配置ACI LDAP身份驗證

目錄

簡介

本文檔介紹如何配置以應用為中心的基礎設施(ACI)輕量級目錄訪問協定(LDAP)身份驗證。

必要條件

需求

思科建議您瞭解以下主題：

- ACI身份驗證、授權和記帳(AAA)策略
- LDAP

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 思科應用程式原則基礎架構控制器(APIC)版本5.2(7f)
- Ubuntu 20.04，帶slapd和phpLDAPadmin

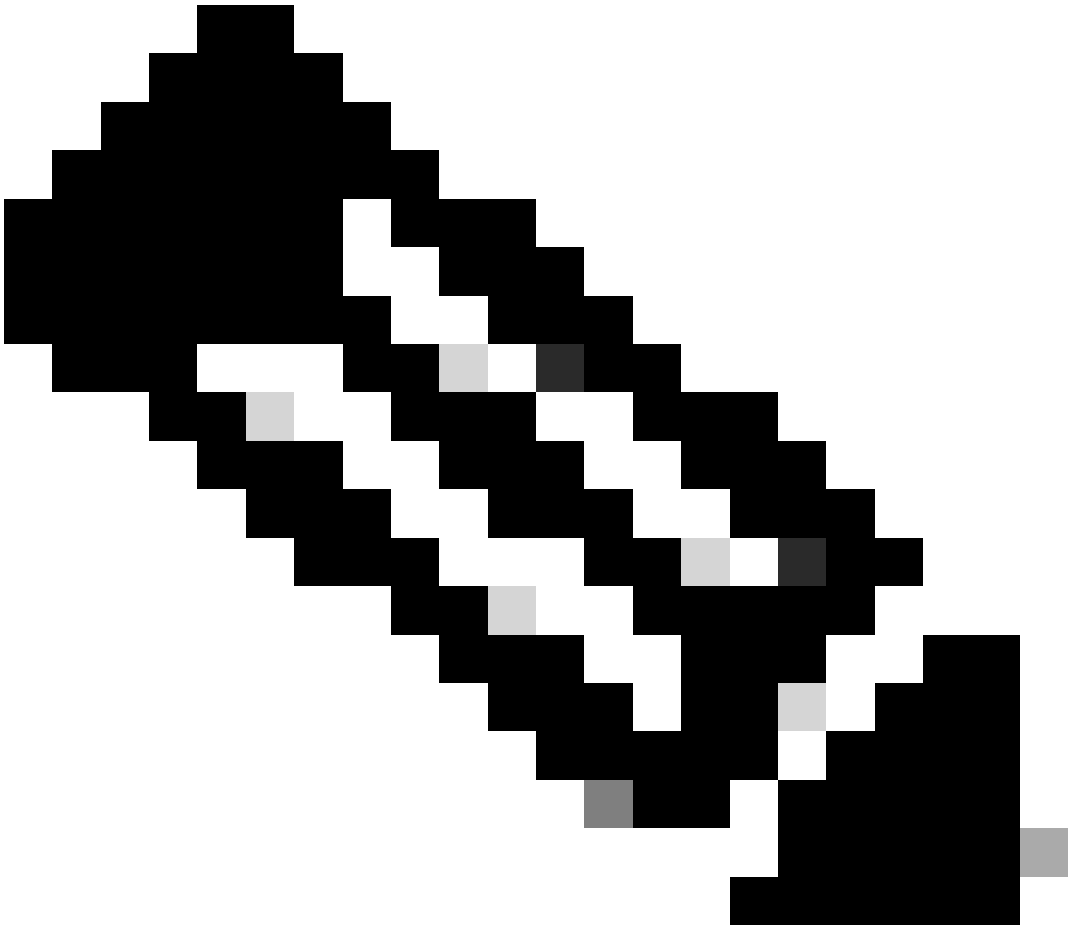
本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

