802.1x EAP-TLS مع مقارنة شهادات ثنائية من NAM و AD وتوصيفات تكوين مثال

المحتويات

المقدمة

يصف هذا المستند تكوين 802.1x مع بروتوكول المصادقة المتوسع - أمان طبقة النقل (EAP-TLS) ونظام التحكم في الوصول (ACS) بينما يجريان مقارنة شهادات ثنائية بين شهادة عميل مقدمة من صاحب الطلب ونفس الشهادة محفوظة في Microsoft Active Directory (AD). يتم إستخدام ملف تعريف AnyConnect Network Access Manager (NAM) للتخصيص. يتم تقديم التكوين لجميع المكونات في هذا المستند، بالإضافة إلى سيناريوهات أستكشاف أخطاء التكوين وإصلاحها.

المتطلبات الأساسية

المتطلبات

لا توجد متطلبات خاصة لهذا المستند.

المكونات المستخدمة

لا يقتصر هذا المستند على إصدارات برامج ومكونات مادية معينة.

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 مباشرة، فتأكد من فهمك للتأثير المحتمل لأي أمر.

الاصطلاحات

راجع اصطلاحات تلميحات Cisco التقنية للحصول على مزيد من المعلومات حول اصطلاحات المستندات.

التكوين

طوبولوجيا

- طالب Windows 7 - 802.1x مع Cisco AnyConnect Secure Mobility Client الإصدار 3.1.01065 (وحدة NAM)
- مصدق 802.1x - محول 2960
- خادم مصادقة ACS - 802.1x، الإصدار 5.4
- ACS مدمج مع Microsoft AD - وحدة التحكم بالمجال - Windows 2008 Server

تفاصيل المخطط

- ACS - 192.168.10.152
- 2960 - 192.168.10.10 (E0/0 - متصل بمتلقي)
- DC - 192.168.10.101
- نظام التشغيل Windows 7 - بروتوكول DHCP

إنجاسا

تحتوي محطة Windows 7 على AnyConnect NAM مثبت، والذي يتم إستخدامه كمطلب للمصادقة على خادم ACS باستخدام طريقة EAP-TLS. يعمل المحول المزود ب 802.1x كمصدق. يتم التحقق من شهادة المستخدم بواسطة ACS ويقوم تفويض النهج بتطبيق السياسات المستندة إلى الاسم الشائع (CN) من الشهادة. وبالإضافة إلى ذلك يجلب ACS شهادة المستخدم من AD ويعقد مقارنة ثنائية مع الشهادة المقدمة من الملتمس.

تكوين المبدّل

المفتاح يتلقى تشكيل أساسي. افتراضيا، الميناء في عزل VLAN 666. أن VLAN له وصول مقيد. بعد تخويل المستخدم، تتم إعادة تكوين شبكة VLAN الخاصة بالمنفذ.

```
aaa authentication login default group radius local
aaa authentication dot1x default group radius
```

```
aaa authorization network default group radius
dot1x system-auth-control

interface Ethernet0/0
switchport access vlan 666
switchport mode access
ip device tracking maximum 10
duplex auto
authentication event fail action next-method
authentication order dot1x mab
authentication port-control auto
dot1x pae authenticator
end

radius-server host 192.168.10.152 auth-port 1645 acct-port 1646 key cisco
```

تجهيز الشهادة

يشترط في EAP-TLS أن تكون هناك شهادة للمطالب وخادم المصادقة. يعتمد هذا المثال على الشهادات التي تم إنشاؤها ل OpenSSL. يمكن إستخدام المرجع المصدق (CA) من Microsoft لتبسيط عملية النشر في شبكات المؤسسات.

1. دخلت in order to خلقت ال CA، هذا أمر:

```
openssl genrsa -des3 -out ca.key 1024
openssl req -new -key ca.key -out ca.csr
cp ca.key ca.key.org
openssl rsa -in ca.key.org -out ca.key
openssl x509 -req -days 365 -in ca.csr -signkey ca.key -out ca.crt
```

يتم الاحتفاظ بشهادة CA في ملف ca.crt والمفتاح الخاص (وغير المحمي) في ملف ca.key.

2. قم بإنشاء ثلاث شهادات مستخدم وشهادة ل ACS، جميعها موقعة من قبل :CA
CN=test1CN=test2CN=test3cn=acs54البرنامج النصي لإنشاء شهادة واحدة موقعة من قبل CA من Cisco هو:

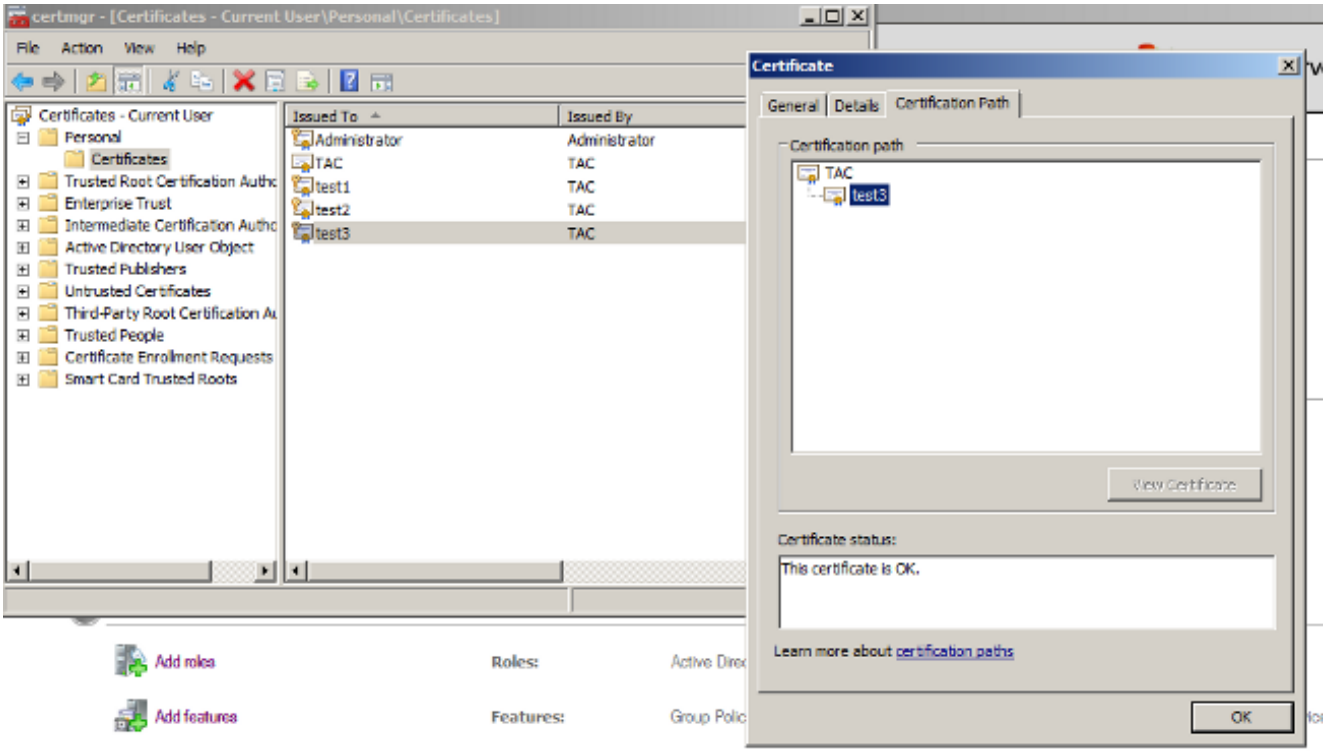
```
openssl genrsa -des3 -out server.key 1024
openssl req -new -key server.key -out server.csr

cp server.key server.key.org
openssl rsa -in server.key.org -out server.key

openssl x509 -req -in server.csr -CA ca.crt -CAkey ca.key -CAcreateserial
out server.crt -days 365-
openssl pkcs12 -export -out server.pfx -inkey server.key -in server.crt
certfile ca.crt-
```

المفتاح الخاص موجود في ملف server.key والشهادة موجودة في ملف server.crt. ال pkcs12 صيغة في ال server.pfx مبرد.

