Configurar a autenticação LDAP da ACI

Contents

Introdução

Este documento descreve como configurar a autenticação do Lightweight Diretory Access Protocol (LDAP) da Application Centric Infrastructure (ACI).

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Política de AAA (Authentication, Authorization, and Accounting) da ACI
- LDAP

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Cisco Application Policy Infrastructure Controller (APIC) versão 5.2(7f)
- Ubuntu 20.04 com slapd e phpLDAPadmin

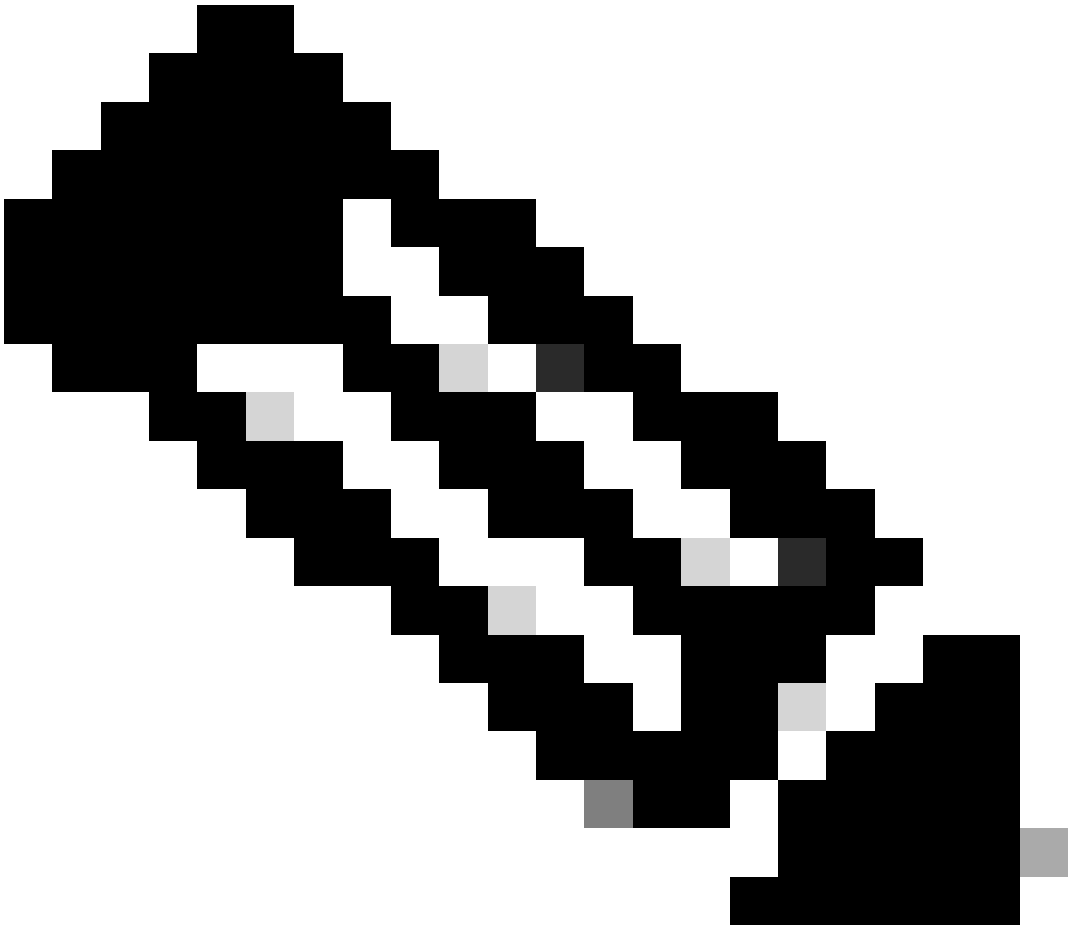
As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Configurar

Esta seção descreve como configurar o APIC para integrar com o servidor LDAP e usar LDAP como o método de autenticação padrão.

