使用外部LDAPS身份庫配置ISE並對其進行故障 排除

目錄
<u>必要條件</u>
採用元件
<u>設定</u>
網路圖表
<u>在Active Directory上配置LDAPS</u>
在域控制器上安裝身份證書
訪問LDAPS目錄結構
<u>將ISE與LDAPS伺服器整合</u>
設定交換器
配置終端
在ISE上配置策略集
<u>驗證</u>
<u>疑難排解</u>
相關資訊

簡介

本文檔介紹思科ISE與作為外部身份源的安全LDAPS伺服器的整合。

必要條件

需求

思科建議您瞭解以下主題:

- 身份服務引擎(ISE)管理基礎知識
- Active Directory/安全輕量型目錄存取通訊協定(LDAPS)基礎知識

採用元件

本文中的資訊係根據以下軟體和硬體版本:

- Cisco ISE 2.6補丁7
- 安裝了Active Directory輕型目錄服務的Microsoft Windows 2012 R2
- 安裝了本機請求方和使用者證書的Windows 10 OS PC

• 採用152-2.E6映像的Cisco交換器C3750X

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。如果您的網路運作中,請確保您瞭解任何指令可能造成的影響。

背景資訊

LDAPS允許在建立目錄繫結時對傳輸中的LDAP資料(包括使用者憑據)進行加密。LDAPS使用 TCP埠636。

LDAPS支援以下身份驗證協定:

- EAP通用權杖卡(EAP-GTC)
- 密碼驗證通訊協定(PAP)
- EAP傳輸層安全(EAP-TLS)
- 受保護的EAP傳輸層安全(PEAP-TLS)

◆ 註:LDAPS外部身份源不支援EAP-MSCHAPV2(作為PEAP、EAP-FAST或EAP-TTLS的內部 方法)、LEAP、CHAP和EAP-MD5。

設定

本節介紹網路裝置的配置以及ISE與Microsoft Active Directory(AD)LDAPS伺服器的整合。

網路圖表

在此配置示例中,端點使用乙太網連線,通過交換機連線到區域網(LAN)。連線的交換機埠配置為 802.1x身份驗證,以通過ISE驗證使用者。在ISE上,LDAPS配置為外部身份庫。

此圖說明所使用的網路拓撲:



Secure LDAP Server

在Active Directory上配置LDAPS

在域控制器上安裝身份證書

若要啟用LDAPS,請在域控制器(DC)上安裝符合以下要求的證書:

- 1. LDAPS證書位於域控制器的個人證書儲存中。
- 2. 與證書匹配的私鑰存在於域控制器的儲存中,並且與證書正確關聯。
- 3. 增強型金鑰使用擴展包括伺服器身份驗證(1.3.6.1.5.5.7.3.1)對象識別符號(也稱為OID)。
- 4. 域控制器的完全限定域名(FQDN)(例如,DC1.testlab.com)必須存在於以下屬性之一中:「主題」(Subject)欄位中的「公用名」(CN)和「主題備用名稱擴展」(Subject Alternative Name Extension)中的DNS條目。
- 5. 證書必須由域控制器和LDAPS客戶端信任的證書頒發機構(CA)頒發。對於可信的安全通訊 ,客戶端和伺服器必須信任對方的根CA和向其頒發證書的中間CA證書。
- 6. 必須使用通道加密服務提供程式(CSP)生成金鑰。

	Certificate	x
General Details	Certification Path	
Show: <all></all>	~	
Field	Value	
Issuer	testlab-DC1-CA-1, testlab, com	
📴 Valid from	Friday, October 11, 2019 2:03:01 AM	
🔄 Valid to	Saturday, October 10, 2020 2:03:01 AM	
Subject	DC1.testlab.com	
📴 Public key	RSA (2048 Bits)	
Certifica	DomainController	
Enhance	Client Authentication (1.3.6.1.5.5.7.3.2), Server Auth	·
<		
Other Name:		
DS Object G	ouid=04 10 a6 36 1d 3c f4 3f a8 47 83 d7 d3 d5 46 20 a3 3	f
Divo Ivallie – DC	1.105000.0011	
Show: <al> Field Field Issuer Valid from Valid to Valid to Subject Public key Certifica Enhance Other Name: DS Object G DNS Name=DC</al>	Value ^ testlab-DC1-CA-1, testlab, com Friday, October 11, 2019 2:03:01 AM Saturday, October 10, 2020 2:03:01 AM DC1.testlab.com RSA (2048 Bits) DomainController III Value	f

