# 802.1x EAP-TLS met een binaire certificaatvergelijking van AD- en NAM-profielen

## Inhoud

Inleiding Voorwaarden Vereisten Gebruikte componenten **Conventies** Configureren Topologie **Details topologie** Flow Switch-configuratie Voorbereiding van het certificaat Configuratie van controller Configuratie van leveranciers ACS-configuratie Verifiëren Problemen oplossen Ongeldige tijdinstellingen voor ACS Geen certificaat ingesteld en gebonden op AD DC Aanpassing van NAM-profiel Gerelateerde informatie

# Inleiding

Dit document beschrijft de configuratie 802.1x met Extensible Authentication Protocol-Transport Layer Security (EAP-TLS) en Access Control System (ACS), aangezien zij een binaire certificaatvergelijking uitvoeren tussen een client-certificaat dat door de aanvrager is geleverd en hetzelfde certificaat dat in Microsoft Active Directory (AD) wordt bewaard. Het AnyConnect Network Access Manager (NAM) profiel wordt gebruikt voor aanpassing. De configuratie voor alle onderdelen wordt in dit document weergegeven, samen met de scenario's voor het oplossen van problemen in de configuratie.

## Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

#### Gebruikte componenten

Dit document is niet beperkt tot specifieke software- en hardware-versies.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

#### Conventies

Raadpleeg de Cisco Technical Tips Convention voor meer informatie over documentconventies.

## Configureren

#### Topologie

- 802.1x applicatie Windows 7 met Cisco AnyConnect Secure Mobility Client release 3.1.010/65 (NAM-module)
- 802.1x authenticator 2960 switch
- 802.1x verificatieserver ACS release 5.4
- ACS geïntegreerd met Microsoft AD Domain Controller Windows 2008-server

#### **Details topologie**

- ACS 192.168.10.152
- 2960 192.168.10.10 (e0/0 aangesloten op smeekbede)
- DC 19.2.168.10.101
- Windows 7 DHCP

#### Flow

Op het Windows 7-station is AnyConnect NAM geïnstalleerd, dat als zodanig wordt gebruikt om met de EAP-TLS-methode op de ACS-server te bevestigen. De switch met 802.1x treedt in als authentiek. Het gebruikerscertificaat wordt door het ACS gecontroleerd en de beleidsvergunning past een beleid toe dat gebaseerd is op de gemeenschappelijke naam (GN) van het certificaat. Bovendien halen de ACS het gebruikerscertificaat van AD en voeren zij een binaire vergelijking uit met het door de aanvrager verstrekte certificaat.

#### Switch-configuratie

De switch heeft een basisconfiguratie. Standaard is de poort in quarantaine VLAN 666. Dat VLAN

heeft een beperkte toegang. Nadat de gebruiker is geautoriseerd, wordt de poort-VLAN opnieuw geconfigureerd.

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

#### Voorbereiding van het certificaat

Voor EAP-TLS is een certificaat vereist voor zowel de aanvrager als de authenticatieserver. Dit voorbeeld is gebaseerd op OpenSSL gegenereerde certificaten. Microsoft certificaatinstantie (CA) kan worden gebruikt om de implementatie in ondernemingsnetwerken te vereenvoudigen.

1. U kunt de CA als volgt genereren:

```
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
```

Het CA-certificaat wordt bewaard in het ca.crt-bestand en de privétoets (en onbeschermd) in het bestand ca.key.

