Konfigurieren der ISE für die Integration mit einem LDAP-Server

Inhalt

Einleitung Voraussetzungen Anforderungen Verwendete Komponenten Hintergrundinformationen Konfigurieren Netzwerkdiagramm OpenLDAP konfigurieren Integration von OpenLDAP in die ISE Konfigurieren des WLC Konfigurieren von EAP-GTC Überprüfung Fehlerbehebung

Einleitung

In diesem Dokument wird beschrieben, wie Sie eine Cisco Identity Services Engine (ISE) für die Integration mit einem Cisco LDAP-Server konfigurieren.

Voraussetzungen

Anforderungen

Es gibt keine spezifischen Anforderungen für dieses Dokument.

Verwendete Komponenten

Die in diesem Dokument enthaltenen Informationen basieren auf den folgenden Software- und Hardwareversionen:

- Cisco ISE Version 1.3 mit Patch 2
- Microsoft Windows Version 7 x64 mit installiertem OpenLDAP
- Cisco Wireless LAN Controller (WLC) Version 8.0.100.0
- Cisco AnyConnect Version 3.1 für Microsoft Windows
- Profileditor für Cisco Network Access Manager

Hinweis: Dieses Dokument gilt für Einrichtungen, die LDAP als externe Identitätsquelle für die ISE-Authentifizierung und -Autorisierung verwenden. Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Hintergrundinformationen

Diese Authentifizierungsmethoden werden von LDAP unterstützt:

- Extensible Authentication Protocol Generic Token Card (EAP-GTC)
- Extensible Authentication Protocol Transport Layer Security (EAP-TLS)
- Protected Extensible Authentication Protocol Transport Layer Security (PEAP-TLS)

Konfigurieren

In diesem Abschnitt wird beschrieben, wie Sie die Netzwerkgeräte konfigurieren und die ISE in einen LDAP-Server integrieren.

Netzwerkdiagramm

In diesem Konfigurationsbeispiel verwendet der Endpunkt einen Wireless-Adapter, um eine Verbindung mit dem Wireless-Netzwerk herzustellen.

Das Wireless LAN (WLAN) auf dem WLC wird so konfiguriert, dass die Benutzer über die ISE authentifiziert werden. Auf der ISE wird LDAP als externer Identitätsspeicher konfiguriert.

Dieses Bild zeigt die Netzwerktopologie, die verwendet wird:



OpenLDAP konfigurieren

Die Installation von OpenLDAP für Microsoft Windows erfolgt über die GUI und ist einfach. Der Standardspeicherort ist **C: > OpenLDAP**. Nach der Installation sollte das folgende Verzeichnis angezeigt werden:

Name	Date modified	Туре	Size
BDBTools	6/3/2015 5:06 PM	File folder	
ClientTools	6/3/2015 5:06 PM	File folder	
🌗 data	6/4/2015 9:09 PM	File folder	
🌗 Idifdata	6/4/2015 11:03 AM	File folder	
퉬 Readme	6/3/2015 5:06 PM	File folder	
퉬 replica	6/3/2015 5:06 PM	File folder	
퉬 run	6/4/2015 9:09 PM	File folder	
퉬 schema	6/3/2015 5:06 PM	File folder	
🐌 secure	6/3/2015 5:06 PM	File folder	
🐌 SQL	6/3/2015 5:06 PM	File folder	
퉬 ucdata	6/3/2015 5:06 PM	File folder	
🚳 4758cca.dll	2/22/2015 5:59 PM	Application extens	18 KB
🚳 aep.dll	2/22/2015 5:59 PM	Application extens	15 KB
🚳 atalla.dll	2/22/2015 5:59 PM	Application extens	13 KB
🚳 capi.dll	2/22/2015 5:59 PM	Application extens	29 KB
🚳 chil.dll	2/22/2015 5:59 PM	Application extens	21 KB
🚳 cswift.dll	2/22/2015 5:59 PM	Application extens	20 KB
🚳 gmp.dll	2/22/2015 5:59 PM	Application extens	6 KB
🚳 gost.dll	2/22/2015 5:59 PM	Application extens	76 KB
🚳 hs_regex.dll	5/11/2015 10:58 PM	Application extens	38 KB
InstallService.Action	5/11/2015 10:59 PM	ACTION File	81 KB
💼 krb5.ini	6/3/2015 5:06 PM	Configuration sett	1 KB
🚳 libeay32.dll	2/22/2015 5:59 PM	Application extens	1,545 KB
🚳 libsasl.dll	2/5/2015 9:40 PM	Application extens	252 KB
maxcrc.ldif	2/5/2015 9:40 PM	LDIF File	1 KB
🚳 nuron.dll	2/22/2015 5:59 PM	Application extens	11 KB
🚳 padlock.dll	2/22/2015 5:59 PM	Application extens	7 KB
slapacl.exe	5/11/2015 10:59 PM	Application	3,711 KB

