Konfigurieren Sie die ACI-LDAP-Authentifizierung

Inhalt

Einleitung

In diesem Dokument wird die Konfiguration der ACI-Authentifizierung (Application Centric Infrastructure) und LDAP-Authentifizierung (Lightweight Directory Access Protocol) beschrieben.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- ACI-AAA-Richtlinie (Authentication, Authorization und Accounting)
- LDAP

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

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

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten

Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

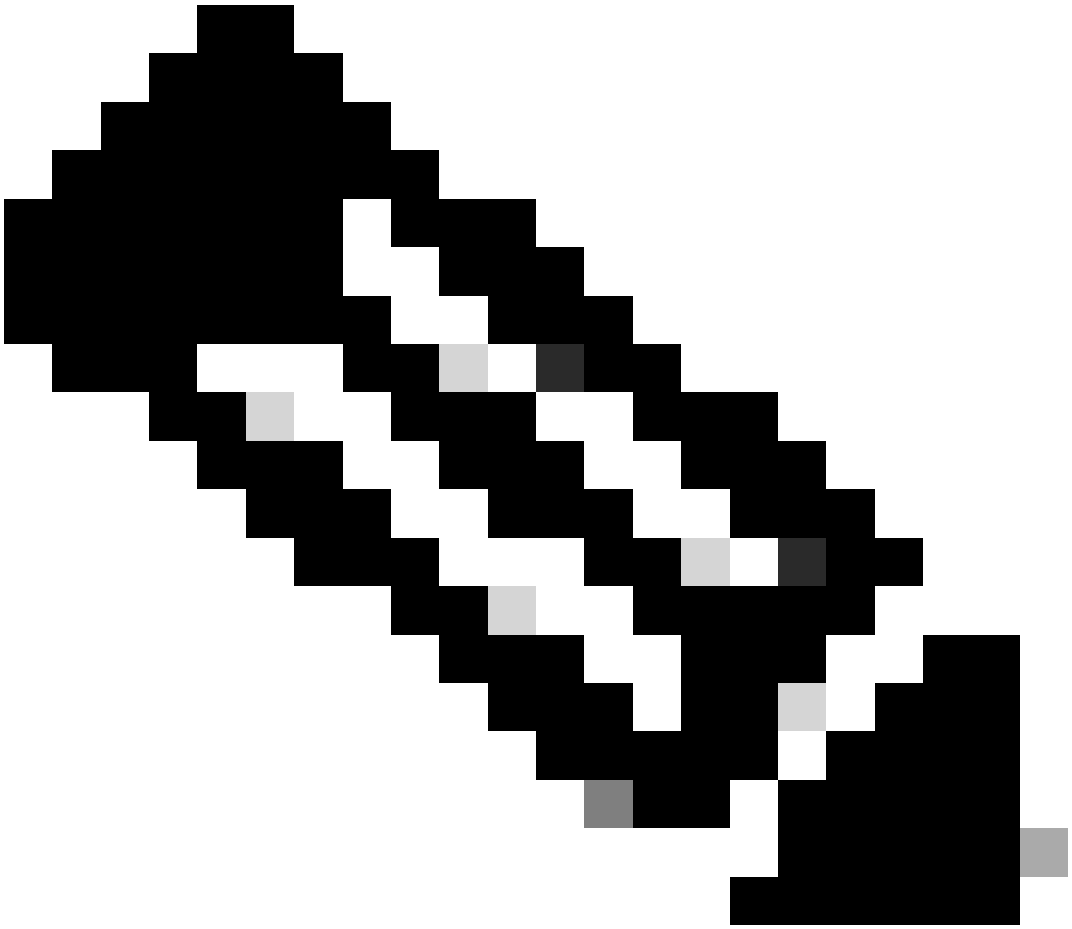
Konfigurieren

In diesem Abschnitt wird beschrieben, wie Sie den APIC konfigurieren, um ihn in den LDAP-Server zu integrieren und LDAP als Standardauthentifizierungsmethode zu verwenden.

