

LDAP configureren in UCS Manager

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Achtergrondinformatie](#)

[Configureren](#)

[Een lokaal verificatiedomein maken](#)

[Een LDAP-provider maken](#)

[Configuratie LDAP-groepsregel](#)

[Een LDAP-provider-groep maken](#)

[Een LDAP-groepstoewijzing maken](#)

[Een LDAP-verificatiedomein maken](#)

[Verifiëren](#)

[Veelvoorkomende LDAP-problemen.](#)

[Problemen oplossen](#)

[Gerelateerde informatie](#)

Inleiding

Dit document beschrijft de configuratie voor toegang tot externe servers met het LDAP-protocol in ONZE Unified Computing System Manager Domain (UCSM).

Voorwaarden

Vereisten

Cisco raadt kennis van deze onderwerpen aan:

- **Unified Computing System Manager Domain (UCSM)**
- Lokale en externe verificatie
- **Lightweight Directory Access Protocol (LDAP)**
- **Microsoft Active Directory (MS-AD)**

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- **Cisco UCS 6454 Fabric Interconnect**
- UCS M versie 4.0(4k)
- **Microsoft Active Directory (MS-AD)**

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een

opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Achtergrondinformatie

Lightweight Directory Access Protocol (LDAP) is een van de kernprotocollen die zijn ontwikkeld voor gidsdiensten die gebruikers en hun toegangsrechten tot IT-middelen veilig beheren.

De meeste directorydiensten gebruiken nog steeds LDAP, hoewel ze ook extra protocollen zoals Kerberos, SAML, RADIUS, SMB, Oauth en anderen kunnen gebruiken.

Configureren

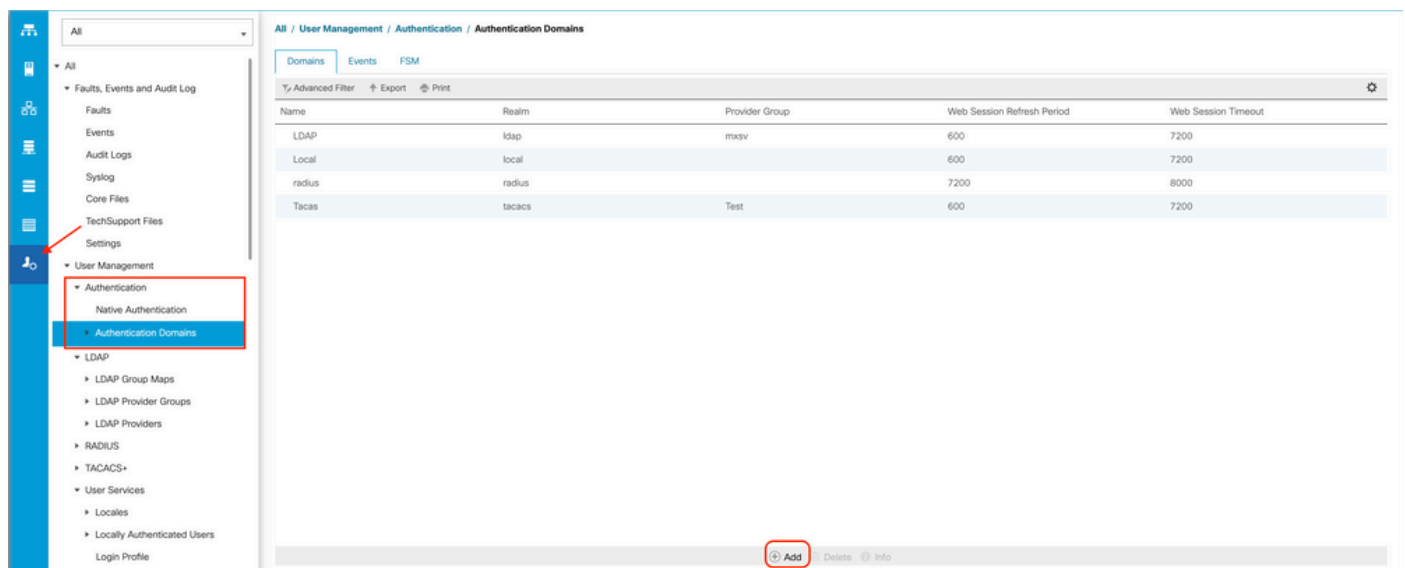
Voordat u begint

Inloggen op Cisco UCS Manager GUI als administratieve gebruiker.

