在UCS Manager中配置LDAP

目录

简介

本文档介绍使用LDAP协议进行远程服务器访问的配置。 **Unified Computing System Manager Domain (UCSM).**

先决条件

要求

建议掌握下列主题的相关知识：

- **Unified Computing System Manager Domain (UCSM)**
- 本地和远程身份验证
- **Lightweight Directory Access Protocol (LDAP)**
- **Microsoft Active Directory (MS-AD)**

使用的组件

本文档中的信息基于以下软件和硬件版本：

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

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

Lightweight Directory Access Protocol (LDAP) 是用于目录服务的核心协议之一，用于安全地管理用户及其对IT资源的访问权限。

目前，大多数目录服务仍使用LDAP，不过它们也可以使用其他协议，如Kerberos、SAML、RADIUS、SMB、Oauth等。

配置

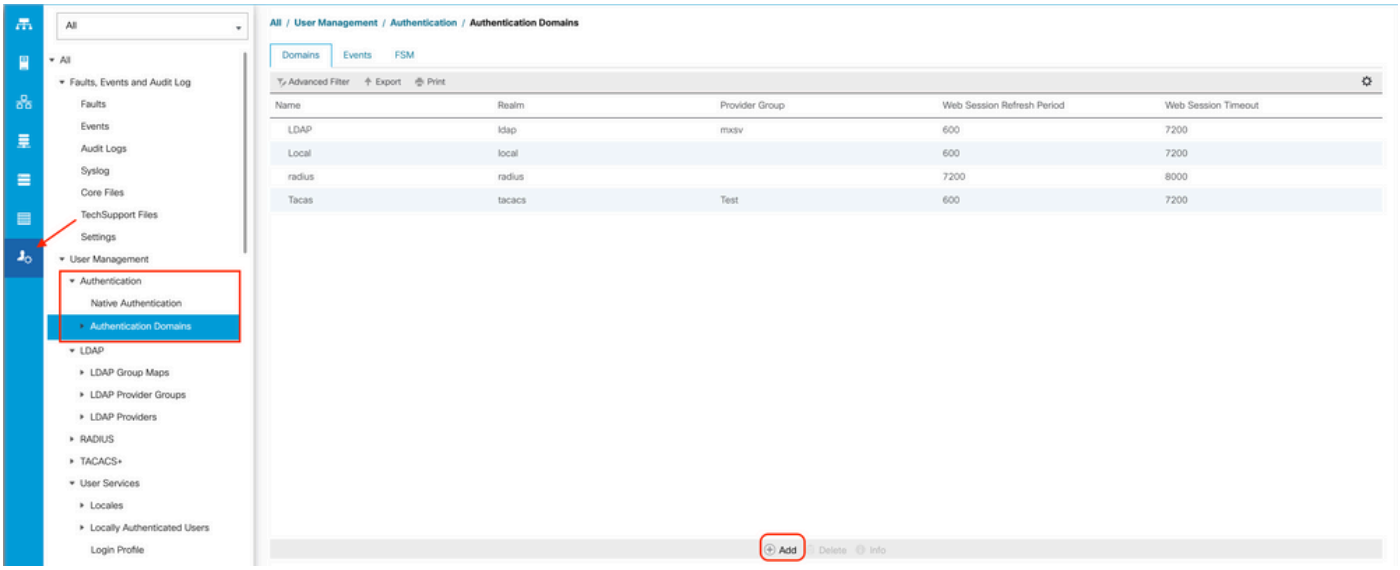
开始使用前

登录**Cisco UCS Manager** GUI作为管理用户。

创建本地身份验证域

步骤1: 如果 **Navigation** 窗格中，点击 **Admin** 选项卡。

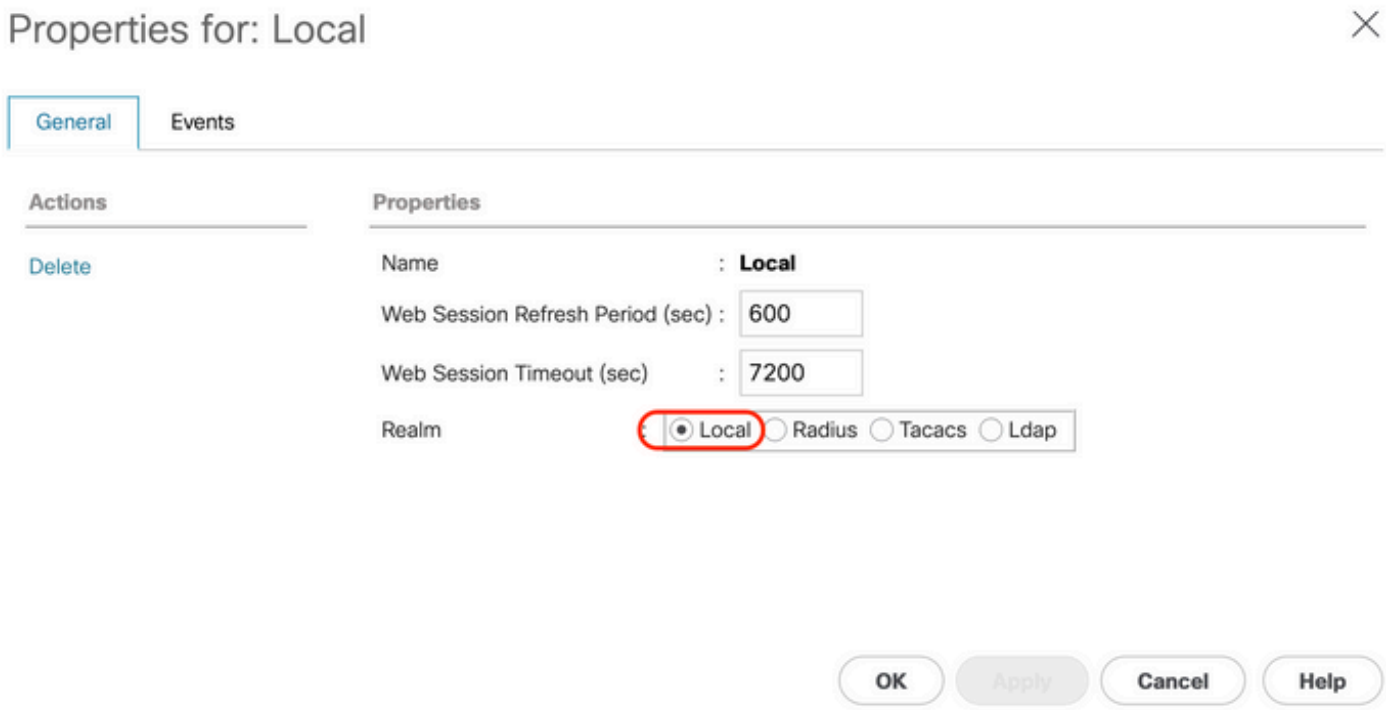
第二步： 在 **Admin** 选项卡，展开 **All > User Management > Authentication**



