

在透過 FMC 管理的 FTD 上，針對 AnyConnect 用戶端設定 AD (LDAP) 驗證和使用者身分識別

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[背景資訊](#)

[設定](#)

[網路圖表和案例](#)

[Active Directory配置](#)

[確定LDAP基本DN和組DN](#)

[建立FTD帳戶](#)

[建立AD組並將使用者新增到AD組 \(可選\)](#)

[複製LDAPS SSL證書根 \(僅對於LDAPS或STARTTLS是必需的\)](#)

[FMC配置](#)

[驗證許可](#)

[設定領域](#)

[配置AnyConnect進行AD身份驗證](#)

[啟用身份策略並為使用者身份配置安全策略](#)

[配置NAT免除](#)

[部署](#)

[驗證](#)

[最終配置](#)

[AAA組態](#)

[AnyConnect配置](#)

[使用AnyConnect連線並驗證訪問控制策略規則](#)

[使用FMC連線事件進行驗證](#)

[疑難排解](#)

[調試](#)

[正在運行的LDAP調試](#)

[無法與LDAP伺服器建立連線](#)

[繫結登入DN和/或密碼不正確](#)

[LDAP伺服器找不到使用者名稱](#)

[使用者名稱密碼不正確](#)

[測試AAA](#)

[封包擷取](#)

[Windows Server事件檢視器日誌](#)

簡介

本檔案介紹如何為連線至Cisco Firepower威脅防禦(FTD)的AnyConnect使用者端設定AD驗證。

必要條件

需求

思科建議您瞭解以下主題：

- FMC上的RA VPN配置基礎知識
- FMC上的LDAP伺服器配置基礎知識
- Active Directory(AD)基礎知識

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- Microsoft 2016伺服器
- 運行6.5.0的FMCv
- 執行6.5.0的FTDv

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

背景資訊

本檔案介紹如何為連線到Cisco Firepower威脅防禦(FTD)(由Firepower管理中心(FMC)管理)的AnyConnect使用者端設定Active Directory(AD)驗證。

使用者身份用於訪問策略中，以將AnyConnect使用者限制為特定IP地址和埠。

設定

網路圖表和案例



Windows伺服器預配置了IIS和RDP以測試使用者身份。在此配置指南中，建立了三個使用者帳戶和兩個組。

使用者帳戶：

- FTD管理員：它用作目錄帳戶，以允許FTD繫結到Active Directory伺服器。
- IT管理員：用於演示使用者身份的測試管理員帳戶。
- 測試使用者：用於演示使用者身份的測試使用者帳戶。

組：

- AnyConnect管理員：新增IT管理員以演示使用者身份的測試組。此組僅具有對Windows Server的RDP訪問許可權。
- AnyConnect使用者：新增測試使用者以演示使用者身份的測試組。此組僅具有對Windows Server的HTTP訪問許可權。

Active Directory配置

若要在FTD上正確設定AD驗證和使用者身分，需要幾個值。

在FMC上完成配置之前，必須在Microsoft伺服器上建立或收集所有這些詳細資訊。主要值包括：

- **域名：**

這是伺服器的域名。在此配置指南中，example.com是域名。

- **伺服器IP/FQDN地址：**

用於訪問Microsoft伺服器的IP地址或FQDN。如果使用FQDN，則必須在FMC和FTD中配置DNS伺服器以解析FQDN。

在本配置指南中，此值為win2016.example.com（解析為192.168.1.1）。

- **伺服器端口：**

LDAP服務使用的埠。預設情況下，LDAP和STARTTLS將TCP埠389用於LDAP，而LDAP over SSL(LDAPS)使用TCP埠636。

- **根CA：**

如果使用LDAPS或STARTTLS，則需要使用根CA來對LDAPS使用的SSL證書進行簽名。

- **目錄使用者名稱和密碼：**

這是FMC和FTD用於繫結到LDAP伺服器、對使用者進行身份驗證以及搜尋使用者和組的帳戶。

為此建立了一個名為FTD Admin的帳戶。

- **基本和群組可分辨名稱(DN)：**

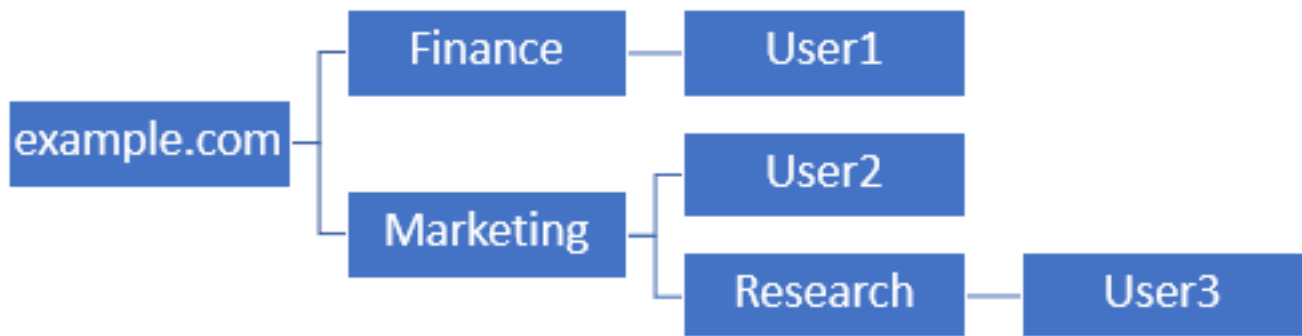
基礎DN是FMC的起點，FTD會告知Active Directory開始搜尋和驗證使用者。

同樣，組DN是起點，FMC會告知Active Directory從何處開始搜尋使用者身份組。

在本配置指南中，根域example.com用作基礎DN和組DN。

但是，對於生產環境，在LDAP層次結構中進一步使用Base DN和Group DN會更好。

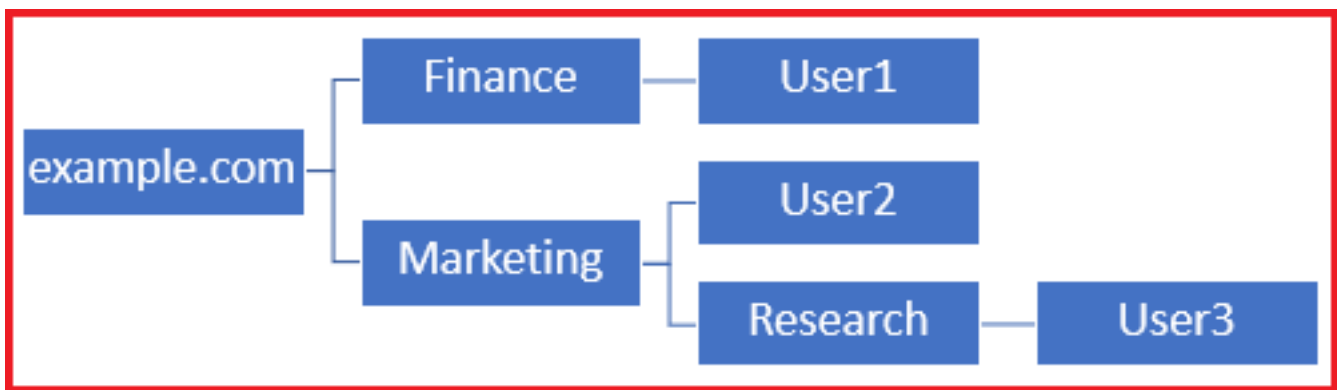
例如，此LDAP層次結構：



如果管理員希望Marketing組織單位中的使用者能夠驗證基本DN，可以將基本DN設定為根 (example.com)。

但是，這也允許Finance組織單位下的User1登入，因為使用者搜尋從根使用者開始，然後轉到Finance、Marketing和Research。

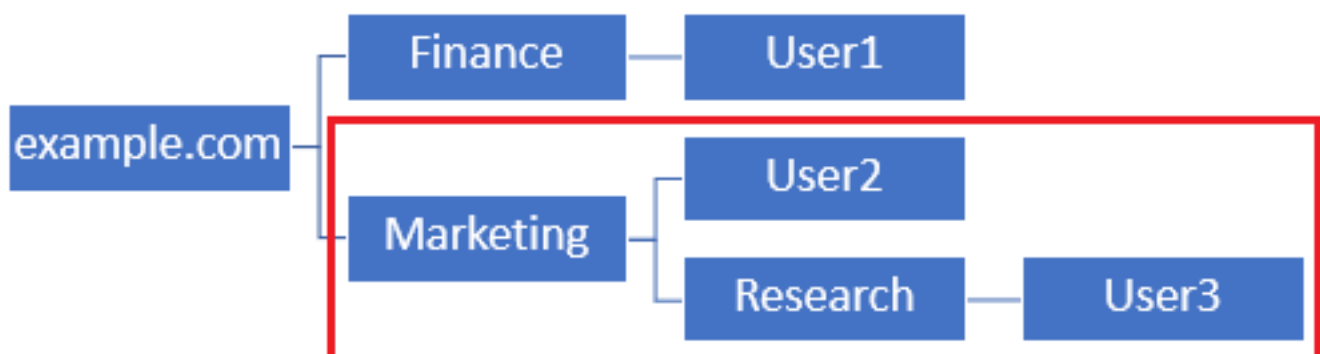
基本DN設定為example.com



為了將登入限制為Marketing組織單位及以下單位中的唯一使用者，管理員可以將Base DN設定為Marketing。

現在只有User2和User3能夠進行身份驗證，因為搜尋從Marketing開始。

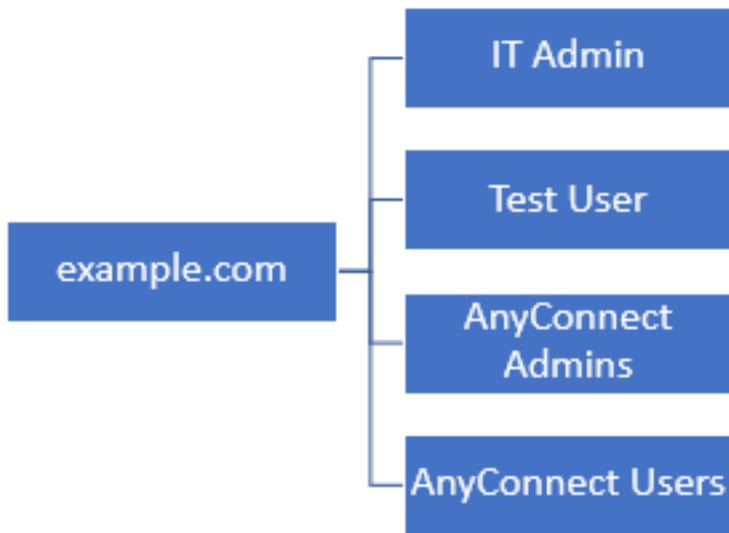
基本DN設定為Marketing



請注意，為了在FTD內進行更精細的控制（允許使用者連線或根據使用者的AD屬性為其分配不同的授權），需要配置LDAP授權對映。

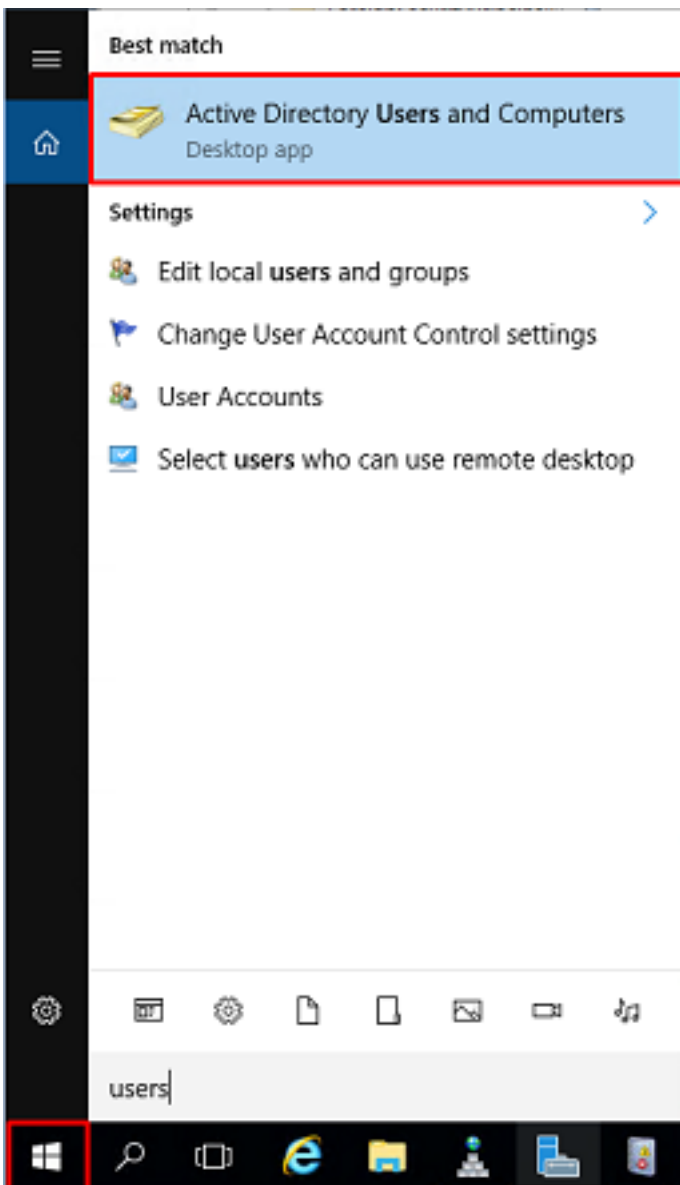
有關此操作的詳細資訊，請參閱：[在Firepower威脅防禦\(FTD\)上配置AnyConnect LDAP對映](#)。

此簡化的LDAP層次結構用於此配置指南，根example.com的DN用於基礎DN和組DN。

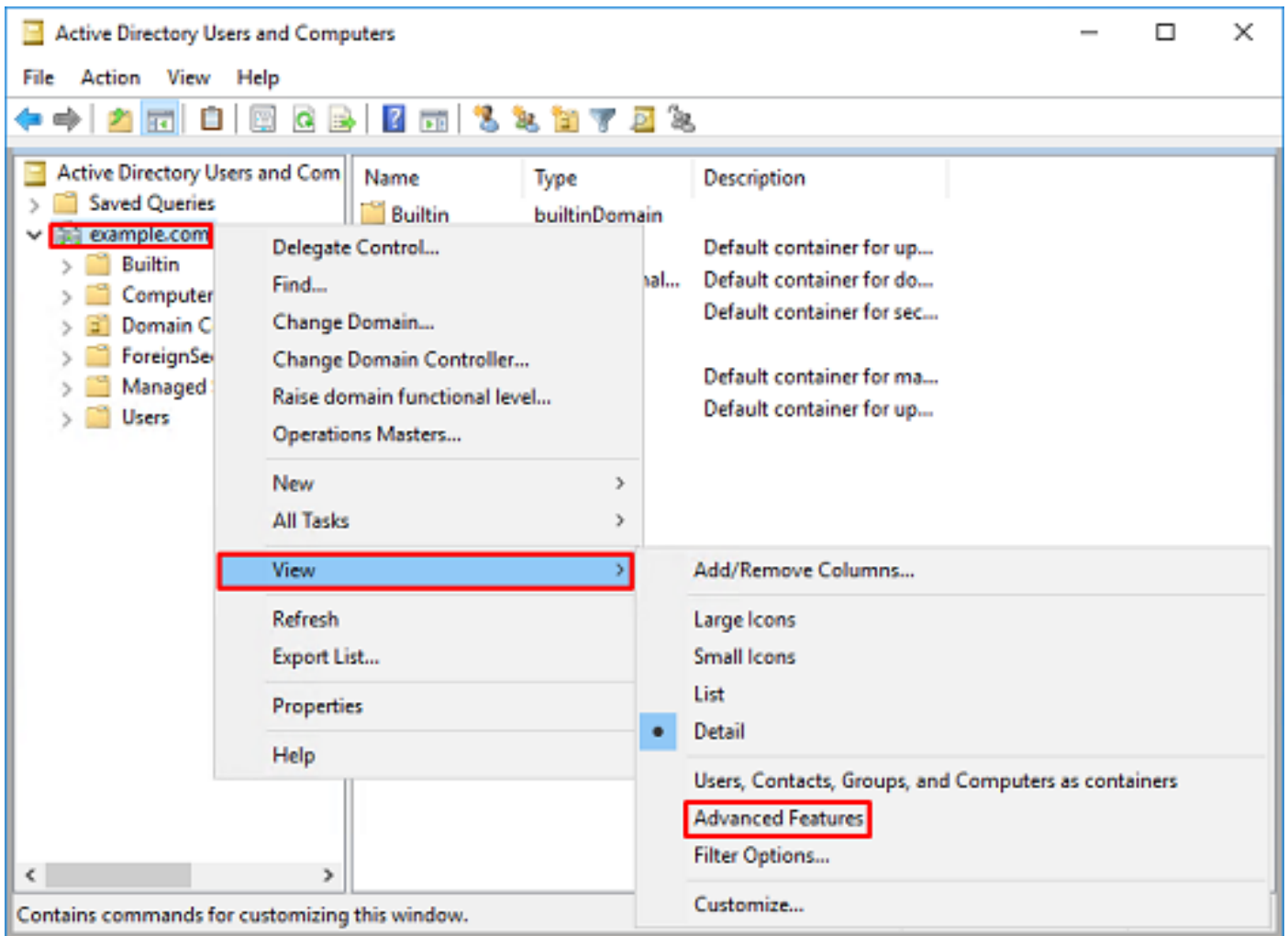


確定LDAP基本DN和組DN

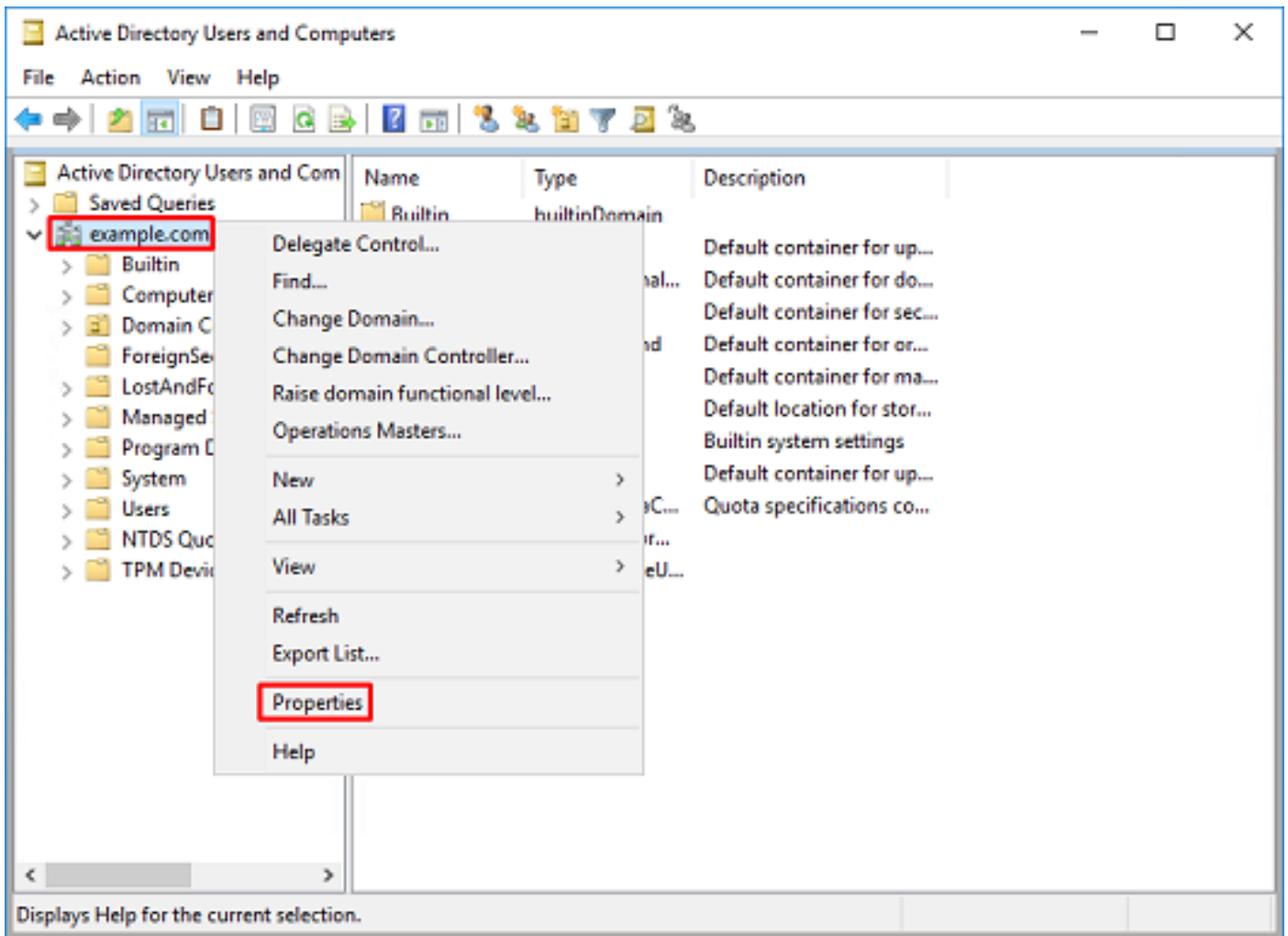
1. 開啟Active Directory使用者和電腦。



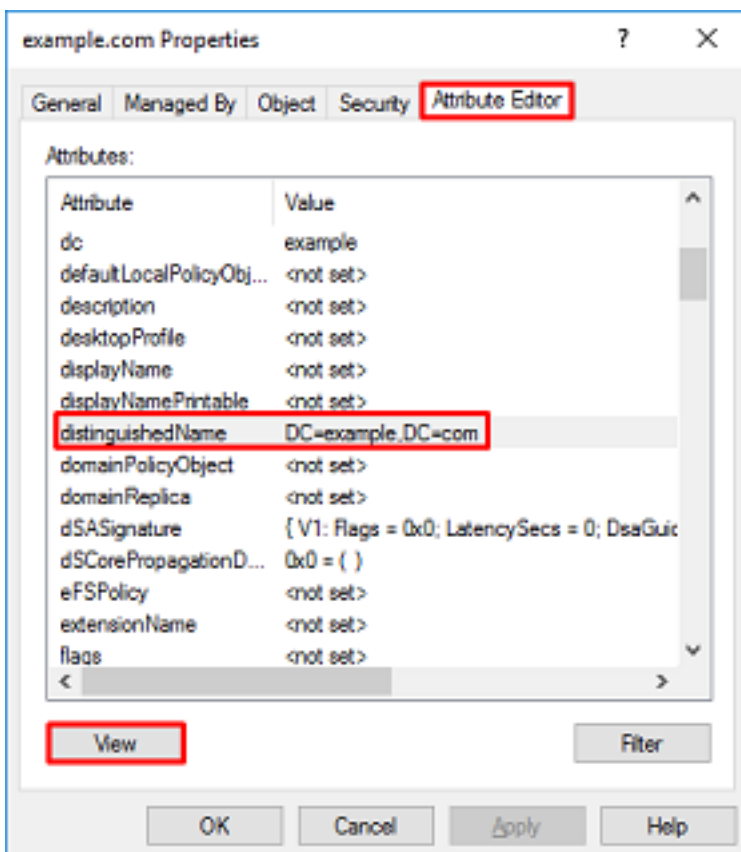
2. 左鍵按一下根域（開啟容器），按一下右鍵根域，然後在View下按一下Advanced Features。



3.這將啟用AD對象下其他屬性的檢視。例如，要查詢根example.com的DN，請按一下右鍵example.com，然後選擇**Properties**。



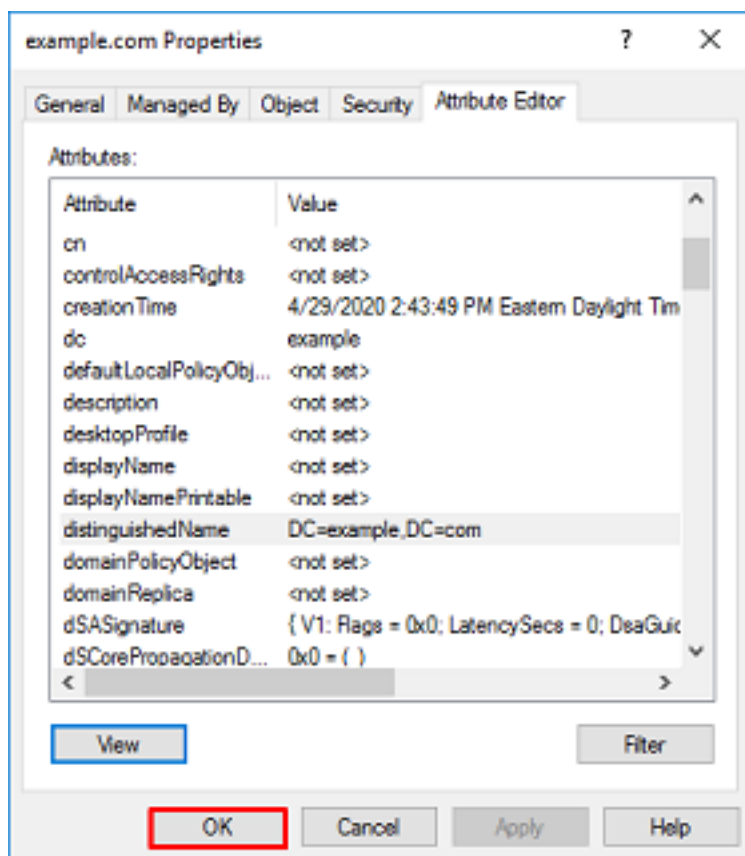
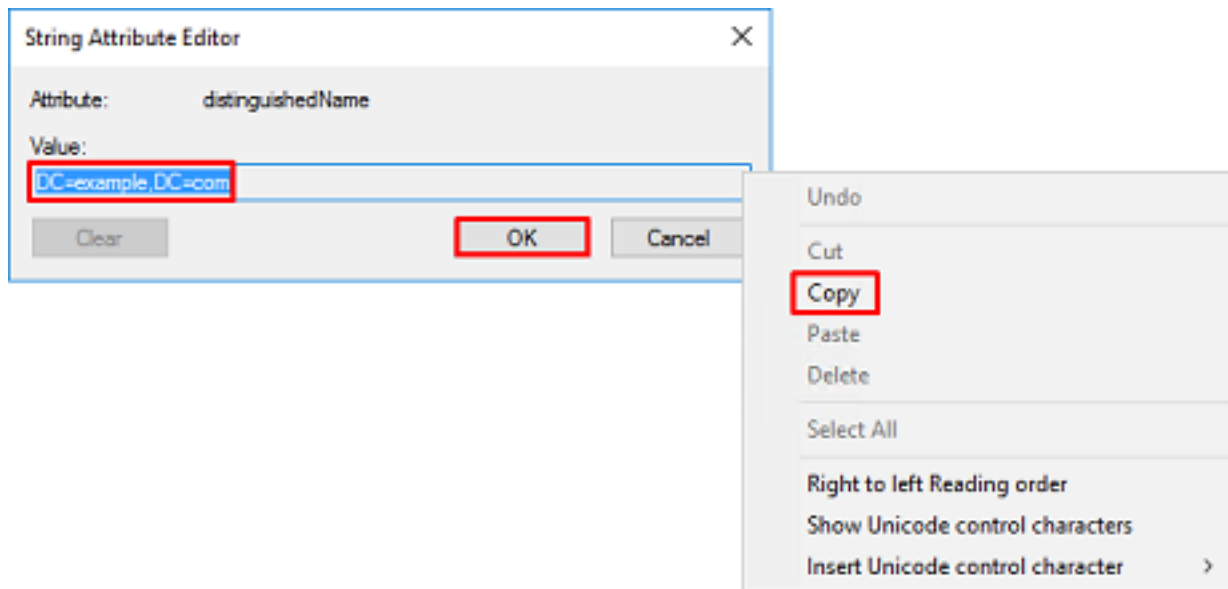
4. 在屬性下，選擇屬性編輯器頁籤。在Attributes下查詢distinguishedName，然後按一下View。



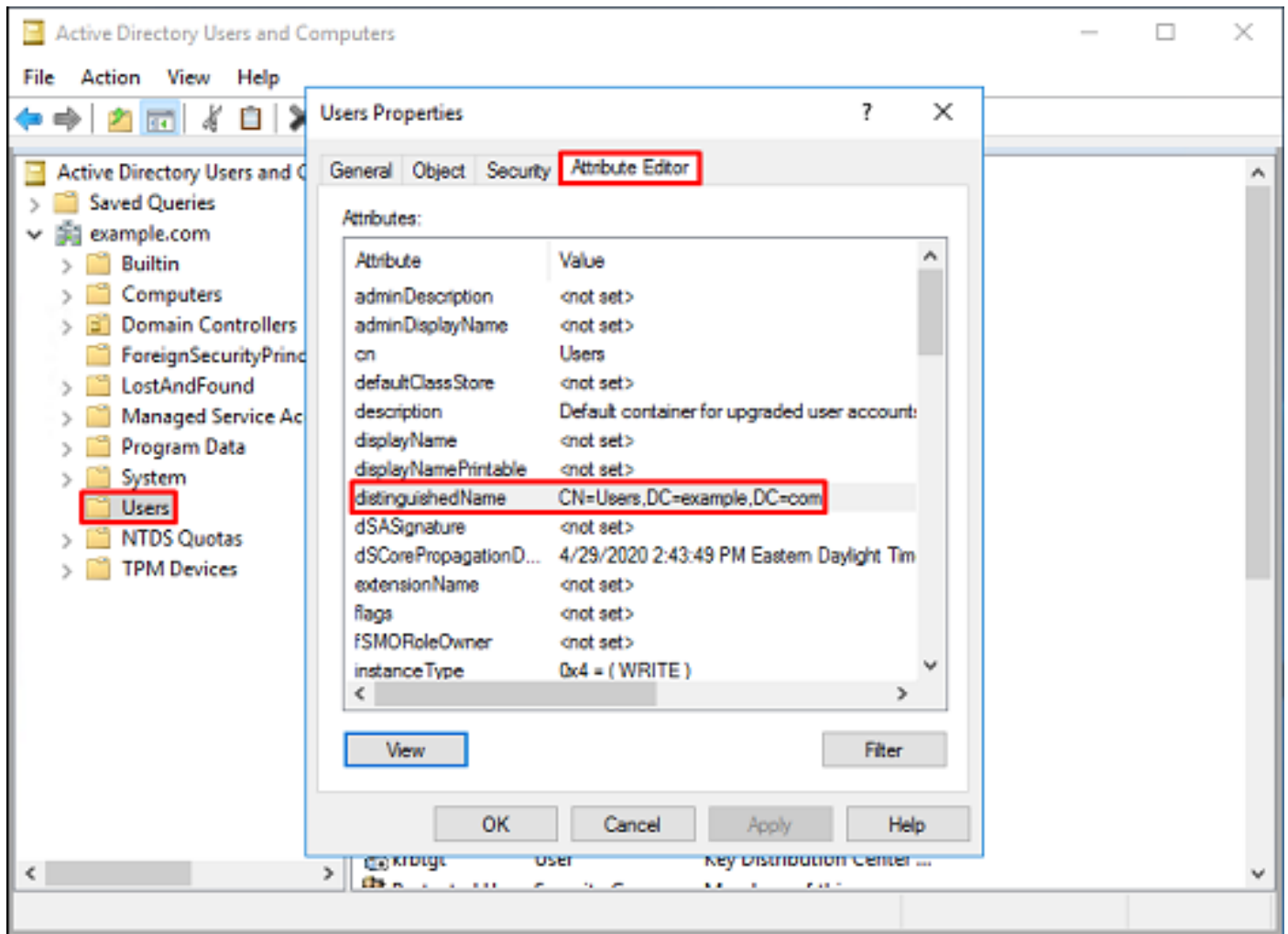
5. 這將開啟一個新視窗，以後可以在其中複製並貼上到FMC中。在本示例中，根DN是

