LDAP im UCS Manager konfigurieren

Inhalt

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

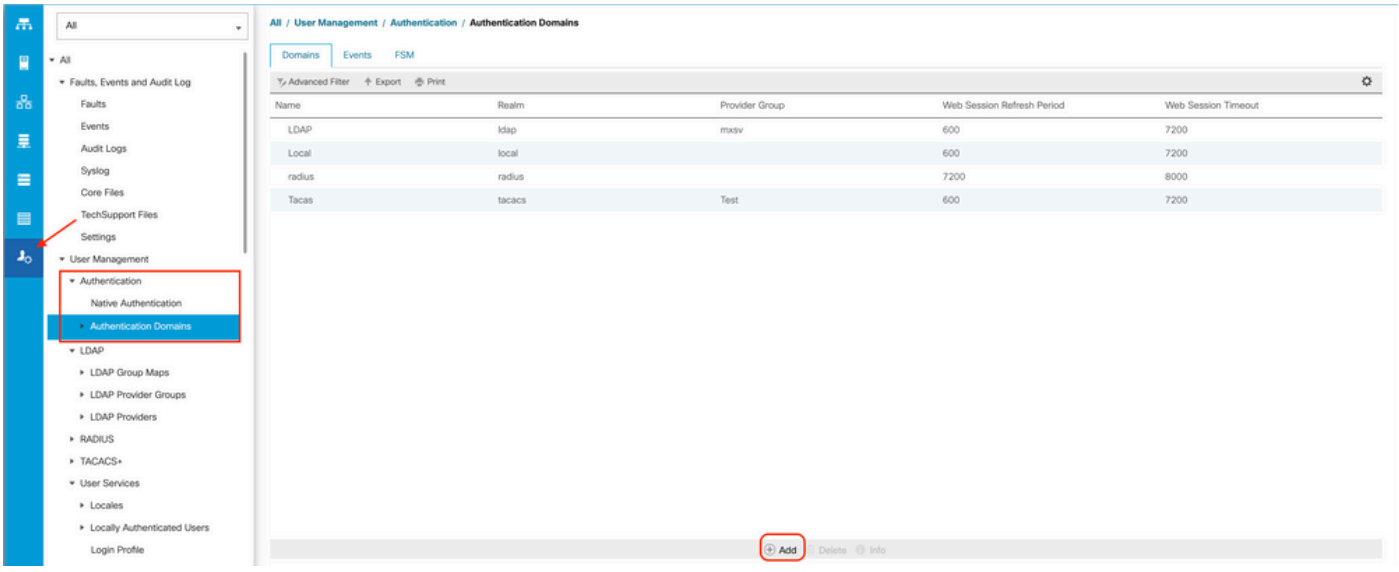
Vorbereitungen

Anmelden**Cisco UCS Manager** GUIals Administrator-Benutzer.

Erstellen einer lokalen Authentifizierungsdomäne

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

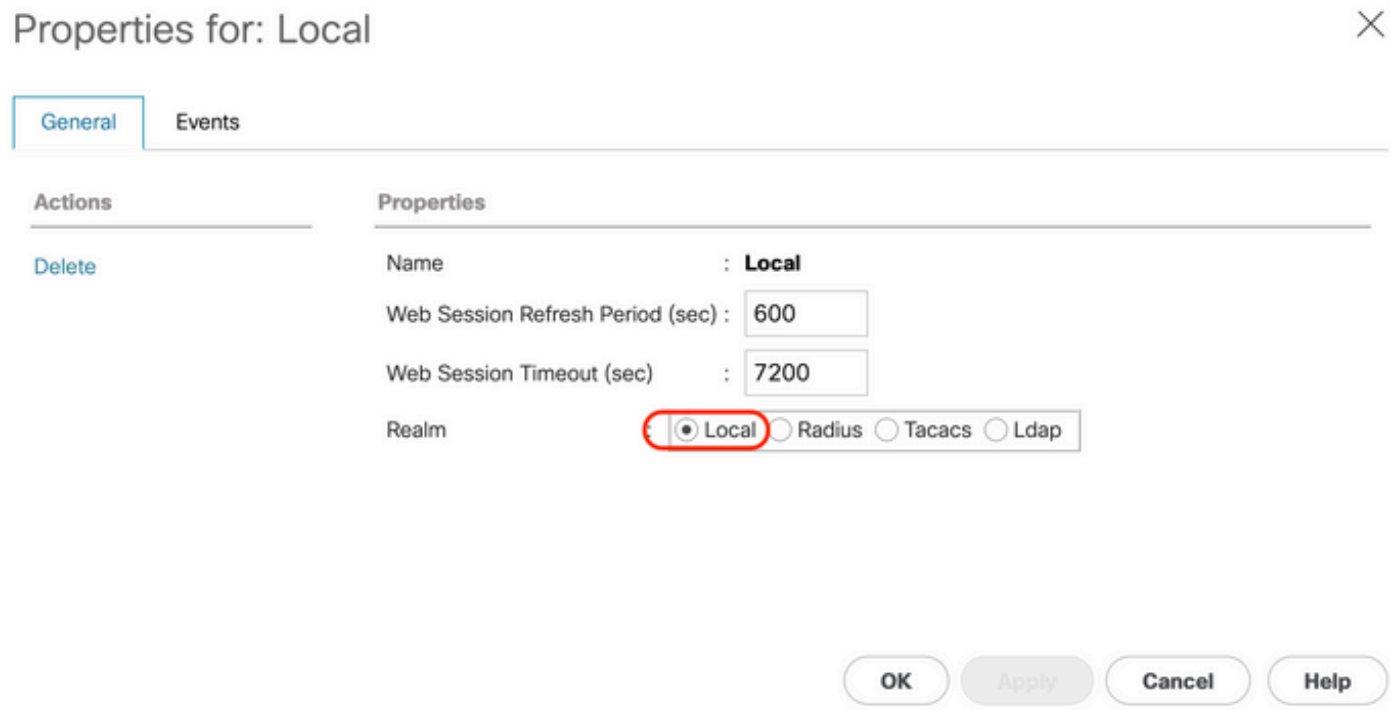
Schritt 2: Auf dem **Admin** Registerkarte, erweitern **All > User Management > Authentication**



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.



