Configurer LDAP sur le & UCS Manager CIMC utilisant des serveurs Linux OpenLDAP et 389-DS

Table des matières

Introduction

Ce document décrit une variété d'options permettant de configurer LDAP comme méthode

d'authentification pour UCS Manager et CIMC à l'aide d'OpenLDAP basé sur Linux et de serveurs d'annuaire 389.

Informations générales

En raison de la grande variabilité des configurations de serveur OpenLDAP, un traitement exhaustif sort du cadre de ce document. Cet article met plutôt l'accent sur les configurations couramment implémentées couvrant plusieurs distributions Linux, des packages de serveur LDAP et des schémas d'attributs. Dans un souci de clarté et de simplicité, ce document traite des configurations LDAP standard. La configuration de LDAP sécurisé (LDAPS) n'est pas traitée dans ce document.

Conditions préalables:

La connaissance de ces sujets est fortement recommandée :

- Gamme UCS B
- Gamme UCS C
- Administration du serveur Linux

Composants utilisés

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

- Version du micrologiciel UCS Manager : 4.3(2c)
- Modèle Fabric Interconnect : UCS-FI-6454
- Modèle de serveur autonome UCS série C : UCSC-C240-M5
- Version du micrologiciel autonome UCS série C : 4.3(2.250045)
- Ubuntu 20.04
- Flux CentOS 10

Paramètres utilisés pour cette démonstration :

- Nom d'hôte du serveur LDAP : épreuve

- Domaine du serveur : xxxxxxxxx.com

- Nom de domaine complet du serveur : test.xxxxxxxxx.com
- Adresse IP du serveur Linux (Ubuntu et CentOS) : X.X.X.19
- Utilisateurs(s) OpenLDAP : testuser1, testuser2
- Groupe(s) OpenLDAP : il
- Compte utilisateur de liaison OpenLDAP : bind_user

Remarque : l'éditeur de texte linux Nano a été utilisé dans ces travaux pratiques.

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.

Scénario 1 : Ubuntu - Debian

La configuration du serveur LDAP peut être effectuée à l'aide d'une interface graphique, telle que le gestionnaire de compte LDAP, ou d'outils de ligne de commande, selon les préférences administratives et le niveau de contrôle requis. Ce scénario examine la configuration à l'aide d'OpenLDAP basé sur Linux, en commençant par un déploiement basé sur une interface graphique utilisateur et en passant ensuite à des utilitaires de ligne de commande pour explorer des fonctionnalités avancées, y compris des plug-ins de superposition (couramment utilisés dans les intégrations avec Cisco UCS Manager).

Option 1: Configurer OpenLDAP à l'aide d'Ubuntu LDAP Account Manager (LAM)

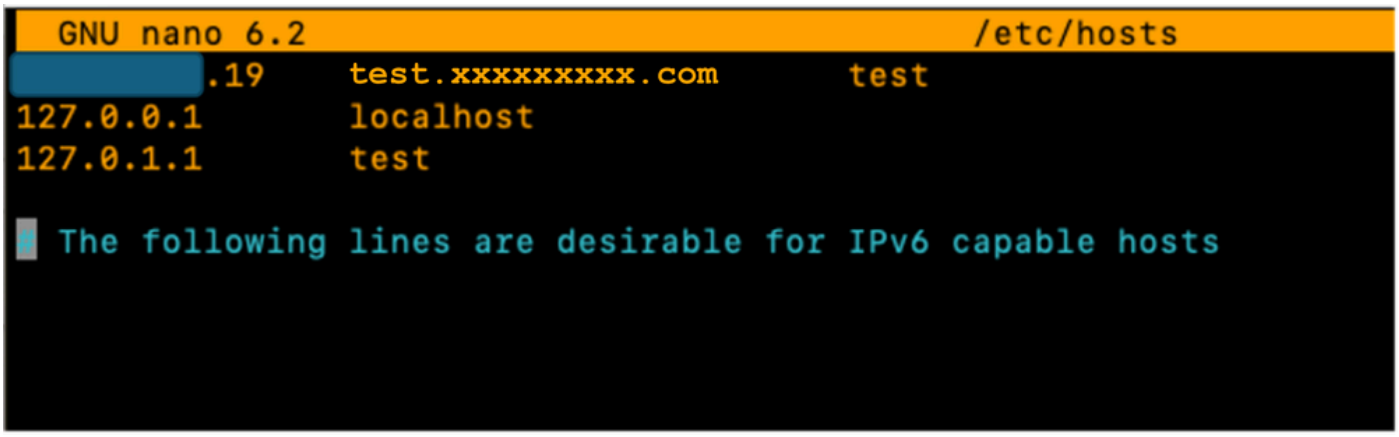
Étape 1: Configuration initiale du nom d'hôte du serveur Linux et des outils réseau.

Mettez à jour ubuntu et installez le paquet net-tools pour accéder à des outils tels que ifconfig, netstat, etc :

```
sudo apt update
sudo apt install net-tools
```

Utilisez la commande « ifconfig » pour vérifier l'adresse IP du serveur, puis ajoutez-la au fichier « /etc/hosts » avec le nom de domaine du serveur (par exemple : « test.xxxxxxxxx.com » utilisé dans ces travaux pratiques) et le nom d'hôte (par exemple : "test") dans le format spécifié.

```
sudo nano /etc/hosts
```



En outre, mettez à jour le fichier « /etc/hostname » en remplaçant son contenu par le nom d'hôte (test).

```
sudo nano /etc/hostname
```

Un redémarrage du serveur est nécessaire pour que ces modifications prennent effet.

```
sudo reboot
```

Étape 2 : Installez SLAPD, Apache, PHP et leurs dépendances

Ensuite, installez Apache, PHP et leurs dépendances. Ils sont utilisés pour activer l'interaction de l'interface graphique utilisateur sur une page Web :

```
sudo apt install apache2 php php-cgi libapache2-mod-php php-mbstring php-common php-pear -y
```

Installer le package de serveur LDAP ouvert « slapd » et ses dépendances (ldap-utils)

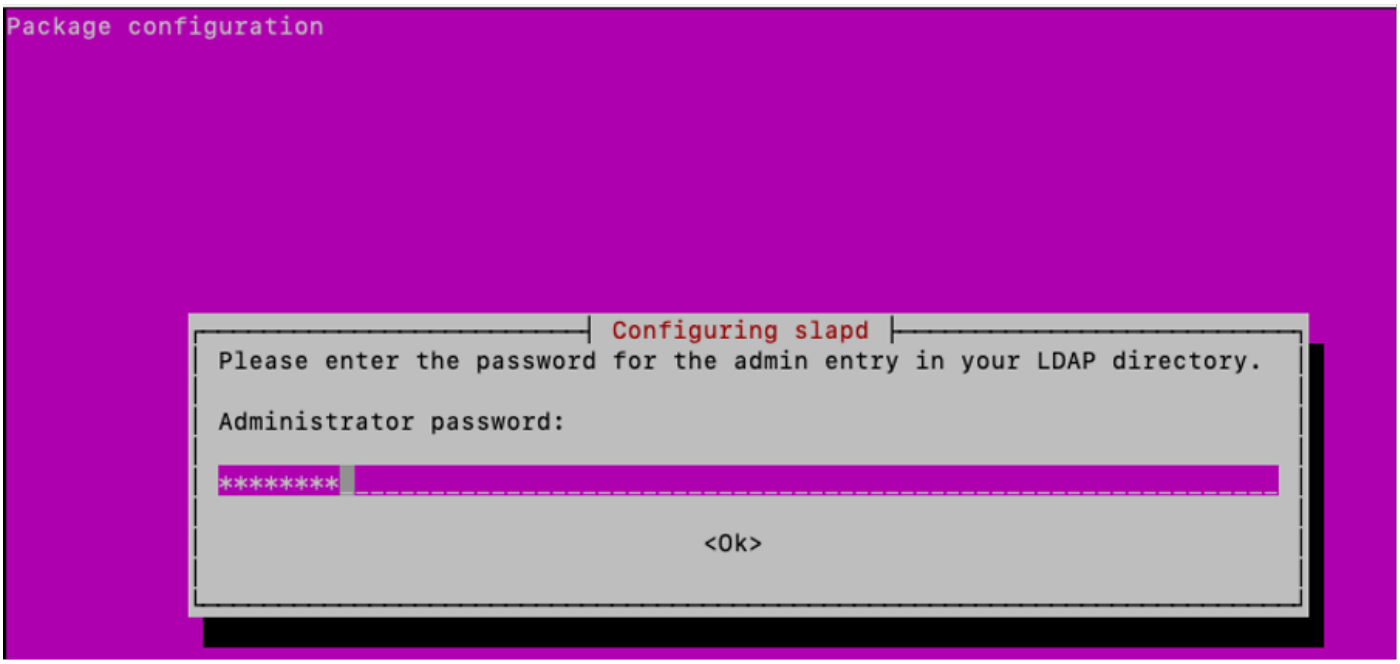
```
sudo apt install slapd ldap-utils -y
```

Lors de l'installation de SLAPD, dans la fenêtre contextuelle GUI présentée, saisissez la configuration de package SLAPD supplémentaire requise.

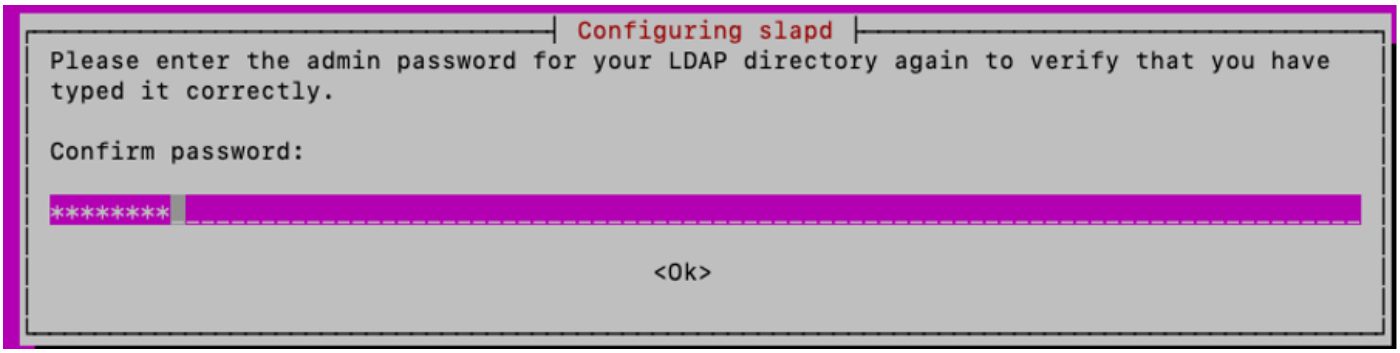
Remarque : La perte du mot de passe nécessite une réinstallation du serveur LDAP.

L'« administrateur » (admin) dans ce contexte est un compte qui est utilisé pour gérer le service, les modules et les configurations OpenLDAP.

Ajoutez le mot de passe « administrator » du package LDAP et appuyez sur la touche Entrée du clavier pour sélectionner « OK ».