DC=example , DC=com。

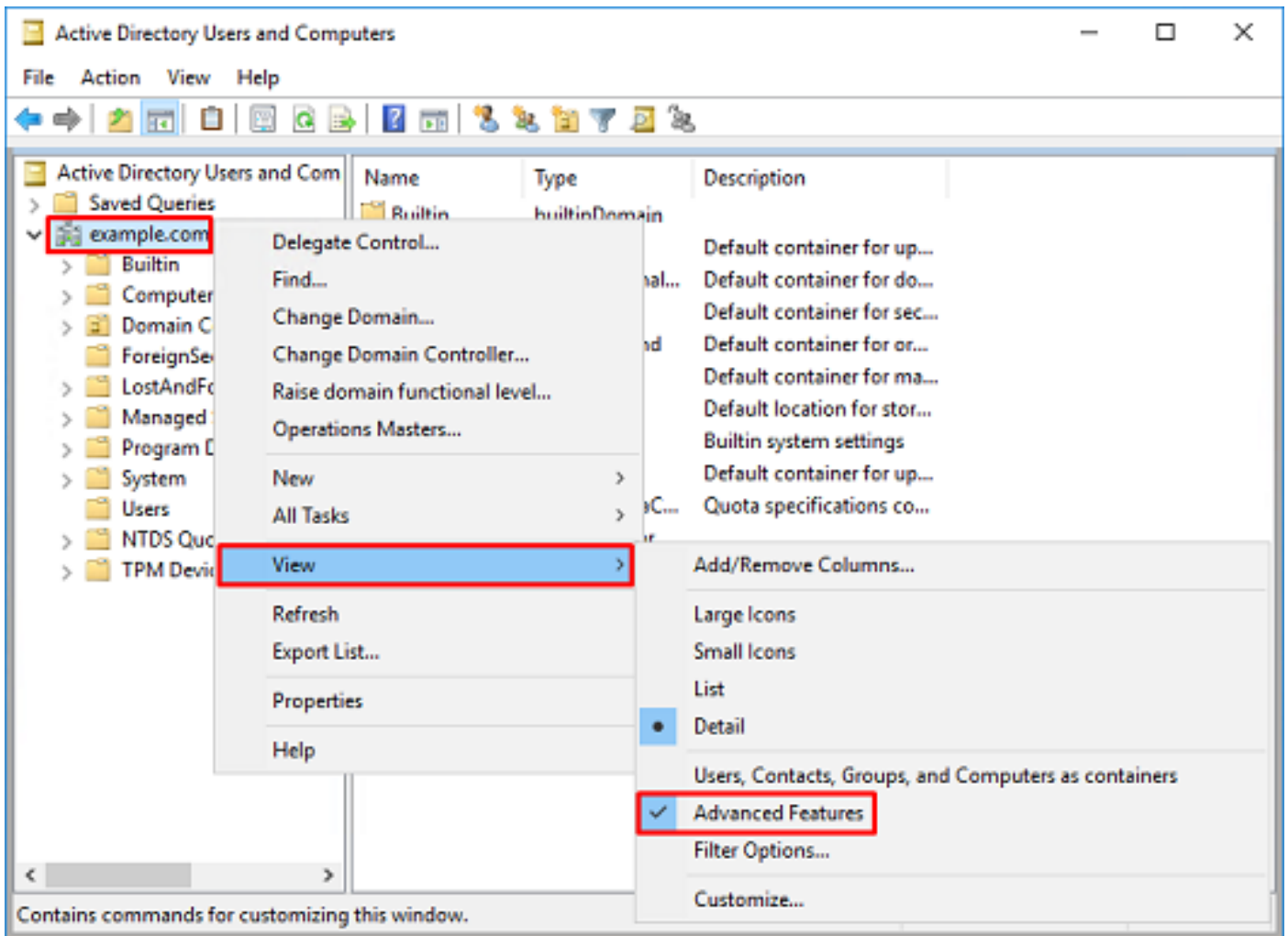
複製值儲存以備以後使用。按一下OK以退出「String Attribute Editor」視窗，然後再次按一下「OK」以退出「Properties」。



這可以對Active Directory中的多個對象執行此操作。例如，以下步驟用於查詢User container的DN:



6.再次按一下右鍵根DN，然後在View下再次按一下Advanced Features，可以刪除Advanced Features檢視。



建立FTD帳戶

此使用者帳戶允許FMC和FTD與Active Directory繫結，以搜尋使用者和組並對使用者進行身份驗證。

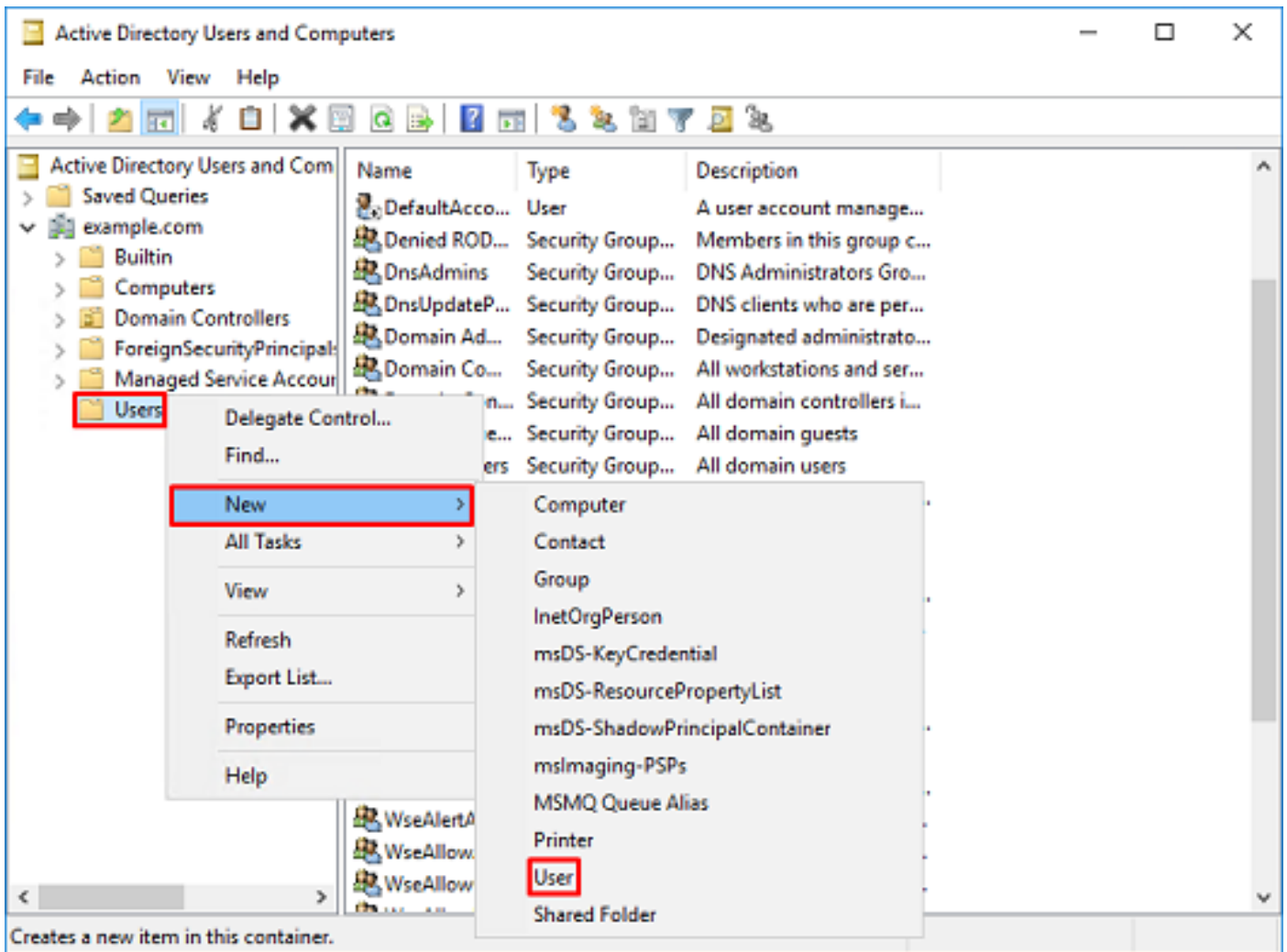
建立單獨的FTD帳戶的目的是，在用於繫結的憑證遭到破壞時，防止網路中其他地方的未經授權存取。

此帳戶無需在基本DN或組DN範圍內。

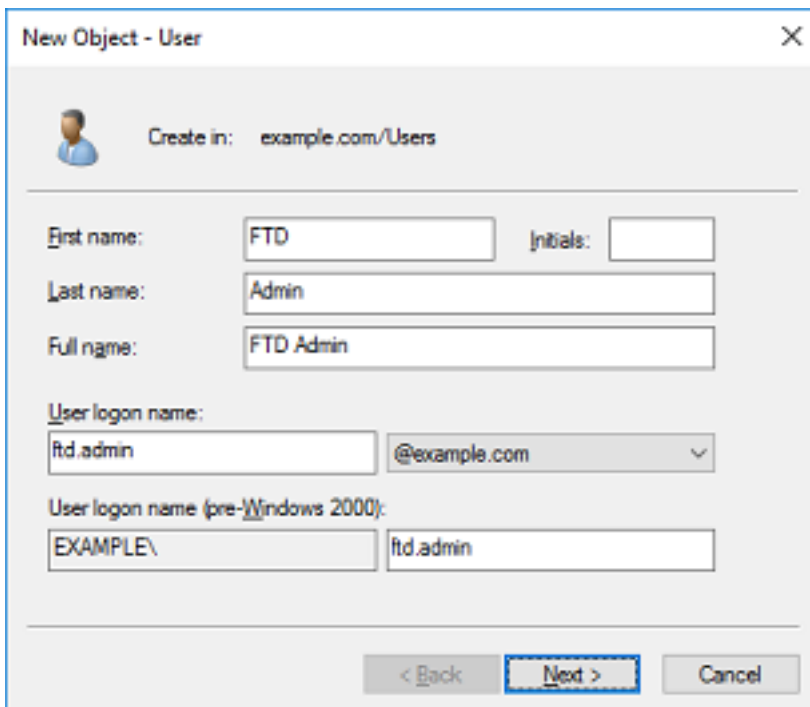
1. 在Active Directory使用者和電腦中，按一下右鍵FTD帳戶新增到的容器/組織。

在此組態中，FTD帳戶會新增到使用者名稱ftd.admin@example.com下Users容器下方。

按一下右鍵Users，然後導航到New > User。



2.完成「新建對象 — 使用者」嚮導。



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:

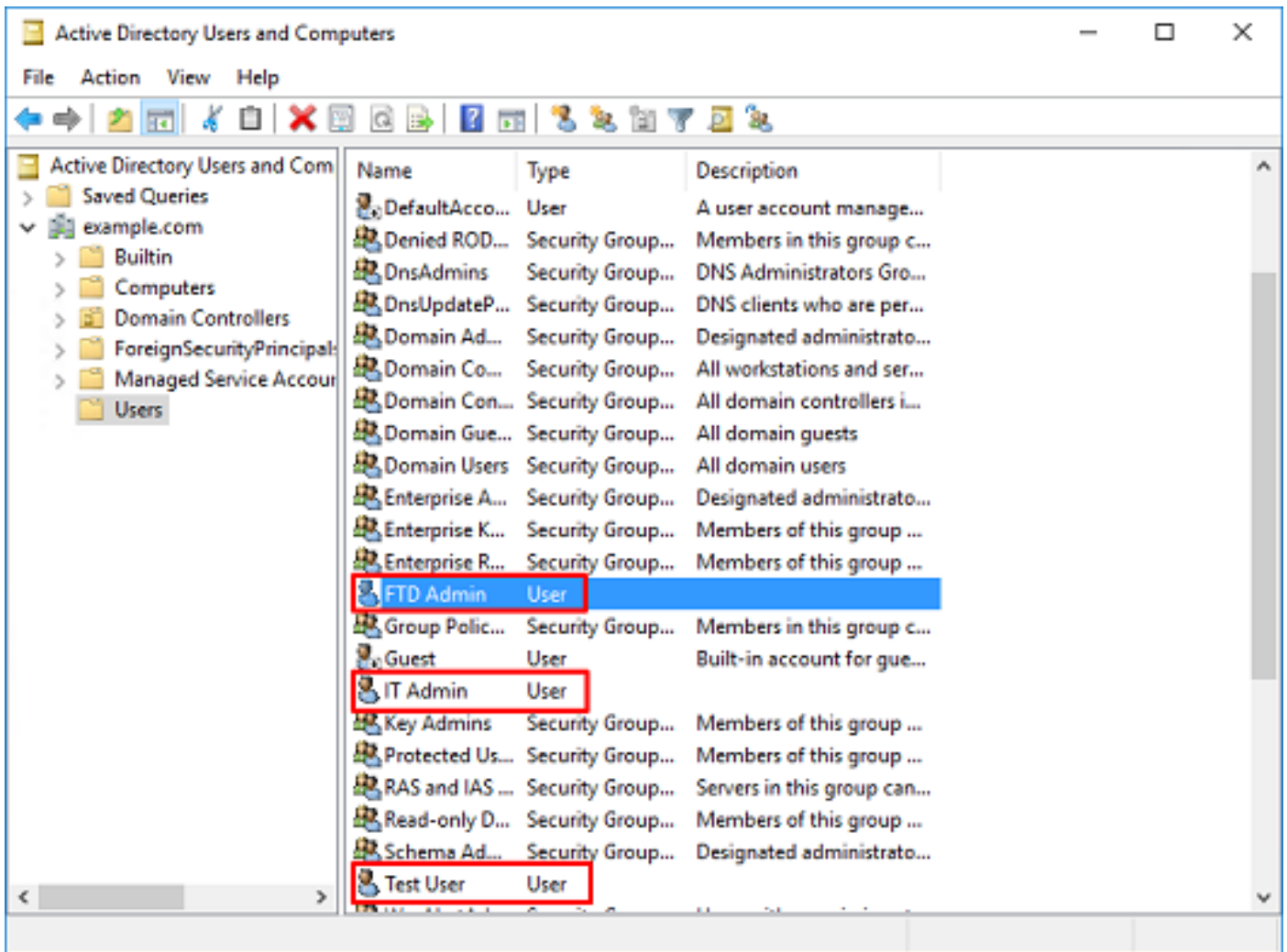
Full name: FTD Admin

User logon name: ftd.admin@example.com

The password never expires.

< Back Finish Cancel

3. 驗證是否已建立FTD帳戶。另外建立了兩個帳戶：IT管理員和測試用戶。



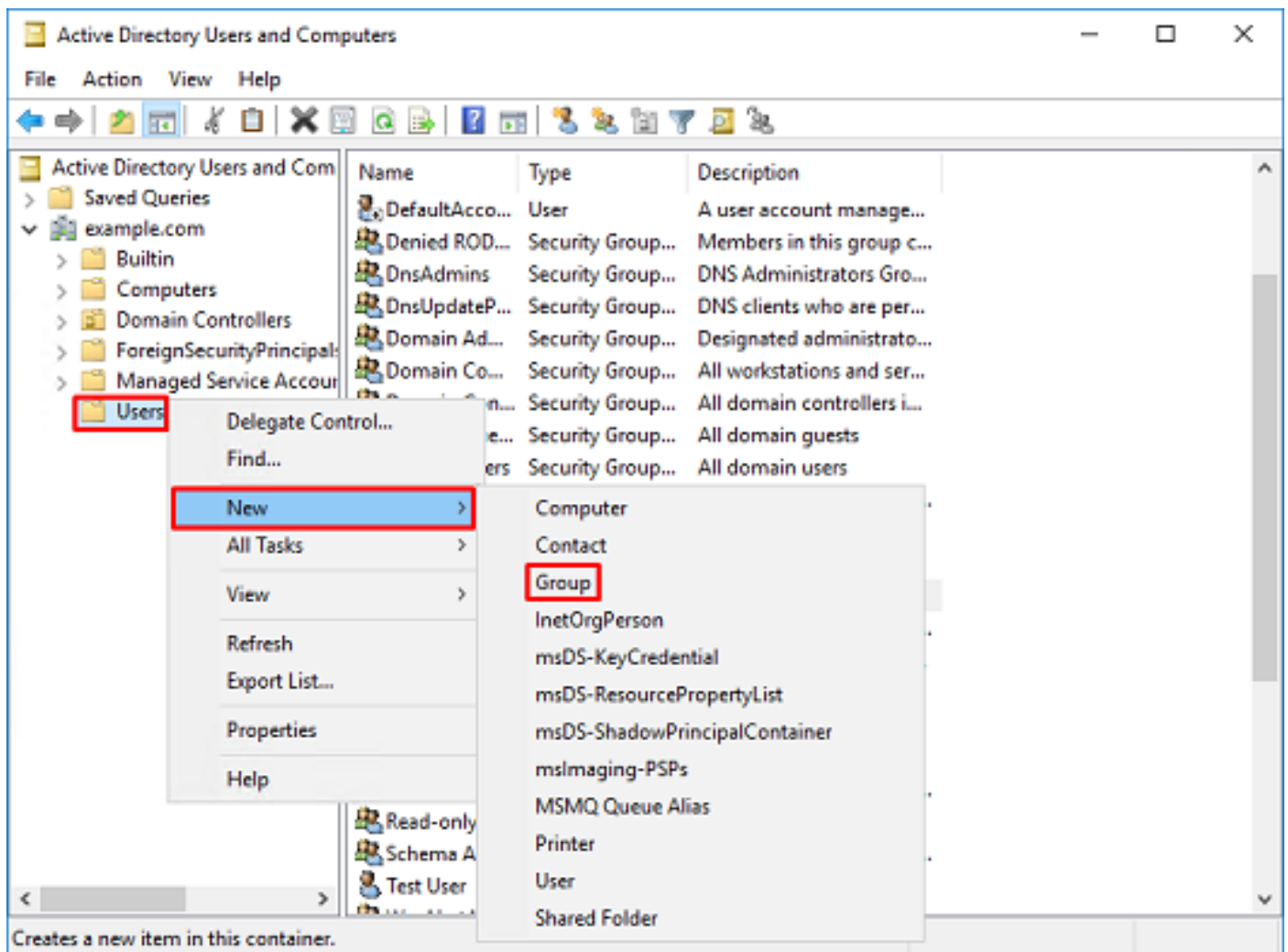
建立AD組並將使用者新增到AD組 (可選)

雖然身份驗證不需要使用組，但可以使用組來簡化將訪問策略應用至多個使用者以及LDAP授權的過程。

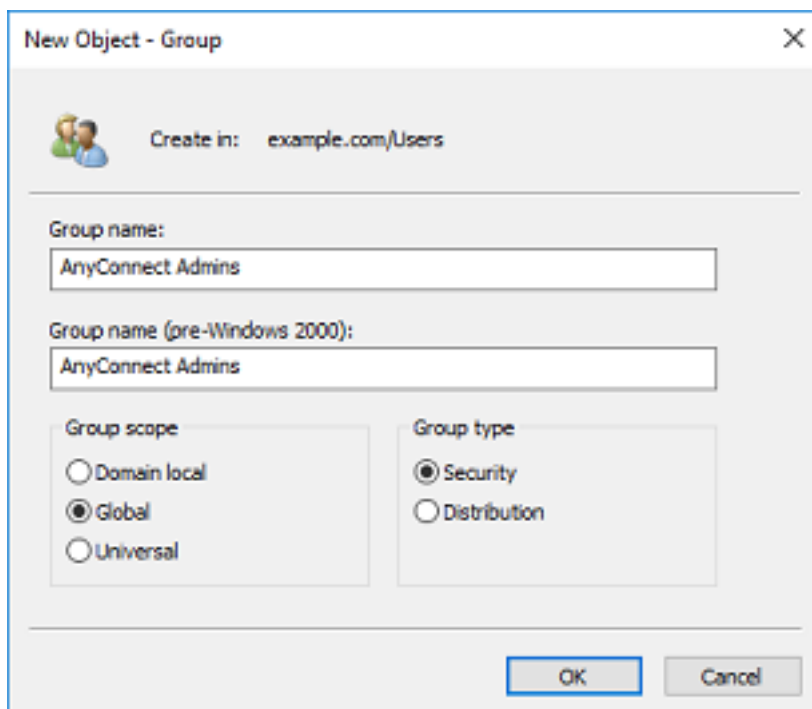
在此配置指南中，組用於稍後通過FMC中的使用者標識應用訪問控制策略設定。

1.在Active Directory使用者和電腦中，按一下右鍵新組新增到其中的容器或組織單元。

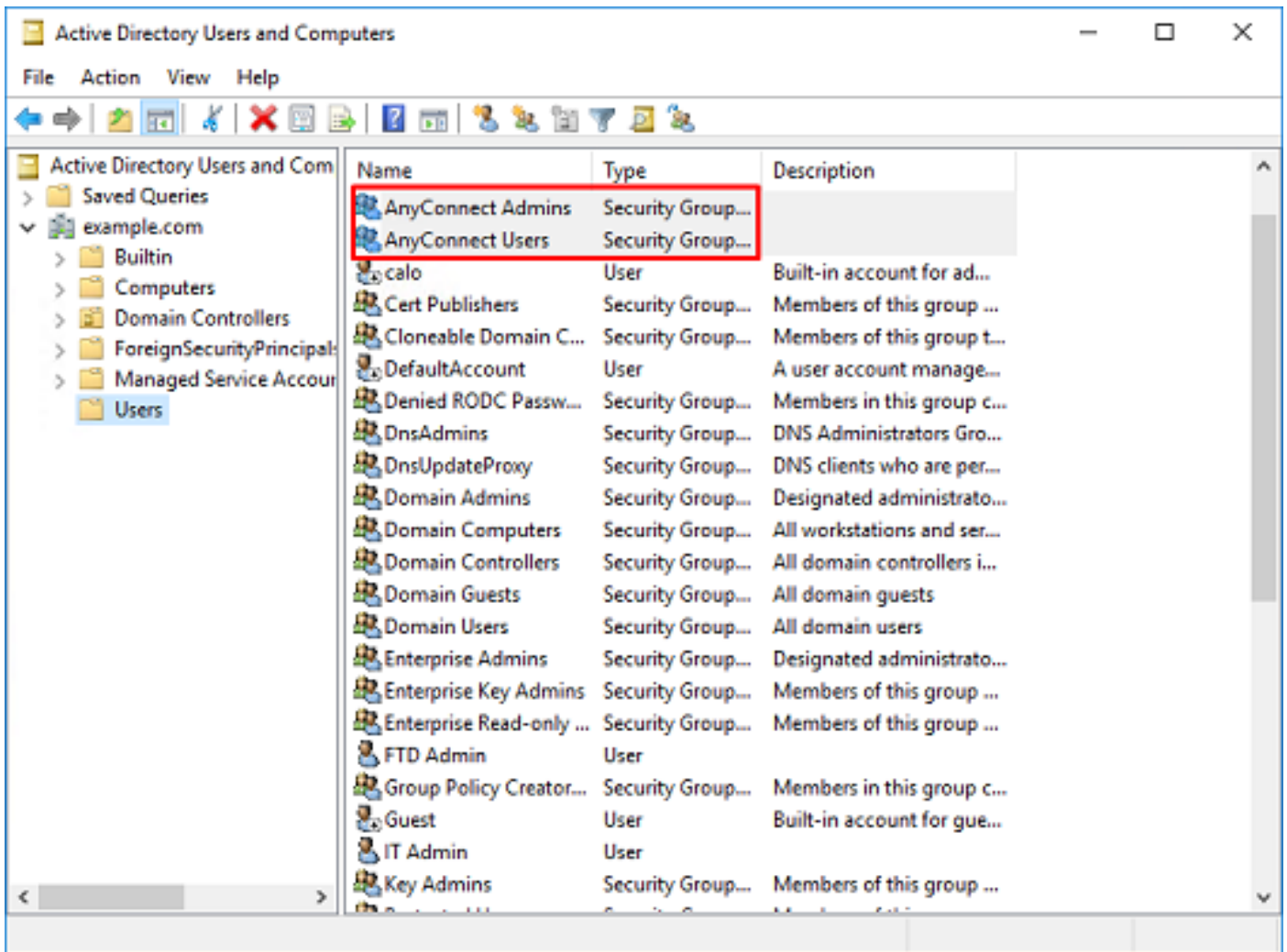
在本示例中，組AnyConnect Admins被新增到Users容器下。按一下右鍵Users，然後導航到New > Group。



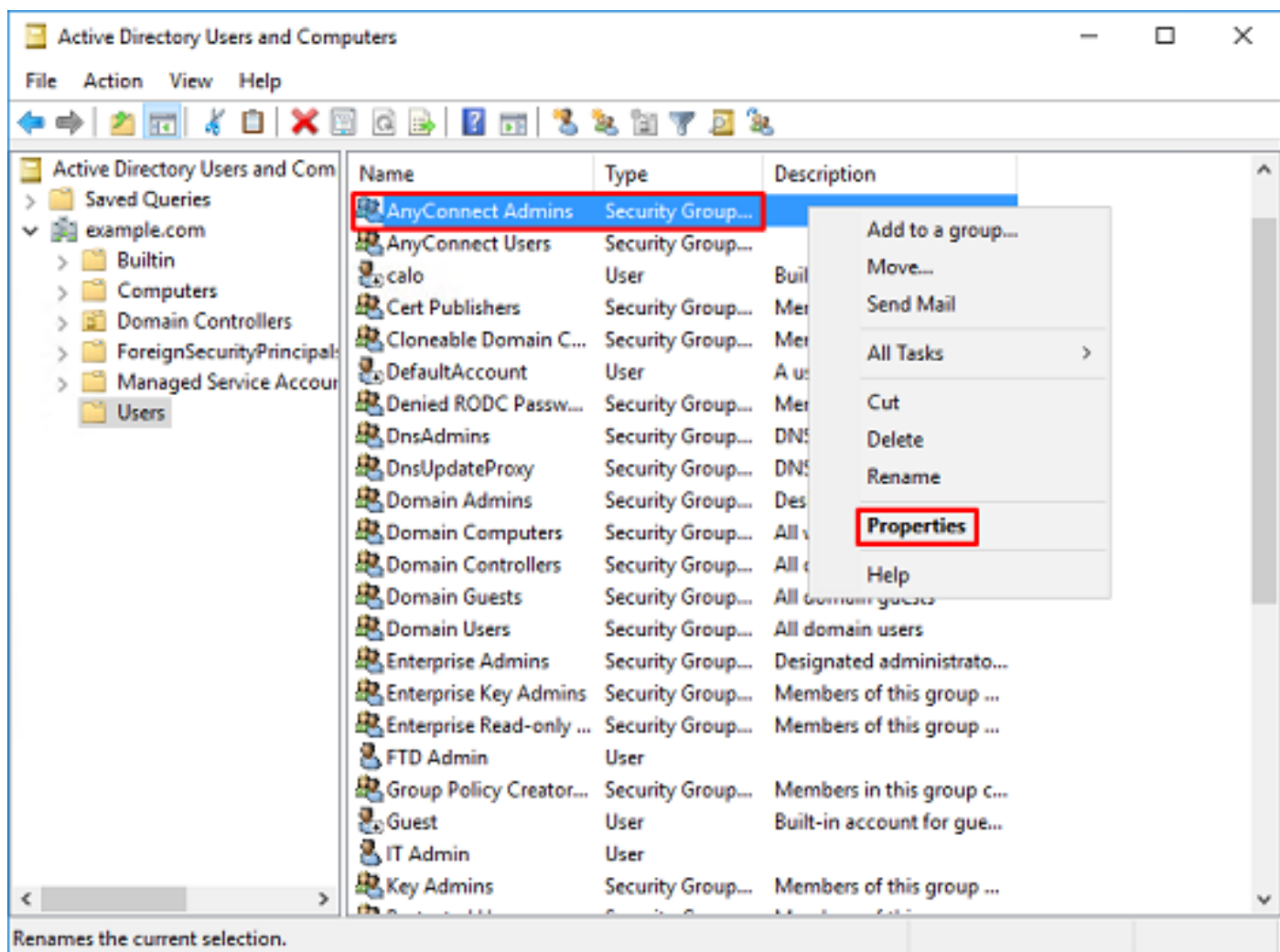
2.完成「新建對象—組」向導。



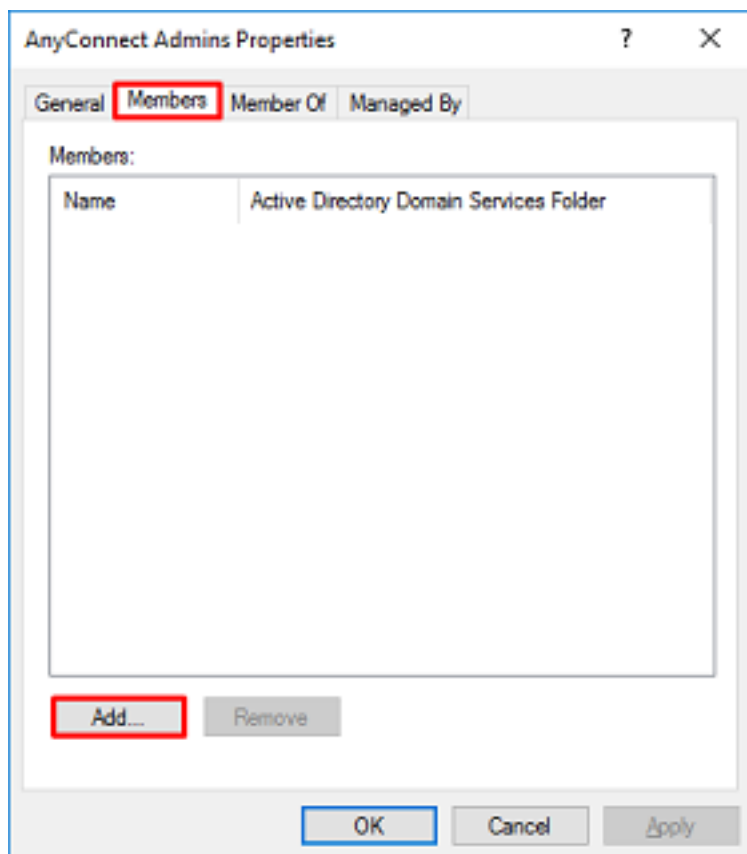
3.驗證是否已建立組。AnyConnect Users組也將建立。



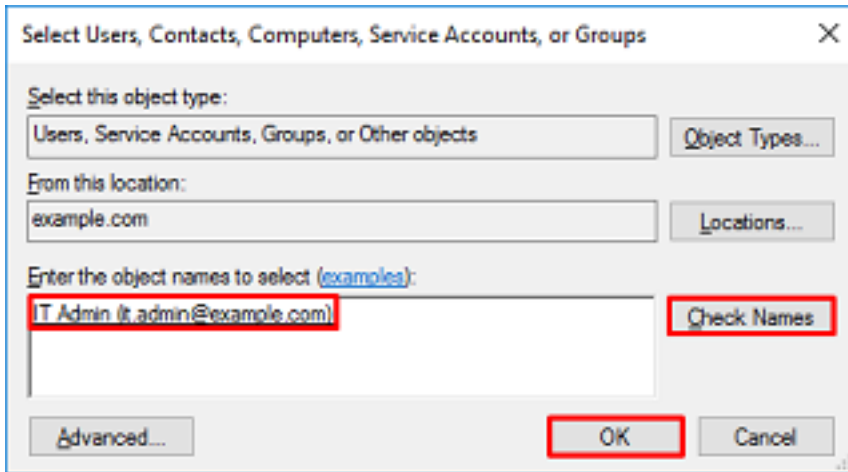
4. 按一下右鍵使用者組，然後選擇屬性。在此配置中，使用者IT Admin新增到AnyConnect Admins組，使用者Test User新增到AnyConnect Users組。



