802.1x EAP-TLS与AD和NAM配置文件的二进制证书比较配置示例

目录

简介

本文档介绍具有可扩展身份验证协议传输层安全(EAP-TLS)和访问控制系统(ACS)的802.1x配置，因为它们在客户端提供的客户端证书与Microsoft Active Directory(AD)中保留的相同证书之间执行二进制证书比较。 AnyConnect网络访问管理器(NAM)配置文件用于自定义。本文档中介绍了所有组件的配置，以及排除配置故障的场景。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档不限于特定的软件和硬件版本。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

规则

有关文档约定的更多信息，请参考 Cisco 技术提示约定。

配置

拓扑

- 802.1x请求方 — Windows 7，带Cisco AnyConnect安全移动客户端版本3.1.01065（NAM模块）
- 802.1x身份验证器 — 2960交换机
- 802.1x身份验证服务器 — ACS版本5.4
- 与Microsoft AD集成的ACS — 域控制器 — Windows 2008 Server

拓扑详细信息

- ACS - 192.168.10.152
- 2960 - 192.168.10.10（e0/0 — 已连接请求方）
- DC - 192.168.10.101
- Windows 7 - DHCP

流

Windows 7工作站安装了AnyConnect NAM，该NAM用作请求方，用EAP-TLS方法向ACS服务器进行身份验证。具有802.1x的交换机充当身份验证器。用户证书由ACS验证，策略授权根据证书中的公用名(CN)应用策略。此外，ACS从AD获取用户证书并执行与请求方提供的证书的二进制比较。

交换机配置

交换机具有基本配置。默认情况下，端口处于隔离区VLAN 666中。该VLAN的访问受限。用户获得授权后，端口VLAN将重新配置。

```
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
```

