# LDAP im UCS Manager konfigurieren

# Inhalt

Einleitung Voraussetzungen Anforderungen Verwendete Komponenten Hintergrundinformationen Konfigurieren Erstellen einer lokalen Authentifizierungsdomäne **Erstellen eines LDAP-Anbieters** LDAP-Gruppenregelkonfiguration Erstellen einer LDAP-Anbietergruppe Erstellen einer LDAP-Gruppenzuordnung Erstellen einer LDAP-Authentifizierungsdomäne Überprüfung Häufige LDAP-Probleme. Fehlerbehebung Zugehörige Informationen

# Einleitung

In diesem Dokument wird die Konfiguration für den Remote-Serverzugriff mit dem LDAP-Protokoll in unserer Unified Computing System Manager Domain (UCSM).

## Voraussetzungen

### Anforderungen

Cisco empfiehlt, sich mit folgenden Themen vertraut zu machen:

- Unified Computing System Manager Domain (UCSM)
- Lokale und Remote-Authentifizierung
- Lightweight Directory Access Protocol (LDAP)
- Microsoft Active Directory (MS-AD)

### Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Cisco UCS 6454 Fabric Interconnect
- UCSM Version 4.0(4 KB)
- Microsoft Active Directory (MS-AD)

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten

Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle verstehen.

# Hintergrundinformationen

Lightweight Directory Access Protocol (LDAP) ist eines der Kernprotokolle für Verzeichnisdienste, die Benutzer und ihre Zugriffsrechte auf IT-Ressourcen sicher verwalten.

Die meisten Verzeichnisdienste verwenden noch heute LDAP, obwohl sie auch zusätzliche Protokolle wie Kerberos, SAML, RADIUS, SMB, Oauth und andere verwenden können.

# Konfigurieren

#### Vorbereitungen

AnmeldenCisco UCS Manager GUIals Administrator-Benutzer.

#### Erstellen einer lokalen Authentifizierungsdomäne

Schritt 1: Im Navigation klicken Sie auf das Admin aus.

Schritt 2: Auf dem Admin Registerkarte, erweitern All > User Management > Authentication

æ	Al *	All / User Management / Authentication / Authentication Domains								
B	* AI	Domains Events FSM								
	▼ Faults, Events and Audit Log	1% Advanced Filter ↑ Export ⊕ Print	Advanced Filter + Export - & Print - &							
*	Faults	Name	Realm	Provider Group	Web Session Refresh Period	Web Session Timeout				
_	Events	LDAP	ldap	mxsv	600	7200				
포	Audit Logs	Local	local		600	7200				
-	Syslog	radius	radius		7200	8000				
_	Core Files	Tacas	tacacs	Test	600	7200				
	TechSupport Files									
	Settings									
30	User Management									
	<ul> <li>Authentication</li> </ul>									
	Native Authentication									
	Authentication Domains									
	✓ LDAP									
	<ul> <li>LDAP Group Maps</li> </ul>									
	<ul> <li>LDAP Provider Groups</li> </ul>									
	<ul> <li>LDAP Providers</li> </ul>									
	RADIUS									
	+ TACACS+									
	<ul> <li>User Services</li> </ul>									
	Locales									
	<ul> <li>Locally Authenticated Users</li> </ul>									
	Login Profile			Add Delete 10 Info						

Schritt 3: Rechtsklick Authentication Domains Und wählen Create a Domain.

Schritt 4: Für die Name Feld, Typ Local.

Schritt 5: Für die Realm, klicken Sie auf Local Optionsfeld.

### Properties for: Local

General Events	
Actions	Properties
Delete	Name : Local
	Web Session Refresh Period (sec) : 600
	Web Session Timeout (sec) : 7200
	Realm Cocal Radius Tacacs Ldap
	Web Session Refresh Period (sec) : 600 Web Session Timeout (sec) : 7200 Realm

OK

Schritt 6: Klicken Sie auf ok.

#### **Erstellen eines LDAP-Anbieters**

Diese Beispielkonfiguration umfasst keine Schritte zum Konfigurieren von LDAP mit SSL.

Schritt 1:Im Navigation klicken Sie auf das Admin aus.

Schritt 2: Auf dem Admin Registerkarte, erweitern All > User Management > LDAP.

Schritt 3: Im work klicken Sie auf das General aus.

