تكوين ISE واستكشاف أخطاءه وإصلاحها باستخدام مخزن تعريف LDAP الخارجي

المحتويات

المقدمة

يصف هذا المستند تكامل Cisco ISE مع خادم LDAP الآمن كمصدر هوية خارجي.

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- المعرفة الأساسية لإدارة محرك خدمة الهوية (ISE)
- معرفة أساسية بالبروتوكول الآمن الخفيف للوصول إلى الدليل/Active Directory (LDAPs)

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج والمكونات المادية التالية:

- Cisco ISE 2.6 Patch 7
- Microsoft Windows الإصدار 2012 R2 مع خدمات Active Directory Lightweight Directory

المثبتة
- كمبيوتر نظام التشغيل Windows 10 المثبت عليه طالب الأصل وشهادة المستخدم
- المحول Cisco Switch C3750X مع صورة 152-2.E6

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك قيد التشغيل، فتأكد من فهمك للتأثير المحتمل لأي أمر.

معلومات أساسية

تسمح LDAPs بتشفير بيانات LDAP (التي تتضمن بيانات اعتماد المستخدم) أثناء النقل عند إنشاء ربط دليل. تستخدم LDAP منفذ TCP 636.

يتم دعم بروتوكولات المصادقة هذه مع LDAPs:

- بطاقة الرمز المميز العام EAP (EAP-GTC)
- بروتوكول مصادقة كلمة المرور (PAP)
- أمان طبقة النقل (EAP-TLS)
- أمان طبقة نقل EAP المحمي (PEAP-TLS)

ملاحظة: EAP-MSCHAPV2 (كأسلوب داخلي لـ PEAP أو EAP-FAST أو EAP-TTLS)، LEAP، CHAP، و EAP-MD5 غير مدعوم مع مصدر الهوية الخارجي لنقاط الوصول إلى الأقل.

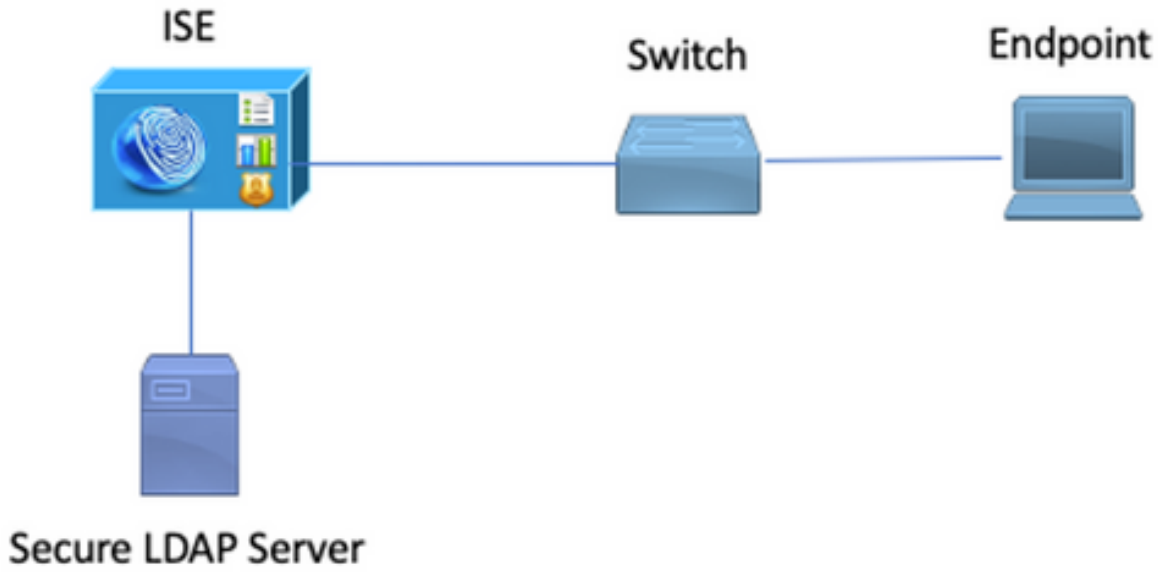
التكوين

يصف هذا القسم تكوين أجهزة الشبكة وتكامل ISE مع خادم Microsoft Active Directory (AD) LDAP.

الرسم التخطيطي للشبكة

في مثال التكوين هذا، تستخدم نقطة النهاية اتصال إيثرنت بمحول للاتصال بشبكة المنطقة المحلية (LAN). يتم تكوين switchport لمصادقة 802.1x لمصادقة المستخدمين مع ISE. على ISE، تم تكوين LDAPs كمخزن هوية خارجي.

يوضح هذا الرسم مخطط الشبكة الذي يتم إستخدامه:



تكوين LDAP على Active Directory

تثبيت شهادة الهوية على وحدة التحكم بالمجال

لتمكين LDAPs، قم بتثبيت شهادة على وحدة التحكم بالمجال (DC) في بهذه المتطلبات:

1. توجد شهادة LDAP في مخزن الشهادات الشخصية لوحدة التحكم بالمجال.

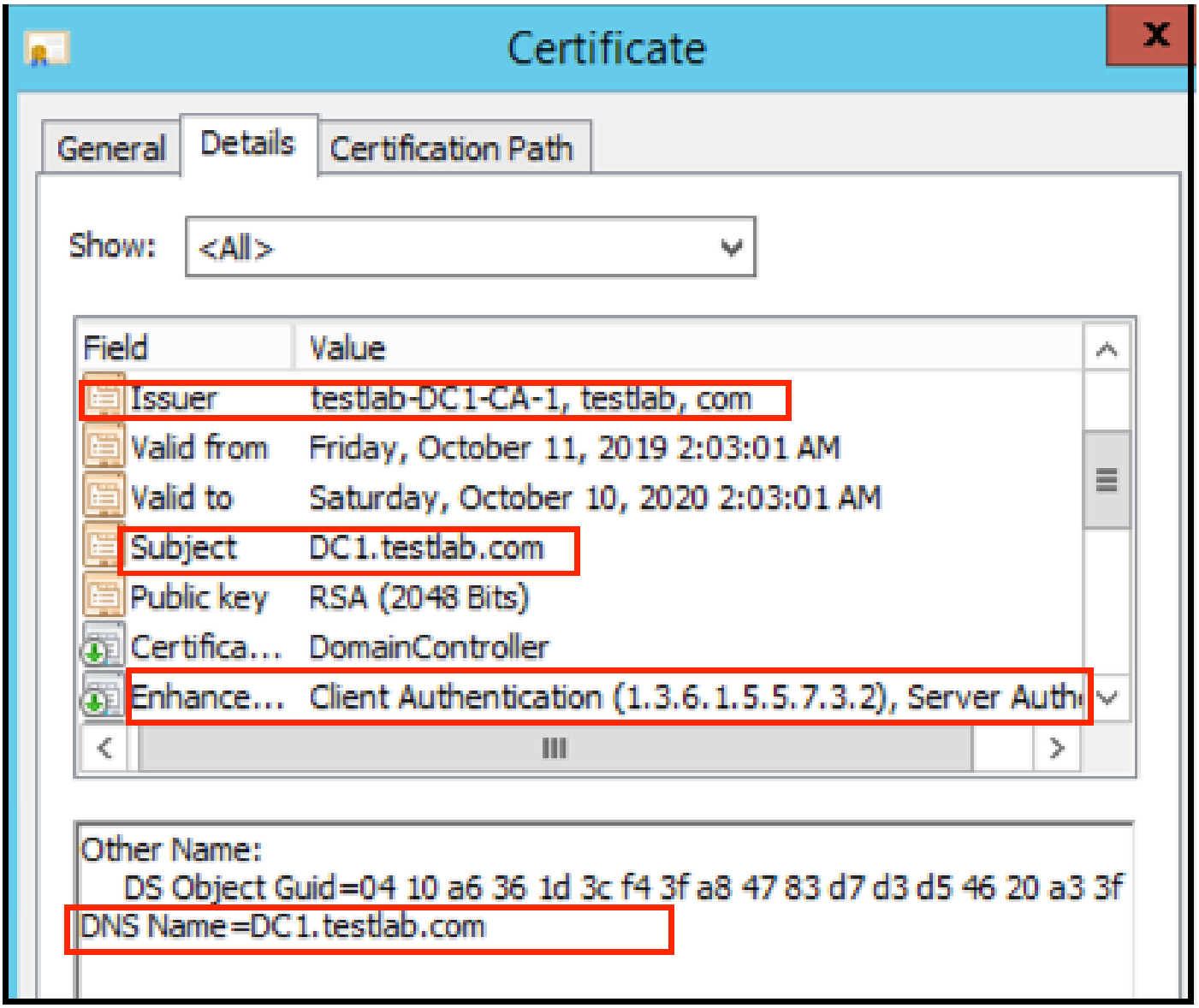
2. يوجد مفتاح خاص مطابق للشهادة في مخزن وحدة التحكم بالمجال ويرتبط بشكل صحيح بالشهادة.

3. يتضمن ملحق إستخدام المفتاح المحسن مصادقة الخادم (1.3.6.1.5.5.7.3.1) معرف الكائن (المعروف أيضا باسم OID).

4. يجب أن يكون اسم المجال المؤهل بالكامل (FQDN) الخاص بوحدة التحكم بالمجال (على سبيل المثال، DC1.testlab.com) موجودا في إحدى هذه السمات: الاسم الشائع (CN) في حقل الموضوع وإدخال DNS في ملحق "الاسم البديل للموضوع".

5. يجب إصدار الشهادة بواسطة مرجع مصدق (CA) يثق به كل من وحدة التحكم بالمجال وعملاء LDAP. للاتصال الآمن الموثوق به، يجب أن يثق العميل والخادم بالمرجع المصدق الجذر الخاص بالآخر وبشهادات المرجع المصدق الوسيطة التي قامت بإصدار شهادات لهم.

6. يجب إستخدام موفر خدمة تشفير Schannel (CSP) لإنشاء المفتاح.



