Configurar e solucionar problemas do ISE com armazenamento de identidade LDAPS externo

Contents

Introdução

Este documento descreve a integração do Cisco ISE com o servidor LDAPS seguro como uma fonte de identidade externa.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Conhecimento básico da administração do Identity Service Engine (ISE)
- Conhecimento básico do Ative Diretory/Secure Lightweight Diretory Access Protocol (LDAPS)

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Cisco ISE 2.6 Patch 7
- Microsoft Windows versão 2012 R2 com Ative Diretory Lightweight Diretory Services instalado
- PC com sistema operacional Windows 10 com suplicante nativo e certificado do usuário instalado
- Switch Cisco C3750X com imagem 152-2.E6

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

O LDAPS permite a criptografia de dados LDAP (que incluem credenciais de usuário) em trânsito quando uma ligação de diretório é estabelecida. O LDAPS usa a porta TCP 636.

Esses protocolos de autenticação são suportados com LDAPS:

- Placa de token genérica EAP (EAP-GTC)
- PAP (Password Authentication Protocol Protocolo de Autenticação de Senha)
- EAP Transport Layer Security (EAP-TLS)
- Segurança da camada de transporte EAP protegida (PEAP-TLS)

> **Observação**: EAP-MSCHAPV2 (como um método interno de PEAP, EAP-FAST ou EAP-TTLS), LEAP, CHAP e EAP-MD5 não são suportados com a Origem de identidade externa LDAPS.

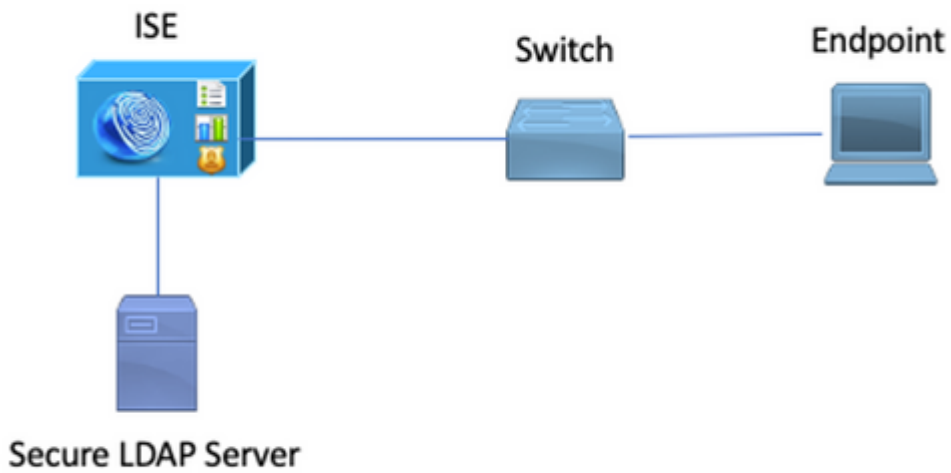
Configurar

Esta seção descreve a configuração dos dispositivos de rede e a integração do ISE com o servidor LDAP do Microsoft Ative Diretory (AD).

Diagrama de Rede

Neste exemplo de configuração, o endpoint usa uma conexão Ethernet com um switch para se conectar à rede local (LAN). A porta de switch conectada está configurada para autenticação 802.1x para autenticar os usuários com o ISE. No ISE, o LDAPS é configurado como um armazenamento de identidade externo.

Esta imagem ilustra a topologia de rede que é usada:



Configurar LDAPS no Ative Diretory

Instalar Certificado de Identidade no Controlador de Domínio

Para habilitar o LDAPS, instale um certificado no DC (Controlador de Domínio) que atenda aos seguintes requisitos:

1. O certificado LDAPS está localizado no Repositório de Certificados Pessoais do Controlador de Domínio.

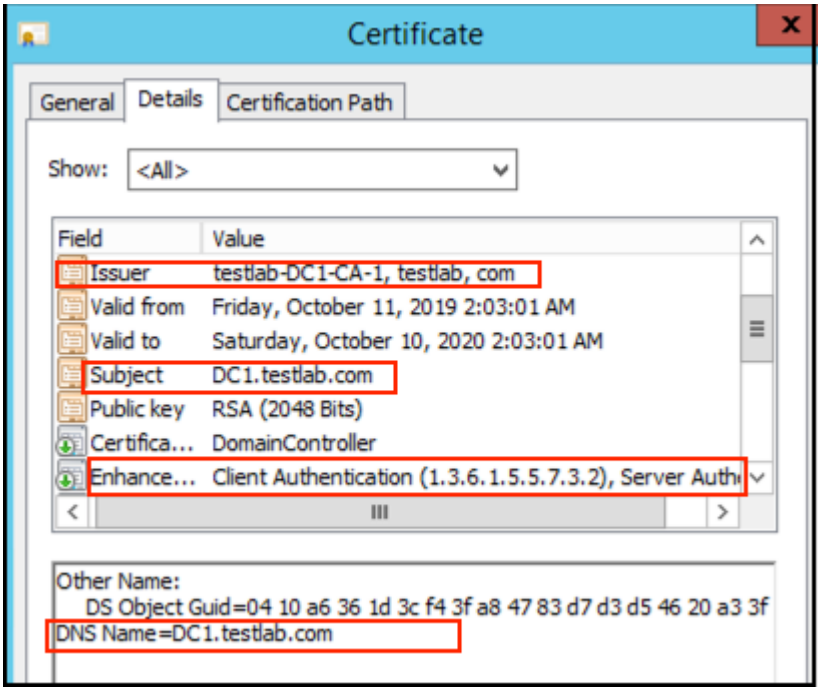
2. Uma chave privada que corresponde ao certificado está presente no repositório do Controlador de Domínio e corretamente associada ao certificado.

3. A extensão Enhanced Key Usage inclui o identificador de objeto (1.3.6.1.5.5.7.3.1) de Autenticação do Servidor (também conhecido como OID).

4. O Nome de Domínio Totalmente Qualificado (FQDN) do Controlador de Domínio (por exemplo, DC1.testlab.com) deve estar presente em um destes atributos: O Nome Comum (CN) no campo Assunto e a entrada DNS na Extensão de Nome Alternativo do Assunto.

5. O certificado deve ser emitido por uma CA (Autoridade de Certificação) em que o Controlador de Domínio e os clientes LDAPS confiam. Para uma comunicação segura confiável, o cliente e o servidor devem confiar na CA raiz um do outro e nos certificados de CA intermediários que emitiram certificados para eles.

6. O provedor de serviços de criptografia (CSP) Schannel deve ser usado para gerar a chave.



Acessar estrutura de diretório LDAPS

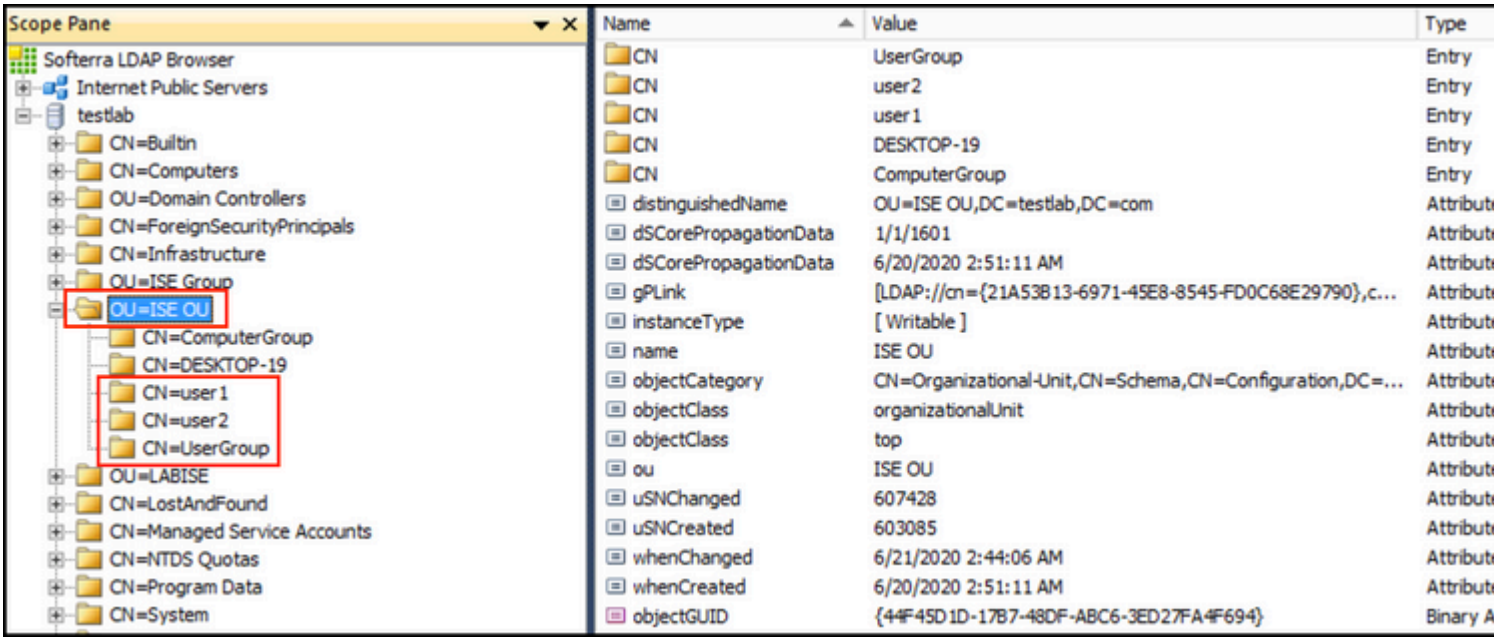
Para acessar o Diretório LDAP no servidor do Ative Diretory, use qualquer navegador LDAP. Neste LABORATÓRIO, o Softerra LDAP Browser 4.5 é usado.

