# ISE configureren en problemen oplossen met externe LDAPS Identity Store

# Inhoud

Inleiding Voorwaarden Vereisten Gebruikte componenten Configureren Netwerkdiagram LDAPS op Active Directory configureren Identiteitscertificaat op domeincontroller installeren Directory-structuur voor toegang tot LDAPS Integreer ISE met LDAPS-server De Switch configureren Het eindpunt configureren Configureer de beleidsset op ISE Verifiëren Problemen oplossen Gerelateerde informatie

# Inleiding

In dit document wordt de integratie van Cisco ISE met de Secure LDAPS-server als externe identiteitsbron beschreven.

# Voorwaarden

### Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Basiskennis van het beheer van Identity Service Engine (ISE)
- Basiskennis van Active Directory/Secure Lichtgewicht Directory Access Protocol (LDAPS)

### Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Cisco ISE-lijnkaart 2.6 voor Windows 7
- Microsoft Windows versie 2012 R2 met Active Directory Lichtgewicht Directory Services geïnstalleerd
- Windows 10 OS-pc met native applicatie en gebruikerscertificaat geïnstalleerd
- Cisco Switch C3750X met 152-2.E6-afbeelding

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

#### Achtergrondinformatie

LDAPS maakt de codering van LDAP-gegevens (met inbegrip van gebruikersreferenties) mogelijk tijdens het transport wanneer een directory bind tot stand is gebracht. LDAPS gebruikt TCP-poort 636.

Deze verificatieprotocollen worden ondersteund met LDAPS:

- EAP Generic Token Card (EAP-GTC)
- Wachtwoordverificatieprotocol (PAP)
- EAP-TLS-beveiliging (Transport Layer Security)
- Beschermde EAP Transport Layer Security (PEAP-TLS)

**Opmerking**: EAP-MSCHAPV2 (als een inwendige methode van PEAP, EAP-FAST of EAP-TTLS), LEAP, CHAP en EAP-MD5 worden niet ondersteund met LDAPS Externe Identiteitsbron.

# Configureren

In dit deel worden de configuratie van de netwerkapparaten en de integratie van de ISE met Microsoft Active Directory (AD) LDAPS-server beschreven.

### Netwerkdiagram

In dit configuratievoorbeeld gebruikt het eindpunt een Ethernet-verbinding met een switch om verbinding te maken met het Local Area Network (LAN). De aangesloten switchpoort is geconfigureerd voor 802.1xverificatie om de gebruikers met ISE te verifiëren. Op de ISE is LDAPS geconfigureerd als een extern identiteitsarchief.

Dit beeld illustreert de netwerktopologie die wordt gebruikt:



# LDAPS op Active Directory configureren

### Identiteitscertificaat op domeincontroller installeren

Installeer een certificaat op Domain Controller (DC) dat aan deze vereisten voldoet om LDAPS in te schakelen:

- 1. Het LDAPS-certificaat bevindt zich in de Domain Controller's Personal Certificate Store.
- 2. Een privé-sleutel die overeenkomt met het certificaat is aanwezig in de winkel van de domeincontroller en wordt correct geassocieerd met het certificaat.
- 3. De Enhanced Key Usage-extensie omvat Server-verificatie (1.3.6.1.5.5.7.3.1) object identifier (ook bekend als OID).
- 4. De volledig gekwalificeerde domeinnaam (FQDN) van de domeincontroller (bijvoorbeeld DC1.testlab.com) moet aanwezig zijn in een van deze eigenschappen: de algemene naam (CN) in het veld Onderwerp en DNS-vermelding in de alternatieve naam extensie Onderwerp.
- 5. Het certificaat moet worden afgegeven door een certificeringsinstantie(CA) die de domeincontroller en de LDAPS-clients vertrouwen. Voor een betrouwbare beveiligde communicatie moeten de client en de server elkaars root-CA en de tussenliggende CA-certificaten die certificaten aan hen hebben afgegeven, vertrouwen.
- 6. De Schannel cryptographic Service Provider (CSP) moet worden gebruikt om de sleutel te genereren.

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 Au	thi∨
< III	>
Other Name:	
DS Object Guid=04 10 a6 36 1d 3c f4 3f a8 47 83 d7 d3 d5 46 20	a3 3f
DNS Name -DC 1. (ESUBD. COM	

#### Directory-structuur voor toegang tot LDAPS

Maak gebruik van een LDAP browser om toegang te krijgen tot de LDAPS Directory op de Active Directory-server. In dit LAB wordt Softerra LDAP Browser 4.5 gebruikt.

