

aci LDAP ۋە قىداصىم نىوكت

تايىوت حملا

[قىدقملا](#)

[قىساس ألا تابل طتملا](#)

[تابل طتملا](#)

[قىمدختسملا تانوكملا](#)

[نىوكتلى](#)

[تانيوكتلى](#)

[ىلۇغ نىيەمدختسماتاعومىجم عاشنارا 1. ۋە ئەنلەپ](#)

[ىلۇغ ئەنلەپ ئەنلەپ 2. ۋە ئەنلەپ](#)

[ىلۇغ ئەنلەپ ئەنلەپ 3. ۋە ئەنلەپ](#)

[ىلۇغ ئەنلەپ ئەنلەپ 4. ۋە ئەنلەپ](#)

[ىلۇغ ئەنلەپ ئەنلەپ 5. ۋە ئەنلەپ](#)

[قىحلىانم قىچتلى](#)

[اهالىسا او ئاطخىلا فاشكىتسا](#)

[قلص تاذ تامولعيم](#)

قىدقملا

لىلدىلا ىلإ فيفخلا لوصوللا لوكوتورب قىداصىم نىوكت ئېفيك دنتسىملا اذه حضوى (ACI) تاقىبىتلىلا ىلۇغ ئەنلەپ ئەنلەپ (LDAP).

قىساس ألا تابل طتملا

تابل طتملا

ئېلاتلا عيضاوملاب ئەفرۇم كېدل نوكت نأب Cisco يصوت:

- ىلۇغ ئەنلەپ ئەنلەپ (AAA) ئەبسا حمل او ضيوفتلا او قىداصىم ئەسايىس تاقىبىتلىلا
- LDAP

قىمدختسملا تانوكملا

ئېلاتلا ئىداملا تانوكملا وجماربلا تارادصىلا ىلإ دنتسىملا اذه يف ئەدراؤلا تامولعيملا دنتسىت:

- رادصىلا Cisco نم (APIC) ئەساس ألا ئېنبللا ئەسايىس قىبىتلىپ ئەصاخلا مەجھتلىلا ئەدھو 5.2(7f)
- Ubuntu 20.04 ئەم SLAPD و phpLDAPadmin

ئەصاخ ئېلىمۇم ئېئىب يف ئەدھو ئەنلەپ ئەنلەپ دنتسىملا اذه يف ئەدراؤلا تامولعيملا ئاشنارا مەتنىڭ اذا (يىشارتفا) حوسىم نىوكتىپ دنتسىملا اذه يف قىمدختسملا ئەزەج ألا ئەيىمچ تادب.

