

ISE configureren en problemen oplossen met externe LDAPS Identity Store

Inhoud

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

Inleiding

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

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

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

Gebruikte componenten

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

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

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

Achtergrondinformatie

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

Deze verificatieprotocollen worden ondersteund met LDAPS:

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

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

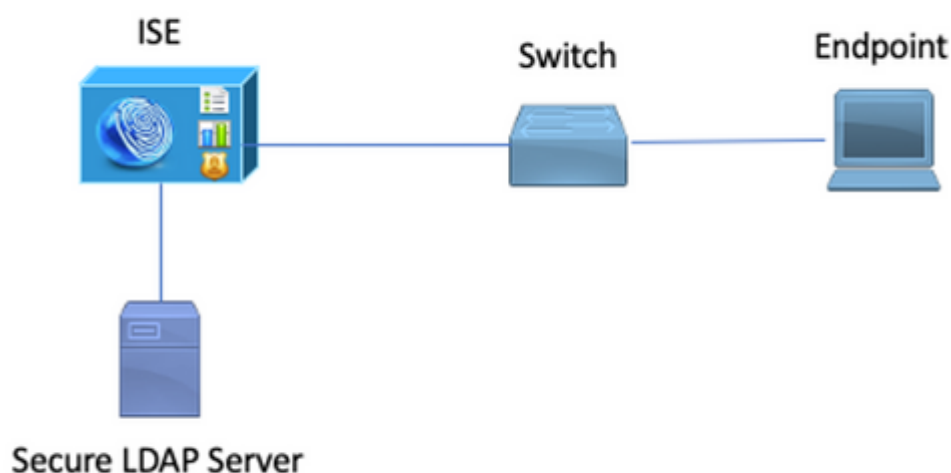
Configureren

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

Netwerkdigram

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

Dit beeld illustreert de netwerktopologie die wordt gebruikt:

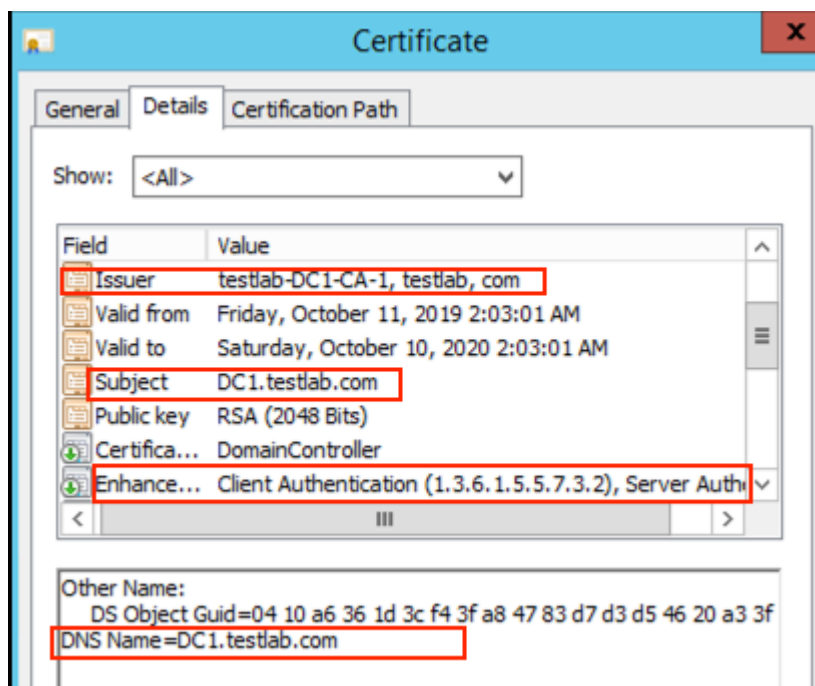


LDAPS op Active Directory configureren

Identiteitscertificaat op domeincontroller installeren

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

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



Directory-structuur voor toegang tot LDAPS

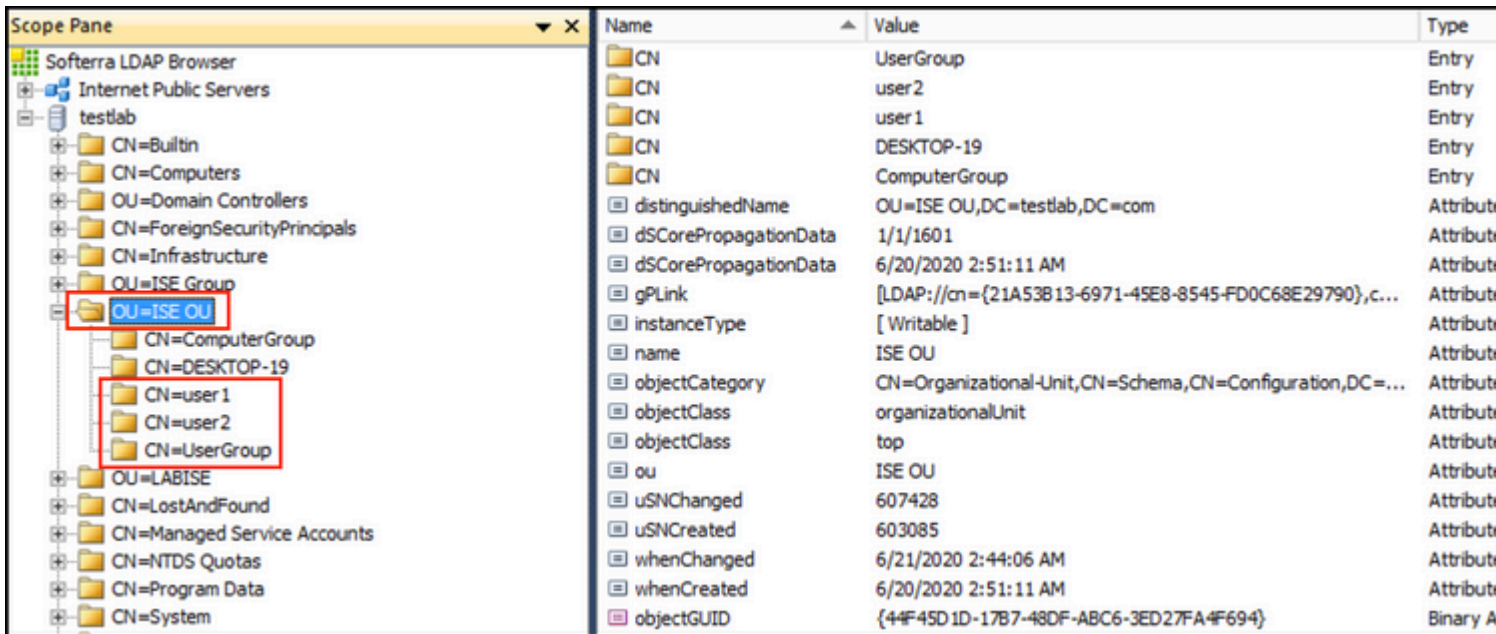
Maak gebruik van een LDAP browser om toegang te krijgen tot de LDAPS Directory op de Active Directory-server. In dit LAB wordt Softerra LDAP Browser 4.5 gebruikt.

