配置ISE以与LDAP服务器集成

目录

简介

広夫条件

要求

使用的组件

背景信息

配置

図格图

配置OpenLDAP

努OpenLDAP与ISE集成

配置 WLC

配置 EAP-GTC

数障排除

简介

本文档介绍如何配置思科身份服务引擎(ISE),以便与思科LDAP服务器集成。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档中的信息基于以下软件和硬件版本:

- 带补丁2的思科ISE版本1.3
- 安装了OpenLDAP的Microsoft Windows版本7 x64
- 思科无线局域网控制器(WLC)版本8.0.100.0
- 适用于Microsoft Windows的Cisco AnyConnect版本3.1
- 思科网络访问管理器配置文件编辑器

注:本文档对使用LDAP作为ISE身份验证和授权的外部身份源的设置有效。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原 始(默认)配置。如果您的网络处于活动状态,请确保您了解所有命令的潜在影响。

背景信息

LDAP支持以下身份验证方法:

- 可扩展身份验证协议 通用令牌卡(EAP-GTC)
- 可扩展身份验证协议 传输层安全(EAP-TLS)
- 受保护的可扩展身份验证协议 传输层安全(PEAP-TLS)

配置

本节介绍如何配置网络设备并将ISE与LDAP服务器集成。

网络图

在此配置示例中,终端使用无线适配器以便与无线网络关联。

WLC上的无线LAN(WLAN)配置为通过ISE对用户进行身份验证。在ISE上,LDAP配置为外部身份库 。

下图说明了使用的网络拓扑:



配置OpenLDAP

OpenLDAP for Microsoft Windows的安装通过GUI完成,并且非常简单。默认位置为C: > OpenLDAP。安装后,您应该看到以下目录:

Name	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	
📗 ldifdata	6/4/2015 11:03 AM	File folder	
\mu Readme	6/3/2015 5:06 PM	File folder	
\mu replica	6/3/2015 5:06 PM	File folder	
🐌 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
slapaci.exe	5/11/2015 10:59 PM	Application	3,711 KB

请特别注意以下两个目录:

- ClientTools 此目录包含一组用于编辑LDAP数据库的二进制文件。
- Idifdata 这是应存储具有LDAP对象的文件的位置。

将此结构添加到LDAP数据库:



在Root目录下,必须配置两个组织单位(OU)。OU=groups OU应有一个子组(在本例中为 cn=domainusers)。

OU=people OU定义属于cn=domainusers组的两个用户帐户。

要填充数据库,必须先创建ldif文件。前面提到的结构是从以下文件创建的:

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

要将对象添加到LDAP数据库,请使用Idapmodify二进制:

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_prepare_socket: 496 ldap_pvt_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"

将OpenLDAP与ISE集成

使用本部分中的映像中提供的信息,以便将LDAP配置为ISE上的外部身份库。

Cisco Identity Services Engine	Home Operations I Policy I Guest Access I Administration I Administratin Adminis
System Identity Management Network Identities Groups External Identity Sources External Identity Sources LDAP Identity Sources Image: Ima	twork Resources Reported Portal Management Report Resources Report Resource Sequences Settings P Identity Source List > LDAP_EXAMPLE AP Identity Source General Connection Directory Organization Groups Attributes
Identities Groups External Identity Sources External Identity Sources LDAP IS Image: Second Sources LDAP IS Image: Second Sources Image: Sources Image: Sources Image: Sources Ima	Identity Source Sequences Settings Identity Source List > LDAP_EXAMPLE AP Identity Source General Connection Directory Organization Groups Attributes
External Identity Sources	AP Identity Source General Connection Directory Organization Groups Attributes
RSA SecurID	* Name LDAP_EXAMPLE Description
	Subject Name Attribute uid Certificate O Subject Objects Contain Reference To Groups
۲	Group Objects Contain Reference To Subjects
	Subjects in Groups Are Stored in Member Attribute As [Distinguished Name 7]

可以从General选项卡配置以下属性:

- Subject Objectclass 此字段对应于Idif文件中用户帐户的对象类。根据LDAP配置,请使用 以下四个类之一:
 - 。顶部
 - 。人员
 - 。组织人员
 - InetOrgPerson
- Subject Name Attribute 这是当ISE查询数据库中是否包含特定用户名时由LDAP检索的属性。在这种情况下,您必须使用john.doe或jan.kowalski作为终端上的用户名。
- Group Objectclass 此字段与ldif文件中组的对象类对应。在此方案中,cn=domainusers组的对象类是posixGroup。
- 组映射属性 此属性定义如何将用户映射到组。在Idif文件中的cn=domainusers组下,可以 看到与用户对应的两个memberUid属性。

ISE还提供一些预配置的方案(Microsoft Active Directory、Sun、Novell):

cisco Identity Services Engine	
The Administration T Policy T Guest Acress T Administration T	
🔆 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 LDAP Identity Sources Ust > LDAP_DCAMPLE \u03c6 \u03c6	
Active Directory Primary Server Si	econdary S
	Enable Se
ADDUS Token * Hostname/P 10.61.106.242 E Hostname/P	
Port 389	389
Access Anonymous Access Access Access Admin DN * Cn=Manager, dc=rease Admin DN * Password * •••••• Password *	Anonymo Authentic
Secure Authentication 🗌 Enable Secure Authentication Secure Authentication	Enable Sc
Root CA Certificate Services Endpoint * Root CA C	Certificate Se
Server Timeout 10 Geconds Server Timeout 1 Max. Admin Connections 20 Test Bind to Server	10 20 Test Bind t

在设置正确的IP地址和管理域名后,您可以Test Bind到服务器。此时,由于尚未配置搜索库,您不 会检索任何主题或组。

在下一个选项卡中,配置主题/组搜索库。这是ISE到LDAP的加入点。您只能检索作为加入点子项的 主题和组。

在此场景中,检索OU=people中的主题和OU=groups中的组:

alulu		License Warning 🛕
CISCO Identity Services Engine		
🔆 System 🛛 😹 Identity Management	📲 Network Resources 🛛 🛃 Device Portal Management 🔄 pxGrid Services 🕞 Feed Service	L 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=mextrt,dc=com * Group Search Base ou=groups,dc=mextrt,dc=com * Group Search Base ou=groups,dc=mextrt,dc=com Search for MAC Address in Format [set sec set	

在Groups选项卡中,您可以从ISE上的LDAP导入组:



配置 WLC

使用这些映像中提供的信息配置WLC进行802.1x身份验证:

սիսիս 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 MAC Filtering Fast Transition Fast Transition Protected Management Frame PMF Disabled WPA+WPA2 Parameters
	WPA Policy WPA2 Policy-AES
	Authentication Key Management
	802.1X II Enable

ululu cisco	MONITOR WL	ANS <u>C</u> ONTROLLER	WIRELE	55 <u>s</u> ecurity	MANAGEMENT	C <u>O</u> MMANDS	HELP	EEEDBACK
WLANs	WLANs > Edi	t 'piborowi_byo	ď					
WLANs WLANs Advanced	General S	Security QoS	Policy-M	apping Adv	vanced			
	Select AAA s Radius Serve Radius Server 1 Server 2 Server 3 Server 4 Server 5 Server 6	Servers below to over ers rver Overwrite interfact Authentication Serv C Enabled IP:10.62.145.51, Port None None None None None None	erride use erride use ters A t:1812 • • •	of default serv led ccounting Serv Enabled IP:10.62.145.51, None None None None	Port:1813	EAP Paramet	ers	
uluih cisco	MONITOR WL	ANS <u>C</u> ONTROLLER	WIRELE	55 <u>s</u> ecurity	MANAGEMENT	C <u>O</u> MMANDS	HELP	<u>F</u> EEDBACK
WLANs	WLANs > Edi	t 'piborowi_byo	d'					

WLANs General	Security QoS Policy-	Mapping Advanced	
Advanced Layer 2	Layer 3 AAA Servers		
Select AAA	servers below to override us	e of default servers on this WLAN	
Radius Ser	vers		
Radius 5	erver Overwrite interface 🛛 🗏 En	abled	
	Authentication Comme	Accounting Comment	EAD Deservations
	Autoentication servers	Accounting servers	EAF Parameters
	Enabled	Enabled	Enable 🖾
Server 1	IP:10.62.145.51, Port:1812 +	IP:10.62.145.51, Port:1813 -	
Server 2	None -	None 🔹	
Server 3	None 👻	None 👻	
Server 4	None 👻	None 👻	
Server 5	None 👻	None 👻	
Server 6	None -	None -	