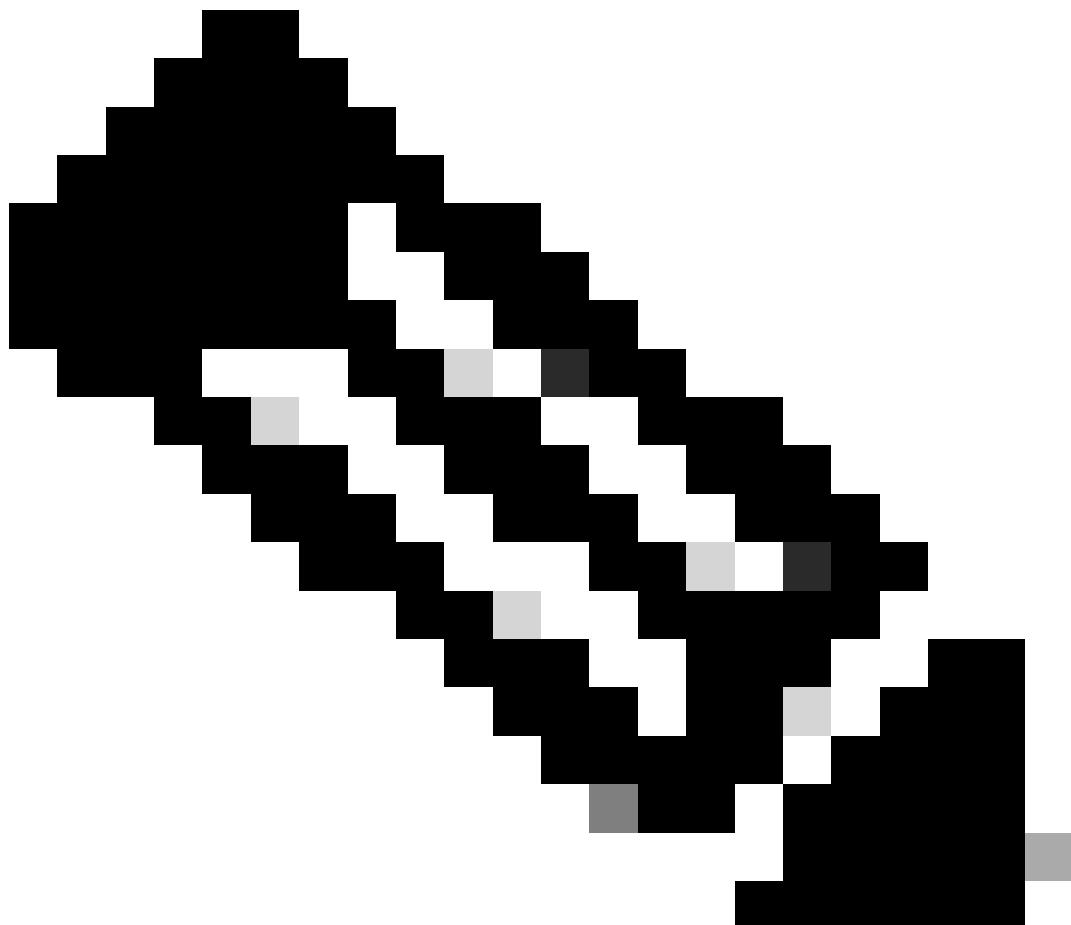
رماً يأْل لمتحمل ريا ثأتلل كمهف نم دكأْتف ،ليغشتلا ديق كتكبش.

نيوكتلا

مادختس او LDAP مداعم لماكتلا لجأْنم APIC نيوكت ئيفيك مسقل اذه فصي ئيضاًرتفالا ئقاداصمل ارقيرطك.

تانيوكتلا

ىلع نيمدختسم/تاعومجم ئاشنإ 1. ۋوطخلانى Ubuntu phpLDAPadmin



بيولالا ىلع يمسرلا Ubuntu عقوم ىلا عجرا ، LDAP مداعك Ubuntu نيوكت لجأْنم : ئاظحالم 2. ۋوطخلاب أدبا ، دوجوم LDAP مداعك ئانه ناك اذى . ئلماش تاداشرا ىلع لوصحلل

تاعومجم ىلا (User1 و User2) نامدختسم يمتنى و ئيساسلىا DN ئكبسش dc=dclab,dc=com دنتسمل اذه يف (DCGgroup).

The screenshot shows the phpLDAPadmin interface. On the left, under 'My LDAP Server', there's a tree view of LDAP entries. It includes a schema browser, search, refresh, info, import, export, and logout buttons. The user is logged in as 'cn=admin'. The tree view shows a root node 'dc=dclab,dc=com' with three children: 'cn=admin', 'ou=Groups (1)', and 'ou=Users (2)'. 'ou=Groups (1)' contains a 'cn=DCGroup' entry with a 'Create new entry here' link. 'ou=Users (2)' contains two entries: 'cn=User1' and 'cn=User2', each with a 'Create new entry here' link. On the right, a message box displays 'Authenticate to server' with the sub-message 'Successfully logged into server.'

2. ۋەطخىل ئىل ع LDAP ىرفووم نىوكت.

