配置ACI LDAP身份验证

目录

简介

本文档介绍如何配置以应用为中心的基础设施(ACI)轻量级目录访问协议(LDAP)身份验证。

先决条件

要求

Cisco 建议您了解以下主题：

- ACI身份验证、授权和记帐(AAA)策略
- LDAP

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 思科应用策略基础设施控制器(APIC)版本5.2(7f)
- Ubuntu 20.04，带slapd和phpLDAPadmin

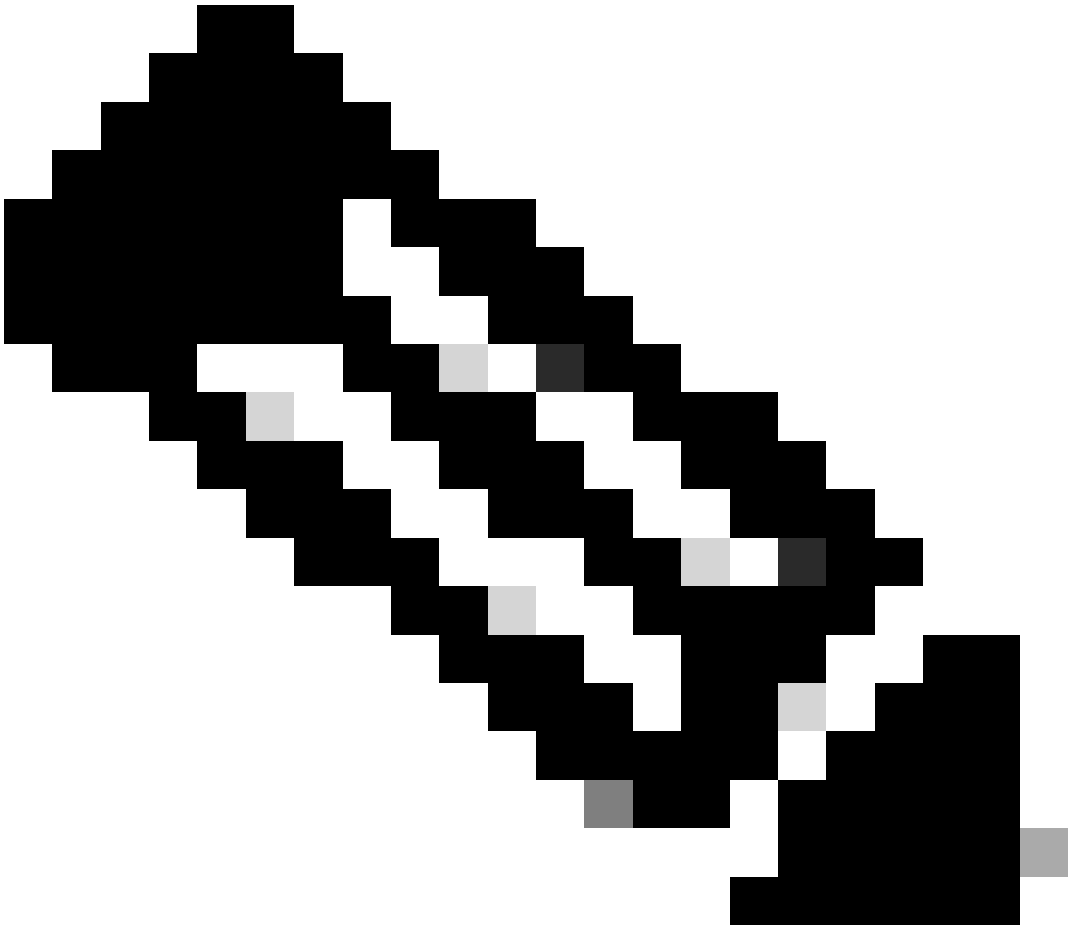
本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