Konfigurationen

Schritt 1: Erstellen von Gruppen/Benutzern unter Ubuntu phpLDAPadmin

---

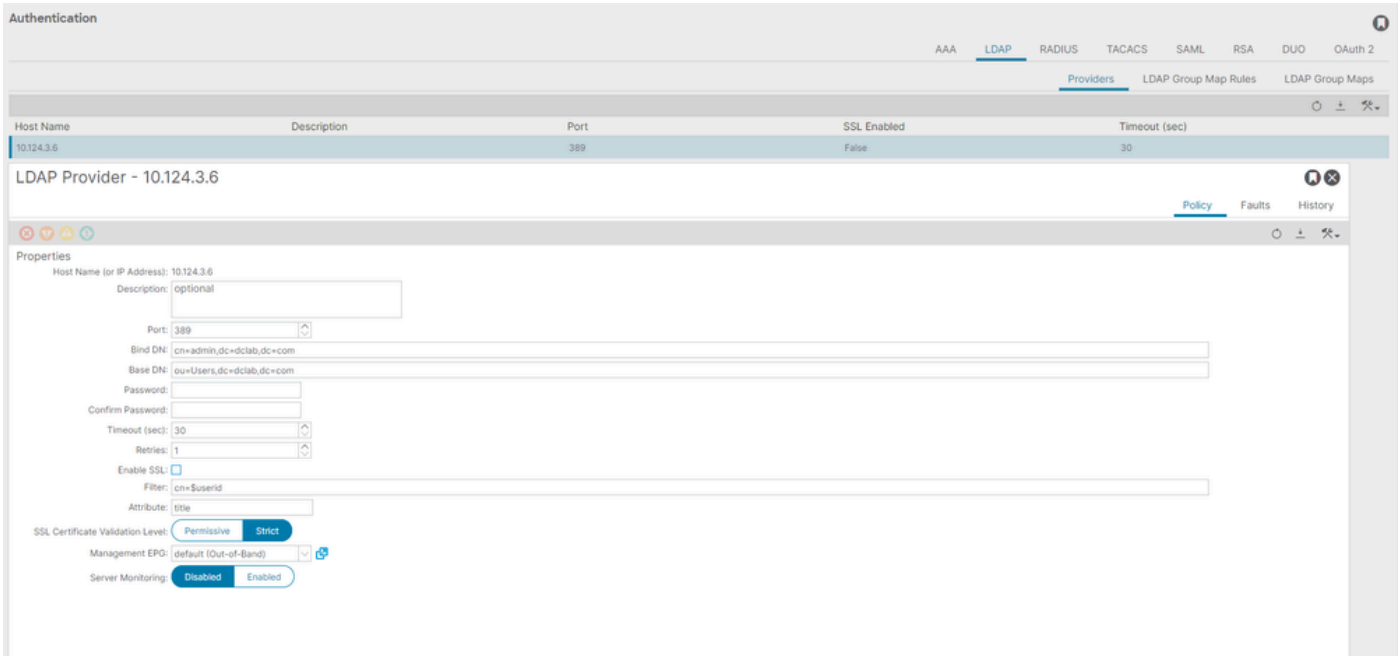


> Hinweis: Um Ubuntu als LDAP-Server zu konfigurieren, finden Sie umfassende Richtlinien auf der offiziellen Ubuntu-Website. Wenn bereits ein LDAP-Server vorhanden ist, beginnen Sie mit Schritt 2.

In diesem Dokument ist die Basis-DN gleich, dc=dclab,dc=com und zwei Benutzer (User1 und User2) gehören zu Gruppen (DCGroup).

Schritt 2: LDAP-Anbieter auf dem APIC konfigurieren

Navigieren Sie in der APIC-Menüleiste wie im Bild dargestellt zuAdmin > AAA > Authentication > LDAP > Providers.



Bind-DN: Die Bind-DN sind die Anmeldeinformationen, die Sie für die Authentifizierung gegenüber einem LDAP verwenden. Der APIC authentifiziert sich mithilfe dieses Kontos, um das Verzeichnis abzufragen.

Basis-DN: Diese Zeichenfolge wird vom APIC als Bezugspunkt für die Suche und Identifizierung von Benutzereinträgen im Verzeichnis verwendet.

Kennwort: Dies ist das erforderliche Kennwort für die Bind-DN, die für den Zugriff auf den LDAP-Server erforderlich ist und mit dem auf Ihrem LDAP-Server eingerichteten Kennwort korreliert.

SSL aktivieren: Wenn Sie eine interne Zertifizierungsstelle oder ein selbstsigniertes Zertifikat verwenden, müssen Sie **Zulässig** auswählen.

