UCS ManagerでのLDAPの設定

内容

概要

このドキュメントでは、LDAPプロトコルを使用したリモートサーバアクセスの設定について説明します。 **Unified Computing System Manager Domain (UCSM).**

前提条件

要件

次の項目に関する知識があることが推奨されます。

- **Unified Computing System Manager Domain (UCSM)**
- ローカルおよびリモート認証
- **Lightweight Directory Access Protocol (LDAP)**
- **Microsoft Active Directory (MS-AD)**

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- **Cisco UCS 6454 Fabric Interconnect**
- UCSMバージョン4.0(4k)
- **Microsoft Active Directory (MS-AD)**

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています

。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

背景説明

Lightweight Directory Access Protocol (LDAP) は、ユーザとITリソースへのアクセス権を安全に管理するディレクトリサービス向けに開発されたコアプロトコルの1つです。

現在でもほとんどのディレクトリサービスはLDAPを使用していますが、Kerberos、SAML、RADIUS、SMB、Oauthなどの追加プロトコルも使用できます。

設定

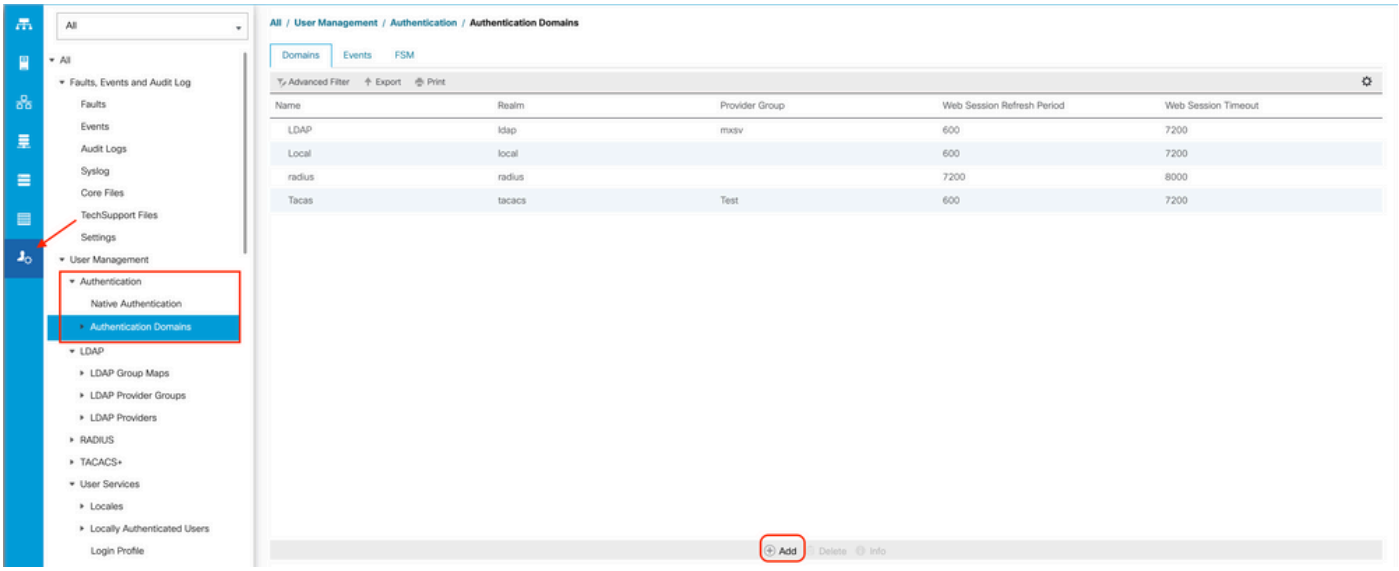
はじめに

ログインする**Cisco UCS Manager** GUI管理ユーザとして設定します。

ローカル認証ドメインの作成

ステップ 1： 内 **Navigation** ペインで、 **Admin** tab.

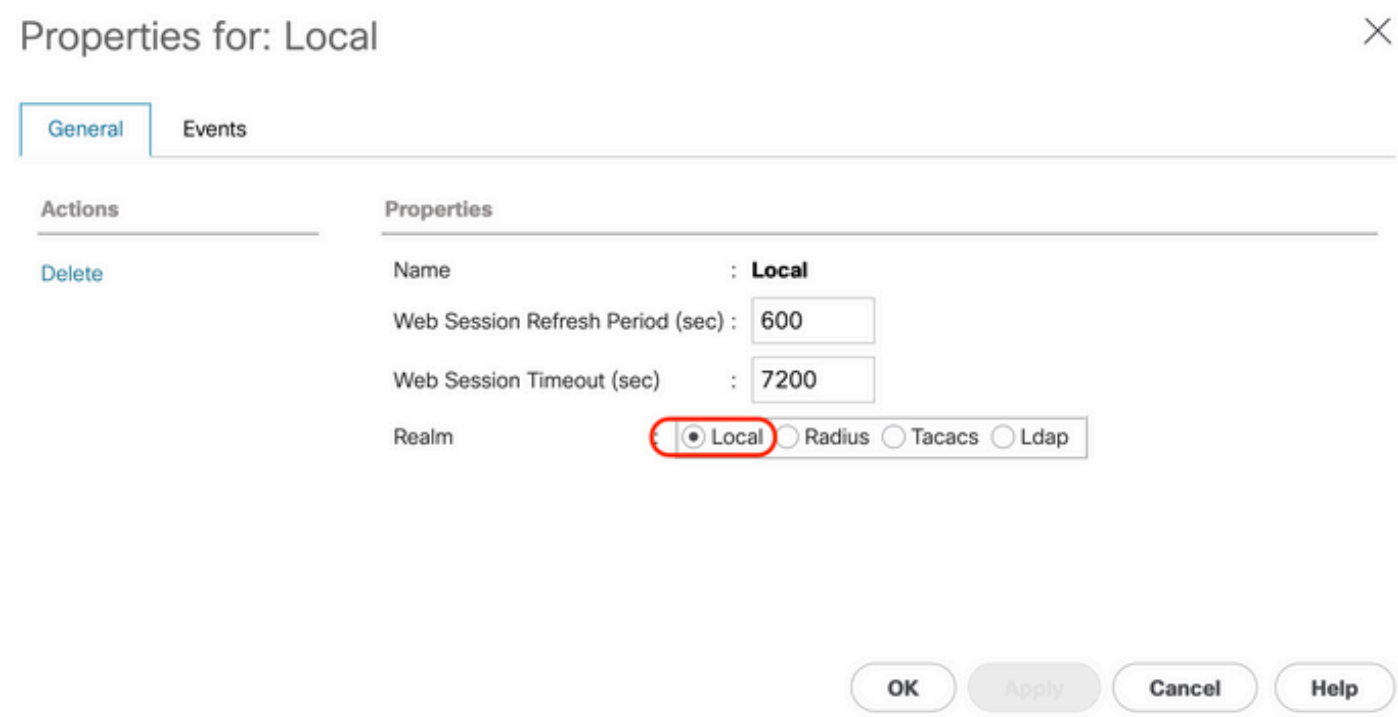
ステップ 2： Cisco Unified Communications Manager **Admin** タブ、展開 **All > User Management > Authentication**



