ACI LDAP 인증 구성

목차

소개

이 문서에서는 ACI(Application Centric Infrastructure) LDAP(Lightweight Directory Access Protocol) 인증을 구성하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

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

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco APIC(Application Policy Infrastructure Controller) 버전 5.2(7f)
- Ubuntu 20.04(slapd 및 phpLDAPadmin 사용)

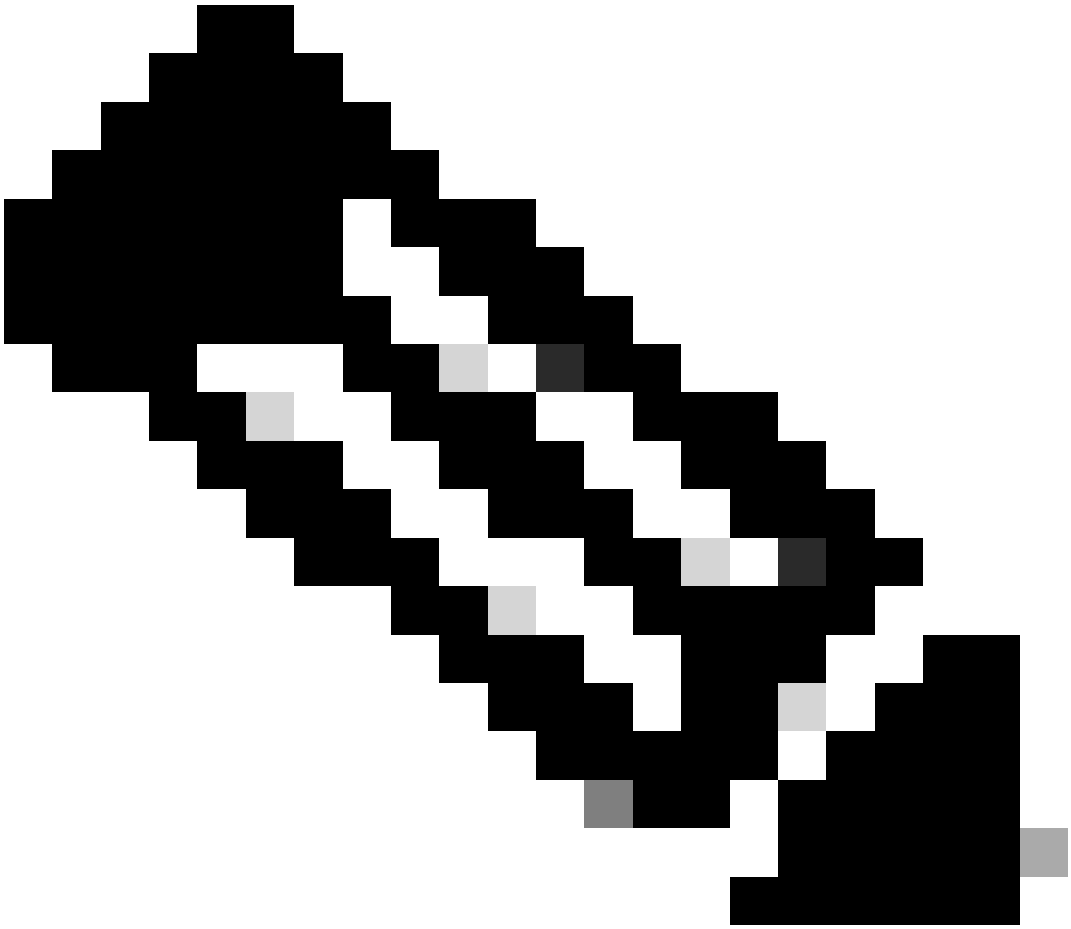
이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

구성

이 섹션에서는 LDAP 서버와 통합하고 기본 인증 방법으로 LDAP를 사용하기 위해 APIC를 구성하는 방법에 대해 설명합니다.

