

AnyConnectクライアント用のAD認証の設定

内容

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[背景説明](#)

[設定](#)

[ネットワークダイアグラムとシナリオ](#)

[Active Directoryの設定](#)

[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 \(オプション \)](#)

[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](#)

[トラブルシューティング](#)

[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](#)

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):

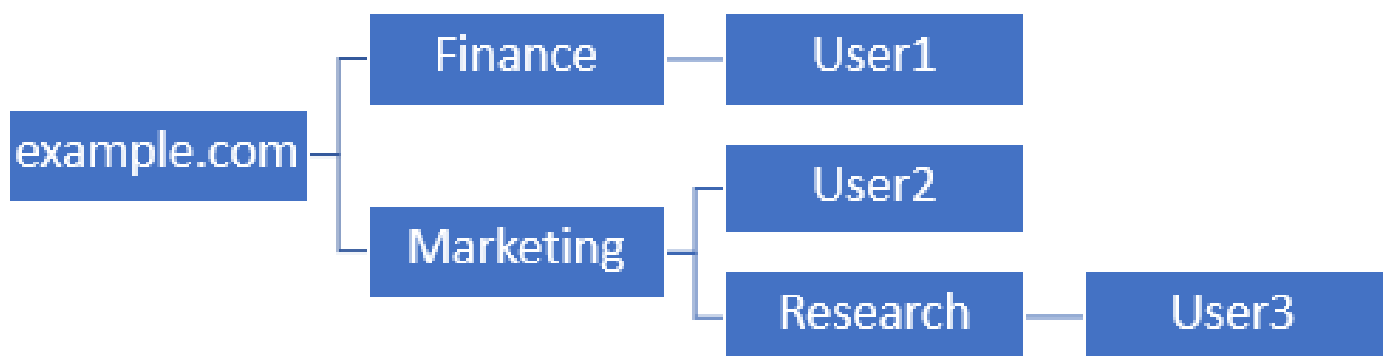
ベースDNはFMCの開始点で、FTDはActive Directoryに対してユーザの検索と認証を開始するように指示します。

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。

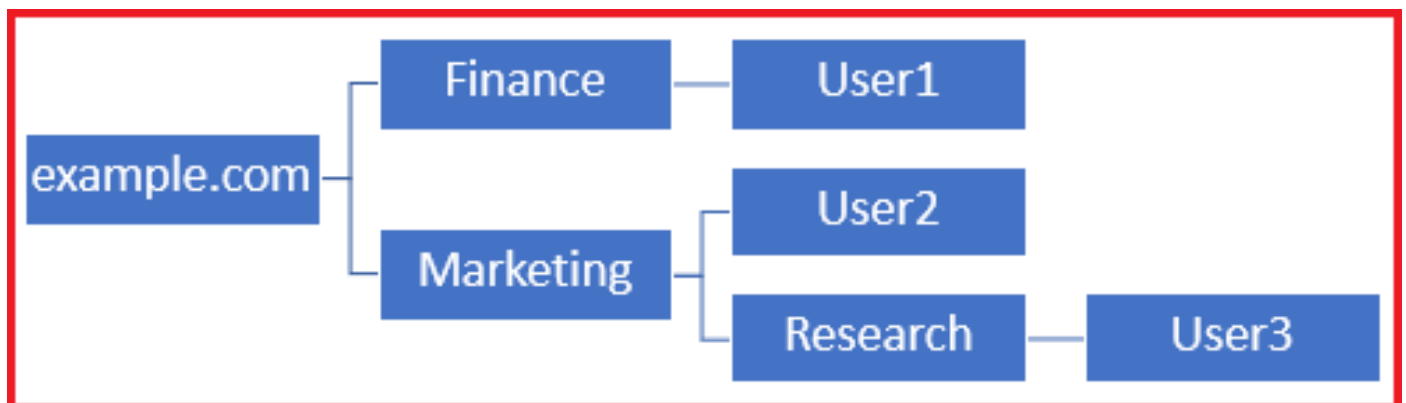
たとえば、次のLDAP階層があります。



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)の下での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

