LDAP サーバと統合するための ISE の設定

内容
<u>はじめに</u>
前提条件
<u>要件</u>
<u>使用するコンポーネント</u>
<u>背景説明</u>
<u>設定</u>
<u>ネットワーク図</u>
<u>OpenLDAP の設定</u>
<u>OpenLDAP と ISE の統合</u>
<u>WLC の設定</u>
<u>EAP-GTC の設定</u>
トラブルシュート

はじめに

このドキュメントでは、Cisco LDAPサーバと統合するためにCisco Identity Services Engine(ISE)を設定する方法について説明します。

前提条件

要件

このドキュメントに関する固有の要件はありません。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- パッチ2が適用された Cisco ISE バージョン 1.3
- ・ OpenLDAP がインストールされた Microsoft Windows 7 x64
- ・ Cisco Wireless LAN Controller (WLC) バージョン 8.0.100.0
- ・ Microsoft Windows 向け Cisco AnyConnect バージョン 3.1
- ・ Cisco Network Access Manager プロファイル エディタ

✤ 注:このドキュメントは、ISE認証および認可の外部アイデンティティソースとして LDAPを使用する設定に有効です。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このド キュメントで使用するすべてのデバイスは、クリアな(デフォルト)設定で作業を開始していま す。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認して ください。

背景説明

LDAP では、次の認証方式がサポートされます。

- ・ 拡張認証プロトコル 汎用トークンカード(EAP-GTC)
- Extensible Authentication Protocol Transport Layer Security(EAP-TLS)
- Protected Extensible Authentication Protocol Transport Layer Security(PEAP-TLS)

設定

ここでは、ネットワーク デバイスを設定して ISE に LDAP サーバを統合する方法を説明します。

ネットワーク図

この設定例では、エンドポイントでワイヤレス アダプタを使用してワイヤレス ネットワークに関 連付けます。

WLC 上のワイヤレス LAN(WLAN)は、ISE を介してユーザを認証するように設定します。ISE では、LDAP を外部 ID ストアとして設定します。

次の図に、使用するネットワーク トポロジを示します。



OpenLDAP の設定

OpenLDAP for Microsoft Windows は、GUI を使用して簡単にインストールできます。デフォルト の場所はC: > OpenLDAPです。インストールが完了すると、このデレクトリは次のように表示さ れます。

Name	Date modified	Туре	Size
BDBTools	6/3/2015 5:06 PM	File folder	
퉬 ClientTools	6/3/2015 5:06 PM	File folder	
🌗 data	6/4/2015 9:09 PM	File folder	
🌗 ldifdata	6/4/2015 11:03 AM	File folder	
퉬 Readme	6/3/2015 5:06 PM	File folder	
🌗 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	
퉬 secure	6/3/2015 5:06 PM	File folder	
퉬 SQL	6/3/2015 5:06 PM	File folder	
🌗 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

次の2つのディレクトリに注目してください。

ClientTools:このディレクトリには、LDAPデータベースを編集するために使用されるバイナリのセットが含まれます。

• Idifdata:これは、LDAPオブジェクトとともにファイルを保存する場所です。

次に示す構造を LDAP データベースに追加してください。

ルート ディレクトリの下に、2 つの組織単位(OU)を設定する必要があります。OU=groups OU には 1 つの子グループを持たせます(この例では cn=domainusers)。

OU=people OU は、cn=domainusers グループに属する 2 つのユーザ アカウントを定義します。

データベースにデータを取り込むには、最初に Idif ファイルを作成する必要があります。前述の 構造は、次のファイルを基に作成されたものです。

dn: ou=groups, dc=maxcrc, dc=comchangetype: 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

LDAPデータベースにオブジェクトを追加するには、Idapmodifyバイナリを使用します。

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"

OpenLDAP と ISE の統合

ISE に LDAP を外部 ID ストアとして設定するには、この項全体を通して記載する図を参考にしてください。

abab		Liceose Warning 🔒
CISCO Identity Services Engine	Home Operations I▼ Policy I▼ Guest Access I▼ Administration I▼	
🔆 System 🛛 👰 Identity Management	🖬 Network Resources 🛛 🛃 Device Portal Management 🕞 pxGnd Services 🕞 Feed Service	L pxGrid Identity Mapping
Identities Groups External Identity St	urces Identity Source Sequences Settings	
External Identity Sources	LDAP Identity Sources General Connection Directory Organization Groups Attributes * Name LDAP_EXAMPLE Description * Schema Quatern T * Subject Objectclass InetOrgPerson * Group Objectclass posteGroup * Subject Name Attribute uid * Group Map Attribute memberUid	
	Subject Objects Contain Reference To Groups Group Objects Contain Reference To Subjects Subjects In Groups Are Stored In Member Attribute As Distinguished Name Reset Reset Reset	Ţ