1. Maak een verbinding met het domein op TCP-poort 636.

Scope Pane	4 X	Name A	Value	Туре	
Softerra LDAP Browser	~	Thernet Public Servers	Not Expanded	Group	
(i) and Internet Public Servers		🗄 testiab	idaps://dc1.testlab.com:636/DC=testlab,DC=com	Server Profile	
🖻 🗐 testlab					

2. Maak ter vereenvoudiging een organisatie-eenheid (OE) met de naam ISE-OE in de advertentie en deze moet een groep met de naam UserGroup hebben. Maak twee gebruikers (user1 en user2) en maak ze lid van de groep UserGroup.

Scope Pane 👻 🗙	Name 🔺	Value	Type
Softerra LDAP Browser	CN	UserGroup	Entry
Internet Public Servers	CN	user2	Entry
i destab	CN	user1	Entry
CN=Builtin	CN	DESKTOP-19	Entry
CN=Computers	CN	ComputerGroup	Entry
OU=Domain Controllers	distinguishedName	OU=ISE OU,DC=testlab,DC=com	Attribut
CN=ForeignSecurityPrincipals	dSCorePropagationData	1/1/1601	Attribut
CN=Infrastructure	dSCorePropagationData	6/20/2020 2:51:11 AM	Attribut
OU=ISE Group	🗉 gPLink	[LDAP://cn={21A53813-6971-45E8-8545-FD0C68E29790},c	Attribut
	instanceType	[Writable]	Attribut
CN=ComputerGroup	🗉 name	ISE OU	Attribut
CN=DESKIOP-19	objectCategory	CN=Organizational-Unit, CN=Schema, CN=Configuration, DC=	Attribut
CN=user2	objectClass	organizationalUnit	Attribut
	objectClass	top	Attribut
	Ξou	ISE OU	Attribut
E-CN=LostAndFound	uSNChanged	607428	Attribut
CN=Managed Service Accounts	uSNCreated	603085	Attribut
	whenChanged	6/21/2020 2:44:06 AM	Attribut
🖻 – 📴 CN=Program Data	whenCreated	6/20/2020 2:51:11 AM	Attribut
E CN=System	objectGUID	{44F45D1D-17B7-48DF-ABC6-3ED27FA4F694}	Binary A

Opmerking: LDAP Identity Source on ISE wordt alleen gebruikt voor gebruikersverificatie.

### **Integreer ISE met LDAPS-server**

1. Voer het CA-certificaat van LDAP Server Root in het Trusted Certificate in.

cisce Identity Services Engine H	iome	Policy      Administrat	ion			
System → Identity Management → N	etwork Resources	pxGrid Services Fee	d Service + Threat Cent	ric NAC		
Deployment Licensing - Certificates	Logging      Maintenance Upgrade      Back	kup & Restore + Admin	Access + Settings			
Certificate Management	Friendly Name DC1	Status	Trusted For	Serial Number	Issued To	Issued B
System Certificates	DC1-CA	Enabled	Infrastructure Cisco Services	18 29 1C A7 00 13	testiab-DC1-CA-1	testlab-D
Trusted Certificates			Enopoints			

2. Valideren van het ISE-beheercertificaat en ervoor zorgen dat het ISE-beheercertificaat ook in het Trusted Certificate Store aanwezig is.

3. Om de LDAPS-server te integreren, maakt u gebruik van de verschillende LDAP-kenmerken uit de LDAPS-directory. Ga naar Administratie > Identiteitsbeheer > Externe Identiteitsbronnen > LDAP Identity Sources > Add.

diala cisco	Identity Service	es Engine	Home	Context Visibility	<ul> <li>Operation</li> </ul>	is → Policy	+ Administration	Work Centers		
► Sys	tem 👻 Identity N	lanagement	Network R	esources + Device	Portal Manager	ment pxGrid Se	rvices + Feed Se	rvice + Threat Centr	ic NAC	
► Ider	ntities Groups	External Ider	ntity Sources	Identity Source Sequ	ences + Sel	ttings				
Ex 🖑	ternal Identity So Certificate Auth Active Directory testlab LDAP DBC RADIUS Token RSA SecuriD SAML Id Provid	entication Profile	@ <b>.</b> ≁	LDAP Identity So LDAP Identity General	Source     Conne     Conne     Name     Description     Schema     t     Objectclass	ttab_Idaps ection Dir testlab_Idaps Custom person	rectory Organization	Groups	Attributes	Advanced Setting:
	Cocial Login			* Subject N	ame Attribute	sAMAccountNam	e	* Group Map Attribute	memberOf	
				<ul> <li>Subjec</li> <li>Group</li> </ul>	t Objects Conta Objects Contair	in Reference To G n Reference To Sut Subjects In	roups bjects Groups Are Stored I	n Member Attribute As	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	telephoneNumbe	r	Country	C0	
				s	treet Address	streetAddress				
				Course Course						
				Save Reset						