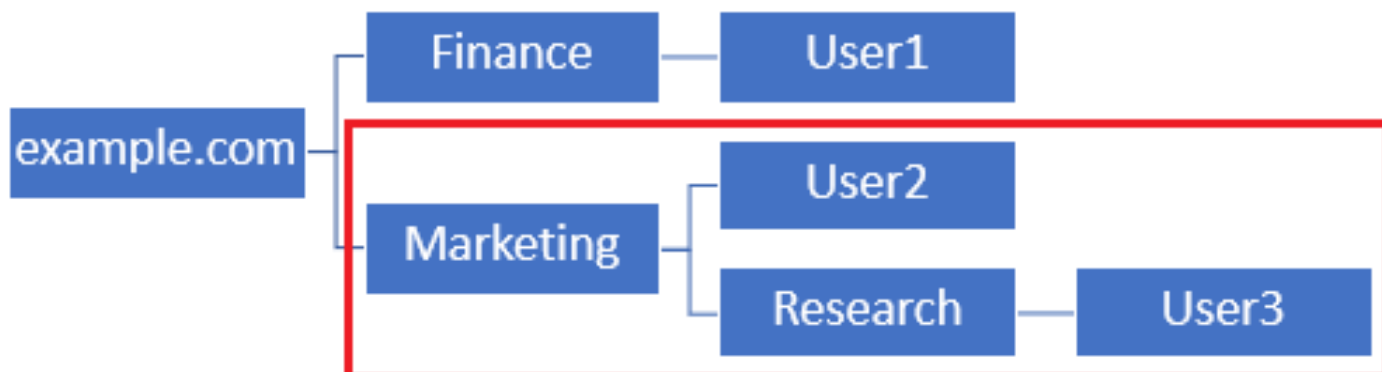


ログインをMarketing組織単位(OU)以下の唯一のユーザに制限するために、管理者はベースDNを

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。

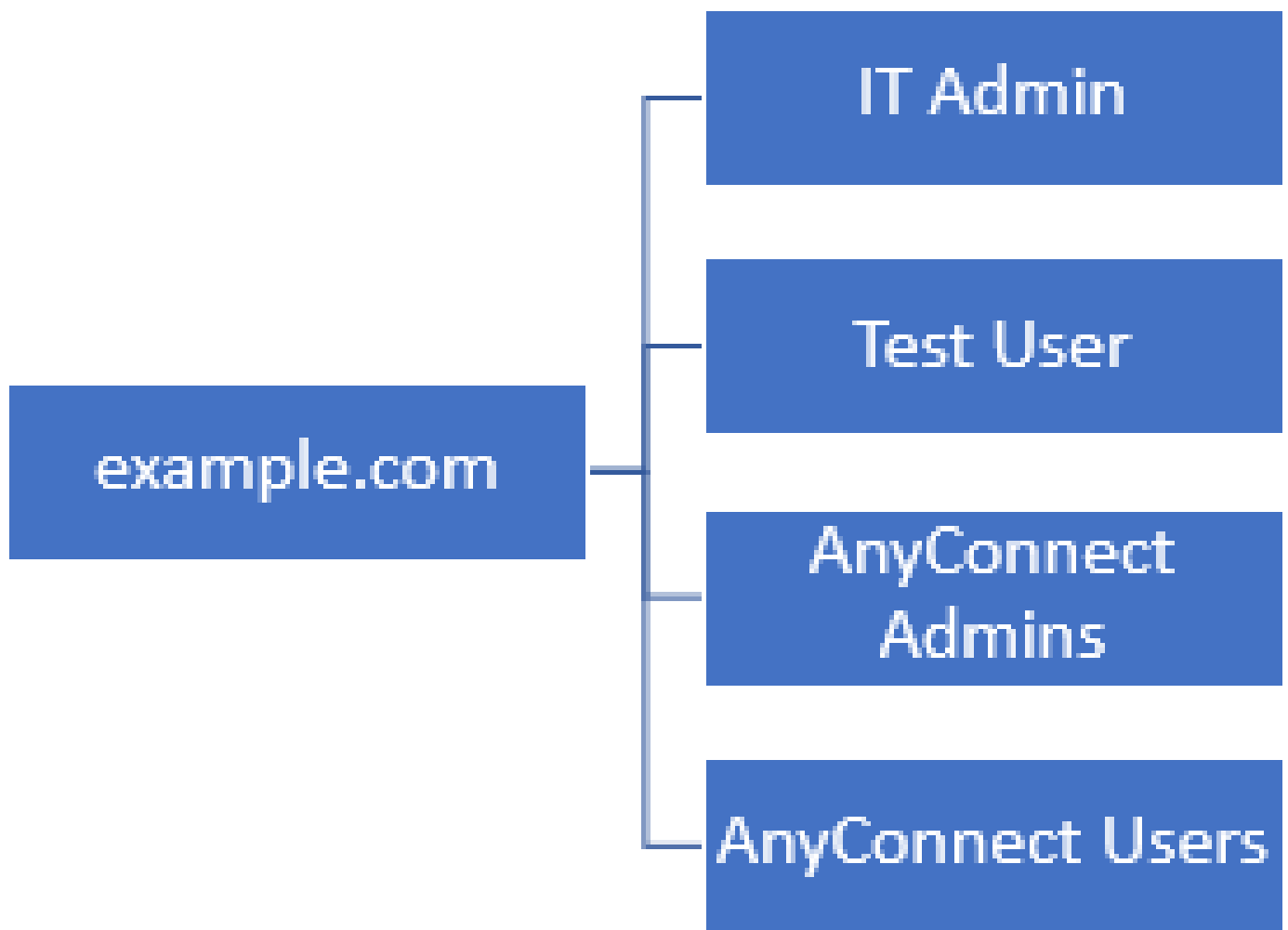
ベースDNをMarketingに設定



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、「[Firepower Threat Defense\(FTD\)でのAnyConnect LDAPマッピングの設定](#)」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。



