

在由FDM管理的FTD上为AnyConnect客户端配置AD(LDAP)身份验证和用户身份

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[配置](#)

[网络图和场景](#)

[AD配置](#)

[确定LDAP基础DN](#)

[创建FTD帐户](#)

[创建AD组并将用户添加到AD组 \(可选\)](#)

[复制LDAP S SSL证书根 \(仅LDAP S或STARTTLS需要\)](#)

[FDM配置](#)

[验证许可](#)

[设置AD身份源](#)

[配置AnyConnect以进行AD身份验证](#)

[启用身份策略并配置用户身份的安全策略](#)

[验证](#)

[最终配置](#)

[使用AnyConnect连接并验证访问控制策略规则](#)

[故障排除](#)

[调试](#)

[工作LDAP调试](#)

[无法与LDAP服务器建立连接](#)

[绑定登录DN和/或密码不正确](#)

[LDAP服务器找不到用户名](#)

[用户名的密码不正确](#)

[测试AAA](#)

[数据包捕获](#)

[Windows Server事件查看器日志](#)

简介

本文档旨在详细说明如何为连接到由Firepower设备管理(FDM)管理的Cisco Firepower威胁防御(FTD)的AnyConnect客户端配置Active Directory(AD)身份验证。用户身份将用于访问策略，以便将AnyConnect用户限制为特定IP地址和端口。

先决条件

要求

Cisco 建议您了解以下主题：

- FDM上RA VPN配置的基本知识
- FDM上LDAP服务器配置的基本知识
- AD的基本知识

使用的组件

本文档中的信息基于以下软件和硬件版本：

- Microsoft 2016服务器
- 运行6.5.0的FTDv

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

配置

网络图和场景



Windows服务器预配置了Internet信息服务(IIS)和远程桌面协议(RDP)，以测试用户身份。在本配置指南中，将创建三个用户帐户和两个组。

用户帐户：

- FTD管理员：此帐户将用作目录帐户，以允许FTD绑定到AD服务器。
- IT管理员：用于演示用户身份的测试管理员帐户。
- 测试用户：用于演示用户身份的测试用户帐户。

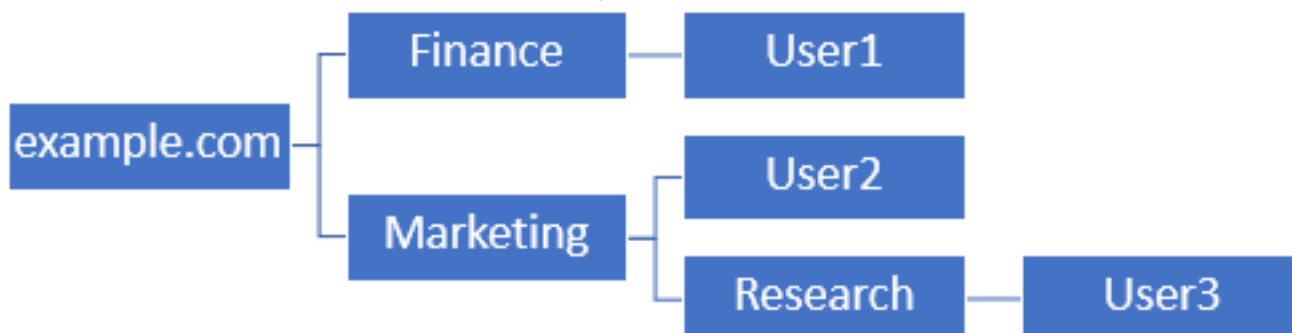
组：

- AnyConnect管理员：IT管理员将添加到的测试组，用于演示用户身份。此组将只有对Windows Server的RDP访问权限
- AnyConnect用户：将添加测试用户的测试组以演示用户身份。此组将只有对Windows Server的HTTP访问权限

AD配置

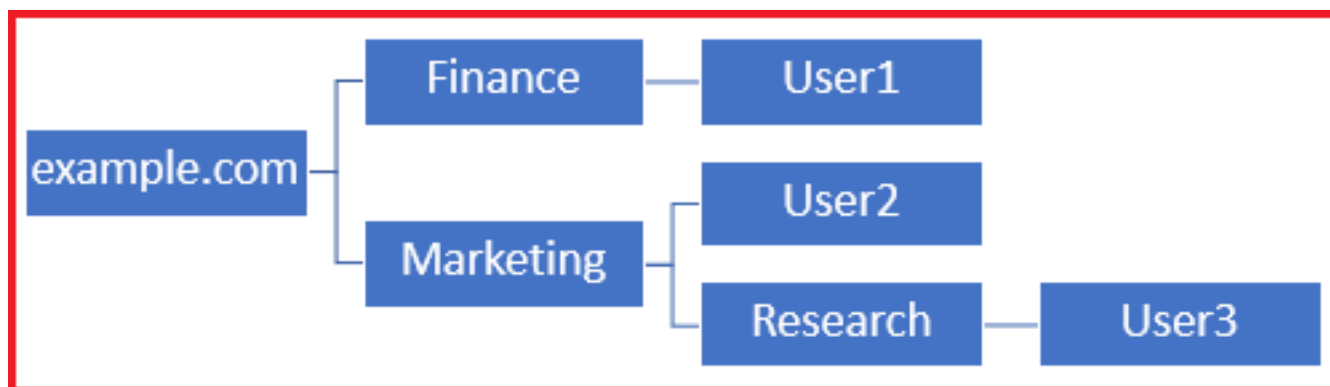
为了在FTD上正确配置AD身份验证和用户身份，需要一些值。在FDM上完成配置之前，必须在Microsoft服务器上创建或收集所有这些详细信息。主要值为：

- 域名：这是服务器的域名。在本配置指南中，example.com是域名。
- 服务器IP/FQDN地址：用于访问Microsoft服务器的IP地址或FQDN。如果使用FQDN，则必须在FDM和FTD中配置DNS服务器以解析FQDN。在本配置指南中，这些值是win2016.example.com，它解析为192.168.1.1。
- 服务器端口:LDAP服务使用的端口。默认情况下，LDAP和STARTTLS将TCP端口389用于LDAP，而LDAPS(LDAPS)将使用TCP端口636。
- 根 CA:如果使用LDAPS或STARTTLS，则需要用于对LDAPS使用的SSL证书进行签名的根CA。
- 目录用户名和密码：这是FDM和FTD用于绑定到LDAP服务器并验证用户和搜索用户和组的帐户。将为此创建名为FTD Admin的帐户。
- 基本可分辨名称(DN):基本DN是FDM的起点，FTD将告知Active Directory在搜索用户时开始。在本配置指南中，根域example.com将用作基本DN;但是，对于生产环境，在LDAP层次结构中进一步使用基础DN可能会更好。例如，以此LDAP层次结构为例：



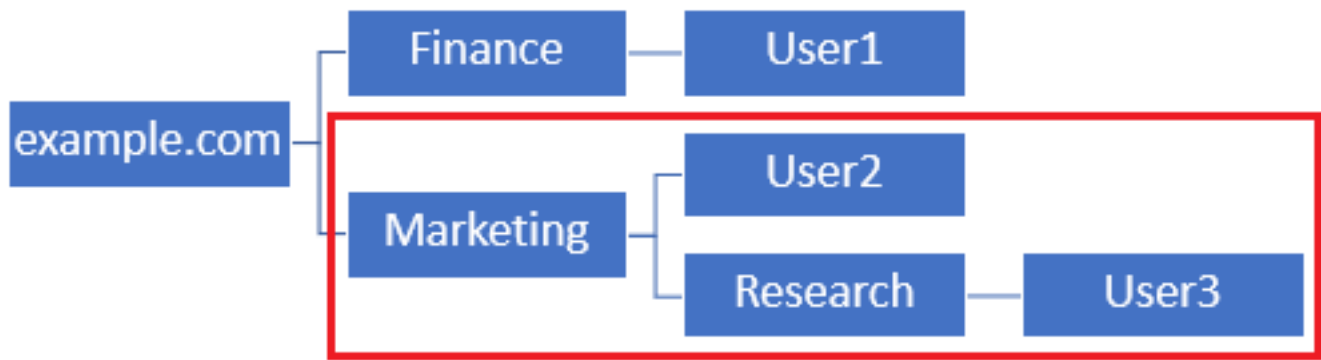
如果管理员希望营销组织单位内的用户能够对基本DN进行身份验证，则可以将其设置为根(example.com)，但这也允许财务组织单位下的用户1也登录，因为用户搜索将从根开始，并向下转到财务、营销和研究部门。

基本DN设置为example.com。



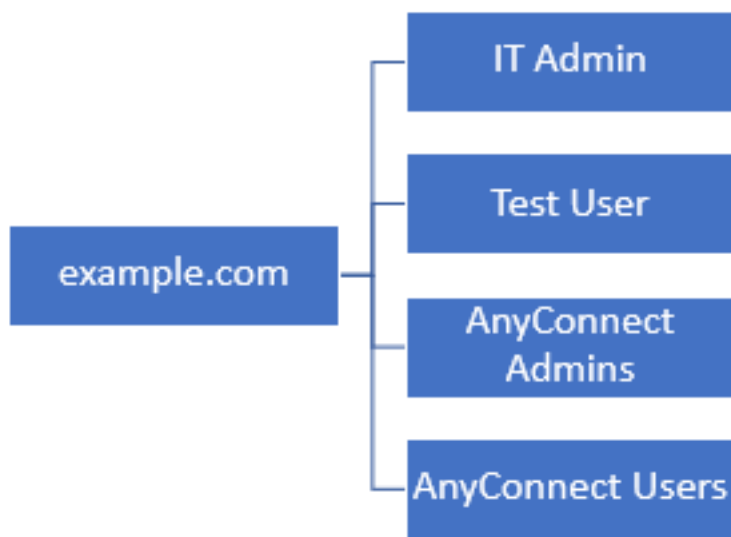
为了仅限市场营销组织单位及以下用户登录，管理员可以将基本DN设置为市场营销。现在，只有User2和User3能够进行身份验证，因为搜索将从营销部开始。

基本DN设置为“营销”：



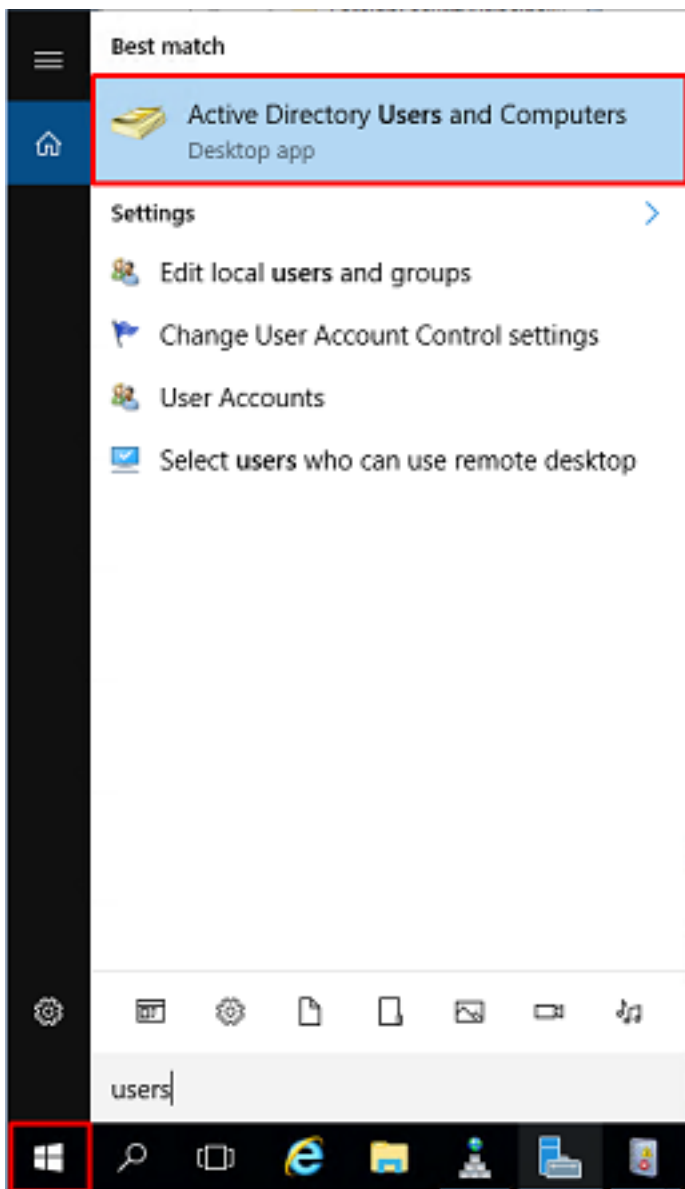
请注意，要在FTD内进行更精细的控制，允许用户根据其AD属性连接或分配不同的授权，需要配置LDAP授权映射。

此简化的LDAP层次结构在本配置指南中使用，根example.com的DN将用于基本DN。

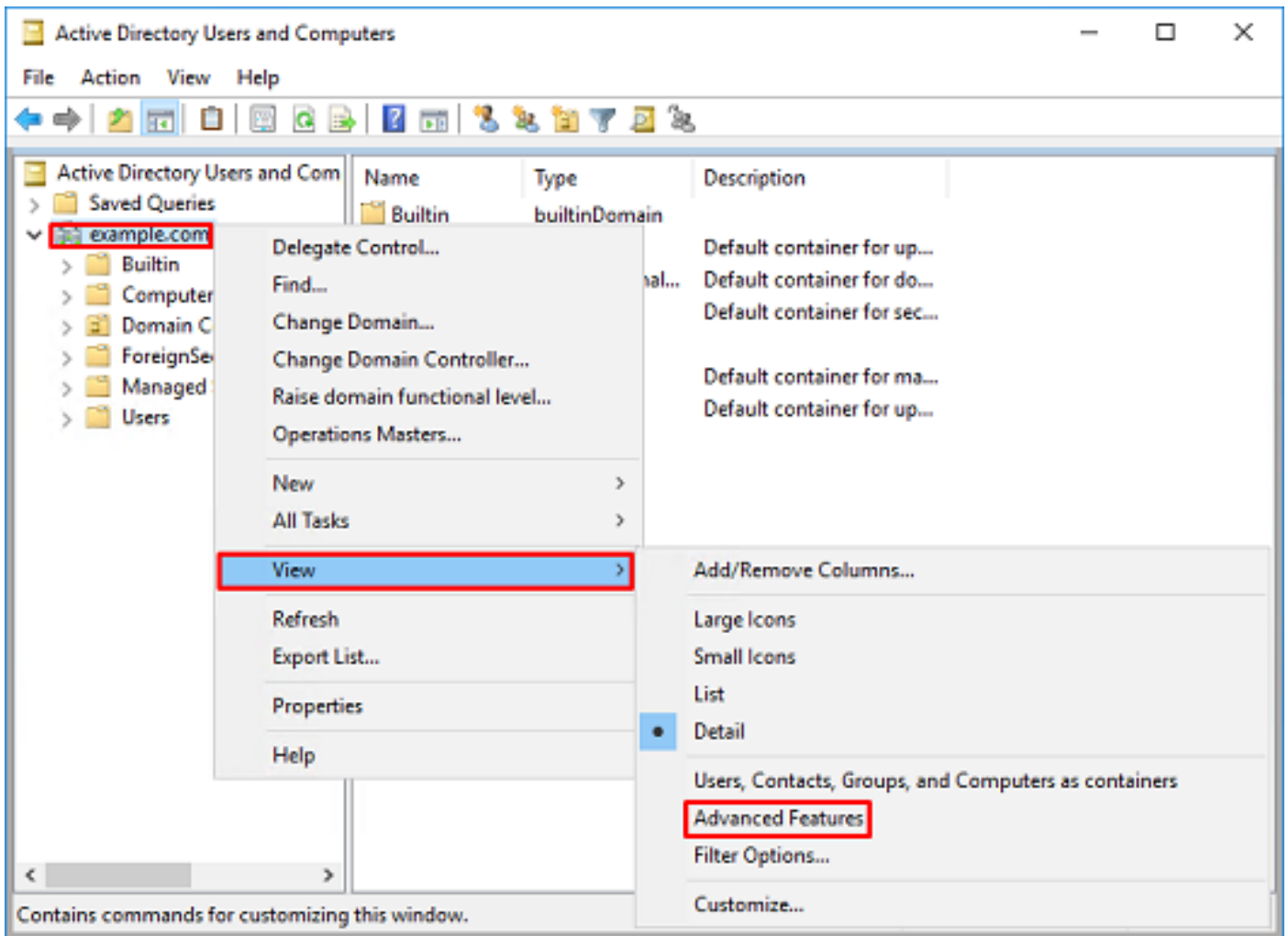


确定LDAP基础DN

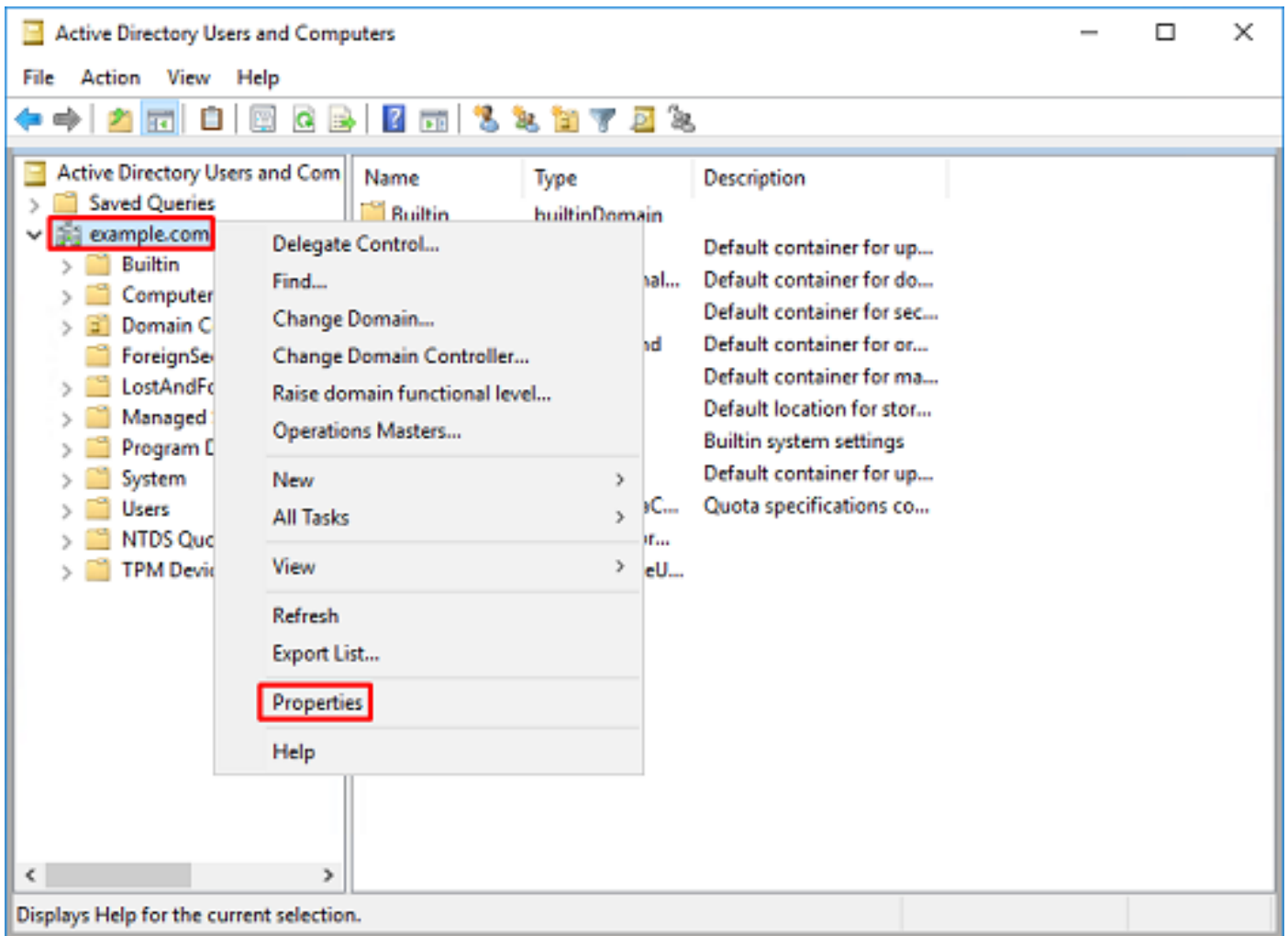
1.打开AD用户和计算机。



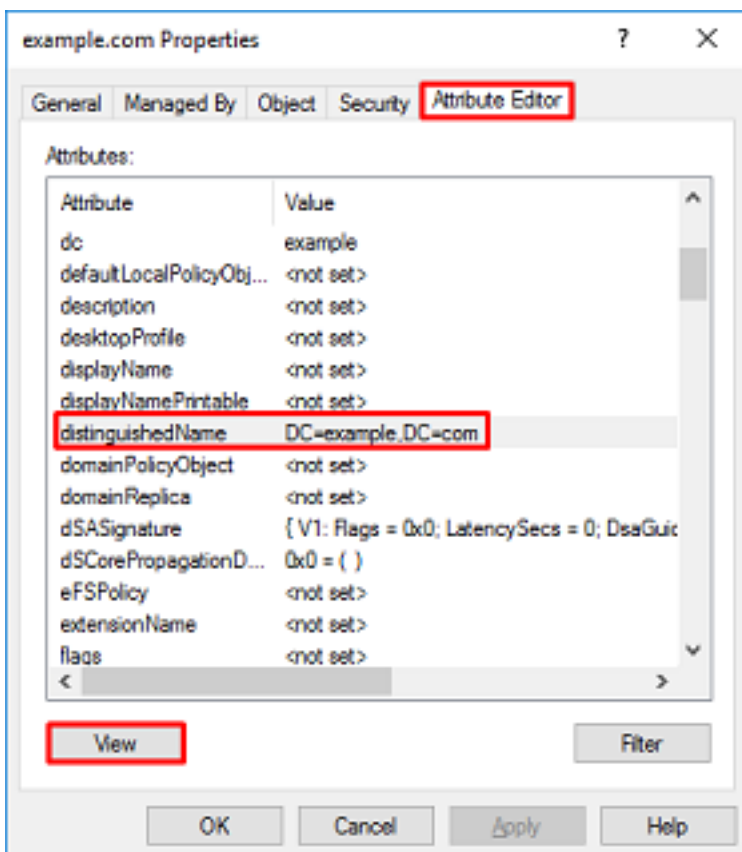
2.左键单击根域（以打开容器），右键单击根域，然后导航到“查看”并单击“高级功能”。



3.这将启用AD对象下其他属性的视图。例如，要查找根example.com的DN，请右键单击example.com，然后导航到“属性”。

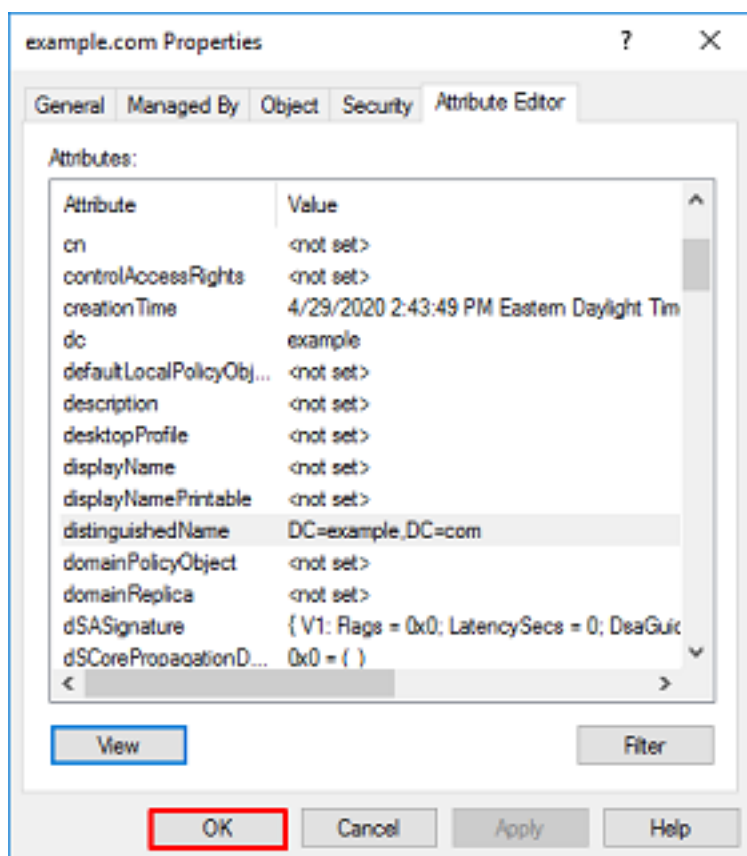
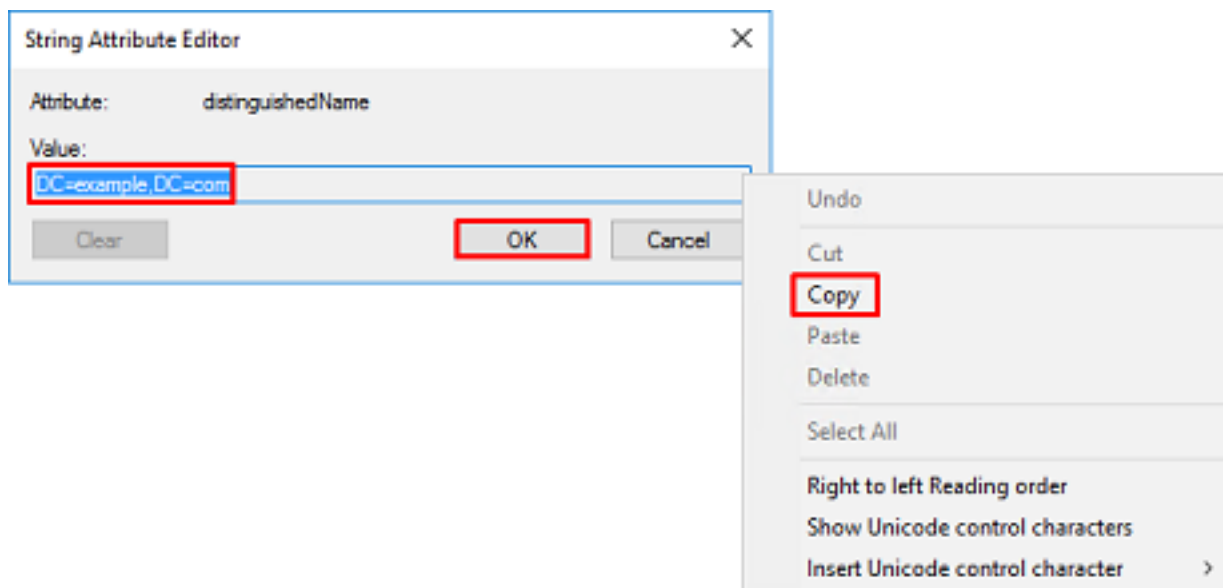


