Configuración de la autenticación LDAP de ACI

Contenido

Introducción

Este documento describe cómo configurar la autenticación del protocolo ligero de acceso a directorios (LDAP) de la infraestructura centrada en aplicaciones (ACI).

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Política de autenticación, autorización y contabilidad (AAA) de ACI
- LDAP

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Cisco Application Policy Infrastructure Controller (APIC) versión 5.2(7f)
- Ubuntu 20.04 con slapd y phpLDAPadmin

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo,

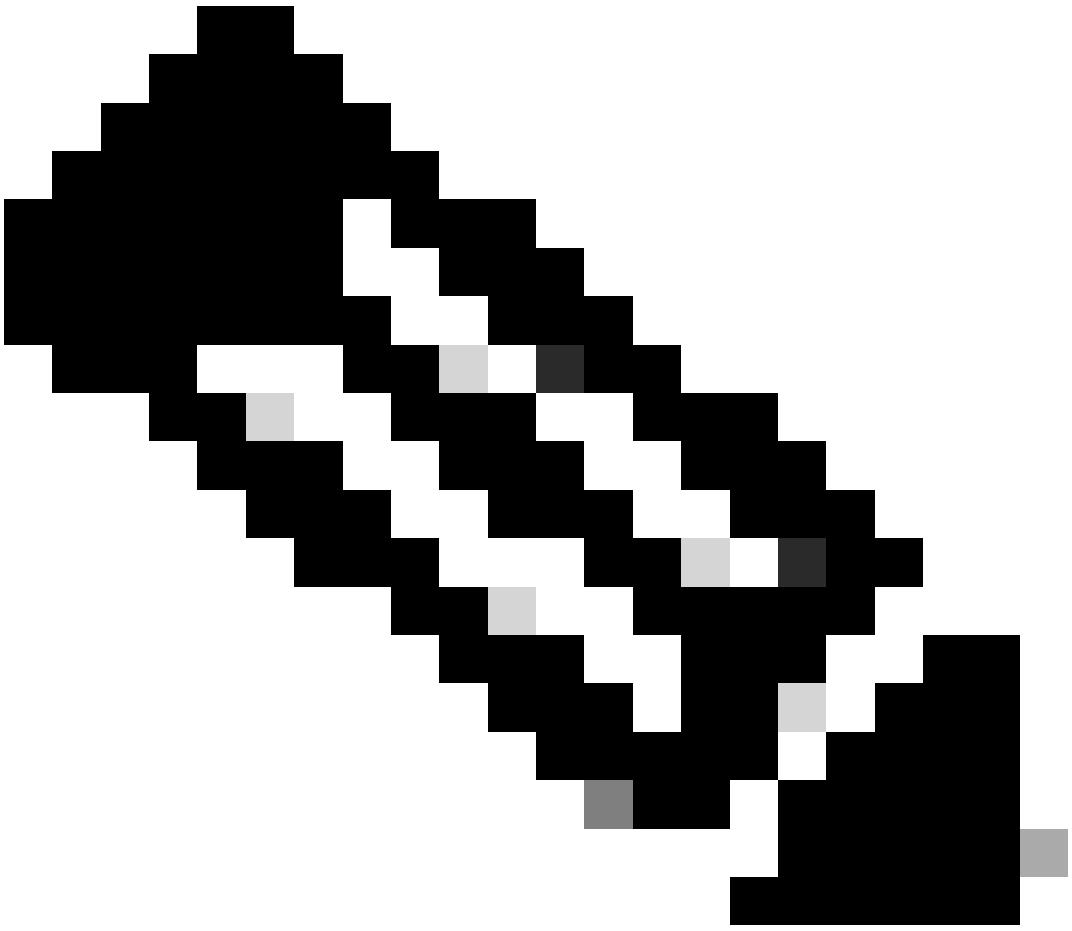
asegúrese de entender el posible impacto de cualquier comando.

Configurar

Esta sección describe cómo configurar APIC para integrarse con el servidor LDAP y utilizar LDAP como el método de autenticación predeterminado.

