Configurer l'authentification LDAP ACI

Table des matières

Introduction

Ce document décrit comment configurer l'authentification LDAP (Lightweight Directory Access Protocol) de l'infrastructure axée sur les applications (ACI).

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Politique AAA (Authentication, Authorization, and Accounting) de l'ACI
- LDAP

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Contrôleur Cisco APIC (Application Policy Infrastructure Controller) version 5.2(7f)
- Ubuntu 20.04 avec slapd et 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. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

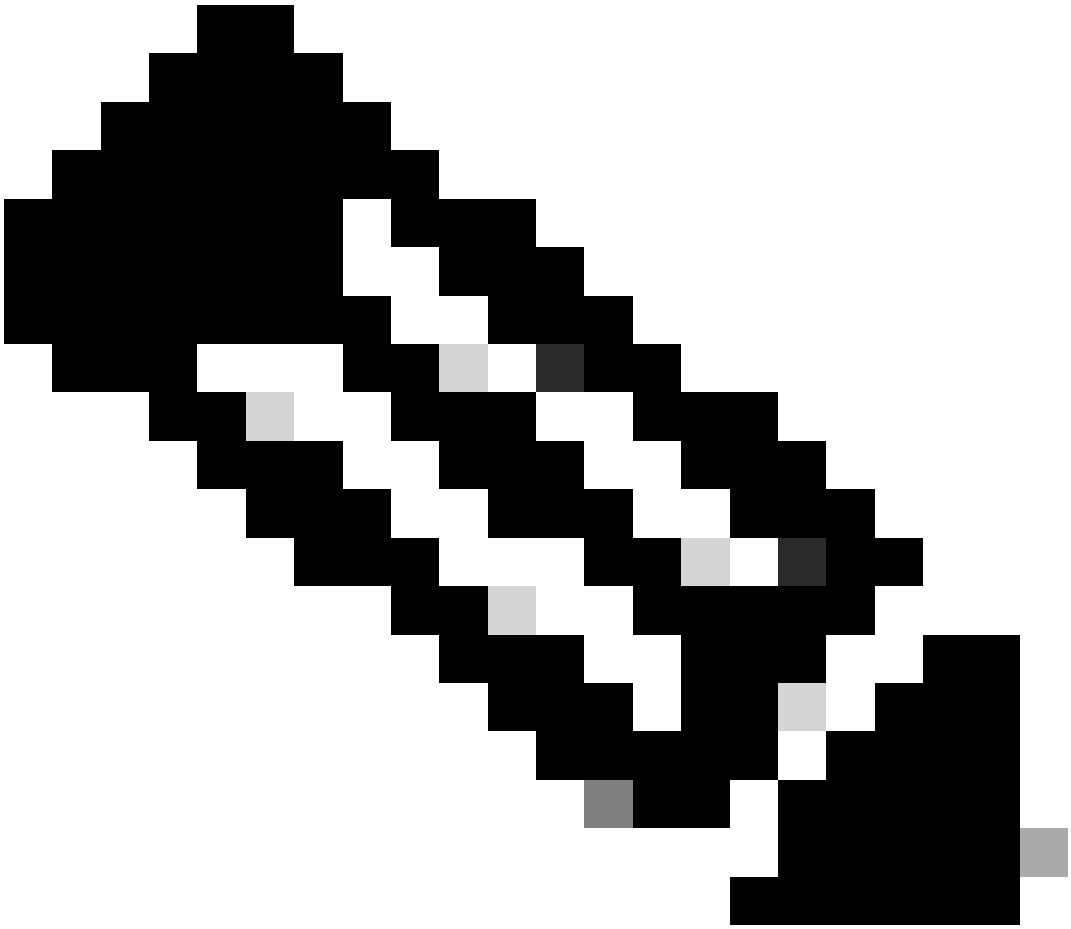
Configurer

Cette section décrit comment configurer le contrôleur APIC afin de l'intégrer au serveur LDAP et utiliser LDAP comme méthode d'authentification par défaut.

