اهحالصإو هئاطخأ فاشكتساو ISE نيوكت يجراخلا LDAP فيرعت نزخم مادختساب

تايوتحملا

<u>ةمدقملا</u> <u>قيساسألا تابلطتملا</u> <u>تابلطتملا</u> <u>ةمدختسملا تانوكملا</u> <u>نىوكتلا</u> <u>ةكېشلل يطيطختلا مسرلا</u> <u>Active Directory یلع LDAP نیوکت</u> لالجمل اب مكحتانا قدحو يانع قيومانا قدامش تيبثت <u>LDAP لېلد قېنب ېلا لوصولا</u> LDAP مداخ عم ISE جمد <u>لوحملا نېوكت</u> <u>قياەنلا ةطقن نيوكت</u> <u>ISE ىل ع چەن لا قعومچم نى وك </u> <u>قحصاا نم ققحتاا</u> <u>امحال ص او ءاطخأل ا ف اش ك ت س ا</u> <u>ةلص تاذ تامولعم</u>

ەمدقملا

.يجراخ ةيوه ردصمك نمآلا LDAP مداخ عم Cisco ISE لماكت دنتسملا اذه فصي

ةيساسألا تابلطتملا

تابلطتملا

:ةيلاتا عيضاوملاب ةفرعم كيدل نوكت نأب Cisco يصوت

- ISE) ةيوەلا ةمدخ كرحم ةرادإل ةيساسألا ةفرعملا

ةمدختسملا تانوكملا

ةيلاتلا ةيداملا تانوكملاو جماربلا تارادصإ ىلإ دنتسملا اذه يف ةدراولا تامولعملا دنتست:

- Cisco ISE 2.6 Patch 7
- Microsoft Windows دادص الدص الدعم 2012 R2 تامدخ عم Active Directory Lightweight Directory

ةتبثملا

- مدختسملا ةداهشو لصألاا بلاط هيلع تبثملا Windows 10 ليغشتلا ماظن رتويبمك •
- isco Switch C3750X لوحملا ∙ 152-2.E6 لوحمل

ةصاخ ةيلمعم ةئيب يف ةدوجوملا ةزهجألاا نم دنتسملا اذه يف ةدراولا تامولعملا ءاشنإ مت. تناك اذإ .(يضارتفا) حوسمم نيوكتب دنتسملا اذه يف ةمدختسُملا ةزهجألا عيمج تأدب رمأ يأل لمتحملا ريثأتلل كمهف نم دكأتف ،ليغشتلا ديق كتكبش.

ةيساسأ تامولعم

ءانثأ (مدختسملا دامتعا تانايب نمضتت يتلاا) LDAP تانايب ريفشتب LDAPs حمست دفنم LDAP مدختست .ليلد طبر ءاشنإ دنع لقنلا

LDAPs: عم هذه ةقداصملا تالوكوتورب معد متي

- حاعلا زيمملا زمرلا ةقاطب EAP (EAP-GTC)
- (PAP) رورملا ةملك ةقداصم لوكوتورب •
- (EAP-TLS) لقنلا ةقبط نامأ
- (PEAP-TLS) يمحملا EAP لقن ةقبط نامأ

م العام EAP-TTLS)، LEAP وأ EAP-ل وأ PEAP ل يلخاد بولسأك) EAP-MSCHAPV2 :ةظحالم EAP-MSCHAPV2 :ةظحالم ل. لقألا يل لوصول اطاقنل يجراخلا ةيوهل ردصم عم موعدم ريغ EAP-MD5 و ،

نيوكتلا

مداخ عم ISE لماكتو ةكبشلا ةزهجأ نيوكت مسقلاا اذه فصي Microsoft Active Directory (AD) LDAP.