ステップ 3： 右クリック **Authentication Domains** を選択し、 **Create a Domain.**

ステップ 4： の場合 **Name** フィールド、タイプ **Local.**

ステップ 5： の場合 **Realm**,ポリシーの横の [レポート（report）] **Local** オプションボタンを選択します。



手順 6：クリック **OK**.

LDAPプロバイダーの作成

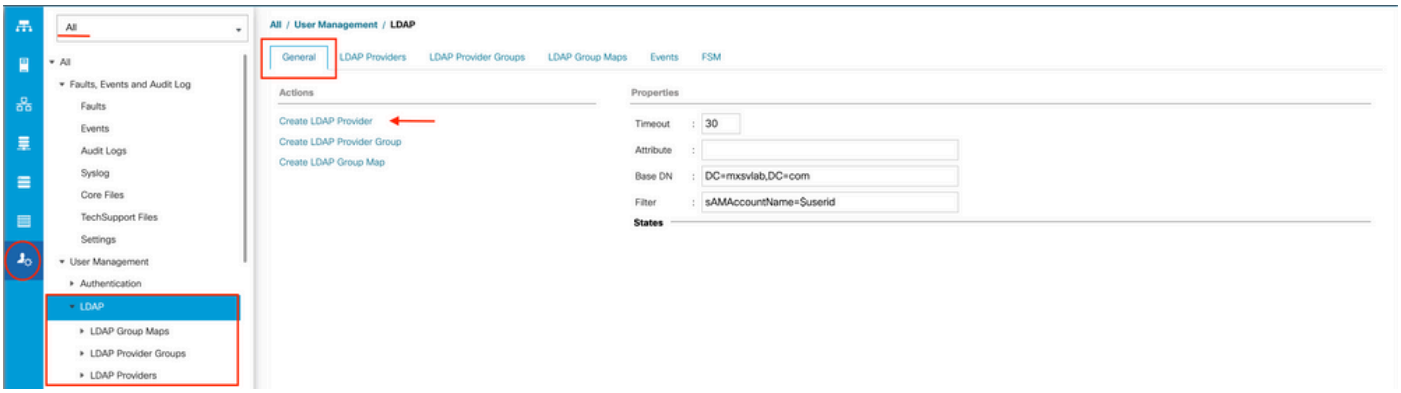
この設定例には、SSLを使用してLDAPを設定する手順は含まれていません。

ステップ 1：内 **Navigation** ペインで、 **Admin** tab.

ステップ 2： Cisco Unified Communications Manager **Admin** タブ、展開 **All > User Management > LDAP**.

ステップ 3： 内 **Work** ペインで、 **General** tab.

ステップ 4： 内 **Actions** エリアを選択し、 **Create LDAP Provider**



ステップ 5： 内 **Create LDAP Provider** ウィザードのページで、適切な情報を入力します。

- 内 **Hostname**フィールドに、ADサーバのIPアドレスまたはホスト名を入力します。
- 内 **Order** フィールドに入力し、 **lowest-available** デフォルトで常に有効になっています。
- 内 **BindDN** フィールドに入力し、AD設定からBindDNをコピーして貼り付けます。

この設定例では、BindDNの値は**CN=ucsbind,OU=CiscoUCS,DC=mxsvlab,DC=com**です。

- 内 **BaseDN** フィールドに入力し、AD設定からBaseDNをコピーして貼り付けます。

この設定例では、BaseDN値は**DC=mxsvlab,DC=com**です。

- Cisco Unified Communications Managerを **Enable SSL** チェックボックスをオフにします。
- 内 **Port** フィールドで、389のデフォルトを受け入れます。
- 内 **Filter** AD設定からフィルタ属性をコピーして貼り付けます。