Configurations

Étape 1. Créer des groupes/utilisateurs sur Ubuntu phpLDAPadmin

---

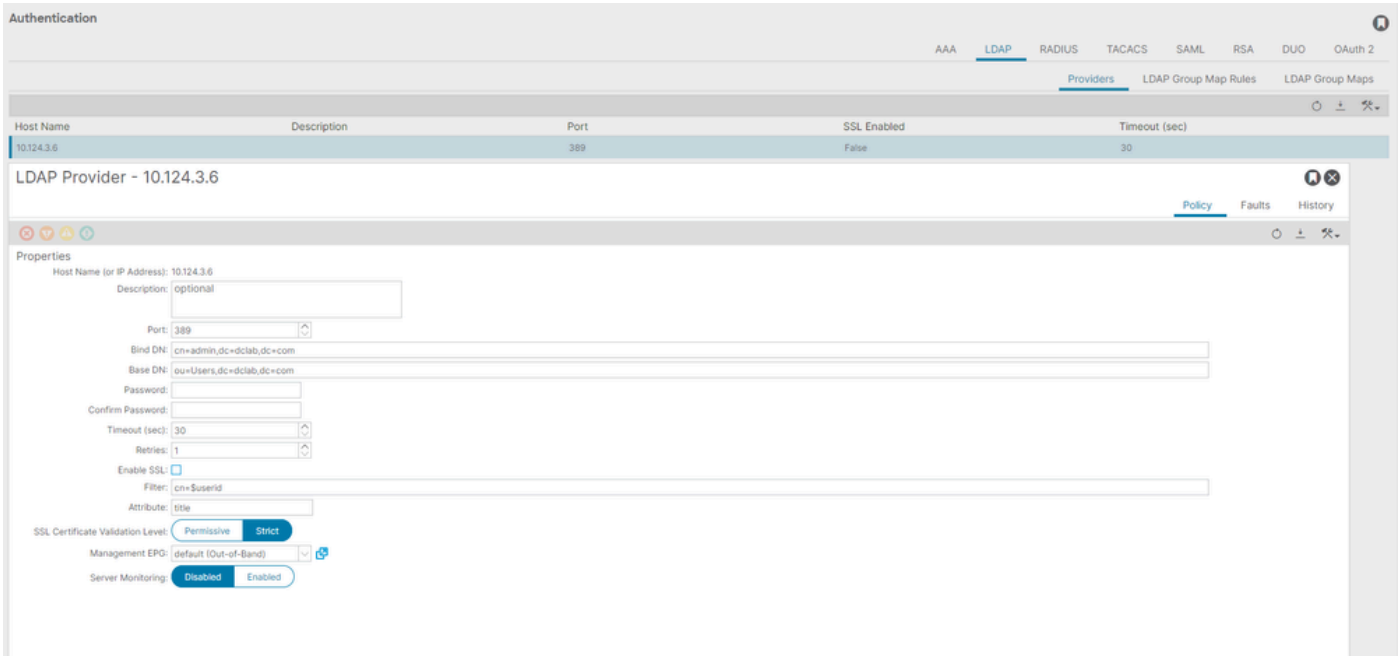


> Remarque : Pour configurer Ubuntu en tant que serveur LDAP, reportez-vous au site Web officiel d'Ubuntu pour obtenir des instructions détaillées. S'il existe un serveur LDAP, commencez à l'étape 2.

Dans ce document, le DN de base est dc=dclab,dc=com et deux utilisateurs (User1 et User2) appartiennent à des groupes (DCGroup).

Étape 2. Configuration des fournisseurs LDAP sur APIC

Dans la barre de menus du module APIC, accédez à commeAdmin > AAA > Authentication > LDAP > Providers indiqué dans l'image.



Bind DN : le DN de liaison est les informations d'identification que vous utilisez pour vous authentifier auprès d'un LDAP. Le contrôleur APIC s'authentifie à l'aide de ce compte pour interroger le répertoire.

Base DN : cette chaîne est utilisée par le contrôleur APIC comme point de référence pour la recherche et l'identification des entrées utilisateur dans le répertoire.

Password : mot de passe requis pour le DN de liaison nécessaire pour accéder au serveur LDAP, en corrélation avec le mot de passe établi sur votre serveur LDAP.

Enable SSL : si vous utilisez une autorité de certification interne ou un certificat auto-signé, vous devez choisir **Permissive**.

