Exemple de configuration d'EAP-TLS 802.1x avec comparaison de certificats binaires à partir de profils AD et NAM

Contenu

Introduction Conditions préalables **Conditions requises Components Used Conventions** Configuration Topologie Détails de la topologie Flux Configuration du commutateur Préparation du certificat Configuration du contrôleur de domaine Configuration du demandeur **Configuration ACS** Vérification Dépannage Paramètres d'heure non valides sur ACS Aucun certificat configuré et lié sur le contrôleur de domaine Active Directory Personnalisation du profil NAM Informations connexes

Introduction

Ce document décrit la configuration 802.1x avec EAP-TLS (Extensible Authentication Protocol-Transport Layer Security) et ACS (Access Control System), car ils effectuent une comparaison de certificats binaires entre un certificat client fourni par le demandeur et le même certificat conservé dans Microsoft Active Directory (AD). Le profil NAM (Network Access Manager) AnyConnect est utilisé pour la personnalisation. La configuration de tous les composants est présentée dans ce document, ainsi que des scénarios de dépannage de la configuration.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Components Used

Ce document n'est pas limité à des versions de matériel et de logiciel spécifiques.

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.

Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à <u>Conventions relatives aux conseils techniques Cisco.</u>

Configuration

Topologie

- Complément 802.1x Windows 7 avec Cisco AnyConnect Secure Mobility Client version 3.1.01065 (module NAM)
- Authentificateur 802.1x commutateur 2960
- Serveur d'authentification 802.1x ACS version 5.4
- ACS intégré à Microsoft AD Contrôleur de domaine Windows 2008 Server

Détails de la topologie

- ACS 192.168.10.152
- 2960 192.168.10.10 (e0/0 demandeur connecté)
- CC 192.168.10.101
- Windows 7 DHCP

Flux

AnyConnect NAM est installé sur la station Windows 7, qui est utilisé comme demandeur pour s'authentifier auprès du serveur ACS avec la méthode EAP-TLS. Le commutateur 802.1x agit en tant qu'authentificateur. Le certificat utilisateur est vérifié par ACS et l'autorisation de stratégie applique des stratégies basées sur le nom commun (CN) du certificat. En outre, ACS récupère le certificat utilisateur d'AD et effectue une comparaison binaire avec le certificat fourni par le demandeur.

Configuration du commutateur

Le commutateur possède une configuration de base. Par défaut, le port est en quarantaine VLAN 666. Ce VLAN a un accès limité. Une fois l'utilisateur autorisé, le VLAN du port est reconfiguré.

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

Préparation du certificat

Pour EAP-TLS, un certificat est requis pour le demandeur et le serveur d'authentification. Cet exemple est basé sur des certificats générés par OpenSSL. Microsoft Certificate Authority (CA) peut être utilisé pour simplifier le déploiement dans les réseaux d'entreprise.

1. Afin de générer l'autorité de certification, entrez les commandes suivantes :

```
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
```

Le certificat CA est conservé dans le fichier ca.crt et la clé privée (et non protégée) dans le fichier ca.key.

