AnyConnectクライアント用にFDMによって管理 されるFTDでのAD(LDAP)認証およびユーザIDの 設定

内容

概要 前提条件 要件 使用するコンポーネント 設定 ネットワークダイアグラムとシナリオ ADの 設定 LDAPベースDNの決定 FTDアカウントの作成 <u>ADグループの作成とADグループへのユーザの追加(オプション)</u> LDAPS SSL証明書ルートのコピー(LDAPSまたはSTARTTLSでのみ必要) FDMの構成 ライセンスの確認 AD IDソースの設定 AD認証用のAnvConnectの設定 アイデンティティポリシーの有効化とユーザIDのセキュリティポリシーの設定 確認 **Final Configuration** AnyConnectによる接続とアクセスコントロールポリシールールの確認 トラブルシュート デバッグ LDAPデバッグの動作 LDAPサーバとの接続を確立できない Binding Login DN and/or Password Incorrect LDAPサーバがユーザ名を見つけることができない ユーザ名のパスワードが正しくない AAAのテスト パケット キャプチャ Windows Serverイベントビューアのログ

概要

このドキュメントの目的は、Firepower Device Management(FDM)によって管理されるCisco Firepower Threat Defense(FTD)に接続するAnyConnectクライアントのActive Directory(AD)認証 を設定する方法を詳しく説明します。 AnyConnectユーザを特定のIPアドレスおよびポートに制 限するために、アクセスポリシーでユーザIDが使用されます。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- FDMでのRA VPN設定に関する基礎知識
- FDMでのLDAPサーバ設定に関する基礎知識
- ADに関する基礎知識

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Microsoft 2016サーバ
- 6.5.0を実行するFTDv

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このド キュメントで使用するすべてのデバイスは、初期(デフォルト)設定の状態から起動しています 。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してく ださい。

設定

ネットワークダイアグラムとシナリオ



Windowsサーバには、ユーザーIDをテストするため、インターネットインフォメーションサービス(IIS)およびリモートデスクトッププロトコル(RDP)があらかじめ設定されています。この設定 ガイドでは、3つのユーザアカウントと2つのグループが作成されます。

ユーザアカウント:

- FTD管理者:これは、FTDがADサーバにバインドできるように、ディレクトリアカウントとして使用されます。
- •IT管理者:ユーザIDを実証するために使用されるテスト管理者アカウント。

・テストユーザー:ユーザIDを実証するために使用されるテストユーザアカウント。
 グループ:

- AnyConnect Admins:ユーザIDを実証するためにIT管理者が追加されるテストグループ。この グループには、Windows ServerへのRDPアクセスのみが許可されます
- AnyConnect ユーザ:ユーザIDを実証するためにテストユーザが追加されるテストグループ。 このグループには、Windows ServerへのHTTPアクセスのみが許可されます

ADの設定

FTDでAD認証とユーザIDを適切に設定するには、いくつかの値が必要です。FDMで構成を行う前 に、これらの詳細をすべてMicrosoft Serverで作成または収集する必要があります。主な値は次の とおりです。

- [Domain Name]:これは、サーバのドメイン名です。この設定ガイドでは、example.comが ドメイン名です。
- ・サーバIP/FQDNアドレス: Microsoftサーバに到達するために使用されるIPアドレスまたは FQDN。FQDNを使用する場合、FQDNを解決するには、FDMおよびFTD内でDNSサーバを 設定する必要があります。この設定ガイドでは、これらの値はwin2016.example.comで、 192.168.1.1に解決されます。
- ・サーバポート:LDAPサービスで使用されるポート。デフォルトでは、LDAPとSTARTTLSは LDAPにTCPポート389を使用し、LDAP over SSL(LDAPS)はTCPポート636を使用します。
- ルートCA:LDAPSまたはSTARTTLSを使用する場合、LDAPSで使用されるSSL証明書の署名 に使用されるルートCAが必要です。
- ディレクトリのユーザ名とパスワード:これは、FDMとFTDがLDAPサーバにバインドし、 ユーザを認証し、ユーザとグループを検索するために使用するアカウントです。この目的で、 FTD Adminという名前のアカウントが作成されます。
- •基本識別名(DN):ベースDNはFDMの開始点であり、FTDはActive Directoryに対してユーザの 検索時に開始するように指示します。この設定ガイドでは、ルートドメインexample.comが ベースDNとして使用されます。ただし、実稼働環境では、LDAP階層内でベースDNをさらに 使用する方が適している場合があります。たとえば、次のLDAP階層を使用します。



管理者がマーケティング組織ユニット内のユーザにベースDNを認証できるようにしたい場合は、 ルート(example.com)に設定できます。ただし、これは、Finance組織ユニットのUser1もログイ ンできます。これは、ユーザ検索がルートで始まり、Finance、Marketing、Researchに移動する ためです。

ベースDNをexample.comに設定します。



ログインをマーケティング組織単位以下のユーザだけに制限するには、管理者がBase DNを Marketingに設定します。これで、User2とUser3のみが認証を実行できます。これは、検索がマ ーケティングで開始されるためです。

[Base DN set to Marketing]:



FTD内でより詳細な制御を行うために、ユーザが接続したり、AD属性に基づいて異なる許可をユ ーザに割り当てたりできるように、LDAP許可マップを設定する必要があることに注意してくだ さい。

この簡素化されたLDAP階層は、この設定ガイドで使用され、ルートexample.comのDNがベース DNに使用されます。



LDAPベースDNの決定

1. ADユーザーとコンピューターを開きます。

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

2.ルートドメイン(コンテナを開くには)を左クリックし、ルートドメインを右クリックして、 [View]に移動し、[Advanced Features]をクリックします。



3.これにより、ADオブジェクトの下に追加のプロパティが表示されます。たとえば、ルート example.comのDNを検索するには、**example.com**を右クリックし**て、Properties**に移動**します**。



4. [プロパティ]の下**の[**属性エディタ]タ**ブをクリック**します。属性の下**でdistinguishedName**を検 索し、[表示]をクリ**ックします**。

example.com Properties					?	×
General Managed By 0	bject	Security	Attribut	te Editor		
Attributes:						
Attribute	Value					^
dc	exam	ple				
defaultLocalPolicyObj	<not a<="" td=""><th>set></th><td></td><td></td><td></td><td></td></not>	set>				
description	<not a<="" td=""><th>set></th><td></td><td></td><td></td><td></td></not>	set>				
desktop Profile	<not a<="" td=""><th>set></th><td></td><td></td><td></td><td></td></not>	set>				
displayName	<not a<="" td=""><th>set></th><td></td><td></td><td></td><td></td></not>	set>				
displayNamePrintable	knot s	set>	_			
distinguishedName	DC-e	scample_D	C=com			
domainPolicyObject	<not s<="" td=""><th>set></th><td></td><td></td><td></td><td></td></not>	set>				
domainReplica	<not s<="" td=""><th>set></th><td></td><td></td><td></td><td></td></not>	set>				
dSASignature	{V1:	Flags = 0x	0; Later	ncySecs	= 0; DsaGui	:
dSCorePropagationD	0x0 =	· ()				
eFSPolicy	<not a<="" td=""><th>set></th><td></td><td></td><td></td><td></td></not>	set>				
extensionName	<not a<="" td=""><th>set></th><td></td><td></td><td></td><td></td></not>	set>				
flags	<not a<="" td=""><th>set></th><td></td><td></td><td></td><td>~</td></not>	set>				~
<					>	
View					Filter	
OK		Cancel		Apply	He	þ

5.これにより、新しいウィンドウが開き、DNを後でコピーしてFDMに貼り付けることができます。この例では、ルートDNはDC=example、DC=comです。値をコピーします。[OK]をクリックして[String Attribute Editor]ウィンドウを終了し、もう一度[OK]をクリックして[Properties]を終了します。

ing Attribute Editor		×		
tribute: distingu	ishedName			
lue: Cexample,DCecom Clear	ОК	Cancel	Undo Cut Copy Paste Delete Select All Right to left Reading order	
			Insert Unicode control character	>
eneral Managed By C Attributes:	bject Security Attribute Editor			
Attribute cn controlAccessRights creationTime dc defautLocalPolicyObj description desktopProfile displayName displayName displayName displayName displayName displayName	Value <not set=""> <not set=""> 4/29/2020 2:43:49 PM Eastern Di example <not set=""> <not s<="" th=""><th>Aaylight Tim</th><th></th><th></th></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not></not>	Aaylight Tim		

