Konfigurationsbeispiel für 802.1x-EAP-TLS mit binärem Zertifikatsvergleich aus AD- und NAM-Profilen

Inhalt

Einführung Voraussetzungen Anforderungen Verwendete Komponenten Konventionen Konfigurieren Topologie **Topologiedetails** Fluss Switch-Konfiguration Zertifikatvorbereitung Domänencontrollerkonfiguration Supplicant-Konfiguration **ACS-Konfiguration** Überprüfen Fehlerbehebung Ungültige Zeiteinstellungen für ACS Kein Zertifikat konfiguriert und auf AD DC gebunden Anpassung des NAM-Profils Zugehörige Informationen

Einführung

In diesem Dokument wird die 802.1x-Konfiguration mit Extensible Authentication Protocol-Transport Layer Security (EAP-TLS) und Access Control System (ACS) beschrieben, da diese einen binären Zertifikatvergleich zwischen einem vom Supplicant bereitgestellten Clientzertifikat und demselben in Microsoft Active Directory (AD) aufbewahrten Zertifikat durchführen. Das AnyConnect Network Access Manager (NAM)-Profil wird zur Anpassung verwendet. Die Konfiguration für alle Komponenten wird in diesem Dokument zusammen mit Szenarien zur Fehlerbehebung bei der Konfiguration vorgestellt.

Voraussetzungen

Anforderungen

Für dieses Dokument bestehen keine speziellen Anforderungen.

Verwendete Komponenten

Dieses Dokument ist nicht auf bestimmte Software- und Hardwareversionen beschränkt.

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie in den <u>Cisco Technical Tips</u> <u>Conventions</u> (Technische Tipps zu Konventionen von Cisco).

Konfigurieren

Topologie

- 802.1x-Komponente Windows 7 mit Cisco AnyConnect Secure Mobility Client Release 3.1.01065 (NAM-Modul)
- 802.1x-Authentifizierer 2960-Switch
- 802.1x-Authentifizierungsserver ACS Version 5.4
- ACS integriert in Microsoft AD Domain Controller Windows 2008 Server

Topologiedetails

- ACS 192.168.10.152
- 2960 192.168.10.10 (e0/0 Komponente verbunden)
- Gleichstrom: 192.168.10.101
- Windows 7 DHCP

Fluss

Auf der Windows 7-Station ist AnyConnect NAM installiert, das als Komponente für die Authentifizierung am ACS-Server mithilfe der EAP-TLS-Methode verwendet wird. Der Switch mit 802.1x fungiert als Authentifizierer. Das Benutzerzertifikat wird vom ACS verifiziert, und die Richtlinienautorisierung wendet Richtlinien an, die auf dem Common Name (CN) des Zertifikats basieren. Darüber hinaus ruft der ACS das Benutzerzertifikat von AD ab und führt einen Binärvergleich mit dem vom Supplicant bereitgestellten Zertifikat durch.

Switch-Konfiguration

Der Switch verfügt über eine Basiskonfiguration. Standardmäßig befindet sich der Port im Quarantäne-VLAN 666. Dieses VLAN hat einen eingeschränkten Zugriff. Nachdem der Benutzer autorisiert wurde, wird das Port-VLAN neu konfiguriert.

aaa authentication login default group radius local aaa authentication dotlx default group radius aaa authorization network default group radius dotlx 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

Zertifikatvorbereitung

Für EAP-TLS ist sowohl für den Supplicant als auch für den Authentifizierungsserver ein Zertifikat erforderlich. Dieses Beispiel basiert auf von OpenSSL generierten Zertifikaten. Microsoft Certificate Authority (CA) kann zur Vereinfachung der Bereitstellung in Enterprise-Netzwerken eingesetzt werden.

- Geben Sie zum Generieren der CA die folgenden Befehle ein:

 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

 Das CA-Zertifikat wird in der Datei ca.crt und der private (und ungeschützte) Schlüssel in der Datei ca.key gespeichert.
- Erstellen Sie drei Benutzerzertifikate und ein Zertifikat f
 ür ACS, die alle von dieser Zertifizierungsstelle signiert werden: CN=Test1CN=Test2CN=Test3CN=ACS54Das Skript zum Generieren eines einzelnen Zertifikats, das von der Cisco Zertifizierungsstelle signiert wird, lautet:

```
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
```

Der private Schlüssel befindet sich in der Datei server.key und das Zertifikat in der Datei server.crt. Die Version pkcs12 befindet sich in der Datei server.pfx.