Cisco UCSはフィルタ値を使用して、ユーザ名（ログイン画面に表示される）が **Cisco UCS Manager**)はADにあります。

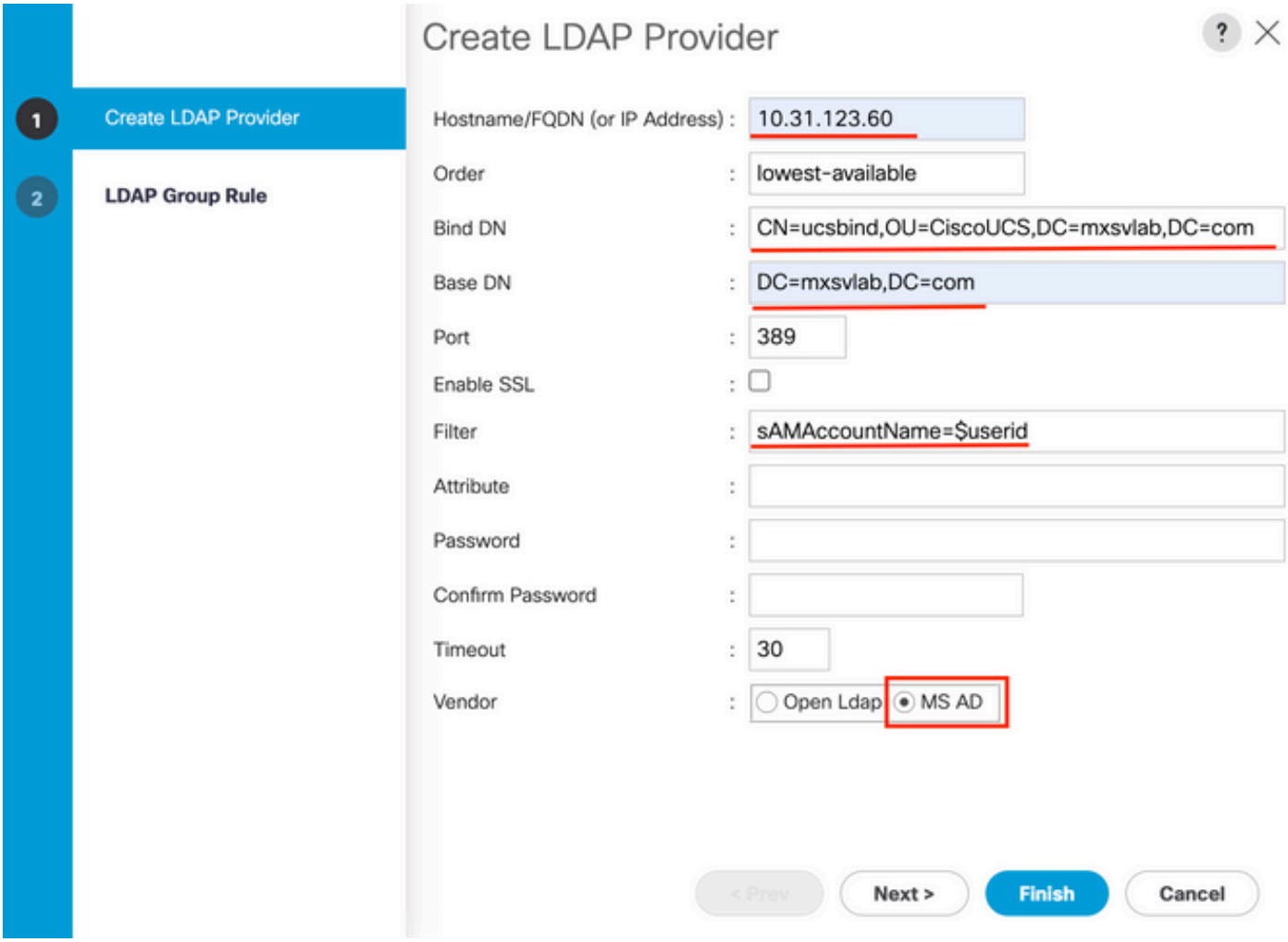
この設定例では、フィルタ値は**sAMAccountName=$userid**で、$useridは **user name** を入力して、**Cisco UCS Manager** ログイン画面。

- Cisco Unified Communications Managerを **Attribute** フィールドが空白です。
- 内 **Password** フィールドに、ADで設定されたucsbindアカウントのパスワードを入力します。

必要に応じて、 **Create LDAP Provider wizard** パスワードをリセットするには、パスワードフィールドが空白の場合は警告しません。

「 **Set: yes** [password]フィールドの横に表示されるメッセージは、パスワードが設定されたことを示します。

- 内 **Confirm Password** フィールドに、ADで設定されたucsbindアカウントのパスワードを再入力します。
- 内 **Timeout** フィールドに入力し、 30デフォルト。
- 内 **Vendor** フィールドで、Microsoft Active DirectoryのMS-ADの**オプシ**ョンボタンを選択します。