配置

本节介绍如何配置APIC以便与LDAP服务器集成并使用LDAP作为默认身份验证方法。

配置

步骤1:在Ubuntu phpLDAPadmin上创建组/用户

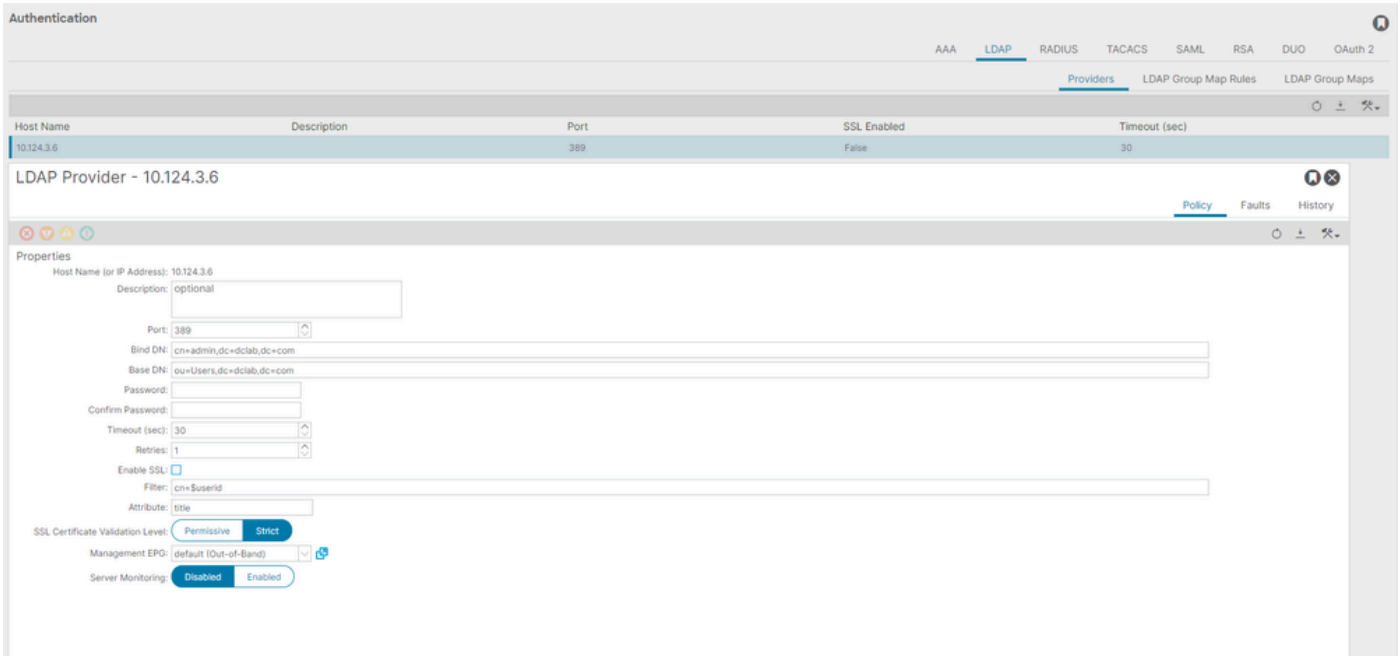


注意：要将Ubuntu配置为LDAP服务器，请参阅官方Ubuntu网站了解综合指南。如果现有LDAP服务器，请从第2步开始。

在本文档中，基本DN为dc=dclab,dc=com，两个用户（User1和User2）属于组(DCGroup)。

第二步：在APIC上配置LDAP提供程序

在APIC菜单栏中，导航至Admin > AAA > Authentication > LDAP > Providers（如图所示）。



Bind DN：绑定DN是您用于针对LDAP进行身份验证的凭证。APIC使用此帐户进行身份验证，以查询目录。

基础DN：APIC使用此字符串作为参考点，搜索和识别目录中的用户条目。

密码：这是访问LDAP服务器所需的绑定DN的必要密码，与LDAP服务器上建立的密码相关联。