3. Doppelklicken Sie auf jedes Zertifikat (PFX-Datei), um es in den Domänencontroller zu importieren. Im Domain Controller sollten alle drei Zertifikate vertrauenswürdig sein.

certmgr - [Certificates - Current	User\Personal\Certificate:	5]			
				ertificate	Jhv
Certificates - Current User Personal Certificates Certificate Enrolment Requests Certificate Roots	Issued To A Administrator TAC Tac Test1 Lest2 Lest3	Issued By Administrator TAC TAC TAC TAC		General Details Certification Path	
				Certificate status:	
	4			This certificate is OK.	
Add roles		Roles:	Active Direc	Learn more about certification paths	
Add features		Features:	Group Polic	ОК	101

Derselbe Prozess kann in Windows 7 (Supplicant) ausgeführt werden oder mithilfe von Active Directory die Benutzerzertifikate übertragen werden.

Domänencontrollerkonfiguration

Das spezifische Zertifikat muss dem jeweiligen Benutzer in AD zugeordnet werden.

- 1. Navigieren Sie von Active Directory-Benutzern und -Computern zum Ordner Benutzer.
- 2. Wählen Sie im Menü Ansicht die Option Erweiterte Funktionen aus.

Active Directory Users and Computers	
File Action View Help	
(new line and line an	7 🔁 🔽
Active Direc Large Icons	Description
Saved (Small Icons	Wbudowane konto do ad
🖃 🙀 cisco-te List	. Wyznaczeni administrator
🗄 🛄 🕒 Detail	. Wyznaczeni administrator
Con Users, Contacts, Groups, and Computers as containers	. Wyznaczeni administrator
Don Advanced Features	Grupa administratorów DNS
	. Klienci DNS, którzy są upo
	Wszyscy goście domeny
E Customize	Wbudowane konto do dos
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
Servery RAS Security Group	Serwery w grupie mogą z
👗 test 1 User	
👗 test2 User	
Security Group	Członkowie tej grupy mog
Buzytkownicy Security Group	Wszyscy użytkownicy do
👫 Wydawcy ce Security Group	Członkowie tej grupy maj

- 3. Fügen Sie diese Benutzer hinzu: Test1Test2Test3Hinweis: Das Kennwort ist nicht wichtig.
- 4. Wählen Sie im Eigenschaftenfenster die Registerkarte Veröffentlichte Zertifikate aus. Wählen Sie das spezifische Zertifikat für den Test aus. Für Test1 ist die Benutzer-CN beispielsweise test1. Hinweis: Verwenden Sie keine Namenszuordnung (klicken Sie mit der rechten Maustaste auf den Benutzernamen). Es wird für verschiedene Services verwendet.