第三步： 右键单击 **Authentication Domains** 并选择 **Create a Domain.**

第四步： 对于 **Name** 字段，类型 **Local.**

第五步： 对于 **Realm**,单击 **Local** 单选按钮.



第六步：点击 **OK**.

创建LDAP提供程序

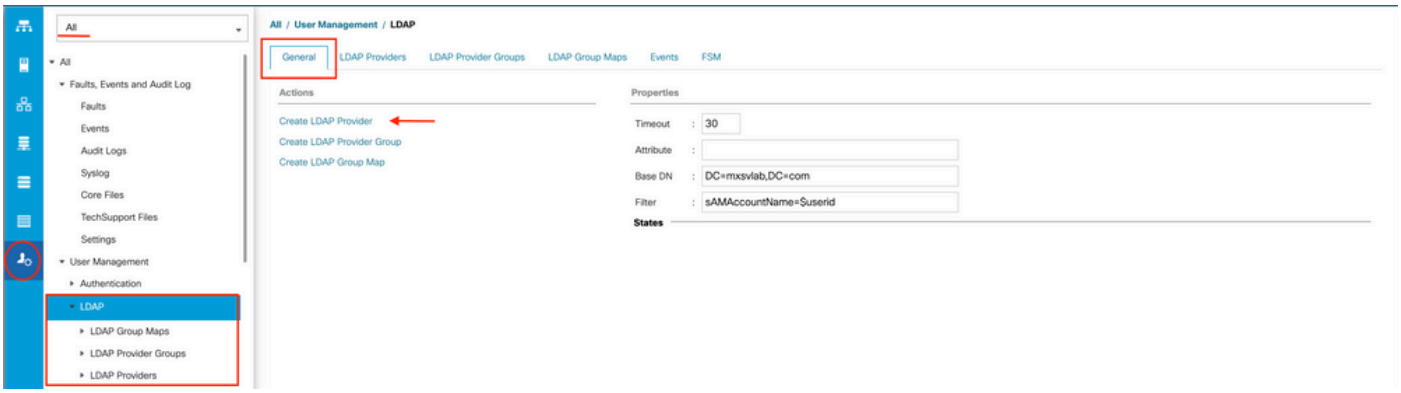
此示例配置不包括使用SSL配置LDAP的步骤。

步骤1:如果 **Navigation** 窗格中，点击 **Admin** 选项卡。

第二步： 在 **Admin** 选项卡，展开 **All > User Management > LDAP**.

第三步： 如果 **Work** 窗格中，点击 **General** 选项卡。

第四步： 如果 **Actions** 区域，单击 **Create LDAP Provider**



第五步： 如果 **Create LDAP Provider** 页面，输入适当的信息：

- 如果 **Hostname**字段中，键入AD服务器的IP地址或主机名。
- 如果 **Order** 字段中，接受 **lowest-available** 默认.
- 如果 **BindDN** 字段中，从AD配置复制并粘贴BindDN。

对于此示例配置，BindDN值为**CN=ucsbind，OU=CiscoUCS，DC=mxsvlab，DC=com**。

- 如果 **BaseDN** 字段中，从AD配置复制并粘贴BaseDN。

对于此示例配置，BaseDN值为**DC=mxsvlab，DC=com**。

- 请离开 **Enable SSL** 复选框取消选中。
- 如果 **Port** 字段中，接受389默认值。
- 如果 **Filter** 字段中，从AD配置复制并粘贴过滤器属性。

