تكوين مصادقة ACI LDAP

المحتويات

المقدمة

يوضح هذا المستند كيفية تكوين مصادقة بروتوكول الوصول الخفيف إلى الدليل (LDAP) للبنية الأساسية المرتكزة على التطبيقات (ACI).

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- سياسة مصادقة والتفويض والمحاسبة (AAA) للبنية الأساسية المرتكزة على التطبيقات
- LDAP

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج والمكونات المادية التالية:

- وحدة التحكم الخاصة بتطبيق سياسة البنية الأساسية (APIC) من Cisco، الإصدار 5.2(7f)
- Ubuntu 20.04 مع SLAPD و phpLDAPadmin

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت

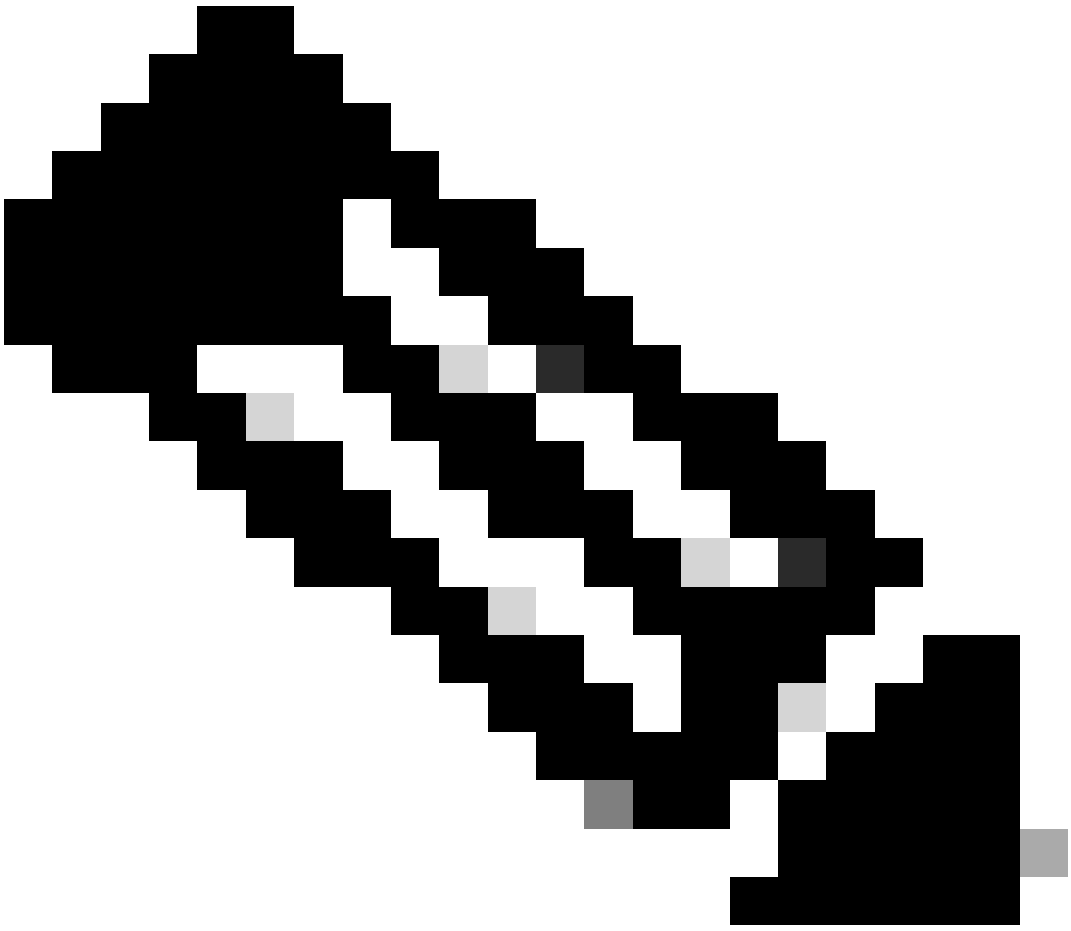
شبكتك قيد التشغيل، فتأكد من فهمك للتأثير المحتمل لأي أمر.

التكوين

يصف هذا القسم كيفية تكوين APIC من أجل التكامل مع خادم LDAP واستخدام LDAP كطريقة المصادقة الافتراضية.

