhHWIRpI JIOBU	
	aLdQaabhipD/ sVs5PneYJX8YKma821uYI6j90YuytmsHBtCieyC062a8BKqOL7N86	~
Allow Overrides		
	Save	Cancel

确认已选择创建的信任点,然后单击Add。

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

? X

新的信任点显示在FTD下。虽然它提到需要导入身份证书,但并不要求FTD能够对LDAPS服务器发送的SSL证书进行身份验证,因此可以忽略此消息。

Overview Analysis	Policies Devices Obje	cts AMP Intell	ligence	Deploy 🔍 System	n Help v admin v
Device Management	NAT VPN VQoS PI	atform Settings F	FlexConfig Certificates		
					🔕 Add
Name	Domain	Enrollment Type	Status		
4 🗐 FTD-1					
FTD-1-PKCS12	Global	PKCS12 file	CA 🔍 D		P 🗘 🗐
4 🗐 FTD-2					
FTD-2-PKCS12	Global	PKCS12 file	a,ca 🔍 🖂		£¢ 🛙
FTD-2-Selfsigned	Global	Self-Signed	S CA 🔍 ID		🕜 ¢ 🗎
LDAPS_ROOT	Global	Manual	🔍 CA 🔺 🛆 Ide	ntity certificate import required	i?¢≣

配置AnyConnect进行AD身份验证

1.这些步骤假设尚未创建远程访问vpn策略。如果已创建策略,请点击该策略的edit按钮,并跳至步 骤3。

导航到设备> VPN >远程访问。



单击Add创建新的远程访问VPN策略

Overview /	Analysis	Policies	Devices	Objects	AMP	Intelligence				Deploy	e , s	iystem	Help 🔻	admin v
Device Manag	gement	NAT	VPN • Remot	te Access	QoS	Platform Settings	FlexConfig	Certificates						
													0	Add
Name						Status		L	ast Modified					

No configuration available Add a new configuration

2.完成远程访问VPN策略向导。在Policy Assignment下,指定策略名称和应用该策略的设备。

Overview Analys	is Policies De	vices Objects AMP	Intelligence				Deploy 🔒 Sy	stem Help v	admin v
Device Management	NAT VPN	Remote Access QoS	Platform Settings	FlexConfig	Certificates				
Remote Access	VPN Policy V	Wizard							
1 Policy Assignm	nent 🛛 📀 G	onnection Profile > 3	AnyConnect >	Access &	Certificate >	S Summary			
	Targeted Devic	es and Protocols	nal stars to configure	the Demote Access	www.eefer.with	Refere You	Chart		~
	a new user-defined	connection profile.	nai steps to compure	the Remote Access	a were poincy with	Before you star	t, ensure the following		
	Name:*	PTD-2-RA-Policy				complete Remote	Access VPN Policy.		
	Description:				$\hat{}$	Configure <u>Realm</u> to authenticate V	or <u>RADIUS Server Group</u> PN dients.		
	VPN Protocols:	SSL IPsec-IKEv2				AnyConnect Clie	ent Package		
	Targeted Devices:	Available Devices	-	Selected Device	s A	Nake sure you h for VPN Client d the relevant Cisc	ave AnyConnect package lownloaded or you have credentials to download		
		ETD-1	-		3	it during the wize	rd.		
		PTD-2				Device Interfac	e		
						Interfaces should targeted <u>devices</u> as a security zo enable VPN acces	be already configured on so that they can be used ne or interface group to a.		
			Add						
									~
							Back	ext Car	icel

在**Connection Profile**下,指定**Connection Profile**的名称,该名称也用作AnyConnect用户在连接时 看到的组别名。

指定以前在Authentication Server下创建的领域。

指定为AnyConnect客户端分配IP地址的方法。

指定用于此连接配置文件的默认组策略。

Overview Analysis Policies Devices Objects AMP	Intelligence		Deploy 0	System	Help 🔻	admin v
Device Management NAT VPN • Remote Access QoS	Platform Settings FlexConfig	Certificates				
Remote Access VPN Policy Wizard						
Policy Assignment O Connection Profile 3	AnyConnect > ④ Access &	Certificate S Summary				
Connection Profile;						~
Connection Profiles specify the tunne accomplished and how addresses are	I group policies for a VPN connection. The assigned. They also include user attribute	se policies pertain to creating the tunnel itself, ho es, which are defined in group policies.	w AAA is			
Connection Profile Name:*	General					
	This name is configured as a connection all	as, it can be used to connect to the VIN gateway				
Authentication, Authorization & A Specify the method of authentication	ccounting (AAA): (AAA, certificates or both), and the AAA :	servers that will be used for VPN connections.				
Authentication Nethod:	AAA Only 👻					
Authentication Server:*	LAB-AD 👻	G - (Realm or RADIUS)				
Authorization Server:	×	(RADIUS)				
Accounting Server:	×	(RADIUS)				
Client Address Assignment: Client IP address can be assigned fro assignment is tried in the order of A/	m AAA server, DHCP server and IP addres A server, DHCP server and IP address po	is pools. When multiple options are selected, 1P a ol.	iddress			
Use AAA Server (RADUS)	aniy) 🕕					
Use IP Address Pools						
IPv4 Address Pools:	AnyConnect-Pool	1				
IPv6 Address Pools:		1				
Group Policy:						
A group policy is a collection of user- or create a Group Policy object.	oriented session attributes which are assi	gned to client when a VPN connection is establish	ed. Select			
Group Policy:*	DfltGrpPolicy ¥	a				
	Edit Group Policy					~
			Dark (Maut		Incol
			Dack	next	0	sincer

