Configurar o ISE para integração com um servidor LDAP

Contents

Introdução
Pré-requisitos
Requisitos
Componentes Utilizados
Informações de Apoio
Configurar
Diagrama de Rede
Configurar OpenLDAP
Integrar o OpenLDAP com o ISE
Configurar o WLC
Configurar EAP-GTC
Verificar
Troubleshooting

Introdução

Este documento descreve como configurar um Cisco Identity Services Engine (ISE) para integração com um servidor LDAP da Cisco.

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

As informações deste documento são baseadas nestas versões de software e hardware:

- Cisco ISE versão 1.3 com patch 2
- Microsoft Windows versão 7 x64 com OpenLDAP instalado
- Cisco Wireless LAN Controller (WLC) versão 8.0.100.0
- Cisco AnyConnect versão 3.1 para Microsoft Windows

• Editor de perfis do Cisco Network Access Manager

Observação: este documento é válido para configurações que usam LDAP como a origem de identidade externa para a autenticação e autorização do ISE.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

Estes métodos de autenticação são suportados com LDAP:

- Protocolo de autenticação extensível placa de token genérica (EAP-GTC)
- Protocolo de autenticação extensível Transport Layer Security (EAP-TLS)
- Protocolo de autenticação extensível protegido Transport Layer Security (PEAP-TLS)

Configurar

Esta seção descreve como configurar os dispositivos de rede e integrar o ISE com um servidor LDAP.

Diagrama de Rede

Neste exemplo de configuração, o endpoint usa um adaptador sem fio para associar-se à rede sem fio.

A Wireless LAN (WLAN) na WLC está configurada para autenticar os usuários através do ISE. No ISE, o LDAP é configurado como um armazenamento de identidade externo.

Esta imagem ilustra a topologia de rede que é usada:



Configurar OpenLDAP

A instalação do OpenLDAP para Microsoft Windows é concluída via GUI e é simples. O local padrão é C: > OpenLDAP. Após a instalação, você deverá ver este diretório:

Nai	me	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	
	Readme	6/3/2015 5:06 PM	File folder	
	replica	6/3/2015 5:06 PM	File folder	
	run	6/4/2015 9:09 PM	File folder	
	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	
٩	4758cca.dll	2/22/2015 5:59 PM	Application extens	18 KB
٩	aep.dll	2/22/2015 5:59 PM	Application extens	15 KB
3	atalla.dll	2/22/2015 5:59 PM	Application extens	13 KB
٩	capi.dll	2/22/2015 5:59 PM	Application extens	29 KB
٩	chil.dll	2/22/2015 5:59 PM	Application extens	21 KB
٩	cswift.dll	2/22/2015 5:59 PM	Application extens	20 KB
٩	gmp.dll	2/22/2015 5:59 PM	Application extens	6 KB
٩	gost.dll	2/22/2015 5:59 PM	Application extens	76 KB
٩	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
٩	libeay32.dll	2/22/2015 5:59 PM	Application extens	1,545 KB
٩	libsasl.dll	2/5/2015 9:40 PM	Application extens	252 KB
	maxcrc.ldif	2/5/2015 9:40 PM	LDIF File	1 KB
٩	nuron.dll	2/22/2015 5:59 PM	Application extens	11 KB
٩	padlock.dll	2/22/2015 5:59 PM	Application extens	7 KB
Ē	slapacl.exe	5/11/2015 10:59 PM	Application	3,711 KB

Tome nota de dois diretórios em particular:

- ClientTools Este diretório inclui um conjunto de binários usados para editar o banco de dados LDAP.
- Idifdata Este é o local no qual você deve armazenar os arquivos com objetos LDAP.

Adicione esta estrutura ao banco de dados LDAP:



No diretório Root, você deve configurar duas OUs (Organizational Units, unidades organizacionais). A OU OU=groups deve ter um grupo filho (cn=domainusers neste exemplo).

A OU OU=people define as duas contas de usuário que pertencem ao grupo cn=domainusers.