Configurações

Etapa 1. Criar grupos/usuários no Ubuntu phpLDAPadmin

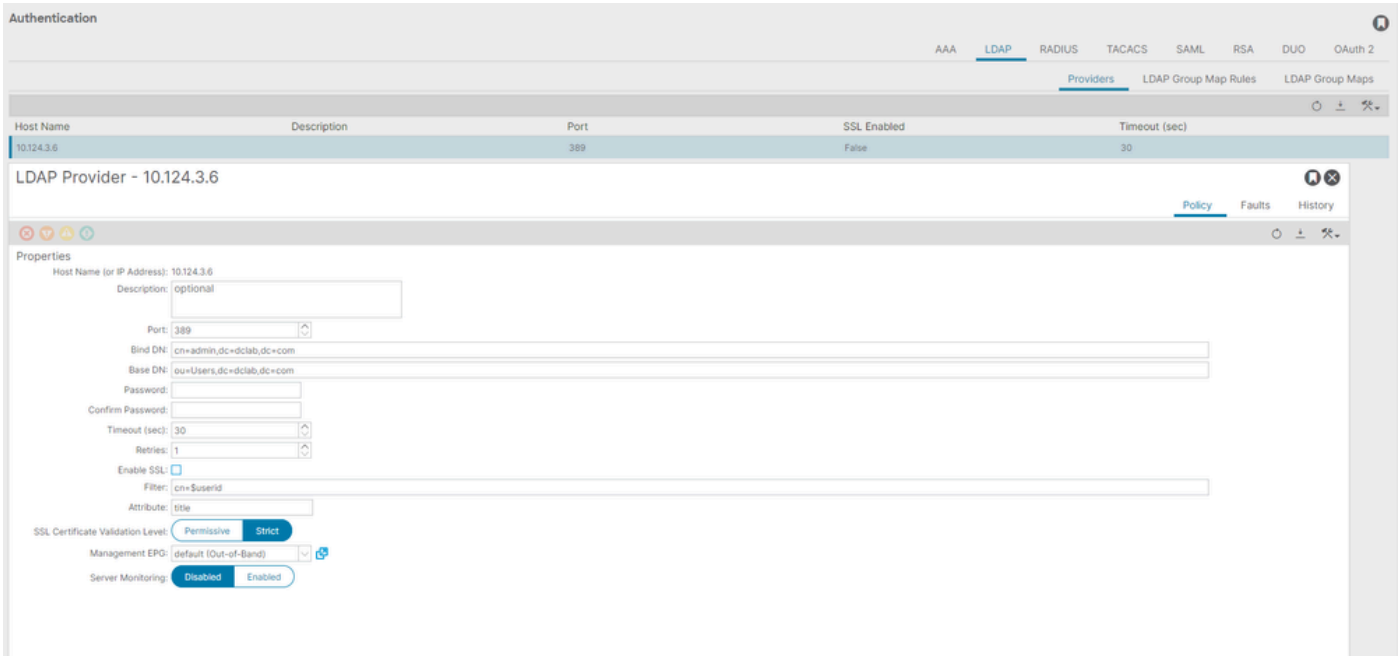


> Observação: para configurar o Ubuntu como um servidor LDAP, consulte o site oficial do Ubuntu para obter diretrizes abrangentes. Se houver um servidor LDAP existente, comece com a Etapa 2.

Neste documento, o DN base é dc=dclab,dc=com e dois usuários (Usuário1 e Usuário2) pertencem a Grupos (DCGroup).

Etapa 2. Configurar provedores LDAP no APIC

Na barra de menus do APIC, navegue até Admin > AAA > Authentication > LDAP > Providers conforme mostrado na imagem.



DN de vinculação: o DN de vinculação é a credencial que você está usando para se autenticar em um LDAP. O APIC autentica usando essa conta para consultar o diretório.

DN base: essa sequência de caracteres é empregada pelo APIC como um ponto de referência para pesquisar e identificar entradas de usuário no diretório.

Senha: Esta é a senha necessária para o DN de vinculação necessário para acessar o servidor LDAP, correlacionando-se com a senha estabelecida em seu servidor LDAP.

Habilitar SSL: se você usar uma CA interna ou um certificado autoassinado, escolha **Permissivo**.