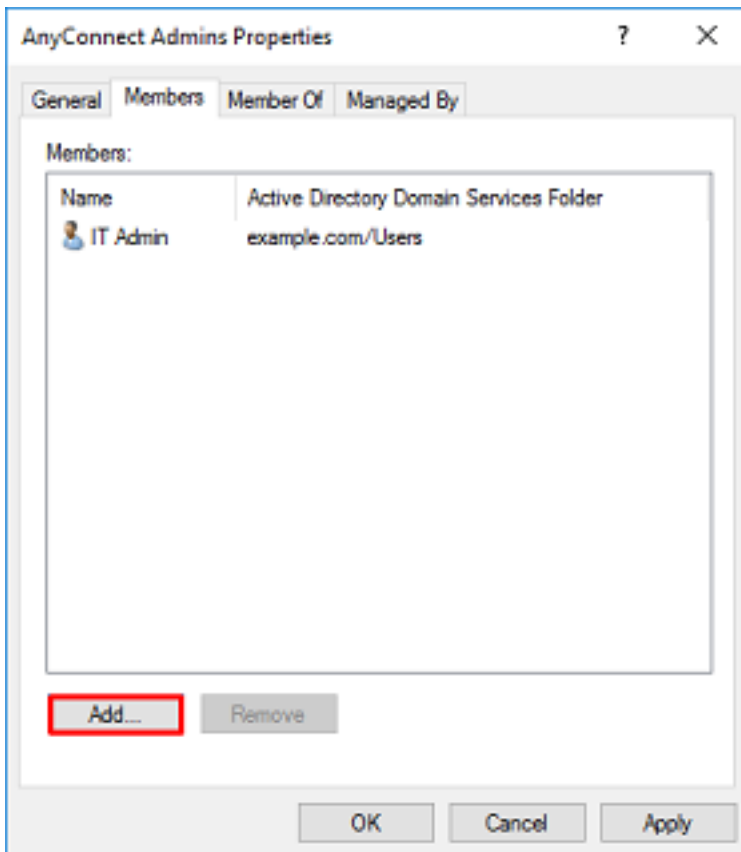
5. 在「成員」頁籤下，按一下新增。



在欄位中輸入使用者，然後按一下**Check Names**以驗證找到該使用者。驗證後，按一下**OK**。

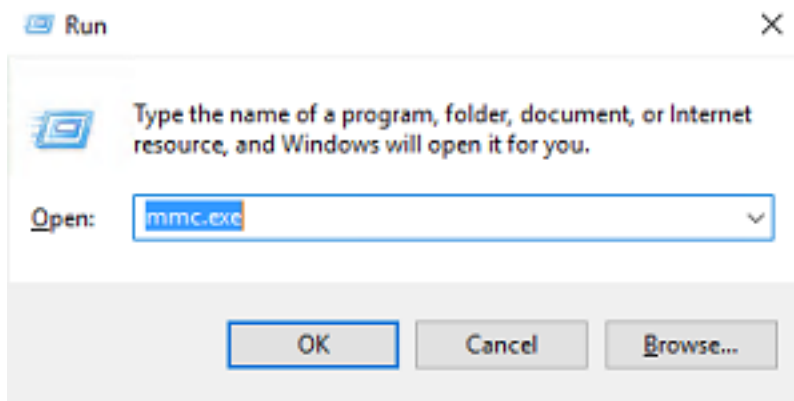


驗證是否新增了正確的使用者，然後按一下「**OK (確定)**」按鈕。使用者測試使用者也會使用相同的步驟新增到**AnyConnect**使用者組。

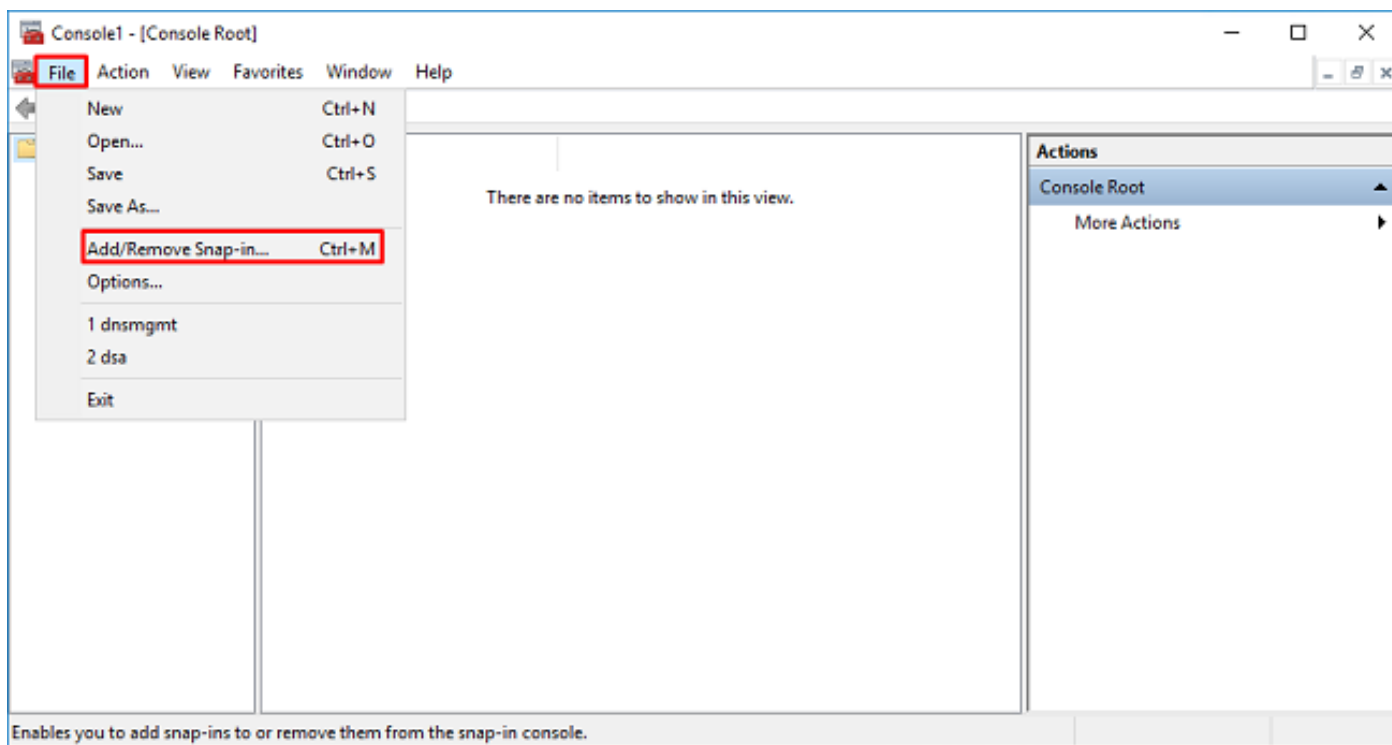


複製LDAPS SSL證書根 (僅對於LDAPS或STARTTLS是必需的)

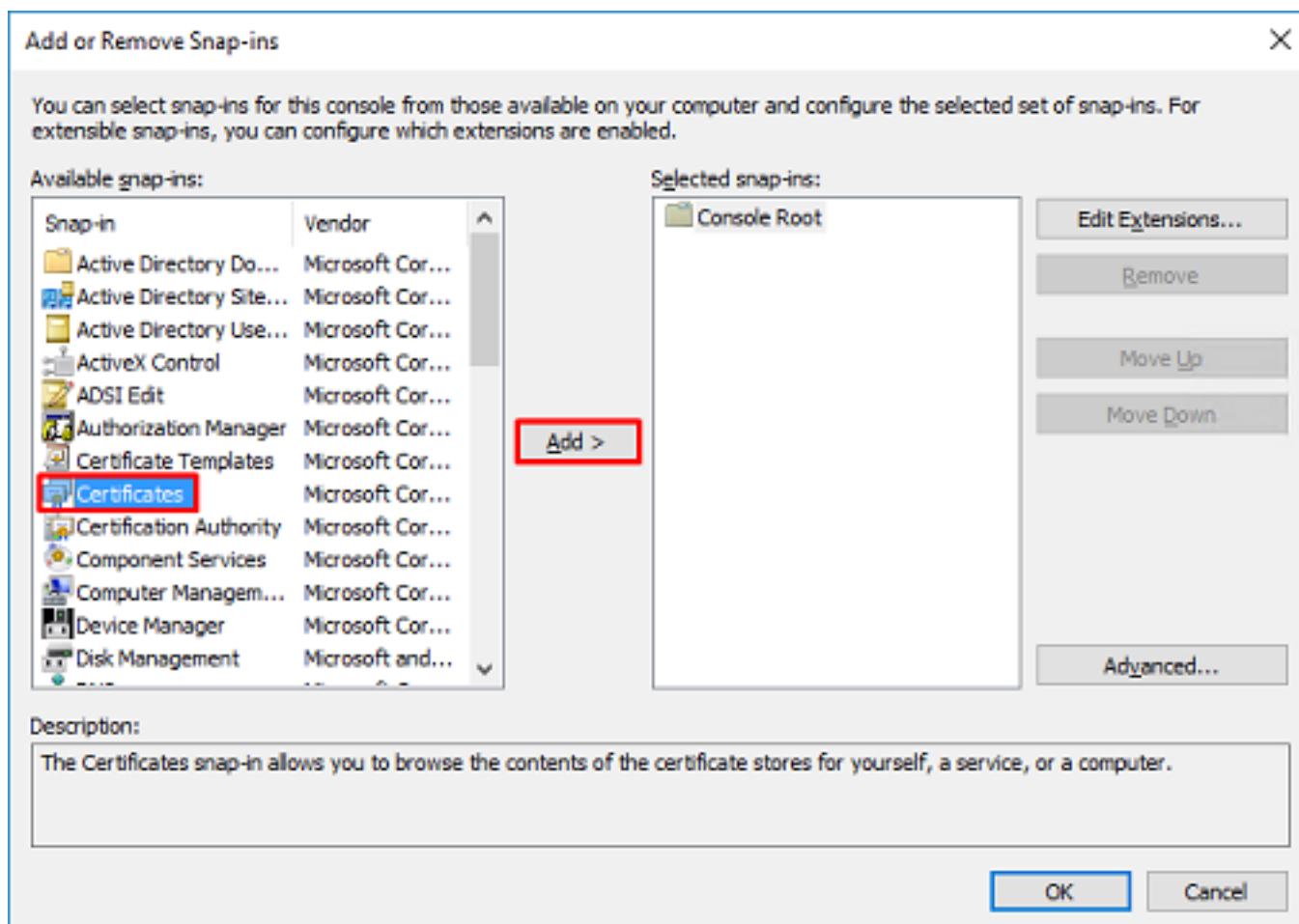
1. 按Win+R並輸入**mmc.exe**，然後按一下「確定」。



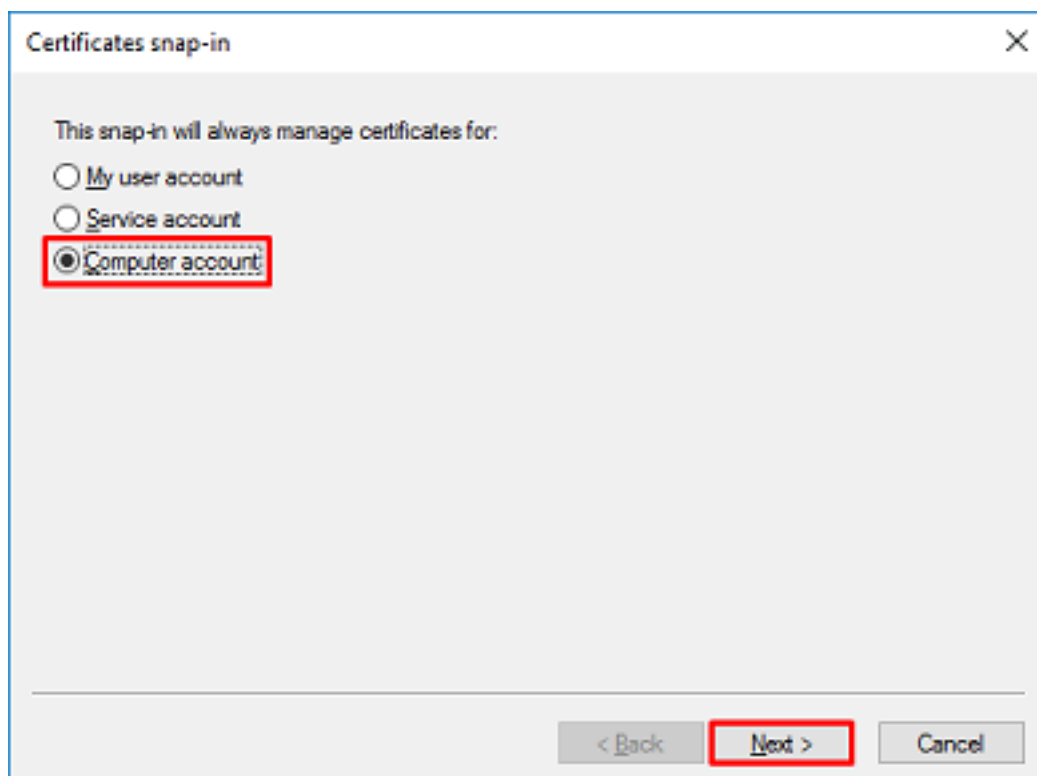
2. 導航到檔案>新增/刪除管理單元.....



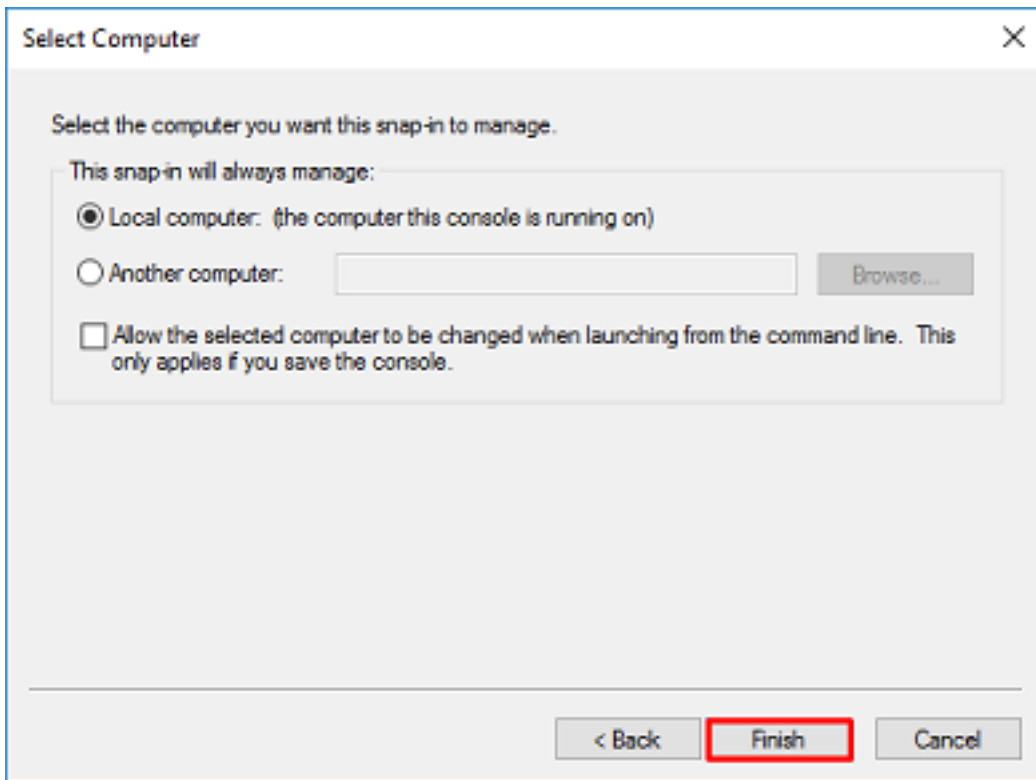
3. 在「可用管理單元」下，選擇Certificates，然後按一下Add。



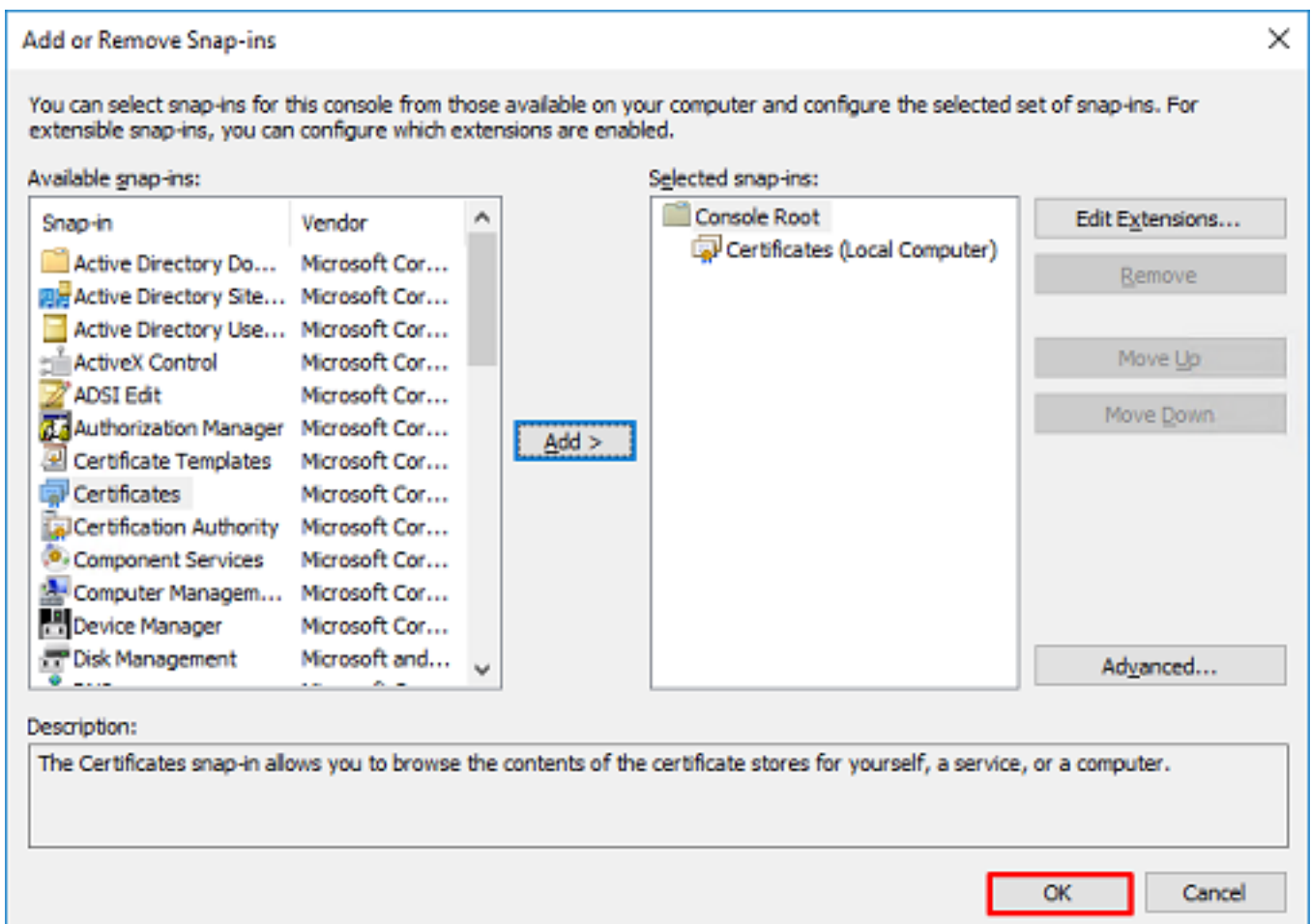
4. 選擇電腦帳戶，然後按一下下一步。



按一下「Finish」（結束）。



5.現在按一下OK。

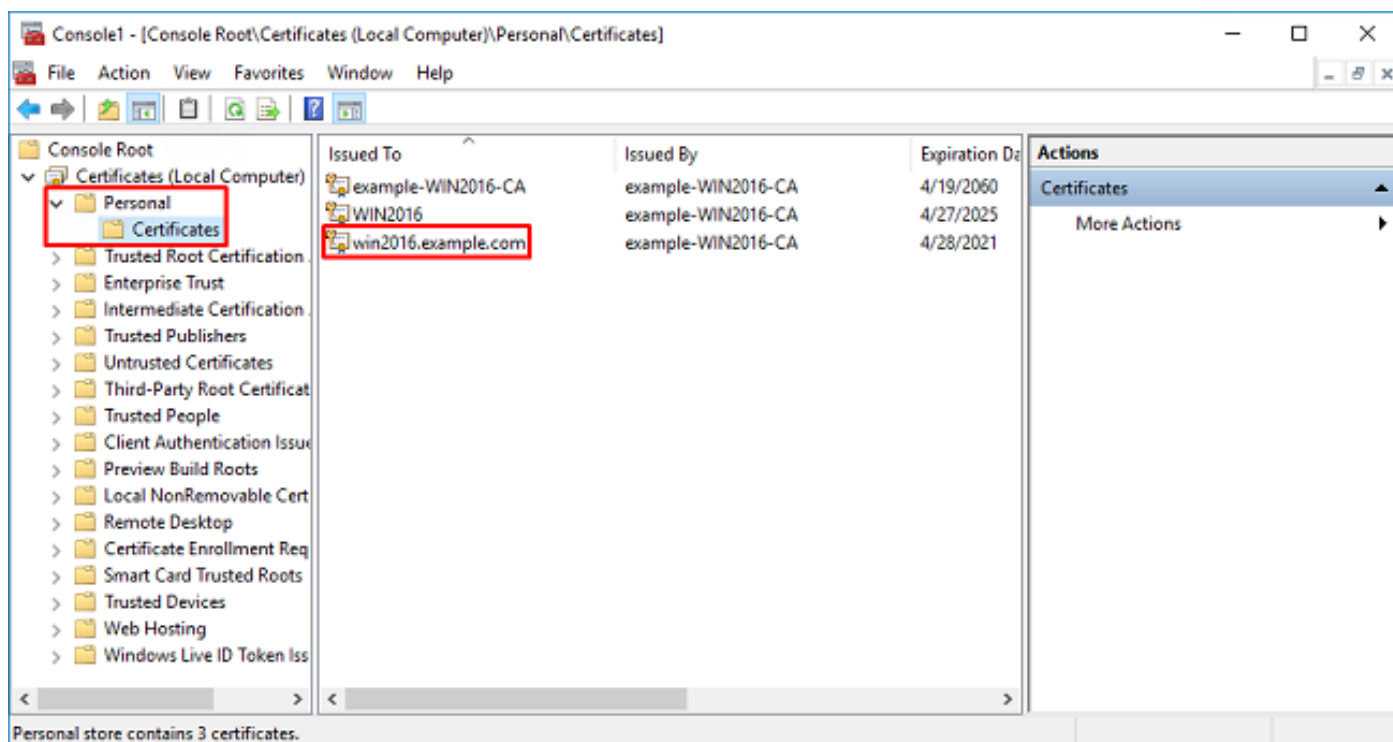


6.展開Personal資料夾，然後按一下Certificates。LDAPS使用的證書頒發給Windows服務器的完全限定域名(FQDN)。在此伺服器上列出了3個憑證。

- 頒發給example-WIN2016-CA的CA證書。

- 由example-WIN2016-CA頒發給WIN2016的身份證書。
- 由example-WIN2016-CA頒發給win2016.example.com的身份證書。

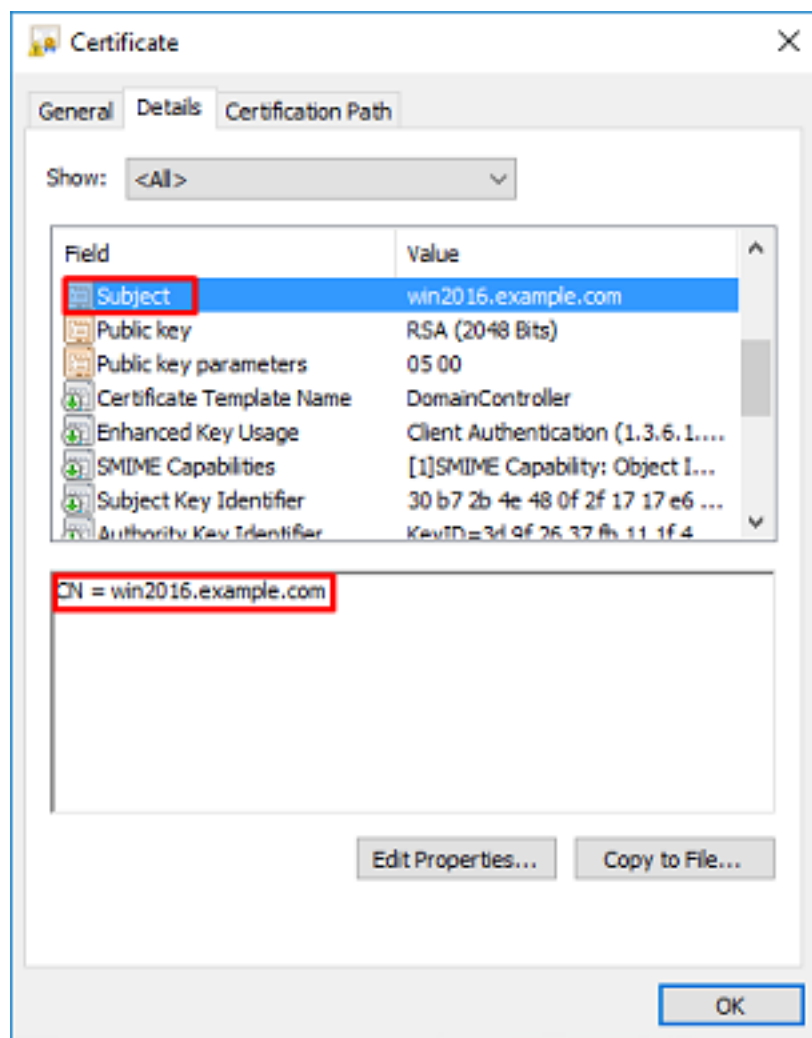
在此配置指南中，FQDN為win2016.example.com，因此前2個證書不能用作LDAPS SSL證書。頒發給win2016.example.com的身份證書是由Windows Server CA服務自動頒發的證書。按兩下證書檢查詳細資訊。

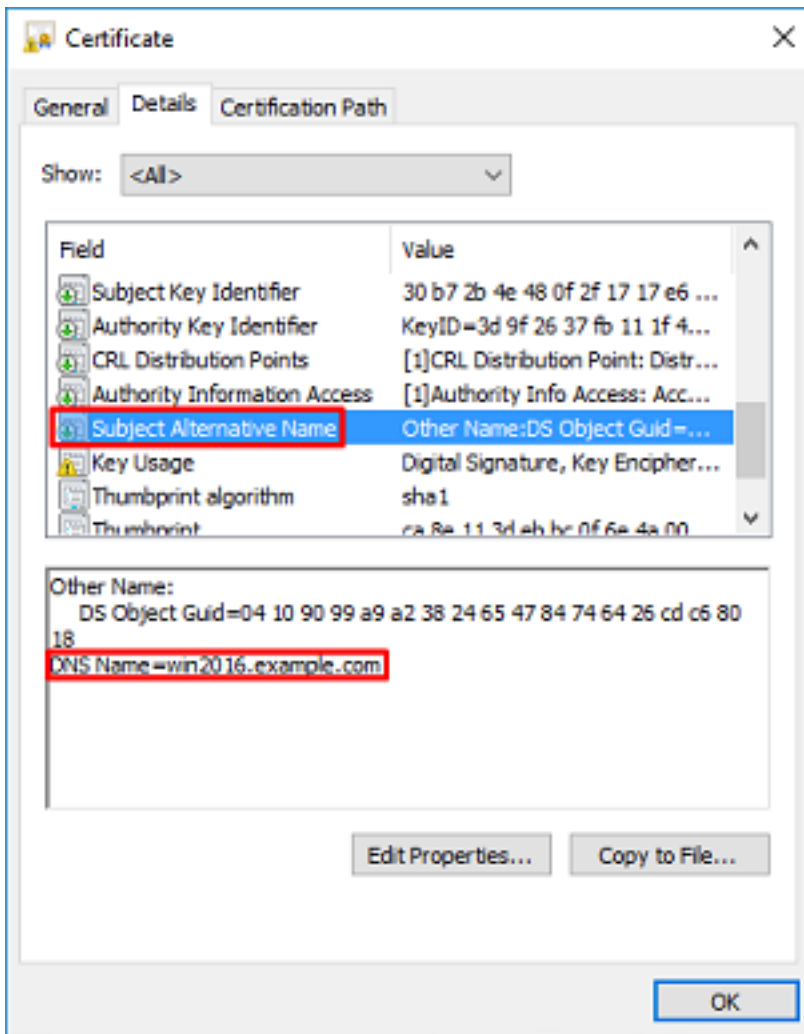


7.要用作LDAPS SSL證書，該證書必須滿足以下要求：

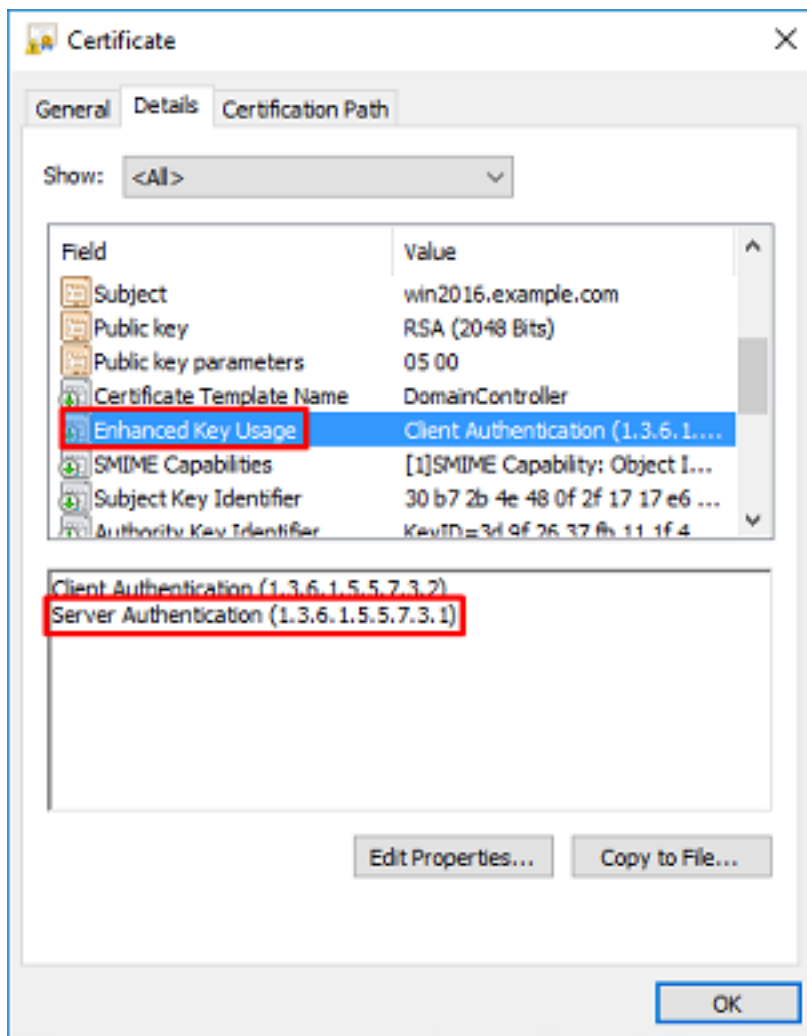
- 公用名或DNS使用者替代名稱與Windows Server的FQDN匹配。
- 在Enhanced Key Usage欄位下，證書具有Server Authentication。