🧧 Active Directory Users and Con	nputers			test2 Prope	rties					?×
Active Directory Users and Con File Action View Help Image: Sevent Queries Image: Sevent Queries Image: Sevent Queries Image: Sevent Queries Image: Sevent Queries Image: Sevent Queries Image: Sevent Queries Image: Sevent Queries Image: Sevent Queries Image: Sevent Queries Image: Sevent Queries Image: Sevent Queries Image: Sevent Queries Image: Sevent Queries Image: Sevent Queries Image: Sevent Queries Image: Sevent Queries Image: Sevent Queries Image: Sevent Queries Image: Sevent Queries Image: Sevent Queries Image: Sevent Queries Image: Sevent Queries Image: Sevent Queries Image: Sevent Queries Image: Sevent Queries Image: Sevent Queries Image: Sevent Queries Image: Sevent Queries Image: Sevent Queries Image: Sevent Queries Image: Sevent Queries Image: Sevent Queries Image: Sevent Queries Image: Sevent Queries Image: Sevent Queries Image: Sevent Queries Image: Sevent Queries Image: Sevent Queries Image: Sevent Queries Image: Sevent Queries Image: Sevent Queries Image: Sevent Queries	Active Directory Users and Computers le Action View Help Image: Computers Image: Computers		Description Woudowane k Wyznaczeni ac Wyznaczeni ac Grupa adminisł Klienci DNS, kt Wszyscy gości Wbudowane k Członkowie tej Członkowie tej Wszystkie stac Wszystkie stac Wszystkie stac Wszystkie stac Wszystkie stac	Security Environment Sessions Remote control Terminal Services Profile COM+ Attribute Editor General Address Account Profile Telephones Organizal Published Certificates Member Of Password Replication Dial-in Ob List of X509 certificates published for the user account Issued To Issued By Intended Purposes Expiration Issued To Issued By Intended Purposes Expiration Image: TAC Server Authentication 2014-03					note control oute Editor Organizati Xal-In Obj Espiratior 2014-03-	Ŷ×
<u> </u>	Kontrolery d Kontrolery d Kontrolery d Sewery RAS Etest1 Twórcy-właś Użytkownicy Wydawcy ce	Security Group Security Group User User Security Group Security Group Security Group	Elementy człor Elementy człor Konto usługi ce Serwery w gru Członkowie tej Wszyscy użytk Członkowie tej	Add from	n Store	Add from File	Berrove	View De	rificate apy to Fie	

In dieser Phase wird das Zertifikat an einen bestimmten Benutzer in AD gebunden. Dies kann

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

Die Beispielergebnisse für Test2 sind wie folgt:

```
# 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==
```

Supplicant-Konfiguration

- 1. Installieren Sie diesen Profil-Editor anyconnect-profile editor-win-3.1.00495-k9.exe.
- 2. Öffnen Sie den Network Access Manager Profile Editor, und konfigurieren Sie das spezifische Profil.
- 3. Erstellen Sie ein bestimmtes kabelgebundenes Netzwerk.

Network Access Manager	Networks Profile: C:\1\prof1.xml								
Networks	Network			4					
and the second s	Name	Media Type	Group*						
	my configured 802	2.1x profile Wired	Local networks						
				Add					
				Edit					
				Delete					

In diesem Stadium ist es sehr wichtig, dem Benutzer die Möglichkeit zu geben, das Zertifikat bei jeder Authentifizierung zu verwenden. Diese Auswahl nicht zwischenspeichern. Verwenden Sie auch den 'username' als ungeschützte ID. Es ist wichtig zu beachten, dass es sich nicht um dieselbe ID handelt, die von ACS verwendet wird, um AD für das Zertifikat abzufragen. Diese ID wird im ACS konfiguriert.

Network Access Manager	Networks Profile: C:\1\prof1.xml								
Authentication Policy	User Identity Unprotected Identity Pattern: User Credentials O Use Single Sign On Credentials Prompt for Credentials Remember Forever	[username] (Requires Smart Card)	Media Type Security Leve Connection Ty User Auth Credentials						
	 Remember while User is I Never Remember Certificate Sources Smart Card or OS certificates 	Remember Smart Card Pin	1						
	Smart Card certificates only	Never Remember							

- 4. Speichern Sie die XML-Datei als c:\Users\All Users\Cisco\Cisco AnyConnect Secure Mobility Client\Network Access Manager\system\configuration.xml.
- 5. Starten Sie den Cisco AnyConnect NAM-Dienst neu.

Dieses Beispiel zeigte eine manuelle Profilbereitstellung. AD könnte verwendet werden, um diese Datei für alle Benutzer bereitzustellen. Bei der Integration in VPNs kann das Profil auch mithilfe der ASA bereitgestellt werden.

