AD 및 NAM 프로파일 컨피그레이션의 이진 인증 서 비교를 사용하는 802.1x EAP-TLS 예

목차

<u>소</u>개 사전 요구 사항 요구 사항 사용되는 구성 요소 표기 규칙 구성 토폴로지 토폴로지 세부 정보 플로우 스위치 구성 인증서 준비 도메인 컨트롤러 구성 신청자 구성 ACS 컨피그레이션 다음을 확인합니다. 문제 해결 ACS에 잘못된 시간 설정 AD DC에 설정 및 바인딩 된 인증서 없음 NAM 프로필 사용자 지정 관련 정보

소개

이 문서에서는 서 플리 컨 트가 제공한 클라이언트 인증서와 Microsoft AD(Active Directory)에 보관 된 동일한 인증서 간에 이진 인증서 비교를 수행할 때 EAP-TLS(Extensible Authentication Protocol-Transport Layer Security) 및 ACS(Access Control System)가 포함된 802.1x 컨피그레이션에 대해 설명합니다. AnyConnect NAM(Network Access Manager) 프로파일이 사용자 지정에 사용됩니다. 모든 구성 요소에 대한 컨피그레이션이 이 문서에 나와 있으며 구성 문제를 해결하는 시나리오가 나와 있습니다.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서는 특정 소프트웨어 및 하드웨어 버전으로 한정되지 않습니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바 이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

표기 규칙

문서 규칙에 대한 자세한 내용은 <u>Cisco 기술 팁 규칙</u>을 참조하십시오.

구성

토폴로지

- 802.1x 신청자 Windows 7 with Cisco AnyConnect Secure Mobility Client Release 3.1.01065(NAM 모듈)
- 802.1x 인증자 2960 스위치
- 802.1x 인증 서버 ACS 릴리스 5.4
- Microsoft AD와 통합된 ACS 도메인 컨트롤러 Windows 2008 Server

토폴로지 세부 정보

- ACS 192.168.10.152
- 2960 192.168.10.10(e0/0 신청자가 연결됨)
- DC 192.168.10.101
- Windows 7 DHCP

플로우

Windows 7 스테이션에는 AnyConnect NAM이 설치되어 있습니다. 이 NAM은 EAP-TLS 방법으로 ACS 서버에 인증하는 신청자로 사용됩니다. 802.1x가 있는 스위치는 인증자 역할을 합니다. 사용 자 인증서는 ACS에서 확인되며 정책 권한 부여는 인증서의 CN(Common Name)에 따라 정책을 적 용합니다. 또한 ACS는 AD에서 사용자 인증서를 가져오고 신청자가 제공한 인증서와 이진 비교를 수행합니다.

스위치 구성

스위치에는 기본 컨피그레이션이 있습니다. 기본적으로 포트는 격리 VLAN 666에 있습니다. 해당 VLAN에는 액세스가 제한됩니다. 사용자에게 권한이 부여되면 포트 VLAN이 다시 구성됩니다.

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

인증서 준비

EAP-TLS의 경우 신청자와 인증 서버 모두에 인증서가 필요합니다. 이 예는 OpenSSL에서 생성한 인증서를 기반으로 합니다. Microsoft CA(Certificate Authority)를 사용하여 엔터프라이즈 네트워크 의 구축을 간소화할 수 있습니다.

- 1. CA를 생성하려면 다음 명령을 입력합니다. 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 인증서는 ca.crt 파일 및 ca.key 파일의 개인(및 보호되지 않음) 키에 보관됩니다.
- 2. 세 개의 사용자 인증서 및 해당 CA에서 서명한 ACS용 인증서를 생성합니다. CN=test1CN=test2CN=테스트3CN=acs54Cisco CA가 서명한 단일 인증서를 생성하는 스크립 트는 다음과 같습니다.

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

개인 키는 server.key 파일에 있으며 인증서는 server.crt 파일에 있습니다. pkcs12 버전이 server.pfx 파일에 있습니다.

