

在FDM管理的FTD上為AnyConnect客戶端配置AD(LDAP)身份驗證和使用者身份

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[設定](#)

[網路圖表和案例](#)

[AD配置](#)

[確定LDAP基本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 \(僅對於LDAPS或STARTTLS是必需的 \)](#)

[FDM配置](#)

[驗證許可](#)

[設定AD身份源](#)

[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](#)

[驗證](#)

[最終配置](#)

[使用AnyConnect連線並驗證訪問控制策略規則](#)

[疑難排解](#)

[調試](#)

[工作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

本文旨在詳細說明如何為連線到由Firepower裝置管理(FDM)管理的Cisco Firepower威脅防禦(FTD)的AnyConnect客戶端配置Active Directory(AD)身份驗證。使用者身份將用於訪問策略，以將AnyConnect使用者限制為特定IP地址和埠。

必要條件

需求

思科建議您瞭解以下主題：

- FDM上RA VPN配置的基本知識
- 有關FDM上的LDAP伺服器配置的基本知識
- 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
- 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。

設定

網路圖表和案例



Windows伺服器已預配置Internet資訊服務(IIS)和遠端案頭協定(RDP)，以便測試使用者身份。在此配置指南中，將建立三個使用者帳戶和兩個組。

使用者帳戶：

- FTD管理員：這將用作目錄帳戶，以允許FTD繫結到AD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。

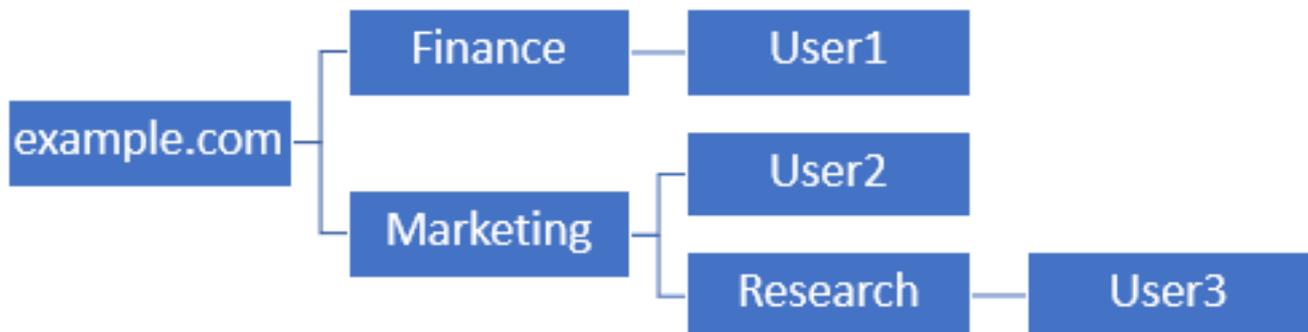
組：

- AnyConnect管理員：IT管理員將新增到以演示使用者身份的測試組。此組將僅具有對Windows Server的RDP訪問許可權
- AnyConnect使用者：測試使用者將新增到的一個測試組，用於演示使用者身份。此組將僅具有對Windows Server的HTTP訪問許可權

AD配置

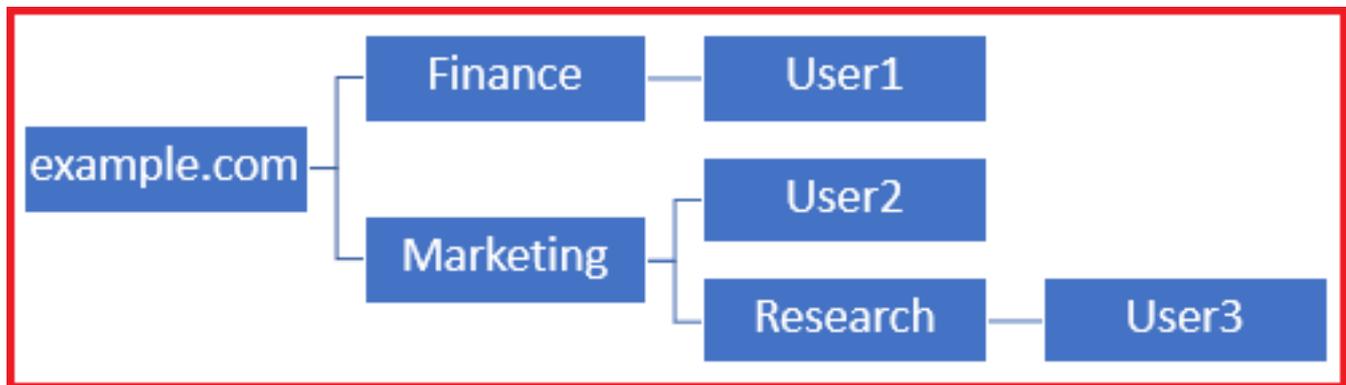
若要在FTD上正確設定AD驗證和使用者身分，需要幾個值。在FDM上完成配置之前，必須在Microsoft Server上建立或收集所有這些詳細資訊。主要值為：

- 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FDM和FTD中配置DNS伺服器才能解析FQDN。在本配置指南中，這些值為win2016.example.com，解析為192.168.1.1。
- 伺服器埠：LDAP服務使用的埠。預設情況下，LDAP和STARTTLS將對LDAP使用TCP埠389，而LDAP over SSL(LDAPS)將使用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FDM和FTD用於繫結到LDAP伺服器、驗證使用者以及搜尋使用者和組的帳戶。將為此建立名為FTD Admin的帳戶。
- 基本可分辨名稱(DN):基礎DN是FDM的起點，FTD將通知Active Directory在搜尋使用者時開始使用。在本配置指南中，根域example.com將用作基礎DN;但是，對於生產環境，在LDAP層次結構中使用基本DN可能更好。例如，以此LDAP層次結構為例：



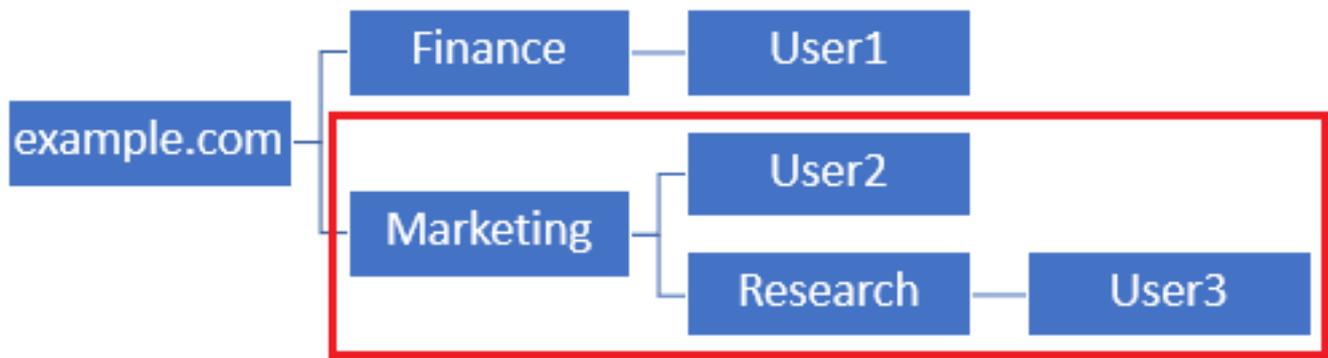
如果管理員希望市場行銷組織單位中的使用者能夠對基本DN進行身份驗證，則可以將基本DN設定為根(example.com)，但是，這也會允許財務組織單位下的User1也登入，因為使用者搜尋將從根開始，並轉到Finance、Marketing和Research。

基本DN設定為example.com。



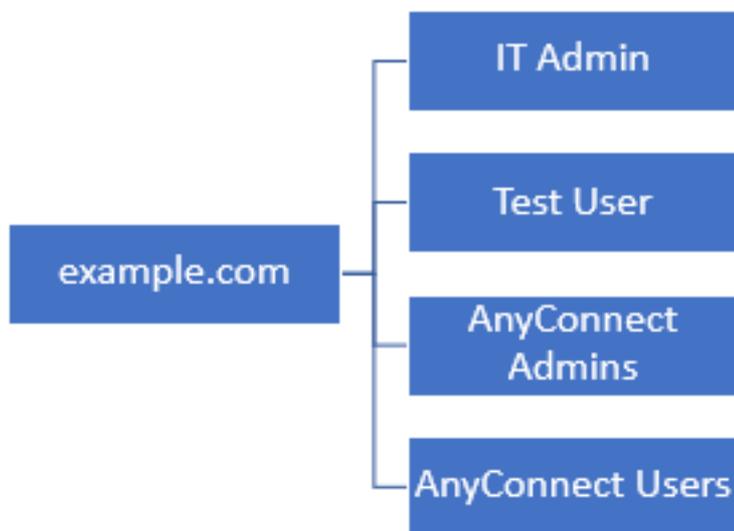
為了將登入限制為Marketing組織單位及以下單位中的使用者，管理員可以將Base DN設定為Marketing。現在只有User2和User3能夠進行身份驗證，因為搜尋將從市場行銷開始。

基本DN設定為Marketing:



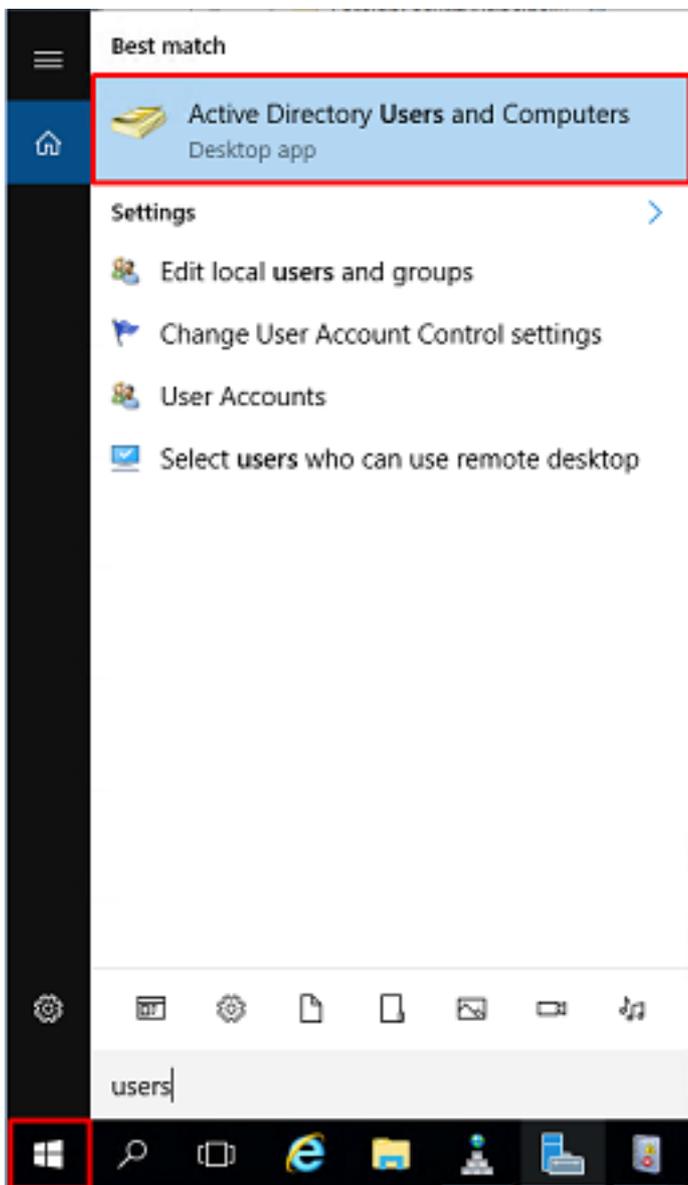
請注意，為了在FTD內實現更精細的控制，允許使用者根據其AD屬性連線或分配不同的授權，需要配置LDAP授權對映。

本配置指南中使用此簡化的LDAP層次結構，根example.com的DN將用於基礎DN。

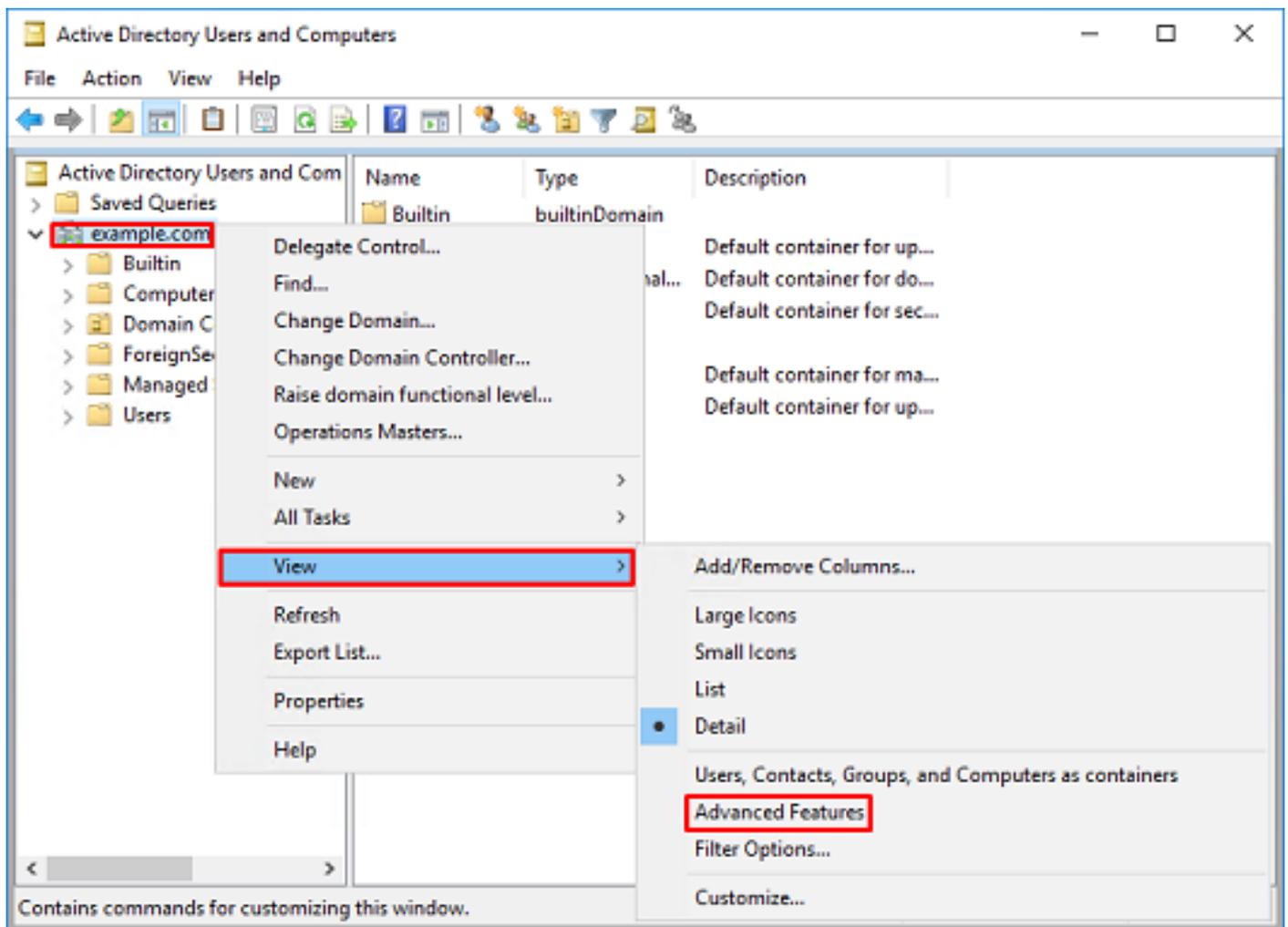


確定LDAP基本DN

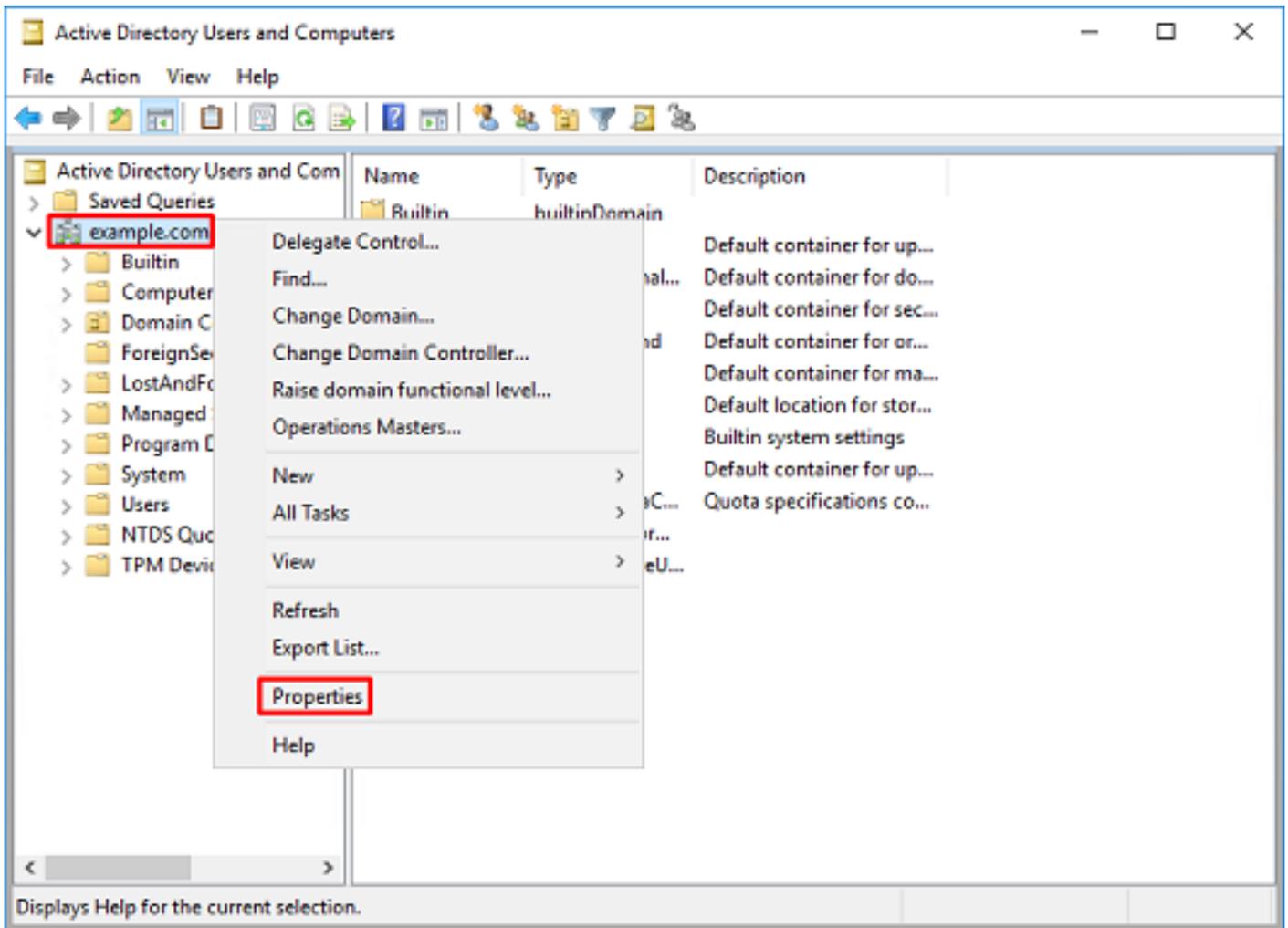
1. 開啟AD使用者和電腦。



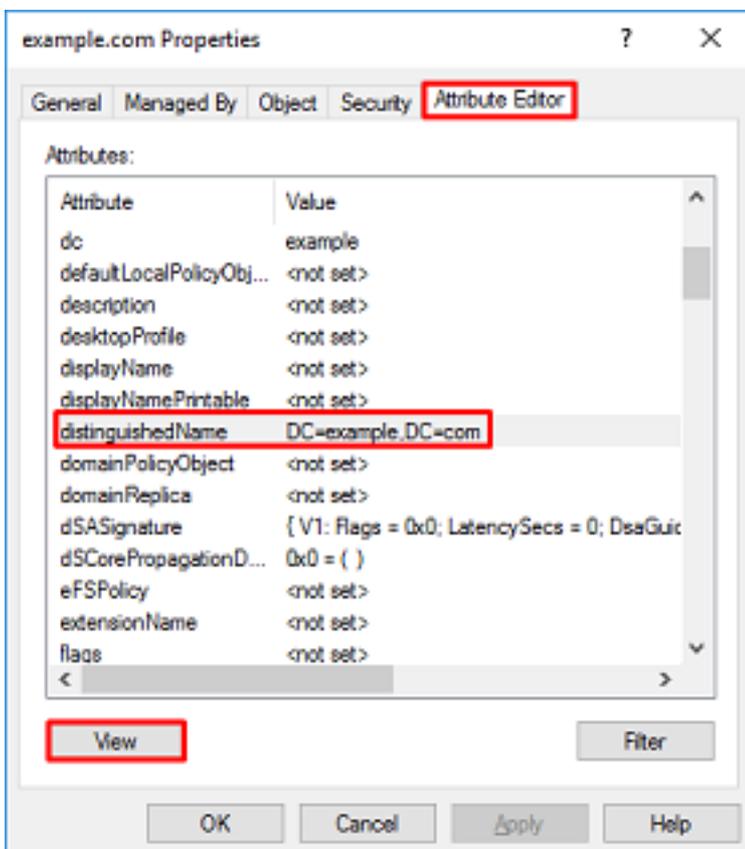
2.左鍵點選根域（以便開啟容器），右鍵點選根域，然後導航到檢視，然後按一下高級功能。



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，然後導航到屬性。

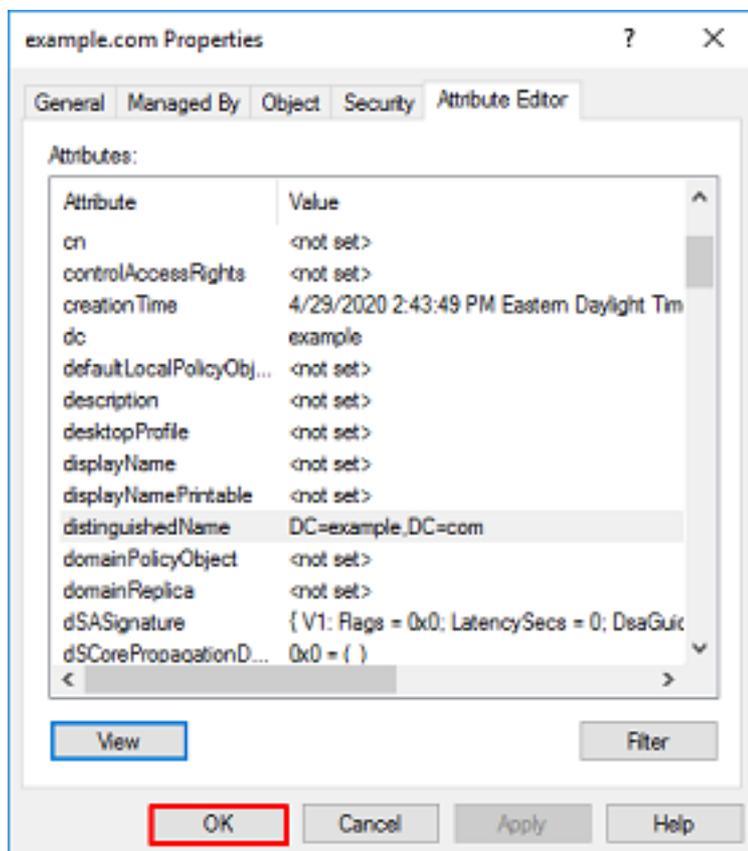
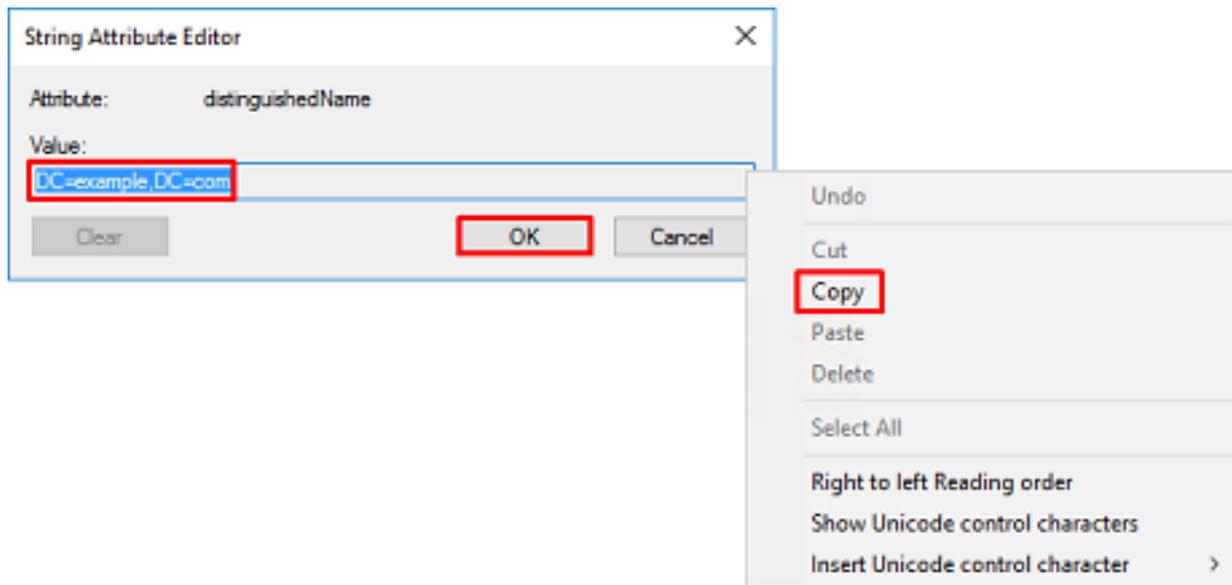