3. انقر نقرا مزدوجا على كل شهادة (.pfx file) لاستيرادها إلى وحدة التحكم بالمجال. في وحدة التحكم بالمجال، يجب الوثوق بجميع الشهادات الثلاثة.

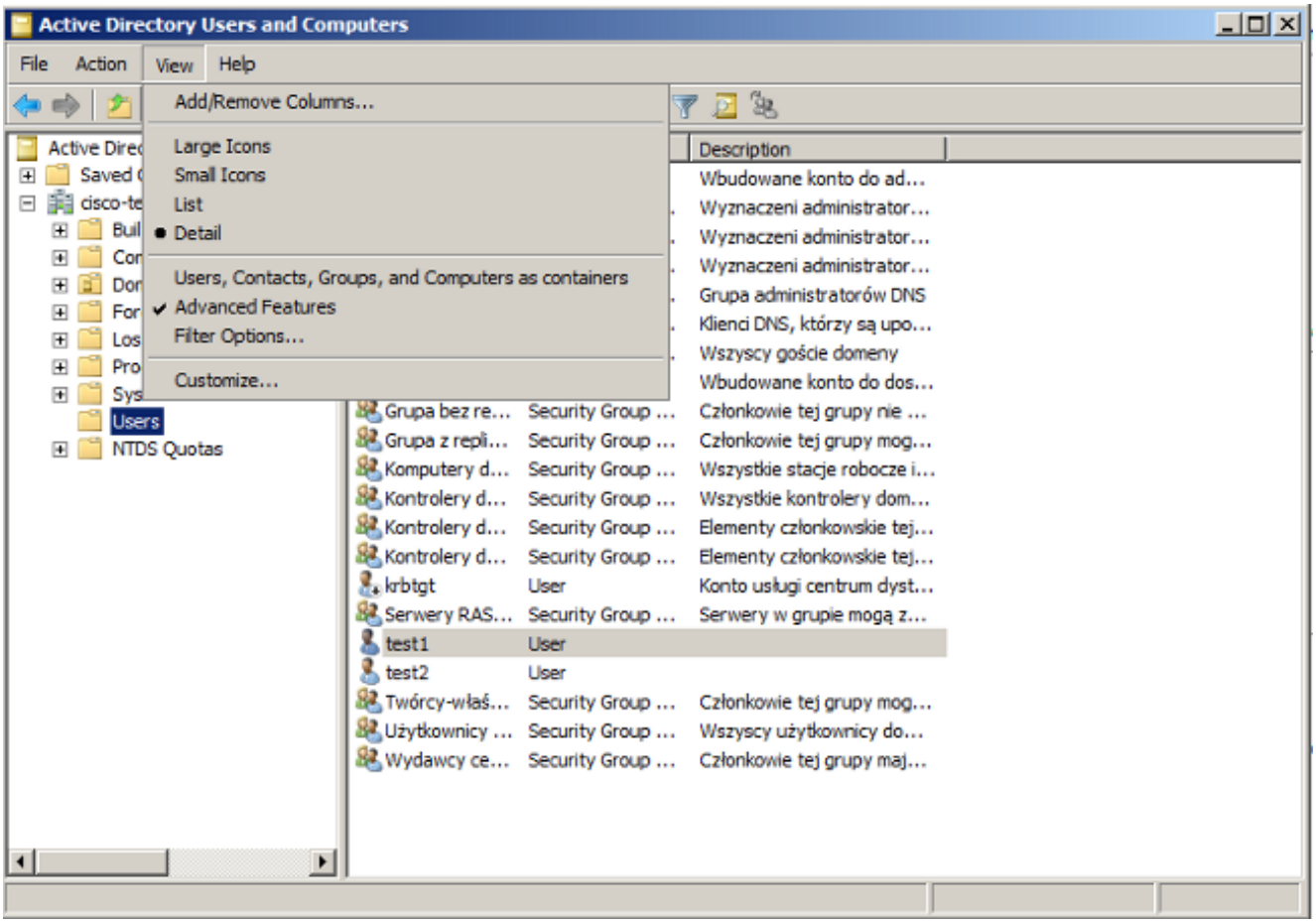


يمكن اتباع نفس العملية في نظام التشغيل Windows 7 (الملحق) أو إستخدام خدمة Active Directory للضغط على شهادات المستخدم.