4. Configureer deze eigenschappen vanuit het tabblad Algemeen:

Objectklasse: dit veld komt overeen met de klasse Object van gebruikersaccounts. Je kunt hier een van de vier klassen gebruiken:

- top
- Persoon
- Organisator
- InetOrgPerson

Scope Pane 🔫 🗙	objectclass	Filter Value	
Scope Pane Softerra LDAP Browser testlab CN=Builtin CN=Computers CN=ForeignSecurityPrincipals CN=Infrastructure CN=Infrastructure CN=ISE Group CN=ISE OU CN=ComputerGroup	objectclass Name   objectClass  objectClass  objectClass  objectClass  objectClass	Filter Value Value user organizationalPerson person top	Type Attribute Attribute Attribute Attribute
CN=DESKTOP-19			

Attribuut onderwerpnaam: Dit veld is de naam van het attribuut dat de gebruikersnaam uit het verzoek bevat. Deze eigenschap wordt uit de LDAPS gehaald wanneer de ISE een specifieke gebruikersnaam in de LDAP-database opvraagt (u kunt cn, sAMAaccountName, enz. gebruiken). In dit scenario wordt de gebruikersnaam 1 op het eindpunt gebruikt.

Scope Pane 👻 🗙	Filter Name	user1		
Softerra LDAP Browser	Name 4	Value		Туре
	🗉 cn	user1		Attribute
CN=Computers	displayName	user1		Attribute
OU=Domain Controllers	distinguishedName	CN=user1,OU=ISE OU,DC=testlab,DC=	-com	Attribute
CN=ForeignSecurityPrincipals	givenName	user1		Attribute
CN=Infrastructure	E name	user1	1	Attribute
OU=ISE Group	sAMAccountName	user1		Attribute
🖶 📴 OU=ISE OU	userPrincipalName	user1@testiab.com	1	Attribute
E CN=ComputerGroup	userCertificate	user1		Binary Attribute
E CN=DESKTOP-19	1			
- CN=user1	1			
CN=user2	1			
E CN=UserGroup	1			

Groepsnaam Attribuut: Dit is het attribuut met de naam van een groep. De waarden van de groepsnaam in uw LDAP-map moeten overeenkomen met de LDAP-groepsnamen op de pagina Gebruikersgroepen

Scope Pane	• ×	Name	Value	Туре
Softerra LDAP Browser		🗉 m	UserGroup	Attrib
🖻 🗐 testlab		distinguishedName	CN=UserGroup,OU=ISE OU,DC=testlab,DC=com	Attrib
😟 🛅 CN=Builtin		dSCorePropagationData	1/1/1601	Attrib
CN=Computers		groupType	[GlobalScope, Security]	Attrib
OU=Domain Controllers		instanceType	[ Writable ]	Attrib
CN=ForeignSecurityPrincipals		member	CN=user1,OU=ISE OU,DC=testlab,DC=com	Attrib
CN=Infrastructure		member	CN=user2,OU=ISE OU,DC=testlab,DC=com	Attrib
OU=ISE Group		🗉 name	UserGroup	Attrib
OU=ISE OU		objectCategory	CN=Group,CN=Schema,CN=Configuration,DC=testlab,DC=com	Attrib
E-CN=ComputerGroup		objectClass	group	Attrib
CN=DESKTOP-19		objectClass	top	Attrib
CN=user1		sAMAccountName	UserGroup	Attrib
CN=UserGroup		sAMAccountType	< samGroupObject >	Attrib

Groep Objectklasse: Deze waarde wordt gebruikt in zoekopdrachten om de objecten te specificeren die als groepen worden herkend.

CN=ComputerGroup	objectSid	S-1-5-21-2960284039-4006096050-347662626-1156	Binary Attribute
I - CN=DESKTOP-19	objectGUID	{39967F90-89BE-44B5-9CC5-B28C0B0EB234}	Binary Attribute
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

Groepskaart Attribute: Deze eigenschap bepaalt hoe de gebruikers aan de groepen in kaart worden gebracht.

