ACI LDAP認証の設定

内容

はじめに

前提条件

- 要件
- 使用するコンポーネント

設定

- コンフィギュレーション
  - ステップ 1：Ubuntu phpLDAPadminでのグループ/ユーザの作成
  - ステップ 2：APICでのLDAPプロバイダーの設定
  - ステップ 3：LDAPグループマップルールの設定
  - ステップ 4：LDAPグループマップの設定
  - ステップ 5：AAA認証ポリシーの設定

確認

トラブルシュート

関連情報

はじめに

このドキュメントでは、アプリケーションセントリックインフラストラクチャ(ACI)のLightweight Directory Access Protocol(LDAP)認証を設定する方法について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- ACI認証、許可、アカウンティング(AAA)ポリシー
- [LDAP]

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Cisco Application Policy Infrastructure Controller(APIC)バージョン5.2(7f)
- Ubuntu 20.04とslapdおよびphpLDAPadmin

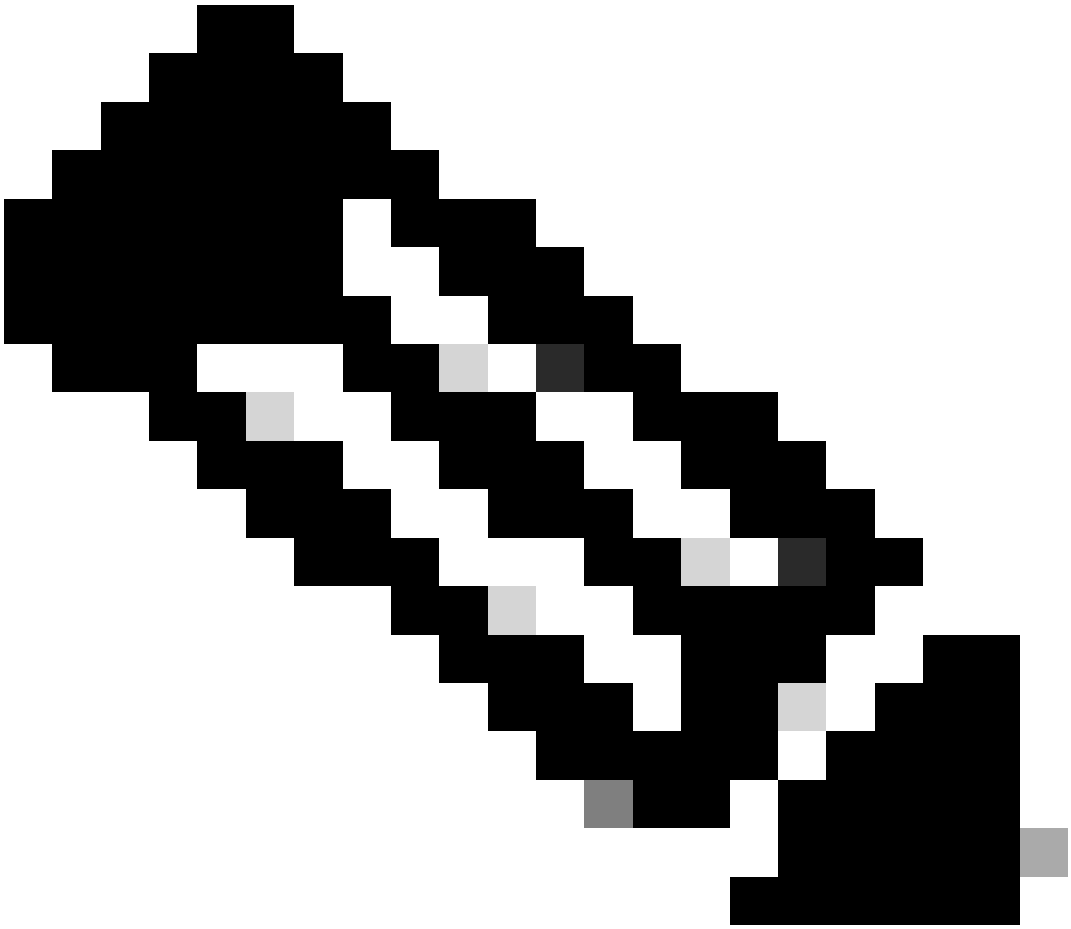
このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

