Configure ACI LDAP Authentication

Contents

Introduction

This document describes how to configure Application Centric Infrastructure (ACI) Lightweight Directory Access Protocol (LDAP) authentication.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- ACI Authentication, Authorization, and Accounting (AAA) policy
- LDAP

Components Used

The information in this document is based on these software and hardware versions:

- Cisco Application Policy Infrastructure Controller (APIC) Version 5.2(7f)
- Ubuntu 20.04 with slapd and phpLDAPadmin

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, ensure that you understand the potential impact of any command.

Configure

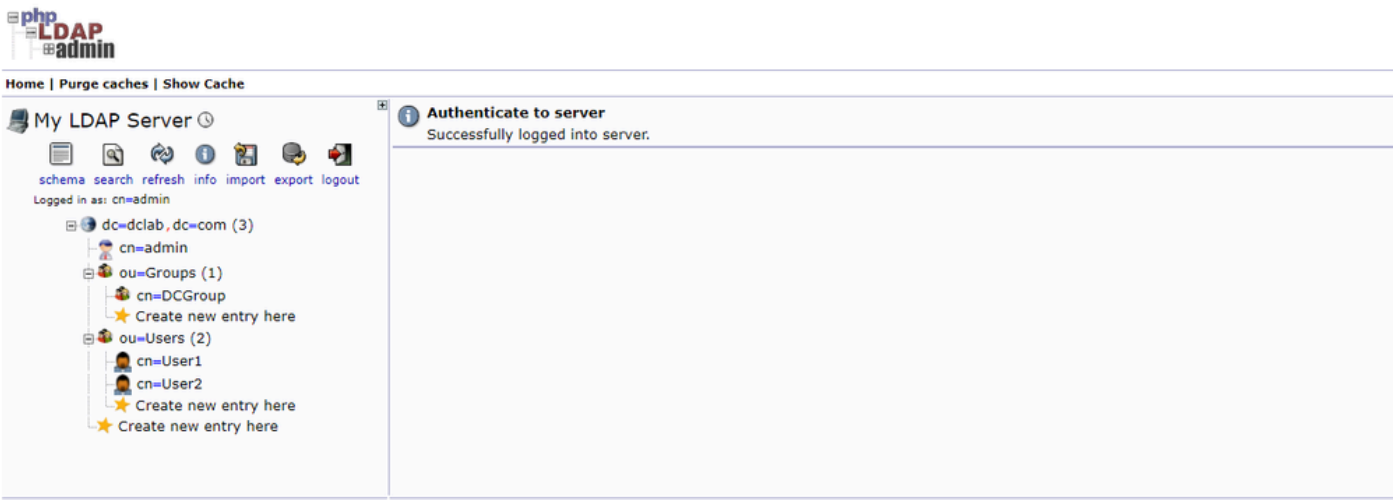
This section describes how to configure APIC in order to integrate with the LDAP server and use LDAP as the default authentication method.

Configurations

Step 1. Create Groups/Users on Ubuntu phpLDAPadmin

Note: In order to configure Ubuntu as an LDAP server, refer to the official Ubuntu website for comprehensive guidelines. If there is an existing LDAP server, start with Step 2.

In this document, base DN is dc=dclab,dc=com and two users (User1 and User2) belong to Groups (DCGroup).



