ISEおよびLDAP属性ベースの認証

内容

<u>概要</u> <u>前提条件</u> <u>要件</u> <u>使用するコンポーネント</u> <u>コンフィギュレーション</u> <u>ネットワーク図</u> <u>設定</u> <u>LDAP の設定</u> <u>スイッチの設定</u> <u>ISE の設定</u> <u>確認</u> トラブルシュート

概要

このドキュメントでは、Cisco Identity Services Engine(ISE)を設定し、Lightweight Directory Access Protocol(LDAP)オブジェクト属性を使用してデバイス を動的に認証および許可する方法について説明します。

注:このドキュメントは、LDAP を ISE 認証および承認のための外部 ID ソースとして使用するセットアップに適用されます。

著者:シスコプロフェッショナルサービスエンジニア、Emmanuel CanoおよびMauricio Ramos

編集: Neri Cruz Cisco TACエンジニア

前提条件

要件

次の項目に関する知識があることが推奨されます。

- ISEポリシーセット、認証、および認可ポリシーに関する基礎知識
- Mac認証バイパス(MAB)
- Radiusプロトコルに関する基礎知識
- Windowsサーバに関する基礎知識

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Cisco ISE、バージョン2.4パッチ11
- Microsoft Windows Serverバージョン2012 R2 x64
- CiscoスイッチCatalyst 3650-24PD、バージョン03.07.05.E(15.2(3)E5)
- Microsoft Windows 7マシン

注: このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは 、初期(デフォルト)設定の状態から起動しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜 在的な影響について確実に理解しておく必要があります。

コンフィギュレーション

このセクションでは、ネットワークデバイスの設定方法、ISEとLDAPの統合、および最終的にISE認可ポリシーで使用するLDAP属性の設定方法について説 明します。

ネットワーク図

次の図に、使用するネットワーク トポロジを示します。



次のネットワーク図にトラフィック フローを示します。

- 1. ユーザは自分のpc/ラップトップを指定スイッチポートに接続します。
- 2. スイッチはそのユーザのRADIUS Access-RequestをISEに送信します
- 3. ISEが情報を受信すると、LDAPサーバに対して特定のユーザフィールドを照会します。これには、認可ポリシー条件で使用される属性が含まれます。
- 4. ISEが属性(スイッチポート、スイッチ名、およびデバイスのMACアドレス)を受信すると、スイッチが提供する情報を比較します。
- 5. スイッチによって提供される属性情報がLDAPによって提供される属性情報と同じ場合、ISEはRADIUS Access-Acceptを、認可プロファイルに設定 された権限とともに送信します。

設定

このセクションでは、LDAP、スイッチ、およびISEを設定します。

設定 [LDAP]

LDAPサーバを設定するには、次の手順を実行します。

1.「サーバー・マネージャ」>「ダッシュボード」>「ツール」>「ADSI編集」に移動します。

taka .	Server manager	
© @-	Server Manager • Dashboard	• 🗇 🍢 Manage Tools View Help
		Active Directory Administrative Center
		Active Directory Domains and Trusts
E Dashboard	WELCOME TO SERVER MANAGER	Active Directory Lightweight Directory Services Setup Wizard
Local Server		Active Directory Module for Windows DowerShall
 Coost Server 		Active precisity module for minuous comeraneli
All Servers	Configure this local conver	Active Directory Sites and Services
IR AD CS	Conligure this local server	Active Directory Users and Computers
M in ac	01000 00000	ADSI Edit
IEI AD DC	CHER & START	

2. ADSI Editアイコンを右クリックし、Connect to...を選択します。



3.接続の設定で名前を定義し、「OK」ボタンを選択して接続を開始します。

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			
 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.同じ[ADSI Edit]メニューでDC接続(DC=ciscodemo、DC=lab)を右クリックし、[New]を選択し、オプション[Object]を選択します



5.新しいオブジェクトとして[OrganizationalUnit]オプションを選択し、[次へ]を選択します。

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.新しいOrganizationalUnitの名前を定義し、[**Next**]を選択します

	Create Object X
Attribute:	ou
Syntax:	Unicode String
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.作成したOrganizationalUnitを右クリックし、[New] > [Object]を選択します

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	ĸ
Select a class:	
builtinDomain dassStore computer contact container country device dfsConfiguration domainDNS domainPolicy friendlyCountry group rrounOff IniqueNames	
< Back Next > Cancel Help	-