2. Drie gebruikerscertificaten en een certificaat voor ACS genereren, allemaal ondertekend door die CA: CN=test1CN=test2CN=test3GN=acs54Het script dat gebruikt wordt om één certificaat te genereren dat ondertekend is door Cisco's CA is:

```
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

De privé sleutel is in het server.key bestand en het certificaat is in het server.crt bestand. De PC12 versie is in het server.pfx bestand.

3. Dubbelklik op elk certificaat (.pfx-bestand) om het in de Domain Controller te importeren. In de Domain Controller zouden alle drie de certificaten moeten worden vertrouwd.

📅 certmgr - [Certificates - Current	User\Personal\Certificate	es]			
File Action View Help					
i 🗢 🧼 🖄 🔚 😹 🖼 🗮 🔀	🗟 🛛 🖬		¢	ertificate X	N.
Certificates - Current User  Personal  Certificates  Trusted Root Certification Autho  Certification Autho  Certification Autho  Active Directory User Object  Certification Autho  Certification Aut	Issued To A Administrator La TAC Tattest1 Catest2 Ealtest3	Issued By Administrato TAC TAC TAC TAC	И	Certification path	
Hoster Packards     Hind-Party Root Certificates     Third-Party Root Certification A.     Trusted People     Certificate Enrolment Requests     Smart Card Trusted Roots					
				Certificate status:	
	[ • ]			This certificate is OK.	
💦 Add roles		Roles:	Active Direc	Learn more about certification paths	
Add features		Features:	Group Polic	ОК	ici

Hetzelfde proces kan in Windows 7 (smeekbede) worden gevolgd of actieve map worden gebruikt om de gebruikerscertificaten aan te drukken.

#### Configuratie van controller

Het specifieke certificaat moet in kaart worden gebracht aan de specifieke gebruiker in AD.

- 1. Vanuit Active Directory-gebruikers en -computers navigeer naar de gebruikersmap.
- 2. Kies in het menu Beeld de optie Geavanceerde functies.

Active Directory Users and Computers	
File Action View Help	
(= ) Add/Remove Columns	7 🗾 🕱
Active Direc Large Icons	Description
표 🧾 Saved 🤇 Small Icons	Wbudowane konto do ad
🖃 🎼 cisco-te List	. Wyznaczeni administrator
🗄 🔛 Bull 🔹 Detail	. Wyznaczeni administrator
Con     Contacts Groups and Computers as containers	Wyznaczeni administrator
Don Users, contacts, Groups, and computers as containers	<ul> <li>Grupa administratorów DNS</li> </ul>
H G Los Elter Options	. Klienci DNS, którzy są upo
	. Wszyscy goście domeny
Customize	Wbudowane konto do dos
Sys & Grupa bez re Security Group	Członkowie tej grupy nie
🗑 🔁 NTDS Quotas 🥵 Grupa z repli Security Group	Członkowie tej grupy mog
Komputery d Security Group	Wszystkie stacje robocze i
& Kontrolery d Security Group	Wszystkie kontrolery dom
🖧 Kontrolery d Security Group	Elementy członkowskie tej
& Kontrolery d Security Group	Elementy członkowskie tej
🐍 krbtgt User	Konto usługi centrum dyst
& Serwery RAS Security Group	Serwery w grupie mogą z