訪問LDAPS目錄結構

要訪問Active Directory伺服器上的LDAPS目錄,請使用任何LDAP瀏覽器。本實驗使用Softerra LDAP Browser 4.5。

1.在TCP埠636上建立到域的連線。

+ Value Type Size Not Expan unknown 3.2 KB Group Server Profile Softerra LDAP Browser Softernet Public Servers

2.為簡單起見,在AD中建立名為ISE OU的組織單元(OU),並且必須具有一個名為UserGroup的組 。建立兩個使用者(user1和user2),並使其成為組UserGroup的成員。



Scope Pane 🔹 🗙	Name 🔺	Value	Type
Softerra LDAP Browser	CN	UserGroup	Entry
😟 📲 Internet Public Servers	CN	user2	Entry
i destab	CN	user1	Entry
E-CN=Builtin	CN	DESKTOP-19	Entry
CN=Computers	CN	ComputerGroup	Entry
OU=Domain Controllers	distinguishedName	OU=ISE OU,DC=testlab,DC=com	Attribute
E CN=ForeignSecurityPrincipals	dSCorePropagationData	1/1/1601	Attribute
CN=Infrastructure	dSCorePropagationData	6/20/2020 2:51:11 AM	Attribute
OU=ISE Group	🗉 gPLink	[LDAP://m={21A53B13-6971-45E8-8545-FD0C68E29790},c	Attribute
	instanceType	[Writable]	Attribute
CN=ComputerGroup	🗉 name	ISE OU	Attribute
CN=UESKTOP-19	objectCategory	CN=Organizational-Unit, CN=Schema, CN=Configuration, DC=	Attribute
CN=user2	objectClass	organizationalUnit	Attribute
CN=LiserGroup	objectClass	top	Attribute
	= ou	ISE OU	Attribute
E CN=LostAndFound	uSNChanged	607428	Attribute
CN=Managed Service Accounts	uSNCreated	603085	Attribute
⊞-☐ CN=NTDS Quotas	whenChanged	6/21/2020 2:44:06 AM	Attribute
😟 – 📴 CN=Program Data	whenCreated	6/20/2020 2:51:11 AM	Attribute
CN=System	objectGUID	{44F45D1D-1787-48DF-ABC6-3ED27FA4F694}	Binary Attribute

將ISE與LDAPS伺服器整合

1.匯入受信任證書中的LDAP伺服器根CA證書。

cisco Identity Services Engine	Home + Context Visibility + Operations + Police	y + Administration + V	Work Centers		
System Identity Management	Network Resources	d Services Feed Service	Threat Centric NAC		
Deployment Licensing Certificates Logging Maintenance Upgrade Backup & Restore Admin Access Settings					
✓ Certificate Management	Friendly Name DC1 O	Status Trusted For	e Serial Number Issued To Issued By		
System Certificates	DC1-CA	Enabled Cisco Servi	ire fices 18 29 1C A7 00 13 testlab-DC1-CA-1 testlab-DC1-CA-1		
Trusted Certificates	L	Endpoints			

2.驗證ISE管理員證書並確保ISE管理員證書頒發者證書也存在於受信任的證書儲存中。

3.為了整合LDAPS伺服器,請使用LDAPS目錄中的不同LDAP屬性。導航到Administration > Identity Management > External Identity Sources > LDAP Identity Sources > Add。

cisco Identity Services Engine Home	Context Visibility Operations	Policy Administration	Work Centers	
System Identity Management Network	Resources	nent pxGrid Services + Feed S	ervice > Threat Centri	c NAC
Identities Groups External Identity Sources	Identity Source Sequences + Sett	ings		
External Identity Sources	LDAP Identity Sources List > test LDAP Identity Source General Connect Name t Description Schema (lab_Idaps tion Directory Organization testlab_Idaps Custom	n Groups	Attributes Advanced Settings
RSA SecurID SAML Id Providers Social Login	Subject Objectclass Subject Name Attribute Group Name Attribute Subject Objects Contain Group Objects Contain	person sAMAccountName dn n Reference To Groups Reference To Subjects Subjects In Groups Are Stored	* Group Objectclass * Group Map Attribute Certificate Attribute In Member Attribute As	Group memberOf userCertificate Distinguished Name
	User Info Attributes 🕧			
	First Name	givenName	Department	department
	Last Name	sn	Organizational Unit	company
	Job Title	title	Locality	1
	Email	mail	State or Province	st
	Telephone	telephoneNumber	Country	0
	Street Address	streetAddress		
	Save Reset			

4.從「常規」頁籤配置以下屬性:

Subject Objectclass:此欄位與使用者帳戶的Object類相對應。您可以在此處使用四個類之一:

- 頂端
- 人員
- 組織人員
- InetOrgPerson

Scope Pane 👻 🗙	objectclass	Filter Value	
Softerra LDAP Browser 	Name A © objectClass © objectClass	Value user organizationalPerson	Type Attribute Attribute
OU=Domain Controllers OU=Domain Controllers OU=ForeignSecurityPrincipals OU=ISE Group OU=ISE OU OU=ISE	objectClass objectClass	person top	Attribute Attribute

Subject Name Attribute:此欄位是包含請求中的使用者名稱的屬性的名稱。當ISE查詢LDAP資料庫中的特定使用者名稱時,會從LDAPS檢索此屬性(您可以使用cn、sAMAccountName等)。在此 方案中,使用終端上的user1使用者名稱。

Scope Pane 👻 🗙	Filter Name	user1		
Softerra LDAP Browser	Name 🔺	Value		Type
E-CN=Builtin	🗉 cn	user1		Attribute
CN=Computers	displayName	user1		Attribute
OU=Domain Controllers	distinguishedName	CN=user1,OU=ISE OU,DC=testlab,DC=0	com	Attribute
CN=ForeignSecurityPrincipals	givenName	user1		Attribute
CN=Infrastructure	= name	user1		Attribute
OU=ISE Group	sAMAccountName	user1		Attribute
E- OU=ISE OU	🖃 userPrincipalName	user1@testlab.com		Attribute
CN=ComputerGroup	userCertificate	user1		Binary Attribute
H- CN=DESKTOP-19				
E-CN=UserGroup				

組名稱屬性:這是儲存組名稱的屬性。LDAP目錄中的組名稱屬性值必須與「使用者組」頁上的 LDAP組名稱相匹配

Scope Pane 🛛 👻 🗙	Name 🔺	Value	Туре
Softerra LDAP Browser	= cn	UserGroup	Attribute
i ⊡… 🗐 testlab	distinguishedName	CN=UserGroup,OU=ISE OU,DC=testlab,DC=com	Attribute
😟 - 📴 CN=Builtin	dSCorePropagationData	1/1/1601	Attribute
CN=Computers	groupType	[GlobalScope, Security]	Attribute
OU=Domain Controllers	instanceType	[Writable]	Attribute
E CN=ForeignSecurityPrincipals	member	CN=user1,OU=ISE OU,DC=testlab,DC=com	Attribute
CN=Infrastructure	member	CN=user2,OU=ISE OU,DC=testlab,DC=com	Attribute
■ OU=ISE Group	🗉 name	UserGroup	Attribute
	objectCategory	CN=Group,CN=Schema,CN=Configuration,DC=testlab,DC=com	Attribute
CN=ComputerGroup	objectClass	group	Attribute
CV=DE2KIOP-14	objectClass	top	Attribute
CN=User 1	sAMAccountName	UserGroup	Attribute
CN=UserGroup	sAMAccountType	< samGroupObject >	Attribute

組Objectclass:在搜尋中使用此值來指定可識別為組的對象。

CN=ComputerGroup	objectSid	S-1-5-21-2960284039-4006096050-347662626-1156	Binary Attribute
E-CN=DESKTOP-19	objectGUID	{39967F90-898E-4485-9CC5-828C080EB234}	Binary Attribute
H-CN=user1	objectClass	top	Attribute
E-CN=user2	objectClass	group	Attribute
CN=UserGroup	objectCategory	CN=Group,CN=Schema,CN=Configuration,DC=testlab,DC=com	Attribute

組對映屬性:此屬性定義如何將使用者對映到組。

Scope Pane 👻 🗙	Filter Name	UserGroup	
Softerra LDAP Browser	Name	Value 🔺	Туре
E- CN=Builtin	memberOf	CN=UserGroup,OU=ISE OU,DC=testlab,DC=com	Attribute
CN=Computers			
OU=Domain Controllers OU=Comain Controllers OU=Comain Controllers			
B- 📴 CN=Infrastructure			
B- OU=ISE Group			
CN=ComputerGroup			
CN=DESKTOP-19			
CN=user1			

證書屬性:輸入包含證書定義的屬性。這些定義可以選擇用於在客戶端被定義為證書身份驗證配置 檔案的一部分時驗證客戶端提供的證書。在這種情況下,會在客戶端證書和從LDAP身份源檢索的 證書之間執行二進位制比較。

1 2 2 1 2 2 2	a second second	1000000000	1111
a a the brack that	and the second second		
a lineari			

5.要配置LDAPS連線,請導航到Connection頁籤:

LDAP Identity Sources List > test	Jab_Idaps						
LDAP Identity Source							
General Connec	tion Directory Organizat	tion Grou	oups Attribut	es Advanced Setti	ngs		
	Primary Server				Secon	dary Server	
					🗌 En	able Secondary Server	
* Hostname/IP	dc1.testlab.com			Hostname/IP			
* Port	636			Por	389		
Specify server for each ISE	node						
A	Anonymous Access				Access	Anonymous Access	
	 Authenticated Access 					Authenticated Acces	ss
Adm	nin DN * CN=poongarg,CN=User	rs,DC=testi		Ad	min DN		
Pas	sword *			Pa	ssword		
Secure Authentie	cation 🗹 Enable Secure Authen	tication		Secure Auther	tication	Enable Secure Authority	entication
	Enable Server Identity	Check				Enable Server Identi	ity Check
LDAP Server Ro	oot CA DC1-CA	Ţ ()		LDAP Server F	toot CA	DST Root CA X3 Certifie	cate Ai 🎽 🕐
Issuer CA of ISE Certifi	licates DC1-CA	•		Issuer CA of ISE Cer	tificates	Select if required (optic	onal) * (i)
* Server Timeout	10	() Seconds		Server Timeout	10		@ Seconds
* Max. Admin Connections	20 Force reconnect every	() () Minutes		Max. Admin Connections	20 Force r	reconnect every	Minutes
	Test Bind to Server				Test Bind	to Server	
Failover	Always Access Primary Server I	linet					
1000101	 Failback To Primary Server After 	5	Minu	95			

6.在域控制器上運行dsquery以獲取用於連線到LDAP伺服器的使用者名稱DN:

PS C:\Users\Administrator> dsquery user -name poongarg "CN=poongarg, CN=Users, DC=testlab, DC=com"

步驟 1.S設定LDAP伺服器的正確IP地址或主機名,定義LDAPS埠(TCP 636)和管理DN以通過SSL與 LDAP建立連線。

步驟 2. 啟用Secure Authentication and Server Identity Check選項。

步驟 3.從下拉選單中,選擇LDAP伺服器根CA證書和ISE管理員證書伺服器CA證書(我們使用證書 頒發機構,安裝在同一LDAP伺服器上以頒發ISE管理員證書)。 步驟 4.選擇「測試繫結到伺服器」。此時,由於尚未配置搜尋庫,因此不會檢索任何主題或組。

7.在Directory Organization頁籤下,配置主題/組搜尋庫。它是ISE到LDAP的加入點。現在您只能檢 索作為該加入點子項的主體和組。在此場景中,主題和組都從OU=ISE OU檢索

LDAP Identity Sources Lis	st > testlab_ldap	5			
LDAP Identity Sour	ce				
General	Connection	Directory Organization	Groups	Attributes	Advanced Settings
* Subject Search Base	OU=ISE OU,D	C=testlab,DC=com Naming	Contexts		
* Group Search Base	OU=ISE OU,D	C=testlab,DC=com Naming	Contexts		
Search for MAC Addre	ss in Format xx	-xx-xx-xx-xx *			
Strip start of su	ibject name up to	the last occurrence of the separat	tor \		
Strip end of sub	bject name from t	he first occurrence of the separate	or		

8.在「組」下,按一下「新增」從ISE上的LDAP匯入組並檢索組,如下圖所示。

DAP Identity Source	s List > testlab_idap s			
DAP Identity So	ource			
General	Connection	Directory Organization	Groups	Attributes
/ Edit 🕂 Add 👻	🗙 Delete Group			
Name				•
CN=UserGrou	up,OU=ISE OU,DC=te	stlab,DC=com		

設定交換器

將交換機配置為802.1x身份驗證。Windows PC已連線到switchport Gig2/0/47

aaa new-model

radius server ISE address ipv4 x.x.x.x auth-port 1812 acct-port 1813 key xxxxx aaa group server radius ISE_SERVERS server name ISE

!

aaa server radius dynamic-author
client x.x.x.x server-key xxxxxx

```
!
aaa authentication dot1x default group ISE_SERVERS local
aaa authorization network default group ISE_SERVERS
aaa accounting dot1x default start-stop group ISE_SERVERS
dot1x system-auth-control
ip device tracking
1
radius-server attribute 6 on-for-login-auth
radius-server attribute 8 include-in-access-req
!
!
interface GigabitEthernet2/0/47
switchport access vlan xx
switchport mode access
authentication port-control auto
dot1x pae authenticator
```