10.「値」フィールドで名前を定義し、「次へ」を選択**します**

	Create Object X
Attribute:	an
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. More Attributes	
< Back Finish Cancel Help	

11.ドロップダウンメニューで、表示するプロパティを選択し**て、macAddressオプションを選択**し、次に**Edit属性フィールドで認証されるエンドポイント Macアドレスを定義し**て、 **[Add]**ボタンをクリックして、デバイスのMACアドレスを保存します。

注:MACアドレスオクテット間には、ドットやハイフンの代わりに二重コロンを使用します。

cn=LaptopTest			
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. [**OK**]を選択して、情報を保存し、デバイスオブジェクトの設定を続行します

13.新しいデバイスオ**ブジェクト**を作成するには、[Finish]を選択します

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.デバイスオブジェクトを右クリックし、[プロパティ]オプションを選択**します**

ADSI Edit

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

15.オプションの[**description**]を選択し、[**Edit**]を選択して、デバイスが接続されるスイッチ名とス イッチポートを定義します。

tribute 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	<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

16.スイッチ名とスイッチポートを定義します。各値をカンマで区切ってください。[追**加]を**選択し、[**OK**]を選択して情報を保存します。

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

- Switchflexconnectはスイッチ名です。
- GigabitEthernet1/0/6は、エンドポイントが接続されているスイッチポートです。

注:スクリプトを使用して特定のフィールドに属性を追加することもできますが、この例では、値を手動で定義します

注: AD属性では大文字と小文字が区別されます。小文字のISEですべてのMacアドレスを使用すると、LDAPクエリ中に大文字に変換されます。 この動作を回避するには、許可されたプロトコルでProcess Host Lookupを無効にします。詳細については、次のリンクを参照してください。 https://www.cisco.com/c/en/us/td/docs/security/ise/3-0/admin_guide/b_ISE_admin_3_0.pdf

スイッチの設定

ISE802.1x

aaa new-model ! aaa group server radius ISE server name ISE deadtime 15 ! aaa authentication dotlx default group ISE aaa authorization network default group ISE aaa accounting update newinfo aaa accounting dotlx 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 ! dotlx system-auth-control dotlx 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 dotlx 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 dotlx mab authentication priority dotlx mab authentication port-control auto authentication periodic authentication timer reauthenticate server authenticator timer inactivity server dynamic authentication violation restrict mab dotlx pae authenticator dotlx 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: グローバルおよびインターフェイスの設定は、環境で調整する必要がある場合があります

ISE の設定

次に、LDAPサーバから属性を取得し、ISEポリシーを設定するためのISEの設定について説明し ます。

1. ISEで、[Administration] > [Identity Management] > [External Identity Sources]に移動し、[LDAP]フォルダを選択し、[Add]をクリックしてLDAPとの

新しい接続を作成します			
dentity Services Engine Home	Context Visibility Operations	Policy Administration	Work Centers
System Identity Management Netwo	k Resources	nt pxGrid Services	
Identities Groups External Identity Source	Identity Source Sequences	gs	
External Identity Sources	Edit Add Ch Duplicate	Delete	
Active Directory	Name	 Descripti 	on
CDAP ODBC RADIUS Token RSA SecurID SAML Id Providers Social Login			

2. [General] タブで名前を定義し、サブジェクト名属性としてMACアドレスを選択します

LDAP Identity Sources List > Id	ap_mab					,	
LDAP Identity Source							
General Conn	ection	Directory Organization	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	distinguishedN	ame	Certificate Attribute				
 Subject Objects Cont 	ain Reference To	Groups					
 Group Objects Conta 	in Reference To 5	lubjects					
	Subjects	In Groups Are Stored	In Member Attribute As	Distinguished Name	e T		
User Info Attributes T							
First Name			Department				
Last Name			Organizational Unit				
Job Title			Locality				
Email			State or Province				
Telephone			Country				
Street Address							

3. [Connection] タブで、LDAPサーバからのIPアドレス、管理DN、およびパスワードを設定し、正常な接続を確立します。

AP Identity Source					
General Connection	Directory Organization	Groups	Attributes	Advanced Settings	
Prima	ry Server				Secondary Server
					Enable Secondary Server
*Hostname/IP 10.8	.127.111			Hostname/IP	<i>x</i>
* Port 389				Port	389
Specify server for each ISE node					
Access	Anonymous Access			Ac	coess 💿 Anonymous Access
	Authenticated Access	_			Authenticated Access
Admin DN	 cn=administrator, cn=users, dc= 	c		Admi	n DN
Password	•			Pass	word
Secure Authentication	Enable Server Identity Check			Secure Authentic	Enable Server Identity Check
LDAP Server Root CA	Certificate Services Root CA - *	x		LDAP Server Roo	CA Certificate Services Root CA - *
Issuer CA of ISE Certificates	Select if required (optional) *	æ.		Issuer CA of ISE Certific	cates Select if required (optional) *