Cisco UCS使用过滤器值确定用户名(在登录屏幕上提供，由 **Cisco UCS Manager**)在AD中。

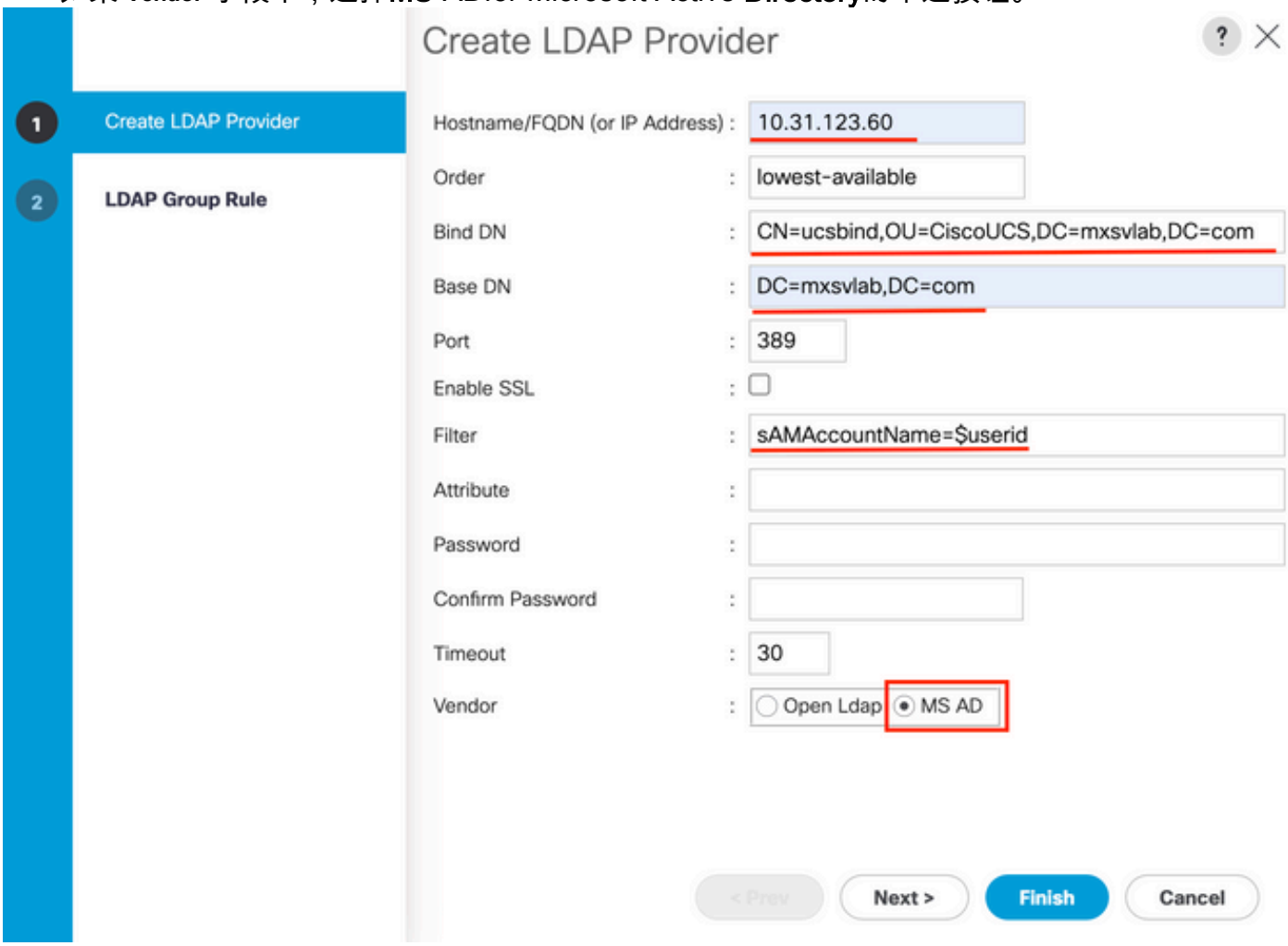
对于此示例配置，过滤器值为**sAMAccountName=$userid**，其中$useridis **user name** 输入 **Cisco UCS Manager** 登录屏幕。

- 请离开 **Attribute** 字段为空。
- 如果 **Password** 字段中，键入在AD中配置的ucsbind帐户的密码。

如果您需要返回到 **Create LDAP Provider wizard** 要重置密码，如果密码字段为空，请不要发出警报。

此 **Set: yes** 密码字段旁显示的消息表示密码已设置。

- 如果 **Confirm Password** 字段中，重新键入AD中配置的ucsbind帐户的密码。
- 如果 **Timeout** 字段中，接受 30个默认值。
- 如果 **Vendor** 字段中，选择**MS-**ADfor Microsoft Active **Directory**的单选按钮。