4. 在屬性下，按一下屬性編輯器頁籤。在「屬性」下查詢distinguishedName，然後按一下檢視。

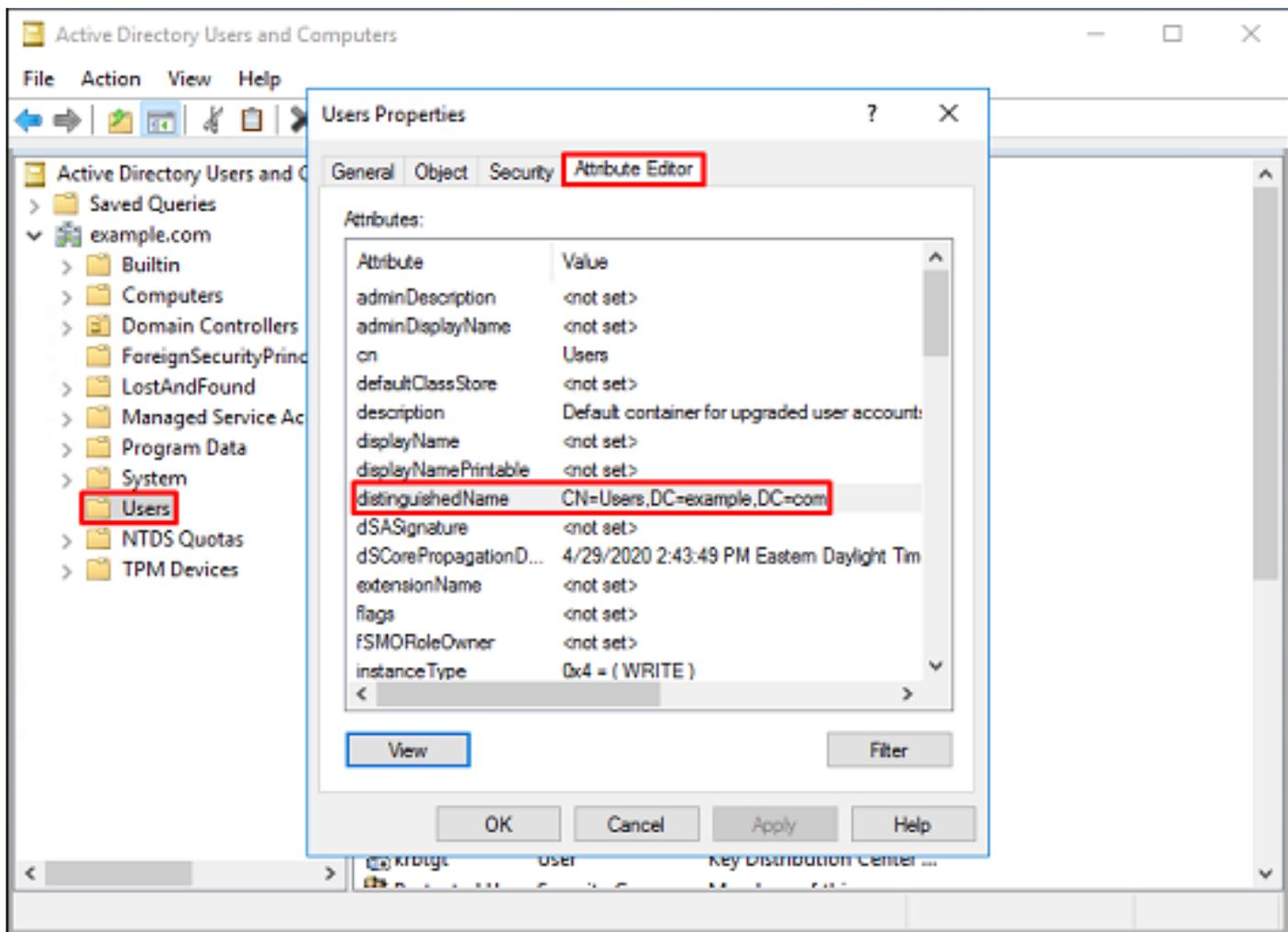


5. 這將開啟一個新視窗，以後可以在其中複製並貼上到FDM中。在本示例中，根DN為

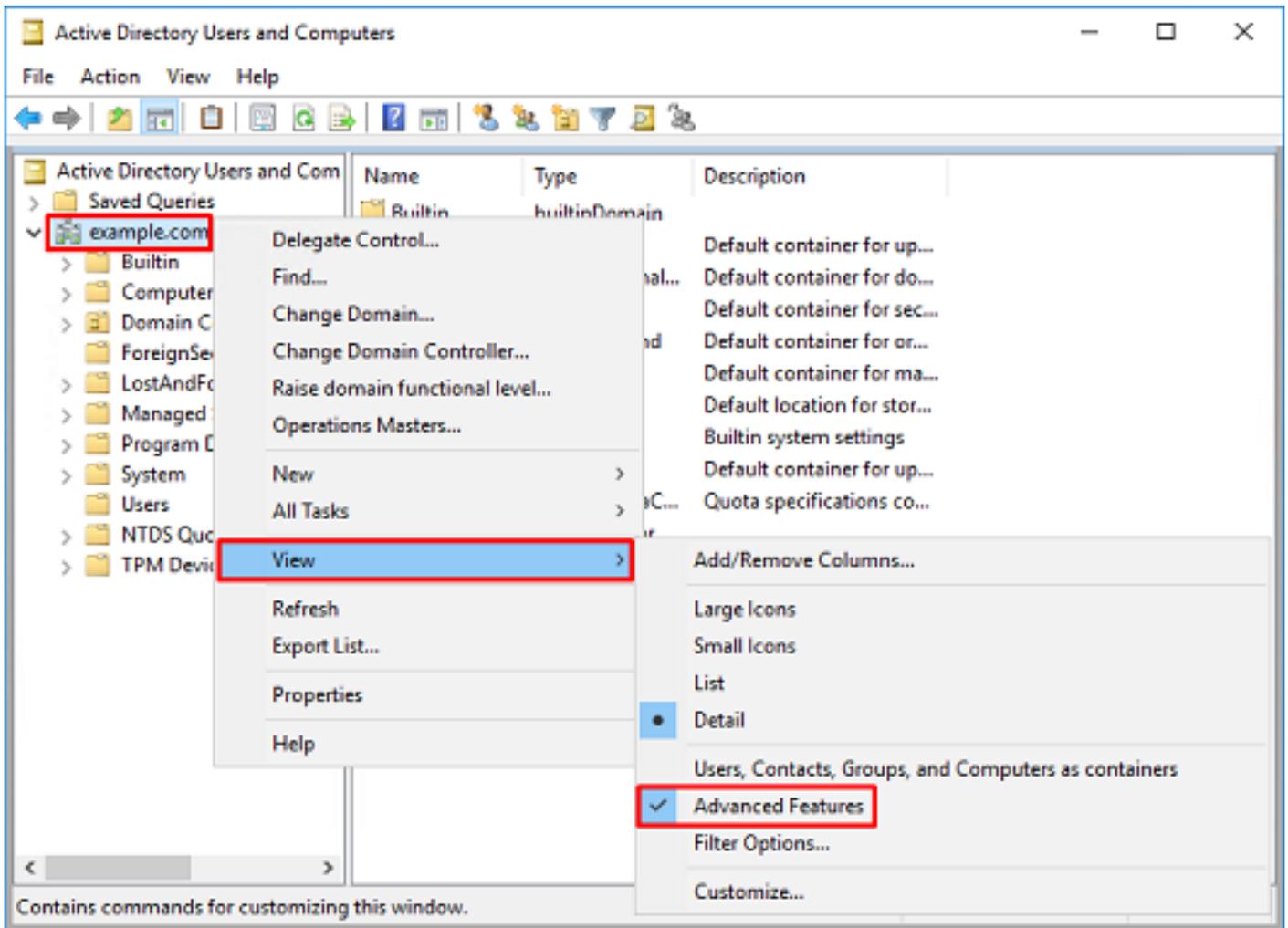
DC=example , DC=com。複製值。按一下OK以退出「字串屬性編輯器」視窗，然後再次按一下OK以退出屬性。



可以對AD內的多個對象執行此操作。例如，以下步驟用於查詢使用者容器的DN:



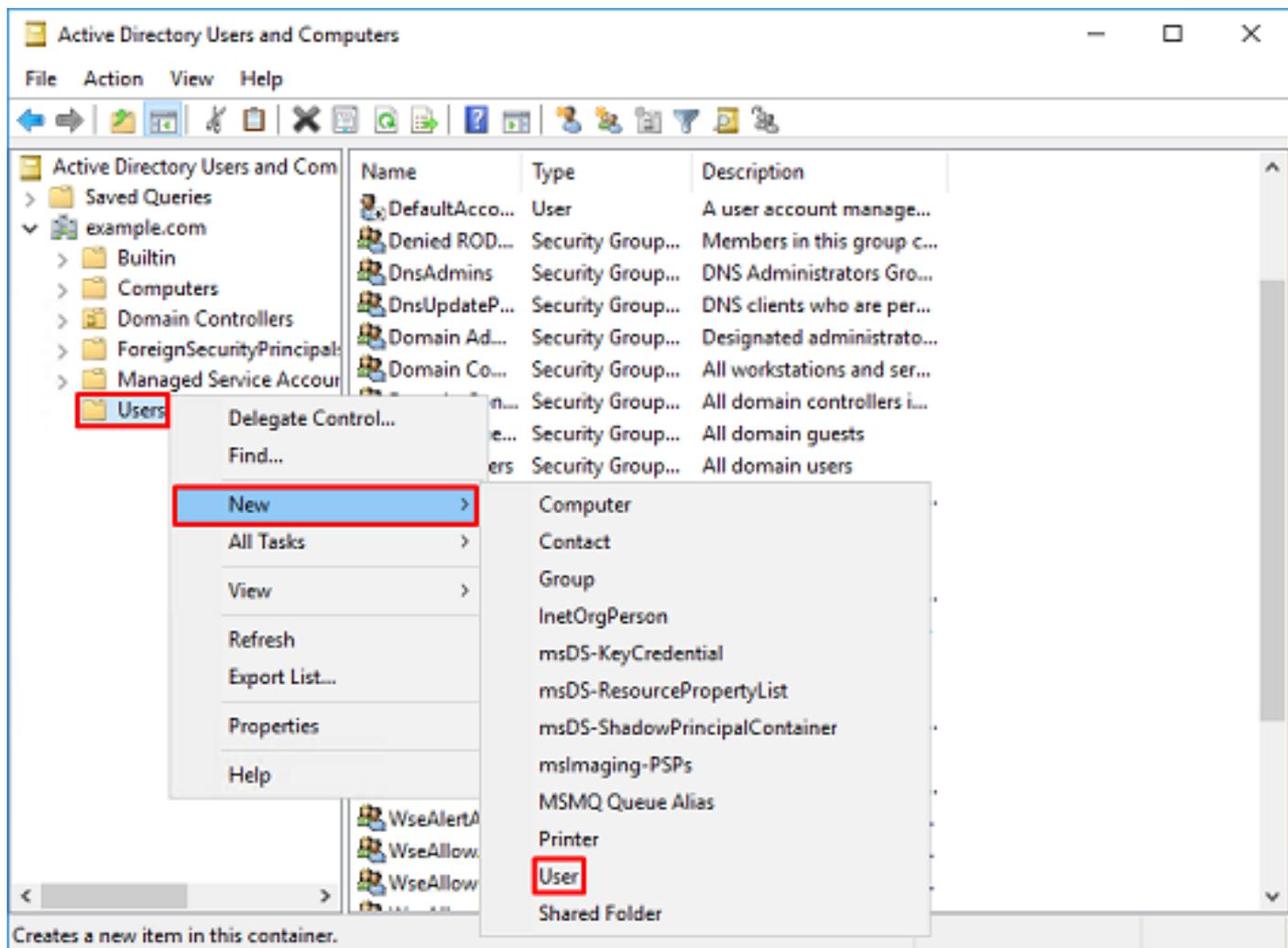
6. 可以刪除「高級功能」檢視。按一下右鍵根DN，導航到View，然後再次按一下Advanced Features。



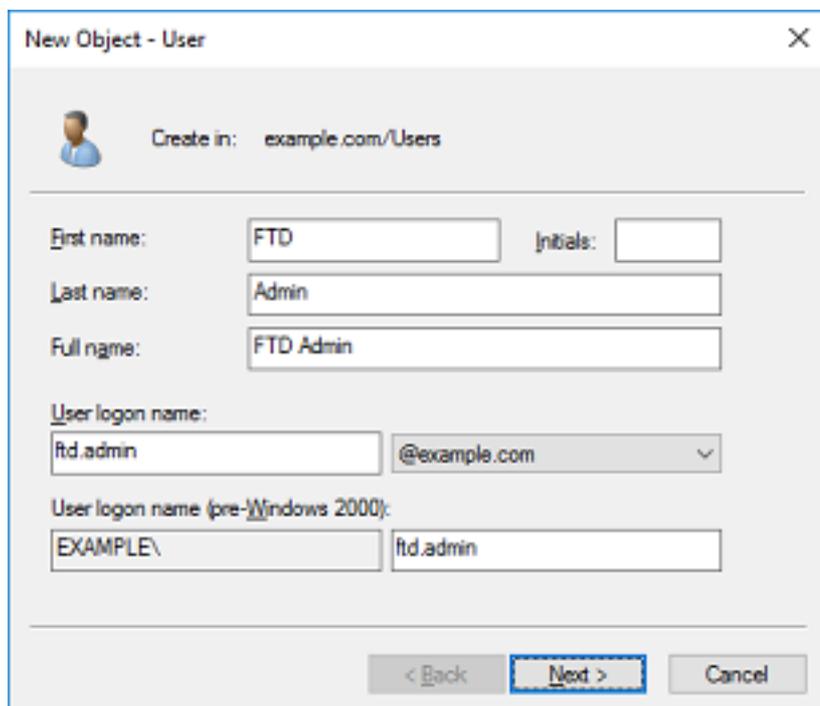
建立FTD帳戶

此使用者帳戶將允許FDM和FTD與AD繫結，以搜尋使用者和組並對它們進行身份驗證。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。此帳戶無需在本機DN範圍內。

1. 在Active Directory使用者和電腦中，按一下右鍵FTD帳戶將新增到其中的容器/組織。在此組態中，FTD帳戶會新增到使用者名稱ftd.admin@example.com下的使用者容器下。按一下右鍵Users，然後按一下New > User。



2. 瀏覽「新建對象 — 使用者向导」。



New Object - User

Create in: example.com/Users

Password:

Confirm password:

User must change password at next logon

User cannot change password

Password never expires

Account is disabled

< Back Next > Cancel

New Object - User

Create in: example.com/Users

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

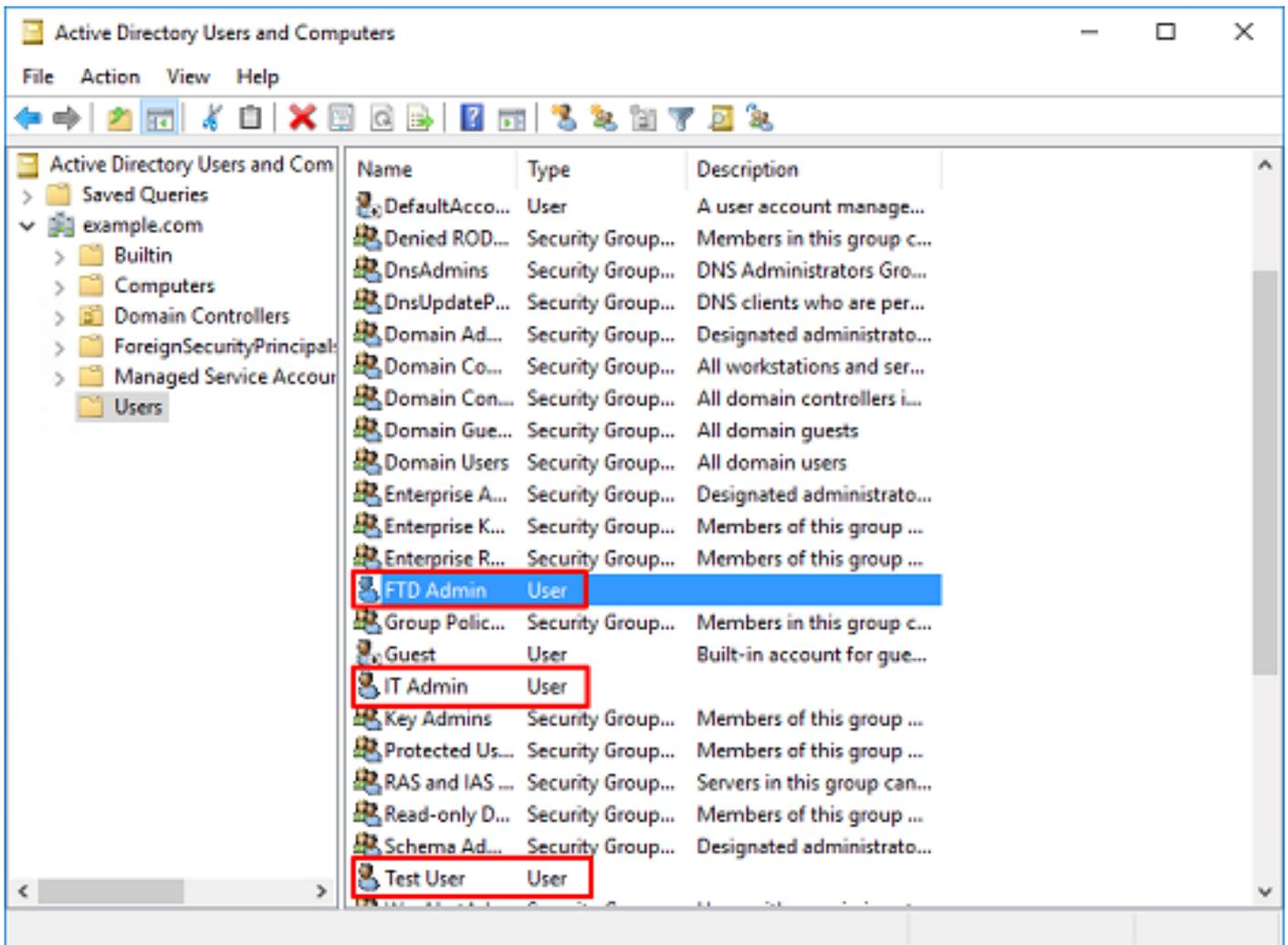
Full name: FTD Admin

User logon name: ftd.admin@example.com

The password never expires.

< Back Finish Cancel

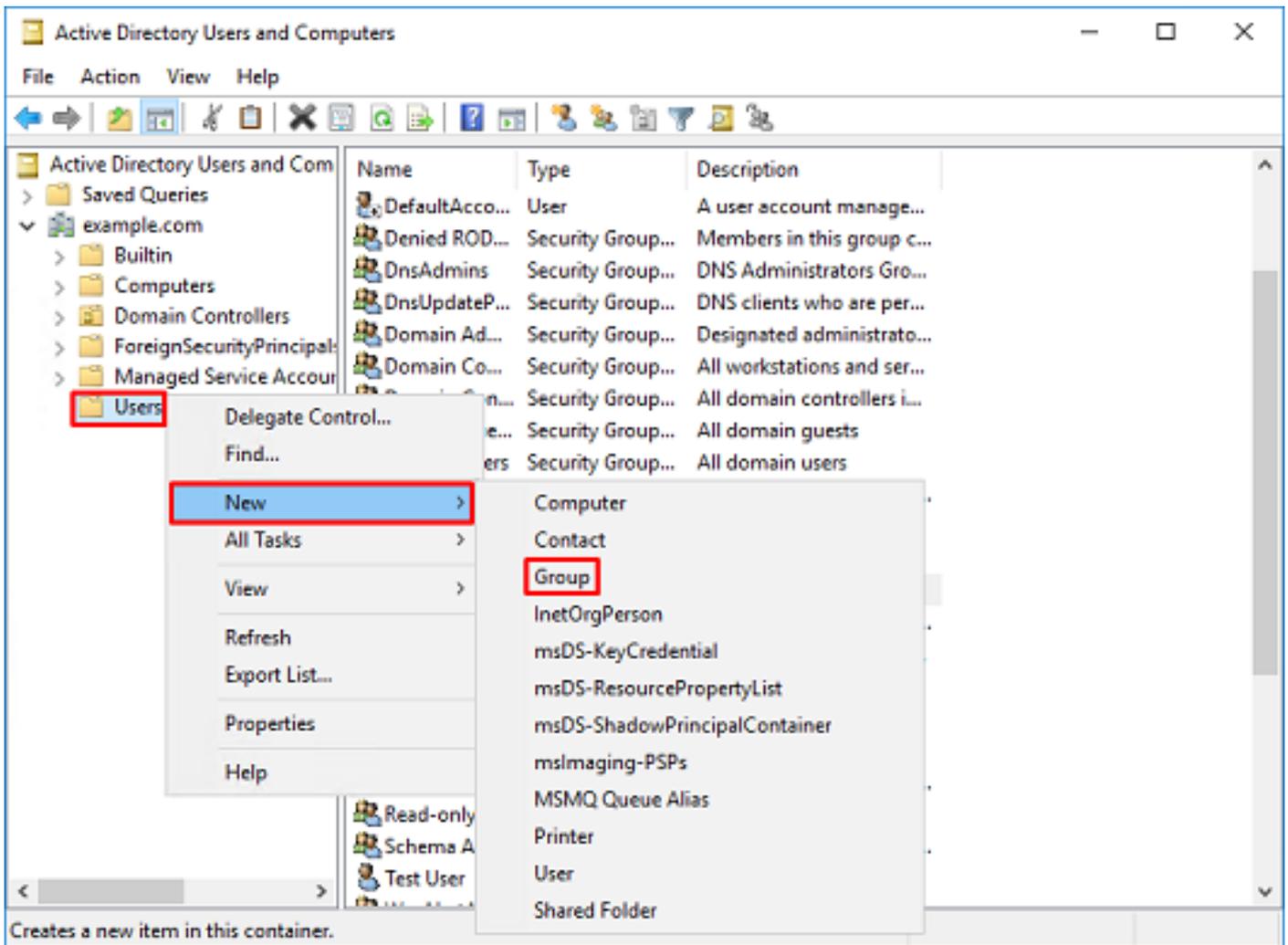
3. 驗證是否已建立FTD帳戶。此外，還另外建立了兩個帳戶，IT管理員和測試使用者。



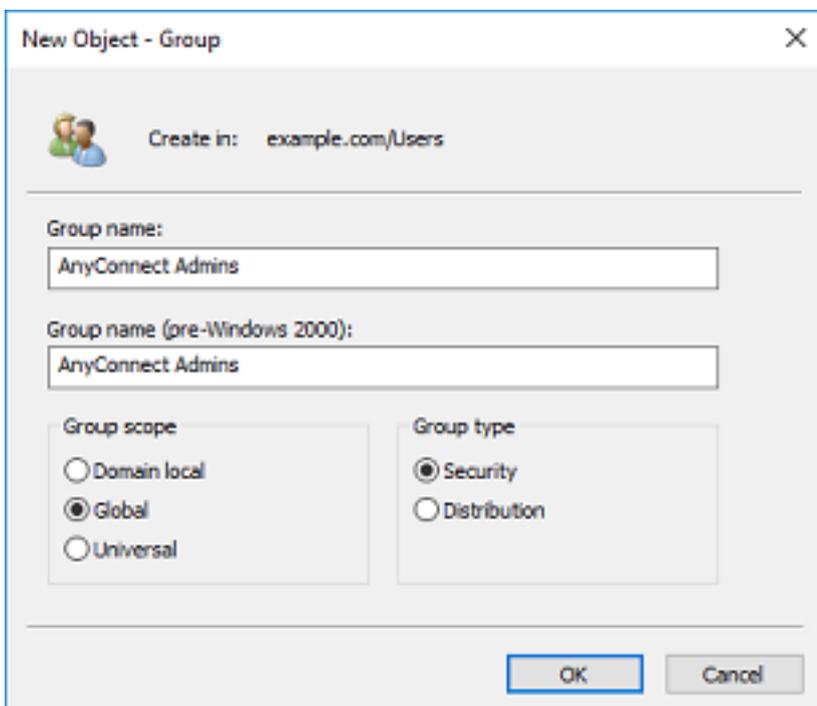
建立AD組並將使用者新增到AD組 (可選)

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，以後將通過FDM中的使用者標識使用組來應用訪問控制策略設定。

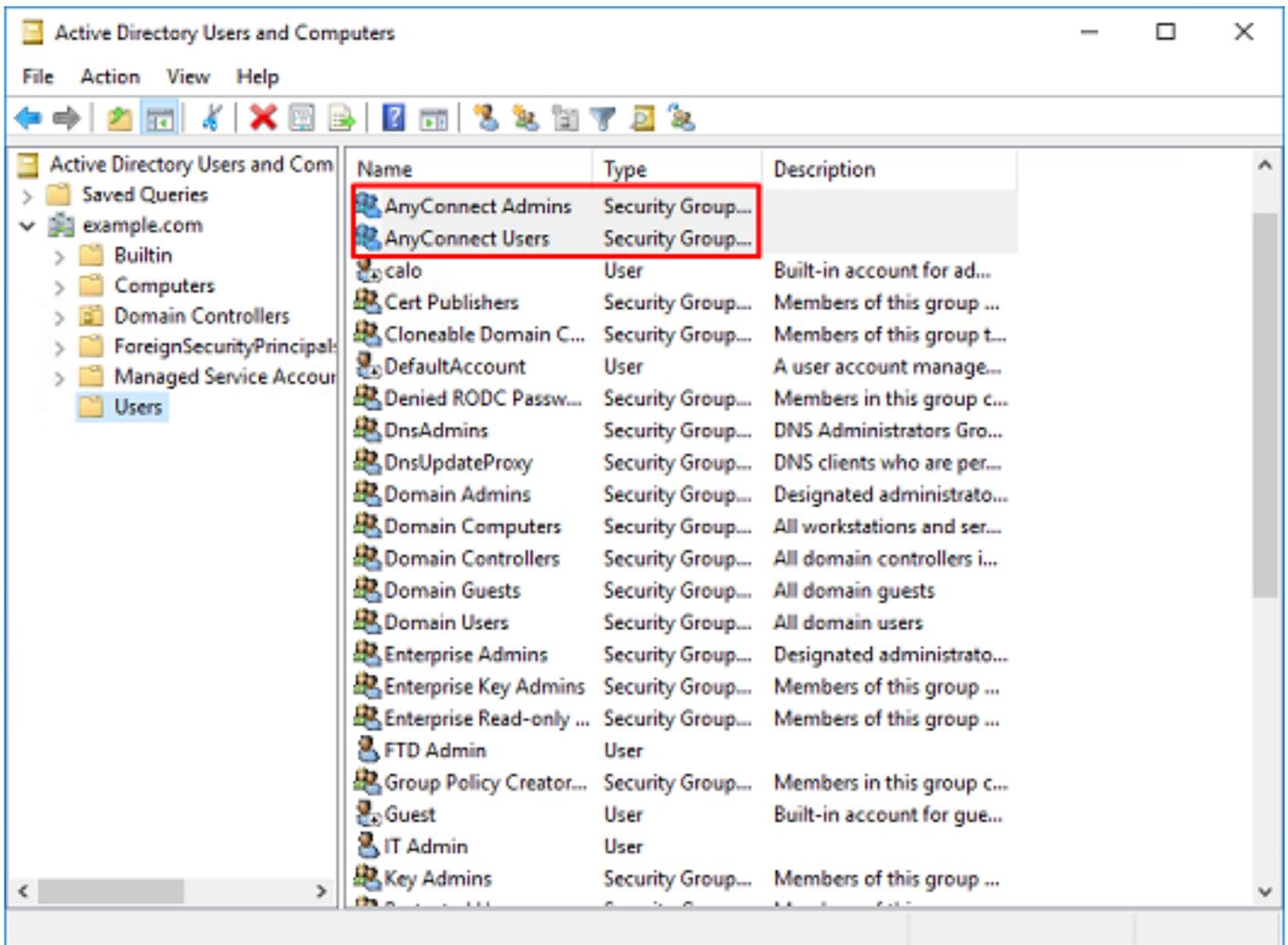
1. 在Active Directory使用者和電腦中，按一下右鍵新組將新增到其中的容器/組織。在本示例中，AnyConnect Admins組將新增到Users容器下。按一下右鍵Users，然後按一下New > Group。



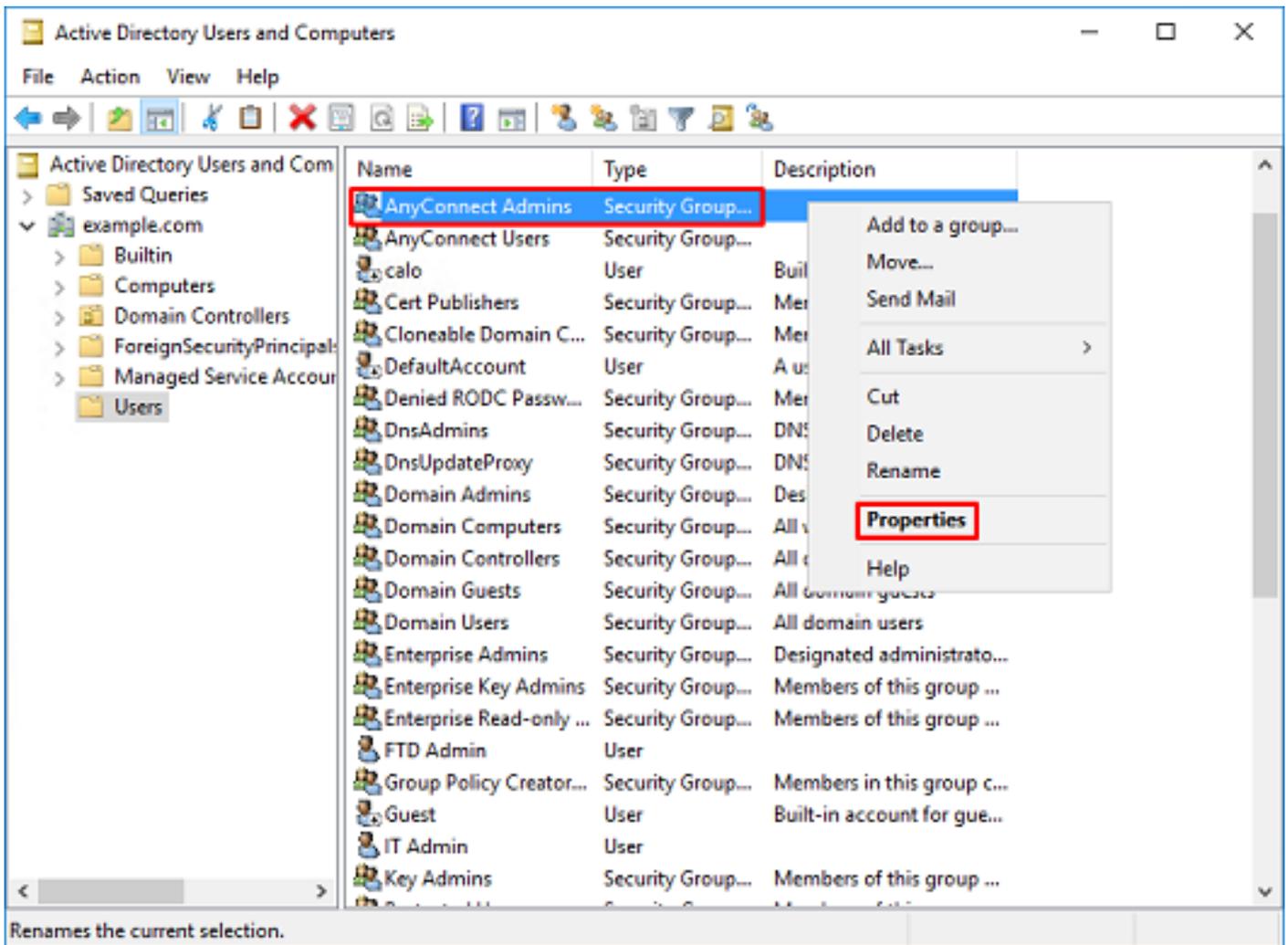
2. 瀏覽「新建對象 — 組」嚮導，如下圖所示。



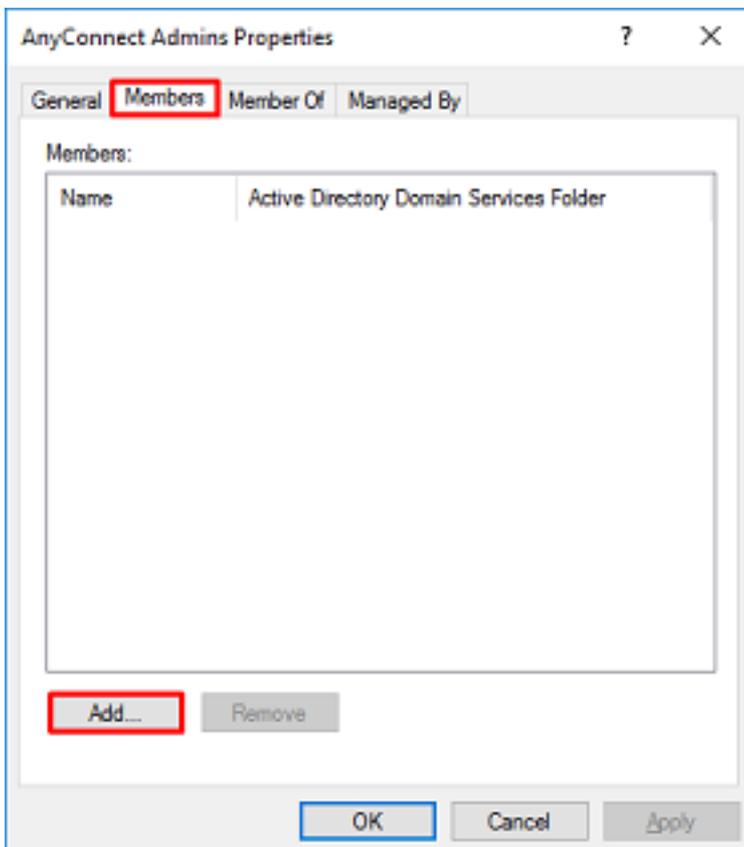
3. 驗證是否已建立組。還建立了AnyConnect Users組。



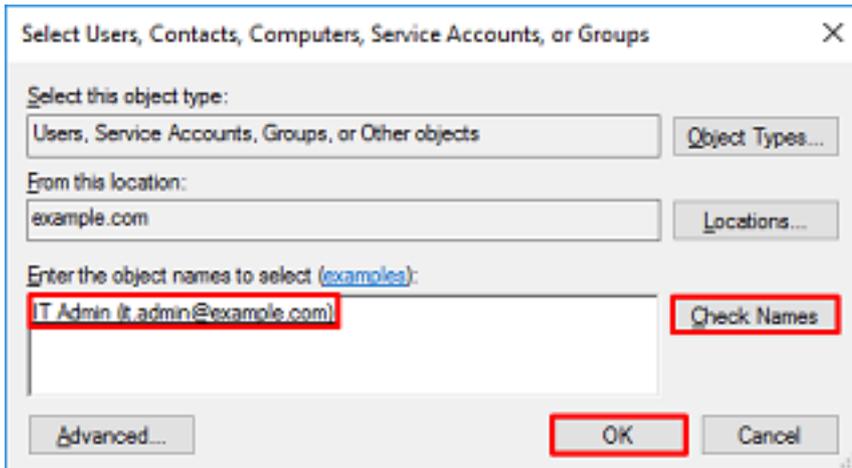
4.按一下右鍵要新增至的使用者的組，然後選擇屬性。在此配置中，使用者IT Admin將新增到AnyConnect Admins組，使用者Test User將新增到AnyConnect Users組。