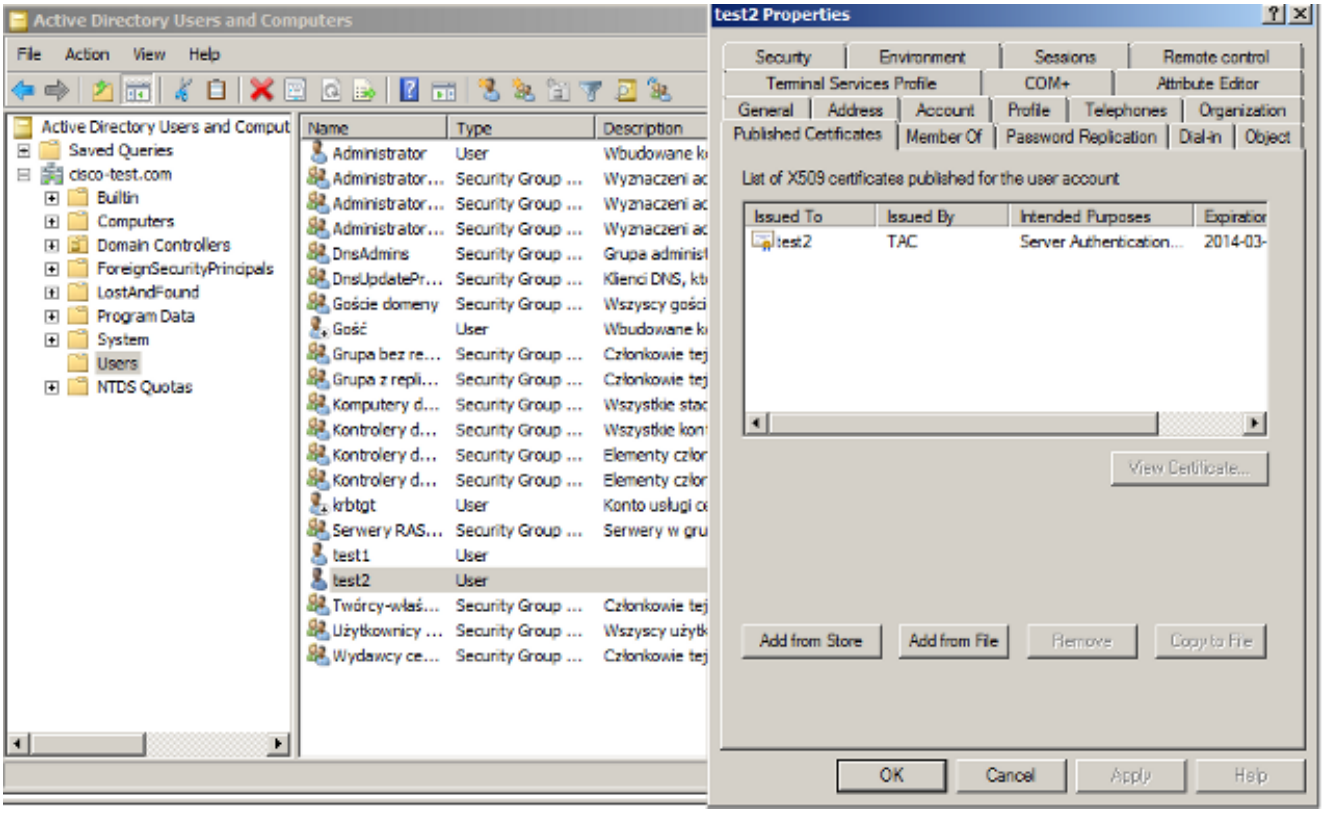
تكوين وحدة التحكم بالمجال

من الضروري تعيين الشهادة المحددة للمستخدم المحدد في AD.

1. من Active Directory Users and Computers، انتقل إلى مجلد **Users**.
2. من قائمة عرض، أختر **ميزات متقدمة**.



3. إضافة هؤلاء المستخدمين: الاختبار 1إختبار 2إختبار 3**ملاحظة**: كلمة المرور غير مهمة.
4. من نافذة الخصائص، أختر علامة التبويب **الشهادات المنشورة**. أختر الشهادة المحددة للاختبار. على سبيل المثال، للاختبار 1 يكون المستخدم CN هو test1.**ملاحظة**: لا تستخدم تعيين الاسم (انقر بزر الماوس الأيمن فوق اسم المستخدم). يتم إستخدامه لخدمات مختلفة.



في هذه المرحلة، يتم ربط الشهادة بمستخدم معين في AD. يمكن التحقق من هذا باستخدام ldapsearch:

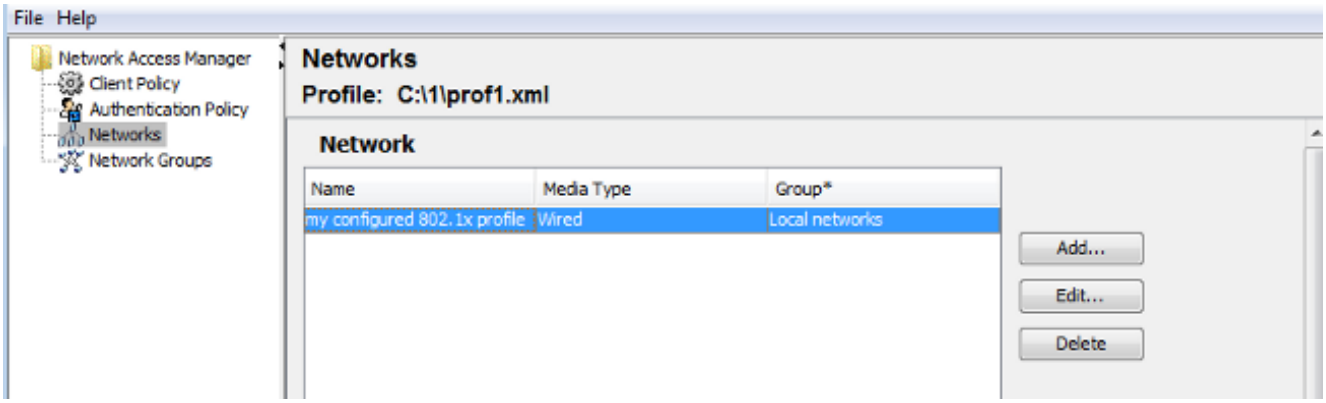
```
ldapsearch -h 192.168.10.101 -D "CN=Administrator,CN=Users,DC=cisco-test,DC=com" -w
"Adminpass -b "DC=cisco-test,DC=com
```

فيما يلي نتائج المثال للاختبار 2:

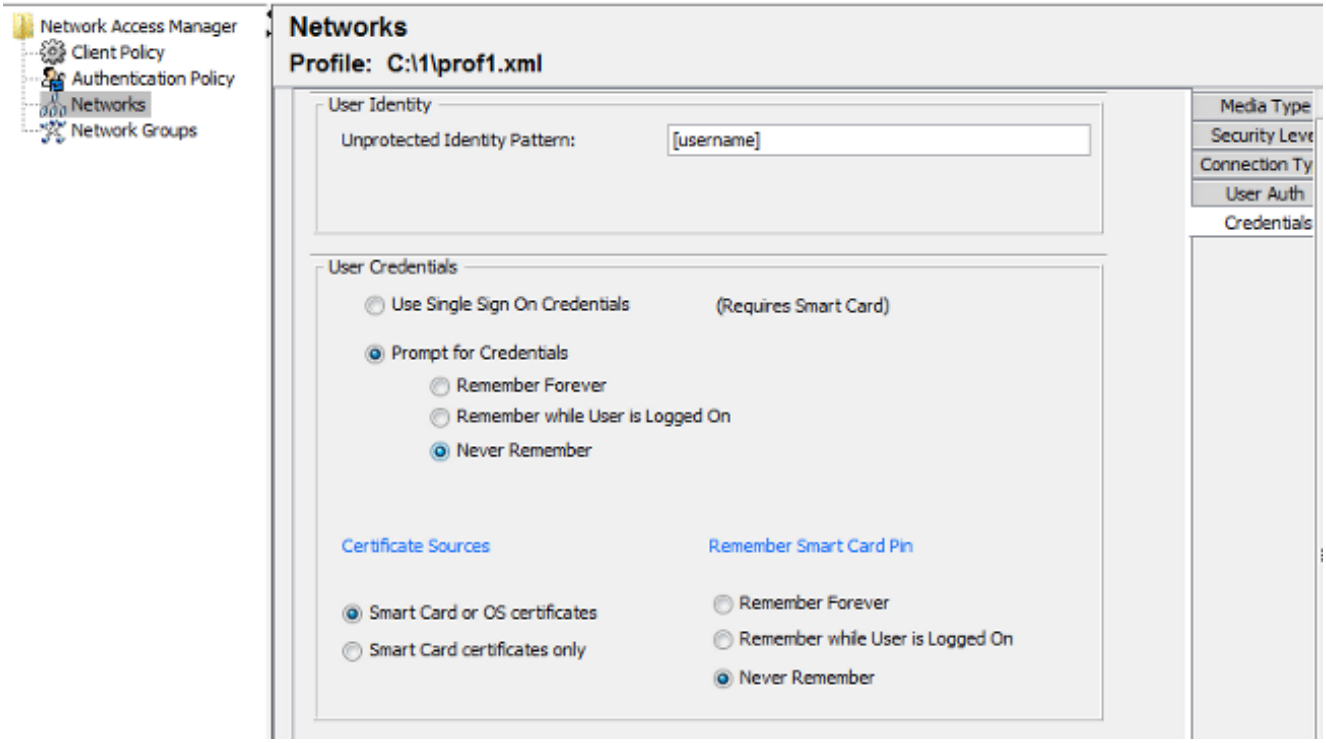
```
test2, Users, cisco-test.com #
dn: CN=test2,CN=Users,DC=cisco-test,DC=com
.................
userCertificate:: MIICuDCCAiGgAwIBAgIJAP6cPWHhMc2yMA0GCSqGSIb3DQEBBQUAMFYxCzAJ
 BgNVBAYTAlBMMQwwCgYDVQQIDANNYXoxDzANBgNVBAcMBldhcnNhdzEMMAoGA1UECgwDVEFDMQwwC
 gYDVQQLDANSQUMxDDAKBgNVBAMMA1RBQzAeFw0xMzAzMDYxMjUzMjdaFw0xNDAzMDYxMjUzMjdaMF
 oxCzAJBgNVBAYTAlBMMQswCQYDVQQIDAJQTDEPMA0GA1UEBwwGS3Jha293MQ4wDAYDVQQKDAVDaXN
 jbzENMAsGA1UECwwEQ29yZTEOMAwGA1UEAwwFdGVzdDIwgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJ
 AoGBAMFQZywrGTQKL+LeI19ovNavCFSG2zt2HGs8qGPrf/h3o4IIvU+nN6aZPdkTdsjiuCeav8HYD
 aRznaK1LURt1PeGtHlcTgcGZ1MwIGptimzG+h234GmPU59k4XSVQixARCDpMH8IBR9zOSWQLXe+kR
 iZpXC444eKOh6wO/+yWb4bAgMBAAGjgYkwgYYwCwYDVR0PBAQDAgTwMHcGA1UdJQRwMG4GCCsGAQU
 FBwMBBggrBgEFBQcDAgYKKwYBBAGCNwoDBAYLKwYBBAGCNwoDBAEGCCsGAQUFBwMBBggrBgEFBQgC
 FQYKKwYBBAGCNwoDAQYKKwYBBAGCNxQCAQYJKwYBBAGCNxUGBggrBgEFBQcDAjANBgkqhkiG9w0BA
 QUFAAOBgQCuXwAgcYqLNm6gEDTWm/OWmTFjPyA5KSDB76yVqZwr11ch7eZiNSmCtH7Pn+VILagf9o
 tiFl5ttk9KX6tIvbeEC4X/mQVgAB3HuJH5sL1n/k2H10XCXKfMqMGrtsZrA64tMCcCeZRoxfAO94n
 ==PulwF4nkcnu1xO/B7x+LpcjxjhQ
```

