# 基於ISE和LDAP屬性的身份驗證

### 目錄

### 簡介

本文檔介紹如何配置思科身份服務引擎(ISE)和使用輕量級目錄訪問協定(LDAP)對象屬性來動態驗證和授權裝置。

附註:本文檔對使用LDAP作為ISE身份驗證和授權的外部身份源的設定有效。

作者:Emmanuel Cano和Mauricio Ramos Cisco專業服務工程師。

由Neri Cruz Cisco TAC工程師編輯。

### 必要條件

### 需求

思科建議您瞭解以下主題:

- ISE策略集、身份驗證和授權策略的基本知識
- Mac Authentication Bypass(MAB)
- Radius通訊協定的基礎知識
- Windows伺服器基礎知識

### 採用元件

本檔案中的資訊是根據以下軟體和硬體版本:

- Cisco ISE 2.4版補丁11
- Microsoft Windows Server 2012 R2 x64版
- 思科交換機Catalyst 3650-24PD,版本03.07.05.E(15.2(3)E5)
- Microsoft Windows 7電腦

**附註:** 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。如果您的網路正在作用 ,請確保您已瞭解任何指令可能造成的影響。

### 組態

本節介紹如何配置網路裝置、ISE與LDAP之間的整合,並最終配置要用於ISE授權策略的LDAP屬性。

### 網路圖表

此圖說明所使用的網路拓撲:



以下是流量傳輸,如網路圖所示:

- 1. 使用者將其pc/筆記型電腦連線到指定的交換機埠。
- 2. 交換機向ISE傳送該使用者的Radius訪問請求
- 3. 當ISE收到資訊時,它將查詢特定使用者欄位的LDAP伺服器,其中包含要在授權策略條件中使用的屬性。
- 4. ISE收到屬性(交換機埠、交換機名稱和裝置mac地址)後,會比較交換機提供的資訊。
- 5. 如果交換機提供的屬性資訊與LDAP提供的屬性資訊相同,則ISE將傳送RADIUS Access-Accept,並在授權配置檔案中配置許可權。

### 組態

使用本節配置LDAP、交換機和ISE。

### 設定 LDAP

完成以下步驟以配置LDAP伺服器:

1.導航到Server Manager > Dashboard > Tools > ADSI Edit



2.按一下右鍵ADSI Edit圖示,然後選擇**Connect to...** 



3.在「連線設定」下,定義名稱並選擇確定按鈕以啟動連線。

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		
<ul> <li>Select or type a domain or server: (Server   Domain [:port])</li> </ul>		
×		
Default (Domain or server that you logged in to)		
Use SSL-based Encryption		
Advanced OK Cancel		

4.在同一ADSI Edit選單下,按一下右鍵DC連線(DC=ciscodemo, DC=lab),選擇**New,然**後選擇選項**Object** 

	h		1		
tin		New	•	0	Object
npute nain C eignSe tAndF naged		Rename Refresh Properties Help		-	
)S Qu( gram D :em /I Devic rs IUsers	ata es				

<sup>5.</sup>選擇選項OrganizationalUnit作為新對象,然後選擇「下一步」。

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

6.定義新OrganizationalUnit的名稱,然後選擇「下一**步」** 

	Create Object X		
Attribute:	0U		
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.按一下右鍵剛建立的OrganizationalUnit,然後選擇**New > Object**

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=Progran	Rename		
CN=System	Refresh		
CN=TPM De	E		
CN=Users	Export List		
CN=VPNUse	Properties		
OU=Develop	Help		
🧾 OU=AppleDe	Tieb		

	Create Object	
Select a da	355:	
	builtinDomain classStore computer contact container country	
	device dfsConfiguration domainDNS domainPolicy friendlyCountry	
	arounOff IniqueNames	
	< Back Next > Cancel Help	

10.在「值」(Value)欄位中定義名稱,然後選擇「下一個」(**Next)** 

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

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

11.對於下拉選單,**選擇要檢視的屬性**,選擇選項**macAddress**,然後在**Edit attribute**欄位下定義要驗證的終端Mac地址,然後選擇 **Add**按鈕儲存裝置MAC地址