第六步： 点击 **Next**

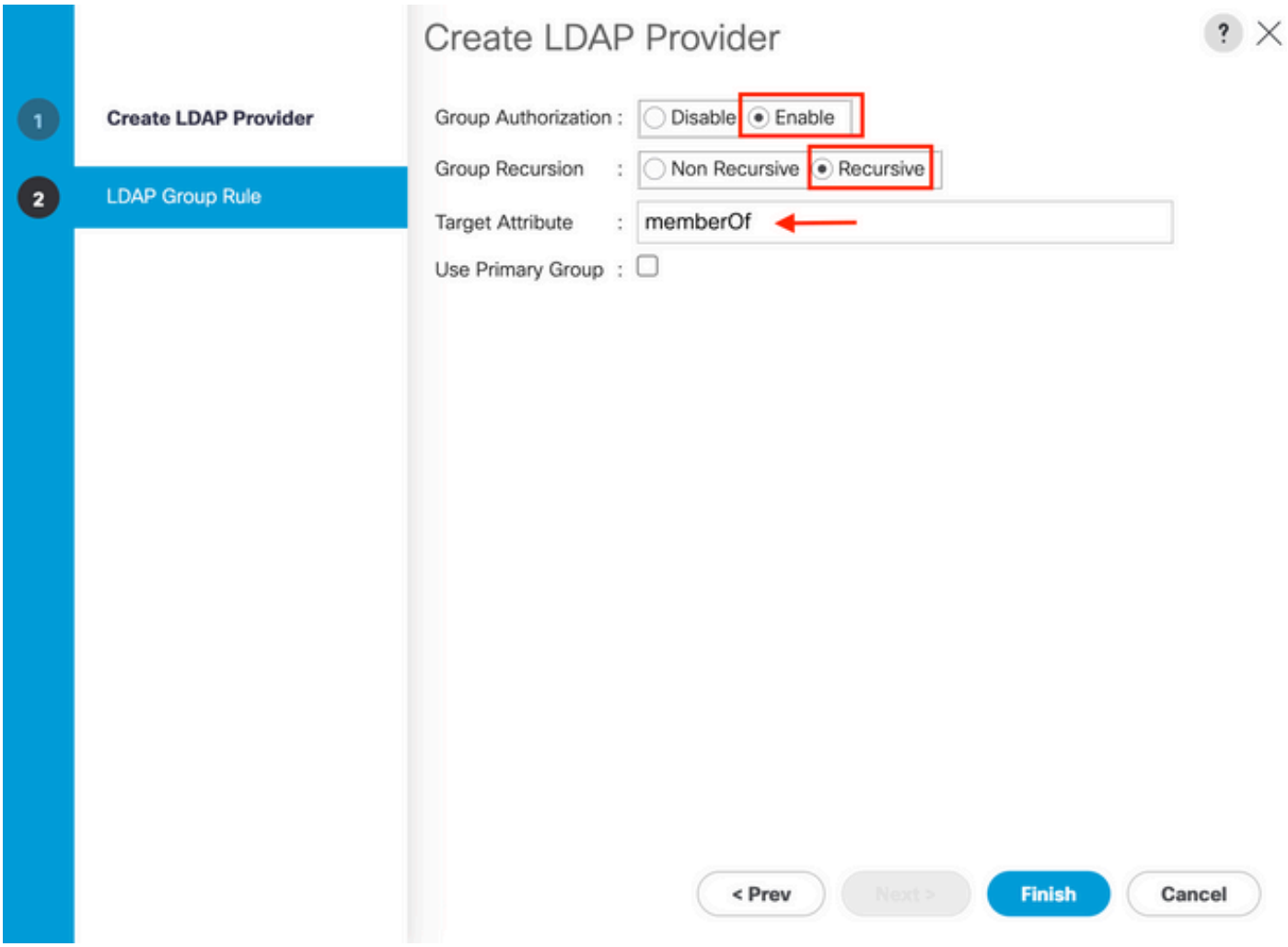
LDAP组规则配置

第 1 步. 在**LDAP Group Rule** 页面，填写以下字段：

- 对于 **Group Authentication** 字段中，点击 **Enable** 单选按钮.
- 对于 **Group Recursion** 字段中，点击 **Recursive** 单选按钮. 这允许系统逐级向下搜索直到找到用户。

如果 **Group Recursion** 设置为 **Non-Recursive**，它将UCS限制为第一级别的搜索，即使搜索没有找到合格用户也是如此。

- 如果 **Target Attribute** 字段中，接受**memberOf** 默认.



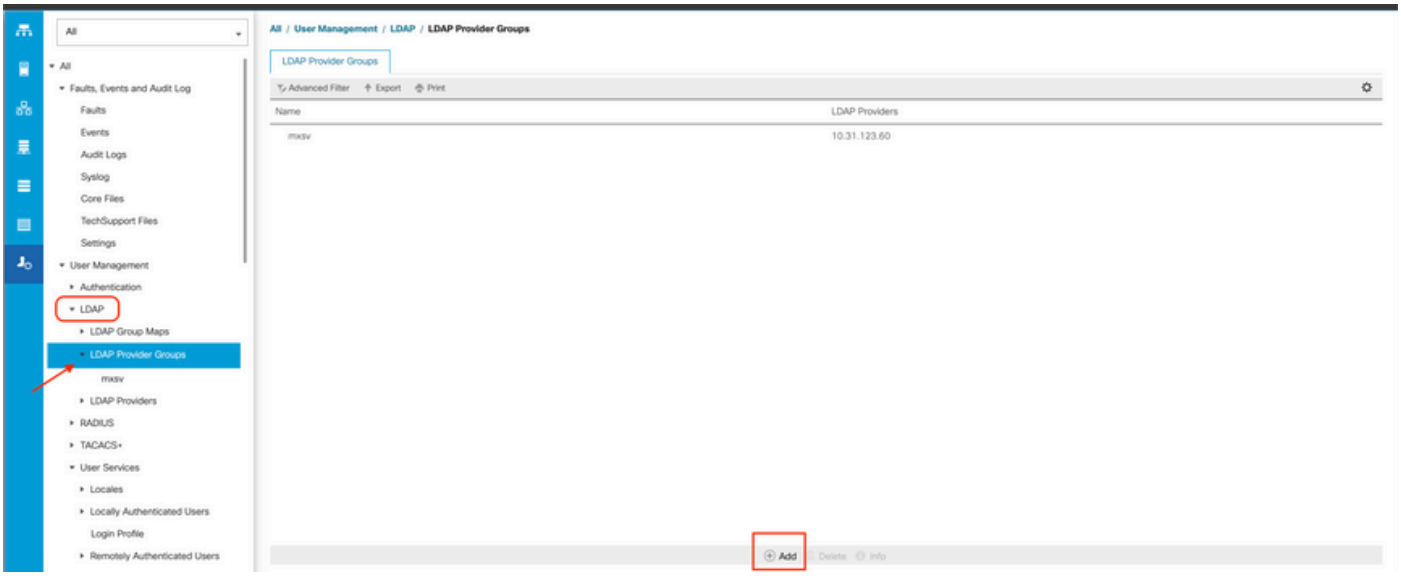
第二步： 点击 **Finish**.

> **注意**：在真实情况下，您很可能有多个LDAP提供程序。对于多个LDAP提供程序，您可以重复这些步骤，为每个LDAP提供程序配置LDAP组规则。但是，在此示例配置中，只有一个LDAP提供程序，因此不必这样做。

