# Configurar autenticação do AD (LDAP) e identidade do usuário no FTD gerenciado pelo FMC para clientes AnyConnect

## Contents

Introduction **Prerequisites Requirements Componentes Utilizados** Informações de Apoio Configurar Diagrama e cenário de rede Configurações do Active Directory Determinar o DN de base e o DN do grupo do LDAP Criar uma conta FTD Criar grupos do AD e adicionar usuários aos grupos do AD (opcional) Copiar a raiz do certificado SSL do LDAPS (necessário apenas para LDAPS ou STARTTLS) Configurações do FMC Verificar licenciamento Configurar realm Configurar AnyConnect para autenticação do AD Ativar política de identidade e configurar políticas de segurança para identidade do usuário Configurar isenção de NAT Implantar Verificar Configuração final Configuração do AAA Configuração do AnyConnect Conectar-se ao AnyConnect e verificar regras de política de controle de acesso Verificar com eventos de conexão do FMC Troubleshoot Debugs Como trabalhar com as depurações do LDAP Não é possível estabelecer uma conexão com o servidor LDAP DN de login de vinculação incorreto e/ou senha incorreta O servidor LDAP não consegue encontrar o nome de usuário Senha incorreta para o nome de usuário AAA de teste Capturas de pacotes Registros do visualizador de eventos do Windows Server

## Introduction

Este documento descreve como configurar a autenticação do AD para clientes do AnyConnect que se conectam ao Cisco Firepower Threat Defense (FTD).

## Prerequisites

#### Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Conhecimento básico da configuração de RA VPN no FMC
- Conhecimento básico da configuração do servidor LDAP no FMC
- Conhecimento básico do Ative Diretory (AD)

#### **Componentes Utilizados**

As informações neste documento são baseadas nestas versões de software e hardware:

- Microsoft 2016 Server
- FMCv executando 6.5.0
- FTDv executando 6.5.0

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

#### Informações de Apoio

Este documento descreve como configurar a autenticação do Active Directory (AD) para clientes AnyConnect que se conectam ao Cisco Firepower Threat Defense (FTD), gerenciado pelo Firepower Management Center (FMC).

A identidade do usuário é usada nas políticas de acesso para restringir os usuários de AnyConnect a endereços IP e portas específicos.

### Configurar

#### Diagrama e cenário de rede



O Windows Server é pré-configurado com IIS e RDP para testar a identidade do usuário. Neste

guia de configuração, três contas de usuário e dois grupos são criados.

Contas do usuário:

- FTD Admin: Usado como a conta de diretório para permitir que o FTD se vincule ao servidor do Ative Diretory.
- Administrador de TI: uma conta de administrador de teste usada para demonstrar a identidade do usuário.
- Usuário de teste: uma conta de usuário de teste usada para demonstrar a identidade do usuário.

Grupos:

- Administradores do AnyConnect: um grupo de teste que o administrador de TI adiciona para demonstrar a identidade do usuário. Esse grupo só tem acesso RDP ao Windows Server.
- Usuários do AnyConnect: um grupo de teste em que o usuário de teste é adicionado para demonstrar a identidade do usuário. Esse grupo só tem acesso HTTP ao Windows Server.

### Configurações do Active Directory

Para configurar adequadamente a autenticação do AD e a identidade do usuário no FTD, alguns valores são necessários.

Todos esses detalhes devem ser criados ou coletados no Microsoft Server, antes que a configuração seja feita no FMC. Os principais valores são:

#### • Nome de domínio:

Este é o nome de domínio do servidor. Neste guia de configuração, example.com é o nome de domínio.

#### • Endereço IP/FQDN do servidor:

O endereço IP ou FQDN usado para acessar o Microsoft Server. Se um FQDN for usado, um servidor DNS deverá ser configurado no FMC e no FTD para resolver o FQDN.

Neste guia de configuração, esse valor é win2016.example.com (que resolve para 192.168.1.1).

#### • Porta do servidor:

A porta usada pelo serviço LDAP. Por padrão, LDAP e STARTTLS usam a porta TCP 389 para LDAP, e LDAP sobre SSL (LDAPS) usa a porta TCP 636.

#### • CA raiz:

Se LDAPS ou STARTTLS for usado, a CA raiz usada para assinar o certificado SSL usado por LDAPS será necessária.

#### • Nome de usuário e senha do diretório:

Esta é a conta usada pelo FMC e pelo FTD para vincular-se ao servidor LDAP, autenticar usuários e procurar usuários e grupos.

Uma conta denominada Administrador de FTD é criada para essa finalidade.

• Nome distinto (DN) de base e de grupo:

O DN de base é o ponto de partida que o FMC e o FTD informam ao Active Directory para iniciar a pesquisa e autenticar os usuários.

Da mesma forma, o DN de grupo é o ponto de partida que o FMC informa ao Active Directory onde começar a procurar grupos para identidade do usuário.

Neste guia de configuração, o domínio raiz example.com é usado como DN base e DN de grupo.

No entanto, para um ambiente de produção, é melhor usar um **DN base** e **DN de grupo** mais adiante na hierarquia LDAP.

Por exemplo, esta hierarquia LDAP:



Se um administrador deseja que os usuários na unidade organizacional**Marketing** possam autenticar o DN base, ele pode ser definido como a raiz (example.com).

No entanto, isso também permite que o Usuário1 na unidade organizacional **Finance** também faça login, uma vez que a pesquisa do usuário começa na raiz e vá para **Finance, Marketing** e **Research**.

DN de base definido como example.com



Para restringir os logins ao único usuário na unidade organizacional de marketing e abaixo, o administrador pode definir o DN de base como marketing.

Agora, apenas User2 e User3 podem ser autenticados, pois a pesquisa começa em marketing.

DN de base definido como marketing



Observe que, para um controle mais granular no FTD, para o qual os usuários têm permissão para se conectar ou atribuir autorizações diferentes a usuários de acordo com os atributos do AD, um mapa de autorização LDAP precisa ser configurado.

Mais informações sobre isso podem ser encontradas aqui: <u>Configure o mapeamento LDAP do</u> <u>AnyConnect no Firepower Threat Defense (FTD)</u>.

Essa hierarquia LDAP simplificada é usada neste guia de configuração e o DN da raiz example.com é usado para o DN de base e o DN de grupo.



Determinar o DN de base e o DN do grupo do LDAP

1. Abra Usuários e Computadores do Ative Diretory.

=	Best match						
ŵ	Active Directory Users and Computers Desktop app						
	Settings >						
	8 Edit local users and groups						
	r Change User Account Control settings						
	User Accounts						
	Select users who can use remote desktop						
۲							
	users						
	ዶ 🗆 差 🛢						

2. Clique com o botão esquerdo do mouse em **domínio raiz** (para abrir o contêiner), clique com o botão direito do mouse no **domínio raiz** e, em **Exibir**, clique em **Recursos avançados**.



3. Isso permite a exibição de propriedades adicionais sob os objetos do AD. Por exemplo, para localizar o DN da raiz example.com, clique com o botão direito do mouse em example.com e escolha **Properties**.



4. Em **Propriedades**, selecione a guia **Editor de Atributos**. Localize **distinguishedName** sob os **Atributos** e clique em **Exibir**.

example.	com Propertie	5				?	×
General	Managed By	Object	Security	Attribut	e Editor		
Attribute	88:						
Attribu	te	Valu	e				^
dc		exan	nple				
defaul	tLocalPolicyOb	j <not< td=""><th>set&gt;</th><td></td><td></td><td></td><td></td></not<>	set>				
descri	ption	knot	set>				
deskte	op Profile	knot	set>				
display	yName	knot	set>				
displa	vNamePrintable	e knot	set>	_			
disting	uishedName	DC=	example.D	C=com			
domai	nPolicyObject	<not< td=""><th>set&gt;</th><td></td><td></td><td></td><td></td></not<>	set>				
domai	nReplica	<not< td=""><th>set&gt;</th><td></td><td></td><td></td><td></td></not<>	set>				
dSAS	ignature	{ V1	: Flags = Ox	0; Laten	icySecs =	= 0; DsaGu	ác 👘
dSCor	rePropagationD	0x0	=()				
eFSP	olicy	<not< td=""><th>set&gt;</th><td></td><td></td><td></td><td></td></not<>	set>				
extent	sionName	<not< td=""><th>set&gt;</th><td></td><td></td><td></td><td></td></not<>	set>				
flags		<not< td=""><th>set&gt;</th><td></td><td></td><td></td><td>~</td></not<>	set>				~
<						3	<u>۲</u>
V	ew					Filter	
	OK		Cancel		Apply	Н	elp

5. Isso abre uma nova janela onde o DN pode ser copiado e colado no FMC posteriormente. Neste exemplo, o DN raiz é DC=example,DC=com.

Copie o valor e salve-o para mais tarde. Clique em **OK** para sair da janela Editor de atributos de string e clique em OK novamente para sair das Propriedades.

tring Attribute Editor		×		
ttribute: distingui	shedName			
C=example,DC=com			Undo	
Clear	OK Cancel		Cut	
			Сору	
			Paste	
			Delete	
			Select All	
			Right to left Reading order	
			Show Unicode control characters	
			Insert Unicode control character	
Attributes: Attribute	Value ^			
Attribute	Value ^			
cn	<not set=""></not>			
controlAccessRights	<not set=""></not>			
creation Time	4/29/2020 2:43:49 PM Eastern Daylight Tim			
defaulti ocal Police Ohi	example (not ext)			
description	(not set)			
desktopProfile	(not set)			
displayName	<not set=""></not>			
displayNamePrintable	<not set=""></not>			
distinguishedName	DC=example,DC=com			
domainPolicyObject	<not set=""></not>			
domain Peplica	<pre><not set=""> //(1: Race = 0x0: Latency:Sace = 0: DesC: //</not></pre>			
dSCorePropagationD	(v): hags = uku, LatencySecs = 0; DisaGuk			
<	>			
View	Fiter			
OK	Cancel Apply Help			

Essa ação pode ser feita para vários objetos no Active Directory. Por exemplo, estas etapas são usadas para encontrar o DN do contêiner Usuário:



6. A view **Advanced Features** pode ser removida clicando com o botão direito do mouse no DN raiz novamente e, em **View**, clique em **Advanced Features** mais uma vez.



#### Criar uma conta FTD

Esta conta de usuário permite que o FMC e o FTD sejam vinculados ao Active Directory para procurar usuários e grupos e autenticar usuários.

O objetivo de criar uma conta FTD separada é evitar o acesso não autorizado em outro lugar na rede, caso as credenciais usadas para vinculação sejam comprometidas.

Essa conta não precisa estar no escopo do DN de base ou do DN de grupo.

1. Em **Usuários e Computadores do Ative Diretory**, clique com o botão direito do mouse no contêiner/organizacional ao qual a conta FTD é adicionada.

Nessa configuração, a conta FTD é adicionada no contêiner Usuários com o nome de usuário ftd.admin@example.com.

Clique com o botão direito do mouse em Usuários e navegue até Novo > Usuário.