ةكبشلل يطيطختلا مسرلا

ةكبشب لاصتالل لوحمب تنرثيإ لاصتا ةياهنلا ةطقن مدختست ،اذه نيوكتلا لاثم يف قوداصمل AN). تقيل switchport نيوكت متي (LAN) قيل ملا ا قوداصمل ISE، تيوكت مت الكا عم نيمدختسمل

همادختسإ متي يذلا ةكبشلا ططخم ةروصلا اذه حضوي:



Secure LDAP Server

Active Directory ىلع LDAP نيوكت

لاجملاب مكحتلا ةدحو ىلع ةيوەلا ةداەش تيبثت

ەذەب يفت (DC) لاجملاب مكحتلا ةدحو ىلع ةداەش تيبثتب مق ،LDAPs نيكمتل تابلطتملا:

- .لاجملاب مكحتلا ةدحول ةيصخشلا تاداهشلا نزخم يف LDAP ةداهش دجوت .1
- لكشب طبتريو لاجملاب مكحتلا ةدحو نزخم يف ةداەشلل قباطم صاخ حاتفم دجوي .2 ةداەشلاب حيحص.
- فرعم (1.3.6.1.5.5.7.3.1) مداخلا ةقداصم نسحملا حاتفملا مادختسا قحلم نمضتي .3 (OID مساب اضيأ فورعملا) نﺉاګلا.
- ىلع) لاجملاب مكحتلا ةدحوب صاخلا (FQDN) لماكلاب لەؤملا لاجملا مسا نوكي نأ بجي .4 يف (CN) عئاشلا مسالا :تامسلا ەذە ىدحإ يف ادوجوم (DC1.testlab.com ،لاثملا ليبس "عوضوملل ليدبلا مسالا" قحلم يف DNS لاخداو عوضوملا لقح
- لاجملاب مكحتلا ةدحو نم لك هب قثي (CA) قدصم عجرم ةطساوب ةداهشلا رادصإ بجي .5 عجرملاب مداخلاو ليمعلا قثي نأ بجي ،هب قوثوملا نمآلا لاصتالل .LDAP ءالمعو رادصإب تماق يتلا ةطيسولا قدصملا عجرملا تاداهشبو رخآلاب صاخلا رذجلا قدصملا .امهل تاداهش
- .حاتفملا ءاشنإل (CSP ريفشت ةمدخ رفوم مادختسإ بجي .6

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	\sim
< III >	
Other Name:	
DS Object Guid=04 10 a6 36 1d 3c f4 3f a8 47 83 d7 d3 d5 46 20 a3	3f
UND Name - DC 1. (ESUBD. COm	

LDAP ليلد ةينب ىلإ لوصولا

اذه يف LDAPs ضرعتسم يأ مدختسأ ،Active Directory مداخ ىلع LDAPs ليلد ىلإ لوصولل Softera LDAP، رادصإلا ،4.5 حفصتم مادختسإ متي ،ربتخملا

1. ذفنم ىلع لاجملاب لاصتا ءاشنإب مق



نأ بجيو ،نالعإلا يف ISE OU ىمست (OU) ةيميظنت ةدحو ءاشنإب مق ،ةطاسبلا لجأ نم .2 (user1 و user1) نيمدختسملا نم نينثإ ءاشنإب مق .UserGroup ىمست ةعومجم ىلع يوتحت قعومجم يف نيوضع امەلعجو UserGroup.



Scope Pane 🔹 🗙	Name 🔺	Value	Туре
Softerra LDAP Browser	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
OU=Domain Controllers	distinguishedName	OU=ISE OU,DC=testlab,DC=com	Attribute
B- CN=ForeignSecurityPrincipals	dSCorePropagationData	1/1/1601	Attribute
E- CN=Infrastructure	dSCorePropagationData	6/20/2020 2:51:11 AM	Attribute
OU=ISE Group	🗉 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
IE- 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
E-CN=System	objectGUID	{44F45D1D-17B7-48DF-ABC6-3ED27FA4F694}	Binary Attribute

