基于ISE和LDAP属性的身份验证

目录

<u>简介</u> <u>先决条件</u> <u>要供配 网配 配 空 交 明 置 络 置 置 4 和 配 配 空 换 配 置 上 D A P <u>I S E 证</u> 排除</u>

简介

本文档介绍如何配置思科身份服务引擎(ISE)和使用轻量级目录访问协议(LDAP)对象属性来动态验证和授权设备。

注意: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。

作者:Emmanuel Cano和Mauricio Ramos思科专业服务工程师。

由Neri Cruz Cisco TAC工程师编辑。

先决条件

要求

思科建议您了解以下主题:

- ISE策略集、身份验证和授权策略的基本知识
- Mac身份验证绕行(MAB)
- Radius协议的基本知识
- Windows服务器的基本知识

使用的组件

本文档中的信息基于以下软件和硬件版本:

- 思科ISE版本2.4补丁11
- Microsoft Windows Server,版本2012 R2 x64
- 思科交换机Catalyst 3650-24PD版本03.07.05.E(15.2(3)E5)
- Microsoft Windows 7计算机

注意: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。如果您使用的是真实 网络,请确保您已经了解所有命令的潜在影响。

配置

本节介绍如何配置网络设备、ISE与LDAP之间的集成,以及最后如何配置LDAP属性以在ISE授权策略中使用。

网络图

此图显示了所使用的网络拓扑:



以下是流量,如网络图所示:

- 1. 用户将其pc/笔记本电脑连接到指定的交换机端口。
- 2. 交换机向ISE发送该用户的Radius访问请求
- 3. 当ISE收到信息时,它会查询LDAP服务器特定用户字段,该字段包含要在授权策略条件中使用的属性。
- 4. ISE收到属性(交换机端口、交换机名称和设备MAC地址)后,会比较交换机提供的信息。
- 5. 如果交换机提供的属性信息与LDAP提供的属性信息相同,ISE将发送RADIUS Access-Accept,其权限在授权配置文件上配置。

配置

使用此部分配置LDAP、交换机和ISE。

配置 LDAP

完成以下步骤以配置LDAP服务器:

1.导航至"服务器**管理器">"控制面板">"工具">"ADSI编辑"**

Server M	Manager • Dashboard	• 🗭 🍢 Manage Tools View Help
III Dashboard	WELCOME TO SERVER MANAGER	Active Directory Administrative Center Active Directory Domains and Trusts Active Directory Lightweight Directory Services Setup Wizard
Local Server All Servers AD CS AD DS	1 Configure this local server	Active Directory Module for Windows PowerShell Active Directory Sites and Services Active Directory Users and Computers ADSI Edit

2.右键单击ADSI Edit图标并选择"连接到......"



3.在"连接设置"下定义一个名称,然后选**择"**确定"按钮以启动连接。

Connection Settings		
Name: Default naming context		
Path: LDAP://WIN-8G7QAP9T36L.ciscoise.lab/Default naming context		
Connection Point		
O Select or type a Distinguished Name or Naming Context:		
×		
Select a well known Naming Context:		
Default naming context 🗸		
Computer		
O Select or type a domain or server: (Server Domain [:port])		
×		
Default (Domain or server that you logged in to)		
Use SSL-based Encryption		
Advanced OK Cancel		

4.在DC连接中的同一ADSI Edit菜单下,右键单击(DC=ciscodemo, DC=lab),选择New,**然后选择**Object选**项**



^{5.}选择选项**OrganizationalUnit**作为新对象,然后选**择下一步。**

Create Object	×
Select a class: msPKI-Key-Recovery-Agent msSFU30MailAliases msSFU30NetId	^
msSFU30NetworkUser msTPM-InformationObjectsContainer nisMap nisNetgroup nisObject oncRpc organization	=
organizationalUnit physicalLocation nrintΩueue	▼
< Back Next >	Cancel Help

