

在由 FMC 管理的面向 AnyConnect 客户端的 FTD 上配置 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](#)

[背景信息](#)

[配置](#)

[网络图和场景](#)

[Active Directory配置](#)

[确定LDAP基本DN和组DN](#)

[创建FTD帐户](#)

[创建AD组并将用户添加到AD组 \(可选\)](#)

[复制LDAPS SSL证书根 \(仅对于LDAPS或STARTTLS是必需的\)](#)

[FMC配置](#)

[验证许可](#)

[设置领域](#)

[配置AnyConnect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](#)

[配置NAT免除](#)

[部署](#)

[验证](#)

[最终配置](#)

[AAA配置](#)

[AnyConnect配置](#)

[使用AnyConnect连接并验证访问控制策略规则](#)

[使用FMC连接事件进行验证](#)

[故障排除](#)

[调试](#)

[正在运行的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

本文档介绍如何为连接到思科Firepower威胁防御(FTD)的AnyConnect客户端配置AD身份验证。

先决条件

要求

Cisco 建议您了解以下主题：

- 基本了解FMC上的RA VPN配置
- 基本了解FMC上的LDAP服务器配置
- Active Directory(AD)基础知识

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FMCv
- 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。

背景信息

本文档介绍如何为连接到Cisco Firepower威胁防御(FTD)(由Firepower管理中心(FMC)管理)的AnyConnect客户端配置Active Directory(AD)身份验证。

用户身份用于访问策略，以将AnyConnect用户限制为特定IP地址和端口。

配置

网络图和场景



Windows服务器预配置了IIS和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：用作目录帐户，以允许FTD绑定到Active Directory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 Admins：添加IT管理员以演示用户身份的测试组。此组仅对Windows Server具有RDP访问权限。
- AnyConnect用户：添加测试用户以展示用户身份的测试组。此组仅对Windows Server具有HTTP访问权限。

Active Directory配置

要在FTD上正确配置AD身份验证和用户身份，需要几个值。

在FMC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。主要值包括：

- **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FMC和FTD中配置DNS服务器以解析FQDN。

在本配置指南中，此值为win2016.example.com（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使用TCP端口389进行LDAP，LDAP over SSL(LDAPS)使用TCP端口636。

- **根CA：**

如果使用LDAPS或STARTTLS，则需要用于签署LDAPS所用SSL证书的根CA。

- **目录用户名和密码：**

这是FMC和FTD用于绑定到LDAP服务器、对用户进行身份验证以及搜索用户和组的帐户。

为此创建了一个名为FTD Admin的帐户。

- **基础和组可分辨名称(DN)：**

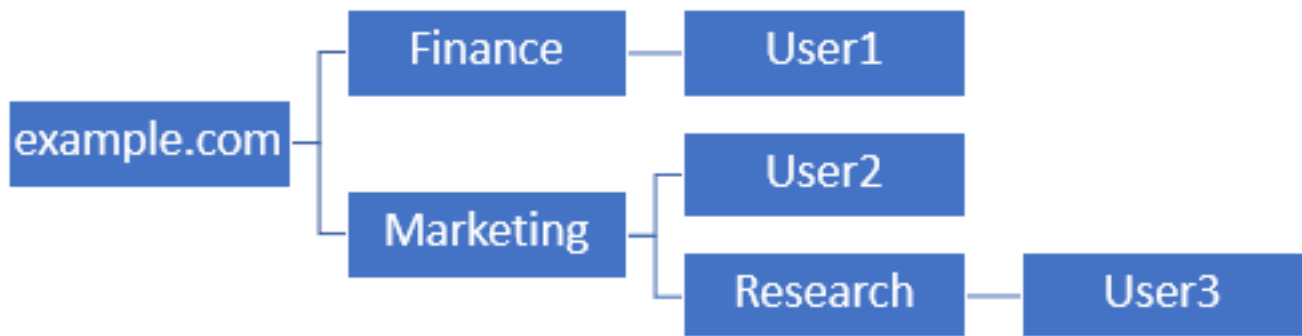
基础DN是FMC的起点，FTD告知Active Directory开始搜索和验证用户。

同样，组DN是起点，FMC告知Active Directory从何处开始搜索用户身份组。

在本配置指南中，根域example.com用作基础DN和组DN。

但是，对于生产环境，在LDAP层次结构中进一步使用Base DN和Group DN会更好。

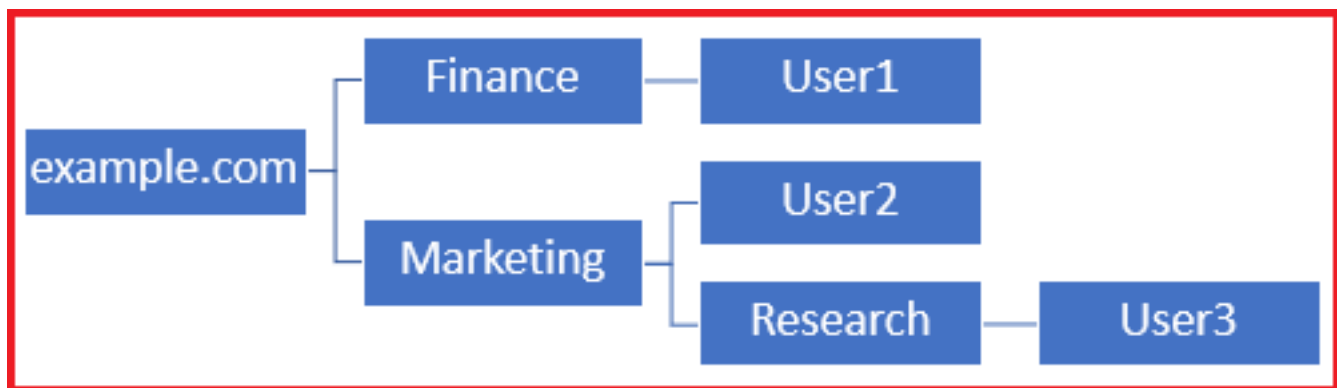
例如，此LDAP层次结构：



如果管理员希望**Marketing**组织单位内的用户能够验证基本DN，可以将基本DN设置为根(example.com)。

但是，这也允许**Finance**组织单元下的User1登录，因为用户搜索从根目录开始，然后转到**Finance**、**Marketing**和**Research**。

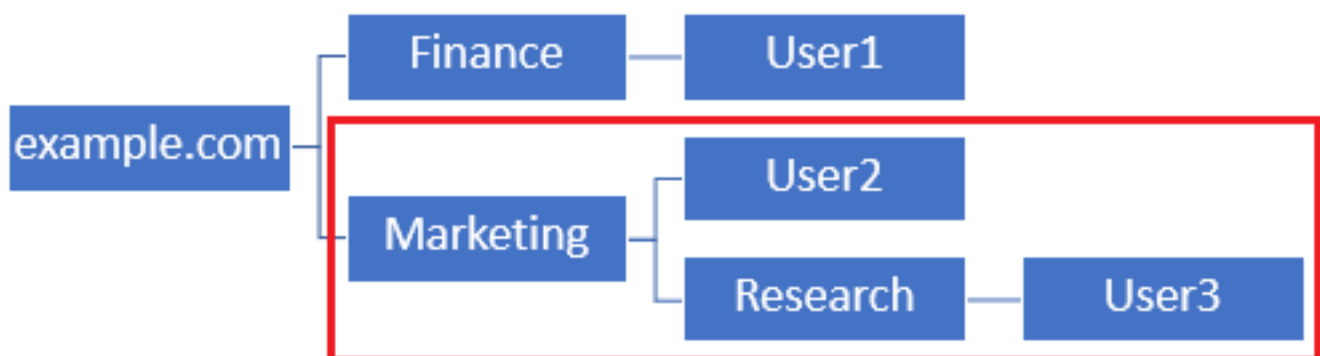
基本DN设置为example.com



要将登录限制为**Marketing**组织单位及以下单位中的唯一用户，管理员可以将Base DN设置为**Marketing**。

现在只有User2和User3能够进行身份验证，因为搜索从**Marketing**开始。

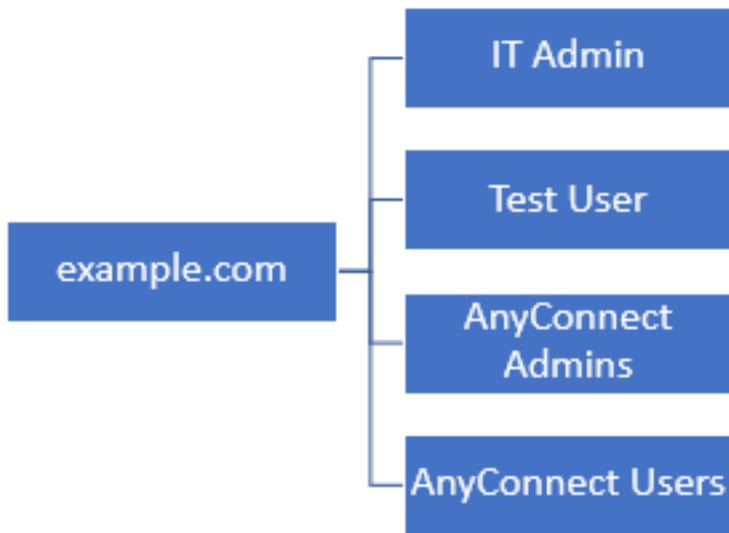
基本DN设置为Marketing



请注意，为了在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。

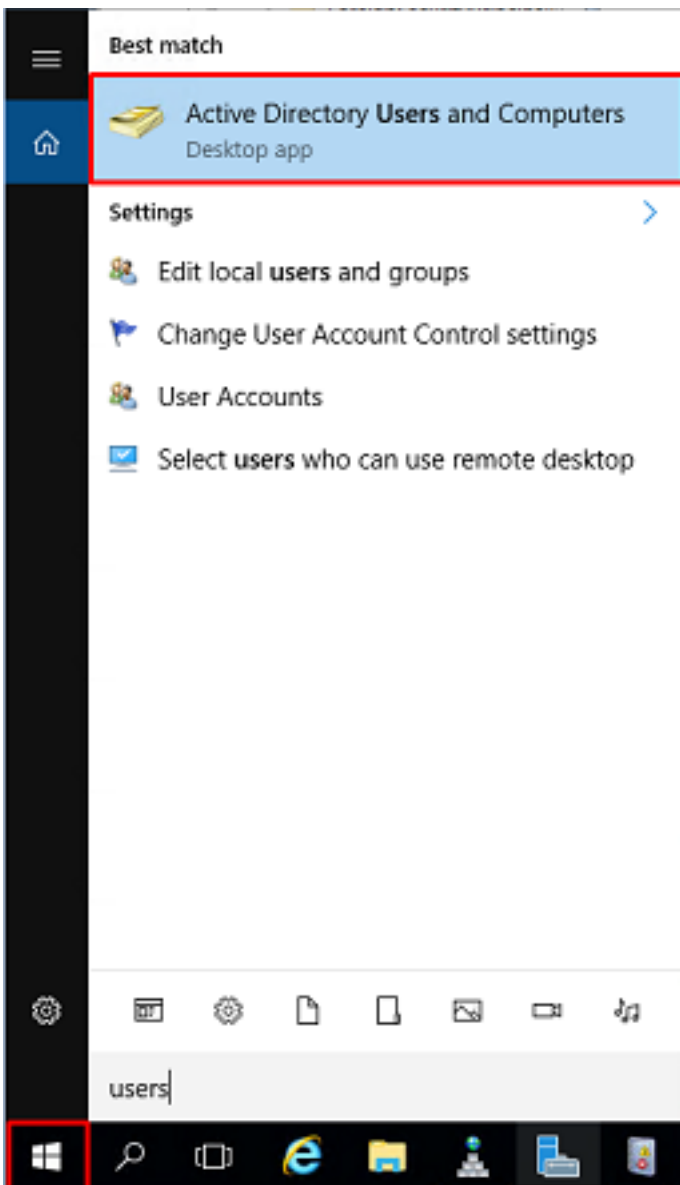
有关这方面的详细信息，请参阅：[在Firepower威胁防御\(FTD\)上配置AnyConnect LDAP映射](#)。

此配置指南中使用此简化的LDAP层次结构，根example.com的DN用于基础DN和组DN。

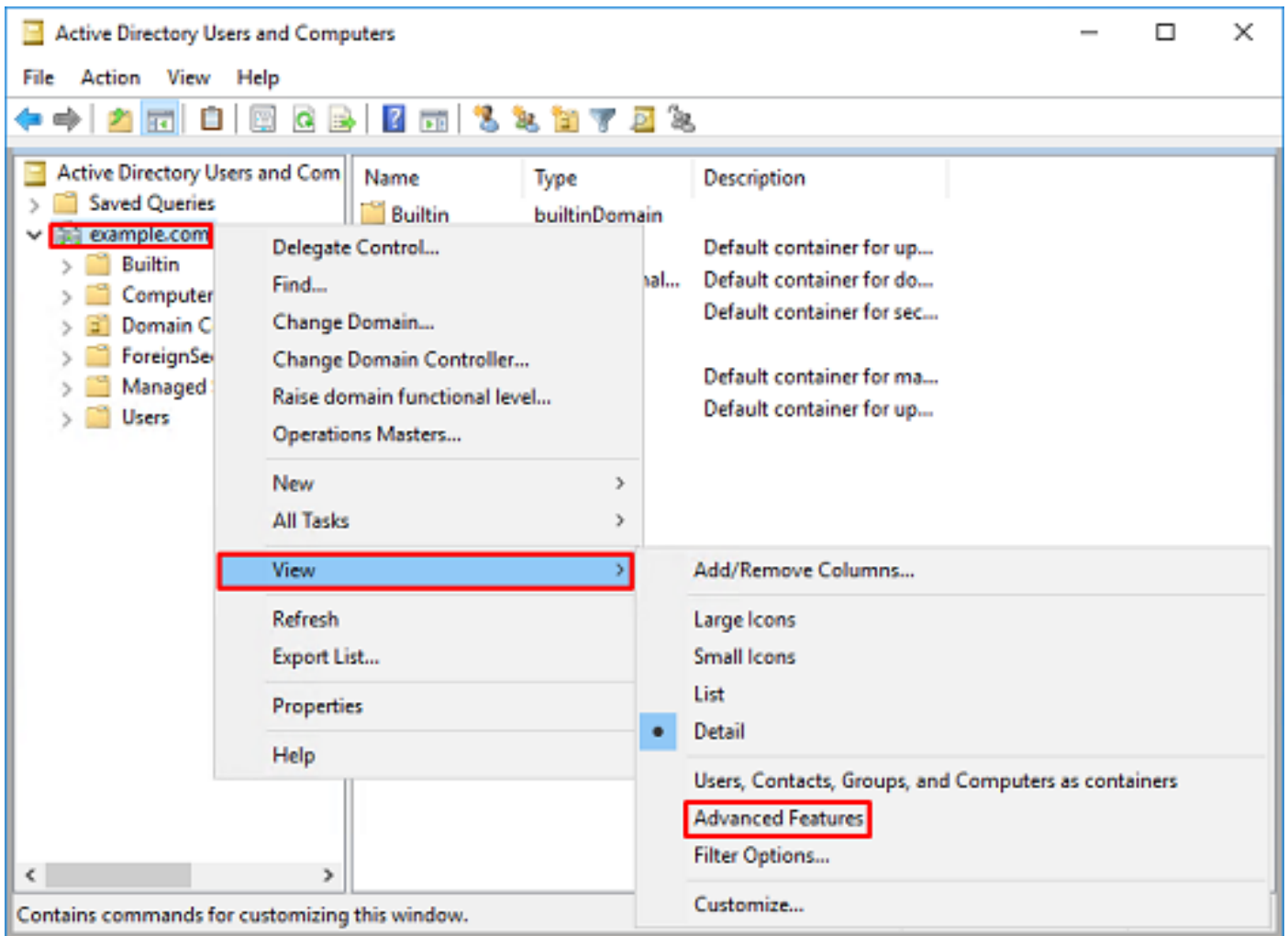


确定LDAP基本DN和组DN

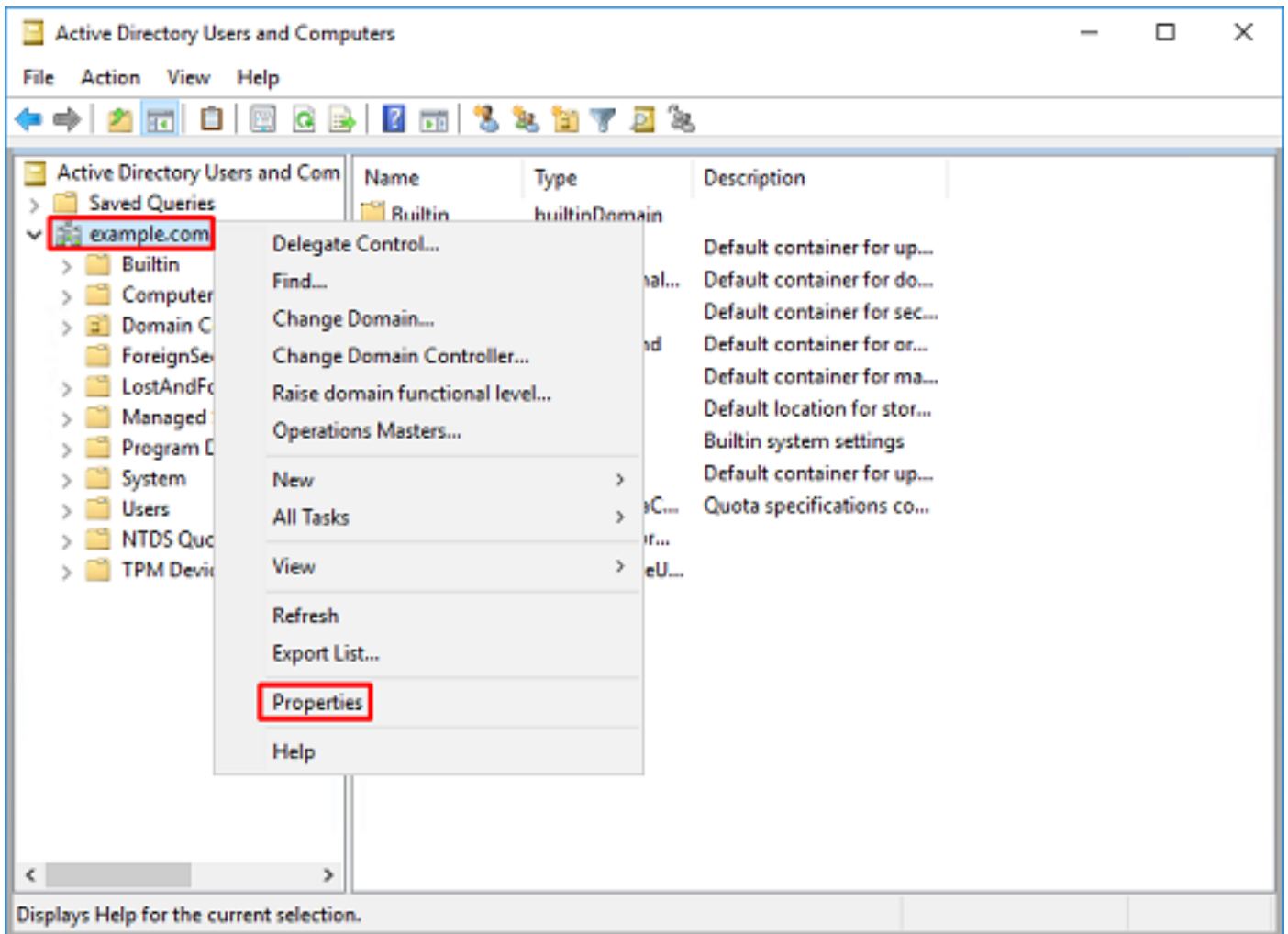
1. 打开Active Directory用户和计算机。



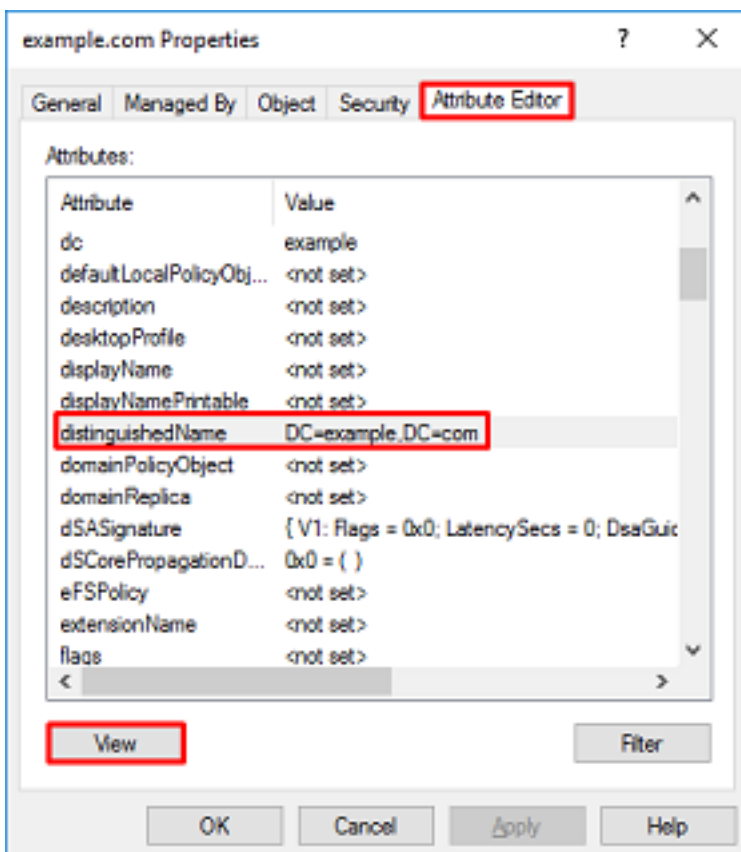
2. 左键点击根域（打开容器），右键点击根域，然后在视图下单击高级功能。



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，然后选择**Properties**。

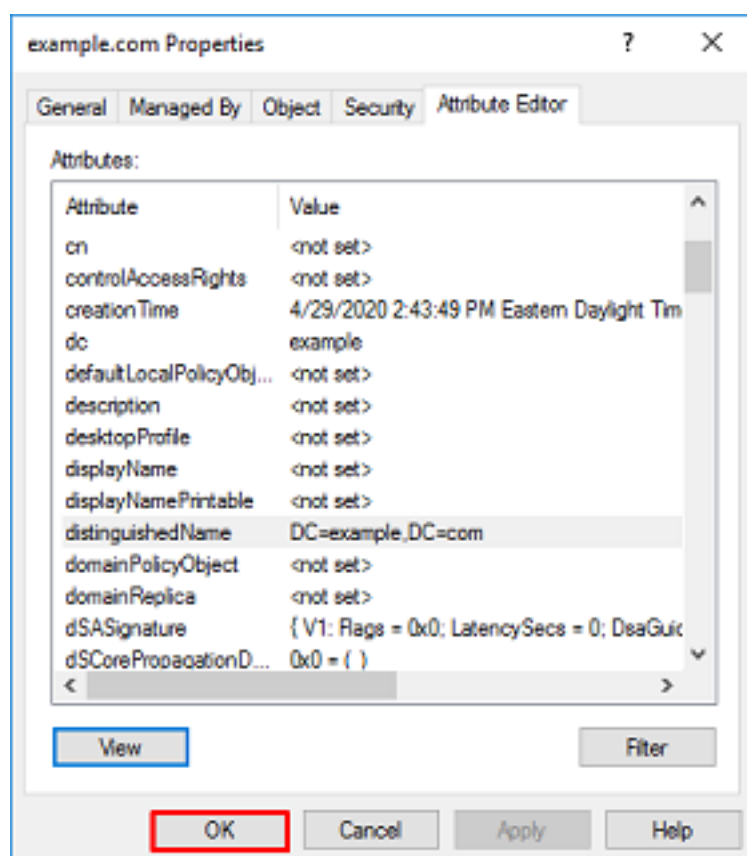
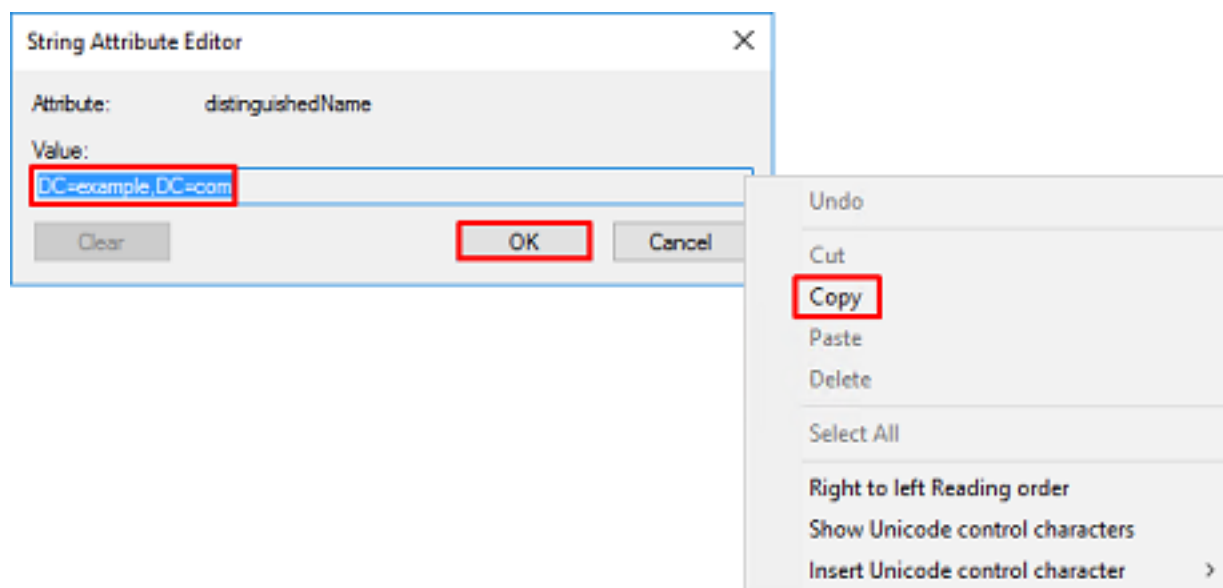


4. 在 **Properties** 下，选择 **Attribute Editor** 选项卡。在 **Attributes** 下查找 **distinguishedName**，然后单击 **View**。

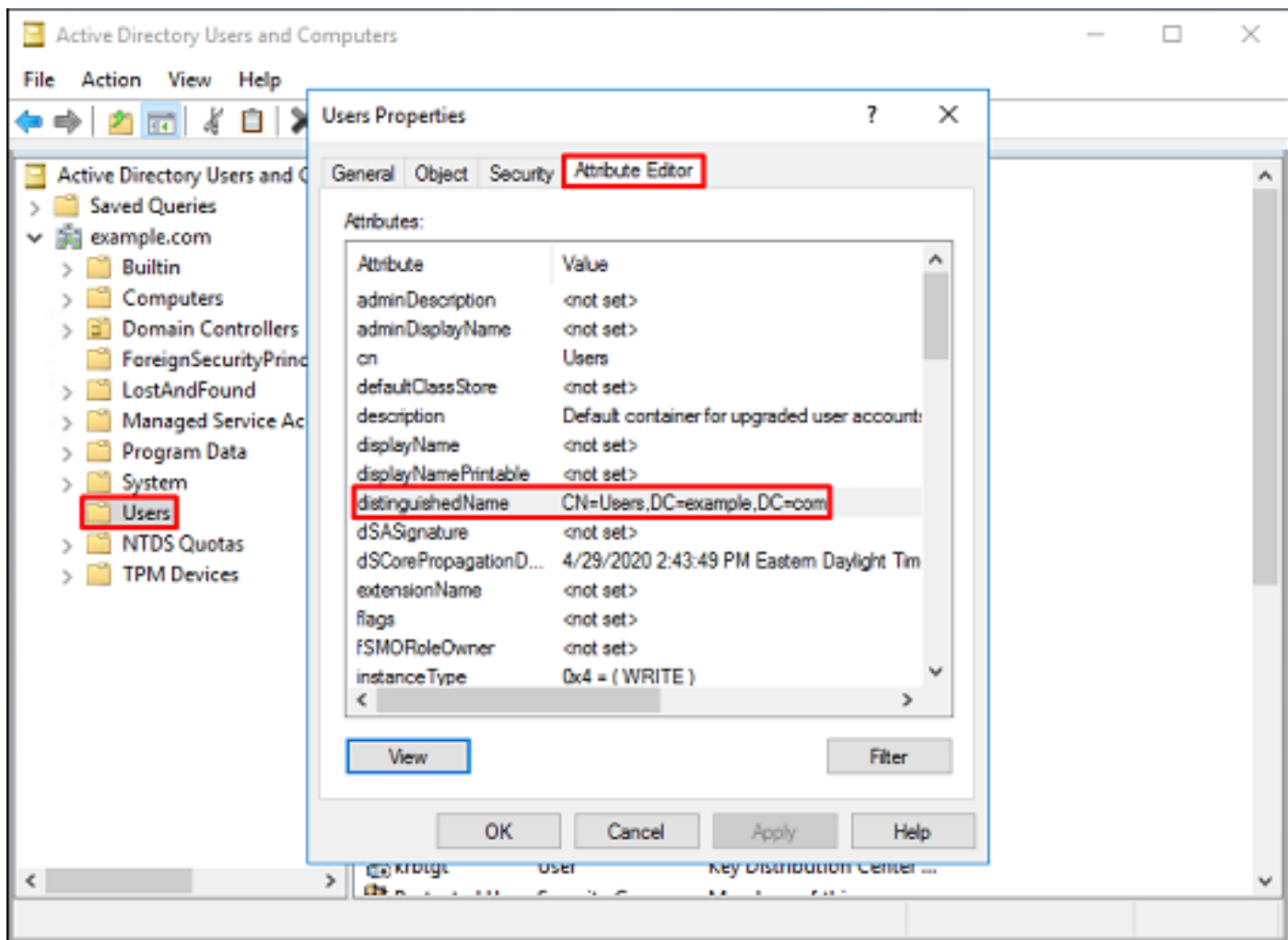


5. 这将打开一个新窗口，以后可以在其中复制并粘贴到FMC中。在本示例中，根DN为DC=example, DC=com。

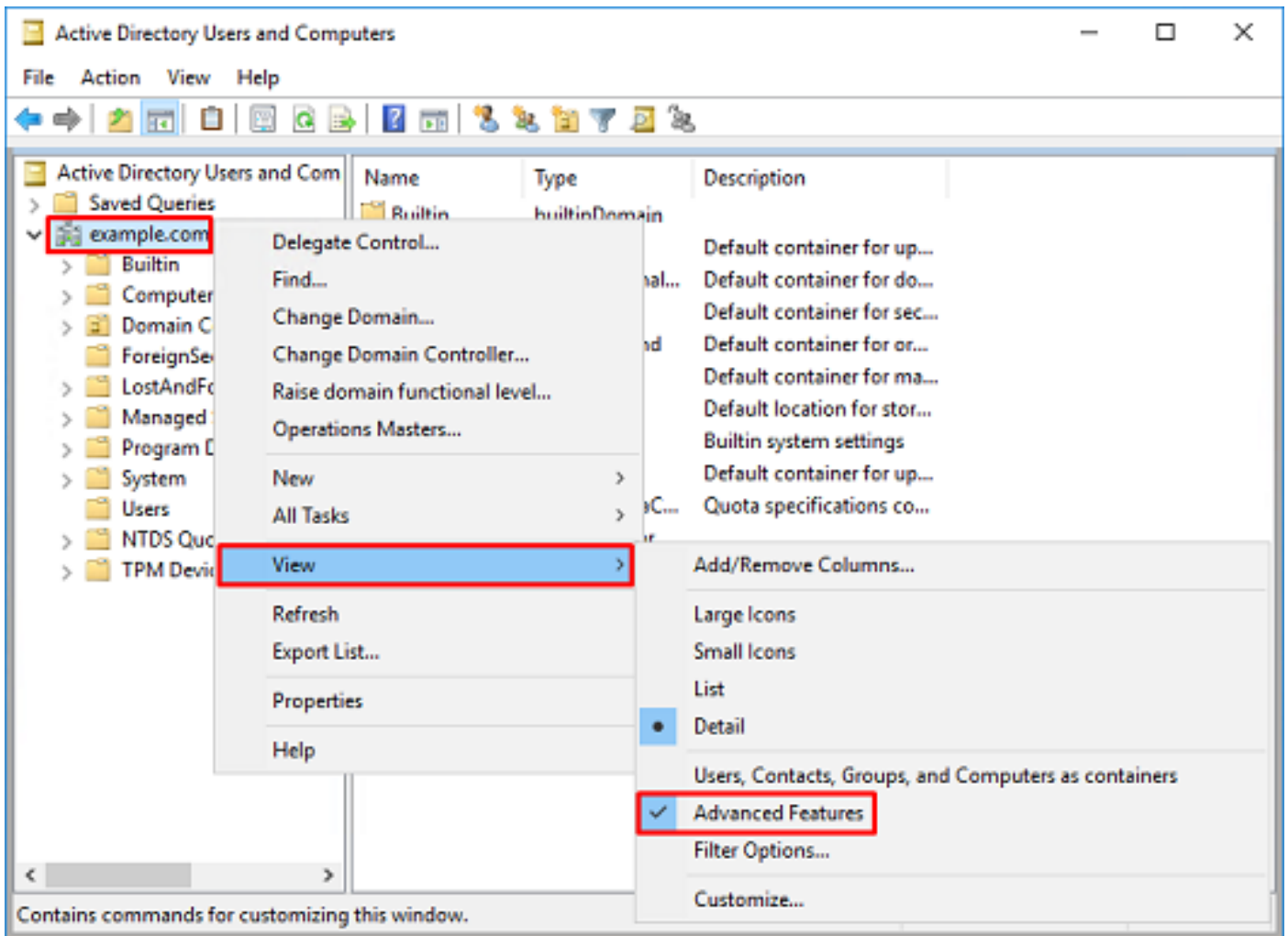
复制值，保存以备后用。单击OK退出String Attribute Editor窗口，然后再次单击OK退出Properties。



