配置ISE以與LDAP伺服器整合

目錄

問介
 必要條件
 憲求
 採用元件
 引景資訊
 設定
 網路圖表
 配置OpenLDAP與ISE整合
 設定WLC
 配置EAP-GTC

<u>驗證</u>

<u>疑難排解</u>

簡介

本文檔介紹如何配置思科身份服務引擎(ISE)以便與思科LDAP伺服器整合。

必要條件

需求

本文件沒有特定需求。

採用元件

本檔案中的資訊是根據以下軟體和硬體版本:

- 帶補丁2的Cisco ISE版本1.3
- 安裝了OpenLDAP的Microsoft Windows版本7 x64
- Cisco無線LAN控制器(WLC)版本8.0.100.0
- 適用於Microsoft Windows的Cisco AnyConnect版本3.1
- 思科網路存取管理員設定檔編輯器

注意:對於使用LDAP作為ISE身份驗證和授權的外部身份源的設定,本文檔有效。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除(預設))的組態來啟動。如果您的網路運作中,請確保您瞭解任何指令可能造成的影響。

背景資訊

LDAP支援以下身份驗證方法:

- 可擴充驗證通訊協定 通用權杖卡(EAP-GTC)
- 可擴展身份驗證協定 傳輸層安全(EAP-TLS)
- 受保護的可擴展身份驗證協定 傳輸層安全(PEAP-TLS)

設定

本節介紹如何配置網路裝置並將ISE與LDAP伺服器整合。

網路圖表

在此配置示例中,終端使用無線介面卡以便與無線網路關聯。

WLC上的無線LAN(WLAN)設定為透過ISE驗證使用者。在ISE上,LDAP配置為外部身份庫。 此圖說明所使用的網路拓撲:



配置OpenLDAP

Microsoft Windows的OpenLDAP安裝通過GUI完成,並且非常簡單。預設位置為C: > OpenLDAP。 安裝後,您應該會看到以下目錄:

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	
📔 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	
\mu 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

請特別注意以下兩種目錄:

- ClientTools 此目錄包含一組用於編輯LDAP資料庫的二進位制檔案。
- Idifdata 這是您應該儲存具有LDAP對象的檔案的位置。

將此結構新增到LDAP資料庫:



在Root目錄下,必須配置兩個組織單位(OU)。OU=groups OU應具有一個子組(在本例中為 cn=domainusers)。

OU=people OU定義屬於cn=domainusers組的兩個使用者帳戶。

要填充資料庫,必須首先創建ldif檔案。前面提到的結構是根據以下檔案建立的:

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

若要將對象新增到LDAP資料庫,請使用Idapmodify binary:

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"

將OpenLDAP與ISE整合

使用本節中影象提供的資訊,將LDAP配置為ISE上的外部身份庫。

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	LepsGrid Identity Mapping
Identities Groups External Identity So	urces Identity Source Sequences Settings	
External Identity Sources	LDAP Identity Sources List > LDAP_DXAMPLE LDAP Identity Source General Connection Directory Organization Groups Attributes * Name LDAP_DXAMPLE Description * Schema Custorn * Subject Objectclass InetOrgPerson * Subject Name Attribute uid Certificate Attribute uid reformed attribute member/Uid	
	Save Reset Save Reset	Ţ

可以從General頁籤配置以下屬性:

- Subject Objectclass 此欄位與ldif檔案中使用者帳戶的對象類對應。根據LDAP配置。請使 用以下四個類之一:
 - 。頂端
 - 。人員
 - 組織人員
 - InetOrgPerson
- Subject Name Attribute 這是LDAP在ISE查詢資料庫中是否包含特定使用者名稱時檢索的屬 性。在此方案中,必須使用john.doe或jan.kowalski作為端點上的使用者名稱。
- Group Objectclass 此欄位與ldif檔案中組的對象類對應。在此方案中,cn=domainusers組的object類是posixGroup。
- 組對映屬性 此屬性定義如何將使用者對映到組。在Idif檔案的cn=domainusers組下,可以 看到兩個與使用者對應的memberUid屬性。

ISE還提供一些預配置的架構(Microsoft Active Directory、Sun、Novell):

ababa	Le	ense Warning 🔥
cisco Identity Services Engine		
🔆 System 🛛 💆 Identity Management	🞬 Network Resources 🛛 😹 Device Portal Management 🛛 🙀 pxGrid Services 🛛 🙀 Feed Service 🛛 🔩 exGrid Iden	tity Mapping
Identities Groups External Identity S	turces Identity Source Sequences Settings	
External Identity Sources	LDAP Identity Sources List > LDAP_CXAMPLE LDAP Identity Source General Connection Directory Organization Groups Attributes	
Active Directory	Primary Server	Secondary S
T EDAP		Enable Se
RADUS Token	* Hostname/P 10.61.106.242 U Hostnameri * Part 290	4 200
	P01 309	009
	Access Anonymous Access Acces	s 💿 Anonymo
	Admin DN 1 on=Manager.dc=rmaxor.dc=com	
	Password * Password *	8
	Secure Authentication Enable Secure Authentication Secure Authentication	n 🗌 Enable Sc
	Root CA Certificate Services Endpoint Root C	Certificate Se
	*Server Timeout 10 CScconds Server Timeou	1 0
	* Max. Admin Connections 20 (1) Max. Admin Connection	8 20
	Test Bind to Server	Test Bind t
	۰. n	
	Save Reset	