Schritt 4: Im Actions Bereich, klicken Sie auf Create LDAP Provider

ж	Al	All / User Management / LDAP
8	• AI	General LDAP Providers LDAP Provider Groups LDAP Group Maps Events FSM
쁆	<ul> <li>Faults, Events and Audit Log</li> <li>Faults</li> </ul>	Actions Properties
Ŧ	Events Audit Logs	Create LDAP Provider  Timeout : 30 Create LDAP Provider Group Attribute :
≡	Syslog Core Files	Create LDAP Group Map Base DN : DC+mxsvlab,DC+com
	TechSupport Files	Hter : SAMACCounterame=Susend
٩	User Management     Authentication	
	* LDAP	
	LDAP Group Maps	
	LDAP Provider Groups     LDAP Providers	

Schritt 5: Im Create LDAP Provider auf der Seite des Assistenten die entsprechenden Informationen ein:

- Im Hostnamedie IP-Adresse oder den Hostnamen des AD-Servers ein.
- Im order Feld, akzeptieren Sie die Iowest-available standard.
- Im BindDN kopieren Sie die BindDN aus Ihrer AD-Konfiguration, und fügen Sie sie ein.

Für diese Beispielkonfiguration lautet der BindDN-Wert

Cancel

Help

#### CN=ucsbind,OU=CiscoUCS,DC=mxsvlab,DC=com.

• Im BaseDN kopieren Sie die BaseDN aus Ihrer AD-Konfiguration, und fügen Sie sie ein. Für diese Beispielkonfiguration lautet der BaseDN-Wert **DC=mxsvlab,DC=com.** 

- Verlassen Sie Enable SSL nicht aktiviert.
- Im Port -Feld den Standardwert 389 zu übernehmen.

• Im Filter -Feld, kopieren Sie das Filterattribut aus Ihrer AD-Konfiguration, und fügen Sie es ein.

Das Cisco UCS ermittelt anhand des Filterwerts, ob der Benutzername (im Anmeldebildschirm von Cisco UCS Manager) ist in AD.

Für diese Beispielkonfiguration lautet der Filterwert **sAMAccountName=\$userid**, wobei \$useridis der user name in das Cisco UCS Manager Anmeldebildschirm.

- Verlassen Sie Attribute Feld leer.
- Im Password das Kennwort für das in AD konfigurierte ucsbind-Konto ein.

Wenn Sie zurück zum Create LDAP Provider wizard um das Kennwort zurückzusetzen, lassen Sie sich nicht warnen, wenn das Kennwortfeld leer ist.

Die Fehlermeldung set: yes -Meldung, die neben dem Kennwortfeld angezeigt wird, bedeutet, dass ein Kennwort festgelegt wurde.

• Im Confirm Password das Kennwort für das in AD konfigurierte ucsbind-Konto erneut eingeben.

Create I DAP Provider

? X

- Im Timeout Feld, akzeptieren Sie die 30 Standard.
- Im vendor das Optionsfeld für MS-AD für Microsoft Active Directory aus.

Create LDAP Provider	Hostname/FQDN (or IP Address) :	10.31.123.60
LDAP Group Rule	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

#### LDAP-Gruppenregelkonfiguration

Schritt 1. Auf demLDAP Group Rule -Seite des Assistenten, füllen Sie die folgenden Felder aus:

- Für die Group Authentication klicken Sie auf das Enable Optionsfeld.
- Für die Group Recursion klicken Sie auf das Recursive Optionsfeld. Dadurch kann das System die Suche auf allen Ebenen fortsetzen, bis es einen Benutzer findet.

Wenn die Group Recursion ist auf Non-Recursivebeschränkt es UCS auf eine Suche auf der ersten Ebene, selbst wenn bei der Suche kein qualifizierter Benutzer gefunden wird.

• Im Target Attribute Feld, akzeptieren Sie diememberOf standard.

		Create LDAP Provider	? ×
1	Create LDAP Provider	Group Authorization : Disable Enable	
2	LDAP Group Rule	Group Recursion : Non Recursive Recursive	
		< Prev Next > Finish	Cancel

Schritt 2: Klicken Sie in Finish.

**Hinweis**: In einem realen Szenario würden Sie wahrscheinlich mehrere LDAP-Anbieter haben. Bei mehreren LDAP-Anbietern würden Sie die Schritte zum Konfigurieren der LDAP-Gruppenregel für jeden LDAP-Anbieter wiederholen. In dieser Beispielkonfiguration gibt es jedoch nur einen LDAP-Anbieter, weshalb dies nicht erforderlich ist. angezeigt.

### Erstellen einer LDAP-Anbietergruppe

Schritt 1: Klicken Sie im Navigationsbereich mit der rechten Maustaste LDAP Provider Groups und wählen Create LDAP Provider Group.

