Configuración de la autenticación de AD (LDAP) y la identidad de usuario en FTD gestionadas por FDM para clientes de AnyConnect

Contenido

Introducción **Prerequisites Requirements Componentes Utilizados** Configurar Diagrama y escenario de red Configuraciones de AD Determinación de LDAP Base DN Crear una cuenta FTD Crear grupos AD y agregar usuarios a grupos AD (opcional) Copie la raíz del certificado SSL de LDAPS (sólo se requiere para LDAPS o STARTTLS) Configuraciones de FDM Verificación de licencias Configurar origen de identidad AD Configurar AnyConnect para la autenticación AD Habilitar la política de identidad y configurar las políticas de seguridad para la identidad de usuario Verificación Configuración final Conéctese con AnyConnect y verifique las normas de política de control de acceso Troubleshoot **Depuraciones** Depuraciones LDAP en funcionamiento No se puede establecer la conexión con el servidor LDAP Enlace de DN de inicio de sesión o contraseña incorrecta El servidor LDAP no puede encontrar el nombre de usuario Contraseña incorrecta para el nombre de usuario Prueba AAA Capturas de paquetes Registros del Visor de eventos de Windows Server

Introducción

El propósito de este documento es detallar cómo configurar la autenticación de Active Directory (AD) para los clientes de AnyConnect que se conectan a un Cisco Firepower Threat Defense (FTD) administrado por Firepower Device Management (FDM). La identidad del usuario se utilizará en las políticas de acceso para restringir a los usuarios de AnyConnect a direcciones IP y puertos específicos.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Conocimiento básico de la configuración de VPN de RA en FDM
- Conocimiento básico de la configuración del servidor LDAP en FDM
- Conocimiento básico de AD

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Microsoft 2016 Server
- FTDv ejecutando 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. Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Configurar

Diagrama y escenario de red



El servidor de Windows está preconfigurado con Servicios de Internet Information Server (IIS) y Protocolo de Escritorio remoto (RDP) para probar la identidad del usuario. En esta guía de configuración, se crearán tres cuentas de usuario y dos grupos.

Cuentas de usuario:

- FTD Admin: Esto se utilizará como la cuenta de directorio para permitir que FTD se enlace al servidor AD.
- Administrador de TI: Cuenta de administrador de pruebas utilizada para demostrar la identidad del usuario.
- Usuario de prueba: Cuenta de usuario de prueba utilizada para demostrar la identidad del usuario.

Grupos:

• Administradores de AnyConnect: Un grupo de prueba al que se agregará el administrador de TI para demostrar la identidad del usuario. Este grupo solo tendrá acceso RDP a Windows Server

 Usuarios de AnyConnect: Grupo de prueba al que se agregará el usuario de prueba para demostrar la identidad del usuario. Este grupo solo tendrá acceso HTTP al servidor de Windows

Configuraciones de AD

Para configurar adecuadamente la autenticación AD y la identidad del usuario en FTD, se necesitarán algunos valores. Todos estos detalles se deben crear o recopilar en Microsoft Server antes de que se pueda realizar la configuración en FDM. Los valores principales son:

- Nombre de dominio: Este es el nombre de dominio del servidor. En esta guía de configuración, example.com es el nombre de dominio.
- Dirección IP/FQDN del servidor: La dirección IP o FQDN utilizados para alcanzar el servidor de Microsoft. Si se utiliza un FQDN, se debe configurar un servidor DNS dentro de FDM y FTD para resolver el FQDN. En esta guía de configuración, estos valores son win2016.example.com que se resuelve en 192.168.1.1.
- Puerto del servidor: El puerto utilizado por el servicio LDAP. De forma predeterminada, LDAP y STARTTLS utilizarán el puerto TCP 389 para LDAP y LDAP sobre SSL (LDAPS) utilizará el puerto TCP 636.
- CA raíz: Si se utiliza LDAPS o STARTTLS, se requiere la CA raíz utilizada para firmar el certificado SSL utilizado por LDAPS.
- Nombre de usuario y contraseña del directorio: Esta es la cuenta utilizada por FDM y FTD para enlazar al servidor LDAP y autenticar usuarios y buscar usuarios y grupos. Se creará una cuenta denominada FTD Admin para este fin.
- Nombre distintivo básico (DN): El DN base es el FDM de punto de partida y el FTD indicará a Active Directory que comience en cuando busque usuarios. En esta guía de configuración, el dominio raíz example.com se utilizará como DN base; sin embargo, para un entorno de producción, el uso de un DN base más dentro de la jerarquía LDAP podría ser mejor. Por ejemplo, tome esta jerarquía LDAP:



Si un administrador desea que los usuarios de la unidad organizativa de marketing puedan autenticar el DN base se puedan establecer en la raíz (ejemplo.com), esto también permitirá que el usuario1 de la unidad organizativa de finanzas también inicie sesión, ya que la búsqueda de usuario comenzará en la raíz y bajará a Finanzas, Marketing e Investigación.

DN base establecido en example.com.



Para restringir los inicios de sesión sólo a los usuarios de la unidad organizativa de marketing y a los usuarios inferiores, el administrador puede establecer el DN base en Marketing. Ahora solo los usuarios 2 y 3 podrán autenticarse porque la búsqueda comenzará en Marketing.

DN base establecido en Marketing:



Tenga en cuenta que para un control más granular dentro del FTD para el cual se permitirá a los usuarios conectar o asignar diferentes autorizaciones según sus atributos de AD, será necesario configurar un mapa de autorización LDAP.

Esta jerarquía LDAP simplificada se utiliza en esta guía de configuración y el DN para el ejemplo raíz.com se utilizará para el DN base.



Determinación de LDAP Base DN

1. Abra Usuarios y ordenadores AD.

=	Best match	
ŵ	Active Directory Users and Computers Desktop app	
	Settings >	
	8 Edit local users and groups	
	陀 Change User Account Control settings	
	8 User Accounts	
	Select users who can use remote desktop	
۲		
	users	
-	ዶ 🗆 🤶 🚍 🤱 🖪	

2. Haga clic con el botón izquierdo en el dominio raíz (para abrir el contenedor), haga clic con el botón derecho en el dominio raíz, luego navegue hasta Ver y haga clic en Funciones avanzadas.



3. Esto habilitará la vista de propiedades adicionales bajo los objetos AD. Por ejemplo, para buscar el DN para la raíz example.com, haga clic con el botón derecho en **example.com** y luego navegue hasta **Propiedades**.



4. En **Propiedades**, haga clic en la ficha **Editor de atributos**. Busque **nombre distinguido** en los atributos y, a continuación, haga clic en **Ver**.

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></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></th><td></td><td></td><td></td><td></td></not<>	set>				
domai	nReplica	<not< td=""><th>set></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></th><td></td><td></td><td></td><td></td></not<>	set>				
extent	sionName	<not< td=""><th>set></th><td></td><td></td><td></td><td></td></not<>	set>				
flags		<not< td=""><th>set></th><td></td><td></td><td></td><td>~</td></not<>	set>				~
<						3	>
V	ew					Filter	
	OK		Cancel		Apply	Н	elp

5. Esto abrirá una nueva ventana donde el DN se puede copiar y pegar en FDM más adelante. En este ejemplo, el DN raíz es DC=ejemplo, DC=com. Copie el valor. Haga clic en **Aceptar** para salir de la ventana del Editor de atributos de cadena y haga clic **Aceptar** nuevamente para salir de las propiedades.

ring Attribute Editor		×		
ttribute: distingui	ishedName			
alue: OC-example,DC-com Clear	ОК	Cancel	Undo Cut Copy Paste Delete	
			Select All Right to left Reading order Show Unicode control characters Insert Unicode control character	>
ample.com Properties Seneral Managed By C Attributes: Attribute	bject Security Attribute Edite	? ×		
cn controlAccessRights creationTime dc defaultLocalPolicyObj description desktopProfile displayName	<not set=""> <not set=""> 4/29/2020 2:43:49 PM Easter example <not set=""> <not set=""> <not set=""> <not set=""> <not set=""></not></not></not></not></not></not></not>	m Daylight Tim		
displayNamePrintable distinguishedName domainPolicyObject domainReplica dSASignature dSCorePropagationD <	<not set=""> DC=example,DC=com <not set=""> <not set=""> {V1: Rags = 0x0; LatencySec 0x0 = ()</not></not></not>	is = 0; DsaGuic >		
Vew	Cancel Acoly	Fiter		

Esto se puede hacer para varios objetos dentro de AD. Por ejemplo, estos pasos se utilizan para buscar el DN del contenedor de usuario:



6. Se puede quitar la vista Funciones avanzadas. Haga clic con el botón derecho del ratón en el DN raíz, navegue hasta Ver y haga clic Funciones avanzadas una vez más.