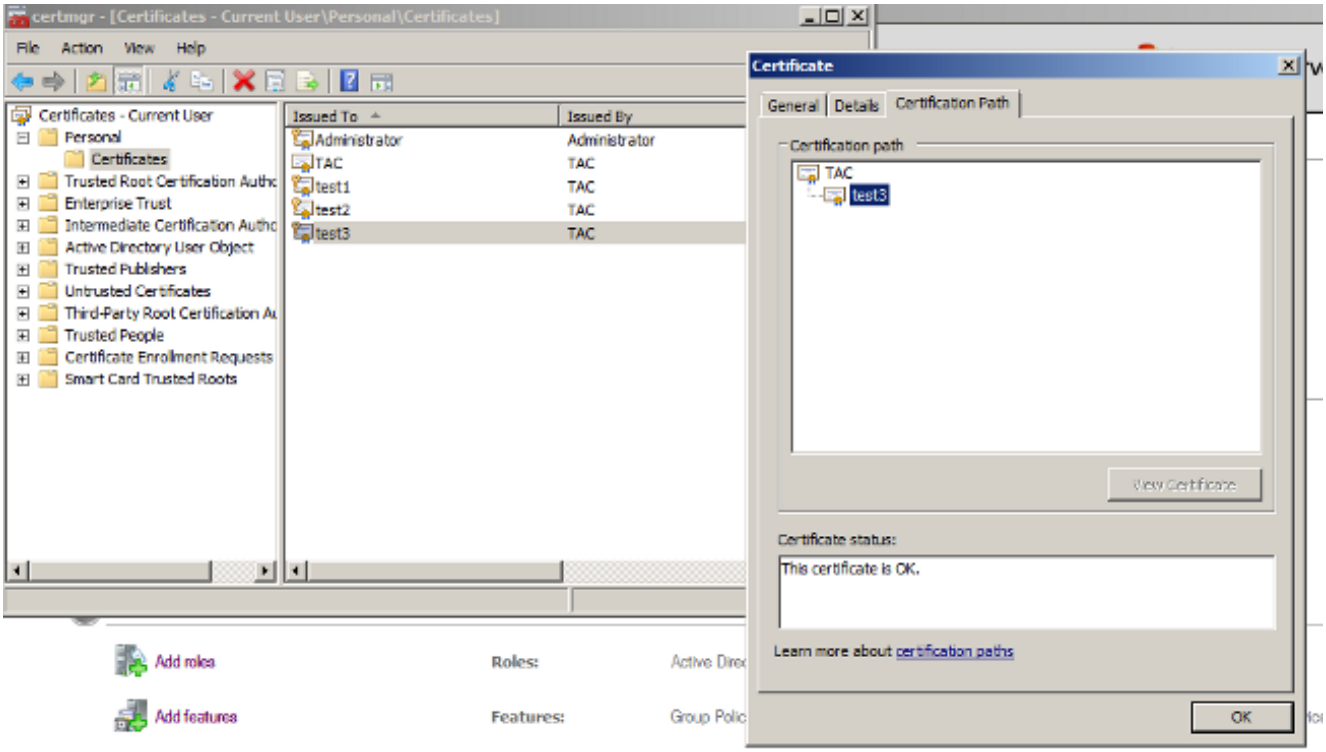
证书准备

对于EAP-TLS，请求方和身份验证服务器都需要证书。此示例基于OpenSSL生成的证书。Microsoft证书颁发机构(CA)可用于简化企业网络中的部署。

1. 要生成CA，请输入以下命令：
   ```
   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证书保留在ca.crt文件中，私有（和未受保护）密钥保留在ca.key文件中。
2. 为ACS生成三个用户证书和一个证书，所有证书都由该CA签名：CN=test1CN=test2CN=test3CN=acs54生成由思科CA签名的单个证书的脚本是：
   ```
   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
   ```
   私钥在server.key文件中，证书在server.crt文件中。pkcs12版本在server.pfx文件中。
3. 双击每个证书（.pfx文件）将其导入域控制器。在域控制器中，所有三个证书都应受信任。