配置終端

使用Windows Native Supplicant客戶端,並且使用LDAP支援的EAP協定之一,EAP-TLS用於使用 者身份驗證和授權。

1.確保PC已配置使用者證書(用於user1),並且其用途為客戶端身份驗證,在受信任的根證書頒 發機構中,PC上存在頒發者證書鏈。



2. 啟用Dot1x身份驗證並選擇Authentication method as Microsoft:Smart Card or other certificate for EAP-TLS authentication。

pciPassthru0 Properties	×
Networking Authentication Sharing	
Select this option to provide authenticated network access for this Ethemet adapter.	
Choose a network authentication method:	
Microsoft: Smart Card or other certificate \checkmark Settings	
time I'm logged on Fallback to unauthorized network access	
Additional Settings	
OK Can	el 🛛

3.按一下「其它設定」,此時將開啟一個視窗。選中specify authentication mode覈取方塊,並選擇 使用者身份驗證,如下圖所示。



在ISE上配置策略集

由於使用EAP-TLS協定,因此在配置策略集之前,需要配置證書身份驗證配置檔案,並在稍後在身 份驗證策略中使用身份源序列。

cisco Identity Services Engine Home	Context Visibility Operations	Policy Administration Work Centers
System Identity Management Network	esources	pxGrid Services + Feed Service + Threat Centric NAC
Identities Groups External Identity Sources	Identity Source Sequences	
	Certificate Authentication Profiles List >	DAPS cert
External Identity Sources	Certificate Authentication Prof	ile
(+) E + ∅.		
Certificate Authentication Profile		
Active Directory	* Name	LDAPS_cert
testian	Description	EAP-TLS certificate based authentication with LDAPS
ODBC		
RADIUS Token		
RSA SecuriD		
SAML Id Providers	Identity Store	testiab_idaps 👔 🕧
Cocial Login		
	Use Identity From	Certificate Attribute Subject - Common Name T
		Any Subject or Alternative Name Attributes in the Certificate (for Active Directory Only) ()
	Match Client Certificate Against	
	Certificate in identity Store (j)	O Never
		 Only to resolve identity ambiguity
		Always perform binary comparison
	Save Reset	
	Save Model	

請參閱Identity Source Sequence中的Certificate Authentication Profile,並在Authentication Search清單中定義LDAPS外部身份源:

altalta cisco	Iden	tity Servio	ces Engine	Home	Context	t Visibility	 Operations 	Policy	- Administration	Work Centers
 Syst 	tem	- Identity	Management	Network F	Resources	Device Po	ortal Management	pxGrid Se	ervices + Feed Ser	vice
Iden	tities	Groups	External Ide	ntity Sources	Identity S	ource Sequen	ces + Settings			
Ident	ity S	ource Se	quence							
▼ Id	entit	y Source	Sequence							
	* Nam	e LDAPS								
Des	criptio	n								
									10	
	ertifi	cate Bas	ed Authentic	ation						
		cace bas	eu Autientie	adon						
		Select Ce	rtificate Auther	tication Profile	LDAPS_0	ert	<u>.</u>			
	Availat Availat Intern Guest All_At rad	A ble al Endpoint al Users D_Join_Poi	Search List	ources that wi	I be accesse	ed in sequenc Selected testlab_ld	e until first authent laps	ication succe	eeds	
Ifas	selecte	d identity s	store cannot be	accessed for a	authenticatio	n				
0	Don	ot access o	other stores in t	ne sequence a	ind set the "	Authentication	istatus" attribute to	ProcessEr	for	
	nea		adi was not lot	na ana procee			odrenice.			
Save	R	eset								

現在為有線Dot1x身份驗證配置策略集:

dialia	dentity Ser	rvices Engine Home	 Context Vir 	ibility Operations	▼ Policy	Administration	► Work Centers			License Warning 🔺	۹	. 0	• •
Policy	Sets Prof	filing Posture Client Provisio	ning Pol	icy Elements									
Policy	Sets →	Wired Dot1x							Rese	et Policyset Hitcount	3	Reset	Save
	Status	Policy Set Name	Descrip	tion	Condition	IS				Allowed Protocols / S	server	Sequenc	e Hits
Search	1												
	Ø	Wired Dot1x			C w	ired_802.1X				Default Network Acces	is	x - 4	453
❤ Aut	hentication	n Policy (2)											
+	Status	Rule Name	Condi	tions					Use			Hits	Actions
Sear	ch												
	0	Detty		Nature Access Nature	DeviceName	FOULLIS LAB-Switch			LDAPS		ж т	223	ò
			-+-						> Optio	ons			+
	Ø	Default							LDAPS		x *		ö
		Linguist							> Optio	ons		Ŭ	-14

M Auth	orization I	Policy (2)								
+					Results					
	Status	Rule Name	Cond	itions	Profiles		Security Groups		Hits	Actions
Searc	h									
	Ø	Users in LDAP Store	45	testiab_idaps-ExternalGroups EQUALS CN=UserGroup,OU=ISE OU,DC=testiab,DC=com	×PermitAccess	+	Select from list	+	207	٥
	Ø	Default			× DenyAccess	+	Select from list	+	11	٥
									Reset	Save

