Configura autenticazione LDAP ACI

Sommario

Introduzione

In questo documento viene descritto come configurare l'autenticazione LDAP (Lightweight Directory Access Protocol) di ACI (Application Centric Infrastructure).

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Policy ACI di autenticazione, autorizzazione e accounting (AAA)
- LDAP

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

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

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali

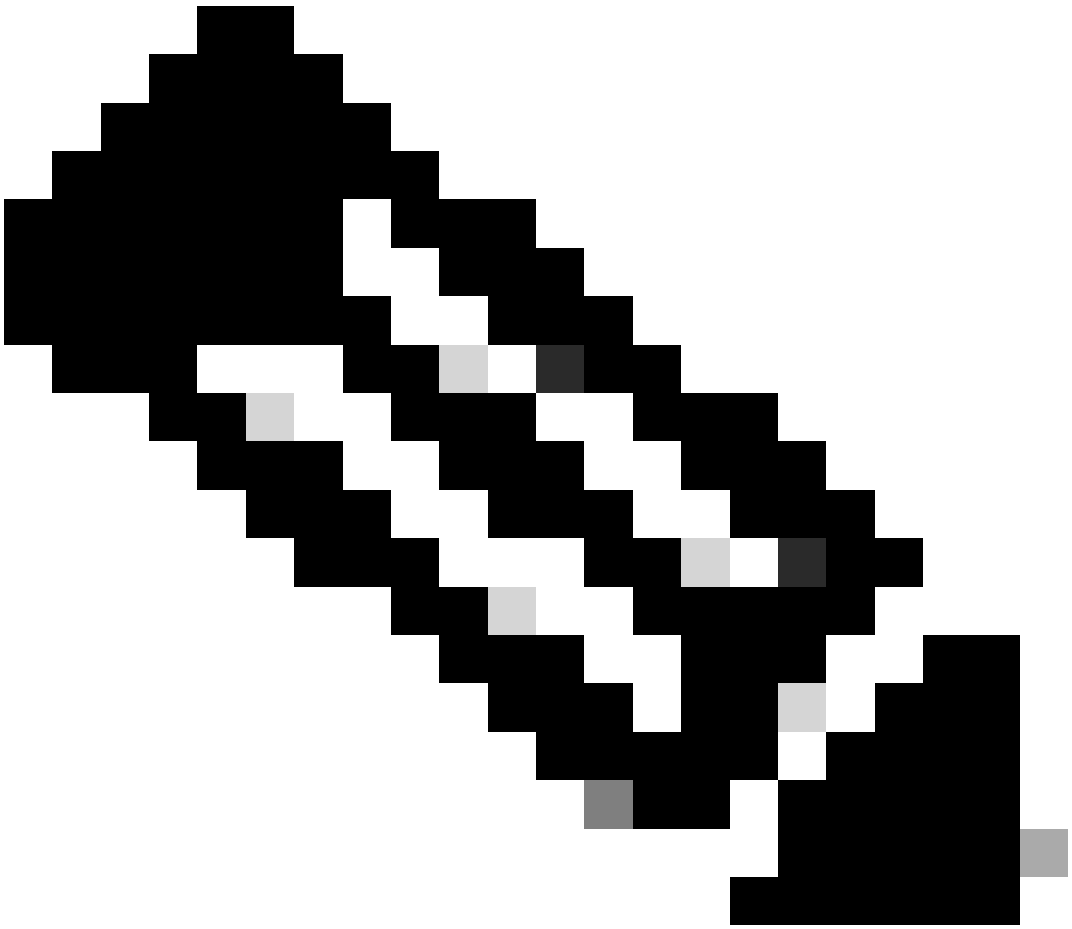
conseguenze derivanti dall'uso dei comandi.

Configurazione

In questa sezione viene descritto come configurare APIC in modo da integrarlo con il server LDAP e utilizzare LDAP come metodo di autenticazione predefinito.