Een lokaal verificatiedomein maken

Stap 1. In het Navigation deelvenster klikt u op het Admin tabblad.

Stap 2. Op de Admin tabblad uitvouwen All > User Management > Authentication



The screenshot shows the Cisco UCS Manager GUI. On the left is a navigation menu with a tree structure. The 'Authentication Domains' item is highlighted with a red box. On the right, the 'Authentication Domains' table is displayed with the following data:

Name	Realm	Provider Group	Web Session Refresh Period	Web Session Timeout
LDAP	ldap	mxsv	600	7200
Local	local		600	7200
radius	radius		7200	8000
Tacacs	tacacs	Test	600	7200

At the bottom of the table, there is an 'Add' button circled in red.

Stap 3. Rechtsklik Authentication Domains en selecteer Create a Domain.

Stap 4. Voor de Name veld, type Local.

Stap 5. Voor de Realm klikt u op de Local keuzerondje.

General	Events
Actions	Properties
Delete	Name : Local
	Web Session Refresh Period (sec) : 600
	Web Session Timeout (sec) : 7200
	Realm : <input checked="" type="radio"/> Local <input type="radio"/> Radius <input type="radio"/> Tacacs <input type="radio"/> Ldap
<input type="button" value="OK"/> <input type="button" value="Apply"/> <input type="button" value="Cancel"/> <input type="button" value="Help"/>	

Stap 6. Klik ok.

Een LDAP-provider maken

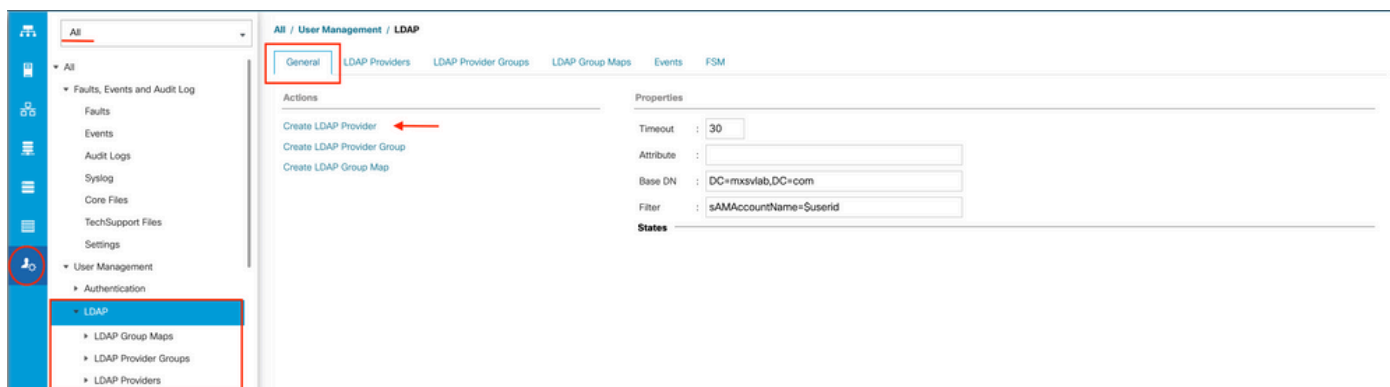
Deze voorbeeldconfiguratie bevat geen stappen om LDAP met SSL te configureren.

Stap 1. In het Navigation deelvenster klikt u op het Admin tabblad.

Stap 2. Op de Admin tabblad uitvouwen All > User Management > LDAP.

