

Configuration et dépannage d'ISE avec le magasin d'identités LDAPS externe

Table des matières

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Configurer](#)

[Diagramme du réseau](#)

[Configurer LDAPS sur Active Directory](#)

[Installer le certificat d'identité sur le contrôleur de domaine](#)

[Accéder à la structure du répertoire LDAPS](#)

[Intégrer ISE au serveur LDAPS](#)

[Configuration du commutateur](#)

[Configuration du terminal](#)

[Configurer le jeu de stratégies sur ISE](#)

[Vérifier](#)

[Dépannage](#)

[Informations connexes](#)

Introduction

Ce document décrit l'intégration de Cisco ISE avec le serveur LDAPS sécurisé en tant que source d'identité externe.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Connaissances de base de l'administration d'Identity Service Engine (ISE)
- Connaissances de base du protocole LDAPS (Active Directory/Secure Lightweight Directory Access Protocol)

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Correctif 7 Cisco ISE 2.6
- Microsoft Windows version 2012 R2 avec Active Directory Lightweight Directory Services installé
- PC sous Windows 10 avec demandeur natif et certificat utilisateur installé
- Commutateur Cisco C3750X avec image 152-2.E6

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. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Informations générales

LDAPS permet le cryptage des données LDAP (qui incluent les informations d'identification de l'utilisateur) en transit lorsqu'une liaison d'annuaire est établie. LDAPS utilise le port TCP 636.

Ces protocoles d'authentification sont pris en charge avec LDAPS :

- Carte à jeton générique EAP (EAP-GTC)
- Protocole PAP (Password Authentication Protocol)
- Sécurité de la couche transport EAP (EAP-TLS)
- PEAP-TLS (Protected EAP Transport Layer Security)

 Remarque : EAP-MSCHAPV2 (en tant que méthode interne de PEAP, EAP-FAST ou EAP-TTLS), LEAP, CHAP et EAP-MD5 ne sont pas pris en charge avec la source d'identité externe LDAPS.

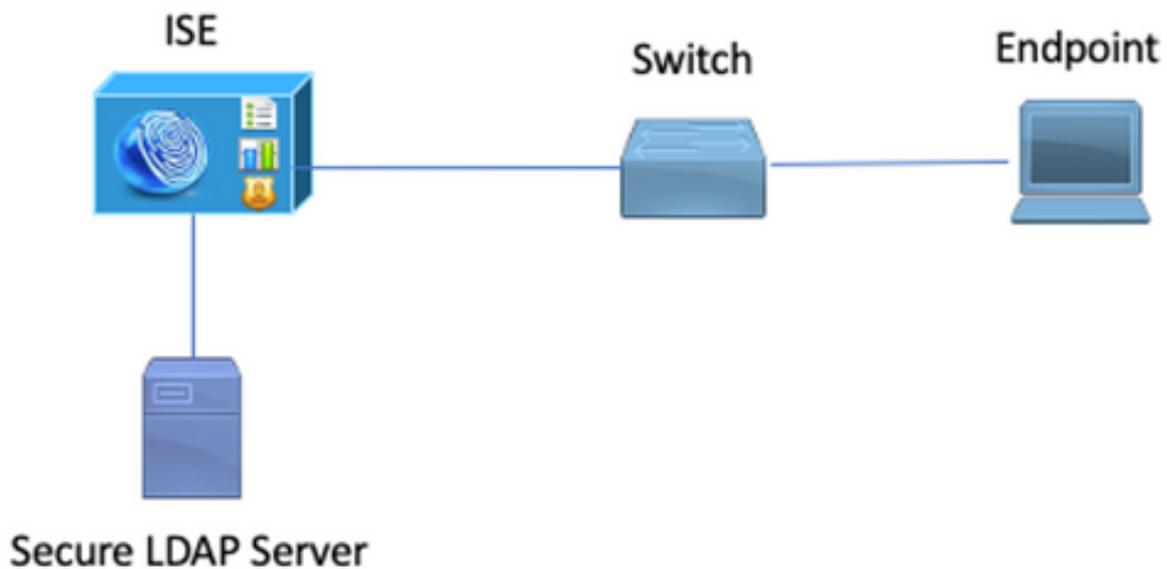
Configurer

Cette section décrit la configuration des périphériques réseau et l'intégration de l'ISE au serveur LDAP Microsoft Active Directory (AD).

Diagramme du réseau

Dans cet exemple de configuration, le point d'extrémité utilise une connexion Ethernet avec un commutateur pour se connecter au réseau local (LAN). Le port de commutation connecté est configuré pour l'authentification 802.1x afin d'authentifier les utilisateurs avec ISE. Sur l'ISE, LDAPS est configuré en tant que magasin d'identités externe.

Cette image illustre la topologie de réseau utilisée :



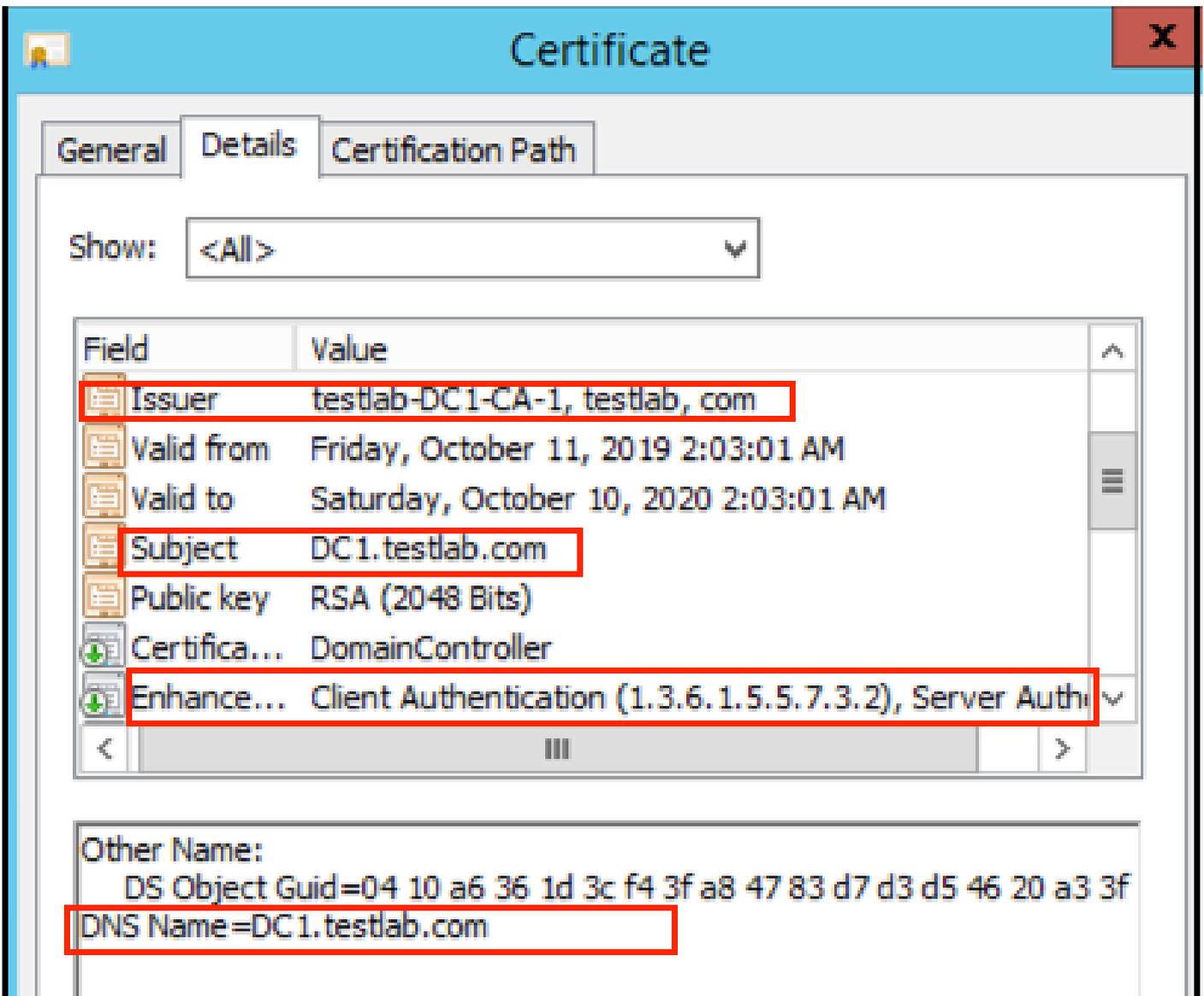
Configurer LDAPS sur Active Directory

Installer le certificat d'identité sur le contrôleur de domaine

Afin d'activer LDAPS, installez un certificat sur le contrôleur de domaine (DC) qui répond à ces exigences :