启用SSL：如果使用内部CA或自签名证书，则必须选择**Permissive**。

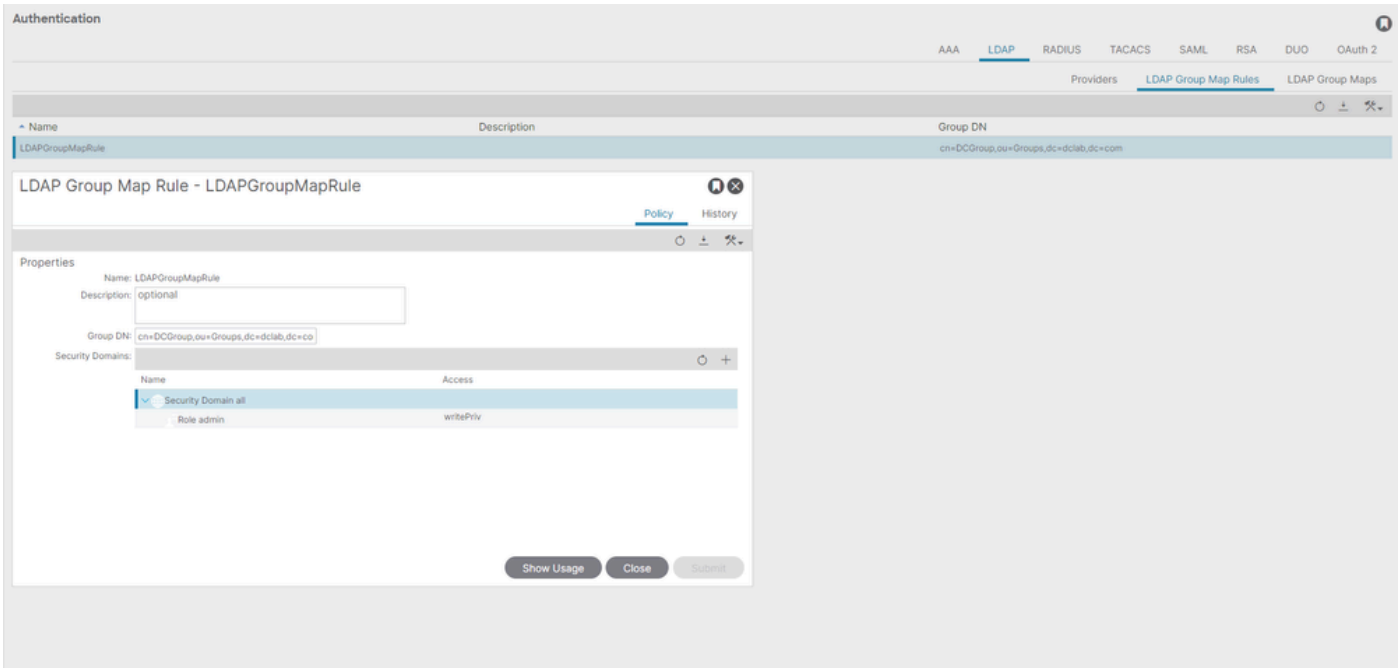
过滤器：默认过滤器设置是cn=$userid，当用户被定义为具有公用名(CN)的对象时，过滤器用于查找基础DN中的对象。

属性：属性用于确定组成员资格和角色。ACI在此处提供两个选项：memberOf和CiscoAVPair.memberOf 是RFC2307bis属性，以便标识组成员身份。目前，OpenLDAP检查RFC2307，因此使用title 该命令。

管理终端组(EPG)：根据所选的网络管理方法，通过带内或带外EPG实现与LDAP服务器的连接。

第三步：配置LDAP组映射规则

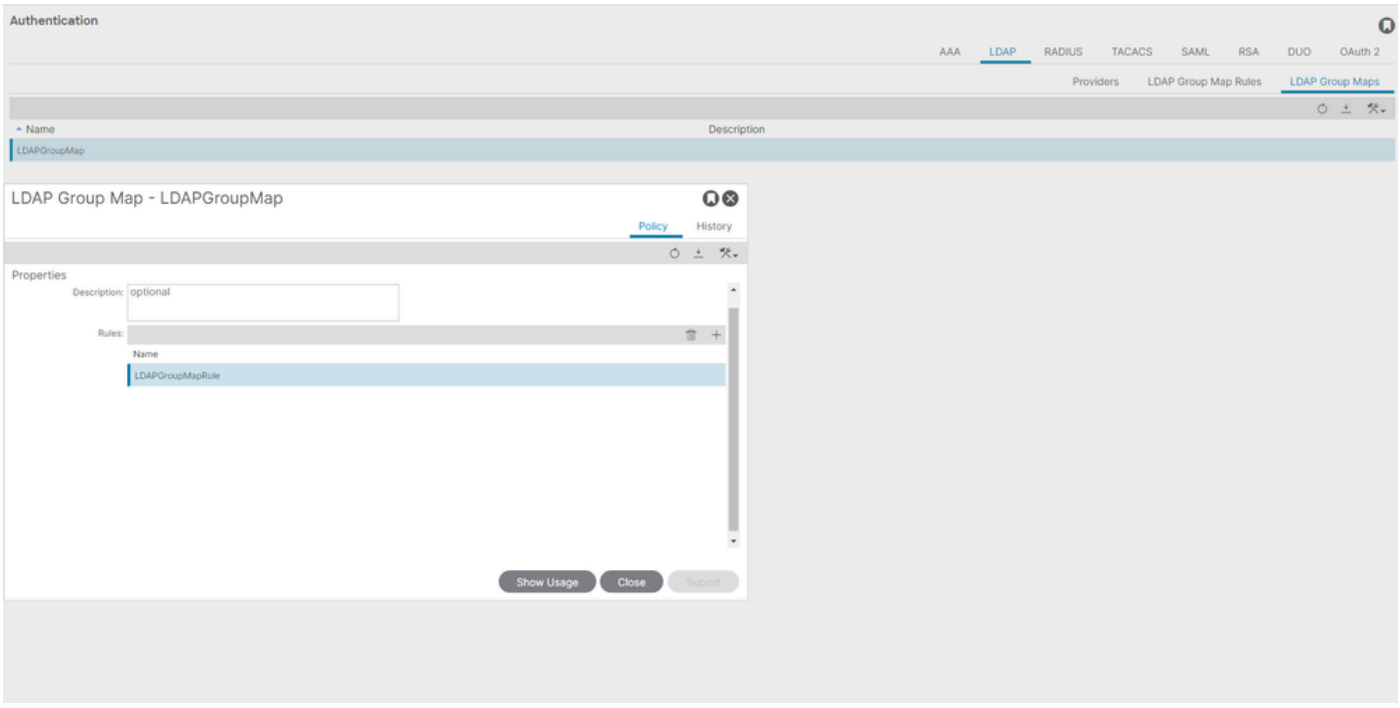
在菜单栏上，导航至Admin > AAA > Authentication > LDAP > LDAP Group Map Rules 如图所示。