1. Estabeleça uma conexão com o domínio na porta TCP 636.

2. Para simplificar, crie uma Unidade Organizacional (UO) chamada ISE OU no AD e ela deve ter um

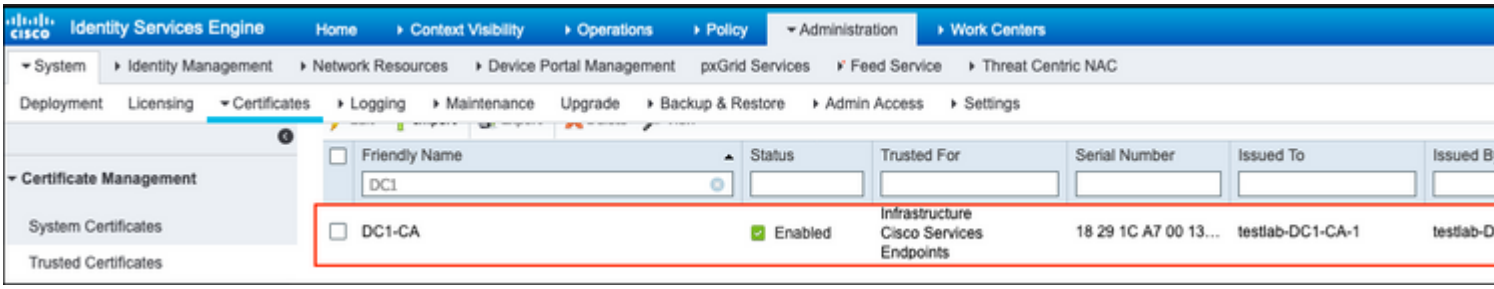
Grupo chamado UserGroup. Crie dois usuários (user1 e user2) e torne-os membros do grupo UserGroup.

Observação: a origem de identidade LDAP no ISE é usada somente para autenticação de usuário.



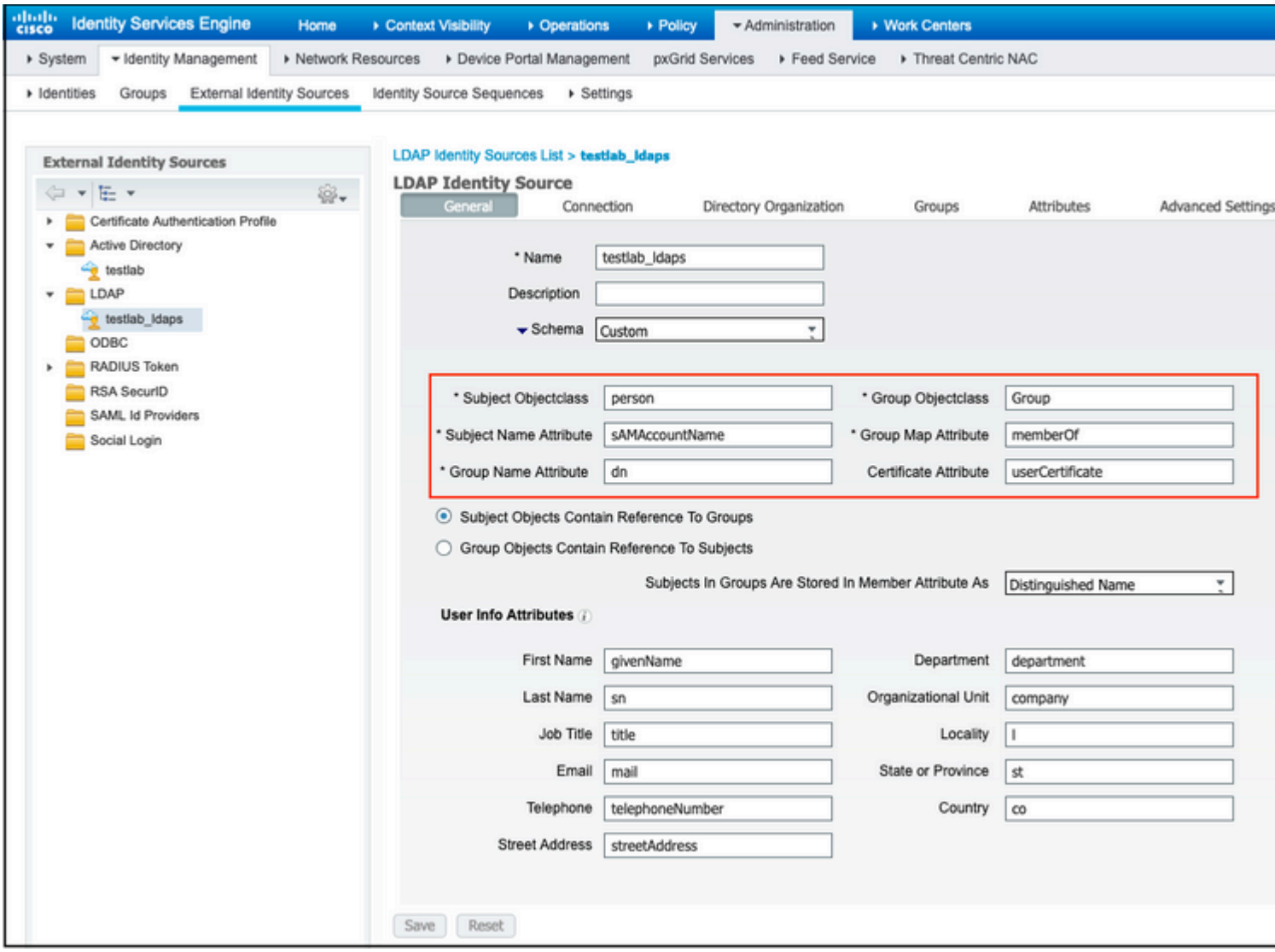
Integrar o ISE com o servidor LDAPS

1. Importe o certificado CA raiz do servidor LDAP no Certificado Confiável.



2. Valide o certificado de administrador do ISE e verifique se o certificado do emissor do certificado de administrador do ISE também está presente no Repositório de Certificados Confiáveis.

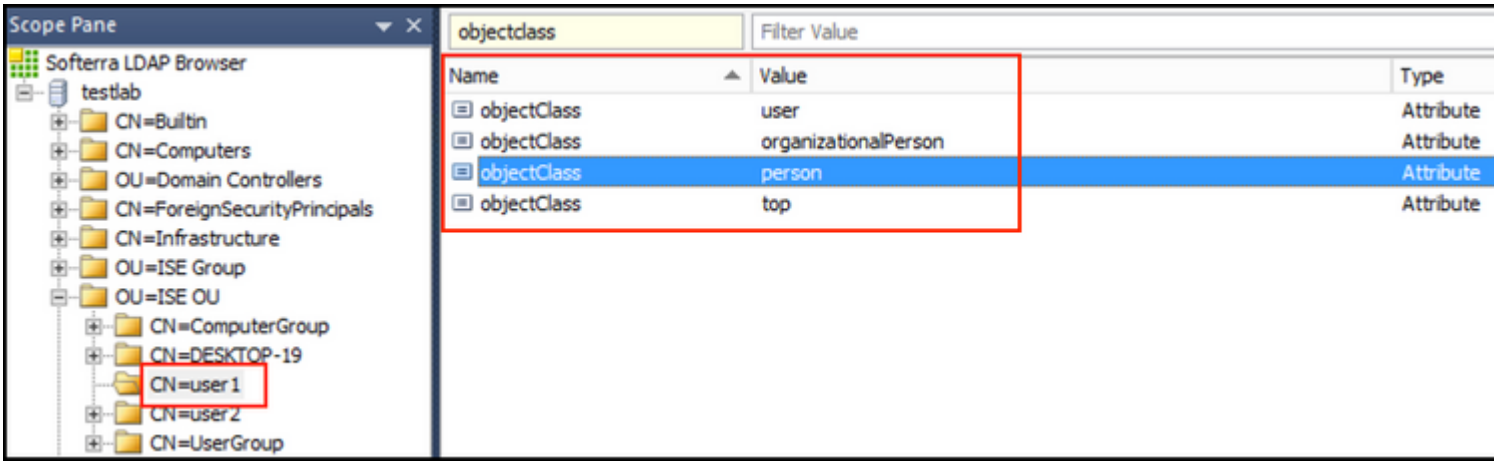
3. Para integrar o servidor LDAPS, use os diferentes atributos LDAP do diretório LDAPS. Navegue até **Administração > Gerenciamento de identidades > Origens de identidade externas > Origens de identidade LDAP > Adicionar**.



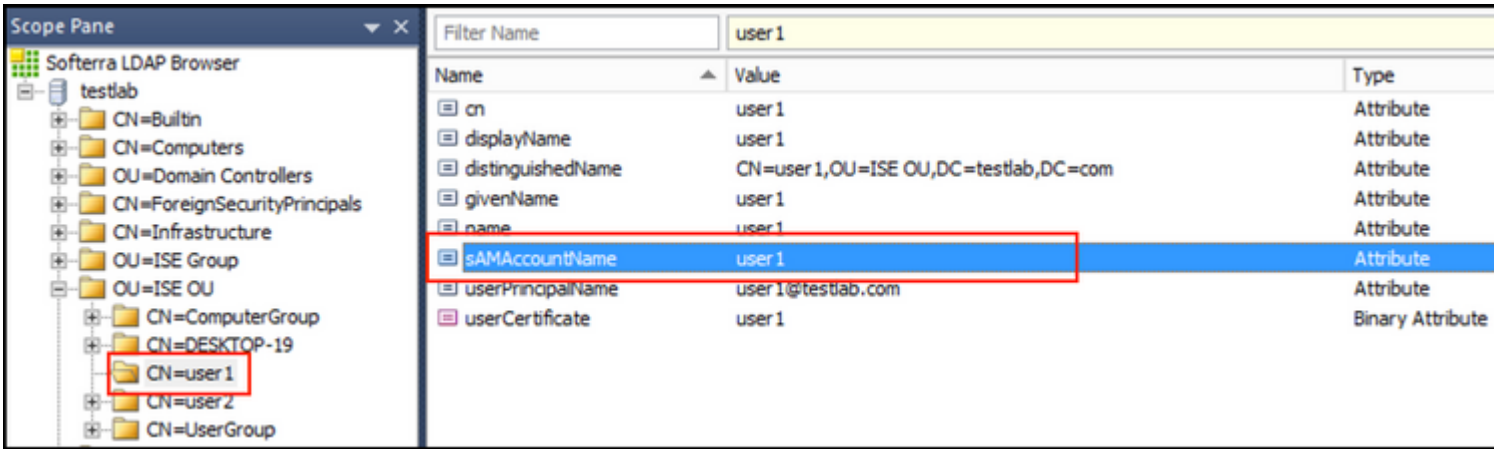
4. Configure estes atributos a partir da Guia Geral:

Classe de Objeto do Assunto: Esse campo corresponde à classe Objeto das contas de usuário. Você pode usar uma das quatro classes aqui:

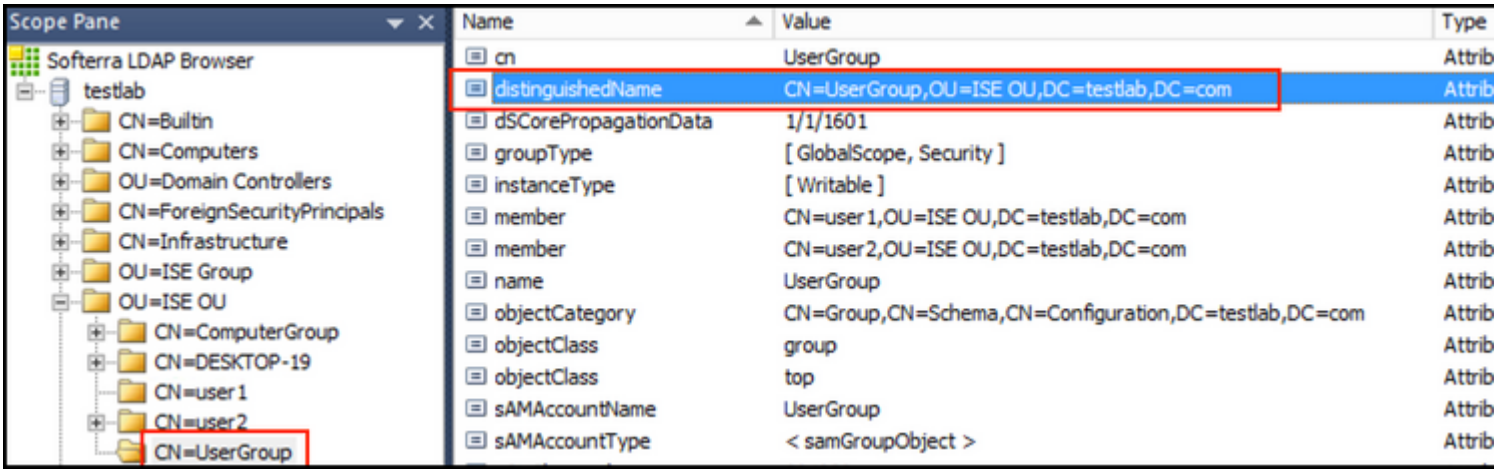
- Superior
- Pessoa
- PessoaOrganizacional
- InetOrgPerson



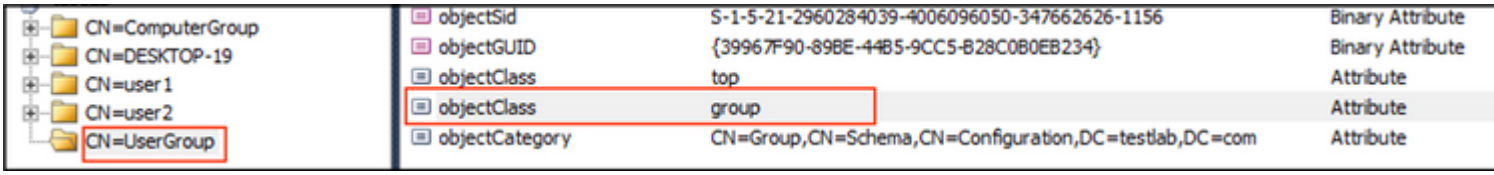
Atributo do Nome do Assunto: Este campo é o nome do atributo que contém o nome de usuário da solicitação. Esse atributo é recuperado do LDAPS quando o ISE consulta um nome de usuário específico no banco de dados LDAP (você pode usar cn, sAMAccountName etc.). Neste cenário, o nome de usuário user1 no ponto final é usado.



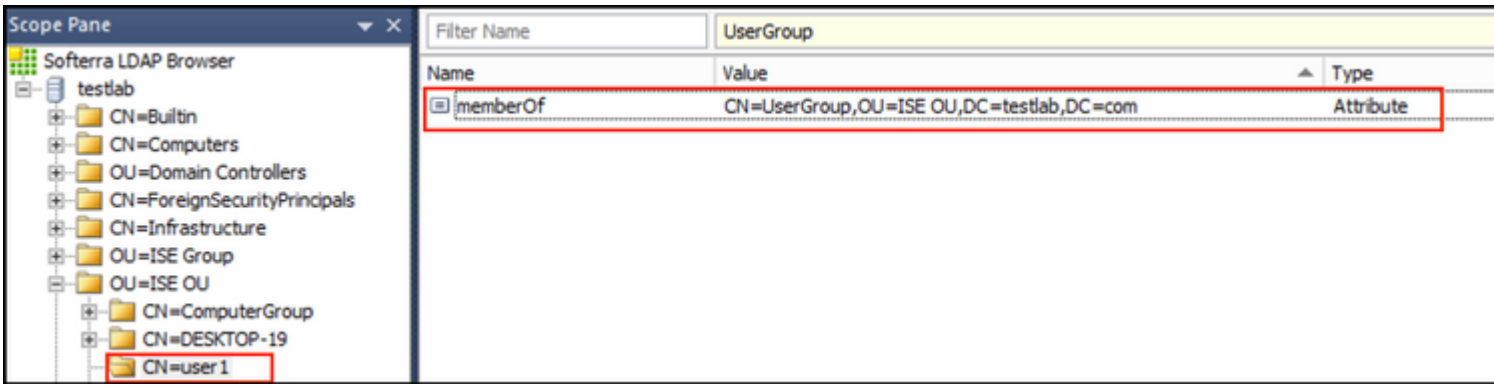
Atributo do Nome do Grupo: Este é o atributo que contém o nome de um grupo. Os valores do atributo Nome do grupo no diretório LDAP devem corresponder aos nomes do grupo LDAP na página Grupos de usuários



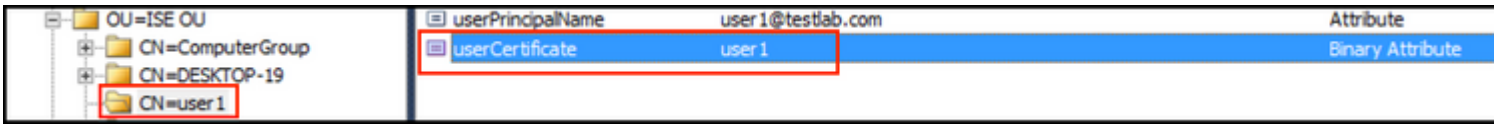
Group Objectclass: esse valor é usado em pesquisas para especificar os objetos que são reconhecidos como grupos.



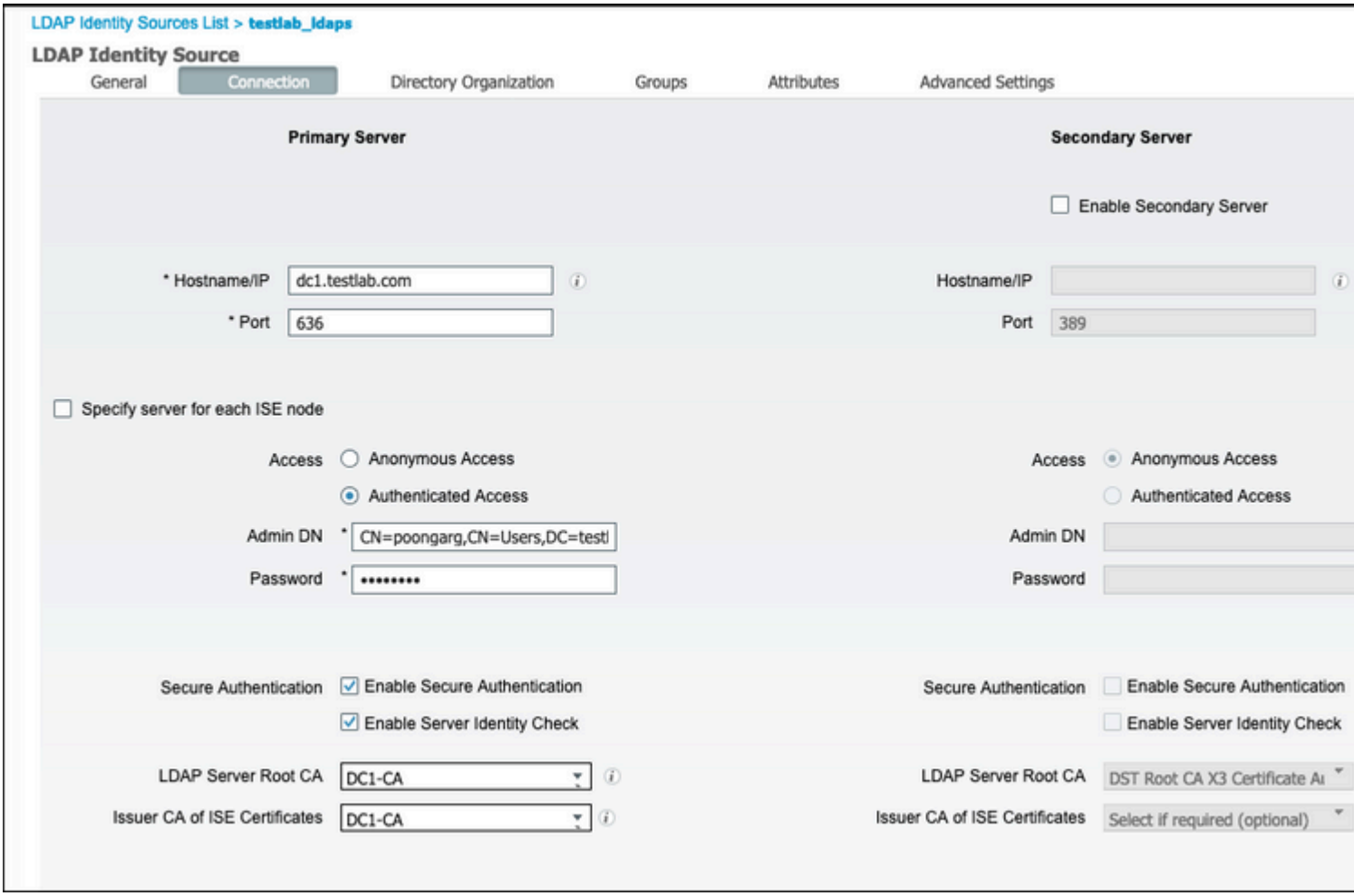
Atributo de mapa de grupo: este atributo define como os usuários são mapeados para os grupos.

