AnyConnectクライアント用のAD認証の設定

Image: Image	内容	
	<u>はじめに</u>	
BE! UIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIII	前提条件	
# # # 3 = 1 = 1 = 1 = 1 = 1 = 1 = 1 = 1 = 1 =	<u>要件</u>	
J Z Z U Z \downarrow \lor \neg	<u>使用するコンポーネント</u>	
BUE: $\Rightarrow \lor \vdash \bigtriangledown - 2STTTS A E SULLATSA = V \vdash \Box - 2STTTS A E SULLATSB = D \vdash \Box - D \cup D$	<u>背景説明</u>	
$\frac{1}{\sqrt{1}} \frac{1}{\sqrt{1}} \frac{1}{\sqrt{1}$	<u>設定</u>	
Active Directorvの設定 LDAPベースDNとグループDND次定 FTDアカウントの作成 ADグループの作成とADグループへのユーザの追加(オブション) LDAPS SSL証明書ルートのコビー(LDAPSまたはSTARTTLSの場合のみ必要) FMCの設定 ダイセンスの確認 レルムの設定 アイデンティナイボリシーの有効化とユーザIDのセキュリティボリシーの設定 NAT免除の設定 雇用 GB GB Final Configuration AAA 設定 AnyConnectを使用した接続とアクセスコントロールボリシールールの確認 FMC接続イベントを使用した確認 トレブレシュート ブレジノ レDAPデバングの動作 レDAPサーバとの接続を確立できない バインライングログインDNまたはバスワードが正しくない レDAPサーバンの支援を確立できない バンワードが正しくない AAQのデスト バマット キャプチャ バマット キャプチャ Madows Serverイベントビューアのログ	<u>ネットワークダイアグラムとシナリオ</u>	
LDAPベースDNとグループDNの決定 FTDアカウントの作成 ADグループの作成とADグループへのユーザの追加(オブション). LDAPS SSL証明書ルートのコピー(LDAPSまたはSTARTTLSの場合のみ必要). FMCの設定 ライセンスの確認 レルムの設定 AD認証用のAnyConnectの設定 アイテ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 NAT免除の設定 運調 確認 Final Configuration AAA 設定 AnyConnectの設定 AnyConnectの設定 AnyConnectの設定 AnyConnectの設定 ADPブ/シュート デブレシュート デバング LDAPデバッグの動作 LDAPサーバズコーザ名を見つけられない ズイティンクログインDNまたはパスワードが正しくない AAAのプススト パスワードが正しくない AAAのプススト パスワードが正しくない	<u>Active Directoryの設定</u>	
FTDアカウントの作成 ADグループの作成とADグループへのユーザの追加(オブション). LDAPS SSL証明書ルートのコビー(LDAPSまたはSTARTTLSの場合のみ必要). FMCの設定 ライセンスの確認 レルムの設定 AD認証用のAnyConnectの設定 アイテンティティ・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 NAT免除の設定 週週 確認 Final Configuration AAA 設定 AnyConnectの設定 FMCを続イベントを使用した確認 トラブルシュート デバッグ LDAPデバッグの動作 LDAPゲバッグロジェンクログインDIまたはパスワードが正しくない バインティングログインDIまたはパスワードが正しくない AAAののススト パワットキャブチャ パロクマスト パワットキャブチャ バリのなどスト パロクマスト	<u>LDAPベースDNとグループDNの決定</u>	
ADグルーブの作成とADグルーブへのユーザの追加(オブション)、 LDAPS SSL証明書ルートのコピー(LDAPSまたはSTARTTLSの場合のみ必要)、 FMCの設定 ライセンスの確認 レルムの設定 AD認証用のAnyConnectの設定 アイデンティティボリシーの有効化とユーザIDのセキュリティボリシーの設定 NAT免除の設定 展開 確認 Final Configuration AAA 設定 AnyConnectの設定 AAA 設定 AnyConnectの設定 ADSUT FUT JDAPデバンコート デバッグ LDAPサーバとの接続を確立できない バインティングログインDNまたはパスワードが正しくない AAAのデスト パケットキャブクト パケットキャブチャ ソーサ名のパスワードが正しくない AAAのデスト パケットキャブチャ Windows Serverイペントビューアのログ	<u>FTDアカウントの作成</u>	