ACS-Konfiguration

1. Treten Sie der AD-Domäne

bei.									
 State 	bolispace Users and/Bentty Bores > External Identity Stores > Active Directory								
(1) Network Resources (1) Network Resources (1) Users and Identity Stores (1) Network Groups	General Directory Groups Directory Abdules Mathine Access Restrictions. Connection Datains								
 Internal Identity Stores Users 	Node	Nade Role	Status	Domain Name	Domain Controller Name				
Hosts	ace54	Primary	Joined and Connected	cisco-test.com	win-grag7bettmt.cisco-test.com				
Hosts arc54 Primary Joined and Connected cisco-test.com win-grag/Twitter.cisco LDAP									
> 🖏 System Administration	- respect to the top								

ACS ordnet AD-Benutzernamen der Verwendung des CN-Felds aus dem Zertifikat zu, das vom Supplicant empfangen wurde (in diesem Fall Test1, test2 oder test3). Der Binärvergleich ist ebenfalls aktiviert. Dadurch wird ACS gezwungen, das Benutzerzertifikat von AD zu erhalten und es mit dem gleichen Zertifikat zu vergleichen, das der Supplicant erhalten hat. Wenn sie nicht übereinstimmt, schlägt die Authentifizierung fehl.

🕨 😚 My Workspace	Users and Identity Stores > Certificate Authentication Profile > Edit: "cert profile 2"
Network Resources	General
Weers and Identity Stores Identity Groups Internal Identity Stores Users Hosts External Identity Stores LDAP Active Directory RSA SecurID Token Servers RADIUS Identity Servers	A Name: cert profile 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 o = Required fields
Certificate Authorities Certificate Authentication Profile Identity Store Sequences	
La Access Policies Monitoring and Reports	
System Administration	

2. Konfigurieren Sie die Identity Store-Sequenzen, die AD für die zertifikatsbasierte Authentifizierung zusammen mit dem Zertifikatprofil verwenden.

🔹 🥳 My Workspace	Users and identity Stores > identity Store Sequences > Edit: "seq"
Network Resources	Conoral
👻 🎒 Users and Identity Stores	o Name: Isea
Identity Groups	Description: Authentication Method List Certificate Authentication Profile 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 Internal Users NAC Profiler
Construction Access Policies Monitoring and Reports System Administration	
	Advanced Options a = Required fields

Dies wird als Identitätsquelle in der RADIUS-Identitätsrichtlinie verwendet.

🕨 😚 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 Pules	
O Default Device Admin	
Identity	
Authorization O Default Network Access	
Identity	
Authorization	
Max Session User Settings	
Max Session Group Settings	
Monitoring and Reports	
System Administration	

3. Konfigurieren Sie zwei Autorisierungsrichtlinien. Die erste Richtlinie wird für test1 verwendet und verweigert diesem Benutzer den Zugriff. Die zweite Richtlinie wird für Test 2 verwendet und ermöglicht den Zugriff mit dem VLAN2-

Profil.										
» 😚 Ny Workspace	Access	Philic ives	» Access	Services > Detaut Network	Access > Authorite	ation				
Network Resources	Standa	erd Pok	ev Excer	tion Policy						
Users and Identity Stores	Netw	And and a start of the start of								
Policy Elements	Eller	31:1	115	Watch P. E.	n els 🗐 Er	ahlad 🗐 🚽	Clear Elter Go 🔫			
🔹 🌉 Access Policies		- Steel		- Harris La	dents - m			B urnaha		
 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>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 Supported on 										
 Was User Session Policy Was Bession User Bettings Was Bession Group Settings 										
Nonitoring and Reports										
System Administration										

VLAN2 ist das Autorisierungsprofil, das RADIUS-Attribute zurückgibt, die den Benutzer an VLAN2 auf dem Switch binden.

🕨 💮 My Workspace	Policy Elements > Authorization and Permissions > Network Access > Authorization Profiles > Edit "V
Interview Resources	
Busers 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 	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 Reauthentication Reauthentication Timer:
 Device Administration Shell Profiles Command Sets Named Permission Objects Downloadable ACLs 	Maintain Connectivity during Reauthentication: QOS Input Policy Map: Not in Use 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 💌
	c = Required fields

4. Installieren Sie das Zertifizierungsstellenzertifikat auf dem

ACS.		-					
🕨 😚 My Workspace	Users an	d identity Stores > (Certificate	Authorities			
Interview Resources	Certif	icate Authorities					
🔹 🎒 Users and Identity Stores	Filter		💌 Ma	tch if:	🐨 Go 🔻		
Identity Groups Internal Identity Stores		Friendly Name	•	Expiration	Issued To	Issued By	Description
Users Hosts		TAC		08:11 16.11.2013	TAC	TAC	
Active Directory RSA SecuriD Token Servers							
RADIUS Identity Servers Certificate Authorities							
Certificate Authentication Profile Identity Store Sequences							

5. Generieren und Installieren des Zertifikats (für die Verwendung des Extensible Authentication Protocol), das von der Cisco CA für ACS signiert wurde.