这可以对Active Directory中的多个对象执行此操作。例如，这些步骤用于查找User容器的DN:



6.再次右键单击根DN，然后在View下再次单击Advanced Features，可以删除Advanced Features视图。



创建FTD帐户

此用户帐户允许FMC和FTD与Active Directory绑定，以搜索用户和组并对用户进行身份验证。

创建单独的FTD帐户的目的是，在用于绑定的凭证遭到入侵时，防止未经授权访问网络内的其他位置。

此帐户无需在基础DN或组DN范围内。

1.在Active Directory用户和计算机中，右键单击FTD帐户添加到的容器/组织。

在此配置中，FTD帐户将添加到用户名ftd.admin@example.com下的**Users**容器下。

右键单击**Users**，然后导航到**New > User**。

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:

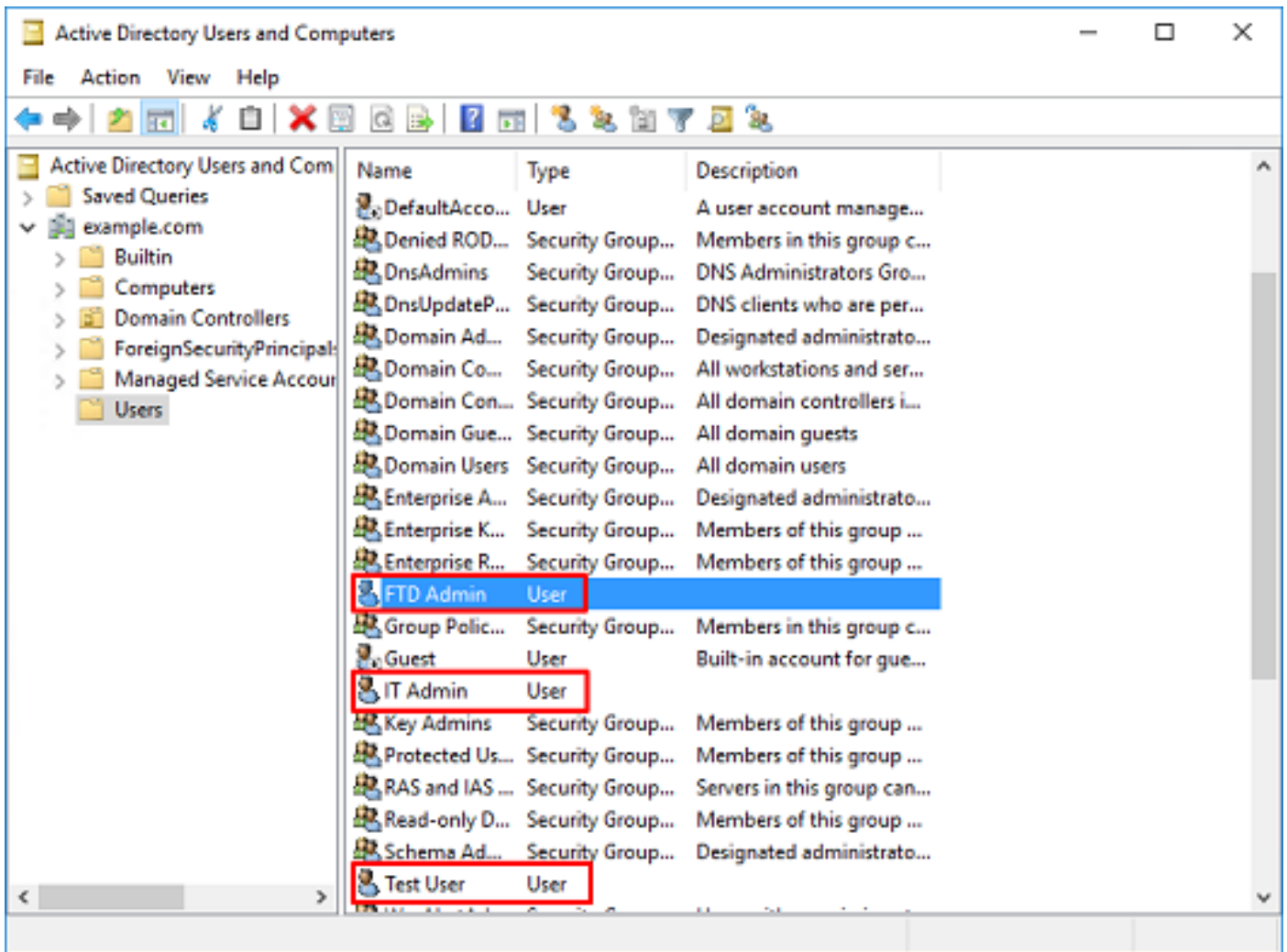
Full name: FTD Admin

User logon name: ftd.admin@example.com

The password never expires.

< Back Finish Cancel

3.验证是否已创建FTD帐户。另外创建了两个帐户：IT管理员和测试用户。



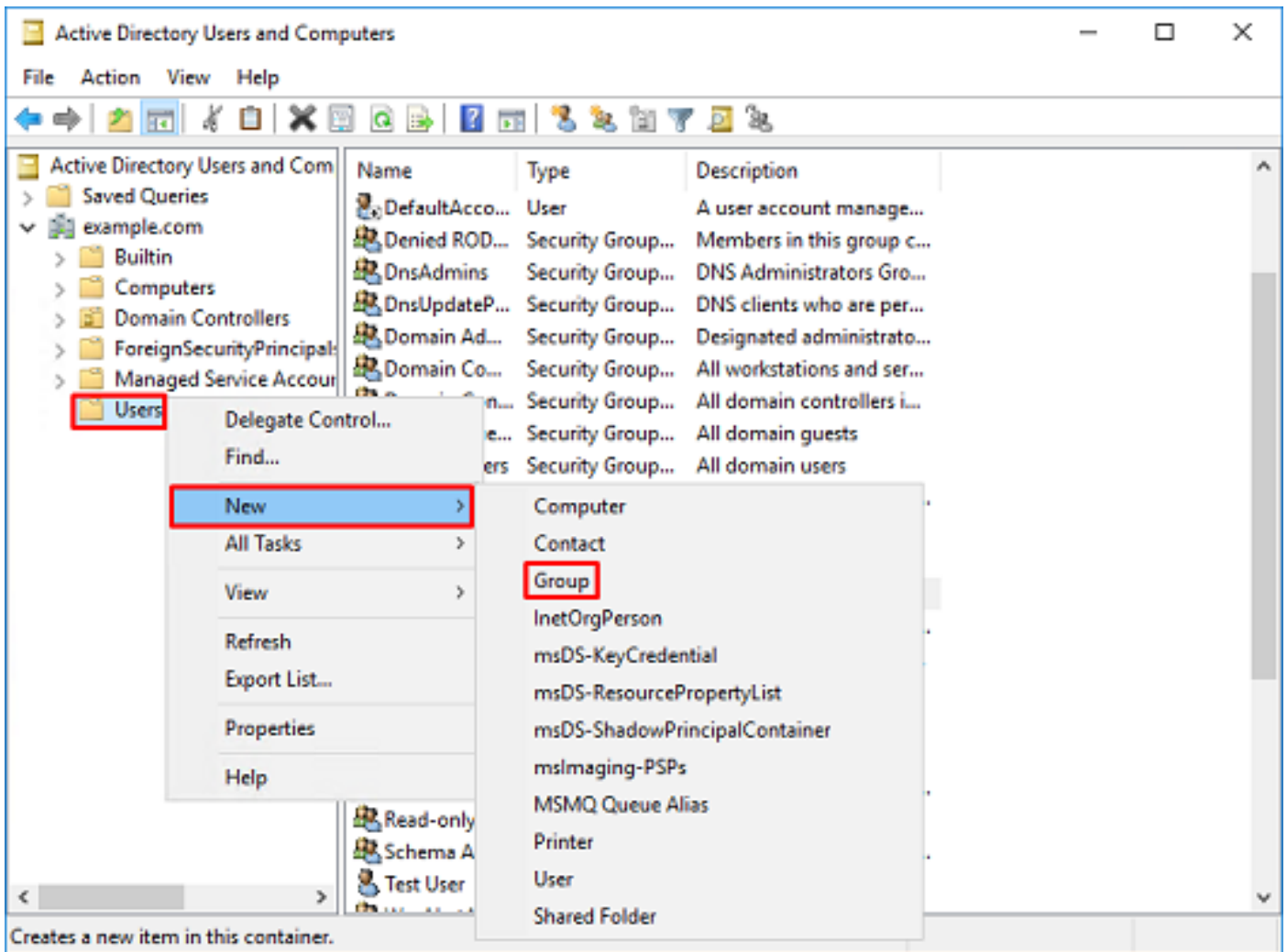
创建AD组并将用户添加到AD组（可选）

虽然身份验证不需要，但可以使用组来简化将访问策略应用至多个用户以及LDAP授权的过程。

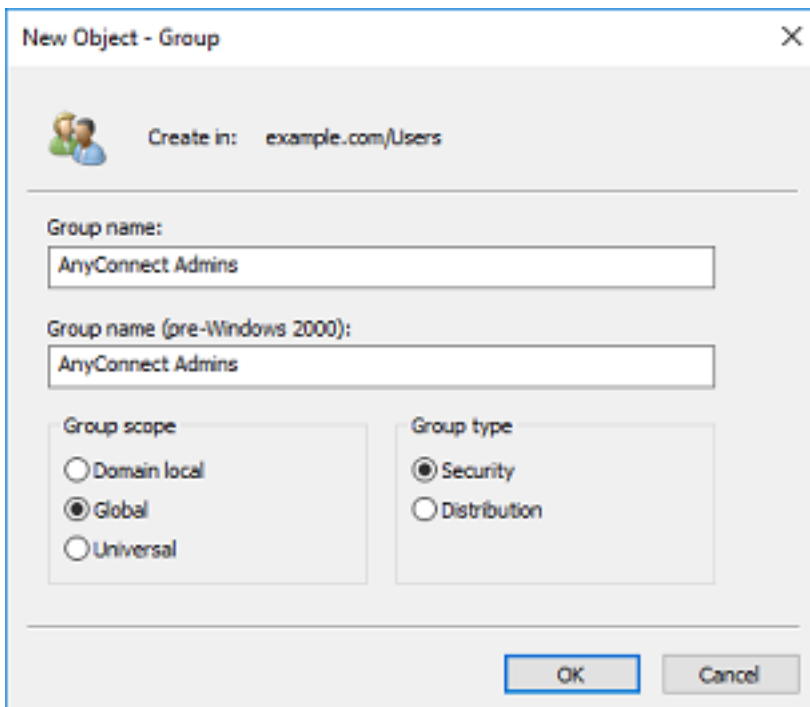
在本配置指南中，组稍后用于通过FMC内的用户身份应用访问控制策略设置。

1. 在Active Directory用户和计算机中，右键单击新组添加到的容器或组织单位。

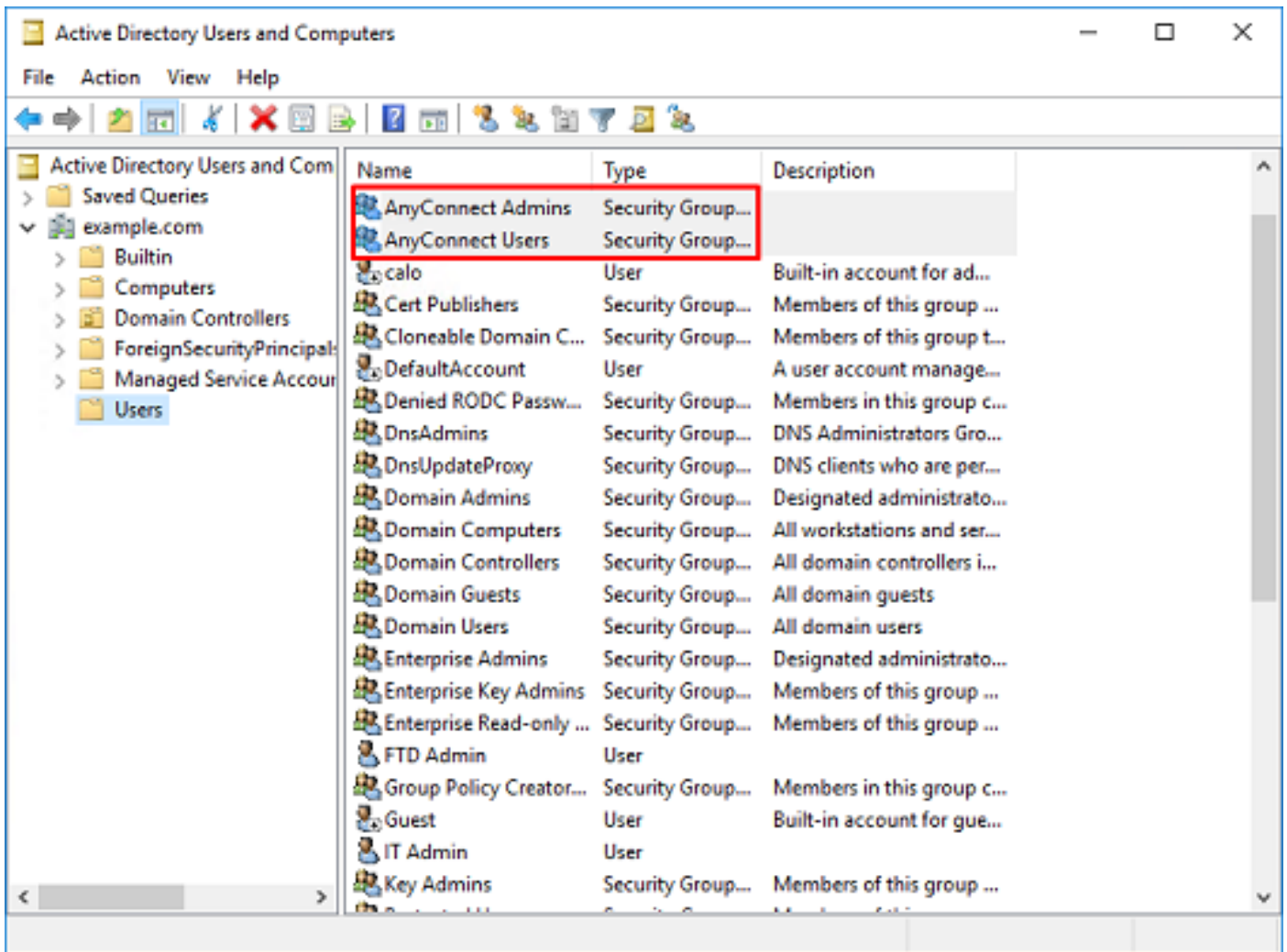
在本示例中，AnyConnect Admins组被添加到Users容器下。右键单击Users，然后导航到New > Group。



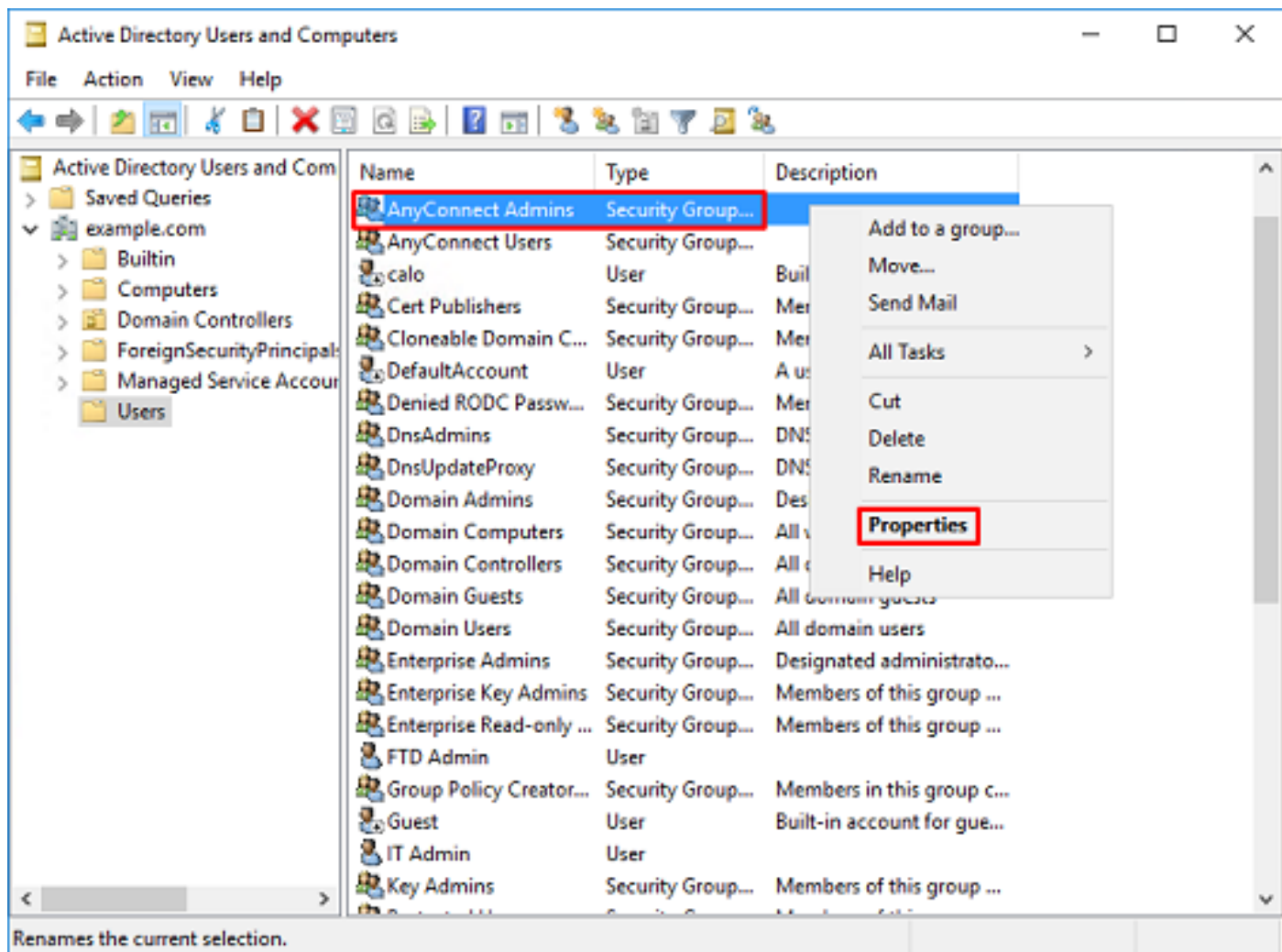
2. 执行“新建对象 — 组”向导。



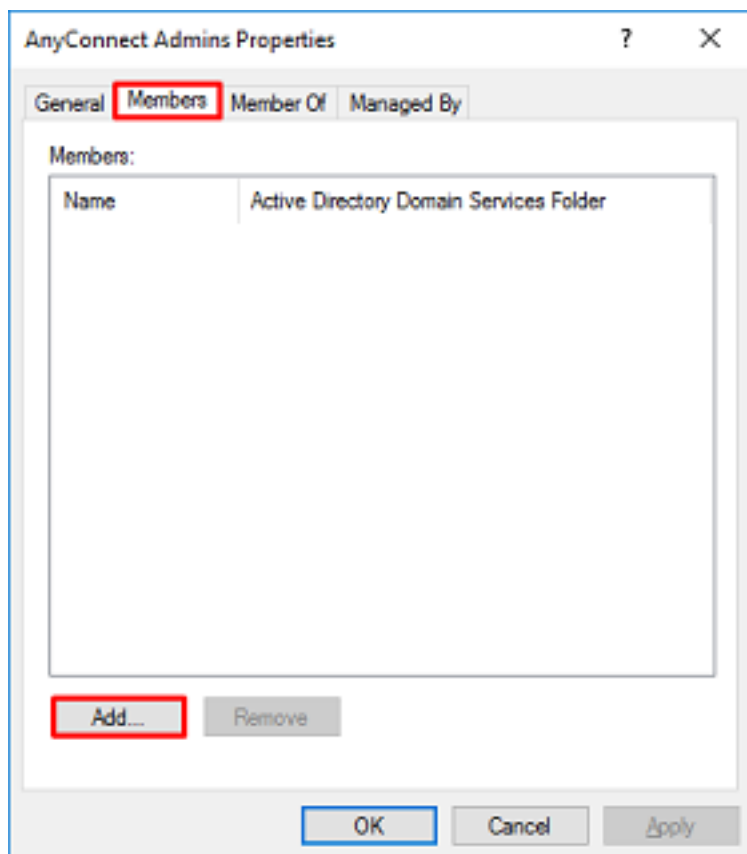
3. 确认已创建组。AnyConnect Users组也将创建。



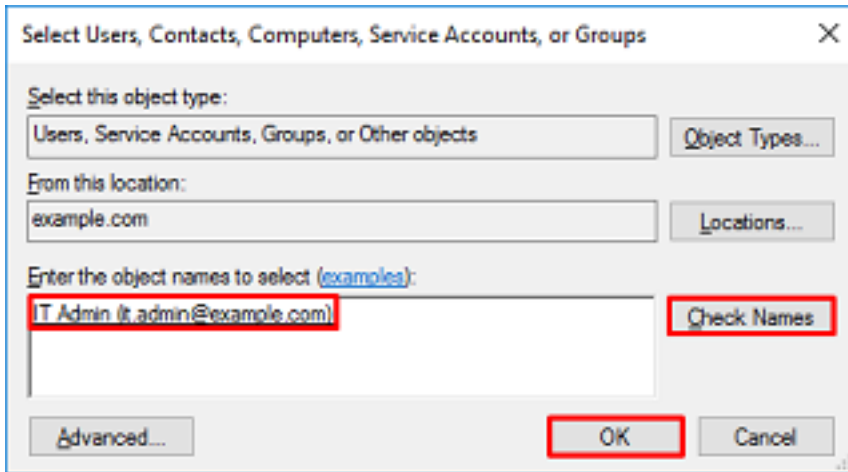
4. 右键单击用户组，然后选择属性。在此配置中，用户IT Admin被添加到AnyConnect Admins组，用户Test User被添加到AnyConnect Users组。



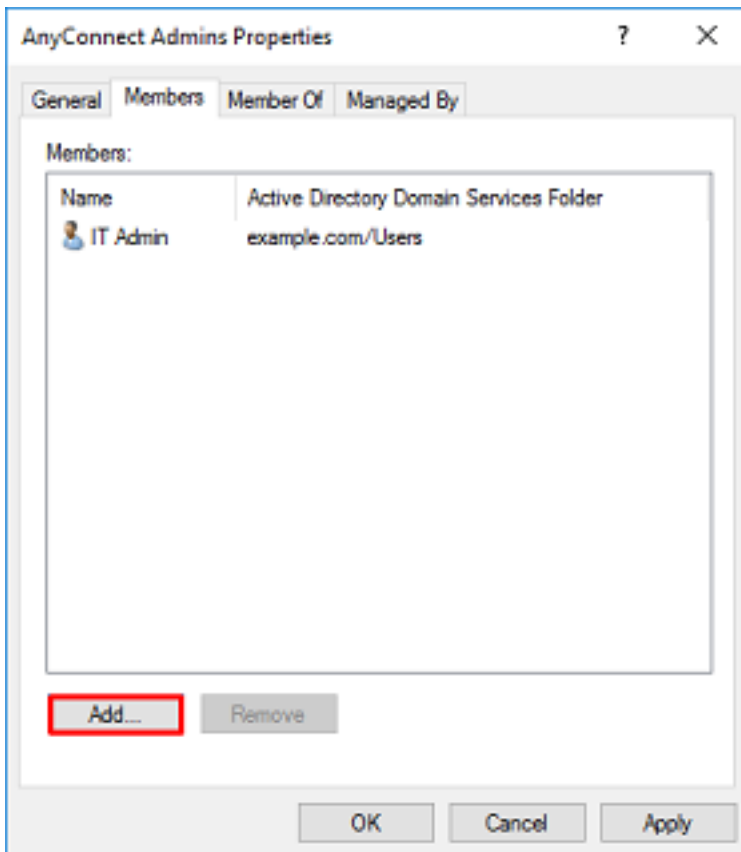
5.在“成员”选项卡下，单击添加。



在字段中输入用户，然后单击**Check Names**以验证是否已找到该用户。验证后，单击**OK**。

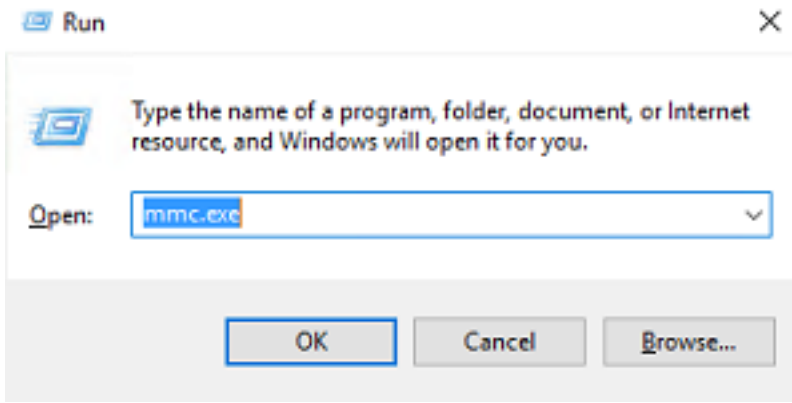


确认已添加正确的用户，然后单击**OK**按钮。用户的**Test User**也会使用相同的步骤添加到**AnyConnect Users**组。

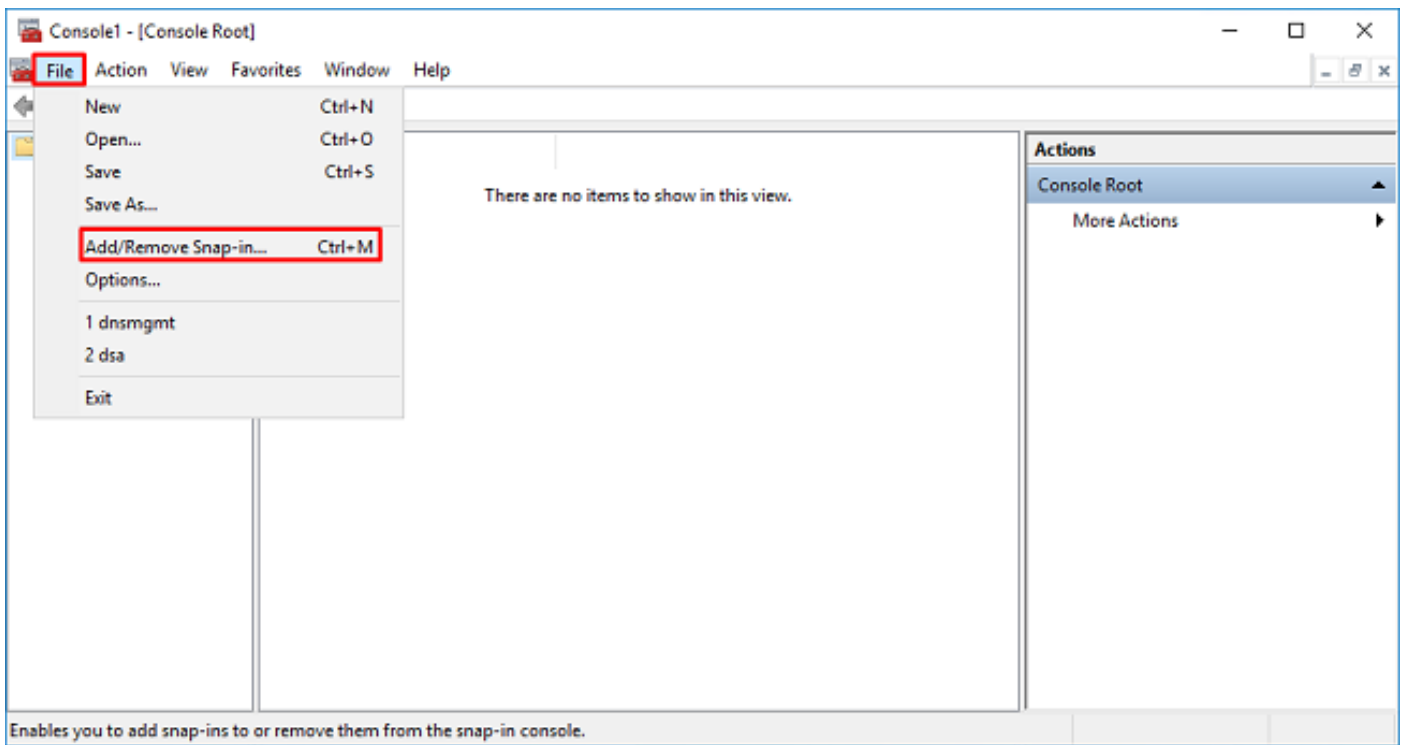


复制LDAPS SSL证书根（仅对于LDAPS或STARTTLS是必需的）

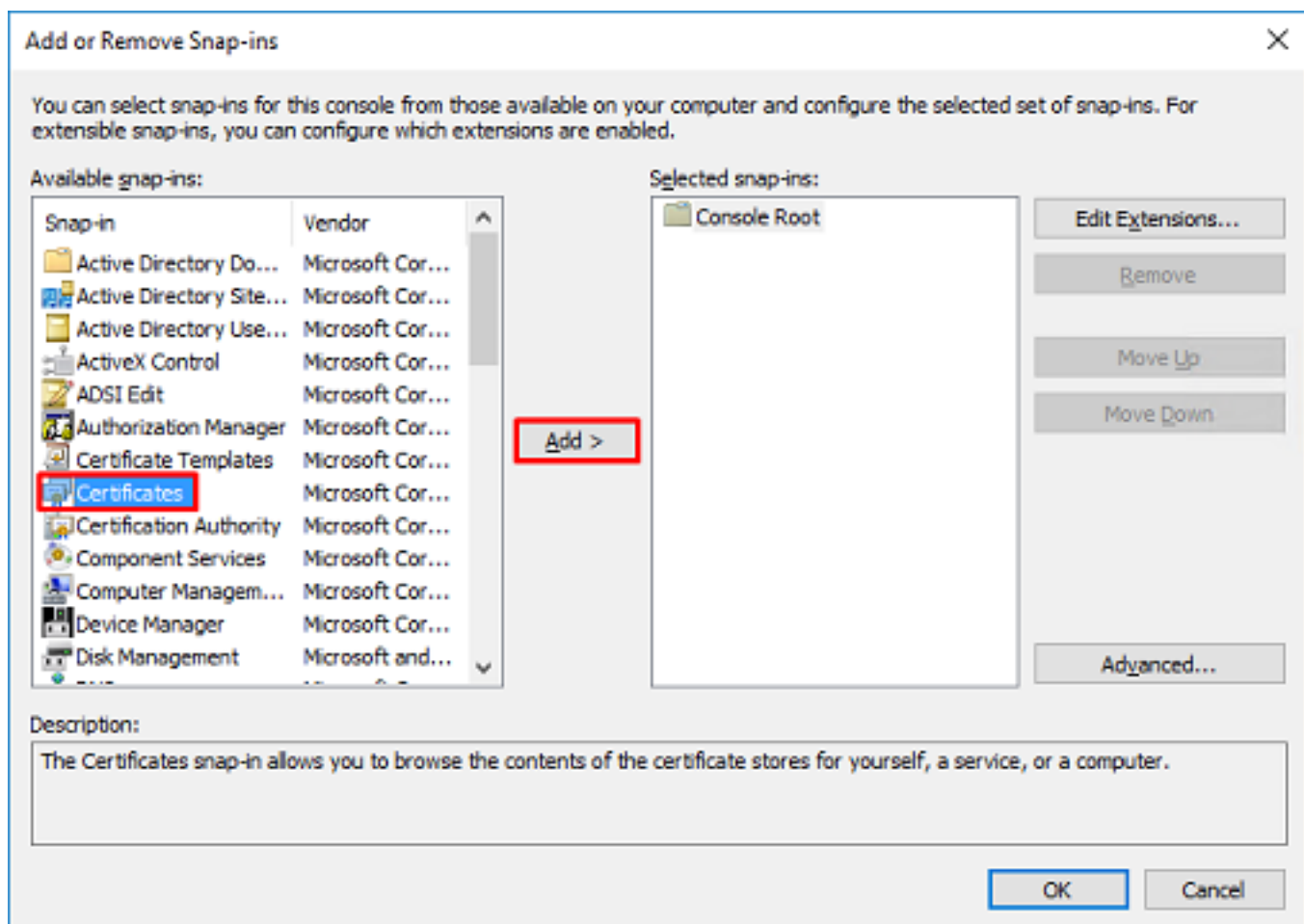
1. 按Win+R并输入**mmc.exe**，然后单击“确定”。



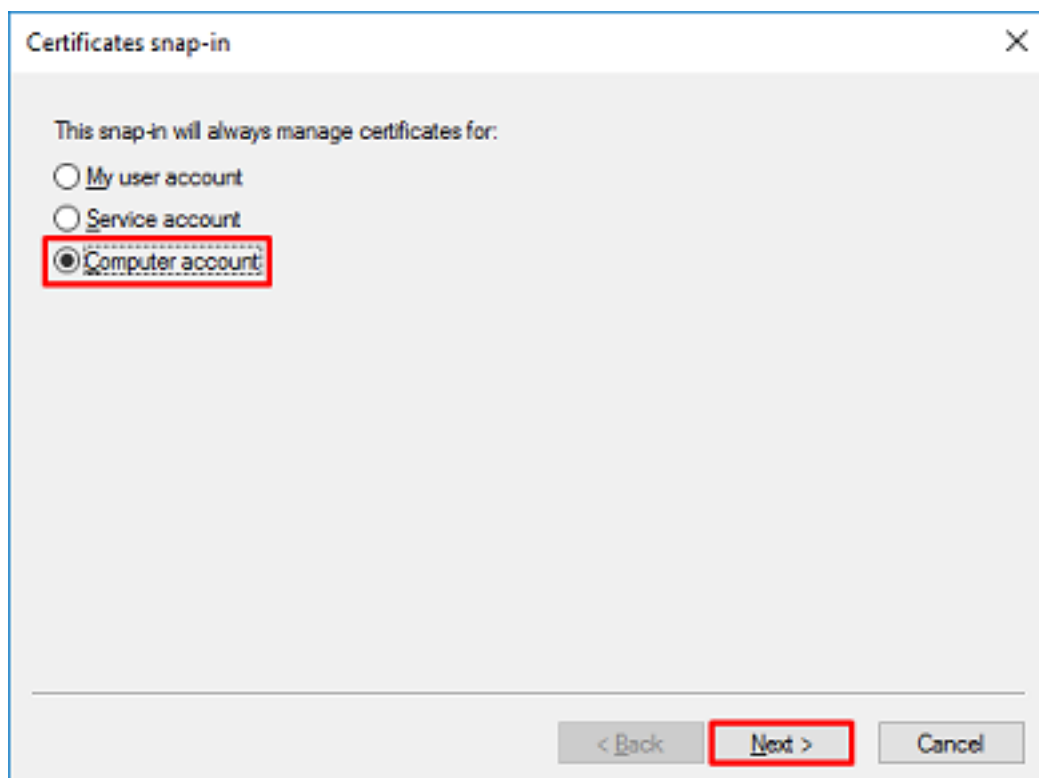
2. 导航到文件>添加/删除管理单元.....



