Configuración de ISE para la integración con un servidor LDAP

Contenido

Introducción
Prerequisites
Requirements
Componentes Utilizados
Antecedentes
Configurar
Diagrama de la red
Configurar OpenLDAP
Integre OpenLDAP con ISE
Configurar la WLC
Configuración de EAP-GTC
Verificación
Troubleshoot

Introducción

Este documento describe cómo configurar Cisco Identity Services Engine (ISE) para la integración con un servidor LDAP de Cisco.

Prerequisites

Requirements

No hay requisitos específicos para este documento.

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware:

- Cisco ISE versión 1.3 con parche 2
- Microsoft Windows versión 7 x64 con OpenLDAP instalado
- Cisco Wireless LAN Controller (WLC) versión 8.0.100.0
- Cisco AnyConnect versión 3.1 para Microsoft Windows

• Editor de perfiles de Cisco Network Access Manager

Nota: este documento es válido para las configuraciones que utilizan LDAP como origen de identidad externo para la autenticación y autorización de ISE.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

Estos métodos de autenticación son compatibles con LDAP:

- Protocolo de autenticación extensible Tarjeta de testigo genérica (EAP-GTC)
- Protocolo de autenticación extensible Seguridad de la capa de transporte (EAP-TLS)
- Protocolo de autenticación extensible protegido Seguridad de la capa de transporte (PEAP-TLS)

Configurar

En esta sección se describe cómo configurar los dispositivos de red e integrar ISE con un servidor LDAP.

Diagrama de la red

En este ejemplo de configuración, el terminal utiliza un adaptador inalámbrico para asociarse con la red inalámbrica.

La LAN inalámbrica (WLAN) en el WLC se configura para autenticar a los usuarios a través de ISE. En ISE, LDAP se configura como un almacén de identidades externo.

Esta imagen ilustra la topología de red que se utiliza:



Configurar OpenLDAP

La instalación de OpenLDAP para Microsoft Windows se realiza a través de la GUI y es muy sencilla. La ubicación predeterminada es C: > OpenLDAP. Después de la instalación, debería ver este directorio:

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	
퉬 Readme	6/3/2015 5:06 PM	File folder	
퉬 replica	6/3/2015 5:06 PM	File folder	
퉬 run	6/4/2015 9:09 PM	File folder	
퉬 schema	6/3/2015 5:06 PM	File folder	
🌗 secure	6/3/2015 5:06 PM	File folder	
🐌 SQL	6/3/2015 5:06 PM	File folder	
🐌 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

Tome nota de dos directorios en particular:

- ClientTools Este directorio incluye un conjunto de binarios que se utilizan para editar la base de datos LDAP.
- Idifdata Esta es la ubicación en la que debe almacenar los archivos con objetos LDAP.

Agregue esta estructura a la base de datos LDAP:



En el directorio Root, debe configurar dos unidades organizativas (OU). La unidad organizativa OU=groups debe tener un grupo secundario (cn=domainusers en este ejemplo).

La unidad organizativa OU=people define las dos cuentas de usuario que pertenecen al grupo cn=domainusers.

Para rellenar la base de datos, primero debe crear el archivo ldif. La estructura mencionada anteriormente se creó a partir de este archivo:

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
```

Para agregar los objetos a la base de datos LDAP, utilice el binario Idapmodify:

```
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"
```

Integre OpenLDAP con ISE

Utilice la información que se proporciona en las imágenes de esta sección para configurar LDAP como un almacén de identidades externo en ISE.

allah		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_EXAMPLE Seneral Connection Directory Organization Groups Attributes * Name LDAP_DXAMPLE Description • Schema • Schema • Schema • Subject Objectclass inetOrgPerson • Group Objectclass posteGroup • Subject Name Attribute uid • Croup 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	<u> </u>
	Save Reset	

Puede configurar estos atributos desde la pestaña General:

- Subject Objectclass: este campo corresponde a la clase de objeto de las cuentas de usuario del archivo Idif. Según la configuración de LDAP. use una de estas cuatro clases:
 - Arriba
 - Persona
 - · PersonaOrganizativa
 - InetOrgPerson
- Atributo de nombre de sujeto: atributo que recupera LDAP cuando ISE pregunta si un nombre de usuario específico está incluido en una base de datos. En este escenario, debe utilizar john.doe o jan.kowalski como el nombre de usuario en el terminal.
- Group Objectclass Este campo corresponde a la clase de objeto para un grupo en el archivo ldif. En este escenario, la clase de objeto para el grupo cn=domainusers es posixGroup.
- Atributo de asignación de grupo: este atributo define cómo se asignan los usuarios a los grupos. En el grupo cn=domainusers del archivo ldif, puede ver dos atributos memberUid que corresponden a los usuarios.

ISE también ofrece algunos esquemas preconfigurados (Microsoft Active Directory, Sun, Novell):

ahaha		License Warning A
cisco Identity Services Engine	Home Operations Policy Guest Acress Administration	
🔆 System 🛛 💆 Identity Management	🞬 Network Resources 🛛 😹 Device Portal Management 🛛 🗔 pxGrid Services 🛛 👼 Feed Service 🛛 🔩 px	Grid Identity Mapping
Identities Groups External Identity So	urces Identity Source Sequences Settings	
External Identity Sources	LDAP Identity Sources Ust > LDAP_EXAMPLE LDAP Identity Source General Connection Directory Organization Groups Attributes	
Active Directory	Primary Server	Secondary S
🔻 🚞 LDAP		Enable Se
T LDAP_EXAMPLE		
RADUS Token	* Hostname/P 10.61.106.242 ① Ho	stname/IP
KSA SECULU	* Port 389	Port 389
	Access O Anonymous Access	Access 💿 Anonymo
	Authenticated Access	O Authentic
	Admin DN * on=Nanager, dc=maxorc, dc=com	Admin DN
	Password	Password
	Secure Authentication Enable Secure Authentication Secure Auth	Boot Ch. Suttinues St
	Room CAR Certificate Services Endpoint	Certificate Si
	* Server Timeout 10 (J.Seconds Serve	er Timeout 10
	* Max. Admin Connections 20 0 Max. Admin Co	nnections 20
	Test Bind to Server	Test Bind t
	۲	
	Save Reset	

Después de establecer la dirección IP y el nombre de dominio administrativo correctos, puede Probar enlace con el servidor. En este momento, no se recupera ningún asunto o grupo porque las bases de búsqueda aún no están configuradas.

En la ficha siguiente, configure la base de búsqueda de sujetos/grupos. Este es el punto de unión para ISE a LDAP. Sólo podrá recuperar los sujetos y grupos que sean hijos del punto de unión.

En este escenario, se recuperan los sujetos de OU=people y los grupos de OU=groups:

ahaha		License Warning 🛕
CISCO Identity Services Engine		
🔆 🔆 System 🛛 👰 Edentity Management	Network Resources 🛛 🛃 Device Portal Management 🕞 pxGrid Services 🕞 Feed Service	L pxGrid Identity Mapping
Identities Groups External Identity Sou	Identity Source Sequences Settings	
External Identity Sources	LDAP Identity Sources Let > LDAP_EXAMPLE EDAP Identity Source General Connection Directory Organization Groups Attributes * Subject Search Base ou=people,dc=maxorc,dc=com Naming Contexts 0 * Group Search Base ou=groups,dc=maxorc,dc=com Naming Contexts 0 Search for MAC Address in Format xxxxxxxxxxxxxxxxx Ship start of subject name up to the fast occurrence of the separator Strip end of subject name from the first occurrence of the separator	

En la pestaña Groups, puede importar los grupos desde LDAP en ISE:



Configurar la WLC

Utilice la información que se proporciona en estas imágenes para configurar el WLC para la autenticación 802.1x:

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 M Enable

ပါပါပ cisco	MONITOR <u>W</u> LANS <u>C</u> ONTROLLER WIRELESS <u>S</u> ECURITY MANAGEMENT C <u>O</u> MMANDS HELP <u>F</u> EEDBACK
WLANs	WLANs > Edit 'piborowi_byod'
WLANS	General Security QoS Policy-Mapping Advanced