 Générez trois certificats utilisateur et un certificat pour ACS, tous signés par cette autorité de certification : CN=test1CN=test2CN=test3CN=acs54Le script permettant de générer un certificat unique signé par l'autorité de certification de Cisco est le suivant :

```
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 clé privée se trouve dans le fichier server.key et le certificat dans le fichier server.crt. La version pkcs12 se trouve dans le fichier server.pfx.

3. Double-cliquez sur chaque certificat (.pfx file) pour l'importer dans le contrôleur de domaine. Dans le contrôleur de domaine, les trois certificats doivent être approuvés.

📅 certmgr - [Certificates - Current	User\Personal\Certificate	es]			
File Action View Help					
i 🗢 🧼 🖄 🔚 😹 🖼 🗮 🔀	🗟 🛛 🖬		¢	ertificate X	N.
Certificates - Current User Personal Certificates Trusted Root Certification Autho Enterprise Trust Intermediate Certification Autho Active Directory User Object Intersted Robidees	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

Le même processus peut être suivi dans Windows 7 (demandeur) ou utiliser Active Directory pour pousser les certificats utilisateur.

Configuration du contrôleur de domaine

Il est nécessaire de mapper le certificat spécifique à l'utilisateur spécifique dans AD.

- 1. Dans Utilisateurs et ordinateurs Active Directory, accédez au dossier Utilisateurs.
- 2. Dans le menu Affichage, sélectionnez **Fonctions avancées**.

Active Directory Users and Computers	
File Action View Help	
(nemove 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 Iterra Contacta Crauma and Computers as containers	. Wyznaczeni administrator
Dor Users, contacts, Groups, and computers as containers	. Grupa administratorów DNS
H For V Auvaliced Features	. Klienci DNS, którzy są upo
	. Wszyscy goście domeny
Customize	Wbudowane konto do dos
Grupa bez re Security Group	Członkowie tej grupy nie
🗑 🔚 NTDS Ouptas 🛛 🎎 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	
🖓 Twórcy-właś Security Group	Członkowie tej grupy mog
👫 Użytkownicy Security Group	Wszyscy użytkownicy do
🖓 Wydawcy ce Security Group	Członkowie tej grupy maj

- 3. Ajoutez ces utilisateurs : test1test 2test3Note: Le mot de passe n'est pas important.
- 4. Dans la fenêtre Propriétés, sélectionnez l'onglet Certificats publiés. Sélectionnez le certificat spécifique pour le test. Par exemple, pour test1, le CN utilisateur est test1.Note: N'utilisez pas le mappage de noms (cliquez avec le bouton droit sur le nom d'utilisateur). Il est utilisé pour différents

services.

📴 Active Directory Users and Com	test2 Properties								
Active Directory Users and Com File Action View Help Active Directory Users and Comput Solution Active Directory Users and Comput Solution Soluti	Administrator Administrator Administrator Administrator Administrator Administrator DnsUpdatePr Cosć DnsUpdatePr Gosć Gosć Goupa bez re Gosć Grupa bez repl Kontrolery d Kontrolery d Kontrolery d Kontrolery d Kontrolery d Kontrolery d Kontrolery d Kontrolery d Kontrolery d Kontrolery d	Type User Security Group Security Group	Event of the second secon	Lest2 Prope Security Termin General Published (List of X5 Issued 1 Galtest2	erties r E ral Services Address Certificates O9 certificat To 2	invironment s Profile Account Member Of less published for Issued By TAC	Sessions COM+ Profile Tel Password Rep r the user accou Intended Pur Server Author	Remote c Attribute E sphones Orga ication Dial-in nt poses Exp ntication 201	rization Object
×	Serwery RAS Stest1 Stest2 Twórcy-właś Dżytkownicy Wydawcy ce	Security Group User User Security Group Security Group Security Group	Serwery w gru Członkowie tej Wszyscy użytk Członkowie tej	Add fro	m Store	Add from Fil	e <u>Berrove</u> Cancel	Copy to	Fie

Àce stade, le certificat est lié à un utilisateur spécifique dans AD. Ceci peut être vérifié avec

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

Les résultats de l'exemple de test2 sont les suivants :