التكوينات

الخطوة 1. إنشاء مجموعات/مستخدمين على Ubuntu phpLDAPadmin

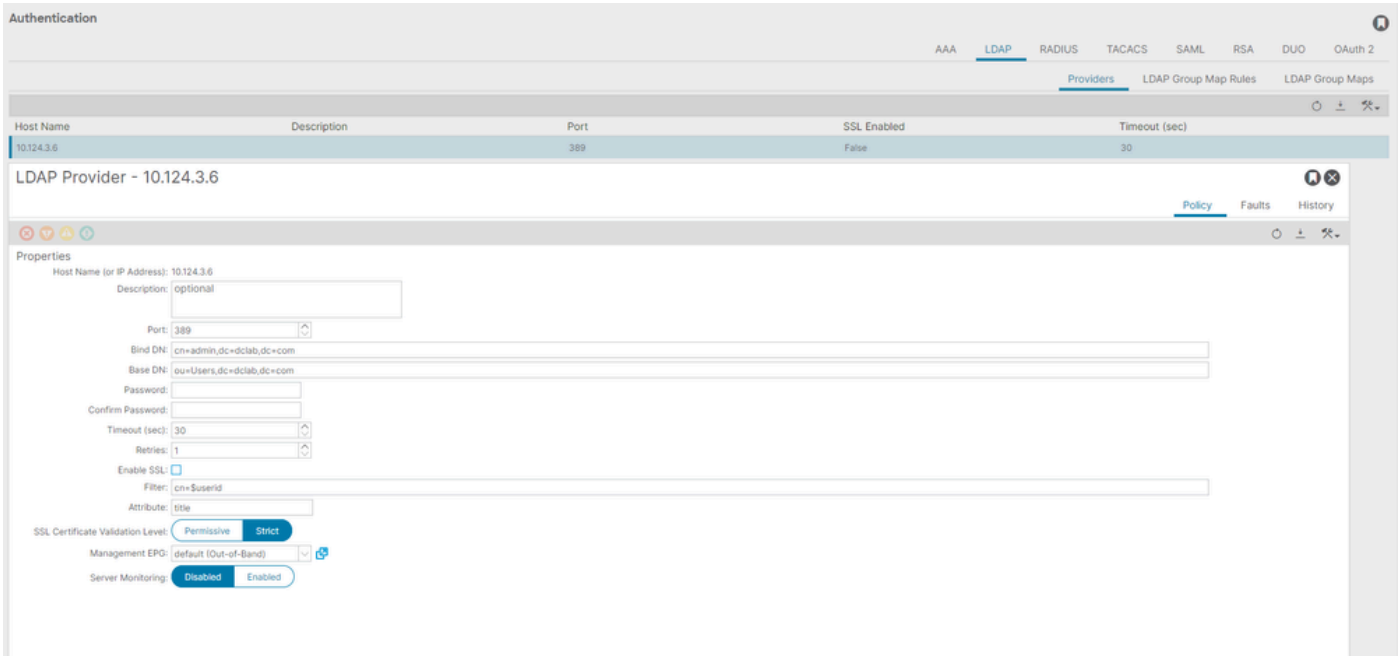


ملاحظة: من أجل تكوين Ubuntu كخادم LDAP، ارجع إلى موقع Ubuntu الرسمي على الويب للحصول على إرشادات شاملة. إذا كان هناك خادم LDAP موجود، ابدأ بالخطوة 2.

في هذا المستند، تقع(User1 و User2) إلى مجموعات (DCGgroup).dc=dclab,dc=com شبكة DN الأساسية وينتمي مستخدمان

الخطوة 2. تكوين موفري LDAP على APIC

في شريط قائمة APIC، انتقل إلى Admin > AAA > Authentication > LDAP > Providers كما هو موضح في الصورة.



Bind DN: يقصد ب Bind DN بيانات الاعتماد التي تستخدمها للمصادقة مقابل LDAP. يقوم APIC بالمصادقة باستخدام هذا الحساب للاستعلام عن الدليل.

DN الأساسي: يتم إستخدام هذه السلسلة بواسطة APIC كنقطة مرجعية للبحث عن إدخالات المستخدم والتعرف عليها داخل الدليل.

كلمة المرور: هذه هي كلمة المرور المطلوبة ل Bind DN الضرورية للوصول إلى خادم LDAP، المرتبطة بكلمة المرور المنشأة على خادم LDAP الخاص بك.

تمكين SSL: إذا كنت تستخدم مصدق داخلي أو شهادة موقعة ذاتيا، يجب أن تختار مستاهل.

