使用轻量级目录访问协议配置基于ISE角色的访问控制

目录

[简介](#)

[先决条件](#)

- [要求](#)

[配置](#)

- [将ISE加入LDAP](#)
- [为LDAP用户启用管理访问](#)
- [将管理员组映射到LDAP组](#)
  - [设置菜单访问的权限](#)
  - [设置数据访问的权限](#)
  - [设置管理员组的RBAC权限](#)

[验证](#)

- [使用AD凭证访问ISE](#)

[故障排除](#)

- [一般信息](#)
- [数据包捕获分析](#)
- [日志分析](#)
  - [检验prrt-server.log](#)
  - [验证theise-psc.log](#)

简介

本文档介绍使用轻量级目录访问协议(LDAP)作为外部身份库对思科身份服务引擎(ISE)管理GUI进行管理访问的配置示例。

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

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

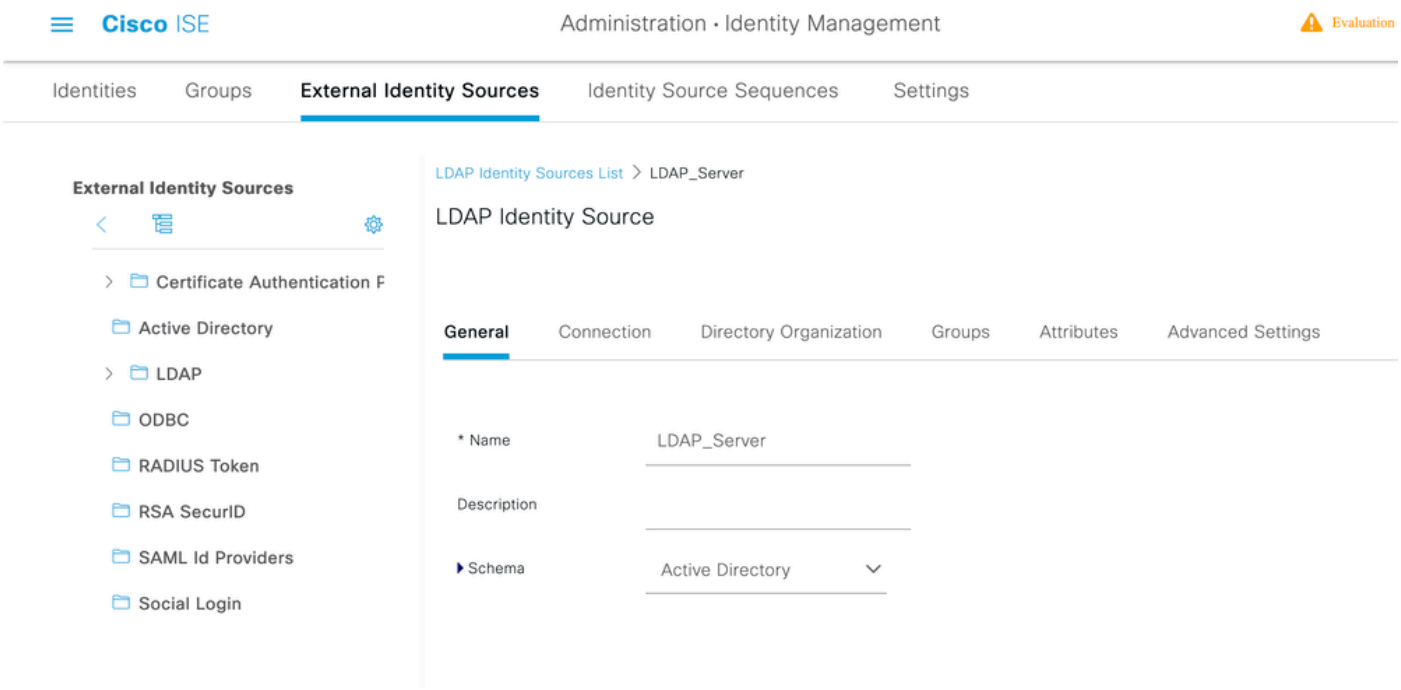
本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

配置

使用部分配置基于LDAP的用户以获取ISE GUI的管理/基于自定义的访问。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. 导航到管理>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，然后选择方案Active Directory。