3. 각 인증서(.pfx 파일)를 두 번 클릭하여 도메인 컨트롤러로 가져옵니다. Domain Controller(도 메인 컨트롤러)에서는 세 가지 인증서를 모두 신뢰해야 합니다.

📅 certmgr - [Certificates - Current User\Personal\Certifica	ites]			_	
File Action View Help			- ·		
♦ 2 1 4 4 × 2 6 2 1			Certificate	٩ľ	v
🔯 Certificates - Current User 🔰 Issued To 🔺	Issued By	(General Details Contincation Path	ı۲	-
E Personal	Administra	ator	Certification path		
Certificates	TAC		TAC	II.	-
Inusted Root Certification Author Testa	TAC		test3		
Enterprise Trust	TAC				
E Active Directory User Object	TAC				
🗉 🧮 Trusted Publishers					
Untrusted Certificates					
Third-Party Root Certification Ac Transfer Decels					
III Certificate Enrolment Requests					
Smart Card Trusted Roots					
				II-	-
			Vew Certificate		
			Certificate status:		
I F I			This certificate is OK.		
	,			H	
💫 Add roles	Roles:	Active Direc	Learn more about <u>pertification paths</u>		
all and a				1	
Add features	Features:	Group Polic	OK	1 1	CI

Windows 7(서 플리 컨 트)에서 동일한 프로세스를 수행하거나 Active Directory를 사용하여 사용자 인증서를 푸시할 수 있습니다.

도메인 컨트롤러 구성

특정 인증서를 AD의 특정 사용자에게 매핑해야 합니다.

- 1. Active Directory Users and Computers(Active Directory 사용자 및 컴퓨터)에서 Users(**사용자**) 폴더**로** 이동합니다.
- 2. 보기 메뉴에서 고급 **기능**을 선택합니다.

Active Directory Users and Computers	
File Action View Help	
(no no line and line	7 🔁 🕱
Active Direc Large Icons	Description
🕀 🧰 Saved 🤇 Small Icons	Wbudowane konto do ad
🖂 🎼 cisco-te List	. Wyznaczeni administrator
🗄 🦲 Bull 🔹 Detail	. Wyznaczeni administrator
Con Lisers Contacts Groups and Computers as containers	. Wyznaczeni administrator
Don osers, contacts, ordaps, and comparers as containers	 Grupa administratorów DNS
	. Klienci DNS, którzy są upo
	 Wszyscy goście domeny
Customize	Wbudowane konto do dos
Users & Grupa bez re Security Group	Członkowie tej grupy nie
🗑 🧰 NTDS Ouotas 🛛 🍇 Grupa z repl 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 uslugi centrum dyst
Serwery RAS Security Group	Serwery w grupie mogą z
👗 test 1 User	
👗 test2 User	
👫 Twórcy-właś Security Group	Członkowie tej grupy mog
🖧 Użytkownicy Security Group	Wszyscy użytkownicy do
& Wydawcy ce Security Group	Członkowie tej grupy maj

- 3. 다음 사용자를 추가합니다. 테스트1테스트2테스트3**참고:** 비밀번호는 중요하지 않습니다.
- 4. 속성 창에서 게시된 **인증서** 탭을 선택합니다. 테스트에 대한 특정 인증서를 선택합니다. 예를 들어 test1의 경우 사용자 CN은 test1입니다.**참고:** 이름 매핑을 사용하지 마십시오(사용자 이 름을 마우스 오른쪽 버튼으로 클릭). 다른 서비스에 사용됩니다

