Ejemplo de Configuración de EAP-TLS 802.1x con Comparación de Certificados Binarios de Perfiles AD y NAM

Contenido

Introducción

Este documento describe la configuración 802.1x con protocolo de autenticación extensible-seguridad de la capa de transporte (EAP-TLS) y sistema de control de acceso (ACS) mientras realizan una comparación de certificado binario entre un certificado de cliente proporcionado por el solicitante y el mismo certificado mantenido en Microsoft Active Directory (AD). El perfil del administrador de acceso de red (NAM) de AnyConnect se utiliza para la personalización. La configuración de todos los componentes se presenta en este documento, junto con escenarios para resolver problemas de la configuración.

Prerequisites

Requirements

No hay requisitos específicos para este documento.

Componentes Utilizados

Este documento no tiene restricciones específicas en cuanto a versiones de software y de hardware.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Convenciones

Consulte Convenciones de Consejos Técnicos de Cisco para obtener más información sobre las convenciones sobre documentos.

Configurar

Topología

- Suplicante 802.1x: Windows 7 con Cisco AnyConnect Secure Mobility Client versión 3.1.01065 (módulo NAM)
- Autenticación 802.1x - switch 2960
- Servidor de autenticación 802.1x - ACS versión 5.4
- ACS integrado con Microsoft AD - controlador de dominio - Windows 2008 Server

Detalles de la topología

- ACS - 192.168.10.152
- 2960 - 192.168.10.10 (e0/0 - suplicante conectado)
- DC - 192.168.10.101
- Windows 7 - DHCP

Flujo

La estación de Windows 7 tiene instalado AnyConnect NAM, que se utiliza como suplicante para autenticarse en el servidor ACS con el método EAP-TLS. El switch con 802.1x actúa como el autenticador. El certificado de usuario es verificado por el ACS y la autorización de política aplica políticas basadas en el Nombre común (CN) del certificado. Además, el ACS obtiene el certificado de usuario de AD y realiza una comparación binaria con el certificado proporcionado por el suplicante.

Configuración del switch

El switch tiene una configuración básica. De forma predeterminada, el puerto se encuentra en la VLAN 666 de cuarentena. Esa VLAN tiene un acceso restringido. Después de que el usuario esté autorizado, el puerto VLAN se reconfigura.

```
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
```

Preparación del certificado

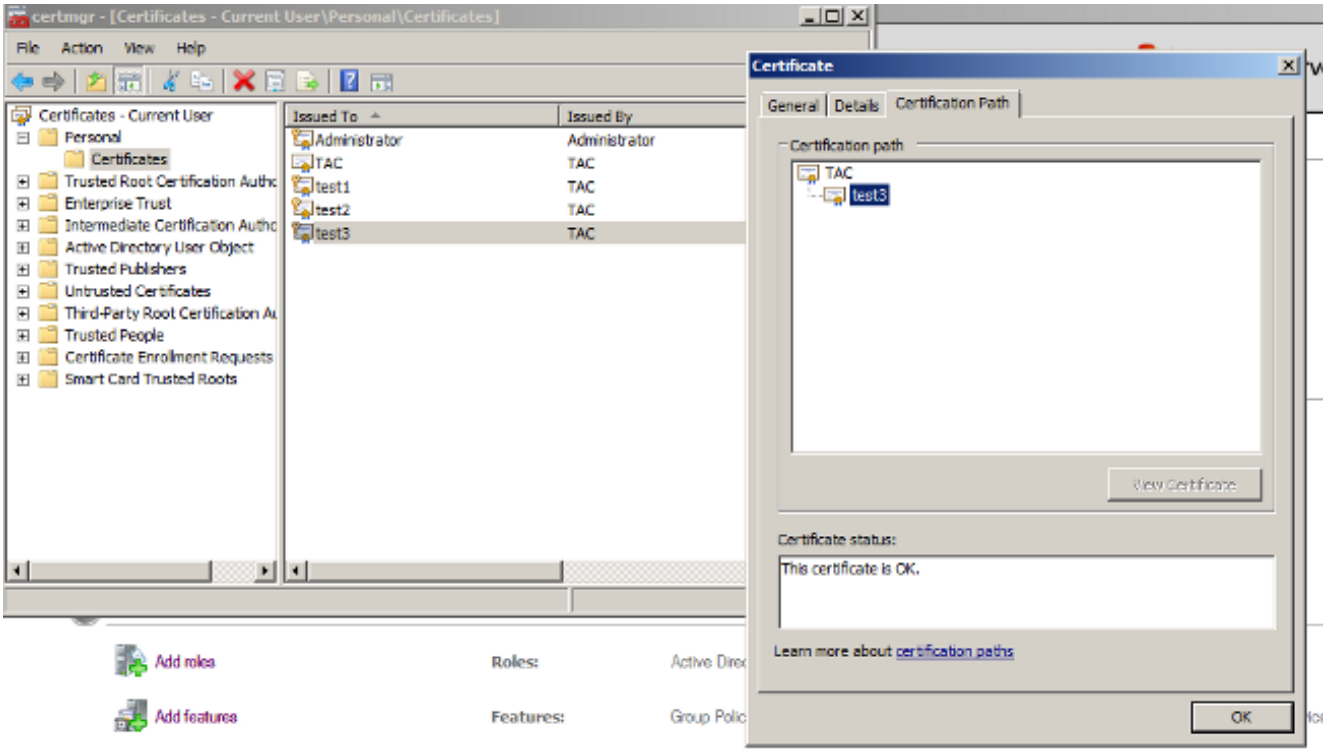
Para EAP-TLS, se requiere un certificado tanto para el suplicante como para el servidor de autenticación. Este ejemplo se basa en certificados generados por OpenSSL. La autoridad certificadora de Microsoft (CA) se puede utilizar para simplificar la implementación en redes empresariales.

1. Para generar la CA, ingrese estos comandos:
   ```
   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
   ```
   El certificado de CA se conserva en el archivo ca.crt y la clave privada (y desprotegida) en el archivo ca.key.
2. Genere tres certificados de usuario y un certificado para ACS, todos firmados por esa CA: CN=test1CN=test2CN=test3CN=acs54La secuencia de comandos para generar un único certificado firmado por la CA de Cisco es:
   ```
   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
   ```
   La clave privada está en el archivo server.key y el certificado está en el archivo server.crt. La versión de pkcs12 se encuentra en el archivo server.pfx.
3. Haga doble clic en cada certificado (archivo .pfx) para importarlo al controlador de dominio.