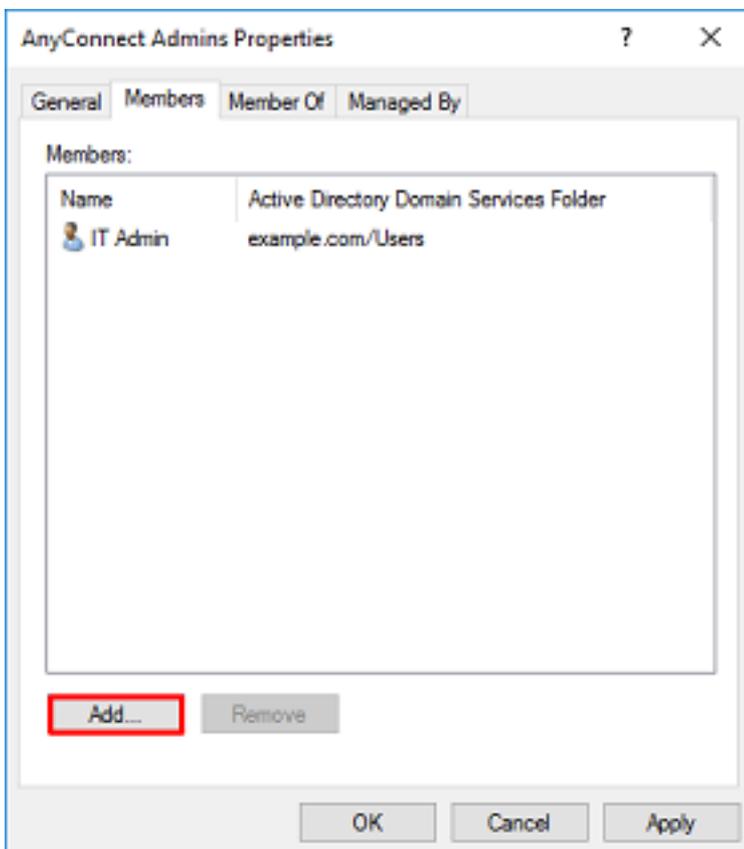
5. 按一下**Members**標籤，然後按一下**Add**，如下圖所示。



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

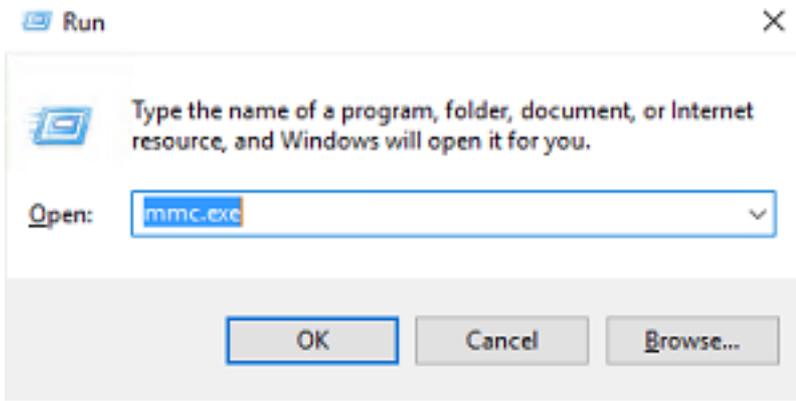


驗證是否新增了正確的使用者，然後按一下**OK**按鈕。使用者測試使用者也使用相同的步驟新增到組AnyConnect使用者。

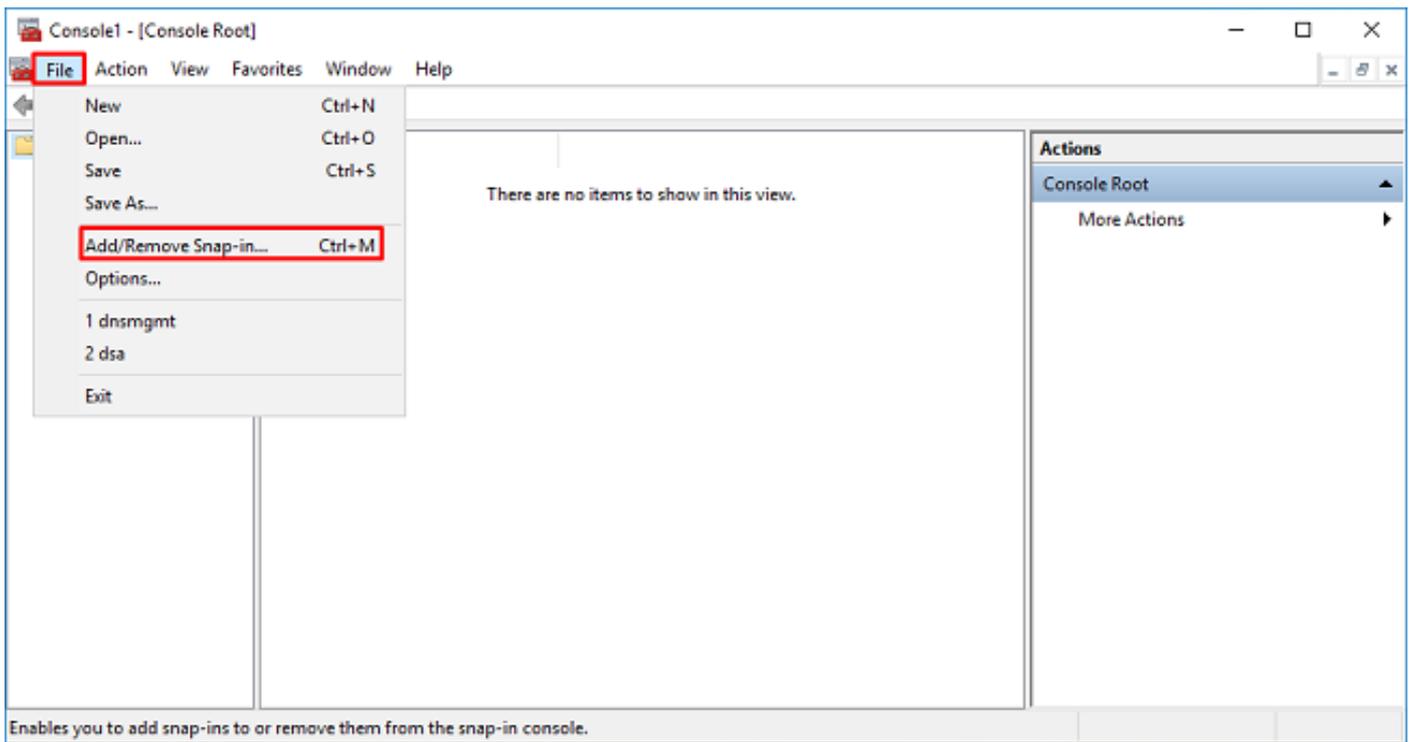


複製LDAPS SSL證書根 (僅對於LDAPS或STARTTLS是必需的)

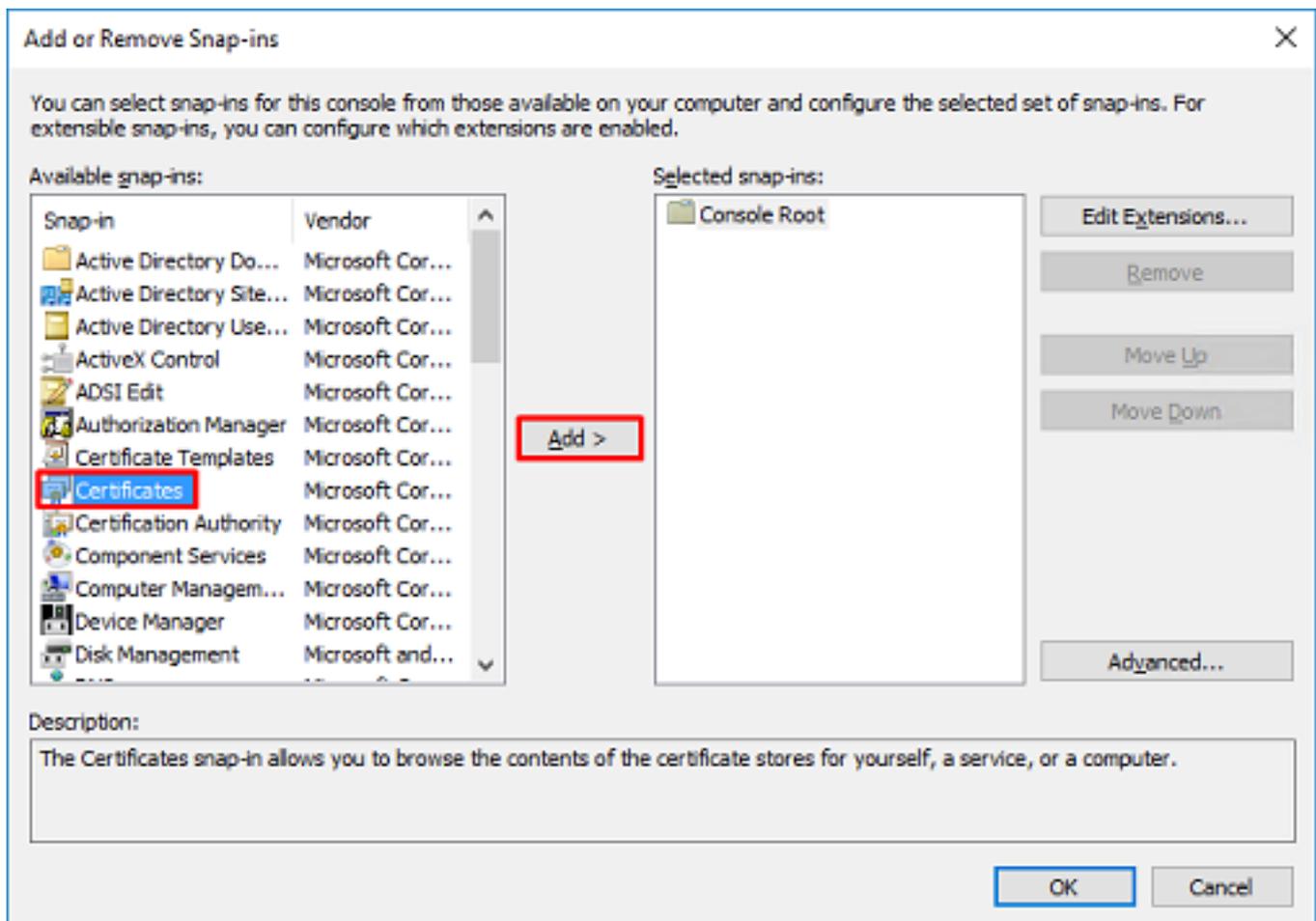
1. 按Win+R並鍵入mmc.exe。按一下「OK」(確定)。



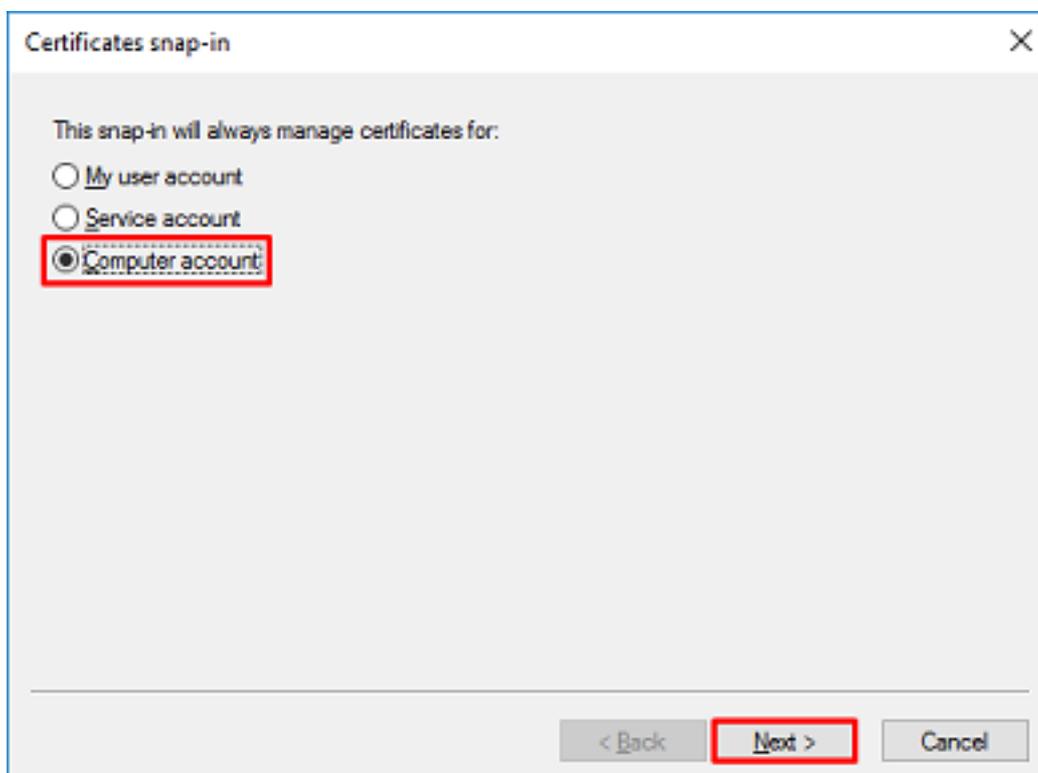
2. 導航到檔案>新增/刪除管理單元..... 如下圖所示。



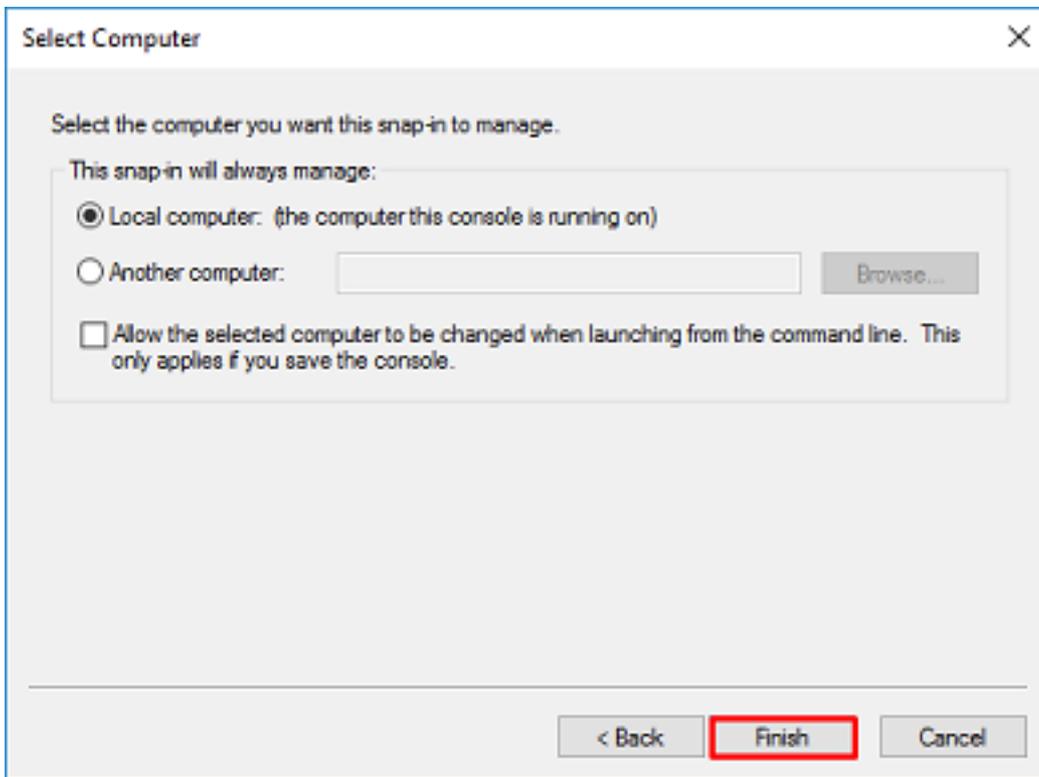
3. 在可用管理單元下，按一下**Certificates**，然後按一下**Add**。



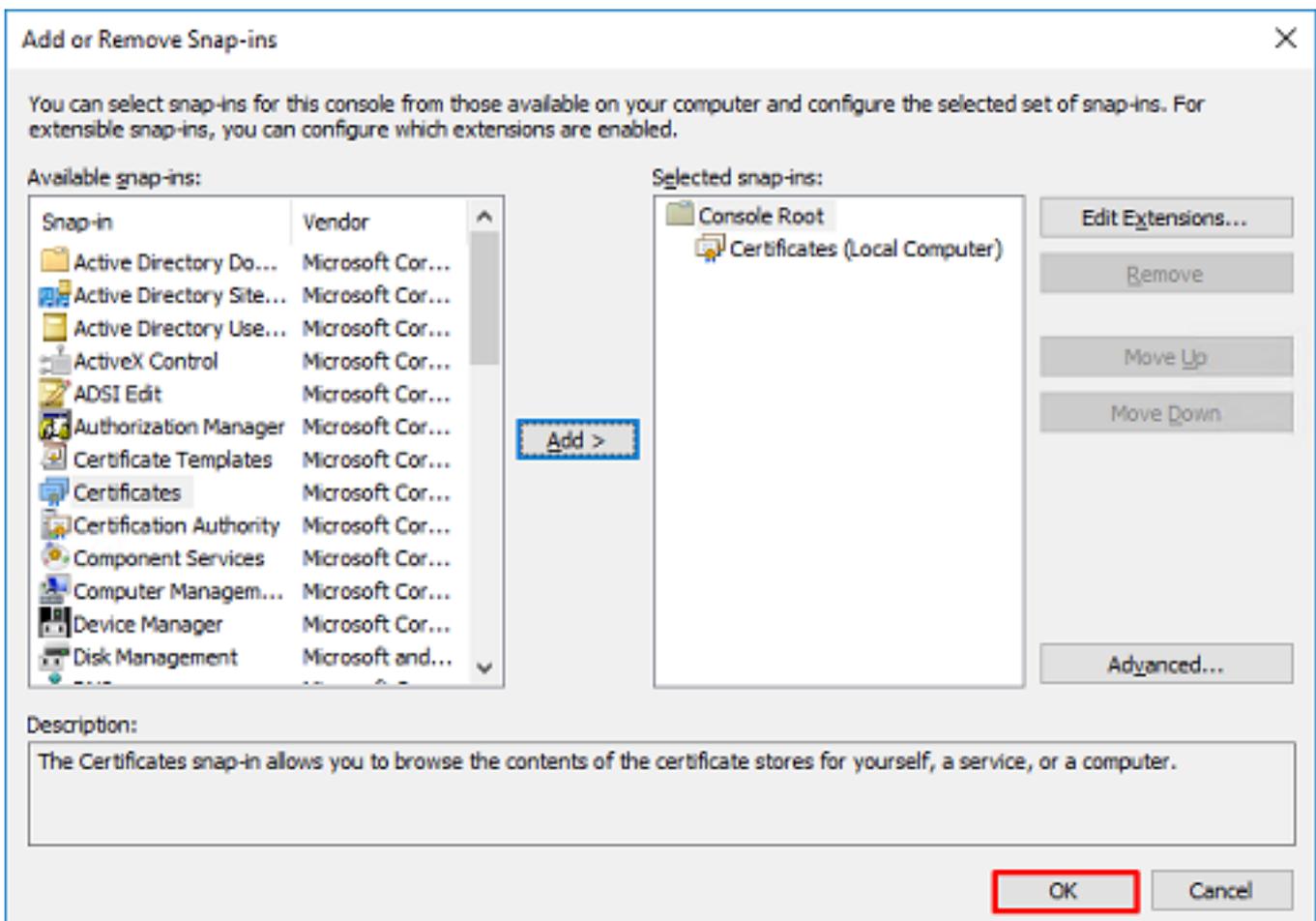
4.選擇「Computer account」，然後按一下「Next」，如下圖所示。



按一下「Finish」（結束）。



5. 按一下**確定**。

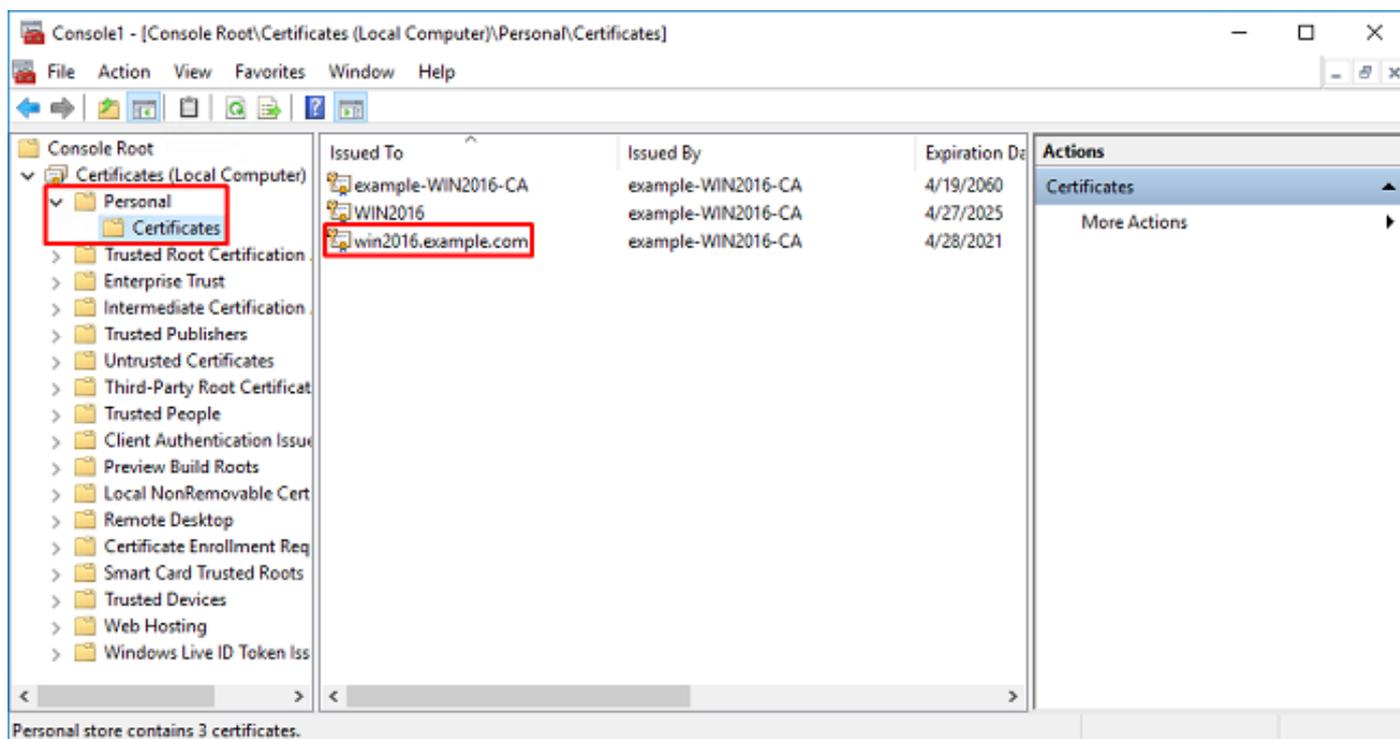


6. 展開**Personal**資料夾，然後按一下**Certificates**。LDAPS使用的證書應頒發給Windows伺服器的完全限定域名(FQDN)。在此伺服器上列出了3個證書。

- 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。

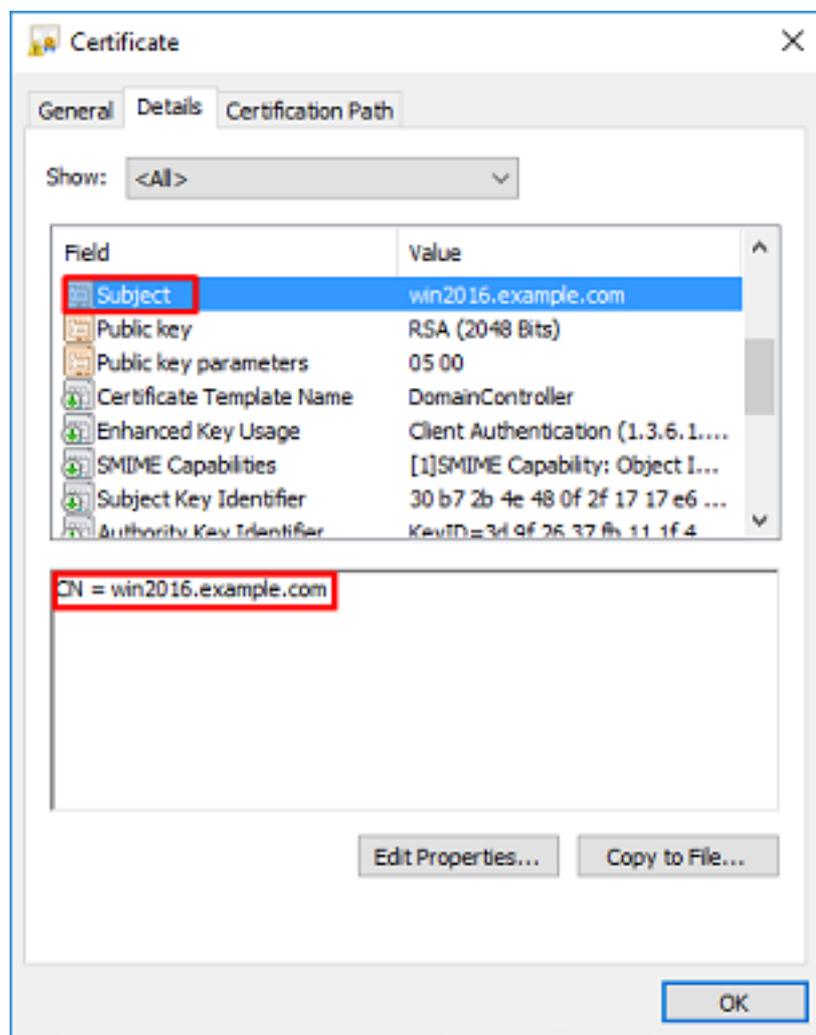
在此配置指南中，FQDN為win2016.example.com，因此前2個證書不能用作LDAPS SSL證書。頒發給win2016.example.com的身份證書是由Windows Server CA服務自動頒發的證書。按兩下證書檢查詳細資訊。