設定

このセクションでは、LDAPサーバと統合し、LDAPをデフォルトの認証方式として使用するようにAPICを設定する方法について説明します。

コンフィギュレーション

ステップ 1：Ubuntu phpLDAPadminでのグループ/ユーザの作成

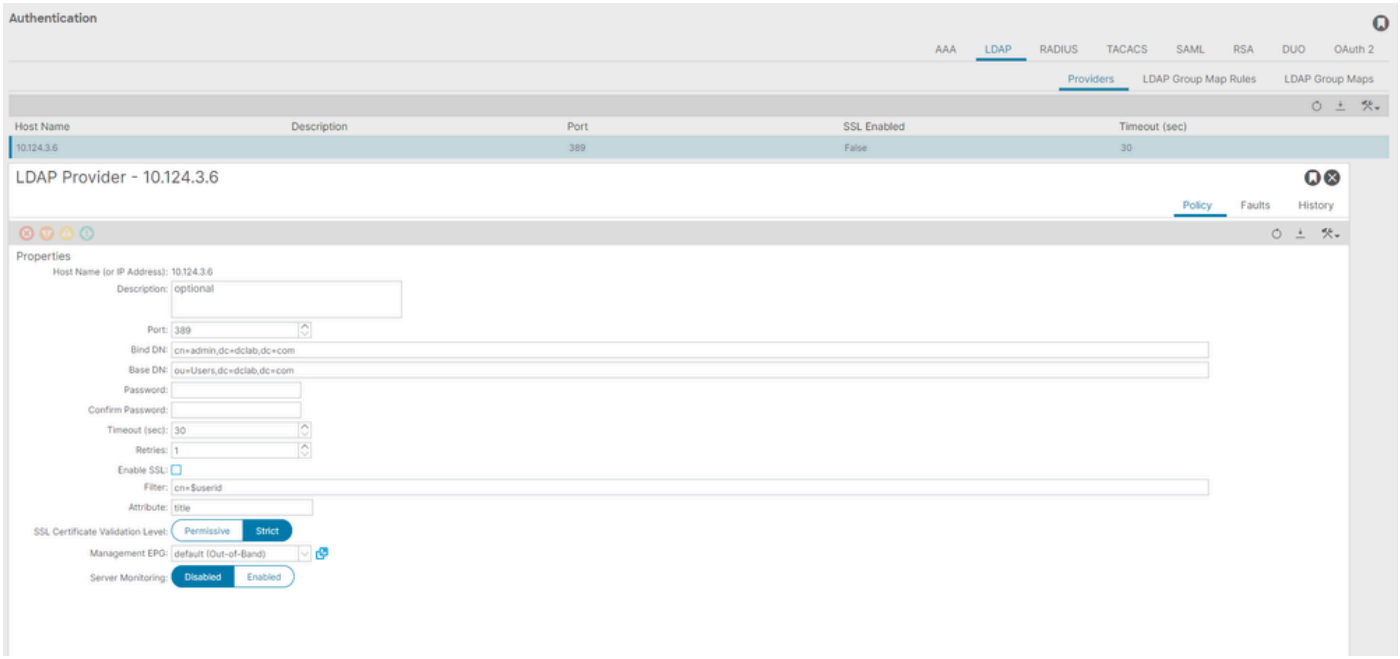


> 注:UbuntuをLDAPサーバとして設定するには、Ubuntuの公式Webサイトで包括的なガイドラインを参照してください。既存のLDAPサーバがある場合は、ステップ2から始めます。

このドキュメントでは、ベースDNはdc=dclab,dc=comで、2人のユーザ（User1とUser2）はグループ(DCGroup)に属しています。

ステップ 2：APICでのLDAPプロバイダーの設定

APICメニューバーで、図に示すようにAdmin > AAA > Authentication > LDAP > Providersに移動します。



バインドDN：バインドDNは、LDAPに対して認証するために使用するクレデンシャルです。APICは、このアカウントを使用してディレクトリを照会することで認証を行います。