```
# 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==
```

Configuration du demandeur

- 1. Installez cet éditeur de profil, anyconnect-profileeditor-win-3.1.00495-k9.exe.
- 2. Ouvrez Network Access Manager Profile Editor et configurez le profil spécifique.
- 3. Créez un réseau câblé spécifique.

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

Àce stade, il est très important de donner à l'utilisateur le choix d'utiliser le certificat à chaque authentification. Ne mettez pas en cache ce choix. En outre, utilisez le nom d'utilisateur comme ID non protégé. Il est important de se rappeler que ce n'est pas le même ID qui est utilisé par ACS pour interroger AD pour le certificat. Cet ID sera configuré dans ACS.

Network Access Manager Clent Policy Authentication Policy Networks Network Groups Ver Identity User Identity Unprotected Identity Pattern: User Credentials Use Single Sign On Credentials Prompt for Credentials Remember Forever Remember while User is Lo Networks	[username] Media Securit Connect User				
	User Credentials Use Single Sign On Credentials Prompt for Credentials Remember Forever Remember while User is I Never Remember	(Requires Smart Card) Logged On	Credentials		
	Certificate Sources Image: Smart Card or OS certificates Image: Smart Card certificates only 	Remember Smart Card Pin Remember Forever Remember while User is Logged On Never Remember 			

- 4. Enregistrez le fichier .xml sous c:\Users\All Users\Cisco\Cisco AnyConnect Secure Mobility Client\Network Access Manager\system\configuration.xml.
- 5. Redémarrez le service NAM Cisco AnyConnect.

Cet exemple montre un déploiement manuel des profils. AD peut être utilisé pour déployer ce fichier pour tous les utilisateurs. En outre, ASA peut être utilisé pour provisionner le profil lorsqu'il est intégré à des VPN.

Configuration ACS

1. Rejoignez le domaine

AD.									
MyWorkspace	Users analitiently Stores > External Identity Stores > Active Directory								
Ap Network Resources Ap Network Resources Applementation and Menthy Stores Menthy Groups	General Directory Groups Directory Atributes Mathine Access Restrictions. Commercises Dotails								
 Internal Identity Stores Users 	Node	Node Role	Status	Domain Name	Domain Controller Name				
Hosts	ace54	Primary	Joined and Connected	cisco-test.com	win-grag7twttmt.cisco-test.com				
External Identity Stores LOAP LOAP LOAP									
RSA SecurID Token Seners RADIUS Identity Servers	you can select Directory Grou Pressing on 'Clear Configura	ps and Directory Athibutes to be a dion'will remove the AD configura	wailable for use in policy rules. Son and remove ACIS machine from the Domain.						
Certificate Authorities	End User Authentication Se	ttings							
Centricate Authentication Profile	Enable password ch	ange							
+ Sy Policy Elements	E Enable machine authentication								
Access Policies	Enable dial-in check Enable calibrate for dial-in classin								
Muniforing and Reports	o = Required fields								
Bystem Administration									

ACS fait correspondre les noms d'utilisateurs AD avec l'utilisation du champ CN du certificat reçu du demandeur (dans ce cas, il s'agit de test1, test2 ou test3). La comparaison binaire est également activée. Cela oblige ACS à obtenir le certificat utilisateur d'AD et à le comparer au même certificat reçu par le demandeur. Si elle ne correspond pas, l'authentification échoue.

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

2. Configurez les séquences du magasin d'identités, qui utilise AD pour l'authentification basée sur les certificats avec le profil de certificat.

My Workspace	Users and Identity Stores > Identity Store Sequences > Edit: "seq"
Interview Resources	General
🔹 🎒 Users and Identity Stores	o Name: seq
Identity Groups Internal Identity Stores Users Hosts External Identity Stores LDAP Active Directory RSA SecurID Token Servers RADIUS Identity Servers Certificate Authorities Certificate Authorities Identity Store Sequences	Description: Authentication Method List Certificate Authentication Profile 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 Users AD1
System Administration	Advanced Options • Required fields

Il est utilisé comme source d'identité dans la stratégie d'identité 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						
Access Services Service Selection Rules						
O Default Device Admin						
Identity Authorization						
 O Default Network Access 						
Identity						
✓ Max User Session Policy						
Max Session User Settings						
Max Session Group Settings						
System Administration						
v vo oyatem Auministration						

3. Configurez deux stratégies d'autorisation. La première stratégie est utilisée pour test1 et refuse l'accès à cet utilisateur. La deuxième stratégie est utilisée pour le test 2 et autorise l'accès avec le profil

VLANZ.											
My Workspace	Access #	ance Relatives & Accesses Services a Default Melowerk Accesses & Aufhontention									
Network Resources	Standa	ndard Policy Exception Policy									
🔹 🚜 Users and Identity Stores	Netwo	fwerk Scress Sutherization Policy									
Policy Elements	E Martin										
- 🛼 Access Policies	P Der	3120	us	▼ Matchit Et	juais 👻 En	anieo 👻	Clear Filter Go 🕈				
 Access Services Service Selection Rules 			Status	Name	NDB(Location	Time And Date	Conditions Compound Condition	Results Authorization Profiles	Hit Count		
👻 😑 Default Device Admin	5		Θ	<u>ONtesti</u>	ANY	-ANY	Certificate Dictionary:Common Name equals test1	DenyAccess	6		
Identity Automation	8			CNtes:2	-ANY-	-ANS	Certificate Dictionary:Common Name equals test2	vtan2	7		
O Default Network Access Identity											
Authorization											
 Was User Session Policy 											
Wax Session Group Settings											
S Nonitoring and Reports											
🕨 🍕 System Administration											

VLAN2 est le profil d'autorisation qui renvoie les attributs RADIUS qui lient l'utilisateur à VLAN2 sur le commutateur.

🕨 🚭 My Workspace	Policy Elements > Authorization and Permissions > Network Access > Authorization Profiles > Edit "
Interview Resources	
B Users and Identity Stores	General Common Tasks RADIUS Attributes
👻 🎭 Policy Elements	Downloadable ACL Name: Not in Use 💌
 Session Conditions Date and Time Custom Network Conditions End Station Filters Device Filters Device Port Filters Authorization and Permissions Network Access Authorization Profiles Device Administration Shell Profiles Command Sets Named Permission Objects 	Filter-ID ACL: Not in Use Proxy ACL: Not in Use Voice VLAN Permission to Join: Not in Use VLAN VLAN VLAN ID/Name: Static Value Reauthentication Reauthentication Timer: Not in Use Maintain Connectivity during Reauthentication: QOS Input Policy Map: Not in Use
Access Policies	802.1X-REV
Monitoring and Reports System Administration	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
	w - Nednied lielus

4. Installez le certificat CA sur

ACS.							
🕨 😚 My Workspace	Users and	d Identity Stores > (Certificate	Authorities			
Network Resources	Certifi	icate Authorities					
🔹 🎳 Users and Identity Stores	Filter		💌 Ma	🐨 Go 🔻	⊽		
Identity Groups Internal Identity Stores		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 SecurID Token Servers							
RADIUS Identity Servers							
Certificate Authentication Profile							
Identity Store Sequences							

5. Générez et installez le certificat (pour l'utilisation du protocole d'authentification extensible) signé par l'autorité de certification Cisco pour ACS.

→ 🔗 MyWorkspace	System	Administration > Conf	iguratio	n > Local Server Ce	Hificates > Local Ce	ertific	cates			
By Network Resources	Loca	I Certificates								
Busers and Identity Stores	Fifte	r.		Match if:	[*]	Gr				
Policy Elements										
Access Policies		Friendly Name	-	Issued to	Issued By		valid From	valid to (Expiration)		Protocol
Image: Monitoring and Reports	븜	<u>acso4</u>		acs::4	DAG		09:23 22.02.2013	13:23 22:02:2014		EAP, Management Interface
System Administration Aumoreation Aumoreation Users Authentication Settings Max User Session Slobal 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-TLS Settings EAP-TLS Settings EAP-TLS Settings EAP-TLS Settings EAP-TLS Settings EAP-TLS Settings Settings Settings Settings Settings Settings Settings		<u>acs54</u>		acs64	acs54		17:21 18.02.2013	17:21 19.05.2013	,	N/A

Vérification

Il est recommandé de désactiver le service 802.1x natif sur le demandeur Windows 7, car AnyConnect NAM est utilisé. Avec le profil configuré, le client est autorisé à sélectionner un certificat spécifique.

Cisco AnyConnect		
Choose certificate for the connection my configured	Cisco AnyConnect Secure Mobility Client	
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: FE9C3D6 1E 131CDB3	Network: Authenticating	
OK Cancel	my configured 802.1x profile	& → ≔
	\$ (i)	ាត្រាត cisco

Lorsque le certificat test2 est utilisé, le commutateur reçoit une réponse de réussite ainsi que les attributs 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=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: COA80A0A00000001000215F0
     Acct Session ID: 0x0000005
          Handle: 0xE8000002
Runnable methods list:
```

