외부 LDAPS ID 저장소로 ISE 구성 및 문제 해결

목차	
<u>소개</u>	
<u>사전 요구 사항</u>	
<u>요구 사항</u>	
사용되는 구성 요소	
<u>구성</u>	
<u>네트워크 다이어그램</u>	
<u>Active Directory에서 LDAPS 구성</u>	
<u>도메인 컨트롤러에 ID 인증서 설치</u>	
LDAPS 디렉토리 구조 액세스	
<u>ISE를 LDAPS 서버와 통합</u>	
<u>스위치 구성</u>	
<u>엔드포인트 구성</u>	
<u>ISE에서 정책 설정 구성</u>	
<u>다음을 확인합니다.</u>	
<u>문제 해결</u>	
과려 정보	

소개

이 문서에서는 Cisco ISE와 Secure LDAPS 서버를 외부 ID 소스로 통합하는 방법을 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- ISE(Identity Service Engine) 관리에 대한 기본 지식
- Active Directory/LDAPS(Secure Lightweight Directory Access Protocol)에 대한 기본 지식

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco ISE 2.6 패치 7
- Active Directory LDS(Lightweight Directory Services)가 설치된 Microsoft Windows 버전 2012 R2
- 기본 신청자 및 사용자 인증서가 설치된 Windows 10 OS PC
- Cisco Switch C3750X with 152-2.E6 image

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바 이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

배경 정보

LDAPS에서는 디렉토리 바인딩이 설정될 때 전송 중인 LDAP 데이터(사용자 자격 증명 포함)의 암 호화를 허용합니다. LDAPS는 TCP 포트 636을 사용합니다.

이러한 인증 프로토콜은 LDAPS에서 지원됩니다.

- EAP Generic Token Card(EAP-GTC)
- PAP(Password Authentication Protocol)
- EAP 전송 계층 보안(EAP-TLS)
- PEAP-TLS(Protected EAP Transport Layer Security)

✤ 참고: EAP-MSCHAPV2(PEAP, EAP-FAST 또는 EAP-TTLS의 내부 방법), LEAP, CHAP 및 EAP-MD5는 LDAPS 외부 ID 소스에서 지원되지 않습니다.

구성

이 섹션에서는 네트워크 디바이스의 컨피그레이션 및 ISE와 Microsoft AD(Active Directory) LDAPS 서버의 통합에 대해 설명합니다.

네트워크 다이어그램

이 컨피그레이션 예에서는 엔드포인트가 LAN(Local Area Network)에 연결하기 위해 스위치와의 이 더넷 연결을 사용합니다. 연결된 switchport는 802.1x 인증을 위해 구성되어 ISE로 사용자를 인증합 니다. ISE에서 LDAPS는 외부 ID 저장소로 구성됩니다.

이 이미지는 사용되는 네트워크 토폴로지를 보여줍니다.



Secure LDAP Server

Active Directory에서 LDAPS 구성

도메인 컨트롤러에 ID 인증서 설치

LDAPS를 활성화하려면 다음 요구 사항을 충족하는 DC(Domain Controller)에 인증서를 설치합니 다.

- 1. LDAPS 인증서는 도메인 컨트롤러의 개인 인증서 저장소에 있습니다.
- 인증서와 일치하는 개인 키가 도메인 컨트롤러의 저장소에 있으며 인증서와 올바르게 연결되 어 있습니다.
- 3. Enhanced Key Usage 확장에는 서버 인증(1.3.6.1.5.5.7.3.1) 개체 식별자(OID라고도 함)가 포 함됩니다.
- 4. 도메인 컨트롤러(예: DC1.testlab.com)의 FQDN(Fully Qualified Domain Name)은 Subject(주 체) 필드의 CN(Common Name) 및 Subject Alternative Name Extension(주체 대체 이름 확장)의 DNS 항목 특성 중 하나에 있어야 합니다.
- 5. 인증서는 도메인 컨트롤러와 LDAPS 클라이언트가 신뢰하는 CA(Certificate Authority)에서 발 급해야 합니다. 신뢰할 수 있는 보안 통신의 경우 클라이언트와 서버는 서로의 루트 CA와 인 증서를 발급한 중간 CA 인증서를 신뢰해야 합니다.
- 6. 키를 생성하려면 Schannel CSP(암호화 서비스 공급자)를 사용해야 합니다.