LDAPS SSL証明書ルートのコピー(LDAPSまたはSTARTTLSの場合のみ必要) FMCの設定 ライセンスの確認 レルムの設定 AD認証用のAnyConnect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 NAT免除の設定 展開 確認 Final Configuration AAA 設定 AnyConnectの設定 AnyConnectの設定 AnyConnectを使用した接続とアクセスコントロールポリシールールの確認 FMC接続イベントを使用した確認 トラブルシュート デバッグ LDAPサーバとの接続を確立できない バインティングロダインDNまたはパスワードが正しくない LDAPサーバがユーザ名を見つけられない 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	<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>	
FMCの設定 ライセンスの確認 レルムの設定 AD認証用のAnyConnectの設定 アイデンティティボリシーの有効化とユーザIDのセキュリティボリシーの設定 NATを絵の設定 展開 確認	<u>LDAPS SSL証明書ルートのコピー(LDAPSまたはSTARTTLSの場合のみ必要)</u>	
ライセンスの確認 レルムの設定 AD認証用のAnyConnectの設定 アイデンティティボリシーの有効化とユーザIDのセキュリティボリシーの設定 NAT免除の設定 展期 確認 Final Configuration AAA 設定 AnyConnectの設定 AnyConnectを使用した接続とアクセスコントロールボリシールールの確認 FMC接続イベントを使用した確認 F/ブグ レDAPデバッグの動作 LDAPデバッグの動作 LDAPデバッグの動作 LDAPサーバどの接続を確立できない パインディングロダインDNまたは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 パロのマスト パケット キャプチャ Windows Serverイベントビューアのログ	<u>FMCの設定</u>	
レルムの設定 AD認証用のAnyConnectの設定 アイデンティティボリシーの有効化とユーザIDのセキュリティボリシーの設定 NAT免除の設定 履聞 確認	<u>ライセンスの確認</u>	
AD認証用のAnyConnectの設定 アイデンティティボリシーの有効化とユーザIDのセキュリティボリシーの設定 NAT免除の設定 展開 確認 Final Configuration AAA 設定 AnyConnectの設定 AnyConnectを使用した接続とアクセスコントロールボリシールールの確認 FMC接続イベントを使用した確認 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 パインティングログインDNまたはパスワードが正しくない LDAPサーバガユーザ名を見つけられない 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		
アイナンティチャホリシーの有効化とユーザ10のセキュリティホリシーの設定 NAT免除の設定 展開 確認 Final Configuration AAA 設定 AnyConnectの設定 AnyConnectを使用した接続とアクセスコントロールボリシールールの確認 FMC接続イベントを使用した確認 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 パインティングログインDNまたはパスワードが正しくない LDAPサーバがユーザ名を見つけられない 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	AD認証用のAnyConnectの設定	
INTIXEVEZE 雇団 確認 Final Configuration AAA 設定 AnyConnectの設定 AnyConnectを使用した接続とアクセスコントロールポリシールールの確認 FMC接続イベントを使用した確認 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 パインティングログインDNまたはパスワードが正しくない LDAPサーバがユーザ名を見つけられない 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	<u> アイデンティティホリンーの有効化とユーザIDのセキュリティホリンーの設定</u>	
確認 Final Configuration AAA 設定 AnyConnectの設定 AnyConnectを使用した接続とアクセスコントロールポリシールールの確認 FMC接続イベントを使用した確認 トラブルシュート デバッグ LDAPサーバとの接続を確立できない パインディングログインDNまたはパスワードが正しくない LDAPサーバガユーザ名を見つけられない 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 ゾバウット ビューアのログ	NAT光味の設定 定問	