1. Le certificat LDAPS se trouve dans le magasin de certificats personnel du contrôleur de domaine.
2. Une clé privée qui correspond au certificat est présente dans le magasin du contrôleur de domaine et est correctement associée au certificat.
3. L'extension Enhanced Key Usage inclut l'identificateur d'objet Server Authentication (1.3.6.1.5.5.7.3.1) (également appelé OID).
4. Le nom de domaine complet (FQDN) du contrôleur de domaine (par exemple, DC1.testlab.com) doit être présent dans l'un de ces attributs : le nom commun (CN) dans le champ Objet et l'entrée DNS dans l'extension Autre nom du sujet.
5. Le certificat doit être émis par une autorité de certification (CA) à laquelle le contrôleur de domaine et les clients LDAPS font confiance. Pour une communication sécurisée approuvée, le client et le serveur doivent faire confiance à l'autorité de certification racine de l'autre et aux certificats d'autorité de certification intermédiaire qui leur ont délivré des certificats.

6. Le fournisseur de services cryptographiques (CSP) Schannel doit être utilisé pour générer la clé.



Accéder à la structure du répertoire LDAPS

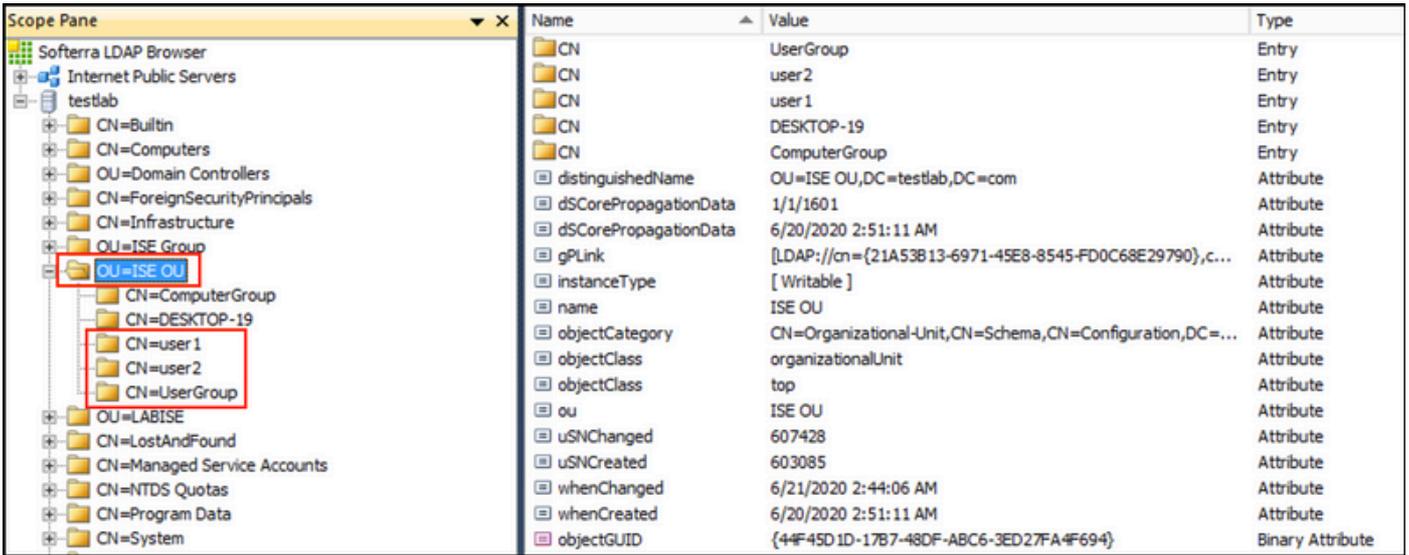
Pour accéder à l'annuaire LDAP sur le serveur Active Directory, utilisez n'importe quel navigateur LDAP. Dans ces travaux pratiques, le navigateur LDAP 4.5 de Softerra est utilisé.

1. Établissez une connexion au domaine sur le port TCP 636.



2. Par souci de simplicité, créez une unité d'organisation nommée unité d'organisation ISE dans Active Directory et elle doit avoir un groupe nommé UserGroup. Créez deux utilisateurs (user1 et user2) et faites-les membres du groupe UserGroup.

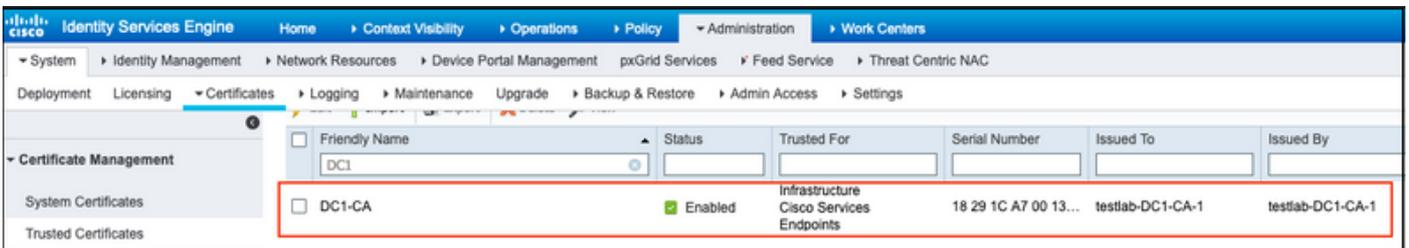
 Remarque : la source d'identité LDAP sur ISE est utilisée uniquement pour l'authentification des utilisateurs.



Name	Value	Type
CN	UserGroup	Entry
CN	user2	Entry
CN	user1	Entry
CN	DESKTOP-19	Entry
CN	ComputerGroup	Entry
distinguishedName	OU=ISE OU,DC=testlab,DC=com	Attribute
dSCorePropagationData	1/1/1601	Attribute
dSCorePropagationData	6/20/2020 2:51:11 AM	Attribute
gPLink	[LDAP://cn={21A53B13-6971-45E8-8545-FD0C68E29790},c...	Attribute
instanceType	[Writable]	Attribute
name	ISE OU	Attribute
objectCategory	CN=Organizational-Unit,CN=Schema,CN=Configuration,DC=...	Attribute
objectClass	organizationalUnit	Attribute
objectClass	top	Attribute
ou	ISE OU	Attribute
uSNChanged	607428	Attribute
uSNCreated	603085	Attribute
whenChanged	6/21/2020 2:44:06 AM	Attribute
whenCreated	6/20/2020 2:51:11 AM	Attribute
objectGUID	{44F45D1D-17B7-48DF-ABC6-3ED27FA4F694}	Binary Attribute