手順 6： クリック **Next**

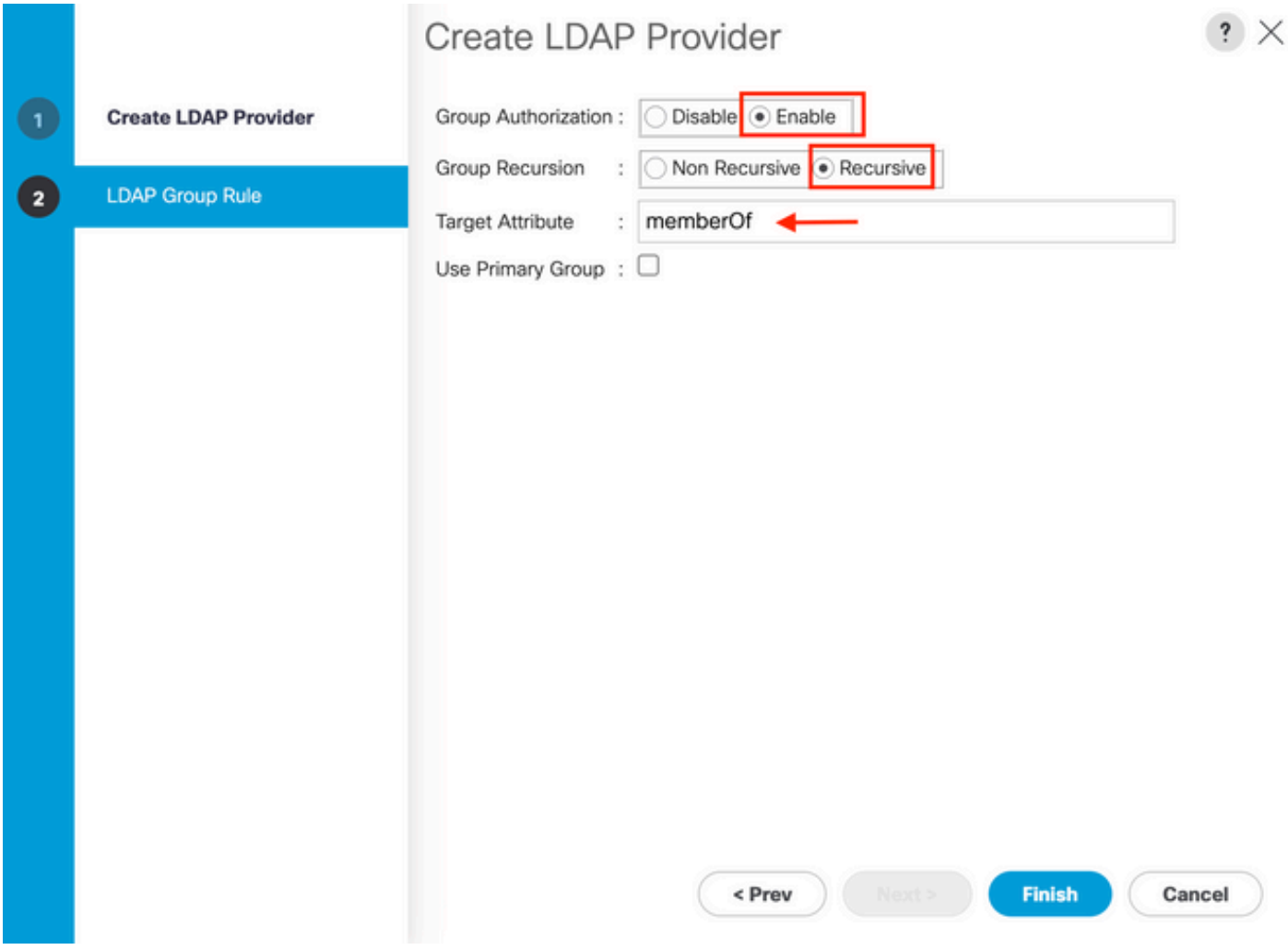
LDAPグループルールの設定

手順 1. Cisco Unified Communications Manager**LDAP Group Rule** ウィザードのページで、次のフィールドに値を入力します。

- の場合 **Group Authentication** フィールドをクリックし、 **Enable** オプションボタンを選択します。
- の場合 **Group Recursion** フィールドをクリックし、 **Recursive** オプションボタンを選択します。これにより、ユーザが見つかるまでレベルごとに検索を続行できます。

If the **Group Recursion** に設定されている **Non-Recursive**を使用すると、UCSが第1レベルの検索に限定されます。検索で条件を満たすユーザが見つからない場合でも同様です。

- 内 **Target Attribute** フィールドに入力し、**memberOf** デフォルトで常に有効になっています。



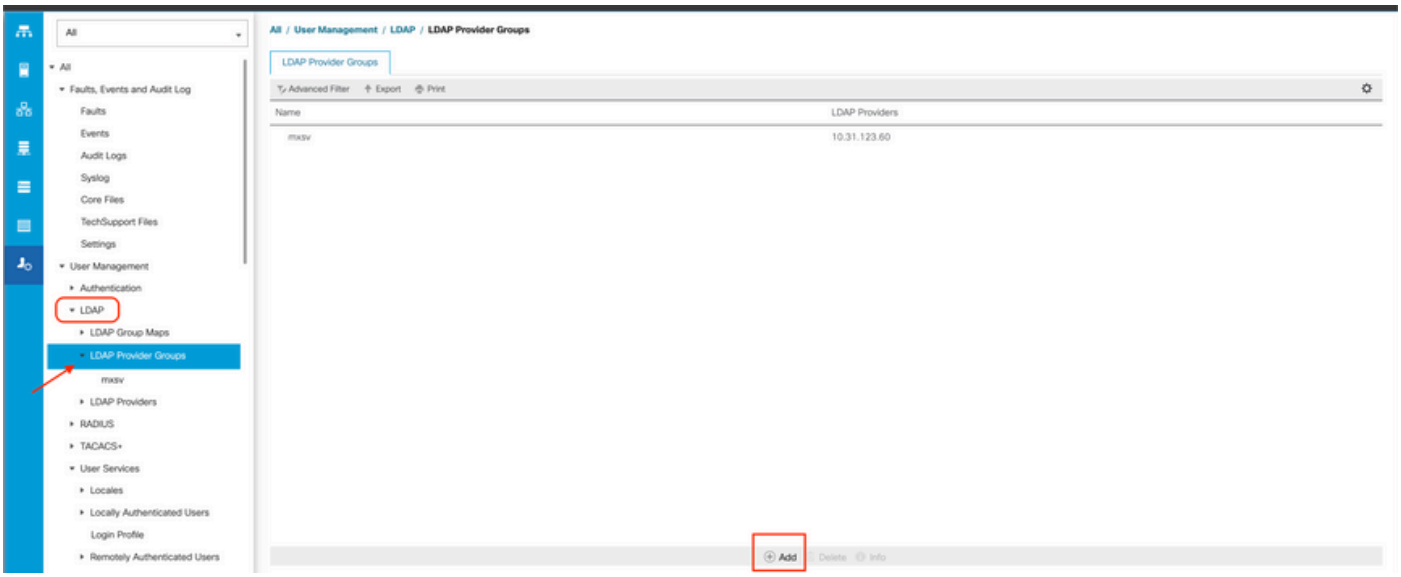
ステップ 2： クリックする **Finish.**

注：実際のシナリオでは、複数のLDAPプロバイダーが存在する可能性が高くなります。複数のLDAPプロバイダーの場合は、各LDAPプロバイダーに対してLDAPグループ規則を設定する手順を繰り返します。ただし、この設定例では、LDAPプロバイダーは1つだけなので、これは必要ありません。