Active Directory	Users and Comp	puters				-	×
File Action View	w Help						
🗢 🔿 🔁 📆	X 🗈 🗙 🛙	0 🔒 🛛	Þ	1 🗏 🐮 🛯	r 🗾 🔍		
Active Directory Users and Com Saved Queries Saved Queries Builtin Builtin Builtin Computers Domain Controllers Managed Service Accour Users Delegate Control Eind		Name DefaultAcc Denied ROI DonsAdmins DonsUpdate Domain Ad Domain Co trol	o D s P i n	Type User Security Group Security Group Security Group Security Group Security Group Security Group	Description A user account manage. Members in this group of DNS Administrators Gro. DNS clients who are per. Designated administrato All workstations and ser. All domain controllers i All domain guests		^
	New           All Tasks           View           Refresh           Export List           Properties	>	ers	Computer Contact Group InetOrgPerson msDS-KeyCreder msDS-ResourceP msDS-ShadowPr	ntial PropertyList incipalContainer		
< Creates a new item in	Help	WseAlertA WseAllow WseAllow		msImaging-PSP: MSMQ Queue Al Printer User Shared Folder	ias		~

### 2. Percorra o Assistente de Novo Objeto - Usuário.

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

New Object - User		×
🤱 Create in: exar	nple.com/Users	
Password:	•••••	
Confirm password:	•••••	
User must change passw	ord at next logon	
User cannot change pass	sword	
Password never expires		
Account is disabled		
	< Back Next >	Cancel
New Object - User		~
New Object - User		×
New Object - User	nple.com/Users	×
New Object - User Create in: exam When you click Finish, the for	nple.com/Users	×
New Object - User Create in: exam When you click Finish, the for Full name: FTD Admin	nple.com/Users Mowing 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 blowing 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 Mowing object will be created: @example.com t.	×
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 Mowing object will be created: @example.com 8.	×
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 Mowing 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	mple.com/Users Mowing 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	mple.com/Users Mowing 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	mple.com/Users Mowing object will be created: @example.com	×

3. Verifique se a **conta FTD** foi criada. Duas contas adicionais são criadas: **administrador de TI** e **usuário de teste**.

Active Directory Users and Computers					х
File Action View Help					
🗢 🔿 🖄 📷 🖌 🗈  🗙 🛙	🖹 🗟 📑 📔 🖬	1 🙎 🔌 🛍 🦷	7 🗾 🗽		
<ul> <li>Active Directory Users and Com</li> <li>Saved Queries</li> <li>Saved Queries</li> <li>Builtin</li> <li>Computers</li> <li>Domain Controllers</li> <li>ForeignSecurityPrincipals</li> <li>Managed Service Accour</li> <li>Users</li> </ul>	Name DefaultAcco DefaultAcco DefaultAcco Domain ROD DosUpdateP Domain Ad Domain Co Domain Co Domain Gue Domain Gue Domain Gue Domain Gue Domain Gue Comain Gue Comain Gue Comain Co Comain Co	Type User Security Group Security Group User User User	Description A user account manage Members in this group c DNS Administrators Gro DNS clients who are per Designated administrato All workstations and ser All domain controllers i All domain guests All domain users Designated administrato Members of this group Members of this group Built-in account for gue		
	Protected Us	Security Group Security Group	Members of this group Members of this group		
	Read-only D	Security Group Security Group	Members of this group Designated administrato		
< >	Test User	User			¥

#### Criar grupos do AD e adicionar usuários aos grupos do AD (opcional)

Embora não sejam necessários para autenticação, os grupos podem ser usados para facilitar a aplicação de políticas de acesso a vários usuários, bem como a autorização LDAP.

Neste guia de configuração, os grupos são usados para aplicar configurações de política de controle de acesso posteriormente usando a identidade do usuário no FMC.

1. Em **Usuários e Computadores do Ative Diretory**, clique com o botão direito do mouse no contêiner ou na unidade organizacional à qual o novo grupo será adicionado.

Neste exemplo, o grupo Administradores de AnyConnect é adicionado ao contêiner Usuários. Clique com o botão direito do mouse em **Usuários** e navegue até **Novo > Grupo**.

Active Directory Users and Con	puters			-	х
File Action View Help					
🗢 🔿 🙍 🚾 🔏 🗈  🗙 🛛	🗉 🖬 📑 🖬	1 🗏 🐮 🛯	r 🗾 🍇		
Active Directory Users and Com Saved Queries Saved Queries Save	Name DefaultAcco Denied ROD DnsAdmins DnsUpdateP Domain Ad Domain Co ntrol ers	Type User Security Group Security Group Security Group Security Group Security Group Security Group Security Group Security Group	Description A user account manage Members in this group c DNS Administrators Gro DNS clients who are per Designated administrato All workstations and ser All domain controllers i All domain guests All domain users		~
All Tasks View Refresh Export List Properties Help	> > A Read-only A Schema A	Computer Contact Group InetOrgPerson msDS-KeyCreder msDS-ResourceF msDS-ShadowPr msImaging-PSPs MSMQ Queue Al Printer User	itial ropertyList incipalContainer ias		
Creates a new item in this container.	(m	Shared Folder			v

2. Vá para o Assistente de Novo Objeto - Grupo.

New Object - Group	×						
Create in: example.com/Users							
Group name:							
AnyConnect Admins							
Group name (ore-Windows 20	103):						
AnyConnect Admins							
Group scope	Group type						
O Domain local	Security						
Global	Obistribution						
OUniversal							
	OK Cancel						

3. Verifique se o grupo foi criado. O grupo Usuários de AnyConnect também foi criado.

Active Directory Users and Com		_	×		
File Action View Help					
🗢 🔿 🖄 📰 🖬	è   🛛 🖬   🐍 🔌 🛍 '	7 🗾 🐍			
Active Directory Users and Com Saved Queries Example.com Builtin Computers Domain Controllers Managed Service Accour Users	Name AnyConnect Admins AnyConnect Users Calo Cert Publishers Cloneable Domain C Cloneable Domain C DefaultAccount DefaultAccount DonsAdmins DonsUpdateProxy Domain Admins Domain Computers Domain Computers Domain Computers Domain Guests Domain Guests Domain Guests Comain Guests Domain Guests Comain Guests Enterprise Admins Enterprise Read-only FTD Admin Group Policy Creator Guest T Admin Key Admins	Type Security Group Security Group User Security Group Security Group User User User	Description Built-in account for ad Members of this group 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 c Built-in account for gue		

4. Clique com o botão direito do mouse no grupo do(s) usuário(s) e escolha **Propriedades**. Nesta configuração, o usuário Administrador de TI é adicionado ao grupo Administradores de AnyConnect e o usuário de teste é adicionado ao grupo Usuários de AnyConnect.

Active Directory Users and Com		-	х		
File Action View Help					
🗢 🔿 🖄 🖂 🖌 🖾  🗶 🛙	i 🗟 🗟 🛛 🖬 😤	ዾ 🛍 🔻 🗾 🎗	8		
Active Directory Users and Com Saved Queries Saved Queries	Name AnyConnect Admins	Type Security Group	Description Add to a group		^
will example.com     will Builtin     will Computers     will Domain Controllars	Cert Publishers	User Security Group	Buil Move Mer Send Mail		
ForeignSecurityPrincipals Managed Service Accounts	Cloneable Domain C DefaultAccount	Security Group User	Mer All Tasks	>	
Managed Service Accour Users	Denied RODC Passw DosAdmins	Security Group Mer Cut Security Group DNS Delete Security Group DNS o	Mer Cut DN: Delete DN: Rename		
	Domain Admins	Security Group Security Group Security Group	All c		
	B Domain Guests	Security Group	Help All comoin gueso		
	Domain Users Enterprise Admins Enterprise Key Admins Enterprise Read-only FTD Admin	Security Group Security Group Security Group Security Group User	All domain users Designated administrato Members of this group Members of this group		
	Group Policy Creator Guest	Security Group User User	Members in this group c Built-in account for gue		
< >>	All Key Admins	Security Group	Members of this group		~
Renames the current selection.					

### 5. Na guia **Membros**, clique em **Adicionar**.

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

Insira o usuário no campo e clique em **Check Names** para verificar se o usuário foi encontrado. Depois de verificado, clique em **OK**.

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

Verifique se o usuário correto foi adicionado e clique no botão OK. O usuário de teste também é adicionado ao grupo Usuários de AnyConnect seguindo as mesmas etapas.

AnyConnect A	AnyConnect Admins Properties						
General Mem	bers	Member Of	Managed By				
Members:							
Name		Active Dire	ectory Domain om/Users	Services Folder			
Add	]	Remove	ОК	Cancel	Ą	ply	

Copiar a raiz do certificado SSL do LDAPS (necessário apenas para LDAPS ou STARTTLS)

1. Pressione **Win+R** e digite **mmc.exe**. em seguida, clique em OK.

_	-	
1000	0.	-
-		
_		

0	Type the name of a program, folder, document, or Interne resource, and Windows will open it for you.	:t
<u>O</u> pen:	mmc.exe	v
	OK Cancel <u>B</u> rowse	

2. Navegue até Arquivo > Adicionar/Remover Snap-in...

🖾 Co	nsole1 - (Conso	le Root]			- п ×
File	Action Vie	w Favorites	Window	Help	
4	New Open		Ctrl+N Ctrl+O	Actions	
	Save Save		Ctrl+S	There are no items to show in this view. Console Root	-
	Add/Remove Options	Snap-in	Ctrl+M	More Actions	٠
	1 dnsmgmt				
	2 dsa				
	Exit				
Enables	you to add sna	p-ins to or rem	ove them fro	om the snap-in console.	

3. Em Snap-ins disponíveis, selecione Certificados e clique em Adicionar.

Add or Remove Snap-ins			:	×		
You can select snap-ins for this console from those available on your computer and configure the selected set of snap-ins. For extensible snap-ins, you can configure which extensions are enabled.						
Available snap-ins:			Selected snap-ins:			
Snap-in	Vendor	^	Console Root Edit Extensions			
Active Directory Do	Microsoft Cor Microsoft Cor		Bemove			
Active Directory Use	Microsoft Cor Microsoft Cor		Move <u>U</u> p			
AUSI Edit	Microsoft Cor		Move Down			
Certificates	Microsoft Cor Microsoft Cor Microsoft Cor		<u>A</u> dd >			
Component Services	Microsoft Cor Microsoft Cor Microsoft Cor					
T Disk Management	Microsoft and	~	Advanced	1		
Description: The Certificates snap-in all	ows you to browse	the	e contents of the certificate stores for yourself, a service, or a computer.			
			OK Cancel			

4. Selecione Conta do computador e clique em Avançar.

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

Clique em Finish.

Select Computer	х
Select the computer you want this snap-in to manage.         This snap-in will always manage: <ul> <li>Local computer: (the computer this console is running on)</li> <li>Another computer:</li> <li>Another computer:</li> <li>Allow the selected computer to be changed when launching from the command line. This only applies if you save the console.</li> </ul>	
< Back Finish Cancel	

#### 5. Agora clique em OK.

Add or Remove Snap-ins							х
You can select snap-ins for this console from those available on your computer and configure the selected set of snap-ins. For extensible snap-ins, you can configure which extensions are enabled.							
Available snap-ins:				Selected snap-ins:			
Snap-in	Vendor	^		Console Root		Edit Extensions	
Active Directory Do	Microsoft Cor			Certificates	(Local Computer)	<u>R</u> emove	
Active Directory Site	Microsoft Cor						
Active Directory Use	Microsoft Cor					Move Up	
ADSI Edit	Microsoft Cor					1.1010 00	-
Authorization Manager	Microsoft Cor					Move <u>D</u> own	
Certificate Templates	Microsoft Cor		Add >				
Certificates	Microsoft Cor						
Certification Authority	Microsoft Cor						
Component Services	Microsoft Cor						
Computer Managem	Microsoft Cor						
E Device Manager	Microsoft Cor						
T Disk Management	Microsoft and	$\checkmark$				Advanced	
		-	1				
Description:							_
The Certificates snap-in allo	ows you to browse	the	contents of the	certificate stores fo	or yourself, a service,	or a computer.	
						OK Cancel	

6. Expanda a pasta **Pessoal** e clique em **Certificados**. O certificado usado pelo LDAPS é emitido para o **Fully Qualified Domain Name (FQDN)** do servidor Windows. Neste servidor, há 3 certificados listados.