4.在“属性”下，单击“属性编辑器”选项卡。在“属性”下查找distinguishedName，然后单击“查看”。

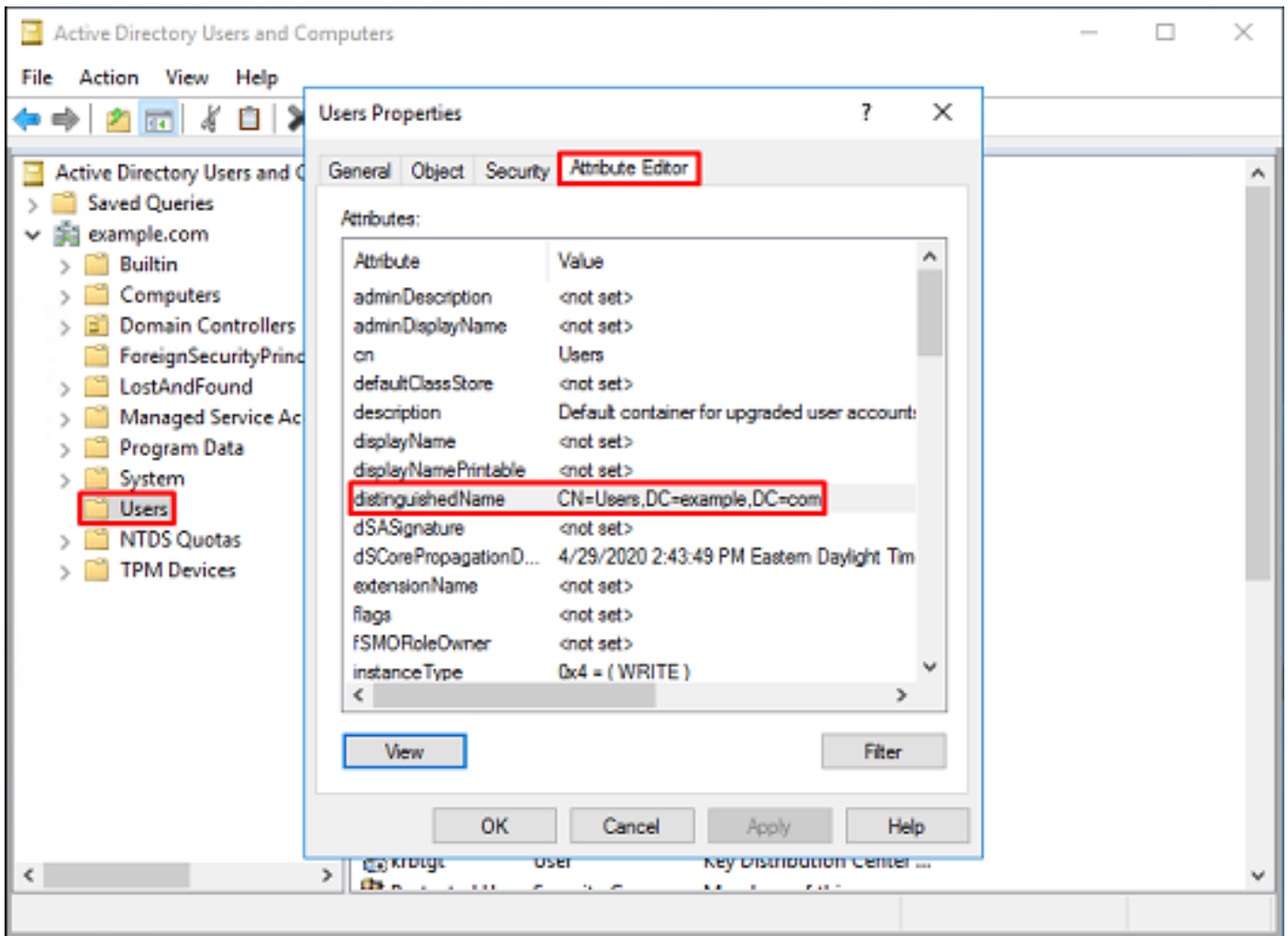


5.这将打开一个新窗口，在该窗口中，DN可以复制并粘贴到FDM中。在本例中，根DN为

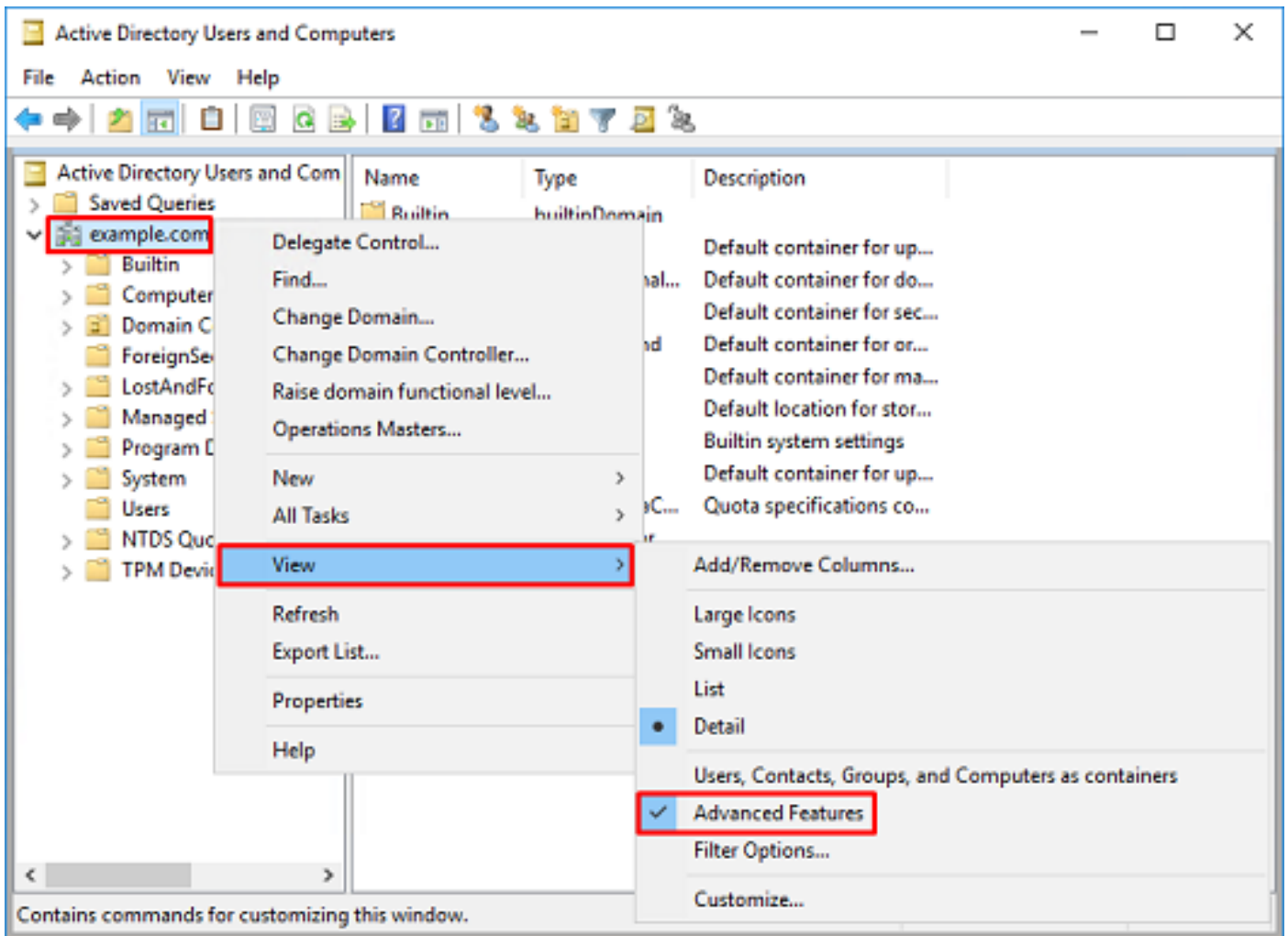
DC=example, DC=com。复制值。单击OK以退出“字符串属性编辑器”窗口，然后再次单击OK以退出“属性”。



这可以针对AD中的多个对象执行。例如，以下步骤用于查找用户容器的DN:



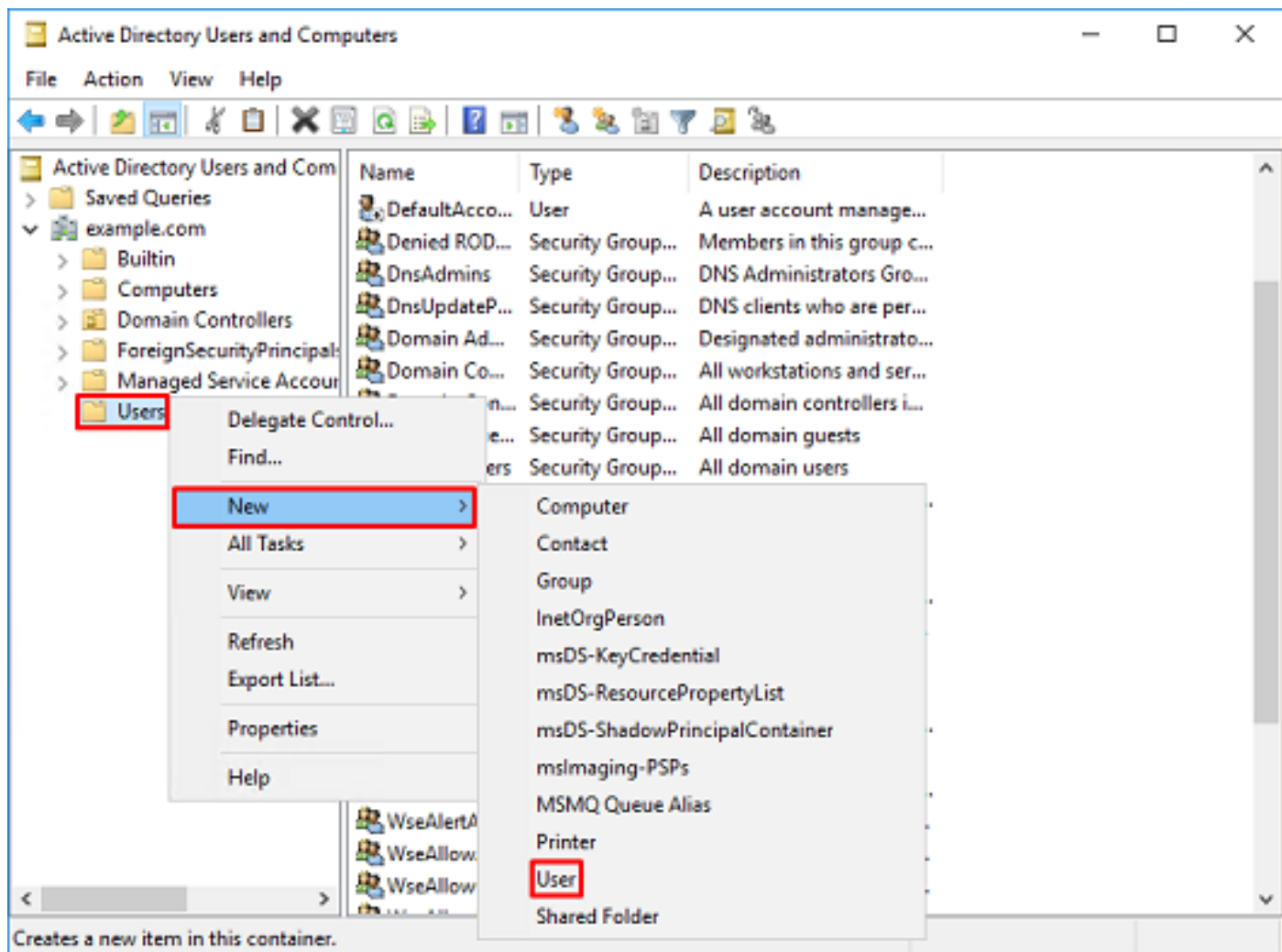
6. 可以删除“高级功能”视图。右键单击根DN，导航至“View (查看)”，然后再次单击“Advanced Features(高级功能)”。



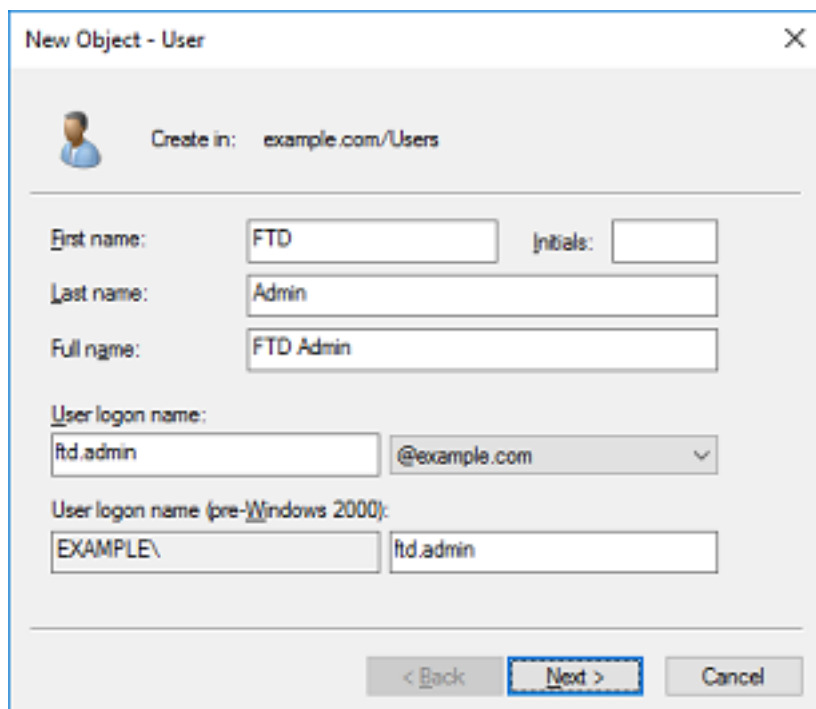
创建FTD帐户

此用户帐户将允许FDM和FTD与AD绑定，以搜索用户和组并对其进行身份验证。创建单独的FTD帐户的目的是防止在用于绑定的凭证受到侵害时未经授权访问网络中的其他位置。此帐户不必在基本DN的范围内。

1.在Active Directory**用户和计算机**中，右键单击将添加FTD帐户的容器/组织。在此配置中，FTD帐户将添加到用户名ftd.admin@example.com下的“用户”(Users)容器下。右键单击“用户”，然后单击“新建”>“用户”。



2.浏览“新建对象 — 用户向导”。



New Object - User

Create in: example.com/Users

Password:

Confirm password:

User must change password at next logon

User cannot change password

Password never expires

Account is disabled

< Back Next > Cancel

New Object - User

Create in: example.com/Users

When you click Finish, the following object will be created:

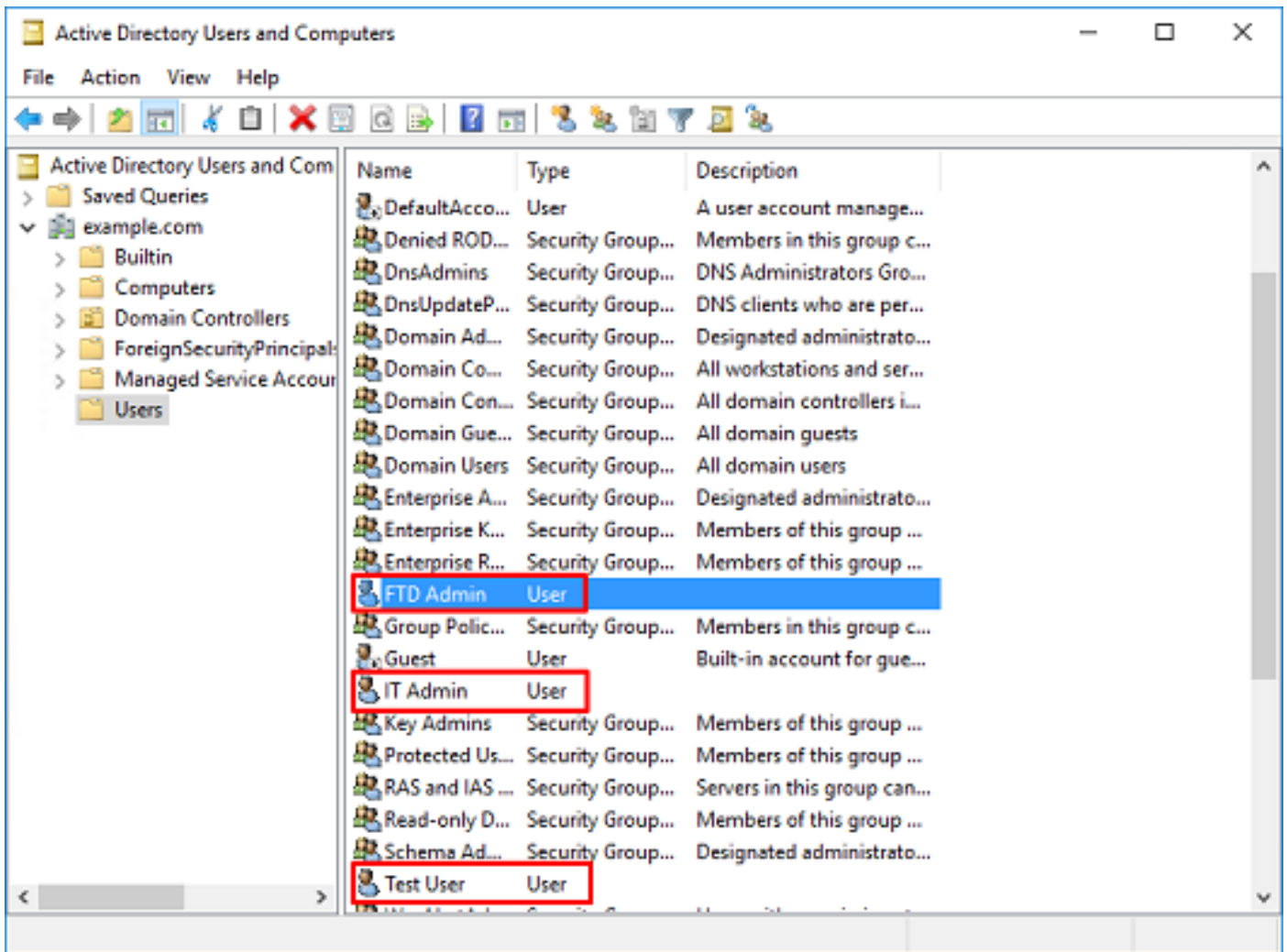
Full name: FTD Admin

User logon name: ftd.admin@example.com

The password never expires.

< Back Finish Cancel

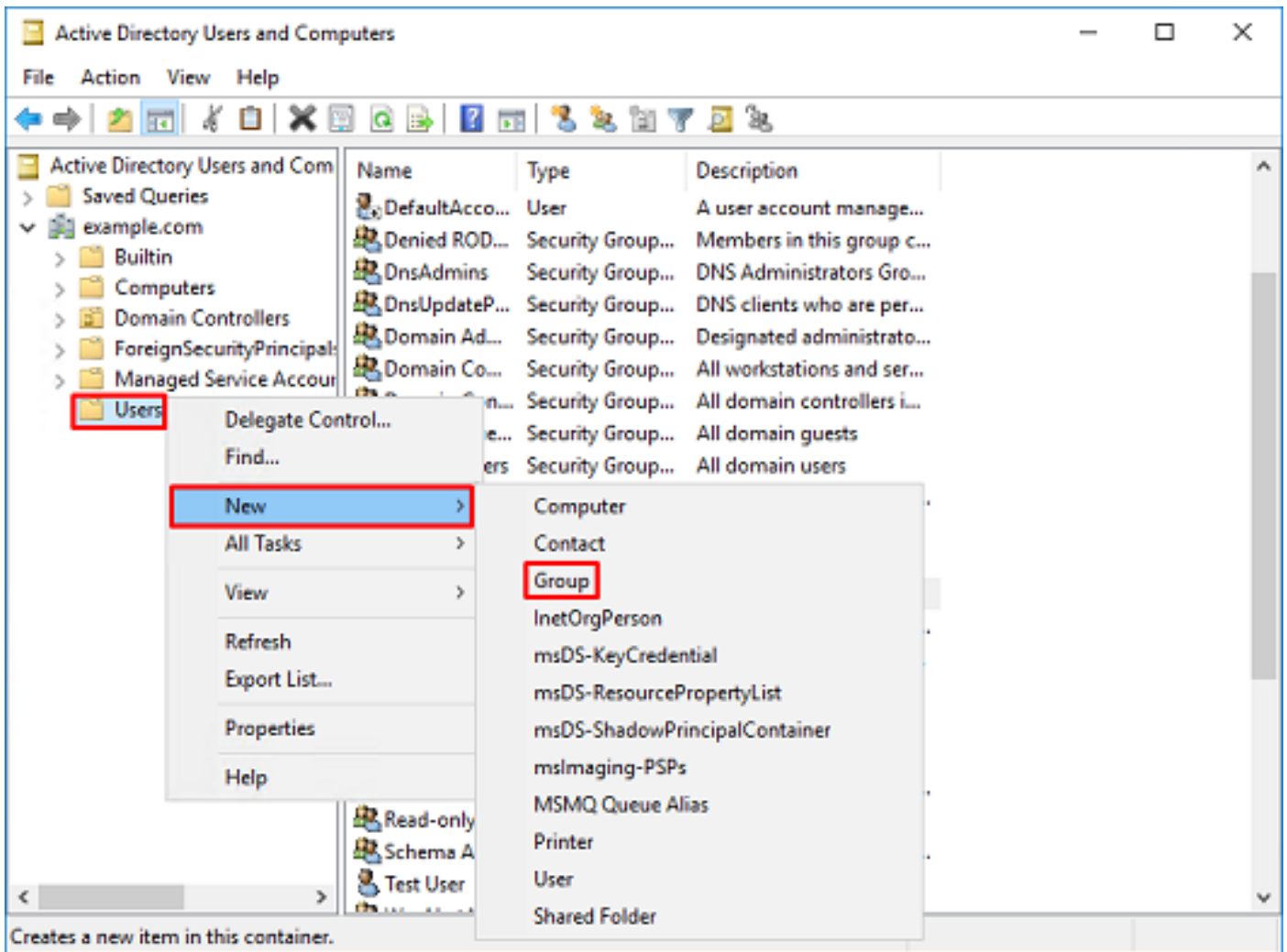
3. 确认已创建FTD帐户。此外，还创建了另外两个帐户，即**IT管理员**和**测试用户**。



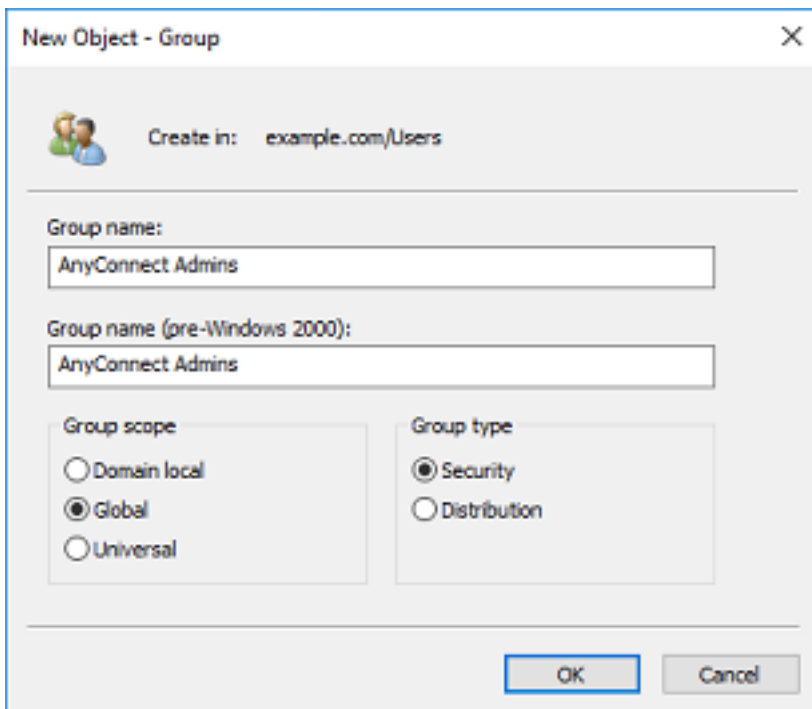
创建AD组并将用户添加到AD组（可选）

虽然身份验证不需要，但可以使用组来简化对多个用户应用访问策略以及LDAP授权的操作。在本配置指南中，组将用于稍后通过FDM中的用户身份应用访问控制策略设置。

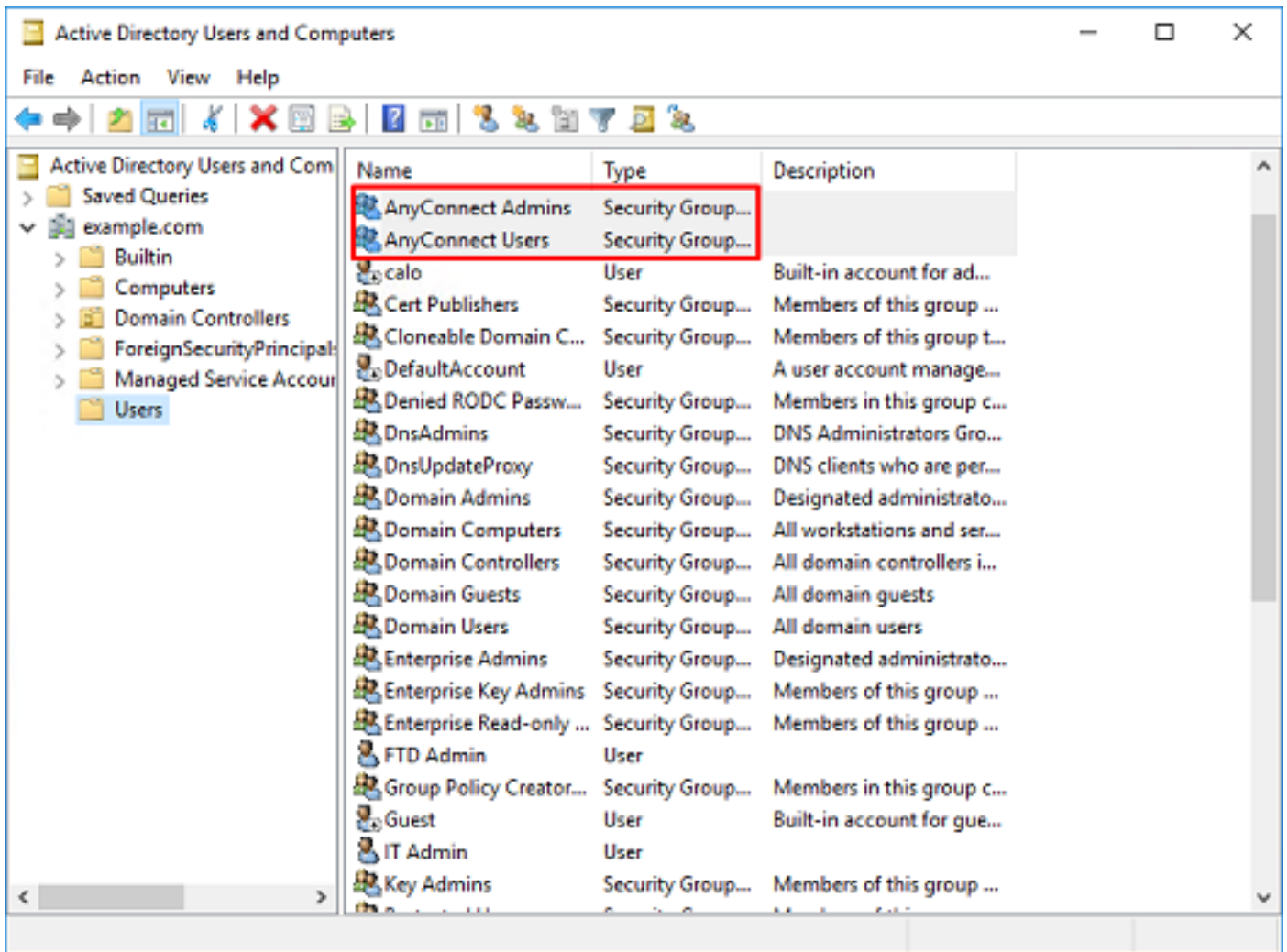
1. 在Active Directory用户和计算机中，右键单击要添加新组的容器/组织。在本示例中，组AnyConnect Admins将添加到“用户”容器下。右键单击“用户”，然后单击“新建”>“组”。



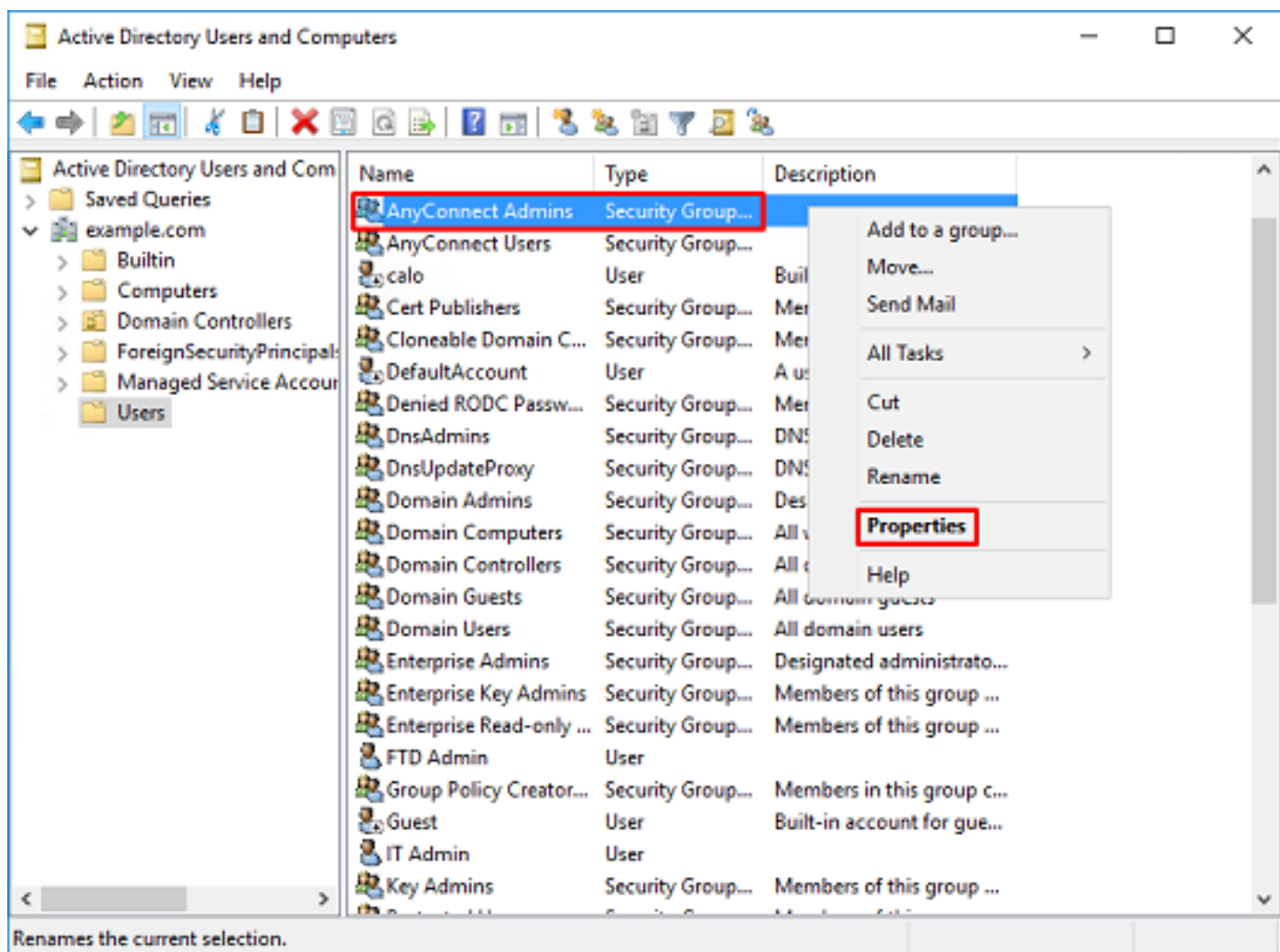
2.浏览“新建对象 — 组向导”，如图所示。



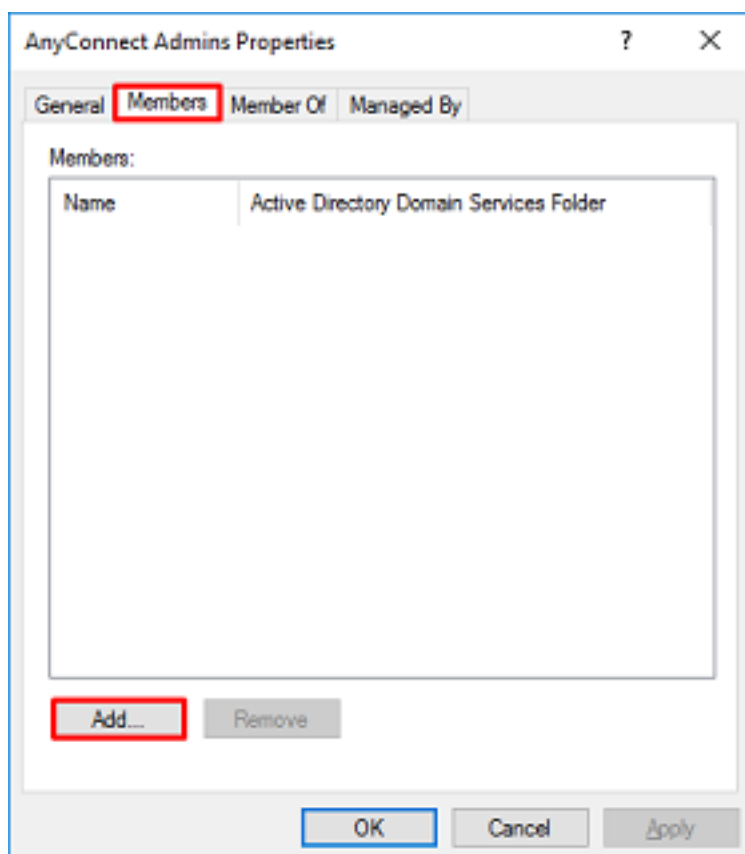
3.检验组是否已创建。还创建了AnyConnect用户组。



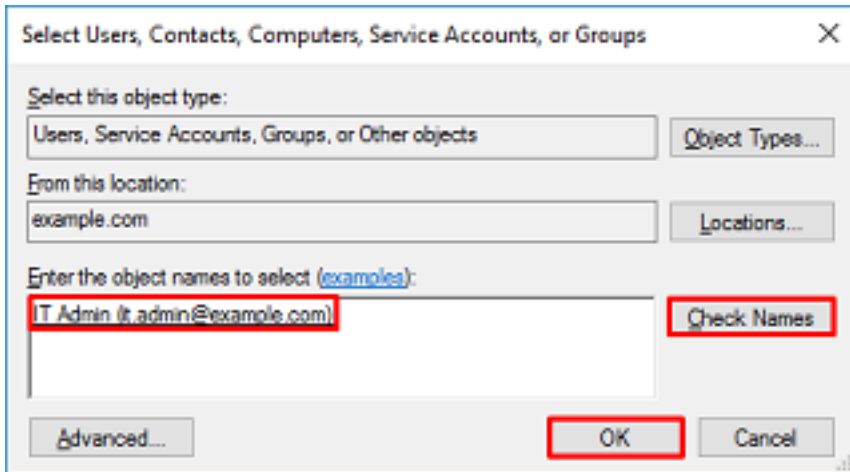
4. 右键单击要添加用户的组，然后选择“属性”。在此配置中，用户IT管理员将添加到组AnyConnect Admins，并且用户测试用户将添加到组AnyConnect Users中。



