在UCS Manager中配置LDAP

目錄

簡介

本文檔介紹使用LDAP協定進行遠端伺服器訪問的配置，該配置位於 **Unified Computing System Manager Domain (UCSM).**

必要條件

需求

思科建議瞭解以下主題：

- **Unified Computing System Manager Domain (UCSM)**
- 本地和遠端身份驗證
- **Lightweight Directory Access Protocol (LDAP)**
- **Microsoft Active Directory (MS-AD)**

採用元件

本文中的資訊係根據以下軟體和硬體版本：

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

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

背景資訊

Lightweight Directory Access Protocol (LDAP) 是為目錄服務開發的核心協定之一，用於安全地管理使用者及其對IT資源的訪問許可權。

目前，大多數目錄服務仍使用LDAP，儘管它們還可以使用其他協定，如Kerberos、SAML、RADIUS、SMB、Oauth等。

設定

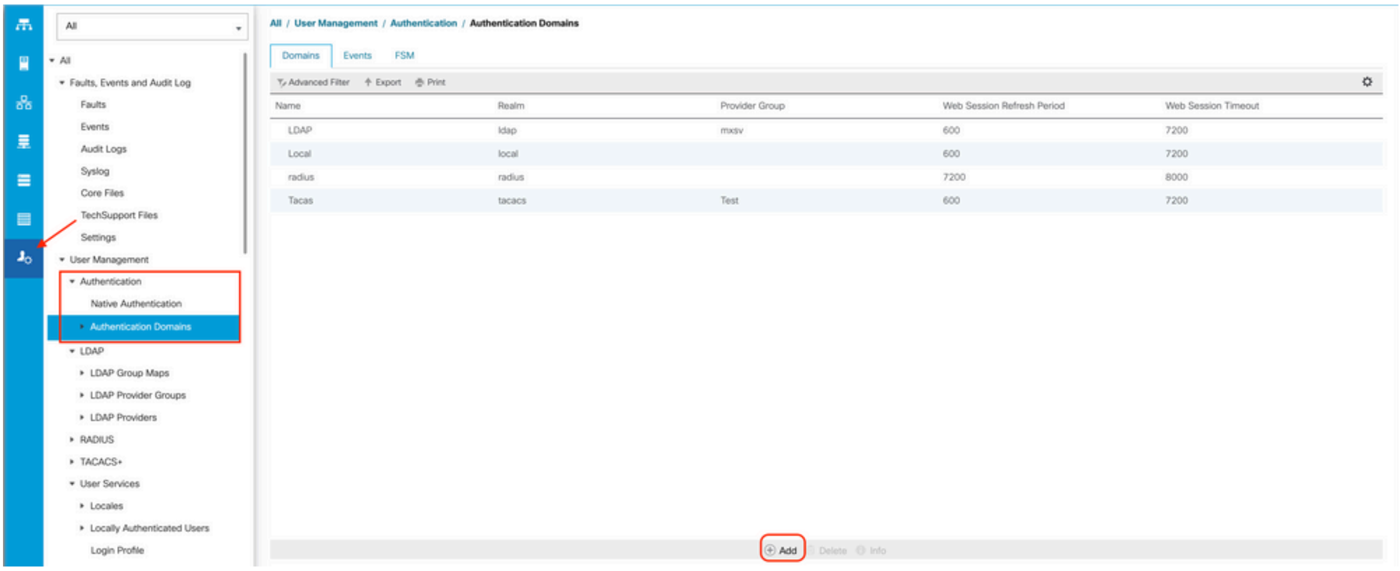
開始之前

登入**Cisco UCS Manager** GUI作為管理使用者。

建立本地身份驗證域

步驟1. 在 **Navigation** 中，按一下 **Admin** 頁籤。

步驟2. 在 **Admin** 頁籤，展開 **All > User Management > Authentication**

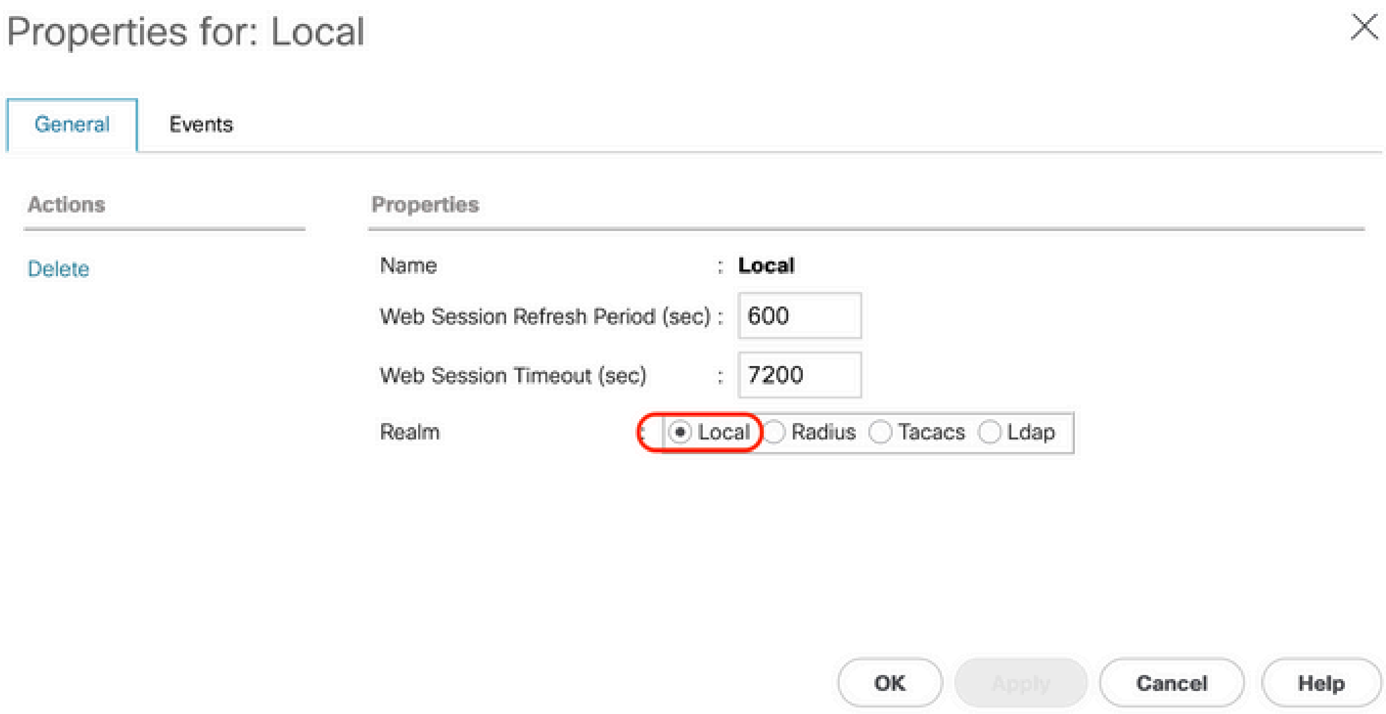


Name	Realm	Provider Group	Web Session Refresh Period	Web Session Timeout
LDAP	ldap	mxsv	600	7200
Local	local		600	7200
radius	radius		7200	8000
Tacas	tacacs	Test	600	7200