Crear una cuenta FTD

Esta cuenta de usuario permitirá que FDM y FTD se enlacen con AD para buscar usuarios y grupos y autenticarlos. El propósito de crear una cuenta FTD independiente es evitar el acceso no autorizado a otras partes de la red si las credenciales utilizadas para el enlace se ven comprometidas. Esta cuenta no necesita estar dentro del alcance del DN base.

1. En Active Directory Users and Computers, haga clic con el botón derecho del ratón en el contenedor/organización al que se agregará la cuenta FTD. En esta configuración, la cuenta FTD se agregará bajo el contenedor Users bajo el nombre de usuario **ftd.admin@example.com**. Haga clic con el botón derecho del ratón en **Usuarios** y, a continuación, haga clic en **Nuevo > Usuario**.

Active Directory	Users and Comp	puters				-	×
File Action View	w Help						
🗢 🔿 🔁 📆	X 🗈 🗙 🛙	0 🔒 🛛	Þ	1 🗏 🐮 🛯	r 🗾 🔍		
Active Directory I Active Directory I Saved Queries Saved Queri	Users and Com s rs Controllers curityPrincipal: Service Accour Delegate Con Find	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. Desplácese por el Asistente Nuevo objeto - Usuario.

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

New Object - User		×
🤱 Create in: exar	nple.com/Users	
Password:	•••••	
Confirm password:	•••••	
User must change passw	rord at next logon	
User cannot change pas	sword	
Password never expires		
Account is disabled		
	< Back Next >	Cancel
New Object - User		×
New Object - User	mple.com/Users	×
New Object - User Create in: exam When you click Finish, the for	mple.com/Users billowing object will be created:	×
New Object - User Create in: exam When you click Finish, the for Full name: FTD Admin	mple.com/Users billowing 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	mple.com/Users billowing object will be created: @example.com	×
New Object - User Create in: example of the second	mple.com/Users billowing 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.adminu The password never expires	mple.com/Users billowing 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.admin The password never expires	mple.com/Users bilowing 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.adminu The password never expires	mple.com/Users bilowing object will be created: @example.com s.	×
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	mple.com/Users ollowing object will be created: @example.com s.	×
New Object - User Create in: exam When you click Finish, the for Full name: FTD Admin User logon name: ftd.adminu The password never expires	mple.com/Users pllowing object will be created: @example.com s.	×

3. Verifique que se haya creado la cuenta FTD. Además, se han creado dos cuentas adicionales, **Administración de TI** y **Usuario de prueba**.

Active Directory Users and Composite	uters			-	×
File Action View Help					
🗢 🔿 🙍 📷 🖌 🗈 🗶 📴	a 🔒 🛛 🖬	1 % 🔌 🛍 🖷	r 🧕 🗽		
Active Directory Users and Com Saved Queries	Name	Type User	Description A user account manage		^
 Builtin Computers Domain Controllers ForeignSecurityPrincipal: Managed Service Accourting Users 	Denied ROD DnsAdmins DnsUpdateP Domain Ad Domain Co Domain Con Domain Gue Domain Users	Security Group Security Group Security Group Security Group Security Group Security Group Security Group	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		
	Kenterprise A Enterprise K Enterprise R FTD Admin Group Polic	Security Group Security Group Security Group User Security Group User	Designated administrato Members of this group Members of this group Members in this group c Built-in account for gue		
<	LT Admin Key Admins Protected Us RAS and IAS Read-only D Schema Ad Test User	User Security Group Security Group Security Group Security Group User	Members of this group Members of this group Servers in this group can Members of this group Designated administrato		~

Crear grupos AD y agregar usuarios a grupos AD (opcional)

Aunque no se requiere para la autenticación, los grupos se pueden utilizar para facilitar la aplicación de políticas de acceso a varios usuarios, así como la autorización LDAP. En esta guía de configuración, los grupos se utilizarán más adelante para aplicar la configuración de la política de control de acceso a través de la identidad del usuario dentro de FDM.

1. En Active Directory Users and Computers, haga clic con el botón derecho en el contenedor/organización al que se agregará el nuevo grupo. En este ejemplo, el grupo Administradores de AnyConnect se agregará debajo del contenedor Usuarios. Haga clic con el botón derecho del ratón en Usuarios y, a continuación, haga clic en Nuevo > Grupo.

Active Directory Users and Com	puters			-	×
File Action View Help					
🗢 🔿 🙇 🚾 🕹 🗱	3 🙆 📑 🖬 🖬	e i 😤 📚 în 🤋	r 🧕 🕱		
Active Directory Users and Com Saved Queries Saved Queries Delegate Con Find	Name DefaultAcco Denied ROD DnsAdmins DnsUpdateP Domain Ad Domain Ad Domain Co ntrol ers	Type User Security Group Security Group Security Group Security Group Security Group Security Group Security Group 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	> > >	Computer Contact Group InetOrgPerson msDS-KevCreder	ntial .		
Export List Properties Help Read-only		msDS-ResourcePropertyList msDS-ShadowPrincipalContainer msImaging-PSPs MSMQ Queue Alias			
Creates a new item in this container.	Schema A	Printer User Shared Folder			~

2. Desplácese por el Asistente Nuevo objeto - grupo como se muestra en la imagen.

New Object - Group	×					
Create in: example.com/Users						
Group name:						
AnyConnect Admins						
Group name (ore-Windows 200	10)·					
AnyConnect Admins	~					
Group scope	Group type					
O Domain local	Security					
Global	Obstribution					
OUniversal						
	OK Cancel					

3. Verifique que se haya creado el grupo. También se ha creado el grupo **Usuarios de AnyConnect**.

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

4. Haga clic con el botón derecho del ratón en el grupo al que se agregarán los usuarios y, a continuación, seleccione **Propiedades**. En esta configuración, el usuario **IT Admin** se agregará al grupo **AnyConnect Admins** y el usuario **Test User** se agregará al grupo **AnyConnect Users**.

Active Directory Users and Computer	iters			-	×
File Action View Help					
🗢 🔿 🙍 📰 🤞 🖾 🔀	@ 🔒 🛛 🖬 🖏	k 🛯 🔻 🧕 🕯	5		
Active Directory Users and Com	Name AnyConnect Admins	Type Security Group	Description		^
Builtin Computers Some Domain Controllers	AnyConnect Users calo	Security Group User Security Group	Buil Move Mer Send Mail		
> ForeignSecurityPrincipal:	Cloneable Domain C DefaultAccount	Security Group User	Mer All Tasks A u:	>	
Users	Denied RODC Passw DnsAdmins DnsUpdateProxy Domain Admins Domain Computers Domain Controllers Domain Guests Domain Users	Security Group Security Group Security Group Security Group Security Group Security Group Security Group	Mer Cut DNS Delete DNS Rename Des All v Properties All v Help All communications All domain users		
	Enterprise Admins Enterprise Key Admins Enterprise Read-only FTD Admin Group Policy Creator Guest IT Admin Key Admins	Security Group Security Group User Security Group User User Security Group	Designated administrato Members of this group Members of this group Members in this group c Built-in account for gue Members of this group		
Renames the current selection.	(h.s				Ŷ

5. Haga clic en la ficha Miembros y luego haga clic en Agregar como se muestra en la imagen.

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

Ingrese el usuario en el campo y haga clic en el botón **Verificar nombres** para verificar que se encuentra el usuario. Una vez verificado, haga clic en **Aceptar**.

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

Compruebe que se ha agregado el usuario correcto y, a continuación, haga clic en el botón **Aceptar**. El usuario Test User también se agrega para agrupar usuarios de AnyConnect con el uso de los mismos pasos.