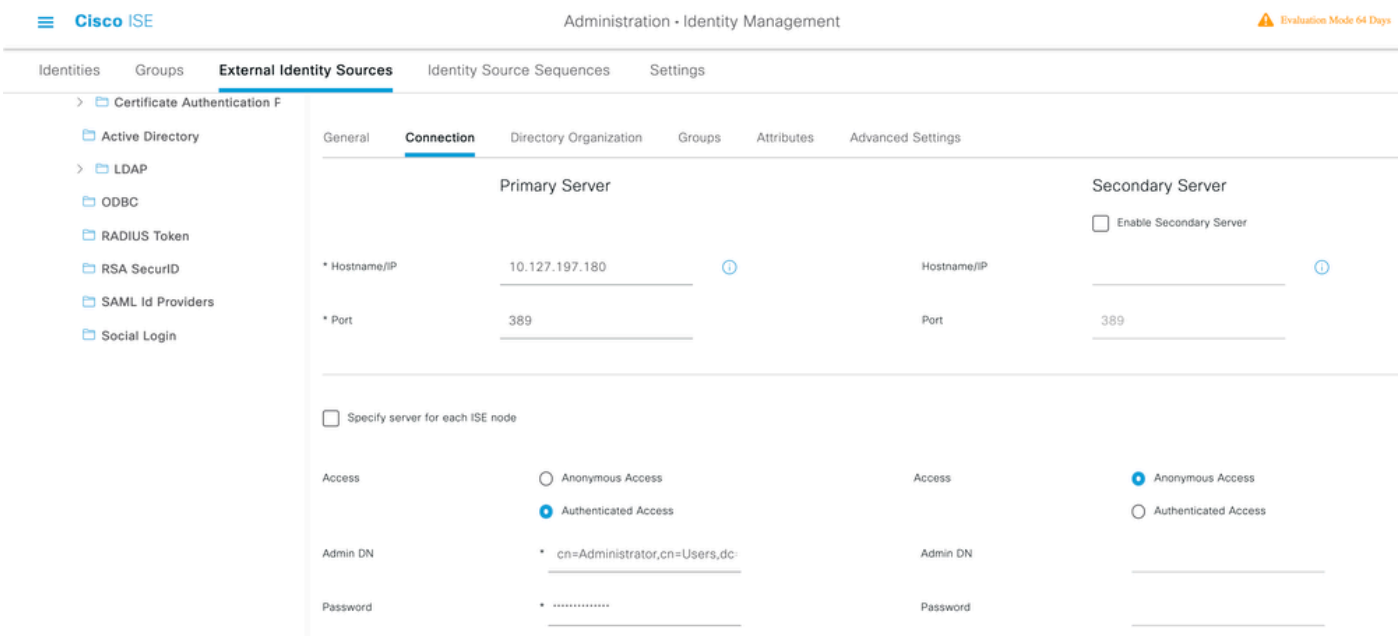
配置连接类型和LDAP配置

1.导航到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)。

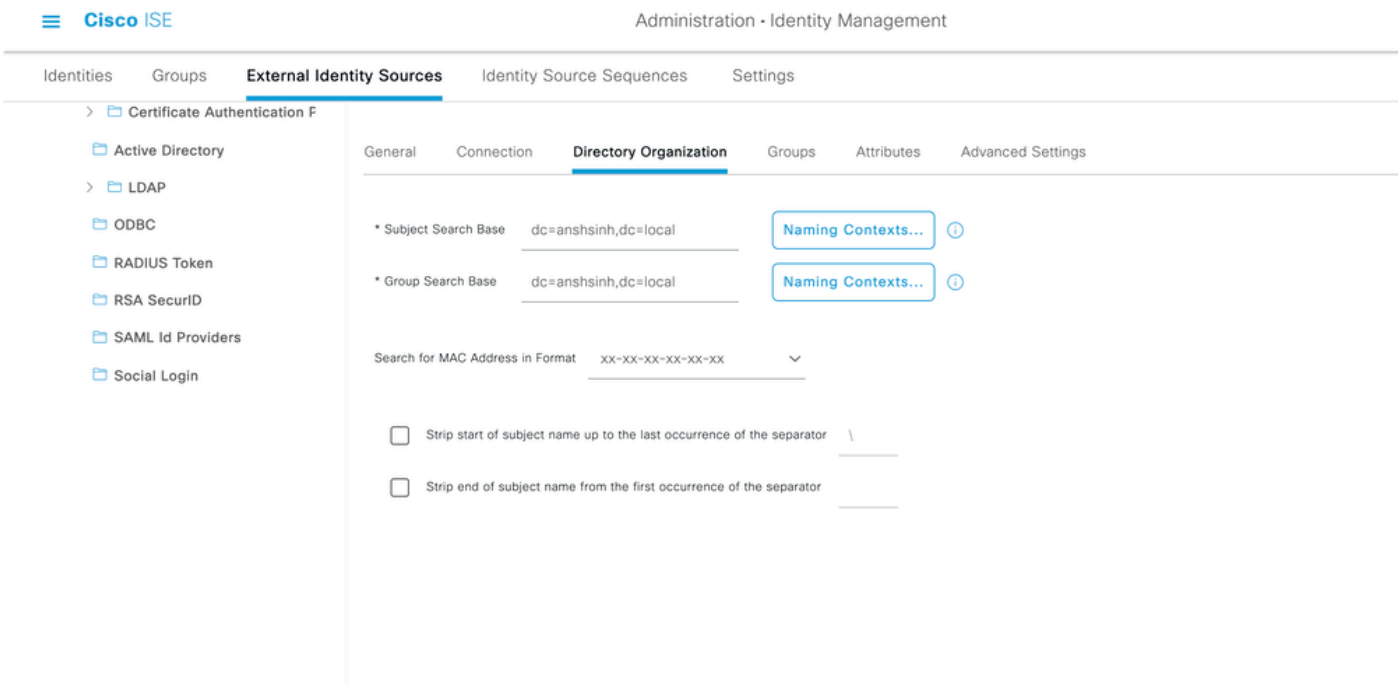
3.输入管理员可分辨名称(DN)的路径以及LDAP服务器的管理员密码。

4.点击Test Bind Server以测试从ISE访问LDAP服务器的能力。



配置目录组织、组和属性

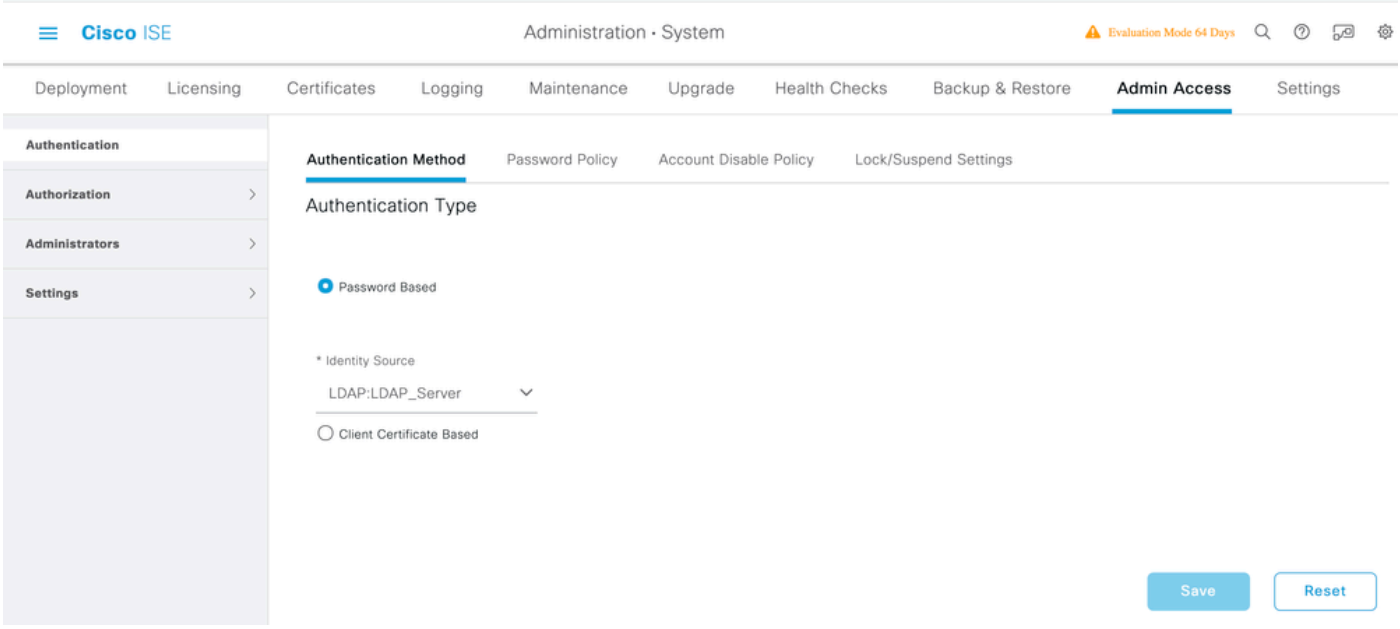