En el controlador de dominio, los tres certificados deben ser de confianza.

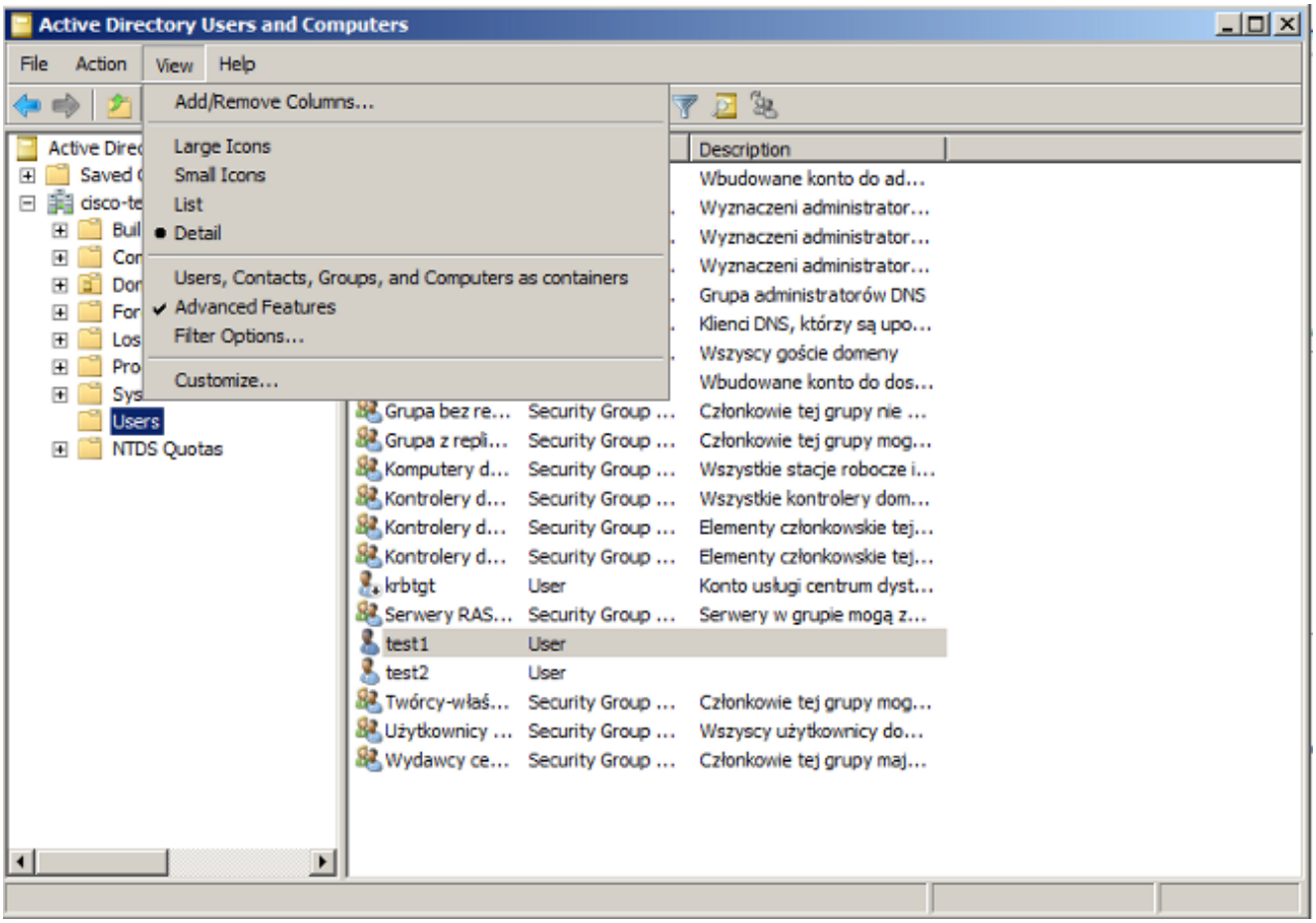


Se puede seguir el mismo proceso en Windows 7 (suplicante) o utilizar Active Directory para enviar los certificados de usuario.

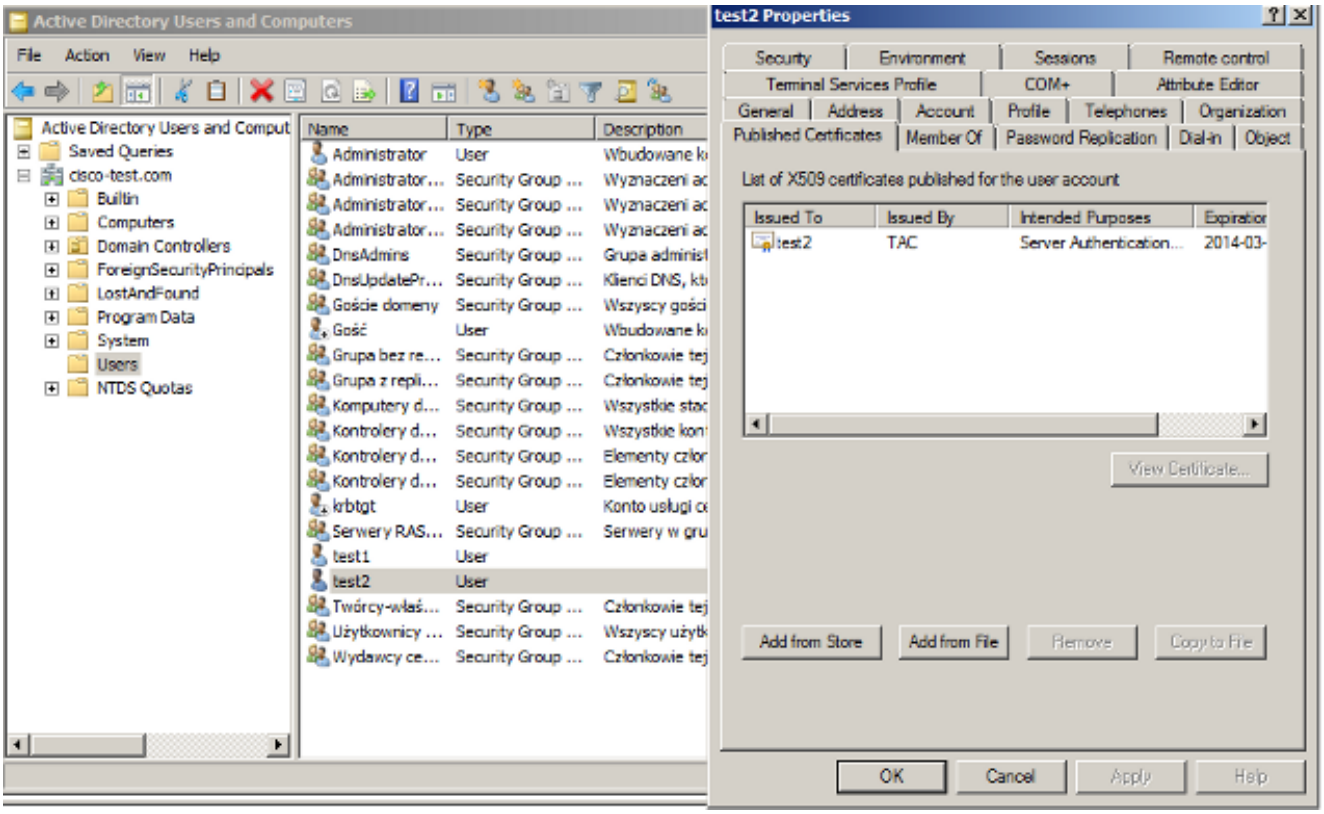
Configuración del controlador de dominio