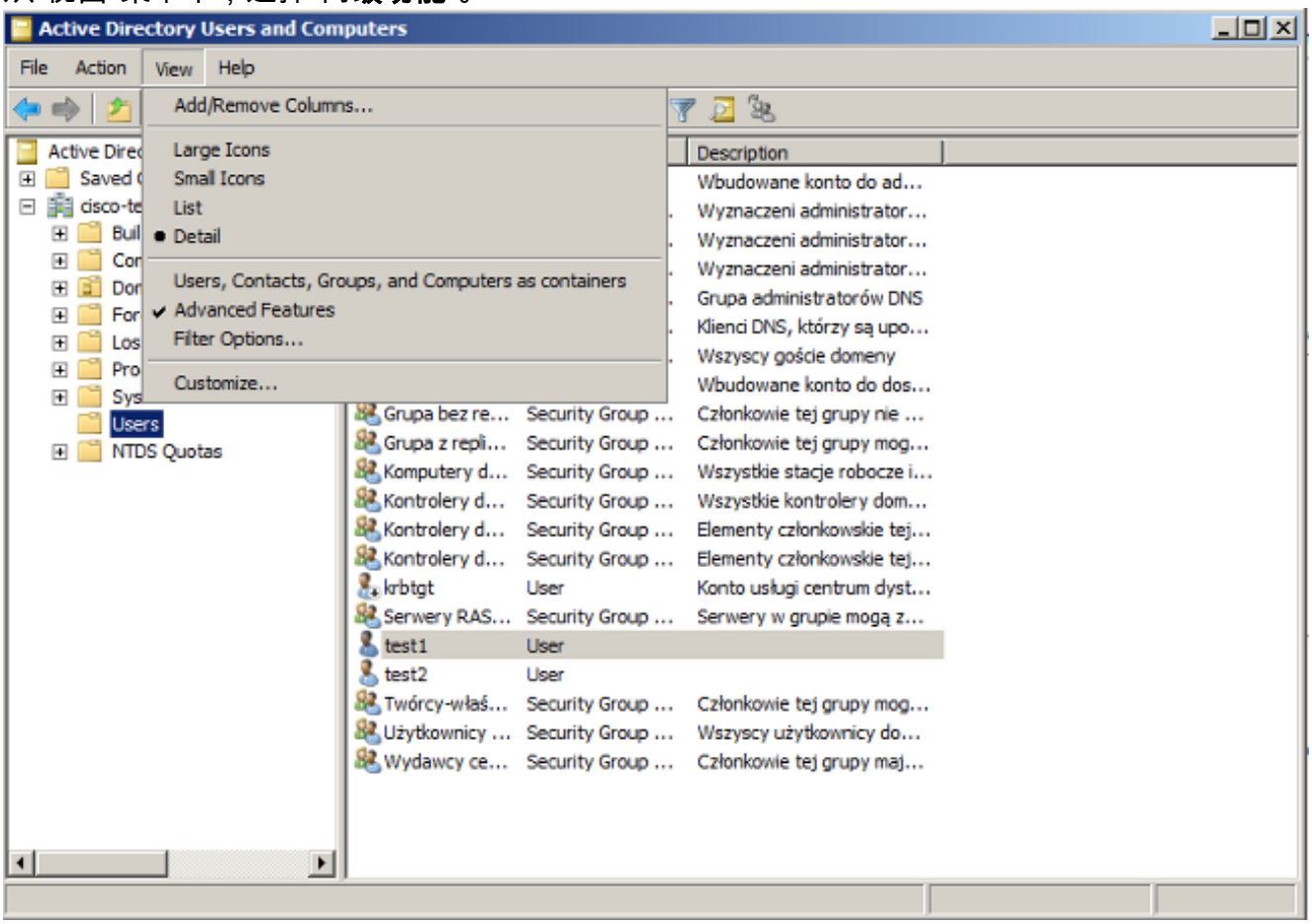


在Windows 7中（请求方）或使用Active Directory推送用户证书时，可以遵循相同的流程。

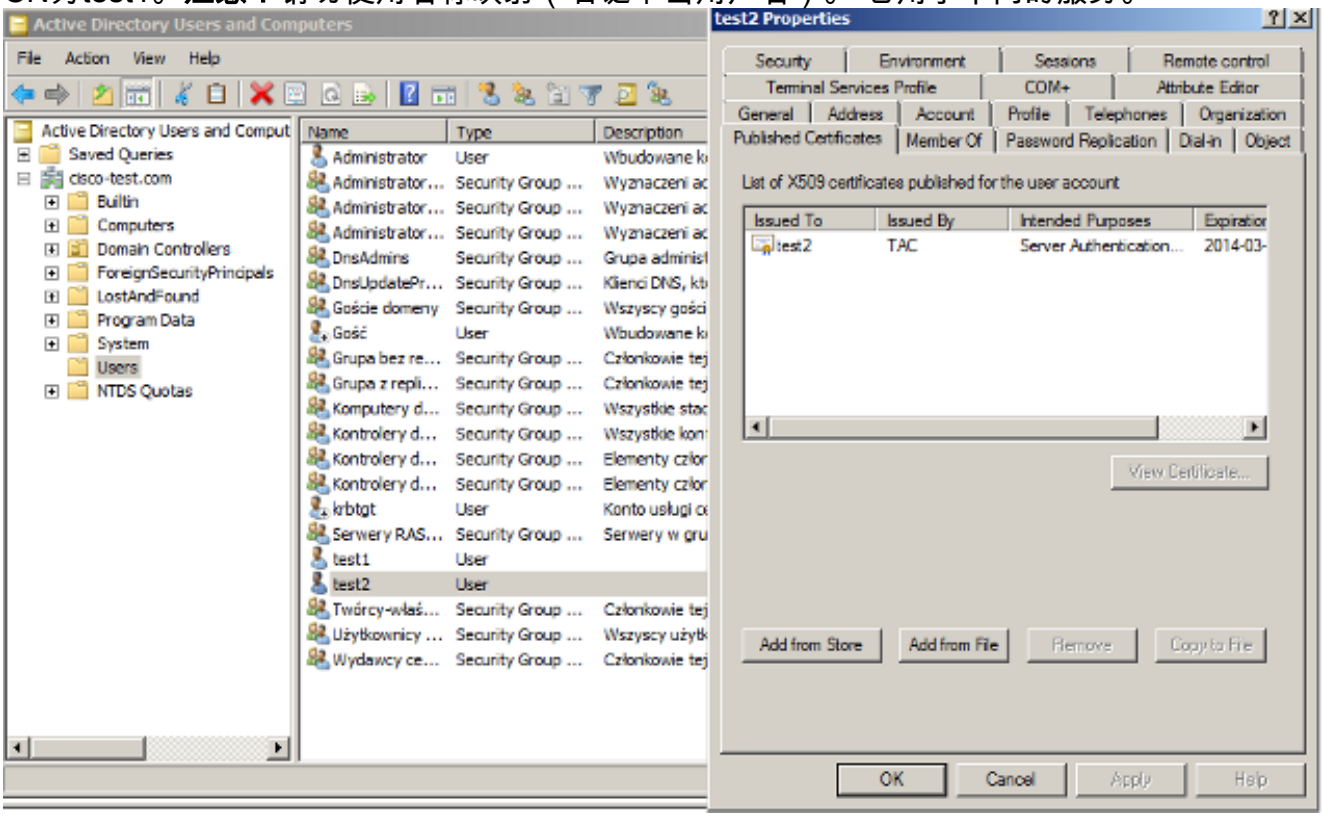
域控制器配置

必须将特定证书映射到AD中的特定用户。

1. 从Active Directory用户和计算机，导航至“用户”文件夹。
2. 从“视图”菜单中，选择“高级功能”。



3. 添加以下用户： test1test2test3**注意：**密码不重要。
4. 从“属性”窗口中，选择“已发**布证书”**选项卡。选择测试的特定证书。例如，对于test1，用户CN为test1。**注意：**请勿使用名称映射（右键单击用户名）。 它用于不同的服务。



在此阶段，证书绑定到AD中的特定用户。这可以通过使用ldapsearch进行验证：

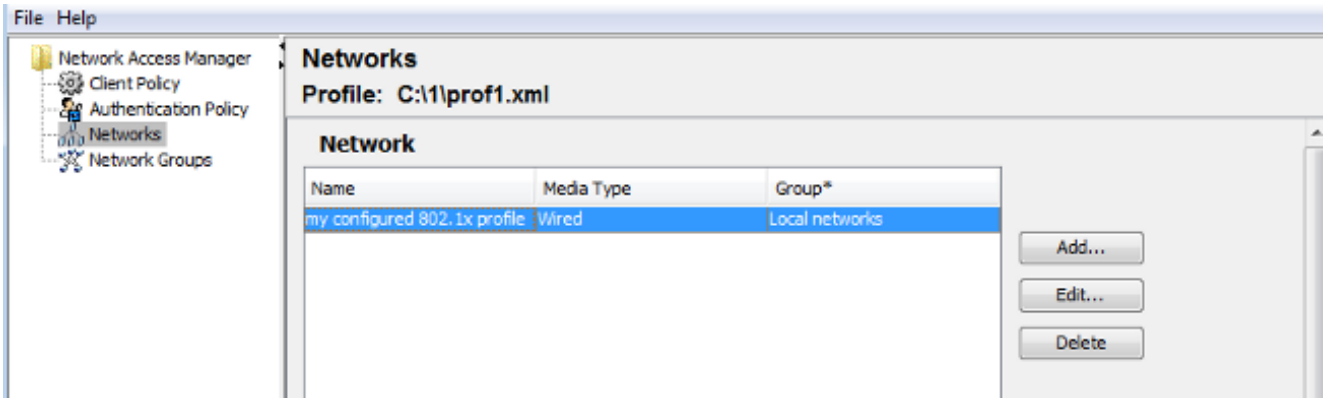
```
ldapsearch -h 192.168.10.101 -D "CN=Administrator,CN=Users,DC=cisco-test,DC=com" -w