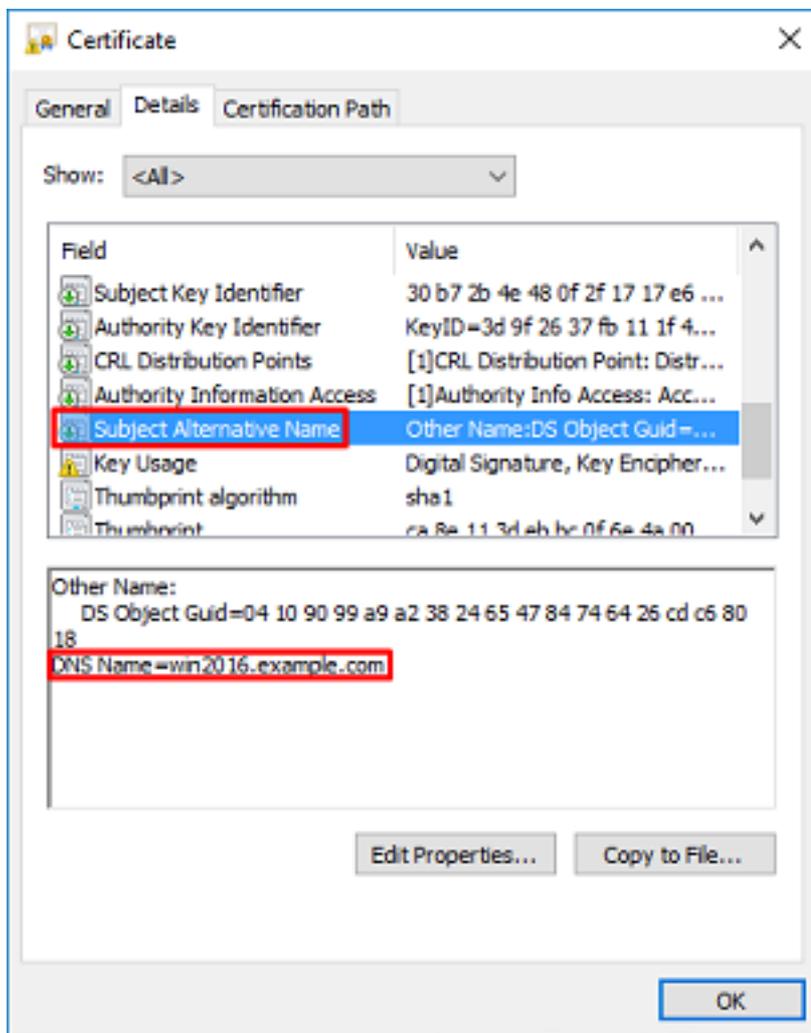


7.要用作LDAPS SSL證書，證書必須符合以下要求：

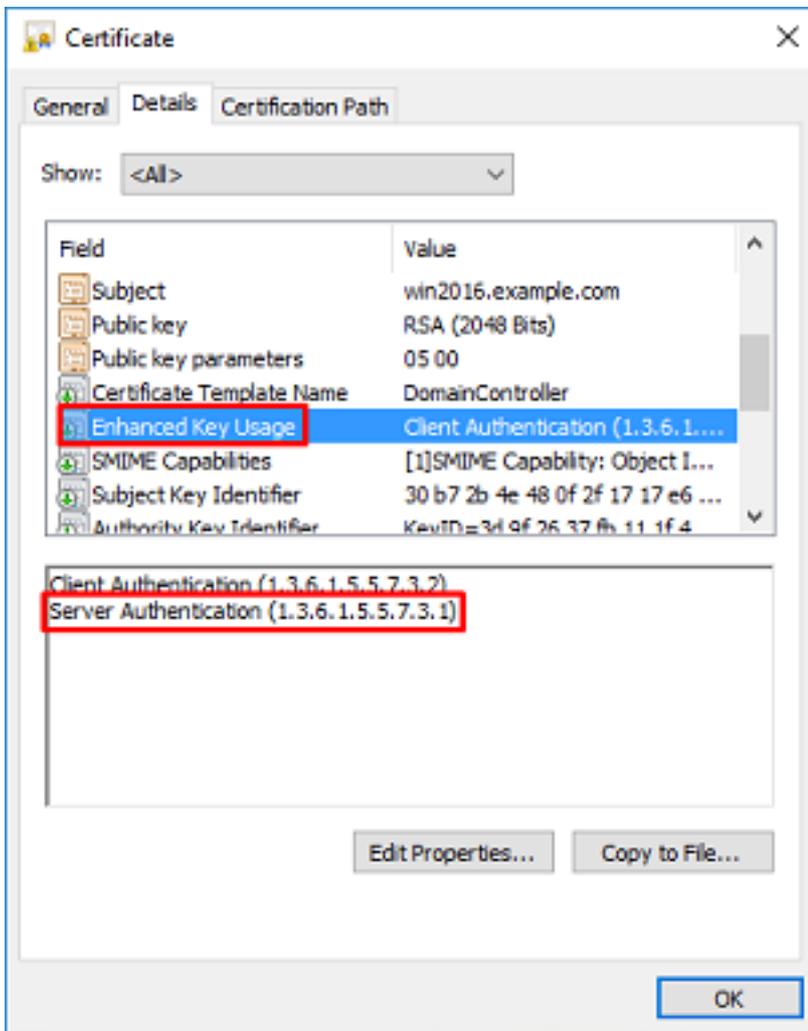
- 公用名稱或DNS使用者替代名稱與Windows Server的FQDN匹配。
- 證書在Enhanced Key Usage欄位下具有伺服器身份驗證。

在證書的「詳細資訊」頁籤下的Subject和Subject替代名稱下，存在FQDN win2016.example.com。

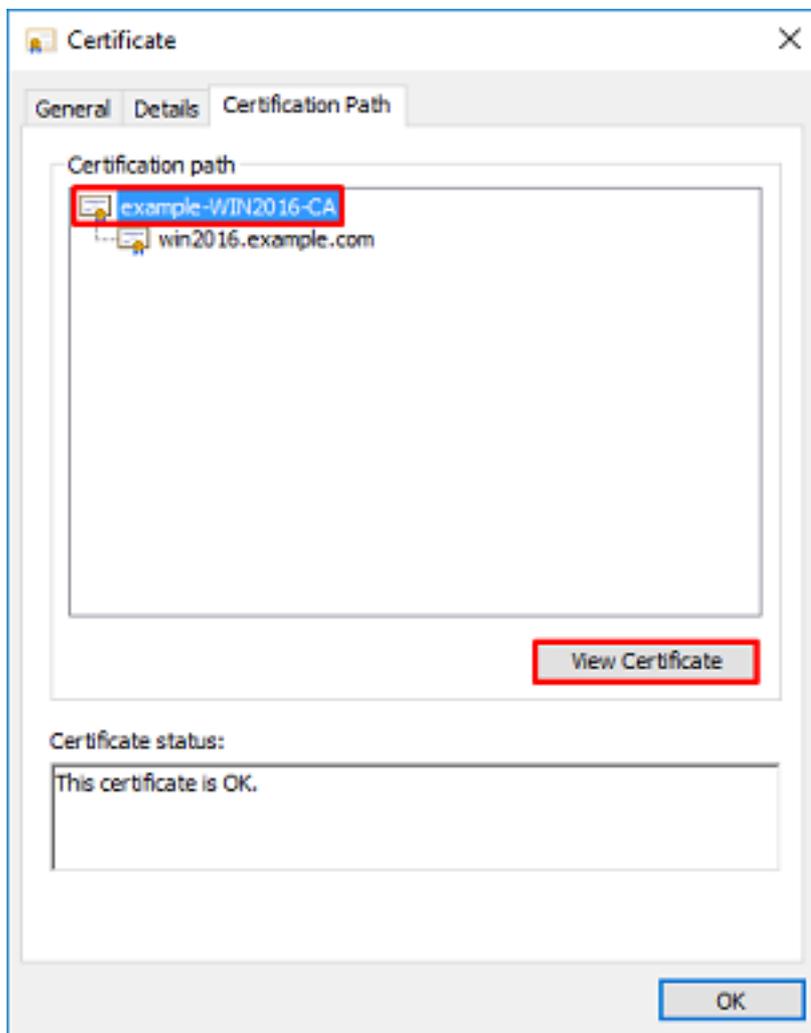




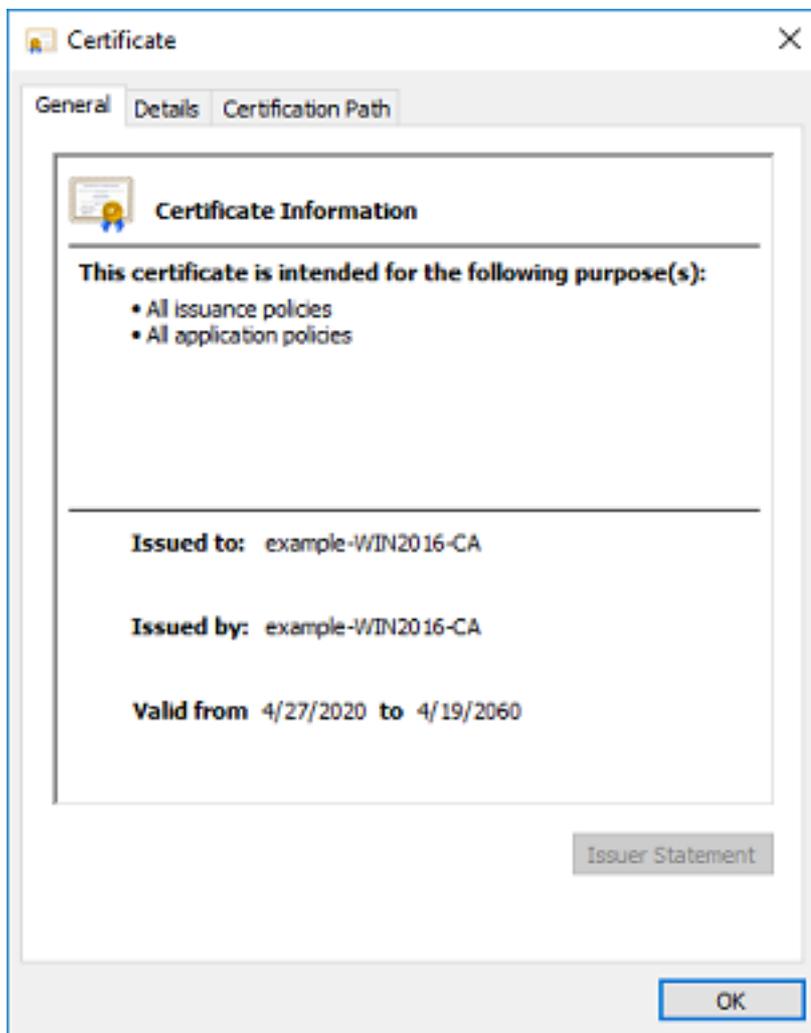
在Enhanced Key Usage下，出現Server Authentication。



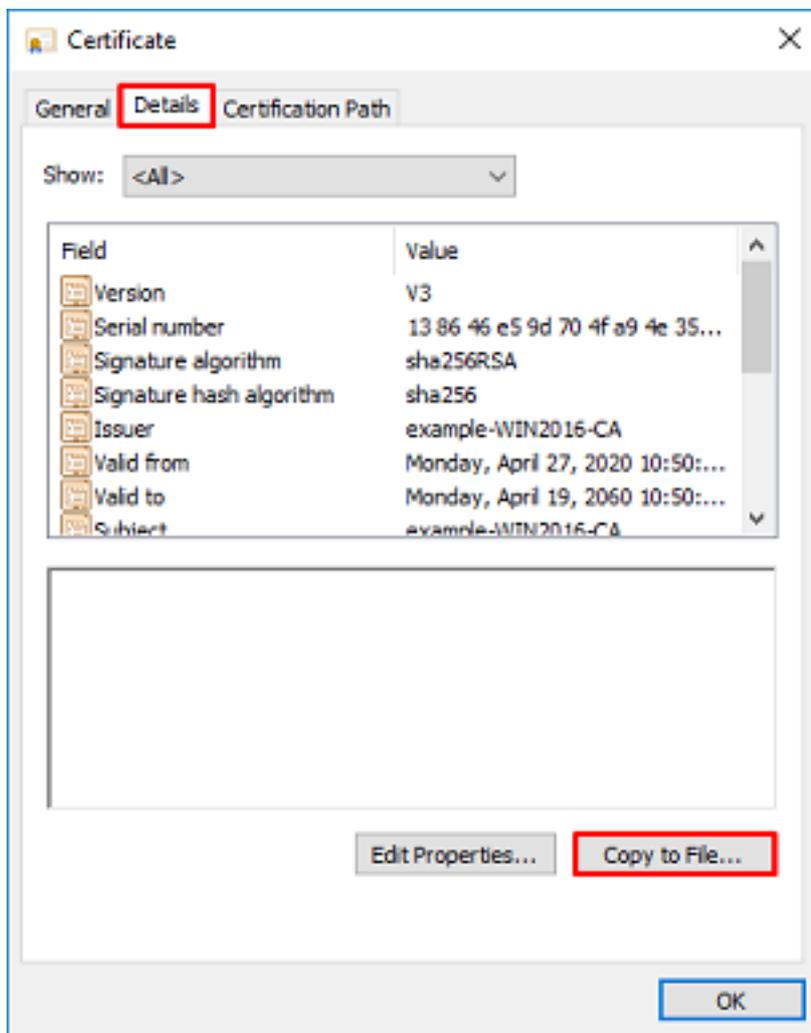
8. 確認後，請導航至認證路徑標籤。按一下應該為根CA證書的頂級證書，然後按一下**View Certificate**按鈕。



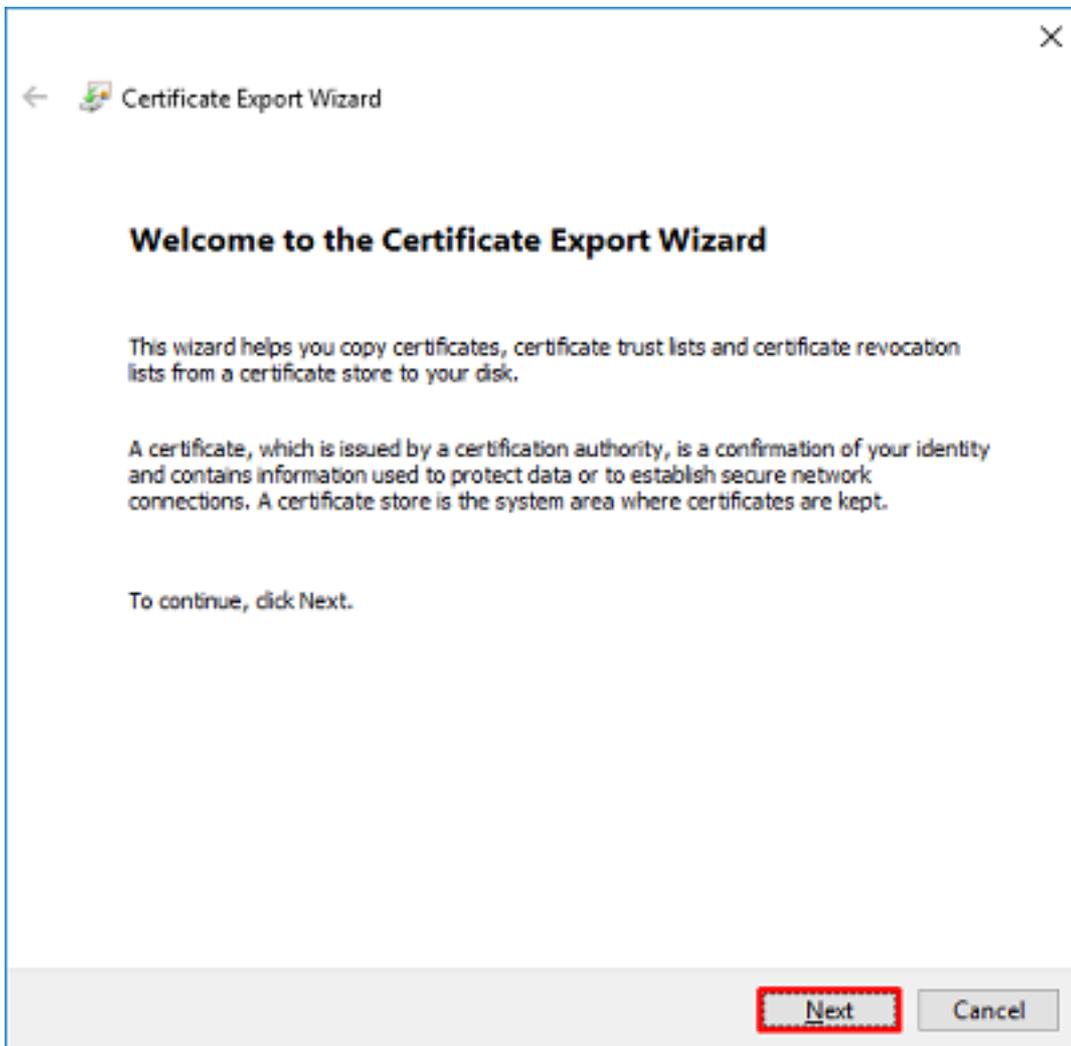
9.這將開啟根CA證書的證書詳細資訊。



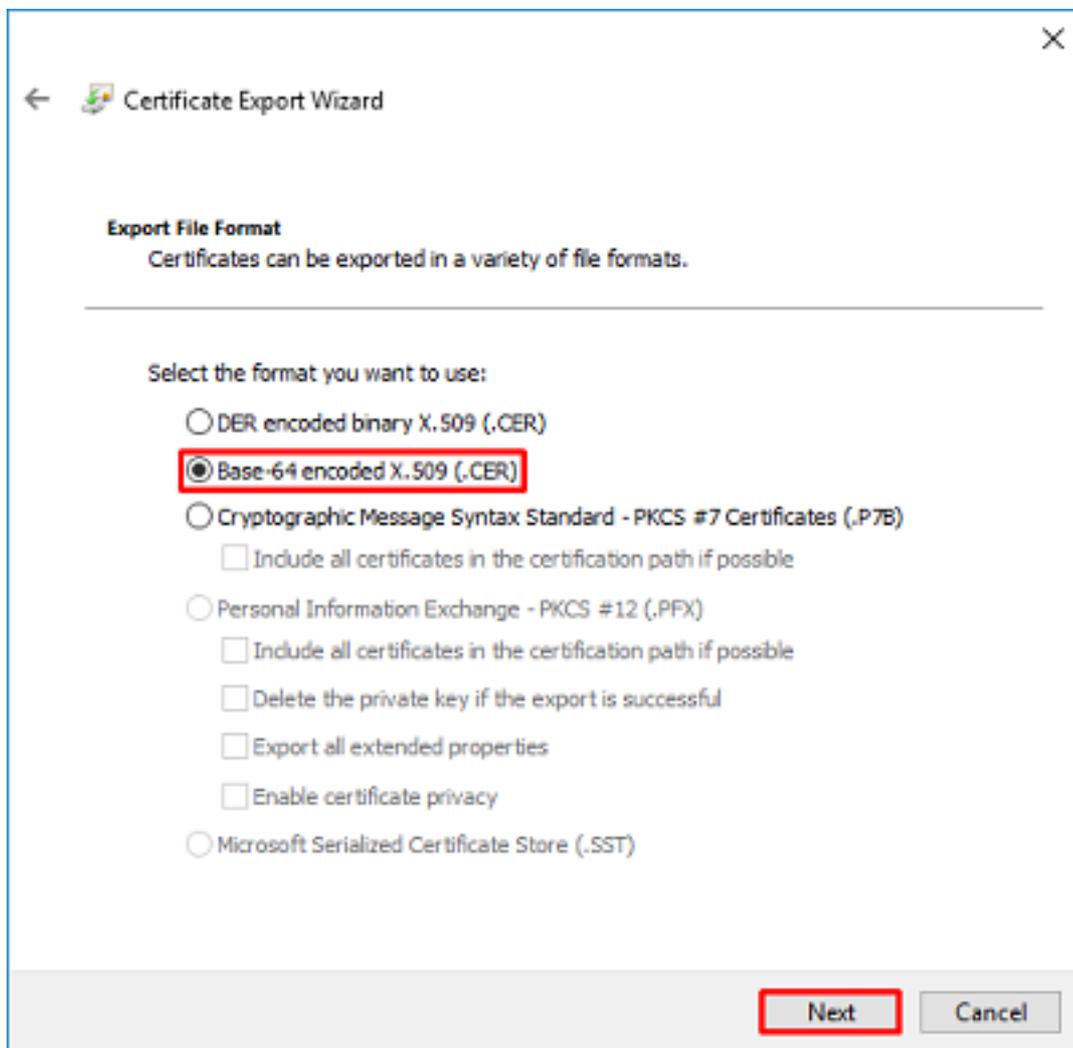
10. 開啟Details頁籤，然後單擊Copy to File... 如下圖所示。



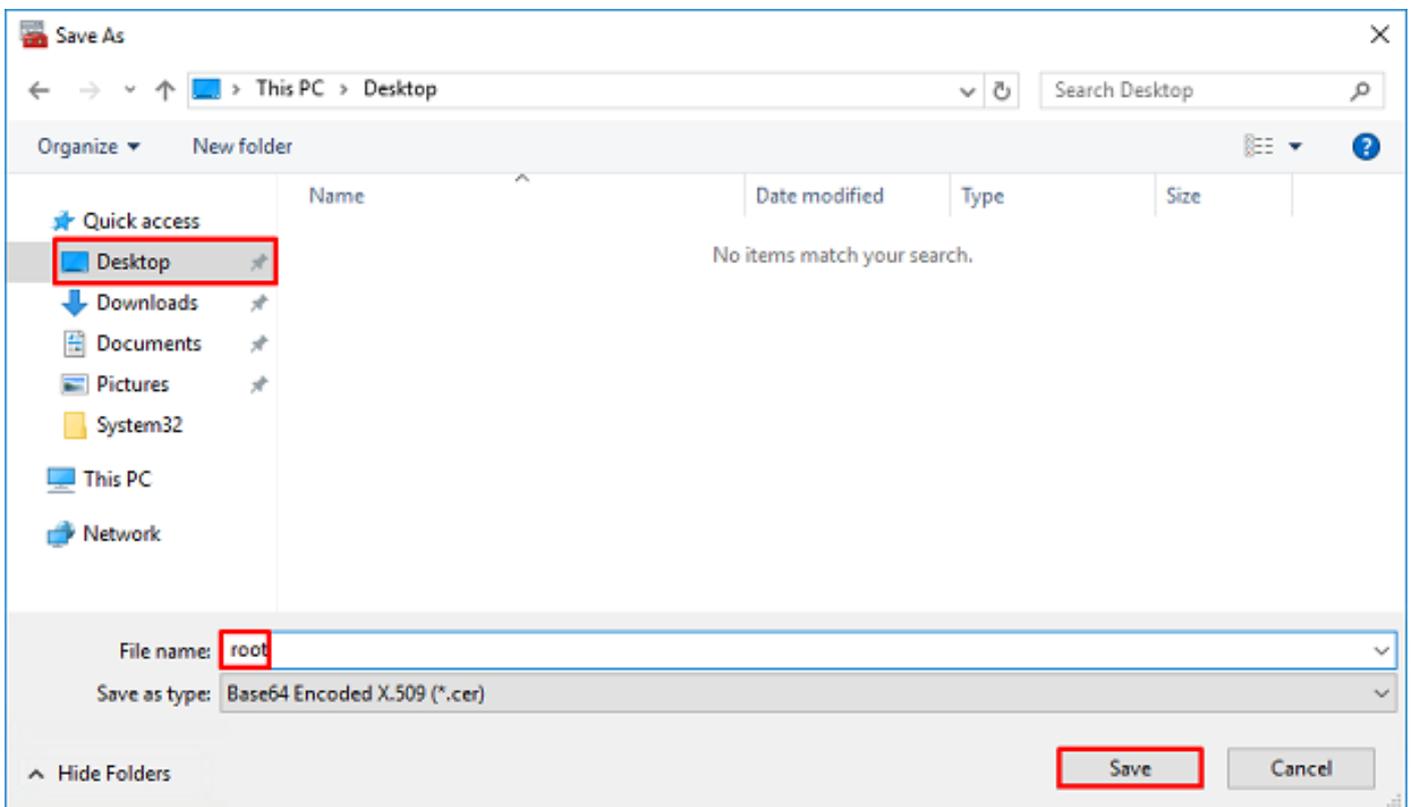
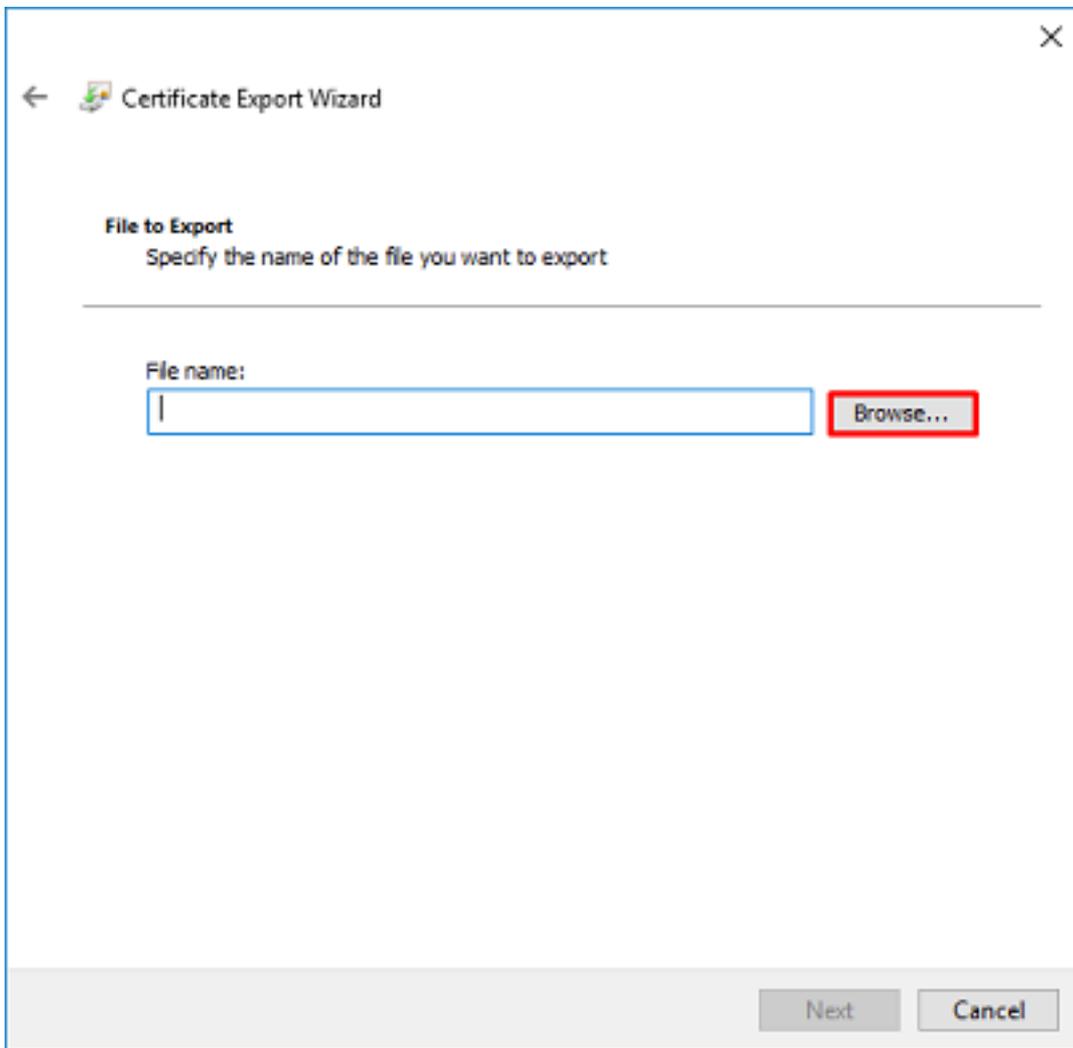
11. 瀏覽將以PEM格式匯出根CA的證書匯出嚮導。

