基于ISE角色的LDAP访问控制

目录

简介

本文档介绍将轻量级目录访问协议(LDAP)用作外部身份库以管理访问思科身份服务引擎(ISE)管理GUI的配置示例。

先决条件

Cisco 建议您了解以下主题：

- 思科ISE版本3.0的配置
- LDAP（轻量级目录访问协议）

要求

本文档中的信息基于以下软件和硬件版本：

- 思科ISE版本3.0
- Windows Server 2016

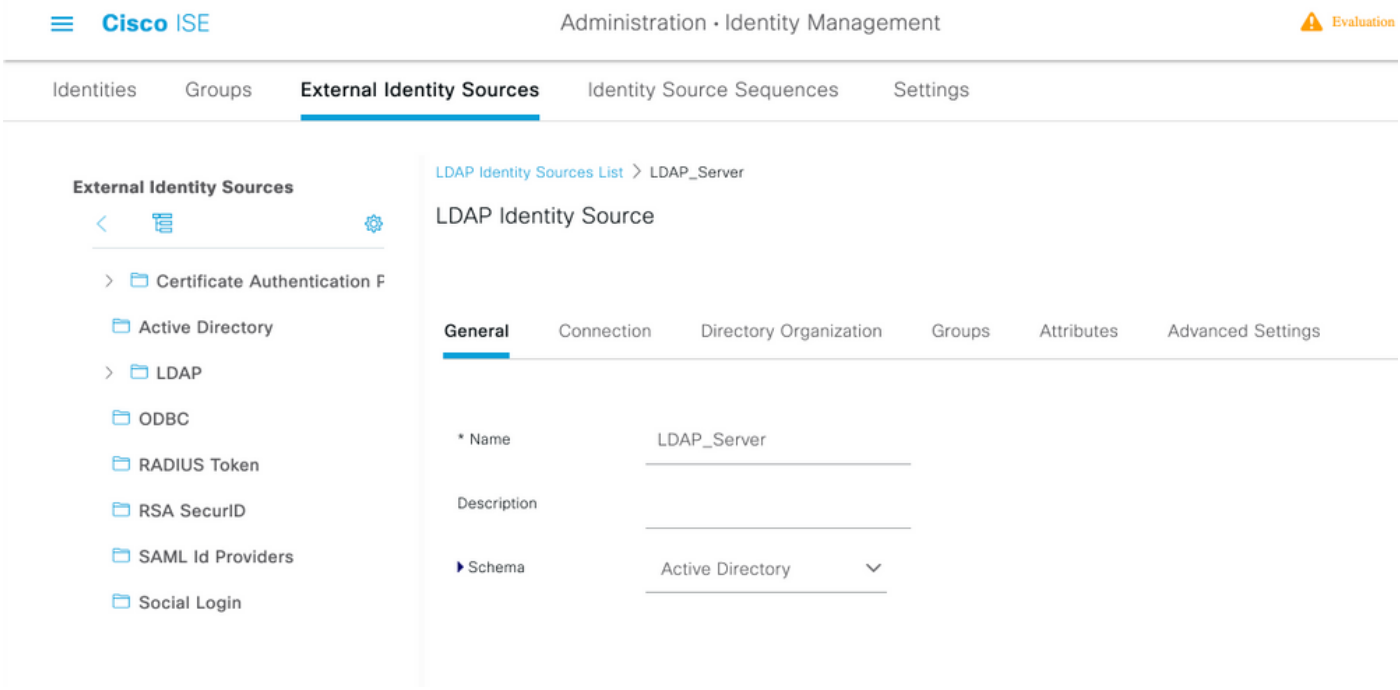
本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

配置

使用以下部分配置基于LDAP的用户，以获得对ISE GUI的基于管理/自定义的访问。以下配置使用LDAP协议查询从Active Directory获取用户以执行身份验证。

将ISE加入LDAP

1. 导航至**管理>身份管理>外部身份源> Active Directory > LDAP。**
2. 在**General**选项卡下，输入LDAP的名称并选择架构Active Directory。