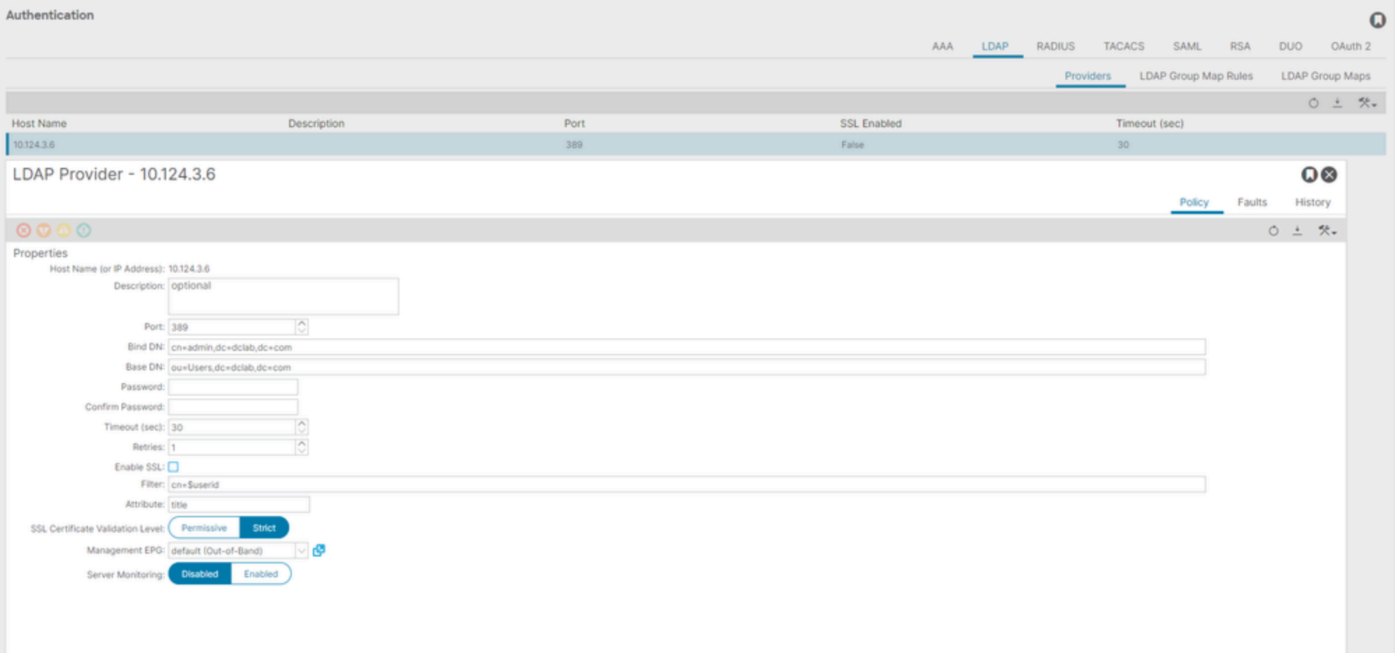
Logged in as: cn=admin

Authenticate to server
Successfully logged into server.

```
dc=dclab,dc=com (3)
  cn=admin
  ou=Groups (1)
    cn=DCGroup
    Create new entry here
  ou=Users (2)
    cn=User1
    cn=User2
    Create new entry here
  Create new entry here
```

Step 2. Configure LDAP Providers on APIC

On the APIC menu bar, navigate to Admin > AAA > Authentication > LDAP > Providers as shown in the image.



Host Name	Description	Port	SSL Enabled	Timeout (sec)
10.124.3.6		389	False	30

LDAP Provider - 10.124.3.6

Properties

Host Name (or IP Address):	10.124.3.6
Description:	optional
Port:	389
Bind DN:	cn=admin,dc=dclab,dc=com
Base DN:	ou=Users,dc=dclab,dc=com
Password:	
Confirm Password:	
Timeout (sec):	30
Retries:	1
Enable SSL:	□
Filter:	cn=$userid
Attribute:	title
SSL Certificate Validation Level:	Permissive [✓ Strict]
Management EPG:	default (Out-of-Band)
Server Monitoring:	[✓ Disabled] Enabled

Bind DN: The bind DN is the credential you are using in order to authenticate against an LDAP. The APIC authenticates using this account to query the directory.

Base DN: This string is employed by the APIC as a reference point for searching and identifying user entries within the directory.

Password: This is the requisite password for the Bind DN necessary to access the LDAP server, correlating with the password established on your LDAP server.

Enable SSL: If you use an internal CA or self-signed certificate, you must choose **Permissive**.

Filter: The default filter setting is cn=$userid when the user is defined as an object with a common name(CN), the filter is used to look for the objects within the Base DN.

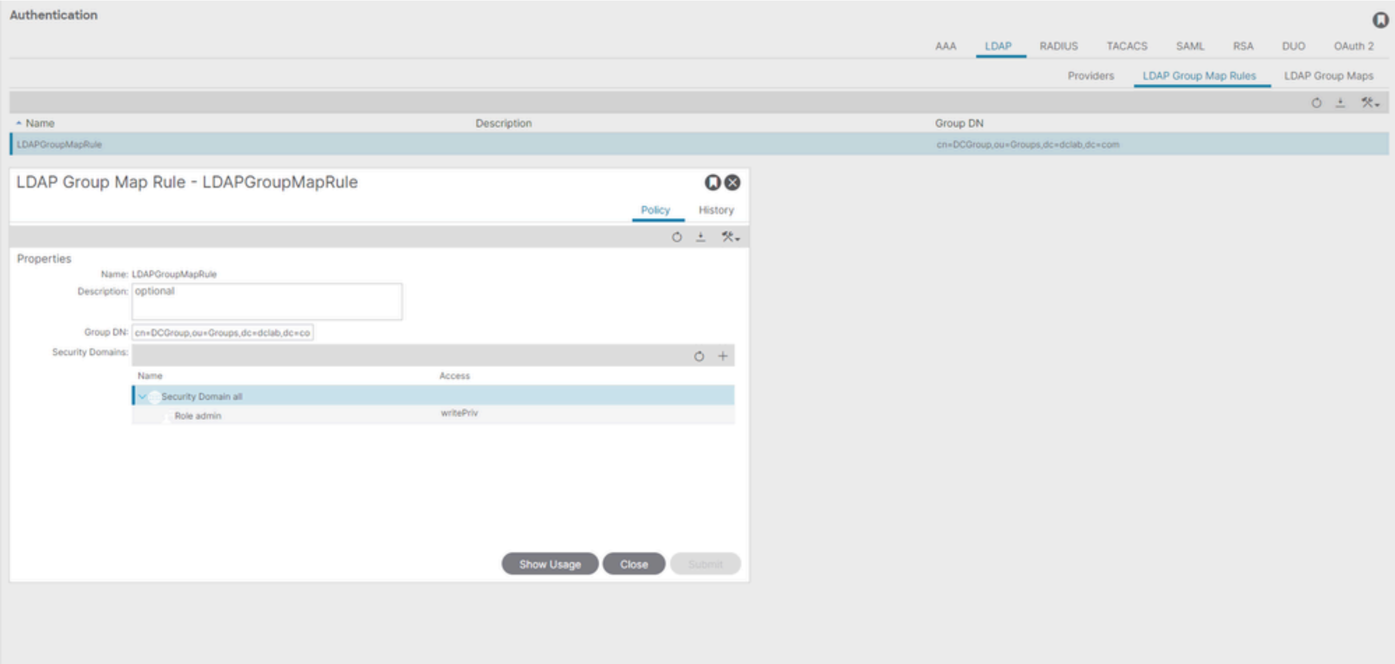
Attribute: Attribute is used to determine group membership and roles. ACI provides two options here: memberOf and CiscoAVPair.memberOf is an RFC2307bis attribute in order to identify group membership.