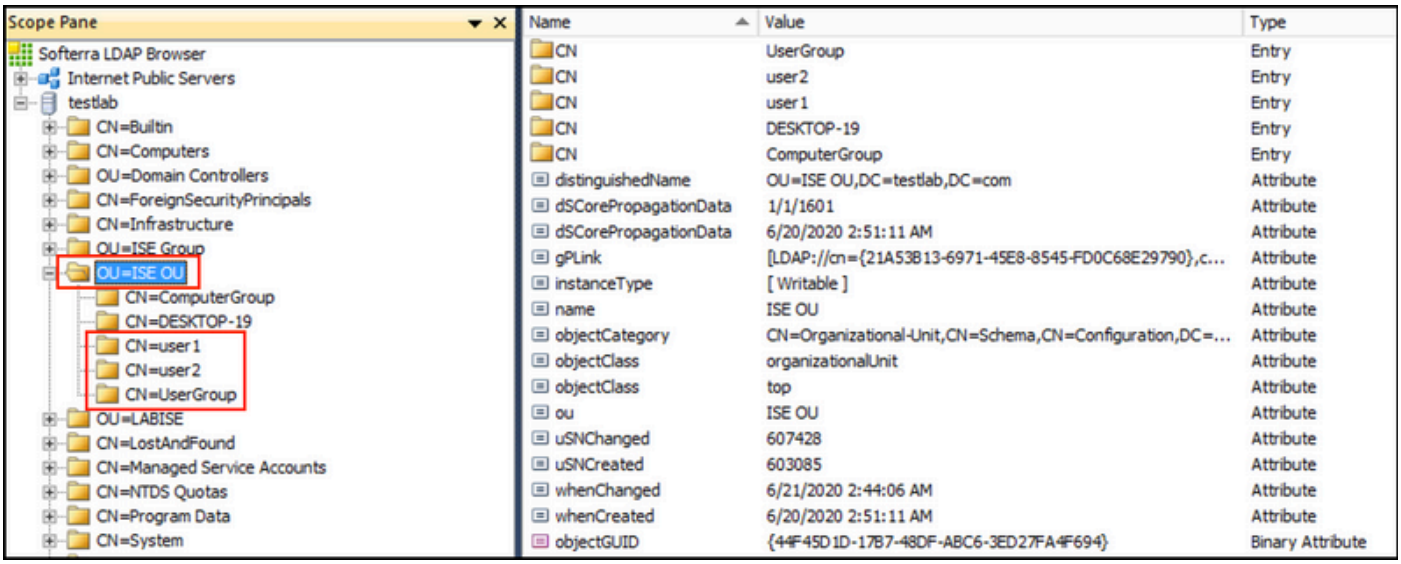
الوصول إلى بنية دليل LDAP

للوصول إلى دليل LDAPs على خادم Active Directory، أستخدم أي مستعرض LDAP. في هذا المختبر، يتم إستخدام متصفح Softera LDAP، الإصدار 4.5.

1. قم بإنشاء اتصال بالمجال على منفذ TCP 636.

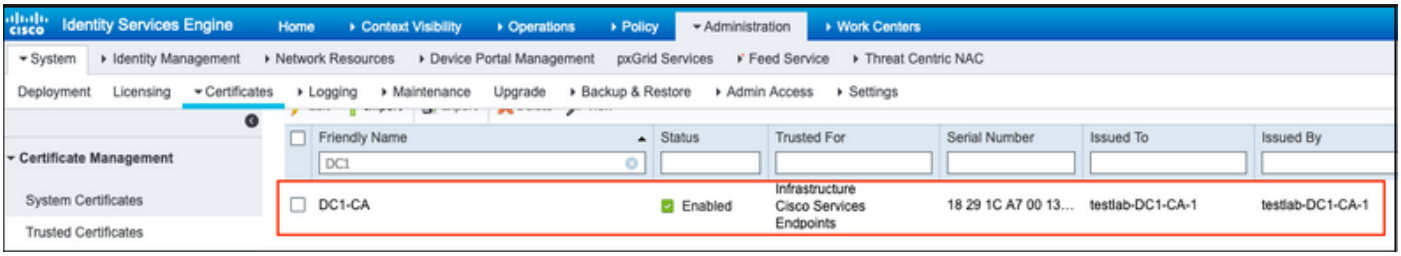
2. من أجل البساطة، قم بإنشاء وحدة تنظيمية (OU) تسمى ISE OU في الإعلان، ويجب أن تحتوي على مجموعة تسمى UserGroup. قم بإنشاء إثنين من المستخدمين (user1 و user2) وجعلهما عضوين في مجموعة UserGroup.

ملاحظة: يستخدم مصدر هوية LDAP على ISE فقط لمصادقة المستخدم.



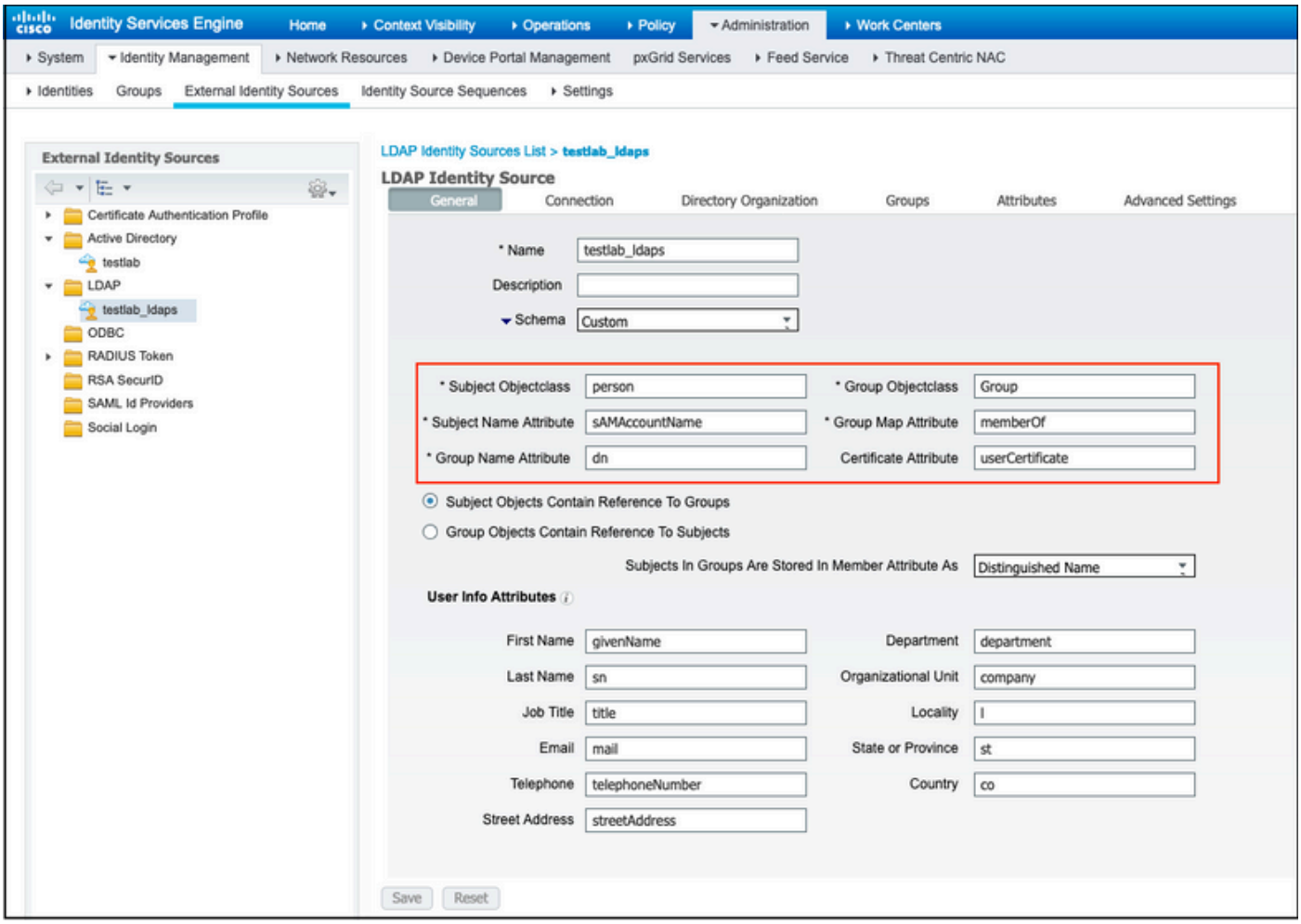
دمج ISE مع خادم LDAP

1. إستيراد شهادة المرجع المصدق الجذر لخادم LDAP في الشهادة الموثوق بها.



2. تحقق من شهادة مسؤول ISE وتأكد من أن شهادة مصدر شهادة مسؤول ISE موجودة أيضا في مخزن الشهادات الموثوق به.

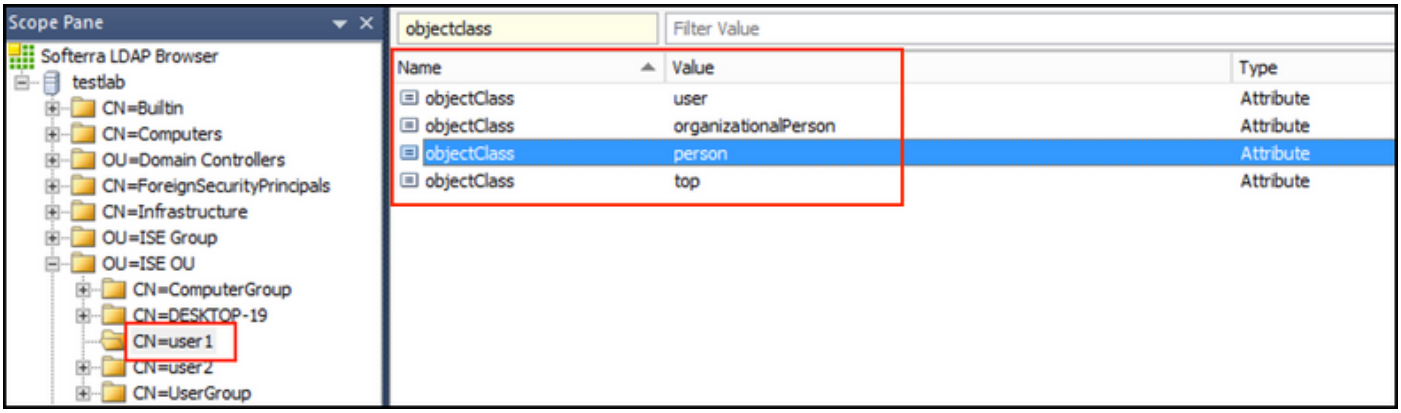
3. من أجل تكامل خادم LDAP، أستخدم سمات LDAP المختلفة من دليل LDAPs. انتقل إلى إدارة > إدارة الهوية > مصادر الهوية الخارجية > مصادر هوية LDAP > إضافة.