注意:在mac地址八位元之間使用雙冒號代替點或連字元。

0

cn=LaptopTest ×				
Attributes				
Path: Class: device				
Select which properties to view:	Optional 🗸			
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.選擇**OK**以儲存資訊並繼續配置裝置對象

13.選擇**完成**以建立新的裝置對象

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.按一下右鍵裝置對象並選擇選項Properties

ADSI Edit

1	Name		Class	Distinguished Name
l	CN=LaptopTest	lame Class CN=LaptopTest device  CN=LaptopTest Delete Rename  Properties Help		CN=LaptopTest,OU=AppleDevices,DC=ciscoise,DC=lab
		Move		
		Delete		
		Rename	:	
1		Propert	ties	
		Help		

15.選擇description選項,然後選擇Edit以定義交換器名稱和裝置所連線的交換器連線埠。

tribute Editor Security	1
Security	
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=Laptop Test,OU=AppleDevices,DC=cisc
dSASignature	<not set=""></not>
dSCorePropagationD	0x0 = ( )
extensionName	<not set=""></not>
flags	<not set=""></not>
<b>fSMORoleOwner</b>	<not set=""></not>
< 111	>
Edit	Filter
OK	Creard Arabi

16.定義交換機名稱和交換機埠,請確保使用逗號分隔每個值。選擇Add,然後選擇Ok以儲存資訊。

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

• Switchapflexconnect是交換機名稱。

● GigabitEthernet1/0/6是終端所連線的交換機埠。

附註: 可以使用指令碼將屬性新增到特定欄位,但是,對於本示例,我們正在手動定義這些值

**附註**: AD屬性區分大小寫,如果您在LDAP查詢期間使用小寫形式的所有Mac地址,則ISE會轉換為大寫。為了避免此行為,請在允許的協定下禁 用進程主機查詢。詳細資訊可以在以下連結中找到:<u>https://www.cisco.com/c/en/us/td/docs/security/ise/3-0/admin\_guide/b\_ISE\_admin\_3\_0.pdf</u>

### 交換器組態

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 !

#### 附註:可能需要在您的環境中調整全域性和介面配置

#### ISE 組態

以下說明在ISE上配置從LDAP伺服器獲取屬性並配置ISE策略。

**1.**在ISE上,轉至**管理— >身份管理— >外部身份源**,選擇LDAP資料夾,然後按一下Add以建立與LDAP的新連線

dentity Services Engine	Home	✓ → Operations →	Policy  Administration	Work Centers     ■
System      Identity Management	Network Resources     Dev	rice Portal Management	pxGrid Services	
Identities Groups External Iden	ntity Sources Identity Source S	equences + Settings		
External Identity Sources	LDAP Ider	Add C Duplicate X Dek	ete Descripti	on

2.在General頁籤下,定義名稱,然後選擇mac地址作為主題名稱屬性

LDAP Identity Sources List > Ide	p_mab				•	
LDAP Identity Source General Conne	ection Directory Organization	n Groups	Attributes	Advanced Settings		
LDAP Identity Source       Connection       Dendory Organization       Groups       Attributes       Advanced Settings         * Name       isag_mab         Description       isag_mab         * Subject Objectitates       device       * Group Rap Attributes       immedian         * Subject Objectitates       device       * Group Rap Attributes       immedian         * Subject Objectitates       device       Certificate Attributes       immedian         * Subject Objectitate Reference To Groups       Gestificate Attributes       immedian         * Subject Objects Contain Reference To Groups       States in Groups Are Stored in Member Attributes in Comparisonal Units       immedian         * Pink Name       Depariment       immedian       immedian         Jub Tile       Loganizational Unit       immedian       immedian         Jub Tile       Loganizational Unit						
* Subject Objectclass	device	* Group Objectclass	Group			
* Subject Name Attribute * Group Name Attribute	distinguishedName	* Group Map Attribute Certificate Attribute	member			
<ul> <li>Subject Objects Conta</li> </ul>	in Reference To Groups					
<ul> <li>Group Objects Contail</li> </ul>	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				
Street Address						

#### 3.在Connection頁籤下,從LDAP伺服器配置IP地址、管理員DN和密碼以成功連線。

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	<ul> <li>Anonymous Access</li> </ul>			Acce	ess 🛞 Anonymous Access
	<ul> <li>Authenticated Access</li> </ul>				<ul> <li>Authenticated Access</li> </ul>
Admin DN	* cn=administrator, cn=users, dc=	c		Admin I	DN
Password	• •••••			Passwo	ord
		_			
Carry a Authentication	Enable Service Authentication			Eastern Authenticati	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 -				