Advanced	Layer 2 Layer 3 AAA Servers
	Select AAA servers below to override use of default servers on this WLAN Radius Servers Radius Server Overwrite interface Enabled Authentication Servers Accounting Servers Enabled Enabled Enabled
	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 Vone
uluulu cisco	MONITOR <u>W</u> LANS <u>C</u> ONTROLLER WIRELESS <u>S</u> ECURITY MANAGEMENT C <u>O</u> MMANDS HELP <u>F</u> EEDBACK
WLANs	WLANs > Edit 'piborowi_byod'
WLANs WLANs	General Security QoS Policy-Mapping Advanced
Advanced	Layer 2 Layer 3 AAA Servers
	Select AAA servers below to override use of default servers on this WLAN Radius Servers

Configuración de EAP-GTC

Uno de los métodos de autenticación compatibles con LDAP es EAP-GTC. Está disponible en Cisco AnyConnect, pero debe instalar el Editor de perfiles del Administrador de acceso de red para configurar el perfil correctamente.

Authentication Servers Accounting Servers

Server 1 IP:10.62.145.51, Port:1812 + IP:10.62.145.51, Port:1813 +

Enabled

None

None

None

None

None

EAP Parameters

Enable

•

Ŧ

Ŧ

Ŧ

Ŧ

También debe editar la configuración del Administrador de acceso de red, que (de forma predeterminada) se encuentra aquí:

Radius Server Overwrite interface Enabled

Enabled

Server 3 None

Server 4 None

Server 2 None

Server 5 None

Server 6 None

C: > ProgramData > Cisco > Cisco AnyConnect Secure Mobility Client > Network Access Manager > sistema > archivo configuration.xml

Utilice la información que se proporciona en estas imágenes para configurar el EAP-GTC en el punto final:

Name: eap_gtc Group Membership In group: In group: Local network In all groups (Global) Choose Your Network Media Wired (802.3) Network Select a wired network if the endstations with a traditional ethernet cable. Wi-Fi (wireless) Network Select a WiFi network if the endstations via a wireless radio connection to an Acc SSID (max 32 chars): Indee Corport	tions will be connecting to the network ons will be connecting to the network Access Point. rowi_byod iddee Naturade
Group Membership In group: Local network In all groups (Global) Choose Your Network Media Wired (802.3) Network Select a wired network if the endstations with a traditional ethernet cable. Wi-Fi (wireless) Network Select a WiFi network if the endstations via a wireless radio connection to an Acc SSID (max 32 chars): piborowi Hidde Corport	tworks
 In group: Local network In all groups (Global) Choose Your Network Media Wired (802.3) Network Select a wired network if the endstations with a traditional ethernet cable. Wi-Fi (wireless) Network Select a WiFi network if the endstations via a wireless radio connection to an Acc SSID (max 32 chars): piborowie Hidde 	tworks User Auth Credentials User Auth Credentials tions will be connecting to the network Access Point. rowi_byod iddea Naturals
 In all groups (Global) Choose Your Network Media Wired (802.3) Network Select a wired network if the endstations with a traditional ethernet cable. WI-FI (wireless) Network Select a WiFi network if the endstations via a wireless radio connection to an Acc SSID (max 32 chars): piborowi Hidde 	tions will be connecting to the network ons will be connecting to the network access Point. rowi_byod iddee Network
 In all groups (Global) Choose Your Network Media Wired (802.3) Network Select a wired network if the endstations with a traditional ethernet cable. Wi-Fi (wireless) Network Select a WiFi network if the endstations via a wireless radio connection to an Acc SSID (max 32 chars): piborowi Hidde 	tions will be connecting to the network ons will be connecting to the network Access Point. rowi_byod
Choose Your Network Media Wired (802.3) Network Select a wired network if the endstations with a traditional ethernet cable. WI-Fi (wireless) Network Select a WIFi network if the endstations via a wireless radio connection to an Acc SSID (max 32 chars): piborowi Hidde Corpo	tions will be connecting to the network ons will be connecting to the network Access Point. rowi_byod
 Wired (802.3) Network Select a wired network if the endstations with a traditional ethernet cable. WI-Fi (wireless) Network Select a WiFi network if the endstations via a wireless radio connection to an Acc SSID (max 32 chars): piborowi Hidde 	tions will be connecting to the network ons will be connecting to the network Access Point. rowi_byod