Method State dot1x Authc Succes

Notez que le VLAN 2 a été attribué. Il est possible d'ajouter d'autres attributs RADIUS à ce profil d'autorisation sur ACS (tels que la liste de contrôle d'accès avancée ou les temporisateurs de réautorisation).

Les journaux sur ACS sont les suivants :

I	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>	ing Group Mapping Policy
	12506	EAP-TLS authentication succeeded
	11503	Prepared EAP-Success
	<u>Evaluat</u>	ing 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

Dépannage

Paramètres d'heure non valides sur ACS

Erreur possible - Erreur interne dans 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.

Aucun certificat configuré et lié sur le contrôleur de domaine Active Directory

Erreur possible - échec de la récupération du certificat utilisateur à partir d'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
Evaluat	ing 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

Personnalisation du profil NAM

Dans les réseaux d'entreprise, est-il conseillé de s'authentifier à l'aide de certificats d'ordinateur et d'utilisateur.Dans un tel scénario, il est conseillé d'utiliser le mode 802.1x ouvert sur le commutateur avec un VLAN restreint. Lors du redémarrage de l'ordinateur pour 802.1x, la première session d'authentification est lancée et authentifiée à l'aide du certificat de l'ordinateur AD. Ensuite, une fois que l'utilisateur fournit des informations d'identification et se connecte au domaine, la deuxième session d'authentification est lancée avec le certificat utilisateur. L'utilisateur est placé dans le VLAN correct (approuvé) avec un accès réseau complet. Il est bien intégré sur ISE (Identity Services Engine).

🐴 AnyConnect Profile Editor - I	Network Access Manager	- • ×
File Help		
File Help Network Access Manager Clent Policy Authentication Policy Networks Network Groups	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 connection will make the network available after the user has logged on. Machine and User Connections	Media Type Security Leve Connection Ty Machine Auth Credentials User Auth Credentials
	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.	

Ensuite, il est possible de configurer des authentifications distinctes à partir des onglets Authentification de l'ordinateur et Authentification de l'utilisateur.

Si le mode 802.1x ouvert n'est pas acceptable sur le commutateur, il est possible d'utiliser le mode 802.1x avant que la fonctionnalité de connexion ne soit configurée dans la stratégie client.

Informations connexes

- Guide de l'utilisateur de Cisco Secure Access Control System 5.3
- Guide de l'administrateur du client Cisco AnyConnect Secure Mobility, version 3.0
- <u>AnyConnect Secure Mobility Client 3.0 : Gestionnaire d'accès réseau et Éditeur de profil sous</u>
 <u>Windows</u>
- Support et documentation techniques Cisco Systems