在設定正確的IP地址和管理域名後,您可以測試繫結到伺服器。此時,您不會檢索任何主題或組 ,因為尚未配置搜尋庫。

在下一個頁籤中,配置主題/組搜尋庫。這是ISE到LDAP的連線點。您只能檢索作為加入點子項的主 題和組。

在此方案中,將檢索OU=people中的主題和OU=groups中的組:

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 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=maxerc,dc=com * Group Search Base ou=groups,dc=maxerc,dc=com * Group Search Base ou=groups,dc=maxerc,dc=com * Group Search Base ou=groups,dc=maxerc,dc=com * Subject Search for MAC Address in Format ou=groups,dc=maxerc,dc=com Search for MAC Address in Format ou=groups,dc=maxerc,dc=com Strip start of subject name up to the last occurrence of the separator image: strip end of subject name from the first occurrence of the separator	

在Groups頁籤中,您可以從ISE上的LDAP匯入組:



設定WLC

使用這些映像中提供的資訊來設定WLC以進行802.1x驗證:

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 VPA+WPA2
	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	d'					
VLANs WLANS	General S	Security QoS	Policy-M	apping Adv	anced			
	Select AAA s Radius Server Radius Server Server 1 Server 2 Server 3 Server 4 Server 5 Server 6	servers below to over ers rver Overwrite interface Authentication Server I Enabled IP:10.62.145.51, Por None None None None None None	erride use erride use ters A t:1812 • 1 • 1 • 1 • 1 • 1	of default serve ed Enabled P:10.62.145.51, Jone Jone Jone Jone	ers on this WLAN	EAP Paramet	ers	
cisco	MONITOR WL	ANS <u>C</u> ONTROLLER	W <u>I</u> RELE:	55 <u>s</u> ecurity	MANAGEMENT	C <u>O</u> MMANDS	HELP	<u>F</u> EEDBACK
WLANs	WLANs > Edi	t 'piborowi_byo	d'					

General	Security QoS Policy-	Mapping Advanced			
Layer 2	Layer 3 AAA Servers				
Select AAA	servers below to override us	e of default servers on this	s WLAN		
Radius Serv	ers				
Radius Se	rver Overwrite interface 🛛 🗏 En	abled			
	Authentication Servers	Accounting Servers		EAP Paramet	ers
	Authentication Servers	Accounting Servers		EAP Paramet	ers
Server 1	Authentication Servers Image: Server serve	Accounting Servers C Enabled IP:10.62.145.51, Port:1813	Ŧ	EAP Paramet	ers 📃
Server 1 Server 2	Authentication Servers Image: Server serve	Accounting Servers Enabled IP:10.62.145.51, Port:1813 None	•	EAP Paramet	E .
Server 1 Server 2 Server 3	Authentication Servers Enabled IP:10.62.145.51, Port:1812 None None	Accounting Servers C Enabled IP:10.62.145.51, Port:1813 None None	• •	EAP Paramet	E
Server 1 Server 2 Server 3 Server 4	Authentication Servers Enabled IP:10.62.145.51, Port:1812 None None None None	Accounting Servers Enabled IP:10.62.145.51, Port:1813 None None None	* * *	EAP Paramete	E
Server 1 Server 2 Server 3 Server 4 Server 5	Authentication Servers Enabled IP:10.62.145.51, Port:1812 None	Accounting Servers Enabled IP:10.62.145.51, Port:1813 None None None None		EAP Paramete	E .

配置EAP-GTC

LDAP支援的身份驗證方法之一是EAP-GTC。它在Cisco AnyConnect中可用,但必須安裝網路訪問 管理器配置檔案編輯器才能正確配置配置檔案。

您還必須編輯網路訪問管理器配置,預設情況下該配置位於以下位置:

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

使用這些映像中提供的資訊在終端上配置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 accorde	
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	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 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 - N 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	

使用這些映像中提供的資訊更改ISE上的身份驗證和授權策略:

ahaha	1000									License Warning 🔥
cisco	Identity Services 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			