DCGroup中的用户具有管理员权限。因此，组DN会cn=DCGroup, ou=Groups, dc=dclab, dc=com. A分配安全域以All，并分配admin的角色与write privilege。

第四步：配置LDAP组映射

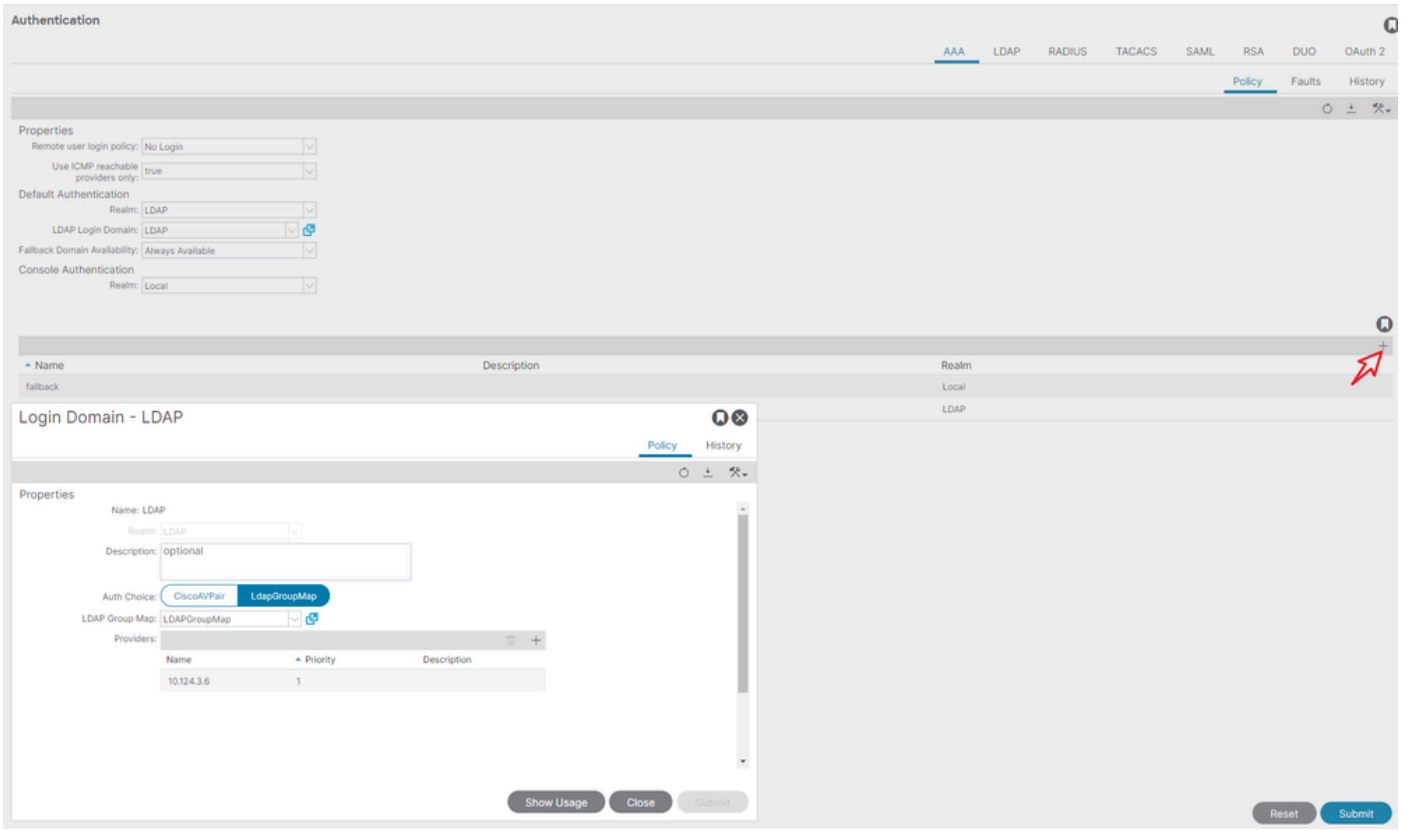
在菜单栏上，导航至Admin > AAA > Authentication > LDAP > LDAP Group Maps 如图所示。



