نم ةيئانث تاداهش ةنراقم عم 802.1x EAP-TLS و AD تافيصوت نيوكت لاثم

المحتويات

<u>المقدمة</u> المتطلبات الأساسية المتطلبات المكونات المستخدمة الاصطلاحات التكوين طوبولوجيا تفاصيل المخطط إنبجاسا تكوين المبدّل تجهيز الشهادة تكوين وحدة التحكم بالمجال تكوين الطالب تكوين ACS التحقق من الصحة استكشاف الأخطاء وإصلاحها اعدادات الوقت غير صالحة على ACS <u>لم يتم تكوين أية شهادة وتثبيتها على AD DC</u> تخصيص ملف تعريف NAM معلومات ذات صلة

المقدمة

يصف هذا المستند تكوين EAP-TLS مع بروتوكول المصادقة المتوسع - أمان طبقة النقل (EAP-TLS) ونظام التحكم في الوصول (ACS) بينما يجريان مقارنة شهادات ثنائية بين شهادة عميل مقدمة من صاحب الطلب ونفس الشهادة محفوظة في Microsoft Active Directory (AD). يتم إستخدام ملف تعريف AnyConnect Network Access (Manager (NAM) للتخصيص. يتم تقديم التكوين لجميع المكونات في هذا المستند، بالإضافة إلى سيناريوهات أستكشاف أخطاء التكوين وإصلاحها.

المتطلبات الأساسية

المتطلبات

لا توجد متطلبات خاصة لهذا المستند.

المكونات المستخدمة

لا يقتصر هذا المستند على إصدارات برامج ومكونات مادية معينة.

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك مباشرة، فتأكد من فهمك للتأثير المحتمل لأي أمر.

الاصطلاحات

راجع <u>اصطلاحات تلميحات Cisco التقنية للحصول على مزيد من المعلومات حول اصطلاحات المستندات.</u>

التكوين

طوبولوجيا

- طالب Cisco AnyConnect Secure Mobility Client مع 802.1x Windows 7 الإصدار 0.01065 (وحدة (NAM
 - مصدق 802.1x محول 2960
 - خادم مصادقة 802.1x ACS، الإصدار 5.4
 - ACS مدمج مع Microsoft AD وحدة التحكم بالمجال Microsoft AD

تفاصيل المخطط

- ACS 192.168.10.152 •
- E0/0) 192.168.10.10 2960
 - DC 192.168.10.101 •
 - نظام التشغيل Windows 7 بروتوكول DHCP

إنبجاسا

تحتوي محطة Windows 7 على AnyConnect NAM مثبت، والذي يتم إستخدامه كمطلب للمصادقة على خادم ACS باستخدام طريقة EAP-TLS. يعمل المحول المزود ب 802.1x كمصدق. يتم التحقق من شهادة المستخدم بواسطة ACS ويقوم تفويض النهج بتطبيق السياسات المستندة إلى الاسم الشائع (CN) من الشهادة. وبالإضافة إلى ذلك يجلب ACS شهادة المستخدم من AD ويعقد مقارنة ثنائية مع الشهادة المقدمة من الملتمس.

تكوين المبدّل

المفتاح يتلقى تشكيل أساسي. افتراضيا، الميناء في عزل VLAN 666. أن VLAN له وصول مقيد. بعد تخويل المستخدم، تتم إعادة تكوين شبكة VLAN الخاصة بالمنفذ.

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

تجهيز الشهادة

يشترط في EAP-TLS أن تكون هناك شهادة للمطالب وخادم المصادقة. يعتمد هذا المثال على الشهادات التي تم إنشاؤها ل OpenSSL. يمكن إستخدام المرجع المصدق (CA) من Microsoft لتبسيط عملية النشر في شبكات المؤسسات.

> .1. دخلت in order to خلقت ال CA، هذا أمر: 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

يتم الاحتفاظ بشهادة CA في ملف ca.crt والمفتاح الخاص (وغير المحمي) في ملف ca.key.