Scope Pane 👻 🗙	Filter Name	UserGroup	
Softerra LDAP Browser	Name	Value 🔺	Туре
B- CN=Builtin	memberOf	CN=UserGroup,OU=ISE OU,DC=testlab,DC=com	Attribute
E-CN=Computers			
OU=Domain Controllers	1		
E CN=ForeignSecurityPrincipals			
E CN=Infrastructure			
OU=ISE Group			
E- OU=ISE OU			
CN=ComputerGroup			
E CN=DESKTOP-19			
- CN=user1			

Certificaatkenmerk: Voer het kenmerk in dat de certificaatdefinities bevat. Deze definities kunnen naar keuze worden gebruikt om certificaten te valideren die door cliënten worden gepresenteerd wanneer zij worden gedefinieerd als deel van een verificatieprofiel van een certificaat. In dergelijke gevallen wordt een binaire vergelijking uitgevoerd tussen het clientcertificaat en het certificaat dat uit de LDAP-identiteitsbron wordt gehaald.

1 - 2 - 10 - 10 - 10 - 10 - 10 - 10			
🖻 – 🛄 OU=ISE OU	userPrincipalName	user1@testlab.com	Attribute
E- CN=ComputerGroup	userCertificate	user1	Binary Attribute
CN=DESKTOP-19			

5. Ga naar het tabblad **Verbinding** om de LDAPS-verbinding te configureren:

AP IDENTITY SC	ource					
General	Connection	Directory Organization	Groups	Attributes	Advanced Setting	S
	Primary	Server				Secondary Server
						Enable Secondary Server
* Ho	ostname/IP dc1.test	lab.com			Hostname/IP	
	* Port 636				Port	389
	Access ()	Anonymous Access			Ad	copee Anonymous Access
	Admin DN *  Password *	Authenticated Access CN=poongarg,CN=Users,DC=tes	ŧ		Admi	Authenticated Access in DN sword
	Admin DN *	Authenticated Access CN=poongarg,CN=Users,DC=tes	t)		Admi Pass	Authenticated Access in DN sword
Secu	Admin DN  Admin DN  Password  ure Authentication	Authenticated Access CN=poongarg,CN=Users,DC=tes Enable Secure Authentication Enable Server Identity Check	zi		Admi Pass Secure Authentic	Authenticated Access Authenticated Access in DN sword Enable Secure Authenticated Enable Server Identity Chec
Secu	Admin DN  Admin DN  Password  Password  PServer Root CA  D	Authenticated Access CN=poongarg,CN=Users,DC=tes Enable Secure Authentication Enable Server Identity Check C1-CA	t 		Admi Pass Secure Authentic LDAP Server Roi	Authenticated Access Authenticated Access In DN Sword Enable Secure Authenticatio Enable Server Identity Chec Ot CA DST Root CA X3 Certificate Ai

* Server Timeout	10	@Seconds	Server Timeout	10	() Secon
* Max. Admin Connections	20	۵.	Max. Admin Connections	20	(I)
	Force reconnect every	<li>(i) Minutes</li>		Force reconnect every	④ Minute
	Test Bind to Server			Test Bind to Server	
Failover	Always Access Primary Server F     Failback To Primary Server After	irst 5	Minutes		

6. Draai dsquery op Domain Controller om de gebruikersnaam DN te gebruiken om een verbinding te maken met LDAP server:

PS C:\Users\Administrator> desquery gebruiker -name poongarg

"CN=poongarg, CN=Gebruikers, DC=testlab, DC=com"

Stap 1. SStel het juiste IP-adres of Hostname van de LDAP-server in, definieer de LDAPS-poort (TCP 636) en Admin DN om een verbinding te maken met LDAP over SSL.

Stap 2. Optie voor beveiligde verificatie en controle van de serveridentiteit inschakelen.

Stap 3. Selecteer in het vervolgkeuzemenu het LDAP Server Root CA-certificaat en het ISEbeheercertificaat ISER CA-certificaat (We hebben het certificaat gebruikt, geïnstalleerd op dezelfde LDAPserver om ook het ISE-beheercertificaat af te geven).

Stap 4. Selecteer de Test Bind to server. Op dit punt worden geen onderwerpen of groepen opgehaald omdat de zoekbases nog niet zijn geconfigureerd.