Configuraciones

Paso 1. Crear grupos/usuarios en Ubuntu phpLDAPadmin

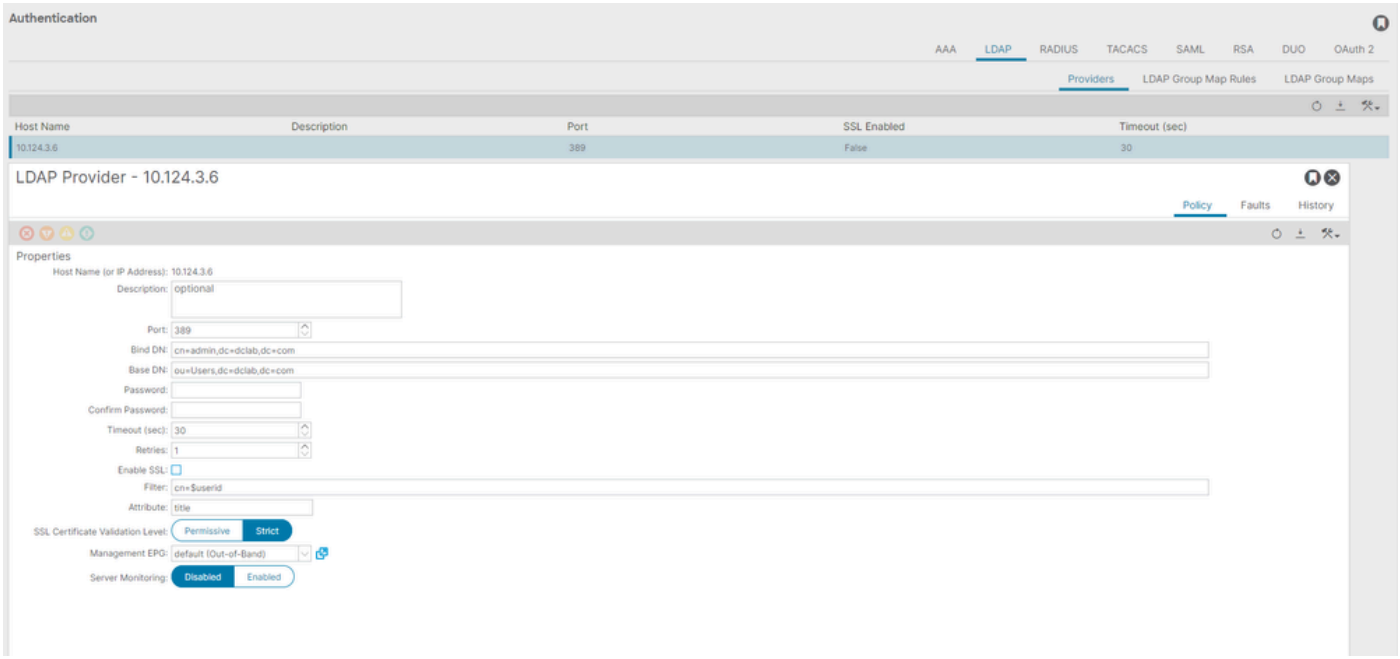


> Nota: Para configurar Ubuntu como un servidor LDAP, consulte el sitio web oficial de Ubuntu para obtener pautas completas. Si ya existe un servidor LDAP, comience por el paso 2.

En este documento, el DN base es dc=dclab,dc=com y dos usuarios (Usuario1 y Usuario2) pertenecen a Grupos (DCGroup).

Paso 2. Configuración de proveedores LDAP en APIC

En la barra de menús de APIC, desplácese hasta Admin > AAA > Authentication > LDAP > Providers como se muestra en la imagen.



Enlazar DN: El DN de enlace es la credencial que está utilizando para autenticarse contra un LDAP. El APIC se autentica utilizando esta cuenta para consultar el directorio.

DN base: esta cadena la utiliza el APIC como punto de referencia para buscar e identificar entradas de usuario en el directorio.

Contraseña: Es la contraseña necesaria para el DN de enlace necesario para acceder al servidor LDAP, que se correlaciona con la contraseña establecida en el servidor LDAP.

Habilitar SSL: si utiliza una CA interna o un certificado autofirmado, debe elegir **Permiso**.

Filtro: La configuración de filtro predeterminada es cn=$userid cuando el usuario se define como un objeto con un nombre común (CN), el filtro se utiliza para buscar los objetos dentro del DN base.