ж.	Al	All / User Management / LDAP / LDAP Provider Groups		
	• Al	LDAP Provider Groups		
	· Faults, Events and Audit Log	Ty Advanced Filter † Export 🗇 Print		0
8	Faults	Name	LDAP Providens	
	Events	musv	10.31.123.60	
	Audit Logs			
_	Syslog			
-	Core Files			
	TechSupport Files			
	Settings			
J <sub>0</sub>	User Management			
	<ul> <li>Authentication</li> </ul>			
	+ LDAP			
	<ul> <li>LDAP Group Maps</li> </ul>			
	LDAP Provider Groups			
	mxsv			
-	LDAP Providers			
	<ul> <li>RADIUS</li> </ul>			
	TACACS+			
	<ul> <li>User Services</li> </ul>			
	<ul> <li>Locales</li> </ul>			
	<ul> <li>Locally Authenticated Users</li> </ul>			
	Login Profile			
	<ul> <li>Remotely Authenticated Users</li> </ul>		Add Delete () Info	

Schritt 2: Im Create LDAP Provider Group angezeigt, geben Sie die entsprechenden Informationen ein:

- Im Name ein, geben Sie einen eindeutigen Namen für die Gruppe ein, z. B. LDAP Providers.
- Im LDAP Providers Tabelle die IP-Adresse für den AD-Server aus.
- Klicken Sie auf die Schaltfläche >>, um den AD-Server Ihrem Included Providers Tabelle.

#### Create LDAP Provider Group

	LDAP Providers					Included Providers	
			\$				3
ostname	Bind DN	Port			Name	Order	
10.31.123	CN=ucsbind,	389				No data available	
			_	>>			
				<<			



? X

Schritt 3: Klicken Sie auf OK.

Ihre Anbietergruppe wird im LDAP Provider Groups Ordner.

#### Erstellen einer LDAP-Gruppenzuordnung

Schritt 1: Klicken Sie im Navigationsbereich auf Adminaus.

Schritt 2: Auf dem Admin Registerkarte, erweitern All > User Management > LDAP.

Schritt 3: Klicken Sie im Arbeitsbereich auf Erstellen. LDAP Group Map.

ж	Al v	All / User Management / LDAP / LDAP Group Maps			
	* All	LDAP Group Maps			
	<ul> <li>Faults, Events and Audit Log</li> </ul>	15 Advanced Filter ↑ Export ⊕ Print			0
윪	Faults	Name	Roles	Locales	
	Events	CN+ucsadmin,OU+CiscoUCS,DC+mxsvlab,DC+com	admin		
	Audit Logs				
_	Syslog				
-	Core Files				
	TechSupport Files				
	Settings				
30	▼ User Management				
	<ul> <li>Authentication</li> </ul>				
	▼ LDAP				
_	LDAP Group Maps				
	<ul> <li>LDAP Provider Groups</li> </ul>				
	<ul> <li>LDAP Providers</li> </ul>				
	<ul> <li>RADIUS</li> </ul>				
	TACACS+				
	* User Services				
	<ul> <li>Locales</li> </ul>				
	<ul> <li>Locally Authenticated Users</li> </ul>				
	Login Profile				
	<ul> <li>Remotely Authenticated Users</li> </ul>				
	<ul> <li>Roles</li> </ul>		🕀 Add 🗎 Dei	lete 🕕 Info	

Schritt 4: Im Create LDAP Group Map angezeigt, geben Sie die entsprechenden Informationen ein:

• Im LDAP Group DN -Feld den Wert aus dem AD-Serverkonfigurationsabschnitt für die LDAP-Gruppe kopieren und einfügen.

Der in diesem Schritt angeforderte Wert für die LDAP-Gruppen-DN entspricht dem Distinguished Name für jede der Gruppen, die Sie in AD unter UCS-Gruppen erstellt haben.

Aus diesem Grund muss der in Cisco UCS Manager eingegebene Group DN-Wert genau mit dem Group DN-Wert im AD-Server übereinstimmen.

In dieser Beispielkonfiguration lautet dieser Wert CN=ucsadmin,OU=CiscoUCS,DC=sampleDesign,DC=com.

• Im Roles Tabelle, klicken Sie auf das Admin ein, und klicken Sie auf OK.

Klicken Sie auf das Kontrollkästchen für eine Rolle, um anzuzeigen, dass Sie allen Benutzern, die in der Gruppenzuordnung enthalten sind, Administratorberechtigungen zuweisen möchten.



**Schritt 5:** Erstellen Sie neue LDAP-Gruppenzuordnungen (verwenden Sie die zuvor von AD aufgezeichneten Informationen) für jede verbleibende Rolle im AD-Server, die Sie testen möchten.