- Um certificado de CA emitido para e por example-WIN2016-CA.
- Um certificado de identidade emitido para WIN2016 por example-WIN2016-CA.
- Um certificado de identidade emitido para win2016.example.com por example-WIN2016-CA.

Neste guia de configuração, o FQDN é win2016.example.com e, portanto, os dois primeiros certificados não são válidos para uso como o certificado SSL do LDAPS. O certificado de identidade emitido para win2016.example.com é um certificado emitido automaticamente pelo serviço de CA do Windows Server. Clique duas vezes no certificado para verificar os detalhes.

ᡖ Console1 - [Console Root\Certific	ates (Local Computer)\Personal\C	ertificates]		-	- 🗆 🗙
File Action View Favorites	Window Help				- 8 ×
🗢 🏟 🖄 📆 📋 🙆 😹					
Console Root     Certificates (Local Computer)     Certificates (Local Computer)     Personal     Certificates     Trusted Root Certification     Intermediate Certification     Intermediate Certificates     Untrusted Publishers     Untrusted Certificates     Trusted People     Client Authentication Issue     Preview Build Roots     Local NonRemovable Cert     Remote Desktop	Issued To Sexample-WIN2016-CA WIN2016 Win2016.example.com	Issued By example-WIN2016-CA example-WIN2016-CA example-WIN2016-CA	Expiration Da 4/19/2060 4/27/2025 4/28/2021	Actions Certificates More Actions	- ,
Certificate Enrollment Req     Smart Card Trusted Roots     Trusted Devices     Web Hosting     Windows Live ID Token Iss	<		>		
Personal store contains 3 certificates.					

7. Para ser utilizado como certificado SSL LDAPS, o certificado deve cumprir os seguintes requisitos:

- O nome comum ou nome alternativo do assunto DNS corresponde ao FQDN do Windows Server.
- O certificado tem autenticação de servidor no campo Uso avançado de chave.

Na guia **Detalhes** do certificado, selecione **Assunto** e **Nome alternativo do assunto**. O FQDN win2016.example.com está presente.

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

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

Em Uso avançado de chave, a autenticação do servidor está presente.

🙀 Certificate	×
General Details Certification	Path
Show: <all></all>	~
Field	Value ^
Subject Public key Public key parameters	win2016.example.com RSA (2048 Bits) 05 00
Certificate Template Name	e DomainController
Subject Key Identifier	[1]SMIME Capability: Object I 30 b7 2b 4e 48 0f 2f 17 17 e6 KevID=3d 9f 26 37 fb 11 1f 4
Server Authentication (1.3.6.	1.5.5.7.3.1)
	Edit Properties Copy to File
	ОК

8. Uma vez confirmado, na guia **Caminho de Certificação**, selecione o certificado superior que é o certificado raiz da CA e clique em **Exibir Certificado**.

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

9. Isso abre os detalhes do certificado para o certificado CA raiz.

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	

Na guia Detalhes, clique em Copiar para arquivo...

Certificate		×
General Details Certification Path		
Show: <all></all>	~	
Field	Value	^
Version Serial number Signature algorithm Signature hash algorithm Signature hash algorithm Valid from 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	dit Properties Copy to File	
	OK	:

10. Use o Assistente para Exportação de Certificados que exporta a CA raiz no formato PEM.

÷	🚰 Certificate Export Wizard	^
	Welcome to the Certificate Export Wizard	
	This wizard helps you copy certificates, certificate trust lists and certificate revocation lists from a certificate store to your disk.	
	A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.	
	To continue, dick Next.	
	<u>N</u> ext Cano	el

Selecione X.509 codificado por Base 64

xport File Format Certificates can be	exported in a variety of file formats.
Select the format yo	ou want to use:
O DER encoded	d binary X.509 (.CER)
Base-64 enco	oded X.509 (.CER)
○ Cryptograph	ic Message Syntax Standard - PKCS #7 Certificates (.P7B)
Include a	Il certificates in the certification path if possible
O Personal Info	ormation Exchange - PKCS #12 (.PFX)
Include a	Il certificates in the certification path if possible
Delete th	e private key if the export is successful
Export al	l extended properties
Enable of	ertificate privacy
O Microsoft Ser	rialized Certificate Store (.SST)

Selecione o nome do arquivo e o local para o qual será exportado.

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

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

Agora clique em Concluir.

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

11. Agora vá para o local e abra o certificado com um bloco de notas ou algum outro editor de texto. Essa ação mostra o certificado em formato PEM. Salve-o para usar mais tarde.

#### ----BEGIN CERTIFICATE----

```
MIIDCDCCAfCgAwIBAgIQE4ZG5Z1wT6lONTjooEQyMTANBgkqhkiG9w0BAQsFADAd
MRswGQYDVQQDExjleGFtcGxlLVdJTjIwMTYtQ0EwIBcNMjAwNDI3MTQ1MDU5WhgP
MjA2MDA0MTkxNDUwNTlaMB0xGzAZBgNVBAMTEmV4YW1wbGUtV010MjAxNi1DQTCC
ASIwDQYJKoZIhvcNAQEBBQADqqEPADCCAQoCqqEBAI8qhT719NzSQpoQPh0YT67b
Ya+PngsxMyvkewP33QLTAWw1HW1Tb9Mk5BDWOItTaVsgHwPBfd++M+bLn3AiZnHV
OO+k6dVVY/E5qVkEKSGoY+v940S2316lzdwReMOFhgbc2qMertIoficrRhihonuU
Cjyeub3CO+meJUuKom2R47C0D35TUvo/FEHGgXJFaJS1se2UrpN07KEMkfAlLPuM
aob4XE/OzxYQpPa18djsNnskfcFqD/HOTFQN4+SrOhHWlRnUIQBUaLdQaabhipD/
sVs5PneYJX8YKma821uYI6j90YuytmsHBtCieyC062a8BKqOL7N86HFPFkMA3u8C
AwEAAaNCMEAwDgYDVR0PAQH/BAQDAgGGMA8GA1UdEwEB/wQFMAMBAf8wHQYDVR00
BBYEFD2fjjf7ER9EM/HCxCVFN5QzqEdvMA0GCSqGSIb3DQEBCwUAA4IBAQB31ZJo
vzwVD3c5Q1nrNP+6Mq62OFpYH91k4Ch9S5g/CEOemhcwg8MDIoxW2dTsjenAEt7r
phFIHZoCoSyjBjMgK3xybmoSeg8vBjCXseYNGEmOc9KW1oFmTOvdNVIb7Xpl1IVa
6tALTt3ANRNgREtxPA6yQbthKGavW0Anfsojk9IcDr2vp0MTjlBCxsTscbubRl+D
dLEFKQqmMeYvkVf+a7a64mqPZsG3Uxo0rd6cZxAPkq/ylcdwNSJFfQV3DqZq+R96
9WLCR3Obig6xyo9Zu+lixcWpdrbADO6zMhbEYEhkhOOjBrUEBBI6Cy83iTZ9ejsk
KgwBJXEu33PplW6E
----END CERTIFICATE-----
```

12. (Opcional) Na situação em que há vários certificados de identidade que podem ser usados por LDAPS e há incerteza sobre qual é usado, ou não há acesso ao servidor LDAPS, é possível extrair a CA raiz de uma captura de pacote feita no servidor Windows ou FTD após.

#### Configurações do FMC

#### Verificar licenciamento

Para implantar a configuração do AnyConnect, o FTD precisa ser registrado no servidor de Smart Licensing e uma licença válida Plus, Apex ou Somente VPN deve ser aplicada ao dispositivo.

1. Navegue até Sistema > Licenças > Smart Licensing.

Overview	Analysis	Policies	Devices	Objects	AMP	Intelligence					Deplo	y 🔍 💁	ystem Help 🔻	admin <del>v</del>
						Configuration	Users	Domains	Integration	Updates	Licenses •	Health 🔻	Monitoring •	Tools •
										Sm	art Licenses			
										Cla	ssic Licenses			

2. Verifique se os dispositivos estão em conformidade e se foram registrados com êxito. Verifique se o dispositivo foi registrado com uma licença Apex, Plus ou Somente VPN do AnyConnect.

Overview Analysis Policies	D	evices Objects	AMP	Intelligence						Deploy 🔒	System	Help 🔻 admir
		(	Configuratio	n Users	Domains	Integration	Updates	Licenses	<ul> <li>Smart Licen</li> </ul>	ses Health	• Monit	oring • Too
Smart License Status					<u>Ciaco Sm</u>	art Software M	maan 😐 🥹					
Usage Authorization:	0	Authorized (Last S	ynchronized (	On May 03 2020	))							
Product Registration:	0	Registered (Last R	enewed On M	lar 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 Stat	us	Device Type			Domain	Gro	up
Firepower Management	Cen	ter Virtual (2)			0							
Þ 💋 Base (2)					0							
🖻 💋 Mahware (1)					0							
D C Threat (2)					0							
🖻 📁 URL Filtering (2)					0							
4 🥬 AnyConnect Apex (1)					0							
FTD-2 192.168.1.17 · Cisco Firepo	ower	Threat Defense for V	/MWare - v6.3	3.0	0		Cisco Firepower	Threat Defen	se for VMWare	Global	N/A	
AnyConnect Plus (0)												
AnyConnect VPN Only (0)												

#### Configurar realm

1. Navegue até Sistema > Integração.

Overview	Analysis	Policies	Devices	Objects	AMP	Intelligence					Deploy	- e,	System	Help 🔻	admin <del>v</del>	
						Configuration	Users	Domains	Integration	Updates	Licenses *	Health	<ul> <li>Mor</li> </ul>	itoring •	Tools *	

2. Em Territórios, clique em Novo território.

Overview Analysis Policie	s Devices Objects	AMP Intell	ligence					Deploy	🛛 🍳 Sys	tem Help <del>v</del>	admin <del>v</del>
			Configuration	Users	Domains	Integration	Updates	Licenses 🔻	Health <b>*</b>	Monitoring •	Tools <b>*</b>
Cloud Services Realms	Identity Sources	Streamer Ho	ost Input Client	Smar	t Software S	atellite					
									K Compa	are realms 🛛 🔅	New realm
Name	Description	Domain	Туре		Base DN	Grou	IP DN	Group Attri	bute	State	

3. Preencha os campos apropriados com base nas informações coletadas do servidor Microsoft. Quando terminar, clique em **OK**.

lame *	LAB-AD		
Description			
Гуре *	AD	~	
AD Primary Domain *	example.com		ex: domain.com
AD Join Username			ex: user@domain
AD 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. Na nova janela, selecione **Diretório**, se ainda não tiver sido escolhido, clique em **Adicionar diretório**.

Overview	Analysis	Policies	Devices	Objects	AMP	Intellige	nce			Deploy	🖉 0, Sys	tem Help 🔻	admin 🔻
				Configur	ration	Users	Domains	Integration	Updates	Licenses 🔻	Health 🔻	Monitoring •	Tools •
LAB-AD Enter Descript	ion											Save	Cancel
Directory	Realm Cont	figuration	User Down	nload									
													dd directory

Preencha os detalhes do servidor do AD. Observe que, se o FQDN for usado, o FMC e o FTD não serão vinculados com sucesso, a menos que o DNS esteja configurado para resolver o FQDN.

Para configurar o DNS para o FMC, navegue para **System > Configuration** e selecione **Management Interfaces**.

Para configurar o DNS para o FTD, navegue para **Devices > Platform Settings**, crie uma nova política ou edite uma atual e vá para o DNS.

Add directory	? ×
Hostname / IP Address	win2016.example.com
Port	389
Encryption	○ STARTTLS ○ LDAPS ④ None
SSL Certificate	✓ ③
	OK Test Cancel

Se LDAPS ou STARTTLS for usado, clique no símbolo verde +, dê um nome ao certificado e copie o certificado de CA raiz no formato PEM. Clique em **Salvar** quando terminar.