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



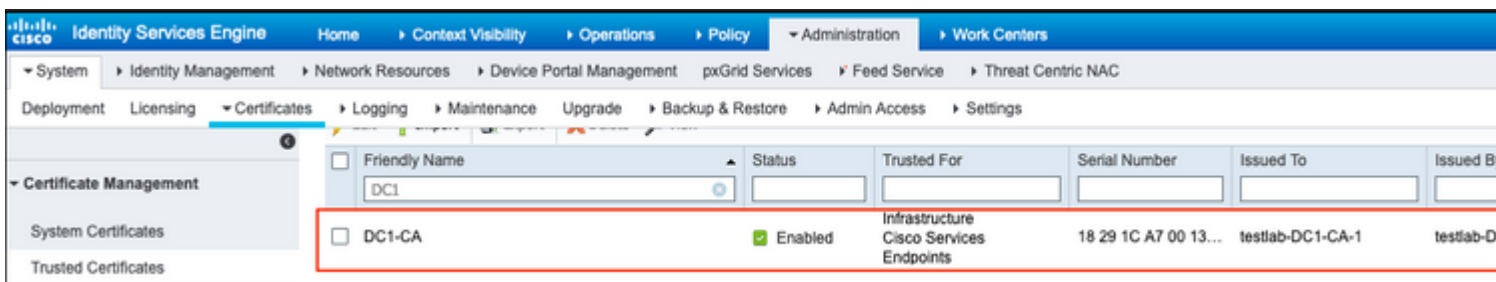
2. Maak ter vereenvoudiging een organisatie-eenheid (OE) met de naam ISE-OE in de advertentie en deze moet een groep met de naam UserGroup hebben. Maak twee gebruikers (user1 en user2) en maak ze lid van de groep UserGroup.