在證書的Details頁籤下，選擇Subject和Subject Alternative Name，此時會顯示FQDN win2016.example.com。

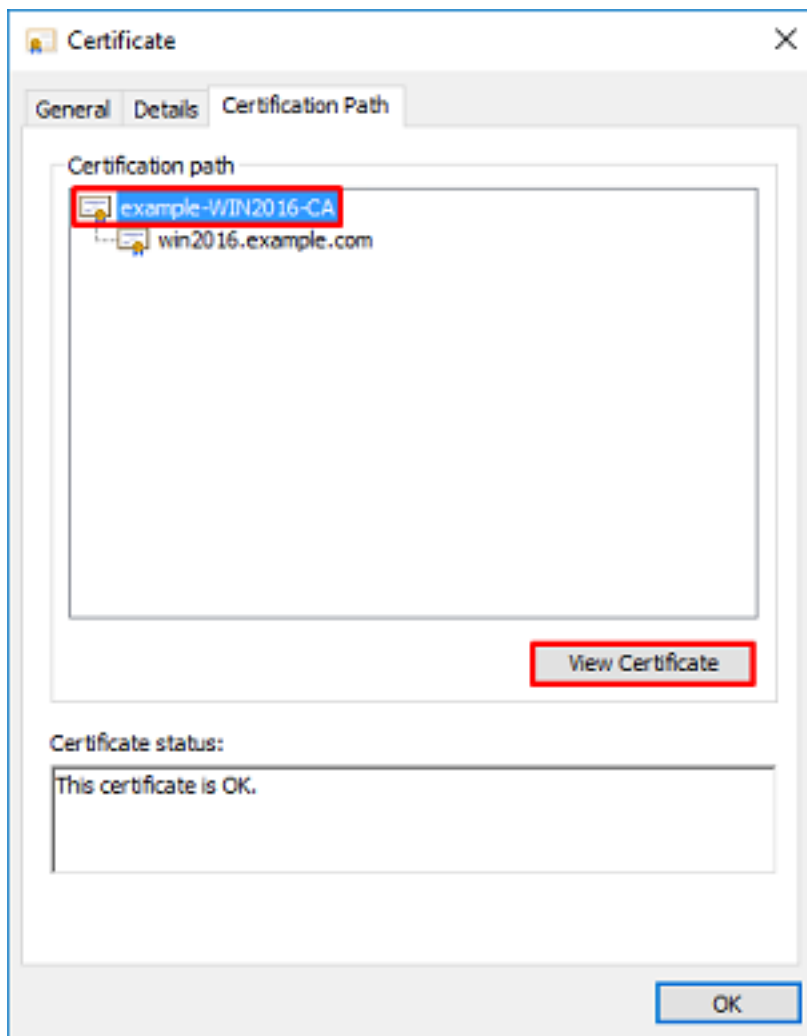




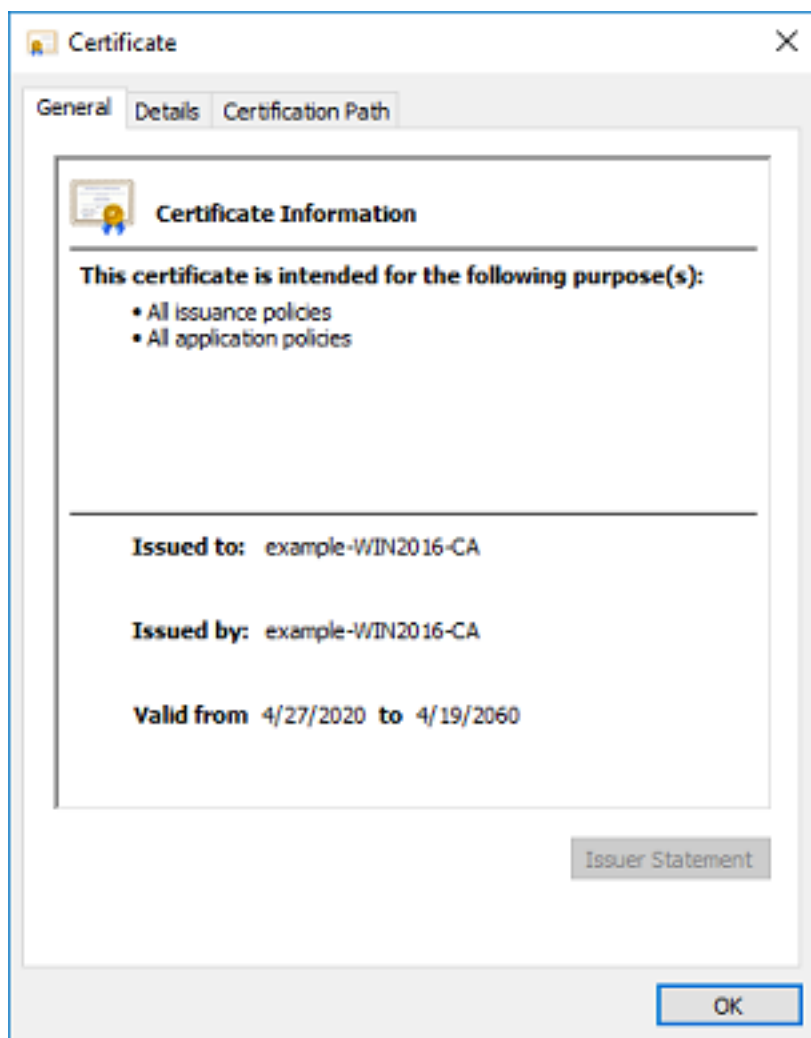
在Enhanced Key Usage下，存在Server Authentication。



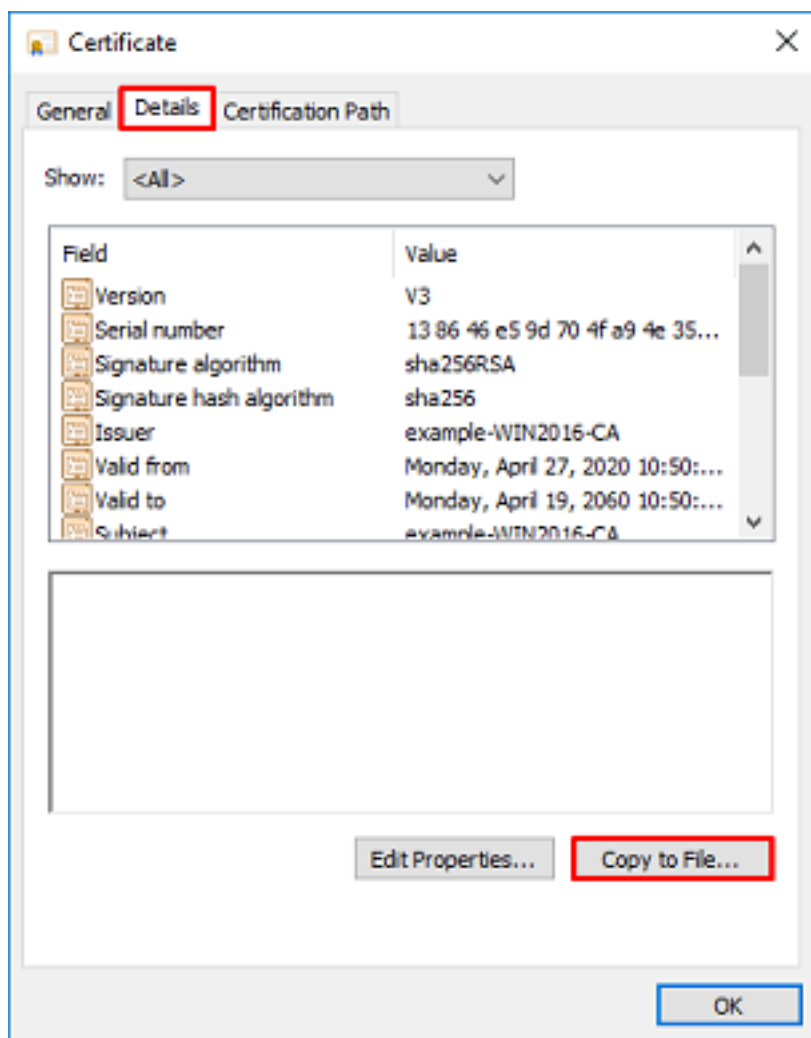
8. 確認後，在 **Certification Path** 頁籤下，選擇作為根CA證書的頂級證書，然後按一下 **View Certificate**。



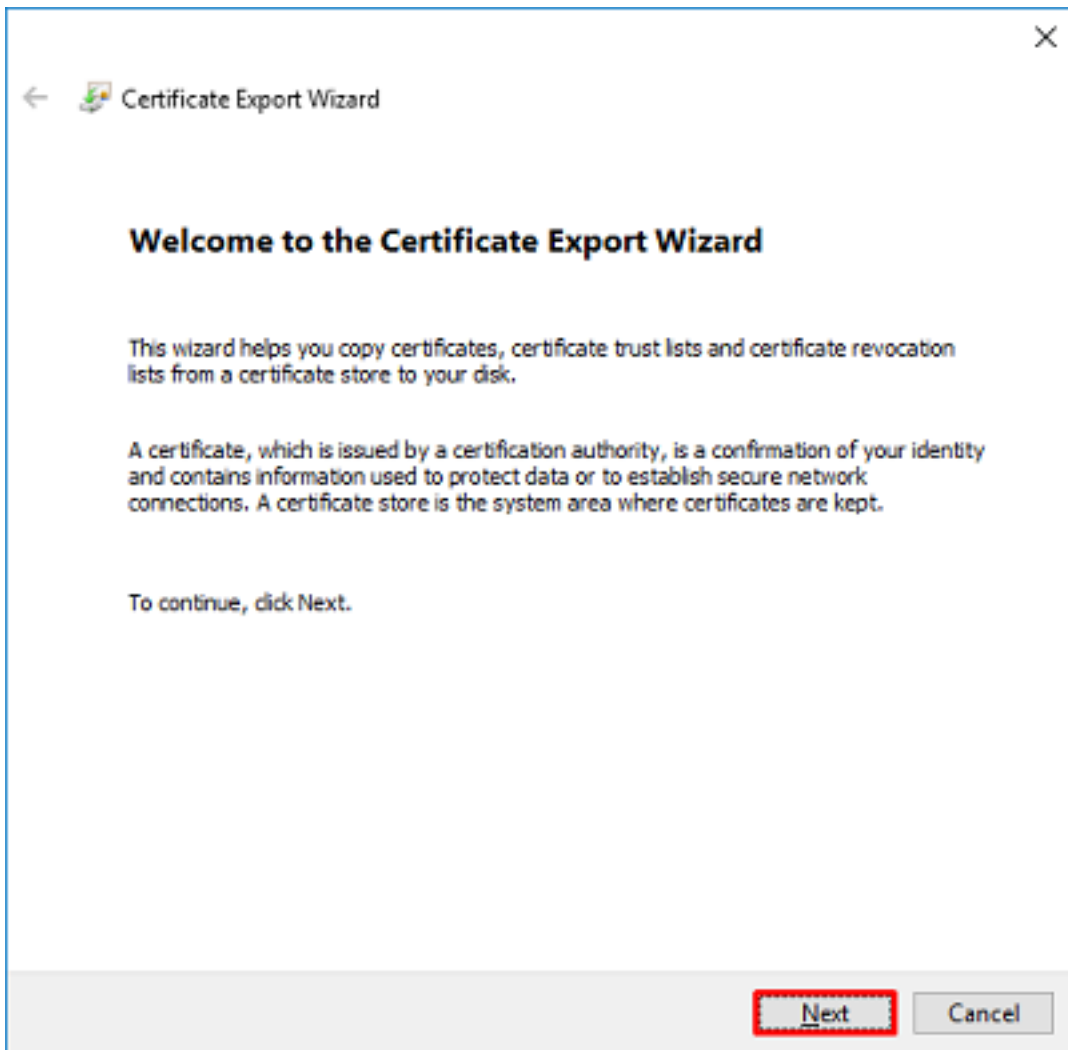
9.這將開啟根CA證書的證書詳細資訊。



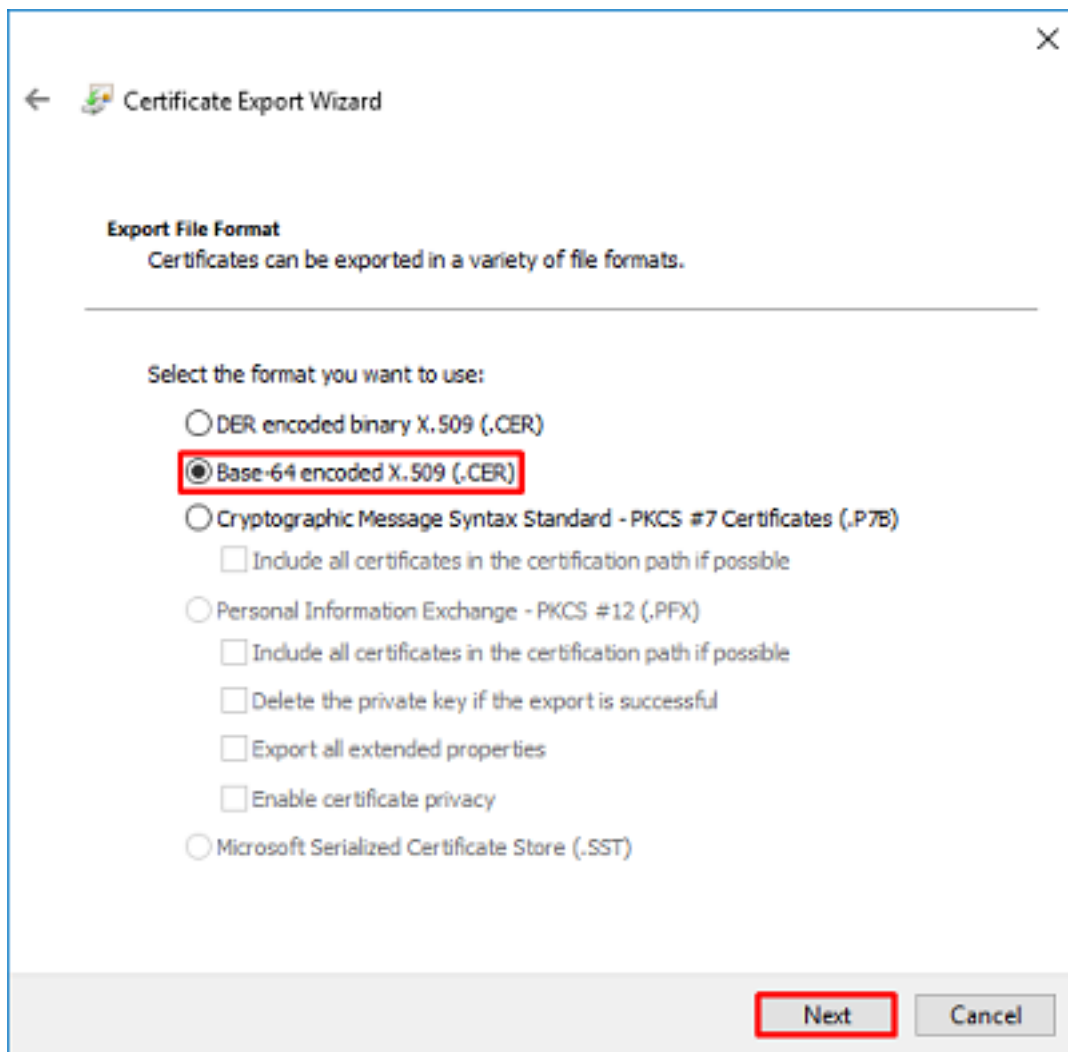
在Details頁籤下，按一下Copy to File...



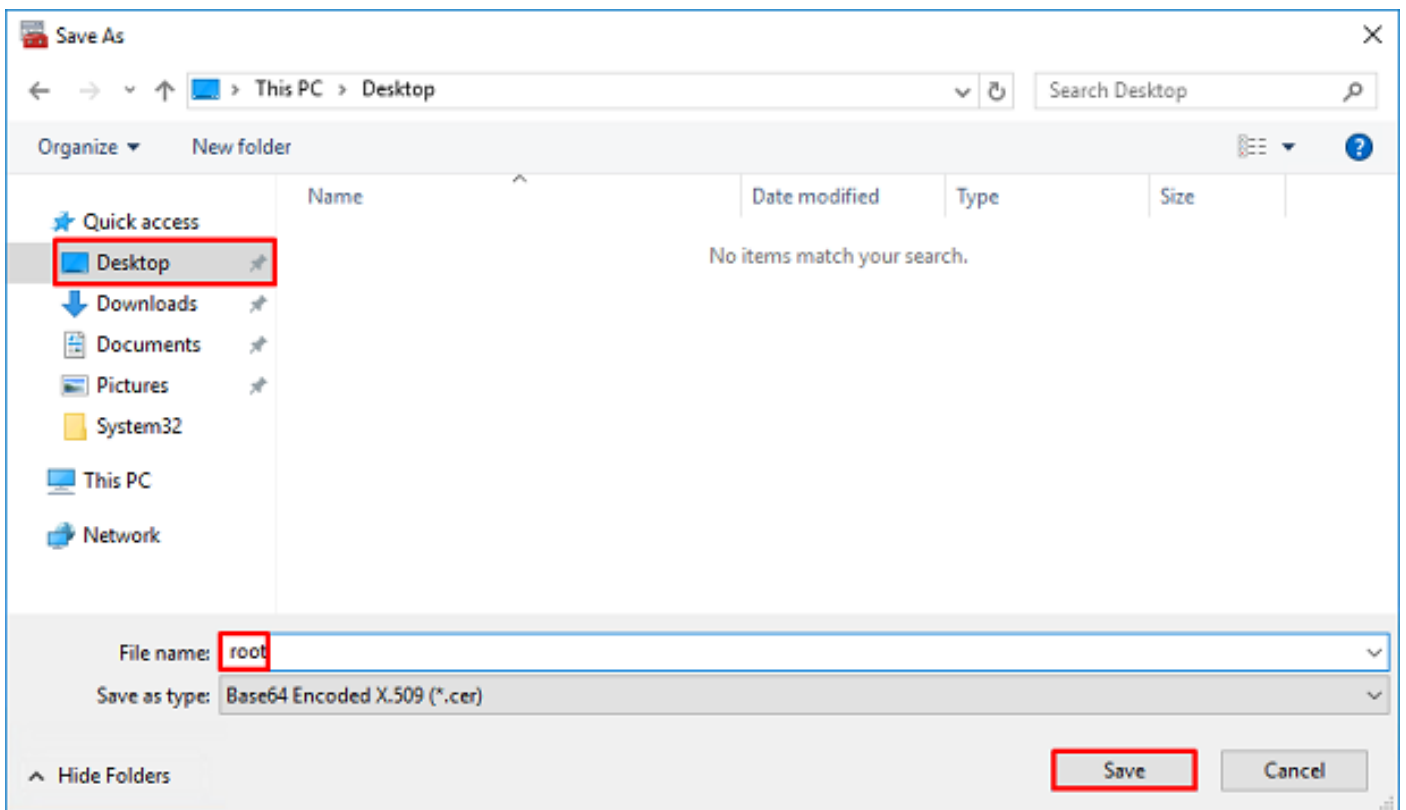
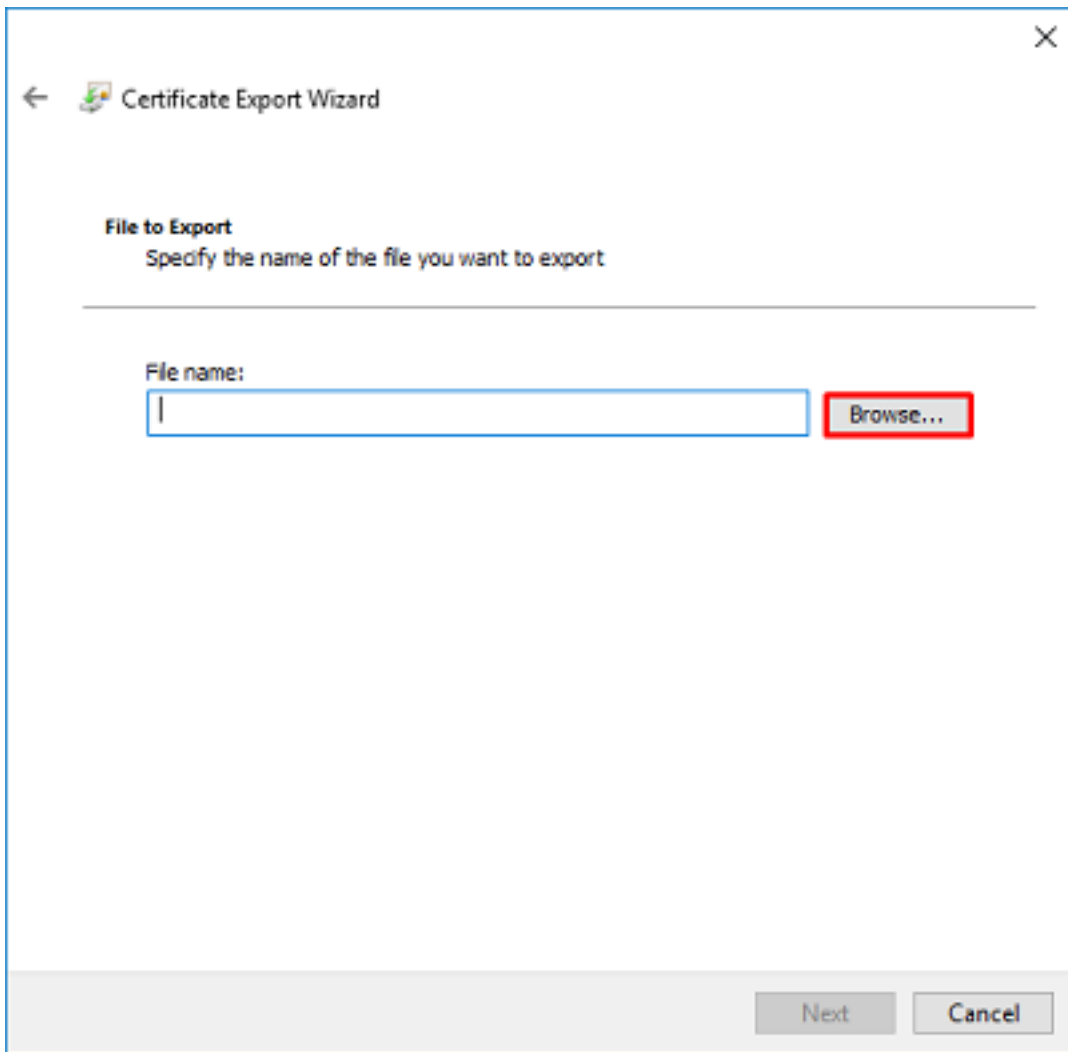
10. 通過證書導出嚮導，以PEM格式匯出根CA。

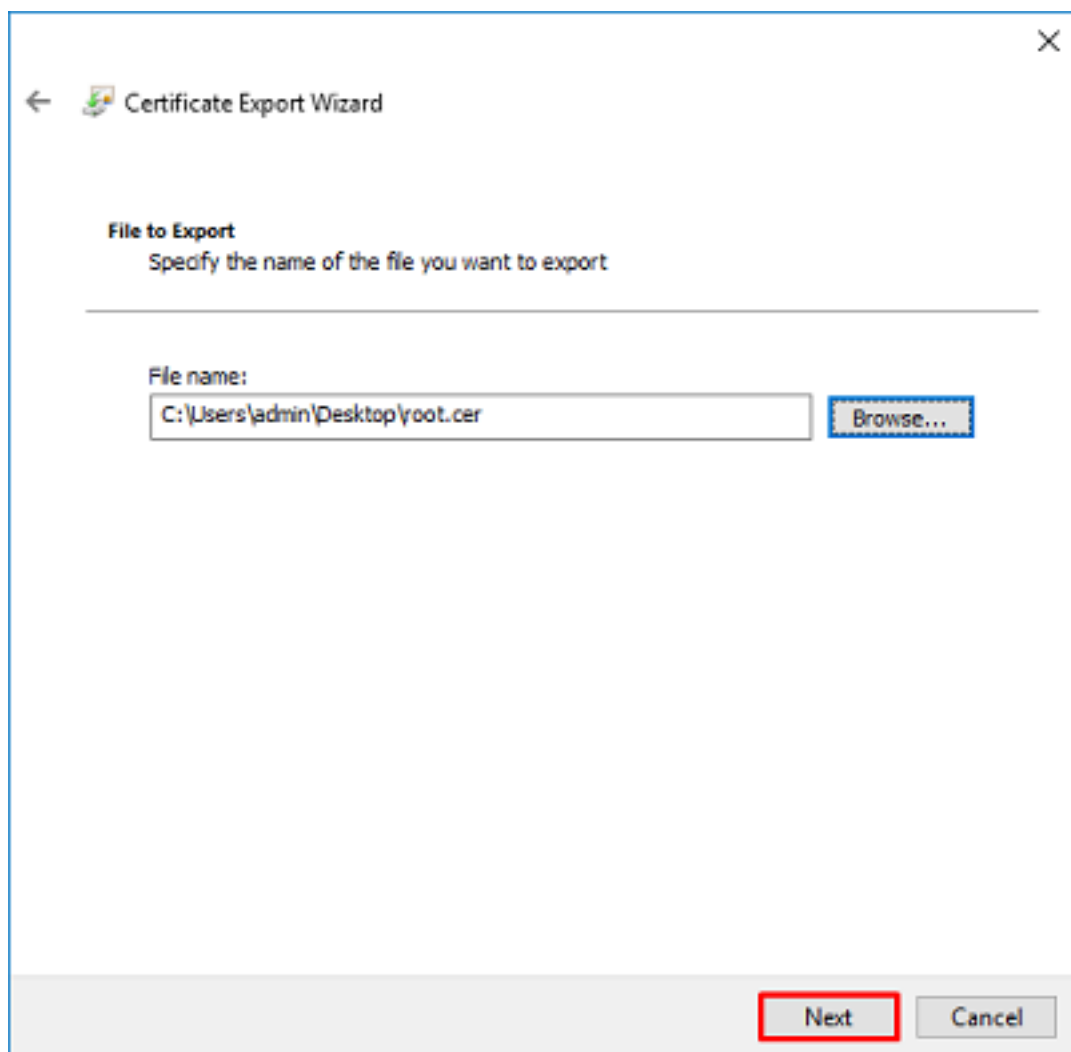


選擇Base-64 encoded X.509

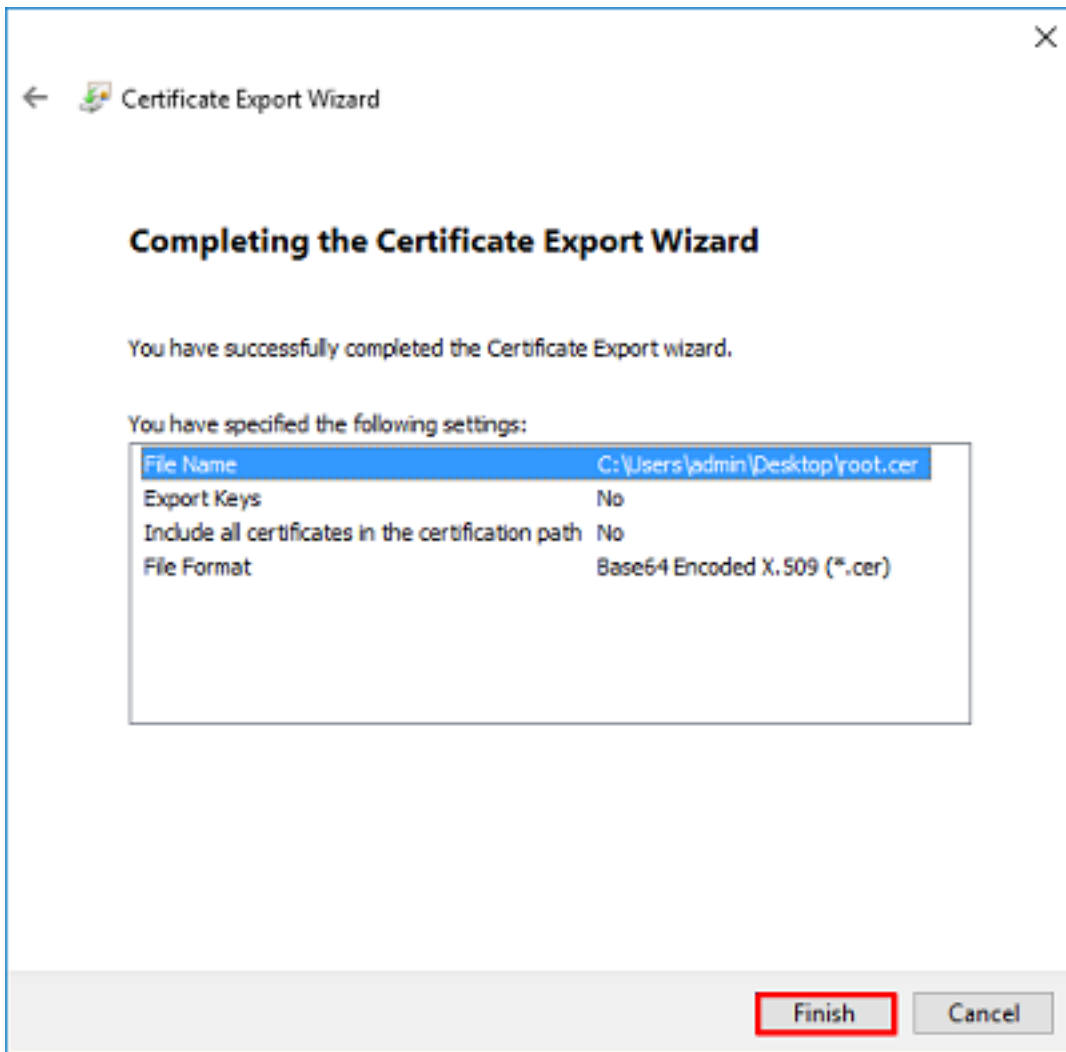


選擇檔案的名稱以及匯出檔案的位置。





現在按一下**完成**。



11. 現在轉到該位置，並使用記事本或其他文本編輯器開啟證書。這顯示PEM格式證書。儲存以備以後使用。

```
-----BEGIN CERTIFICATE-----
MIIDCCCAfCgAwIBAgIQE4ZG5Z1wT61ONTjooEQyMTANBgkqhkiG9w0BAQsFADAd
MRswGQYDVQQDEeJleGFtcGxlLVdJTjIwMTYtQ0EwIBcNMjAwNDI3MTQ1MDU5WhgP
MjA2MDA0MTkxNDUwNTlAMB0xGZAZBgNVBAMTEmV4YW1wbGUtV01OMjAxNi1DQTCC
ASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAl8ghT719NzSQpoQPh0YT67b
Ya+PngsxMyvkewP33QLTAWw1HW1Tb9Mk5BDWOItTaVsgHwPBfd++M+bLn3AiZnHV
OO+k6dVVY/E5qVkeKSGoY+v940S2316lzdWReMOFhgbc2qMertIoficrRihonuU
Cjyeub3CO+meJUuKom2R47C0D35TUvo/FEHGgXJFajS1se2UrpNO7KEMkfAlLPuM
aob4XE/OzxYQpPa18djsNnskfcFqD/HOTFQN4+SrOhHWlRnUIQBuaLdQaabhipD/
sVs5PneYJX8YKma821uYI6j90YuytmsHBtCieyC062a8BKqOL7N86HFPfkMA3u8C
AwEAAaNCMEAwDgYDVR0PAQH/BAQDAgGMA8GA1UdEwEB/wQFMAMBAf8wHQYDVR0O
BBYEFD2fJjf7ER9EM/HCxCVFN5QzqEdvMA0GCSqGSIb3DQEBCwUAA4IBAQB3lZJo
vzwVD3c5Q1nrNP+6Mq62OFpYH91k4Ch9S5g/CEOemhcwg8MDIoxW2dTsjenAEt7r
pFIHZoCoSyjBjMgK3xybmoSeg8vBjCXseYNGEm0c9KW1oFmTOvdNVIb7Xp11IVa
6tALTt3ANRNgREtXPA6yQbthKGavW0Anfsojk9IcDr2vp0MTj1BCxsTscubRl+d
dLEFKQqmMeYvkVf+a7a64mqPZsG3Uxo0rd6cZxAPkq/ylcdwNSJFFfQV3DgZg+R96
9WLCR30big6xyo9Zu+lixwPdrbAD06zMhbEYEHkh00jBrUEBBI6Cy83iTz9ejsk
KgwbJXEu33PplW6E
-----END CERTIFICATE-----
```