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/ sVs5PneYJX8YKma821uY16j90YuytmsHBtCieyC062a8BKq0L7N86HFPFkMA3u8C AwEAAaNCMEAwDgYDVR0PAQH/BAQDAgGGMA8GA1UdEwEB/wQFMAMBAf8wHQYDVR00 BBYEFD2fJjf7ER9EM/HCxCVFN5QzqEdvMA0GCSqGSIb3DQEBCwUAA4IBAQB31ZJo vzwVD3c5Q1nrNP+6Mq62OFpYH91k4Ch9S5g/CEOemhcwg8MDIoxW2dTsjenAEt7r phFIHZoCoSyjBjMgK3xybmoSeg8vBjCXseYNGEmOc9KW10FmT0vdNVIb7Xpl1IVa 6tALTt3ANRNgREtxPA6yQbthKGavW0Anfsojk91cDr2vp0MTjlBCxsTscbubRl+D dLEFKQqmMeYvkVf+a7a64mqPZsG3Ux00rd6cZxAPkq/ylcdwNSJFfQV3DgZg+R96 9WLCR3Obig6xyo9Zu+lixcWpdrbADO6zMhbEYEhkhO0jBrUEBBI6Cy83iTZ9ejsk KgwBJXEu33PpIW6E FND_CERTIFICATE	~
	$\sim$
Encrypted, and the password is:	
Save	Cancel

Selecione a CA raiz recém-adicionada na lista suspensa ao lado do certificado SSL e clique em STARTTLS ou LDAP.
Edit directory	? >	<
Hostname / IP Address	win2016.example.com	
Port	636	
Encryption	○ STARTTLS	
SSL Certificate	LDAPS_ROOT 💙 💿	
	OK Test Cancel	

Clique em Testar para garantir que o FMC possa ser associado com sucesso ao nome de usuário e à senha do diretório fornecidos na etapa anterior.

Como esses testes são iniciados a partir do FMC e não através de uma das interfaces roteáveis configuradas no FTD (como interno, externo, dmz), uma conexão bem-sucedida (ou com falha) não garante o mesmo resultado para a autenticação do AnyConnect porque as solicitações de autenticação LDAP do AnyConnect são iniciadas a partir de uma das interfaces roteáveis do FTD.

Para obter mais informações sobre como testar as conexões LDAP no FTD, revise as seções AAA de teste e Captura de pacotes na área Solução de problemas.

Status	
$(\mathbf{i})$	Test connection succeeded
	(OK)

5. Em **Download do Usuário**, faça o download dos grupos que são usados para a identidade do usuário em etapas posteriores.

Marque a caixa **Download users** and groups e a coluna para **Available Groups** será preenchida com os grupos configurados no Ative Diretory.

Os grupos podem ser incluídos ou excluídos. No entanto, por padrão, todos os grupos encontrados no DN de grupo são incluídos.

Usuários específicos também podem ser incluídos ou excluídos. Os grupos e usuários incluídos estão disponíveis para serem selecionados para a identidade do usuário posteriormente.

Ao concluir, clique em Save (Salvar).

Overview Analysis Policies Devices Objects AMP Intel	ligence			Deploy	0 System He	lp 🔻 admin 🔻
	Configuration Users	Domains Integrati	on Upd	lates Licenses •	Health  Monitor	ing • Tools •
LAB-AD Enter Description				You have uns	aved changes 🔡 Sav	e 🕄 Cancel
Directory Realm Configuration User Download						
Download users and groups						
Begin automatic download at 8 V PN V America/New York Repeat Every	24 V Hours					
Available Groups 😋	Groups to Include (2)			Groups to Exclude (0	)	
a Search by name	AnyConnect Admins		8	None		
AnyConnect Admins	AnyConnect Users		8			
A DnsUpdateProxy						
A WseRemoteAccessUsers						
A WseInvisibleToDashboard						
Allowed RODC Password Replication Group						
A Enterprise Key Admins Include						
🛃 Domain Admine Add to						
A WseAlertAdministrators						
🝰 Event Log Readers						
A Replicator						
🝰 Domain Guests						
A Windows Authorization Access Group						
Account Operators						
🝰 Hyper-V Administrators 🗸 🗸 🗸	The second se					
💑 System Managed Accounts Group	Enter User Indusion		Add	Enter User Exclusion		Add

#### 6. Ative o novo realm.

Overview Analysis Polici	es Devices Objec	ts AMP I	ntelligence							Deploy	0 Sys	stem Hel	p <del>v</del> admin <del>v</del>
			Configura	tion U:	sers I	Domains	Integra	tion Upda	ites Li	censes 🔻	Health *	Monitoria	ng ▼ Tools ▼
Cloud Services Realms	Identity Sources	eStreamer	Host Input	t Client	Smart	Software S	atellite						
											Comp	are realms	🔕 New realm
Name	Description	Domain	1	Туре	Bas	se DN		Group DN		Group Attri	bute	State	
LAB-AD		Global	4	AD	DC-	-example,DC	-com	DC=example,D	C=com	member			ቷ 🥒 🔁 🖯

7. Se LDAPS ou STARTTLS for usado, a CA raiz também precisa ser confiável pelo FTD. Para fazer isso, primeiro navegue até **Dispositivos > Certificados**.

Overview Analysis	Policie	s Dev	ices	Objects	AMP II	ntelligence		Deploy	0	System	Help 🔻	admin 🔻
Device Management	NAT	VPN 🔻	QoS	Platforn	n Settings	FlexConfig	Certificates					

Clique em Adicionar no canto superior direito.

Overview Analysis	Polici	es Devi	ices 0	Objects AMP In	telligence		Deploy	0	System	Help 🔻	admin v	
Device Management	NAT	VPN •	QoS	Platform Settings	FlexConfig	Certificates						
										0	Add	

Selecione o FTD e a configuração LDAP será adicionada; em seguida, clique no símbolo verde +.

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

Dê um nome ao ponto confiável e escolha Inscrição manual no menu suspenso Tipo de inscrição. Cole o certificado de CA raiz em formato PEM aqui e clique em **Salvar**.

Add Cert Enrollme	nt	? ×
Name*	LDAPS_ROOT	
Description		
CA Information	Certificate Parameters Key Revocation	
Enrollment Type:	Manual 👻	^
CA Certificate:*	<ul> <li>MIIDCDCCAfCgAwIBAgIQE4ZG5Z1wT6lONTjooEQyMTANBgkqhki</li> <li>G9w0BAQsFADAd</li> <li>MRswGQYDVQQDExJleGFtcGxlLVdJTjIwMTYtQ0EwIBcNMjAwNDI</li> <li>3MTQ1MDU5WhgP</li> <li>MjA2MDA0MTkxNDUwNTlaMB0xGzAZBgNVBAMTEmV4YW1wbGU</li> <li>tv0lOMjAxNi1DQTCC</li> <li>ASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAI8ghT719N</li> <li>zSQpoQPh0YT67b</li> <li>Ya+PngsxMyvkewP33QLTAWw1HW1Tb9Mk5BDWOItTaVsgHwPBf</li> <li>d++M+bLn3AiZnHV</li> <li>OO+k6dVVY/E5qVkEKSGoY+v940S2316lzdwReMOFhgbc2qMertIo</li> <li>ficrRhihonuU</li> <li>Cjyeub3CO+meJUuKom2R47C0D35TUvo/FEHGgXJFaJS1se2UrpN</li> <li>O7KEMkfA1LPuM</li> <li>aob4XE/OzxYQpPa18djsNnskfcFqD/HOTFQN4+SrOhHWlRnUIQBU</li> <li>aLdQaabhipD/</li> <li>vS5PneYJX8YKma821uYI6j90YuytmsHBtCieyC062a8BKgOL7N86</li> </ul>	~
Allow Overrides		
	Save	Cancel

Verifique se o ponto confiável criado foi selecionado e clique em Adicionar.

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

O novo ponto de confiança aparece sob o FTD. Embora mencione que a importação do certificado Identity é necessária, não é necessário para o propósito do FTD ser capaz de autenticar o certificado SSL enviado pelo servidor LDAPS e, portanto, esta mensagem pode ser ignorada.

Overview Analysis Polici	es Devices Object	ts 🛛 AMP Intelliç	gence	Deploy 🔒	System Help	▼ admin ▼
Device Management NAT	VPN VOS Pla	tform Settings Fle	exConfig Certificates			
					O	Add
Name	Domain	Enrollment Type	Status			
4 🗐 FTD-1						
FTD-1-PKCS12	Global	PKCS12 file	CA D		£	Φ 🖬
4 🗐 FTD-2						
FTD-2-PKCS12	Global	PKCS12 file	CA 🔍 ID		Ð	Φ 🗎
FTD-2-Selfsigned	Global	Self-Signed	O CA ID		U.	Φ 🗎
LDAPS_ROOT	Global	Manual	🔍 CA 🔺 ID 🔺 Identi	ity certificate import requir	red 📝	Φ 🗎

## Configurar AnyConnect para autenticação do AD

1. Estas etapas supõem que nenhuma política de vpn de acesso remoto já tenha sido criada. Se uma política já foi criada, clique no botão Editar dessa política e vá para a etapa 3.

Navegue até **Devices > VPN > Remote Access**.

Overview Analysis	Policies	Device	s Obje	ects AMP Intel	ligence			Deploy	0	System	Help 🔻	admin 🔻
Device Management	NAT	VPN •	QoS	Platform Settings	FlexConfig	Certificates						
		Site To S	ite									
		Remote /	Access									
		Troubles	hooting	1								

Clique em Adicionar para criar uma nova política de VPN de acesso remoto



2. Conclua o **Assistente de Política de VPN de Acesso Remoto**. Em **Atribuição de política**, especifique um nome para a política e os dispositivos aos quais a política é aplicada.

Overview Analysis Policies Objects AMP Intelligence Deploy	🔒 🚱 System Help 🔻 admin 🔻									
Device Management NAT VPN • Remote Access QoS Platform Settings FlexConfig Certificates										
Remote Access VPN Policy Wizard										
1 Policy Assignment 2 Connection Profile 3 AnyConnect 4 Access & Certificate 5 Summary										
Targeted Devices and Protocols	~									
This wizard will guide you through the required minimal steps to configure the Remote Access VPN policy with a new user-defined connection profile.										
Before you start, ensure th configuration elements to be	in place to									
Name:* PTD-2-RA-Policy complete Remote Access VPN	Policy.									
Description: Authentication Server	anun Greun									
to authenticate VPN dients.	erve drowe									
VPN Protocols: M SSL M IPsec-IKEv2 AnyConnect Client Package										
Targeted Devices: Available Devices Selected Devices Make sure you have AnyConn for VPV Client downloaded of	ect package ar you have									
it during the wizard.	to download									
Device Interface										
Interfaces should be already or targeted <u>devices</u> so that they	onfigured on can be used									
as a security zone or interfa enable VPN access.	ce group to									
	~									
Back Next Cancel										

Em Perfil de conexão, especifique o nome do Perfil de conexão que também é usado como o alias de grupo que os usuários de AnyConnect visualizam quando se conectam.

Especifique o realm criado anteriormente em Servidor de autenticação.

Especifique que os clientes AnyConnect são endereços IP atribuídos.

Especifique a política de grupo padrão usada para esse perfil de conexão.