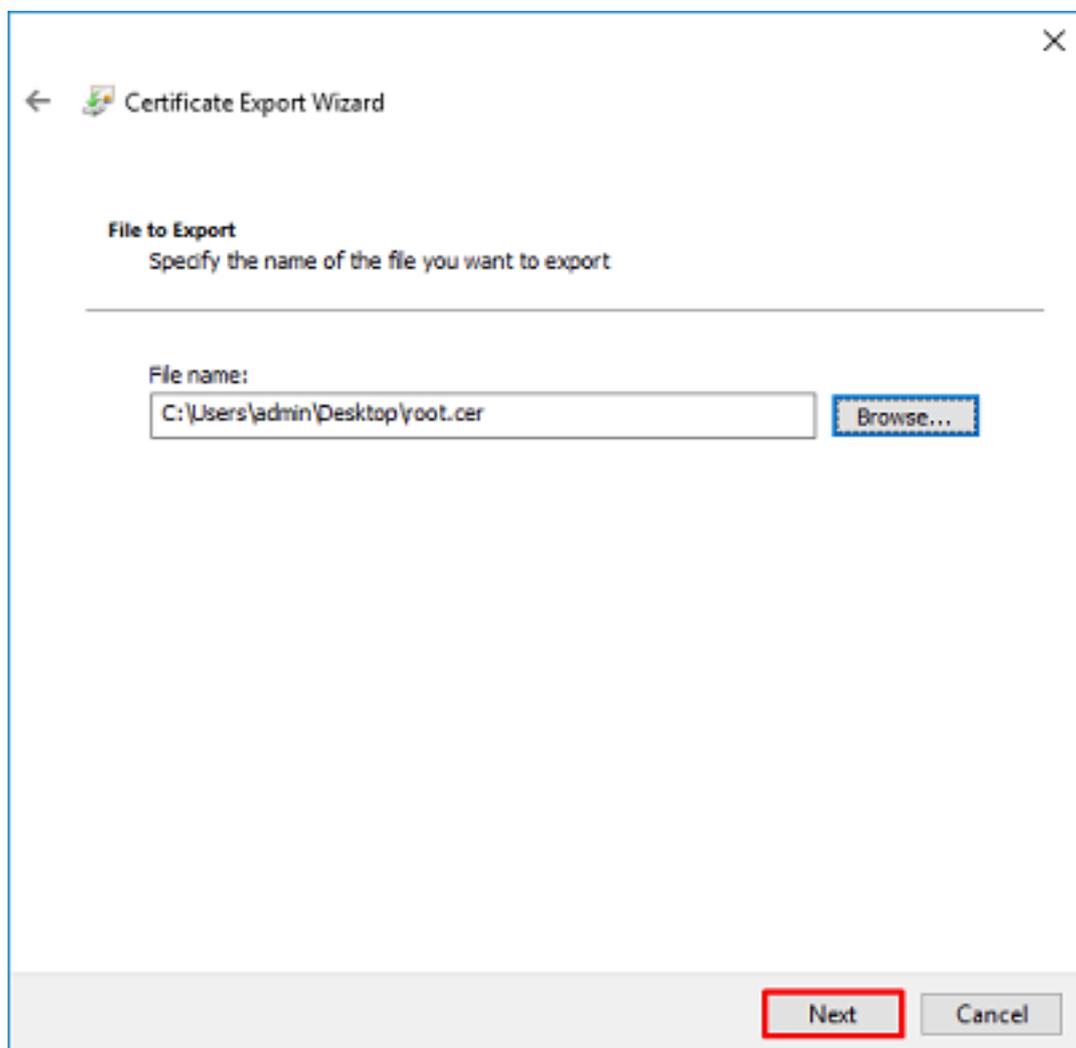


12.選擇Base-64 encoded X.509。

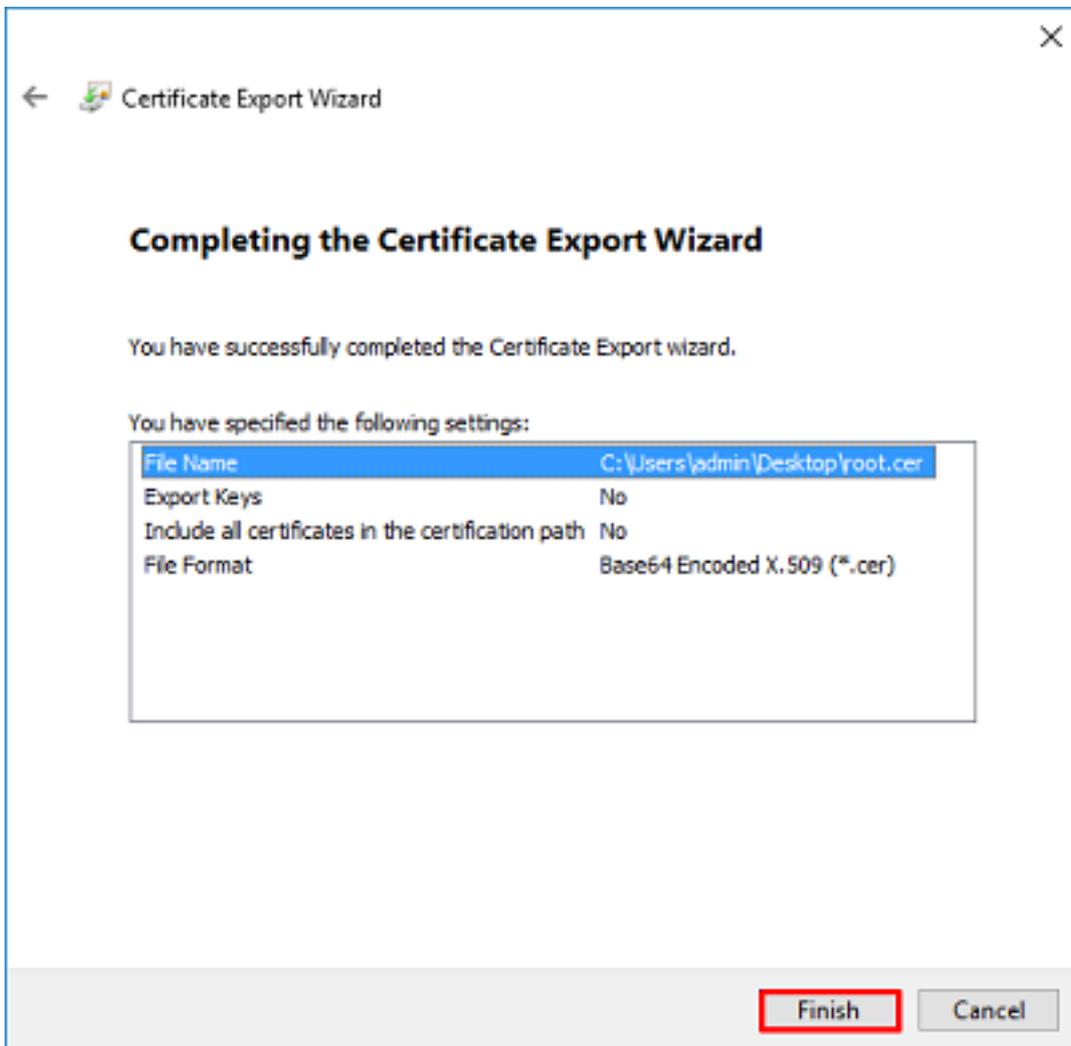


13.選擇檔案的名稱和匯出位置。





14. 按一下完成。



15.現在，導航到該位置，並使用記事本或其他文本編輯器開啟證書。這將顯示PEM格式證書。儲存以備以後使用。

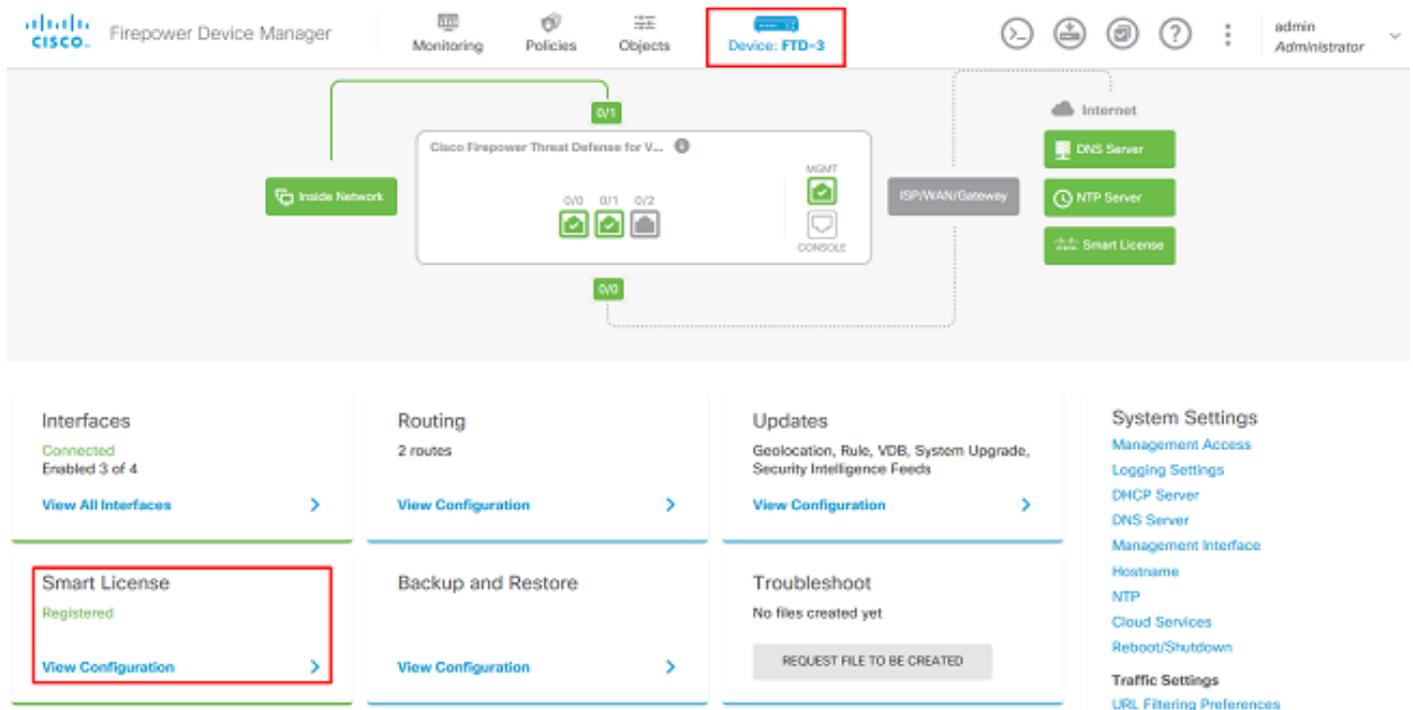
```
-----BEGIN CERTIFICATE-----
MIIDCCCAFcgAwIBAgIQE4ZG5Z1wT61ONTjooEQyMTANBgkqhkiG9w0BAQsFADAd
MRswGQYDVQQDEeJleGFtcGxlLVdJTjIwMTYtQ0EwIBcNMjAwNDI3MTQ1MDU5WhgP
MjA2MDA0MTkxNDUwNTlAMB0xGzAZBgNVBAMTEmV4YW1wbGUtV01OMjAxNi1DQTCC
ASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAl8ghT719NzSQpoQPh0YT67b
Ya+PngsxMyvkewP33QLTAWw1HW1Tb9Mk5BDWOItTaVsgHwPBfd++m+bLn3AiZnHV
OO+k6dVVY/E5qVkeKSGoY+v940S2316lzdWReMOFhgbc2qMertIoficrRihonuU
Cjyeub3CO+meJUuKom2R47C0D35TUvo/FEHGgXJFaJS1se2UrpNO7KEMkfAlLPuM
aob4XE/OzxYQpPa18djsNnskfcFqD/HOTFQN4+SrOhHWlRnUIQBuaLdQaabhipD/
sVs5PneYJX8YKma821uYI6j90YuytmsHBtCieyC062a8BKqOL7N86HFPfkMA3u8C
AwEAAaNCMEAwDgYDVR0PAQH/BAQDAgGMA8GA1UdEwEB/wQFMAMBAf8wHQYDVR0O
BBYEFD2fJjf7ER9EM/HCxCVFN5QzqEdvMA0GCSqGSIb3DQEBCwUAA4IBAQB31ZJo
vzwVD3c5Q1nrNP+6Mq62OFpYH91k4Ch9S5g/CEOemhcwg8MDIoxW2dTsjenAEt7r
phFIHzoCoSyjBjMgK3xybmoSeg8vBjCXseYNGEm0c9KW1oFmTOvdNVIb7Xp11IVa
6tALTt3ANRNgrEtXPA6yQbthKGavW0Anfsojk9IcDr2vp0MTj1BCxsTscubR1+d
dLEFKQqmMeYvkVf+a7a64mqPZsG3Uxo0rd6cZxAPkq/ylcdwNSJFFfQV3DgZg+R96
9WLCR30big6xyo9Zu+lixWpdrbADO6zMHbEYEHkh00jBrUEBBI6Cy83iTZ9ejsk
KgWBJXEu33PplW6E
-----END CERTIFICATE-----
```

FDM配置

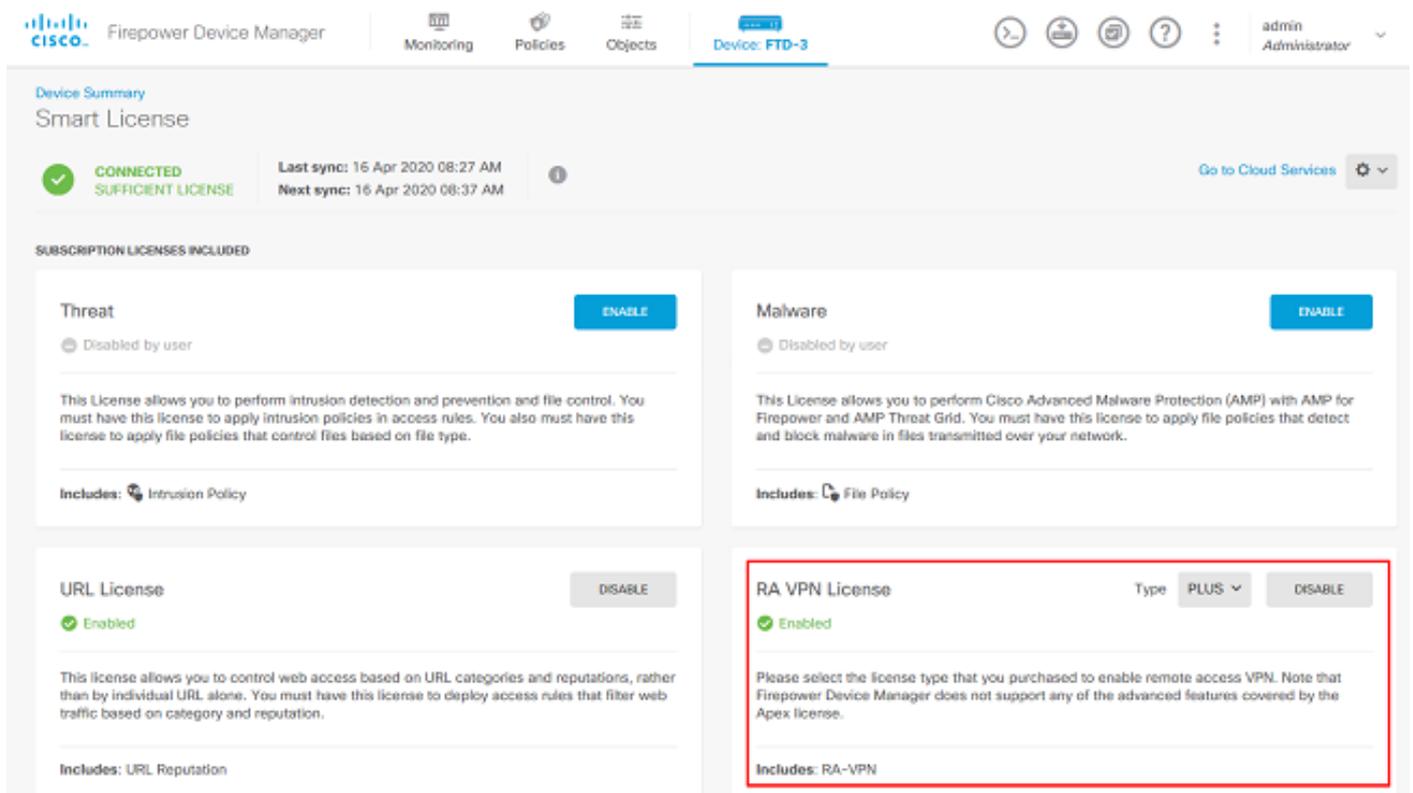
驗證許可

要在FDM上配置AnyConnect，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許可證。

1.導覽至Device > Smart License，如下圖所示。

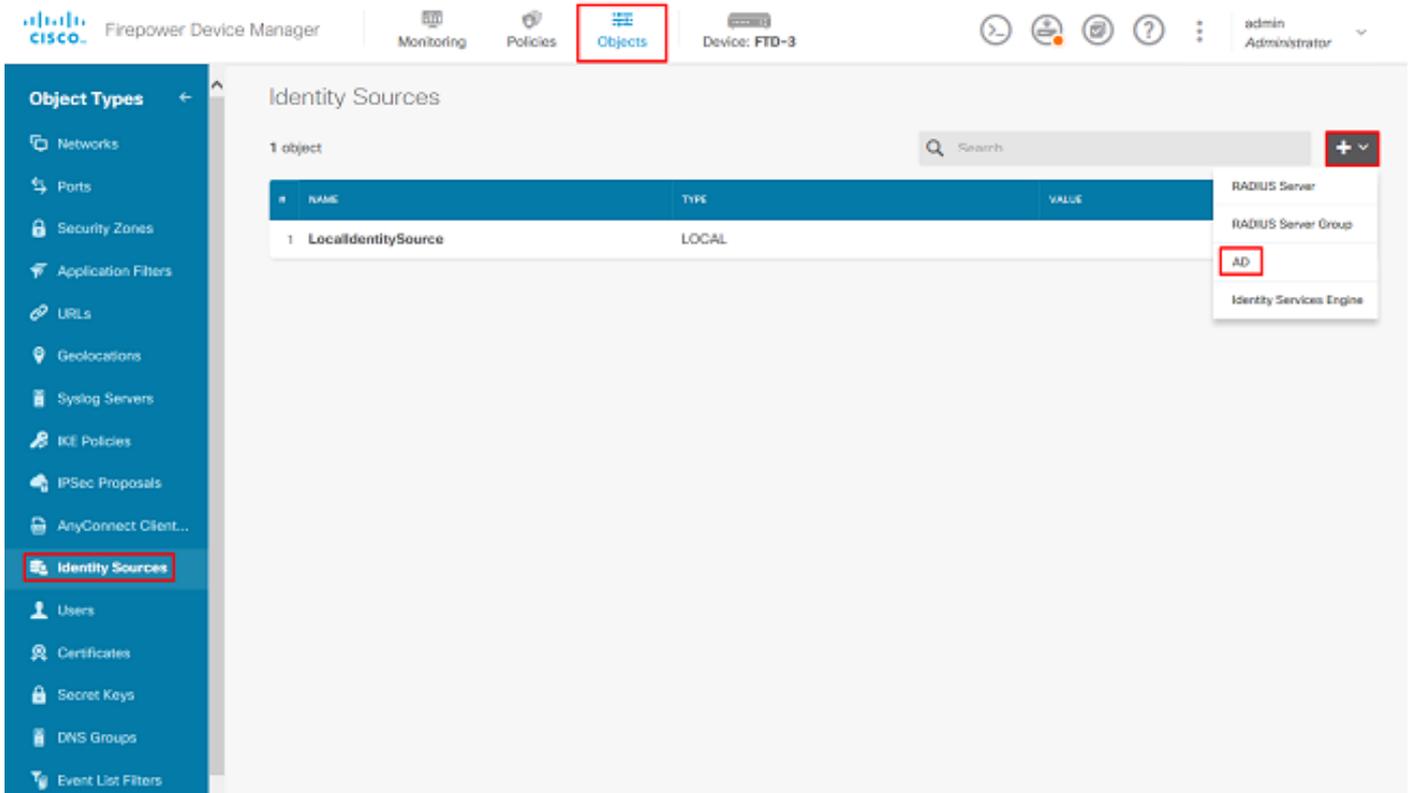


2.驗證FTD是否已註冊到智慧許可伺服器，以及是否已啟用AnyConnect Plus、Apex或VPN Only許可證。



設定AD身份源

1.導覽至對象>身份源，然後按一下+符號並選擇AD，如下圖所示。



2. 使用之前收集的資訊填充Active Directory伺服器的相應設定。如果為Microsoft伺服器使用主機名(FQDN)而不是IP地址，請確保在對象> DNS組下建立適當的DNS組。然後導航到Device > System Settings > DNS Server，然後在Management Interface和Data Interface下應用DNS組，即可將該DNS組應用到FTD，然後為DNS查詢指定適當的輸出介面。按一下Test按鈕以驗證是否成功設定以及是否可從FTD的管理介面連線。由於這些測試是從FTD的管理介面啟動，而不是通過FTD上設定的其中一個可路由介面（例如內部、外部、dmz）來啟動，因此成功（或失敗）的連線並不能保證AnyConnect驗證有相同的結果，因為AnyConnect LDAP驗證要求會從FTD的一個可路由介面啟動。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。

Add Identity Realm



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

Name

LAB-AD

Type

Active Directory (AD)

Directory Username

ftd.admin@example.com

e.g. user@example.com

Directory Password

••••••••

Base DN

DC=example,DC=com

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

AD Primary Domain

example.com

e.g. example.com

Directory Server Configuration

win2016.example.com:389

Hostname / IP Address

win2016.example.com

e.g. ad.example.com

Port

389

Encryption

NONE

Trusted CA certificate

Please select a certificate

TEST

✓ Connection to realm is successful

[Add another configuration](#)

CANCEL

OK

如果使用LDAPS或STARTTLS，請選擇適當的Encryption，然後選擇Trusted CA證書。如果尚未新增根CA，請按一下**Create New Trusted CA Certificate**。提供根CA證書的名稱，然後貼上之前收集的PEM格式根CA證書。

Add Trusted CA Certificate ? ✕

Name

LDAPS_ROOT

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

```

-----BEGIN CERTIFICATE-----
MIIDCCCAfCgAwIBAgIQE4ZG5Z1wT6IONTjooEQyMTANBgkqhkiG9w0BAQsFADAd
MRswGQYDVQQDEExJleGFtcG9uLmVudjJlMTYtQ0EwIENMjAwNDI3MTQ1MDU5WhgP
MjA2MDA0MTkxNDUwNTIaMB0xGzAZBgNVBAMTEmV4YW1wbGUtV0IOMjAxNi1DQTC
AShwDQYJKoZIhvcNAQEFBQADQgEPADCCAQoCggEFRAI8chT719NzS0ncOPh0YT67h

```

CANCEL OK

Directory Server Configuration

win2016.example.com:636 ▲

<p>Hostname / IP Address</p> <p style="border: 1px solid #ccc; padding: 2px;">win2016.example.com</p> <p><small>e.g. ad.example.com</small></p>	<p>Port</p> <p style="border: 1px solid #ccc; padding: 2px;">636</p>
<p>Encryption</p> <p style="border: 1px solid #ccc; padding: 2px;">LDAPS ▼</p>	<p>Trusted CA certificate</p> <p style="border: 1px solid #ccc; padding: 2px;">LDAPS_ROOT ▼</p>

TEST ✔ Connection to realm is successful

在此配置中，使用以下值：

- 名稱:LAB-AD
- 目錄使用者名稱：ftd.admin@example.com
- 基本DN:DC=example，DC=com
- AD主域：example.com
- 主機名/IP地址：win2016.example.com
- 連接埠:389

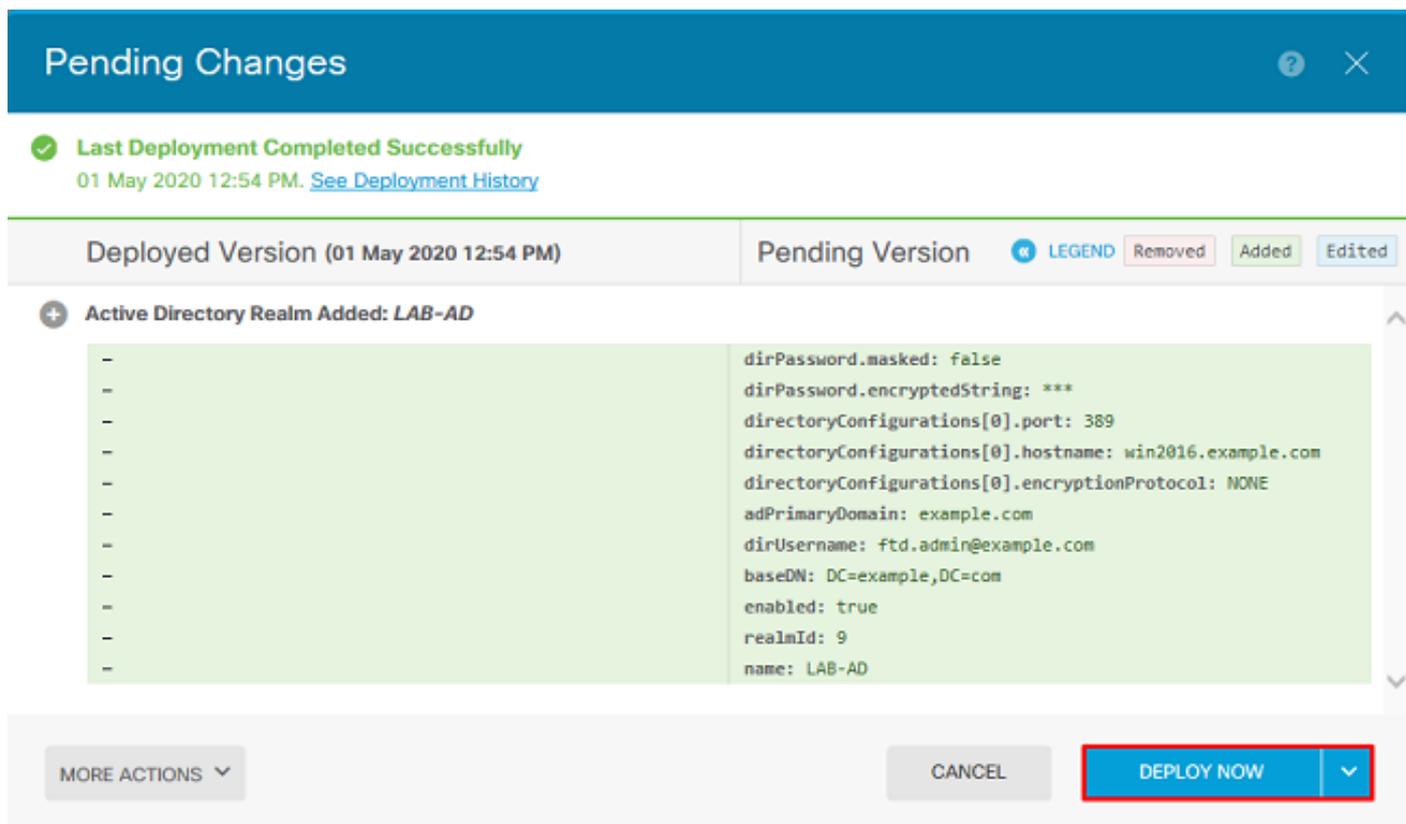
3.按一下右上角的「待定更改」按鈕，如下圖所示。

The screenshot shows the Cisco Firepower Device Manager interface. The top navigation bar includes 'Monitoring', 'Policies', 'Objects', and 'Device: FTD-3'. The 'Objects' tab is active. On the left, a sidebar shows 'Object Types' with categories like Networks, Ports, Security Zones, and Application Filters. The main content area is titled 'Identity Sources' and shows a table with 2 objects:

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

A red box highlights the 'Pending Changes' icon (a red circle with a white exclamation mark) in the top right corner of the interface.

4. 按一下Deploy Now按鈕。



Pending Changes

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

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

+ Active Directory Realm Added: LAB-AD

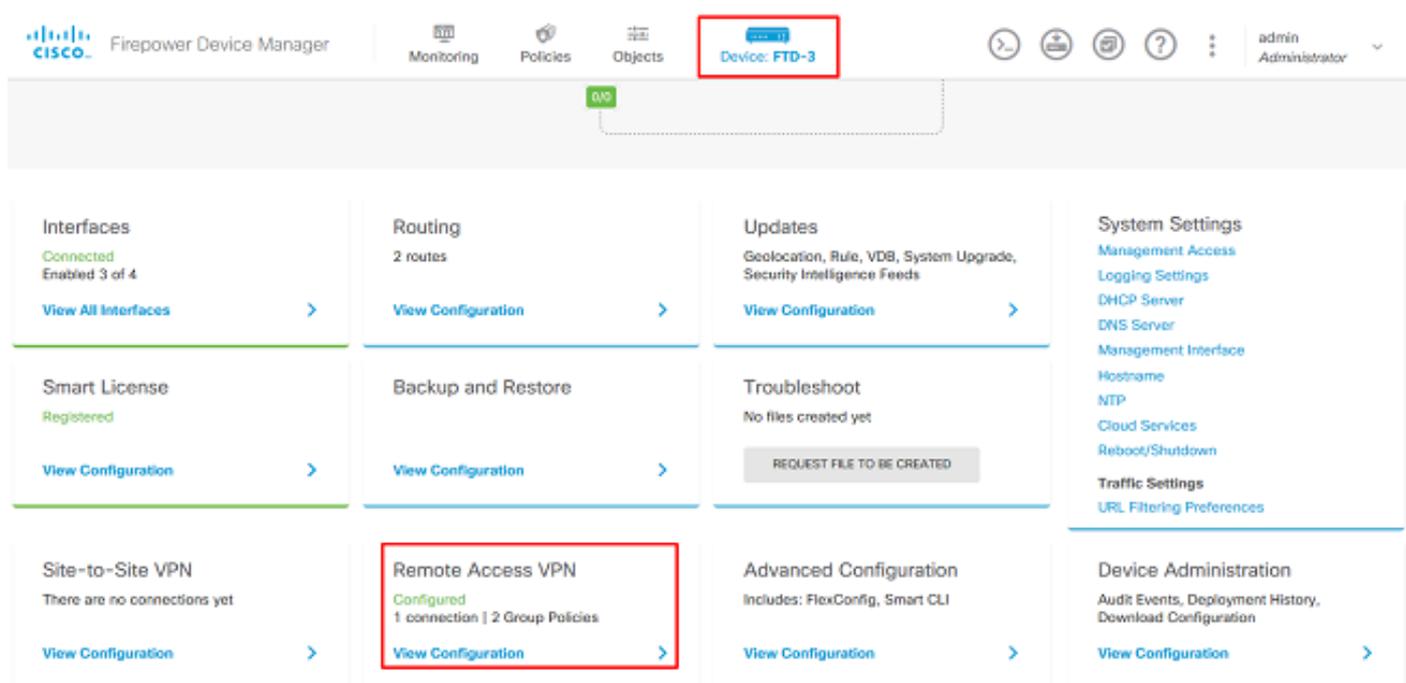
```
dirPassword.masked: false
dirPassword.encryptedString: ***
directoryConfigurations[0].port: 389
directoryConfigurations[0].hostname: win2016.example.com
directoryConfigurations[0].encryptionProtocol: NONE
adPrimaryDomain: example.com
dirUsername: ftd.admin@example.com
baseDN: DC=example,DC=com
enabled: true
realmId: 9
name: LAB-AD
```

MORE ACTIONS ▼ CANCEL DEPLOY NOW ▼

配置AnyConnect進行AD身份驗證

要使用配置的AD身份源，需要將其應用到AnyConnect配置。

1. 導覽至Device > Remote Access VPN，如下圖所示。



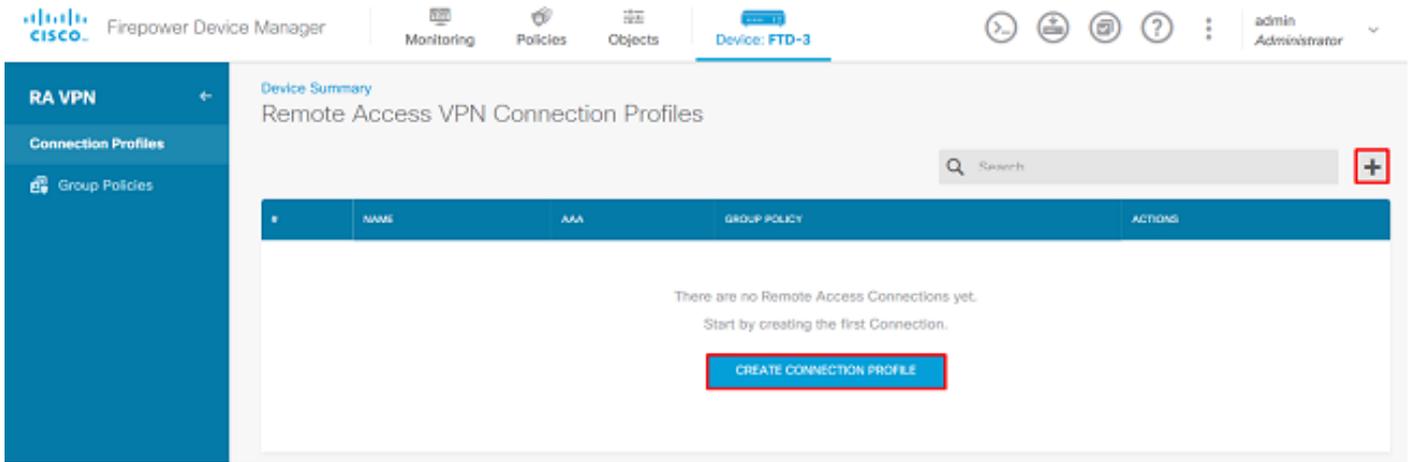
Cisco Firepower Device Manager

Monitoring Policies Objects Device: FTD-3

0/0

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

2. 按一下+符號或Create Connection Profile按鈕，如下圖所示。



3.在「連線和客戶端配置」部分下，選擇之前建立的AD身份源。為包括連線配置檔名稱和客戶端地址池分配在內的其他部分設定適當的值。完成後按一下**Submit Query**。

Connection and Client Configuration

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

Connection Profile Name

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

General

Group Alias: General

Group URL: [Empty]

[Add Group Alias](#) [Add Group URL](#)

Primary Identity Source

Authentication Type

AAA Only | Client Certificate Only | AAA and Client Certificate

Primary Identity Source for User Authentication

Filter: [Dropdown]

- LocalIdentitySource
- LAB-AD** (highlighted with a red box)
- Special-Identities-Realm

[Create new](#)

Fallback Local Identity Source ⚠

Please Select Local Identity Source [Dropdown]

Client Address Pool Assignment

IPv4 Address Pool

Endpoints are provided an address from this pool



AnyConnect-Pool

IPv6 Address Pool

Endpoints are provided an address from this pool



DHCP Servers



CANCEL

SUBMIT QUERY

4.在「遠端使用者體驗」部分下，選擇適當的組策略。預設情況下，將使用DfltGrpPolicy;但是，可以建立另一個模板。

DfltGrpPolicy

Policy Group Brief Details

DNS + BANNER		Edit
DNS Server	None	
Banner Text for Authenticated Clients	None	
SESSION SETTINGS		
Maximum Connection Time / Alert Interval	Unlimited / 1 Minutes	
Idle Time / Alert Interval	30 / 1 Minutes	
Simultaneous Login per User	3	
SPLIT TUNNELING		
IPv4 Split Tunneling	Allow all traffic over tunnel	
IPv6 Split Tunneling	Allow all traffic over tunnel	
ANYCONNECT CLIENT		
AnyConnect Client Profiles	None	

BACK

SUBMIT QUERY

5.在「全域性設定」部分下，至少指定SSL證書、外部介面和AnyConnect包。如果之前未建立證書，可以選擇預設自簽名證書([DefaultInternalCertificate](#))，但是會看到不受信任的伺服器證書消息。應取消選中解密流量的旁路訪問控制策略(sysopt permit-vpn)，以便使用者身份訪問策略規則稍後生效。此處也可以配置NAT豁免。在此配置中，從內部介面到AnyConnect客戶端IP地址的所有ipv4流量均來自NAT。對於更複雜的設定（例如外部到外部髮夾），需要根據NAT策略建立其他NAT規則。AnyConnect軟體包可在思科支援站點找到：<https://software.cisco.com/download/home>。需要有效的Plus或Apex許可證才能下載AnyConnect軟體包。

Global Settings

These settings control the basic functioning of the connection. Changes to any of these options apply to all connection profiles; you cannot configure different settings in different profiles.