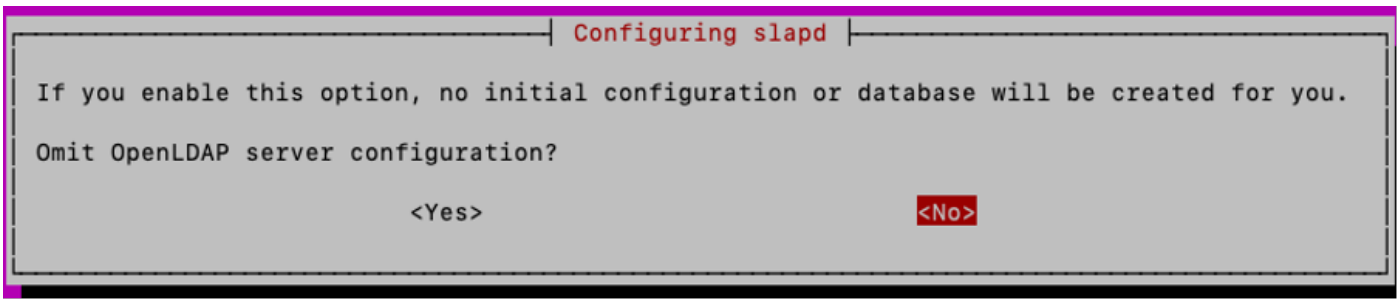
Confirmez le mot de passe :



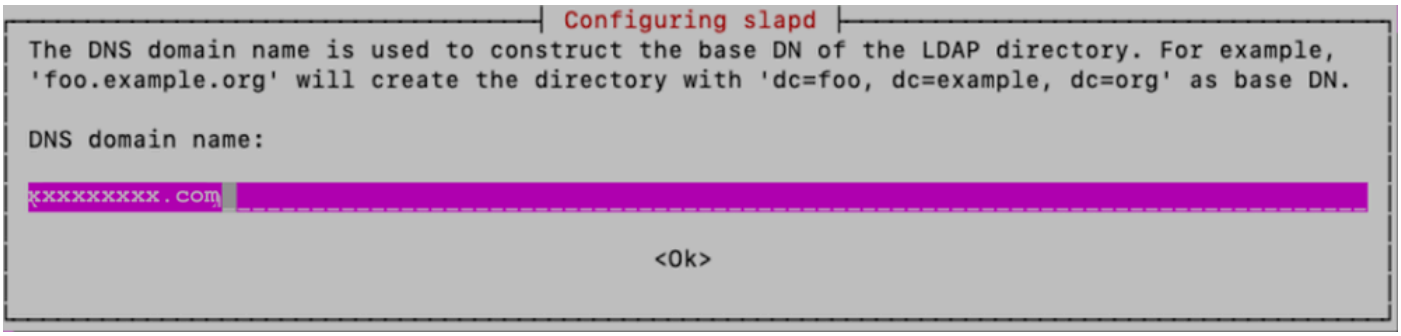
Une fois l'installation terminée, vous pouvez utiliser la commande spécifiée pour reconfigurer le package SLAPD, en ajoutant les informations de domaine :

```
sudo dpkg-reconfigure slapd
```

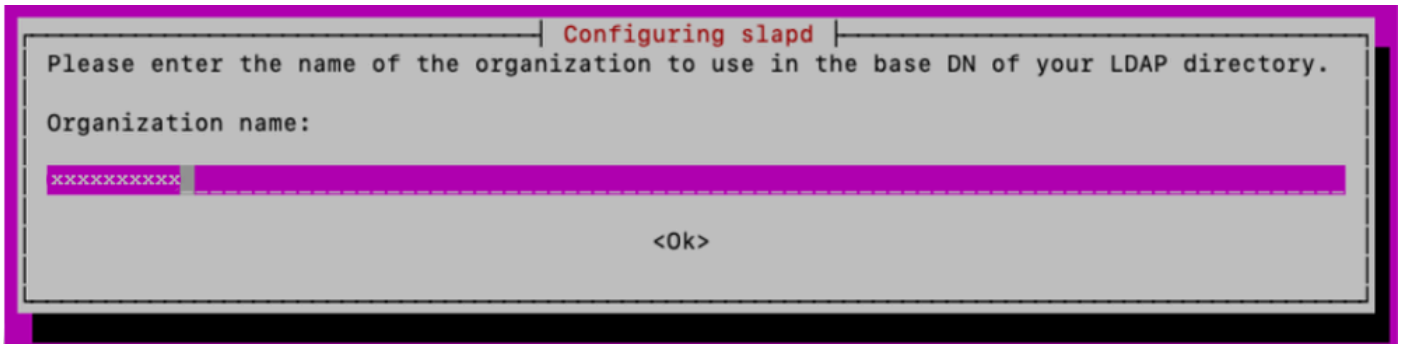
Vous pouvez accepter l'option par défaut « Non » pour « Omettre la configuration du serveur OpenLDAP » et appuyer sur Entrée :



Saisissez le nom de domaine et appuyez sur Entrée :



Pour ces travaux pratiques, « xxxxxxx » est utilisé comme « Nom de l'entreprise » :

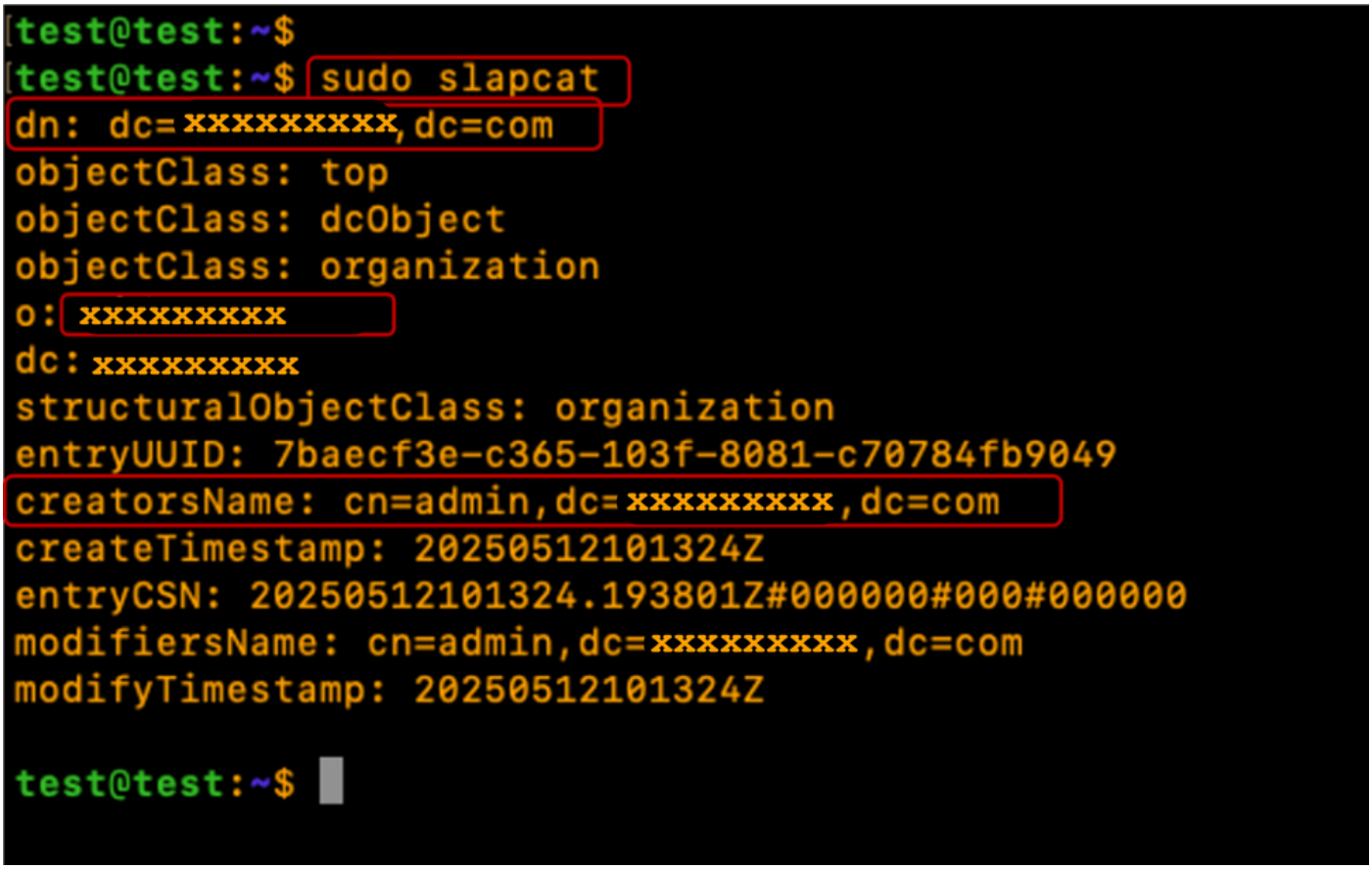


Entrez ensuite le « mot de passe administrateur », puis confirmez-le

Pour les autres options de configuration, conservez les valeurs par défaut et appuyez sur la touche Entrée du clavier pour terminer la configuration.

Vérifiez l'installation SLAPD à l'aide de la commande :

```
sudo slapcat
```



Étape 3 : Installation du gestionnaire de compte LDAP

Installez le gestionnaire de compte LDAP (LAM) pour la création et la gestion des utilisateurs et des groupes LDAP :

```
sudo apt -y install ldap-account-manager
```

Activez l'extension PHP-CGI, requise par LAM.

```
sudo a2enconf php*-cgi
```

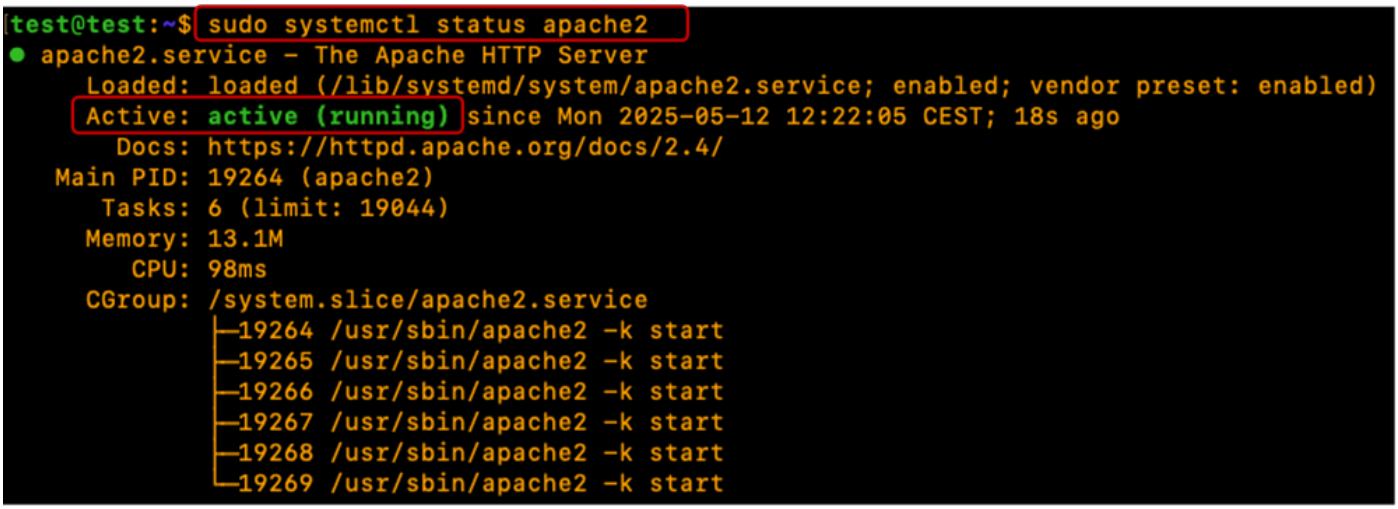
Rechargez Apache pour activer la nouvelle configuration.