注:ポート389はデフォルトで使用されるポートです。

4. [Attributes] タブでmacAddress属性とdescription属性を選択すると、これらの属性が認可ポリシーで使用されます

LDAP Identity Sources List > Idap_mab

LDAP Identity Source

General C	connection	1	Directory Organization	Groups	Attributes	Advanced Settings
/ Edit 🕂 Add 👻 🗙 De	elete Attrib	ute				
Name	-	Туре	Default	Internal Name		
description		STRING		description		
distinguishedName		STRING		distinguishedNan	ne	
macAddress	- 4	STRING		macAddress		

5.許可されたプロトコルを作成するには、[**Policy] -> [Policy Elements] -> [Results] -> [Authentication] -> [Allowed Protocols]に移動します。**許可される唯一 のプロトコルとして、[Process Host Lookup]と[Allow PAP/ASCII]を定義して選択します。最後に[保存]を選択**します**

cisco Identity 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	ols Services List > M otocols	IAB_MacAddres	•		
Allowed Protocols	Name	MAB_MacAddress]		
Authorization	Description	Description				
Profiling						
Posture	 Allowed Pr 	rotocols				
+ Client Provisioning	Auth	Authentication Bypass				
	Auth	entication Protocol				
		Allow PAP/ASCII				

6.認可プロファイルを作成するには、[**Policy] -> [Policy Elements] -> [Results] -> [Authorization] -> [Authorization Profiles]に移動します。[Add]</mark>を選択し、エ ンドポイントに割り当てる権限を定義します。**

eligite Identity Services Engine	Iome	Operations Policy	 Administration 	• Work Centers
Policy Sets Policy Elements				
Dictionaries Conditions Results				
0				
Authentication	Standard Authorization F	Profiles		
- Authorization	For Policy Export go to Administr	ration > System > Backup &	& Restore > Policy Export	t Page
Authorization Profiles	/ Edit Add Duplicate	X Delete		
Downloadable ACLs	Name	P	Profile	
Dominious abio Proces	Blackhole_Wireless_Acces	S d	ដ Cisco 🕀	
▶ Profiling	Cisco_IP_Phones	4	Cisco 🕀	
→ Posture	Cisco_Temporal_Onboard	đ	🕫 Cisco 🕀	
	-			

dentity Services Engine	Home	Operations Policy	Administration	Work Centers
Policy Sets Policy Elements				
Dictionaries + Conditions - Resul	ts			
Authentication	Authorization Profiles > New Aut Authorization Profile	thorization Profile		
 Authorization 	* Name MA	CPORTSWITCHLDAP]	
Authorization Profiles	Description			li.
Downloadable ACLs	* Access Type ACC	CESS_ACCEPT ·		
Profiling	Network Device Profile	Cisco 👻 🕀		
Posture	Service Template			
Client Provisioning	Track Movement	D		
	Passive Identity Tracking 🔄 🛛	Ð		
	✓ Common Tasks			
	DACL Name	PERMIT_ALL_IPV	4_TRAFFIC 📀	

7. [Policy] -> [Policy Set] に移動し、事前に定義された条件Wired_MABと手順5で作成した許可プロトコルを使用してポリシーセットを作成します。

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

8.新しいポリシーセットで作成された認証ポリシーは、定義済みの**Wired_MAB** Libraryと**LDAP**接続を外部アイデンティティソースシーケンスとして使用し ます

Authe	ntication	Policy (2)							
٠	Status	Rule Name	Con	itions		Use		Hits	Actions
Search									
						idap_mab	ж т		
						▼ Options			
						If Auth fail			
	Ø	Auth MAB LDAP		Wired MAB		REJECT	× *	0	0
			_			If User not found			
						REJECT	× *		
						If Process fail			
					DROP	**			
						DenyAccess	**		
	0	Default			¢	> Options		0	•

