802.1x EAP-TLS with Binary Certificate Comparison from AD and NAM Profiles配置示例

目錄

簡介

本檔案介紹具有可擴充驗證通訊協定 — 傳輸層安全(EAP-TLS)和存取控制系統(ACS)的802.1x組態，因為它們會在請求方提供的使用者端憑證與保留在Microsoft Active Directory(AD)中的同一憑證之間執行二進位憑證比較。 AnyConnect網路訪問管理器(NAM)配置檔案用於自定義。本文提供所有元件的配置，以及排除配置故障的場景。

必要條件

需求

本文件沒有特定需求。

採用元件

本文件所述內容不限於特定軟體和硬體版本。

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。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

慣例

請參閱思科技術提示慣例以瞭解更多有關文件慣例的資訊。

設定

拓撲

- 802.1x請求方 — Windows 7，帶Cisco AnyConnect安全移動客戶端版本3.1.01065（NAM模組）
- 802.1x驗證器 — 2960交換機
- 802.1x身份驗證伺服器 — ACS版本5.4
- ACS與Microsoft AD整合 — 域控制器 — Windows 2008 Server

拓撲詳細資訊

- ACS - 192.168.10.152
- 2960 - 192.168.10.10（e0/0 — 請求方已連線）
- 直流 — 192.168.10.101
- Windows 7 - DHCP

流

Windows 7工作站安裝了AnyConnect NAM，它用作請求方使用EAP-TLS方法向ACS伺服器進行身份驗證。具有802.1x的交換機充當身份驗證器。使用者證書由ACS驗證，並且策略授權基於證書中的公用名(CN)應用策略。此外，ACS從AD讀取使用者證書，並與請求方提供的證書執行二進位制比較。

交換器組態

交換器具有基本組態。預設情況下，埠位於隔離VLAN 666中。該VLAN具有受限訪問。使用者獲得授權後，連線埠VLAN會重新設定。

```
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
```

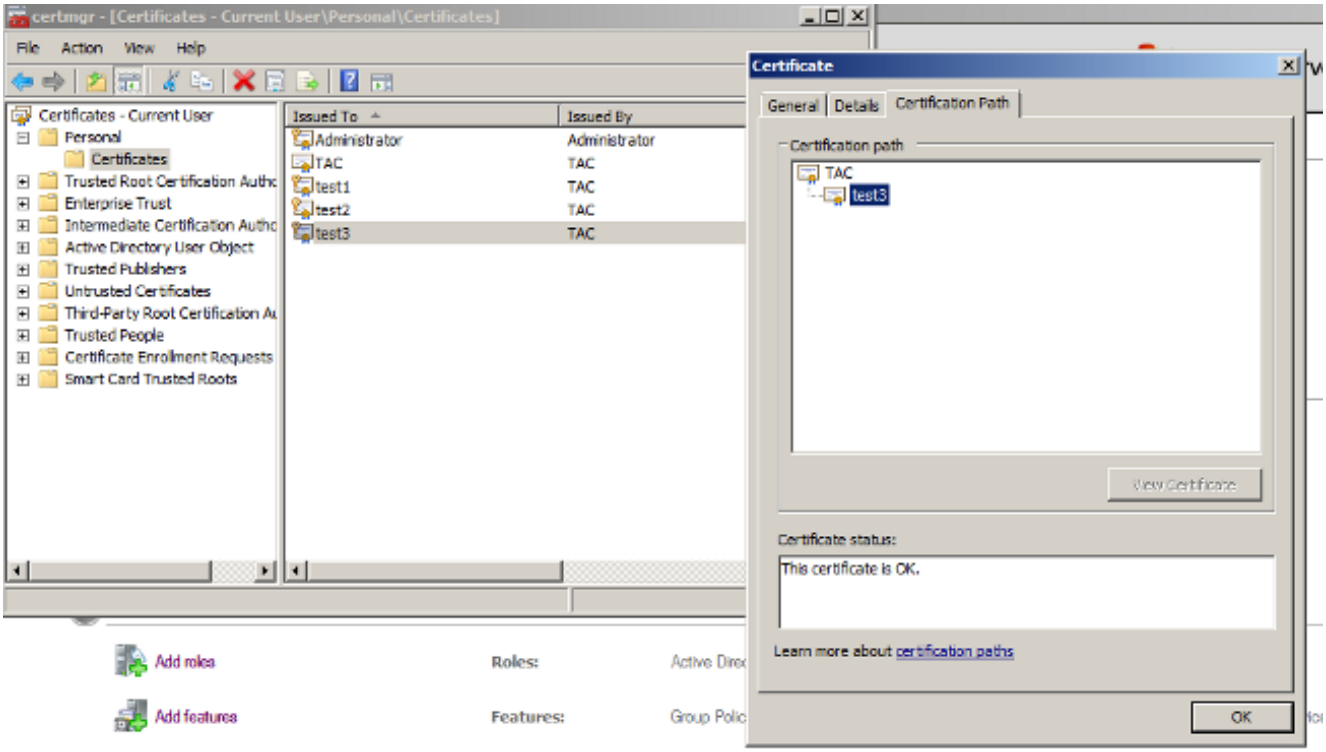
證書準備

對於EAP-TLS，請求方和身份驗證伺服器都需要證書。此範例基於OpenSSL產生的憑證。Microsoft Certificate Authority(CA)可用於簡化企業網路中的部署。

1. 若要產生CA，請輸入以下命令：
   ```
   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
   ```
   CA證書儲存在ca.crt檔案中，而專用（和未受保護）金鑰儲存在ca.key檔案中。
2. 為ACS生成三個使用者證書和一個證書，全部由該CA簽名：
   CN=test1CN=test2CN=test3CN=acs54生成由思科CA簽名的單個證書的指令碼為：
   ```
   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
   ```
   私鑰在server.key檔案中，證書在server.crt檔案中。pkcs12版本位於server.pfx檔案中。
3. 按兩下每個證書（.pfx檔案）以將其匯入域控制器。在域控制器中，應該信任所有三個證書。