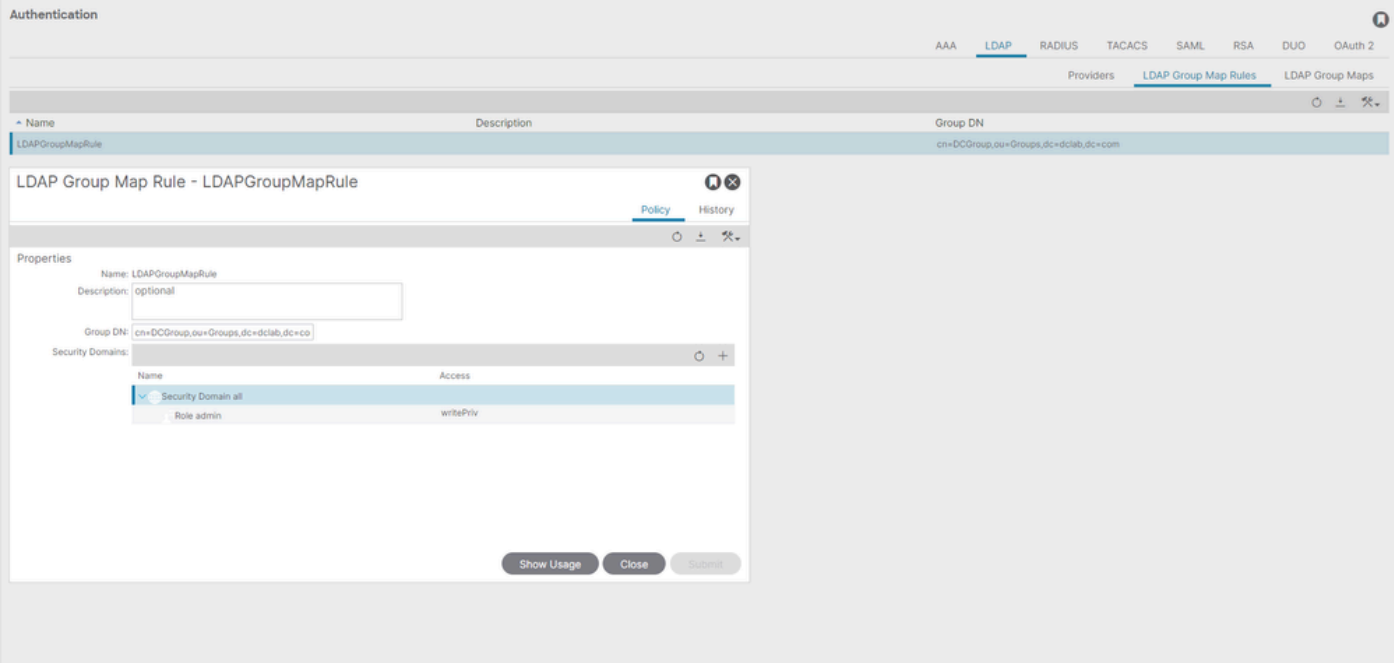
Filter: Die Standardfiltereinstellung ist, cn=$userid wenn der Benutzer als Objekt mit einem gemeinsamen Namen (CN) definiert ist, wird der Filter verwendet, um nach den Objekten innerhalb der Basis-DN zu suchen.

Attribut: Ein Attribut wird verwendet, um die Gruppenmitgliedschaft und die Gruppenrollen zu bestimmen. Die ACI bietet hier zwei Optionen: memberOf und CiscoAVPair.memberOf ist ein RFC2307bis-Attribut zur Identifizierung der Gruppenmitgliedschaft. Derzeit überprüft OpenLDAP RFC2307, title wird also stattdessen verwendet.

Management-Endpunktgruppe (EPG): Die Verbindung zum LDAP-Server wird je nach gewähltem Netzwerkmanagement-Ansatz entweder über die In-Band- oder die Out-of-Band-EPG hergestellt.