4. قم بتكوين هذه السمات من علامة التبويب "عام":

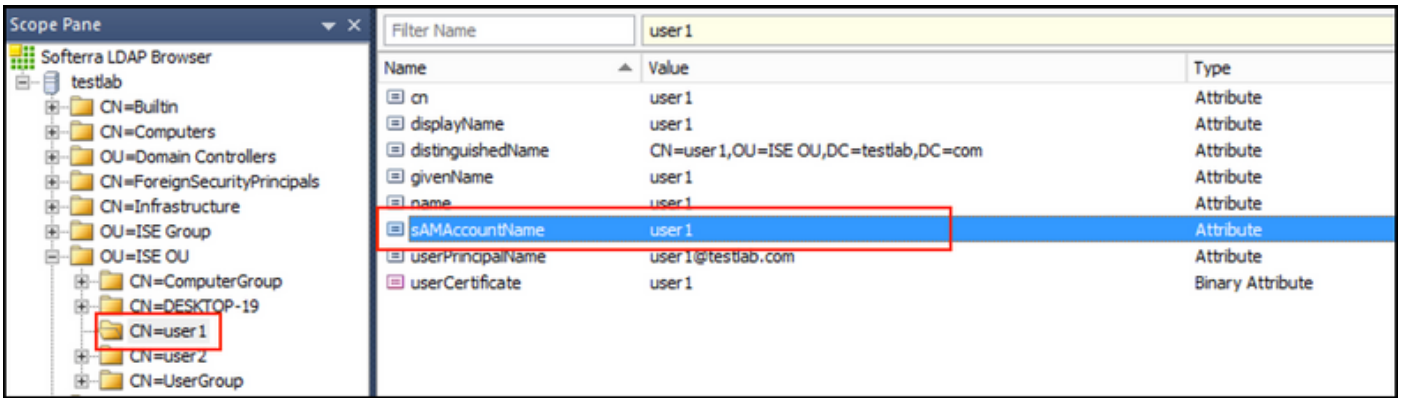
ObjectClass للموضوع: يتوافق هذا الحقل مع فئة Object لحسابات المستخدمين. يمكنك إستخدام أحد الفصول الأربعة هنا:

- أعلى
- شخص
- موظف تنظيمي
- InetOrgPerson

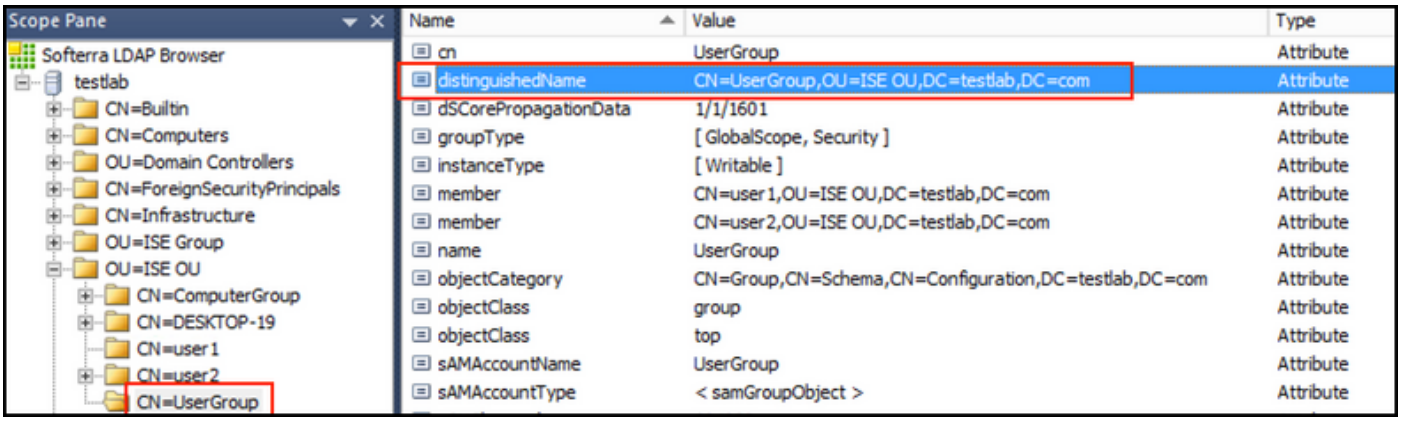


سمة اسم الموضوع: هذا الحقل هو اسم السمة التي تحتوي على اسم المستخدم من الطلب. يتم إستردادهذه السمة من LDAPs عندما يستفسر ISE عن اسم مستخدم محدد في قاعدة

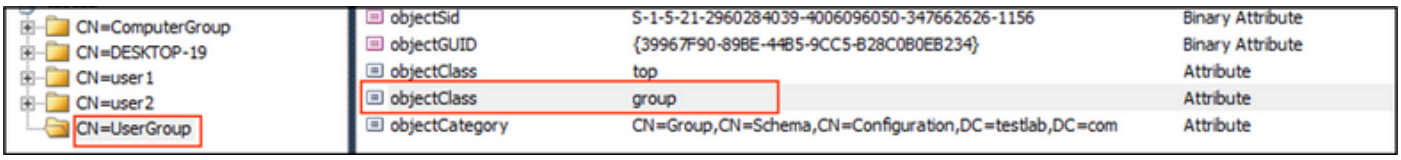
بيانات LDAP (يمكنك إستخدام cn، sAMAccountName، وما إلى ذلك). في هذا السيناريو، يتم إستخدام اسم مستخدم1 على نقطة النهاية.



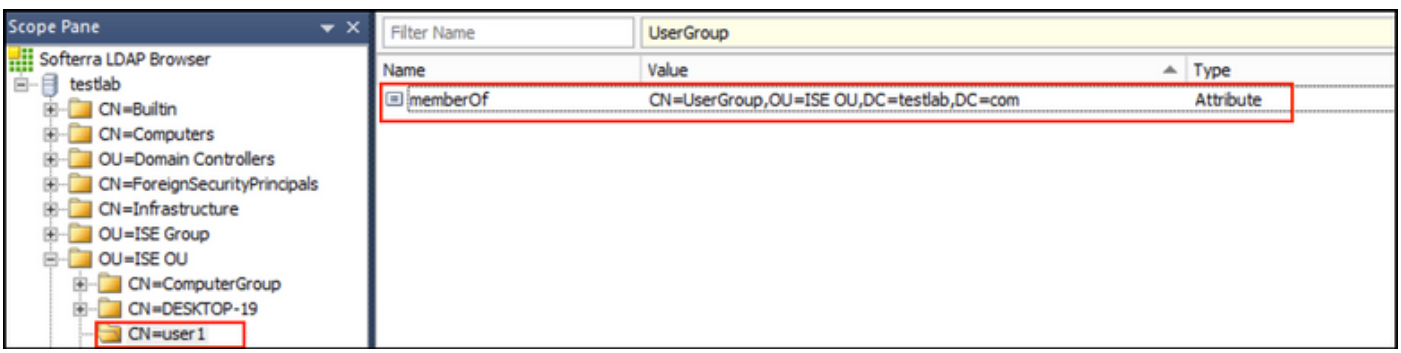
سمة اسم المجموعة: هذه هي السمة التي تحمل اسم مجموعة. يجب أن تتطابق قيم سمة اسم المجموعة الموجودة في دليل LDAP مع أسماء مجموعة LDAP الموجودة في صفحة مجموعات المستخدمين



ObjectClass للمجموعة: يتم إستخدام هذه القيمة في عمليات البحث لتحديد الكائنات المتعرف عليها كمجموعات.



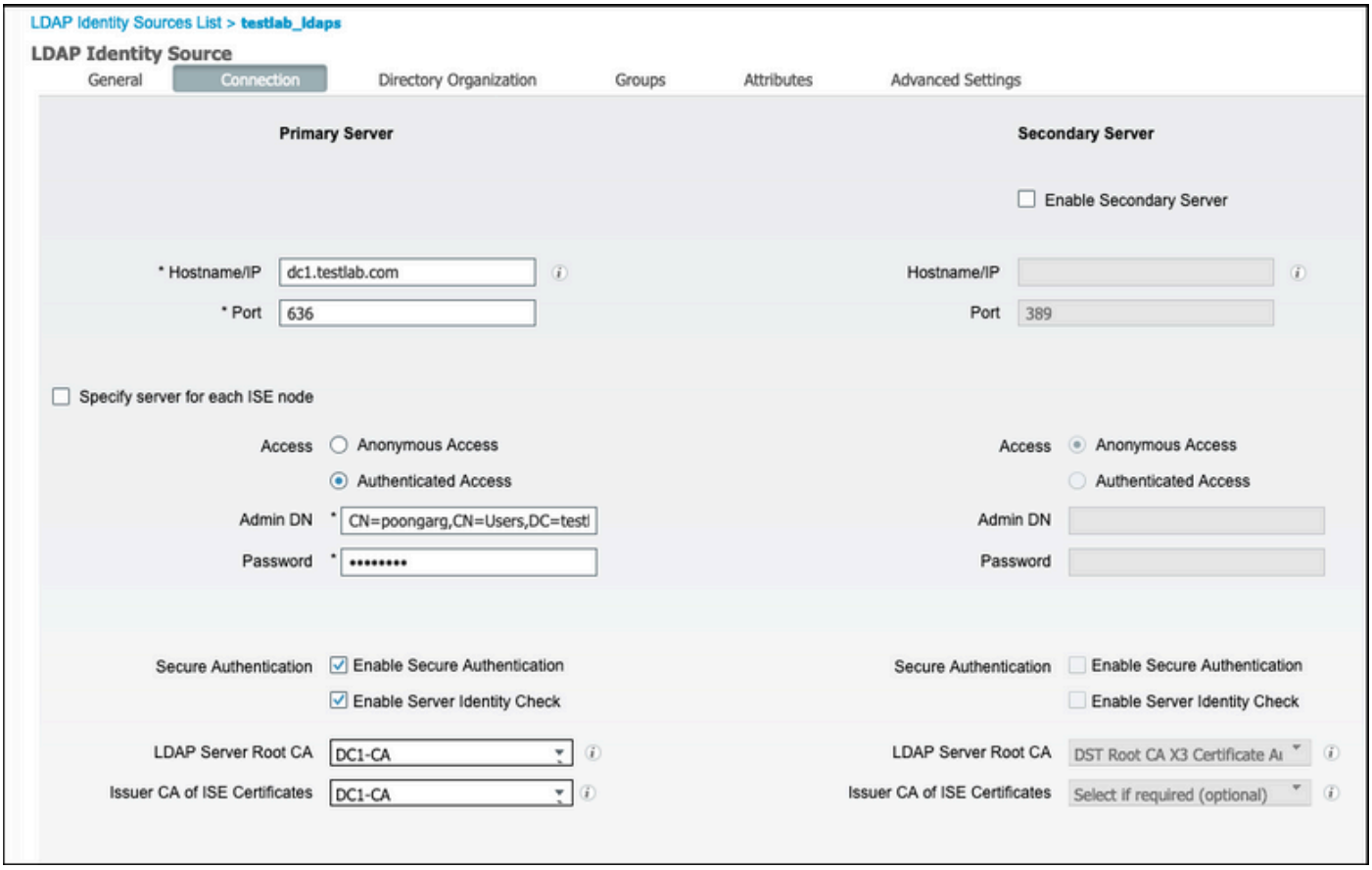
سمة مخطط المجموعة: تحدد هذه السمة كيفية تعيين المستخدمين إلى المجموعات.