配置EAP-GTC

LDAP支持的身份验证方法之一是EAP-GTC。它在Cisco AnyConnect中可用,但必须安装网络访问 管理器配置文件编辑器才能正确配置配置文件。

您还必须编辑网络访问管理器配置,默认情况下,该配置位于以下位置:

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

使用这些映像中提供的信息在终端上配置EAP-GTC:

Signops Name: eap_gtc Media Type Group Membership In group: Local networks Security Level Ornection Typ In group: Local networks User Auth Ornection Typ In all groups (Global) Choose Your Network Media Orredentials Ornection Typ Choose Your Network Media Orredentials Orredentials Ornection Typ Choose Your Network Media Orredentials Orredentials Ornection Typ Select a wired network if the endstations will be connecting to the network with a traditional ethernet cable. Ornection Type Ornection Timeout Select a WiFi network if the endstations will be connecting to the network via a wireless radio connection to an Access Point. SSID (max 32 chars): pborowi_byod Hidden Network Corporate Network Association Timeout Seconds Common Settings Script or application on each user's machine to run when connected. Browse Local Machine Connection Timeout 40 seconds Description	ent Policy thentication Policy Profile:ility Client\N	etwork Access Manager\system\configuration.xml	
Comps Intervent Security Level Groups In group: Local networks Connection Typ In all groups (Global) Choose Your Network Media Vired (802.3) Network Credentials Choose Your Network Media Wired (802.3) Network Select a wired network if the endstations will be connecting to the network with a traditional ethernet cable. Wiref (Wireless) Network Select a WiFi network if the endstations will be connecting to the network via a wireless radio connection to an Access Point. SSID (max 32 chars): pborowi_byod Hidden Network Corporate Network Association Timeout Seconds Common Settings Script or application on each user's machine to run when connected. Browse Local Machine Connection Timeout 40 seconds Seconds	tworks	and obt	Media Type
Connection Typ In group: Local networks In groups (Global) Choose Your Network Media Wired (802.3) Network Select a wired network if the endstations will be connecting to the network with a traditional ethernet cable. WH-FI (wireless) Network Select a WiFi network if the endstations will be connecting to the network via a wireless radio connection to an Access Point. SSID (max 32 chars): pborowi_byod Hidden Network Corporate Network Association Timeout 5 Script or application on each user's machine to run when connected. Browse Local Machine Connection Timeout 40	work Groups Group Membership	cap_gu	Security Level
In group: Local networks In groups (Global) Choose Your Network Media Image: Wired (802.3) Network Select a wired network if the endstations will be connecting to the network with a traditional ethernet cable. WirFi (wireless) Network Select a WiFi network if the endstations will be connecting to the network via a wireless radio connection to an Access Point. SSED (max 32 chars): Image: piborowi_byod Image: Corporate Network Association Timeout 5 Script or application on each user's machine to run when connected. Browse Local Machine Connection Timeout 40	aroup remodiany		Connection Type
In all groups (Global) Choose Your Network Media Wired (802.3) Network Select a wired network if the endstations will be connecting to the network with a traditional ethernet cable. WI-Fi (wireless) Network Select a WiFi network if the endstations will be connecting to the network via a wireless radio connection to an Access Point. SSID (max 32 chars): ploorowi_byod Hidden Network Corporate Network Association Timeout 5 seconds Common Settings Script or application on each user's machine to run when connected. Connection Timeout 40 seconds	In group:	Local networks v	User Auth
Choose Your Network Media Wired (802.3) Network Select a wired network if the endstations will be connecting to the network with a traditional ethernet cable. WI-FI (wireless) Network Select a WIF network if the endstations will be connecting to the network via a wireless radio connection to an Access Point. SSID (max 32 chars): plborowi_byod Hidden Network Comporte Network Association Timeout 5 seconds Common Settings Script or application on each user's machine to run when connected. Browse Local Machine Connection Timeout 40 seconds	 In all groups (Global) 		Credentials
Image: Select a wired (802.3) Network Select a wired network if the endstations will be connecting to the network with a traditional ethernet cable. Image:	Choose Your Network Media		