ADサーバのIPアドレスは、ナビゲーションペインの[LDAP] > [LDAP Providers] に表示されます。

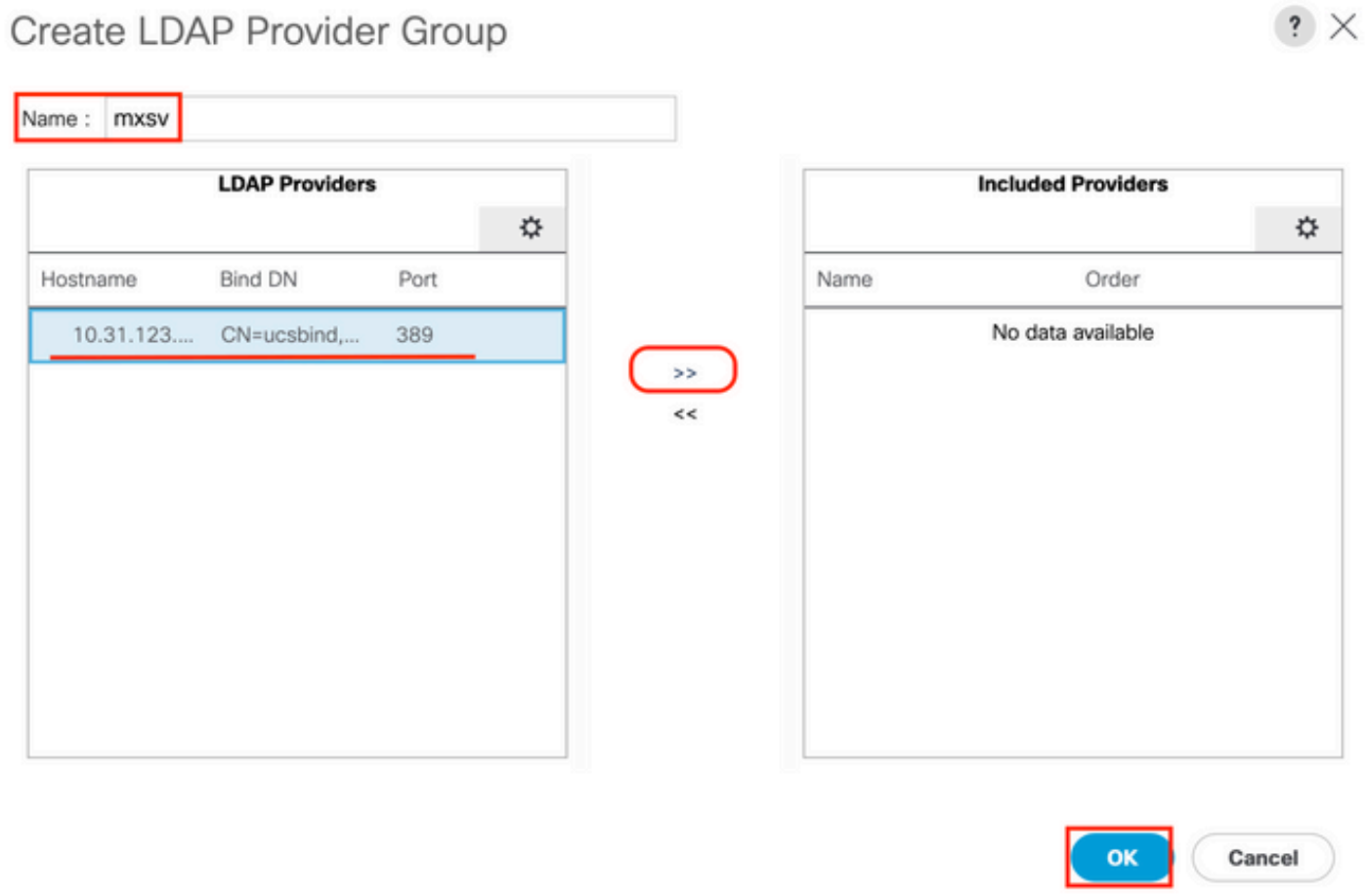
LDAPプロバイダーグループの作成

ステップ 1： ナビゲーションペインで右クリックします **LDAP Provider Groups** を選択し、 **Create LDAP Provider Group**.



ステップ 2： 内 **Create LDAP Provider Group** ダイアログボックスで、次の情報を適宜入力します。

- 内 **Name** フィールドにグループの一意の名前を入力します。たとえば、 **LDAP Providers**.
- 内 **LDAP Providers** 表で、ADサーバのIPアドレスを選択します。
- **>>ボタンをクリックして、ADサーバを Included Providers テーブル.**