Redémarrez et activez le service Apache pour qu'il démarre automatiquement au démarrage :

```
sudo systemctl reload apache2
sudo systemctl restart apache2
sudo systemctl enable apache2
```

Vérifiez que l'état du serveur Apache est en cours d'exécution et actif

```
sudo systemctl status apache2
```

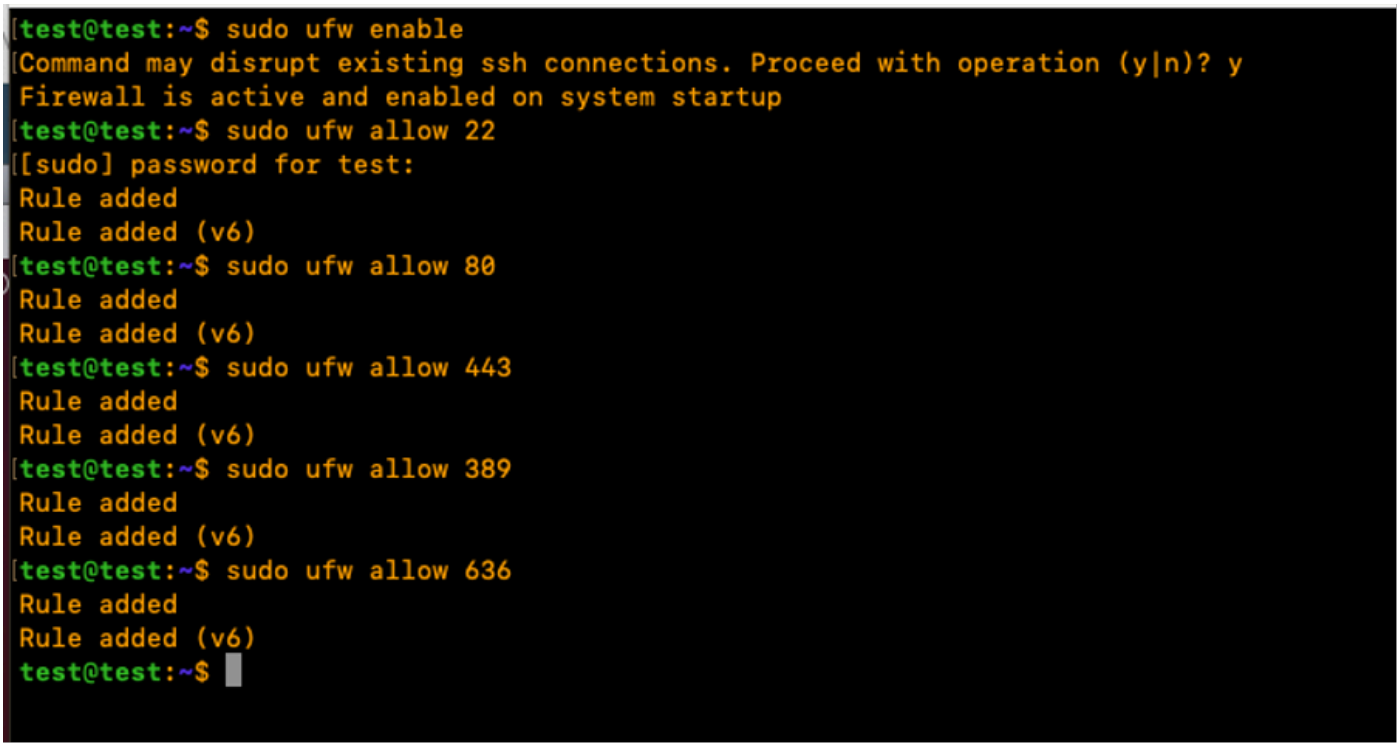


Configurez le pare-feu Ubuntu pour autoriser le port 80(Web), 443 (Web sécurisé), 389(LDAP) et 636 (LDAP sécurisé si nécessaire)

```
sudo ufw enable
sudo ufw allow 22
```

```
sudo ufw allow 80
sudo ufw allow 443
sudo ufw allow 389
```

```
sudo ufw allow 636
```



Vérifiez l'état du pare-feu Ubuntu :

```
sudo ufw status
```

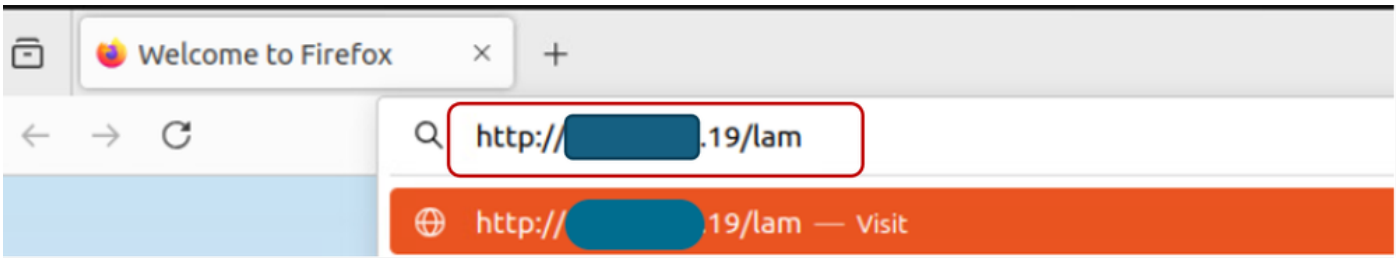
```
test@test:~$ sudo ufw status
Status: active

To                         Action      From
--                         ------      ----
22                         ALLOW       Anywhere
80                         ALLOW       Anywhere
443                        ALLOW       Anywhere
389                        ALLOW       Anywhere
636                        ALLOW       Anywhere
22 (v6)                    ALLOW       Anywhere (v6)
80 (v6)                    ALLOW       Anywhere (v6)
443 (v6)                   ALLOW       Anywhere (v6)
389 (v6)                   ALLOW       Anywhere (v6)
636 (v6)                   ALLOW       Anywhere (v6)
```

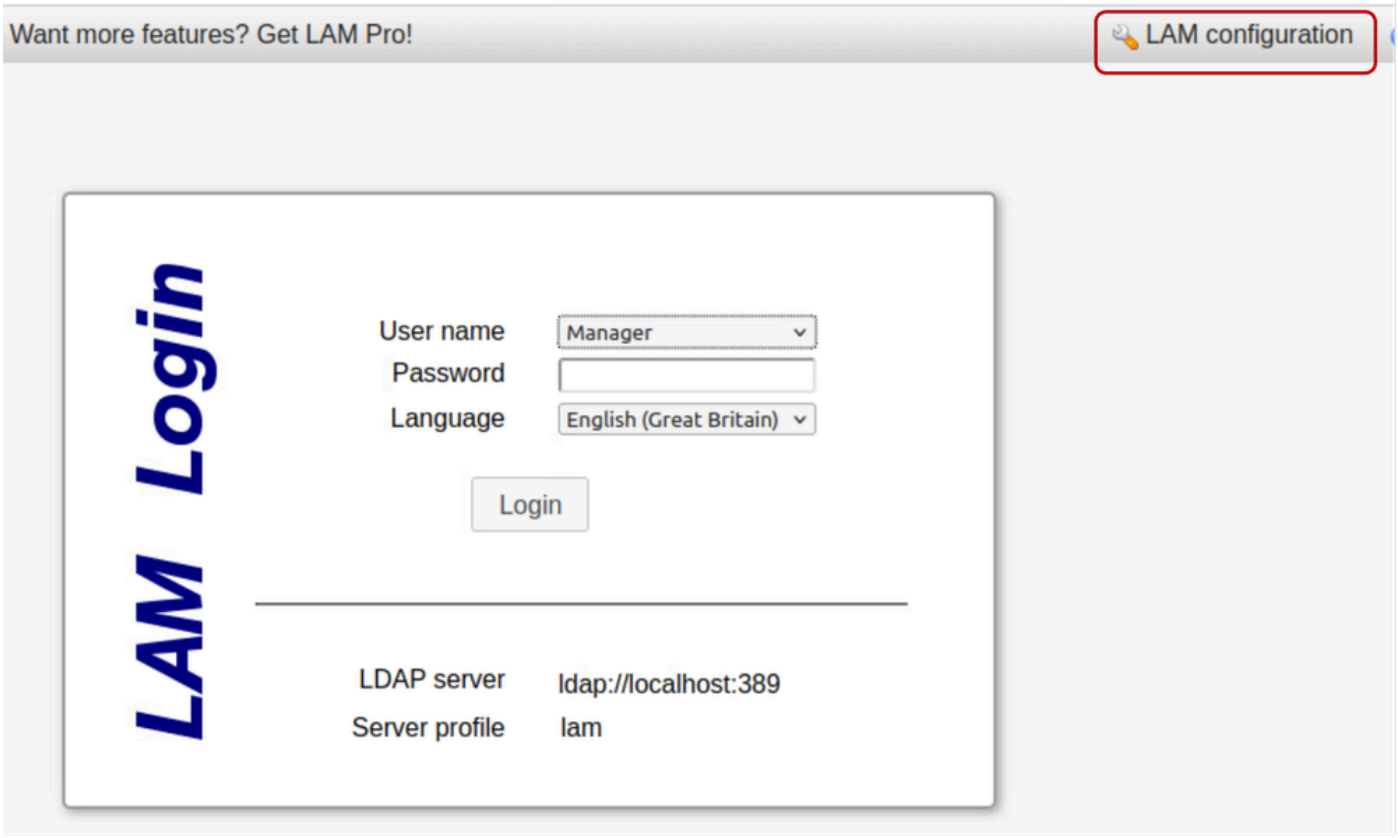
Étape 4: Configurer le gestionnaire de compte LDAP

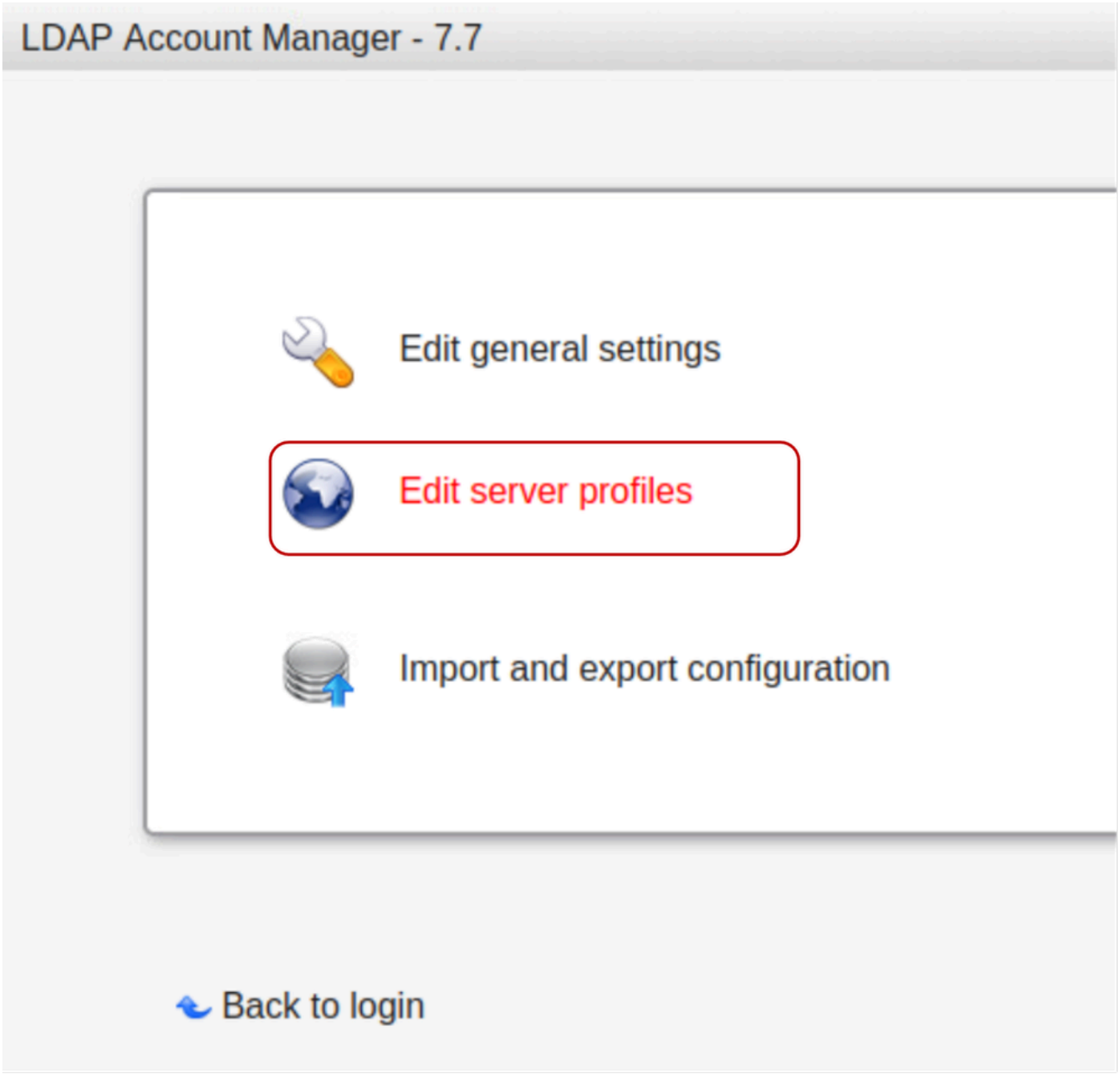
Pour configurer le gestionnaire de compte LDAP (LAM) à partir de l'interface utilisateur graphique, ouvrez un navigateur Web, entrez l'adresse IP du serveur Linux et ajoutez-y le chemin « lam » comme indiqué :

```
http://X.X.X.19/lam
```