🐍 test 1 User	
🐍 test2 User	
R Twórcy-właś Security Group	Członkowie tej grupy mog
🖧 Użytkownicy Security Group	Wszyscy użytkownicy do
& Wydawcy ce Security Group	Członkowie tej grupy maj

- 3. Voeg deze gebruikers toe: test1test2test3**Opmerking:** Het wachtwoord is niet belangrijk.
- 4. Kies in het venster Eigenschappen het tabblad Gepubliceerde certificaten. Kies het specifieke certificaat voor de test. Bijvoorbeeld, voor test1 is de gebruiker CN test1.Opmerking: Gebruik geen Name mapping (klik met de rechtermuisknop op de gebruikersnaam). Het wordt gebruikt voor verschillende diensten.

📔 Active Directory Users and Com	puters		test2 Properties	? ×
File Action View Help			Security Environment Sessions Remote control	
冬 🔿 🖄 🛅 🔏 🗎	2 🖸 😹 🛛 🖬 🕄 😹 🖄 🤊	7 🗵 🗷 👘	Terminal Services Profile     COM+ Attribute Editor     General Address Associated Dedte Telephones Comprised	
Active Directory Users and Comput Saved Queries Saved Queries Computers Computers Domain Controllers Computers Domain Controllers ForeignSecurityPrincipals Computers System Users NTDS Quotas	Name         Type           Administrator         User           Administrator         Security Group           BonsAdmins         Security Group           BonsLpdatePr         Security Group           Gosć         User           Gosć         User           Grupa bez re         Security Group           Gosć         User           Grupa z repli         Security Group           Kontrolery d         Security Group           Kest1         User           Lest2         User           Lizytkownicy         Security Group           Wydawcy ce         Security Group	Description Wbudowane k Wyznaczeni ac Wyznaczeni ac Grupa administ Klienci DNS, kti Wszyscy gości Wbudowane k Członkowie tej Członkowie tej Wszystkie stac Wszystkie stac Wszystkie kon Elementy człor Elementy człor Konto usługi cz Serwery w gru Członkowie tej Wszyscy użytk Członkowie tej	General     Address     Account     Profile     Telephones     Organizati       Published Certificates     Member Of     Password Replication     Dial-in     Obj       List of X509 certificates published for the user account     Issued To     Issued By     Intended Purposes     Expiration       Issued To     Issued By     Intended Purposes     Expiration     2014-03-       Image: Server Authentication     2014-03-     Image: Server Authentication     2014-03-       Image: Server Authentication     Yew Certificate     Image: Server Authentication     2014-03-       Image: Server Authentication     Yew Certificate     Image: Server Authentication     Yew Certificate	ect
۲ <u>۲</u>			OK Cancel Apply Help	

In dit stadium is het certificaat gebonden aan een specifieke gebruiker in AD. Dit kan worden

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

#### De resultaten van test2 zijn als volgt:

```
# test2, Users, cisco-test.com
dn: CN=test2, CN=Users, DC=cisco-test, DC=com
. . . . . . . . . . . . . . . . . .
userCertificate:: MIICuDCCAiGgAwIBAgIJAP6cPWHhMc2yMA0GCSqGSIb3DQEBBQUAMFYxCzAJ
BgNVBAYTA1BMMQwwCgYDVQQIDANNYXoxDzANBgNVBAcMBldhcnNhdzEMMAoGA1UECgwDVEFDMQwwC
gYDVQQLDANSQUMxDDAKBgNVBAMMA1RBQzAeFw0xMzAzMDyxMjUzMjdaFw0xNDAzMDyxMjUzMjdaMF
jbzENMAsGA1UECwwEQ29yZTEOMAwGA1UEAwwFdGVzdDIwgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJ
AoGBAMFQZywrGTQKL+LeI19ovNavCFSG2zt2HGs8qGPrf/h3o4IIvU+nN6aZPdkTdsjiuCeav8HYD
aRznaK1LURt1PeGtHlcTgcGZ1MwIGptimzG+h234GmPU59k4XSVQixARCDpMH8IBR9zOSWQLXe+kR
iZpXC444eK0h6w0/+yWb4bAgMBAAGjgYkwgYYwCwYDVR0PBAQDAgTwMHcGA1UdJQRwMG4GCCsGAQU
FBwMBBggrBgEFBQcDAgYKKwYBBAGCNwoDBAYLKwYBBAGCNwoDBAEGCCsGAQUFBwMBBggrBgEFBQgC
QUFAAOBgQCuXwAgcYqLNm6gEDTWm/OWmTFjPyA5KSDB76yVqZwr11ch7eZiNSmCtH7Pn+VILagf9o
tiFl5ttk9KX6tIvbeEC4X/mQVgAB3HuJH5sL1n/k2H10XCXKfMqMGrtsZrA64tMCcCeZRoxfA094n
PulwF4nkcnu1xO/B7x+LpcjxjhQ==
```

#### Configuratie van leveranciers

- 1. Installeer deze profieleditor, anyconnect-profileeditor-win-3.1.00495-k9.exe.
- 2. Open de editor van het netwerktoegangsprofiel en bevestig het specifieke profiel.
- 3. Maak een specifiek bekabeld netwerk.

File Help				
Network Access Manager	Networks Profile: C:\1	prof1.xml		
Networks	Network			4
55	Name	Media Type	Group*	
	my configured 803	2.1x profile Wired	Local networks	
				Add
				Edit
				Delete

In dit stadium is het van groot belang de gebruiker de keuze te geven het certificaat bij elke echtheidscontrole te gebruiken. Stel die keuze niet in. Gebruik ook de "gebruikersnaam" als de onbeschermde identificatie. Het is belangrijk eraan te herinneren dat het niet dezelfde identificatie is die door ACS wordt gebruikt om AD voor het certificaat te vragen. Die hulp zal in ACS worden

ingesteld.

Network Access Manager	Networks Profile: C:\1\prof1.xml	[username]	Media Type Security Leve Connection Ty User Auth
	User Credentials Use Single Sign On Credentials Prompt for Credentials Remember Forever Remember while User is Never Remember	(Requires Smart Card) Logged On	Crebentias
	Certificate Sources      Smart Card or OS certificates      Smart Card certificates only	Remember Smart Card Pin <ul> <li>Remember Forever</li> <li>Remember while User is Logged On</li> <li>Never Remember</li> </ul>	

- 4. Het bestand .xml opslaan als c:\Users\All Users\Cisco\Cisco AnyConnect Secure Mobility Client\Network Access Manager\system\configuration.xml.
- 5. Start de Cisco AnyConnect NAM-service opnieuw.

Dit voorbeeld toonde een handmatige profielplaatsing. AD zou kunnen worden gebruikt om dat bestand voor alle gebruikers in te voeren. ASA zou ook kunnen worden gebruikt om het profiel te voorzien bij integratie met VPN's.

#### ACS-configuratie

1. Doe mee met het AD-

domein.									
» ⊕ MyWorkspace	Users and identity Stores > External is	ves and literity Stores > Edemai klenity Stores > Addive Directory							
B Network Resources     B Users and Identity Stores     Menths Groups	General Directory Groups Directory Abstrates Machine Access Restrictions								
<ul> <li>Internal Identity Stores</li> <li>Users</li> </ul>	Node	Nade Role	Status	Domain Name	Domain Controller Name				
Hosts	ace54	Primary	Joined and Connected	cisco-test.com	win-grag7b#tmt.cisco-test.com				
<ul> <li>External Identity Stores</li> <li>LDAP</li> </ul>	Join/Test Connection	Leave	•						
LDAP         Active Directory         RSB SecuritD Taken Sensors         RADUS Identity Servers         Certificate Authorities         Enables         Solutions         Policy Elements         > Solutions         Certificate Authorities         Certificate Authorities         Certificate Authorities         Certificate Authorities         Certificate Authorities         Solutions         Enable password change         Enable password change </th									
* 📆 System Administration	G - Requiresteros								