Schritt 3: LDAP-Gruppenzuordnungsregeln konfigurieren

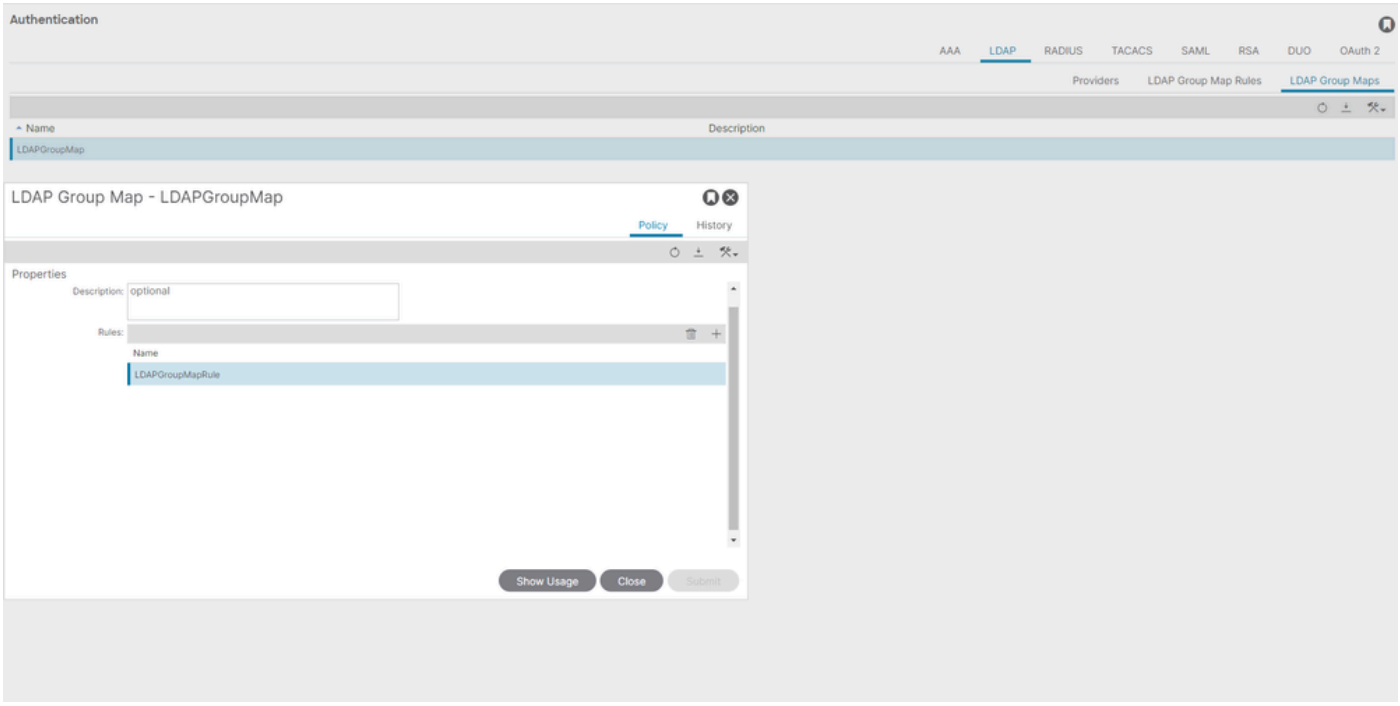
Navigieren Sie in der Menüleiste zu, Admin > AAA > Authentication > LDAP > LDAP Group Map Rules wie im Bild dargestellt.



Benutzer in der DCGroup haben Administratorrechte. Aus diesem Grund weist die Gruppen-DN der Sicherheitsdomäne