설정

1단계. Ubuntu phpLDAPadmin에서 그룹/사용자 생성

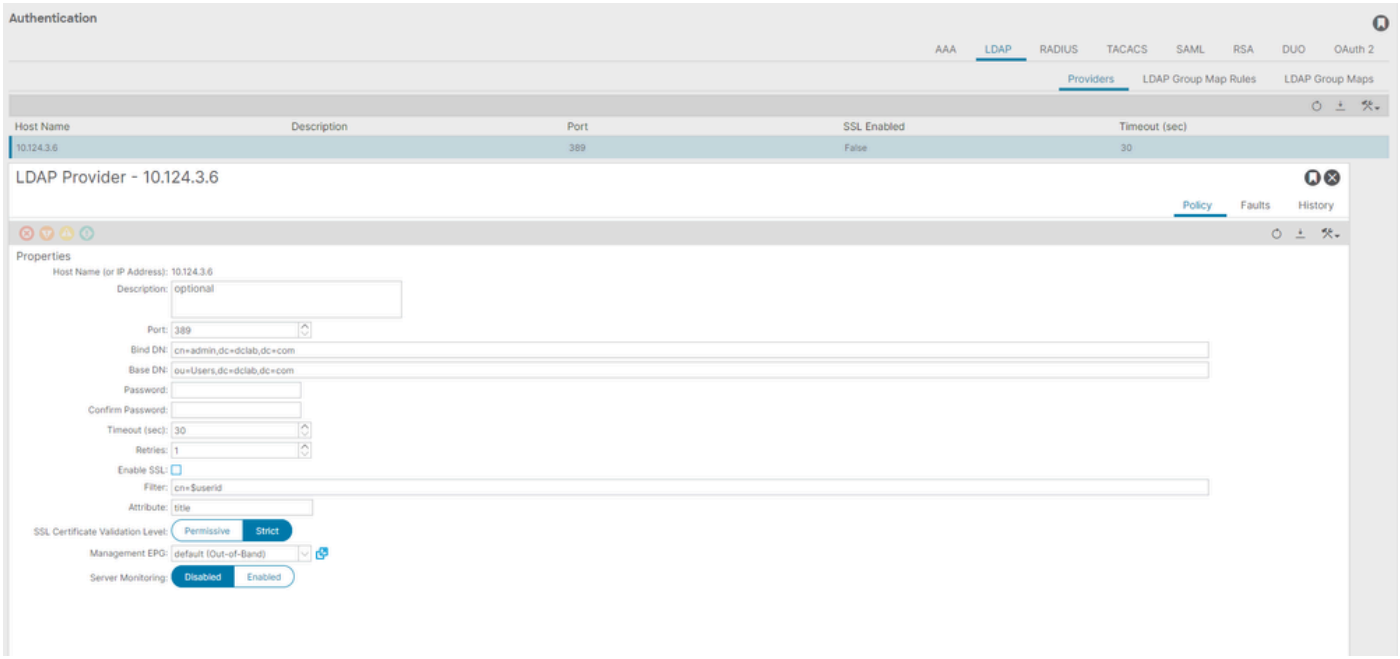


> 참고: Ubuntu를 LDAP 서버로 구성하려면 공식 Ubuntu 웹 사이트에서 종합적인 지침을 참조하십시오. 기존 LDAP 서버가 있는 경우 2단계로 시작합니다.

이 문서에서 기본 DN은dc=dclab,dc=com 이며 두 사용자(User1 및 User2)가 그룹(DCGroup)에 속합니다.

2단계. APIC에서 LDAP 제공자 구성

APIC 메뉴 모음에서 그림과 같이 로Admin > AAA > Authentication > LDAP > Providers 이동합니다.



바인드 DN: 바인드 DN은 LDAP에 대해 인증하기 위해 사용 중인 자격 증명입니다. APIC는 이 계정을 사용하여 디렉터리를 쿼리합니다.

Base DN: 이 문자열은 APIC에서 디렉토리 내의 사용자 항목을 검색하고 식별하기 위한 참조 지점으로 사용됩니다.

비밀번호: LDAP 서버에 액세스하는 데 필요한 바인드 DN의 필수 비밀번호이며, LDAP 서버에 설정된 비밀번호와 상관관계가 있습니다.

SSL 활성화: 내부 CA 또는 자체 서명 인증서를 사용하는 경우 허용을 선택해야 **합니다**.

필터: 기본 필터 설정은 사용자를 CN(Common Name)의 개체로 정의할 때 필터를 사용하여 기본 DN 내에서 개체를 찾는 것입니다 cn=$userid.

