Controle de acesso baseado em função do ISE com LDAP

Contents

Introduction

Este documento descreve um exemplo de configuração para o uso do Lightweight Diretory Access Protocol (LDAP) como um repositório de identidade externa para acesso administrativo à GUI de gerenciamento do Cisco Identity Services Engine (ISE).

Prerequisites

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Configuração do Cisco ISE versões 3.0
- LDAP (Lightweight Diretory Access Protocol)

Requirements

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

- Cisco ISE versão 3.0
- Windows Server 2016

The information in this document was created from the devices in a specific lab environment. All of

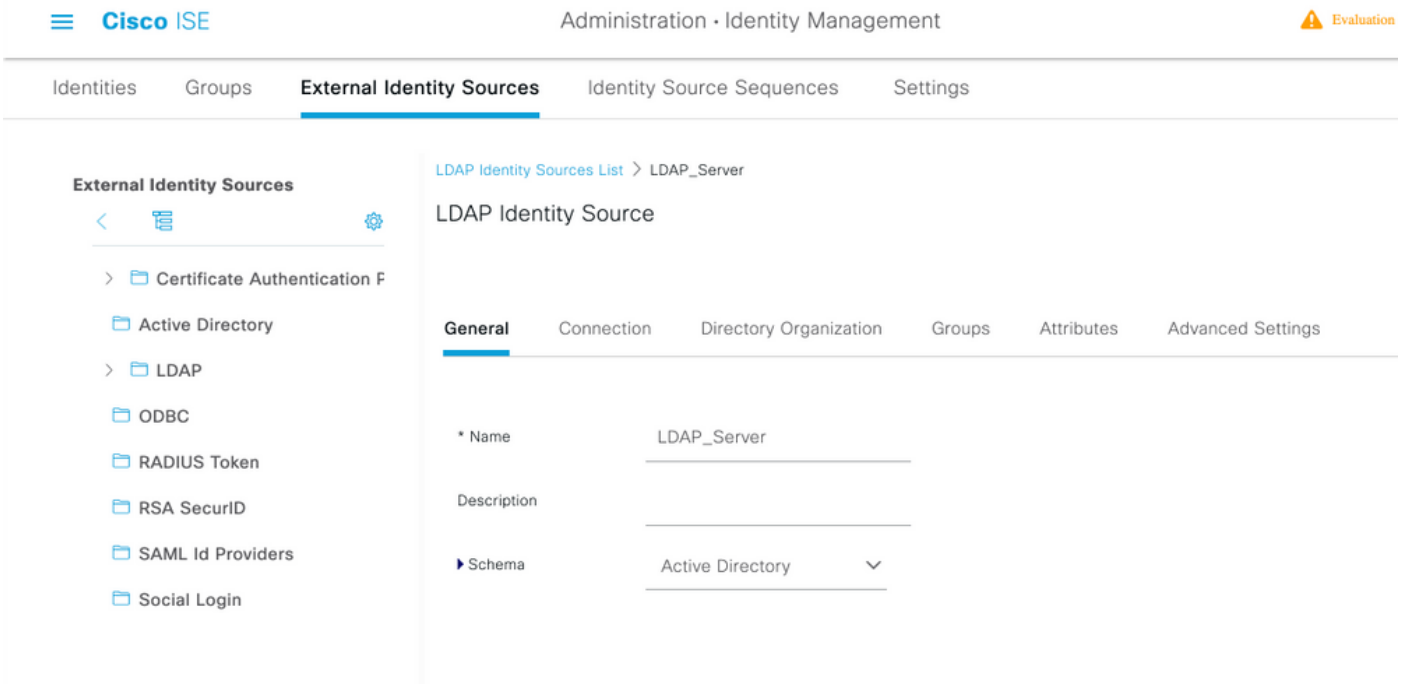
the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Configurações

Use a seção abaixo para configurar um usuário baseado em LDAP para obter o acesso baseado em administração/personalizado à GUI do ISE . A configuração abaixo usa as consultas do protocolo LDAP para buscar o usuário do Ative Diretory para executar a autenticação.

Ingressar ISE em LDAP

1. Navegue até **Administration > Identity Management > External Identity Sources > Ative Diretory > LDAP.**
2. Na guia **Geral**, insira o nome do LDAP e escolha o esquema Ative Diretory.



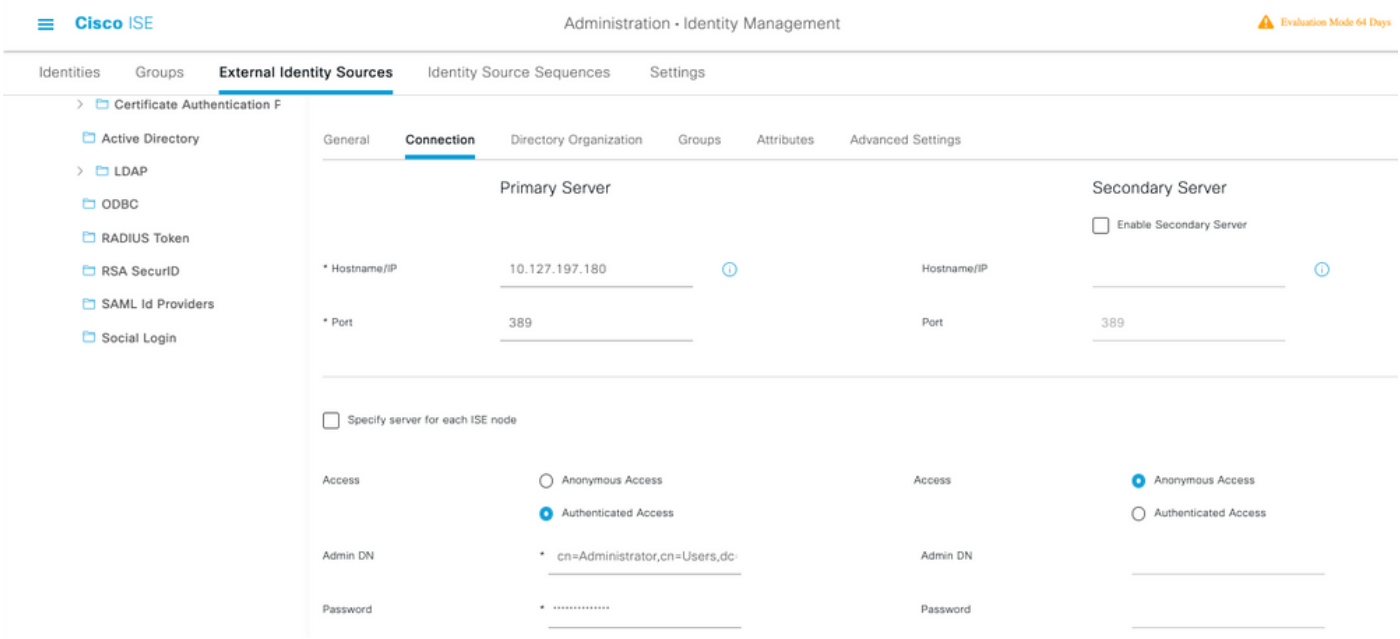
Configurar o tipo de conexão e a configuração LDAP