ACS komt overeen met AD-gebruikersnamen met gebruikmaking van het GN-veld van het certificaat dat van de aanvrager is ontvangen (in dit geval is het test1, test2 of test3). Binaire vergelijking wordt ook ingeschakeld. Dit dwingt ACS om het gebruikerscertificaat van AD te verkrijgen en vergelijkt het met het zelfde certificaat dat door de aanvrager wordt ontvangen. Als deze niet overeenkomt, faalt de authenticatie.

2. Configureer de sequenties van de Identity Store. Deze zijn gebaseerd op AD voor certificatie op basis van certificaten en hebben tevens betrekking op het certificeringsprofiel.

My Workspace	Users and Identity Stores > Identity Store Sequences > Edit: "seq"
Network Resources     Users and Identity Stores	General Second
Identity Groups   Internal Identity Stores Users Hosts External Identity Stores LDAP Active Directory RSA SecurID Token Servers RADIUS Identity Servers Certificate Authorities Certificate Authonication Profile Identity Store Sequences	Authentication Method List     Certificate Authentication Profile     Certificate Based     Certificate Based     Certificate Based     Certificate Based     Certificate Based     Certificate Based     Additional Attribute Retrieval Search List     An optional set of additional identity stores from which attributes will be retrieved     Available     Selected     Internal Hosts     AD1     Certificate Based     AD1     Certificate Based     AD1     Certificate Based     Cer
<ul> <li>Policy Elements</li> <li>Access Policies</li> <li>Monitoring and Reports</li> <li>System Administration</li> </ul>	NAC Profiler win2k3

Dit wordt gebruikt als de Bron van de Identiteit in het beleid van de Identiteit van de RADIUS.

🕨 🚭 My Workspace	Access Policies > Access Services > Default Network Access > Identity
Network Resources	Single result selection O Rule based result selection
B Users and Identity Stores	Identity Source: seq Select
Policy Elements	Advanced Options
👻 🍌 Access Policies	
<ul> <li>Access Services</li> <li>Service Selection Rules</li> <li>Operault Device Admin Identity Authorization</li> <li>Operault Network Access Identity Authorization</li> <li>Max User Session Policy Max Session User Settings Max Session Group Settings</li> </ul>	
Monitoring and Reports	
<ul> <li>System Administration</li> </ul>	

3. Configureer twee autorisatiebeleid. Het eerste beleid wordt gebruikt voor test1 en ontkent toegang tot die gebruiker. Het tweede beleid wordt gebruikt voor test 2 en het maakt toegang met het VLAN2 profiel

m	iogelijk.										
	🔆 Ny Workspace	Access	nee Palolaes & Access Services & Defaul Maleverk Access & Automation								
	Op Network Resources     Standard Policy Exception Policy										
÷	🕌 Users and Identity Stores	Netwo	Reference Andrease Authoritation Dalica								
۰	🗫 Policy Elements	E Hor									
	🐍 Access Policies	- 154	Jan Sha		· Hattin E	quars - En	entres -				
٣	Access Services Service Selection Rules			Status	Name	NDB:Location	Time And Date	Conditions Compound Condition	Results Authorization Profiles	Hit Count	
	🔹 \Theta Default Device Admin	5			<u>CNtesti</u>	ANY	-ANY	Certificate Dictionary:Common Name equals test1	DenyAccess	6	
	Identity Authorization	8			CNtes:2	-ANY	-ANS	Certificate Dictionary:Common Name equals test2	vtan2	7	
	O Default Network Access Identity Sufferences Nac Seesion Policy Wax Session User Settings Wax Session Group Settings Nontoring and Reports System Administration										

VLAN2 is het autorisatieprofiel dat de eigenschappen van de RADIUS teruggeeft die de gebruiker aan VLAN2 op de switch binden.

My Workspace	Policy Elements > Authorization and Permissions > Network Access > Authorization Profiles > Edit	t "\
Network Resources		_
B Users and Identity Stores	General Common Tasks RADIUS Attributes	
🔻 🎭 Policy Elements	Downloadable ACL Name: Not in Use 🔻	