Intégrer ISE au serveur LDAPS

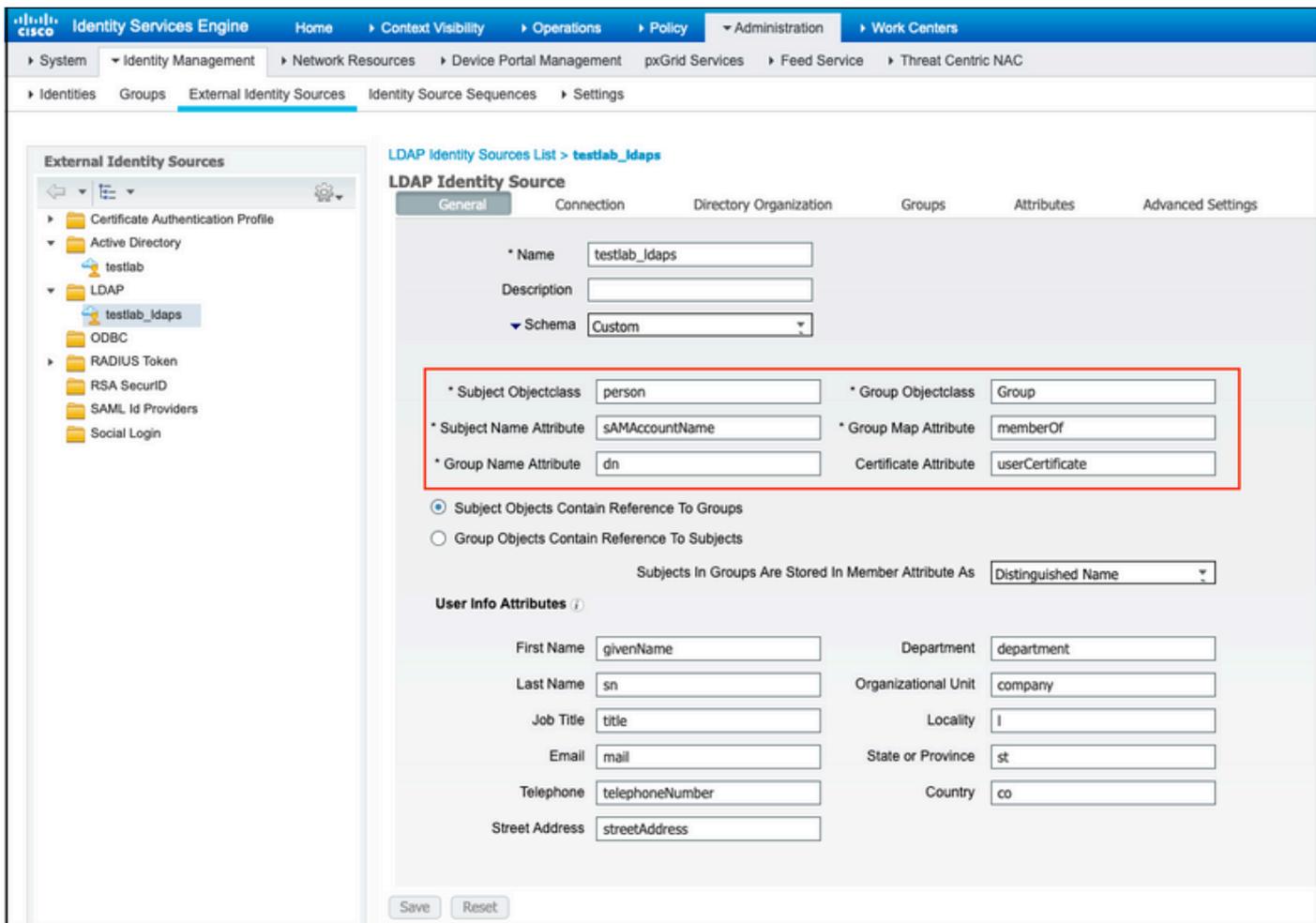
1. Importez le certificat d'autorité de certification racine du serveur LDAP dans le certificat approuvé.



Friendly Name	Status	Trusted For	Serial Number	Issued To	Issued By
DC1					
DC1-CA	Enabled	Infrastructure Cisco Services Endpoints	18 29 1C A7 00 13...	testlab-DC1-CA-1	testlab-DC1-CA-1

2. Validez le certificat d'administration ISE et assurez-vous que le certificat d'émetteur du certificat d'administration ISE est également présent dans le magasin de certificats de confiance.

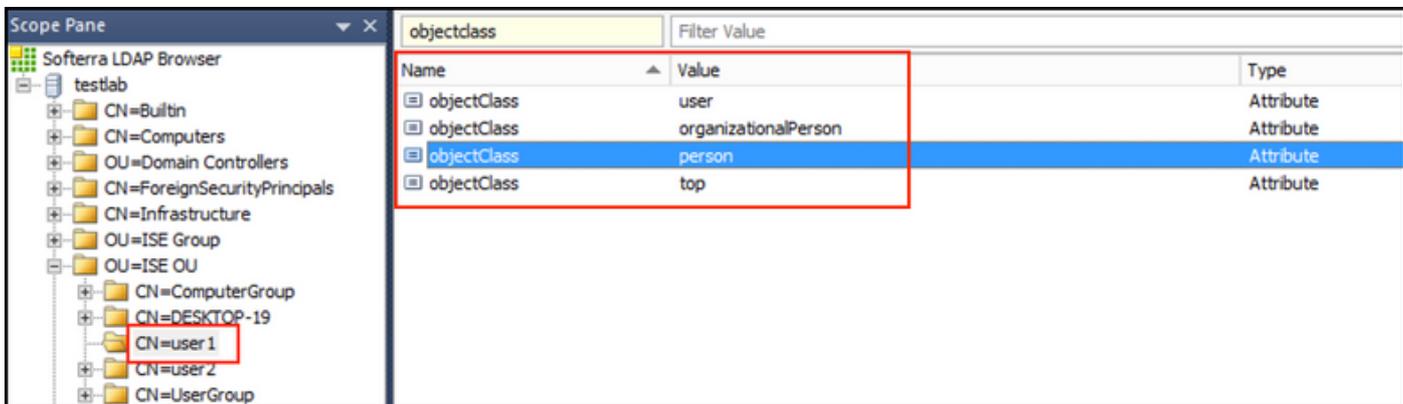
3. Afin d'intégrer le serveur LDAP, utilisez les différents attributs LDAP du répertoire LDAPS. Accédez à Administration > Identity Management > External Identity Sources > LDAP Identity Sources > Add.



4. Configurez ces attributs dans l'onglet Général :

Subject Object Class : ce champ correspond à la classe Object des comptes d'utilisateurs. Vous pouvez utiliser l'une des quatre classes suivantes :

- Haut
- Personne
- PersonneOrganisationnelle
- PersonnelnetOrg



Subject Name Attribute : ce champ est le nom de l'attribut contenant le nom d'utilisateur de la demande. Cet attribut est récupéré à partir du LDAP lorsque l'ISE recherche un nom d'utilisateur

spécifique dans la base de données LDAP (vous pouvez utiliser cn, sAMAccountName, etc.). Dans ce scénario, le nom d'utilisateur user1 du point d'extrémité est utilisé.

Scope Pane: Softerra LDAP Browser, testlab

Filter Name: user1

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

Attribut de nom de groupe : attribut contenant le nom d'un groupe. Les valeurs d'attribut Nom de groupe de votre annuaire LDAP doivent correspondre aux noms de groupe LDAP sur la page Groupes d'utilisateurs

Scope Pane: Softerra LDAP Browser, testlab

Name	Value	Type
cn	UserGroup	Attribute
distinguishedName	CN=UserGroup,OU=ISE OU,DC=testlab,DC=com	Attribute
dSCorePropagationData	1/1/1601	Attribute
groupType	[GlobalScope, Security]	Attribute
instanceType	[Writable]	Attribute
member	CN=user1,OU=ISE OU,DC=testlab,DC=com	Attribute
member	CN=user2,OU=ISE OU,DC=testlab,DC=com	Attribute
name	UserGroup	Attribute
objectCategory	CN=Group,CN=Schema,CN=Configuration,DC=testlab,DC=com	Attribute
objectClass	group	Attribute
objectClass	top	Attribute
sAMAccountName	UserGroup	Attribute
sAMAccountType	< samGroupObject >	Attribute

Group Object Class : cette valeur est utilisée dans les recherches pour spécifier les objets reconnus comme groupes.

Scope Pane: Softerra LDAP Browser, testlab

objectSid	S-1-5-21-2960284039-4006096050-347662626-1156	Binary Attribute
objectGUID	{39967F90-89BE-44B5-9CC5-828C080EB234}	Binary Attribute
objectClass	top	Attribute
objectClass	group	Attribute
objectCategory	CN=Group,CN=Schema,CN=Configuration,DC=testlab,DC=com	Attribute

Attribut de mappage de groupe : cet attribut définit la façon dont les utilisateurs sont mappés aux groupes.