在AnyConnect下,上传并指定使用的AnyConnect软件包。



在Access & Certificate下,指定AnyConnect用户为AnyConnect访问的接口。

创建和/或指定FTD在SSL握手期间使用的证书。

确保取消选中解密流量的**旁路访问控制策略**(sysopt permit-vpn)复选框,以便稍后创建的用户身份对 RAVPN连接生效。

Overview Analysis Policies Devices Objects AMP Intelligence			Deploy 🧕 🍳	System	Help 🔻	admin v
Device Management NAT VPN > Remote Access QoS Platform Setting	s FlexConfig Certificates	1				
Remote Access VPN Policy Wizard						
1 Policy Assignment > 2 Connection Profile > 3 AnyConnect	Access & Certificate	5 Summary				
Network Interface for Incoming VPN A Select or create an Interface Group or a Security connections.	ccess Zone that contains the network in	terfaces users wil access for VPN				-
Interface group/Security Zone:" outside-zo	ne 🗡 😋-					
I Erable	DTLS on member interfaces					
Device Certificates Device certificate (also called Identity certificate) certificate which is used to authenticate the VPN	identifies the VPN gateway to the gateway.	remote access clients. Select a				
Certificate Enrollment:* FTD-2-Se	fsigned 💌 🔇					
Internet to	he selected certificate object on the	target devices				
Access Control for VPN Traffic All decrypted traffic in the VPN tunnel is subject bypass decrypted traffic from the Access Control	d to the Access Control Policy by d Policy.	efault. Select this option to				
Bypass Access Control policy for decrypted to This option bypasses the Access Control Policy AAA server are attil applied to V79V traffic.	effic (sysopt permit-vpn) inspection, but VPN filter ACL and au	thorization ACL downloaded from				
			Back	Next	Ca	ancel

在Summary下,查看配置,然后单击Finish。



3.在远程访问VPN策略下,点击编辑以获取相应的连接配置文件。

Overview Analysis Policies Devices Objects	AMP Intelligence	Deploy 🔍 System Help 🔻 admin 🔻
Device Management NAT VPN • Remote Access	QoS Platform Settings FlexConfig Certificates	
FTD-2-RA-Policy Enter Description		Save Save
Connection Profile Access Interfaces Advanced		🧧 Policy Assignments (1)
		G
Name	AAA (Sroup Policy
DefaultWEBVPNGroup	Authentication: None E Authorization: None Accounting: None	🛓 DfkGrpPolicy 🥜 🗓
General	Authentication: LAB-AD (AD) Authorization: 1000 Accounting: 1000	2 DftkGrpPviloy

确保身份验证服务器设置为之前创建的领域。

在Advanced Settings下,可以选中Enable Password Management以允许用户在其密码到期时或到 期之前更改其密码。

但是,此设置要求领域使用LDAPS。如果进行了任何更改,请单击Save。

Edit Connection Pr	ofile		? ×
Connection Profile:* Group Policy:* Client Address Assign	General DfltGrpPolicy Edit Group Po ment AA	/ V 3 licy A Aliases	
Authentication			
Authentication Meth	od:	AAA Only 👻	
Authentication Serve	er:	LAB-AD (AD)	
Use secondary au Authorization	uthentication		
Accounting	•	Allow connection only if user exists in authorization database	
Accounting Server:		×	
Advanced Setting	gs username		
Strip Group from	username		
Enable Password Notify User Notify user on the second secon	Management days prio	r to password expiration rord expiration	
		Save Cance	I)

完成后,点击右上角的Save。



启用身份策略并配置用户身份的安全策略

1.导航到**策略>访问控制>身份**。

Overview An	alysis Policies De	vices Objects AMP	Intelligence			Deploy	e,	System	Help 🔻	admin v
Access Control •	Network Discover	Y Application Detectors	Correlation	Actions v						
Access Control										
Intrusion										
Malware & File										
DNS										
Identity										
SSL										
Prefilter										

创建新的身份策略。

Overview Analysis Policies Devices Objects A	MP Intelligence	Deploy 🔒 Sy	rstem Help ▼ admin ▼
Access Control > Identity Network Discovery Application	on Detectors Correlation Actions •		
		Object	Management Access Control
		(K Comp	are Policies 🔍 New Policy
Identity Policy	Domain	Status	Last Modified
	Theorem 1997	and add a second bar	

There are no policies created. Add a new policy

指定新**身份**策略的**名称**。

Name	FTD-2 Identity Policy	
Description		

2.单击**添加规则**。

C	verview Analysis Poli	icies Device	s Objects	AMP Intellig	jence				De	play 🔒 Sys	tem Help v	admin 🔻
A	ccess Control > Identity	Network Disc	overy Appli	ication Detectors	Correlation	Actions *						
F	TD-2 Identity Poli ter Description	icy									E Save	Cancel
R	Active Authentication											
								Add Category	Add Rule	Search Rules		×
	Name	Source Zo	Dest Zones	Source Net	Dest Netw	VLAN Tags	Source Ports	Dest Ports	Realm	Action	Auth Prot	ocol

3.为新规则指定Name。确保已启用该功能并将操作设置为"被动身份验证"。

单击Realm & Settings选项卡,然后选择之前创建的领域。完成后,单击Add。

ame RAVPN					🖌 Enables	d	Insert	into Category		*	Standard Rules	
tion Passive	Authentication			Realm:	LAB-AD (AD)	Authentication Pr	otocol:	HTTP Basic Ex	clude HTTP	Jser-	Agents: None	
Remote	access VPN sessio	s are acti	vely authent	icated by VPN	. Other session	s use the rule Action	-					
Zones Ne	tworks VLAN	ans P	orts								Realm & S	Setting
		aya .										
ealm *		40 (40)										
the second of the second se		AD (AD)				Y 0						
1	LAG	AD (AD)			15.1.1	<u> </u>						
Use active a	authentication if pa	ssive or VI	PN identity c	annot be esta	blished	<u> </u>						
] Use active a	authentication if pa	ssive or VI	PN identity c	annot be esta	blished	¥ 0/						
) Use active a	authentication if pa	ssive or VI	PN identity c	annot be esta	blished	<u> </u>						
Use active a	authentication if pa	ssive or VI	PN identity c	annot be esta	blished	× 0						
) Use active a	authentication if pa	ssive or VI	PN identity c	annot be esta	blished	V 2						
) Use active a	authentication if pa	ssive or VI	PN identity c	annot be esta	blished							
Use active a	authentication if pa	ssive or VI	PN identity c	annot be esta	blished							
Use active a	authentication if pa	ssive or VI	PN identity c	annot be esta	blished							
Use active a	authentication if pa	ssive or VI	PN identity c	annot be esta	blished							
Use active :	authentication if pa	ssive or VI	PN identity c	annot be esta	blished							
Use active a	authentication if pa	ssive or VI	PN identity c	annot be esta	blished							