ステップ 3： [OK] をクリックします。

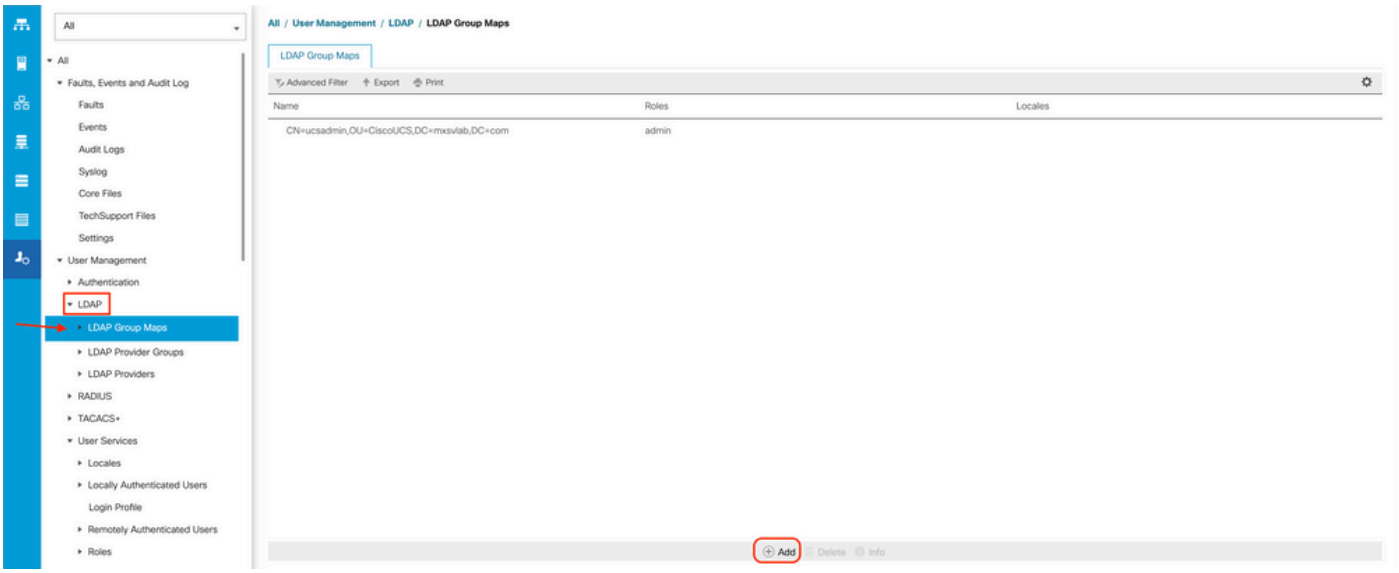
プロバイダーグループが **LDAP Provider Groups** フォルダ。

LDAPグループマップの作成

ステップ 1： ナビゲーションペインで、 **Admin**tab.

ステップ 2： Cisco Unified Communications Manager **Admin** タブ、展開 **All > User Management > LDAP.**

ステップ 3： 作業ペインで、[Create]をクリックします **LDAP Group Map.**



ステップ 4： 内 **Create LDAP Group Map** ダイアログボックスで、次の情報を適宜入力します。

- 内 **LDAP Group DN** フィールドに入力し、LDAPグループのADサーバ設定セクションにある値をコピーして貼り付けます。

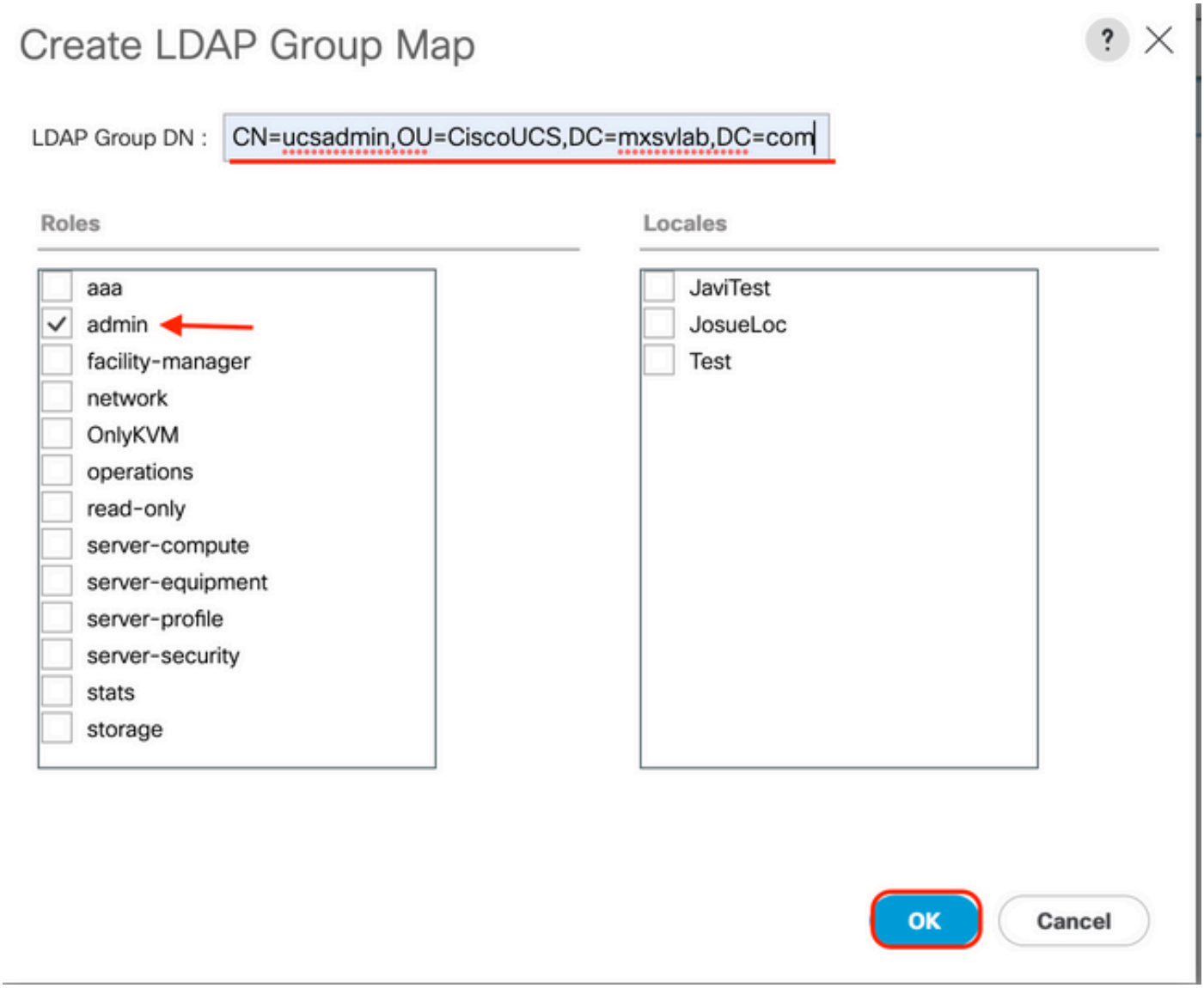
この手順で要求されるLDAPグループDN値は、UCSグループの下でADで作成した各グループの識別名にマッピングされます。