Scope Pane: Softerra LDAP Browser, testlab

Filter Name: UserGroup

Name	Value	Type
memberOf	CN=UserGroup,OU=ISE OU,DC=testlab,DC=com	Attribute

Certificate Attribute : saisissez l'attribut qui contient les définitions de certificat. Ces définitions peuvent éventuellement être utilisées pour valider les certificats présentés par les clients lorsqu'ils sont définis dans le cadre d'un profil d'authentification de certificat. Dans ce cas, une comparaison binaire est effectuée entre le certificat client et le certificat récupéré à partir de la source d'identité LDAP.



5. Afin de configurer la connexion LDAPS, accédez à l'onglet Connection :

LDAP Identity Sources List > testlab_idaps

LDAP Identity Source

General **Connection** Directory Organization Groups Attributes Advanced Settings

Primary Server

* Hostname/IP ⓘ

* Port

Specify server for each ISE node

Access Anonymous Access Authenticated Access

Admin DN ⓘ

Password

Secure Authentication Enable Secure Authentication Enable Server Identity Check

LDAP Server Root CA ⓘ

Issuer CA of ISE Certificates ⓘ

Secondary Server

Enable Secondary Server

Hostname/IP ⓘ

Port

Access Anonymous Access Authenticated Access

Admin DN

Password

Secure Authentication Enable Secure Authentication Enable Server Identity Check

LDAP Server Root CA ⓘ

Issuer CA of ISE Certificates ⓘ

* Server Timeout ⓘ Seconds

* Max. Admin Connections ⓘ

Force reconnect every ⓘ Minutes

Failover Always Access Primary Server First Failback To Primary Server After Minutes

Server Timeout ⓘ Seconds

Max. Admin Connections ⓘ

Force reconnect every ⓘ Minutes

6. Exécutez dsquery sur le contrôleur de domaine pour obtenir le nom d'utilisateur DN à utiliser pour établir une connexion au serveur LDAP :

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

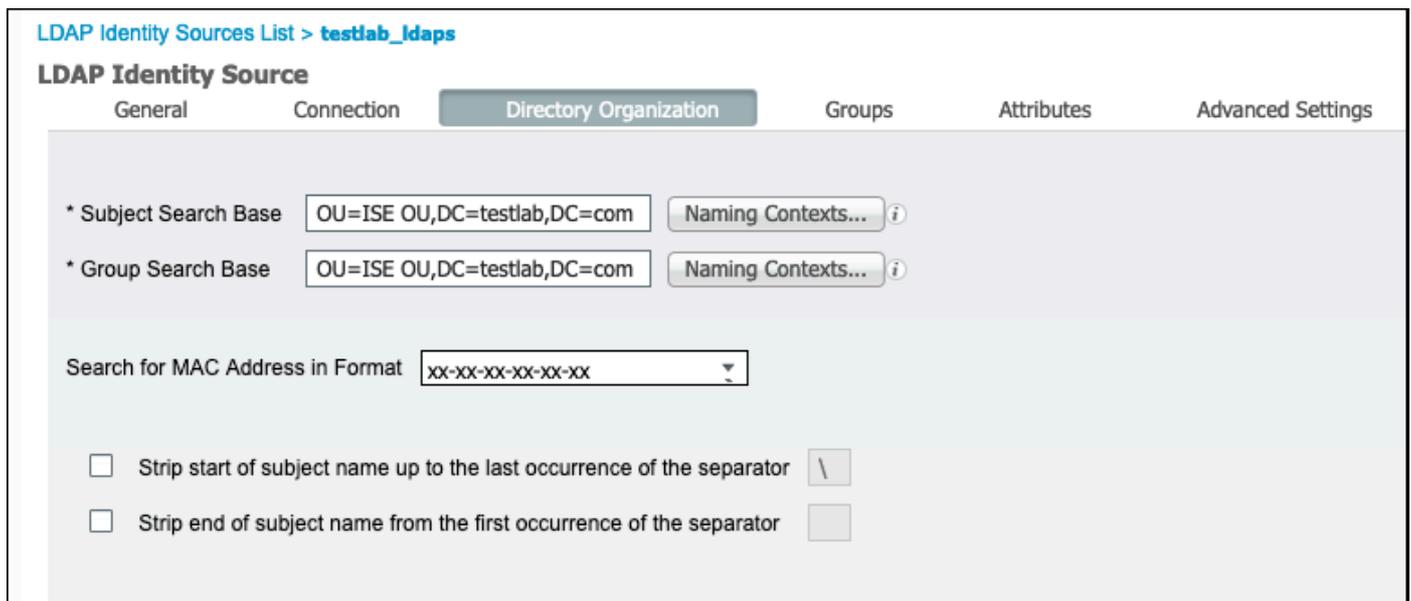
Étape 1. Définissez l'adresse IP ou le nom d'hôte du serveur LDAP, définissez le port LDAP (TCP 636) et le nom de domaine d'administration pour établir une connexion avec le serveur LDAP via SSL.

Étape 2. Option Activer l'authentification sécurisée et la vérification de l'identité du serveur.

Étape 3. Dans le menu déroulant, sélectionnez le certificat d'autorité de certification racine du serveur LDAP et le certificat d'administration ISE certificat d'autorité de certification de l'utilisateur (nous avons utilisé l'autorité de certification, installée sur le même serveur LDAP pour émettre également le certificat d'administration ISE).

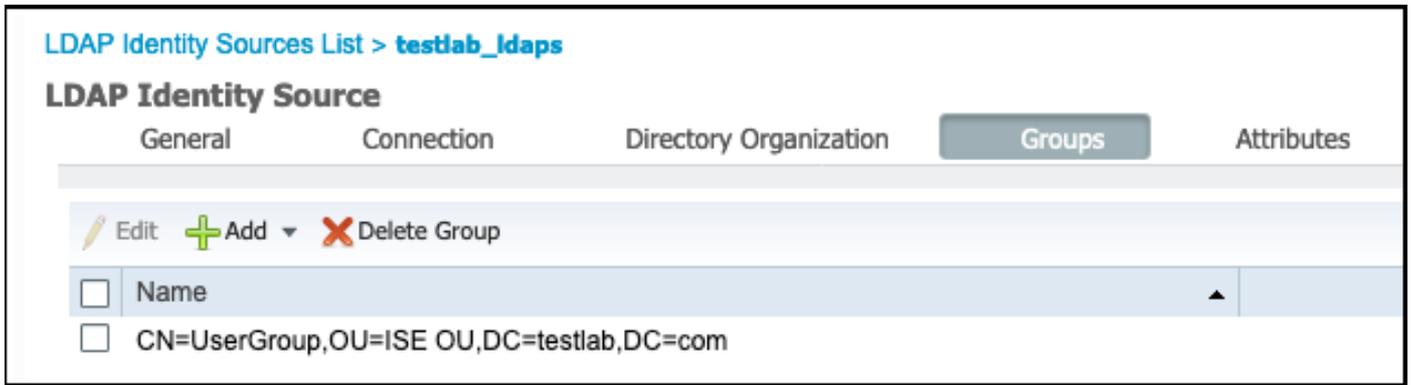
Étape 4. Sélectionnez le test de liaison au serveur. À ce stade, les sujets ou les groupes ne sont pas récupérés car les bases de recherche ne sont pas encore configurées.

7. Sous l'onglet Directory Organization, configurez la base de recherche de sujet/groupe. Il s'agit du point de jonction entre l'ISE et le LDAP. Vous pouvez désormais récupérer uniquement les sujets et les groupes qui sont des enfants du point de jonction. Dans ce scénario, l'objet et le groupe sont récupérés à partir de l'unité d'organisation OU=ISE



The screenshot shows the 'LDAP Identity Source' configuration page for 'testlab_ldaps'. The 'Directory Organization' tab is selected. The 'Subject Search Base' and 'Group Search Base' are both set to 'OU=ISE OU,DC=testlab,DC=com'. Below these, there is a 'Search for MAC Address in Format' dropdown menu with the value 'xx-xx-xx-xx-xx-xx'. At the bottom, there are two checkboxes: 'Strip start of subject name up to the last occurrence of the separator' (unchecked) and 'Strip end of subject name from the first occurrence of the separator' (unchecked).