LDAP مداخ عم ISE جمد

.اەب قوثوملا ةداەشلا يف LDAP مداخل رذجلا قدصملا عجرملا ةداەش داريتسإ .1

cisco Identity Services Engine	Home Context Visibility Operations Policy	→ Administratio	on Work Centers			
System Identity Management	Network Resources	Services Feed	Service + Threat Centr	ic NAC		
Deployment Licensing - Certificates	Logging Maintenance Upgrade Backup & R	estore Admin A	ccess + Settings			
0		Otation 1	To only of Free	Control Municipation	Increased The	Increased Day
- Certificate Management	Priendly Name	Status	Irusted Por	Senal Number	Issued to	Issued By
· Certificate management	DC1					
System Certificates	DC1-CA	Enabled	Infrastructure Cisco Services	18 29 1C A7 00 13	testlab-DC1-CA-1	testlab-DC1-CA-1
Trusted Certificates			Endpoints			

يف اضيأ ةدوجوم ISE لوؤسم ةداەش ردصم ةداەش نأ نم دكأتو ISE لوؤسم ةداەش نم ققحت .2 مب قوثوملا تاداەشلا نزخم.

ة. قرادإ ىلإ لقتنا. LDAPs ليلد نم ةفلتخملا LDAP تامس مدختسأ ،LDAP مداخ لماكت لجأ نم قوادإ < LDAPs قيوه رداصم < قيجراخلا قيوهلا رداصم < قيوهلا قرادإ <.

tisco Identity Services Engine Home	Context Visibility Operations	Policy Administration	Work Centers	
System Identity Management Network	Resources + Device Portal Manageme	ent pxGrid Services + Feed Ser	vice	NAC
Identities Groups External Identity Sources	Identity Source Sequences + Settin	ngs		
External Identity Sources	LDAP Identity Sources List > testin LDAP Identity Source General Connect * Name te Description • Schema co	ab_idaps ion Directory Organization stlab_idaps	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 User Info Attributes ()	AMAccountName dn Reference To Groups Reference To Subjects Subjects In Groups Are Stored In	* Group Objectclass * Group Map Attribute Certificate Attribute	Group memberOf userCertificate Distinguished Name
	First Name	pivenName	Department	department
	Last Name	sn	Organizational Unit	company
	Job Title t	title	Locality	
	Email	mail	State or Province	st
	Telephone	telephoneNumber	Country	0
	Street Address	streetAddress		
	Save Reset			

4. "ماع" بيوبتلا ةمالع نم تامسلا هذه نيوكتب مق":

كنكمي .نيمدختسملا تاباسحل Object ةئف عم لقحلا اذه قفاوتي :عوضوملل ObjectClass انه ةعبرألا لوصفلا دحأ مادختسإ:

- ىلءأ •
- صخش •
- يميظنت فظوم •
- InetOrgPerson

Scope Pane 🗸 🗙	objectclass	Filter Value		
Softerra LDAP Browser testlab CN=Builtin CN=Computers CN=Computers CN=ForeignSecurityPrincipals CN=ForeignSecurityPrincipals CN=Infrastructure CN=Infrastructure CN=INFrastructure CN=ISE Group OU=ISE Group OU=ISE Group CN=DESKTOP-19 CN=User1 CN=user1 CN=user2 CN=UserGroup	Name A SobjectClass SobjectClass SobjectClass SobjectClass	Value user organizationalPerson person top	Type Attrib Attrib Attrib	e bute bute bute

ببلطلا نم مدختسملا مسا ىلع يوتحت يتلا ةمسلا مسا وه لقحلا اذه :عوضوملا مسا ةمس. ةدعاق يف ددحم مدختسم مسا نع ISE رسفتسي امدنع LDAPs نم ةمسلا هذه دادرتسإ متي مادختسإ كنكمي) LDAP تانايب دn، sAMAccountName، مادختسإ كنكمي) متي ،ويرانيسلا اذه يف ةياهنلا ةطقن يلع 1مدختسم مسا مادختسإ.