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



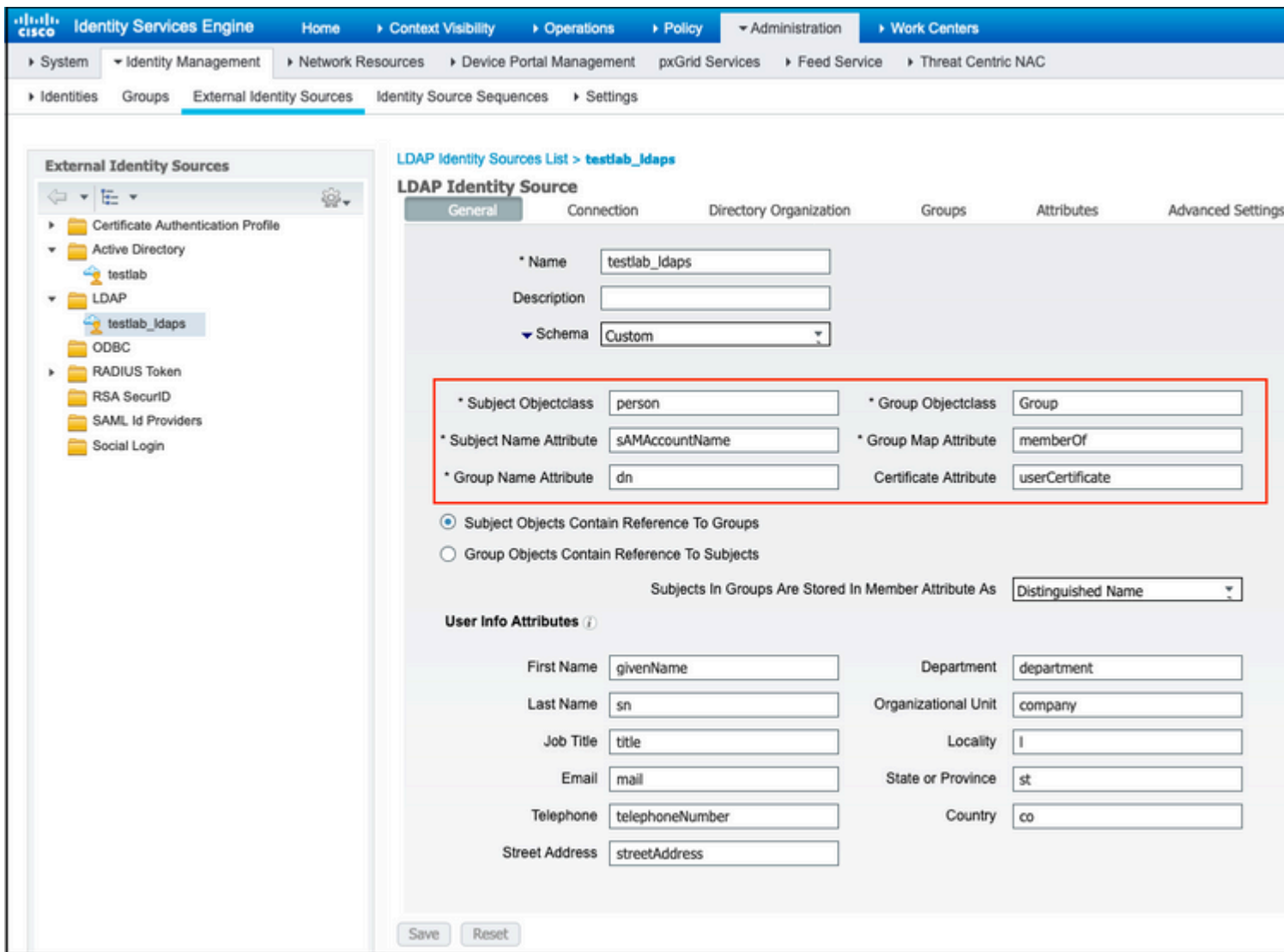
Integreer ISE met LDAPS-server

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



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

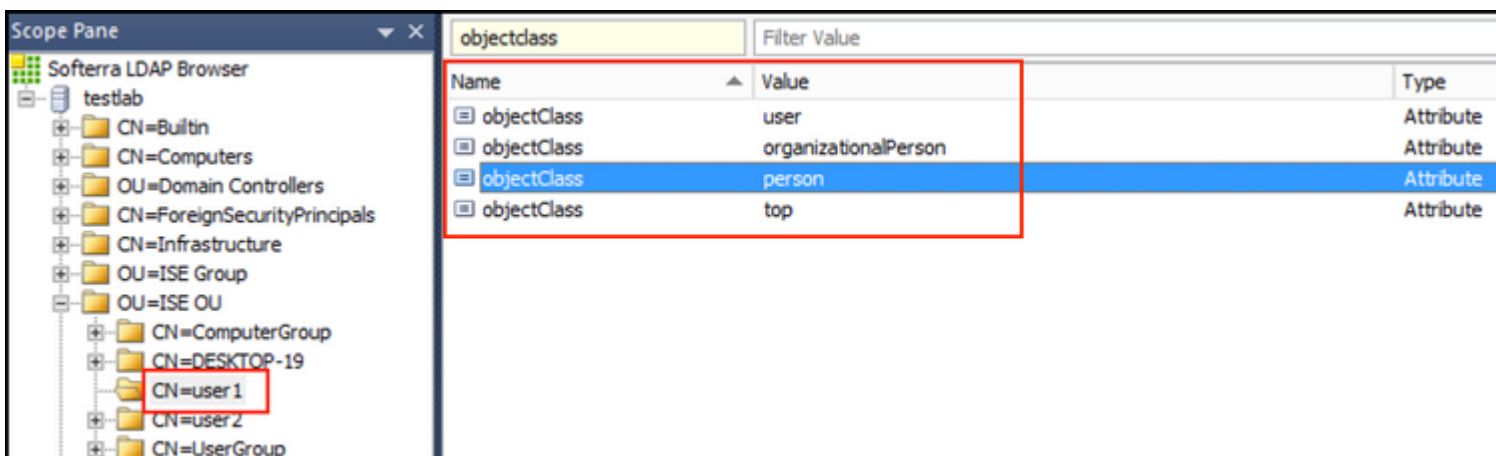
3. Om de LDAPS-server te integreren, maakt u gebruik van de verschillende LDAP-kenmerken uit de LDAPS-directory. Ga naar **Administratie > Identiteitsbeheer > Externe Identiteitsbronnen > LDAP Identity Sources > Add**.



4. Configureer deze eigenschappen vanuit het tabblad Algemeen:

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

- top
- Persoon
- Organisator
- InetOrgPerson



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

The screenshot shows the 'Scope Pane' on the left with a tree view of LDAP objects. The 'CN=user1' object is selected and highlighted with a red box. The main pane on the right displays a table of attributes for this user.

Name	Value	Type
cn	user 1	Attribute
displayName	user 1	Attribute
distinguishedName	CN=user 1,OU=ISE OU,DC=testlab,DC=com	Attribute
givenName	user 1	Attribute
name	user 1	Attribute
sAMAccountName	user 1	Attribute
userPrincipalName	user1@testlab.com	Attribute
userCertificate	user 1	Binary Attribute

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

The screenshot shows the 'Scope Pane' on the left with a tree view of LDAP objects. The 'CN=UserGroup' object is selected and highlighted with a red box. The main pane on the right displays a table of attributes for this group.

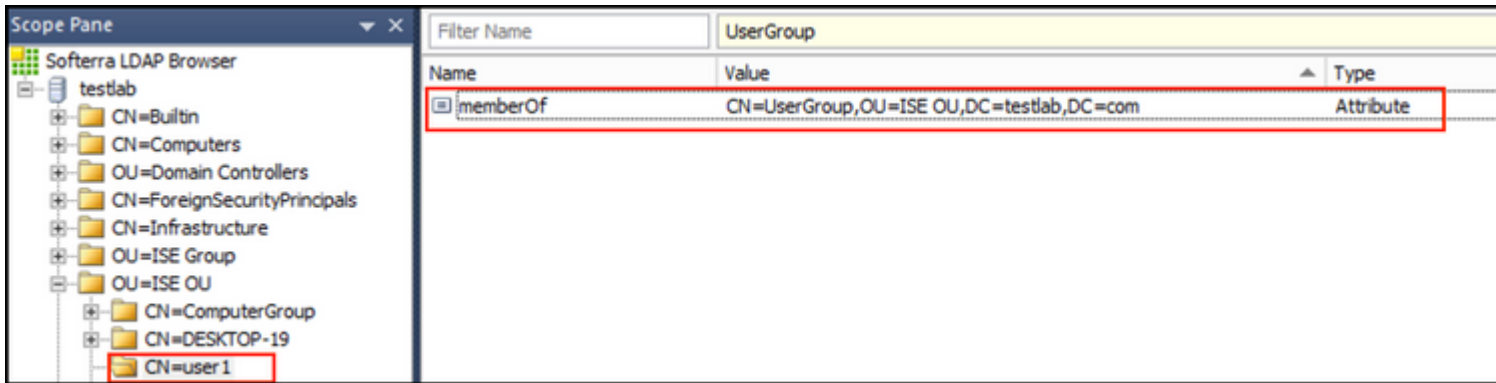
Name	Value	Type
cn	UserGroup	Attrib
distinguishedName	CN=UserGroup,OU=ISE OU,DC=testlab,DC=com	Attrib
dSCorePropagationData	1/1/1601	Attrib
groupType	[GlobalScope, Security]	Attrib
instanceType	[Writable]	Attrib
member	CN=user 1,OU=ISE OU,DC=testlab,DC=com	Attrib
member	CN=user 2,OU=ISE OU,DC=testlab,DC=com	Attrib
name	UserGroup	Attrib
objectCategory	CN=Group,CN=Schema,CN=Configuration,DC=testlab,DC=com	Attrib
objectClass	group	Attrib
objectClass	top	Attrib
sAMAccountName	UserGroup	Attrib
sAMAccountType	< samGroupObject >	Attrib

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

The screenshot shows the 'Scope Pane' on the left with a tree view of LDAP objects. The 'CN=UserGroup' object is selected and highlighted with a red box. The main pane on the right displays a table of object class attributes.

objectSid	S-1-5-21-2960284039-4006096050-347662626-1156	Binary Attribute
objectGUID	{39967F90-89BE-44B5-9CC5-B28C0B0EB234}	Binary Attribute
objectClass	top	Attribute
objectClass	group	Attribute
objectCategory	CN=Group,CN=Schema,CN=Configuration,DC=testlab,DC=com	Attribute