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 Auther	~
< III >	
Other Name:	
DS Object Guid=04 10 a6 36 1d 3c f4 3f a8 47 83 d7 d3 d5 46 20 a3 3	\$f
DNS Name=DC1.testiab.com	

LDAPS 디렉토리 구조 액세스

Active Directory 서버의 LDAPS Directory에 액세스하려면 LDAP 브라우저를 사용합니다. 이 LAB에 서는 Software LDAP Browser 4.5를 사용합니다.

1. TCP 포트 636에서 도메인에 대한 연결을 설정합니다.



2. 간소화를 위해 AD에서 ISE OU라는 OU(Organizational Unit)를 만들고 UserGroup이라는 그룹이 있어야 합니다. 두 명의 사용자(user1 및 user2)를 만들고 이 사용자를 UserGroup 그룹의 멤버로 만 듭니다.



Scope Pane 🔹 🗙	Name 🔺	Value	Туре
Softerra LDAP Browser	CN CN	UserGroup	Entry
🖲 📲 Internet Public Servers	CN	user2	Entry
i − 🗐 testiab	CN	user1	Entry
E CN=Builtin	CN	DESKTOP-19	Entry
CN=Computers	CN	ComputerGroup	Entry
B- 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
	🗉 gPLink	[LDAP://cn={21A53B13-6971-45E8-8545-FD0C68E29790},c	Attribute
	instanceType	[Writable]	Attribute
CN=ComputerGroup	🗉 name	ISE OU	Attribute
	objectCategory	CN=Organizational-Unit, CN=Schema, CN=Configuration, DC=	Attribute
CN=user2	objectClass	organizationalUnit	Attribute
CN=UserGroup	objectClass	top	Attribute
- OU=LABISE	= ou	ISE OU	Attribute
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-17B7-48DF-ABC6-3ED27FA4F694}	Binary Attribute

ISE를 LDAPS 서버와 통합

1. 신뢰할 수 있는 인증서에서 LDAP 서버 루트 CA 인증서를 가져옵니다.

cisco Identity Se	rvices Engine	Home	e	Operations Polic	y - Administra	tion			
System Identity Management Network Resources Device Portal Management pxGrid Services Feed Service Threat Centric NAC									
Deployment Lice	Deployment Licensing Certificates Logging Maintenance Upgrade Backup & Restore Admin Access Settings								
	0	_	Friendly Name		Status	Trusted For	Serial Number	Issued To	Issued Ry
- Certificate Manage	ement		DC1	0					
System Certificate	s		DC1-CA		Enabled	Infrastructure Cisco Services	18 29 1C A7 00 13	testlab-DC1-CA-1	testlab-DC1-CA-1
Trusted Certificate	s					Endpoints			

2. ISE 관리자 인증서를 검증하고 ISE 관리자 인증서 발급자 인증서가 신뢰할 수 있는 인증서 저장 소에도 있는지 확인합니다.

3. LDAPS 서버를 통합하려면 LDAPS 디렉토리의 다른 LDAP 속성을 사용합니다.

Administration(관리) > Identity Management(ID 관리) > External Identity Sources(외부 ID 소스) > LDAP Identity Sources(LDAP ID 소스) > Add(추가)로 이동합니다.