Es necesario asignar el certificado específico al usuario específico en AD.

1. Desde Usuarios y equipos de Active Directory, desplácese a la carpeta **Usuarios**.
2. En el menú Ver, elija **Funciones avanzadas**.



3. Agregue estos usuarios: test1test2test3**Nota:** La contraseña no es importante.
4. En la ventana Propiedades, elija la ficha **Certificados publicados**. Elija el certificado específico para la prueba. Por ejemplo, para test1, el CN del usuario es test1.**Nota:** No utilice Asignación de nombres (haga clic con el botón derecho en el nombre de usuario). Se utiliza para diferentes
servicios.



En esta etapa, el certificado se enlaza a un usuario específico en AD. Esto se puede verificar con

el uso de ldapsearch:

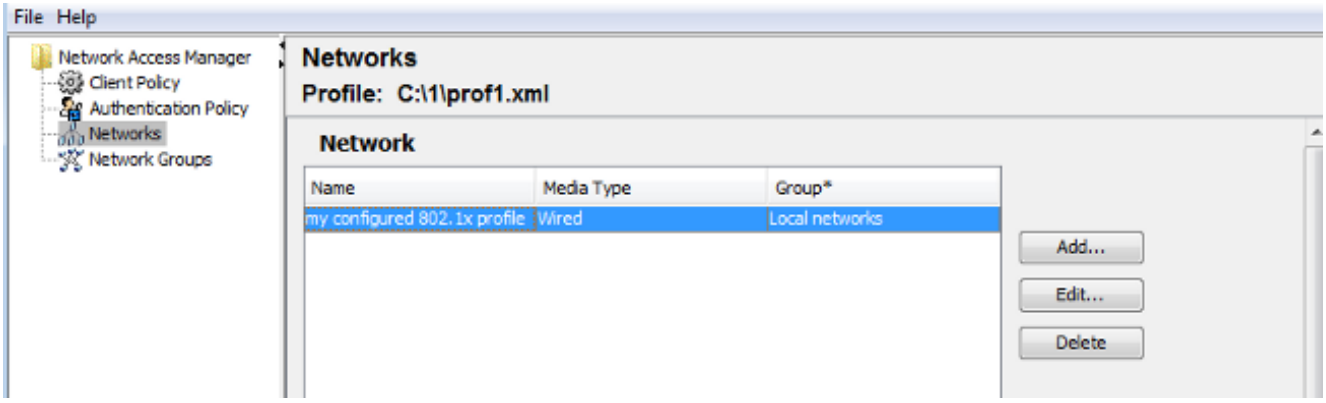
```
ldapsearch -h 192.168.10.101 -D "CN=Administrator,CN=Users,DC=cisco-test,DC=com" -w
Adminpass -b "DC=cisco-test,DC=com"
```

Los resultados de ejemplo para la prueba 2 son los siguientes:

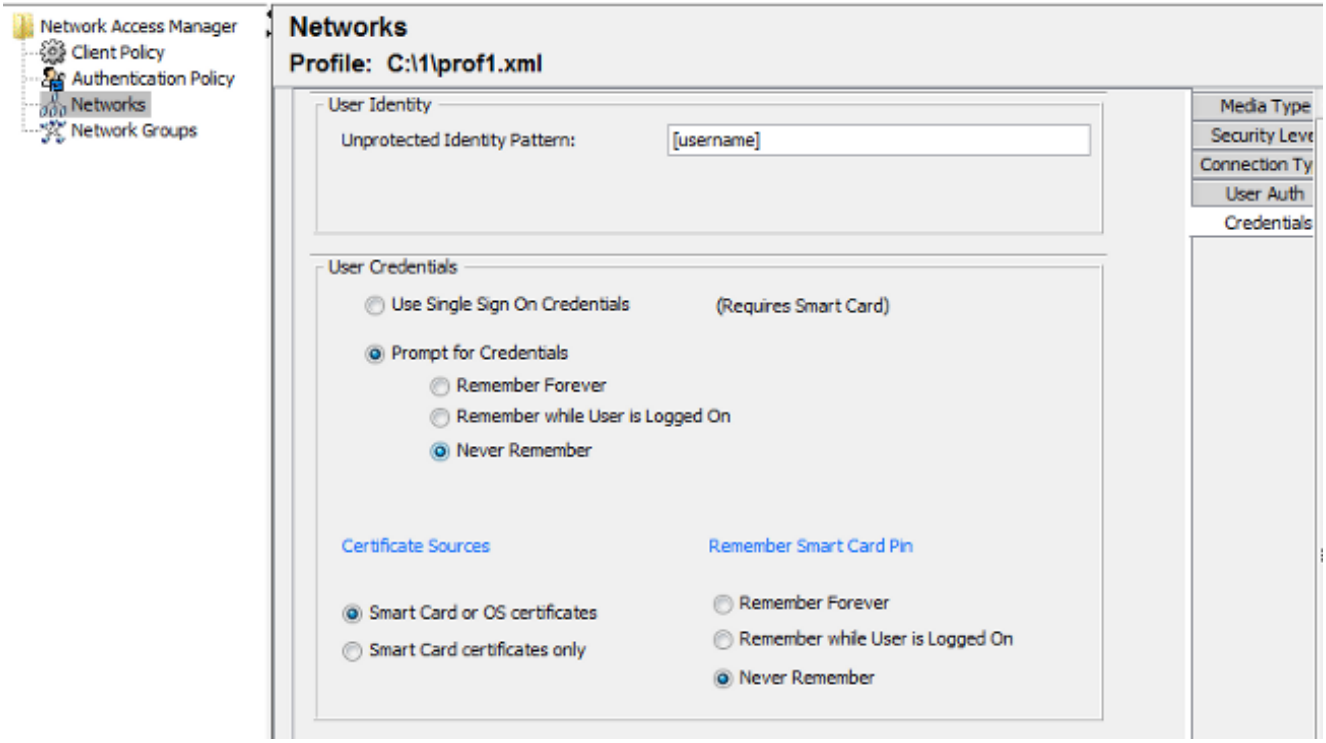
```
# test2, Users, cisco-test.com
dn: CN=test2,CN=Users,DC=cisco-test,DC=com
.................
userCertificate:: MIICuDCCAiGgAwIBAgIJAP6cPWHhMc2yMA0GCSqGSIb3DQEBBQUAMFYxCzAJ
BgNVBAYTAlBMMQwwCgYDVQQIDANNYXoxDzANBgNVBAcMBldhcnNhdzEMMAoGA1UECgwDVEFDMQwwC
gYDVQQLDANSQUMxDDAKBgNVBAMMA1RBQzAeFw0xMzAzMDYxMjUzMjdaFw0xNDAzMDYxMjUzMjdaMF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

Configuración del supplicant

1. Instale este editor de perfiles, anyconnect-profileeditor-win-3.1.00495-k9.exe.
2. Abra el Editor de perfiles del administrador de acceso de red y configure el perfil específico.
3. Cree una red específica con cables.



En esta etapa es muy importante dar al usuario la opción de utilizar el certificado en cada autenticación. No almacenar en caché