<pre>UEE&> Final Configuration AAA 設定 AnyConnectの設定 AnyConnectを使用した接続とアクセスコントロールポリシールールの確認 FMC接続イベントを使用した確認 トラブルシュート プバッグ LDAPデバッグの動作 LDAPサーバとの接続を確立できない バインディングログインDNまたはパスワードが正しくない LDAPサーバがユーザ名を見っけられない 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 </pre>		
Final Configuration AAA 設定 AnyConnectの設定 AnyConnectを使用した接続とアクセスコントロールポリシールールの確認 FMC接続イベントを使用した確認 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 バインディングログインDNまたはパスワードが正しくない LDAPサーバがユーザ名を見つけられない 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イペントビューアのログ		
AAA 設定 AnyConnectの設定 AnyConnectを使用した接続とアクセスコントロールポリシールールの確認 FMC接続イベントを使用した確認 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 バインディングログインDNまたはパスワードが正しくない LDAPサーバがユーザ名を見つけられない 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	Final Configuration	
AnyConnectを使用した接続とアクセスコントロールポリシールールの確認 FMC接続イベントを使用した確認 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 バインディングログインDNまたはパスワードが正しくない LDAPサーバがユーザ名を見つけられない 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	AAA 設定	
AnyConnectを使用した複数 FMC接続イベントを使用した確認 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 バインディングログインDNまたはパスワードが正しくない LDAPサーバがユーザ名を見つけられない 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		
FMC 接続イベントを使用した確認 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 バインディングログインDNまたはパスワードが正しくない LDAPサーバがユーザ名を見つけられない 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	AnyConnectを使用した接続とアクセスコントロールホ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 バインディングログインDNまたはパスワードが正しくない LDAPサーバがユーザ名を見つけられない 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		
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 バインディングログインDNまたはパスワードが正しくない LDAPサーバがユーザ名を見つけられない 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		
LDAPデバッグの動作 LDAPサーバとの接続を確立できない バインディングログインDNまたはパスワードが正しくない LDAPサーバがユーザ名を見つけられない 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	<u>デバッグ</u>	
LDAPサーバとの接続を確立できない バインディングログインDNまたはパスワードが正しくない LDAPサーバがユーザ名を見つけられない 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	LDAPデバッグの動作	
<u> </u>	<u>LDAPサーバとの接続を催立できない</u> バインディングログインDNまたはパスロードがエレイたい	
<u>ユーザ名のパスワードが正しくない</u> AAAのテスト <u>パケット キャプチャ</u> Windows Serverイベントビューアのログ		
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	<u>- レローン パルユーン 古てた シャラれない</u> フーザ名のパスワードが正しくない	
<u>パケット キャプチャ</u> <u>パケット キャプチャ</u> <u>Windows Serverイベントビューアのログ</u>		
<u>ハワットイェノナェ</u> <u>Windows Serverイベントビューアのログ</u>		
Windows Serverイベントビューアのログ		
	Windows Serverイベントビューアのロク	