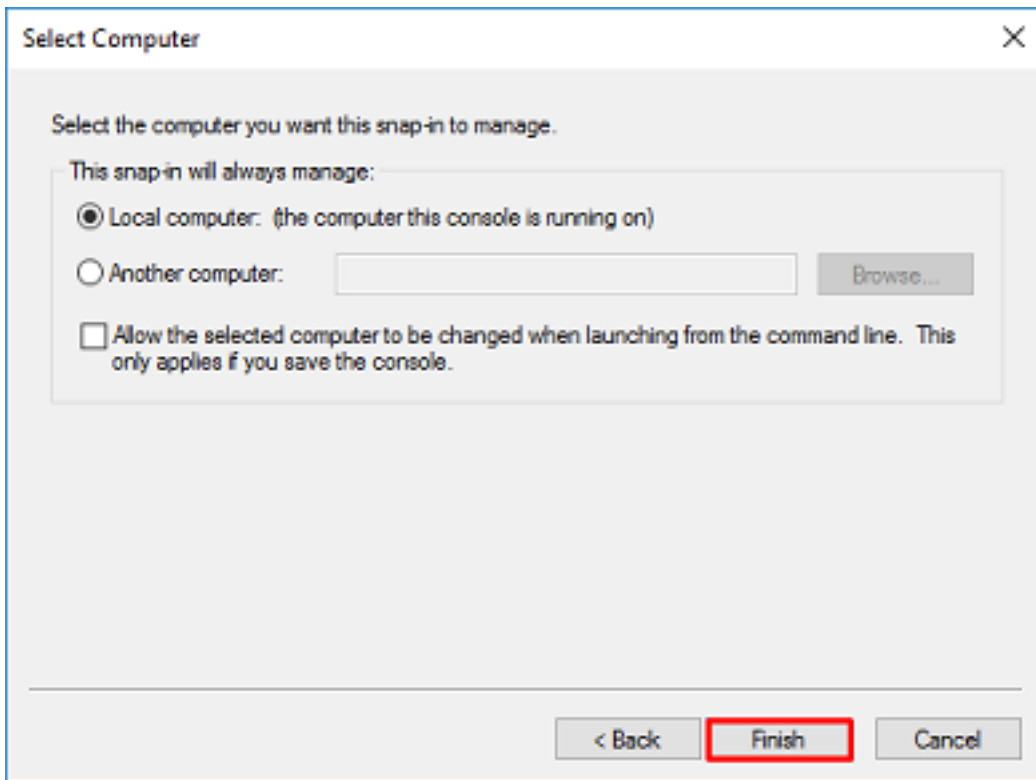
3. 在“可用管理单元”下，选择证书，然后单击添加。



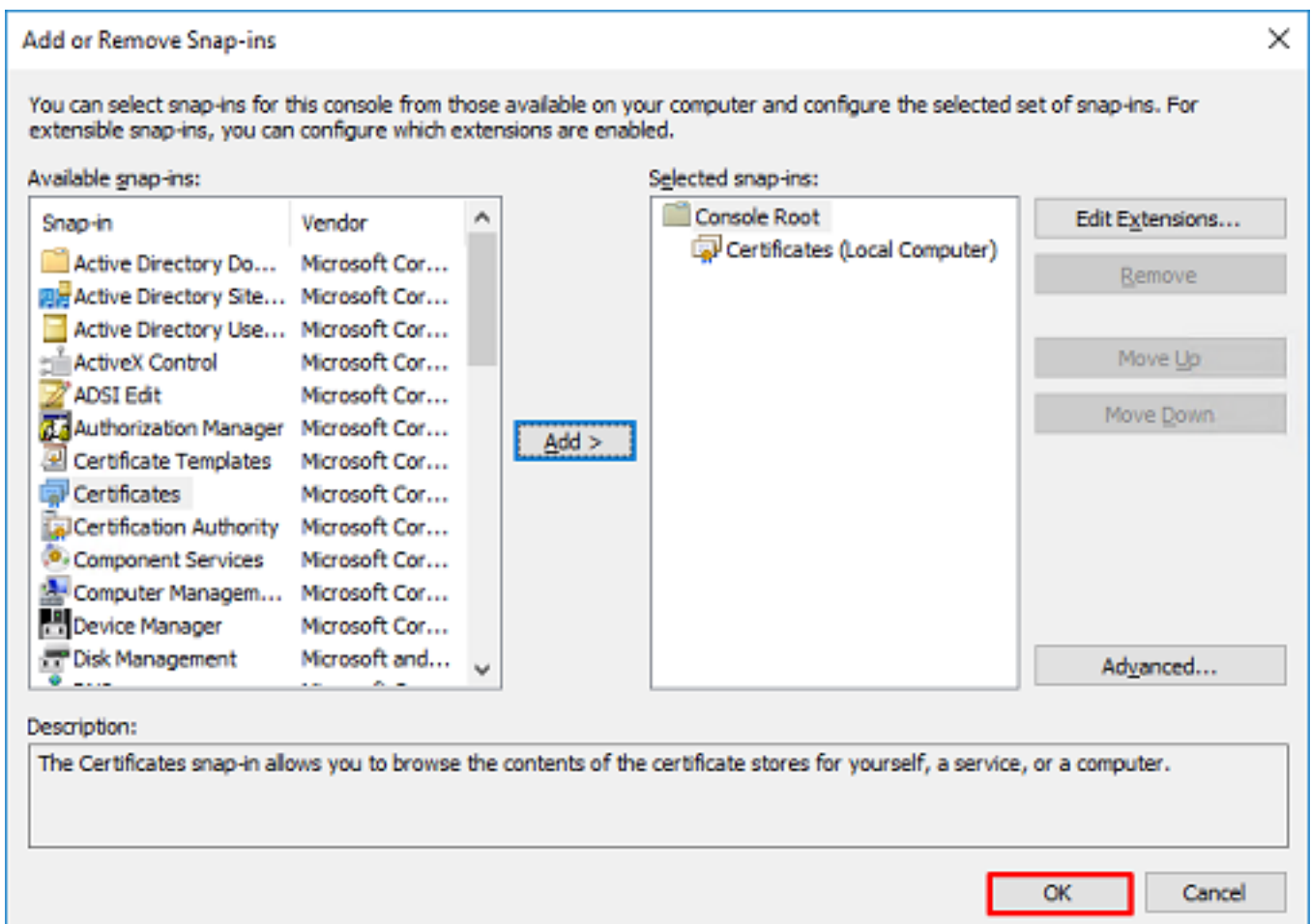
4.选择计算机帐户，然后单击下一步。



单击完成。



5.现在单击**确定**。

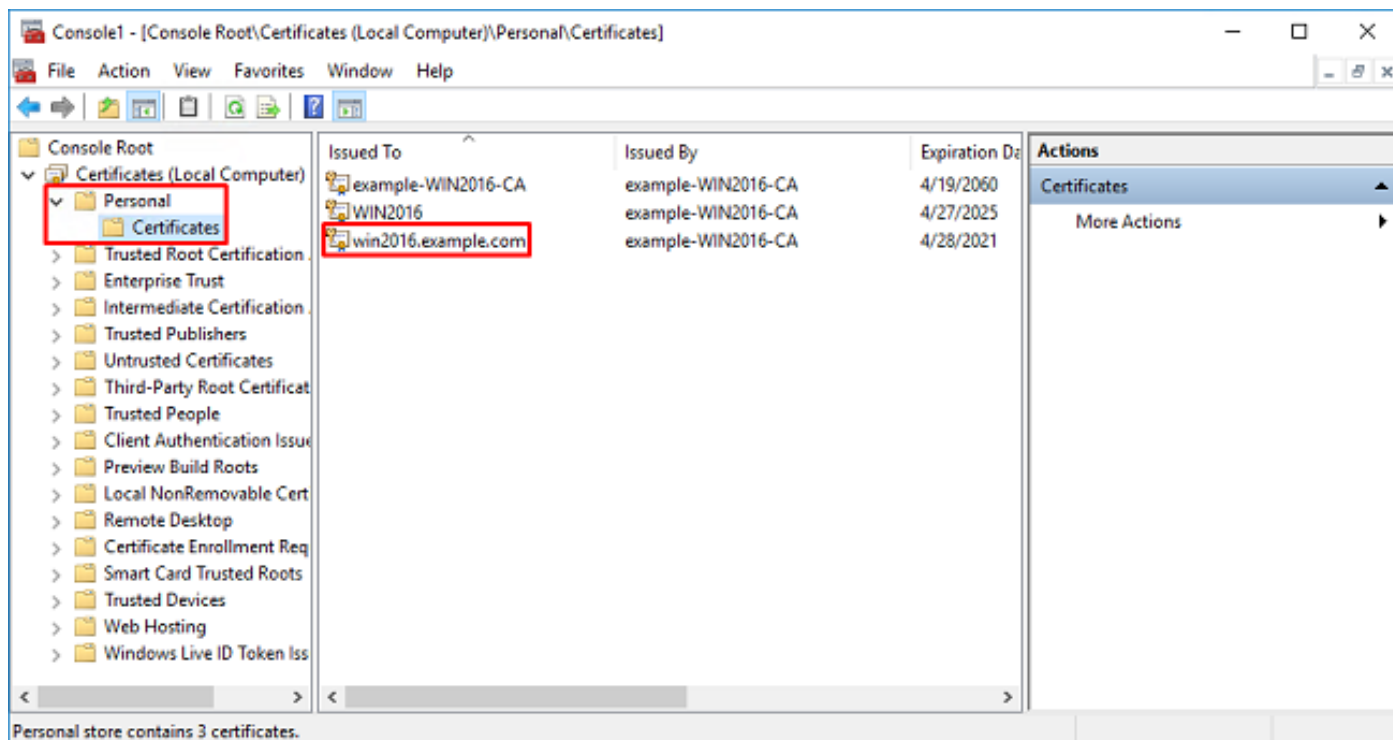


6.展开**Personal**文件夹，然后单击**Certificates**。LDAPS使用的证书颁发给**Windows服务器的完全限定域名(FQDN)**。此服务器上列出了3个证书。

- 颁发给example-WIN2016-CA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。

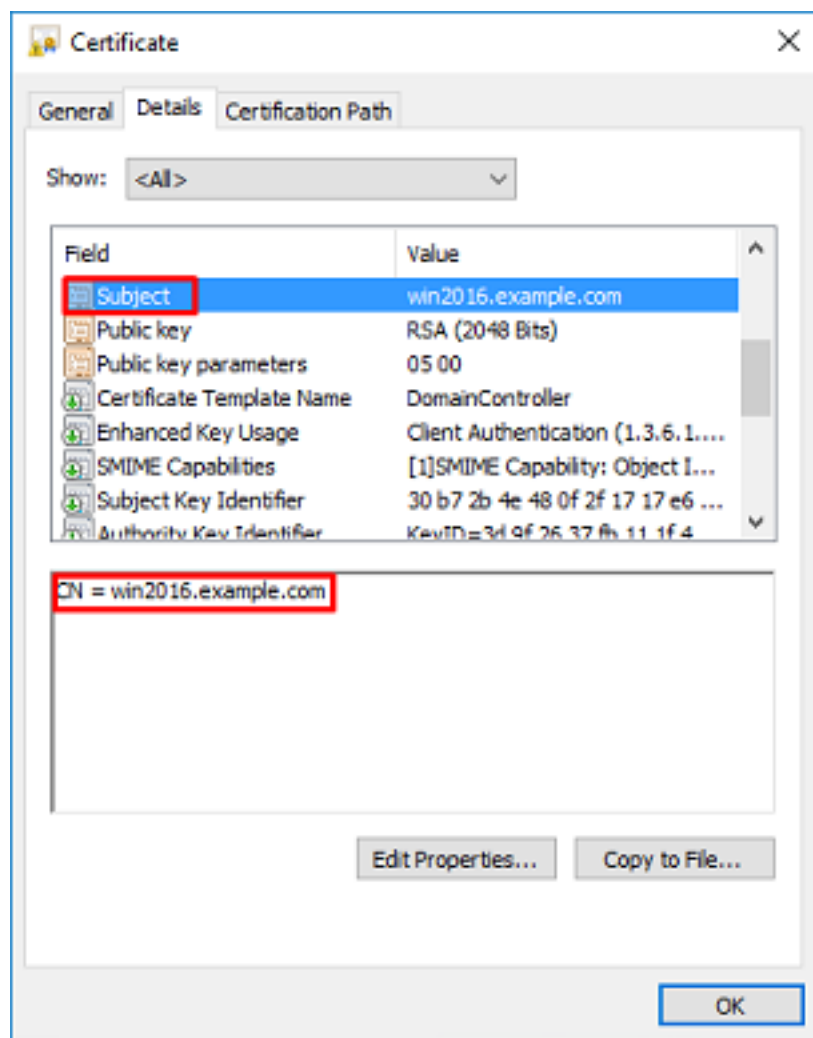
在本配置指南中，FQDN为win2016.example.com，因此前2个证书不能用作LDAPS SSL证书。颁发给win2016.example.com的身份证书是由Windows Server CA服务自动颁发的证书。双击证书检查详细信息。

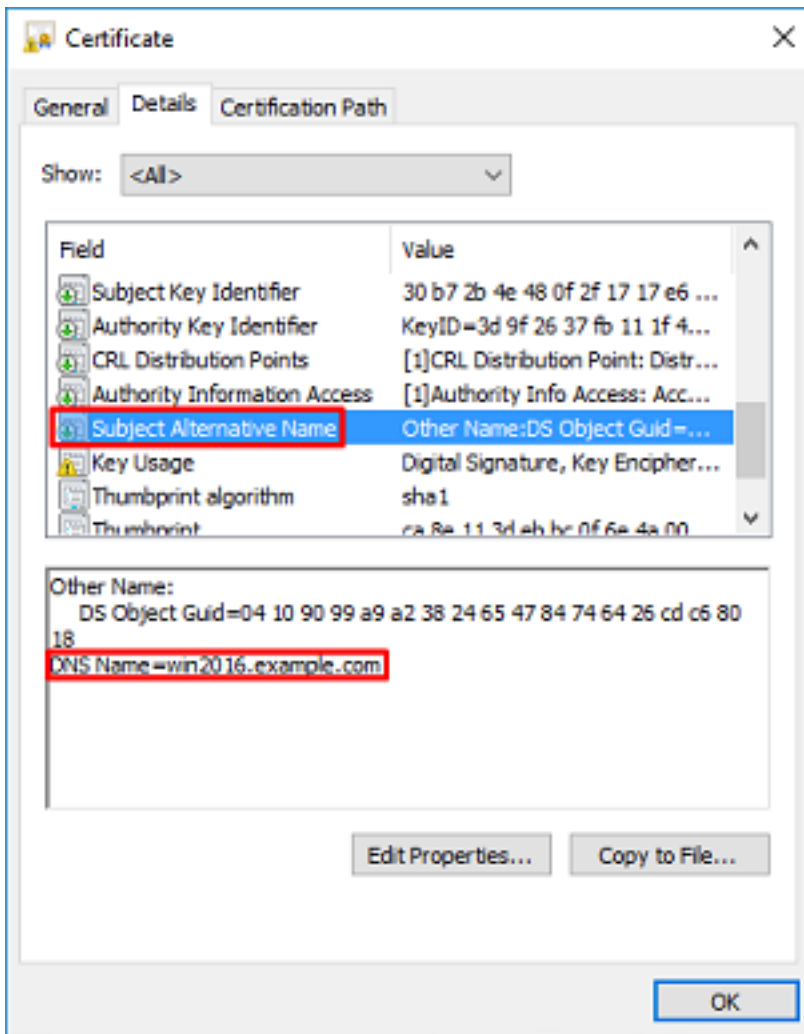


7.要用作LDAPS SSL证书，证书必须满足以下要求：

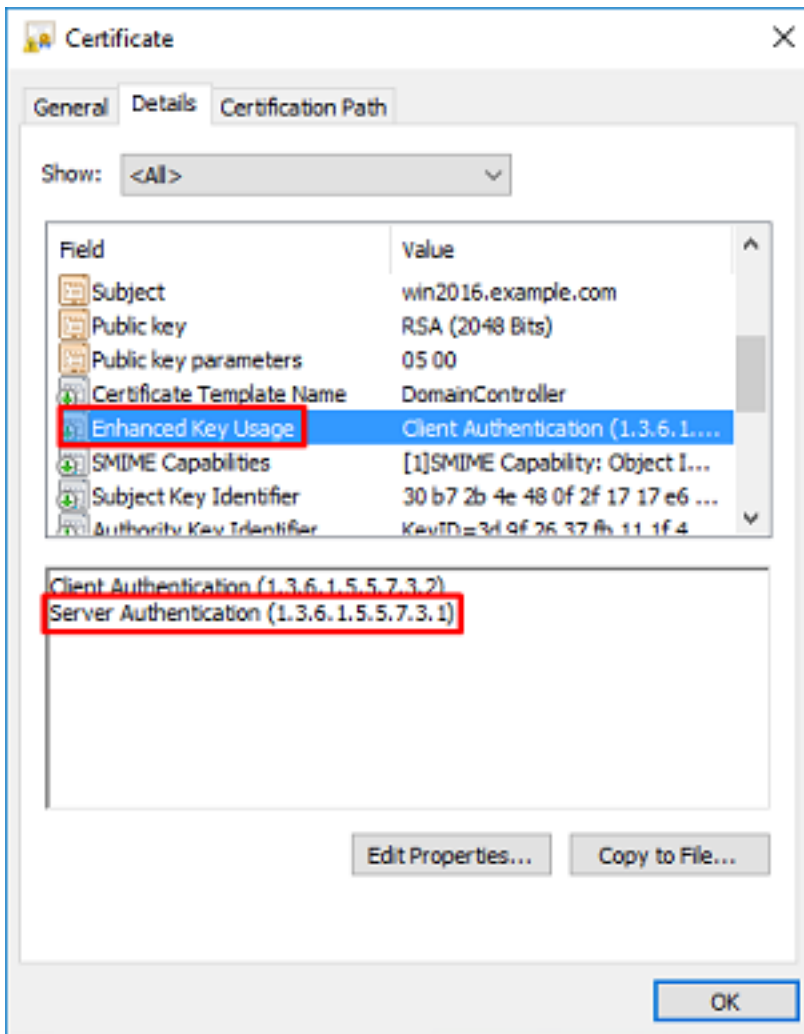
- 公用名或DNS主体备用名称(DNS Subject Alternate Name)与Windows Server的FQDN匹配。
- 证书在Enhanced Key Usage字段下有Server Authentication。

在证书的Details选项卡下，选择Subject和Subject Alternative Name，此时会显示FQDN win2016.example.com。

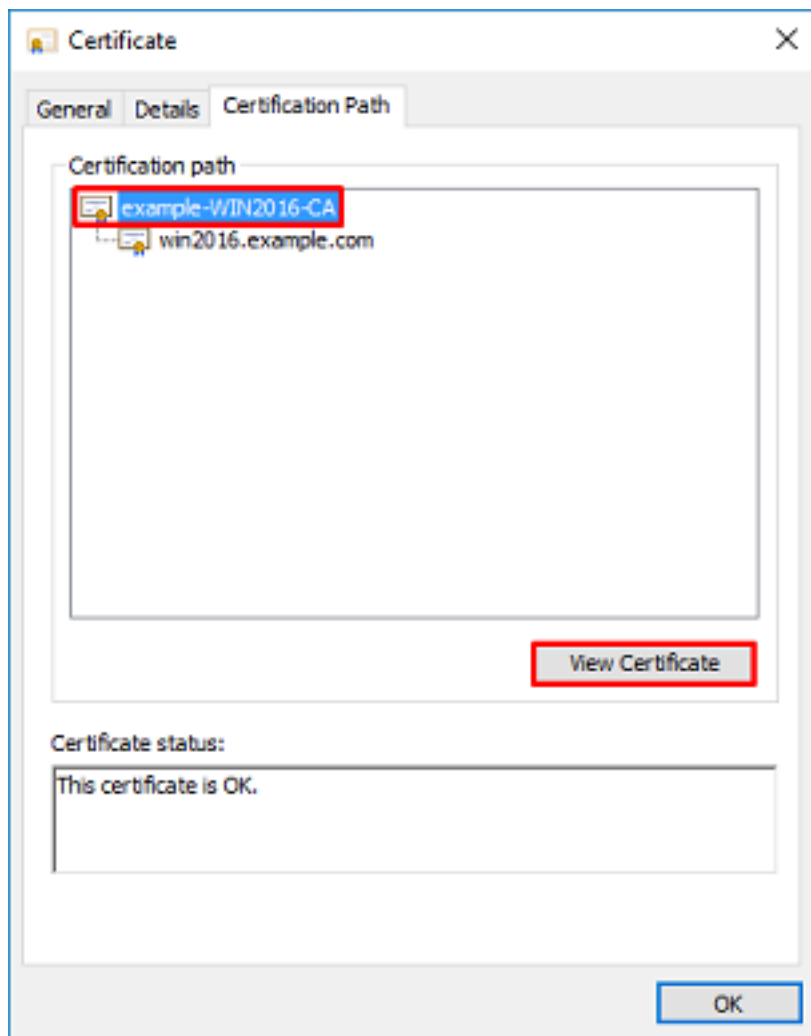




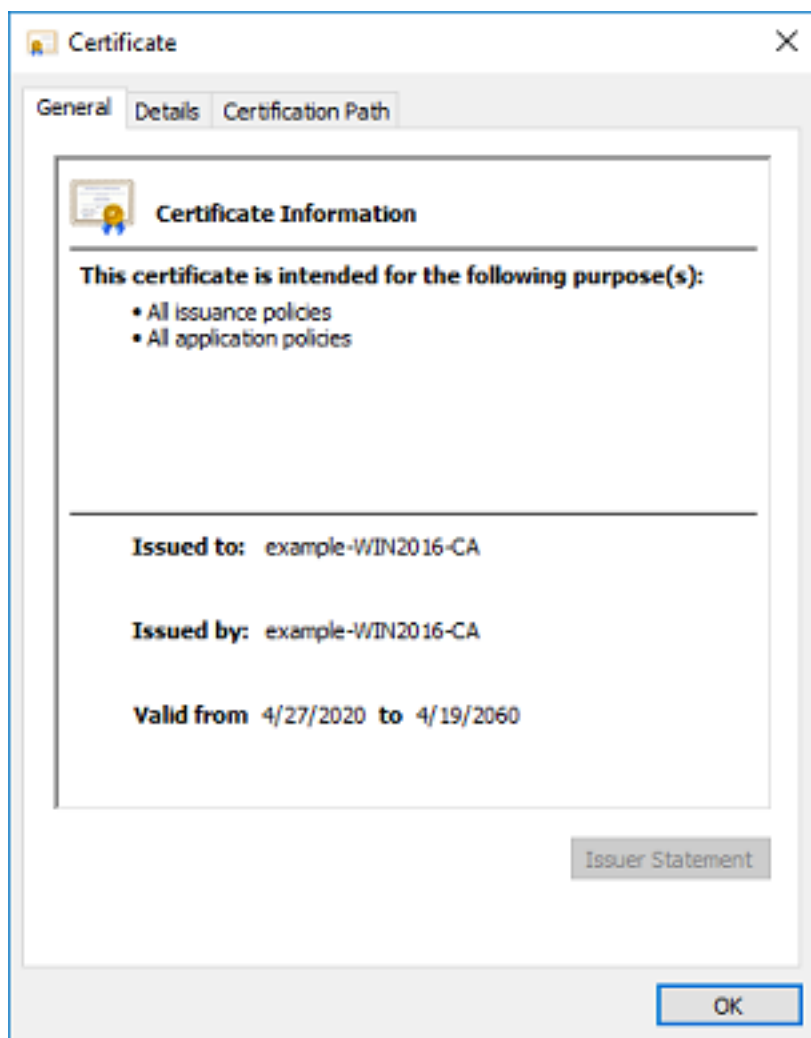
在Enhanced Key Usage下，存在Server Authentication。



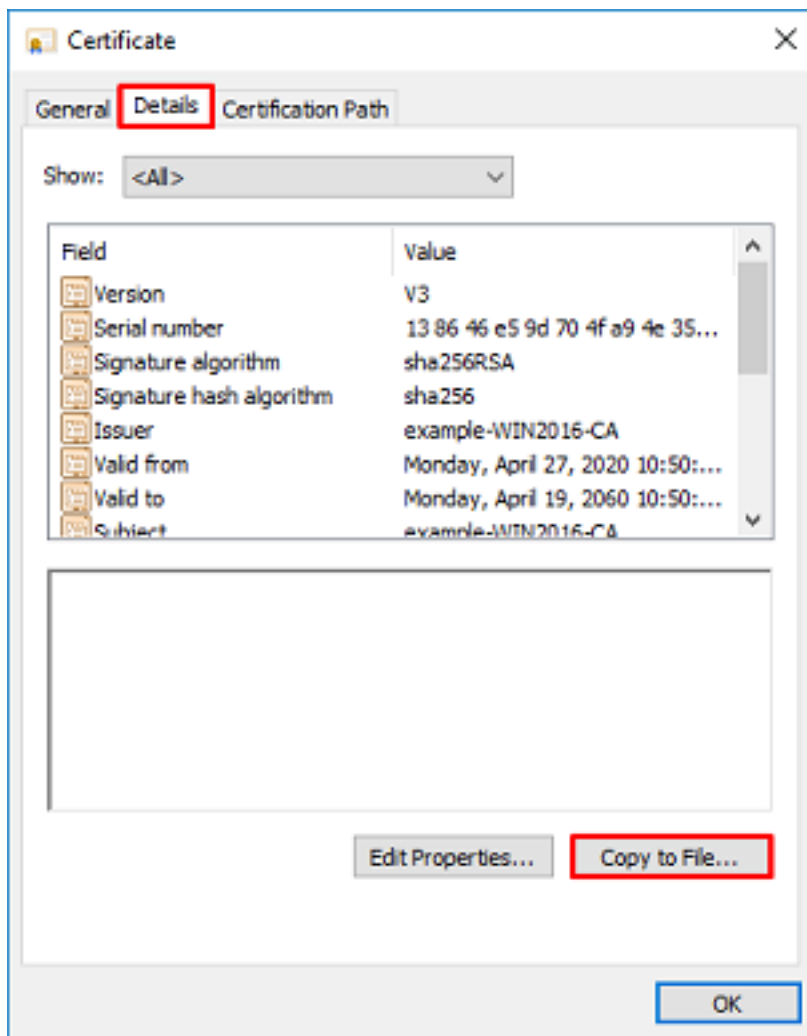
8.确认后，在**Certification Path**选项卡下，选择作为根CA证书的顶级证书，然后单击**View Certificate**。



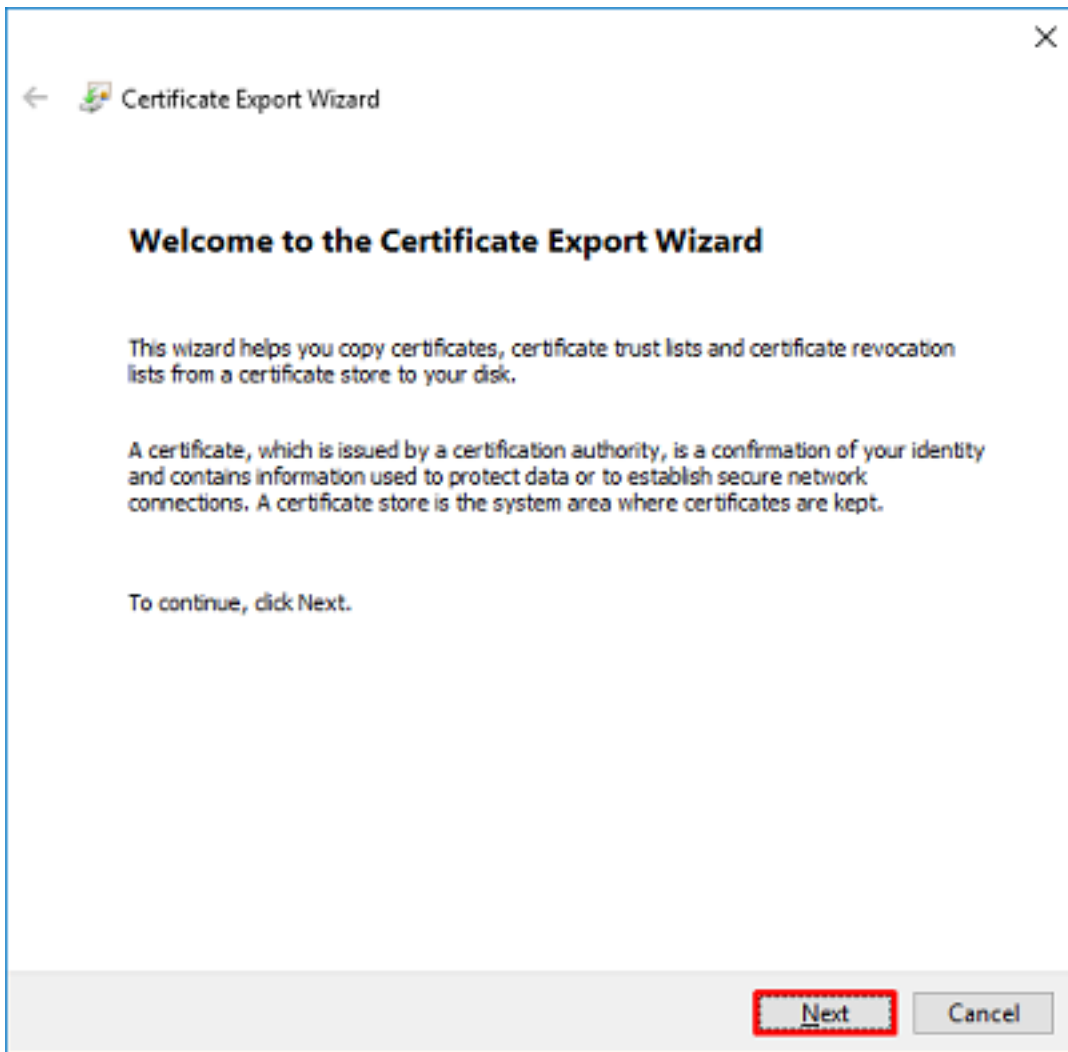
9.这将打开根CA证书的证书详细信息。



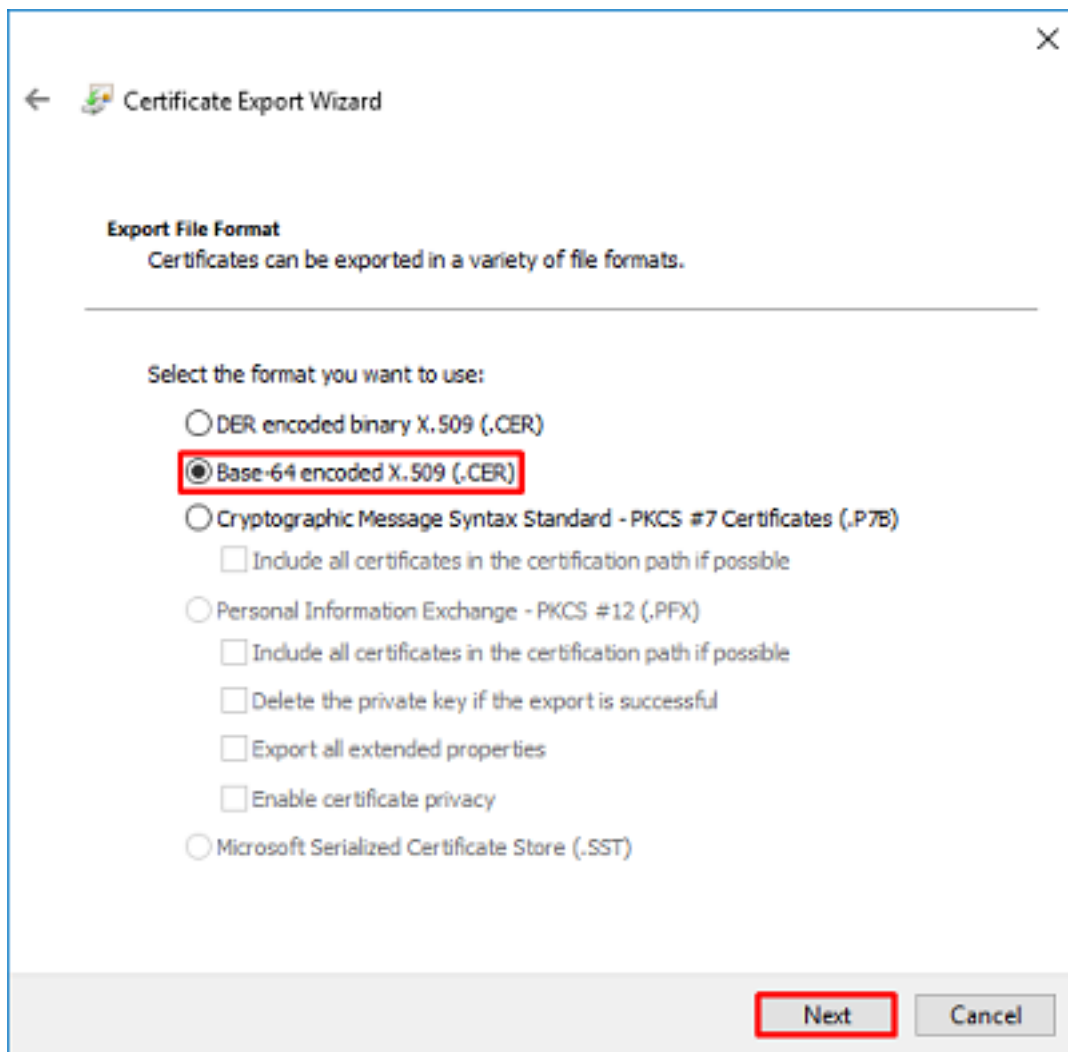
在详细信息选项卡下，单击复制到文件.....



