Configure and Troubleshoot ISE with External LDAPS Identity Store

Contents

Introduction **Prerequisites** Requirements **Components Used** Configure **Network Diagram** Configure LDAPS on Active Directory Install Identity Certificate on Domain Controller Access LDAPS Directory Structure Integrate ISE with LDAPS Server Configure the Switch Configure the Endpoint **Configure Policy Set on ISE** Verify Troubleshoot **Related Information**

Introduction

This document describes the integration of the Cisco ISE with the Secure LDAPS server as an External Identity Source.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Basic knowledge of Identity Service Engine (ISE) administration
- Basic knowledge of Active Directory/Secure Lightweight Directory Access Protocol (LDAPS)

Components Used

The information in this document is based on these software and hardware versions:

- Cisco ISE 2.6 Patch 7
- Microsoft Windows version 2012 R2 with Active Directory Lightweight Directory Services installed
- Windows 10 OS PC with native supplicant and user certificate installed
- Cisco Switch C3750X with 152-2.E6 image

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Background Information

LDAPS allows for the encryption of LDAP data (which includes user credentials) in transit when a directory bind is established. LDAPS uses TCP port 636.

These authentication protocols are supported with LDAPS:

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

Note: EAP-MSCHAPV2 (as an inner method of PEAP, EAP-FAST or EAP-TTLS), LEAP, CHAP, and EAP-MD5 are not supported with LDAPS External Identity Source.

Configure

This section describes the configuration of the network devices and integration of the ISE with Microsoft Active Directory (AD) LDAPS server.

Network Diagram

In this configuration example, the endpoint uses an Ethernet connection with a switch to connect with the Local Area Network (LAN). The connected switchport is configured for 802.1x authentication to authenticate the users with ISE. On the ISE, LDAPS is configured as an external identity store.

This image illustrates the network topology that is used:



Configure LDAPS on Active Directory

Install Identity Certificate on Domain Controller

In order to enable LDAPS, Install a certificate on Domain Controller (DC) that meets these requirements:

- 1. The LDAPS certificate is located in the Domain Controller's Personal Certificate Store.
- 2. A private key that matches the certificate is present in the Domain Controller's store and is correctly associated with the certificate.
- 3. The Enhanced Key Usage extension includes Server Authentication (1.3.6.1.5.5.7.3.1) object identifier (also known as OID).
- 4. The Fully Qualified Domain Name (FQDN) of the Domain Controller (for example, DC1.testlab.com) must be present in one of these attributes: The Common Name (CN) in the Subject field and DNS entry in the Subject Alternative Name Extension.
- 5. The certificate must be issued by a Certificate Authority(CA) that the Domain Controller and the LDAPS clients trust. For a trusted secure communication, the client and the server must trust each other's root CA and the intermediate CA certificates which issued certificates to them.

6. The Schanne	l cryptographic ser	vice provider (CSP) must be used to	generate the key.
----------------	---------------------	--------------------	-------------------	-------------------

R	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	
D Public key	RSA (2048 Bits)	
Certifica	DomainController	
Enhance	Client Authentication (1.3.6.1.5.5.7.3.2), Server Auth	~
<	III >	
<u> </u>		
Other Name:		
DS Object O	Guid=04 10 a6 36 1d 3c f4 3f a8 47 83 d7 d3 d5 46 20 a3	3f
DNS Name=DC	1.testlab.com	

Access LDAPS Directory Structure

In order to access the LDAPS Directory on the Active Directory server, make use of any LDAP browser. In this LAB, Softerra LDAP Browser 4.5 is used.

1. Establish a connection to the domain on TCP port 636.

Scope Pane		Name A	Value	Type	
Softerra LDAP Browser	~	Tinternet Public Servers	Not Expanded	Group	
Internet Public Servers		estab	ldaps://dc1.testlab.com:636/DC=testlab,DC=com	Server Profile	
R- I testab		-			

2. For simplicity, Create an Organizational Unit (OU) named ISE OU in the AD, and it must have a Group named UserGroup. Create two users (user1 and user2) and make them members of the group UserGroup.

Note: LDAP Identity Source on ISE is used only for User authentication.

Scope Pane 🔷 👻 🗙	Name 🔺	Value	Type
Softerra LDAP Browser	CN	UserGroup	Entry
Internet Public Servers	CN	user2	Entry
E- dtestab	CN	user1	Entry
CN=Builtin	CN	DESKTOP-19	Entry
B-□ CN=Computers	CN	ComputerGroup	Entry
B- Domain Controllers	distinguishedName	OU=ISE OU,DC=testlab,DC=com	Attribut
CN=ForeignSecurityPrincipals	dSCorePropagationData	1/1/1601	Attribut
B- 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=DESKTOP-19	objectCategory	CN=Organizational-Unit, CN=Schema, CN=Configuration, DC=	Attribut
CN=user1	objectClass	organizationalUnit	Attribut
CN=UserGroup	objectClass	top	Attribut
	= ou	ISE OU	Attribut
B-CN=LostAndFound	uSNChanged	607428	Attribut
CN=Managed Service Accounts	uSNCreated	603085	Attribut
E CN=NTDS Quotas	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

Integrate ISE with LDAPS Server

1. Import the LDAP Server Root CA certificate in the Trusted Certificate.

cisco Identity Services Engine	Home	Policy - Administratio	on Work Centers			
System Identity Management N	Network Resources	pxGrid Services Feed	Service + Threat Cent	ic NAC		
Deployment Licensing - Certificates	Logging Maintenance Upgrade Back	µp & Restore → Admin A	ccess + Settings			
0	· · · · · · · · · · · · · · · · · · ·					
-	Friendly Name	 Status 	Trusted For	Serial Number	Issued To	Issued B
- Certificate Management	DC1	•				
System Certificates	DC1-CA	Enabled	Infrastructure Cisco Services	18 29 1C A7 00 13	testlab-DC1-CA-1	testlab-D
Trusted Certificates			Endpoints			

2. Validate the ISE admin certificate and ensure that the ISE admin certificate issuer certificate is also present in the Trusted Certificate Store.

3. In order to integrate the LDAPS server, make use of the different LDAP attributes from the LDAPS directory. Navigate to Administration > Identity Management > External Identity Sources > LDAP Identity Sources > Add.

System * identify Management * Network Resources * Device Portal Management pxGrid Services * Feed Service * Threat Centric NAC identifies Groups External Identify Sources Identify Source Sequences * Settings Conflictede Authentication Profile Subject Objecticas person * Subject Objecticas person * Subject Objecticas person * Subject Objecticas person * Subject Objects Contain Reference To Groups Subject In Broups Are Stored In Member Attribute As User Info Attributes Subject In Groups Are Stored In Member Attribute As User Info Attributes Subject In Groups Are Stored In Member Attribute As User Info Attributes Subject Informer Job Title Title Title State or Province it TitlephoneNumber Country co Street Address Street Addres Street Address Street Address Street Address S	diada cisco	Identity Service	es Engine	Home	Context Visibility	Operation	ts → Policy	- Administration	Work Centers		
Identities Groups External Identity Sources Identity Sources Quences > Settings Identities Groups External Identity Sources Identity Sources List > testabe Lideps Image: Contract Authentication Profile Image: Connection Directory Organization Groups Attributes Advanced Setting testabe Conception Image: Contract Authentication Profile Image: Connection Directory Organization Group Attributes Advanced Setting testabe Conception Image: Contract Authentication Profile Image: Connection Directory Organization Group Attributes Conception Image: Contract Contract Authentication Profile Image: Connection Directory Organization Group Attribute Image: Contract Cont	 System 	tem 👻 Identity N	Nanagement	 Network R 	esources + Device	Portal Manage	ment pxGrid Ser	vices + Feed Se	rvice + Threat Centr	ric NAC	
External Identity Sources EAP Identity Sources List > testabs_ldaps Cardinata Authentication Profile Active Directory Istabs ODP Stability Idensi ODP Stability Idensi ODP Stability Idensi Group Dipetity Idensi Group Idensi Idensi Stability Idensi Stability Idensi Country company Stability Idensi Country company Street Address Street Address Street Address Street Address 	Ider	ntities Groups	External Ide	ntity Sources	Identity Source Seq	uences + Se	ttings				
SAML id Providers Social Login Subject Name Attribute <u>sAMAccountName</u> * Group Map Attribute <u>memberOf</u> Group Name Attribute <u>dn</u> Certificate Attribute <u>userCertificate</u> Subject Objects Contain Reference To Groups Group Objects Contain Reference To Subjects Subject In Groups Are Stored In Member Attribute As <u>Distinguished Name</u> User Info Attributes IFirst Name givenName Department department Last Name <u>sn</u> Organizational Unit <u>company</u> Job Title <u>title</u> Locality <u>I</u> Email <u>mail</u> State or Province <u>st</u> Telephone telephoneNumber <u>County</u> <u>co</u>	Ext 🖓	Certificate Auth Certificate Auth Active Directory testlab LDAP DBC RADIUS Token RSA SecuriD	entication Profil	ie Ie	LDAP Identity So LDAP Identit General	vrces List > tes y Source Conne Name [Description [✓ Schema [tlab_ldaps ection Dir testlab_ldaps Custom	rectory Organization	Groups	Attributes	Advanced Settings
 Group Name Attribute dn Group Objects Contain Reference To Groups Group Objects Contain Reference To Subjects Subject In Groups Are Stored In Member Attribute As Distinguished Name * User Info Attribute First Name givenName Department department Last Name sn Organizational Unit company Job Title title Locality 1 Email mail State or Province st Teiephone telephoneNumber Country co 		SAML Id Provid	ers		* Subject I	Name Attribute	sAMAccountName	e	* Group Map Attribute	memberOf	
 Subject Objects Contain Reference To Groups Group Objects Contain Reference To Subjects Subjects In Groups Are Stored In Member Attribute As Distinguished Name : User Info Attributes () First Name givenName Department department Last Name sn Organizational Unit company Job Title title Locality I Email mail State or Province st Telephone telephoneNumber Country co Street Address streetAddress 					* Group N	ame Attribute	dn		Certificate Attribute	userCertificate	
User Info Attributes First Name givenName Department department Last Name sn Organizational Unit company Job Title title Locality I .					 Subject Group 	t Objects Conta Objects Contai	in Reference To Gr n Reference To Sub Subjects In	roups bjects Groups Are Stored	In Member Attribute As	Distinguished Name	Ţ
First Name givenName Department department Last Name sn Organizational Unit company Job Title title Locality I Email mail State or Province st Telephone telephoneNumber Country co Street Address streetAddress streetAddress					User Info	Attributes (j)					
Last Name sn Organizational Unit company Job Title title Locality I Email mail State or Province st Telephone telephoneNumber Country co Street Address streetAddress streetAddress						First Name	givenName		Department	department	
Job Title title Locality I Email mail State or Province st Telephone telephoneNumber Country co Street Address streetAddress						Last Name	sn		Organizational Unit	company	
Email mail State or Province st Telephone telephoneNumber Country co Street Address streetAddress						Job Title	title		Locality	1	
Telephone telephoneNumber Country co Street Address streetAddress						Email	mail		State or Province	st	
Street Address streetAddress						Telephone	telephoneNumber	r	Country	0	
						Street Address	streetAddress				
Save Reset					Save Dece						