Overview Analysis Policies Devices Objects   AMP	Intelligence	Deploy 🔒 System Help 🕶 admin	•
Device Management NAT VPN + Remote Access QoS	Platform Settings FlexConfig Certificates		
Remote Access VPN Policy Wizard			
Policy Assignment     2 Connection Profile     3	AnyConnect > ( Access & Certificate > ( Summary)		
Connection Profile:			^
Connection Profiles specify the tunne accomplished and how addresses are	group policies for a VPN connection. These policies pertain to creating the tunnel itself, assigned. They also include user attributes, which are defined in group policies.	how AAA is	
Connection Profile Name:*	General		
	This name is configured as a connection alias, it can be used to connect to the VTN gateway		4
Authentication, Authorization & A	ccounting (AAA):		
Specify the method of authentication	(AAA, certificates or both), and the AAA servers that will be used for VPN connections.		
Authentication Method:	AAA Only 👻		
Authentication Server:*	LAB-AD V G+ (Realm or RADIUS)		
Authorization Server:	Y 🕄 (RADIUS)		
Accounting Server:	Y (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 address pools. When multiple options are selected, IF A server, DHCP server and IP address pool.	' address	
Use AAA Server (RADIUS	niy) 🕕		
Use DHCP Servers			
M Use IP Address Pools			
IPv4 Address Pools:	AnyConnect-Pool 🥜		
IPv6 Address Pools:	/		
Group Policy: A group policy is a collection of user- or create a Group Policy object.	riented session attributes which are assigned to client when a VPN connection is establi	shed. Select	
Group Policy:*	DftGrpPolicy 👻 🗯		
	Edit Group Policy		~
		Back Next Cancel	

Em AnyConnect, carregue e especifique os pacotes usados do AnyConnect.

Overview Analysis Polic	ies	Devices Objects	AMP	Intelligence					Deploy	0 <sub>5</sub> System	Help 🔻	admin <del>v</del>
Device Management NAT	V	PN > Remote Access	QoS	Platform Settings	FlexConfig	Certific	ates					
Remote Access VPN F	Poli	cy Wizard										
1 Policy Assignment	0	) Connection Profile	3	AnyConnect	Access &	Certifica	te > 🗿 Sumn	ary				
	An The initi	Connect Client Image VPN gateway can automatic ated. Minimize connection set	ally down	nload the latest AnyConr by choosing the appropria	rect package to t ate OS for the sel	he client o	levice when the VPN co	nnection is				^
	Dov	inload AnyConnect Client pad	kages fro	m Cisco Software Downlo	ad Center.			-				
						5	how Re-order buttons	8				
	2	AnyConnect File Object	Name	AnyConnect Client	Package Name		Operating System					
	V	anyconnect-linux64-4.7.03	052-we	anyconnect-linux64-4	4.7.03052-webde;	ploy-k9	Linux	*				
	V	anyconnect-win-4.7.00136	webde	anyconnect-win-4.7.0	00136-webdeploy	-k9.pkg	Windows	*				~
									Back	Next	Ca	incel

Em **Acesso e certificado**, especifique a interface que os usuários de AnyConnect acessam para o AnyConnect.

Crie e/ou especifique o certificado usado pelo FTD durante o handshake SSL.

Certifique-se de que a caixa de seleção **Política de controle de acesso de contorno** para tráfego descriptografado (sysopt permit-vpn) esteja desmarcada para que a identidade do usuário criada posteriormente entre em vigor para conexões RAVPN.

Overview Analysis Policies Devices Objects AMP	Intelligence	Deploy	🔍 System	Help 🔻	admin 🔻
Device Management NAT VPN > Remote Access QoS	Platform Settings FlexConfig Certificates				
Remote Access VPN Policy Wizard					
Policy Assignment     2 Connection Profile     3	AnyConnect 🔰 🖪 Access & Certificate 🔰 🌖 Summary 🔄				
Network Interface for I	ncoming VPN Access				
Select or create an Interface connections.	Group or a Security Zone that contains the network interfaces users will access for VPN	i .			í í
Interface group/Security Zo	ne:" outside-zone V Q+				
	Enable DTLS on member interfaces				
Device Certificates					
Device certificate (also called certificate which is used to as	Identity certificate) identifies the VPN gateway to the remote access clients. Select a thenticate the VPN gateway.				
Certificate Enrollment:*	FTD-2-Selfsigned Y				
	Enroll the selected certificate object on the target devices				
Access Control for VPN	Traffic				
All decrypted traffic in the VP bypass decrypted traffic from	I tunnel is aubjected to the Access Control Policy by default. Select this option to the Access Control Policy.				
Bypass Access Control po This option bypasses the AAA server are still applied	icy for decrypted traffic (sysopt permit-vpn) ccess Control Policy Inspection, but VPN filter ACL and authorization ACL downloaded from to VPN traffic.				
		Back	Next	<b>_ _ _ _</b>	ancel

## Em Resumo, revise a configuração e clique em Concluir.



3. Na Política de VPN de Acesso Remoto, clique em editar para o Perfil de Conexão apropriado.

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		E Policy Assignments (1)
		0
Name	AAA Group Policy	
DefaultWEBVPNGroup	Authentication: None Et Dft:GrpPolicy Authorization: None Accounting: None	/ 0
General	Authentication: LAB-AD (AD) Ex Dft:GrpPolicy Authorization: Idente Accounting: Acres	20

Verifique se o servidor de autenticação foi definido para o realm criado anteriormente.

Em **Configurações avançadas**, a opção **Habilitar gerenciamento de senha** pode ser marcada para permitir que os usuários alterem a senha quando a senha expirar ou antes.

No entanto, essa configuração exige que o realm use LDAPS. Se alguma alteração tiver sido feita, clique em **Salvar**.

Edit Connection Pr	ofile			? ×
Connection Profile:* Group Policy:*	General DfltGrpPolic Edit Group Po	y licy	<b>~</b> ©	
Client Address Assign	ment AA	A Aliases		
Authentication				
Authentication Meth	nod:	AAA Only		*
Authentication Serv	er:	LAB-AD (AD)		*
Use secondary a Authorization Authorization Serve	uthentication r:	Allow connection only	/ if user exists in authorizat	▼ ion database
Accounting Server:				×
Advanced Settin	gs			
Strip Realm from	n username			
Strip Group from	username			
Enable Password     Notify User     Notify user on the second secon	days price days price day of passy	t or to password expiration vord expiration		
				Save Cancel

Quando terminar, clique em Salvar no canto superior direito.



Ativar política de identidade e configurar políticas de segurança para identidade do usuário

1. Navegue até Policies > Access Control > Identity.



Crie uma nova política de identidade.

Overview Analysis Policies Devices O	bjects AMP Intelligence	0	Deploy 🔒 System Help 🔻 admin 🔻
Access Control > Identity Network Discovery	Application Detectors Correlation	an Actions •	
			Object Management Access Control
Identity Policy	Domain	Status	Last Modified
	-	There are no policies created. Add a new polic	v

Especifique um nome para a nova política de identidade.

	D-2 Identity Policy
Description	

## 2. Clique em Adicionar Regra.



3. Especifique um **Nome** para a nova regra. Verifique se ela foi ativada e se a ação foi definida como Autenticação passiva.

Clique na guia **Realm e configurações** e selecione o realm criado anteriormente. Clique em **Add** quando terminar.

Add Rule

Name R	AVPN			🖌 Enabled	l Insert	into Category	*	Standard Rules	~
lction P	Passive Authentic	cation	*	Realm: LAB-AD (AD)	Authentication Protocol:	HTTP Basic Exclude I	HTTP User-	Agents: None	
Re	emote access VP	W sessions are a	actively authentic	ated by VPN. Other session	s use the rule Action.				
Zones	Networks	VLAN Tags	Ports					Realm & S	ettings
Realm *		LAB-AD (A	D)						
	ution authentical	tion if parries of	v VEN identity ca	nost he established	- W				
_ Use a	active authentical	tion it passive o	r vere identity ca	nnot be established					
• Require	red Field								
								Add	ancel

## 4. Clique em Salvar.

Overview Analysis Poli	icies Device	es Objects	AMP Intelli	gence				Dep	oloy 🧛 System	Help 🔻 ad	dmin <del>v</del>
Access Control + Identity	Network Disc	covery Appl	cation Detectors	Correlation	Actions •						
FTD-2 Identity Poli Enter Description	icy							You have	unsaved changes	Save <table-cell></table-cell>	Cancel
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 Protoco	al
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. navegue até Policies > Access Control > Access Control.

Overview Analysis Policies Devices Objects AMP Intelligence	Deploy	🧛 System	Help 🔻	admin <del>v</del>
Access Control + Identity Network Discovery Application Detectors Correlation Actions •				
Access Control				
Intrusion				
Malware & File				
DNS				
Identity				
5SL				
Prefilter				

## 6. Edite a **Política de Controle de Acesso** na qual o FTD está configurado.

Overview Analysis Policies	Devices Objects	AMP Intelligence				Deploy	🔒 System	Help 🔻 admin	Ŧ
Access Control > Access Control	Network Discovery	Application Detectors	Correlation	Actions <b>*</b>					
					Object Management 1	Intrusion Netwo	rk Analysis Policy	DNS Import/Expo	at
								New Policy	
Access Control Policy		Status			Last Modified				
Default-Policy		Targeting 1 de Up-to-date on	evices all targeted device	65	2020-05-04 09:15:56 Modified by "admin"			Pa 🛛 🖉 6	

7. Clique no valor ao lado de Política de Identidade.



Selecione a política de identidade criada anteriormente e clique em OK.

Identity Policy	
FTD-2 Identity Policy	▼ Ø
Revert to Defaults	OK Cancel

8. Clique em **Adicionar Regra** para criar uma nova regra de ACP. Essas etapas criam uma regra para permitir que o usuário no grupo Administradores de AnyConnect seja conectado aos dispositivos dentro da rede interna usando RDP.

Overview Analysis Policies Devices Ob	ojects AMP Intelligence	Deploy 🧕 System Help 🔻 admin 🔻
Access Control > Access Control Network Dis	covery Application Detectors Correlation Actions •	
Default-Policy Enter Description		You have unsaved changes 🛛 Analyze Hit Counts 🗍 🔛 Save 📄 🔞 Cancel
Prefilter Policy: Default Prefilter Policy	SSL Policy: None	Identity Policy: FTD-2 Identity Policy
		📑 Inheritance Settings   🛃 Policy Assignments (1)
Rules Security Intelligence HTTP Responses	Logging Advanced	
it filter by Device	Show Rule Conflicts 🥹 🧿	Add Category 🕜 Add Rule 🛫 Search Rules 🗙
a Name Sourc Dest Z Sourc	. Dest N VLAN Users Applic Sourc Dest P U	RLs Sourc Dest S Action 🙂 🐚 🕭 💷 🔍
➡ Mandatory - Default-Policy (-)		
There are no rules in this section. Add Rule or Add Catego	ry	
- Default - Default-Policy (-)		
There are no rules in this section. Add Rule or Add Catego	17Y	
Default Action		Access Control: Block All Traffic 🛛 👻 🔳

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

Especifique um nome para a regra. Verifique se a regra foi ativada e tem a ação adequada.

Na guia Zonas, especifique as zonas adequadas para o tráfego de interesse.

O tráfego RDP iniciado pelos usuários entra no FTD originado pela interface do outside-zone e sai do inside-zone.

Add Rule											? X
Name AC RDP Access					inabled	Insert	into Manda	tory	•		
Action 🖌 Allow			v 0 D 8	8 4 5							
Zones Networks	VLAN Tags	Users	Applications	Ports	URLs	SGT/ISE Attributes			Inspection	Logging	Comments
Available Zones  🗯				Sour	ce Zones	(1)		Destinat	ion Zones (1)		
🔍 side		×		÷.	outside-zo	ne	6	🚠 insid	e-zone		6
슈 inside-zone 슈 outside-zone			Add to Source Add to Destination								
										Add	Cancel

Em Redes, defina as redes de origem e de destino.