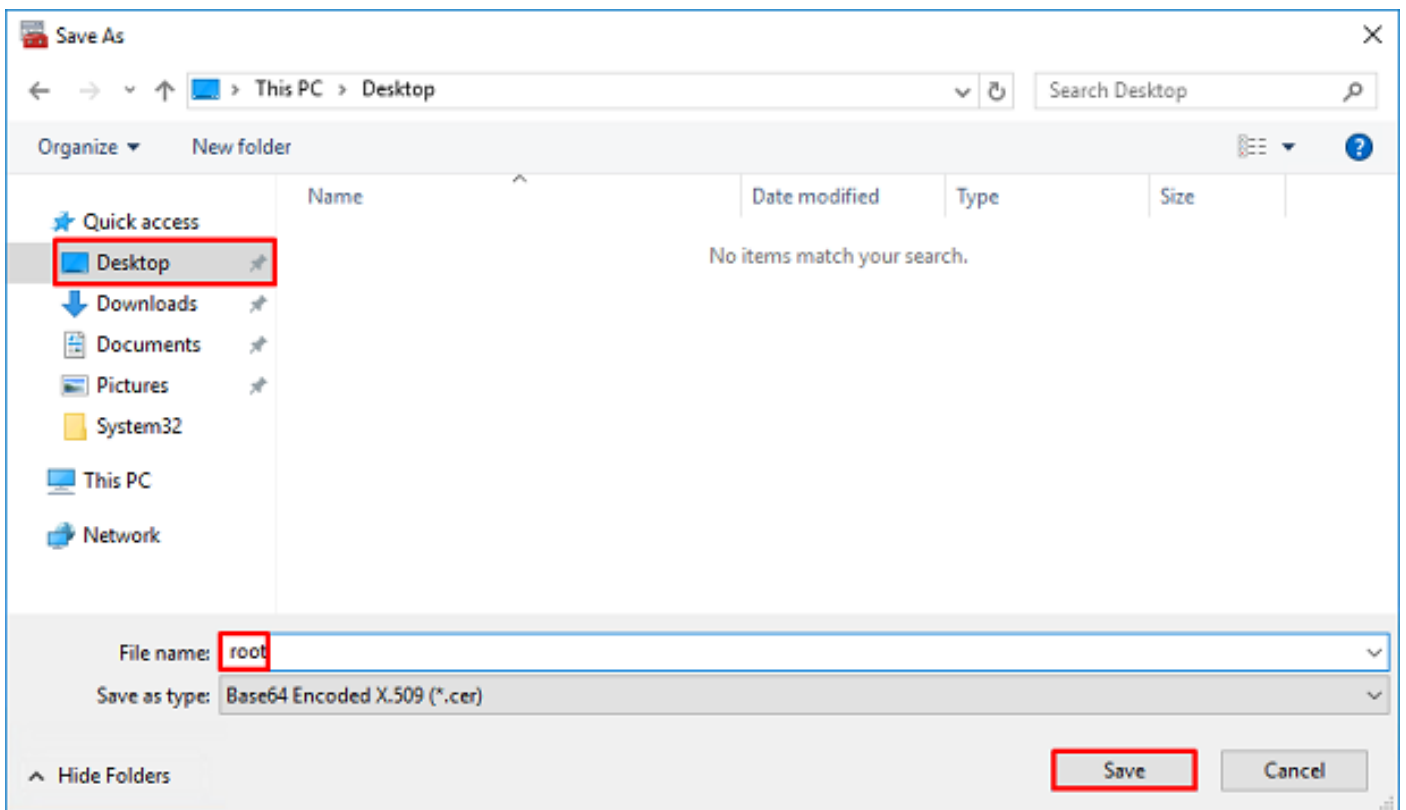
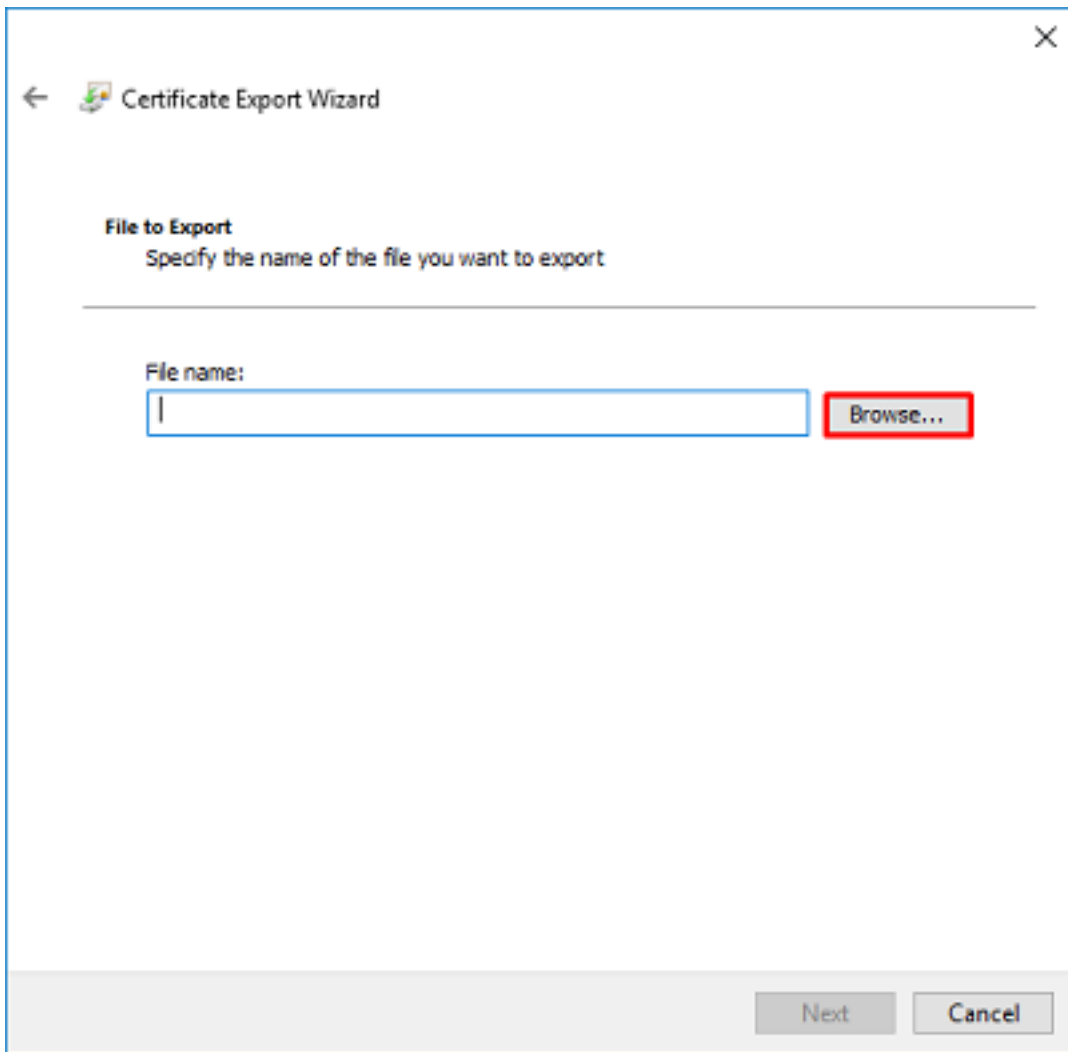
10.通过以PEM格式导出根CA的证书导出向导。

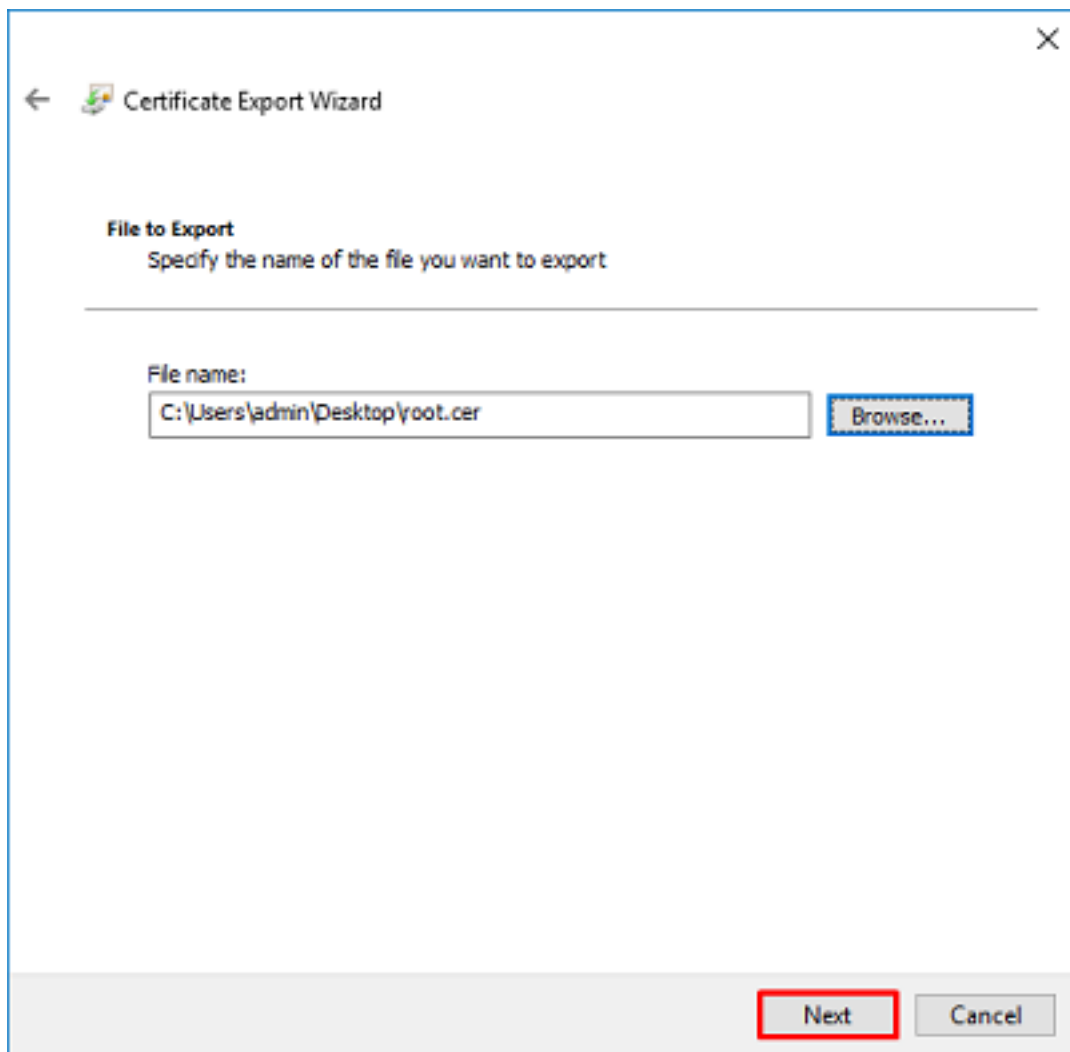


选择Base-64编码X.509

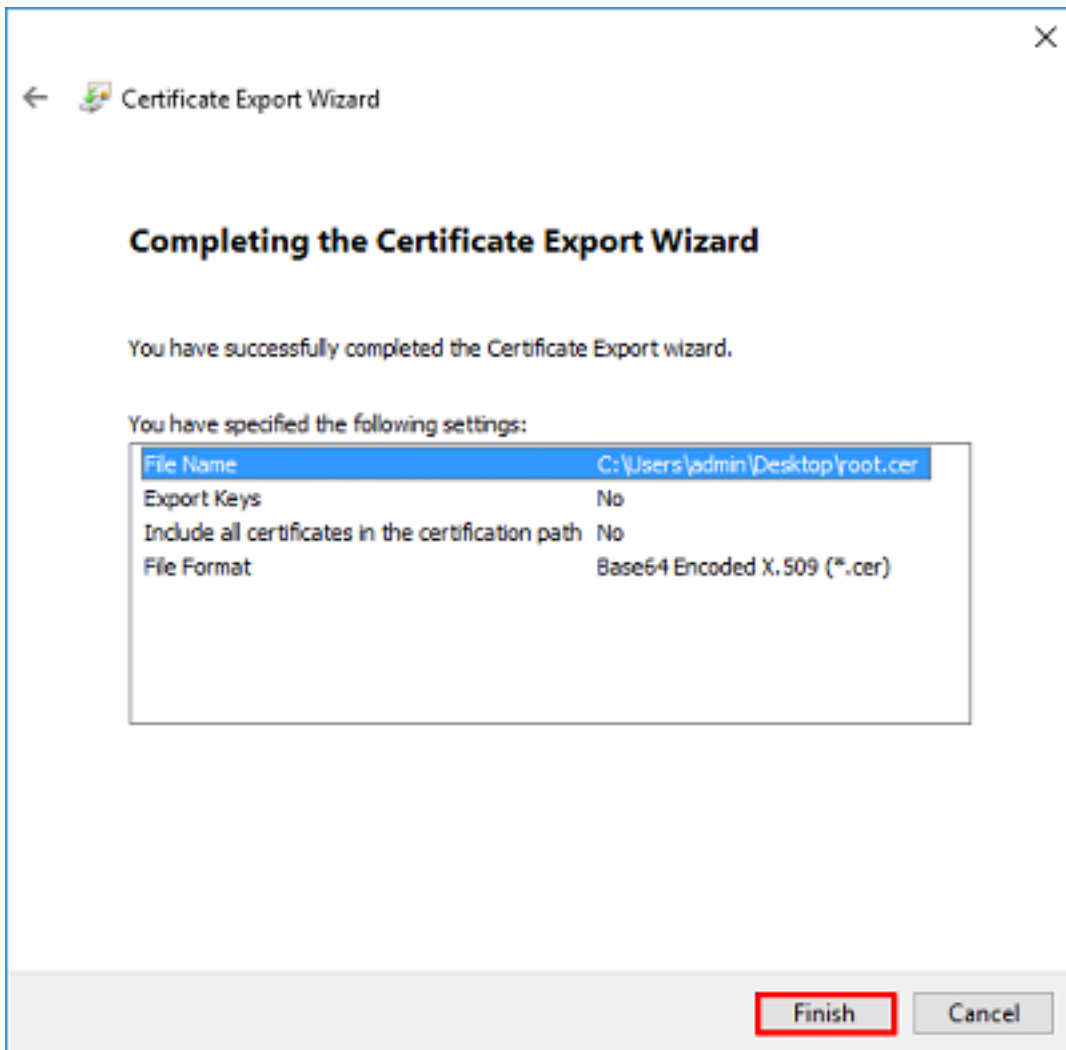


选择文件的名称以及导出文件的位置。





现在单击Finish。



11.现在转到该位置并使用记事本或其他文本编辑器打开证书。这显示PEM格式证书。请保存以备后用。

```
-----BEGIN CERTIFICATE-----
MIIDCCCAfCgAwIBAgIQE4ZG5Z1wT61ONTjooEQyMTANBgkqhkiG9w0BAQsFADAd
MRswGQYDVQQDEeXleGFtYXN0eGx1LVdJTjIwMTYtQ0EwIBcNMjAwNDIzMTQ1MDU5WhgP
MjA2MDA0MTkxNDUwNTlAMB0xGZAZBgNVBAMTEmV4YW1wbGUtV01OMjAxNi1DQTCC
ASiWdQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAl8ghT719NzSQpoQPh0YT67b
Ya+PngsxMyvkewP33QLTAWw1HW1Tb9Mk5BDWOItTaVsgHwPBfd++M+bLn3AiZnHV
OO+k6dVVY/E5qVkeKSGoY+v940S2316lzdWReMOFhgbc2qMertIoficrRihonuU
Cjyeub3CO+meJUuKom2R47C0D35TUvo/FEHGgXJFajS1se2UrpNO7KEMkfAlLPuM
aob4XE/OzxYQpPa18djsNnskfcFqD/HOTFQN4+SrOhHWlRnUIQBuaLdQaabhipD/
sVs5PneYJX8YKma82luYI6j90YuytmsHBtCieyC062a8BKqOL7N86HFPfkMA3u8C
AwEAAaNCMEAwDgYDVR0PAQH/BAQDAgGMA8GA1UdEwEB/wQFMAMBAf8wHQYDVR0O
BBYEFD2fJjf7ER9EM/HCxCVFN5QzqEdvMA0GCSqGSIb3DQEBCwUAA4IBAQB3lZJo
vzwVD3c5Q1nrNP+6Mq62OFpYH91k4Ch9S5g/CEOemhcwg8MDIoxW2dTsjenAEt7r
phFIHzoCoSyjBjMgK3xybmoSeg8vBjCXseYNGEm0c9KW1oFmTOvdNVIb7Xp11IVa
6tALTt3ANRNgREtXPA6yQbthKGavW0Anfsojk9IcDr2vp0MTj1BCxsTscubRl+d
dLEFKQqmMeYvkVf+a7a64mqPZsG3Uxo0rd6cZxAPkq/ylcdwNSJFFfQV3DgZg+R96
9WLCR30big6xyo9Zu+lixWpdrbAD06zMHbEYEHkh00jBrUEBBI6Cy83iTZ9ejsk
KgWBJXEu33PplW6E
-----END CERTIFICATE-----
```

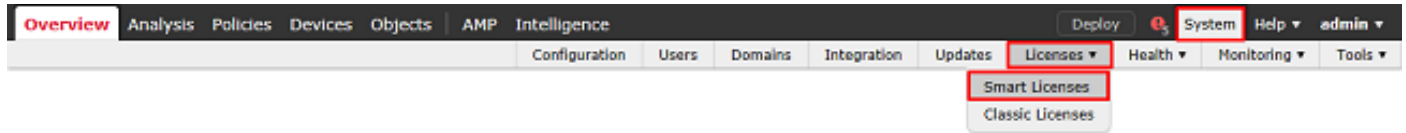
12. (可选) 如果LDAPS可以使用多个身份证书，并且使用哪个身份证书存在不确定性，或者无法访问LDAPS服务器，则可以从在Windows服务器或FTD之后完成的数据包捕获中提取根ca。

FMC配置

验证许可

要部署AnyConnect配置，FTD需要注册到智能许可服务器，并且必须将有效的Plus、Apex或仅VPN许可证应用到设备。

1.导航到系统>许可证>智能许可。



2.确认设备符合要求并成功注册。确保设备已注册到AnyConnect Apex、Plus或仅VPN许可证。

Smart License Status

Usage Authorization: ✔ Authorized (Last Synchronized On May 03 2020)

Product Registration: ✔ Registered (Last Renewed On Mar 03 2020)

Assigned Virtual Account: SEC TAC

Export-Controlled Features: Enabled

Cisco Success Network: Disabled ⓘ

Cisco Support Diagnostics: Disabled ⓘ

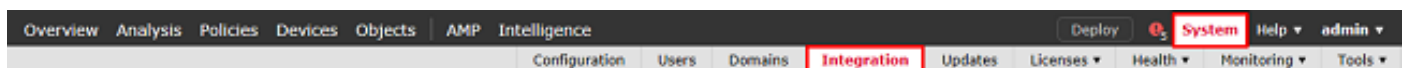
Smart Licenses

License Type/Device Name	License Status	Device Type	Domain	Group
Firepower Management Center Virtual (2)	✔			
Base (2)	✔			
Malware (1)	✔			
Threat (2)	✔			
URL Filtering (2)	✔			
AnyConnect Apex (1)	✔			
FTD-2 192.168.1.17 - Cisco Firepower Threat Defense for VMWare - v6.3.0	✔	Cisco Firepower Threat Defense for VMWare	Global	N/A
AnyConnect Plus (0)				
AnyConnect VPN Only (0)				

Note: Container Instances of same blade share feature licenses

设置领域

1.定位至系统>集成。



2.在领域下，单击新建领域。

Realms

Compare realms ✔ **New realm**

Name	Description	Domain	Type	Base DN	Group DN	Group Attribute	State
------	-------------	--------	------	---------	----------	-----------------	-------

3.根据从Microsoft服务器收集的信息填写相应字段。完成后，单击OK。

Add New Realm

Name * LAB-AD

Description

Type * AD

AD Primary Domain * example.com ex: domain.com

AD Join Username ex: user@domain

AD Join Password Test AD Join

Directory Username * ftd.admin@example.com ex: user@domain

Directory Password *

Base DN * DC=example,DC=com ex: ou=user,dc=cisco,dc=com

Group DN * DC=example,DC=com ex: ou=group,dc=cisco,dc=com

Group Attribute Member

* Required Field

OK Cancel

4.在新窗口中，选择Directory（如果尚未选择），然后单击Add directory。

Overview Analysis Policies Devices Objects AMP Intelligence Deploy System Help admin

Configuration Users Domains Integration Updates Licenses Health Monitoring Tools

LAB-AD

Enter Description Save Cancel

Directory Realm Configuration User Download

Add directory

填写AD服务器的详细信息。请注意，如果使用FQDN，则除非将DNS配置为解析FQDN，否则FMC和FTD无法成功绑定。

要设置FMC的DNS，请导航到System > Configuration，然后选择Management Interfaces。

要设置FTD的DNS，请导航到Devices > Platform Settings，创建新策略，或编辑当前策略，然后转到DNS。

Add directory

Hostname / IP Address win2016.example.com

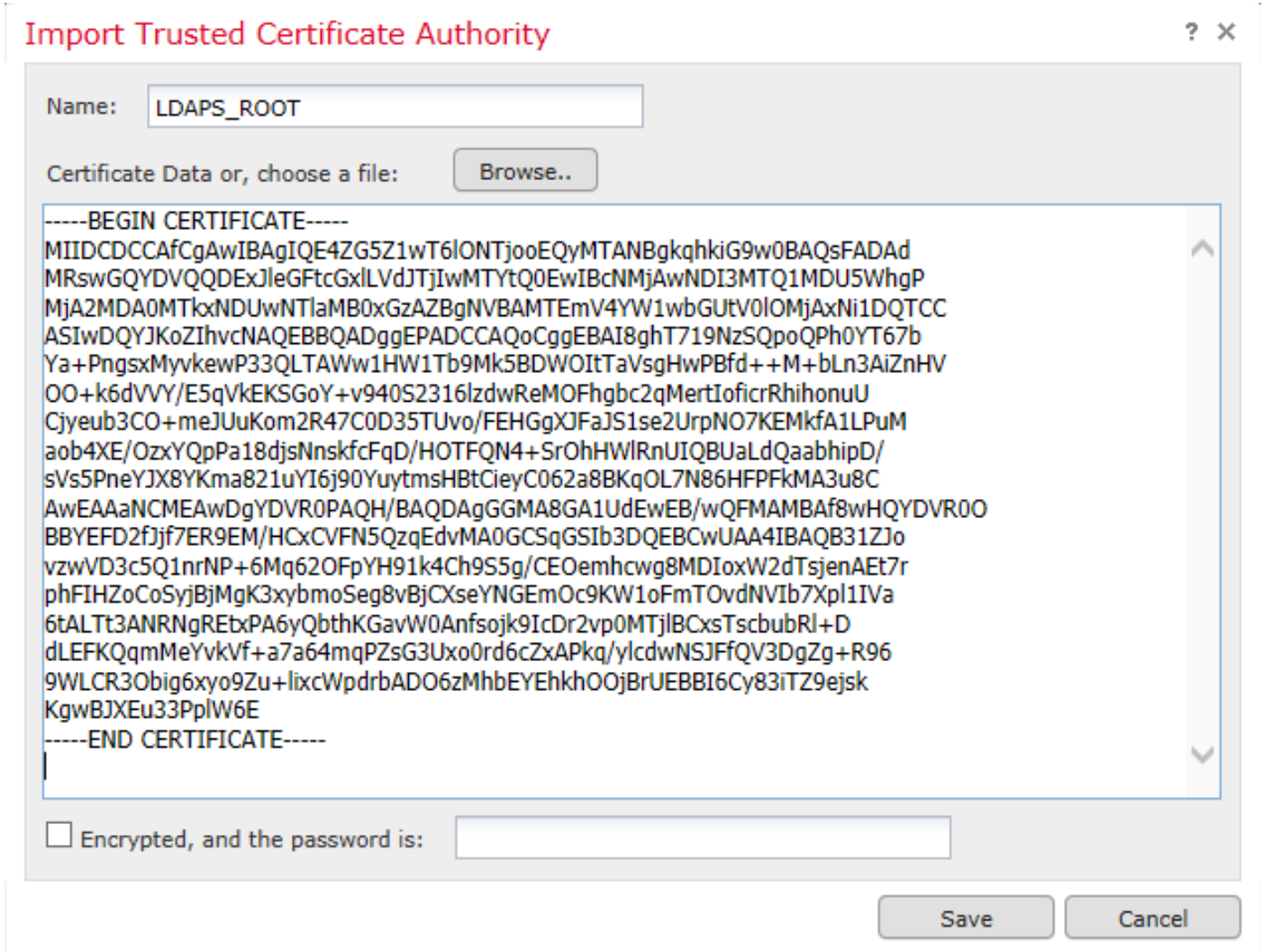
Port 389

Encryption STARTTLS LDAPS None

SSL Certificate [dropdown] +

OK Test Cancel

如果使用LDAPS或STARTTLS，请单击绿色+符号，为证书指定一个名称，然后复制PEM格式的根CA证书。完成后单击**Save**。



Import Trusted Certificate Authority ? X

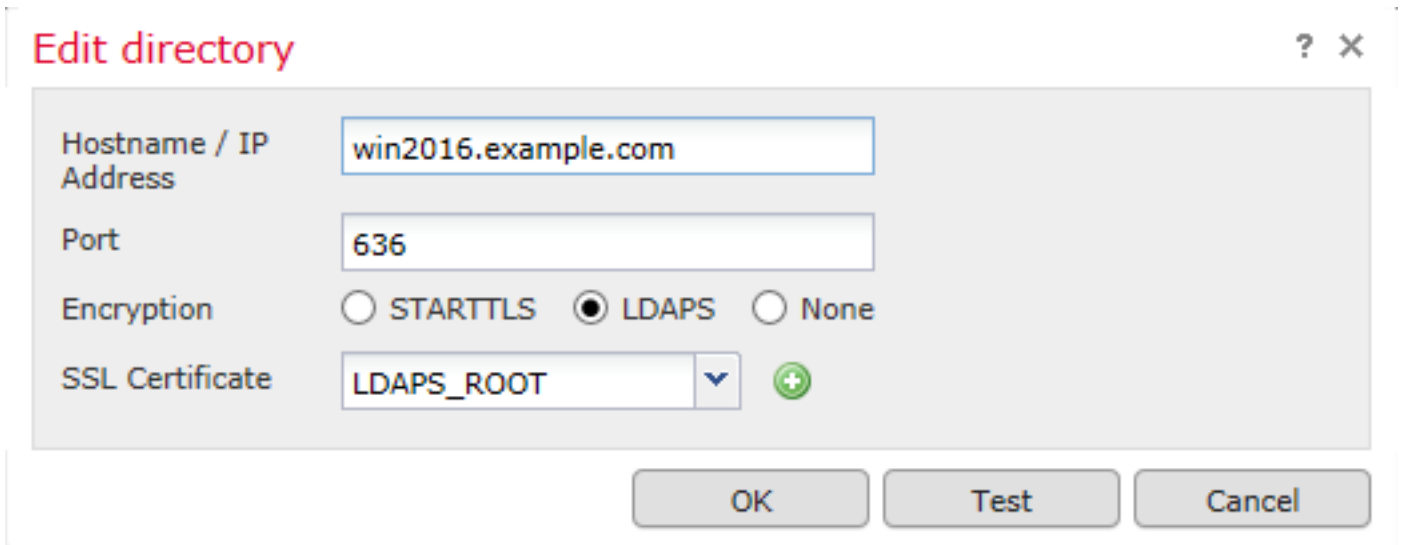
Name:

Certificate Data or, choose a file:

```
-----BEGIN CERTIFICATE-----
MIIDCDCCAfCgAwIBAgIQE4ZG5Z1wT6lONTjooEQyMTANBgkqhkiG9w0BAQsFADAd
MRswGQYDVQQDEExleGFtZXVudjEwMTYtQ0EwIBcNMjAwNDI3MTQ1MDU5WhgP
MjA2MDA0MTkxNDUwNTlaMB0xGzAZBgNVBAMTEV4YVw1wbGUV0lOMjAxNi1DQTCC
ASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAl8ghT719NzSQpoQPh0YT67b
Ya+PngsxMyvkewP33QLTAWw1HW1Tb9Mk5BDWOItaVsgHwPBfd++M+bLn3AiZnHV
OO+k6dVVY/E5qVKEKSGoY+v940S2316lzdwrReMOFhgbc2qMertIoficrRihonuU
Cjyeub3CO+meJUuKom2R47C0D35TUvo/FEHGgXJFaJS1se2UrpNO7KEMkFA1LPuM
aob4XE/OzxYQpPa18djsNnskfCfQD/HOTFQN4+SrOhHWIRnUIQBUaLdQaabhipD/
sVs5PneYJX8YKma821uYI6j90YuytmsHBtCieyC062a8BKqOL7N86HFPfMA3u8C
AwEAAaNCMEAwDgYDVR0PAQH/BAQDAgGGMA8GA1UdEwEB/wQFMAMBAf8wHQYDVR0O
BBYEFD2fj7ER9EM/HcXCVFN5QzqEdvMA0GCSqGSIb3DQEBCwUAA4IBAQB31ZJo
vzwVD3c5Q1nrNP+6Mq62OfpYH91k4Ch9S5g/CEOemhwcg8MDIoxW2dTsjenAet7r
phFIHZoCoSyjBjMgK3xybmoSeg8vBjCXseYNGEmOc9KW1oFmTOvdNVIb7Xpl1IVa
6tALTt3ANRNgREtPA6yQbthKGavW0Anfsojk9IcDr2vp0MTjBCxsTscubRI+D
dLEFKQqmMeYvkVf+a7a64mqPZsG3Uxo0rd6cZxAPkq/yIcdwNSJFFQV3DgZg+R96
9WLCR3Obig6xyo9Zu+lixwPdrbADO6zMhbEYEHkhOOjBrUEBBI6Cy83iTZ9ejsk
KgwBJXEu33PplW6E
-----END CERTIFICATE-----
```

Encrypted, and the password is:

从SSL Certificate旁边的下拉列表中选择新添加的根CA，然后单击STARTTLS或LDAPS。



Edit directory ? X

Hostname / IP Address:

Port:

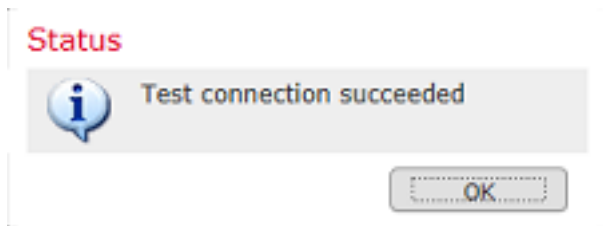
Encryption: STARTTLS LDAPS None

SSL Certificate:

单击Test以确保FMC能够成功绑定上一步中提供的目录用户名和密码。

由于这些测试是从FMC启动的，而不是通过FTD上配置的某个可路由接口（例如内部、外部和dmz）启动，因此成功（或失败）的连接不能保证AnyConnect身份验证的相同结果，因为AnyConnect LDAP身份验证请求是从FTD可路由接口之一启动的。