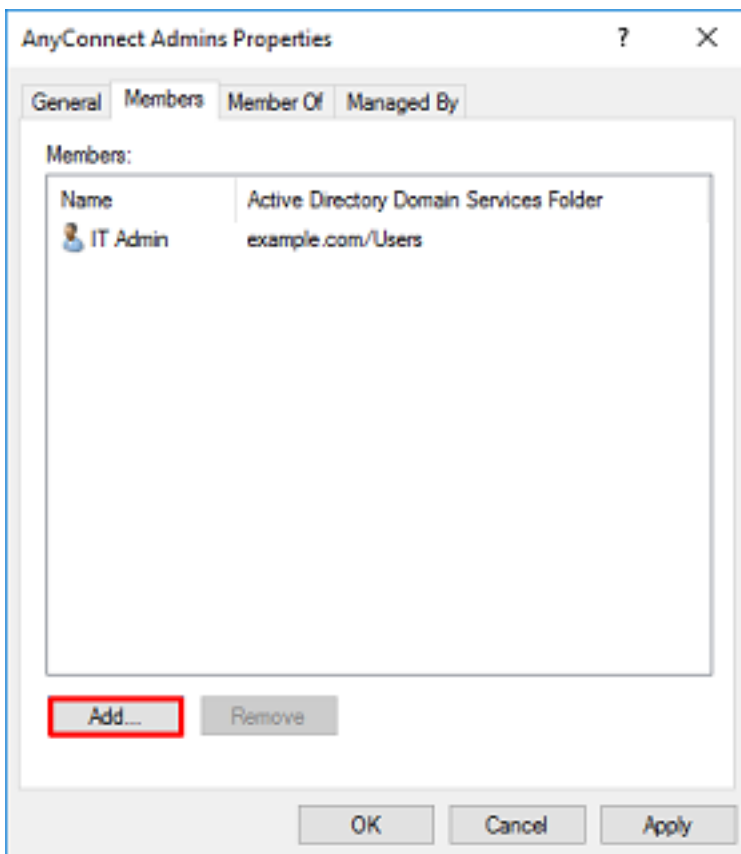
5.单击“成员”选项卡，然后单击“添加”，如图所示。



在字段中输入用户，然后单击“Check Names(检查名称)”按钮以验证是否找到该用户。验证后，单击OK。

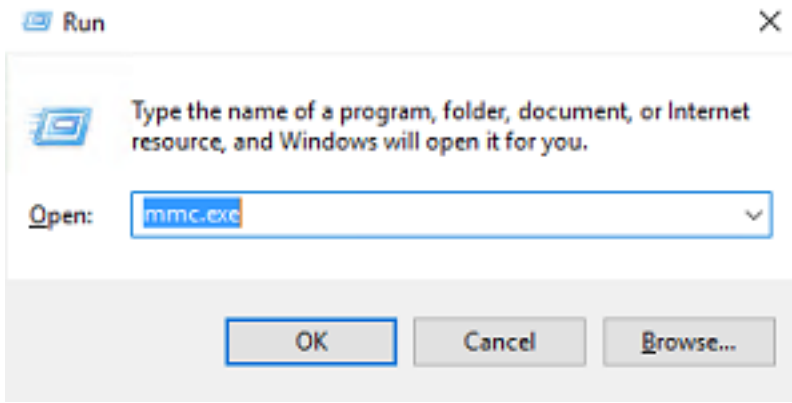


验证是否添加了正确的用户，然后单击“确定”按钮。用户测试用户也会使用相同的步骤添加到AnyConnect用户组。

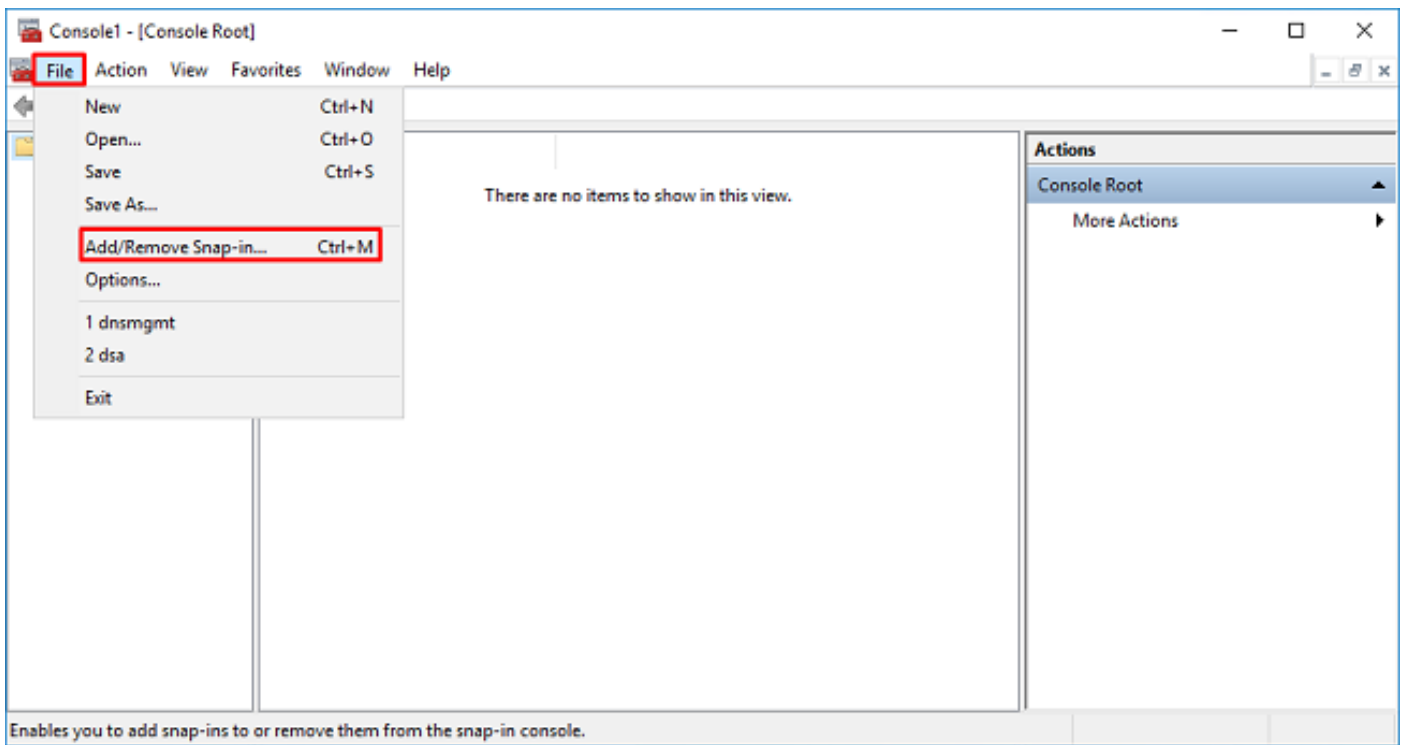


复制LDAPS SSL证书根（仅LDAPS或STARTTLS需要）

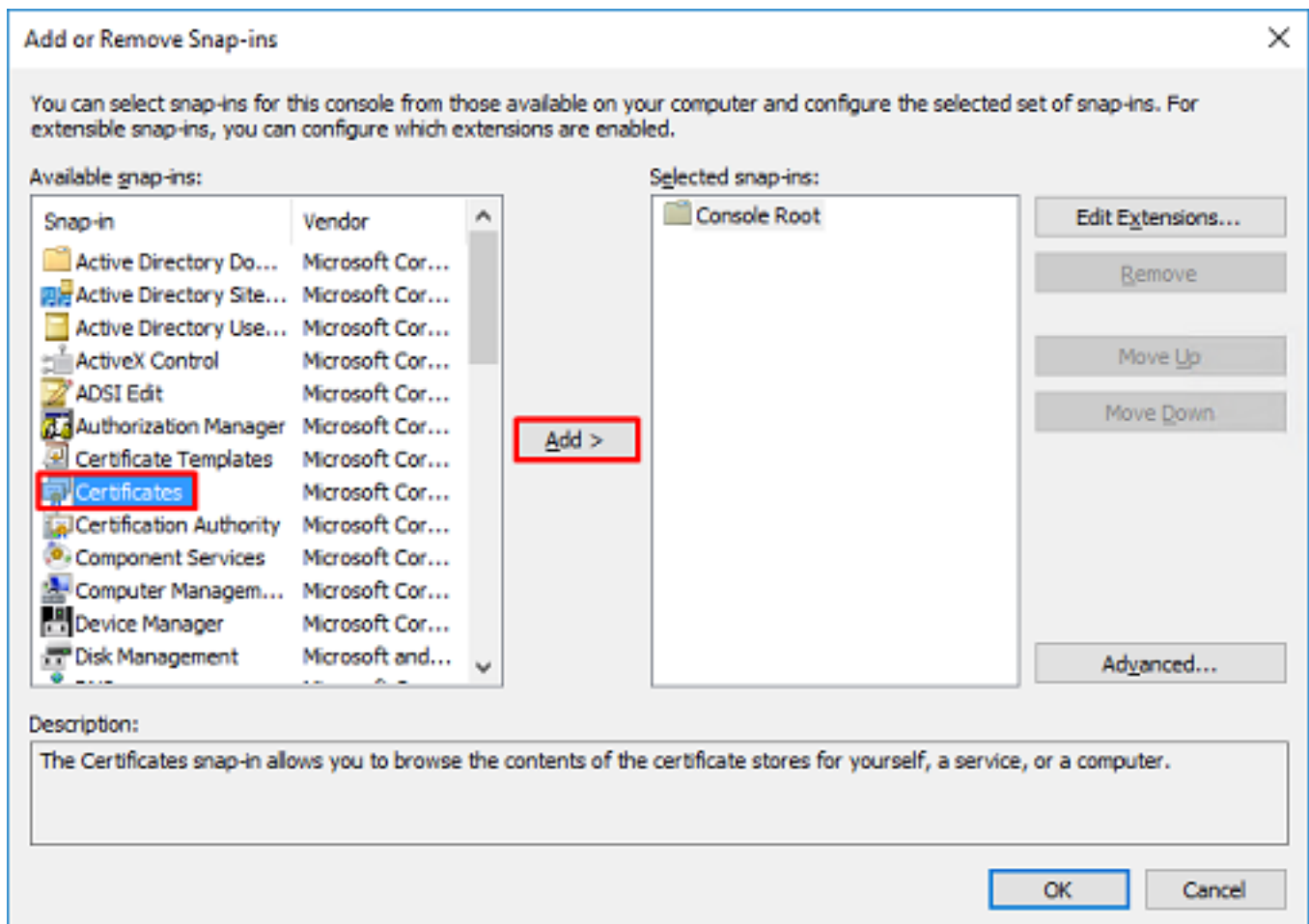
1.按Win+R键并键入mmc.exe。Click OK.



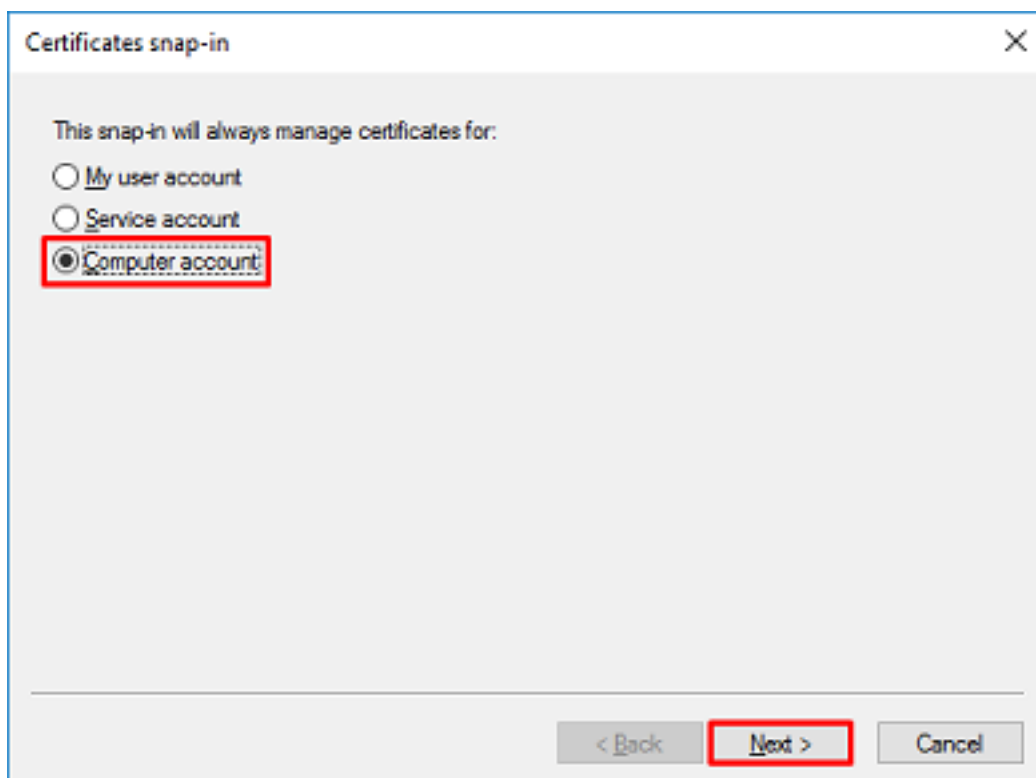
2. 导航至“文件”>“添加/删除管理单元.....” 如图所示.



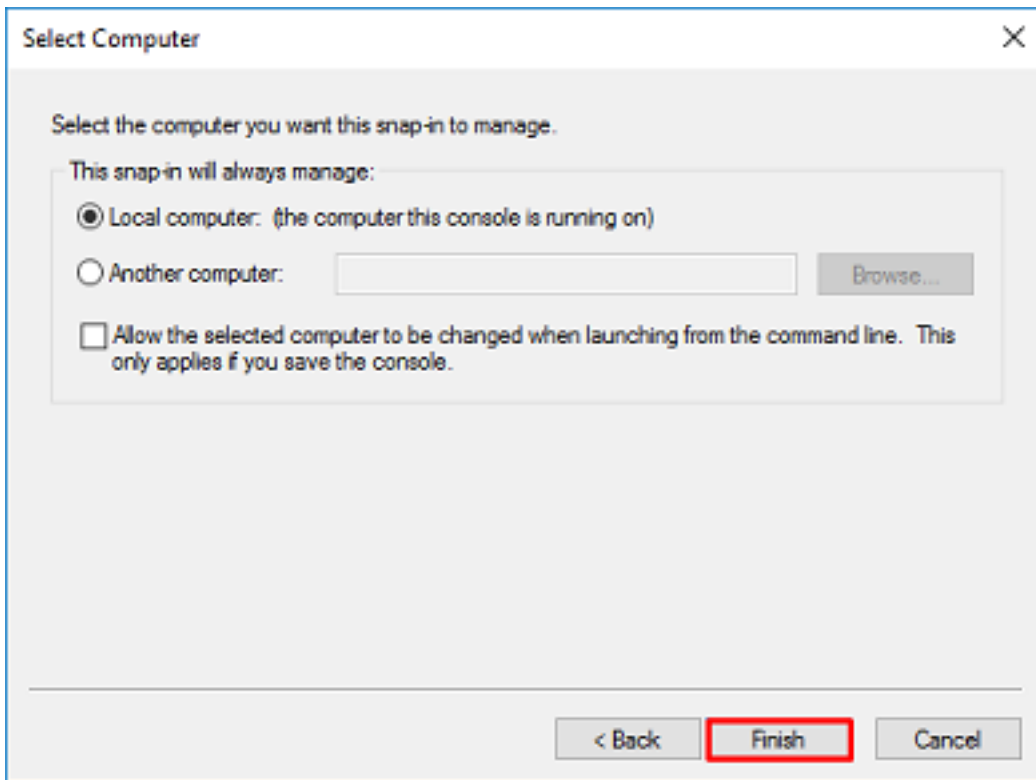
3. 在可用管理单元下，单击“证书”，然后单击“添加”。



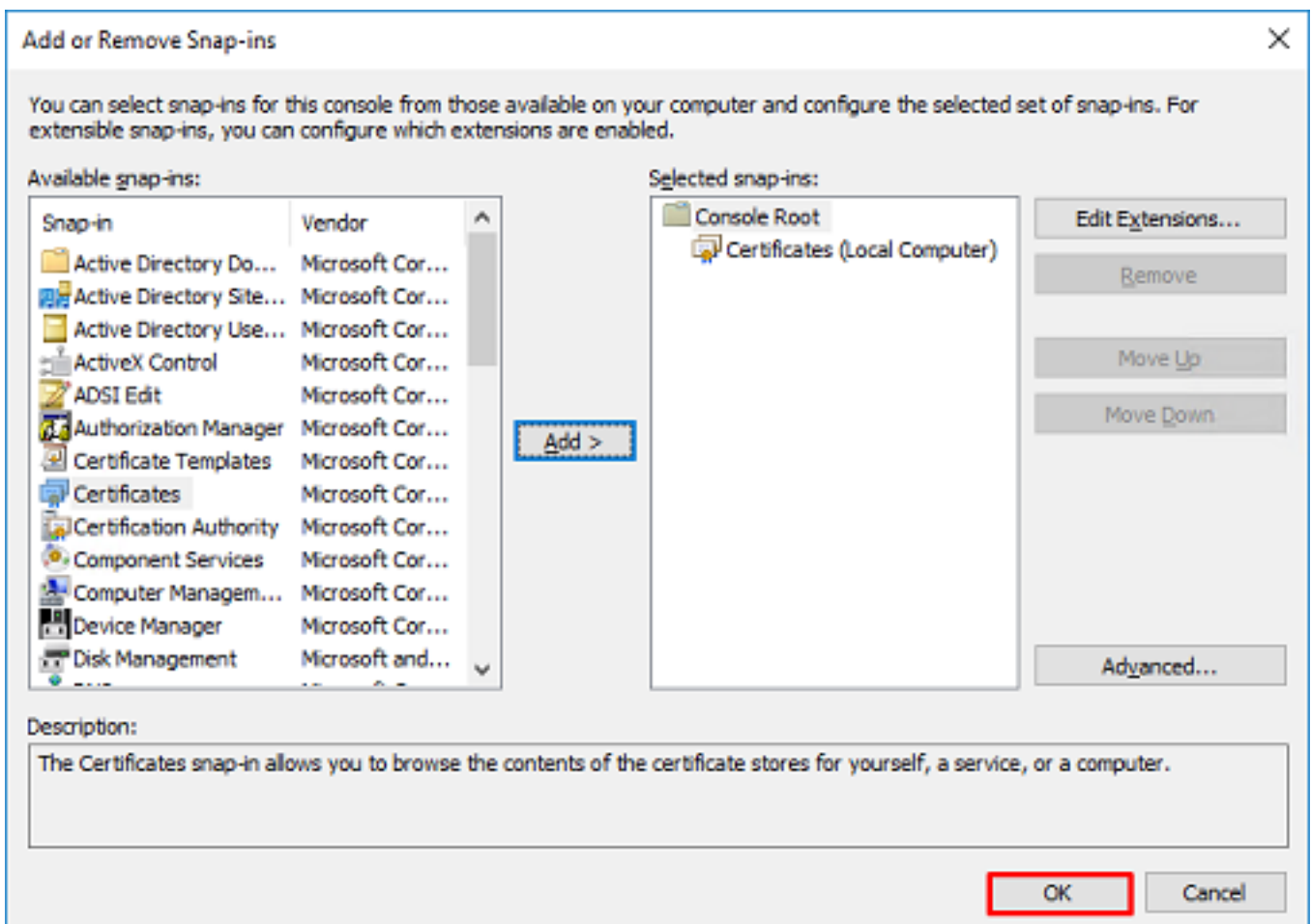
4. 选择“计算机帐户”，然后单击“下一步”，如图所示。



单击 完成。



5.单击“确定”。

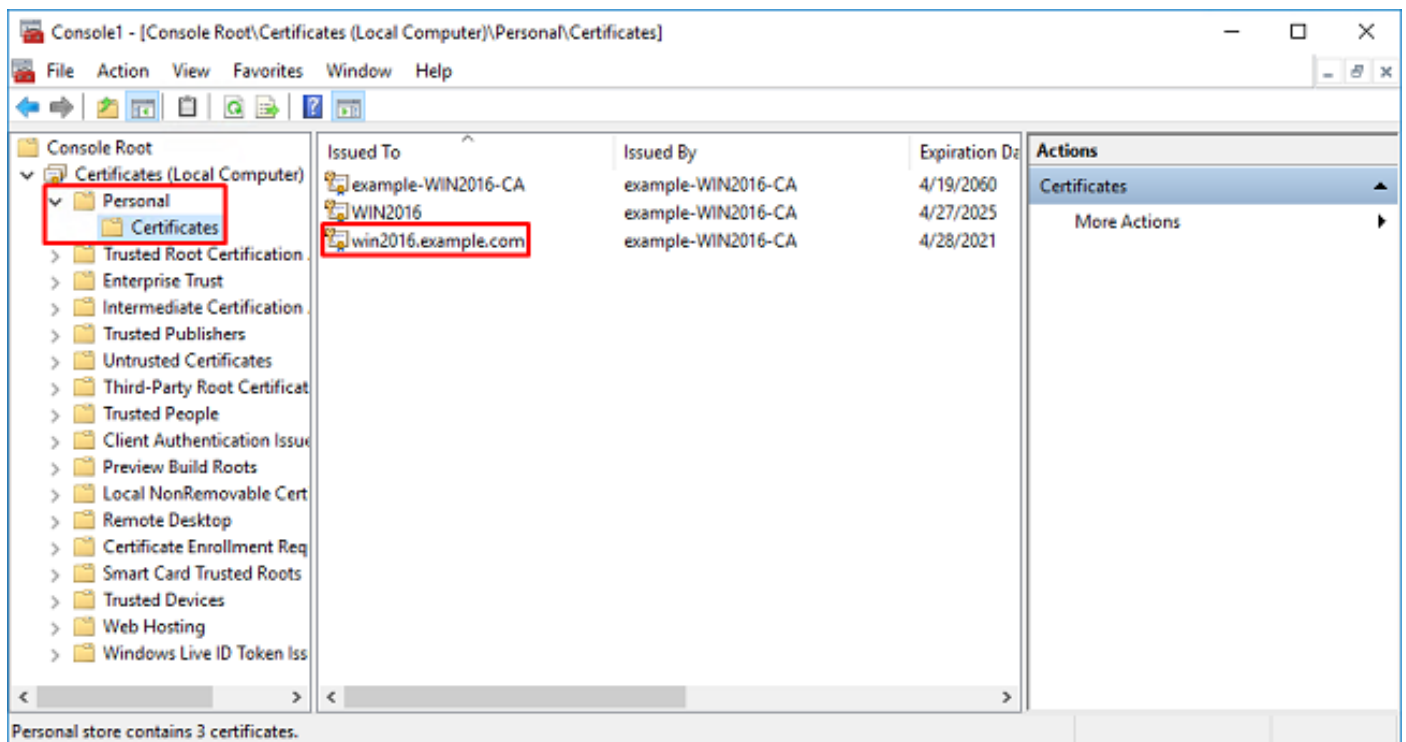


6.展开“个人”文件夹，然后单击“证书”。LDAPs使用的证书应颁发给Windows服务器的完全限定域名(FQDN)。在此服务器上，列出了3个证书。

- 颁发给WIN2016-CA的CA证书和由WIN2016-CA颁发的CA证书。

- 由example-WIN2016-CA颁发给WIN2016的身份证书。
- 由example-WIN2016-CA颁发给win2016.example.com的身份证书。

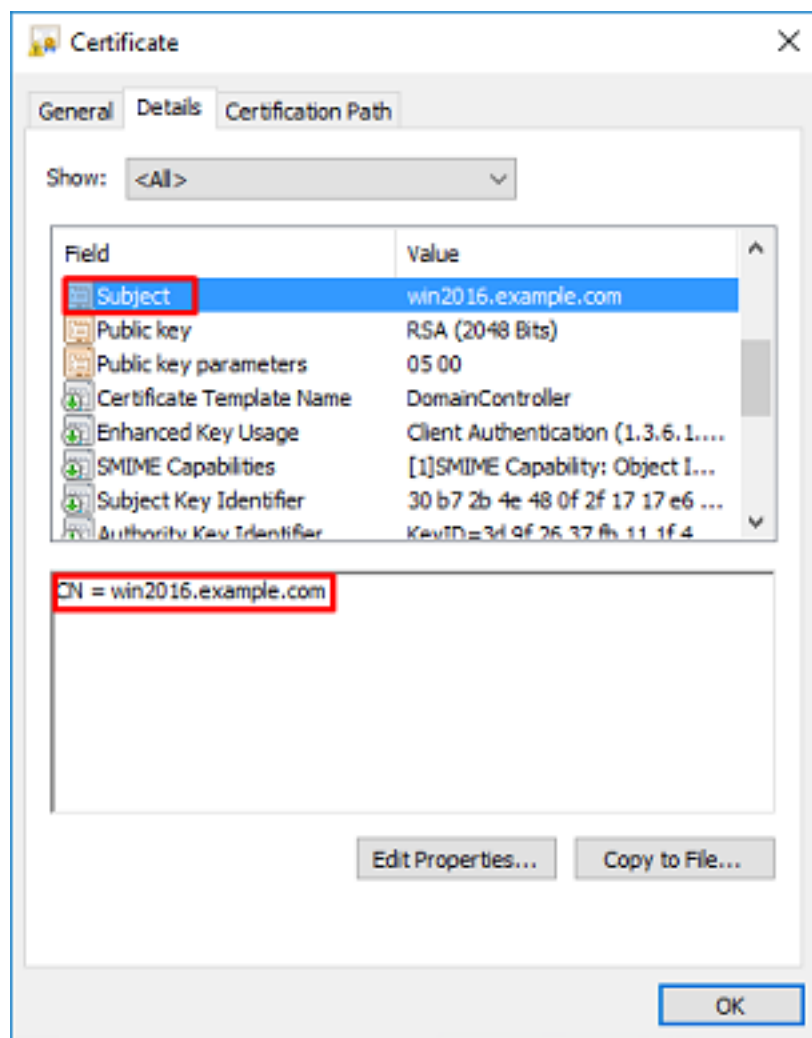
在本配置指南中，FQDN为win2016.example.com，因此前2个证书无效，无法用作LDAPS SSL证书。颁发给win2016.example.com的身份证书是Windows Server CA服务自动颁发的证书。双击证书以检查详细信息。