これは、AD内の複数のオブジェクトに対して実行できます。たとえば、ユーザコンテナのDNを 検索するには、次の手順を使用します。



6. [拡張機能]ビューは削除できます。ルートDNを右クリックし、[View]に移動し、[Advanced Features]をもう一度クリックします。



FTDアカウントの作成

このユーザアカウントを使用すると、FDMとFTDをADにバインドし、ユーザとグループを検索し て認証できます。別のFTDアカウントを作成する目的は、バインディングに使用されるクレデン シャルが侵害された場合に、ネットワーク内の他の場所で不正アクセスを防止することです。こ のアカウントは、ベースDNの範囲内である必要はありません。

1. [Active Directory Users and Computers]で、FTDアカウントを追加するコンテナまたは組織を 右クリックします。この構成では、FTDアカウントがユーザ名ftd.admin@example.comの下の Usersコンテナに追加**されます**。[Users]を右クリック**し、**[New] > [User]**をクリックします**。

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		^
Find 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. 「新規オブジェクト – ユーザー」**ウィザードをナビゲート**します。

New Object - User		×
🤱 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	<u>Wi</u> ndows 2000):	
EXAMPLE\	ftd.admin	
	< Back Next > Cancel	

New Object - User		х
Create in: example.com	n/Users	
Password:	••••	
Contirm password:	••••	
User must change password at n	ext logon	
User cannot change password		
Password never expires		
Account is disabled		
[< Back Next > Cancel	
New Object - User		х
New Object - User	n/Users	×
New Object - User Create in: example.com When you click Finish, the following	n/Users object will be created:	~
New Object - User Create in: example.com When you click Finish, the following Full name: FTD Admin	n/Users object will be created:	×
New Object - User Create in: example.com When you click Finish, the following Full name: FTD Admin User logon name: ftd.admin@example.com	n/Users object will be created:	×
New Object - User Create in: example.com When you click Finish, the following of Full name: FTD Admin User logon name: ftd.admin@examp The password never expires.	n/Users object will be created: xle.com	×
New Object - User Create in: example.com When you click Finish, the following Full name: FTD Admin User logon name: ftd.admin@examp The password never expires.	n/Users object will be created: xle.com	×
New Object - User Create in: example.com When you click Finish, the following Full name: FTD Admin User logon name: ftd.admin@examp The password never expires.	n/Users object will be created: n/e.com	×
New Object - User Create in: example.com When you click Finish, the following Full name: FTD Admin User logon name: ftd.admin@examp The password never expires.	n/Users object will be created: lle.com	×
New Object - User Create in: example.com When you click Finish, the following Full name: FTD Admin User logon name: ftd.admin@examp The password never expires.	n/Users object will be created: Ne.com	×
New Object - User Create in: example.com When you click Finish, the following Full name: FTD Admin User logon name: ftd.admin@examp The password never expires.	n/Users object will be created: we.com	×

3. FTDアカウントが作成されたことを確認します。さらに、IT Adminと**Test User**という2つの追 加アカウン**トが作成**さ**れました**。

Active Directory Users and Comp	puters			-	×
File Action View Help					
🗢 🔿 🖄 📅 🐇 🗈	i 🧟 🔒 🛛 🖬	1 🙁 🔌 🛍 🦷	7 🗾 🗽		
Active Directory Users and Com > Saved Queries > \$ avent of the set of th	Name DefaultAcco Denied ROD	Type User Security Group	Description A user account manage Members in this group c		^
 Builtin Computers Domain Controllers ForeignSecurityPrincipal: Managed Service Accour Users 	DnsAdmins DnsUpdateP Domain Ad Domain Co Domain Co Domain Gue Domain Gue Enterprise A Enterprise K	Security Group Security Group Security Group Security Group Security Group Security Group Security Group Security Group Security Group	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		
	Enterprise R FTD Admin Group Polic Guest	Security Group User Security Group User User	Members of this group Members in this group c Built-in account for gue		
	Key Admins Protected Us RAS and IAS Read-only D Schema Ad Test User	Security Group 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		
, ,	128.112 11 11 11		n <u>si rr</u>		Ŷ

ADグループの作成とADグループへのユーザの追加(オプション)

認証に不要なグループを使用すると、アクセスポリシーを複数のユーザに簡単に適用したり、 LDAP認可を適用したりできます。この構成ガイドでは、グループを使用して、後でFDM内のユ ーザーIDを介してアクセス制御ポリシー設定を適用します。

1. [Active Directory Users and Computers]で、新しいグループが追加されるコンテナ/組織を右ク リックします。この例では、グループAnyConnect AdminsがUsersコンテナの下に追加されます 。[ユーザー]を右クリックし、[新規作成] > [グループ]をクリックします。

Active Directory Users and Comp	puters			-	×
File Action View Help					
🗢 🔿 🙍 📅 🔏 🗈 🗶 🛛	i 🖸 🔒 🖬 🖬	1 🗏 🐮 🛙 🤊	r 🧕 🔍		
Active Directory Users and Com Active Directory Users and Com Saved Queries Example.com Builtin Computers Domain Controllers Domain Controllers Domain Controllers Domain Ad. Domain Ad. Domain Co. Users Delegate Control Find New All Tasks View Refresh Export List Properties Help		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 guests All domain users		^
		Contact Group InetOrgPerson msDS-KeyCreder msDS-ResourceP msDS-ShadowPr msImaging-PSPs MSMQ Queue Al	itial PropertyList incipalContainer ias		
Creates a new item in this container.	Schema A	Printer User Shared Folder			Ŷ

2.図に示すように、**New Object - Group** Wizardをナビゲートします。

New Object - Group	×
🥵 Create in: exan	nple.com/Users
Group name:	
AnyConnect Admins	
Group name (are Windows 20	200)+
AnyConnect Admins	~~~
Group scope	Group type
O Domain local	Security
Global	Obstribution
OUniversal	
	OK Cancel

3.グループが作成されたことを確認します。AnyConnect Users**グループ**も作成されています。

Active Directory Users and Complexity	puters			-	×
File Action View Help					
🗢 🔿 🖄 📰 🕹 🔛 🗉	è 🛛 📼 🐍 🗽 🛍 '	🔻 🗾 🙇			
Active Directory Users and Com Active Directory Users and Com Builtin Builtin Computers Domain Controllers ForeignSecurityPrincipals Managed Service Accour Users	Name AnyConnect Admins AnyConnect Users Calo Cert Publishers Cloneable Domain C DefaultAccount DefaultAccount Donain RODC Passw DnsUpdateProxy DonsAdmins DonsUpdateProxy Domain Admins Domain Computers Domain Computers Domain Computers Domain Guests Domain Guests Domain Guests Domain Users Enterprise Admins Enterprise Read-only FTD Admin Group Policy Creator Guest IT Admin	Type Security Group Security Group User Security Group Security Group 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 users Designated administrato Members of this group Members of this group c Built-in account for gue		
< >>	(h				¥

4.ユーザーを追加するグループを右クリックし、「プロパティ」を選**択します**。この構成では、 ユーザーIT AdminがグループAnyConnect Adminsに追加され、ユーザーTest Userがグループ AnyConnect Usersに追加されます。

Active Directory Users and Comp		-	×		
File Action View Help					
🗢 🔿 🙍 📅 🐇 🗈 🗶 🖫] @ 🔒 🛛 🖬 🖏 !	k 🛙 🔻 🧕 🕯	6		
Active Directory Users and Com > 2 Saved Queries	Name	Type Security Group	Description		^
 ✓ is example.com > is Builtin > is Computers > is Domain Controllers > is ForeignSecurityPrincipal: > is Managed Service Accourticy 	AnyConnect Users Celo Cert Publishers Cloneable Domain C DefaultAccount	Security Group User Security Group Security Group User	Add to a group Buil Move Mer Send Mail Mer All Tasks	>	
Users 🗋	Comparing Controllers Comparing Controllers	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		
	Domain Users Control Users Co	Security Group Security Group Security Group Security Group User User User User Security Group	All domain users Designated administrato Members of this group Members of this group Members in this group c Built-in account for gue		
Renames the current selection.	(h.s				Ŷ