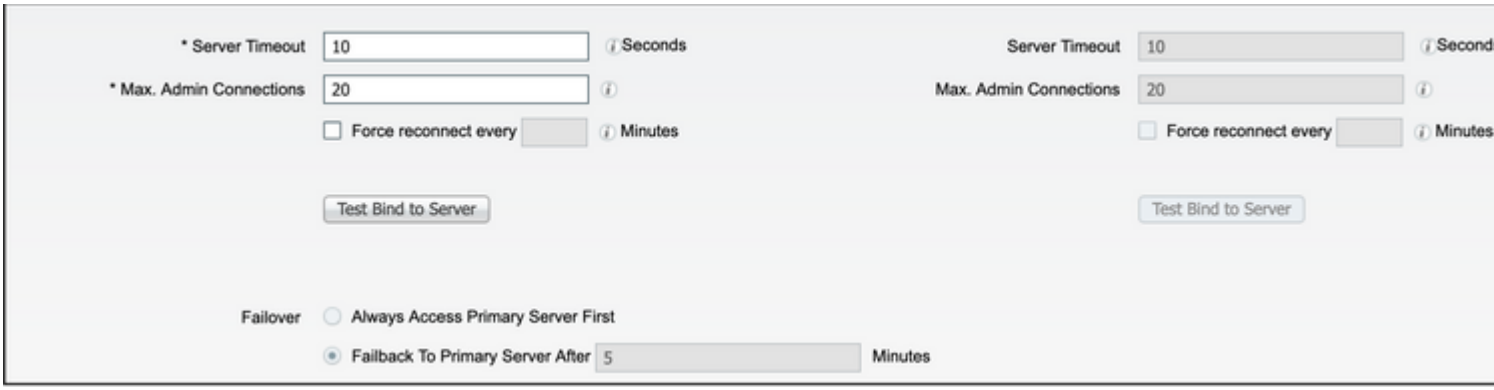


Atributo do Certificado: Informe o atributo que contém as definições do certificado. Essas definições podem ser usadas opcionalmente para validar certificados apresentados por clientes quando eles são definidos como parte de um perfil de autenticação de certificado. Nesses casos, uma comparação binária é realizada entre o certificado do cliente e o certificado recuperado da origem da identidade LDAP.



5. Para configurar a conexão LDAPS, navegue até a guia **Connection**:





6. Execute dsquery no controlador de domínio para obter o DN do nome de usuário a ser usado para estabelecer uma conexão com o servidor LDAP:

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

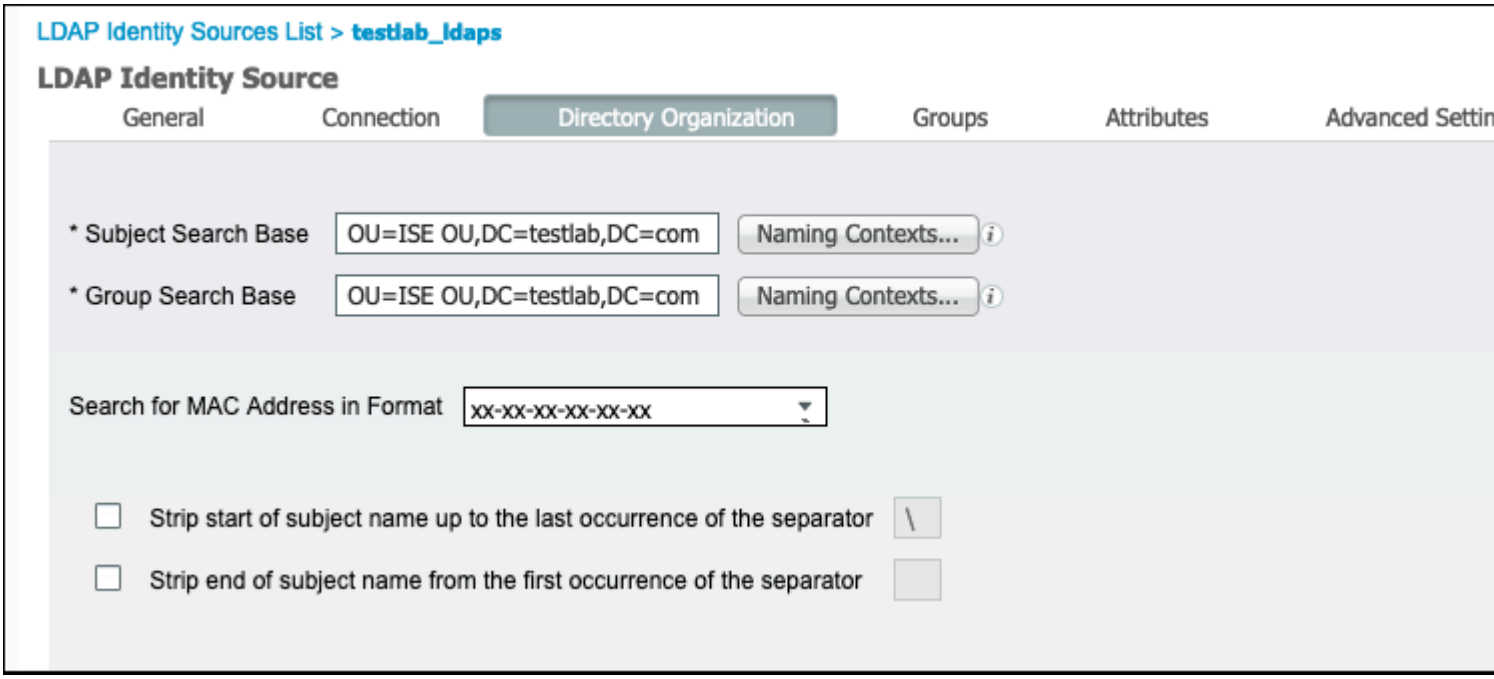
Etapa 1. SDefina o endereço IP ou o nome de host correto do servidor LDAP, defina a porta LDAPS (TCP 636) e o DN Admin para fazer uma conexão com o LDAP sobre SSL.

Etapa 2. Opção Habilitar Autenticação Segura e Verificação de Identidade de Servidor.

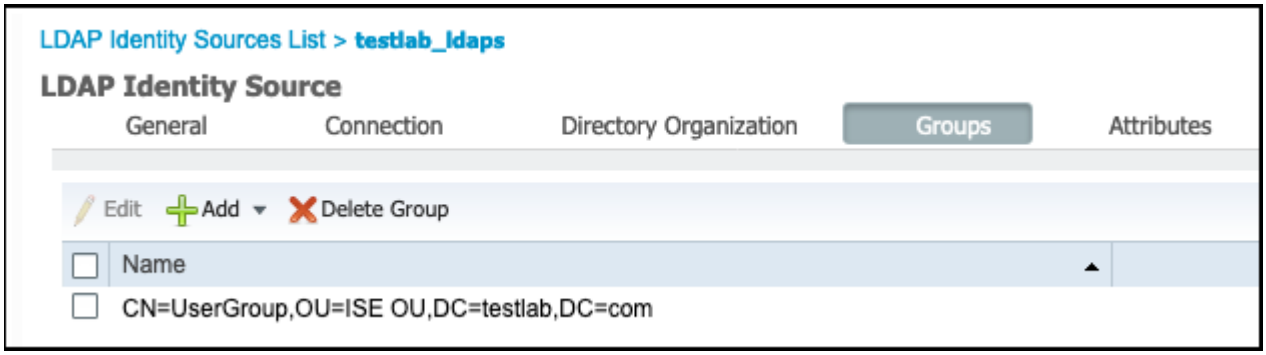
Etapa 3. No menu suspenso, selecione o certificado CA raiz do servidor LDAP e o certificado administrador ISE Emissor CA (usamos autoridade de certificação, instalada no mesmo servidor LDAP para emitir o certificado admin ISE também).

Etapa 4. Selecione Testar Ligação com o servidor. Neste ponto, nenhum assunto ou grupo será recuperado porque as bases de pesquisa ainda não estão configuradas.

7. Na guia **Diretory Organization**, configure a Base de Pesquisa de Assunto/Grupo. É o ponto de junção do ISE com o LDAP. Agora você pode recuperar apenas assuntos e grupos que são filhos do ponto de união. Nesse cenário, o assunto e o grupo são recuperados da OU=ISE OU



8. Em Grupos, clique em Adicionar para importar os grupos do LDAP no ISE e recuperar os grupos, como mostrado nesta imagem.