このため、Cisco UCS Managerに入力するグループDNの値は、ADサーバのグループDNの値と正確に一致する必要があります。

この設定例では、この値は**CN=ucsadmin,OU=CiscoUCS,DC=sampledesign,DC=com**です。

- 内 **Roles** テーブルを選択し、 **Admin** チェックボックスをオンにし、[OK] をクリックします。

ロールのチェックボックスをクリックすると、グループマップに含まれるすべてのユーザに管理者権限を割り当てることが示されます。



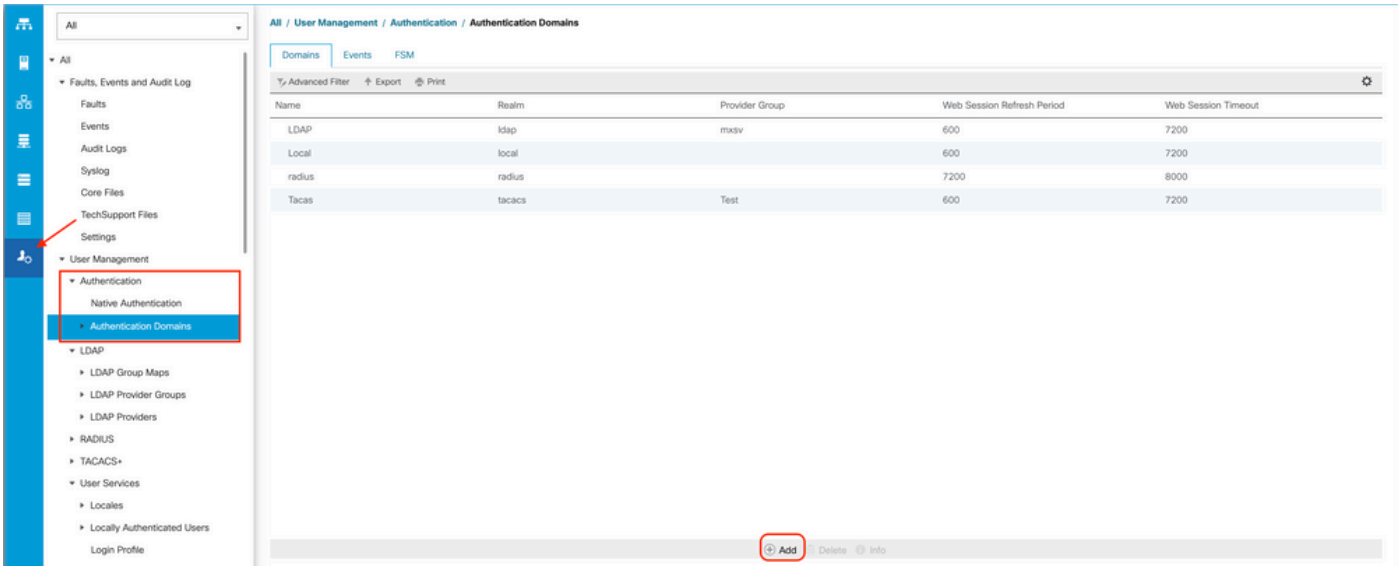
ステップ 5： テストするADサーバ内の各残りのロールに対して、新しいLDAPグループマップを作成します（前にADから記録した情報を使用）。

次のトピック:LDAP認証ドメインを作成します。

LDAP認証ドメインの作成

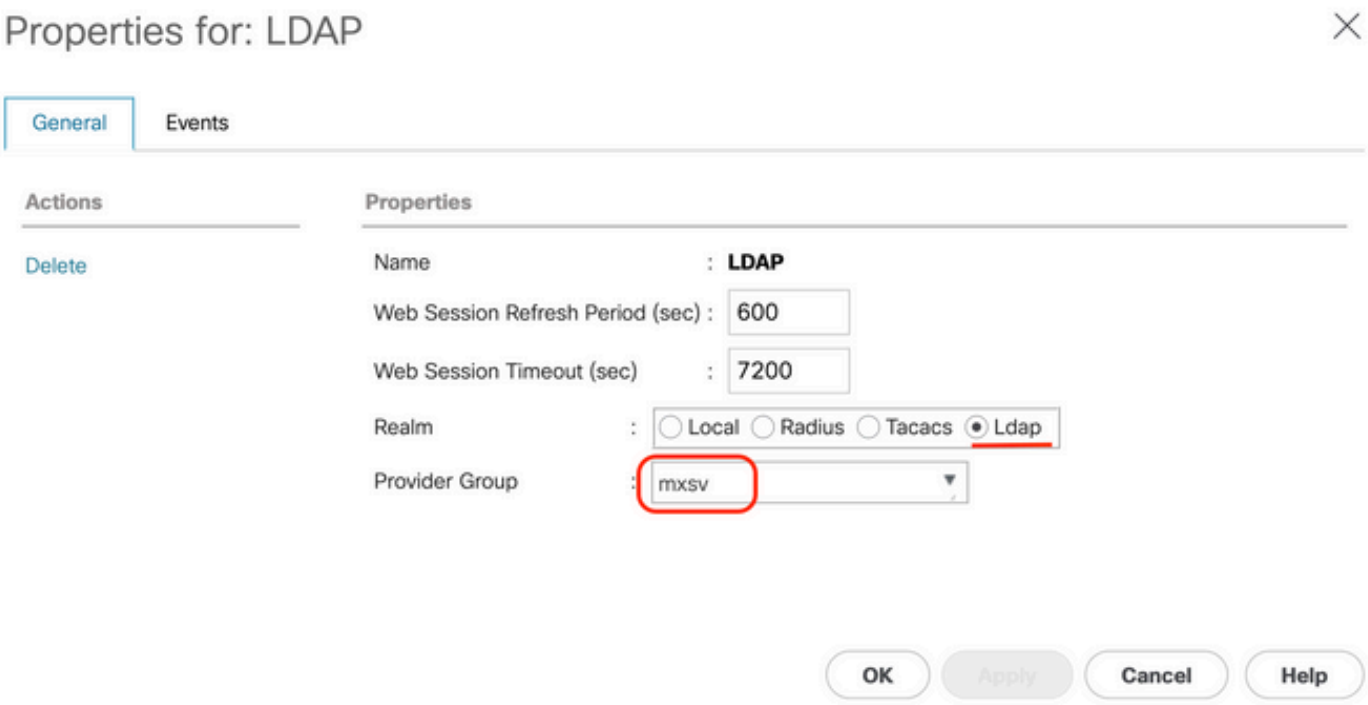
ステップ 1： Cisco Unified Communications Manager [管理（Admin）] タブ、展開 **All > User Management > Authentication**