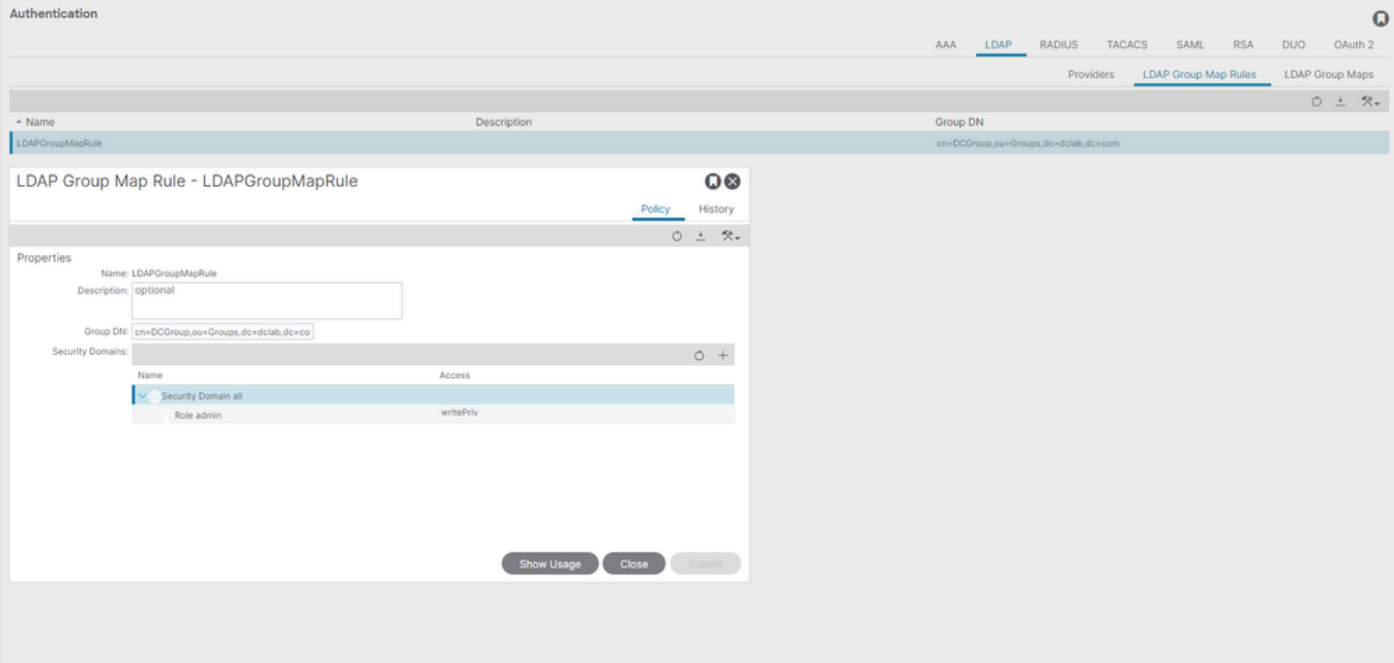
속성: 속성은 그룹 멤버십 및 역할을 결정하는 데 사용됩니다. ACI는 여기에 두 가지 옵션을 제공합니다. memberOf CiscoAVPair.memberOf

은 그룹 멤버십을 식별하기 위한 RFC2307bis 특성입니다. 현재 OpenLDAP는 RFC2307을 확인하므로 title 대신 사용됩니다.

EPG(Management Endpoint Group): 선택한 네트워크 관리 방식에 따라 대역 내(In-band) 또는 대역 외(Out-of-band) EPG를 통해 LDAP 서버에 연결합니다.

3단계. LDAP 그룹 맵 규칙 구성

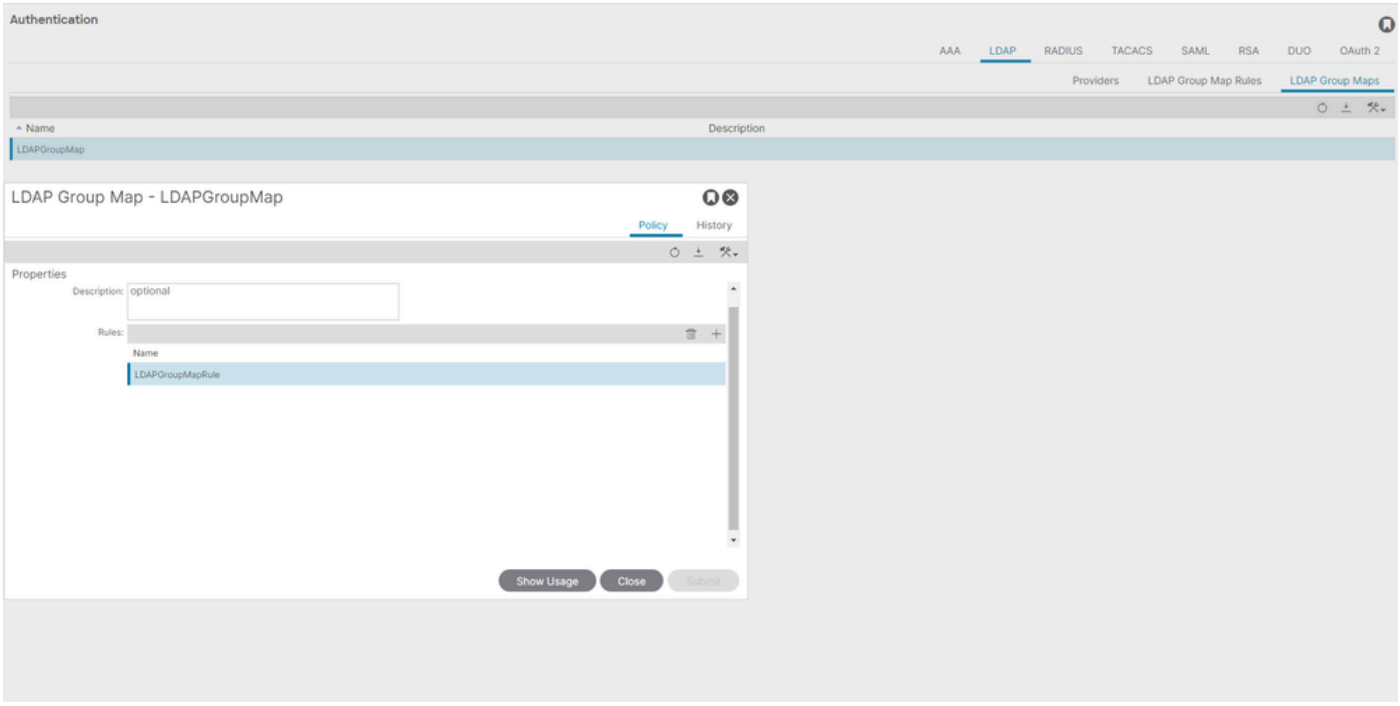
메뉴 모음에서 이미지에 표시된 Admin > AAA > Authentication > LDAP > LDAP Group Map Rules 대로 이동합니다.