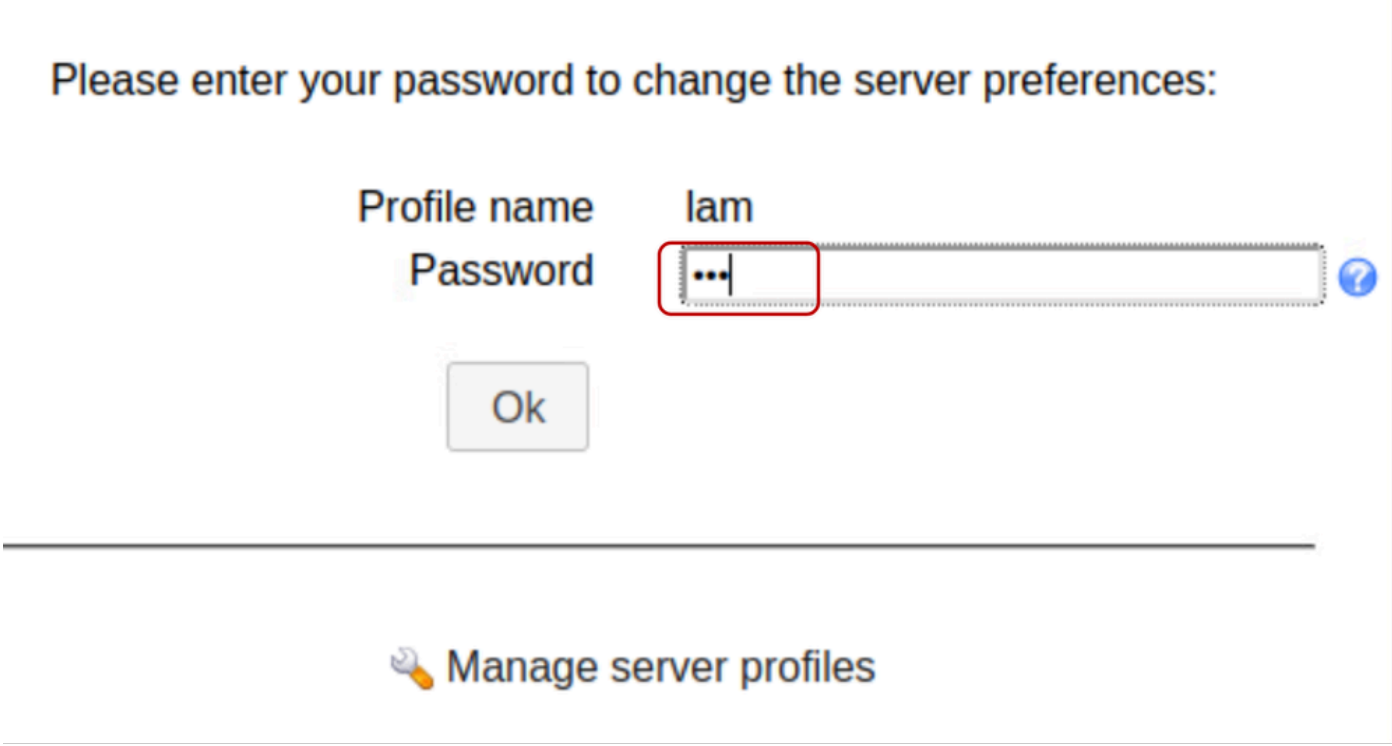


Cliquez sur "Configuration LAM" puis sélectionnez "Modifier les profils de serveur".


Want more features? Get LAM Pro!
LAM configuration
LAM Login
User name
Manager
Password
Language
English (Great Britain)
Login
LDAP server
ldap://localhost:389
Server profile
lam



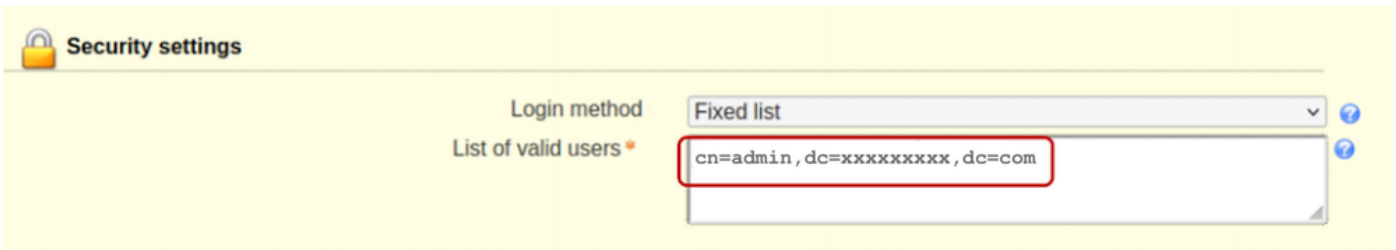
Entrez le mot de passe lam par défaut « lam » pour vous connecter.



Dans l'onglet General Settings, vérifiez les paramètres du serveur, la langue et le fuseau horaire.

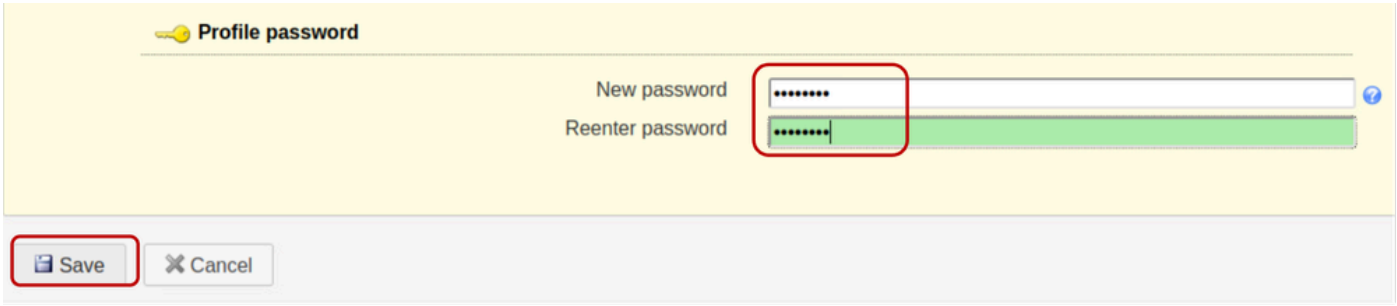
Dans la section Paramètres de l'outil, modifiez et ajoutez le nom de domaine requis dans le champ Suffixe de l'arborescence, comme indiqué ci-dessous :

Modifiez la section Security settings pour inclure un utilisateur « admin » utilisé pour gérer le service SLAPD.



Définissez un mot de passe de profil. Ce mot de passe est utilisé pour les connexions ultérieures à l'interface de configuration LAM. Dans cet exemple, « cisco123 » est configuré à la place du mot de passe « lam » par défaut.

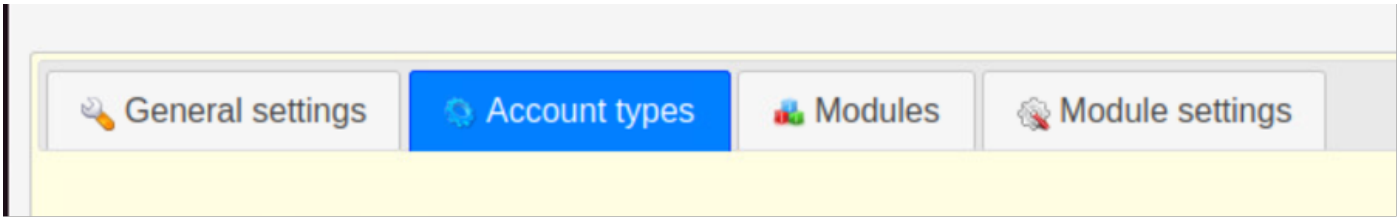
Enregistrez la configuration :



La session est ensuite redémarrée sur l'interface utilisateur graphique de configuration LAM.

Reconnectez-vous (configuration LAM >> Modifier les profils de serveur) en utilisant le nouveau mot de passe créé.

Cliquez sur le lien « Types de comptes »,



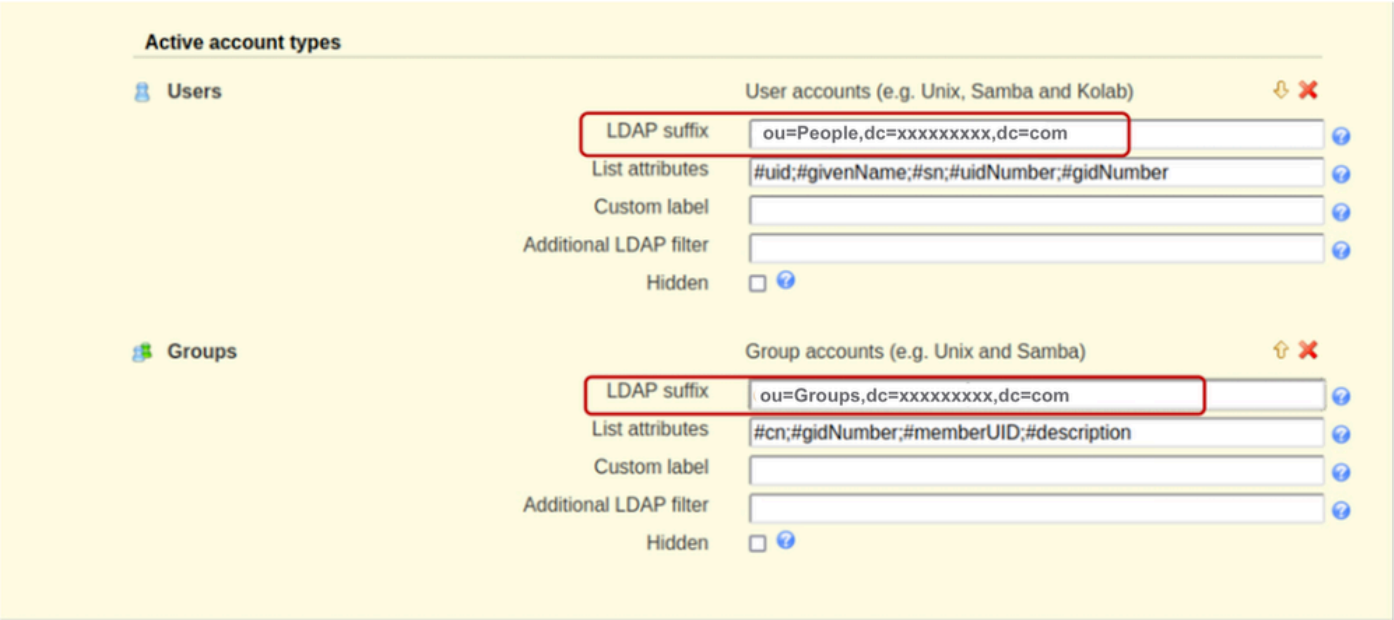
Faites défiler vers le bas et modifiez les types de comptes actifs par défaut avec les informations de nom de domaine dans le champ de suffixe LDAP. Par exemple, le contenu par défaut du champ « Suffixe LDAP » affiche la valeur « ou=People, dc=my-domain, dc=com ».

Si vous devez créer de nouvelles unités d'organisation, remplacez le contenu du champ « Suffixe LDAP » par le nom de l'unité d'organisation.

Le format affiché est « ou=<unité_d'organisation>,dc=xxxxxxx,dc=com ».

Pour cette démonstration, l'unité d'organisation pour les utilisateurs est « Personnes » et l'unité d'organisation pour les groupes est « Groupes ».