zu, cn=DCGroup, ou=Groups, dc=dclab, dc=com. Aund weist dieser All die Rollen von admin mit write privilege zu.

Schritt 4: LDAP-Gruppenzuordnungen konfigurieren

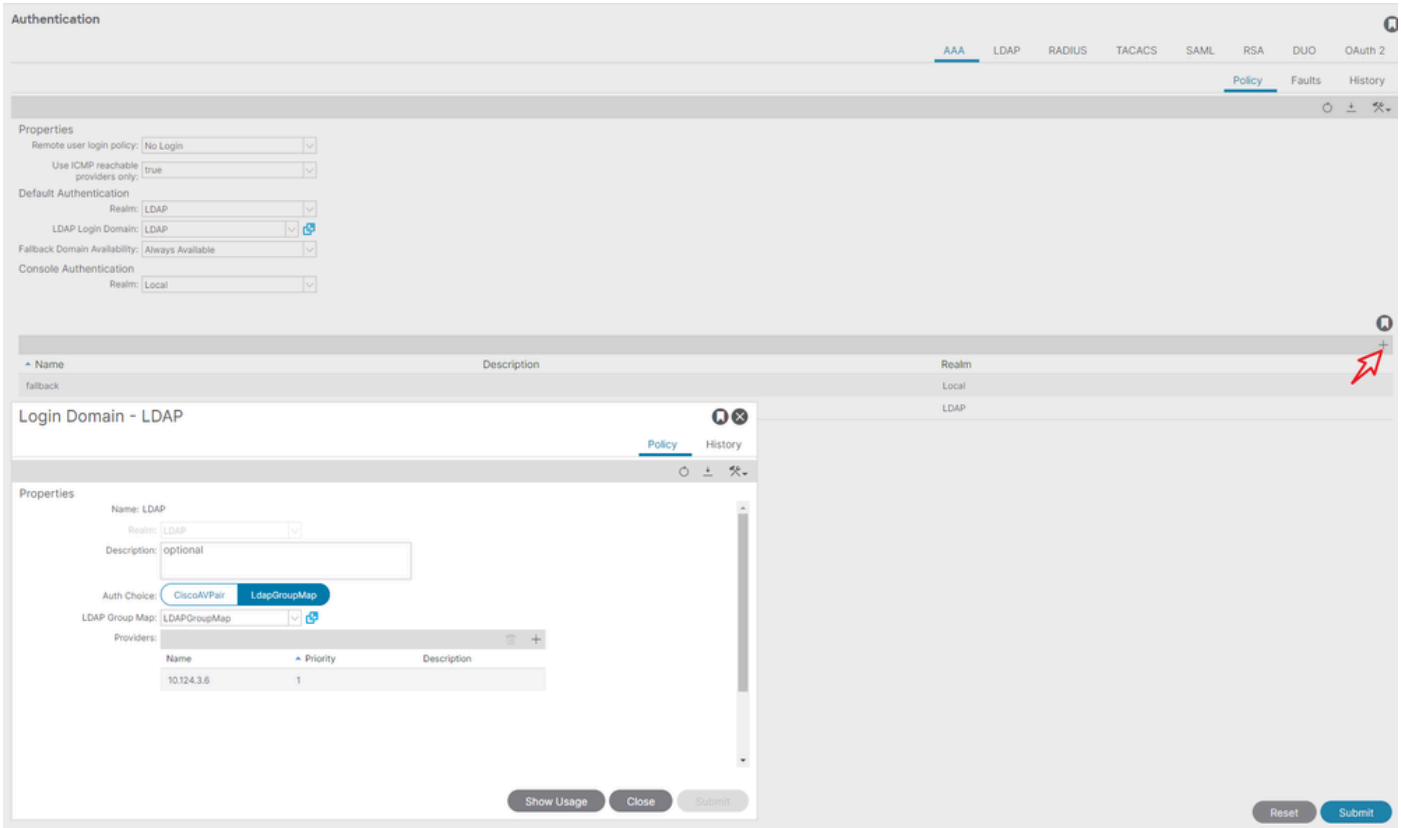
Navigieren Sie in der Menüleiste zu, Admin > AAA > Authentication > LDAP > LDAP Group Maps wie im Bild dargestellt.