Scope Pane 👻 🗙	Filter Name	user1	
Softerra LDAP Browser	Name 🔺	Value	Туре
E-CN=Builtin	≡ cn ≡ displavName	user1 user1	Attribute Attribute
OU=Computers OU=Domain Controllers	distinguishedName	CN=user1,OU=ISE OU,DC=testlab,DC=com	Attribute
CN=ForeignSecurityPrincipals CN=Infrastructure	givenivame	user1	Attribute
OU=ISE Group	sAMAccountName	user1	Attribute
CN=ComputerGroup		user1	Binary Attribute
CN=user1			

مسا ةمس ميق قباطتت نأ بجي .ةعومجم مسا لمحت يتلا ةمسلا يه هذه :ةعومجملا مسا ةمس تاعومجم ةحفص يف ةدوجوملا LDAP ةعومجم ءامسأ عم LDAP ليلد يف ةدوجوملا ةعومجملا نيمدختسملا

Scope Pane 🛛 👻 🗙	Name 🔺	Value	Туре
Softerra LDAP Browser	= m	UserGroup	Attribute
Ė… 🗐 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

تانئاكلا ديدحتل ثحبلا تايلمع يف ةميقلا هذه مادختساٍ متي :ةعومجملل ObjectClass تاعومجمك اهيلع فرعتملا.

	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
H- CN=user2	objectClass	group	Attribute
CN=UserGroup	objectCategory	CN=Group,CN=Schema,CN=Configuration,DC=testlab,DC=com	Attribute

تاعومجملا ىلٍ نيمدختسملا نييعت ةيفيك ةمسلا هذه ددحت :ةعومجملا ططخم ةمس.

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

هذه مادختسإ نكمي .ةداهشلا تافيرعت ىلع يوتحت يتلا ةمسلا لخدأ :ةداهشلا ةمس

امدنع ءالمعلا ةطساوب اهميدقت متي يتلا تاداهشلا ةحص نم ققحتلل ايرايتخإ تافيرعتلا ءارجإ متي ،تالاحلا هذه لثم يفو .ةداهشلا ةقداصم فيرعت فلم نم ءزجك اهفيرعت متي LDAP. قيوه ردصم نم اهدادرتسإ مت يتلا ةداهشلاو ليمعلا ةداهش نيب ةيئانث ةنراقم

+ Coloradora	a deleter	10113
a design of		

: ليصوت بيوبتلا ةمالع ىلإ لقتنا ،LDAPs لاصتا نيوكتل

LDAP Identity Sources List > test	lab_idap	15							
LDAP Identity Source	rtion	Directory Organization		Groups	Attributes	Advanced Sett	inas		
	Primar	y Server		0.000	100000		Seco	ndary Server	
							E	nable Secondary Ser	ver
* Hostname/IP	dc1.te	stlab.com	٢			Hostname/IF	•		Ð
* Port	636					Por	t 389		
Specify server for each ISE	Enode								
A	ccess	Anonymous Access Authenticated Access					Access	 Anonymous Act Authenticated A 	ccess
Adm	Admin DN * CN=poongarg,CN=Users,DC=testi		C=testi		Admin DN				
Pas	sword	• ••••••				P	assword		
Secure Authenti	cation	Enable Secure Authentica Enable Server Identity Ch	tion eck			Secure Auther	ntication	Enable Secure A	Authentication Sentity Check
LDAP Server Ro	oot CA	DC1-CA	•			LDAP Server	Root CA	DST Root CA X3 Co	ertificate Ai 🎽 🕢
Issuer CA of ISE Certif	ficates	DC1-CA	Ţ (ł)		Issue	r CA of ISE Ce	rtificates	Select if required (optional) *
* Server Timeout	10	a	Seconds		5	Server Timeout	10		() Seconds
* Max. Admin Connections	20				Max. Admi	in Connections	20		Ð
	E For	ce reconnect every	Minutes				Force	reconnect every	 Minutes
	Test E	Bind to Server					Test Bin	d to Server	
Failover	Alw	avs Access Primary Server First							

6. مدختسملا مسا ىلع لوصحلل لاجملاب مكحتلا ةدحو ىلع تانايبلا ليغشتب مق مداخب لاصتا ءارجإ يف همادختسال LDAP:

Minutes

PS C:\Users\Administrator>مدختسم مدختسم مدختسم -name poongarg "CN=poongarg،CN=Users،DC=testlab،DC=com"

Failback To Primary Server After 5

ذفنم فيرعتب مقو ،LDAP مداخل حيحصلا فيضملا مسا وأ حيحصلا IP ناونع ددحLos ةوطخلا

ل LDAPs (TCP 636)، دربع LDAPs عم لاصتا ءارجإل SSL.