[General] タブで次の属性を設定します。:

- Subject Objectclass:このフィールドは、Idifファイル内のユーザアカウントのオブジェクト クラスに対応します。LDAP設定に従います。次の4つのクラスのいずれかを使用します。
 - Top
 - Person
 - OrganizationalPerson
 - InetOrgPerson
- サブジェクト名属性:これは、ISEが特定のユーザ名がデータベースに含まれているかどう かを問い合わせたときにLDAPによって取得される属性です。このシナリオでは、エンドポ イントのユーザ名としてjohn.doeまたはjan.kowalskiを使用する必要があります。
- Group Objectclass:このフィールドは、ldifファイル内のグループのオブジェクトクラスに 対応します。このシナリオでは、cn=domainusers グループのオブジェクト クラスは posixGroup です。
- グループマップ属性:この属性は、ユーザをグループにマッピングする方法を定義します。 ldif ファイル内の cn=domainusers グループの下に、ユーザに対応する 2 つの memberUid 属性があります。

ISE には、事前設定されたスキーマ(Microsoft Active Directory、Sun、Novell)も用意されてい

ま	す	0



正しい IP アドレスと管理ドメイン設定した後、サーバとのバインディングのテスト を実行でき ます。この時点では、検索ベースがまだ設定されていないため、サブジェクトまたはグループは 取得されません。

次のタブで、件名/グループ検索ベースを設定します。これが、ISE と LDAP の結合ポイントになります。取得できるサブジェクトとグループは、統合ポイントの子となっているものだけです。

このシナリオでは、サブジェクトは OU=people からを取得され、グループは OU=groups から取 得されます。

abab		License Warning 🛕
cisco Identity Services Engine		
🔆 System 🛛 😹 Identity Management	📲 Network Resources 🛛 🛃 Device Portal Management 🛛 🔄 pxGrid Services 🛛 👼 Feed Service	Le pxGrid Identity Mapping
Identities Groups External Identity So	urces Identity Source Sequences Settings	
External Identity Sources	LDAP Identity Sources List > LDAP_EXAMPLE LDAP Identity Source General Connection Directory Organization Groups Attributes	
Certificate Authentication Profile Active Directory	Subject Search Base au-papele de-mayor de-cam Namina Contracts	
 EDAP LDAP_EXAMPLE 	* Group Search Base eurgroups,dc=maxtrc,dc=com Naming Contexts	
ADIUS Token GSA SecuriD	Search for MAC Address in Format 300 300 300 300 300 300 300 300 300 30	
	Strip start of subject name up to the fast occurrence of the separator Strip end of subject name from the first occurrence of the separator	

[Groups] タブで、LDAP から ISE にグループをインポートできます。、



WLC の設定

以下の図を参考に、802.1x 認証に対応するよう WLC を設定してください。

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

ululu cisco	MONITOR WL	ANS <u>C</u> ONTROLLER	WIREL	ess <u>s</u> ec	URITY M <u>a</u> na	GEMENT	C <u>O</u> MMANDS	HELP	FEEDBACK
WLANs	WLANs > Edi	t 'piborowi_byo	ď						
WLANs WLANs	General	Security QoS	Policy-	Mapping	Advanced				
Advanced	Layer 2	Layer 3 AAA S	ervers						
	Select AAA s Radius Serv Radius Se	servers below to ov ers rver Overwrite interfac	erride us	e of defaul abled	t servers on t	his WLAN			
		Authentication Serv	/ers	Accounting	g Servers		EAP Paramete	ers	
		Enabled		Enabled			Enable		
	Server 1	IP:10.62.145.51, Por	t:1812 🔻	IP:10.62.1	45.51, Port:181	3 🗸			
	Server 2	None	•	None		-			
	Server 3	None	-	None		-			
	Server 4	None	•	None		-			
	Server 5	None	-	None		-			
		1010	•	None		·			
ululu cisco	MONITOR WL	ANS <u>C</u> ONTROLLER	WIREL	ESS <u>S</u> EC	URITY M <u>a</u> na	GEMENT	C <u>O</u> MMANDS	HELP	FEEDBACK
WLANs	WLANs > Edi	t 'piborowi_byo	d'						
WLANs WLANs	General	Security QoS	Policy-	Mapping	Advanced				