1.根据LDAP服务器中存储的用户的层次结构选择正确的用户组织组。



为LDAP用户启用管理访问

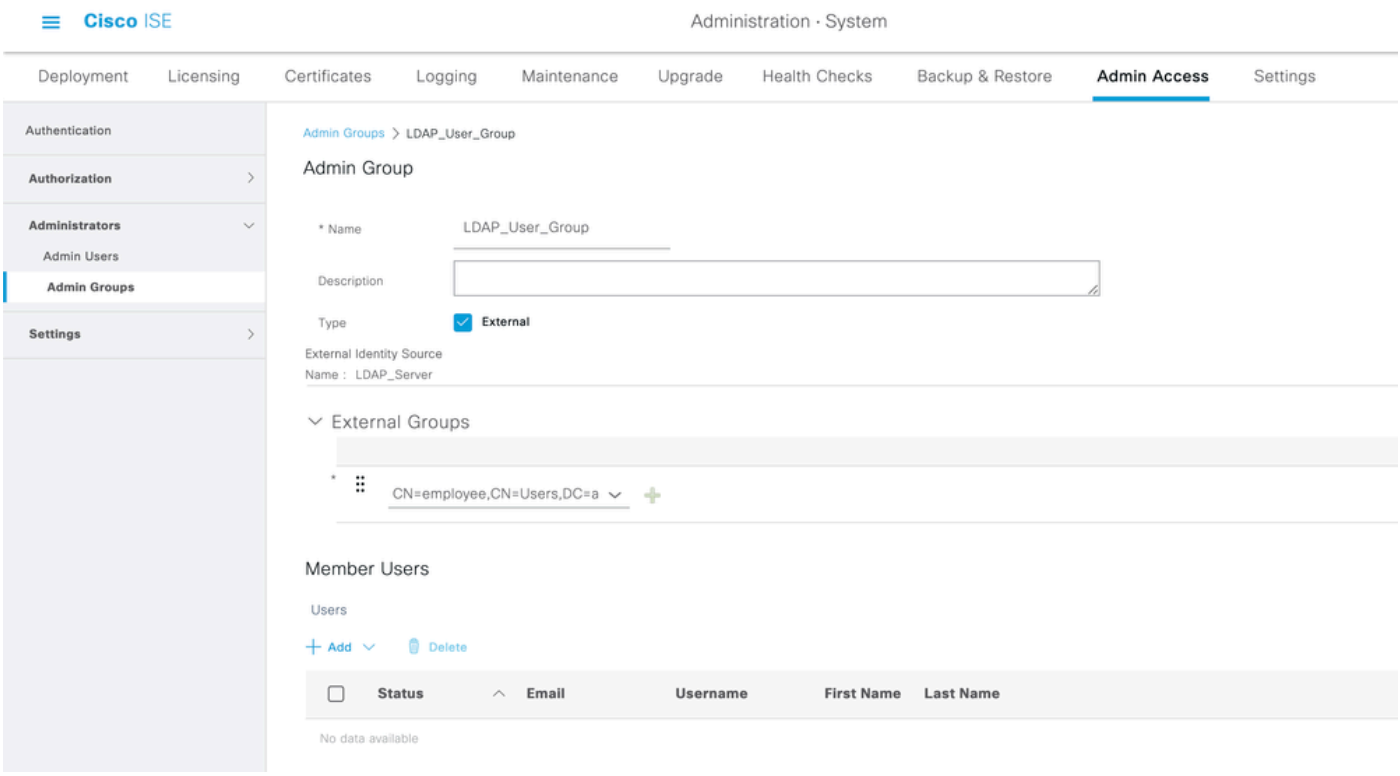
要启用基于密码的身份验证，请完成以下步骤。

1. 导航到ISE > Administration > System > Admin Access > Authentication。
2. 在Authentication Method选项卡下，选择Password-Based选项。
3. 从Identity Source下拉菜单中选择LDAP。
