

使用外部LDAPS身份庫配置ISE並對其進行故障排除

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[設定](#)

[網路圖表](#)

[在Active Directory上配置LDAPS](#)

[在域控制器上安裝身份證書](#)

[訪問LDAPS目錄結構](#)

[將ISE與LDAPS伺服器整合](#)

[設定交換器](#)

[配置終端](#)

[在ISE上配置策略集](#)

[驗證](#)

[疑難排解](#)

[相關資訊](#)

簡介

本文檔介紹思科ISE與作為外部身份源的安全LDAPS伺服器的整合。

必要條件

需求

思科建議您瞭解以下主題：

- 身份服務引擎(ISE)管理基礎知識
- Active Directory/安全輕量型目錄存取通訊協定(LDAPS)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：

- Cisco ISE 2.6補丁7
- 安裝了Active Directory輕型目錄服務的Microsoft Windows 2012 R2
- 安裝了本機請求方和使用證書的Windows 10 OS PC

- 採用152-2.E6映像的Cisco交換器C3750X


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

LDAPS允許在建立目錄繫結時對傳輸中的LDAP資料 (包括使用者憑據) 進行加密。LDAPS使用TCP埠636。

LDAPS支援以下身份驗證協定：

- EAP通用權杖卡(EAP-GTC)
- 密碼驗證通訊協定(PAP)
- EAP傳輸層安全(EAP-TLS)
- 受保護的EAP傳輸層安全(PEAP-TLS)

 註:LDAPS外部身份源不支援EAP-MSCHAPV2 (作為PEAP、EAP-FAST或EAP-TTLS的內部方法)、LEAP、CHAP和EAP-MD5。

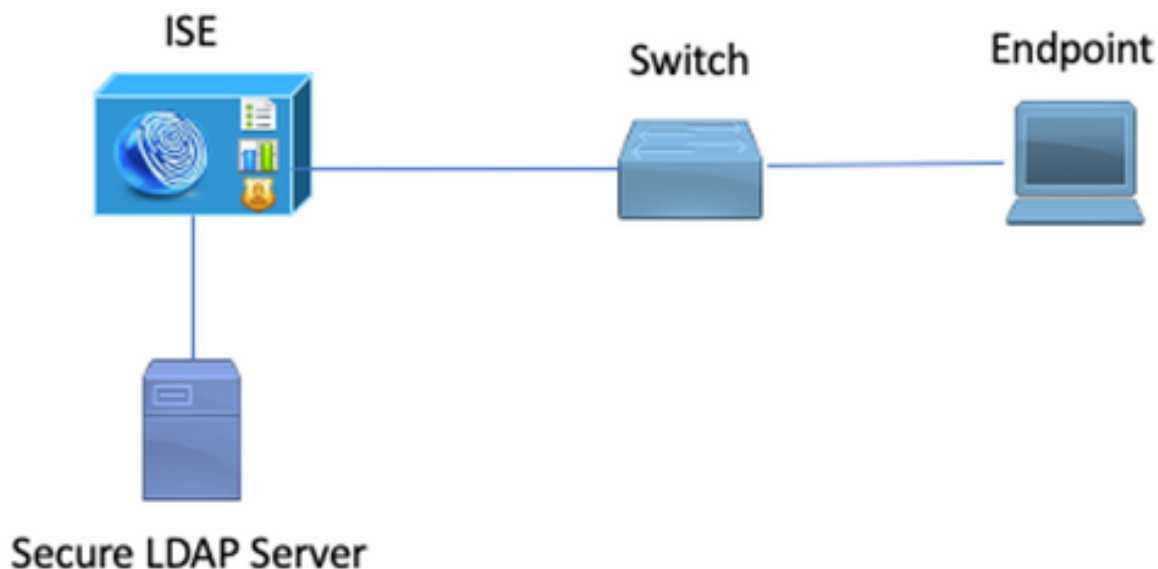
設定

本節介紹網路裝置的配置以及ISE與Microsoft Active Directory(AD)LDAPS伺服器的整合。

網路圖表

在此配置示例中，端點使用乙太網連線，通過交換機連線到區域網(LAN)。連線的交換機埠配置為802.1x身份驗證，以通過ISE驗證使用者。在ISE上，LDAPS配置為外部身份庫。

