Configurer LDAP dans UCS Manager

Table des matières

Introduction

Ce document décrit la configuration de l'accès au serveur distant avec le protocole LDAP dans notre **Unified Computing System Manager Domain (UCSM).**

Conditions préalables

Exigences

Cisco recommande de connaître les sujets suivants :

- **Unified Computing System Manager Domain (UCSM)**
- Authentification locale et distante
- **Lightweight Directory Access Protocol (LDAP)**
- **Microsoft Active Directory (MS-AD)**

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- **Cisco UCS 6454 Fabric Interconnect**

- UCSM version 4.0(4 Ko)
- **Microsoft Active Directory (MS-AD)**

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Informations générales

Lightweight Directory Access Protocol (LDAP) est l'un des principaux protocoles développés pour les services d'annuaire qui gère de manière sécurisée les utilisateurs et leurs droits d'accès aux ressources informatiques.

La plupart des services d'annuaire utilisent encore LDAP aujourd'hui, bien qu'ils puissent également utiliser des protocoles supplémentaires tels que Kerberos, SAML, RADIUS, SMB, Oauth, etc.

Configurer

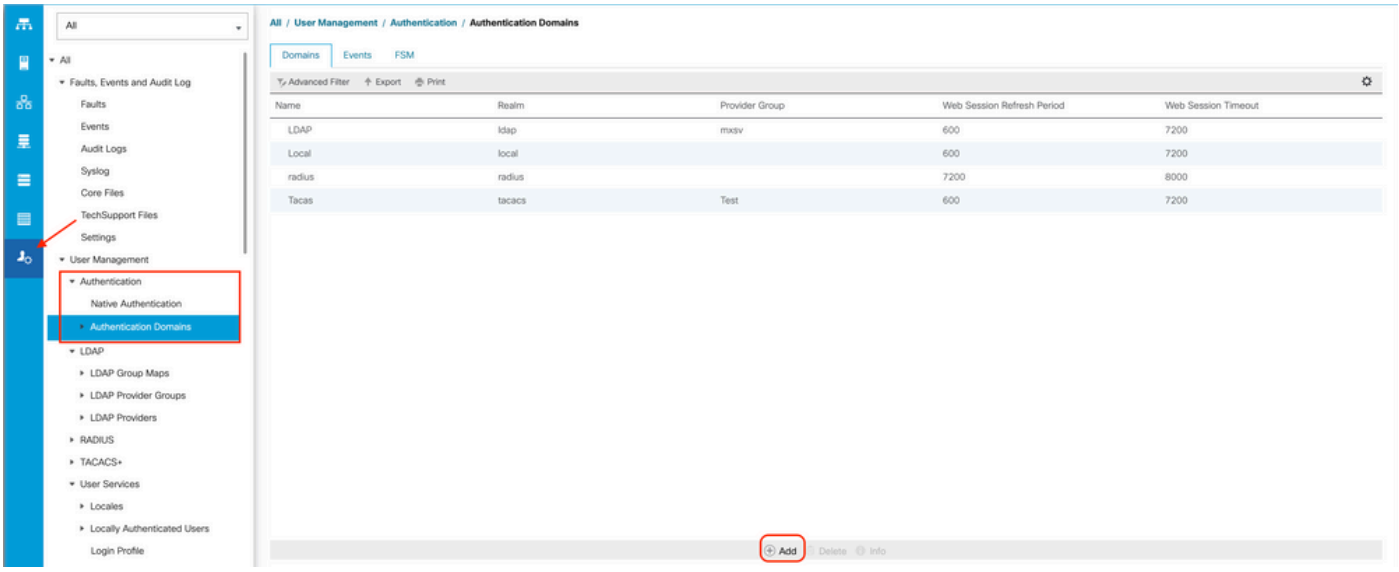
Avant de commencer

Se connecter à**Cisco UCS Manager** IUGen tant qu'utilisateur administrateur.

Créer un domaine d'authentification local

Étape 1. Dans la **Navigation** , cliquez sur le bouton **Admin** s'affiche.

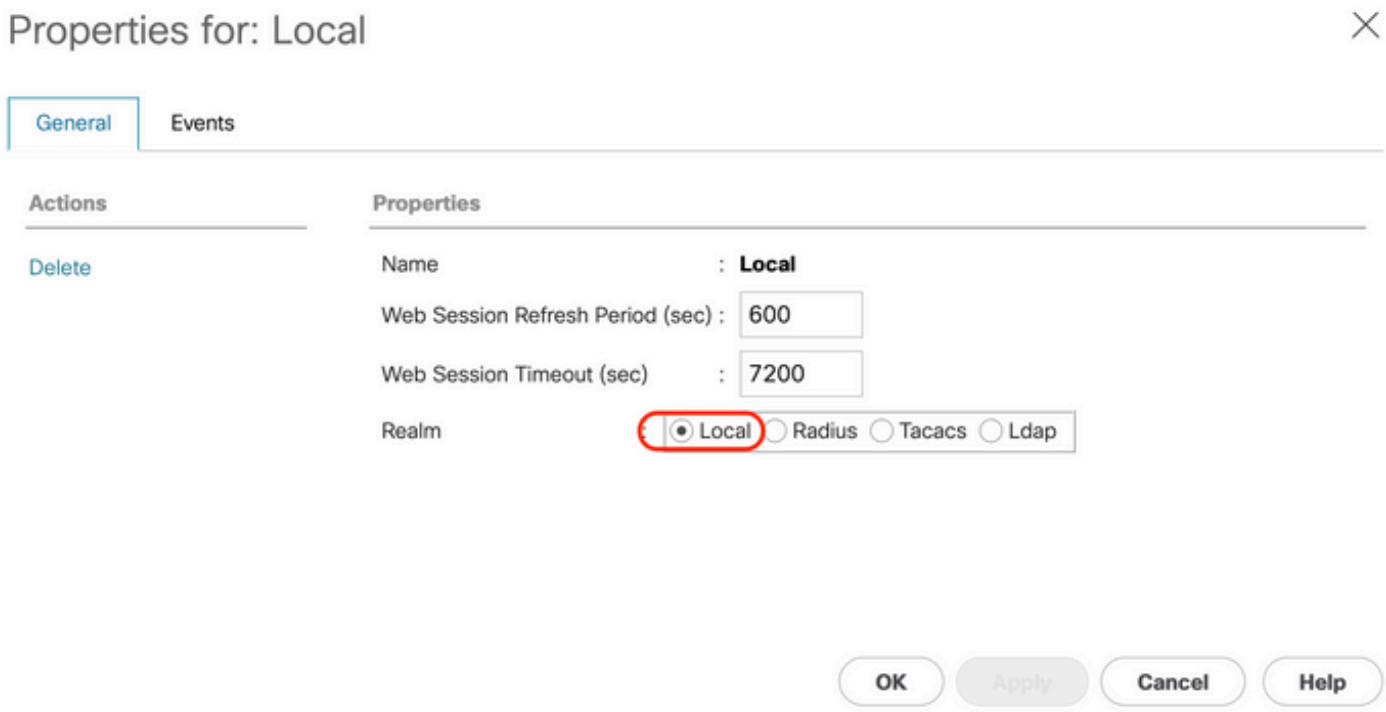
Étape 2. Sur la page **Admin** , développez **All** > **User Management** > **Authentication**



Étape 3. Cliquer avec le bouton droit **Authentication Domains** et sélectionnez **Create a Domain**.