Stap 3. In het work deelvenster klikt u op het General tabblad.

Stap 4. In het Actions gebied klikt u op Create LDAP Provider



Stap 5. In het Create LDAP Provider pagina van de wizard, voert u de juiste informatie in:

- In het Hostnameveld typt u het IP-adres of de hostnaam van de AD-server.
- In het order veld, accepteert u de lowest-available standaard.
- In het BindDN veld, kopieer en plak de BindDN van uw AD-configuratie.

Voor deze voorbeeldconfiguratie is de waarde BindDN
CN=sbind,OU=CiscoUCS,DC=mxsvlab,DC=com.

- In het **BaseDN** veld, kopieer en plak de BaseDN van uw AD-configuratie.

Voor deze voorbeeldconfiguratie is de BaseDN-waarde **DC=mxsvlab,DC=com**.

- Laat de **Enable SSL** selectievakje niet ingeschakeld.
- In het **Port** veld, accepteert de standaardinstelling 389.
- In het **Filter** het veld, kopieert en plakt het filterkenmerk van uw AD-configuratie.

Cisco UCS gebruikt de filterwaarde om te bepalen of de gebruikersnaam (die op het aanmeldingsscherm wordt verstrekt door **Cisco UCS Manager**) is in AD.

Voor deze voorbeeldconfiguratie is de filterwaarde **sAMAccountName=\$userid**, waarbij \$userid is de user name in het **Cisco UCS Manager** inlogscherm.

- Laat de **Attribute** veldspatie.
- In het **Password Typ** in het veld het wachtwoord voor de bind-account die in AD is ingesteld.

Als u terug moet gaan naar de **Create LDAP Provider** wizard om het wachtwoord opnieuw in te stellen, wordt niet gealarmeerd als het wachtwoordveld leeg is.

Het **Set: yes** bericht dat naast het wachtwoordveld verschijnt, geeft aan dat er een wachtwoord is ingesteld.

- In het **Confirm Password Typ** in het veld het wachtwoord voor de bind-account die in AD is ingesteld.
- In het **Timeout** veld, accepteert u de 30 standaard.
- In het **vendor** in het veld selecteert u het keuzerondje voor **MS-AD** voor Microsoft Active Directory.

Create LDAP Provider

1 Create LDAP Provider

2 LDAP Group Rule

Hostname/FQDN (or IP Address) : 10.31.123.60

Order : lowest-available

Bind DN : CN=ucsbind,OU=CiscoUCS,DC=mxsvlab,DC=com

Base DN : DC=mxsvlab,DC=com

Port : 389

Enable SSL :

Filter : sAMAccountName=\$userid

Attribute :

Password :

Confirm Password :

Timeout : 30

Vendor : Open Ldap MS AD

< Prev Next > Finish Cancel

Stap 6. Klik **Next**

Configuratie LDAP-groepsregel

Stap 1. Op deLDAP Group Rule pagina van de wizard, vult u de volgende velden in:

- Voor de **Group Authentication** veld klikt u op de **Enable** keuzerondje.
- Voor de **Group Recursion** veld klikt u op de **Recursive** keuzerondje. Hierdoor kan het systeem de zoekactie op niveau doorzetten tot het een gebruiker vindt.

Indien de **Group Recursion** is ingesteld op **Non-Recursive**Maar het beperkt UCS tot een zoekopdracht op het eerste niveau, zelfs als de zoekopdracht geen gekwalificeerde gebruiker vindt.

- In het **Target Attribute** veld, accepteert u de **memberOf** standaard.

Stap 2. Klik in **Finish**.