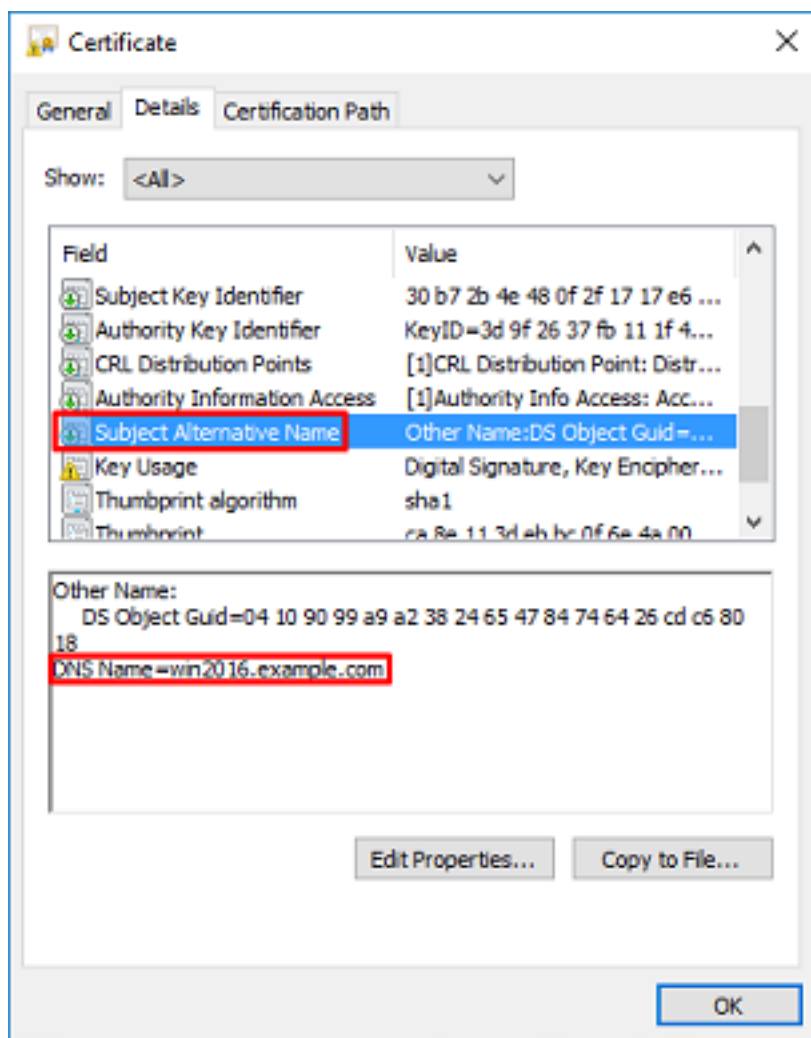


7.要用作LDAPS SSL证书，证书必须满足以下要求：

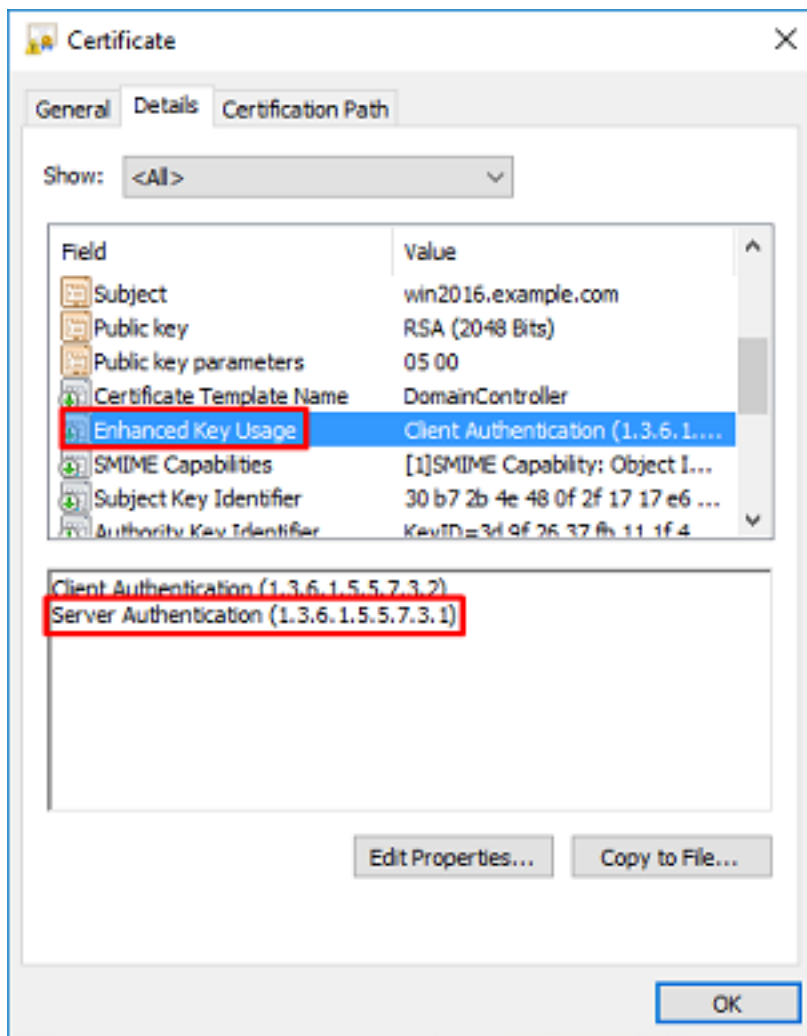
- 公用名或DNS使用者备用名与Windows Server的FQDN匹配。
- 证书在Enhanced Key Usage字段下具有Server Authentication。

在证书的Details选项卡下，在Subject和Subject Alternative Name下，FQDN win2016.example.com出现。

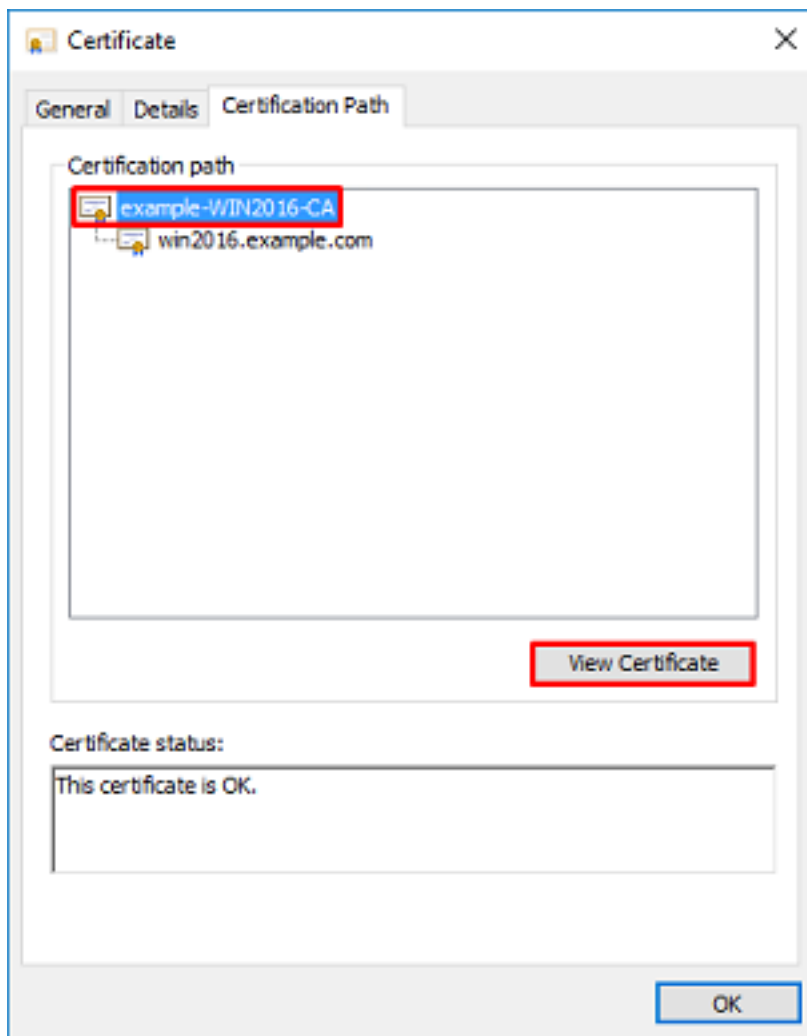




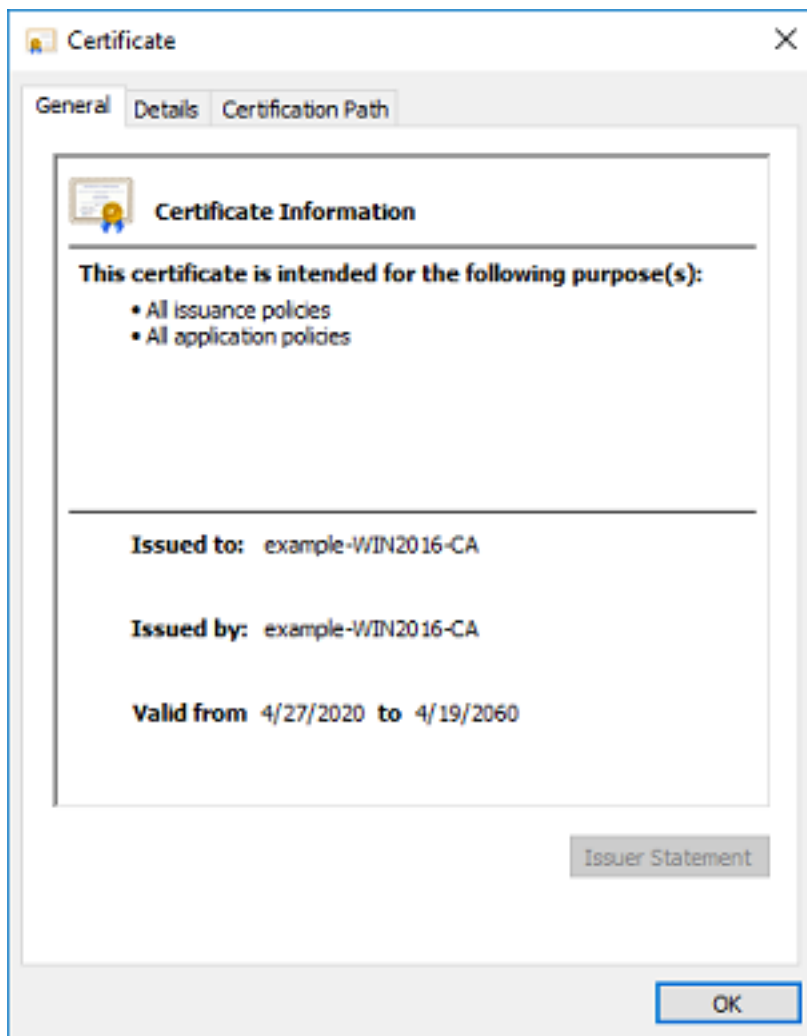
在“增强的密钥使用”下，出现“服务器身份验证”。



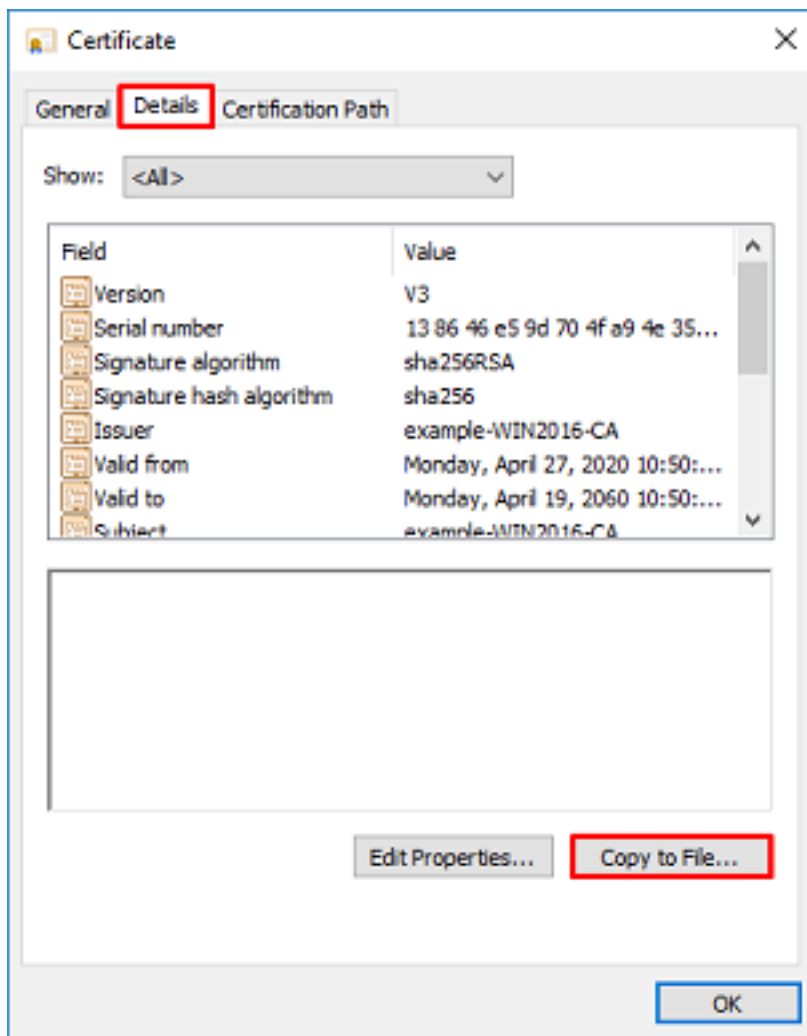
8.确认后，导航至“认证路径”选项卡。单击应是根CA证书的顶级证书，然后单击“查看证书”按钮。



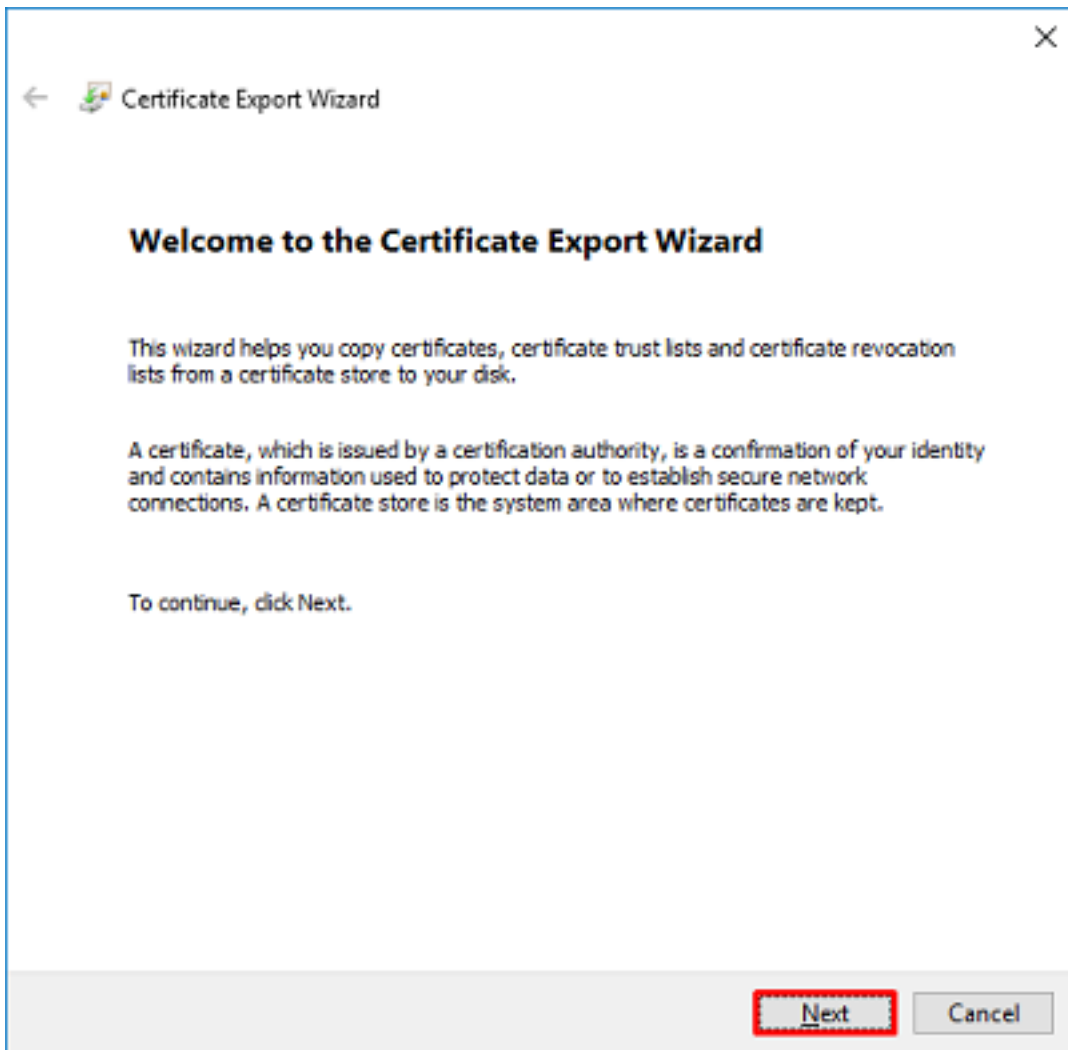
9.这将打开根CA证书的证书详细信息。



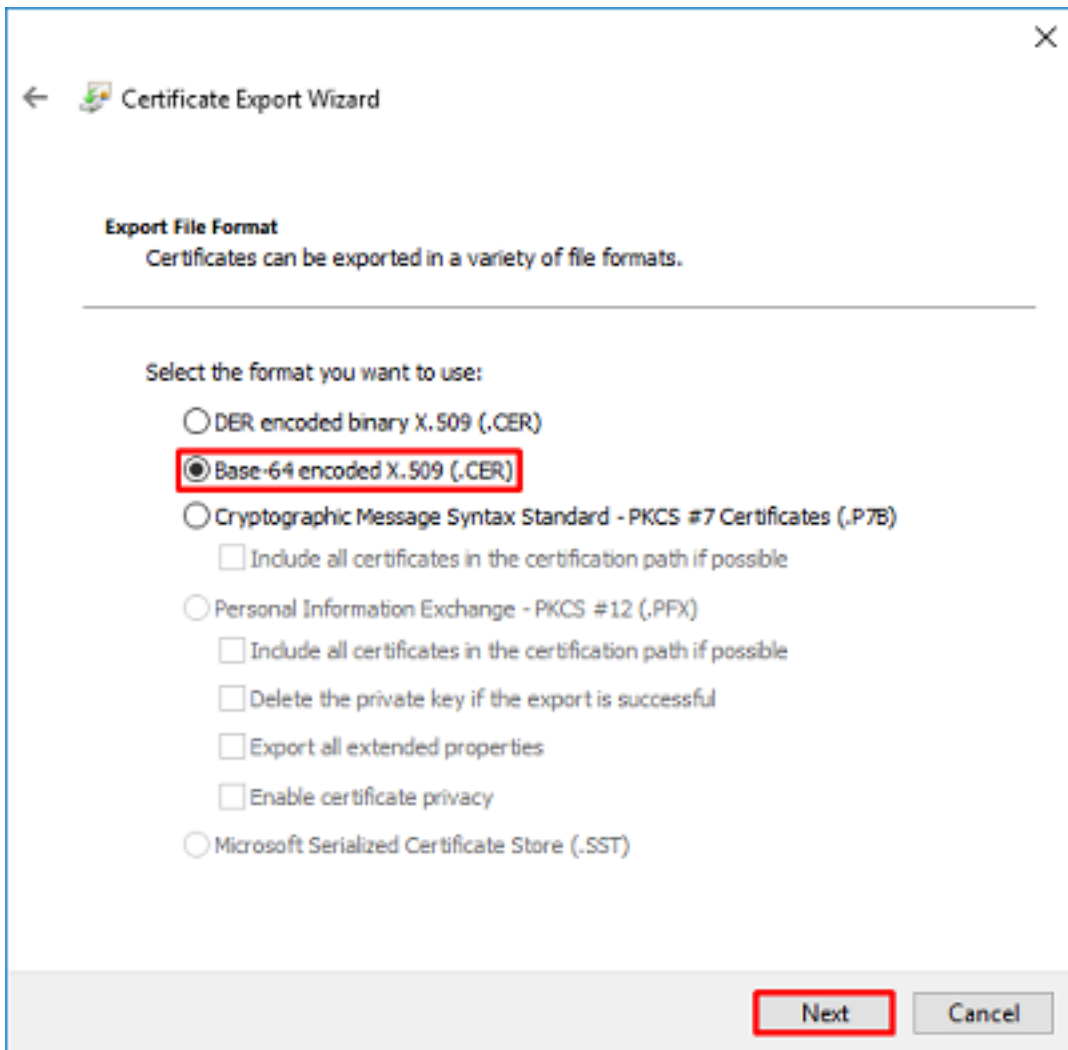
10. 打开“详细信息”选项卡，然后单击“复制到文件……” 如图所示。



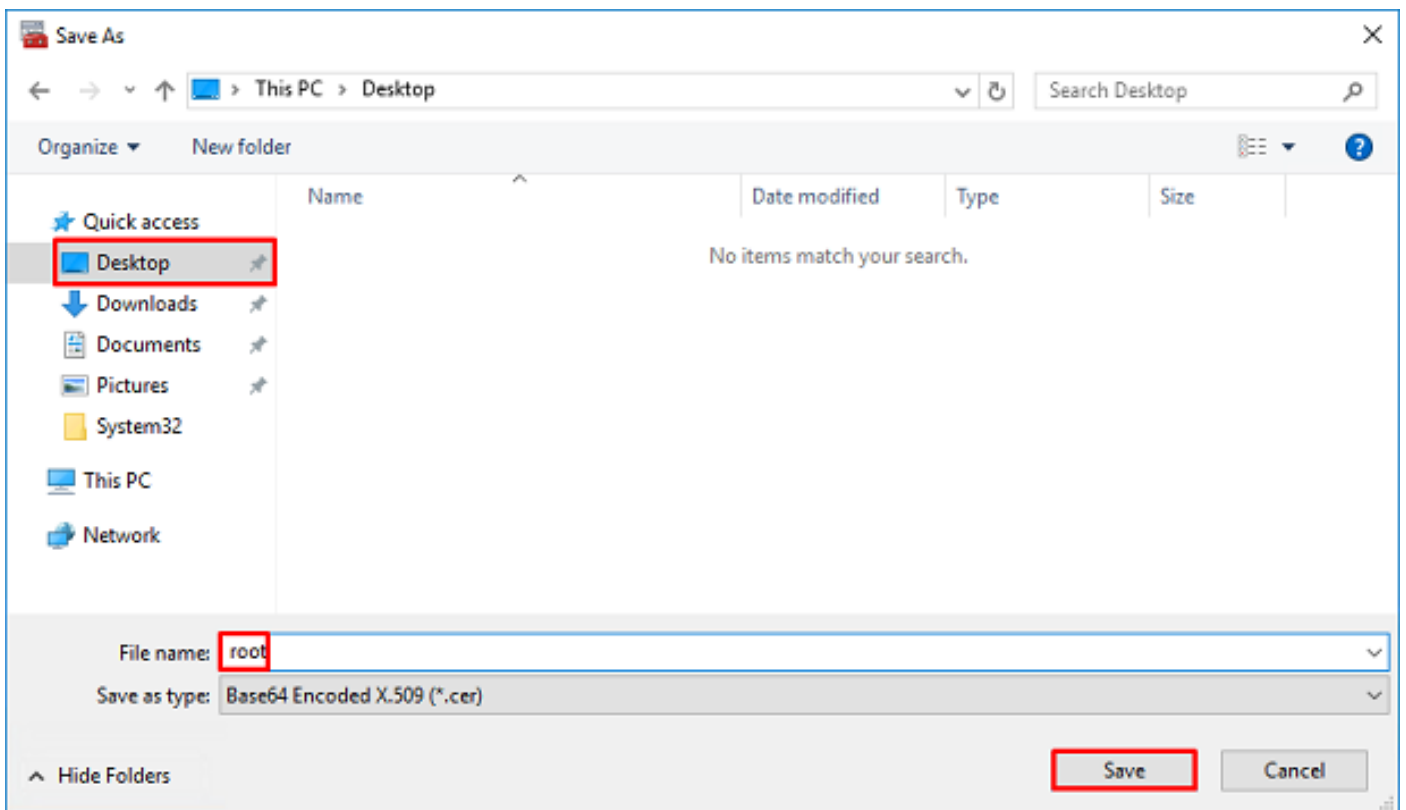
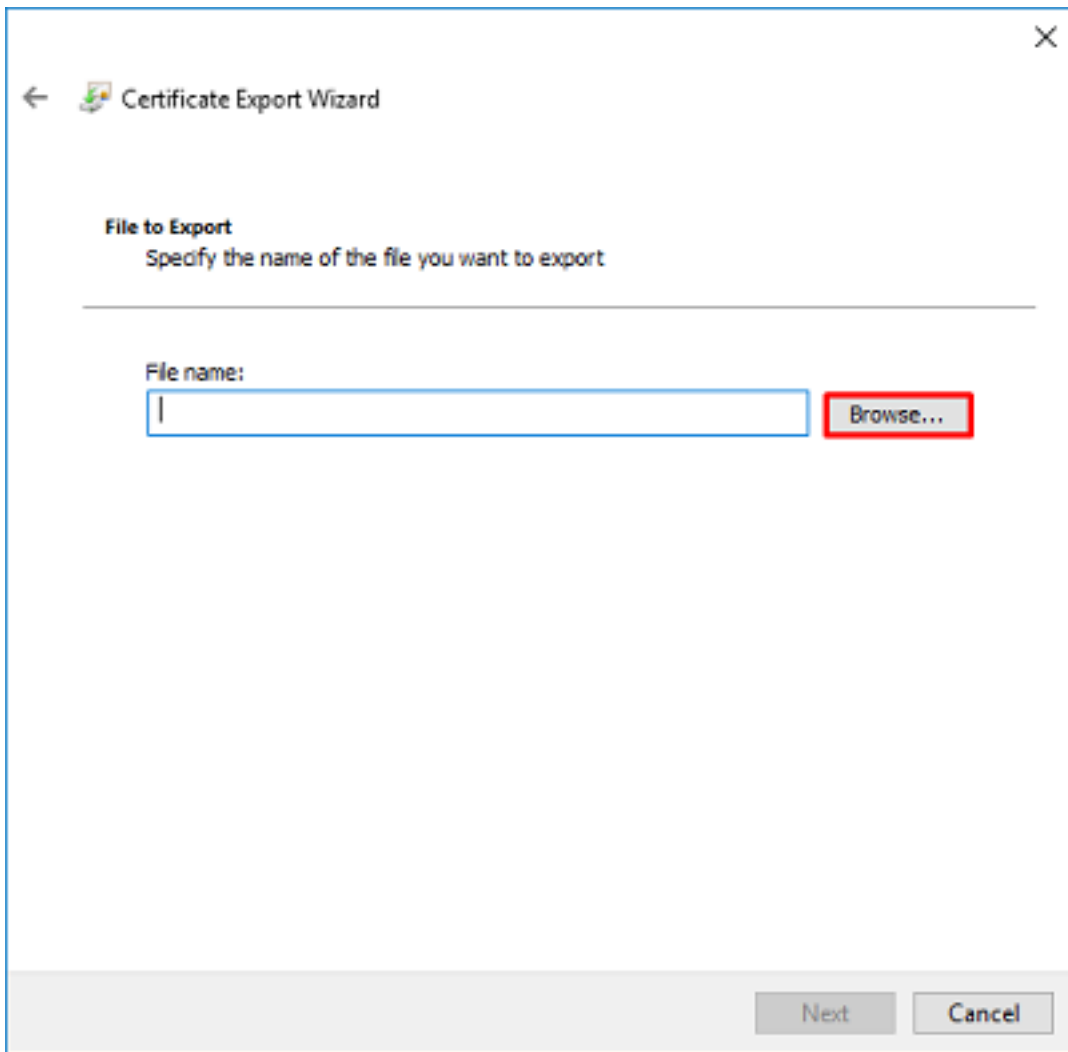
11.浏览以PEM格式导出根CA的证书导出向导。