Étape 4. Pour le **Name** champ, type **Local**.

Étape 5. Pour le **Realm**, cliquez sur le bouton **Local** de l'assistant.



Étape 6. Cliquer **OK**.

Créer un fournisseur LDAP

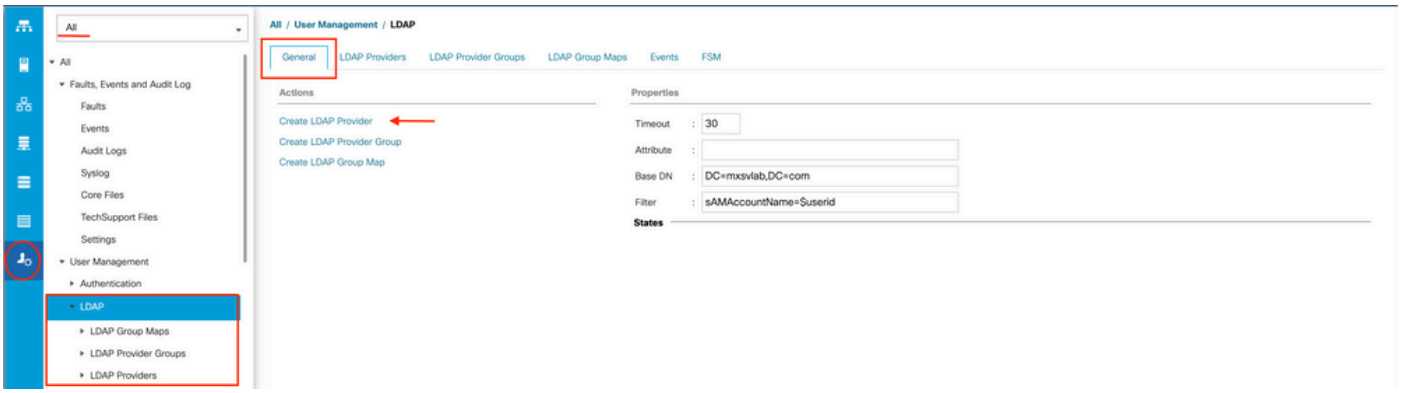
Cet exemple de configuration n'inclut pas les étapes de configuration de LDAP avec SSL.

Étape 1.Dans la **Navigation** , cliquez sur le bouton **Admin** s'affiche.

Étape 2. Sur la page **Admin** , développez **All** > **User Management** > **LDAP**.

Étape 3. Dans la **Work** , cliquez sur le bouton **General** s'affiche.

Étape 4. Dans la **Actions** , cliquez sur **Create LDAP Provider**



Étape 5. Dans la **Create LDAP Provider** de l'assistant, saisissez les informations appropriées :

- Dans la **Hostname**, saisissez l'adresse IP ou le nom d'hôte du serveur AD.
- Dans la **Order** , acceptez la commande **lowest-available** par défaut.

- Dans la **BindDN** , copiez et collez le BindDN à partir de votre configuration Active Directory.

Pour cet exemple de configuration, la valeur BindDN est CN=ucsbind, OU=CiscoUCS, DC=mxsvlab, DC=com.

- Dans la **BaseDN** , copiez et collez le BaseDN à partir de votre configuration AD.

Pour cet exemple de configuration, la valeur BaseDN est DC=mxsvlab,DC=com.

- Quittez le **Enable SSL** n'est pas cochée.
- Dans la **Port** , acceptez la valeur par défaut 389.
- Dans la **Filter** , copiez et collez l'attribut filter de votre configuration AD.

Cisco UCS utilise la valeur de filtre pour déterminer si le nom d'utilisateur (fourni sur l'écran de connexion par **Cisco UCS Manager**) est dans AD.