Weiter: Erstellen Sie Ihre LDAP-Authentifizierungsdomäne.

### Erstellen einer LDAP-Authentifizierungsdomäne

Schritt 1: Auf dem Administrator Registerkarte, erweitern All > User Management > Authentication

Schritt 2: Rechtsklick Authentifizierung Authentication Domains und wählen Create a Domain.

æ	All	All / User Management / Authentication / Authentication Domains						
	* Al	Domains Events FSM						
	<ul> <li>Faults, Events and Audit Log</li> </ul>	1% Advanced Filter 🔶 Export ⊕	Print				٥	
8	Faults	Name	Realm	Provider Group	Web Session Refresh Period	Web Session Timeout		
_	Events	LDAP	Idap	mxsv	600	7200		
-	Audit Logs	Local	local		600	7200		
=	Syslog	radius	radius		7200	8000		
-	Core Files	Tacas	tacacs	Test	600	7200		
	TechSupport Files							
	Settings							
<b>J</b> 0	▼ User Management							
	<ul> <li>Authentication</li> </ul>							
	Native Authentication							
	Authentication Domains							
	▼ LDAP							
	<ul> <li>LDAP Group Maps</li> </ul>							
	<ul> <li>LDAP Provider Groups</li> </ul>							
	LDAP Providers							
	RADIUS							
	TACACS+							
	<ul> <li>User Services</li> </ul>							
	<ul> <li>Locales</li> </ul>							
	<ul> <li>Locally Authenticated Users</li> </ul>							
	Login Profile			🕀 Add 🖯 Delete 👘				

Schritt 3:In&nbspCreate a Domain schließen Sie die nächsten Schritte ab:

- Im Name ein, geben Sie einen Namen für Ihre Domäne ein, z. B. LDAP.
- Im Realm auf das Ldap Optionsfeld.

Properties for: I DAP

• Über die Provider Group aus, wählen Sie die LDAP Provider Group zuvor erstellt haben, und klicken Sie auf OK.

X

ctions	Properties
elete	Name : LDAP
	Web Session Refresh Period (sec): 600
	Web Session Timeout (sec) : 7200
	Realm : CLocal Radius Tacacs Ldap
	Provider Group

Die Authentifizierungsdomäne wird angezeigt unter Authentication Domains.

# Überprüfung

Ping an LDAP Provider IP oder 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

Um die Authentifizierung über NX-OS zu testen, verwenden Sie den test aaa (nur über NX-OS verfügbar).

Wir validieren die Konfiguration unseres Servers:

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

### Häufige LDAP-Probleme.

- Basiskonfiguration.
- Falsches Kennwort oder ungültige Zeichen.

- Falscher Anschluss oder falsches Filterfeld.
- Keine Kommunikation mit unserem Anbieter aufgrund einer Firewall- oder Proxy-Regel.
- FSM liegt nicht bei 100 %.
- Zertifikatprobleme.

### Fehlerbehebung

#### UCSM-LDAP-Konfiguration überprüfen:

Sie müssen sicherstellen, dass UCSM die Konfiguration erfolgreich implementiert hat, da der Status der Finite State Machine (FSM) wird als 100% abgeschlossen angezeigt.

So überprüfen Sie die Konfiguration über die Befehlszeile von 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-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:	

So überprüfen Sie die Konfiguration über das NX-OS:

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
```

Die effektivste Methode, um Fehler zu sehen, ist die Fehlersuche zu aktivieren. Mit dieser

Ausgabe können wir die Gruppen, die Verbindung und die Fehlermeldung sehen, die die Kommunikation verhindert.

 Öffnen Sie eine SSH-Sitzung f
ür FI, melden Sie sich als lokaler Benutzer an, wechseln Sie zum NX-OS CLI-Kontext, und starten Sie den Terminalmonitor.

ucs # connect nxos

ucs(nxos)# terminal monitor

 Aktivieren Sie Debug-Flags, und überprüfen Sie die SSH-Sitzungsausgabe in der Protokolldatei.

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
```

- Öffnen Sie nun eine neue GUI- oder CLI-Sitzung, und versuchen Sie, sich als Remote-Benutzer (LDAP) anzumelden.
- Sobald Sie eine Meldung über einen Anmeldefehler erhalten haben, deaktivieren Sie die Debugs.

# Zugehörige Informationen

- Technischer Support und Dokumentation für Cisco Systeme
- <u>UCSM LDAP-Beispielkonfiguration</u>
- Konfigurationsleitfaden für die GUI der Cisco UCS C-Serie

#### Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.