2. قم بإنشاء ثلاث شهادات مستخدم وشهادة ل ACS، جميعها موقعة من قبل :CA ICN=test1CN=test2CN=test3cn=acs54برنامج النصي لإنشاء شهادة واحدة موقعة من قبل CA من

Cisco هو:

openssl genrsa -des3 -out server.key 1024 openssl req -new -key server.key -out server.csr

cp 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 365openssl pkcs12 -export -out server.pfx -inkey server.key -in server.crt certfile ca.crt-

المفتاح الخاص موجود في ملف server.key والشهادة موجودة في ملف server.crt. ال pkcs12 صيغة في ال server.pfx مبرد.

انقر نقرا مزدوجا على كل شهادة (.pfx file) لاستيرادها إلى وحدة التحكم بالمجال. في وحدة التحكم بالمجال*3،* يجب الوثوق بجميع الشهادات الثلاثة.

📅 certmgr - [Certificates - Current	User\Personal\Certificat		4		
File Action View Help					
🗢 ə> 🖄 🔐 🔏 🔀 🗒	1 🔒 🛛 🖬			Lertificate X	S
Certificates - Current User Certificates Certificates Certificates Certification Autho Certification Autho	Issued To A Administrator TAC test1 test2 test3	Issued E Administ TAC TAC TAC TAC	ly rator	Certification path	
Active Directory User Object Active Directory User Object Tursted Publishers One Untrusted Certificates Third-Party Root Certification Au One Trusted People One Certificate Enrolment Requests One Smart Card Trusted Roots					
				Vew Certificate	-
				Certificate status:	
	<u> </u>			This certificate is OK.	
💫 Add rolea		Roles:	Active Direc	Learn more about certification paths	
🚑 Add features		Features:	Group Polic	ОК	ci

يمكن اتباع نفس العملية في نظام التشغيل Windows 7 (الملحق) أو إستخدام خدمة Active Directory للضغط على شهادات المستخدم.

تكوين وحدة التحكم بالمجال

من الضروري تعيين الشهادة المحددة للمستخدم المحدد في AD.

- 1. من Active Directory Users and Computers، انتقل إلى مجلد Users.
 - 2. من قائمة عرض، أختر **ميزات متقدمة**.

Active Directory Users and Computers	
File Action View Help	
(=) Add/Remove Columns	7 🗾 🕱
Active Direc Large Icons	Description
Saved (Small Icons	Wbudowane konto do ad
E page asco-te List	Wyznaczeni administrator
E Detail	 Wyznaczeni administrator
Users, Contacts, Groups, and Computers as containers	Wyznaczeni administrator
E G For Advanced Features	Grupa administratorów DNS
E C Los Filter Options	. Klienci DNS, którzy są upo
E Pro	 Wszyscy goście domeny
E Customize	Wbudowane konto do dos
Users & Grupa bez re Security Group	Członkowie tej grupy nie
🕀 📫 NTDS Quotas 🦉 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 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. إضافة هؤلاء المستخدمين: الاختبار 1إختبار 2إختبار 3**ملاحظة**: كلمة المرور غير مهمة.
- 4. من نافذة الخصائص، أختر علامة التبويب **الشهادات المنشورة**. أختر الشهادة المحددة للاختبار. على سبيل المثال، للاختبار 1 يكون المستخدم CN هو test1.**ملاحظة**: لا تستخدم تعيين الاسم (انقر بزر الماوس الأيمن فوق اسم المستخدم). يتم إستخدامه لخدمات

						محتلفة.
🔁 Active Directory Users and Com	puters		test2 Propert	ies		<u>গ</u> ×
File Action View Help			Security	Environment	Sessions	Remote control
🗢 🔿 🖄 🛅 🖌 🛽	2 🙆 🗟 🛛 📅 🗏 🎗	2 🗄 🍸 💆 🕱 👘	General	Address Profile	COM+ Profile Tolon	Attribute Editor
Active Directory Users and Comput Saved Queries Computers Compu	Name Type Administrator User Administrator Security () BonsAdmins Security () Goscie domeny Security () Grupa terpi Security () Grupa terpi Security () Kontrolery d Security () Itati User Serwery RAS Security () List1 User List2 User List2 User List2 User List2 Security () List2 Security () List2 User List3 Security () List4 User <	Description Woudowane k Wyznaczeni a Wyznaczeni a roup … Wyznaczeni a roup … Wyznaczeni a roup … Wyznaczeni a roup … Klienci DNS, kł roup … Klienci DNS, kł roup … Członkowie te roup … Członkowie te roup … Elementy czło roup … Elementy czło roup … Serwery w gru roup … Członkowie te roup … Członkowie te	General Published Ce List of X509 Issued To altest2	Address Account trificates Member Of certificates published fo Issued By TAC	Profile Telep Password Replic r the user account Intended Purpo Server Authent	hones Organization ation Dial-in Object ses Expiration ication 2014-03-
I F						
				OK (Cancel A	pply Help