AD服务器的IP地址显示在“导航”(Navigation)窗格的**LDAP>LDAP提供程序**下。

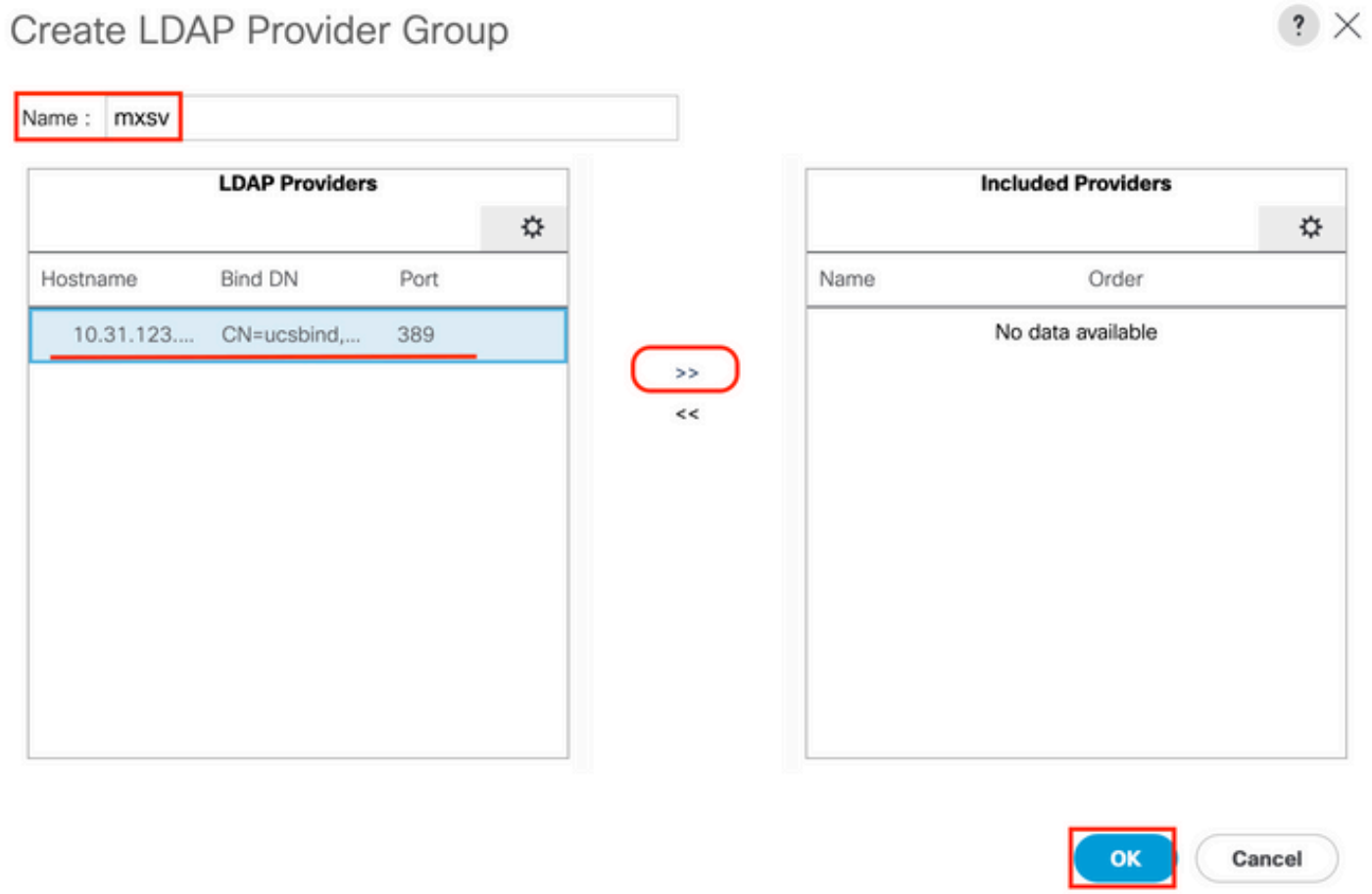
创建LDAP提供程序组

步骤1: 在“导航”(Navigation)窗格中，右键单击 **LDAP Provider Groups** 并选择 **Create LDAP Provider Group**.



第二步： 如果 **Create LDAP Provider Group** 对话框，请相应地填写信息：

- 如果 **Name** 字段中，输入组的唯一名称，例如 **LDAP Providers**.
- 如果 **LDAP Providers** 表，选择AD服务器的IP地址。
- 单击**>>**按钮将AD服务器添加到 **Included Providers** 表。



第三步： Click OK.

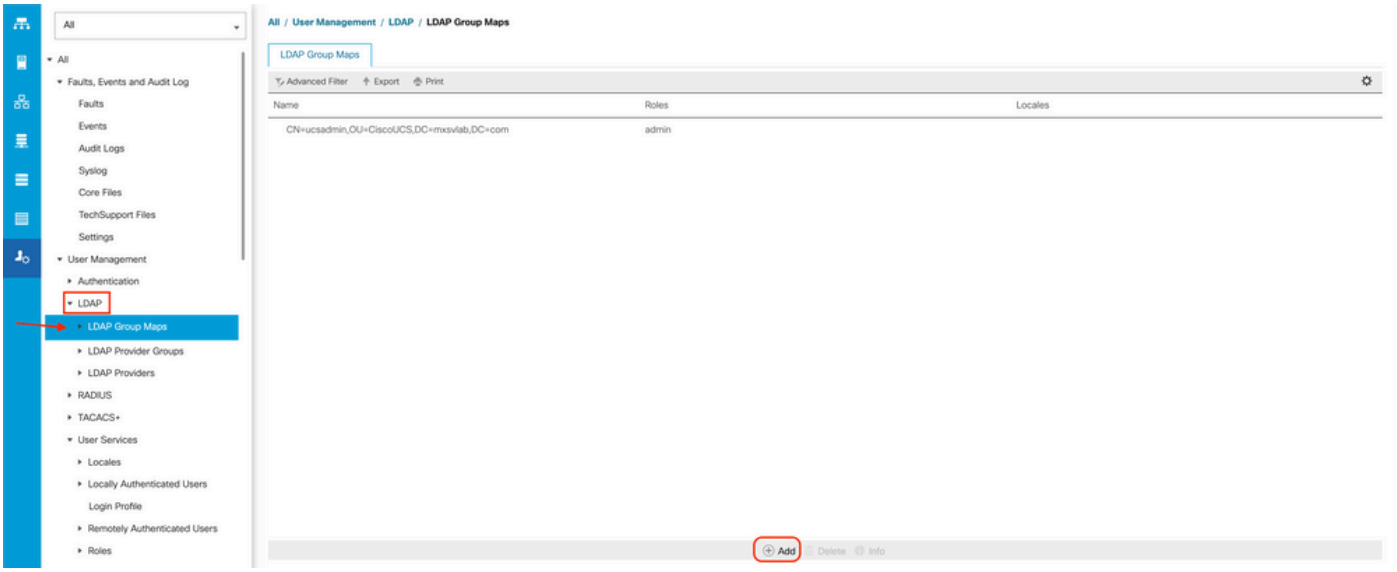
您的提供商组将显示在 **LDAP Provider Groups** 文件夹。

创建LDAP组映射

步骤1: 在Navigation窗格中，点击 **Admin**选项卡。

第二步： 在 **Admin** 选项卡，展开 **All > User Management > LDAP**.

第三步： 在工作窗格中，点击创建 **LDAP Group Map**.