4. Configure these attributes from the General Tab:

Subject Objectclass: This field corresponds to the Object class of user accounts. You can use one of the four classes here:

- Top
- Person
- OrganizationalPerson
- InetOrgPerson

Scope Pane 👻 🗙	objectclass	Filter Value	
Scope Pane Softerra LDAP Browser testlab CN=Builtin CN=Computers CN=Computers CN=ForeignSecurityPrincipals CN=Infrastructure CN=Infrastructure CN=Infrastructure CN=Infrastructure CN=Infrastructure CN=Infrastructure CN=Infrastructure CN=Infrastructure CN=Infrastructure CN=Infrastructure CN=Infrastructure CN=ISE Group CN=DESKTOP-19 CN=user1	objectclass Name = objectClass = objectClass = objectClass = objectClass	Filter Value Value user organizationalPerson person top	Type Attribute Attribute Attribute
CN=user2 CN=UserGroup			

Subject Name Attribute: This field is the name of the attribute containing the username from the request. This attribute is retrieved from the LDAPS when the ISE inquires a specific user name in the LDAP database (you can use cn, sAMAccountName, etc). In this scenario, user1 username on the endpoint is used.

Scope Pane 🔫	• ×	Filter Name	user1		
Softerra LDAP Browser		Name	Value		Туре
H- CN=Builtin		🗉 cn	user1		Attribute
CN=Computers		displayName	user1		Attribute
OU=Domain Controllers		distinguishedName	CN=user1,OU=ISE OU,DC=testlab,DC=cor	m	Attribute
E- CN=ForeignSecurityPrincipals		givenName	user1		Attribute
CN=Infrastructure		E name	user1		Attribute
OU=ISE Group		sAMAccountName	user1		Attribute
E- DU=ISE OU		💷 userPrincipalName	user1@testlab.com		Attribute
CN=ComputerGroup		💷 userCertificate	user1		Binary Attribute
CN=DESKTOP-19					
CN=user2					
CN=UserGroup		1			

Group Name Attribute: This is the attribute holding the name of a group. The Group name attribute values in your LDAP directory must match LDAP group names on the User groups page

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

Group Objectclass: This value is used in searches to specify the objects that are recognized as groups.

CN=ComputerGroup CN=DESKTOP-19	 objectSid objectGUID objectClass 	S-1-5-21-29602840 {39967F90-898E-4 top	Binary Attribute Binary Attribute Attribute	
CN=User1 CN=User2 CN=UserGroup	objectClass objectCategory	group CN=Group,CN=Sch	nema,CN=Configuration,DC=testlab,DC=com	Attribute Attribute

Group Map Attribute: This attribute defines how the users are mapped to the groups.

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			
CN=ForeignSecurityPrincipals CN=Infrastructure			
OU=ISE Group			
- OU=ISE OU			
E-CN=ComputerGroup			
CN=DESKTOP-19			

Certificate Attribute: Enter the attribute that contains the certificate definitions. These definitions can optionally be used to validate certificates that are presented by clients when they are defined as part of a certificate authentication profile. In such cases, a binary comparison is performed between the client certificate and the certificate retrieved from the LDAP identity source.

1 - 2 - 5 - 5 - 5 - 5 - 5 - 5 - 5 - 5 - 5			
⊟- OU=ISE OU	userPrincipalName	user1@testlab.com	Attribute
E- CN=ComputerGroup	userCertificate	user1	Binary Attribute
CN=DESKTOP-19			

5. In order to configure the LDAPS connection, navigate to the Connection tab :

General Connect	tion Directory Organization	Groups	Attributes Ar	dvanced Setting	5		
	Primary Server				Secon	dary Server	
					🗌 Ena	able Secondary Serve	r
* Hostname/IP	dc1.testlab.com			Hostname/IP			
* Port	636			Port	389		
Specify server for each ISE	node						
Ad	ccess O Anonymous Access			A	ccess	Anonymous Acces	55
	 Authenticated Access 	_				 Authenticated Acc 	ess
Admi	n DN * CN=poongarg,CN=Users,DC=test			Adm	in DN		
Pass	word	_		Pas	sword		
Secure Authentic	ation I Enable Secure Authentication		s	Secure Authentic	cation	Enable Secure Aut	hentication
	Enable Server Identity Check					Enable Server Ider	ntity Check
LDAP Server Roo	ot CA DC1-CA	<i>x</i>	L	DAP Server Ro	ot CA	DST Root CA X3 Cert	ificate Ai 🎽
Issuer CA of ISE Certific	cates DC1-CA	D	Issuer C	CA of ISE Certifi	cates	Select if required (op	tional) 🔻
* Server Timeout	10 () Secon	ds	Se	rver Timeout	.0		() Second
* Max. Admin Connections	20		Max. Admin	Connections 2	20		Ð
	Force reconnect every	15			Force	reconnect every	 Minutes
	Test Bind to Server				Test Bind	d to Server	
Failover	Always Access Primary Server First						
	Failback To Primary Server After 5		Minutes				

6. Run dsquery on Domain controller to get the username DN to be used to make a connection to LDAP server:

PS C:\Users\Administrator> dsquery user -name poongarg

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

Step 1. Set the correct IP address or Hostname of the LDAP server, define the LDAPS port (TCP 636), and Admin DN to make a connection with the LDAP over SSL.

Step 2. Enable Secure Authentication and Server Identity Check option.

Step 3. From the drop-down menu, select the LDAP Server Root CA certificate and ISE admin certificate Isser CA certificate (We have used certificate authority, installed on the same LDAP server to issue the ISE admin certificate as well).

Step 4. Select the Test Bind to server. At this point, any subjects or groups are not retrieved because the search bases are not yet configured.

7. Under **Directory Organization** tab, configure the Subject/Group Search Base. It is the join point for the ISE to the LDAP. Now you are able to retrieve only subjects and groups that are children of the joining point. In this scenario, both the subject and group are retrieved from the OU=ISE OU

	LDAP Identity Sources List > to	estlab_Idaps			
	LDAP Identity Source				
	General Con	nection Directory Organization	Groups	Attributes	Advanced Settin
	* Subject Search Base O	U=ISE OU,DC=testlab,DC=com Naming O	Contexts		
	* Group Search Base 0	U=ISE OU,DC=testlab,DC=com Naming O	Contexts		
		[]			
	Search for MAC Address in	Format xx-xx-xx-xx-xx T			
	Strip start of subject	name up to the last occurrence of the separat	tor \		
	Strip end of subject	name from the first occurrence of the separato	or 👘		
1					

8. Under Groups, click Add to import the groups from the LDAP on the ISE and retrieve the groups, as shown in this image.

LDAP Identity Source	s List > testlab_idaps D UICE	i -		
General	Connection	Directory Organization	Groups	Attributes
✓ Edit + Add +	🗙 Delete Group			
Name				▲
CN=UserGrou	up,OU=ISE OU,DC=te	stlab,DC=com		

Configure the Switch

Configure the switch for 802.1x authentication. Windows PC is connected to switchport Gig2/0/47

```
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
!
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
!
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
```

Configure the Endpoint

Windows Native Supplicant is used and one of the LDAP supported EAP protocol is utilized, EAP-TLS for user authentication and authorization.