Select a wired network if the endstations will be connecting to the network with a traditional ethernet cable. Image: Mil-Fi (wireless) Network Select a WiFi network if the endstations will be connecting to the network via a wireless radio connection to an Access Point. SSID (max 32 chars): piborowi_byod Image: Hidden Network Image: Corporate Network Association Timeout 5 Script or application on each user's machine to run when connected. Image: Decomposition Timeout 40 seconds	Wired (802.3) Network	k	
with a traditional ethernet cable. Image: Wi-Fi (wireless) Network Select a WiFi network if the endstations will be connecting to the network via a wireless radio connection to an Access Point. SSID (max 32 chars): piborowi_byod Hidden Network Corporate Network Association Timeout 5 Script or application on each user's machine to run when connected. Encomection Timeout 40 seconds	Select a wired network	k if the endstations will be connecting to the network	
WI-Fi (wireless) Network Select a WFi network if the endstations will be connecting to the network via a wireless radio connection to an Access Point. SSID (max 32 chars): piborowi_byod Hidden Network Corporate Network Association Timeout 5 Script or application on each user's machine to run when connected. Browse Local Machine Connection Timeout 40	with a traditional ether	rnet cable.	
Select a WIFi network if the endstations will be connecting to the network via a wireless radio connection to an Access Point. SSID (max 32 chars): piborowi_byod Hidden Network Corporate Network Association Timeout 5 Script or application on each user's machine to run when connected. Browse Local Machine Connection Timeout 40	Wi-Fi (wireless) Netwo	ork	
via a wireless radio connection to an Access Point. SSID (max 32 chars): piborowi_byod Hidden Network Corporate Network Association Timeout 5 Script or application on each user's machine to run when connected. Browse Local Machine Connection Timeout 40	Select a WiFi network	if the endstations will be connecting to the network	
SSID (max 32 chars): piborowi_byod Hidden Network Corporate Network Association Timeout 5 Script or application on each user's machine to run when connected. Connection Timeout 40 seconds	via a wireless radio co	nnection to an Access Point.	
Hidden Network Corporate Network Association Timeout 5 Script or application on each user's machine to run when connected. Browse Local Machine Connection Timeout 40	SSID (max 32 chars):	piborowi_byod	
Corporate Network Association Timeout 5 seconds Common Settings Script or application on each user's machine to run when connected. Browse Local Machine Connection Timeout 40 seconds		Eirklen Network	
Association Timeout 5 seconds Common Settings Script or application on each user's machine to run when connected. Browse Local Machine Connection Timeout 40 seconds		Corporate Network	
Common Settings Script or application on each user's machine to run when connected. Browse Local Machine Connection Timeout 40 seconds	Approxiption Times t	E arrada	
Common Settings Script or application on each user's machine to run when connected. Browse Local Machine Connection Timeout 40 seconds	Association Inneouc	5 Seconds	
Browse Local Machine Connection Timeout 40	Association Timeout Common Settings	5 seconds	
Browse Local Machine Connection Timeout 40 seconds			
Connection Timeout 40 seconds		Browse Local Machine	
Connection Imeout 40 seconds	Constant Toront		
	Connection Timeout	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						
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 Association Mode WPA2 Enterprise (AES) 	Security Level Connection Type User Auth Credentials					
	Next Cancel						

🚰 AnyConnect Profile Editor - N	letwork Access Manager	
File Help		
AnyConnect Profile Editor - I File Help Network Access Manager Clent Polcy Authentication Policy Networks 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 FAD Methods FAD Me	\configuration.xml
Network Groups	Media Type
© EAP-TLS	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	

🚰 AnyConnect Profile Editor - N	Network Access Manager		
File Help			
Network Access Manager	Networks Profile:ility Client\Network	Access Manager\system\configuration.xml	Media Type
Network Groups	Lipprotected Identity Pattern	inho doe	Security Level
	onprotected identity Pattern.	Junitade	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 i	s Logged On	
	Never Remember		
	💮 Use Static Credentials		
	Password: passwo	rds	
	Done	Cancel	