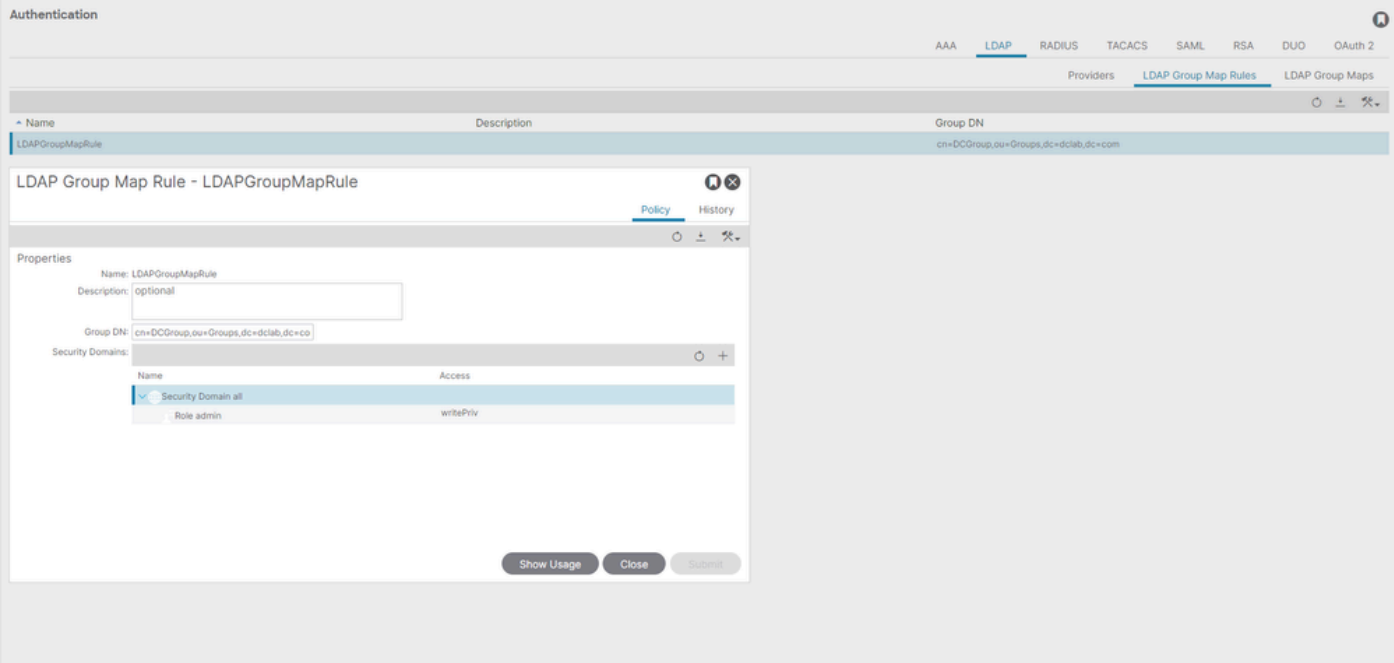
Filtre : le paramètre de filtre par défaut est cn=$userid lorsque l'utilisateur est défini en tant qu'objet avec un nom commun (CN), le filtre est utilisé pour rechercher les objets dans le DN de base.

Attribut : l'attribut est utilisé pour déterminer l'appartenance au groupe et les rôles. L'ACI offre deux options ici : memberOf et CiscoAVPair.memberOf est un attribut RFC2307bis afin d'identifier l'appartenance au groupe. Actuellement, OpenLDAP vérifie RFC2307, donc title est utilisé à la place.