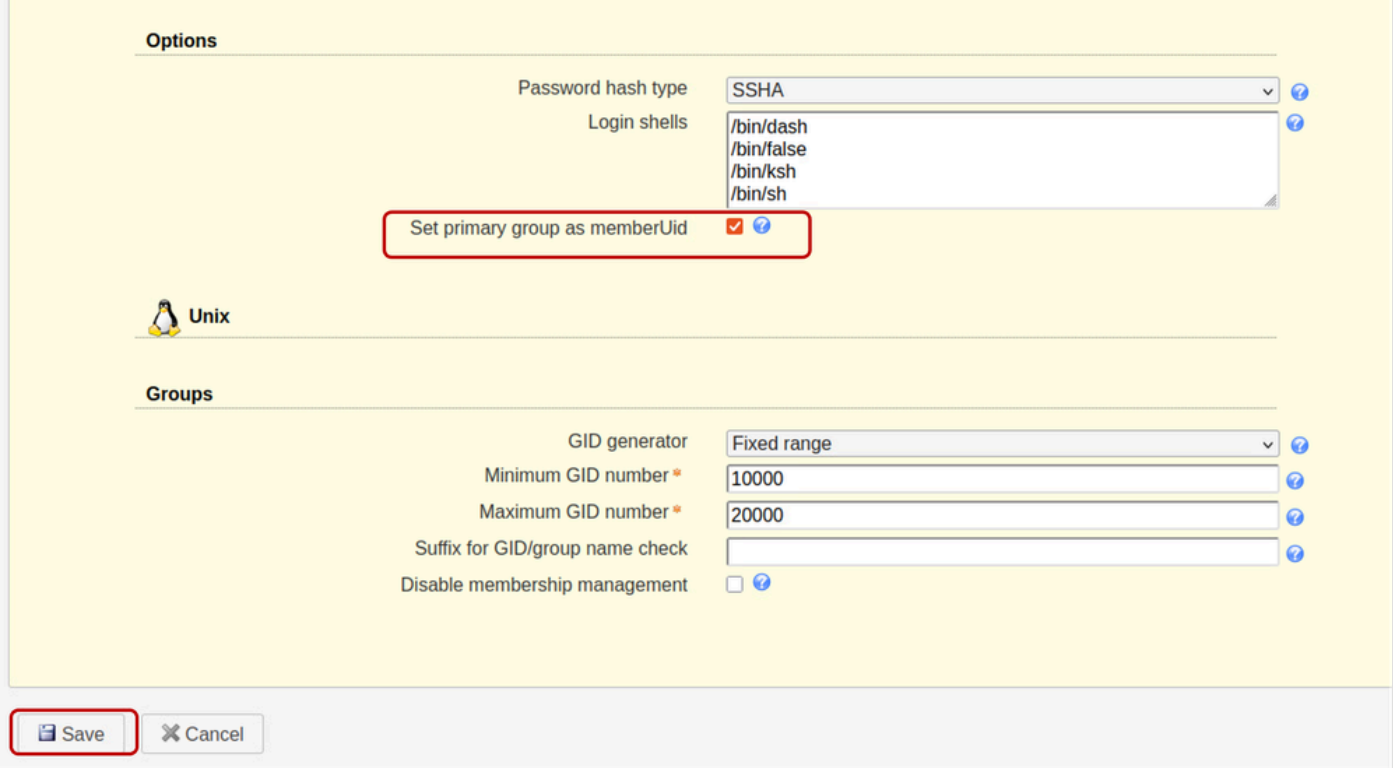
Enregistrez la configuration.



Faites défiler jusqu'à la section Options et assurez-vous de cocher la case « Set primary group as memberUid ».

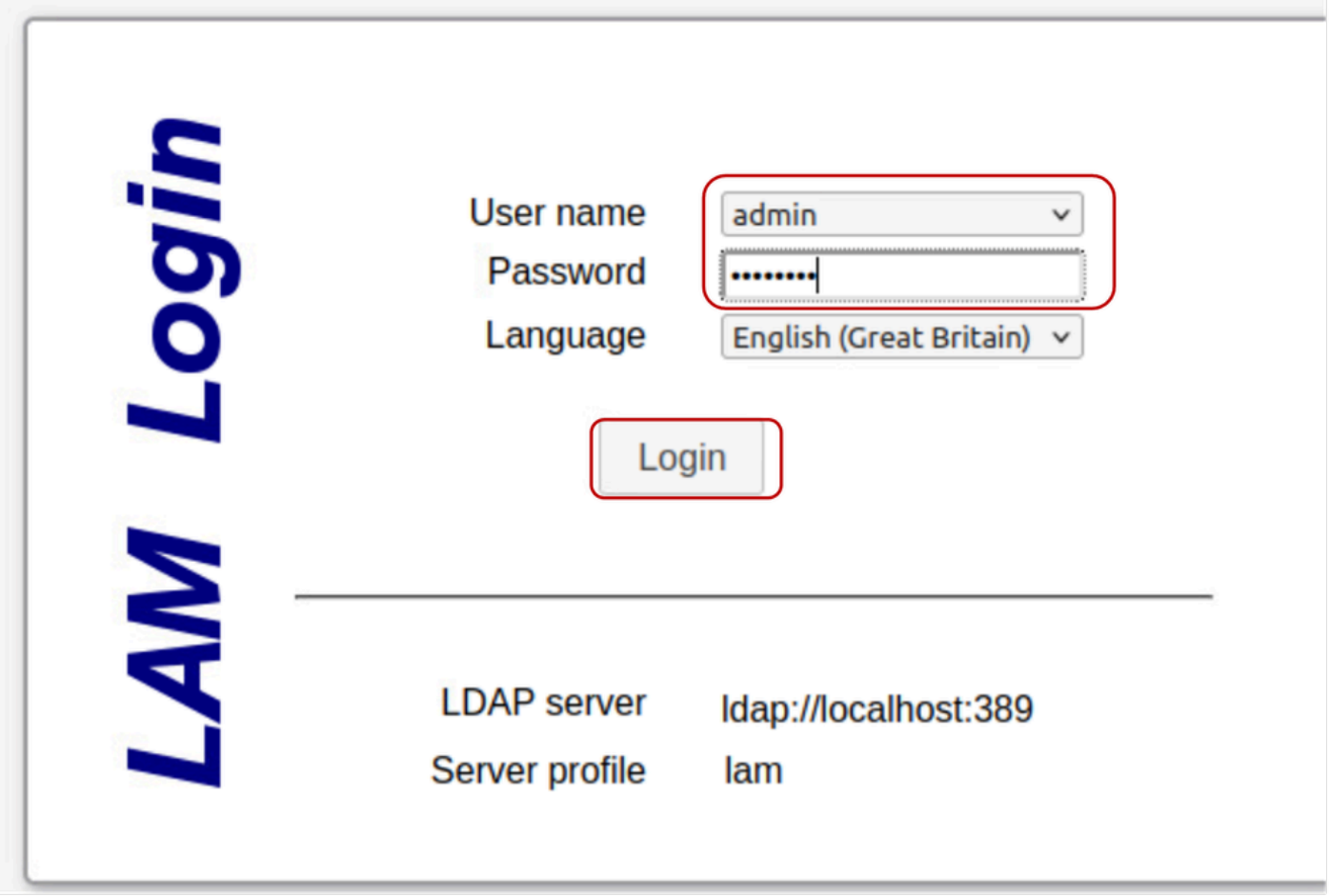
Par défaut, l'option « Définir le groupe principal en tant que memberUid » n'est pas définie sur les objets de groupe. L'activation de cette option permet d'utiliser OpenLDAP « Groupe principal » comme un groupe LDAP standard, où le « MemberUid » peut être référencé (Par exemple : Dans la configuration du serveur UCS série C). Si cette option n'est pas cochée, la connexion des utilisateurs appartenant à un groupe principal échoue.

Enregistrez la configuration.

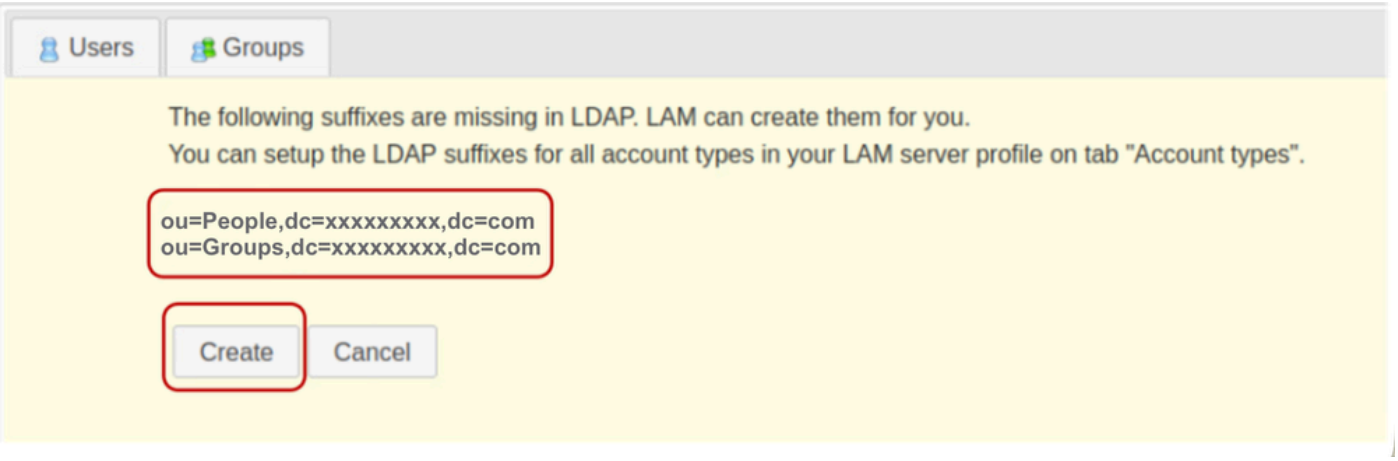


Étape 5 : Créez des unités organisationnelles, des groupes et des utilisateurs

Connectez-vous à LAM en tant qu'utilisateur « admin » avec le même mot de passe que celui créé lors de l'installation, pour créer des utilisateurs et des groupes appartenant aux unités organisationnelles créées précédemment (Personnes et Groupes) respectivement :

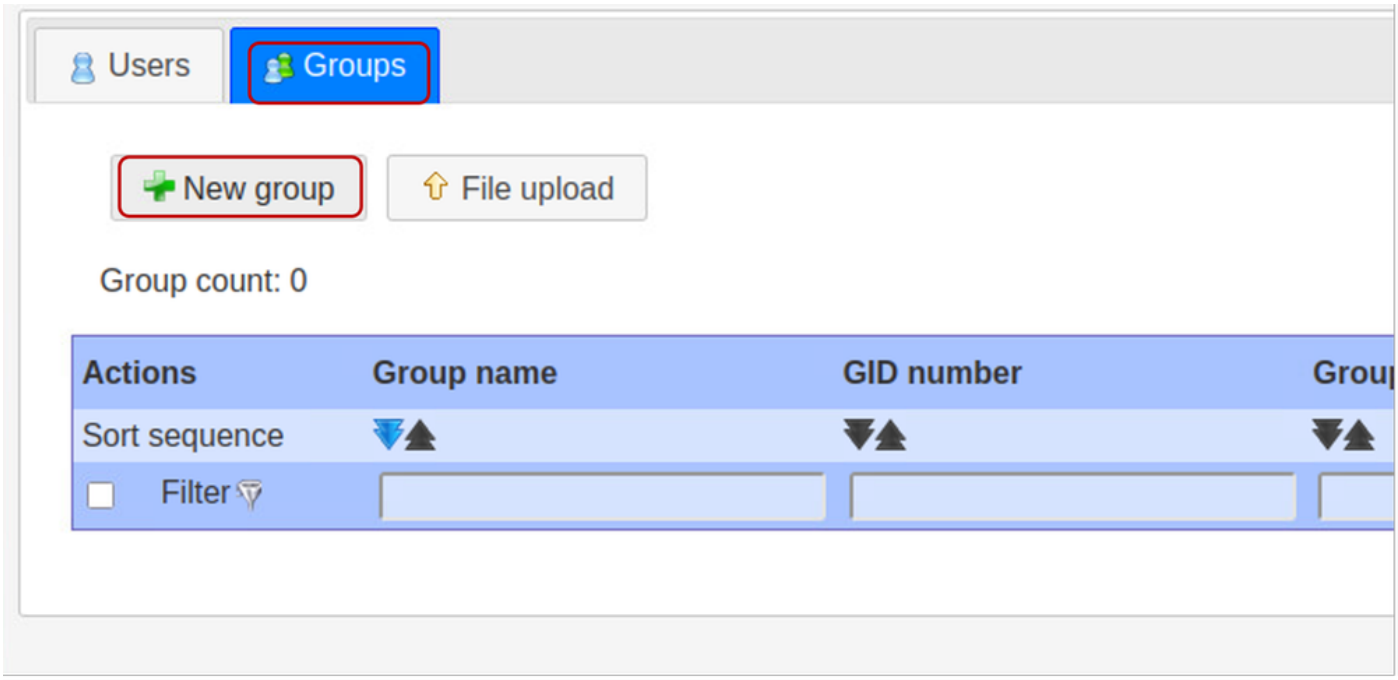


Créez les unités organisationnelles spécifiées précédemment dans la section Configuration LAM. Cliquez sur Créer.