8. Sous Groupes, cliquez sur Ajouter pour importer les groupes à partir du serveur LDAP sur l'ISE et récupérer les groupes, comme illustré dans cette image.



Configuration du commutateur

Configurez le commutateur pour l'authentification 802.1x. Le PC Windows est connecté au port de commutation 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
!

!

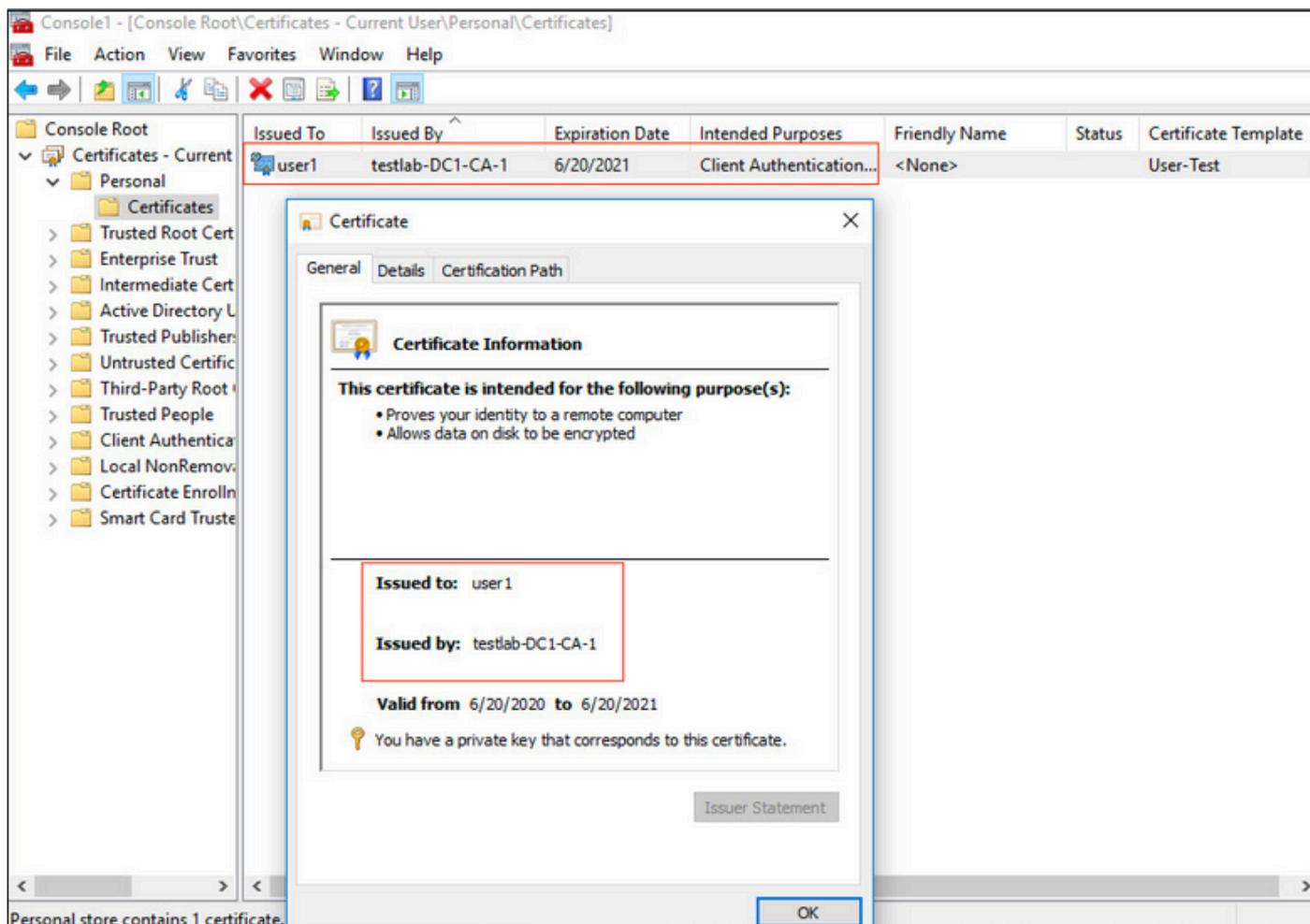
interface GigabitEthernet2/0/47
switchport access vlan xx
switchport mode access
authentication port-control auto
dot1x pae authenticator

```

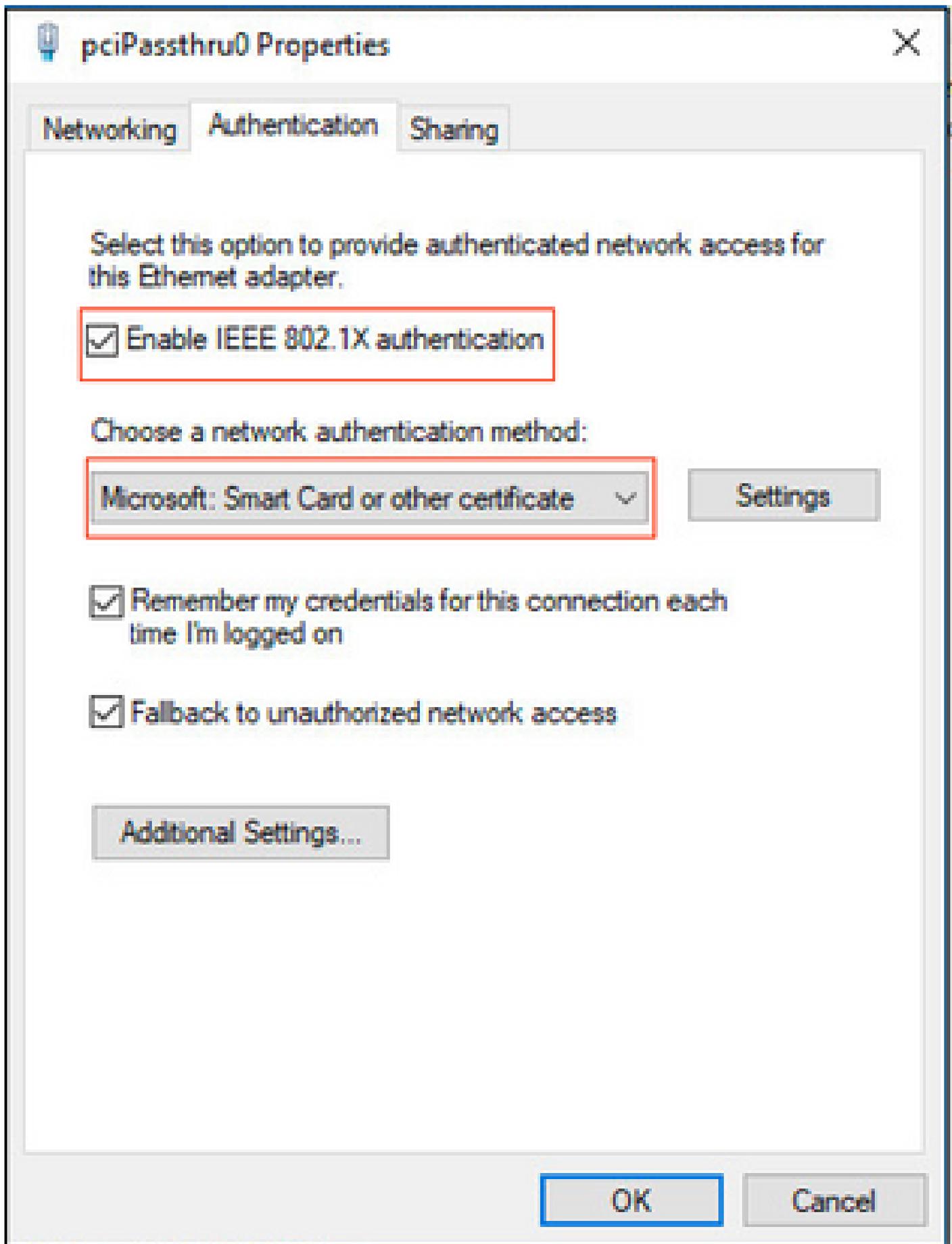
Configuration du terminal

Le demandeur natif Windows est utilisé et l'un des protocoles EAP pris en charge par LDAP est utilisé, EAP-TLS pour l'authentification et l'autorisation des utilisateurs.

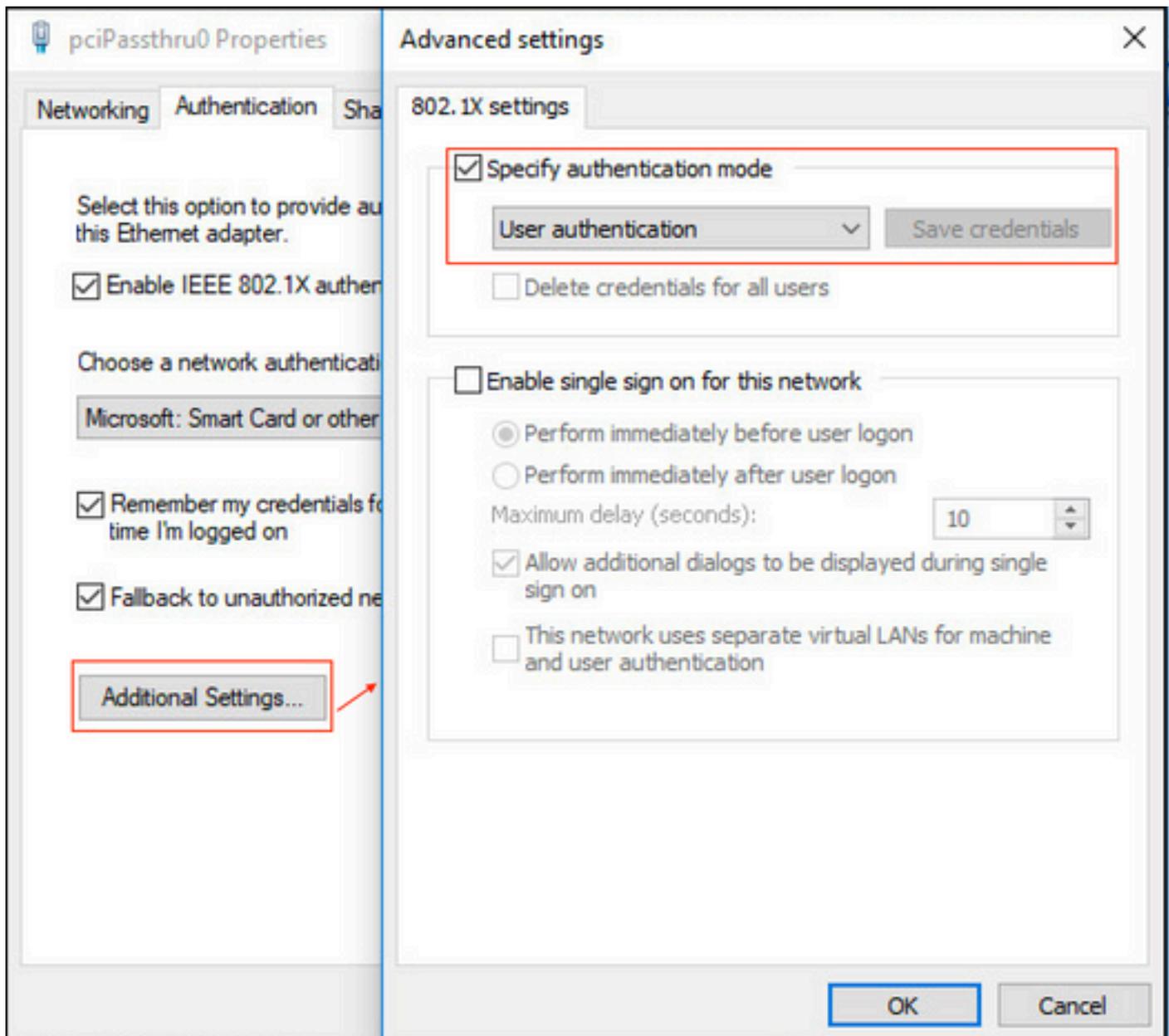
1. Assurez-vous que le PC est doté d'un certificat utilisateur (pour l'utilisateur 1) et qu'il a l'objectif d'authentifier le client et que, dans les autorités de certification racines de confiance, la chaîne de certificats de l'émetteur est présente sur le PC.



2. Activez l'authentification Dot1x et sélectionnez la méthode d'authentification Microsoft : Smart Card ou un autre certificat pour l'authentification EAP-TLS.

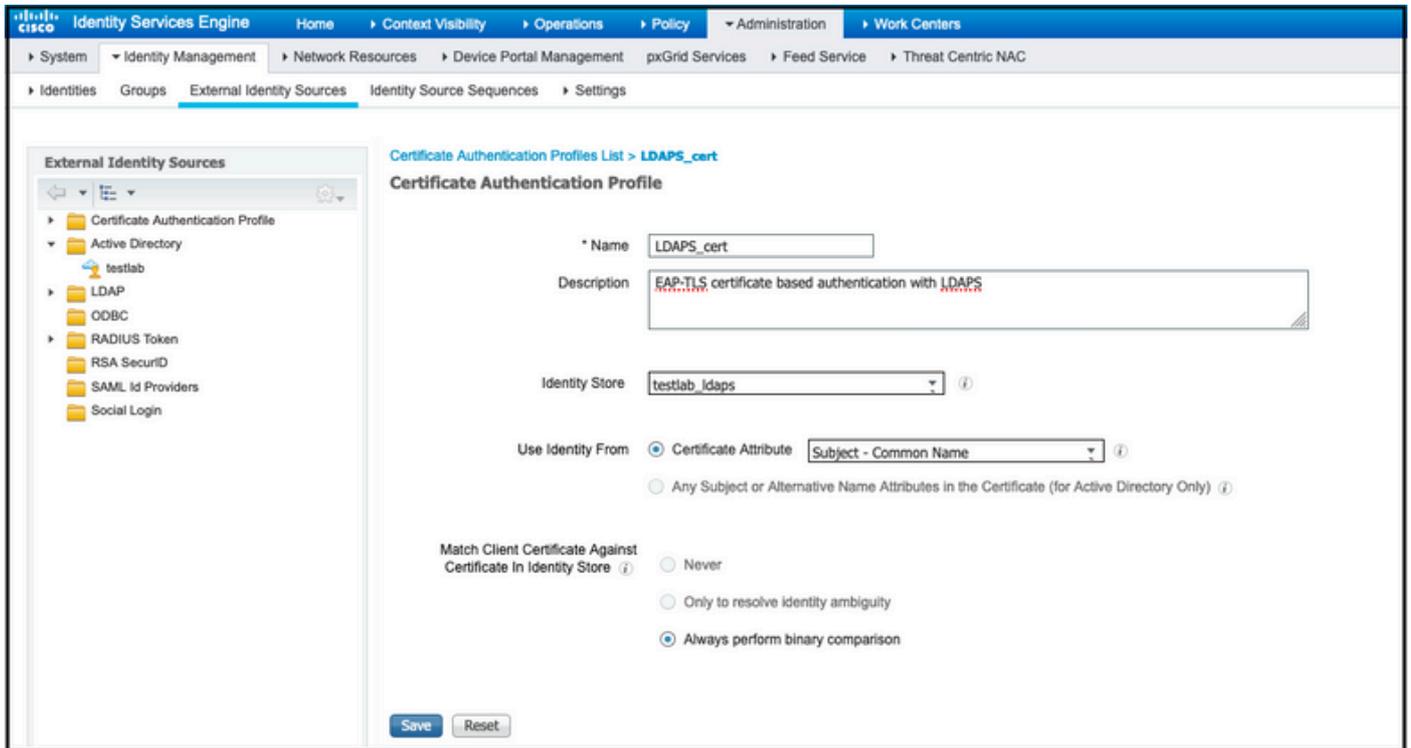