4.单击**保存**。

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

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

5.定位至**策略>访问控制>访问控制**。

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

6.编辑FTD**配置在**下的访问控制策略。

Overview Analysis Policies	Devices Objects	AMP Intelligence				Deploy	🛛 🔍 s	iystem	Help 🔻	admin v
Access Control + Access Control	Network Discovery	Application Detectors	Correlation	Actions *						
					Object Management In	trusion Netv	vork Analys	is Policy	DNS Imp	port/Export
									O New	Policy
Access Control Policy		Status			Last Modified					
Default-Policy		Targeting 1 de Up-to-date on	evices all targeted device	5	2020-05-04 09:15:56 Modified by "admin"				G 6	26

7.单击Identity Policy(身份策略)旁边的值。

Overview Analysis Policies	Devices Objects	AMP Intelligence			Deploy 🧕 System Help 🔻 admin 🔻
Access Control > Access Control	Network Discovery	Application Detectors	Correlation	Actions *	
Default-Policy Enter Description					Analyze Hit Counts 🛛 🔠 Save 🛛 😮 Cancel
Prefilter Policy: Default Prefilter Policy		55	& Policy: <u>None</u>		Identity Policy: Rone
					Theritance Settings 📉 Policy Assignments (1)

选择之前创建的Identity Policy,然后单击OK。

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

8.单击**添加规则**以创建新的ACP规则。这些步骤将创建一个规则,允许AnyConnect管理员组中的用 户使用RDP连接到内部网络中的设备。

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

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

指定规则的名称。确保规则已启用并具有相应的操作。

在Zones选项卡下,为相关流量指定适当的区域。

用户发起的RDP流量进入源自外部区域接口的FTD并出口内部区域。

Add Rule							? X
Name AC RDP Access		Enabled	Insert	into Mandatory			
Action 🖌 Allow	▼ ∪ D &	115					
Zones Networks VLAN	N Tags Users Applications	Ports URLs	SGT/ISE Attributes		Inspection	Logging	Comments
Available Zones		Source Zones	: (1)	Destinatio	n Zones (1)		
🔍 side	×	🚑 outside-zo	ne	🗐 🔒 inside	zone		<u>ii</u>
🚠 inside-zone	Add to Source Add to Destination						
						Add	Cancel

在**网络**下,定义源网络和目标网络。

对象AnyConnect_Pool包括分配给AnyConnect客户端的IP地址。

对象Inside_Net包括内部网络子网。

Name Action	AC RDP Access			• • • 8] ⊻ ∈ 1:1	abled		Insert	into Manda	tory		~
Zones	Networks	VLAN Tags	Users	Applications	Ports	URLs	SGT/ISE	Attributes		Inspection	Logging	Comments
Available	eNetworks 🖸		0		Sourc	e Netwo	rks (1)			Destination Networks	(1)	
🔍 Sear	ch by name or value					Source	e	Original (Client	📰 Inside_Net		Ö
•	letworks	Geolocati	on		a a	nyConned	t_Pool		6			
Insid Pv4 Pv4 Pv4 Pv4 Pv4 Pv4 Pv4 Pv4 Pv4 Pv4	e_Net -Benchmark-Tests -Link-Local -Multicast -Private-10.0.0.0-8 -Private-172.16.0.0- -Private-192.168.0.0 -Private-All-RFC1918	-12)-16 3	^ 	Add To Source Networks Add to Destination		- 10 - 4	faces -					
IPv6	-IPv4-Mapped				Enter	an IP ad	dress		Add	Enter an IP address		Add
											Add	Cancel

在Users下,单击Available Realms下之前创建的领域,单击Available Users下相应的组/用户,然后 单击Add to Rule。

如果Available Users部分下没有可用的用户或组,请确保FMC能够下载realm部分下的Users和 Groups,并且包含相应的Groups/User。

从源角度检查此处指定的用**户/组**。

Add Rule

例如,根据此规则到目前为止所定义的内容,FTD评估流量是源自外部区域并发往内部区域,源自 AnyConnect_Pools对象中的网络并发往Inside_Net对象中的网络,而流量源自AnyConnect Admins组中的用户。

Add Rule						? >
Name AC RDP Access	✓ Enabled	Insert	into Mandatory 👻			
Action 🖌 Allow	▼ ∪ D & ± J					
Zones Networks VLAN Tags Users	Applications Ports URLs	SGT/ISE Attributes		Inspection	Logging	Comments
Available Realms 🖸	Available Users 🖸		Selected U	lsers (1)		
🔍 Search by name or value	Search by name or value		🛃 LAB-AI)/AnyConnect	Admins	6
() Special Identities	IAB-AD/*					
🜐 LAB-AD	📣 AnyConnect Admins					
	🝰 AnyConnect Users					
	a it.admin	Ad	dd to Rule			
	test.user					
				_		
					Add	Cancel

在Ports下,创建并添加自定义RDP对象以允许TCP和UDP端口3389。请注意,本可以在 Applications部分下添加RDP,但为简单起见,只检查端口。