7. Configureer onder **het** tabblad **Indexorganisatie** de Onderwerp/Groep Zoekbasis. Het is het verbindingspunt voor de ISE naar de LDAP. Nu kunt u alleen onderwerpen en groepen ophalen die kinderen zijn van het verbindingspunt. In dit scenario worden zowel het onderwerp als de groep opgehaald uit OU=ISE

_						
	LDAP Identity Sources Li	st > <b>testlab_ida</b>	ps			
	LDAP Identity Sour	ce				
	General	Connection	Directory Organization	Groups	Attributes	Advanced Settir
	* Subject Search Base	OU=ISE OU,	DC=testlab,DC=com Naming C	ontexts)i)		
	* Group Search Base	OU=ISE OU,	DC=testlab,DC=com Naming C	ontexts i		
	Search for MAC Addre	ess in Format	x-xx-xx-xx-xx -			
	Strip start of su	ubject name up t	o the last occurrence of the separate	r \		
	Strip end of su	bject name from	the first occurrence of the separator			

8. Klik onder Groepen op Add om de groepen te importeren vanuit de LDAP op de ISE en de groepen op te halen, zoals in deze afbeelding wordt getoond.

LDAP Identity Sources List > testlab_Idaps							
LDAP Identity Se	ource						
General	Connection	Directory Organization	Groups	Attributes			
/ Edit 🕂 Add 👻	🗙 Delete Group						
Name				•			
CN=UserGrou	up,OU=ISE OU,DC=te	stlab,DC=com					