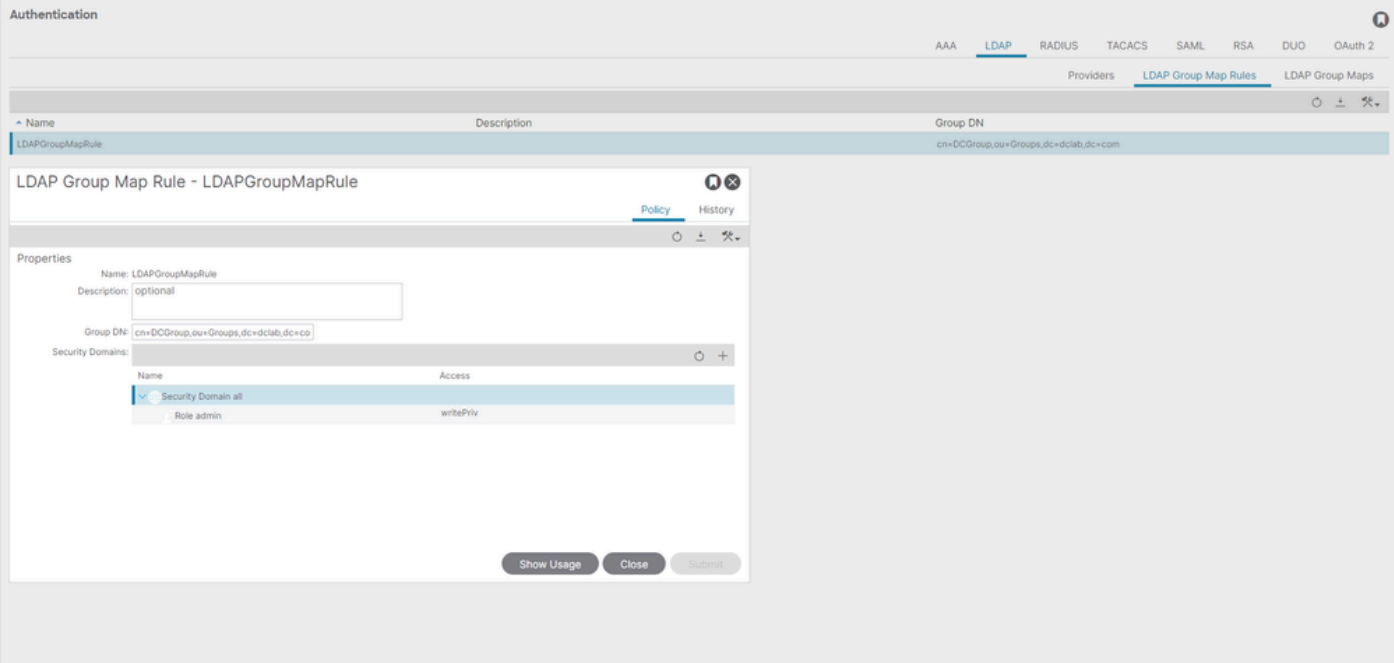
Filtro: A definição de filtro default é cn=$userid quando o usuário é definido como um objeto com um nome comum (CN), o filtro é usado para procurar os objetos dentro do DN de Base.

Atributo: O atributo é usado para determinar a associação de grupo e as funções. A ACI oferece duas opções aqui: memberOf e CiscoAVPair.memberOf é um atributo RFC2307bis para identificar a associação de grupo. Atualmente, o OpenLDAP verifica o RFC2307, portanto title é usado.