Name AC RDP Access		Enabled	Insert into Man	datory 👻	
Action 🖌 Allow	• 00,	3 to 5			
Zones Networks VLAN	Tags Users Applications	Ports URLs SGT/	ISE Attributes	Inspection	Logging Comments
Available Ports 🖸	0	Selected Source Port	ts (0)	Selected Destination F	Ports (2)
Search by name or value		any		RDP-TCP	6
AOL				→ RDP-UDP	6
Je Bittorrent	^				
P DNS_over_TCP	Add to				
DNS_over_UDP	Source				
JP FMC-HTTPS	Add to Destination				
JP FMC-SSH					
J FTD-3-FDM					
JFTD-3-SSH					
J FTP	<u>_</u>				
🥜 НТТР				Protocol TCP (6)	Port Enter a Add
					Add Cancel

? ×

Add Rule

最后,在Logging下,Log at End of Connection会进行检查,以便稍后进行其他验证。完成后单击 Add。

Add Ru	le											? ×
Name	AC RDP Access					Enabled	Ins	ert int	to Mandatory	•		
Action	Allow			• 00,	8 🗠 📕							
Zone	s Networks	VLAN Tags	Users	Applications	Ports	URLs	SGT/ISE Attribute	s		Inspection	Logging	Comments
Log File Ever Send Co Sysk SNM	at Beginning of C at End of Connec hts: Files nnection Events t It Viewer og Server (Using IP Trap Select ar	tion to: default syslog co n SNMP Alert Con	onfiguration.	n in Access Contri 	ol Logging	i) Show O	verrides					
											Add	Cancel

9.为HTTP访问创建了一个附加规则,以允许组**AnyConnect** User**中的用**户访问**Windows Server** IIS网站。Click **Save**.

Overview Analysis Policies Devices Obj	ects AMP Intelligence	Deploy 🔍 System Help 🔻 admin 🖲
Access Control + Access Control Network Disc	very Application Detectors Correlation Actions •	
Default-Policy Enter Description		You have unsaved changes Analyze Hit Counts Save 🕃 Cancel
Prefilter Policy: Default Prefilter Policy	551. Policy: None	Identity Policy: FTD-2 Identity Policy
		Tig Inheritance Settings 🖳 Policy Assignments (1)
Rules Security Intelligence HTTP Responses	Logging Advanced	
B Filter by Device	Show Rule Con	ficta 😣 🔾 Add Category 😋 Add Rule 🗰 Search Rules 🔅 🔅
a Name Source Zo Dest Zones	Source Networks Dest Netwo V., Users	A., S., Dest Ports U., S., D., Action
Mandatory - Default-Policy (1-2)		
1 AC RDP Access Access inside-zone Access	AnyConnect_Pool 🛛 🚍 Inside_Net 🖉 Arc 🍰 LAB-AD/AnyConnect Admins	Any Any 🏂 RDP-TCP - Any Any Any 🗸 Allow 🖯 🗅 🔗 📩 🗐 O 🥒 🗑
2 AC HTTP Access da outside-zone da inside-zone	aryConnect_Pool 😹 Inside_Net 🗛 & LAB-AD/AnyConnect Users	- Any Any PHTTP - Any Any Any VAlow 🛈 🖸 🖻 💿 🥒 🖯
▼ Default - Default-Policy (-)		
There are no rules in this section. Add Rule or Add Category		
Default Action		Access Control: Block All Traffic 🛛 👻 🧧

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

配置NAT免除

如果存在影响AnyConnect流量的NAT规则(如互联网PAT规则),则必须配置NAT免除规则,以使 AnyConnect流量不会受到NAT影响。

1.导航到**设备> NAT**。

Overview Analysis	s Polici	es Dev	ices 0	bjects AMP Int	elligence		Deploy	e,	System	Help 🔻	admin v
Device Management	NAT	VPN •	QoS	Platform Settings	FlexConfig	Certificates					

选择应用于FTD的NAT策略。

Overview Analysis	Policies	Devices	s Obje	ects /	AMP	Intelligence		(t	Deploy	e 5	System	Help 🔻	admin 🔻
Device Management	NAT	VPN V	QoS	Platform	Setting	s FlexConfig	Certificates						
												🔾 New	Policy
NAT Policy						Device Type		Status					
FTD-2-NAT-Policy					Т	hreat Defense		Targeting 1 devices Up-to-date on all targeted	devices			Ф В <mark>.</mark>	/ 6

2.在此NAT策略中,在末尾有一个动态PAT,该PAT会影响从外部接口传出到外部接口的所有流量 (包括AnyConnect流量)。

要防止AnyConnect流量受NAT影响,请点击右上角的Add Rule。

Overview A	nalysis	Policies Devi	ces Objects	AMP	Intelligence			Dep	loy 🔍 🔩	System	Help 🔻	admin 🔻
Device Manage	ment	NAT VPN *	QoS Platfor	m Setting	s FlexConfig	Certificates						
FTD-2-NA	AT-Poli	cy							Show Warning	s 📄	Save [😫 Cancel
Rules										5	Policy As	signments (1)
A Filter by Device											0	Add Rule
					Original Pack	et		Translated Packet				
# Direction	Туре	Source Interface Obje	Destination Interface Object	Original Sources	Original Destinatio	Orig Service	Translated Sources	Translated Destinations	Trans Services	Options		
▼ NAT Rules Befo	re											
 Auto NAT Rules 	;											
÷ +	Dynamic	🍓 any	🚠 outside-zone	👼 obj-an	W.		4 Interface			🝓 Dnsif	false	0
▼ NAT Rules Afte	r											

