在FMC管理的FTD上使用RA VPN的LDAP配置密 码管理

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 确定LDAP基本DN和组DN 复制LDAPS SSL证书根 在LDAP服务器上的本地计算机存储中安装多个证书的情况下(可选) FMC配置 验证许可 设置领域 配置AnyConnect进行密码管理 部署 最终配置 AAA配置 AnyConnect配置 确认 使用AnyConnect连接并验证用户连接的密码管理过程 故障排除 调试 工作密码管理调试 密码管理过程中遇到的常见错误

简介

本文档介绍如何使用LDAP为连接到思科Firepower威胁防御(FTD)的AnyConnect客户端配置密码管理。

先决条件

要求

Cisco 建议您具有以下主题的基础知识:

- 基本了解FMC上的RA VPN(远程访问虚拟专用网络)配置
- 基本了解FMC上的LDAP服务器配置

• Active Directory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 2012 R2服务器
- 运行7.3.0的FMCv
- 运行7.3.0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



Windows服务器预配置了ADDS和ADCS以测试用户密码管理过程。在本配置指南中,将创建这些 用户帐户。

用户帐户:

- 管理员:此帐户用作目录帐户,以允许FTD绑定到Active Directory服务器。
- admin:用于演示用户身份的测试管理员帐户。

确定LDAP基本DN和组DN

1. Open(未解决) Active Directory Users and Computers 通过服务器管理器控制面板。

Server Ma	anager • Dashboard				CO Manage Tools View Help Active Directory Administrative Center
		Active Directory Domains and Trusts			
III Dashboard	WELCOME TO SERVER MANAGER	Active Directory Module for Windows PowerShell			
Local Server		Active Directory Sites and Services			
All Servers	Carl	in we this least service			Active Directory Users and Computers
HE AD CS	Cont	igure this local server			AD FS Management
III AD DS	QUICK START				ADSI Edit
10 000 S	2 Ad	d roles and features			Certification Authority
AD PS			Component Services		
DNS	3 Ad	Computer Management			
■ File and Storage Services ▷	WHAT'S NEW	Defragment and Optimize Drives			
ED IIS	4 Cre	eate a server group			DNS
P NAP					Group Policy Management
					Group Policy Management
	LEARN MORE				Internet Information Services (IIS) Manager
					iSCSI Initiator
					Local Security Policy
	ROLES AND SERVER GROUPS	1			Network Policy Server
	Roles: 7 Server groups: 1 Servers total				ODBC Data Sources (32-bit)
	R AD CS 1			DNS 1 File .	ODBC Data Sources (64-bit)
	8 10 00			Serv	Performance Monitor
	Manageability	Manageability	Manageability	Manageability ① Mana	Resource Monitor
	Events	Events	Events	Events Event	Security Configuration Wizard
	Services	Services	Consister	Sanisar Sani	Services
	Services	Services	Services	Services Servi	System Configuration
	Performance	Performance	Performance	Performance Perfo	System Information
	BPA results	BPA results	BPA results	BPA results BPA r	Task Scheduler
					Windows Firewall with Advanced Security
					Windows Memory Diagnostic
					Windows PowerShell
					Windows PowerShell (x86)
	😰 IIS 1	NAP 1	Local Server 1	All Servers 1	Windows Powershell ISE Windows DowerShell ISE (v06)
	Manageability	Manageability	Manageability) Manageability	Windows Powersneii isc (xoo) Windows Server Backup
	Events	Events	Events	Events	
	Services	Services	Services	Services	
	Dedemons	0 demonstra	De de services	De de manage	
	Performance	Performance	Performance	Performance	Activate Windows
	BPA results	BPA results	BPA results	BPA results	Go to Action Center to activate Windows.

2. 打开 View Option 并启用 Advanced Features,如图所示:

	Active Directory U	sers and Computers	_ D X			
File Action View	v Help					
🗢 🔿 🖄 [Add/Remove Columns					
Active Dired	Large Icons Small Icons	n				
⊿ 🙀 razor.loc	List	ntainer for up				
▷ 🔛 Built ▷ 🚞 Com 🔍	Detail	ntainer for do				
⊳ 🛅 Dom	Users, Contacts, Groups, and Computers as containers	ntainer for or				
▷ □ Fore ✓ ▷ □ Lost	Advanced Features	ntainer for ma				
⊳ 🚞 Man	Filter Options	tem settings				
▷ Prog ▷ System	Customize	ntainer for up				
Image: System Image: System<						
Displays items in a list						
Displays items in a list	•					

3. 这允许查看AD对象下的其他属性。

例如,要查找根的DN, razor.local右键点击 razor.local,然后选择 Properties,如下图所示:

3	Active Directory Users and Computers	_ 🗆 X
File Action View Help		
(+ +) 2 📰 🗀 🖾 Q 💀 🛛 🖬 🖏 🗞	1 7 D &	
Active Directory Users and Com Name Typ Carlo Saved Queries Builtin built	Description	
Forei Syste Syste TPM Properties Properties Help	 ner Default container for up zational Default container for do ner Default container for sec aFound Default container for ma ner Default location for stor ner Default container for up QuotaC Quota specifications co infor uctureU 	
Opens the properties dialog box for the current selection.		

4. 低于 Properties,选择 Attribute Editor 选项卡。查找 distinguishedName 在Attributes下,单击 View,如图所示.