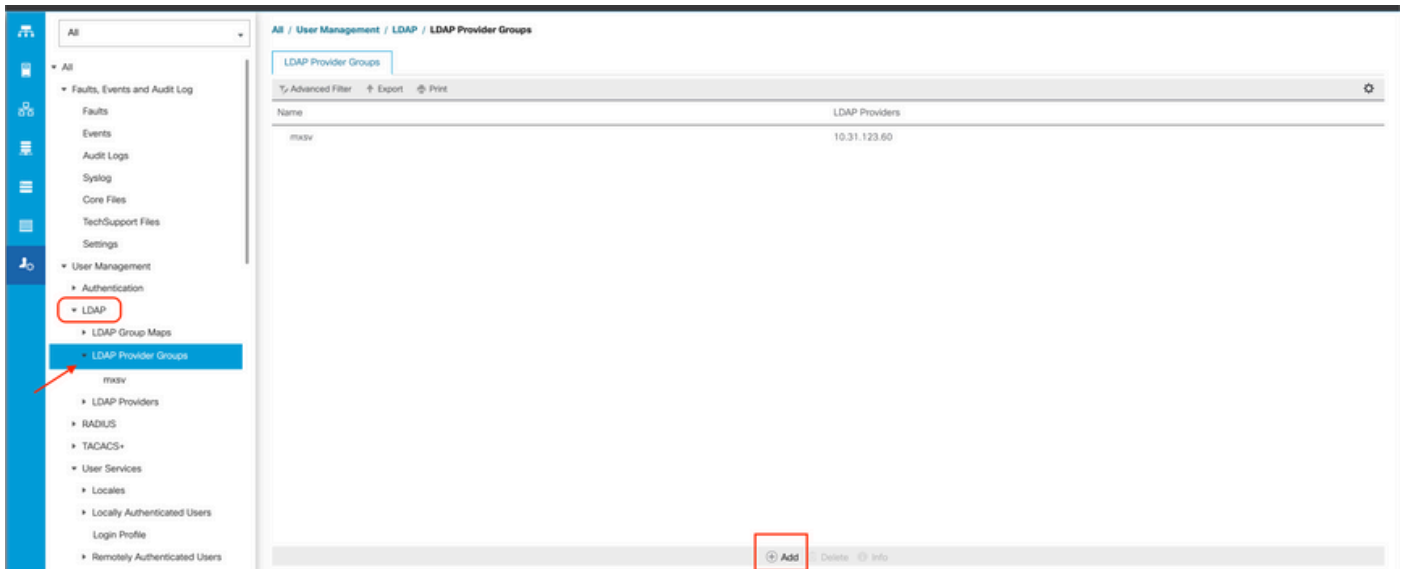
Opmerking: in een scenario in de echte wereld hebt u waarschijnlijk meerdere LDAP-providers. Voor meerdere LDAP-providers herhaalt u de stappen om de LDAP Group Rule te configureren voor elke LDAP provider. In deze voorbeeldconfiguratie is er echter maar één LDAP-provider, dus dit is niet nodig.

Het IP-adres voor de AD-server wordt weergegeven in het navigatiedeelvenster **onder**

LDAP>LDAP-providers.

Een LDAP-provider-groep maken

Stap 1. Klik met de rechtermuisknop in het navigatiedeelvenster **LDAP Provider Groups** en selecteer **Create LDAP Provider Group**.



Stap 2. In het **Create LDAP Provider Group** dialoogvenster vult u de informatie op de juiste manier in:

- In het **Name** veld voert u een unieke naam in voor de groep, zoals **LDAP Providers**.
- In het **LDAP Providers** Kies in de tabel het IP-adres voor uw AD-server.
- Klik op de knop **>>** om de AD-server aan uw **Included Providers** tabel.

Create LDAP Provider Group

Name : mxsv

LDAP Providers		
Hostname	Bind DN	Port
10.31.123....	CN=ucsbind,...	389

>>
<<

Included Providers	
Name	Order
No data available	

OK Cancel

Stap 3. Klik op OK.