ベースDN：この文字列は、ディレクトリ内のユーザエントリを検索および識別するためのリファレンスポイントとしてAPICに採用されます。

パスワード：これは、LDAPサーバにアクセスするために必要なバインドDNの必須パスワードであり、LDAPサーバに設定されたパスワードと関連付けられます。

SSLの有効化：内部CAまたは自己署名証明書を使用する場合は、**Permissive**を選択する必要があります。

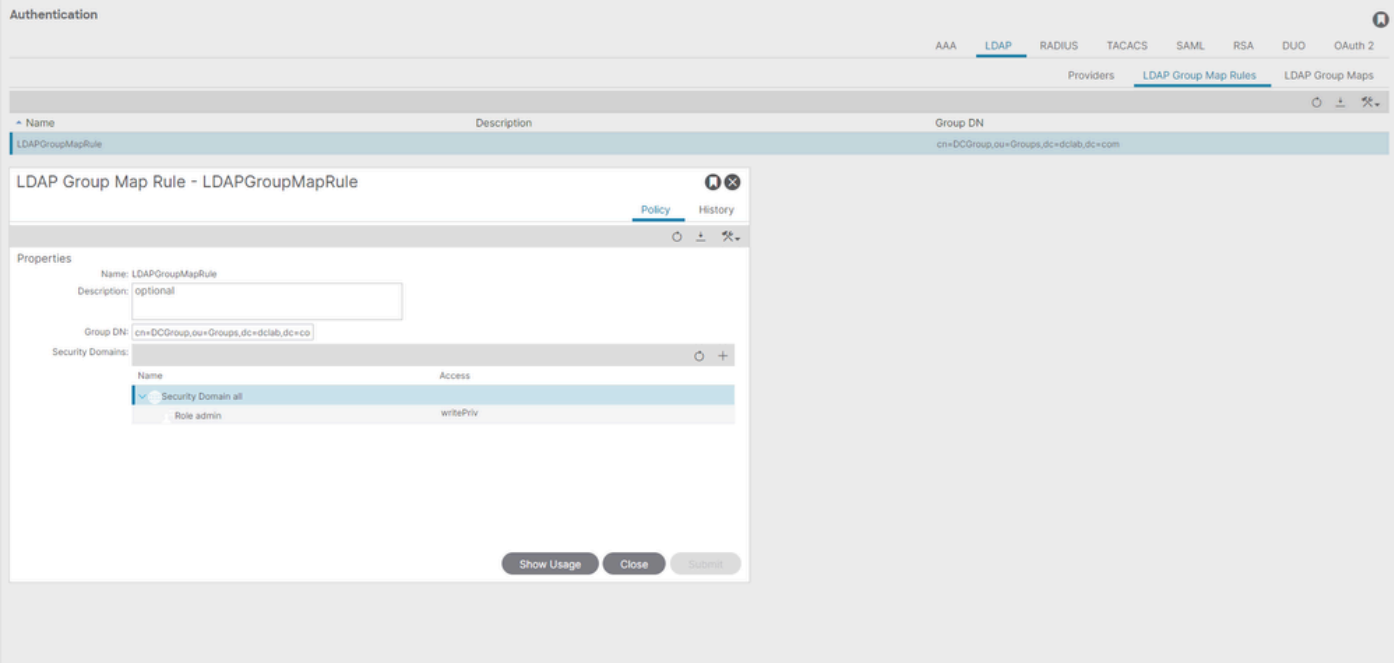
Filter:デフォルトのフィルタ設定はcn=$userid、ユーザが共通名(CN)を持つオブジェクトとして定義されている場合に、ベースDN内のオブジェクトを検索するために使用されます。

属性：属性は、グループメンバーシップとロールを決定するために使用されます。ここでは、ACIに2つのオプションが用意されています。memberOfおよびCiscoAVPair.memberOf は、グループメンバーシップを識別するためのRFC2307bis属性です。現在、OpenLDAPはRFC2307をチェックするため、代わりにtitle が使用されます。

管理エンドポイントグループ(EPG):LDAPサーバへの接続は、選択されたネットワーク管理アプローチに応じて、インバンドまたはアウトオブバンドのEPGを介して実現されます。