Currently, OpenLDAP checks RFC2307, so title is used instead.

Management endpoint group (EPG): Connectivity to the LDAP server is achieved through either the In-band or Out-of-band EPG, depending on the chosen network management approach.

Step 3. Configure LDAP Group Map Rules

On the menu bar, navigate to Admin > AAA > Authentication > LDAP > LDAP Group Map Rules as shown in the image.



Name	Description	Group DN
LDAPGroupMapRule		cn=DCGroup,ou=Groups,dc=dclab,dc=com

LDAP Group Map Rule - LDAPGroupMapRule

Properties

Name: LDAPGroupMapRule

Description: optional

Group DN: cn=DCGroup,ou=Groups,dc=dclab,dc=co

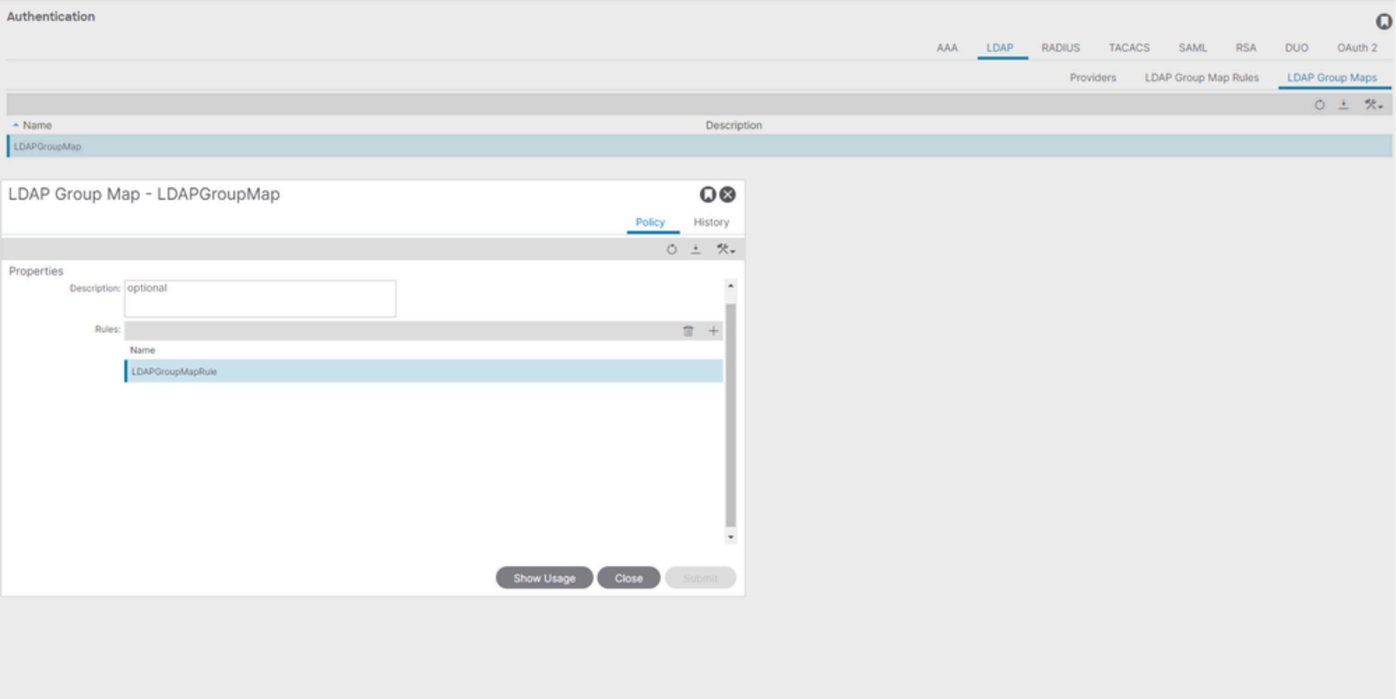
Security Domains:

Name	Access
Security Domain all	
Role admin	writePriv

Users in DCGroup have admin privileges. Therefore, the Group DN is cn=DCGroup, ou=Groups, dc=dclab, dc=com. Assign the security domain to All and allocate the roles of admin with write privilege .

Step 4. Configure LDAP Group Maps

On the menu bar, navigate to Admin > AAA > Authentication > LDAP > LDAP Group Maps as shown in the image.