5.図に示すように、[メン**バ**]タブをクリック**し**、[追加]をクリックします。

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

フィールドにユーザを入力し、[Check Names]**ボタンをク**リックして、ユーザが見つかったこと を確認します。確認したら、[**OK**]をクリ**ックします**。

Select Users, Contacts, Computers, Service Accounts, or Groups	×
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 (t.admin@example.com)	Check Names
Advanced OK	Cancel

正しいユーザーが追加されていることを確認し、[**OK**]ボタンをク**リック**します。同じ手順を使用 して、ユーザTest UserをグループAnyConnect Usersに追加します。

AnyConn	ect Admin	s Properties			?	×
General	Members	Member Of	Managed By			
Membe	rs:					
Name <u></u> IT	Admin	Active Dire	ectory Domain : om/Users	Services Folder		
Ad	d	Remove	ОК	Cancel	Ар	ply

LDAPS SSL証明書ルートのコピー(LDAPSまたはSTARTTLSでのみ必要)

1. Win+Rを押し、mmc.exeと入力します。[OK] をクリックします。

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

2. [ファイ**ル] > [スナップインの追加と削除…]に移動します。**図に示すように

ᡖ Console1 - [Console I	Root]		-	o x
File Action	View	Favorites	Window	Help	_ 8 ×
Mew New			Ctrl+N		
Open			Ctrl+O	Actions	
Save			Ctrl+S	There are no items to show in this view.	
Save As				More Actions	•
Add/Re	move Sna	ip-in	Ctrl+M		
Options					
1 dnsm	gmt				
2 dsa					
Exit					

3.使用可能なスナップインの下で、[証明書]をクリックし、[追加]をクリ**ックします**。

Add or Remove Snap-ins			:	×
You can select snap-ins for extensible snap-ins, you can	this console from the configure which e	nose exter	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 <u>U</u> p	
Authorization Manager	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	Ļ	Advanced	
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.図に示すように、[コ**ンピュータ**アカウント]を選択し、[次へ]をクリックします。

Certificates snap-in	×
This snap-in will always manage certificates for: <u>Service account</u> <u>Computer account</u>	
< <u>B</u> ack <u>N</u> ext >	Cancel

[Finish] をクリックします。

Select Computer	×
Select the computer you want this snap-in to manage. This snap-in will always manage:	
< Back Finish Cancel	

5. 「OK」をクリックします。

Add or Remove Snap-ins				:	×	
You can select snap-ins for this console from those available on your computer and configure the selected set of snap-ins. For extensible snap-ins, you can configure which extensions are enabled.						
Available snap-ins: Selected snap-ins:						
Snap-in	Vendor	^		Console Root Edit Extensions		
Active Directory Do	Microsoft Cor Microsoft Cor			Certificates (Local Computer)		
Active Directory Use	Microsoft Cor Microsoft Cor			Move <u>U</u> 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					
E Device Manager	Microsoft Cor					
T Disk Management	Microsoft and	~		Advanced		
Description:			1		_	
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. [Personal]フォルダを展開**し**、[**Certificates**]をクリッ**クします**。LDAPSで使用される証明書は、 Windowsサーバの完全修飾ドメイン名(FQDN)に発行する必要があります。このサーバには3つの 証明書がリストされています。

- example-WIN2016-CAとの間で発行されるCA証明書。
- example-WIN2016-CAによってWIN2016に発行されたID証明書。
- example-WIN2016-CAによってwin2016.example.comに発行されたID証明書。

この設定ガイドでは、FQDNはwin2016.example.comであるため、最初の2つの証明書はLDAPS SSL証明書として使用するには有効ではありません。win2016.example.comに発行されるID証明 書は、Windows Server CAサービスによって自動的に発行された証明書です。証明書をダブルク リックして詳細を確認します。

Gonsole1 - [Console Root\Cert	ificates (Local Computer)\Personal\	Certificates]			- 0 ×
Eile Action View Eavorite	es Window Help				- 7 ×
	2 👼				
Console Root	Issued To	Issued By	Expiration Da	Actions	
✓ ☐ Certificates (Local Compute	r) 🛱 example-WIN2016-CA	example-WIN2016-CA	4/19/2060	Certificates	
Certificates	25 WIN2016	example-WIN2016-CA	4/27/2025	More Actions	+
> Trusted Root Certification	m win2016.example.com	example-WIN2016-CA	4/28/2021		
> 🔛 Enterprise Trust					
> intermediate Certification	m.				
> iii Trusted Publishers					
> Intrusted Certificates					
> iii Third-Party Root Certific	at				
> iii Trusted People					
> Client Authentication Is	sue				
> Preview Build Roots					
> iii Local NonRemovable Collection	ert				
> C Remote Desktop					
> Certificate Enrollment R	eq				
> iii Smart Card Trusted Root	ts				
> iii Trusted Devices					
> iii Web Hosting					
> 🔛 Windows Live ID Token	s				
<	> <		>	1	
Personal store contains 3 certificates	i.				

7. LDAPS SSL証明書として使用するには、証明書が次の要件を満たしている必要があります。

• 共通名またはDNSサブジェクト代替名は、Windows ServerのFQDNと一致します。

• 証明書の[Enhanced Key Usage]フィールドに[Server Authentication]が表示されます。 証明書の[Details]タブの[Subject] と[Subject Alternative Name] に、FQDN win2016.example.comが表示されます。

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

🙀 Certi	ficate			×
General	Details	Certification Path		
Show:	<ai></ai>		~	
Field	bject Key thority Ke L Distribu thority In	Identifier ty 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 Other Name:D5 Object Guid=	^
Ke Th Th	y Usage umbprint umborint	algorithm	Digital Signature, Key Encipher sha1 ca Re 11 3d eb bc 0f 6e 4a 00	*
Other M DS (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	< .

[Enhanced Key Usage] の下に[**Server Authentication]が表示**されています。

🙀 Certi	ficate			×
General	Details	Certification Path		
Show:	<aI></a		~	
Field			Value	^
E Sul	bject blic key		win2016.example.com RSA (2048 Bits)	
- D	blic key pa	arameters	05 00	
Ce	rtificate T	emplate Name	DomainController	
ST EN	hanced Ko IIME Capa	ey Usage bilities	Clent Authentication (1.3.6.1 [1]SMIME Capability: Object I	
a Sul	bject Key	Identifier	30 b7 2b 4e 48 0f 2f 17 17 e6	
Jeel Au	thority Ke	v Identifier	KevID=3d 9f 26 37 fb 11 1f 4	•
Client / Server	Authentic	tion (1.3.6.1.5.5.) ation (1.3.6.1.5.5	7.3.2) 7.3.1)	
		Ed	It Properties Copy to File	
			0	ĸ

8.確認したら、[Certification Path]タブに**移動し**ます。ルートCA証明書にする証明書の一番上をク リックし、[**View Certificate**]ボタンをクリ**ックし**ます。

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

9.これにより、ルートCA証明書の証明書の詳細が開きます。

	~
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	

10. [詳細]タブを**開き**、[ファイ**ルにコピー…]をクリックします。** 図に示すように

Certificate		×
General Details Certification Path	1	
Show: <all></all>	~	
Field	Value	^
Version Serial number Signature algorithm Signature hash algorithm Signature hash algorithm Valid from Valid from 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	