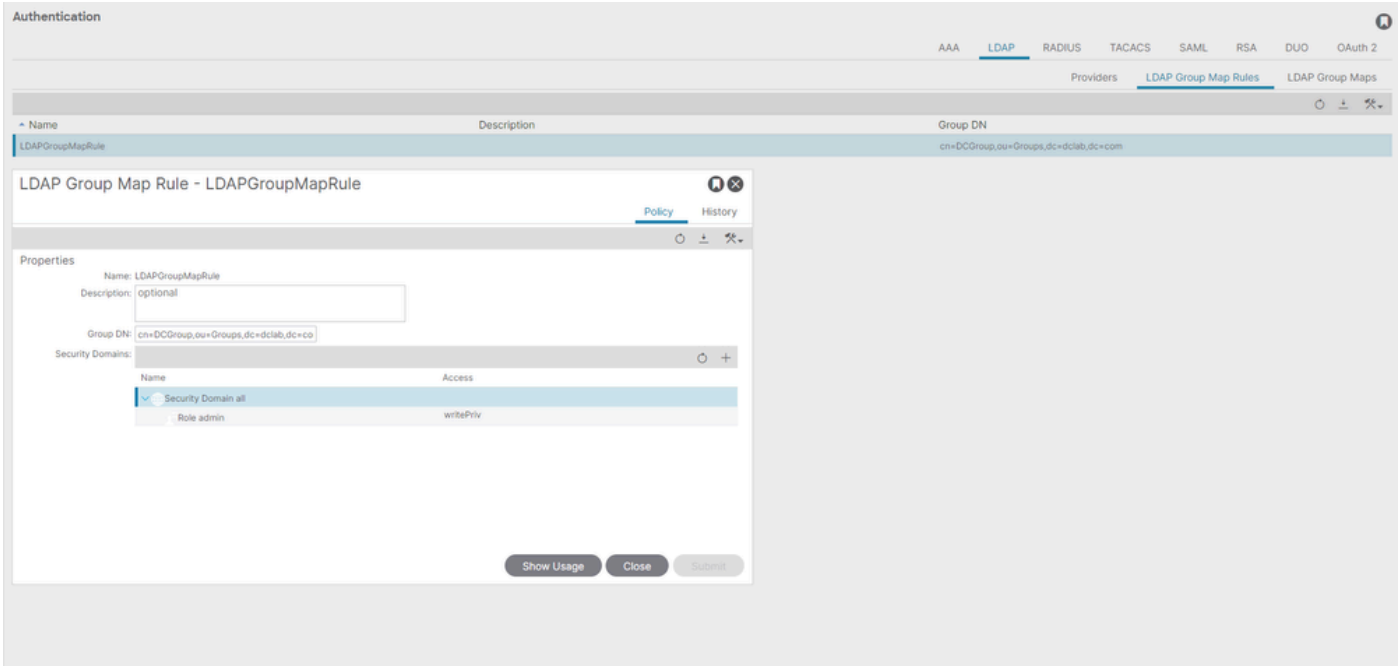
Atributo: el atributo se utiliza para determinar la pertenencia al grupo y los roles. ACI proporciona dos opciones aquí: memberOf y

CiscoAVPair.memberOf es un atributo RFC2307bis para identificar la pertenencia al grupo. Actualmente, OpenLDAP verifica RFC2307, por lo que title se utiliza en su lugar.

Grupo de terminales de administración (EPG): la conectividad con el servidor LDAP se consigue a través del EPG en banda o fuera de banda, en función del enfoque de administración de red elegido.

Paso 3. Configurar reglas de mapa de grupo LDAP

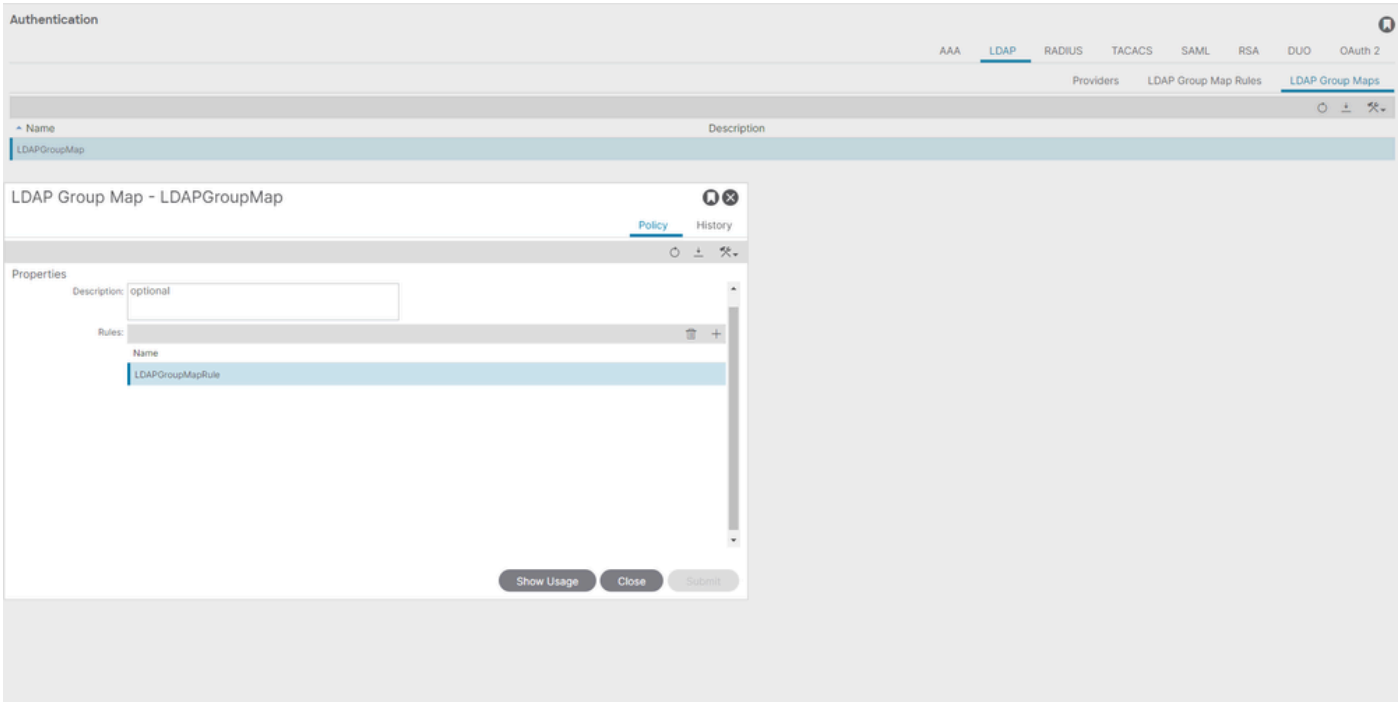
En la barra de menús, desplácese hasta Admin > AAA > Authentication > LDAP > LDAP Group Map Rules como se muestra en la imagen.