有关从FTD测试LDAP连接的详细信息，请查看Troubleshooting区域中的Test AAA and Packet Capture部分。



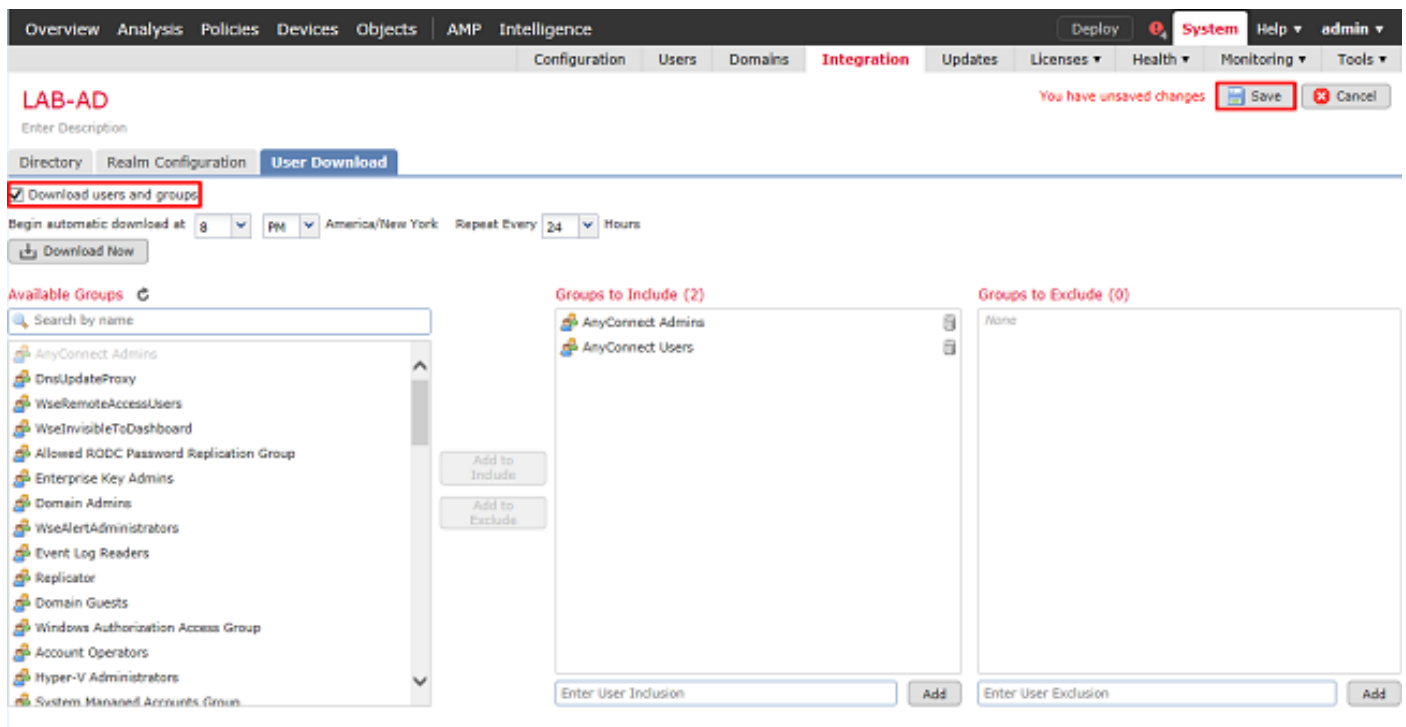
5.在User Download下，下载后续步骤中用于用户身份的组。

选中Download users and groups复选框，Available Groups列将使用Active Directory中配置的组进行填充。

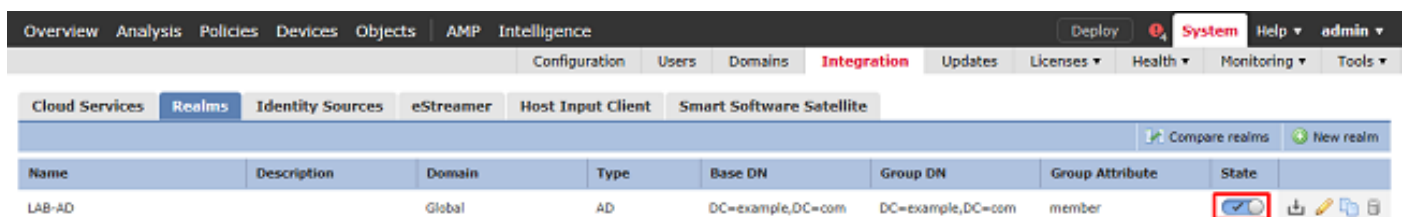
组可以包括(Included)或排除(Excluded)，但默认情况下包括组DN下找到的所有组。

也可以包括或排除特定用户。任何包含的组和用户都可以在以后选择用于用户身份。

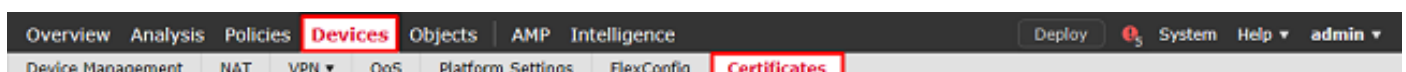
完成后，单击 Save (保存)。



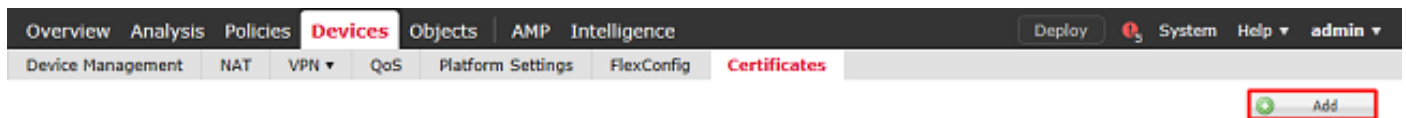
6.启用新领域。



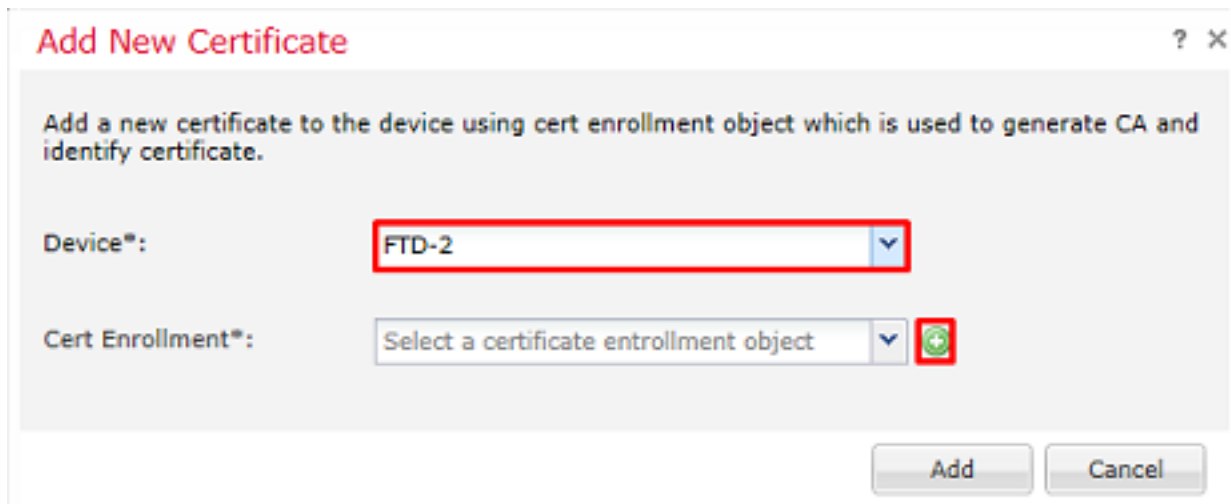
7.如果使用LDAPS或STARTTLS，则根CA也需要由FTD信任。为此，请首先导航到设备>证书。



点击右上角的Add。



选择FTD，将LDAP配置添加到中，然后点击绿色+符号。



为信任点指定Name，然后从Enrollment Type下拉列表中选择Manual enrollment。将PEM根ca证书粘贴到此处，然后单击Save。

Add Cert Enrollment



Name*

Description

CA Information Certificate Parameters Key Revocation

Enrollment Type:

CA Certificate:*
-----BEGIN CERTIFICATE-----
MIIDCDCAfCgAwIBAgIQE4ZG5Z1wT6lONTjooEQyMTANBgkqhkiG9w0BAQsFADAdMRswGQYDVQQDEExJeGFtcGxlLVdJTjIwMTYtQ0EwIBcNMjAwNDIzMTQ1MDU5WhgPMjA2MDA0MTkxNDUwNTIlaMB0xGzAZBgNVBAMTEmV4YW1wbGUvV0lOMjAxNi1DQTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAI8ghT719NzSQpoQPh0YT67bYa+PngsxMyvkewP33QLTAWw1HW1Tb9Mk5BDWOItaVsgHwPbf d++M+bLn3AiZnHV OO+k6dVvY/E5qVKEKSGoY+v940S2316lzdWReMOFhgbc2qMertIo ficrRhohonuU Cjyeub3CO+meJUuKom2R47C0D35TUvo/FEHGgXJFaJS1se2UrpN O7KEMkfa1LPuM aob4XE/OzxYQpPa18djsNnskfcFqD/HOTFQN4+SrOhHWIRnUIQBU aLdQaabhipD/ sVs5PneYJX8YKma821uYI6i90YuytmsHBTcIeyC062a8BKqOL7N86

Allow Overrides

确认已选择创建的信任点，然后单击Add。

Add New Certificate



Add a new certificate to the device using cert enrollment object which is used to generate CA and identify certificate.

Device*:

Cert Enrollment*:

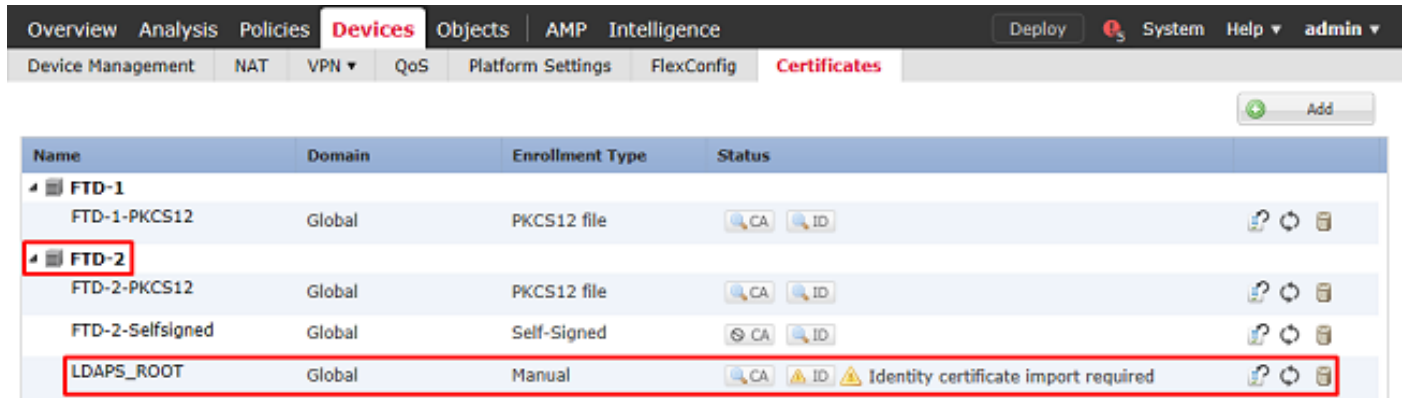
Cert Enrollment Details:

Name: LDAPS_ROOT

Enrollment Type: Manual

SCEP URL: NA

新的信任点显示在FTD下。虽然它提到需要导入身份证书，但并不要求FTD能够对LDAPS服务器发送的SSL证书进行身份验证，因此可以忽略此消息。

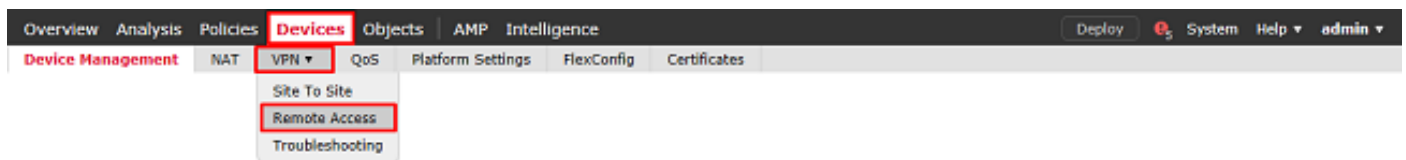


Name	Domain	Enrollment Type	Status
FTD-1			
FTD-1-PKCS12	Global	PKCS12 file	CA ID
FTD-2			
FTD-2-PKCS12	Global	PKCS12 file	CA ID
FTD-2-Selfsigned	Global	Self-Signed	CA ID
LDAPS_ROOT	Global	Manual	CA ID Identity certificate import required

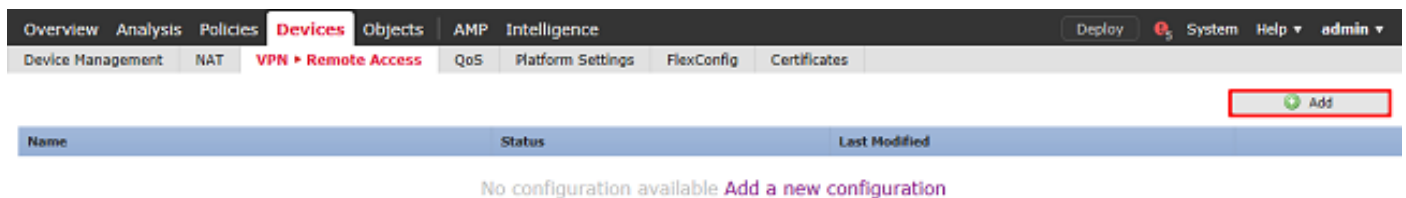
配置AnyConnect进行AD身份验证

1. 这些步骤假设尚未创建远程访问vpn策略。如果已创建策略，请点击该策略的edit按钮，并跳至步骤3。

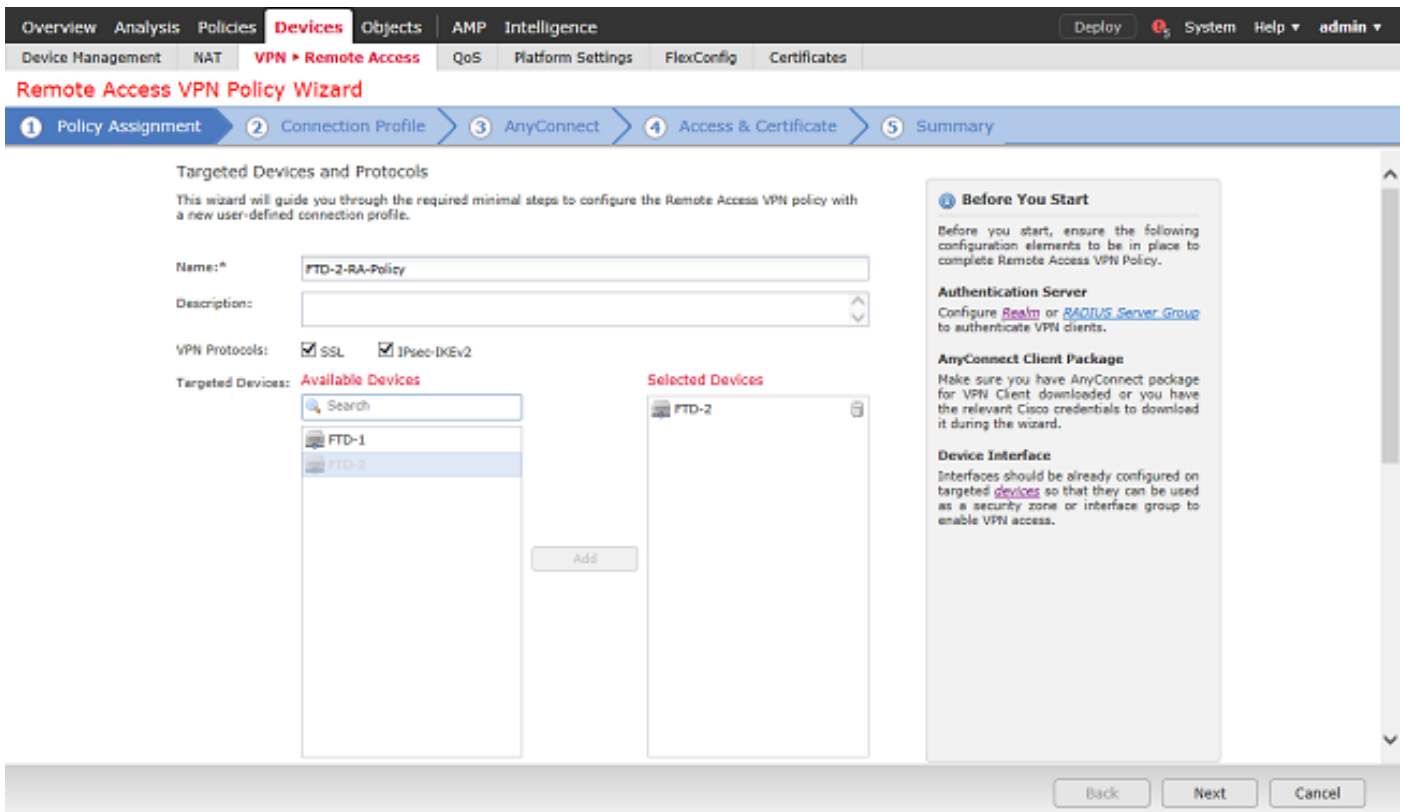
导航到设备 > VPN > 远程访问。



单击Add创建新的远程访问VPN策略



2. 完成远程访问VPN策略向导。在Policy Assignment下，指定策略名称和应用该策略的设备。

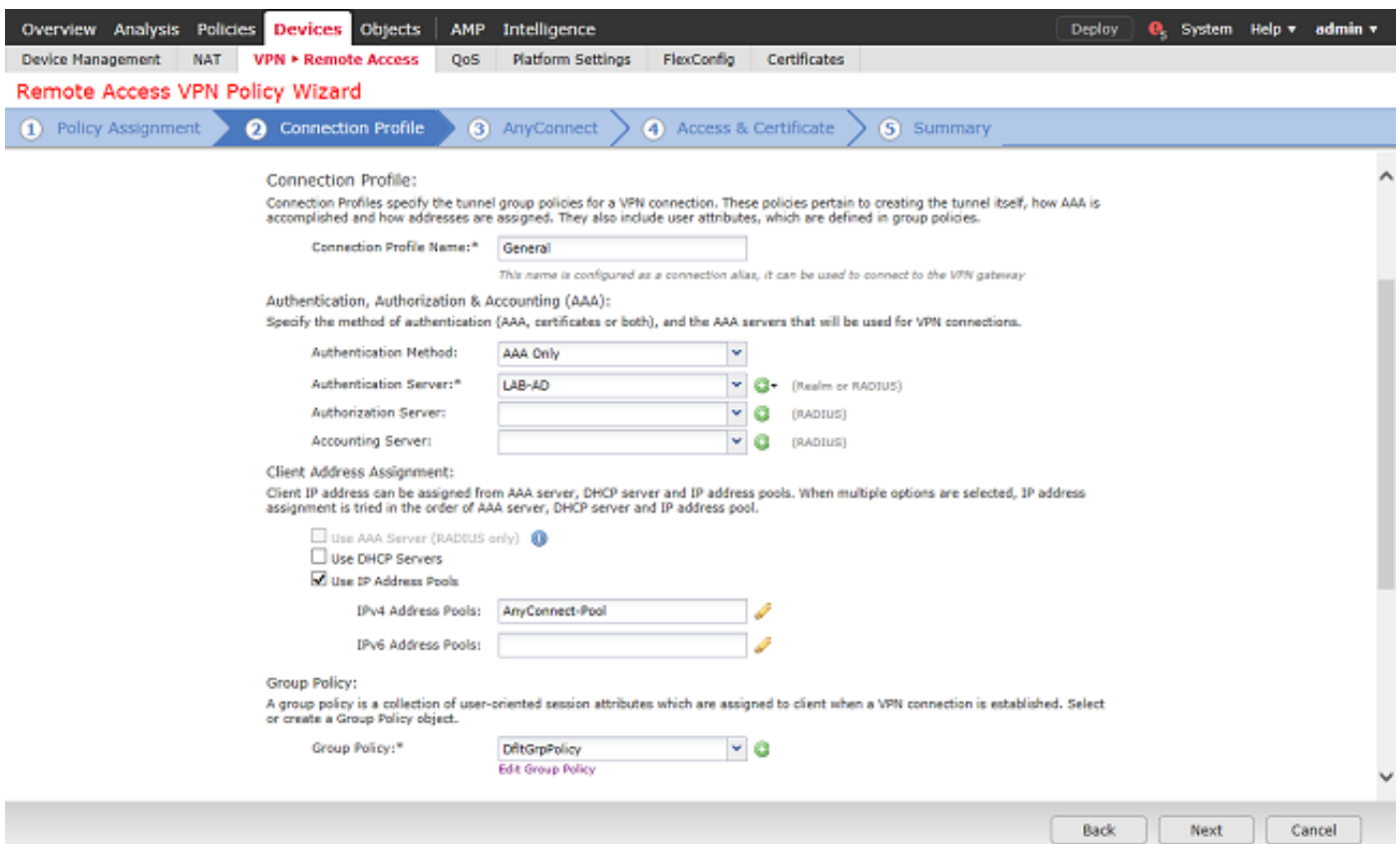


在Connection Profile下，指定Connection Profile的名称，该名称也用作AnyConnect用户在连接时看到的组别名。

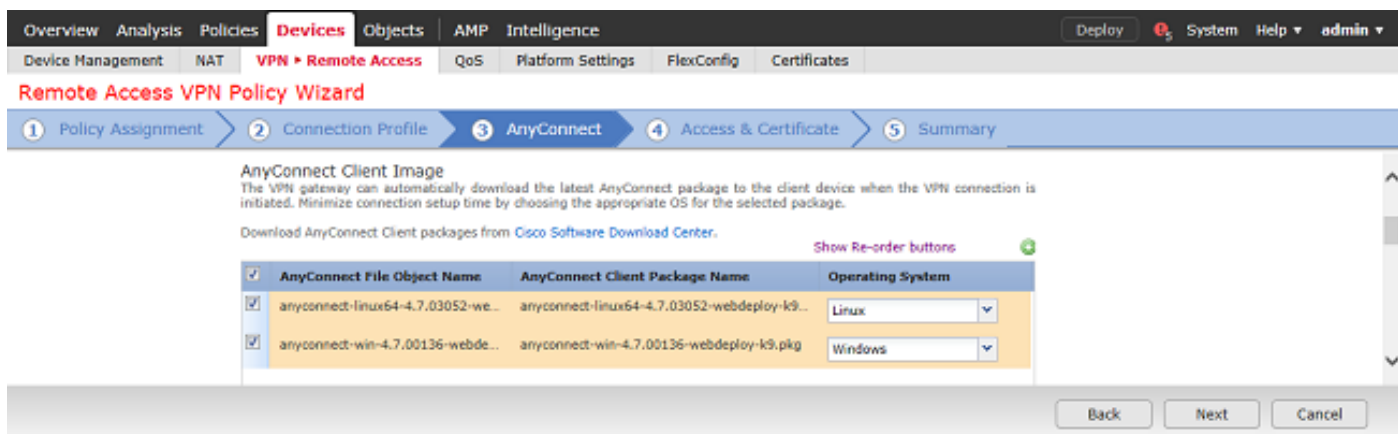
指定以前在Authentication Server下创建的领域。

指定为AnyConnect客户端分配IP地址的方法。

指定用于此连接配置文件的默认组策略。



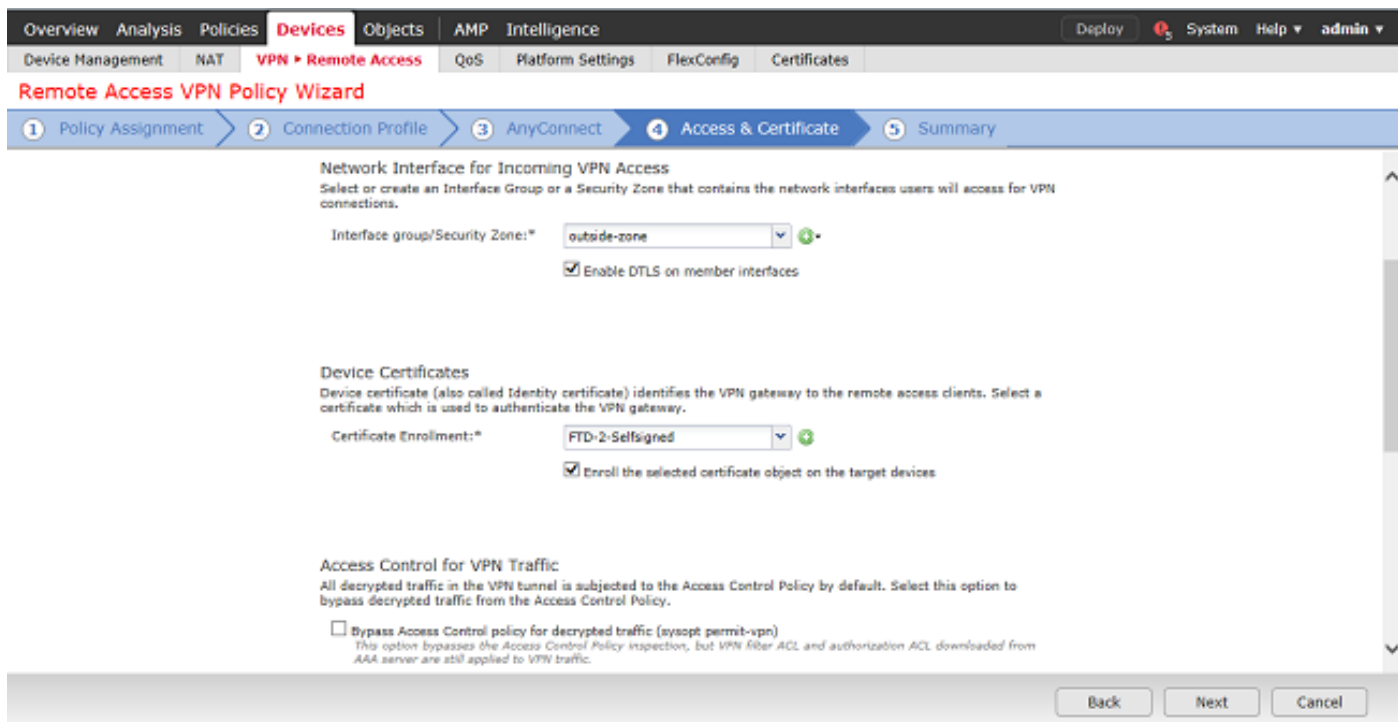
在AnyConnect下，上传并指定使用的AnyConnect软件包。



在Access & Certificate下，指定AnyConnect用户为AnyConnect访问的接口。

创建和/或指定FTD在SSL握手期间使用的证书。

确保取消选中解密流量的旁路访问控制策略(sysopt permit-vpn)复选框，以便稍后创建的用户身份对RAVPN连接生效。



在Summary下，查看配置，然后单击Finish。

Overview Analysis Policies **Devices** Objects AMP Intelligence Deploy System Help admin

Device Management NAT **VPN Remote Access** QoS Platform Settings FlexConfig Certificates

Remote Access VPN Policy Wizard

1 Policy Assignment 2 Connection Profile 3 AnyConnect 4 Access & Certificate 5 Summary

Remote Access VPN Policy Configuration

Firepower Management Center will configure an RA VPN Policy with the following settings

Name: FTD-2-RA-Policy

Device Targets: FTD-2

Connection Profile: General

Connection Alias: General

AAA:

- Authentication Method: AAA Only
- Authentication Server: LAB-AD
- Authorization Server: -
- Accounting Server: -

Address Assignment:

- Address from AAA: -
- DHCP Servers: -
- Address Pools (IPv4): AnyConnect-Pool
- Address Pools (IPv6): -

Group Policy: DfltGrpPolicy

AnyConnect Images:

- anyconnect-linux64-4.7.03052-webdeploy-k9.pkg
- anyconnect-win-4.7.00136-webdeploy-k9.pkg

Interface Objects: outside-zone

Device Certificates: FTD-2-Selfsigned

Device Identity Certificate Enrollment

Certificate enrollment object 'FTD-2-Selfsigned' is not installed on one or more targeted devices. Certificate installation will be initiated on the targeted devices on finishing the wizard. Go to the [Certificates](#) page to check the status of the installation.

Additional Configuration Requirements

After the wizard completes, the following configuration needs to be completed for VPN to work on all device targets.

- Access Control Policy Update**
An [Access Control](#) rule must be defined to allow VPN traffic on all targeted devices.
- NAT Exemption**
If NAT is enabled on the targeted devices, you must define a [NAT Policy](#) to exempt VPN traffic.
- DNS Configuration**
To resolve hostname specified in AAA Servers or CA Servers, configure DNS using [FlexConfig Policy](#) on the targeted devices.
- Port Configuration**
SSL will be enabled on port 443. IPsec-IKEv2 uses port 500 and Client Services will be enabled on port 443 for Anyconnect image download. NAT Traversal will be enabled by default and will use port 4500. Please ensure that these ports are not used in [NAT Policy](#) or other services before deploying the configuration.