Configurazioni

Passaggio 1. Crea gruppi/utenti su Ubuntu phpLDAPadmin

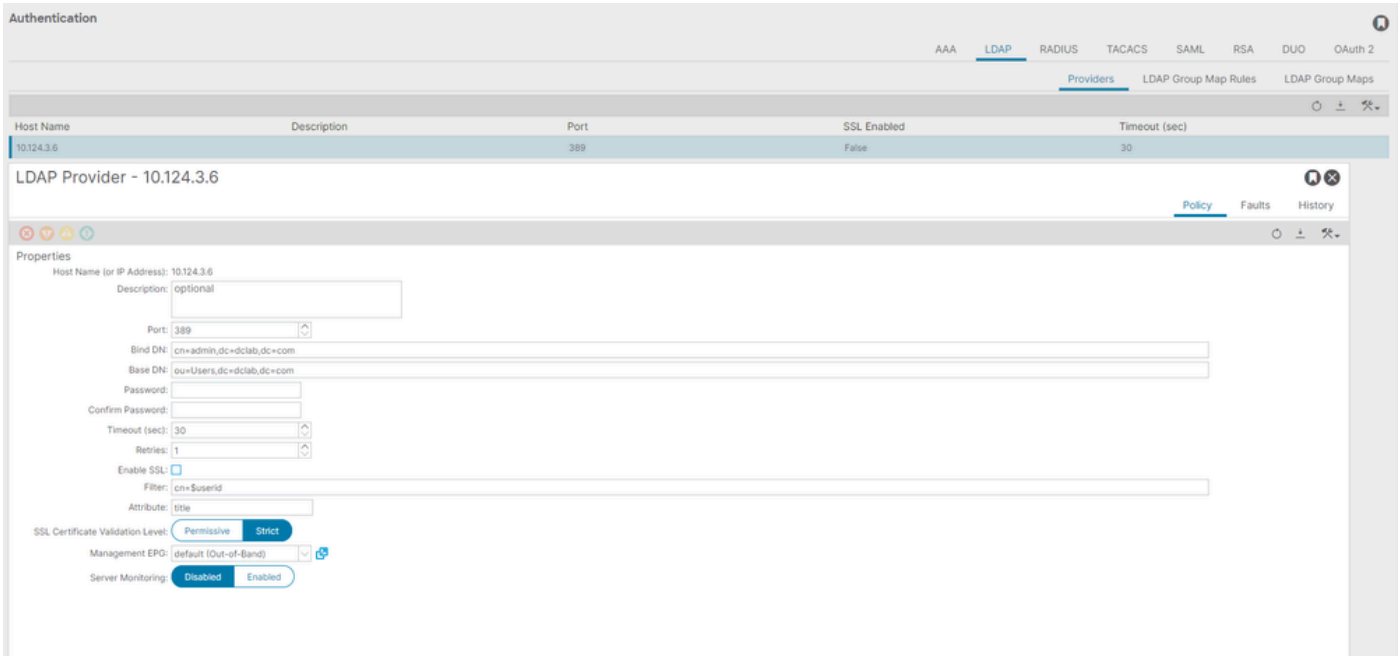


> Nota: per configurare Ubuntu come server LDAP, consultare il sito ufficiale di Ubuntu per le linee guida complete. Se è presente un server LDAP esistente, iniziare con il passo 2.

In questo documento, il DN di base è dc=dclab,dc=com e due utenti (Utente1 e Utente2) appartengono a Gruppi (DCGroup).

Passaggio 2. Configurare i provider LDAP su APIC

Sulla barra dei menu APIC, spostarsi suAdmin > AAA > Authentication > LDAP > Providers come mostrato nell'immagine.



DN di binding: il DN di binding è la credenziale utilizzata per l'autenticazione in base a un LDAP. APIC esegue l'autenticazione utilizzando questo account per eseguire query sulla directory.

DN di base: questa stringa viene utilizzata dall'APIC come punto di riferimento per la ricerca e l'identificazione delle voci utente all'interno della directory.

Password: la password richiesta per il DN di binding necessaria per accedere al server LDAP, correlata alla password impostata sul server LDAP.

Abilita SSL: se si utilizza una CA interna o un certificato autofirmato, è necessario scegliere **Permissivo**.