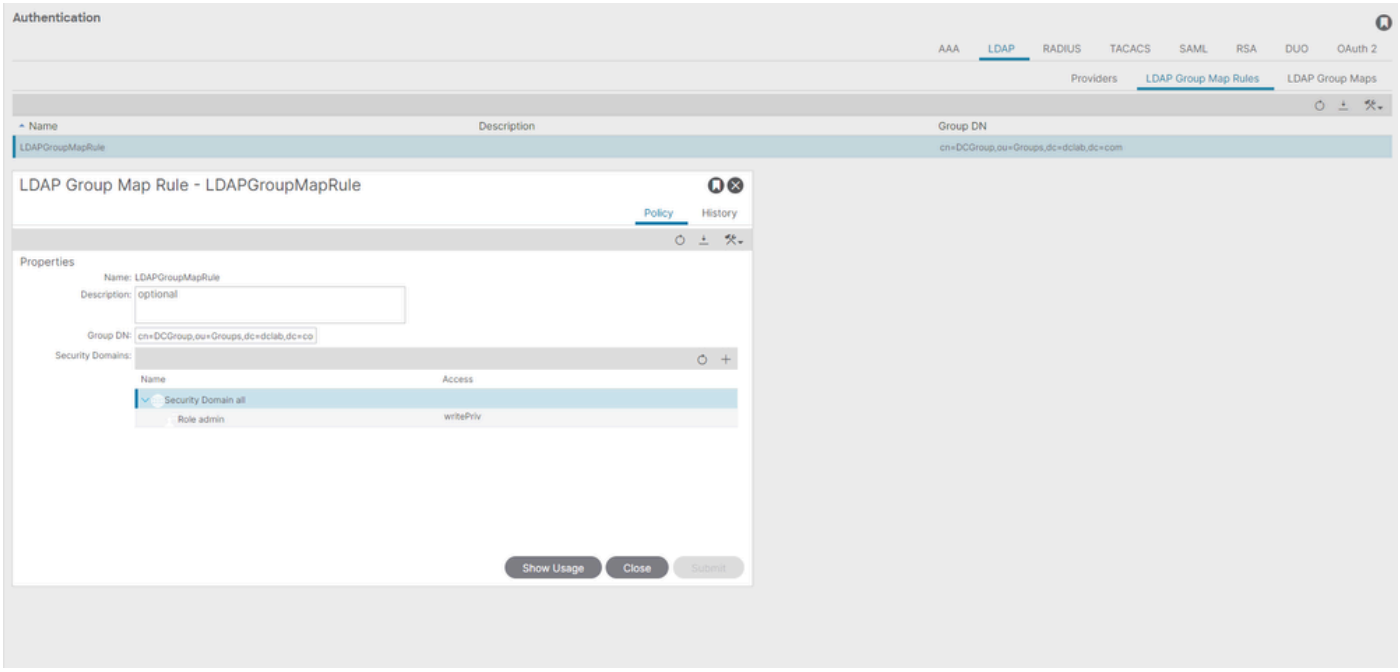
عامل التصفية: يكونcn=$userid إعداد عامل التصفية الافتراضي وهو عندما يتم تعريف المستخدم ككائن له اسم مشترك (CN)، ويتم إستخدام عامل التصفية للبحث عن الكائنات داخل DN الأساسي.

السمة: يتم إستخدام السمة لتحديد عضوية المجموعة والأدوار. توفر واجهة التحكم في الوصول (ACI) خيارين هنا: memberOf CiscoAVPair.memberOf هي سمة RFC2307bis من أجل تحديد عضوية المجموعة. حالياً، يتحقق OpenLDAP من RFC2307، لذلك title يتم إستخدامه بدلاً من ذلك.

مجموعة نقاط نهاية الإدارة (EPG): يتم الاتصال بخادم LDAP إما من خلال EPG داخل النطاق أو خارج النطاق، وذلك حسب نهج إدارة الشبكة المختار.