設定

本節介紹如何配置APIC以便與LDAP伺服器整合並使用LDAP作為預設身份驗證方法。

組態

步驟 1.在Ubuntu phpLDAPadmin上建立組/使用者

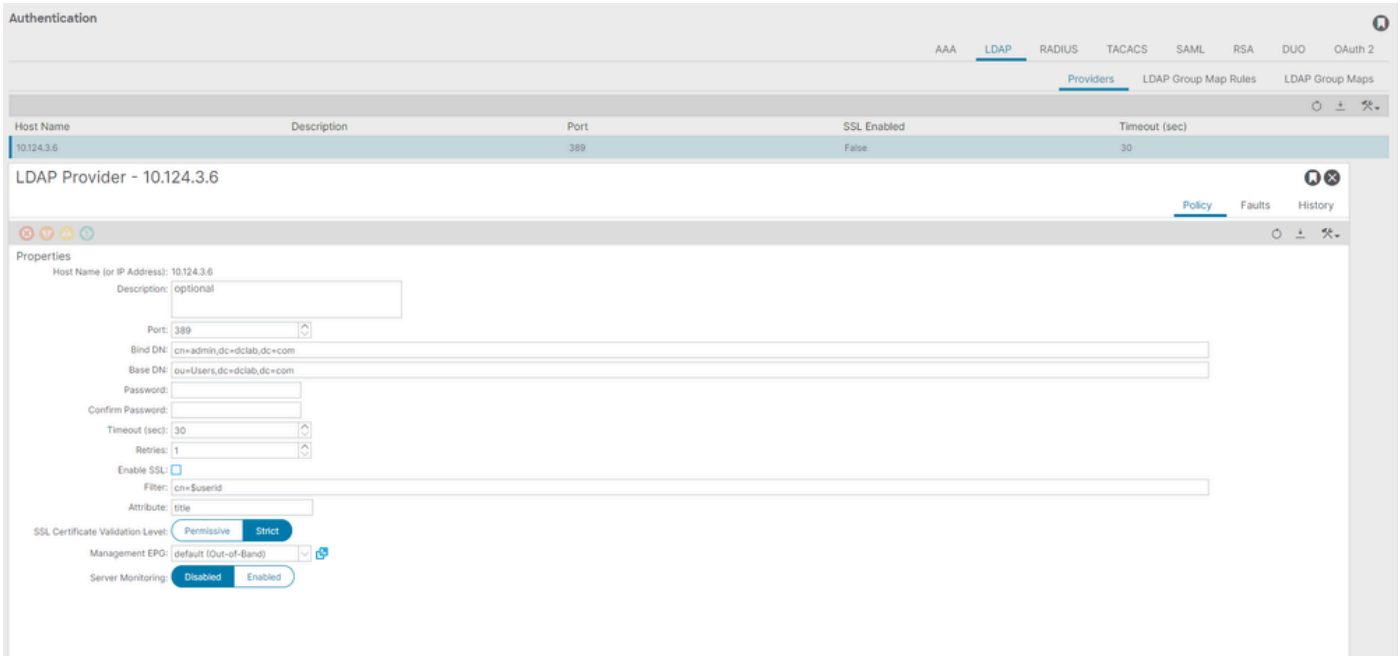


注意：要將Ubuntu配置為LDAP伺服器，請參閱官方Ubuntu網站瞭解綜合指南。如果有現有的LDAP伺服器，請從Step 2開始。

在本文檔中，基本DN是dc=dclab,dc=com，兩個使用者（User1和User2）屬於組(DCGroup)。

步驟 2.在APIC上配置LDAP提供程式