这将打开一个新窗口,可在其中复制DN并在以后粘贴到FMC。

在本示例中,根DN是 DC=razor, DC=local.复制该值并保存以备后用。点击 OK 要退出"字符串属性编辑器"窗口,请单击 OK 以退出属性。

raz	zor.local Properties ?	x		
General Managed By Ob	oject Security Attribute Editor			
Attributes:				
Attribute	Value	~		
defaultLocalPolicyObj	<not set=""></not>			
description	<not set=""></not>			
desktopProfile	<not set=""></not>	=		
displayName	<not set=""></not>			
displayNamePrintable	<not set=""></not>			
distinguishedName	DC=razor,DC=local			
domainPolicyObject	<not set=""></not>			
domainReplica	<not set=""></not>			
dSASignature	{ V1: Flags = 0x0; LatencySecs = 0; DsaGuid			
dSCorePropagationD	0x0 = ()			
eFSPolicy	<not set=""></not>			
extensionName	<not set=""></not>			
flags	<not set=""></not>			
forceLogoff	(never)	~		
< 111	>			
View	Filter			
Stri	ng Attribute Editor	x		
Attribute: distinguishedName				
Value:				
DC=razor,DC=local				
Clear	OK Cano	el		

复制LDAPS SSL证书根

1. 按 Win+R 并输入 mmc.exe, 然后单击 OK, 如图所示。



2. 导航至 File > Add/Remove Snap-in...,如图所示:

8			Console1 - [Console Root]		_ 🗆 X
🚡 File	Action View Favorites Window	Help			_ 8 ×
	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			
	C:\Windows\system32\dsa				
	3 C:\Windows\system32\certmar				
	4 C:\Windows\system32\certsrv				
	Exit				
Enables	you to add snap-ins to or remove them fr	om the snap	o-in console.		

3. 在可用管理单元下,选择 Certificates 然后单击 Add,如下图所示:

p-in	Vendor	^		Console Root	Edit Extensions.
Active Directory Do	Microsoft Cor				Remove
Active Directory Site	Microsoft Cor				Genere
Active Directory Use	Microsoft Cor				
ActiveX Control	Microsoft Cor				Move Up
ADSI Edit	Microsoft Cor				Move Down
Authorization Manager	Microsoft Cor		<u>A</u> dd >		
Certificate Templates	Microsoft Cor				
Certificates	Microsoft Cor				
Certification Authority	Microsoft Cor				
Computer Managem	Microsoft Cor				
Device Manager	Microsoft Cor				
Disk Management	Microsoft and	~			Ad <u>v</u> anced
intion:					
ipuon.					

4. 选择 Computer account 然后单击 Next,如下图所示:

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>Back</u> <u>N</u> ext > Cancel	

如图所示,单击 Finish.

Select Computer	\times
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: 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. 现在,单击 ок,如图所示。

ap-in	Vendor	^	Console Root	Edit Extensions
Active Directory Do	Microsoft Cor		Lev ^P Certificates (Local Computer)	Remove
Active Directory Site	Microsoft Cor			14
Active Directory Use	Microsoft Cor			Maria M
ActiveX Control	Microsoft Cor			Move Up
ADSI Edit	Microsoft Cor			Move Down
Authorization Manager	Microsoft Cor		<u>A</u> dd >	
Certificate Templates	Microsoft Cor			
Certification Authority	Microsoft Cor			
Component Services	Microsoft Cor			
Computer Managem	Mcrosoft Cor			
Device Manager	Microsoft Cor			
Disk Management	Microsoft and	~		Advanced
		_		

- 6. 展开 Personal 文件夹,然后单击 Certificates.LDAP使用的证书必须颁发给Windows服务器的完全限 定域名(FQDN)。在此服务器上列出三个证书:
- CA证书颁发给和颁发者 razor-WIN-E3SKFJQD6J7-CA.
- 颁发给和颁发者的CA证书 supinfo-WIN-FNJVP9QUEH9-CA.
- 身份证书颁发给 WIN-E3SKFJQD6J7.razor.local 通过 razor-WIN-E3SKFJQD6J7-CA.

在本配置指南中,FQDN是 WIN-E3SKFJQD6J7.razor.local 因此,前两个证书不能用作LDAP的SSL证书。 颁发给的标识证书 WIN-E3SKFJQD6J7.razor.local 是由Windows Server CA服务自动颁发的证书。双击证书 以检查详细信息。



- 7. 要用作LDAP的SSL证书,证书必须满足以下要求:
- 公用名或DNS主题备用名与Windows Server的FQDN匹配。
- 证书在Enhanced Key Usage字段下有Server Authentication。

在 Details 选项卡中,选择 Subject Alternative Name,其中FQDN WIN-E3SKFJQD6J7.razor.local 存在。

Cer	tificate	x				
General Details Certification Path						
Show: <all></all>	~					
Field Image: Enhanced Key Usage Image: Application Policies Image: Subject Key Identifier Image: Subject Key Identifier Image: CRL Distribution Points Image: CRL Distribution Points Image: Authority Information Access Image: Subject Alternative Name DNS Name = WIN-E3SKFJQD6J7.raz DNS Name = razor.local DNS Name = RAZOR	Value Client Authentication (1.3.6.1 [1]Application Certificate Polic 1b 34 75 f8 c4 3e ef 58 fb 43 KeyID=cf 83 92 a4 14 00 e7 5 [1]CRL Distribution Point: Distr [1]Authority Info Access: Acc Digital Signature, Key Encipher DNS Name=WIN-E3SKFJQD6J					
Edit Properties Copy to File Learn more about <u>certificate details</u>						
	OK					

低于 Enhanced Key Usage, Server Authentication 存在。

Cer	tificate X					
General Details Certification Path						
Show: <all></all>	~					
Field	Value ^ Template=LDAPoverSSL(1.3.6					
Enhanced Key Usage	Client Authentication (1.3.6.1					
Client Authentication (1.3.6.1.5.5.) Smart Card Logon (1.3.6.1.5.2.3.)	[1] Application Certificate Polic 1b 34 75 f8 c4 3e ef 58 fb 43 KeyID=cf 83 92 a4 14 00 e7 5 [1] CRL Distribution Point: Distr [1] Authority Info Access: Acc Digital Signature, Key Encipher ✓ 7.3.2) 7.3.1) 1.20.2.2) 5)					
Ec Learn more about <u>certificate details</u>	Edit Properties Copy to File Learn more about <u>certificate details</u>					
	ОК					