Name	Description
LDAPGroupMap	

LDAP Group Map - LDAPGroupMap

Properties

Description: optional

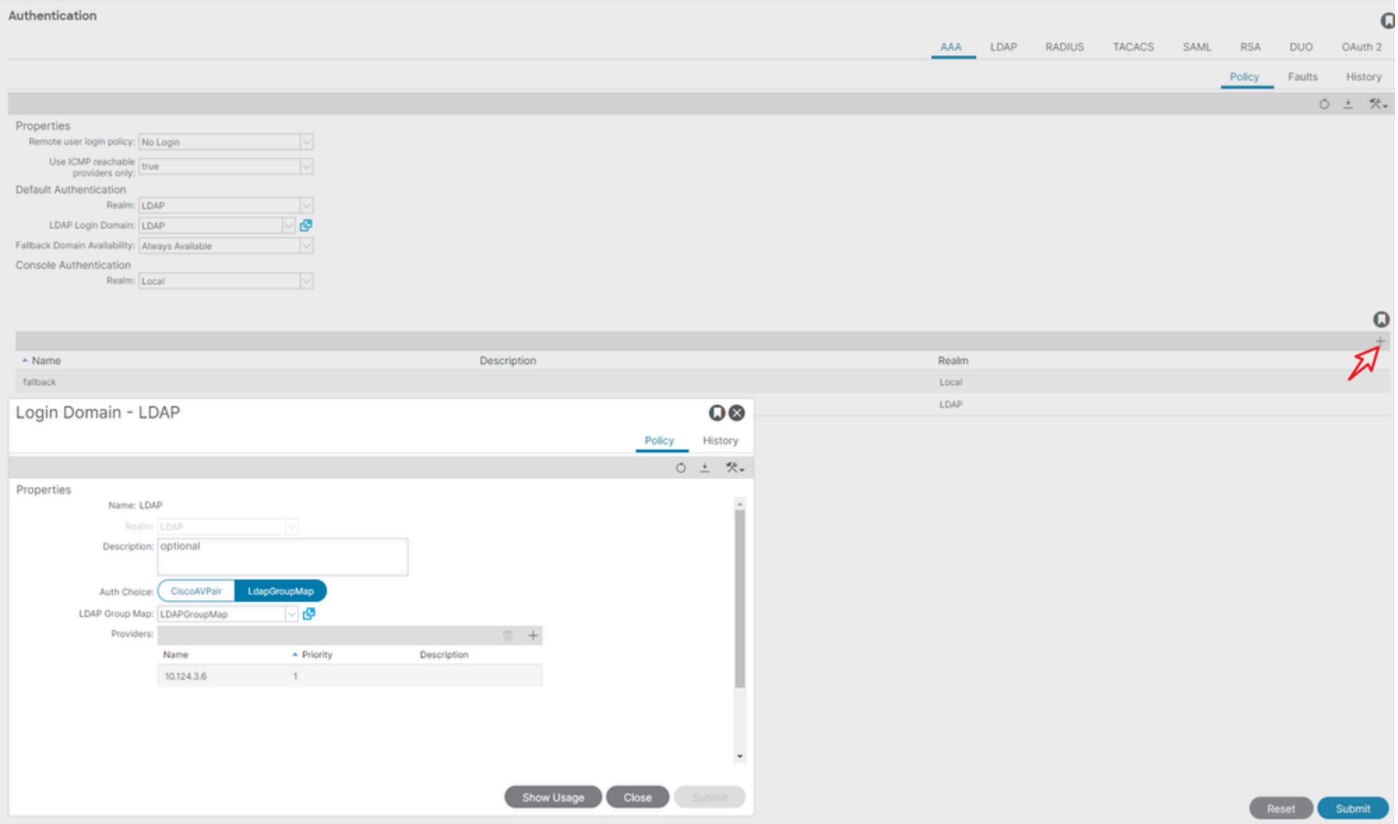
Rules:

Name
LDAPGroupMapRule

Create an LDAP Group Map that contains LDAP Group Map Rules created in Step 2.

Step 5. Configure AAA Authentication Policy

On the menu bar, navigate to Admin > AAA > Authentication > AAA > Policy > Create a login domainas shown in the image.