在APIC選單欄上，導航至Admin > AAA > Authentication > LDAP > Providers（如圖所示）。



連結DN：連結DN是您用來根據LDAP進行驗證的憑證。APIC使用此帳戶進行身份驗證，以查詢目錄。

基本DN：APIC使用此字串作為參考點，以搜尋和辨識目錄中的使用者條目。

密碼：這是存取LDAP伺服器所需的「連結DN」的必要密碼，與LDAP伺服器上建立的密碼相關。

啟用SSL：如果使用內部CA或自簽名證書，則必須選擇**Permissive**。

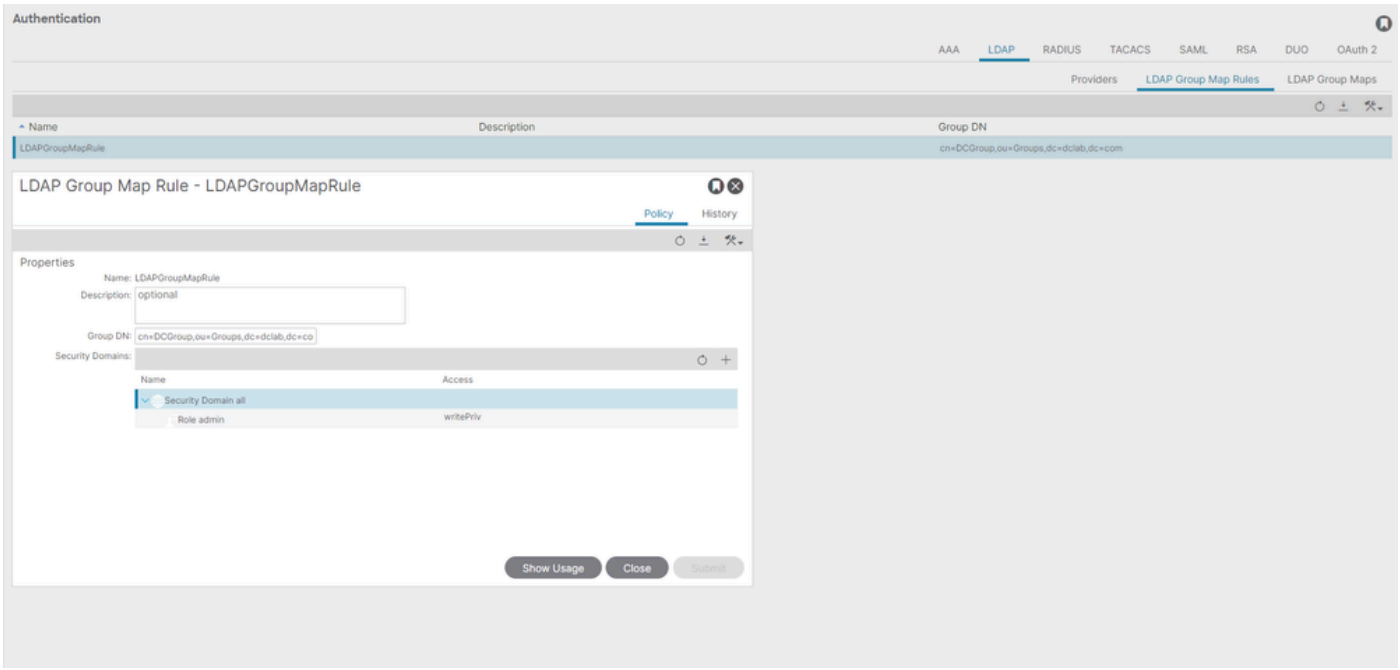
篩選：預設篩選設定是cn=$userid，當使用者定義為具有一般名稱(CN)的物件時，會使用篩選來尋找「基本DN」中的物件。