6.为新组织单位定义名称并选择"下一**步"**

	Create Object X	
Attribute:	ou	
Syntax:	Unicode String	
Description:	Description: Organizational-Unit-Name	
Value:	AppleDevices	
	< Back Next > Cancel Help	

Create Object	x
To complete the creation of this object, click Finish.	
To set more attributes, click More Attributes. More Attributes	
	_
< Back Finish Cancel Help	

8.右键单击刚创建的OrganizationalUnit,然后选择"新建">**"对象"**

CN=Builtin CN=Comput OU=Domain	Move New Connection from Here		
CN=Foreign!	New	•	Object
CN=LostAnc	View		
🧮 CN=Manage	VIEW	_	
CN=NTDS Q	Delete		
CN=Program	Rename		
CN=System	Refresh		
CN=TPM De			
CN=Users	Export List		
CN=VPNUse	Properties		
OU=Develop	Help		
🧾 OU=AppleDe	Trep		

Create Object	×
Select a class:	
builtinDomain classStore computer contact container country device dfsConfiguration domainDNS domainPolicy friendlyCountry group crouinOff IniqueNames	 Image: Constraint of the second second
< Back Next > C	ancel Help

10.在"值"字段中定义名称并选择"下一**步"**

	Create Object X
Attribute:	an
Syntax:	Unicode String
Description:	Common-Name
Value:	LaptopTest
	< Back Next > Cancel Help

Create Object	
To complete the creation of this object, click Finish.	
To set more attributes, click More Attributes. More Attributes	
< Back Finish Cancel Help	

11.对于下拉菜单,**选择要查看的**属性,选**择选项macAddress,**然后在"编辑属性"字段下定义要验证的终**端Mac地址,并选**择 **添加**按钮以保存设备MAC地址。

注意: 在mac地址八位组之间使用双冒号, 而不是点或连字符。

cn=L	aptopTest ×	
Attributes		
Path: Class: device		
Select which properties to view:	Optional V	
Select a property to view:	macAddress 🗸	
Attribute Values		
Syntax: IA5String		
Edit Attribute:		
Value(s): 6C:B2:AE:3A:68:6C		
	Add Remove	
	OK Cancel	

12.选择**OK**以保存信息并继续设备对象配置

13.选择"完**成"**以创建新设备对象

Create Object	x
To complete the creation of this object, click Finish.	
To set more attributes, click More Attributes. More Attributes	
< Back Finish Cancel Help	

14.右键单击设备对象并选择"属性"选**项**

ADSI Edit

1	Name		Class	Distinguished Name
	CN=LaptopTest		device	CN=LaptopTest,OU=AppleDevices,DC=ciscoise,DC=lab
		Move		
		Delete		
		Rename		
1		Propert	ies	
		Help		

15.选择选项**说明**并选择**编辑**,以定义将连接设备的交换机名称和交换机端口。

tribute Editor Security	
occurry	
Attributes:	
Attribute	Value ^
adminDescription	<not set=""></not>
adminDisplayName	<not set=""></not>
bootFile	<not set=""></not>
bootParameter	<not set=""></not>
cn	Laptop Test
description	<not set=""></not>
displayName	<not set=""></not>
displayNamePrintable	<not set=""></not>
distinguishedName	CN=LaptopTest,OU=AppleDevices,DC=cisc
dSASignature	<not set=""></not>
dSCorePropagationD	0x0 = ()
extensionName	<not set=""></not>
flags	<not set=""></not>
fSMORoleOwner	<not set=""></not>
<	>
Edit	Filter
OK	Cancel Annly Help

16.定义交换机名称和交换机端口,请确保使用逗号分隔每个值。选择**添加**,然后**选择**确定以保存信息。

Multi-valued String Editor		x
Attribute: description		
Value to add:		
switchapflexconnect,GigabitEthemet1/0/6	Add	
Values:		
	Remove	e
ОК	Cancel	