Adminpass -b "DC=cisco-test,DC=com"
```

测试2的示例结果如下：

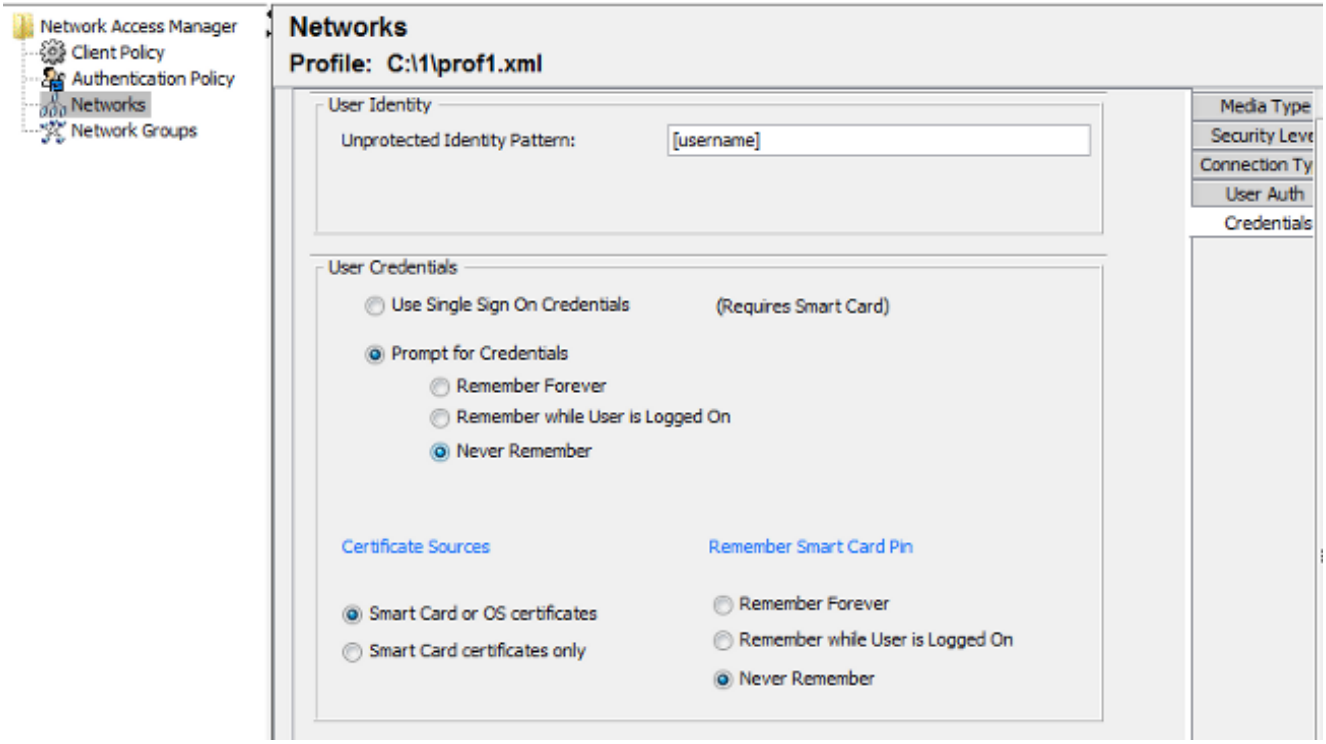
```
# test2, Users, cisco-test.com
dn: CN=test2,CN=Users,DC=cisco-test,DC=com
.................
userCertificate:: MIICuDCCAiGgAwIBAgIJAP6cPWHhMc2yMA0GCSqGSIb3DQEBBQUAMFYxCzAJ
BgNVBAYTAlBMMQwwCgYDVQQIDANNYXoxDzANBgNVBAcMBldhcnNhdzEMMAoGA1UECgwDVEFDMQwwC
gYDVQQLDANSQUMxDDAKBgNVBAMMA1RBQzAeFw0xMzAzMDYxMjUzMjdaFw0xNDAzMDYxMjUzMjdaMF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