はじめに

このドキュメントでは、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について説明します。

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。

- Firepower Manage Center(FMC)でのRAバーチャルプライベートネットワーク(VPN)の設定
- FMCでのLightweight Directory Access Protocol(LDAP)サーバの設定
- Active Directory (AD)
- 完全修飾ドメイン名(FQDN)
- Intersightインフラストラクチャサービス(IIS)
- ・ リモートデスクトッププロトコル(RDP)

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サーバー
- 6.5.0が稼働するFMCv
- 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、クリアな(デフォルト)設定で作業を開始していま 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。

背景説明

このドキュメントでは、Firepower Threat Defense(FTD)に接続し、Firepower Management Center(FMC)で管理するAnyConnectクライアントのActive Directory(AD)認証を設定する方法につ いて説明します。

ユーザIDは、AnyConnectユーザを特定のIPアドレスとポートに制限するためにアクセスポリシー で使用されます。

設定

ネットワークダイアグラムとシナリオ



Windowsサーバでは、ユーザIDをテストするためにIISとRDPが事前設定されています。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 Admin:FTDをActive Directoryサーバにバインドするためのディレクトリアカウントとして使用されます。
- IT管理者:ユーザーIDを示す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:ユーザIDを示すために使用されるテストユーザアカウント。

グループ:

- AnyConnect管理者:ユーザIDを示すためにIT管理者が追加するテストグループ。このグル ープは、Windows Serverに対するRDPアクセスのみを持ちます。
- AnyConnectユーザ:ユーザIDを示す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アクセス権しかありません。

Active Directory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。

これらの詳細はすべて、FMCで設定を行う前にMicrosoftサーバ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。このコンフィギュレーションガイドでは、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を使用する場合は、FQDNを解決するためにDNSサーバをFMCおよびFTD内で設定する必要があります。

このコンフィギュレーションガイドでは、この値はwin2016.example.com(192.168.1.1に解決される)です。

・ サーバポート:

LDAPサービスが使用するポート。デフォルトでは、LDAPおよび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で使用するSSL証明書の署名に使用するルート CAが必要です。

ディレクトリユーザ名とパスワード:

これは、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

FMCとFTDによって使用されるアカウントです。

この目的のために、FTD Adminという名前のアカウントが作成されます。

• ベースとグループの識別名(DN):

ベースDNはFMCの開始点で、FTDはActive Directoryに対してユーザの検索と認証を開始するよう に指示します。

同様に、グループDNは、FMCがActive DirectoryにユーザIDのグループ検索を開始する場所を指示する開始点です。

このコンフィギュレーションガイドでは、ルートドメインexample.comがベースDNおよびグルー プDNとして使用されます。

ただし、実稼働環境の場合は、LDAP階層内のベースDNとグループDNを使用する方が適していま す。

たとえば、次のLDAP階層があります。



管理者が、Marketing組織単位(OU)内のユーザがベースDNを認証できるようにする必要がある場合は、ルート(example.com)に設定できます。

ただし、これによってFinance組織単位(OU)の下のUser1もログインできます。これは、ユーザ検索がルートから始まり、Finance、Marketing、およびResearchに移動するためです。

ベースDNをexample.comに設定



ログインをMarketing組織単位(OU)以下の唯一のユーザに制限するために、管理者はベースDNを

Marketingに設定できます。

Marketingで検索が開始されるため、ここで認証できるのはUser2とUser3だけです。

ベースDNをMarketingに設定



ユーザが接続を許可される、またはユーザにAD属性に基づいた異なる許可を割り当てる、FTD内 でのさらに細かい制御のために、LDAP認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。

詳細については、「<u>Firepower Threat Defense(FTD)でのAnyConnect LDAPマッピングの設定</u>」を 参照してください。

この簡素化されたLDAP階層がこの設定ガイドで使用され、ルートexample.comのDNがベース DNとグループDNの両方に使用されます。



LDAPベースDNとグループDNの決定

1. Active Directory Users and Computersを開きます。



2. Connectionの下で、Connectを選択します。

😭 Ldp		_		×
Connection Browse V	/iew Options Utilities Help			
Connect Bind Ct Disconnect	trl+B			
New Ct Save Save As	rl+N			
Exit				
			NILINA	
			NUM	

3. サーバーのlocalhostおよび適切なポートを指定し、OKをクリックします。

Connect		×
Server:	localhost	
<u>P</u> ort:	389	Connectionless
<u>0</u> K		<u>C</u> ancel