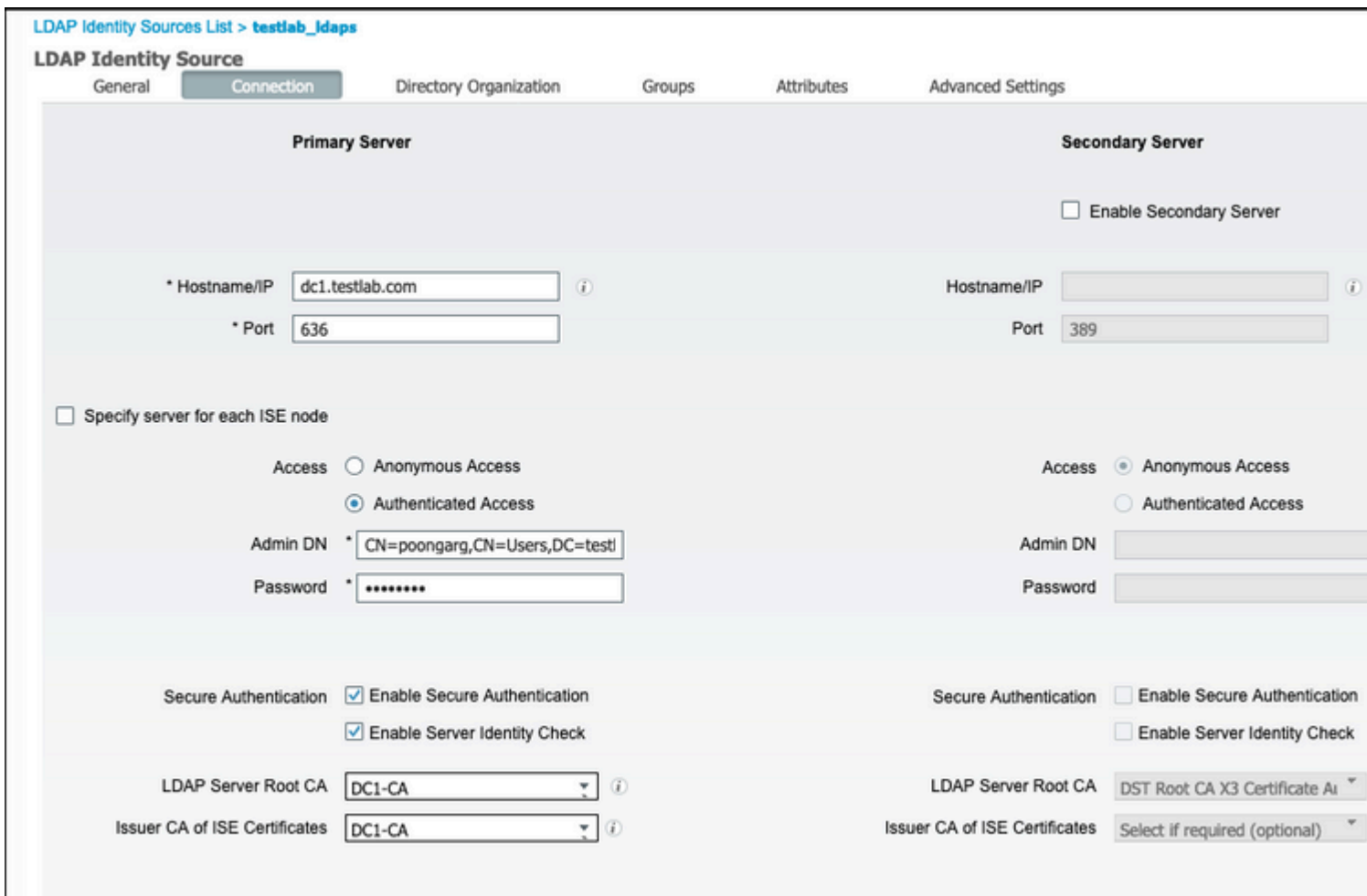
Groepskaart Attribute: Deze eigenschap bepaalt hoe de gebruikers aan de groepen in kaart worden gebracht.

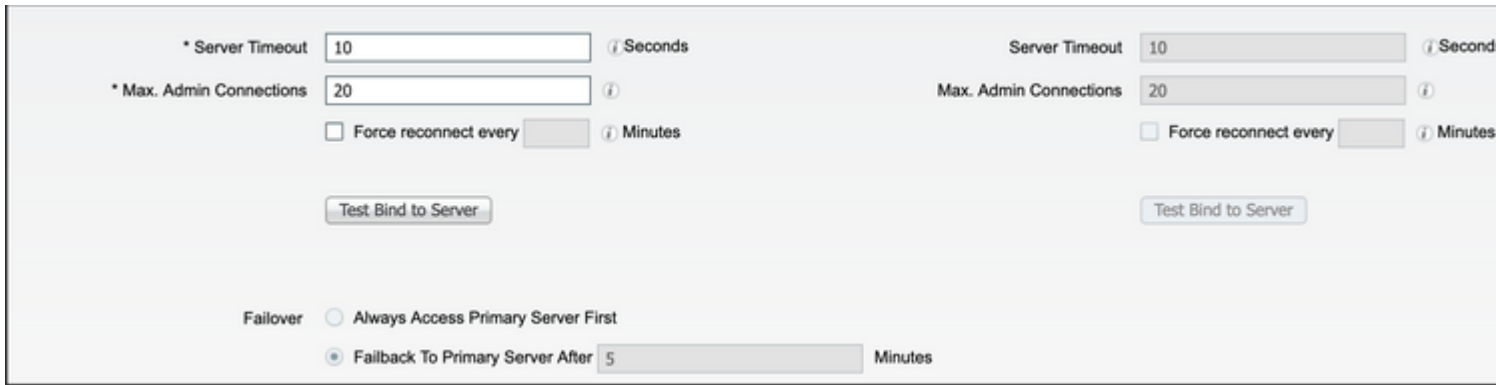


Certificaatkenmerk: Voer het kenmerk in dat de certificaatdefinities bevat. Deze definities kunnen naar keuze worden gebruikt om certificaten te valideren die door cliënten worden gepresenteerd wanneer zij worden gedefinieerd als deel van een verificatieprofiel van een certificaat. In dergelijke gevallen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



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





* Server Timeout (i) Seconds

* Max. Admin Connections (i)