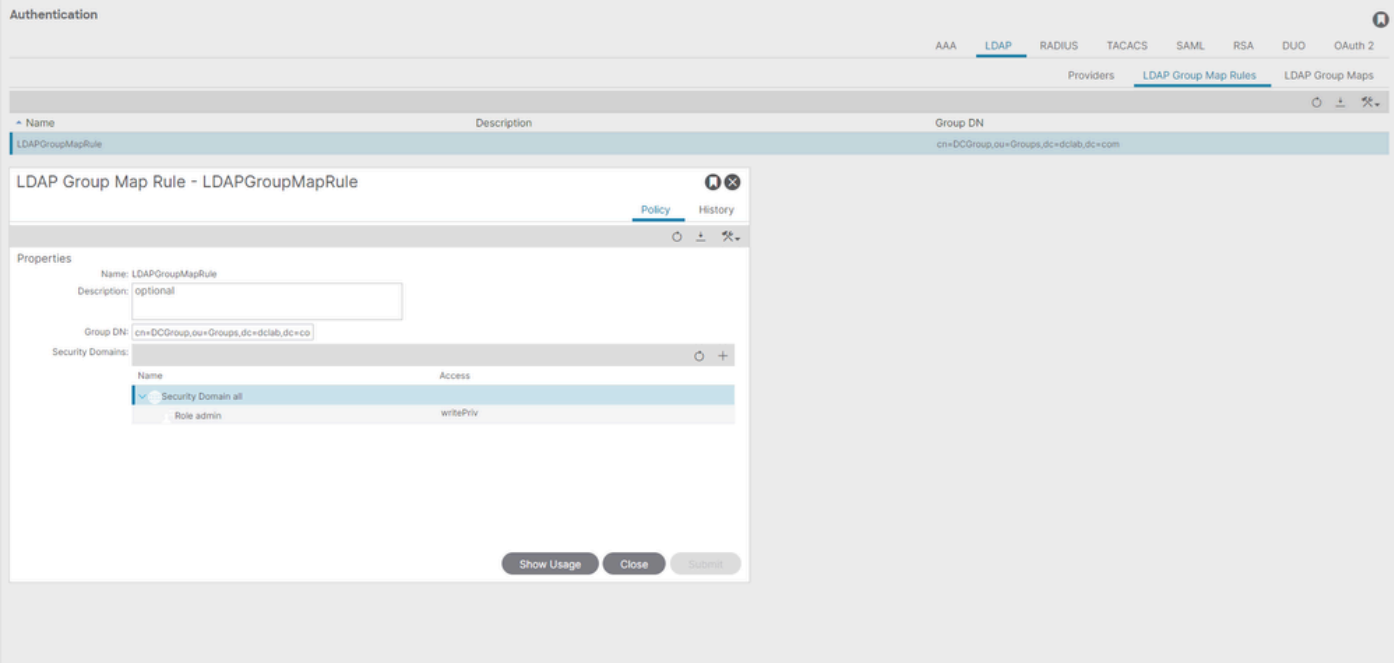
Filtro: l'impostazione predefinita del filtro è cn=$userid quando l'utente è definito come un oggetto con un nome comune (CN), il filtro viene utilizzato per cercare gli oggetti all'interno del DN di base.

Attributo: l'attributo viene utilizzato per determinare l'appartenenza al gruppo e i ruoli. ACI fornisce due opzioni qui: memberOf e CiscoAVPair.memberOf è un attributo RFC2307bis per identificare l'appartenenza al