Schritt 6: Klicken Sie auf **OK**.

Erstellen eines LDAP-Anbieters

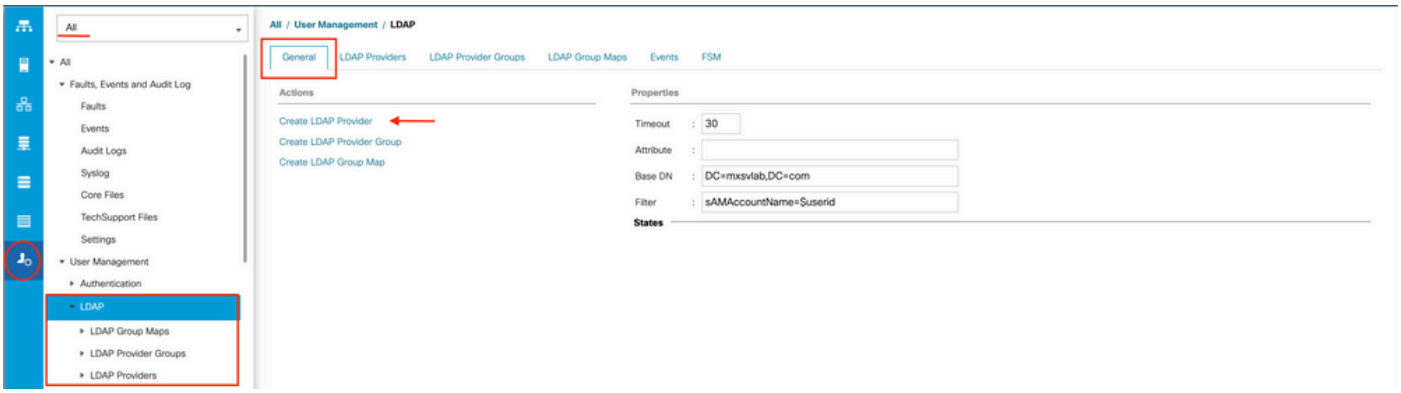
Diese Beispielkonfiguration umfasst keine Schritte zum Konfigurieren von LDAP mit SSL.

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**



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

- Im **Hostname**die IP-Adresse oder den Hostnamen des AD-Servers ein.
- Im **Order** Feld, akzeptieren Sie die **lowest-available** standard.
- Im **BindDN** kopieren Sie die BindDN aus Ihrer AD-Konfiguration, und fügen Sie sie ein.

Für diese Beispielkonfiguration lautet der BindDN-Wert

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.

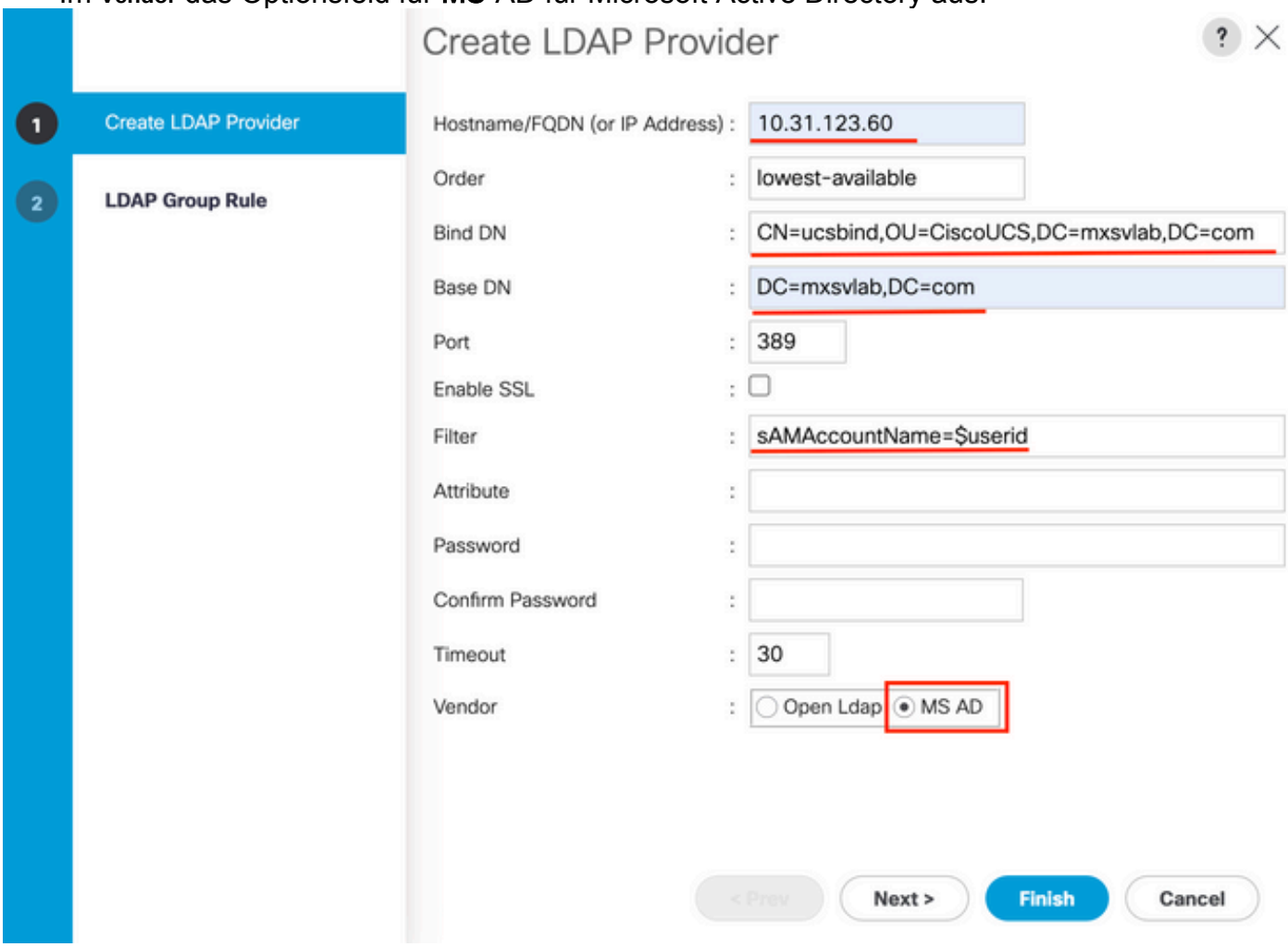
Für diese Beispielkonfiguration lautet der Filterwert **sAMAccountName=$userid**, wobei $useridis der **user name** in das **Cisco UCS Manager** Anmeldebildschirm.