1. Ensure that PC is provisioned with user certificate (for user1) and have intended purpose as Client Authentication and in the Trusted Root Certification Authorities, the issuer certificate chain is present on the PC.



2. Enable Dot1x authentication and Select Authentication method as Microsoft:Smart Card or other certificate for EAP-TLS authentication.

pciPasst	hru0 Properties		×
Networking	Authentication	Sharing	
Select th this Ethe	is option to provid met adapter.	de authenticated netwo	k access for
🗹 Enabl	e IEEE 802.1X a	uthentication	
Choose	a network auther	tication method:	
Microso	ft: Smart Card or	other certificate \sim	Settings
Fallba	ack to unauthoriz	ed network access	
Additio	onal Settings	ed network access	

3. Click on Additional Settings, and a window opens. Check the box with specify authentication mode and choose user authentication, as shown in this image.

			_
Select this option to provide au this Ethernet adapter.	User authentication woo	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 lo	gon	
	O Perform immediately after user log	on	
Remember my credentials for time I'm logged on	Maximum delay (seconds):	10	*
Fallback to unauthorized ne	Allow additional dialogs to be displating sign on	ayed during sing	gle
Additional Settings	This network uses separate virtual and user authentication	LANs for machi	ine

Configure Policy Set on ISE

Since EAP-TLS protocol is used, before Policy Set is configured, Certificate Authentication Profile needs to be configured and the Identity Source Sequence is used in the Authentication policy later.

cisco Identity Services Engine Home	Context Visibility Operations	Policy Administration Work Centers
System Identity Management Network	Resources	pxGrid Services + Feed Service + Threat Centric NAC
Identities Groups External Identity Sources	Identity Source Sequences	
External Identity Sources	Certificate Authentication Profiles List > Certificate Authentication Prof	LDAPS_cert Tile
Certificate Authentication Profile Active Directory Settab	* Name	LDAPS_cert EAP.TI S certificate based authentication with LDAPS
DDAP ODBC RADIUS Token RSA SecuriD	Lascibiou	
SAML Id Providens	Identity Store	testiab_idaps 🝸 🕡
	Use Identity From	Certificate Attribute Subject - Common Name Subject or Alternative Name Attributes in the Certificate (for Active Directory Only) ()
	Match Client Certificate Against Certificate In Identity Store ()	Never
		Only to resolve identity ambiguity Always perform binary comparison
	Save	

Refer to the Certificate Authentication Profile in the Identity Source Sequence and define the LDAPS external identity source in the Authentication Search list:

▶ System • Identity Management • Network Resources • Device Portal Management pxGrid Services • Feed Service • Threat Centric NAC • Identities Groups External Identity Sources Identity Source Sequences • Settings • Identity Source Sequence • Name LDAPS Identity • Name LDAPS Identitication • Certificate Based Authentication Profile LDAPS_cert ▼	;
Identities Groups External Identity Sources Identity Source Sequence * Identity Source Sequence *Name LDAPS Description	
Identity Source Sequence * Name LDAPS Description Certificate Based Authentication Select Certificate Authentication Profile LDAPS_cert Select Certificate Authentication Profile LDAPS_cert Select Certificate Authentication Profile 	
✓ Identity Source Sequence * Name LDAPS Description ✓ Certificate Based Authentication ✓ Select Certificate Authentication Profile LDAPS_cert	
* Name LDAPS Description	
Description ✓ Certificate Based Authentication ✓ Select Certificate Authentication Profile LDAPS_cert	
 ✓ Certificate Based Authentication ✓ Select Certificate Authentication Profile LDAPS_cert 	
 ✓ Certificate Based Authentication ✓ Select Certificate Authentication Profile LDAPS_cert 	
Select Certificate Authentication Profile	
 Authentication Search List 	
A set of identity sources that will be accessed in sequence until first authentication succeeds	
Available Selected	
Internal Endpoints testlab_Idaps	
Internal Users Guest Users	
testlab All_AD_Join_Points	
rad	
Advanced Search List Settings If a selected identity store cannot be accessed for authentication	
Do not access other stores in the sequence and set the "AuthenticationStatus" attribute to "ProcessError"	
Ireat as if the user was not found and proceed to the next store in the sequence	
Save Reset	

Now configure policy set for Wired Dot1x authentication:

ahaha k	dentity Se	vices Engine Hor	me	ibility + Operation	s ▼Policy	Administration	Work Centers
Policy S	Sets Pro	filing Posture Client	Provisioning + Pol	cy Elements			
Policy	Sets →	Wired Dot1x					
	Status	Policy Set Name	Descrip	tion	Conditio	ns	
Search	0						
	0	Wired Dot1x			C V	Vired_802.1X	
❤ Aut	henticatio	n Policy (2)					
+	Status	Rule Name	Condi	lions			
Sean	ch						
	ø	Dot1x		Network Access-Netv	vorkDeviceNam	e EQUALS LAB-Switch	
	0	Default					

Y Auth	orization F	Policy (2)				
					Results	
+	Status	Rule Name	Cond	itions	Profiles	
Search	1					
	\odot	Users in LDAP Store	串	testlab_Idaps-ExternalGroups EQUALS CN=UserGroup,OU=ISE OU,DC=testlab,DC=com	× PermitAccess	+
	ø	Default			× DenyAccess	+

After this configuration, we can authenticate the Endpoint using EAP-TLS protocol against the LDAPS Identity source.

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

Verify

1. Check the authentication session on the switchport connected to PC:

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)
Service religious	e. permoel_eximple_react_shoep_secone (prioricy 190)
Server Policies:	
Method status list:	
Method	State
dot1x	Authc Success

2. In order to verify the LDAPS and ISE configurations, you are able to retrieve the subjects and groups with a test connection to the server:

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		 Authenticated Access 	
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. Verify the user authentication report:

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

4. Check the detailed authentication report for the endpoint:

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 0A6A26390000130C98CE6088									
Audit Session Id										
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_Idaps
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	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. Validate the data is encrypted between the ISE and LDAPS server by taking packet capture on the ISE towards the LDAPS server:

No. Time A Source Destination Protocol Length Address 64 28 2828-66-24 164:824.264:331 16:197.164.21 TCF 74 488:62:97:86:123.8.0.1 22 2828-66-24 16:42:24.266:31 16:197.164.21 TCF 74 488:62:97:88:12:28.0. 23 2828-66-24 16:42:24.266:61 16:197.164.22 10:197.164.22 TCF 74 488:62:97:88:12:28.0. 24 2828-66-24 16:42:24.21:28:61 10:197.164.22 10:197.164.22 10:197.164.22 10:197.164.22 10:197.164.22 10:197.164.22 10:197.164.22 10:197.164.22 10:197.164.21 10:197.16																		
20 2020-06-24 10:40:24.20550 10:197.164.22 10:197.164.21 TCP 74 00:50:29:99:co:28.0. 22 2020-06-24 10:40:24.20550 10:197.164.22 10:197.164.21 TCP 74 00:50:29:99:co:28.0. 23 2020-06-24 10:40:24.20561 10:197.164.22 10:197.164.21 TLSV1.2 207 00:70:29:99:co:28.0. 24 2020-06-24 10:40:24.20561 10:197.164.22 10:197.164.21 TLSV1.2 203 00:80:29:99:co:28.0. 25 2020-06-24 10:40:24.21561 10:197.164.22 10:197.164.21 TLSV1.2 203 00:80:29:99:co:28.0. 26 2020-06-24 10:40:24.21561 10:197.164.22 10:197.164.21 TLSV1.2 203 00:80:29:99:co:28.0. 27 2020-06-24 10:40:24.21561 10:197.164.22 10:197.164.22 TLSV1.2 175 00:80:56:00:30:77.0. 28 2020-06-24 10:40:24.21561 10:197.164.22 10:197.164.22 TLSV1.2 173 00:59:56:00:30:77.0. 28 2020-06-24 10:40:24.21561 10:197.164.22 10:197.164.22 TLSV1.2 197 00:80:56:00:30:77.0. 28 2020-06-24 10:40:24.21561 10:197.164.22 10:197.164.22 TLSV1.2 197 00:80:56:00:30:77.0. 28 2020-06-24 10:40:24.21551 10:197.164.22 10:197.164.22 TLSV1.2 197 00:80:56:00:30:77.0. 30 2020-06-24 10:40:24.21551 10:197.164.22 10:197.164.22 TLSV1.2 179 00:80:56:00:30:77.0. 31 2020-06-24 10:40:24.21551 10:197.164.22 10:197.164.21 TLSV1.2 205 00:00:00:30:30:77.0. 32 2020-06-24 10:40:24.21551 10:197.164.22 10:197.164.21 TLSV1.2 205 00:00:00:30:377.0. 33 2020-06-24 10:40:24.21551 10:197.164.22 10:197.164.21 TLSV1.2 205 00:00:00:30:377.0. 35 2020-06-24 10:40:24.21551 10:197.164.22 10:197.164.21 TLSV1.2 205 00:00:00:39:70:02.8.0. 36 2020-06-24 10:40:24.21552 10:197.164.21 TLSV1.2 205 00:00:00:30:77.0. 37 2020-06-24 10:40:57.946551 10:197.164.22 10:197.164.21 TLSV1.2 155 00:00:00:29:99:co:28.0. 38 2020-06-24 10:40:57.946551 10:197.164.22 10:197.164.21 TLSV1.2 155 00:00:00:29:99:co:28.0. 39 Franz 30:0 (crtor 10:40:57.946551 10:197.164.22 10:197.164.21 TLSV1.2 155 00:00:00:29:99:co:28.0. 30 Franz 30:0 (crtor 10:40:57.946551 10:197.164.22 10:197.164.21 TLSV1.2 157 00:00:00:29:99:co:28.0. 30 TC 209:00-024 10:40:57.946551 10:197.164.22 10:197.164.21 TLSV1.2 157 00:00:00:00:29:99:co:28.0. 30 Franz 30:0 (crtor 10:30] Seq0					Time						Source		Destination	Protocol	Length	Address	64bits	Info
21 2020-06-24 10:402:24, 2025:05 10:197.164:21 110:197.164:22 10:197.164:21 22 2020-06-24 10:402:24, 2025:06 10:197.164:21 10:197.164:21 1155:12 207 00:40:22:98:ca:28,0. 24 2020-06-24 10:402:24, 2025:06 10:197.164:21 10:197.164:21 1155:12 207 00:40:22:98:ca:28,0. 25 2020-06-24 10:402:24, 215:11 10:197.164:21 10:197.164:21 1155:12 208 00:40:22:98:ca:28,0. 26 2020-06-24 10:40:24, 215:11 10:197.164:21 1155:12 208 00:40:22:98:ca:28,0. 27 2020-06-24 10:40:24, 215:11 10:197.164:21 1155:12 208 00:40:22:98:ca:28,0. 28 2020-06-24 10:40:24, 215:18 10:197.164:21 1155:12 219 00:40:22:98:ca:28,0. 31 2020-06-24 10:40:24, 215:48 10:197.164:21 1155:12 219 00:40:25:98:ca:28,0. 32 2020-06-24 10:40:24, 215:48 10:197.164:21 1155:12 159 00:40:22:98:ca:28,0. 34 2020-06-24 10:40:25:25:48:0:37 10:197.164:21 1155:12				20	2020-06-2	4 1	10:40	:24.2	205431		10.197.164.22	5	10.197.164.21	TCP	74	00:0c:29:98:ca:28,0	5	28057 - 636 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 S
<pre>22 2020-06-24 10:40:24,206613 10:197.164.22 10:197.164.21 TCP 66 00:0c:20:98:co:28.0. 23 2020-06-24 10:40:24,210413 10:197.164.22 10:197.164.21 TLSV1.2 2050 00:0c:20:98:co:28.0. 25 2020-06-24 10:40:24,210508 10:197.164.22 10:197.164.21 TLSV1.2 2050 00:0c:20:98:co:28.0. 26 2020-06-24 10:40:24,210578 10:197.164.22 10:197.164.21 TLSV1.2 2050 00:0c:20:98:co:28.0. 27 2020-06-24 10:40:24,210578 10:197.164.22 10:197.164.21 TLSV1.2 173 00:0c:98:0c:28.0. 28 2020-06-24 10:40:24,210578 10:197.164.21 10:197.164.22 TLSV1.2 173 00:0c:98:0c:28.0. 29 2020-06-24 10:40:24,230834 10:197.164.21 10:197.164.21 TLSV1.2 157 00:0c:98:0c:28.0. 30 2020-06-24 10:40:24,23889 10:197.164.21 10:197.164.22 TLSV1.2 157 00:0c:98:0c:28.0. 31 2020-06-24 10:40:24.23889 10:197.164.21 10:197.164.22 TLSV1.2 1879 00:0c:99:59:0c:28.0. 32 2020-06-24 10:40:24.23889 10:197.164.21 10:197.164.21 TLSV1.2 279 00:0c:29:98:co:28.0. 34 2020-06-24 10:40:24.23889 10:197.164.21 10:197.164.21 TLSV1.2 253 00:0c:98:56:a0:30:7f.0. 35 2020-06-24 10:40:24.23889 10:197.164.22 10:197.164.21 TLSV1.2 255 00:05:05:30:30:7f.0. 36 2020-06-24 10:40:24.23889 10:197.164.22 10:197.164.21 TLSV1.2 255 00:05:05:30:30:7f.0. 36 2020-06-24 10:40:24.23889 10:197.164.22 10:197.164.21 TLSV1.2 255 00:05:05:30:30:7f.0. 36 2020-06-24 10:40:24.239332 10:197.164.22 10:197.164.21 TLSV1.2 255 00:05:05:30:30:7f.0. 36 2020-06-24 10:40:24.239332 10:197.164.22 10:197.164.21 TLSV1.2 255 00:05:05:30:30:co:28.0. 87 2020-06-24 10:40:24.239332 10:197.164.22 10:197.164.21 TLSV1.2 151 00:0c:239:80:co:28.0. 87 2020-06-24 10:40:257.997:050 10:197.164.22 10:197.164.21 TLSV1.2 151 00:0c:239:80:co:28.0. 87 2020-06-24 10:40:257.997:050 10:197.164.22 10:197.164.21 TCP 66 00:0c:239:80:co:28.0. 87 2020-06-24 10:40:257.997:050 10:197.164.22 10:197.164.21 TCP 66 00:0c:239:80:co:28.0. 87 2020-06-24 10:40:257.997:050 10:197.164.22 10:197.164.21 TCP 66 00:0c:239:80:co:28.0. 87 Ethernet TL, Src: Ymae,a90:3c:rf (00:05:55:a0:30:rf), 00:tvs:230:00:00:00:00:00:00:00:00:00:00:00:00:0</pre>			1	21	2828-86-2	4 1	10:40	:24.7	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
<pre>23 2020-06-24 10:40:24,206961 10:197.164.22 10:197.164.21 TL5V1.2 207 00:00:02:298:cc:28.0. 24 2020-06-24 10:40:24,216508 10:197.164.21 10:197.164.21 TL5V1.2 208 00:00:02:298:cc:28.0. 25 2020-06-24 10:40:24,215211 10:197.164.22 10:197.164.21 TL5V1.2 208 00:00:02:298:cc:28.0. 26 2020-06-24 10:40:24,215211 10:197.164.22 10:197.164.21 TL5V1.2 109 00:00:02:98:cc:28.0. 29 2020-06-24 10:40:24,21511 10:197.164.21 10:197.164.21 TL5V1.2 109 00:00:02:98:cc:28.0. 29 2020-06-24 10:40:24,21511 10:197.164.21 10:197.164.21 TL5V1.2 1159 00:00:02:98:cc:28.0. 31 2020-06-24 10:40:24,23558 10:197.164.21 10:197.164.22 TL5V1.2 179 00:00:02:98:cc:28.0. 33 2020-06-24 10:40:24,23558 10:197.164.21 10:197.164.21 TL5V1.2 179 00:00:02:98:cc:28.0. 33 2020-06-24 10:40:24,23558 10:197.164.21 10:197.164.21 TL5V1.2 253 00:00:02:98:cc:28.0. 33 2020-06-24 10:40:24,23558 10:197.164.21 10:197.164.21 TL5V1.2 253 00:00:02:98:cc:28.0. 34 2020-06-24 10:40:24,23558 10:197.164.21 10:197.164.21 TL5V1.2 253 00:00:02:98:cc:28.0. 35 2020-06-24 10:40:24,23558 10:197.164.21 10:197.164.21 TL5V1.2 253 00:00:02:98:cc:28.0. 36 2020-06-24 10:40:24,23558 10:197.164.21 10:197.164.21 TL5V1.2 253 00:00:02:98:cc:28.0. 36 2020-06-24 10:40:24,23558 10:197.164.22 10:197.164.21 TL5V1.2 253 00:00:02:98:cc:28.0. 36 2020-06-24 10:40:24,23558 10:197.164.22 10:197.164.21 TL5V1.2 253 00:00:02:98:cc:28.0. 36 2020-06-24 10:40:24,23558 10:197.164.22 10:197.164.21 TL5V1.2 253 00:00:02:98:cc:28.0. 37 2020-06-24 10:40:24,23558 10:197.164.22 10:197.164.21 TL5V1.2 150 00:00:02:98:cc:28.0. 38 2020-06-24 10:40:24,23558 10:197.164.22 10:197.164.21 TL5V1.2 150 00:00:02:98:cc:28.0. 37 2020-06-24 10:40:57.49553 10:197.164.22 10:197.164.21 TL5V1.2 150 00:00:02:98:cc:28.0. 38 2020-06-24 10:40:57.49553 10:197.164.22 10:197.164.21 TL5V1.2 150 00:00:02:98:cc:28.0. 39 Fame 28:199 bytes on vire (1592 bits), 199 bytes captured (1592 bits) 50 Ethernet 11, 57c: Vmare.00:3c:13152 10:107.164.22 10:177.164.21 TL5V1.2 150 00:00:02:98:cc:28.0. 50 Ethernet 133 Sequence number: 2076 (relative sequence num</pre>				22	2828-86-2	4 1	10:40	:24.2	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