3. Cliquez sur Additional Settings et une fenêtre s'ouvre. Cochez la case en spécifiant le mode d'authentification et choisissez l'authentification de l'utilisateur, comme illustré dans cette image.



Configurer le jeu de stratégies sur ISE

Puisque le protocole EAP-TLS est utilisé, avant que le jeu de stratégies soit configuré, le profil d'authentification de certificat doit être configuré et la séquence source d'identité est utilisée dans la stratégie d'authentification plus tard.



Reportez-vous au profil d'authentification de certificat dans la séquence de source d'identité et définissez la source d'identité externe LDAPS dans la liste de recherche d'authentification :

Identity Services Engine 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: LDAPS

Description:

Certificate Based Authentication

Select Certificate Authentication Profile: LDAPS_cert

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

Save Reset

Configurez maintenant le jeu de stratégies pour l'authentification Wired Dot1x :

Identity Services Engine Administration Work Centers License Warning

Policy Sets Profiling Posture Client Provisioning Policy Elements

Policy Sets → Wired Dot1x

Reset Policyset Hitcounts Reset Save

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits
✔	Wired Dot1x		Wired_802.1X	Default Network Access	453

Authentication Policy (2)

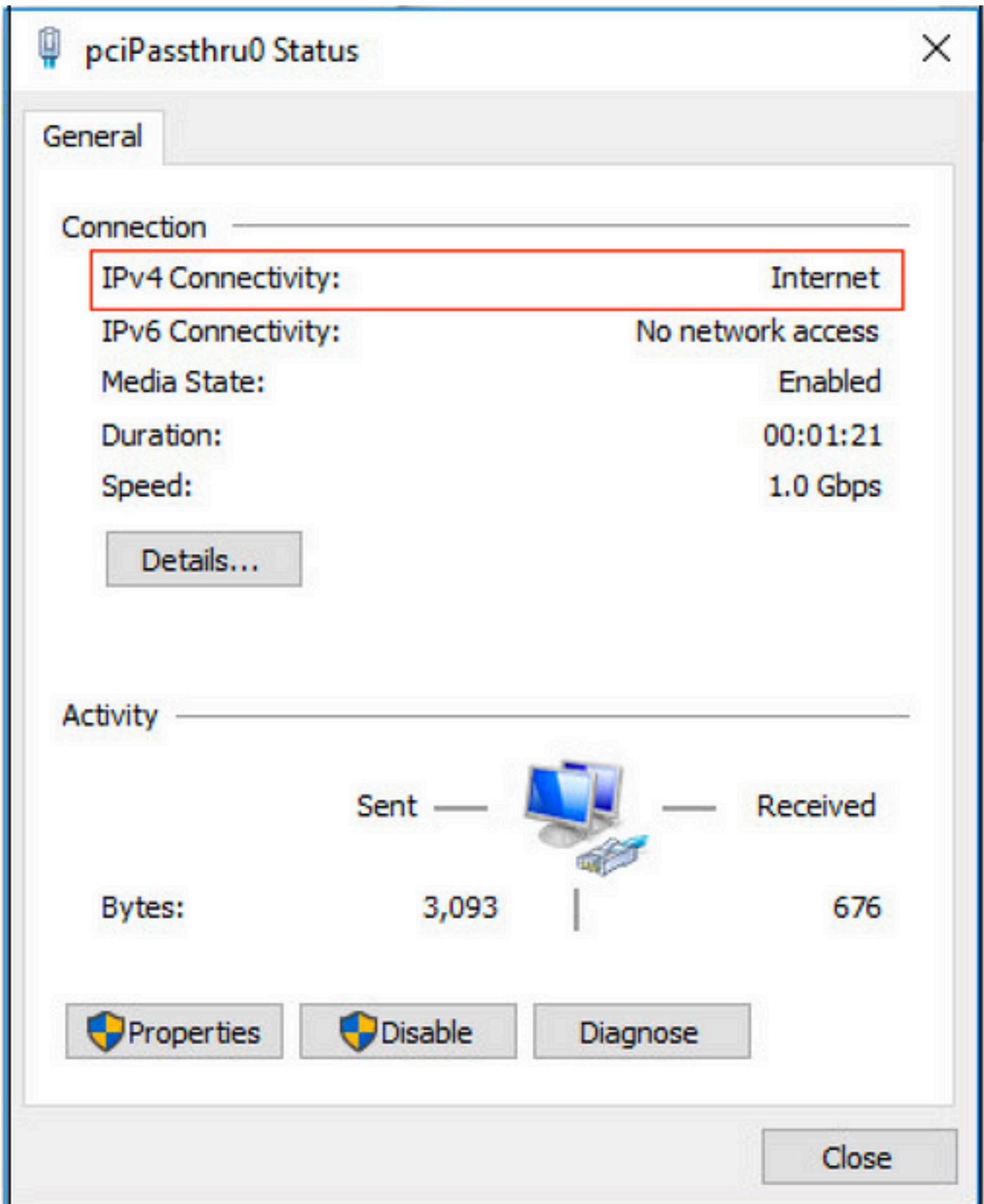
Status	Rule Name	Conditions	Use	Hits	Actions
✔	Dot1x	Network Access-NetworkDeviceName EQUALS LAB-Switch	LDAPS	223	Options
✔	Default		LDAPS	0	Options

Authorization Policy (2)

+	Status	Rule Name	Conditions	Results			Hits	Actions	
				Profiles	Security Groups				
Search									
+	✔	Users in LDAP Store	testlab_idaps-ExternalGroups EQUALS CN=UserGroup,OU=ISE OU,DC=testlab,DC=com	PermitAccess	+	Select from list	+	207	⚙
+	✔	Default		DenyAccess	+	Select from list	+	11	⚙

Reset Save

Après cette configuration, nous pouvons authentifier le terminal à l'aide du protocole EAP-TLS par rapport à la source d'identité LDAPS.



Vérifier

1. Vérifiez la session d'authentification sur le port de commutation connecté au PC :

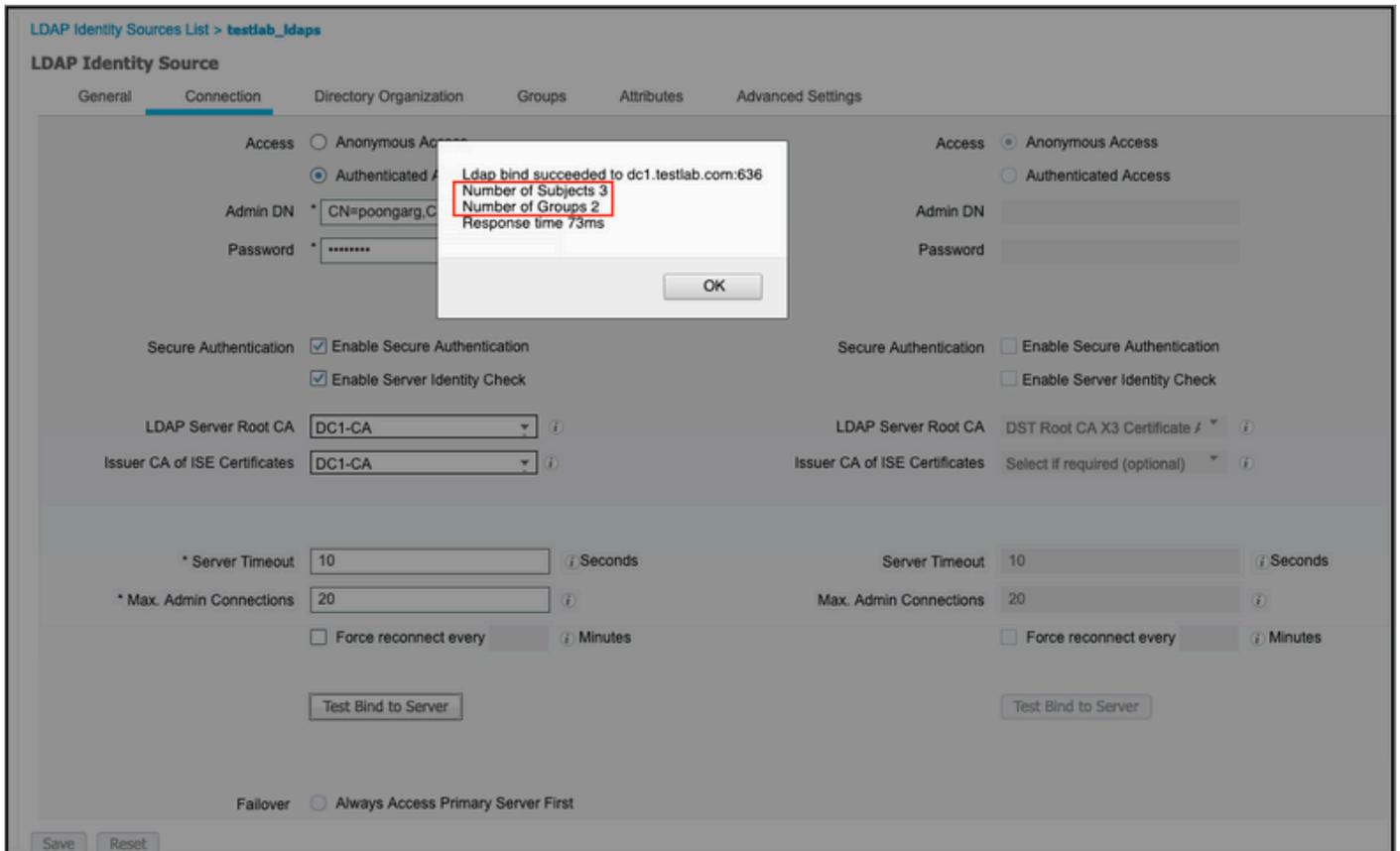
```
SW1#sh auth sessions int g2/0/47 de
      Interface: GigabitEthernet2/0/47
      MAC Address: b496.9126.dec0
      IPv6 Address: Unknown
      IPv4 Address: 10.106.38.165
      User-Name: user1
      Status: Authorized
      Domain: DATA
      Oper host mode: single-host
      Oper control dir: both
      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. Afin de vérifier les configurations LDAPS et ISE, vous pouvez récupérer les sujets et les groupes avec une connexion test au serveur :