ステップ 3：LDAPグループマップルールの設定

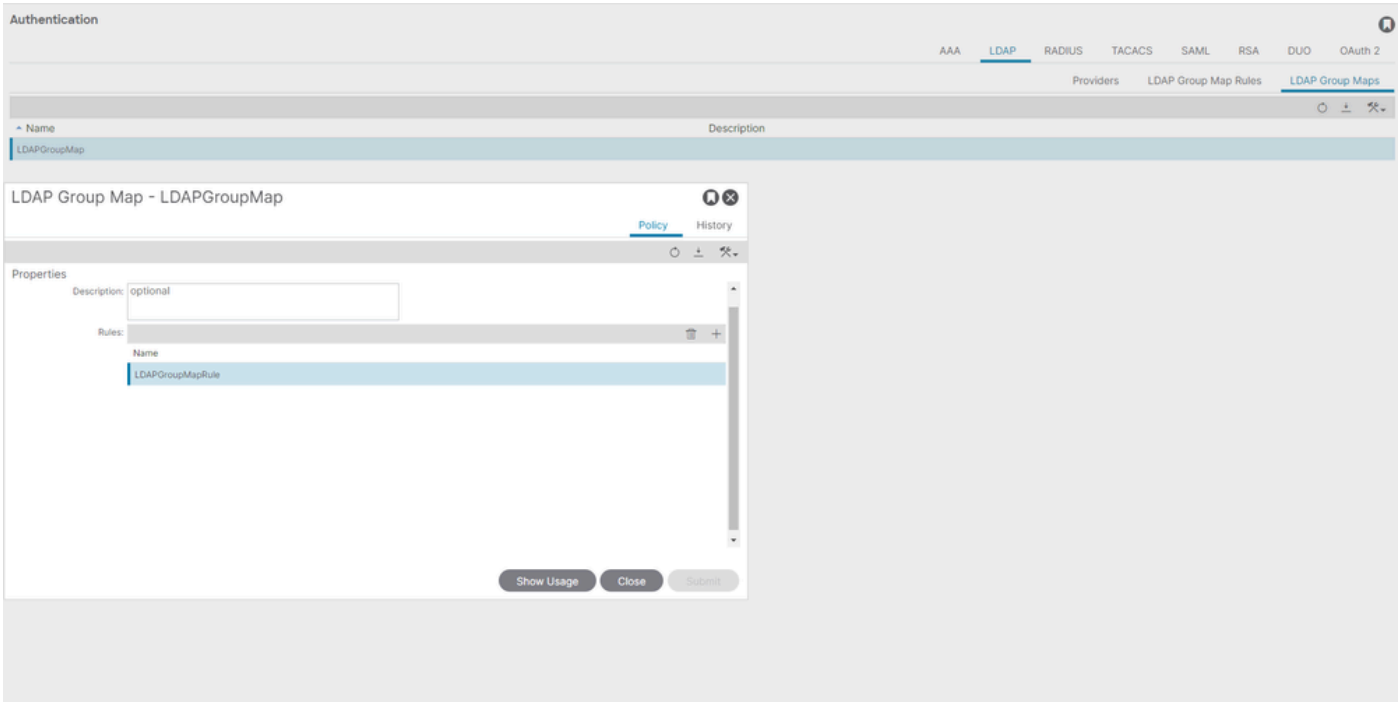
メニューバーで、図に示すようにAdmin > AAA > Authentication > LDAP > LDAP Group Map Rules に移動します。



DCGroup内のユーザーは管理者権限を持ちます。したがって、グループDNはセキュリティドメインをcn=DCGroup, ou