1. Navegue até **ISE > Administration > Identity Management > External Identity Sources > LDAP.**

2. Configure o nome de host do servidor LDAP primário junto com a porta 389(LDAP)/636 (LDAP-Secure) .

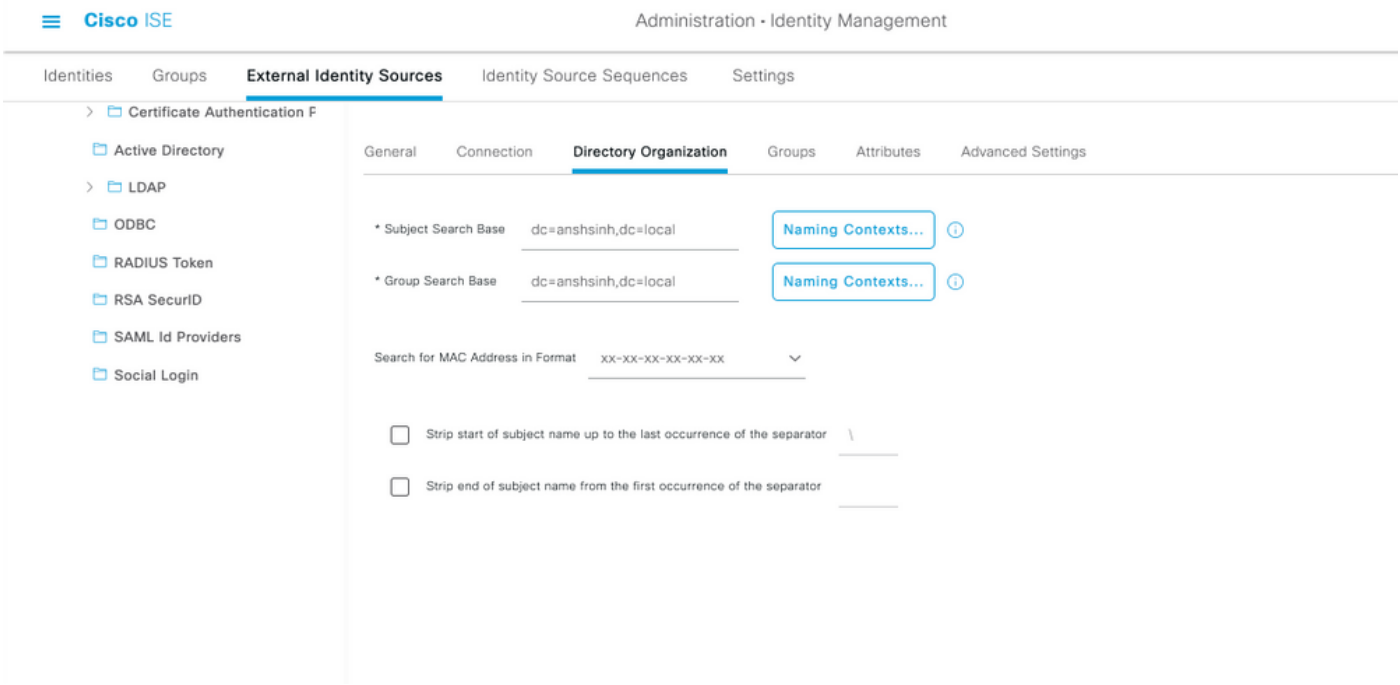
3. Insira o caminho para o DN (Admin Distinguished Name, nome distinto de administrador) com a senha de administrador para o servidor LDAP .

4.Clique em Test Bind Server para testar a acessibilidade do servidor LDAP do ISE .