O objeto AnyConnect\_Pool inclui os endereços IP atribuídos aos clientes do AnyConnect.

O objeto Inside\_Net inclui a sub-rede interna.

Add Ru	le											
Name	AC RDP Access				🖌 En	abled		Insert	into Manda	story		~
Action	Allow			V 🛛 🖉	<b>1</b> 5							
Zone	s Networks VLA	N Tags	Users	Applications	Ports	URLs	SGT/ISE	Attributes		Inspection	Logging	Comments
Availabl	e Networks 🖸		0		Source	e Netwo	rks (1)			Destination Networks	i (1)	
🔍 Sear	ch by name or value					Source		Original (	Client	📰 Inside_Net		6
	Networks	Geolocation	n		Ar	yConned	_Pool		6			
Inside IPv4	de_Net I-Benchmark-Tests I-Link-Local I-Multicast I-Private-10.0.0.0-8 I-Private-172.16.0.0-12 I-Private-192.168.0.0-16 I-Private-All-RFC1918 I-Private-All-RFC1918		~	Add To Source Networks Add to Destination	Enter	an IP add	fress		Add	Foter an IP address		844
											Add	Cancel

Em Usuários, clique no território criado anteriormente em Territórios disponíveis, clique no grupo/usuário apropriado em Usuários disponíveis e clique em Adicionar à regra.

Se não houver usuários ou grupos disponíveis na seção Usuários disponíveis, verifique se o FMC baixou os usuários e grupos na seção Realm e se os Grupos/usuários adequados foram incluídos.

Os usuários/grupos especificados aqui são verificados da perspectiva de origem.

Por exemplo, com o que foi definido nesta regra até agora, o FTD avalia se o tráfego foi originado no outside-zone e destinado ao inside-zone, originado na rede no objeto AnyConnect\_Pools e destinado à rede do Inside\_Net, e se o tráfego foi originado em um usuário no grupo Administradores de AnyConnect.

Add Ri	ile												? ×
Name	AC RDP Access				E E	nabled	1	Insert	into Mandato	ory	·		
Action	Allow			▼ 0 0 8	105								
Zone	s Networks	VLAN Tags	Users	Applications	Ports	URLs	SGT/ISE Attrib	utes			Inspection	Logging	Comments
Availab	le Realms 🛭 🗯			Available User	Ċ					Selected	Users (1)		
🔍 Sea	rch by name or va	lue		Search by n	ame or va	alue		]		🝰 LAB-/	AD/AnyConnect	: Admins	6
📑 Spe	cial Identities			HAB-AD/*									
🌐 LAB	I-AD			AnyConnect	Admins								
				AnyConnect	Users								
				a it.admin				A	dd to Rule				
				test.user									
												Add	Cancel

Em Portas, os objetos RDP personalizados foram criados e adicionados para permitir a porta TCP e UDP 3389. Observe que não foi possível adicionar RDP na seção Aplicações, mas para simplificar, apenas as portas são verificadas.

Add Rule					? ×
Name AC RDP Access		✓ Enabled	Insert into Mand	datory 👻	
Action 🖌 Allow	V 00.	6 to 5			
Zones Networks VLAN T	ags Users Applications	Ports URLs SGT	/ISE Attributes	Inspection	Logging Comments
Available Ports 🖸	0	Selected Source Po	rts (0)	Selected Destination Po	orts (2)
Search by name or value  AOL  Bittorrent  DNS_over_TCP  DNS_over_UDP  FMC-HTTPS  FMC-SSH  FTD-3-FDM  FTD-3-SSH  FTP  HTTP	Add to Source Add to Destination	any		Protocol TCP (6)	Port Enter a Add
					Add Cancel

Por fim, em **Registro**, o **Registro ao final da conexão** é marcado para uma verificação adicional posteriormente. Clique em **Adicionar** quando terminar.

Add Rule ✓ Enabled Name AC RDP Access ¥ Insert into Mandatory V O B A 🕁 🗾 Action 🖌 Allow Inspection Logging Zones Networks VLAN Tags Users Applications Ports URLs SGT/ISE Attributes Comments Log at Beginning of Connection Log at End of Connection File Events: Send Connection Events to: Event Viewer Syslog Server (Using default syslog configuration in Access Control Logging) Show Overrides SNMP Trap Select an SNMP Alert Configuration.. v O Add Cancel

9. Uma regra adicional é criada para o acesso HTTP para permitir que os usuários no grupo AnyConnect User acessem o site do Windows Server IIS. Click Save.

Overview Analysis Policies	Devices Objects	AMP Intellig	gence								eploy	0, System	Help v	admi	n v
Access Control + Access Control	Network Discovery	y Application De	tectors Cor	rrelation	Actions *										
Default-Policy Enter Description								You have uns	aved ch	inges 📝	nalyze Hit	Counts	Save	😢 Can	cel
Prefilter Policy: Default Prefilter Policy			SSL Poli	cy: <u>None</u>				Ident	ity Polis	y: <u>PTD-2</u>	Identity Po	alay.			
										Te 2	nheritence	Settings   🛃	Policy Assig	nmenta	(1)
Rules Security Intelligence H	TTP Responses Log	ging Advanced													
# Filter by Device					Show Rule C	onficta 🐧	ð -	Add Category	y G	Add Rule	- <b>-</b>	Search Rules			×
a Name Source Zo	Dest Zones So	ource Networks	Dest Netwo	V., User	5	A	S	Dest Ports	U 5	š D	Action	005	a 🕁 🗊	. 0	)
➡ Mandatory - Default-Policy (1-2)															
1 AC RDP Access Ac outside-zo	ne 🚓 inside-zone  🚊	AnyConnect_Pool	📾 Inside_Net	An 💣 U	AB-AD/AnyConnect Admin	s Any	Any	ROP-TCP	Any	Any Any	🗸 Allo	• 004	e 🗈 🔳 (	0	8
2 AC HTTP Access A outside-zo	ne 🗄 inside-zone	AnyConnect_Pool	👼 Inside_Net	Arg 💣 U	AB-AD/AnyConnect Users	Any	Any	🖉 НТТР	Any	Any Any	Allo	.00.	8 🖄 🖉 (	0	8
▼ Default - Default-Policy (-)															
There are no rules in this section. Add i	ule or Add Category														
Default Action								Access Con	trol: Die	ck All Treff	ĥc			*	

Displaying 1 - 2 of 2 rules |< < Page 1 of 1 > >| C | Rules per page: 100 \*

## Configurar isenção de NAT

Se houver regras de NAT que afetem o tráfego do AnyConnect, como as regras de PAT da Internet, é importante configurar as regras de isenção de NAT para que o tráfego do AnyConnect não seja afetado pelo NAT.

#### 1. Navegue até Devices > NAT.

Overview Analysis	s Polici	es Devi	ices 0	bjects AMP Int	telligence		Deploy	🔒 System	Help 🔻	admin 🔻
Device Management	NAT	VPN •	QoS	Platform Settings	FlexConfig	Certificates				

Selecione a política de NAT aplicada ao FTD.

0	verview	Analysis	Policie	s Devi	ces	Objects	AMP	Int	elligence			Deploy	0	System	Help 🔻	admin v
D	evice Mana	agement	NAT	VPN *	QoS	Platfo	rm Settir	ngs	FlexConfig	Certificates						
															🔾 Nev	Policy
	NAT Pol	icy						Devi	ice Type		Status					
	FTD-2-	NAT-Policy						Threa	at Defense		Targeting 1 devices Up-to-date on all targe	eted devices			<b>D</b> E	/ 6

? X

2. Nesta Política de NAT, há um PAT dinâmico no final do qual o PAT afeta todo o tráfego (incluindo o tráfego do AnyConnect) que sai da interface externa para a interface externa.

Para evitar que o tráfego do AnyConnect seja afetado pelo NAT, clique em Adicionar regra na parte superior direita.

Overview A	nalysis	Policies Devi	ices Objects	AMP Inte	elligence			Deple	oy 🔒 :	System Help 🔻	admin 🔻
Device Manage	ment l	VPN VPN V	QoS Platfor	m Settings	FlexConfig	Certificates					
FTD-2-NA	AT-Poli	cy						🔔 s	how Warning	s 🔚 Save	😫 Cancel
Rules										Policy A	ssignments (1
B Filter by Device										<u></u>	Add Rule
					Original Pack	,t		Translated Packet			
# Direction	Туре	Source Interface Object	Destination Interface Object	Original Sources	Original Destination	Orig Service	Translated Sources	Translated Destinations	Trans Services	Options	
▼ NAT Rules Befo	re										
<ul> <li>Auto NAT Rules</li> </ul>											
= +	Dynamic	🥞 any	🚠 outside-zone	💂 obj-any			🥵 Interface			🍓 Dns:false	a 🖉
<ul> <li>NAT Rules After</li> </ul>	r										
						Displayin	g 1-1 of 1 rows  4	< Page 1 of	1 > >	C Rows per p	age: 100 •

3. Configure uma regra de isenção de NAT, certifique-se de que a regra seja Manual NAT Rule with Type Static. Essa é uma regra NAT bidirecional que se aplica ao tráfego do AnyConnect.

Com essas configurações, quando o FTD detecta o tráfego originado em Inside\_Net e destinado ao endereço IP do AnyConnect (definido por AnyConnect\_Pool), a origem é convertida no mesmo valor (Inside\_Net) e o destino é convertido no mesmo valor (AnyConnect\_Pool), quando o tráfego entra no inside\_zone e sai do outside\_zone. Basicamente, isso ignora a NAT quando essas condições são atendidas.

Add NAT Rule							? ×
NAT Rule:	Manual NAT Ru	le 👻	I	nsert:	In Category	VAT Rules Before	~
Type:	Static	~	🗹 Enable				
Description:							0
Interface Objects	Translation	PAT Pool	Advance	d			
Available Interface Ob	ojects 🖒			Source Interface Object	ts (1)	Destination Interface Ob	ojects (1)
🔍 zone		×		💼 inside-zone	6	💼 outside-zone	6
📩 inside-zone							
📩 outside-zone		A	dd to ource				
		A	dd to				
		Des	tination				
						0	K Cancel

Add NAT Rule					
NAT Rule:	Manual NAT Rule	Insert:	In Category	✓ NAT Rules Before ✓	
Type:	Static 💌	Enable			
Description:					(
Interface Objects 🚺	ranslation PAT Pool	Advanced			
Original Packet			Translated Packet		
Original Source:*	Inside_Net	<b>~</b> O	Translated Source:	Address	~
Original Destination:	Address	*		Inside_Net	<b>~</b>
	AnyConnect_Pool	<b>~</b> ()	Translated Destination:	AnyConnect_Pool	~ «
Original Source Port:		¥ ()	Translated Source Port:		~ (
Original Destination Por	t:	× 0	Translated Destination Port:		~ «
				ок	Cancel

Além disso, o FTD é definido para executar uma pesquisa de rota nesse tráfego e não o ARP de proxy. Clique em **OK** quando terminar.