<pre>24 2028-06-24 10:40:224.218413 10:197.164.21 10:197.164.22 TCPL 2010 00:50:2998:ca:28.0. 25 2028-06-24 10:40:24.215211 10:197.164.22 10:197.164.21 TCPL 2000 00:50:2998:ca:28.0. 27 2028-06-24 10:40:24.218678 10:197.164.21 10:197.164.21 TLSVL.2 173 00:50:556:a0:267.0. 28 2028-06-24 10:40:24.218678 10:197.164.21 10:197.164.21 TLSVL.2 173 00:50:556:a0:26.0. 29 2028-06-24 10:40:24.218878 10:197.164.21 10:197.164.21 TLSVL.2 199 00:50:556:a0:28.0. 29 2028-06-24 10:40:24.218889 10:197.164.21 10:197.164.21 TLSVL.2 199 00:50:556:a0:30:77.0. 30 2028-06-24 10:40:24.218889 10:197.164.21 10:197.164.21 TLSVL.2 179 00:50:556:a0:30:77.0. 31 2028-06-24 10:40:24.218889 10:197.164.22 10.197.164.21 TLSVL.2 1879 00:50:556:a0:30:77.0. 32 2028-06-24 10:40:24.23889 10:197.164.22 10.197.164.21 TCPL 2010 00:50:556:a0:30:77.0. 33 2028-06-24 10:40:24.238589 10:197.164.22 10.197.164.21 TCPL 2010 00:50:556:a0:30:77.0. 34 2028-06-24 10:40:24.239322 10:197.164.22 10:197.164.21 TCPL 2010 00:50:556:a0:30:77.0. 35 2028-06-24 10:40:27.945553 10:197.164.22 10:197.164.21 TCPL 2010 00:50:556:a0:30:77.0. 36 2028-06-24 10:40:57.946553 10:197.164.22 10:197.164.21 TCPL 2010 00:50:29:98:ca:28.0. 35 2028-06-24 10:40:57.946553 10:197.164.22 10:197.164.21 TCPL 2010 00:50:29:98:ca:28.0. 36 2028-06-24 10:40:57.946553 10:197.164.22 10:197.164.21 TCPL 2010 00:50:29:98:ca:28.0. 36 2028-06-24 10:40:57.946553 10:197.164.22 10:197.164.21 TCPL 2010 00:50:29:98:ca:28.0. 36 2028-06-24 10:40:57.94655 10:197.164.22 10:197.164.21 TCPL 2010 00:50:29:98:ca:28.0. 37 Constant and and and and and and and and and and</pre>			1	23	2020-06-2	4 1	10:40	:24.2	206961		10.197.164.22		10.197.164.21	TLSv1.2	207	00:0c:29:98:ca:28,0		Client Hello
<pre>25 2028-06-24 10:40:24.218568 10:197.164.22 10:197.164.21 TCP 66 00:60:29:98:ca:28, 0. 26 2028-06-24 10:40:24.218678 10:197.164.22 10:197.164.22 TLSV1.2 173 00:50:56:a0:39:7f, 0. 28 2028-06-24 10:40:24.219113 10:197.164.22 10:197.164.22 TLSV1.2 199 00:00:2998:ca:28, 0. 30 2028-06-24 10:40:24.2131712 10:197.164.21 10:197.164.22 TLSV1.2 199 00:00:2998:ca:28, 0. 31 2028-06-24 10:40:24.213098 10:197.164.21 10:197.164.22 TLSV1.2 199 00:00:2998:ca:28, 0. 32 2028-06-24 10:40:24.213098 10:197.164.21 10:197.164.22 TLSV1.2 199 00:00:2998:ca:28, 0. 33 2028-06-24 10:40:24.213098 10:197.164.21 10:197.164.22 TLSV1.2 299 00:50:56:a0:30:7f, 0. 33 2028-06-24 10:40:24.213098 10:197.164.21 10:197.164.21 TLSV1.2 295 00:55:6:a0:30:7f, 0. 33 2028-06-24 10:40:24.233052 10:197.164.22 10:197.164.21 TLSV1.2 295 00:50:56:a0:30:7f, 0. 34 2028-06-24 10:40:24.233052 10:197.164.22 10:197.164.21 TLSV1.2 295 00:50:56:a0:30:7f, 0. 35 2028-06-24 10:40:24.233052 10:197.164.22 10:197.164.21 TLSV1.2 295 00:50:298:ca:28, 0. 86 2028-06-24 10:40:24.233052 10:197.164.22 10:197.164.21 TLSV1.2 295 00:50:298:ca:28, 0. 87 2028-06-24 10:40:24.233052 10:197.164.22 10:197.164.21 TLSV1.2 151 00:00:2998:ca:28, 0. 87 2028-06-24 10:40:24.233052 10:197.164.22 10:197.164.21 TLSV1.2 151 00:00:2998:ca:28, 0. 87 2028-06-24 10:40:24.233052 10:197.164.22 10:197.164.21 TLSV1.2 151 00:00:2998:ca:28, 0. 87 2028-06-24 10:40:24.233052 10:197.164.22 10:197.164.21 TLSV1.2 151 00:00:2998:ca:28, 0. 87 2028-06-24 10:40:24.23052 10:197.164.22 10:197.164.21 TLSV1.2 177 66 00:00:29998:ca:28, 0. 87 2028-06-24 10:40:24.200 Stort 0.150 Stort 10:197.164.21 TLSV1.2 151 00:00:2998:ca:28, 0. 87 2028-06-24 10:40:24.200 Stort 0.157 20057, Dst Port: 636, Seg: 336, Ack: 2078, Len: 133 Source Port: 20057 Segment Len: 133] Sequence number: 409 (relative sequence number) Next sequence number: 306 (relative sequence number) Acknowledgement number: 409 (relative sequence number) Acknowledgement number: 208 (Set 10:197.164.22 Set 10:197.164.21 TLSV1.2 RCSOT 10:1000 Size 2098 Checksum Stavz: Sup</pre>			1	24	2020-06-2	4 1	10:40	:24.2	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 duri
<pre>26 2020-06-24 10:40:24.215211 10.197.164.22 10.197.164.21 TLSV1.2 260 00:6c:29:98:ca:28,0. 27 2020-06-24 10:40:24.218678 10.197.164.21 10.197.164.21 TLSV1.2 173 00:50:56:a0:3e:7f,0. 28 2020-06-24 10:40:24.21913 10.197.164.22 10.197.164.21 TLSV1.2 199 00:6c:29:98:ca:28,0. 29 2020-06-24 10:40:24.21913 10.197.164.21 10.197.164.21 TLSV1.2 199 00:6c:29:98:ca:28,0. 31 2020-06-24 10:40:24.23889 10.197.164.21 10.197.164.21 TLSV1.2 179 00:50:55:a0:3e:7f,0. 32 2020-06-24 10:40:24.23889 10.197.164.22 10.197.164.21 TLSV1.2 279 00:50:55:a0:3e:7f,0. 32 2020-06-24 10:40:24.23889 10.197.164.22 10.197.164.21 TLSV1.2 263 00:0c:29:98:ca:28,0. 33 2020-06-24 10:40:24.235858 10.197.164.22 10.197.164.21 TLSV1.2 263 00:0c:29:98:ca:28,0. 34 2020-06-24 10:40:24.235258 10.197.164.22 10.197.164.21 TLSV1.2 265 00:0c:29:98:ca:28,0. 35 2020-06-24 10:40:24.23525 10.197.164.22 10.197.164.21 TLSV1.2 266 00:0c:29:98:ca:28,0. 86 2020-06-24 10:40:24.23525 10.197.164.22 10.197.164.21 TLSV1.2 151 00:0c:29:98:ca:28,0. 87 2020-06-24 10:40:25.94760 10.197.164.22 10.197.164.21 TCP 66 00:0c:29:98:ca:28,0. 9 Frame 28: 199 bytes on wire (1592 bits), 199 bytes captured (1592 bits) 9 Ethernet II, Src: Wmare_08:26:7f (00:56:56:30:3e:7f), Dst Vmare_08:ca:28 (00:0c:29:98:ca:28,0. 9 Frame 28: 199 bytes on wire (1592 bits), 199 bytes captured (1592 bits) 9 Ethernet FI, Src: Wmare_08:26:7f (00:56:56:30:3e:7f), Dst Vmare_08:ca:28 (00:0c:29:98:ca:28,0. 9 Frame 28: 199 bytes on wire (1592 bits), 199 bytes captured (1592 bits) 9 Ethernet FI, Src: Wmare_08:26:7f (00:56:56:30:3e:7f), Dst Vmare_08:ca:28 (00:0c:29:98:ca:28,0. 9 Frame 28: 199 bytes on wire (1592 bits), 199 bytes captured (1592 bits) 9 Ethernet FI, Src: Wmare_08:26:7f (00:56:76:30:26:7f), Dst Vmare_08:ca:28 (00:0c:29:98:ca:28,0. 9 Erassision Control Protocol, Src Port: 2067, Dst Port: 636, Seq: 336, Ack: 2078, Len: 133 9 Source Port: 20857 0 estimation Port: 636 1 [Stream Index: 2] 1 [Thernet Examps] 1 [Thernet Examps] 1 [Thernet Examps] 1 [Thernet Examps] 1 [SteVAK analysis</pre>			1	25	2828-86-2	4 1	10:40	:24.2	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
<pre>27 2020-06-24 10:40:24,218678 10.197.164.21 10.197.164.22 TLSv1.2 173 00:58:56:a8:2e:77,0. 28 2020-06-24 10:40:24,219113 10.197.164.22 10.197.164.21 TLSv1.2 199 00:8c:29:98:ca:28,0. 29 2020-06-24 10:40:24,23834 10.197.164.22 10.197.164.22 TLSv1.2 167 00:58:56:a8:2e:77,0. 30 2020-06-24 10:40:24,238388 10.197.164.22 10.197.164.22 TLSv1.2 1879 00:8c:29:98:ca:28,0. 32 2020-06-24 10:40:24,238388 10.197.164.22 10.197.164.22 TLSv1.2 209 00:8c:29:98:ca:28,0. 32 2020-06-24 10:40:24,23858 10.197.164.22 10.197.164.22 TLSv1.2 205 00:58:56:a8:2e:77,0. 33 2020-06-24 10:40:24,23858 10.197.164.22 10.197.164.21 TLSv1.2 205 00:8c:29:98:ca:28,0. 34 2020-06-24 10:40:24,23855 10.197.164.22 10.197.164.21 TLSv1.2 205 00:8c:29:98:ca:28,0. 35 2020-06-24 10:40:24,23855 10.197.164.22 10.197.164.21 TLSv1.2 205 00:8c:29:98:ca:28,0. 86 2020-06-24 10:40:24,29332 10.197.164.22 10.197.164.21 TLSv1.2 205 00:8c:29:98:ca:28,0. 87 2020-06-24 10:40:24,29332 10.197.164.22 10.197.164.21 TLSv1.2 151 00:8c:23:98:ca:28,0. 87 2020-06-24 10:40:25.95 bits), 199 bytes captured (1592 bits) • Frame 21 199 bytes on wire (1592 bits), 199 bytes captured (1592 bits) • Ethernet II, Src: Vmaore,00:3e:13e(00:8c:29:98:ca:28,0. • Transission Control Protocol, Src Port: 20057, Dst: Port: 636, Seq: 336, Ack: 2078, Len: 133 Source Port: 20057 Oestimation Porto 635 [Stream index: 2] TrAnsmission Control Protocol, Src Port: 20057, Dst: Port: 636, Seq: 336, Ack: 2078, Len: 133 Source Port: 20057 Oestimation Porto 635 [Calculated windew size: 33152] [Window size calling factor: 128] Checksum: 0x5661 [unverified] [Checksum Staus: Noverified] [Checksum Staus: Moverified] [Checksum Staus: Noverified] [Checksum Staus: Noverified] [Checksum Staus: Noverified] [Checksum Staus: Noverified] [Checksum Staus: Nover: 128] * ESQUACK analysis] * [StoyACK analysis] * [StoyACK analysis] * [StoyACK analysis] * [Stoware Application Data Protocol: Ldap Content Type: Application Data Protocol: Ldap Content Type: Application Data Protocol: Ldap Version</pre>			-	26	2020-06-2	4 1	10:40	:24.2	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
28 2828-66-24 10:49:24,219113 10:197.164.22 10:197.164,22 TLSv1.2 199 00:80:29:98:ca:28,0. 29 2020-66-24 10:40:24,230304 10:197.164.22 10:197.164,22 TLSv1.2 107 00:50:56:a0:32:77,0. 31 2020-66-24 10:40:24,230305 10:197.164.22 10:197.164,21 TLSv1.2 127 00:50:56:a0:32:77,0. 32 2020-66-24 10:40:24,230355 10:197.164.21 10:197.164,21 TLSv1.2 250 00:60:c1:29:98:ca:28,0. 33 2020-66-24 10:40:24,230322 10:197.164.22 10:197.164,21 TLSv1.2 255 00:60:c1:29:98:ca:28,0. 34 2020-66-24 10:40:24,23322 10:197.164.22 10:197.164,21 TLSv1.2 255 00:80:c1:29:98:ca:28,0. 35 2020-66-24 10:40:24,23322 10:197.164.22 10:197.164,21 TLSv1.2 151 00:60:c2:9:98:ca:28,0. 86 2020-66-24 10:497.156.22 10:197.164.21 TCSv1.2 151 00:60:c2:9:98:ca:28,0. 87 2020-66-24 10:40:62:59:98:ca:28,0. 10:197.164.21 TCSv1.2 10:00:0:ca:29:98:ca:28,0.			1	27	2020-06-2	4 1	10:40	:24.7	18678		10.197.164.21		10.197.164.22	TLSv1.2	173	00:50:56:a0:3e:7f,0		Change Cipher Spec, Encrypted Handshake Message