esa opción. Además, use el 'nombre de usuario' como la ID desprotegida. Es importante recordar que no es la misma ID que utiliza ACS para consultar AD para el certificado. Ese id se configurará en
ACS.

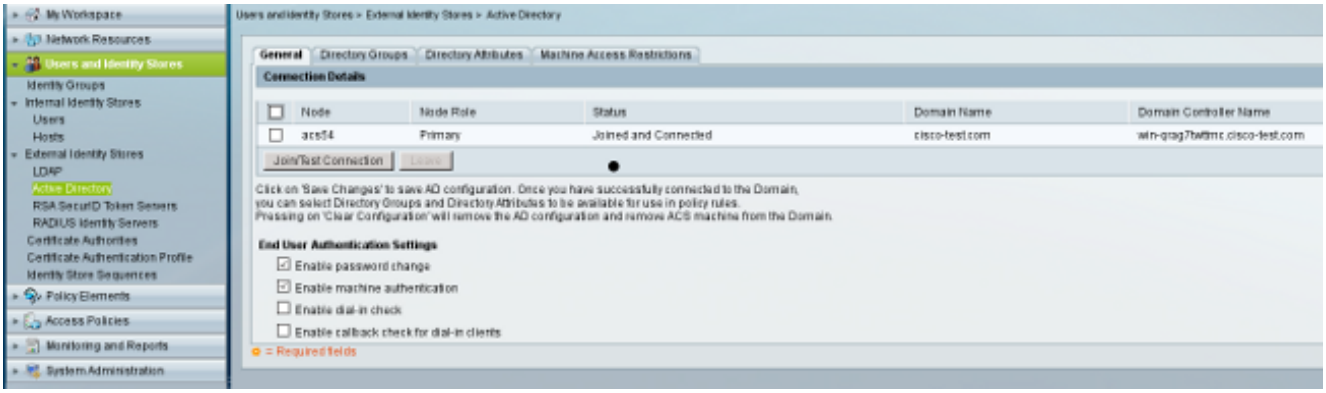


4. Guarde el archivo .xml como c:\Users\All Users\Cisco\Cisco AnyConnect Secure Mobility Client\Network Access Manager\system\configuration.xml.
5. Reinicie el servicio Cisco AnyConnect NAM.

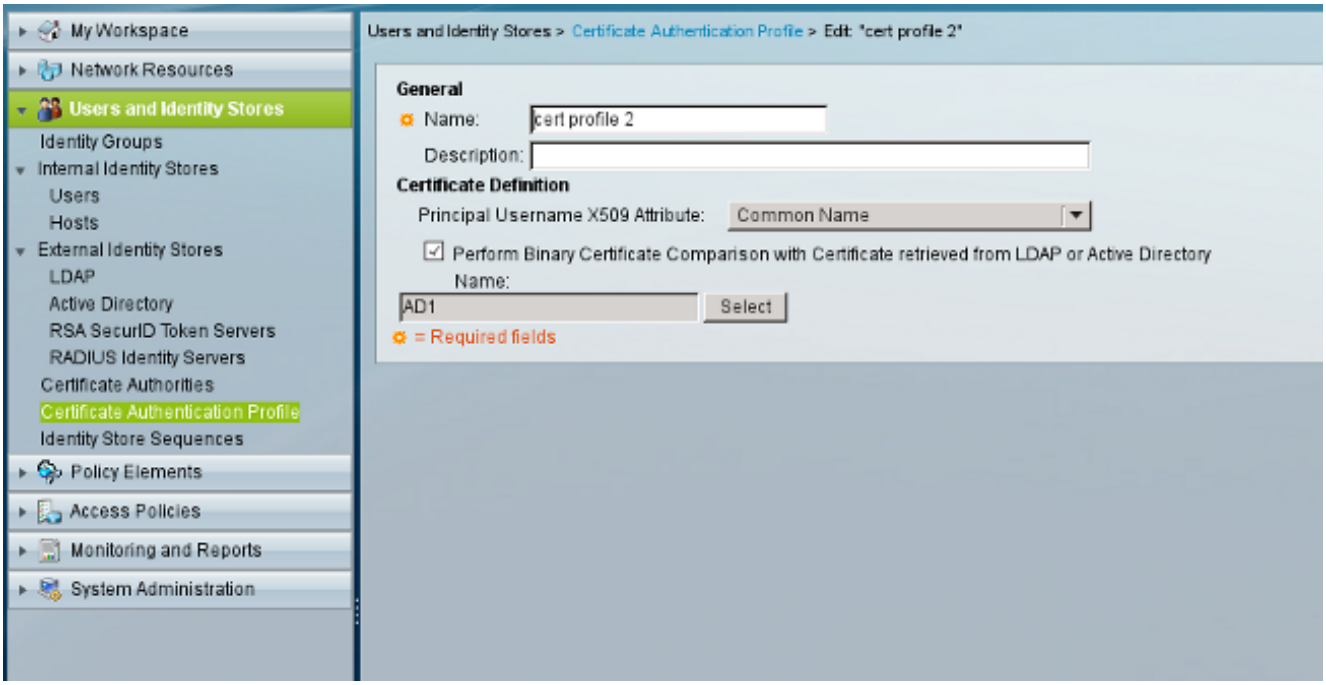
Este ejemplo mostró una implementación manual del perfil. AD podría utilizarse para implementar ese archivo para todos los usuarios. Además, ASA se podría utilizar para aprovisionar el perfil cuando se integra con VPN.

Configuración ACS

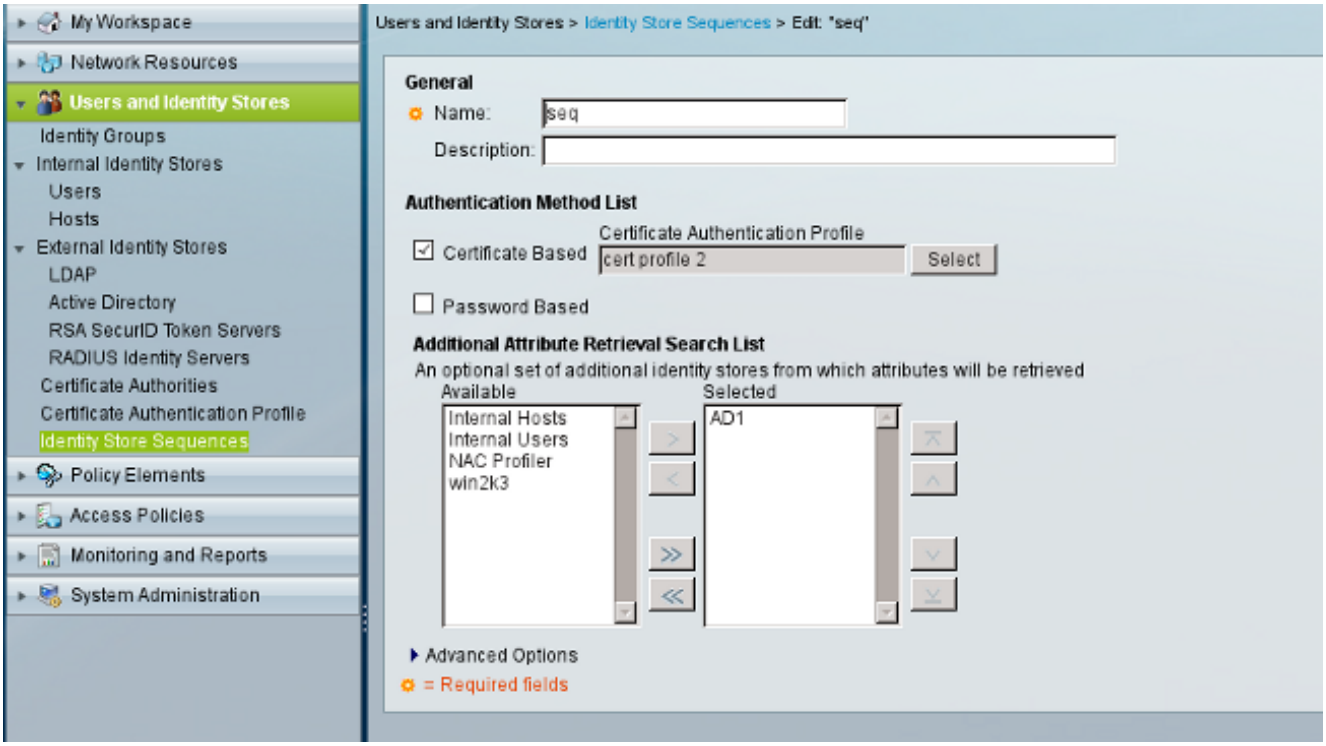
1. Únase al dominio
AD.



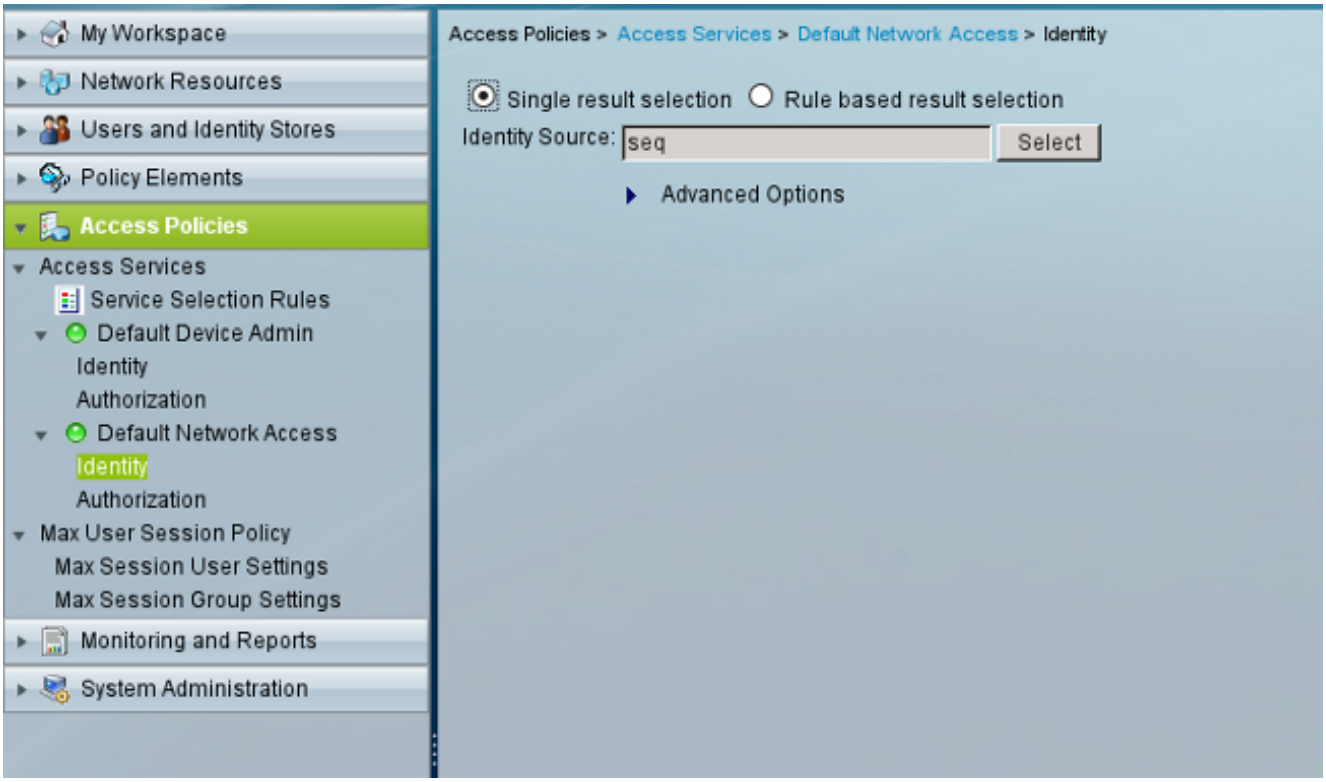