DCGroup의 사용자는 관리자 권한을 갖습니다. 따라서 그룹 DN은 cn=DCGroup, ou=Groups, dc=dclab, dc=com. A에 대한 역할을 All할당하도록 보안 도메인을admin write privilege지정합니다.

4단계. LDAP 그룹 맵 구성

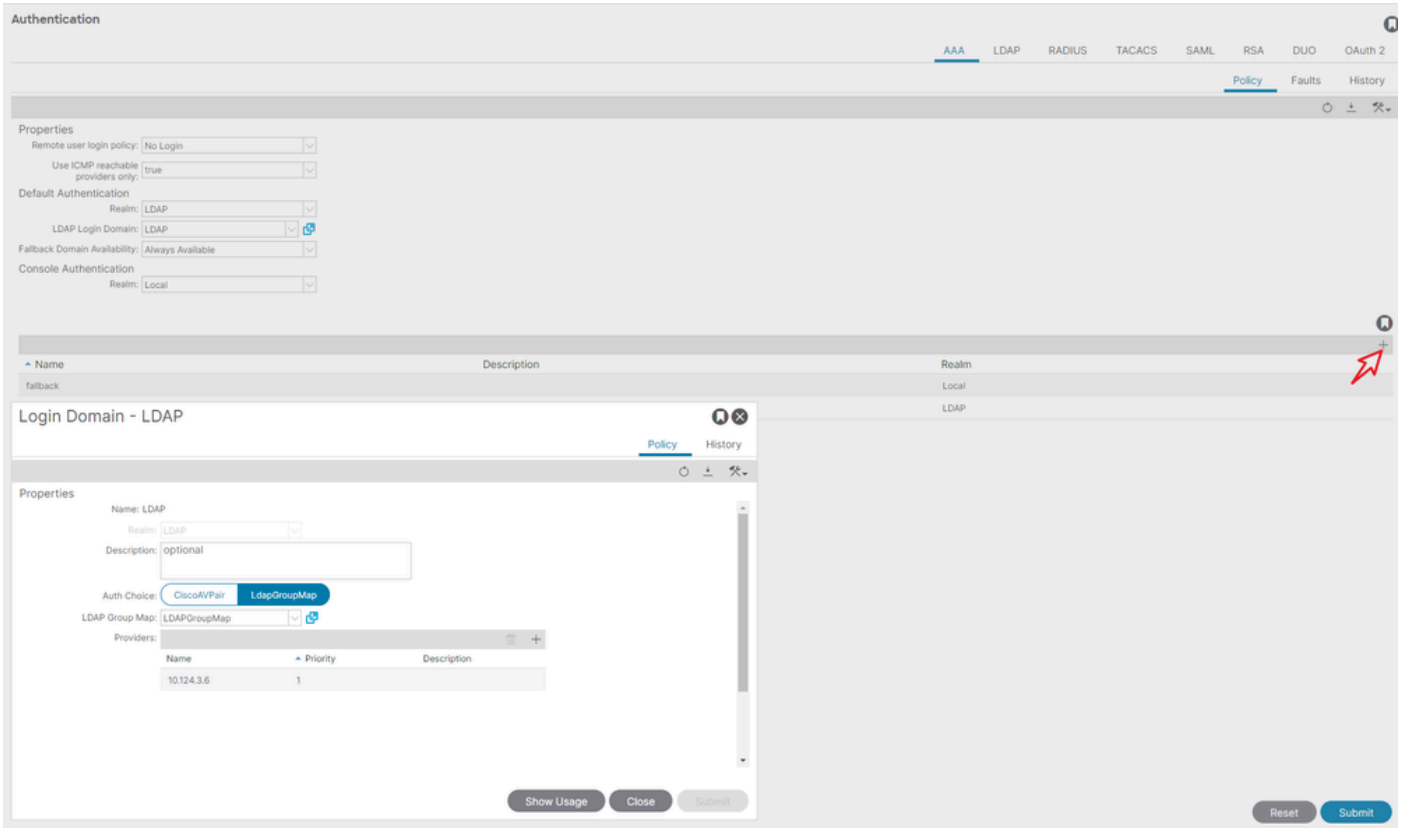
메뉴 모음에서 이미지에 표시된 Admin > AAA > Authentication > LDAP > LDAP Group Maps 대로 이동합니다.