Configurar o switch

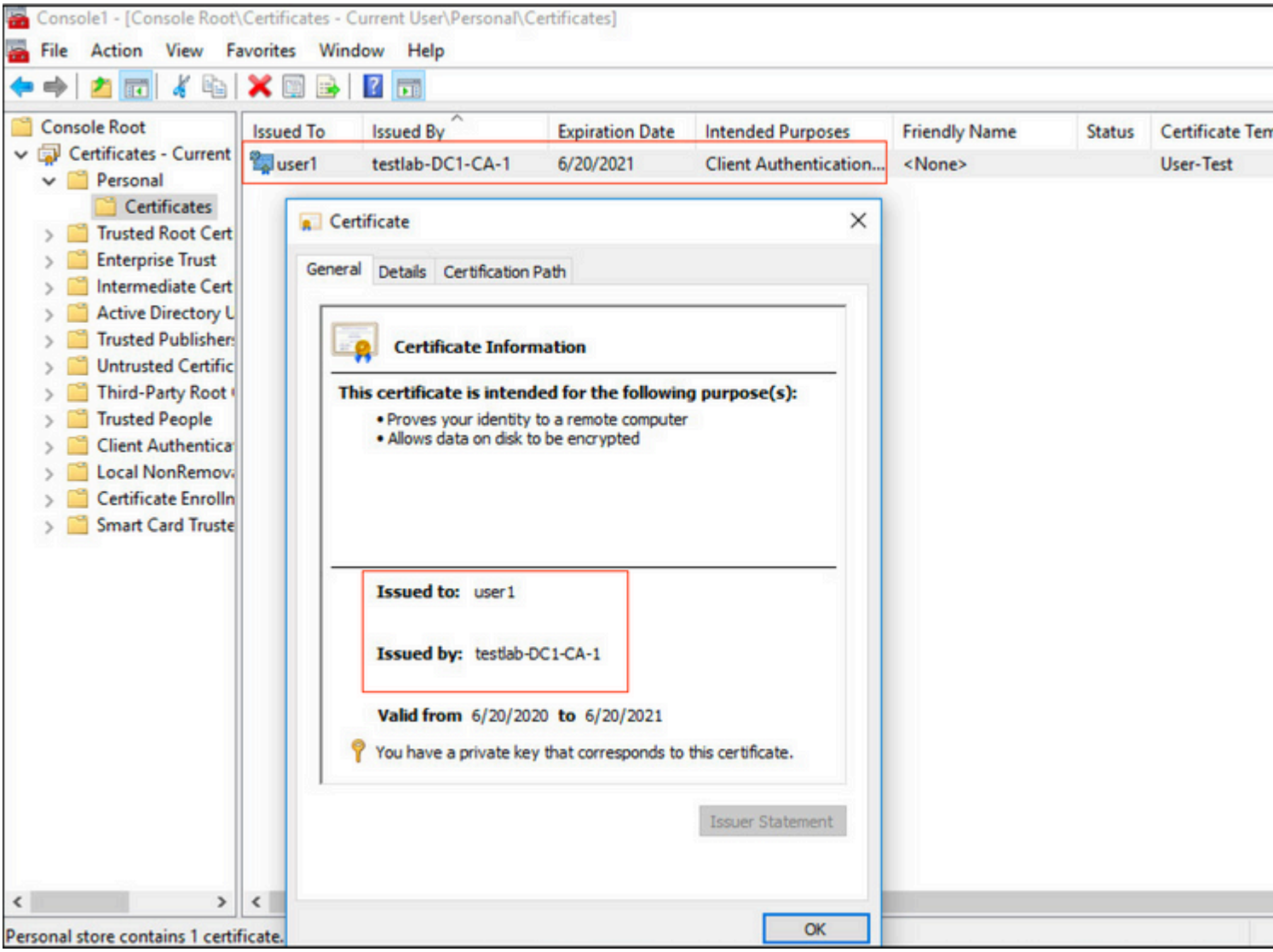
Configure o switch para a autenticação 802.1x. O PC com Windows está conectado à porta de switch Gig2/0/47

```
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
```

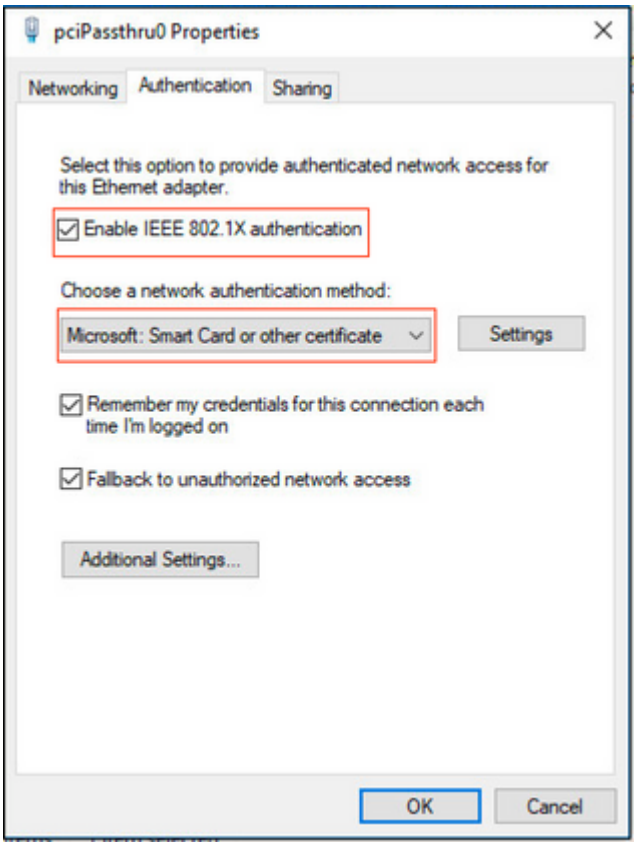
Configurar o endpoint

O Windows Native Supplicant é usado e um dos protocolos EAP suportados pelo LDAP é utilizado, EAP-TLS para autenticação e autorização do usuário.

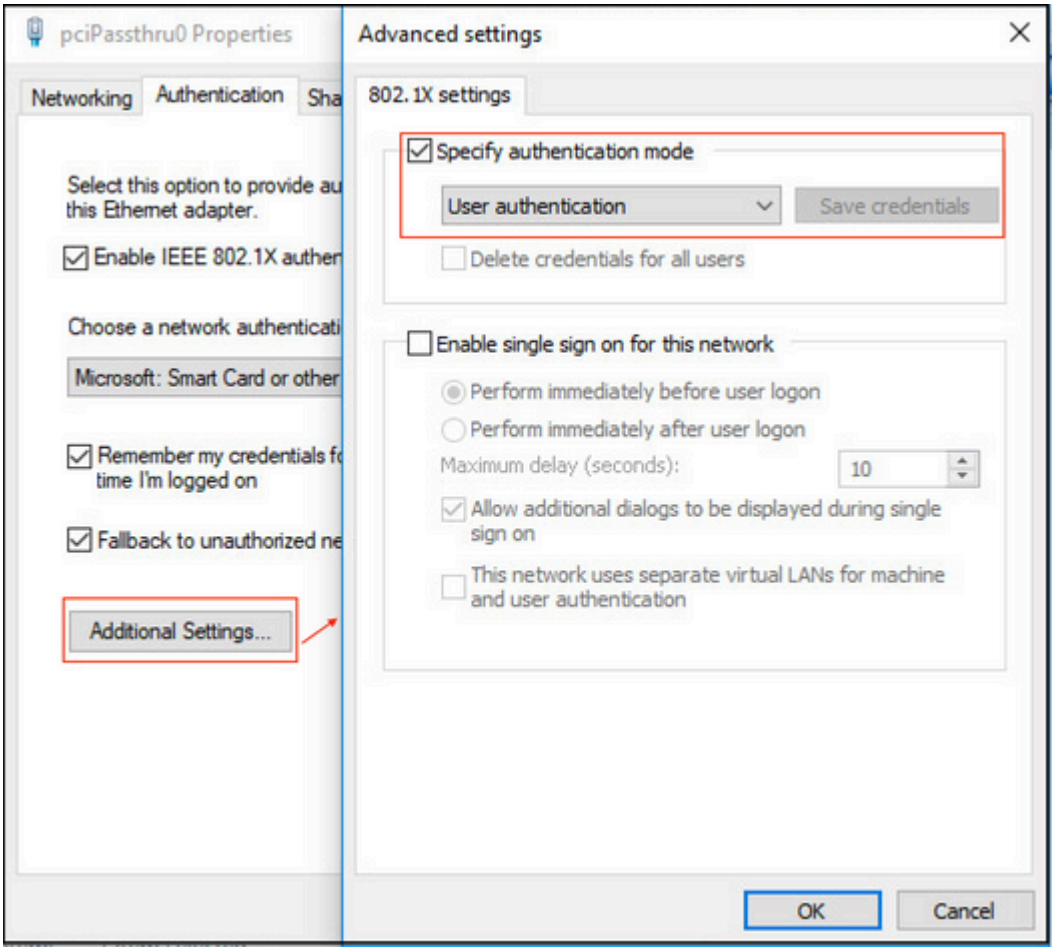
1. Verifique se o PC foi provisionado com o certificado do usuário (para o usuário1) e se a finalidade pretendida é a Autenticação do Cliente e, nas Autoridades de Certificação Raiz Confiáveis, se a cadeia de certificados do emissor está presente no PC.



2. Ative a autenticação Dot1x e selecione o método de autenticação como Microsoft:Smart Card ou outro certificado para a autenticação EAP-TLS.