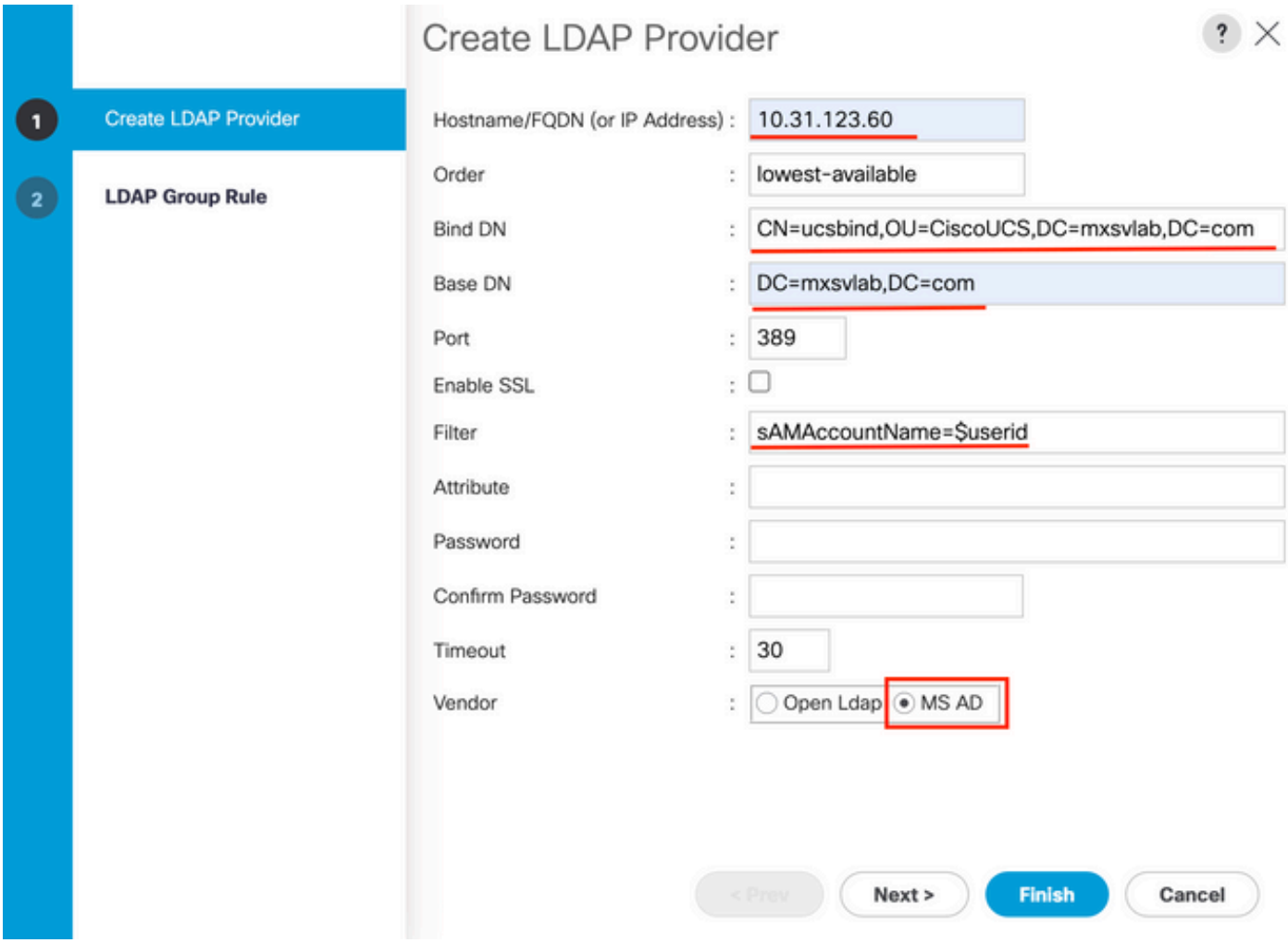
Pour cet exemple de configuration, la valeur du filtre est sAMAccountName=$userid, où $userid est la valeur **user name** inscrire sur la liste **Cisco UCS Manager** écran de connexion.

- Quittez le **Attribute** champ vide.
- Dans la **Password** , saisissez le mot de passe du compte ucsbind configuré dans Active Directory.

Si vous devez revenir à la page **Create LDAP Provider wizard** pour réinitialiser le mot de passe, ne soyez pas alarmé si le champ mot de passe est vide.

Les **Set: yes** Le message qui apparaît en regard du champ Mot de passe indique qu'un mot de passe a été défini.

- Dans la **Confirm Password** , retapez le mot de passe du compte ucsbind configuré dans Active Directory.
- Dans la **Timeout** , acceptez la commande 30 par défaut.
- Dans la **Vendor** , sélectionnez la case d'option MS-AD pour Microsoft Active Directory.



Étape 6. Cliquer **Next**

Configuration des règles de groupe LDAP

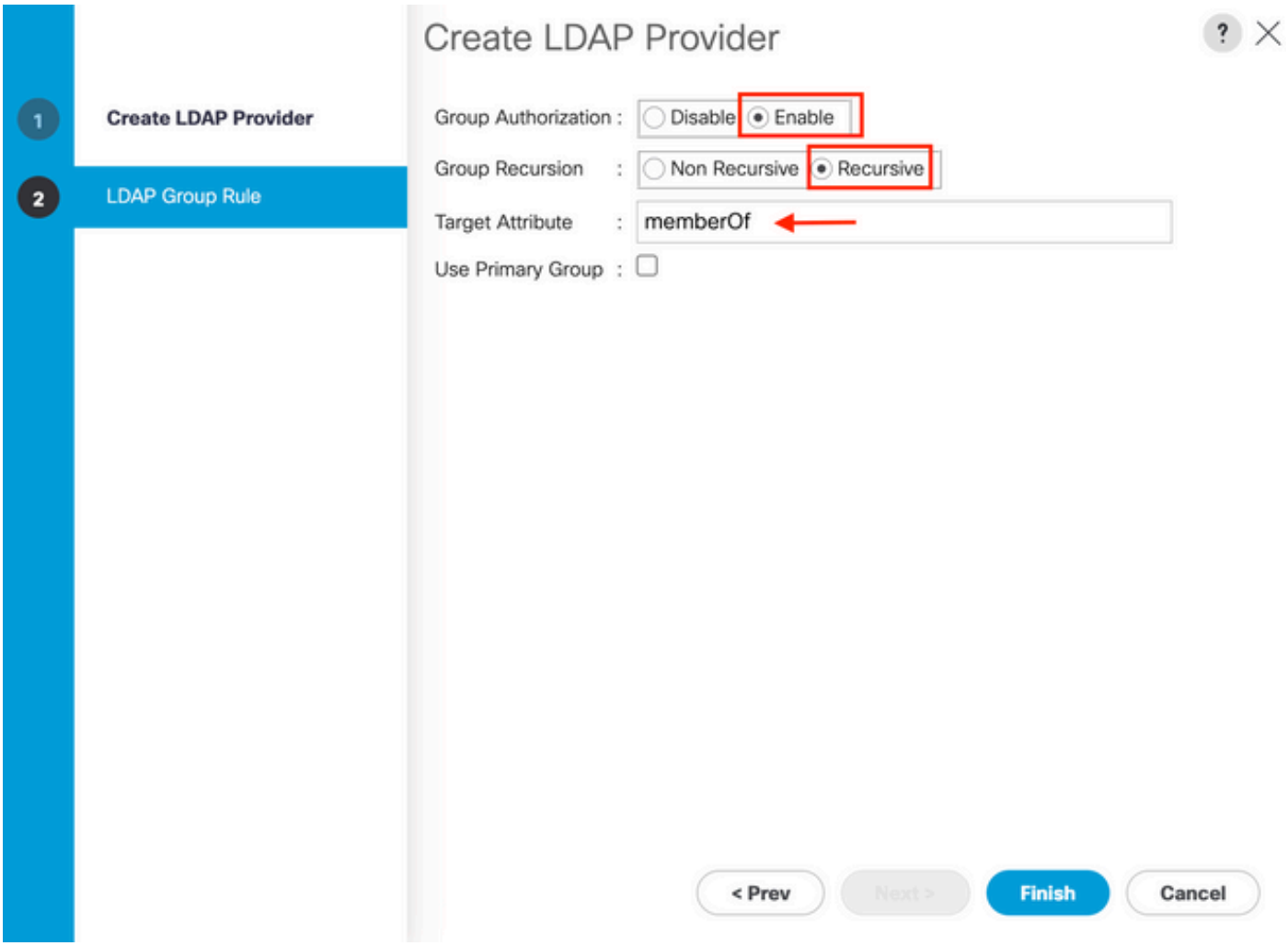
Étape 1. Sur la page**LDAP Group Rule** de l'assistant, renseignez les champs suivants :

- Pour le **Group Authentication** , cliquez sur le bouton **Enable** de l'assistant.
- Pour le **Group Recursion** , cliquez sur le bouton **Recursive** de l'assistant.