ةروصلار يىف حضورم وە امك APIC ئىل لقتنى Admin > AAA > Authentication > LDAP > Providers.

The screenshot shows the Cisco ACI AAA configuration interface. Under 'Authentication', the 'LDAP' tab is selected. A table lists a single LDAP provider: 'LDAP Provider - 10.124.3.6'. The provider details are as follows:

| Host Name | Description | Port | SSL Enabled | Timeout (sec) |
|------------|-------------|------|-------------|---------------|
| 10.124.3.6 | | 389 | False | 30 |

The 'Properties' section provides more configuration options:

- Host Name (or IP Address): 10.124.3.6
- Description: optional
- Port: 389
- Bind DN: cn=admin,dc=dclab,dc=com
- Base DN: ou=Users,dc=dclab,dc=com
- Password: (password field)
- Confirm Password: (password field)
- Timeout (sec): 30
- Retries: 1
- Enable SSL: (checkbox checked)
- Filter: cn+UserId
- Attribute: title
- SSL Certificate Validation Level: Strict
- Management EPG: default (Out-of-Band)
- Server Monitoring: Enabled

اذه مادختساب ئاق داصملاب APIC موقى. Bind DN: LDAP لباقم ئاق داصملل اهم دختسىت يىتلار دامتعالا تانايىپ ب دصقىي. لىلدىلا نع مالعتسالل باسحىلار.

اهىل ع فرعىتلار مادختسىملىكا تالاخدا نع ثىحبلىل ئىعجمرم ئاطقنىڭ APIC ئاسألا مادختسىا مىتى: يىسالا DN.

أاشنەملى رورملا ئەملىك ب ئەطبىترملى، LDAP مادخ ئىل لوصولل ئىرورمىلى رورملا ئەملىك يە هەزه: رورملا ئەملىك ب صاخلى لىخاد.

لەاسىتم راتخت نا بجى، اىتاذ ئۇقۇم ئەدەش وا يىلخاد قىصىم مادختسىت تىنك اذا: SSL نىكىت.

كىرتىشىم مسا هل نئاكك مادختسىملى فېرىعەت مىتى امدىنەن وە يىضارىت فالا ئىفصىتلار لىماع دادع cn=\$userid نونوکىي: ئەي فىصىتلار لىماع (CN).

انه نيراي خ (ACI) لوصول ايف مكحفل او رفوت .راودا او عومجملا ئيوضع ديتحت ئامسلا مادختسا متى :ئامسلا كلذل ،CiscoAVPair.memberOf RFC2307bis ئامس يه RFC2307 نم OpenLDAP ققحتى ،ايلاح .عومجملا ئيوضع ديتحت لجأ نم title كلذ نم الدب ھ مادختسا متى .

ةرادا جەن بسح كلذو ،قاطنلا جراخ وأ قاطنلا لخاد EPG لالخ نم اما LDAP مداخب لاصتالا متى :ةرادا EPG (EPG) ئامسلا طاقن ئاعومجم راتخملار كبسلا .

3. ۋەطخلار ئاعومجم LDAP ئىيىعىت دعاوقى نىوكت .

ةروصلار ئىف حضوم وە امك Admin > AAA > Authentication > LDAP > LDAP Group Map Rules ئىلى لقتنا .ةمىاقلا طىرش ئىف .

| Name | Description | Group DN |
|------------------|-------------|--------------------------------------|
| LDAPGroupMapRule | optional | cn=DCGroup,ou=Groups,dc=dclab,dc=com |

LDAP Group Map Rule - LDAPGroupMapRule

Properties

- Name: LDAPGroupMapRule
- Description: optional
- Group DN: cn=DCGroup,ou=Groups,dc=dclab,dc=com
- Security Domains:

 - Name: Security Domain all
 - Access: writePriv
 - Role: admin

Show Usage Close Submit

يىف نومدختسمىلا عتمتىي DCGgroup موقى ،كلذ لوؤسىملا تازايتىماب Group DN cn=DCGroup, ou=Groups, dc=dclab, dc=com .All راودا admin ع write privilege امىيىصختى .