Los usuarios de DCGroup tienen privilegios de administrador. Por lo tanto, el DN de grupo está cn=DCGroup, ou=Groups, dc=dclab, dc=com. Aasignando el dominio de seguridad a All y asignando las funciones de admin con write privilege .

Paso 4. Configuración de Mapas de Grupo LDAP

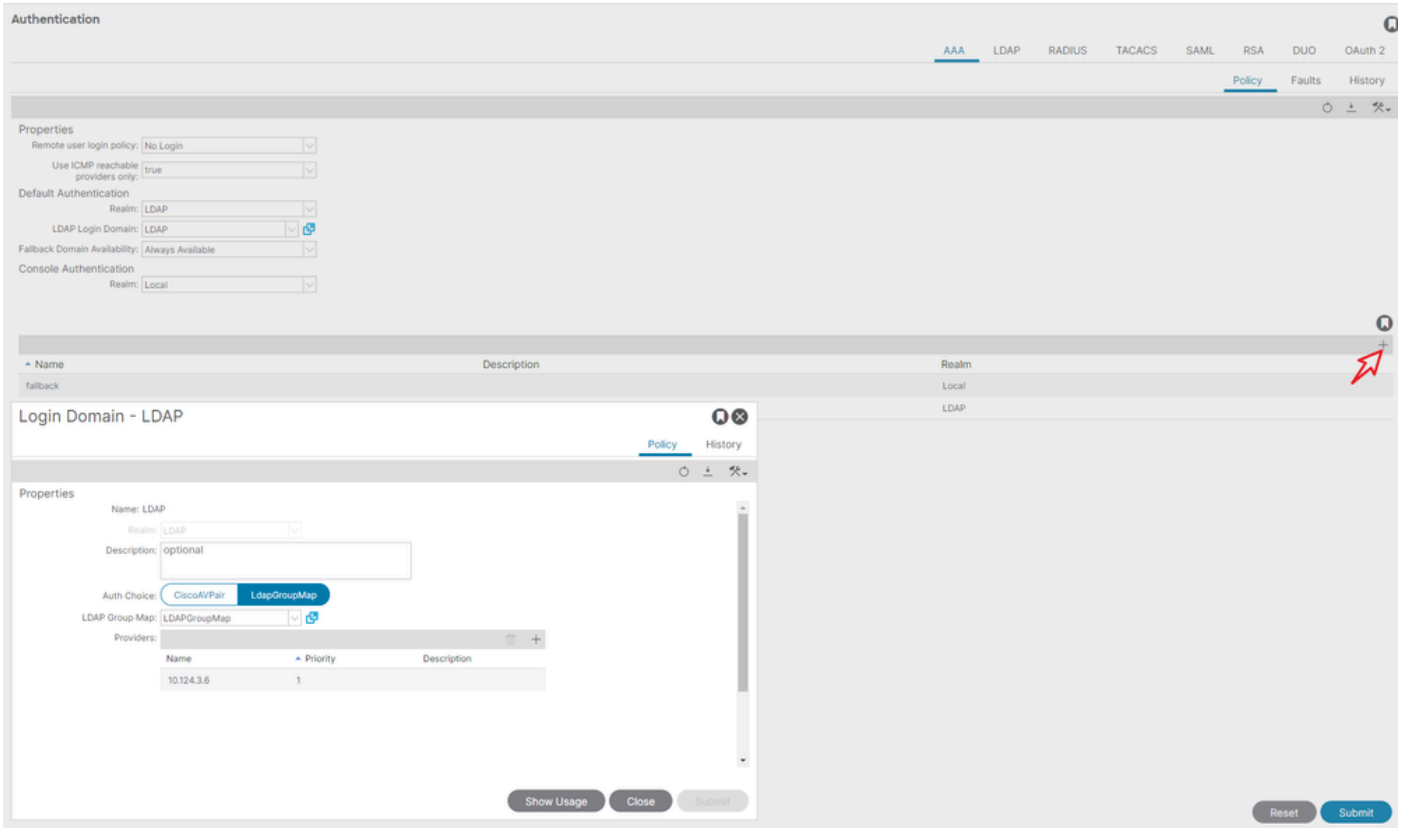
En la barra de menús, desplácese hasta Admin > AAA > Authentication > LDAP > LDAP Group Maps como se muestra en la imagen.