ACS coincide con los nombres de usuario AD con el uso del campo CN del certificado recibido del solicitante (en este caso es test1, test2 o test3). También se habilita la comparación binaria. Esto obliga a ACS a obtener el certificado de usuario de AD y compararlo con el mismo certificado recibido por el solicitante. Si no coincide, la autenticación
falla.



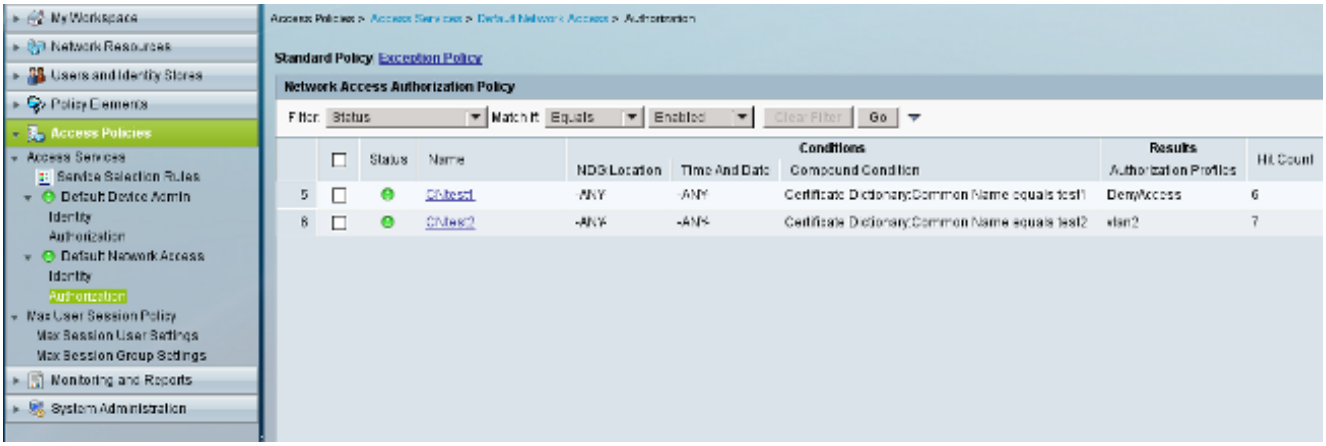
2. Configure las Secuencias del almacén de identidad, que utiliza AD para la autenticación basada en certificados junto con el perfil de certificado.



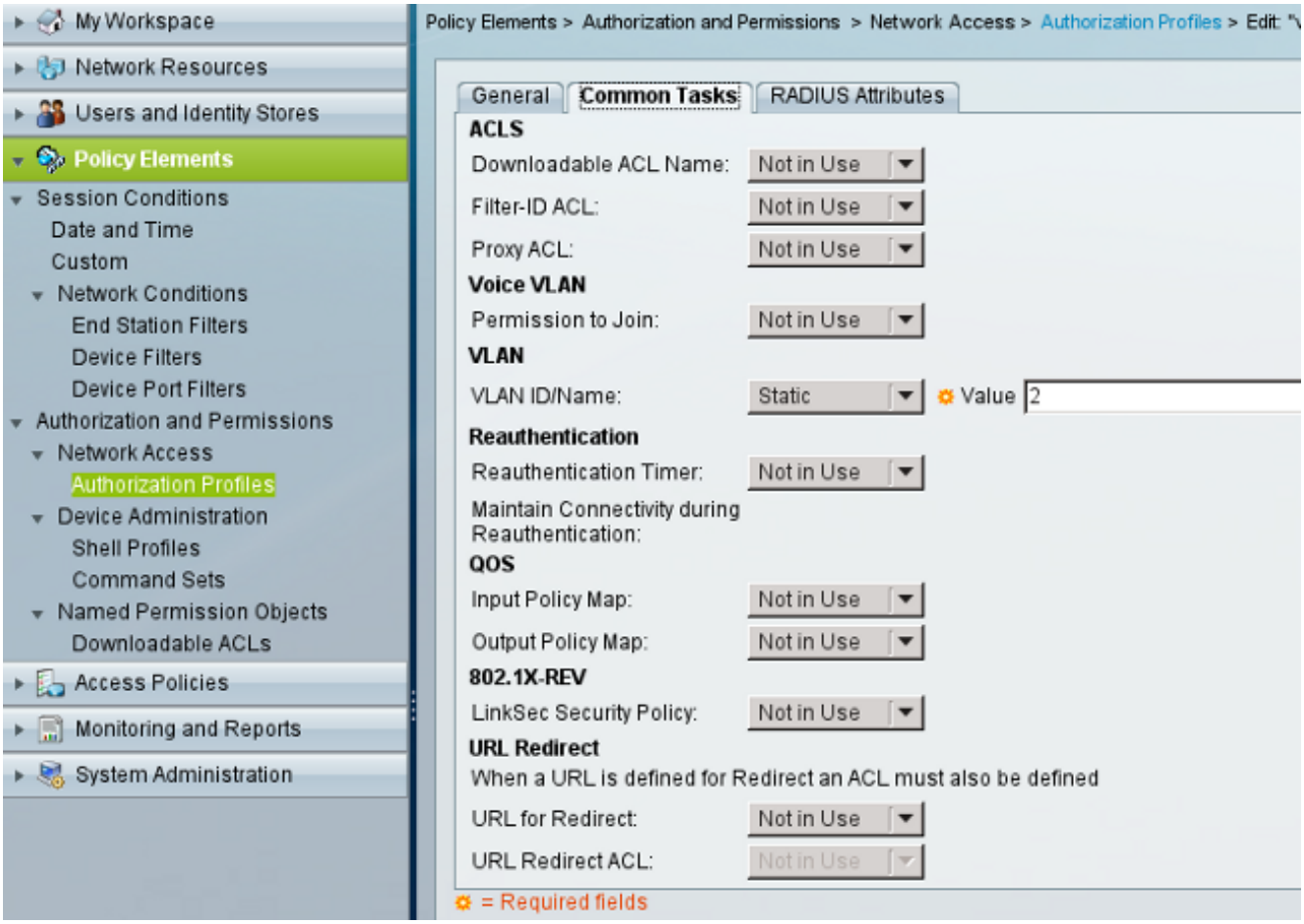
Esto se utiliza como origen de identidad en la política de identidad RADIUS.



3. Configure dos políticas de autorización. La primera política se utiliza para test1 y deniega el acceso a ese usuario. La segunda política se utiliza para la prueba 2 y permite el acceso con el perfil