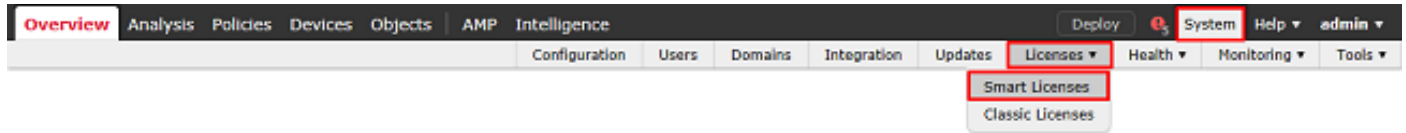
12. (可選) 如果LDAPS可使用多個身份證書，且使用哪個身份證書存在不確定性，或者無法訪問LDAPS伺服器，則可以從在Windows伺服器或FTD之後完成的資料包捕獲中提取根ca。

FMC配置

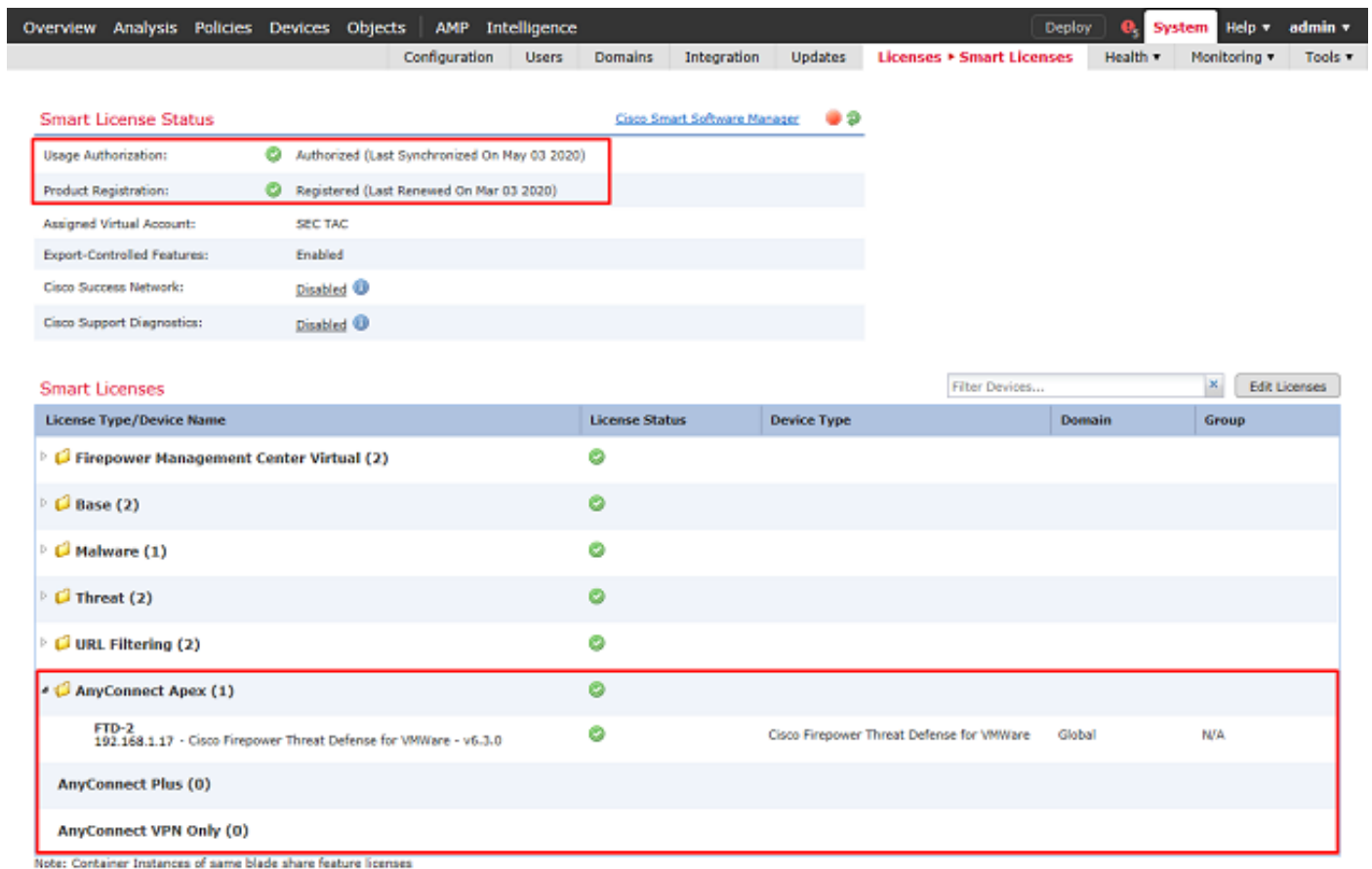
驗證許可

為了部署AnyConnect配置，FTD需要在智慧許可伺服器中註冊，並且必須向裝置應用有效的Plus、Apex或VPN僅許可證。

1. 導航至系統>許可證>智慧許可。



2. 驗證裝置是否合規並成功註冊。確保裝置已註冊到AnyConnect Apex、Plus或VPN Only許可證。



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 ⓘ

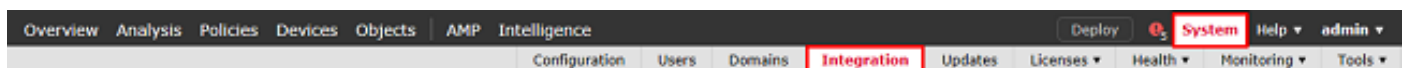
Smart Licenses

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)				

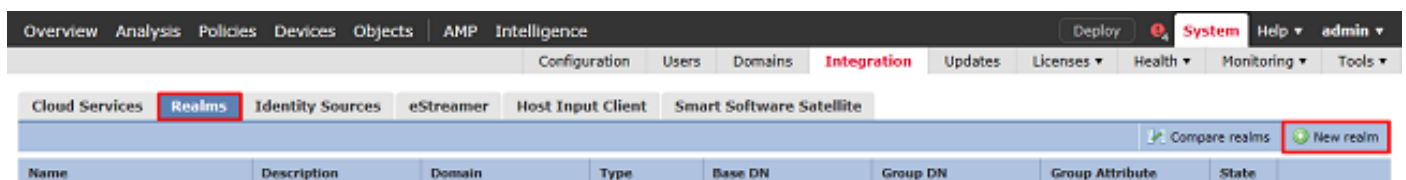
Note: Container Instances of same blade share feature licenses

設定領域

1. 定位至系統>整合。



2. 在領域下，按一下新建領域。



3. 根據從Microsoft伺服器收集的資訊填寫相應的欄位。完成後，按一下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. 在新視窗中，選擇Directory (如果尚未選擇)，然後按一下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

填寫AD伺服器的詳細資訊。請注意，如果使用FQDN，則除非將DNS配置為解析FQDN，否則FMC和FTD無法成功繫結。

要設定FMC的DNS，請導航至System > Configuration，然後選擇Management Interfaces。

若要為FTD設定DNS，請導覽至Devices > Platform Settings，建立一個新原則，或編輯目前的原則，然後前往DNS。

Add directory

Hostname / IP Address win2016.example.com

Port 389

Encryption STARTTLS LDAPS None

SSL Certificate

OK Test Cancel

如果使用LDAPS或STARTTLS，請按一下綠色+符號，為證書指定一個名稱，然後複製PEM格式的根CA證書。完成後按一下**Save**。

Import Trusted Certificate Authority

Name:

Certificate Data or, choose a file:

```
-----BEGIN CERTIFICATE-----
MIIDCDCCAFcGAWIBAgIQE4ZG5Z1wT6lONTjooEQyMTANBgkqhkiG9w0BAQsFADAd
MRswGQYDVQQDEExleGFtZG93LmVudG93LmVudG93LmVudG93LmVudG93LmVudG93
MjA2MDA0MTkxNDUwNTlaMB0xGzAZBgNVBAMTEV4YVw1wbG93LmVudG93LmVudG93
ASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAl8ghT719NzSQpoQPh0YT67b
Ya+PngsxMyvkewP33QLTAWw1HW1Tb9Mk5BDWOItaVsgHwPBfd++M+bLn3AiZnHV
OO+k6dVVVY/E5qVKEKSGoY+v940S2316lzdwrReMOFhgbc2qMertIoficrRihonuU
Cjyeub3CO+meJUuKom2R47C0D35TUvo/FEHGgXJFaJS1se2UrpNO7KEMkFA1LPuM
aob4XE/OzxYQpPa18djsNnskfCfQD/HOTFQN4+SrOhHWIRnUIQBUaLdQaabhipD/
sVs5PneYJX8YKma821uYI6j90YuytmsHBtCieyC062a8BKqOL7N86HFPFkMA3u8C
AwEAAaNCMEAwDgYDVR0PAQH/BAQDAgGGMA8GA1UdEwEB/wQFMAMBAf8wHQYDVR0O
BBYEFD2fj7ER9EM/HcXCVFN5QzqEdvMA0GCSqGSIb3DQEBCwUAA4IBAQB31ZJo
vzwVD3c5Q1nrNP+6Mq62OFpYH91k4Ch9S5g/CEOemhcgw8MDIoxW2dTsjenAet7r
phFIHZoCoSyjBjMgK3xybmoSeg8vBjCXseYNGEmOc9KW1oFmTOvdNVIb7Xpl1IVa
6tALTt3ANRNgREtPA6yQbthKGavW0Anfsojk9IcDr2vp0MTjBCxsTscubRI+D
dLEFKQqmMeYvkvf+a7a64mqPZsG3Uxo0rd6cZxAPkq/yIcdwNSJFFQV3DgZg+R96
9WLCR3Obig6xyo9Zu+lixwPdrbADO6zMhbEYEHkhOOjBrUEBBI6Cy83iTZ9ejsk
KgwBJXEu33PplW6E
-----END CERTIFICATE-----
```

Encrypted, and the password is:

從SSL Certificate旁邊的下拉選單中選擇新增的根CA，然後按一下STARTTLS或LDAPS。

Edit directory

Hostname / IP Address:

Port:

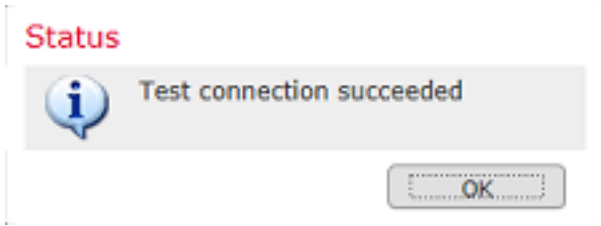
Encryption: STARTTLS LDAPS None

SSL Certificate:

按一下測試以確保FMC能夠使用上一步中提供的目錄使用者名稱和密碼成功繫結。

由於這些測試是從FMC啟動的，而不是通過FTD上配置的某個可路由介面（如內部、外部、dmz），因此成功（或失敗）的連線不能保證AnyConnect身份驗證的相同結果，因為AnyConnect LDAP身份驗證請求是從FTD可路由介面之一啟動的。

有關從FTD測試LDAP連線的更多資訊，請檢視「故障排除」區域中的「測試AAA」和「資料包捕獲」部分。



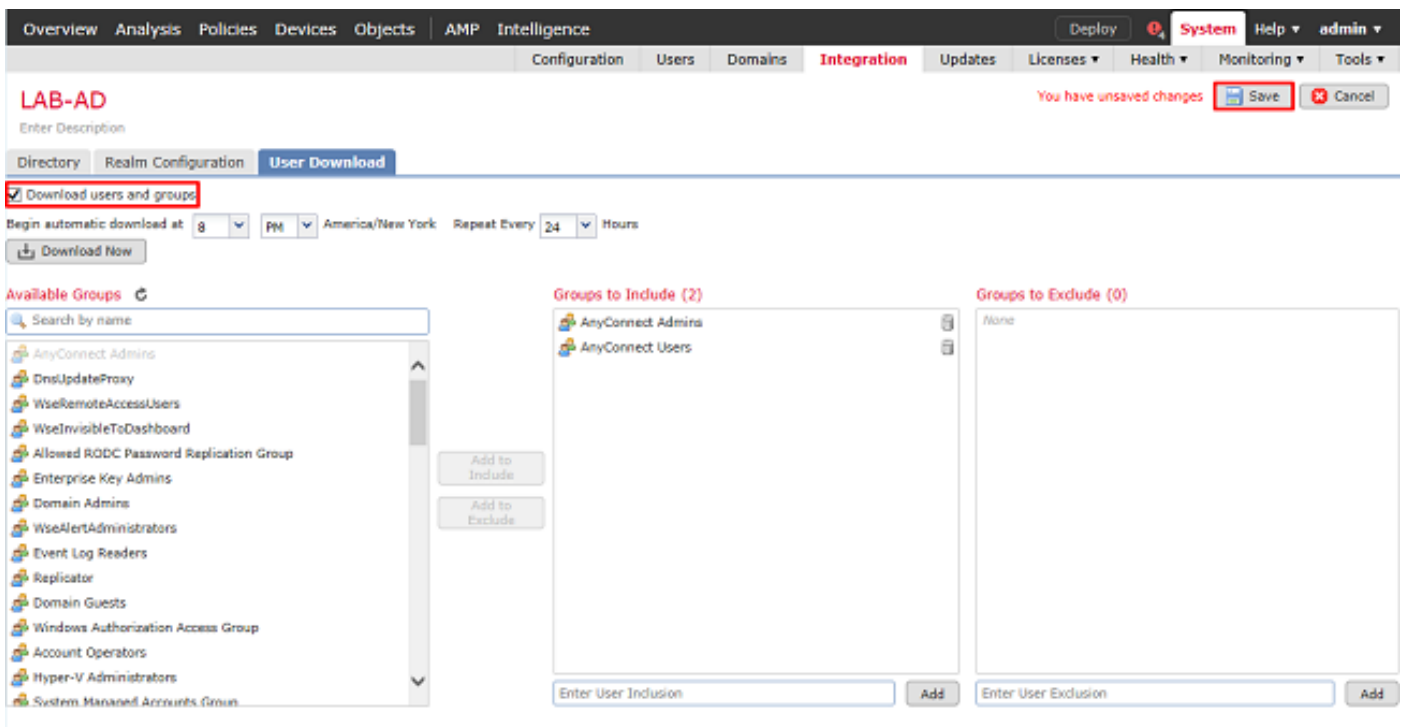
5.在User Download下，在後續步驟中下載用於使用者身份的組。

選中Download users and groups覈取方塊，Available Groups列將填充在Active Directory中配置的組。

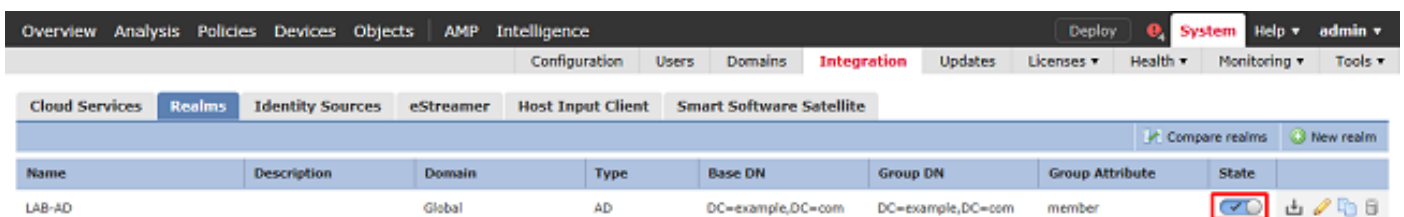
組可以包括(Included)或排除(Excluded)，但預設情況下包括組DN下找到的所有組。

也可以包括或排除特定使用者。任何包含的組和使用者都可供以後選擇用於使用者身份。

完成後，按一下「Save」。



6.啟用新領域。



7.如果使用LDAPS或STARTTLS，則根CA也需要由FTD信任。為此，請首先導覽至Devices > Certificates。

按一下右上角的Add。

選擇FTD，將LDAP配置新增到中，然後點選綠色+符號。

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*: 

為信任點指定名稱，然後從註冊型別下拉選單中選擇手動註冊。將PEM根ca證書貼上到此處，然後按一下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 ficrRihonuU Cjyeub3CO+meJUuKom2R47C0D35TUvo/FEHGgXJFaJS1se2UrpN O7KEMkfA1LPuM aob4XE/OzxYQpPa18djsNnskfcFqD/HOTFQN4+SrOhHWIRnUIQBU aLdQaabhipD/ sVs5PneYJX8YKma821uYI6i90YuytmsHBTcieyC062a8BKqOL7N86

Allow Overrides

驗證已選擇建立的信任點，然後按一下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

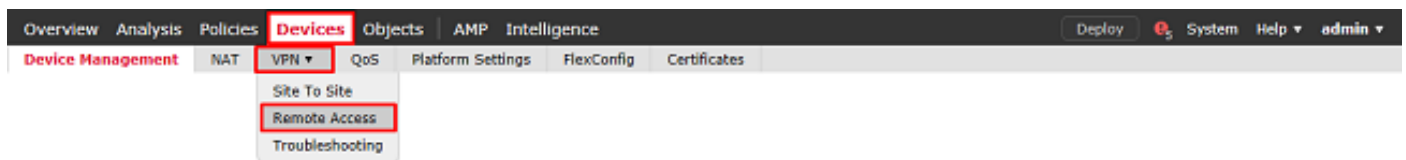
新信任點將出現在FTD下。雖然其中提到需要匯入身份證書，但對於FTD而言，並不要求能夠對LDAPS伺服器傳送的SSL證書進行身份驗證，因此可以忽略此消息。

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

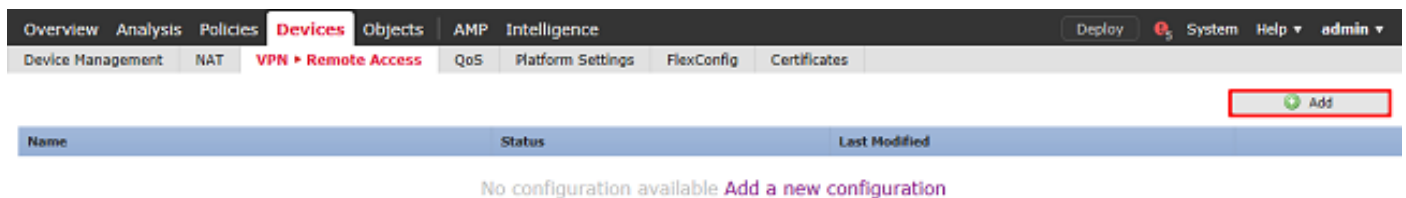
配置AnyConnect進行AD身份驗證

1.這些步驟假定尚未建立遠端訪問vpn策略。如果已建立策略，請點選該策略的edit按鈕，並跳至步驟3。

導覽至Devices > VPN > Remote Access。



按一下Add建立新的遠端訪問VPN策略



2.完成遠端訪問VPN策略嚮導。在Policy Assignment下，指定策略名稱和應用該策略的裝置。

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

Targeted Devices and Protocols
This wizard will guide you through the required minimal steps to configure the Remote Access VPN policy with a new user-defined connection profile.

Name: *

Description:

VPN Protocols: SSL IPsec-IKEv2

Targeted Devices: **Available Devices** **Selected Devices**

Available Devices: FTD-1 FTD-2

Selected Devices: FTD-2

Add

Before You Start

Before you start, ensure the following configuration elements to be in place to complete Remote Access VPN Policy.

Authentication Server
Configure [Realm](#) or [RADIUS Server Group](#) to authenticate VPN clients.

AnyConnect Client Package
Make sure you have AnyConnect package for VPN Client downloaded or you have the relevant Cisco credentials to download it during the wizard.

Device Interface
Interfaces should be already configured on targeted [devices](#) so that they can be used as a security zone or interface group to enable VPN access.

Back Next Cancel

在Connection Profile下，指定Connection Profile的名稱，該名稱也用作AnyConnect使用者在連線時看到的組別名。

指定以前在Authentication Server下建立的領域。

指定為AnyConnect客戶端分配IP地址的方法。

指定用於此連線配置檔案的預設組策略。

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

Connection Profile:
Connection Profiles specify the tunnel group policies for a VPN connection. These policies pertain to creating the tunnel itself, how AAA is accomplished and how addresses are assigned. They also include user attributes, which are defined in group policies.

Connection Profile Name: *
This name is configured as a connection alias, it can be used to connect to the VPN gateway

Authentication, Authorization & Accounting (AAA):
Specify the method of authentication (AAA, certificates or both), and the AAA servers that will be used for VPN connections.

Authentication Method:

Authentication Server: * (Realm or RADIUS)

Authorization Server: (RADIUS)

Accounting Server: (RADIUS)

Client Address Assignment:
Client IP address can be assigned from AAA server, DHCP server and IP address pools. When multiple options are selected, IP address assignment is tried in the order of AAA server, DHCP server and IP address pool.

Use AAA Server (RADIUS only) ⓘ

Use DHCP Servers

Use IP Address Pools

IPv4 Address Pools: ⓘ

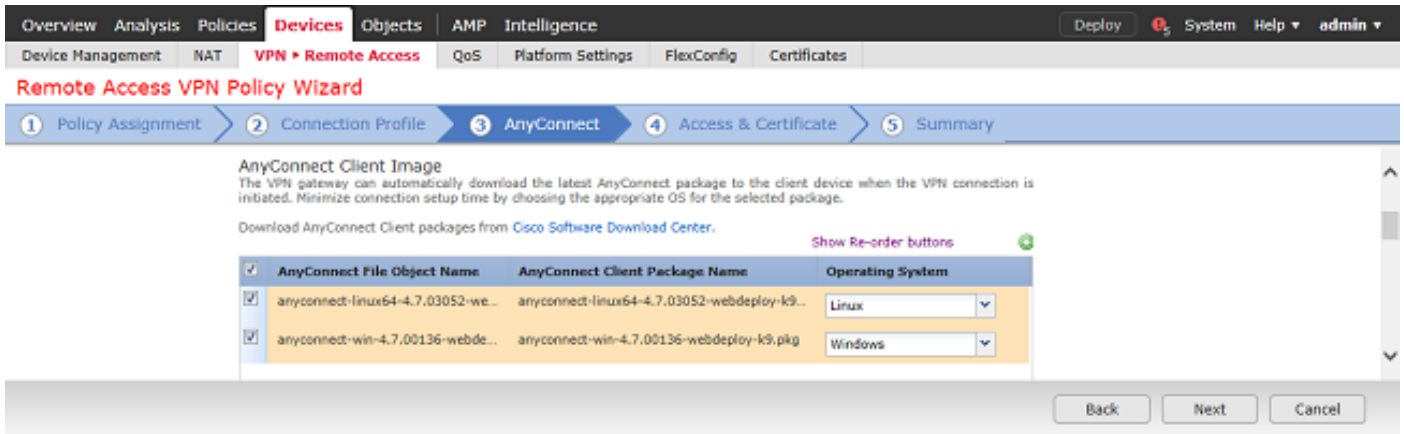
IPv6 Address Pools: ⓘ

Group Policy:
A group policy is a collection of user-oriented session attributes which are assigned to client when a VPN connection is established. Select or create a Group Policy object.

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

Back Next Cancel

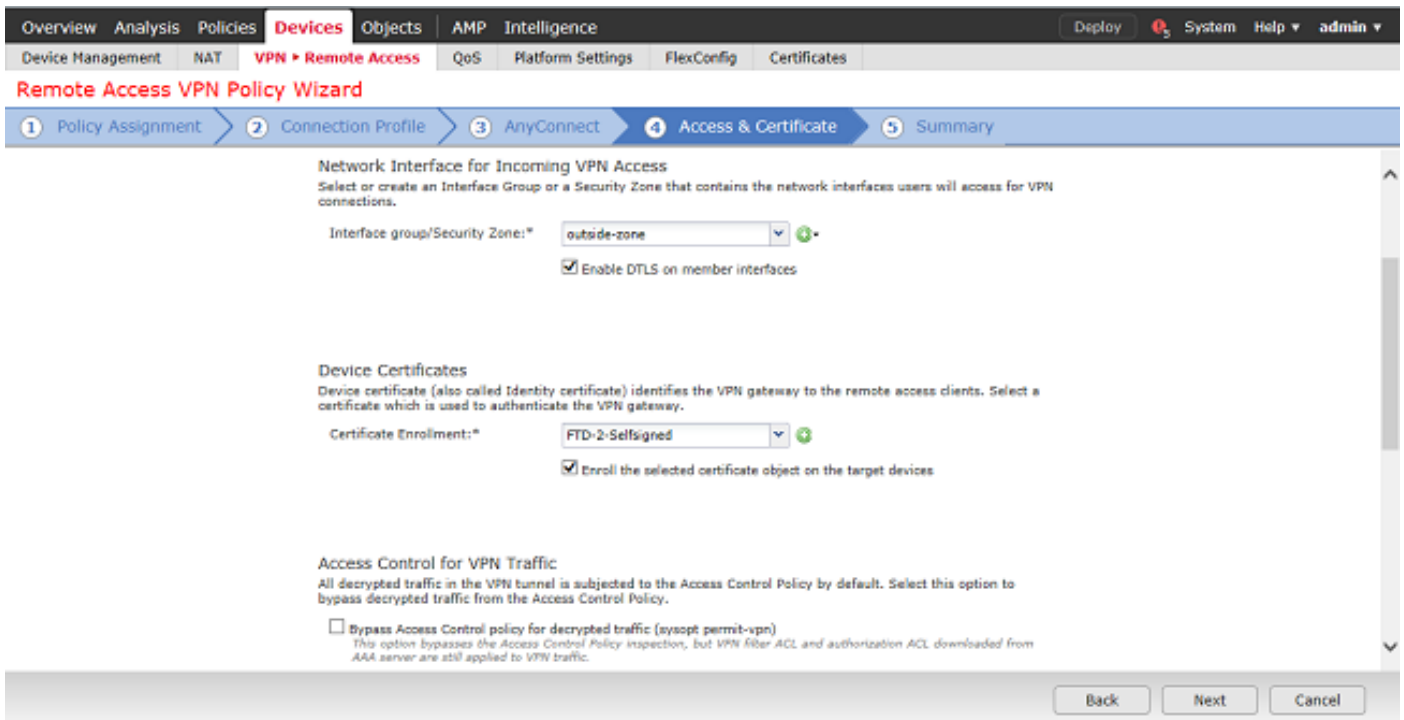
在AnyConnect下，上傳並指定使用的AnyConnect軟體包。



在Access & Certificate下，指定AnyConnect使用者訪問AnyConnect的介面。

建立和/或指定FTD在SSL交握期間使用的憑證。

確保取消選中解密流量(sysopt permit-vpn)的旁路訪問控制策略覈取方塊，以便以後建立的使用者標識對RAVPN連線生效。



在Summary下，按一下Finish檢視配置。

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: DftGrpPolicy

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Remote Access VPN Policy下，按一下相應的Connection Profile的edit。

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	<input type="checkbox"/> DftGrpPolicy
General	Authentication: LAB-AD (AD) Authorization: None Accounting: None	<input checked="" type="checkbox"/> DftGrpPolicy

確保將身份驗證伺服器設定為之前建立的領域。

在Advanced Settings下，可以選中Enable Password Management，以允許使用者在其密碼到期時或之前更改其密碼。

但是，此設定要求領域使用LDAPS。如果進行了任何更改，請按一下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

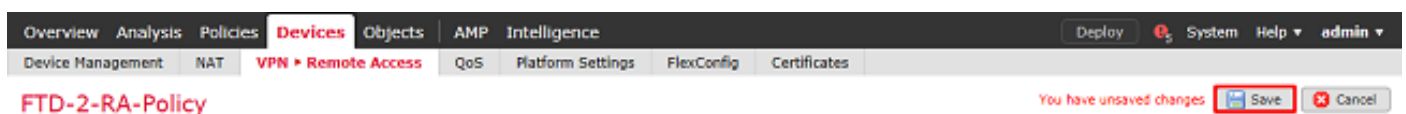
Enable Password Management

Notify User days prior to password expiration

Notify user on the day of password expiration

Save **Cancel**

完成後，按一下右上角的**Save**。



啟用身份策略並為使用者身份配置安全策略

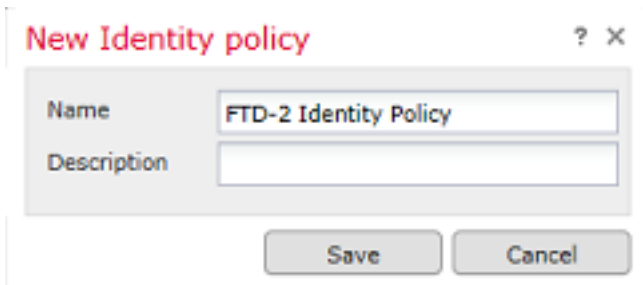
1. 定位至策略>訪問控制>標識。



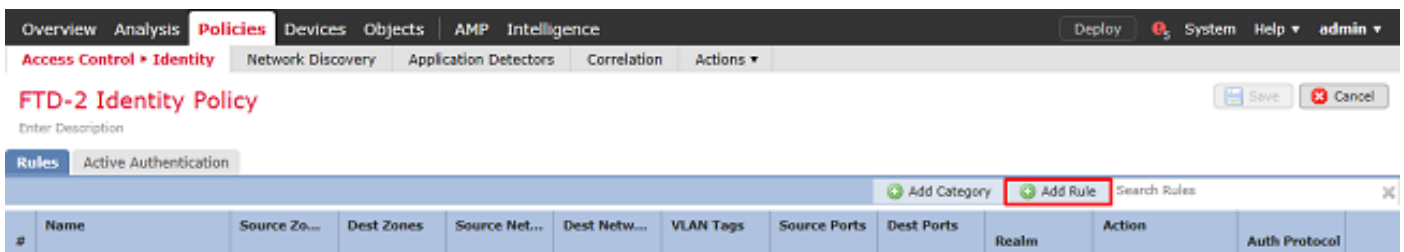
建立新的身份策略。



指定新身份策略的名稱。

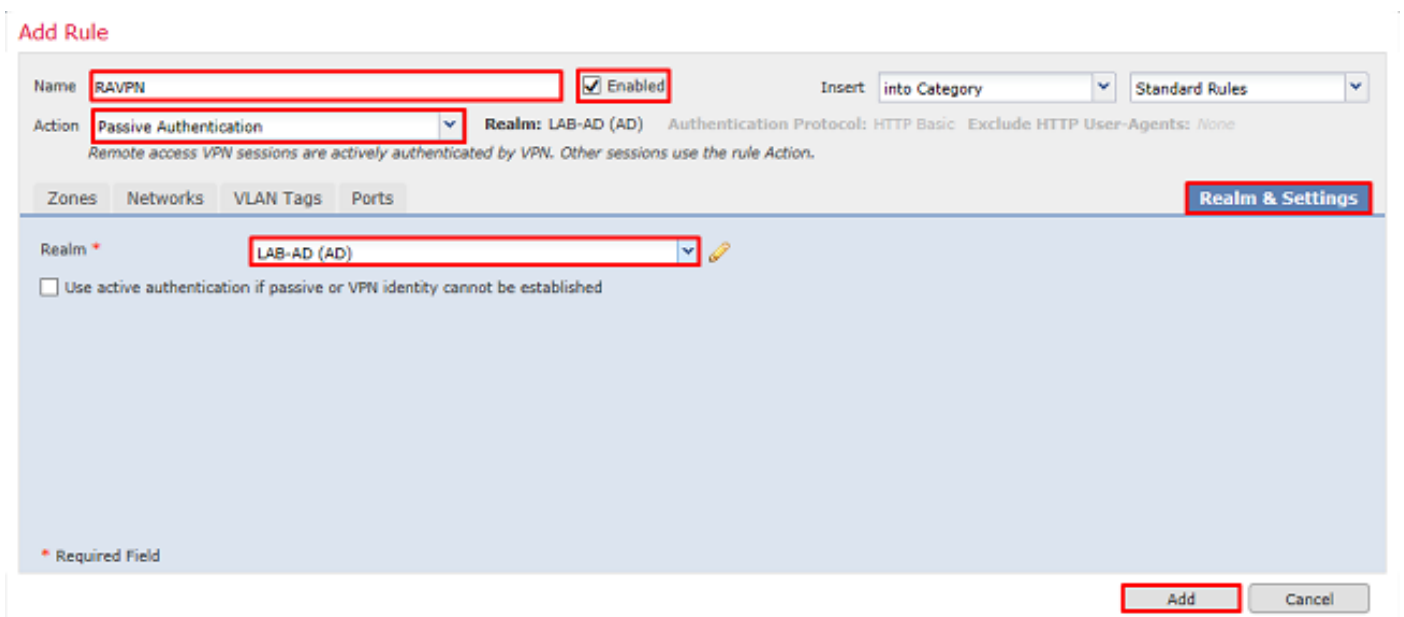


2. 按一下新增規則。

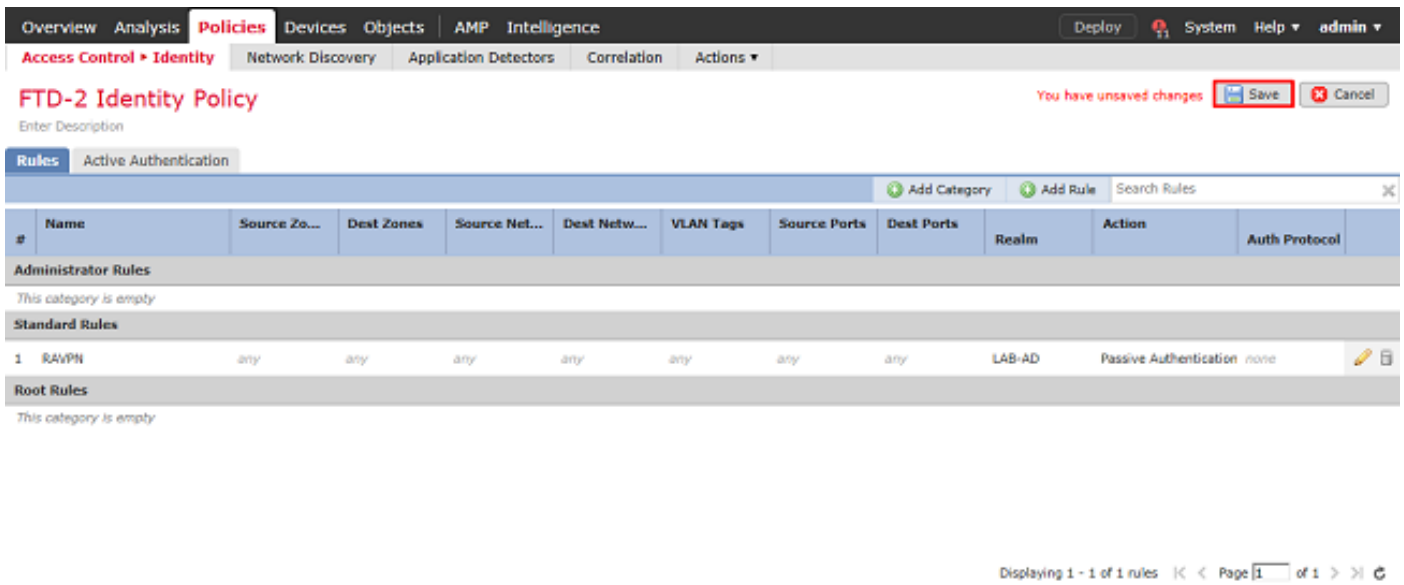


3. 為新規則指定名稱。請確保已啟用該功能，並將操作設定為Passive Authentication。

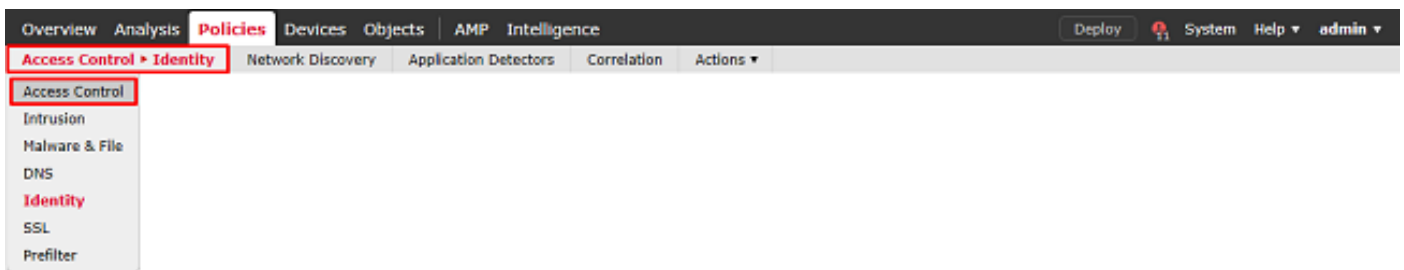
按一下Realm & Settings頁籤，然後選擇之前建立的領域。完成後按一下Add。