8. 一旦确认,在 Certification Path 选项卡,选择作为根CA证书的顶级证书,然后单击 View Certificate.这 将打开根CA证书的证书详细信息,如图所示:

Certificate	x	Certificate X
General Details Certification Path Certification path and a statement of the statement of t		General Details Certification Path Image: Certificate Information Certificate Information This certificate is intended for the following purpose(s): • All issuance policies • All application policies • All application policies
		Issued to: razor-WIN-E3SKFJQD6J7-CA
View Certificate		Issued by: razor-WIN-E3SKFJQD6J7-CA
Certificate status:		Valid from 3/22/2021 to 3/22/2026
Learn more about <u>certification paths</u>		Learn more about <u>certificates</u>
OK		OK

9. 在 Details 根CA证书,点击 Copy to File 并浏览Certificate Export Wizard 该命令以PEM格式导出根CA。

选择 Base-64 encoded X.509 作为文件格式。

e 🦻	Certificate Export Wizard		
	Completing the Certificate Exp	oort Wizard	
	You have successfully completed the Certificate	Export wizard.	
	You have specified the following settings:		
	File Name	C:\Users\Administrator\Downloads\ro	٩
	Export Keys Include all certificates in the certification path	No No	
	File Format	Base64 Encoded X.509 (*.cer)	
		>	
			_
		Finish	Cancel

10. 使用记事本或其他文本编辑器打开计算机上选定位置中存储的根CA证书。

这显示PEM格式证书。请保存以备后用。

----BEGIN CERTIFICATE-----

MIIDfTCCAmWgAwIBAgIQV4ymxtI3BJ9JHnDL+luYazANBgkqhkiG9w0BAQUFADBRMRUwEwYKCZImiZPyLGQBGRYFbG9jYWwxFTATBgo vcjEhMB8GA1UEAxMYcmF6b3ItV010LUUzU0tGS1FENko3LUNBMB4XDTIxMDMyMjE0MzMxNVoXDTI2MDMyMjE0NDMxNVowUTEVMBMGCgr BWxvY2FsMRUwEwYKCZImiZPyLGQBGRYFcmF6b3IxITAfBgNVBAMTGHJhem9yLVdJTi1FM1NLRkpRRDZKNy1DQTCCASIwDQYJKoZIhvcl CCAQoCggEBAL803nQ6xPpazjj+HBZYc+8fV++RXCG+cUnb1xwtX0B2G4UxZ3LRrWznjXaS02Rc3qVw41nOAziGs4ZMNM1X8UWeKuwi8 9dkncZaGtQ1cPmqcnCWunfTsaENKbgoKi4eXjpwwUSbEYwU30aiiI/tp422ydy3Kg17Iqt1s4XqpZmTezykWra7dUyXfkuESk61E0AV CSkTQTRXYryy8dJrWjAF/n6A3VnS/17Uhuj1x4CD20BkfQy6p5HpGxdc4GMTTnDzUL46ot6imeBXPHF0IJehh+tZk3bxpoxTDXECAwE, DAgGGMA8GA1UdEwEB/wQFMAMBAf8wHQYDVR00BBYEFM+DkqQUA0dY379NnViaMIJAVTZ1MBAGCSsGAQQBgjcVAQQDAgEAMA0GCSqGSI AA4IBAQCiSm5U7U6Y7zXdx+d1eJd0QmGgKayAAuYAD+MWNwC4NzFD8Yr7Bn06f/VnF6VGYPXa+Dvs7VLZewMNkp3i+VQpkBCKdhAV6q 4sMZffbVrG1Rz7twWY36J5G5vhNUhzZ1N20Lw6wtHg2S08X1vpTS5fAnyCZgSK3VPKfXnn1HLp7UH5/SWN2JbPL15r+wCW84b8nry1b GuDsepY7/u2uWfy/vpTJigeok2DH6HFf0ET3sE+7rsIAY+of0kWW5gNwQ4h0wv4Goqj+YQRAXXi20Zy1tHR1dfUUbwVENSFQtDnFA7X ----END CERTIFICATE-----

在LDAP服务器上的本地计算机存储中安装多个证书的情况下(可选)

1.在LDAPS可以使用多个身份证书的情况下,当使用哪个身份证书存在不确定性,或者无法访问 LDAPS服务器时,仍然可以从在FTD上完成的数据包捕获中提取根CA。

2.如果您在LDAP服务器(如AD DS域控制器)本地计算机证书存储中有多个有效进行服务器身份验 证的证书,则可以注意到不同的证书用于LDAPS通信。解决此类问题的最佳方法是从本地计算机证 书存储中删除所有不必要的证书,并且仅有一个对服务器身份验证有效的证书。

但是,如果有正当理由需要两个或更多证书并且至少具有一个Windows Server 2008 LDAP服务器 ,则Active Directory域服务(NTDS\Personal)证书存储区可用于LDAP通信。

以下步骤演示如何将启用LDAPS的证书从域控制器本地计算机证书存储导出到Active Directory域服务证书存储(NTDS\Personal)。

- 导航到Active Directory服务器上的MMC控制台,选择文件,然后单击 Add/Remove Snap-in.
- 点击 Certificates 然后单击 Add.
- 如果 Certificates snap-in,选择 Computer account 然后单击 Next.
- 在 Select Computer,选择 Local Computer,单击 OK,然后单击 Finish.在 Add or Remove Snap-ins,单击 OK.
- 在包含用于服务器身份验证的证书的计算机的证书控制台中,右击 certificate,单击 All Tasks,然 后单击 Export.