Configurar a organização, os grupos e os atributos do diretório

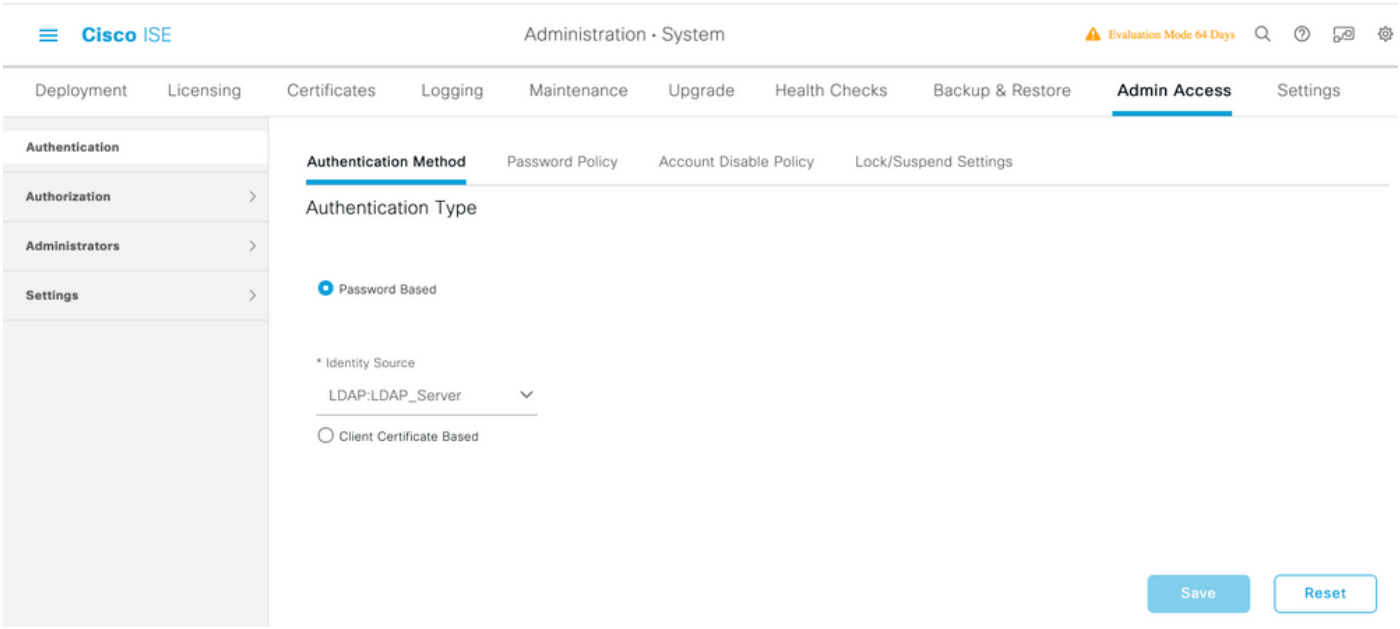
1. Escolha o grupo de Organização correto do usuário com base na hierarquia de usuários armazenados no servidor LDAP .



Habilitar acesso administrativo para usuários LDAP

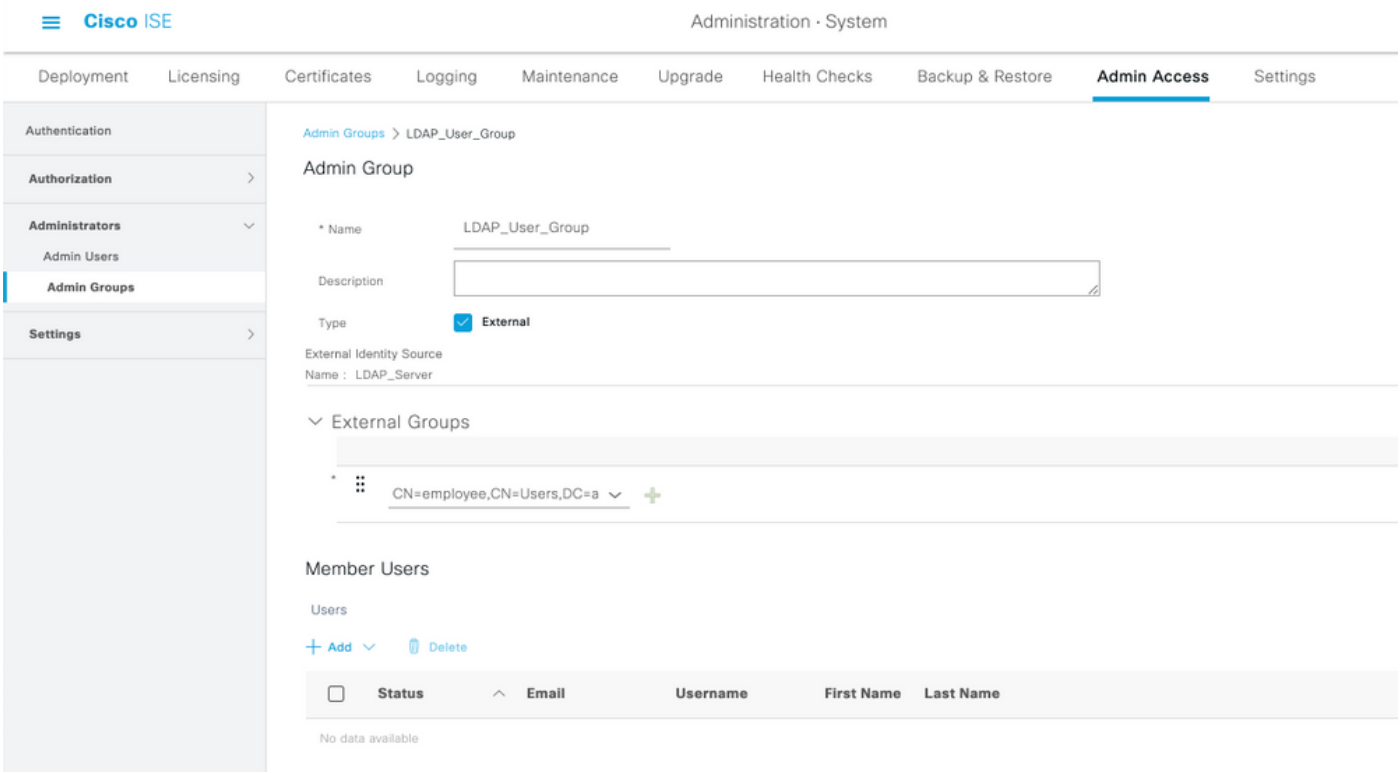
Conclua estes passos para habilitar a autenticação baseada em senha.

1. Navegue até **ISE > Administration > System > Admin Access > Authentication**.
2. Na guia **Authentication Method**, selecione a opção **Password-Based**.
3. Selecione **LDAP** no menu suspenso **Origem da identidade**.
4. Clique em **Salvar alterações**.