Cree un mapa de grupo LDAP que contenga las reglas de mapa de grupo LDAP creadas en el paso 2.

Paso 5. Configurar política de autenticación AAA

En la barra de menús, desplácese hasta Admin > AAA > Authentication > AAA > Policy > Create a login domaincomo se muestra en la imagen.

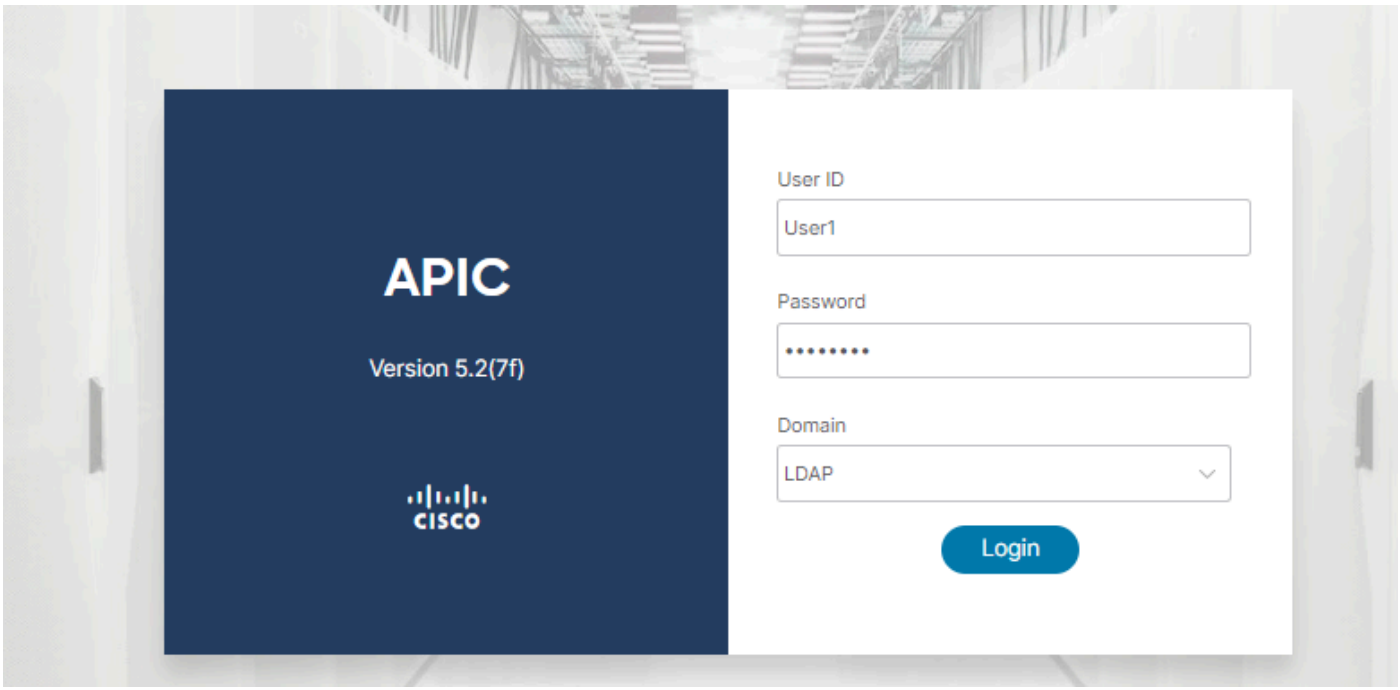


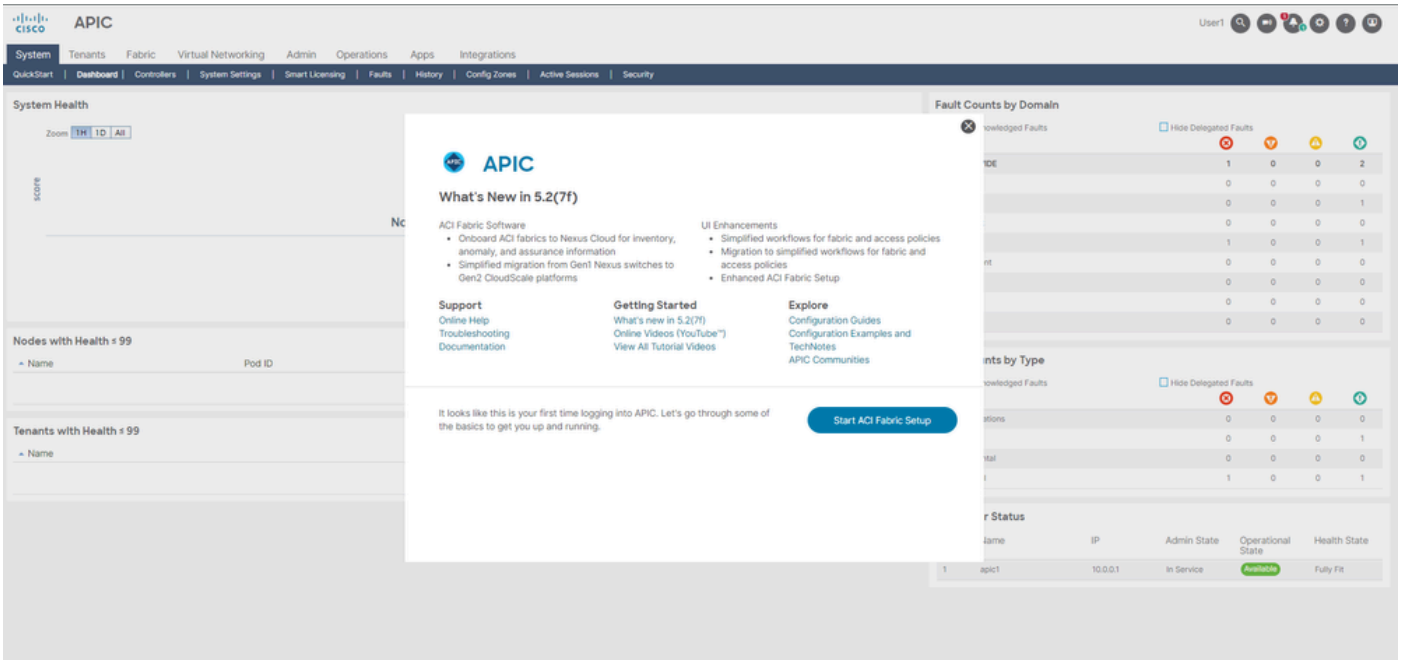
En la barra de menús, desplácese hasta Admin > AAA > Authentication > AAA > Policy > Default Authentication como se muestra en la imagen.

Cambie la autenticación predeterminada Realm a LDAP y seleccione LDAP Login Domain Created .

Verificación

Utilize esta sección para confirmar que su configuración funcione correctamente.