### **附註**:埠389是使用的預設埠。

4.在Attributes頁籤下,選擇macAddress和description屬性,這些屬性將在授權策略中使用

vanced Settings
va

5.要建立允許的協定,請轉至**策略 — >策略元素 — >結果 — >身份驗證 — >允許的協定。**定義並選擇進程主機查詢和允許PAP/ASCII作為唯一允許的協定。 最後選擇**儲存** 

dentity Services Engine	Home + C	ontext Visibility	Operations	* Policy	+ Administration
Policy Sets Profiling Posture	Client Provisioning	* Policy Elements			
Dictionaries + Conditions • Re	sults				
- Authentication	Allowed Protoc     Allowed Protoc	ois Services List > M otocols	AB_MacAddres	•	
Allowed Protocols	Name	MAB_MacAddress		]	
Authorization	Description				1
Profiling					
Posture	<ul> <li>Allowed Pr</li> </ul>	rotocols			
Client Provisioning	Auth	entication Bypass			
		Process Host Lookup	(i)		
	Auth	entication Protocols	•		
		Allow PAP/ASCII			

6.要建立授權配置檔案,請轉到**策略 — >策略元素 — >結果 — >授權 — >授權配置檔案。選擇Add**並定義將分配給終結點的許可權。

dentity Services Engine	Iome	<ul> <li>Operations</li> </ul>	- Policy	Administration	<ul> <li>Work Centers</li> </ul>
Policy Sets   Policy Elements					
Dictionaries  Conditions Results					
0					
Authentication	Standard Authorizati	on Profiles			
- Authorization	For Policy Export go to Adm	ninistration > System	m > Backup 8	Restore > Policy Expo	ort Page
Authorization Profiles	🥖 Edit 🕂 Add 🕞 Duplic	ate 🗙 Delete			
Downloadable ACI s	Name		Pi	rofile	
Dominoadable AGEs	Blackhole_Wireless_A	ccess	40	🕻 Cisco 🕀	
▶ Profiling	Cisco_IP_Phones		-	Cisco 🕀	
▶ Posture	Cisco_Temporal_Onb	pard		🕻 Cisco 🕀	

dentity Services Engine	Home	<ul> <li>Operations</li> </ul>	Policy Administrat	ion	
Policy Sets					
Dictionaries + Conditions - Resul	is				
Authentication     Authorization	Authorization Profiles > New Authorization Profile * Name	Authorization Profile	P		
Authorization Profiles Downloadable ACLs	Description  * Access Type	ACCESS_ACCEPT	Ţ		
Profiling	Network Device Profile	👬 Cisco 👻 🕀			
▶ Posture	Service Template				
Client Provisioning	Track Movement Passive Identity Tracking				
	Common Tasks     DACL Name	PERM	IT_ALL_IPV4_TRAFFIC	0	

### 7.轉至Policy-> Policy Set,使用預定義條件Wired\_MAB和步驟5中建立的允許協定建立策略集。

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

### 8.在新建立的策略集下,使用預定義的Wired\_MAB庫和LDAP連線作為外部身份源序列建立身份驗證策略

+ Status Rule Name	Conditions	Use	,	Hits Action
earch				
		ldap_mab	х т	
		✓ Options		
		If Auth fail		
Auth MAB LDAP	E Wred MAB	REJECT	× *	
		If User not found		
		REJECT	* *	
		If Process fail		
		DROP	**	
		Development		
<ul> <li>Default</li> </ul>				• •
Ueraux		Options		•

9.在**授權策略**下,使用LDAP屬性說明、Radius NAS-Port-Id和NetworkDeviceName定義名稱並建立複合條件。最後,新增在步驟6中建立的授權配置檔案。