2단계에서 생성한 LDAP 그룹 맵 규칙을 포함하는 LDAP 그룹 맵을 생성합니다.

5단계. AAA 인증 정책 구성

메뉴 모음에서 이미지에 표시된 Admin > AAA > Authentication > AAA > Policy > Create a login domain대로 이동합니다.

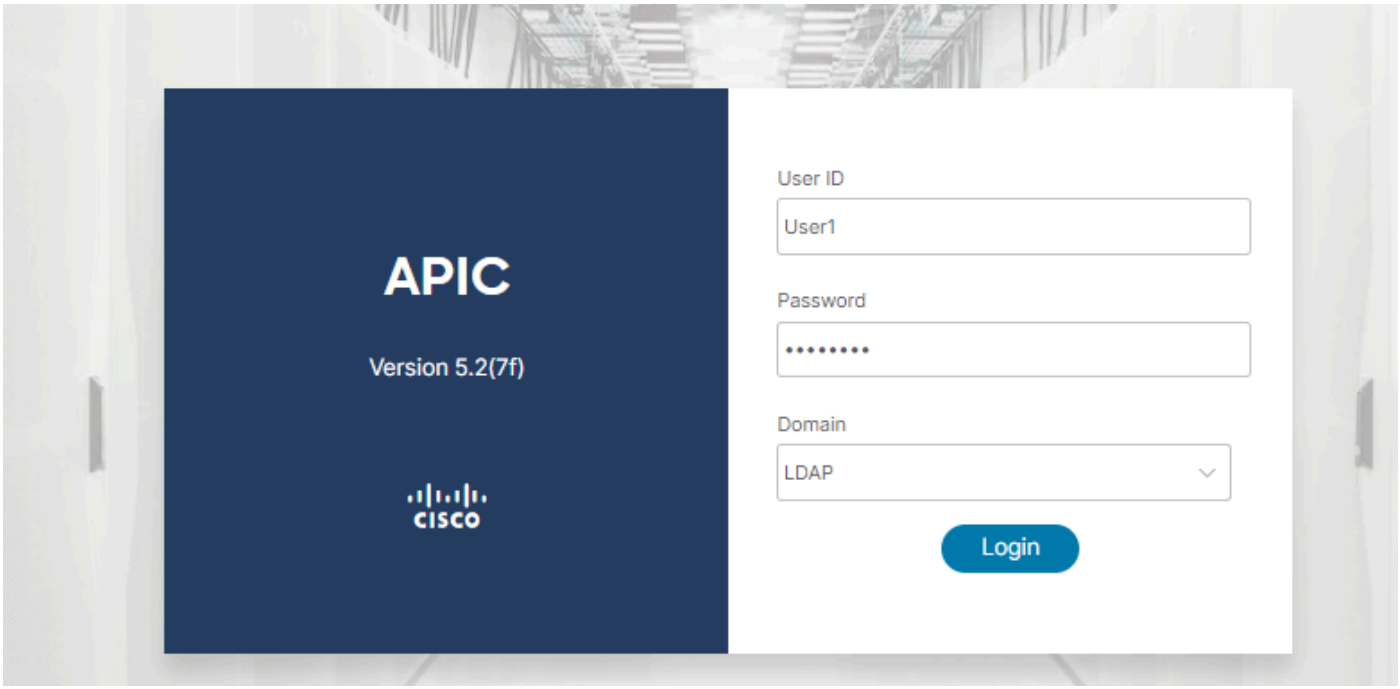


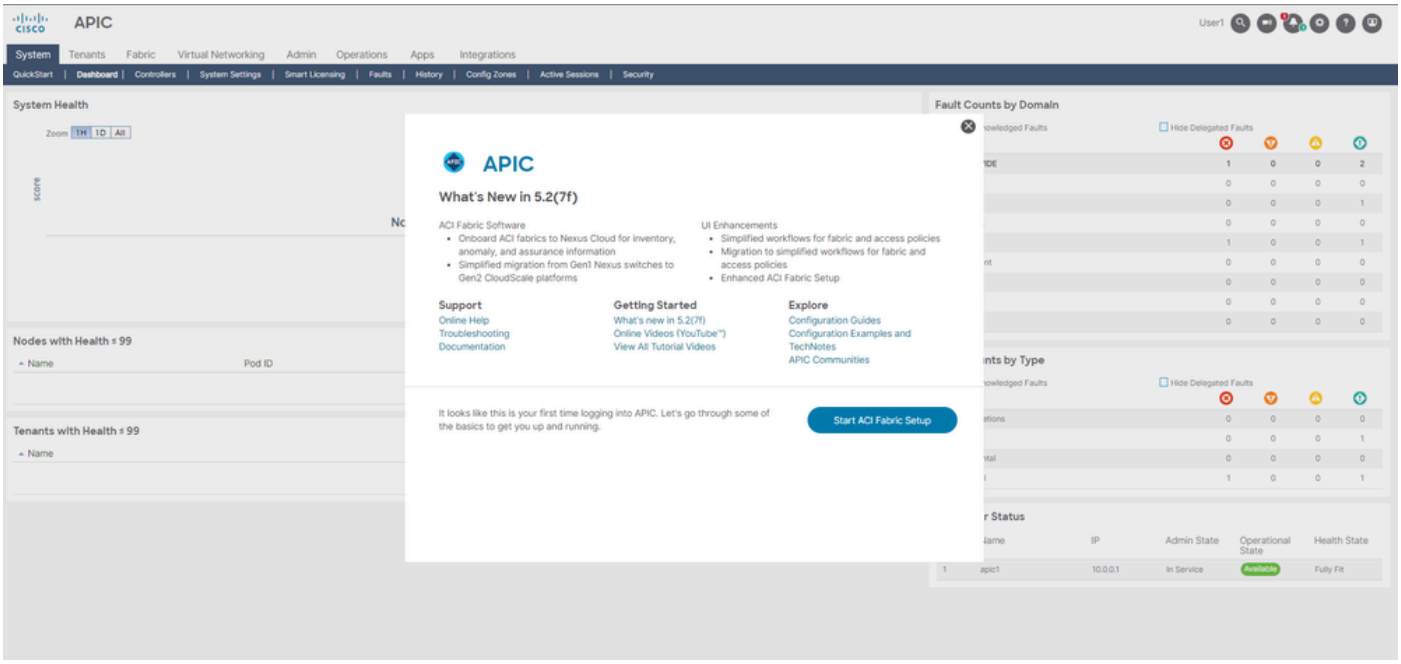
메뉴 모음에서 이미지에 표시된 Admin > AAA > Authentication > AAA > Policy > Default Authentication 대로 이동합니다.

기본 인증을 LDAPRealm로 변경하고 created를 LDAP Login Domain 선택합니다.

다음을 확인합니다.

구성이 올바르게 작동하는지 확인하려면 이 섹션을 활용하십시오.