使用这些映像中提供的信息更改ISE上的身份验证和授权策略:

ahaha	1000									License Warning 🔥
cisco	Identity Serv	rices Engine		(a) Home	Operations •	Policy •	Guest Access	Administration		
📕 Aut	hentication	O Authorization	Profiling	💽 Posture	👸 Client Pro	ovisioning	🚮 TrustSec	🐴 Policy Elements		
Authent	ication Policy									
Define the	Authentication P	olicy by selecting	the protocols that ISE s	hould use to co	mmunicate with th	he network de	vices, and the ident	ity sources that it should	d use for authentication.	-
For Policy 0 Policy Typ	Export go to Adm e 🔿 Simple	 inistration > Syst Rule-Based 	em > Backup & Restore :	> Policy Export	Page					
	МАВ	:	If Wired_MAB OR Wireless_MAB			Allow F	rotocols : Default	Network Access	and	
	🗹 Default		: use Internal Endpo	ints						
	Dot1X	:	If Wired_802.1X OR Wireless_802.1X			Alow F	rotocols : Default	Network Access	and	
	🗹 Default		: USR LDAP_EXAMPL	E						
2	Default Rule	(If no match) :	Allow Protocols : Defau	it Network Acco	155	and use :	Al_User_ID_Stores			

ahaha										License Warning A
CIS	CISCO Identity Services Engine			A Home Operations I▼ Policy I▼ Guest Acce			Guest Access	Adm	inistration 1 💌	
4	Authentic	ation 💿 Authorization	🔀 Profiling	🖄 Posture	Gient Pro	visioning	🚊 TrustSec	🐥 Poli	cy Elements	
Auth	orization	Policy								
Define	the Auth	orization Policy by configuring rules	based on identity (groups and/or o	ther conditions. D	rag and drop	rules to change the o	order.		
For Po	icy Export	go to Administration > System > I	Sackup & Restore	> Policy Export	Page					
First N	Astched Ru	ile Applies 🔹								
⊁в	ceptions	(0)								
Sta	ndard									
_	Status	Rule Name	Cond	tions (identity g	roups and other o	onditions)			Permissions	
1	2	Users in LDAP store	if (Wire cn=d	less_802.1X AN omainusers.ou=	D LDAP_EXAMPLE groups,dc=maxer	:ExternalGrou c,dc=com)	ps EQUALS	then	PermitAccess	
1	×	Wireless Black List Default	if Black	dist AND Wirele	ss_Access			then	Blackhole_Wireless_A	Access
1	2	Profiled Cisco IP Phones	if Cisco	-IP-Phone				then	Cisco_IP_Phones	
Ĩ	~	Profiled Non Cisco IP Phones	f Non_	Cisco_Profiled_I	hones			then	Non_Osco_IP_Phone	25
÷	2	Basic_Authenticated_Access	if Netw	ork_Access_Au	thentication_Passe	d		then	PermitAccess	
	V	Default	if no mat	ches, then D	enyAccess					

应用配置后,您应该能够连接到网络:

Sisco AnyCor	nnect Secure Mobility Client		
	Network: Connected (10.0.13.87) eap_gtc	− الله ⊖	
_			
in and the second			denotes de
\$ (i)			altalta cisco

验证

要验证LDAP和ISE配置,请检索与服务器的测试连接的主题和组:

սիսիս					Liow	we Warning A
cisco Identity Services Engine	🙆 Home 0	perations 💌 Policy 🗐	Guest Access	tministration I 🔻		
🔆 System 🛛 👹 Identity Management	🖬 Network Resources 🛛 🛃 De	evice Portal Management	pxGnd Services	Feed Service	Le pxGnd Identit	y Mapping
Identities Groups External Identity St	urces Identity Source Sequer	nces Settings				
External Identity Sources	LDAP Identity Sources List > LDAP LDAP Identity Source General Conne	EXAMPLE	nanization Group	s Attributos		
Certificate Authentication Profile	1	rimary Server	Bind successful to 10.61.	108.242.389		Secondary S
			Result of testing this conf Number of Subjects: 2 Number of Groups: 1	iguration is as follows:		Enable S
 EAOIUS Token 	* Hostname/IP	10.61.106.242			Hostname/IP	
RSA SecurID	* Port	389	Response time:1636ms		Port	389
	Access (Admin DN * Password *	Anonymous Access Authenticated Access or - Manager, dc=maxor ******	_	СК	Access Admin DN Password	 Anonymo Authentica
	Secure Authentication [Enable Secure Authentical	lion	Sec	ure Authentication	Enable Se
	Root CA	Certificate Services Endpoint	*		Root CA	Certificate Se
	* Server Timeout [* Max. Admin Connections [10	#Beconds #	Max. Ac	Server Timeout	10 20
	1	Test Bind to Server				Test Bind t
				11		_
	Save Reset					

以下图像说明来自ISE的示例报告:

cisco Identity Se	ervices Engine		(Home Op	erations T Policy T	Guest Access 🔻 Ad	ministration =	Liener Wroning 🔏 🛛 Vedit 🛛 Joh
D Authentications	🚊 Reports	👿 Endpoint Protecti	on Service 💦 💊 1	Troubleshoot			
Msconfigur	red Supplicants 🔞 1	м	sconfigured Network O	Devices (3)	RADIUS Dr. 1305	ipa (i)	Clent Stopped Responding @ 0
a Show Live Sessions	🎲 Add ar Remove C	alumns 🔻 🏀 Refresh 🛛 🔞	Reset Repeat Counts				Refresh Every 1 minute
me	• Status Al • Details	Repeat Count	Endpoint]	D D Endpoint Prof	Authentication Pole	Authorization Po	ky ① Authorization Profiles
015-06-04 21:50:45.5 015-06-04 21:59:45.5	38 🚺 🔓	0 johnudo johnudo	e C0:4A:00:1 e C0:4A:00:1	4:80:48 Windows7-Wo 4:80:48 Windows7-Wo	rkst rkst Default >> Dot1X >	> Default — Default >> Users	s in LDAP store PermitAccess
Overvie	w						
Event			5200 Au	thentication su	cceeded		
Username	e		iohn.doe	• •			

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

2015-06-04 21:59:45.509
2015-06-04 21:59:45.51
ise13
5200 Authentication succeeded
john.doe
C0:4A:00:14:8D:4B
Windows7-Workstation
LDAP_EXAMPLE
Workstation
0a3e9465000010035570b956
dot1x
PEAP (EAP-GTC)
Framed
cn=domainusers,ou=groups,dc=maxcrc,dc=com
uid=john.doe,ou=people,dc=maxcrc,dc=com

故障排除

本节介绍此配置遇到的一些常见错误以及如何排除这些错误:

- 安装OpenLDAP后,如果您遇到错误以指示gssapi.dll丢失,请重新启动Microsoft Windows。
- 可能无法直接编辑Cisco AnyConnect的configuration.xml文件。将新配置保存到其他位置,然 后使用它替换旧文件。
- 在身份验证报告中,出现以下错误消息:

<#root>

Authentication method is not supported by any applicable identity store

此错误消息表明LDAP不支持您选择的方法。

确保同一报告中的身份验证协议显示其中一个受支持的方法(EAP-GTC、EAP-TLS或PEAP-TLS)。

 在身份验证报告中,如果您注意到在身份存储中找不到主题,则报告中的用户名与LDAP数据 库中任何用户的Subject Name Attribute不匹配。

在此方案中,此属性值设置为uid,这意味着ISE在尝试查找匹配项时查找LDAP用户的uid值。

• 如果在绑定到服务器测试期间未正确检索主题和组,则搜索库的配置不正确。

请记住,必须从枝叶到根和dc(可包含多个单词)指定LDAP层次结构。

✔ 提示:要对WLC端的EAP身份验证进行故障排除,请参阅<u>使用WLAN控制器的EAP身份验证</u> (WLC)配置示例
思科文档。

关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言,希望全球的用户都能通过各 自的语言得到支持性的内容。

请注意:即使是最好的机器翻译,其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任,并建议您总是参考英文原始文档(已提供 链接)。