Certificate of Device Identity

FTD-3-Manual

Outside Interface

outside (GigabitEthernet0/0)

Fully-qualified Domain Name for the Outside Interface

ftd3.example.com

e.g. ravpn.example.com

Access Control for VPN Traffic

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

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

NAT Exempt



Inside Interfaces

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



inside (GigabitEthernet0/1)

Inside Networks

The internal networks remote access VPN users are allowed to use. The IP versions of the internal networks and address pools must match, either IPv4, IPv6, or both.



any-ipv4

AnyConnect Package

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

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

You must have the necessary AnyConnect software license.

Packages

UPLOAD PACKAGE

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

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

BACK

NEXT

6.在「摘要」部分下，驗證AnyConnect是否設定正確，然後按一下提交查詢。

^ Summary

Review the summary of the Remote Access VPN configuration.

General

STEP 1: CONNECTION AND CLIENT CONFIGURATION

Primary Identity Source

Authentication Type AAA Only

Primary Identity Source LAB-AD

Fallback Local Identity Source -

Strip Identity Source server from username No

Strip Group from Username No

Secondary Identity Source

Secondary Identity Source for User Authentication -

Fallback Local Identity Source -

Advanced

Authorization Server

Accounting Server

Client Address Pool Assignment

IPv4 Address Pool

BACK SUBMIT QUERY

7.按一下右上角的「待決更改」按鈕，如下圖所示。

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

RA VPN

Connection Profiles

Group Policies

Device Summary

Remote Access VPN Connection Profiles

1 object

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

8.按一下立即部署。

Pending Changes

?
✕
Close

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

Deployed Version (16 Apr 2020 12:41 PM)	Pending Version																										
<div style="background-color: #e6f2ff; padding: 5px; border: 1px solid #0070C0; margin-bottom: 5px;"> + Network Object Added: AnyConnect-Pool </div> <table border="1" style="width: 100%; border-collapse: collapse;"> <tr><td style="width: 50%; padding: 2px;">-</td><td style="padding: 2px;">subType: Network</td></tr> <tr><td style="padding: 2px;">-</td><td style="padding: 2px;">value: 10.10.10.0/24</td></tr> <tr><td style="padding: 2px;">-</td><td style="padding: 2px;">isSystemDefined: false</td></tr> <tr><td style="padding: 2px;">-</td><td style="padding: 2px;">dnsResolution: IPV4_AND_IPV6</td></tr> <tr><td style="padding: 2px;">-</td><td style="padding: 2px;">name: AnyConnect-Pool</td></tr> </table>		-	subType: Network	-	value: 10.10.10.0/24	-	isSystemDefined: false	-	dnsResolution: IPV4_AND_IPV6	-	name: AnyConnect-Pool																
-	subType: Network																										
-	value: 10.10.10.0/24																										
-	isSystemDefined: false																										
-	dnsResolution: IPV4_AND_IPV6																										
-	name: AnyConnect-Pool																										
<div style="background-color: #e6f2ff; padding: 5px; border: 1px solid #0070C0; margin-bottom: 5px;"> + RA VPN Added: NGFW-Remote-Access-VPN </div> <table border="1" style="width: 100%; border-collapse: collapse;"> <tr><td style="width: 50%; padding: 2px;">-</td><td style="padding: 2px;">vpnGatewaySettings[0].exemptNatRule: true</td></tr> <tr><td style="padding: 2px;">-</td><td style="padding: 2px;">vpnGatewaySettings[0].outsideFqdn: ftd3.example.com</td></tr> <tr><td style="padding: 2px;">-</td><td style="padding: 2px;">vpnGatewaySettings[0].bypassAccessControlForVPNTraffic: t...</td></tr> <tr><td style="padding: 2px;">-</td><td style="padding: 2px;">name: NGFW-Remote-Access-VPN</td></tr> <tr><td style="padding: 2px;">anyconnectPackageFiles:</td><td></td></tr> <tr><td style="padding: 2px;">-</td><td style="padding: 2px;">anyconnect-win-4.7.03052-webdeploy-k9.pkg</td></tr> <tr><td style="padding: 2px;">vpnGatewaySettings[0].serverCertificate:</td><td></td></tr> <tr><td style="padding: 2px;">-</td><td style="padding: 2px;">FTD-3-Manual</td></tr> <tr><td style="padding: 2px;">vpnGatewaySettings[0].outsideInterface:</td><td></td></tr> <tr><td style="padding: 2px;">-</td><td style="padding: 2px;">outside</td></tr> <tr><td style="padding: 2px;">vpnGatewaySettings[0].insideInterfaces:</td><td></td></tr> <tr><td style="padding: 2px;">-</td><td style="padding: 2px;">inside</td></tr> <tr><td style="padding: 2px;">vpnGatewaySettings[0].insideNetworks:</td><td></td></tr> </table>		-	vpnGatewaySettings[0].exemptNatRule: true	-	vpnGatewaySettings[0].outsideFqdn: ftd3.example.com	-	vpnGatewaySettings[0].bypassAccessControlForVPNTraffic: t...	-	name: NGFW-Remote-Access-VPN	anyconnectPackageFiles:		-	anyconnect-win-4.7.03052-webdeploy-k9.pkg	vpnGatewaySettings[0].serverCertificate:		-	FTD-3-Manual	vpnGatewaySettings[0].outsideInterface:		-	outside	vpnGatewaySettings[0].insideInterfaces:		-	inside	vpnGatewaySettings[0].insideNetworks:	
-	vpnGatewaySettings[0].exemptNatRule: true																										
-	vpnGatewaySettings[0].outsideFqdn: ftd3.example.com																										
-	vpnGatewaySettings[0].bypassAccessControlForVPNTraffic: t...																										
-	name: NGFW-Remote-Access-VPN																										
anyconnectPackageFiles:																											
-	anyconnect-win-4.7.03052-webdeploy-k9.pkg																										
vpnGatewaySettings[0].serverCertificate:																											
-	FTD-3-Manual																										
vpnGatewaySettings[0].outsideInterface:																											
-	outside																										
vpnGatewaySettings[0].insideInterfaces:																											
-	inside																										
vpnGatewaySettings[0].insideNetworks:																											

MORE ACTIONS ▼

CANCEL

DEPLOY NOW
▼

啟用身份策略並為使用者身份配置安全策略

此時，AnyConnect使用者應該能夠成功連線，但可能無法訪問特定資源。此步驟將啟用使用者身份，以便只有AnyConnect管理員中的使用者才能使用RDP連線到內部資源，並且只有組AnyConnect使用者中的使用者才能使用HTTP連線到內部資源。

1. 導航到 **Policies > Identity**，然後點選 **Enable Identity Policy**。

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

Security Policies

SSL Decryption → **Identity** → Security Intelligence → NAT → Access Control → Intrusion

Establishing User Identity

You can use identity policies to collect user identity information from connections. You can then view usage based on user identity in the dashboards, and configure access control based on user or user group. By linking network behavior, traffic, and events directly to individual users, the system can help you identify the source of policy breaches, attacks, or network vulnerabilities.

How Identity policies work

Passive authentication | Active authentication

USERS → PASSIVE AUTHENTICATION → LEVERAGE IDENTITY

MULTIPLE IDENTITIES → IDENTITY SOURCES → PASSIVE AUTHENTICATION

ENABLE IDENTITY POLICY

對於此配置，不需要進一步的配置，並且預設操作就足夠了。

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

Security Policies

SSL Decryption → **Identity** → Security Intelligence → NAT → Access Control → Intrusion

Identity Policy

Search

#	NAME	AUTHENTICATION	AUTH. TYPE	SOURCE			DESTINATION			ACTIONS
				ZONES	NETWORKS	PORTS	ZONES	NETWORKS	PORTS/PROTO...	
There are no Identity rules yet. Start by creating the first identity rule.										
CREATE IDENTITY RULE										

Default Action: **Passive Auth** | Any Identity Source

2. 導航到 **Policies > NAT**，確保正確配置 NAT。如果 AnyConnect 設定中配置的 NAT 異常足夠，則無需在此進行其他配置。

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

Security Policies

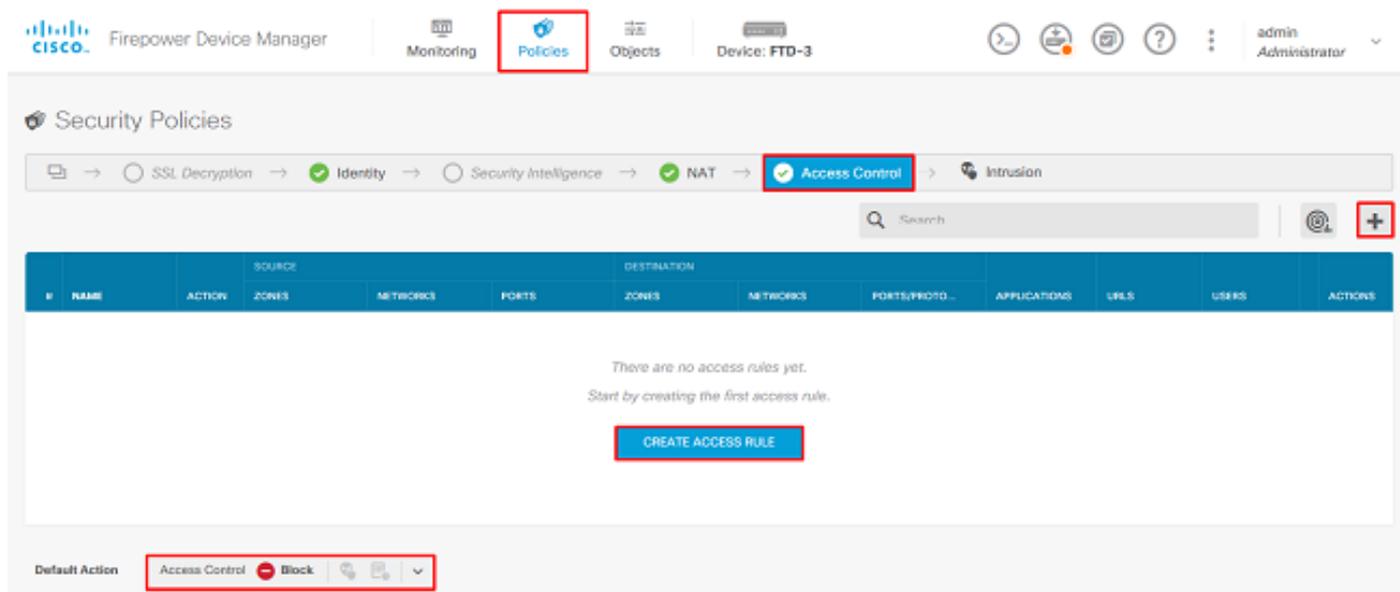
SSL Decryption → **Identity** → Security Intelligence → **NAT** → Access Control → Intrusion

1 rule

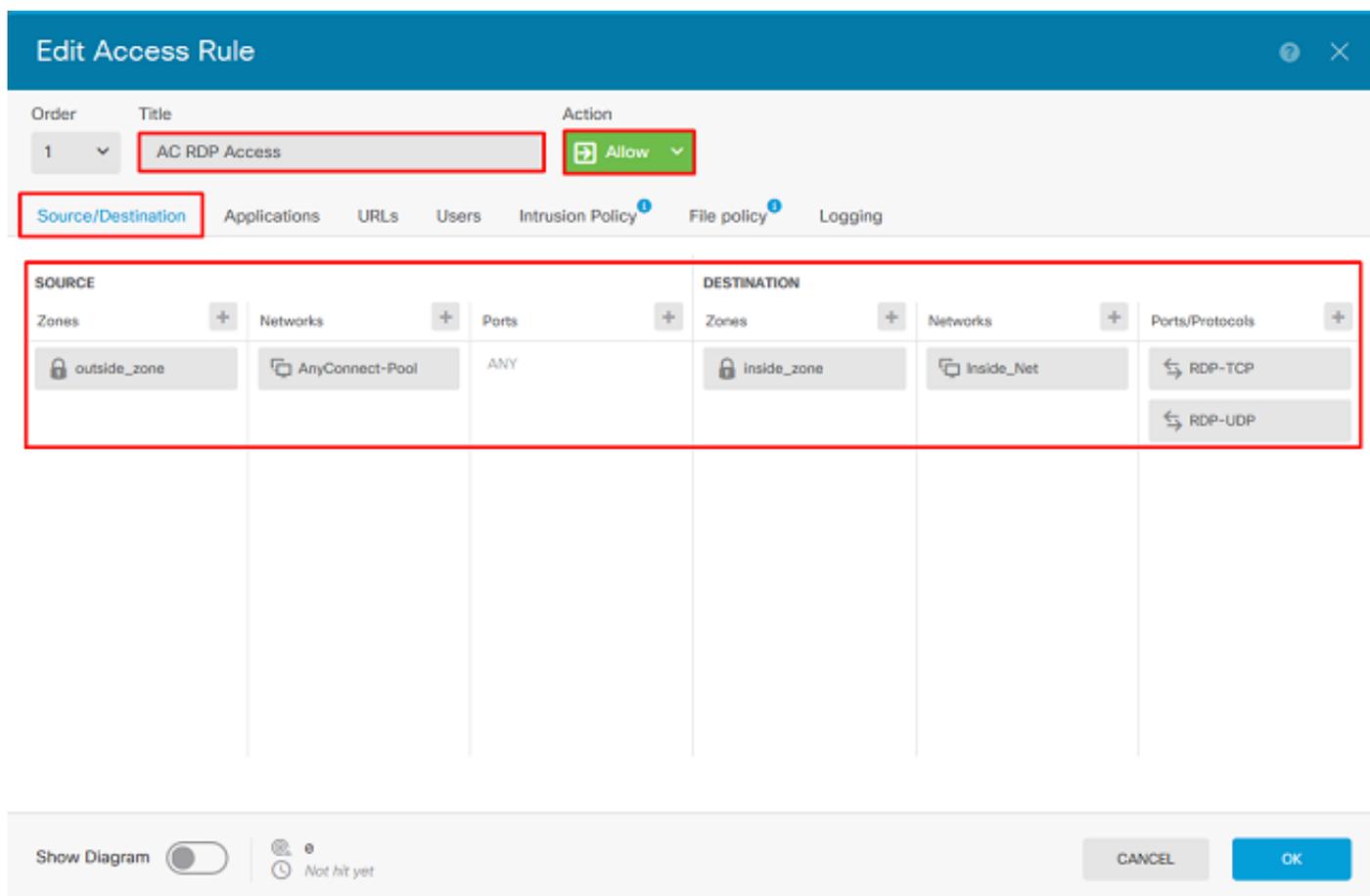
Search

#	NAME	TYPE	INTERFACES	ORIGINAL PACKET			TRANSLATED PACKET				ACTIONS	
				SOURCE AD...	DESTINATIO...	SOURCE PORT	DESTINATIO...	SOURCE AD...	DESTINATIO...	SOURCE PORT		DESTINATIO...
Auto NAT Rules												
>	#	Internet_PAT	DYNAMIC	ANY outside	any-ipv4	ANY	ANY	ANY	Interface	ANY	ANY	ANY

3.定位至**策略>訪問控制**。在本節中，Default Action設定為Block，並且未建立任何訪問規則，因此一旦AnyConnect使用者連線，他們將無法訪問任何內容。按一下+符號或Create Access Rule新增規則。



4.使用適當的值填寫欄位。在此配置中，AnyConnect Admins組內的使用者應該對內部網路中的Windows Server具有RDP訪問許可權。對於源，區域配置為outside_zone，這是AnyConnect使用者將要連線的外部介面，網路配置為AnyConnect-Pool對象，該對象之前配置為將IP地址分配給AnyConnect客戶端。對於FDM中的使用者身份，源必須是使用者將從中啟動連線的區域和網路。對於目標，區域配置為inside_zone（即Windows Server所在的內部介面），網路配置為Inside_Net對象（即定義Windows Server所在子網的對象），埠/協定設定為兩個自定義埠對象，以允許通過TCP 3389和UDP 3389進行RDP訪問。



在Users部分下，將新增組AnyConnect Admins，以便允許此組以外的使用者對Windows Server進行RDP訪問。按一下+符號，按一下「組」(Groups)頁籤，按一下相應的組，然後按一下「確定」(OK)。請注意，也可以選擇單個使用者和身份源。

The screenshot shows the 'Add Access Rule' dialog box. At the top, there is a table with columns 'Order', 'Title', and 'Action'. The first row shows '1' in the Order column, 'AC RDP Access' in the Title column, and 'Allow' in the Action column. Below the table, there are tabs for 'Source/Destination', 'Applications', 'URLs', 'Users', 'Intrusion Policy', 'File policy', and 'Logging'. The 'Users' tab is selected and highlighted with a red box. Under the 'Users' tab, there is a sub-tab 'Groups' which is also highlighted with a red box. Below the sub-tab, there is a list of available users and groups. The group 'LAB-AD \ AnyConnect Admins' is selected and highlighted with a red box. At the bottom of the dialog box, there are buttons for 'Create new Identity Realm', 'CANCEL', and 'OK'. The 'OK' button is highlighted with a red box.

選擇適當的選項後，按一下**確定**。

Add Access Rule

Order	Title	Action
1	AC RDP Access	Allow

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

AVAILABLE USERS +

- LAB-AD \ AnyConnect Admins

CONTROLLING ACCESS FOR USERS AND USER GROUPS

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

Show Diagram

CANCEL OK

5. 根據需要建立更多訪問規則。在此配置中，將建立另一個訪問規則，以允許AnyConnect使用者組中的使用者通過HTTP訪問Windows Server。

Edit Access Rule

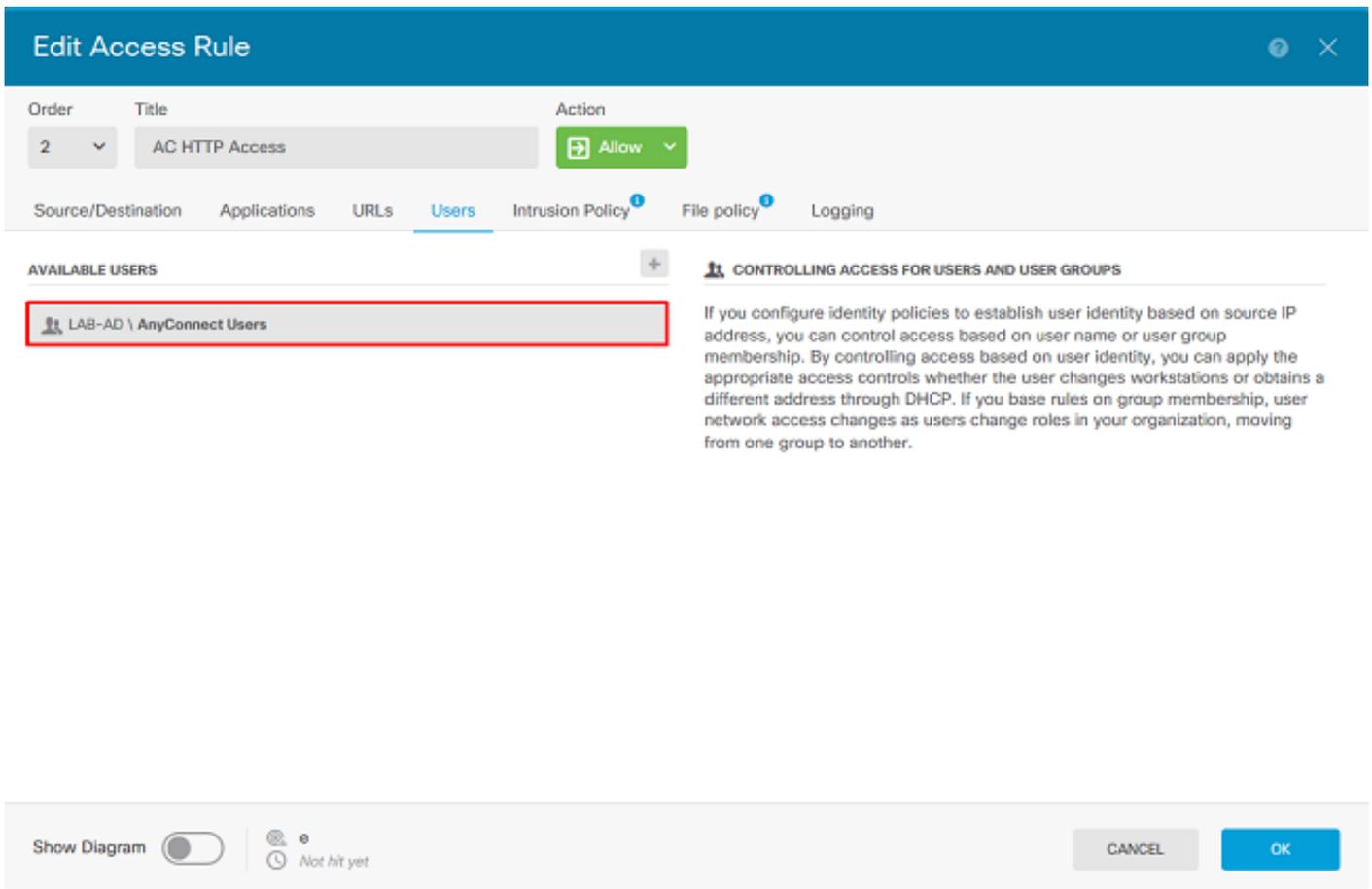
Order	Title	Action
2	AC HTTP Access	Allow

Source/Destination Applications URLs Users Intrusion Policy File policy Logging

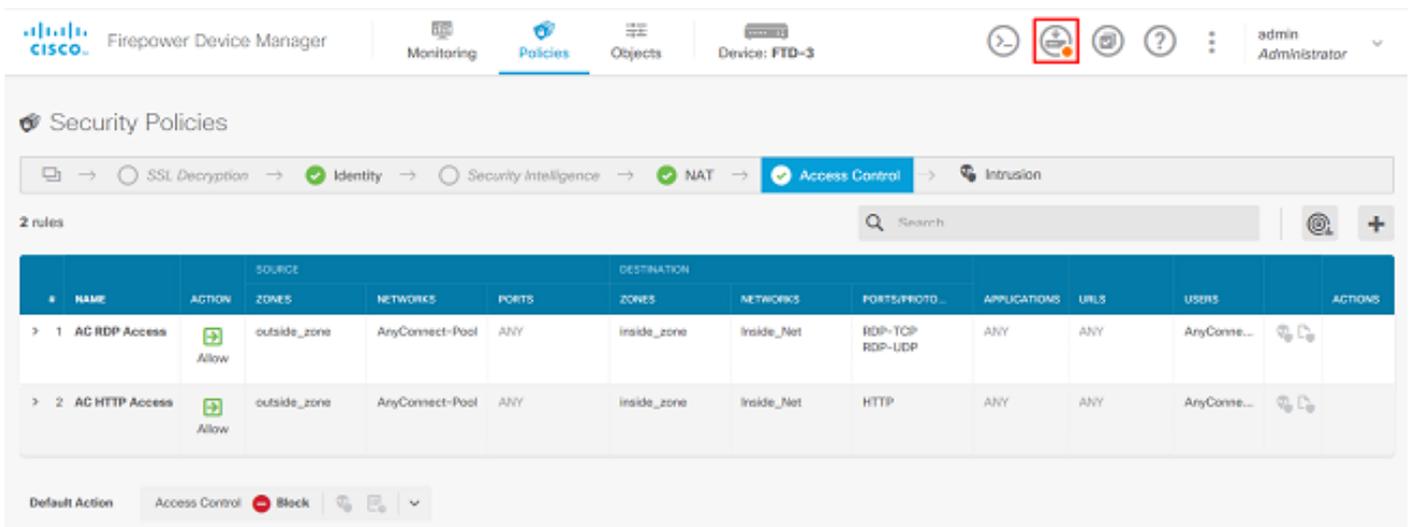
SOURCE			DESTINATION		
Zones	Networks	Ports	Zones	Networks	Ports/Protocols
outside_zone	AnyConnect-Pool	ANY	inside_zone	Inside_Net	HTTP

Show Diagram Not hit yet

CANCEL OK



6. 驗證訪問規則配置，然後按一下右上角的Pending Changes按鈕，如下圖所示。



7. 驗證更改，然後按一下Deploy Now。

Pending Changes



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

Deployed Version (28 Apr 2020 01:35 PM)

Pending Version

LEGEND

Removed

Added

Edited

+ Access Rule Added: AC HTTP Access

-	users[0].name: AnyConnect Users
-	logFiles: false
-	eventLogAction: LOG_NONE
-	ruleId: 268435467
-	name: AC HTTP Access
sourceZones:	
-	outside_zone
destinationZones:	
-	inside_zone
sourceNetworks:	
-	AnyConnect-Pool
destinationNetworks:	
-	Inside_Net
destinationPorts:	
-	HTTP
users[0].identitySource:	
-	LAB-AD