  Cela permet au système de poursuivre la recherche, niveau par niveau, jusqu'à ce qu'il trouve un utilisateur.

Si la **Group Recursion** est défini sur **Non-Recursive**, elle limite UCS à une recherche de premier niveau, même si la recherche ne permet pas de localiser un utilisateur qualifié.

- Dans la **Target Attribute** , acceptez la commande**memberOf** par défaut.



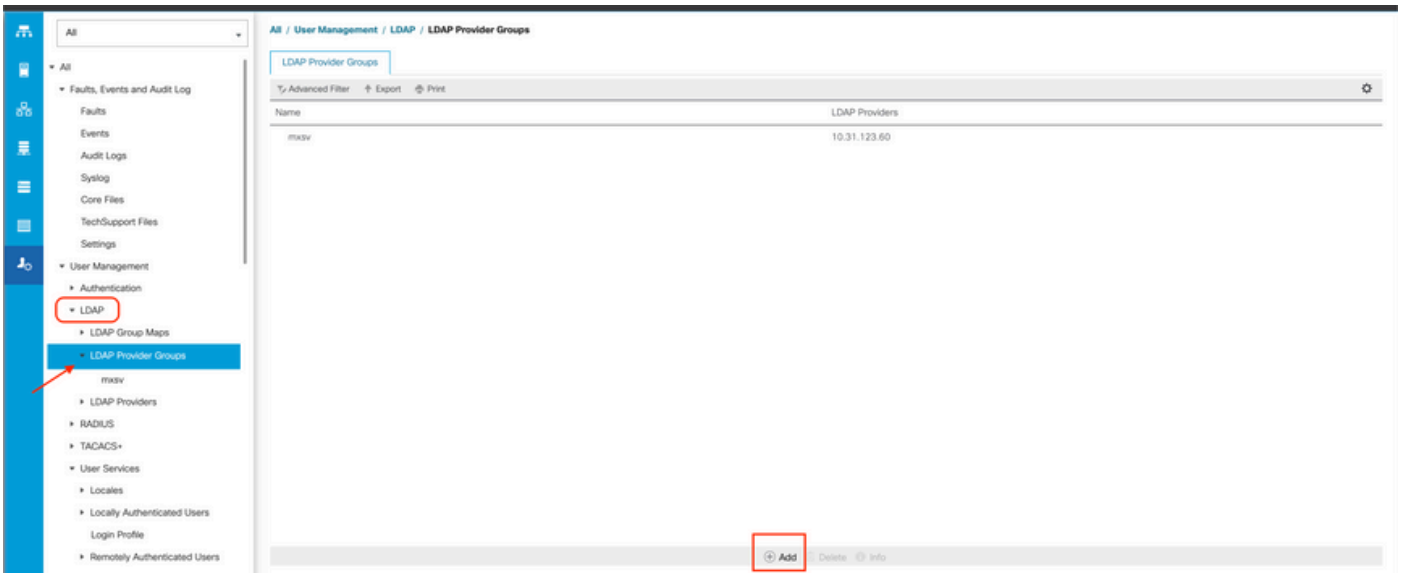
Étape 2. Cliquez dans **Finish**.

> Remarque : dans un scénario réel, il est très probable que vous ayez plusieurs fournisseurs LDAP. Pour plusieurs fournisseurs LDAP, répétez les étapes de configuration de la règle de groupe LDAP pour chaque fournisseur LDAP. Cependant, dans cet exemple de configuration, il n'y a qu'un seul fournisseur LDAP, ce qui n'est donc pas nécessaire.

L'adresse IP du serveur AD est affichée dans le volet de navigation sous LDAP>Fournisseurs LDAP.