11.ルートCAをPEM形式でエクスポートする証明書エクスポートウィザードをナビゲートします 。

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

 \sim

12. Base-64 encoded X.509を選択します。

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

13.ファイルの名前とエクスポート先を選択します。

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

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

14. 「完了」をクリ**ックします**。

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

15.ここで、場所に移動し、メモ帳などのテキストエディタで証明書を開きます。PEM形式の証明 書が表示されます。後で保存します。

----BEGIN CERTIFICATE----

```
MIIDCDCCAfCgAwIBAgIQE4ZG5Z1wT6lONTjooEQyMTANBgkqhkiG9w0BAQsFADAd
MRswGQYDVQQDExJleGFtcGxlLVdJTjIwMTYtQ0EwIBcNMjAwNDI3MTQ1MDU5WhgP
MjA2MDA0MTkxNDUwNTlaMB0xGzAZBgNVBAMTEmV4YW1wbGUtV010MjAxNi1DQTCC
ASIwDQYJKoZIhvcNAQEBBQADqqEPADCCAQoCqqEBAI8qhT719NzSQpoQPh0YT67b
Ya+PngsxMyvkewP33QLTAWw1HW1Tb9Mk5BDW0ItTaVsgHwPBfd++M+bLn3AiZnHV
00+k6dVVY/E5qVkEKSGoY+v940S2316lzdwReMOFhgbc2qMertIoficrRhihonuU
Cjyeub3CO+meJUuKom2R47C0D35TUvo/FEHGgXJFaJS1se2UrpN07KEMkfA1LPuM
aob4XE/OzxYQpPa18djsNnskfcFqD/HOTFQN4+SrOhHWlRnUIQBUaLdQaabhipD/
sVs5PneYJX8YKma821uYI6j90YuytmsHBtCieyC062a8BKqOL7N86HFPFkMA3u8C
\texttt{AwEAAaNCMEAwDgYDVR0PAQH/BAQDAgGGMA8GA1UdEwEB/wQFMAMBAf8wHQYDVR0O}
BBYEFD2fJjf7ER9EM/HCxCVFN5QzqEdvMA0GCSqGSIb3DQEBCwUAA4IBAQB31ZJo
vzwVD3c5Q1nrNP+6Mq62OFpYH91k4Ch9S5g/CEOemhcwg8MDIoxW2dTsjenAEt7r
phFIHZoCoSyjBjMgK3xybmoSeg8vBjCXseYNGEmOc9KW1oFmTOvdNVIb7Xpl1IVa
6tALTt3ANRNgREtxPA6yQbthKGavW0Anfsojk9IcDr2vp0MTj1BCxsTscbubR1+D
dLEFKQqmMeYvkVf+a7a64mqPZsG3Uxo0rd6cZxAPkq/y1cdwNSJFfQV3DqZq+R96
9WLCR3Obig6xyo9Zu+lixcWpdrbADO6zMhbEYEhkhOOjBrUEBBI6Cy83iTZ9ejsk
KgwBJXEu33Pp1W6E
```

----END CERTIFICATE-----

FDMの構成

ライセンスの確認

FDMでAnyConnectを設定するには、FTDをスマートライセンスサーバに登録し、有効なPlus、 Apex、またはVPN Onlyライセンスをデバイスに適用する必要があります。



1.図に示すように、[Device] > [Smart License]に移動します。

2. FTDがスマートライセンスサーバに登録され、AnyConnect Plux、Apex、またはVPN Onlyライ センスが有効になっていることを確認します。



AD IDソースの設定

1. [Objects] > [Identity Sources]に移動し、+記号をクリックし、図に示すように[AD]を選択します

cisco. Firepower De	avice Manager Monitoring	Policies Objects Device: FTD-3	> 😩 🕲 ? 🗄	admin Administrator
Object Types 🗧 🗧	 Identity Sources 			
C Networks	1 object		Q Search	+ ~
9 Ports	* NAME	THE	VALUE	RADIUS Server
🔒 Security Zones	1 LocalIdentitySource	LOCAL		RADIUS Server Group
Application Filters				AD
🖉 URLs				Identity Services Engine
Geolocations				
Syslog Servers				
8 IKE Policies				
🄄 IPSec Proposals				
AnyConnect Client				
Identity Sources				
1 Users				
R Certificates				
🔒 Secret Keys				
DNS Groups				
Yevent List Filters				

2. Active Directoryサーバの適切な設定に、以前に収集した情報を入力します。IPアドレスの代わ りにMicrosoftサーバにホスト名(FQDN)を使用する場合は、[Objects] > [DNS Group]で適切な DNSグループを必ず作成してください。次に、[Device] > [System Settings] > [DNS Server]に移 動し、[Management Interface]および[Data Interface]でDNSグループを適用し、DNSクエリに適 切な出力インターフェイスを指定して、そのDNSグループをFTDにに適用します。Testボタンを クリックして、FTDの管理インターフェイスから正常な設定と到達可能性を確認します。これら のテストはFTDの管理インターフェイスから開始され、FTDに設定されているルーティング可能 インターフェイス(内部、外部、dmzなど)からは開始されないため、正常な(または失敗した)接続ではAnyConnect認証の結果は保証されません。FTDからのLDAP接続のテストの詳細につ いては、「トラブルシューティング」領域の「AAAのテスト」および「パケットキャプチャ」の 項を参照してください。 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	Port 389
Hostname / IP Address win2016.example.com e.g. ad.example.com	Port 389
Hostname / IP Address win2016.example.com e.g. ad.example.com Encryption	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 success	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 success 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 success Add another configuration	Port 389 Trusted CA certificate Please select a certificate ful CANCEL OK

LDAPSまたはSTARTTLSを使用する場合は、適切な暗号化を選択し、信頼できるCA証明書を選択します。ルートCAがまだ追加されていない場合は、[Create New Trusted CA Certificate]をクリックします。ルートCA証明書の[Name]を指定し、先ほど収集したPEM形式のルートCA証明書を貼り付けます。

Add Trusted CA Certificate

Name LDAPS_ROOT	
Paste certificate, or choose file: UPLOAD CERTIFICATE The supported formats are: PEM, DER.	
BEGIN CERTIFICATE MIIDCDCCAfCgAwIBAgIQE4ZG5Z1wT6IONTjooEQyMTANBgkqhkiG9w0BAQsFADAd MRswGQYDVQQDExJleGFtcGxlLVdJTjIwMTYtQ0EwIBcNMjAwNDI3MTQ1MDU5WhgP MjA2MDA0MTkxNDUwNTIaMB0xGzAZBgNVBAMTEmV4YW1wbGUtV0IOMjAxNi1DQTCC ASIwDOX IKoZlbycNAOEBB0ADggEPADCCAOgCggEBAI8ghT719NzSOpgOPb0YT67b	< >
CANCEL	
Directory Server Configuration	

8 X

win2016.example.com:636		^
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	ccessful	

この設定では、次の値が使用されています。

- [Name]: ラボ広告
- [Directory Username] : ftd.admin@example.com
- [Base DN] : dc=example,dc=com
- [AD Primary Domain] : example.com
- [Hostname/IP Address] : win2016.example.com
- [Port] : 389
- 3.図に示すように、右上の[Pending Changes]ボタンをクリックします。

cisco. Firepower Devi	ice Manager Monitoring Policies	Objects Device: FTD-3	S 🖨 🔊 ()	* admin * Administrator
Object Types 🔶 ^	Identity Sources			
C Networks	2 objects		Q Search	+ ~
S Ports	M NAME	TYPE	VALUE	ACTIONS
Security Zones	1 LocalidentitySource	LOCAL		
💞 Application Filters	2 LAB-AD	AD	win2016.example.com	

4. [今すぐ展開]ボタン**をクリック**します。

Pe	ending Changes	0 ×	Ç
0	Last Deployment Completed Successfully 01 May 2020 12:54 PM. See Deployment History		
	Deployed Version (01 May 2020 12:54 PM)	Pending Version CEGEND Removed Added Edit	ed.
0	Active Directory Realm Added: LAB-AD		^
	- - - - - - -	<pre>dirPassword.masked: false dirPassword.encryptedString: *** directoryConfigurations[0].port: 389 directoryConfigurations[0].hostname: win2016.example.com directoryConfigurations[0].encryptionProtocol: NONE adPrimaryDomain: example.com dirUsername: ftd.admin@example.com baseDN: DC=example,DC=com enabled: true realmId: 9 name: LAB-AD</pre>	
M	ORE ACTIONS Y	CANCEL DEPLOY NOW	