VLAN2.

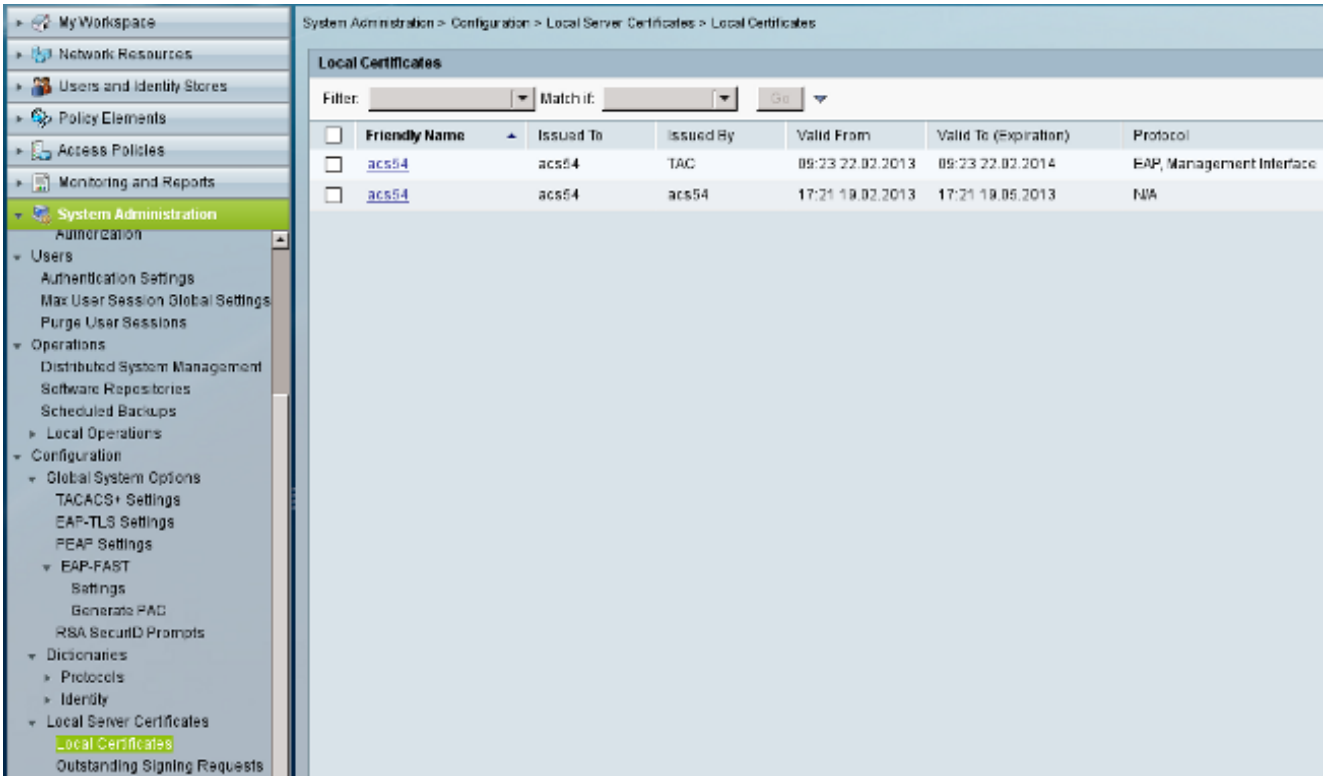


VLAN2 es el perfil de autorización que devuelve los atributos RADIUS que unen al usuario a VLAN2 en el
switch.



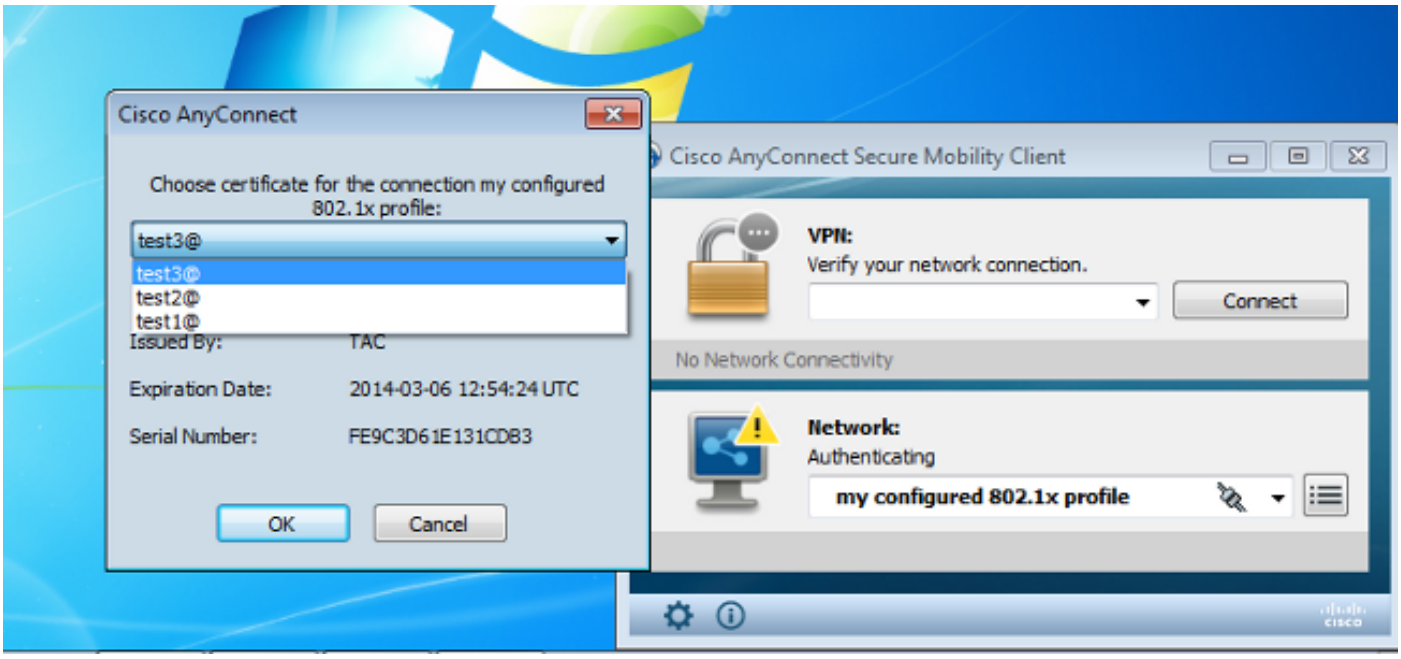
4. Instale el certificado de CA en ACS.

5. Genere e instale el certificado (para uso del protocolo de autenticación extensible) firmado por la CA de Cisco para ACS.



Verificación

Es una buena práctica desactivar el servicio 802.1x nativo en el suplicante de Windows 7 ya que se utiliza AnyConnect NAM. Con el perfil configurado, el cliente puede seleccionar un certificado específico.



Cuando se utiliza el certificado test2, el switch recibe una respuesta satisfactoria junto con los atributos RADIUS.