gruppo. Attualmente, OpenLDAP controlla RFC2307, quindi title viene utilizzato.

Management Endpoint Group (EPG): la connettività al server LDAP viene ottenuta tramite EPG in-band o out-of-band, a seconda dell'approccio di gestione della rete scelto.

Passaggio 3. Configura regole mapping gruppi LDAP

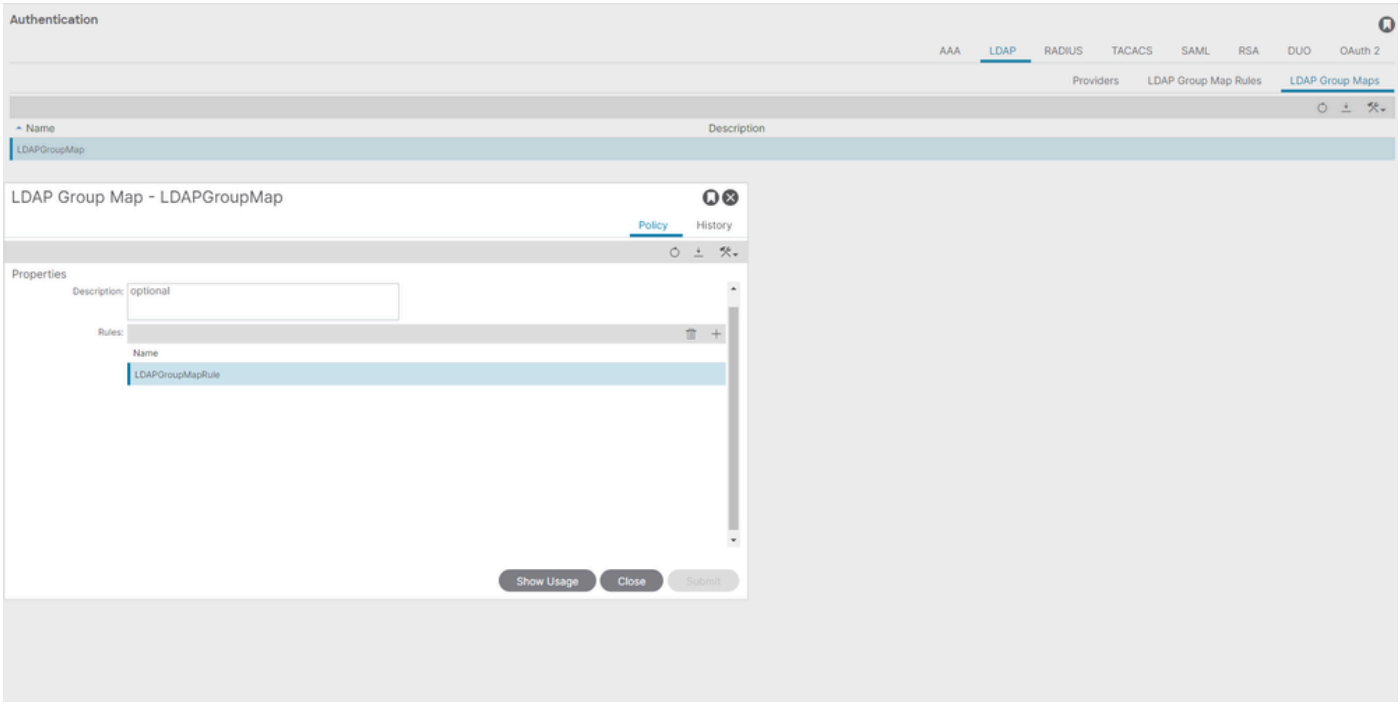
Sulla barra dei menu, passare a Admin > AAA > Authentication > LDAP > LDAP Group Map Rules come mostrato nell'immagine.