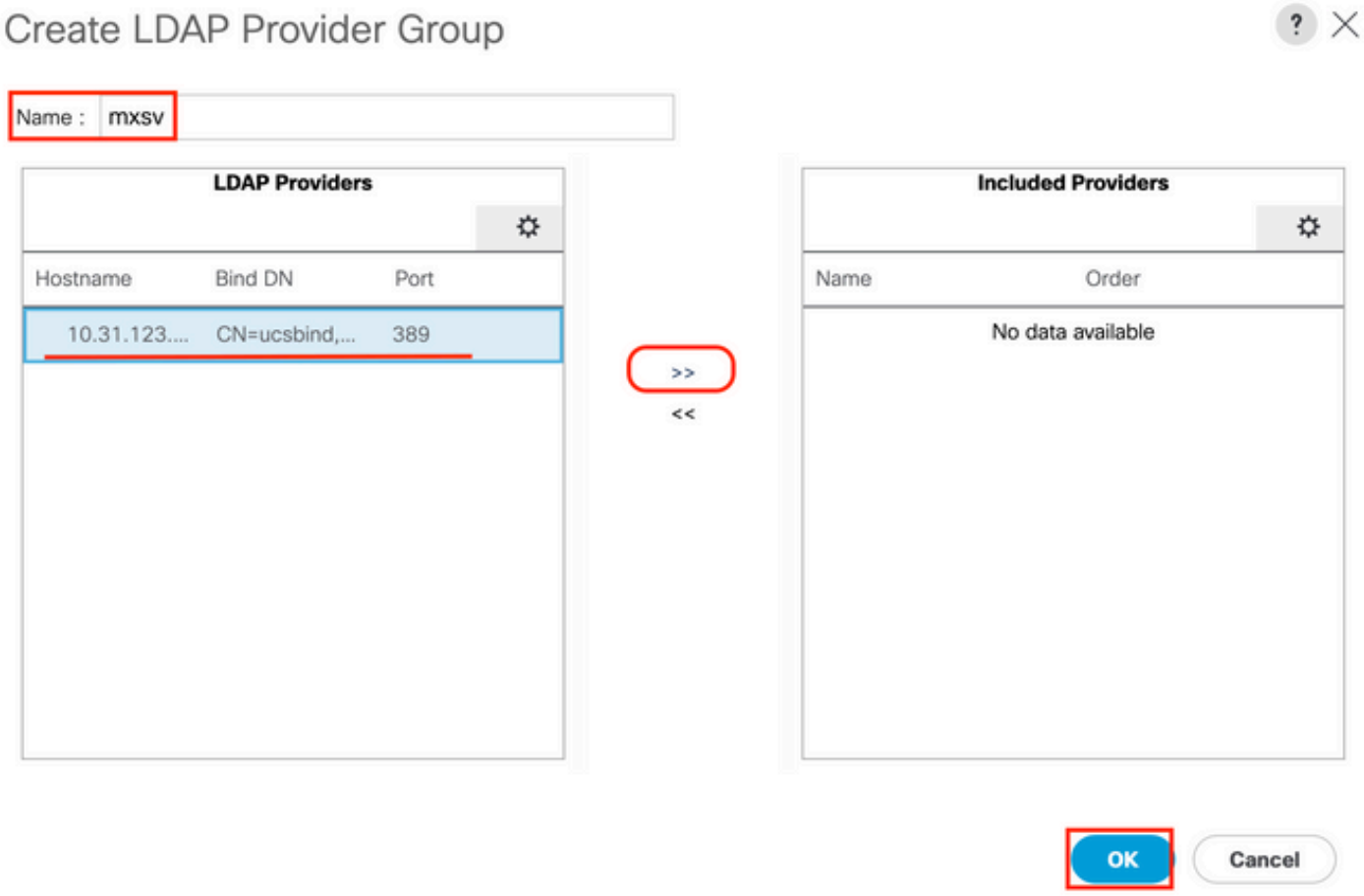
Créer un groupe de fournisseurs LDAP

Étape 1. Dans le volet de navigation, cliquez avec le bouton droit de la souris **LDAP Provider Groups** et sélectionnez **Create LDAP Provider Group**.



Étape 2. Dans la **Create LDAP Provider Group** , remplissez les informations de manière appropriée :

- Dans la **Name** , saisissez un nom unique pour le groupe, par exemple **LDAP Providers.**
- Dans la **LDAP Providers** , choisissez l'adresse IP de votre serveur AD.
- Cliquez sur le bouton >> pour ajouter le serveur AD à votre **Included Providers** tableau.



Étape 3. Click OK.

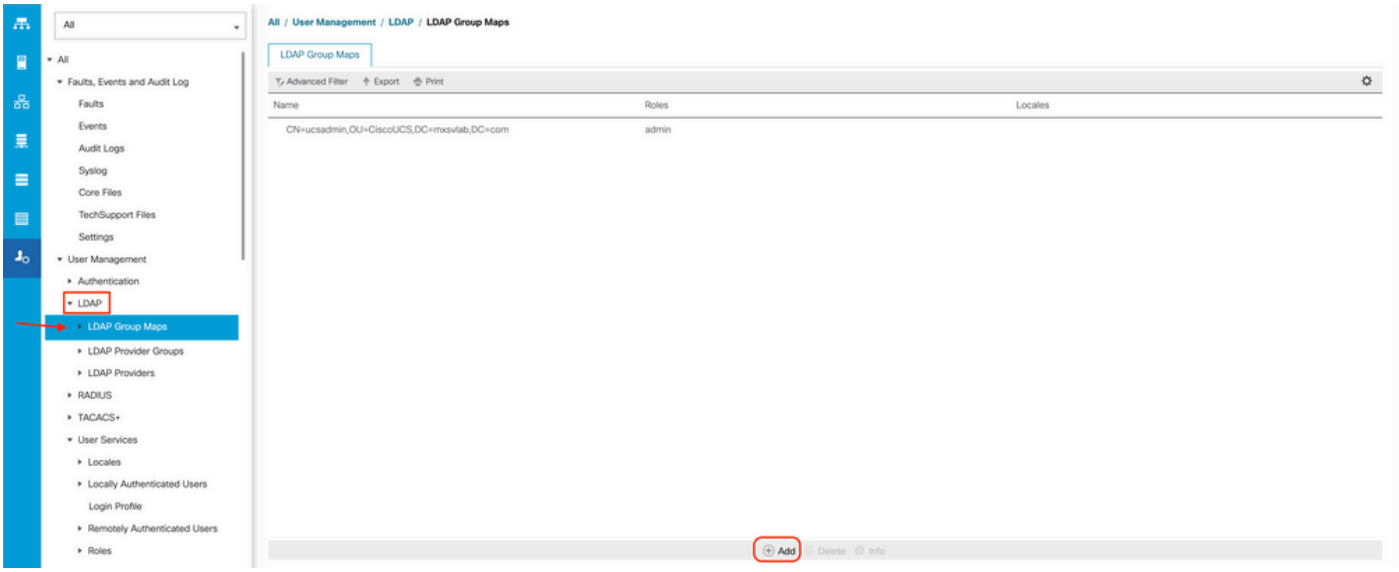
Votre groupe de fournisseurs apparaît dans la **LDAP Provider Groups** dossier.

Créer un mappage de groupe LDAP

Étape 1. Dans le volet de navigation, cliquez sur le bouton **Admin**s'affiche.

Étape 2. Sur la page **Admin** , développez **All** > **User Management** > **LDAP**.

Étape 3. Dans le volet de travail, cliquez sur Créer **LDAP Group Map**.



Étape 4. Dans la **Create LDAP Group Map** , remplissez les informations de manière appropriée :

- Dans la **LDAP Group DN** , copiez et collez la valeur que vous avez dans la section de configuration du serveur AD pour votre groupe LDAP.