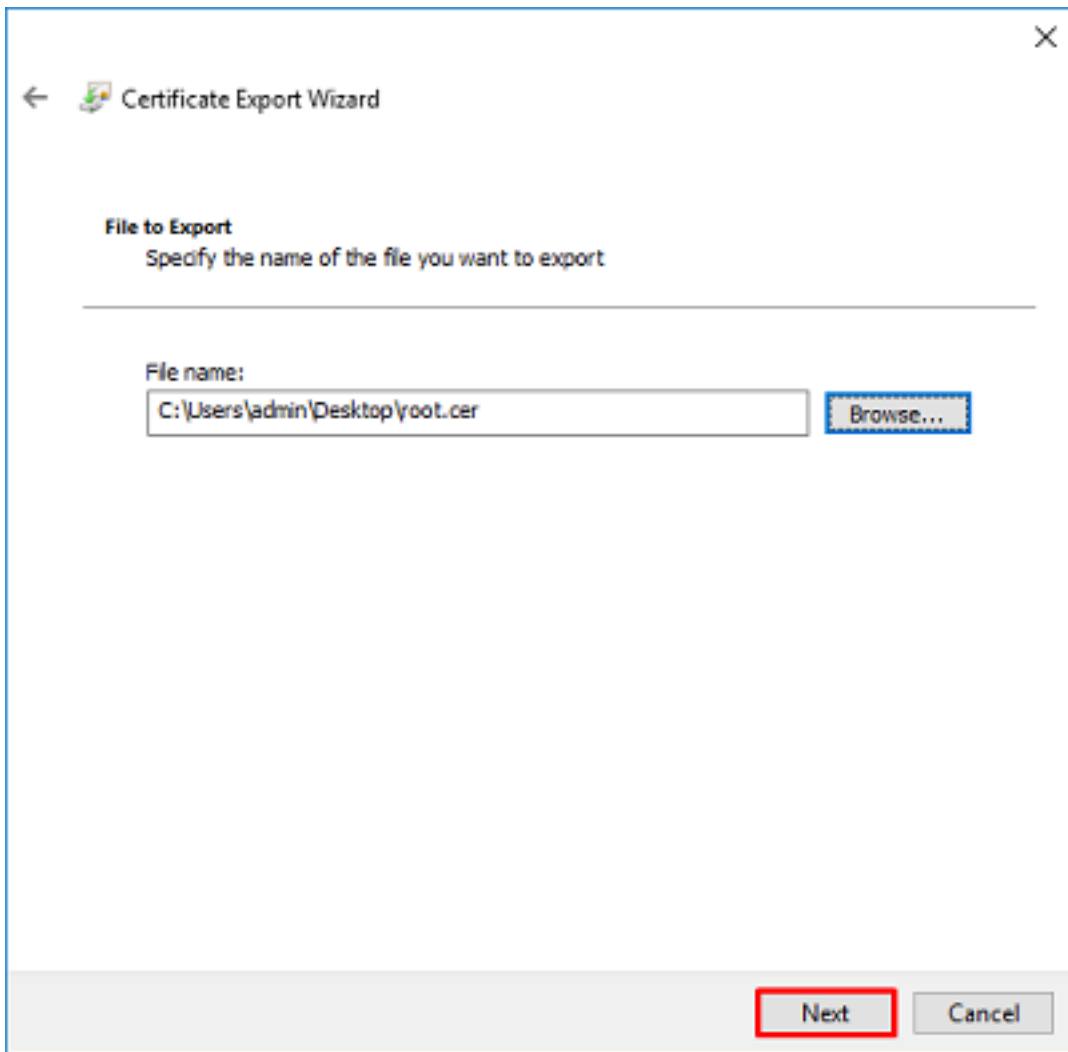


12.选择Base-64编码的X.509。

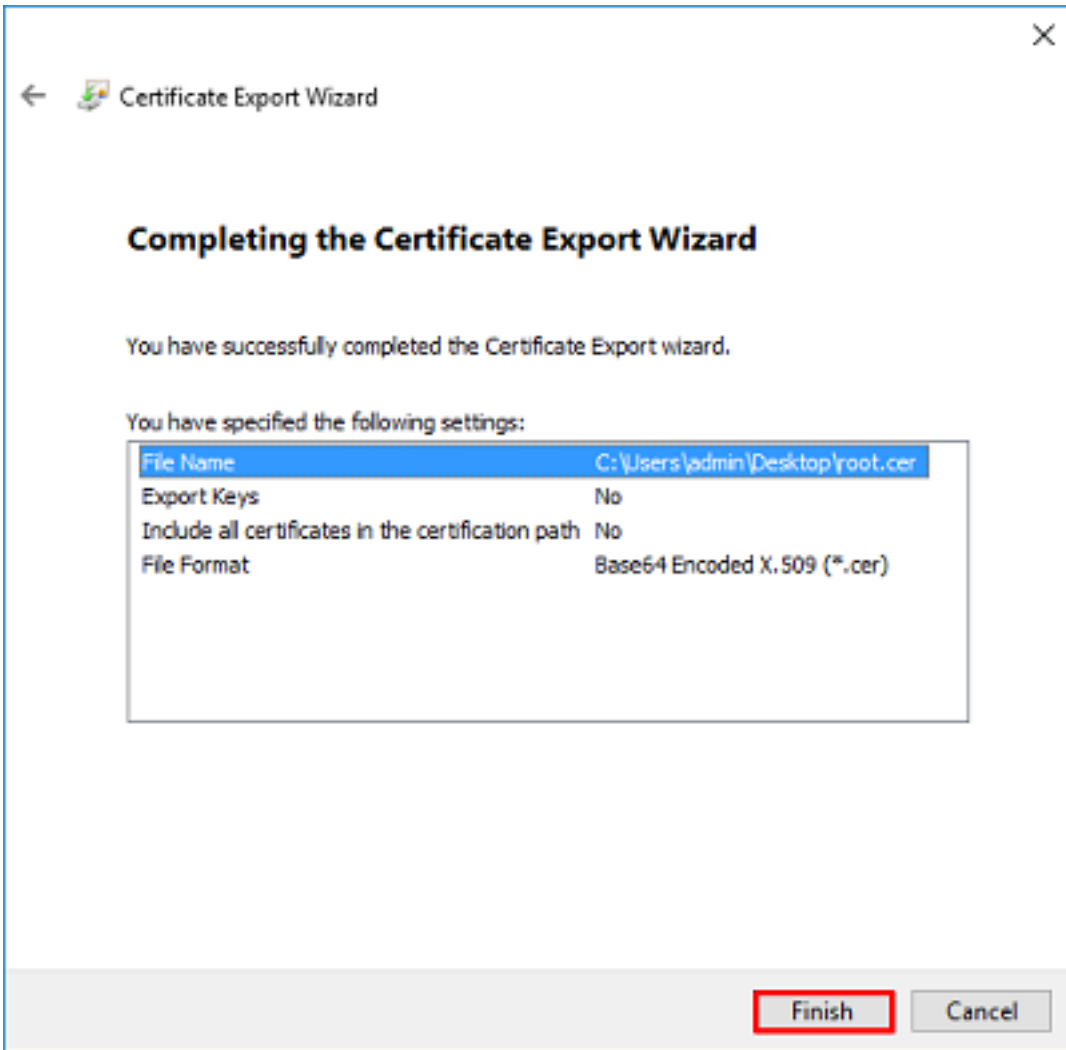


13.选择文件的名称及其导出位置。





14.单击“完成”。



15.现在，导航到该位置，使用记事本或其他文本编辑器打开证书。这将显示PEM格式证书。保存此内容以备以后使用。

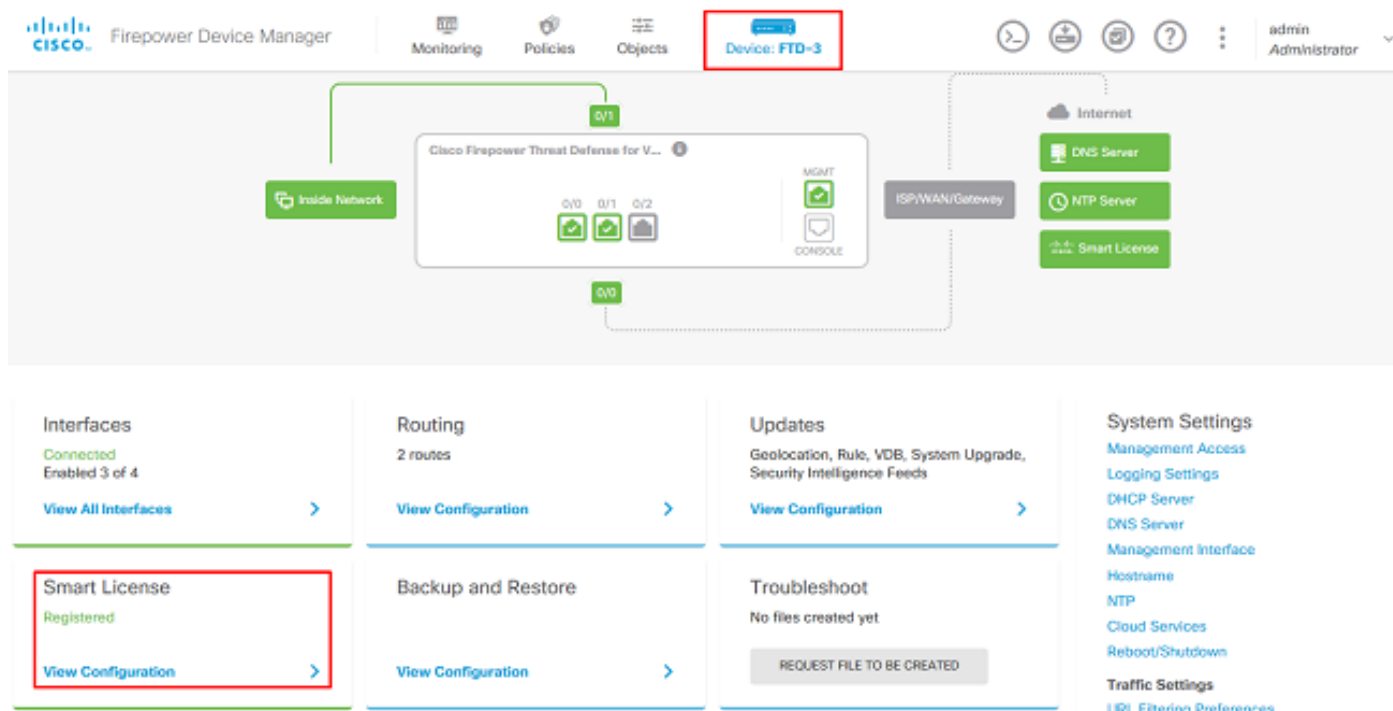
```
-----BEGIN CERTIFICATE-----
MIIDCCAfCgAwIBAgIQE4ZG5Z1wT61ONTjooEQyMTANBgkqhkiG9w0BAQsFADAd
MRswGQYDVQQDEeJleGFtcGxlLVdJTjIwMTYtQ0EwIBcNMjAwNDI3MTQ1MDU5WhgP
MjA2MDA0MTkxNDUwNTlAMB0xGzAZBgNVBAMTEmV4YW1wbGUtV01OMjAxNi1DQTCC
ASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAl8ghT719NzSQpoQPh0YT67b
Ya+PngsxMyvkewP33QLTAWw1HW1Tb9Mk5BDWOItTaVsgHwPBfd++M+bLn3AiZnHV
OO+k6dVVY/E5qVkeKSGoY+v940S2316lzdWReMOFhgbc2qMertIoficrRihonuU
Cjyeub3CO+meJUuKom2R47C0D35TUvo/FEHGgXJFaJS1se2UrpNO7KEMkfAlLPuM
aob4XE/OzxYQpPa18djsNnskfcFqD/HOTFQN4+SrOhHWlRnUIQBuaLdQaabhipD/
sVs5PneYJX8YKma821uYI6j90YuytmsHBtCieyC062a8BKqOL7N86HFPfKMA3u8C
AwEAAaNCMEAwDgYDVR0PAQH/BAQDAgGMA8GA1UdEwEB/wQFMAMBAf8wHQYDVR0O
BBYEFD2fJjf7ER9EM/HCxCVFN5QzqEdvMA0GCSqGSIb3DQEBCwUAA4IBAQB31ZJo
vzwVD3c5Q1nrNP+6Mq62OFpYH91k4Ch9S5g/CEOemhcgw8MDIoxW2dTsjenAEt7r
pHFIHZoCoSyjBjMgK3xybmoSeg8vBjCXseYNGEm0c9KW1oFmTOvdNVIb7Xp11IVa
6tALTt3ANRNgREtXPA6yQbthKGavW0Anfsojk9IcDr2vp0MTj1BCxsTscubR1+d
dLEFKQqmMeYvkVf+a7a64mqPZsG3Uxo0rd6cZxAPkq/ylcdwNSJFFfQV3DgZg+R96
9WLCR30big6xyo9Zu+lixwPdrbADO6zMHbEYEHkh00jBrUEBBI6Cy83iTZ9ejsk
KgwbJXEu33PplW6E
-----END CERTIFICATE-----
```

FDM配置

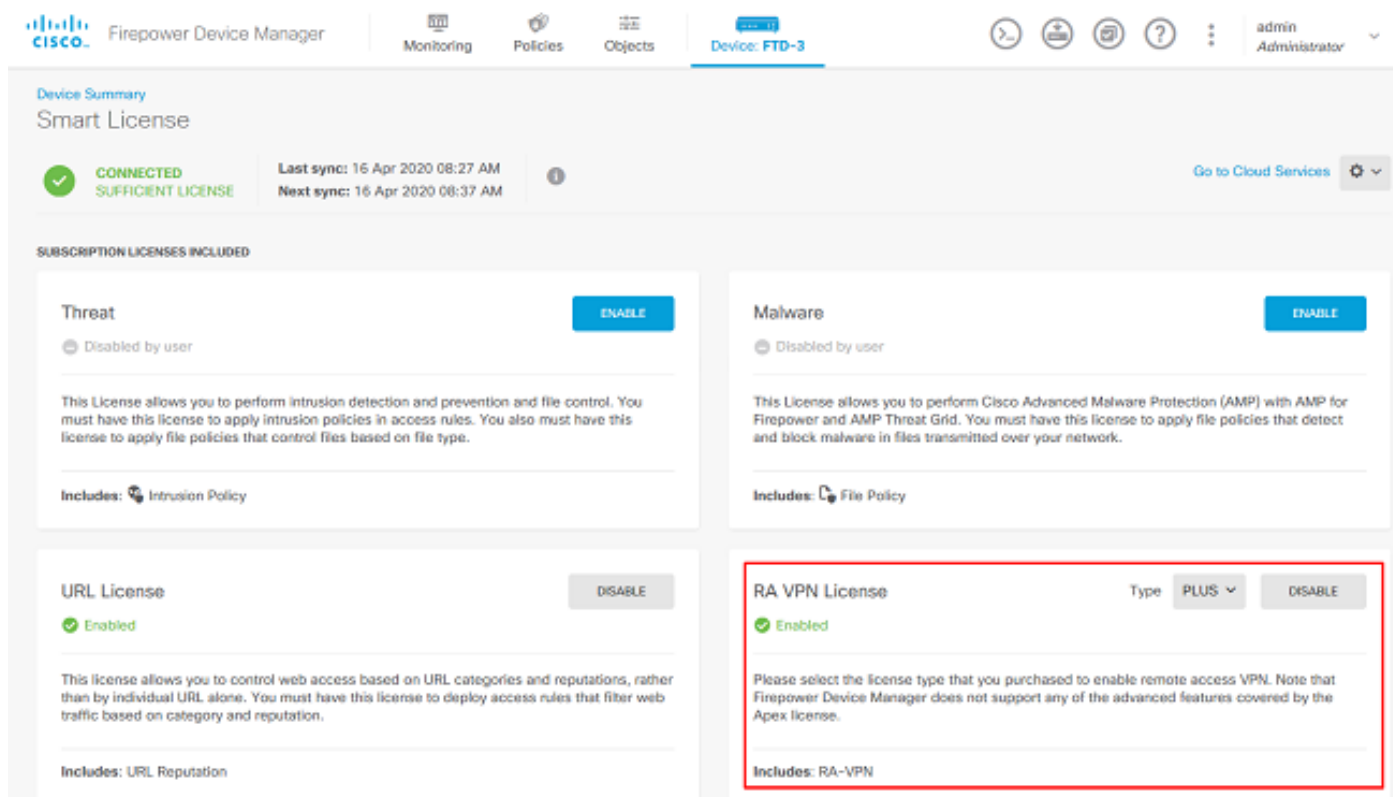
验证许可

要在FDM上配置AnyConnect，FTD需要向智能许可服务器注册，并且必须向设备应用有效的Plus、Apex或VPN专用许可证。

1. 导航至“设备”>“智能许可证”，如图所示。

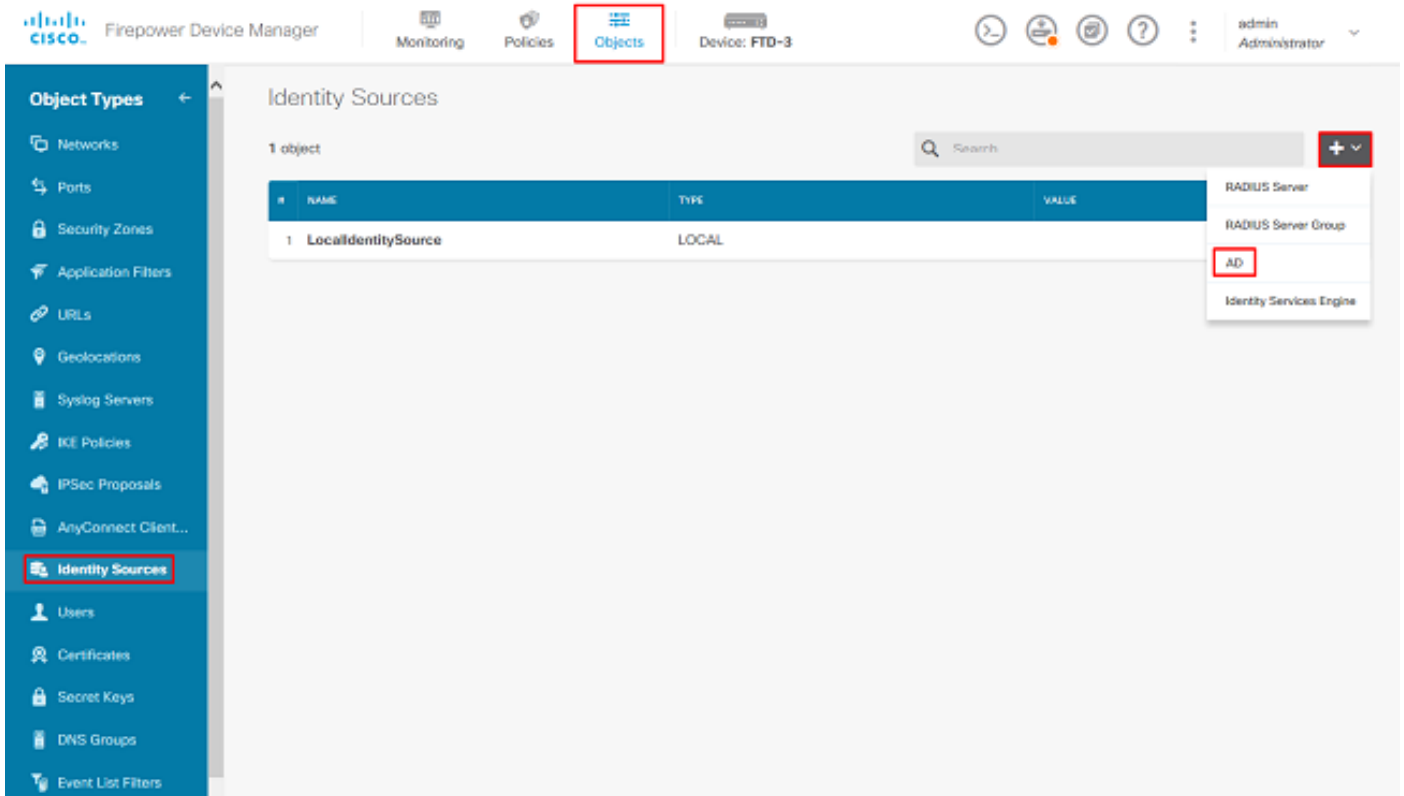


2. 验证FTD是否已注册到智能许可服务器，并且AnyConnect Plus、Apex或仅VPN许可证已启用。



设置AD身份源

1. 导航至“对象”>“身份源”，然后单击+符号并选择AD，如图所示。



2. 使用之前收集的信息填写Active Directory服务器的适当设置。如果主机名(FQDN)用于Microsoft服务器而不是IP地址，请确保在“对象”(Objects)>“DNS组”(DNS Group)下**创建适当的DNS组**。然后，导航到**Device > System Settings > DNS Server**，在**Management Interface** 和**Data Interface** 下应用DNS组，然后为DNS查询指定适当的出口接口，将该DNS组应用到FTD。单击**Test**按钮以验证是否成功配置并从FTD的管理接口访问。由于这些测试是从FTD的管理接口而不是通过在FTD上配置的可路由接口（如内部、外部、dmz）启动的，因此成功（或失败）连接不能保证AnyConnect身份验证的结果相同，因为AnyConnect LDAP身份验证请求将从FTD的可路由接口之一启动。有关从FTD测试LDAP连接的详细信息，请查看故障排除区域中的测试AAA和数据包捕获部分。

Add Identity Realm



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

Name

LAB-AD

Type

Active Directory (AD)

Directory Username

ftd.admin@example.com

e.g. user@example.com

Directory Password

••••••••

Base DN

DC=example,DC=com

e.g. ou=user, dc=example, dc=com

AD Primary Domain

example.com

e.g. example.com

Directory Server Configuration

win2016.example.com:389

Hostname / IP Address

win2016.example.com

e.g. ad.example.com

Port

389

Encryption

NONE

Trusted CA certificate

Please select a certificate

TEST

✓ Connection to realm is successful

[Add another configuration](#)

CANCEL

OK

如果使用LDAPS或STARTTLS，请选择适当的加密，然后选择受信任CA证书。如果尚未添加根CA，请点击Create New Trusted CA Certificate。为根CA证书提供名称，然后粘贴之前收集的PEM格式根CA证书。

Add Trusted CA Certificate

Name


LDAPS_ROOT

Paste certificate, or choose file: UPLOAD CERTIFICATE The supported formats are: PEM, DER.

```
-----BEGIN CERTIFICATE-----
MIIDCCCAfCgAwIBAgIQE4ZG5Z1wT6IONTjooEQyMTANBgkqhkiG9w0BAQsFADAd
MRswGQYDVQQDEExJleGFtcG9uLmV4YW1udjEwMTYtQ0EwIBcNMjAwNDI3MTQ1MDU5WhgP
MjA2MDA0MTkxNDUwNTIaMB0xGzAZBgNVBAMTEmV4YW1udjEwMTYtQ0EwIBcNMjAwNDI3MTQ1MDU5WhgP
AShwDQYJKoZIhvcNAQEFBQADQgEPADCCAQoCggEFRAI8ghT719NzSQncOPh0YT67h
```

CANCEL OK

Directory Server Configuration

 **win2016.example.com:636**

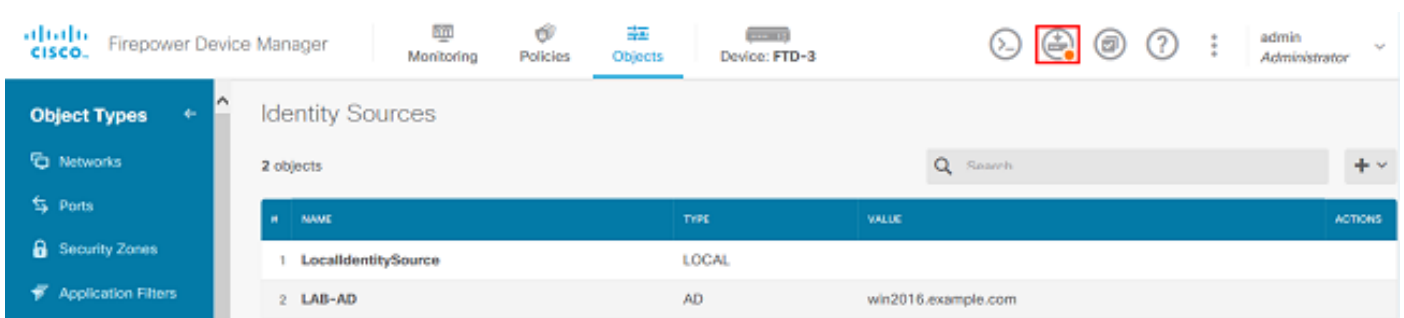
<p>Hostname / IP Address</p> <p>win2016.example.com</p> <p><i>e.g. ad.example.com</i></p>	<p>Port</p> <p>636</p>
<p>Encryption</p> <p>LDAPS</p>	<p>Trusted CA certificate</p> <p>LDAPS_ROOT</p>

TEST ✔ Connection to realm is successful

在此配置中，使用了以下值：

- 名称：LAB-AD
- 目录用户名：ftd.admin@example.com
- 基准 DN:DC=example, DC=com
- AD主域：example.com
- 主机名/IP地址：win2016.example.com
- 端口：389

3.单击右上角的“待更改”按钮，如图所示。



The screenshot shows the Cisco Firepower Device Manager interface. The top navigation bar includes "Monitoring", "Policies", and "Objects". The "Objects" tab is active, showing a table of Identity Sources. The table has columns for ID, NAME, TYPE, VALUE, and ACTIONS. Two objects are listed: "LocalIdentitySource" (LOCAL) and "LAB-AD" (AD) with value "win2016.example.com". A red box highlights a button in the top right corner of the interface, which is the "待更改" (Needs Change) button.

#	NAME	TYPE	VALUE	ACTIONS
1	LocalIdentitySource	LOCAL		
2	LAB-AD	AD	win2016.example.com	

4.单击“立即部署”按钮。

Pending Changes

✓ **Last Deployment Completed Successfully**
01 May 2020 12:54 PM. [See Deployment History](#)

Deployed Version (01 May 2020 12:54 PM) | Pending Version **LEGEND** Removed Added Edited

+ **Active Directory Realm Added: LAB-AD**

```
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
```

MORE ACTIONS ▼ | CANCEL | **DEPLOY NOW** ▼

配置AnyConnect以进行AD身份验证

要使用已配置的AD身份源，需要将其应用到AnyConnect配置。

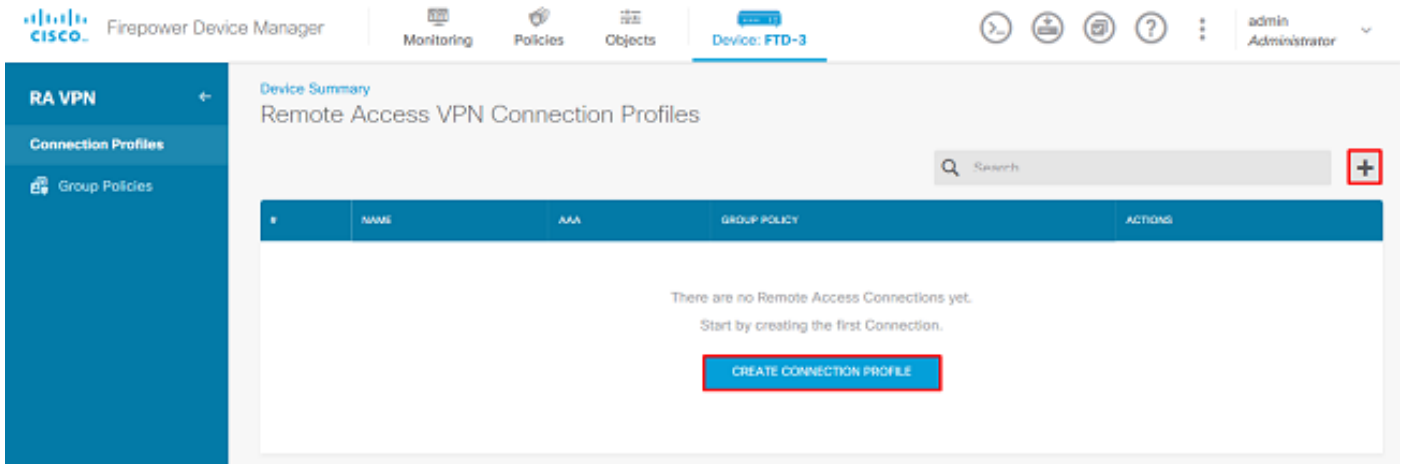
1.导航到Device > Remote Access VPN，如图所示。

Firepower Device Manager | Monitoring | Policies | Objects | **Device: FTD-3** | admin Administrator

0/0

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

2.单击+符号或“创建连接配置文件”按钮，如图所示。



3.在“连接和客户端配置”部分下，选择之前创建的AD身份源。为其他部分设置适当的值，包括连接配置文件名称和客户端地址池分配。完成后单击“提交查询”。

Connection and Client Configuration

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

Connection Profile Name

This name is configured as a connection alias, it can be used to connect to the VPN gateway

General

Group Alias

General

[Add Group Alias](#)

Group URL

[Add Group URL](#)

Primary Identity Source

Authentication Type

AAA Only Client Certificate Only AAA and Client Certificate

Primary Identity Source for User Authentication

Filter

- LocalIdentitySource
- LAB-AD
- Special-Identities-Realm

Create new

Fallback Local Identity Source ⚠

Please Select Local Identity Source

Client Address Pool Assignment

IPv4 Address Pool

Endpoints are provided an address from this pool



 AnyConnect-Pool

IPv6 Address Pool

Endpoints are provided an address from this pool



DHCP Servers



CANCEL

SUBMIT QUERY

4.在“远程用户体验”部分下，选择适当的组策略。默认情况下，将使用DfltGrpPolicy;但是，可以创建另一个。

DfltGrpPolicy

Policy Group Brief Details

DNS + BANNER		Edit
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	

BACK

SUBMIT QUERY

5.在“全局设置”(Global Settings)部分下，至少指定SSL证书、外部接口和AnyConnect软件包。如果之前未创建证书，则可以选择默认自签名证书([DefaultInternalCertificate](#))，但会看到不受信任的服务器证书消息。应取消选中已解密流量(sysopt permit-vpn)的绕行访问控制策略，以使用户身份访问策略规则稍后生效。NAT免除也可在此处配置。在此配置中，从内部接口到AnyConnect客户端IP地址的所有ipv4流量除来自NAT外。对于更复杂的设置（如外部到外部迂回），需要在NAT策略下创建其他NAT规则。AnyConnect软件包可在思科支持站点找到：<https://software.cisco.com/download/home>。要下载AnyConnect软件包，需要有效的Plus或Apex许可证。

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

FTD-3-Manual

Outside Interface

outside (GigabitEthernet0/0)

Fully-qualified Domain Name for the Outside Interface

ftd3.example.com

e.g. ravpn.example.com

Access Control for VPN Traffic

Decrypted VPN traffic is subjected to access control policy inspection by default. Enabling the Bypass Access Control policy for decrypted traffic option bypasses the access control policy, but for remote access VPN, the VPN Filter ACL and the authorization ACL downloaded from the AAA server are still applied to VPN traffic

Bypass Access Control policy for decrypted traffic (sysopt permit-vpn)

NAT Exempt



Inside Interfaces

The interfaces through which remote access VPN users can connect to the internal networks

+

inside (GigabitEthernet0/1)

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.

+

any-ipv4

AnyConnect Package

If a user does not already have the right AnyConnect package installed, the system will launch the AnyConnect installer when the client authenticates for the first time. The user can then install the package from the system.

You can download AnyConnect packages from software.cisco.com.

You must have the necessary AnyConnect software license.

Packages

UPLOAD PACKAGE

Windows: anyconnect-win-4.7.03052-webdeploy-k9.pkg

Linux: anyconnect-linux64-4.7.03052-webdeploy-k9.pkg

BACK

NEXT

6.在“摘要”部分下，验证AnyConnect是否已正确设置，然后单击“提交查询”。

^ Summary

Review the summary of the Remote Access VPN configuration.

