

外部LDAPS IDストアを使用したISEの設定およびトラブルシューティング

内容

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[設定](#)

[ネットワーク図](#)

[Active DirectoryでのLDAPSの設定](#)

[ドメインコントローラへのID証明書のインストール](#)

[LDAPSディレクトリ構造へのアクセス](#)

[ISEとLDAPSサーバの統合](#)

[スイッチの設定](#)

[エンドポイントの設定](#)

[ISEでのポリシーセットの設定](#)

[確認](#)

[トラブルシュート](#)

[関連情報](#)

はじめに

このドキュメントでは、Cisco ISEとSecure LDAPSサーバを外部アイデンティティソースとして統合する方法について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- Identity Service Engine(ISE)の管理に関する基礎知識
- Active Directory/Secure Lightweight Directory Access Protocol(LDAPS)の基礎知識

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Cisco ISE 2.6パッチ7
- Active DirectoryライトウェイトディレクトリサービスがインストールされているMicrosoft

Windowsバージョン2012 R2

- ネイティブアプリケーションとユーザ証明書がインストールされたWindows 10 OS PC
- CiscoスイッチC3750X (152-2.E6イメージ搭載)

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな (デフォルト) 設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

背景説明

LDAPSを使用すると、ディレクトリバインドが確立されたときに、転送中のLDAPデータ (ユーザクレデンシャルを含む) を暗号化できます。LDAPSはTCPポート636を使用します。

LDAPSでは、次の認証プロトコルがサポートされています。

- EAP汎用トークンカード(EAP-GTC)
- Password Authentication Protocol (PAP; パスワード認証プロトコル)
- EAP Transport Layer Security(EAP-TLS)
- Protected EAP Transport Layer Security(PEAP-TLS)

 注:EAP-MSCHAPV2 (PEAP、EAP-FAST、またはEAP-TTLSの内部方式)、LEAP、CHAP、およびEAP-MD5は、LDAPS外部アイデンティティソースではサポートされません。

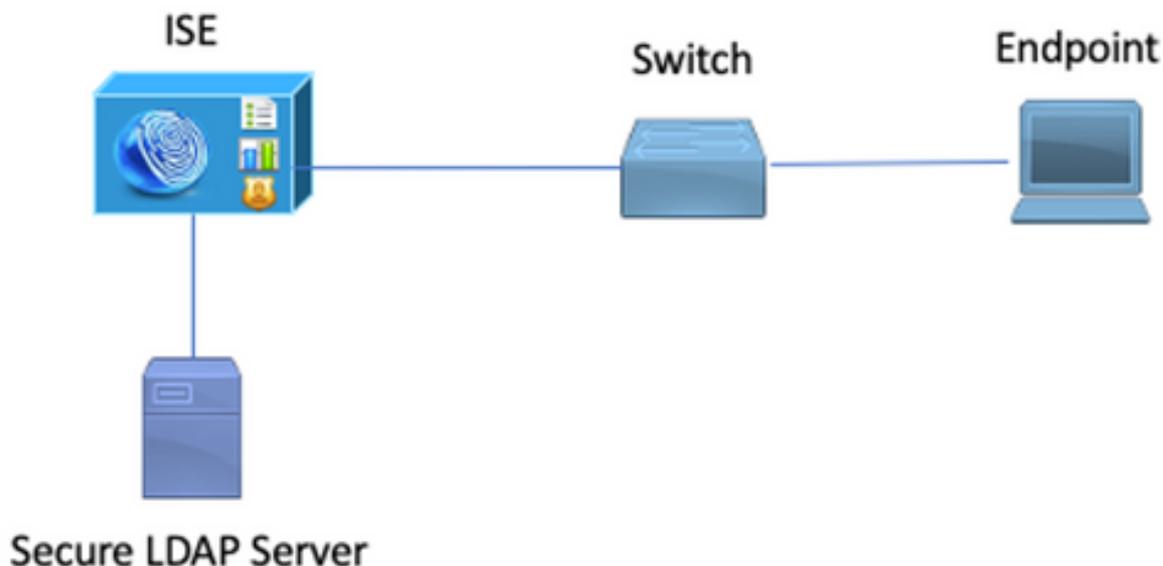
設定

このセクションでは、ネットワークデバイスの設定と、ISEとMicrosoft Active Directory(AD)LDAPSサーバの統合について説明します。

ネットワーク図

この設定例では、エンドポイントはスイッチとのイーサネット接続を使用して、ローカルエリアネットワーク(LAN)に接続します。接続されたスイッチポートは、ISEでユーザを認証するために802.1x認証用に設定されます。ISEでは、LDAPSは外部IDストアとして設定されます。