- Switchapflexconnect是交换机名称。
- GigabitEthernet1/0/6是终端连接到的交换机端口。

注意: 可以使用脚本将属性添加到特定字段,但是,在本例中,我们将手动定义值

注意:AD属性区分大小写,如果在LDAP查询期间使用ISE转换为大写的所有Mac地址。为避免此行为,请在允许的协议下禁用进程主机查找。详 细信息可在以下链接中找到:<u>https://www.cisco.com/c/en/us/td/docs/security/ise/3-0/admin_guide/b_ISE_admin_3_0.pdf</u>

交换机配置

ISE802.1x

aaa new-model ! aaa group server radius ISE server name ISE deadtime 15 ! aaa authentication dot1x default group ISE aaa authorization network default group ISE aaa accounting update newinfo aaa accounting dot1x default start-stop group ISE ! aaa server radius dynamic-author client 10.81.127.109 server-key XXXXabc ! aaa session-id common switch 1 provision ws-c3650-24pd ! dot1x system-auth-control dot1x critical eapol diagnostic bootup level minimal spanning-tree mode rapid-pvst spanning-tree extend system-id hw-switch switch 1 logging onboard message level 3 ! interface GigabitEthernet1/0/6 description VM for dot1x switchport access vlan 127 switchport mode access authentication event fail action next-method authentication event server dead action authorize vlan 127 authentication event server alive action reinitialize authentication host-mode multi-domain authentication open authentication order dot1x mab authentication priority dot1x mab authentication port-control auto authentication periodic authentication timer reauthenticate server authenticator timer inactivity server dynamic authentication violation restrict mab dot1x pae authenticator dot1x timeout tx-period 10 spanning-tree portfast ! radius server ISE address ipv4 10.81.127.109 auth-port 1812 acct-port 1813 automate-tester username radiustest idle-time 5 key XXXXabc !

注意:可能需要在您的环境中调整全局和接口配置

ISE配置

以下描述ISE上的配置,以从LDAP服务器获取属性并配置ISE策略。

1. 在ISE上,转到Administration -> Identity Management -> External Identity Sources并选择LDAP文件夹,然后单击Add 以创建与LDAP的新连接

dentity Services Engine	Home	 Operations 	Policy A	dministration	Work Centers
System Identity Management Identity Management	Network Resources	Portal Management	pxGrid Services	3	
Identities Groups External Identity	Sources Identity Source Seq	uences + Settings			
External Identity Sources	LDAP Identit	ty Sources			
Certificate Authentication Profile	/ Edit 🕂 Add	Duplicate XD	elete		
Active Directory	Name			 Description 	00
ODBC					
RADIUS Token					
RSA SecurID					
SAML Id Providers					
Social Login					

2.在"常规"选项卡下定义一个名称,并选择mac地址作为"主题名称属性"

LDAP Identity Sources List > Ide	ng mab				
LDAP Identity Source					
General Conn	ection Directory Organizatio	n Groups	Attributes	Advanced Settings	
* Name	ldap_mab				
Description					
- Schema	Custom .				
* Subject Objectclass	device	* Group Objectclass	Group		
* Subject Name Attribute	macAddress	* Group Map Attribute	member		
* Group Name Attribute	distinguishedName	Certificate Attribute			
 Subject Objects Confa 	ain Reference To Groups				
Group Objects Contail	n Reference To Subjects				
	Subjects In Groups Are Stored	In Member Attribute As	Distinguished Name		
User Info Attributes ()					
First Name		Department	[
Last Name		Organizational Unit			
Job Title		Locality	[
Email		State or Province	[
Telephone		Country	[
Character & defense		country			
Street Address					