Beachten Sie insbesondere zwei Verzeichnisse:

- **ClientTools** Dieses Verzeichnis enthält eine Reihe von Binärdateien, die zum Bearbeiten der LDAP-Datenbank verwendet werden.
- ldifdata Dies ist der Speicherort, an dem Sie die Dateien mit LDAP-Objekten speichern sollten.

Fügen Sie diese Struktur der LDAP-Datenbank hinzu:



Unter dem *Stammverzeichnis* müssen Sie zwei Organisationseinheiten (OUs) konfigurieren. Die *OU=groups*-OU sollte eine untergeordnete Gruppe aufweisen (in diesem Beispiel **cn=domainusers**).

Die OU=people OU definiert die beiden Benutzerkonten, die zur Gruppe cn=domainusers gehören.

Um die Datenbank zu füllen, müssen Sie zuerst die *ldif*-Datei erstellen. Die zuvor erwähnte Struktur wurde aus dieser Datei erstellt:

dn: ou=groups,dc=maxcrc,dc=com changetype: add ou: groups description: All groups in organisation objectclass: organizationalunit dn: ou=people,dc=maxcrc,dc=com changetype: add ou: people description: All people in organisation objectclass: organizationalunit dn: uid=john.doe,ou=people,dc=maxcrc,dc=com changetype: add objectClass: top objectClass: person objectClass: organizationalPerson objectClass: inetOrgPerson uid: john.doe givenName: John sn: Doe cn: John Doe mail: john.doe@example.com userPassword: password

dn: uid=jan.kowalski,ou=people,dc=maxcrc,dc=com
changetype: add

objectClass: top objectClass: person objectClass: organizationalPerson objectClass: inetOrgPerson uid: jan.kowalski givenName: Jan sn: Kowalski cn: Jan Kowalski mail: jan.kowalski@example.com userPassword: password dn: cn=domainusers,ou=groups,dc=maxcrc,dc=com changetype: add objectClass: top objectClass: posixGroup gidNumber: 678 memberUid: uid=john.doe,ou=people,dc=maxcrc,dc=com memberUid: uid=jan.kowalski,ou=people,dc=maxcrc,dc=com

Um die Objekte zur LDAP-Datenbank hinzuzufügen, verwenden Sie die Binärdatei Idapchange:

C:\OpenLDAP\ClientTools>ldapmodify.exe -a -x -h localhost -p 389 -D "cn=Manager, dc=maxcrc,dc=com" -w secret -f C:\OpenLDAP\ldifdata\test.ldif ldap_connect_to_host: TCP localhost:389 ldap_new_socket: 496 ldap_connect_to_host: Trying ::1 389 ldap_pvt_connect: fd: 496 tm: -1 async: 0 attempting to connect: connect success adding new entry "ou=groups,dc=maxcrc,dc=com" adding new entry "ou=people,dc=maxcrc,dc=com" adding new entry "uid=john.doe,ou=people,dc=maxcrc,dc=com" adding new entry "uid=jan.kowalski,ou=people,dc=maxcrc,dc=com"

Integration von OpenLDAP in die ISE

Verwenden Sie die Informationen, die in den Abbildern in diesem Abschnitt bereitgestellt werden, um LDAP als externen Identitätsspeicher auf der ISE zu konfigurieren.

ahah		License Warning
cisco Identity Services Engine	Administration I▼ Policy I▼ Guest Access I▼ Administration I▼	
🔆 System 🛛 🥵 Identity Management	Network Resources 🛛 R Device Portal Management 🕞 pxGrid Services 🙀 Feed Service	Le pxGrid Identity Mapping
Mentities Groups External Identity So	arces Identity Source Sequences Settings	
External Identity Sources	LDAP Identity Sources List > LDAP_EXAMPLE LDAP Identity Source General Connection Directory Organization Groups Attributes	
Active Directory CDAP LDAP LDAP LDAP_CXAMPLE ACDUS Token	* Name LDAP_EXAMPLE	
 RSA SecurID 	Schema Custom T	
	* Subject Objectclass netOrgPerson * Group Objectclass poskGroup	
	* Subject Name Attribute uid * Group Map Attribute memberUid	
	Certificate Attribute userCertificate	
	O Subject Objects Contain Reference Te Groups	
	Group Objects Contain Reference To Subjects	
	Subjects in Groups Are Stored in Member Attribute As Distinguished Name	T
	Save Reset	