General

STEP 1: CONNECTION AND CLIENT CONFIGURATION

Primary Identity Source

Authentication Type AAA Only

Primary Identity Source LAB-AD

Fallback Local Identity Source -

Strip Identity Source server from username No

Strip Group from Username No

Secondary Identity Source

Secondary Identity Source for User Authentication -

Fallback Local Identity Source -

Advanced

Authorization Server

Accounting Server

Client Address Pool Assignment

IPv4 Address Pool

BACK SUBMIT QUERY

7.单击右上角的“待更改”按钮，如图所示。

Firepower Device Manager | Monitoring | Policies | Objects | Device: FTD-3 | admin Administrator

RA VPN

Connection Profiles

Group Policies

Device Summary

Remote Access VPN Connection Profiles

1 object

#	NAME	AAA	GROUP POLICY	ACTIONS
1	General	Authentication: AAA Only Authorization: None Accounting: None	DfltGrpPolicy	

8.单击“立即部署”。

Pending Changes

?
✕
Close

✔ Last Deployment Completed Successfully
16 Apr 2020 12:41 PM, [See Deployment History](#)

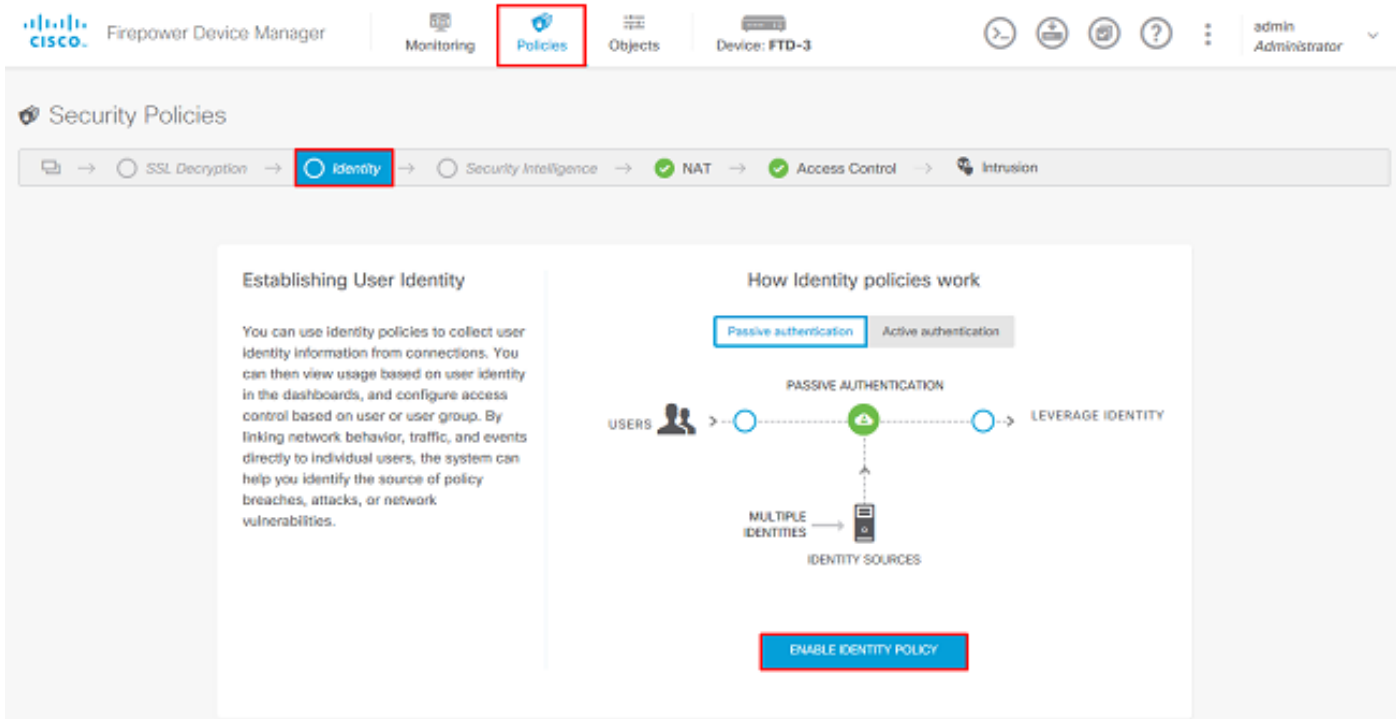
Deployed Version (16 Apr 2020 12:41 PM)	Pending Version
+ Network Object Added: <i>AnyConnect-Pool</i>	
-	subType: Network
-	value: 10.10.10.0/24
-	isSystemDefined: false
-	dnsResolution: IPV4_AND_IPV6
-	name: AnyConnect-Pool
+ RA VPN Added: <i>NGFW-Remote-Access-VPN</i>	
-	vpnGatewaySettings[0].exemptNatRule: true
-	vpnGatewaySettings[0].outsideFqdn: ftd3.example.com
-	vpnGatewaySettings[0].bypassAccessControlForVPNTraffic: t...
-	name: NGFW-Remote-Access-VPN
anyconnectPackageFiles:	
-	anyconnect-win-4.7.03052-webdeploy-k9.pkg
vpnGatewaySettings[0].serverCertificate:	
-	FTD-3-Manual
vpnGatewaySettings[0].outsideInterface:	
-	outside
vpnGatewaySettings[0].insideInterfaces:	
-	inside
vpnGatewaySettings[0].insideNetworks:	

MORE ACTIONS ▾
CANCEL
DEPLOY NOW ▾

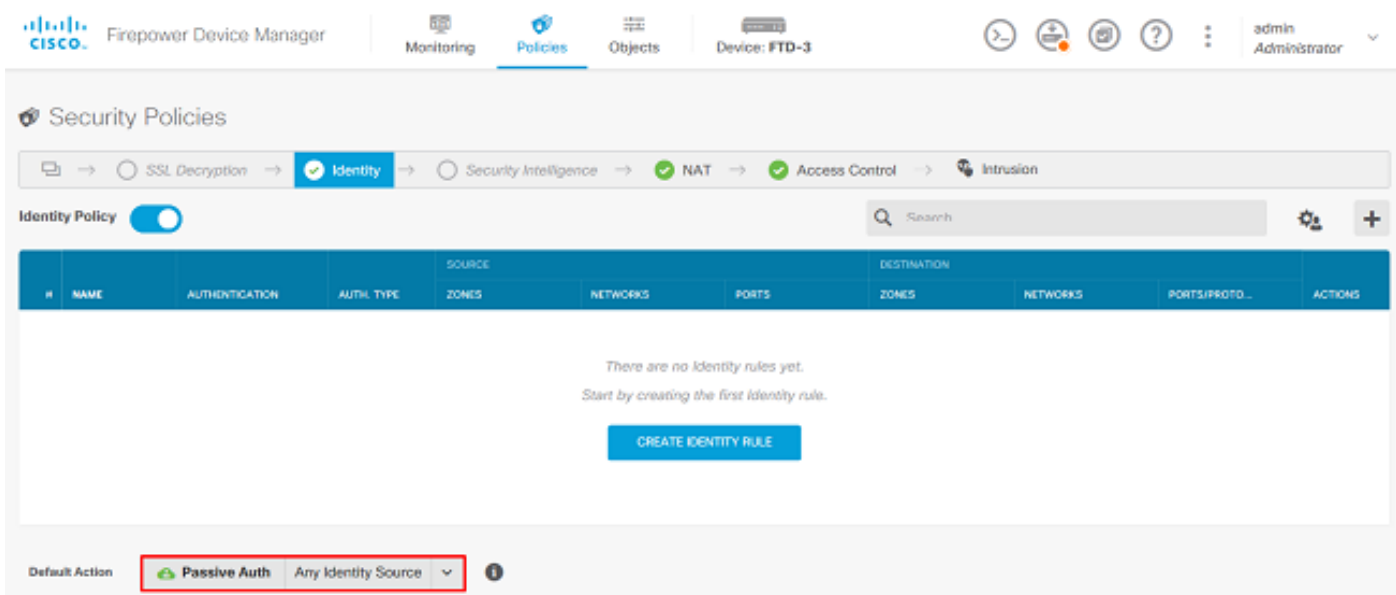
启用身份策略并配置用户身份的安全策略

此时，AnyConnect用户应该能够成功连接，但可能无法访问特定资源。此步骤将启用用户身份，以便只有AnyConnect管理员中的用户可以使用RDP连接到内部资源，并且只有组AnyConnect用户中的用户可以使用HTTP连接到内部资源。

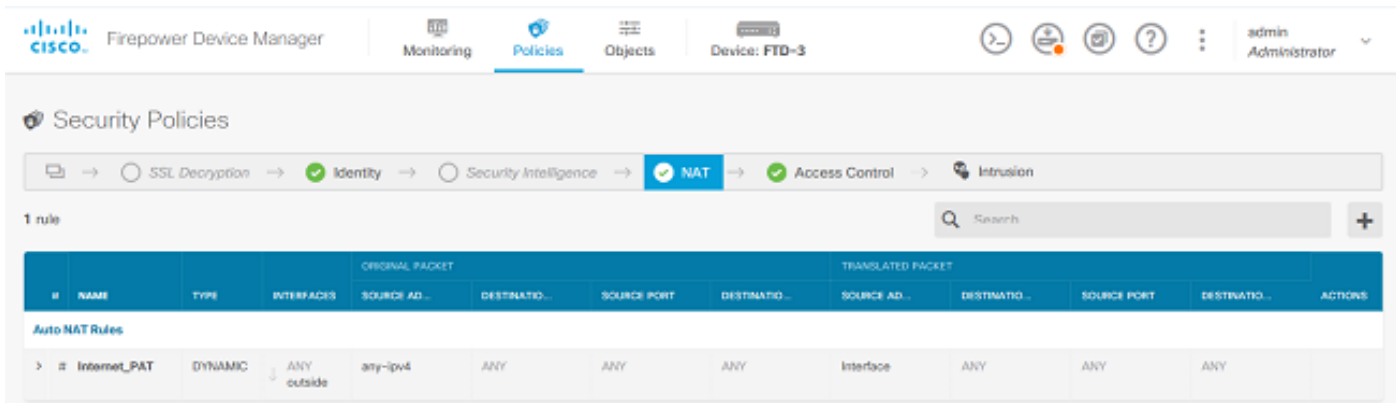
1. 导航至Policies > Identity，然后单击Enable Identity Policy。



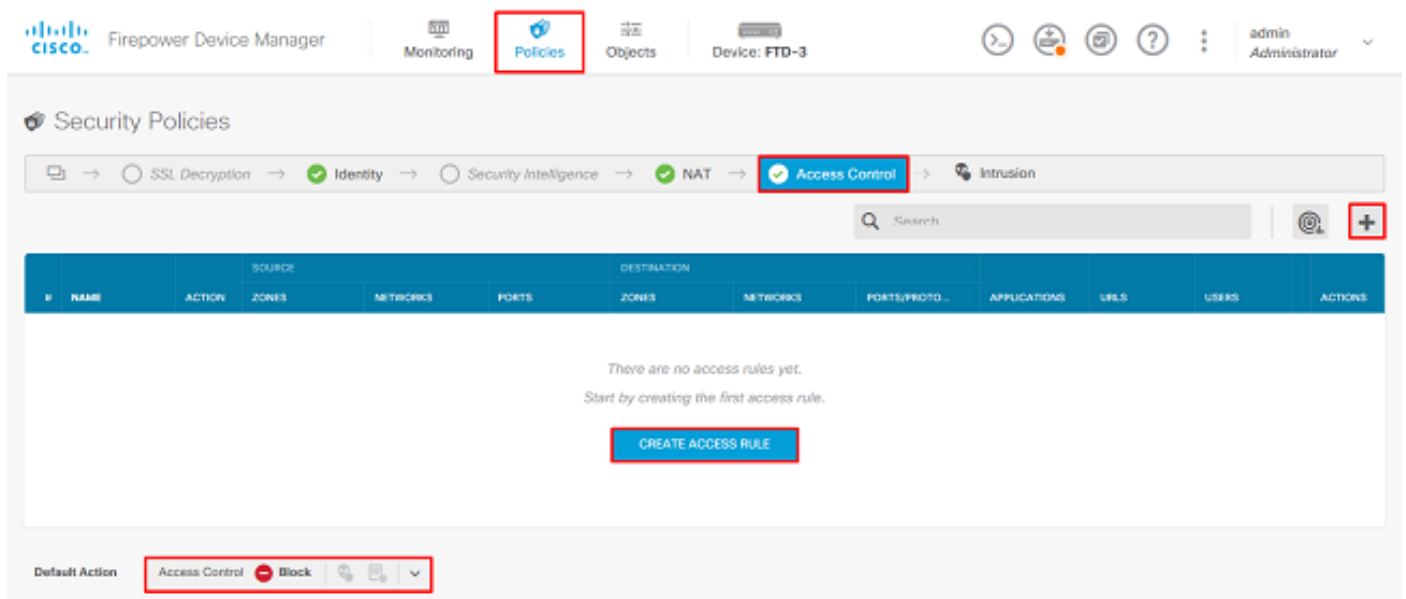
对于此配置，无需进一步配置，默认操作就足够了。



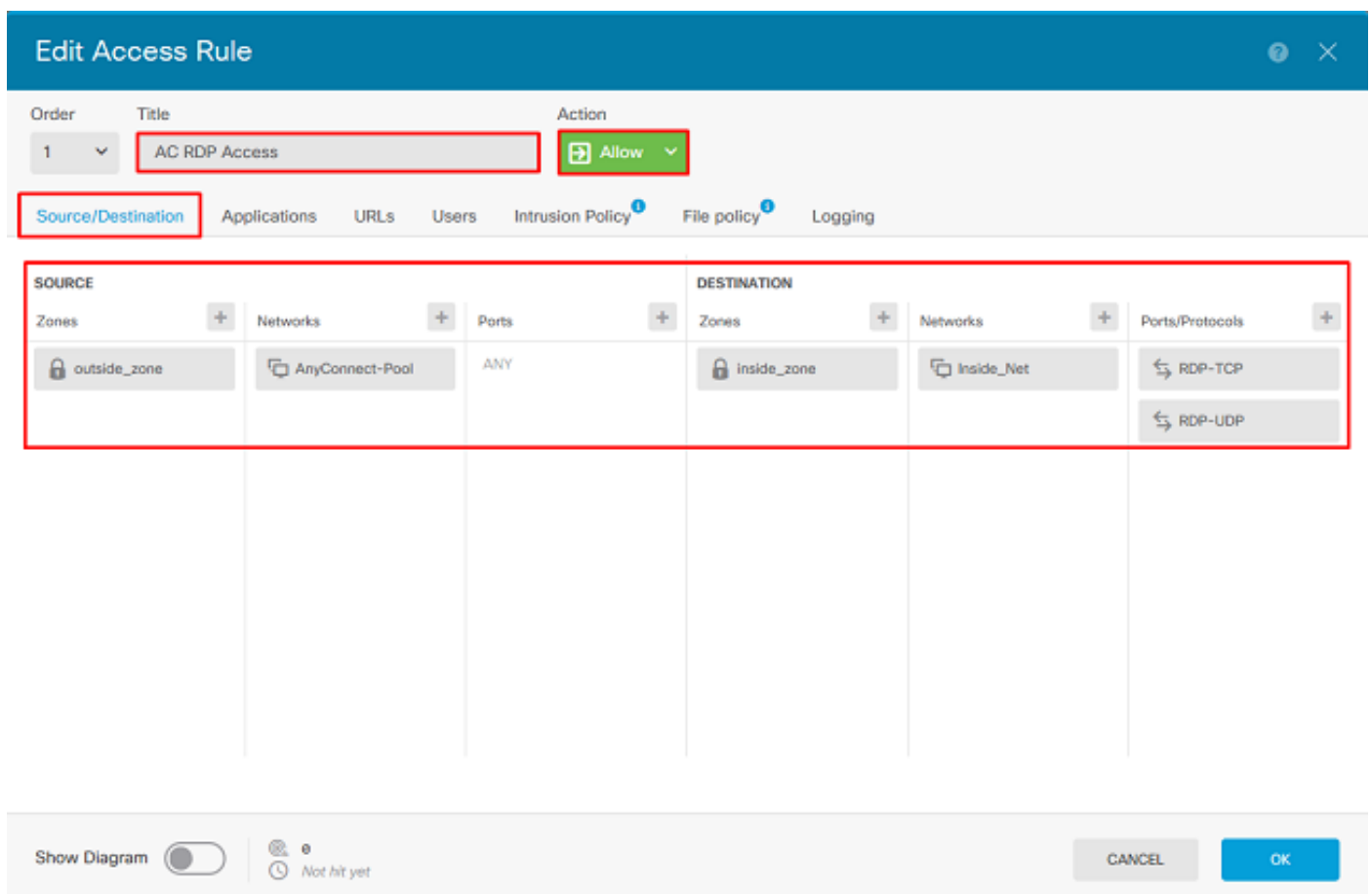
2. 导航至 **Policies > NAT**，确保 NAT 配置正确。如果在 AnyConnect 设置中配置的 NAT 异常已足够，则无需在此处进行其他配置。



3. 导航至“策略”>“访问控制”。在本节中，Default Action（默认操作）设置为Block（阻止），并且未创建访问规则，因此，一旦AnyConnect用户连接，他们将无法访问任何内容。单击+符号或创建访问规则以添加新规则。



4. 用适当的值填写字段。在此配置中，AnyConnect Admins组内的用户应具有对内部网络中Windows服务器的RDP访问权限。对于源，区域配置为outside_zone，该外部接口是AnyConnect用户将要连接到的外部接口，而网络配置为AnyConnect-Pool对象，此对象之前配置为向AnyConnect客户端分配IP地址。对于FDM中的用户身份，源必须是用户从发起连接的区域和网络。对于目标，区域配置为Windows Server所在的内部接口inside_zone，网络配置为定义Windows Server所在子网的Inside_Net对象，端口/协议设置为两个自定义端口对象以允许通过TCP 3389和UDP 3389进行RDP访问。



在“用户”部分下，将添加组AnyConnect管理员，以便允许此组以外的用户通过RDP访问Windows服务器。单击+符号，单击“组”选项卡，单击适当的组，然后单击“确定”。请注意，也可以选择单个用户和身份源。

Add Access Rule

Order	Title	Action
1	AC RDP Access	Allow

Source/Destination Applications URLs **Users** Intrusion Policy File policy Logging

AVAILABLE USERS

Filter

Identity Sources **Groups** Users

- LAB-AD \ Account Operators
- LAB-AD \ Administrators
- LAB-AD \ Allowed RODC Password Replication Group
- LAB-AD \ AnyConnect Admins**
- LAB-AD \ AnyConnect Users

Create new Identity Realm CANCEL OK

CONTROLLING ACCESS FOR USERS AND USER GROUPS

If you configure identity policies to establish user identity based on source IP address, you can control access based on user name or user group membership. By controlling access based on user identity, you can apply the appropriate access controls whether the user changes workstations or obtains a different address through DHCP. If you base rules on group membership, user network access changes as users change roles in your organization, moving from one group to another.

Show Diagram CANCEL OK

选择适当的选项后，单击“确定”。

Add Access Rule

Order	Title	Action
1	AC RDP Access	Allow

Source/Destination Applications URLs **Users** Intrusion Policy File policy Logging

AVAILABLE USERS + **CONTROLLING ACCESS FOR USERS AND USER GROUPS**

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 OK

5. 根据需要创建更多访问规则。在此配置中，会创建另一个访问规则以允许AnyConnect用户组内的用户通过HTTP访问Windows服务器。

Edit Access Rule

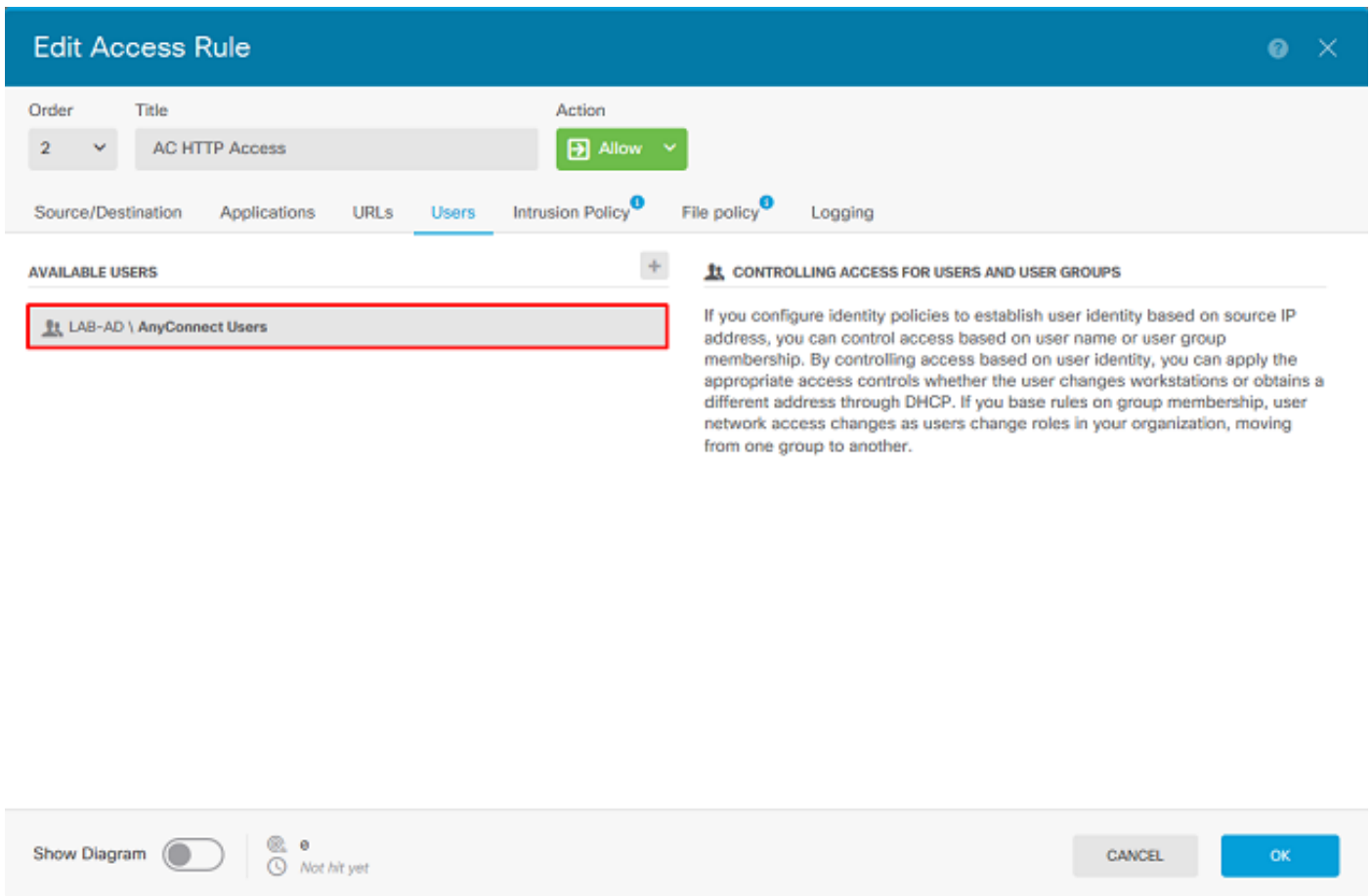
Order	Title	Action
2	AC HTTP Access	Allow

Source/Destination Applications URLs **Users** Intrusion Policy File policy Logging

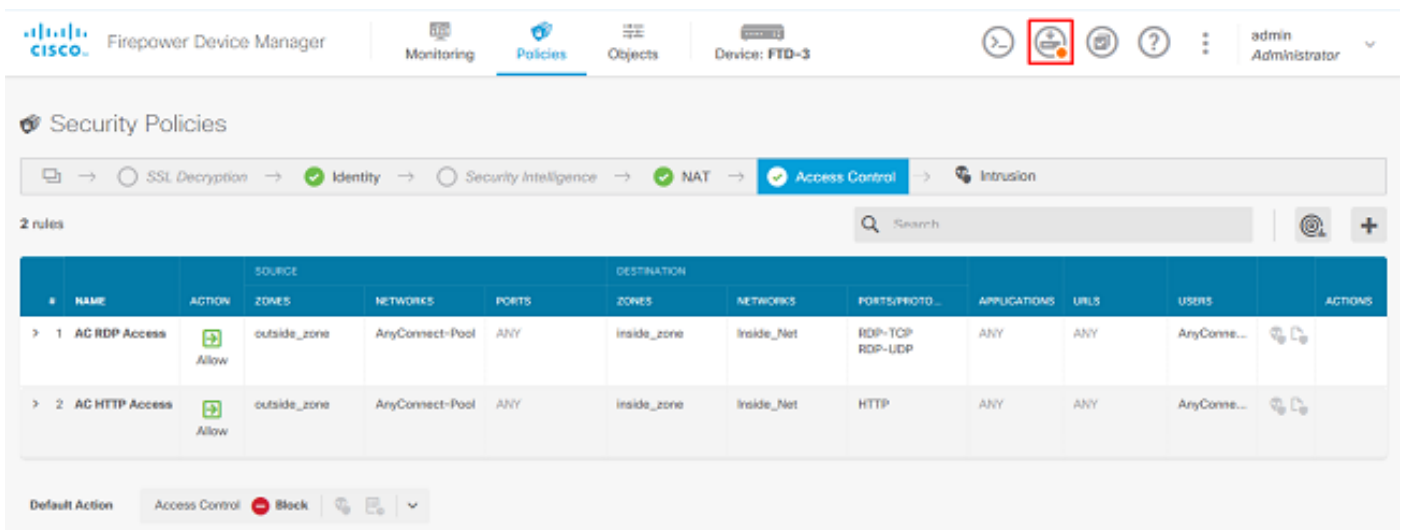
SOURCE			DESTINATION		
Zones	Networks	Ports	Zones	Networks	Ports/Protocols
outside_zone	AnyConnect-Pool	ANY	inside_zone	Inside_Net	HTTP

Show Diagram Not hit yet

CANCEL OK



6. 验证访问规则配置，然后单击右上角的Pending Changes按钮，如图所示。



7. 验证更改，然后单击“立即部署”。

Pending Changes



✓ Last Deployment Completed Successfully
28 Apr 2020 01:35 PM. [See Deployment History](#)

Deployed Version (28 Apr 2020 01:35 PM)

Pending Version

LEGEND Removed Added Edited

+ 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
destinationZones:	
-	inside_zone
sourceNetworks:	
-	AnyConnect-Pool
destinationNetworks:	
-	Inside_Net
destinationPorts:	
-	HTTP
users[0].identitySource:	
-	LAB-AD

+ Access Rule Added: AC RDP Access

MORE ACTIONS ▾

CANCEL

DEPLOY NOW ▾

验证

使用本部分可确认配置能否正常运行。

最终配置

AAA配置

```
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
```

配置AnyConnect

```
> show running-config webvpn
webvpn
enable outside
http-headers
hsts-server
enable
max-age 31536000
include-sub-domains
no preload
```