مداخلا ةيوه نم ققحتلا رايخو ةنمآلا ةقداصملا نيكمتب مق .2 ةوطخلا.

لوؤسم ةداەشو LDAP مداخل رذجلا قدصملا عجرملا ةداەش ددح ،ةلدسنملا ةمئاقلا نم .3 ةوطخلا ISE مداخ سفن ىلع تبثملا ةداەشلا عجرم انمدختسا دقل) قدصملا عجرملا قداەش اصيأ ISE لوؤسم ةداەش رادصإل.

تاعومجم وأ صاخشأ يأ دادرتسإ متي ال ،ةطقنلا هذه دنع .مداخلاب طبرلا رابتخإ ددح .4 ةوطخلا دعب ثحبلا دعاوق نيوكت متي مل هنأل.

اهنإ .ةعومجملا/عوضوملا ثحب ةدعاق نيوكتب مق ،ليلدلا ةسسؤم بيوبتلا ةمالع تحت .7 يه يتلا تاعومجملاو عيضاوملا طقف عاجرتسإ كنكمي نآلا .LDAP عم ISE ل طبرلا ةطقن نم ةعومجملاو عوضوملا نم لك دادرتسإ متي ،ويرانيسلا اذه يف .طبرلا ةطقن لافطأ OU=ISE OU

LDAP Ide	entity Sources Lis	st > testlab_idaps				
(General	Connection	Directory Organization	Groups	Attributes	Advanced Settings
* Subj * Grou Searc	ect Search Base up Search Base h for MAC Addre Strip start of su Strip end of sul	OU=ISE OU,DC OU=ISE OU,DC ss in Format xx-x	e last occurrence of the separato	iontexts i iontexts i pr \		
	Strip end of sul	bject name from the	first occurrence of the separato	r		

8. دادرتساو ISE ىلع LDAP نم تاعومجملا داريتسال ةفاضإ قوف رقنا ،تاعومجملا تحت . ةروصلا هذه يف حضوم وه امك ،تاعومجملا.

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

لوحملا نيوكت

```
switchport gig2/0/47 ب لصتم Windows رتويبمك زاهج .802.1x ةقداصمل لوحملا نيوكتب مق
```

```
aaa new-model
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
Т
aaa server radius dynamic-author
client x.x.x.x server-key xxxxx
1
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
1
!
interface GigabitEthernet2/0/47
switchport access vlan xx
switchport mode access
authentication port-control auto
dot1x pae authenticator
```

ةياەنلا ةطقن نيوكت

مدختسي Windows Native Plus تالوكوتورب دحأ مدختسيو LDAP، EAP-TLS ةموعدملا EAP تالوكوتورب دحأ مدختسيو. ضيوفتلاو مدختسملا ةقداصمل.

دوصقملا ضرغلا دوجو نمو (1 مدختسملل) مدختسملا ةداەشب رتويبمكلا ديوزت نم دكأت .1 تاداەش ةلسلس نأو ،"اەب قوثوملا رذجلا قيدصتلا تائيە" يفو ليمعلا ةقداصمك ەنم يصخشلا رتويبمكلا ىلع ةدوجوم ردصملا.



2. ىرخأ ةداەش وأ Microsoft:Smart ةقاطبك ةقداصملا بولسأ ديدحتو dot1x ققداصم نيكمت قوداصمل EAP-TLS.