CISCO Identity Services Engine										License Warning AL
					Policy 1 *	Policy 🔻 Guest Access 💌 Adr		inistration 1 =		
4	Authentic	ation 😑 Authorization	🔀 Profiling	🔀 Posture	Gient Pro	visioning	🚊 TrustSec	🐥 Polis	ky Elements	
Authorization Policy										
Define the Authorization Policy by configuring rules based on identity groups and/or other conditions. Drag and drop rules to change the order.										
For Pol	icy Export	go to Administration > System > I	Backup & Restore	> Policy Export	Page					
First M	latched Ru	ile Applies 👻								
▶ Ex	ceptions	(0)								
Sta	ndard									
	Status	Rule Name	Condi	tions (identity g	roups and other o	onditions)			Permissions	
1		Users in LDAP store	if (Wire cn=d	less_802.1X AN lomainusers, ou=	D LDAP_EXAMPLE groups,dc=maxtre	:ExternalGrou c,dc=com)	ps EQUALS	then	PermitAccess	
ł	2	Wireless Black List Default	if Black	dist AND Wirele	ss_Access			then	Blackhole_Wireless_Access	
Ē	2	Profiled Cisco IP Phones	if Cisco	-IP-Phone				then	Cisco_IP_Phones	
ī	2	Profiled Non Cisco IP Phones	if Non_	Cisco_Profiled_F	hones			then	Non_Osco_IP_Phones	
ł	2	Basic_Authenticated_Access	if Netw	ork_Access_Au	thentication_Passe	d		then	PermitAccess	
	X	Default	if no mat	ches, then D	enyAccess					

套用組態後, 您應該能連線到網路:

S Cisco AnyCo	nnect Secure Mobility Client		23
	Network: Connected (10.0.13.87) eap_gtc	e III)
Ö (i)			

驗證

為了驗證LDAP和ISE配置,請檢索與伺服器具有測試連線的主題和組:

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
			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					

以下影象說明來自ISE的示例報告:

lialia Lisco Identity	Services Engine	Ê	Home Operations	Policy T Gu	est Access 💌 Administration I	Licence Max	aine 🔏 Xedil Adai
D Authentications	💼 🚊 Reports	Endpoint Protection Serv	ce 💦 💊 Troublesho	at			
Misconfig	jured Supplicanta 🔅 1	Msconfy	ared Network Devices	D	RADIUS Drops © 1305	Client Sto	oped Responding (3) O
Show Uve Sessions	🙀 Add or Renove	Columns 🔻 🏀 Refresh 🛛 🔞 Reset i	lepeat Counts			Refreat	Every 1 minute
TR.	▼ Status Ali ▼ Detai	s Repeat Count	Endpoint ID	Endpoint Profile 3	Authentication Policy	Authorization Policy	Authorization Profiles
15-06-04 21:50:45	.538 🕥 🔒	0 john.doe	C0:4A:00:14:80:48	Windows7-Workst			
15-06-04 21:59:45	.510 🔽 🚡	(ohnutice	60x4A:00:14:80x48	Windows7-Workst	Default >> Dot1X >> Default	Default >> Users in LDAP store	PermitAccess
Overvi	ew						
Event			5200 Authenti	cation succe	eded		
			a har da a Ø				

Usernamejohn.doeEndpoint IdC0:4A:00:14:8D:4B ⊕Endpoint ProfileWindows7-WorkstationAuthentication PolicyDefault >> Dot1X >> DefaultAuthorization ResultPermitAccess

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

疑難排解

本節介紹此設定遇到的一些常見錯誤以及如何進行疑難排解:

- 安裝OpenLDAP後,如果您遇到錯誤指示gssapi.dll丢失,請重新啟動Microsoft Windows。
- 可能無法直接編輯Cisco AnyConnect的configuration.xml檔案。將新配置儲存到其他位置,然 後使用它替換舊檔案。
- 在驗證報告中,出現以下錯誤消息:

<#root>

Authentication method is not supported by any applicable identity store

此錯誤消息表明LDAP不支援您選擇的方法。

確保同一報告中的身份驗證協定顯示其中一個受支援的方法(EAP-GTC、EAP-TLS或PEAP-TLS)。

 在身份驗證報告中,如果您注意到在身份儲存中找不到主題,則報告中的使用者名稱與 LDAP資料庫中任何使用者的主題名稱屬性不匹配。

在此方案中,此屬性值設定為uid,這意味著ISE在嘗試查詢匹配項時查詢LDAP使用者的uid值。

• 如果在繫結到伺服器測試期間未正確檢索到主題和組,則搜尋庫的配置不正確。

請記住,必須從枝葉到根和dc(可包含多個單詞)指定LDAP層次結構。

✔ 提示:若要對WLC端的EAP身份驗證進行故障排除,請參閱<u>使用WLAN控制器(WLC)的EAP身</u> <u>份驗證配置示例</u>思科文檔。

關於此翻譯

思科已使用電腦和人工技術翻譯本文件,讓全世界的使用者能夠以自己的語言理解支援內容。請注 意,即使是最佳機器翻譯,也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準 確度概不負責,並建議一律查看原始英文文件(提供連結)。