الخطوة 3. تكوين قواعد تعيين مجموعة LDAP

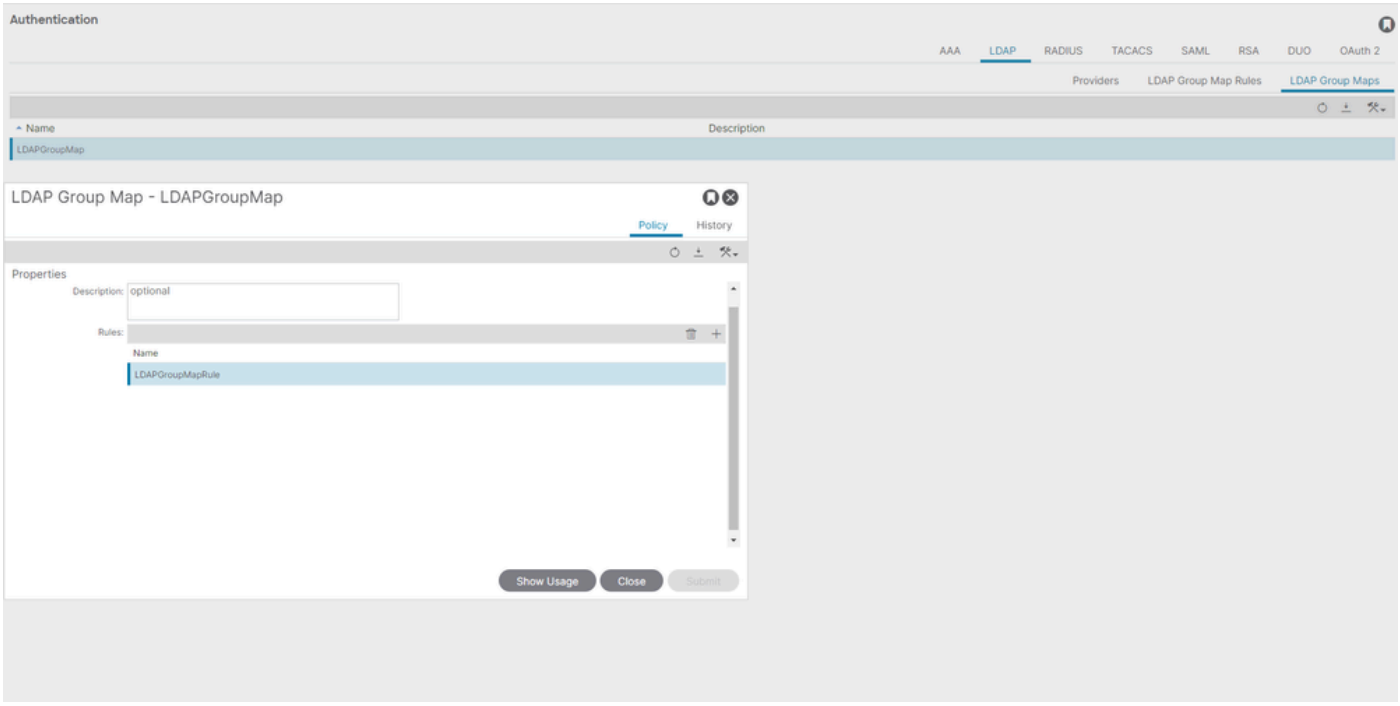
في شريط القائمة، انتقل إلى Admin > AAA > Authentication > LDAP > LDAP Group Map Rules كما هو موضح في الصورة.



يتمتع المستخدمون في DCGgroup بامتيازات المسؤول. لذلك، يقوم Group DN