Gli utenti in DCGroup dispongono di privilegi di amministratore. Il DN gruppo cn=DCGroup, ou=Groups, dc=dclab, dc=com. Aassegna pertanto il dominio di protezione a All e alloca i ruoli di admin con write privilege .

Passaggio 4. Configura mapping gruppi LDAP

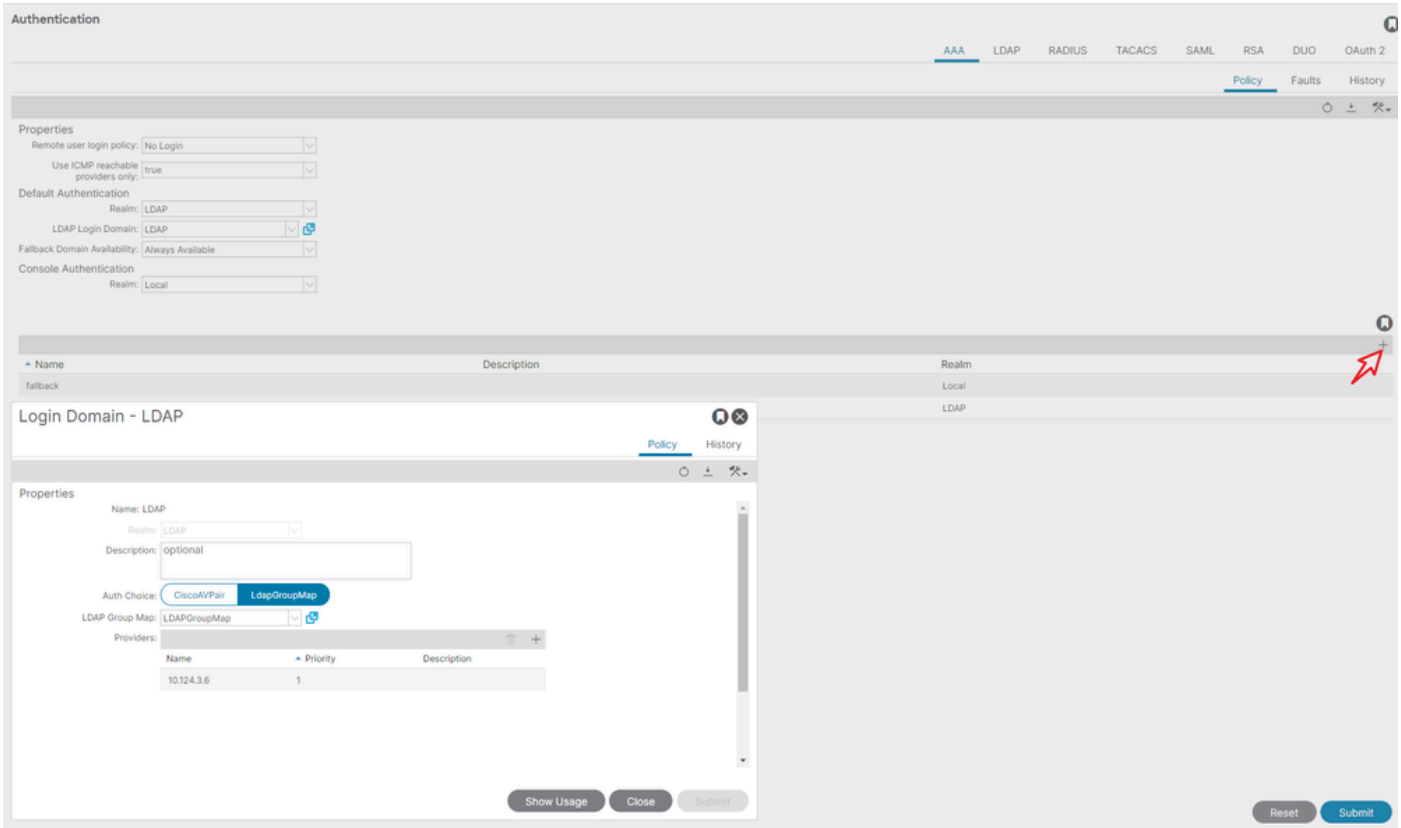
Sulla barra dei menu, passare a Admin > AAA > Authentication > LDAP > LDAP Group Maps come mostrato nell'immagine.