Grupo de endpoint de gerenciamento (EPG): a conectividade com o servidor LDAP é obtida por meio do EPG dentro da banda ou fora da banda, dependendo da abordagem de gerenciamento de rede escolhida.

Etapa 3. Configurar regras de mapa de grupo LDAP

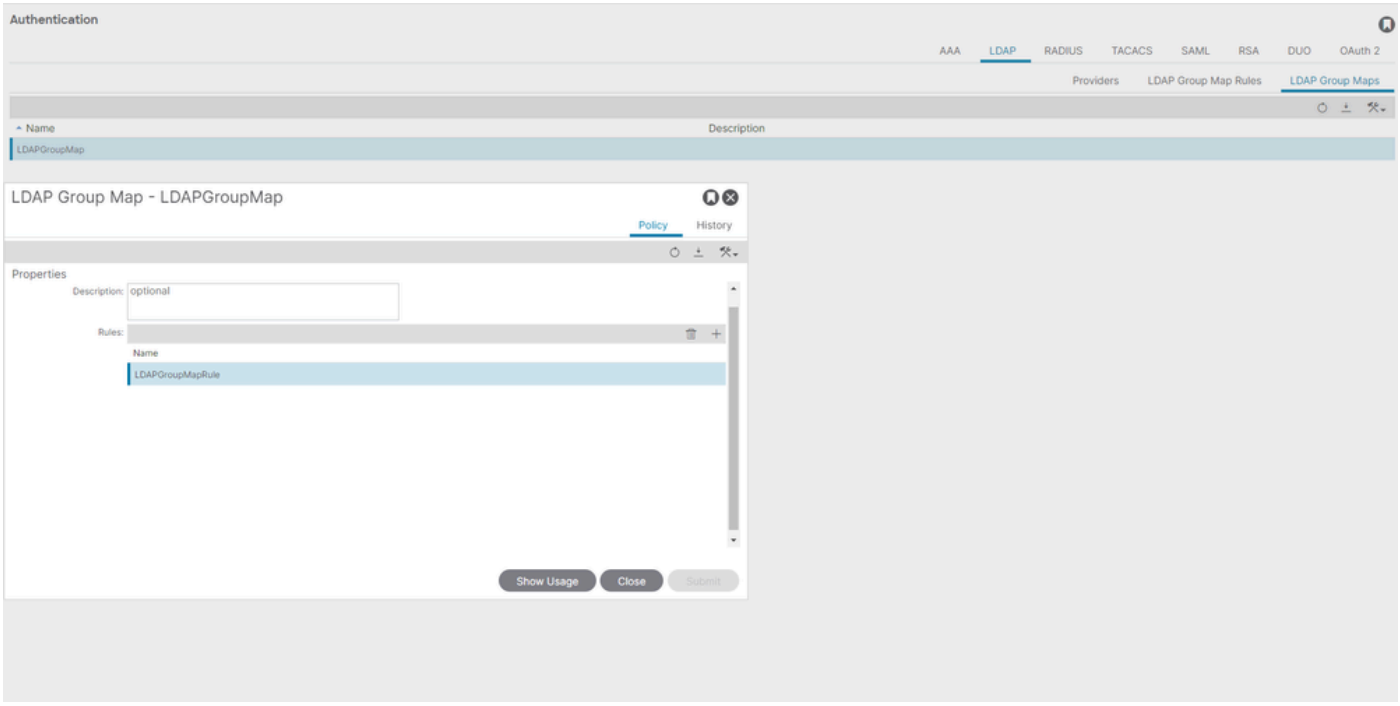
Na barra de menus, navegue até Admin > AAA > Authentication > LDAP > LDAP Group Map Rules conforme mostrado na imagem.