屬性：屬性用於確定組成員資格和角色。ACI在此處提供兩個選項：memberOf和CiscoAVPair.memberOf 是RFC2307bis屬性，以便標識組成員身份。目前，OpenLDAP檢查RFC2307，因此使用title 來代替。

管理終端組(EPG)：根據選擇的網路管理方法，透過帶內或帶外EPG連線到LDAP伺服器。

步驟 3.配置LDAP組對映規則

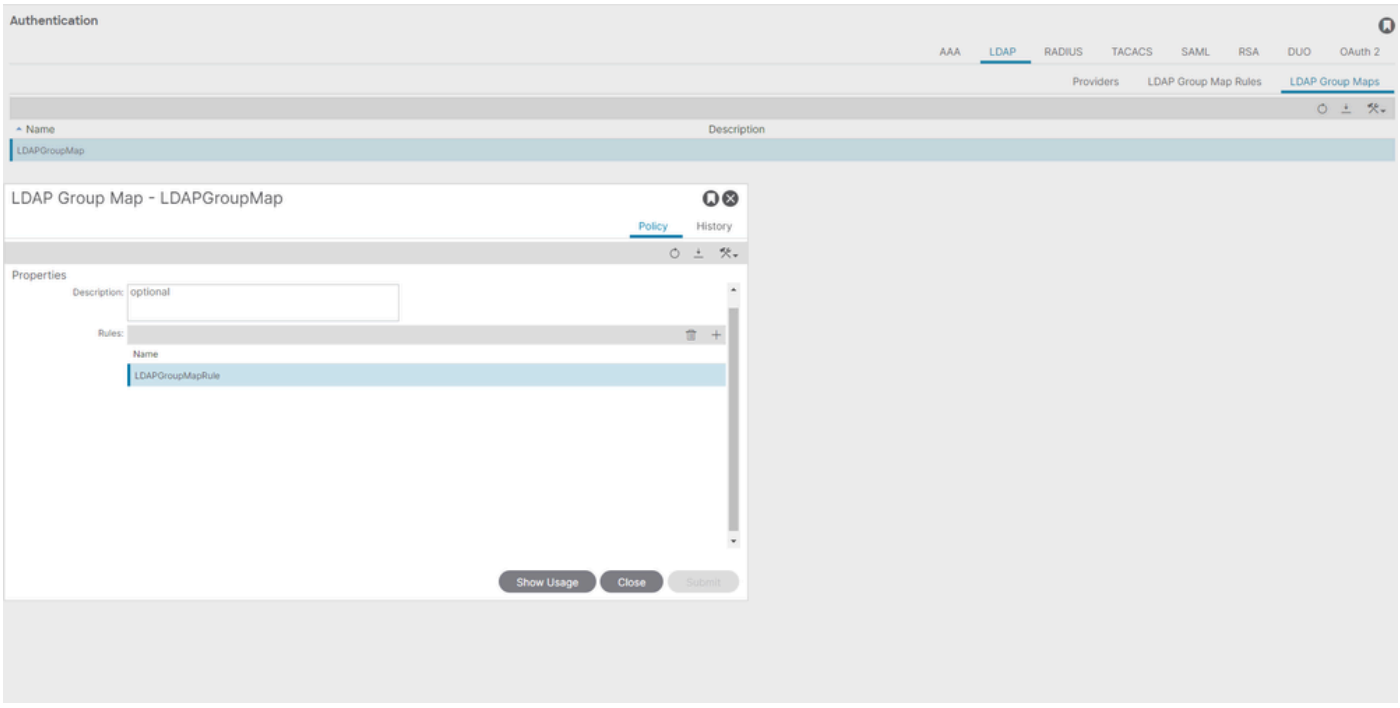
在功能表列上，導覽至Admin > AAA > Authentication > LDAP > LDAP Group Map Rules 如下圖所示。