次の図に、使用するネットワークトポロジを示します。

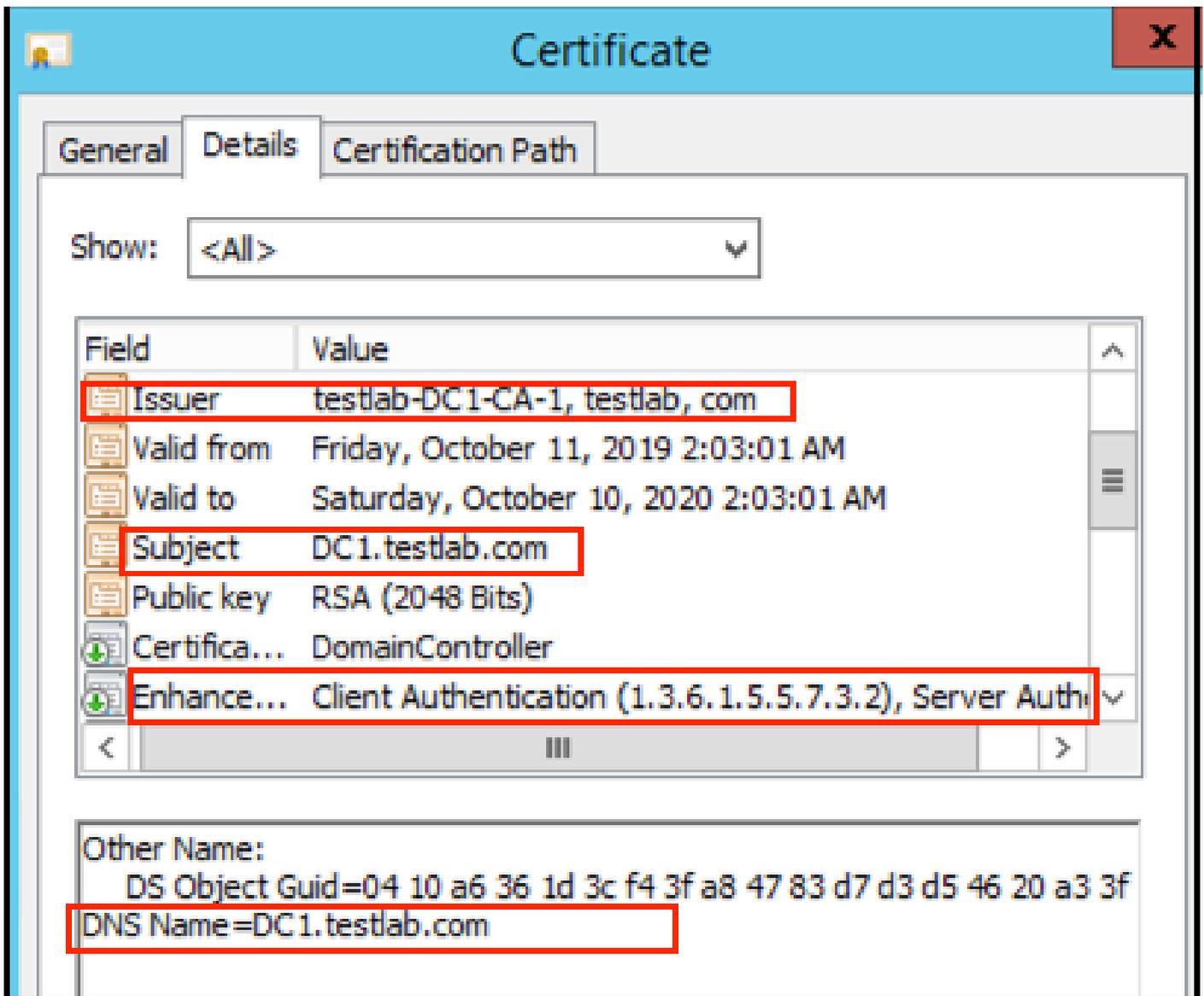


Active DirectoryでのLDAPSの設定

ドメインコントローラへのID証明書のインストール

LDAPSを有効にするには、次の要件を満たす証明書をドメインコントローラ(DC)にインストールします。

1. LDAPS証明書は、ドメインコントローラの個人証明書ストアにあります。
2. 証明書に一致する秘密キーがドメインコントローラのストアにあり、証明書に正しく関連付けられています。
3. 拡張キー使用法(EKU)拡張には、サーバ認証(1.3.6.1.5.5.7.3.1)オブジェクト識別子 (OIDとも呼ばれる) が含まれています。
4. ドメインコントローラの完全修飾ドメイン名(FQDN) (DC1.testlab.comなど)は、次のいずれかの属性に含まれている必要があります: [件名]フィールドの共通名(CN)、[サブジェクトの別名]拡張のDNSエントリ。
5. 証明書は、ドメインコントローラとLDAPSクライアントが信頼する認証局(CA)によって発行される必要があります。信頼できるセキュアな通信を実現するには、クライアントとサーバは互いのルートCAと、証明書を発行した中間CA証明書を信頼する必要があります。
6. キーを生成するには、Schannel暗号化サービスプロバイダー(CSP)を使用する必要があります。



LDAPSディレクトリ構造へのアクセス

Active Directoryサーバ上のLDAPSディレクトリにアクセスするには、任意のLDAPブラウザを使用します。この実習では、Softerra LDAPブラウザ4.5を使用します。

1. TCPポート636でドメインへの接続を確立します。



2. 分かりやすくするために、ADにISE OUという名前の組織単位(OU)を作成します。この組織単位には、UserGroupという名前のグループが必要です。2人のユーザ (user1とuser2) を作成し、グループUserGroupのメンバーにします。

 注:ISEのLDAPアイデンティティソースは、ユーザ認証にのみ使用されます。

Name	Value	Type
OU=ISE OU		
OU=LABISE		
CN=user1		
CN=user2		
CN=UserGroup		
CN=ComputerGroup		
CN=DESKTOP-19		
CN=ComputerGroup		
CN=	ComputerGroup	Entry
CN=	DESKTOP-19	Entry
CN=	user1	Entry
CN=	user2	Entry
CN=	UserGroup	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