步驟3. 按一下右鍵 **Authentication Domains** 並選取 **Create a Domain.**

步驟4. 對於 **Name** 欄位，型別 **Local.**

步驟5. 對於 **Realm**，按一下 **Local** 單選按鈕。



Properties for: Local

Name : **Local**

Web Session Refresh Period (sec) : 600

Web Session Timeout (sec) : 7200

Realm : ● Local ○ Radius ○ Tacacs ○ Ldap

步驟6.按一下 **OK.**

建立LDAP提供程式

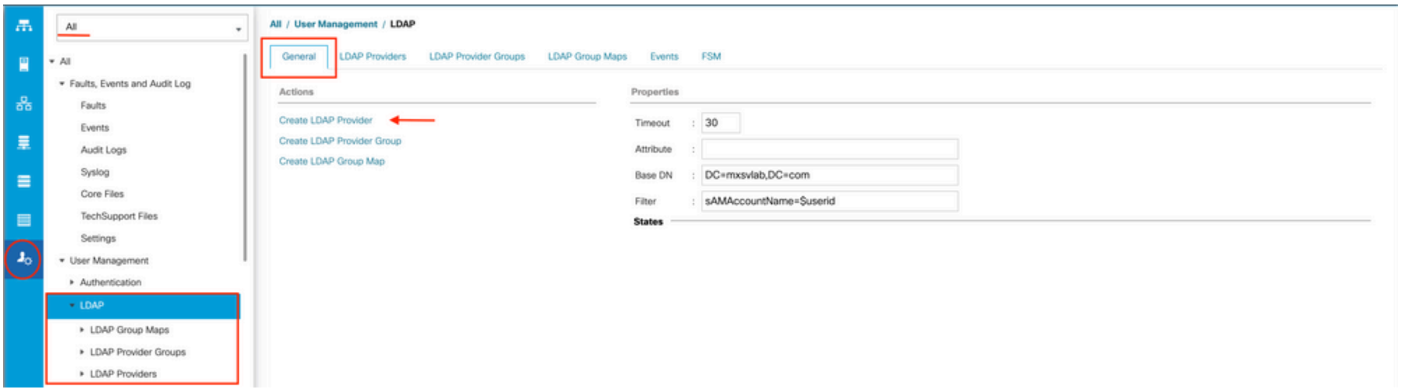
此示例配置不包括使用SSL配置LDAP的步驟。

步驟1.在 **Navigation** 中，按一下 **Admin** 頁籤。

步驟2. 在 **Admin** 頁籤，展開 **All > User Management > LDAP.**

步驟3. 在 **Work** 中，按一下 **General** 頁籤。

步驟4. 在 **Actions** 區域，按一下 **Create LDAP Provider**



Timeout : 30

Attribute :

Base DN : DC=mxsvlab,DC=com

Filter : sAMAccountName=$userid

步驟5. 在 **Create LDAP Provider** 頁面，輸入相應的資訊：

- 在 **Hostname**欄位中，鍵入AD伺服器的IP地址或主機名。
- 在 **Order** 欄位，接受 **lowest-available** 預設值。
- 在 **BindDN** 欄位中，從AD配置複製並貼上BindDN。

對於此示例配置，BindDN值為**CN=ucsbind，OU=CiscoUCS，DC=mxsvlab，DC=com**。

- 在 **BaseDN** 欄位中，從AD配置複製並貼上BaseDN。

對於此示例配置，BaseDN值為**DC=mxsvlab，DC=com**。

- 離開 **Enable SSL** 覈取方塊。
- 在 **Port** 欄位中，接受389預設值。
- 在 **Filter** 欄位中，從AD配置複製並貼上過濾器屬性。

Cisco UCS使用篩選值來確定使用者名稱(在登入螢幕上提供，由 **Cisco UCS Manager**)在AD中。

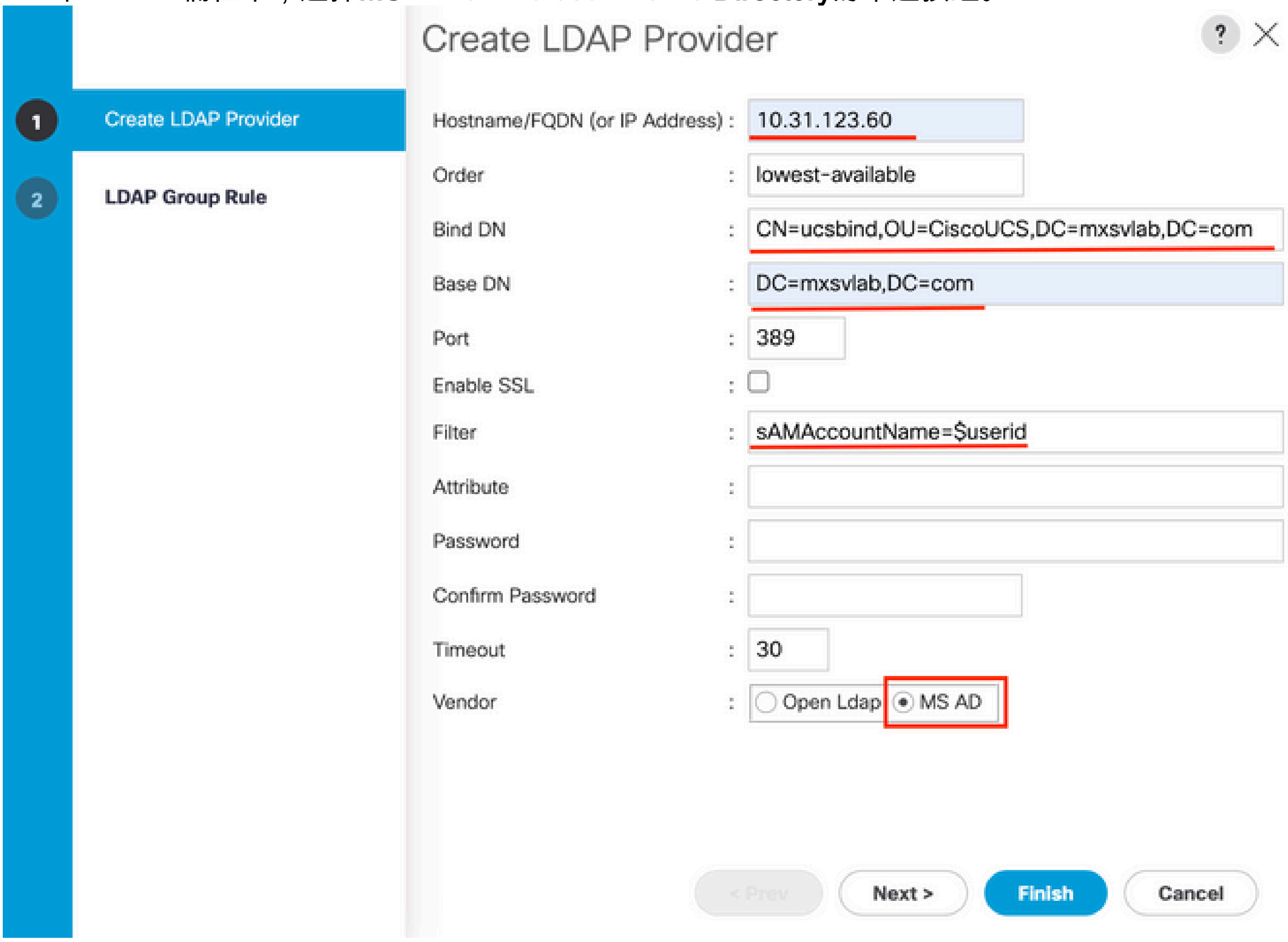
對於此示例配置，篩選器值為**sAMAccountName=$userid**，其中$useridis **user name** 在 **Cisco UCS Manager** 登入螢幕。

- 離開 **Attribute** 欄位為空。
- 在 **Password** 欄位中，鍵入AD中配置的ucsbbind帳戶的密碼。

如果您需要返回到 **Create LDAP Provider wizard** 要重置密碼，如果密碼欄位為空，則不要驚慌。

其 **Set: yes** 密碼欄位旁顯示的消息表明已設定密碼。

- 在 **Confirm Password** 欄位中，重新鍵入AD中配置的ucsbbind帳戶的密碼。
- 在 **Timeout** 欄位，接受 30默認值。
- 在 **Vendor** 欄位中，選擇**MS**-ADfor Microsoft Active **Directory**的單選按鈕。