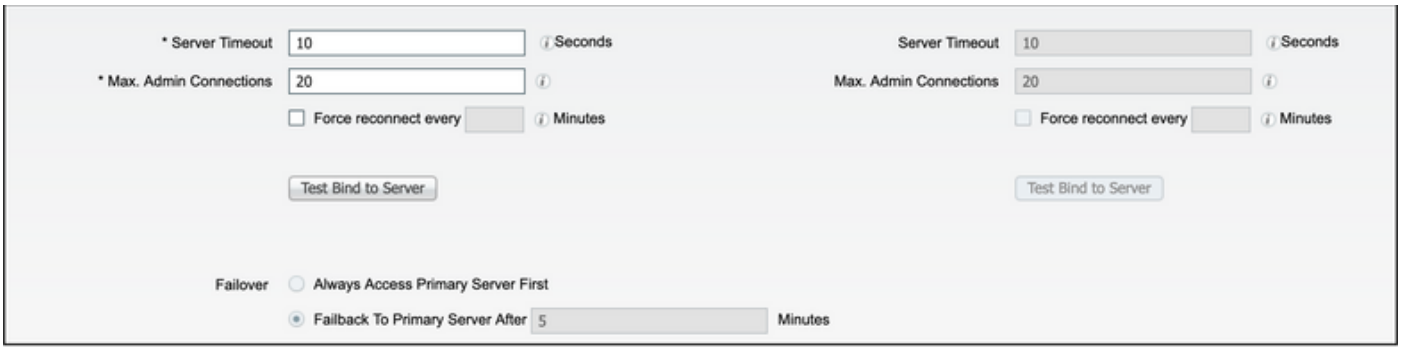


سمة الشهادة: أدخل السمة التي تحتوي على تعريفات الشهادة. يمكن إستخدام هذه

التعريفات إختياري للتحقق من صحة الشهادات التي يتم تقديمها بواسطة العملاء عندما يتم تعريفها كجزء من ملف تعريف مصادقة الشهادة. وفي مثل هذه الحالات، يتم إجراء مقارنة ثنائية بين شهادة العميل والشهادة التي تم إستردادها من مصدر هوية LDAP.

5. لتكوين اتصال LDAPs، انتقل إلى علامة التبويب توصيل :





6. قم بتشغيل البيانات على وحدة التحكم بالمجال للحصول على اسم المستخدم DN لاستخدامه في إجراء اتصال بخادم LDAP:

PS C:\Users\Administrator>مستخدم مستخدم -name poongarg
"CN=poongarg،CN=Users،DC=testlab،DC=com"

الخطوة 1. Sحدد عنوان IP الصحيح أو اسم المضيف الصحيح لخادم LDAP، وقم بتعريف منفذ

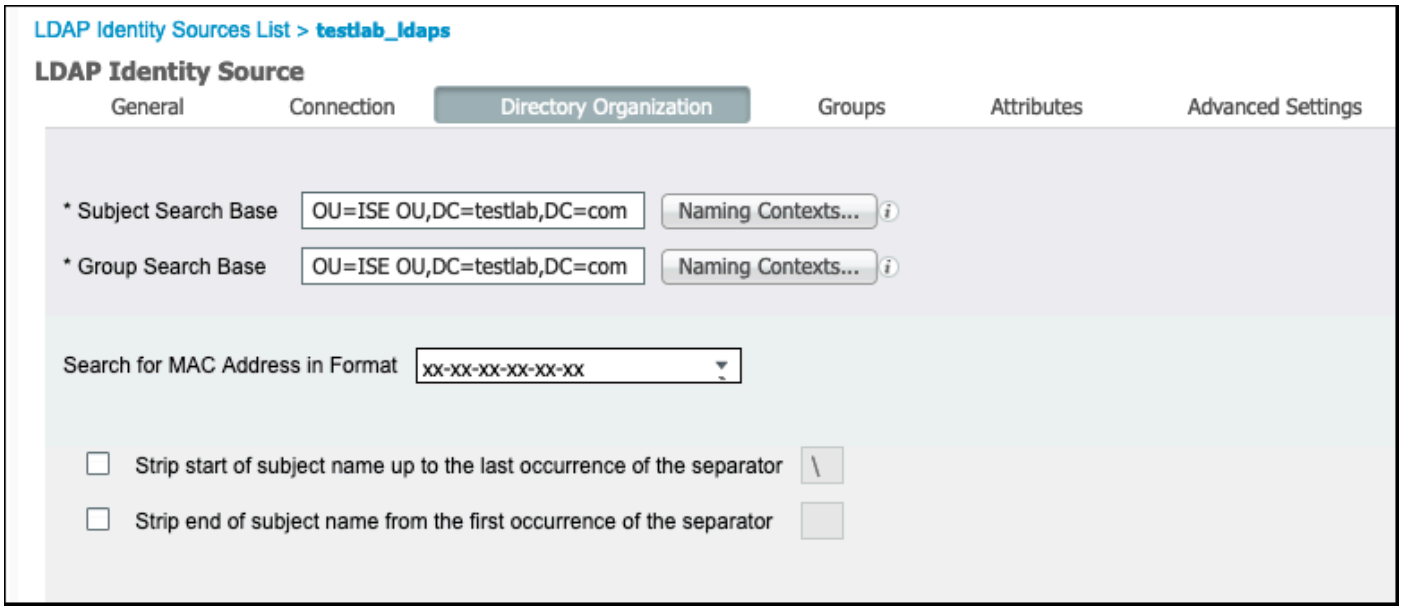
LDAPs (TCP 636)، و Admin DN لإجراء اتصال مع LDAP عبر SSL.

الخطوة 2. قم بتمكين المصادقة الآمنة وخيار التحقق من هوية الخادم.

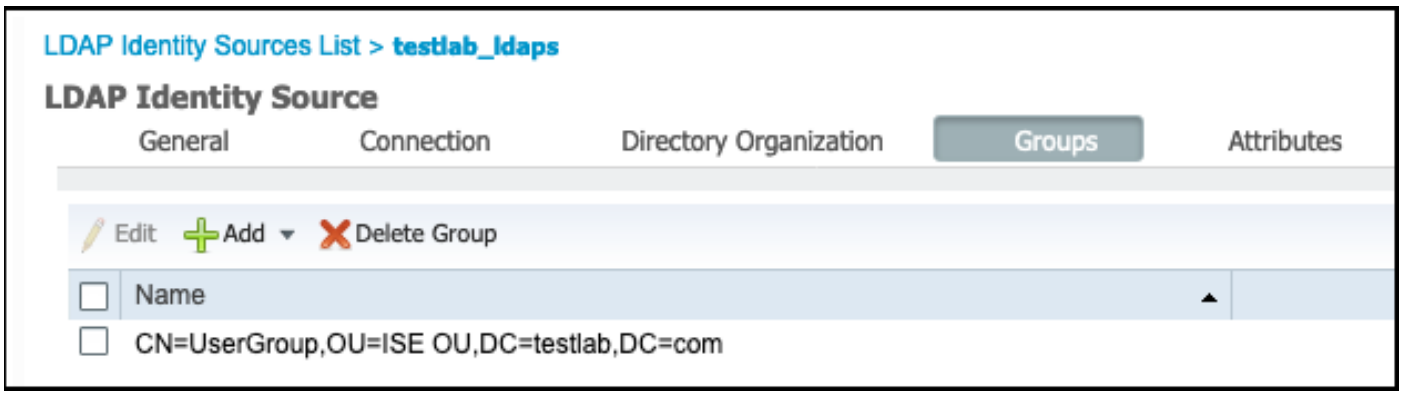
الخطوة 3. من القائمة المنسدلة، حدد شهادة المرجع المصدق الجذر لخادم LDAP وشهادة مسؤول ISE شهادة المرجع المصدق (لقد إستخدمنا مرجع الشهادة المثبت على نفس خادم LDAP لإصدار شهادة مسؤول ISE أيضا).

الخطوة 4. حدد إختبار الربط بالخادم. عند هذه النقطة، ال يتم إسترداد أي أشخاص أو مجموعات لأنه لم يتم تكوين قواعد البحث بعد.

7. تحت علامة التبويب مؤسسة الدليل، قم بتكوين قاعدة بحث الموضوع/المجموعة. إنها نقطة الربط ل ISE مع LDAP. الآن يمكنك إسترجاع فقط المواضيع والمجموعات التي هي أطفال نقطة الربط. في هذا السيناريو، يتم إسترداد كل من الموضوع والمجموعة من OU=ISE OU



8. تحت المجموعات، انقر فوق إضافة لاستيراد المجموعات من LDAP على ISE واسترداد المجموعات، كما هو موضح في هذه الصورة.