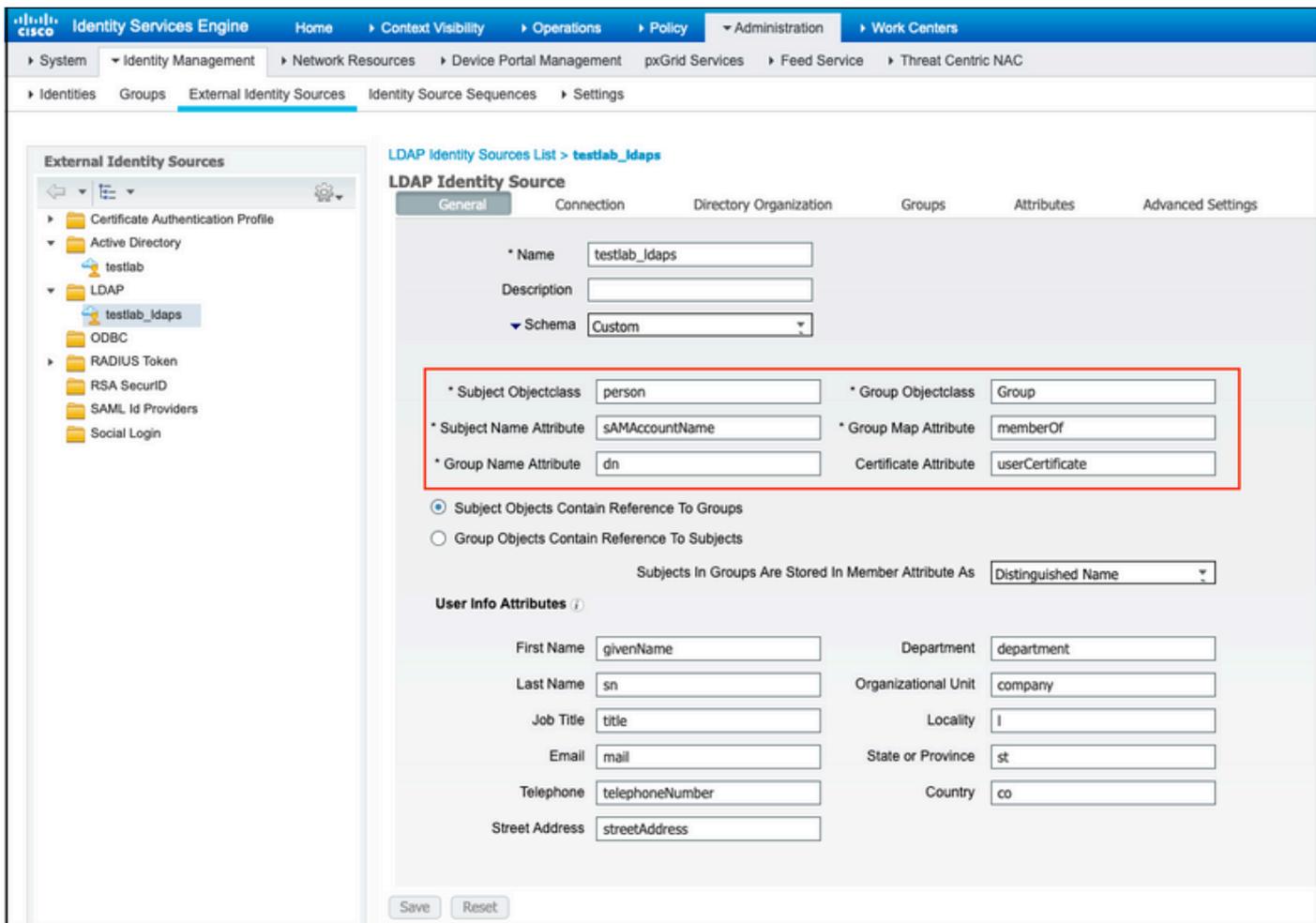
ISEとLDAPSサーバの統合

1.信頼できる証明書にLDAPサーバのルートCA証明書をインポートします。

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. ISE管理証明書を検証し、ISE管理証明書発行者証明書が信頼できる証明書ストアにも存在することを確認します。

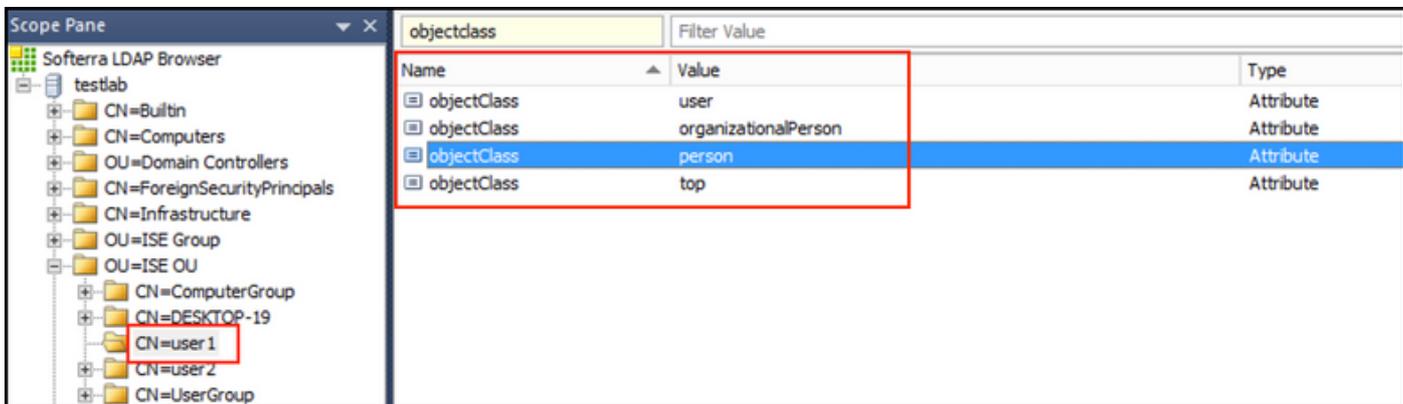
3. LDAPSサーバを統合するには、LDAPSディレクトリのさまざまなLDAP属性を使用します。
Administration > Identity Management > External Identity Sources > LDAP Identity Sources > Addの順に移動します。



4. 「一般」タブから次の属性を構成します。

Subject Objectclass：このフィールドは、ユーザアカウントのObjectクラスに対応しています。ここでは、次の4つのクラスのいずれかを使用できます。

- Top
- Person
- OrganizationalPerson
- InetOrgPerson



サブジェクト名属性：このフィールドは、要求のユーザ名を含む属性の名前です。この属性は、ISEがLDAPデータベースで特定のユーザ名を照会するときLDAPSから取得されます (cn、

sAMAccountNameなどを使用できます)。このシナリオでは、エンドポイントのuser1ユーザ名が使用されます。

LDAP browser showing details for user1. The sAMAccountName attribute is highlighted with a red box.

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

グループ名属性：グループの名前を保持する属性です。LDAPディレクトリのGroup name属性値は、User groupsページのLDAPグループ名と一致している必要があります

LDAP browser showing details for UserGroup. The distinguishedName attribute is highlighted with a red box.

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 Objectclass:この値は、グループとして認識されるオブジェクトを指定するために検索で使用されます。

LDAP browser showing details for UserGroup. The objectClass attribute is highlighted with a red box.

Name	Value	Type
objectSid	S-1-5-21-2960284039-4006096050-347662626-1156	Binary Attribute
objectGUID	{39967F90-89BE-44B5-9CC5-828C0B0EB234}	Binary Attribute
objectClass	top	Attribute
objectClass	group	Attribute
objectCategory	CN=Group,CN=Schema,CN=Configuration,DC=testlab,DC=com	Attribute

グループマップ属性：この属性は、ユーザをグループにマップする方法を定義します。

LDAP browser showing details for user1. The memberOf attribute is highlighted with a red box.

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

Certificate Attribute:証明書定義を含む属性を入力します。これらの定義は、オプションで、証明書認証プロファイルの一部として定義されている場合にクライアントから提示される証明書を検

証するために使用できます。この場合、クライアント証明書とLDAPアイデンティティソースから取得した証明書の間でバイナリ比較が実行されます。



5. LDAPS接続を設定するには、Connectionタブに移動します（図4の矢印Aを参照）。

LDAP Identity Sources List > testlab_ldaps

LDAP Identity Source

General Connection Directory Organization Groups Attributes Advanced Settings

Primary Server

Secondary Server

Enable Secondary Server

* Hostname/IP dc1.testlab.com ⓘ

* Port 636

Hostname/IP ⓘ

Port 389

Specify server for each ISE node

Access Anonymous Access Authenticated Access

Admin DN * CN=poongarg,CN=Users,DC=testlab

Password * *****

Admin DN ⓘ

Password ⓘ

Secure Authentication Enable Secure Authentication Enable Server Identity Check

Secure Authentication Enable Secure Authentication Enable Server Identity Check

LDAP Server Root CA DC1-CA ⓘ

LDAP Server Root CA DST Root CA X3 Certificate Authority ⓘ

Issuer CA of ISE Certificates DC1-CA ⓘ

Issuer CA of ISE Certificates Select if required (optional) ⓘ

* Server Timeout 10 ⓘ Seconds

Server Timeout 10 ⓘ Seconds

* Max. Admin Connections 20 ⓘ

Max. Admin Connections 20 ⓘ

Force reconnect every ⓘ Minutes

Force reconnect every ⓘ Minutes

Test Bind to Server

Test Bind to Server

Failover Always Access Primary Server First Fallback To Primary Server After 5 Minutes