+ Access Rule Added: AC RDP Access

MORE ACTIONS ▾

CANCEL

DEPLOY NOW ▾

驗證

使用本節內容，確認您的組態是否正常運作。

最終配置

AAA組態

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

配置AnyConnect

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

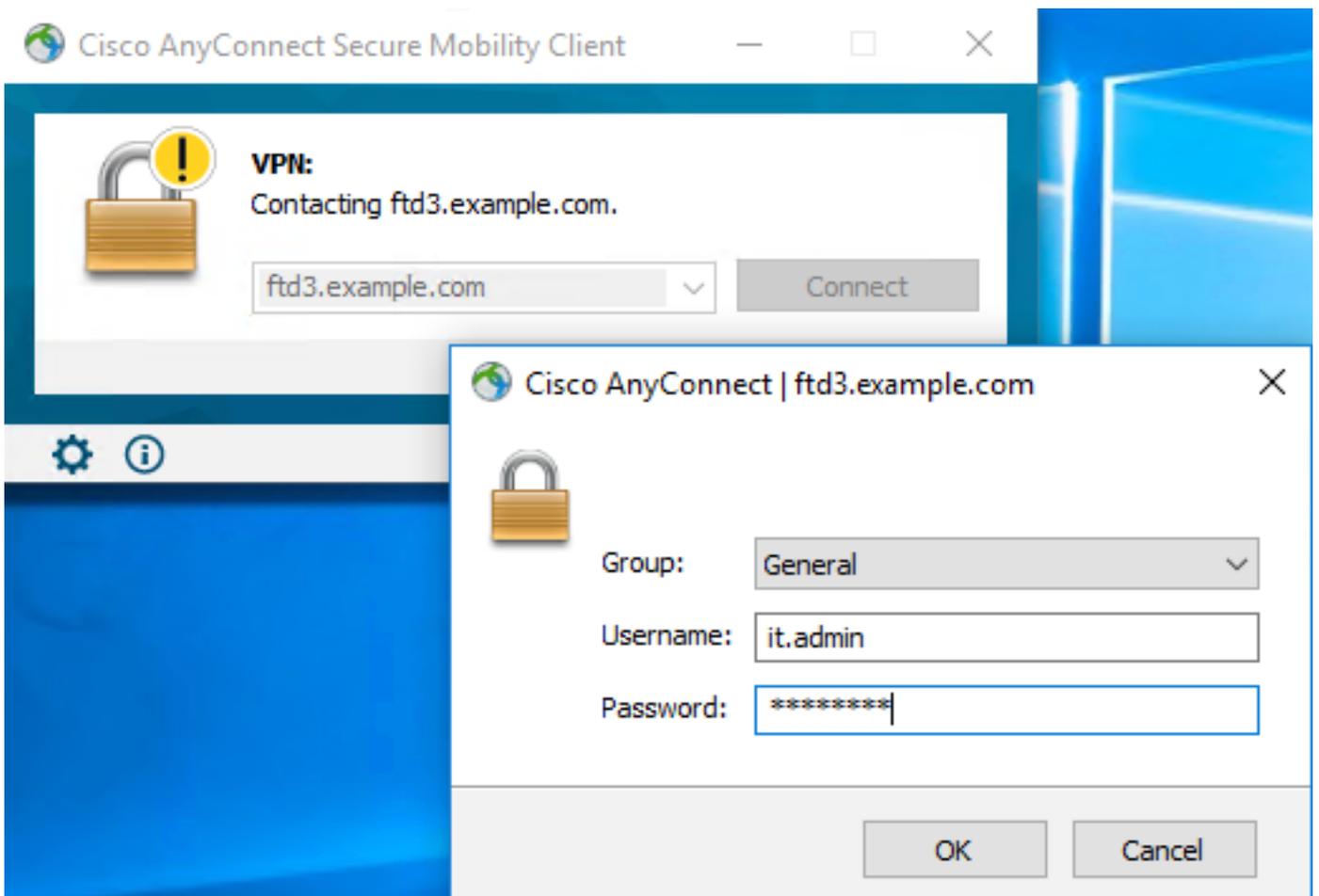
```
hsts-client
  enable
x-content-type-options
x-xss-protection
content-security-policy
anyconnect image disk0:/anyconnpkgs/anyconnect-linux64-4.7.03052-webdeploy-k9.pkg 1
anyconnect image disk0:/anyconnpkgs/anyconnect-win-4.7.03052-webdeploy-k9.pkg 2
anyconnect enable
tunnel-group-list enable
cache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

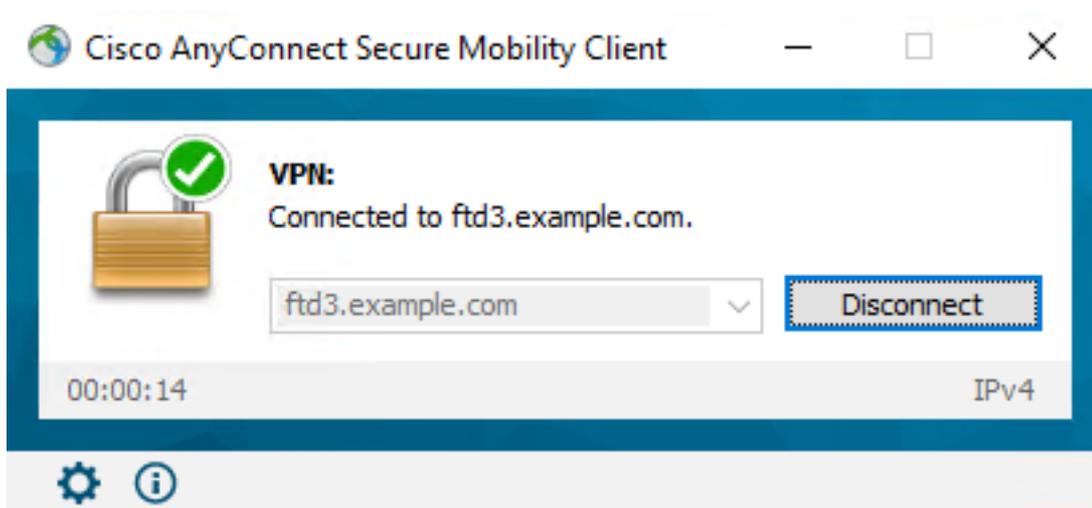
> show running-config tunnel-group
tunnel-group General type remote-access
tunnel-group General general-attributes
  address-pool AnyConnect-Pool
  authentication-server-group LAB-AD
tunnel-group General webvpn-attributes
  group-alias General enable

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

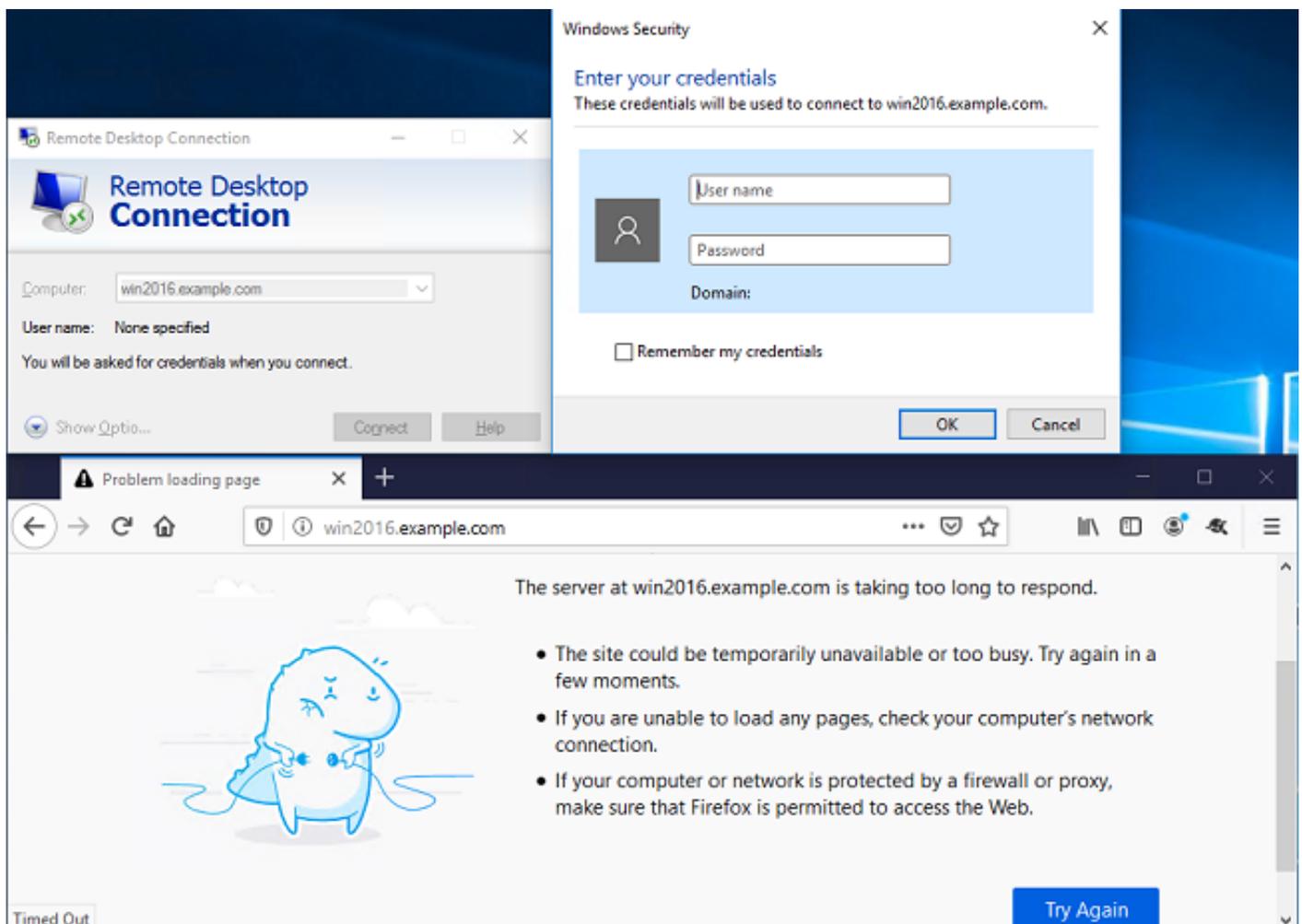
> show running-config ssl
ssl trust-point FTD-3-Manual outside
```

使用AnyConnect連線並驗證訪問控制策略規則

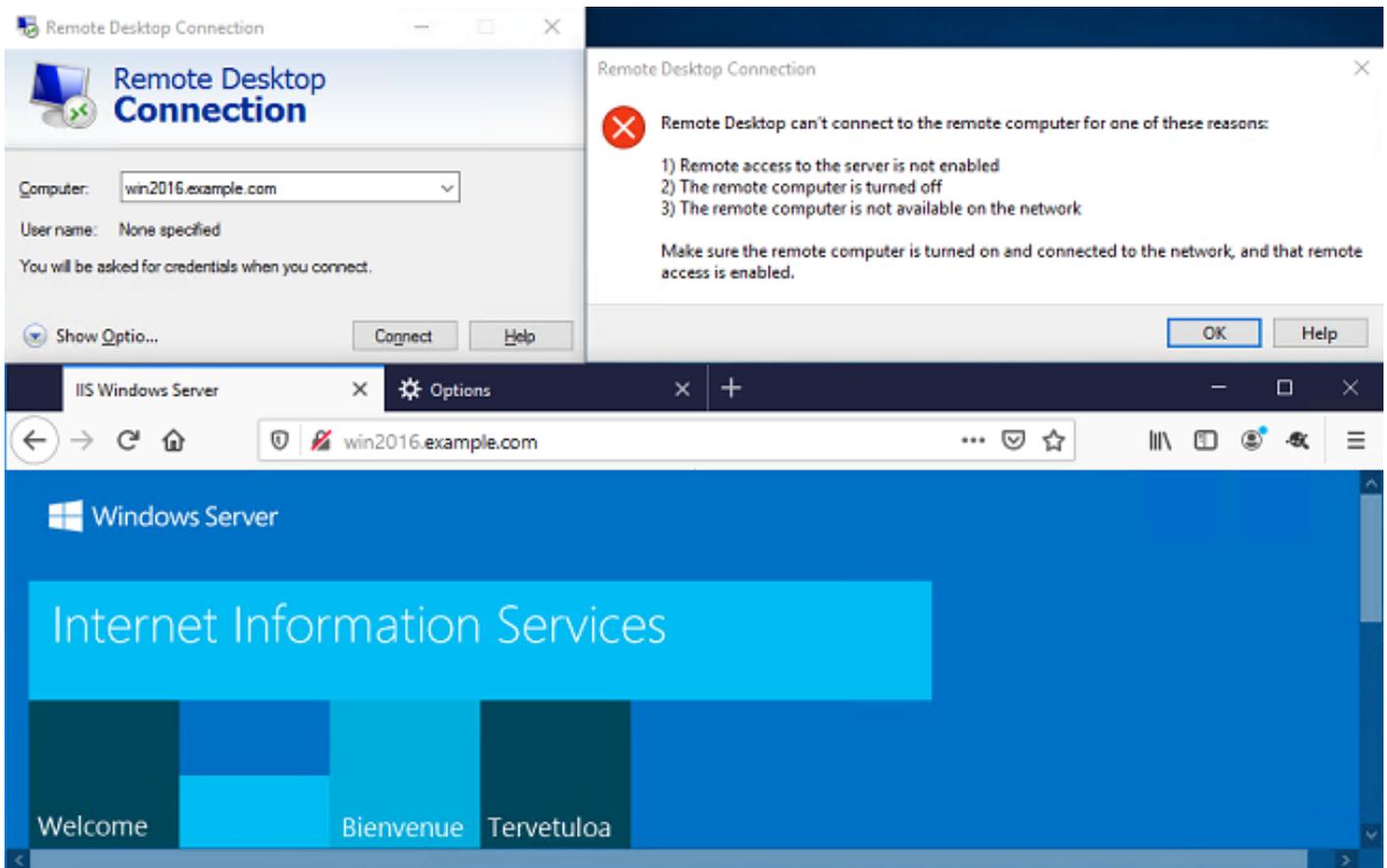




使用者IT Admin位於對Windows Server具有RDP訪問許可權的AnyConnect Admins組中，但是沒有對HTTP的訪問許可權。開啟與此伺服器的RDP和Firefox會話將驗證此使用者只能通過RDP訪問伺服器。



如果以組中的AnyConnect使用者（該使用者具有HTTP訪問許可權但沒有RDP訪問許可權）中的測試使用者登入，則可以驗證訪問控制策略規則是否生效。



疑難排解

使用本節內容，確認您的組態是否正常運作。

調試

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

為了排查使用者身份訪問控制策略問題，可以秘密運行`system support firewall-engine-debug`，以確定流量被允許或意外阻止的原因。

工作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...;.....}...
[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伺服器的回應。

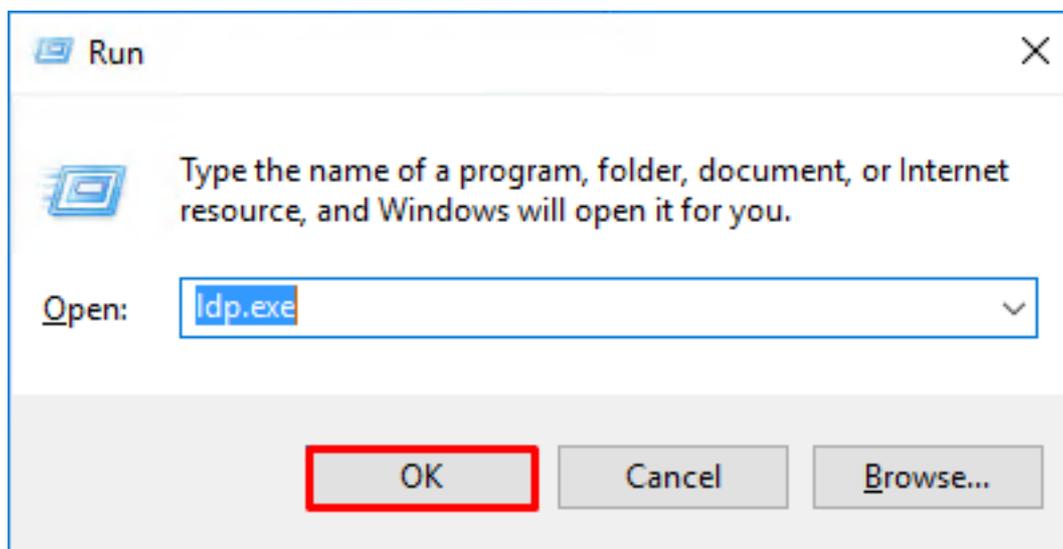
- 如果使用LDAPS或STARTTLS，請確保信任正確的根CA證書，以成功完成SSL握手。
- 驗證使用了正確的IP地址和埠。如果使用主機名，請驗證DNS是否能夠將其解析為正確的IP地址

繫結登入DN和/或密碼不正確

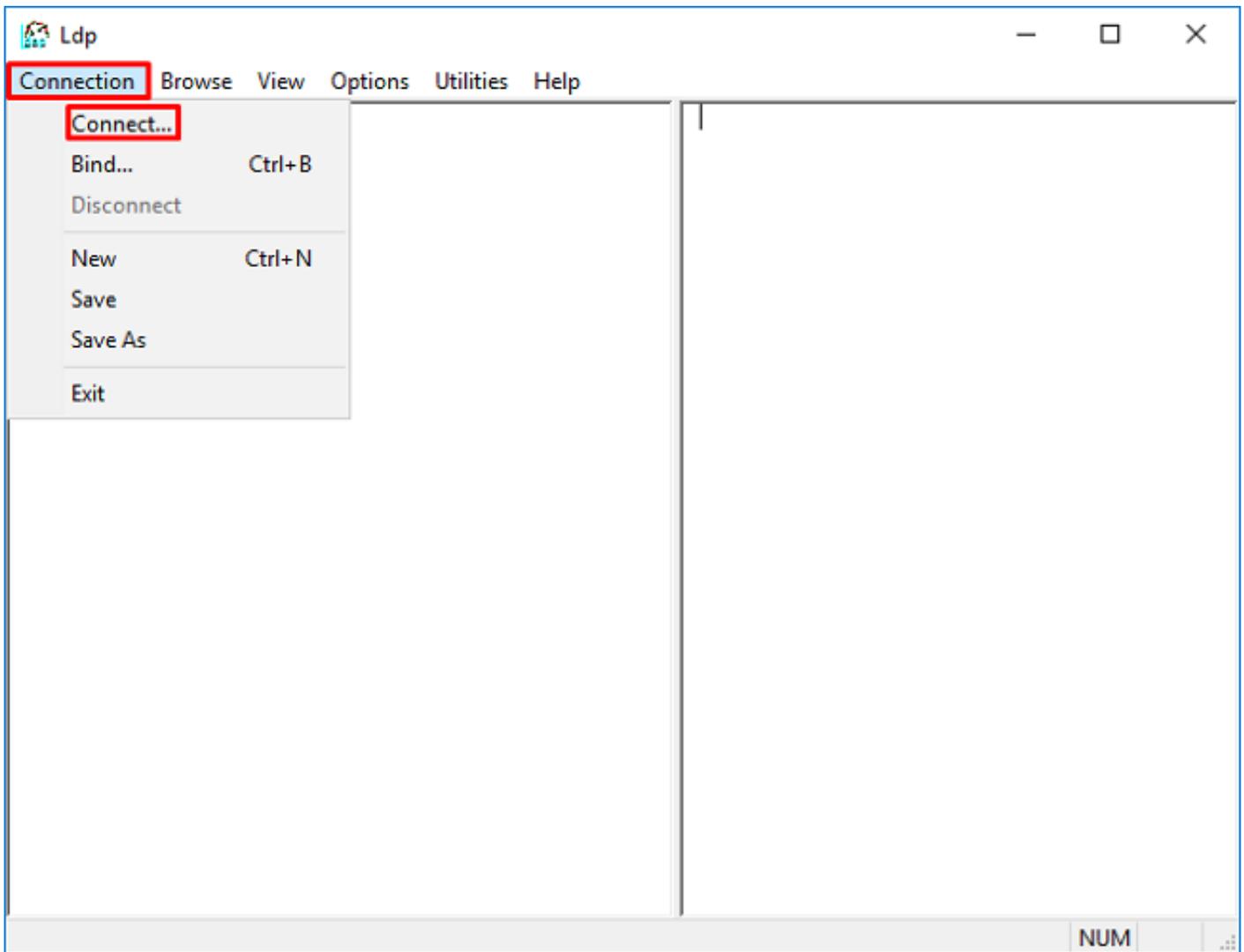
```
[ -2147483615] Session Start
[ -2147483615] New request Session, context 0x00007f9e65ccdc40, reqType = Authentication
[ -2147483615] Fiber started
[ -2147483615] Creating LDAP context with uri=ldap://192.168.1.1:389
[ -2147483615] Connect to LDAP server: ldap://192.168.1.1:389, status = Successful
[ -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：確認登入DN和登入密碼是否正確設定。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，請瀏覽以下步驟：

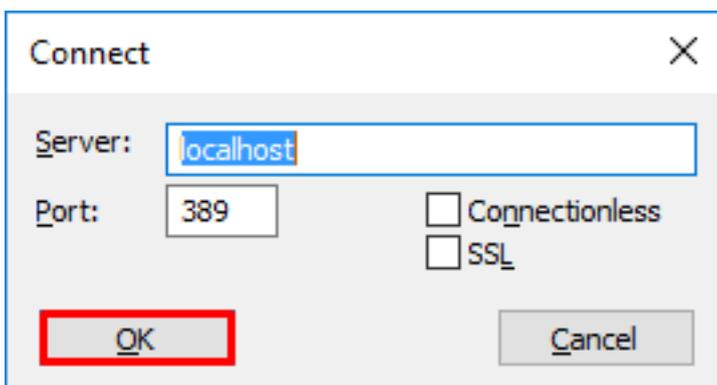
1. 在AD伺服器上，按Win+R並搜尋ldp.exe。



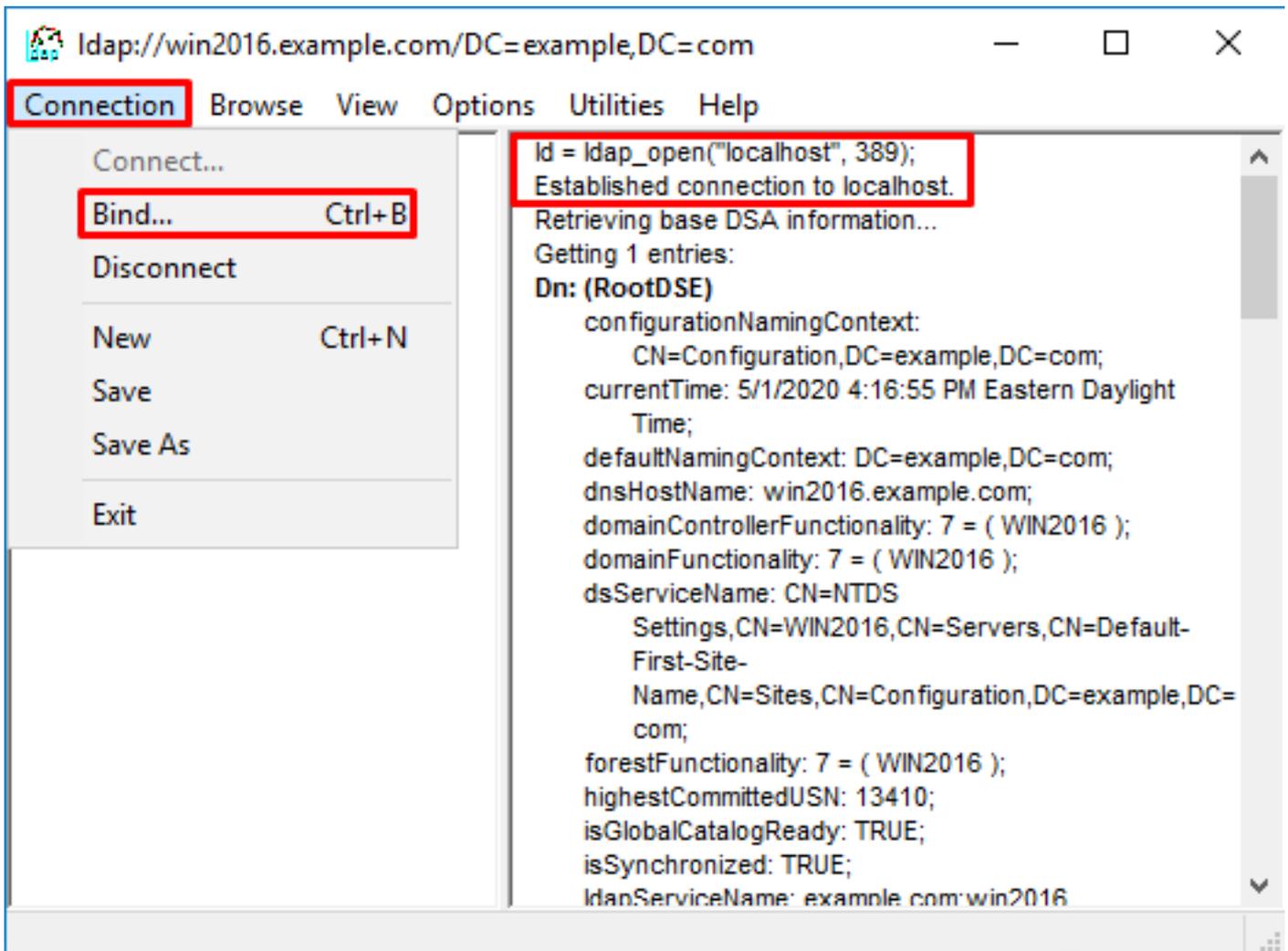
2. 按一下連線>連線..... 如下圖所示。



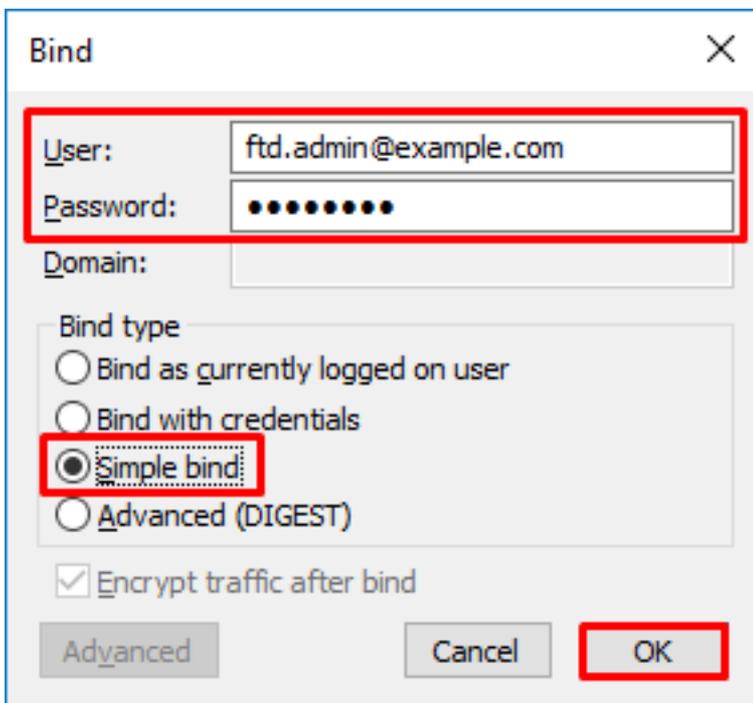
3. 指定伺服器的本地主機和相應的埠，然後按一下**確定**。



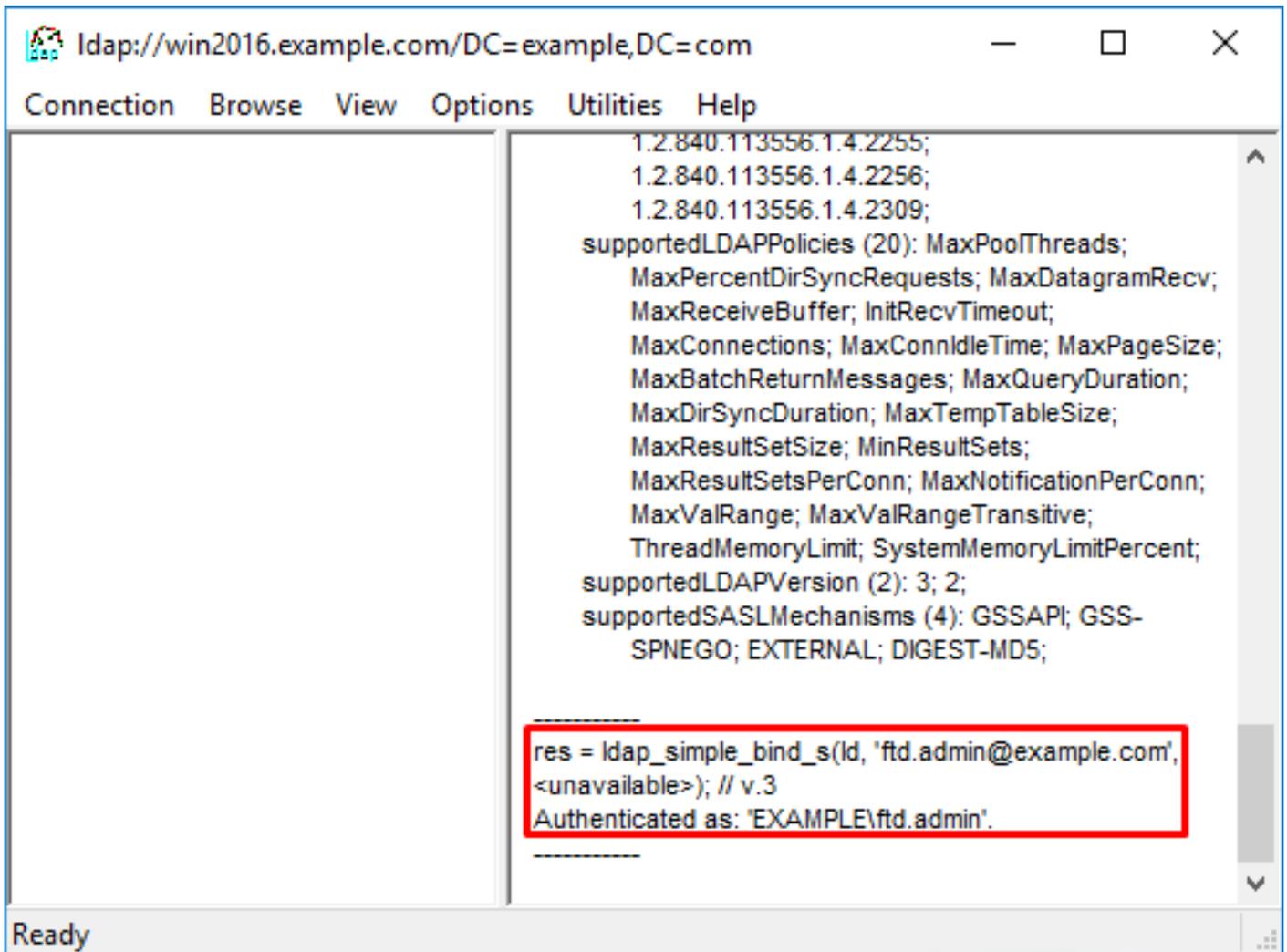
4. 「右」列顯示表示連線成功的文本。按一下**Connection > Bind...** 如下圖所示。



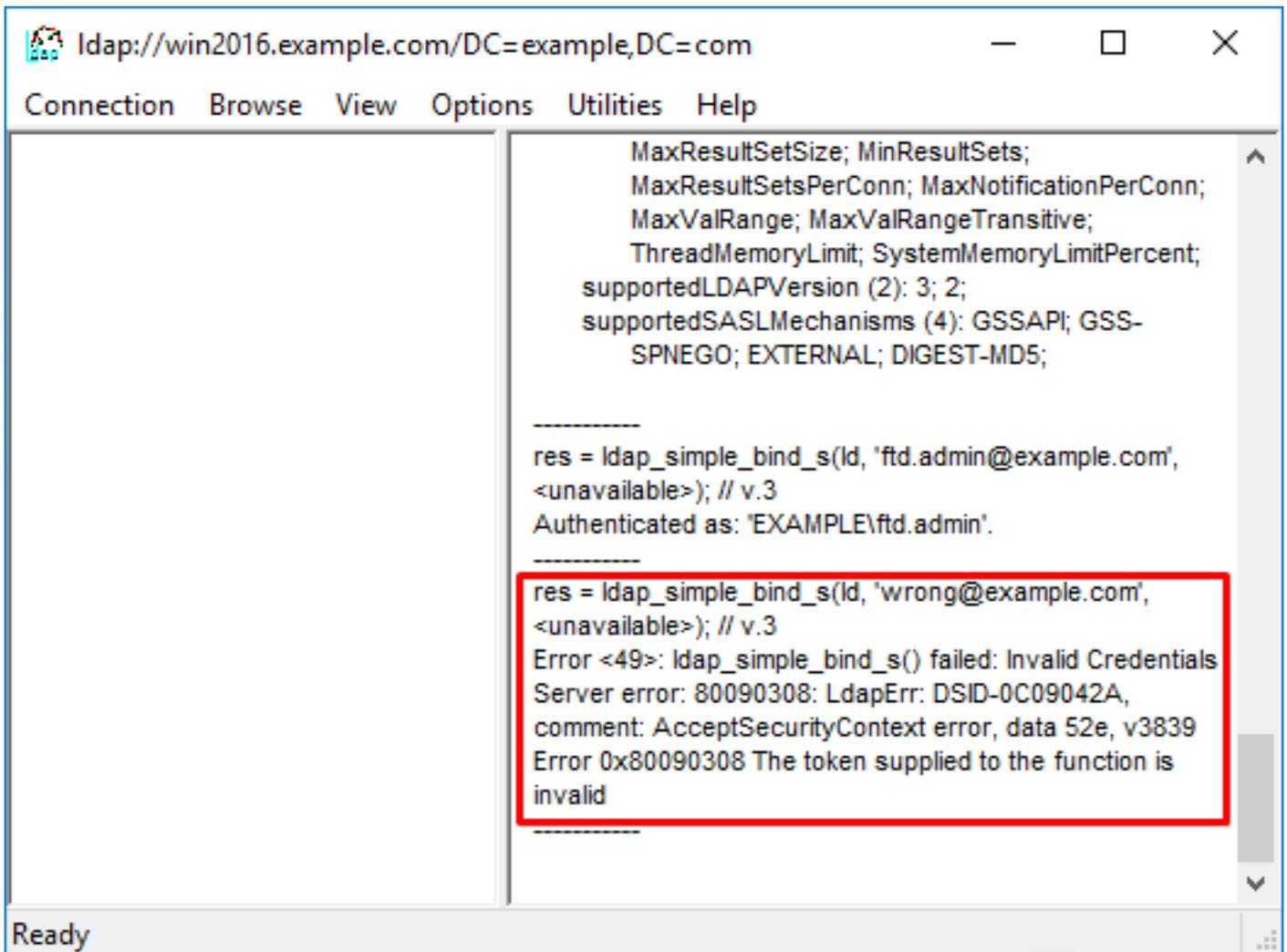
5. 選擇 Simple Bind，然後指定目錄帳戶使用者名稱和密碼。按一下「OK」（確定）。



成功繫結後，ldp將顯示驗證為DOMAIN\username。



如果嘗試使用無效的使用者名稱或密碼進行繫結，將會導致類似這樣的失敗。

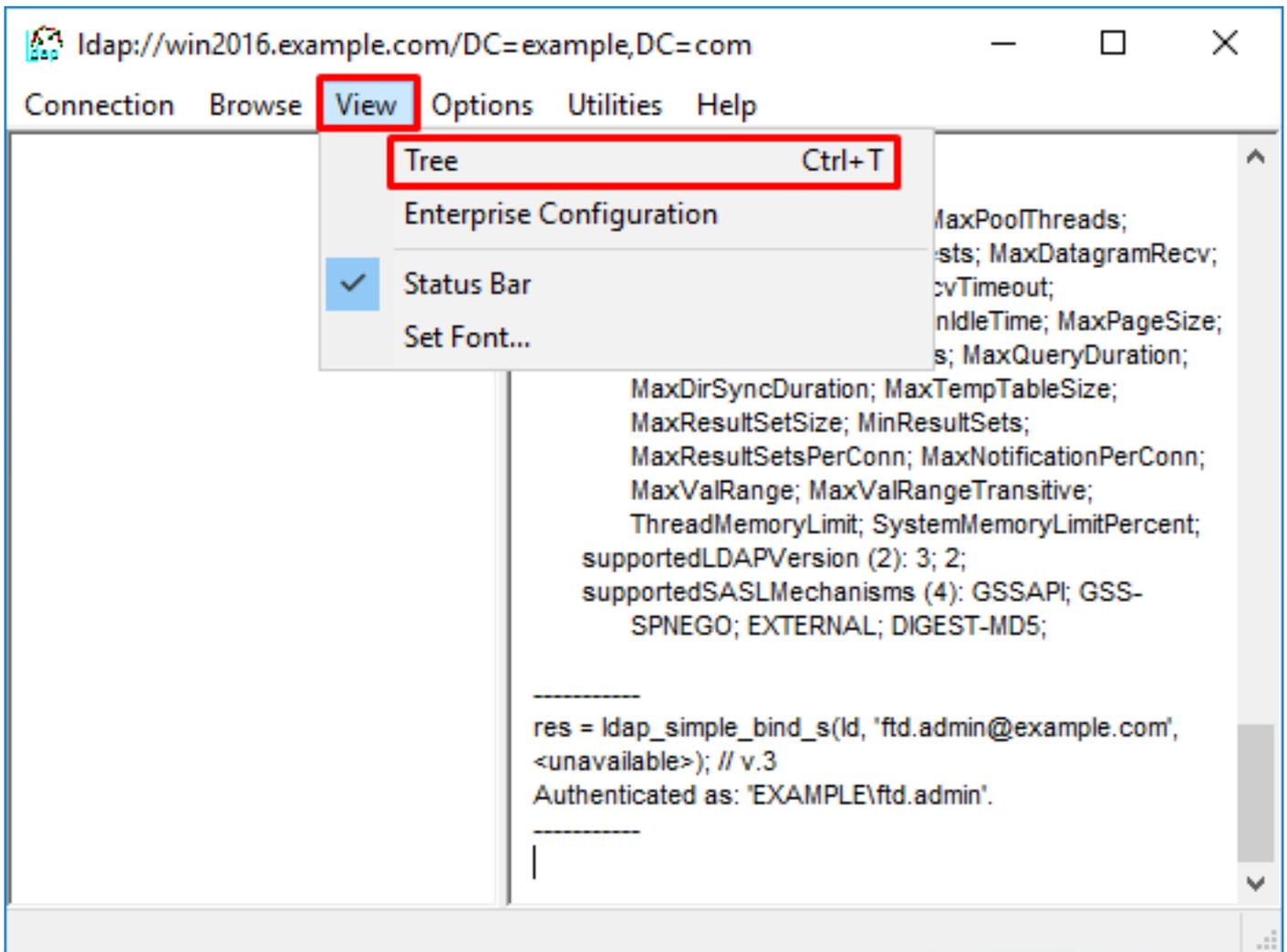


LDAP伺服器找不到使用者名稱

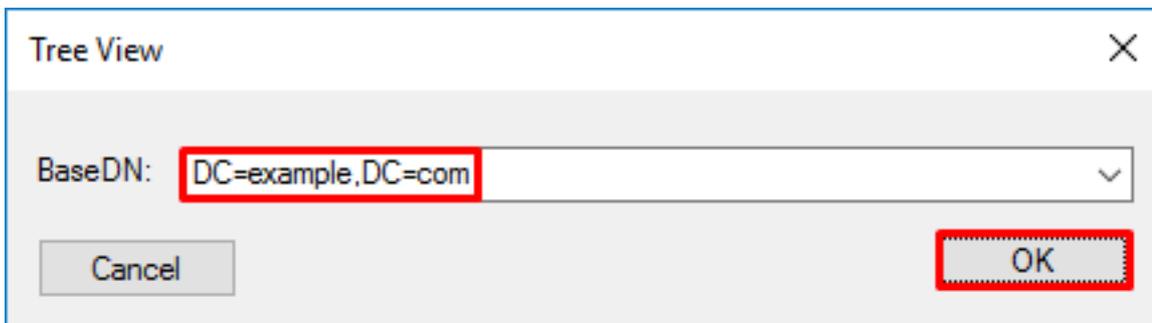
```
[ -2147483612] Session Start
[ -2147483612] New request Session, context 0x00007f9e65ccdc40, reqType = Authentication
[ -2147483612] Fiber started
[ -2147483612] Creating LDAP context with uri=ldap://192.168.1.1:389
[ -2147483612] Connect to LDAP server: ldap://192.168.1.1:389, status = Successful
[ -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：確認AD可以通過FTD完成的搜尋找到使用者。這也可以使用ldp.exe來完成。