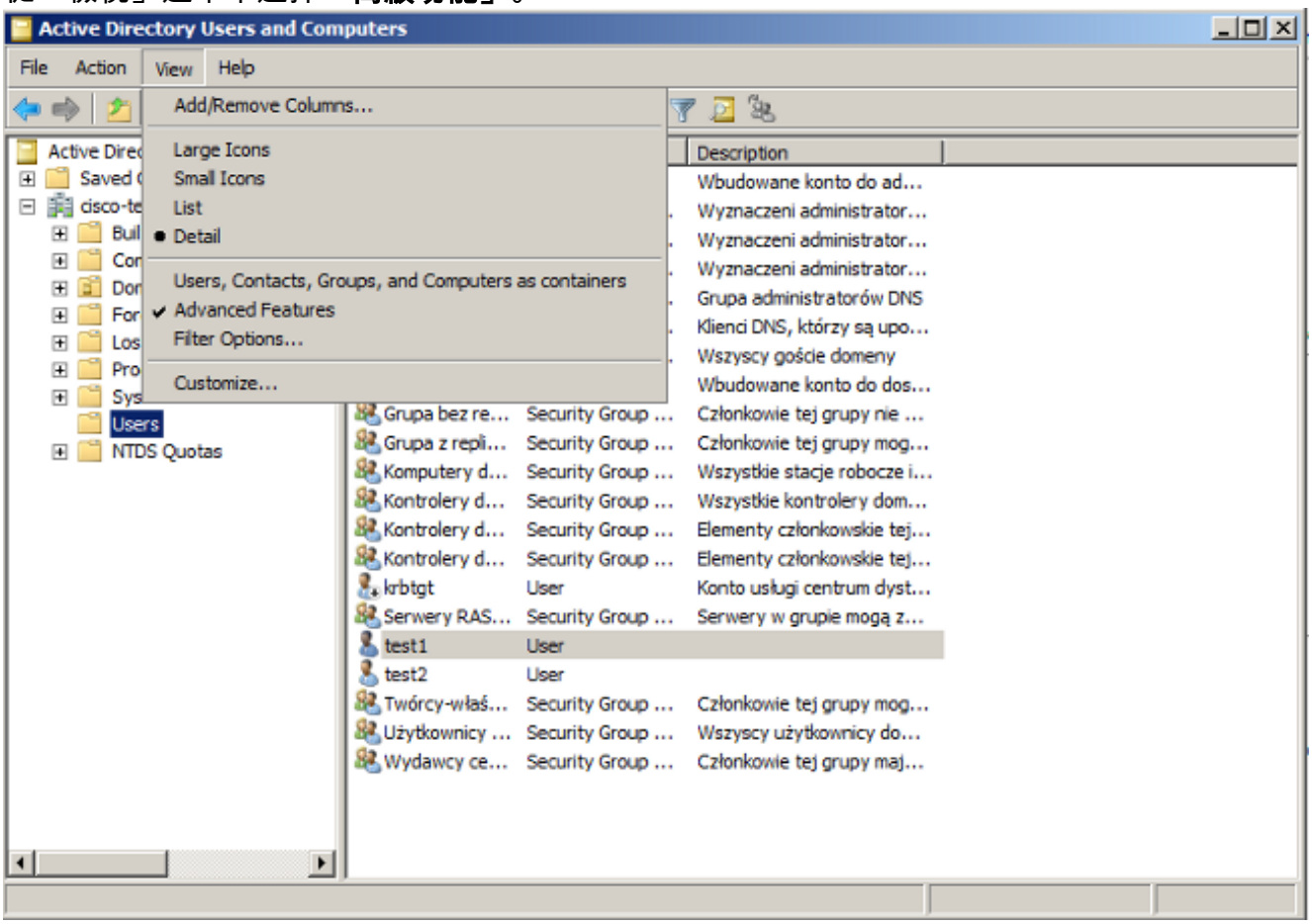


在Windows 7（請求方）或使用Active Directory推送使用者證書時可以遵循相同的流程。

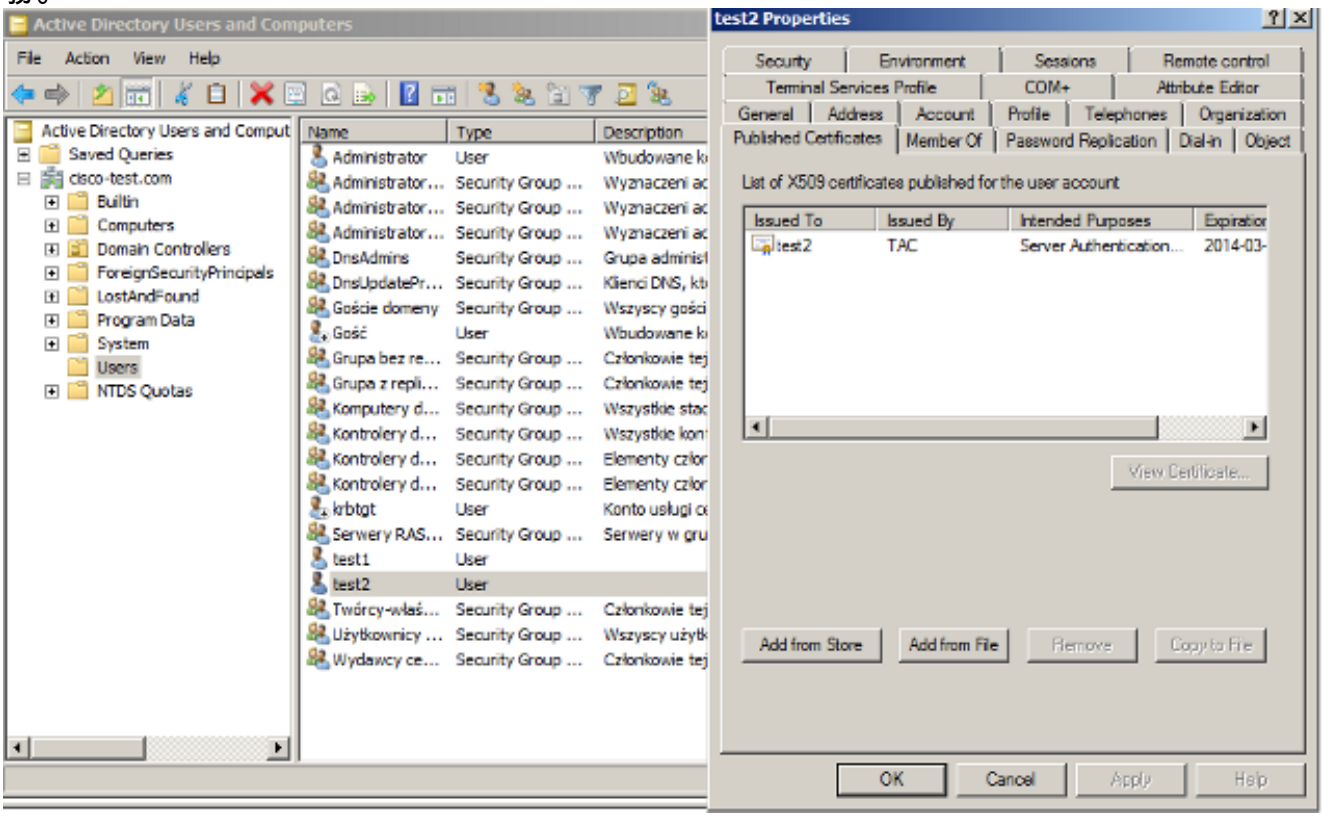
域控制器配置

需要將特定證書對映到AD中的特定使用者。

1. 在Active Directory使用者和電腦中，導航到**Users**資料夾。
2. 從「檢視」選單中選擇**「高級功能」**。



3. 新增以下使用者： 測試1測試2測試3**附註**：密碼不重要。