في هذه المرحلة، يتم ربط الشهادة بمستخدم معين في AD. يمكن التحقق من هذا باستخدام Idapsearch:

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

فيما يلي نتائج المثال للاختبار 2:

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

.

userCertificate:: MIICuDCCAiGgAwIBAgIJAP6cPWHhMc2yMA0GCSqGSIb3DQEBBQUAMFYxCzAJ BgNVBAYTA1BMMQwwCgYDVQQIDANNYXoxDzANBgNVBAcMB1dhcnNhdzEMMAoGA1UECgwDVEFDMQwwC gYDVQQLDANSQUMxDDAKBgNVBAMMA1RBQzAeFw0xMzAzMDYxMjUzMjdaFw0xNDAzMDYxMjUzMjdaMF oxCzAJBgNVBAYTA1BMMQswCQYDVQQIDAJQTDEPMA0GA1UEBwwGS3Jha293MQ4wDAYDVQQKDAVDaXN jbzENMAsGA1UECwwEQ29yZTEOMAwGA1UEAwwFdGVzdDIwgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJ AoGBAMFQZywrGTQKL+LeI19ovNavCFSG2zt2HGs8qGPrf/h3o4IIvU+nN6aZPdkTdsjiuCeav8HYD aRznaK1LURt1PeGtH1cTgcGZ1MwIGptimzG+h234GmPU59k4XSVQixARCDpMH8IBR9zOSWQLXe+kR iZpXC444eKOh6wO/+yWb4bAgMBAAGjgYkwgYYwCwYDVR0PBAQDAgTwMHcGA1UdJQRwMG4GCCsGAQU FBwMBBggrBgEFBQcDAgYKKwYBBAGCNwoDBAYLKwYBBAGCNwoDBAEGCCsGAQUFBwMBBggrBgEFBQgC FQYKKwYBBAGCNwoDAQYKKwYBBAGCNxQCAQYJKwYBBAGCNxUGBggrBgEFBQcDAjANBgkqhkiG9w0BA QUFAAOBgQCuXwAgcYqLNm6gEDTWm/OWmTFjPyA5KSDB76yVqZwr11ch7eZiNSmctH7Pn+VILagf9o tiF15ttk9KX6tIvbeEC4X/mQVgAB3HuJH5sL1n/k2H10XCXKfMqMGrtsZrA64tMCcCceZRoxfAO94n ==PulwF4nkcnu1x0/B7x+LpcjxjhQ

تكوين الطالب

- 1. قم بتثبيت محرر ملف التعريف هذا، AnyConnect-profileeditor-win-3.1.00495-k9.exe.
 - 2. افتح محرر ملف تعريف مدير الوصول إلى الشبكة وقم بتكوين ملف التعريف المحدد.
 - 3. إنشاء شبكة سلكية معينة.

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

من المهم جدا في هذه المرحلة إعطاء المستخدم خيار إستخدام الشهادة في كل مصادقة. لا تقم بتخزين هذا الخيار مؤقتا. أستخدم أيضا "اسم المستخدم" كمعرف غير محمي. من المهم تذكر أنه ليس نفس المعرف الذي يستخدمه ACS للاستعلام عن AD للشهادة. سيتم تكوين هذا المعرف في ACS.

かる Networks 深た Network Groups	User Identity	Media Type Security Leve Connection Ty User Auth	
	User Credentials Use Single Sign On Credentials Prompt for Credentials Remember Forever Remember while User is I Never Remember	(Requires Smart Card) Logged On	Crevenuals
	Certificate Sources	Remember Smart Card Pin	
	 Smart Card or OS certificates Smart Card certificates only 	 Remember Forever Remember while User is Logged On Never Remember 	

- 4. احفظ ملف .xml ك xml دادنا xml .Access Manager\system\configuration.xml
 - 5. قم بإعادة تشغيل خدمة AnyConnect NAM من Cisco.