Force reconnect every (i) Minutes

Failover Always Access Primary Server First

Failback To Primary Server After Minutes

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

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

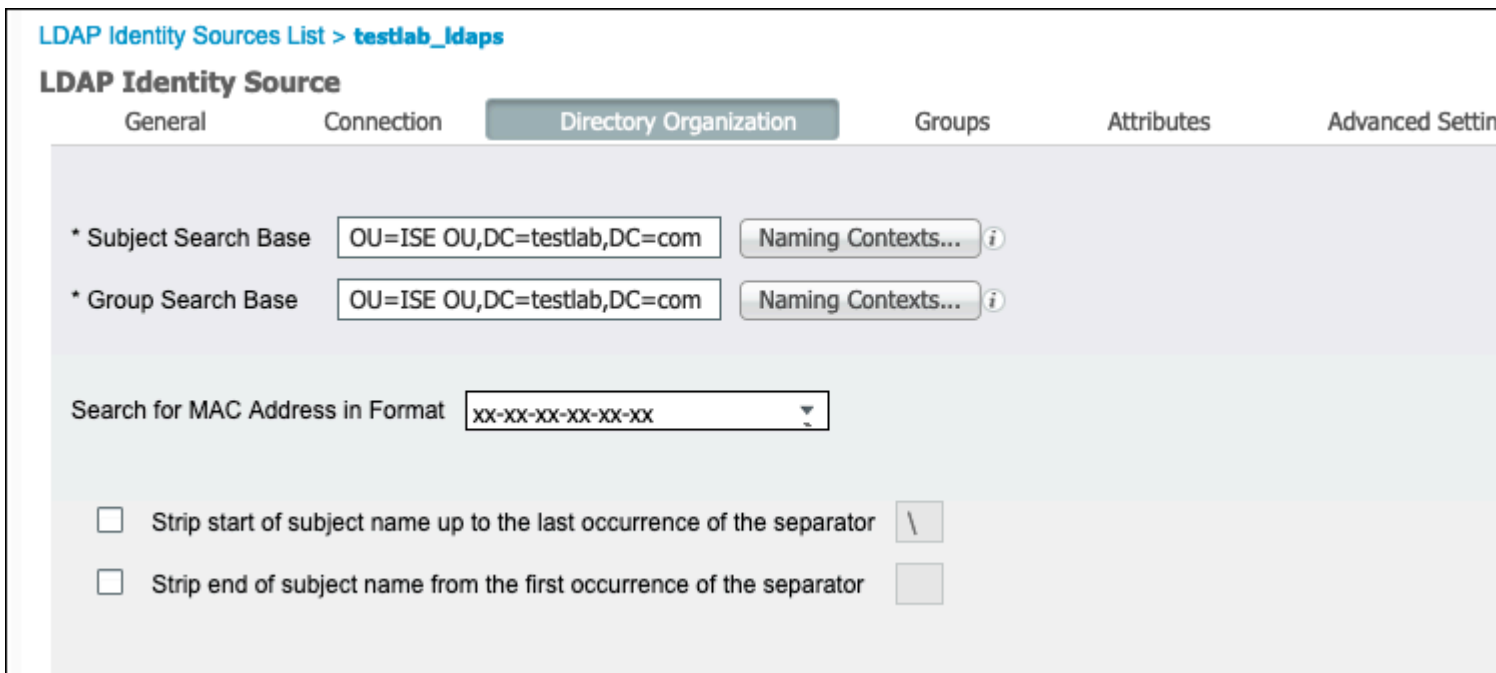
Stap 1. Stel het juiste IP-adres of Hostname van de LDAP-server in, definieer de LDAPS-poort (TCP 636) en Admin DN om een verbinding te maken met LDAP over SSL.

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

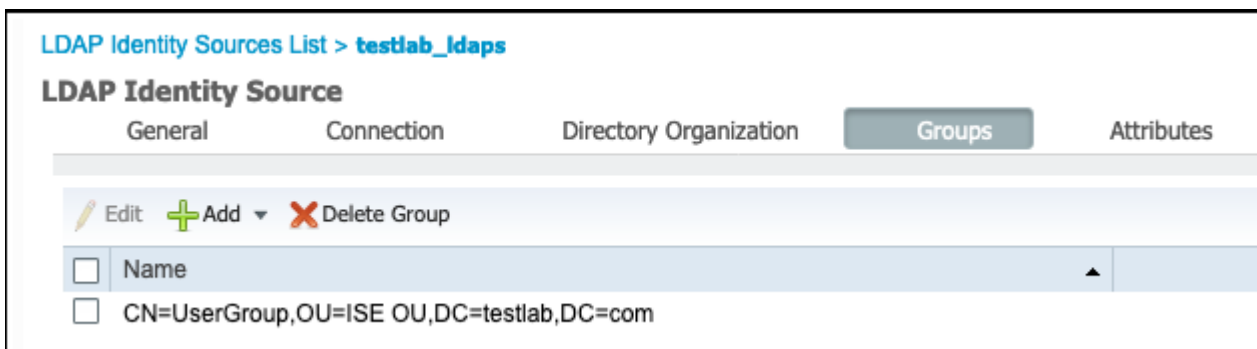
Stap 3. Selecteer in het vervolgkeuzemenu het LDAP Server Root CA-certificaat en het ISE-beheercertificaat ISER CA-certificaat (We hebben het certificaat gebruikt, geïnstalleerd op dezelfde LDAP-server om ook het ISE-beheercertificaat af te geven).

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

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



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



De Switch configureren

Configureer de switch voor 802.1x-verificatie. Windows PC is aangesloten op switchport Gig2/0/47

```

aaa new-model

radius server ISE
address ipv4 x.x.x.x auth-port 1812 acct-port 1813
key 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
!