完成此配置後,我們可以使用EAP-TLS協定對LDAPS身份源對終端進行身份驗證。

onnection		
IPv4 Connectivity	/: Inte	ernet
IPv6 Connectivity	/: No network ac	cess
Media State:	Ena	abled
Duration:	00:0	1:21
Speed:	1.0	Gbps
tivity —	Sent — Rece	ived
Bytes:	Sent — Rece 3,093	ived 676

驗證

1.檢查連線到PC的switchport上的身份驗證會話:

SW1#sh auth sessions in	t g2/0/47 de
Interface:	GigabitEthernet2/0/47
MAC Address:	b496.9126.dec0
IPv6 Address:	Unknown
IPv4 Address:	10.106.38.165
User-Name:	user1
Status:	Authorized
Domain:	DATA
Oper host mode:	single-host
Oper control dir:	both
Session timeout:	N/A
Restart timeout:	N/A
Periodic Acct timeout:	N/A
Session Uptime:	43s
Common Session ID:	ØA6A26390000130798C66612
Acct Session ID:	0x00001224
Handle:	0x6800002E
Current Policy:	POLICY_Gi2/0/47
Local Policies:	
Service Templat	e: DEFAULT_LINKSEC_POLICY_SHOULD_SECURE (priority 150)
Server Policies:	
Method status list:	
Method	State
dot1x	Authc Success

2.為了驗證LDAPS和ISE配置,您可以檢索與伺服器有測試連線的主題和組:

LDAP Identity Sources List > testiab_ide	sps			
LDAP Identity Source				
General Connection	Directory Organization Groups Attributes Advan	ced Settings		
Access	O Anonymous Ag	Access	Anonymous Access	
	Authenticated / Ldap bind succeeded to dc1.testlab.com:636 Number of Subjects 3		 Authenticated Access 	
Admin DN	CN=poongarg,C Number of Groups 2 Response time 73ms	Admin DN		
Password	•	Password		
	ОК			
Secure Authentication	C Enable Secure Authentication	Secure Authentication	Enable Secure Authentication	
	Enable Server Identity Check		Enable Server Identity Check	
LDAP Server Root CA	DC1-CA T	LDAP Server Root CA	DST Root CA X3 Certificate # *	Ð
Issuer CA of ISE Certificates	DC1-CA T	Issuer CA of ISE Certificates	Select if required (optional)	۵.
* Server Timeout	10 (7) Seconds	Server Timeout	10	(i)Seconds
* Max. Admin Connections	20 ①	Max. Admin Connections	20	()
	Force reconnect every		Force reconnect every	(i) Minutes
	Test Bind to Server		Test Bind to Server	
Fallover	Always Access Primary Server First			
Save Reset				

3.驗證使用者身份驗證報告:

C Refre	esh O Reset Repeat Coun	ts 💆 Expor	t To 🕶								🝸 Filter 🕶 🔷 🗸
Ti	me	Status	Details	Identity	Endpoint ID	Authentication Po	Authorization Policy	Authorization Profi	Network De	Device Port	Authentication Pro
×		•		Identity	Endpoint ID	Authentication Policy	Authorization Policy	Authorization Profiles	Network Device	Device Port	Authentication Protocc
Ju	in 24, 2020 04:45:21.727 AM	0	0	user1	B4:96:91:26:DE:C0	Wired Dot1x >> Dot1x	Wired Dot1x >> Users in LDAP Store	PermitAccess		GigabitEthemet2/0/47	EAP-TLS
Ju	in 24, 2020 04:45:20.671 AM		Q	user1	B4:96:91:26:DE:C0	Wired Dot1x >> Dot1x	Wired Dot1x >> Users in LDAP Store	PermitAccess	LAB-Switch	GigabitEthernet2/0/47	EAP-TLS

4.檢查終端的詳細身份驗證報告:

verview	
Event	5200 Authentication succeeded
Username	user1
Endpoint Id	B4:96:91:26:DE:C0 ⊕
Endpoint Profile	Unknown
Authentication Policy	Wired Dot1x >> Dot1x
Authorization Policy	Wired Dot1x >> Users in LDAP Store
Authorization Result	PermitAccess