Best match



Active Directory Users and Computers

Desktop app

Settings



Edit local users and groups



Change User Account Control settings



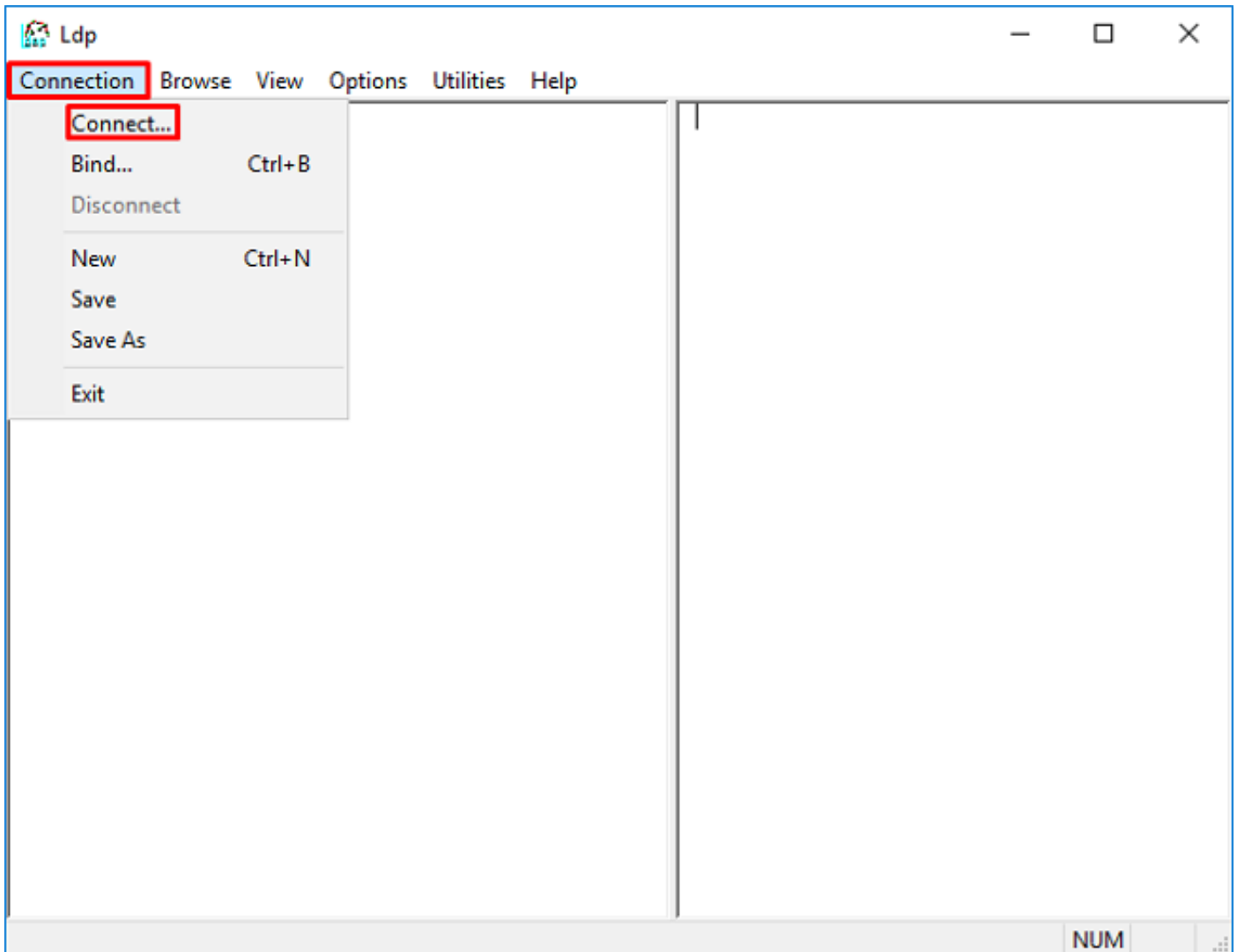
User Accounts



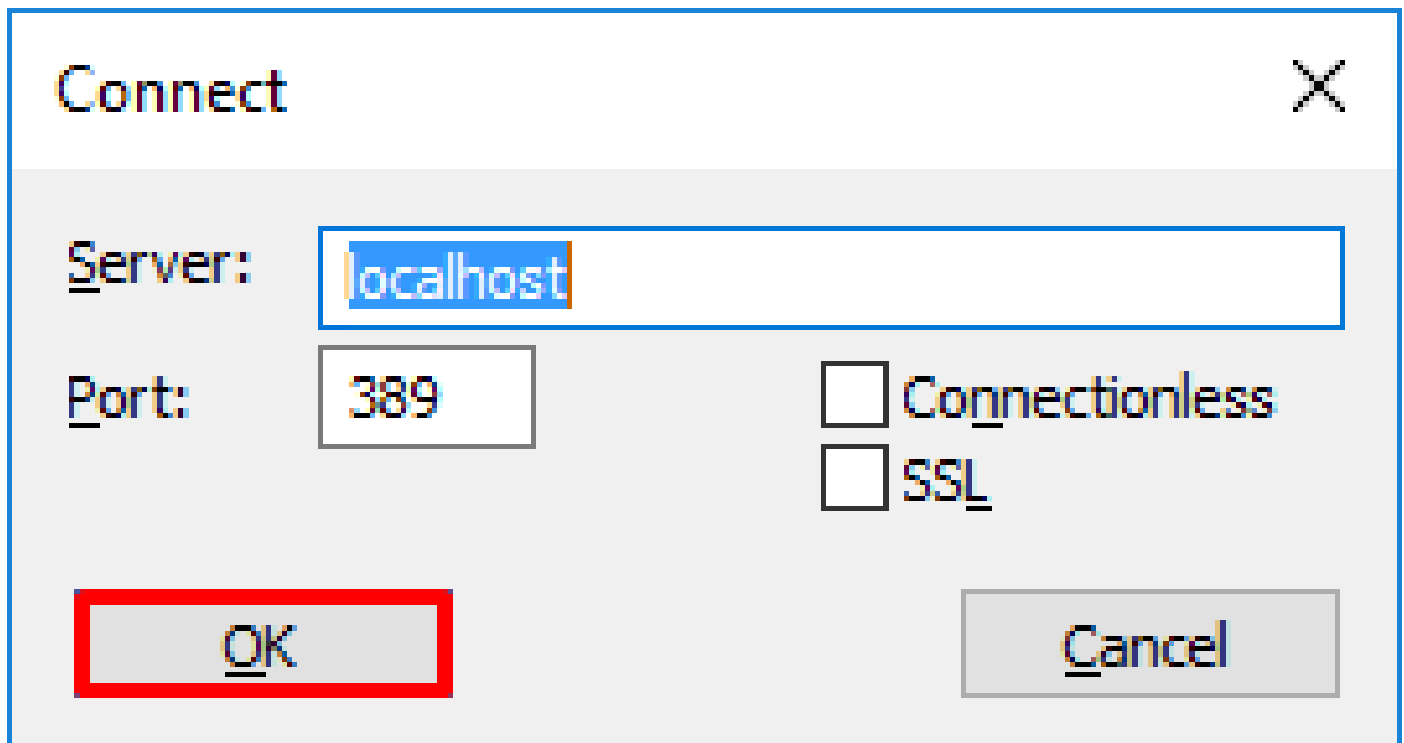
Select users who can use remote desktop



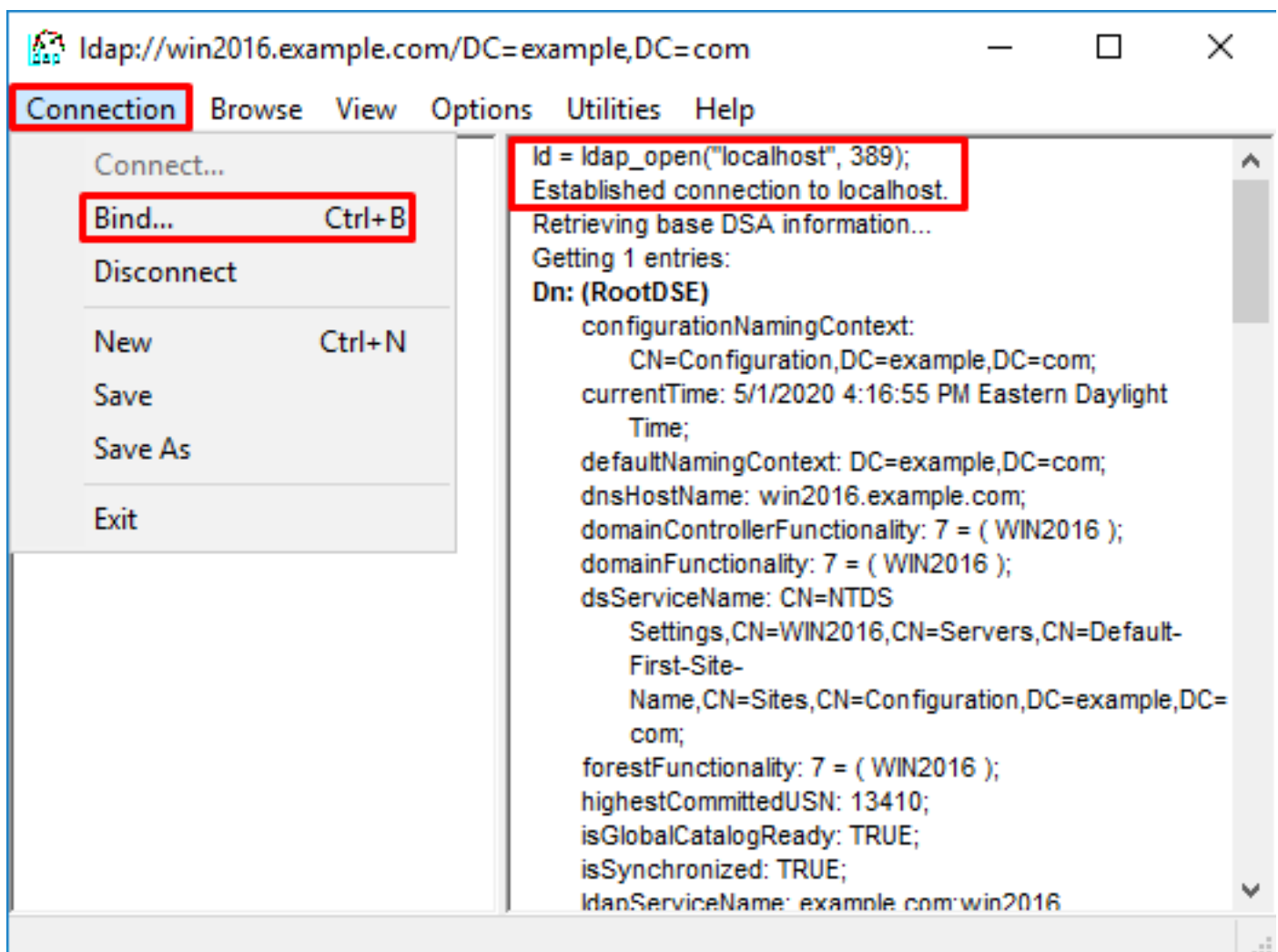