Groupe de terminaux de gestion (EPG) : la connectivité au serveur LDAP est assurée par le groupe de terminaux de gestion (EPG) intrabande ou hors bande, en fonction de l'approche de gestion du réseau choisie.

Étape 3. Configurer les règles de mappage de groupe LDAP

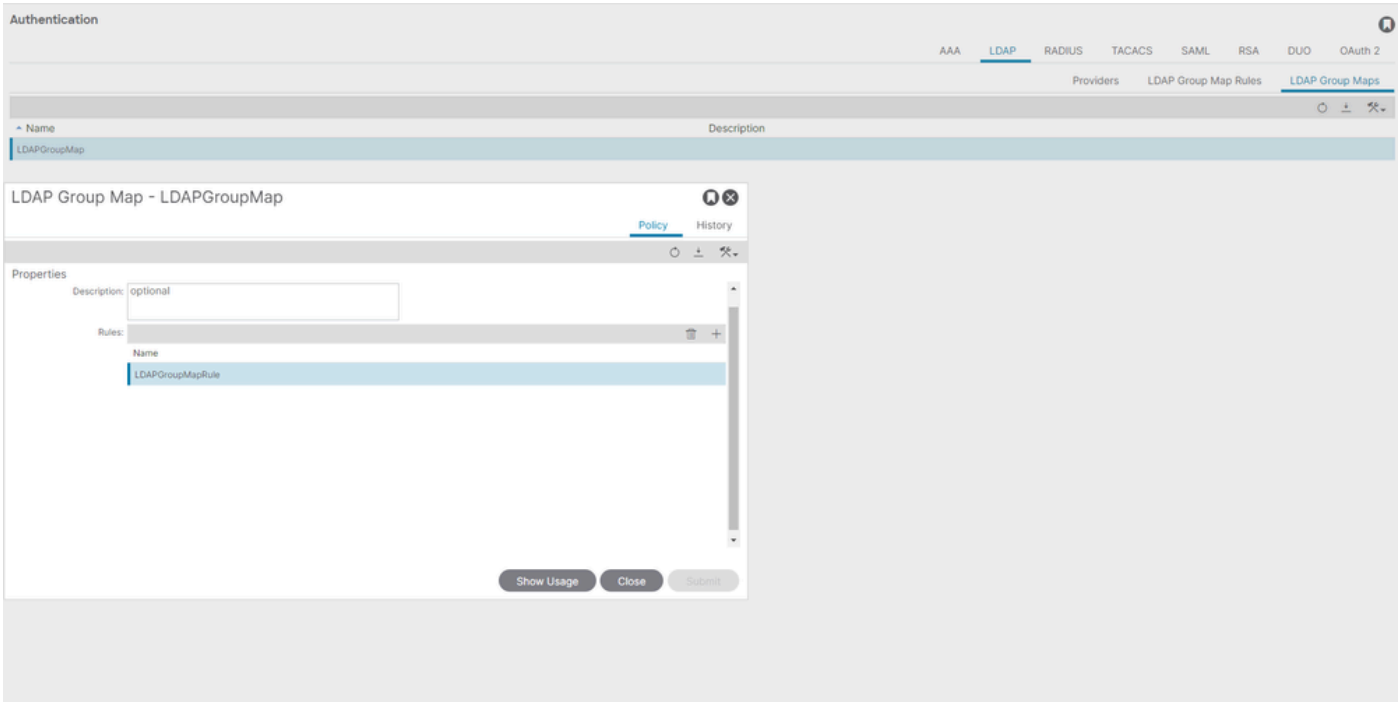
Dans la barre de menus, accédez à Admin > AAA > Authentication > LDAP > LDAP Group Map Rules comme indiqué dans l'image.