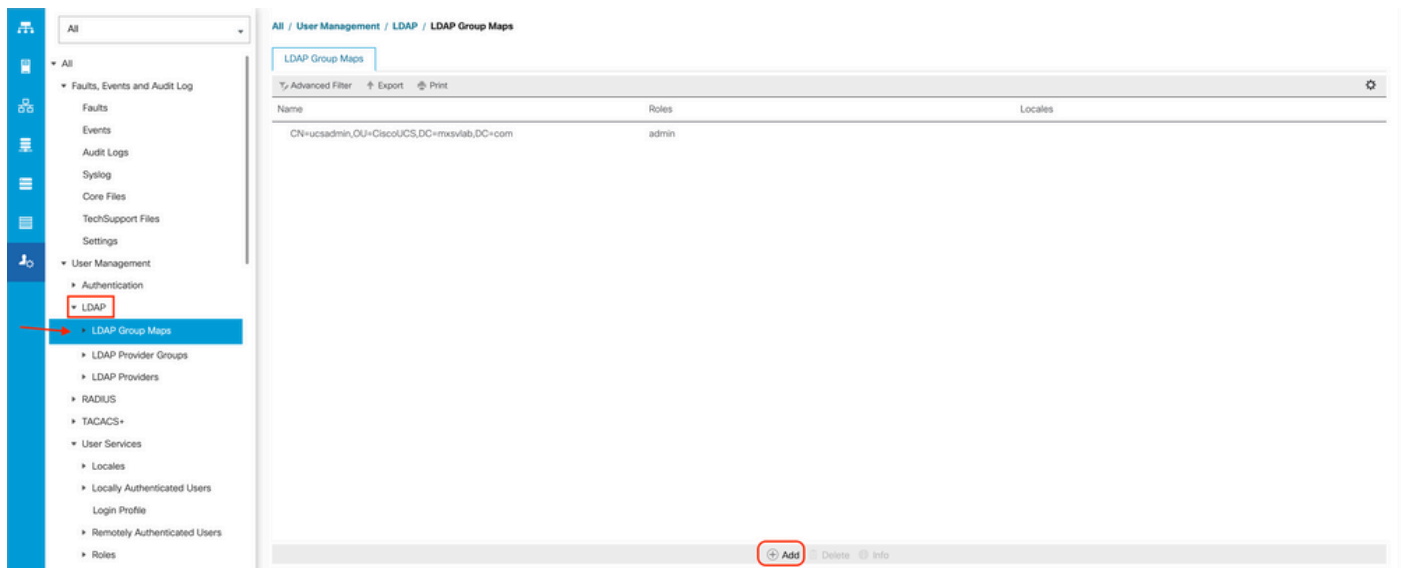
Uw providergroep wordt weergegeven in de **LDAP Provider Groups** map.

Een LDAP-groepstoewijzing maken

Stap 1. Klik in het navigatiedeelvenster op de **Admin** tabblad.

Stap 2. Op de **Admin** tabblad uitvouwen **All > User Management > LDAP**.

Stap 3. Klik in het werkvenster op **Maken LDAP Group Map**.



Stap 4. In het **Create LDAP Group Map** dialoogvenster vult u de informatie op de juiste manier in:

- In het **LDAP Group DN** de waarde die u in de sectie voor de configuratie van de AD-server voor uw LDAP-groep hebt, kopiëren en plakken.

De in deze stap gevraagde LDAP Group DN-waarde brengt de voorname naam in kaart voor elk van de groepen die u in AD onder UCS-groepen hebt gemaakt.

Om deze reden moet de DN-waarde voor de groep die in Cisco UCS Manager is ingevoerd, exact overeenkomen met de DN-waarde voor de groep in de AD-server.

In deze voorbeeldconfiguratie is deze waarde **CN=ucsadmin, OU=CiscoUCS, DC=sampladesign, DC=com**.

- In het **Roles** klikt u op de **Admin** vink het vakje aan en klik op **OK**.

Klik op het aanvinkvakje voor een rol geeft aan dat u beheerdersrechten wilt toewijzen aan alle gebruikers die in de groepskaart zijn opgenomen.