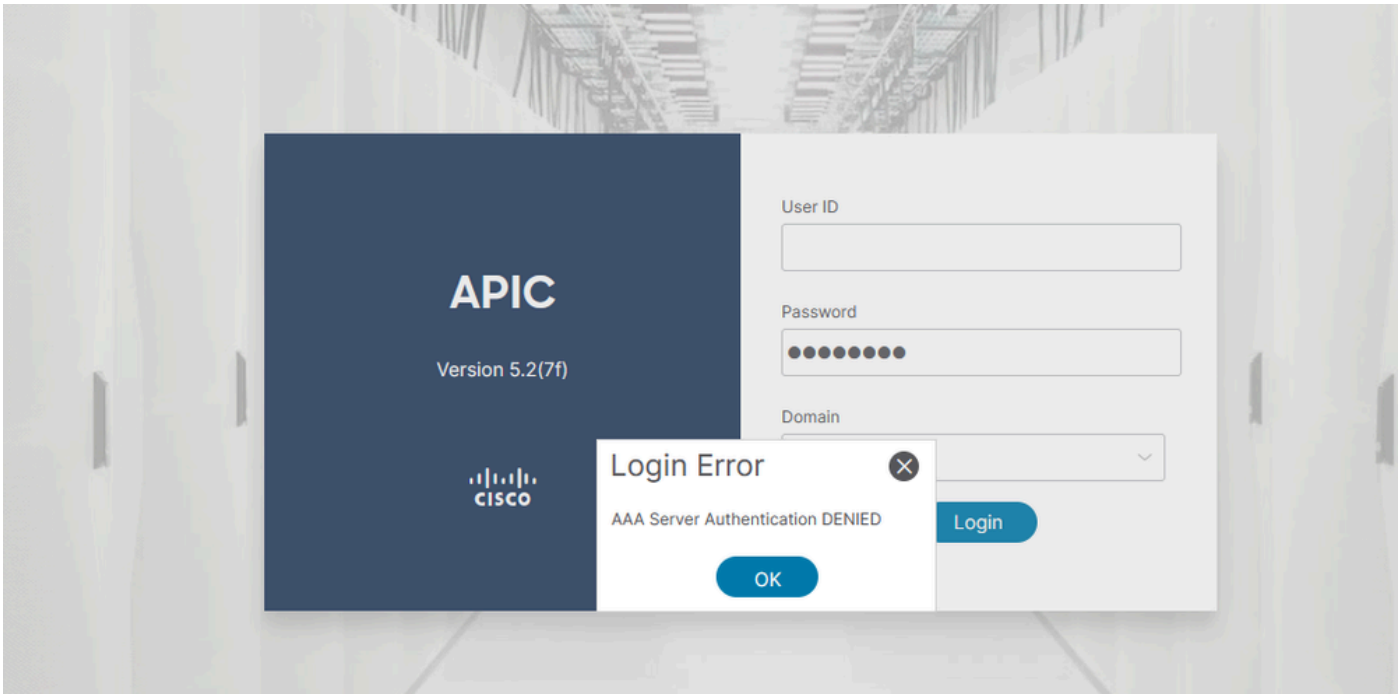


Verifique que el usuario LDAP User1 inicie sesión en APIC correctamente con el rol de administrador y el privilegio de escritura.