DCGroup中的使用者具有管理員許可權。因此，組DN將cn=DCGroup, ou=Groups, dc=dclab, dc=com. A分配安全域All，並使用write privilege分配admin的角色。

步驟 4.配置LDAP組對映

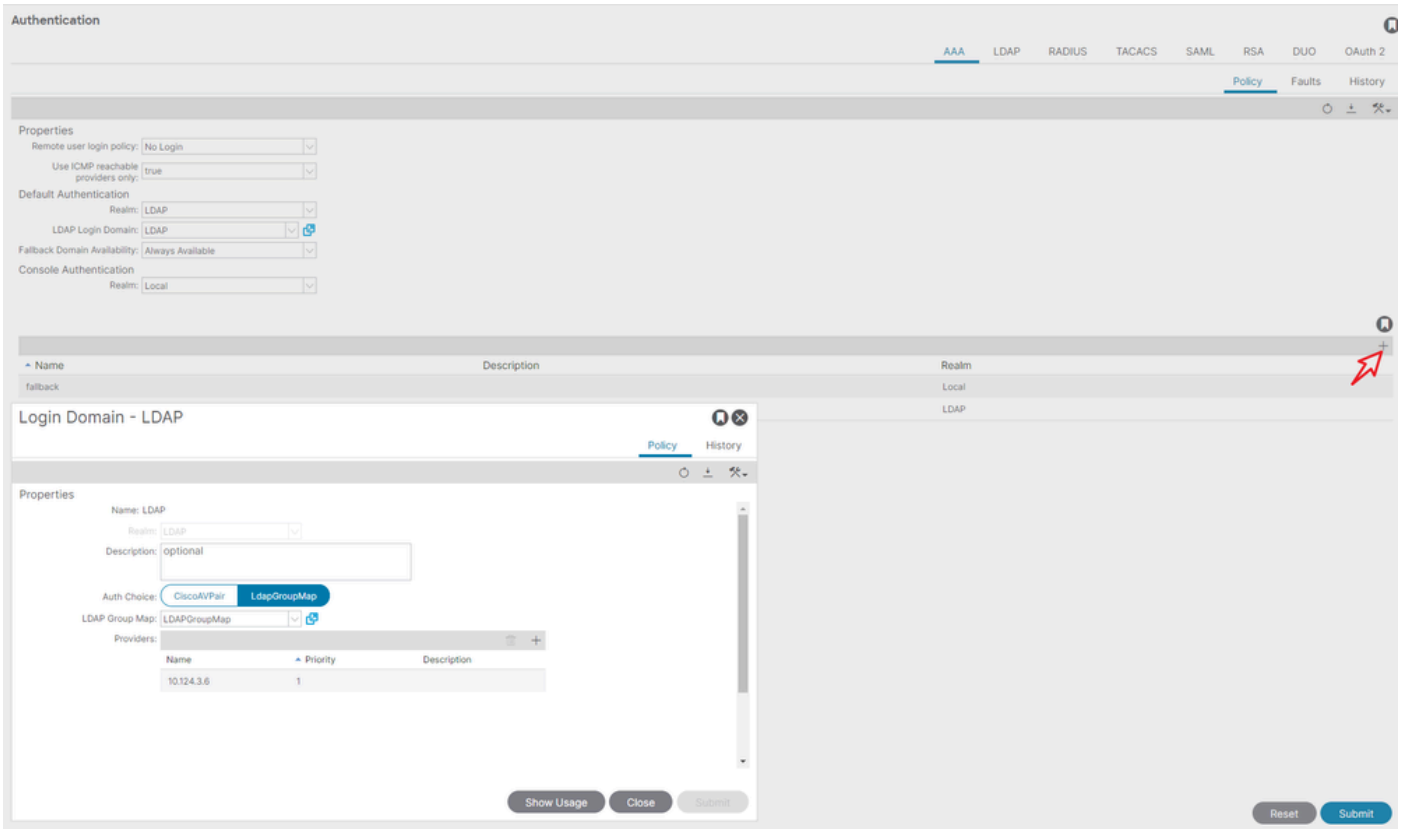
在功能表列上，導覽至Admin > AAA > Authentication > LDAP > LDAP Group Maps 如下圖所示。