AD認証用のAnyConnectの設定

設定されたAD IDソースを使用するには、AnyConnect設定に適用する必要があります。

1.図に示すように、[Device] > [Remote Access VPN]に移動します。

cisco. Firepower Device Man	ager	Monitoring Policies	讀 Objects	Device: FTD-3	6	admin	Ý
			0/0	J			
Interfaces Connected Enabled 3 of 4 View All Interfaces	>	Routing 2 routes View Configuration	>	Updates Geolocation, Rule, VDB, System Up Security Intelligence Feeds View Configuration	ograde,	System Settings Management Access Logging Settings DHCP Server DNS Server	
Smart License Registered View Configuration	>	Backup and Restore	>	Troubleshoot No files created yet REQUEST FILE TO BE CREATED		Management Interface Hostname NTP Cloud Services Reboot/Shutdown Traffic Settings URL Filtering Preferences	
Site-to-Site VPN There are no connections yet View Configuration	>	Remote Access VPN Configured 1 connection 2 Group Polici View Configuration	es >	Advanced Configuration Includes: FlexConfig, Smart CLI View Configuration	>	Device Administration Audit Events, Deployment History, Download Configuration View Configuration	>

2.図に示すように、+**記号または[接続プロフ**ァイルの作成]ボタンをクリックします。



3. [Connection and Client Configuration]セクションで、以前に作成したAD IDソースを選択します 。[接続プロファイル名(Connection Profile Name)]や[クライアントアドレスプールの割り当て (Client Address Pool Assignment)]など、他のセクションに適切な値を設定します。完了したら **[Submit Query]を**クリックします。

Connection and Client Configuration

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

des Des Clis Marson

Connection Profile Name This name is configured as a connection alias, it co	can be used to connect to the VPN gateway
General	
Group Alias	Group URL
Add Group Alias	Add Group URL
Primary Identity Source Authentication Type	
AAA Only Client Certificate Only	AAA and Client Certificate
Filter	Please Select Local Identity Source Please Select Local Identity Source
1t LocalidentitySource	^
LAB-AD Special-Identities-Realm	<u> </u>
Create new 🜱	

Client Address Pool Assignment

IPv4 Address Pool Endpoints are provided an address from this pool	IPv6 Address Pool Endpoints are provided an address from this pool +
AnyConnect-Pool	
HCP Servers	
CANCEL	SUBMIT QUERY

4. [Remote User Experience]セクションで、適切なグループポリシーを選択します。デフォルト では、DfltGrpPolicy**が使用**されます。ただし、別のものを作成できます。

```
View Group Policy
```

DfltGrpPolicy

Policy Group Brief Details

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

5. [Global Settings]セクションで、少なくとも[SSL Certificate]、[Outside Interface]、および [AnyConnect]パッケージを指定します。証明書が以前に作成されていない場合は、デフォルトの 自己署名証明書(DefaultInternalCertificate)を選択できますが、信頼できないサーバ証明書メッセ ージが表示されます。ユーザIDアクセスポリシーのルールが後で有効になるように、復号化され たトラフィック(sysopt permit-vpn)のBypass Access Control policyをオフにする必要があります 。NAT免除は、ここでも設定できます。この設定では、AnyConnectクライアントのIPアドレスに 向かう内部インターフェイスからのipv4トラフィックはすべて、NAT以外のものです。外部から 外部へのヘアピニングなどのより複雑な設定では、NATポリシーの下に追加のNATルールを作成 する必要があります。AnyConnectパッケージは、シスコのサポートサイトにあります。 https://software.cisco.com/download/homeAnyConnectパッケージをダウンロードするには、有効 なPlusライセンスまたはApexライセンスが必要です。

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 Inter	face
ftd3.example.com	
e.g. ravpn.example.com	
Access Control for VPN Traffic Decrypted VPN traffic is subjected to access control polic policy for decrypted traffic option bypasses the access co and the authorization ACL downloaded from the AAA serv Bypass Access Control policy for decrypted to	y inspection by default. Enabling the Bypass Access Control entrol policy, but for remote access VPN, the VPN Filter ACL ver are still applied to VPN traffic traffic (sysopt permit-vpn)
NAT Exempt	
Inside Interfaces The interfaces through which remote access VPN users can connect to the Internal networks	Inside Networks The internal networks remote access VPN users are allowed to use. The IP versions of the internal networks and address pools must match, either IPv4, IPv6, or both.
	C any-ipv4
AnyConnect Package	
If a user does not already have the right AnyConnect packs installer when the client authenticates for the first time. The	age installed, the system will launch the AnyConnect a user can then install the package from the system.
You can download AnyConnect packages from software.cl You must have the necessary AnyConnect software license	sco.com. a.



6. [Summary]セクションで、AnyConnectが適切に設定されていることを確認し、[**Submit Query**]をクリ**ックします**。

Summary

Review the summary of the Remote Access VPN configuration.

General		
STEP 1: CONNECTION AND CLIENT CONFIGURATION	N	
Primary Identity Source		
Authentication Type	AAA Only	
Primary Identity Source	It LAB-AD	
Frithary Identity Gource	22 010-10	
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	-	
Fallback Local Identity Source	-	
Advanced		
V Advanced		
Authorization Server		
Accounting Server		
Client Address Pool Assignment		

7.図に示すように、右上の[Pending Changes]ボタンをクリックします。

cisco. Firepower Der	vice Manager 👼 🐨 🚟	ts Device: FTD-3	o. 🖨 🗐 ? :	admin Administrator
RA VPN ←	Device Summary Remote Access VPN Connection Pr	ofiles		
Connection Profiles	1 object	c) Search	+
	· NAME	***	GROUP POLICY	ACTIONS
	1 General	Authentication: AAA Only Authorization: None Accounting: None	DfttGrpPolicy	

8. [今すぐ展開]をクリックします。

Pe	ending Changes	0	× Cler
0	Last Deployment Completed Successfully 16 Apr 2020 12:41 PM. <u>See Deployment History</u>		cius
	Deployed Version (16 Apr 2020 12:41 PM)	Pending Version C LEGEND Removed Added Ed	ited
0	Network Object Added: AnyConnect-Pool		^
	- - - -	<pre>subType: Network value: 10.10.10.0/24 isSystemDefined: false dnsResolution: IPV4_AND_IPV6 name: AnyConnect-Pool</pre>	
0	RA VPN Added: NGFW-Remote-Access-VPN		
	-	<pre>vpnGatewaySettings[0].exemptNatRule: true vpnGatewaySettings[0].outsideFqdn: ftd3.example.com vpnGatewaySettings[0].bypassAccessControlForVPNTraffic: t_ name: NGFW-Remote-Access-VPN</pre>	ľ
	anyconnectPackageFiles:		
	-	anyconnect-win-4.7.03052-webdeploy-k9.pkg	
	<pre>vpmGatewaySettings[0].serverCertificate: -</pre>	FTD-3-Manual	
	<pre>vpnGatewaySettings[0].outsideInterface:</pre>	TTO STRINGS	
	-	outside	
	<pre>vpnGatewaySettings[0].insideInterfaces:</pre>		
	-	inside	
	<pre>vpnGatewaySettings[0].insideNetworks:</pre>		
M	DRE ACTIONS Y	CANCEL DEPLOY NOW	2

アイデンティティポリシーの有効化とユーザIDのセキュリティポリシーの設定

この時点で、AnyConnectユーザは正常に接続できますが、特定のリソースにアクセスできない可 能性があります。この手順では、ユーザIDを有効にして、AnyConnect Admins内のユーザだけが RDPを使用して内部リソースに接続でき、AnyConnect Usersグループ内のユーザだけがHTTPを 使用して内部リソースに接続できるようにします。

1. [Policies] > [Identity]に移動し、[Enable Identity Policy]をクリックします。



この設定では、これ以上の設定は必要なく、デフォルトアクションで十分です。

cisco. Firepo	wer Device Manag	er Mon	itoring Policies	読記 Objects	Device: FTD-3	(2 🚑 🛛	? : a	ámin dministrator	~
🛷 Security P	olicies									
₽ → Os	SL Decryption \rightarrow	ldentity \Rightarrow	O Security Intelliger	ice 🔿 🕝 NA	AT $ ightarrow$ 📀 Acces	ss Control 🚽 🦉 🛙	trusion			
Identity Policy	D					Q Search			¢ <u>a</u>	+
			SOURCE	1		DESTINATION				
H NAME	AUTHENTICATION	AUTH, TYPE	ZONES	NETWORKS	PORTS	ZONES	NETWORKS	PORTS/PROTO	ACTIONS	
				There are no k	dentity rules yet.					
				Start by creating t	he first identity rule.					
				CREATE ID	ENTITY RULE					
Default Action	An Passive Auth	y Identity Source	~ 0							