请求方配置

1. 安装此配置文件编辑器anyconnect-profileeeditor-win-3.1.00495-k9.exe。
2. 打开网络访问管理器配置文件编辑器并配置特定配置文件。
3. 创建特定有线网络。



在此阶段，让用户选择在每次身份验证时使用证书非常重要。不要缓存该选项。另外，使用“username”作为未受保护的ID。请务必记住，它与ACS用于查询AD的证书的ID不同。该ID将在ACS中配置。



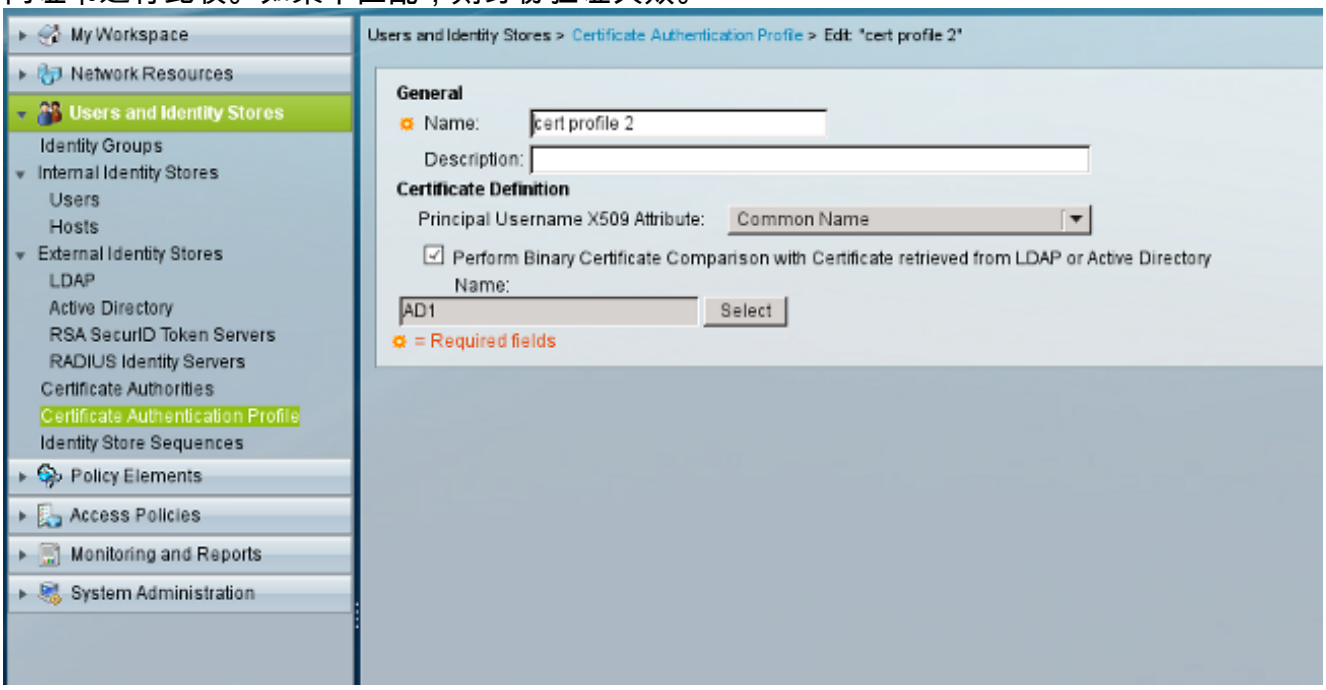
4. 将.xml文件另存为c:\Users\All Users\Cisco\Cisco AnyConnect Secure Mobility Client\Network Access Manager\system\configuration.xml。
5. 重新启动Cisco AnyConnect NAM服务。