Active Directory Users and Complete Series and Complete Series (Series 2019)	puters			test2 Prope	rties				<u>१×</u>
Active Directory Users and Com File Action View Help Active Directory Users and Comput Saved Queries Saved Queries Saved Queries Saved Queries Domain Controllers Domain Controllers Domain Controllers Soveram Data System Users NTDS Quotas	Image: Second	Type User Security Group Security Group User Security Group User Security Group User Security Group	Description Woudowane k Wyznaczeni ac Wyznaczeni ac Wyznaczeni ac Grupa administ Kienci DNS, kti Wszyscy gości Wbudowane k Członkowie tej Członkowie tej Wszystkie stac Serweny w gru Członkowie tej	Security Termin General Published C List of X50 Issued T	rties al Service: Address Certificates 19 certificat	Environment s Profile Account Account Member Of Member Of Issued By TAC	Sessions COM+ Profile Teles Password Replic rthe user account Intended Purp Server Authen	Rem Attrib phones cation Di cation Di cation	Ŷ × note control ute Editor Organization al-in Object Expiratior 2014-03- Micete
1 1	Użytkownicy	Security Group Security Group	Wszyscy użytk Członkowie tej	Add from	n Store	Add from File	Bemove	Ca	ay to File
					(ок с	ancel /	sply	Help

이 단계에서는 인증서가 AD의 특정 사용자에게 바인딩됩니다. Idapsearch를 사용하여 확인할 수 있습니다.

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

test2의 결과는 다음과 같습니다.

test2, Users, cisco-test.com
dn: CN=test2,CN=Users,DC=cisco-test,DC=com

.

userCertificate:: MIICuDCCAiGgAwIBAgIJAP6cPWHhMc2yMA0GCSqGSIb3DQEBBQUAMFYxCzAJ BgNVBAYTA1BMMQwwCgYDVQQIDANNYXoxDzANBgNVBAcMB1dhcnNhdzEMMAoGA1UECgwDVEFDMQwwC gYDVQQLDANSQUMxDDAKBgNVBAMMA1RBQzAeFw0xMzAzMDYxMjUzMjdaFw0xNDAzMDYxMjUzMjdaMF oxCzAJBgNVBAYTA1BMMQswCQYDVQQIDAJQTDEPMA0GA1UEBwwGS3Jha293MQ4wDAYDVQQKDAVDaXN jbzENMASGA1UECwwEQ29yZTEOMAwGA1UEAwwFdGVzdDIwgZ&wDQYJKoZIhvcNAQEBBQADgY0AMIGJ AoGBAMFQZywrGTQKL+LeI19ovNavCFSG2zt2HGs&qGPrf/h3o4IIvU+nN6aZPdkTdsjiuCeav&HYD aRznaK1LURt1PeGtH1cTgcGZ1MwIGptimzG+h234GmPU59k4XSVQixARCDpMH8IBR9zOSWQLXe+kR iZpXC444eKOh6wO/+yWb4bAgMBAAGjgYkwgYYwCwYDVR0PBAQDAgTwMHcGA1UdJQRwMG4GCCsGAQU FBwMBBggrBgEFBQcDAgYKKwYBBAGCNwoDBAYLKwYBBAGCNwoDBAEGCCsGAQUFBwMBBggrBgEFBQgC FQYKKwYBBAGCNwoDAQYKKwYBBAGCNxQCAQYJKwYBBAGCNxUGBggrBgEFBQcDAjANBgkqhkiG9w0BA QUFAAOBgQCuXwAgcYqLNm6gEDTWm/OWmTFjPyA5KSDB76yVqZwr11ch7eZiNSmCtH7Pn+VILagf9o tiF15ttk9KX6tIvbeEC4X/mQVgAB3HuJH5sL1n/k2H10XCXKfMqMGrtsZrA64tMCcCeZRoxfAO94n PulwF4nkcnu1x0/B7x+LpcjxjhQ==

신청자 구성

- 1. 이 프로파일 편집기인 anyconnect-profileeditor-win-3.1.00495-k9.exe를 설치합니다.
- 2. Network Access Manager 프로파일 편집기를 열고 특정 프로파일을 구성합니다.
- 3. 특정 유선 네트워크를 생성합니다.