第四步： 如果 **Create LDAP Group Map** 对话框，请相应地填写信息：

- 如果 **LDAP Group DN** 字段中，复制并粘贴LDAP组的AD服务器配置部分中的值。

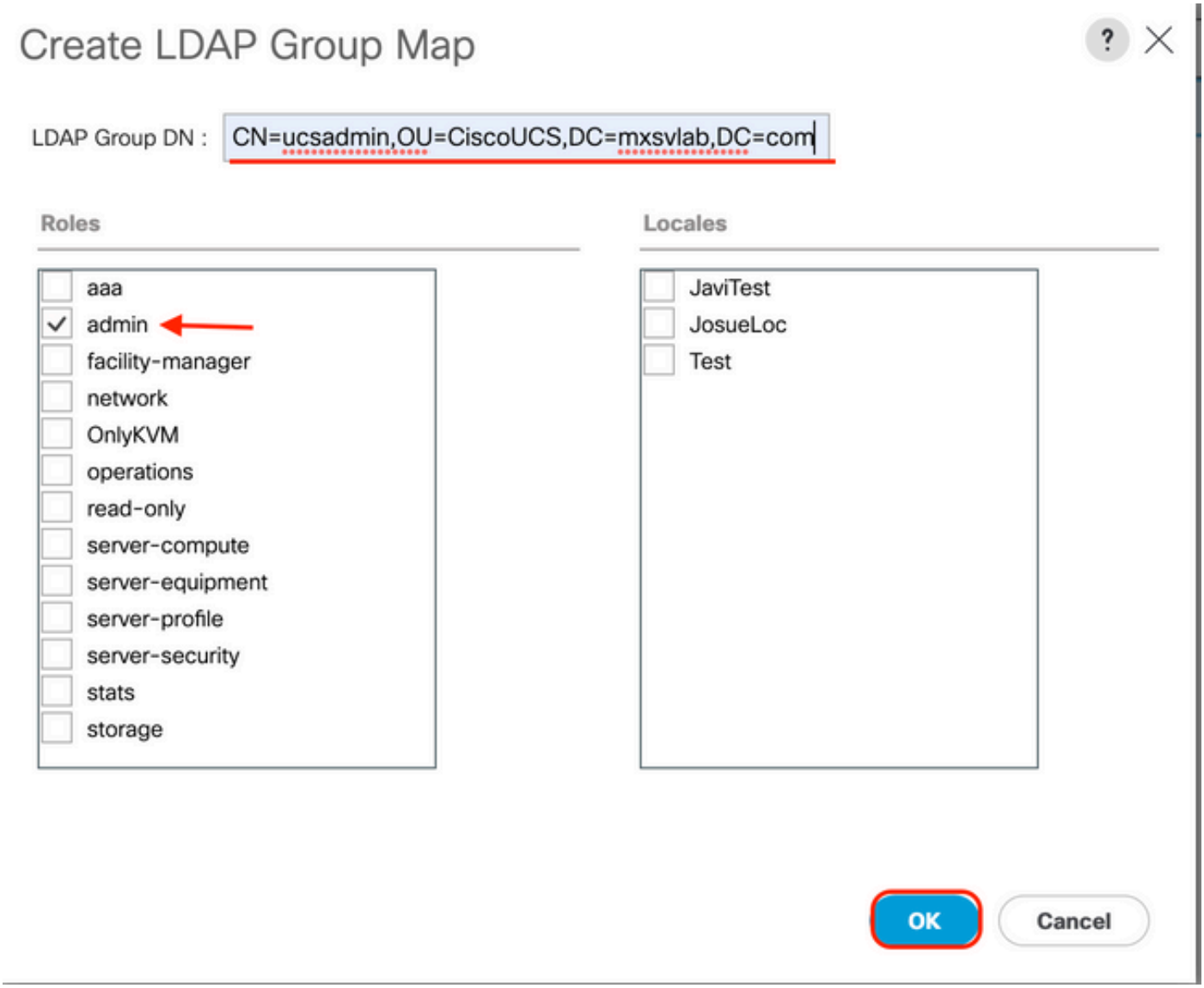
此步骤中请求的LDAP组DN值映射到在UCS组下在AD中创建的每个组的可分辨名称。

因此，在Cisco UCS Manager中输入的组DN值必须与AD服务器中的组DN值完全匹配。

在此示例配置中，此值为CN=ucsadmin，OU=CiscoUCS，DC=sampledesign，DC=com。

- 如果 **Roles** 表，点击 **Admin** 复选框，然后单击OK。

单击某个角色的复选框，表示您要将管理员权限分配给组映射中包含的所有用户。



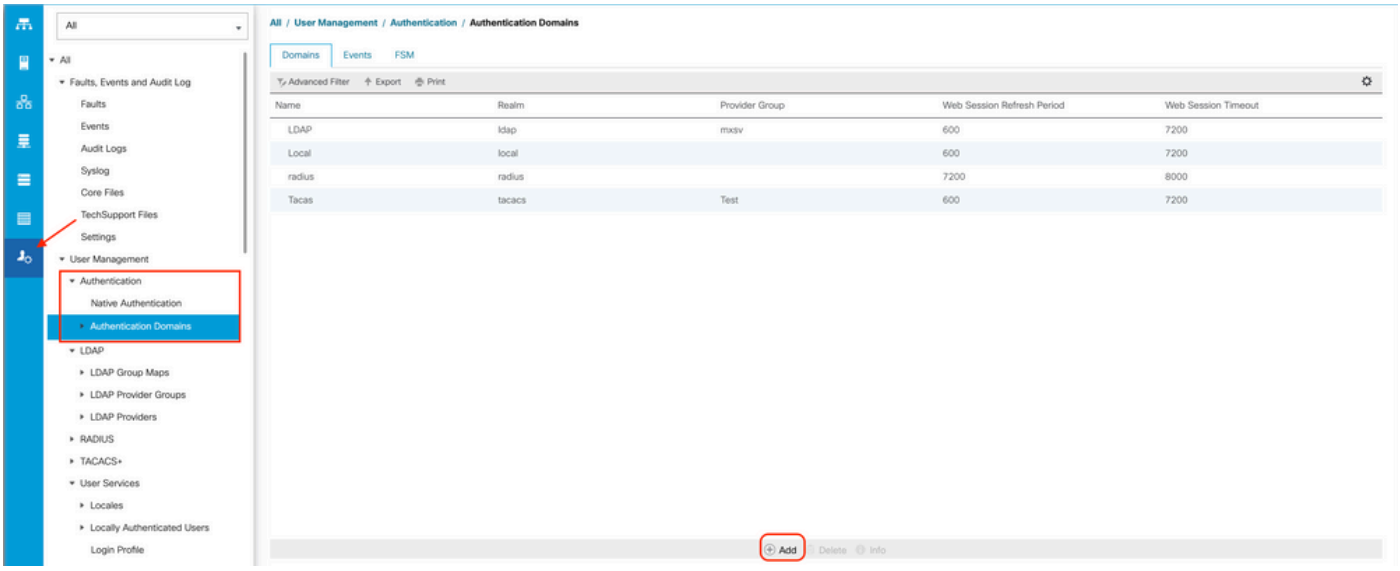
第五步： 为要测试的AD服务器中的每个剩余角色创建新的LDAP组映射（使用之前从AD记录的信息）。