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



Schritt 6: Klicken Sie auf **Next**

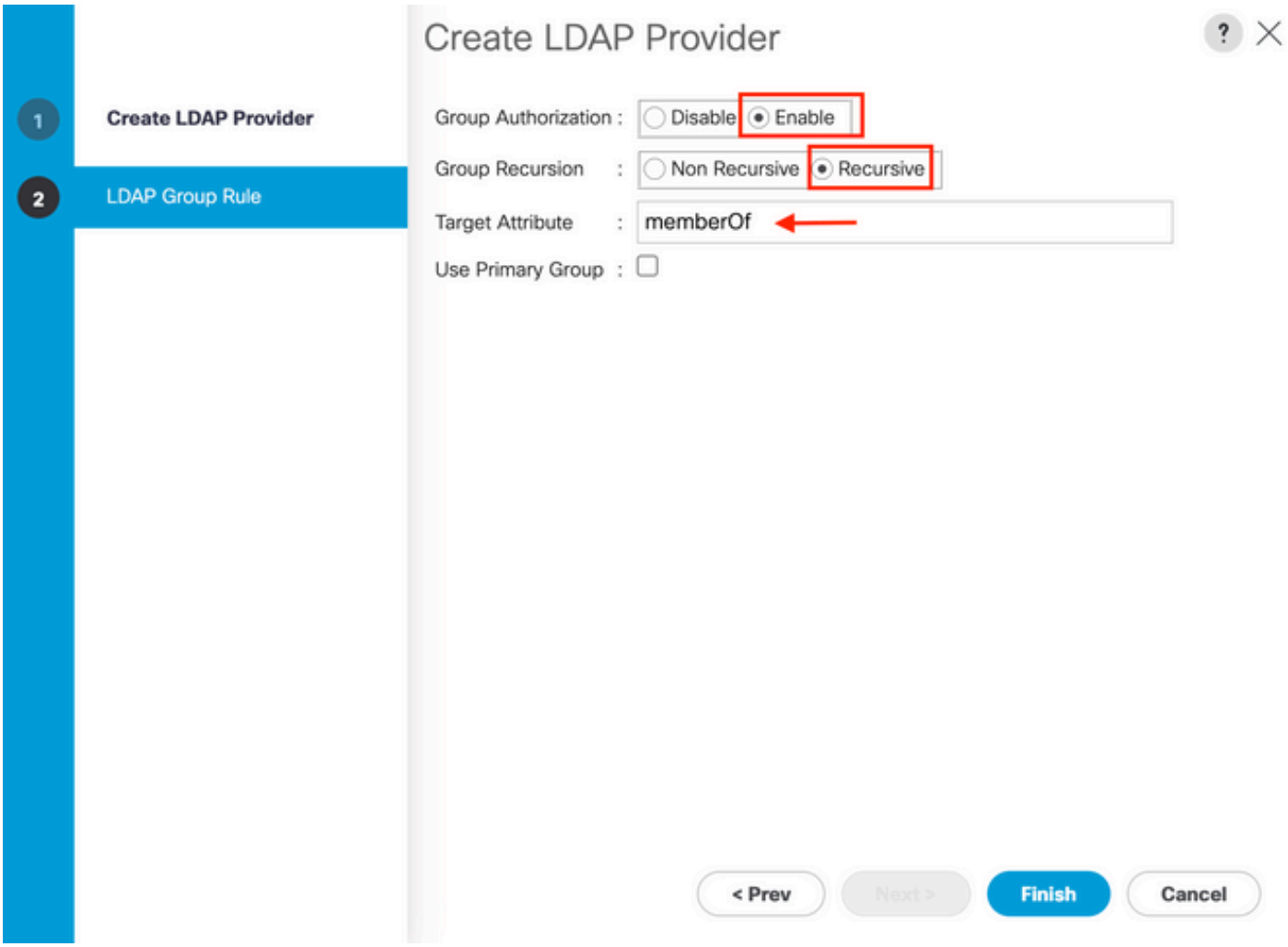
LDAP-Gruppenregelkonfiguration

Schritt 1. Auf dem**LDAP 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-Recursive**beschränkt 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 die**memberOf** standard.