تكوين المحول

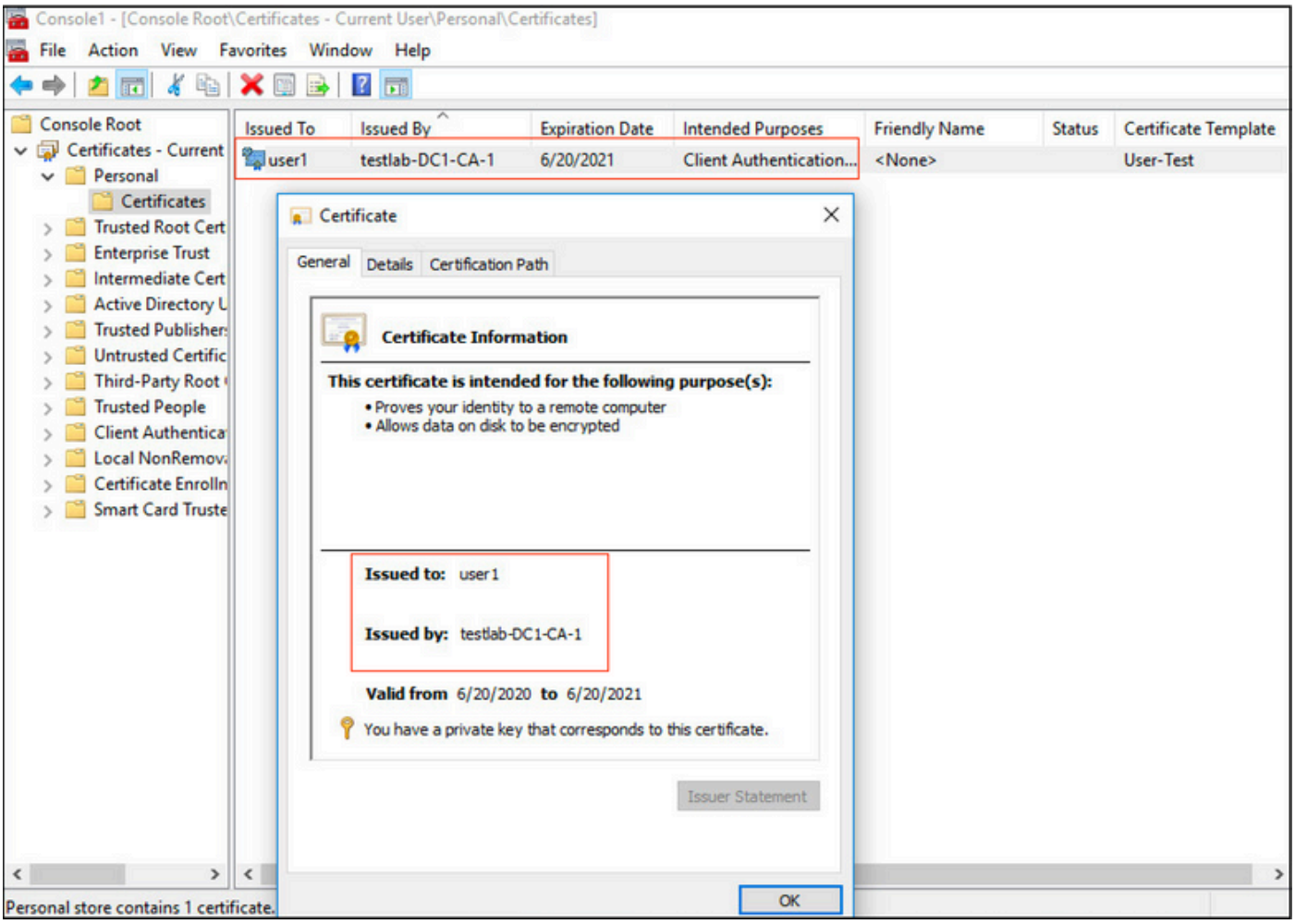
قم بتكوين المحول لمصادقة 802.1x. جهاز كمبيوتر Windows متصل بـ switchport gig2/0/47

```
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
```

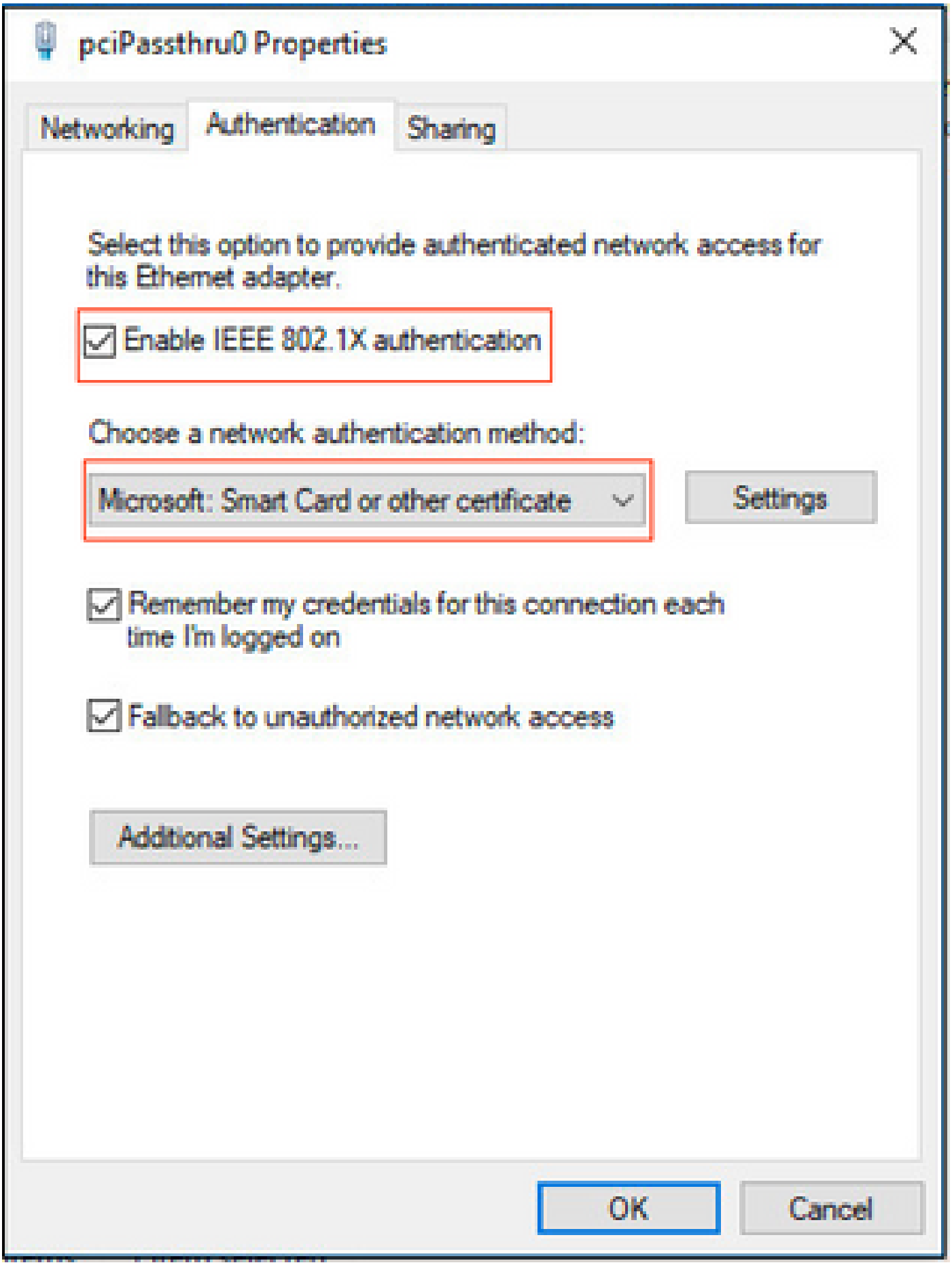
تكوين نقطة النهاية

يستخدم Windows Native Plus ويستخدم أحد بروتوكولات EAP المدعومة LDAP، EAP-TLS لمصادقة المستخدم والتفويض.