Properties

Remote user login policy: No Login

Use ICMP reachable providers only: true

Default Authentication

Realm: LDAP

LDAP Login Domain: LDAP

Fallback Domain Availability: Always Available

Console Authentication

Realm: Local

Name	Description	Realm
fallback		Local
		LDAP

Login Domain - LDAP

Properties

Name: LDAP

Realm: LDAP

Description: optional

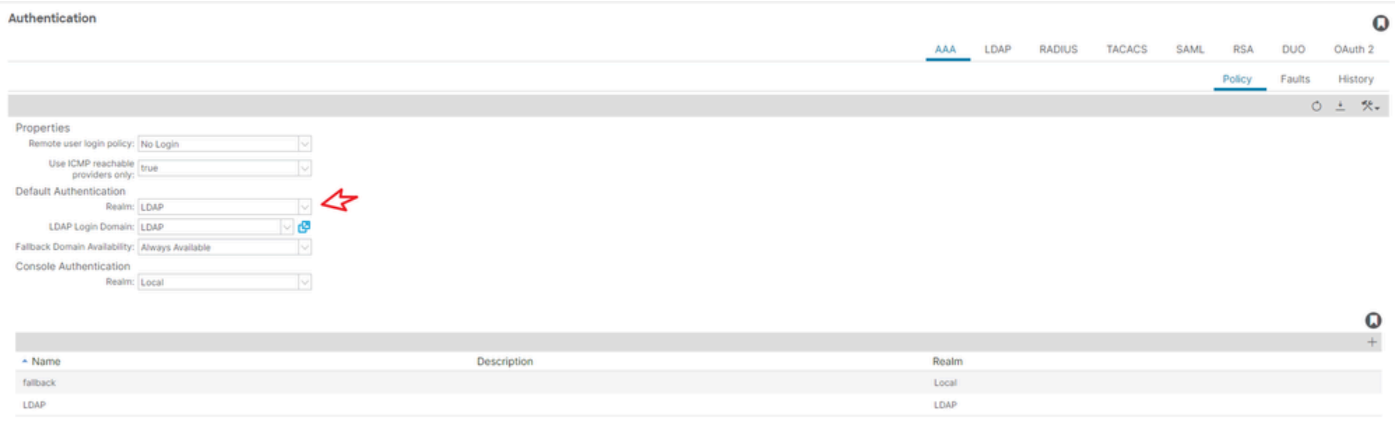
Auth Choice: CiscoAVPair LdapGroupMap

LDAP Group Map: LDAPGroupMap

Providers:

Name	Priority	Description
10.124.3.6	1	

On the menu bar, navigate to Admin > AAA > Authentication > AAA > Policy > Default Authentication as shown in the image.



Authentication

Properties

Remote user login policy: No Login

Use ICMP reachable providers only: true

Default Authentication

Realm: LDAP

LDAP Login Domain: LDAP

Fallback Domain Availability: Always Available

Console Authentication

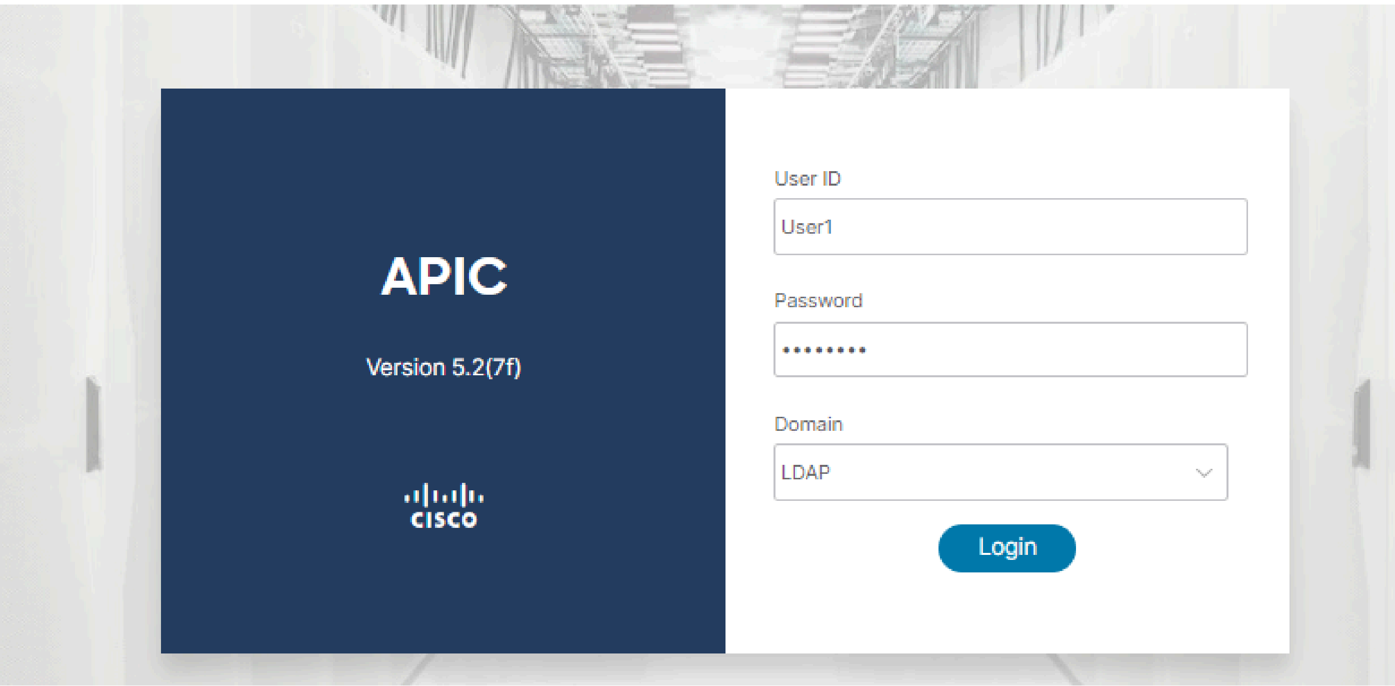
Realm: Local

Name	Description	Realm
fallback		Local
LDAP		LDAP

Change default authentication Realm to LDAP and select LDAP Login Domain created.