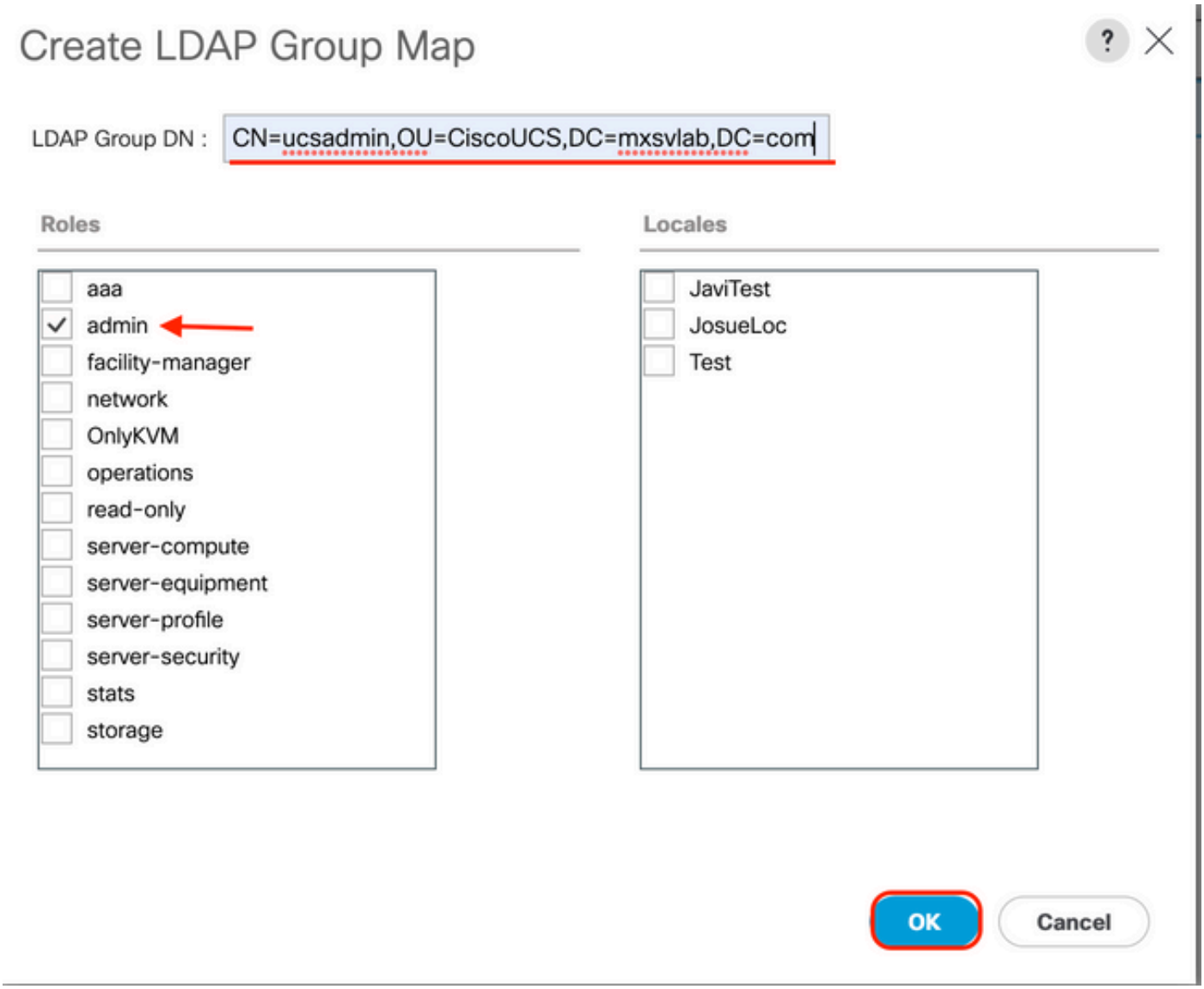
La valeur DN du groupe LDAP demandée dans cette étape correspond au nom unique de chacun des groupes que vous avez créés dans Active Directory sous Groupes UCS.

Pour cette raison, la valeur DN du groupe saisie dans Cisco UCS Manager doit correspondre exactement à la valeur DN du groupe sur le serveur AD.

Dans cet exemple de configuration, cette valeur est CN=ucsadmin, OU=CiscoUCS, DC=sampledesign, DC=com.

- Dans la **Roles** , cliquez sur le bouton **Admin** et cliquez sur OK.

Cliquez sur la case à cocher d'un rôle pour indiquer que vous souhaitez attribuer des privilèges d'administrateur à tous les utilisateurs inclus dans le plan de groupe.



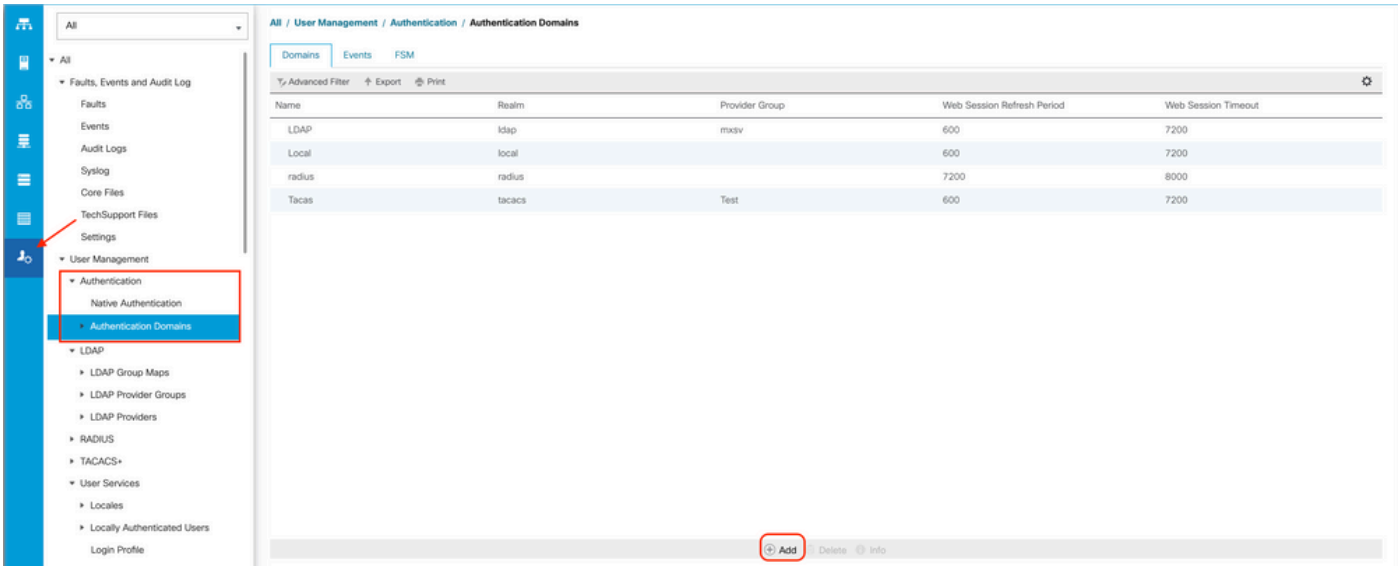
Étape 5. Créez de nouveaux mappages de groupes LDAP (utilisez les informations que vous avez enregistrées précédemment à partir d'AD) pour chacun des rôles restants dans le serveur AD que vous souhaitez tester.