Os usuários no DCGroup têm privilégios de administrador. Portanto, o DN do grupo está cn=DCGroup, ou=Groups, dc=dclab, dc=com. Aatribuindo o domínio de segurança a All e alocando as funções de admin com write privilege .

Etapa 4. Configurar mapas de grupo LDAP

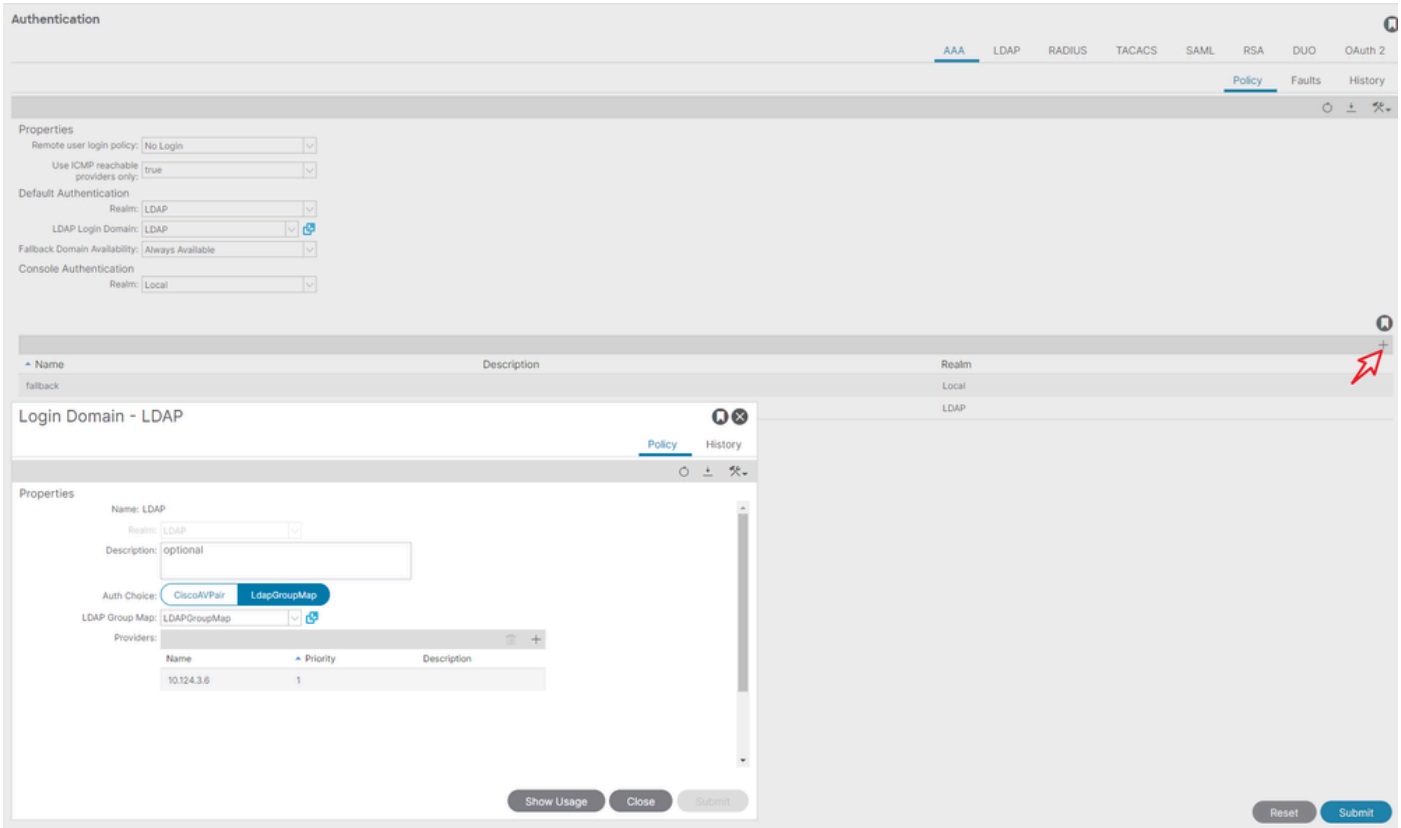
Na barra de menus, navegue até Admin > AAA > Authentication > LDAP > LDAP Group Maps conforme mostrado na imagem.