Creare una mappa di gruppo LDAP che contenga le regole della mappa di gruppo LDAP create nel passo 2.

Passaggio 5. Configura criterio di autenticazione AAA

Sulla barra dei menu, passare a Admin > AAA > Authentication > AAA > Policy > Create a login domaincome mostrato nell'immagine.

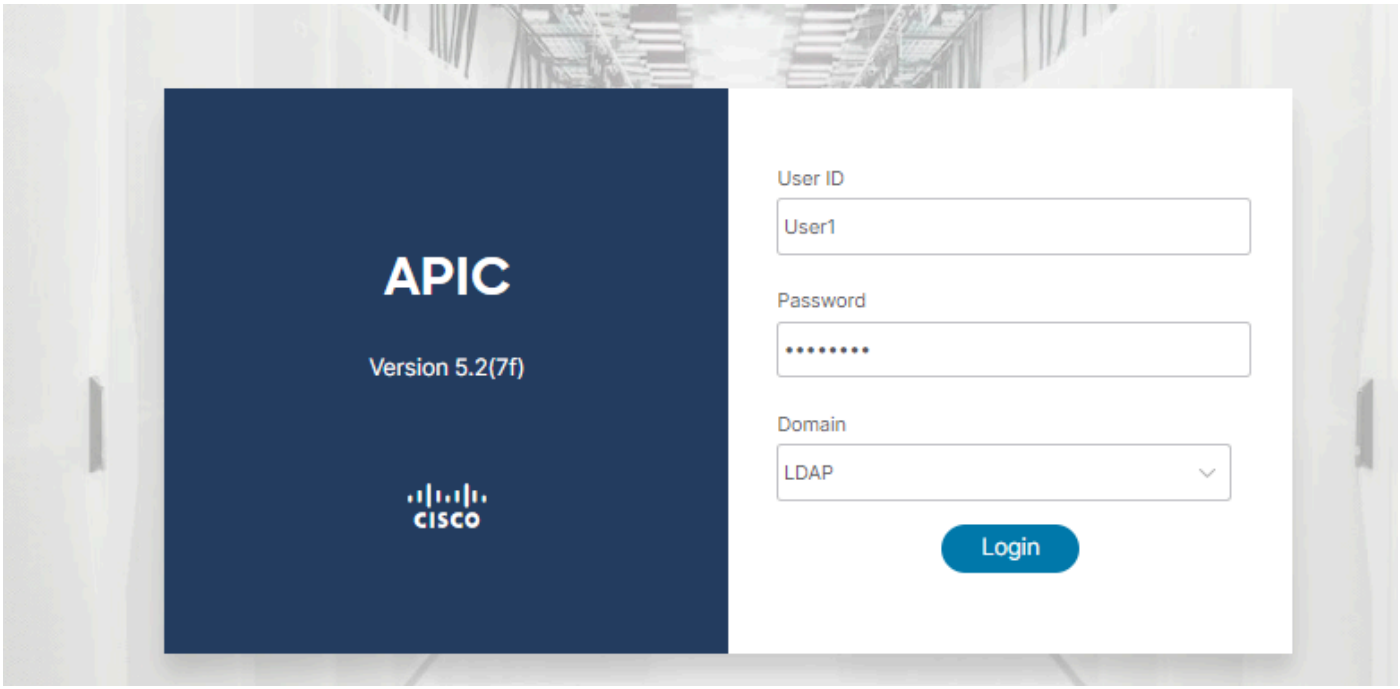


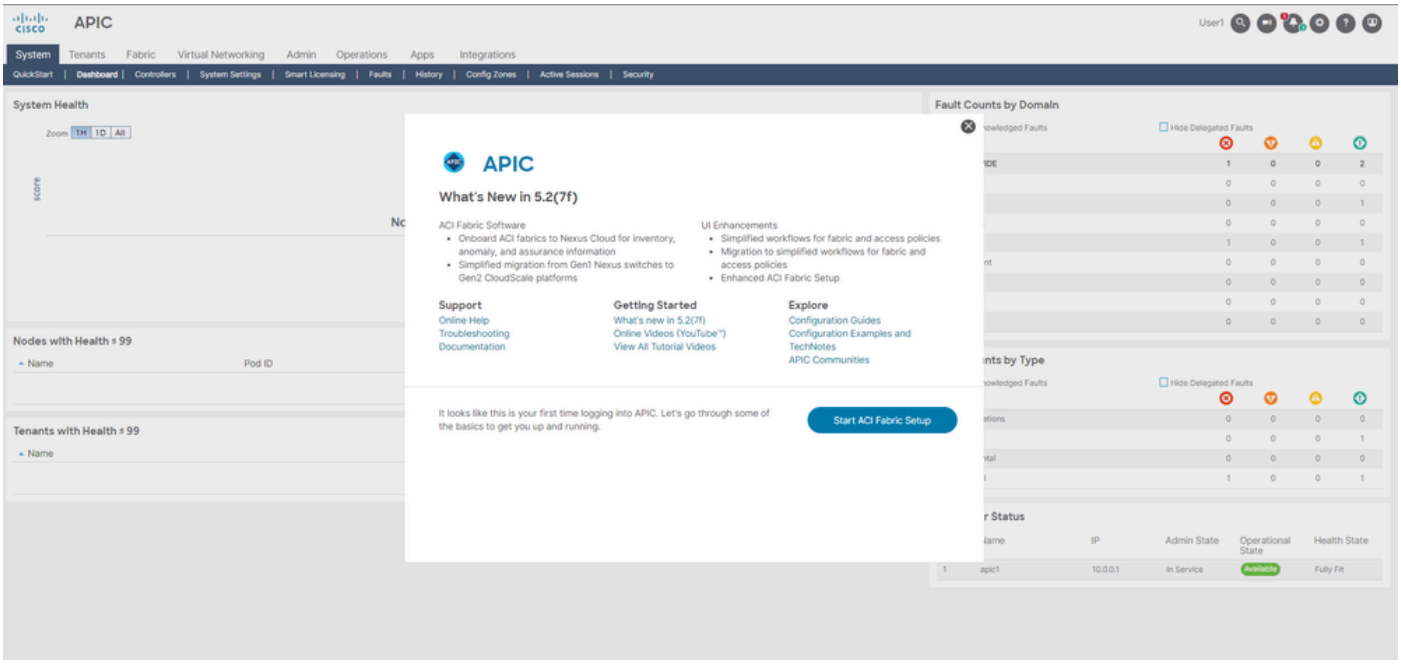
Sulla barra dei menu, passare a Admin > AAA > Authentication > AAA > Policy > Default Authentication come mostrato nell'immagine.

Cambiare l'autenticazione predefinita Realm in LDAP e selezionare LDAP Login Domain creato.

Verifica

Fare riferimento a questa sezione per verificare che la configurazione funzioni correttamente.