4. 右側の列には、接続が正常に行われたことを示すテキストが表示されます。Connection > Bindの順に移動します。

🔝 Idap://win2016.exa	ample.co	om/DC=	example,DC	=com		_		×	
Connection Browse	View	Optior	ns Utilities	Help					
Connection Browse Connect Bind Disconnect New Save Save As Exit	View Ctrl+B Ctrl+N	Optior	ns Utilities Id = Idap_op Established Retrieving back Getting 1 en Dn: (RootD) configur CN= current Time defaultN dnsHost domain dsServi Sett Firs	Help en("localh connection ase DSA in tries: SE) rationNami Configura Time: 5/1/2 e; lamingCon tName: win ControllerFi functionalit ceName: C tings,CN=V t-Site-	ost", 389); n to localhost. nformation ngContext: tion,DC=examp 020 4:16:55 PM text: DC=example unctionality: 7 = y: 7 = (WIN201 N=NTDS VIN2016,CN=Se	le,DC=co I Eastern ple,DC=co .com; = (WIN20 I6); ervers,CN	m; Daylight om; 16); I=Default-		
			Nan com forestFu highest(isGlobal isSynch IdanSer	ne,CN=Site n; unctionality CommittedU CatalogRe uronized: T viceName:	s,CN=Configur : 7 = (WIN2010 JSN: 13410; ady: TRUE; RUE; example.com;	ation,DC= 6); win2016	example,[)C=	,
									.:

5. Simple Bindを選択し、ディレクトリ・アカウント・ユーザー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:	•••••
Domain: Bind type Bind as cur Bind with c Simple bind	rrently logged on user redentials
✓ Encrypt tra Advanced	affic after bind Cancel OK

バインドが正常に行われると、ldpにはAuthenticated as: DOMAIN\usernameと表示されます。

🔐 Idap://w	in2016.exa	mple.co	om/DC=ex	ample,DC	=com		—		\times
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 edLDAPPoli PercentDir ReceiveBu Connection BatchRetur DirSyncDu ResultSetS (ResultSetS (ValRange; edLDAPVer edSASLMe IEGO; EXTE	5.1.4.2255; 5.1.4.2256; 5.1.4.2309; cies (20): Ma SyncReques ffer; InitRecues ration; MaxConnern Messages ration; MaxTonesue PerConn; MaxTonesue Conn; MaxValRang Limit; System rsion (2): 3; chanisms (4 RNAL; DIGE _s(Id, 'ftd.ad	axPoolThr sts; MaxDa vTimeout; idleTime; I ; MaxQuei empTable: ultSets; axNotificat geTransiti mMemoryL 2;): GSSAPI ST-MD5; min@exar min'.	reads; atagramRe MaxPageS ryDuration Size; tionPerCo ve; .imitPerce l; GSS- mple.com	ecv; Size; n; nn; ent;
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、次に示す2つのエラーが発 生します。

Connection Browse View Options Utilities Help	
MaxResultSetSize; MinResultSets; MaxResultSetsPerConn; MaxNotificationPerConn; MaxValRange; MaxValRangeTransitive; ThreadMemoryLimit; SystemMemoryLimitPercent; supportedLDAPVersion (2): 3; 2; supportedSASLMechanisms (4): GSSAPI; GSS- SPNEGO; EXTERNAL; DIGEST-MD5; 	^
Error <49>: ldap_simple_bind_s() failed: Invalid Credentials Server error: 80090308: LdapErr: DSID-0C09042A, comment: AccentSecurityContext error_data 52e_v3839	
Error 0x80090308 The token supplied to the function is invalid	
Ready	۷.