dentity Services Engine	ome	Policy Administration	▶ Work Centers	
	twork Resources	pxGrid Services + Feed Ser	vice + Threat Centric N	AC
Identities Groups External Identity	ources Identity Source Sequences + Settings	1		
External Identity Sources	LDAP Identity Sources List > testlab LDAP Identity Source Connection Name testl Description Schema Custo	Jdaps Directory Organization ab_Idaps om v	Groups	Attributes Advanced Settings
RSA SecurID SAML Id Providers Social Login	Subject Objectclass per Subject Name Attribute SAU Group Name Attribute dn Subject Objects Contain Ref Group Objects Contain Ref	son MAccountName eference To Groups lerence To Subjects Subjects In Groups Are Stored In	Group Objectclass Group Map Attribute n Certificate Attribute u	roup memberOf serCertificate istinguished Name
	First Name giv Last Name sn Job Title title Email ma Telephone tele Street Address street	enName	Department d Organizational Unit c Locality 1 State or Province s Country c	epartment

4. [일반 사항] 탭에서 다음 속성을 구성합니다.

Subject Objectclass: 이 필드는 사용자 계정의 Object 클래스에 해당합니다. 다음 네 가지 클래스 중 하나를 사용할 수 있습니다.

- 상단
- 개인
- 조직인
- InetOrg사람

Scope Pane 👻 🗙	objectclass	Filter Value	
Softerra LDAP Browser testlab CN=Builtin CN=Computers CN=ForeignSecurityPrincipals CN=Infrastructure C	Name A CobjectClass CobjectClass CobjectClass CobjectClass CobjectClass	Value user organizationalPerson person top	Type Attribute Attribute Attribute Attribute

주체 이름 특성: 이 필드는 요청의 사용자 이름을 포함하는 특성의 이름입니다. 이 특성은 ISE가 LDAP 데이터베이스의 특정 사용자 이름을 조회할 때 LDAPS에서 검색됩니다(cn,

sAMAccountName 등을 사용할 수 있음). 이 시나리오에서는 엔드포인트의 user1 사용자 이름이 사 용됩니다.

Scope Pane 🛛 👻 🗙	Filter Name	user1				
Softerra LDAP Browser	Name 🔺	Value	Туре			
CN=Builtin CN=Computers OU=Domain Controllers	≡ cn ≡ displayName ≡ distinguishedName	user1 user1 CN=user1,OU=ISE OU,DC=testiab,DC=com	Attribute Attribute Attribute			
CN=ForeignSecurityPrincipals CN=Infrastructure OU=ISE Group	givenName name sAMAccountName	user1 user1	Attribute Attribute Attribute			
OU=ISE OU CN=ComputerGroup CN=DESKTOP-19 CN=user1 CN=user2 CN=UserGroup CN=UserGroup	■ userPrinopalName ■ userCertificate	user1@testiab.com user1	Attribute Binary Attribute			

Group Name Attribute(그룹 이름 특성): 그룹 이름을 보유한 특성입니다. LDAP 디렉토리의 그룹 이 름 속성 값은 User groups(사용자 그룹) 페이지의 LDAP 그룹 이름과 일치해야 합니다

Scope Pane 🛛 👻 🗙	Name 🔺	Value	Туре
Softerra LDAP Browser	Ξ თ	UserGroup	Attribute
Ė… 🗐 testlab	distinguishedName	CN=UserGroup,OU=ISE OU,DC=testlab,DC=com	Attribute
😟 - 🚞 CN=Builtin	dSCorePropagationData	1/1/1601	Attribute
E 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
CN=DESKTOP-19	objectClass	top	Attribute
CN=user1	sAMAccountName	UserGroup	Attribute
CN=UserGroup	sAMAccountType	< samGroupObject >	Attribute

Group Objectclass: 이 값은 검색에서 그룹으로 인식되는 객체를 지정하는 데 사용됩니다.

H- CN=ComputerGroup	objectSid	S-1-5-21-2960284039-4006096050-347662626-1156	Binary Attribute
H-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

그룹 맵 특성: 이 특성은 사용자가 그룹에 매핑되는 방법을 정의합니다.