Schritt 2: Klicken Sie in **Finish**.

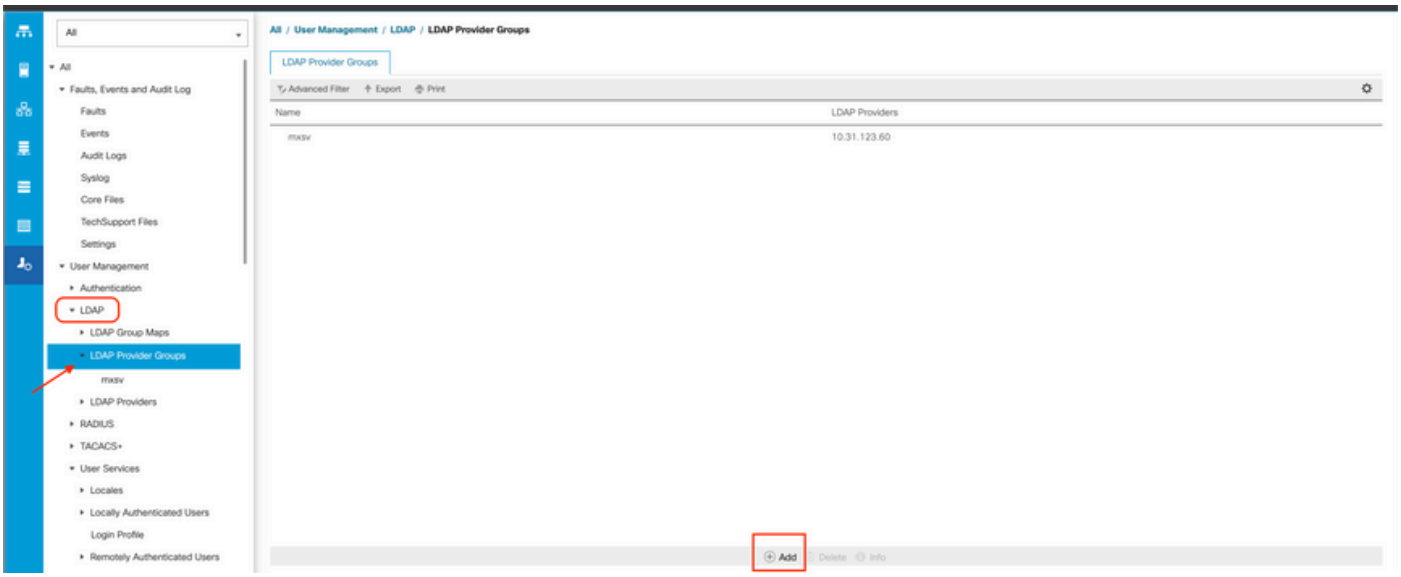
> **Hinweis**: In einem realen Szenario würden Sie wahrscheinlich mehrere LDAP-Anbieter haben. Bei mehreren LDAP-Anbietern würden Sie die Schritte zum Konfigurieren der LDAP-Gruppenregel für jeden LDAP-Anbieter wiederholen. In dieser Beispielkonfiguration gibt es jedoch nur einen LDAP-Anbieter, weshalb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

Die IP-Adresse für den AD-Server wird im Navigationsbereich **unter LDAP>LDAP Providers**

angezeigt.