cn=DCGroup, ou=Groups, dc=dclab, dc=com. Aبإرسال مجال المأمن إلىAll أدوار admin مع write privilege وتخصيصها .

الخطوة 4. تكوين خارطة مجموعة LDAP

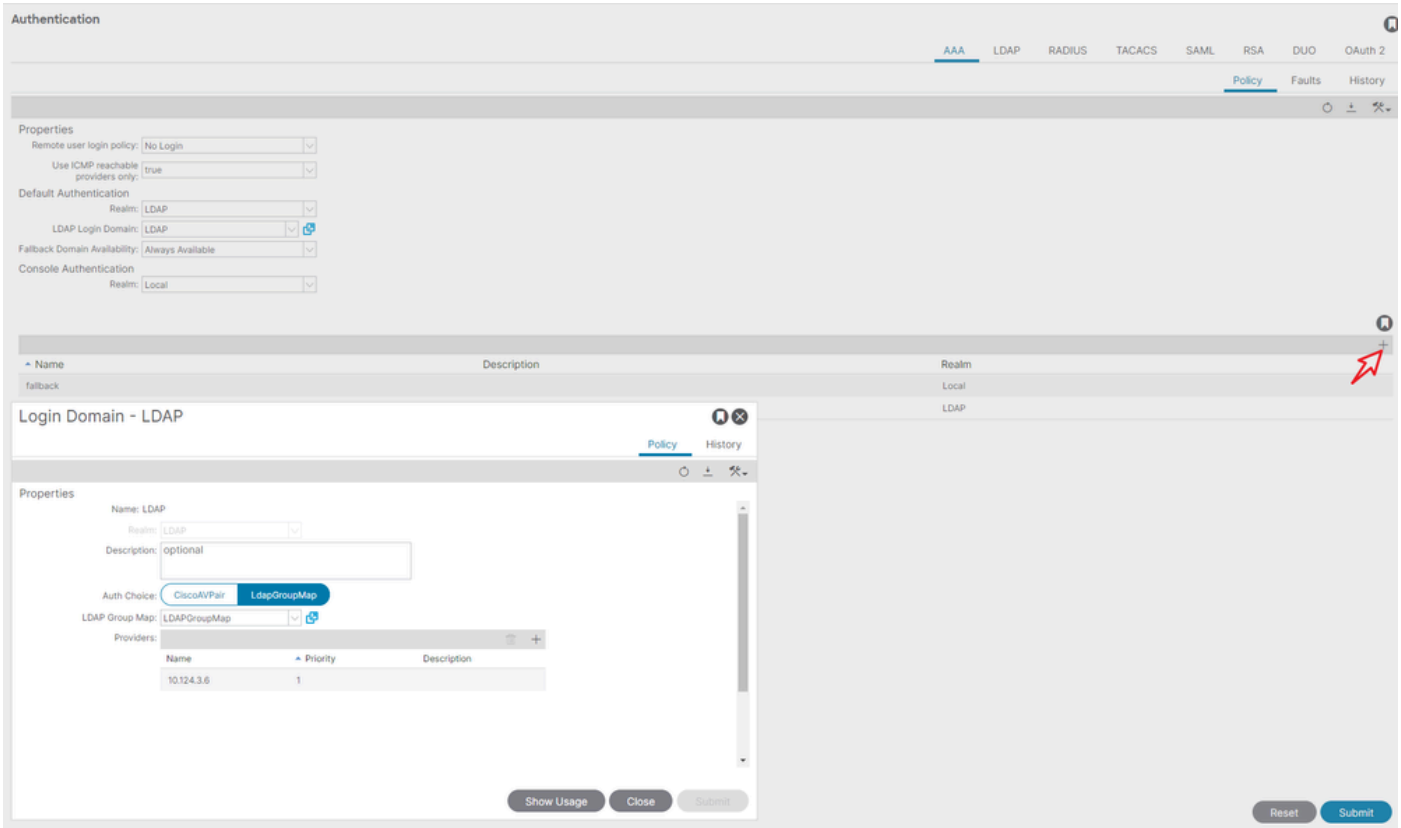
في شريط القائمة، انتقل إلى Admin > AAA > Authentication > LDAP > LDAP Group Maps كما هو موضح في الصورة.