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=Controllers OU=Controllers			
CN=Infrastructure			
OU=ISE Group			
OU=ISE OU OU=ComputerGroup			
E CN=DESKTOP-19			
- CN=user1			

Certificate Attribute(인증서 특성): 인증서 정의를 포함하는 특성을 입력합니다. 이러한 정의는 선택 적으로 클라이언트가 인증서 인증 프로필의 일부로 정의할 때 제시하는 인증서를 검증하는 데 사용 할 수 있습니다. 이러한 경우 클라이언트 인증서와 LDAP ID 소스에서 검색된 인증서 간에 이진 비 교가 수행됩니다.

E a Contraction of Contraction of Contraction			and the second sec	1000
the second residue of	a a declaration of the	the local section in		the second s
	 A characterize of 			
	a disease			

5. LDAPS 연결을 구성하려면 [연결] 탭으로 이동합니다.

LDAP Id	entity Sources List > testi	ab_ld	aps							
LDAP 1	Identity Source									
(General Connect	tion	Directory Organization	1	Groups	Attributes	Advanced Sett	ngs		
		Prima	ary Server					Seco	ndary Server	
								E	nable Secondary Server	,
	* Hostname/IP	dc1.	testlab.com				Hostname/IF			
	* Port	636					Por	389		
□ s	pecify server for each ISE	node								
	A	ccess	 Anonymous Access 					Access	Anonymous Acces	s
			Authenticated Access						 Authenticated Acc 	ess
	Admin DN CN=poongarg,CN=Users,D		DC=testi			Ac	imin DN			
	Pass	sword	•••••				Pi	assword		
	Secure Authentic	ation	Enable Secure Authentica Enable Server Identity Ch	ition eck			Secure Auther	ntication	Enable Secure Aut	hentication htity Check
	LDAP Server Ro	ot CA	DC1-CA	Ţ.			LDAP Server F	Root CA	DST Root CA X3 Certi	ficate At *
	Issuer CA of ISE Certifi	cates	DC1-CA	Y.		Issuer CA of ISE Certificates Select if requ		Select if required (opt	tional) 🕴 🕧	
	* Server Timeout	10		Seconds			Server Timeout	10		() Seconds
	* Max. Admin Connections	20				Ma	x. Admin Connections	20		Ð
		L F	orce reconnect every (i	Minutes				Force	reconnect every	 Minutes
		Tes	Bind to Server					Test Bin	d to Server	
	Failover) A	ways Access Primary Server Firs	t						
		• F	ailback To Primary Server After 5			Minutes				

6. 도메인 컨트롤러에서 dsquery를 실행하여 LDAP 서버에 연결하는 데 사용할 사용자 이름 DN을 가져옵니다.

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

1단계. 초LDAP 서버의 올바른 IP 주소 또는 호스트 이름을 설정하고, LDAPS 포트(TCP 636) 및 관 리 DN을 정의하여 SSL을 통해 LDAP에 연결합니다. 2단계. 보안 인증 및 서버 ID 확인 옵션을 활성화 합니다.

3단계. 드롭다운 메뉴에서 LDAP Server Root CA 인증서 및 ISE admin certificate Isser CA 인증서 를 선택합니다(동일한 LDAP 서버에 설치된 인증 기관을 사용하여 ISE 관리 인증서도 발행함).

4단계. Test Bind to server를 선택합니다. 이 시점에서는 검색 기반이 아직 구성되지 않았기 때문에 어떤 주제나 그룹도 검색되지 않습니다.

7. Directory Organization(디렉토리 조직) 탭 아래에서 Subject/Group Search Base(주체/그룹 검색 기반)를 구성합니다. ISE가 LDAP에 조인하는 지점입니다. 이제 조인 지점의 하위 항목인 주체 및 그룹만 검색할 수 있습니다. 이 시나리오에서는 주체 및 그룹이 모두 OU=ISE OU에서 검색됩니다

LDAP Identity Sources Li	st > testlab_idaps				
LDAP Identity Sour	ce				
General	Connection	Directory Organization	Groups	Attributes	Advanced Settings
* Subject Search Base	OU=ISE OU,DC	=testlab,DC=com Naming Co	i		
* Group Search Base	OU=ISE OU,DC	=testlab,DC=com Naming Co	i) iii		
Search for MAC Addre	ess in Format xx-x	x-xx-xx-xx *			
Strip start of su	ubject name up to th	e last occurrence of the separato	r \		
Strip end of su	bject name from the	first occurrence of the separator			

8. 이 이미지에 표시된 대로 Groups(그룹)에서 Add(추가)를 클릭하여 ISE의 LDAP에서 그룹을 가져 오고 그룹을 검색합니다.