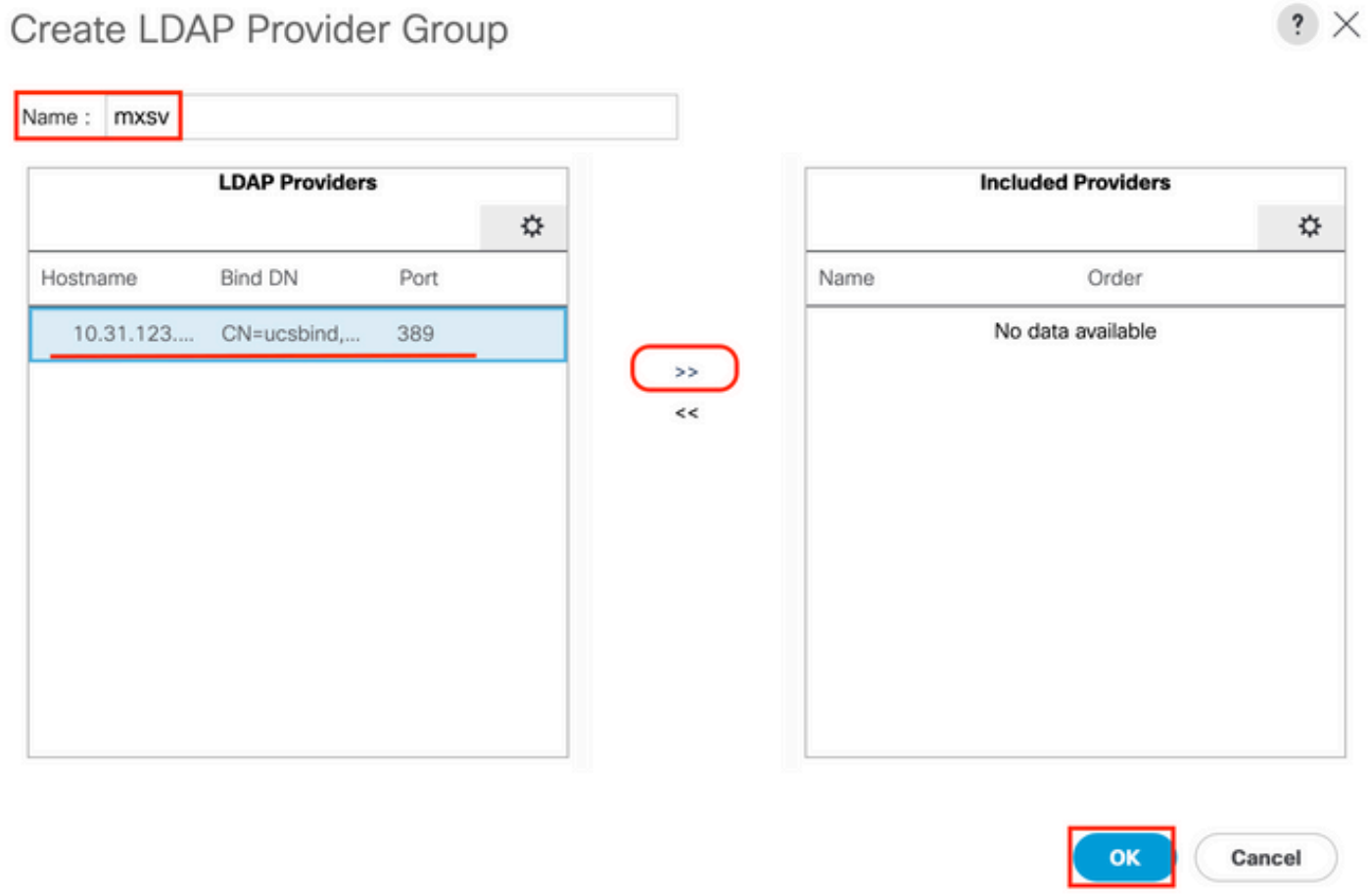
Erstellen einer LDAP-Anbietergruppe

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



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.



Schritt 3: Klicken Sie auf OK.

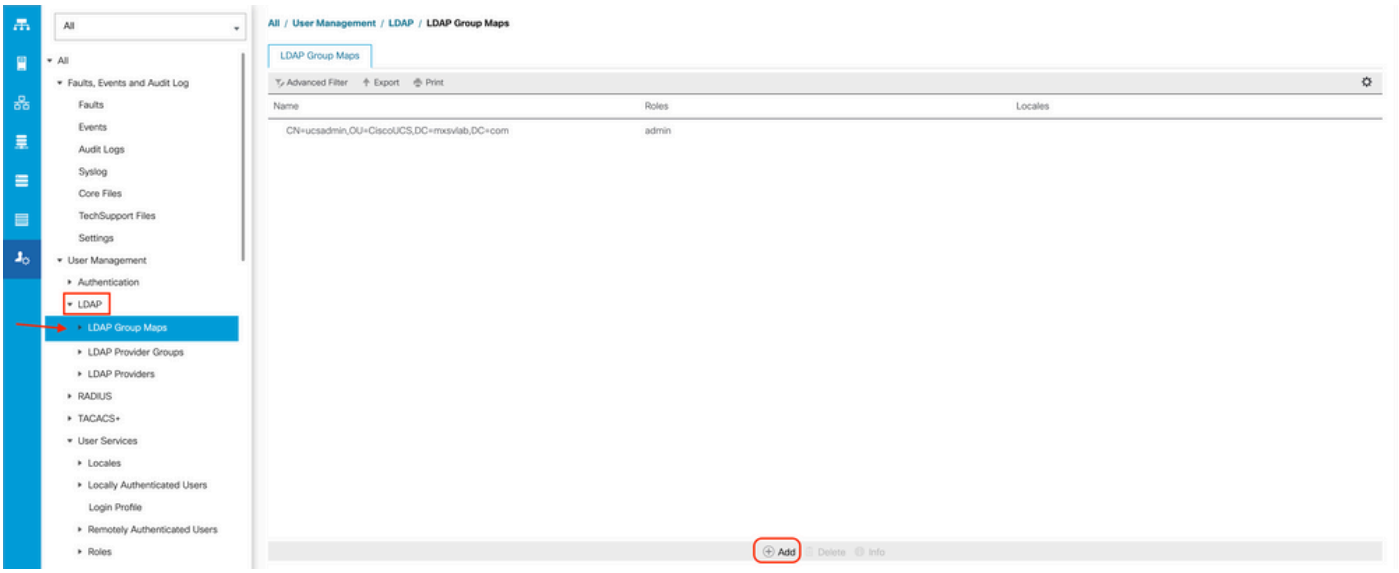
Ihre Anbietergruppe wird im **LDAP Provider Groups** Ordner.

Erstellen einer LDAP-Gruppenzuordnung

Schritt 1: Klicken Sie im Navigationsbereich auf **Admin**aus.

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

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



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.