2. [Policies] > [NAT] に移動し、NATが適切に設定されていることを確認します。AnyConnect設定 で設定されたNAT例外で十分な場合、ここでは追加の設定は必要ありません。

cisco. Firepowe	er Device I	Manager	Biji Monitoring	Ø Policies	iii Objects	Device: FTD-3		0	2 💿 ?	admin Admini	strator
🕫 Security Po	licies										
⊡ → O sst	Decryption	-> 🕑 ki	entity \rightarrow () is	Security Intelligenc	e 🔶 🥑 NA	T 🔿 📀 Acce	ess Control \Rightarrow	S Intrusion			
1 rule								Q Search			+
			OFFICINAL PACKET				TRANSLATED PACKE	π			
a NAME	TYPE	INTERFACES	SOURCE AD	DESTINATIO	SOUNCE PORT	DESTINATIO	SOUNCE AD	DESTINATIO	SOURCE PORT	DESTINATIO	ACTIONS
Auto NAT Rules											

3.[Policies] > [Access Control] に移動します。このセクションでは、[Default Action]が[Block]に設 定されており、アクセスルールは作成されていないため、AnyConnectユーザが接続すると、何に もアクセスできなくなります。+記号または[**アク**セス規則の作成]をクリックして、新しい規則を 追加します。

cisco. Firepov	ver Device Manager	题 Monitoring	Ø Policies	前面 Objects	Device: FTD-3		۵. 🚑		adm Adm	in v inistrator
🛷 Security P	olicies									
₽ → 0 %	SL Decryption \rightarrow 🥑 🛛	dentity \rightarrow () S	ecurity Intelligence	> - 🕗 nat	f $ ightarrow$ Access	Control - 🧐	Intrusion			
						Q Search				©. +
	SOURCE			DESTINATION						
* 8444	ACTION ZONES	METWORKS	PORTS	ZONES	NETWORKS	PORTS/PROTO	APPLICATIONS	URLS	USERS	ACTIONS
				There are no ao	cess rules yet.					
			St	art by creating the	e first access rule.					
				CREATE ACC	CESS RULE					
Default Action	Access Control 🤤 Block 🗌	€ E ×								

4.フィールドに適切な値を入力します。この設定では、AnyConnect Adminsグループ内のユーザ は、内部ネットワーク内のWindows ServerにRDPアクセスできる必要があります。送信元の場合 、ゾーンはoutside_zoneとして設定されます。これはAnyConnectユーザが接続する外部インター フェイスであり、ネットワークはAnyConnectクライアントにIPアドレスを割り当てるために以前 に設定されたAnyConnect-Poolオブジェクトです。FDMのユーザーIDの場合、ソースはユーザー が接続を開始するゾーンとネットワークである必要があります。宛先に対して、ゾーンは Windows Serverの内部インターフェイスであるinside_zone、ネットワークはWindows Serverの サブネットを定義するオブジェクトであるInside_Netオブジェクト、ポート/プロトコルは2つのカ スタムポートオブジェクトに設定され、TCP 3389とUDP 3389で9への8への8RDP8アクセス8を 8を8を8可能8可能8に89

Edit Access	Rul	e									×
Order Title 1 AC R Source/Destination	DP Ad	pplications URLs (Jsers	Action Allow Intrusion Policy	File policy ⁰ Lo	gging					
SOURCE					DESTINATION						
Zones	+	Networks	÷	Ports +	Zones	+	Networks	+	Ports/Protocols		+
G outside_zone		C AnyConnect-Pool		ANY	G inside_zone		Inside_Net		$\underset{RDP-TCP}{\leftrightarrows}$		
									\Leftrightarrow RDP-UDP		
Show Diagram	\supset	O Not hit yet						CA	INCEL	ок	

[Users]セクションで、グループAnyConnect Adminsが追加され、このグループ以外のユーザは Windows ServerへのRDPアクセスが許可されます。+記号をク**リック**し、[グループ]タブをクリッ クし、該当するグループをクリックして、[**OK**]をクリ**ックします**。個々のユーザとアイデンティ ティソースも選択できます。

Add Access Rule	0 ×
Order Title 1 AC RDP Access Source/Destination Applications URLs Users	Action Allow Intrusion Policy File policy
AVAILABLE USERS Y Filter Identity Sources Groups LAB-AD \ Account Operators LAB-AD \ Administrators LAB-AD \ Allowed RODC Password Replication Group LAB-AD \ Allowed RODC Password Replication Group LAB-AD \ AnyConnect Admins LAB-AD \ AnyConnect Users Create new Identity Realm CANCEL	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 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

適切なオプションを選択したら、[**OK**]をクリッ**クします**。

Add Access Rule		o ×
Order Title	Action	
1 V AC RDP Access	🔁 Allow 🛛 🗡	
Source/Destination Applications URLs Users	Intrusion Policy	File policy Logging
AVAILABLE USERS	+	1 CONTROLLING ACCESS FOR USERS AND USER GROUPS
1 LAB-AD \ AnyConnect Admins		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

5.必要に応じて、さらにアクセスルールを作成します。この設定では、AnyConnect Usersグルー

プ内のユーザがWindows ServerにHTTPアクセスできるように、別のアクセスルールが作成され ます。

Edit Access Rule			0 ×
Order Title	Action		
2 Y AC HTTP Access	🔁 Allow \vee		
Source/Destination Applications URLs Users Intrus	sion Policy ⁰ File policy ⁰ Log	ging	
SOURCE	DESTINATION		
Zones + Networks + Ports	+ Zones	+ Networks	+ Ports/Protocols +
avyConnect-Pool ANY	inside_zone	Inside_Net	5 нттр
Show Diagram			CANCEL OK
Ordar Titla	Artino		
2 V AC HTTP Access	Allow Y		
Source/Destination Applications URLs Users Intrus	sion Policy ⁰ File policy ⁹ Loga	aina	
AVAILABLE USERS	+ tt. CONTROLLING	ACCESS FOR USERS AND USER GR	OUPS
LAB-AD \ AnyConnect Users	If you configure id address, you can membership. By c appropriate access different address t network access ch from one group to	entity policies to establish user control access based on user controlling access based on use is controls whether the user cha through DHCP. If you base rule hanges as users change roles in another.	identity based on source IP ame or user group r identity, you can apply the anges workstations or obtains a s on group membership, user n your organization, moving
Show Diagram			CANCEL OK

6.アクセスルールの設定を確認し、図に示すように、右上の[Pending Changes]ボタンをクリック

Not hit yet



cisco. Firepowe	er Devic	e Manager	Monitoring	Ø Policies	i‡E Objects 0	Device: FTD-3		0	0	D: ;	edmin Administra	tor
2 rules	orea yaraa			contra mengenne			Q Search				0	+
		SOURCE			DESTINATION	Language						
> 1 AC RDP Access	Allow	outside_zone	AnyConnect-Pool	ANY	inside_zone	Inside_Net	RDP-TCP RDP-UDP	ANY	ANY	AnyConne	Ф.С.	Actions
> 2 AC HTTP Access	Allow	outside_zone	AnyConnect-Pool	ANY	inside_zone	Inside_Net	HTTP	ANY	ANY	AnyConne	Ф.С.	
Default Action Access Control 🖨 Block 🗠 🕞 🛩												

7.変更を確認し、[今すぐ展開]をク**リックします**。

P	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 CLEGEND Removed	Added	Edited
0	Access Rule Added: AC HTTP Access			^
	- - - -	users[0].name: AnyConnect Users logFiles: false eventLogAction: LOG_NONE ruleId: 268435467 name: AC HTTP Access		
	sourceZones:			
	-	outside_zone		
	-	inside zone		
	sourceNetworks:			
	-	AnyConnect-Pool		
	destinationNetworks:			
	-	Inside_Net		
	destinationPorts:			
	-	HTTP		
	users[0].identitySource:			
	-	LAB-AD		
0	Access Rule Added: AC RDP Access			~
				_
N	IORE ACTIONS Y	CANCEL DEPLOY N	ow	~

確認

ここでは、設定が正常に機能しているかどうかを確認します。

Final Configuration

```
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
```

aaa-server LAB-AD protocol ldap realm-id 7 aaa-server LAB-AD host win2016.example.com serverport 389 ldap-base-dn DC=example,DC=com ldap-scope subtree ldap-login-password ***** ldap-login-