Crie um mapa de grupo LDAP que contenha regras de mapa de grupo LDAP criadas na Etapa 2.

Etapa 5. Configurar a Política de Autenticação AAA

Na barra de menus, navegue até Admin > AAA > Authentication > AAA > Policy > Create a login domainconforme mostrado na imagem.

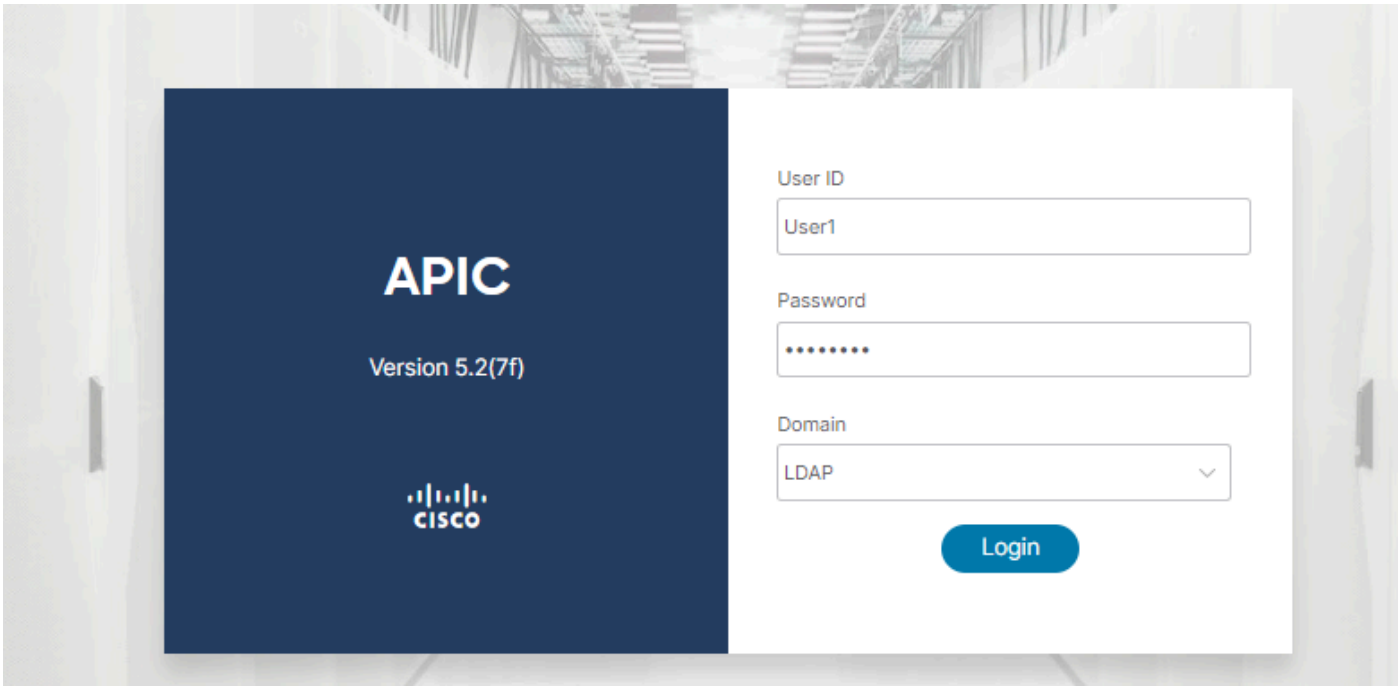


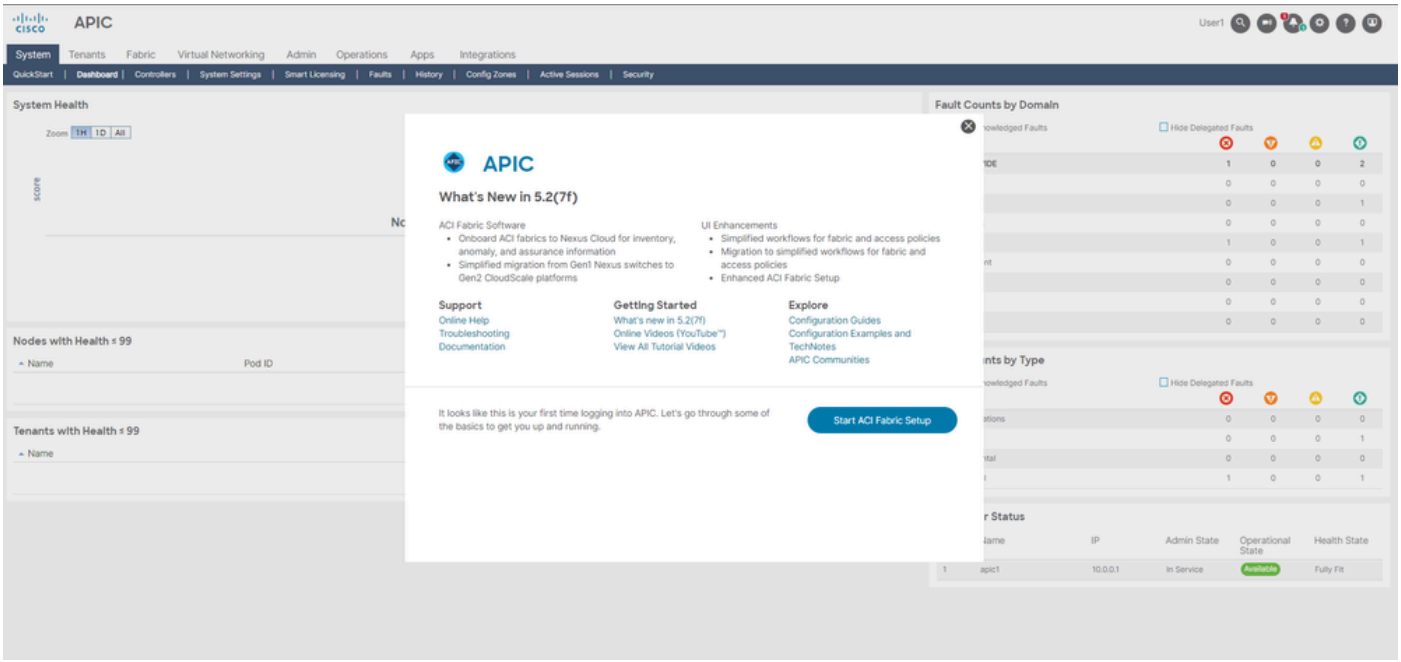
Na barra de menus, navegue até Admin > AAA > Authentication > AAA > Policy > Default Authentication conforme mostrado na imagem.

Altere a autenticaçãoRealm padrão para LDAP e selecione LDAP Login Domain created.

Verificar

Use esta seção para confirmar se a sua configuração funciona corretamente.