Para preencher o banco de dados, você deve criar o arquivo ldif primeiro. A estrutura mencionada anteriormente foi criada a partir deste arquivo:

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 adicionar os objetos ao banco de dados LDAP, use o binário 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_oprepare_socket: 496 ldap_opre_connect: td: 496 tm: -1 async: 0 attempting to connect: connect success adding new entry "ou=groups,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" adding new entry "cn=domainusers,ou=groups,dc=maxcrc,dc=com"

Integrar o OpenLDAP com o ISE

Use as informações fornecidas nas imagens ao longo desta seção para configurar o LDAP como um armazenamento de identidade externo no ISE.

ahah		License Warning
CISCO Identity Services Engine	Home Operations I▼ Policy I▼ Guest Access I▼ Administration I▼	
🔆 System 🛛 😥 Identity Management	Network Resources 🛛 Revice Portal Management 🔂 pxGnd Services 🔂 Feed Service	L pxGrid 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_EXAMPLE Description * Schema Qustom * Schema Qustom * Subject Objectclass InetOrgPerson * Group Objectclass poseGroup * Subject Name Attribute uid Certificate Attribute uid Certificate Attribute userCertificate Subject Objects Contain Reference To Groups Group Objects Contain Reference To Subjects Subject In Groups Are Stored In Member Attribute As Distinguished Name	<u>v</u>
	Save Reset	

Você pode configurar esses atributos na guia Geral:

- Subject Objectclass Este campo corresponde à classe de objeto das contas de usuário no arquivo ldif. De acordo com a configuração LDAP. use uma destas quatro classes:
 - Superior
 - Pessoa
 - PessoaOrganizacional
 - InetOrgPerson
- Atributo do nome do assunto Este é o atributo recuperado pelo LDAP quando o ISE consulta se um nome de usuário específico está incluído em um banco de dados. Neste cenário, você deve usar john.doe ou jan.kowalski como o nome de usuário no ponto final.
- Group Objectclass Este campo corresponde à classe de objeto de um grupo no arquivo ldif. Neste cenário, a classe de objeto para o grupo cn=domainusers é posixGroup.
- Atributo de mapa de grupo Este atributo define como os usuários são mapeados para os grupos. No grupo cn=domainusers no arquivo ldif, você pode ver dois atributos memberUid que correspondem aos usuários.

O ISE também oferece alguns esquemas pré-configurados (Microsoft Ative Diretory, 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	

Depois de definir o endereço IP e o nome de domínio administrativo corretos, você pode Testar associação ao servidor. Neste ponto, você não recupera nenhum assunto ou grupo porque as bases de pesquisa ainda não estão configuradas.

Na próxima guia, configure a Base de pesquisa de assunto/grupo. Este é o ponto de junção do ISE para o LDAP. Você pode recuperar apenas assuntos e grupos que sejam filhos do seu ponto de junção.

Neste cenário, os assuntos de OU=people e os grupos de OU=groups são recuperados:

abab		Literae 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 Image: The second seco	IDAP Identity Sources Let > LDAP_EXAMPLE EDAP Identity Sources General Connection Directory Organization Groups Attributes * Subject Search Base ou=people,dc=maxerc,dc=com Naming Contexts 0 * Group Search Base ou=groups,dc=maxerc,dc=com Naming Contexts 0 Search for MAC Address in Format xx xx xx xx xx xx Strip start of subject name up to the last occurrence of the separator Strip end of subject name from the first occurrence of the separator	

Na guia Groups, você pode importar os grupos do LDAP no ISE:



Configurar o WLC

Use as informações fornecidas nestas imagens para configurar a WLC para a autenticação 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
	Fast Transition
	Protected Management Frame
	PMF Disabled WPA+WPA2 Parameters
	WPA Policy WPA2 Policy-AES
	Authentication Key Management
	802.1X I Enable

ululu cisco	MONITOR WL	ANS <u>C</u> ONTROLLER W <u>I</u> REI	.ESS <u>S</u> ECURITY M <u>A</u> NAGEMENT	C <u>O</u> MMANDS HELP <u>F</u> EEDBACK
WLANs	WLANs > Edi	t 'piborowi_byod'		
WLANs	General	Security QoS Policy	Mapping Advanced	
Advanced	Layer 2	Layer 3 AAA Servers		
	Select AAA s Radius Serve Radius Server 1 Server 2	servers below to override users ers rver Overwrite interface En Authentication Servers Enabled IP:10.62.145.51, Port:1812 • None •	e of default servers on this WLAN abled Accounting Servers Finabled IP:10.62.145.51, Port:1813 • None •	EAP Parameters Enable
	Server 3	None -	None 👻	
	Server 4	None -	None -	
	Server 6	None -	None -	
cisco	MONITOR WU	ANS <u>C</u> ONTROLLER WIRE	.ess <u>s</u> ecurity m <u>a</u> nagement	COMMANDS HELP FEEDBACK
WLANs	WLANs > Edit	t 'piborowi_byod'		
VLANs	General S	Security QoS Policy	Mapping Advanced	
Advanced	Layer 2	Layer 3 AAA Servers	e of default servers on this WLAN	

	Authentication Servers	Ac	counting Servers	EAP Par	ameter
	Enabled	V	Enabled	Enable	E
Server 1	IP:10.62.145.51, Port:1812	- If	2:10.62.145.51, Port:1813	•	
Server 2	None	▼ N	one ·	•	
Server 3	None	▼ N	one	•	
Server 4	None	▼ N	one	•	
		1.00			

Configurar EAP-GTC

Um dos métodos de autenticação suportados para LDAP é EAP-GTC. Ele está disponível no Cisco AnyConnect, mas você deve instalar o Editor de perfis do gerenciador de acesso à rede para configurar o perfil corretamente.

Você também deve editar a configuração do Network Access Manager, que (por padrão) está localizada aqui:

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

Use as informações fornecidas nessas imagens para configurar o EAP-GTC no endpoint:

Notworke	Fromeinty chemaver	work Access Manager\system\configuration.xr	mi
Network Groups	Name:	eap_gtc	Security Leve
Checken creeps	Group Membership		Connection Tur
	In group:	Local networks	User Auth
		L	Credentials
	 In all groups (Global) 		
	Choose Your Network Media		
	Wired (802.3) Network		
	Salast a wined astrony if	the endstations will be seenesting to the actuals	
	select a wred network in	trable	
	wara dabidonai edieme	(cable.	
	Wi-Fi (wireless) Network		
	Select a WiFi network if t	he endstations will be connecting to the network	
	via a wireless radio conne	ction to an Access Point.	
	SSID (max 32 chars):	piborowi_byod	
		Tidden Network	
		Corporate Network	
	Association Timeout	5 seconds	
	Common Settings		
	Script or application on each us	er's machine to run when connected.	
		Browse Local Machine	
	Connection Timeout	40 seconds	
	Connection Inneous	-to becomes	

🚰 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 - 1	Network Access Manager				
File Help					
Network Access Manager Client Policy Authentication Policy Muthentication Policy					
Network Groups	User Identity Unprotected Identity Pattern: Protected Identity Pattern:	Media Type Security Level Connection Type User Auth Credentials			
	User Credentials	s r is Logged On ords Cancel			

Use as informações fornecidas nessas imagens para alterar as políticas de autenticação e autorização no ISE:

ahah									Loanse Warning 🔒
cisco	Identity Serv	rices Engine		🙆 Home	Operations •	Policy •	Guest Access	Administration 💌	
📕 Au	thentication	Authorization	🔀 Profiling	💽 Posture	👸 Client Pro	visioning	TrustSec	🐴 Policy Elements	
Authen	tication Policy								
Define the	e Authentication P	olicy by selecting the	protocols that ISE sh	hould use to co	mmunicate with th	e network de	vices, and the ident	ity sources that it should	use for authentication.
For Policy Policy Typ	Export go to Adm	 inistration > System : Rule-Based 	> Backup & Restore :	Policy Export	Page				
		0							
	MAB NAB	: 1f	Wired_MAB OR Wireless_MAB			Allow P	rotocols : Default	Network Access	and
	🛃 Default	:	use Internal Endpoi	ints					
1	Dot1X	: 1f	Wired_802.1X OR Wireless_802.1X			Allow P	rotocols : Default	Network Access	and
	🗹 Default		USE LDAP_EXAMPLE						
E.	Default Rule	(If no match) : Allo	w Protocols : Defaul	t Network Acco	155	and use :	Al_User_ID_Stores		

