De ISE voor integratie met een LDAP-server configureren

Inhoud

Inleiding Voorwaarden Vereisten Gebruikte componenten Achtergrondinformatie Configureren Netwerkdiagram OpenLDAP configureren OpenDAP integreren met de ISE-software De WLC configureren EAP-GTC configureren Verifiëren Problemen oplossen

Inleiding

Dit document beschrijft hoe u een Cisco Identity Services Engine (ISE) kunt configureren voor integratie met een Cisco LDAP-server.

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

De informatie in dit document is gebaseerd op deze software- en hardwareversies:

- Cisco ISE versie 1.3 met patch 2
- Microsoft Windows versie 7 x64 met geïnstalleerde OpenLDAP
- Cisco draadloze LAN-controller (WLC) versie 8.0.10.0
- Cisco AnyConnect versie 3.1 voor Microsoft Windows
- Cisco Network Access Manager-profieleditor

Opmerking: dit document is geldig voor instellingen die LDAP gebruiken als externe identiteitsbron voor de ISE-verificatie en -autorisatie.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle

apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Achtergrondinformatie

Deze verificatiemethoden worden ondersteund met LDAP:

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

Configureren

In dit deel wordt beschreven hoe u de netwerkapparaten kunt configureren en de ISE kunt integreren met een LDAP-server.

Netwerkdiagram

In dit configuratievoorbeeld gebruikt het eindpunt een draadloze adapter om een koppeling te maken met het draadloze netwerk.

Draadloze LAN (WLAN) op de WLC is geconfigureerd om de gebruikers via de ISE te verifiëren. Op de ISE is LDAP ingesteld als externe identiteitsopslag.

Dit beeld illustreert de netwerktopologie die wordt gebruikt:



OpenLDAP configureren

De installatie van OpenLDAP voor Microsoft Windows is voltooid via de GUI, en het is eenvoudig. De standaardlocatie is C: > OpenLDAP. Na installatie, zou u deze folder moeten zien:

Name	<u>^</u>	Date modified	Туре	Size
BDBTools		6/3/2015 5:06 PM	File folder	
ClientTools		6/3/2015 5:06 PM	File folder	
퉬 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	
퉬 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.Act	ion	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

Neem nota van twee directory's:

- **ClientTools** Deze map bevat een aantal binaire bestanden die worden gebruikt om de LDAPdatabase te bewerken.
- ldifdata Dit is de locatie waar u de bestanden met LDAP-objecten moet opslaan.

Voeg deze structuur toe aan de LDAP-database:



Onder de map *Root* moet u twee Organisatorische Eenheden (OU's) configureren. OU = groups OU zou één kindgroep moeten hebben (**cn=domainusers** in dit voorbeeld).

De *OE=people* OE definieert de twee gebruikersaccounts die behoren tot de groep *cn=domainusers*.

U moet het *ldif*-bestand eerst maken om de database te kunnen vullen. De eerder vermelde structuur is met behulp van dit bestand gemaakt:

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

Om de objecten aan de LDAP-database toe te voegen, gebruikt u het binaire ldapmodificatie:

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"

OpenDAP integreren met de ISE-software

Gebruik de informatie die in de beelden door deze sectie wordt verstrekt om LDAP als externe identiteitsopslag op ISE te vormen.

ahah		Liceose Warning
cisco Identity Services Engine	Administration ▼ Policy ▼ Guest Access ▼ Administration ▼	
🔆 System 🛛 👰 Identity Management	📷 Network Resources 🛛 😹 Device Portal Management 🛛 🔂 pxGrid Services 🛛 🙀 Feed Service	LepxGrid Identity Mapping
Identities Groups External Identity S	urces Identity Source Sequences Settings	
External Identity Sources	LDAP Identity Sources List > LDAP_EXAMPLE LDAP Identity Source	
	General Connection Directory Organization Groups Attributes	
Active Directory DAP LDAP LDAP LDAP RADUS Token RADUS Token RSA SecuriD	* Name LDAP_EXAMPLE Description * Schema Custom * Subject Objectclass inetOrgPerson * Group Objectclass postkGroup * Subject Name Attribute ud * Group Map Attribute memberUid Certificate Attribute	
	Subject Objects Contain Reference To Groups Group Objects Contain Reference To Subjects Subjects In Groups Are Stored In Member Attribute As Datinguished Name	Ţ
	Save Reset	