Sie können diese Attribute auf der Registerkarte Allgemein konfigurieren:

- **Subject ObjectClass** (Betreff-Objektklasse): Dieses Feld entspricht der Objektklasse der Benutzerkonten in der *ldif*-Datei. Verwenden Sie gemäß der LDAP-Konfiguration eine dieser vier Klassen:
 - Oben
 - Person
 - Organisatorische Person
 - InetOrgPerson
- **Betreffnamenattribut** Dies ist das Attribut, das vom LDAP abgerufen wird, wenn die ISE abfragt, ob ein bestimmter Benutzername in einer Datenbank enthalten ist. In diesem Szenario müssen Sie **john.doe** oder **jan.kowalski** als Benutzernamen auf dem Endpunkt verwenden.
- Group ObjectClass (Gruppenobjektklasse) Dieses Feld entspricht der Objektklasse für eine Gruppe in der *ldif*-Datei. In diesem Szenario ist die Objektklasse für die Gruppe *cn=domainusers* **posixGroup**.
- **Gruppenzuordnungsattribut** Dieses Attribut definiert, wie die Benutzer den Gruppen zugeordnet werden. Unter der Gruppe *cn=domainusers* in der Datei *ldif* sehen Sie zwei *memberUid*-Attribute, die den Benutzern entsprechen.

Die ISE bietet auch einige vorkonfigurierte Schemas (Microsoft Active Directory, Sun, Novell):

cisco Identity Services Engine	Home Operations Policy Guest Access Administration	License Warning A
🔆 System 🦉 Identity Management	Network Resources 🛃 Device Portal Management 🔂 pxGrid Services 🗔 Feed Service	±∰ pxGrid Identity Mapping
Identities Groups External Identity So	Inces Identity Source Sequences Settings	
External Identity Sources	LDAP Identity Source: Ust > LDAP_CXAMPLE LDAP Identity Source: Operation Operation Operation Operation Attributes	
Certificate Authentication Profile Active Directory	Primary Server	Secondary 5
■ ADAP EXAMPLE		Enable Se
 RADOUS Token 	* Hostname/IP 10.61.106.242	Hostname/IP
RSA Securation	* Port 389	Port 389
	Access Anonymous Access Authenticated Access Admin DN * Con=Manager, dc=maxorc, dc=com Password *	Access Anonymo Authentic Admin DN Password
	Secure Authentication 🗌 Enable Secure Authentication	Secure Authentication 🗌 Enable Se
	Root CA Certificate Services Endpoint *	Root CA Certificate Se
	* Server Timeout 10 ①Seconds * Max. Admin Connections 20 ② ③ ② Ma	Server Timeout 10 c. Admin Connections 20 Test Bind t
	Seve Reset	

Nachdem Sie die richtige IP-Adresse und den richtigen Domänennamen festgelegt haben, können Sie die *Testbindung* an den Server durchführen. An dieser Stelle rufen Sie keine Themen oder Gruppen ab, da die Suchbasis noch nicht konfiguriert ist.

Konfigurieren Sie auf der nächsten Registerkarte die Suchbasis für Betreff/Gruppe. Dies ist der *Verknüpfungspunkt* für die ISE mit dem LDAP. Sie können nur Themen und Gruppen abrufen, die untergeordnete Elemente Ihres Verbindungspunkts sind.