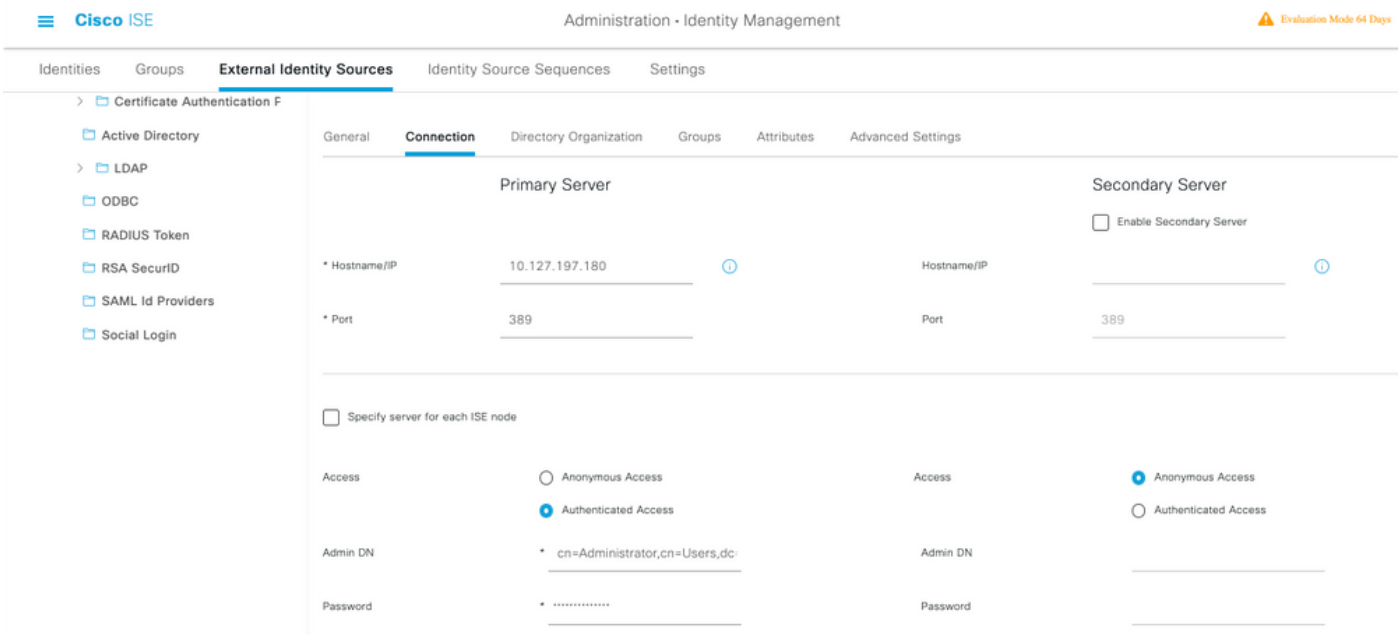
配置连接类型和LDAP配置

1.导航至**ISE >管理>身份管理>外部身份源> LDAP。**

2.配置主LDAP服务器的主机名以及端口389(LDAP)/636(LDAP-Secure)。

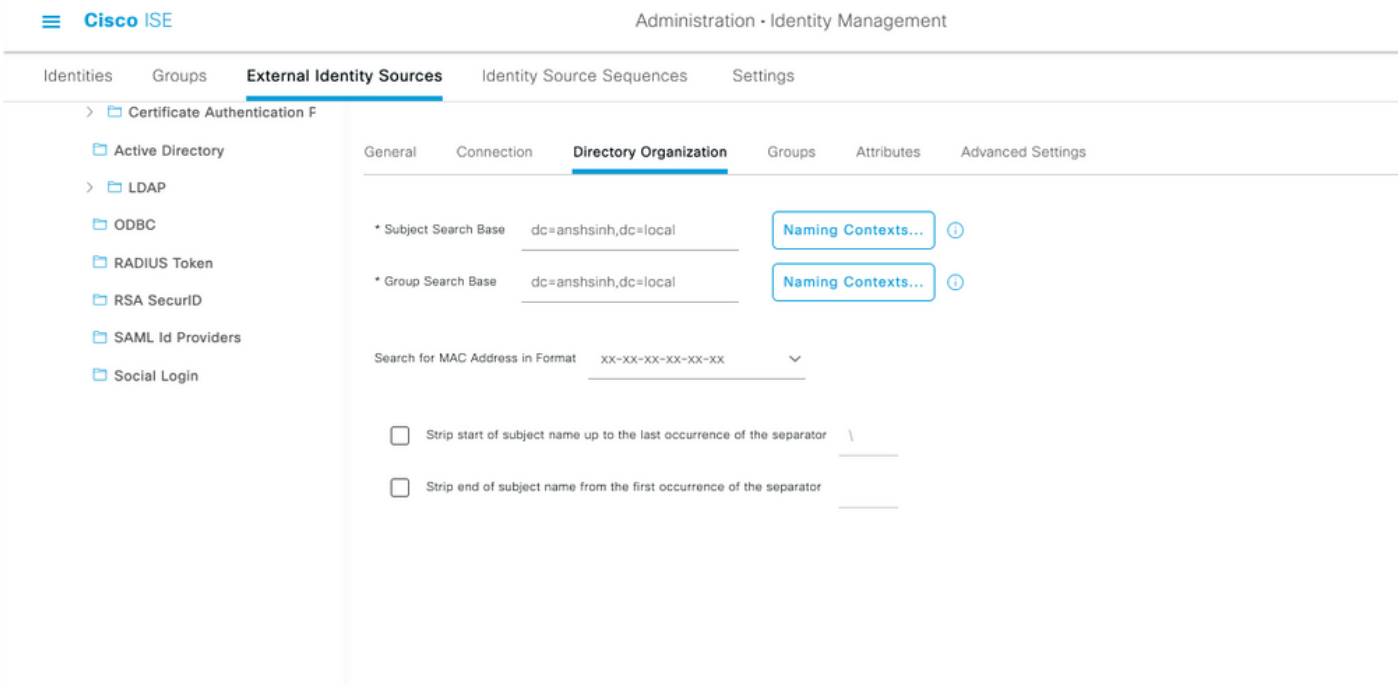
3.输入管理员可分辨名称(DN)的路径和LDAP服务器的管理员密码。