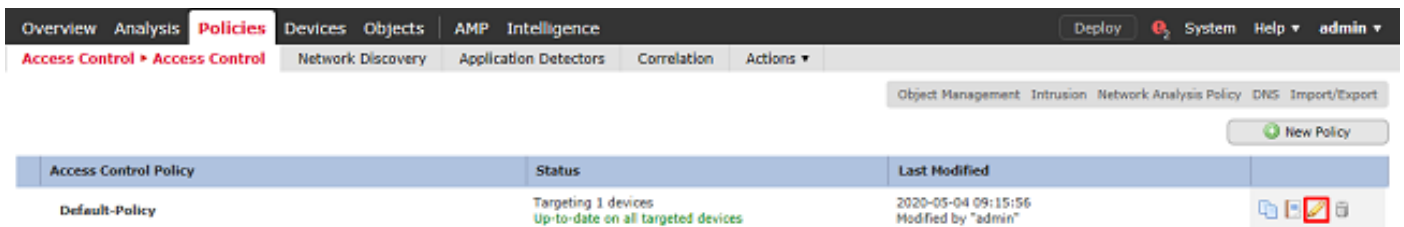
4. 按一下Save。



5. 定位至策略>訪問控制>訪問控制。



6. 編輯FTD配置所在的訪問控制策略。



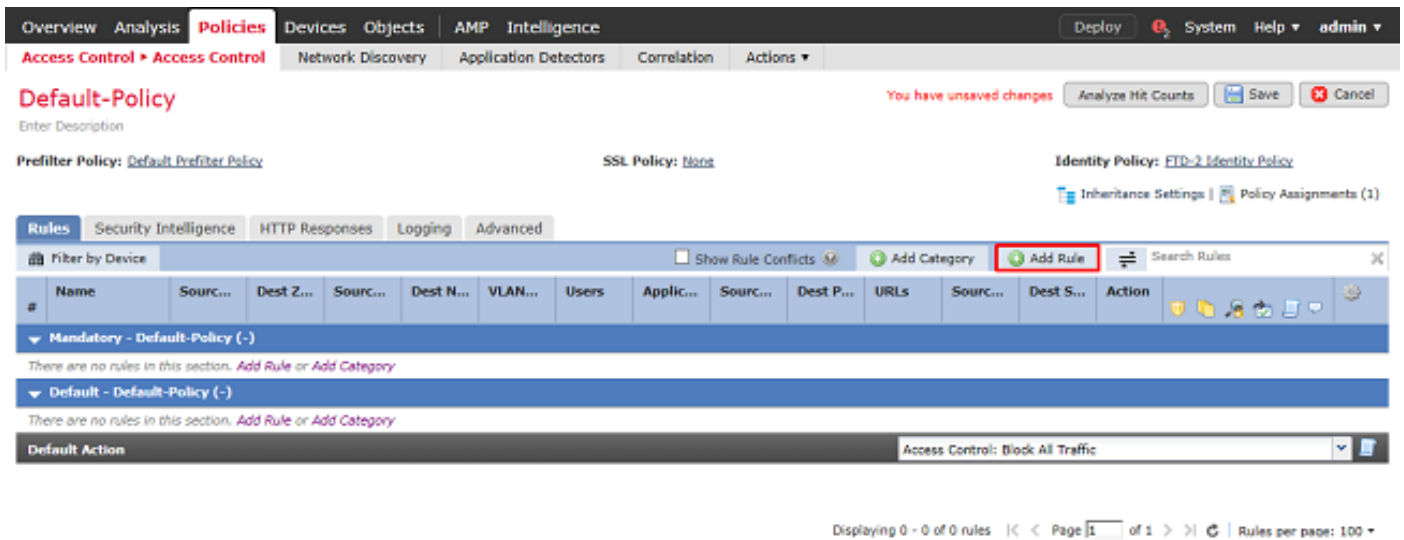
7. 按一下Identity Policy旁邊的值。



選擇之前建立的身份策略，然後按一下確定。



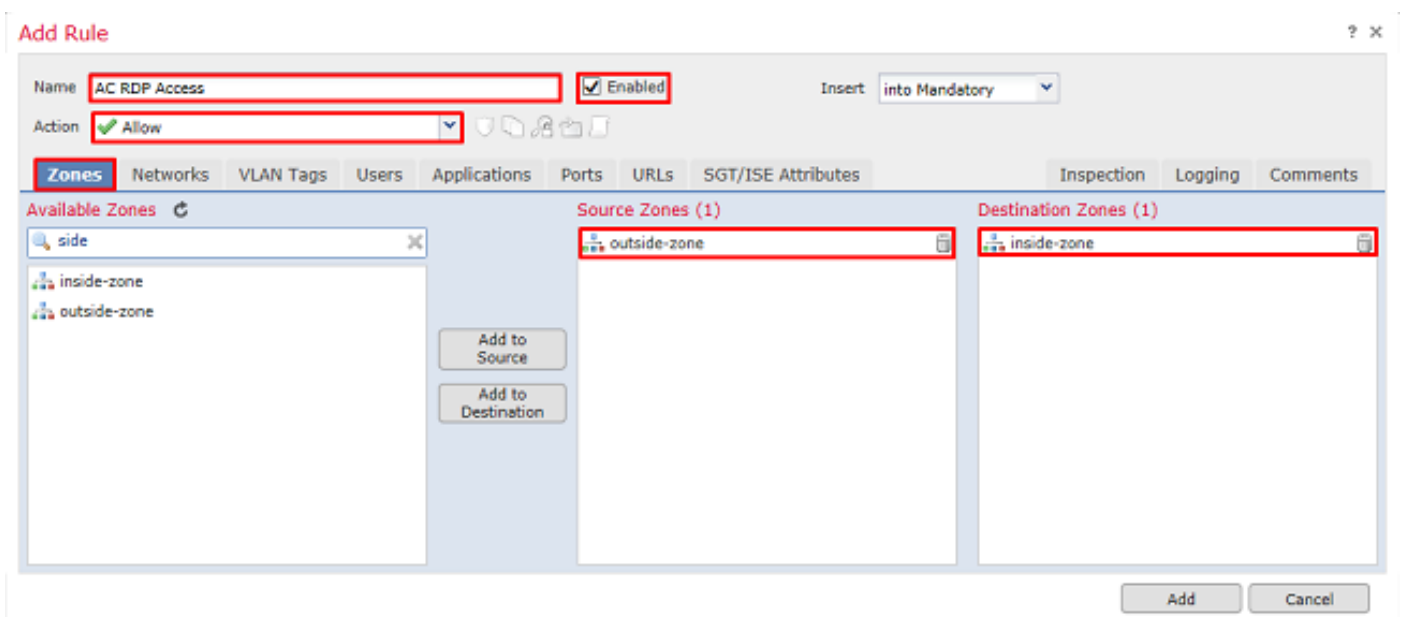
8. 按一下Add Rule以建立新的ACP規則。這些步驟建立規則以允許AnyConnect Admins組中的使用者使用RDP連線到內部網路中的裝置。



指定規則的名稱。確保規則已啟用並具有相應的操作。

在**Zones**頁籤下，為相關流量指定適當的區域。

使用者所起始的RDP流量會進入源自外部區域介面的FTD，然後輸出內部區域。



在**Networks**下，定義源網路和目標網路。

對象AnyConnect_Pool包括分配給AnyConnect客戶端的IP地址。

對象Inside_Net包括內部網路子網。

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

Source Networks (1)

Source	Original Client
AnyConnect_Pool	

Destination Networks (1)

Inside_Net

Enter an IP address Add Add

Add Cancel

在Users下，按一下Available Realms下之前建立的領域，在Available Users下按一下相應的組/使用者，然後按一下Add to Rule。

如果Available Users部分下沒有可用的使用者或組，請確保FMC能夠下載realm部分下的Users和Groups，並且包含適當的Groups/User。

從源角度檢查此處指定的使用者/組。

例如，根據此規則到目前為止所定義的內容，FTD會評估以下情況：流量來源為外部區域，且目的地為內部區域，來源為AnyConnect_Pools對象中的網路，且目的地為Inside_Net對象中的網路，而流量來源為AnyConnect Admins組中的使用者。

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

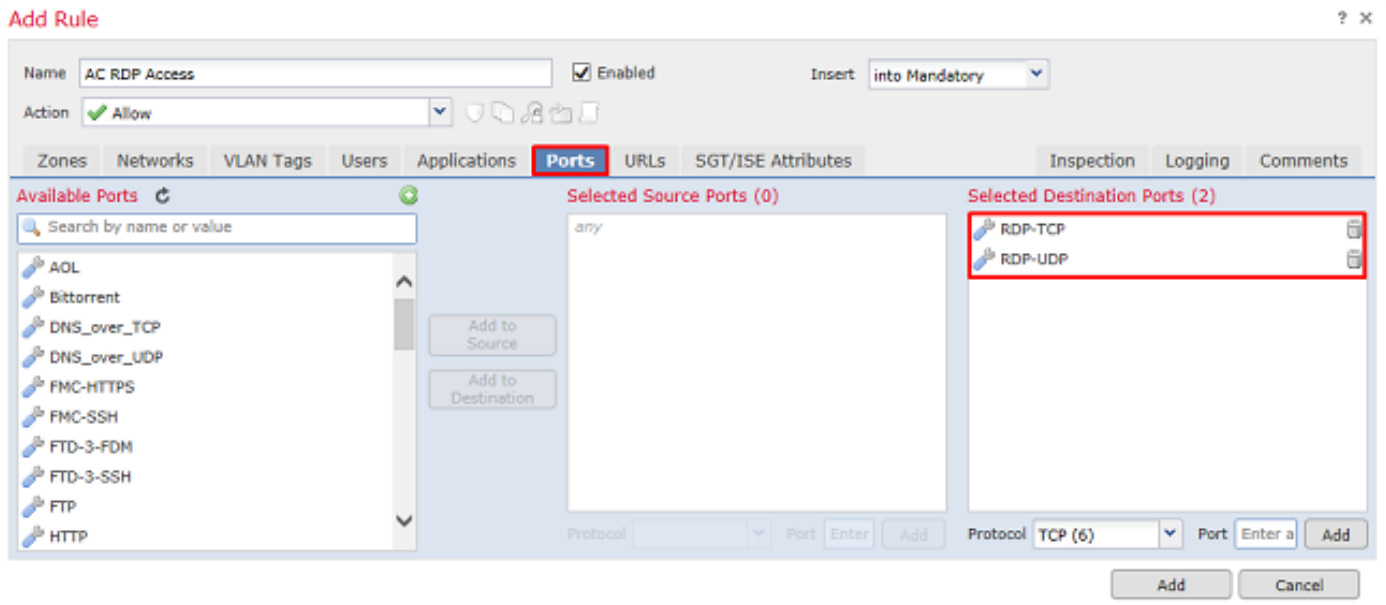
Selected Users (1)

LAB-AD/AnyConnect Admins

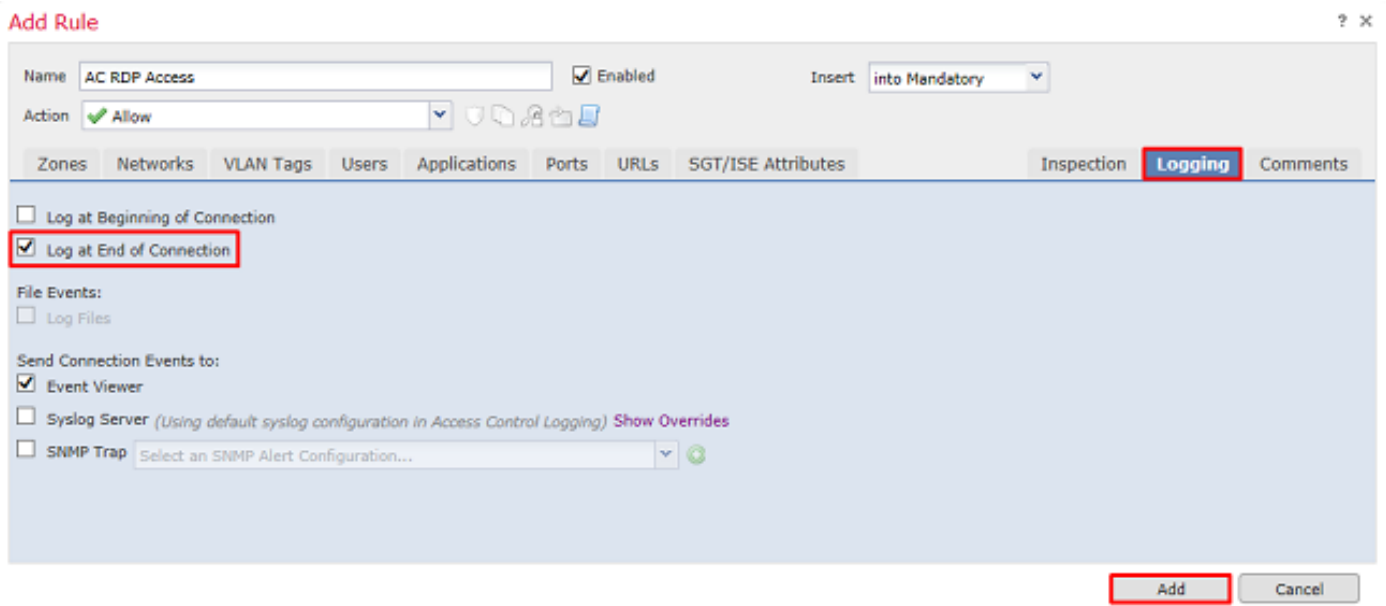
Add to Rule

Add Cancel

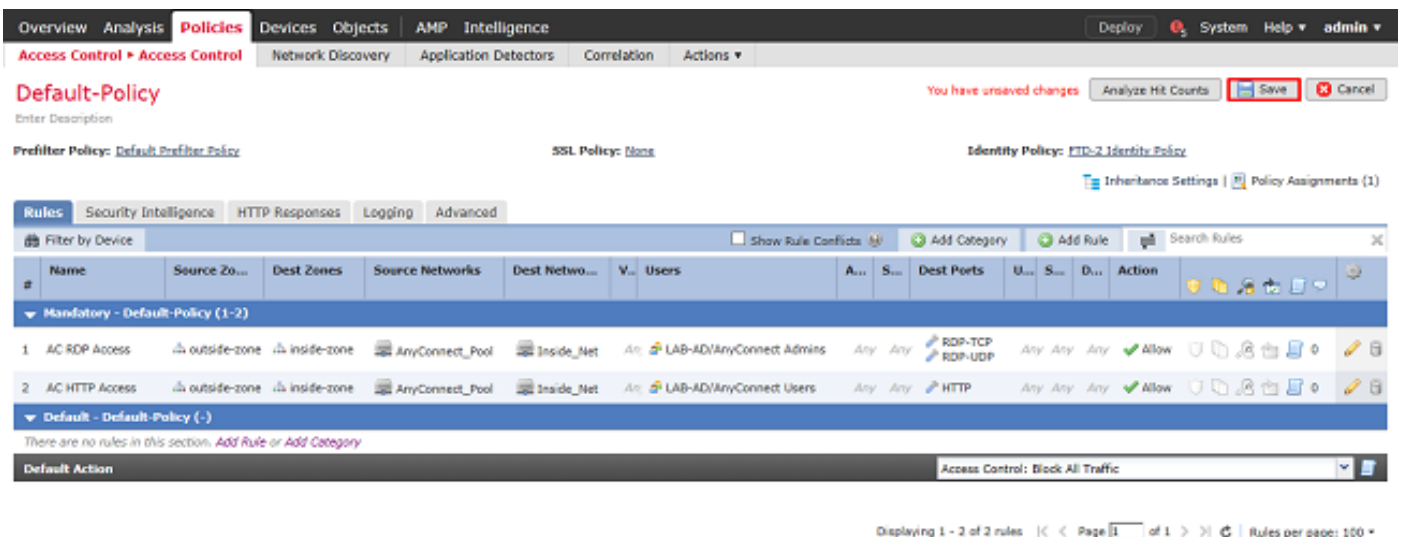
在Ports下，建立並新增自定義RDP對象以允許TCP和UDP埠3389。請注意，本可以在Applications部分下新增RDP，但為簡單起見，只檢查埠。



最後，在Logging下，稍後會檢查Log at End of Connection以進行其他驗證。完成後按一下Add。



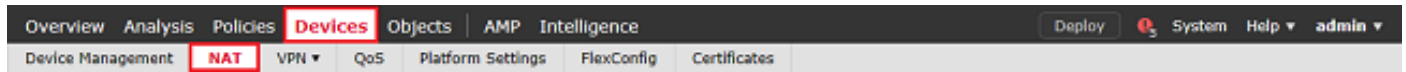
9.為HTTP訪問建立了一個附加規則，以允許組AnyConnect User中的用戶訪問Windows Server IIS網站。按一下「Save」。



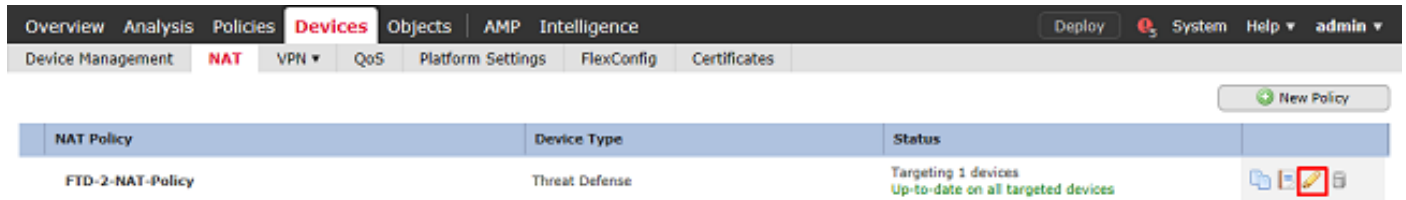
配置NAT免除

如果存在影響AnyConnect流量的NAT規則（如網際網路PAT規則），則必須配置NAT免除規則，以使AnyConnect流量不會受NAT影響。

1. 導航到Devices > NAT。

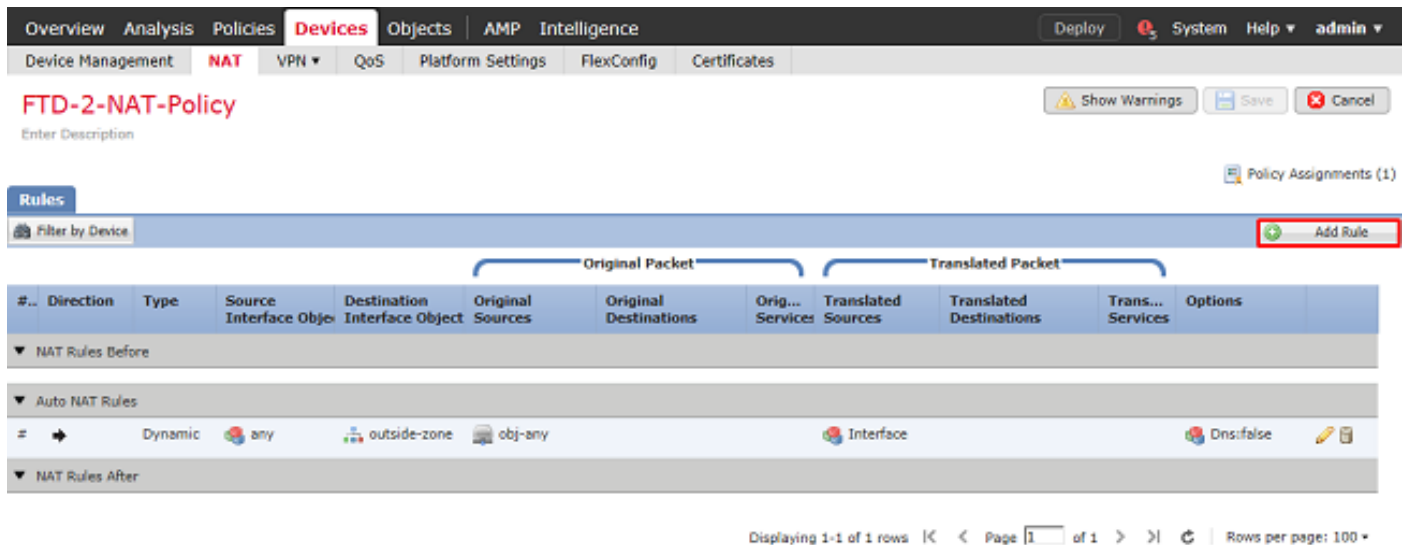


選擇應用於FTD的NAT策略。



2. 在該NAT策略中，終端有一個動態PAT，該PAT會影響從外部介面到外部介面的所有流量（包括AnyConnect流量）。

要防止AnyConnect流量受NAT影響，請按一下右上角的Add Rule。



3. 配置NAT免除規則，確保該規則是型別為Static的手動NAT規則。這是適用於AnyConnect流量的雙向NAT規則。

透過這些設定，當FTD偵測來源為Inside_Net且目的地為AnyConnect IP位址（由AnyConnect_Pool定義）的流量時，來源會轉換為相同的值(Inside_Net)，而目的地會在流量進入inside_zone且離開outside_zone時轉換為相同的值(AnyConnect_Pool)。在滿足這些條件時，這基本上會繞過NAT。

Add NAT Rule ? x

NAT Rule: **Manual NAT Rule** Insert: In Category NAT Rules Before

Type: **Static** Enable

Description:

Interface Objects Translation PAT Pool Advanced

Available Interface Objects

Source Interface Objects (1) **inside-zone**

Destination Interface Objects (1) **outside-zone**

OK Cancel

Add NAT Rule ? x

NAT Rule: Manual NAT Rule Insert: In Category NAT Rules Before

Type: Static Enable

Description:

Interface Objects **Translation** PAT Pool Advanced

Original Packet

Original Source:* **Inside_Net**

Original Destination: Address

Original Source Port:

Original Destination Port:

Translated Packet

Translated Source: Address **Inside_Net**

Translated Destination: **AnyConnect_Pool**

Translated Source Port:

Translated Destination Port:

OK Cancel

此外，FTD設定為對此流量執行路由查詢，而不是代理ARP。完成後按一下OK。

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. 按一下**Save**。

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

Device Management **NAT** VPN QoS Platform Settings FlexConfig Certificates You have unsaved changes Show Warnings Cancel

FTD-2-NAT-Policy Enter Description Policy Assignments (1)

Rules Add Rule

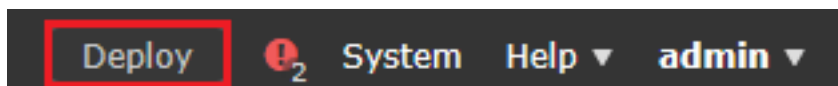
Filter by Device

#	Direction	Type	Original Packet		Translated Packet		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								

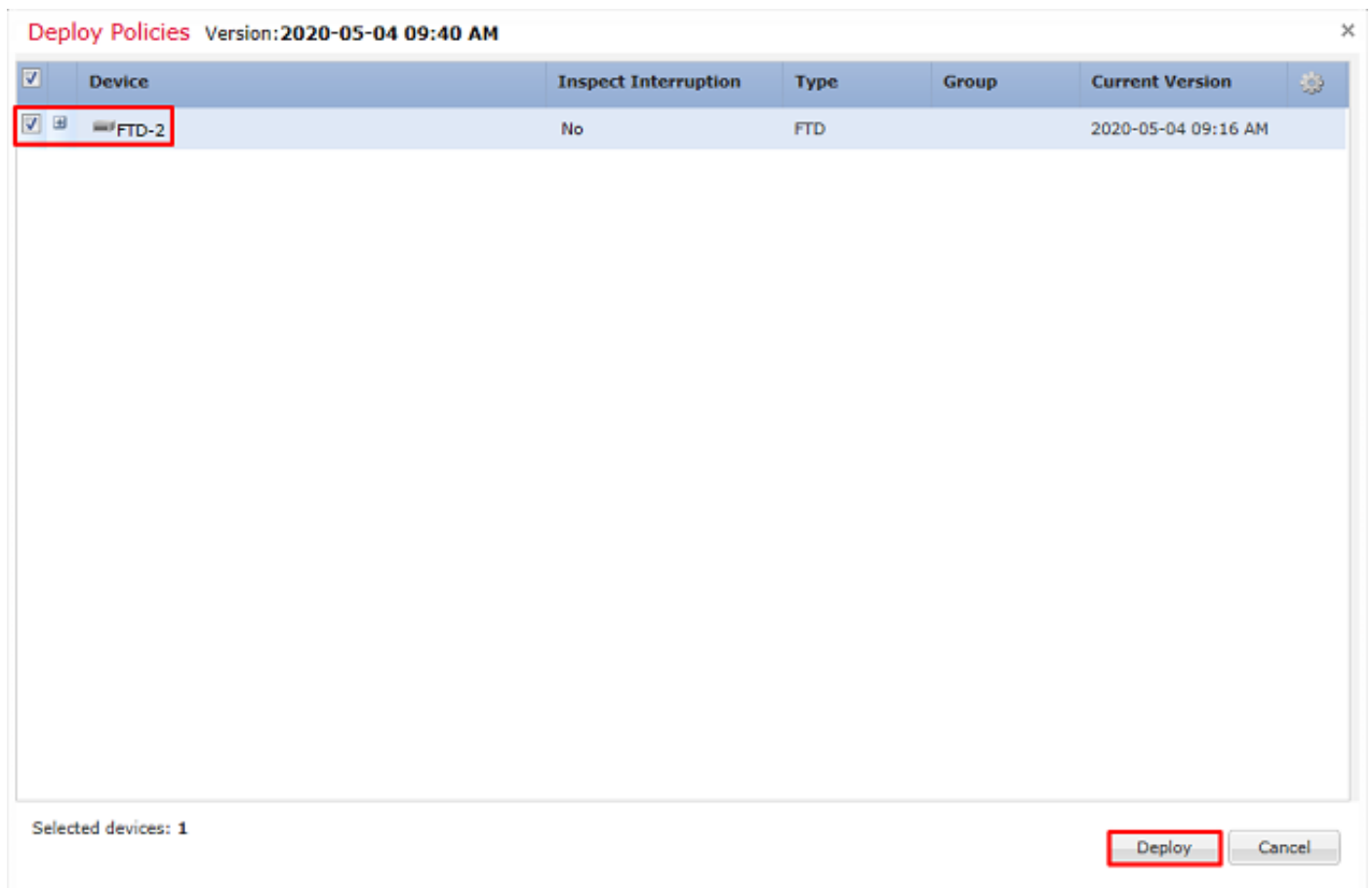
Displaying 1-2 of 2 rows Page 1 of 1 Rows per page: 100