Erstellen Sie eine LDAP-Gruppenzuordnung mit den in Schritt 2 erstellten LDAP-Gruppenzuordnungsregeln.

Schritt 5: AAA-Authentifizierungsrichtlinie konfigurieren

Navigieren Sie in der Menüleiste zu, Admin > AAA > Authentication > AAA > Policy > Create a login domainwie im Bild dargestellt.

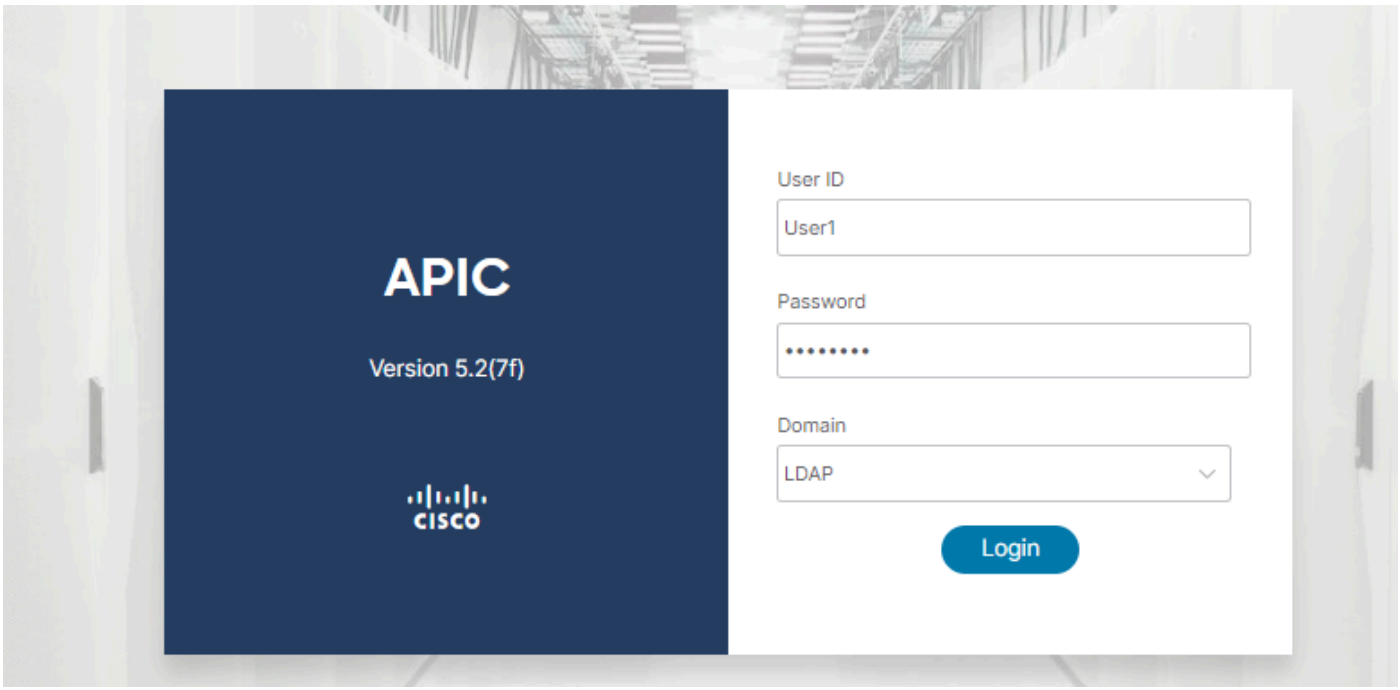


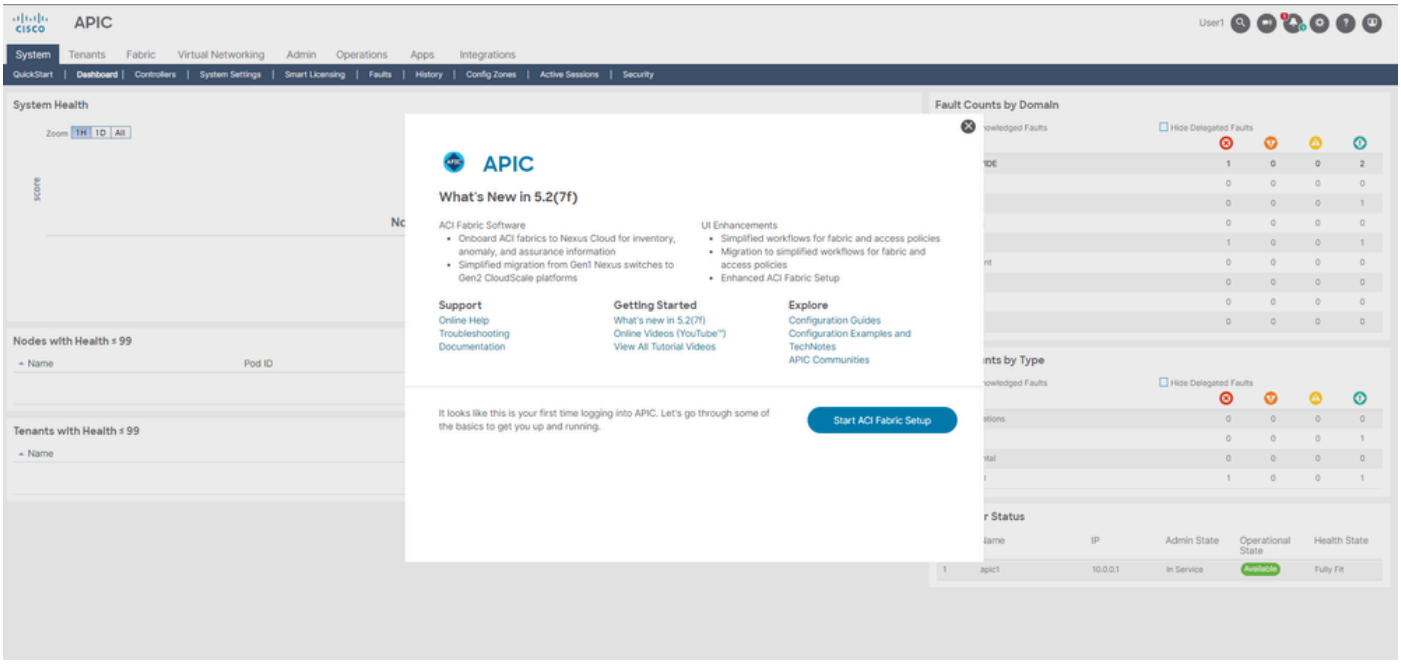
Navigieren Sie in der Menüleiste zu, Admin > AAA > Authentication > AAA > Policy > Default Authentication wie im Bild dargestellt.

Ändern Sie die Standardauthentifizierung Realm in LDAP, und wählen Sie LDAP Login Domain erstellt aus.

Überprüfung

Verwenden Sie diesen Abschnitt, um zu überprüfen, ob Ihre Konfiguration ordnungsgemäß funktioniert.