Les utilisateurs de DCGroup disposent de privilèges d'administrateur. Par conséquent, le DN du groupe cn=DCGroup, ou=Groups, dc=dclab, dc=com. Aattribue le domaine de sécurité à All et alloue les rôles de admin avec write privilege .

Étape 4. Configurer les mappages de groupe LDAP

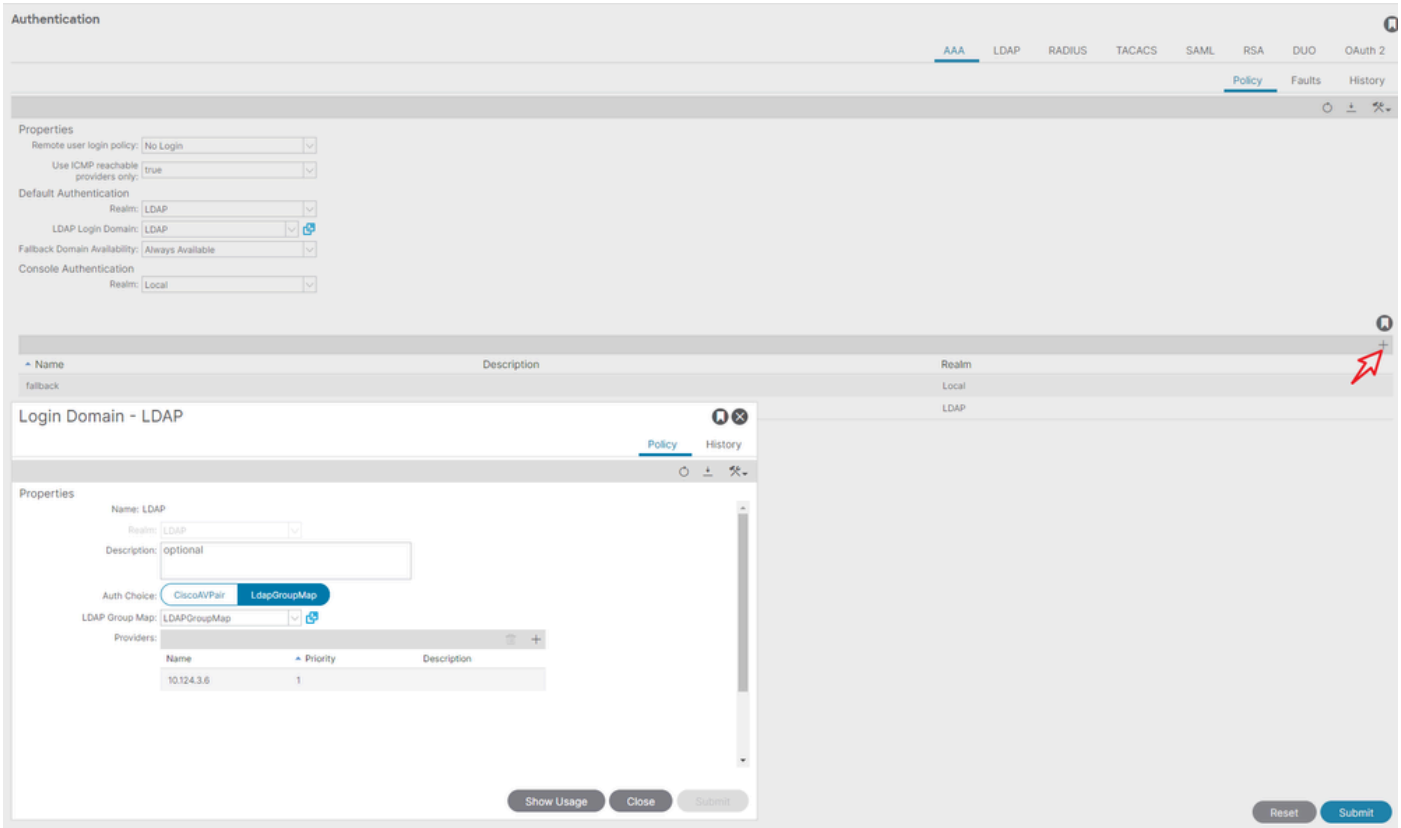
Dans la barre de menus, accédez à Admin > AAA > Authentication > LDAP > LDAP Group Maps comme indiqué dans l'image.