ab	aha 🖉										License Warning A
cis	co Iden	tity Services Engine		🟠 Home	Operations 🔻	Policy •	Guest Access	Adm	inistration 🛛		
4	Authentic	ation 🕘 Authorization	🔀 Profiling	🔀 Posture	Gient Pro	visioning	🚊 TrustSec	🐥 Polis	cy Elements		
Auth	orization	Policy									
Define For Pr	the Authorit	rization Policy by configuring rules b op to Administration > System > P	based on identit	ty groups and/or o > Policy Export I	ther conditions. Dr	ag and drop r	ules to change the o	rder.			
	nej enpore	go to namineciation y operative t		erreicj Dørei	- ago						
First	Matched Ru	le Applies 🔻									
) E	xceptions	(0)									
st	andard										
_	Status	Rule Name	Cor	nditions (identity g	roups and other o	onditions)			Permissions		
1	2	Users in LDAP store	if (W	freless_802.1X AN =domainusers,ou=	DILDAP_EXAMPLE groups,dc=maxtre	ExternalGroup ,dc=com)	ps EQUALS	then	PermitAccess		
÷	×	Wireless Black List Default	if Bla	cklist AND Wirele	ss_Access			then	Blackhole_Wire	less_Access	
Ē.	×	Profiled Cisco IP Phones	if Cis	co-IP-Phone				then	Cisco_IP_Phone	25	
ī.	2	Profiled Non Cisco IP Phones	if No	n_Cisco_Profiled_P	hones			then	Non_Osco_IP_I	Phones	
÷	2	Basic_Authenticated_Access	if Ne	twork_Access_Aut	thentication_Passe	d		then	PermitAccess		
	V	Default	if no n	atches, then D	enyAccess						

Depois de aplicar a configuração, você poderá se conectar à rede:

Sisco AnyCor	nnect Secure Mobility Client		
	Network: Connected (10.0.13.87) eap_gtc	الله 🖻	- =
			_
\$ ()			alialis cisco

Verificar

Para verificar as configurações LDAP e ISE, recupere os assuntos e grupos com uma conexão de teste ao servidor:

CESCO Telentity Services Fagins I home Operators * Poky * Guet Access * Anoministration * Services Fagins I home Operators * Poky * Guet Access * Anoministration * Services Fagins I home Operators * Poky * Guet Access * Anoministration * Services Fagins I home Operators * Poky * Guet Access * Anoministration * Centered Identity Sources I home Operators * Poky * Guet Access * Anoministration * Centered Identity Sources I home Operators * Poky * Guet Access * Anoministration * Centered Identity Sources I home Operators * Dental Management I home Operators * Poky * Guet Access * I home Operators * Poky * Guet Access * I home Operators * I home of Groups * I home of Bugets * I home	ախալիս						Liow	w Warning A
	cisco Identity Services En	igine	🏠 Home 🔇	Operations 💌 Policy 🖃	Guest Access	Administration 1 🔻		
Verticitis Verticity Sources Methy Sources Settings Consection Consection </th <th>😽 System 🛛 🛃 Identity Ma</th> <th>nagement 🛛 🖬 Netwo</th> <th>ork Resources 🛛 🛃 D</th> <th>evice Portal Management</th> <th>😹 pxGrid Services</th> <th>Feed Service</th> <th>Le pxGnd Identit</th> <th>y Mapping</th>	😽 System 🛛 🛃 Identity Ma	nagement 🛛 🖬 Netwo	ork Resources 🛛 🛃 D	evice Portal Management	😹 pxGrid Services	Feed Service	Le pxGnd Identit	y Mapping
Deternal Identity Sources Image: Source Authentication Profile Image: Advector Image: Source Authentication Profile Image: Advector Image: Source Authentication Profile Image: Source Authentication Image: Sour	Identities Groups	ctemal Identity Sources	Identity Source Seque	ences Settings				
Certificate Authentication Profile Active Directory Case Active Directory Case Data Economy Server Bind successful to 10.81.108.242.339 Result of fasting this configuration is as follows: Number of Subjects: 2 Number of Subj	External Identity Sources		dentity Sources List > LDAP, P Identity Source General Conn	EXAMPLE	cantration Sco	uns Attributes		
 Result of testing this configuration is as follows: Number of Stropes: 1 * RADIUS Token * Server Timeout 10 * Max. Admin Connections 20 * Tax Bind to Sarvar * Rest 	Certificate Authentication Prof Actual Directory	file		Primary Server	Bind successful to 10.6	1.108.242.389		Secondary S
 * RADUS Token * HastnamedP * RSA Securit * HastnamedP * Port 380 Access Anonymous Access Anonymous Accesters<td>* DAP_EXAMPLE</td><td></td><td></td><td></td><td>Result of testing this co Number of Subjects: 2 Number of Grouper, 1</td><td>nfiguration is as follows: 2</td><td></td><td>Enable S</td>	* DAP_EXAMPLE				Result of testing this co Number of Subjects: 2 Number of Grouper, 1	nfiguration is as follows: 2		Enable S
Read	RADIUS Token		* Hostname/IP	10.61.106.242	Hernoer er ereepe. T		Hostname/IP	
Access Anonymous Access Authenticated Access Authenticated Access Authenticated Access Authenticated Access Authenticated Access Admin DN Password Password Becure Authentication Enable Secure Authentication Root CA Certificate Services Endpoint * Secure Authentication Enable Sec Root CA Certificate Services Endpoint * Server Timeout 10 * Max. Admin Connections 20 Test End to Server Root CA Certificate Server Access Anonymo Access Anonymo Access Anonymo Authentic Authent	 RSA SecuriD 		* Port	389	Response time:1636m	15	Port	389
Password * ••••• Password * ••••• Password *			Access Admin DN	Anonymous Access Authenticated Access Ton=Manager,dc=maxore		ОК	Access Admin DN	 Anonymo Authentics
Secure Authentication Enable Secure Authentication Root CA Certificate Services Endpoint * * Server Timeout 10 * Max. Admin Connections 20 Test Root to Server Test Root to Server * * * * * * * * * * * * * * * * * *			Password	* *****			Password	
Secure Authentication Enable Secure Authentication Secure Authentication Enable Secure Authentication E								
Root CA Certificate Services Endpoint * Root CA Certificate Services Endpoint * * Server Timeoul 10 Ø Boconds Server Timeoul 10 * Max. Admin Connections 20 Ø Max. Admin Connections 20 (Test Bind to Server) Test Bind to Server Test Bind to Server Test Bind to Server			Secure Authentication	Enable Secure Authentical	tion	Sec	ure Authentication	Enable Se
* Server Timeout 10 (FiSoconds Server Timeout 10 * Max. Admin Connections 20 (Test Bind to Server) * Test Bind to Server) * Test Bind to Server Timeout 10 Test Bind to Server Timeout 10 * Max. Admin Connections 20 Test Bind to Server Timeout 10 * Max. Admin Connections 20			Root CA	Certificate Services Endpoint	<u>. *</u>		Root CA	Certificate S
* Server Timeout 10 * Max. Admin Connections 20 * Max. Admin Connections 20 * Test Bind to Server * Save Reset								
* Max. Admin Connections 20 (Test Bind to Server) (Test Bind to Server) (Test Bind to Server) (Test Bind to Server)			* Server Timeput	10	0.Seconds		Server Timeout	10
Test Bind to Server			Max. Admin Connections	20	w	Max. A	dmin Connections	20
۲ Save Roset				Test Bind to Server				Test Bind t
Save Reset		-						
			e Reset					