=Groups, dc=dclab, dc=com. A割り当てAll、adminwrite privilegeとの役割を割り当てます。

ステップ 4：LDAPグループマップの設定

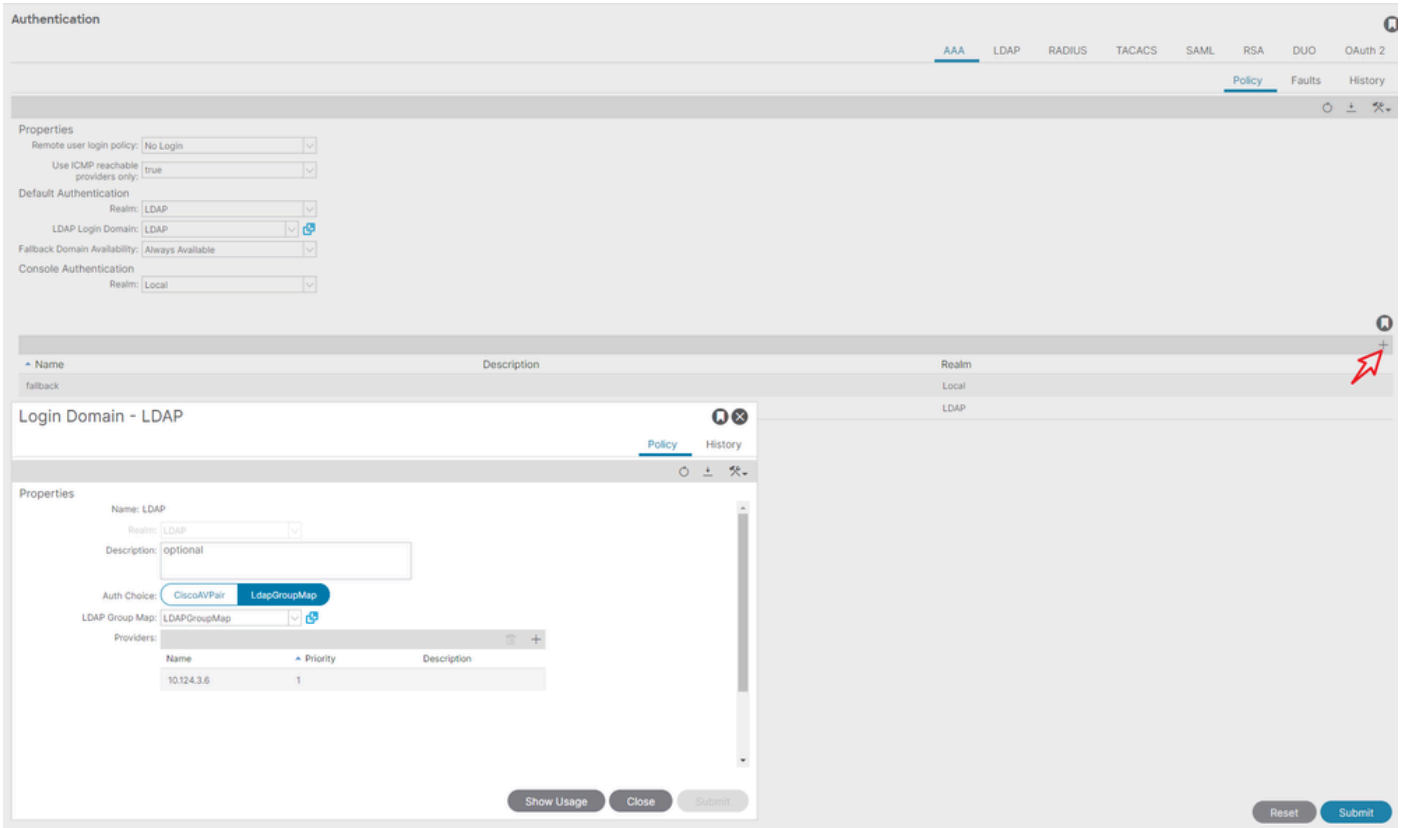
メニューバーで、図に示すようにAdmin > AAA > Authentication > LDAP > LDAP Group Maps に移動します。