<ul> <li>Session Conditions         <ul> <li>Date and Time</li> <li>Custom</li> <li>Network Conditions</li> <li>End Station Filters</li> <li>Device Filters</li> <li>Device Port Filters</li> </ul> </li> <li>Authorization and Permissions</li> </ul>	Filter-ID ACL:       Not in Use         Proxy ACL:       Not in Use         Voice VLAN         Permission to Join:       Not in Use         VLAN         VLAN ID/Name:       Static	
<ul> <li>Network Access         <ul> <li>Authorization Profiles</li> <li>Device Administration</li> <li>Shell Profiles</li> <li>Command Sets</li> <li>Named Permission Objects</li> <li>Downloadable ACLs</li> </ul> </li> </ul>	Reauthentication         Reauthentication Timer:       Not in Use         Maintain Connectivity during Reauthentication:         QOS         Input Policy Map:         Output Policy Map:         Not in Use	
<ul> <li>Access Policies</li> <li>Monitoring and Reports</li> <li>System Administration</li> </ul>	802.1X-REV         LinkSec Security Policy:       Not in Use         URL Redirect         When a URL is defined for Redirect an ACL must also be defined         URL for Redirect:       Not in Use         URL Redirect ACL:       Not in Use         C = Required fields	

#### 4. Installeer het CA-certificaat op

ACS.									
🕨 😚 My Workspace	Users and	Jsers and identity Stores > Certificate Authorities							
Interview Resources	Certificate Authorities								
Busers and Identity Stores	Filter:		💌 Ma	tch if:	🔽 Go 🔻				
<ul> <li>Identity Groups</li> <li>Internal Identity Stores</li> </ul>		Friendly Name		Expiration	Issued To	Issued By	Description		
Users Hosts		TAC		08:11 16.11.2013	TAC	TAC			
✓ External Identity Stores LDAP									
Active Directory									
RSA Securib loken Servers RADIUS Identity Servers									
Certificate Authorities Certificate Authonitication Profile									
Identity Store Sequences									

5. Generate en installeer het certificaat (voor Verlenbaar Verificatieprotocol) dat door Cisco's CA voor ACS wordt ondertekend.

> 🔗 MyWorkspace	System	Administration > Conf	guratio	n > Local Server Cer	tificates > Local O	ertific	ates		
By Network Resources	Loca	il Certificates							
Busers and Identity Stores	Fifte	r.		Match if:	[ <b>*</b> ]	Gr			
Policy Elements									P
Access Policies		Friendly Name	-	Issued to	Issued By		valid From	valid to (Expiration)	Protocol
Image: Monitoring and Reports	븝	<u>acs54</u>		acs::4	DAG		09:23 22:02:2013	09:23 22:02:2014	EAP, Management Interface
System Administration     Aumoreation     Aumoreation     Users     Authentication Settings     Max User Session Global Settings     Purge User Sessions     Operations     Distributed System Management     Software Repositories     Scheduled Backups     Local Operations     Configuration     Clobal System Options     TACACS+ Settings     EAP-TLS Settings     EAP-TLS Settings     EAP-TAST     Settings     Generate PAD     RSA SecurtD Prompts     Dictionaries     Protocols     Identity     Local Server Certificates     Local Certificates     Dustanding Signing Requests		<u>acs54</u>		acs54	acs54		17:21 19.02.2013	17:21 19.05.2013	Ν/Α

## Verifiëren

Het is een goede praktijk om native 802.1x-service op de Windows 7-applicatie uit te schakelen omdat AnyConnect NAM wordt gebruikt. Bij het ingestelde profiel mag de client een specifiek certificaat selecteren.

	Cisco AnyConnect		
	Choose certificate for the connection my configured	Cisco AnyConnect Secure Mobility Client	
	802.1x profile: test3@ test3@	VPN: Verify your network connection.	
/	test2@ test1@ Issued By: TAC	No Network Connectivity	Connect
	Expiration Date: 2014-03-06 12:54:24 UTC Serial Number: FE9C3D61E131CDB3	Network: Authenticating my configured 802.1x profile	8 <b>-</b> III
	OK Cancel		
		<b>\$</b> ()	(1) (1) (1) (1) (0)

Wanneer het test2 certificaat wordt gebruikt, ontvangt de switch een succesrespons samen met de RADIUS-kenmerken.

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=C0A80A0A0000001000215F0| 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: COA80A0A0000001000215F0

Acct Session ID: 0x0000005

Handle: 0xE8000002
```