建立包含步驟2中建立的LDAP組對映規則的LDAP組對映。

步驟 5.配置AAA身份驗證策略

在功能表列上，導覽至Admin > AAA > Authentication > AAA > Policy > Create a login domain如下圖所示。

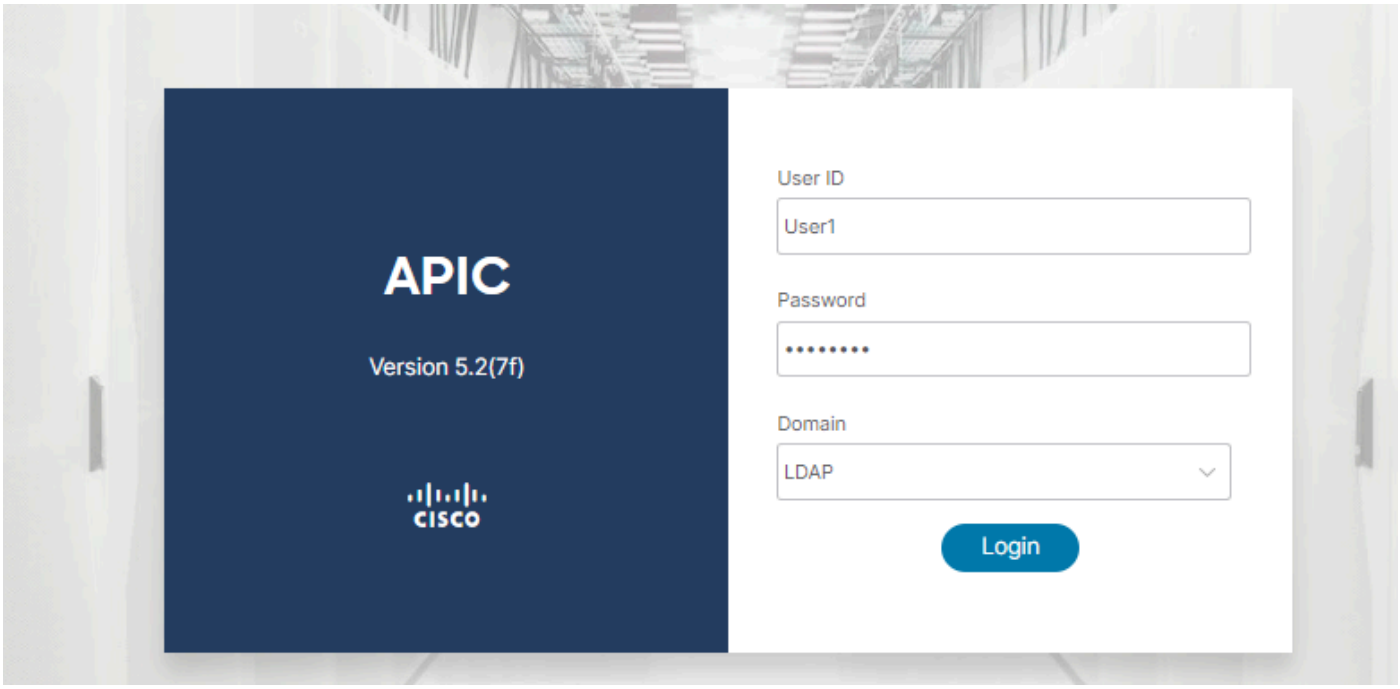


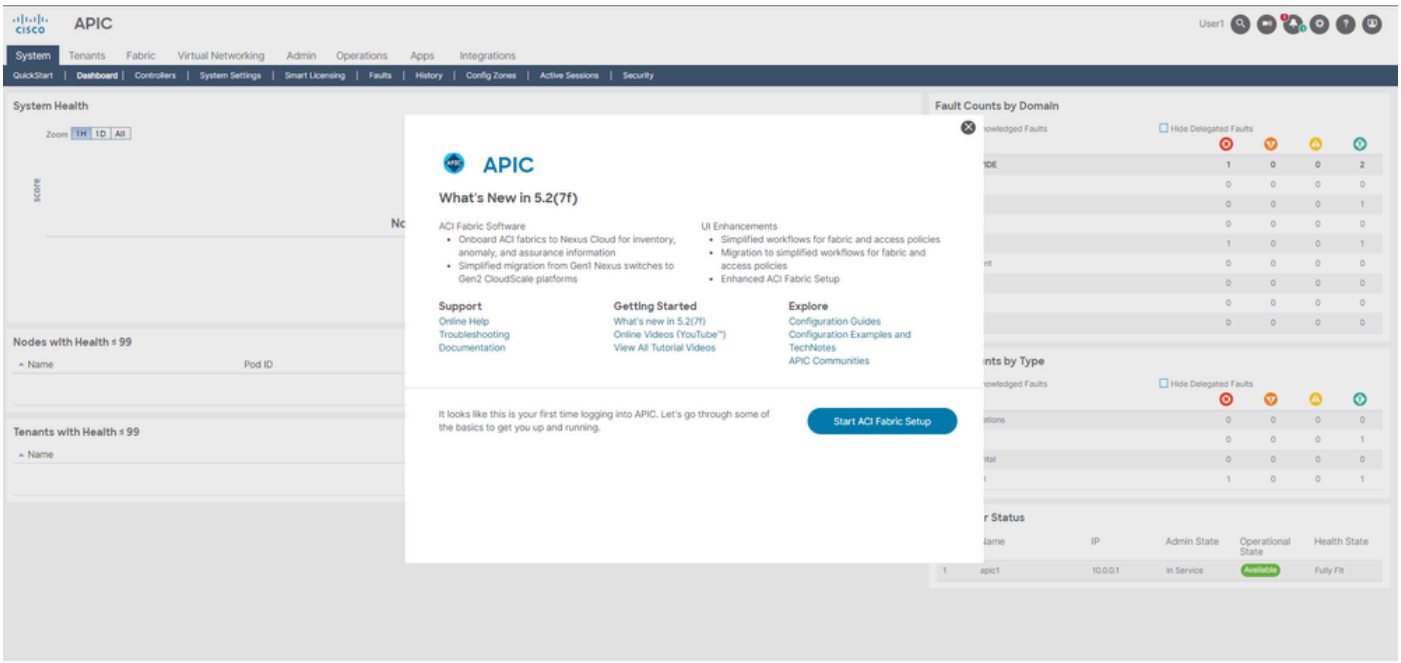
在功能表列上，導覽至Admin > AAA > Authentication > AAA > Policy > Default Authentication 如下圖所示。