Create LDAP Group Map



LDAP Group DN : CN=ucsadmin,OU=CiscoUCS,DC=mxsvlab,DC=com

Roles

- aaa
- admin ←
- facility-manager
- network
- OnlyKVM
- operations
- read-only
- server-compute
- server-equipment
- server-profile
- server-security
- stats
- storage

Locales

- JaviTest
- JosueLoc
- Test

OK

Cancel

Stap 5. Maak nieuwe LDAP-groepskaarten (gebruik de informatie die u eerder van AD heeft opgenomen) voor elk van de overgebleven rollen in de AD-server die u wilt testen.

Volgende: Maak uw LDAP-verificatiedomein.

Een LDAP-verificatiedomein maken

Stap 1. Op de Beheerder tabblad uitvouwen All > User Management > Authentication

Stap 2. Rechtsklik **Verificatie** Authentication Domains en selecteer Create a Domain.

Name	Realm	Provider Group	Web Session Refresh Period	Web Session Timeout
LDAP	ldap	mxsv	600	7200
Local	local		600	7200
radius	radius		7200	8000
Tacacs	tacacs	Test	600	7200

Stap 3. In de **Create a Domain** het volgende dialoogvenster voltooien:

- In het **Name** veld, typt u een naam voor uw domein zoals LDAP.
- In het **Realm** gebied klikt u op de **Ldap** keuzerondje.
- Van de **Provider Group** vervolgkeuzelijst selecteert u de **LDAP Provider Group** eerder gemaakt en klik op **OK**.

Properties for: LDAP ✕

General

Events

Actions

Delete

Properties

Name : **LDAP**

Web Session Refresh Period (sec) :

Web Session Timeout (sec) :

Realm : Local Radius Tacacs **Ldap**

Provider Group :

Het verificatiedomein wordt weergegeven onder **Authentication Domains**.

Verifiëren

Pingen op LDAP Provider IP voor FQDN:

```
UCS-AS-MXC-P25-02-B-A# connect local-mgmt
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (c) 2009, Cisco Systems, Inc. All rights reserved.
The copyrights to certain works contained in this software are
owned by other third parties and used and distributed under
license. Certain components of this software are licensed under
the GNU General Public License (GPL) version 2.0 or the GNU
Lesser General Public License (LGPL) Version 2.1. A copy of each
such license is available at
http://www.opensource.org/licenses/gpl-2.0.php and
http://www.opensource.org/licenses/lgpl-2.1.php
```

```
UCS-AS-MXC-P25-02-B-A(local-mgmt)# ping 10.31.123.60
PING 10.31.123.60 (10.31.123.60) from 10.31.123.8 : 56(84) bytes of data.
64 bytes from 10.31.123.60: icmp_seq=1 ttl=128 time=0.302 ms
64 bytes from 10.31.123.60: icmp_seq=2 ttl=128 time=0.347 ms
64 bytes from 10.31.123.60: icmp_seq=3 ttl=128 time=0.408 ms
```

Om de verificatie van NX-OS te testen, gebruikt u de `test aaa` opdracht (alleen beschikbaar bij NXOS).

We valideren de configuratie van onze server:

```
ucs(nxos)# test aaa server ldap <LDAP-server-IP-address or FQDN> <username> <password>
[UCS-AS-MXC-P25-02-B-A# connect nxos
Bad terminal type: "xterm-256color". Will assume vt100.
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (C) 2002-2020, Cisco and/or its affiliates.
All rights reserved.
The copyrights to certain works contained in this software are
owned by other third parties and used and distributed under their own
licenses, such as open source. This software is provided "as is," and unless
otherwise stated, there is no warranty, express or implied, including but not
limited to warranties of merchantability and fitness for a particular purpose.
Certain components of this software are licensed under
the GNU General Public License (GPL) version 2.0 or
GNU General Public License (GPL) version 3.0 or the GNU
Lesser General Public License (LGPL) Version 2.1 or
Lesser General Public License (LGPL) Version 2.0.
A copy of each such license is available at
http://www.opensource.org/licenses/gpl-2.0.php and
http://opensource.org/licenses/gpl-3.0.html and
http://www.opensource.org/licenses/lgpl-2.1.php and
http://www.gnu.org/licenses/old-licenses/library.txt.
[UCS-AS-MXC-P25-02-B-A(nx-os)# test aaa server ldap 10.31.123.60 admin Cisco123
```

Veelvoorkomende LDAP-problemen.