ステップ 2： 右クリック **[Authentication]** Authentication Domains **を選択し、** Create a Domain.



ステップ 3：nbsp(&N)**Create a Domain** ダイアログボックスで、次の手順を実行します。

- 内 **Name** フィールドに、LDAPなどのドメインの名前を入力します。
- 内 **Realm** エリアをクリックし、 **Ldap** オプションボタンを選択します。
- **Provider Group** ドロップダウンリストから、 **LDAP Provider Group** 以前に作成したファイルを選択し、**OK**をクリックします。



認証ドメインは、 **Authentication Domains.**

確認

Ping to **LDAP Provider IP** または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
```

NX-OSから認証をテストするには、 **test aaa** コマンドを使用します（NXOSからのみ使用可能）。

サーバの設定を検証します。

```
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
```

一般的なLDAPの問題。

- 基本設定.
- パスワードが正しくないか、無効な文字です。

- ポートまたはフィルタフィールドが正しくありません。
- ファイアウォールまたはプロキシのルールにより、プロバイダーとの通信が行われない。
- FSMが100 %ではありません。
- 証明書の問題。

トラブルシュート

UCSM LDAP設定を確認します。

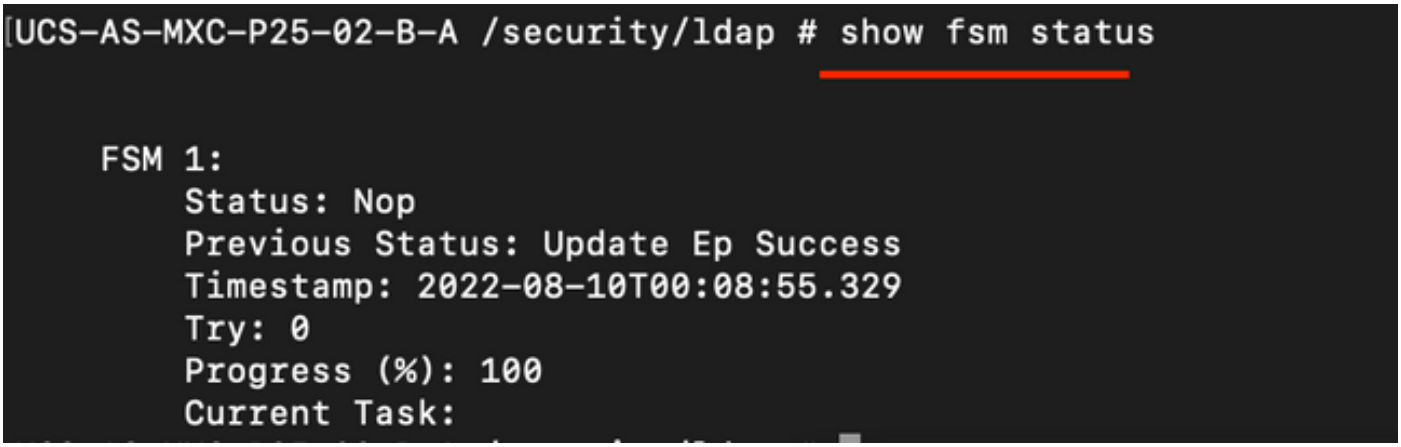
UCSMが設定を正常に実装したことを確認する必要があります。これは、 **Finite State Machine (FSM)** は100%完了として表示されます。

UCSMのコマンドラインから設定を確認するには、次の手順を実行します。

```
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
```



NXOSから設定を確認するには、次の手順を実行します。

```
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
```

エラーを確認する最も効果的な方法は、デバッグを有効にすることです。この出力では、グルー

プ、接続、および通信を妨げるエラーメッセージを確認できます。

- SSHセッションをFIに対して開き、ローカルユーザとしてログインし、NX-OS CLIコンテキストに変更して端末モニタを起動します。

```
 ucs # connect nxos

ucs(nxos)# terminal monitor
```

- デバッグフラグを有効にし、ログファイルへのSSHセッションの出力を確認します。

```
 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
```

- ここで、新しいGUIまたはCLIセッションを開き、リモート(LDAP)ユーザとしてログインを試みます。
- ログイン失敗メッセージを受信したら、デバッグをオフにします。

関連情報

- テクニカル サポートとドキュメント – Cisco Systems

- UCSM LDAPの設定例
- 『Cisco UCS C Series GUI Configuration Guide』

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。