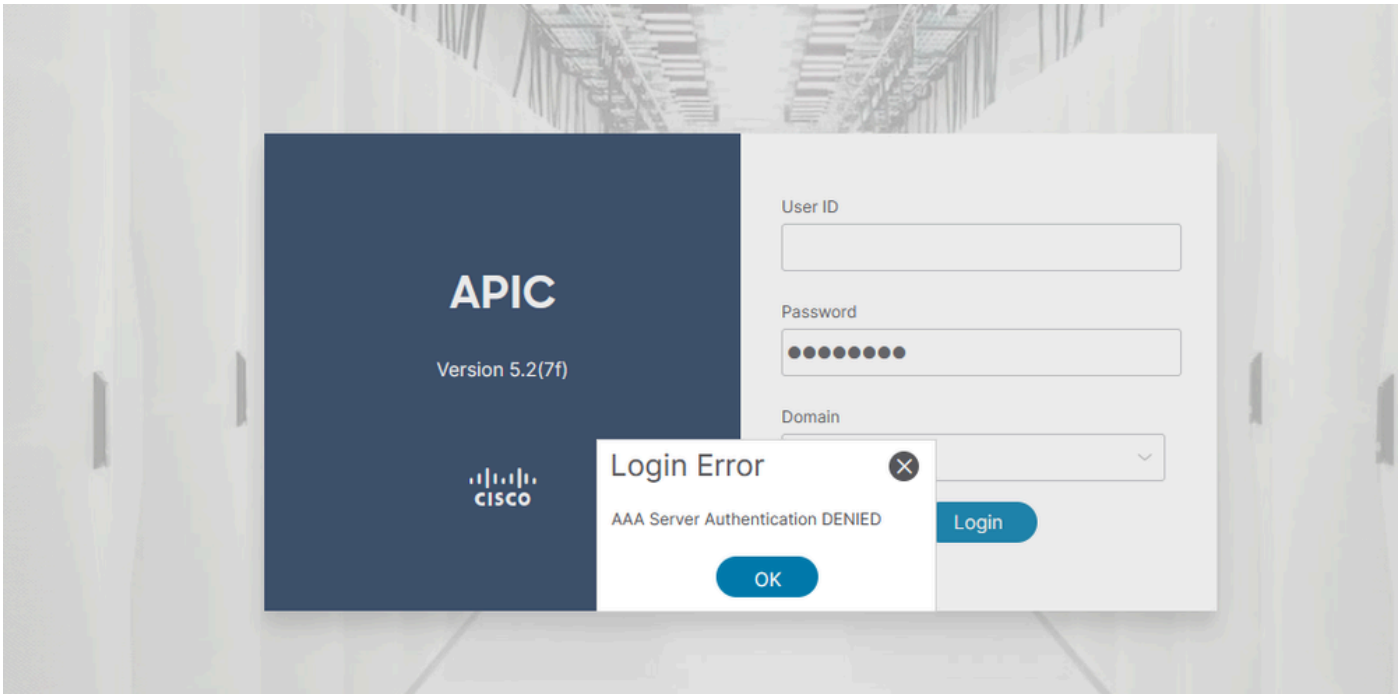


Verificare che l'utente LDAP User1 esegua correttamente l'accesso ad APIC con il ruolo di amministratore e il privilegio di scrittura.