3.在"连接"**选项卡**下,配置LDAP服务器的IP地址、管理DN和密码,以便成功连接。

AP Identity Source General Connection	Directory Organization	Groups	Attributes	Advanced Settings	
Prima	ry Server			Se	econdary Server
					,,
					Enable Secondary Server
* Hostname/IP 10.83	.127.111			Hostname/IP	
* Post 280				Post 1	80
Pon 307				Port 13	07
Specify server for each ISE node					
Access	 Anonymous Access 			Acce	ess 🛞 Anonymous Access
	 Authenticated Access 				 Authenticated Access
Admin DN	* cn=administrator, cn=users, dc=	c		Admin I	DN
Password	• •••••			Passwo	ord
		_			
Carry a Authentication	Enable Service Authentication			East on Arthentical	ine Enable Service Authentication
accure Authentication	Enable Secure Authentication			Secure Authenticat	Enable Sever Hartity Chark
	Enable derver identity cireck				Change on the relenant Grant
	Contractor Constructions Construction 1	æ.		LDAP Server Root	CA Certificate Services Root CA - *
LDAP Server Root CA	Certificate Services Root CA -				

注意:端口389是使用的默认端口。

4.在"属性"选**项**卡下,选择macAddress和说明属性,这些属性将用于授权策略

LDAP	Identity Sources List > I	dap_m	ab				
LDAF	Identity Source				_		
	General Cor	nectio	n	Directory Organization	Groups	Attributes	Advanced Settings
1	Edit 🕂 Add 👻 🗙 Dele	te Attri	bute				
	Name	-	Туре	Default	Internal Name		
	description		STRING		description		
	distinguishedName		STRING		distinguishedName	9	
	macAddress		STRING		macAddress		

5.要创建允许的协议,请转到**Policy->Policy Elements->Results->Authentication->Allowed Protocols。**定义并选择进程主机查找和允许PAP/ASCII作为唯一允 许的协议。最后选择"**保存"**

cisco Identity Services Engine	Home + C	ontext Visibility	Operations	* Policy	+ Administration
Policy Sets Profiling Posture	Client Provisioning	▼Policy Elements			
Dictionaries Conditions Resu	ults				
- Authentication	Allowed Protoc Allowed Protoc	ols Services List > M atocols	AB_MacAddres	•	
Allowed Protocols	Name	MAB_MacAddress]	
Authorization	Description				7
Profiling					
Posture	 Allowed Pr 	rotocols			
Client Provisioning	Authentication Bypass				
		Process Host Lookup	(E)		
	Auth	entication Protocoli	•		
		Allow PAP/ASCII			

6.要创建授权配置文件,请转至Policy->Policy Elements->Results->Authorization->Authorization Profiles。选择Add并定义将分配给终端的权限。

dentity Services Engine	Home	 Operations 	- Policy	Administration	Work Centers
Policy Sets Policy Elements					
Dictionaries Conditions Results	•				
Authentication	Standard Authorizati For Policy Export go to Adm	on Profiles inistration > Syster	m > Backup 8	Restore > Policy Expo	ort Page
- Authorization					
Authorization Profiles	/ Edit Add Lo Duplic	ate X Delete			
Downloadable ACLs	Name		Pi	rofile	
	Blackhole_Wireless_A	ccess	a di	🕻 Cisco 🕀	
Profiling	Cisco_IP_Phones			🕻 Cisco 🕀	
Posture	Cisco_Temporal_Onbo	pard	đ	🕻 Cisco 🕀	

dentity Services Engine	Home Context Visibility Operations Policy Administration Work Centers
Policy Sets Policy Elements	
Dictionaries + Conditions - Re	ults
Authentication	Authorization Profiles > New Authorization Profile Authorization Profile IName MACROPTSWITCHI DAP
Authorization Profiles	Description //
Downloadable ACLs	* Access Type ACCESS_ACCEPT T
Profiling	Network Device Profile 🛛 🗰 Cisco 💌 🕀
Posture	Service Template
Client Provisioning	Track Movement Passive Identity Tracking
	✓ Common Tasks
	DACL Name PERMIT_ALL_IPV4_TRAFFIC

7.转到Policy-> Policy Set,使用预定义条件Wired_MAB和步骤5中创建的Allowed Protocol创建策略集。

Policy Sets → MAB_LDAP			Reset Policyset Hitcounts Reset	Save
Status Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits
Search				
MAB_LDAP		Wred_MAB	MAB_MacAddress x v +	0