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	
 Remember my credentials for this connection each time I'm logged on Fallback to unauthorized network access 	
Additional Settings	
OK Canc	ы

رتخاو ةقداصملا عضو ديدحت عم عبرملا ددح .راطإ حتفيو ،"ةيفاضإ تادادعإ" قوف رقنا .3 ةروصلا هذه يف حضوم وه امك ،مدختسملا ةقداصم.



ISE ىلع جەنلا ةعومجم نيوكت

فيرعت فلم نيوكت مزلي ،جەنلا ةعومجم نيوكت لبقو ،EAP-TLS لوكوتورب مادختسإ ذنم دعب اميف ةقداصملا جەن يف ةيوەلا ردصم لسلست مادختساو ةداەشلا ةقداصم.

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	

يجراخلا ةيوەلا ردصم ددحو ةيوەلا ردصم لسلست يف ةداەشلا ةقداصم فيرعت فلم ىلإ عجرا LDAP :ةقداصملا نع ثحبلا ةمئاق يف

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								

wired Dot1x: ةقداصمل نآلا جەنلا ةعومجم نيوكت

cisco	dentity Ser	rvices Engine Home	Context Visibility	Operations Policy	Administration	► Work Centers			License Warning 🔺	۹ 0	•	0
Policy	Sets Pro	filing Posture Client Provis	ioning Policy Elements	3								
Policy	Sets →	Wired Dot1x						Reset P	olicyset Hitcounts	Reset	S	ave
	Status	Policy Set Name	Description	Conditio	ons			AI	lowed Protocols / Se	ver Seque	nce	Hits
Search												
	0	Wired Dot1x		8	Wired_802.1X				Default Network Access	х т	+	453
❤ Aut	hentication	n Policy (2)										
+	Status	Rule Name	Conditions					Use		Hits	Acti	ions
Seat	ch											
	Ø	Dot1x	Network Ac	ccess-NetworkDeviceNan	e EQUALS LAB-Switch			LDAPS	0	. •	*	¢.
			-1-					> Options				
LDAPS				0		4	Ġ					
		and the second sec						> Options				-

► Auth	orization F	Policy (2)								
+					Results					
\smile	Status	Rule Name	le Name Conditions		Profiles		Security Groups		Hits	Actions
Searc	1									
	ø	Users in LDAP Store	串	testlab_idaps-ExternalGroups EQUALS CN=UserGroup,OU=ISE OU,DC=testlab,DC=com	× PermitAccess	+	Select from list	- +	207	٥
	\odot	Default			× DenyAccess	+	Select from list	• +	11	٥
									Reset	Save

لباقم EAP-TLS لوكوتورب مادختساب ةياهنلا ةطقن ةقداصم اننكمي ،نيوكتلا اذه دعب قيوه ردصم LDAP.

onnection		
IPv4 Connectiv	ity:	Internet
IPv6 Connectiv	ity:	No network access
Media State:		Enabled
Duration:		00:01:21
Speed:		1.0 Gbps
Details]	
Details] Sent —	Received
Details ctivity Bytes:	Sent — 5.000 3,093	Received

ةحصلا نم ققحتلا

:يصخشلا رتويبمكلاب لصتملا Switchport ىلع ةقداصملا ةسلج نم ققحت .1

SW1#sh auth sessions in	nt g2/0/47 de
Interface:	GigabitEthernet2/0/47
MAC Address:	b496.9126.dec0
IPv6 Address:	Unknown
IP∨4 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)
Service remptat	the person let more locate locate (b) for fey and
Server Policies:	
Method status list:	
Method	State
dot1x	Authc Success

مادختساب تاعومجملاو تاعوضوملا دادرتسإ كنكمي ،ISE و LDAP تانيوكت نم ققحتلل .2 مداخلاب رابتخإ لاصتا:

LDAP Identity Sources List > testiab_ide	sps			
LDAP Identity Source				
General Connection	Directory Organization Groups Attributes Advan	ced Settings		
Access	O Anonymous Ac	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	
	C Enable Server Identity Check		Enable Server Identity Check	
LDAP Server Root CA	DC1-CA T	LDAP Server Root CA	DST Root CA X3 Certificate / *	()
Issuer CA of ISE Certificates	DC1-CA 🝸 🕖	Issuer CA of ISE Certificates	Select if required (optional)	()
* Server Timeout	10 (i Seconds	Server Timeout	10	@Seconds
* Max. Admin Connections	20 ①	Max. Admin Connections	20	Ð
	Force reconnect every ① Minutes		Force reconnect every	(i) Minutes
	Test Bind to Server		Test Bind to Server	
Failover	Always Access Primary Server First			
Save Reset				

3. مدختسملا ةقداصم ريرقت نم ققحتلا:

c	Refresh O Reset Repeat Coun	ts 💆 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 Protocc
	Jun 24, 2020 04:45:21.727 AM	0	ò	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

ةياەنلا ةطقنل يليصفتلا ةقداصملا ريرقت نم ققحت .4

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_ldaps.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					

ة اجتاب ISE ىلع مزحلا طاقتلاا لالخ نم LDAP مداخو ISE نيب تانايبلا ريفشت نم ققحت .5 مداخ LDAPs:

No.		Time	A Source	Destination	Protocol	Length	Address	64bits	Info		
-	20	2020-06-24 10:40:24.205431	10.197.164.22	10.197.164.21	TCP	74	00:0c:29:98:ca:28,0		28057 → 636 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK PERM=1 TSval=140972872 TSecr=0 WS=128		
	21	2828-86-24 18:48:24.286585	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 MSS=1460 WS=256 SACK PERM=1 TSval=30158962 TSecr=140972872		
	22	2020-06-24 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	2020-06-24 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	2020-06-24 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	2020-06-24 10:40:24.210508	10.197.164.22	10.197.164.21	TCP	66	00:0c:29:98:ca:28,0_		28057 → 636 [ACK] Seq=142 Ack=1971 Win=33152 Len=0 TSval=140972877 TSecr=30158962		
	26	2020-06-24 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		
1	27	2020-06-24 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	2020-06-24 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	2020-06-24 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	2020-06-24 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	2020-06-24 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	2020-06-24 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	2020-06-24 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	2020-06-24 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	2020-06-24 10:40:24.293322	10.197.164.22	10.197.164.21	TCP	66	00:0c:29:98:ca:28,0_		28057 → 636 [ACK] Seq=879 Ack=4221 Win=39680 Len=0 TSval=140972960 TSecr=30158967		
	86	2020-06-24 10:40:57.946553	10.197.164.22	10.197.164.21	TLSv1.2	151	00:0c:29:98:ca:28,0		Application Data		
1	87	2020-06-24 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=39680 Len=0 TSval=141006614 TSecr=30158967		
 Ethernet II, Src: Vmware_a0:3e:7f (00:50:56:a0:3e:7f), Dst: Vmware_90:ca:28 (00:0c:29:90:ca:28) Internet Protocol Version 4, Src: 10:197.164.22, Dst: 10:197.164.21 Transmission Control Protocol, Src Port: 20057, Dst Port: 636, Seq: 336, Ack: 2078, Len: 133 Source Port: 20057 											
Destinution Port: 636 [Stream index: 2] [ICF Segment Len: 133] Sequence number: 356 (relative sequence number) [Next sequence number: 2678 (relative sequence number)] Acknowledgment number: 2678 (relative ack number) 1000 = Header Length: 32 bytes (8) F Flags: 0x081 (PSH, ACK) Window size value: 259 [Calculated window size: 31352] [Window size salise: 259 [Calculated window size: 31352] [Checksum: 0x5651 [unverited] Urgent pointer: 00 b Options: (12 Dytes), No-Operation (NOP), No-Operation (NOP), Timestamps ▶ [ISG2(KX analysis)] TCP apyload (133 bytes) Secure Sockets Layer w TLSv1.2 Record Layer: Application Data Protocol: [dap											
▼ TLSV1.2 Record Layer: Application Data Protocol: Idap Content Type: Application Data (23) Version: TLS 1.2 (0x0303) Length: 128 Encrypted Application Data: 173d1b0b2f280a13cc17815e54447bb9ac8af8a881a9eb84											

اهحالصإو ءاطخألا فاشكتسا

ةيفيكو نيوكتلا اذه عم اهتفداصم متت يتلا ةعئاشلا ءاطخألا ضعب مسقلا اذه فصي اهحالصإو ءاطخألا فاشكتساً.