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

3.配置NAT免除规则,确保该规则是类型为Static的手动NAT规则。这是适用于AnyConnect流量的 双向NAT规则。

使用这些设置,当FTD检测到从Inside_Net发往AnyConnect IP地址(由AnyConnect_Pool定义)的 流量时,源地址将转换为相同的值(Inside_Net),当流量进入inside_zone并离开outside_zone时,目 标地址将转换为相同的值(AnyConnect_Pool)。当满足这些条件时,这基本上会绕过NAT。

Add NAT Rule							? ×
NAT Rule:	Manual NAT Ru	le 🔽	Insert:		In Category	V NAT Rules Before	
Type:	Static		Fnable				
Descriptions			CD Chable				~
Description							\checkmark
Interface Objects	Translation	PAT Pool	Advanced				
Available Interface O	bjects 🖒		Sourc	e Inte	rface Objects (1)	Destination Interface Objects	5 (1)
a, zone		×	🚠 in	side-zo	one 📋	🚠 outside-zone	ii ii
inside-zone			Id to				
atta outside-zone			ource				
		A	dd to tination				
						OK	Cancel
						U.	Concor
Add NAT Rule							? ×
NAT Rule:	Manual NAT Ru	le v	Insert:		In Category	V NAT Rules Before	
Turner	Statio				in outegoiny		
Type:	Static	•	M Enable				
Description:							$\hat{}$
Interface Objects	Translation	PAT Pool	Advanced				
Original Packet				_	Translated Packet		
Original Source:*	Inside_Ne	t	*	0	Translated Source:	Address	*
Original Destination:	Address		~			Inside_Net	v 🔘
	AnyConne	ct Pool	~	0	Translated Destination:	AnyConnect Pool	
Original Source Port:			*	0	Translated Source Port:		¥ ()
Original Destination P	ort:		*	0	Translated Destination Port:		 O
						OK	Cancel

此外,FTD设置为对此流量执行路由查找,而不是代理ARP。完成后单击确定。

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

4.单击**保存**。

0	verview	Analysis	Policies Dev	ices Objects	AMP Inte	elligence				Dej	oloy 🔒	System Help 🔻	admin 🔻
D	evice Manag	ement	NAT VPN *	QoS Platfor	m Settings	FlexConfig	Certificat	es					
F	TD-2-N ter Descriptio	AT-Poli	су						You have un	nsaved changes [🗻	Show Warning	gs 🔚 Save	S Cancel
Ru	iles											📑 Policy A	ssignments (
8	Filter by Device											0	Add Rule
						Original Packs	et			Translated Packet			
*	Direction	Туре	Source Interface Obje	Destination Interface Object	Original Sources	Original Destination	ns	Orig Services	Translated Sources	Translated Destinations	Trans Services	Options	
•	NAT Rules Be	fore											
1	47	Static	🐴 inside-zone	📩 outside-zone	👼 Inside_Net	t 👼 AnyConi	nect_Pool		📰 Inside_Net	👼 AnyConnect_Po	l	🍓 Dns:false 🍓 route-lookup 🍓 no-proxy-arp	J 6
•)	Auto NAT Ruk	es											
#	+	Dynamic	🍓 any	👬 outside-zone	🚌 obj-any				🍓 Interface			🝓 Dns:false	Ø 6
•	NAT Rules Aft	er											

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

部署

1.配置完成后,点击右上角的**Deploy**按钮。



2.点击应用配置的FTD旁边的复选框,然后点击**部署**。

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

Deploy

Cancel

Selected devices: 1

验证

最终配置

AAA配置

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

AnyConnect配置

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

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

http-comp none

activex-relay disable file-entry disable file-browsing disable url-entry 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-simultaneous-logins 10
vpn-tunnel-protocol ikev2 ssl-client
split-tunnel-policy tunnelspecified
split-tunnel-network-list value Lab
user-authentication-idle-timeout none
webvpn
 anyconnect keep-installer none
 anyconnect modules value dart
 anyconnect ask none default anyconnect
```