Authentication Details					
Source Timestamp	2020-06-24 04:40:52.124				
Received Timestamp	2020-06-24 04:40:52.124				
Policy Server	ISE26-1				
Event	5200 Authentication succeeded				
Username	user1				
Endpoint Id	B4:96:91:26:DE:C0				
Calling Station Id	B4-96-91-26-DE-C0				
Endpoint Profile	Unknown				
IPv4 Address	10.106.38.165				
Authentication Identity Store	testlab_ldaps				
Identity Group	Unknown				
Audit Session Id	0A6A26390000130C98CE6088				
Authentication Method	dot1x				
Authentication Protocol	EAP-TLS				
Service Type	Framed				
Network Device	LAB-Switch				

15041	Evaluating Identity Policy
15048	Queried PIP - Network Access.NetworkDeviceName
22072	Selected identity source sequence - LDAPS
22070	Identity name is taken from certificate attribute
15013	Selected Identity Source - testlab_Idaps
24031	Sending request to primary LDAP server - testlab_ldaps
24016	Looking up user in LDAP Server - testlab_ldaps
24023	User's groups are retrieved - testlab_ldaps
24004	User search finished successfully - testlab_ldaps
22054	Binary comparison of certificates succeeded
22037	Authentication Passed
22001	

15036	Evaluating Authorization Policy					
24209	Looking up Endpoint in Internal Endpoints IDStore - user1					
24211	Found Endpoint in Internal Endpoints IDStore					
15048	Queried PIP - testlab_Idaps.ExternalGroups					
15016	Selected Authorization Profile - PermitAccess					
22081	Max sessions policy passed					
22080	New accounting session created in Session cache					
11503	Prepared EAP-Success					
11002	Returned RADIUS Access-Accept					

5.驗證ISE和LDAPS伺服器之間的資料已加密,方法是在ISE上向LDAPS伺服器捕獲資料包:

N).	Time		Source	Destination	Protocol	Length	Address	64bits	Info
	20	2020-06-24 10:40:24.2054	31	10.197.164.22	10.197.164.21	TCP	74	00:0c:29:98:ca:28,0_		28057 + 636 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=140972872 TSecr=0 WS=128
	21	2020-06-24 10:40:24.20650	85	10.197.164.21	10.197.164.22	TCP	74	00:50:56:a0:3e:7f,0_		636 - 28057 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1 TSval=30158962 TSecr=140972872
П	22	2020-06-24 10:40:24.2066	13	10.197.164.22	10.197.164.21	TCP	66	00:0c:29:98:ca:28,0_		28057 - 636 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=140972873 TSecr=30158962
	23	2020-06-24 10:40:24.20696	61	10.197.164.22	10.197.164.21	TLSv1.2	207	00:0c:29:98:ca:28,0_		Client Hello
	24	2020-06-24 10:40:24.21041	13	10.197.164.21	10.197.164.22	TLSv1.2	2036	00:50:56:a0:3e:7f,0_		Server Hello, Certificate[Packet size limited during capture]
	25	2020-06-24 10:40:24.21050	88	10.197.164.22	10.197.164.21	TCP	66	00:0c:29:98:ca:28,0_		28057 → 636 [ACK] Seq=142 Ack=1971 Win=33152 Len=0 TSval=140972877 TSecr=30158962
	26	2020-06-24 10:40:24.21523	11	10.197.164.22	10.197.164.21	TLSv1.2	260	00:0c:29:98:ca:28,0_		Certificate, Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
Ł	27	2020-06-24 10:40:24.2186	78	10.197.164.21	10.197.164.22	TLSv1.2	173	00:50:56:a0:3e:7f,0_		Change Cipher Spec, Encrypted Handshake Message
	28	2020-06-24 10:40:24.2191	13	10.197.164.22	10.197.164.21	TLSv1.2	199	00:0c:29:98:ca:28,0_		Application Data
П	29	2020-06-24 10:40:24.23038	84	10.197.164.21	10.197.164.22	TLSv1.2	167	00:50:56:a0:3e:7f,0_	_	Application Data
	30	2020-06-24 10:40:24.2317	12	10.197.164.22	10.197.164.21	TLSv1.2	279	00:0c:29:98:ca:28,0_		Application Data
	31	2020-06-24 10:40:24.23888	89	10.197.164.21	10.197.164.22	TLSv1.2	1879	00:50:56:a0:3e:7f,0_		Application Data[Packet size limited during capture]
	32	2020-06-24 10:40:24.23895	58	10.197.164.22	10.197.164.21	TCP	66	00:0c:29:98:ca:28,0_		28057 → 636 [ACK] Seg=682 Ack=3992 Win=36864 Len=0 TSval=140972905 TSecr=30158965
	33	2020-06-24 10:40:24.25194	44	10.197.164.22	10,197,164,21	TLSv1.2	263	00:0c:29:98:ca:28.0.		Application Data
	34	2828-86-24 18:48:24.25365	58	10.197.164.21	10,197,164,22	TLSv1.2	295	00:50:56:a0:3e:7f.0_		Application Data
	35	2828-86-24 18:48:24.2933	22	10.197.164.22	10.197.164.21	TCP	66	00:0c:29:98:ca:28,0_		28057 → 636 [ACK] Seg=879 Ack=4221 Win=39680 Len=0 TSval=140972960 TSecr=30158967
	86	2020-06-24 10:40:57,94655	53	10,197,164,22	10,197,164,21	TLSv1.2	151	00:0c:29:98:ca:28.0.		Application Data
10	87	2828-86-24 18:48:57.94768	88	10.197.164.22	10.197.164.21	TCP	66	00:0c:29:98:ca:28.0_		28057 → 636 [FIN, ACK] Seg=964 Ack=4221 Win=39680 Len=0 TSval=141006614 TSecr=30158967
A P	 Elternet 11, STC: Wmare_dw15er/17 (W01905)site/stc/17/, USI: Wmare_ds1Calce/ V001905(25/3905Calce/ Elternet Protocol Version 4, STC: 10.197.164.22, DSI: 10.197.164.21 Transmission Control Protocol, Src Port: 20057, Dst Port: 636, Seq: 336, Ack: 2078, Len: 133 Source Port: 20057 Destination Port: 636 									
F	[St [TC] Seq [Ne: Ack 100 ▶ Fla Win [Ca [Win Che [Ch Urg P 0pt ► [SE] ► [Ti] TCP Secure	ream index: 2] P Segnent Len: 133] uence number: 336 (rela xt sequence number: 42078 0 = Header Length: 2 35: 00488 (PSH, AKK) dow size value: 259 lculated window size: 3315 ndow size value: 259 lculated window size; 3315 ndow size; 3315 ndow size value: 259 lculated window size; 3315 ndow size value: 259 lculated window size; 3315 ndow size value: 3315 ndow size; 3315 ndow	(re (re 2 byt 128)	sequence number) lative sequence number elative ack number) les (8) h (NOP), No-Operation	r)] (NOP), Timestamps					
ľ	▼ TLSV1.2 Record Layer: Application Data Protocol: ldap Content Type: Application Data (23) Version: TLS 1.2 (20x0803) Length: 128 Encrypted Application Data: 173d1b0b2f280a13cc17815e54447bb9ac8af8a881a9eb84									