Verify

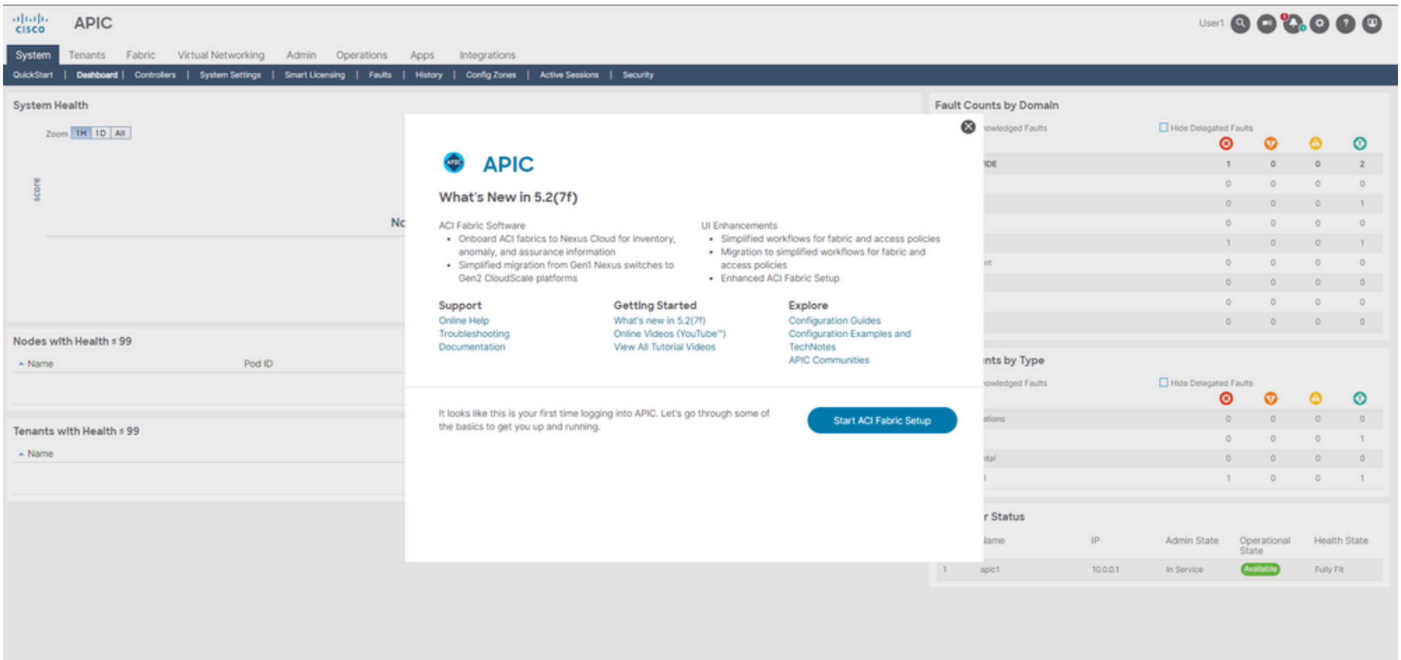
Use this section in order to confirm that your configuration works properly.



User ID: User1

Password: ••••••••

Domain: LDAP



APIC

What's New in 5.2(7f)

ACI Fabric Software
- Onboard ACI fabrics to Nexus Cloud for inventory, anomaly, and assurance information
- Simplified migration from Gen1 Nexus switches to Gen2 CloudScale platforms

UI Enhancements
- Simplified workflows for fabric and access policies
- Migration to simplified workflows for fabric and access policies
- Enhanced ACI Fabric Setup

Support
Online Help
Troubleshooting
Documentation

Getting Started
What's new in 5.2(7f)
Online Videos (YouTube™)
View All Tutorial Videos

Explore
Configuration Guides
Configuration Examples and TechNotes
APIC Communities

It looks like this is your first time logging into APIC. Let's go through some of the basics to get you up and running.