4. ۋەطخلار ئاعومجم طئارخ نىوكت .

ةروصلار ئىف حضوم وە امك Admin > AAA > Authentication > LDAP > LDAP Group Maps ئىلى لقتنا .ةمىاقلا طىرش ئىف .

Authentication

AAA **LDAP** RADIUS TACACS SAML RSA DUO OAuth 2

Providers LDAP Group Map Rules **LDAP Group Maps**

Name Description

LDAPGroupMap

LDAP Group Map - LDAPGroupMap

Policy History

Description: optional

Rules:

Name

LDAPGroupMapRule

Show Usage Close Submit

This screenshot shows the 'LDAP Group Maps' configuration screen. At the top, there are tabs for AAA, LDAP, RADIUS, TACACS, SAML, RSA, DUO, and OAuth 2. Below that, sub-tabs for Providers, LDAP Group Map Rules, and LDAP Group Maps are shown, with 'LDAP Group Maps' being the active tab. On the left, a tree view shows a node named 'LDAPGroupMap'. The main area is titled 'LDAP Group Map - LDAPGroupMap' and contains sections for Properties (Description: 'optional') and Rules (a list box containing 'LDAPGroupMapRule'). At the bottom are buttons for Show Usage, Close, and Submit.

بروکس لی ایف حضور م و او امکن Admin > AAA > Authentication > AAA > Policy > Create a login domain طریق لی ایف.

Authentication

AAA LDAP RADIUS TACACS SAML RSA DUO OAuth 2

Properties

Remote user login policy: No Login

Use ICMP reachable providers only: true

Default Authentication

Realm: LDAP

LDAP Login Domain: LDAP

Fallback Domain Availability: Always Available

Console Authentication

Realm: Local

Name Description Realm

fallback Local

LDAP Group Map

Name: LDAP

Realm: LDAP

Description: optional

Auth Choice: CiscoAVPair LdapGroupMap

LDAP Group Map: LDAPGroupMap

Providers:

| Name | Priority | Description |
|------------|----------|-------------|
| 10.124.3.6 | 1 | |

Show Usage Close Submit

Reset Submit

روصلایف حضویم وہ امک Admin > AAA > Authentication > AAA > Policy > Default Authentication

Authentication

AAA LDAP RADIUS TACACS SAML RSA DUO OAuth 2

Properties

Remote user login policy: No Login
Use ICMP reachable providers only: true

Default Authentication

Realm: LDAP
LDAP Login Domain: LDAP
Fallback Domain Availability: Always Available
Console Authentication