PAP Identity S	ource			
General	Connection	Directory Organization	Groups	Attribute
/ Edit 🕂 Add 🗸	X Delete Group			
Name				.

스위치 구성

802.1x 인증을 위해 스위치를 구성합니다. Windows PC가 switchport Gig2/0/47에 연결되었습니다.

```
radius server ISE
address ipv4 x.x.x.x auth-port 1812 acct-port 1813
key xxxxxx
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
1
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
```

엔드포인트 구성

dot1x pae authenticator

aaa new-model

Windows 네이티브 서 플리 컨 트가 사용 되고 LDAP 지원 EAP 프로토콜 중 하나가 사용 됩니다, 사용자 인증 및 권한 부여를 위한 EAP-TLS.

1. PC에 사용자 인증서(user1용)가 프로비저닝되어 있고 클라이언트 인증의 용도로 사용되고 있는 지, 신뢰할 수 있는 루트 인증 기관에서 발급자 인증서 체인이 PC에 있는지 확인합니다.



2. Dot1x 인증을 활성화하고 Microsoft:Smart Card 또는 EAP-TLS 인증을 위한 기타 인증서로 인증 방법을 선택합니다.

pciPassthru0 Properties	×
Networking Authentication Sharing	
Select this option to provide authenticated network access for this Ethemet adapter. ✓ Enable IEEE 802.1X authentication Choose a network authentication method: Microsoft: Smart Card or other certificate ✓ ✓ Remember my credentials for this connection each time I'm logged on	
✓ Fallback to unauthorized network access Additional Settings	
OK Cance	ы

 추가 설정을 클릭하면 창이 열립니다. 이 이미지에 표시된 대로 인증 모드를 지정하고 사용자 인 증을 선택합니다.



ISE에서 정책 설정 구성

EAP-TLS 프로토콜이 사용되므로 정책 집합을 구성하기 전에 인증서 인증 프로파일을 구성해야 하며 ID 소스 시퀀스가 나중에 인증 정책에서 사용됩니다.

cisco Identity Services Engine Home	Context Visibility Operations	Policy Administration Work Centers
System Identity Management Network R	esources	pxGrid Services + Feed Service + Threat Centric NAC
Identities Groups External Identity Sources	Identity Source Sequences	
External Identity Sources	Certificate Authentication Profiles List > I	LDAPS_cert
(+ + E +),	Certificate Authentication Profi	ile
Certificate Authentication Profile Certificate Authenticate Authenticate Authenticate Authenticate Authenticate Authenticate A	* Name	LDAPS_cert FAP.TI S certificate based authentication with I DAPS
CDAP COBC Comparison Comparison	Description	XX.13. Certaine based accusing and that XXX.X
CASA SecuriD SAML Id Providers Social Login	Identity Store	testiab_idaps 🝸 🕖
	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	

ID 소스 시퀀스의 인증서 인증 프로파일을 참조하고 인증 검색 목록에서 LDAPS 외부 ID 소스를 정 의합니다.