> show running-config ssl
ssl trust-point FTD-3-Manual outside

AnyConnectによる接続とアクセスコントロールポリシールールの確認

webvpn

AnyConnectの設定

> show running-config webvpn

show running-configuration aaa-server

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

🚳 Cisco AnyCo	onnect Secure M	lobility Cli	ent -	- [×	-	
	VPN: Contacting ftd3. ftd3.example.c	example.co	om.	Conr	nect		
	_	🕙 Cisco	o AnyConne	ct ftd3.	example.com		×
¢ ()			Group: Username: Password:	General it.admin	**		
					ОК	Cancel	
🔇 Cisco AnyCo	onnect Secure M	lobility Cli	ent -	- [×		
	VPN: Connected to fto ftd3.example.c	13.example	.com.	Discor	nnect		
00:00:14					IPv4		
¢ ()							

ユーザIT Adminは、Windows ServerにRDPアクセスできるグループAnyConnect Adminsに属して いますが、HTTPにアクセスできません。このサーバーに対してRDPおよびFirefoxセッションを 開くと、このユーザーはRDP経由でのみサーバーにアクセスできます。



HTTPアクセスを持ち、RDPアクセスを持たないグループAnyConnect Usersに属するテストユー ザでログインした場合、アクセスコントロールポリシールールが有効であることを確認できます 。



トラブルシュート

ここでは、設定が正常に機能しているかどうかを確認します。

デバッグ

このデバッグは、LDAP認証に関連する問題をトラブルシューティングするために、診断CLIで実 行できます。debug Idap 255を使用します。

ユーザIDのアクセスコントロールポリシーの問題をトラブルシューティングするために、system support firewall-engine-debugをclishで実行し、トラフィックが予期せず許可またはブロックされ る理由を判別できます。

LDAPデバッグの動作

```
[53] Session Start
[53] New request Session, context 0x00002b1d13f4bbf0, reqType = Authentication
[53] Fiber started
[53] Creating LDAP context with uri=ldap://192.168.1.1:389
[53] Connect to LDAP server: ldap://192.168.1.1:389, status = Successful
[53] supportedLDAPVersion: value = 3
[53] supportedLDAPVersion: value = 2
[53] LDAP server 192.168.1.1 is Active directory
[53] Binding as ftd.admin@example.com
[53] Performing Simple authentication for ftd.admin@example.com to 192.168.1.1
[53] LDAP Search:
Base DN = [DC=example,DC=com]
Filter = [sAMAccountName=it.admin]
```

```
Scope
              = [SUBTREE]
[53] User DN = [CN=IT Admin, CN=Users, DC=example, DC=com]
[53] Talking to Active Directory server 192.168.1.1
[53] Reading password policy for it.admin, dn:CN=IT Admin, CN=Users, DC=example, DC=com
[53] Read bad password count 6
[53] Binding as it.admin
[53] Performing Simple authentication for it.admin to 192.168.1.1
[53] Processing LDAP response for user it.admin
[53] Message (it.admin):
[53] Authentication successful for it.admin to 192.168.1.1
[53] Retrieved User Attributes:
       objectClass: value = top
[53]
[53]
       objectClass: value = person
[53]
       objectClass: value = organizationalPerson
[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]
[53]
       displayName: value = IT Admin
      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
      codePage: value = 0
[53]
[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 = 1601010100000.0Z
[53]
       lastLogonTimestamp: value = 132319755825875876
[53] Fiber exit Tx=515 bytes Rx=2659 bytes, status=1
[53] Session End
```

LDAPサーバとの接続を確立できない

```
[-2147483611] Session Start
[-2147483611] New request Session, context 0x00007f9e65ccdc40, reqType = Authentication
[-2147483611] Fiber started
[-2147483611] Creating LDAP context with uri=ldap://171.16.1.1:389
[-2147483611] Connect to LDAP server: ldap://172.16.1.1:389, status = Failed
[-2147483611] Unable to read rootDSE. Can't contact LDAP server.
[-2147483611] Fiber exit Tx=0 bytes Rx=0 bytes, status=-2
[-2147483611] Session End
```

潜在的なソリューション:

- ルーティングを確認し、FTDがLDAPサーバから応答を受信することを確認します。
- LDAPSまたはSTARTTLSを使用する場合は、SSLハンドシェイクが正常に完了できるように、正しいルートCA証明書が信頼されていることを確認します。
- ・正しいIPアドレスとポートが使用されていることを確認します。ホスト名を使用する場合は、DNSが正しいIPアドレスに解決できることを確認します

Binding Login DN and/or Password Incorrect

```
[-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
```

考えられる解決策:ログインDNとログインパスワードが適切に設定されていることを確認します。これは、ADサーバでldp.exeを使用して確認**できます**。アカウントがldpを使用して正常にバインドできることを確認するには、次の手順を実行します。

1. ADサーバーでWin+Rを押し、ldp.exeを検索します。

💷 Run	×
0	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. [接続] > [接続]をクリックします。 図に示すように

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

3.サーバーにlocalhostと適切なポートを指定し、「OK」をクリックします。

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

4. [Right]列には、接続が成功したことを示すテキストが表示されます。「接**続」>「バインド」を** クリックします。 図に示すように



5.「簡易バインド」**を選択**し、ディレクトリ・アカウントのユーザー名とパスワードを指定します。[OK] をクリックします。

Bind	×				
<u>U</u> ser:	ftd.admin@example.com				
Password: •••••••					
Bind type Bind as currently logged on user Bind with credentials Simple bind Advanced (DIGEST) Encrypt traffic after bind Advanced OK					

バインドが成功すると、ldpはDOMAIN\usernameとしてAuthenticatedと表示されます。

🔐 Idap://w	in2016.exa	mple.co	om/DC=ex	ample, DC	=com		_		×	(
Connection	Browse	View	Options	Utilities	Help					
				1.2.3 1.2.3 1.2.3 Supporte Max Max Max Max Max Max Max Max	840.113556 840.113556 840.113556 edLDAPPolic PercentDirS ReceiveBut Connection BatchRetur DirSyncDur ResultSetSi ResultSetSi ResultSetSi ValRange; I edLDAPVer edSASLMed IEGO; EXTER	.1.4.2255; .1.4.2256; .1.4.2309; cies (20): Ma SyncReques ffer; InitReco s; MaxConn nMessages ation; MaxT ize; MinReso PerConn; Ma MaxValRang Limit; Syster sion (2): 3; chanisms (4 RNAL; DIGE	axPoolThr sts; MaxDa vTimeout; IdleTime; I ; MaxQue empTable ultSets; axNotificat geTransition MemoryL 2;): GSSAP ST-MD5; min@exar	eads; atagramR MaxPage ryDuratio Size; tionPerCo ve; .imitPerce l; GSS-	ecv; Size; n; onn; ent;	^
			Ā	uthenticate	ed as: 'EXAN	/IPLE\ftd.ad	min'.			
			-							~
Ready										

無効なユーザ名またはパスワードを使用してバインドしようとすると、次のようなエラーが発生 します。

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 unavailable unavailable suthenticate	ResultSetS ResultSets ValRange; eadMemory edLDAPVe edSASLMe IEGO; EXTE imple_bind >; // v.3 ed as: 'EXA	Size; MinResu PerConn; Ma MaxValRang (Limit; Syster rsion (2): 3; 2 chanisms (4 RNAL; DIGE _s(Id, 'ftd.ad MPLE\ftd.adr _s(Id, 'wrong	ultSets; axNotificat geTransition MemoryL 2;): GSSAP ST-MD5; min@exan min". g@examp	tionPerConr ve; .imitPercent I; GSS- mple.com',	;
			< E S C E ir	unavailable rror <49>: I server error comment: Ac rror 0x8009 ivalid	>); // v.3 Idap_simple :: 80090308 cceptSecur 90308 The	e_bind_s() fa 3: LdapErr: D rityContext e token supplie	ailed: Inval SID-0C09 rror, data ed to the f	id Credentia 042A, 52e, v3839 unction is	ils ∀
Ready									

LDAPサーバがユーザ名を見つけることができない

```
[-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
考えられる解決策:ADがFTDによる検索でユーザを検索できることを確認します。これは、
ldp.exeでも実行できます。
```