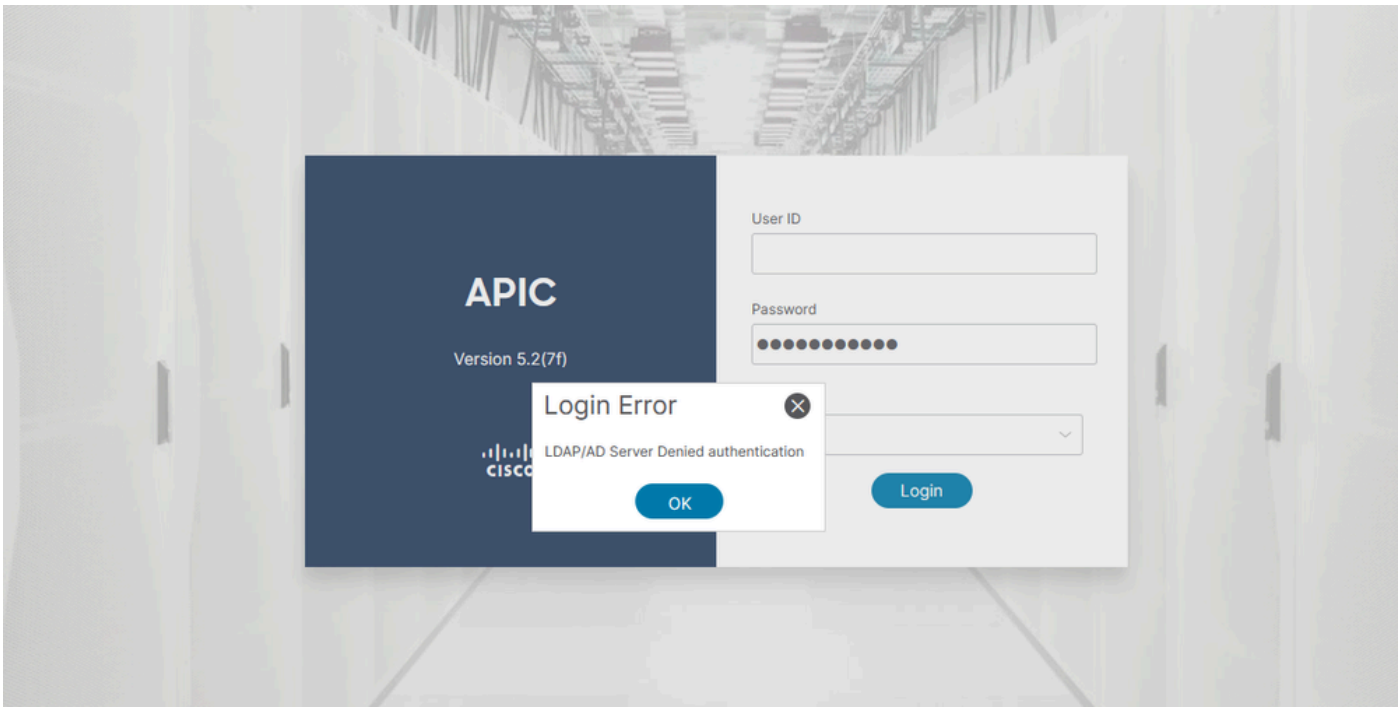
Troubleshoot

En esta sección se brinda información que puede utilizar para resolver problemas en su configuración.

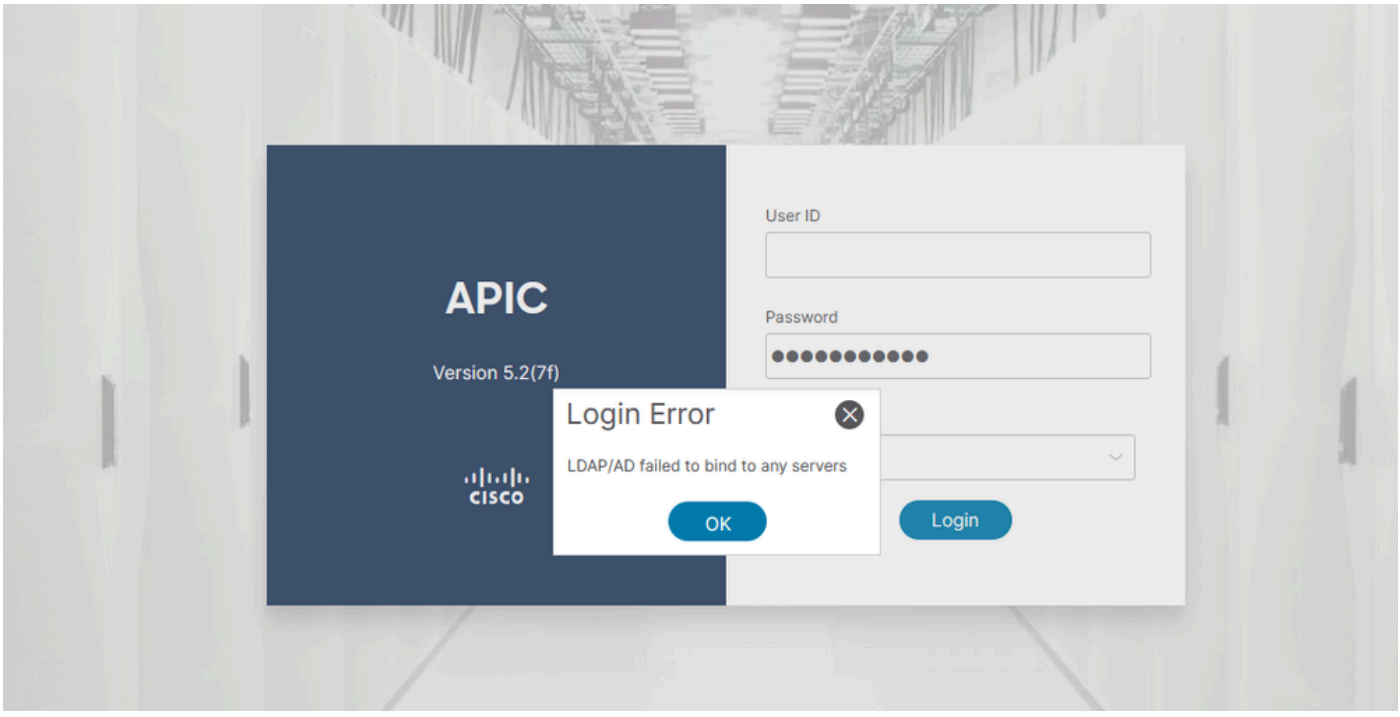
Cuando el usuario no existe en la base de datos LDAP:



Cuando la contraseña es incorrecta:



Cuando el servidor LDAP es inalcanzable:



Comandos para resolución de problemas:

<#root>

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

Si necesita más ayuda, póngase en contacto con Cisco TAC.

Información Relacionada

- Guía de configuración de seguridad de Cisco APIC, versión 5.2(x)
- Soporte técnico y descargas de Cisco

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).