2. Connectionの下で、Connectを選択します。



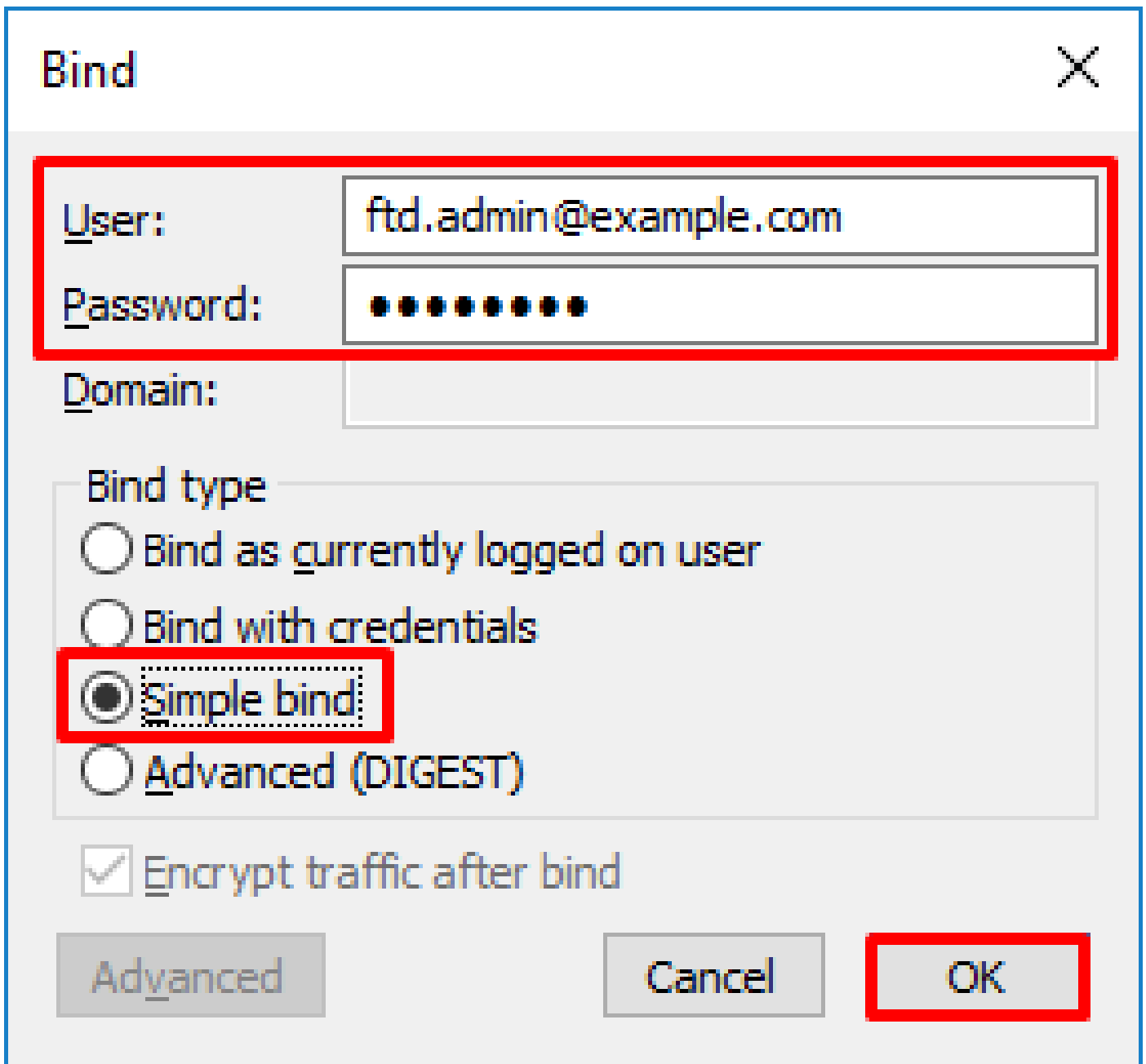
3. サーバーのlocalhostおよび適切なポートを指定し、OKをクリックします。



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。



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 [X]

User: ftd.admin@example.com

Password: ●●●●●●●●

Domain:

Bind type

Bind as currently logged on user

Bind with credentials

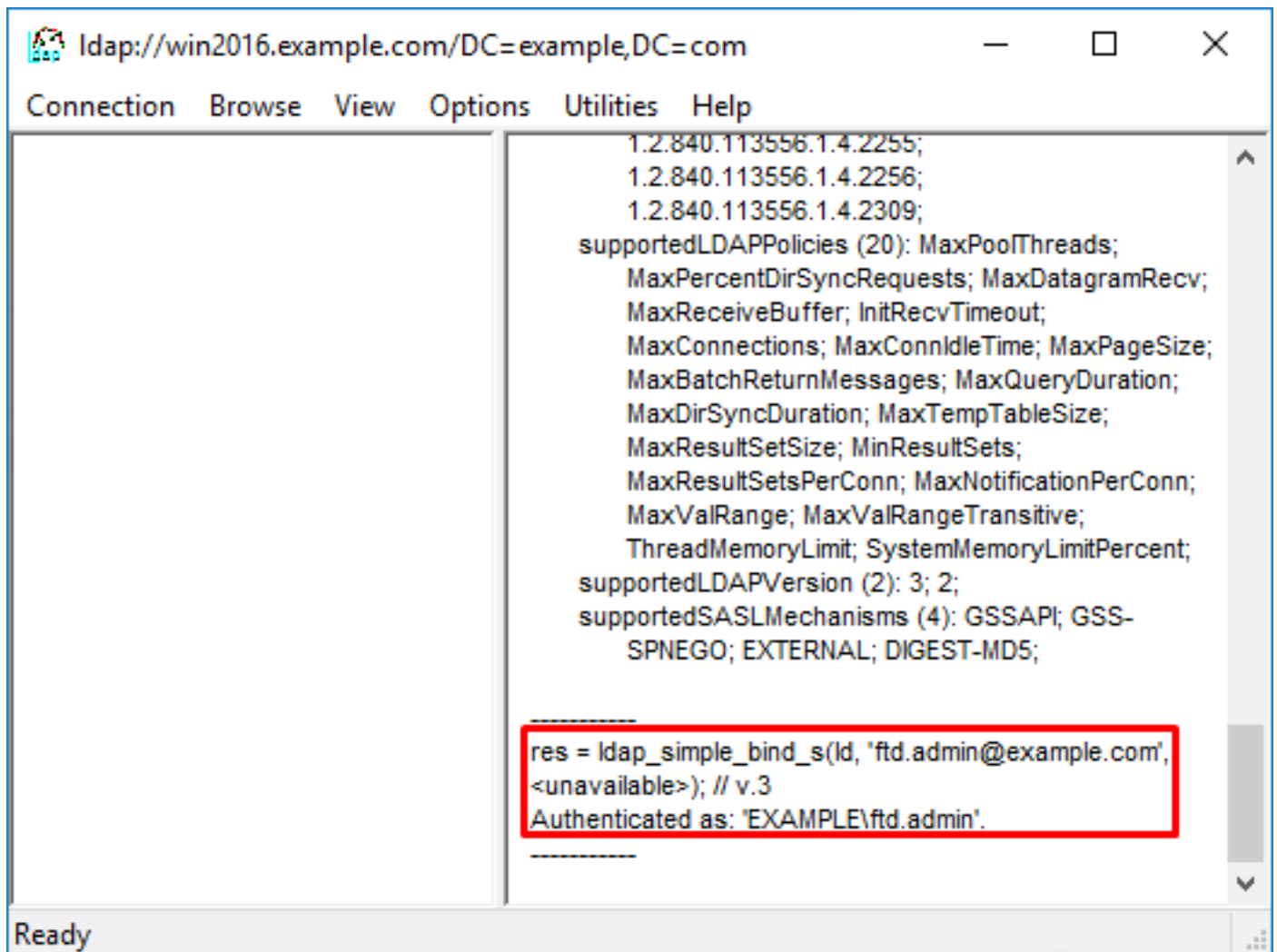
Simple bind

Advanced (DIGEST)