下一步：创建LDAP身份验证域。

创建LDAP身份验证域

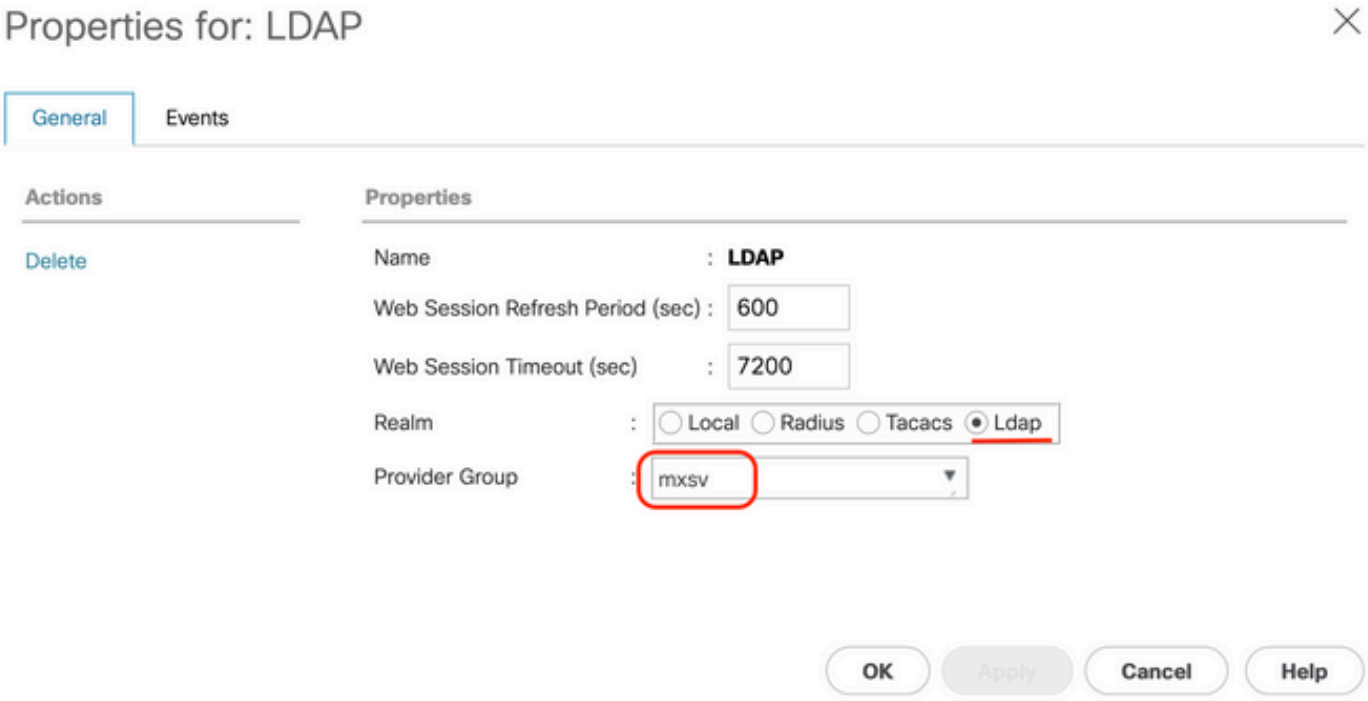
步骤1: 在 管理员 选项卡，展开 **All > User Management > Authentication**

第二步： 右键单击 **身份验证** Authentication Domains **并选择** Create a Domain.



第三步：在 中**Create a Domain** 对话框，请完成下一步：

- 如果 **Name** 字段中，键入域的名称，例如LDAP。
- 如果 **Realm** 区域，单击 **Ldap** 单选按钮.
- 从 **Provider Group** 下拉列表中，选择 **LDAP Provider Group** 并点击**确定**。



身份验证域显示在 **Authentication Domains**.

验证

Ping到 **LDAP Provider IP** 或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
```

要从NX-OS测试身份验证，请在执行模式下使用 **test aaa** 命令（仅适用于NXOS）。

我们验证服务器的配置：