```

```
dot1x system-auth-control

ip device tracking
!
radius-server attribute 6 on-for-login-auth
radius-server attribute 8 include-in-access-req
!

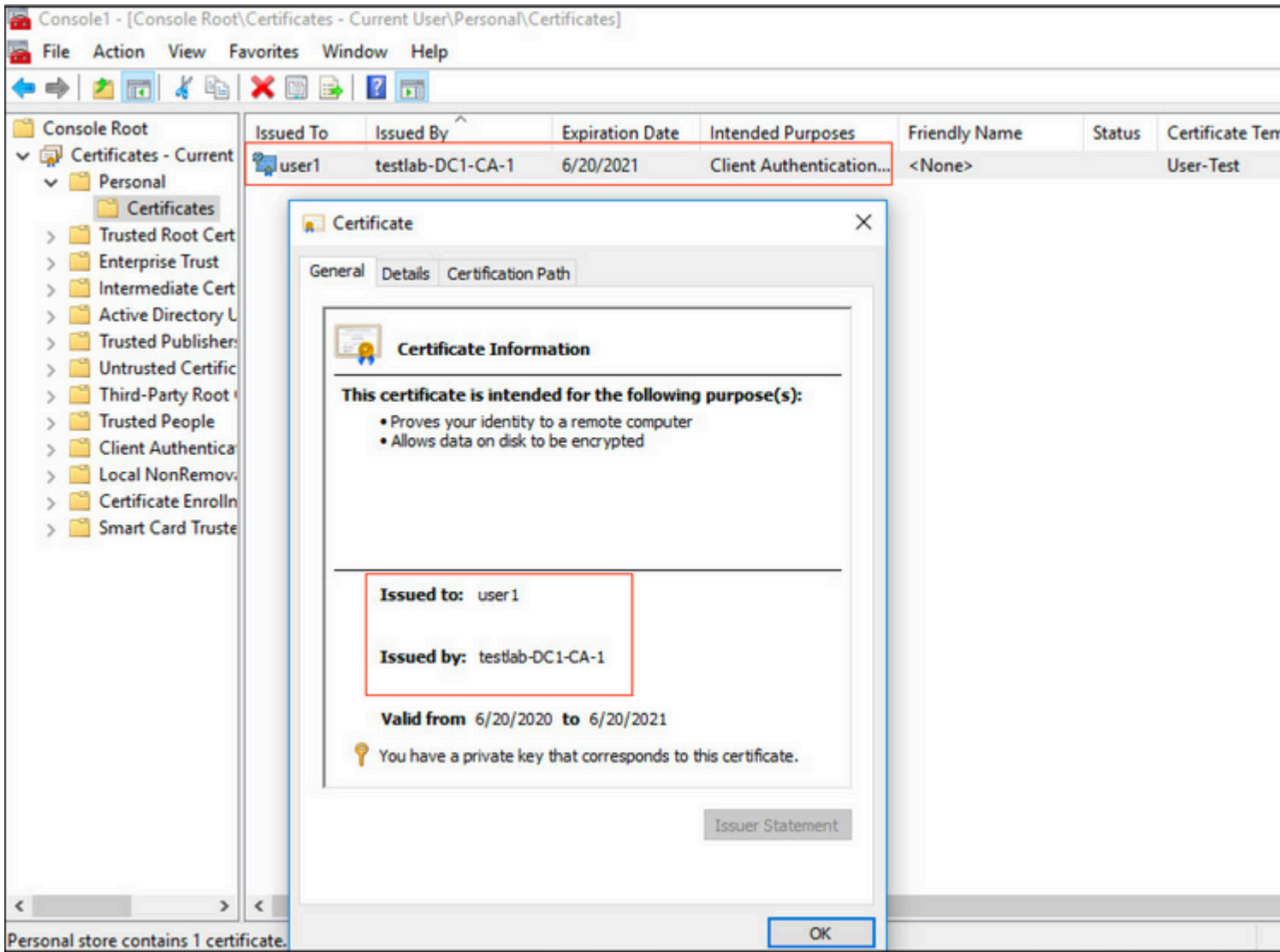
!

interface GigabitEthernet2/0/47
switchport access vlan xx
switchport mode access
authentication port-control auto
dot1x pae authenticator
```

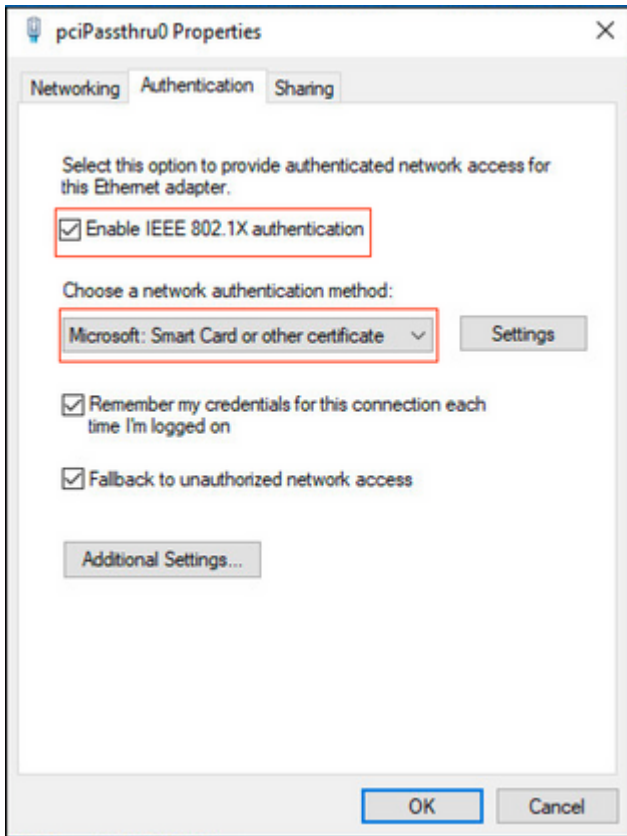
Het eindpunt configureren

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

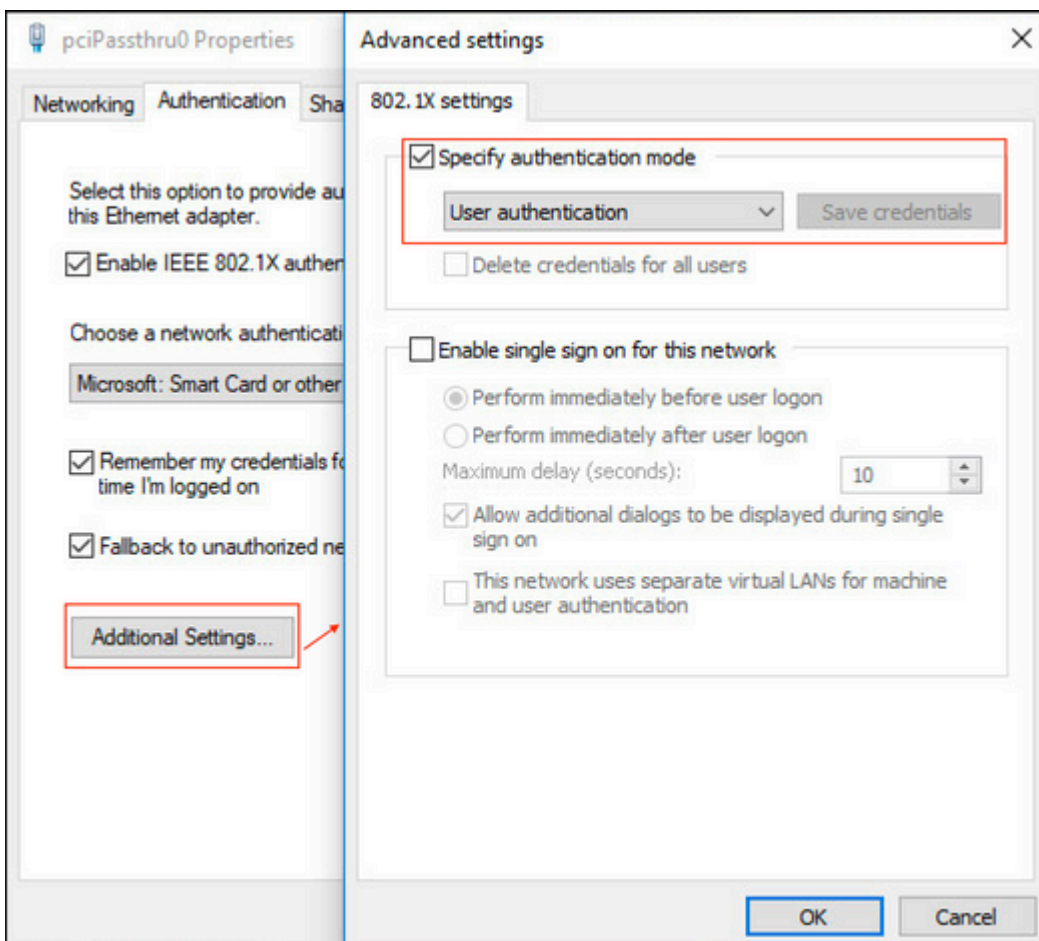
1. Zorg ervoor dat PC is voorzien van gebruikerscertificaat (voor gebruiker 1) en bedoeld zijn als clientverificatie en in de Trusted Root-certificeringsinstanties, de emittent-certificaatketen op de PC aanwezig is.