4.点击Test Bind Server以测试ISE中LDAP服务器的可达性。



配置目录组织、组和属性

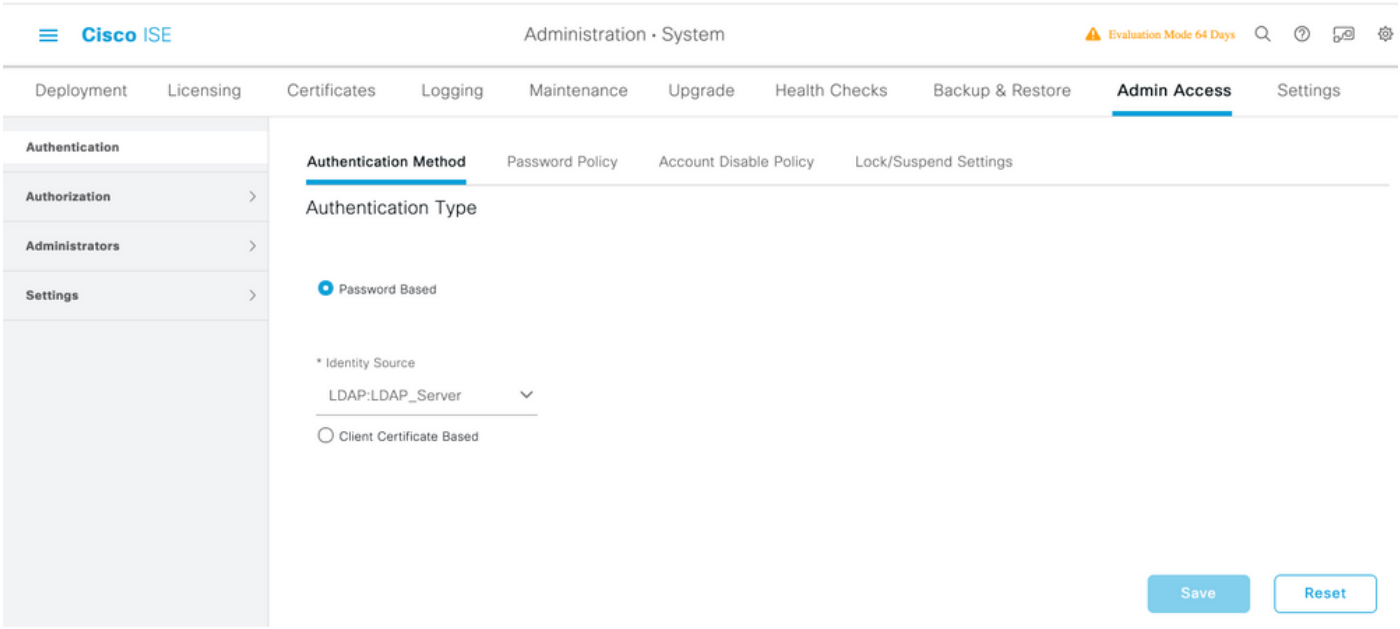
1.根据LDAP服务器中存储的用户的层次结构选择用户的正确组织组。



为LDAP用户启用管理访问

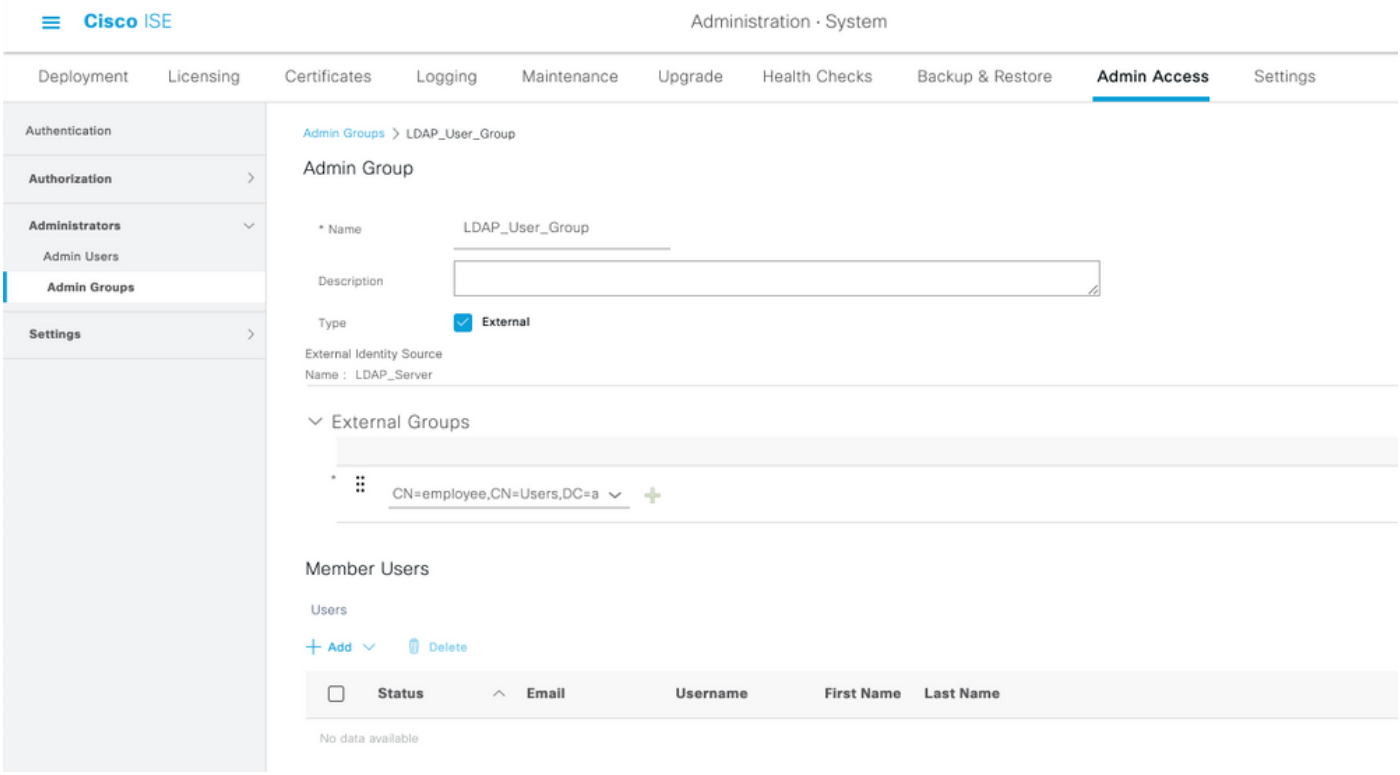
要启用基于密码的身份验证，请完成以下步骤。

1. 导航至**ISE > Administration > System > Admin Access > Authentication**。
2. 在Authentication Method选**项卡下**，选择Password-**Based选**项。
3. 从“**身份**源”下**拉菜**单中选择LDAP。
4. 点击Save Changes。