LDAPサーバがユーザ名を見つけられない

<#root>

```
[-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

考えられる解決方法:ADがFTDによる検索でユーザを見つけられることを確認します。これは ldp.exeでも実行できます。

1. 前述のように正常にバインドされた後、「表示」>「ツリー」にナビゲートします。

Connection Browse View Options Utilities Help	_
Tree Ctrl+T	^
Enterprise Configuration //axPoolThreads;	
Status Bar sts; MaxDatagramRecv;	
Set Font nldleTime; MaxPageSize; s: MaxQueryDuration;	
MaxDirSyncDuration; MaxTempTableSize; MaxResultSetSize; MinResultSets; MaxResultSetsPerConn; MaxNotificationPerConn; MaxValRange; MaxValRangeTransitive; ThreadMemoryLimit; SystemMemoryLimitPercent; supportedLDAPVersion (2): 3; 2; supportedSASLMechanisms (4): GSSAPI; GSS- SPNEGO; EXTERNAL; DIGEST-MD5;	
res = ldap_simple_bind_s(ld, 'ftd.admin@example.com', <unavailable>); // v.3 Authenticated as: 'EXAMPLE\ftd.admin'. </unavailable>	
	¥

2. FTDで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. ベースDNを右クリックし、検索をクリックします。

🔛 Idap://wi	n2016.exa	mple.co	om/DC=ex	ample,DC	=com	- o >	<
Connection	Browse	View	Options	Utilities	Help		
DC=exam	ple,DC=c	om	Search Virtual L Delete Modify Modify Add chil Compar Advance	ist View DN Id e	Ctrl+S Ctrl+D Ctrl+M Ctrl+R Ctrl+A	cipals,DC=example,DC=com; 11D2B9AA00C04F79F805:CN =example,DC=com; E11D297C400C04FD8D5CD:C =example,DC=com; 11D1ADED00C04FD8D5CD:C =example,DC=com; 11D1ADED00C04FD8D5CD:C ble,DC=com; 11D1AA4B00C04FD7D83A:O s,DC=example,DC=com; 11D1ADED00C04FD8D5CD:C ample,DC=com; 311D1ADED00C04FD8D5CD:C	^
Contractor			Copy Di Copy Select al Clear ou	N I Itput	Ctrl+C Ctrl+N	e,DC=com; 0 3:43:59 PM Eastern Daylight 2:41:57 PM Eastern Daylight	~
Create a new d	locument						.:

4. デバッグに表示されるのと同じBase DN、Filter、およびScopeの値を指定します。

この例では、次のようになります。

- ・ベースDN:dc=example,dc=com
- ・フィルタ: samaccountname=it.admi
- ・ スコープ:サブツリー

🔐 Idap://w	n2016.example.com/DC=example,DC=com	– 🗆 X	
Connection	Browse View Options Utilities Help		
Search	×	C=example,DC=com; S8811D1ADED00C04FD8D5CD:C DC=example,DC=com;	^
Base DN:	DC=example,DC=com ~	58811D1ADED00C04FD8D5CD:C	
Filter:	sAMAccountName=it.admi ~	ample,DC=com; D211D1AA4B00C04FD7D83A:0	
Scope O Base	One Level Subtree	lers,DC=example,DC=com; \$8811D1ADED00C04FD8D5CD:C example,DC=com;	
Attributes:	objectClass;name;description;canonicalName ~	68811D1ADED00C04FD8D5CD:C mple,DC=com;	
Options	Run Close	2020 3:43:59 PM Eastern Daylight	
	***Searching kdap_search_s(kd, "DC=0 "sAMAccountName=it.ad Getting 0 entries:	example,DC=com", 2, dmi", attrList, 0, &msg)	~
Ready			.::

ベースDN dc=example,dc=comの下にsAMAccountname it.admiを持つユーザアカウントがないため、ldpは0エントリを検索します。

正しいsAMAccountname it.adminを使用した別の試行では、異なる結果が表示されます。ldpはベースDN dc=example,dc=comの下の1つのエントリを見つけ、そのユーザDNを出力します。

🟠 Idap://w	n2016.example.com/DC=example	DC=com	- 0	×
Connection	Browse View Options Utilit	es Help		
Search		×	58811D1ADED00C04FD8 DC=example,DC=com; 58811D1ADED00C04FD8	SD5CD:C
Base <u>D</u> N:	DC=example,DC=com	~	ample,DC=com;	
<u>F</u> ilter:	sAMAccountName=it.admin	~	D211D1AA4B00C04FD7 lers,DC=example,DC=co	7D83A:0 m;
Scope	○ <u>O</u> ne Level <u>Subtree</u>		 s8811D1ADED00C04FD8 example,DC=com; 68811D1ADED00C04FD8 mple DC=com; 	8D5CD:C
<u>A</u> ttributes:	objectClass;name;description;canon	calName 🗸	020 3:43:59 PM Eastern	Daylight
Options	<u>R</u> un	<u>C</u> lose)20 2:41:57 PM Eastern [Daylight
	***Searc dap_se "sAMAc Getting Dn: CN= can nam obje	hing arch_s(ld, "DC=6 countName=it.ac entries: IT Admin,CN=0 nicalName: exa e: IT Admin; ctClass (4): top; user;	example,DC=com", 2, dmin", attrList, 0, &msg) U sers,DC=example,DC= mple.com/Users/IT Admin; person; organizationalPer	com rson;
Ready				

ユーザ名のパスワードが正しくない

<#root>