2	Console1 - [Console Root\Certif	icates (Local Computer)\Perso	nal\Certificates]	_ □ X
🚟 File Action View Favorites Windo	w Help			_ 8 ×
🗢 🔿 🙍 🐻 🐇 🖬 😖				
Console Root	Issued To	Issued By	Expiration Date	Actions
∠ → Certificates (Local Computer) ∠ → Personal	razor-WIN-E3SKFJQD6J7-CA	razor-WIN-E3SKFJQD6J7-CA supinfo-WIN-ENJVP9OUEH9-CA	3/22/2026	Certificates
Certificates	WIN-E3SKFJQD6J7.razor.local	razor-WIN-E3SKFJQD617_CA	A/25/2022	More Actions
Trusted Root Certification Autho Enterprise Trust		Open		WIN-E3SKEIOD617 razor local
Intermediate Certification Autho		All Tasks	s > Op	en 🔶
Trusted Publishers		Cut	Rec	quest Certificate with New Key
Third-Party Root Certification Au		Copy	Ker	new Certificate with New Key
▷ Invited People		Propertie	es Ad	vanced Operations
Client Authentication Issuers Other People		Help	E Fyr	ort
Remote Desktop		Thep		
Certificate Enrollment Requests Smart Card Trusted Roots				
Trusted Devices				
♦ 🔛 Web Hosting 🛛 ✓	<		>	
Export a certificate	16 .			,

在中导出证书 pfx 在后续章节中设置。有关如何在中导出证书的文章,请参阅 pfx 来自MMC的格式:

https://www.cisco.com/c/en/us/support/docs/security/web-security-appliance/118339-technotewsa-00.html。

- 导出证书后,导航至 Add/Remove Snap-in 在 MMC console.点击 Certificates 然后单击 Add.
- 选择 Service account 然后单击 Next.

Certificates snap-in

х

This snap-in will always manage certificates for:

- O My user account
- Service account
- Computer account
- 如果 Select Computer 对话框,选择 Local Computer 并点击 Next.
- 选择 Active Directory Domain Services 然后单击 Finish.

Certificate	s snap-in		x
Select a service account to manage on the local co	omputer.		
Service account:			
Active Directory Certificate Services Active Directory Domain Services Active Directory Web Services AD FS Windows Service Application Experience Application Host Helper Service Application Identity Application Information Application Layer Gateway Service Application Management			
ASP.NET State Service Background Intelligent Transfer Service Background Tasks Infrastructure Service Base Filtering Engine		~	
	< Back	Finish Cancel	

- 在 Add/Remove Snap-ins 对话框,单击 OK.
- 扩大采购 Certificates Services (Active Directory Domain Services) 然后单击 NTDS\Personal.
- 右键单击 NTDS\Personal, 单击 All Tasks, 然后单击 Import.

Console1 - [Console Root\Certifica	ates - Service (Active Directory Domain Services) on Local Computer\NTDS\F	Personal] 🗕 🗖 🗙
藩 File Action View Favorites Window Help		_ & ×
🗢 🔿 🙍 🖬 📋 🧟 🐋 🖬 📷		
Console Root Object Type	Actions	
Certificates (Local Computer) Certificates - Service (Active Directory D	es NTDS\Pe	ersonal 🔺
	More	Actions
Find Certificates		
▶ NT All Tasks Fir	ind Certificates	
D In View → In	nport	
Image: Market Mark	dvanced Operations	
▷ NT New Taskpad View		
NT Refresh		
Export List		
Help		
Add a certificate to a store	11	

- 在 Certificate Import Wizard 欢迎屏幕,单击 Next.
- 在"要导入的文件"屏幕上,单击 Browse,并找到先前导出的证书文件。
- 在"打开"屏幕上,确保个人信息交换(*pfx,*.p12)被选为文件类型,然后导航文件系统以查找先前 导出的证书。然后,点击该证书。

a	Ope	n	I.		x
€ 🕘 ▾ ↑ 📑 ኑ Libr	raries + Documents		♥ 🖒 Search Do	ocuments	Q
Organize 👻 New folder				· ·	0
쑦 Favorites	Name	Date modified	Туре	Size	
Desktop	🏂 ldapcert	4/25/2022 12:01	Personal Informati	5 KB	
🐞 Downloads 🖳 Recent places					
🥽 Libraries					
Documents					
J Music					
Pictures					
📑 Videos					
🖳 Computer					
👊 Network					
File nar	me: Idapcert		✓ Personal	Information Exchan	ge 🗸
			Оре	n Cance	e l

- 点击 Open 然后单击 Next.
- 在"密码"屏幕上,输入为文件设置的密码,然后单击 Next.
- 在Certificate Store页面上,确保选中Place all certificates并阅读Certificate Store: NTDS\Personal 然后单击 Next.

€	🔗 Certificate Import Wizard
	Certificate Store
	Certificate stores are system areas where certificates are kept.
	Windows can automatically select a certificate store, or you can specify a location for the certificate.
	\bigcirc Automatically select the certificate store based on the type of certificate
	Place all certificates in the following store
	Certificate store:
	NTDS\Personal Browse
	Learn more about certificate stores
	Next Cancel

х

• 在 Certificate Import Wizard 完成屏幕,单击 Finish.然后您会看到一条消息,表明导入成功。点击 OK.可以看到证书已导入到证书存储区下: NTDS\Personal.