### De Switch configureren

Configureer de switch voor 802.1x-verificatie. Windows PC is aangesloten op 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 xxxxx
!
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
!
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
```

#### Het eindpunt configureren

Windows Native Supplicant wordt gebruikt en er wordt gebruik gemaakt van een EAP-protocol dat door LDAP wordt ondersteund, EAP-TLS voor gebruikersverificatie en -autorisatie.

1. Zorg ervoor dat PC is voorzien van gebruikerscertificaat (voor gebruiker 1) en bedoeld zijn als clientverificatie en in de Trusted Root-certificeringsinstanties, de emittent-certificaatketen op de PC aanwezig is.



2. Schakel Dot1x-verificatie in en selecteer een verificatiemethode als Microsoft:Smart Card of ander certificaat voor EAP-TLS-verificatie.

pciPassthru0 Properties	×
Networking Authentication Sharing	
Select this option to provide authenticated network acc this Ethemet adapter.	ess for
Enable IEEE 802.1X authentication	
Choose a network authentication method:	
Microsoft: Smart Card or other certificate	Settings
Fallback to unauthorized network access	
Additional Settings	
ОК	Cancel

3. Klik op Aanvullende instellingen en een venster wordt geopend. Schakel het selectievakje in met de verificatiemodus en kies gebruikersverificatie, zoals in deze afbeelding.

	Specify authentication mode		
Select this option to provide au this Ethernet adapter.	User authentication $$	Save crede	ntials
Enable IEEE 802.1X auther	Delete credentials for all users		
Choose a network authenticati	Enable single sign on for this network		
Microsoft: Smart Card or other	Perform immediately before user log	jon	
	O Perform immediately after user logo	n	
Remember my credentials for time I'm logged on	Maximum delay (seconds):	10	*
Fallback to unauthorized ne	Allow additional dialogs to be display sign on	yed during sing	le
Additional Settings	This network uses separate virtual l and user authentication	ANs for machi	ne

### Configureer de beleidsset op ISE

Aangezien EAP-TLS-protocol wordt gebruikt, moet, voordat Policy Set is geconfigureerd, het Certificaatverificatieprofiel worden geconfigureerd en wordt de Identity Source Sequence later gebruikt in het Verificatiebeleid.

cisco	Identity Service	es Engine	Home	Context Visibility	<ul> <li>Operations</li> </ul>	Policy	- Administration	Work Centers
► Sys	stem 👻 Identity N	fanagement	<ul> <li>Network R</li> </ul>	esources + Device P	Portal Management	pxGrid Serv	ices + Feed S	Service
► Ide	ntities Groups	External Ider	ntity Sources	Identity Source Seque	ences + Settings			
Ex	ternal Identity Se	ources entication Profil	्रि <sub>*</sub>	Certificate Authent	ication Profiles List > thentication Pro	LDAPS_cert	t	
) )	DDBC				Description	EAP-TLS of	rtificate based a	uthentication with LDAPS
	SAML Id Provid	ers			Identity Store	testiab_ida	ps	T D
					Use Identity From	Certifica     Any Sut	te Attribute Su	ibject - Common Name
				Match Clie Certificate	nt Certificate Agains In Identity Store ()	Never Only t Alway	o resolve identity s perform binary	r ambiguity comparison
				Save Reset	)			

Raadpleeg het verificatieprofiel van het certificaat in de Identity Source Sequence en definieer de externe identiteitsbron van LDAPS in de zoeklijst voor verificatie:

cisco	Identity Services Engine	Home   Conte	xt Visibility 🔹 🕨	Operations +	Policy -	Administration	Work Centers
<ul> <li>Sys</li> </ul>	tem 🛛 🕶 Identity Management	Network Resources	Device Portal	Management p	pxGrid Service	Feed Servi	ce
Ider	ntities Groups External Ider	ntity Sources Identity	Source Sequences	<ul> <li>Settings</li> </ul>			
Ident	ity Source Sequence						
▼ Id	entity Source Sequence						
	* Name LDAPS						
Des	scription						
						14.	
- (	Certificate Based Authentic	ation					
	Solort Cortificate Authors		cost N	Г			
	Select Certificate Autrient	ucation Profile [LDAPS]	cert :				
* /	Authentication Search List A set of identity se Available Internal Endpoints Internal Users Guest Users testlab All_AD_Join_Points rad	ources that will be acces	sed in sequence un Selected testlab_Idaps	ntil first authentical	tion succeeds		
If a :	selected identity store cannot be	accessed for authentica	tion				
0	Do not access other stores in th	ne sequence and set the	"AuthenticationSta	tus" attribute to "P	rocessError"		
۲	i reat as if the user was not four	nd and proceed to the n	3xt store in the sequ	uence			
Save	Reset						

Configureer nu beleidsset voor bekabelde Dot1x-verificatie:

alialia cisco	Identity S	arvices Engine	Home +	Context Visib	ility Operations	▼Pol	icy Administration	n → Work Centers
Policy	Sets Pr	ofiling Posture	Client Provisionin	ng + Policy	Elements			
-								
Policy	y Sets -	Wired Dot1	ĸ					
	Status	Policy Set Nan	ne	Descriptio	n	Cond	tions	
Searc	:h							
	0	Wired Dot1x					Wired_802.1X	
<b>√</b> Au	uthentication	on Policy (2)						