此圖說明所使用的網路拓撲：

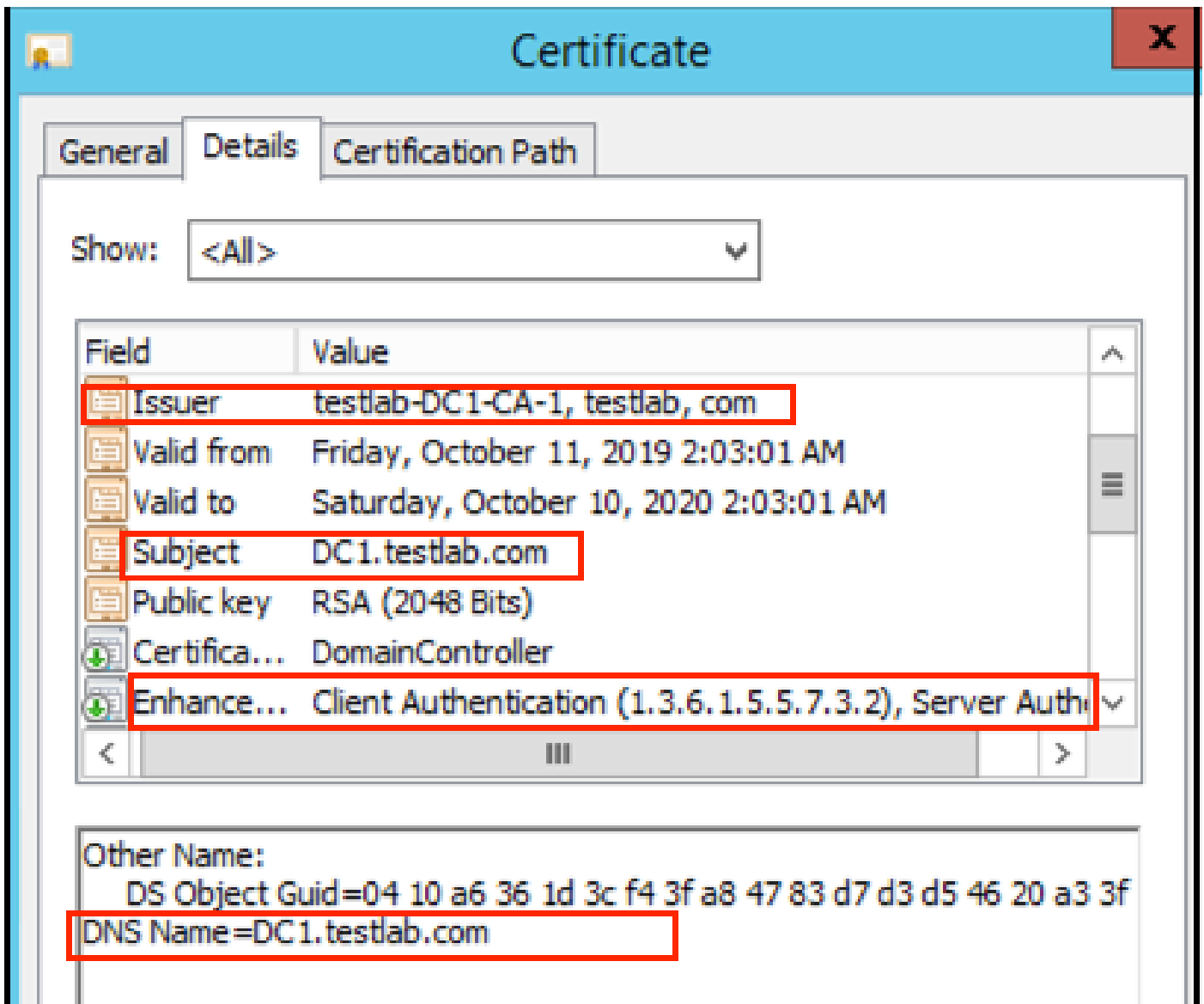


在Active Directory上配置LDAPS

在域控制器上安裝身份證書

若要啟用LDAPS，請在域控制器(DC)上安裝符合以下要求的證書：

1. LDAPS證書位於域控制器的個人證書儲存中。
2. 與證書匹配的私鑰存在於域控制器的儲存中，並且與證書正確關聯。
3. 增強型金鑰使用擴展包括伺服器身份驗證(1.3.6.1.5.5.7.3.1)對象識別符號 (也稱為OID)。
4. 域控制器的完全限定域名(FQDN)(例如，DC1.testlab.com)必須存在於以下屬性之一中：「主題」(Subject)欄位中的「公用名」(CN)和「主題備用名稱擴展」(Subject Alternative Name Extension)中的DNS條目。
5. 證書必須由域控制器和LDAPS客戶端信任的證書頒發機構(CA)頒發。對於可信的安全通訊，客戶端和伺服器必須信任對方的根CA和向其頒發證書的中間CA證書。
6. 必須使用通道加密服務提供程式(CSP)生成金鑰。




訪問LDAPS目錄結構

要訪問Active Directory伺服器上的LDAPS目錄，請使用任何LDAP瀏覽器。本實驗使用Softerra LDAP Browser 4.5。

1.在TCP埠636上建立到域的連線。



2.為簡單起見，在AD中建立名為ISE OU的組織單元(OU)，並且必須具有一個名為UserGroup的組。建立兩個使用者 (user1和user2)，並使其成為組UserGroup的成員。

 注意:ISE上的LDAP身份源僅用於使用者身份驗證。

Name	Value	Type
DN	UserGroup	Entry
DN	user2	Entry
DN	user1	Entry
DN	DESKTOP-19	Entry
DN	ComputerGroup	Entry
distinguishedName	OU=ISE OU,DC=testlab,DC=com	Attribute
dSCorePropagationData	1/1/1601	Attribute
dSCorePropagationData	6/20/2020 2:51:11 AM	Attribute
gPLink	[LDAP://cn={21A53B13-6971-45E8-8545-FD0C68E29790},c...	Attribute
instanceType	[Writable]	Attribute
name	ISE OU	Attribute
objectCategory	CN=Organizational-Unit,CN=Schema,CN=Configuration,DC=...	Attribute
objectClass	organizationalUnit	Attribute
objectClass	top	Attribute
ou	ISE OU	Attribute
uSNChanged	607428	Attribute
uSNCreated	603085	Attribute
whenChanged	6/21/2020 2:44:06 AM	Attribute
whenCreated	6/20/2020 2:51:11 AM	Attribute
objectGUID	{44F45D1D-17B7-48DF-ABC6-3ED27FA4F694}	Binary Attribute

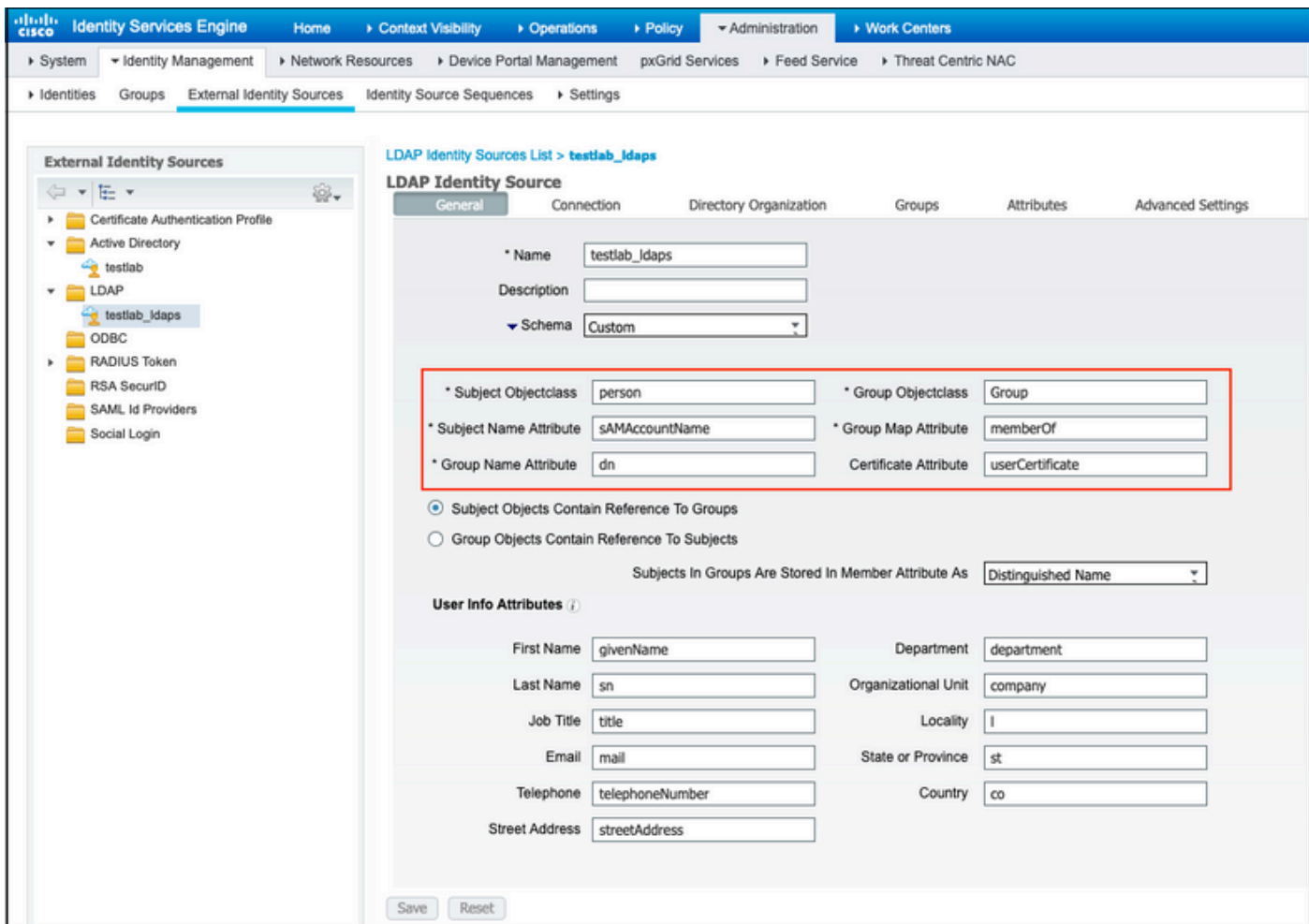
將ISE與LDAPS伺服器整合

1. 匯入受信任證書中的LDAP伺服器根CA證書。

Friendly Name	Status	Trusted For	Serial Number	Issued To	Issued By
DC1					
DC1-CA	Enabled	Infrastructure Cisco Services Endpoints	18 29 1C A7 00 13...	testlab-DC1-CA-1	testlab-DC1-CA-1