		rapping narancea		
Layer 2	Layer 3 AAA Servers			
Colort AAA	en e		- 14/1 - 14	
SCIECT AAA	servers below to override us	e of default servers on the	S WLAN	
Radius Serv	ers			
Radius Se	rver Overwrite interface	abled		
		00100		
	Authentication Servers	Accounting Servers		EAP Parameters
	Enabled	Enabled		Enable 📃
Server 1	IP:10.62.145.51, Port:1812 +	IP:10.62.145.51, Port:1813	•	
Server 2	Mana			
Derver z	None	None		
Server 3	None •	None	•	
Server 3 Server 4	None None	None None	•	
Server 3 Server 4 Server 5	None None None None None None None None None None None None None None None	None None None	• • •	

EAP-GTC の設定

EAP-GTC は、LDAP でサポートされる認証方式の 1 つです。Cisco AnyConnect ではこの認証方 式を使用できますが、それには Network Access Manager プロファイル エディタをインストール して、プロファイルを正しく設定する必要があります。

Network Access Managerの設定も編集する必要があります(デフォルト)。この設定は次の場所 にあります。

C: > ProgramData > Cisco > Cisco AnyConnect Secure Mobility Client > Network Access Manager > system > configuration.xmlファイル

以下の図を参考に、エンドポイントに EAP-GTC を設定してください。

Client Policy Authentication Policy Profile:ili	ty Client\Net	work Access Mar	nager\system\configur	ation.xml	
Networks Name:		eap atc			Media Type
Group Membe	ership	entral to			Security Leve
In gra	ID:	Local networks			Connection Ty
					Credentials
 In all g 	roups (Global)				Cocherta
Choose Your	Network Media —				
O Wired	(802.3) Network				
		al a state provide the second state of the sec	and the second		
Select	a wired network if	the endstations will be o	onnecting to the network		
with a	traditional etherne	et cable.			
@ Wi-Fi (wireless) Network	:			
Select	a WiFi network if t	the endstations will be co	nnecting to the network		
via a w	ireless radio conn	ection to an Access Point			
SSID (r	max 32 chars):	piborowi_byod			
		Hidden Networ	k		
		Corporate Net	work		
Associ	ation Timeout	5	seconds		
Common Sett	ings				
Carint as and					
Sciptor app	ication on each us	ser sinachine to run when	Connecteu.		
			Browse Local Ma	chine	
Connection T	meout	40	seconds		

🚰 AnyConnect Profile Editor - N	letwork Access Manager	
File Help		
Network Access Manager	Networks Profile:ility Client\Network Access Manager\system\configuration.xml Security Level	Media Type
Network Groups	 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 Networks use a shared key to encrypt data between end stations and network access points. This medium security level is suitable for small/home offices. Authenticating Network Authenticating networks provide the highest level of security and are perfect for enterprise level networks. Authentication networks require radius servers, and other network infrastructure. 802. 1X Settings authPeriod (sec.) 30 startPeriod (sec.) 30 heldPeriod (sec.) 60 maxStart 3 	Security Level Connection Type User Auth Credentials
	Next Cancel	

🚰 AnyConnect Profile Editor - N	letwork Access Manager	
File Help		
AnyConnect Profile Editor - File Help Network Access Manager Clent Polcy Authentication Policy Authentication Policy Metworks Network Groups	Network Access Manager Profile:ility Client\Network Access Manager\system\configuration.xml Network Connection Type Image: 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. Image: User Connection The user connection should be used when a machine connection is not needed. A user connection will make the network available after the user has logged on. Image: 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.	Media Type Security Level Connection Type User Auth Credentials
	Next Cancel	

Client Policy Authentication Policy For Methods For Me	\configuration.xml
Network Groups	Media Type
C EAP-TLS O PEAP	Connection Type
C EAP-TTLS C 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	
EAP-GTC	
EAP-TLS, using a Certificate	
Authenticate using a Token and EAP-GTC	