4. 点击Save Changes。



将管理员组映射到LDAP组

在ISE上配置管理员组并将其映射到AD组。这允许配置的用户根据基于组成员资格的管理员配置的RBAC权限，根据授权策略获得访问权限。

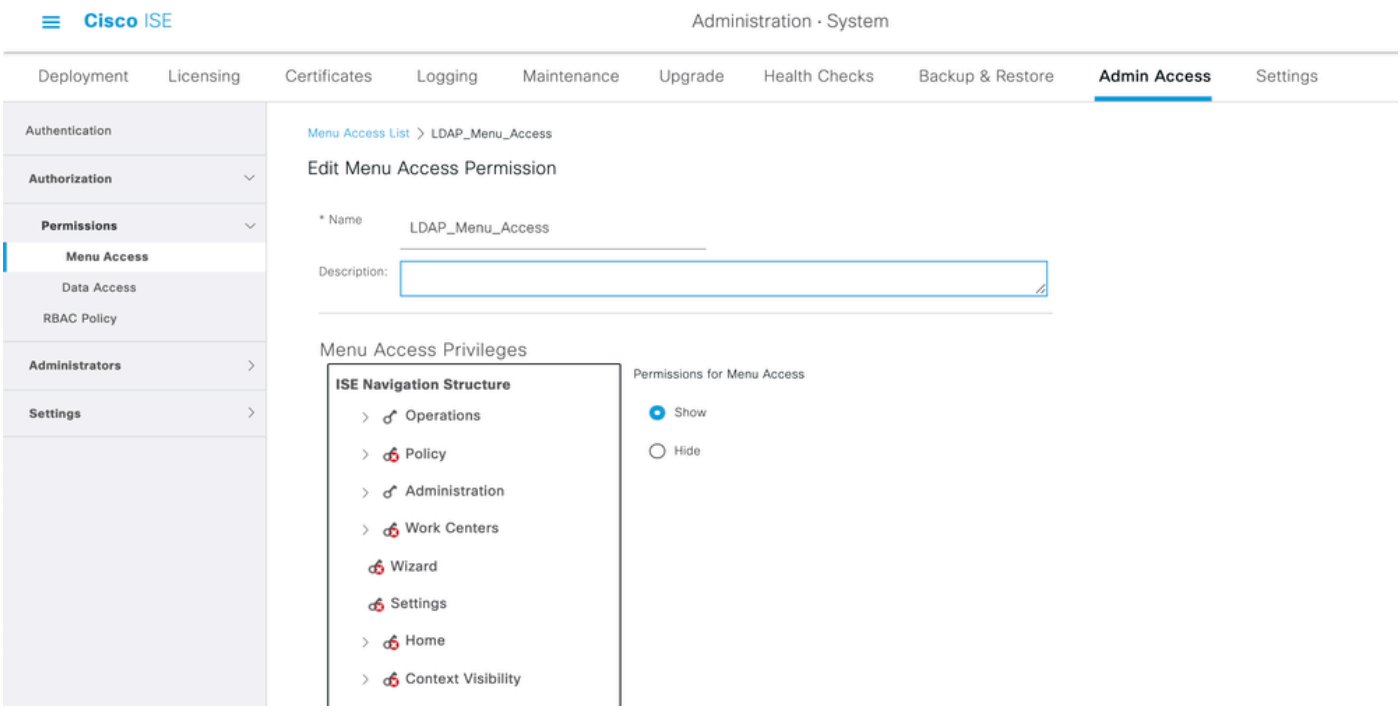


设置菜单访问的权限

1.导航到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。您可以配置在GUI上显示或隐藏的子实体，以便用户进行自定义访问，从而仅在需要时执行一组操作。