Network Interface Configuration

Make sure to add interface from targeted devices to SecurityZone object 'outside-zone'

Back Finish Cancel

3.在远程访问VPN策略下，点击编辑以获取相应的连接配置文件。

Overview Analysis Policies **Devices** Objects AMP Intelligence Deploy System Help admin

Device Management NAT **VPN Remote Access** QoS Platform Settings FlexConfig Certificates

FTD-2-RA-Policy

Enter Description Save Cancel

Policy Assignments (1)

Connection Profile Access Interfaces **Advanced**

Name	AAA	Group Policy
DefaultWEBVPNGroup	Authentication: None Authorization: None Accounting: None	DfltGrpPolicy
General	Authentication: LAB-AD (AD) Authorization: None Accounting: None	DfltGrpPolicy

确保身份验证服务器设置为之前创建的领域。

在Advanced Settings下，可以选中Enable Password Management以允许用户在其密码到期时或到期之前更改其密码。

但是，此设置要求领域使用LDAPS。如果进行了任何更改，请单击Save。

Edit Connection Profile

Connection Profile:*

Group Policy:* [Edit Group Policy](#)

Client Address Assignment **AAA** Aliases

Authentication

Authentication Method:

Authentication Server:

Use secondary authentication

Authorization

Authorization Server:

Allow connection only if user exists in authorization database

Accounting

Accounting Server:

Advanced Settings

Strip Realm from username

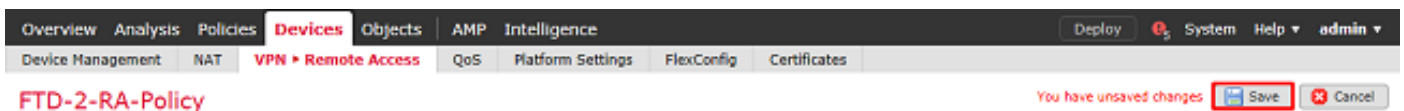
Strip Group from username

Enable Password Management

Notify User days prior to password expiration

Notify user on the day of password expiration

完成后，点击右上角的**Save**。



启用身份策略并配置用户身份的安全策略

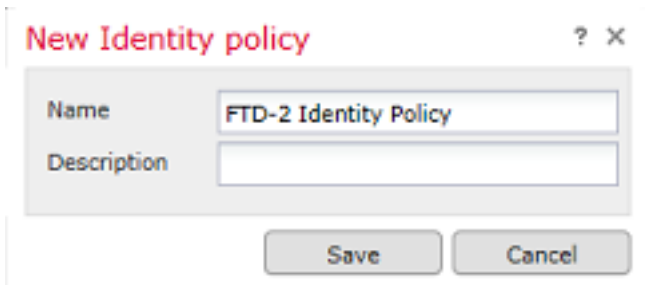
1. 导航到策略>访问控制>身份。



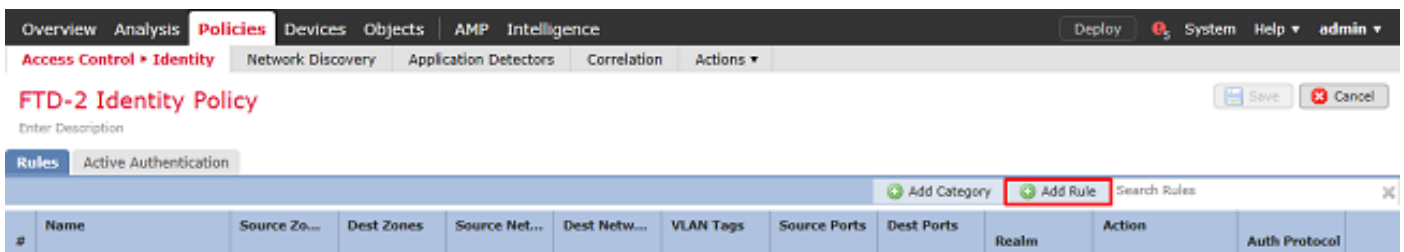
创建新的身份策略。



指定新身份策略的名称。

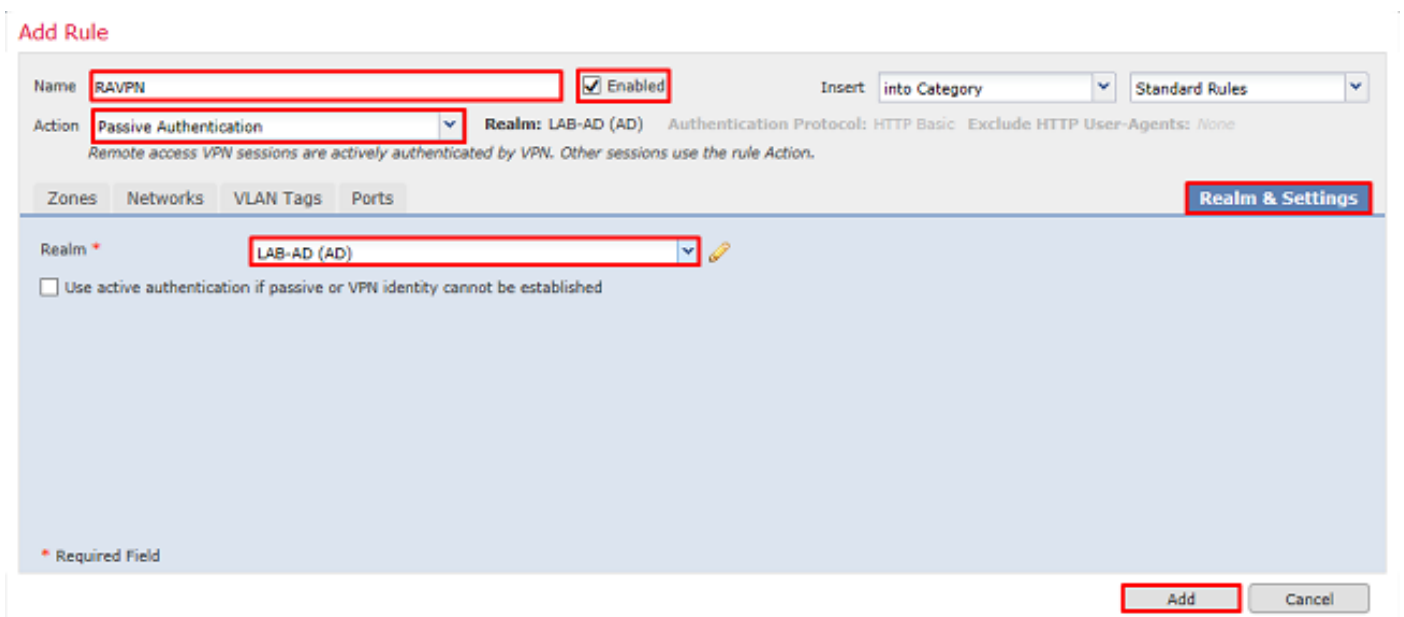


2.单击添加规则。

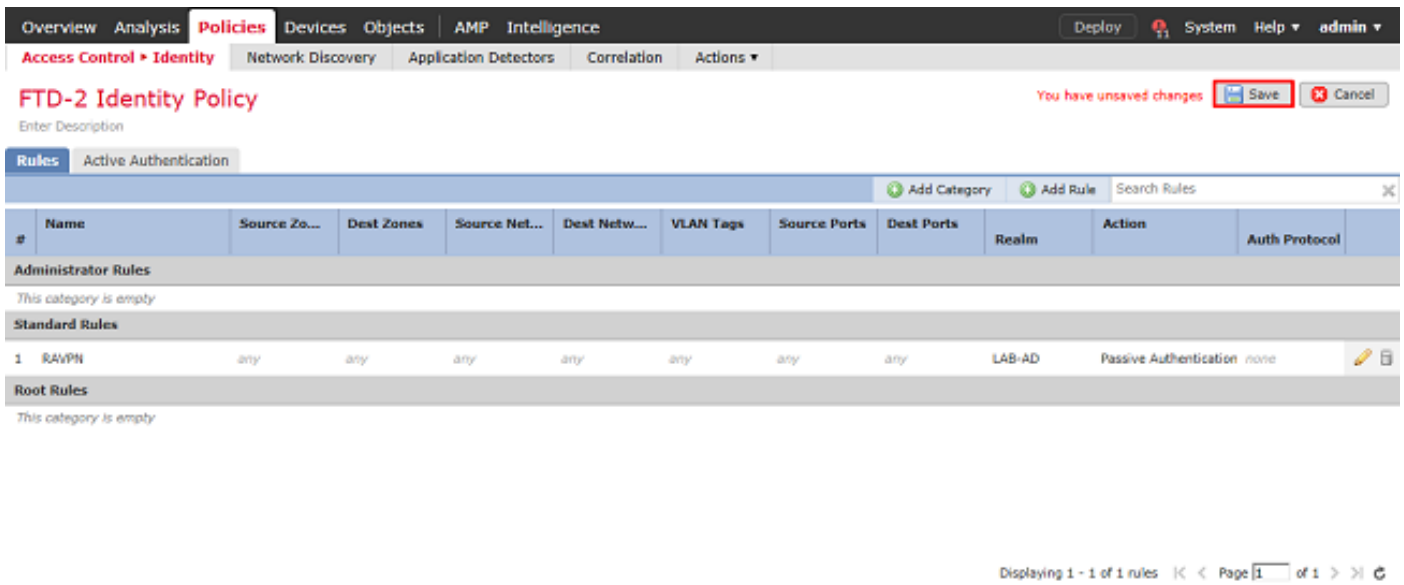


3.为新规则指定Name。确保已启用该功能并将操作设置为“被动身份验证”。

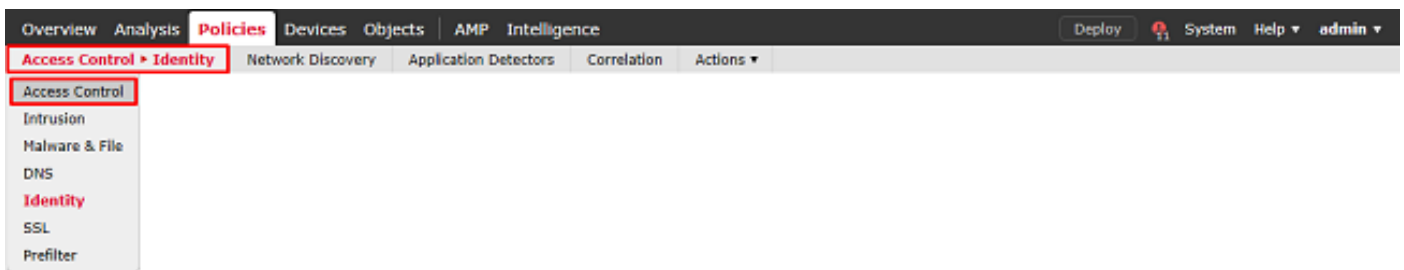
单击Realm & Settings选项卡，然后选择之前创建的领域。完成后，单击Add。



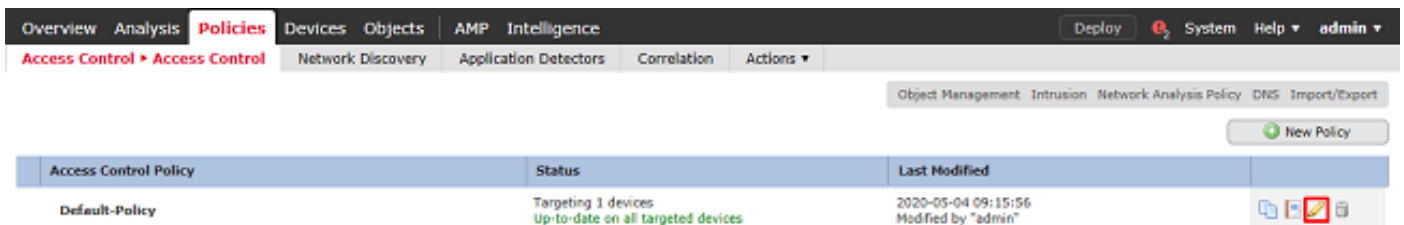
4.单击保存。



5. 定位至策略>访问控制>访问控制。



6. 编辑FTD配置在下的访问控制策略。



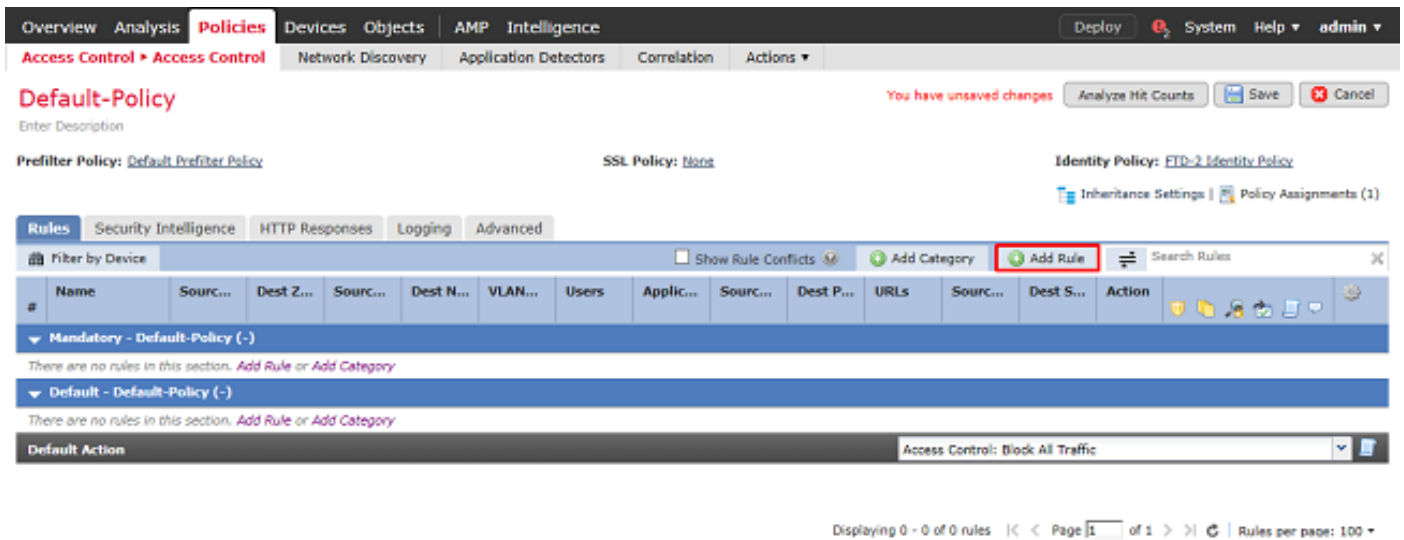
7. 单击Identity Policy (身份策略) 旁边的值。



选择之前创建的Identity Policy，然后单击OK。



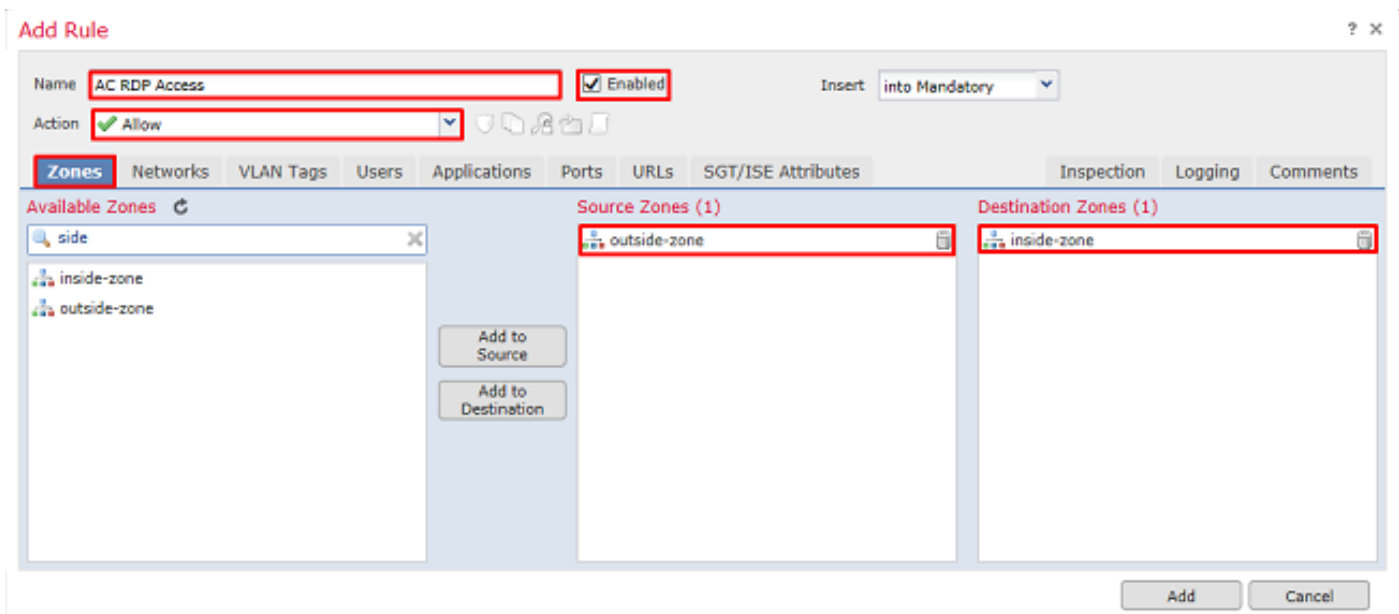
8. 单击添加规则以创建新的ACP规则。这些步骤将创建一个规则，允许AnyConnect管理员组中的用户使用RDP连接到内部网络中的设备。



指定规则的名称。确保规则已启用并具有相应的操作。

在Zones选项卡下，为相关流量指定适当的区域。

用户发起的RDP流量进入源自外部区域接口的FTD并出口内部区域。



在**网络**下，定义源网络和目标网络。

对象AnyConnect_Pool包括分配给AnyConnect客户端的IP地址。

对象Inside_Net包括内部网络子网。

Add Rule

Name: AC RDP Access Enabled Insert: into Mandatory

Action: Allow

Zones: **Networks** VLAN Tags Users Applications Ports URLs SGT/ISE Attributes Inspection Logging Comments

Available Networks

Search by name or value

Networks Geolocation

- Inside_Net
- IPv4-Benchmark-Tests
- IPv4-Link-Local
- IPv4-Multicast
- IPv4-Private-10.0.0.0-8
- IPv4-Private-172.16.0.0-12
- IPv4-Private-192.168.0.0-16
- IPv4-Private-All-RFC1918
- IPv6-IPv4-Mapped

Add To Source Networks

Add To Destination

Source Networks (1)

Source	Original Client
AnyConnect_Pool	

Enter an IP address Add

Destination Networks (1)

Inside_Net

Enter an IP address Add

Add Cancel

在Users下，单击Available Realms下之前创建的领域，单击Available Users下相应的组/用户，然后单击Add to Rule。

如果Available Users部分下没有可用的用户或组，请确保FMC能够下载realm部分下的Users和Groups，并且包含相应的Groups/User。

从源角度检查此处指定的用户/组。

例如，根据此规则到目前为止所定义的内容，FTD评估流量是源自外部区域并发往内部区域，源自AnyConnect_Pools对象中的网络并发往Inside_Net对象中的网络，而流量源自AnyConnect Admins组中的用户。

Add Rule

Name: AC RDP Access Enabled Insert: into Mandatory

Action: Allow

Zones: Networks VLAN Tags **Users** Applications Ports URLs SGT/ISE Attributes Inspection Logging Comments

Available Realms

Search by name or value

- Special Identities
- LAB-AD

Available Users

Search by name or value

- LAB-AD/*
- AnyConnect Admins
- AnyConnect Users
- it.admin
- test.user

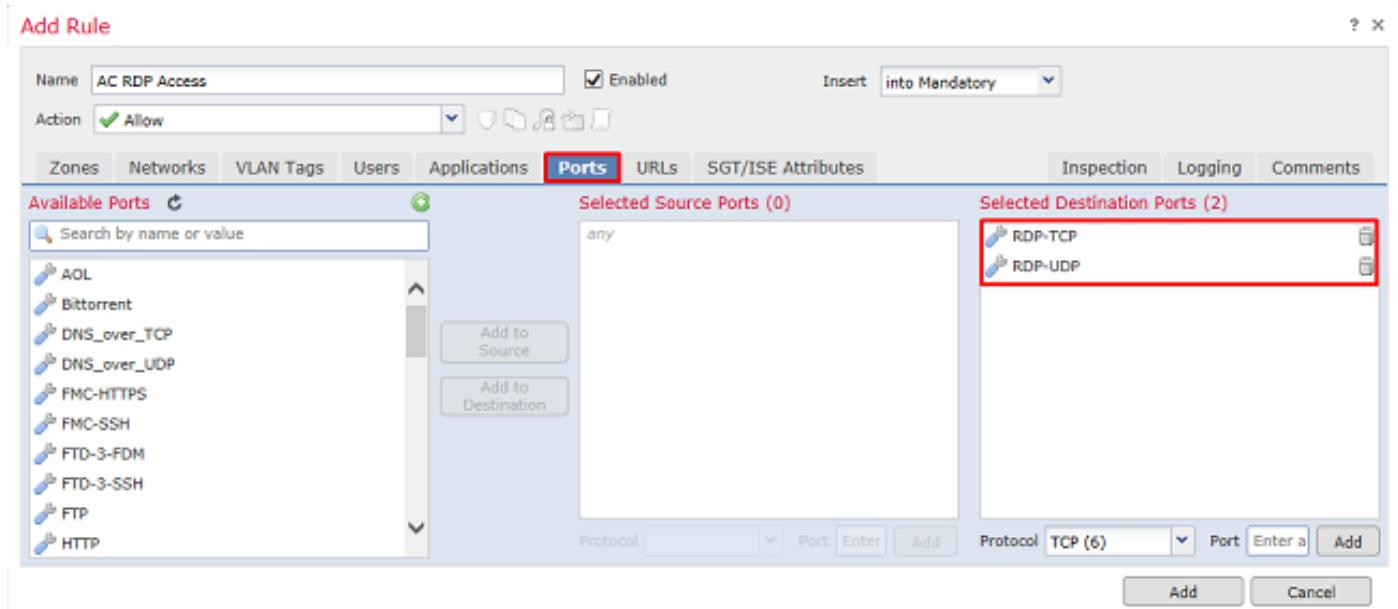
Add to Rule

Selected Users (1)

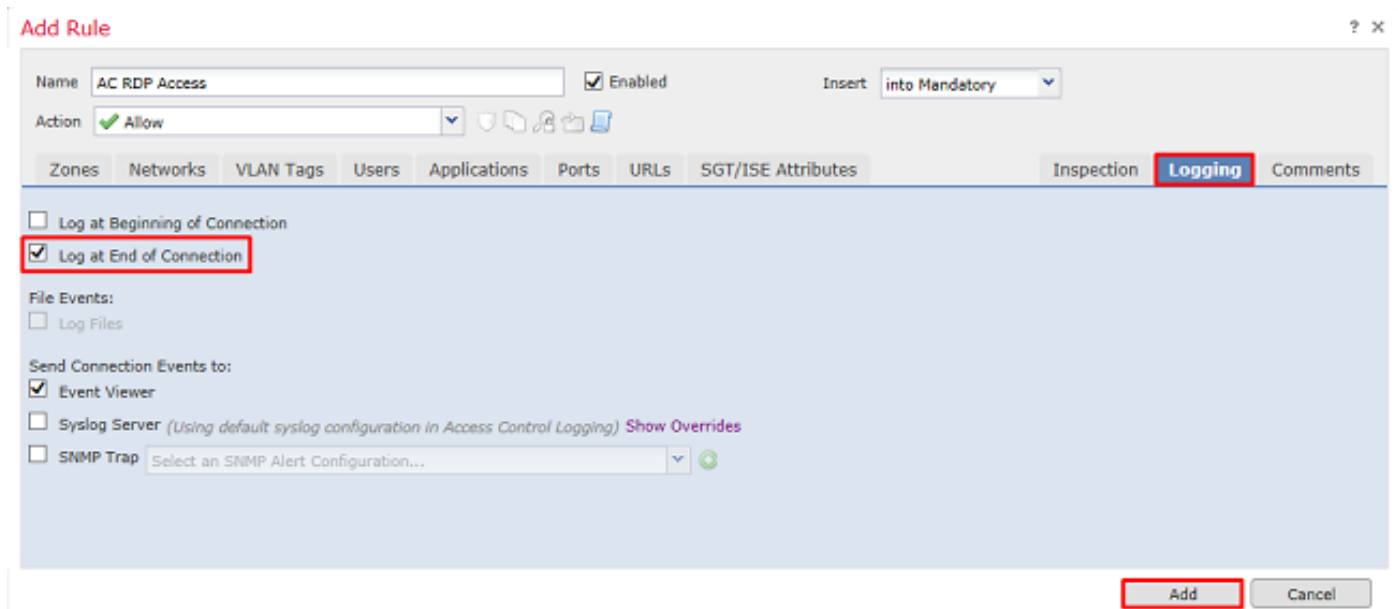
LAB-AD/AnyConnect Admins

Add Cancel

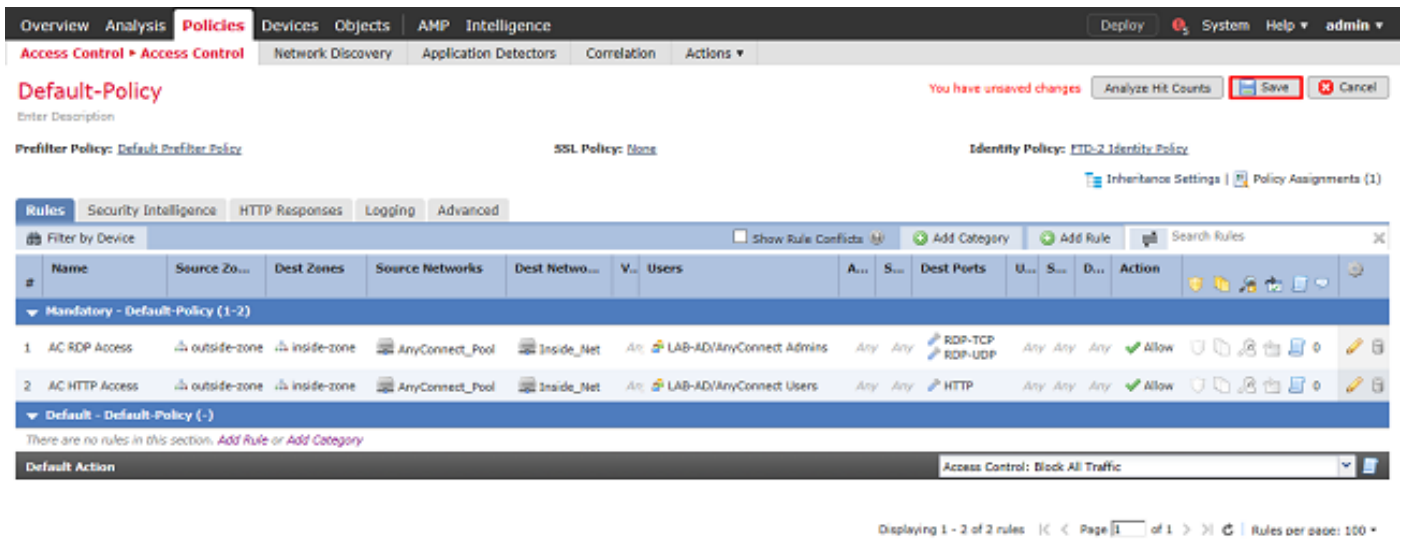
在Ports下，创建并添加自定义RDP对象以允许TCP和UDP端口3389。请注意，本可以在Applications部分下添加RDP，但为简单起见，只检查端口。



最后，在Logging下，Log at End of Connection会进行检查，以便稍后进行其他验证。完成后单击Add。



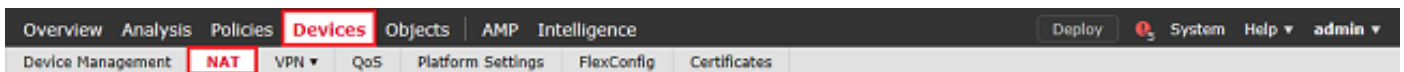
9.为HTTP访问创建了一个附加规则，以允许组AnyConnect User中的用户访问Windows Server IIS网站。Click Save.



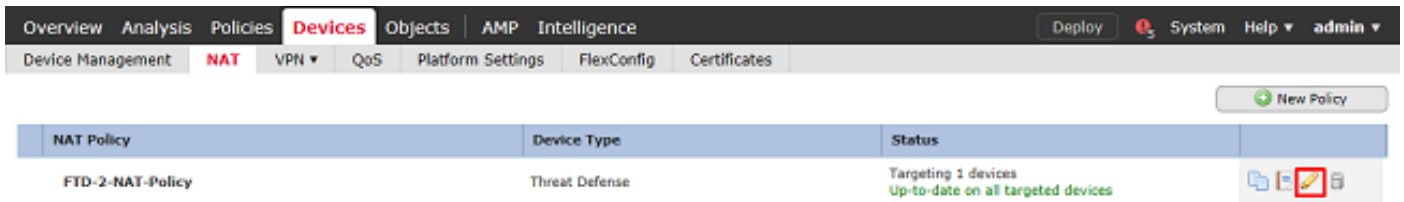
配置NAT免除

如果存在影响AnyConnect流量的NAT规则（如互联网PAT规则），则必须配置NAT免除规则，以使AnyConnect流量不会受到NAT影响。

1. 导航到设备 > NAT。

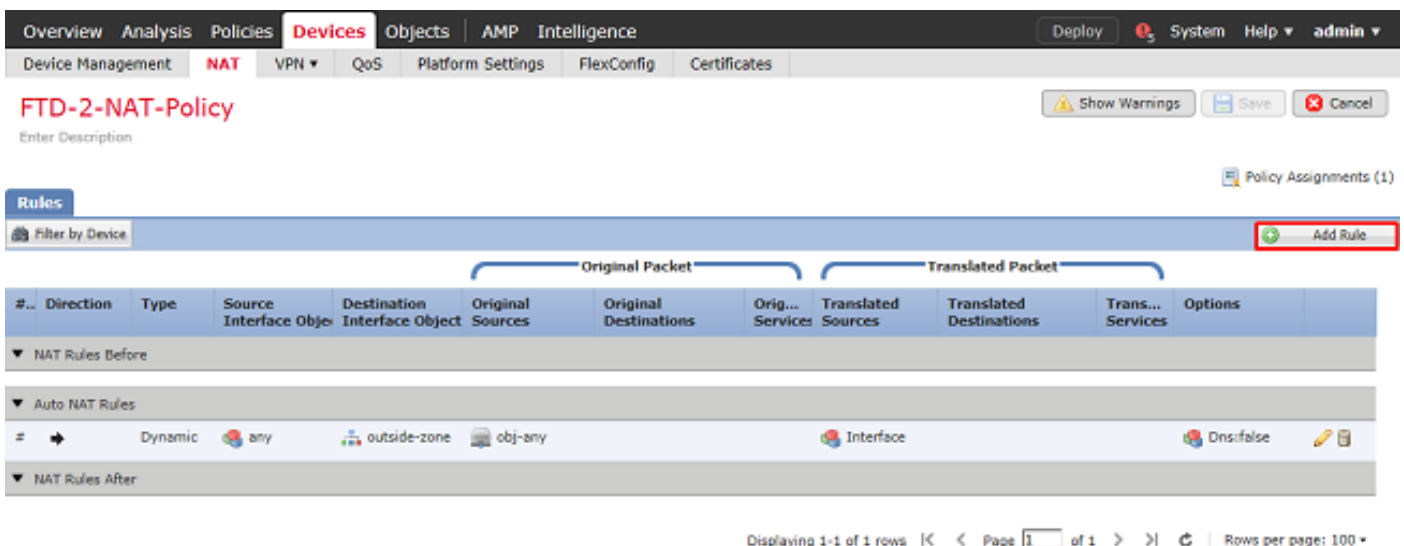


选择应用于FTD的NAT策略。



2. 在此NAT策略中，在末尾有一个动态PAT，该PAT会影响从外部接口传出到外部接口的所有流量（包括AnyConnect流量）。

要防止AnyConnect流量受NAT影响，请点击右上角的Add Rule。



3.配置NAT免除规则，确保该规则是类型为Static的手动NAT规则。这是适用于AnyConnect流量的双向NAT规则。

使用这些设置，当FTD检测到从Inside_Net发往AnyConnect IP地址（由AnyConnect_Pool定义）的流量时，源地址将转换为相同的值(Inside_Net)，当流量进入inside_zone并离开outside_zone时，目标地址将转换为相同的值(AnyConnect_Pool)。当满足这些条件时，这基本上会绕过NAT。

The screenshot shows the 'Add NAT Rule' dialog box with the following settings:

- NAT Rule: Manual NAT Rule
- Type: Static
- Enable:
- Source Interface Objects (1): inside-zone
- Destination Interface Objects (1): outside-zone

The screenshot shows the 'Add NAT Rule' dialog box with the following settings in the 'Translation' tab:

- Original Packet:
 - Original Source: Inside_Net
 - Original Destination: AnyConnect_Pool
- Translated Packet:
 - Translated Source: Address
 - Translated Destination: AnyConnect_Pool

此外，FTD设置为对此流量执行路由查找，而不是代理ARP。完成后单击确定。

Add NAT Rule ? X

NAT Rule: Insert:

Type: Enable

Description:

Interface Objects Translation PAT Pool **Advanced**

Translate DNS replies that match this rule

Fallthrough to Interface PAT(Destination Interface)

IPv6

Net to Net Mapping

Do not proxy ARP on Destination Interface

Perform Route Lookup for Destination Interface

Unidirectional

4.单击保存。

Overview Analysis Policies **Devices** Objects AMP Intelligence Deploy System Help admin

Device Management **NAT** VPN QoS Platform Settings FlexConfig Certificates

FTD-2-NAT-Policy You have unsaved changes

Enter Description Policy Assignments (1)

Rules Add Rule

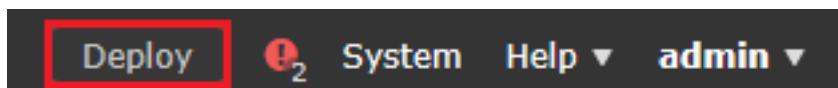
Filter by Device

#	Direction	Type	Original Packet		Translated Packet		Orig... Services	Translated Sources	Translated Destinations	Trans... Services	Options
			Source Interface Object	Destination Interface Object	Original Sources	Original Destinations					
▼ NAT Rules Before											
1	↔	Static	inside-zone	outside-zone	Inside_Net	AnyConnect_Pool		Inside_Net	AnyConnect_Pool		Dns:false route-lookup no-proxy-arp
▼ Auto NAT Rules											
=	↔	Dynamic	any	outside-zone	obj-any			Interface			Dns:false
▼ NAT Rules After											

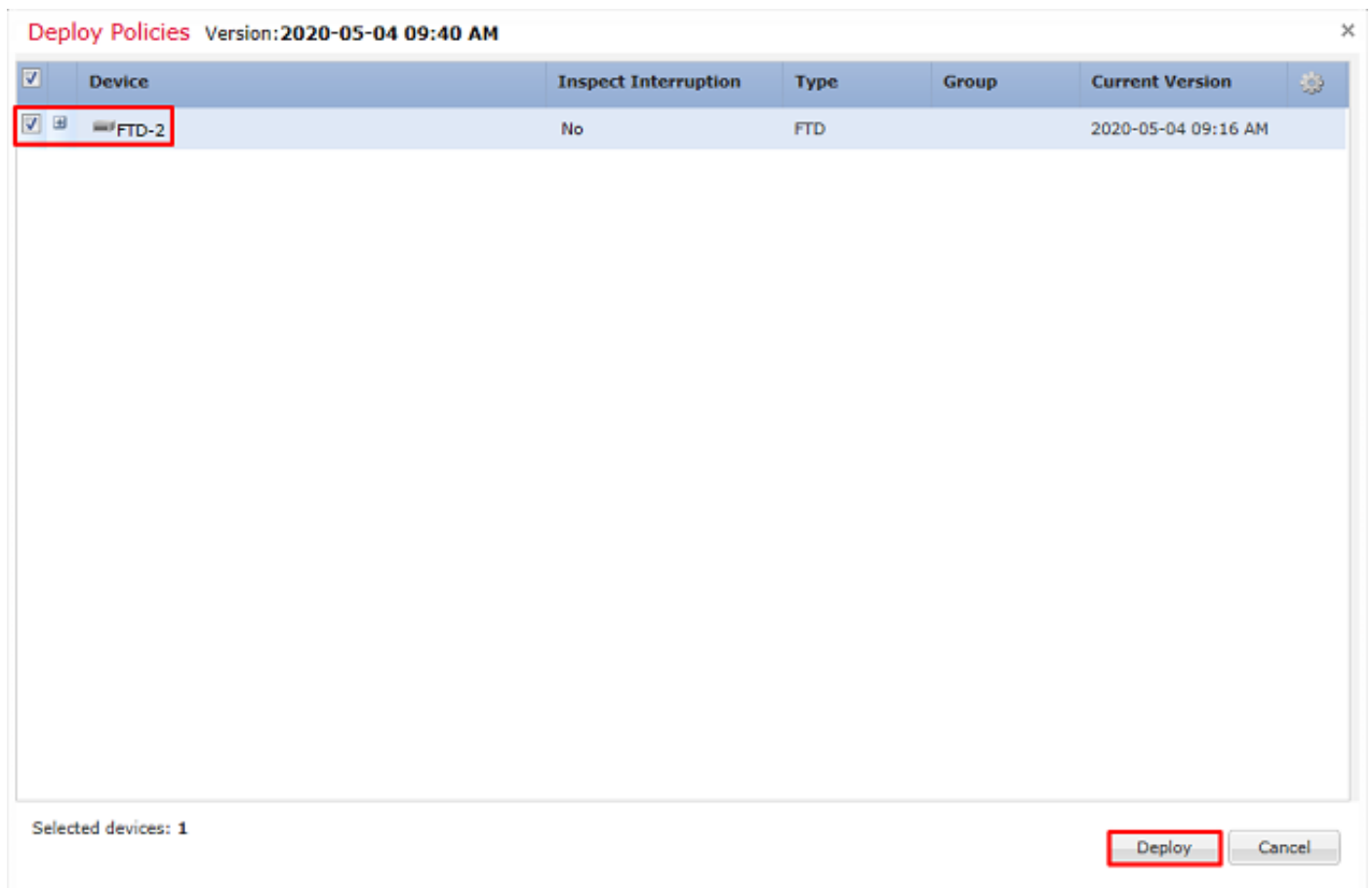
Displaying 1-2 of 2 rows | Page 1 of 1 | Rows per page: 100