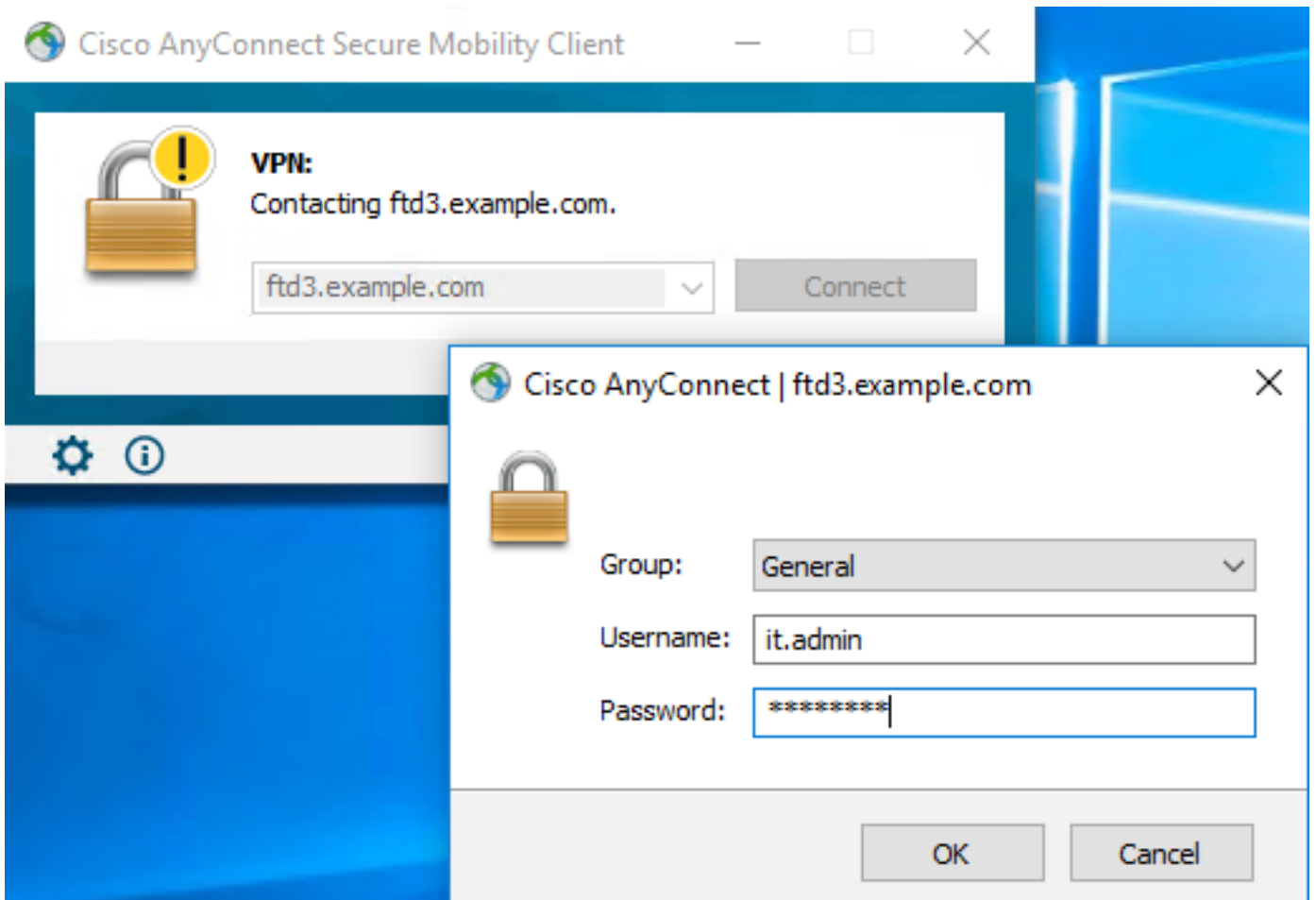
```
hsts-client
  enable
x-content-type-options
x-xss-protection
content-security-policy
anyconnect image disk0:/anyconnpkgs/anyconnect-linux64-4.7.03052-webdeploy-k9.pkg 1
anyconnect image disk0:/anyconnpkgs/anyconnect-win-4.7.03052-webdeploy-k9.pkg 2
anyconnect enable
tunnel-group-list enable
cache
  disable
error-recovery disable

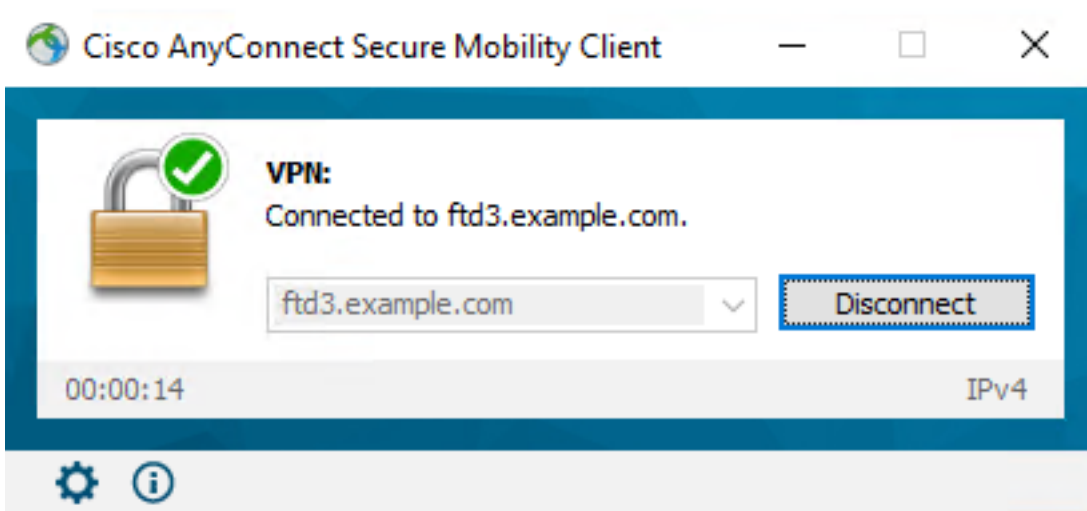
> show running-config tunnel-group
tunnel-group General type remote-access
tunnel-group General general-attributes
  address-pool AnyConnect-Pool
  authentication-server-group LAB-AD
tunnel-group General webvpn-attributes
  group-alias General enable

> show running-config group-policy
group-policy DfltGrpPolicy attributes
  vpn-tunnel-protocol ssl-client
  split-tunnel-policy tunnelspecified
  split-tunnel-network-list value DfltGrpPolicy|splitAcl
webvpn
  anyconnect ssl dtls none

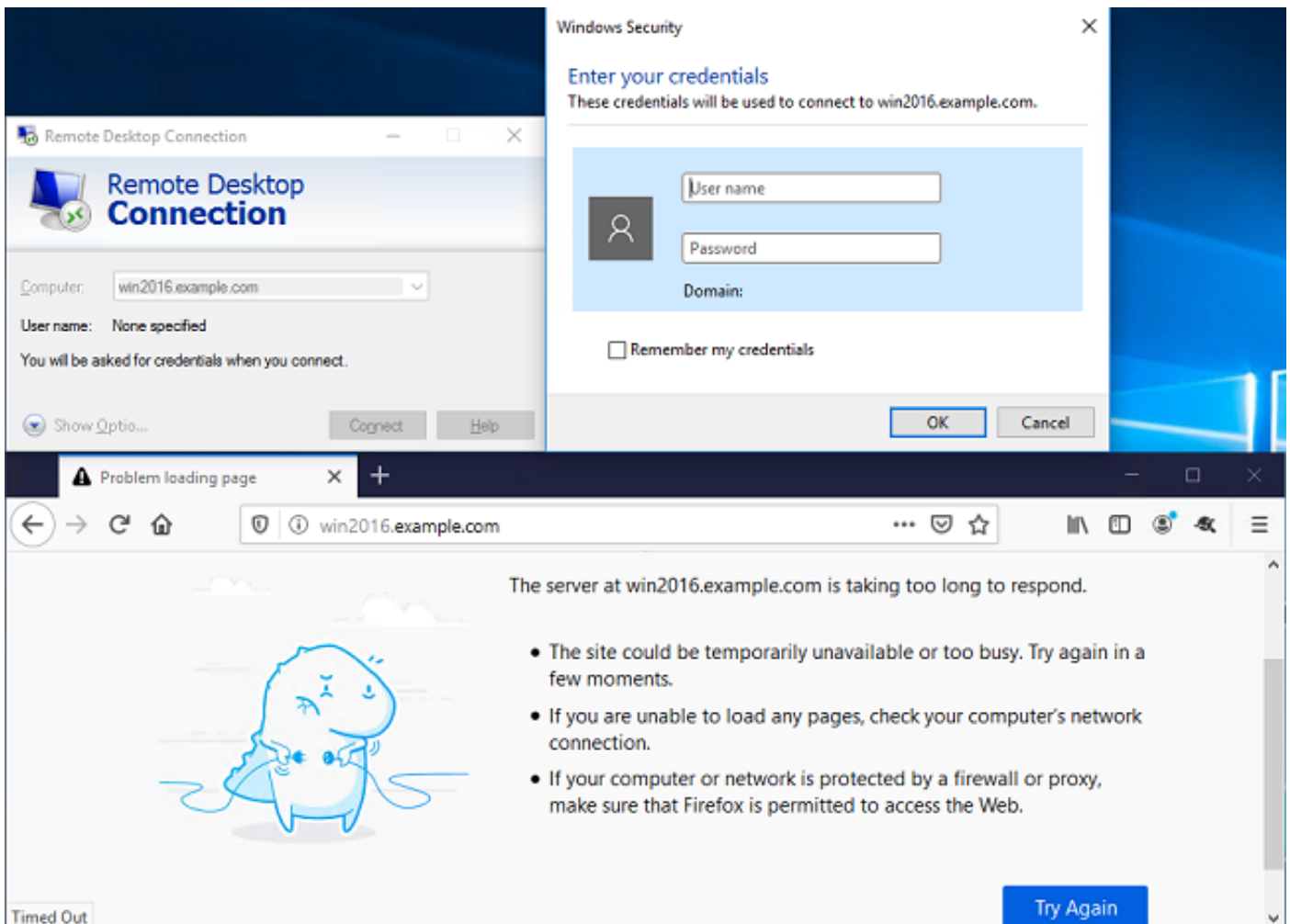
> show running-config ssl
ssl trust-point FTD-3-Manual outside
```

使用AnyConnect连接并验证访问控制策略规则

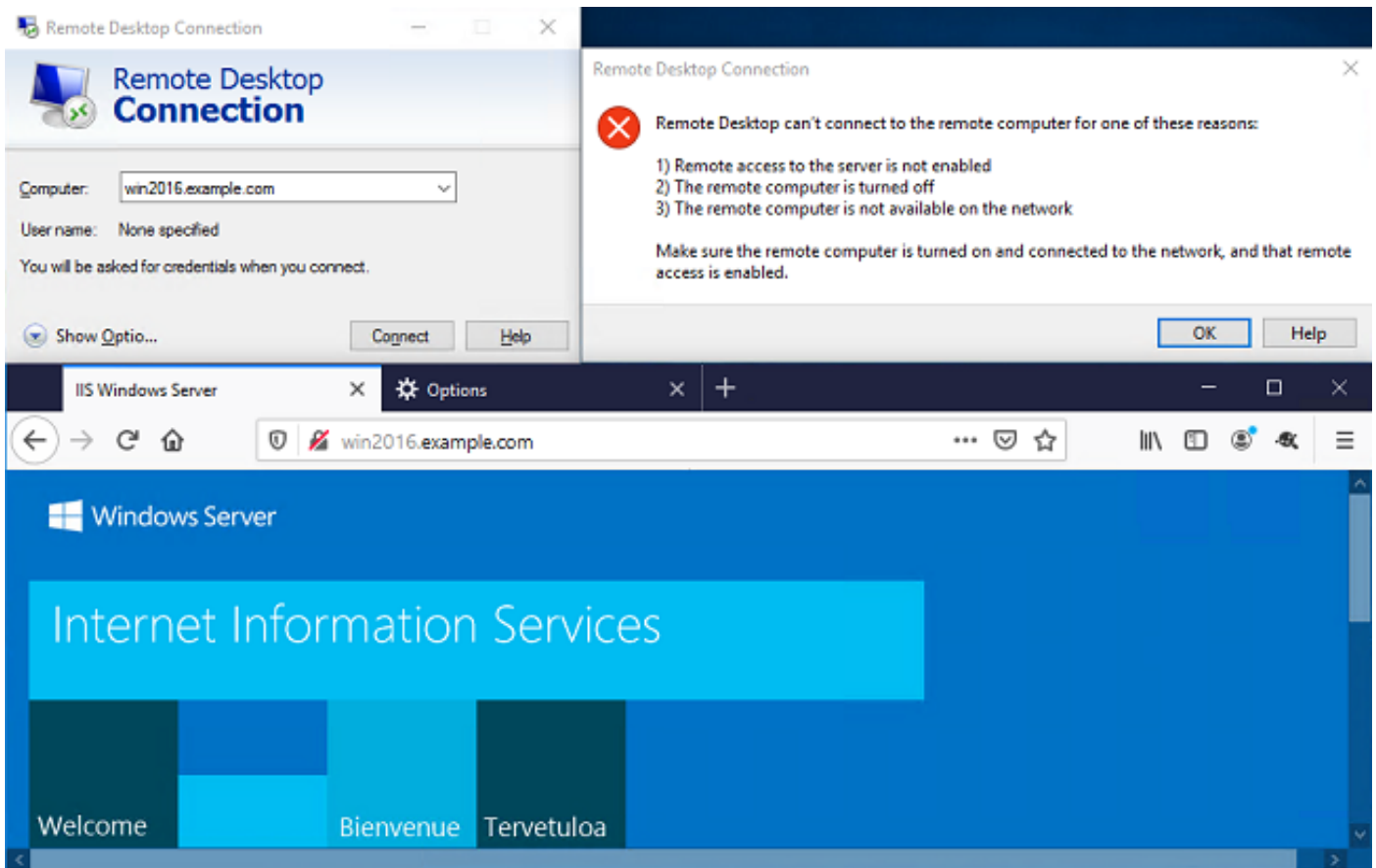




用户IT管理员位于组AnyConnect管理员中，该管理员具有对Windows Server的RDP访问权限，但无权访问HTTP。打开到此服务器的RDP和Firefox会话，验证此用户是否只能通过RDP访问服务器。



如果使用AnyConnect用户组中具有HTTP访问权限但没有RDP访问权限的测试用户登录，则可以验证访问控制策略规则是否生效。



故障排除

使用本部分可确认配置能否正常运行。

调试

此调试可在诊断CLI中运行，以排除与LDAP身份验证相关的问题：**debug ldap 255**。

为了排除用户身份访问控制策略问题，系统支持**firewall-engine-debug**，以便确定流量被意外允许或阻止的原因。

工作LDAP调试

```
[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:
[53]   objectClass: value = top
[53]   objectClass: value = person
[53]   objectClass: value = organizationalPerson
[53]   objectClass: value = user
[53]   cn: value = IT Admin
[53]   sn: value = Admin
[53]   givenName: value = IT
[53]   distinguishedName: value = CN=IT Admin,CN=Users,DC=example,DC=com
[53]   instanceType: value = 4
[53]   whenCreated: value = 20200421025811.0Z
[53]   whenChanged: value = 20200421204622.0Z
[53]   displayName: value = IT Admin
[53]   uSNCreated: value = 25896
[53]   memberOf: value = CN=AnyConnect Admins,CN=Users,DC=example,DC=com
[53]   uSNChanged: value = 26119
[53]   name: value = IT Admin
[53]   objectGUID: value = &...J..O..2w...c
[53]   userAccountControl: value = 512
[53]   badPwdCount: value = 6
[53]   codePage: value = 0
[53]   countryCode: value = 0
[53]   badPasswordTime: value = 132320354378176394
[53]   lastLogoff: value = 0
[53]   lastLogon: value = 0
[53]   pwdLastSet: value = 132319114917186142
[53]   primaryGroupID: value = 513
[53]   objectSid: value = .....{I...;.....}...
[53]   accountExpires: value = 9223372036854775807
[53]   logonCount: value = 0
[53]   sAMAccountName: value = it.admin
[53]   sAMAccountType: value = 805306368
[53]   userPrincipalName: value = it.admin@example.com
[53]   objectCategory: value = CN=Person,CN=Schema,CN=Configuration,DC=example,DC=com
[53]   dSCorePropagationData: value = 16010101000000.0Z
[53]   lastLogonTimestamp: value = 132319755825875876
[53] Fiber exit Tx=515 bytes Rx=2659 bytes, status=1
[53] Session End
```

无法与LDAP服务器建立连接

```
[-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
```

潜在解决方案：

- 检查路由并确保FTD收到来自LDAP服务器的响应。

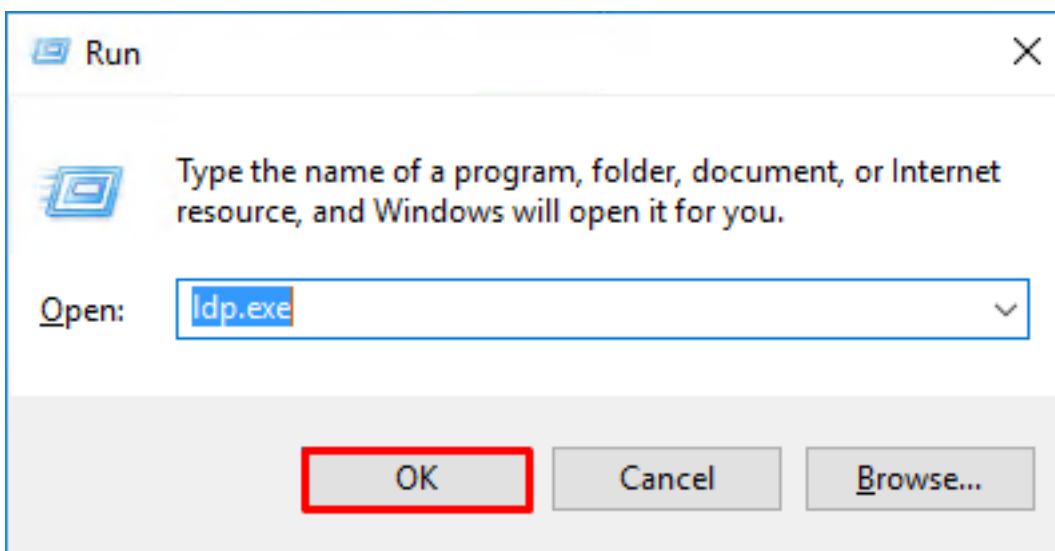
- 如果使用LDAPS或STARTTLS，请确保正确的根CA证书受信任，以便SSL握手可以成功完成。
- 检验使用的IP地址和端口是否正确。如果使用主机名，请验证DNS是否能将其解析为正确的IP地址

绑定登录DN和/或密码不正确

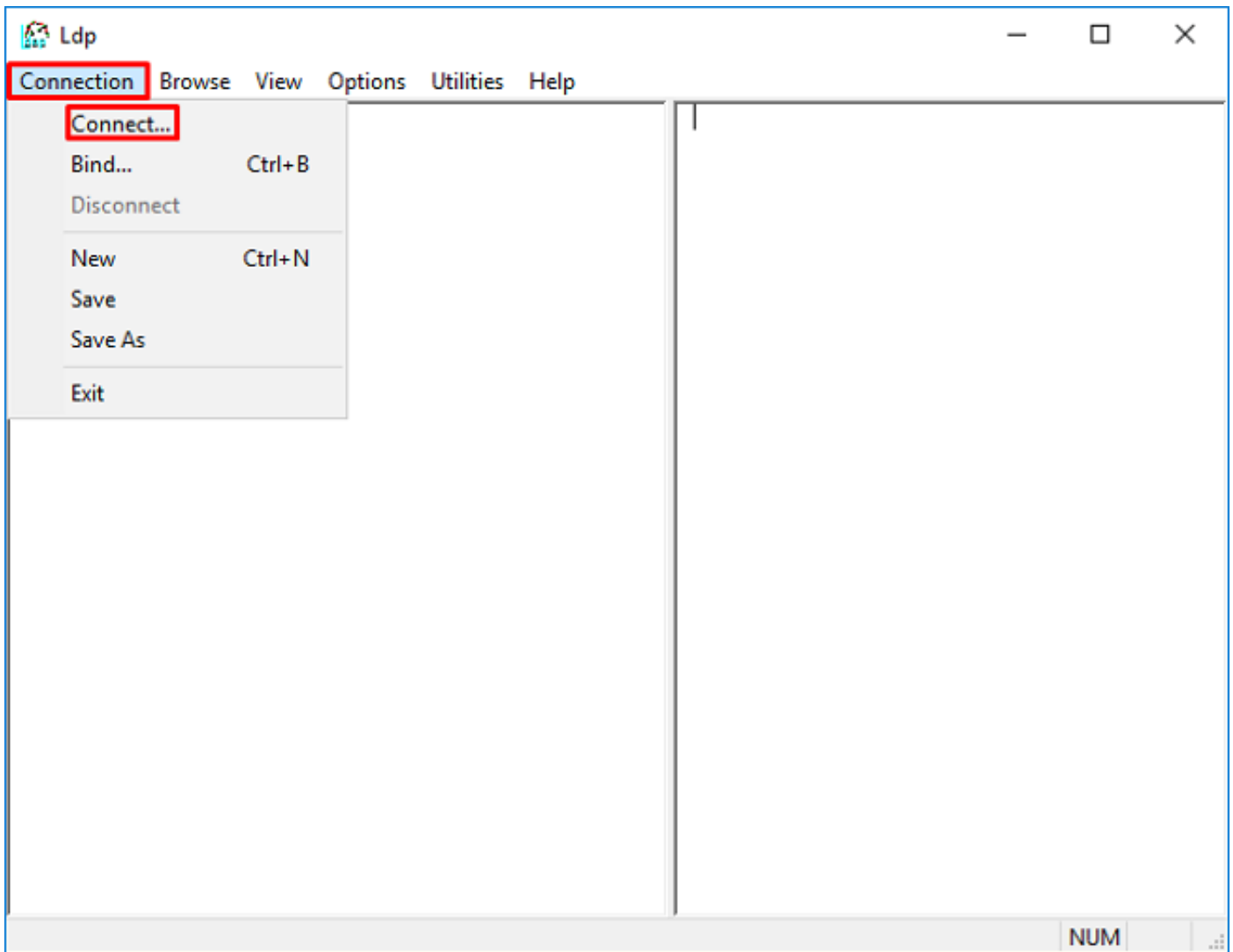
```
[ -2147483615] Session Start
[ -2147483615] New request Session, context 0x00007f9e65ccdc40, reqType = Authentication
[ -2147483615] Fiber started
[ -2147483615] Creating LDAP context with uri=ldap://192.168.1.1:389
[ -2147483615] Connect to LDAP server: ldap://192.168.1.1:389, status = Successful
[ -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
```

潜在解决方案：验证登录DN和登录密码是否已正确配置。这可以在AD服务器上使用ldp.exe进行验证。要验证帐户是否可以成功绑定使用ldp，请浏览以下步骤：

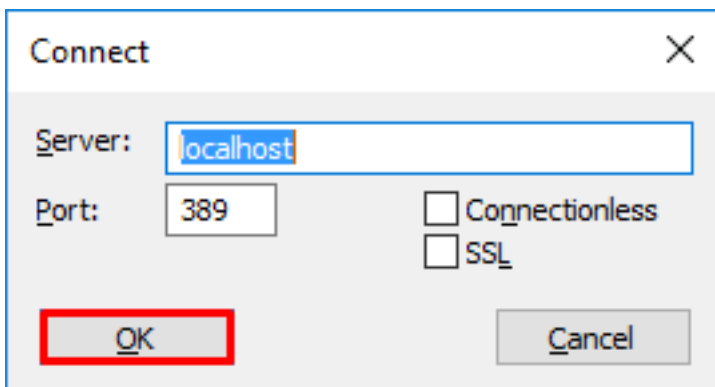
1.在AD服务器上，按Win+R并搜索ldp.exe。



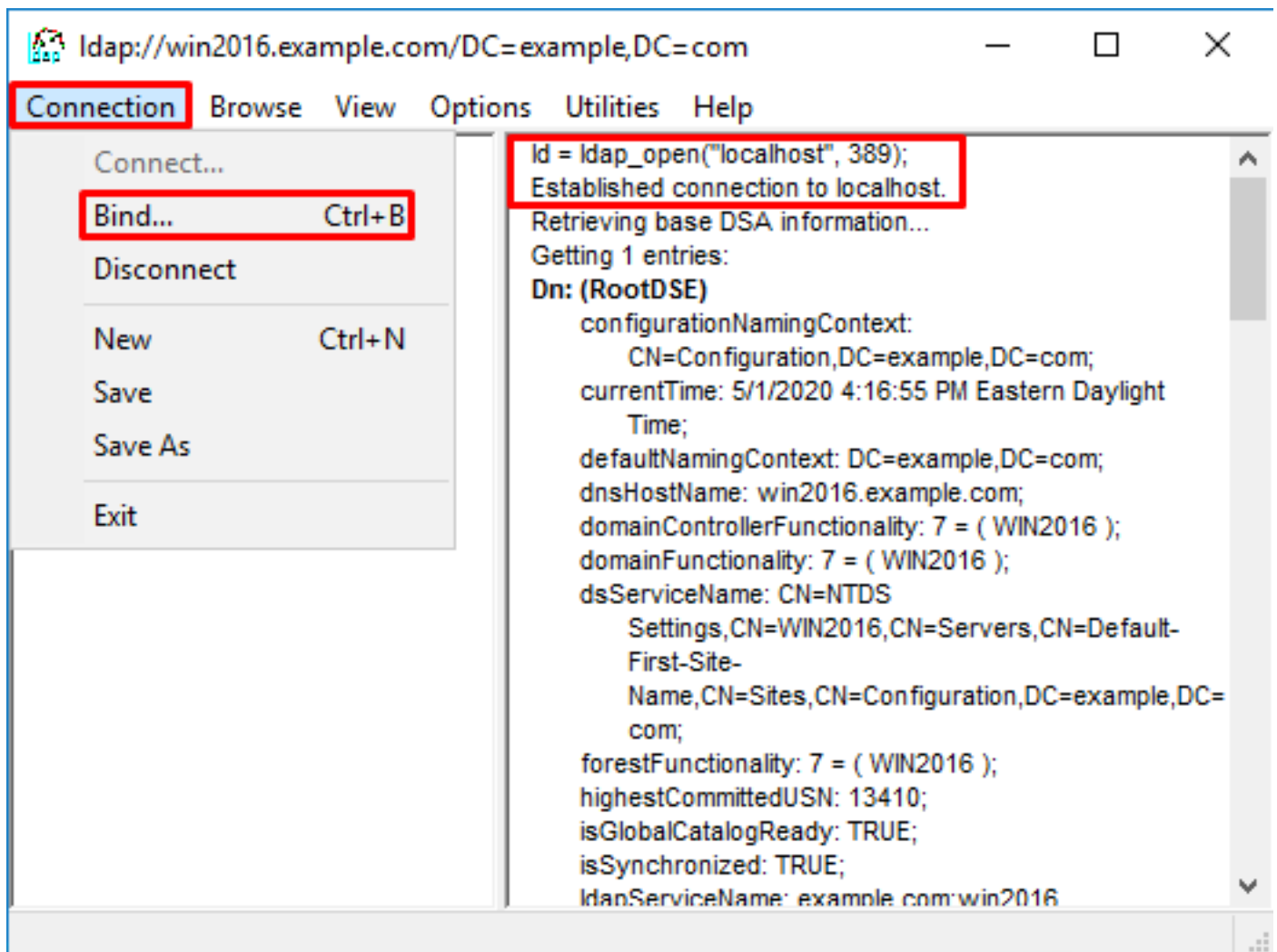
2.单击“连接”>“连接……” 如图所示。



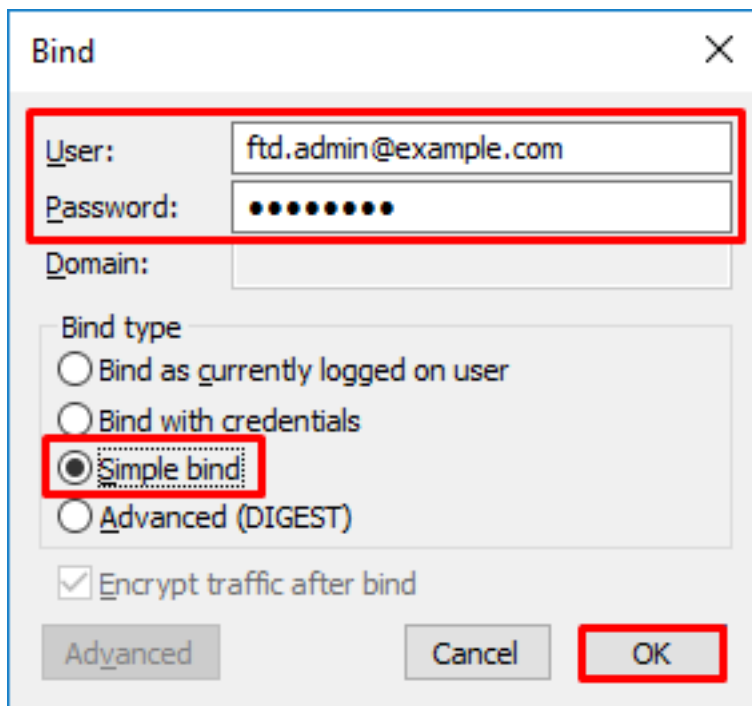
3.为服务器和相应的端口指定localhost，然后单击OK。



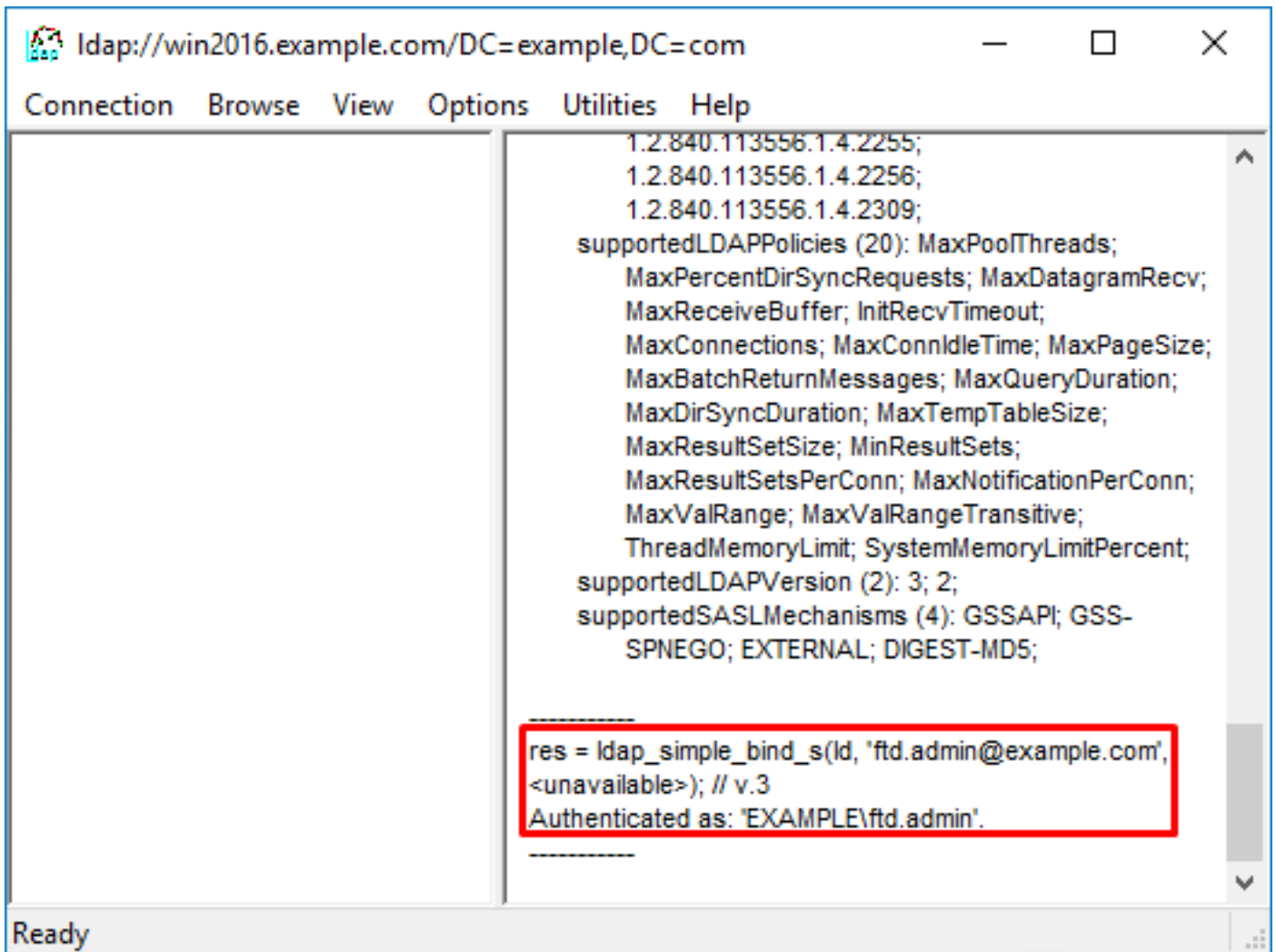
4.右列显示指示连接成功的文本。单击**Connection > Bind...** 如图所示.