6. ドメインコントローラでdsqueryを実行し、LDAPサーバへの接続に使用するユーザ名DNを取得します。

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

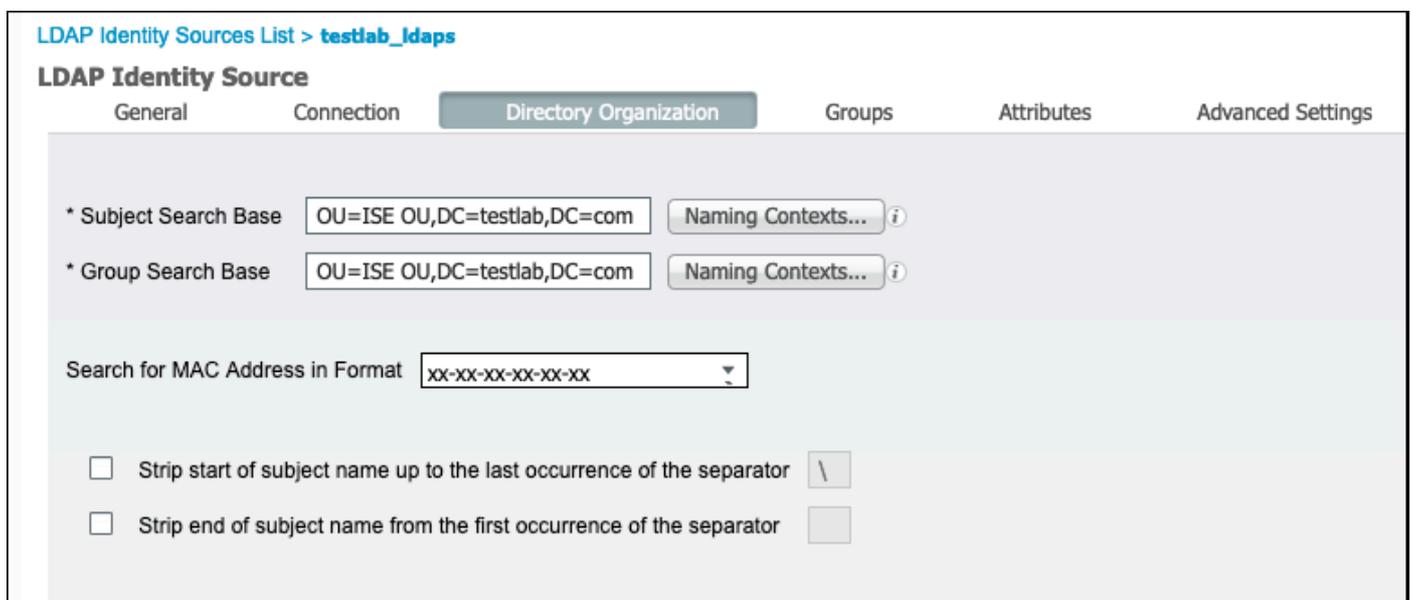
ステップ 1 : Sldapサーバの正しいIPアドレスまたはホスト名を設定し、LDAPポート(TCP 636)とAdmin DNを定義して、LDAP over SSLとの接続を確立します。

ステップ 2 : Secure AuthenticationおよびServer Identity Checkオプションを有効にします。

ステップ 3 : ドロップダウンメニューから、LDAPサーバルートCA証明書とISE管理証明書Issuer CA証明書を選択します (ISE管理証明書を発行するために、同じLDAPサーバにインストールされた認証局を使用しています) 。

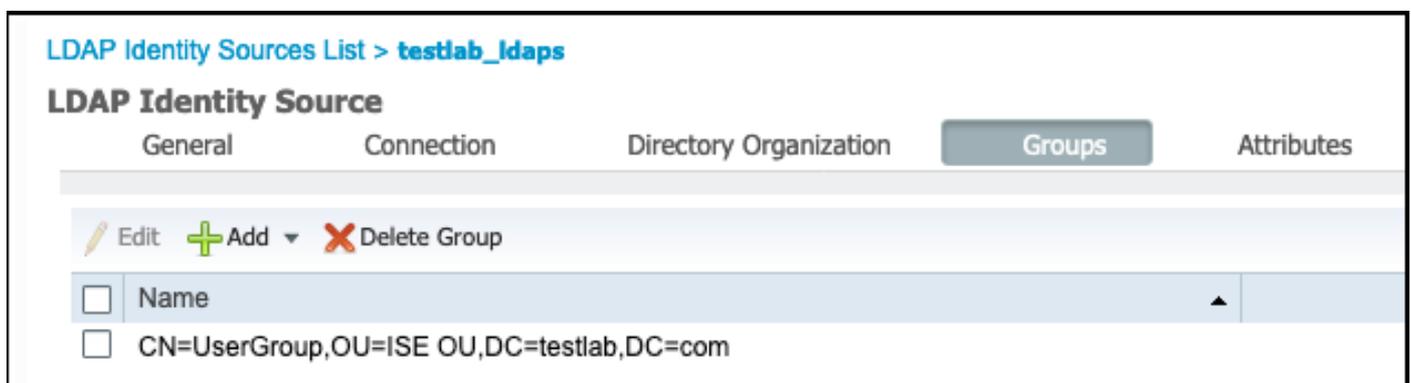
ステップ 4 : サーバへのテストバインドを選択します。この時点では、検索ベースがまだ設定されていないため、サブジェクトまたはグループは取得されません。

7. Directory Organizationタブで、Subject/Group Search Baseを設定します。これはISEからLDAPへの結合ポイントです。これで、結合ポイントの子であるサブジェクトとグループのみを取得できるようになりました。このシナリオでは、サブジェクトとグループの両方がOU=ISE OUから取得されます



The screenshot shows the 'LDAP Identity Source' configuration page for 'testlab_idaps'. The 'Directory Organization' tab is selected. The 'Subject Search Base' and 'Group Search Base' fields are both set to 'OU=ISE OU,DC=testlab,DC=com'. There are 'Naming Contexts...' buttons with information icons next to each. Below these, there is a 'Search for MAC Address in Format' dropdown menu set to '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' (with a backslash separator) and 'Strip end of subject name from the first occurrence of the separator', both of which are currently unchecked.

8. [Groups]で[Add]をクリックして、ISE上のLDAPからグループをインポートし、グループを取得します (次の図を参照) 。



The screenshot shows the 'LDAP Identity Source' configuration page for 'testlab_idaps', now with the 'Groups' tab selected. At the top, there are icons for 'Edit', '+ Add', and 'X Delete Group'. Below this, there is a table with two rows. The first row has a checkbox and the text 'Name'. The second row has a checkbox and the text 'CN=UserGroup,OU=ISE OU,DC=testlab,DC=com'. The table has a scrollable area on the right side.