ステップ2で作成したLDAPグループマップルールを含むLDAPグループマップを作成します。

ステップ 5：AAA認証ポリシーの設定

メニューバーで、図に示すようにAdmin > AAA > Authentication > AAA > Policy > Create a login domainに移動します。

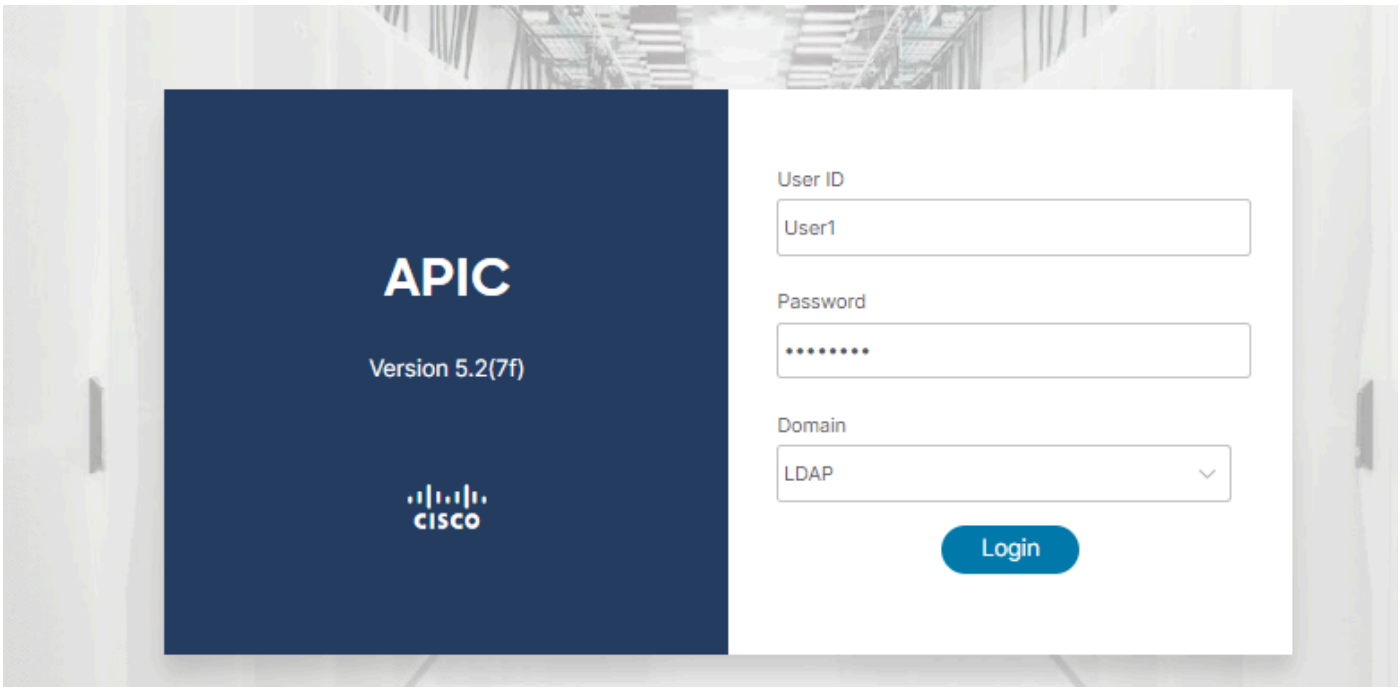


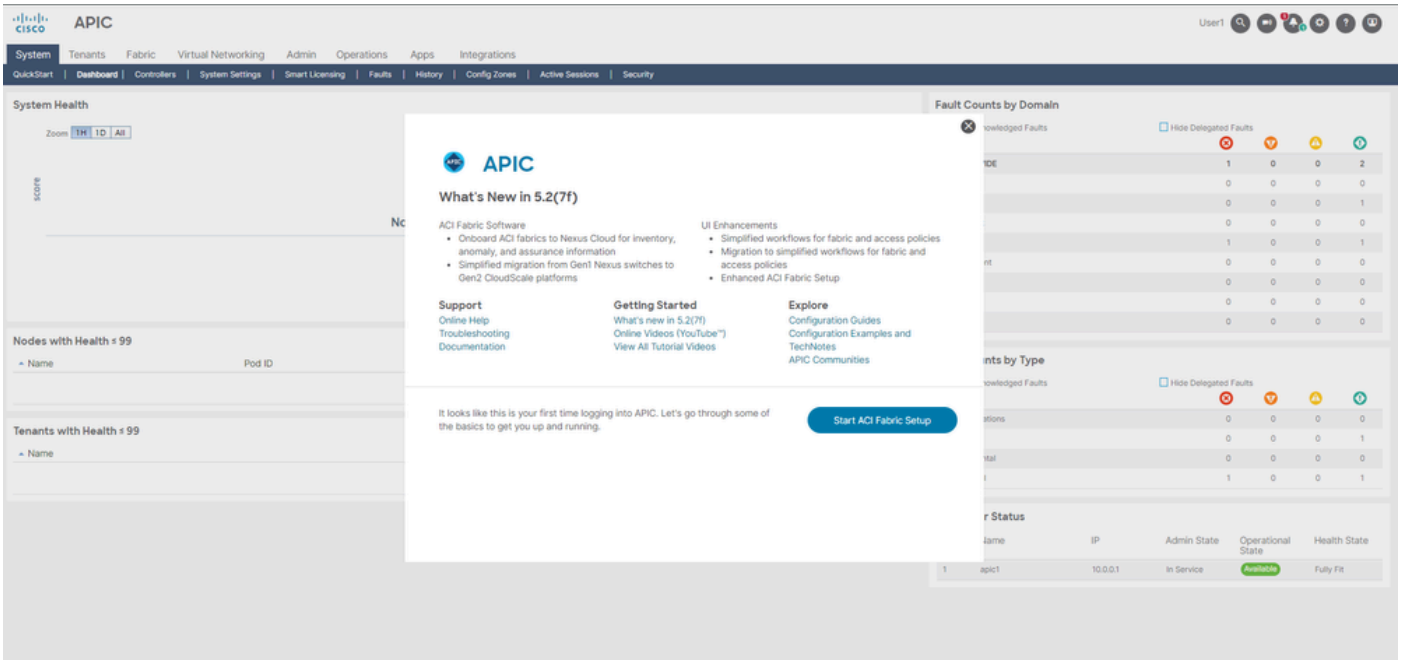
メニューバーで、図に示すようにAdmin > AAA > Authentication > AAA > Policy > Default Authentication に移動します。