强 AnyConnect Profile Editor - N	letwork Access Manager					
File Help						
Network Access Manager	Networks Profile:ility Client\Network /	Access Manager\system\configuration.x	mi Media Turo			
Network Groups	Lineratacted Identity Patterny	isha daa	Security Level			
	onprotected Identity Pattern:	John.doe	Connection Type			
	Protected Identity Pattern:	john.doe	User Auth			
			Credentials			
	User Credentials					
	O Use Single Sign On Credentials					
	Prompt for Credentials					
	Remember Forever					
	Remember while User is Logged On					
	Never Remember					
	Use Static Credentials					
	Password: passwo	rds				
	Done	Cancel				
I I						

以下の図を参考に、ISE の認証および承認ポリシーを変更してください。

ahaha									Loarse Warring 🛓
cisco	Identity Serv	vices Engine		🙆 Home	Operations •	Policy •	Guest Access	Administration	
📕 Aut	hentication	Authorization	🛃 Profiling	🔀 Posture	👸 Client Pro	ntsioning	🛃 TrustSec	🐴 Policy Elements	
Authent	ication Policy								
Define the	Authentication I	Policy by selecting th	ne protocols that ISE si	hould use to co	mmunicate with th	ne network de	vices, and the ident	ity sources that it should	use for authentication.
For Policy Policy Typ	Export go to Adr e 🔿 Simple	ninistration > System	n > Backup & Restore :	Policy Export	Page				
	МАВ	: 1	f Wired_MAB OR Wireless_MAB			Alow I	Protocols : Default I	Network Access	and
	🛃 Default		: use Internal Endpo	ints					
	Dot1X	: 1	f Wired_802.1X OR Wireless_802.1X			Allow I	Protocols : Default (Network Access	and
	🗹 Default		:USE LDAP_EXAMPL	E					
	Default Rule	(of no match) : Al	low Protocols : Defau	t Network Aco	ess	and use :	Al_User_ID_Stores		

ababa									Elsevie Warning A
cisco Ide	ntity Services Engine		🟠 Home	Operations I 🔻	Policy *	Guest Access	Adm	inistration 1 •	
🛓 Authenti	cation 🧧 🙆 Authorization	🔀 Profiling	🔀 Posture	Gient Pro	visioning	🚊 TrustSec	🐥 Poli	cy Elements	
Authorizatio	n Policy								
Define the Auth For Policy Exper	torization Policy by configuring rules l	based on identity	groups and/or o	ther conditions. Dr	rag and drop r	rules to change the or	der.		
For Policy Expor	C go to Aunineciación > system > t	second of rescure	> Policy Export	raye					
First Matched R	ule Applies +								
Exception	s (0)								
Standard									
Clanara									
Status	Rule Name	Cond	itions (identity g	roups and other o	onditions)			Permissions	
1	Users in LDAP store	if (Win on=o	eless_802.1X AN domainusers, ou=	D LDAP_EXAMPLE groups,dc=maxcro	:ExternalGroup ;,dc=com)	ps EQUALS	then	PermitAccess	
1	Wireless Black List Default	if Blad	klist AND Wirele	ss_Access			then	Blackhole_Wireless_Access	
	Profiled Cisco IP Phones	if Ciso	o-IP-Phone				then	Cisco_IP_Phones	
i 🖉	Profiled Non Cisco IP Phones	if Non,	Cisco_Profiled_P	hones			then	Non_Osco_IP_Phones	
1	Basic_Authenticated_Access	if Netv	vork_Access_Aut	thentication_Passe	d		then	PermitAccess	
	Default	if no ma	tches, then D	enyAccess					

以上の設定を適用すると、ネットワークに接続できるようになっているはずです。

🕥 Cisco AnyCo	nnect Secure Mobility Client	
	Network: Connected (10.0.13.87) eap_gtc	- III
\$ ()		albaha cisco

確認

LDAPとISEの設定を確認するには、サーバへのテスト接続を使用してサブジェクトとグループを 取得します。

CISCO Identity Services Engine	
👷 System 📑 Identity Management 📰 Network Resources 🛛 🛃 Device Portal Management 🕞 pxGrid Services 🕞 Feed Service 🕰 pxGrid Identity Mappin	ping
Identities Groups External Identity Sources Identity Source Sequences Settings	
External Identity Sources UDAP Identity Sources List > LDAP_EXAMPLE LDAP Identity Source General Connectory Description Groups Attributes	
Certificate Authentication Profile Drimmer: Senser Bind successful to 10.81.108.242.389 Senser	adam S
Active Directory Primary Server Enter Succession in 1051-1051-1051-1051-1051-1051-1051-1051	idaly 5
Besuit of testing this configuration is as follows: Enable Number of Subjects: 2	able Se
Number of Groups: 1	
Real Security Port 380 Port 380 Port 380	
Response time:1636ms	
Access O Anonymous Access Anony	lonymo
Authenticated Access CK Advise DN 3 CK Advise DN 3 CK Advise DN CK CK	thentics
Admin DN dr=Manager, dc=maxdr	
Password Password	
Secure Authentication Enable Secure Authentication Secure Authentication Enable	able Sc
Root CA Certificate Services Endpoint * Root CA Certificat	cate S
* Server Timeout 10 0. Seconds Server Timeout 10	
* Max. Admin Connections 20 (i) Max. Admin Connections 20	
Test Bind to Server	t Bind t
-	
Save Reset	