スイッチの設定

スイッチを802.1x認証用に設定します。スイッチポートGig2/0/47にWindows PCが接続されている

```
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
!

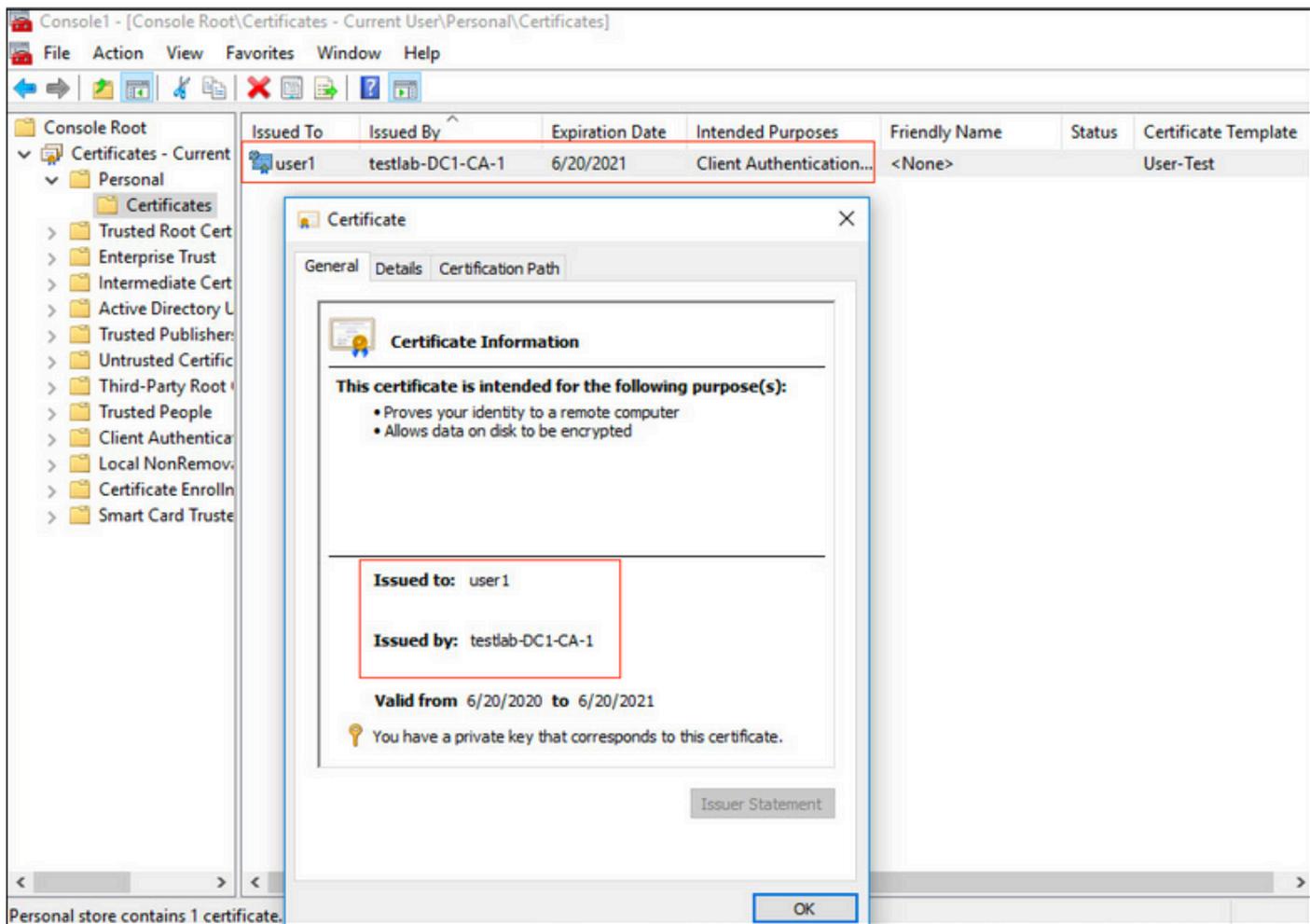
!

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

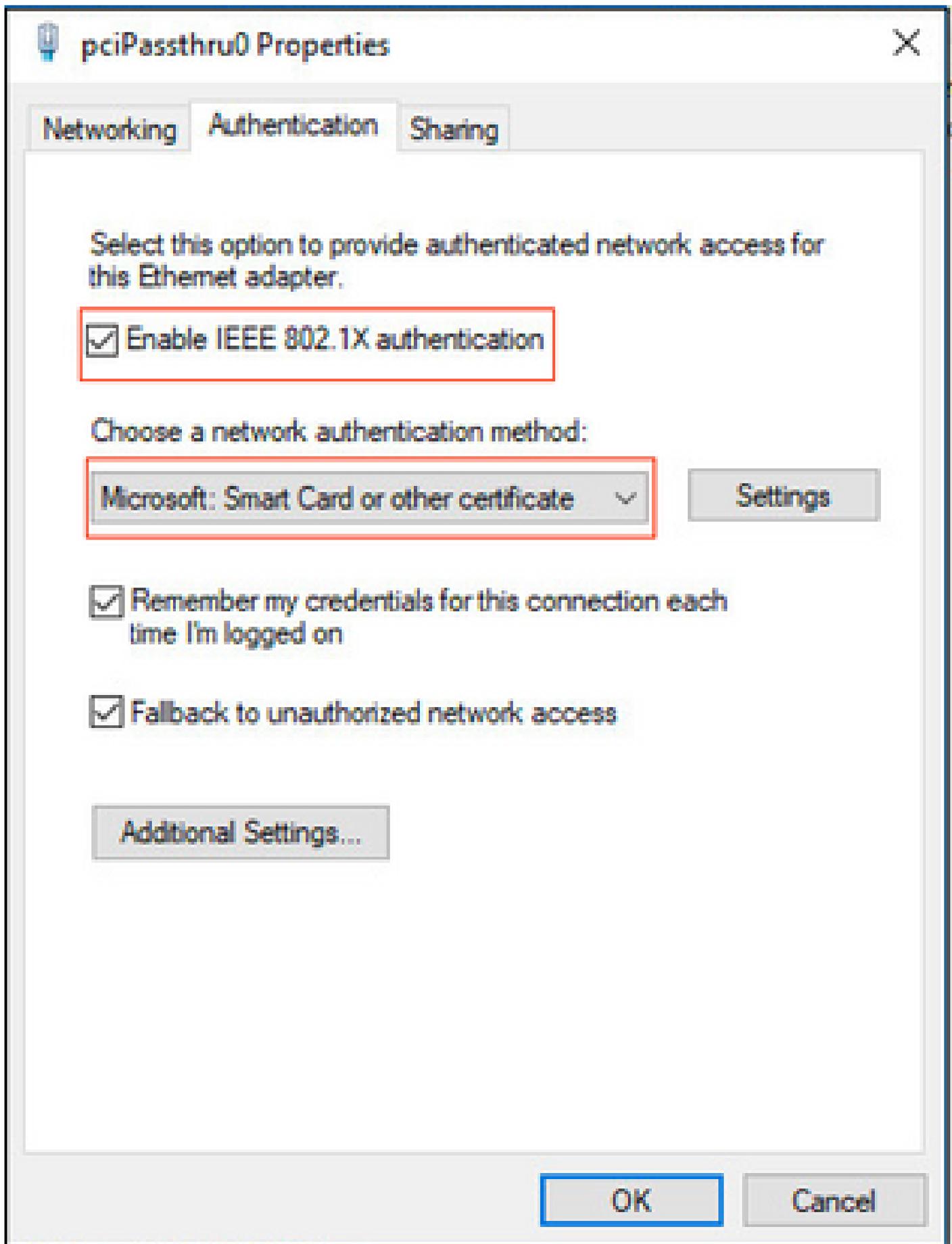
エンドポイントの設定

Windowsネイティブサブリカントが使用され、LDAPでサポートされるEAPプロトコルの1つであるEAP-TLSがユーザ認証と認可に使用されます。

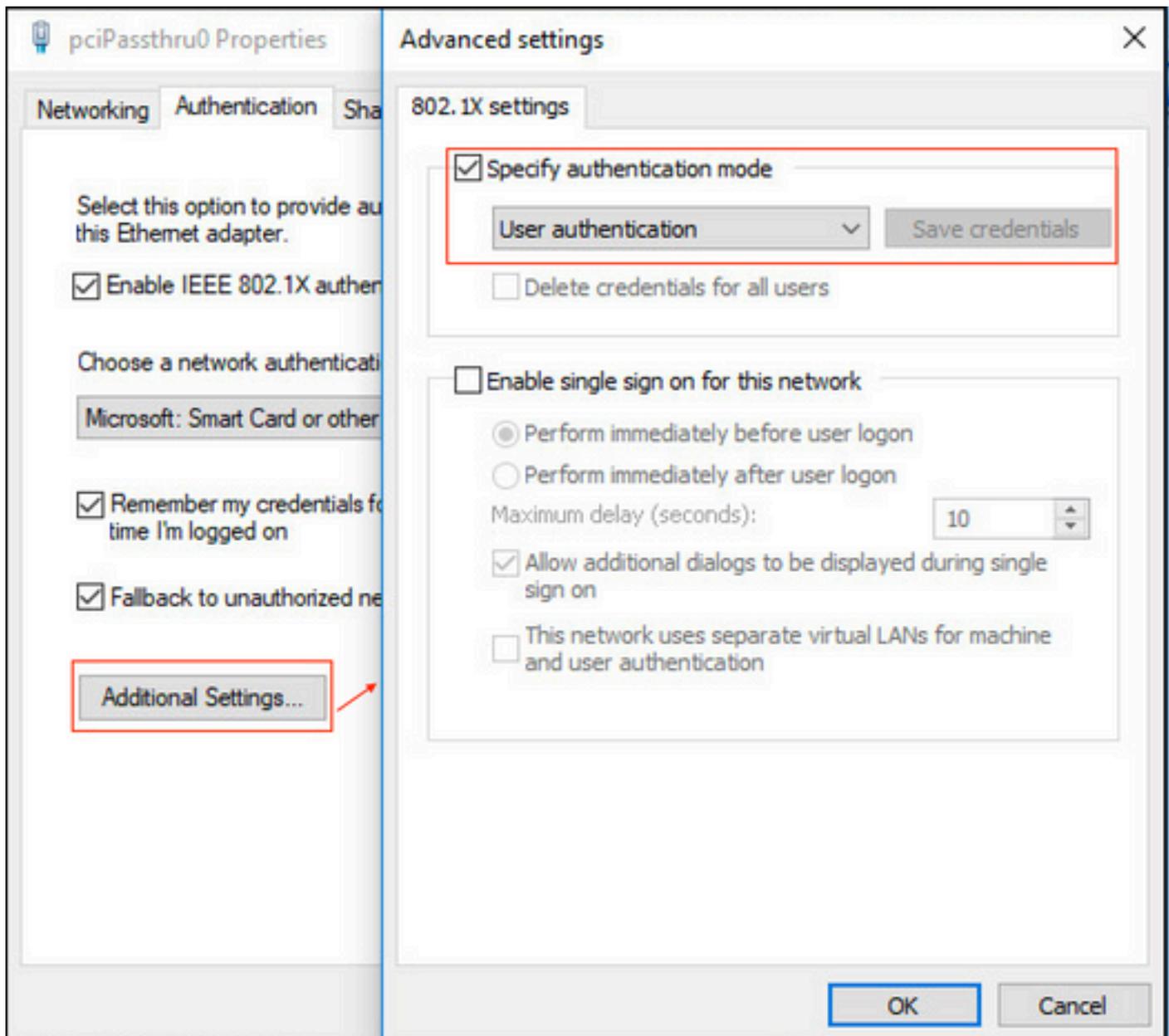
1. PCにユーザ証明書 (user1用) がプロビジョニングされていて、クライアント認証としての目的があり、信頼されたルート証明機関に発行者の証明書チェーンがPCに存在することを確認します。



2. EAP-TLS認証用にDot1x認証を有効にし、認証方法としてMicrosoft : スマートカードまたはその他の証明書を選択します。

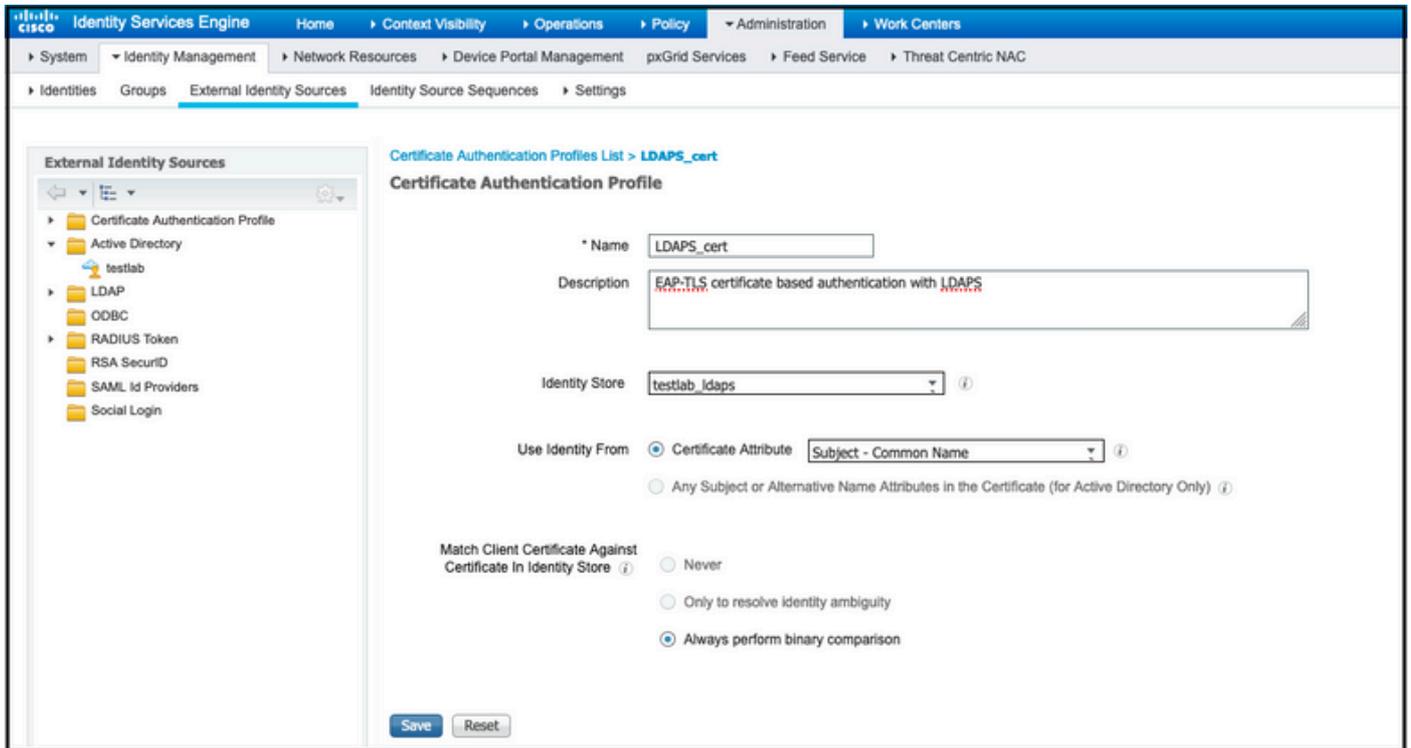


3. 「追加設定」をクリックすると、ウィンドウが開きます。次の図に示すように、specify authentication modeのチェックボックスをオンにし、user authenticationを選択します。