4. 在「屬性」視窗中，選擇**Published Certificates**頁籤。選擇測試的特定證書。例如，對於test1，使用者CN為test1。**附註**：不使用名稱對映（按一下右鍵使用者名稱）。 用於不同的服務。



在這個階段，證書繫結到AD中的特定使用者。可以使用ldapsearch進行驗證：

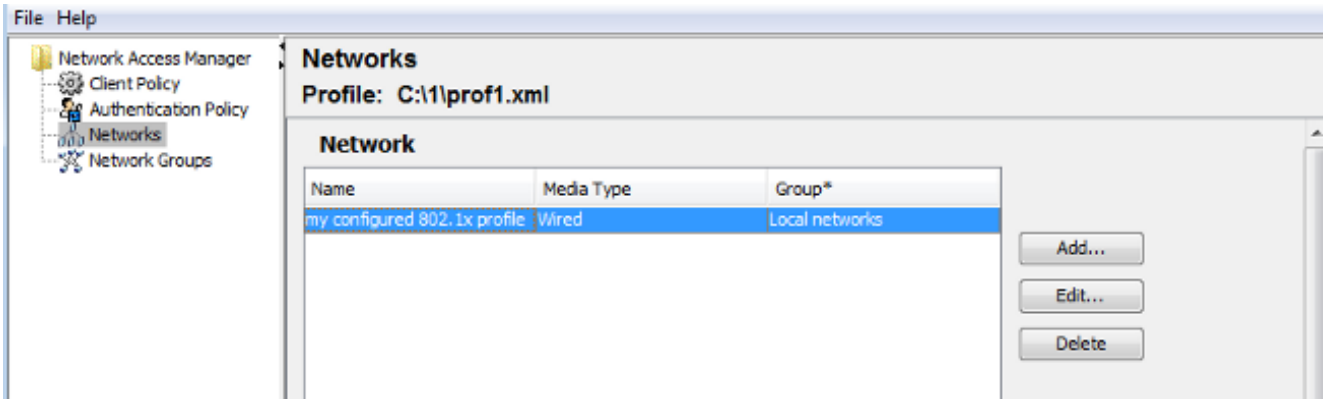
```
ldapsearch -h 192.168.10.101 -D "CN=Administrator,CN=Users,DC=cisco-test,DC=com" -w
Adminpass -b "DC=cisco-test,DC=com"
```