将管理组映射到LDAP组

在ISE上配置管理组并将其映射到AD组。这允许已配置用户根据基于组成员资格的管理员已配置的RBAC权限，根据授权策略获取访问权限。

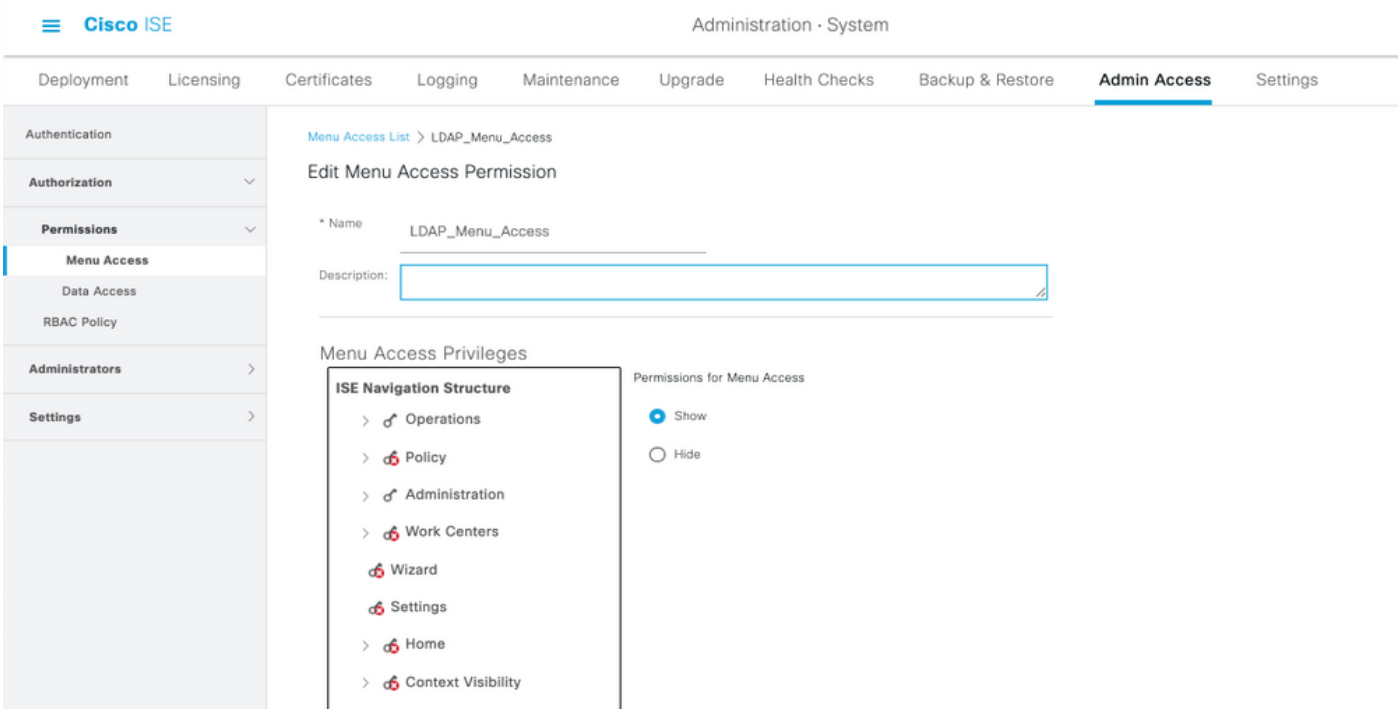


设置菜单访问权限

1.导航至**ISE >管理>系统>授权>权限>菜单访问**

2.定义管理员用户访问ISE GUI的菜单访问权限。我们可以配置要在GUI上显示或隐藏的子实体，以便用户在需要时仅执行一组操作时进行自定义访问。

3.单击“保存”。

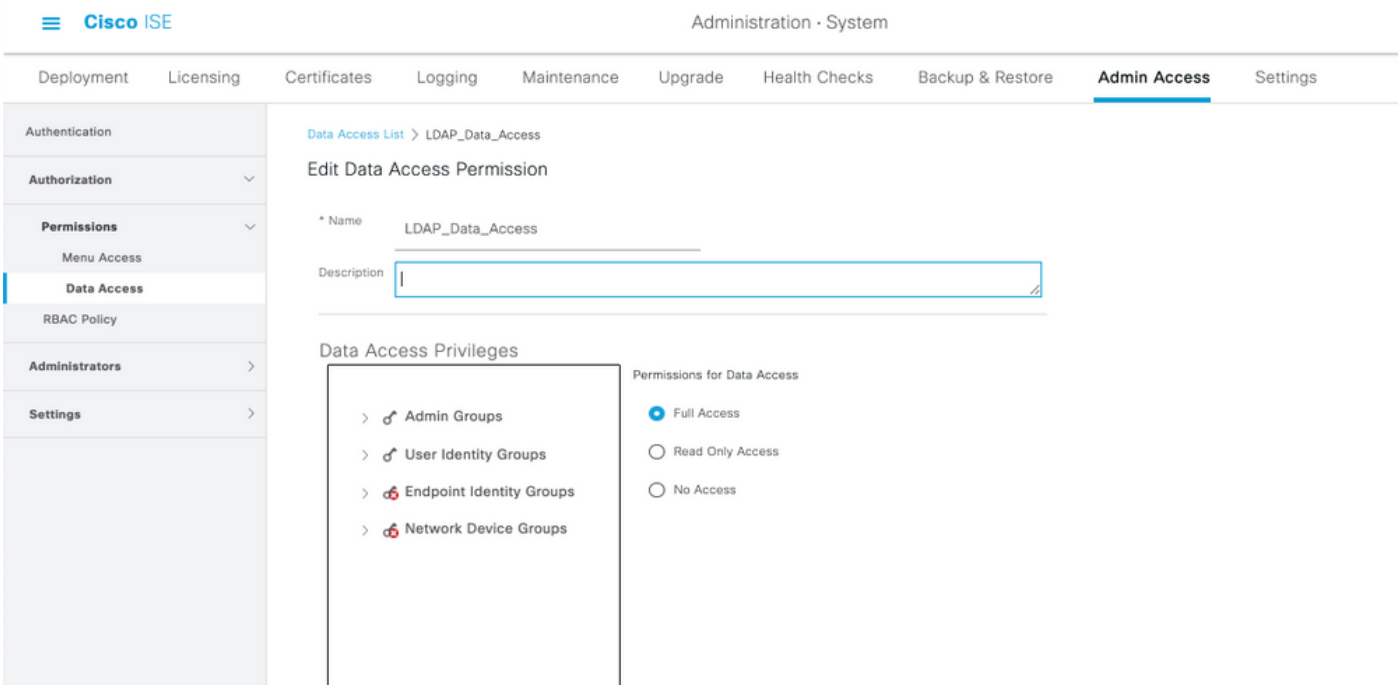


设置数据访问权限

1.导航至**ISE > Administration > System > Authorization > Permissions > Data access**