3.单击Save。

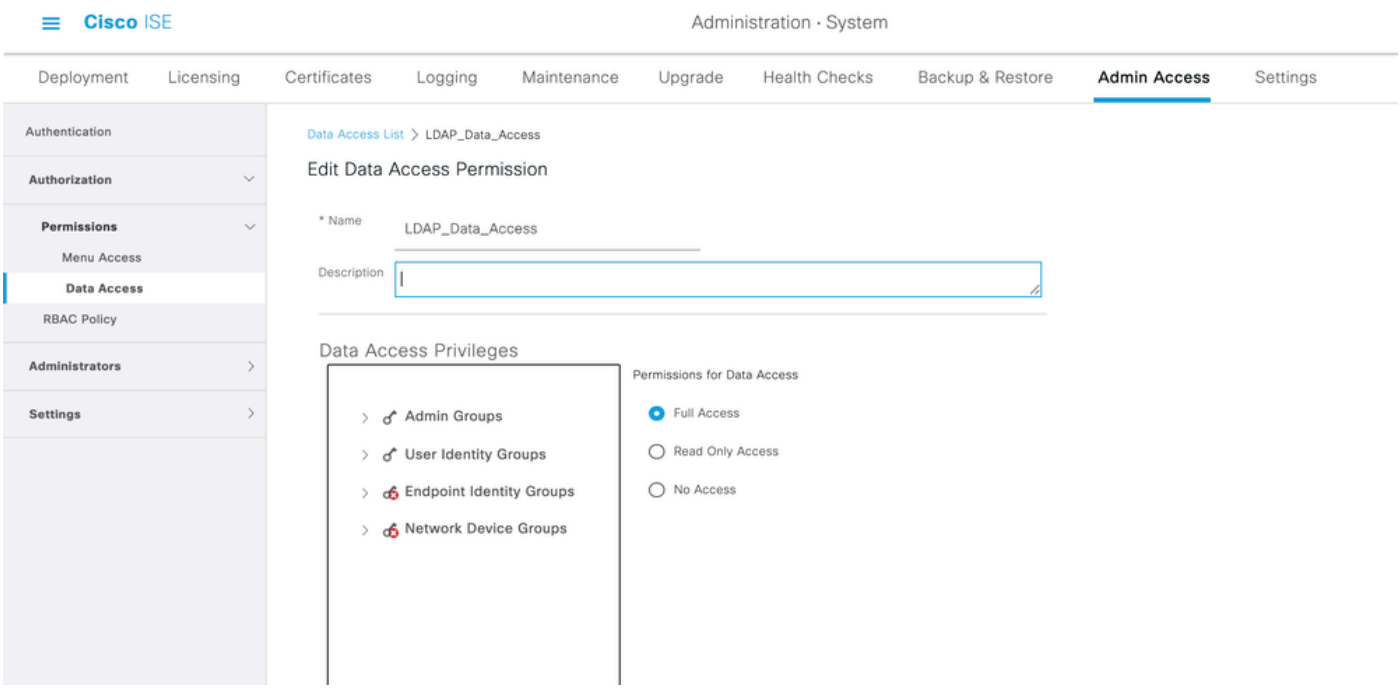


设置数据访问的权限

1.导航到ISE >管理>系统>授权>权限>数据访问。

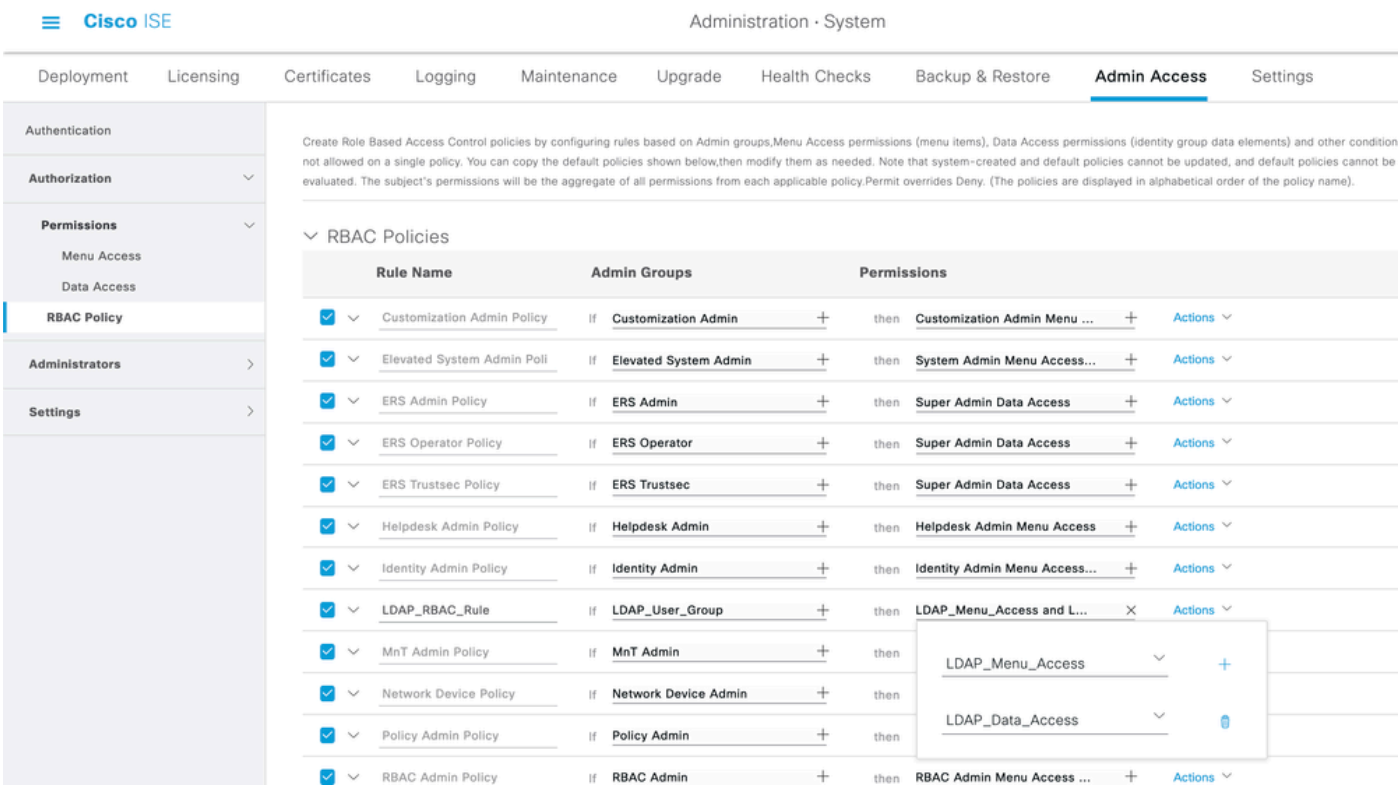
2.定义管理员用户的数据访问权限，使其对ISE GUI上的身份组具有完全访问权限或只读访问权限。