Select a wired network if the endstations with a traditional ethernet cable. WI-FI (wireless) Network Select a WIFI network if the endstations via a wireless radio connection to an Acc SSID (max 32 chars): piborowil Hidde Corpo	tions will be connecting to the network ons will be connecting to the network Access Point. rowi_byod
with a traditional ethernet cable. WI-FI (wireless) Network Select a WIFI network if the endstations via a wireless radio connection to an Acc SSID (max 32 chars):	ons will be connecting to the network Access Point. rowi_byod
Wir-Fi (wireless) Network Select a WiFi network if the endstations via a wireless radio connection to an Acc SSID (max 32 chars): piborowi Hidde Corpo	ons will be connecting to the network Access Point. rowi_byod
WI-FI (wireless) Network Select a WIFI network if the endstations via a wireless radio connection to an Acc SSID (max 32 chars): piborowi Hidde Corpo	ons will be connecting to the network Access Point. rowi_byod
Select a WiFi network if the endstations via a wireless radio connection to an Acc SSID (max 32 chars): piborowi Hidde	ons will be connecting to the network Access Point. rowi_byod
via a wireless radio connection to an Acc SSID (max 32 chars): piborowi Hidde	Access Point. rowi_byod
SSID (max 32 chars): piborowi	rowi_byod
Hidde	Iddae Mahuada
Corpo	IDDEN NETWORK
	orporate Network
Annual Mark Thread Annual	
Association Timeout 5	seconds
Common Settings	

🚰 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 - N File Help Network Access Manager Clent Policy 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	

Authentication Policy Networks	EAP Methods -	Media Type
Network Groups	@ FAP-TLS @ PEAP	Security Level
	0	Connection Typ
	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	
	O Authenticate using a Token and EAP-GTC	

🚰 AnyConnect Profile Editor - I	Network Access Manager		
File Help			
Network Access Manager	Networks Profile:ility Client\Network	k Access Manager\system\configuration.xml	I
Networks	User Identity Unprotected Identity Pattern: Protected Identity Pattern:	john.doe john.doe	Media Type Security Level Connection Type User Auth Credentials
	User Credentials Use Single Sign On Credentials Prompt for Credentials Remember Forever Remember while Use Never Remember Use Static Credentials Password: passw	als er is Logged On words Cancel	

Utilice la información que se proporciona en estas imágenes para cambiar las políticas de autenticación y autorización en ISE:

ahaha										License Warring 🚠
cisco Identity Services Engine				🙆 Home	Operations •	Policy •	Guest Access	Administration -		
📕 Aut	hentication	Authorization	K Profiling	🖲 Posture	👸 Client Pro	visioning	🚊 TrustSec	noicy Elements 🚯		
Authent	ication Policy									
Define the	Authentication I	Policy by selecting the	e protocols that ISE she	ould use to con	mmunicate with th	ie network de	vices, and the ident	ity sources that it should	use for authenticat	tion.
For Policy I Rober Typ	Export go to Adr	ninistration > System	> Backup & Restore >	Policy Export I	Page					
Party 199	a () ships	() Non-taired								
	МАВ	: If	Wired_MAB OR Wireless_MAB			Allow P	rotocols : Default	Network Access	and	
	🛃 Default	:	use Internal Endpoin	its						
	Dot1X	: If	Wred_802.1X OR Wreless_802.1X			Allow P	rotocols : Default	Network Access	and	
	🗹 Default	E	:USE LDAP_EXAMPLE							
	Default Rule	(If no match) : Allo	w Protocols : Default	Network Acce	-55	and use :	Al_User_ID_Stores	i		

ababi .										Liceose Warning A	
CISCO Identity Services Engine				🟠 Home Operations 🔻 Policy 🗖		Policy •	Guest Access		ministration I •		
4	Authentica	ation 😑 Authorization	K Profiling	🔀 Posture	Gient Pro	visioning	🚊 TrustSec	🐥 Poli	cy 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.											
	icy capare	go to Hammedaton > system > t	echop of neecon	e > Porcy Exporce	raya						
First N	Aatched Ru	le Applies 🔻									
) b	ceptions	(0)									
Sta	brebox										
	Status	Rule Name	Con	ditions (identity g	roups and other o	onditions)			Permissions		
1		Users in LDAP store	if (W on-	ireless_802.1X AN -domainusers,ou	D LDAP_EXAMPLE: groups,dc=maxtre	ExternalGrou ,dc=com)	os EQUALS	then	PermitAccess		
÷	2	Wireless Black List Default	if Bla	cklist AND Wirele	ss_Access			then	Blackhole_Wirel	ess_Access	
I	×	Profiled Cisco IP Phones	i Cis	co-IP-Phone				then	Cisco_IP_Phone	5	
I	2	Profiled Non Cisco IP Phones	if Nor	n_Cisco_Profiled_P	hones			then	Non_Osco_IP_P	hones	
÷	2	Basic_Authenticated_Access	if Net	twork_Access_Aut	thentication_Passe	d		then	PermitAccess		
	x	Default	if no m	atches, then D	enyAccess						