إنشاء خريطة مجموعة LDAP تحتوي على قواعد خريطة مجموعة LDAP التي تم إنشاؤها في الخطوة 2.

الخطوة 5. تكوين سياسة مصادقة AAA

في شريط القائمة، انتقل إلى Admin > AAA > Authentication > AAA > Policy > Create a login domain كما هو موضح في الصورة.

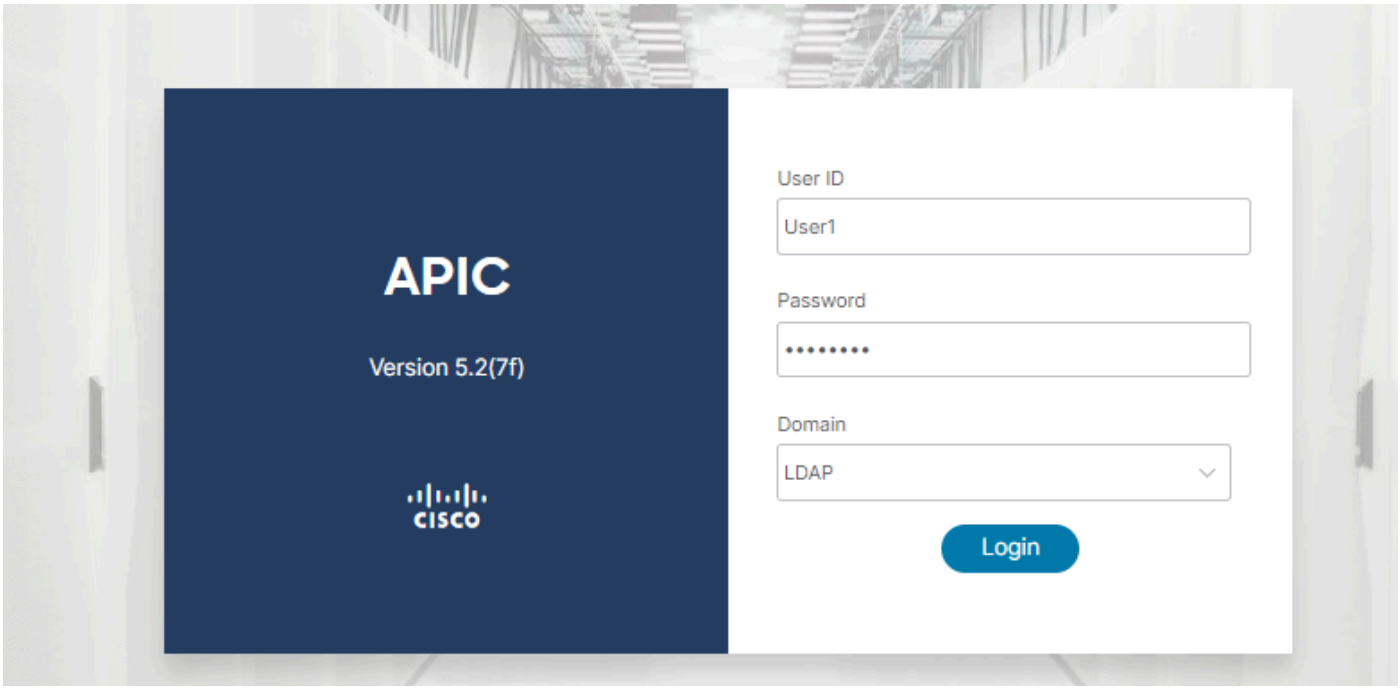


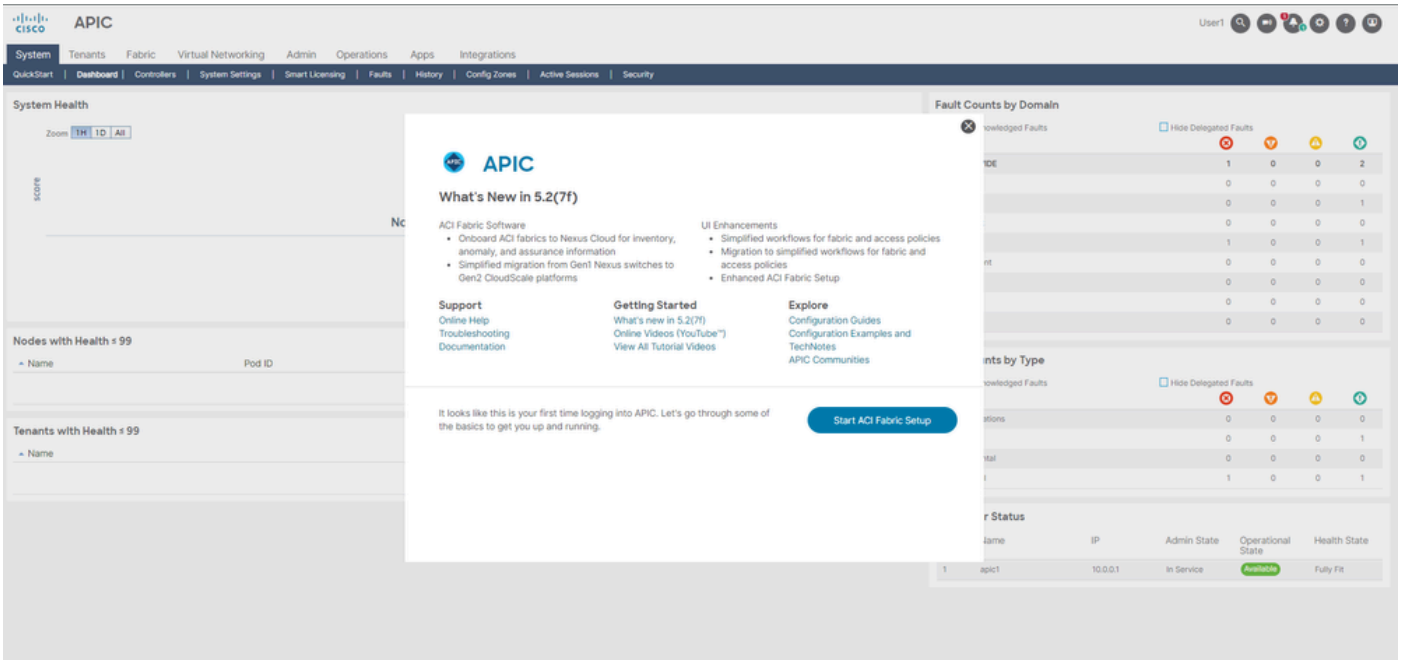
في شريط القائمة، انتقل إلى Admin > AAA > Authentication > AAA > Policy > Default Authentication كما هو موضح في الصورة.

قم بتغيير المصادقة الافتراضية Realm إلى LDAP وحدد LDAP Login Domain المنشأة.

التحقق من الصحة

استخدم هذا القسم لتأكيد عمل التكوين بشكل صحيح.