1.バインドが正常に完了したら、図に示すように[View] > [Tree]に移動します。

🔝 Idap://w	in2016.exa	mple.	.com/DC=	example,DC	=com			_		\times		
Connection	Browse	View	/ Option	s Utilities	Help							
			Tree			Ctrl+T				^		
			Enterprise	e Configurat	ion		/axP	/laxPoolThreads; sts; MaxDatagramRecv; cvTimeout;				
		\checkmark	Status Ba	r			sts; vTin					
			Set Font				nidie s: Ma	eTime; N axQuer	/laxPage ∿Duratio	Size; n:		
	MaxDirSyncDuration; MaxTempTableSize; MaxResultSetSize; MinResultSets; MaxResultSetsPerConn; MaxNotificationPerConn MaxValRange; MaxValRangeTransitive; ThreadMemoryLimit; SystemMemoryLimitPercent supportedLDAPVersion (2): 3; 2; supportedSASLMechanisms (4): GSSAPI; GSS- SPNEGO; EXTERNAL; DIGEST-MD5;							nn; :nt;				
res = ldap_simple_bind_s(ld, 'ftd.admin@example.com', <unavailable>); // v.3 Authenticated as: 'EXAMPLE\ftd.admin'.</unavailable>							,					
				I						~		

2. FTDに設定されているベースDNを指定し、[**OK**]をクリック**します**。

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

3. [Base DN]を右クリックし、図に示すように[Search]をクリックします。

🔝 Idap://wi	n2016.exa	– 🗆 ×	<				
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	ist View DN Id e ed	Ctrl+S Ctrl+D Ctrl+M Ctrl+R Ctrl+A >	cipals,DC=example,DC=com; 11D2B9AA00C04F79F805:CN =example,DC=com; 11D297C400C04FD8D5CD:C =example,DC=com; 11D1ADED00C04FD8D5CD:C =example,DC=com; 11D1ADED00C04FD8D5CD:C ple,DC=com; 11D1AA4B00C04FD7D83A:O 3,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	^
			Clear ou	tput	Ctrl+N		
Create a new d	locument		1				×

4.デバッグに示されているのと同じベースDB、フィルタ、スコープの値を指定します。この例で は、次の項目を示します。

- [Base DN] : dc=example,dc=com
- [Filter] : samaccountname=it.admi
- スコープ:サブツリー

🟠 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は、**samaccountname=it.admi**のユーザアカウントがベースDN dc=example,dc=comに存在しないため、0エントリを見つけます。

正しい**samaccountname=it.admin**を使用して再**試行すると、**結果が異なります。ldpは、ベース DN dc=example,dc=comの下に1つのエントリを見つけ、そのユーザのDNを出力します。

🔝 Idap://w	in2016.example.com/l	DC=example,DC	=com		_		×
Connection	Browse View Op	tions Utilities	Help				
Search			2	× 58 D	811D1ADED000 C=example,DC= 811D1ADED000	C04FD8D50 com; C04FD8D50	
Base <u>D</u> N:	DC=example,DC=com	1	· · · ·	⊿ an	nple,DC=com;		
<u>F</u> ilter:	sAMAccountName=it.a	admin	```		s,DC=example,	DC=com;	3A:0
Scope O <u>B</u> ase	O <u>O</u> ne Level	Subtree		58 =e: 68	811D1ADED000 xample,DC=com 811D1ADED00 ble.DC=com:	C04FD8D50 1; C04FD8D50	D:C CD:C
<u>A</u> ttributes:	objectClass;name;des	cription;canonical	Name 🕓	- 0.	20 3:43:59 PM E	astern Day	/light
Options		<u>R</u> un	<u>C</u> lose)2	0 2:41:57 PM Ea	istern Dayl	ight
		***Searching Idap_search "sAMAccou Getting 1 en Dn: CN=IT / canonic name: fi objectC use	g n_s(ld, "DC intName=it. itries: Admin,CN calName: e: F Admin; lass (4): to er;	C=exar .admin I=Use xample op; per	nple,DC=com", 2 ", attrList, 0, &r rs,DC=exampl e.com/Users/IT son; organizatio	2, msg) l e,DC=con Admin; onalPerson	n ;
Ready							

ユーザ名のパスワードが正しくない

[-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]	<pre>supportedLDAPVersion: value = 3</pre>
[-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 I	<pre>N = [dc=example,dc=com]</pre>
Filter	= [samaccountname=it.admin]
Scope	= [SUBTREE]
[-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

考えられる解決策:ユーザのパスワードが適切に設定され、期限が切れていないことを確認します 。Login DNと同様に、FTDはユーザのクレデンシャルを使用してADに対してバインドを実行しま す。このバインドは、ADが同じユーザ名とパスワードのクレデンシャルを認識できることを確認 するために、ldpでも実行できます。ldpの手順は、「ログインDNのバインド」セクションと「パ スワードが正しくな**い」セクションのいずれかまたは両方で示されています**。さらに、 Microsoftサーバのイベントビューアのログを確認して、潜在的な理由を調べることができます。

AAAのテスト

test aaa-serverコマンドを使用すると、FTDから特定のユーザ名とパスワードを使用した認証の 試みをシミュレートできます。これは、接続または認証の失敗をテストするために使用できます 。コマンドはtest aaa-server authentication [AAA-server] host [AD IP/hostname]です。

```
> 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)
```

パケット キャプチャ

> show route 192.168.1.1

INFO: Authentication Successful

パケットキャプチャは、ADサーバへの到達可能性を確認するために使用できます。LDAPパケットがFTDから送信されても応答がない場合は、ルーティングの問題を示している可能性があります。

双方向LDAPトラフィックを示すキャプチャを次に示します。

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
                           192.168.1.17.61960 > 192.168.1.1.389: S 3681912834:3681912834(0) win
  1: 23:02:16.770712
32768 <mss 1460,nop,nop,timestamp 1061373057 0>
                          192.168.1.1.389 > 192.168.1.17.61960: S 491521506:491521506(0) ack
  2: 23:02:16.772009
3681912835 win 8192 <mss 1460,nop,nop,timestamp 762393884 1061373057>
                           192.168.1.17.61960 > 192.168.1.1.389: . ack 491521507 win 32768
   3: 23:02:16.772039
<nop,nop,timestamp 1061373058 762393884>
   4: 23:02:16.772482
                           192.168.1.17.61960 > 192.168.1.1.389: P 3681912835:3681912980(145)
ack 491521507 win 32768 <nop,nop,timestamp 1061373059 0>
   5: 23:02:16.772924
                          192.168.1.1.389 > 192.168.1.17.61960: P 491521507:491522141(634) ack
3681912980 win 65160 <nop,nop,timestamp 762393885 1061373059>
   6: 23:02:16.772955
                           192.168.1.17.61960 > 192.168.1.1.389: . ack 491522141 win 32768
<nop,nop,timestamp 1061373059 762393885>
   7: 23:02:16.773428
                          192.168.1.17.61960 > 192.168.1.1.389: P 3681912980:3681913024(44)
ack 491522141 win 32768 <nop,nop,timestamp 1061373060 0>
                          192.168.1.1.389 > 192.168.1.17.61960: P 491522141:491522163(22) ack
  8: 23:02:16.775030
3681913024 win 65116 <nop,nop,timestamp 762393887 1061373060>
  9: 23:02:16.775075
                          192.168.1.17.61960 > 192.168.1.1.389: . ack 491522163 win 32768
<nop, nop, timestamp 1061373061 762393887>
[...]
54 packets shown
```

Windows Serverイベントビューアのログ

ADサーバのバンに関するイベントビューアのログには、障害が発生した理由に関する詳細情報が 記載されています。

1.イベントビューアを検索して開きます。

=	Best mat	ch								
ŵ	Event Viewer Desktop app									
	Settings	Settings >								
	🖄 Vie	🔠 View event logs								
۲	10	۲	ß		5	₽	វុក			
	event									
	ו כ	:[])	e	-	1	2	8			

2. [**Windows** Logs]を展開**し**、[**Security]**をクリッ**クします**。図に示すように、ユ**ーザーのアカ**ウン ト名で[Audit Failure]を検索し、[Failure Information]を確認します。



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