2. 驗證ISE管理員證書並確保ISE管理員證書頒發者證書也存在於受信任的證書儲存中。

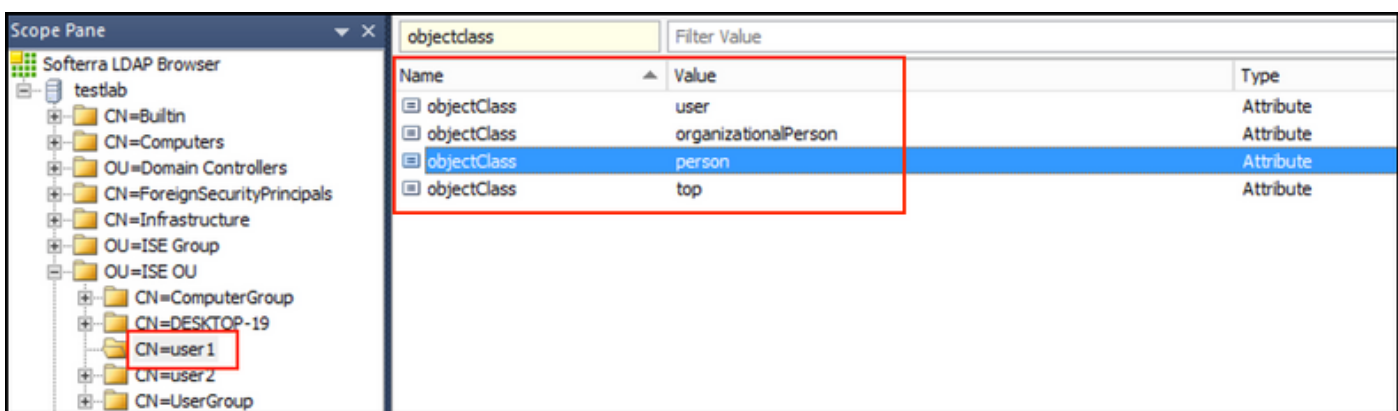
3. 為了整合LDAPS伺服器，請使用LDAPS目錄中的不同LDAP屬性。導航到Administration > Identity Management > External Identity Sources > LDAP Identity Sources > Add。



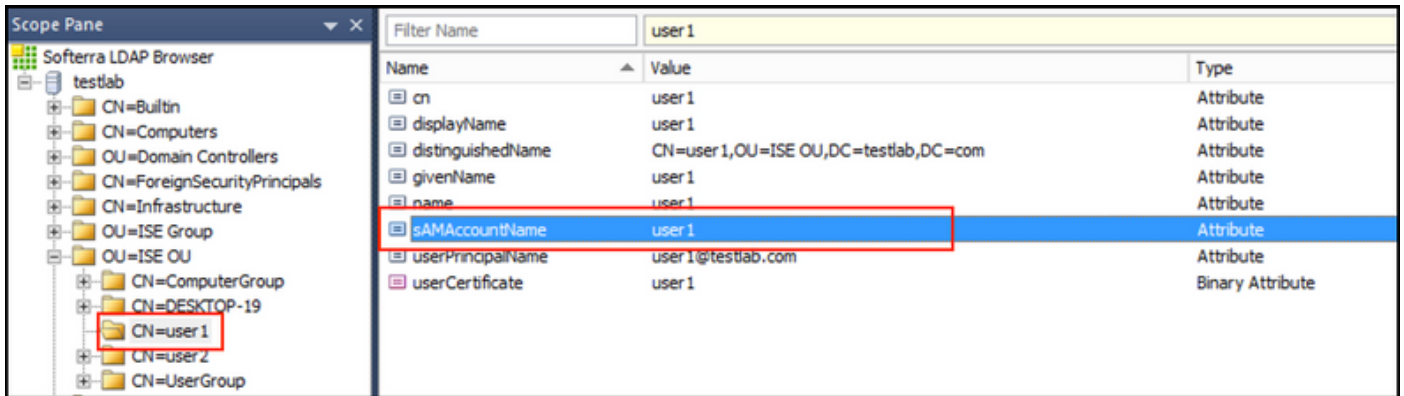
4.從「常規」頁籤配置以下屬性：

Subject Objectclass：此欄位與使用者帳戶的Object類相對應。您可以在此處使用四個類之一：

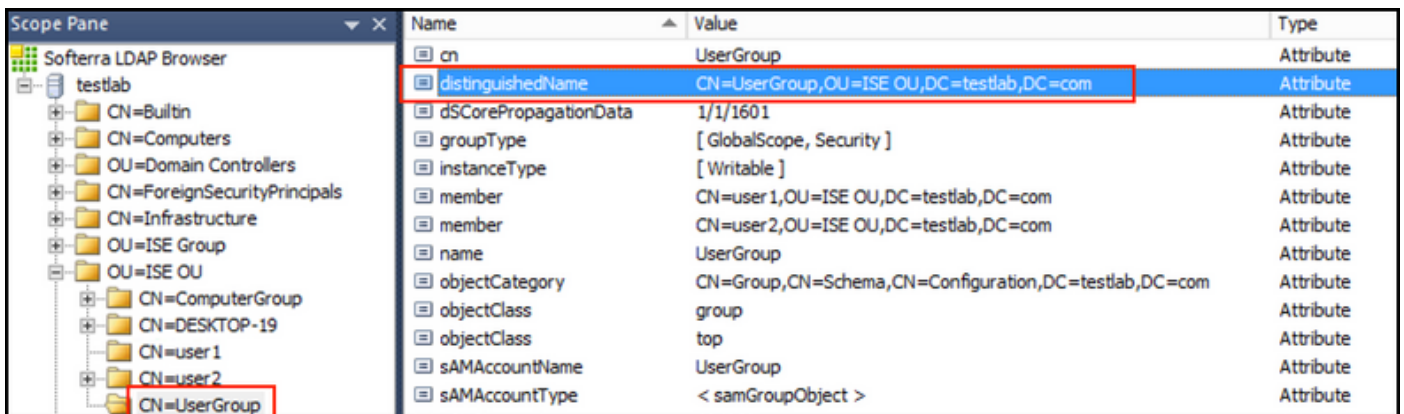
- 頂端
- 人員
- 組織人員
- InetOrgPerson



Subject Name Attribute：此欄位是包含請求中的使用者名稱的屬性的名稱。當ISE查詢LDAP資料庫中的特定使用者名稱時，會從LDAPS檢索此屬性（您可以使用cn、sAMAccountName等）。在此方案中，使用終端上的user1使用者名稱。



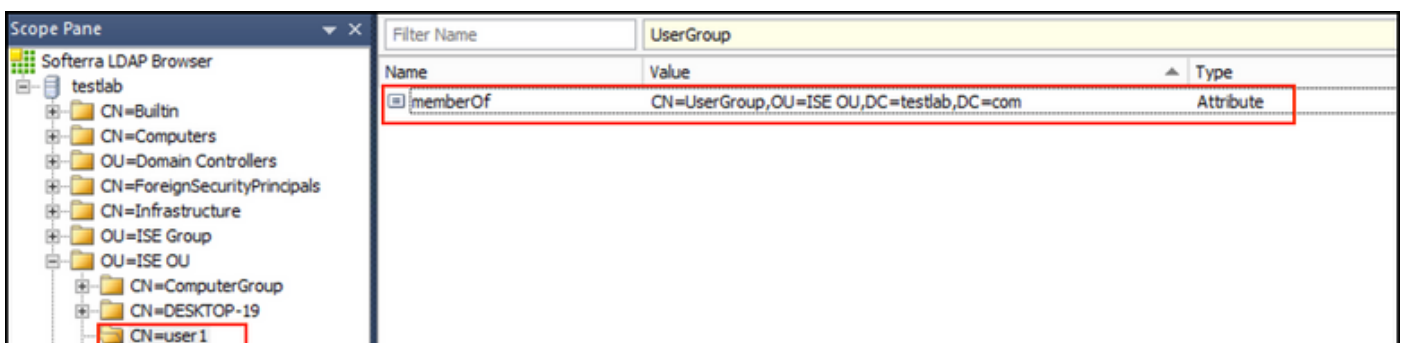
組名稱屬性：這是儲存組名稱的屬性。LDAP目錄中的組名稱屬性值必須與「使用者組」頁上的LDAP組名稱相匹配