Runnable methods list: Method State dot1x Authc Succes

Merk op dat VLAN 2 is toegewezen. Het is mogelijk andere RADIUS-kenmerken aan dat autorisatieprofiel toe te voegen op ACS (zoals geavanceerde toegangscontrolelijst of hermachtigingstermijnen).

De logbestanden op ACS zijn als volgt:

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
<u>Evaluat</u>	ting 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
<u>Evaluat</u>	ting Group Mapping Policy
12506	EAP-TLS authentication succeeded
11503	Prepared EAP-Success
<u>Evaluat</u>	ting Exception Authorization Policy
15042	No rule was matched
<u>Evaluat</u>	ting 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

# Problemen oplossen

### Ongeldige tijdinstellingen voor ACS

Mogelijke fout - interne fout in ACS actieve map

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.

#### Geen certificaat ingesteld en gebonden op AD DC

Mogelijke fout - heeft het gebruikerscertificaat niet uit actieve map opgehaald

12571 A	ACS will continue to CRL verification if it is configured for specific CA
12811 E	Extracted TLS Certificate message containing client certificate.
12812 E	Extracted TLS ClientKeyExchange message.
12813 E	Extracted TLS CertificateVerify message.
12804 E	Extracted TLS Finished message.
12801 F	Prepared TLS ChangeCipherSpec message.
12802 F	Prepared TLS Finished message.
12816 T	TLS handshake succeeded.
12509 E	EAP-TLS full handshake finished successfully
12505 F	Prepared EAP-Request with another EAP-TLS challenge
11006 F	Returned RADIUS Access-Challenge
11001 F	Received RADIUS Access-Request
11018 F	RADIUS is re-using an existing session
12504 E	Extracted EAP-Response containing EAP-TLS challenge-response
Evaluatin	ng Identity Policy
15006 M	Matched Default Rule
24432 L	Looking up user in Active Directory - test2
24416 U	User's Groups retrieval from Active Directory succeeded
24100 9	Some of the expected attributes are not found on the subject record. The default values, if configured, will be used for these attributes.
24468 F	Failed to retrieve the user certificate from Active Directory.
22049 E	Binary comparison of certificates failed
22057 1	The advanced option that is configured for a failed authentication request is used.
22061 T	The 'Reject' advanced option is configured in case of a failed authentication request.
12507 E	EAP-TLS authentication failed
11504 F	Prepared EAP-Failure
11003 F	Returned RADIUS Access-Reject

#### Aanpassing van NAM-profiel

In Enterprise-netwerken is het raadzaam zowel de machine- als de gebruikerscertificaten te authentiseren. In dat geval is het raadzaam de modus open 802.1x op de switch met beperkt VLAN te gebruiken. Na het opnieuw opstarten van de machine voor 802.1x, wordt de eerste authenticatiesessie gestart en gewaarmerkt met het gebruik van het AD machine certificaat. Daarna, nadat de gebruiker geloofsbrieven en loggen op het domein verstrekt, wordt de tweede authentificatiesessie begonnen met het gebruikerscertificaat. De gebruiker wordt in het juiste (vertrouwde) VLAN gezet met volledige netwerktoegang. Het is volledig geïntegreerd in Identity Services Engine (ISE).

🐴 AnyConnect Profile Editor -	Network Access Manager	- • ×
File Help		
File Help Network Access Manager Client Policy Authentication Policy	<ul> <li>Networks         Profile: C:\1\prof1.xml         Network Connection Type         Machine Connection         This should be used if the end station should log onto the network before the user logs in.         This is typically used for connecting to domains, to get GPO's and other updates from the network before the user has access.         User Connection         The user connection should be used when a machine connection is not necessary. A user     </li> </ul>	Media Type Security Leve Connection Ty Machine Auth Credentials User Auth Credentials
	<ul> <li>Connection will make the network available after the user has logged on.</li> <li>Machine and User Connections</li> <li>This type of connection will be made automatically when the machine boots. It will then be brought down, and back up again with different credentials when the user logs in.</li> </ul>	

Vervolgens kan u afzonderlijke authenticaties configureren naast de tabbladen Machine en Gebruikersverificatie.

Als de modus 802.1x open niet acceptabel is op de switch, kan de 802.1x-modus worden gebruikt voordat de inlogfunctie is ingesteld in het clientbeleid.

## Gerelateerde informatie

- <u>Gebruikershandleiding voor Cisco Secure Access Control System 5.3</u>
- <u>Cisco AnyConnect Secure Mobility Client-beheerdershandleiding, release 3.0</u>
- <u>AnyConnect Secure Mobility Client 3.0: Network Access Manager en Profile Editor voor</u> <u>Windows</u>
- <u>Technische ondersteuning en documentatie Cisco Systems</u>