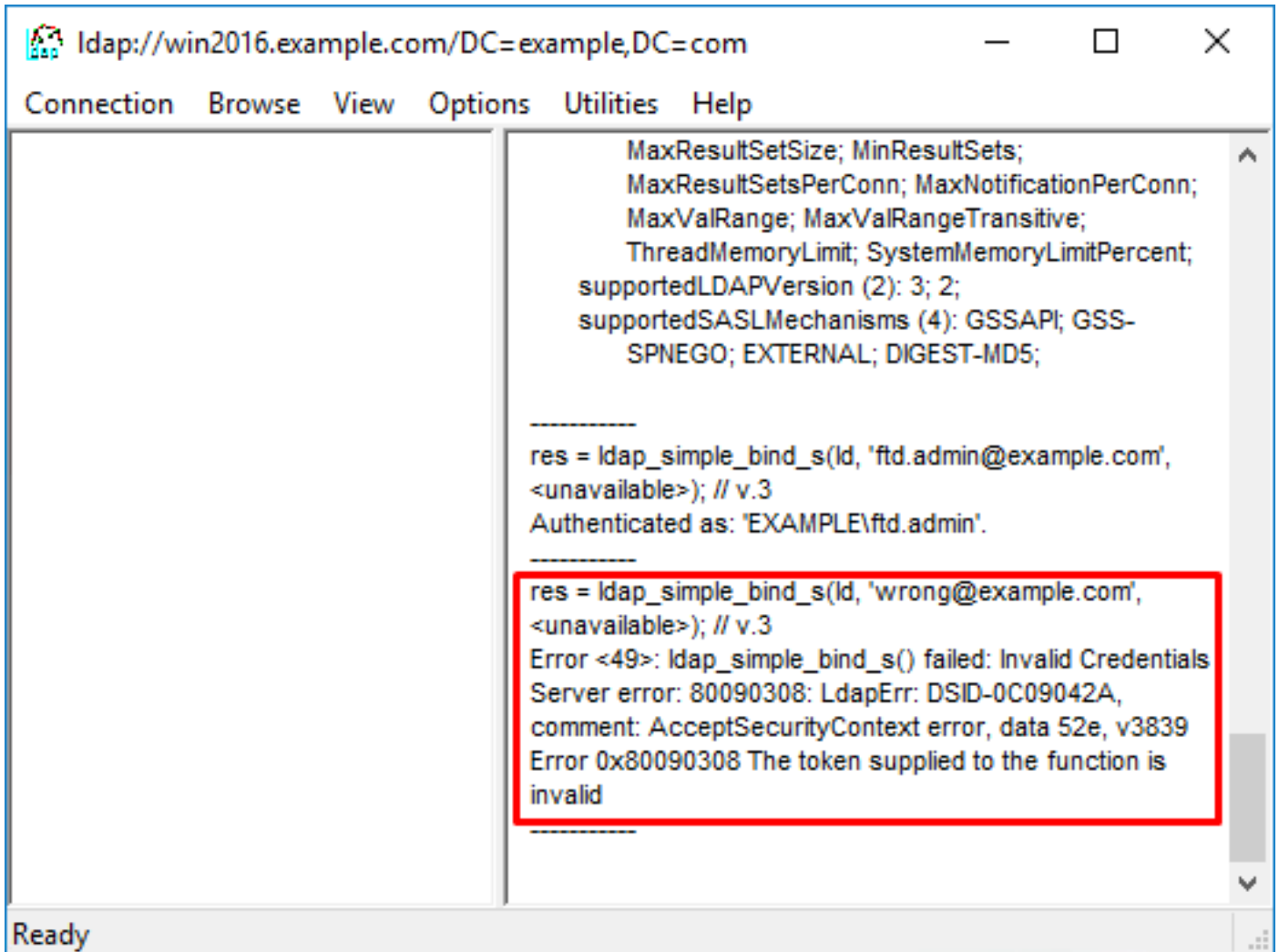
Encrypt traffic after bind

Advanced Cancel **OK**

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



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、次に示す2つのエラーが発生します。



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]

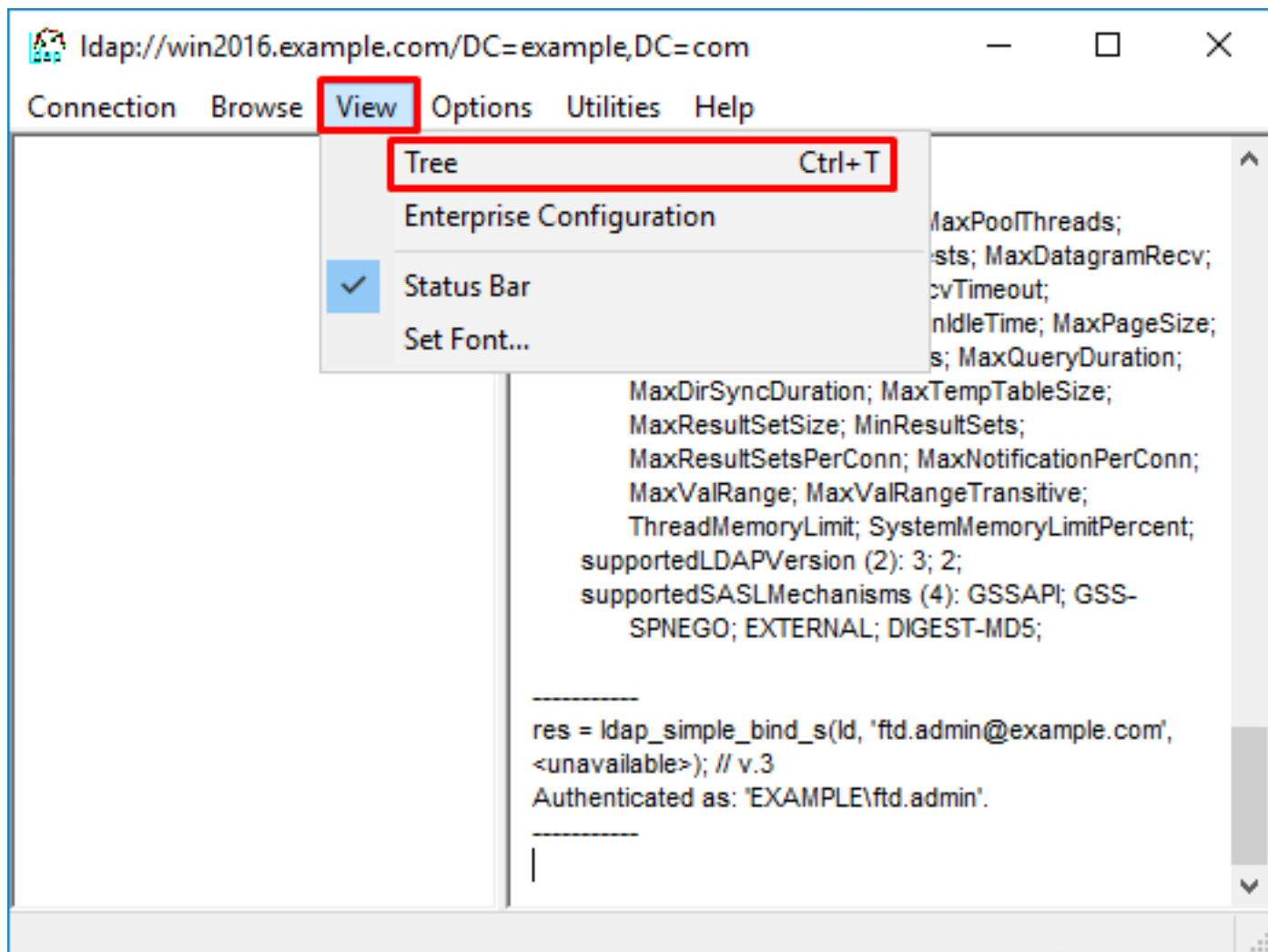
Search result parsing returned failure status