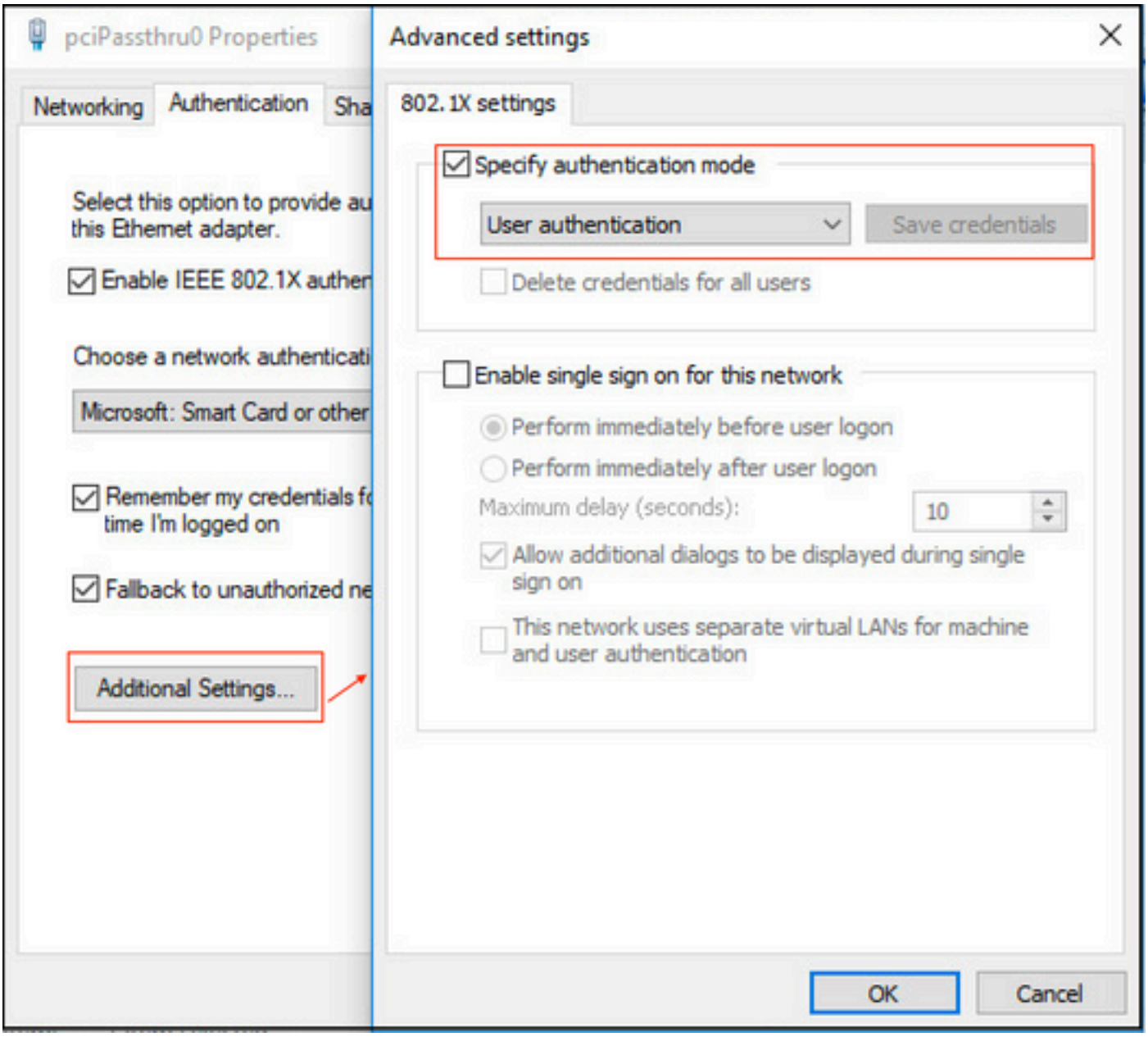
1. تأكد من وزارة الكمبيوتر بشهادة المستخدم (للمستخدم 1) ومن وجود الغرض المقصود منه مصادقة العميل في "شهادات التصديق الجذر الموثوق بها"، أو سلسلة شهادات مماثلة موجودة على الكمبيوتر الشخصي.



2. تمكين مصادقة dot1x وتحديد أسلوب المصادقة كبطاقة Microsoft:Smart أو شهادة أخرى لمصادقة EAP-TLS.

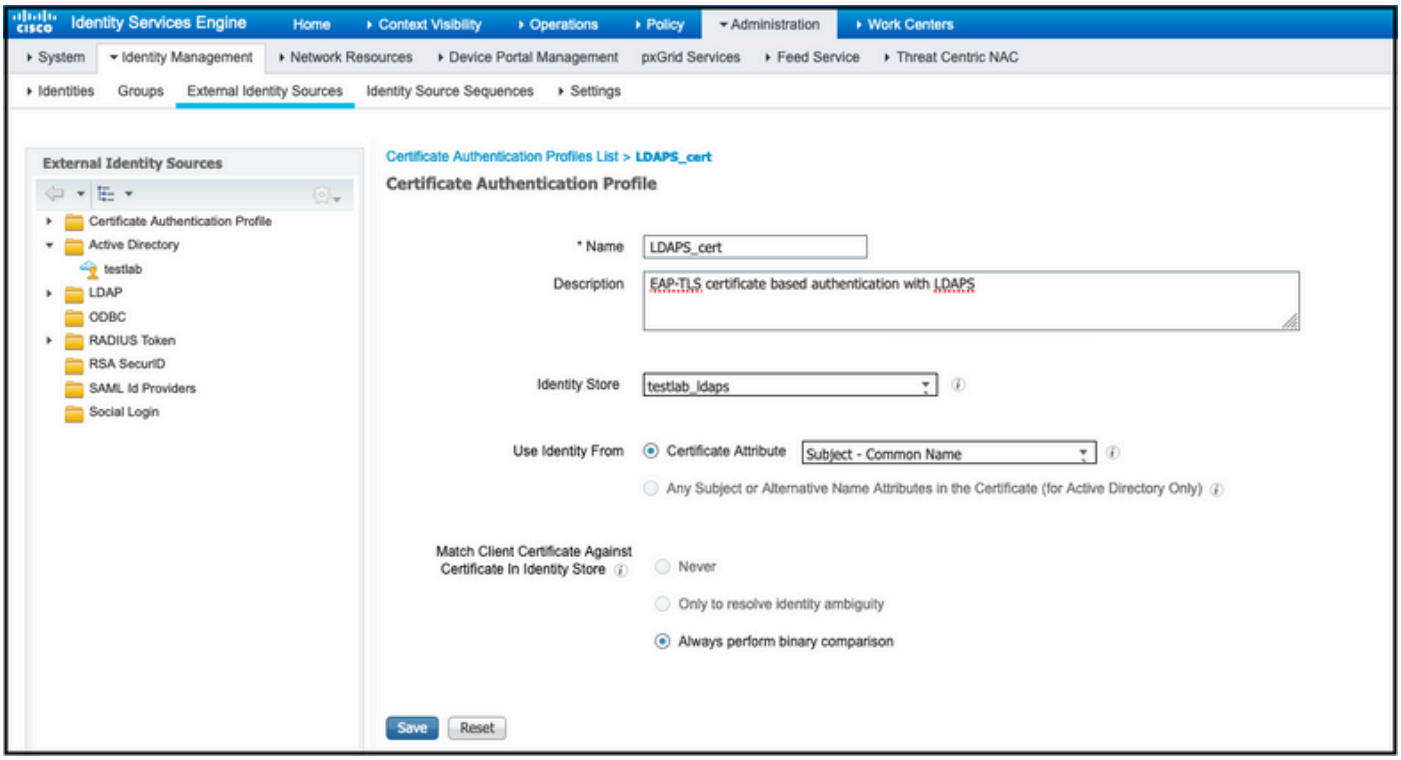


3. انقر فوق "إعدادات إضافية"، ويفتح إطار. حدد المربع مع تحديد وضع المصادقة واختر مصادقة المستخدم، كما هو موضح في هذه الصورة.