組Objectclass:在搜尋中使用此值來指定可識別為組的對象。



組對映屬性：此屬性定義如何將使用者對映到組。



證書屬性：輸入包含證書定義的屬性。這些定義可以選擇用於在客戶端被定義為證書身份驗證配置檔案的一部分時驗證客戶端提供的證書。在這種情況下，會在客戶端證書和從LDAP身份源檢索的證書之間執行二進位制比較。



5.要配置LDAPS連線，請導航到Connection頁籤：

The screenshot shows the 'LDAP Identity Source' configuration page in Cisco ISE, specifically the 'Connection' tab. The page is divided into two main sections: 'Primary Server' and 'Secondary Server'. The 'Primary Server' section is active and contains the following fields and options:

- Hostname/IP:** dc1.testlab.com
- Port:** 636
- Specify server for each ISE node
- Access:** Authenticated Access (with Anonymous Access also visible)
- Admin DN:** CN=poongarg,CN=Users,DC=testlab
- Password:** [Redacted]
- Secure Authentication:** Enable Secure Authentication and Enable Server Identity Check
- LDAP Server Root CA:** DC1-CA
- Issuer CA of ISE Certificates:** DC1-CA

The 'Secondary Server' section is currently disabled, indicated by the 'Enable Secondary Server' checkbox being unchecked. Its fields include:

- Enable Secondary Server
- Hostname/IP:** [Empty]
- Port:** 389
- Access:** Anonymous Access (with Authenticated Access also visible)
- Admin DN:** [Empty]
- Password:** [Empty]
- Secure Authentication:** Enable Secure Authentication and Enable Server Identity Check
- LDAP Server Root CA:** DST Root CA X3 Certificate Authority
- Issuer CA of ISE Certificates:** Select if required (optional)

The screenshot shows the 'Advanced Settings' section of the LDAP Identity Source configuration page. It contains the following fields and options:

- Server Timeout:** 10 Seconds
- Max. Admin Connections:** 20
- Force reconnect every [Empty] Minutes
- Test Bind to Server:** [Button]
- Failover:** Fallback To Primary Server After 5 Minutes (with Always Access Primary Server First also visible)

6.在域控制器上運行dsquery以獲取用於連線到LDAP伺服器的使用者名稱DN:

```
PS C:\Users\Administrator> dsquery user -name poongarg  
"CN=poongarg , CN=Users , DC=testlab , DC=com"
```

步驟 1.設定LDAP伺服器的正確IP地址或主機名，定義LDAPS埠(TCP 636)和管理DN以通過SSL與LDAP建立連線。

步驟 2.啟用Secure Authentication and Server Identity Check選項。

步驟 3.從下拉選單中，選擇LDAP伺服器根CA證書和ISE管理員證書伺服器CA證書 (我們使用證書頒發機構，安裝在同一LDAP伺服器上以頒發ISE管理員證書)。

步驟 4.選擇「測試繫結到伺服器」。此時，由於尚未配置搜尋庫，因此不會檢索任何主題或組。

7.在Directory Organization頁籤下，配置主題/組搜尋庫。它是ISE到LDAP的加入點。現在您只能檢索作為該加入點子項的主體和組。在此場景中，主題和組都從OU=ISE OU檢索

The screenshot shows the 'LDAP Identity Source' configuration page for 'testlab_ldaps'. The 'Directory Organization' tab is selected. The 'Subject Search Base' and 'Group Search Base' are both set to 'OU=ISE OU,DC=testlab,DC=com'. There are two 'Naming Contexts...' buttons with information icons. Below, there is a 'Search for MAC Address in Format' dropdown menu set to 'xx-xx-xx-xx-xx-xx'. At the bottom, there are two unchecked checkboxes: 'Strip start of subject name up to the last occurrence of the separator \\' and 'Strip end of subject name from the first occurrence of the separator'.

8.在「組」下，按一下「新增」從ISE上的LDAP匯入組並檢索組，如下圖所示。

The screenshot shows the 'LDAP Identity Source' configuration page for 'testlab_ldaps'. The 'Groups' tab is selected. At the top, there are buttons for 'Edit', '+ Add', and 'X Delete Group'. Below, there is a table with two columns: 'Name' and an empty column. The first row in the table has a checkbox and the text 'CN=UserGroup,OU=ISE OU,DC=testlab,DC=com'.

設定交換器

將交換機配置為802.1x身份驗證。Windows PC已連線到switchport Gig2/0/47

```
aaa new-model
```

```
radius server ISE
address ipv4 x.x.x.x auth-port 1812 acct-port 1813
key xxxxxx
aaa group server radius ISE_SERVERS
server name ISE
```

```
!
```