AnyConr	nect Admin	s Properties			?	×
General	Members	Member Of	Managed By			
Membe	ns:					_
Name 😤 IT	Admin	Active Dir example.c	ectory Domain S com/Users	Services Folder		
Ad	id	Remove	ОК	Cancel	Ар	ply

Copie la raíz del certificado SSL de LDAPS (sólo se requiere para LDAPS o STARTTLS)

1. Presione **Win+R** y escriba **mmc.exe**. Click OK.

💷 Run		×
9	Type the name of a program, folder, doo resource, and Windows will open it for y	cument, or Internet rou.
<u>O</u> pen:	mmc.exe	~
	OK Cancel	Browse

2. Vaya a Archivo > Agregar/quitar complemento... como se muestra en la imagen.

🖀 Console1 - [Console Root]		-	σ×
File Action View Favorites Window	Help		- 8 ×
New Ctrl+N			
Open Ctrl+O	Act	ions	
Save Ctrl+S	There are no items to show in this view.	nsole Root	_
Save As		More Actions	+
Add/Remove Snap-in Ctrl+M			
Options			
1 dnsmgmt			
2 dsa			
Exit			
Enables you to add snap-ins to or remove them fr	om the snap-in console.		

3. En los complementos disponibles, haga clic en Certificados y, a continuación, haga clic en Agregar.

Add or Remove Snap-ins				X
You can select snap-ins for t extensible snap-ins, you car	this console from the configure which e	nose xter	e available on your computer and configure the selected set of snap-ins. For ensions are enabled.	
Available snap-ins:			Selected snap-ins:	_
Snap-in	Vendor	^	Console Root Edit Extensions	
Active Directory Do	Microsoft Cor Microsoft Cor		Bemove	
Active Directory Use	Microsoft Cor Microsoft Cor		Move Up	1
AUSI Edit	Microsoft Cor		Add >	
Certificates	Microsoft Cor			
Component Services	Microsoft Cor			
Device Manager	Microsoft Cor			_
Disk Management	Microsoft and	\checkmark	Advanced	
Description:	we you to browea	the	e contants of the certificate stores for yourself, a service, or a computer	
	nis you to bromse		e contento or are certandate stores for yoursen, a service, or a computer.	
			OK Cancel	

4. Seleccione Computer account y luego haga clic en Next como se muestra en la imagen.

Certificates snap-in	×
This snap-in will always manage certificates for: 	
< Back Next > Cancel	

Haga clic en Finish (Finalizar).

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

5. Click OK.

Add or Remove Snap-ins					×
You can select snap-ins for t extensible snap-ins, you can	his console from the configure which e	nose exter	available on you nsions are enable	ur computer and configure the selected set of snap-ins. For ed.	
Available snap-ins:				S <u>e</u> lected snap-ins:	
Snap-in	Vendor	^		Console Root Edit Extensions	
Active Directory Do	Microsoft Cor Microsoft Cor			Certificates (Local Computer)	
Active Directory Use	Microsoft Cor Microsoft Cor			Move <u>U</u> p	
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				
Device Manager	Microsoft Cor				
📅 Disk Management	Microsoft and	~		Advanced	
Description: The Certificates snap-in allo	ws you to browse	the	contents of the	certificate stores for yourself, a service, or a computer.	
				OK Cancel	

6. Expanda la carpeta **Personal** y, a continuación, haga clic en **Certificados**. El certificado utilizado por LDAPS se debe emitir al nombre de dominio completo (FQDN) del servidor de Windows. En este servidor, hay 3 certificados en la lista.

- Un certificado CA emitido a y por ejemplo-WIN2016-CA.
- Un certificado de identidad emitido a WIN2016 por ejemplo-WIN2016-CA.
- Un certificado de identidad emitido para win2016.example.com por ejemplo-WIN2016-CA.

En esta guía de configuración, el FQDN es win2016.example.com, por lo que los primeros 2 certificados no son válidos para utilizarse como certificado SSL de LDAPS. El certificado de identidad emitido para win2016.example.com es un certificado que fue emitido automáticamente por el servicio CA de Windows Server. Haga doble clic en el certificado para comprobar los detalles.



- 7. Para ser utilizado como certificado SSL LDAPS, el certificado debe cumplir estos requisitos:
 - El nombre común o el nombre alternativo del asunto DNS coincide con el FQDN del servidor de Windows.
 - El certificado tiene autenticación de servidor en el campo Uso mejorado de clave.

En la pestaña Detalles del certificado, bajo **Asunto** y **Nombre alternativo del sujeto**, está presente el FQDN **win2016.example.com**.

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

🙀 Certi	ficate			×
General	Details	Certification Path		
Show:	<al)></al)>		~	
Field Sul Au Au Au	bject Key thority Ke L Distribu thority In bject Alte	Identifier y Identifier tion Points formation Access mative Name	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 Other Name:DS Object Guid=	^
Ke Th Th	y Usage umbprint umborint	algorithm	Digital Signature, Key Encipher sha1 <u>ca 8e 11 3d eb bc 0f 6e 4a.00</u>	~
Other N DS 0 18 DNS Na	Name: Object Gu Ime = 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	< .

En Uso mejorado de claves, Server Authentication está presente.

🙀 Certificate	×
General Details Certification Pa	th
Show: <all></all>	~
Field	Value ^
Subject Public key Public key parameters	win2016.example.com RSA (2048 Bits) 05 00
Certificate Template Name	DomainController
SMIME Capabilities Subject Key Identifier Authority Key Identifier Client Authentication (1.3.6.1.5.	[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. Una vez que se confirme, vaya a la pestaña **Ruta de certificación**. Haga clic en el certificado superior que debe ser el certificado de CA raíz y luego haga clic en el botón **Ver certificado**.

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

9. Esto abrirá los detalles del certificado para el certificado de CA raíz.

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 Statemen	t
OK	

10. Abra la pestaña **Detalles** y haga clic en **Copiar a archivo...** como se muestra en la imagen.

Certificate		×
General Details Certification Path		
Show: <all></all>	\checkmark	
Field	Value /	•
Version Serial number Signature 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	lit Properties Copy to File	3
	ОК	

11. Desplácese por el Asistente para exportación de certificados que exportará la CA raíz en 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 Cance	1

12. Seleccione Base-64 codificada X.509.

Ð	cort File Format
	Certificates can be exported in a valiety of the formats.
	Select the format you want to use:
	O DER encoded binary X.509 (.CER)
	Base-64 encoded X.509 (.CER)
	Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)
	Include all certificates in the certification path if possible
	 Personal Information Exchange - PKCS #12 (.PFX)
	 Include all certificates in the certification path if possible
	 Delete the private key if the export is successful
	Export all extended properties
	Enable certificate privacy
	 Microsoft Serialized Certificate Store (.SST)

13. Seleccione el nombre del archivo y el lugar al que se exportará.

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

		×
÷	🐉 Certificate Export Wizard	
	File to Export Specify the name of the file you want to export	
		-
	File name:	
	C:\Users\admin\Desktop\root.cer Browse	
	Next Cancel	

14. Haga clic en Finish (Finalizar).

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

15. Ahora, desplácese a la ubicación y abra el certificado con un bloc de notas o con algún otro editor de texto. Esto mostrará el certificado de formato PEM. Guarde esto para más adelante.

----BEGIN CERTIFICATE-----

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

Configuraciones de FDM

Verificación de licencias

Para configurar AnyConnect en FDM, el FTD deberá estar registrado con el servidor de licencias inteligente y se debe aplicar una licencia válida Plus, Apex o VPN Only al dispositivo.

1. Vaya a **Device > Smart License** como se muestra en la imagen.



2. Verifique que el FTD esté registrado en el servidor de licencias inteligente y que la licencia AnyConnect Plux, Apex o VPN Only esté habilitada.