Créez un mappage de groupe LDAP contenant les règles de mappage de groupe LDAP créées à l'étape 2.

Étape 5. Configurer la stratégie d'authentification AAA

Dans la barre de menus, accédez à Admin > AAA > Authentication > AAA > Policy > Create a login domaincomme indiqué dans l'image.

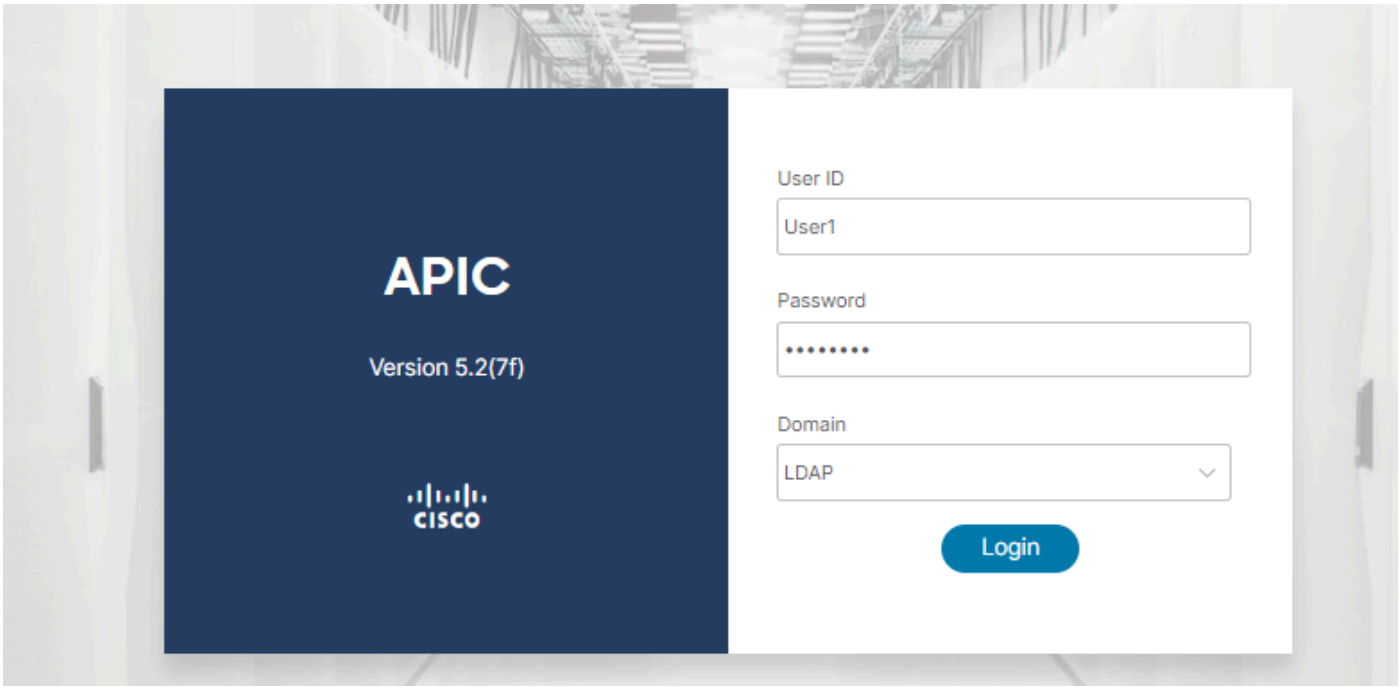


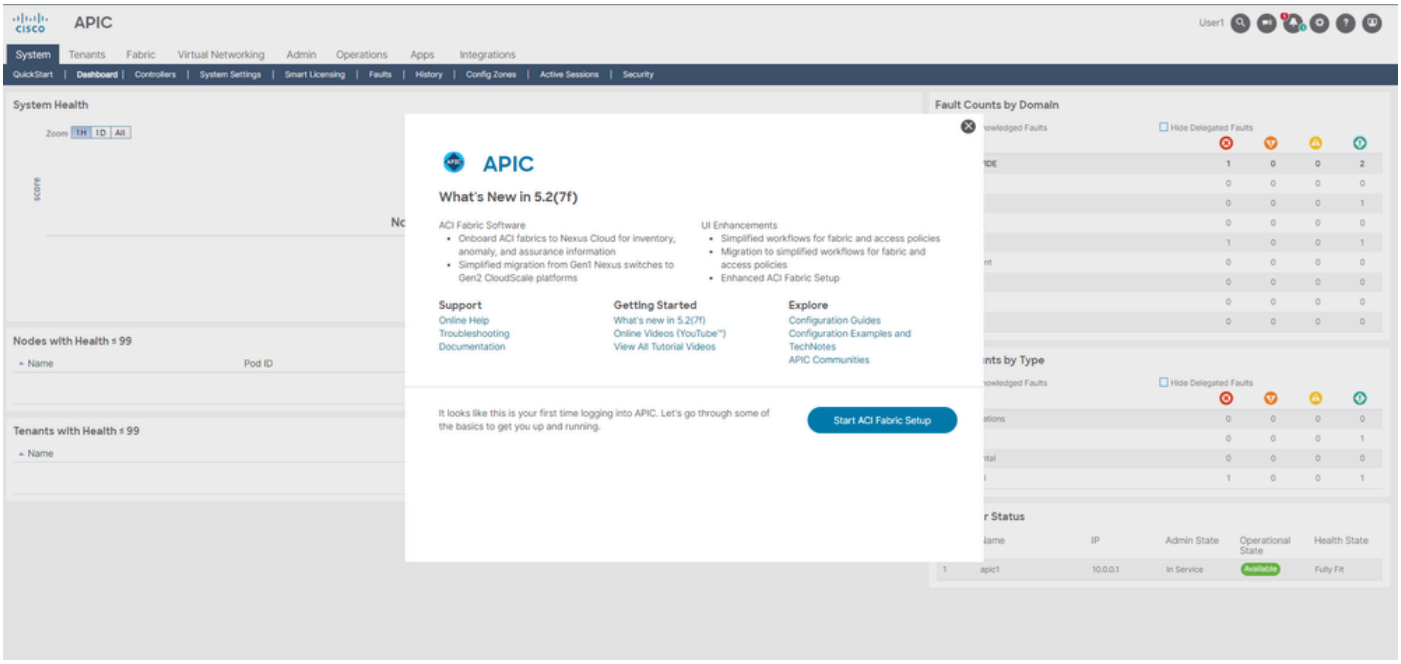
Dans la barre de menus, accédez à Admin > AAA > Authentication > AAA > Policy > Default Authentication comme indiqué dans l'image.

Remplacez l'authentification par défaut Realm par LDAP et sélectionnez LDAP Login Domain créé.

Vérifier

Utilisez cette section pour confirmer que votre configuration fonctionne correctement.