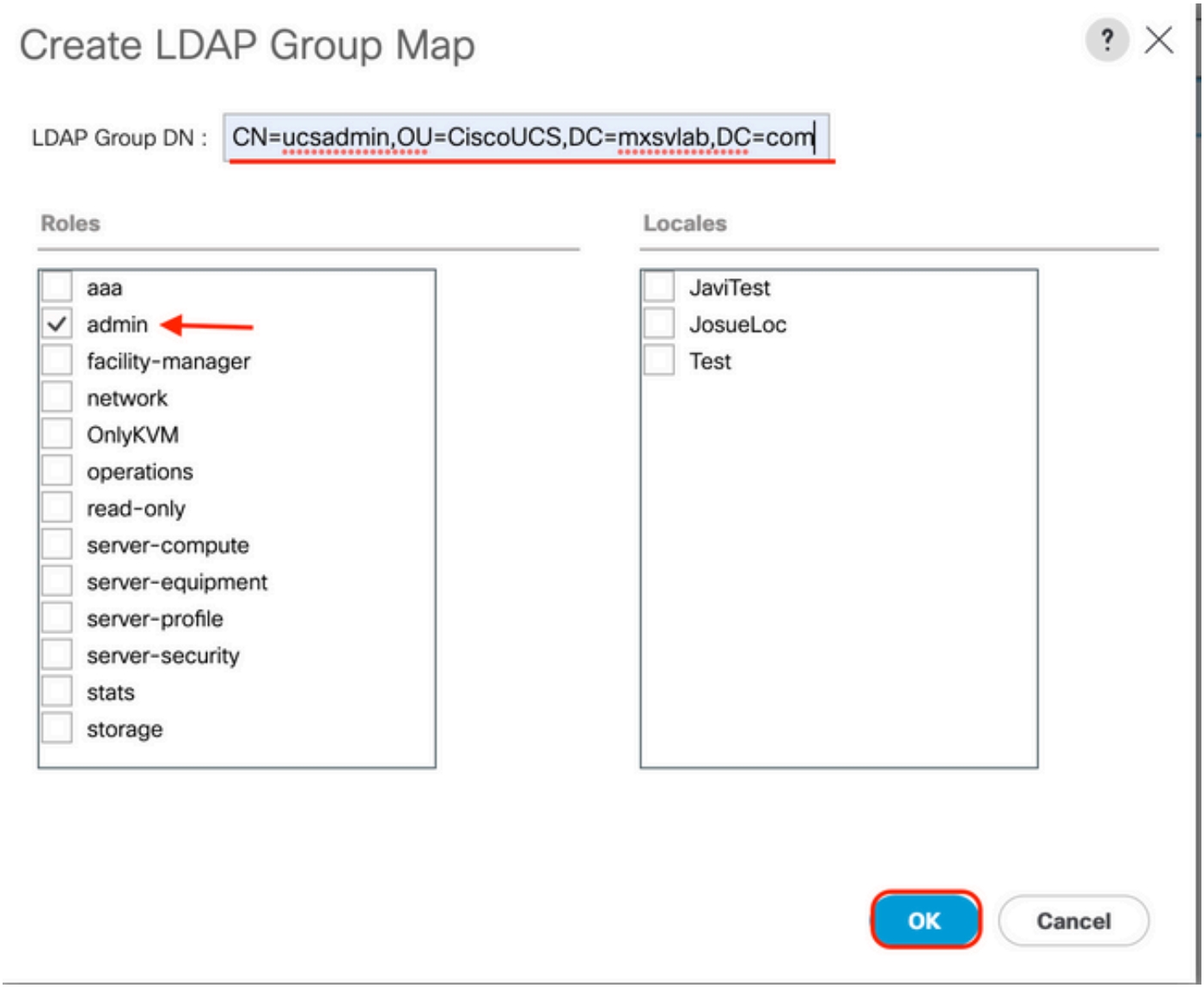
Der in diesem Schritt angeforderte Wert für die LDAP-Gruppen-DN entspricht dem Distinguished Name für jede der Gruppen, die Sie in AD unter UCS-Gruppen erstellt haben.

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.



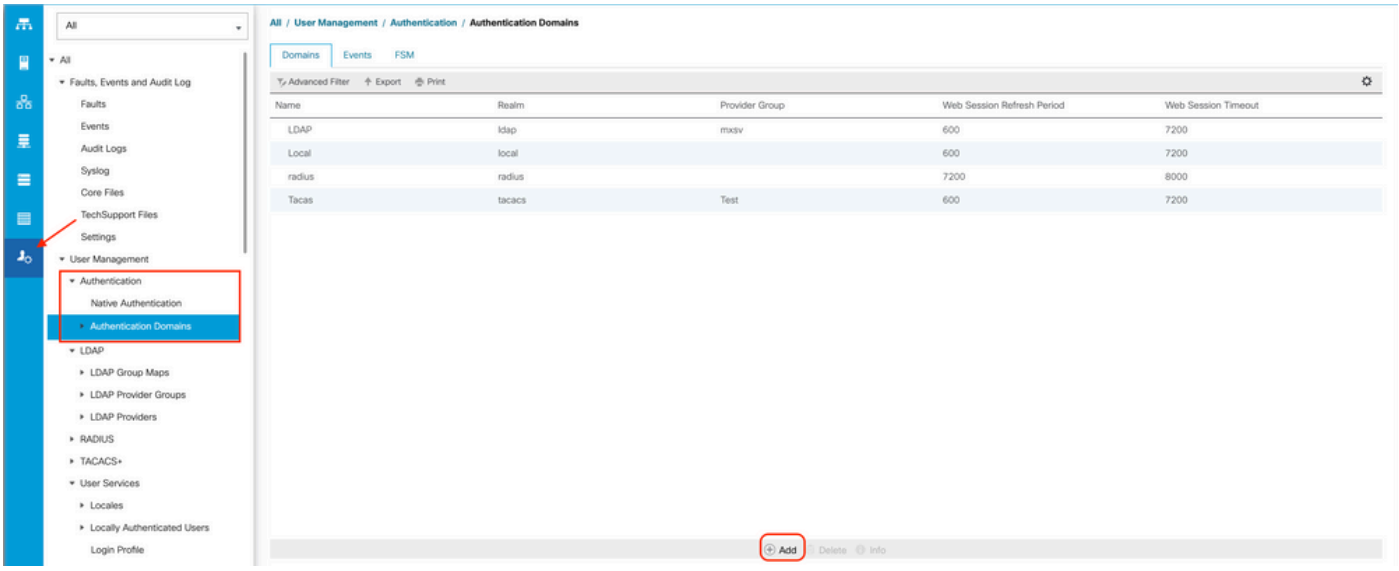
Schritt 5: Erstellen Sie neue LDAP-Gruppenzuordnungen (verwenden Sie die zuvor von AD aufgezeichneten Informationen) für jede verbleibende Rolle im AD-Server, die Sie testen möchten.