Realm: Local

Name Description Realm

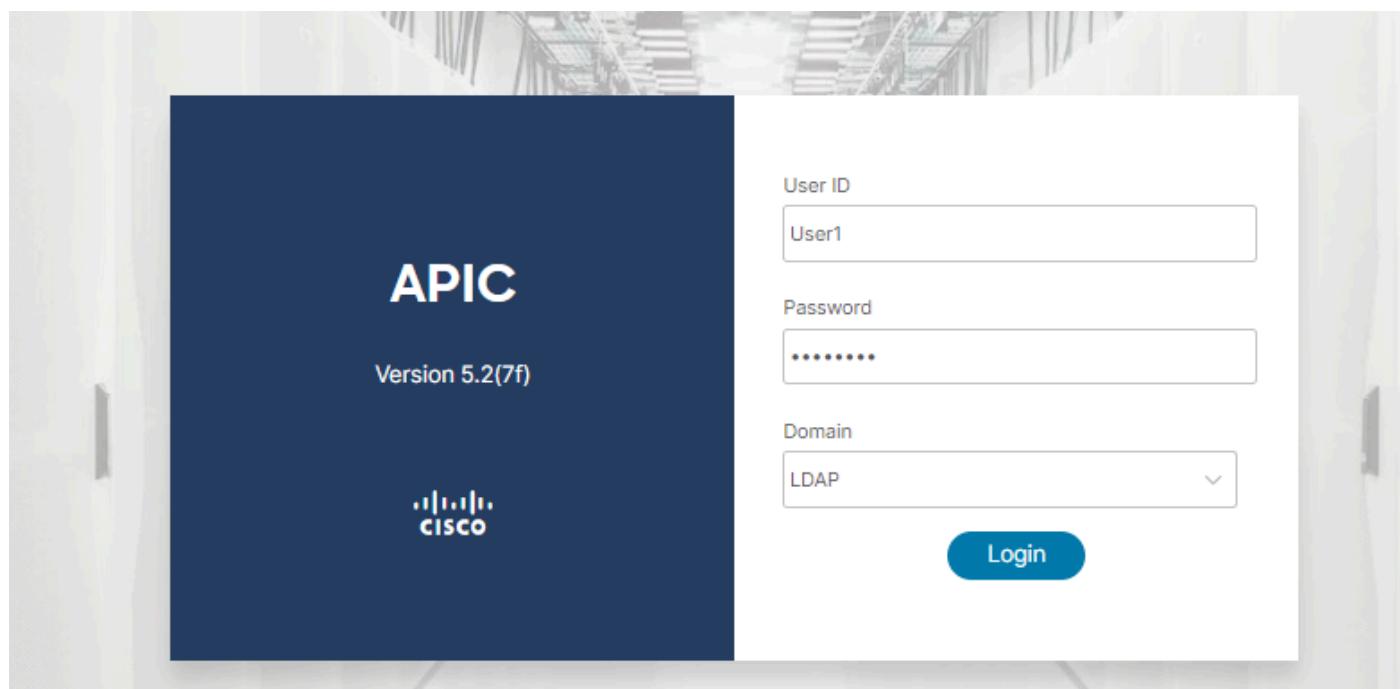
fallback Local

LDAP LDAP

أشنملا ددحو LDAP Realm لى| ارتفالا قداصلما ريفغتب مق.

وحصلنا نم ققحتلا

حيحص لكشب نيوكتلار مع ديكأتل مسقلنا اذه مدخلتسا.