ISEでのポリシーセットの設定

EAP-TLSプロトコルが使用されるため、ポリシーセットを設定する前に証明書認証プロファイルを設定する必要があり、認証ポリシーで後からアイデンティティソースシーケンス(ID)が使用されます。



アイデンティティソースシーケンスの証明書認証プロファイルを参照し、認証検索リストでLDAPS外部アイデンティティソースを定義します。

Identity Services Engine Administration > Identity Source Sequences

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

次に、有線Dot1x認証用のポリシーセットを設定します。

Identity Services Engine Administration > Policy > Policy Sets

Policy Sets → Wired Dot1x

Reset Policyset Hitcounts

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

Authentication Policy (2)

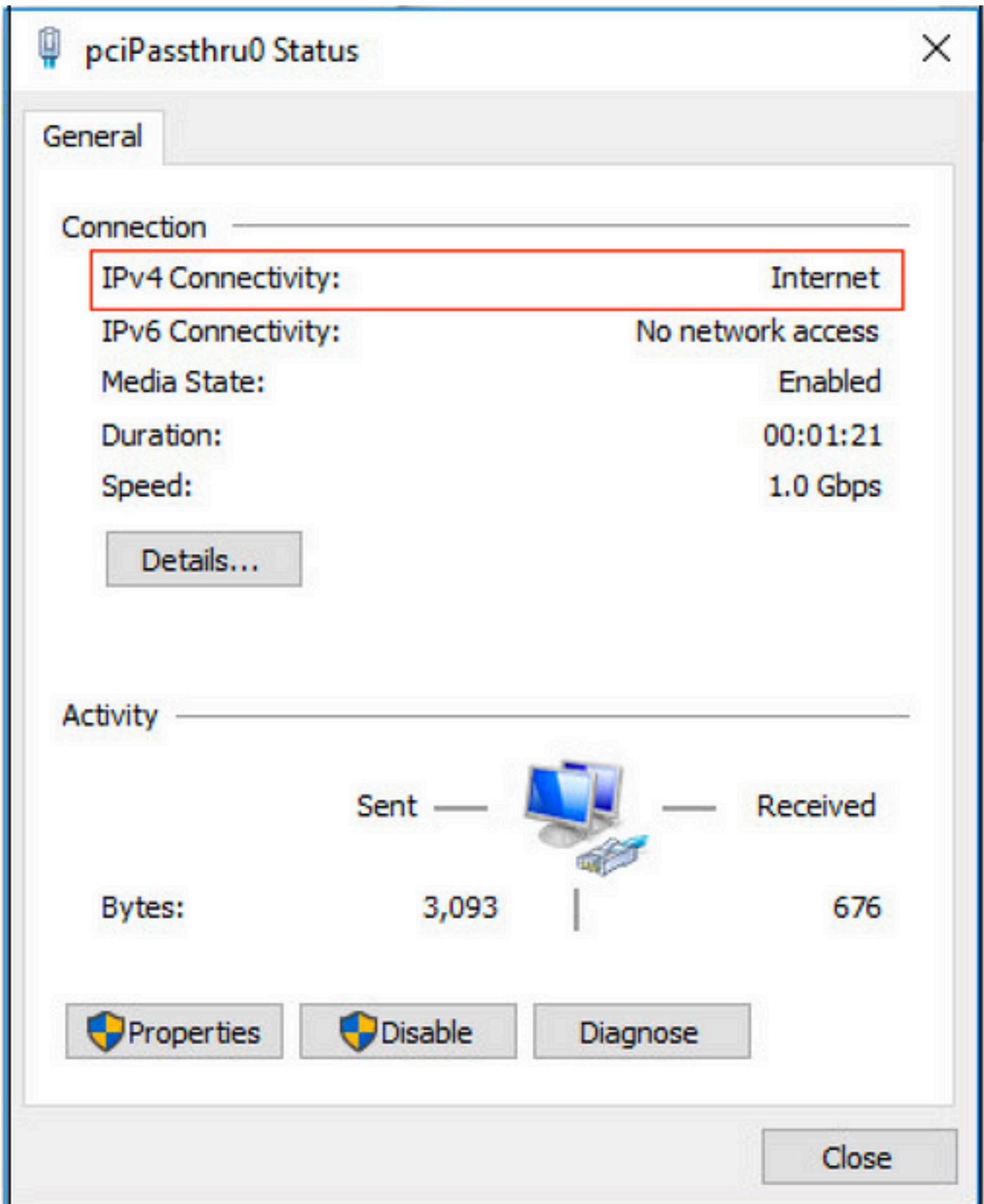
Status	Rule Name	Conditions	Use	Hits	Actions
✔	Dot1x	Network Access-NetworkDeviceName EQUALS LAB-Switch	LDAPS	223	Options