3. Vérifiez le rapport d'authentification utilisateur :

Time	Status	Details	Identity	Endpoint ID	Authentication Po...	Authorization Policy	Authorization Profi...	Network De...	Device Port	Authentication Pro...
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		GigabitEthernet2/0/47	EAP-TLS
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	LAB-Switch	GigabitEthernet2/0/47	EAP-TLS

4. Consultez le rapport d'authentification détaillé pour le terminal :

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. Validez que les données sont chiffrées entre le serveur ISE et le serveur LDAPS en effectuant une capture de paquets sur le serveur ISE vers le serveur LDAPS :

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 SACK_PERM=1 TSval=140972872 TSecr=0 WS=128
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 MSS=1460 WS=256 SACK_PERM=1 TSval=30158962 TSecr=140972872
22	2020-06-24 10:40:24.206613	10.197.164.22	10.197.164.21	TCP	66	00:0c:29:98:ca:28,0...		28057 → 636 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=140972873 TSecr=30158962
23	2020-06-24 10:40:24.206961	10.197.164.22	10.197.164.21	TLSv1.2	207	00:0c:29:98:ca:28,0...		Client Hello
24	2020-06-24 10:40:24.210413	10.197.164.21	10.197.164.22	TLSv1.2	2036	00:50:56:a0:3e:7f,0...		Server Hello, Certificate [Packet size limited during capture]
25	2020-06-24 10:40:24.210588	10.197.164.22	10.197.164.21	TCP	66	00:0c:29:98:ca:28,0...		28057 → 636 [ACK] Seq=142 Ack=1971 Win=33152 Len=0 TSval=140972877 TSecr=30158962
26	2020-06-24 10:40:24.215211	10.197.164.22	10.197.164.21	TLSv1.2	260	00:0c:29:98:ca:28,0...		Certificate, Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
27	2020-06-24 10:40:24.218678	10.197.164.21	10.197.164.22	TLSv1.2	173	00:50:56:a0:3e:7f,0...		Change Cipher Spec, Encrypted Handshake Message
28	2020-06-24 10:40:24.219113	10.197.164.22	10.197.164.21	TLSv1.2	199	00:0c:29:98:ca:28,0...		Application Data
29	2020-06-24 10:40:24.230384	10.197.164.21	10.197.164.22	TLSv1.2	167	00:50:56:a0:3e:7f,0...		Application Data
30	2020-06-24 10:40:24.231712	10.197.164.22	10.197.164.21	TLSv1.2	279	00:0c:29:98:ca:28,0...		Application Data
31	2020-06-24 10:40:24.238889	10.197.164.21	10.197.164.22	TLSv1.2	1879	00:50:56:a0:3e:7f,0...		Application Data [Packet size limited during capture]
32	2020-06-24 10:40:24.238958	10.197.164.22	10.197.164.21	TCP	66	00:0c:29:98:ca:28,0...		28057 → 636 [ACK] Seq=682 Ack=3992 Win=36864 Len=0 TSval=140972905 TSecr=30158965
33	2020-06-24 10:40:24.251944	10.197.164.22	10.197.164.21	TLSv1.2	263	00:0c:29:98:ca:28,0...		Application Data
34	2020-06-24 10:40:24.253658	10.197.164.21	10.197.164.22	TLSv1.2	295	00:50:56:a0:3e:7f,0...		Application Data
35	2020-06-24 10:40:24.293322	10.197.164.22	10.197.164.21	TCP	66	00:0c:29:98:ca:28,0...		28057 → 636 [ACK] Seq=879 Ack=4221 Win=39680 Len=0 TSval=140972960 TSecr=30158967
86	2020-06-24 10:40:57.946553	10.197.164.22	10.197.164.21	TCP	151	00:0c:29:98:ca:28,0...		Application Data
87	2020-06-24 10:40:57.947600	10.197.164.22	10.197.164.21	TCP	66	00:0c:29:98:ca:28,0...		28057 → 636 [FIN, ACK] Seq=964 Ack=4221 Win=39680 Len=0 TSval=141006614 TSecr=30158967

```

> Frame 28: 199 bytes on wire (1592 bits), 199 bytes captured (1592 bits)
> Ethernet II, Src: Vmware_00:3e: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: 17301b0b2f280a13cc17815e54447bb9ac8af8a881a9eb84...
  <-- Encrypted Data
  
```

Dépannage

Cette section décrit quelques erreurs courantes rencontrées avec cette configuration et explique comment les résoudre.

- Dans le rapport d'authentification, vous pouvez voir le message d'erreur suivant :

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

Ce message d'erreur indique que la méthode sélectionnée n'est pas prise en charge par LDAP. Assurez-vous que le protocole d'authentification dans le même rapport affiche l'une des méthodes prises en charge (EAP-GTC, EAP-TLS ou PEAP-TLS).

- Le test de liaison au serveur s'est terminé par une erreur.

Cela est généralement dû à l'échec du contrôle de validation du certificat du serveur LDAP. Afin de dépanner de tels types de problèmes, prenez une capture de paquets sur ISE et activez les trois composants runtime et prt-jni au niveau du débogage, recréez le problème et vérifiez le fichier prt-server.log.

La capture de paquets se plaint d'un certificat incorrect et port-server affiche :

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

 Remarque : le nom d'hôte de la page LDAP doit être configuré avec le nom du sujet du certificat (ou l'un des autres noms du sujet). Par conséquent, à moins que vous ne disposiez d'une telle adresse dans l'objet ou dans le SAN, cela ne fonctionne pas, le certificat avec l'adresse IP dans la liste SAN est nécessaire.

3. Dans le rapport d'authentification, vous pouvez remarquer que l'objet est introuvable dans le magasin d'identités. Cela signifie que le nom d'utilisateur du rapport ne correspond pas à l'attribut Nom de l'objet d'un utilisateur de la base de données LDAP. Dans ce scénario, la valeur a été définie sur sAMAccountName pour cet attribut, ce qui signifie que l'ISE recherche les valeurs sAMAccountName pour l'utilisateur LDAP lorsqu'il tente de trouver une correspondance.

4. Les sujets et les groupes n'ont pas pu être récupérés correctement lors d'un test de liaison au serveur. La cause la plus probable de ce problème est une configuration incorrecte pour les bases de recherche. N'oubliez pas que la hiérarchie LDAP doit être spécifiée de leaf à root et dc (peut être constituée de plusieurs mots).

Informations connexes

- <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>

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.