Console1 - [Console Root\Certifica	ates - Service (Active Directory	Domain Services) on Local C	computer\NTDS\Pe	ersonal\Certificates] 🗕 🗖	x
藩 File Action View Favorites Window	/ Help			_ (5 ×
🗢 🔿 🙋 📰 🤞 💺 🖬 🛃					
Console Root	Issued To	Issued By	Expiration Date	Actions	
Certificates (Local Computer)	razor-WIN-E3SKFJQD6J7-CA	razor-WIN-E3SKFJQD6J7-CA	3/22/2026	Certificates	
⊿ GU Certificates - Service (Active Directory D)	WIN-E3SKFJQD6J7.razor.local	razor-WIN-E3SKFJQD6J7-CA	4/25/2023	More Actions	•
⊿ IntoS\Personal				More Actions	·
NTDS\Trusted Root Certification Au				WIN-E3SKFJQD6J7.razor.local	-
NTDS\Enterprise Trust				More Actions	•
NTDS\Intermediate Certification Au					
NTDS\Trusted Publishers					
NTDS\Untrusted Certificates					
NTDS\Third-Party Root Certification					
INTDS\Trusted People					
NTDS\Client Authentication Issuers					
< III >	< III		>		
NTDS\Personal store contains 2 certificates.					

FMC配置

验证许可

要部署AnyConnect配置,FTD必须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。

设置领域

1. 导航至 System > Integration.导航至 Realms,然后单击 Add Realm,如下图所示:

Overview Analys	sis Policies Devices Objects	AMP Intelligence								-	Deploy Sys	stem Help 🔻	admin 🔻
				Configuration	Users	Domains	Integration	Updates	Licenses v	Logging •	Health •	¹ Monitoring •	Tools •
	3						2						
Cloud Services	Realms Identity Sources	High Availability eStr	eamer Host Input Client	Smart Software Mana	nger On-Pr	rem							
Realms R	tealm Sequences Sync Results												4
											Compa	re Realms Ad	d Realm
Name 👻	Description	Туре	Domain	AD Primary Domain	,		Base DN				State		

2. 根据从Microsoft LDAP服务器收集的信息填写显示的字段。在此之前,请导入在Windows Server上签署LDAP服务证书的根CA证书 Objects > PKI > Trusted CAs > Add Trusted CA,因为在Directory Server Configuration 领域。完成后,单击 OK.

Firepower Manag Objects / Object Manage	ement Center Overview Analy	sis Policies Devices Objects AMP Intelligence		Deploy Q 🚱 🔅 (admin 🔹
AAA Server Access List Address Pools Application Elitere	Trusted CAs Trusted certificate authority (CA) object	represents a CA public key certificate belonging to a trusted CA. You can use e	xternal CA objects in	Add Trusted CA Q. Filter SSL policy, realm configurations and ISE/ISE-PIC connection	on.
AS Path Cipher Suite List Community List	Name ISRG-Root-X1 Izence.com			Value CN=ISRG Root X1, ORG=Internet Security Research G CN=Izenoe.com, ORG=IZENPE S.A., C=ES	11
DNS Server Group External Attributes Eile List	LDAPS-ROOT-CERT Microsec-e-Szigno-Root-CA-2009	Edit Trusted Certificate Authority	0	CN=razor-WIN-E3SKFJQD6J7-CA CN=Microsec e-Szigno Root CA 2009, ORG=Microse	11
FlexConfig Geolocation Interface	NetLock-Arany-Class-Gold-FAtanAosAtv OISTE-WISeKey-Global-Root-GA-CA	Name: LDAPS-ROOT-CERT		CN=NetLock Arany (Class Gold) FA tanA2sÅtvÅjny, CN=OISTE WISeKey Global Root GA CA, ORG=WISeK	/1
Key Chain Network V PKI	OISTE-WISeKey-Global-Root-GB-CA OISTE-WISeKey-Global-Root-GC-CA	Subject: Common Name: razor-WIN-E3SKFJQD6J7-CA Organization:		CN=OISTE WISeKey Global Root GB CA, ORG=WISeK CN=OISTE WISeKey Global Root GC CA, ORG=WISeK	/1
Cert Enrollment External Cert Groups External Certs	QuoVadis-Root-CA-1-G3 QuoVadis-Root-CA-2	Organization Unit: Issuer: Common Name: razor-WIN-E3SKFJQD6J7-CA		CN=QuoVadis Root CA 1 G3, ORG=QuoVadis Limited, CN=QuoVadis Root CA 2, ORG=QuoVadis Limited, C=	/1
Internal CA Groups Internal CAs Internal Cert Groups	QuoVadis-Root-CA-3 QuoVadis-Root-CA-3-G3	Organization: Organization Unit: Not Valid Before:		CN=QuoVadis Root CA 3, ORG=QuoVadis Limited, C= CN=QuoVadis Root CA 3 G3, ORG=QuoVadis Limited,	11
Internal Certs Trusted CA Groups Trusted CAs	QuoVadis-Root-Certification-Authority Secure-Global-CA	Mar 22 14:33:15 2021 GMT Not Valid After: Mar 22 14:43:15 2026 GMT		CN=QueVadis Root Certification Authority, ORG=QueV CN=Secure Global CA, ORG=SecureTrust Corporation	11
Policy List Port	SecureTrust-CA	Install Certificate Cance	el Save	CN*SecureTrust CA, ORG*SecureTrust Corporation, Displaying 81 - 100 of 125 rows < < Page 5	/ ⊒ 017 > > C