3.单击保存。



设置管理员组的RBAC权限

1. 导航到ISE > Administration > System > Admin Access > Authorization > Policy。
2. 从右侧的Actions下拉菜单中，选择Insert New Policy以添加新策略。
3. 创建一个名为LDAP_RBAC_policy的新规则，以在Enable Administrative Access for AD部分中定义的管理员组对其进行映射，并为其分配菜单访问和数据访问的权限。
4. 单击Save Changes,GUI的右下角将显示已保存的更改的确认。



注意：超级管理员用户无法修改默认系统生成的RBAC策略和权限。为此，您必须根据自己的需要创建具有必要权限的新RBAC策略，并将这些策略映射到管理员组。

注意：只有默认超级管理员组中的管理员用户才能修改或删除其他管理员用户。即使是使用超级管理员组的菜单和数据访问权限克隆的管理员组的外部映射用户，也无法修改或删除管理员用户。

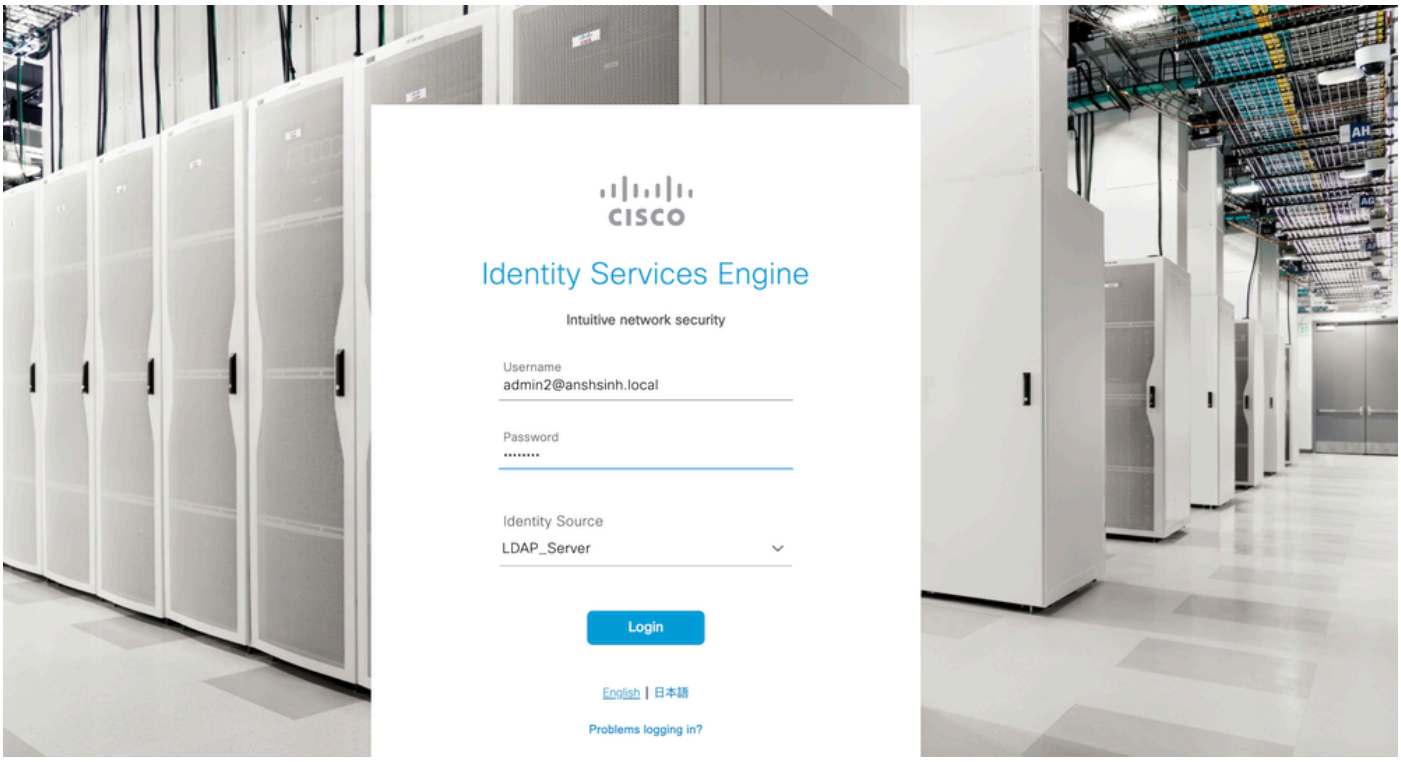
验证

使用本部分可确认配置能否正常运行。

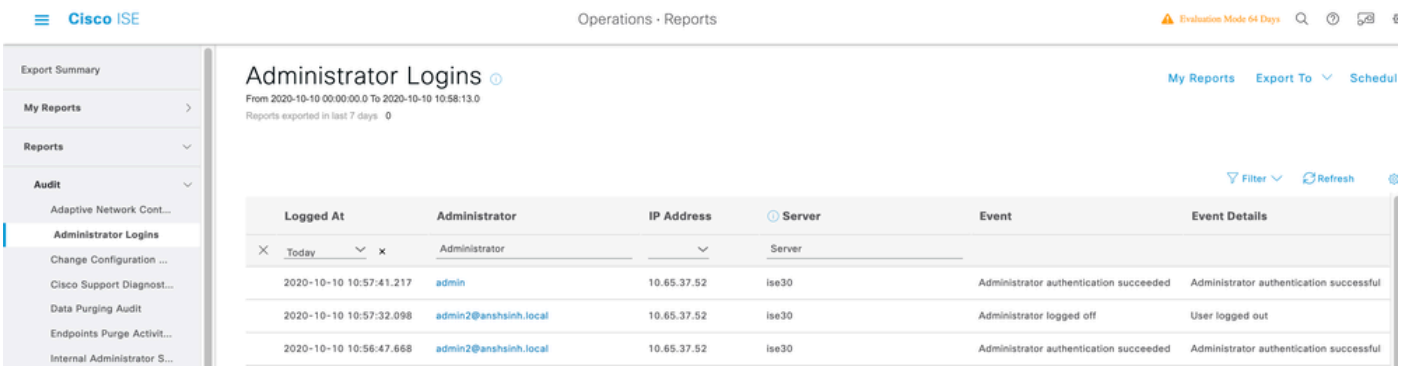
使用AD凭证访问ISE

完成以下步骤以使用AD凭证访问ISE:

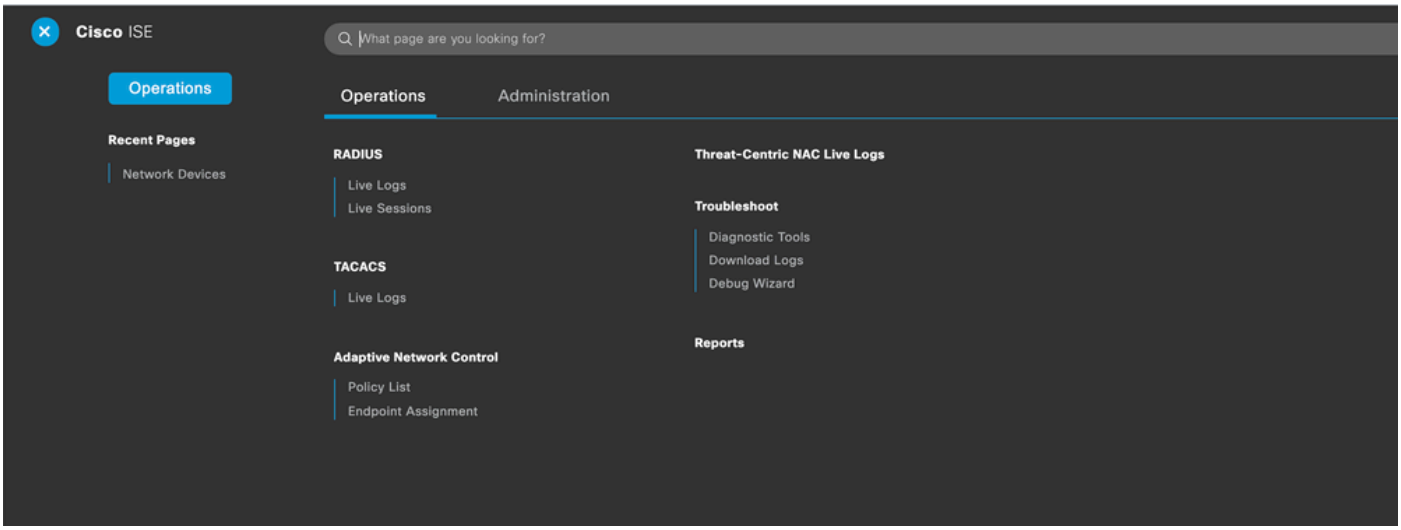
1. 打开ISE GUI以使用LDAP用户登录。
2. 从Identity Source下拉菜单中选择LDAP_Server。
3. 从LDAP数据库输入UPN和密码，然后登录。