```
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
```

Tenga en cuenta que se ha asignado la VLAN 2. Es posible agregar otros atributos RADIUS a ese perfil de autorización en ACS (como Lista de control de acceso avanzado o temporizadores de reautorización).

Los registros en ACS son los siguientes:

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

Troubleshoot

Configuración de hora no válida en ACS

Posible error - error interno en 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.

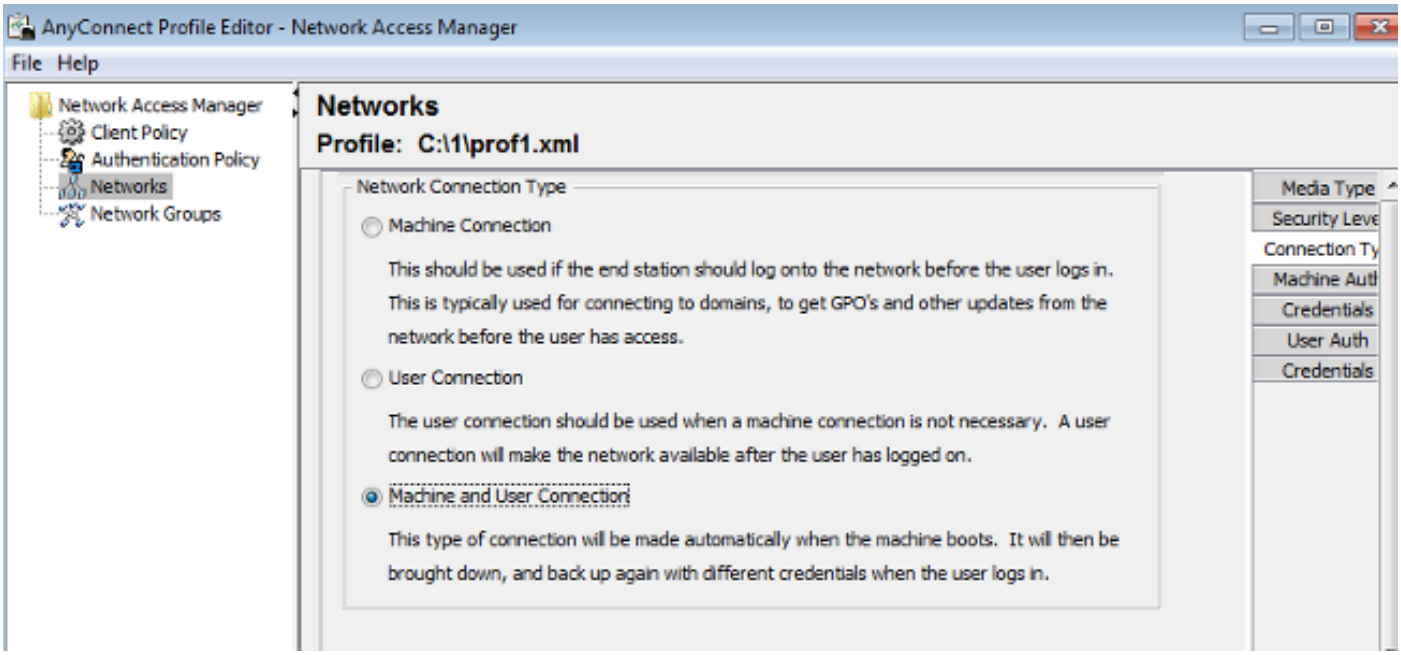
No hay certificado configurado y vinculado en AD DC

Posible error: no se pudo recuperar el certificado de usuario de 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

Personalización del perfil NAM

En redes empresariales, se recomienda autenticarse con el uso de certificados de equipo y de usuario.En este escenario, se recomienda utilizar el modo 802.1x abierto en el switch con VLAN restringida. Al reiniciar la máquina para 802.1x, la primera sesión de autenticación se inicia y se autentica con el uso del certificado de la máquina AD. Luego, después de que el usuario proporcione las credenciales y se registre en el dominio, se inicia la segunda sesión de autenticación con el certificado de usuario. El usuario se coloca en la VLAN correcta (fiable) con acceso completo a la red. Está bien integrado en Identity Services Engine (ISE).



A continuación, es posible configurar autenticaciones separadas de las fichas Autenticación de

equipo y Autenticación de usuario.

Si el modo 802.1x abierto no es aceptable en el switch, es posible utilizar el modo 802.1x antes de que la función de inicio de sesión se configure en la política de cliente.

Información Relacionada

- Guía del usuario de Cisco Secure Access Control System 5.3
- Guía del administrador de Cisco AnyConnect Secure Mobility Client, versión 3.0
- AnyConnect Secure Mobility Client 3.0: Administrador de acceso de red y Editor de perfiles en Windows
- Soporte Técnico y Documentación - Cisco Systems