✔	Default		LDAPS	0	Options

Authorization Policy (2)

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

Reset Save

この設定後、LDAPSアイデンティティソースに対してEAP-TLSプロトコルを使用してエンドポイントを認証できます。



確認

1. PCに接続されているスイッチポートの認証セッションを確認します。

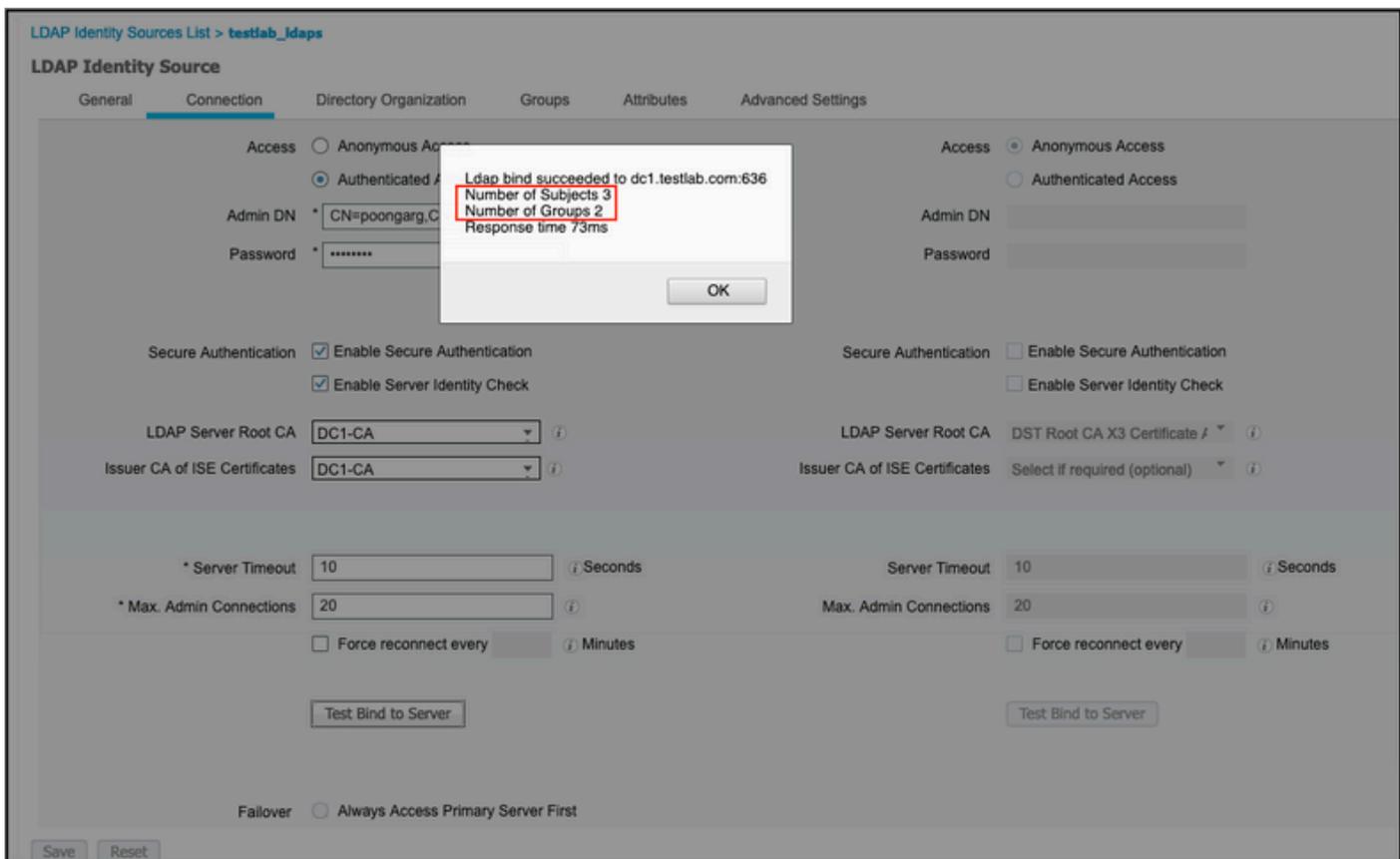
```
SW1#sh auth sessions int g2/0/47 de
      Interface: GigabitEthernet2/0/47
      MAC Address: b496.9126.dec0
      IPv6 Address: Unknown
      IPv4 Address: 10.106.38.165
      User-Name: user1
      Status: Authorized
      Domain: DATA
      Oper host mode: single-host
      Oper control dir: both
      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. LDAPSとISEの設定を確認するために、サーバへのテスト接続を使用してサブジェクトとグループを取得できます。