部署

1. 配置完成後，按一下右上角的**Deploy**按鈕。



2. 按一下FTD旁的覈取方塊，然後按一下「**Deploy**」。



驗證

最終配置

AAA組態

```
> 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
```

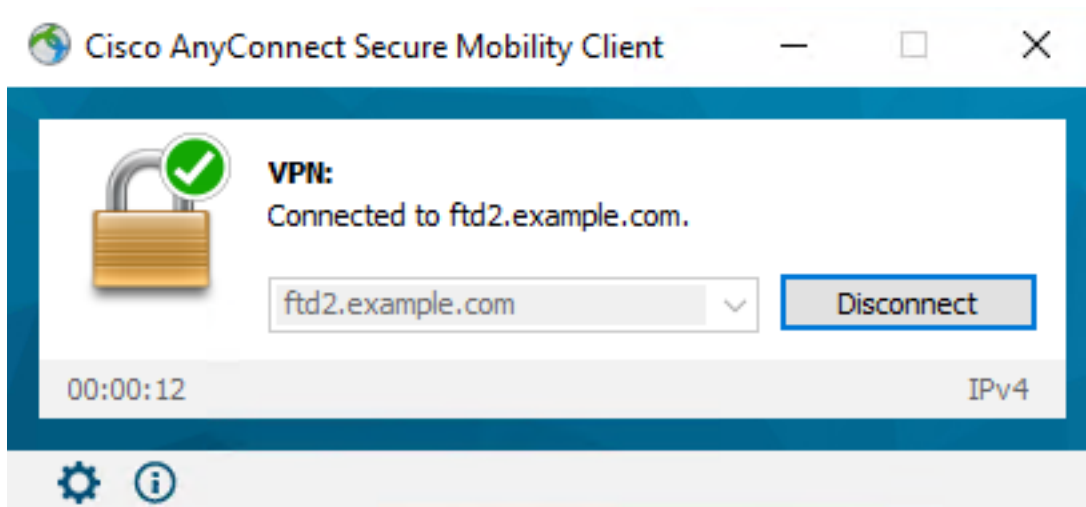
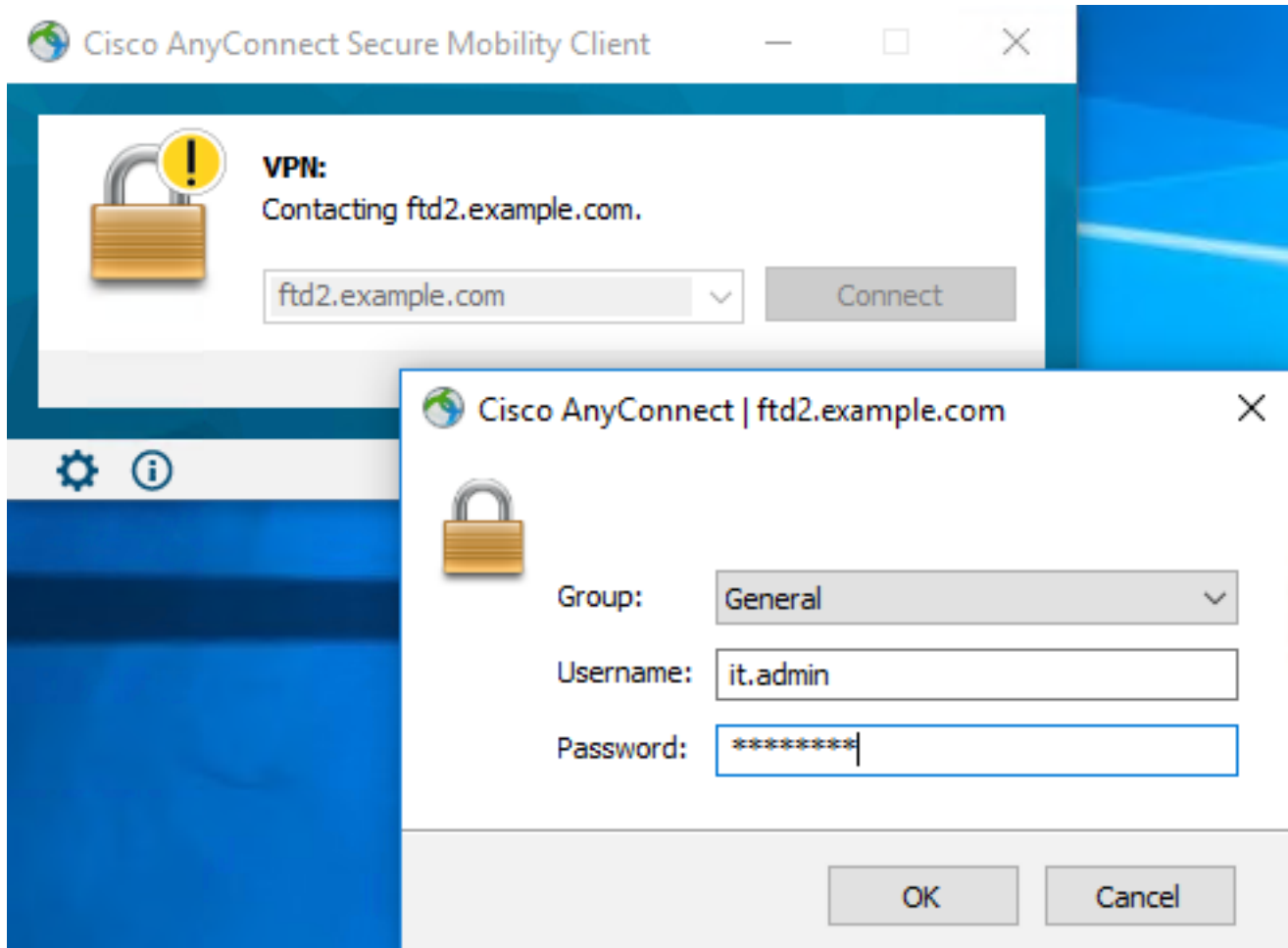
```
anyconnect enable
tunnel-group-list enable
cache
  no disable
error-recovery disable

> 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

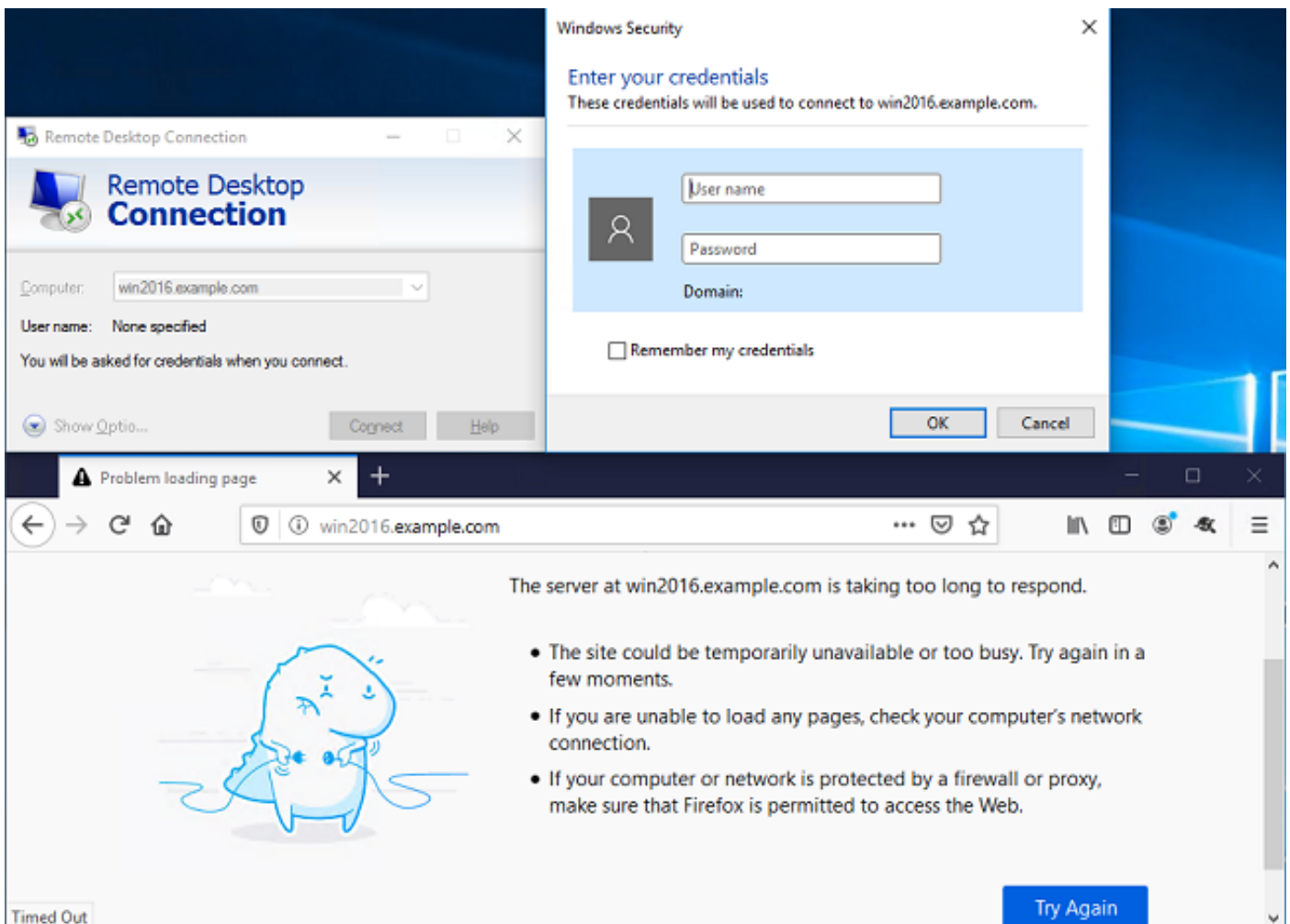
> show running-config ssl
ssl trust-point FTD-2-SelfSigned outside
```

使用AnyConnect連線並驗證訪問控制策略規則

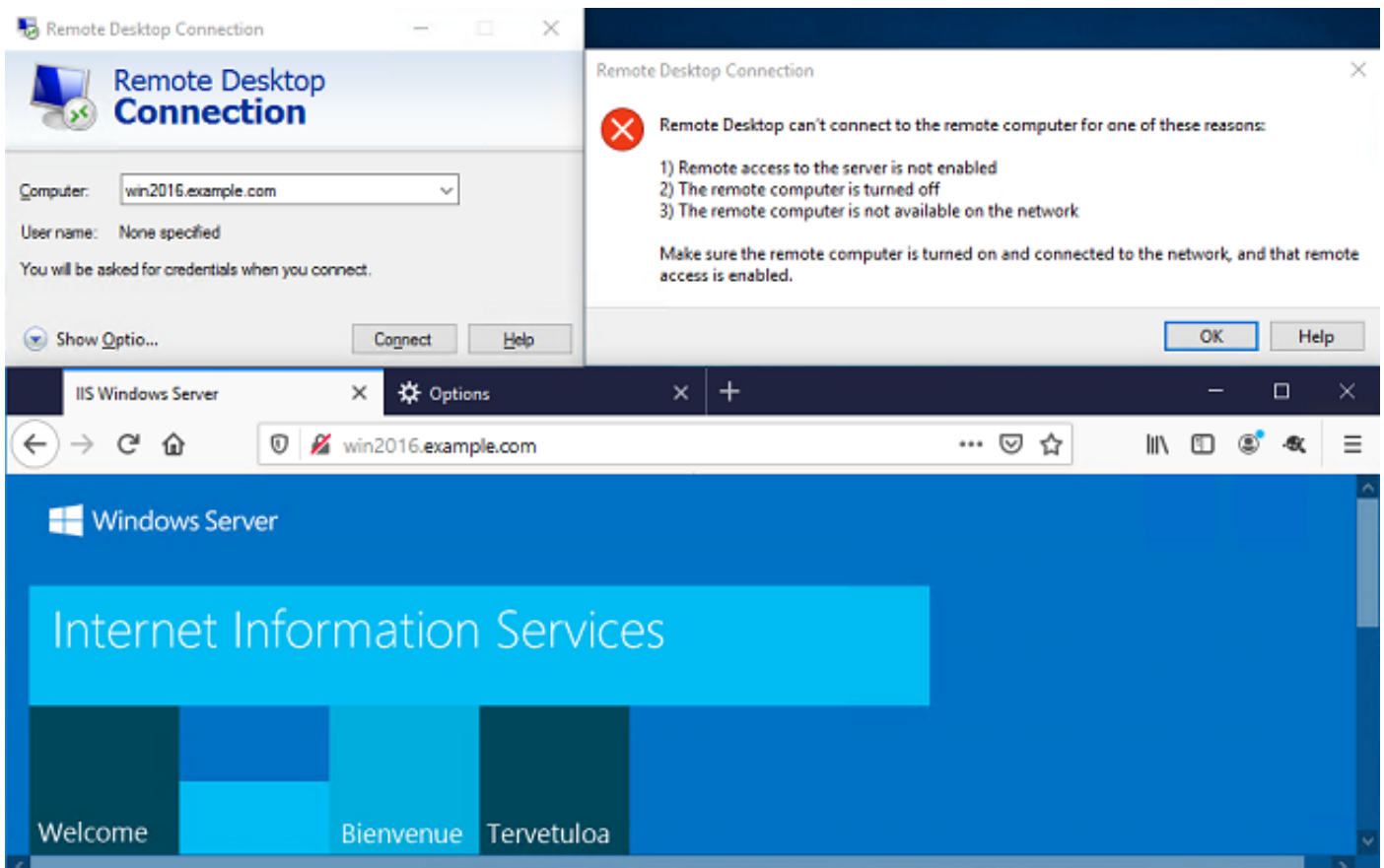


使用者IT Admin位於對Windows Server具有RDP訪問許可權的AnyConnect Admins組中，但是沒有對HTTP的訪問許可權。

開啟與此伺服器的RDP和Firefox會話將驗證此使用者只能通過RDP訪問伺服器。



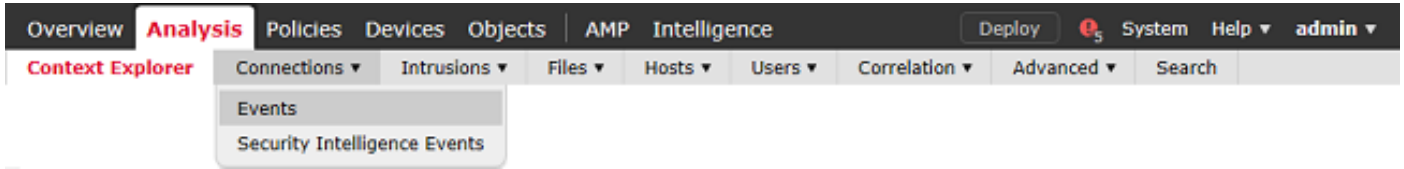
如果使用AnyConnect使用者組（作為HTTP訪問但不是RDP訪問）中的使用者測試使用者登入，我們可以驗證訪問控制策略規則是否生效。



使用FMC連線事件進行驗證

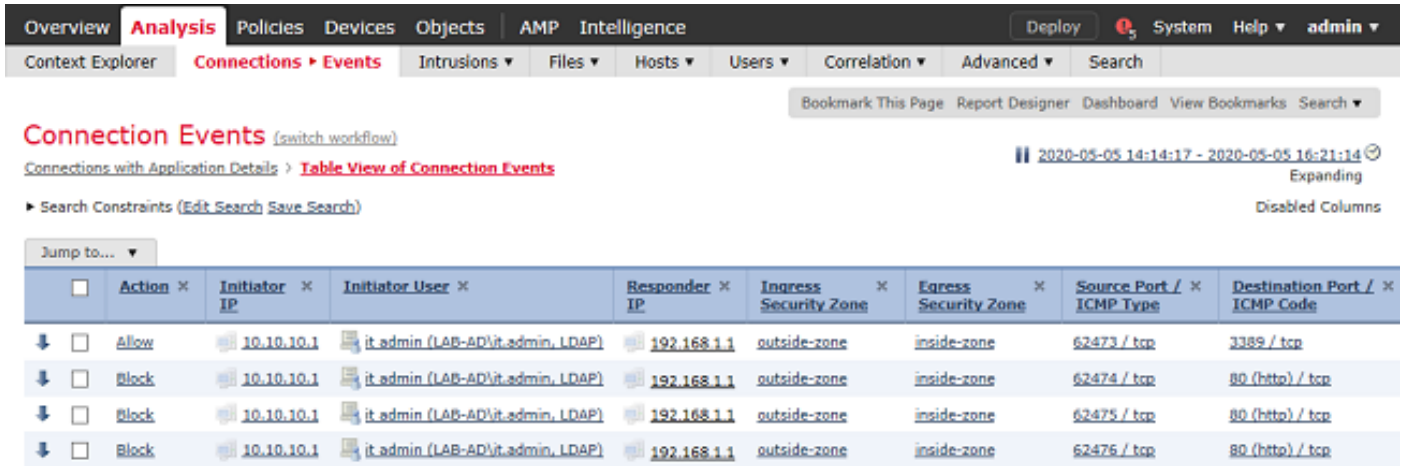
由於在訪問控制策略規則中啟用了日誌記錄，因此可以檢查連線事件中是否存在與這些規則匹配的任何流量

導航到分析>連線>事件。

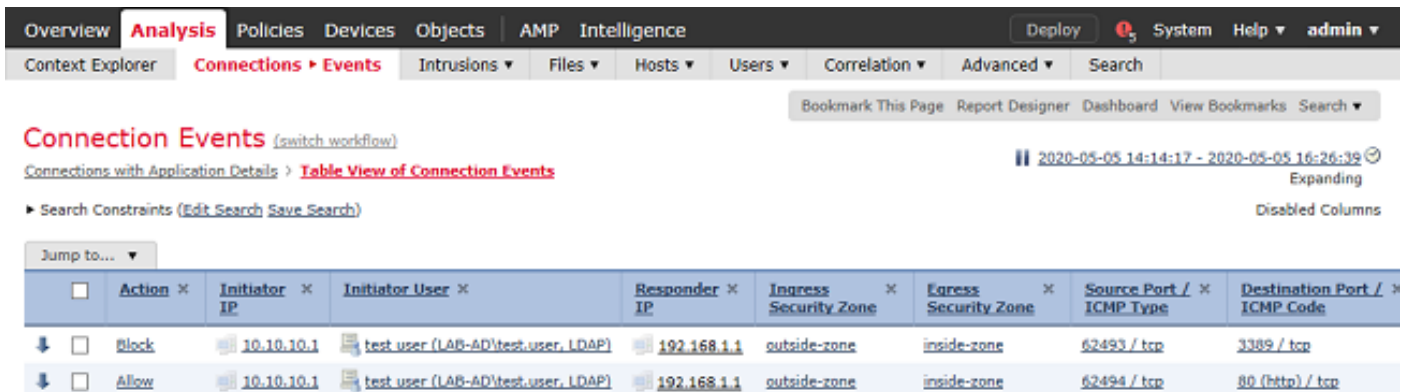


在Table View of Connection Events下，日誌被過濾為僅顯示IT管理員的連線事件。

在這裡，您可以驗證到伺服器的RDP流量（TCP和UDP 3389）是否被允許，但是埠80流量被阻止。



對於使用者測試使用者，可以驗證到伺服器的RDP流量是否被阻止，以及埠80流量是否被允許。



疑難排解

調試

此調試可以在診斷CLI中運行，以對LDAP身份驗證相關問題進行故障排除：`debug ldap 255`

要排除使用者身份訪問控制策略問題，可以私下運行`system support firewall-engine-debug`以確定流量被允許或意外阻止的原因。

正在運行的LDAP調試

```
[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
```

無法與LDAP伺服器建立連線

```
[-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
```

潛在解決方案：

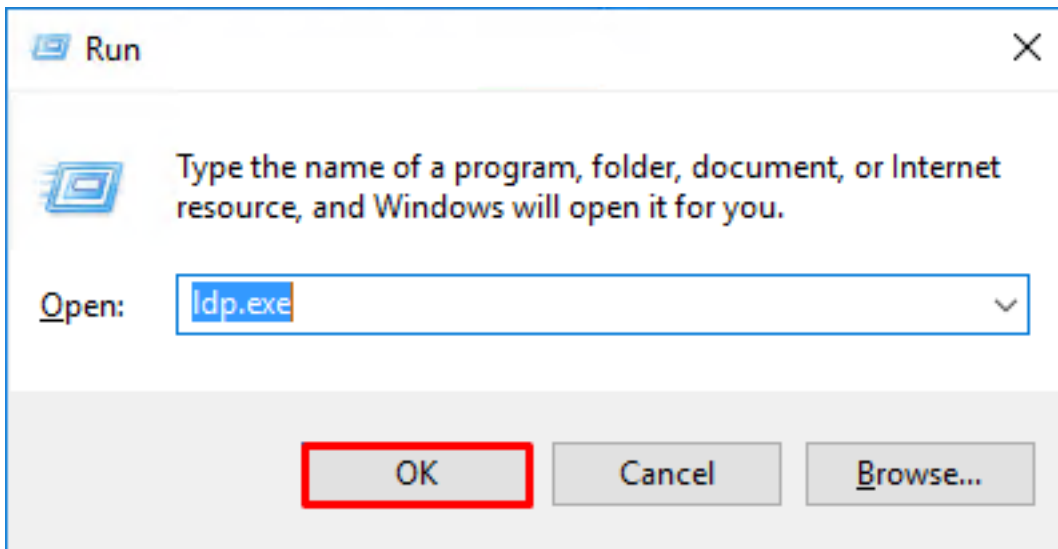
- 檢查路由並確保FTD收到來自LDAP伺服器的響應。
- 如果使用LDAPS或STARTTLS，請確保信任的根CA證書正確無誤，以成功完成SSL握手。
- 驗證使用了正確的IP地址和埠。如果使用主機名，請確認DNS能夠將其解析為正確的IP地址。