[-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
```

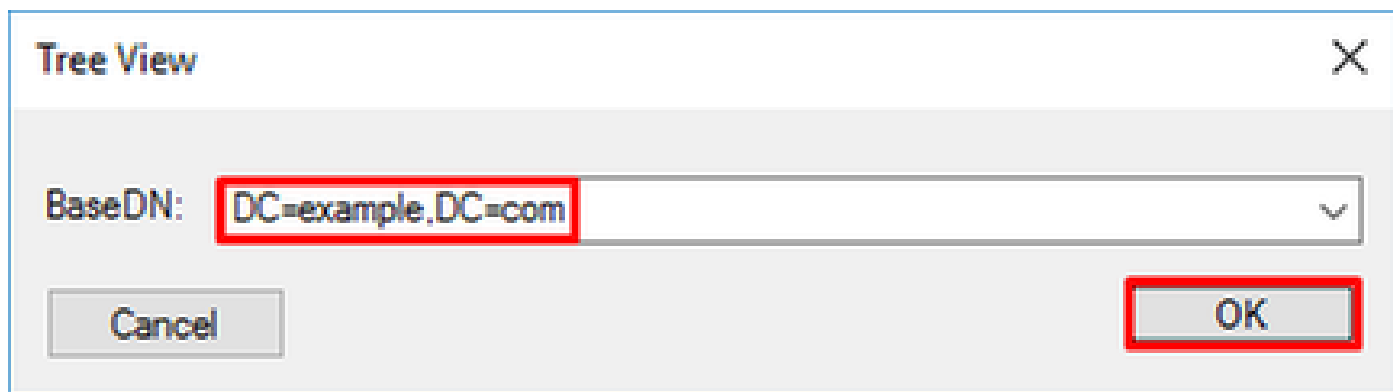
[-2147483612] Fiber exit Tx=456 bytes Rx=1082 bytes, status=-1
[-2147483612] Session End

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。

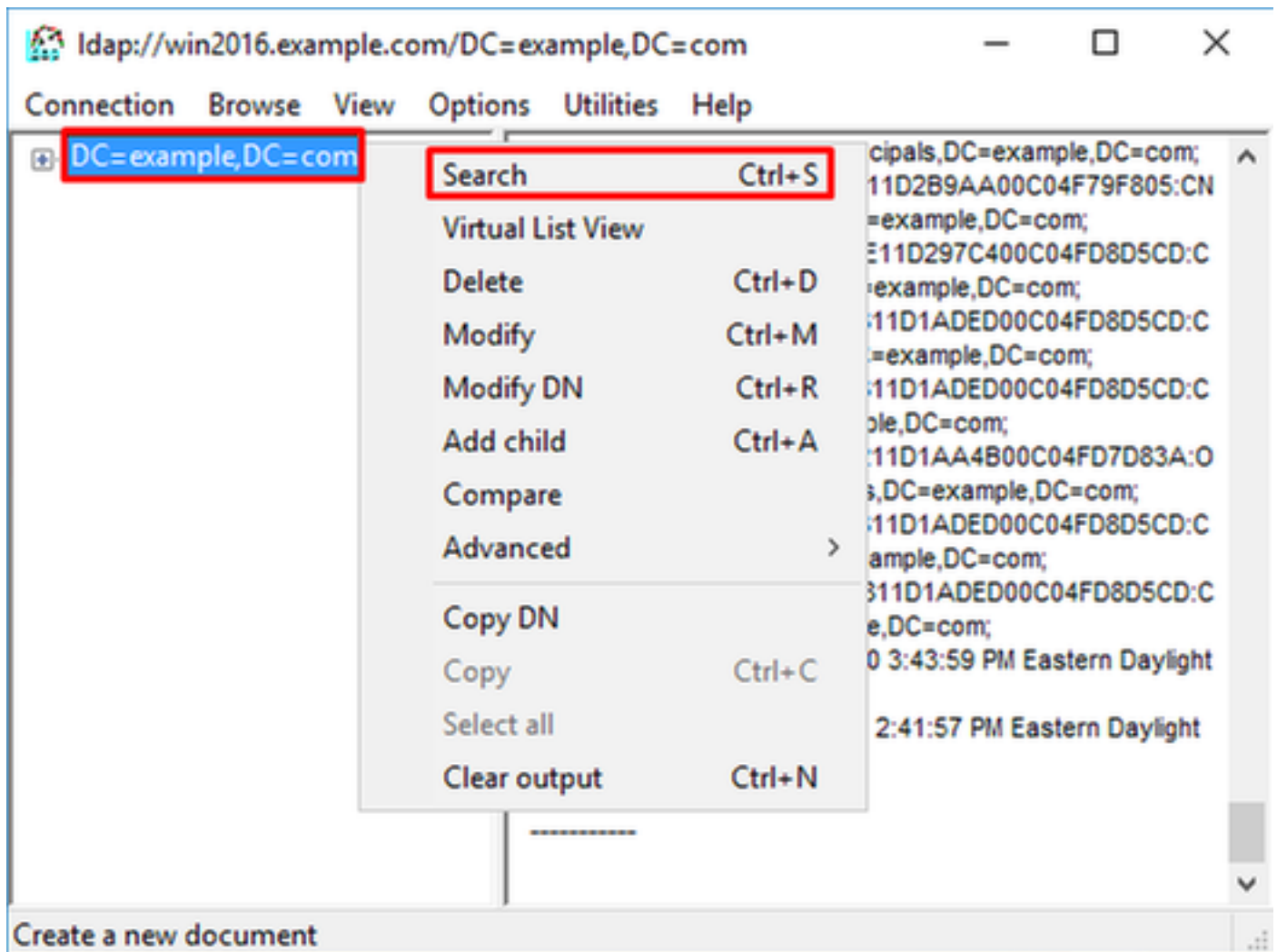
1. 前述のように正常にバインドされた後、「表示」>「ツリー」にナビゲートします。



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。



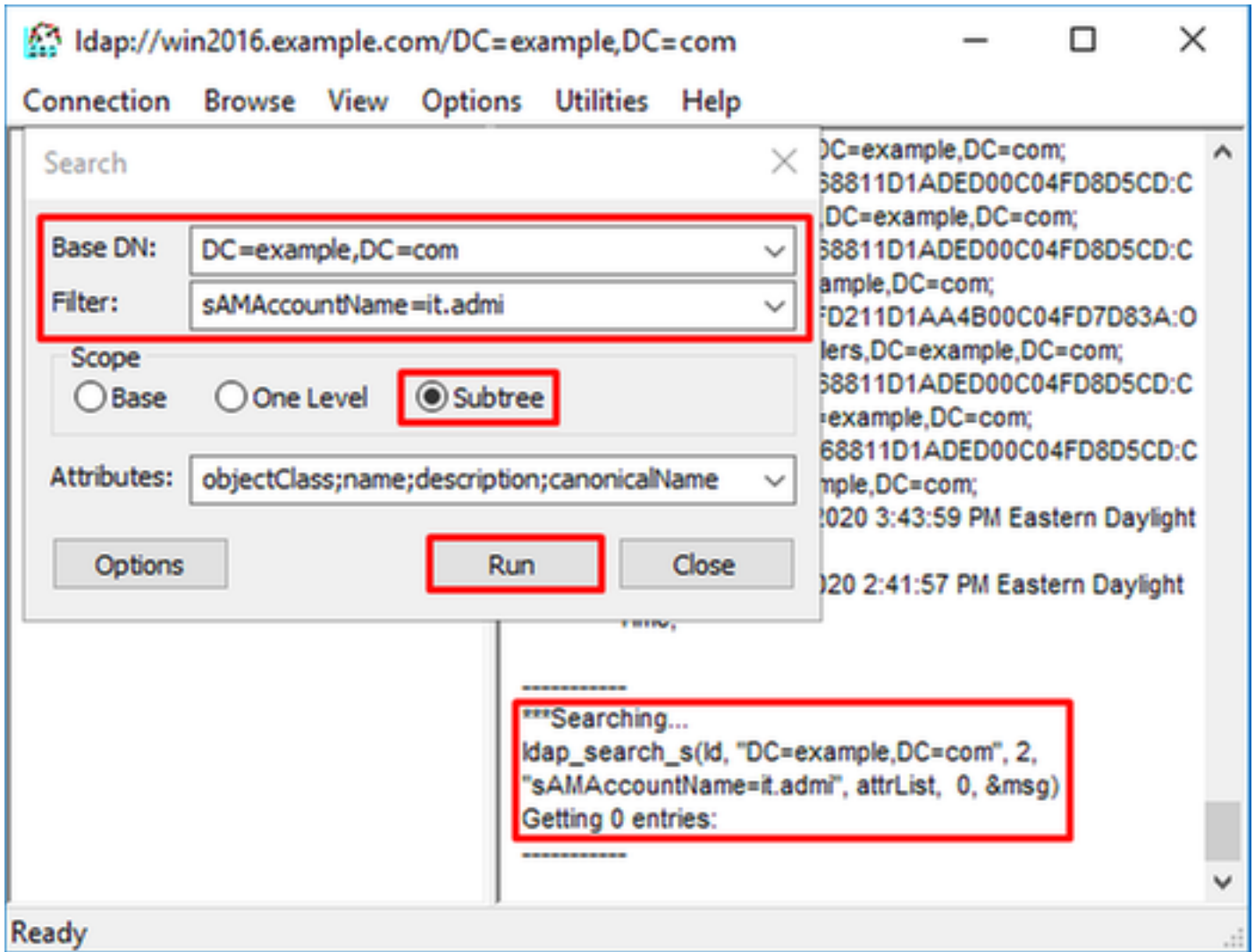
3. ベースDNを右クリックし、検索をクリックします。



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。

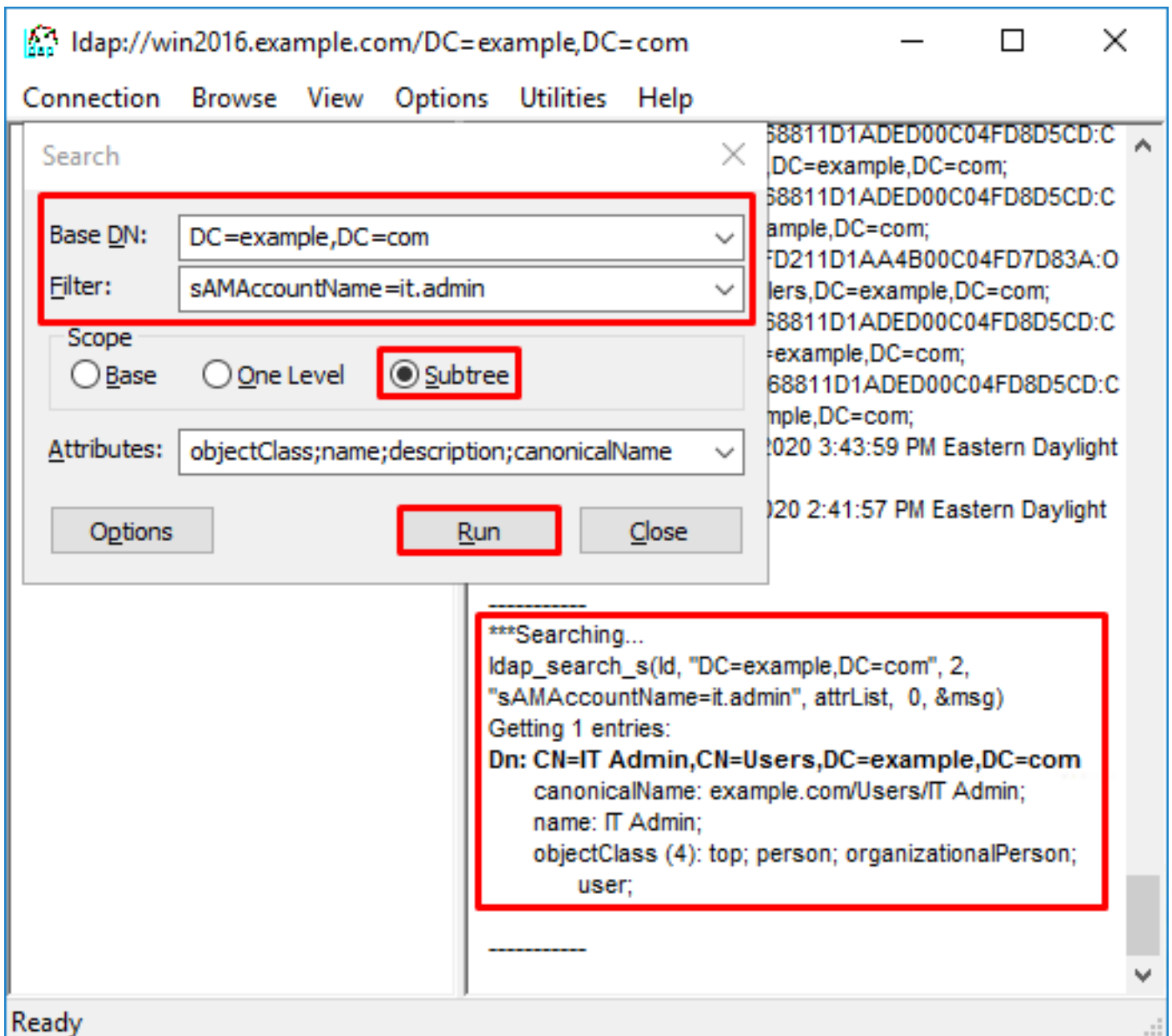
この例では、次のようになります。

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



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。



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]
      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
[-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

  1: 23:02:16.770712      192.168.1.17.61960 > 192.168.1.1.389: S 3681912834:3681912834(0) win 32768
  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
  7: 23:02:16.773428      192.168.1.17.61960 > 192.168.1.1.389: P 3681912980:3681913024(44) ack 49152
  8: 23:02:16.775030      192.168.1.1.389 > 192.168.1.17.61960: P 491522141:491522163(22) ack 3681913
  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。



Best match



Event Viewer

Desktop app

Settings



View event logs



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。