test2的示例結果如下：

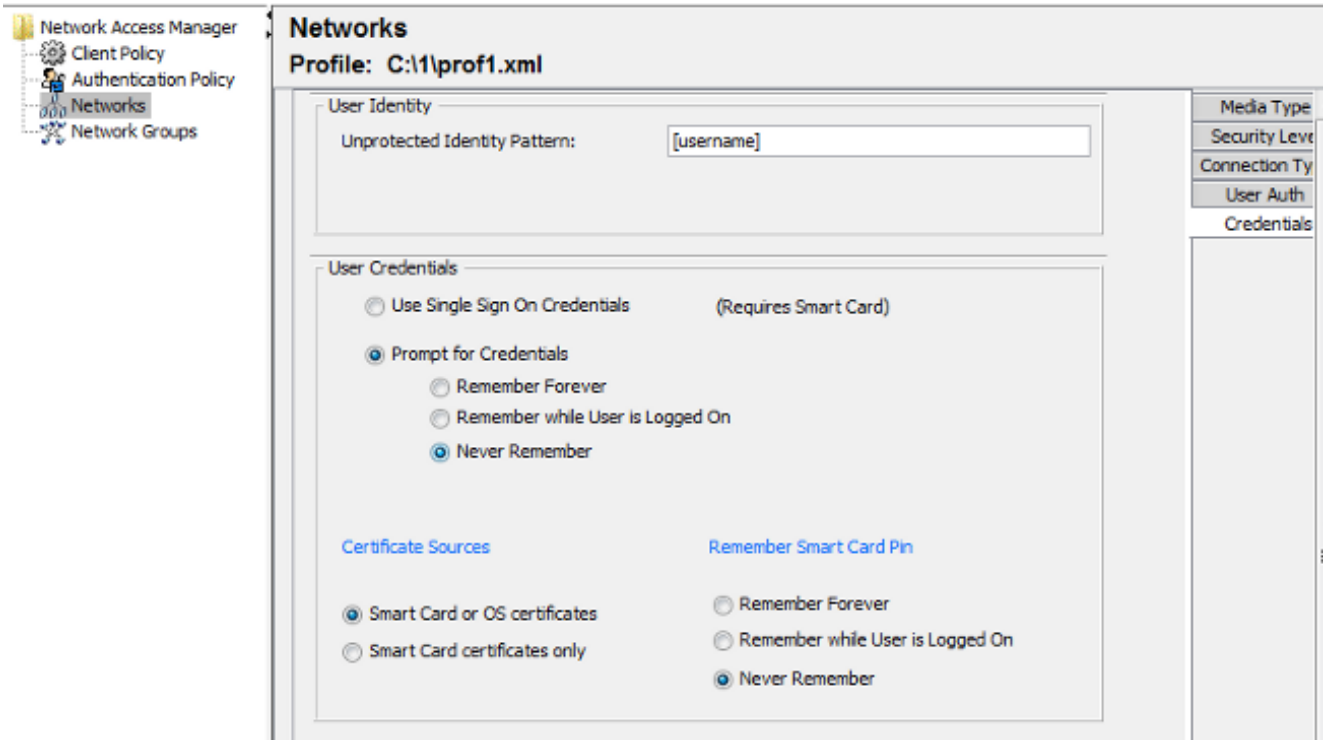
```
# test2, Users, cisco-test.com
dn: CN=test2,CN=Users,DC=cisco-test,DC=com
.................
userCertificate:: MIICuDCCAiGgAwIBAgIJAP6cPWHhMc2yMA0GCSqGSIb3DQEBBQUAMFYxCzAJ
BgNVBAYTAlBMMQwwCgYDVQQIDANNYXoxDzANBgNVBAcMBldhcnNhdzEMMAoGA1UECgwDVEFDMQwwC
gYDVQQLDANSQUMxDDAKBgNVBAMMA1RBQzAeFw0xMzAzMDYxMjUzMjdaFw0xNDAzMDYxMjUzMjdaMF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