تكوين الطالب

1. قم بتثبيت محرر ملف التعريف هذا، AnyConnect-profileeditor-win-3.1.00495-k9.exe.
2. افتح محرر ملف تعريف مدير الوصول إلى الشبكة وقم بتكوين ملف التعريف المحدد.
3. إنشاء شبكة سلكية معينة.



من المهم جدا في هذه المرحلة إعطاء المستخدم خيار إستخدام الشهادة في كل مصادقة. لا تقم بتخزين هذا الخيار مؤقتا. أستخدم أيضا "اسم المستخدم" كمعرف غير محمي. من المهم تذكر أنه ليس نفس المعرف الذي يستخدمه ACS للاستعلام عن AD للشهادة. سيتم تكوين هذا المعرف في ACS.



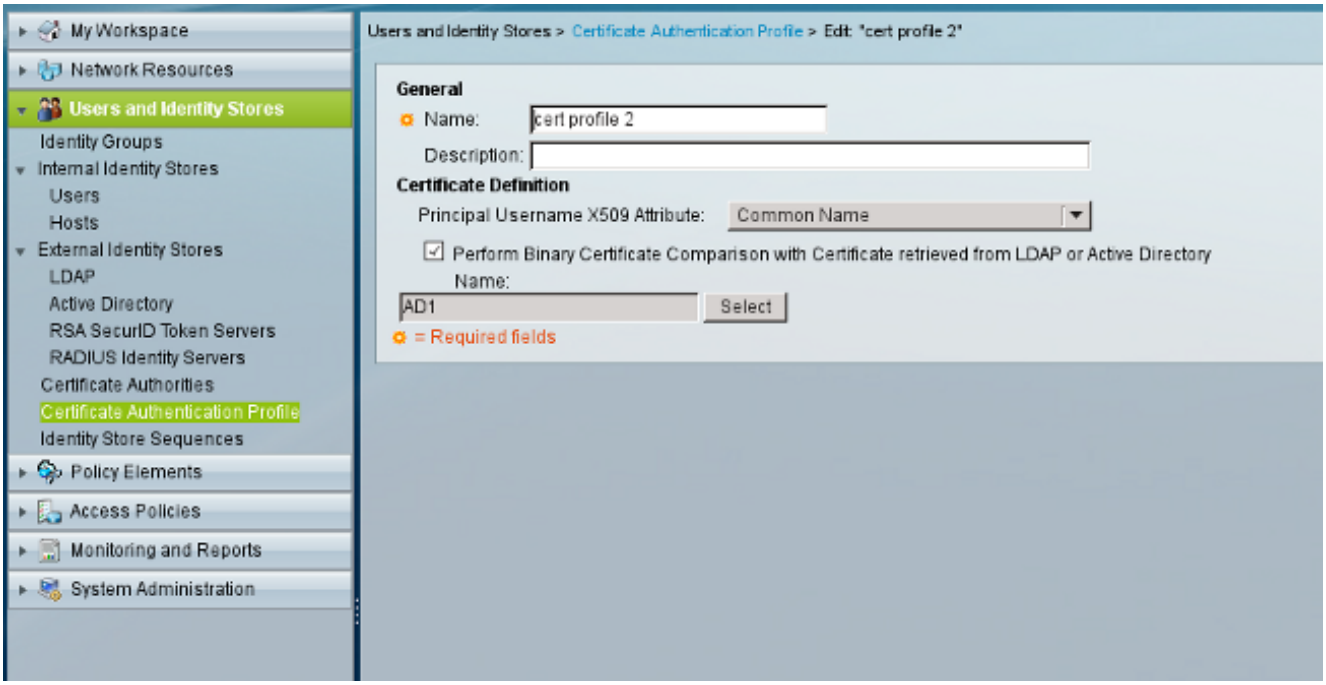
4. احفظ ملف .xml ك c:\Users\All Users\Cisco\Cisco AnyConnect Secure Mobility Client\Network Access Manager\system\configuration.xml.
5. قم بإعادة تشغيل خدمة AnyConnect NAM من Cisco.

يوضح هذا المثال عملية نشر ملفات التعريف اليدوية. يمكن إستخدام AD لنشر هذا الملف لكافة المستخدمين. كما يمكن إستخدام ASA لتوفير ملف التعريف عند دمجه مع شبكات VPN.