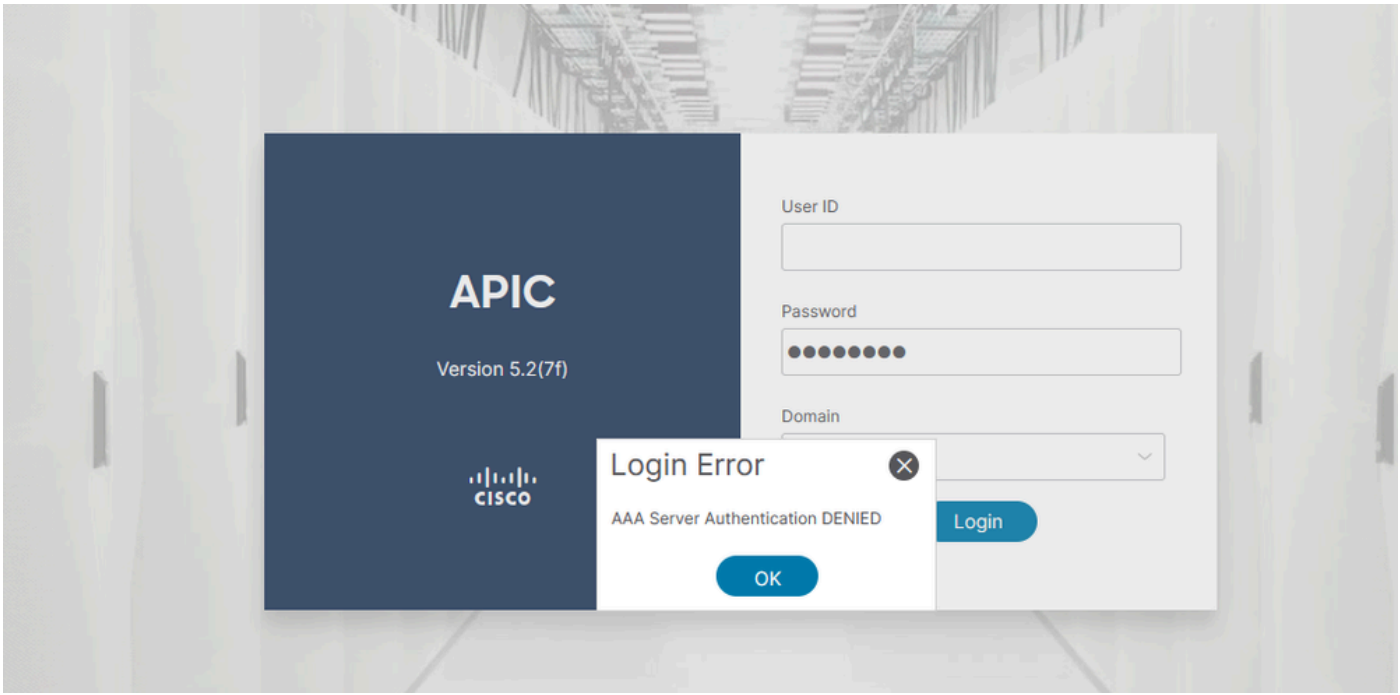


LDAP 사용자가 관리자 역할User1 및 쓰기 권한으로 APIC에 성공적으로 로그인했는지 확인합니다.