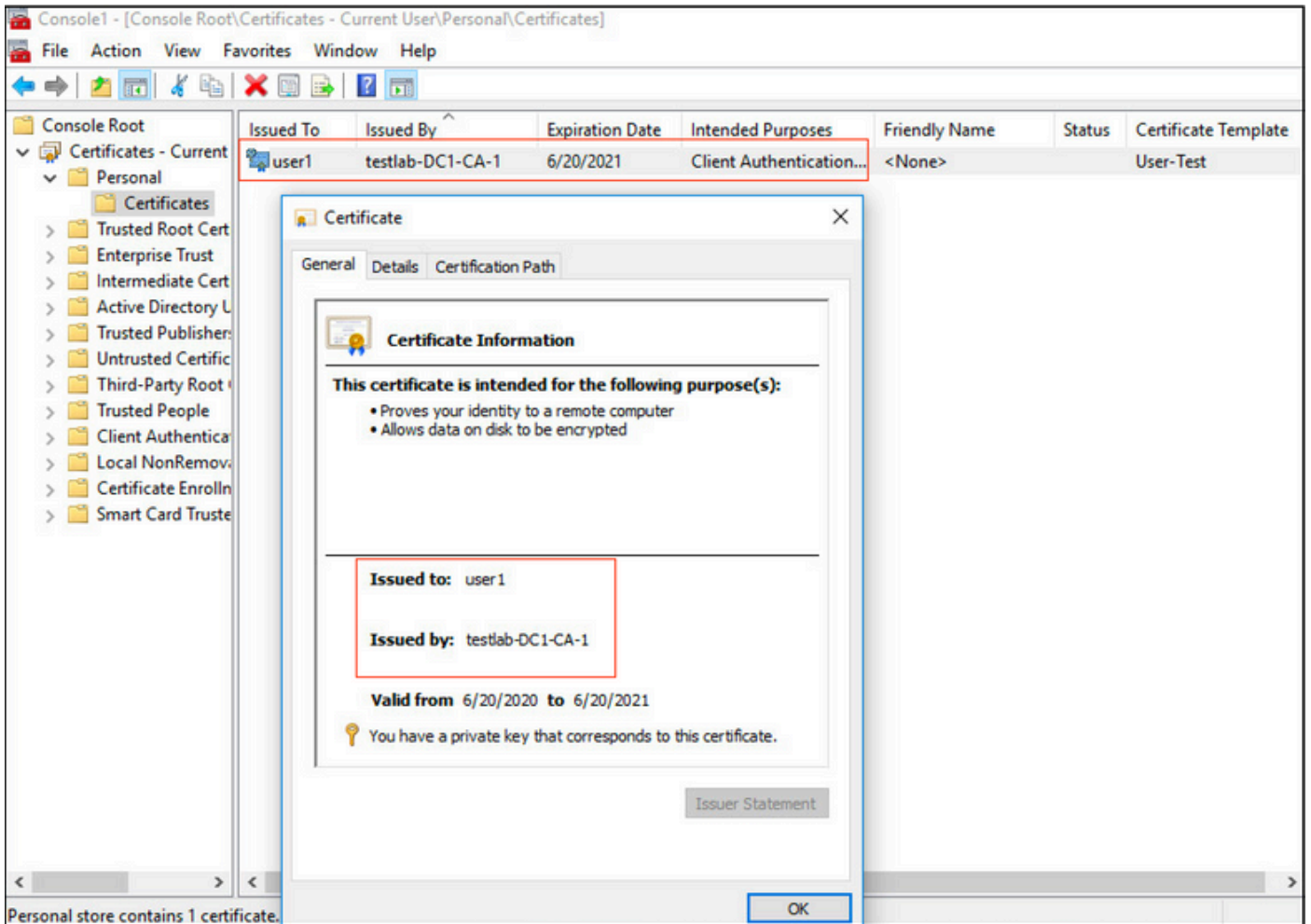
```
aaa server radius dynamic-author
client x.x.x.x server-key xxxxxx
```

```
!  
aaa authentication dot1x default group ISE_SERVERS local  
aaa authorization network default group ISE_SERVERS  
aaa accounting dot1x default start-stop group ISE_SERVERS  
!  
dot1x system-auth-control  
  
ip device tracking  
!  
radius-server attribute 6 on-for-login-auth  
radius-server attribute 8 include-in-access-req  
!  
  
!  
  
interface GigabitEthernet2/0/47  
switchport access vlan xx  
switchport mode access  
authentication port-control auto  
dot1x pae authenticator
```