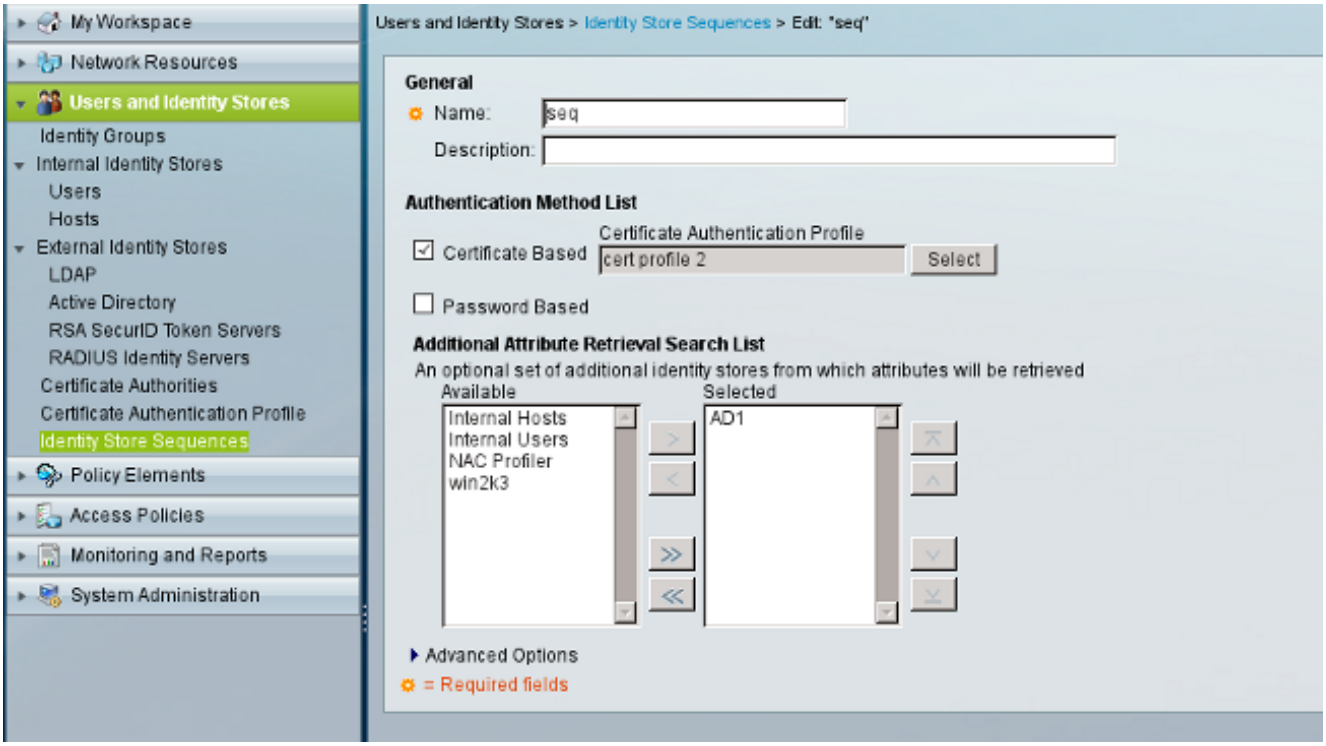
تكوين ACS

1. انضم إلى مجال AD.

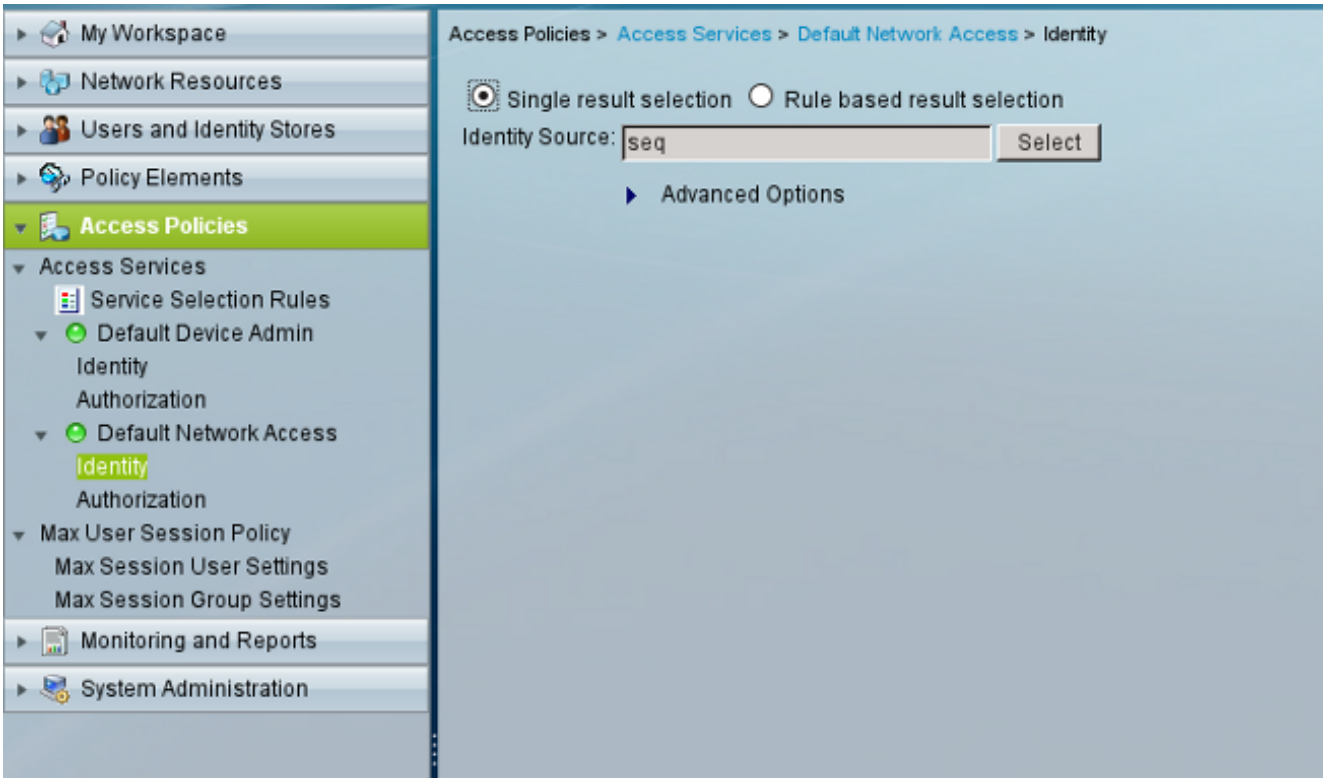
يطابق ACS أسماء مستخدمي AD دون إستخدام حقل CN من الشهادة المستلمة من المتلقي (في هذه الحالة يكون test2 ،test1، أو test3). كما تم تمكين المقارنة الثنائية. وهذا يجبر ACS على الحصول على شهادة المستخدم من AD ومقارنتها مع نفس الشهادة التي يستلمها الملتمس. وإذا لم تتطابق تفشل المصادقة.



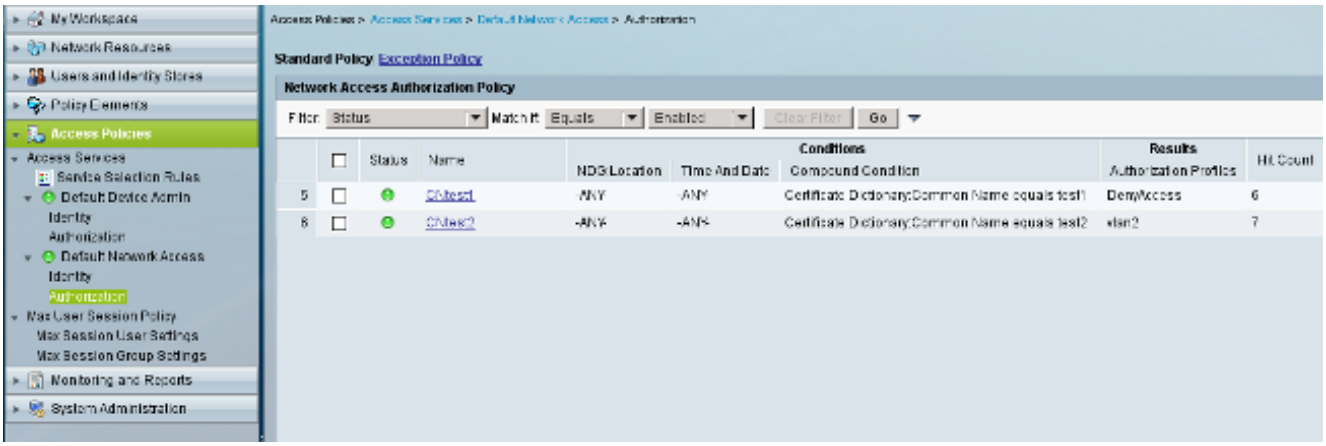
2. تشكيل تسلسلات مخزن الهويات الذي يستخدم AD للمصادقة المستندة إلى شهادة مع توصيف الشهادة.