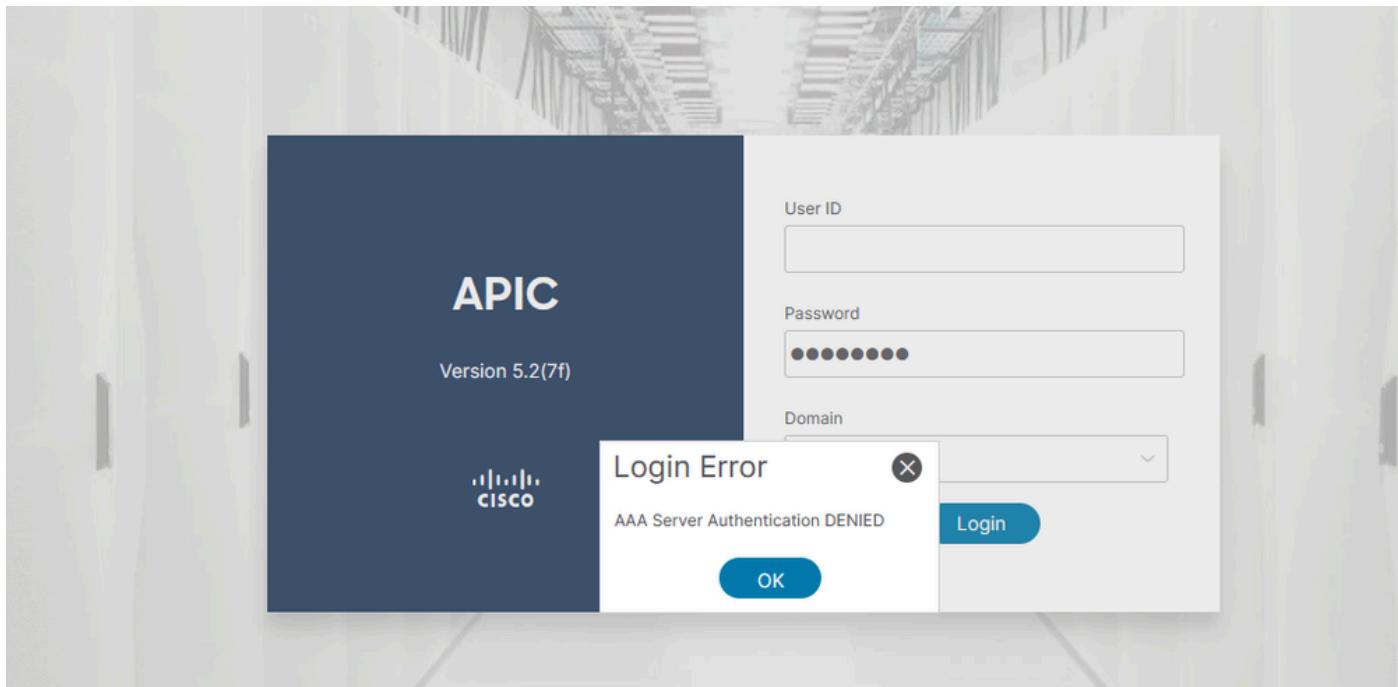


ۋەتاك زايىتما رىي دم رو دىم حاجنې APIC User1 يف لىمعتىسىم لىجس LDAP نا تىققىد.