- Basisconfiguratie.
- Fout wachtwoord of ongeldige tekens.

- Verkeerde poort of filterveld.
- Geen communicatie met onze provider vanwege een firewall of proxyregel.
- FSM is niet 100%.
- Problemen met het certificaat.

Problemen oplossen

Controleer de UCS M LDAP-configuratie:

U moet ervoor zorgen dat de UCSM de configuratie met succes heeft geïmplementeerd vanwege de status van de Finite State Machine (FSM) wordt weergegeven als 100% compleet.

U kunt de configuratie als volgt controleren vanaf de opdrachtregel van onze UCSM:

```
ucs # scope security
ucs /security# scope ldap
ucs /security/ldap# show configuration
UCS-AS-MXC-P25-02-B-A /security # scope security
UCS-AS-MXC-P25-02-B-A /security # scope security
UCS-AS-MXC-P25-02-B-A /security # scope ldap
UCS-AS-MXC-P25-02-B-A /security/ldap # show configuration
scope ldap
  enter auth-server-group mxsv
    enter server-ref 10.31.123.60
      set order 1
    exit
  exit
enter ldap-group "CN=ucsadmin,OU=CiscoUCS,DC=mxsvlab,DC=com"
exit
enter server 10.31.123.60
  enter ldap-group-rule
    set authorization enable
    set member-of-attribute memberOf
    set traversal recursive
    set use-primary-group no
  exit
  set attribute ""
  set basedn "DC=mxsvlab,DC=com"
  set binddn "CN=ucsbind,OU=CiscoUCS,DC=mxsvlab,DC=com"
  set filter ""
  set order 1
  set port 389
  set ssl no
  set timeout 30
  set vendor ms-ad
!
  set password
  exit
  set attribute ""
  set basedn "DC=mxsvlab,DC=com"
  set filter sAMAccountName=$userid
  set timeout 30
exit
UCS-AS-MXC-P25-02-B-A /security/ldap # █
```

```
ucs /security/ldap# show fsm status
```

```
[UCS-AS-MXC-P25-02-B-A /security/ldap # show fsm status
```

```
FSM 1:  
  Status: Nop  
  Previous Status: Update Ep Success  
  Timestamp: 2022-08-10T00:08:55.329  
  Try: 0  
  Progress (%): 100  
  Current Task:
```