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



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



Configureer de beleidsset op ISE

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

The screenshot shows the Cisco Identity Services Engine (ISE) configuration page for a Certificate Authentication Profile. The breadcrumb navigation is: Home > Context Visibility > Operations > Policy > Administration > Work Centers > External Identity Sources > Identity Source Sequences > Settings. The left sidebar shows a tree view of External Identity Sources, with 'Certificate Authentication Profile' selected. The main content area is titled 'Certificate Authentication Profile' and shows the following configuration:

- Name:** LDAPS_cert
- Description:** EAP-TLS certificate based authentication with LDAPS
- Identity Store:** testlab_idaps
- Use Identity From:** Certificate Attribute (Selected), Subject - Common Name
- Match Client Certificate Against Certificate In Identity Store:** Always perform binary comparison (Selected)

Buttons for 'Save' and 'Reset' are located at the bottom of the configuration area.

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

Identity Services Engine Home > Context Visibility > Operations > Policy > Administration > Work Centers

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

Identity Source Sequence

* Name

Description

Certificate Based Authentication

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_ldaps	⬆
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"
- Treat as if the user was not found and proceed to the next store in the sequence

Configureer nu beleidsset voor bekabelde Dot1x-verificatie:

Identity Services Engine Home > Context Visibility > Operations > Policy > Administration > Work Centers

Policy Sets Profiling Posture Client Provisioning > Policy Elements

Policy Sets → Wired Dot1x

Status	Policy Set Name	Description	Conditions
	Wired Dot1x		Wired_802.1X

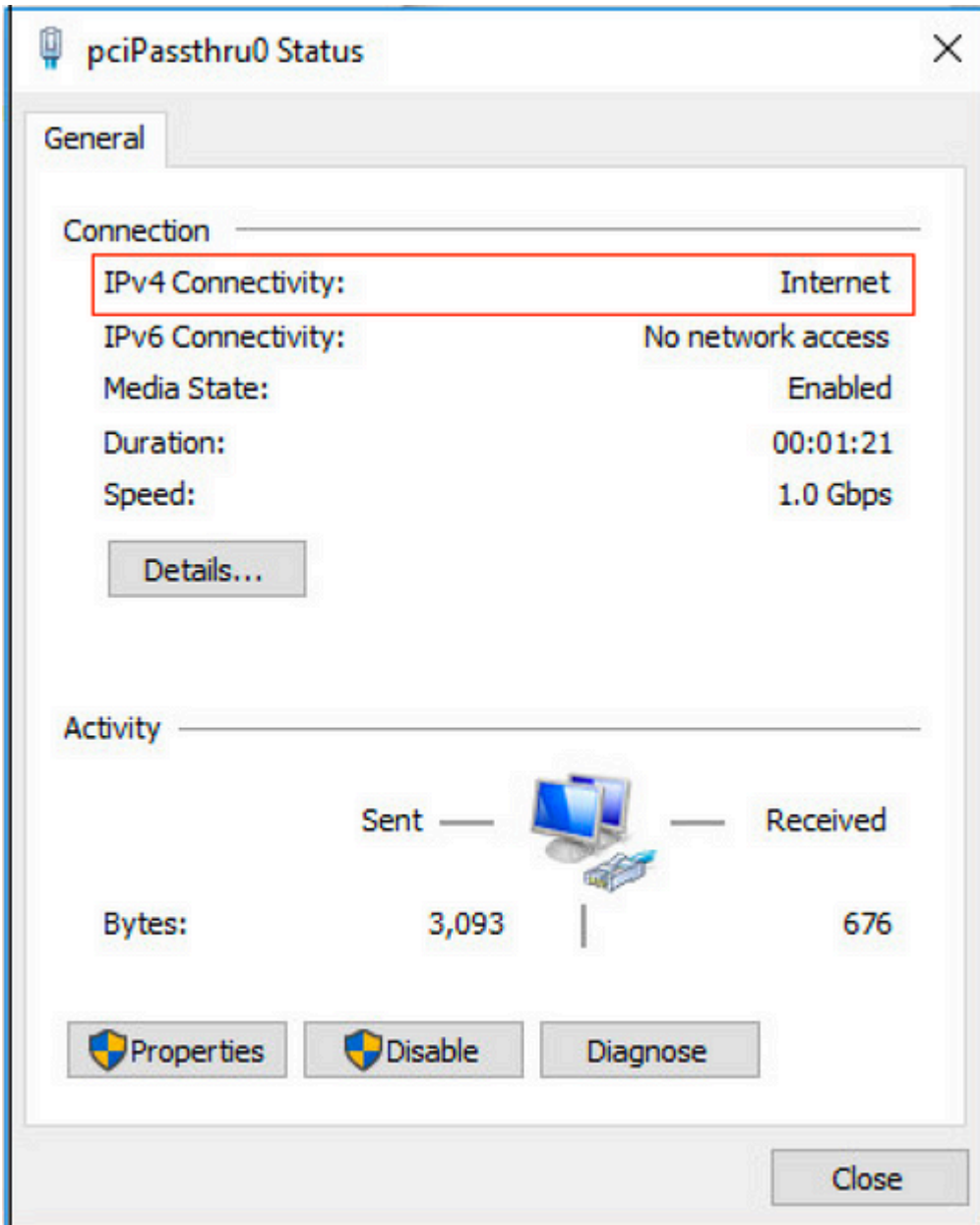
Authentication Policy (2)

+ Status	Rule Name	Conditions
	Dot1x	Network Access-NetworkDeviceName EQUALS LAB-Switch
	Default	

Authorization Policy (2)

+ Status	Rule Name	Conditions	Results	Profiles
	Users in LDAP Store	testlab_ldaps-ExternalGroups EQUALS CN=UserGroup,OU=iSE OU,DC=testlab,DC=com	PermitAccess	
	Default		DenyAccess	