U kunt deze eigenschappen configureren op het tabblad Algemeen:

- **Object class** Dit veld komt overeen met de objectklasse van de gebruikersaccounts in het *ldif*bestand. Volgens de LDAP-configuratie. Gebruik een van deze vier klassen:
 - top
 - Persoon
 - Organisator
 - InetOrgPerson
- Attribuut onderwerpnaam Dit is het attribuut dat door de LDAP wordt opgehaald wanneer de ISE vraagt of een specifieke gebruikersnaam in een database is opgenomen. In dit scenario moet u **john.doe** of **jan.kowalski** gebruiken als de gebruikersnaam op het eindpunt.
- Groep Objectklasse Dit veld komt overeen met de objectklasse voor een groep in het *ldif*-bestand. In dit scenario is de objectklasse voor de groep *cn=domainusers* posixGroup.
- Group Map Attribute Deze eigenschap bepaalt hoe de gebruikers aan de groepen worden toegewezen. Onder de groep *cn=domainusers* in het *ldif*-bestand kunt u twee *memberUid*-kenmerken zien die overeenkomen met de gebruikers.

De ISE biedt ook enkele vooraf ingestelde schema's (Microsoft Active Directory, Sun, Novell):

ababe as a second second		License Warning A
cisco Identity Services Engine	The American Policy Torus Access Administration	
🔆 System 🛛 💆 Identity Management	📲 Network Resources 🛛 🛃 Device Portal Management 🗔 pxGrid Services 🖓 Feed Service 🕰 pxGrid	Identity Mapping
Identities Groups External Identity	Sources Identity Source Sequences Settings	
External Identity Sources	LDVP Identity Sources List > LDAP_COMPLE LDAP Identity Source General Connection Directory Organization Groups Attributes	
Active Directory	Primary Server	Secondary 5
		Enable Se
 RADUS Token 	* Hostname/P 10.61.106.242	amedP
RSA Securit	*Put 389	Port 389
	Access Anonymous Access	Access Anonymo Authentic
	Password * Pas	ssword
	Secure Authentication Enable Secure Authentication Secure Authentication Root CA. Certificate Services Endpoint *	tication Enable Sc toot CA Certificate Sc
	*Server Timeout 10 @Seconds Server T	îmeout 10
	* Max. Admin Connections 20 (i) Max. Admin Connections	ections 20
	Test Bind to Server	Test Bind t
	۲. II	
	Save Reset	

Nadat u het juiste IP-adres en de beheerdomeinnaam hebt ingesteld, kunt u *Bind testen* op de server. Op dit punt, vindt u geen onderwerpen of groepen terug omdat de zoekbases nog niet zijn geconfigureerd.

In het volgende tabblad configureert u de Onderwerp/Groep Zoekbasis. Dit is het *samenvoegpunt* voor de ISE naar de LDAP. Je kunt alleen onderwerpen en groepen ophalen die kinderen zijn van je toetredingspunt.

In dit scenario worden de onderwerpen uit *OU=people* en de groepen uit *OU=groups* opgehaald:

abab		License Warning 🔥
CISCO Identity Services Engine	Administration 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 Sou	rces Identity Source Sequences Settings	
External Identity Sources	LDAP Identity Sources Let > LDAP_EXAMPLE LDAP Identity Sources General Connection Directory Organization Groups Attributes * Subject Search Base ou=people,dc=maxrc,dc=com Naming_Contexts 0 * Group Search Base ou=groups,dc=maxrc,dc=com Naming_Contexts 0 Search for MAC Address in Format paxxx xx xx xx Strip start of subject name up to the last occurrence of the separator Strip end of subject name from the first occurrence of the separator	