		E	litor								$\sim$
Search by Name											00
♥ ☞ □ ▲ ● 및 ⊕ ₽ © ⊉ € © 1 ● Ł ♥				Ê.	Click to acc	an aun	Attribute uniture				
					Equals	-	Attricute value			-	0
Guest_Flow		0	10.1	L	Click to add an attribute						
MAC_in_SAN		ø	440 •	C,	Equals	•	Attribute value				
Network_Access	Authentication_Passed	Ø									
Non_Cisco_Profi	ed_Phones	0									2
Non_Compliant_Devices		Ø		Set to 'ls not' Du					Duplicate	Save	
Switch_Local_W	b_Authentication	Ø									
Switch_Web_Aut	hentication	0									
Wired 802.1X		Ø									
		0									
Wired_MAB		ω									
Wired_MAB		W									

套用組態後,您應該能夠連線到網路,無需使用者干預。

### 驗證

連線到指定的交換機埠後,可以鍵入show authentication session interface GigabitEthernet X/X/X details以驗證裝置的身份驗證和授權狀態。

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即時日誌進行確認。

C Refresh O Reset Repeat Counts 🕹 Export To +										
	Time	Status	Details	Repeat	Identity	Endpoint ID	Endpoint P Authentication Policy	Server	Authorization Profiles	
×					Identity	Endpoint ID	Endpoint Prof Authentication Policy	Server	Authorization Profiles	
	Jan 20, 2020 06:21:47.825 PM	<ul> <li>a</li> <li>o</li> </ul>		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	

## 疑難排解

在LDAP伺服器上,驗證建立的裝置是否配置了Mac地址、正確的交換機名稱和交換機埠

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	Cancel Apply Help

CN=	LaptopTest Properties ? ×					
Attribute Editor Security						
Attributes:						
Attribute	Value ^					
adminDescription	<not set=""></not>					
admin DisplayName	<not set=""></not>					
bootFile	<not set=""></not>					
bootParameter	<not set=""></not>					
cn	Laptop Test					
description	switchapflexconnect,GigabitEthernet1/0/6					
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					
ОК	Cancel Apply Help					

### 在ISE上,您可以進行資料包捕獲(轉至**操作 — >故障排除 — >診斷工具 — >TCP轉儲**)以驗證從LDAP傳送到ISE的值

_										
	27	134,204090	18.81.127.189	18,81,127,111	LENP	201	searchiequest(2) *8x4gplabruloes,8C+classdem,8C+latP wholefultree			
	28	124.308017	36.41.127.111	38.01.127.300	LOW	202	searchilesCetry/2) *Ol-Laptaphort,00-Applatectors,80-clacations,80-lab*	neart/Mexbore(3)	B&CODER	
	29	324.202231	18.81.127.189	38.81.127.111	1.010*	233	searchRepuest131 "Rhdyp1eDextors.3C+classedees.3C-full" whefefbeltree			
	-	324, 128283	18.81.127.111	18,81,107,189	1.010	110	searchiestery(3) *06-LagtapText,00-App1etexices,80-ciacadeea,80-lab*	searchedure(3)	Saccess -	
	31	124,201273	18.81.127.189	18,81,127,111	LENP	100	searchRequest(4) "WvAgpleDevices,DCvclassdemo,DCvlas" wholeSubtree			
	32	124,305384	10.01.127.111	18.41.127.349	LEMP	- 64	searchNexDerai4i saccoss [] resaited			14
	33	121,494343	14.41.127.149	38.41.127.111	LENP	3/89	searchRepuest(5) "WeightBeckers,80+classelees,80-fait" wheirfultree			12
	1.4	and monthly			1.000	-	manufacture and the second states and the se			
		+ attribut	est 3 pleas							
		v Paris	AND INCOME.	description.						
		1.0	and description inc.							
			and the second second							
			act a 1740			-				
			BUILT (BALLENGT OF 1 1941)	tchop? Lexcement 4, Coper	(1)(pre-set 2)	e. e.				
		<ul> <li>Perta</li> </ul>	AMENTING AND A LOSS	distinguishediane						
		1.6	e: distinguishedNam							
		11 Mail	at 1 item							
			Anti-constantiations (Sec.	and such as a diffusion further	term Martine		- Ministra			
			all and the set of the	and the state of t	100000-0000					
		1 10111	PORTO INCOME INT. LONG	Max. Materials						
		1,6	Peri mechenines							
		T 19	act 3 sham							
			AntroputeNalues 80:8	12:AE:3A:68:60						