> 🔗 MyWorkspace	System	Administration > Conf	guratio	n > Local Server Cer	tificates > Local O	ertific	sates		
By Network Resources	Loca	il Certificates							
Busers and Identity Stores	Fifte	r.		Match if:	[*]	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

Überprüfen

Es empfiehlt sich, den nativen 802.1x-Dienst auf der Windows 7-Komponente zu deaktivieren, da AnyConnect NAM verwendet wird. Mit dem konfigurierten Profil kann der Client ein bestimmtes Zertifikat auswählen.

+		
	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	Connect No Network Connectivity
	Expiration Date: 2014-03-06 12:54:24 UTC Serial Number: FE9C3D61E131CD83	Network: Authenticating
	OK Cancel	🔚 my configured 802.1x profile 🔌 👻 📰

Wenn das Test2-Zertifikat verwendet wird, erhält der Switch zusammen mit den RADIUS-Attributen eine Erfolgsantwort.

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
```

```
{\tt switch} \# {\tt 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

Beachten Sie, dass VLAN 2 zugewiesen wurde. Es ist möglich, diesem Autorisierungsprofil auf ACS weitere RADIUS-Attribute hinzuzufügen (z. B. eine erweiterte Zugriffskontrollliste oder Timer für die erneute Autorisierung).

Die Protokolle für den ACS sind wie folgt:

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>	ing Exception Authorization Policy
15042	No rule was matched
Evaluat	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

Fehlerbehebung

Ungültige Zeiteinstellungen für ACS

Möglicher Fehler - interner Fehler in 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.

Kein Zertifikat konfiguriert und auf AD DC gebunden

Möglicher Fehler - Abruf des Benutzerzertifikats von Active Directory fehlgeschlagen

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

Anpassung des NAM-Profils

In Enterprise-Netzwerken wird empfohlen, die Authentifizierung mithilfe von Computer- und Benutzerzertifikaten vorzunehmen. In einem solchen Szenario wird empfohlen, den offenen 802.1x-Modus auf dem Switch mit eingeschränktem VLAN zu verwenden. Beim Neustart des Computers für 802.1x wird die erste Authentifizierungssitzung initiiert und mithilfe des Zertifikats des AD-Systems authentifiziert. Nachdem der Benutzer Anmeldeinformationen bereitgestellt und sich bei der Domäne angemeldet hat, wird die zweite Authentifizierungssitzung mit dem Benutzerzertifikat initiiert. Der Benutzer wird in das richtige (vertrauenswürdige) VLAN mit vollständigem Netzwerkzugriff gesetzt. Sie ist nahtlos in die Identity Services Engine (ISE) integriert.

🚰 AnyConnect Profile Editor - I	Network Access Manager	- • ×
File Help		
File Help Network Access Manager Clent Policy Authentication Policy Networks X 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.	Media Type Security Leve Connection Ty Machine Auth Credentials User Auth Credentials
	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.	

Anschließend können separate Authentifizierungen von den Registerkarten "Machine Authentication" (Computerauthentifizierung) und "User Authentication" (Benutzerauthentifizierung) konfiguriert werden.

Wenn der offene 802.1x-Modus auf dem Switch nicht akzeptiert werden kann, kann der 802.1x-Modus verwendet werden, bevor die Anmeldungsfunktion in der Client-Richtlinie konfiguriert wird.

Zugehörige Informationen

- Benutzerhandbuch zum Cisco Secure Access Control System 5.3
- <u>Administratorhandbuch für Cisco AnyConnect Secure Mobility Client, Version 3.0</u>
- <u>AnyConnect Secure Mobility Client 3.0: Network Access Manager und Profile Editor unter</u> <u>Windows</u>
- <u>Technischer Support und Dokumentation Cisco Systems</u>