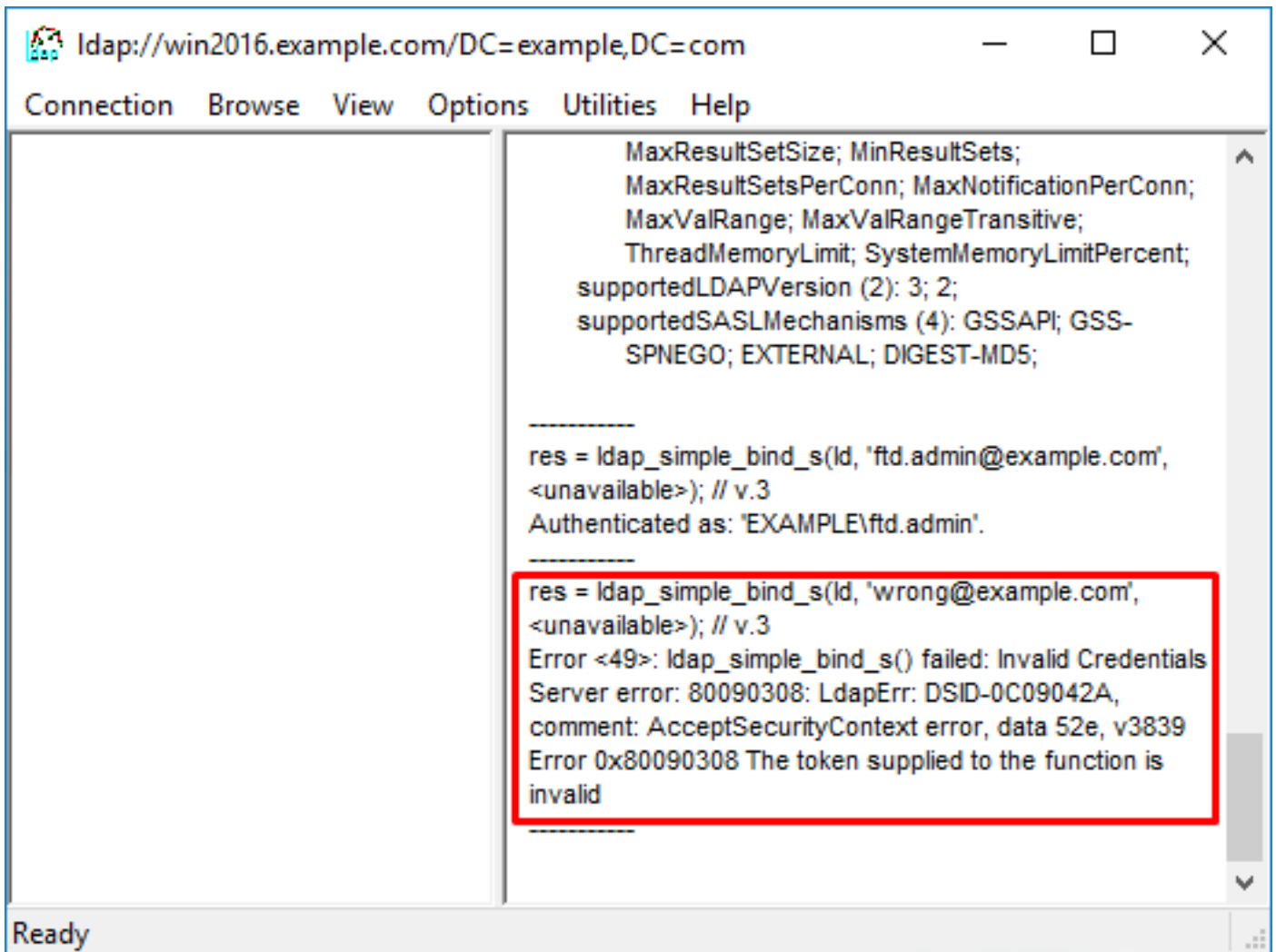
5.选择“简单绑定”，然后指定“目录帐户用户名和密码”。Click OK.



如果绑定成功，则Idp将显示Authenticated为DOMAIN\username。



如果尝试使用无效的用户名或密码进行绑定，将导致此类失败。

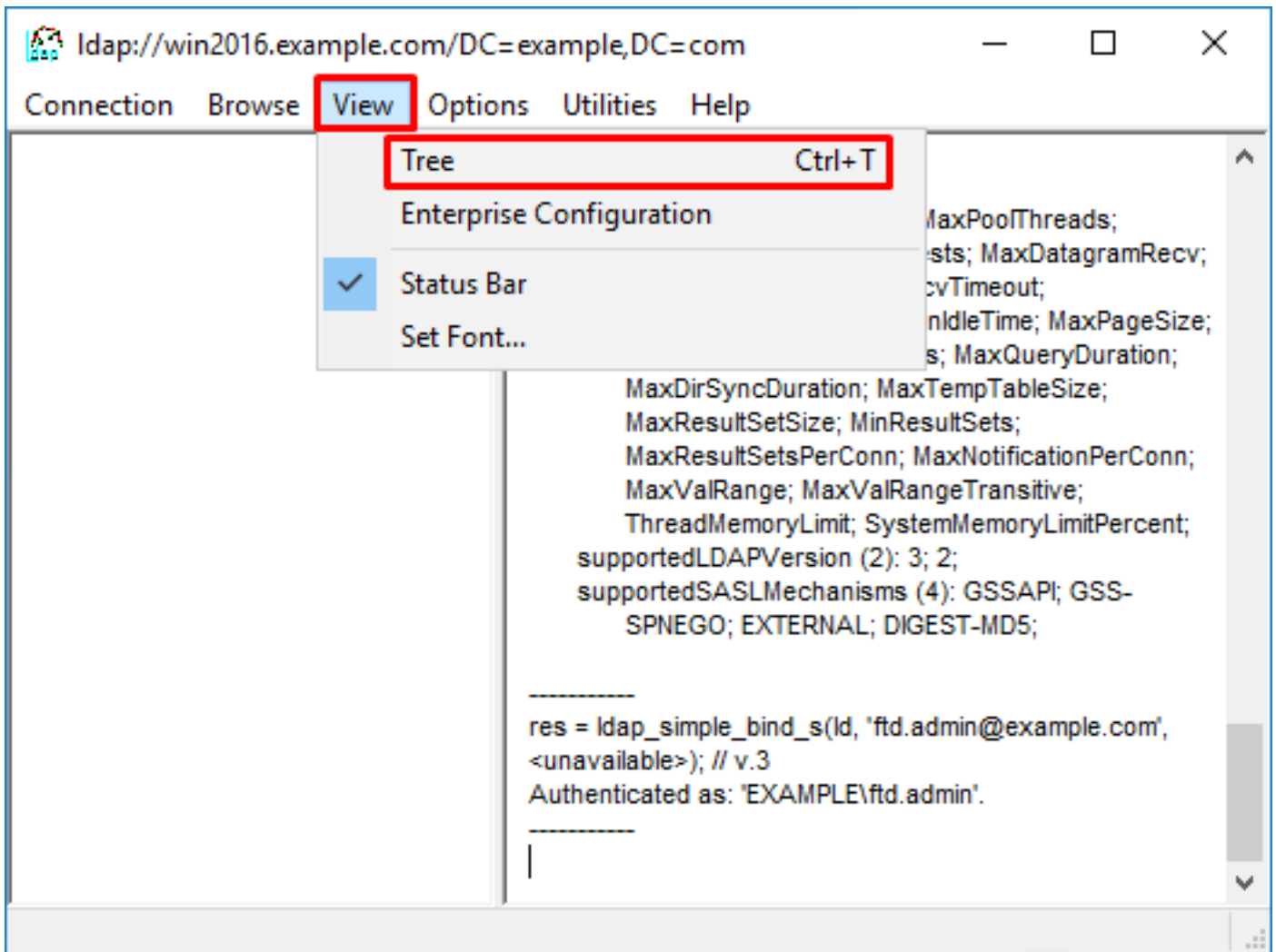


LDAP服务器找不到用户名

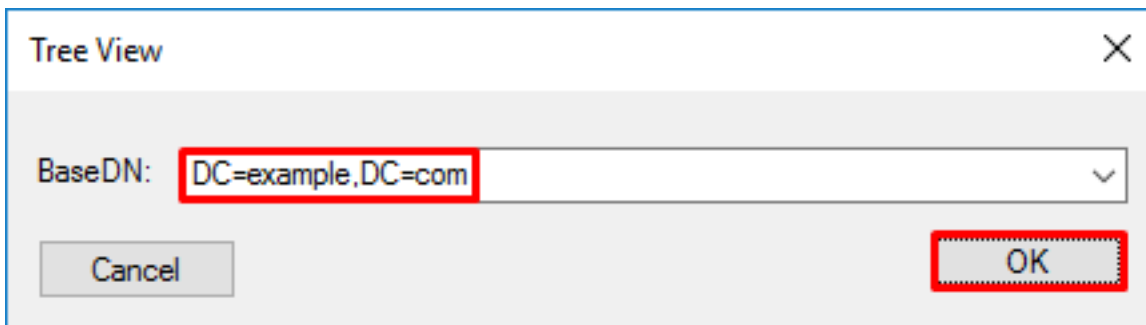
```
[-2147483612] Session Start
[-2147483612] New request Session, context 0x00007f9e65ccdc40, reqType = Authentication
[-2147483612] Fiber started
[-2147483612] Creating LDAP context with uri=ldap://192.168.1.1:389
[-2147483612] Connect to LDAP server: ldap://192.168.1.1:389, status = Successful
[-2147483612] 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
```

潜在解决方案：验证AD是否可以通过FTD完成搜索找到用户。这也可以通过ldp.exe完成。

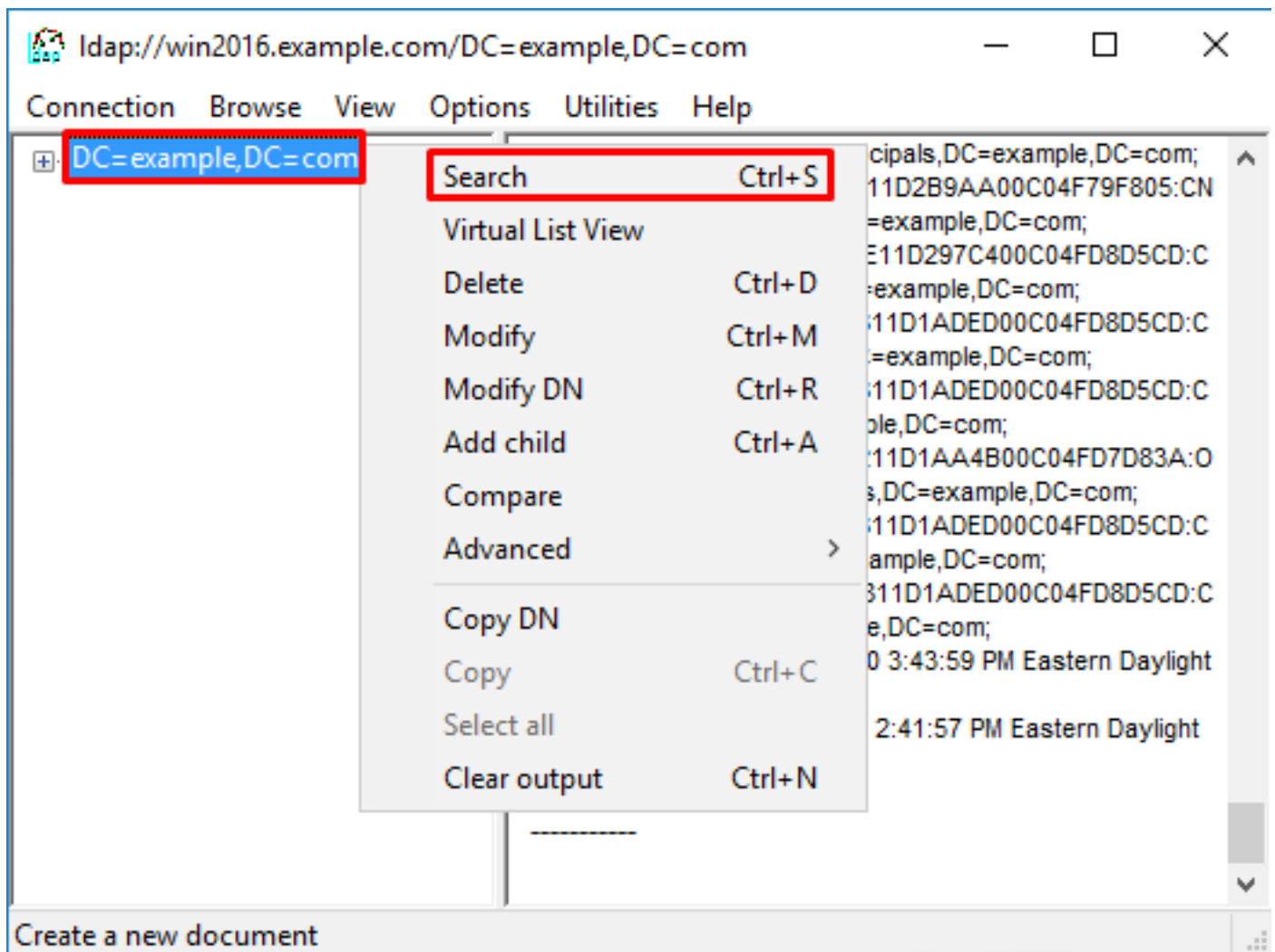
1.成功绑定后，导航至“视图”>“树”，如图所示。



2.指定在FTD上配置的基本DN，然后单击OK。

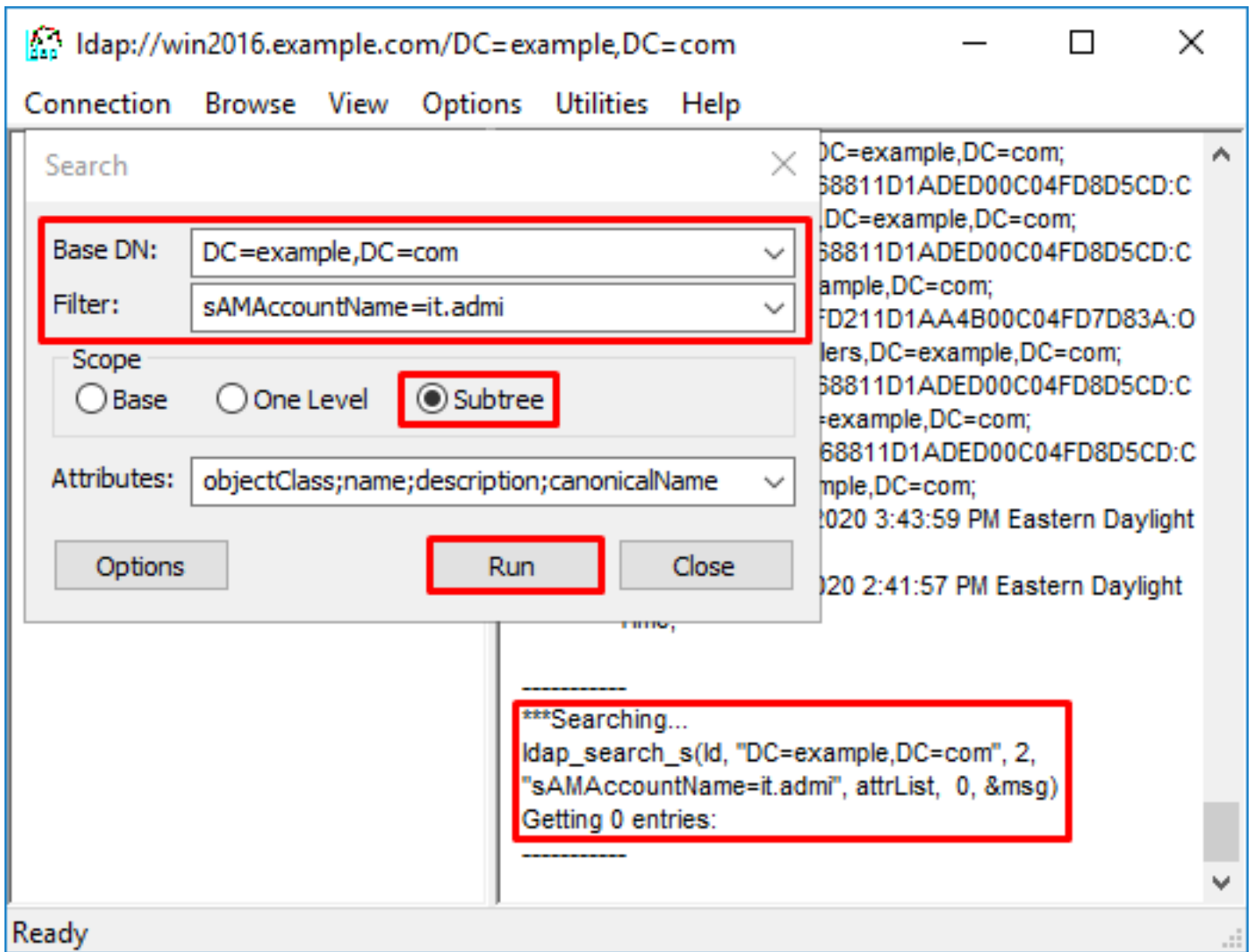


3.右键点击Base DN，然后点击Search，如图所示。



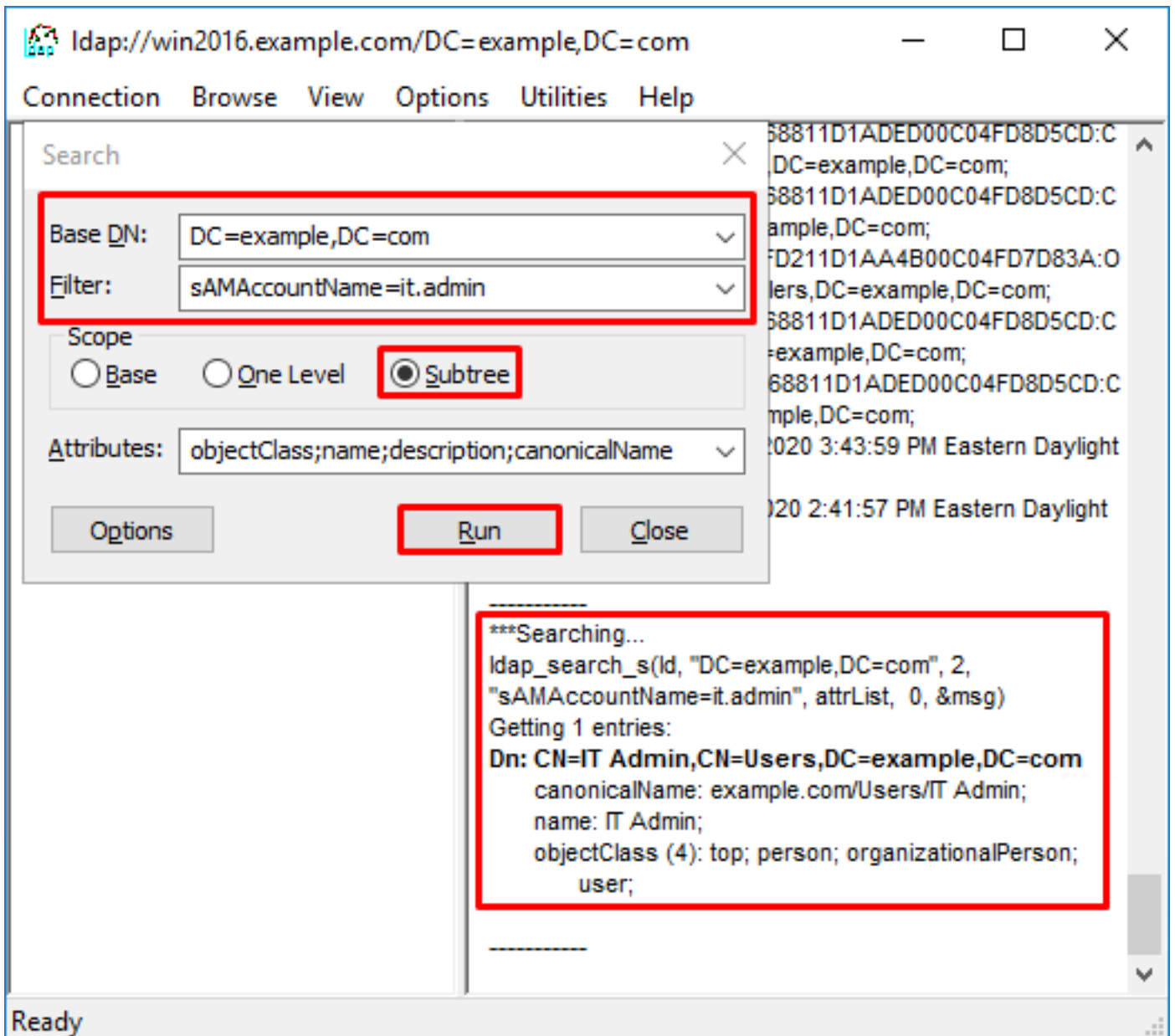
4.指定调试中看到的相同的Base DB、Filter和Scope值。在本例中，以下是：

- 基准 DN:dc=example , dc=com
- 过滤器 : samaccountname=it.admi
- 范围 : 子树



ldap查找0个条目，因为在Base DN dc=example，dc=com下没有具有sAMAccountName=it.admi的用户帐户。

再次尝试使用正确的sAMAccountName=it.admin显示的结果不同。ldap在Base DN dc=example，dc=com下查找1个条目并打印该用户的DN。



用户名的密码不正确

```

[-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, data 52e, v3839
[-2147483613] Invalid password for it.admin
[-2147483613] Fiber exit Tx=514 bytes Rx=2764 bytes, status=-1
[-2147483613] Session End
```

潜在解决方案：验证用户的密码是否配置正确且未过期。与登录DN类似，FTD将使用用户凭证对AD进行绑定。此绑定也可以在ldp中完成，以验证AD是否能够识别相同的用户名和密码凭证。ldp中的步骤显示在绑定登录DN和/或密码不正确部分中。此外，还可以出于可能的原因查看Microsoft服务器事件查看器日志。

测试AAA

test aaa-server命令可用于使用特定用户名和密码模拟来自FTD的身份验证尝试。这可用于测试连接或身份验证失败。命令是test aaa-server authentication [AAA-server] host [AD IP/hostname]。

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

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

数据包捕获

数据包捕获可用于验证到AD服务器的可达性。如果LDAP数据包离开FTD，但没有响应，这可能表示路由问题。

以下是显示双向LDAP流量的捕获完成：

```
> show route 192.168.1.1

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

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

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

> test aaa-server authentication LAB-AD host win2016.example.com username it.admin password
*****
```

```
INFO: Attempting Authentication test to IP address (192.168.1.1) (timeout: 12 seconds)
INFO: Authentication Successful
```

```
> show capture
```

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

```
> show capture AD
```

```
54 packets captured
```

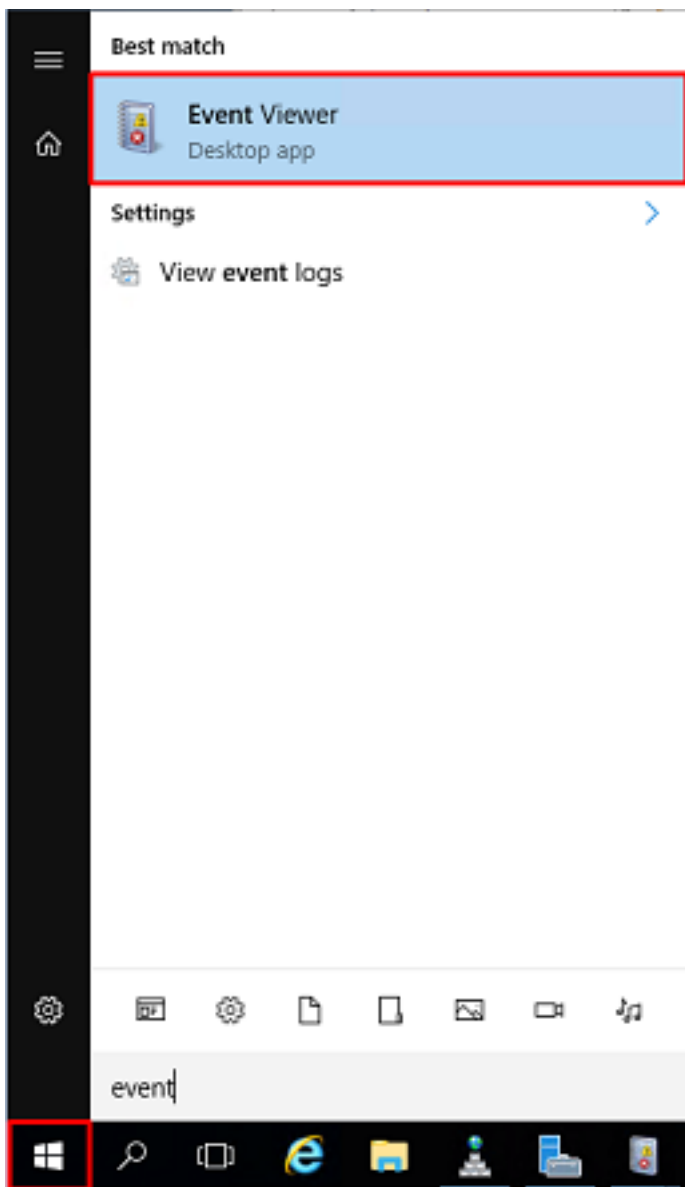
```
  1: 23:02:16.770712      192.168.1.17.61960 > 192.168.1.1.389: S 3681912834:3681912834(0) win
32768 <mss 1460,nop,nop,timestamp 1061373057 0>
  2: 23:02:16.772009      192.168.1.1.389 > 192.168.1.17.61960: S 491521506:491521506(0) ack
3681912835 win 8192 <mss 1460,nop,nop,timestamp 762393884 1061373057>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

```
54 packets shown
```

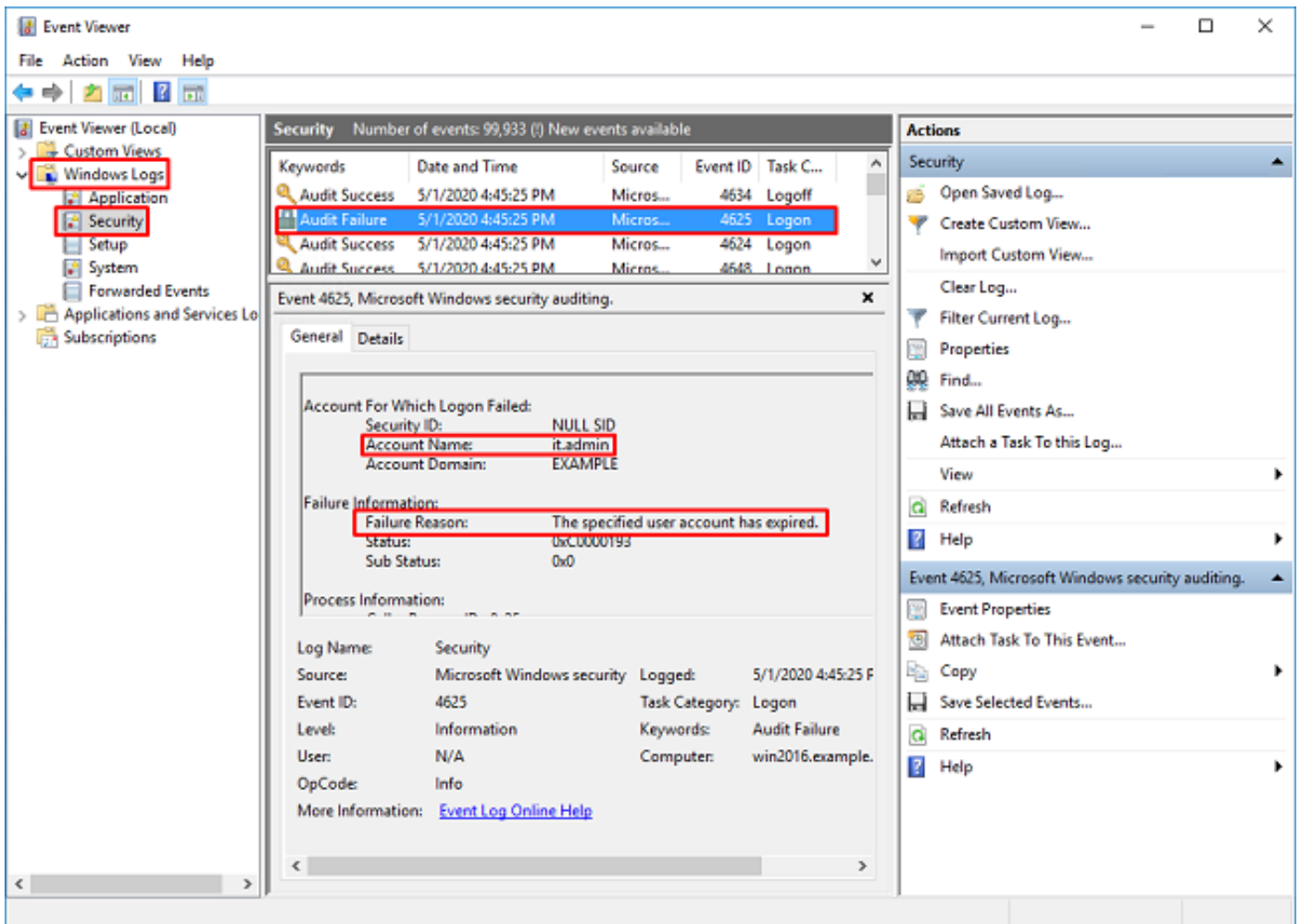
Windows Server事件查看器日志

AD服务器范上的事件查看器日志提供了有关失败原因的更多详细信息。

1.搜索并打开事件查看器。



2.展开“Windows日志”并单击“安全”。使用用户的帐户名搜索“审核失败”，并查看“失败信息”，如图所示。



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