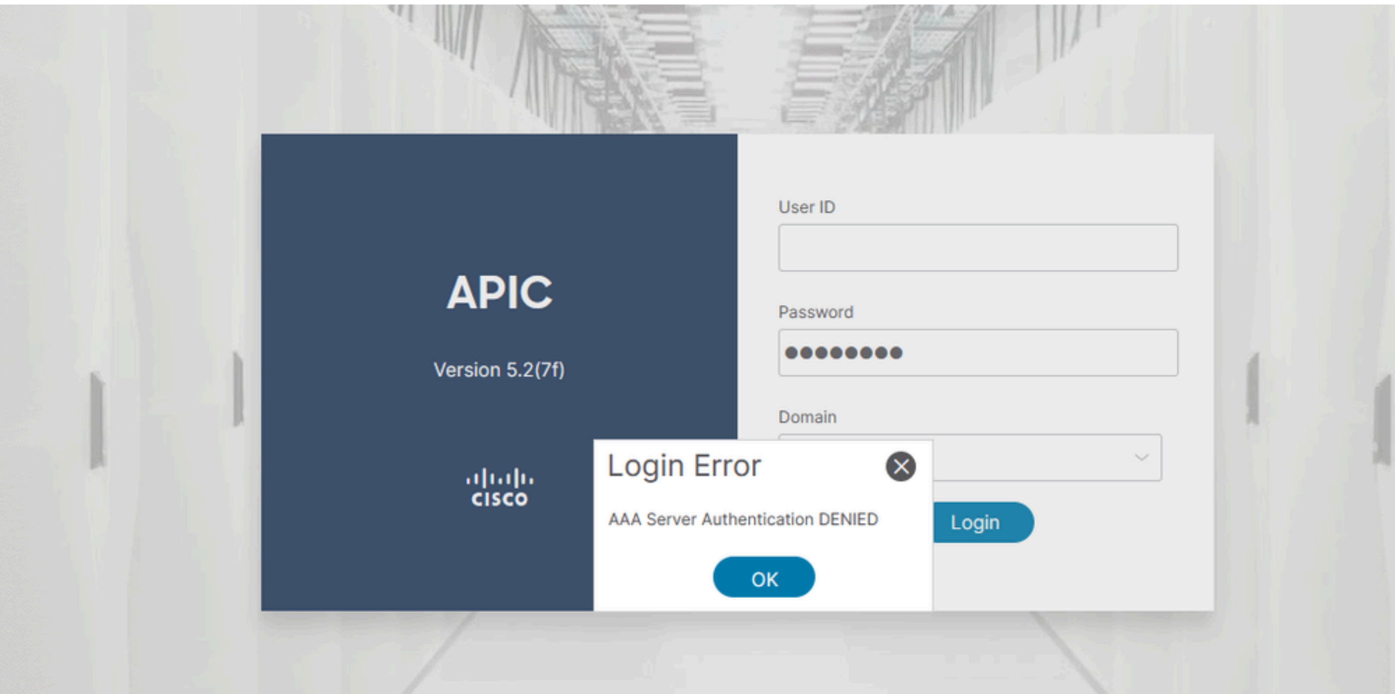
Start ACI Fabric Setup

Verify that the LDAP user User1 logs in APIC successfully with admin role and write privilege.

Troubleshoot

This section provides information you can use in order to troubleshoot your configuration.

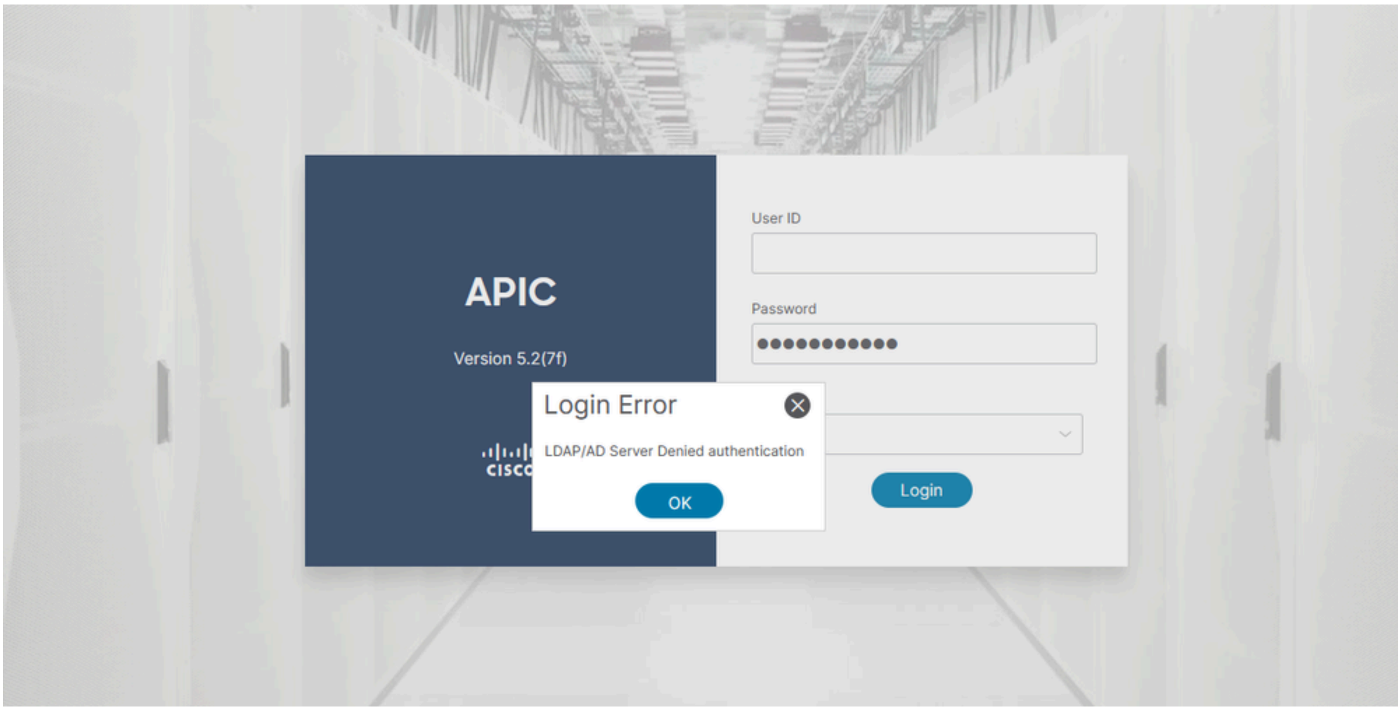
When the user does not exist in the LDAP database:



Login Error

AAA Server Authentication DENIED

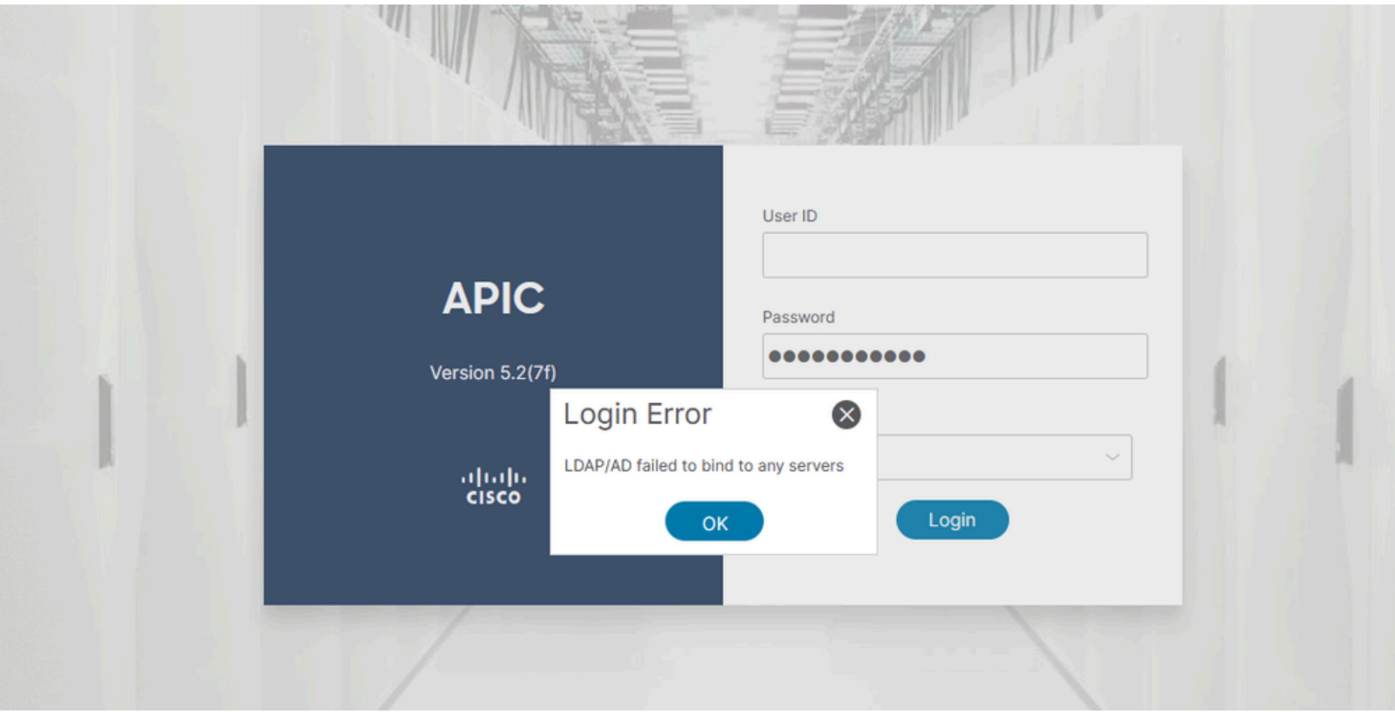
When the password is incorrect:



Login Error

LDAP/AD Server Denied authentication

When the LDAP server is unreachable:



Login Error

LDAP/AD failed to bind to any servers

Troubleshooting commands:

```
apic1# moquery -c aaaLdapProvider
Total Objects shown: 1

# aaa.LdapProvider
name                 : 10.124.3.6
SSLValidationLevel : strict
annotation           :
attribute            : title
basedn               : ou=Users,dc=dclab,dc=com
```

```
childAction        :
descr              :
dn                 : uni/userext/ldapext/ldapprovider-10.124.3.6
enableSSL          : no
epgDn              : uni/tn-mgmt/mgmtp-default/oob-default
extMngdBy          :
filter             : cn=$userid
key                :
lcOwn              : local
modTs              : 2024-03-26T07:01:51.868+00:00
monPolDn           : uni/fabric/monfab-default
monitorServer      : disabled
monitoringPassword :
monitoringUser     : default
nameAlias          :
operState          : unknown
ownerKey           :
ownerTag           :
port               : 389
retries            : 1
rn                 : ldapprovider-10.124.3.6
rootdn             : cn=admin,dc=dclab,dc=com
snmpIndex          : 1
status             :
timeout            : 30
uid                : 15374
userdom            : :all:
vrfName            :

apic1# show aaa authentication
Default : ldap
Console : local

apic1# show aaa groups
Total number of Groups: 1

RadiusGroups :
RsaGroups :
TacacsGroups :
LdapGroups   : LDAP

apic1# show aaa sessions
 Username    User Type   Host              Login Time
 ----------  ----------  ---------------   ------------------------------
 User1       remote      10.140.233.70     2024-04-08T07:51:09.004+00:00
 User1       remote      10.140.233.70     2024-04-08T07:51:11.357+00:00
```

If you need more help, get in touch with Cisco TAC.

Related Information

- Cisco APIC Security Configuration Guide, Release 5.2(x)
- Cisco Technical Support & Downloads