Create LDAP Provider

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

步驟6. 按一下 **Next**

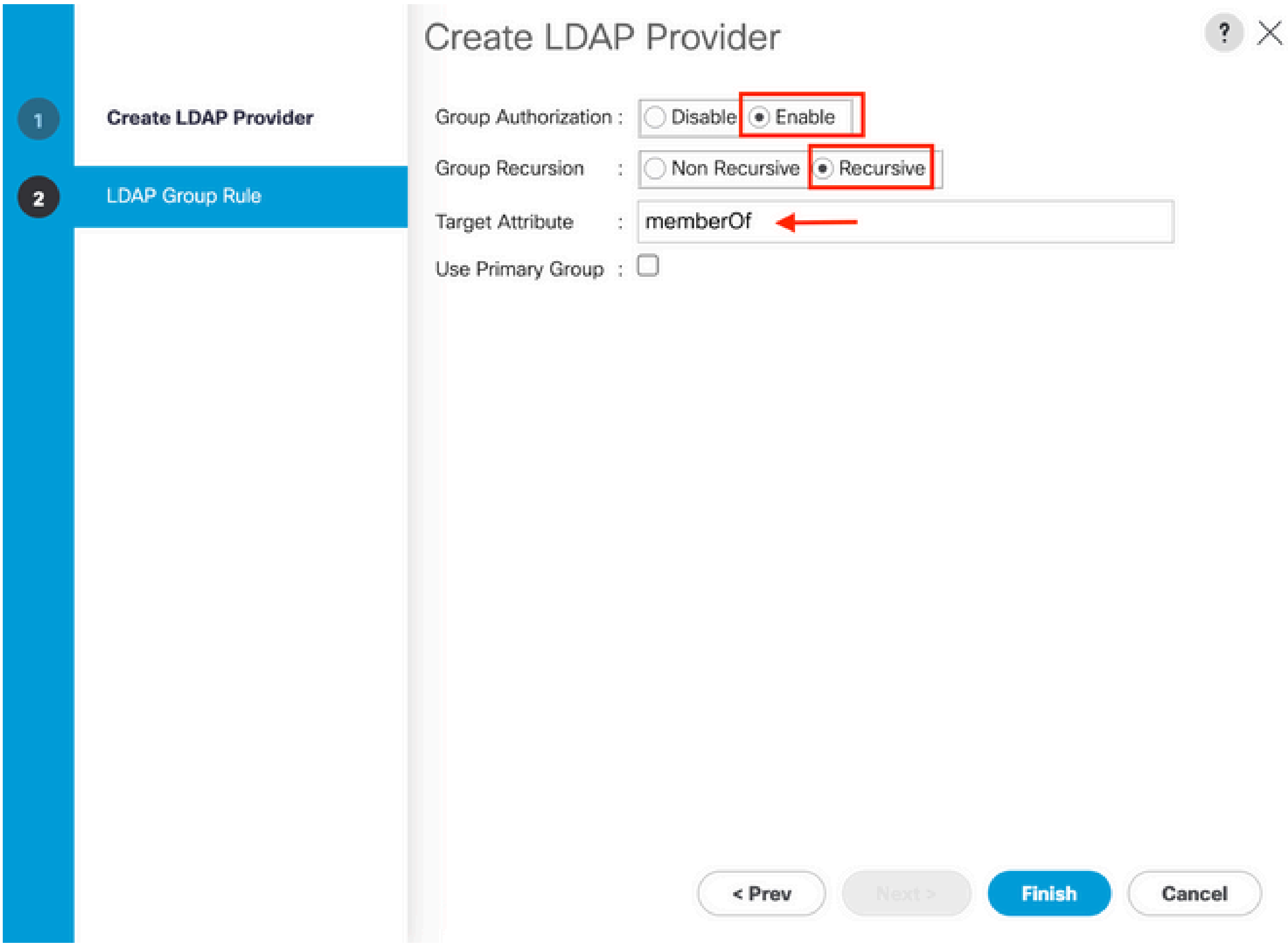
LDAP組規則配置

步驟1. 在**LDAP Group Rule** 頁面，填寫以下欄位：

- 對於 **Group Authentication** 欄位中，按一下 **Enable** 單選按鈕。
- 對於 **Group Recursion** 欄位中，按一下 **Recursive** 單選按鈕。 這樣，系統可以逐級向下搜尋直到找到使用者。

如果 **Group Recursion** 設定為 **Non-Recursive**，它將UCS限制在第一級搜尋，即使搜尋找不到合格的使用者。

- 在 **Target Attribute** 欄位，接受**memberOf** 預設值。



Create LDAP Provider

Group Authorization : ○ Disable ● Enable

Group Recursion : ○ Non Recursive ● Recursive

Target Attribute : memberOf

Use Primary Group : □

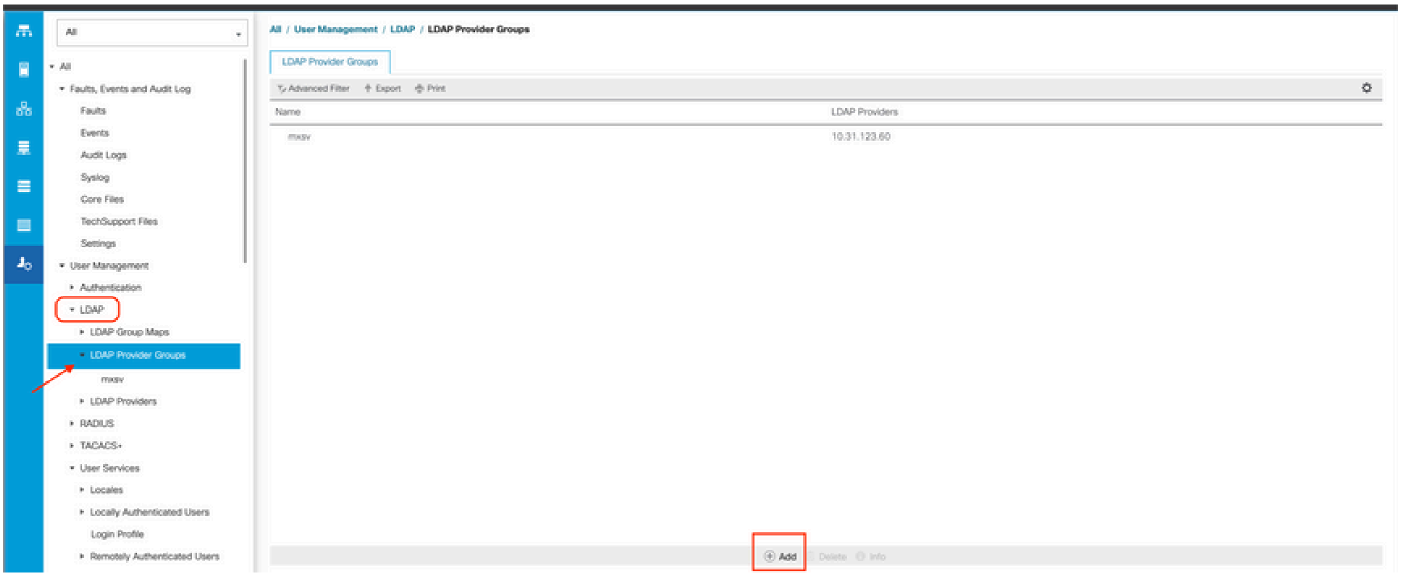
步驟2。 點選 **Finish.**

> **注意**：在真實情況下，您很可能有多個LDAP提供程式。對於多個LDAP提供程式，您需要重複這些步驟，為每個LDAP提供程式配置LDAP組規則。但是，在此示例配置中，只有一個LDAP提供程式，因此不必這樣做。