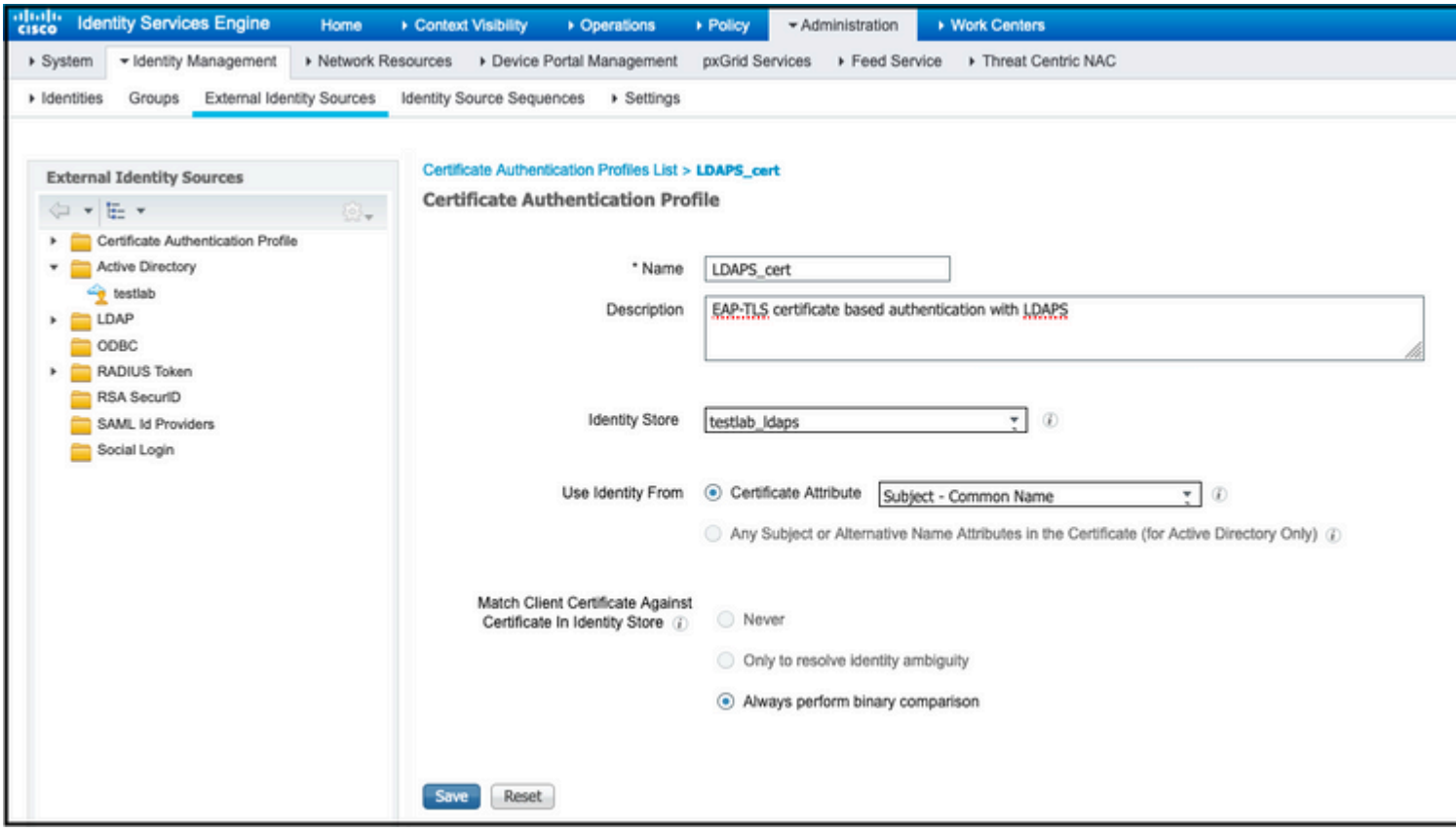


3. Clique em Configurações Adicionais e uma janela será aberta. Marque a caixa com especificar o modo de autenticação e escolha a autenticação do usuário, conforme mostrado nesta imagem.

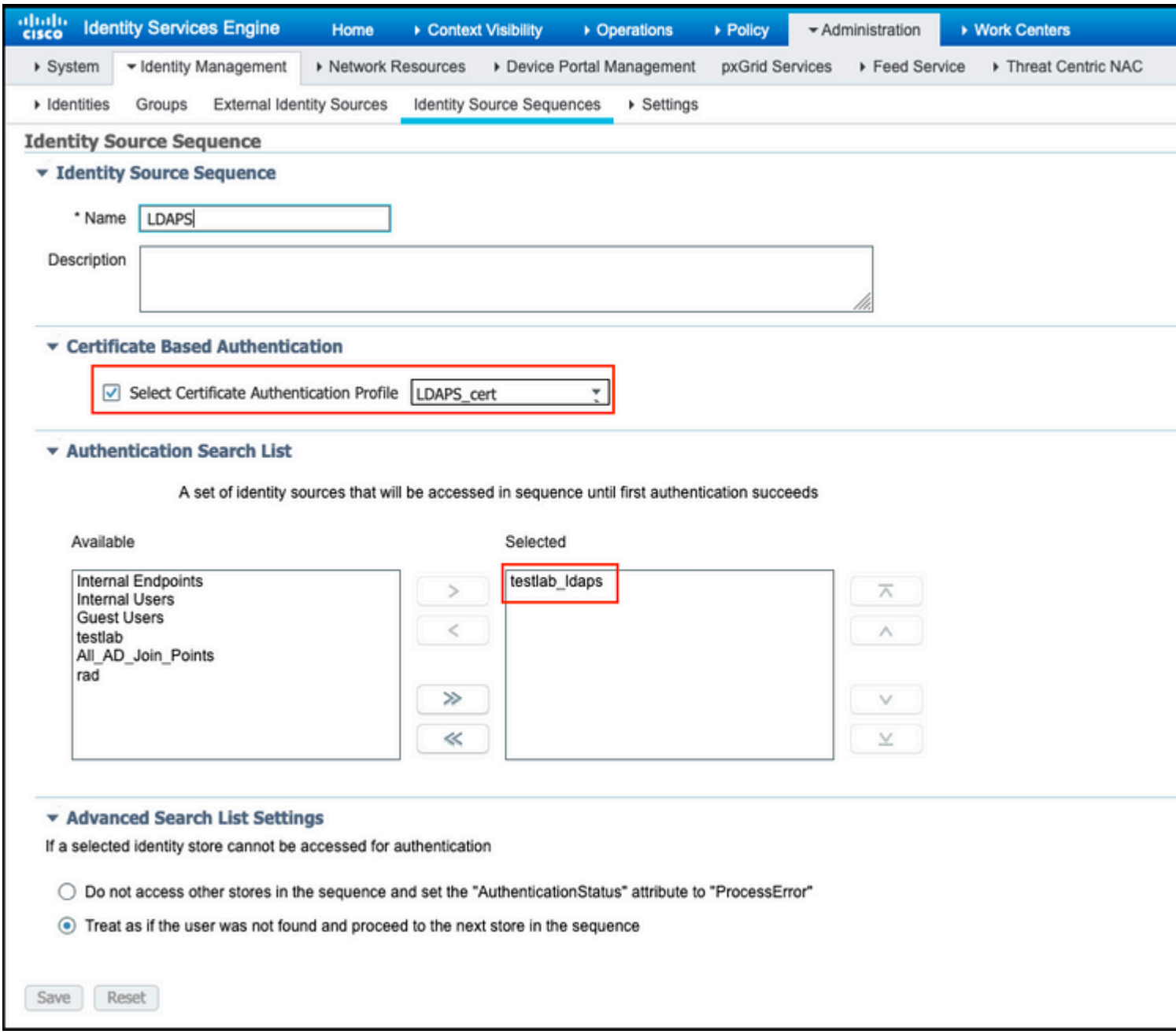


Configurar definição de política no ISE

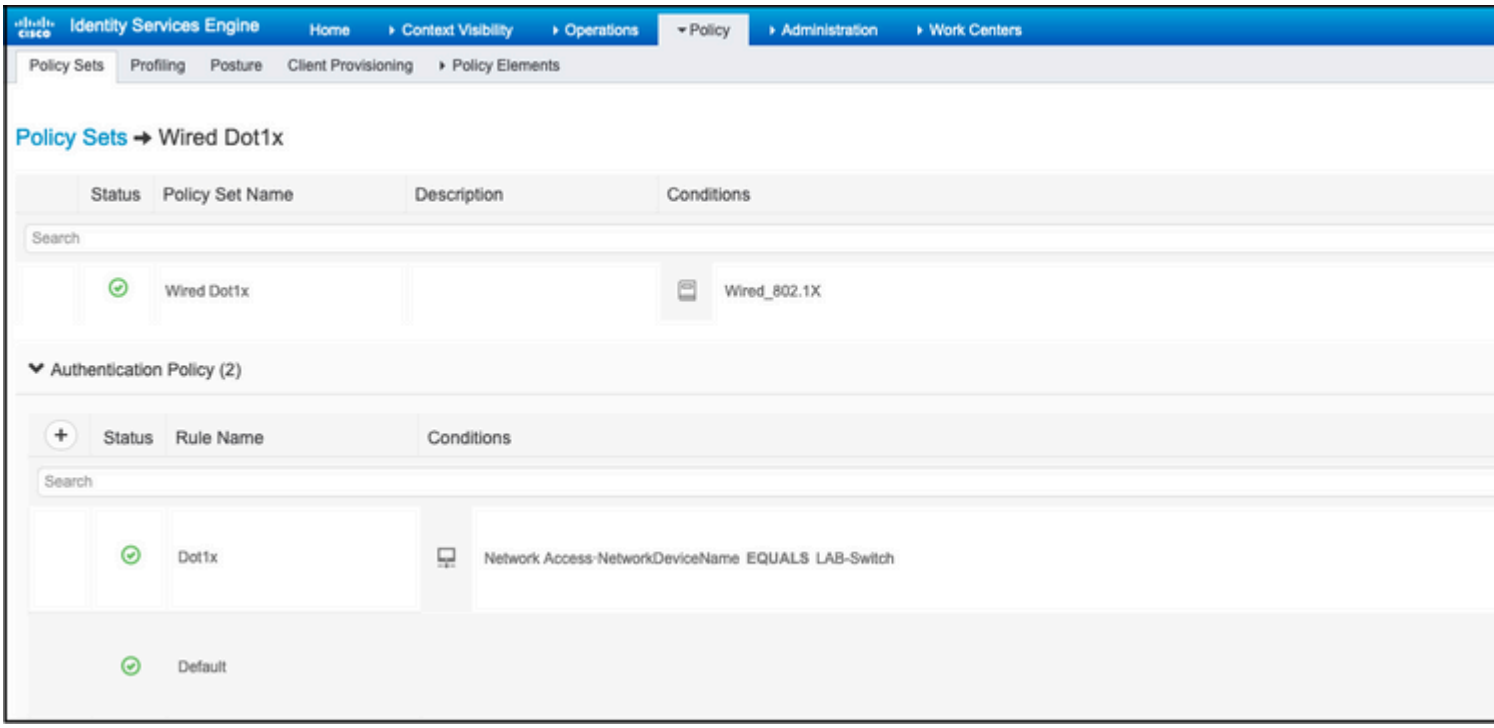
Como o protocolo EAP-TLS é usado, antes de o conjunto de políticas ser configurado, o perfil de autenticação de certificado precisa ser configurado e a sequência de origem de identidade é usada mais tarde na política de autenticação.