```
[-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 erro [-2147483613]

Invalid password for it.admin

[-2147483613] Fiber exit Tx=514 bytes Rx=2764 bytes, status=-1 [-2147483613] Session End

考えられる解決方法:ユーザーパスワードが適切に構成され、有効期限が切れていないことを確認します。ログインDNと同様に、FTDはユーザクレデンシャルを使用してADに対するバインド 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で実行することもできます。ldpの手順は、「ログインDNまたはパスワードのバインデ ィングが正しくない」のセクションを参照してください。

また、潜在的な障害の原因を確認するために、MicrosoftサーバのEvent Viewerログを確認できま す。

AAAのテスト

test aaa-serverコマンドを使用すると、特定のユーザ名とパスワードを使用したFTDからの認証 試行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。

<#root>

> 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

パケット キャプチャ

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。

キャプチャは、双方向のLDAPトラフィックを示しています。

> show route 192.168.1.1

Routing entry for 192.168.1.0 255.255.255.0
Known via "connected", distance 0, metric 0 (connected, via interface)
Routing Descriptor Blocks:
* directly connected, via inside
Route metric is 0, traffic share count is 1

> capture AD interface inside match tcp any host 192.168.1.1 eq 389

> show capture
capture AD type raw-data interface inside [Capturing - 0 bytes]
match tcp any host 192.168.1.1 eq ldap

> test aaa-server authentication LAB-AD host win2016.example.com username it.admin password ******
INFO: Attempting Authentication test to IP address (192.168.1.1) (timeout: 12 seconds)
INFO: Authentication Successful

> show capture
capture AD type raw-data interface inside [Capturing - 10905 bytes]
match tcp any host 192.168.1.1 eq ldap

> show capture AD

54 packets captured

192.168.1.17.61960 > 192.168.1.1.389: S 3681912834:3681912834(0) win 327681: 23:02:16.770712 2: 23:02:16.772009 192.168.1.1.389 > 192.168.1.17.61960: S 491521506:491521506(0) ack 36819128 3: 23:02:16.772039 192.168.1.17.61960 > 192.168.1.1.389: . ack 491521507 win 32768 <nop,nop,ti 4: 23:02:16.772482 192.168.1.17.61960 > 192.168.1.1.389: P 3681912835:3681912980(145) ack 4915 5: 23:02:16.772924 192.168.1.1.389 > 192.168.1.17.61960: P 491521507:491522141(634) ack 368191 6: 23:02:16.772955 192.168.1.17.61960 > 192.168.1.1.389: . ack 491522141 win 32768 <nop,nop,ti 192.168.1.17.61960 > 192.168.1.1.389: P 3681912980:3681913024(44) ack 49152 7: 23:02:16.773428 192.168.1.1.389 > 192.168.1.17.61960: P 491522141:491522163(22) ack 3681913 8: 23:02:16.775030 9: 23:02:16.775075 192.168.1.17.61960 > 192.168.1.1.389: . ack 491522163 win 32768 <nop,nop,ti [...]

54 packets shown

Windows Serverイベントビューアのログ

ADサーバの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録されます。

1. イベントビューアを検索して開きます。



翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人に よる翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっ ても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性につ いて法的責任を負いません。原典である英語版(リンクからアクセス可能)もあわせて参照する ことを推奨します。