Add NAT Rule					? ×
NAT Rule:	Manual NAT Rule	Insert:	In Category	▼ NAT Rules Before ▼	
Туре:	Static 💌	Enable			
Description:					$\bigcirc$
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	Cancel

4. Clique em Salvar.

	Overview	Analysis	Policies Devi	ces Objects	AMP Intell	ligence			Deploy	, 0,	System I	Help 🔻	admin 🔻
	Device Manag	jement	NAT VPN *	QoS Platfor	m Settings	FlexConfig Certifica	tes						
	FTD-2-N Enter Descriptio	AT-Poli	cy					You have uns	aved changes [ 🔌 Sh	ow Warning	is 📙 S	ave	Cancel
	Rules										<u>E</u>	Policy As	signments (1)
đ	B Filter by Devic											0	Add Rule
						Original Packet			ranslated Packet				
1	Direction	Туре	Source Interface Obje	Destination Interface Object	Original Sources	Original Destinations	Orig Services	Translated Sources	Translated Destinations	Trans Services	Options		
•	NAT Rules Be	fore											
1	- <del>4</del> 2	Static	🚠 inside-zone	📩 outside-zone	👼 Inside_Net	🚃 AnyConnect_Pool		👼 Inside_Net	RhyConnect_Pool		🧐 Dns:fi 🥞 route- 🥞 no-pri	alse ·lookup oxy-arp	/ 6
•	Auto NAT Rul	es-											
;	= <b>+</b>	Dynamic	🍓 any	🚠 outside-zone	📻 obj-any			🍓 Interface			🝓 Dosifi	alse	08
•	<ul> <li>NAT Rules Aft</li> </ul>	er											
							Displaying	1-2 of 2 rows 1<	< Page 1 of 1	> >	C Rov	vs per pa	ge: 100 •

## Implantar

1. Quando a configuração estiver concluída, clique no botão Implantar no canto superior direito.



2. Clique na caixa de seleção ao lado do FTD ao qual a configuração foi aplicada e clique em **Implantar**.

Depl	oy Policies Version:2020-05-04 09:40 AM					×
V	Device	Inspect Interruption	Туре	Group	Current Version	٢
₹ 3	=/FTD-2	No	FTD		2020-05-04 09:16 AM	
Select	ed devices: 1				Deploy Car	icel

# Verificar

## Configuração final

## Configuração do AAA

```
> 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
```

## Configuração do AnyConnect

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

deny-message none anyconnect ssl df-bit-ignore enable

> show running-config ssl
ssl trust-point FTD-2-SelfSigned outside

## Conectar-se ao AnyConnect e verificar regras de política de controle de acesso

🚳 Cisco AnyConnect S	ecure Mobility Client — 🗆 🗙
Contact ftd2.ex	ng ftd2.example.com. cample.com ~ Connect
<b>\$</b> (i)	Scisco AnyConnect   ftd2.example.com ×
	Group: General ~
	Username: it.admin
	Password: ******
	OK Cancel
🚳 Cisco AnyConnect S	ecure Mobility Client — 🗆 🗙
Connect ftd2.ex	ed to ftd2.example.com. ample.com
00:00:12	IPv4
<b>O</b>	

O usuário Administrador de TI está no grupo Administradores de AnyConnect que tem acesso RDP ao Windows Server, mas não tem acesso ao HTTP.

Abrir uma sessão RDP e Firefox para esse servidor verifica se esse usuário só pode acessar o servidor usando RDP.



Se estivermos conectados com o usuário de teste que está no grupo Usuários de AnyConnect que tem acesso HTTP, mas não tem acesso RDP, podemos verificar se as regras de política de controle de acesso estão entrando em vigor.

🌄 Remote Desktop Connection 🛛 🗌 🗙	
Remote Desktop	Remote Desktop Connection ×
Tonnection	Remote Desktop can't connect to the remote computer for one of these reasons:
Computer: win2016.example.com ~	1) Remote access to the server is not enabled     2) The remote computer is turned off     3) The remote computer is not available on the network
User name: None specified You will be asked for credentials when you connect.	Make sure the remote computer is turned on and connected to the network, and that remote access is enabled.
Show Optio Connect Help	OK Help
IIS Windows Server X 🛠 Options	× + – – ×
← → C <sup>I</sup>	♡☆ Ⅲ\ ① ⑧ ≪ ☰
H Windows Server	
Internet Information Serv	vices
Welcome Rienvenue Tonyotu	
Serverde Terverd	

## Verificar com eventos de conexão do FMC

Como o registro foi ativado nas regras de política de controle de acesso, os eventos de conexão podem ser verificados para qualquer tráfego que corresponda a essas regras

Navegue até Análise > Conexões > Eventos.

Overview Analys	sis Policies D	Devices Object	ts AMP	Intellig	ence	C	Deploy 0	System	Help 🔻	admin 🔻
Context Explorer	Connections <b>v</b>	Intrusions 🔻	Files 🔻	Hosts 🔻	Users v	Correlation •	Advanced	<ul> <li>Search</li> </ul>	h	
	Events									
	Security Intellig	ence Events								

Na **Visualização da tabela de eventos de conexão**, os registros são filtrados para mostrar apenas os eventos de conexão para o administrador de TI.

Aqui, você pode verificar se o tráfego RDP para o servidor (TCP e UDP 3389) é permitido, no entanto, o tráfego da porta 80 é bloqueado.

¢	)verv	iew	Analysi	s Policies I	Devices	Objects	AMP	Intellig	ence				Depl	γ <b>Q</b>	System	Help 🔻	admin 🔻
C	ontex	t Exp	plorer C	onnections + E	vents	Intrusions	▼ Fil	es 🕶 🕴	losts v U	sers 🔻	Correlation	r▼ Adv	anced 🔻	Search			
										6	lookmark This	Page Repo	rt Designe	r Dashboar	d View B	ookmarks	Search +
¢	Coni	onnection Events (switch workflow)															
2	onnect	tions v	with Applicati	ion Details > Tab	le View of	f Connection	Events						202	0-05-05 14	14:17 - 2	120-05-05 E	Expanding
•	Searc	arch Constraints ( <u>Edit Search Save Search</u> ) Disabled Columns															
1	Jump	to	•														
	Jump	to	▼ Action ×	Initiator ×	Initiato	r User ×		Be	esponder ×	Ingre	ty Zone	Egress Security	× Zone	Source P	ort / ×	Destinal ICMP Co	tion Port / ×
	Jump C	to	Action ×	Initiator × IP 10.10.10.1	Initiato	<u>r User</u> × nin (LAB-AD\it	admin, L	DAP)	esponder ×	Ingre Securi	ty Zone ×	Egress Security	Zone	Source P ICMP Typ 62473 / to	p <u>ort /</u> × He	Destinal ICMP Co 3389 / to	t <u>ion Port /</u> × s <u>de</u> 2
	Jump C J L C L	to	Action × Allow Block	Initiator × IP 10.10.10.1 10.10.10.1	Initiator	<mark>r User</mark> × nin (LAB-AD\it nin (LAB-AD\it	admin, L	DAP)	<u>esponder</u> × 192.168.1.1 192.168.1.1	Ingre- Securi	zone	Egress Security inside-zon	Zone ×	Source P ICMP Typ 62473 / to 62474 / to	0 <b>rt / ×</b> 96 0 0	Destinal ICMP Co 3389 / to 80 (http)	tion Port / × ade 2 / top
	qmut ] ] ↓ ] ↓	to	Action × Allow Block Block	Initiator × IP 10.10.10.1 10.10.10.1 10.10.10.1	Initiator it adm	r User × nin (LAB-AD\it nin (LAB-AD\it nin (LAB-AD\it	.admin, L .admin, L .admin, L	DAP)	192.168.1.1 192.168.1.1 192.168.1.1	Ingre Secur outside outside	ty Zone Zone Zone	Earess Security inside-zon inside-zon	Zone ×	Source P ICMP Typ 62473 / to 62474 / to 62475 / to	ent / × Me P P P	Destinat ICMP Co 3389 / to 80 (http) 80 (http)	tion Port / × ade 2 / tsp / tsp

Para o usuário de teste, você pode verificar se o tráfego RDP para o servidor está bloqueado e se o tráfego da porta 80 é permitido.

Overview	Overview Analysis Policies Devices Objects AMP Intelligence Deploy 0, System Help • admin •											
Context Exp	olorer C	onnections •	Events	Intrusions •	Files 🔻	Hosts V Us	sers 🔻	Correlation	<ul> <li>Advanced •</li> </ul>	Search		
							Bo	okmark This P	age Report Designer	Dashboard	View Bookn	narks Search 🕶
Connections Connections Search Con Jump to	Connection Events (switch workflow)         immediate this rage Report Designer Designeres Designeres Designeres Designer Designer Designer Designer Desi											
	Action ×	Initiator × IP	Initiato	r User ×		Responder × IP	Ingres	s × ty Zone	Egress X Security Zone	Source P	ort/× D	estination Port / >
1	Block	10.10.10.1	📇 <u>test u</u>	iser (LAB-AD\tes	t.user, LDAP)	192.168.1.1	outside	zone	inside-zone	<u>62493 / to</u>	p <u>3</u>	389 / tcp
4	Allow	10.10.10.1	📇 test u	iser (LAB-AD\tes	t.user, LDAP)	192.168.1.1	outside	zone	inside-zone	<u>62494 / to</u>	p <u>8</u>	0 (http) / tcp

# Troubleshoot

## Debugs

Essa depuração pode ser executada na CLI de diagnóstico para solucionar problemas relacionados à autenticação LDAP: **debug Idap 255** 

Para solucionar problemas na política de controle de acesso da identidade do usuário, o comando **system support firewall-engine-debug** pode ser executado no Clish para determinar o motivo pelo qual o tráfego está sendo permitido ou bloqueado inesperadamente.

## Como trabalhar com as depurações do LDAP

```
[53] Session Start
[53] New request Session, context 0x00002bldl3f4bbf0, reqType = Authentication
[53] Fiber started
[53] Creating LDAP context with uri=ldap://192.168.1.1:389
[53] Connect to LDAP server: ldap://192.168.1.1:389, status = Successful
[53] supportedLDAPVersion: value = 3
[53] supportedLDAPVersion: value = 2
[53] LDAP server 192.168.1.1 is Active directory
[53] Binding as ftd.admin@example.com
[53] Performing Simple authentication for ftd.admin@example.com to 192.168.1.1
[53] LDAP Search:
Base DN = [DC=example,DC=com]
```

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

#### Não é possível estabelecer uma conexão com o servidor LDAP

```
[-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
```

Possíveis soluções:

- Verifique o roteamento e certifique-se de que o FTD esteja recebendo uma resposta do servidor LDAP.
- Se LDAPS ou STARTTLS for usado, verifique se o certificado de CA raiz correto é confiável para que o handshake SSL possa ser concluído com sucesso.
- Verifique se a porta e o endereço IP corretos foram usados. Se um nome de host for usado, verifique se o DNS pode resolvê-lo para o endereço IP correto.

#### DN de login de vinculação incorreto e/ou senha incorreta

```
[-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
```

Solução em potencial: verifique se o DN de login e a senha de login estão configurados corretamente. Isso pode ser verificado no servidor do AD com **Idp.exe**. Para verificar se uma conta pode ser vinculada usando o Idp, siga estas etapas:

1. No servidor do AD, pressione Win+R e procure Idp.exe

🗐 Run	×
Ø	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. Em Conexão, escolha Conectar...

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

3. Especifique localhost para o servidor e a porta apropriada e clique em OK.

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

4. A coluna Direita mostra o texto que indica uma conexão bem-sucedida. Navegue até Conexão
 > Vincular...

🟠 Idap://w	in2016.exa	ample.co	om/DC	= example, DC	=com		—		×
Connection	Browse	View	Optio	ns Utilities	Help				
Connec Bind Discon New Save Save As Exit	nect	Ctrl+B		Id = Idap_op Established Retrieving b Getting 1 en Dn: (RootD) configur CN= current Time defaultM dnsHosi domain dsServi Sett Firs Nan com forestFo highest( isGlobal isSynch	en("localhos connection f ase DSA inf tries: SE) rationNaming Configuratio Time: 5/1/202 e; VamingConte tName: win2 ControllerFur Functionality: iceName: CN tings,CN=WI st-Site- ne,CN=Sites, n; unctionality: CommittedUS ICatalogReac tronized: TR viceName: e	st", 389); to localhost. formation gContext: on,DC=examp 20 4:16:55 PM ext: DC=example nctionality: 7 = : 7 = ( WIN201 I=NTDS N2016,CN=Se ,CN=Configur 7 = ( WIN2010 SN: 13410; dy: TRUE; UE; example.comm	le,DC=c 1 Eastern ple,DC=c .com; = ( WIN2 16 ); ervers,C ation,DC 6 ); win2016	om; n Daylight com; 016 ); N=Default- :=example,D	∩  C= ↓

5. Selecione **Bind Simples** e, em seguida, especifique o **Nome de Usuário da Conta do Diretório** e a **Senha**. Click **OK**.