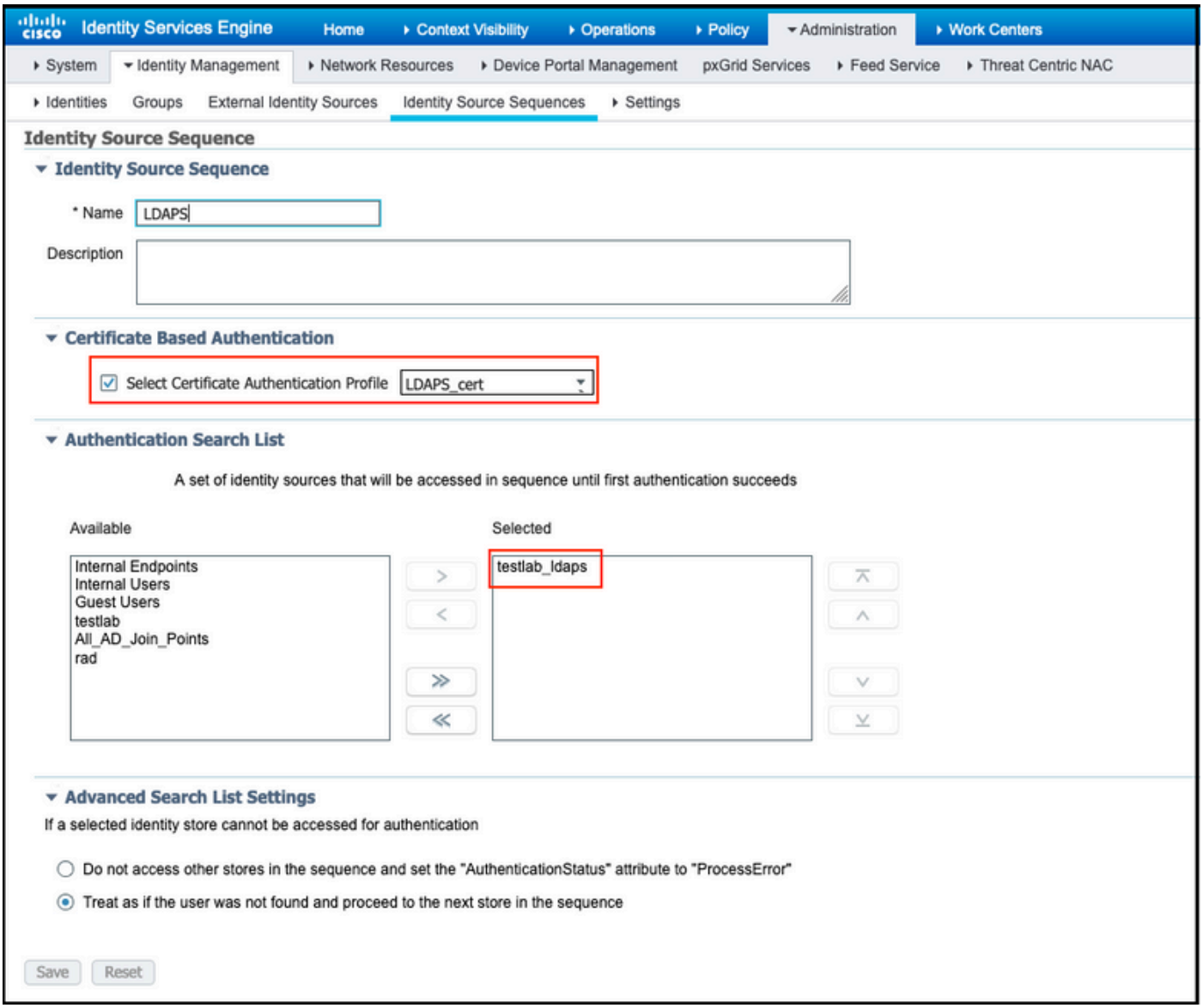


تكوين مجموعة النهج على ISE

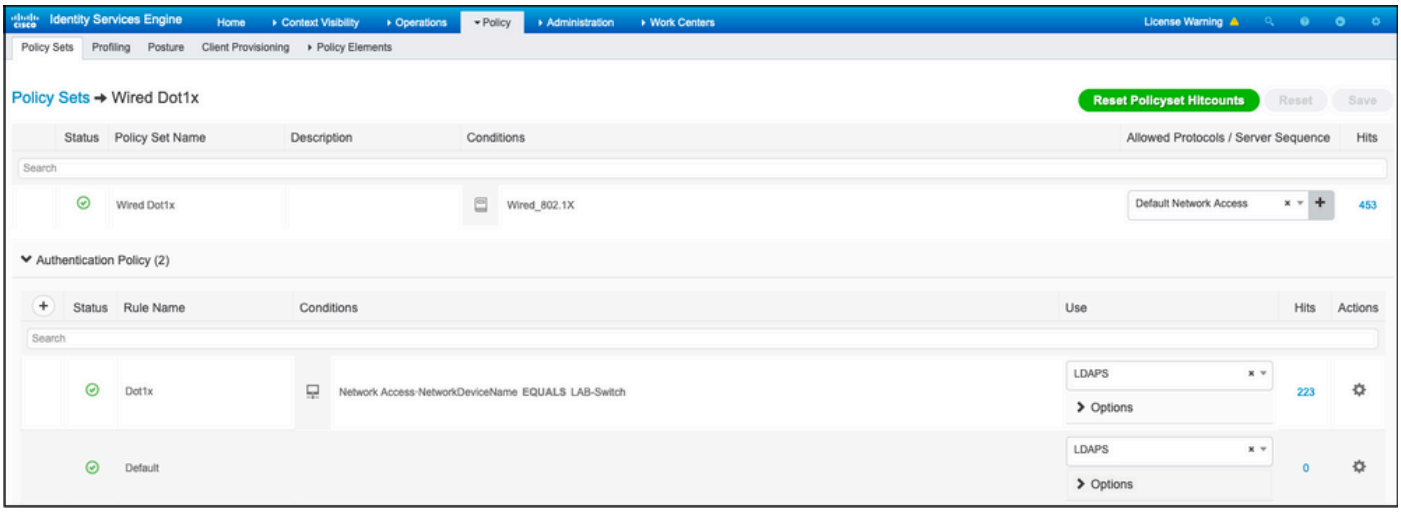
منذ إستخدام بروتوكول EAP-TLS، وقبل تكوين مجموعة النهج، يلزم تكوين ملف تعريف مصادقة الشهادة واستخدام تسلسل مصدر الهوية في نهج المصادقة فيما بعد.



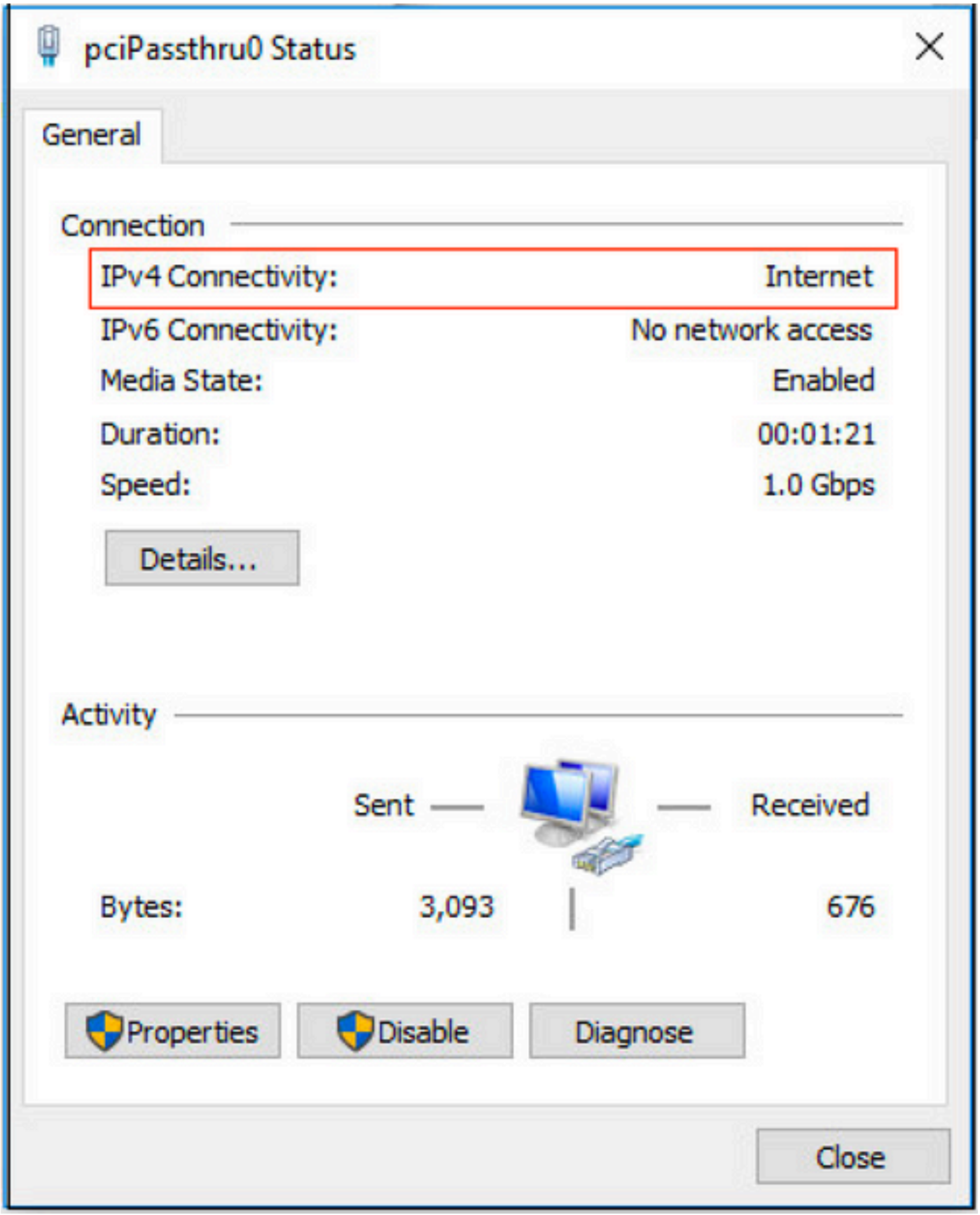
ارجع إلى ملف تعريف مصادقة الشهادة في تسلسل مصدر الهوية وحدد مصدر الهوية الخارجي LDAP في قائمة البحث عن المصادقة:



تكوين مجموعة النهج الآن لمصادقة Wired Dot1x:



بعد هذا التكوين، يمكننا مصادقة نقطة النهاية باستخدام بروتوكول EAP-TLS مقابل مصدر هوية LDAP.

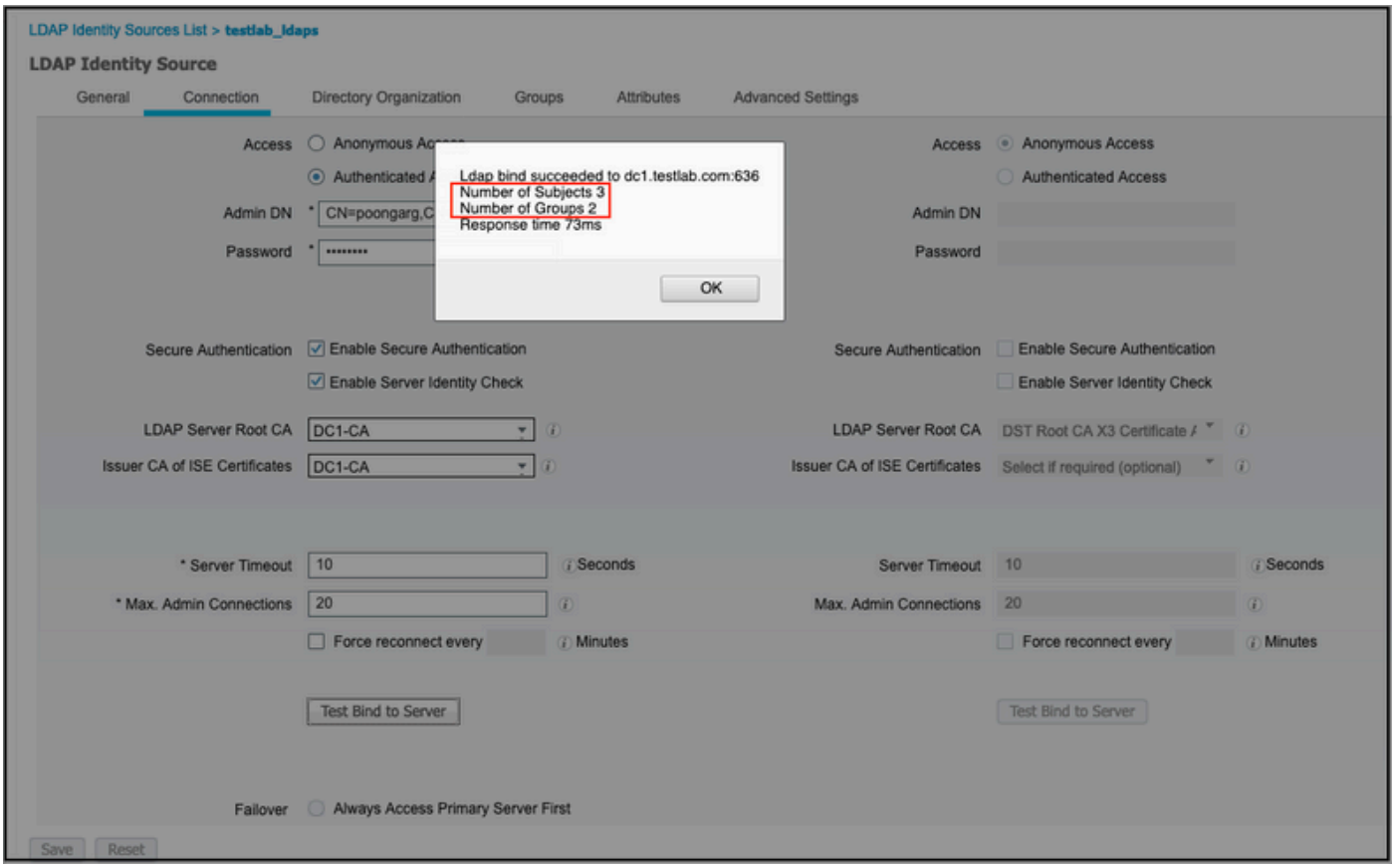


التحقق من الصحة

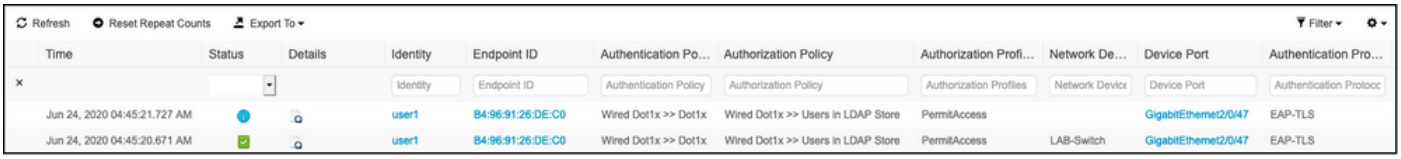
1. تحقق من جلسة المصادقة على Switchport المتصل بالكمبيوتر الشخصي:

```
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:  0A6A263900000130798C66612
     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
```