以下の図に、ISE からのレポート例を示します。

Authorsteetings 72 Researchs Int Ende	ant Sector tes Sector Transfer		
Risconfigured Supplements	Misconfigured Network Devices	RADIUS Drops @	Clent Stopped Reconding
1	0	1305	0
hav Live Sessions – 🎡 Add ar Remove Columns 🔻 🔞	Refresh 🔞 Reset Repeat County		Refiesh Every 1 minute
▼ Status All ▼ Detais Repeat Co.	ant Identity (D) Endpoint (D) (D) Endpoint P	Authentication Policy	Authorization Policy
06 04 21:50:45.538 🕥 🚡	0 john.doe C0:44:00:14:80:48 Windows7	Workst	
06-04 21:59:45.510 🔽 🚡	johnutoe 0094A:00:14:80:48 Windows7-	Workst Default >> Dot1X >> Default	Default >> Users in LDAP store PermitAccess
)verview			
Dverview Event	5200 Authentication s	ucceeded	
Dverview Event	5200 Authentication s	ucceeded	
Dverview Event Username	5200 Authentication s john.doe	ucceeded	
Dverview Event Username Endpoint Id	5200 Authentication s john.doe C0:4A:00:14:8D:4B ⊕	ucceeded	
Overview Event Username Endpoint Id Endpoint Profile	5200 Authentication s john.doe C0:4A:00:14:8D:4B ⊕ Windows7-Workstatio	ucceeded	
Overview Event Username Endpoint Id Endpoint Profile Authentication Policy	5200 Authentication s john.doe C0:4A:00:14:8D:4B ⊕ Windows7-Workstatio Default >> Dot1X >> D	ucceeded m Default	
Dverview Event Username Endpoint Id Endpoint Profile Authentication Policy Authorization Policy	5200 Authentication s john.doe C0:4A:00:14:8D:4B ⊕ Windows7-Workstatio Default >> Dot1X >> D Default >> Users in L	ucceeded on Default DAP store	

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

トラブルシュート

ここでは、この設定で発生する一般的なエラーと、そのトラブルシューティング方法を説明しま す。

- OpenLDAPのインストール後に、gssapi.dllがないことを示すエラーが発生した場合は、 Microsoft Windowsを再起動します。
- Cisco AnyConnect の configuration.xml ファイルを直接編集できない場合があります。新しい構成を別の場所に保存してから、そのファイルで古いファイルを置き換えてください。
- 認証レポートに、次のエラーメッセージが表示されます。

<#root>

Authentication method is not supported by any applicable identity store

このエラー メッセージは、選択した認証方式が LDAP でサポートされないことを意味しま す。

同じレポート内に、認証プロトコル としてサポートされている方式(EAP-GTC、EAP-TLS、 PEAP-TLS)のいずれかが示されていることを確認してください。

• 認証レポートで、サブジェクトがIDストアで見つからなかった場合、レポートからのユーザ 名が、LDAPデータベース内のどのユーザのサブジェクト名属性とも一致しません。

このシナリオでは、この属性の値が uid に設定されているため、ISE は一致を見つけようとする ときに、LDAP ユーザの uid 値を調べます。

 サーバへのバインドテスト中にサブジェクトとグループが正しく取得されなかった場合、検 索ベースの設定が正しくありません。

LDAP 階層は、リーフからルートの方向および dc(複数の単語で構成可能)で指定する必要があ ることに注意してください。

レント:WLC側でEAP認証のトラブルシューティングを行うには、シスコのドキュメント『
<u>WLANコントローラ(WLC)でのEAP認証の設定例</u>』を参照してください。

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人に よる翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっ ても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性につ いて法的責任を負いません。原典である英語版(リンクからアクセス可能)もあわせて参照する ことを推奨します。