يوضح هذا المثال عملية نشر ملفات التعريف اليدوية. يمكن إستخدام AD لنشر هذا الملف لكافة المستخدمين. كما يمكن إستخدام ASA لتوفير ملف التعريف عند دمجه مع شبكات VPN.

تکوین ACS

1. انضم إلى مجال ¤D

					.AD						
» ⊕ MsWorkspace	Users and identity Stores > External	Identity Stores > Active Directory									
 Istwork Resources 											
- 🗿 Users and Identity Stores	General Directory Groups Directory Athibutes Nathine Access Restitutions Cennectien Botalis										
Identity Groups											
 Internal Identity Stores Users 	Node Node	Nade Role	Status	Domain Name	Domain Controller Name						
Hosts	acs54	Primary	Joined and Connected	cisco-test.com	win-grag7b#time.cisco-test.com						
 External Identity Stores LDAP 	Join/Test Connection	Leave	•								
Adde Directory RSA SecuriD Token Sensers RADIUS Identity Servers	Click on Sawe Changes' to save AD configuration. Dirce you have successfully connected to the Domain, you can select Directory Dirupts and Directory Athlobas to be evaluated in trues in policy rules. Processing on Chan Configuration will simply advantate and enzymove ACS matching from the Domain.										
Certificate Authorities	End User Authentication Se	ttings									
Certificate Authentication Profile	Enable password the	inge									
Identity Store Sequences	Enable machine auth	entication									
 Policy Elements 											
Access Policies	Evable railback then	k for distant classic									
Signature State	• = Required fields										
Bystem Administration											

يطابق ACS أسماء مستخدمي AD دون إستخدام حقل CN من الشهادة المستلمة من المتلقي (في هذه الحالة يكون test1، test2، أو test3). كما تم تمكين المقارنة الثنائية. وهذا يجبر ACS على الحصول على ا شهادة المستخدم من AD ومقارنتها مع نفس الشهادة التي يستلمها الملتمس. وإذا لم تتطابق تفشل المصادقة.

🕨 🞲 My Workspace	Users and Identity Stores > Certificate Authentication Profile > Edit "cert profile 2"
Book Resources Book Resources Book Resources Identity Groups	General O Name: Cert profile 2 Description:
Internal Identity Stores Users Hosts External Identity Stores LDAP Active Directory RSA SecurID Token Servers RADIUS Identity Servers Certificate Authorities Certificate Authentication Profile Identity Store Sequences	Certificate Definition Principal Username X509 Attribute: Common Name ✓ Perform Binary Certificate Comparison with Certificate retrieved from LDAP or Active Directory Name: AD1 Select o = Required fields
Specific Elements Access Policies Monitoring and Reports System Administration	

2. تشكيل تسلسلات مخزن الهويات الذي يستخدم AD للمصادقة المستندة إلى شهادة مع توصيف الشهادة.

My Workspace	Users and identity Stores > identity Store Sequences > Edit: "seq"
In the second	Ganaral
🔹 🎒 Users and Identity Stores	o Name: Iseq
Identity Groups Internal Identity Stores Users Hosts External Identity Stores LDAP Active Directory RSA SecurID Token Servers RADIUS Identity Servers Certificate Authorities Certificate Authentication Profile Identity Store Sequences	Description: Authentication Method List Certificate Authentication Profile Certificate Based 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 AD1
Policy Elements Access Policies	win2k3
Monitoring and Reports	>>> · · · · · · · · · · · · · · · · · ·
System Administration	Advanced Options

يستخدم هذا كمصدر هوية في نهج هوية 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 Operault Device Admin Identity Authorization Operault Network Access Identity Authorization Max User Session Policy Max Session User Settings Max Session Group Settings Monitoring and Reports 	
System Administration	

3. تكوين نهجي تفويض. يتم إستخدام النهج الأول للاختبار 1 ويرفض الوصول إلى ذلك المستخدم. يتم إستخدام السياسة الثانية للاختبار 2 وتسمح بالوصول مع ملف تعريف VLAN2.