繫結登入DN和/或密碼不正確

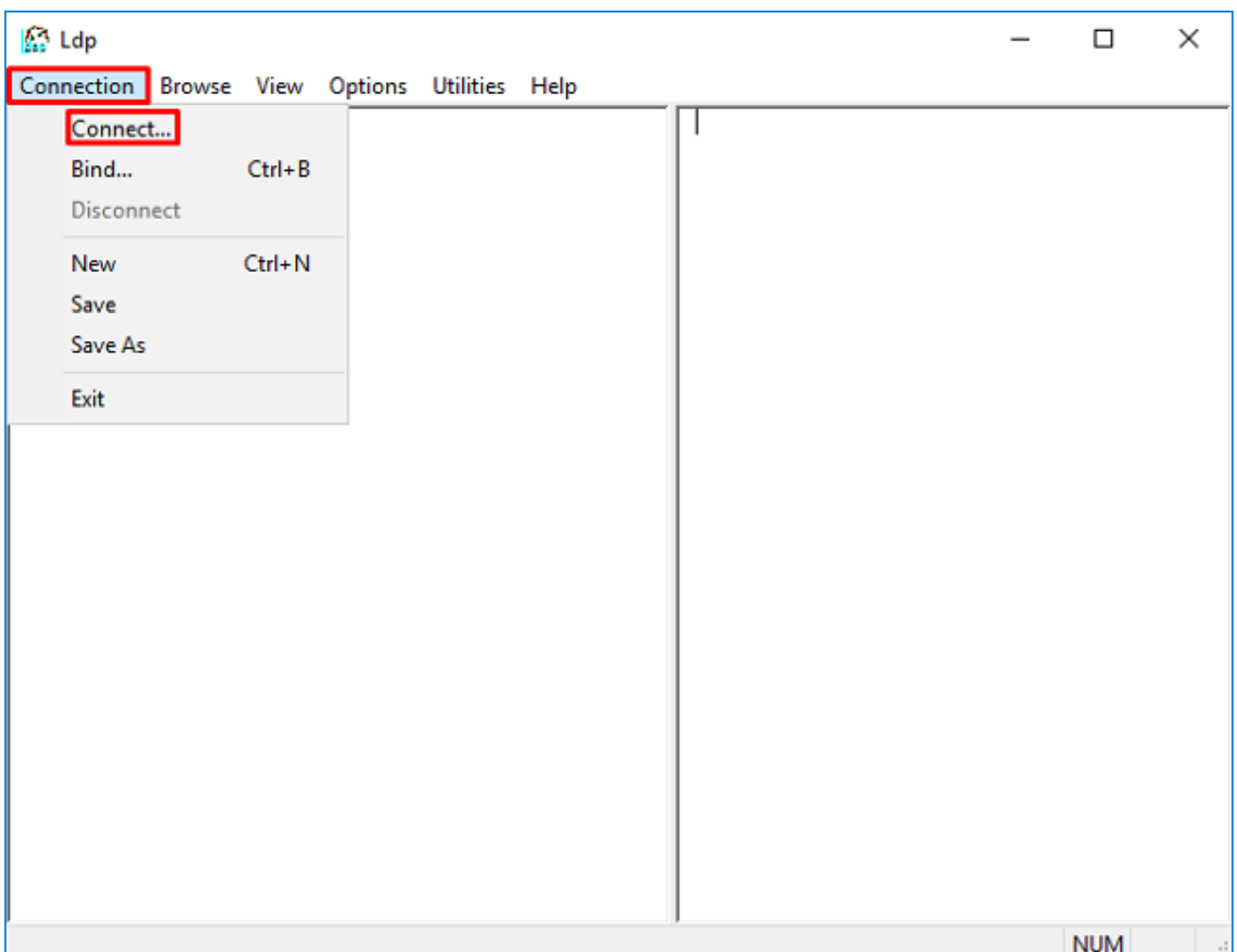
```
[-2147483615] Session Start
[-2147483615] New request Session, context 0x00007f9e65ccdc40, reqType = Authentication
[-2147483615] Fiber started
[-2147483615] Creating LDAP context with uri=ldap://192.168.1.1:389
[-2147483615] Connect to LDAP server: ldap://192.168.1.1:389, status = Successful
[-2147483615]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

潛在解決方案：驗證登入DN和登入密碼是否正確配置。這可以在使用ldp.exe的AD伺服器上驗證。要驗證帳戶是否可以使用ldp成功繫結，請完成以下步驟：

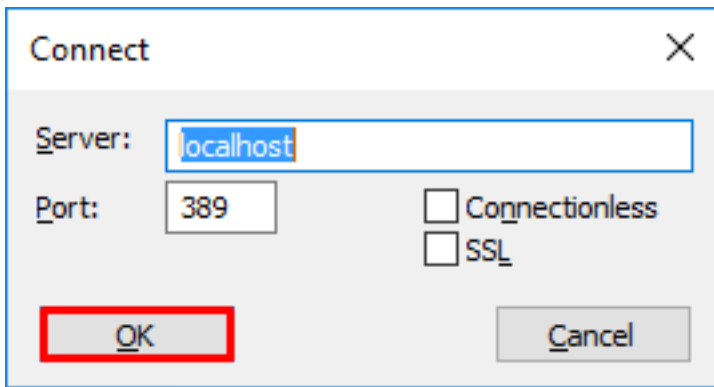
1. 在AD伺服器上，按Win+R並搜尋ldp.exe



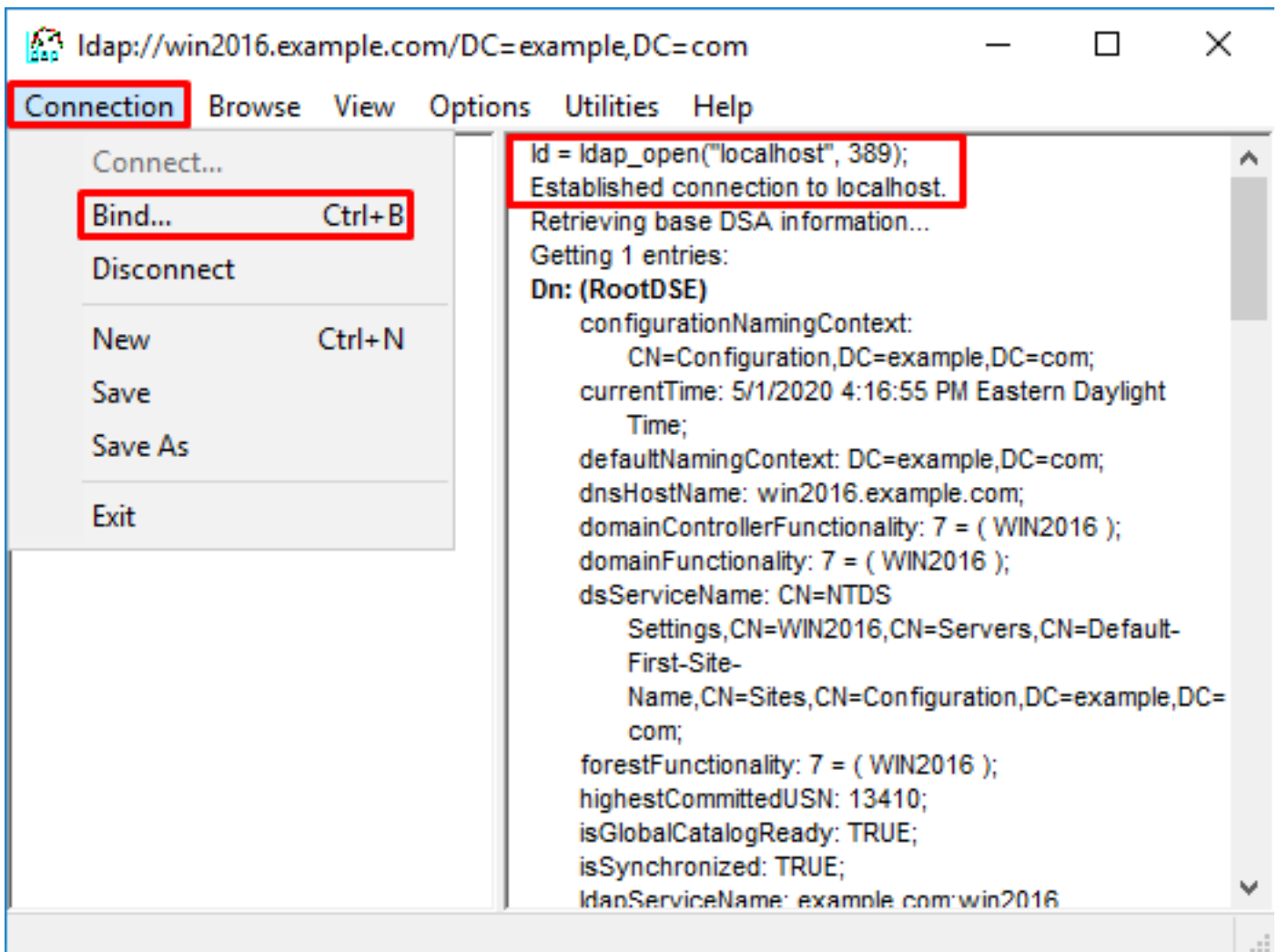
2. 在Connection下，選擇Connect...



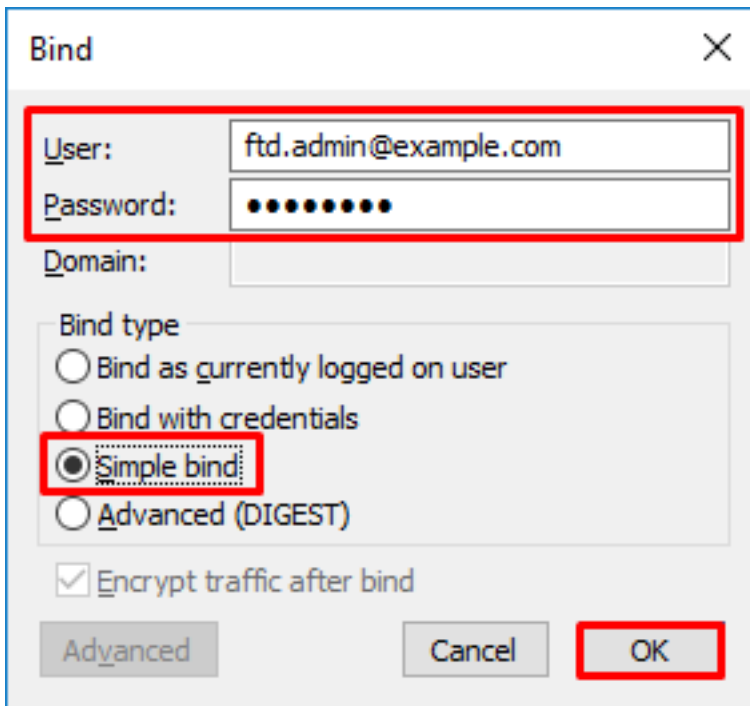
3. 指定伺服器的本地主機和相應的埠，然後按一下**確定**。



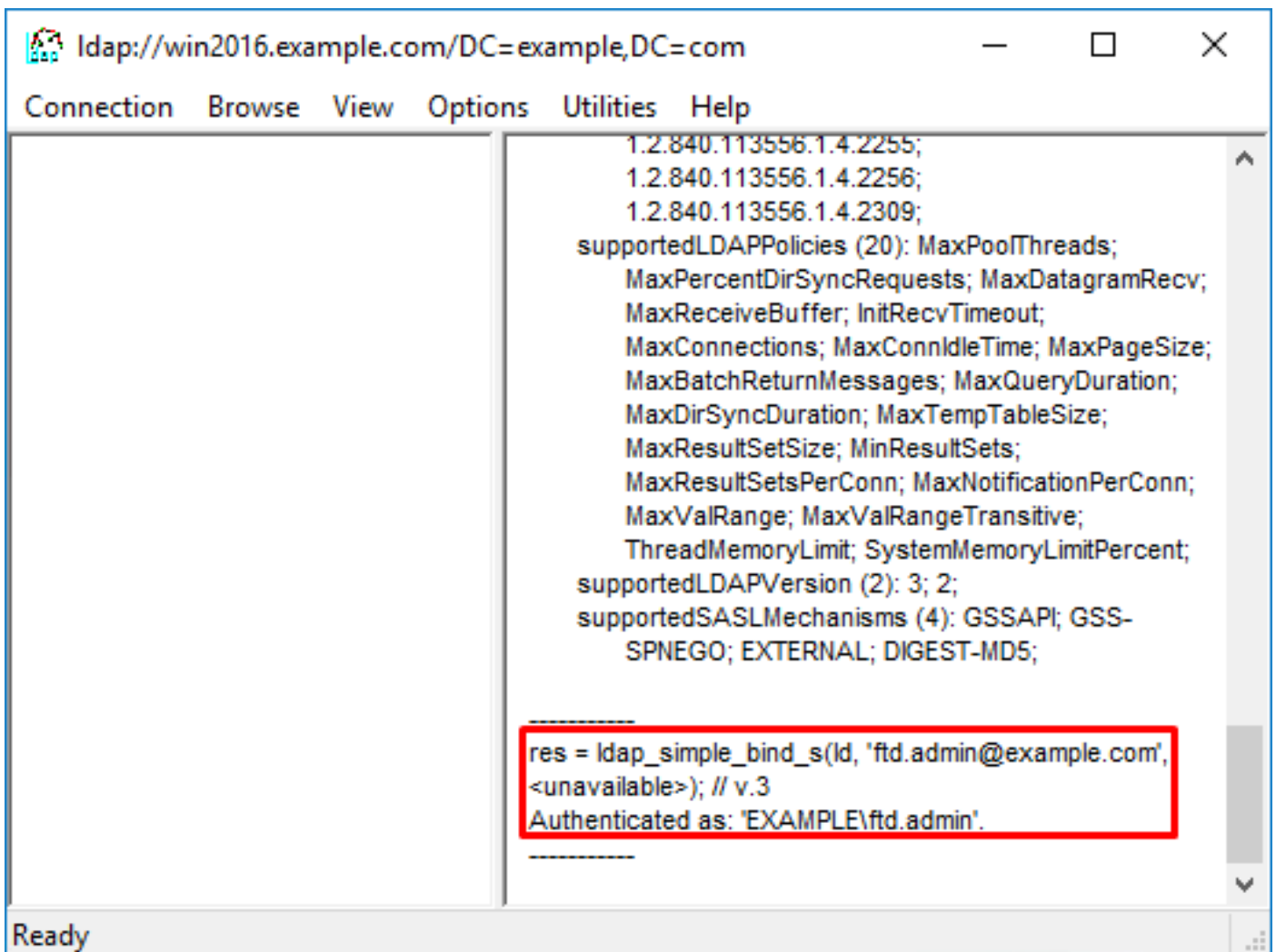
4. 「右」列顯示指示連線成功的文本。導航到**Connection > Bind...**



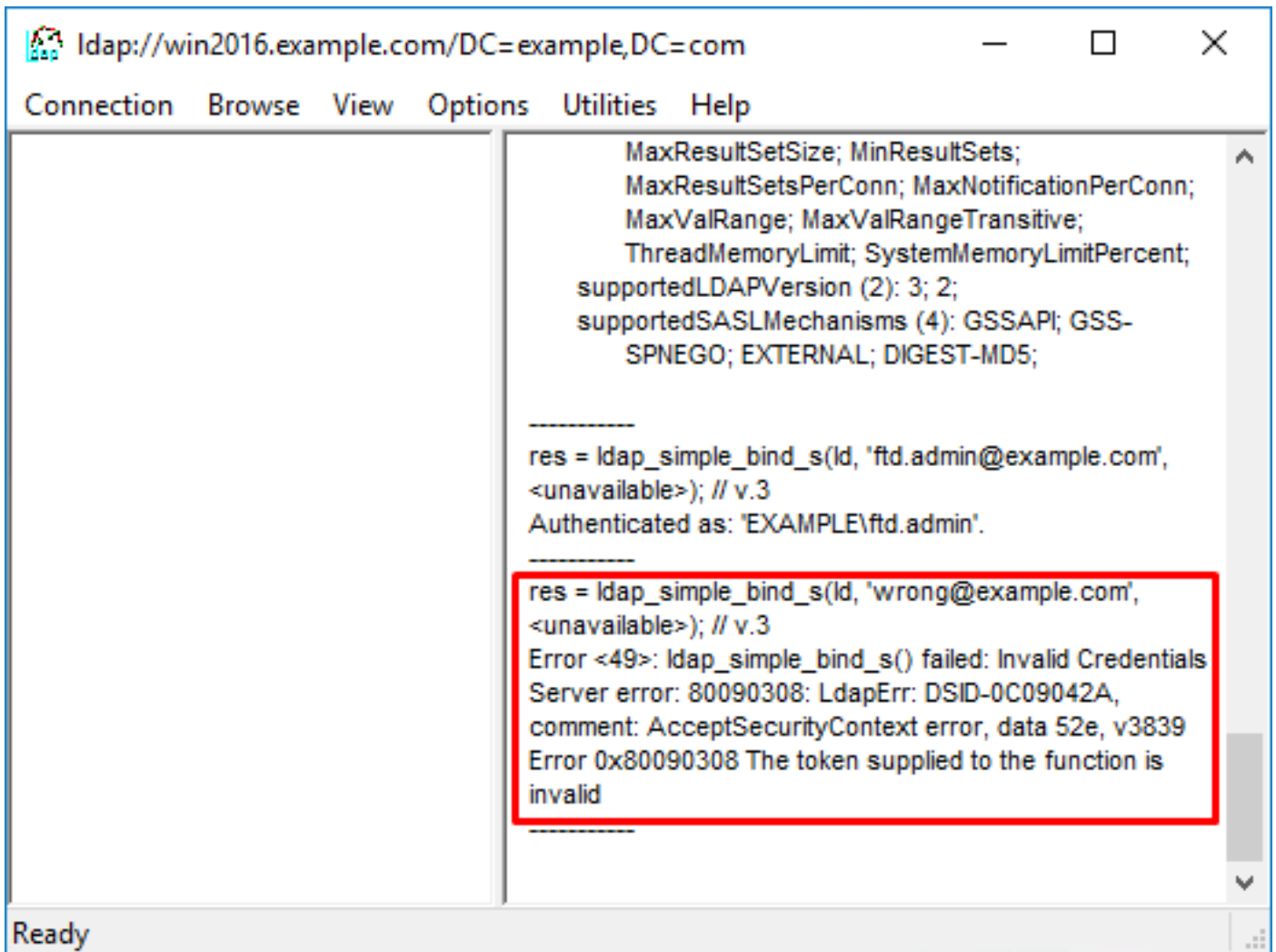
5.選擇Simple Bind，然後指定Directory Account Username和Password。按一下「OK」（確定）。



如果繫結成功，則ldp顯示驗證為：DOMAIN\username



嘗試使用無效的使用者名稱或密碼進行繫結會導致失敗，如此處所示的兩個錯誤。

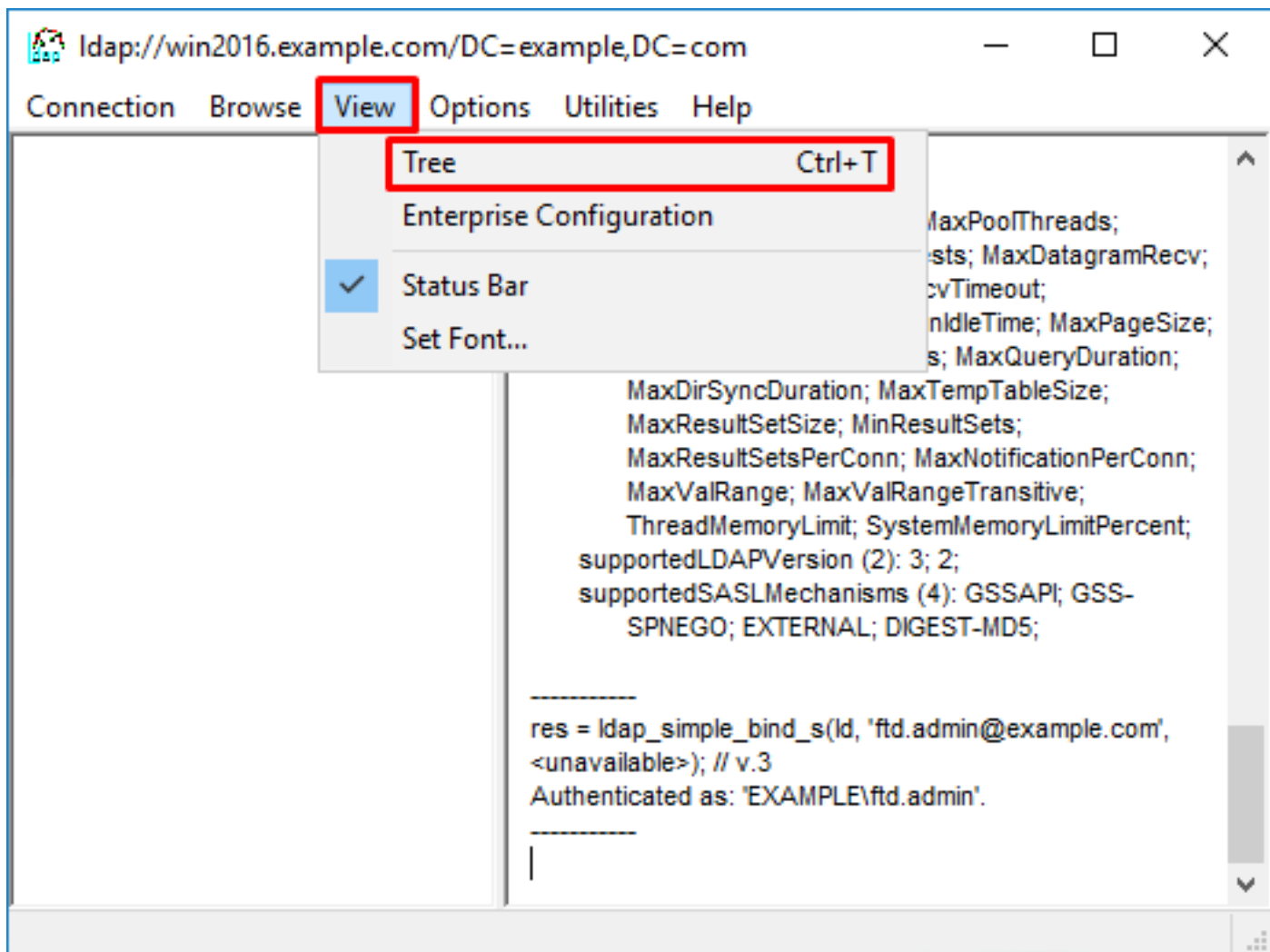


LDAP伺服器找不到使用者名稱

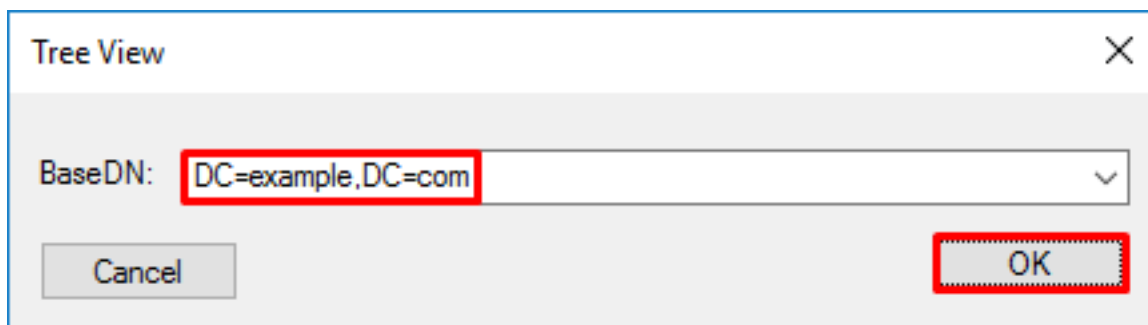
```
[ -2147483612] Session Start
[ -2147483612] New request Session, context 0x00007f9e65ccdc40, reqType = Authentication
[ -2147483612] Fiber started
[ -2147483612] Creating LDAP context with uri=ldap://192.168.1.1:389
[ -2147483612] Connect to LDAP server: ldap://192.168.1.1:389, status = Successful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

潛在解決方案：驗證AD能否使用FTD完成的搜尋找到使用者。這也可使用ldp.exe完成。

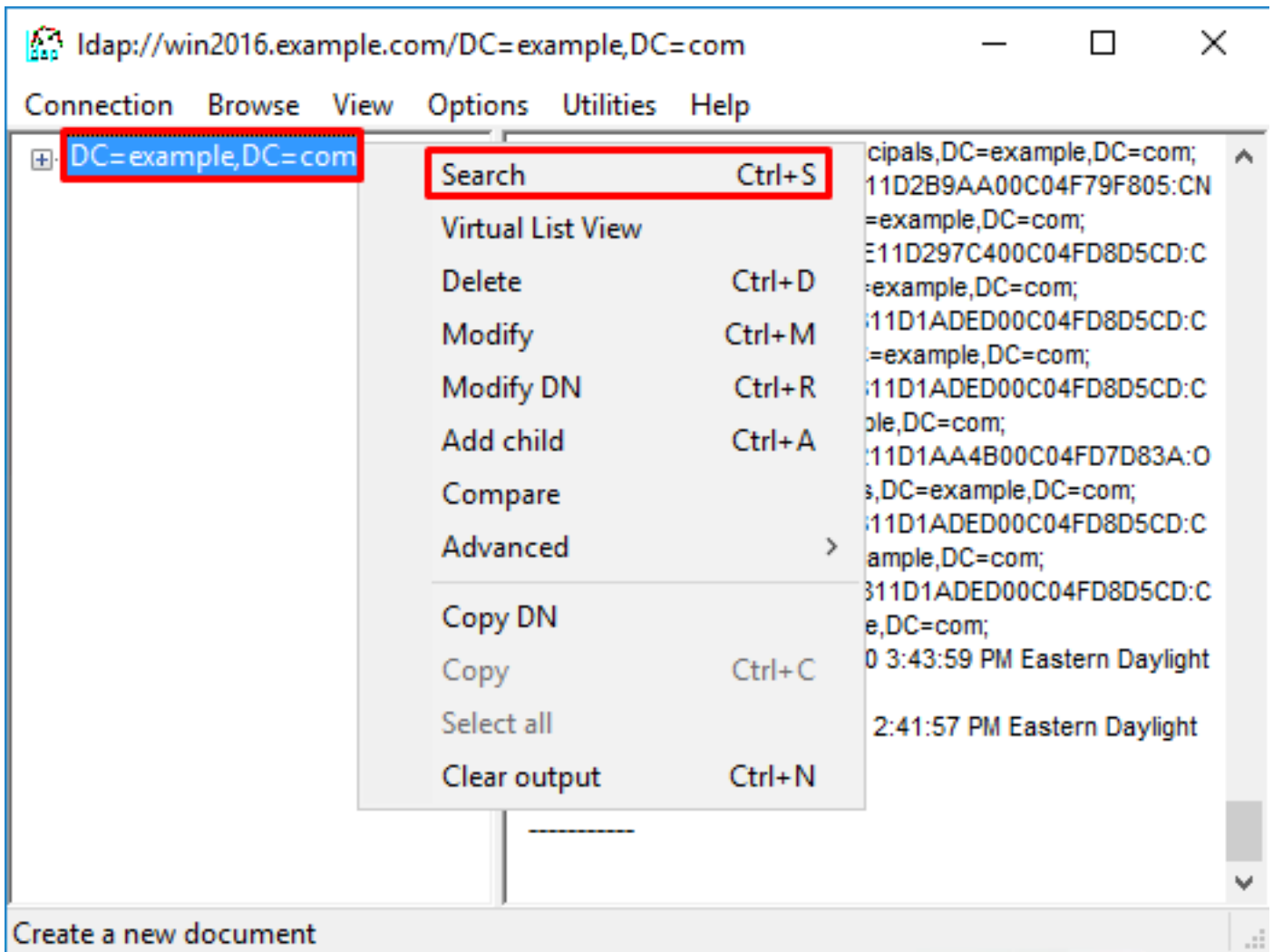
1.成功繫結後（如上所示），導航到檢視>樹。



2. 指定在FTD上設定的基本DN，然後按一下「OK」



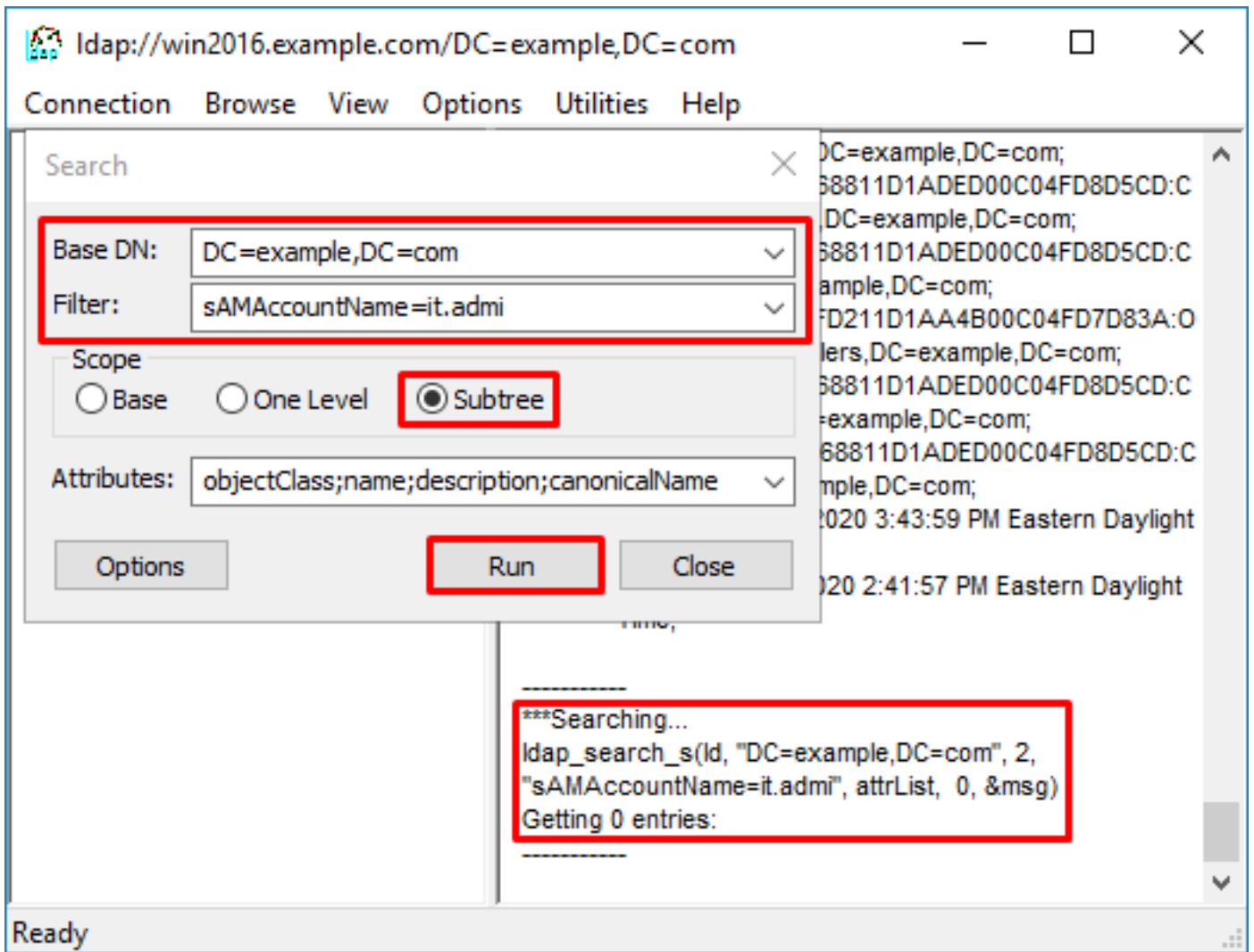
3. 按一下右鍵基本DN，然後按一下Search。



4. 指定與debug中相同的Base DB、Filter和Scope值。

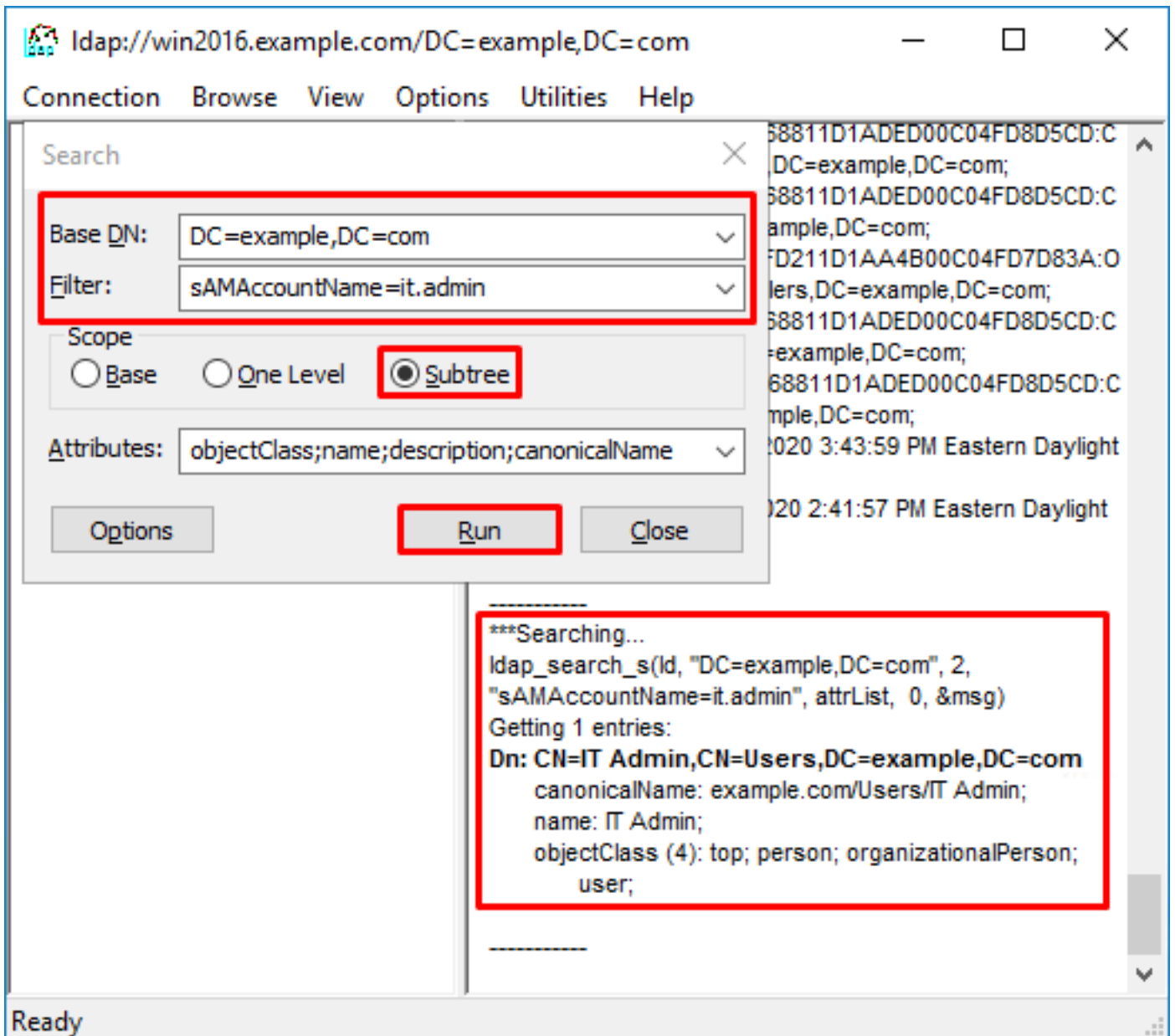
在此範例中，這些如下：

- 基本DN:dc=example , dc=com
- 篩選器 : samaccountname=it.admi
- 範圍 : 子樹



ldap發現0個條目，因為在Base DN dc=example，dc=com下沒有具有samaccountname **it.admi**的使用者帳戶

使用正確的samaccountname **it.admin**的另一嘗試顯示不同的結果。ldap在Base DN dc=example，dc=com下找到1個條目，並列印該使用者DN。



使用者名稱密碼不正確

```

[-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
```

潛在解決方案：驗證使用者密碼是否正確配置且未過期。與登入DN類似，FTD會使用使用者憑證與AD進行繫結。

此繫結也可以在ldp中完成，以驗證AD是否能夠識別相同的使用者名稱和密碼憑據。ldp中的步驟顯示在繫結登入DN和/或密碼不正確一節中。

此外，還可以檢視Microsoft伺服器事件檢視器日誌，以瞭解可能的原因。

測試AAA

test aaa-server命令可用於使用特定使用者名稱和密碼來模擬從FTD進行的身份驗證嘗試。這可用於測試連線或身份驗證失敗。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
```

封包擷取

封包擷取可用於驗證與AD伺服器的連線能力。如果LDAP封包離開FTD，但沒有回應，這可能表示路由問題。

Capture顯示雙向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

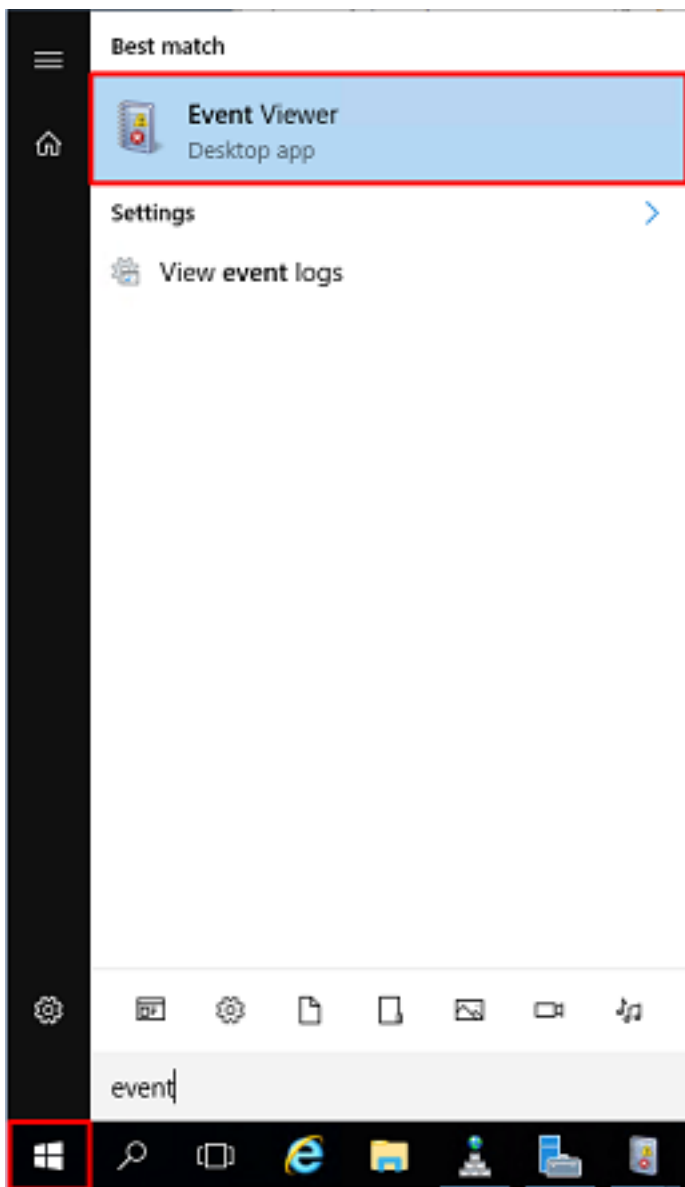
54 packets captured

  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
```

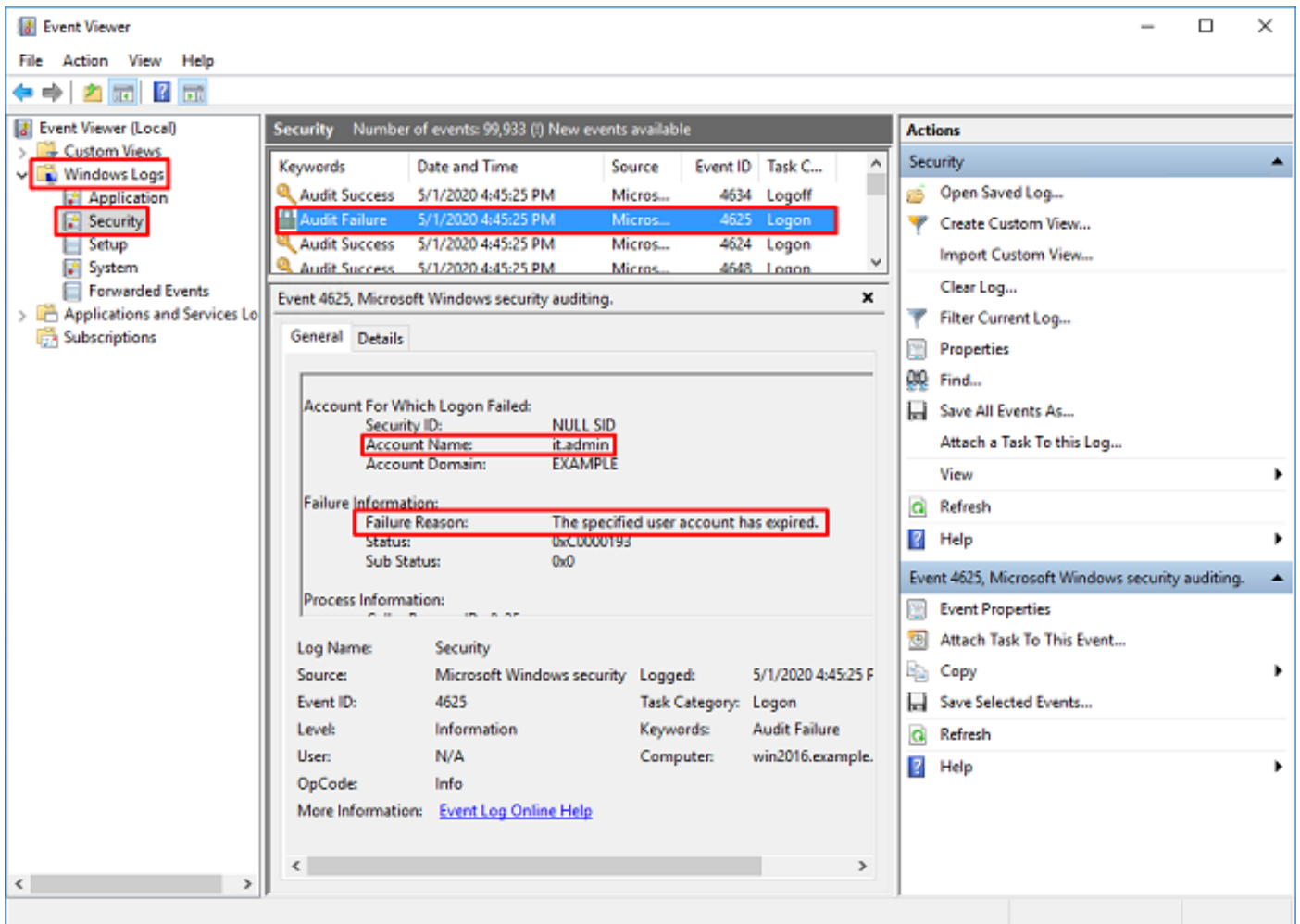
Windows Server事件檢視器日誌

AD伺服器上的事件檢視器日誌可以提供有關失敗原因的更詳細資訊。

1. 搜尋並開啟「事件查看器」。



2.展開Windows Logs，然後按一下Security。使用使用者帳戶名稱搜尋稽核失敗並檢視失敗資訊。



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

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。