Ensuite, dans le gestionnaire de comptes LDAP, créez le groupe « it » :

Sélectionnez l'onglet Groupes et cliquez sur Nouveau groupe

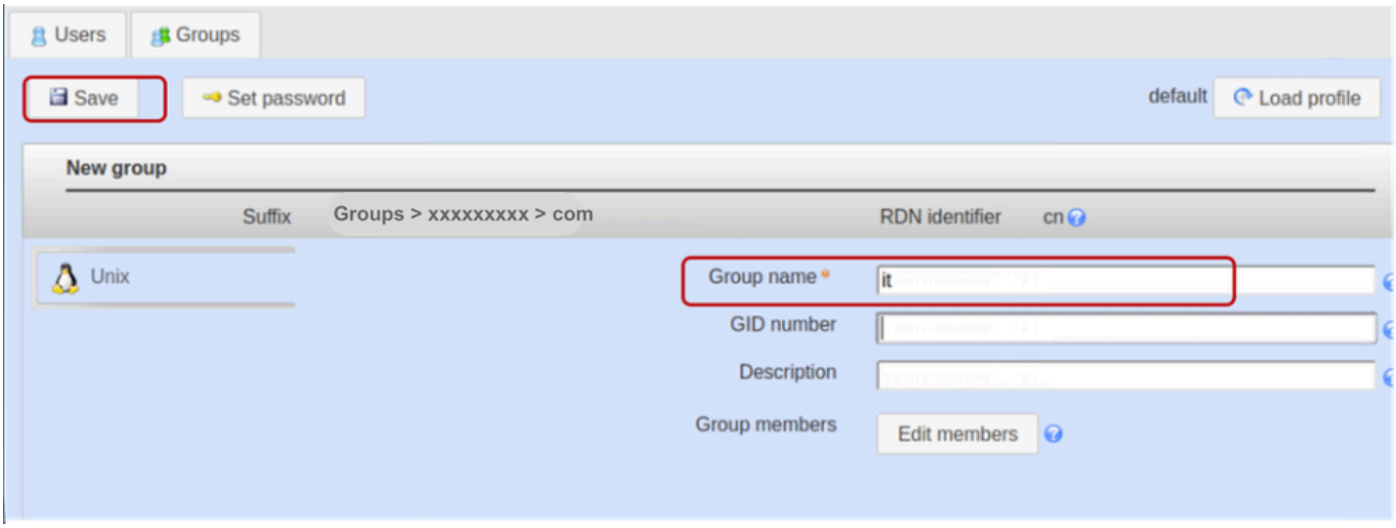


Définissez le nom du groupe sur « it ».

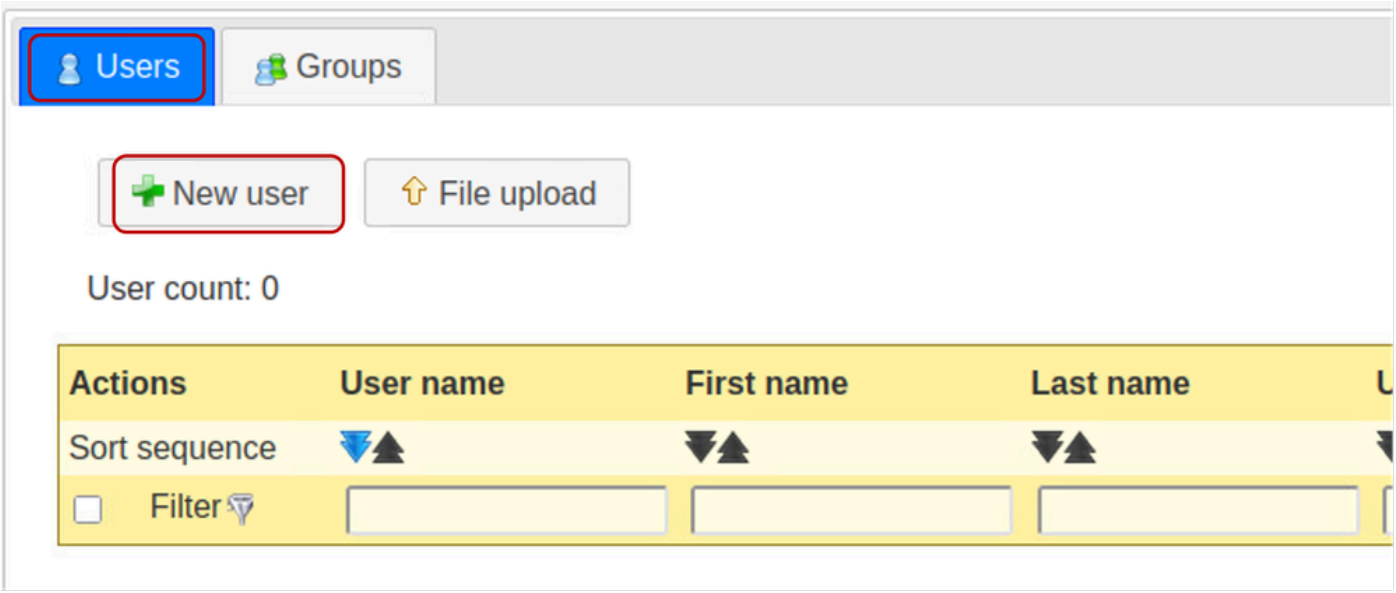
Remarque : Bien que les systèmes Cisco UCS soient généralement résistants aux variations de casse, le maintien des conventions d'attribution de noms en minuscules est une pratique recommandée pour garantir une interopérabilité à long terme entre divers environnements d'infrastructure de serveur LDAP.

Laissez le champ GID Number vide. Le gestionnaire de compte LDAP (LAM) est conçu pour remplir automatiquement ce champ avec la valeur disponible suivante.

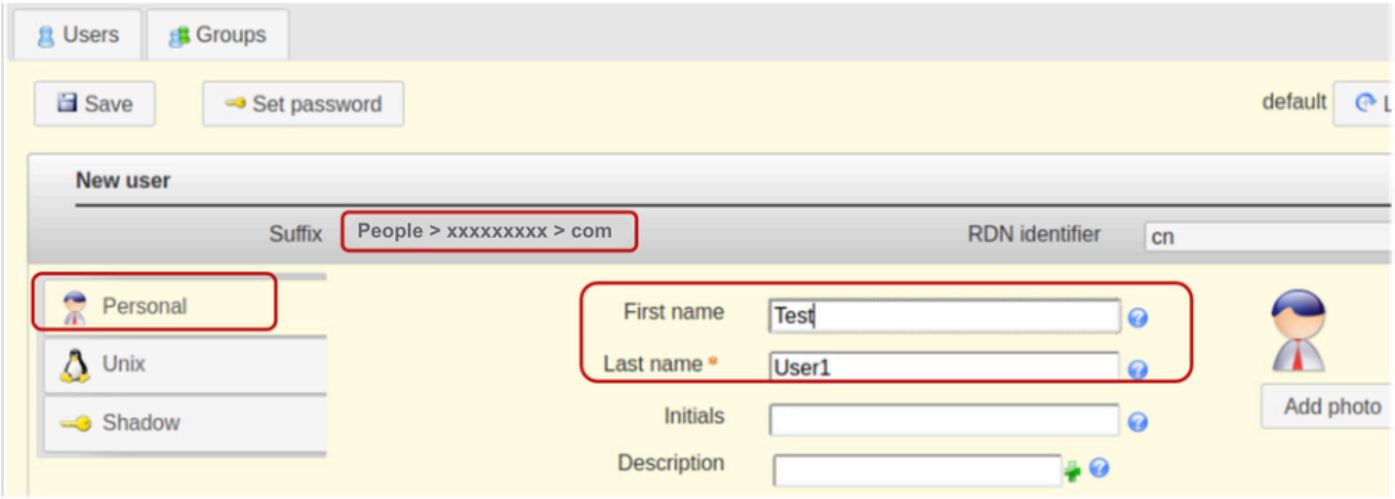
Fournissez une description si vous le souhaitez et cliquez sur Enregistrer



Cliquez sur l'onglet « Utilisateurs » pour créer des comptes d'utilisateurs et sélectionnez « Nouvel utilisateur ».



Renseignez les champs obligatoires de l'utilisateur « testuser1 » dans l'onglet Personnel.



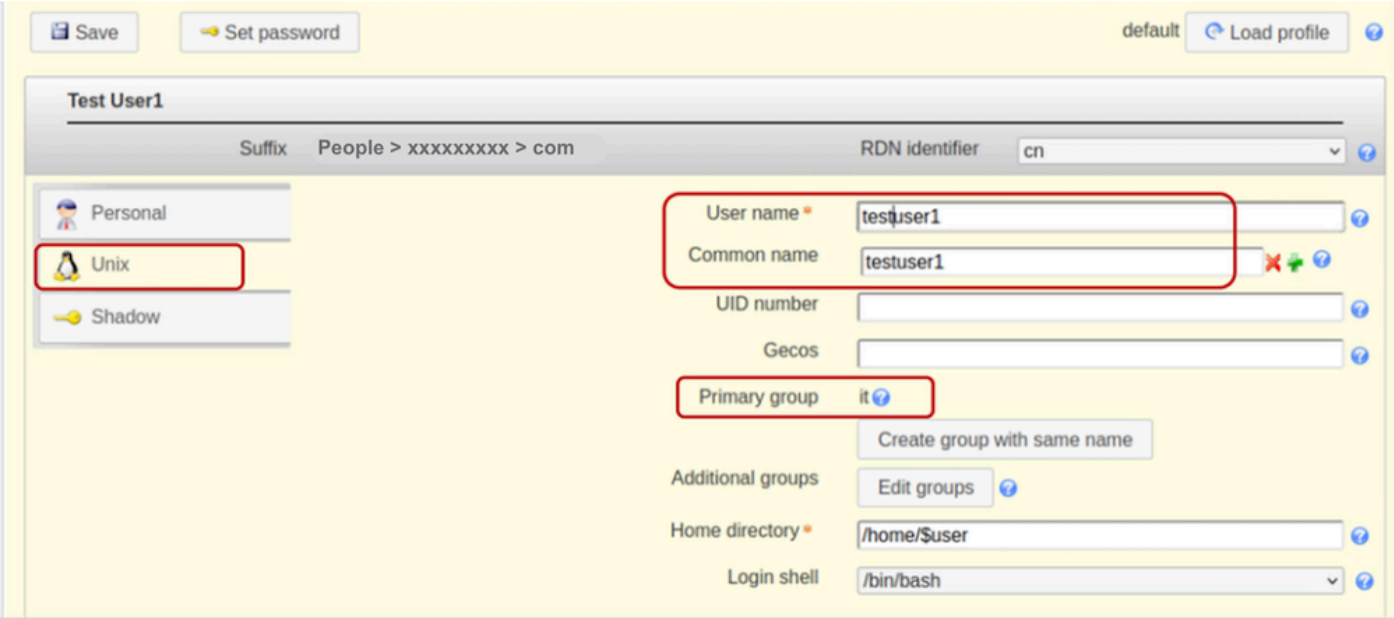
Sélectionnez l'onglet Unix, ajoutez testuser1 dans le champ User name. Inclure l'utilisateur dans le groupe « it ».

Pour cette démonstration, seul le groupe « it » existe et il est donc déjà prérempli.

Conservez l'identificateur RDN comme « Nom commun » (cn). Cela permet au système de remplir automatiquement le champ « Nom commun » à l'aide de la valeur spécifiée dans le champ « Nom d'utilisateur ».

Ne renseignez pas le champ UID Number, car LAM renseigne automatiquement le champ avec

les valeurs disponibles.