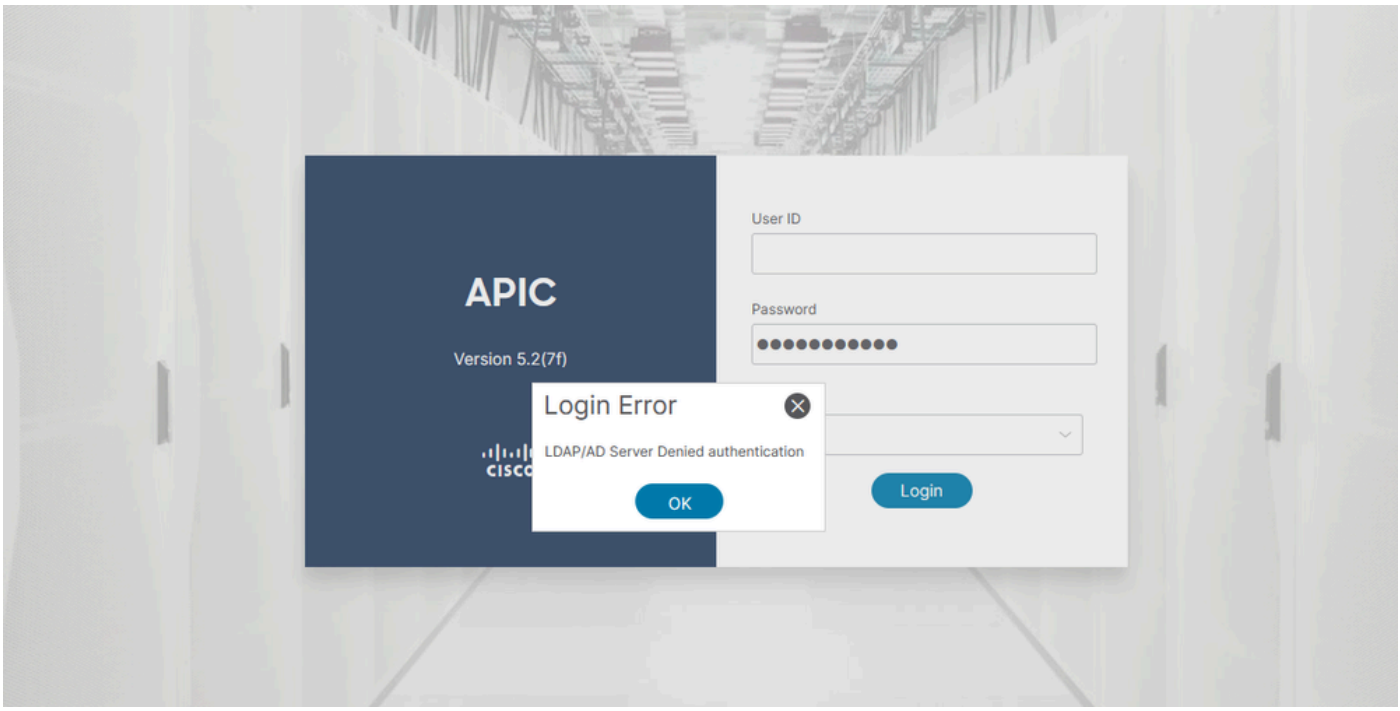
Risoluzione dei problemi

Le informazioni contenute in questa sezione permettono di risolvere i problemi relativi alla configurazione.

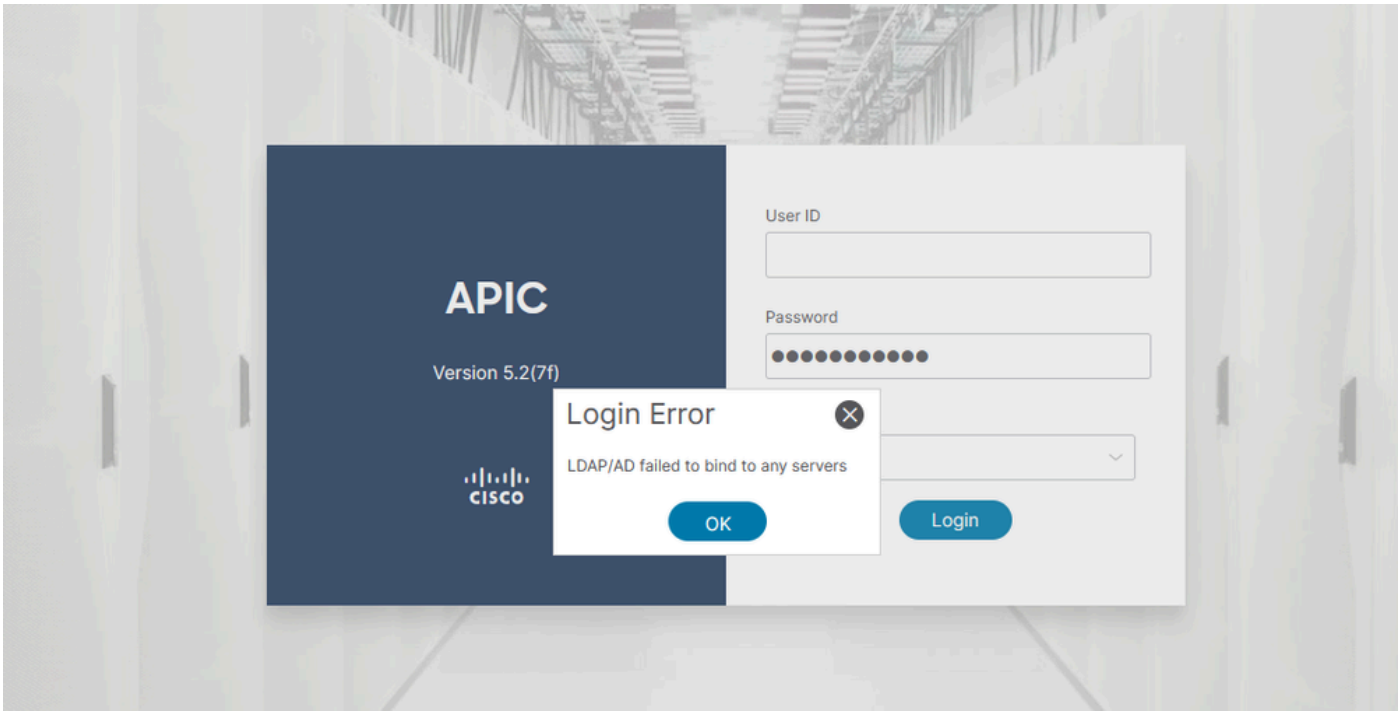
Se l'utente non esiste nel database LDAP:



Se la password è errata:



Quando il server LDAP non è raggiungibile:



Comandi per la risoluzione dei problemi:

<#root>

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

Per ulteriore assistenza, contattare Cisco TAC.

Informazioni correlate

- Guida alla configurazione della sicurezza di Cisco APIC, versione 5.2(x)
- Supporto tecnico Cisco e download

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).