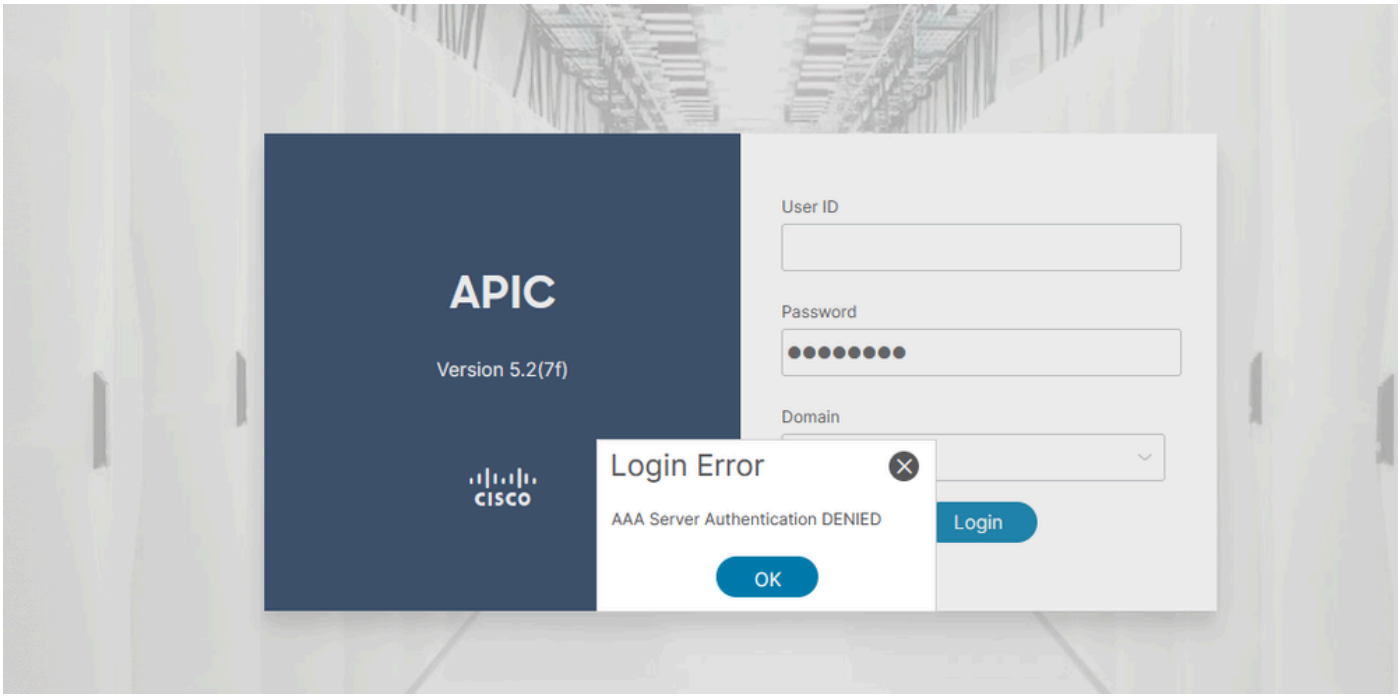


Vérifiez que l'utilisateur LDAP se connecteUser1 au contrôleur APIC avec le rôle admin et le privilège d'écriture.