altalta cisco	Identity Serv	ices Engine	Home	► Context \	Visibility 🕨 K	perations	Policy	- Administration	Work Centers
 Syst 	em 👻 Identity	y Management	 Network F 	Resources	Device Portal	Management	pxGrid Se	ervices + Feed Se	rvice
Iden	tities Groups	External Ide	ntity Sources	Identity So	urce Sequences	 Settings 			
Ident	ity Source S	equence							
▼ Id	entity Source	Sequence							
	Name LDAP	s							
Des	cription								
								111	
	ertificate Rad	sed Authentic	ation						
		Autoritation				7			
	Select C	ertificate Auther	tication Profile	LDAPS_cer	t Ţ	J			
- A	uthenticatio	n Search List							
	A	set of identity s	ources that wi	I be accessed	d in sequence un	til first authent	ication succe	eeds	
	vailable				Selected				
Г	Internal Endpoir	nts		1	testlab Idaps	1			
	Internal Users Guest Users				loonds_loops				
	testlab All AD Join Po	pints		<					
	rad								
l									
- (14)									
▼ A Ifas	dvanced Sea	store cannot be	accessed for a	authentication	1				
0									
0	Treat as if the	other stores in t	ne sequence a	and set the "A	store in the secu	us attribute to	ProcessEr	for	
	rica, as il ule	user was not 10t	and procee		store in the sequ	0100			
Save	Reset								

이제 유선 Dot1x 인증에 대한 정책 집합을 구성합니다.

altalta cisco	Identity S	ervices Engine Home	Context Visibility Operation	is Policy Administration Work Centers	License Warning 🔺 🧠	0	• •
Policy	Sets Pr	ofiling Posture Client Provisi	oning				
Polic	/ Sets -	Wired Dot1x			Reset Policyset Hitcounts	Reset	Save
	Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server	Sequence	e Hits
Sean	h						
	0	Wired Dot1x		Wired_802.1X	Default Network Access	× • •	453
∨ A.	thentication	on Policy (2)					
	Statu	s Rule Name	Conditions		Use	Hits	Actions
Sec	irch						
	0	Delte			LDAPS × *		~
	•	DOIX	Network Addess Netw	KINDEVICENTINE ENULALS LAD-SWITCH	> Options	223	*
	0	Default			LDAPS x +		ö
	•	Line of the second seco			> Options	Ŭ	~

► Auth	orization I	Policy (2)								
+					Results					
	Status	Rule Name	Cond	itions	Profiles		Security Groups		Hits	Actions
Searc	1									
	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

이 컨피그레이션 후 LDAPS ID 소스에 대해 EAP-TLS 프로토콜을 사용하여 엔드포인트를 인증할 수 있습니다.

	us	
eneral		
Connection		
IPv4 Connectivity		Internet
IPv6 Connectivity	: 1	No network access
Media State:		Enabled
Duration:		00:01:21
Speed:		1.0 Gbps
Activity	Sent — 🔟	Received
Activity	Sent — 1000 3,093	- Received 676
Activity Bytes:	Sent — 3,093 Diagr	Received 676

다음을 확인합니다.

1. PC에 연결된 스위치 포트에서 인증 세션을 확인합니다.

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. LDAPS 및 ISE 컨피그레이션을 확인하기 위해 서버에 대한 테스트 연결을 통해 주체 및 그룹을 검색할 수 있습니다.

LDAP Identity Sources List > testlab_Id	aps			
LDAP Identity Source				
General Connection	Directory Organization Groups Attributes Advan	nced Settings		
Access	O Anonymous Ac	Access	Anonymous Access	
	Authenticated A Ldap bind succeeded to dc1.testlab.com:636 Number of Subjects 3		Authenticated Access	
Admin DN	* CN=poongarg,C Response time 73ms	Admin DN		
Password	•	Password		
	ОК			
Secure Authentication	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 # *	æ
Issuer CA of ISE Certificates	DC1-CA T	Issuer CA of ISE Certificates	Select if required (optional)	۵
* Server Timeout	10 @Seconds	Server Timeout	10	() Seconds
* Max. Admin Connections	20	Max. Admin Connections	20	⁽¹⁾
	Force reconnect every Minutes		Force reconnect every	(j) Minutes
	Test Bind to Server		Test Bind to Server	
Failmar	Always Access Primary Server First			
Save Reset				

3. 사용자 인증 보고서를 확인합니다.