Mapear o grupo de administração para o grupo LDAP

Configure o grupo Admin no ISE e mapeie-o para o grupo AD. Isso permite que o usuário configurado obtenha acesso com base nas políticas de autorização com base nas permissões de RBAC configuradas para o administrador com base na associação do grupo.

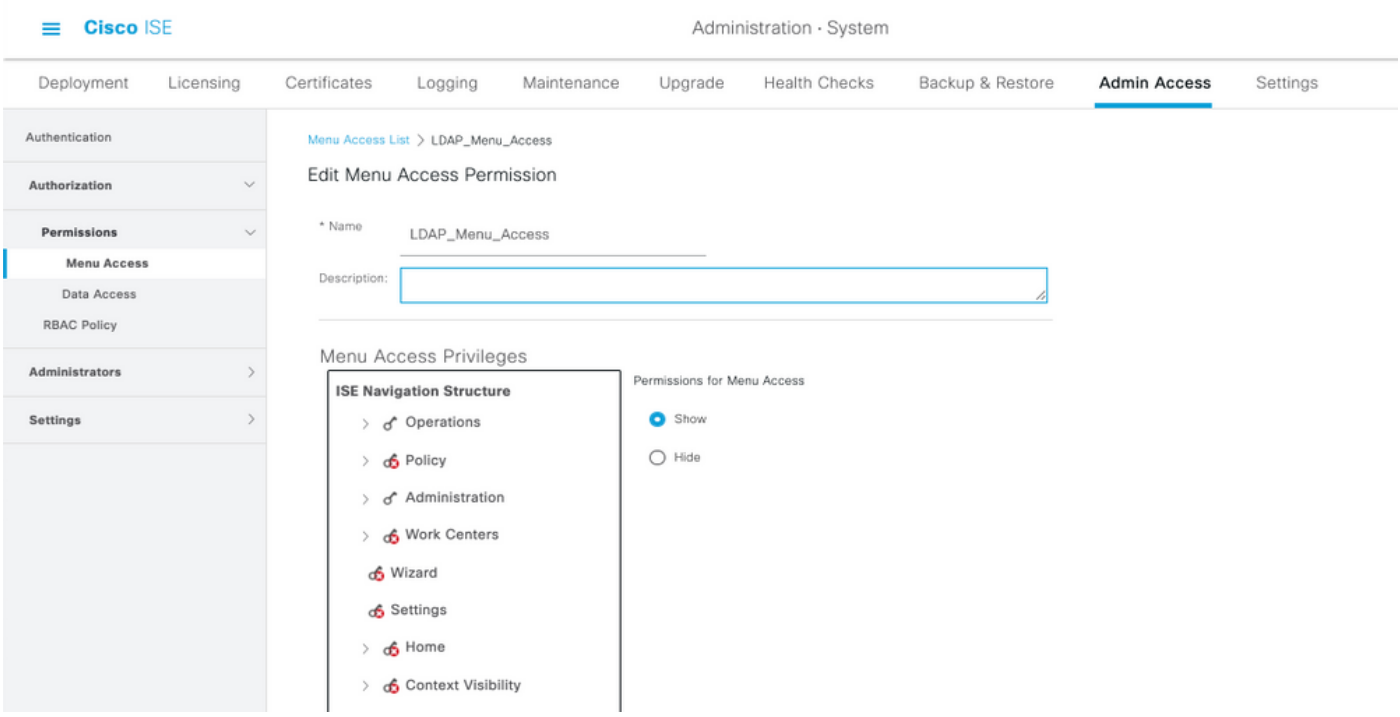


Definir permissões para acesso ao menu

1. Navegue até **ISE > Administration > System > Authorization > Permissions > Menu access**

2. Defina o acesso ao menu para que o usuário administrador acesse a GUI do ISE. Podemos configurar as subentidades a serem mostradas ou ocultadas na GUI para acesso personalizado para que um usuário execute apenas um conjunto de operações, se necessário.