8.在新创建的策略集下,使用预定义的Wired_MAB库和LDAP连**接作为外**部身份**源序**列创建身份验证策略

Authentication	Policy (2)					
+ Status	Rule Name	Conditions		Use	Hits	Actions
learch						
				idap_mab ×	•	
				✓ Options		
				If Auth fail		
0	Auth_MAB_LDAP	Wind_MA8		REJECT * *	0	۰
		-		If User not found		
			REJECT * *			
				If Process fail		
				DROP × *		
0	Defeuit			DenyAccess ×		0
· ·			¢,	> Options		-

9.在授权策**略下**,使用LDAP属性说明、Radius NAS-Port-Id和NetworkDeviceName定义名称并创建复合条件。最后,添加在步骤6中创建的授权配置文件。

Library			Editor								
Search by Name				Click to add an attribute						00	
•		2 H G 1 G L 7		B	Equals	•	Attribute value				
	Cuest Flow	0			Click to add an attribute						0
MAC_in_SAN	Ø	AND •	E,	Equals	٠	Attribute value					
Image: Network_Access_Authentication_Passed () Image: Non_Cisco_Profiled_Phones () Image: Non_Compliant_Devices ()		ation_Passed ()			+ New AND OR						
		s ()		Set to Te and					Dunicate	Save	
			0010101	ion.				Dopicate	Charry		
C	Switch_Local_Web_Authen	tication 🕖									
C	Switch_Web_Authentication	0									
C	Wired_802.1X	Ø									
l p	Wired_MA8	Ø									
							Results				
Rule	Name Conditions						Results Profiles	Security Groups		Hits	Action
Rule	Name Conditions	klap_mab-description CONTAINS	Radius NAS-Port-Id Network Access Netw	vorkDeviceName			Results Profiles * MACPORTSWITCHLDAP	Security Groups	• *	Hits	Action ©

应用配置后,您应该能够连接到网络,而无需用户干预。

验证

连接到指定的交换机端口后,您可以键入show authentication session interface GigabitEthernet X/X/X details ,以验证设备的身份验证和授权状态。

Sw3650-mauramos#show auth sess inter gi 1/0/6 details Interface: GigabitEthernet1/0/6 IIF-ID: 0x103DFC000000B5 MAC Address: 6cb2.ae3a.686c IPv6 Address: Unknown IPv4 Address: User-name: 6C-B2-AE-3A-68-6C Status: Authorized Domain: Data Oper host mode: multi-domain Oper control dir: both Session timeout: N/A Restart timeout: N/A Common Session ID: 0A517F65000013DA87E85A24 Acct session ID: 0x000015D9 Handle: 0x9300005C Current Policy: Policy_Gi1/0/6 Local Policies: Service Template: DEFAULT_LINKSEC_POLICY_SHOULD_SECURE (priority 150) Security Policy: Should Secure Security Status: Link Unsecure Method status list: Method State mab Authc Success 在ISE上,您可以使用Radius实时日志进行确认。

0	Refresh O Reset Repeat Count	Export To 🕶								
	Time	Status	Details	Repeat	Identity	Endpoint ID	Endpoint P Au	uthentication Policy	Server	Authorization Profiles
×		•			Identity	Endpoint ID	Endpoint Prof A	Authentication Policy	Server	Authorization Profiles
	Jan 20, 2020 06:21:47.825 PM	•	0	0	employee1@ciscodemo.lab	6C:82:AE:3A:68:6C	Unknown		ise23-1	MACPORTSWITCHLDAP
	Jan 20, 2020 06:21:47.801 PM		0		employee1@ciscodemo.lab	6C:82:AE:3A:68:6C	Unknown		ise23-1	MACPORTSWITCHLDAP