<pre>29 2020-06-24 10:40:24.230344 10:197.164.21 10.197.164.21 TLSV1.2 167 00:50:56:30:30:77, 6. 30 2020-06-24 10:40:24.233899 10.197.164.22 10.197.164.22 TLSV1.2 1879 00:00:29:98:ca:28, 6. 31 2020-06-24 10:40:24.233899 10.197.164.22 10.197.164.22 TLSV1.2 1879 00:00:29:98:ca:28, 6. 32 2020-06-24 10:40:24.233895 10.197.164.22 10.197.164.21 TCP 66 00:00:29:98:ca:28, 6. 33 2020-06-24 10:40:24.23558 10.197.164.21 10.197.164.22 TLSV1.2 205 00:50:55:30:30:77, 6. 35 2020-06-24 10:40:24.23355 10.197.164.21 10.197.164.22 TLSV1.2 205 00:50:55:30:30:77, 6. 35 2020-06-24 10:40:24.23352 10.197.164.22 10.197.164.21 TCP 66 00:00:29:98:ca:28, 6. 87 2020-06-24 10:40:57.944560 10.197.164.22 10.197.164.21 TCP 66 00:00:29:98:ca:28, 6. 87 2020-06-24 10:40:57.944560 10.197.164.22 10.197.164.21 TCP 66 00:00:29:98:ca:28, 6. 87 2020-06-24 10:40:57.944560 10.197.164.22 10.197.164.21 TCP 66 00:00:29:98:ca:28, 6. 87 2020-06-24 10:40:57.944560 10.197.164.22 10.197.164.21 TCP 66 00:00:29:98:ca:28, 6. 87 2020-06-24 10:40:57.947560 10.197.164.22 10.197.164.21 TCP 66 00:00:29:98:ca:28, 6. 87 2020-06-24 10:40:57.947560 10.197.164.22 10.197.164.21 TCP 66 00:00:29:98:ca:28, 6. 87 2020-06-24 10:40:57.947560 10.197.164.22 10.197.164.21 TCP 66 00:00:29:98:ca:28, 6. 87 2020-06-24 10:40:57.947560 10.197.164.22 10.197.164.21 TCP 66 00:00:29:98:ca:28, 6. 87 2020-06-24 10:40:57.947560 10.197.164.22 10.197.164.21 TCP 66 00:00:29:98:ca:28, 6. 87 2020-06-24 10:40:57.947560 10.197.164.22 10.197.164.21 TCP 66 00:00:29:98:ca:28, 6. 87 2020-06-24 10:40:57.947560 10.197.164.22 10.197.164.21 TCP 66 00:00:29:98:ca:28, 6. 87 2020-06-24 10:40:57.947660 10.197.164.22 10.197.164.21 TCP 66 00:00:29:98:ca:28, 6. 87 2020-06-24 10:40:57.947560 10.197.164.22 10.197.164.21 TCP 66 00:00:29:98:ca:28, 6. 87 2020-06-24 10:40:133 [50curce Port: 20057 Dost Port: 20057 Dost Port: 636, Seq: 336, Ack: 2078, Len: 133 50curce Port: 20057 [75 Cource Solid Port: 606 [55 Cource Solid Port: 120] 1000 = Hodder Length: 32 Dytes (0) 8 Flaps: 0x018 (Sist Vertified] 1000 = Hodder Le</pre>				28	2020-06-2	4 1	10:40	:24.2	219113	l.	10.197.164.22		10.197.164.21	TLSv1.2	199	00:0c:29:98:ca:28.0.		Application Data
<pre>30 2020-06-24 10:40:24.231712 10.197.164.22 10.197.164.21 TLSV1.2 279 00:60:29:98:ca:28, 0. 31 2020-06-24 10:40:24.23858 10.197.164.21 10.197.164.21 TLSV1.2 1879 00:50:56:00:30:77, 0. 32 2020-06-24 10:40:24.23858 10.197.164.21 10.197.164.21 TLSV1.2 263 00:00:29:98:ca:28, 0. 33 2020-06-24 10:40:24.251944 10.197.164.22 10.197.164.21 TLSV1.2 263 00:00:29:98:ca:28, 0. 34 2020-06-24 10:40:24.23322 10.197.164.21 10.197.164.21 TLFV1.2 265 00:00:29:98:ca:28, 0. 35 2020-06-24 10:40:24.293322 10.197.164.22 10.197.164.21 TLFV1.2 255 00:50:56:00:30:77, 0. 35 2020-06-24 10:40:25.94663 10.197.164.22 10.197.164.21 TLFV1.2 151 00:00:29:98:ca:28, 0. 86 2020-06-24 10:40:57.946553 10.197.164.22 10.197.164.21 TLFV1.2 151 00:00:29:98:ca:28, 0. 87 2020-06-24 10:40:59.54608 10.0197.164.22 10.197.164.21 TLFV1.2 151 00:00:29:98:ca:28, 0. 87 2020-06-24 10:40:59.54608 10.0197.164.22 10.197.164.21 TLFV1.2 151 00:00:29:98:ca:28, 0. 87 2020-06-24 10:40:59.54608 10.0197.164.22 10.197.164.21 TLFV1.2 151 00:00:29:98:ca:28, 0. 87 2020-06-24 10:40:59.54608 10.0197.164.22 10.197.164.21 TLFV1.2 151 00:00:29:98:ca:28, 0. 87 2020-06-24 10:40:59.561:00:30:577 (DSI:00:00:152) 20151) 8 Ethernet 11, 5rc: Vmaare_08:20:77 (DOI:50:561:00:30:77), DSI: Vmaare_98:ca:28 (D0:00:29:98:ca:28, 0. 87 2020-06-24 10:40:59.551:00:30:77), DSI: Vmaare_98:ca:28 (D0:00:29:98:ca:28, 0. 87 2020-06-24 10:40:29:98:ca:28, 0. 87 2020-06-24 2020-06-24, 0. 87 2030 87 2030 87 20400-24 2040 97 20400-24 203 97 20</pre>		-		29	2020-06-2	4 1	10:40	:24.2	230384		10.197.164.21		10.197.164.22	TLSv1.2	167	00:50:56:a0:3e:7f,0	_	Application Data
<pre>31 2020-06-24 10:40:24.23889 10.197.164.21 10.197.164.22 TLSV1.2 1879 00:50:56:a0:3e:7f, 0. 32 2020-06-24 10:40:24.238958 10.197.164.21 10.197.164.21 TCP 66 00:0c:29:98:ca:28, 0. 33 2020-06-24 10:40:24.253658 10.197.164.21 10.197.164.22 TLSV1.2 255 00:56:a0:38:7f, 0. 34 2020-06-24 10:40:24.253658 10.197.164.21 10.197.164.22 TLSV1.2 255 00:56:a0:38:7f, 0. 35 2020-06-24 10:40:27.93222 10.197.164.22 10.197.164.21 TLSV1.2 255 00:56:a0:38:7f, 0. 86 2020-06-24 10:40:57.947680 10.197.164.22 10.197.164.21 TLFV1.2 151 00:0c:29:98:ca:28, 0. 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. 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. 87 2020-06-24 10:40:57.947680 10.197.164.22 20.107.164.21 TCP 66 00:0c:29:98:ca:28, 0. 87 2020-06-24 10:40:57.947680 10.97.164.22 0.517.164.21 TCP 66 00:0c:29:98:ca:28, 0. 87 2020-06-24 10:40:57.947680 10.97.164.22 0.517.164.21 TCP 66 00:0c:29:98:ca:28, 0. 87 2020-06-24 10:40:57.947680 10.97.164.22 0.511 0.197.164.21 TCP 66 00:0c:29:98:ca:28, 0. 87 2020-06-24 10:40:57.947680 10.97.164.22 0.511 0.197.164.21 TCP 66 00:0c:29:98:ca:28, 0. 87 2020-06-24 10:40:57.947680 10.97.164.22 0.511 0.197.164.21 TCP 66 00:0c:29:98:ca:28, 0. 9 Internet Protocol Version 4, Src: 10.197.164.22, Dst: 10.197.164.21 TCP 66 00:0c:29:98:ca:28, 0. 9 Internet Protocol Version 4, Src: 10.197.164.22, Dst: 10.197.164.21 TCP 66 00:0c:29:98:ca:28, 0. 9 Internet Protocol Version 4, Src: 10.197.164.22, Dst: 10.197.164.21 TCP 60 00:0c:29:98:ca:28, 0. 9 Internet Protocol Version 4, Src: 10.197.164.22, Dst: 10.197.164.21 TCP 66 00:0c:29:98:ca:28, 0. 9 Internet Protocol Version 4, Src: 10.197.164.22, Dst: 10.197.164.21 TCP 60 00:0c:29:98:ca:28, 0. 9 Internet Protocol Version 4, Src: 10.197.164.22, Dst: 10.197.164.21 TCP 60 00:0c:29:98:ca:28, 0. 9 Fiags: 0x0818 (PSH, ACK) Window size value: 259 [Calculated window size: 33152] [Window size value: 259 [Calculated window size: 33152] [Window size value: 259 [Calculated window size: 33152] [Window size</pre>			-	30	2020-06-2	4 1	10:40	:24.7	231712		10.197.164.22		10.197.164.21	TLSv1.2	279	00:0c:29:98:ca:28.0.		Application Data
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. 33 2020-06-24 10:40:24.251944 10.197.164.22 10.197.164.21 TLSV1.2 263 00:06:29:98:ca:28,0. 34 2020-06-24 10:40:24.293322 10.197.164.22 10.197.164.21 TLSV1.2 25 00:56:50:30:37:7,0. 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. 86 2020-06-24 10:40:57.946553 10.197.164.22 10.197.164.21 TCP 66 00:0c:29:98:ca:28,0. 87 2020-06-24 10:40:57.946553 10.197.164.22 10.197.164.21 TCP 60 00:0c:29:98:ca:28,0. 87 2020-06-24 10:40:57.946553 10.197.164.22 10.197.164.21 TCP 60 00:0c:29:98:ca:28,0. 87 2020-06-24 10:40:57.946553 10.197.164.22 10:197.164.21 TCP 60 00:0c:29:98:ca:28,0. 87 2020-06-24 10:40:57.946553 10:197.164.22 10:197.164.21 TCP 60 00:0c:29:98:ca:28,0. 87 2020-06-24 10:40:59.50 trist 10:197.164.21 TCP 60 00:0c:29:98:ca:28,0. 87 2020-06-24 10:40:40:40 trist 10:197.164.22 10:197.164.21 TCP 60 00:0c:29:98:ca:28,0. 9 Ethernet II, Src: Waware_00:3e:7f (00:50:56:a0:3e:7f), Dst: Yuware_90:ca:28 (00:0c:29:98:ca:28) 1 Internet Protocol, Src Port: 20057, Dst Port: 636, Seq: 336, Ack: 2078, Len: 133 1 Source Port: 2057 1 TCP Segment Len: 133] 1 Sequence number: 30 (relative sequence number) 1 Acknowledgment number: 2078 (relative sequence number) 1 Acknowledgment number: 2078 (relative sequence number) 1 Acknowledgment number: 2078 (relative sequence number) 1 Checksum: 90561 [unverified] 1 Window size saling factor: 128] 1 Checksum Status: Unverified] 1 Window size saling factor: 128] 2 Mondow size saling factor: 128] 2 Mondow size saling factor: 128] 3 Mondow size scaling factor: 128] 3 Mondow size scaling factor: 128] 3 Mondow size			-	31	2828-86-2	4 1	10:40	:24.7	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 captur