Suivant : Créez votre domaine d'authentification LDAP.

Créer un domaine d'authentification LDAP

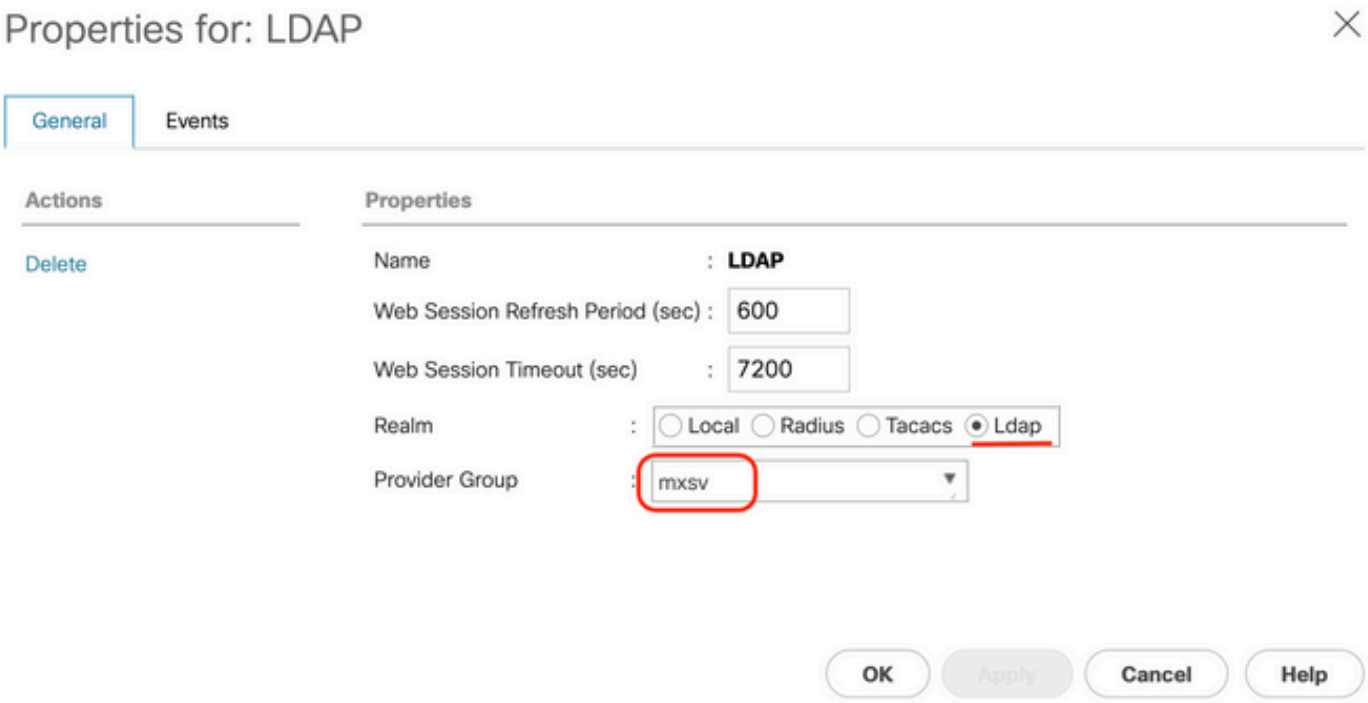
Étape 1. Sur la page Admin , développez **All** > **User Management** > **Authentication**

Étape 2. Cliquer avec le bouton droit Authentification **Authentication Domains** et sélectionnez **Create a Domain**.



Étape 3.Dans le Create a Domain , complétez la boîte de dialogue suivante :

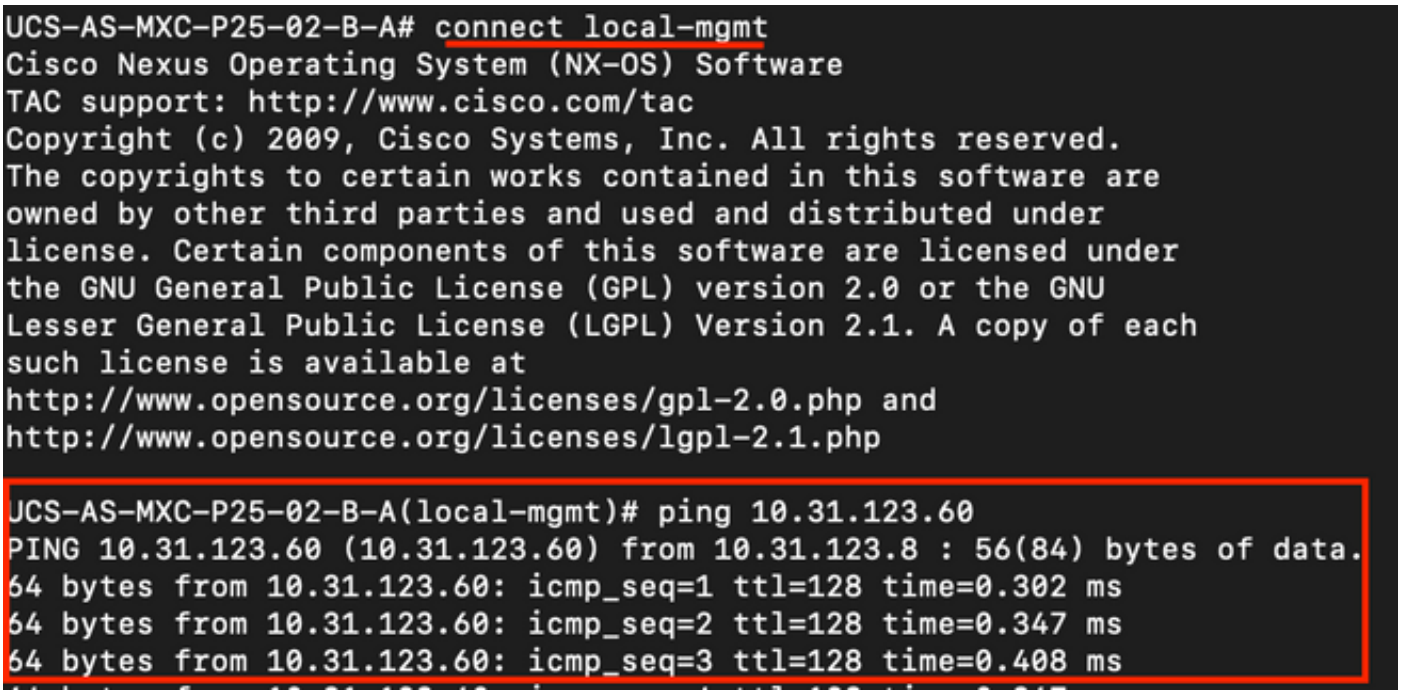
- Dans la **Name** , saisissez un nom pour votre domaine tel que LDAP.
- Dans la **Realm** , cliquez sur l'icône **Ldap** de l'assistant.
- A partir des versions **Provider Group** dans la liste déroulante, sélectionnez le **LDAP Provider Group** précédemment créé et cliquez sur OK.