G	Cint	Dula Mana		Gendille				
	Statu	s Rule Name		Conditio	ns			
Sea	irch							
	ø	Dot1x		₽,	letwork Access-Networ	kDeviceN	ame EQUALS LAB-Swi	vitch
	Ø	Default						

► Auth	orization F	Policy (2)				
					Results	
•	Status	Rule Name	Cond	itions	Profiles	
Search						
	ø	Users in LDAP Store	忠	testlab_ldaps-ExternalGroups EQUALS CN=UserGroup,OU=ISE OU,DC=testlab,DC=com	× PermitAccess	+
	ø	Default			× DenyAccess	+

Na deze configuratie kunnen we het Endpoint authenticeren met behulp van het EAP-TLS-protocol tegen de LDAPS-identiteitsbron.

neral		
onnection		
IPv4 Connectiv	vity:	Internet
IPv6 Connectiv	vity:	No network access
Media State:		Enabled
Duration:		00:01:21
Speed:		1.0 Gbps
tivity	5 ml	Received
	Sent — 🛌	
Bytes:	3,093	676

# Verifiëren

1. Controleer de verificatiesessie op de switchpoort die is aangesloten op de PC:

SW1#sh auth sessions i	nt 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 Templa	te: DEFAULT_LINKSEC_POLICY_SHOULD_SECURE (priority 150)
Server Policies:	
Method status list:	
Method	State
dot1x	Authc Success

2. Om de configuraties van LDAPS en ISE te verifiëren, kunt u de onderwerpen en de groepen met een testverbinding aan de server terugwinnen:

LDAP Identity Sources List > testiab_ide	aps				
LDAP Identity Source					
General Connection	Directory Organization Gro	ups Attributes Advan	ced Settings		
Access	O Anonymous Accord		Access	Anonymous Access	
	Authenticated / Ldap bind support of S	ucceeded to dc1.testlab.com:636 Subjects 3		<ul> <li>Authenticated Access</li> </ul>	
Admin DN	* CN=poongarg,C Number of C Response to	3roups 2 me 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 *	۵.	LDAP Server Root CA	DST Root CA X3 Certificate # *	Ð
Issuer CA of ISE Certificates	DC1-CA	Ĩ.	Issuer CA of ISE Certificates	Select if required (optional)	۵
* Server Timeout	10	] () Seconds	Server Timeout	10	() Seco
* Max. Admin Connections	20	0	Max. Admin Connections	20	D
	Force reconnect every	① Minutes		Force reconnect every	③ Minute
	Test Bind to Server			Test Bind to Server	
Failover	Always Access Primary Server	First			
Save Reset					

### 3. Controleer het gebruikersverificatierapport:

C Refresh O Reset Repeat Counts 🛃 Export To -								
	Time	Status	tus Details Identity Endpoint ID		Authentication Po	Authentication Po Authorization Policy		
×		•		Identity	Endpoint ID	Authentication Policy	Authorization Policy	Authorization Profiles
	Jun 24, 2020 04:45:21.727 AM	•	0	user1	B4:96:91:26:DE:C0	Wired Dot1x >> Dot1x	Wired Dot1x >> Users in LDAP Store	PermitAccess
	Jun 24, 2020 04:45:20.671 AM	2	ò	user1	B4:96:91:26:DE:C0	Wired Dot1x >> Dot1x	Wired Dot1x >> Users in LDAP Store	PermitAccess

4. Controleer het gedetailleerde verificatierapport voor het eindpunt:

Event	5200 Authentication succeeded
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 Unknown						
Endpoint Profile							
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_Idaps
24016	Looking up user in LDAP Server - testlab_Idaps
24023	User's groups are retrieved - testlab_ldaps
24004	User search finished successfully - testlab_ldaps
22054	Binary comparison of certificates succeeded
22037	Authentication Passed
12506	EAP-TLS authentication succeeded

15036	Evaluating Authorization Policy						
24209	Looking up Endpoint in Internal Endpoints IDStore - user1						
24211	Found Endpoint in Internal Endpoints IDStore						
15048	48 Queried PIP - testlab_Idaps.ExternalGroups						
15016	Selected Authorization Profile - PermitAccess						
22081	22081 Max sessions policy passed						
22080 New accounting session created in Session cache							
11503	Prepared EAP-Success						
11002	002 Returned RADIUS Access-Accept						

5. Bevestig dat de gegevens worden versleuteld tussen de ISE- en LDAPS-server door pakketopname op de ISE naar de LDAPS-server te nemen:

i	No.	Time		Source	Destination	Protocol	Length	Address	64bits	Info
1	20	2020-06-24 10	8:40:24.205431	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 Se
	21	2020-06-24 10	8:48:24.286585	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 M
1	22	2020-06-24 10	0:40:24.206613	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 TSva
	23	2020-06-24 10	0:40:24.206961	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	8:48:24.218413	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
	25	2020-06-24 10	8:40:24.210508	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
	26	2020-06-24 10	0:40:24,215211	10.197.164.22	10,197,164,21	TLSv1.2	260	00:0c:29:98:ca:28.0		Certificate, Client Key Exchange, Change Cipher Sp
J	27	2020-06-24 10	8:40:24.218678	10.197.164.21	10.197.164.22	TLSv1.2	173	00:50:56:a0:3e:7f.0_		Change Cipher Spec, Encrypted Handshake Message
ł	28	2828-86-24 18	1:48:24.219113	18, 197, 164, 22	18, 197, 164, 21	TLSv1.2	199	88:8c:29:98:ca:28.8		Application Data
1	29	2020-06-24 10	1:40:24,230384	18,197,164,21	10,197,164,22	TLSv1.2	167	00:50:56:a0:3e:7f.0_		Application Data