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 34 2020-06-24 10:40:24.253658 10.197.164.21 10.197.164.22 TLSv1.2 295 00:50:56:a0:30:7f,0 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 87 2020-06-24 10:40:57.947680 10.197.164.22 10.197.164.21 TLSv1.2 151 00:0c:29:98:ca:28,0 87 2020-07:2000 Version 4, Src: 10:197.164.22, Dst: Vmware_90:ca:28 (00:0c:29:98:ca:28,0 9 Internet Protocol Version 4, Src: 10:197.164.22, Dst: 10:197.164.21 9 Transmission Control Protocol, Src Port: 20057, Dst Port: 636, Seq: 336, Ack: 2078, Len: 133 Source Port: 20057 0estination Port: 636 15trem index: 2] 1000 = Header Length: 32 bytes (8) 9 Flags: 0x018 (PSH, ACK) Window size value: 259 1020 Louted window size: 33152] 10400 wize scaling factor: 128 Checksum: 0x5651 [unverified] 10400 urgent pointer: 0 9 Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps > [SEQ/ACK analysis] 7 TLSv1.2 Record Layer: Application Data Protocol: ldap Content Type: Application Data (23) Version: TLS 1.2 (0x0803)			-	32	2828-86-2	4 1	10:40	:24.2	238958		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
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. 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. 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. 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. 9 Frame 28: 199 bytes on wire (1592 bits), 199 bytes captured (1592 bits) Ethernet TI, Src: Vmacr_00:55:6:36:30:36:7f, 00:55:6:36:30:36:7f, 0.55: 9 Internet Protocol Version 4, Src: 10.197.164.22, Dst: 10.197.164.21 7 Transmission Control Protocol, Src Port: 20057, Dst Port: 636, Seq: 336, Ack: 2078, Len: 133 Source Port: 20057 Destination Port: 636 [Stream index: 2] [TCP Segment Len: 133] Sequence number: 336 (relative sequence number)]Mext sequence number: 459 (relative sequence number)]Mext sequence number: 2078 (relative sequence number)]Mext sequence number: 2078 (relative sequence number) [Acknowledgment number: 2078 (relative sequence number)] Acknowledgment number: 2078 (relative sequence number) [Mext sequence number: 3152] [Vindow size value: 259 [Calculated window size: 33152] [Window size value: 259 [Calculated window size: 33152] [Window size value: 259 [Calculated window size: 33152] [Window size scaling factor: 128] Checksum \$tatus: lonverified] [Checksum \$tatus: lo			-	33	2828-86-2	4 1	10:40	:24.7	251944		10,197,164,22		10,197,164,21	TLSv1.2	263	00:0c:29:98:ca:28.0_		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_ 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_ 87 2020-06-24 10:40:457.946583 10:197.164.22 10:197.164.21 TCP 66 00:0c:29:98:ca:28,0_ 9 Frame 28: 199 bytes on wire (1592 bits), 199 bytes captured (1592 bits) Ethernet II, Src: Vmware_a0:3e:77 (00:50:50:a0:3e:77), Dst: Vmware_98:ca:28 (00:0c:29:98:ca:28) > Internet Protocol Version 4, Src: 10.197.164.22, Dst: 10.197.164.21 Y Transmission Control Protocol, Src Port: 28057, Dst Port: 636, Seq: 336, Ack: 2078, Len: 133 Source Port: 28057 Destination Port: 636 [Stream index: 2] [TCP Segment Len: 133] Sequence number: 336 (relative sequence number) [Next sequence number: 2078 (relative ack number) 1000 # Header Length: 32 bytes (8) # Flags: 0x018 (PSH, ACK) Window size value: 259 [Callated window size: 33152] [Window size scaling factor: 128] [Checksum: 8x5651 [unverified] Urgent pointer: 0 # Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps # Secure Socketst Layer #			-	34	2828-86-2	4 1	10:40	:24.7	53658		10,197,164,21		10,197,164,22	TLSv1.2	295	00:50:56:a0:3e:7f.0_		Application Data
86 2020-06-24 10:40:57.946553 10.197.164.22 10.197.164.21 TLSv1.2 151 00:00:20:29:98:ca:28,0			-	35	2828-86-2	4 1	10:40	:24.7	93322		18, 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
<pre>B0 2020-06-24 10:40:57.947680 10:197.164.22 10:197.164.21 TCP 66 00:00:29:99:ca:28,0_ Frame 28: 199 bytes on wire (1592 bits), 199 bytes captured (1592 bits) E Ethernet II, Src: Vmware_00:3e:7f (00:50:56:00:3e:7f), Dst: Vmware_90:ca:28 (00:00:29:98:ca:28) Internet Protocol Version 4, Src: 10:197.164.21 TCP 66 00:00:29:98:ca:28) Internet Protocol Version 4, Src: 10:197.164.21 Transmission Control 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 Destination Port: 636 [Stream index: 2] [TCP Segment Len: 133] Sequence number: 336 (relative sequence number)] Acknowledgment number: 2078 (relative sequence number)] Acknowledgment number: 2078 (relative sequence number) Next sequence number: 335 (relative sequence number) [Next sequence number: 335 (relative sequence number)] Acknowledgment number: 259 [Calculated window size: 33152] [Window size value: 259 [Calculated window size: 33152] [Window size scaling factor: 128] Checksum: 0x5eti [unverified] [Checksum Status: Unverified] Urgent pointer: 0 b Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps b [SEQ/ACK analysis] b [Timestamps] TCP payload (133 bytes) Fencervented [Version: TLS 1.2 (0x0303) Fencervented [Fencerven</pre>			ŝ	R6	2828-86-2	4 1	10:40	-57.0	46557		10.197.164.22		18, 197, 164, 21	TI Sv1.2	151	88:8c:29:98:ca:28.8		Application Data
<pre>Frame 28: 199 bytes on wire (1592 bits), 199 bytes captured (1592 bits) Ethernet II, Src: Vmware_a0:3e:7f (00:50:56:a0:3e:7f), Dst: Vmware_98:ca:28 (00:0c:29:98: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] [TCP Segment Len: 133] Sequence number: 336 (relative sequence number) [Next sequence number: 2078 (relative sequence number)] Acknowledgment number: 2078 (relative ack number) 1000 = Header Length: 32 bytes (8) F Flags: 0x018 (PSH, ACK) Window size value: 259 [Calculated window size: 33152] [Window size scaling factor: 128] Checksum: 0x5661 [unverified] [Checksum Status: Unverified] Urgent pointer: 0 Flags(12) bytes), No-Operation (NOP), No-Operation (NOP), Timestamps [SEQ/ACK analysis] F [Timestamps] TCP payload (133 bytes) Fencrypted [Secure Sockets Layer: Application Data Protocol: ldap Content Type: Application Data (23) Version: TLS 1.2 (0x0303) Version: TLS 1.2 (0x0303) Version: TLS 1.2 (0x0304) Version: TLS 1.2 (0x0304) Version: TLS 1.2 (0x0304) Factor Sockets Layer: Application Data (23) Version: TLS 1.2 (0x0304) Version: TLS 1.2 (0x0304</pre>		-	-	87	2828-85-2	4 1	18:48	:57.5	4768	_	10,197,164,22		18, 197, 164, 21	TCP	66	88:8c:29:98:ca:28.8		28057 + 636 [FIN, ACK] Seg=964 Ack=4221 Win=39688
Destination Port: 636 [Stream index: 2] [TCP Segment Len: 133] Sequence number: 336 (relative sequence number) [Next sequence number: 2078 (relative ack number)] Acknowledgment number: 2078 (relative ack number) 10000 = Header Length: 32 bytes (8) > Flags: 0x018 (PSH, ACK) Window size value: 259 [Calculated window size: 33152] [Window size scaling factor: 128] Checksum: 0x5e61 [unverified] [Checksum Status: Unverified] Urgent pointer: 0 > Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps > [SEQ/ACK analysis] > [TCP payload (133 bytes)	 Ethernet II, Src: Vmware_a0:3e:7f (00:50:56:a0:3e:7f), Dst: Vmware_98:ca:28 (00:0c:29:98:ca:28) 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 																	
<pre>Intervent of the sequence number is the</pre>		_	D	act	ination P	ort	. 63	6										
Secure Sockets Layer TLSv1.2 Record Layer: Application Data Protocol: Idap Content Type: Application Data (23) Version: TLS 1.2 (0x0303) Fncrvnted [* * *		Str TCP equ Nex ckn 800 lag ind Cal Win hec Che rge pti SEQ Tim CP	eam index Segment ence numb t sequenc. owledgmen = H s: 0x018 ow size v culated w dow size ksum: 0x5 cksum Sta nt pointe ons: (12 //ACK anal estamps) payload (: 2 Len er: e n t n ead (PS alu ind sca e61 tus r: byt ysi 133	<pre>2] 1: 13 336 sumbe tumbe</pre>	3] (r: 46 r: 20 ength CK) 59 ize: fact verif verif No-0 es)	relat 9 78 : 32 33152 or: 1 ied] ied] perat	ive (re (ro byto] 28]	e sequence numb elative sequenc elative ack nu es (8) h (NOP), No-Ope	er) e numbe nber) ration	r)] (NOP), Timestam	35				
TLSv1.2 Record Layer: Application Data Protocol: ldap Content Type: Application Data (23) Version: TLS 1.2 (0x0303)	5	Sec	cui	re :	Sockets La	aye	r											
Length: 128 Encrypted Application Data: 173d1b0b2f280a13cc17815e54447bb9ac8af8a881a9eb84		Ŧ	T		1.2 Record Content Ty Version: T Length: 12 Encrypted	d L pe: LS 8 App	ayer : App 1.2 plica	: App licat (0x03	licat tion [303) Data:	ion lata 17	Data Protocol (23) 73d1b0b2f280a13	: ldap cc17815	e54447bb9ac8af8	a881a9eb84		→ Encrypte	d Da	ta