CI	Refresh O Reset Repeat Coun	its 💆 Expor	t To 🕶								▼ Filter • • •
	Time	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 Protoco
	Jun 24, 2020 04:45:21.727 AM	0	<u>o</u>	user1	B4:96:91:26:DE:C0	Wired Dot1x >> Dot1x	Wired Dot1x >> Users in LDAP Store	PermitAccess		GigabitEthemet2/0/47	EAP-TLS
	Jun 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. 엔드포인트에 대한 자세한 인증 보고서를 확인합니다.

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 ISE26-1 5200 Authentication succeeded						
Policy Server							
Event							
Username	user1						
Endpoint Id	B4:96:91:26:DE:C0						
Calling Station Id	B4-96-91-26-DE-C0						
Endpoint Profile	Unknown 10.106.38.165						
IPv4 Address							
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. ISE에서 LDAPS 서버로 향하는 패킷 캡처를 수행하여 ISE와 LDAPS 서버 간에 데이터가 암호화 되었는지 확인합니다.

No	Tim	ie A	Source	Destination	Protocol	Length	Address	64bits	Info
	20 202	0-06-24 10:40:24.205431	10,197,164,22	10,197,164,21	TCP	74	00:0c:29:98:ca:28.0.		28057 -+ 636 [SYN] Seg=0 Win=29200 Len=0 MSS=1460 SACK PERM=1 TSval=140972872 TSecr=0 WS=128
1	21 202	0-06-24 10:40:24.206505	10.197.164.21	10.197.164.22	TCP	74	00:50:56:a0:3e:7f.0_		636 → 28057 [SYN, ACK] Seg=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK PERM=1 TSval=30158962 TSecr=140972872
	22 282	0-06-24 10:40:24.206613	10.197.164.22	10.197.164.21	TCP	66	00:0c:29:98:ca:28,0_	_	28057 + 636 [ACK] Seg=1 Ack=1 Win=29312 Len=0 TSval=140972873 TSecr=30158962
	23 202	0-06-24 10:40:24.206961	10.197.164.22	10.197.164.21	TLSv1.2	207	00:0c:29:98:ca:28,0_		Client Hello
	24 282	0-06-24 10:40:24.210413	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]
	25 282	0-06-24 10:40:24.210508	10.197.164.22	10.197.164.21	TCP	66	00:0c:29:98:ca:28,0_		28057 - 636 [ACK] Seg=142 Ack=1971 Win=33152 Len=0 TSval=140972877 TSecr=30158962
	26 202	0-06-24 10:40:24.215211	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
k	27 202	0-06-24 10:40:24.218678	10.197.164.21	10.197.164.22	TLSv1.2	173	00:50:56:a0:3e:7f,0_		Change Cipher Spec, Encrypted Handshake Message
	28 202	0-06-24 10:40:24.219113	10.197.164.22	10.197.164.21	TLSv1.2	199	00:0c:29:98:ca:28.0_		Application Data
	29 282	0-06-24 10:40:24.230384	10.197.164.21	10.197.164.22	TLSv1.2	167	00:50:56:a0:3e:7f,0_	_	Application Data
	30 202	0-06-24 10:40:24.231712	10.197.164.22	10.197.164.21	TLSv1.2	279	00:0c:29:98:ca:28,0_		Application Data
	31 202	0-06-24 10:40:24.238889	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]
	32 202	0-06-24 10:40:24.238958	10.197.164.22	10.197.164.21	TCP	66	00:0c:29:98:ca:28,0_		28057 - 636 [ACK] Seq=682 Ack=3992 Win=36864 Len=0 TSval=140972905 TSecr=30158965
	33 202	0-06-24 10:40:24.251944	10.197.164.22	10.197.164.21	TLSv1.2	263	00:0c:29:98:ca:28,0_		Application Data
	34 282	0-06-24 10:40:24.253658	10.197.164.21	10.197.164.22	TLSv1.2	295	00:50:56:a0:3e:7f,0_		Application Data
	35 282	0-06-24 10:40:24.293322	10.197.164.22	10.197.164.21	TCP	66	00:0c:29:98:ca:28,0_		28857 + 636 [ACK] Seq=879 Ack=4221 Win=39688 Len=0 TSval=140972960 TSecr=30158967
	86 202	0-06-24 10:40:57.946553	10.197.164.22	10.197.164.21	TLSv1.2	151	00:0c:29:98:ca:28,0_		Application Data
100	87 202	0-06-24 10:40:57.947680	10.197.164.22	10.197.164.21	TCP	66	00:0c:29:98:ca:28,0_		28057 → 636 [FIN, ACK] Seq=964 Ack=4221 Win=39688 Len=0 TSval=141006614 TSecr=30158967
* *	Internet Protocol Version 4, Src: 10.197.164.22, Dst: 10.197.164.21 Transmission Control Protocol, Src Port: 28057, Dst Port: 636, Seq: 336, Ack: 2078, Len: 133 Source Port: 28057 Uestination Port: 636								
Ocstination Profile 635 [Stream index: 2] [TCP Segment Len: 133] Sequence number: 365 (relative sequence number) [Mext sequence number: 2076 (relative sequence number)] Acknowledgenet number: 2076 (relative sequence number) 1000 = Header Length: 32 bytes (8) F Flags: Molls (FSH, ACK) Window size value: 259 [Calculated window size: 33152] [Window size value: 0.00000000000000000000000000000000000									
	▼ TLSUL2 Record Layer: Application Data Protocol: ldap Content Type: Application Data (23) Version: TLS 1.2 (008083) Length: 128 Encrypted Application Data: 173d1b0b2f280a13cc17815e54447bb9ac8af8a881a9eb84								