Bind X								
User:	ftd.admin@example.com							
Password:								
Bind type Bind as currently logged on user Bind with credentials Simple bind Advanced (DIGEST) Encrypt traffic after bind								

Com uma associação bem-sucedida, Idp mostra Authenticated as: DOMAIN\username

Idap://win2016.example.com/DC=example,DC=com						—		$\times$		
Connection	Browse	View	Options	Utilities	Help					
				1.2. 1.2. 1.2. supporte Max Max Max Max Max Max Max Max	840.11355 840.11355 840.11355 edLDAPPo PercentDi ReceiveB Connectio BatchRetu DirSyncDu ResultSet ValRange edLDAPVe edSASLMe IEGO; EXT	6.1.4.2255; 6.1.4.2256; 6.1.4.2309; ficies (20): Marchar rSyncReques uffer; InitRecvons; MaxConn urnMessages uration; MaxTons sperConn; Marthar sperConn; Marchar yLimit; System ersion (2): 3; 2 echanisms (4) ERNAL; DIGE d_s(Id, 'ftd.adm	axPoolThre ts; MaxDa /Timeout; IdleTime; M ; MaxQuer empTables utSets; uxNotificat geTransitiv nMemoryL 2; ): GSSAPI ST-MD5; min@exar min".	eads; itagramRe MaxPageS ryDuration Size; ionPerCon /e; imitPerce ; GSS-	ecv; Size; n; nn; ent;	
Ready										

Uma tentativa de vinculação com um nome de usuário ou uma senha inválida resulta em uma falha, como as duas vistas aqui.

🔝 Idap://win2016.example.com/DC=example,DC=com — 🗆 🗙									×
Connection	Browse	View	Options	Utilities	Help				
				Max Max Max Thre supporte supporte SPN es = Idap_s unavailable uthenticate	ResultSetSiz ResultSetsP ValRange; N eadMemoryL edLDAPVers edSASLMec IEGO; EXTER simple_bind_s ed as: 'EXAM	ze; MinResu erConn; Max laxValRang imit; System sion (2): 3; 2 hanisms (4) RNAL; DIGES s(Id, 'ftd.adm PLE\ftd.adm s(Id, 'wrong	ItSets; xNotificat eTransitiv MemoryL ; : GSSAPI ST-MD5; nin@exar nin". @examp	ionPerConn /e; imitPercent; ; GSS- nple.com',	7
			< E S C E ir	unavailable rror <49>: I erver error omment: Ac rror 0x8009 ivalid	i// v.3 idap_simple_ :: 80090308: cceptSecurit 90308 The to	bind_s() fai LdapErr: DS yContext er ken supplie	led: Invali SID-0C090 ror, data d to the f	d Credentia 042A, 52e, v3839 unction is	is V
Ready									

## O servidor LDAP não consegue encontrar o nome de usuário

```
[-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
```

Solução potencial: verifique se o AD pode encontrar o usuário com a pesquisa feita pelo FTD. Isso também pode ser feito com o **Idp.exe**.

1. Após a vinculação bem-sucedida conforme visto acima, navegue até Exibir > Árvore.

Idap://win2016.example.com/DC=example,DC=com									×	
Connection	Browse	View	v Options	; Utilities	Help					
Connection	Browse	View	Tree Enterprise Status Bar Set Font	Configurat	Help ion DirSyncl ResultSe ResultSe ValRang adMemo edLDAP edSASLI EGO; EX imple_bin >); // v.3 ed as: 'E>	Ctrl+T Duration; Ma etSize; MinR etSPerConn; e; MaxValR oryLimit; Sys /ersion (2): Mechanisms (TERNAL; Di nd_s(Id, 'ftd (AMPLE\ftd.	/axPool sts; Ma vTimeo nldleTim s; MaxO axTempTa esultSets ; MaxNotif angeTran stemMemo 3; 2; s (4): GSS IGEST-MD .admin@e .admin'.	Threads; xDatagram out; he; MaxPag QueryDurat bleSize; ; icationPer( sitive; oryLimitPer SAPI; GSS- 95; example.co	nRecv; jeSize; ion; Conn; cent; m',	~

2. Especifique o DN de Base configurado no FTD e clique em  $\mathbf{O}\mathbf{K}$ 

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

3. Clique com o botão direito do mouse no DN de Base e, em seguida, clique em Pesquisar.

Idap://win2016.ex	– 🗆 ×	(				
Connection Browse	View	Options	Utilities	Help		
DC= example, DC=	com	Search Virtual L Delete Modify Modify Add chil Compar Advance Copy D Copy Select al Clear ou	ist View DN Id eed 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; 11D297C400C04FD8D5CD:C example,DC=com; 11D1ADED00C04FD8D5CD:C =example,DC=com; 11D1ADED00C04FD8D5CD:C ole,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 documer	t	J				×

4. Especifique os mesmos valores Base DB, Filter e Scope vistos nas depurações.

Neste exemplo, eles são:

- DN base: dc=example,dc=com
- Filtro: samaccountname=it.admi
- Scope:SUBTREE

🟠 Idap://w	n2016.example.com/DC=example,DC=com	– 🗆 ×	
Connection	Browse View Options Utilities Help		
Search	×	C=example,DC=com; 58811D1ADED00C04FD8D5CD:C	^
Base DN:	DC=example,DC=com ~	58811D1ADED00C04FD8D5CD:C	
Filter:	sAMAccountName=it.admi ~	ample,DC=com; D211D1AA4B00C04FD7D83A:O	
Scope O Base	One Level Subtree	lers,DC=example,DC=com; 58811D1ADED00C04FD8D5CD:C example,DC=com;	
Attributes:	objectClass;name;description;canonicalName $\sim$	68811D1ADED00C04FD8D5CD:C mple,DC=com; 2020 3:43:59 PM Eastern Davlight	
Options	Run Close	)20 2:41:57 PM Eastern Daylight	
	***Searching ldap_search_s(ld, "DC= "sAMAccountName=it.a Getting 0 entries:	example,DC=com", 2, dmi", attrList, 0, &msg)	~
Ready			

o ldp localiza 0 entradas porque não há nenhuma conta de usuário com o samaccountname **it.admi** no DN base dc=example,dc=com

Outra tentativa com o samaccountname **it.admin** correto mostra um resultado diferente. Idp localiza 1 entrada sob o DN base dc=example,dc=com e imprime esse DN de usuário.

🔐 Idap://w	in2016.example.	com/DC=ex	ample,DC:	=com		- □ >	<
Connection	Browse View	Options	Utilities	Help			
Search					$\times$	58811D1ADED00C04FD8D5CD:C DC=example,DC=com;	^
Base <u>D</u> N: Filter:	DC=example,DC	C=com ne=it.admin			~	58811D1ADED00C04FD8D5CD:C ample,DC=com; D211D1AA4B00C04FD7D83A:C lers DC=example DC=com;	) )
Scope	O <u>O</u> ne Level	● <u>S</u> ubtree	e			58811D1ADED00C04FD8D5CD:C example,DC=com; 68811D1ADED00C04FD8D5CD:C mple DC=com;	2
<u>A</u> ttributes:	objectClass;nam	e;descriptior	n;canonicalN	lame	$\sim$	020 3:43:59 PM Eastern Dayligh	t
Options		<u>R</u> un		<u>C</u> lose		)20 2:41:57 PM Eastern Daylight	
		k G D	**Searching dap_search sAMAccour Setting 1 ent On: CN=IT A canonica name: IT objectCla user	I _s(Id, "I ntName= tries: Admin,( alName: Admin; ass (4): r;	DC=e =it.ad C <b>N=U</b> exar top;	min", attrList, 0, &msg) <b>Isers,DC=example,DC=com</b> mple.com/Users/IT Admin; person; organizationalPerson;	
Ready							

#### Senha incorreta para o nome de usuário

```
[-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
```

Possível solução: verifique se a senha do usuário está configurada corretamente e se não expirou. Semelhante ao DN de Logon, o FTD faz uma associação com o AD com as credenciais do usuário.

Essa vinculação também pode ser feita no ldp para verificar se o AD pode reconhecer as mesmas credenciais de nome de usuário e senha. As etapas no ldp são mostradas na seção Vinculação do DN de logon e/ou senha incorreta.

Além disso, os registros do visualizador de eventos do Microsoft Server podem ser analisados quanto aos possíveis motivos.

## AAA de teste

O comando test aaa-server pode ser usado para simular uma tentativa de autenticação do FTD com um nome de usuário e uma senha específicos. Ele pode ser usado para testar falhas de conexão ou autenticação. O comando é *t*est 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
```

## Capturas de pacotes

As capturas de pacotes podem ser usadas para verificar a acessibilidade ao servidor do AD. Se os pacotes LDAP saem do FTD, mas não há resposta, isso pode indicar um problema de roteamento.

A captura mostra o tráfego LDAP bidirecional.

```
> show route 192.168.1.1
Routing entry for 192.168.1.0 255.255.255.0
Known via "connected", distance 0, metric 0 (connected, via interface)
Routing Descriptor Blocks:
```

```
* directly connected, via inside
     Route metric is 0, traffic share count is 1
> capture AD interface inside match tcp any host 192.168.1.1 eq 389
> show capture
capture AD type raw-data interface inside [Capturing - 0 bytes]
 match tcp any host 192.168.1.1 eq ldap
> test aaa-server authentication LAB-AD host win2016.example.com username it.admin password
*****
INFO: Attempting Authentication test to IP address (192.168.1.1) (timeout: 12 seconds)
INFO: Authentication Successful
> show capture
capture AD type raw-data interface inside [Capturing - 10905 bytes]
 match tcp any host 192.168.1.1 eq ldap
> show capture AD
54 packets captured
   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>
  6: 23:02:16.772955
                      192.168.1.17.61960 > 192.168.1.1.389: . ack 491522141 win 32768
<nop,nop,timestamp 1061373059 762393885>
  7: 23:02:16.773428
                        192.168.1.17.61960 > 192.168.1.1.389: P 3681912980:3681913024(44)
ack 491522141 win 32768 <nop,nop,timestamp 1061373060 0>
                        192.168.1.1.389 > 192.168.1.17.61960: P 491522141:491522163(22) ack
  8: 23:02:16.775030
3681913024 win 65116 <nop,nop,timestamp 762393887 1061373060>
   9: 23:02:16.775075
                           192.168.1.17.61960 > 192.168.1.1.389: . ack 491522163 win 32768
<nop,nop,timestamp 1061373061 762393887>
[...]
54 packets shown
```

## Registros do visualizador de eventos do Windows Server

Os registros do visualizador de eventos no servidor do AD podem fornecer informações mais detalhadas sobre o motivo da falha.

1. Procure e abra o Visualizador de Eventos.

=	Best match								
ŵ	Event Viewer Desktop app								
	Settings					>			
	🐵 View ev	<b>rent</b> logs							
æ		<b>P</b>		5	~	ła			
89	ы (S)	Ц	Ц		L4	411			
	event								
-	D D	e	-	-	1	8			

2. Expanda Logs do Windows e clique em Segurança. Procure por falhas de auditoria com o nome da conta do usuário e revise as informações de falha.



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
## Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.