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



Verifiëren

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

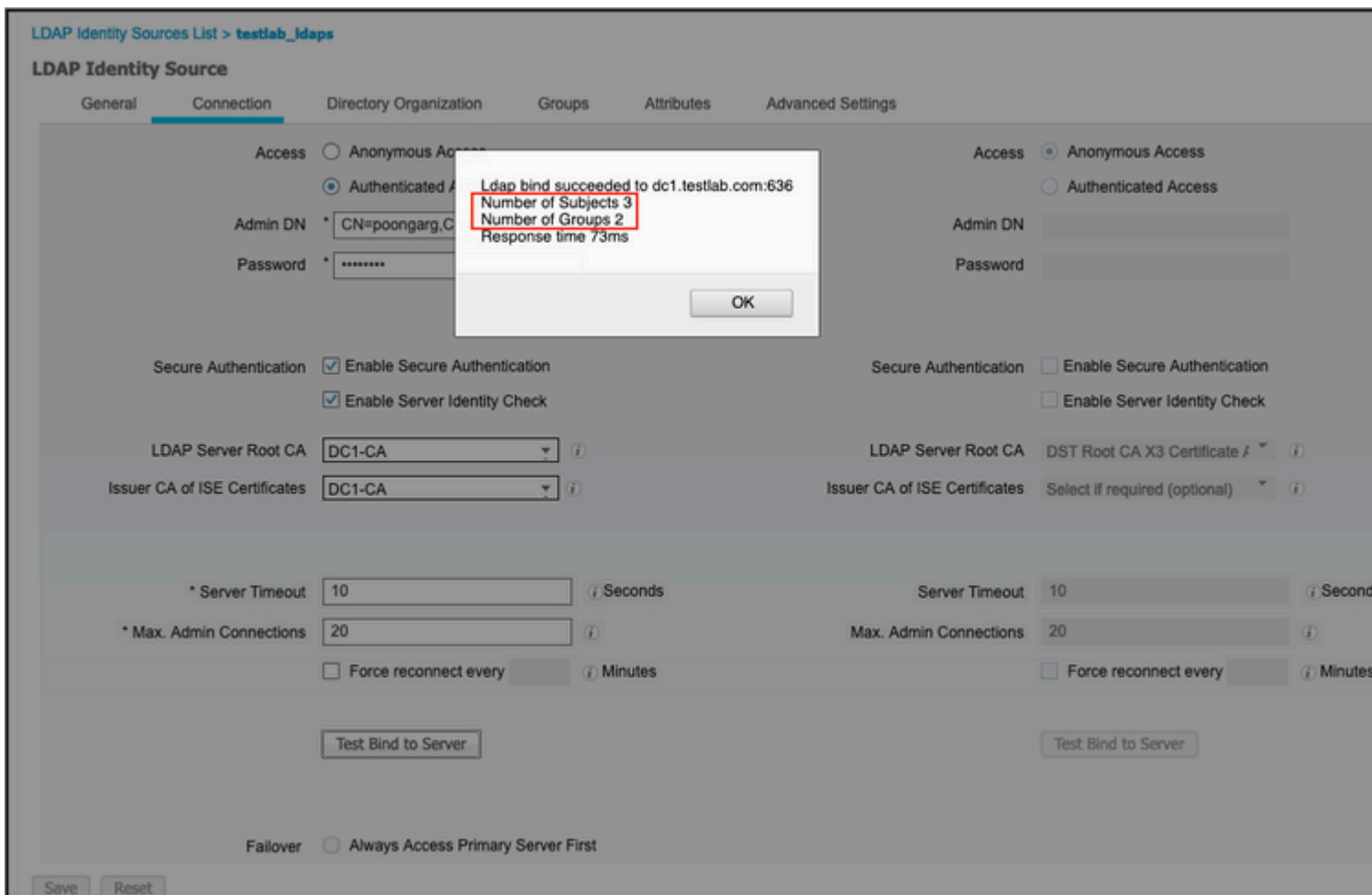

```
SW1#sh auth sessions int g2/0/47 de
  Interface: GigabitEthernet2/0/47
  MAC Address: b496.9126.dec0
  IPv6 Address: Unknown
  IPv4 Address: 10.106.38.165
  User-Name: user1
  Status: Authorized
  Domain: DATA
  Oper host mode: single-host
  Oper control dir: both
  Session timeout: N/A
  Restart timeout: N/A
  Periodic Acct timeout: N/A
  Session Uptime: 43s
  Common Session ID: 0A6A26390000130798C66612
  Acct Session ID: 0x00001224
  Handle: 0x6800002E
  Current Policy: POLICY_Gi2/0/47

Local Policies:
  Service Template: DEFAULT_LINKSEC_POLICY_SHOULD_SECURE (priority 150)

Server Policies:

Method status list:
  Method      State
  dot1x      Authc Success
```

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



3. Controleer het gebruikersverificatierapport:

Time	Status	Details	Identity	Endpoint ID	Authentication Po...	Authorization Policy	Authorization Profi...
Jun 24, 2020 04:45:21.727 AM			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			user1	B4:96:91:26:DE:C0	Wired Dot1x >> Dot1x	Wired Dot1x >> Users in LDAP Store	PermitAccess

4. Controleer het gedetailleerde verificatierapport voor het eindpunt:

Overview

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_idaps

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_ldaps
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
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_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

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

No.	Time	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 SA...
21	2020-06-24 10:40:24.206505	10.197.164.21	10.197.164.22	TCP	74	00:50:56:a0:3e:7f,0...		636 → 28057 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 M...
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] Seq=1 Ack=1 Win=29312 Len=0 TSval...
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 durin...
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
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 Spe...
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
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
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
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 L...

```

▶ 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: 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: 469 (relative sequence number)]
  Acknowledgment number: 2078 (relative ack number)
  1000 .... = Header Length: 32 bytes (8)
  ▶ Flags: 0x018 (PSH, ACK)
  Window size value: 259
  [Calculated window size: 33152]
  [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]
  ▶ [Timestamps]
  TCP payload (133 bytes)
  Secure Sockets Layer
  ▼ TLSv1.2 Record Layer: Application Data Protocol: ldap
    Content Type: Application Data (23)
    Version: TLS 1.2 (0x0303)
    Length: 128
    Encrypted Application Data: 173d1b0b2f280a13cc17815e54447bb9ac8af8a881a9eb84...

```

Encrypted Data

Problemen oplossen

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

- In het verificatierapport kunt u deze foutmelding zien:

```
Authentication method is not supported by any applicable identity store
```

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

- Test bind aan server eindigde met een fout.

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

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

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

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

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

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

Gerelateerde informatie

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

Over deze vertaling

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