請求方配置

1. 安裝此配置檔案編輯器anyconnect-profileeditor-win-3.1.00495-k9.exe。
2. 開啟網路訪問管理器配置檔案編輯器並配置特定配置檔案。
3. 建立特定的有線網路。



在這個階段，很重要的一點是讓使用者在每次身份驗證時選擇使用證書。不要快取該選擇。此外，請使用「username」作為未受保護的ID。請務必記住，它與ACS用於查詢AD以獲取證書的ID不同。該ID將在ACS中配置。



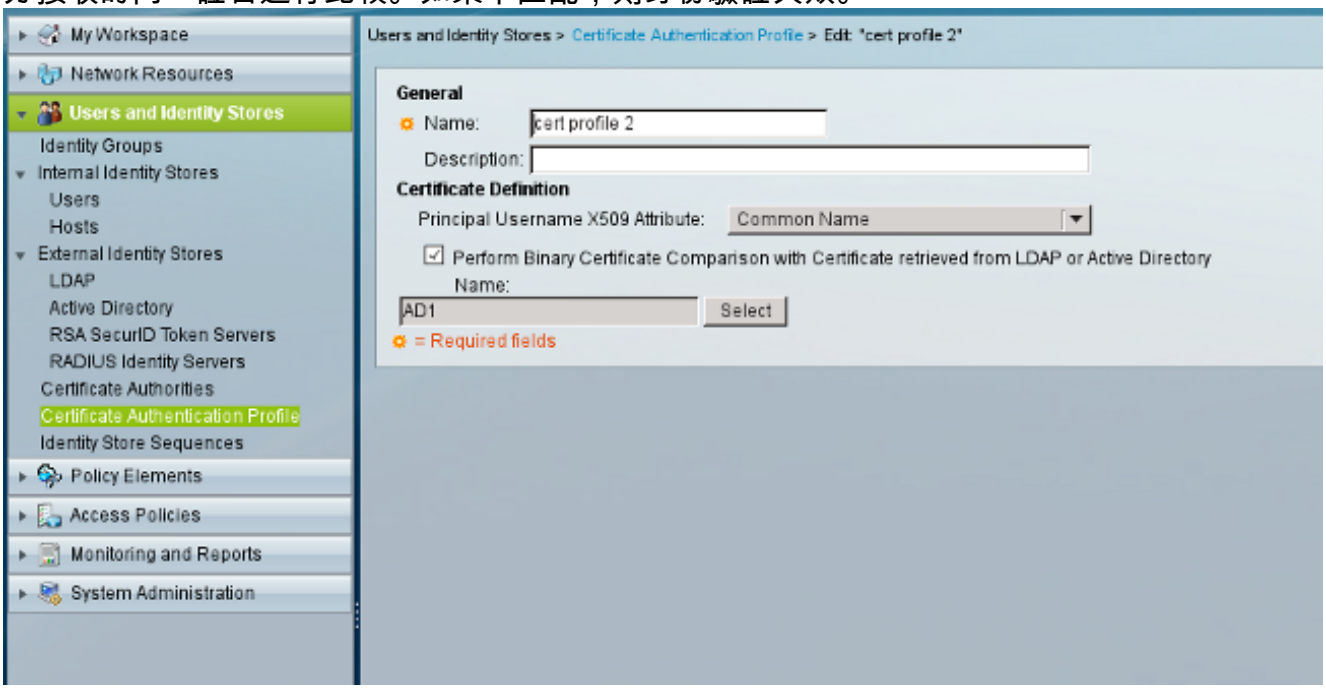
4. 將.xml檔案另存為c:\Users\All Users\Cisco\Cisco AnyConnect Secure Mobility Client\Network Access Manager\system\configuration.xml。
5. 重新啟動Cisco AnyConnect NAM服務。