File Help												
Network Access Manager	Networks Profile: C:\1	Networks Profile: C:\1\prof1.xml										
Networks	Network			_								
55	Name	Media Type	Group*									
	my configured 80	2.1x profile Wired	Local networks	Add Edit Delete								

이 단계에서는 사용자에게 각 인증에서 인증서를 사용할 수 있는 선택권을 제공하는 것이 매 우 중요합니다. 선택 사항을 캐시하지 마십시오. 또한 'username'을 보호되지 않는 ID로 사용 합니다. ACS에서 인증서를 AD에 쿼리하는 데 사용하는 ID와 동일하지 않다는 점을 기억해야 합니다. 해당 ID는 ACS에서 구성됩니다

Networks Profile: C:\1\prof1.xml									
dia Type urity Leve ection Ty er Auth edentials									

- 4. .xml 파일을 c:\Users\All Users\Cisco\Cisco AnyConnect Secure Mobility Client\Network Access Manager\system\configuration.xml으로 저장합니다.
- 5. Cisco AnyConnect NAM 서비스를 다시 시작합니다.

이 예에서는 수동 프로파일 구축을 보여 줍니다. AD를 사용하여 모든 사용자에 대해 해당 파일을 구 축할 수 있습니다. 또한 VPN과 통합할 때 ASA를 사용하여 프로파일을 프로비저닝할 수 있습니다.

ACS 컨피그레이션

1. AD 도메인에 가입합니다

•										
# GA My Workspace	Jaers and Werthy Stores > External Identity Stores > Active Directory									
 Instwork Resources 	Ierbook Resources General Concess Restrictions General Concess Restrictions Ceneral Concess Restrictions									
- 48 Users and Identity Stores										
Marth Gunna										
- Internal Martik Stream										
Users	Node Node	Node Role	Status	Domain Name	Domain Controller Name					
Hosts	ace54	Primary	Joined and Connected	cisco-test.com	win-grag7b#tmt.cisco-test.com					
 External Identity Stores 	Join/Test Connection	Lewe	-							
LDAP			•							
Active Directory	Click on 'Bave Changes' to:	save AD configuration. Dr	ce you have successfully connected to the Domain	n,						
RSA SecuriD Token Servers	Pressing on 'Clear Configu	ups and Directory Adribut ation will remove the AD	as to be available for use in policy rules. configuration and remove ACB machine from the t	Domain.						
RADIUS Identity Servers			•							
Certificate Authorities Rueflin	End User Authentication S	ettings								
Manthe Stree Somerican	Enable password cf	hange								
· O. Salise Tempole	Enable machine aut	hentication								
* Go Parcy Elements	Enable dial-in check									
Access Policies	Enable calibrack the	ek for dial-in cliante								
S Monitoring and Reports	· = Required fields	and the second points								
Bystem Administration										

ACS는 신청자로부터 받은 인증서에서 CN 필드를 사용하지 않고 AD 사용자 이름을 매칭합니 다(이 경우 test1, test2 또는 test3). 이진 비교도 활성화됩니다. 이렇게 하면 ACS가 AD에서 사 용자 인증서를 가져와 신청자가 수신한 것과 동일한 인증서와 비교합니다. 일치하지 않으면 인증이 실패합니다

🕨 😚 My Workspace	Users and Identity Stores > Certificate Authentication Profile > Edit "cert profile 2"
Internal Identity Stores Internal Identity Stores	General Control Cert profile 2 Description: Certificate Definition
Users Hosts External Identity Stores LDAP Active Directory RSA SecurID Token Servers RADIUS Identity Servers Certificate Authonities Certificate Authentication Profile Identity Store Sequences	Principal Username X509 Attribute: Common Name Perform Binary Certificate Comparison with Certificate retrieved from LDAP or Active Directory Name: AD1 Select C = Required fields
 Policy Elements Constraints Access Policies Monitoring and Reports System Administration 	

2. 인증서 프로파일과 함께 인증서 기반 인증에 AD를 사용하는 ID 저장소 시퀀스를 구성합니다.

My Workspace	Users and Identity Stores > Identity Store Sequences > Edit: "seq"
In the second	General
👻 🎒 Users and Identity Stores	o Name: Iseq
 Solution of the state of the st	 Name: seq Description: Authentication Method List Certificate Authentication Profile Certificate Based Certificate Based Certificate Based Password Based Additional Attribute Retrieval Search List An optional set of additional identity stores from which attributes will be retrieved Available Selected Internal Hosts NAC Profiler Win2k3 AD1 Xelected Available AD1 Xelected Xelected Xelected
	Advanced Options o = Required fields

RADIUS ID 정책에서 ID 소스로 사용됩니다

.