AD伺服器的IP地址顯示在「導航」(Navigation)窗格的「LDAP」(**LDAP)>「LDAP提供程式」(LDAP Providers**)下。

建立LDAP提供程式組

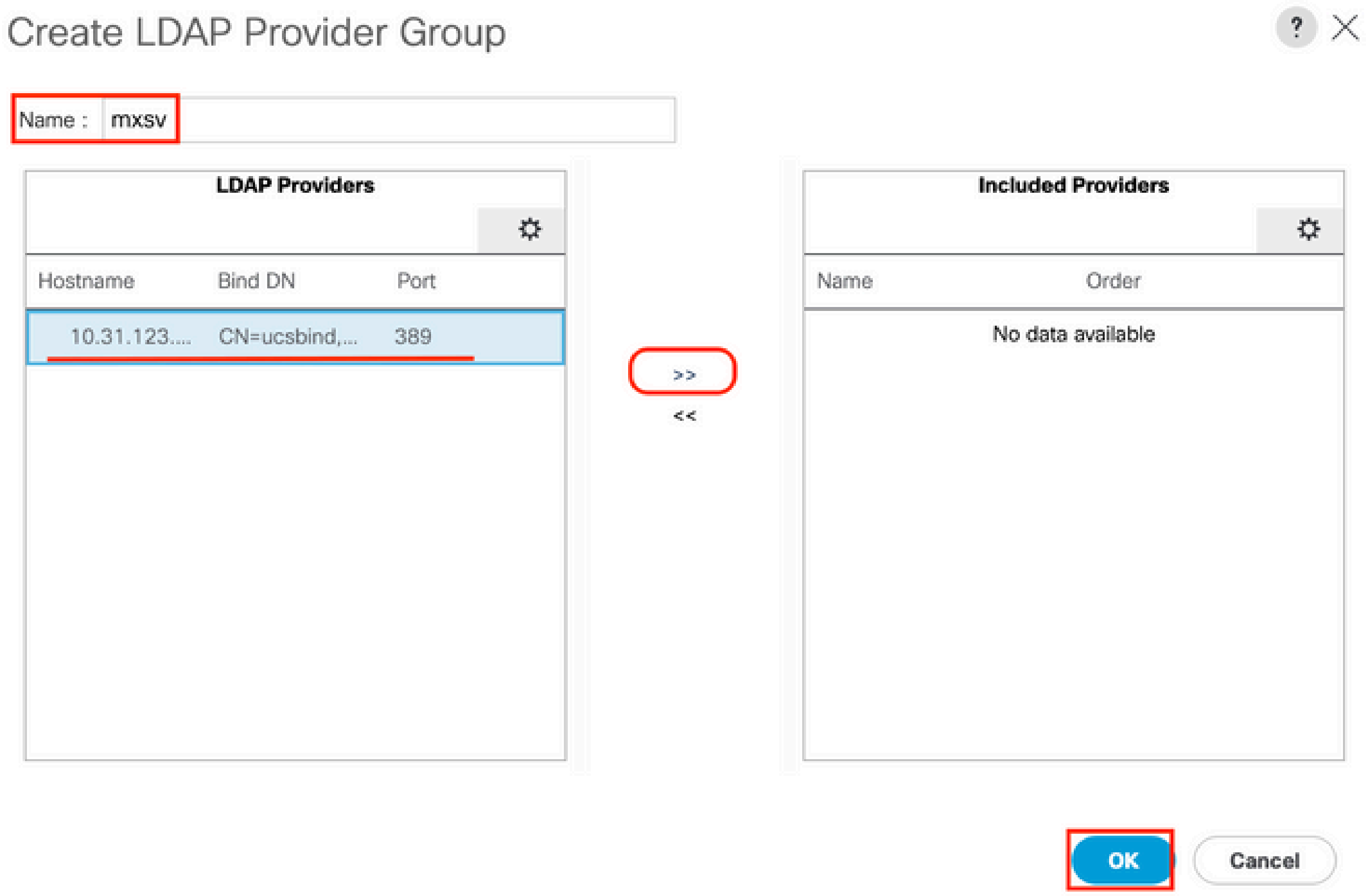
步驟1. 在「導航」窗格中，按一下右鍵 **LDAP Provider Groups** 並選取 **Create LDAP Provider Group.**



Name	LDAP Providers
mxsv	10.31.123.60

步驟2. 在 **Create LDAP Provider Group** 對話方塊中，適當填寫資訊：

- 在 **Name** 欄位中，輸入組的唯一名稱，例如 **LDAP Providers.**
- 在 **LDAP Providers** 表，選擇您的AD伺服器的IP地址。
- 按一下**>>**按鈕將AD伺服器新增到 **Included Providers** 表。



Name : mxsv

LDAP Providers

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

Included Providers

Name	Order
No data available	

步驟3. 按一下「OK」（確定）。

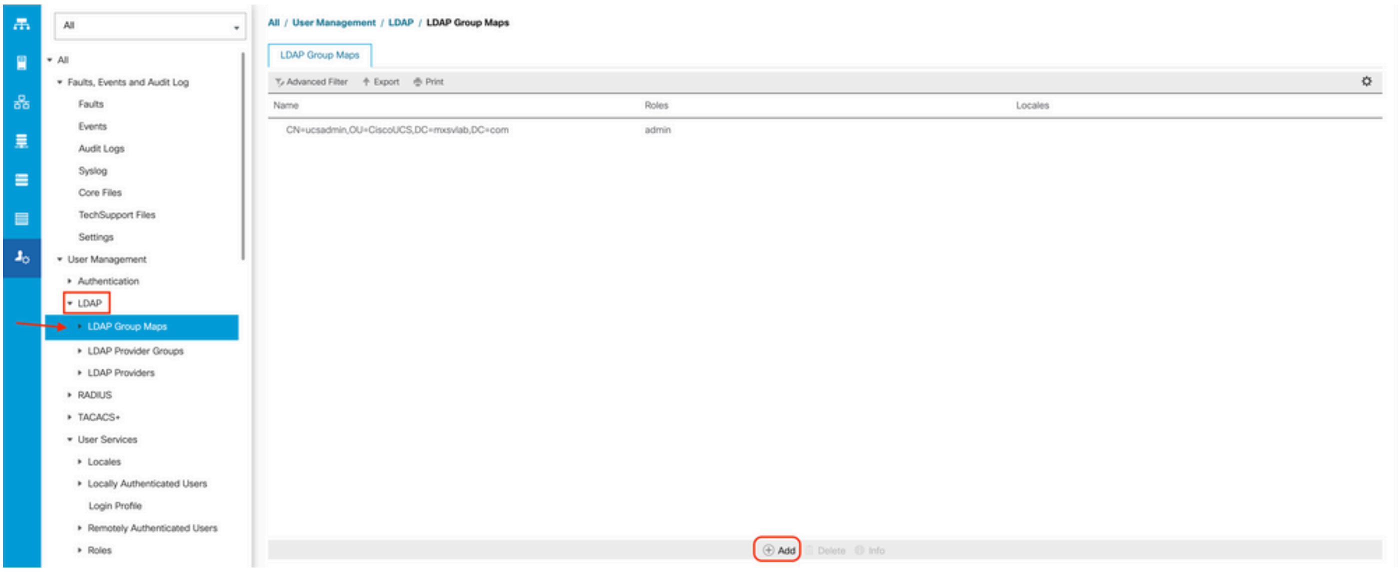
您的提供商組將顯示在 **LDAP Provider Groups** 資料夾。