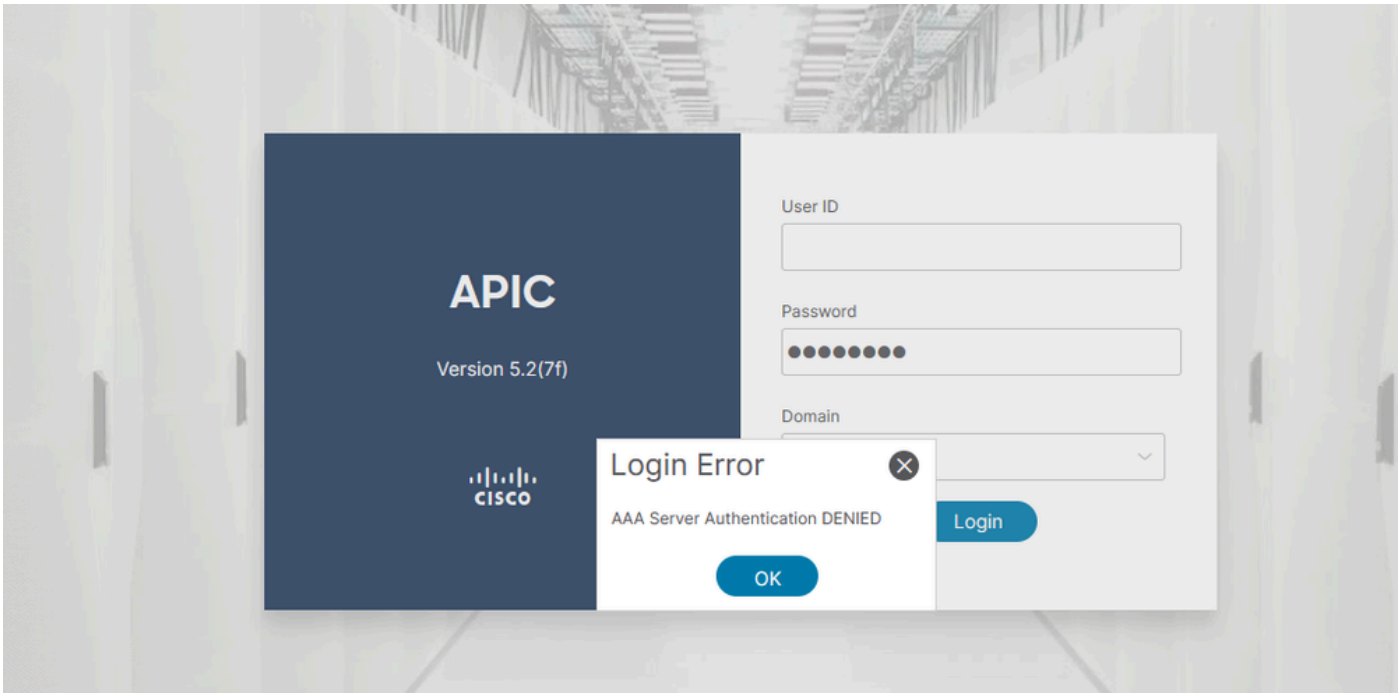


Vergewissern Sie sich, dass sich der LDAP-Benutzer User1 erfolgreich mit der Admin-Rolle und den Schreibberechtigungen im APIC anmeldet.