Vanuit het tabblad Groepen kunt u de groepen importeren vanuit de LDAP op de ISE:

cisco Identity Services Engine	Harre Operations * Policy * Guest Access * Administration *	54
System Directly Management	🖬 Network Resources 📧 Device Partal Management 🔤 pxGrid Services 🔛 Feed Service 🔺 pxGrid Identity Rapping Incis Identity Source Sequences Settings	
External Identity Sources	LDAP Mently Source Lat > EDAP_DOARNEL LDAP Mently Source General Connection Breatory Organization Groups Attributes //Edt + 4dd - X Delete Group	
	Select Directory Groups This dialog is used to select groups from the Directory Click Relitieve Groups, to read directory	×
* 🔲 RSA Securiti	Filte: Retireve Groups: Numb Nume cn=dcmainus.era.cu=groups.dc=maxOt; dc=com 	
O mite		Cancel

De WLC configureren

Gebruik de informatie in deze afbeeldingen om de WLC voor 802.1x-verificatie te configureren:

սիսիս cisco	MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP EEEDBACK
WLANs	WLANs > Edit 'piborowi_byod'
WLANS	General Security QoS Policy-Mapping Advanced
Advanced	Layer 2 Layer 3 AAA Servers
	Layer 2 Security WPA+WPA2 MAC Filtering
	Fast Transition
	Protected Management Frame PMF Disabled WPA+WPA2 Parameters
	WPA Policy WPA2 Policy-AES
	Authentication Key Management
	802.1X 🗹 Enable

uluilu cisco	MONITOR WL	ANS <u>C</u> ONTROLLER	WIREL	ESS <u>S</u> ECL	IRITY M <u>A</u> N	GEMENT	C <u>O</u> MMANDS	HELP	EEEDBACK
WLANs	WLANs > Edi	t 'piborowi_byoo	4.						
WLANs WLANs Advanced	General S Layer 2	Security QoS	Policy-	Mapping	Advanced				
	Select AAA s Radius Serve Radius Serve	servers below to ove ers rver Overwrite interfact Authentication Serv.	erride us e Ena	e of default obled Accounting	servers on t	his WLAN	EAP Paramet		
		Enabled		Enabled			Enable		
	Server 1	IP:10.62.145.51, Port	:1812 🔻	IP:10.62.14	5.51, Port:181	3 🔻			
	Server 2	None	•	None		-			
	Server 3	None	-	None		•			
	Server 4	None	•	None		*			
	Server 5	None	-	None		-			
	Server 6	None	•	None		-			

ululu cisco	MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGE	EMENT C <u>O</u> MMANDS	HELP EEEDBACK
WLANs	WLANs > Edit 'piborowi_byod'		
WLANS	General Security QoS Policy-Mapping Advanced		
	Select AAA servers below to override use of default servers on this Radius Servers Radius Server Overwrite interface Enabled Authentication Servers Accounting Servers Image:	EAP Paramete Enable	ers

EAP-GTC configureren

Een van de ondersteunde verificatiemethoden voor LDAP is EAP-GTC. Het is beschikbaar in Cisco AnyConnect, maar u moet de Network Access Manager Profile Editor installeren om het profiel correct te kunnen configureren.

U moet ook de configuratie van Network Access Manager bewerken, die (standaard) hier te vinden is:

C: > Program Data > Cisco > Cisco AnyConnect Secure Mobility Client > Network Access Manager > systeem > Configuration.xml-bestand

Gebruik de informatie in deze afbeeldingen om de EAP-GTC op het eindpunt te configureren:

AnyConnect Profile Editor - N	Network Access Manager		
Network Access Manager	Networks Profile:ility Client\Net	work Access Manager\system\configuration.xml	
Network Access Manager Clent 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: lity 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.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\configura	tion.xml				
	User Identity	Media Type					
····· % Network Groups	Unprotected Identity Pattern:	john.doe	Security Level				
	Protected Identify Patterny		Connection Type				
	Protected Identity Pattern:	John.doe	User Auth				
			Credentials				
	User Credentials						
	🛞 Use Single Sign On Credential	🔘 Use Single Sign On Credentials					
	 Prompt for Credentials Remember Foreveri Remember while User Never Remember Use Static Credentials Password: password: 	r is Logged On					
	Done	Cancel					

Gebruik de informatie in deze afbeeldingen om het authenticatie- en autorisatiebeleid op de ISE te wijzigen:

ab	aha										License Warring 🚠
cis	ico	Identity Servi	ces Engine		🙆 Home	Operations 💌	Policy *	Guest Access	Administration		
-	Auth	entication	S. Authorization	🔀 Profiling	💽 Posture	👸 Client Pro	visioning	TrustSec	🔥 Policy Elements		
Auth	entio	ation Policy									
Define	the .	Authentication Pe	licy by selecting the	protocols that ISE sh	ould use to con	municate with th	e network de	vices, and the ide	ntity sources that it sho	uld use for authenticat	ion.
For Po Policy	iky E Type	port go to Admir O Simple	istration > System : Rule-Based	> Backup & Restore >	Policy Export I	,aðe					
		0									
1	1	МАВ	: If	Wired_MAB OR Wireless_MAB			Alow P	rotocols : Defau	It Network Access	and	
		🛃 Default		use Internal Endpoi	nts						
1	~	Dot1X	: 1f	Wred_802.1X OR Wreless_802.1X			Alow P	rotocols : Defau	It Network Access	and	
		🛃 Default	:	USE LDAP_EXAMPLE							
	~	Default Rule (I	f no match) : Allov	v Protocols : Default	Network Acce	25	and use :	Al_User_ID_Stor	85		

aha	do 👘										Disease (counting T
cise	co Iden	tity Services Engine		🟠 Home	Operations I 🔻	Policy •	Guest Access	Admi	nistration •		
4	Authentica	ition 🛛 🙆 Authorization	🔀 Profiling	🔀 Posture	Gient Pro	visioning	🚊 TrustSec	🐥 Polic	y Elements		
Autho	orization	Policy									
Define For Pol	the Autho icy Export	rization Policy by configuring rules b go to Administration $>$ System $>$ B	ased on iden ackup & Rest	tity groups and/or of ore > Policy Export P	ther conditions. Dr Page	ag and drop	rules to change the or	der.			
First M	latched Ru	ie Applies 👻									
▶ Ex	ceptions	(0)									
Sta	ndard										
	Status	Rule Name	C	onditions (identity g	roups and other o	onditions)			Permissions		
1		Users in LDAP store	if (Wireless_802.1X AN n=domainusers,ou=/	DLDAP_EXAMPLE: groups,dc=maxtrc	ExternalGrou ,dc=com)	ps EQUALS	then	PermitAccess		
1	×	Wireless Black List Default	if B	Blacklist AND Wirele	ss_Access			then	Blackhole_Wire	less_Access	
1	×	Profiled Cisco IP Phones	ii d	isco-IP-Phone				then	Cisco_JP_Phone	es	
ī	2	Profiled Non Cisco IP Phones	f N	ion_Cisco_Profiled_P	hones			then	Non_Osco_IP_I	Phones	
÷	×	Basic_Authenticated_Access	if N	letwork_Access_Aut	hentication_Passe	d		then	PermitAccess		
	2	Default	if no	matches, then De	enyAccess						

Nadat u de configuratie hebt toegepast, moet u verbinding kunnen maken met het netwerk:



Verifiëren

Om de LDAP- en ISE-configuraties te verifiëren, haalt u de onderwerpen en groepen op met een testverbinding naar de server:

ahaha					Lieve	we Warning A
cisco Identity Services Engine	🏠 Home 🛛 0	perations 🖙 — Policy 🖛	Guest Access	Administration 1 🔻		
🔆 System 🛛 🛃 Identity Management	📰 Network Resources 🛛 🛃 D	evice Portal Management	属 pxGnd Services	Feed Service	🚛 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 Connection	EXAMPLE	canitation Score	ins 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 RSA SecurID	* Hostname/IP * Port	10.61.106.242 389	Response time:1636m	15	Hostname/IP Port	
	Access (Admin DN	 Anonymous Access Authenticated Access Gn=Manager,dc=maxor 		ОК	Access Admin DN	 Anonymo Authentic
	Password '	******			Password	
	Secure Authentication Root CA	Enable Secure Authentica Certificate Services Endpoint	tion *	S	ecure Authentication Root CA	Enable Se Certificate S
	* Server Timeoul	10	(1)Seconds		Server Timeout	10
	-max Aomin Connections	Test Bind to Server		Max.	Admin Connections	Test Bind #
and and and has been dead and and and and has been been						
	Save Reset					

Deze beelden illustreren een voorbeeldrapport van de ISE:

cisco Identity Services Engine	Home Operations	Policy Guest Access Administration	Tarava Maxime 🔏 Avdā admin
🔲 Authentications 🛛 🚊 Reports	🔄 🔯 Endpoint Protection Service 💦 💊 Troublesho	oot	
Nisconfigured Supplicants	Misconfigured Network Devices	D RADIUS Drops	Clent Stopped Responding @
1	0	1305	0
🗐 Shaw Uve Sessions – 🎡 Add at Remove Ca	unns 🔻 🏀 Refresh 🛛 🔯 Reset Repeat Counts		Refresh Every 1 minute *
Time v Status Al v Detais	Repeat Count Identity D Endpoint ID D	Endpoint Profile (2) Authentication Policy (2)	Authorization Policy T Authorization Profiles T
2015-06-04 21:50:45.538 🕤 🔂	0 john.doe C0:4A:00:14:80:48	Windows7-Workst	
2015-06-04 21:59:45.510 🔽 🚡	(obs.doe 00:44:00:14:80:48	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

Problemen oplossen

In deze sectie worden enkele veelvoorkomende fouten beschreven die bij deze configuratie worden aangetroffen en hoe u deze kunt oplossen:

- Na installatie van de OpenLDAP, als u een fout tegenkomt om aan te geven dat een **gssapi.dll** ontbreekt, start Microsoft Windows opnieuw.
- Mogelijk is het niet mogelijk het bestand *Configuration.xml* voor Cisco AnyConnect rechtstreeks te bewerken. Sla uw nieuwe configuratie op een andere locatie op en gebruik deze om het oude bestand te vervangen.
- In het verificatierapport staat deze foutmelding:

<#root>

Authentication method is not supported by any applicable identity store

Deze foutmelding geeft aan dat de gekozen methode niet wordt ondersteund door LDAP.

Zorg ervoor dat het *verificatieprotocol* in hetzelfde rapport een van de ondersteunde methoden toont (EAP-GTC, EAP-TLS of PEAP-TLS).

• Als u in het verificatierapport opmerkt dat het onderwerp niet in het identiteitsarchief is gevonden, komt de gebruikersnaam uit het rapport niet overeen met het *kenmerk Onderwerpnaam* voor een gebruiker in de LDAP-database.

In dit scenario is de waarde ingesteld op **uid** voor deze eigenschap, wat betekent dat de ISE naar de *uid*-waarden voor de LDAP-gebruiker kijkt wanneer deze een overeenkomst probeert te vinden.

• Als de onderwerpen en groepen niet correct worden teruggehaald tijdens een *bind aan server* test, is het een onjuiste configuratie voor de zoekbases.

Vergeet niet dat de LDAP-hiërarchie van blad tot wortel en *dc* moet worden gespecificeerd (kan uit meerdere woorden bestaan).

Tip: Raadpleeg voor het oplossen van problemen met EAP-verificatie aan de WLC-zijde het <u>configuratievoorbeeld van EAP-verificatie met WLAN-controllers (WLC) voor</u> Cisco-document.

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.