建立LDAP組對映

步驟1. 在「導航」窗格中，按一下 **Admin**頁籤。

步驟2. 在 **Admin** 頁籤，展開 **All > User Management > LDAP.**

步驟3. 在Work窗格中，點選Create **LDAP Group Map.**



Name	Roles	Locales
CN=ucsadmin,OU=CiscoUCS,DC=mxsvlab,DC=com	admin	

步驟4. 在 **Create LDAP Group Map** 對話方塊中，適當填寫資訊：

- 在 **LDAP Group DN** 欄位中，複製並貼上在LDAP組的AD伺服器配置部分中的值。

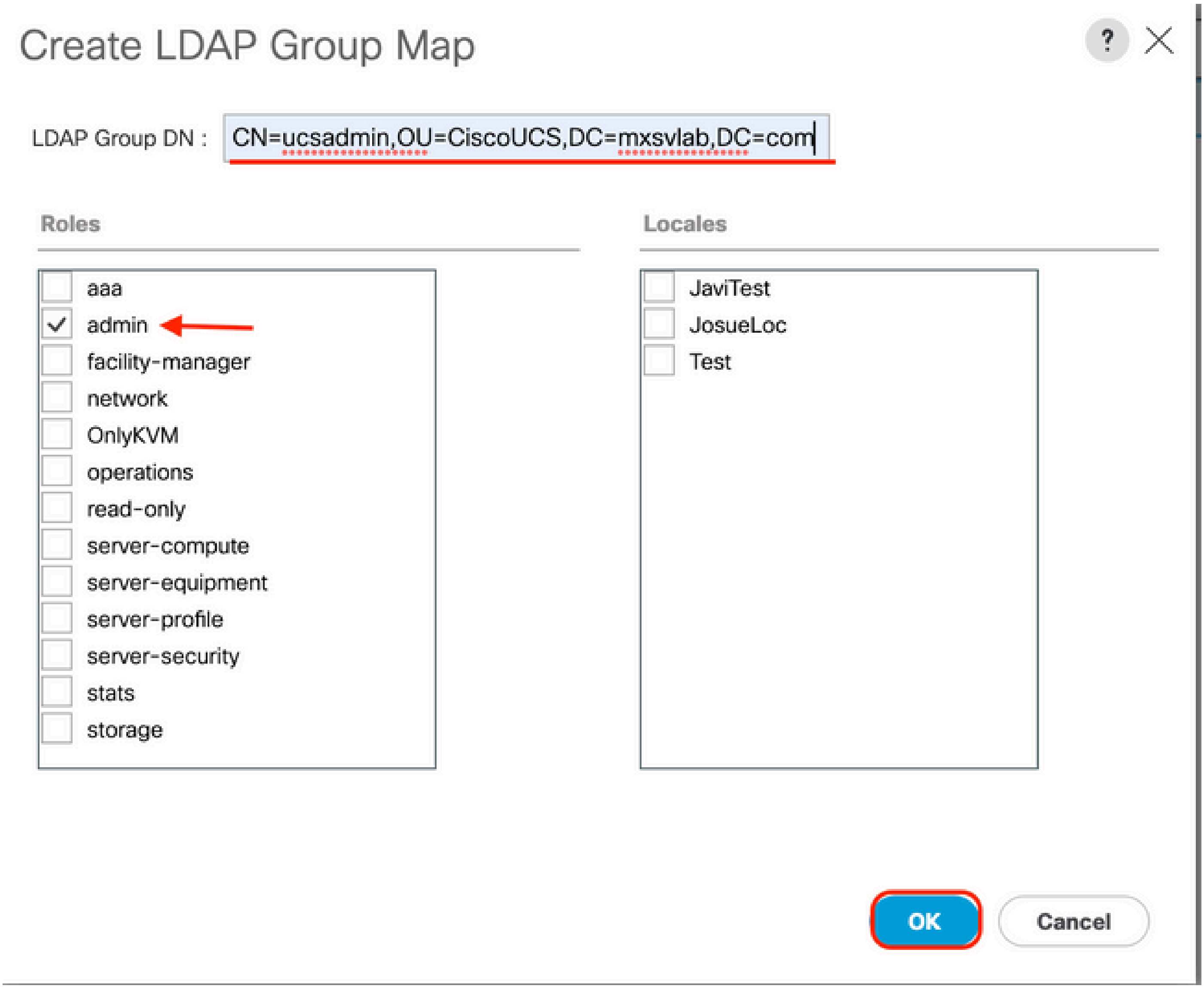
在此步驟中請求的LDAP組DN值對映到在UCS組下在AD中建立的每個組的唯一判別名。

因此，在Cisco UCS Manager中輸入的組DN值必須與AD伺服器中的組DN值完全匹配。

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

- 在 **Roles** 表中，按一下 **Admin** 覈取方塊，然後按一下**OK**。

按一下角色對應的覈取方塊表示您要為組對映中包含的所有使用者分配管理員許可權。


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

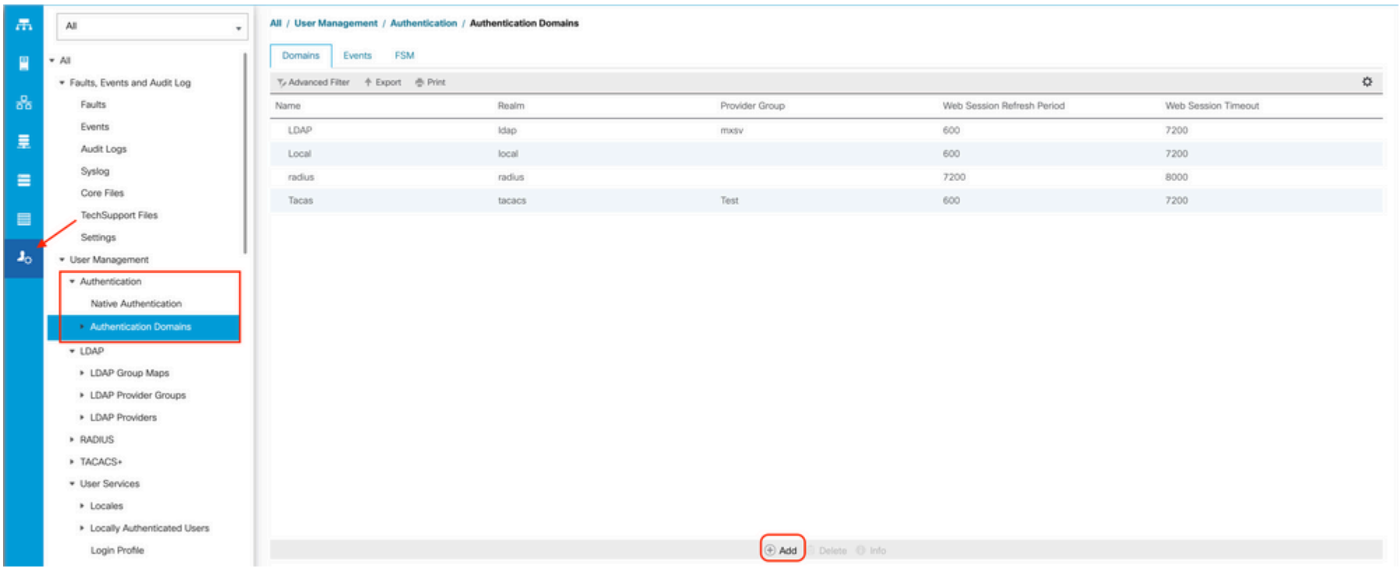
步驟5. 為您要測試的AD伺服器中的每個保留角色建立新的LDAP組對映（使用之前從AD記錄的資訊）。