將預設身份驗證Realm更改為LDAP，然後選擇已LDAP Login Domain 建立。

驗證

使用本節內容，確認您的組態是否正常運作。



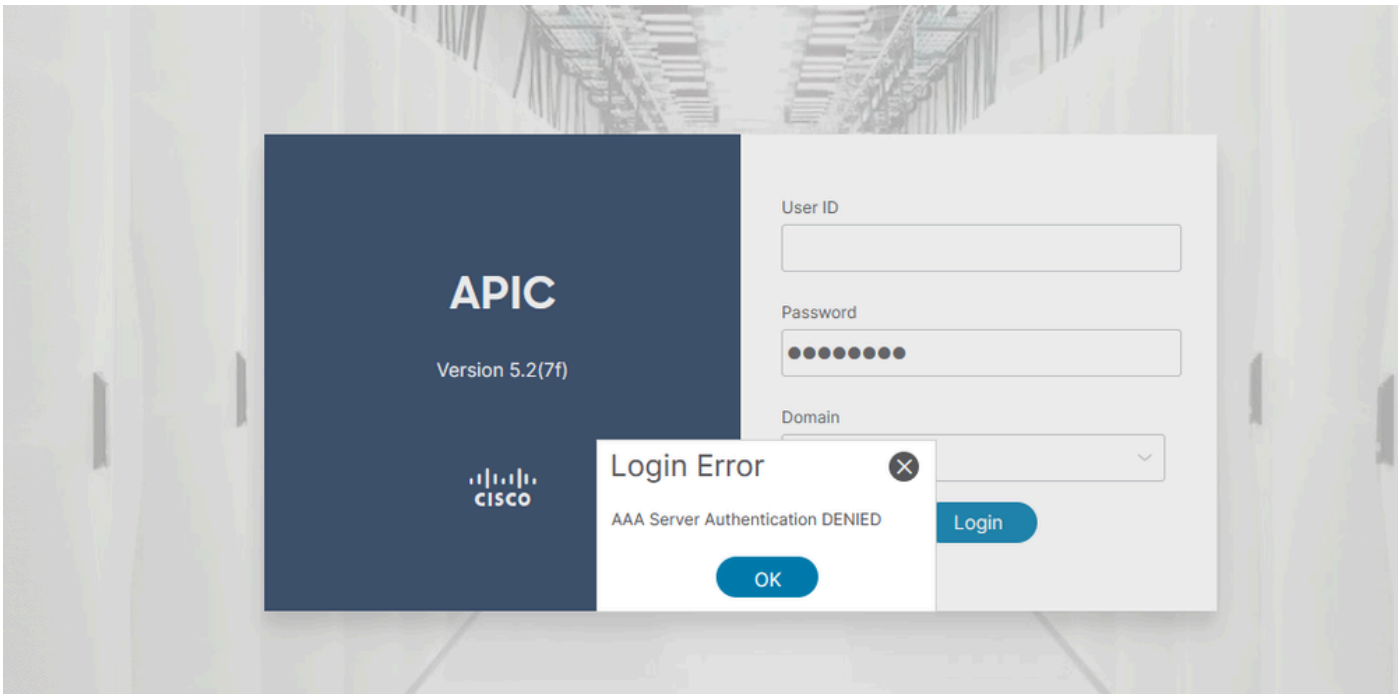


驗證LDAP使用者User1是否使用管理員角色和寫入許可權成功登入APIC。

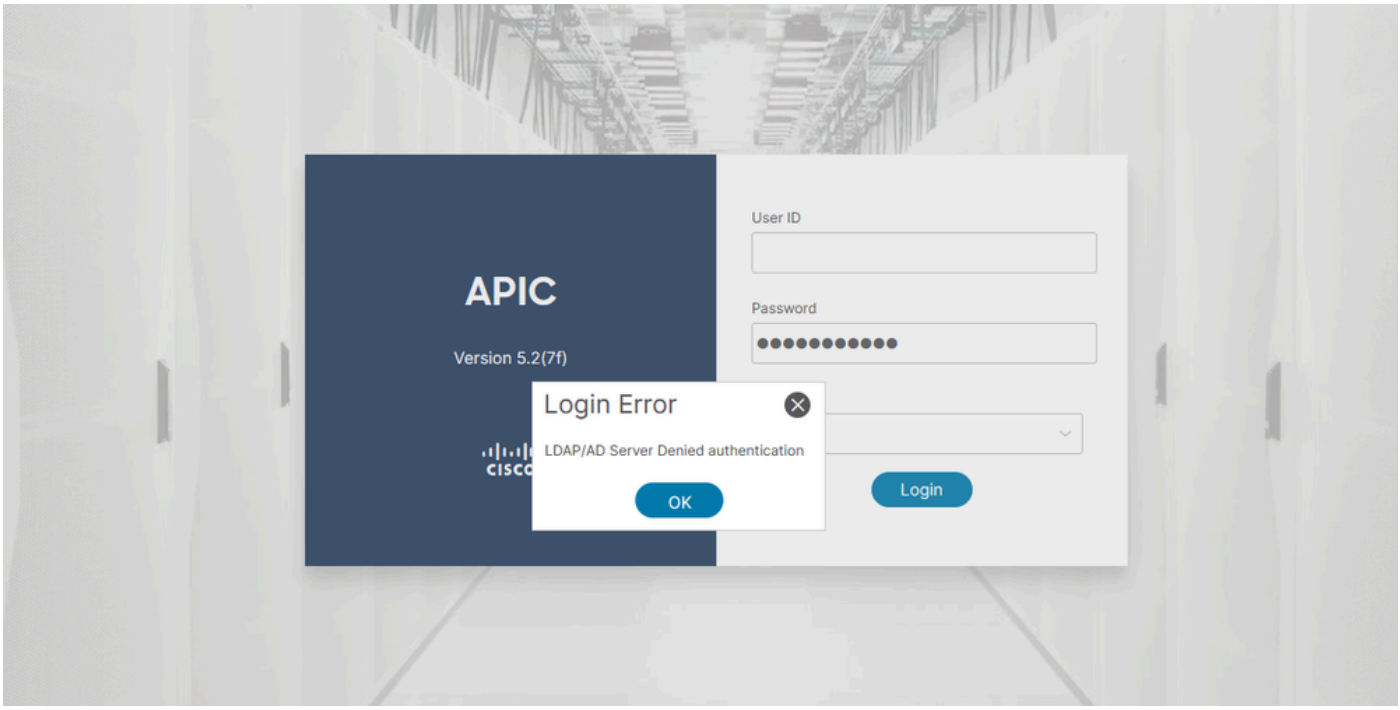
疑難排解

本節提供的資訊可用於對組態進行疑難排解。

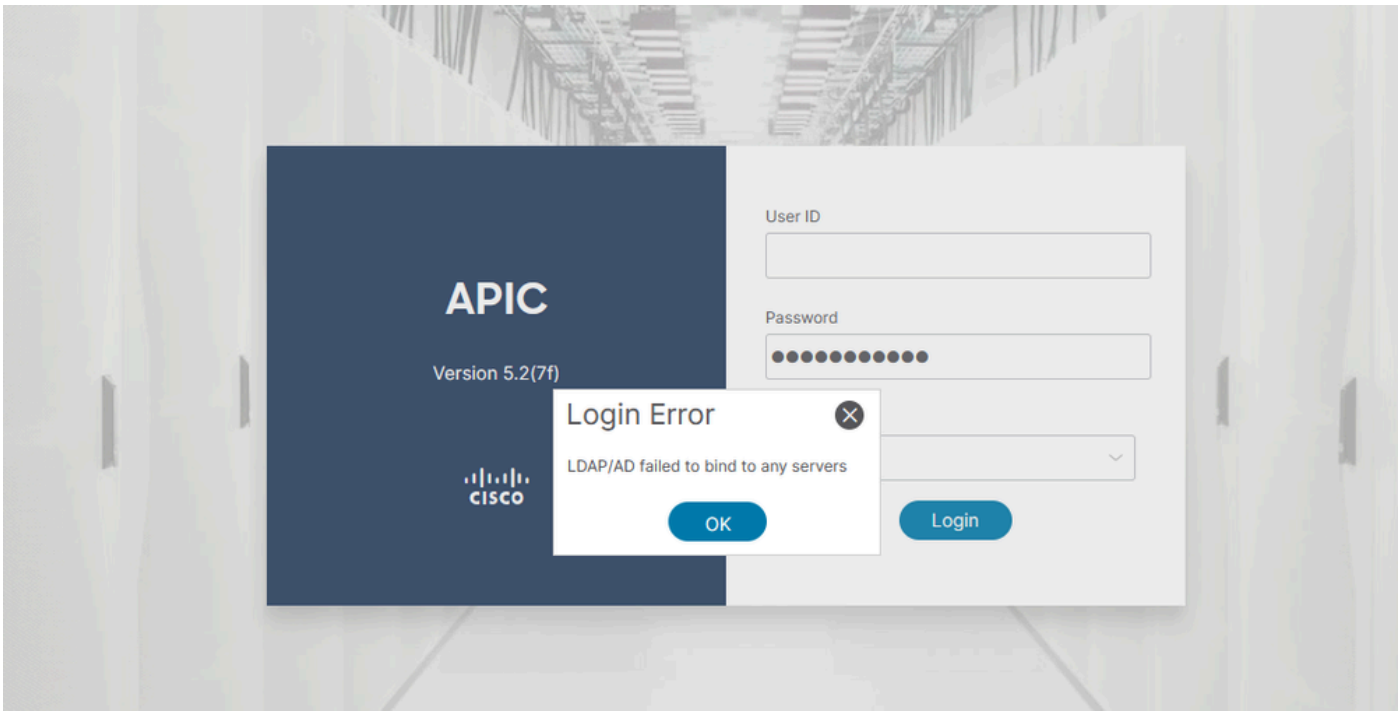
當使用者不存在於LDAP資料庫中時：



當密碼不正確時：



當LDAP伺服器無法連線時：



疑難排解指令:

<#root>

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

如果您需要更多幫助，請與Cisco TAC聯絡。

相關資訊

- 思科APIC安全配置指南5.2(x)版
- 思科技術支援與下載

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。