In diesem Szenario werden die Subjekte aus der OU=people und die Gruppen aus der OU=groups abgerufen:

abab		License Warning 🛕
CISCO Identity Services Engine	Mome Operations I▼ Policy I▼ Guest Access I▼ Administration I▼	
🔆 System 🛛 💆 Identity Management	🖀 Network Resources 🛛 🛃 Device Portal Management 🛛 🔯 pxGrid Services 🖉 Feed Service	Le pxGrid Identity Mapping
Identities Groups External Identity S	urces Identity Source Sequences Settings	
External Identity Sources	LDAP Identity Sources Let > LDAP_EXAMPLE LDAP Identity Source General Connection Directory Organization Groups Attributes * Subject Search Base ou=poople,dc=mexcrc,dc=com * Group Search Base ou=groups,dc=mexcrc,dc=com * Search for MAC Address in Format xxx xx xx xx xx xx xx	
	Strip end of subject name up to the fast occurrence of the separator Strip end of subject name from the first occurrence of the separator	

Auf der Registerkarte Gruppen können Sie die Gruppen aus dem LDAP auf der ISE importieren:

cisco Identity Services Engine	Hume Operations * Poky * Guest Acces * Administration *	Set
Honor Coups Determine States	Network Resources 💽 Device Fortal Management 🔤 poOrd Services 🔤 Feed Service 🍂 poOrd Service Repuing	
External Identity Sources Image: Sources Image: Sources Image	LDMP Menthy Source LDMP_COMPLE LDAP MentBy Source General Connection Directory Organization Groups Attributes / Edit -+Adi - XDeles Group	
 LOAP_SKAMPUS AvOUS Toten RSA Securit0 	Select Directory Groups This datagis used to select groups from the Directory. Click Retireve Groups. to read directory. Filte: * * * * • * • * • * • * • * • * • *	×
0.00		Gancel

Konfigurieren des WLC

Verwenden Sie die Informationen in diesen Images, um den WLC für die 802.1x-Authentifizierung zu konfigurieren:

սիսիս cisco	MONITOR WLANS		WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP	EEEDBACK
WLANs	WLANs > Edit 'p	iborowi_byod	ľ					
WLANs	General Secu	rity QoS	Policy-Mappi	ng Advan	iced			
Advanced	Layer 2 Lay	er 3 AAA Se	rvers					
	Layer 2 Security	WPA+WPA2	-					
	Fast Transition Fast Transition							
	PMF WPA+WPA2 Para	Disab	led 🔻					
	WPA Policy WPA2 Policy-AE	s V						
	Authentication Key Management							
	802.1X	🗹 Enable						

uluilu cisco	MONITOR WL	ANS <u>C</u> ONTROLLER W <u>I</u> R	ELESS <u>S</u> ECURITY M <u>A</u> NAGEME	NT C <u>o</u> mmands he <u>l</u> p <u>e</u> eedback
WLANs	WLANs > Edi	t 'piborowi_byod'		
WLANs WLANs Advanced	General S	Security QoS Polic	y-Mapping Advanced	
Select AAA servers below to override use of default servers on this WLAI Radius Servers Radius Server Overwrite interface Enabled Authentication Servers Accounting Servers				EAP Parameters
	Server 1	P:10.62.145.51, Port:1812	✓ Enabled ✓ IP:10.62.145.51, Port:1813 ▼	Enable
	Server 2	None	▼ None ▼	
	Server 3	None	▼ None ▼	
	Server 4	None	▼ None ▼	
	Server 5	None	▼ None ▼	
	Server 6	None	× None ×	

cisco	MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEME	NT C <u>o</u> mmands he <u>l</u> p <u>f</u> eedback
WLANs	WLANs > Edit 'piborowi_byod'	
WLANs WLANs	General Security QoS Policy-Mapping Advanced	
▶ Advanced	Layer 2 Layer 3 AAA Servers Select AAA servers below to override use of default servers on this WL Radius Servers Radius Server Overwrite interface Enabled Authentication Servers Ø Enabled Ø Enabled Server 1 IP:10.62.145.51, Port:1812 • IP:10.62.145.51, Port:1812 • IP:10.62.145.51, Port:1813 • Server 2 None • Server 3 None • Server 4 None • Server 5 None • Server 6 None •	AN EAP Parameters Enable

Konfigurieren von EAP-GTC

Eine der unterstützten Authentifizierungsmethoden für LDAP ist EAP-GTC. Die Funktion ist in Cisco AnyConnect verfügbar, Sie müssen jedoch den Network Access Manager Profile Editor installieren, um das Profil richtig zu konfigurieren.