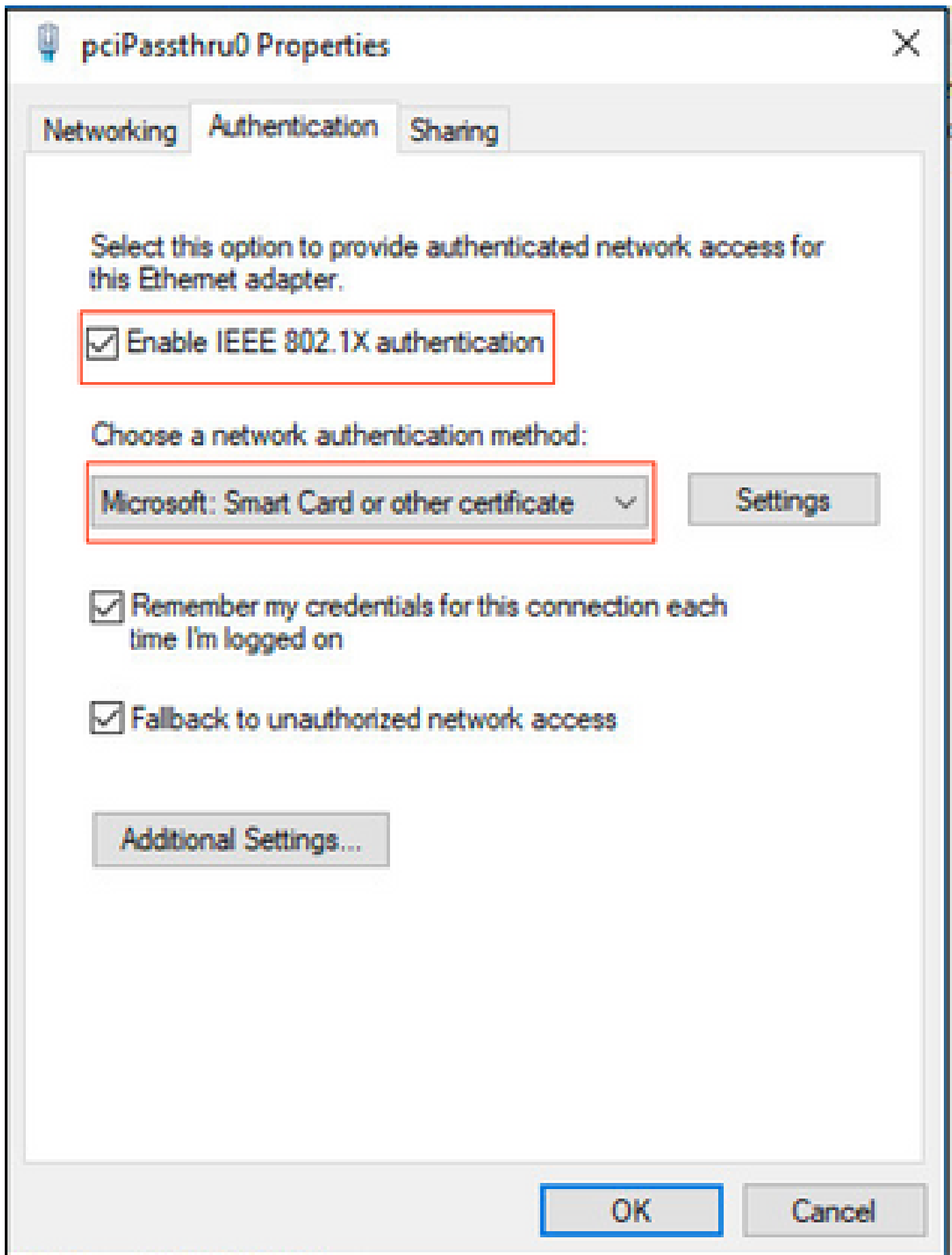
配置終端

使用Windows Native Supplicant客戶端，並且使用LDAP支援的EAP協定之一，EAP-TLS用於使用者身份驗證和授權。

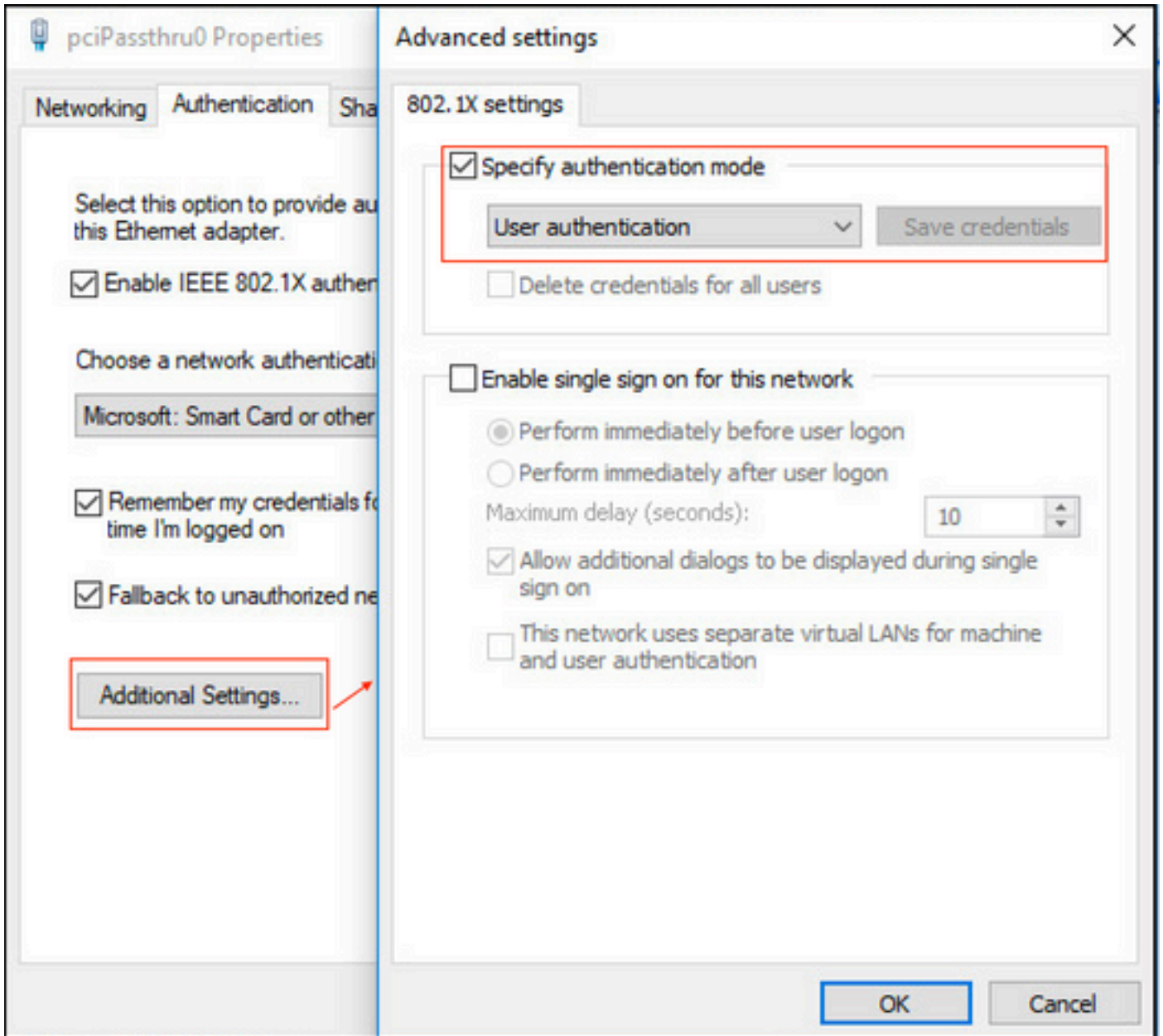
1.確保PC已配置使用者證書（用於user1），並且其用途為客戶端身份驗證，在受信任的根證書頒發機構中，PC上存在頒發者證書鏈。



2. 啟用Dot1x身份驗證並選擇Authentication method as Microsoft:Smart Card or other certificate for EAP-TLS authentication。

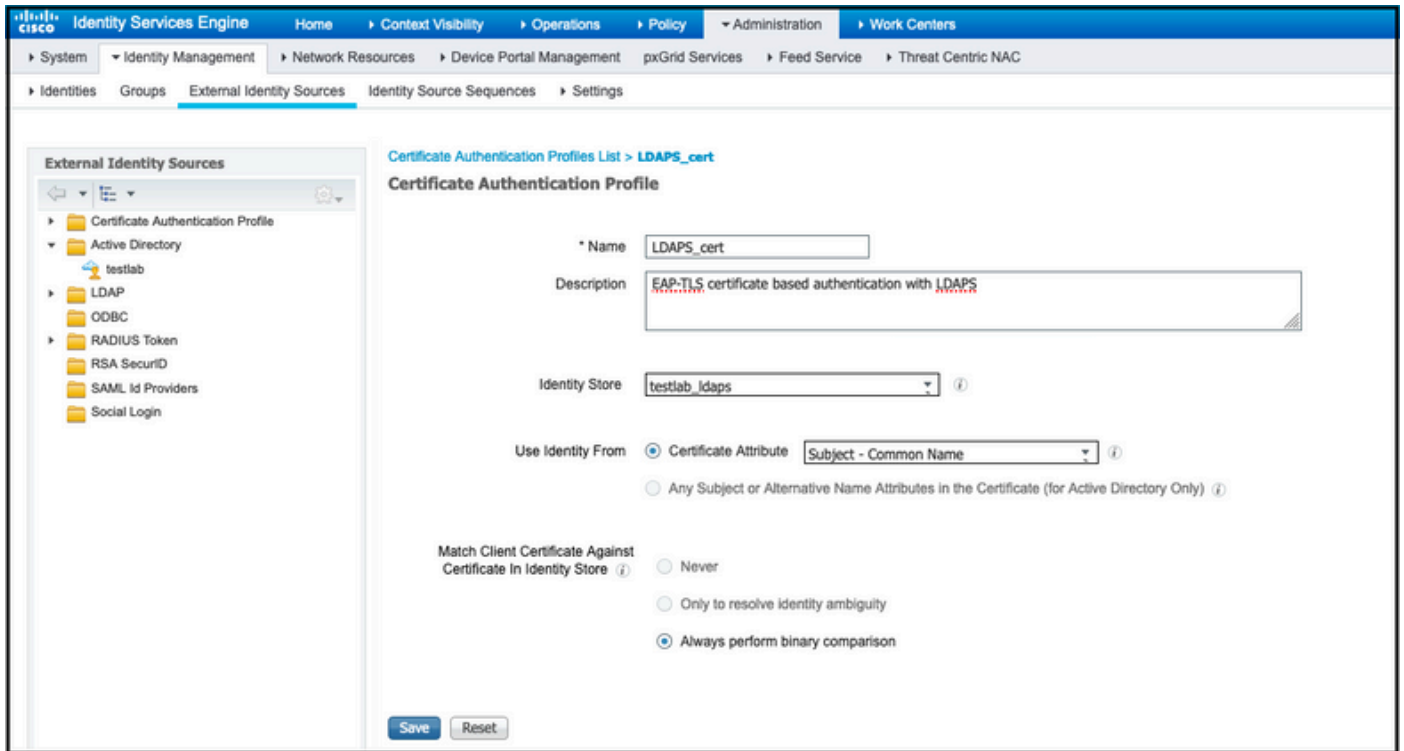


3.按一下「其它設定」，此時將開啟一個視窗。選中specify authentication mode覈取方塊，並選擇使用者身份驗證，如下圖所示。



在ISE上配置策略集

由於使用EAP-TLS協定，因此在配置策略集之前，需要配置證書身份驗證配置檔案，並在稍後在身份驗證策略中使用身份源序列。



請參閱Identity Source Sequence中的Certificate Authentication Profile，並在Authentication Search清單中定義LDAPS外部身份源：

Identity Services Engine Administration > Identity Source Sequences

Identity Source Sequence

Identity Source Sequence

* Name:

Description:

Certificate Based Authentication

Select Certificate Authentication Profile:

Authentication Search List

A set of identity sources that will be accessed in sequence until first authentication succeeds

Available		Selected	
Internal Endpoints	>	testlab_ldaps	⌵
Internal Users	<		⬆
Guest Users			⬇
testlab	>>		⬇
All_AD_Join_Points	<<		⬆
rad			⬇

Advanced Search List Settings

If a selected identity store cannot be accessed for authentication

- Do not access other stores in the sequence and set the "AuthenticationStatus" attribute to "ProcessError"
- Treat as if the user was not found and proceed to the next store in the sequence