此示例顯示了手動配置檔案部署。AD可用於為所有使用者部署該檔案。此外，ASA還可用於在與VPN整合時調配配置檔案。

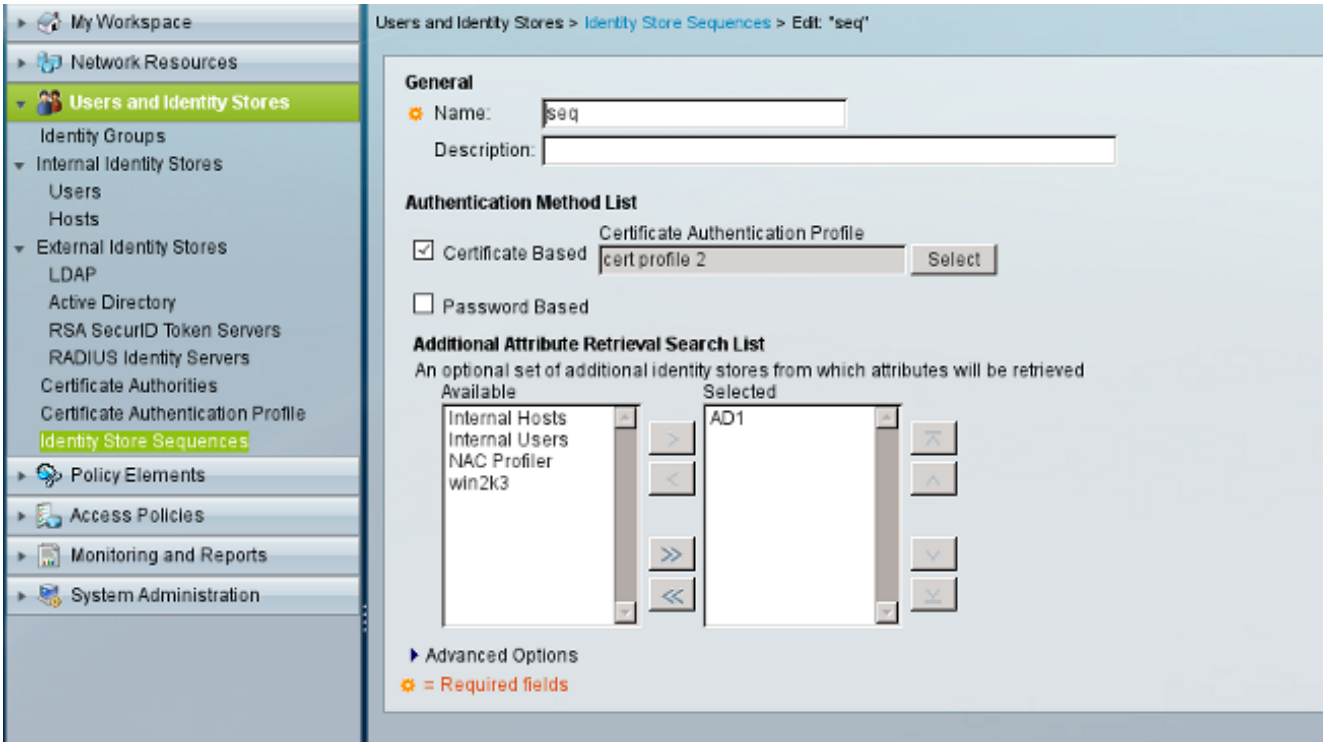
ACS配置

1. 加入AD域。

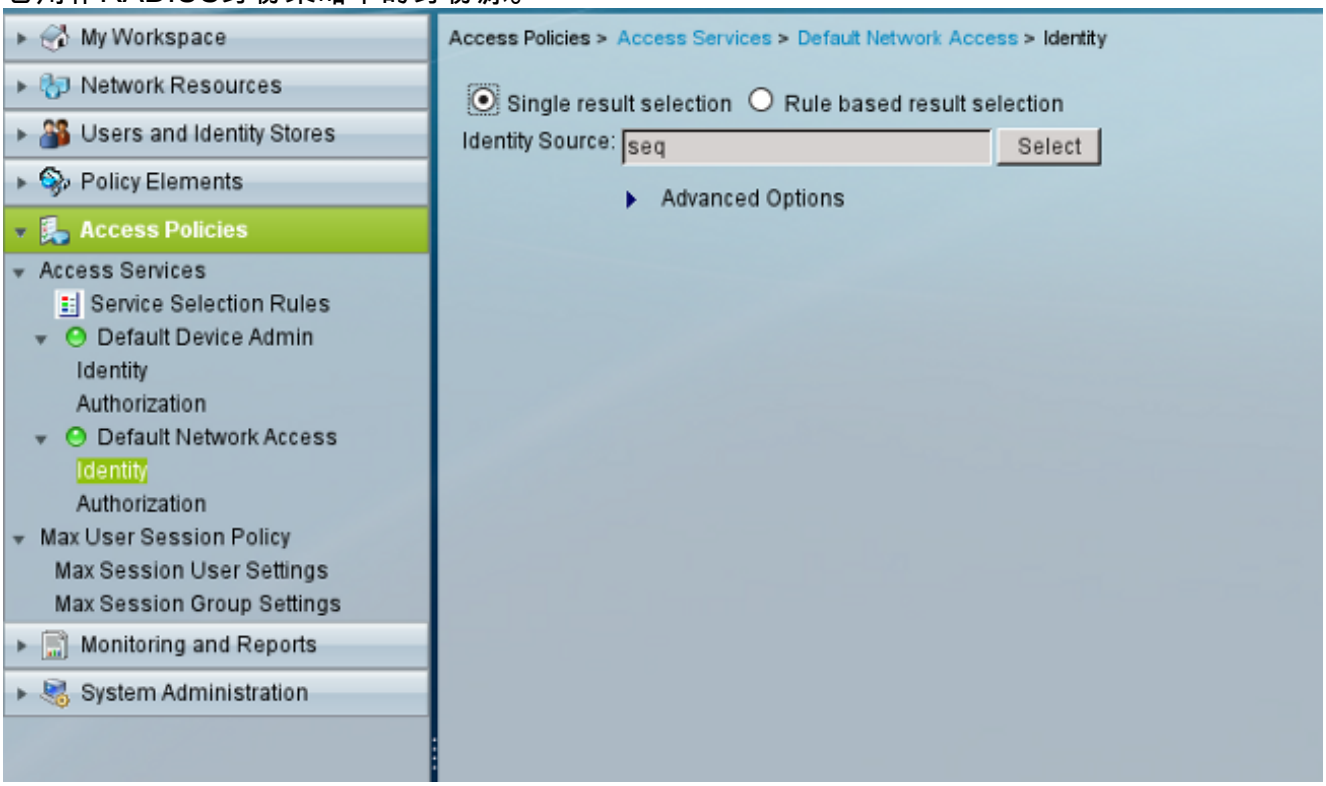
ACS匹配AD使用者名稱，而不使用從請求方接收的證書中的CN欄位（在本例中為test1、test2或test3）。 還啟用了二進位制比較。這會強制ACS從AD獲取使用者證書，並將其與請求方接收的同一證書進行比較。如果不匹配，則身份驗證失敗。



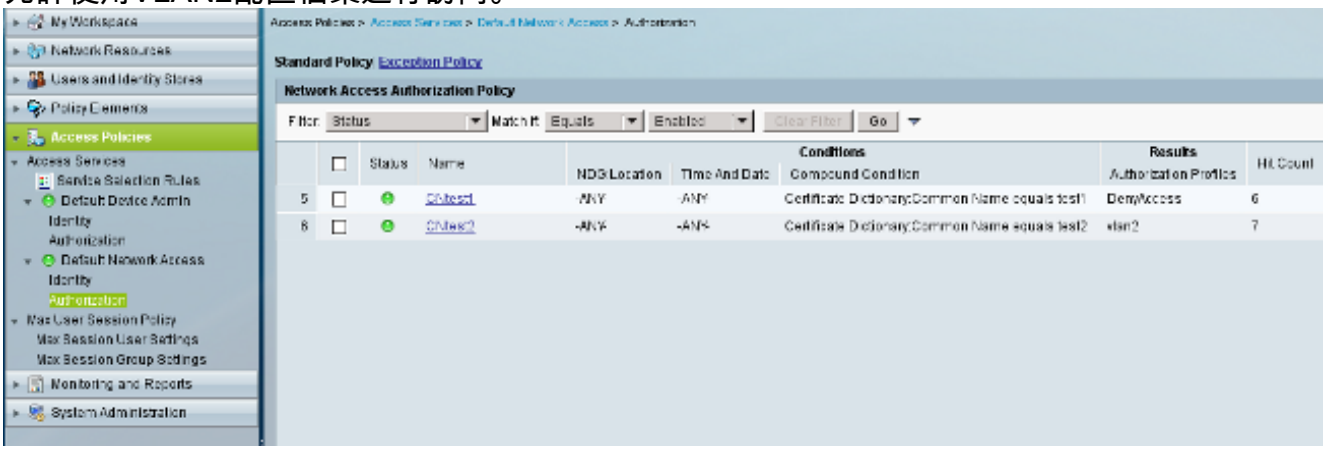
2. 配置身份庫序列，該序列將AD與證書配置檔案一起用於基於證書的身份驗證。



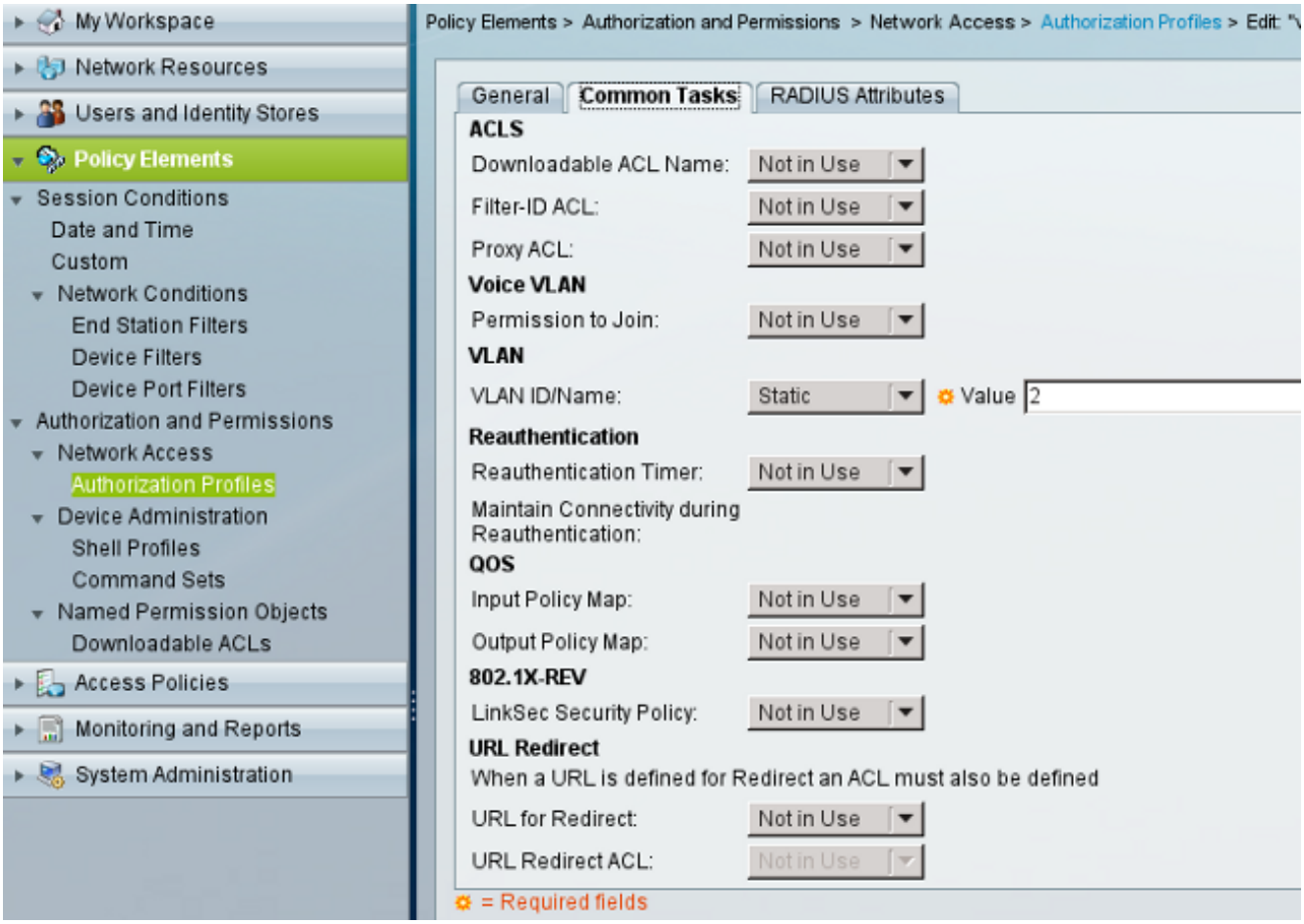
它用作RADIUS身份策略中的身份源。