Sie müssen auch die Konfiguration des Network Access Manager bearbeiten, die sich (standardmäßig) hier befindet:

C: > ProgramData > Cisco > Cisco AnyConnect Secure Mobility Client > Network Access Manager > System > configuration.xml-Datei

Verwenden Sie die Informationen in diesen Images, um EAP-GTC auf dem Endpunkt zu konfigurieren:

AnyConnect Profile Editor - N	Network Access Manager		
Network Access Manager Gient Policy	Networks Profile:ility Client\Net	work Access Manager\system\configuration.xml	
Network Access Manager Client Polcy Authentication Policy Networks Network Groups	Profile:ility Client\Net Name: Group Membership In group: In all groups (Global) Choose Your Network Media Wired (802.3) Network Select a wired network if with a traditional etherne Wi-Fi (wireless) Network Select a WiFi network if t via a wireless radio come SSID (max 32 chars):	work Access Manager\system\configuration.xml eap_gtc Local networks the endstations will be connecting to the network et cable. the endstations will be connecting to the network ection to an Access Point. plorowi_byod Hidden Network Corporate Network	Media Type Security Level Connection Type User Auth Credentials
	Common Settings Script or application on each us Connection Timeout	er's machine to run when connected. Browse Local Machine 40 seconds Next Cancel	

🚰 AnyConnect Profile Editor - N	letwork Access Manager	
File Help		
File Help Network Access Manager Client Policy Client Policy Authentication Policy Networks Network Groups	Networks Profile:ility Client\Network Access Manager\system\configuration.xml Security Level Open Network Open networks have no security, and are open to anybody within range. This is the least secure type of network. Shared Key Network Shared Key Network Shared Key Networks use a shared key to encrypt data between end stations and network access points. This medium security level is suitable for	Media Type Security Level Connection Type User Auth Credentials
	small/home offices.	
	authPeriod (sec.) 30 startPeriod (sec.) 30 heldPeriod (sec.) 60 maxStart 3 Association Mode WPA2 Enterprise (AES) •	
	Next Cancel	

🚰 AnyConnect Profile Editor -	Network Access Manager	
File Help		
File Help Network Access Manager Clent Policy Authentication Policy Networks Network Groups	Network Access Manager Networks Profile:ility Client\Network Access Manager\system\configuration.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 needed. 	Media Type Security Level Connection Type User Auth Credentials
	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. Next Cancel	

🚰 AnyConnect Profile Editor - Net	twork Access Manager	
File Help		
Network Access Manager	Networks Profile:ility Client\Network Access Manager\system\configuration	ı.xml
	- EAP Methods	Media Type
····· 34 Network Groups	C EAP-TLS O PEAP	Security Level
		Connection Type
	© EAP-TTLS © EAP-FAST	User Auth
	🛞 LEAP	Credentials
	Extend user connection beyond log off	
	EAP-PEAP Settings	
	Validate Server Identity	
	Enable Fast Reconnect	
	Disable when using a Smart Card	
	Inner Methods based on Credentials Source	
	Authenticate using a Password	
	EAP-MSCHAPv2	
	V EAP-GTC	
	EAP-TLS, using a Certificate	
	Authenticate using a Token and EAP-GTC	
	Next Cancel	

🚰 AnyConnect Profile Editor - N	letwork Access Manager					
File Help						
Network Access Manager	Networks Profile:ility Client\Network	Access Manager\system\configuration.xml				
	User Identity	Media Type				
	Unprotected Identity Pattern:	john.doe	Security Level			
	Protected Identity Pattern:	ishe dee	Connection Type			
		Johnade	User Auth			
			Credentials			
	User Credentials					
	O Use Single Sign On Credentials	5				
	Prompt for Credentials					
	Remember Forever					
	Remember while User					
	Never Remember					
	Ose State Credentials					
	Password: passwo	ords				
	Done	Cancel				

Verwenden Sie die Informationen in diesen Images, um die Authentifizierungs- und Autorisierungsrichtlinien auf der ISE zu ändern:

ah	dia -									Loanse Warning
cis	co i	Identity Service	s Engine		🙆 Home	Operations •	Policy *	Guest Access	Administration 💌	
_	Autho	entication 🧕 🧕	Authorization	K Profiling	💘 Posture	👸 Client Pro	visioning	🚊 TrustSec	🐴 Policy Elements	
Auth	entic	ation Policy								
Define	the A	uthentication Polic	y by selecting the p	rotocols that ISE s	hould use to cor	mmunicate with th	e network de	vices, and the ident	ity sources that it should	use for authentication.
For Po	ky Ex	port go to Administ	tration > System >	Backup & Restore	> Policy Export	Page				
Policy	Тура	🔿 Simple 💿	Rule-Based							
	_									
	1	MAB	: 1f	Wired_MAB OR Wireless_MAB			Allow P	rotocols : Default	Network Access	and
		🗹 Default	:1	ise Internal Endpo	ints					
1	~	Dot1X	: If	Wired_802.1X OR Wireless_802.1X			Alow P	rotocols : Default	Network Access	and
		🔄 Default	:1	ISE LDAP_EXAMPL	E					
	1	Default Rule (If n	io match) : Allow	Protocols : Defau	it Network Acce	55	and use :	Al_User_ID_Stores		