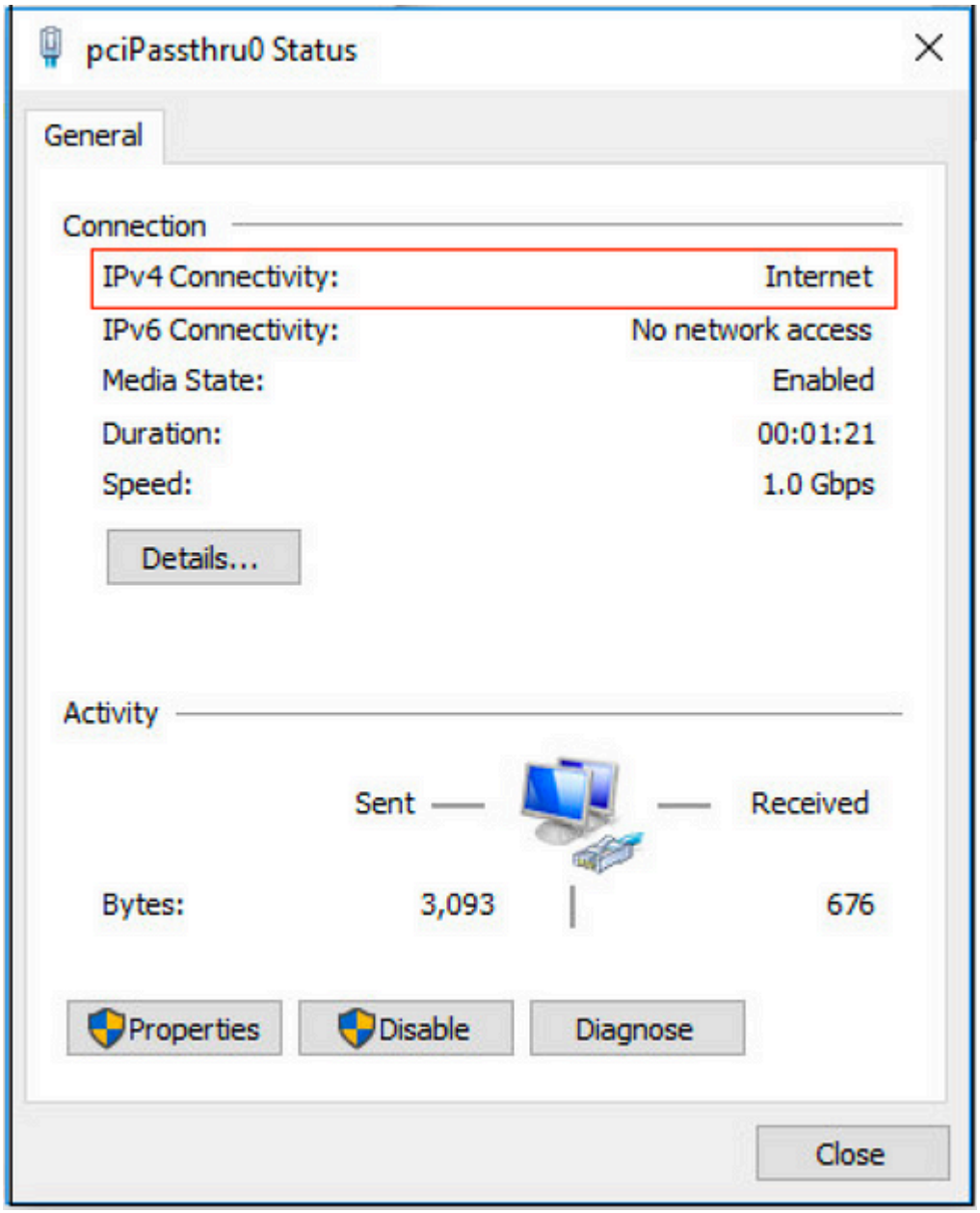
Consulte o Perfil de autenticação de certificado na Sequência de origem da identidade e defina a origem de identidade externa LDAPS na lista de pesquisa de autenticação:



Agora configure o conjunto de políticas para autenticação Wired Dot1x:



Após essa configuração, podemos autenticar o endpoint usando o protocolo EAP-TLS na fonte de identidade LDAPS.