3. Clique em **Salvar**.

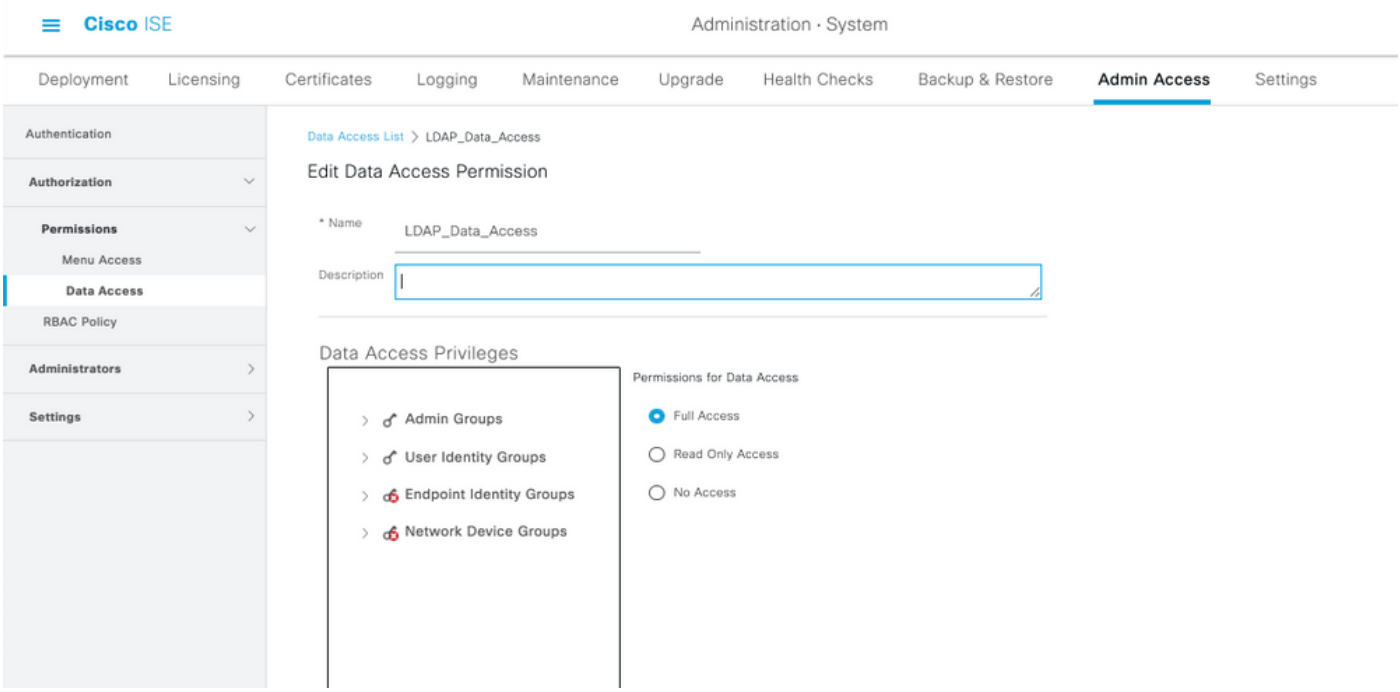


Definir permissões para acesso a dados

1. Navegue até **ISE > Administration > System > Authorization > Permissions > Data access**

2. Defina o acesso aos dados para que o usuário administrador tenha acesso total ou somente leitura aos grupos de identidade na GUI do ISE.

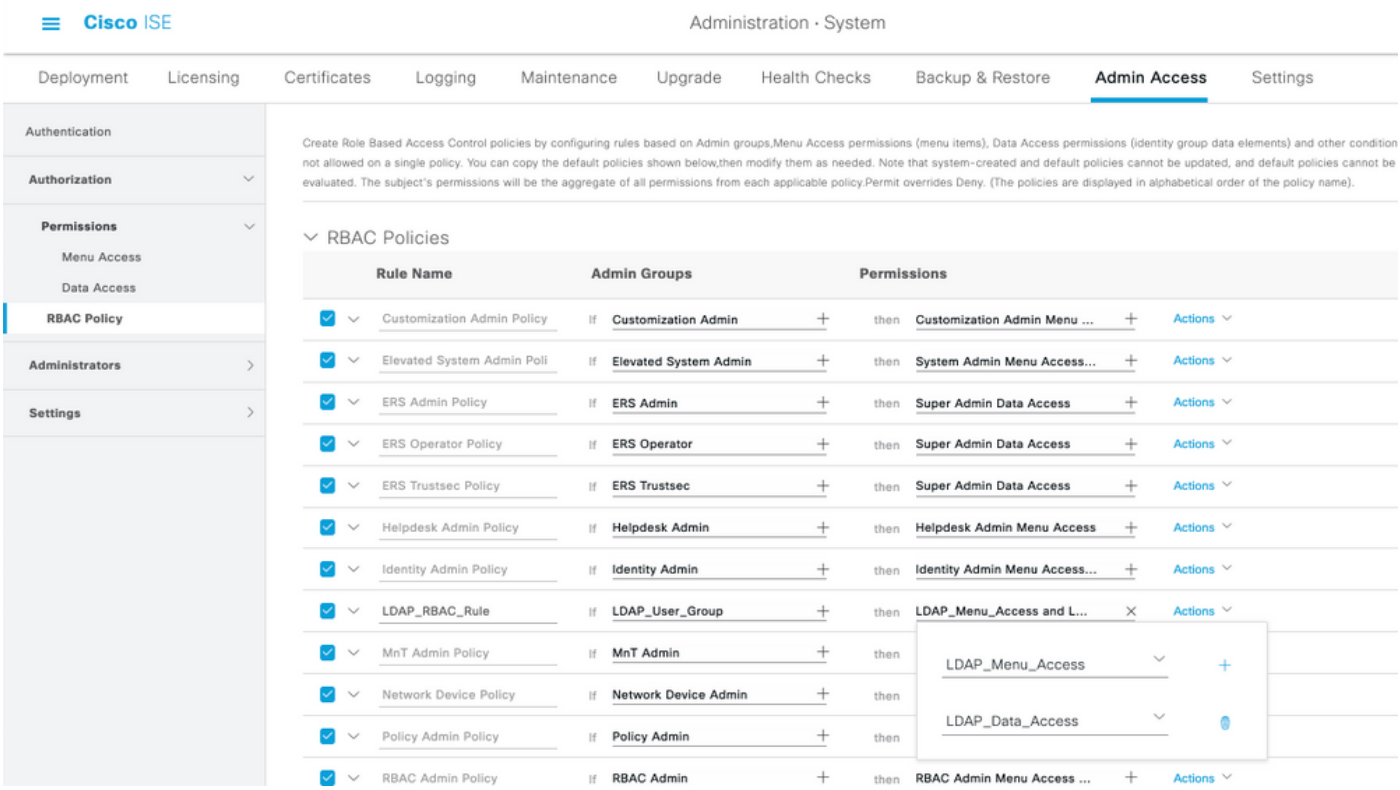
3. Clique em **Salvar**.



Definir permissões RBAC para o grupo de administração

1. Navegue até **ISE > Administration > System > Admin Access > Authorization > Policy**.

2. No menu suspenso **Ações** à direita, selecione **Inserir nova política abaixo** para adicionar uma nova política.
3. Crie uma nova regra chamada LDAP_RBAC_policy e mapeie-a com o Grupo Admin definido na seção Ativar acesso administrativo para AD e atribua-lhe permissões para acesso a menu e acesso a dados.
4. Clique em **Save Changes** e a confirmação das alterações salvas será exibida no canto inferior direito da GUI.