Configurar origen de identidad AD

1. Navegue hasta Objetos > Orígenes de identidad, luego haga clic en el + símbolo y seleccione

AD como se muestra en la imagen.

cisco. Firepower Device	Manager Monitoring Policies	Cbjects Device: FTD-3	o 🔒 🗐 ? 🗄	admin Administrator
Object Types 🔶 🔶	Identity Sources			
C Networks	1 object		Q Search	+~
와 Ports	a NAME	THE	VALUE	RADIUS Server
🔒 Security Zones	1 LocalidentitySource	LOCAL		RADIUS Server Group
🐬 Application Filters				AD
Ø URLS				Identity Services Engine
Geolocations				
Syslog Servers				
🔏 IKE Policies				
🐴 IPSec Proposals				
🔒 AnyConnect Client				
E Identity Sources				
1 Users				
R Certificates				
🔒 Secret Keys				
DNS Groups				
Vert List Filters				

2. Complete los parámetros adecuados para el servidor de Active Directory con la información recolectada anteriormente. Si se utiliza un nombre de host (FQDN) para el servidor de Microsoft en lugar de una dirección IP, asegúrese de crear un grupo DNS adecuado en **Objetos > Grupo DNS**. A continuación, aplique ese grupo DNS al FTD navegando a **Device > System Settings > DNS Server**, aplicando el grupo DNS en **Management Interface** y **Data Interface**, y luego especifique la interfaz de salida adecuada para las consultas DNS. Haga clic en el botón **Prueba** para verificar una configuración y alcance exitosos desde la interfaz de administración de FTD. Dado que estas pruebas se inician desde la interfaz de administración del FTD y no a través de una de las interfaces enrutables configuradas en el FTD (como interna, externa, dmz), una conexión exitosa (o fallida) no garantiza el mismo resultado para la autenticación de AnyConnect, ya que las solicitudes de autenticación LDAP de AnyConnect se iniciarán desde una de las interfaces enrutables del FTD. Para obtener más información sobre la prueba de conexiones LDAP desde el FTD, revise las secciones Test AAA y Packet Capture en el área Troubleshooting.

Add Identity Realm

Ŀ.

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

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

Si se utiliza LDAPS o STARTTLS, seleccione el cifrado adecuado y, a continuación, seleccione el certificado de CA de confianza. Si la CA raíz no se ha agregado aún, haga clic en **Crear nuevo certificado de CA de confianza**. Proporcione un nombre para el certificado de CA raíz y luego pegue el certificado de CA raíz del formato PEM recolectado anteriormente.

Add Trusted CA Certificate

Name LDAPS_ROOT	
Paste certificate, or choose file: UPLOAD CERTIFICATE The supported formats are: PEM, DER.	
BEGIN CERTIFICATE MIIDCDCCAfCgAwIBAgIQE4ZG5Z1wT6IONTjooEQyMTANBgkqhkiG9w0BAQsFADAd MRswGQYDVQQDExJleGFtcGxILVdJTjIwMTYtQ0EwIBcNMjAwNDI3MTQ1MDU5WhgP MjA2MDA0MTkxNDUwNTIaMB0xGzAZBgNVBAMTEmV4YW1wbGUtV0IOMjAxNi1DQTCC ASIwDOX_IKoZlbwcNAOEBB0ADcoEPADCCAOccoEBAl8abT719NzSOnoOPb0YT67b	
CANCEL	ОК
Directory Server Configuration	
win2016.example.com:636	*

8 ×

Hostname / IP Address		Port	
win2016.example.com		636	
e.g. ad.example.com			
Encryption		Trusted CA certificate	
LDAPS	*	LDAPS_ROOT	~
TEST ✓ Connection to realm is suc	cessful		

En esta configuración, se utilizaron estos valores:

- Nombre: LAB-AD
- Nombre de usuario del directorio: ftd.admin@example.com
- DN base: DC=ejemplo,DC=com
- Dominio primario de AD: example.com
- Nombre de host/Dirección IP: win2016.example.com
- Puerto: 389

3. Haga clic en el botón **Cambios pendientes** en la parte superior derecha, como se muestra en la imagen.

cisco. Firepower De	wice Manager	题 Monitoring	Ø Policies	書面 Objects	Device: FTD-3		S 🖨 @	0	*	admin Administrator
Object Types 🛛 🗧 🗧	Identity So	urces								
C Networks	2 objects					Q	Search			+ ~
S Ports	H NAME			т	YPE	VALUE				ACTIONS
Security Zones	1 Localidenti	tySource		U	OCAL					
Application Filters	2 LAB-AD			A	D	win2016.exa	ample.com			

4. Haga clic en el botón Implementar ahora.

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

Configurar AnyConnect para la autenticación AD

Para utilizar el origen de identidad AD configurado, deberá aplicarse a la configuración de AnyConnect.

1. Vaya a **Device > Remote Access VPN** como se muestra en la imagen.

CISCO. Firepower Device Manager	题 👘 📅 Monitoring Policies Objects	Device: FTD-3	admin Administrator		
	0.0 [
Interfaces Connected Enabled 3 of 4 View All Interfaces > Smart License Registered View Configuration >	Routing 2 routes View Configuration > Backup and Restore View Configuration >	Updates Geolocation, Rule, VDB, System Upgrade, Security Intelligence Feeds View Configuration	System Settings Management Access Logging Settings DHCP Server DNS Server Management Interface Hostname NTP Cloud Services Reboot/Shutdown Traffic Settings		
Site-to-Site VPN There are no connections yet View Configuration	Remote Access VPN Configured 1 connection 2 Group Policies View Configuration	Advanced Configuration Includes: FlexConfig, Smart CLI View Configuration	Device Administration Audit Events, Deployment History, Download Configuration		

2. Haga clic en el símbolo + o en el botón Crear perfil de conexión como se muestra en la imagen.

cisco. Firepower Dev	vice Manager Monitoring	Policies Objects	Device: FTD-3	> 🖨 @ ?	admin Administrator
RA VPN +	Device Summary Remote Access VPN	Connection Prof	iles		
Connection Profiles					
Group Policies				Q. Search	+
	• NAME	***	GROUP POLICY	ACTIONS	
			There are no Remote Access	Connections yet.	
			Start by creating the first	Connection.	
			CREATE CONNECTION	PROFILE	

3. En la sección Connection and Client Configuration, seleccione el origen de identidad AD creado anteriormente. Configure los valores adecuados para las demás secciones, incluidos el nombre del perfil de conexión y la asignación del grupo de direcciones del cliente. Haga clic en **Enviar consulta** cuando haya terminado.

Connection and Client Configuration

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

Connection Profi This name is config	le Name ured as a connection allas, it ca	n be used	to connect to the VPN gateway
General			
Group Alias			Group URL
General			
Add Group Alias			Add Group URL
Primary Ident	ity Source		
Authentication Ty	/pe		
AAA Only	Client Certificate Only	AAA ai	nd Client Certificate
Primary Identity S	Source for User Authentica	tion	Fallback Local Identity Source 🔔
Filter		~	Please Select Local Identity Source 🗸
1 Localide	ntitySource		^
<u></u> LAB-AD		0	
11 Special-	Identities-Realm		✓
Create new 💙			
Client Addres	s Pool Assignment		
IPv4 Address Poo	bl		IPv6 Address Pool
Endpoints are provid	led an address from this pool		Endpoints are provided an address from this pool
C AnyConnect-F	Pool		
DHCP Servers			
+			
	CANCEL		SUBMIT QUERY

4. En la sección Experiencia de usuario remoto, seleccione la política de grupo adecuada. De forma predeterminada, se utilizará **DfltGrpPolicy**; sin embargo, se puede crear uno diferente.

```
View Group Policy
```

DfltGrpPolicy

Policy Group Brief Details

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

5. En la sección Configuración global, como mínimo, especifique los paquetes SSL Certificate, Outside Interface y AnyConnect. Si no se ha creado un certificado previamente, se puede seleccionar un certificado autofirmado predeterminado (<u>DefaultInternalCertificate</u>) sin embargo se verá un mensaje de certificado de servidor no confiable. La política de control de acceso de omisión para el tráfico descifrado (sysopt permit-vpn) debe desmarcarse para que las reglas de la política de acceso de identidad de usuario entren en vigor más adelante. La exención de NAT también se puede configurar aquí. En esta configuración, todo el tráfico ipv4 desde la interfaz interna que va a las direcciones IP del cliente AnyConnect es excepto desde NAT. Para configuraciones más complejas como el hairpinning externo a externo, se deberán crear reglas NAT adicionales bajo la política NAT. Los paquetes de AnyConnect se pueden encontrar en el sitio de soporte de Cisco: <u>https://software.cisco.com/download/home</u>. Se requiere una licencia Plus o Apex válida para descargar el paquete AnyConnect.

Global Settings

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

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



6. En la sección Resumen, verifique que AnyConnect esté configurado correctamente y, a continuación, haga clic en Enviar consulta.

Summary

Review the summary of the Remote Access VPN configuration.