Después de aplicar la configuración, debería poder conectarse a la red:

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

Verificación

Para verificar las configuraciones de LDAP e ISE, recupere los sujetos y grupos con una conexión de prueba con el servidor:

alaha					Liown	we Warning A
cisco Identity Services Engine	🏠 Home 🛛 G	perations 💌 Policy 🖃	Guest Access	dministration 🔻		
🔆 System 🛛 👹 Identity Management	📰 Network Resources 🛛 🛃 D	evice Portal Management	🙀 pxGnd Services	Feed Service	L pxGnd Identit	y Mapping
Identities Groups External Identity 9	ources Identity Source Seque	nces Settings				
External Identity Sources	LDAP Identity Sources List > LDAP LDAP Identity Source General Connection	EXAMPLE	nanitation Grout	ns Attributos		
Certificate Authentication Profile		Primary Server	Bind successful to 10.61	106.242.389		Secondary S
EDAP EDAP_EXAMPLE	Result of testing this configuration is as follows Number of Subjects: 2					Enable Se
 RADIUS Token 	* Hostname/IP	10.61.106.242	Number of Groups: 1	Hostname/IP		
 RSA SecuriD 	* Port	389	Response time:1636ms		Port	.389
	Access Admin DN	Anonymous Access Authenticated Access ani-Manager,dc=maxor		СК	Access Admin DN	 Anonymo Authentics
	Password				Password	
	Secure Authentication	Enable Secure Authentical	lion	Sea	ire Authentication	Enable Se
	Root CA	Certificate Services Endpoint	· *		Root CA	Certificate Se
	* Server Timeout	10	ØSeconds		Server Timeout	10
	* Max. Admin Connections	20	æ	Max. Ad	min Connections	20
	ł	Test Bind to Server				Test Bind t
	•			11		
	Save					

Estas imágenes ilustran un ejemplo de informe de ISE:

🖬 Authent K	t cations 🧃 Visconfigured Sup	Reports	😰 Endpoint P	instantion Secul	5				
R	Visconfigured Sup			Telescont and the	ce 🔨 Troublesho	ot			
	1	picanta 🤷		Misconfiga	red Network Devices ⁰ O	D	RADIUS Drops (2) 1305	Clent S	itopped Responding (2) O
Show Live 9	Sessions 🙀 Add	i ar Renove Ca	unns 🐑 🏀 Refix	ech 🕐 Reset P	lepest Counts			Refr	esh Every 1 minute 🔹
P	• Stat	us Tetals	Repeat Count	Identity 🕐	Endpoint ID	Endpoint Profile 🍈	Authentication Policy	Authorization Policy	Authorization Profiles
15-06-04 21 15-06-04 21	1:50:45.538 (1:59:45.510		0]	ohnudoe ohnudoe	C094A:00:14:80:48 C094A:00:14:80:48	Windows7-Workst Windows7-Workst	Default >> Dot1X >> Default	Default >> Users in LDAP store	a PermitAccess
Over Ever	rview				5200 Authentio	cation succee	eded		
User	rname				john.doe 🕀				
Endp	point Id				C0:4A:00:14:8	D:4B ⊕			
Endpoint Profile				Windows7-Workstation					
Authentication Policy				Default >> Dot1X >> Default					
Authorization Policy				Default >> Users in LDAP store					
Auth	orization	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

Troubleshoot

Esta sección describe algunos errores comunes que se encuentran con esta configuración y cómo solucionarlos:

- Después de la instalación de OpenLDAP, si encuentra un error que indique que falta un archivo gssapi.dll, reinicie Microsoft Windows.
- Puede que no sea posible editar el archivo configuration.xml para Cisco AnyConnect directamente. Guarde la nueva configuración en otra ubicación y, a continuación, utilícela para sustituir el archivo antiguo.
- En el informe de autenticación, aparece este mensaje de error:

<#root>

Authentication method is not supported by any applicable identity store

Este mensaje de error indica que el método seleccionado no es soportado por LDAP.

Asegúrese de que el protocolo de autenticación del mismo informe muestre uno de los métodos compatibles (EAP-GTC, EAP-TLS o PEAP-TLS).

• En el informe de autenticación, si observa que no se encontró el asunto en el almacén de identidades, el nombre de usuario del informe no coincide con el atributo de nombre de sujeto para ningún usuario de la base de datos LDAP.

En este escenario, el valor se estableció en uid para este atributo, lo que significa que ISE busca los valores uid para el usuario LDAP cuando intenta encontrar una coincidencia.

• Si los sujetos y grupos no se recuperan correctamente durante una prueba de enlace al servidor, es una configuración incorrecta para las bases de búsqueda.

Recuerde que la jerarquía de LDAP debe especificarse desde hoja a raíz y dc (puede constar de varias palabras).

Sugerencia: Para resolver problemas de autenticación EAP en el lado del WLC, consulte el documento de Ejemplo de Configuración de Autenticación EAP con Controladores WLAN (WLC) de Cisco.

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).