🕨 🚭 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	
 Access Services Service Selection Rules Opfault Device Admin Identity	
Monitoring and Reports	
System Administration	

3. 두 권한 부여 정책을 구성합니다. 첫 번째 정책은 test1에 사용되며 해당 사용자에 대한 액세스 를 거부합니다. 두 번째 정책은 테스트 2에 사용되며 VLAN2 프로파일을 사용하여 액세스를 허용합니다

My Workspace	Access	issens Policies > Access Services > Detail Heliver's Access > Actestonich											
In two Resources	Standa	Standard Policy Exception Policy											
Users and Identity Stores	Netw	Network Access Authorization Policy											
Policy Flements		with He		in a constant only									
The second distances	Filter	Flict. Status 💌 Match it Equals 💌 Enabled 💌 Clear Fliter 60 🐨											
· Micross Policies							Conditions	Results					
 Access Services Service Selection Rules 			Status	Name	NDB:Location	Time And Date	Compound Condition	Authorization Profiles	Hit Count				
👻 \Theta Default Device Admin	5		Θ	<u>ONtesti</u>	ANY	-ANY	Certificate Dictionary:Common Name equals test1	DenyAccess	6				
Identity	8			CNtes:2	-ANY-	-ANS	Certificate Dictionary:Common Name equals test2	vtan2	7				
Authorization													
V O Debut Network Access													
Autronzation													
 Max User Session Policy 													
Viex Session User Settings													
Wax Bession Group Settings													
Monitoring and Reports													
» 🍕 System Administration													

VLAN2는 사용자를 스위치의 VLAN2에 바인딩하는 RADIUS 특성을 반환하는 권한 부여 프로 파일입니다

.

My Workspace	Poli	cy Elements :	> Authorization and P	Permissions > Network Access > Authorization Profiles > Edit. *
Network Resources	Г			
B Users and Identity Stores		General ACLS	Common Tasks	RADIUS Attributes
🔹 🎭 Policy Elements		Download	lable ACL Name:	Not in Use 🛛 🔻
 Session Conditions Date and Time Custom 		Filter-ID A Proxy ACL	CL:	Not in Use 🛛 🕶
 Network Conditions 		Voice VLA	N	
End Station Filters		Permissio	on to Join:	Not in Use 🛛 🔻
Device Filters		VLAN		
Device Port Filters		VLAN ID/N	lame:	Static 🔽 🗸 Value 2
 Authorization and Permissions Network Access 		Reauthen	tication	
Authorization Profiles		Reauthen	tication Timer:	Not in Use 🛛 💌
Device Administration Shell Profiles Command Sate		Maintain (Reauthen QOS	Connectivity during tication:	
 Named Permission Objects 		Input Polic	cy Map:	Not in Use 🛛 🔻
Downloadable ACLs		Output Po	licy Map:	Not in Use 🛛 💌
Access Policies		802.1X-RE	V	
Monitoring and Reports		LinkSec S	ecurity Policy:	Not in Use 🛛 💌
System Administration		URL Redir	ect PL is defined for P	Padirant on ACL must also ha defined
so system Administration		when a O	RL IS defined for R	Redirect an ACL must also be defined
		URL for R	edirect:	Notin Use
		URL Redi	rect ACL:	Not in Use 🔻
		🜣 = Requir	ed fields	

4. ACS에 CA 인증서를 설치합니다

.