現在為有線Dot1x身份驗證配置策略集：

Identity Services Engine Administration > Policy > Policy Sets

Policy Sets → Wired Dot1x




Reset Policyset Hitcounts

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits
✔	Wired Dot1x		Wired_802.1X	Default Network Access	453

Authentication Policy (2)

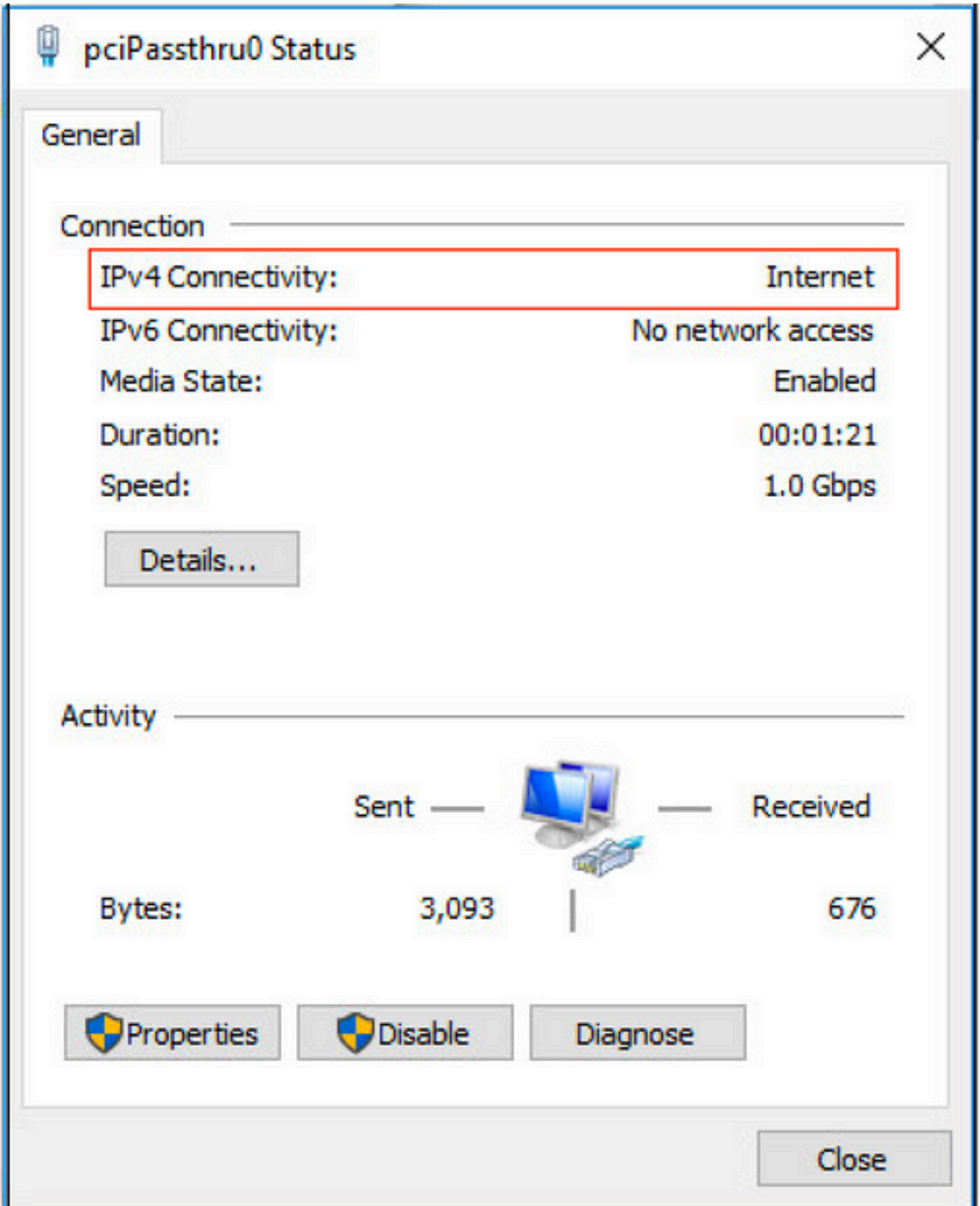
Status	Rule Name	Conditions	Use	Hits	Actions
✔	Dot1x	Network Access-NetworkDeviceName EQUALS LAB-Switch	LDAPS	223	Options
✔	Default		LDAPS	0	Options

Authorization Policy (2)

+	Status	Rule Name	Conditions	Results			Hits	Actions
				Profiles	Security Groups			
Search								
<input checked="" type="checkbox"/>	Users in LDAP Store		testlab_ldaps-ExternalGroups EQUALS CN=UserGroup,OU=ISE OU,DC=testlab,DC=com	<input type="text" value="x PermiAccess"/> +	<input type="text" value="Select from list"/> +	207		
<input checked="" type="checkbox"/>	Default			<input type="text" value="x DenyAccess"/> +	<input type="text" value="Select from list"/> +	11		

Reset Save

完成此配置後，我們可以使用EAP-TLS協定對LDAPS身份源對終端進行身份驗證。



驗證

1. 檢查連線到PC的switchport上的身份驗證會話：

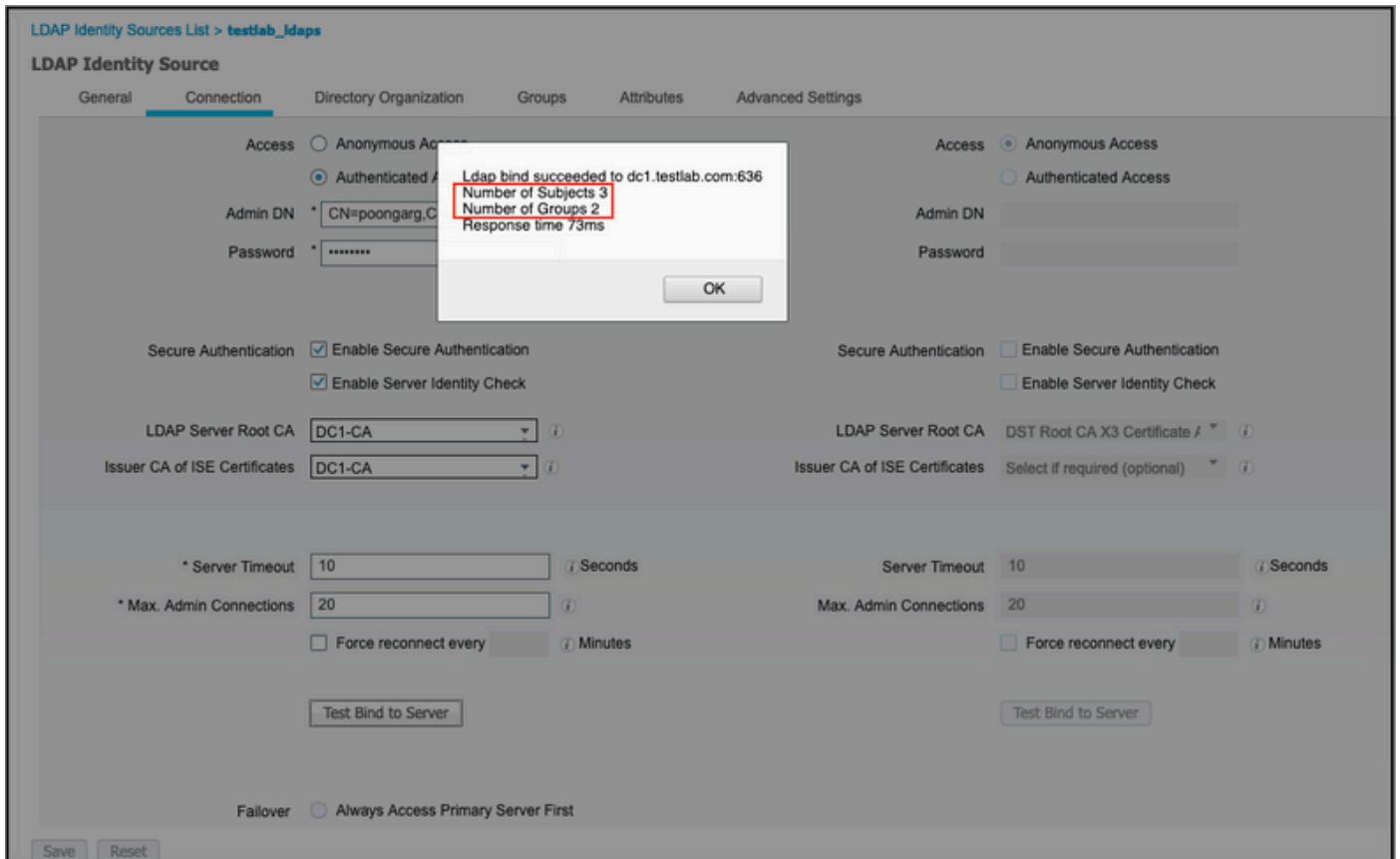
```
SW1#sh auth sessions int g2/0/47 de
      Interface: GigabitEthernet2/0/47
      MAC Address: b496.9126.dec0
      IPv6 Address: Unknown
      IPv4 Address: 10.106.38.165
      User-Name: user1
      Status: Authorized
      Domain: DATA
      Oper host mode: single-host
      Oper control dir: both
      Session timeout: N/A
      Restart timeout: N/A
      Periodic Acct timeout: N/A
      Session Uptime: 43s
      Common Session ID: 0A6A26390000130798C66612
      Acct Session ID: 0x00001224
      Handle: 0x6800002E
      Current Policy: POLICY_Gi2/0/47

Local Policies:
      Service Template: DEFAULT_LINKSEC_POLICY_SHOULD_SECURE (priority 150)

Server Policies:

Method status list:
      Method          State
      dot1x           Authc Success
```