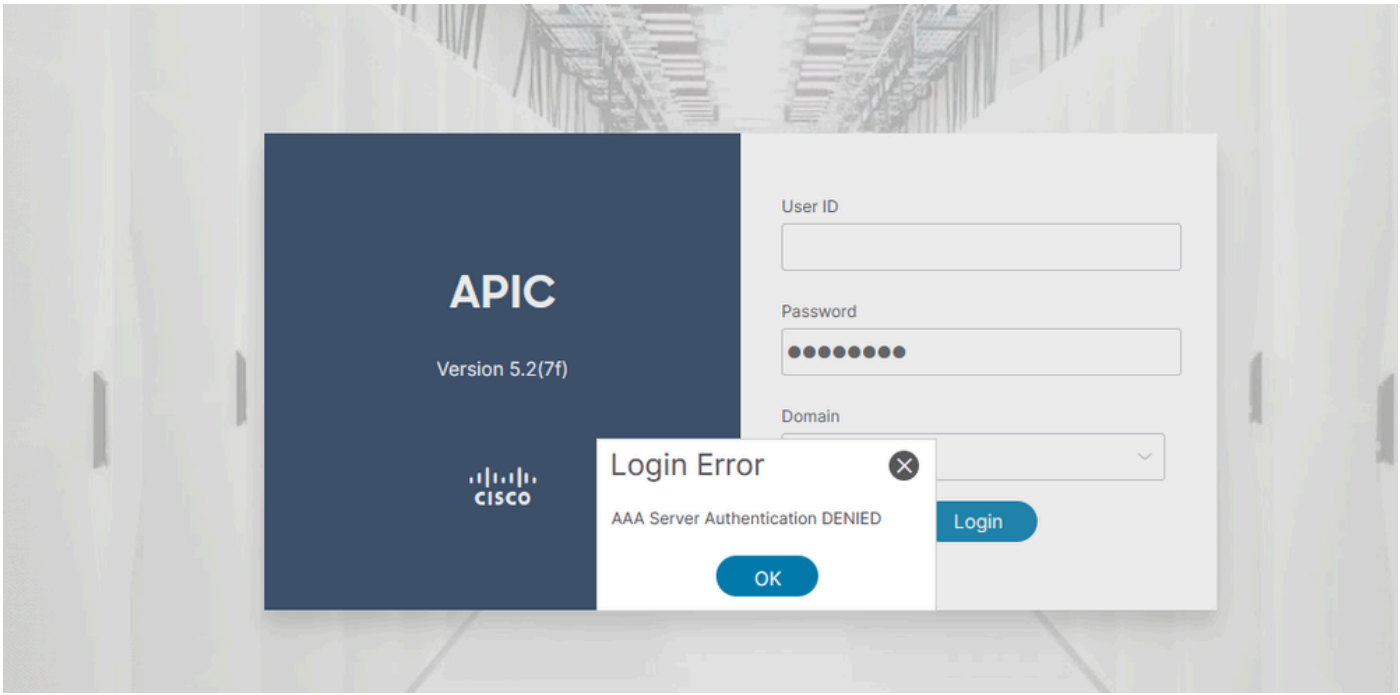


دقق أن ال LDAP User1 سجل مستعمل في APIC بنجاح مع دور مدير وامتياز كاتب.