Essas imagens ilustram um relatório de exemplo do ISE:

cisco Identity Services Engine	The Operations Policy	Guest Access Administration T	Licrosz Waxnine, 🔥 Kretił odnin
🔟 Authentications 📑 Reports 🔤 E	ndpoint Protection Service 💊 Troubleshoot		
Nisconfigured Supplicanta 🛞 1	Misconfigured Network Devices (8) 0	RAONUS Drops (C) 1305	Clent Stopped Responding (2) 0
🛃 Shaw Live Sessions – 🎡 Add ar Remove Columns 💌	🏀 Refrech 🛛 🔞 Reset Repeat Counts		Refresh Every 1 minute *
ime v Status Al v Detais Repeat	Count identity () Endpoint () () Endpoint ()	Authentication Policy (2) Author	Authorization Profiles
2015-06-04 21:50:45.538 🕚 🚡 2015-06-04 21:59:45.510 🛛 🚡	0 johnuloe C0x4Ax00:14:80:48 Windows7- johnuloe C0x4Ax00:14:80:48 Windows7-	Workst Default >> Dot1X >> Default Default	t >> Users in LDAP store PermitAccess
Overview	5200 Authentication s	ucceeded	
Username	john.doe⊕		
Endpoint Id	C0:4A:00:14:8D:4B 🕀		
Endpoint Profile	Windows7-Workstatio	n	
Authentication Policy	Default >> Dot1X >> D	Default	
Authorization Policy	Default >> Users in L	DAP store	
Authorization Result	PermitAccess		

Authentication Details	
Source Timestamp	2015-06-04 21:59:45.509
Received Timestamp	2015-06-04 21:59:45.51
Policy Server	ise13
Event	5200 Authentication succeeded
Failure Reason	
Resolution	
Root cause	
Username	john.doe
User Type	
Endpoint Id	C0:4A:00:14:8D:4B
Endpoint Profile	Windows7-Workstation
IP Address	
Authentication Identity Store	LDAP_EXAMPLE
Identity Group	Workstation
Audit Session Id	0a3e9465000010035570b956
Authentication Method	dot1x
Authentication Protocol	PEAP (EAP-GTC)
Service Type	Framed
AD ExternalGroups	cn=domainusers,ou=groups,dc=maxcrc,dc=com
IdentityDn	uid=john.doe,ou=people,dc=maxcrc,dc=com
RADIUS Username	john.doe

Troubleshooting

Esta seção descreve alguns erros comuns encontrados com esta configuração e como solucionálos:

- Após a instalação do OpenLDAP, se você encontrar um erro para indicar que um gssapi.dll está ausente, reinicie o Microsoft Windows.
- Talvez não seja possível editar o arquivo configuration.xml diretamente para o Cisco AnyConnect. Salve a nova configuração em outro local e use-a para substituir o arquivo antigo.
- No relatório de autenticação, há esta mensagem de erro:

<#root>

Authentication method is not supported by any applicable identity store

Esta mensagem de erro indica que o método selecionado não é suportado pelo LDAP.

Verifique se o protocolo de autenticação no mesmo relatório mostra um dos métodos suportados (EAP-GTC, EAP-TLS ou PEAP-TLS).

 No relatório de autenticação, se você observar que o assunto não foi encontrado no armazenamento de identidades, o nome de usuário do relatório não corresponde ao atributo de nome de assunto para qualquer usuário no banco de dados LDAP.

Nesse cenário, o valor foi definido como uid para esse atributo, o que significa que o ISE procura os valores uid para o usuário LDAP quando ele tenta encontrar uma correspondência.

• Se os assuntos e grupos não forem recuperados corretamente durante um teste vincular ao servidor, é uma configuração incorreta para as bases de pesquisa.

Lembre-se de que a hierarquia LDAP deve ser especificada de folha para raiz e dc (pode consistir em várias palavras).

Dica: para solucionar problemas de autenticação EAP no lado da WLC, consulte o documento <u>Exemplo de Configuração de Autenticação EAP com Controladoras WLAN</u> (WLC) da Cisco.

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.