Troubleshoot

This section describes some common errors that are encountered with this configuration and how to troubleshoot them.

• In the authentication report, you could see this error message:

Authentication method is not supported by any applicable identity store

This error message indicates that the method you picked is not supported by LDAP. Ensure that the Authentication Protocol in the same report shows one of the supported methods (EAP-GTC, EAP-TLS, or PEAP-TLS).

• Test bind to server ended with an error.

Most commonly this is due to the LDAPS server certificate validation check failure. In order to troubleshoot such types of issues, take a packet capture on ISE and enable all the three runtime and prrt-jni components at debug level, recreate the issue, and check the prrt-server.log file.

Packet capture complains about a bad certificate and prrt-server shows:

Note: The hostname in the LDAP page must be configured with the subject name of the certificate (or any of the Subject Alternate Name). So unless you have such in the subject or SAN, it does not work, the certificate with the IP address in the SAN list is needed.

3. In the authentication report, you could notice that the subject was not found in the identity store. This means that the user name from the report does not match the Subject Name Attribute for any user in the LDAP database. In this scenario, the value was set to sAMAccountName for this attribute, which means that the ISE looks to the sAMAccountName values for the LDAP user when it attempts to find a match.

4. The subjects and groups could not be retrieved correctly during a bind to server test. The most probable cause of this issue is an incorrect configuration for the search bases. Remember that the LDAP hierarchy must be specified from the leaf-to-root and dc (can consist of multiple words).

Related Information

- <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>