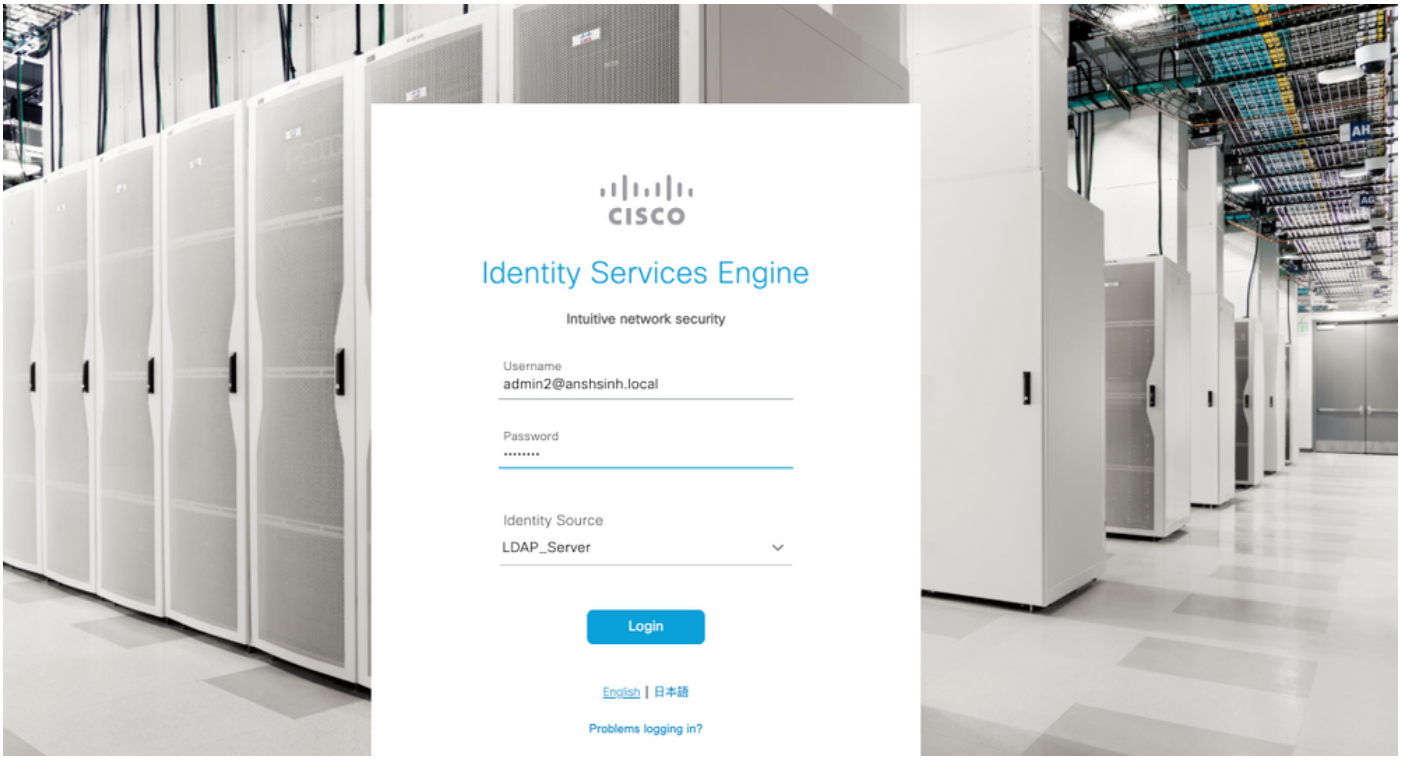


Verificar

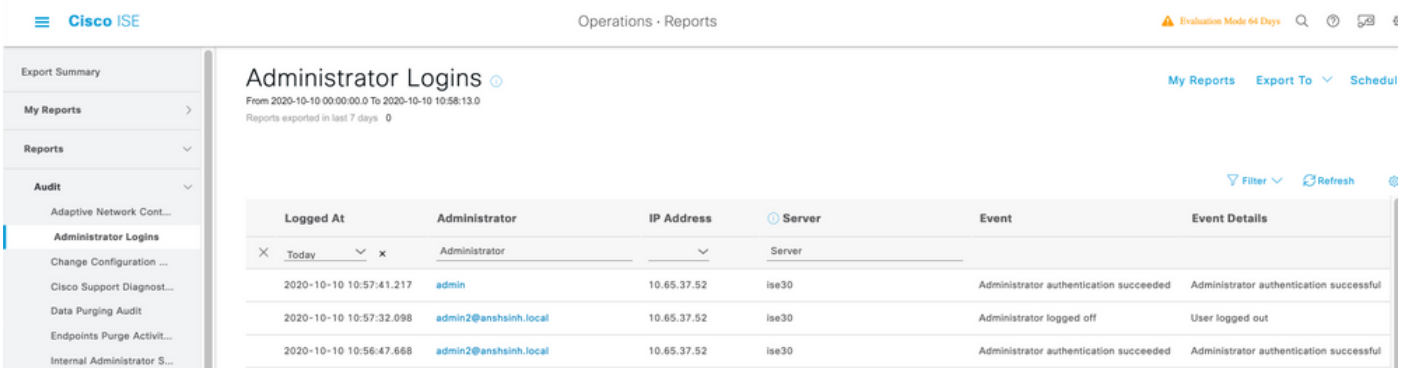
Acesse o ISE com credenciais do AD

Conclua estes passos para acessar o ISE com credenciais do AD:

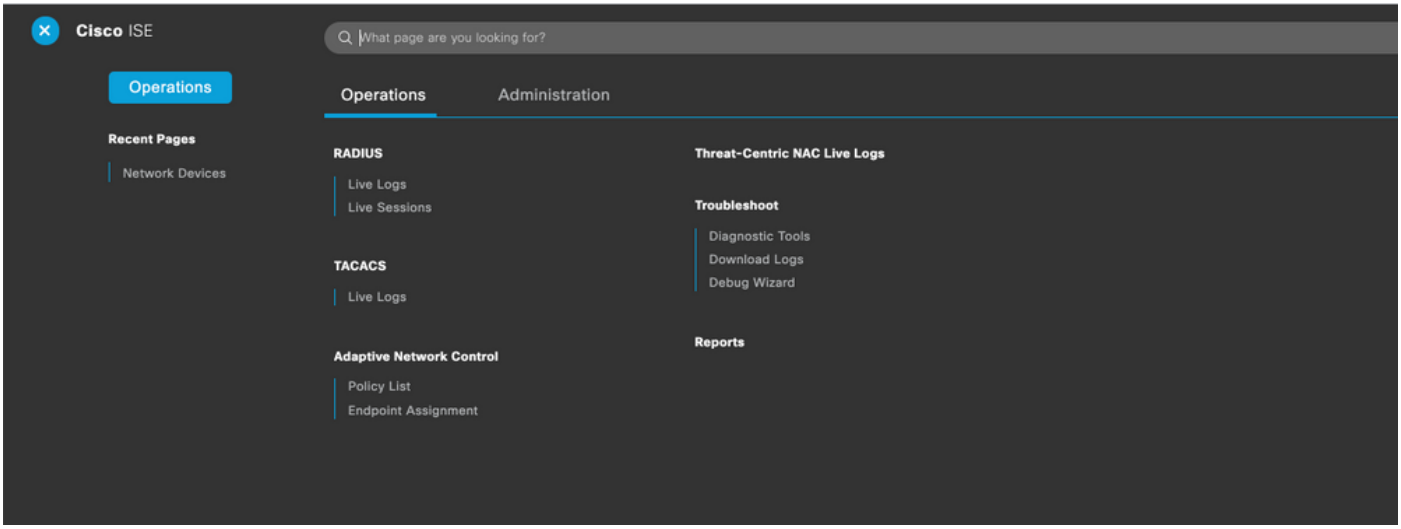
1. Abra a GUI do ISE para fazer login com o usuário LDAP.
2. Selecione LDAP_Server no menu suspenso **Origem da identidade**.
3. Insira o nome de usuário e a senha do banco de dados LDAP e faça login.



Verifique o login do administrador nos Relatórios de auditoria. Navegue até **ISE > Operations > Reports > Audit > Administrators Logins.**



Para confirmar se essa configuração funciona corretamente, verifique o nome de usuário autenticado no canto superior direito da GUI do ISE. Defina um acesso personalizado que tenha acesso limitado ao menu como mostrado aqui:



Troubleshoot

Informações gerais

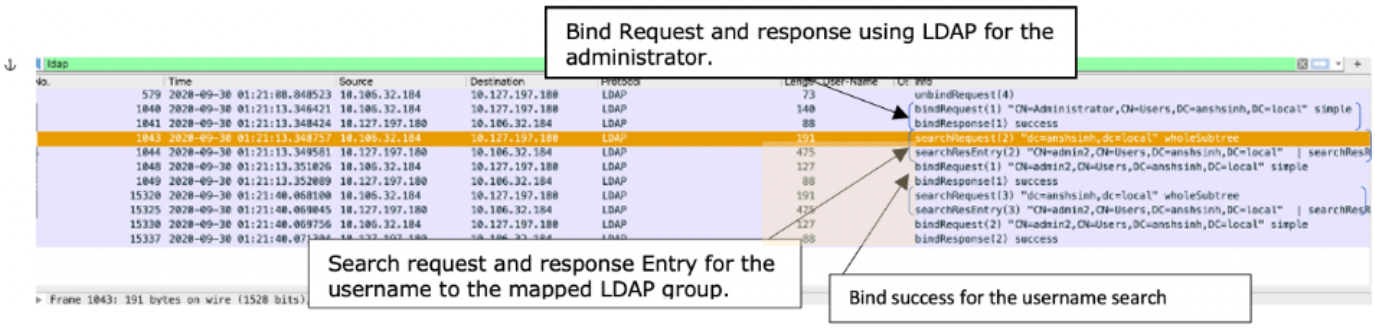
Para solucionar problemas do processo de RBAC, esses componentes do ISE precisam ser ativados na depuração no nó de administração do ISE :

RBAC - Isso imprimirá a mensagem relacionada ao RBAC quando tentarmos fazer login (ise-psc.log)

access-filter - Isso imprimirá o acesso ao filtro de recursos (ise-psc.log)

runtime-AAA - Isso imprimirá os logs para mensagens de interação de login e LDAP (prrt-server.log)