3. 配置兩個授權策略。第一個策略用於test1，它拒絕訪問該使用者。第二個策略用於測試2，它允許使用VLAN2配置檔案進行訪問。

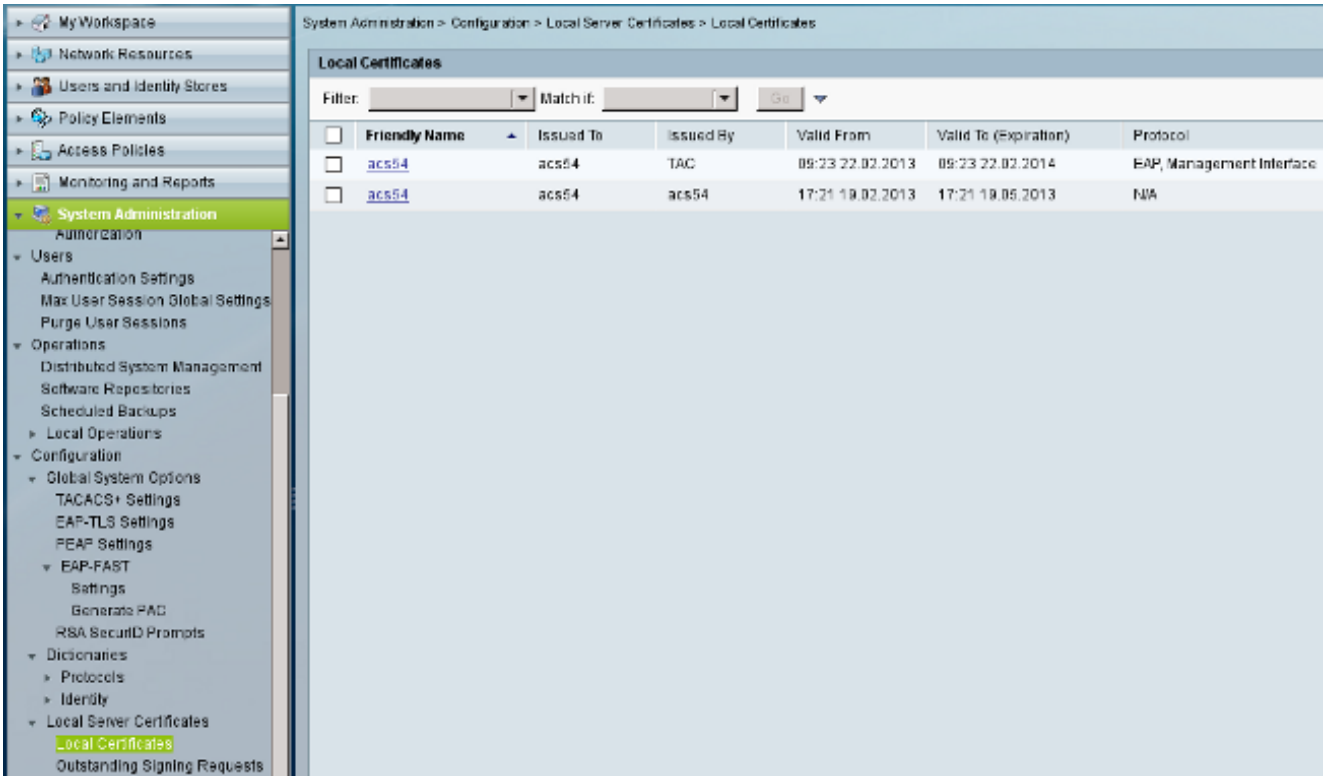


VLAN2是授權配置檔案，它返回將使用者繫結到交換機上VLAN2的RADIUS屬性。



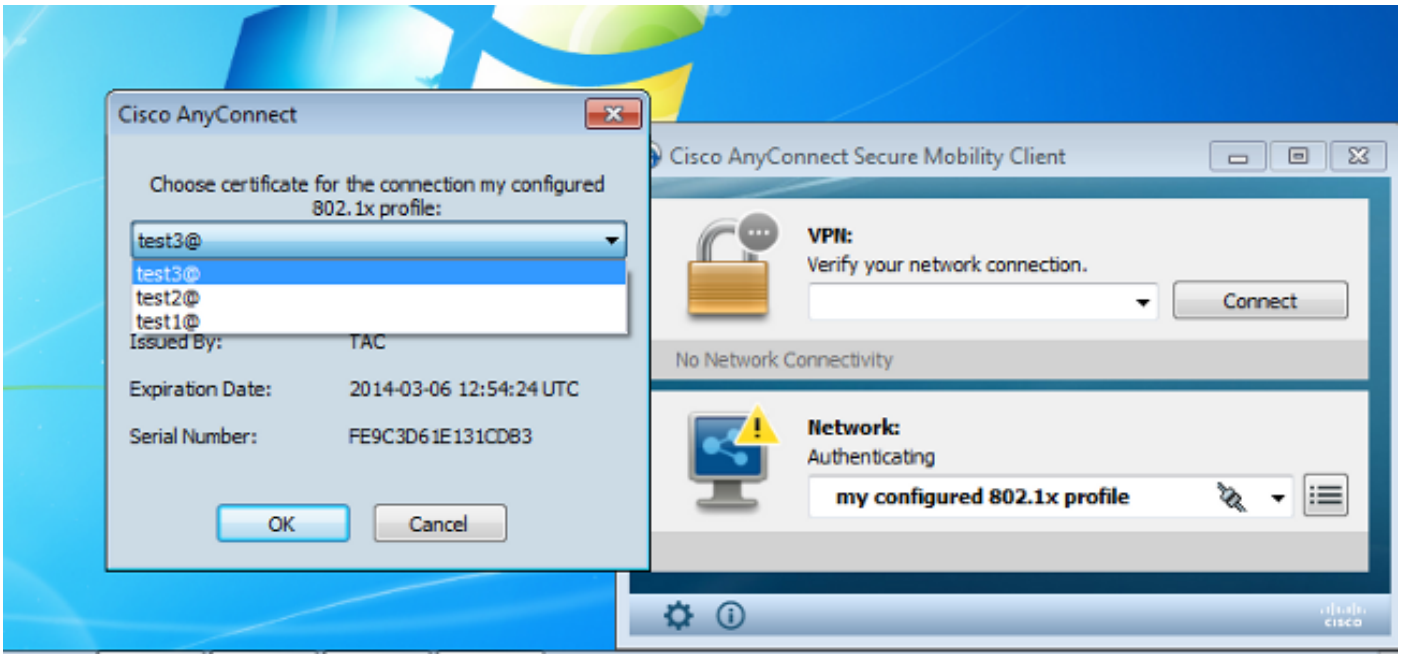
4. 在ACS上安裝CA證書。

5. 生成並安裝由思科CA為ACS簽名的證書（用於可擴展身份驗證協定使用）。



驗證

使用AnyConnect NAM後，最好在Windows 7請求方上禁用本機802.1x服務。使用配置的配置檔案，允許客戶端選擇特定證書。



使用test2憑證時，交換器會收到成功回應以及RADIUS屬性。

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