2.定义管理员用户对ISE GUI上的身份组具有完全访问权限或只读访问权限的数据访问权限。

3.单击“保存”。

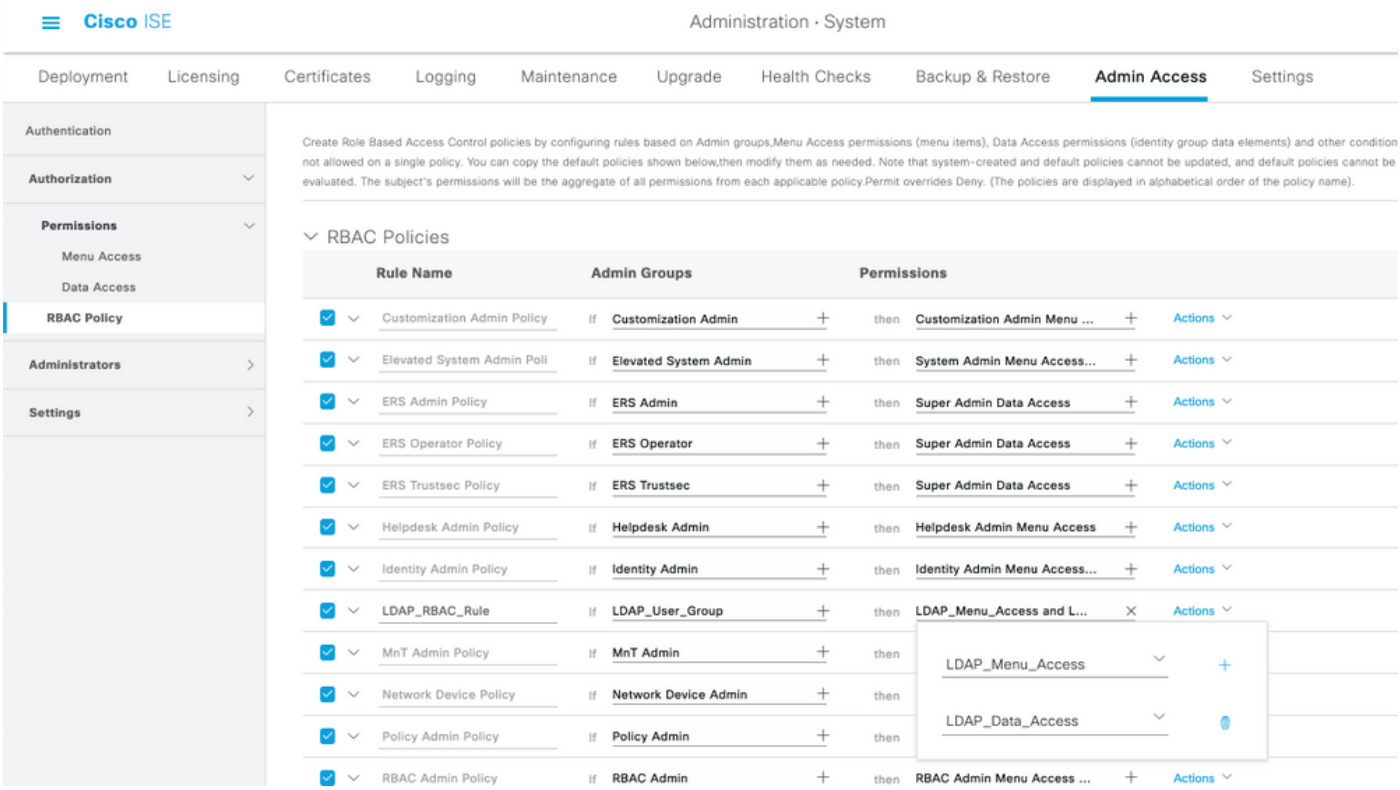


为管理员组设置RBAC权限

1. 导航至**ISE > Administration > System > Admin Access > Authorization > Policy**。
2. 从右侧**的“操**作”下拉菜单中，选择**Insert New Policy Below** 以添加新策略。
3. 创建名为LDAP_RBAC_policy的新规则，并将其与在“启用AD的管理访问”部分中定义的管理组