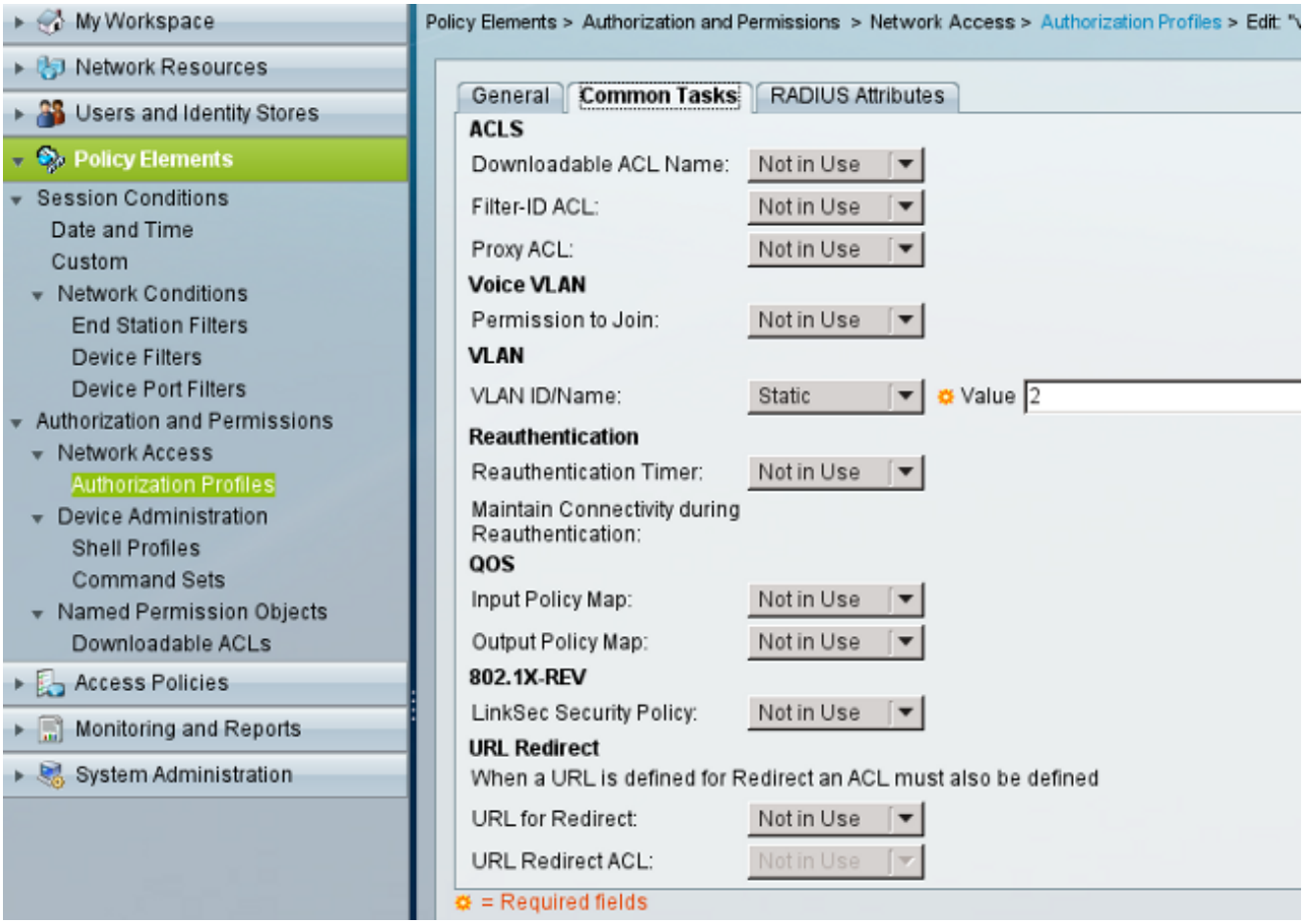
يستخدم هذا كمصدر هوية في نهج هوية RADIUS.



3. تكوين نهجي تفويض. يتم إستخدام النهج الأول للاختبار 1 ويرفض الوصول إلى ذلك المستخدم. يتم إستخدام السياسة الثانية للاختبار 2 وتسمح بالوصول مع ملف تعريف VLAN2.

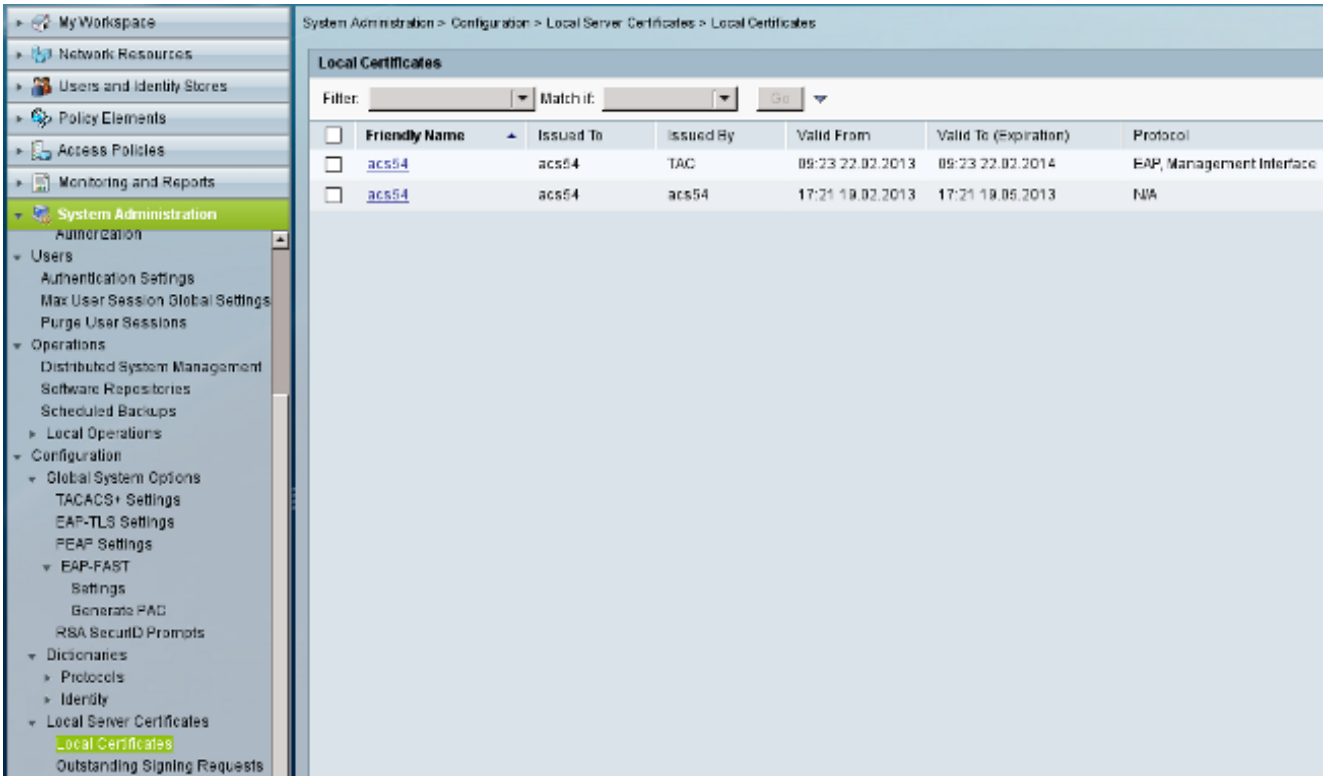


VLAN2 هو ملف تعريف التخويل الذي يرجع سمات RADIUS التي تربط المستخدم بشبكة VLAN2 على المحول.