abab											Disease Warning A
cisco	Identi	ty Services Engine		🙆 Home	Operations 🔻	Policy •	Guest Access	Adm	inistration 1 💌		
🔤 🗛 Au	thenticati	on 🕒 Authorization	🔣 Profiling	🔀 Posture	Gient Pro	visioning	🚊 TrustSec	🐥 Polic	y Elements		
Authorb	zation P	olicy									
Define the For Policy	e Authoria Export oc	ation Policy by configuring rules b to Administration > System > B	ased on ider ackup & Res	ntity groups and/or of tore > Policy Export P	ther conditions. Dr Page	ag and drop	rules to change the o	der.			
First Mate	thed Rule	Apples +									
E Exce	ntions ((1)									
- Land		·)									
Stand	ard										
St	tatus P	tule Name		Conditions (identity g	roups and other o	onditions)			Permissions		
		Isers in LDAP store	ï	(Wireless_802.1X AN cn=domainusers,ou=)	DILDAP_EXAMPLE: groups,dc=maxcro	:ExternalGrou ,dc=com)	ps EQUALS	then	PermitAccess		
i 🛛	v	Vireless Black List Default	If	Blacklist AND Wirele	ss_Access			then	Blackhole_Wirel	ess_Access	
	P	rofiled Cisco IP Phones	iî.	Cisco-IP-Phone				then	Cisco_JP_Phone	**	
	P	rofiled Non Cisco IP Phones	f	Non_Cisco_Profiled_P	hones			then	Non_Osco_IP_0	hones	
	6	asic_Authenticated_Access	if .	Network_Access_Aut	thentication_Passe	d		then	PermitAccess		
	0	lefault	if no	matches, then De	enyAccess						

Nachdem Sie die Konfiguration angewendet haben, sollten Sie in der Lage sein, eine Verbindung zum Netzwerk herzustellen:



Überprüfung

Um die LDAP- und ISE-Konfigurationen zu überprüfen, rufen Sie die Themen und Gruppen mit einer Testverbindung zum Server ab:

alata					Lieve	we Warning A
cisco Identity Services Engine	🙆 Home 🛛 🙆	perations 🖙 Policy 🖙	Guest Access	Administration •		
🔆 System 🛛 🖉 Identity Management	📰 Network Resources 🛛 🛃 D	evice Portal Management	🙀 pxGnd Services	Feed Service	Le pxGnd Identit	y Mapping
Identities Groups External Identity S	ources Identity Source Seque	nces Settings				
External Identity Sources	LDAP Identity Sources List > LDAP LDAP Identity Source General Conne	EXAMPLE	nanitation Gra	uns Attributos		
Certificate Authentication Profile Active Directory		Primary Server	Bind successful to 10.6	1.108.242.389		Secondary S
			Result of testing this co Number of Subjects: 2 Number of Groups: 1	nfiguration is as follows: 2		🗌 Enable S
 RADIUS Token 	* Hostname/IP	10.61.106.242			Hostname/IP	
RSA SecurID	* Port	389	Response time: 1636m	15	Port	389
	Access (Admin DN 1 Password 1	Anonymous Access Authenticated Access an=Manager,dc=maxor 		ОК	Access Admin DN Password	Anonymo Authentic
	Secure Authentication Root CA] Enable Secure Authentica Certificate Services Endpoint	tion t *	3	Secure Authentication Root CA	Enable St Certificate S
	* Server Timeout * Max. Admin Connections	10 20	©Seconds ©	Max	Server Timeout Admin Connections	10 20
	3	Test Bind to Server				Test Bind t
the set of the local set of the set of the local set of the local set	1 Constanting of the local division of the l					
	Save Reset					