下一步：建立LDAP身份驗證域。

建立LDAP身份驗證域

步驟1. 在 Admin 頁籤，展開 **All > User Management > Authentication**

步驟2. 按一下右鍵 **驗證** **Authentication Domains** **並選取** **Create a Domain.**

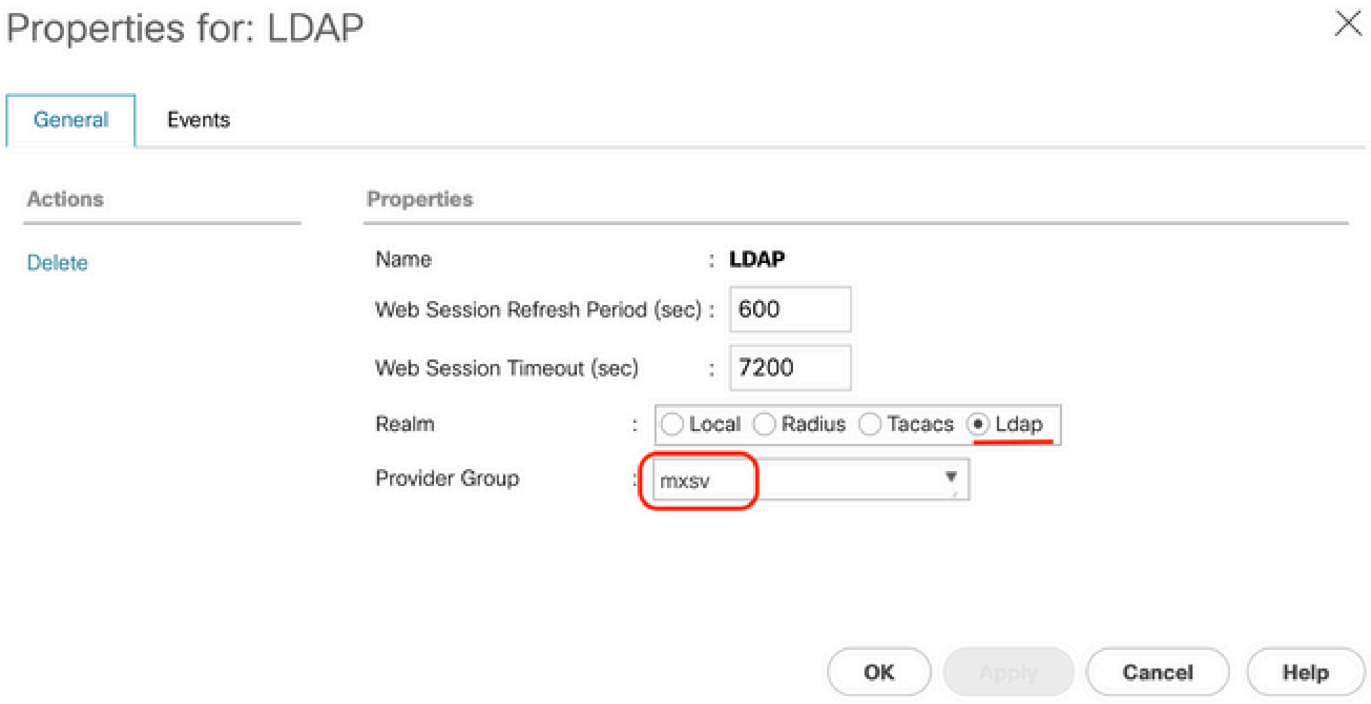


All / User Management / Authentication / Authentication Domains

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

步驟3.在&nbsp中**Create a Domain** 對話方塊中，完成以下操作：

- 在 **Name** 欄位中，鍵入域的名稱（例如LDAP）。
- 在 **Realm** 區域中，按一下 **Ldap** 單選按鈕。
- 從 **Provider Group** 下拉選單中，選擇 **LDAP Provider Group** ，然後按一下OK。



Properties for: LDAP

Name : **LDAP**

Web Session Refresh Period (sec) : 600

Web Session Timeout (sec) : 7200

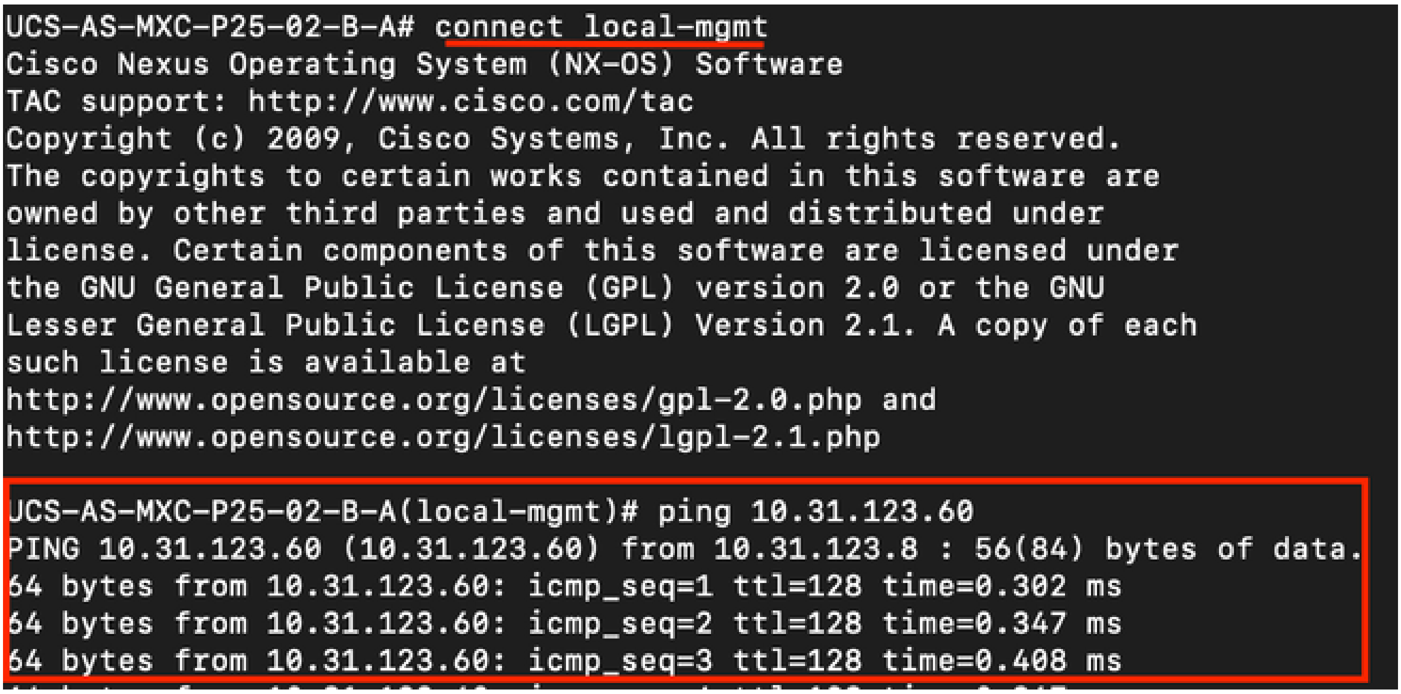
Realm : ○ Local ○ Radius ○ Tacacs ● Ldap

Provider Group : mxsv

身份驗證域出現在 **Authentication Domains**.

驗證

Ping到 **LDAP Provider IP** 或FQDN:



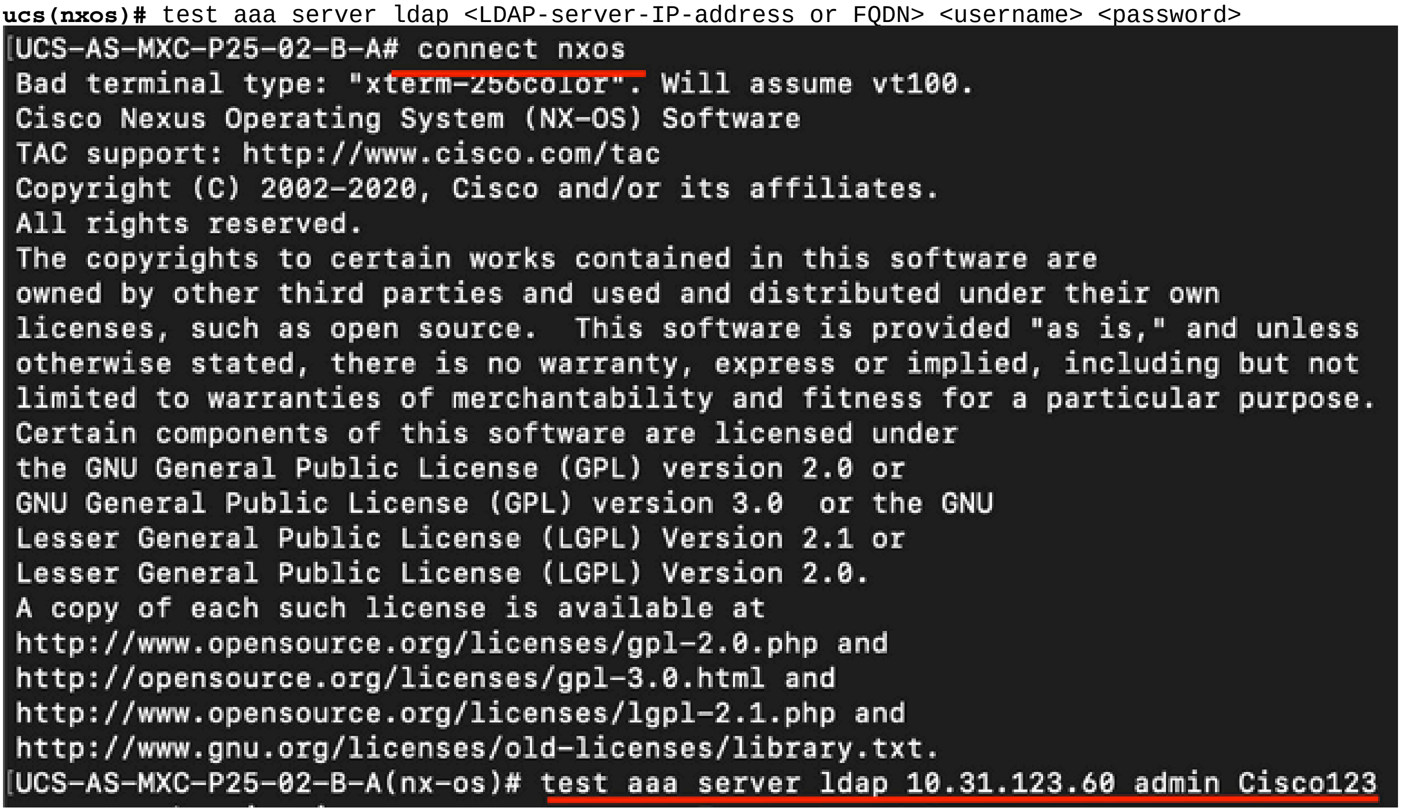
```
UCS-AS-MXC-P25-02-B-A# connect local-mgmt
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (c) 2009, Cisco Systems, Inc. All rights reserved.
The copyrights to certain works contained in this software are
owned by other third parties and used and distributed 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
```