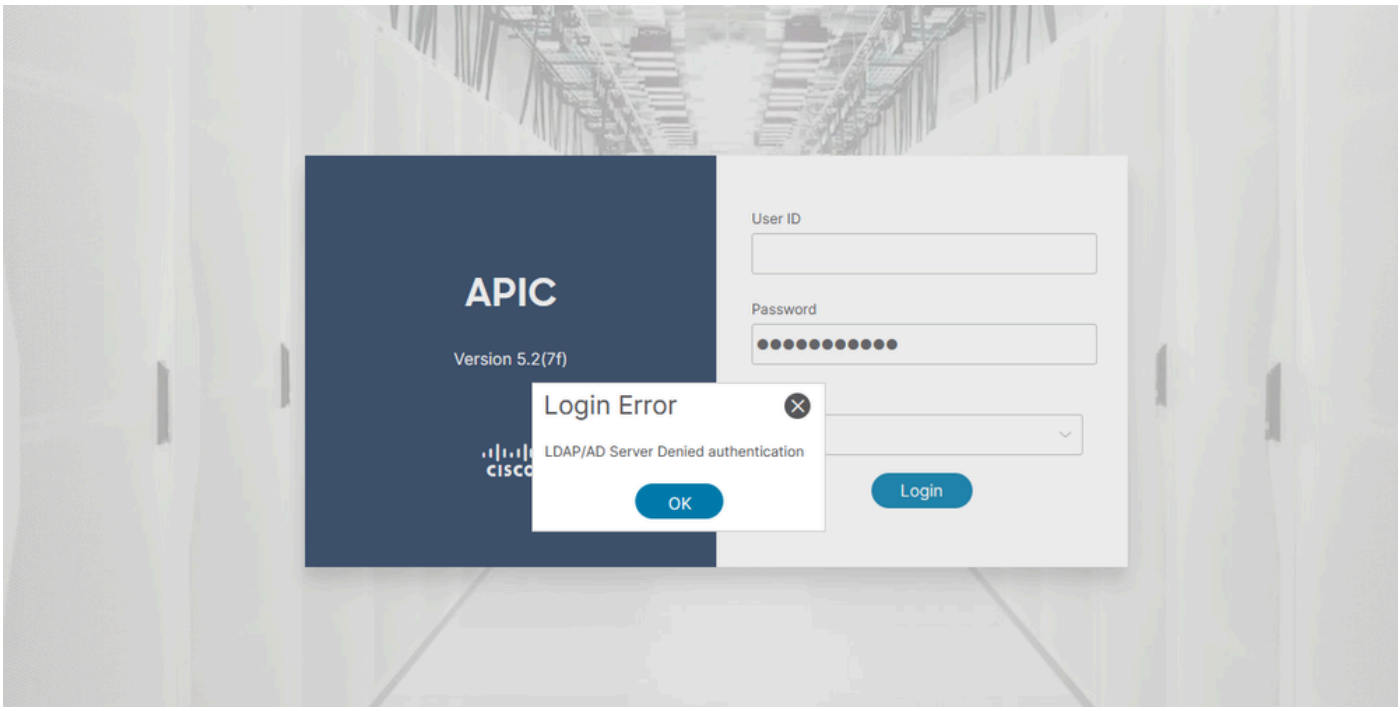
Fehlerbehebung

In diesem Abschnitt erhalten Sie Informationen zur Behebung von Fehlern in Ihrer Konfiguration.

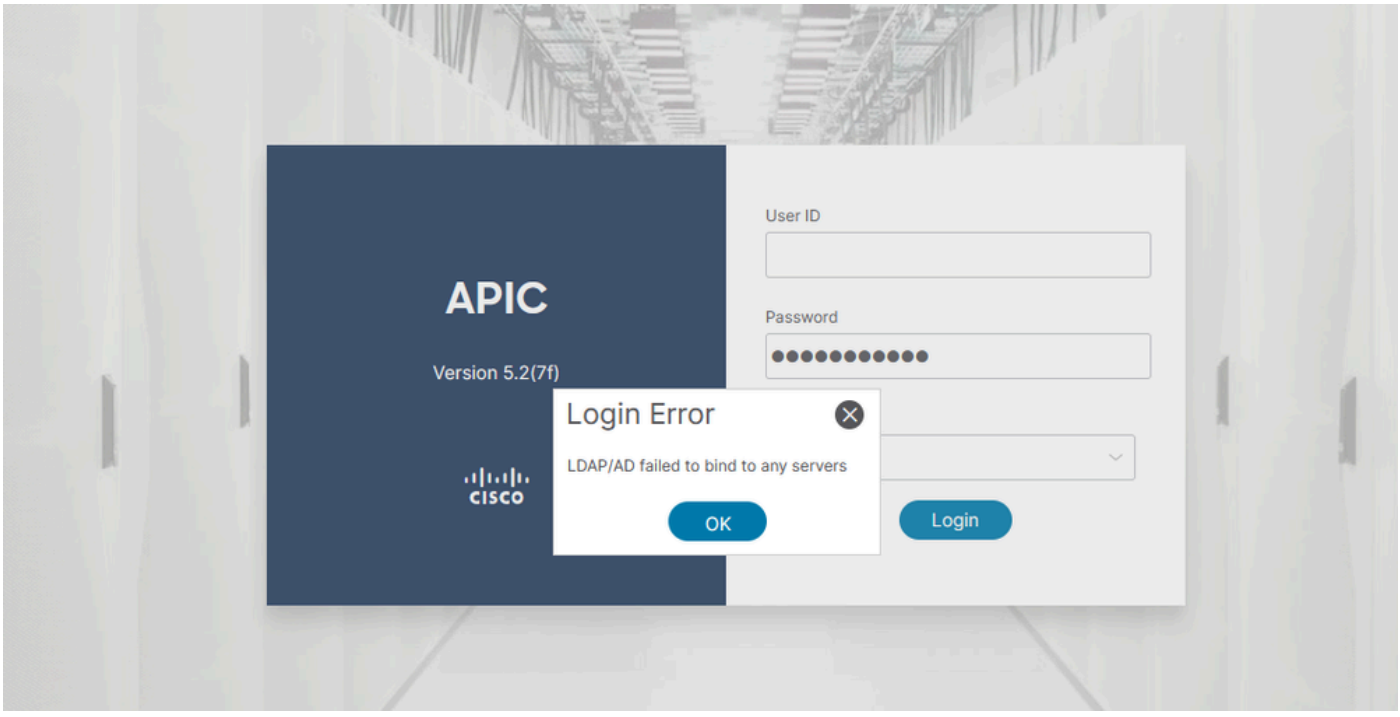
Wenn der Benutzer nicht in der LDAP-Datenbank vorhanden ist:



Wenn das Kennwort falsch ist:



Wenn der LDAP-Server nicht erreichbar ist:



Befehle für die Fehlerbehebung:

<#root>

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

Wenn Sie weitere Unterstützung benötigen, wenden Sie sich an das Cisco TAC.

Zugehörige Informationen

- Cisco APIC Security Konfigurationsleitfaden, Version 5.2(x)
- Technischer Support und Downloads von Cisco

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.