My Workspace	Access	Proline ivers	» Access	Services > Detaut Melwork	Access > Authorite	ation						
Network Resources	Standa	ndard Policy Exception Policy										
Users and identity Stores	Made											
Police Flements	Netw	etwork Access Authorization Policy										
	Filto	r. Stat	us	▼ Match It Et	quais 🔻 Er	abled 💌	Clear Filter Go					
a process Policies		_					Conditions	Results				
Service Selection Pules			status	Marrie	NDG:Location	Time And Date	Compound Condition	Authorization Profiles	HICCOUNT			
👻 \Theta Default Device Admin	5			<u>CNtesti</u>	ANY	-ANY	Certificate Dictionary:Common Name equals test1	DenyAccess	6			
Identity	8			CNtest2	-ANY	-ANS	Certificate Dictionary:Common Name equals test2	vtan2	7			
Authonization												
V C Listadi, New OKACLASS												
Autorization												
 Nas User Session Policy 												
Wax Session User Settings												
Wax Bession Group Settings												
Nonitoring and Reports												
🕨 🎭 System Administration												

VLAN2 هو ملف تعريف التخويل الذي يرجع سمات RADIUS التي تربط المستخدم بشبكة VLAN2 على المحول.

My Workspace	Policy Elements > Authorization and Permissions > Network Access > Authorization Profiles > Edit: "
Network Resources	
B Users and Identity Stores	General Common Tasks RADIUS Attributes
- Delicy Flements	ACLS
- Ression Conditions	Downloadable ACL Name: Not In Ose
Date and Time	Filter-ID ACL: Not in Use
Custom	Proxy ACL: Not in Use 🔽
 Network Conditions 	Voice VLAN
End Station Filters	Permission to Join: Not in Use 🔽
Device Filters	VLAN
Device Port Filters	VLAN ID/Name: Static 🔽 🔅 Value 2
 Authorization and Permissions 	Reauthentication
Network Access Authorization Profiles	Reauthentication Timer: Not in Use 💌
 Device Administration 	Maintain Connectivity during
Shell Profiles	Reauthentication:
Command Sets	QOS
 Named Permission Objects 	Input Policy Map: Not in Use 🔻
Downloadable ACLs	Output Policy Map: Not in Use 🔽
Access Policies	802.1X-REV
Monitoring and Reports	LinkSec Security Policy: Not in Use
	URL Redirect
System Administration	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
	o = Required fields

4. قم بتثبيت شهادة المرجع المصدق على ACS

							./\00
🔸 💮 My Workspace	Users and	Identity Stores > (Certificate	Authorities			
Interview Resources	Certifi	cate Authorities					
🔹 🎒 Users and Identity Stores	Filter	-	💌 Ma	tch if:	[▼ _ Go ▼		
Identity Groups							
		Friendly Name	*	Expiration	Issued To	Issued By	Description
Users		TAC		08:11 16.11.2013	TAC	TAC	
Hosts	-						
 External Identity Stores 							
LDAP							
Active Directory							
RSA SecurID Token Servers							
RADIUS Identity Servers							
Certificate Authorities							
Certificate Authentication Profile							
Identity Store Sequences							

5. قم بإنشاء الشهادة وتثبيتها (لاستخدام بروتوكول المصادقة المتوسع) الموقعة من قبل المرجع المصدق (CA) من Cisco ل ACS.

> 🔗 MyWorkspace	System /	Voluministration > Config	uratio	n > Local Server Cert	ficates > Local Certi	ficates			
By Network Resources	Local Certificates								
Busers and Identity Stores	Fifter			Match it		30 🛛 👻			
Policy Elements									Restored.
Access Policies		Friendly Name	*	Issued to	Issued By	Valid From		valid to (Expiration)	Protocol
Southering and Reports		acs54		acso4	DAC:	09:23 22:02	.2013	09:23 22:02:2014	EAP, Management Interface
 System Administration Authorization Users Authorization Settings Max User Session Global Settings Purge User Sessions Operations Distributed System Management Software Repositories Scheduled Backups Local Operations Global System Options TACACS+ Settings EAP-FAST Satings EAP-FAST Satings Dictionaries Protocols Identity Local Server Certificates Local Server Certificates Outstanding Signing Requests 		<u>acs54</u>		acs54	acs54	17:21 18:02	.2013	17:21 19.05.2013	N/A

التحقق من الصحة

من الممارسات الجيدة تعطيل الخدمة الأصلية بمعيار 802.1x على عميل Windows 7 نظرا لاستخدام AnyConnect NAM. مع التوصيف الذي تم تكوينه، يسمح للعميل بتحديد شهادة معينة.