General		
STEP 1: CONNECTION AND CLIENT CONFIGURATION	ON	
Primary Identity Source		
Authentication Type	AAA Only	
Primary Identity Source	赴 LAB-AD	
Fallback Local Identity Source	-	
Strip Identity Source server from username	No	
Strip Group from Username	No	
Secondary Identity Source		
Secondary Identity Source for User Authentication	n –	
Fallback Local Identity Source	-	
✓ Advanced		
Authorization Server		
Accounting Server		
Client Address Pool Assignment		

7. Haga clic en el botón **Cambios pendientes** en la parte superior derecha, como se muestra en la imagen.

cisco. Firepower Dev	ice Manager 🕅 😚 🗄 Monitoring Policies Ob	jects Device: FTD-3	S 🚑 🛛 🤅	admin Administrator				
RA VPN ←	Device Summary Remote Access VPN Connection I	Device Summary Remote Access VPN Connection Profiles						
Connection Profiles	Lablest		0. 6					
🚑 Group Policies	1 object		Q Search	÷				
	# NAME	***	GROUP POLICY	ACTIONS				
	1 General	Authentication: AAA Only Authorization: None Accounting: None	DfttGrpPoEcy					

8. Haga clic en Implementar ahora.

Pe		• • • • •	05
 ↓ ↓ 	ast Deployment Completed Successfully 16 Apr 2020 12:41 PM. See Deployment History		
	Deployed Version (16 Apr 2020 12:41 PM)	Pending Version CLEGEND Removed Added Edited]
0	Network Object Added: AnyConnect-Pool		^
	-	<pre>subType: Network value: 10.10.00/24 isSystemDefined: false dnsResolution: IPV4_AND_IPV6 name: AnyConnect-Pool</pre>	
0	RA VPN Added: NGFW-Remote-Access-VPN		
		<pre>vpnGatewaySettings[0].exemptNatRule: true vpnGatewaySettings[0].outsideFqdn: ftd3.example.com vpnGatewaySettings[0].bypassAccessControlForVPNTraffic: t name: NGFW-Remote-Access-VPN</pre>	
	anyconnectPackageFiles:		
	-	anyconnect-win-4.7.03052-webdeploy-k9.pkg	
	<pre>vpnGatewaySettings[0].serverCertificate:</pre>	FTD_3_Manual	
	<pre>vpnGatewaySettings[0].outsideInterface;</pre>	110-9-Honoox	
	-	outside	
	<pre>vpnGatewaySettings[0].insideInterfaces:</pre>		
	- vpnGatewaySettings[0].insideNetworks;	inside	~
MC	JRE AGTIONS *	CANGEL DEPLOT NOW V	

Habilitar la política de identidad y configurar las políticas de seguridad para la identidad de usuario

En este momento, los usuarios de AnyConnect deben poder conectarse correctamente, pero es posible que no puedan acceder a recursos específicos. Este paso habilitará la identidad del usuario de modo que sólo los usuarios de AnyConnect Admins puedan conectarse a los recursos internos con el uso de RDP y sólo los usuarios del grupo AnyConnect usuarios pueden conectarse a los recursos internos con el uso de HTTP.

1. Navegue hasta **Políticas > Identidad** y haga clic en **Habilitar política de identidad**.

cisco. Firepower De	wice Manager Monitoring	Policies Obj	bjects	Device: FTD-3	5_	۵ ۵	?	÷	admin Administrator	×
Security Policie ⊡ → ○ SSL Decry	S ption → <mark>Oktontity</mark> → OSec	wity intelligence \rightarrow	> 🕑 NAT	O Access Control	ightarrow Intrusic	on				
	Establishing User Identity You can use identity policies to collect identity information from connections, can then view usage based on user idi in the dashboards, and configure acce control based on user or user group. B linking network behavior, traffic, and e directly to individual users, the system help you identify the source of policy breaches, attacks, or network vulnerabilities.	user You entity ss Y USE vents can	iers 👥 ;	How Identity polic Passive authentication Act PASSIVE AUTHENTIC PASSIVE AUTHENTIC MULTIPLE MULTIPLE MULTIPLE DENTITY SOURCE IDENTITY SOURCE	CES	LEVERAGE IDE	NTITY			

Para esta configuración, no se necesita ninguna configuración adicional y la Acción predeterminada es suficiente.

nistrator	~						
Security Policies							
¢ <u>s</u>	+						
ACTION	5						
	¢2						

2. Navegue hasta **Políticas > NAT** y asegúrese de que NAT esté configurada apropiadamente. Si la excepción NAT configurada en los parámetros de AnyConnect es suficiente, no se necesitará ninguna configuración adicional aquí.

cisco. Firepowe	er Device I	Manager	Monitori	ng Policies	i≑≣ Objects	Device: FTD-3		۵ 🚑	0 ?	admin Admini	strator
Security Pol	licies										
⊡ → O SSL	Decryption	-> 🕑 ld	entity \rightarrow ()	Security Intelligen	ce 🔶 <table-cell> NA</table-cell>	T 🔿 🕝 Acce	ess Control \Rightarrow	Intrusion			
1 rule								Q Search			+
			OFFICINAL PACKET				TRANSLATED PACK	tπ.			
a NAME	TYPE	INTERFACES	SOUNCE AD	DESTINATIO	SOUNCE PORT	DESTINATIO	SOUNCE AD	DESTINATIO	SOURCE PORT	DESTINATIO	ACTIONS
Auto NAT Rules											
> # Internet_PAT	DYNAMIC	J ANY outside	any-ipv4	ANY	ANY	ANY	Interface	ANY	ANY	ANY	

3. Vaya a **Políticas > Control de acceso**. En esta sección, la acción predeterminada se establece en Block (Bloquear) y no se han creado reglas de acceso, por lo que una vez que un usuario de AnyConnect se conecte, no podrá acceder a nada. Haga clic en el símbolo + o en Crear regla de acceso para agregar una nueva regla.

cisco. Firepo	ower Device Manager	题 Monitoring	Ø Policies	前面 Objects	Device: FTD-3		0 🖨		* ad * Ac	imin Iministrator
🕫 Security i	Policies									
$\square \rightarrow \bigcirc$	SSL Decryption \rightarrow 🥏	Identity \rightarrow () :	iecurity Intellige	nce 🔶 📀 NA	AT $ ightarrow$ Acce	ss Control 🔿 🛛 🎙	Intrusion			
						Q Search				®. +
	sounce			DESTINATION						
e NAME	ACTION ZONES	NETWORKS	PORTS	20118	NETWORKS	PORTS/PROTO	APPLICATIONS	URLS	USERS	ACTIONS
				There are no a	iccess rules yet.					
				Start by creating (the first access rule.					
				CREATE A	CCESS RULE					
Default Action	Access Control 😑 Block	9, E, 🗸								

4. Rellene los campos con los valores adecuados. En esta configuración, los usuarios del grupo Administradores de AnyConnect deben tener acceso RDP a Windows Server en la red interna. Para el origen, la zona se configura como outside_zone, que es la interfaz exterior a la que se conectarán los usuarios de AnyConnect y la red se configura como el objeto AnyConnect. Pool que se configuró anteriormente para asignar direcciones IP a los clientes de AnyConnect. Para la identidad de usuario en FDM, el origen debe ser la zona y la red desde la que el usuario iniciará la conexión. Para el destino, la zona se configura como inside_zone, que es la interfaz interna en la que se encuentra Windows Server, la red se configura como el objeto Inside_Net, que es un objeto que define la subred en la que se encuentra Windows Server, y los puertos/protocolos se establecen en dos objetos de puerto personalizados para permitir el acceso RDP a través de TCP 3389 y UDP 3389.

Edit Access	Rul	e										×
Order Title 1 AC R Source/Destination	DP Ad	pplications URLs	Use	rs Intru	Action Allow	File policy ⁹ Log	ging					
SOURCE						DESTINATION						
Zones	+	Networks	÷	Ports	+	Zones	+	Networks	+	Ports/Protocols		+
outside_zone		C AnyConnect-Pool		ANY		inside_zone		Dinside_Net				
										\Leftrightarrow RDP-UDP		
Show Diagram	\supset	Not hit yet							CA	WCEL	ок	

En la sección Users (Usuarios), se agregará el grupo AnyConnect Admins para que se permita el acceso RDP a Windows Server a los usuarios que no formen parte de este grupo. Haga clic en el símbolo +, haga clic en la ficha Grupos, haga clic en el grupo correspondiente y, a continuación, haga clic en **Aceptar**. Tenga en cuenta que también se pueden seleccionar usuarios individuales y el origen de identidad.