Die folgenden Bilder illustrieren einen Beispielbericht der ISE:

clisco Identity Services Engine	A Home Operations	Policy T Guest Access T Administration T	Lizzanz Microlais 🔏 Andil Scholar
🔲 Authentications 📑 Reports	🔄 Endpoint Protection Service 💦 💊 Troublesho	at	
Neconfigured Suppleants $^{(\ell)}$ 1	Misconfigured Network Devices ⁽ O	0 RADIUS Grops (0) 1305	Clent Stopped Responding (2) 0
🔒 Shaw Une Sessions 🗌 🎡 Add at Remove Calu	nns 🔻 🏀 Refresh 🛛 🕲 Reset Repeat Counts		Refresh Every 1 minute *
Time T Status Details	Repeat Count Identity (C Endpoint ID (C)	Endpoint Profile (1) Authentication Policy (2)	Authorization Policy T Authorization Profiles T
2015-06-04 21:50:45.538 🕥 🔓	0 john.doe C094A:00:14:80:48	Windows7-Workst	
2015-06-04 21:59:45.510 🛛 🔓	(ohn.doe 00x4A:00:14:80:48	Windows7-Workst Default >> Dot1X >> Default	Default >> Users in LDAP store PermitAccess

Overview	
Event	5200 Authentication succeeded
Username	john.doe ⊕
Endpoint Id	C0:4A:00:14:8D:4B ⊕
Endpoint Profile	Windows7-Workstation
Authentication Policy	Default >> Dot1X >> Default
Authorization Policy	Default >> Users in LDAP store
Authorization Result	PermitAccess

Authentication Details	
Source Timestamp	2015-06-04 21:59:45.509
Received Timestamp	2015-06-04 21:59:45.51
Policy Server	ise13
Event	5200 Authentication succeeded
Failure Reason	
Resolution	
Root cause	
Username	john.doe
User Type	
Endpoint Id	C0:4A:00:14:8D:4B
Endpoint Profile	Windows7-Workstation
IP Address	
Authentication Identity Store	LDAP_EXAMPLE
Identity Group	Workstation
Audit Session Id	0a3e9465000010035570b956
Authentication Method	dot1x
Authentication Protocol	PEAP (EAP-GTC)
Service Type	Framed
AD ExternalGroups	cn=domainusers,ou=groups,dc=maxcrc,dc=com
IdentityDn	uid=john.doe,ou=people,dc=maxcrc,dc=com
RADIUS Username	john.doe

Fehlerbehebung

In diesem Abschnitt werden einige häufige Fehler beschrieben, die bei dieser Konfiguration aufgetreten sind, und es wird beschrieben, wie diese Fehler behoben werden:

- Wenn nach der Installation von OpenLDAP ein Fehler auftritt, der anzeigt, dass eine **gssapi.dll** fehlt, starten Sie Microsoft Windows neu.
- Möglicherweise ist es nicht möglich, die Datei *configuration.xml* für Cisco AnyConnect direkt zu bearbeiten. Speichern Sie die neue Konfiguration an einem anderen Speicherort, und ersetzen Sie dann die alte Datei.
- Im Authentifizierungsbericht wird die folgende Fehlermeldung angezeigt:

<#root>

Authentication method is not supported by any applicable identity store

Diese Fehlermeldung zeigt an, dass die ausgewählte Methode nicht von LDAP unterstützt wird.

Stellen Sie sicher, dass das *Authentifizierungsprotokoll* im gleichen Bericht eine der unterstützten Methoden anzeigt (EAP-GTC, EAP-TLS oder PEAP-TLS).

• Wenn Sie im Authentifizierungsbericht feststellen, dass der Betreff nicht im Identitätsspeicher gefunden wurde, stimmt der Benutzername aus dem Bericht nicht mit dem *Betreffnamenattribut* für einen Benutzer in der LDAP-Datenbank überein.

In diesem Szenario wurde der Wert für dieses Attribut auf **uid** gesetzt, was bedeutet, dass die ISE die *uid*-Werte für den LDAP-Benutzer überprüft, wenn sie versucht, eine Übereinstimmung zu finden.

• Wenn die Themen und Gruppen während eines *Binding an Server*-Tests nicht korrekt abgerufen werden, ist dies eine falsche Konfiguration für die Suchbasen.

Denken Sie daran, dass die LDAP-Hierarchie von Leaf-to-Root und *DC* angegeben werden muss (kann aus mehreren Wörtern bestehen).

Tipp: Informationen zur Fehlerbehebung der EAP-Authentifizierung auf WLC-Seite finden Sie im Dokument <u>EAP Authentication with WLAN Controllers (WLC) Configuration Example</u> Cisco.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.