在“审计报告”中验证管理员登录的登录。导航到ISE > Operations > Reports > Audit > Administrator Logins。



要确认此配置正常工作，请验证ISE GUI右上角的身份验证用户名。定义对菜单具有有限访问权限的基于自定义的访问，如下所示：



故障排除

本部分提供了可用于对配置进行故障排除的信息。

一般信息

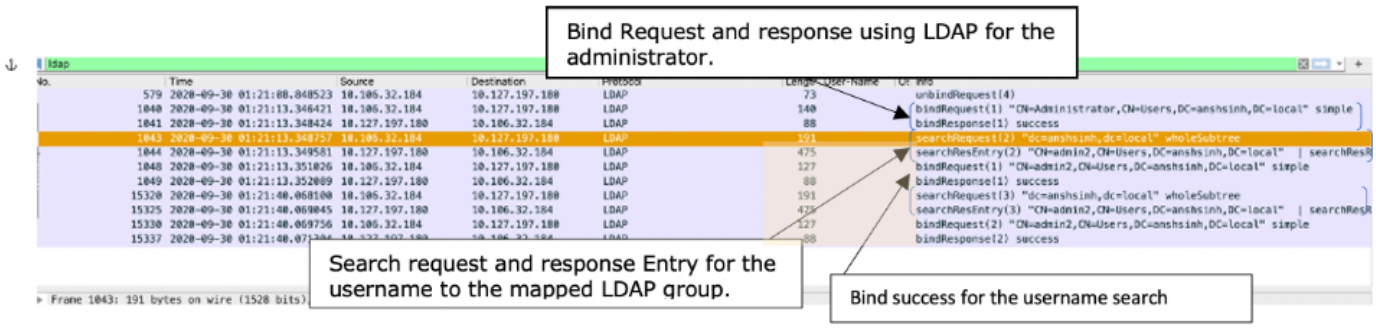
要排除RBAC进程故障，必须在ISE管理节点的调试中启用这些ISE组件：

RBAC — 这会在我们尝试登录时打印RBAC相关的消息(ise-psc.log)

access-filter — 用于打印资源过滤器访问权限(ise-psc.log)

runtime-AAA — 用于打印登录和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

IdentitySequence,2020-10-10 08:54:00,627,DEBUG,0x7f852c4e9700,cntx=0002480105,sesn=ise30/389444264/3178

LDAPIDStore,2020-10-10 08:54:00,628,DEBUG,0x7f852c4e9700,cntx=0002480105,sesn=ise30/389444264/3178,CPMS

Server,2020-10-10 08:54:00,634,DEBUG,0x7f85293b8700,cntx=0002480105,sesn=ise30/389444264/3178,CPMSessio

Connection,2020-10-10 08:54:00,634,DEBUG,0x7f85293b8700,LdapConnectionContext::sendSearchRequest(id = 1
```

```
Server,2020-10-10 08:54:00,635,DEBUG,0x7f85293b8700,cntx=0002480105,sesn=ise30/389444264/3178,CPMSessio

Server,2020-10-10 08:54:00,635,DEBUG,0x7f85293b8700,cntx=0002480105,sesn=ise30/389444264/3178,CPMSessio

Server,2020-10-10 08:54:00,636,DEBUG,0x7f85293b8700,cntx=0002480105,sesn=ise30/389444264/3178,CPMSessio

Server,2020-10-10 08:54:00,636,DEBUG,0x7f85293b8700,cntx=0002480105,sesn=ise30/389444264/3178,CPMSessio

Connection,2020-10-10 08:54:00,636,DEBUG,0x7f85293b8700,LdapConnectionContext::sendBindRequest(id = 122
Server,2020-10-10 08:54:00,640,DEBUG,0x7f85293b8700,cntx=0002480105,sesn=ise30/389444264/3178,CPMSessio


LDAPIDStore,2020-10-10 08:54:00,641,DEBUG,0x7f852c6eb700,cntx=0002480105,sesn=ise30/389444264/3178,CPMS
```

验证ise-psc.log

通过这些日志，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@anshs
2020-10-10 08:54:24,524 INFO   [admin-http-pool51][] cpm.admin.ac.actions.NetworkDevicesLPInputAction -
2020-10-10 08:54:24,524 DEBUG  [admin-http-pool51][] cisco.ise.rbac.authorization.RBACAuthorization -:a
2020-10-10 08:54:24,526 DEBUG  [admin-http-pool51][] ise.rbac.evaluator.impl.DataPermissionEvaluatorImp
2020-10-10 08:54:24,526 DEBUG  [admin-http-pool51][] ise.rbac.evaluator.impl.DataPermissionEvaluatorImp
2020-10-10 08:54:24,528 DEBUG  [admin-http-pool51][] cisco.ise.rbac.authorization.RBACAuthorization -:a
2020-10-10 08:54:24,528 INFO   [admin-http-pool51][] cpm.admin.ac.actions.NetworkDevicesLPInputAction -
2020-10-10 08:54:24,534 INFO   [admin-http-pool51][] cisco.cpm.admin.license.TrustSecLicensingUIFilter
2020-10-10 08:54:24,593 DEBUG  [admin-http-pool51][] cisco.ise.rbac.authorization.RBACAuthorization -:a
2020-10-10 08:54:24,595 DEBUG  [admin-http-pool51][] ise.rbac.evaluator.impl.DataPermissionEvaluatorImp
2020-10-10 08:54:24,597 DEBUG  [admin-http-pool51][] ise.rbac.evaluator.impl.DataPermissionEvaluatorImp
2020-10-10 08:54:24,604 INFO   [admin-http-pool51][] cisco.cpm.admin.license.TrustSecLicensingUIFilter
```

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。