Add New Realm

Name*	Description					
LDAP-Server						
Туре						
LDAP						
Directory Username*	Directory Password*					
Administrator@razor.local						
E.g. user@domain.com						
Base DN*	Group DN*					
DC=razor,DC=local	DC=razor,DC=local					
E.g. ou=group,dc=cisco,dc=com	E.g. ou=group,dc=cisco,dc=com					
Directory Server Configuration						
 WIN-E3SKFJQD6J7.razor.local:636 						
Hostname/IP Address*	Port*					
WIN-E3SKFJQD6J7.razor.local	636					
Encryption	CA Certificate*					
LDAPS V	LDAPS-ROOT-CERT V +					
Interface used to connect to Directory server (
Resolve via route lookup						
Default: Management/Diagnostic Interface	× ·					
Test						
Add another directory						

0 ×

3. 点击 Test 为了确保FMC能够成功绑定到前面步骤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上配置的可路由接口(例如内部、外部和dmz)之一启动,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身份验证请求是从一个FTD可路由接口启动的。

Add Directory	@ ×
Hostname/IP Address* WIN-E3SKFJQD6J7.razor.loc	Port* 636
Encryption	CA Certificate*
LDAPS	LDAPS-ROOT-CERT V +
Interface used to connect to Dire	ctory server 🚺
Resolve via route lookup	
O Choose an interface	
Default: Management/Diag	nostic Interface 🗸
Test 📀 Test connection s	succeeded
	Cancel OK

4. 启用新领域。

Overden, Ann	husia Balisian Davison Objects	AND Intelligence								•	Dealers	teen Hele -	admin -
Overview Ana	liysis Policies Devices Objects	AMP Intelligence		Configuration	Users E	Domains	Integration	Updates	Licenses •	Logging V	Health •	Monitoring V	Tools •
				comgaración	00010			opourco	Electroco -	cogging -	The arter of the	riointornig .	10010
Cloud Service	es Realms Identity Sources	High Availability eStreame	Host Input Client	Smart Software Man	ager On-Prei	m							
Realms	Realm Sequences Sync Results												
											Compa	re Realms Ad	d Realm
Name +	Description	Туре	Domain	AD Primary Domai	n		Base DN				State		
AC-Local		LOCAL	Global								🛑 Enable	ed 🗼 🌶	· B 🗑
LDAP		AD	Global	cisco01.com			OU=Users,0	U=CISCO,D	C=cisco01,DC=	com	C Enabl	ed 🛓 🌶	/ fb 🗑
LDAP-Server		AD	Global	razor.local			DC=razor,D	C=local			C Enable	ed 🛨 🌶	- B 🗑

配置AnyConnect进行密码管理

 选择现有连接配置文件,或创建新连接配置文件(如果是AnyConnect的初始设置)。此处使 用名为"AnyConnect-AD"且映射了本地身份验证的现有连接配置文件。

Overview Analysis Policies Devices Objects AMP Inte	elligence	e	Deploy System Help * admin *
Device Management Device Upgrade NAT VPN > Remote Acc	cess QoS Platform Settings FlexConfig Certificates		
AnyConnect Enter Description			Save Save
			Policy Assignments (1)
		Local Realm: asa	Dynamic Access Policy: Hostscan
Connection Profile Access Interfaces Advanced			
			0
Name	AAA	Group Policy	
DefaultWEBVPNGroup	Authentication: None Authorization: None Accounting: None	DftGrpPolicy	/ 5
AnyConnect	Authentication: Radius (RADIUS) Authorization: Radius (RADIUS) Accounting: Anone	DftGrpPolicy	/ 6
AnyConnect-AD	Authensication: LOCAL Authorization: None Accounting: None	AnyConnect-Group	/ 9

2. 在连接配置文件的AAA设置下,编辑连接配置文件并映射在之前步骤中配置的新LDAP服务器。完成后,单击 Save 在右上角。

CISCO Devices / VPN / Edit Connection Profile Overview	Analysis Policies Devices Objects AMP Intelligence	Deploy 🔍 💕 🌣 🞯 admin 🔻
AnyConnect Enter Description		Save Cancel
Connection Profile Access Interfaces Advanced	Edit Connection Profile Local Real	n: None Dynamic Access Policy: Hostscan
	Connection Profile:* AnyConnect-AD Group Policy:* AnyConnect-Group + +	+
Name	Edit Group Policy Client Address Assignment AAA Aliases	
DefaultWEBVPNGroup	Authentication	/1
AnyConnect	Authentication Method: AAA Only	/¥
AnyConnect-AD	Authentication Server: LDAP-Server (AD) Fallback to LOCAL Authentication	∕≆_
	Use secondary authentication	
	Authorization	
	Authorization Server: Use same authentication server	
	Accounting	
	Accounting Server:	
	 Advanced Settings 	
	Strip Realm from username	
	Cancel Save	

3. 在 AAA > Advanced Settings 并保存配置。

Overview Analysis Policies Devices Objects AMP Intellige Device Management Device Upgrade NAT VPN + Remote Access	CG QoS Platform Settings FlexConfig Certificates		🔥 Dep	loy System Help + admin +
AnyConnect				Save Cancel
enter Description			Local Realm: asa	Policy Assignments (1) Dynamic Access Policy: <u>Hostscan</u>
Connection Profile Access Interfaces Advanced	Edit Connection Profile	? ×		
Name	Connection Profile: * AnyConnect-AD Group Policy: * AnyConnect-Group * • •			0
DefaultWEBVPNGroup	Client Address Assignment AAA Aliases			/8
AnyConnect	LDAP-Server (AD) Pallback to LOCAL Authentication	•		/8
AnyConnect-AD	Use secondary authentication			08
	Authorization Authorization Server: Use same authentication server :	v		
sjobs /	 Allow connection only if user exists in authorization Configure LDAP Attribute Map 	n database		/ 8
	Configure LDAP Attribute Map Accounting Accounting Server: Advanced Settings Strip Realm from username Strip Group from username E Enable Password Management Modify User 1 days prior to password expiration Notify user on the day of password expiration	Save Cancel		