2. 為了驗證LDAPS和ISE配置，您可以檢索與伺服器有測試連線的主題和組：



3. 驗證使用者身份驗證報告：

Time	Status	Details	Identity	Endpoint ID	Authentication Po...	Authorization Policy	Authorization Profi...	Network De...	Device Port	Authentication Pro...
Jun 24, 2020 04:45:21.727 AM	●		user1	B4-96:91:26:DE:C0	Wired Dot1x >> Dot1x	Wired Dot1x >> Users in LDAP Store	PermitAccess	GigabitEthernet2/0/47	EAP-TLS	
Jun 24, 2020 04:45:20.671 AM	●		user1	B4-96:91:26:DE:C0	Wired Dot1x >> Dot1x	Wired Dot1x >> Users in LDAP Store	PermitAccess	LAB-Switch	GigabitEthernet2/0/47	EAP-TLS

4. 檢查終端的詳細身份驗證報告：

Overview

Event 5200 Authentication succeeded

Username user1

Endpoint Id B4:96:91:26:DE:C0 ⊕

Endpoint Profile Unknown

Authentication Policy Wired Dot1x >> Dot1x

Authorization Policy Wired Dot1x >> Users in LDAP Store

Authorization Result PermitAccess

Authentication Details

Source Timestamp	2020-06-24 04:40:52.124
Received Timestamp	2020-06-24 04:40:52.124
Policy Server	ISE26-1
Event	5200 Authentication succeeded
Username	user1
Endpoint Id	B4:96:91:26:DE:C0
Calling Station Id	B4-96-91-26-DE-C0
Endpoint Profile	Unknown
IPv4 Address	10.106.38.165
Authentication Identity Store	testlab_idaps
Identity Group	Unknown
Audit Session Id	0A6A26390000130C98CE6088
Authentication Method	dot1x
Authentication Protocol	EAP-TLS
Service Type	Framed
Network Device	LAB-Switch

15041 Evaluating Identity Policy
15048 Queried PIP - Network Access.NetworkDeviceName
22072 Selected identity source sequence - LDAPS
22070 Identity name is taken from certificate attribute
15013 Selected Identity Source - testlab_ldaps
24031 Sending request to primary LDAP server - testlab_ldaps
24016 Looking up user in LDAP Server - testlab_ldaps
24023 User's groups are retrieved - testlab_ldaps
24004 User search finished successfully - testlab_ldaps
22054 Binary comparison of certificates succeeded
22037 Authentication Passed
12506 EAP-TLS authentication succeeded

15036 Evaluating Authorization Policy
24209 Looking up Endpoint in Internal Endpoints IDStore - user1
24211 Found Endpoint in Internal Endpoints IDStore
15048 Queried PIP - testlab_ldaps.ExternalGroups
15016 Selected Authorization Profile - PermitAccess
22081 Max sessions policy passed
22080 New accounting session created in Session cache
11503 Prepared EAP-Success
11002 Returned RADIUS Access-Accept

5. 驗證ISE和LDAPS伺服器之間的資料已加密，方法是在ISE上向LDAPS伺服器捕獲資料包：

The image shows a Wireshark packet capture of a TLSv1.2 connection. The 'Application Data' field in the packet details pane is highlighted in red and labeled 'Encrypted Data'. The packet list pane shows several packets, with the selected packet (No. 28) being a TLSv1.2 packet. The packet bytes pane shows the raw data of the packet, including the TLS record structure and the encrypted application data.

疑難排解

本節介紹此配置遇到的一些常見錯誤以及如何進行故障排除。

- 在驗證報告中，您可能會看到以下錯誤消息：

```
Authentication method is not supported by any applicable identity store
```


此錯誤消息表明LDAP不支援您選擇的方法。確保同一報告中的身份驗證協定顯示其中一個受支援的方法 (EAP-GTC、EAP-TLS或PEAP-TLS)。

- 到伺服器的測試繫結已結束，但出現錯誤。

這通常是由於LDAPS伺服器證書驗證檢查失敗。若要解決此類問題，請在ISE上捕獲資料包，並在調試級別啟用所有三個運行時和prtt-jni元件，重新建立問題，並檢查prtt-server.log檔案。

封包擷取會抱怨憑證錯誤，且連線埠伺服器顯示：

```
04:10:20,197,ERROR,0x7f9c5b6f1700,LdapSslConnectionContext::checkCryptoResult(id = 1289): error message
```

 註:LDAP頁中的主機名必須配置有證書的使用者名稱 (或任何使用者替代名稱)。因此，除非主題或SAN中存在此類證書，否則它不起作用，因此需要使用SAN清單中具有IP地址的證書。

3.在身份驗證報告中，您可能會注意到在身份儲存庫中找不到主題。這意味著報告的使用者名稱與LDAP資料庫中任何使用者的「使用者名稱屬性」不匹配。在此方案中，此屬性值設定為sAMAccountName，這意味著ISE在嘗試查詢匹配項時查詢LDAP使用者的sAMAccountName值。

4.在繫結到伺服器測試期間無法正確檢索主題和組。導致此問題的最可能原因是搜尋基的配置不正確。請記住，必須從枝葉到根和dc（可包含多個單詞）指定LDAP層次結構。

相關資訊

- <https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine/119149-configure-ise-00.html#anc9>
- <https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine/214975-configure-eap-tls-authentication-with-is.html>

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）。