此示例显示手动配置文件部署。AD可用于为所有用户部署该文件。此外，ASA可用于在与VPN集成时调配配置文件。

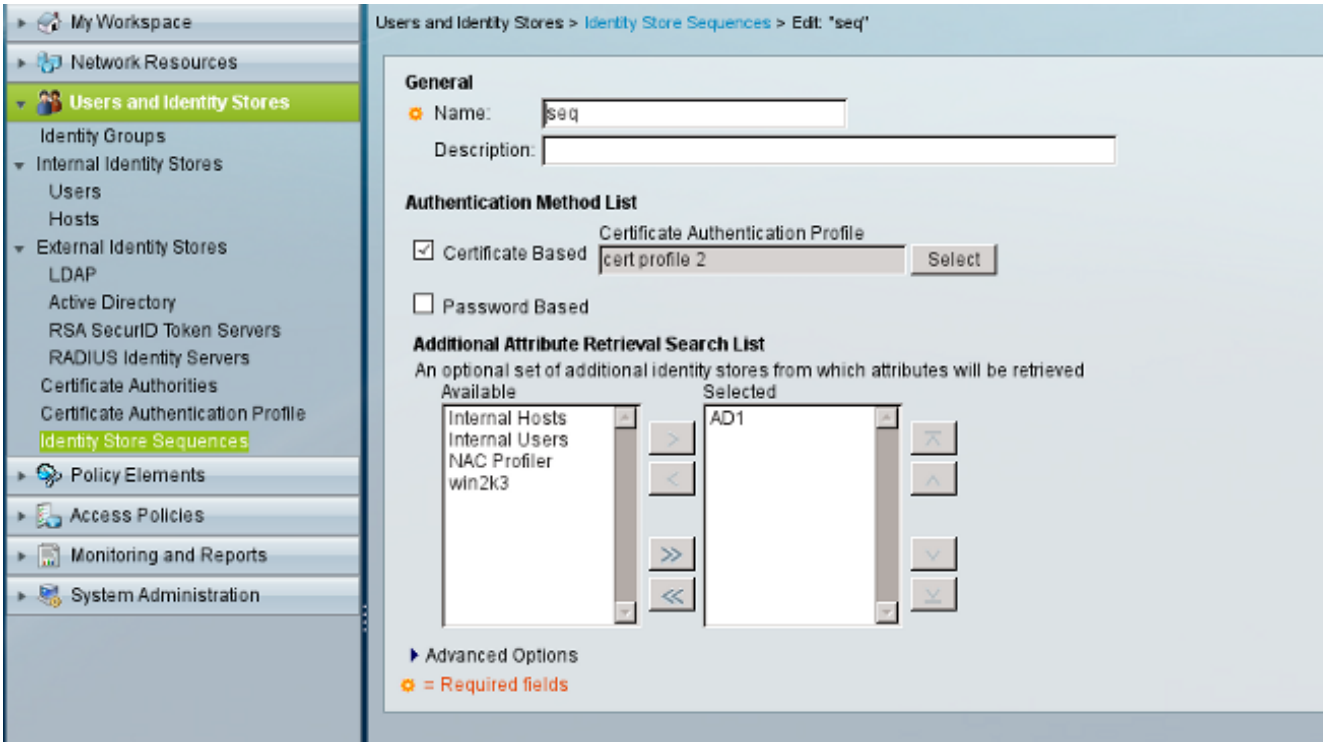
ACS配置

1. 加入AD域。

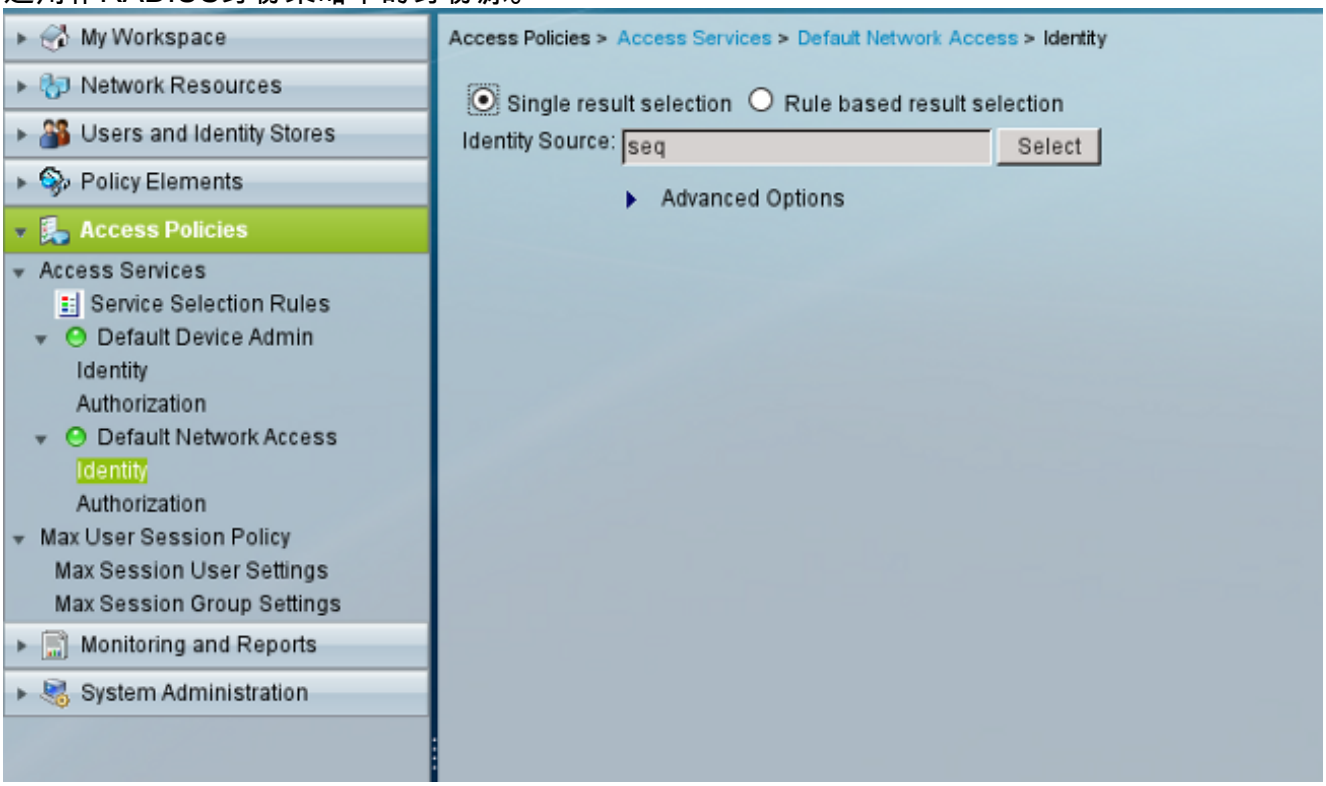
ACS使用从请求方收到的证书中的CN字段匹配AD用户名（在本例中为test1、test2或test3）。 还启用了二进制比较。这会强制ACS从AD获取用户证书，并将其与请求方收到的相同证书进行比较。如果不匹配，则身份验证失败。