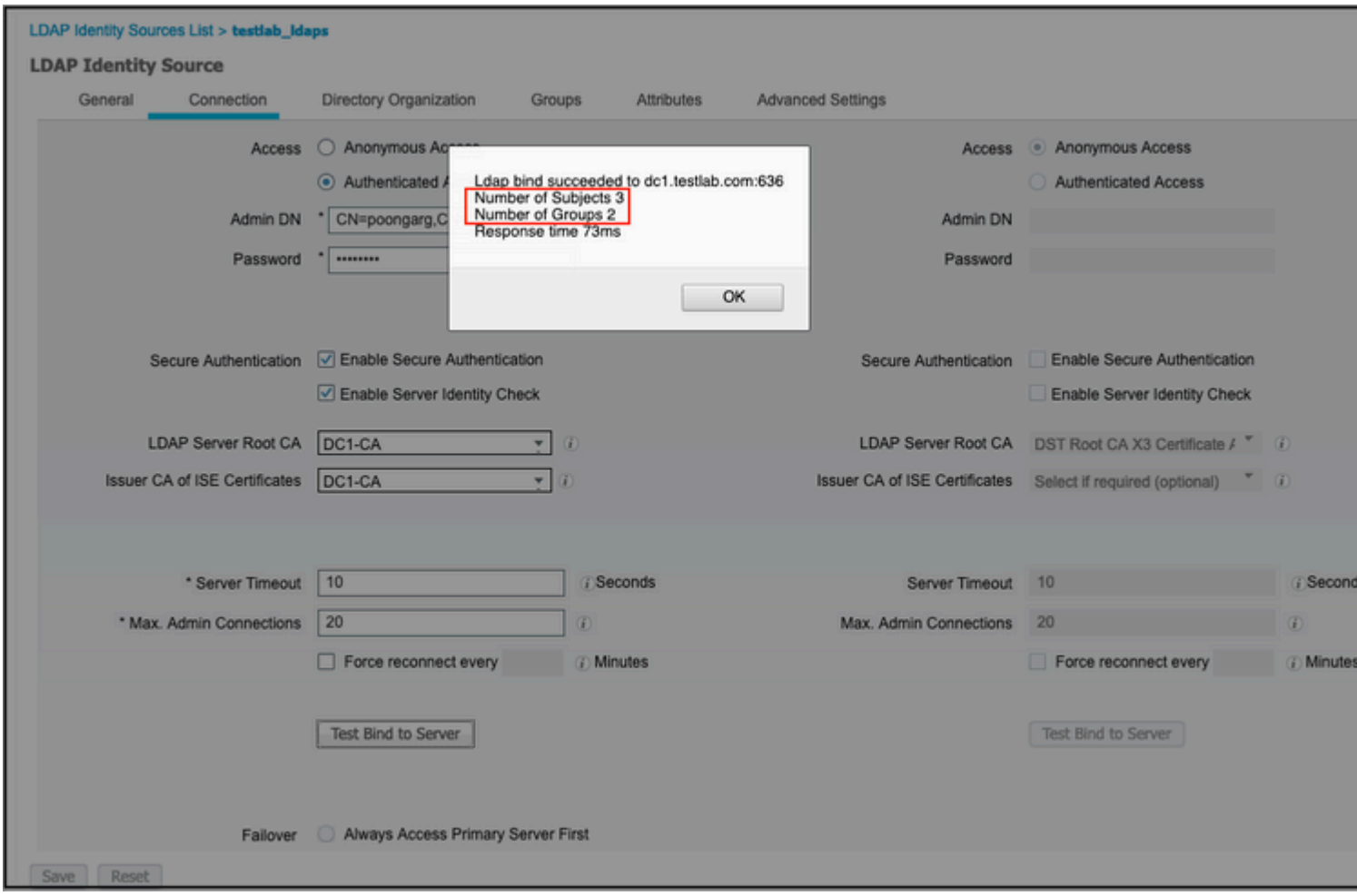


Verificar

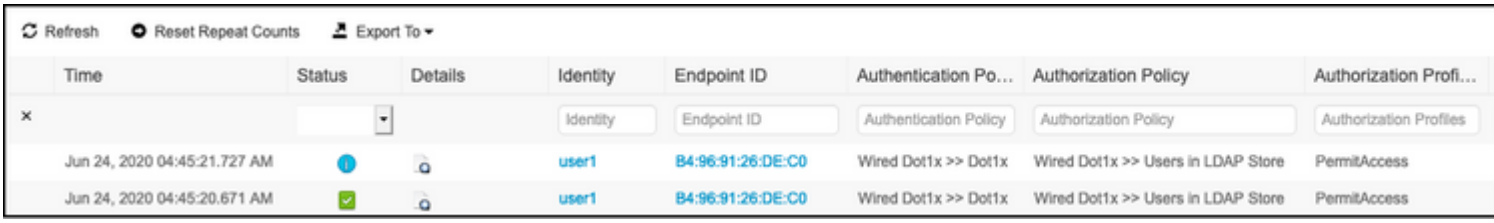
1. Verifique a sessão de autenticação na porta do switch conectada ao PC:

```
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:  0A6A263900000130798C66612
     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. Para verificar as configurações de LDAPS e ISE, você pode recuperar os assuntos e grupos com uma conexão de teste com o servidor:



3. Verifique o relatório de autenticação do usuário:



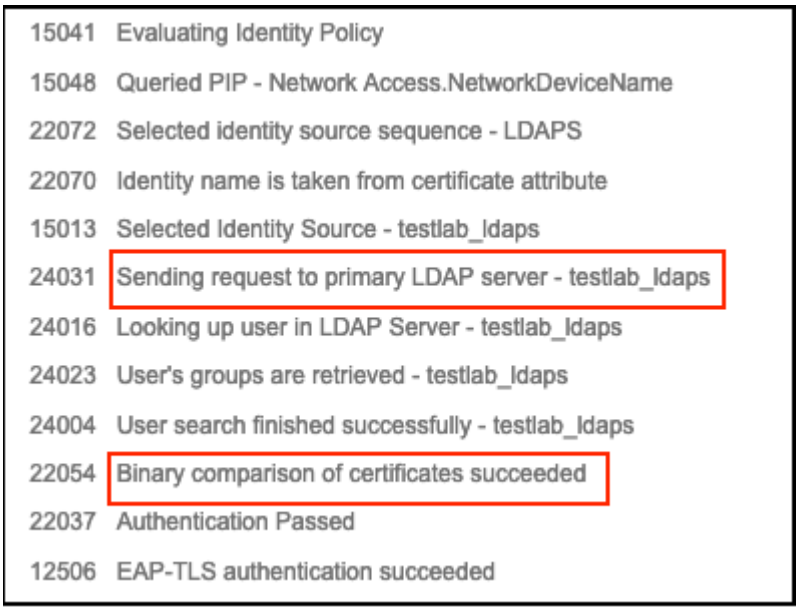
4. Verifique o relatório de autenticação detalhado do ponto final:

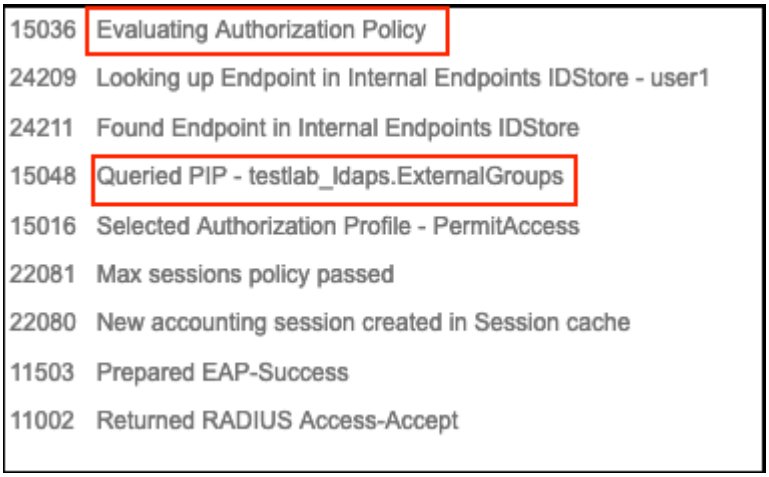
Overview

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

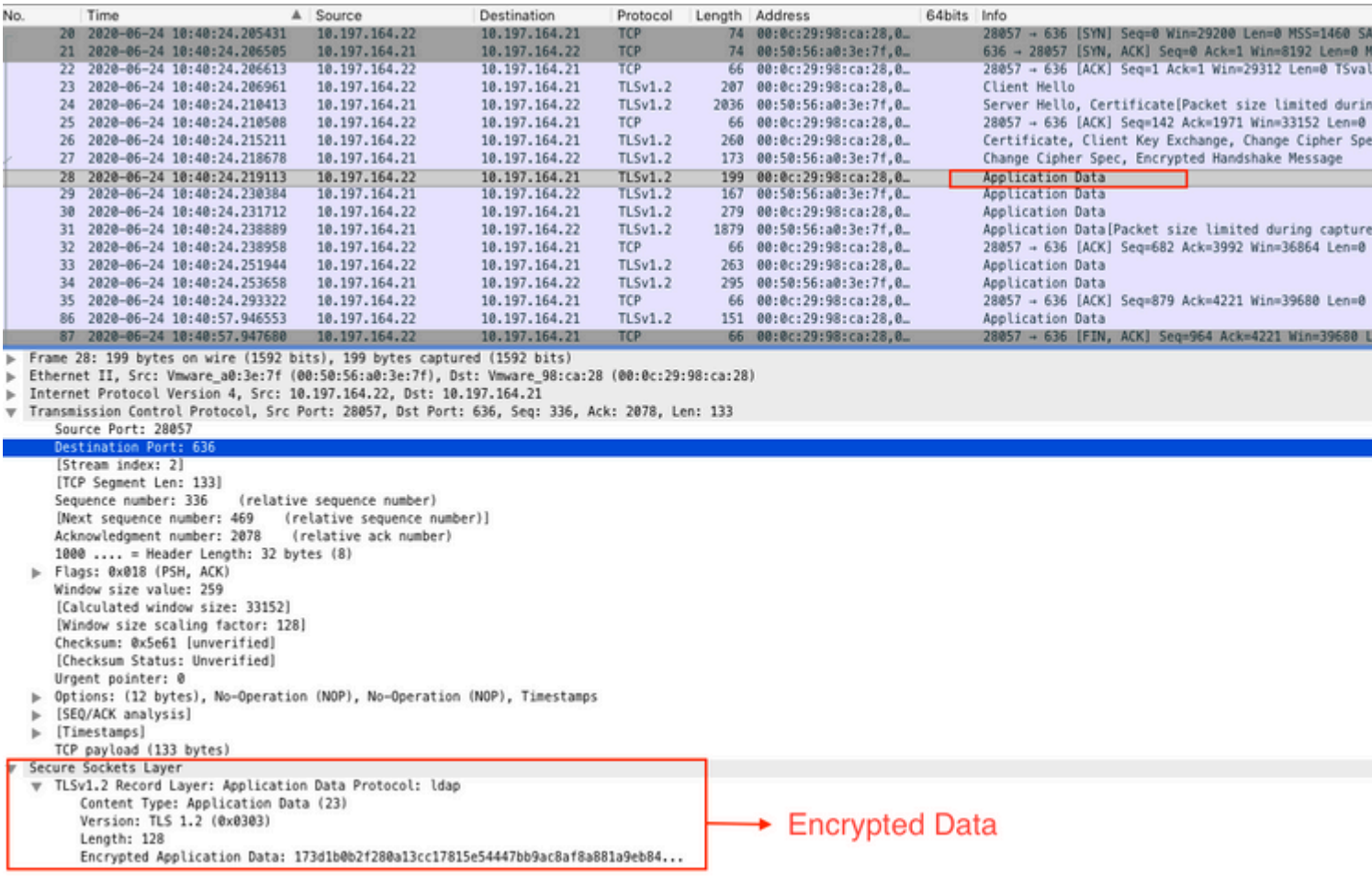
Authentication Details

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_ldaps
Identity Group	Unknown
Audit Session Id	0A6A26390000130C98CE6088
Authentication Method	dot1x
Authentication Protocol	EAP-TLS
Service Type	Framed
Network Device	LAB-Switch





5. Valide se os dados estão criptografados entre o ISE e o servidor LDAPS, fazendo a captura de pacotes no ISE para o servidor LDAPS:



Troubleshooting

Esta seção descreve alguns erros comuns encontrados com essa configuração e como solucioná-los.

- No relatório de autenticação, você pode ver esta mensagem de erro:

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

Esta mensagem de erro indica que o método selecionado não é suportado pelo LDAP. Verifique se o protocolo de autenticação no mesmo relatório mostra um dos métodos suportados (EAP-GTC, EAP-TLS ou PEAP-TLS).

- O teste de ligação ao servidor terminou com um erro.

Geralmente, isso se deve a uma falha na verificação de validação de certificado do servidor LDAPS. Para solucionar esses tipos de problemas, capture um pacote no ISE e ative todos os três componentes de tempo de execução e prt-jni no nível de depuração, recrie o problema e verifique o arquivo prrt-server.log.

A captura de pacotes reclama de um certificado incorreto e o servidor de porta mostra:

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

Observação: o nome do host na página LDAP deve ser configurado com o nome do assunto do certificado (ou qualquer um dos Nomes Alternativos do Assunto). Portanto, a menos que isso esteja no assunto ou na SAN, isso não funcionará, o certificado com o endereço IP na lista de SANs será necessário.

3. No relatório de autenticação, você pode observar que o assunto não foi encontrado no armazenamento de identidade. Isso significa que o nome de usuário do relatório não corresponde ao atributo de nome do assunto de nenhum usuário no banco de dados LDAP. Nesse cenário, o valor foi definido como sAMAccountName para esse atributo, o que significa que o ISE procura os valores de sAMAccountName para o usuário LDAP quando ele tenta encontrar uma correspondência.

4. Não foi possível recuperar corretamente os assuntos e grupos durante um teste de ligação com o servidor. A causa mais provável desse problema é uma configuração incorreta das bases de pesquisa. Lembre-se de que a hierarquia LDAP deve ser especificada de folha para raiz e dc (pode consistir em várias palavras).

Informações Relacionadas

- **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**

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.