Weiter: Erstellen Sie Ihre LDAP-Authentifizierungsdomäne.

Erstellen einer LDAP-Authentifizierungsdomäne

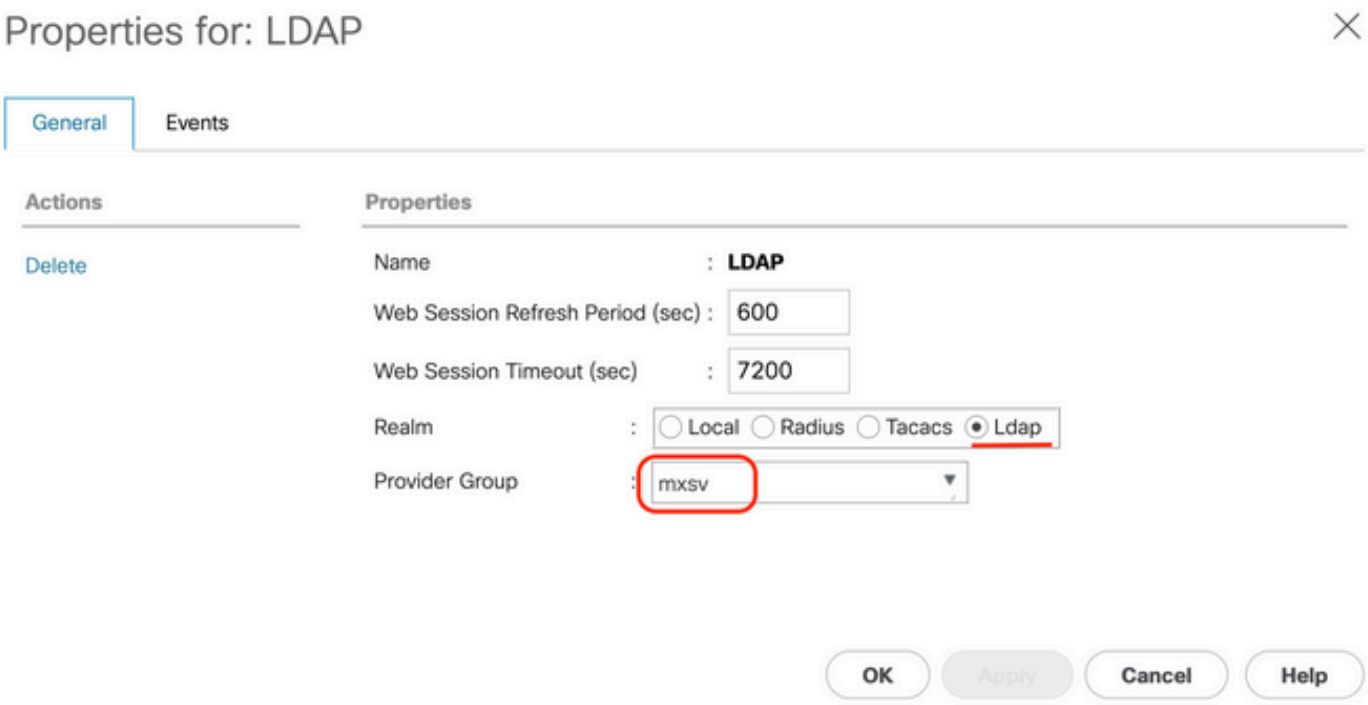
Schritt 1: Auf dem Administrator Registerkarte, erweitern **All > User Management > Authentication**

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



Schritt 3: In **Create 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.
- Über die **Provider Group** aus, wählen Sie die **LDAP Provider Group** zuvor erstellt haben, und klicken Sie auf **OK**.



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.