► 😚 My Workspace	Users and	d Identity Stores > (Certificate	Authorities			
Network Resources	Certifi	cate Authorities					
Bars and Identity Stores Identity Groups	Filter		∫▼ Ma	tch if:	[▼ Go マ		
Internal Identity Stores Users		Friendly Name	*	Expiration 08:11.16.11.2013	Issued To TAC	issued By TAC	Description
Hosts • External Identity Stores LDAP Active Directory RSA SecurID Token Servers RADIUS Identity Servers							
Certificate Authorities Certificate Authentication Profile Identity Store Sequences							

5. Cisco CA for ACS에서 서명한 인증서(확장 가능 인증 프로토콜 사용용)를 생성하고 설치합니 다

> 🔗 My Workspace	System	Administration > Conf	guratio	n > Local Server Ce	rtificates > Local O	ertific	sates			
By Network Resources	Loca	Local Certificates								
Isers and Identity Stores	Fifte	r	[Match if:	[*]	Gr				
Policy Elements									_	Bender of
Access Policies		Friendly Name	-	Issued to	Issued By		valid From	valid to (Expiration)		Protocol
Image: Monitoring and Reports	븟	acs54		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-FAST Satings Generate PAC RSA SecurtD Prompts Dictionaries Protocols Identity Local Server Certificates Outstanding Signing Requests		<u>acs54</u>		acs54	ac 554		17:21 19.02.2013	17:21 19.05.2013		Ν/Α

다음을 확인합니다.

AnyConnect NAM이 사용되므로 Windows 7 신청자에서 네이티브 802.1x 서비스를 비활성화하는 것이 좋습니다. 구성된 프로파일을 사용하여 클라이언트는 특정 인증서를 선택할 수 있습니다.

-			
	Cisco AnyConnect		
	Choose certificate for the connection my configured	Cisco AnyConnect Secure Mobility Client	
	test3@ test3@ test2@	VPN: Verify your network connection.	Connect
/.	test1@ Issued By: TAC	No Network Connectivity	
	Serial Number: FE9C3D61E131CDB3	Network: Authenticating	<u>ب</u> ه
	OK Cancel		
		\$ (i)	ាត្រាត់ citeo

test2 인증서를 사용하면 RADIUS 특성과 함께 성공 응답을 받습니다.

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: COA80A0A0000001000215F0

Acct Session ID: 0x0000005

Handle: 0xE8000002
```

Runnable methods list:

Method State dot1x Authc Succes

VLAN 2가 할당되었습니다. ACS의 권한 부여 프로파일(예: Advanced Access Control List 또는 재 권한 부여 타이머)에 다른 RADIUS 특성을 추가할 수 있습니다.

ACS의 로그는 다음과 같습니다.

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

문제 해결

ACS에 잘못된 시간 설정

가능한 오류 - ACS Active Directory의 내부 오류

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 DC에 설정 및 바인딩 된 인증서 없음

가능한 오류 - Active Directory에서 사용자 인증서를 검색하지 못했습니다.

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	s.,
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 프로필 사용자 지정

엔터프라이즈 네트워크에서는 머신 및 사용자 인증서를 모두 사용하여 인증하는 것이 좋습니다.이 러한 시나리오에서는 제한된 VLAN을 사용하는 스위치에서 열린 802.1x 모드를 사용하는 것이 좋 습니다. 802.1x에 대해 시스템을 재부팅하면 첫 번째 인증 세션이 시작되고 AD 머신 인증서를 사용 하여 인증됩니다. 그런 다음 사용자가 자격 증명을 제공하고 도메인에 로그온하면 사용자 인증서로 두 번째 인증 세션이 시작됩니다. 사용자는 전체 네트워크 액세스 권한이 있는 올바른(신뢰할 수 있 는) VLAN에 배치됩니다. ISE(Identity Services Engine)에 원활하게 통합됩니다.



그런 다음 시스템 인증 및 사용자 인증 탭에서 별도의 인증을 구성할 수 있습니다.

열린 802.1x 모드가 스위치에서 허용되지 않는 경우, 클라이언트 정책에서 로그온 기능을 구성하기 전에 802.1x 모드를 사용할 수 있습니다.

관련 정보

- Cisco Secure Access Control System 5.3 사용 설명서
- <u>Cisco AnyConnect Secure Mobility Client 관리자 설명서, 릴리스 3.0</u>
- <u>AnyConnect Secure Mobility Client 3.0: Windows의 네트워크 액세스 관리자 및 프로파일 편집</u> <u>기</u>
- <u>기술 지원 및 문서 Cisco Systems</u>