```
deny-message none
anyconnect ssl df-bit-ignore enable
> show running-config ssl
ssl trust-point FTD-2-SelfSigned outside
使用AnyConnect连接并验证访问控制策略规则
```

🚳 Cisco AnyCo	onnect Secu	ıre Mobili	ty Client	—		\times	
	VPN: Contacting ftd2.exam	ftd2.exam	ple.com.	~ (Connect		
		🕥 Cisc	o AnyConne	ect ftd2.ex	ample.c	om	×
¢ ()							
			Group:	General			~
			Username:	it.admin			
			Password:	******	*		
					ОК		Cancel
🔇 Cisco AnyCo	onnect Secu	ıre Mobili	ty Client	÷		×	
	VPN: Connected	to ftd2.ex	ample.com.				
	ftd2.exam	ple.com		V	isconnect		
00:00:12					I	Pv4	
Ö (i)							

用户IT Admin位于AnyConnect Admins组中,该组具有Windows Server的RDP访问权限,但无权访问HTTP。

打开与此服务器的RDP和Firefox会话将验证此用户只能通过RDP访问服务器。



如果使用AnyConnect Users(作为HTTP访问而不是RDP访问)组中的用户测试用户登录,我们可 以验证访问控制策略规则是否生效。



使用FMC连接事件进行验证

由于访问控制策略规则中启用了日志记录,因此可以检查连接事件中是否存在与这些规则匹配的任 何流量

导航到**分析>连接>事件**。

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

在Table View of Connection Events下,日志被过滤为仅显示IT管理员的连接事件。

在这里,您可以验证是否允许到服务器的RDP流量(TCP和UDP 3389),但端口80流量被阻止。

Ove	rview	Analysi	s Policies I	Devices	Objects	AMP Int	elligence		Dep	loy 🧕 65 System	Help 🔻 admin 🔻	
Cont	ext E	plorer C	onnections + E	vents	Intrusions	▼ Files ▼	Hosts • U	sers • Correlati	on • Advanced •	Search		
								Bookmark Th	is Page Report Design	er Dashboard View B	Bookmarks Search •	
Conn Conn	nne ections	ction Ev	ents (switch)	workflow) le View of	f Connection I	Events			1 20	20-05-05 14:14:17 - 2	020-05-05 16:21:14 O Expanding	
► Search Constraints (Edit Search Save Search) Disabled Columns												
Ju	mp to.											
		Action ×	Initiator × IP	Initiato	<u>r User</u> ×		Responder ×	Ingress × Security Zone	Egress Security Zone	Source Port / × ICMP Type	Destination Port / × ICMP Code	
4		Allow	<u>iii 10.10.10.1</u>	📇 <u>it adn</u>	nin (LAB-AD\it.	admin, LDAP)	<u>192.168.1.1</u>	outside-zone	inside-zone	62473 / tcp	3389 / tcp	
4		Block	10.10.10.1	📇 it adm	nin (LAB-AD\it	admin, LDAP)	<u>192.168.1.1</u>	outside-zone	inside-zone	62474 / tcp	80 (http) / tcp	
4		Block	10.10.10.1	🖳 <u>it adn</u>	nin (LAB-AD\it.	admin, LDAP)	192.168.1.1	outside-zone	inside-zone	62475 / tcp	80 (http) / tcp	
4		Block	10.10.10.1	📇 it. adn	nin (LAB-AD\it.	admin, LDAP)	192.168.1.1	outside-zone	inside-zone	62476 / tcp	80 (http) / tcp	

对于用户Test User,您可以验证到服务器的RDP流量是否被阻止,以及端口80流量是否被允许。

Overvie	w Analysi	s Policies	Devices	Objects	AMP	Intelligence				Deplo	y 🔒	System	Help 🔻	admin 🔻
Context	Explorer C	onnections • I	Events	Intrusions •	r File	es 🔻 Hosts 🔻	Users v	Correlat	tion 💌	Advanced •	Search			
								Bookmark T	his Page	Report Designer	Dashboar	d View Ba	okmarks	Search •
Connectio Connectio Search Jump b	ection Ev ns with Applicat Constraints (Ed	/ents (switch ion Details > Tab it Search Save Sea	workflow) le View of (arch)	Connection E	vents					II 2020	-05-05 14:	14:17 - 20	Disab	16:26:39 ⁽²⁾ Expanding bled Columns
	Action ×	Initiator × IP	Initiator	User X		Responde IP	r × Inc Sec	ress urity Zone	×	ecurity Zone	Source P ICMP Ty	<u>ort/</u> ×	Destin ICMP (ation Port / 3 Code
1	Block	10.10.10.1	📑 test us	ser (LAB-AD\te	st.user, l	LDAP) 192.16	8.1.1 outs	ide-zone	in	side-zone	<u>62493 / t</u>	æ	3389 /	top
4	Allow	10.10.10.1	📇 <u>test us</u>	ser (LAB-AD\te	st.user, l	LDAP) 192.16	8.1.1 outs	ide-zone	in	side-zone	<u>62494 / tr</u>	æ	80 (http	p) / top

故障排除

调试

此调试可以在诊断CLI中运行,以对LDAP身份验证相关问题进行故障排除:debug Idap 255

要排除用户身份访问控制策略问题,可以在云中运行system support firewall-engine-debug,以确 定流量被意外允许或阻止的原因。

正在运行的LDAP调试