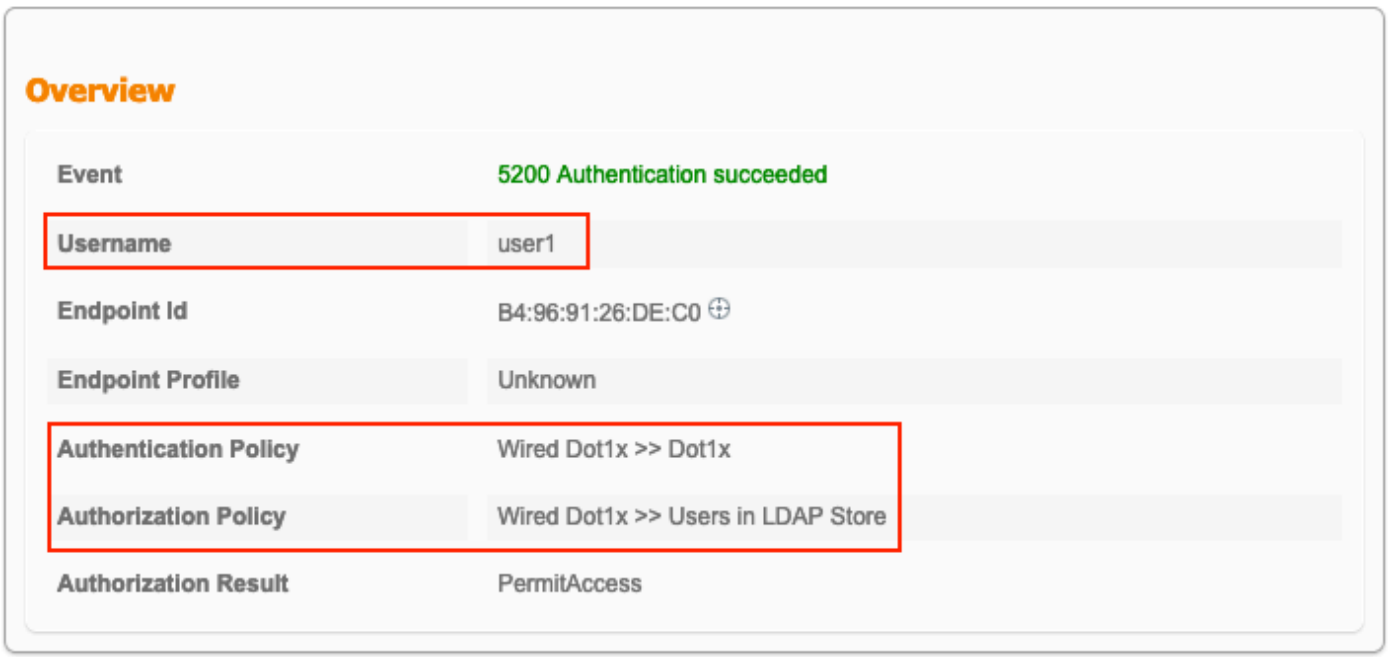
2. للتحقق من تكوينات LDAP و ISE، يمكنك إستدراد الموضوعات والمجموعات باستخدام اتصال إختبار بالخادم:



3. التحقق من تقرير مصادقة المستخدم:



4. تحقق من تقرير المصادقة التفصيلي لنقطة النهاية:



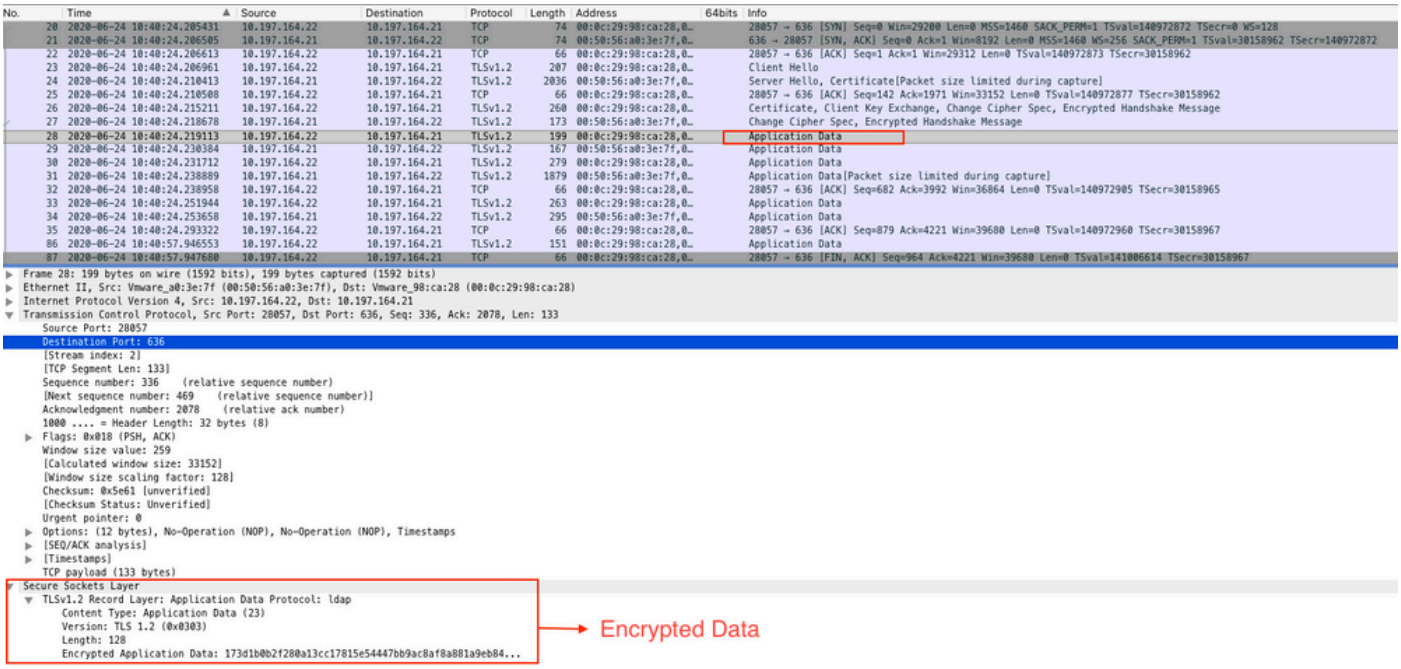
Authentication Details

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_ldaps
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. تحقق من تشفير البيانات بين ISE وخادم LDAP من خلال التقاط الحزم على ISE باتجاه خادم LDAPs:



استكشاف الأخطاء وإصلاحها

يصف هذا القسم بعض الأخطاء الشائعة التي تتم مصادفتها مع هذا التكوين وكيفية أستكشاف الأخطاء وإصلاحها.

- في تقرير المصادقة، يمكنك رؤية رسالة الخطأ هذه:

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

تشير رسالة الخطأ هذه إلى أن الأسلوب الذي إخترته غير معتمد بواسطة LDAP. تأكد من أن بروتوكول المصادقة في نفس التقرير يوضح إحدى الطرق المدعومة (EAP-GTC أو EAP-TLS أو PEAP-TLS).

- انتهى إختبار الربط بالخادم مع حدوث خطأ.

يرجع السبب في ذلك بشكل شائع إلى فشل التحقق من صحة شهادة خادم LDAPS. in order to تحريت هذا نوع إصدار، أخذت ربط التقاط على ISE وتمكنت all the ثلاثة وقت تشغيل ومكونات prrt-jni على مستوى تصحيح الأخطاء، أنعشت الإصدار، وفحصت ال prrt-server.log مبرد.

يشكو التقاط الحزمة حول شهادة سيئة وعروض خادم المنفذ:

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

ملاحظة: يجب تكوين اسم المضيف في صفحة LDAP باسم موضوع الشهادة (أو أي اسم من الاسم البديل للموضوع). لذلك ما لم يكن لديك مثل هذا في الموضوع أو شهادة شبكة منطقة التخزين (SAN)، فلا يعمل، فيلزمك ترخيص بعنوان IP في شهادة شبكة منطقة التخزين (SAN).

3. في تقرير المصادقة، يمكنك ملاحظة عدم العثور على الموضوع في مخزن الهوية. هذا يعني أن اسم المستخدم من التقرير السابق هو اسم الموضوع لأي مستخدم في قاعدة بيانات LDAP. في هذا السيناريو، تم تعيين القيمة إلى sAMAccountName لهذه السمة، مما يعني أن ISE ينظر إلى قيمة sAMAccountName لمستخدم LDAP عندما يحاول العثور على تطابق.

4. تعذر إسترداد الموضيع والمجموعات بشكل صحيح أثناء إختبار ربط الخادم. السبب الأكثر إحتمالا لهذه المشكلة هو تكوين غير صحيح لقواعد البحث. تذكر أنه يجب تحديد التسلسل الهيكلي ل LDAP من الوحدة الطرفية إلى الجذر و dc (يمكن أن يتكون من كلمات متعددة).

معلومات ذات صلة

- 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

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).