创建包含步骤2中创建的LDAP组映射规则的LDAP组映射。

第五步：配置AAA身份验证策略

在菜单栏上，导航至Admin > AAA > Authentication > AAA > Policy > Create a login domain如图所示。

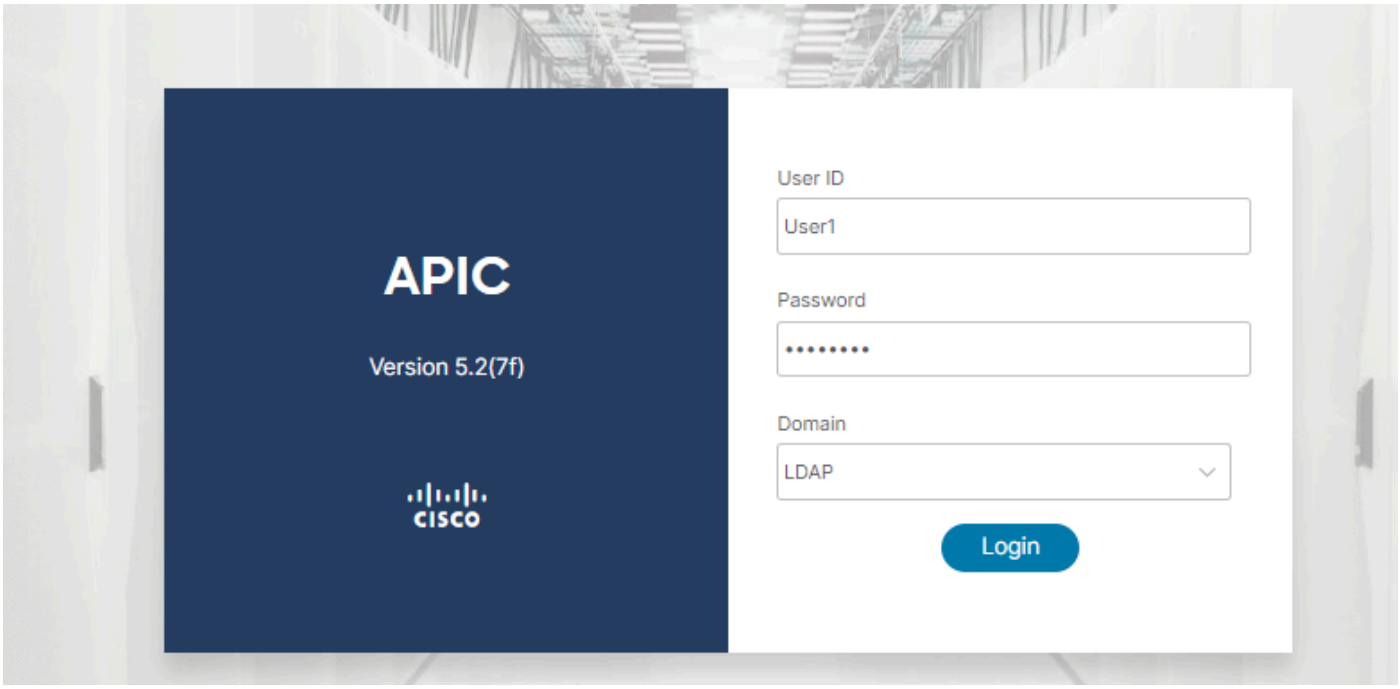


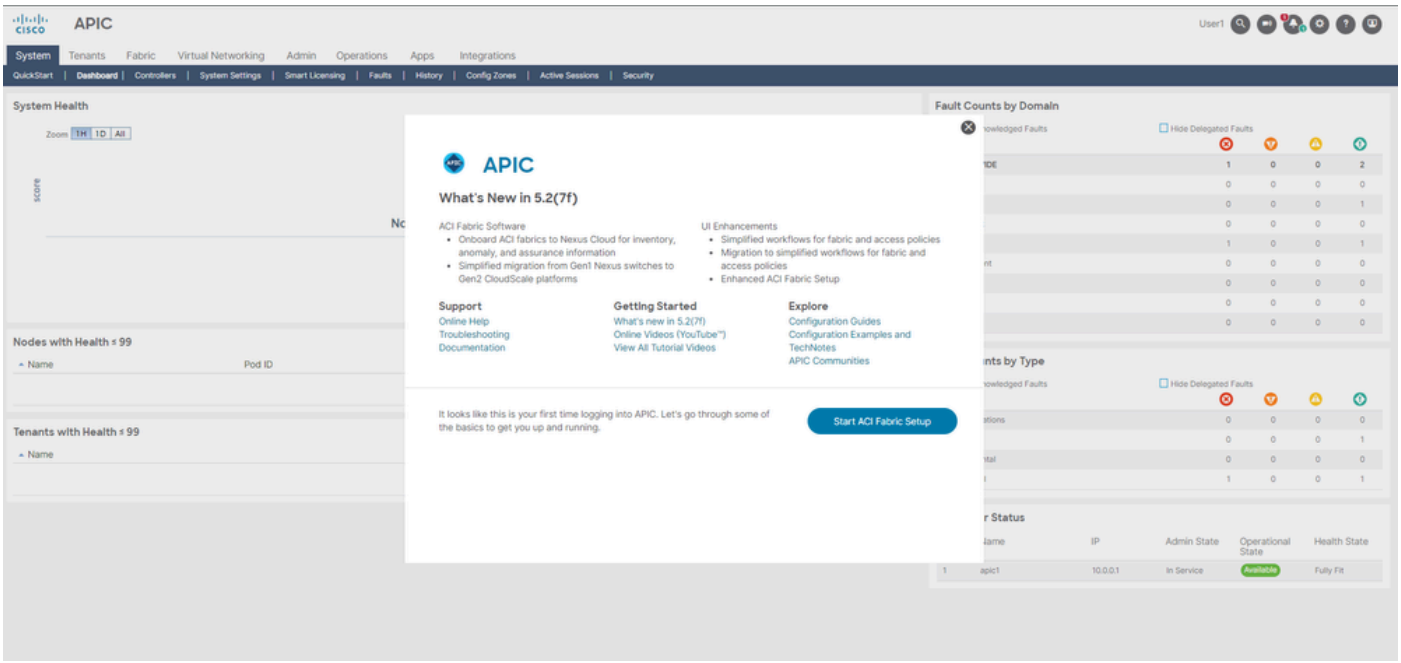
在菜单栏上，导航至Admin > AAA > Authentication > AAA > Policy > Default Authentication 如图所示。