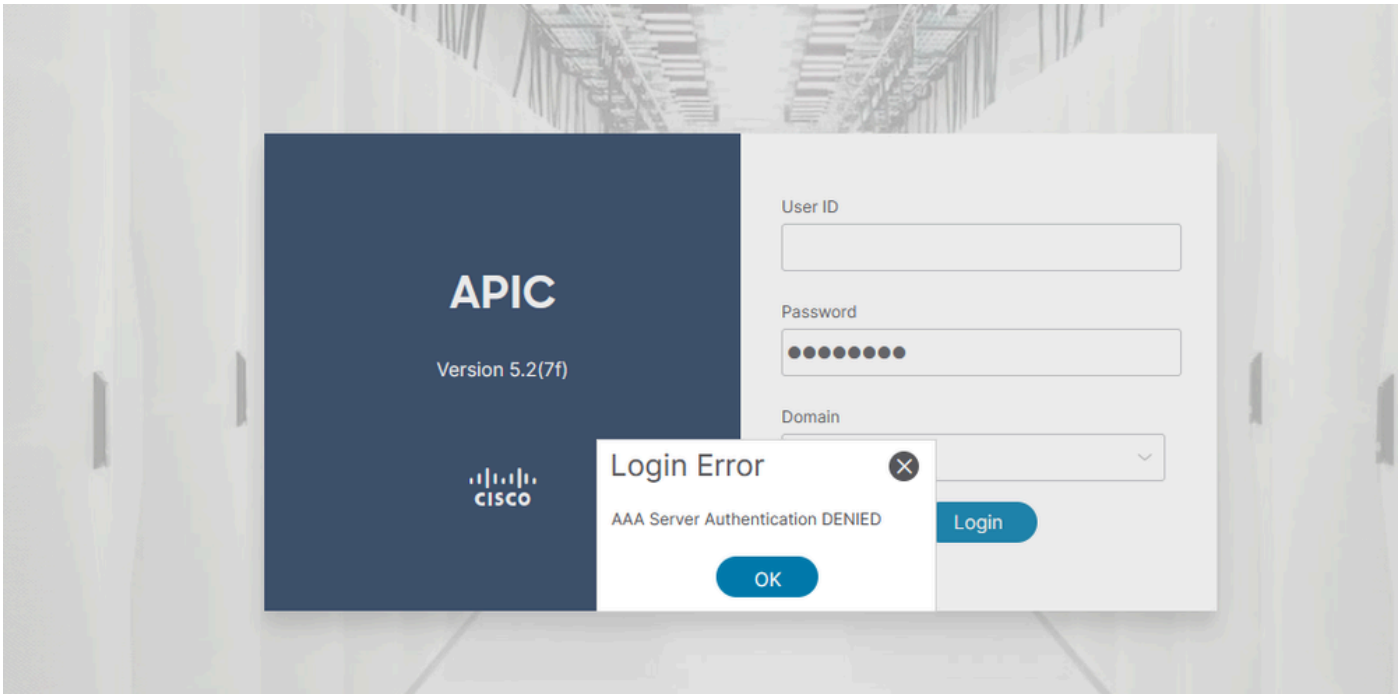


Verifique se o usuárioUser1 LDAP faz login no APIC com êxito com função de administrador e privilégio de gravação.