要測試來自NX-OS的身份驗證，請使用 **test aaa** 命令（僅適用於NXOS）。

我們驗證伺服器的配置：

```
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
```

常見LDAP問題。

- 基本配置。
- 密碼錯誤或字元無效。
- 錯誤的埠或過濾器欄位。

- 由於防火牆或代理規則，無法與提供商通訊。
- FSM不是100%。
- 憑證問題。

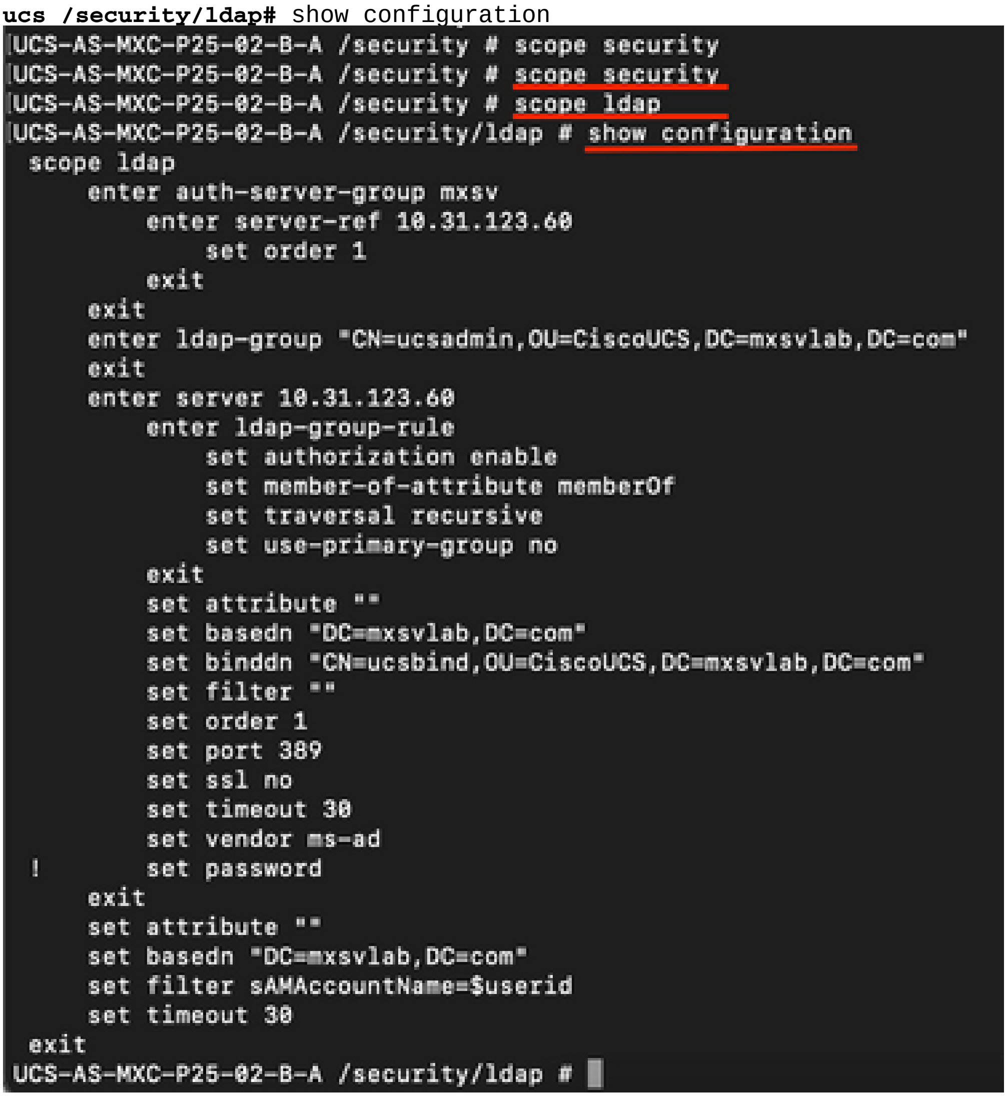
疑難排解

驗證UCSM LDAP配置：

您必須確保UCSM已成功實施配置，因為 **Finite State Machine (FSM)** 顯示為100%完成。

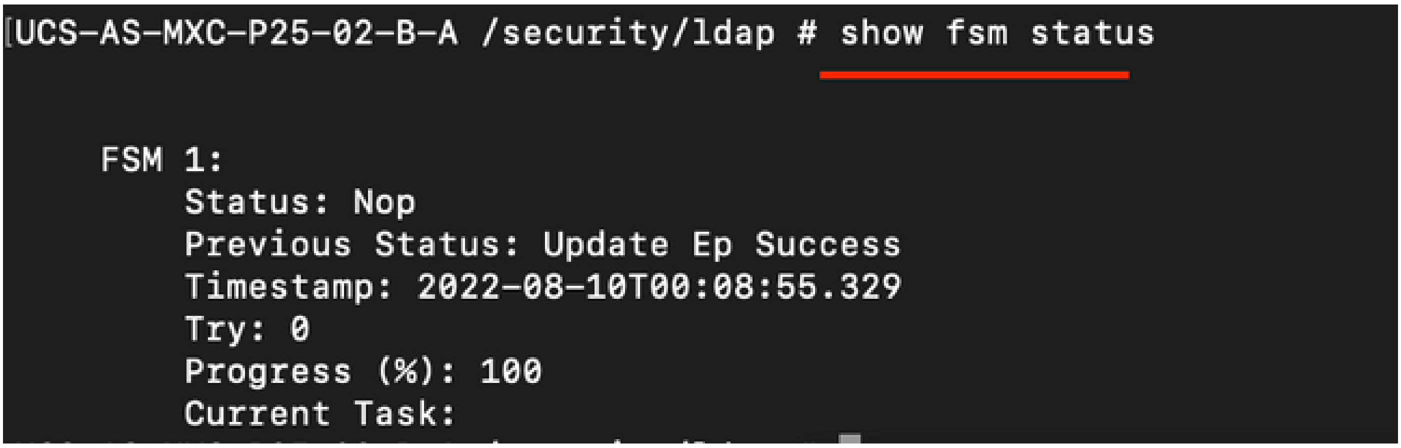
要從UCSM的命令列驗證配置：

```
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
```