```
[53] Session Start
[53] New request Session, context 0x00002bld13f4bbf0, reqType = Authentication
[53] Fiber started
[53] Creating LDAP context with uri=ldap://192.168.1.1:389
[53] Connect to LDAP server: ldap://192.168.1.1:389, status = Successful
[53] supportedLDAPVersion: value = 3
[53] supportedLDAPVersion: value = 2
[53] LDAP server 192.168.1.1 is Active directory
[53] Binding as ftd.admin@example.com
[53] Performing Simple authentication for ftd.admin@example.com to 192.168.1.1
[53] LDAP Search:
        Base DN = [DC=example,DC=com]
        Filter = [sAMAccountName=it.admin]
        Scope = [SUBTREE]
[53] User DN = [CN=IT Admin, CN=Users, DC=example, DC=com]
[53] Talking to Active Directory server 192.168.1.1
[53] Reading password policy for it.admin, dn:CN=IT Admin,CN=Users,DC=example,DC=com
[53] Read bad password count 6
[53] Binding as it.admin
[53] Performing Simple authentication for it.admin to 192.168.1.1
[53] Processing LDAP response for user it.admin
[53] Message (it.admin):
[53] Authentication successful for it.admin to 192.168.1.1
[53] Retrieved User Attributes:
       objectClass: value = top
[53]
[53]
       objectClass: value = person
[53]
      objectClass: value = organizationalPerson
      objectClass: value = user
[53]
[53]
      cn: value = IT Admin
      sn: value = Admin
[53]
      givenName: value = IT
[53]
       distinguishedName: value = CN=IT Admin,CN=Users,DC=example,DC=com
[53]
      instanceType: value = 4
[53]
       whenCreated: value = 20200421025811.0Z
[53]
      whenChanged: value = 20200421204622.0Z
[53]
[53]
      displayName: value = IT Admin
[53]
      uSNCreated: value = 25896
      memberOf: value = CN=AnyConnect Admins,CN=Users,DC=example,DC=com
[53]
       uSNChanged: value = 26119
[53]
[53]
       name: value = IT Admin
[53]
       objectGUID: value = &...J..O..2w...c
       userAccountControl: value = 512
[53]
[53]
      badPwdCount: value = 6
      codePage: value = 0
[53]
       countryCode: value = 0
[53]
      badPasswordTime: value = 132320354378176394
[53]
[53]
       lastLogoff: value = 0
[53]
       lastLogon: value = 0
[53]
      pwdLastSet: value = 132319114917186142
[53]
      primaryGroupID: value = 513
[53]
       objectSid: value = ......{I...;....j...
[53]
       accountExpires: value = 9223372036854775807
      logonCount: value = 0
[53]
[53]
       sAMAccountName: value = it.admin
       sAMAccountType: value = 805306368
[53]
[53]
       userPrincipalName: value = it.admin@example.com
[53]
       objectCategory: value = CN=Person, CN=Schema, CN=Configuration, DC=example, DC=com
[53]
       dSCorePropagationData: value = 1601010100000.0Z
[53]
        lastLogonTimestamp: value = 132319755825875876
[53] Fiber exit Tx=515 bytes Rx=2659 bytes, status=1
```

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正在从LDAP服务器收到响应。
- 如果使用LDAPS或STARTTLS,请确保信任正确的根CA证书,以便SSL握手可以成功完成。
- 检验是否使用了正确的IP地址和端口。如果使用主机名,请验证DNS是否能够将其解析为正确的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和登录密码是否正确配置。这可以在带有**ldp.exe**的AD服务器上进行验 证。要验证某个帐户是否可以使用ldp成功绑定,请执行以下步骤:

1.在AD服务器上,按Win+R并搜索ldp.exe

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

2.在**连接**下,选择**连接……**

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

3.指定服务器的本地主机和适当的端口,然后单击**确定**。

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

4.右列显示指示连接成功的文本。导航到**连接>绑定……**

🔝 Idap://w	in2016.exa	ample.co	om/DC:	example,DC	=com		_		×
Connection	Browse	View	Optio	ns Utilities	Help				
Connec	:t			ld = ldap_op Established	en("localh connectio	ost", 389); n to localhost			^
Bind		Ctrl+B		Retrieving b	ase DSA i	nformation			
Disconr	nect			Getting 1 en Dn: (RootD	tries: SE)				
New		Ctrl+N		configu CN=	rationNami =Configura	ingContext: ition,DC=examp	le,DC=co	om;	
Save				current	Time: 5/1/2	020 4:16:55 PM	Easterr	n Daylight	
Save As	;			Tim defaultN	e; JaminoCon	text: DC=exam	ole.DC=c	:om:	
Exit				dnsHos domain(tName: wi	n2016.example unctionality: 7 =	.com; : (WIN2(016);	
				domain dsServi	-unctionali ceName: C	ty: 7 = (WIN201 CN=NTDS	16);		
				Set	tings,CN=V t-Site-	VIN2016,CN=Se	rvers,Cl	N=Default-	
				Nan con	ne,CN=Site n;	es,CN=Configura	ation,DC	=example,D)C=
				forestFi	unctionality	/: 7 = (WIN2016	5);		
				highest	Committed	USN: 13410;			
				isSynch IdanSer	icatalogRe ironized: T viceName:	ady: TRUE; RUE; : example.com:\	win2016		~

5.选择Simple Bind,然后指定Directory Account Username和Password。Click OK.

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

如果绑定成功,则ldp显示身份验证为**:DOMAIN\username**

🔝 Idap://w	in2016.exa	mple.co	om/DC=ex	ample,DC	=com		_		\times	<
Connection	Browse	View	Options	Utilities	Help					
				1.2. 1.2. 1.2. support Max Max Max Max Max Max Max Max Max Support support support support support support	840.113556 840.113556 840.113556 edLDAPPoli (PercentDir (ReceiveBu (Connection (BatchRetur (DirSyncDu (ResultSetS (ResultSetS (ValRange; eadMemory edLDAPVer edSASLMe IEGO; EXTE	5.1.4.2255; 5.1.4.2256; 5.1.4.2309; icies (20): M SyncReques ffer; InitRec is; MaxConn rnMessages ration; MaxT ize; MinRes PerConn; Max MaxValRan Limit; Syster rsion (2): 3; chanisms (4 RNAL; DIGE _s(Id, 'ftd.ad	axPooIThr sts; MaxDa vTimeout; IdleTime; I s; MaxQue empTable ultSets; axNotifical geTransiti mMemoryL 2; I): GSSAP ST-MD5; Imin@exal min'.	reads; atagramRe MaxPageS ryDuration Size; tionPerCo ve; LimitPerce 1; GSS-	ecv; Size; n; nn; ent;	*
Ready										

尝试使用无效的用户名或密码进行绑定会导致失败,例如此处看到的两个。

🔐 Idap://w	in2016.exa	mple.co	om/DC=ex	ample,DC	=com		—		×
Connection	Browse	View	Options	Utilities	Help				
			r v E S c E ir	Max Max Max Three supporte supporte SPN es = Idap_s unavailable unavailable rror <49>: I server error comment: Ac rror 0x8009 trailed	ResultSetSi (ResultSetsF (ValRange; I eadMemoryL edLDAPVers edSASLMed IEGO; EXTEF simple_bind_ e>); // v.3 ed as: 'EXAM simple_bind_ e>); // v.3 idap_simple_ :: 80090308: cceptSecuri 90308 The to	ze; MinResu PerConn; Ma: MaxValRang imit; System sion (2): 3; 2 thanisms (4) RNAL; DIGES s(Id, 'ftd.adm IPLE\ftd.adm s(Id, 'wrong bind_s() fai LdapErr: DS tyContext er oken supplie	ItSets; xNotificat eTransitiv MemoryL ; : GSSAPI ST-MD5; nin@exar nin@exar nin". @exampl led: Invali SID-0C090 ror, data d to the fi	ionPerConn /e; .imitPercent; ; GSS- nple.com', le.com', d Credentia 042A, 52e, v3839 unction is	is
Ready			ļ						¥

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可以通过FTD完成的搜索找到用户。这也可通过Idp.exe完成。
```