```
       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
```

請注意，VLAN 2已分配。 可以將其他RADIUS屬性新增到ACS上的授權配置檔案（例如高級訪問控制清單或重新授權計時器）。

ACS上的日誌如下：

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

疑難排解

ACS上的時間設定無效

可能的錯誤 — ACS Active Directory中的內部錯誤

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.

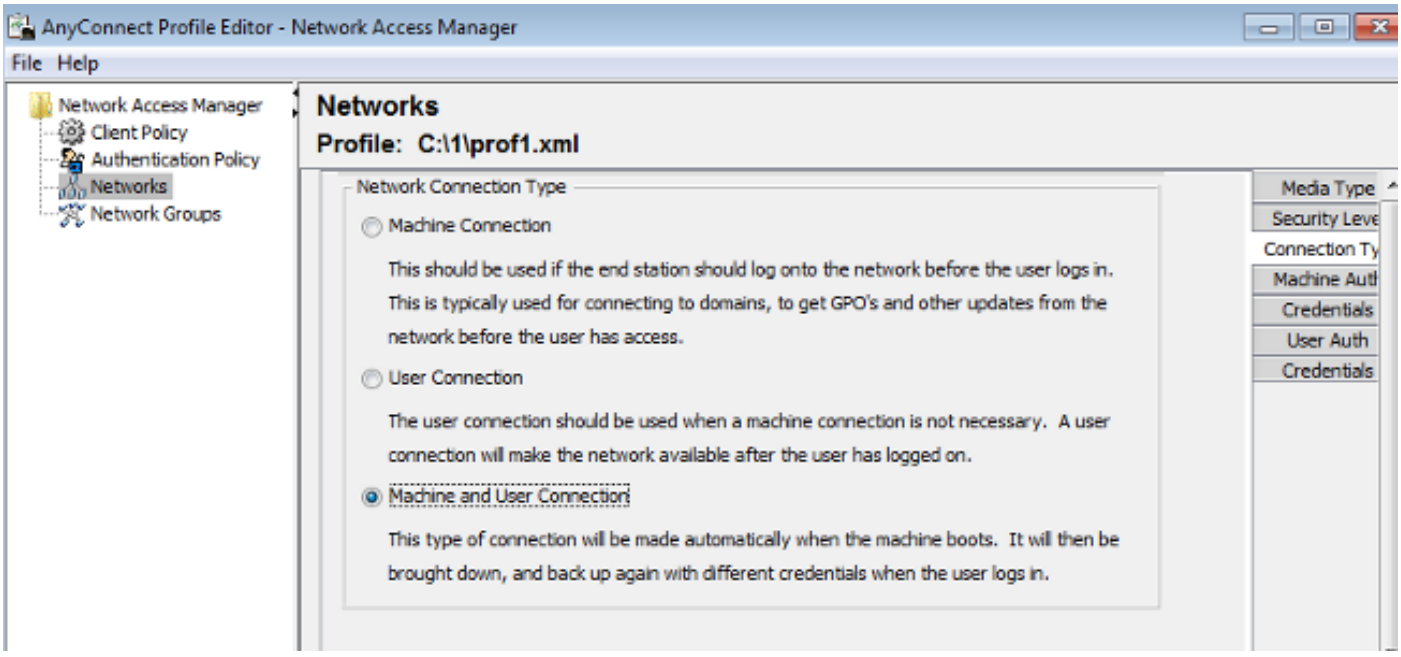
AD DC上沒有配置和繫結的證書

可能的錯誤 — 無法從Active Directory檢索使用者證書

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

NAM配置檔案自定義

在企業網路中，建議使用電腦和使用者證書進行身份驗證。在這種情況下，建議在具有受限VLAN的交換機上使用開放式802.1x模式。在802.1x的機器重新啟動後，將啟動第一個身份驗證會話，並使用AD機器證書進行身份驗證。然後，在使用者提供憑據並登入到域後，將使用使用者證書啟動第二個身份驗證會話。將使用者置於具有完全網路訪問的正確（受信任）VLAN中。它在身份服務引擎(ISE)上整合良好。



然後，可以從Machine Authentication和User Authentication頁籤配置單獨的身份驗證。

如果交換機上不接受開啟802.1x模式，則可以在客戶端策略中配置登入功能之前使用802.1x模式。

相關資訊

- 思科安全訪問控制系統5.3使用手冊
- Cisco AnyConnect安全移動客戶端管理員指南3.0版
- AnyConnect安全行動化使用者端3.0:Windows上的網路訪問管理器和配置檔案編輯器
- 技術支援與文件 - Cisco Systems