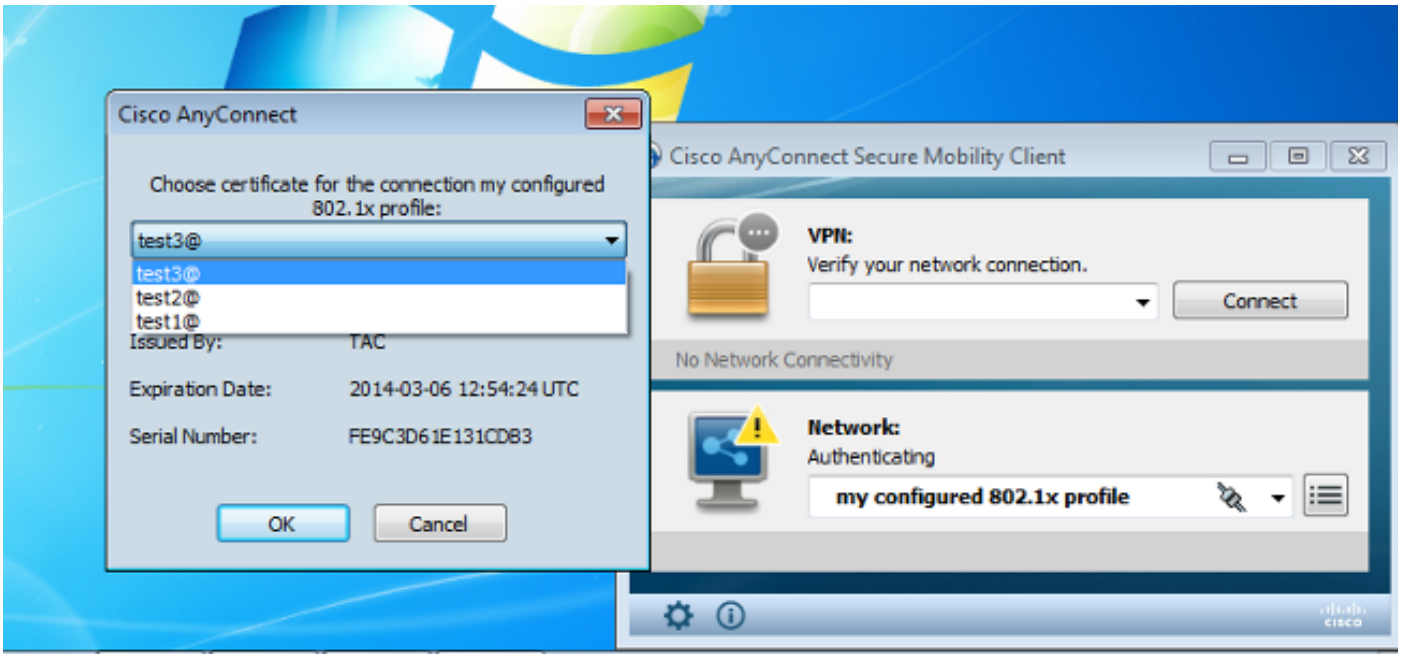
4. قم بتثبيت شهادة المرجع المصدق على
.ACS

5. قم بإنشاء الشهادة وتثبيتها (لاستخدام بروتوكول المصادقة المتوسع) الموقعة من قبل المرجع المصدق (CA) من Cisco ل
.ACS



التحقق من الصحة

من الممارسات الجيدة تعطيل الخدمة الأصلية بمعيار 802.1x على عميل Windows 7 نظرا لاستخدام AnyConnect NAM. مع التوصيف الذي تم تكوينه، يسمح للعميل بتحديد شهادة معينة.



عند إستخدام شهادة Test2، يتلقى المحول إستجابة نجاح مع خصائص RADIUS.

```
DOT1X-5-SUCCESS: Authentication successful for client% :00:02:51
                                    0800.277f.5f64) on Interface Et0/0)
'AUTHMGR-7-RESULT: Authentication result 'success' from 'dot1x% :00:02:51
                                    for client (0800.277f.5f64) on Interface Et0/0
                                                                    #switch
|EPM-6-POLICY_REQ: IP=0.0.0.0| MAC=0800.277f.5f64% :00:02:51
```

```
|AUDITSESID=C0A80A0A00000001000215F0| AUTHTYPE=DOT1X
                                    EVENT=APPLY

switch#show authentication sessions interface e0/0
                Interface:  Ethernet0/0
              MAC Address:  0800.277f.5f64
                 IP Address:  Unknown
                   User-Name:  test2
                  Status:  Authz Success
                            Domain:  DATA
               Oper host mode:  single-host
                     Oper control dir:  both
          Authorized By:  Authentication Server
                        Vlan Policy:  2
                       Session timeout:  N/A
                       Idle timeout:  N/A
        Common Session ID:  C0A80A0A00000001000215F0
                    Acct Session ID:  0x00000005
                        Handle:  0xE8000002

                                :Runnable methods list
                                  Method   State
                               dot1x    Authc Succes
```

لاحظ أنه قد تم تعيين شبكة VLAN رقم 2. من الممكن إضافة سمات RADIUS أخرى إلى ملف تعريف التخويل هذا على ACS (مثل قائمة التحكم بالوصول المتقدم أو مؤقتات إعادة التخويل).

السجلات على ACS هي كما يلي:

12813 Extracted TLS CertificateVerify message.
12804 Extracted TLS Finished message.
12801 Prepared TLS ChangeCipherSpec message.
12802 Prepared TLS Finished message.
12816 TLS handshake succeeded.
12509 EAP-TLS full handshake finished successfully
12505 Prepared EAP-Request with another EAP-TLS challenge
11006 Returned RADIUS Access-Challenge
11001 Received RADIUS Access-Request
11018 RADIUS is re-using an existing session
12504 Extracted EAP-Response containing EAP-TLS challenge-response
Evaluating Identity Policy
15006 Matched Default Rule
24432 Looking up user in Active Directory - test2
24416 User's Groups retrieval from Active Directory succeeded
24469 The user certificate was retrieved from Active Directory successfully.
22054 Binary comparison of certificates succeeded.
22037 Authentication Passed
22023 Proceed to attribute retrieval
22038 Skipping the next IDStore for attribute retrieval because it is the one we authenticated against
22016 Identity sequence completed iterating the IDStores
Evaluating Group Mapping Policy
12506 EAP-TLS authentication succeeded
11503 Prepared EAP-Success
Evaluating Exception Authorization Policy
15042 No rule was matched
Evaluating Authorization Policy
15004 Matched rule
15016 Selected Authorization Profile - vlan2
22065 Max sessions policy passed
22064 New accounting session created in Session cache
11002 Returned RADIUS Access-Accept