故障排除

在LDAP服务器上,验证创建的设备是否配置了Mac地址、正确的交换机名称和交换机端口

CN=	LaptopTest Properties ? ×							
Attribute Editor Security								
Attributes:								
Attribute	Value 🔨							
lastKnownParent	<not set=""></not>							
macAddress	6C:B2:AE:3A:68:6C							
manager	<not set=""></not>							
mS-DS-ConsistencyC	<not set=""></not>							
mS-DS-ConsistencyG	<not set=""></not>							
msDS-LastKnownRDN	<not set=""></not>							
msDS-NcType	<not set=""></not>							
msSFU30Aliases	<not set=""></not>							
msSFU30Name	<not set=""></not>							
msSFU30NisDomain	<not set=""></not>							
name	LaptopTest							
nisMapName	<not set=""></not>							
0	<not set=""></not>							
objectCategory	CN=Device,CN=Schema,CN=Configuration, [🗸							
< 111	>							
Edit	Filter							
ОК	OK Cancel Apply Help							

CN=	LaptopTest Properties ? X						
Attributes:							
Attribute	Value						
adminDescription	(not set)						
adminDisplayName	<pre>cnot set></pre>						
bootFile	(not set)						
bootParameter	(not set)						
bootrarameter							
description	switchanflexconnect GigabitEthemet1/0/6						
disolavName	switchaphexconnect, digabitethemet 1/0/6						
displayName Printable	<not set=""> <not set=""> CN=LaptopTest,OU=AppleDevices,DC=cisco <not set=""></not></not></not>						
distinguishedName							
distinguistieutvattie							
dSCorePresentiaeD							
astoneiropagationD							
Race	<not set=""></not>						
Inags ISMO Dele Owner	<not set=""></not>						
rsivioRoleOwner	<not set=""></not>						
<	>						
Edit	Filter						
ОК	Cancel Apply Help						

在ISE上,您可以执行数据包捕获(转到**操作 — >故障排除 — >诊断工具 — >TCP转储**)以验证从LDAP发送到ISE的值

27 124,204080	16.61.127.189	18,81,127,111	Line	201	searchilequest(2) *80-Applebryloss_30-classdem_30-fait* wholafubtree		
28 124,388917	36.40.127.111	38.01.127.300	LOW	202	acanthheadetry(2) *OlecaptepText,00-AppTabexSces,80+clacadema,00+lab*	searchAudona(3)	BRECOTER .
29 314 MA281	18.81.127.189	38.45.127.113	LENP	233	searchRepuest131 "BondgeLeBentoes_DC+classidees_BC-fuilt" shefteftuiltiree		
10 114.108083	18.81.127.111	18,81,107,189	1.010	3502	searchMediatry(3) *Oh-Lagtaphert,Oh-AppleDevices,AD-classeea,AD-1ab*	searchAstbure(3)	\$800P\$8
31 134, 101373	18.81.127.189	18,81,127,111	LEMP	209	searchiequest(4) "BU-Appledevices_bC-classdemo_bC-las" wholefultree		
32 124, 305384	10.01.127.111	18.01.127.109	LEMP	- 04	scard/Audoral4) accoss 12 resulted		
33 315.404043	58.85.527.589	38.41.127.111	LENP	5/89	start/Meguest151 "RH/gp/eBrxtors_XC+classion_XC-fait" whitefultives		
					manufacture and the second sec		
* attribute	es: 3 liters						
V Parila	ART/IBURELIST LINE	description .					
1.00	el description						
* val	and 2 share						
	statistical and included in the	chap? (as come 1, 5) and	and the second of the	18.18			
v Partis	Anti-though in the	distinguished to a					
140	and still installations						
2 val	at 1 item	-					
	enclosed along the	and such that the latter	dama defenda	-	Bhilan .		
	Anness and the state	and the state of t	100000-000				
1 Parts	COLUMN STREAM FILST FLORE	Max. Materials					
1,00	El machelanes						
* vel	AC 3 1748						
	provident and all over 10 rd	2-18-18-18-18-					