部署

1. 完成所有配置后,点击Deploy 按钮右上角。

Overview Analysis Policies Devices Objects AMP Intelligence

🇛 Deploy System Help 🔻 admin 🕶

2. 点击应用到它的FTD配置旁边的复选框,然后点击 Deploy,如下图所示:

Overview	Analysis Policies Devices Objects	s AMP Intelligence					90 Deploy System Help + admin +
							Deployment Deployment History
T Q	Search using device name, user name, type	a, group or status					1 device selected Deploy time: Estimate
•	Device	Modified by	Inspect Interruption	Type Grou	Last Deploy Time	Preview	Status
> 🛛	10.197.224.190_FTD1	admin		FTD	May 30, 2022 7:34 AM	E9.	Pending

最终配置

这是成功部署后在FTD CLI中看到的配置。

AAA配置

<#root>

> show running-config aaa-server

```
aaa-server LDAP-Server protocol ldap
```

```
max-failed-attempts 4
```

```
realm-id 8
```

aaa-server LDAP-Server host WIN-E3SKFJQD6J7.razor.local

<----- LDAPs Server to which the queries are sent

server-port 636

- ldap-base-dn DC=razor,DC=local
- ldap-group-base-dn DC=razor,DC=local
- ldap-scope subtree
- ldap-naming-attribute sAMAccountName
- ldap-login-password *****
- ldap-login-dn *****@razor.local
- ldap-over-ssl enable
- server-type microsoft

AnyConnect配置

<#root>

> show running-config webvpn

webvpn

```
enable Outside
```

```
anyconnect image disk0:/csm/anyconnect-win-4.10.01075-webdeploy-k9.pkg 1 regex "Windows"
```

```
anyconnect profiles FTD-Client-Prof disk0:/csm/ftd.xml
```

anyconnect enable

tunnel-group-list enable

cache

no disable

error-recovery disable

tunnel-group AnyConnect-AD type remote-access
tunnel-group AnyConnect-AD general-attributes

address-pool Pool-1

authentication-server-group LDAP-Server

default-group-policy AnyConnect-Group

password-management password-expire-in-days 1

tunnel-group AnyConnect-AD webvpn-attributes

group-alias Dev enable

> show running-config group-policy AnyConnect-Group

group-policy

AnyConnect-Group

internal

<----- Group-Policy configuration that is mapped once the user is authenticated</pre>

<---- LDAPs Serve

<---- Protocol

<---- Password-management

group-policy AnyConnect-Group attributes

vpn-simultaneous-logins 3

vpn-idle-timeout 35791394

vpn-idle-timeout alert-interval 1

vpn-session-timeout none

vpn-session-timeout alert-interval 1

vpn-filter none

vpn-tunnel-protocol ikev2 ssl-client

split-tunnel-policy tunnelspecified

split-tunnel-network-list value Remote-Access-Allow

default-domain none split-dns none split-tunnel-all-dns disable client-bypass-protocol disable vlan none address-pools none webvpn anyconnect ssl dtls enable anyconnect mtu 1406 anyconnect firewall-rule client-interface public none anyconnect firewall-rule client-interface private none anyconnect ssl keepalive 20 anyconnect ssl rekey time none anyconnect ssl rekey method none anyconnect dpd-interval client 30 anyconnect dpd-interval gateway 30 anyconnect ssl compression none anyconnect dtls compression none anyconnect modules value none anyconnect profiles value FTD-Client-Prof type user anyconnect ask none default anyconnect anyconnect ssl df-bit-ignore disable

> show running-config ssl

ssl trust-point ID-New-Cert Outside

<----- FTD ID-cert trustpoint name mapped to the outside interface on which AnyConnect Connections

确认

使用AnyConnect连接并验证用户连接的密码管理过程

1.发起到相关连接配置文件的连接。一旦在初始登录时确定必须更改密码,因为较早的密码已过期 ,被Microsoft Server拒绝,系统将提示用户更改密码。

S Cisco AnyConnect FTD-Hostname ×	
Group: Dev v Username: admin Passwork: [Cisco AnyConnect Secure Mobility Client Viii Contexto pTD-Hosthame. FTD-Hosthame Connect
OK Cancel	

Cisco AnyConnect FTD-Hostname New Password: Venfy Password: Password: Password: Password change required, you must enter a new		
password with a minimum length of 7 to continue.	Cisco AnyConnect Secure Mobility Client — X VPIE Contacting FTD Hostname. FTD Hostname Continue Continue	
	¢ () eteb	

2. 用户输入登录新密码后,连接成功建立。

S Cisco AnyConnect Secure Mobility Client			-		×
	VPN: Connected to FTD-Hostname. FTD-Hostname	~		Disconnec	t
00:02:43					IPv4
۞ (i)					diala cisco

3. 验证FTD CLI上的用户连接:

<#root>

FTD_2# sh vpn-sessiondb anyconnect

Session Type: AnyConnect Username : admin Index : 7 <----- Username, IP address assigned information of the client Assigned IP : 10.1.x.x Public IP : 10.106.xx.xx Protocol : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel License : AnyConnect Premium Encryption : AnyConnect-Parent: (1)none SSL-Tunnel: (1)AES-GCM-256 DTLS-Tunnel: (1)AES-GCM-256 Hashing : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA384 DTLS-Tunnel: (1)SHA384 Bytes Tx : 16316 Bytes Rx : 2109 Group Policy : AnyConnect-Group Tunnel Group : AnyConnect-AD Login Time : 13:22:24 UTC Mon Apr 25 2022 Duration : 0h:00m:51s Inactivity : 0h:00m:00s VLAN Mapping : N/A VLAN : none Audt Sess ID : 0ac5e0fa000070006266a090 Security Grp : none Tunnel Zone : 0