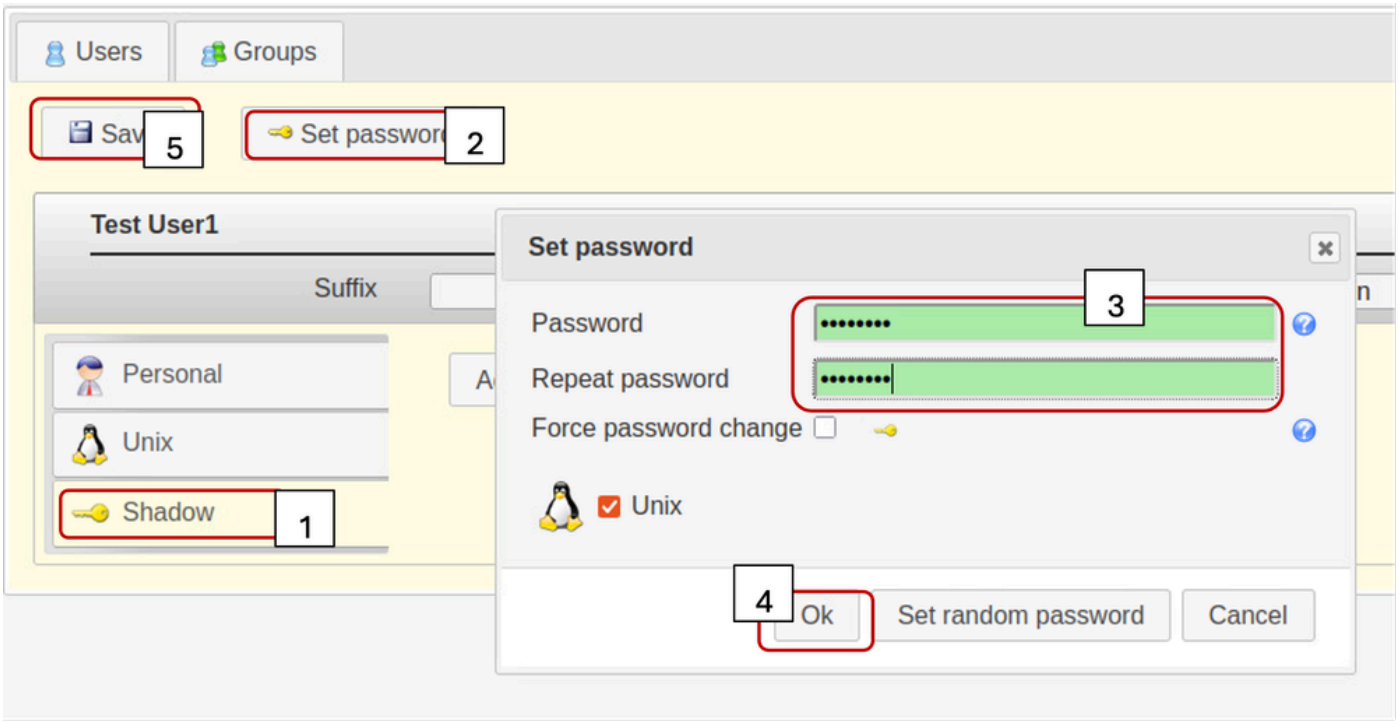
Sélectionnez l'onglet Ombre,

L'extension du compte fantôme n'est pas utilisée.

Cliquez sur « Définir le mot de passe ».

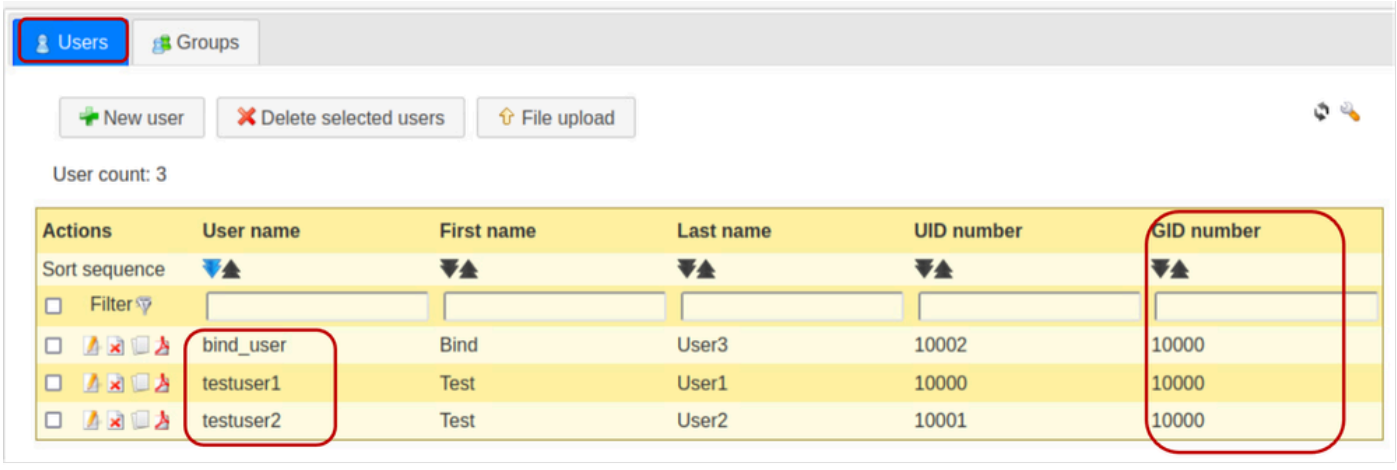
Définir le mot de passe utilisateur

Cliquez sur OK et sur Enregistrer



Répétez les étapes décrites précédemment afin de créer le compte d'utilisateur « testuser2 » et le compte « bind_user ».

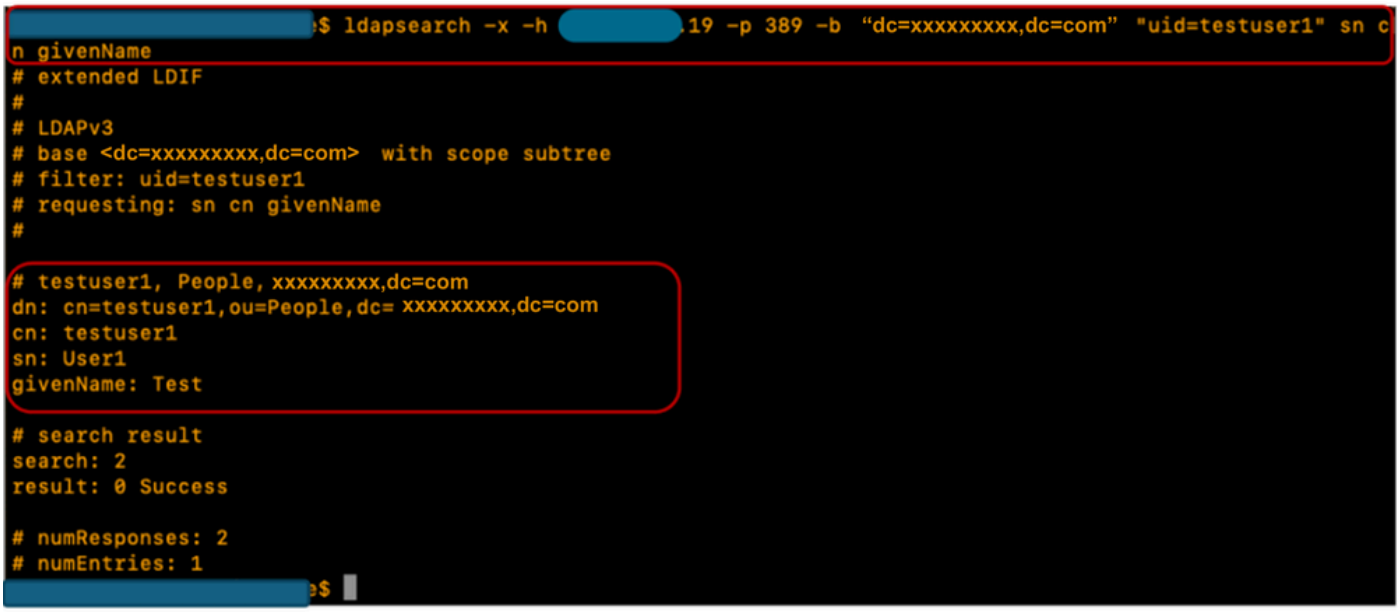
Cliquez sur l'onglet « Utilisateurs » pour vérifier la création de tous les utilisateurs souhaités. (La même valeur dans la colonne gidNumber confirme que les utilisateurs créés appartiennent au même groupe - it)



Étape 6 : Teste la connexion LDAP locale

Connectez-vous à un autre système basé sur Linux, ayant accès au serveur OpenLDAP. Exécutez la commande ldapsearch spécifiée pour vérifier que LDAP fonctionne :

```
ldapsearch -x -h X.X.X.19 -p 389 -b "dc=xxxxxxxxx,dc=com" "uid=testuser1" sn cn givenName
```



Paramètres de configuration sur CIMC

Connectez-vous à CIMC.

Dans le volet de navigation, sélectionnez Admin, User Management et LDAP.

Renseignez les paramètres de configuration LDAP comme indiqué ci-dessous :

- Enable LDAP : coché
- DN de base : dc=xxxxxxx, dc=com

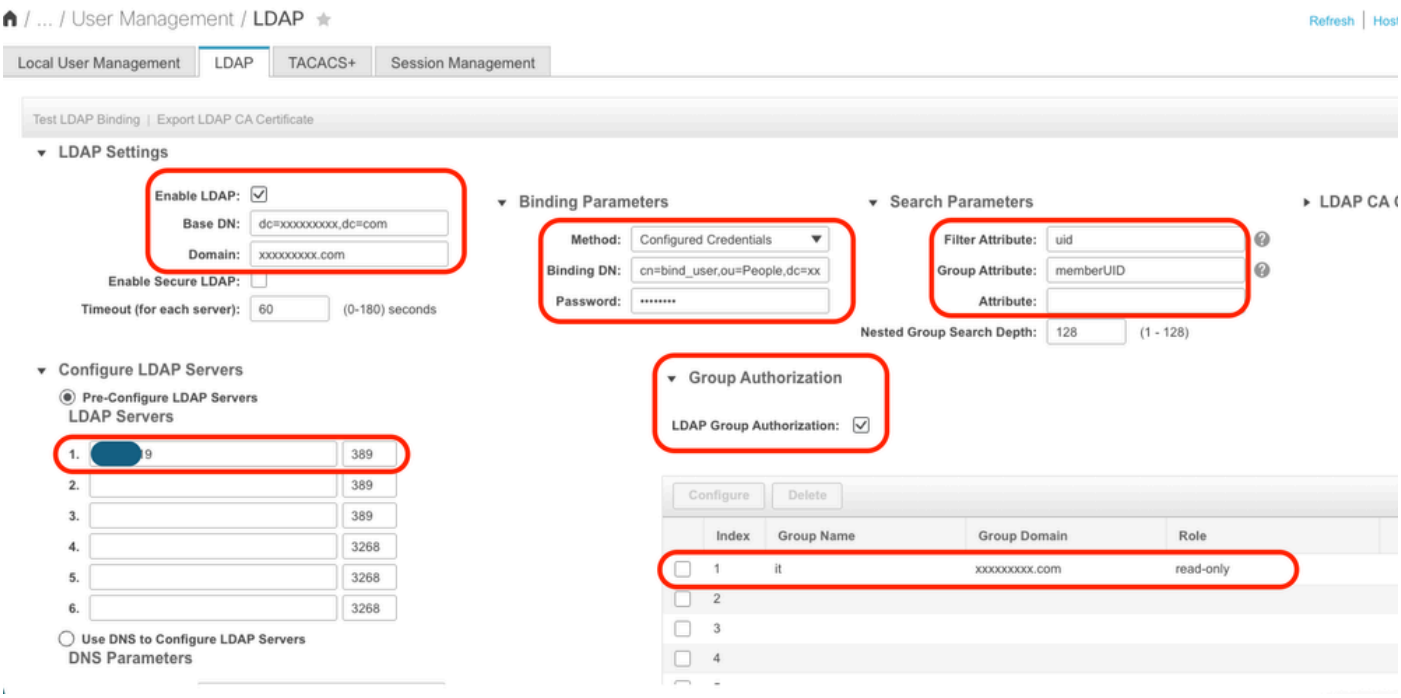
- Domaine : xxxxxxxxx.com

- Serveur LDAP : <ldap_server_IP ou FQDN> X.X.X.19

- Paramètres de liaison : « Identifiants de connexion » ou « Identifiants configurés »
  - Lors de l'utilisation des informations d'identification configurées, ajoutez le DN bind_user exactement comme configuré sur le serveur LDAP :
    - Par exemple : cn=bind_user,ou=People,dc=xxxxxxx,dc=com

- Paramètres de recherche :
  - Attribut de filtre : « cn » ou « uid »
  - Attribut de groupe : memberUID

- Autorisation de groupe LDAP - Coché
  - Nom du groupe : il
  - Domaine du groupe : xxxxxxxxx.com
  - Rôle : lecture seule (tout rôle souhaité)



Enregistrez la configuration et testez la connexion utilisateur LDAP.