Add Access Rule	0 ×
Order Title 1 V AC RDP Access Source/Destination Applications URLs Users In	Action Allow Allow Intrusion Policy Elle policy
AVAILABLE USERS	CONTROLLING ACCESS FOR USERS AND USER GROUPS
Y Filter	If you configure identity policies to establish user identity based on source IP address, you can control access based on user name or user group membership. By controlling access based on user identity, you can apply the appropriate access controls whether the user changes workstations or obtains a different address through DHCP. If you base rules on group membership, user
北, LAB-AD \ Account Operators ① 上AB-AD \ Administrators	network access changes as users change roles in your organization, moving from one group to another.
LAB-AD \ Allowed RODC Password Replication Group LAB-AD \ AnyConnect Admins	
1t, LAB-AD \ AnyConnect Users	
Create new Identity Realm CANCEL OK	
Show Diagram	CANCEL OK

Una vez seleccionadas las opciones correspondientes, haga clic en Aceptar.

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

5. Cree más reglas de acceso si es necesario. En esta configuración, se crea otra regla de acceso

para permitir que los usuarios del grupo Usuarios de AnyConnect accedan a HTTP al servidor de Windows.

Edit Access Rule					ø ×
Order Title		Action			
2 Y AC HTTP Acce	ess	🛃 Allow 🗸			
Source/Destination Applic	cations URLs Users	Intrusion Policy	File policy Logging		
SOURCE			DESTINATION		
Zones + N	Networks + Po	rts +	Zones +	Networks	+ Ports/Protocols +
G outside_zone	AnyConnect-Pool A	WY	inside_zone	C Inside_Net	чттн 🔁
Show Diagram	e Not hit yet				CANCEL OK
Edit Access Rule					ø ×
Order Title		Action			
2 Y AC HTTP Acce	ess	🔁 Allow 🗠			
Source/Destination Applic	cations URLs Users	Intrusion Policy	File policy Logging		
AVAILABLE USERS		+	1 CONTROLLING ACCESS	FOR USERS AND USER GRO	DUPS
LAB-AD \ AnyConnect Users	5		If you configure identity p address, you can control membership. By controllin appropriate access contro different address through network access changes from one group to anothe	olicies to establish user i access based on user na ng access based on user ols whether the user cha DHCP. If you base rules as users change roles in r.	identity based on source IP ame or user group r identity, you can apply the inges workstations or obtains a on group membership, user a your organization, moving
Show Diagram	Not hit yet				CANCEL OK

6. Verifique la configuración de la regla de acceso y luego haga clic en el botón Cambios

pendientes en la parte superior derecha como se muestra en la imagen.

al) CIS	Firepower Device Manager												
Ø	🕫 Security Policies												
Ģ	$h \rightarrow O sst$	Decryptio	o 🔶 📀 Iden	tity → 🔘 Se	curity Intelligence	ightarrow 🕗 NAT	→ <table-cell> Access</table-cell>	Control $ ightarrow$	Intrusion				
2 rule	s							Q Search				0	+
			SOURCE			DESTINATION							
•	NAME	ACTION	ZONES	NETWORKS	PORTS	ZONES	NETWORKS	PORTS/PROTO_	APPLICATIONS	UNLS	USENS		ACTIONS
>	1 AC RDP Access	→ Allow	outside_zone	AnyConnect-Pool	ANY	inside_zone	Inside_Net	RDP-TCP RDP-UDP	ANY	ANY	AnyConne	đ.C	
>	2 AC HTTP Access	Allow	outside_zone	AnyConnect-Pool	ANY	inside_zone	Inside_Net	HTTP	ANY	ANY	AnyConne	Ф.С.	
Defe	Default Action Access Control 😄 Block 🖏 📴 🖌												

7. Verifique los cambios y luego haga clic en Implementar ahora.

Pe	ending Changes		0	×
0	Last Deployment Completed Successfully 28 Apr 2020 01:35 PM. See Deployment History			
	Deployed Version (28 Apr 2020 01:35 PM)	Pending Version	LEGEND Removed Added	Edited
0	Access Rule Added: AC HTTP Access			^
	- - - -	users[0].name: AnyConnect User logFiles: false eventLogAction: LOG_NONE ruleId: 268435467 name: AC HTTP Access	rs	
	sourceZones:	outside_zone		
	destinationZones:			
	-	inside_zone		
	sourceNetworks:	And annual Back		
	-	AnyConnect-Pool		
	-	Inside Net		
	destinationPorts:			
	-	HTTP		
	users[0].identitySource:			
	-	LAB-AD		
0	Access Rule Added: AC RDP Access			~
-				_
M	DRE ACTIONS V	CANCEL	DEPLOY NOW	~

Verificación

Utilize esta sección para confirmar que su configuración funcione correctamente.

Configuración final

Configuración AAA

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

Configurar AnyConnect

```
> show running-config webvpn
webvpn
enable outside
http-headers
 hsts-server
  enable
  max-age 31536000
  include-sub-domains
  no preload
 hsts-client
  enable
 x-content-type-options
 x-xss-protection
 content-security-policy
anyconnect image disk0:/anyconnpkgs/anyconnect-linux64-4.7.03052-webdeploy-k9.pkg 1
anyconnect image disk0:/anyconnpkgs/anyconnect-win-4.7.03052-webdeploy-k9.pkg 2
anyconnect enable
tunnel-group-list enable
 cache
 disable
error-recovery disable
> show running-config tunnel-group
tunnel-group General type remote-access
tunnel-group General general-attributes
address-pool AnyConnect-Pool
authentication-server-group LAB-AD
tunnel-group General webvpn-attributes
group-alias General enable
> show running-config group-policy
group-policy DfltGrpPolicy attributes
vpn-tunnel-protocol ssl-client
split-tunnel-policy tunnelspecified
split-tunnel-network-list value DfltGrpPolicy|splitAcl
webvpn
 anyconnect ssl dtls none
> show running-config ssl
```

ssl trust-point FTD-3-Manual outside

Conéctese con AnyConnect y verifique las normas de política de control de acceso

Cisco AnyConnect Secure VPN: Contacting ftd: ftd3.example	Mobility Client – × B.example.com.
	Cisco AnyConnect ftd3.example.com Group: General Username: it.admin Password:
	OK Cancel
🚳 Cisco AnyConnect Secure	Mobility Client — 🗆 🗙
Connected to f ftd3.example	td3.example.com.
00:00:14	IPv4
O (i)	

User IT Admin se encuentra en el grupo AnyConnect Admins que tiene acceso RDP a Windows Server; sin embargo, no tiene acceso a HTTP. Al abrir una sesión RDP y Firefox en este servidor, se comprueba que este usuario sólo puede acceder al servidor a través de RDP.



Si ha iniciado sesión con un usuario de prueba que se encuentra en el grupo Usuarios de AnyConnect que tienen acceso HTTP pero no RDP, puede verificar que las reglas de la política de control de acceso están surtiendo efecto.



Troubleshoot

Utilize esta sección para confirmar que su configuración funcione correctamente.

Depuraciones

Este debug se puede ejecutar en la CLI de diagnóstico para resolver problemas relacionados con la autenticación LDAP: **debug Idap 255**.

Para resolver problemas de la política de control de acceso de identidad del usuario, el **sistema soporta firewall-engine-debug** se puede ejecutar en clish para determinar por qué el tráfico se permite o se bloquea inesperadamente.