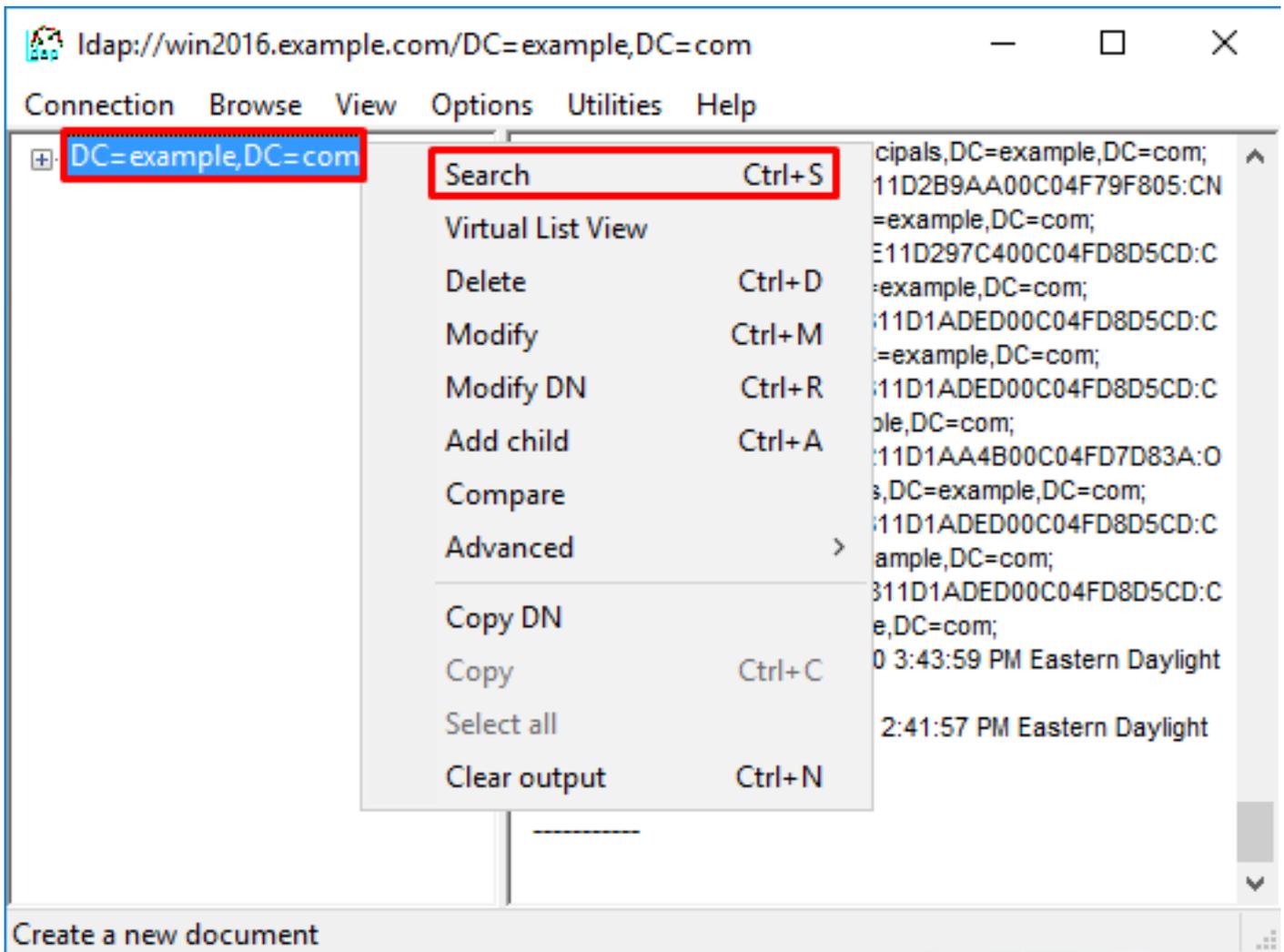
1.成功繫結後，導航到檢視>樹，如下圖所示。



2. 指定在FTD上設定的基本DN，然後按一下OK。

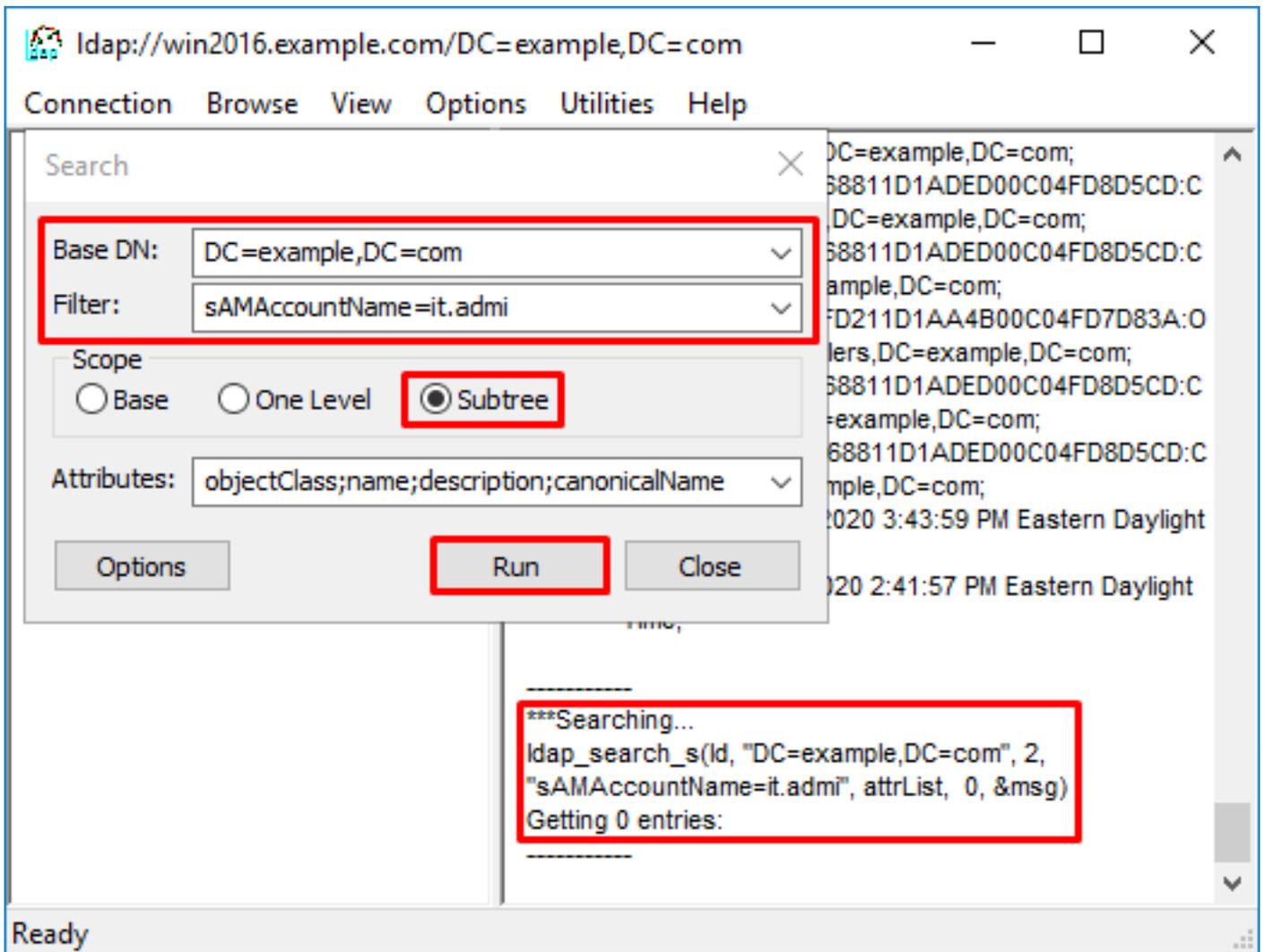


3. 按一下右鍵「基本DN」，然後按一下「搜尋」，如下圖所示。



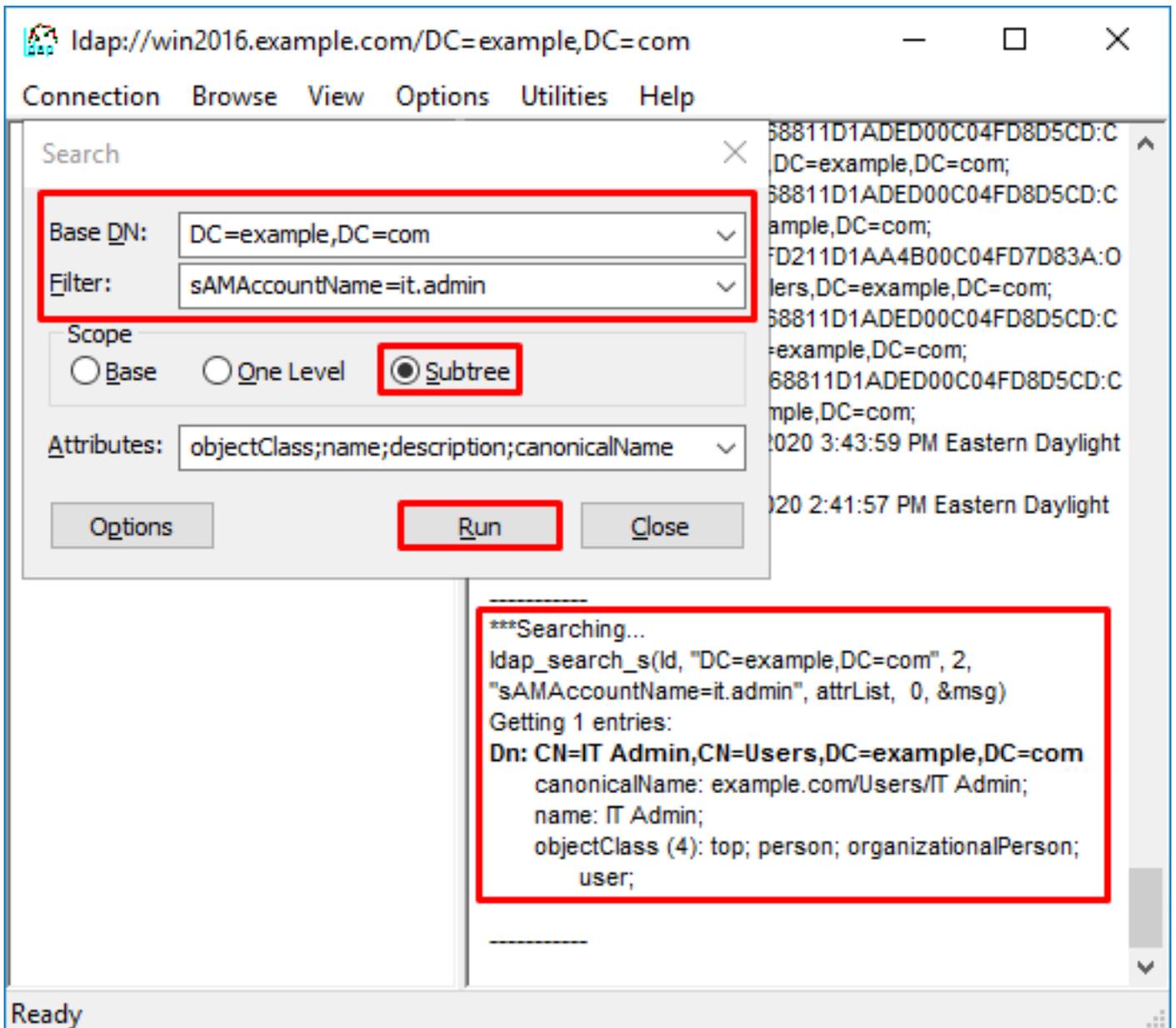
4. 指定與debug中相同的基本DB、篩選器和範圍值。在此範例中，這些如下：

- 基本DN:dc=example , dc=com
- Filter: (篩選條件 :)samaccountname=it.admi
- 範圍：子樹



由於Base DN dc=example , dc=com下沒有具有samaccountname=it.admi的使用者帳戶，LDP會找到0個條目。

使用正確的samaccountname=it.admin再次嘗試顯示不同的結果。ldp在Base DN dc=example , dc=com下找到1個條目，並列印該使用者的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：驗證使用者的密碼是否正確配置且未過期。與登入DN類似，FTD會使用使用者憑證對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的潛在原因。

測試AAA

test aaa-server命令可用於使用特定使用者名稱和密碼模擬來自FTD的驗證嘗試。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。

以下是顯示雙向LDAP流量的捕獲：

```
> 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
```

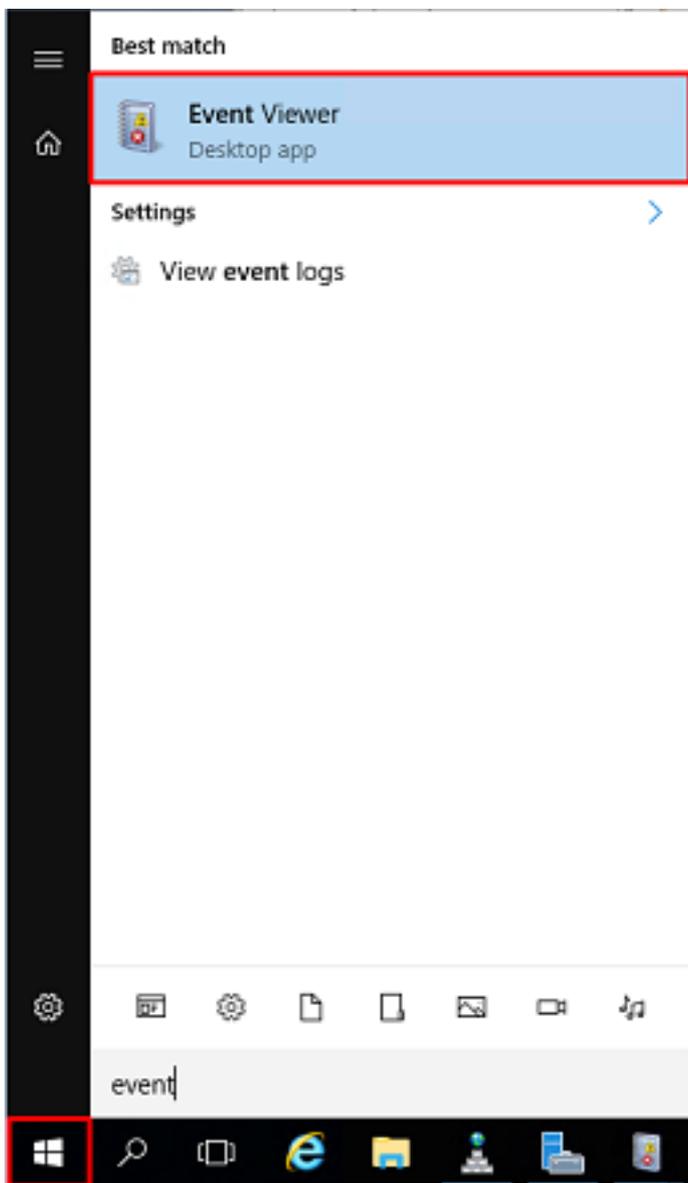
```
  1: 23:02:16.770712      192.168.1.17.61960 > 192.168.1.1.389: S 3681912834:3681912834(0) win
32768 <mss 1460,nop,nop,timestamp 1061373057 0>
  2: 23:02:16.772009      192.168.1.1.389 > 192.168.1.17.61960: S 491521506:491521506(0) ack
3681912835 win 8192 <mss 1460,nop,nop,timestamp 762393884 1061373057>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

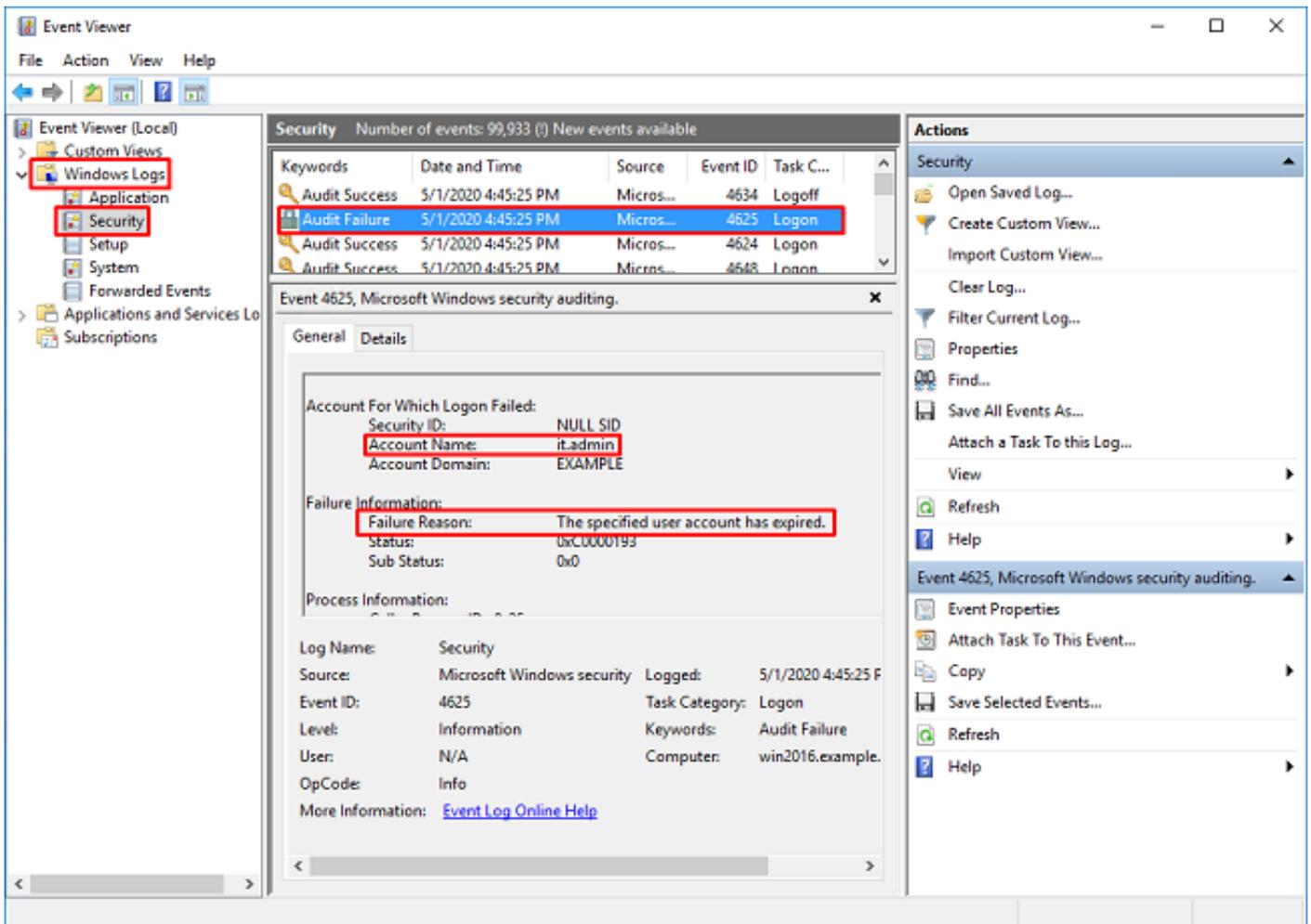
Windows Server事件檢視器日誌

AD伺服器Van上的事件檢視器日誌提供了更多有關失敗原因的詳細資訊。

1. 搜尋並開啟事件檢視器。



2. 展開Windows Logs，然後按一下Security。使用使用者的Account Name搜尋Audit Failure，然後檢視Failure Information，如下圖所示。



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