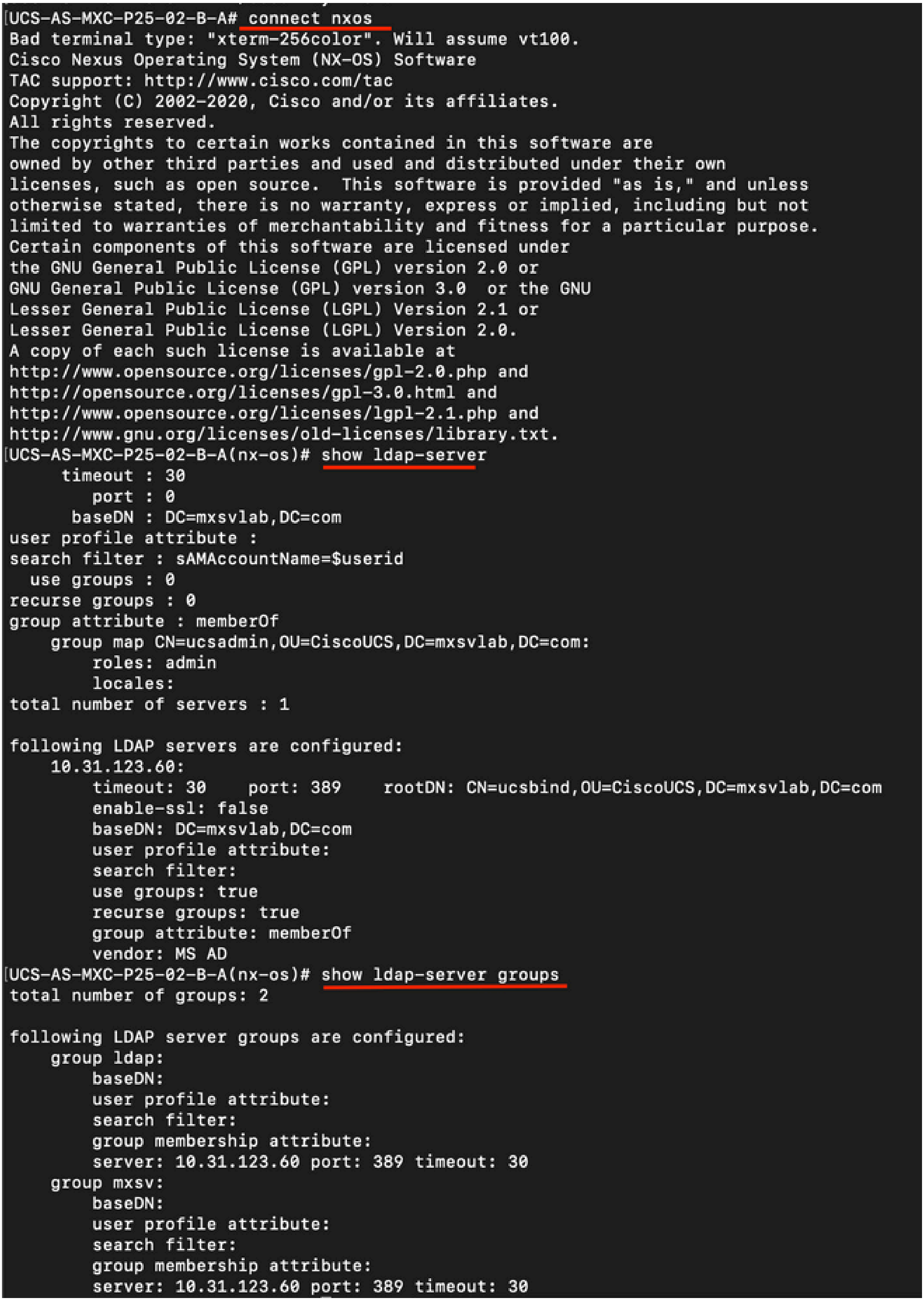


```
[UCS-AS-MXC-P25-02-B-A /security/ldap # show fsm status

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

從NXOS驗證配置：

```
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
```

檢視錯誤的最有效方法是啟用調試，通過此輸出，我們可以看到阻止通訊的組、連線和錯誤消息。

- 開啟與FI的SSH會話並以本地使用者身份登入，然後轉到NX-OS CLI上下文並啟動終端監視器。

```
 ucs # connect nxos

ucs(nxos)# terminal monitor
```

- 啟用調試標誌並驗證SSH會話輸出到日誌檔案。

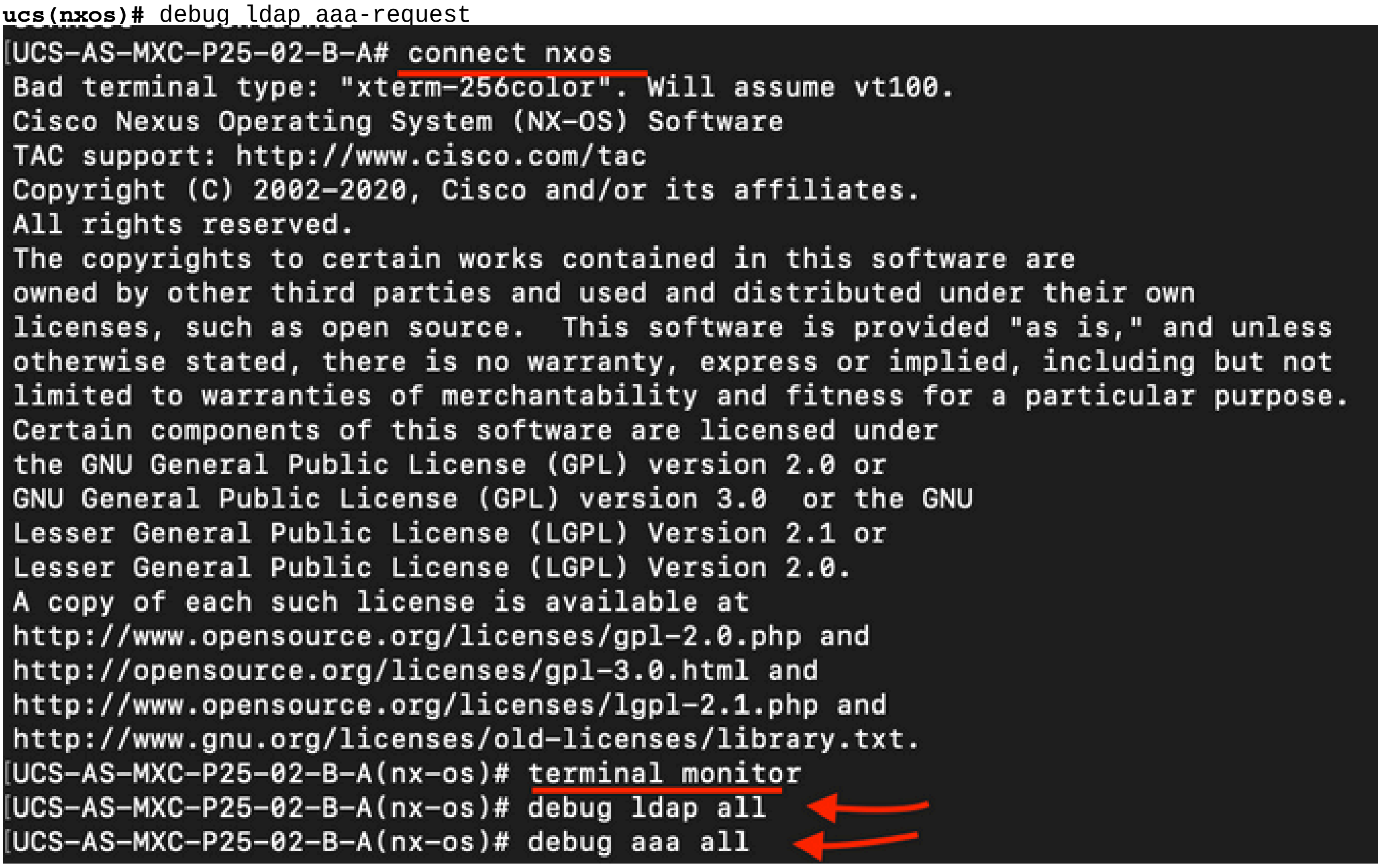
```
 ucs(nxos)# debug aaa all <<< not required, incase of debugging authentication problems

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
```

- 現在開啟一個新的GUI或CLI會話，並嘗試以遠端(LDAP)使用者身份登入。
- 收到登入失敗消息後，關閉調試。

相關資訊

- **技術支援與文件 - Cisco Systems**
- UCSM LDAP示例配置
- Cisco UCS C系列GUI配置指南

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。