Depuraciones LDAP en funcionamiento

```
[53] Session Start
[53] New request Session, context 0x00002bld13f4bbf0, reqType = Authentication
[53] Fiber started
[53] Creating LDAP context with uri=ldap://192.168.1.1:389
[53] Connect to LDAP server: ldap://192.168.1.1:389, status = Successful
[53] supportedLDAPVersion: value = 3
[53] supportedLDAPVersion: value = 2
[53] LDAP server 192.168.1.1 is Active directory
[53] Binding as ftd.admin@example.com
[53] Performing Simple authentication for ftd.admin@example.com to 192.168.1.1
[53] LDAP Search:
Base DN = [DC=example,DC=com]
Filter = [sAMAccountName=it.admin]
```

```
Scope
              = [SUBTREE]
[53] User DN = [CN=IT Admin, CN=Users, DC=example, DC=com]
[53] Talking to Active Directory server 192.168.1.1
[53] Reading password policy for it.admin, dn:CN=IT Admin,CN=Users,DC=example,DC=com
[53] Read bad password count 6
[53] Binding as it.admin
[53] Performing Simple authentication for it.admin to 192.168.1.1
[53] Processing LDAP response for user it.admin
[53] Message (it.admin):
[53] Authentication successful for it.admin to 192.168.1.1
[53] Retrieved User Attributes:
      objectClass: value = top
[53]
       objectClass: value = person
[53]
[53]
       objectClass: value = organizationalPerson
[53]
      objectClass: value = user
      cn: value = IT Admin
[53]
[53]
      sn: value = Admin
[53]
      givenName: value = IT
[53]
      distinguishedName: value = CN=IT Admin, CN=Users, DC=example, DC=com
      instanceType: value = 4
[53]
       whenCreated: value = 20200421025811.0Z
[53]
       whenChanged: value = 20200421204622.0Z
[53]
       displayName: value = IT Admin
[53]
      uSNCreated: value = 25896
[53]
[53]
      memberOf: value = CN=AnyConnect Admins,CN=Users,DC=example,DC=com
[53]
      uSNChanged: value = 26119
      name: value = IT Admin
[53]
       objectGUID: value = &...J..O..2w...c
[53]
[53]
       userAccountControl: value = 512
[53]
      badPwdCount: value = 6
[53]
      codePage: value = 0
[53]
      countryCode: value = 0
      badPasswordTime: value = 132320354378176394
[53]
[53]
      lastLogoff: value = 0
[53]
      lastLogon: value = 0
[53]
       pwdLastSet: value = 132319114917186142
      primaryGroupID: value = 513
[53]
      objectSid: value = .....{I...;....j...
[53]
[53]
      accountExpires: value = 9223372036854775807
[53]
      logonCount: value = 0
[53]
      sAMAccountName: value = it.admin
      sAMAccountType: value = 805306368
[53]
[53]
       userPrincipalName: value = it.admin@example.com
[53]
       objectCategory: value = CN=Person, CN=Schema, CN=Configuration, DC=example, DC=com
[53]
       dSCorePropagationData: value = 16010101000000.0Z
[53]
       lastLogonTimestamp: value = 132319755825875876
[53] Fiber exit Tx=515 bytes Rx=2659 bytes, status=1
[53] Session End
```

No se puede establecer la conexión con el 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
```

Soluciones potenciales:

- Verifique el ruteo y asegúrese de que el FTD reciba una respuesta del servidor LDAP.
- Si se utiliza LDAPS o STARTTLS, asegúrese de que se confía en el certificado de CA raíz correcto para que el intercambio de señales SSL pueda completarse correctamente.
- Verifique que se utilicen la dirección IP y el puerto correctos. Si se utiliza un nombre de host, verifique que DNS pueda resolverlo a la dirección IP correcta

Enlace de DN de inicio de sesión o contraseña incorrecta

```
[-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
```

Solución potencial: Verifique que el DN de inicio de sesión y la contraseña de inicio de sesión estén configurados correctamente. Esto se puede verificar en el servidor AD con **Idp.exe**. Para verificar que una cuenta puede enlazarse correctamente con el uso de Idp, navegue a través de estos pasos:

1. En el servidor AD, presione Win+R y busque Idp.exe.

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

2. Haga clic en Connection > Connect... como se muestra en la imagen.

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

3. Especifique localhost para el servidor y el puerto apropiado, luego haga clic en Aceptar.

Connect		×
<u>S</u> erver:	localhost	
Port:	389	Co <u>n</u> nectionless
<u>0</u> K		<u>C</u> ancel

4. La columna Derecha muestra el texto que indica una conexión correcta. Haga clic en Conexión
> Enlazar... como se muestra en la imagen.

🔐 Idap://w	/in2016.ex	ample.co	om/DC	= example, DC	=com		—		×
Connection	Browse	View	Optio	ns Utilities	Help				
Connee Bind Discon New Save Save As Exit	ct nect	Ctrl+B		Id = Idap_op Established Retrieving b Getting 1 en Dn: (RootD configu CN= current Tim defaultM dnsHos domain0 domain0 dosServi Set Firs Nan con forestFi highest isGlobal isSynch	en("localhos connection ase DSA inf tries: SE) rationNaming =Configurati Time: 5/1/20 e; VamingConte tName: win2 ControllerFui functionality iceName: CN tings,CN=Wi st-Site- ne,CN=Sites n; unctionality: CommittedU? ICatalogRea pronized: TR viceName: (st", 389); <u>to localhost.</u> formation gContext: on,DC=examp 20 4:16:55 PM ext: DC=example nctionality: 7 = (2016.example nctionality: 7 = (2016.example nctionality: 7 = (2016.example nctionality: 7 = (2016.example	le,DC=cl 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. Seleccione **Simple Bind** y especifique el nombre de usuario y la contraseña de la cuenta de directorio. Click OK.

Bind	×							
<u>U</u> ser: Password:	ftd.admin@example.com							
<u>D</u> omain:								
Bind type Bind as <u>c</u> u Bind with c <u>Simple bind</u> <u>A</u> dvanced	rrently logged on user redentials (DIGEST) affic after bind							
Ad <u>v</u> anced	Cancel OK							

Con un enlace exitoso, Idp mostrará Authenticated como DOMAIN\username.

🔐 Idap://w	in2016.exa	mple.co	om/DC=ex	ample,DC	=com		_		\times	
Connection	Browse	View	Options	Utilities	Help					
		1.2.840.113556.1.4.2255; 1.2.840.113556.1.4.2256; 1.2.840.113556.1.4.2309; supportedLDAPPolicies (20): MaxPoolThreads; MaxPercentDirSyncRequests; MaxDatagramRec MaxReceiveBuffer; InitRecvTimeout; MaxConnections; MaxConnldleTime; MaxPageSiz MaxBatchReturnMessages; MaxQueryDuration; MaxDirSyncDuration; MaxTempTableSize; MaxResultSetSize; MinResultSets; MaxResultSetsPerConn; MaxNotificationPerConn MaxValRange; MaxValRangeTransitive; ThreadMemoryLimit; SystemMemoryLimitPercent supportedLDAPVersion (2): 3; 2; supportedSASLMechanisms (4): GSSAPI; GSS- SPNEGO; EXTERNAL; DIGEST-MD5;								
			re < 	es = Idap_s unavailable authenticate	imple_bind e>); // v.3 d as: 'EXA	_s(ld, 'ftd.adn MPLE\ftd.adm	nin@exar nin'.	nple.com		
l Ready			J						×	

Si intenta un enlace con un nombre de usuario o una contraseña no válidos, se producirá un error como este.

Idap://win2016.example.com/DC=example,DC=com - 🛛											
Connection	Browse	View	Options	Utilities	Help						
			<pre>maxResultSetSize; MinResultSetS; MaxResultSetSPerConn; MaxNotificationPerConn; MaxValRange; MaxValRangeTransitive; ThreadMemoryLimit; SystemMemoryLimitPercent; supportedLDAPVersion (2): 3; 2; supportedSASLMechanisms (4): GSSAPI; GSS- SPNEGO; EXTERNAL; DIGEST-MD5; </pre>								
			r K E S C E ir	es = Idap_s sunavailable rror <49>: I server error comment: Ac rror 0x8009 nvalid	imple_bind_ i>); // v.3 idap_simple_ :: 80090308: cceptSecuri 90308 The to	s(Id, 'wrong _bind_s() fai : LdapErr: DS tyContext er oken supplie	@exampl iled: Invali SID-0C09(ror, data d to the fi	le.com', d Credentia 042A, 52e, v3839 unction is	s V		
Ready											

El servidor LDAP no puede encontrar el nombre de usuario