Le domaine d'authentification apparaît sous **Authentication Domains**.

Vérifier

Ping vers **LDAP Provider IP** ou FQDN :



Pour tester l'authentification à partir de NX-OS, utilisez la **test aaa** (disponible uniquement sur NXOS).

Nous validons la configuration de notre serveur :

<#root>

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
```

Problèmes LDAP courants.

- Configuration de base.
- Mot de passe incorrect ou caractères non valides.
- Port ou champ de filtre incorrect.
- Aucune communication avec notre fournisseur en raison d'une règle de pare-feu ou de proxy.
- FSM n'est pas à 100 %.
- Problèmes de certificat.

Dépannage

Vérifiez la configuration LDAP UCSM :

Vous devez vous assurer que l'UCSM a correctement mis en oeuvre la configuration, car l'état du **Finite State Machine (FSM)** est affichée comme 100 % terminée.

Pour vérifier la configuration à partir de la ligne de commande de votre UCSM :

<#root>

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 #
```

<#root>

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:
```

Pour vérifier la configuration à partir de NXOS :

<#root>

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
```

La méthode la plus efficace pour voir les erreurs est d'activer notre débogage, avec ce résultat, nous pouvons voir les groupes, la connexion et le message d'erreur qui empêche la communication.

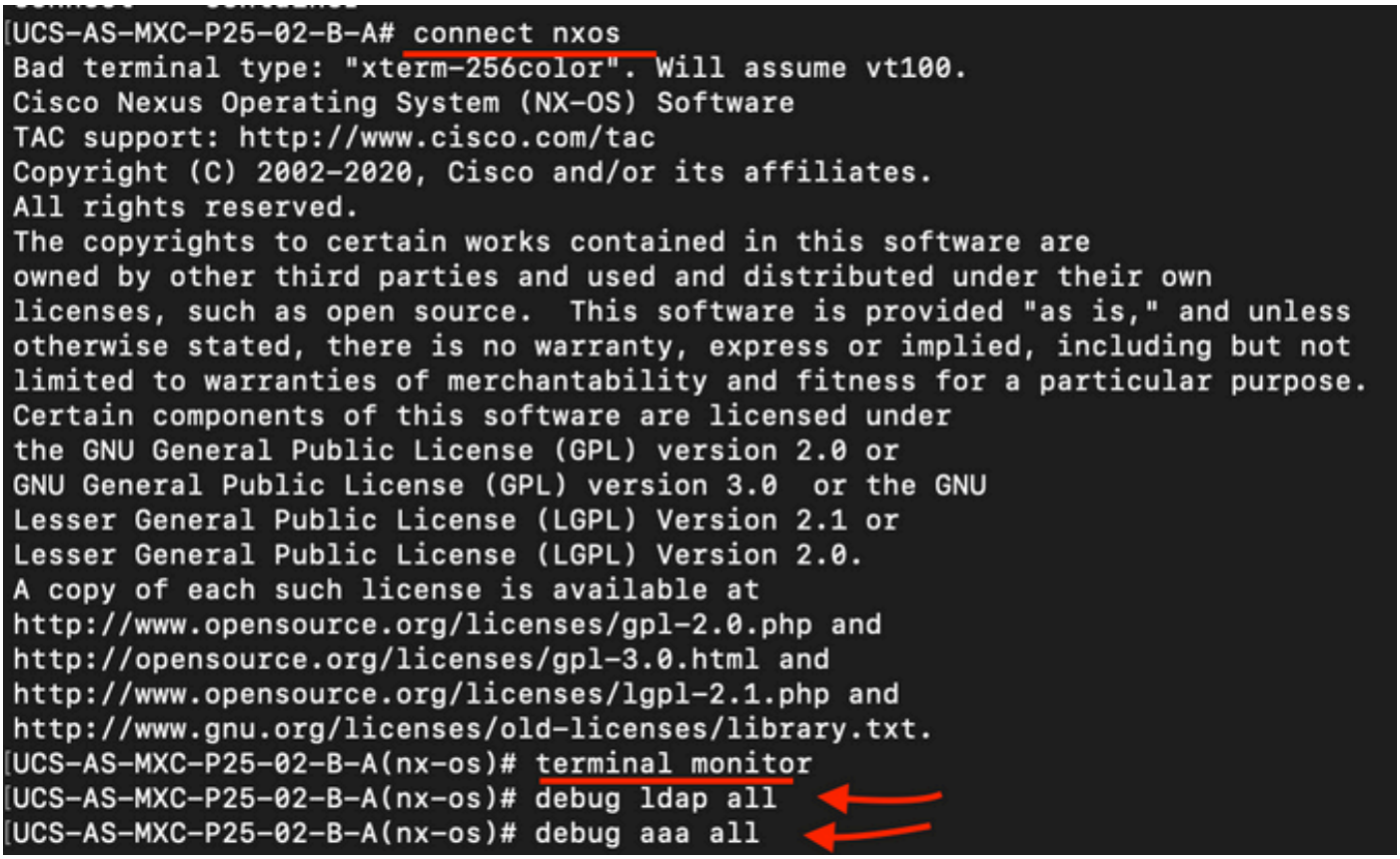
- Ouvrez une session SSH sur FI et connectez-vous en tant qu'utilisateur local, passez au contexte CLI de NX-OS et démarrez le moniteur de terminal.

```
ucs # connect nxos

ucs(nxos)# terminal monitor
```

- Activez les indicateurs de débogage et vérifiez le résultat de la session SSH dans le fichier journal.

<#root>

```
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
```



- Ouvrez à présent une nouvelle session GUI ou CLI et essayez de vous connecter en tant qu'utilisateur (LDAP) distant.
- Une fois que vous avez reçu un message d'échec de connexion, désactivez les débogages.

Informations connexes

- Assistance et documentation techniques - Cisco Systems

- Exemple de configuration UCSM LDAP
- Guide de configuration de l'interface utilisateur graphique Cisco UCS série C

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.