	30	2828-86-24 18	1:40:24.231712	10,197,164,22	10,197,164,21	TLSv1.2	279	00:0c:29:98:ca:28.0_		Application Data
	31	2828-86-24 18	1:48:24,238889	18, 197, 164, 21	18, 197, 164, 22	TLSv1.2	1879	00:50:56:a0:3e:7f.0_		Application Data[Packet size limited during capture
	32	2828-86-24 18	1:48:24.238958	18, 197, 164, 22	18, 197, 164, 21	TCP	66	88:8c:29:98:ca:28.8		28857 + 636 [ACK] Sequ682 Ack=3992 Win=36864 Len=8
	33	2020-06-24 10	1:48:24.251944	10.197.164.22	10.197.164.21	TL Sv1.2	263	88:8c:29:98:ca:28.8		Application Data
	3.4	2020-06-24 10	1-40-24-251544	10 107 164 21	10 197 164 22	TI Su1 2	205	88:58:56:38:30:7f 8		Application Data
	25	2020-00-24 10	- 48-24 203030	10 107 164 22	18 107 164 21	TCP	66	88+8c+20+08+c++28 8		20057 - 636 [ACK] Same970 Ark=4221 Win=30600 Lan=0
	95	2020-00-24 10	A. 40.57 046553	10.107.164.22	10.107.164.21	TLSu1 2	151	00.0c.29.90.ca.20,0		Application Data
ł	97	2020-00-24 10	40.57.940333	10.107.164.22	10.197.104.21	TCP	151	00:00:29:50:00:00;00	_	20057 . C2C (ETN ACV) ConnOCA Ark-4221 Min-20500
	07	2020-00-24 10	1:40:37.347000	10.137.104.22	10.13/.104.21	TOP	00	00:00:29:30:00:20,0-		2003/ + 030 [FIN, ACK] 300=304 ACK=4221 H1H=33000 [
1	Frame 2	28: 199 bytes o	on wire (1592 bit	ts), 199 bytes capture	d (1592 bits)	100.0				
J	▶ Etherne	et II, Src: Vm	ware_a0:3e:7f (00	8:50:56:a0:3e:7f), Dst	: Vmware_98:ca:28	(00:0c:29:	98:ca:28	)		
J	▶ Internet	et Protocol Ver	rsion 4, Src: 10.	.197.164.22, Dst: 10.1	97.164.21					
	Transmi	ission Control	Protocol, Src Po	ort: 28057, Dst Port:	636, Seq: 336, Ac	k: 2078, Le	n: 133			
÷	Sou	rce Port: 2805	7							
	Des	tination Port:	636							
	lSt	ream index: 2]								
	[TCP Segment Len: 133]									
Sequence number: 336 (relative sequence number)										
[Next sequence number: 469 (relative sequence number)]										
Acknowledgment number: 2078 (relative ack number)										
1000 = Header Length: 32 bytes (8) ▶ Flags: 0x018 (PSH, ACK)										
Window size value: 259 [Calculated window size: 33152]										
	[Wii	ndow size scal	ing factor: 128]							
	Che	cksum: 0x5e61	[unverified]							
	[Ch	ecksum Status:	Unverified]							
	Urg	ent pointer: 0								
	Dotions: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps									
	► [SE]	0/ACK analysis	1							
	► [Ti	nestanosl								
	TCP	payload (133)	bytes)							
1	r Secure	Sockets Laver								
▼ TLSv1.2 Record Layer: Application Data Protocol: Idap Content Type: Application Data (23) Version: TLS 1.2 (0x0303)										
							to			
		Length: 128	10/03/03/					<ul> <li>Encrypted</li> </ul>	Da	la
		Encounted Anni	lication Data: 17	341686262885137715	a54447hhQac8a40.00	1ageb84				
J		encitation white	creation paras 1/	20100011200012001/012	C344470030C0010000	1030004111				

# Problemen oplossen

In deze sectie worden enkele veelvoorkomende fouten beschreven die bij deze configuratie optreden en hoe u deze kunt oplossen.

• In het verificatierapport kunt u deze foutmelding zien:

Authentication method is not supported by any applicable identity store

Deze foutmelding geeft aan dat de gekozen methode niet wordt ondersteund door LDAP. Zorg ervoor dat het verificatieprotocol in hetzelfde rapport een van de ondersteunde methoden toont (EAP-GTC, EAP-TLS of PEAP-TLS).

• Test bind aan server eindigde met een fout.

Meestal is dit te wijten aan de fout in de validatie van het LDAPS-servercertificaat. Om dit soort problemen op te lossen, neemt u een pakketopname op ISE en schakelt u alle drie de runtime- en poortjni-componenten op debug-niveau in, ontspant u het probleem en controleert u het bestand poortserver.log.

Packet Capture klaagt over een slecht certificaat en toont de printerserver:

**Opmerking**: de hostnaam op de LDAP-pagina moet worden geconfigureerd met de onderwerpnaam van het certificaat (of een van de alternatieve onderwerpnaam). Dus, tenzij u dergelijke in het onderwerp of SAN hebt, werkt het niet, is het certificaat met het IP-adres in de SAN-lijst nodig.

3. In het verificatierapport kunt u opmerken dat het onderwerp niet in het identiteitsarchief is gevonden. Dit betekent dat de gebruikersnaam uit het rapport niet overeenkomt met het kenmerk Onderwerpnaam voor een gebruiker in de LDAP-database. In dit scenario is de waarde voor deze eigenschap ingesteld op sAMAaccountName, wat betekent dat de ISE naar de AMAaccountName-waarden kijkt voor de LDAPgebruiker wanneer deze een overeenkomst probeert te vinden.

4. De onderwerpen en groepen konden niet correct worden teruggehaald tijdens een bind-to-server test. De meest waarschijnlijke oorzaak van dit probleem is een onjuiste configuratie voor de zoekbases. Vergeet niet dat de LDAP hiërarchie moet worden gespecificeerd van blad-tot-wortel en dc (kan uit meerdere woorden bestaan).

# Gerelateerde informatie

- <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-configure-eap-tls-authentication-with-is.html</u>

#### Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.