```
[-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
```

Solución potencial: Verifique que AD pueda encontrar al usuario con la búsqueda realizada por el FTD. Esto también se puede hacer con ldp.exe.

1. Después de enlazar correctamente, navegue hasta Ver > Árbol como se muestra en la imagen.

Idap://win2016.example.com/DC=example,DC=com										Х		
Connection	Browse	View	/ Options	Utilities	Help							
		~	Tree Enterprise Status Bar	Configurat	ion	Ctrl+T	/axP sts; cvTir	/axPoolThreads; sts; MaxDatagramRec				
			Set Font				nidle s: Mi	eTime; I axQue	MaxPage: rvDuratio	Size; n:		
				s; MaxQueryDuration MaxDirSyncDuration; MaxTempTableSize; MaxResultSetSize; MinResultSets; MaxResultSetsPerConn; MaxNotificationPerC MaxValRange; MaxValRangeTransitive; ThreadMemoryLimit; SystemMemoryLimitPerc supportedLDAPVersion (2): 3; 2; supportedLDAPVersion (2): 3; 2; SPNEGO; EXTERNAL; DIGEST-MD5;								
				res = ldap_simple_bind_s(ld, 'ftd.admin@example.com', <unavailable>); // v.3 Authenticated as: 'EXAMPLE\ftd.admin'. </unavailable>								
			J								×	

2. Especifique el DN base configurado en el FTD y haga clic en Aceptar.

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

3. Haga clic con el botón derecho del ratón en el DN base y, a continuación, haga clic en Buscar como se muestra en la imagen.

🔝 Idap://wi	n2016.exa	– 🗆 X				
Connection	Browse	View	Options	Utilities	Help	
DC = exam	ple,DC= c	om	Search Virtual L Delete Modify Modify Add chil Compar Advance Copy DN Copy Select al Clear ou	ist View DN Id e ed N	Ctrl+S Ctrl+D Ctrl+M Ctrl+R Ctrl+A Ctrl+A	cipals,DC=example,DC=com; 11D2B9AA00C04F79F805:CN =example,DC=com; 11D297C400C04FD8D5CD:C =example,DC=com; 11D1ADED00C04FD8D5CD:C =example,DC=com; 11D1AADED00C04FD7D83A:O s,DC=example,DC=com; 11D1ADED00C04FD8D5CD:C ample,DC=com; 11D1ADED00C04FD8D5CD:C ample,DC=com; 11D1ADED00C04FD8D5CD:C e,DC=com; 0 3:43:59 PM Eastern Daylight 2:41:57 PM Eastern Daylight
			-			•
Create a new d	locument					

4. Especifique los mismos valores Base DB, Filter y Scope que se ven en las depuraciones. En este ejemplo, estos son:

- DN base: dc=ejemplo,dc=com
- Filtro: samaccounting tname=it.admi
- Ámbito:SUBTREE

🟠 Idap://w	n2016.example.com/DC=example,DC=com	– 🗆 ×
Connection	Browse View Options Utilities Help	
Search	>	C=example,DC=com; S8811D1ADED00C04FD8D5CD:C
Base DN:	DC=example,DC=com	58811D1ADED00C04FD8D5CD:C
Filter:	sAMAccountName=it.admi ~	ample,DC=com; D211D1AA4B00C04FD7D83A:O
Scope Base	One Level Subtree	lers,DC=example,DC=com; 58811D1ADED00C04FD8D5CD:C example,DC=com;
Attributes:	objectClass;name;description;canonicalName ~	68811D1ADED00C04FD8D5CD:C mple,DC=com; :020 3:43:59 PM Eastern Daylight
Options	Run Close)20 2:41:57 PM Eastern Daylight
	***Searching Idap_search_s(Id, "DC "sAMAccountName=it. Getting 0 entries:	=example,DC=com", 2, admi", attrList, 0, &msg) ∀
Ready		

ldp encuentra 0 entradas debido a que no hay una cuenta de usuario con el **samaccounting tname=it.admi** bajo el DN base dc=example,dc=com.

Intentar de nuevo con el **samaccountname=it.admin** correcto muestra un resultado diferente. Idp encuentra 1 entrada bajo el DN base dc=example,dc=com e imprime el DN del usuario.

Idap://win2016.example.com/DC=exam	ple,DC	=com		– 🗆 ×
Connection Browse View Options U	tilities	Help		
Search			×	58811D1ADED00C04FD8D5CD:C DC=example,DC=com; 58811D1ADED00C04FD8D5CD:C
Base DN: DC=example,DC=com			\sim	ample,DC=com;
Filter: sAMAccountName=it.admin			\sim	lers,DC=example,DC=com;
Scope O <u>B</u> ase O <u>O</u> ne Level <u>Subtree</u>				58811D1ADED00C04FD8D5CD:C example,DC=com; 68811D1ADED00C04FD8D5CD:C mple,DC=com;
Attributes: objectClass;name;description;ca	nonicali	Name	\sim	020 3:43:59 PM Eastern Daylight
O <u>p</u> tions <u>R</u> un		<u>C</u> lose)20 2:41:57 PM Eastern Daylight
***Se Idap "sAM Getti Dn:	earching search Accou ing 1 en CN=IT A canonic name: IT objectCl use	g n_s(ld, " ntName tries: Admin, alName Admin; ass (4): r;	DC=e =it.ad CN=U : exar ; : top;	example,DC=com", 2, Imin", attrList, 0, &msg) Jsers,DC=example,DC=com mple.com/Users/IT Admin; person; organizationalPerson;
Ready				

Contraseña incorrecta para el nombre de usuario

```
[-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
```

Solución potencial: Verifique que la contraseña del usuario esté configurada correctamente y que no haya caducado. Al igual que el DN de inicio de sesión, el FTD realizará un enlace contra AD con las credenciales del usuario. Este enlace también se puede hacer en ldp para verificar que AD pueda reconocer las mismas credenciales de nombre de usuario y contraseña. Los pasos en ldp se muestran en la sección **Enlace de DN de Inicio de Sesión y/o Contraseña Incorrecta**. Además, los registros del Visor de eventos del servidor de Microsoft se pueden revisar por un posible motivo.

Prueba AAA

El comando test aaa-server se puede utilizar para simular un intento de autenticación del FTD con un nombre de usuario y una contraseña específicos. Esto se puede utilizar para probar las fallas de conexión o autenticación. El comando es **test aaa-server authentication [AAA-server] host [AD IP/hostname]**.

```
> show running-configuration aaa-server
aaa-server LAB-AD protocol ldap
realm-id 7
aaa-server LAB-AD host win2016.example.com
server-port 389
ldap-base-dn DC=example,DC=com
ldap-scope subtree
ldap-login-password *****
ldap-login-dn ftd.admin@example.com
server-type auto-detect
> test aaa-server authentication LAB-AD host win2016.example.com
Username: it.admin
Password: *******
INFO: Attempting Authentication test to IP address (192.168.1.1) (timeout: 12 seconds)
INFO: Authentication Successful
```

Capturas de paquetes

Las capturas de paquetes se pueden utilizar para verificar el alcance del servidor AD. Si los paquetes LDAP dejan el FTD, pero no hay respuesta, esto podría indicar un problema de ruteo.

Esta es una captura hecha que muestra el tráfico LDAP bidireccional:

> 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>
                        192.168.1.17.61960 > 192.168.1.1.389: P 3681912835:3681912980(145)
   4: 23:02:16.772482
ack 491521507 win 32768 <nop,nop,timestamp 1061373059 0>
                        192.168.1.1.389 > 192.168.1.17.61960: P 491521507:491522141(634) ack
  5: 23:02:16.772924
3681912980 win 65160 <nop,nop,timestamp 762393885 1061373059>
                          192.168.1.17.61960 > 192.168.1.1.389: . ack 491522141 win 32768
   6: 23:02:16.772955
<nop,nop,timestamp 1061373059 762393885>
   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>
  8: 23:02:16.775030
                          192.168.1.1.389 > 192.168.1.17.61960: P 491522141:491522163(22) ack
3681913024 win 65116 <nop,nop,timestamp 762393887 1061373060>
   9: 23:02:16.775075
                          192.168.1.17.61960 > 192.168.1.1.389: . ack 491522163 win 32768
<nop,nop,timestamp 1061373061 762393887>
[...]
54 packets shown
```

Registros del Visor de eventos de Windows Server

Los registros del Visor de eventos en la furgoneta del servidor AD proporcionan información más detallada sobre el motivo del error.

1. Busque y abra Event Viewer.

=	Best match											
ŵ	Event Viewer Desktop app											
	Settings	Settings >										
	🖄 Vie	ever	nt logs									
۲	D1	٢	ß		2	æ	រុក					
	event											
-	Q	([])	e	-	2		8					

2. Expanda **Registros de Windows** y haga clic en **Seguridad**. Busque **Falla de Auditoría** con el Nombre de Cuenta del usuario y revise la Información de Fallas como se muestra en la imagen.



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