进行映射，并为其分配菜单访问和数据访问权限。

4. 单击**Save Changes**,GUI右下角将显示保存的更改的确认。

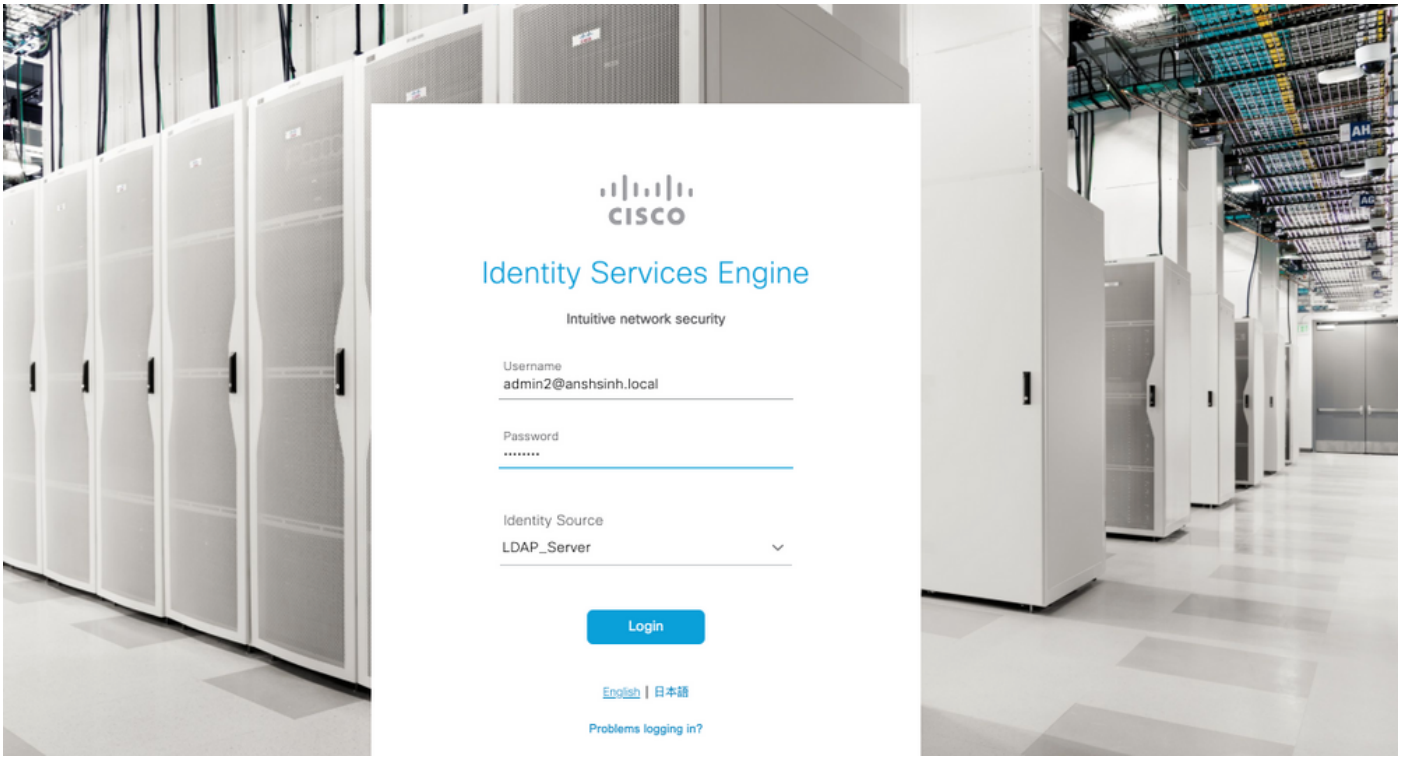


验证

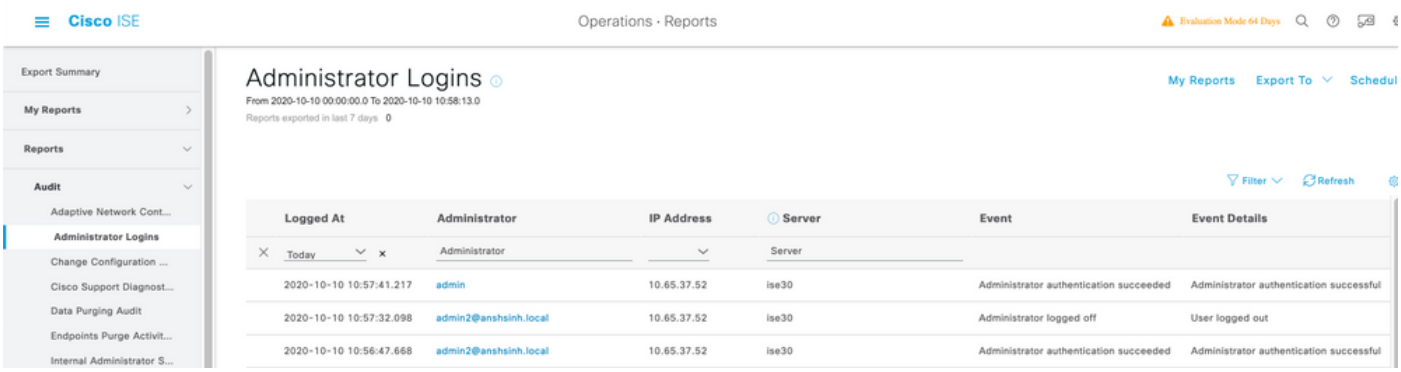
使用AD凭证访问ISE

要使用AD凭证访问ISE，请完成以下步骤：

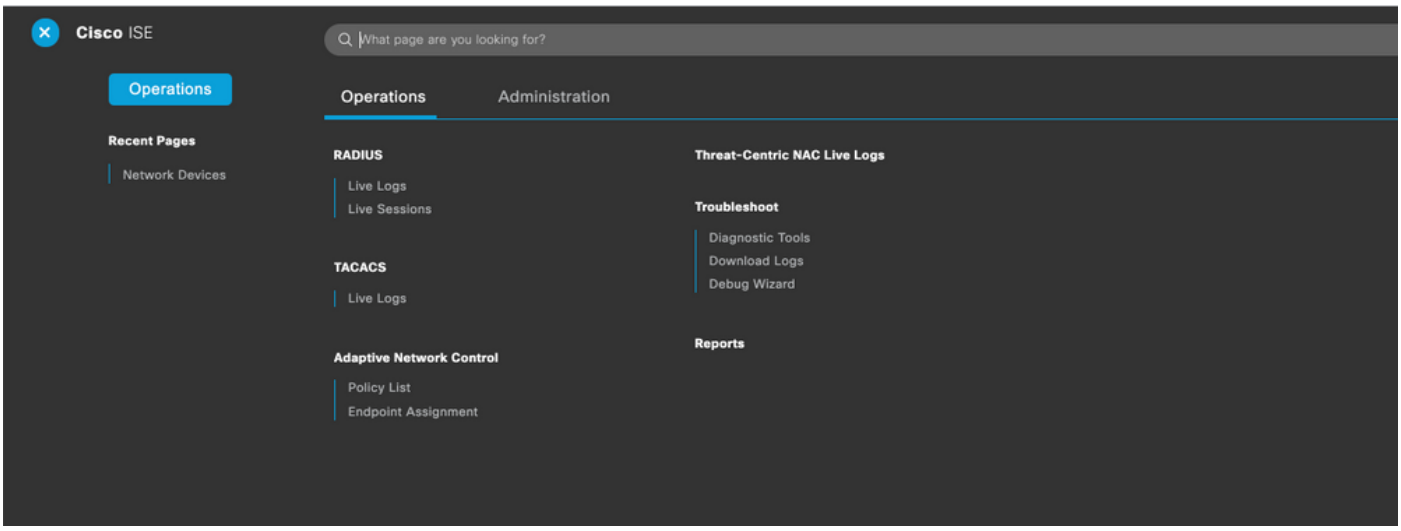
1. 打开ISE GUI以使用LDAP用户登录。
2. 从Identity Source下拉菜单中选择**LDAP**_Server。
3. 从LDAP数据库输入用户名和密码，然后登录。



在审核报告中验证管理员登录的登录。导航至**ISE > Operations > Reports > Audit > Administrators Logins**。



要确认此配置工作正常，请在ISE GUI右上角验证经过身份验证的用户名。定义基于自定义的访问权限，该权限对菜单的访问受限，如下所示：