将默认身份验证Realm更改为LDAP并选择LDAP Login Domain created。

验证

使用本部分可确认配置能否正常运行。



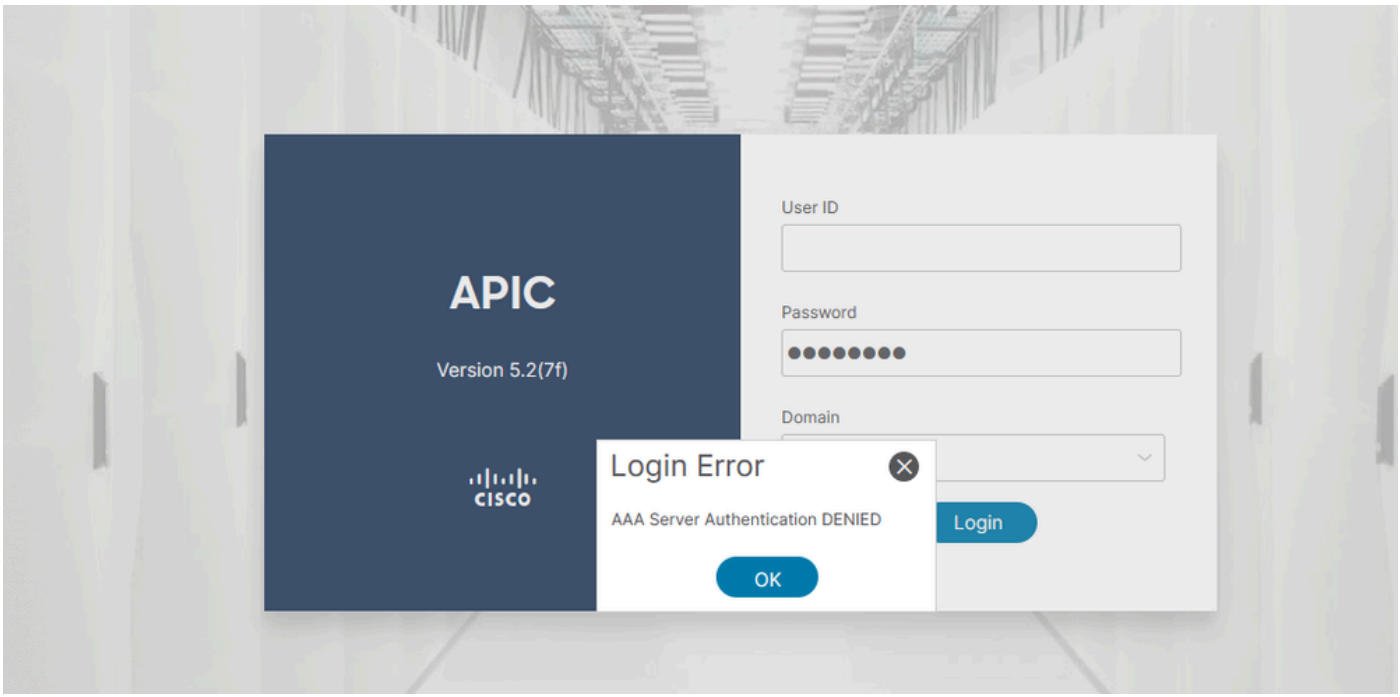


验证LDAP用户User1是否使用管理员角色和写入权限成功登录APIC。

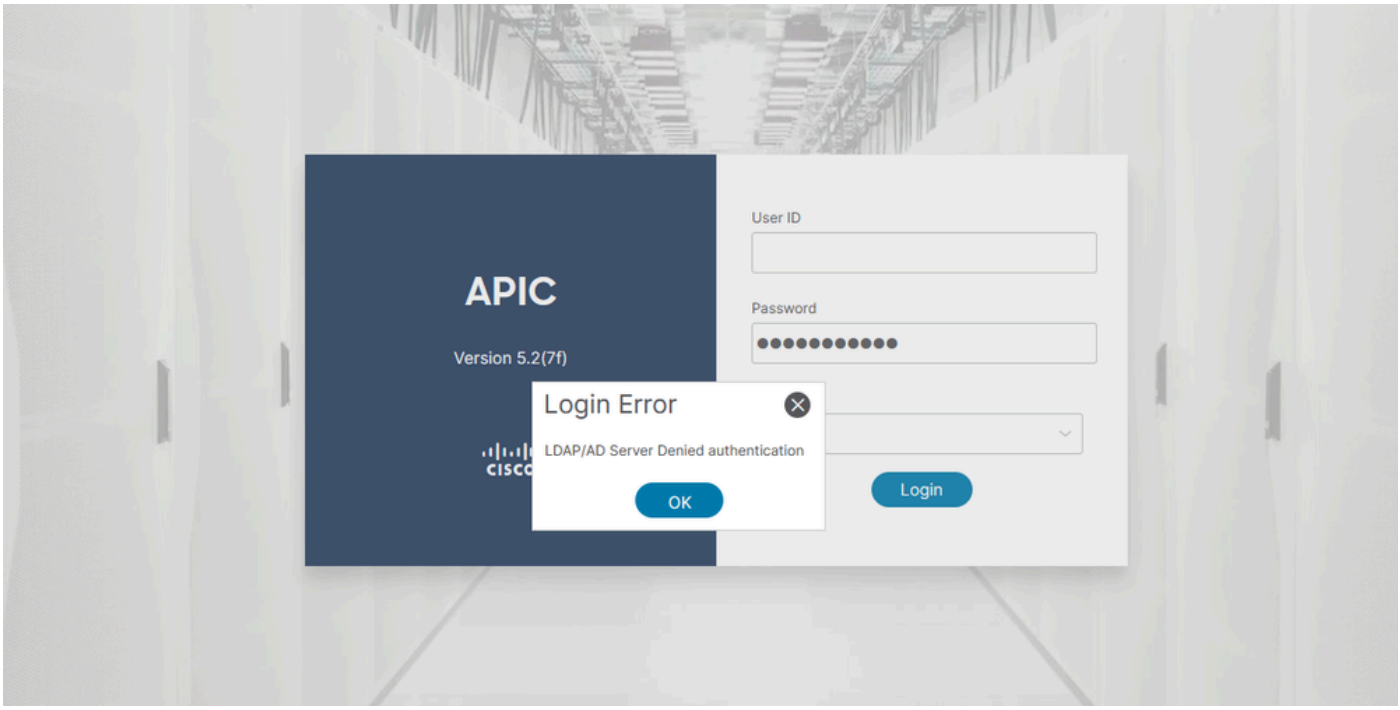
故障排除

本部分提供了可用于对配置进行故障排除的信息。

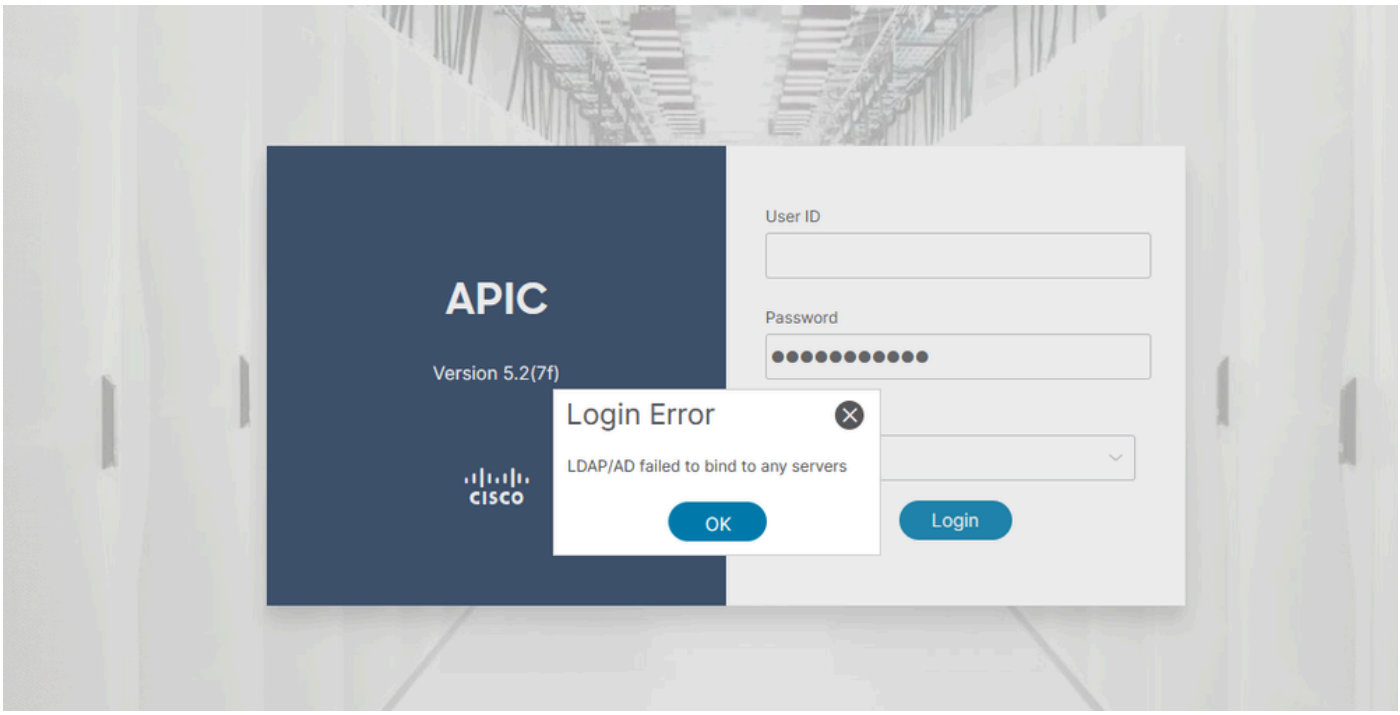
当LDAP数据库中不存在该用户时：



当密码不正确时：



当LDAP服务器无法访问时：



故障排除命令:

<#root>

```
apic1# moquery -c aaaLdapProvider Total Objects shown: 1 # aaa.LdapProvider name : 10.124.3.6 SSLValida
```

如需更多帮助，请联系Cisco TAC。

相关信息

- 思科APIC安全配置指南5.2(x)版
- 思科技术支持和下载

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）。