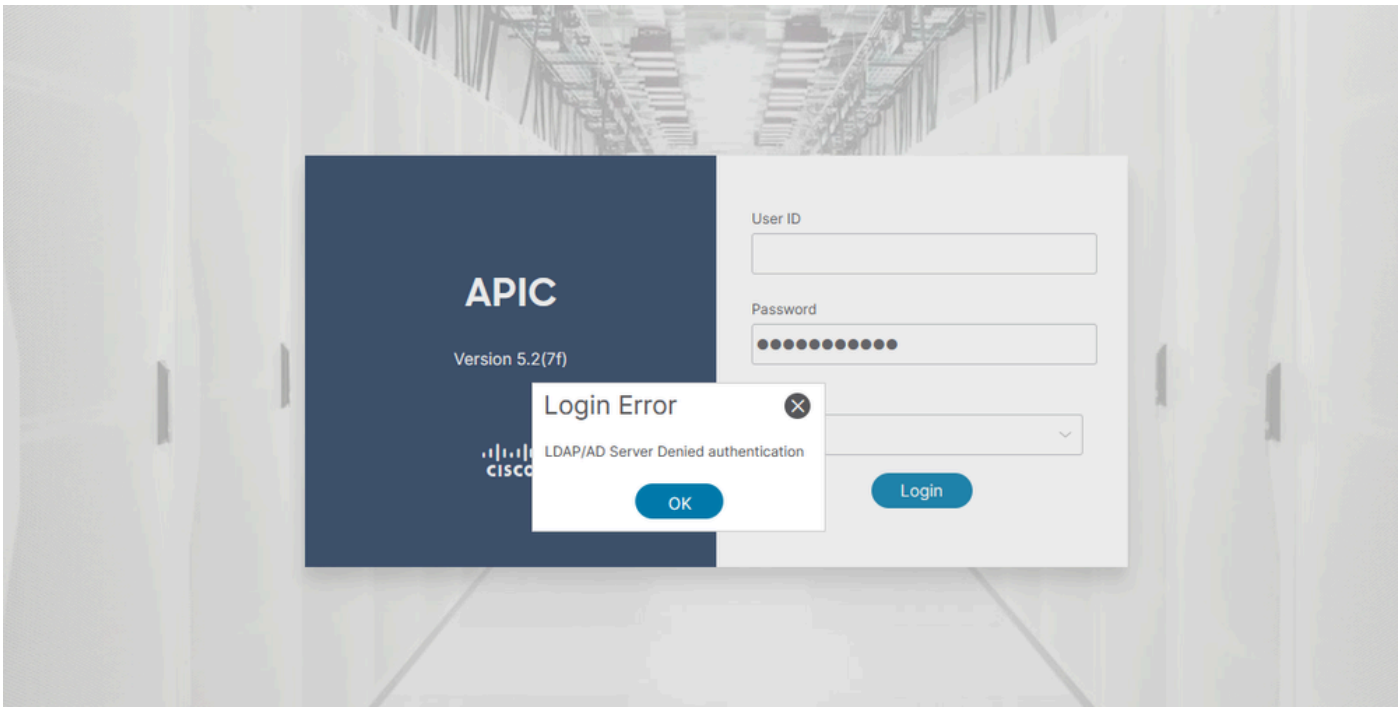
Troubleshooting

Esta seção disponibiliza informações para a solução de problemas de configuração.

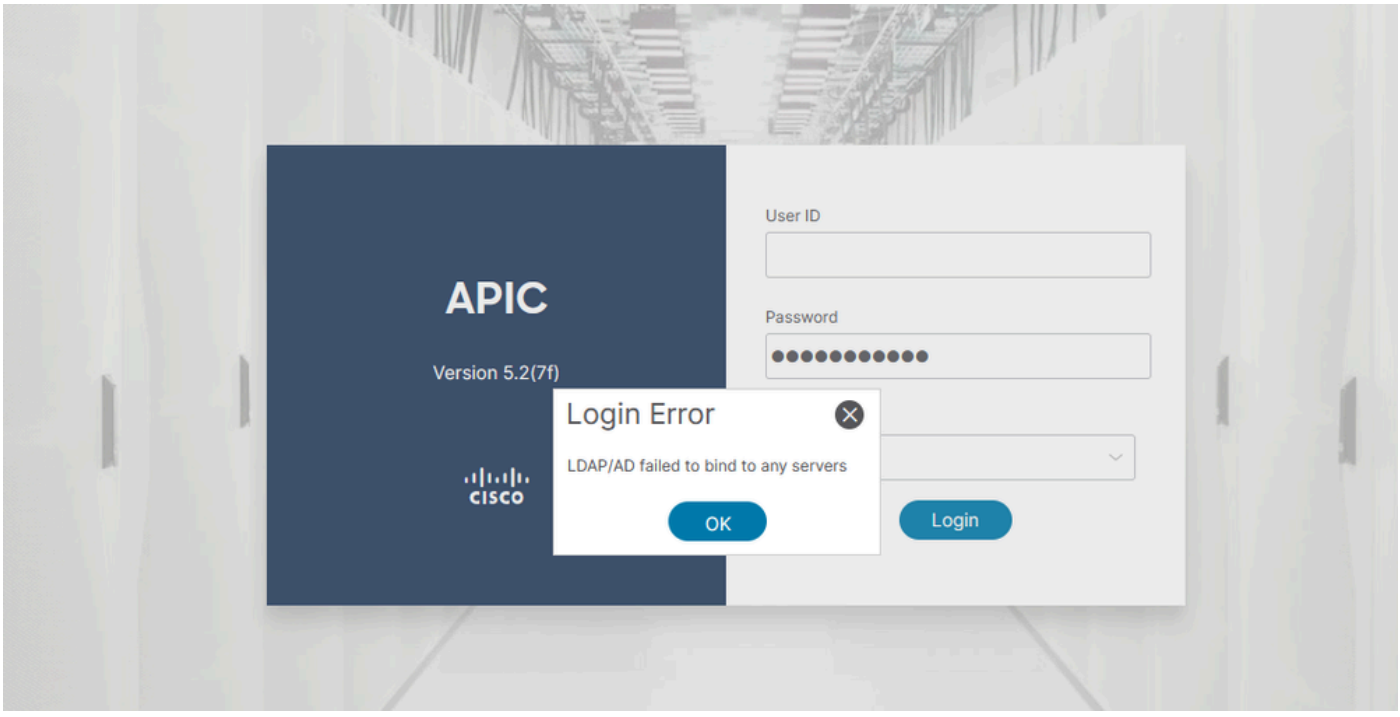
Quando o usuário não existir no banco de dados LDAP:



Quando a senha estiver incorreta:



Quando o servidor LDAP estiver inacessível:



Comandos para Troubleshooting:

<#root>

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

Se precisar de mais ajuda, entre em contato com o Cisco TAC.

Informações Relacionadas

- Guia de configuração de segurança do Cisco APIC, versão 5.2(x)
- Suporte técnico e downloads da Cisco

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.