部署

1.配置完成后，点击右上角的Deploy按钮。



2.点击应用配置的FTD旁边的复选框，然后点击部署。



验证

最终配置

AAA配置

```
> show running-configuration aaa-server
aaa-server LAB-AD protocol ldap
  max-failed-attempts 4
  realm-id 5
aaa-server LAB-AD host win2016.example.com
  server-port 389
  ldap-base-dn DC=example,DC=com
  ldap-group-base-dn DC=example,DC=com
  ldap-scope subtree
  ldap-naming-attribute samaccountname
  ldap-login-password *****
  ldap-login-dn ftd.admin@example.com
  server-type microsoft
```

AnyConnect配置

```
> show running-config webvpn
webvpn
  enable Outside
  anyconnect image disk0:/csm/anyconnect-linux64-4.7.03052-webdeploy-k9.pkg 1 regex "Linux"
  anyconnect image disk0:/csm/anyconnect-win-4.7.00136-webdeploy-k9.pkg 2 regex "Windows"
  anyconnect profiles Lab disk0:/csm/lab.xml
```

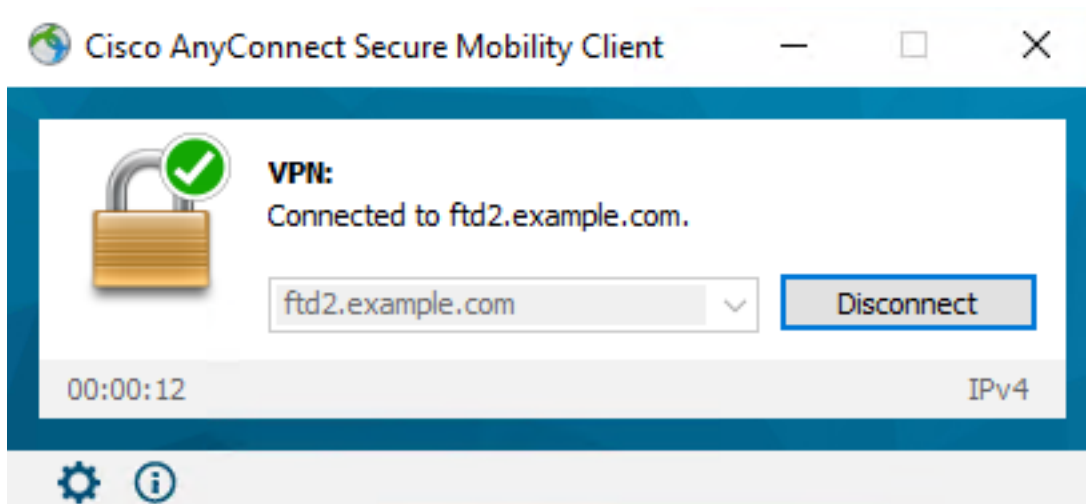
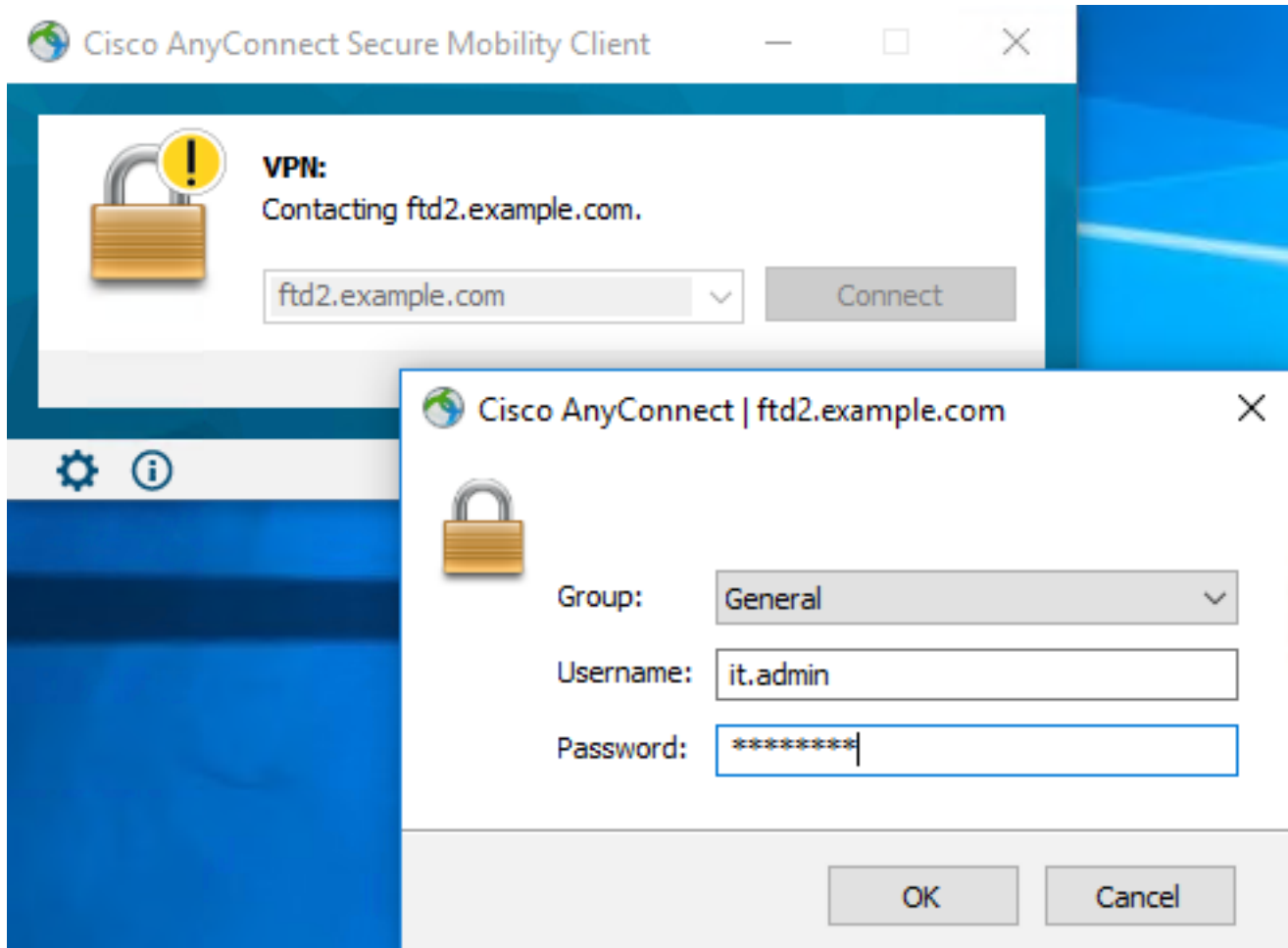
```
anyconnect enable
tunnel-group-list enable
cache
  no disable
error-recovery disable

> 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-simultaneous-logins 10
  vpn-tunnel-protocol ikev2 ssl-client
  split-tunnel-policy tunnelspecified
  split-tunnel-network-list value Lab
  user-authentication-idle-timeout none
webvpn
  anyconnect keep-installer none
  anyconnect modules value dart
  anyconnect ask none default anyconnect
  http-comp none
  activex-relay disable
  file-entry disable
  file-browsing disable
  url-entry disable
  deny-message none
  anyconnect ssl df-bit-ignore enable

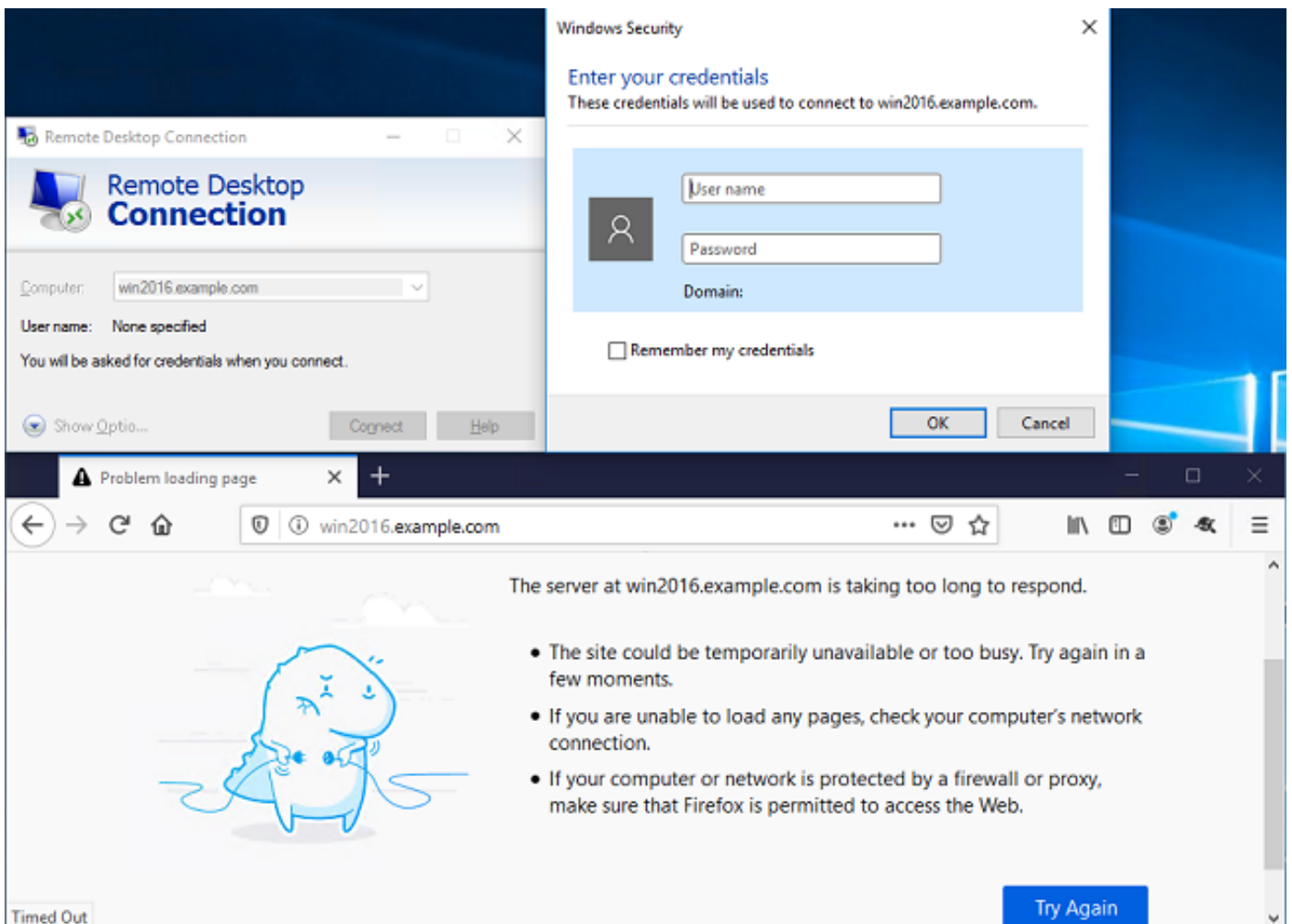
> show running-config ssl
ssl trust-point FTD-2-SelfSigned outside
```

使用AnyConnect连接并验证访问控制策略规则

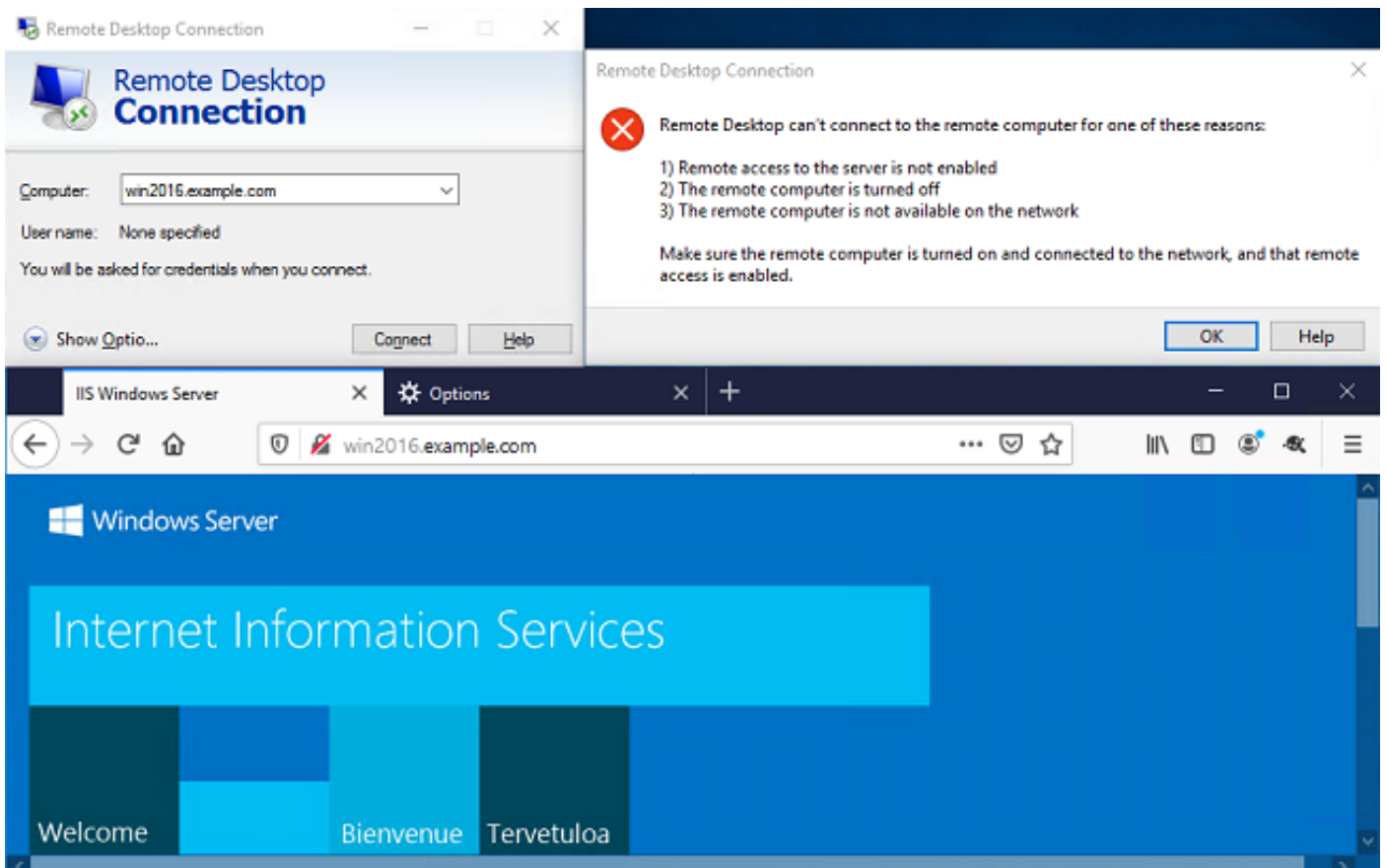


用户IT Admin位于AnyConnect Admins组中，该组具有Windows Server的RDP访问权限，但无权访问HTTP。

打开与此服务器的RDP和Firefox会话将验证此用户只能通过RDP访问服务器。



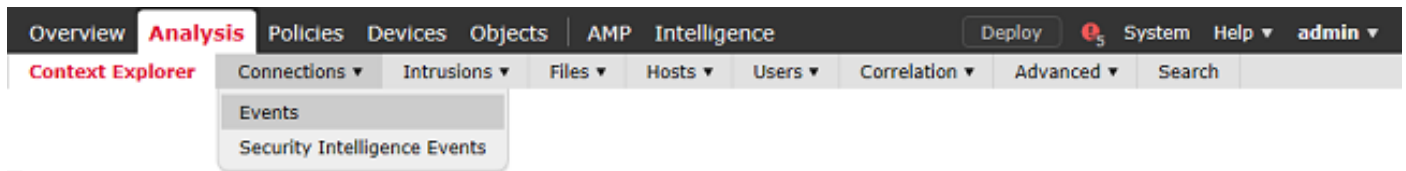
如果使用AnyConnect Users（作为HTTP访问而不是RDP访问）组中的用户测试用户登录，我们可以验证访问控制策略规则是否生效。



使用FMC连接事件进行验证

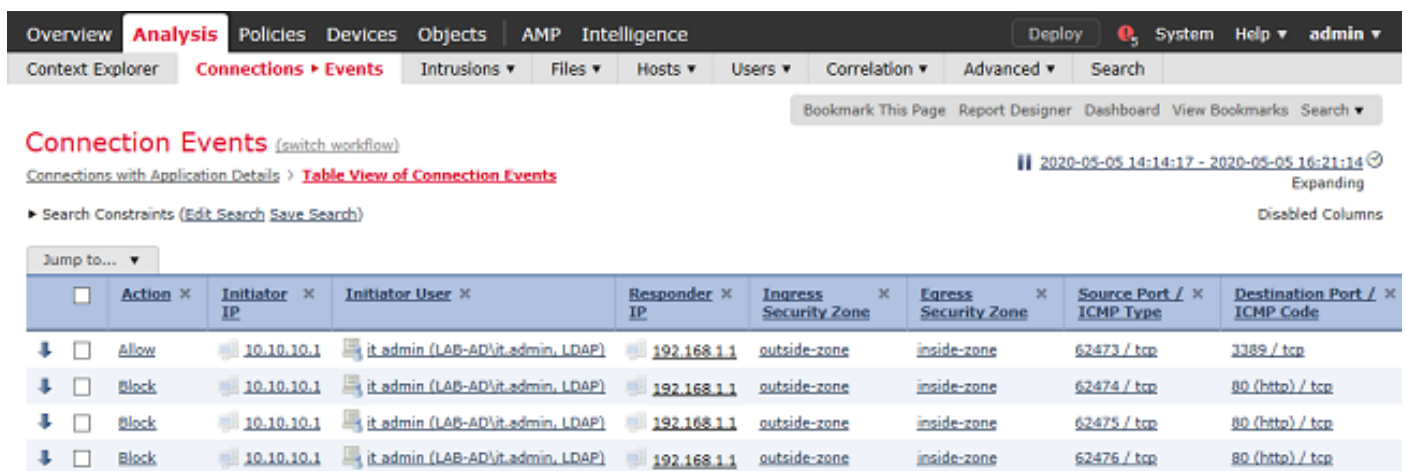
由于访问控制策略规则中启用了日志记录，因此可以检查连接事件中是否存在与这些规则匹配的任何流量

导航到分析>连接>事件。

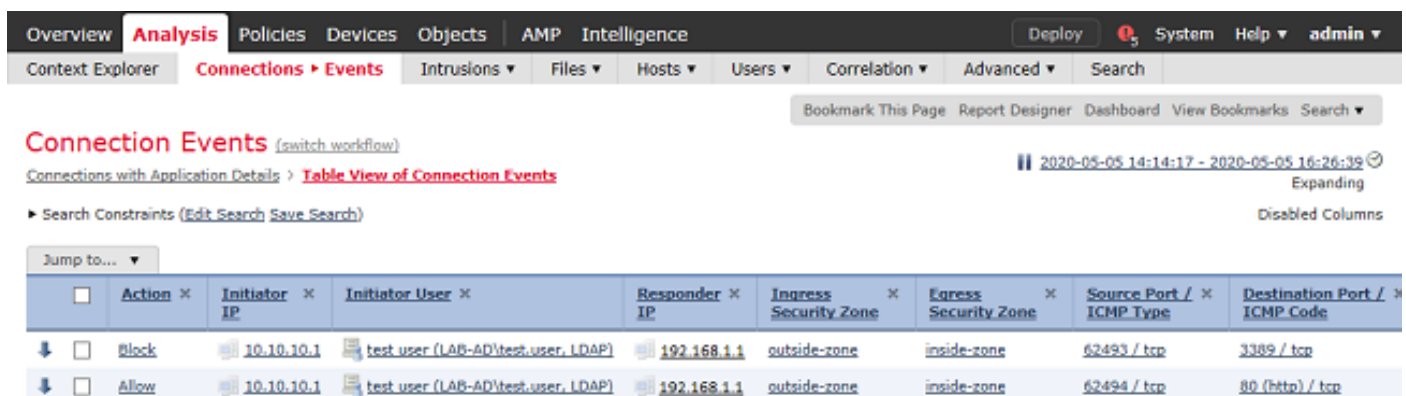


在Table View of Connection Events下，日志被过滤为仅显示IT管理员的连接事件。

在这里，您可以验证是否允许到服务器的RDP流量（TCP和UDP 3389），但端口80流量被阻止。



对于用户Test User，您可以验证到服务器的RDP流量是否被阻止，以及端口80流量是否被允许。



故障排除

调试

此调试可以在诊断CLI中运行，以对LDAP身份验证相关问题进行故障排除：`debug ldap 255`

要排除用户身份访问控制策略问题，可以在云中运行`system support firewall-engine-debug`，以确定流量被意外允许或阻止的原因。

正在运行的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...;.....j...
[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：

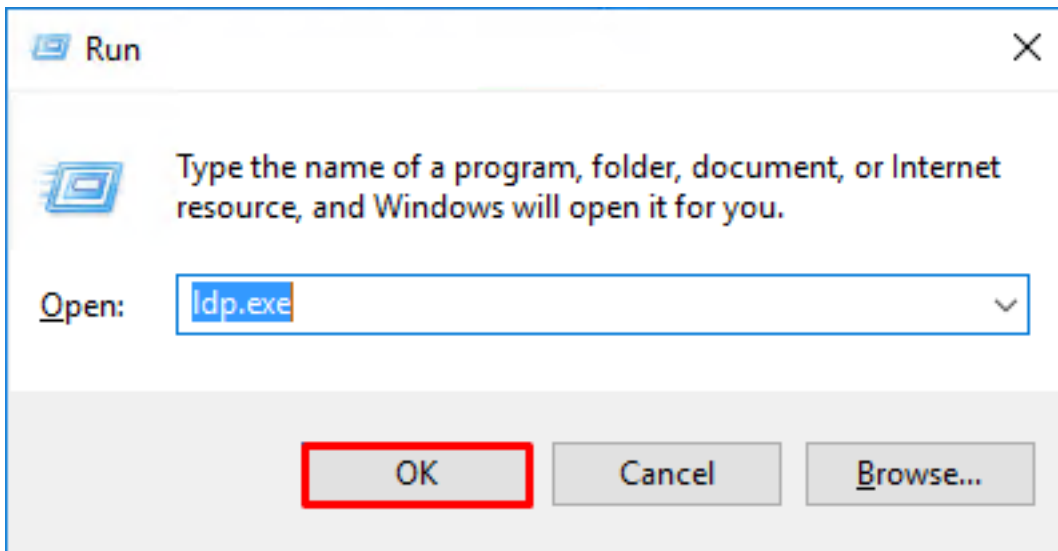
- 检查路由并确保FTD正在从LDAP服务器收到响应。
- 如果使用LDAPS或STARTTLS，请确保信任正确的根CA证书，以便SSL握手可以成功完成。
- 检验是否使用了正确的IP地址和端口。如果使用主机名，请验证DNS是否能够将其解析为正确的IP地址。