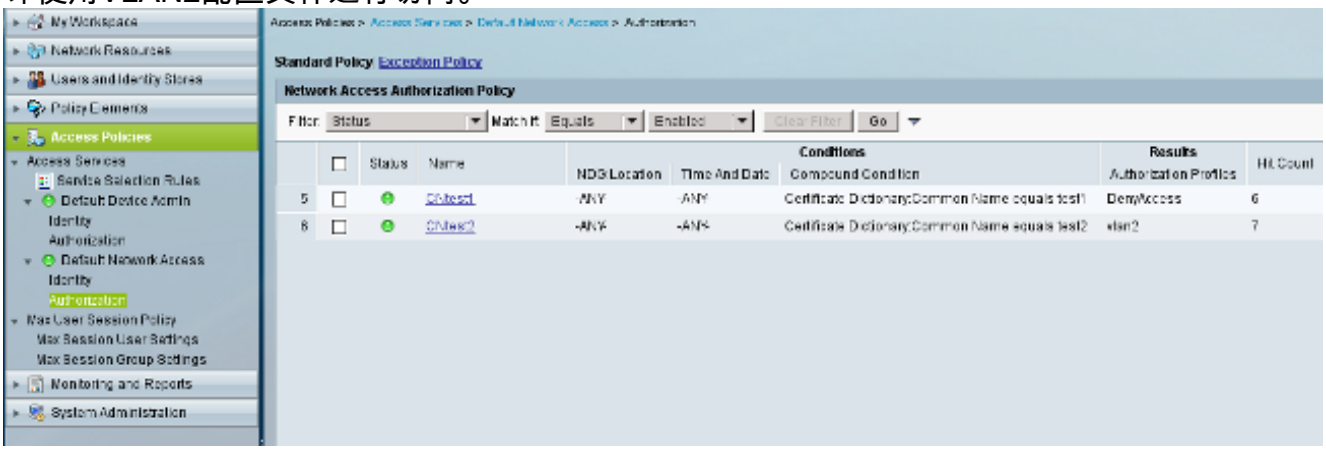
2. 配置身份库序列，该序列使用AD与证书配置文件一起进行基于证书的身份验证。



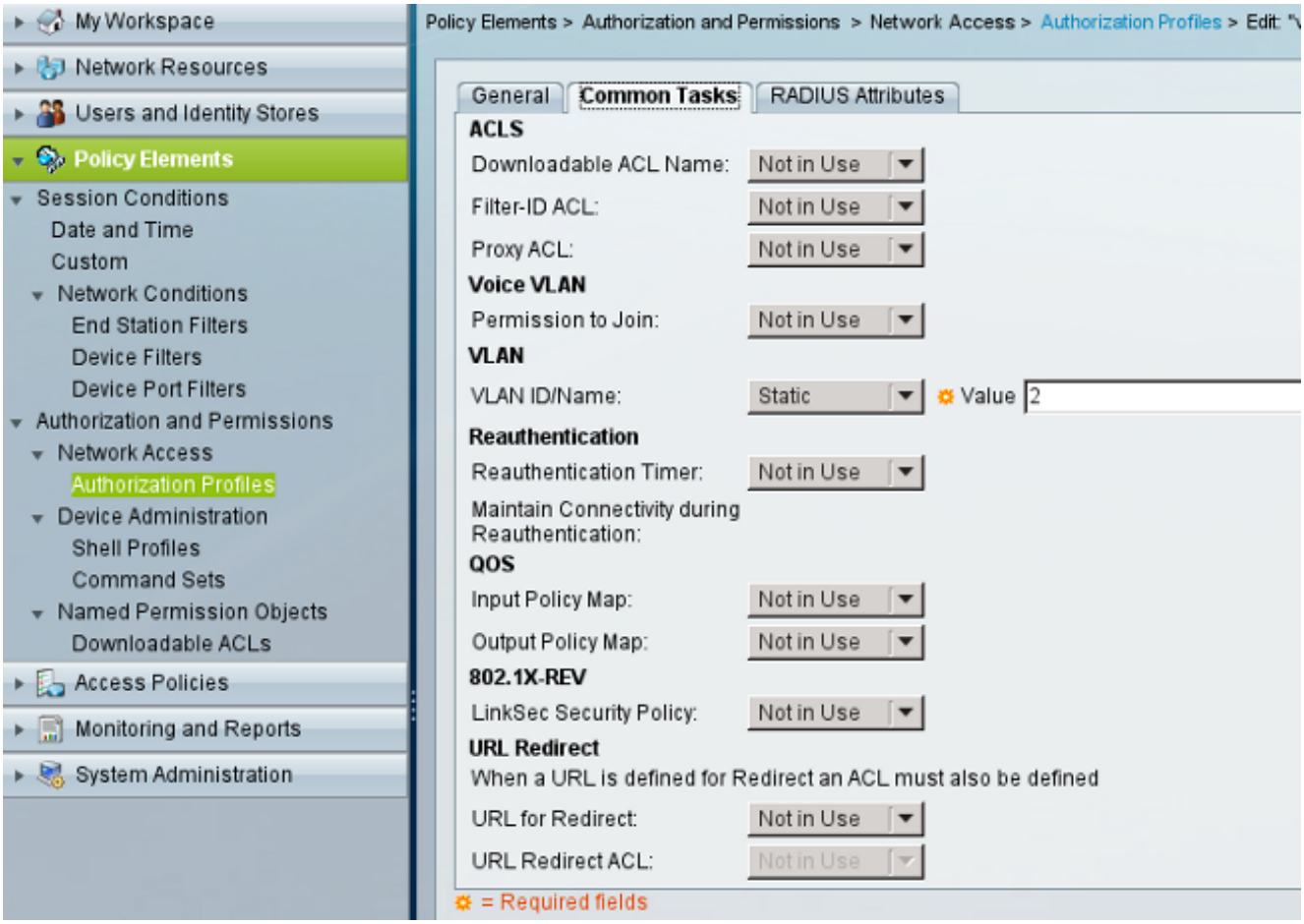
这用作RADIUS身份策略中的身份源。



3. 配置两个授权策略。第一个策略用于test1，它拒绝访问该用户。第二个策略用于测试2，它允许使用VLAN2配置文件进行访问。

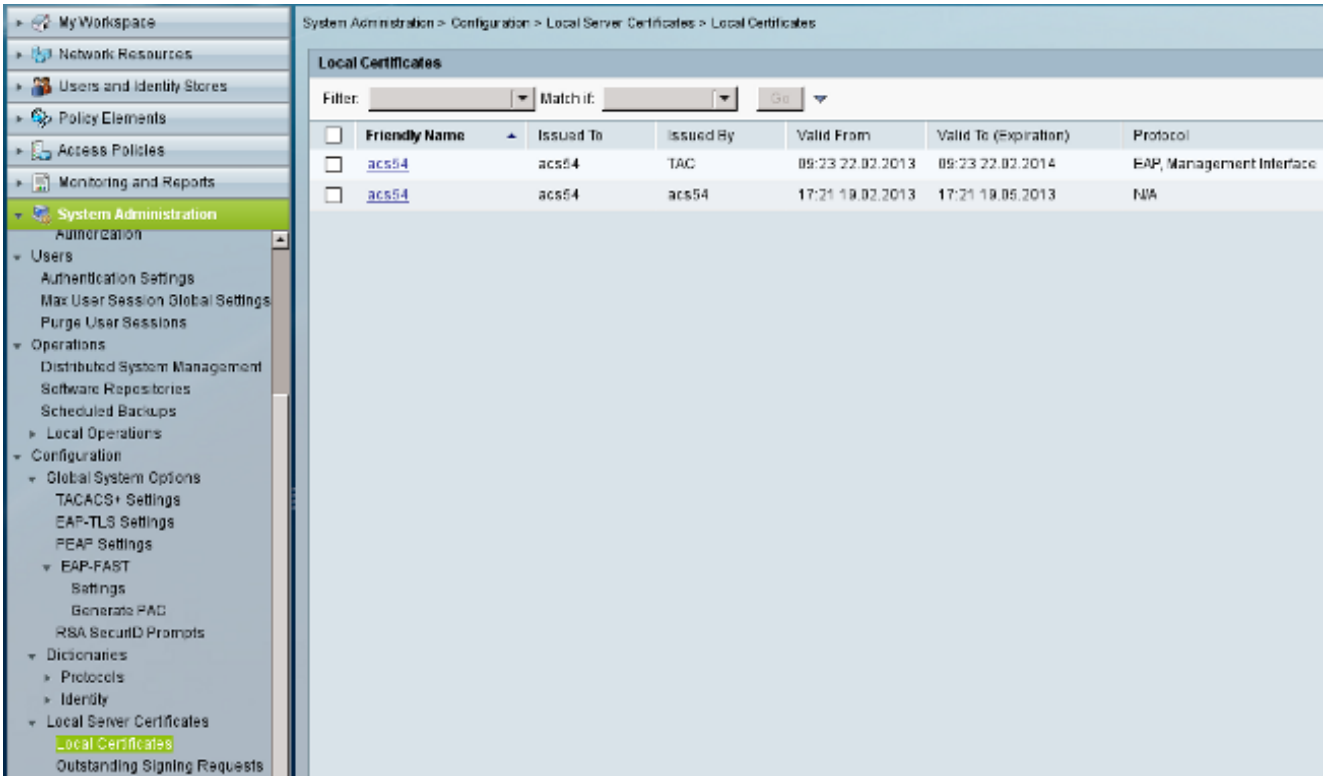


VLAN2是授权配置文件，返回将用户绑定到交换机上VLAN2的RADIUS属性。



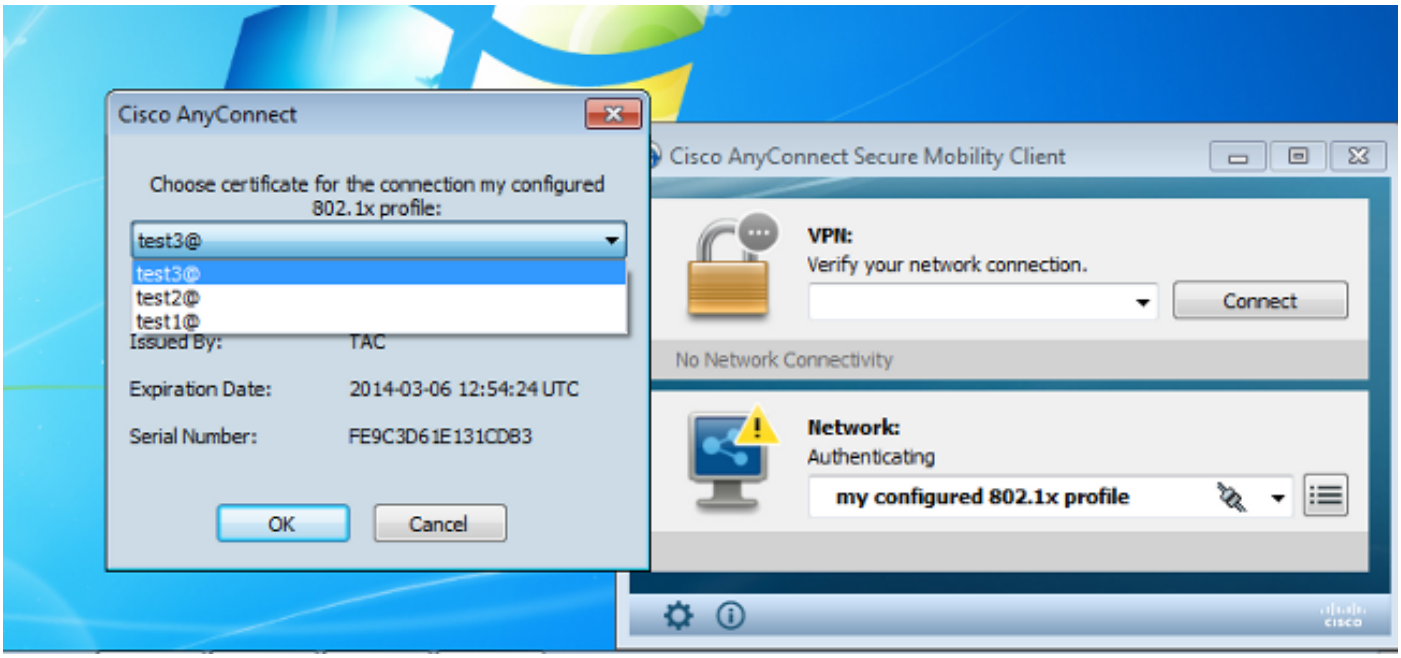
4. 在ACS上安装CA证书。

5. 生成并安装由思科CA for ACS签名的证书（用于可扩展身份验证协议）。



验证

在Windows 7请求方上禁用本地802.1x服务是一种好的做法，因为使用的是AnyConnect NAM。使用配置文件，客户端可以选择特定证书。



使用test2证书时，交换机会收到成功响应和RADIUS属性。

```
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
```

请注意，已分配VLAN 2。 可以在ACS上将其他RADIUS属性添加到该授权配置文件（例如高级访问控制列表或重新授权计时器）。

ACS上的日志如下：

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