```
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
```

常见LDAP问题。

- 基本配置.
- 密码错误或字符无效。
- 错误的端口或过滤器字段。

- 由于防火墙或代理规则，无法与提供商通信。
- FSM不是100%。
- 证书问题。

故障排除

验证UCSM LDAP配置：

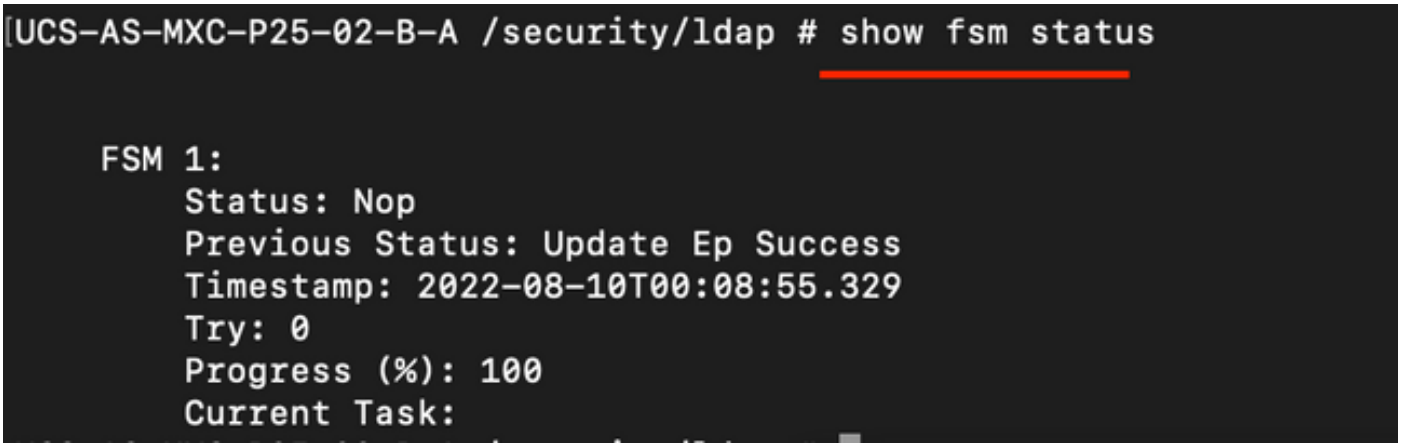
您必须确保UCSM已成功实施配置，因为 **Finite State Machine (FSM)** 显示为100%完成。

要从UCSM的命令行验证配置，请执行以下操作：

```
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
```



从NXOS验证配置：

```
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
```

发现错误的最有效方法是启用调试，通过此输出，我们可以看到阻止通信的组、连接和错误消息。

- 打开与FI的SSH会话并以本地用户身份登录，然后切换到NX-OS CLI上下文并启动终端监控。

```
ucs # connect nxos

ucs(nxos)# terminal monitor
```

- 启用调试标志，并验证到日志文件的SSH会话输出。

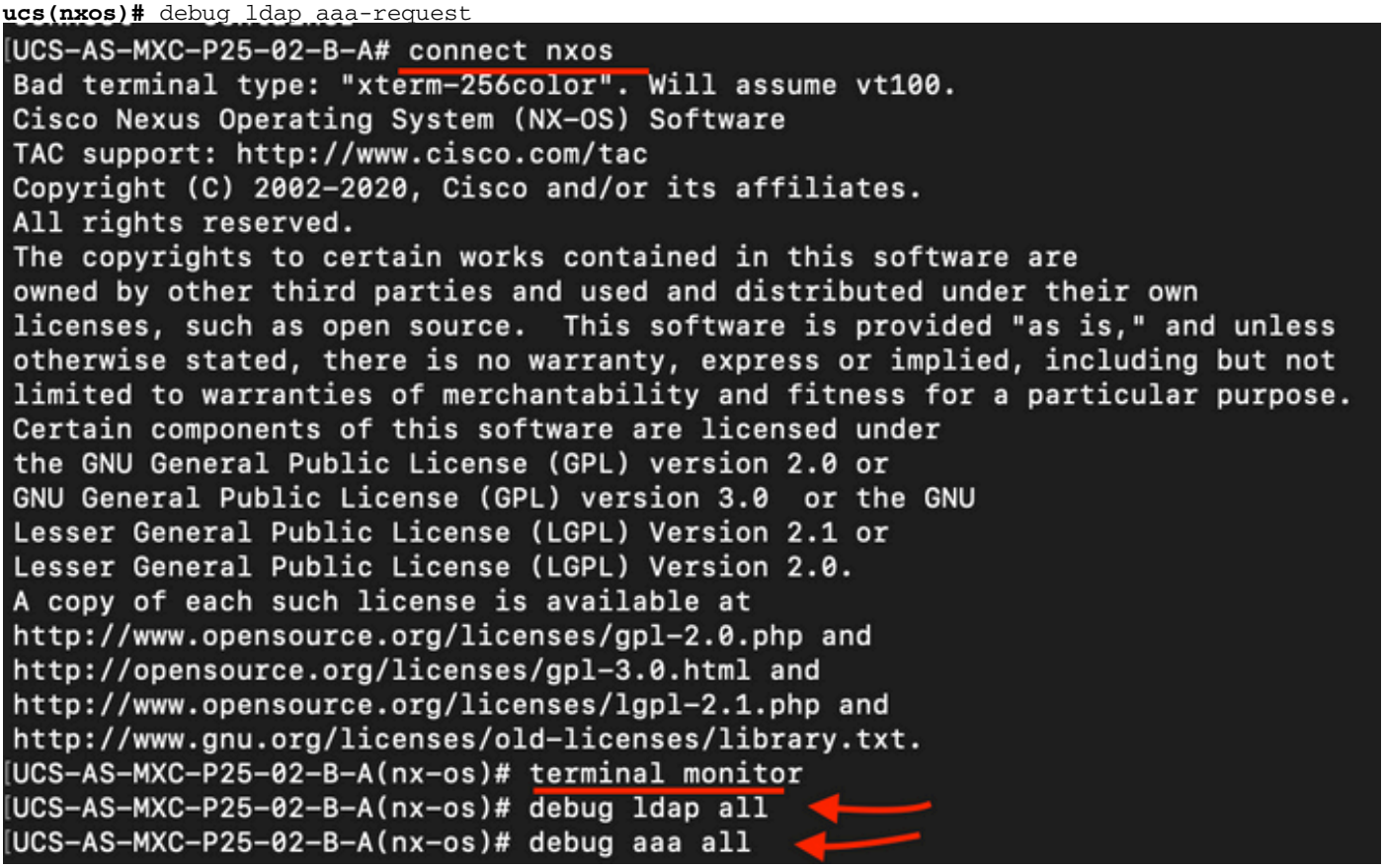
```
ucs(nxos)# debug aaa all <<< not required, incase of debugging authentication problems

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
```



- 现在打开新的GUI或CLI会话，并尝试以远程(LDAP)用户身份登录。
- 收到登录失败消息后，关闭调试。

相关信息

- [技术支持和文档 - Cisco Systems]
- UCSM LDAP示例配置
- Cisco UCS C系列GUI配置指南

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。