疑難排解

本節介紹此配置遇到的一些常見錯誤以及如何進行故障排除。

• 在驗證報告中,您可能會看到以下錯誤消息:

Authentication method is not supported by any applicable identity store

此錯誤消息表明LDAP不支援您選擇的方法。確保同一報告中的身份驗證協定顯示其中一個受支援的方法(EAP-GTC、EAP-TLS或PEAP-TLS)。

• 到伺服器的測試繫結已結束,但出現錯誤。

這通常是由於LDAPS伺服器證書驗證檢查失敗。若要解決此類問題,請在ISE上捕獲資料包,並在 調試級別啟用所有三個運行時和prrt-jni元件,重新建立問題,並檢查prrt-server.log檔案。

封包擷取會抱怨憑證錯誤,且連線埠伺服器顯示:

04:10:20,197,ERROR,0x7f9c5b6f1700,LdapSslConnectionContext::checkCryptoResult(id = 1289): error message

註:LDAP頁中的主機名必須配置有證書的使用者名稱(或任何使用者替代名稱)。因此,除非 主題或SAN中存在此類證書,否則它不起作用,因此需要使用SAN清單中具有IP地址的證書。 3.在身份驗證報告中,您可能會注意到在身份儲存庫中找不到主題。這意味著報告的使用者名稱與 LDAP資料庫中任何使用者的「使用者名稱屬性」不匹配。在此方案中,此屬性值設定為 sAMAccountName,這意味著ISE在嘗試查詢匹配項時查詢LDAP使用者的sAMAccountName值。

4.在繫結到伺服器測試期間無法正確檢索主題和組。導致此問題的最可能原因是搜尋基的配置不正 確。請記住,必須從枝葉到根和dc(可包含多個單詞)指定LDAP層次結構。

相關資訊

- <u>https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine/119149-</u> <u>configure-ise-00.html#anc9</u>
- <u>https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine/214975-</u> <u>configure-eap-tls-authentication-with-is.html</u>

關於此翻譯

思科已使用電腦和人工技術翻譯本文件,讓全世界的使用者能夠以自己的語言理解支援內容。請注 意,即使是最佳機器翻譯,也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準 確度概不負責,並建議一律查看原始英文文件(提供連結)。