故障排除

调试

此调试可以在诊断CLI中运行,以便排除与密码管理相关的问题:debug ldap 255。

工作密码管理调试

<#root>

- [24] Session Start
- [24] New request Session, context 0x0000148f3c271830, reqType = Authentication
- [24] Fiber started
- [24] Creating LDAP context with uri=ldaps://10.106.71.234:636

[24] Connect to LDAP server: ldaps://10.106.71.234:636, status = Successful

[24] supportedLDAPVersion: value = 3

- [24] supportedLDAPVersion: value = 2
- [24] Binding as *****@razor.local
- [24] Performing Simple authentication for *****@razor.local to 10.106.71.234
- [24] LDAP Search:
 - Base DN = [DC=razor,DC=local]
 - Filter = [sAMAccountName=admin]
 - Scope = [SUBTREE]
- [24] User DN = [CN=admin,CN=Users,DC=razor,DC=local]
- [24] Talking to Active Directory server 10.106.71.234
- [24] Reading password policy for admin, dn:CN=admin,CN=Users,DC=razor,DC=local

[24] Read bad password count 3

[24] Binding as admin

[24] Performing Simple authentication for admin to 10.106.71.234

[24] Simple authentication for admin returned code (49) Invalid credentials

[24] Message (admin): 80090308: LdapErr: DSID-0C0903C5, comment: AcceptSecurityContext error, data 773,

```
[24] Checking password policy
```

[24] New password is required for admin

[24] Fiber exit Tx=622 bytes Rx=2771 bytes, status=-1

[24] Session End

[25] Session Start

- [25] New request Session, context 0x0000148f3c271830, reqType = Modify Password
- [25] Fiber started
- [25] Creating LDAP context with uri=ldaps://10.106.71.234:636
- [25] Connect to LDAP server: ldaps://10.106.71.234:636, status = Successful

[25] supportedLDAPVersion: value = 3

- [25] supportedLDAPVersion: value = 2
- [25] Binding as *****@razor.local
- [25] Performing Simple authentication for *****@razor.local to 10.106.71.234
- [25] LDAP Search:

```
Base DN = [DC=razor,DC=local]
```

Filter = [sAMAccountName=admin]

```
Scope = [SUBTREE]
```

- [25] User DN = [CN=admin,CN=Users,DC=razor,DC=local]
- [25] Talking to Active Directory server 10.106.71.234
- [25] Reading password policy for admin, dn:CN=admin,CN=Users,DC=razor,DC=local

[25] Read bad password count 3

[25] Change Password for admin successfully converted old password to unicode

[25] Change Password for admin successfully converted new password to unicode

```
[25] Password for admin successfully changed
```

- [25] Retrieved User Attributes:
- [25] objectClass: value = top
- [25] objectClass: value = person
- [25] objectClass: value = organizationalPerson
- [25] objectClass: value = user
- [25] cn: value = admin
- [25] givenName: value = admin
- [25] distinguishedName: value = CN=admin,CN=Users,DC=razor,DC=local
- [25] instanceType: value = 4
- [25] whenCreated: value = 20201029053516.0Z
- [25] whenChanged: value = 20220426032127.0Z
- [25] displayName: value = admin
- [25] uSNCreated: value = 16710
- [25] uSNChanged: value = 98431
- [25] name: value = admin
- [25] objectGUID: value = ..0.].LH.....9.4
- [25] userAccountControl: value = 512
- [25] badPwdCount: value = 3
- [25] codePage: value = 0
- [25] countryCode: value = 0
- [25] badPasswordTime: value = 132610388348662803
- [25] lastLogoff: value = 0
- [25] lastLogon: value = 132484577284881837
- [25] pwdLastSet: value = 0

- [25] primaryGroupID: value = 513
- [25] objectSid: value =7Z|....RQ...
- [25] accountExpires: value = 9223372036854775807
- [25] logonCount: value = 0
- [25] sAMAccountName: value = admin
- [25] sAMAccountType: value = 805306368
- [25] userPrincipalName: value = *****@razor.local
- [25] objectCategory: value = CN=Person,CN=Schema,CN=Configuration,DC=razor,DC=local
- [25] dSCorePropagationData: value = 20220425125800.0Z
- [25] dSCorePropagationData: value = 20201029053516.0Z
- [25] dSCorePropagationData: value = 16010101000000.0Z
- [25] lastLogonTimestamp: value = 132953506361126701
- [25] msDS-SupportedEncryptionTypes: value = 0
- [25] uid: value = *****@razor.local
- [25] Fiber exit Tx=714 bytes Rx=2683 bytes, status=1
- [25] Session End

密码管理过程中遇到的常见错误

通常,如果在用户提供新密码期间未满足Microsoft Server设置的密码策略,连接将终止,并显示错 误"Password does the Password Policy Requirements"。因此,请确保新密码符合Microsoft Server为LDAP设置的策略。

S Cisco AnyCon	nect FTD-Hostname	×			
Cannot ci password complexit	omplete password change because the password does not meet the policy requirements. Check the minimum password length, password ly, and password history requirements.				
Group:	Dev 🗸	S Cisco A	AnyConnect Secure Mobility Client — 🗆 🗙		
Username	e: admin		VPN		
Password	ź:	' 🖆	Cannot complete password change because the password does not meet the password policy requirements. Check		
	OK Cancel		FTD-Hostname V Connect		
		\$ ()	allada Cisco		
		Cisco Ar	nyConnect >	×	
			Cannot complete password change because the password does not meet the password policy requirements. Check the minimum password length, password complexity, and password history requirements.		
			ОК		

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)。