故障排除

ACS上的时间设置无效

可能的错误 — ACS Active Directory中出现内部错误

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.

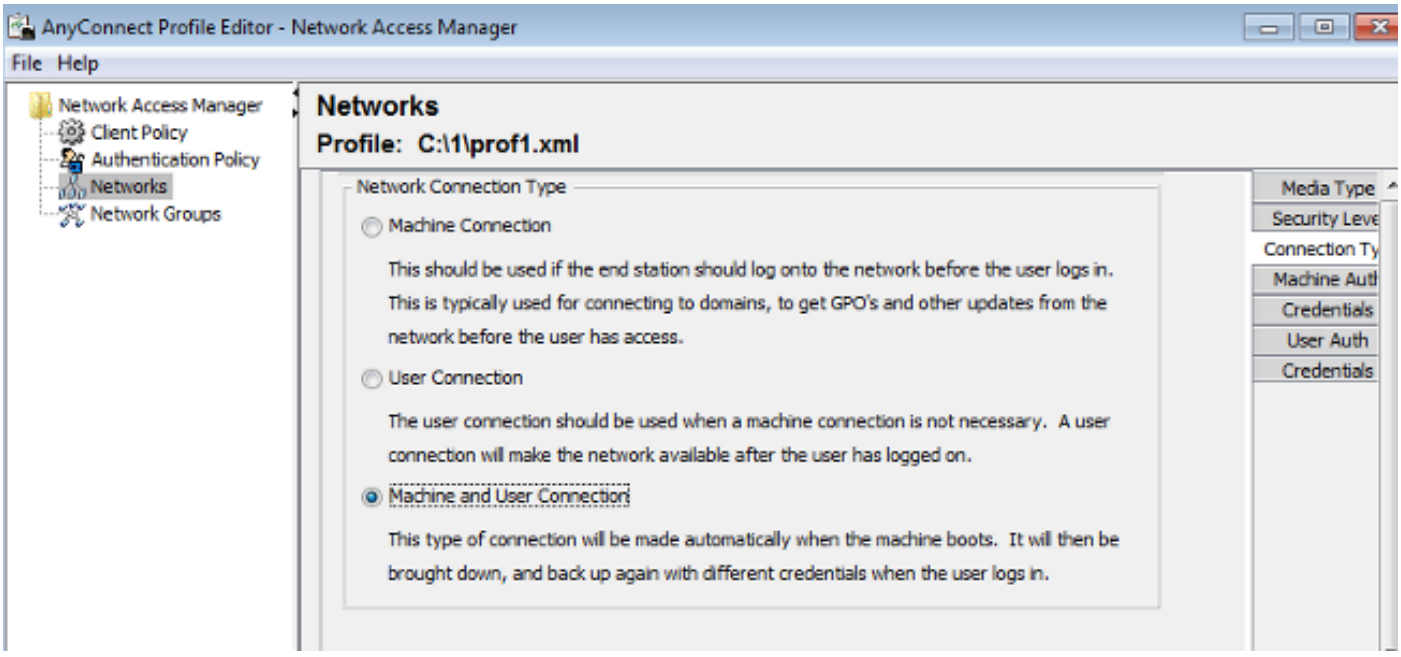
AD DC上未配置和绑定证书

可能的错误 — 无法从Active Directory检索用户证书

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配置文件自定义

在企业网络中，建议同时使用计算机和用户证书进行身份验证。在这种情况下，建议在具有受限VLAN的交换机上使用开放式802.1x模式。在802.1x的计算机重新启动后，将启动第一个身份验证会话并使用AD计算机证书进行身份验证。然后，在用户提供凭证并登录域后，使用用户证书启动第二个身份验证会话。用户被置于正确（受信任）的VLAN中，具有完全网络访问。它与身份服务引擎(ISE)完美集成。



然后，可以从Machine Authentication和User Authentication选项卡配置单独的身份验证。

如果交换机上不允许打开802.1x模式，则在客户端策略中配置登录功能之前，可以使用802.1x模式

。

相关信息

- 思科安全访问控制系统5.3用户指南
- Cisco AnyConnect安全移动客户端管理员指南，版本3.0
- AnyConnect安全移动客户端3.0:Windows上的网络访问管理器和配置文件编辑器
- 技术支持和文档 - Cisco Systems