3. ユーザ認証レポートを確認します。

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. エンドポイントの詳細な認証レポートを確認します。

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. LDAPSサーバに向けてISE上のパケットキャプチャを取得することにより、ISEとLDAPSサーバ間でデータが暗号化されていることを確認します。

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...		28857 → 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 → 28857 [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...		28857 → 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 10:40:24.210508	10.197.164.22	10.197.164.21	TCP	66	00:0c:29:98:ca:28,0...		28857 → 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 10:40:24.230304	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 10:40:24.238809	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...		28857 → 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...		28857 → 636 [ACK] Seq=879 Ack=4221 Win=39680 Len=0 TSval=140972960 TSecr=30158967
86	2020-06-24 10:40:57.946553	10.197.164.22	10.197.164.21	TLSv1.2	151	00:0c:29:98:ca:28,0...		Application Data
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...		28857 → 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: 28857, Dst Port: 636, Seq: 336, Ack: 2078, Len: 133
  Source Port: 28857
  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

トラブルシューティング

このセクションでは、この設定で発生する一般的なエラーとそのトラブルシューティング方法について説明します。

- 認証レポートに、次のエラーメッセージが表示される場合があります。

Authentication method is not supported by any applicable identity store

このエラーメッセージは、選択した認証方式がLDAPでサポートされないことを意味します。同じレポート内に、認証プロトコルとしてサポートされている方式 (EAP-GTC、EAP-TLS、PEAP-TLS) のいずれかが示されていることを確認してください。

- サーバーへのテストバインドがエラーで終了しました。

最も一般的な原因は、LDAPSサーバの証明書検証チェックの失敗です。このような問題のトラブルシューティングを行うには、ISEでパケットキャプチャを取得し、3つのランタイムコンポーネントとprtt-jniコンポーネントをすべてデバッグレベルで有効にして、問題を再現し、prtt-server.logファイルを確認します。

パケットキャプチャは不正な証明書について苦情を言い、prtt-serverは次のように表示します。

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

 注:LDAPページのホスト名は、証明書のサブジェクト名 (またはサブジェクトの別名) を使用して設定する必要があります。したがって、サブジェクトまたはSANに証明書がない場合は機能せず、SANリストにIPアドレスを持つ証明書が必要です。

3.認証レポートで、サブジェクトがIDストアに見つからなかったことがわかりました。これは、レポートに示されているユーザ名と一致する [Subject Name] 属性を持つユーザが LDAP データベース内で見つからなかったことを意味します。このシナリオでは、この属性の値は sAMAccountName に設定されています。これは、ISE が一致を見つけようとするときに、LDAP ユーザの sAMAccountName 値を参照することを意味します。

4.サーバーバインドのテスト中に、サブジェクトとグループを正しく取得できませんでした。この問題の原因として最も可能性が高いのは、検索ベースが誤って設定されていることです。LDAP 階層は、リーフからルートの方角および dc (複数の単語で構成可能) で指定する必要があることに注意してください。

関連情報

- <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>

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。