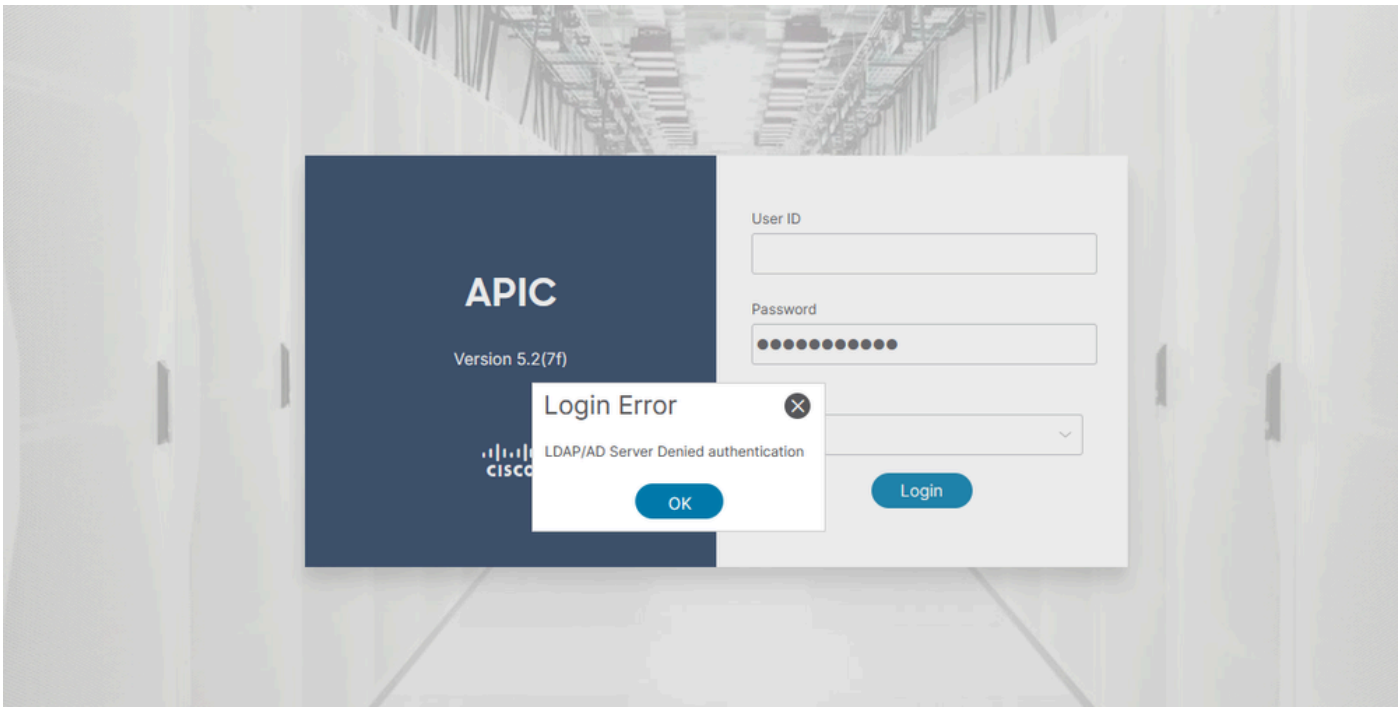
استكشاف الأخطاء وإصلاحها

يوفر هذا القسم معلومات يمكنك إستخدامها لاستكشاف أخطاء التكوين وإصلاحها.

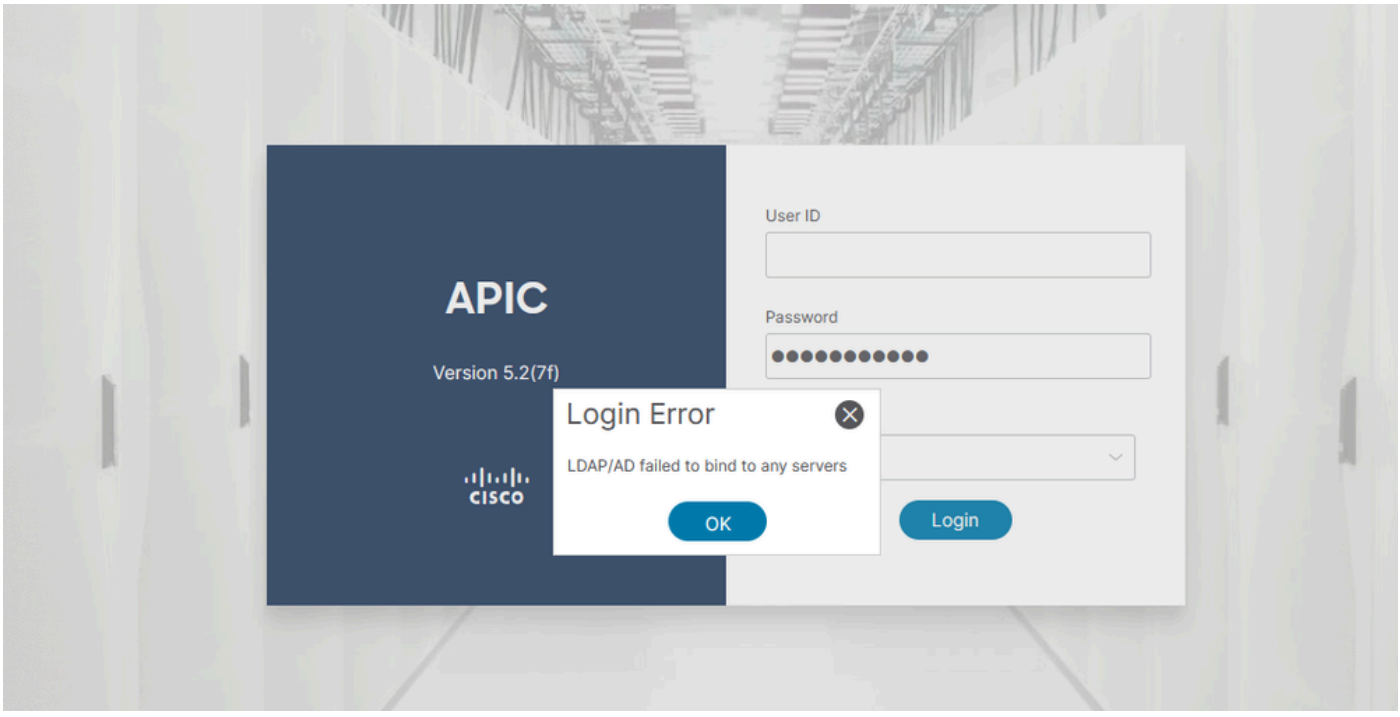
عندما يكون المستخدم غير موجود في قاعدة بيانات LDAP:



عندما تكون كلمة المرور غير صحيحة:



عندما يتعذر الوصول إلى خادم LDAP:



أوامر استكشاف الأخطاء وإصلاحها:

<#root>

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

إن يحتاج أنت كثير مساعدة، اتصل ب cisco TAC.

معلومات ذات صلة

- دليل تكوين أمان واجهة برمجة التطبيقات من Cisco، الإصدار 5.2(x)
- الدعم الفني والتنزيلات من Cisco

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).