문제 해결

이 섹션에서는 이 컨피그레이션에서 발생하는 몇 가지 일반적인 오류와 그 해결 방법에 대해 설명 합니다.

• 인증 보고서에서 다음 오류 메시지를 볼 수 있습니다.

Authentication method is not supported by any applicable identity store

이 오류 메시지는 선택한 방법이 LDAP에서 지원되지 않음을 나타냅니다. 동일한 보고서의 인증 프 로토콜이 지원되는 방법(EAP-GTC, EAP-TLS 또는 PEAP-TLS) 중 하나를 표시하는지 확인합니다.

• 서버에 대한 테스트 바인딩이 오류와 함께 종료되었습니다.

가장 일반적으로 이는 LDAPS 서버 인증서 유효성 검사 실패 때문입니다. 이러한 유형의 문제를 해 결하려면 ISE에서 패킷 캡처를 수행하고 디버그 레벨에서 세 가지 런타임 및 prrt-jni 구성 요소를 모 두 활성화하고, 문제를 다시 생성한 다음 prrt-server.log 파일을 확인합니다.

패킷 캡처가 잘못된 인증서에 대해 불평하고 포트 서버가 다음을 표시합니다.

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

참고: LDAP 페이지의 호스트 이름은 인증서의 주체 이름(또는 임의의 주체 대체 이름)으로 구 성해야 합니다. 따라서 주체 또는 SAN에 이러한 인증서가 없으면 작동하지 않으며 SAN 목록 에 IP 주소가 있는 인증서가 필요합니다.

3. 인증 보고서에서 ID 저장소에서 주체를 찾을 수 없음을 알 수 있습니다. 즉, 보고서의 사용자 이름 이 LDAP 데이터베이스의 사용자에 대한 Subject Name Attribute와 일치하지 않습니다. 이 시나리 오에서는 이 특성의 값이 sAMAccountName으로 설정되었습니다. 즉 ISE가 LDAP 사용자가 일치하 는 항목을 찾으려고 할 때 LDAP 사용자의 sAMAccountName 값을 확인합니다.

4. 서버 테스트에 바인딩하는 동안 제목 및 그룹을 올바르게 검색할 수 없습니다. 이 문제의 가장 큰 원인은 검색 기준에 대한 잘못된 컨피그레이션입니다. LDAP 계층 구조는 leaf-to-root 및 dc(여러 단 어로 구성 가능)에서 지정해야 합니다.

관련 정보

- <u>https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine/119149-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>

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번 역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.