Análise de Captura de Pacotes



Análise de log

Verifique o servidor da porta.log

```
PAPAuthenticator,2020-10-10
08:54:00,621,DEBUG,0x7f852bee3700,cntx=0002480105,sesn=ise30/389444264/3178,CPMSessionID=ise30:u
serauth286,user=admin2@anshsinh.local,validateEvent: Username is [admin2@anshsinh.local]
bIsMachine is [0] isUtf8Valid is [1],PAPAuthenticator.cpp:86 IdentitySequence,2020-10-10
08:54:00,627,DEBUG,0x7f852c4e9700,cntx=0002480105,sesn=ise30/389444264/3178,CPMSessionID=ise30:u
serauth286,user=admin2@anshsinh.local,******* Authen
IDStoreName:LDAP_Server,IdentitySequenceWorkflow.cpp:377 LDAPIDStore,2020-10-10
08:54:00,628,DEBUG,0x7f852c4e9700,cntx=0002480105,sesn=ise30/389444264/3178,CPMSessionID=ise30:u
serauth286,user=admin2@anshsinh.local,Send event to LDAP_Server_924OqzxSbv_199_Primary
server,LDAPIDStore.h:205 Server,2020-10-10
08:54:00,634,DEBUG,0x7f85293b8700,cntx=0002480105,sesn=ise30/389444264/3178,CPMSessionID=ise30:u
serauth286,user=admin2@anshsinh.local,LdapServer::onAcquireConnectionResponse: succeeded to
acquire connection,LdapServer.cpp:724 Connection,2020-10-10
08:54:00,634,DEBUG,0x7f85293b8700,LdapConnectionContext::sendSearchRequest(id = 1221): base =
dc=anshsinh,dc=local, filter =
(&(objectclass=Person)(userPrincipalName=admin2@anshsinh.local)),LdapConnectionContext.cpp:516
Server,2020-10-10
08:54:00,635,DEBUG,0x7f85293b8700,cntx=0002480105,sesn=ise30/389444264/3178,CPMSessionID=ise30:u
serauth286,user=admin2@anshsinh.local,LdapSubjectSearchAssistant::processAttributes: found
CN=admin2,CN=Users,DC=anshsinh,DC=local entry matching admin2@anshsinh.local
subject,LdapSubjectSearchAssistant.cpp:268 Server,2020-10-10
```

```
08:54:00,635,DEBUG,0x7f85293b8700,cntx=0002480105,sesn=ise30/389444264/3178,CPMSessionID=ise30:u
serauth286,user=admin2@anshsinh.local,LdapSubjectSearchAssistant::processGroupAttr: attr =
memberOf, value = CN=employee,CN=Users,DC=anshsinh,DC=local,LdapSubjectSearchAssistant.cpp:389
Server,2020-10-10
08:54:00,636,DEBUG,0x7f85293b8700,cntx=0002480105,sesn=ise30/389444264/3178,CPMSessionID=ise30:u
serauth286,user=admin2@anshsinh.local,LdapServer::onAcquireConnectionResponse: succeeded to
acquire connection,LdapServer.cpp:724 Server,2020-10-10
08:54:00,636,DEBUG,0x7f85293b8700,cntx=0002480105,sesn=ise30/389444264/3178,CPMSessionID=ise30:u
serauth286,user=admin2@anshsinh.local,LdapServer::authenticate: user = admin2@anshsinh.local, dn
= CN=admin2,CN=Users,DC=anshsinh,DC=local,LdapServer.cpp:352 Connection,2020-10-10
08:54:00,636,DEBUG,0x7f85293b8700,LdapConnectionContext::sendBindRequest(id = 1223): dn =
CN=admin2,CN=Users,DC=anshsinh,DC=local,LdapConnectionContext.cpp:490 Server,2020-10-10
08:54:00,640,DEBUG,0x7f85293b8700,cntx=0002480105,sesn=ise30/389444264/3178,CPMSessionID=ise30:u
serauth286,user=admin2@anshsinh.local,LdapServer::handleAuthenticateSuccess: authentication of
admin2@anshsinh.local user succeeded,LdapServer.cpp:474 LDAPIDStore,2020-10-10
08:54:00,641,DEBUG,0x7f852c6eb700,cntx=0002480105,sesn=ise30/389444264/3178,CPMSessionID=ise30:u
serauth286,user=admin2@anshsinh.local,LDAPIDStore::onResponse:
LdapOperationStatus=AuthenticationSucceeded -> AuthenticationResult=Passed,LDAPIDStore.cpp:336
```

Verifique o ise-psc.log

Nesses registros, você pode verificar a política de RBAC usada para o usuário admin2 quando tentar acessar o recurso de dispositivo de rede -

```
2020-10-10 08:54:24,474 DEBUG [admin-http-pool51][] com.cisco.cpm.rbacfilter.AccessUtil -
:admin2@anshsinh.local:::- For admin2@anshsinh.local on /NetworkDevicesLPInputAction.do --
ACCESS ALLOWED BY MATCHING administration_networkresources_devices 2020-10-10 08:54:24,524 INFO
[admin-http-pool51][] cpm.admin.ac.actions.NetworkDevicesLPInputAction -
:admin2@anshsinh.local:::- In NetworkDevicesLPInputAction container method 2020-10-10
08:54:24,524 DEBUG [admin-http-pool51][] cisco.ise.rbac.authorization.RBACAuthorization -
:admin2@anshsinh.local:::- :::::::::Inside RBACAuthorization.getDataEntityDecision::::::
userName admin2@anshsinh.local dataType RBAC_NETWORK_DEVICE_GROUP permission ALL 2020-10-10
08:54:24,526 DEBUG [admin-http-pool51][] ise.rbac.evaluator.impl.DataPermissionEvaluatorImpl -
:admin2@anshsinh.local:::- In DataPermissionEvaluator:hasPermission 2020-10-10 08:54:24,526
DEBUG [admin-http-pool51][] ise.rbac.evaluator.impl.DataPermissionEvaluatorImpl -
:admin2@anshsinh.local:::- Data access being evaluated:LDAP_Data_Access 2020-10-10 08:54:24,528
DEBUG [admin-http-pool51][] cisco.ise.rbac.authorization.RBACAuthorization -
:admin2@anshsinh.local:::- :::::::::Inside RBACAuthorization.getDataEntityDecision::::::
permission retrieved false 2020-10-10 08:54:24,528 INFO [admin-http-pool51][]
cpm.admin.ac.actions.NetworkDevicesLPInputAction -:admin2@anshsinh.local:::- Finished with rbac
execution 2020-10-10 08:54:24,534 INFO [admin-http-pool51][]
cisco.cpm.admin.license.TrustSecLicensingUIFilter -:admin2@anshsinh.local:::- Should TrustSec be
visible :true 2020-10-10 08:54:24,593 DEBUG [admin-http-pool51][]
cisco.ise.rbac.authorization.RBACAuthorization -:admin2@anshsinh.local:::- :::::::::Inside
RBACAuthorization.getPermittedNDG:::::: userName admin2@anshsinh.local 2020-10-10 08:54:24,595
DEBUG [admin-http-pool51][] ise.rbac.evaluator.impl.DataPermissionEvaluatorImpl -
:admin2@anshsinh.local:::- In DataPermissionEvaluator:getPermittedNDGMap 2020-10-10 08:54:24,597
DEBUG [admin-http-pool51][] ise.rbac.evaluator.impl.DataPermissionEvaluatorImpl -
:admin2@anshsinh.local:::- processing data Access :LDAP_Data_Access 2020-10-10 08:54:24,604 INFO
[admin-http-pool51][] cisco.cpm.admin.license.TrustSecLicensingUIFilter -
:admin2@anshsinh.local:::- Should TrustSec be visible :true
```