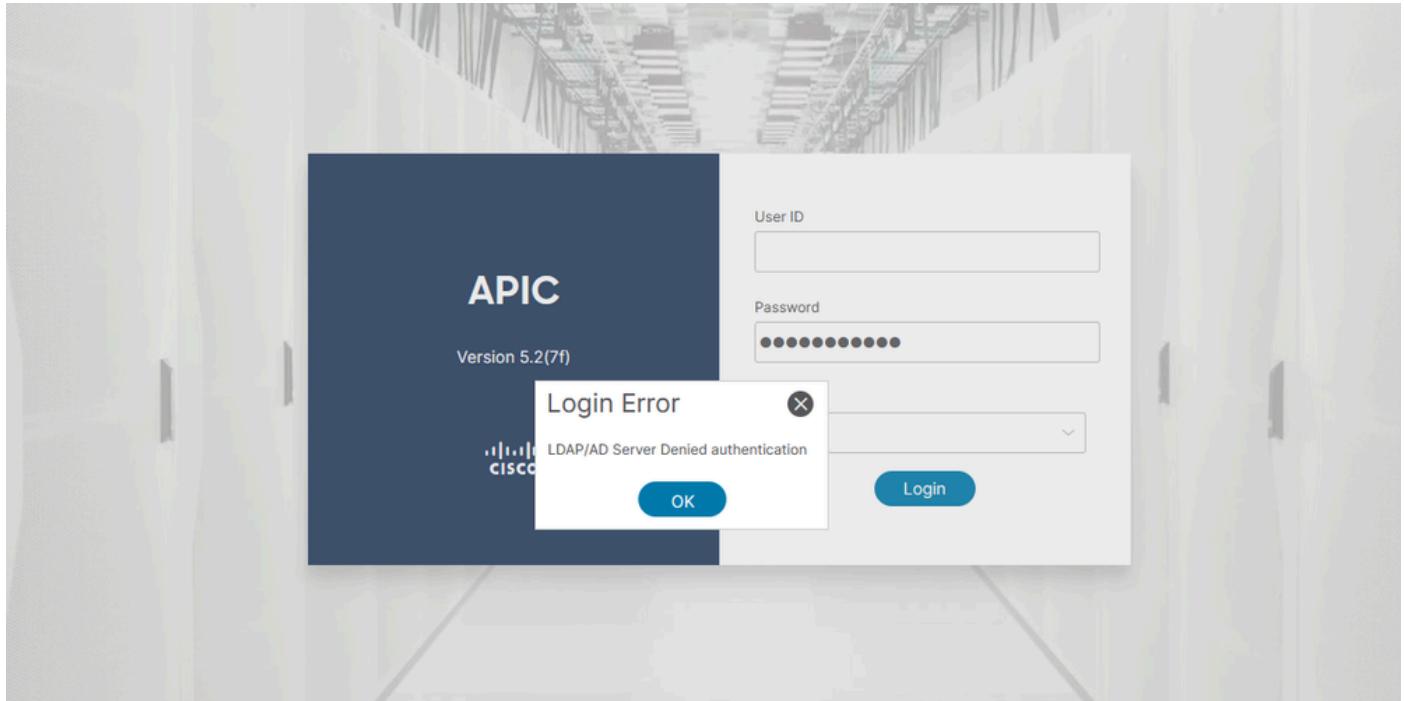
اچالىص او ئاطخىلار فاش كىتسا

اچالىص او نىوكتىلا ئاطخىلار فاش كىتسا اهمادختىسى كىممى تامولۇم مىسىلى اذه رفۇي.

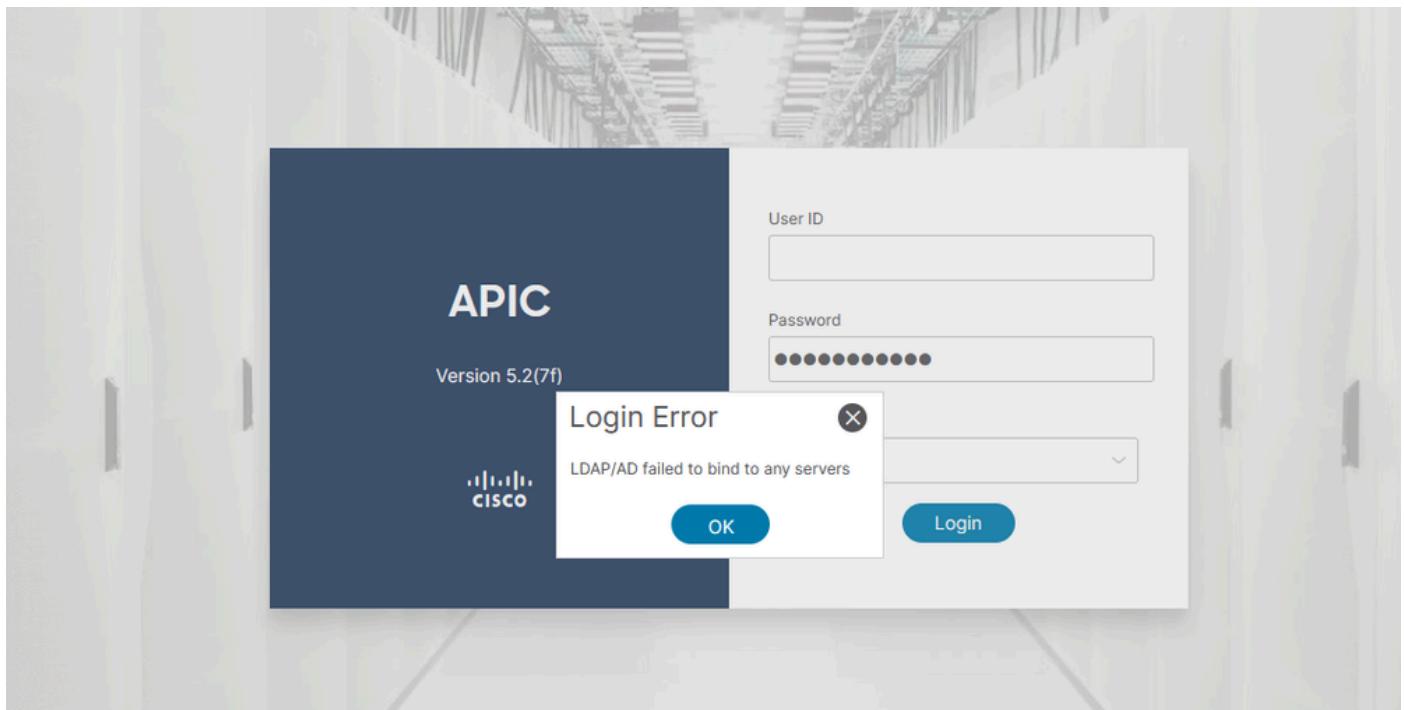
تانايىب ۋەداعىق يف دوجوم رىغ مىدىتىسىملا نوکىي امىدىع LDAP:



حىچىص رىغ رورملا ئەملىك نوكت امىدىع:



مدادخیل امدادنی رذعتی وصولاً LDAP:



اهم امور اس کے تصور میں رہا۔

<#root>

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

cisco TAC. نا جاتحي تنا رييثك اسما دعه ب لصت

مـولـعـاـمـهـاـذـاـتـصـلـ

- Cisco نـمـتـاقـيـبـطـتـلـاـقـجـمـرـبـوـنـامـأـنـيـوـكـلـيـلـدـ 5.2(x)
- Cisco نـمـتـالـيـزـنـتـلـاوـيـنـفـلـاـمـعـدـلـاـ

هـ ذـ هـ لـ وـ حـ جـ رـ تـ لـ ا

ةـ يـ لـ آـ لـ اـ تـ اـ يـ نـ قـ تـ لـ اـ نـ مـ مـ حـ مـ وـ عـ مـ اـ دـ خـ تـ سـ اـ بـ دـ نـ تـ سـ مـ لـ اـ اـ ذـ هـ تـ مـ جـ رـ تـ
لـ اـ عـ لـ اـ ءـ اـ حـ نـ اـ عـ يـ مـ جـ يـ فـ نـ يـ مـ دـ خـ تـ سـ مـ لـ لـ مـ عـ دـ ئـ وـ تـ حـ مـ يـ دـ قـ تـ لـ ةـ يـ رـ شـ بـ لـ اـ وـ
اـ مـ كـ ةـ قـ يـ قـ دـ نـ وـ كـ تـ نـ لـ ةـ يـ لـ آـ ةـ مـ جـ رـ تـ لـ ضـ فـ اـ نـ اـ ةـ ظـ حـ اـ لـ مـ ئـ جـ رـ يـ .ـ صـ اـ خـ لـ اـ مـ هـ تـ غـ لـ بـ
يـ لـ خـ تـ .ـ فـ رـ تـ حـ مـ مـ جـ رـ تـ مـ اـ هـ دـ قـ يـ يـ تـ لـ اـ ةـ يـ فـ اـ رـ تـ حـ اـ لـ اـ ةـ مـ جـ رـ تـ لـ اـ عـ مـ لـ اـ حـ لـ اـ وـ
ىـ لـ إـ أـ مـ ئـ اـ دـ عـ وـ جـ رـ لـ اـ بـ يـ صـ وـ تـ وـ تـ اـ مـ جـ رـ تـ لـ اـ هـ ذـ هـ ةـ قـ دـ نـ عـ اـ هـ تـ يـ لـ وـ ئـ سـ مـ
(رـ فـ وـ تـ مـ طـ بـ اـ رـ لـ اـ)ـ يـ لـ صـ أـ لـ اـ يـ زـ يـ لـ جـ نـ إـ لـ اـ دـ نـ تـ سـ مـ لـ اـ).