استكشاف الأخطاء وإصلاحها

إعدادات الوقت غير صالحة على ACS

خطأ محتمل - خطأ داخلي في ACS Active Directory

12504 Extracted EAP-Response containing EAP-TLS challenge-response
12571 ACS will continue to CRL verification if it is configured for specific CA
12571 ACS will continue to CRL verification if it is configured for specific CA
12811 Extracted TLS Certificate message containing client certificate.
12812 Extracted TLS ClientKeyExchange message.
12813 Extracted TLS CertificateVerify message.
12804 Extracted TLS Finished message.
12801 Prepared TLS ChangeCipherSpec message.
12802 Prepared TLS Finished message.
12816 TLS handshake succeeded.
12509 EAP-TLS full handshake finished successfully
12505 Prepared EAP-Request with another EAP-TLS challenge
11006 Returned RADIUS Access-Challenge
11001 Received RADIUS Access-Request
11018 RADIUS is re-using an existing session
12504 Extracted EAP-Response containing EAP-TLS challenge-response
Evaluating Identity Policy
15006 Matched Default Rule
24432 Looking up user in Active Directory - test1
24416 User's Groups retrieval from Active Directory succeeded
24463 Internal error in the ACS Active Directory
22059 The advanced option that is configured for process failure is used.
22062 The 'Drop' advanced option is configured in case of a failed authentication request.

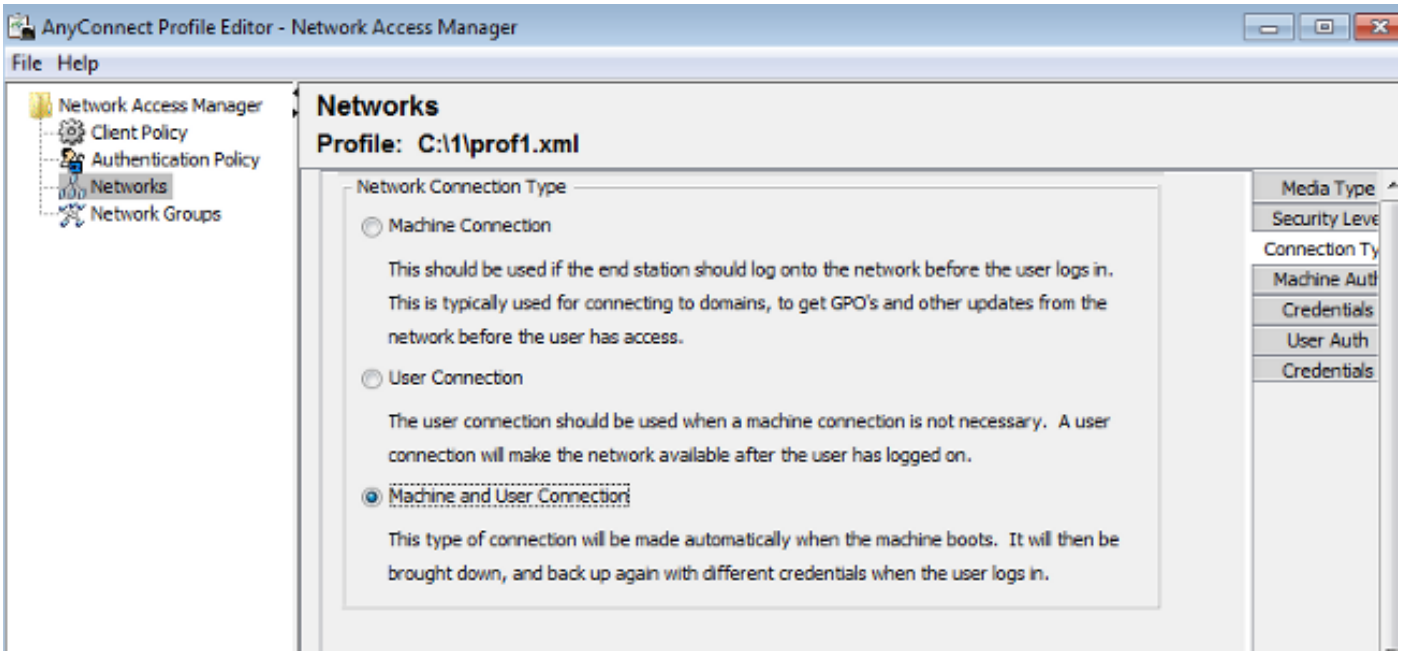
لم يتم تكوين أية شهادة وتثبيتها على AD DC

خطأ محتمل - فشل إسترداد شهادة المستخدم من Active Directory

12571 ACS will continue to CRL verification if it is configured for specific CA
12811 Extracted TLS Certificate message containing client certificate.
12812 Extracted TLS ClientKeyExchange message.
12813 Extracted TLS CertificateVerify message.
12804 Extracted TLS Finished message.
12801 Prepared TLS ChangeCipherSpec message.
12802 Prepared TLS Finished message.
12816 TLS handshake succeeded.
12509 EAP-TLS full handshake finished successfully
12505 Prepared EAP-Request with another EAP-TLS challenge
11006 Returned RADIUS Access-Challenge
11001 Received RADIUS Access-Request
11018 RADIUS is re-using an existing session
12504 Extracted EAP-Response containing EAP-TLS challenge-response
Evaluating Identity Policy
15006 Matched Default Rule
24432 Looking up user in Active Directory - test2
24416 User's Groups retrieval from Active Directory succeeded
24100 Some of the expected attributes are not found on the subject record. The default values, if configured, will be used for these attributes.
24468 Failed to retrieve the user certificate from Active Directory.
22049 Binary comparison of certificates failed
22057 The advanced option that is configured for a failed authentication request is used.
22061 The 'Reject' advanced option is configured in case of a failed authentication request.
12507 EAP-TLS authentication failed
11504 Prepared EAP-Failure
11003 Returned RADIUS Access-Reject

تخصيص ملف تعريف NAM

في شبكات المؤسسة، من المستحسن المصادقة باستخدام شهادات الجهاز والمستخدم على حد سواء.في مثل هذا السيناريو، ينصح باستخدام وضع 802.1x المفتوح على المحول مع شبكة VLAN المقيدة. عند إعادة تمهيد الجهاز ل 802.1x، تبدأ جلسة المصادقة الأولى وتتم مصادقتها باستخدام شهادة جهاز AD. بعد ذلك، وبعد أن يوفر المستخدم بيانات الاعتماد والسجلات إلى المجال، يتم بدء جلسة عمل المصادقة الثانية بشهادة المستخدم. وضع المستخدم في شبكة VLAN الصحيحة (الموثوق بها) مع الوصول الكامل إلى الشبكة. وهو مدمج بشكل رائع في محرك خدمات الهوية (ISE).



وبعد ذلك، من الممكن تكوين مصادقة منفصلة من علامات تبويب مصادقة الجهاز ومصادقة المستخدم.

إذا لم يكن وضع 802.1x المفتوح مقبولا على المحول، فمن الممكن إستخدام وضع 802.1x قبل تكوين ميزة تسجيل الدخول في نهج العميل.

معلومات ذات صلة

- دليل المستخدم لنظام التحكم بالوصول الآمن من Cisco 5.3
- دليل مسؤول Cisco AnyConnect Secure Mobility Client، الإصدار 3.0
- AnyConnect Secure Mobility Client 3.0: مدير الوصول إلى الشبكة ومحرر ملف التعريف على Windows
- الدعم التقني والمستندات - Cisco Systems

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).