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	nect
Expiration Date: 2014-03-06 12:54:24 UTC		
Serial Number: FE9C3D61E131CDB3	Network: Authenticating	
OK Cancel		
	‡ ()	cisco

عند إستخدام شهادة Test2، يتلقى المحول إستجابة نجاح مع خصائص RADIUS.

DOT1X-5-SUCCESS: Authentication successful for client% :00:02:51 0800.277f.5f64) on Interface Et0/0) 'AUTHMGR-7-RESULT: Authentication result 'success' from 'dot1x% :00:02:51 for client (0800.277f.5f64) on Interface Et0/0 #switch |EPM-6-POLICY_REQ: IP=0.0.0.0| MAC=0800.277f.5f64% :00:02:51 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

لاحظ أنه قد تم تعيين شبكة VLAN رقم 2. من الممكن إضافة سمات RADIUS أخرى إلى ملف تعريف التخويل هذا على ACS (مثل قائمة التحكم بالوصول المتقدم أو مؤقتات إعادة التخويل).

السجلات على ACS هي كما يلي:

Authc Succes

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

استكشاف الأخطاء وإصلاحها

إعدادات الوقت غير صالحة على ACS

خطأ محتمل - خطأ داخلي في 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.

لم يتم تكوين أية شهادة وتثبيتها على AD DC

خطأ محتمل - فشل إسترداد شهادة المستخدم من 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

تخصيص ملف تعريف NAM

في شبكات المؤسسة، من المستحسن المصادقة باستخدام شهادات الجهاز والمستخدم على حد سواء.في مثل هذا السيناريو، ينصح باستخدام وضع 802.1x المفتوح على المحول مع شبكة VLAN المقيدة. عند إعادة تمهيد الجهاز ل 802.1x، تبدأ جلسة المصادقة الأولى وتتم مصادقتها باستخدام شهادة جهاز AD. بعد ذلك، وبعد أن يوفر المستخدم بيانات الاعتماد والسجلات إلى المجال، يتم بدء جلسة عمل المصادقة الثانية بشهادة المستخدم. وضع المستخدم في شبكة VLAN الصحيحة (الموثوق بها) مع الوصول الكامل إلى الشبكة. وهو مدمج بشكل رائع في محرك خدمات الهوية (ISE).

AnyConnect Profile Editor - N	Vetwork Access Manager	- • •
File Help		
File Help Network Access Manager Client 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	Media Type Security Leve Connection Ty Machine Auth Credentials User Auth Credentials
	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 Connection 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.	

وبعد ذلك، من الممكن تكوين مصادقة منفصلة من علامات تبويب مصادقة الجهاز ومصادقة المستخدم.

إذا لم يكن وضع 802.1x المفتوح مقبولا على المحول، فمن الممكن إستخدام وضع 802.1x قبل تكوين ميزة تسجيل الدخول في نهج العميل.

معلومات ذات صلة

- <u>دليل المستخدم لنظام التحكم بالوصول الآمن من Cisco 5.3</u>
- دليل مسؤول Cisco AnyConnect Secure Mobility Client، الإصدار 3.0
- AnyConnect Secure Mobility Client 3.0: مدير الوصول إلى الشبكة ومحرر ملف التعريف على Windows
 - الدعم التقني والمستندات Cisco Systems

ةمجرتاا مذه لوح

تمجرت Cisco تايان تايانق تال نم قعومجم مادختساب دنتسمل اذه Cisco تمجرت ملاعل العامي عيمج يف نيم دختسمل لمعد يوتحم ميدقت لقيرشبل و امك ققيقد نوكت نل قيل قمجرت لضفاً نأ قظعالم يجرُي .قصاخل امهتغلب Cisco ياخت .فرتحم مجرتم اممدقي يتل القيفارت عال قمجرت اعم ل احل اوه يل إ أم اد عوجرل اب يصوُتو تامجرت الاذة ققد نع اهتي لوئسم Systems الما يا إ أم الا عنه يل الان الانتيام الال الانتيال الانت الما