デフォルトの認証RealmをLDAPに変更し、「LDAP Login Domain created」を選択します。

確認

ここでは、設定が正常に機能しているかどうかを確認します。



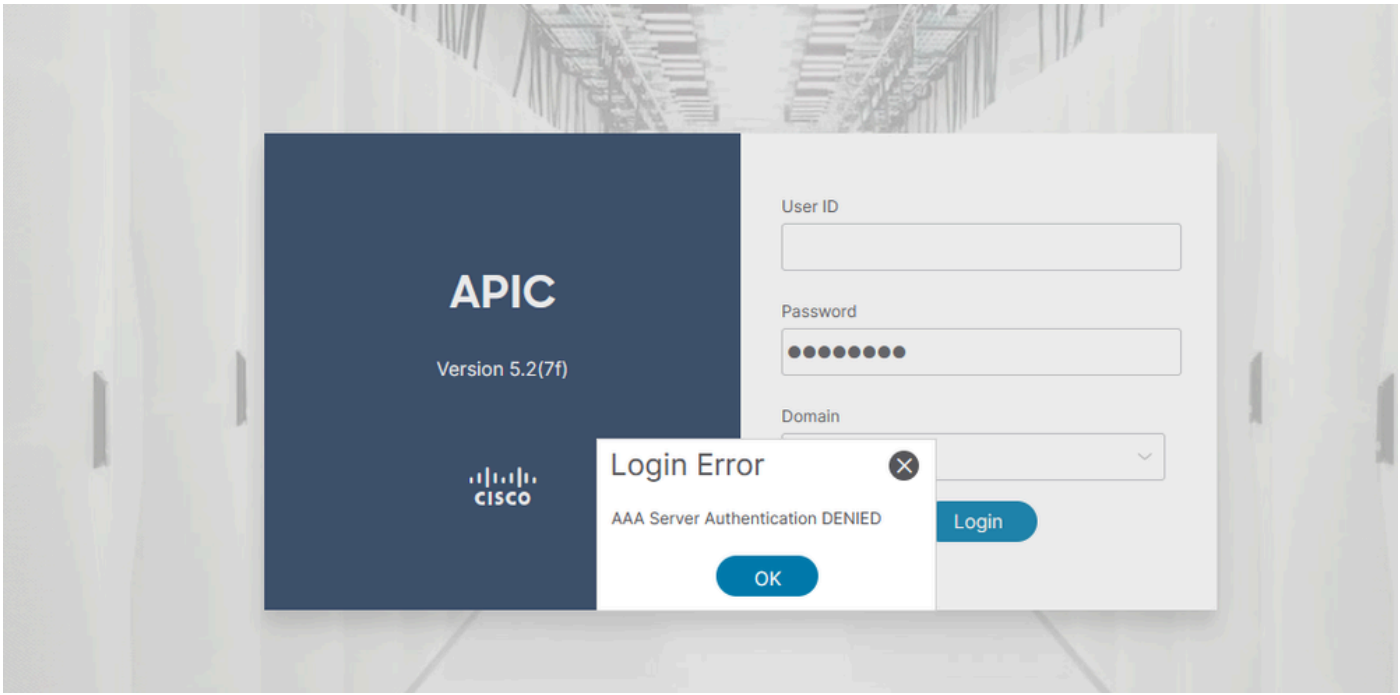


LDAPユーザがUser1、管理者ロールと書き込み権限を使用してAPICに正常にログインできることを確認します。

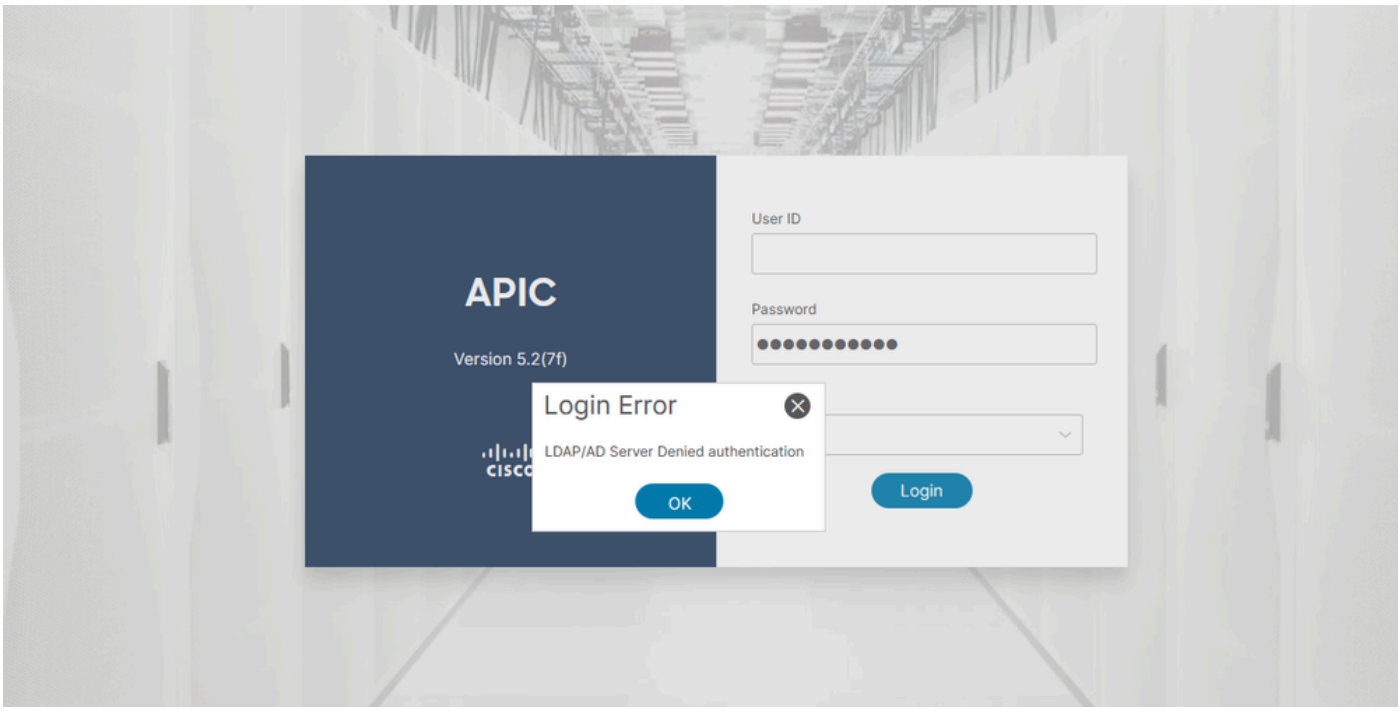
トラブルシュート

ここでは、設定のトラブルシューティングに使用できる情報を示します。

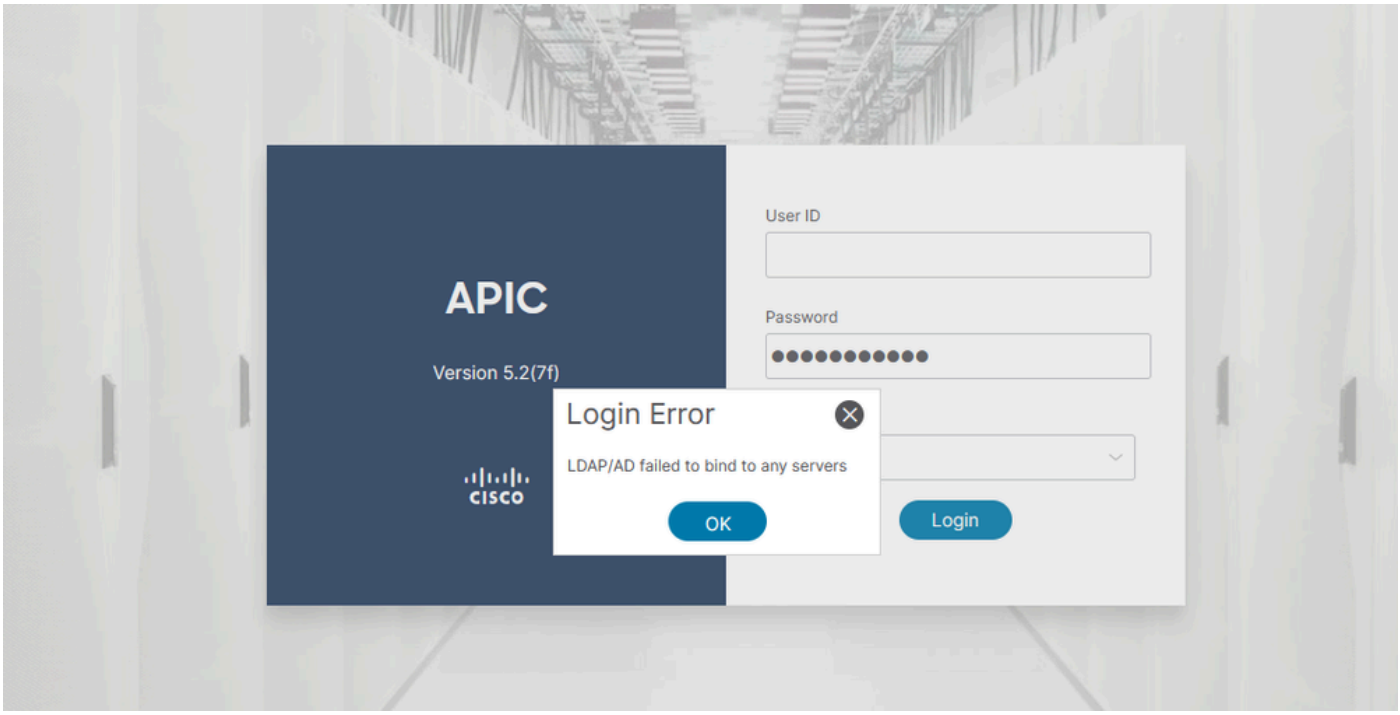
ユーザがLDAPデータベースに存在しない場合：



パスワードが正しくない場合：



LDAPサーバに到達できない場合：



トラブルシューティング コマンド:

<#root>

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

さらにサポートが必要な場合は、Cisco TACまでお問い合わせください。

関連情報

- Cisco APICセキュリティ設定ガイド、リリース5.2(x)
- シスコのテクニカルサポートとダウンロード

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。