故障排除

一般信息

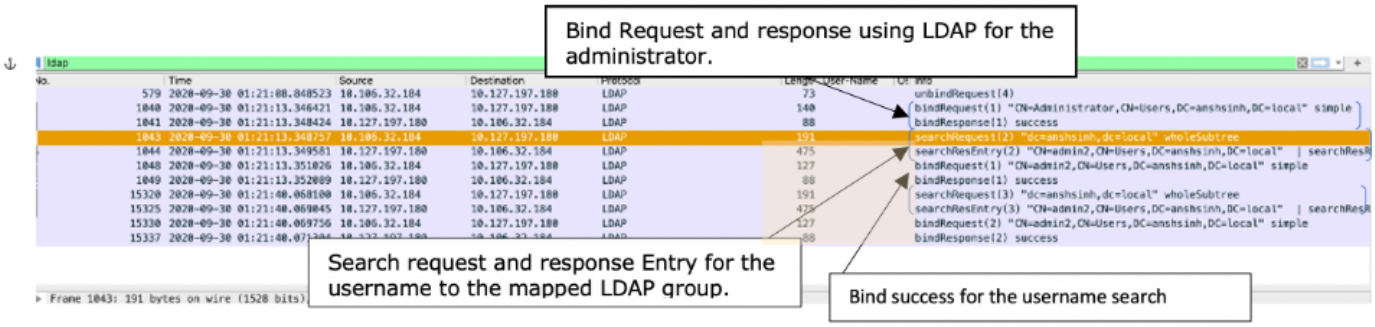
要排除RBAC进程故障，必须在ISE管理节点的调试中启用这些ISE组件：

RBAC — 当我们尝试登录时(ise-psc.log)，此操作将打印RBAC相关消息

access-filter — 将打印资源过滤器访问(ise-psc.log)

runtime-AAA — 这将打印登录和LDAP交互消息的日志(prrt-server.log)

数据包捕获分析



日志分析

检验prrt-server.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
```

验证ise-psc.log

从这些日志中，您可以验证在尝试访问网络设备资源时用于admin2用户的RBAC策略 —

```
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
```