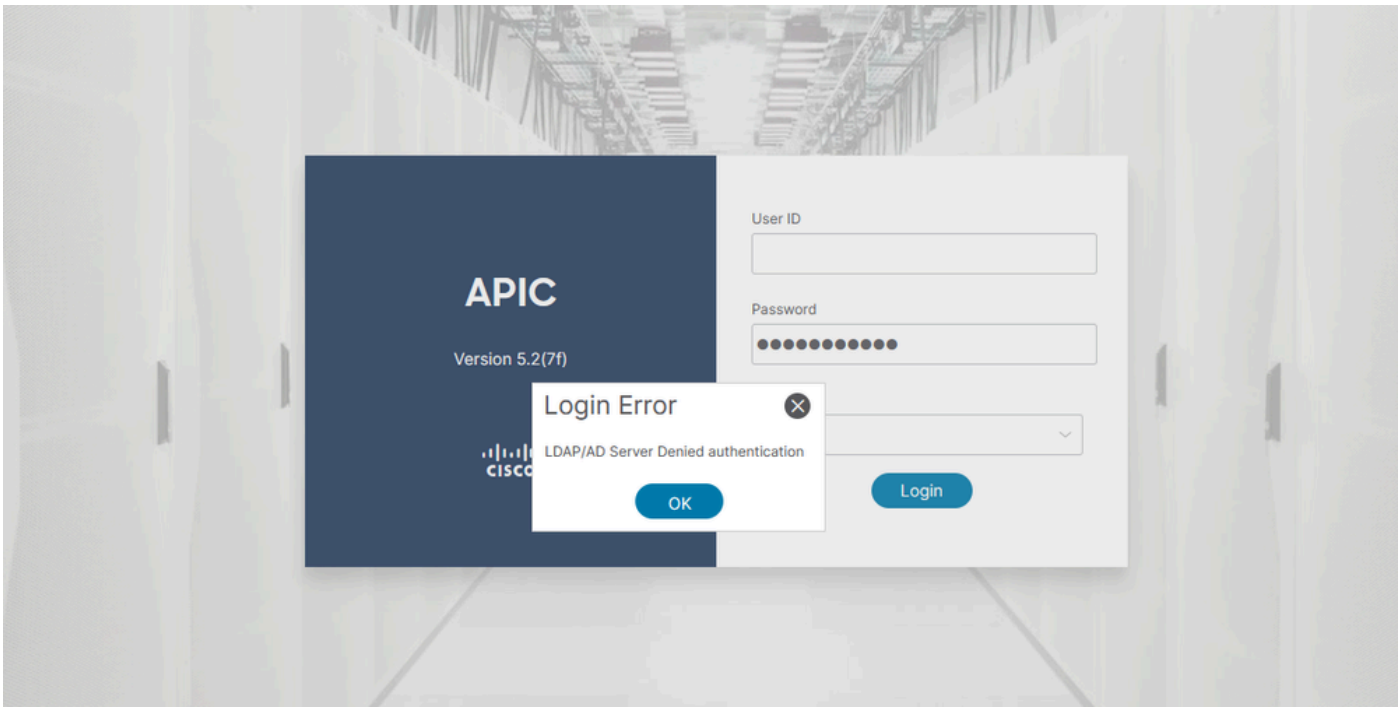
Dépannage

Cette section fournit des informations que vous pouvez utiliser pour dépanner votre configuration.

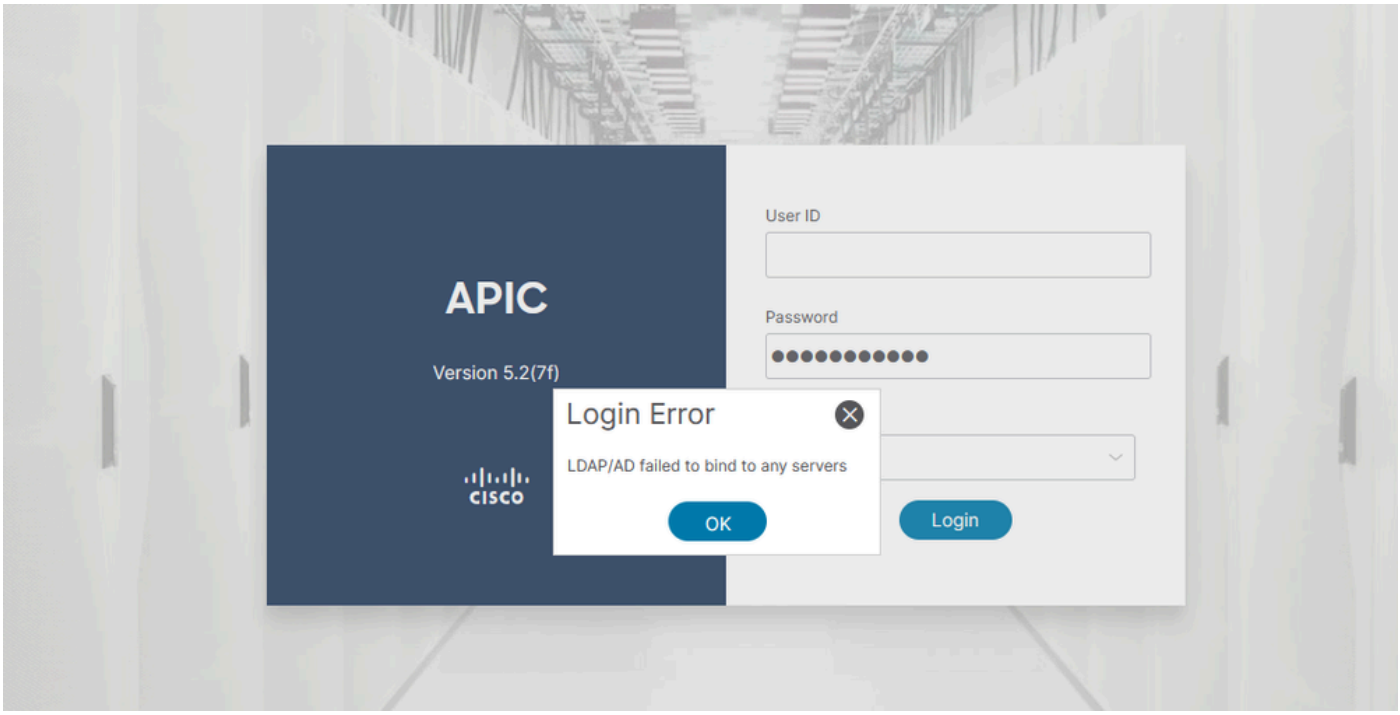
Lorsque l'utilisateur n'existe pas dans la base de données LDAP :



Lorsque le mot de passe est incorrect :



Lorsque le serveur LDAP est inaccessible :



Dépannage des commandes:

<#root>

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

Si vous avez besoin d'aide, contactez le TAC Cisco.

Informations connexes

- Guide de configuration de la sécurité Cisco APIC, version 5.2(x)
- Assistance technique de Cisco et téléchargements

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.