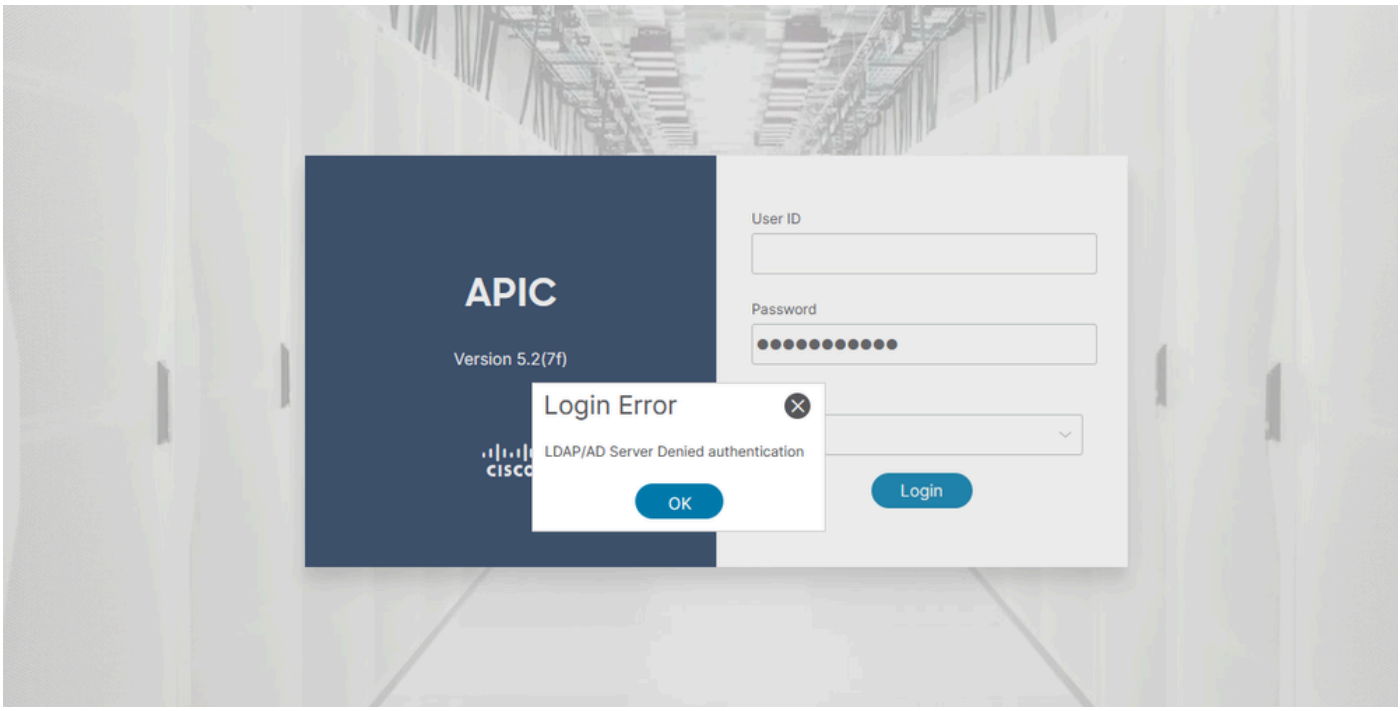
문제 해결

이 섹션에서는 설정 문제 해결을 위해 사용할 수 있는 정보를 제공합니다.

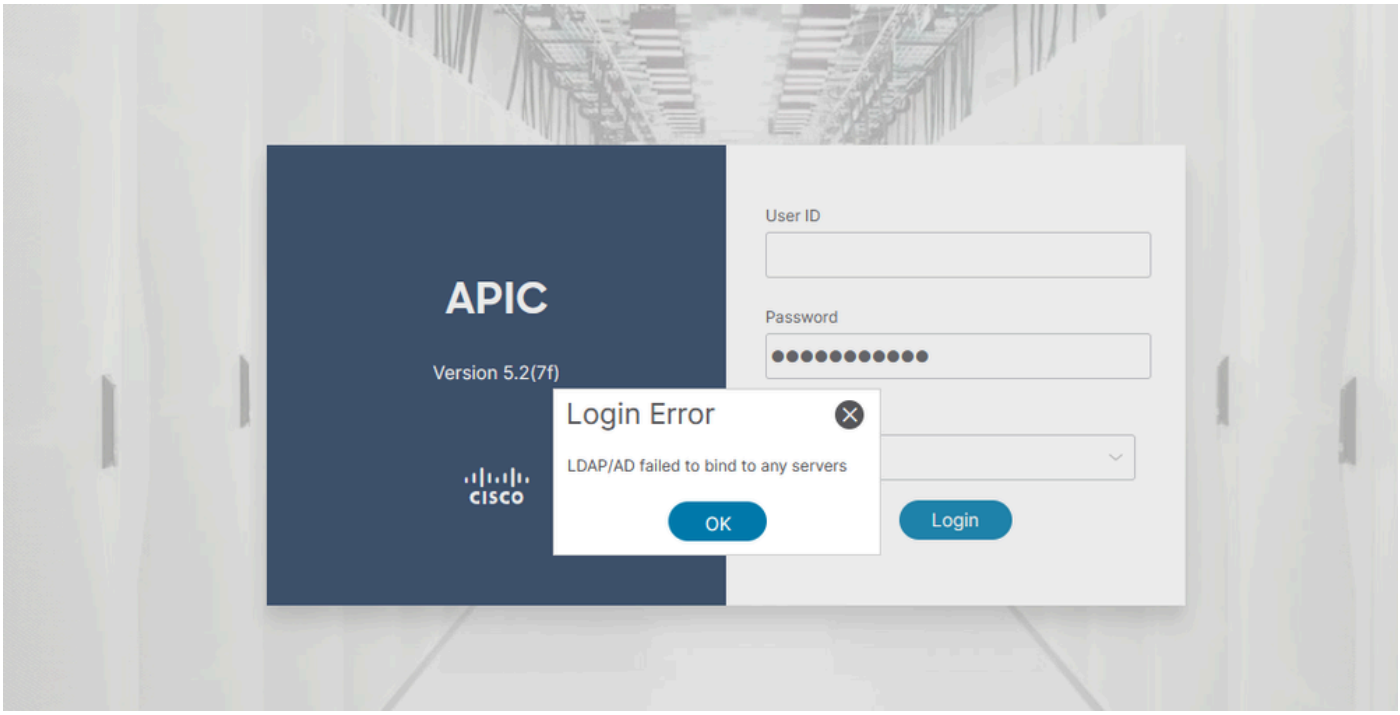
사용자가 LDAP 데이터베이스에 없는 경우:



암호가 올바르지 않은 경우:



LDAP 서버에 연결할 수 없는 경우:



문제 해결 명령:

<#root>

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

추가 지원이 필요한 경우 Cisco TAC에 문의하십시오.

관련 정보

- Cisco APIC 보안 컨피그레이션 가이드, 릴리스 5.2(x)
- Cisco 기술 지원 및 다운로드

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.