绑定登录DN和/或密码不正确

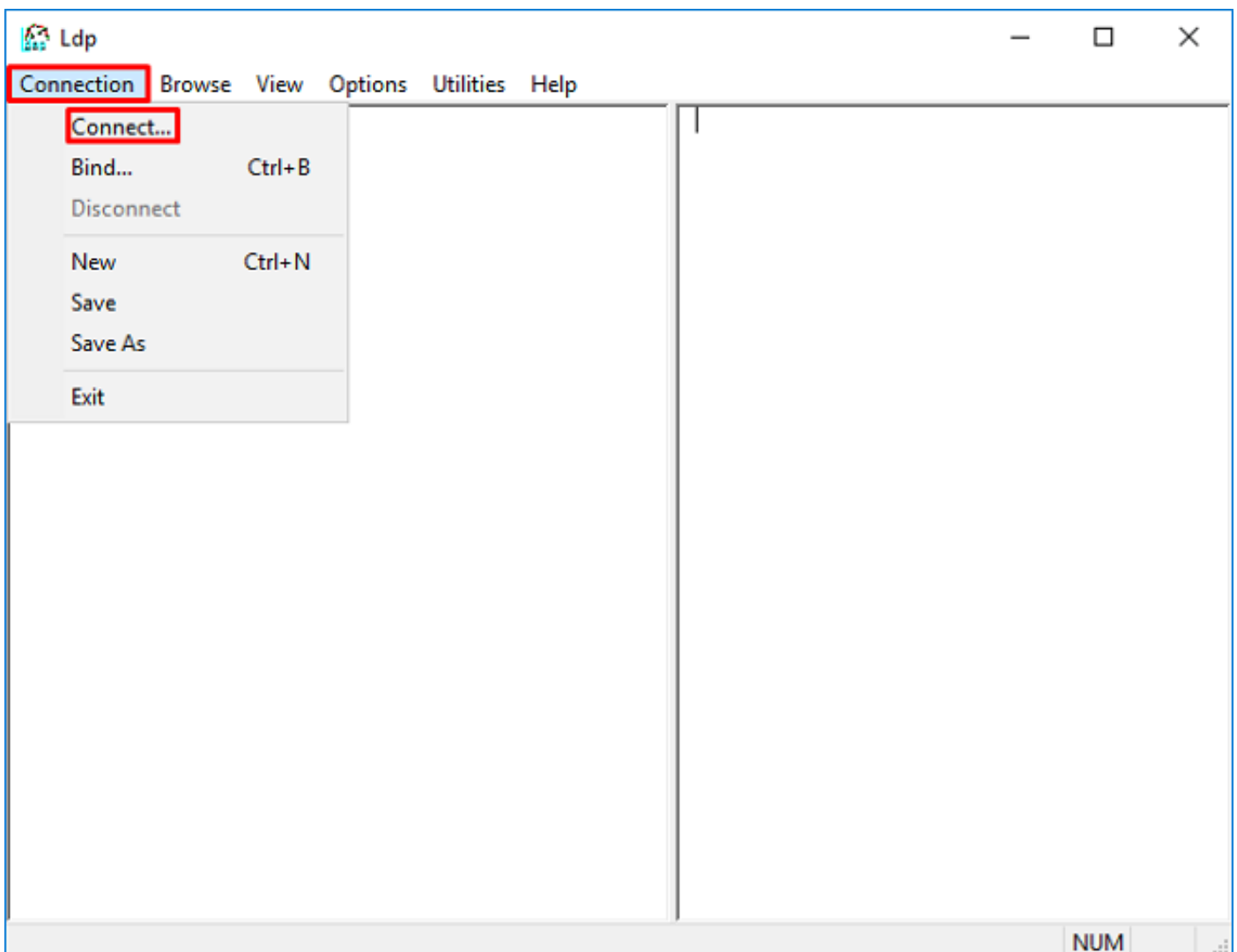
```
[-2147483615] Session Start
[-2147483615] New request Session, context 0x00007f9e65ccdc40, reqType = Authentication
[-2147483615] Fiber started
[-2147483615] Creating LDAP context with uri=ldap://192.168.1.1:389
[-2147483615] Connect to LDAP server: ldap://192.168.1.1:389, status = Successful
[-2147483615] 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和登录密码是否正确配置。这可以在带有ldp.exe的AD服务器上进行验证。要验证某个帐户是否可以使用ldp成功绑定，请执行以下步骤：

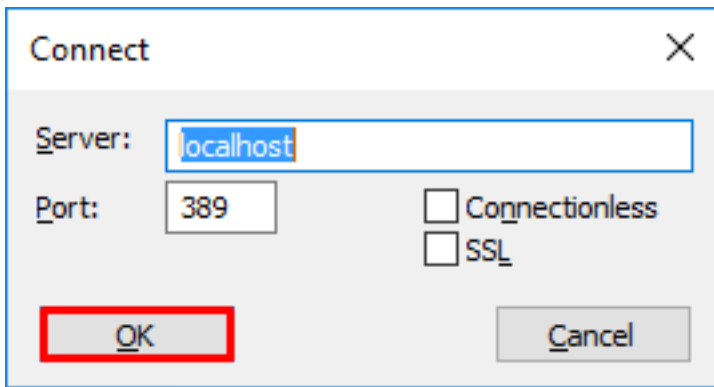
1.在AD服务器上，按Win+R并搜索ldp.exe



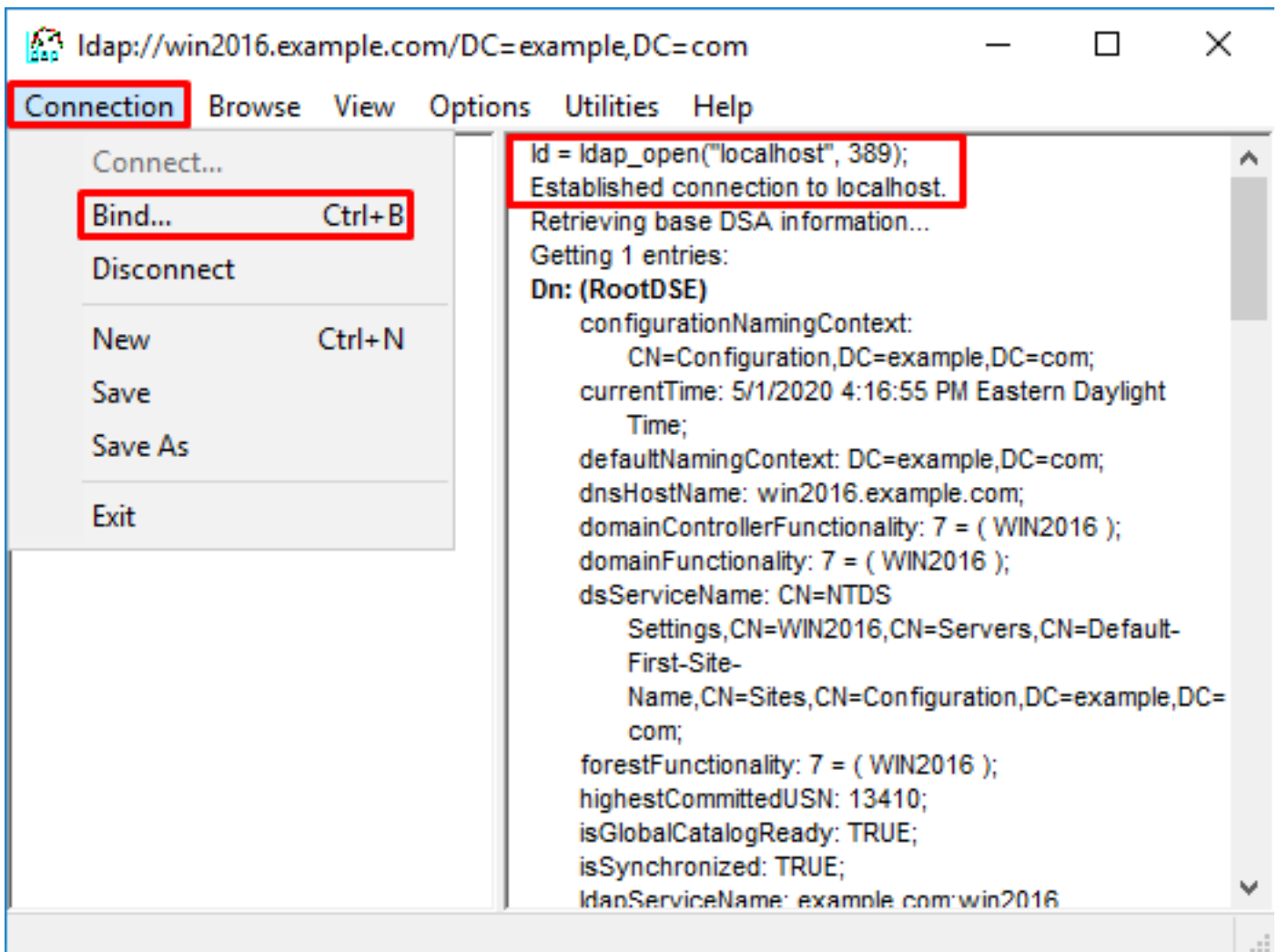
2.在连接下，选择连接.....



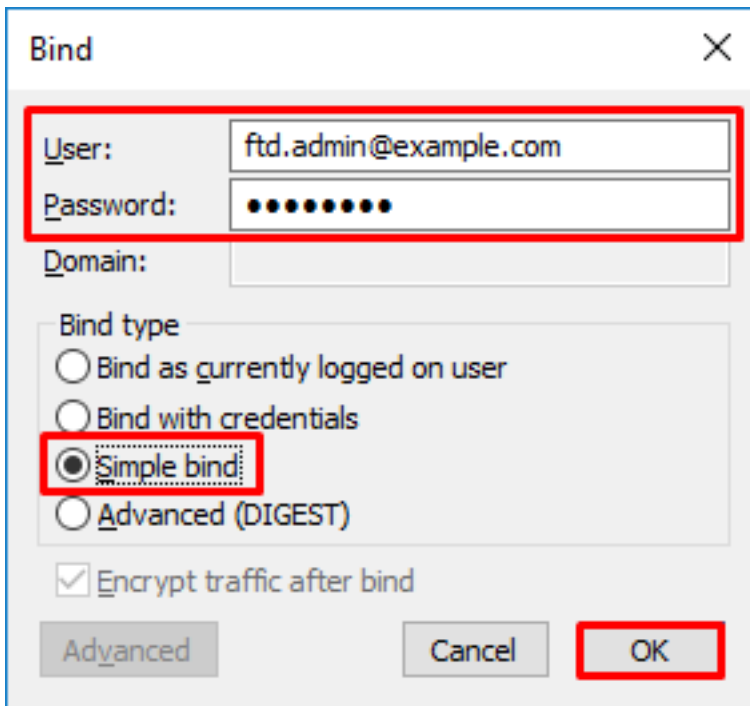
3.指定服务器的本地主机和适当的端口，然后单击确定。



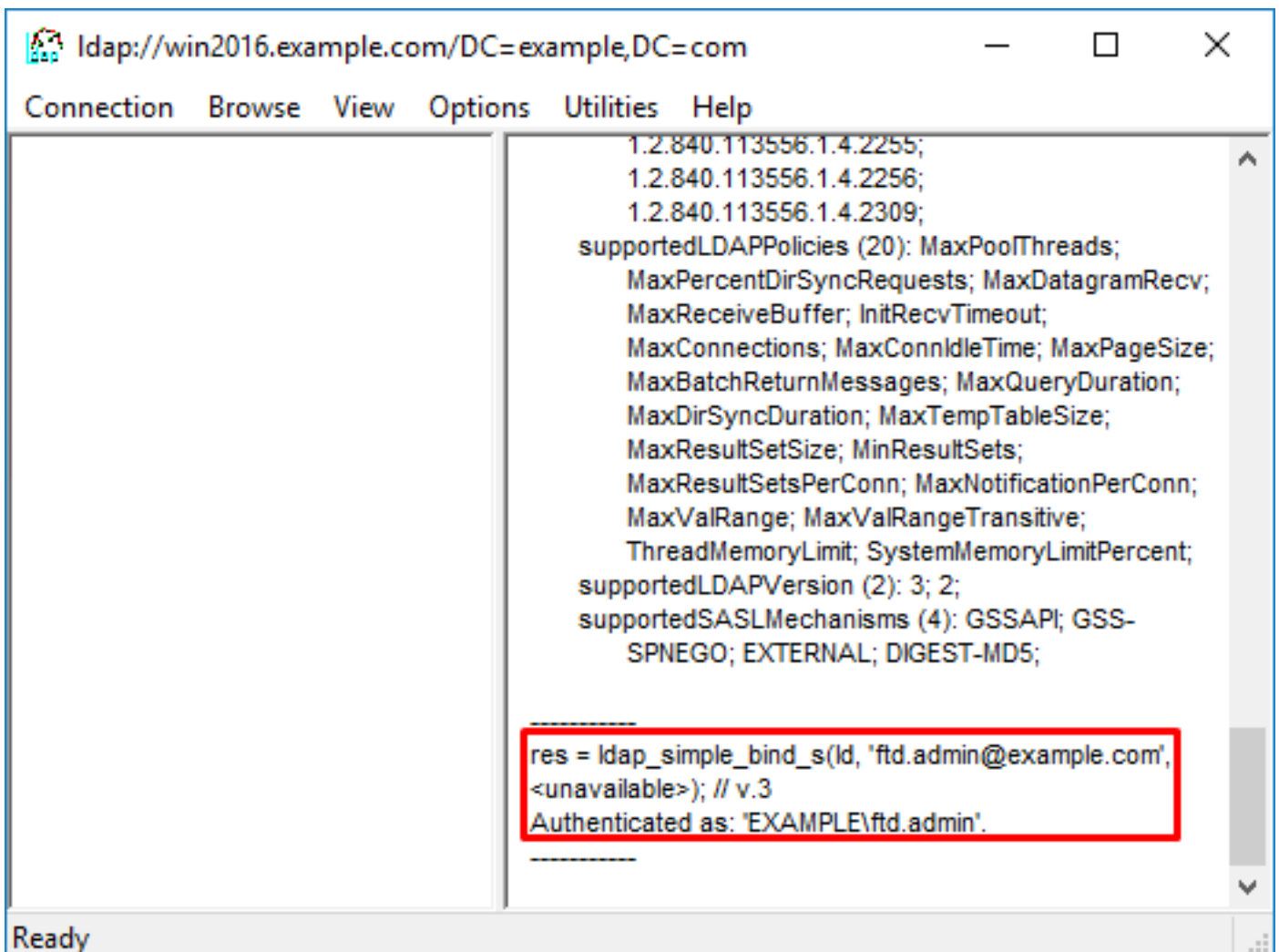
4.右列显示指示连接成功的文本。导航到**连接>绑定.....**



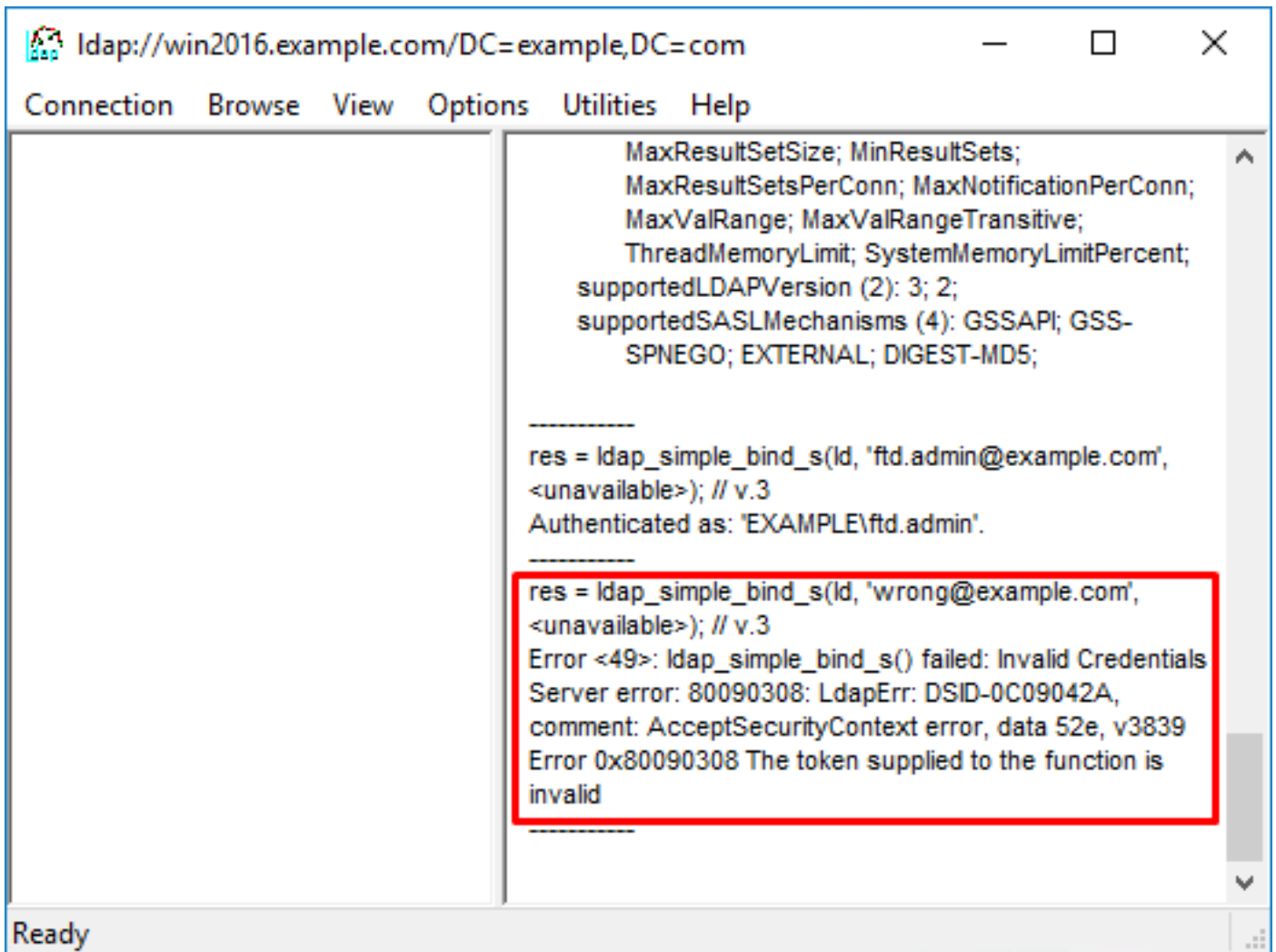
5.选择Simple Bind , 然后指定Directory Account Username和Password。Click OK.



如果绑定成功，则ldp显示身份验证为:DOMAINusername



尝试使用无效的用户名或密码进行绑定会导致失败，例如此处看到的两个。

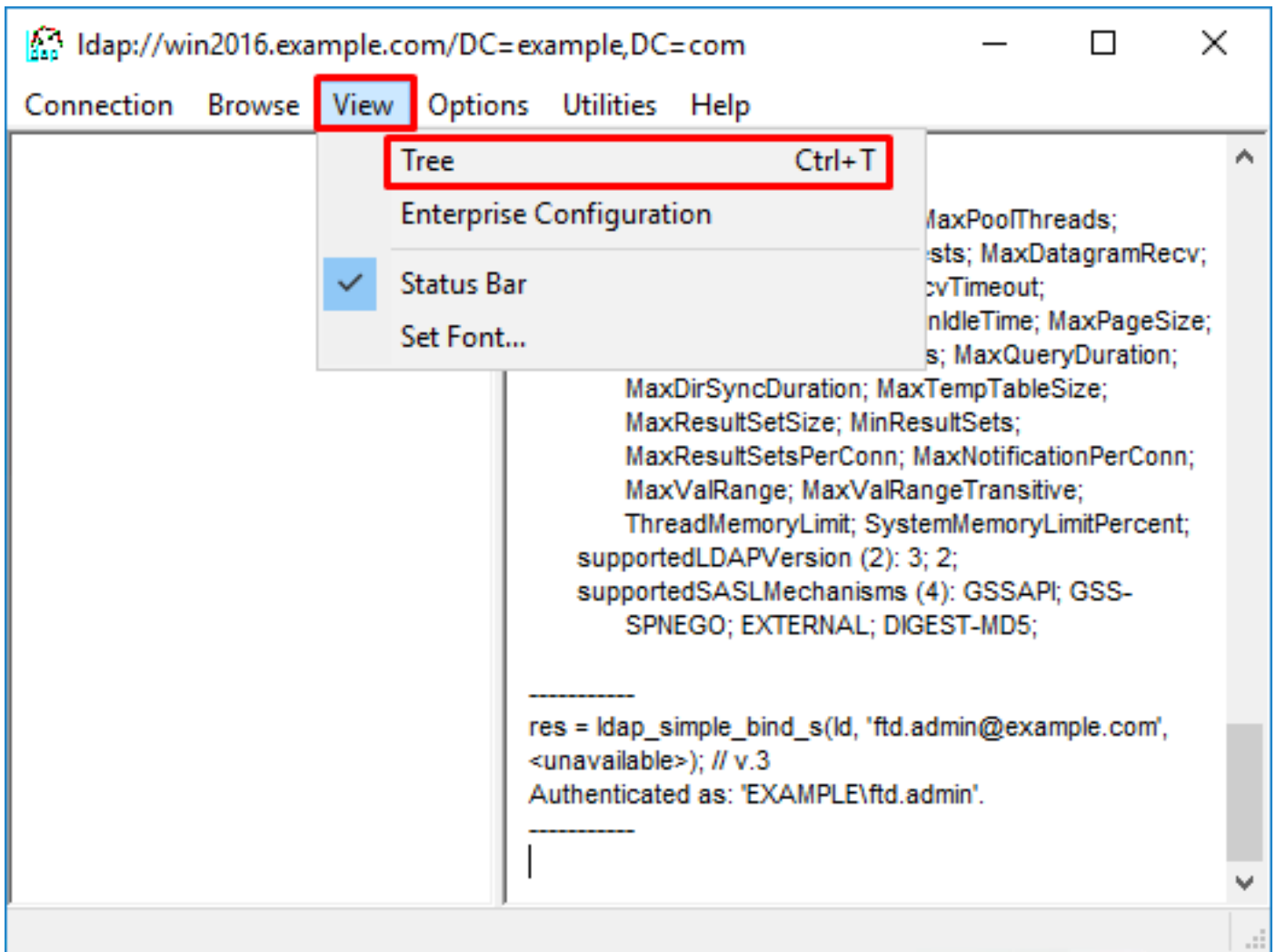


LDAP服务器找不到用户名

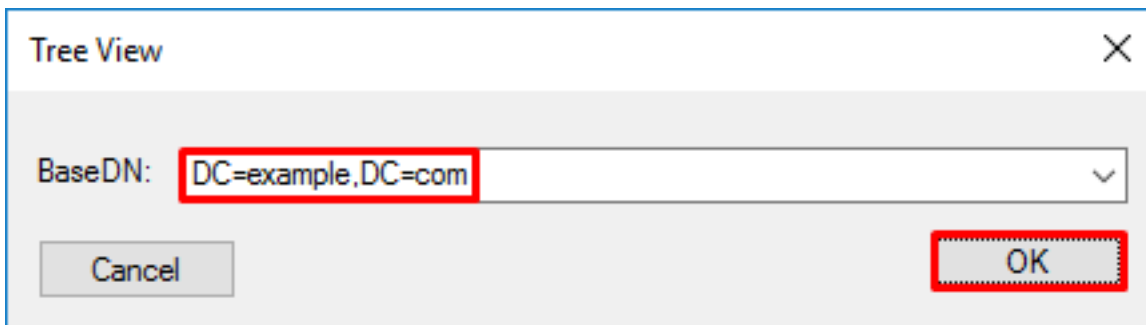
```
[ -2147483612] Session Start
[ -2147483612] New request Session, context 0x00007f9e65ccdc40, reqType = Authentication
[ -2147483612] Fiber started
[ -2147483612] Creating LDAP context with uri=ldap://192.168.1.1:389
[ -2147483612] Connect to LDAP server: ldap://192.168.1.1:389, status = Successful
[ -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可以通过FTD完成的搜索找到用户。这也可通过Ldp.exe完成。

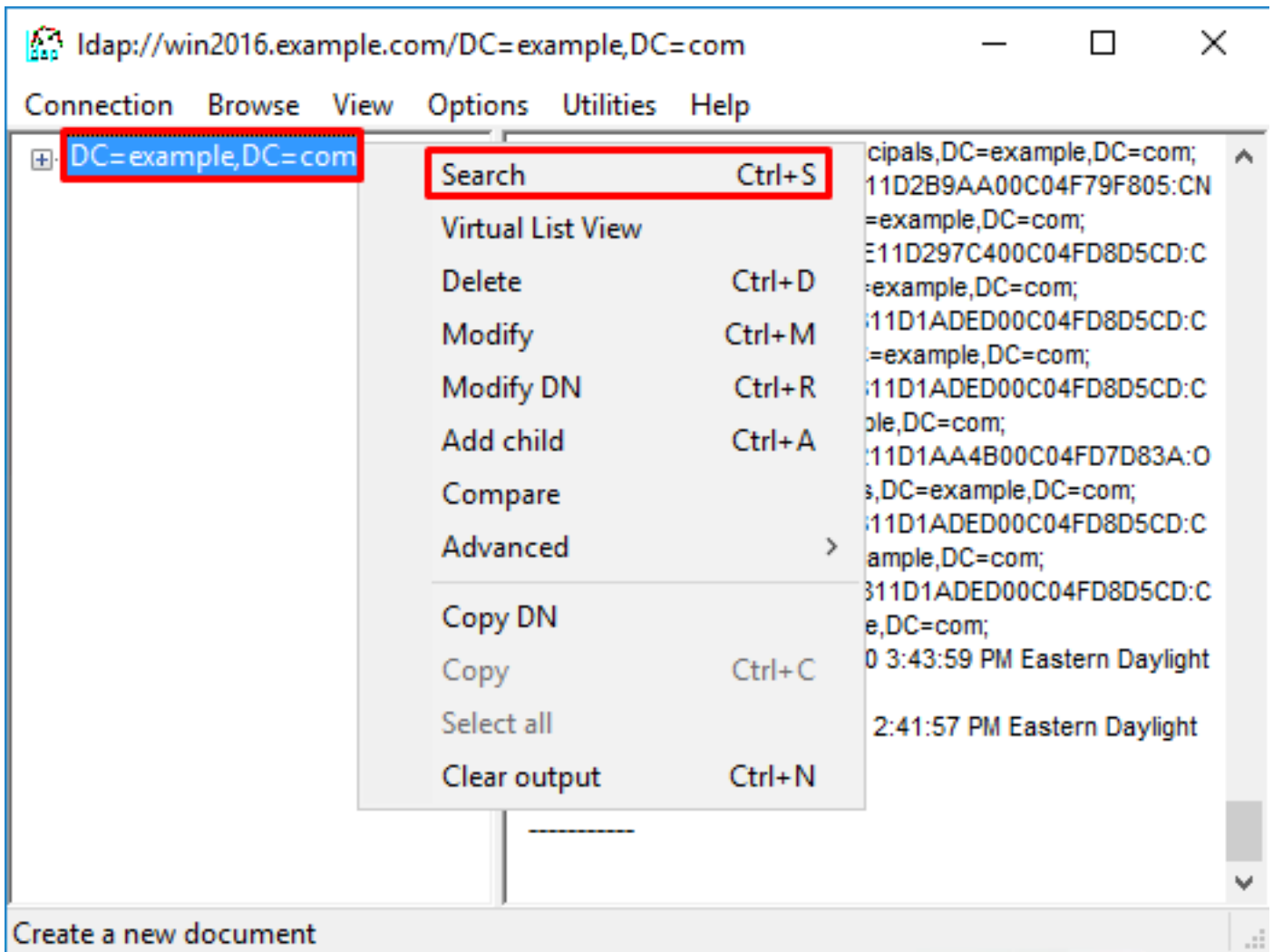
1.成功绑定后（如上所示），导航到视图>树。



2.指定在FTD上配置的基本DN，然后点击**确定**



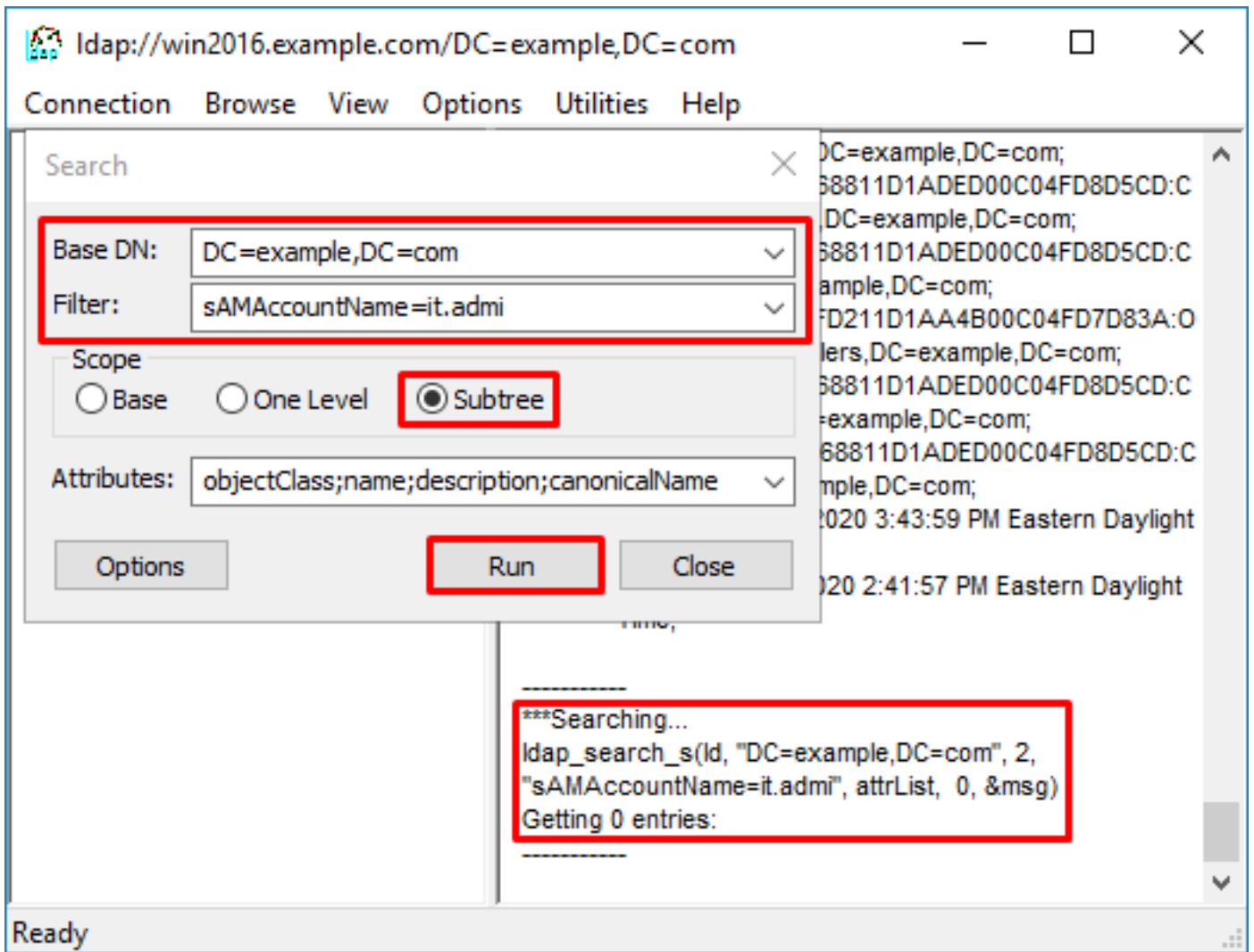
3.右键单击基础DN，然后单击**Search**。



4. 指定与调试中看到的相同Base DB、Filter和Scope值。

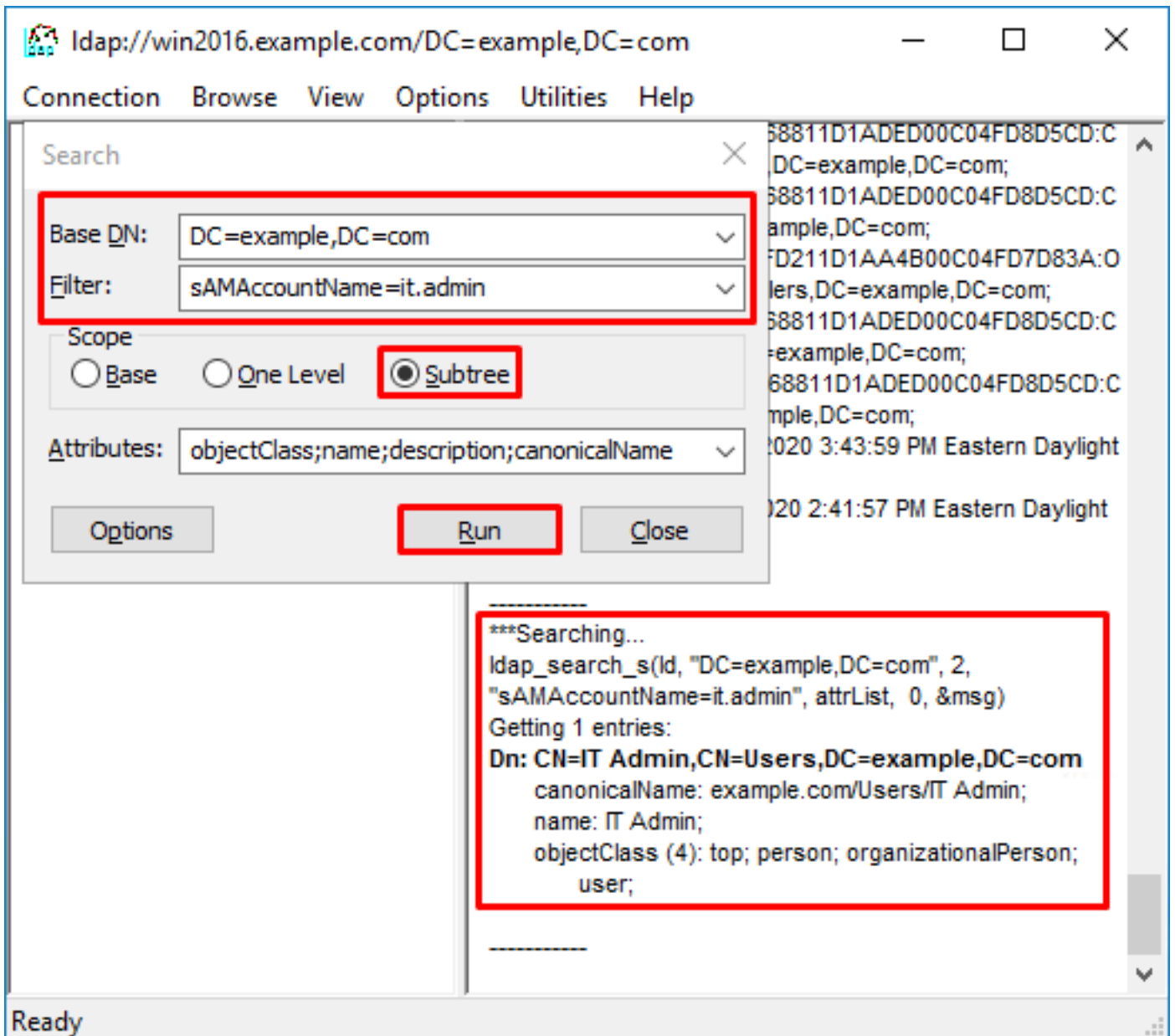
在本例中，包括：

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



ldap发现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

使用正确的samaccountname **it.admin**进行的另一次尝试显示不同的结果。ldap在Base DN dc=example，dc=com下找到1个条目，并打印该用户DN。



用户名密码不正确

```

[-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：验证用户密码配置正确且未过期。与登录DN类似，FTD使用用户凭证对AD执行绑定。

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中的步骤在绑定登录DN和/或密码不正确部分中显示。

此外，还可以查看Microsoft服务器事件查看器日志的潜在原因。

测试AAA

test aaa-server命令可用于使用特定用户名和密码模拟从FTD进行的身份验证尝试。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与AD服务器的可达性。如果LDAP数据包离开FTD，但没有响应，这可能表明存在路由问题。

捕获显示双向LDAP流量。

```
> 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

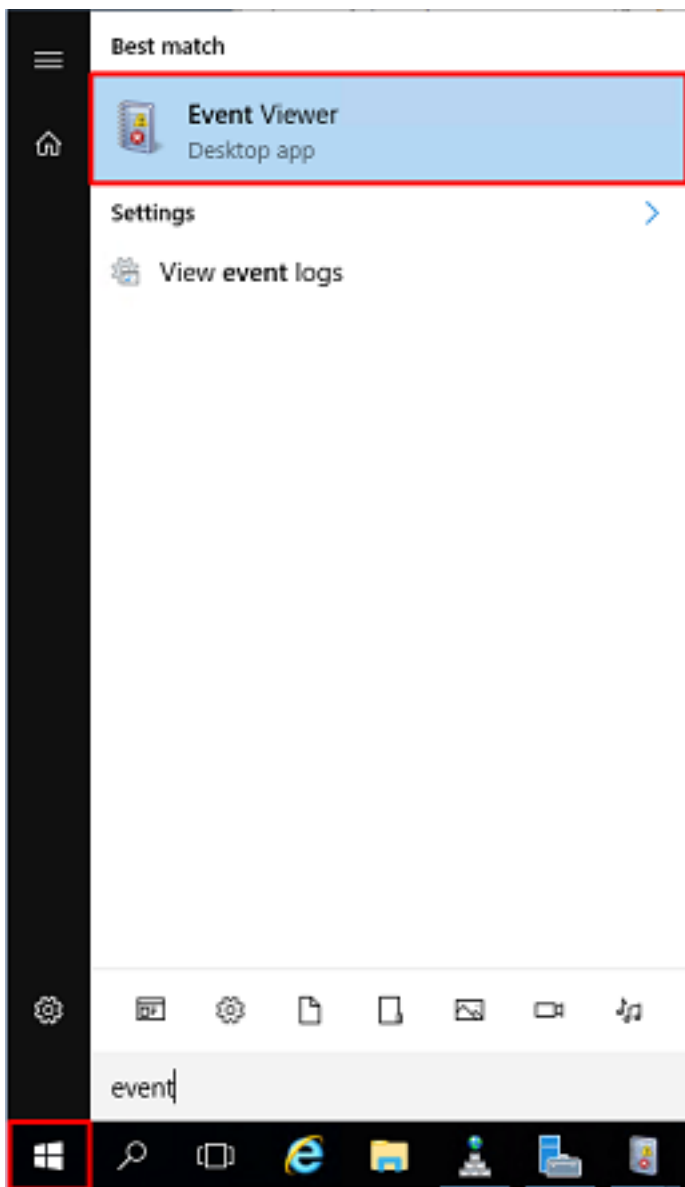
  1: 23:02:16.770712      192.168.1.17.61960 > 192.168.1.1.389: S 3681912834:3681912834(0) win
32768 <mss 1460,nop,nop,timestamp 1061373057 0>
  2: 23:02:16.772009      192.168.1.1.389 > 192.168.1.17.61960: S 491521506:491521506(0) ack
3681912835 win 8192 <mss 1460,nop,nop,timestamp 762393884 1061373057>
  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
```

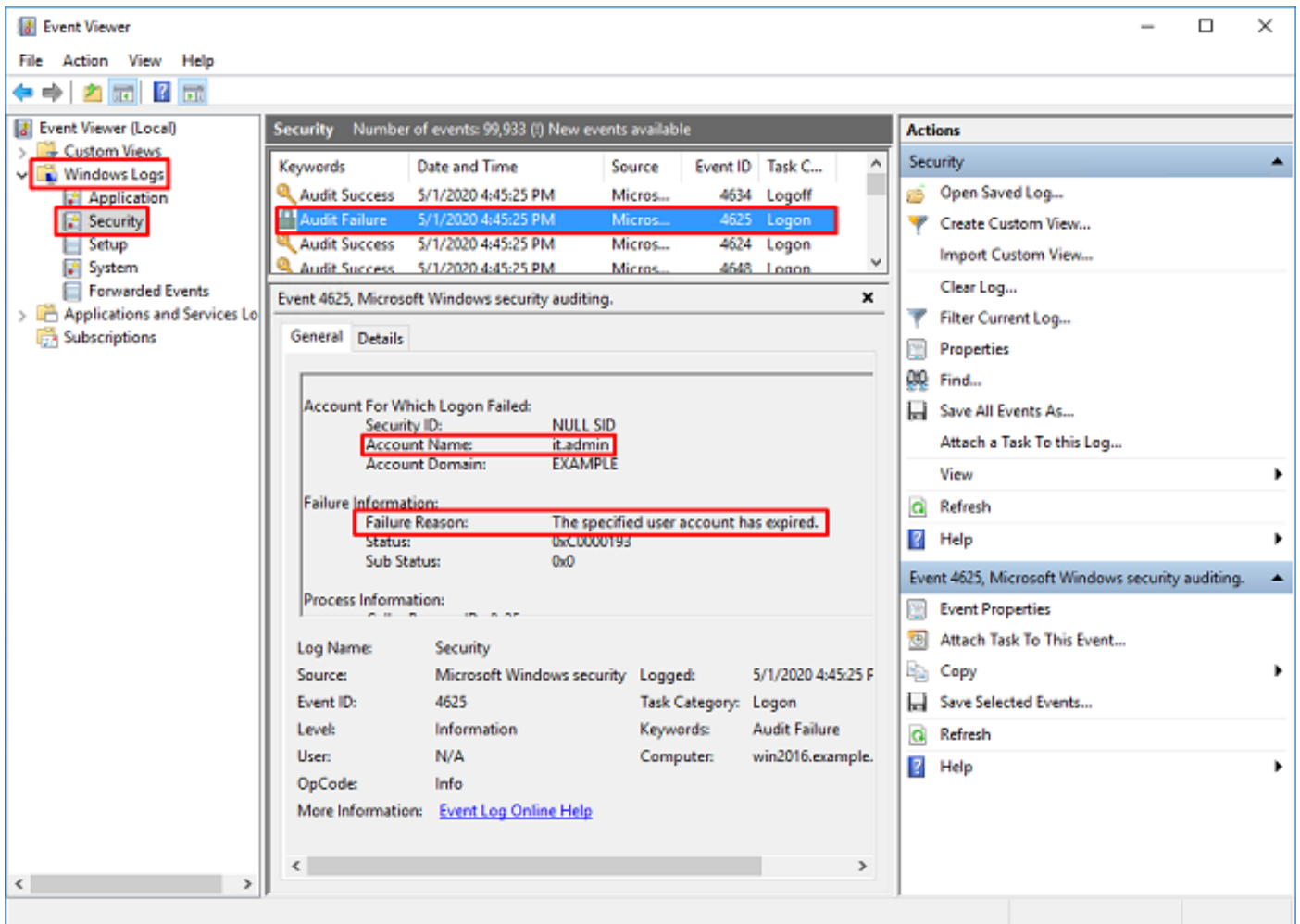
Windows Server事件查看器日志

AD服务器上的Event Viewer日志可以提供有关失败原因的更详细信息。

1.搜索并打开“事件查看器”。



2. 展开Windows Logs，然后单击Security。使用用户帐户名称搜索Audit Failures，然后查看失败信息。



An account failed to log on.

Subject:

Security ID:SYSTEM
Account Name:WIN2016\$\nAccount 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

关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。