9. [Authorization Policy] で、LDAP属性の説明、Radius NAS-Port-Id、およびNetworkDeviceNameを使用して名前を定義し、複合条件を作成します。最後 に、手順6で作成した認可プロファイルを追加します。

Conditions Studio	Editor)×
	7 6	Click to add an attribute	n attribute		
EAP-TLS		Equals • Attribute value	9		0
Guest_Flow Ø	AND • E	Click to add an attribute Equals Attribute value	2		
Network_Access_Authentication_Passed		+ New AND OR			
Non_Cisco_Profiled_Phones Non_Compliant_Devices	Set	s not	o S a	wo	
Switch_Local_Web_Authentication					
Switch_Web_Authentication					
Wired_MAB Ø					
		Results			
Rule Name Conditions		Profiles	Security Groups	Hits	Action
MAB_LDAP AND L Idap_mab-description CONT	AINS Radius NAS-Port-Id AINS Network Access NetworkDevic	* MACPORTSWITCHLD	AP Select from list	•	۰
			and the second sec	100	

構成を適用した後、ユーザーの介入なしにネットワークに接続できるようになります。

確認

指定スイッチポートに接続したら、<mark>show authentication session interface GigabitEthernet X/X/X detailsを入力して、デバイスの認証および許可ステータス</mark> **を確認できま**す。

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 ISEでは、RADIUSライブログを使用して確認できます。

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	•	0	0	employee1@ciscodemo.lab	6C:82:AE:3A:68:6C	Unknown		ise23-1	MACPORTSWITCHLDAP
	Jan 20, 2020 06:21:47.801 PM		Q		employee1@ciscodemo.lab	6C:82:AE:3A:68:6C	Unknown		ise23-1	MACPORTSWITCHLDAP

トラブルシュート

LDAPサーバで、作成したデバイスにMacアドレス、適切なスイッチ名、およびスイッチポートが設定されていることを確認します

CN=LaptopTest Properties ? X						
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 ? X				
Attribute Editor Security					
Attributes:					
Attribute	Value ^				
adminDescription	<not set=""></not>				
adminDisplayName	<not set=""></not>				
bootFile	<not set=""></not>				
bootParameter	<not set=""></not>				
cn	LaptopTest				
description	switchapflexconnect,GigabitEthemet1/0/6				
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				

ISEでパケットキャプチャ(**Operations->Troubleshoot->Diagnostic Tool->TCP Dumps**)を実行し、LDAPからISEに送信される値を検証できます

_								
	27	134,204090	18.81.127.189	18,81,127,111	LENP	201 searching	est121 "Workplatevices,80-classees,80-fath" whitelatives	
	28	124,308017	58.40.127.111	38.81.127.300	LEMP	202 searchillend	stry(2) "Ok-Laptophort,00-Appladencions,80-clacations,90-late" searchileadene(2) account	
	29	324.202231	18.81.127.189	38,41,127,113	LEHP	233 searchillog.	ext131 "Rodgetebeviors,3C+classdem,3C+las" whitebatives	
	- 10	324, 128283	18.81.127.111	18,81,127,189	1.010	INJ searchillerd	stry(3) "Ok-Laptaphert, 00-Appleden/cost, 80-Clarabea, 80-lab" usarr/Medbae(3) saccess	
	31	124, 101273	18.81.127.189	18,81,127,111	LEMP	200 searchiles	esti41 "Rowgplebewices,DC+classdemo,DC+las" wholeholdrive	
	32	124, 305384	10.01.127.111	18.01.127.109	LEMP	di searchied	wei4) access (2 results)	
	33	325,494545	58.85.527.589	38.41.127.111	LENP	100 searchillers	est151 "Rivigeladexions,80-ciscolom,80-lati" whiteSubtree	
		and monoral			- 81108		support account of an elast	
		* attribut	tes: 3 items					
		V Parts	aMUVIAANI De	 description 				
		19	pel description					
		- VE	fail 3 Jhem					
			Annesburghung sur-	tchap/Texcomect_dapab	(ADD-enset)./B	a		
		 Parts 	WATTY INVESTIGATION	 #Ls/Linguis/indiane 				
		1.0	pe: distinguishedMar	No.				
		7 V8	taci 1 item					
			Antrobutativities On-	LaptourTest_200-AppTothev	ices. Rectarge	dene, BO+Late		
		 Pariti 	information in the	a manifederate				
		1.0	peci machildrass					
		7.14	lac 3 item					
			AttributeValues 801	82-AE-3A-68-6C				