1.成功绑定后(如上所示),导航到视图>树。

🔝 Idap://w	_	· [×						
Connection	Browse	View	/ Option	s Utilities	Help					
		~	Tree Enterprise Status Ba Set Font	e Configurat r	AaxPoolThreads; sts; MaxDatagramRecv; cvTimeout; nldleTime; MaxPageSize; s; MaxQueryDuration;					
				Max Max Max Thre support support SPN	DirSyncl ResultSe ValRang adMemo edLDAP\ edSASLI EGO; EX	Duration; Ma etSize; MinR etsPerConn; je; MaxValR oryLimit; Sys /ersion (2): Mechanisms (TERNAL; D	axTempTa ResultSets ; MaxNoti RangeTra stemMem 3; 2; s (4): GSS IGEST-MI	ableSize; s; ficationP nsitive; oryLimitP SAPI; GS D5;	erConn Percent; S-	;
 res = ldap_simple_bind_s(ld, 'ftd.admin@example.com <unavailable>); // v.3 Authenticated as: 'EXAMPLE\ftd.admin'. </unavailable>								.com',	~	

2.指定在FTD上配置的基本DN,然后点击**确定**

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

3.右键单击基础DN,然后单击**Search**。

Idap://win2016.example.com/DC=example,DC=com - 🛛								
Connection Browse	View	Options	Utilities	Help				
DC= example, DC= 0	com	Search Virtual L Delete Modify Modify Add chil Compar Advance Copy DN Copy Select al Clear ou	ist View DN Id ee ed N	Ctrl+S Ctrl+D Ctrl+M Ctrl+R Ctrl+A > Ctrl+C Ctrl+C	cipals,DC=example,DC=com; 11D2B9AA00C04F79F805:CN =example,DC=com; E11D297C400C04FD8D5CD: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; 311D1ADED00C04FD8D5CD:C e,DC=com; 0 3:43:59 PM Eastern Daylight 2:41:57 PM Eastern Daylight	~		
Create a new documen	t							

4.指定与调试中看到的相同Base DB、Filter和Scope值。

在本例中,包括:

- 基础DN:dc=example,dc=com
- 过滤器:samaccountname=it.admi
- •范围:子树

🟠 Idap://w	n2016.example.com/DC=example,DC=com	– 🗆 X
Connection	Browse View Options Utilities Help	
Search	×	C=example,DC=com; \$8811D1ADED00C04FD8D5CD: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; \$8811D1ADED00C04FD8D5CD:C =example,DC=com;
Attributes:	objectClass;name;description;canonicalName \sim	68811D1ADED00C04FD8D5CD:C mple,DC=com;
Options	Run Close	2020 3:43:59 PM Eastern Daylight 20 2:41:57 PM Eastern Daylight
	 ***Searching Idap_search_s(Id, "DC= "sAMAccountName=it.a Getting 0 entries:	=example,DC=com", 2, admi", attrList, 0, &msg)
Ready		

ldp发现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

使用正确的samaccountname **it.admin**进行的另一次尝试显示不同的结果。ldp在Base DN dc=example,dc=com下找到1个条目,并打印该用户DN。

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

用户名密码不正确

```
[-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
```

[-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 潜在解决方案:验证用户密码配置正确且未过期。与登录DN类似,FTD使用用户凭证对AD执行绑

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中的步骤在**绑定** 登录DN和/或密码不正确部分中显示。

此外,还可以查看Microsoft**服务器**事件查看器日志的潜在原因。

测试AAA

定。

test **aaa-server**命令可用于使用特定用户名和密码模拟从FTD进行的身份验证尝试。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与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 明存在路由问题。

捕获显示双向LDAP流量。

```
> show route 192.168.1.1
Routing entry for 192.168.1.0 255.255.255.0
Known via "connected", distance 0, metric 0 (connected, via interface)
Routing Descriptor Blocks:
 * directly connected, via inside
        Route metric is 0, traffic share count is 1
> capture AD interface inside match tcp any host 192.168.1.1 eq 389
> show capture
capture AD type raw-data interface inside [Capturing - 0 bytes]
```

> 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> 2: 23:02:16.772009 192.168.1.1.389 > 192.168.1.17.61960: S 491521506:491521506(0) ack 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> 192.168.1.1.389 > 192.168.1.17.61960: P 491521507:491522141(634) ack 5: 23:02:16.772924 3681912980 win 65160 <nop,nop,timestamp 762393885 1061373059> 192.168.1.17.61960 > 192.168.1.1.389: . ack 491522141 win 32768 6: 23:02:16.772955 <nop,nop,timestamp 1061373059 762393885> 192.168.1.17.61960 > 192.168.1.1.389: P 3681912980:3681913024(44) 7: 23:02:16.773428 ack 491522141 win 32768 <nop,nop,timestamp 1061373060 0> 8: 23:02:16.775030 192.168.1.1.389 > 192.168.1.17.61960: P 491522141:491522163(22) ack 3681913024 win 65116 <nop,nop,timestamp 762393887 1061373060> 9: 23:02:16.775075 192.168.1.17.61960 > 192.168.1.1.389: . ack 491522163 win 32768 <nop,nop,timestamp 1061373061 762393887> [...] 54 packets shown

Windows Server事件查看器日志

match tcp any host 192.168.1.1 eq ldap

AD服务器上的Event Viewer日志可以提供有关失败原因的更详细信息。

1.搜索并打开"事件查看器"。

=	Best ma	Best match											
ŵ	Event Viewer Desktop app												
	Setting	s					>						
	曫 Vi	ew ever	nt logs										
۲	10	۲	ß		53	□	រុក						
	event												
	Q	([])	e		1	2	8						

2.展开Windows Logs,然后单击Security。使用用户帐户名称搜索Audit Failures,然后查看失败信 息。



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

关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言,希望全球的用户都能通过各 自的语言得到支持性的内容。

请注意:即使是最好的机器翻译,其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任,并建议您总是参考英文原始文档(已提供 链接)。