ەذە أطخلا ةلاسر ةيۇر كنكمي ،ةقداصملا ريرقت يف

Authentication method is not supported by any applicable identity store

نأ نم دكأت .LDAP ةطساوب دمتعم ريغ هترتخإ يذلا بولسألاا نأ ىلإ هذه أطخلا ةلاسر ريشت EAP-TLS وأ EAP-GTC) ةموعدملا قرطلا ىدحإ حضوي ريرقتلا سفن يف ةقداصملا لوكوتورب وأ PEAP-TLS).

أطخ ثودح عم مداخلاب طبرلا رابتخإ ىەتنا.

مداخ ةداەش ةحص نم ققحتال لشف ىلإ عئاش لكشب كلذ يف ببسلا عجري to ليغشت تقو ةثالث all the تنكمو ISE ىلع طاقتال طبر تذخأ ،رادصإ عون اذه تيرحت وانوكمو prrt-jni تانوكمو الا تشعنا ،ءاطخالا حيحصت ىوتسم ىلع prrt-jni تانوكمو .دربم

ذفنملا مداخ ضورعو ةئيس ةداهش لوح ةمزحلا طاقتلا وكشي

مسا يأ وأ) ةداهشلاا عوضوم مساب LDAP ةحفص يف فيضملا مسا نيوكت بجي :ةظحالم ةكبش وأ عوضوملا يف اذه لثم كيدل نكي مل ام كلذل .(عوضوملل ليدبلاا مسالا نم ةكبش ةمئاق يف IP ناونعب صيخرت كمزليف ،لمعي الف ،(SAN) نيزختلا ةقطنم قلينم.(SAN) نيزختلا ةقطنم

3. اذه .ةيوهلا نزخم يف عوضوملا ىلع روثعلا مدع ةظحالم كنكمي ،ةقداصملا ريرقت يف ةدعاق يف مدختسم يأل عوضوملا مسا ةمس قباطي ال ريرقتلا نم مدختسملا مسا نأ ينعي امم ،ةمسلا هذهل SAMAccountName ىل قميقلا نييعت مت ،ويرانيسلا اذه يف LDAP تانايب ىلع روثعلا لواحي امدنع LDAP مدختسمل sAMAccountName ميق ىلإ رظني ISE نأ ينعي قباطت

4. ببسلا .مداخلاب طبر رابتخإ ءانثأ حيحص لكشب تاعومجملاو عيضاوملا دادرتسإ رذعت ديدحت بجي هنأ ركذت .ثحبلا دعاوقل حيحص ريغ نيوكت وه ةلكشملا هذهل الامتحإ رثكألا تاملك نم نوكتي نأ نكمي) dc و رذجلا ىلإ ةيفرطلا ةدحولا نم LDAP ل يلكيهلا لسلستلا (قددعتم.

ةلص تاذ تامولعم

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

ةمجرتاا مذه لوح

تمجرت Cisco تايان تايانق تال نم قعومجم مادختساب دنتسمل اذه Cisco تمجرت ملاعل العامي عيمج يف نيم دختسمل لمعد يوتحم ميدقت لقيرشبل و امك ققيقد نوكت نل قيل قمجرت لضفاً نأ قظعالم يجرُي .قصاخل امهتغلب Cisco ياخت .فرتحم مجرتم اممدقي يتل القيفارت عال قمجرت اعم ل احل اوه يل إ أم اد عوجرل اب يصوُتو تامجرت الاذة ققد نع اهتي لوئسم Systems الما يا إ أم الا عنه يل الان الانتيام الال الانتيال الانت الما