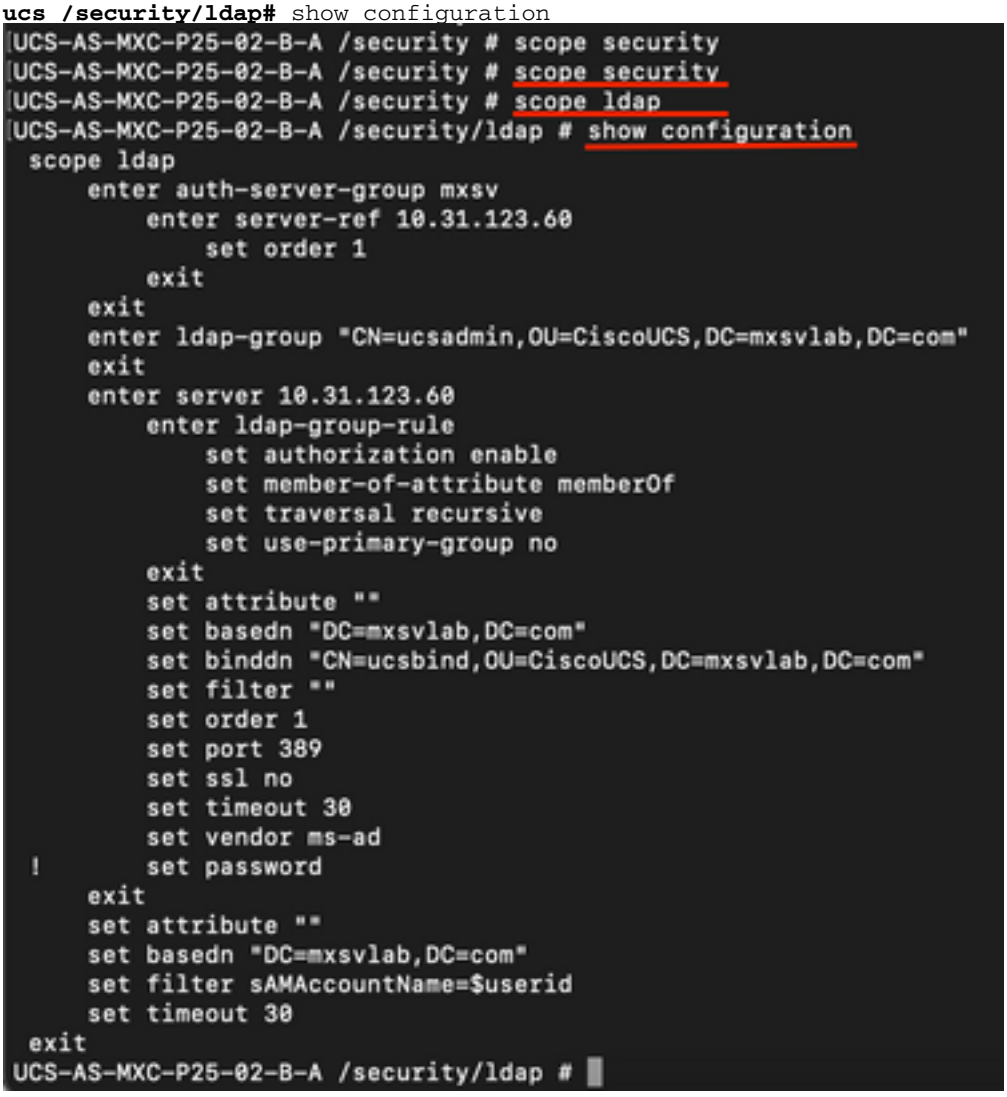
Fehlerbehebung

UCSM-LDAP-Konfiguration überprüfen:

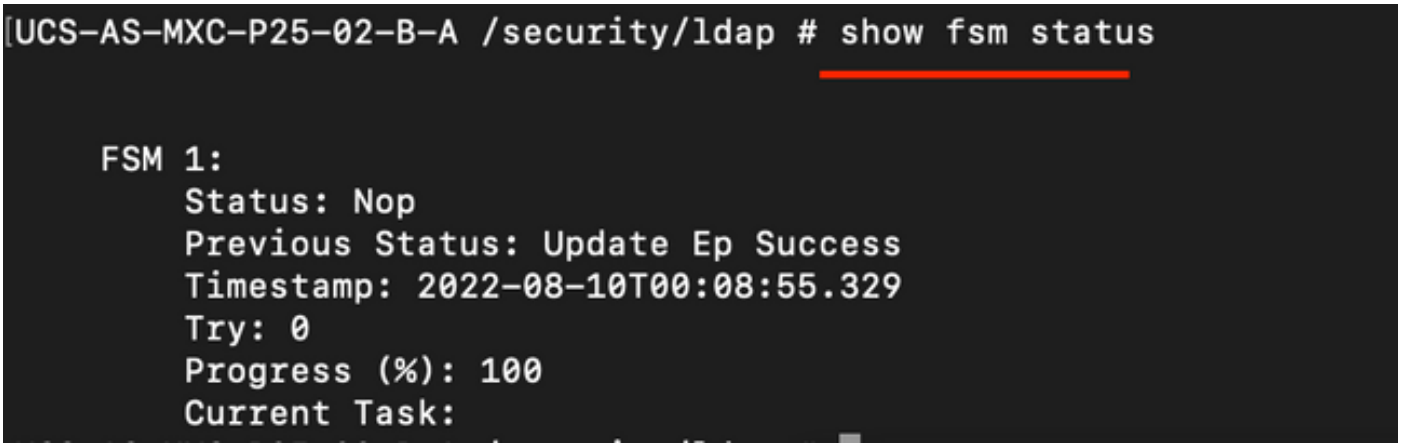
Sie müssen sicherstellen, dass UCSM die Konfiguration erfolgreich implementiert hat, da der Status der **Finite State Machine (FSM)** wird als 100% abgeschlossen angezeigt.

So überprüfen Sie die Konfiguration über die Befehlszeile von UCSM:

```
ucs # scope security
ucs /security# scope ldap
ucs /security/ldap# show configuration
```




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



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 für 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
- UCSM LDAP-Beispielkonfiguration
- 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.