Zo verifieert u de configuratie via de NXOS:

```
ucs# connect nxos  
ucs(nxos)# show ldap-server  
ucs(nxos)# show ldap-server groups
```

```

UCS-AS-MXC-P25-02-B-A# connect nxos
Bad terminal type: "xterm-256color". Will assume vt100.
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (C) 2002-2020, Cisco and/or its affiliates.
All rights reserved.
The copyrights to certain works contained in this software are
owned by other third parties and used and distributed under their own
licenses, such as open source. This software is provided "as is," and unless
otherwise stated, there is no warranty, express or implied, including but not
limited to warranties of merchantability and fitness for a particular purpose.
Certain components of this software are licensed under
the GNU General Public License (GPL) version 2.0 or
GNU General Public License (GPL) version 3.0 or the GNU
Lesser General Public License (LGPL) Version 2.1 or
Lesser General Public License (LGPL) Version 2.0.
A copy of each such license is available at
http://www.opensource.org/licenses/gpl-2.0.php and
http://opensource.org/licenses/gpl-3.0.html and
http://www.opensource.org/licenses/lgpl-2.1.php and
http://www.gnu.org/licenses/old-licenses/library.txt.
UCS-AS-MXC-P25-02-B-A(nx-os)# show ldap-server
  timeout : 30
  port : 0
  baseDN : DC=mxsvlab,DC=com
user profile attribute :
search filter : sAMAccountName=$userid
  use groups : 0
recurse groups : 0
group attribute : memberOf
  group map CN=ucsadmin,OU=CiscoUCS,DC=mxsvlab,DC=com:
    roles: admin
    locales:
total number of servers : 1

following LDAP servers are configured:
  10.31.123.60:
    timeout: 30    port: 389    rootDN: CN=ucsbind,OU=CiscoUCS,DC=mxsvlab,DC=com
    enable-ssl: false
    baseDN: DC=mxsvlab,DC=com
    user profile attribute:
    search filter:
    use groups: true
    recurse groups: true
    group attribute: memberOf
    vendor: MS AD
UCS-AS-MXC-P25-02-B-A(nx-os)# show ldap-server groups
total number of groups: 2

following LDAP server groups are configured:
  group ldap:
    baseDN:
    user profile attribute:
    search filter:
    group membership attribute:
    server: 10.31.123.60 port: 389 timeout: 30
  group mxsv:
    baseDN:
    user profile attribute:
    search filter:
    group membership attribute:
    server: 10.31.123.60 port: 389 timeout: 30

```

De meest effectieve methode om fouten te zien is om onze debug toe te laten, met deze output

kunnen we de groepen, de verbinding, en de foutmelding zien die communicatie verhindert.

- Open een SSH-sessie voor FI en login als lokale gebruiker en wijzig deze naar de NX-OS CLI-context en start de terminal monitor.

```
ucs # connect nxos
```

```
ucs(nxos)# terminal monitor
```

- Schakel debug-vlaggen in en controleer de SSH-sessieuitvoer naar het logbestand.

```
ucs(nxos)# debug aaa all <<< not required, incase of debugging authentication problems
```

```
ucs(nxos)# debug aaa aaa-requests
```

```
ucs(nxos)# debug ldap all <<< not required, incase of debugging authentication problems.
```

```
ucs(nxos)# debug ldap aaa-request-lowlevel
```

```
ucs(nxos)# debug ldap aaa-request
```

```
[UCS-AS-MXC-P25-02-B-A# connect nxos
Bad terminal type: "xterm-256color". Will assume vt100.
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (C) 2002-2020, Cisco and/or its affiliates.
All rights reserved.
The copyrights to certain works contained in this software are
owned by other third parties and used and distributed under their own
licenses, such as open source. This software is provided "as is," and unless
otherwise stated, there is no warranty, express or implied, including but not
limited to warranties of merchantability and fitness for a particular purpose.
Certain components of this software are licensed under
the GNU General Public License (GPL) version 2.0 or
GNU General Public License (GPL) version 3.0 or the GNU
Lesser General Public License (LGPL) Version 2.1 or
Lesser General Public License (LGPL) Version 2.0.
A copy of each such license is available at
http://www.opensource.org/licenses/gpl-2.0.php and
http://opensource.org/licenses/gpl-3.0.html and
http://www.opensource.org/licenses/lgpl-2.1.php and
http://www.gnu.org/licenses/old-licenses/library.txt.
[UCS-AS-MXC-P25-02-B-A(nx-os)# terminal monitor
[UCS-AS-MXC-P25-02-B-A(nx-os)# debug ldap all ←
[UCS-AS-MXC-P25-02-B-A(nx-os)# debug aaa all ←
```

- Open nu een nieuwe GUI- of CLI-sessie en probeer in te loggen als een externe gebruiker (LDAP).
- Zodra u een bericht van de inlogfout hebt ontvangen, schakelt u de debugs uit.

Gerelateerde informatie

- [Technische ondersteuning en documentatie – Cisco Systems](#)

- [UCS M LDAP-voorbeeldconfiguratie](#)
- [Configuratiehandleiding voor Cisco UCS C Series GUI](#)

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document ([link](#)) te raadplegen.