Paramètres de configuration sur UCS Manager

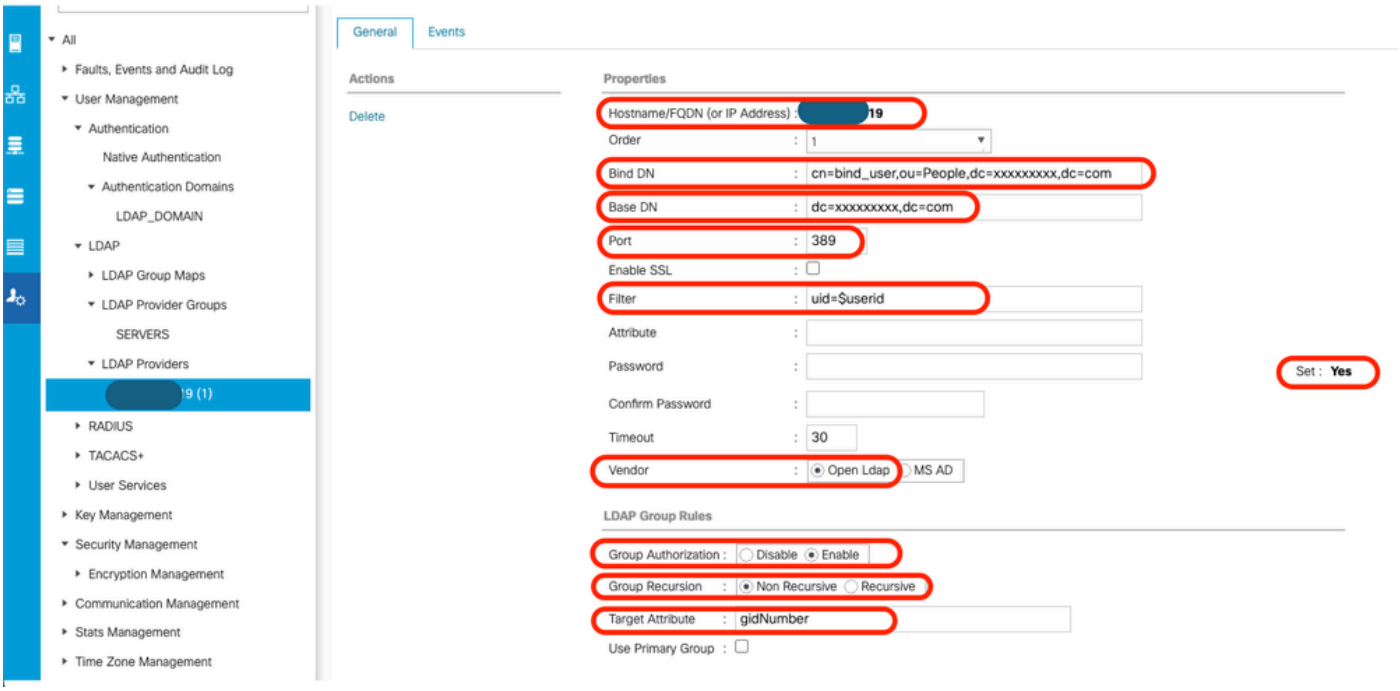
Connectez-vous à UCS Manager.

Dans le volet de navigation, sélectionnez Admin, User Management et LDAP.

Renseignez les paramètres de configuration LDAP comme indiqué ci-dessous :

- Fournisseurs LDAP :
  - Nom d'hôte : <nom de domaine complet ou adresse IP du serveur LDAP>
  - DN de liaison : cn=bind_user,ou=People,dc=xxxxxxx,dc=com
  - DN de base : dc=xxxxxxx, dc=com
  - Port : 389
  - Activer SSL : Désactivé
  - Filtre : uid=$userid
  - Autorisation de groupe : Activée
  - Récursivité du groupe : Non récursif

    - Attribut cible : gidNumber
- Mappages de groupes LDAP :
    - DN du groupe LDAP : 10000 <gidNumber pour le groupe « it »>

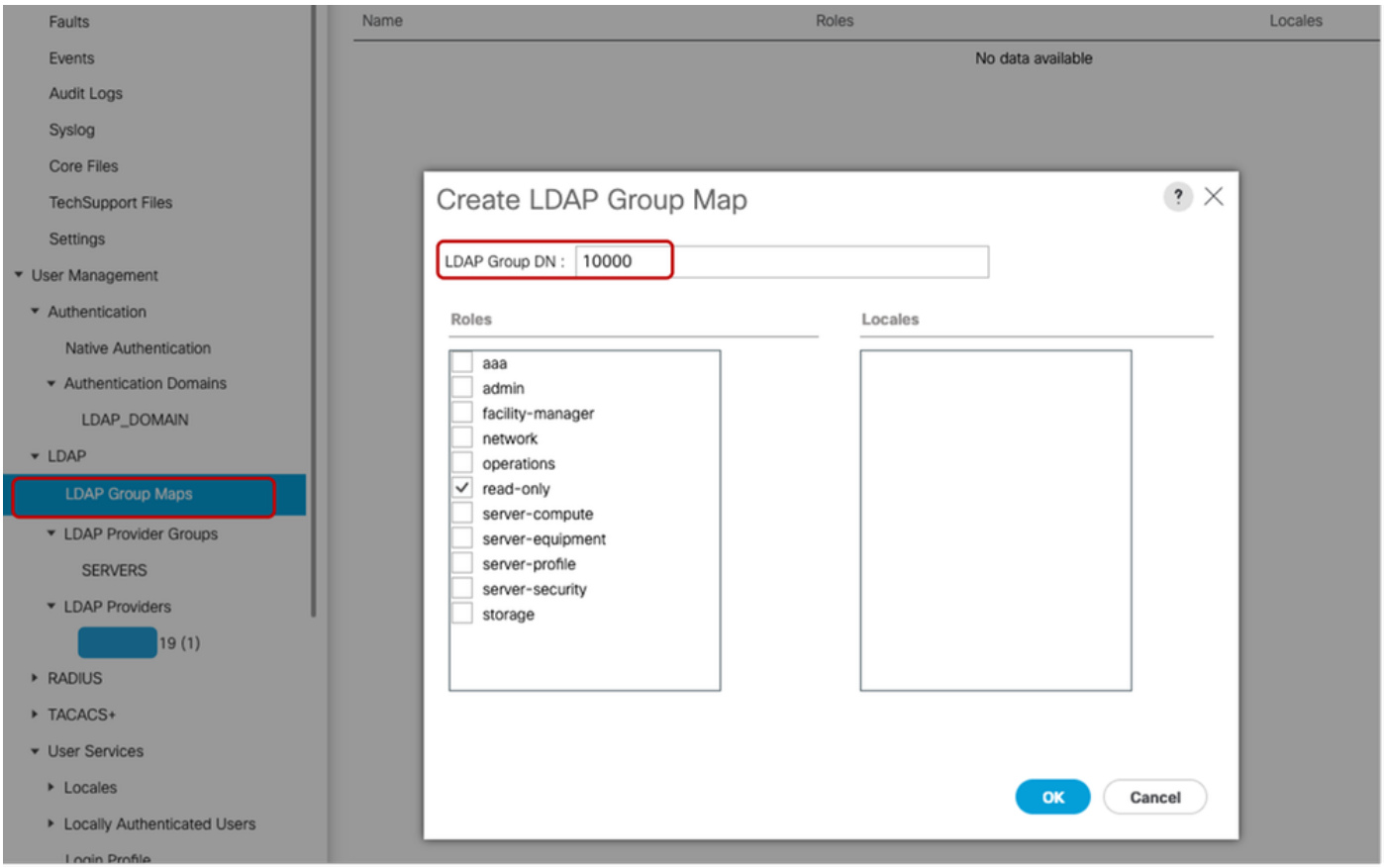


Sous All >> User Management >> LDAP >> LDAP Providers> LDAP Group Rules, l'attribut cible par défaut pour UCS Manager est « memberOf ». Par défaut, cet attribut n'est pas activé sur les serveurs OpenLDAP. Par conséquent, si vous définissez la valeur de l'attribut cible sur « memberOf » (ou si vous la laissez vide), les connexions des utilisateurs échouent, car le serveur OpenLDAP ne reconnaît pas la valeur d'attribut demandée.

Dans cet exemple, la valeur « Target Attribute » a été définie sur « gidNumber ».

Ajoutez le fournisseur LDAP configuré à un groupe de fournisseurs LDAP. Pour cette démonstration, le groupe de fournisseurs LDAP « SERVERS » a été créé.

Lors de la configuration des « mappages de groupes LDAP » dans « Tous >> Gestion des utilisateurs >> LDAP >>>>> », la valeur gidNumber (dans ce cas « 10000 ») est utilisée comme « mappage de DN de groupe », comme indiqué :



Configurez un domaine d'authentification LDAP (LDAP_DOMAIN) dans « Tous >> Gestion des utilisateurs >> Authentification >> Domaines d'authentification » faisant référence aux groupes de fournisseurs LDAP et testez la connexion des utilisateurs LDAP.

Remarque : Si l'attribut memberOf est requis pour répondre à des exigences environnementales spécifiques ou pour implémenter la fonctionnalité « Group Recursion », il est recommandé d'utiliser la deuxième option de configuration ci-dessous, qui nécessite LDAP avec les extensions de superposition activées.

Bien que le gestionnaire de compte LDAP (LAM) prenne en charge la configuration de superposition, cette fonctionnalité nécessite une licence appropriée.

Pour plus d'informations sur la configuration de LDAP en utilisant LAM, référez-vous à la documentation officielle du gestionnaire de compte LDAP.

Option 2: Configurer OpenLDAP à l'aide des outils et superpositions Ubuntu CLI

Afin d'utiliser OpenLDAP pour l'authentification UCS Manager, deux superpositions sont nécessaires pour garantir que les groupes sont associés aux utilisateurs d'une manière compréhensible par le système UCS (UCS Manager et CIMC).

La configuration côté OpenLDAP nécessite :

- superposition "member of" : Cette superposition crée un mappage entre les utilisateurs et les groupes de sorte que si un DN utilisateur est interrogé, l'attribut memberOf peut être demandé dans le cadre de cette requête. Par défaut, aucun attribut n'est attribué aux utilisateurs pour l'appartenance à un groupe, sauf si le membre de superposition est ajouté à openLDAP
- superposition "raffiner" : Cette superposition est configurée pour valider que les entrées de l'attribut de membre dans les objets de groupe restent synchronisées avec l'attribut memberOf des objets utilisateur. Sans ce service, si un utilisateur est supprimé sans modifier le groupe, les noms distinctifs (DN) orphelins peuvent rester dans l'objet groupe. Le service raffiné assure la cohérence dans les deux directions.

Étape 1 : Initialisation de net-tools et configuration du nom d'hôte du serveur Linux

Répétez l'étape 1 dans l'option 1.

Étape 2 : installation de SLAPD

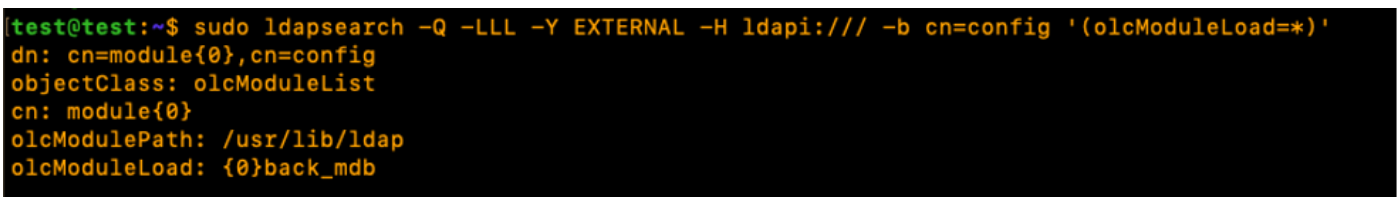
Répétez l'étape 2 dans l'option 1. (À l'exception de l'installation de PHP et Apache car l'option 2 ne nécessite pas leur fonctionnement - pas de LAM)

Assurez-vous d'autoriser les ports requis via le pare-feu Ubuntu.

Étape 3: Installer la superposition « memberOf » sur le serveur LDAP

Vérifiez si la superposition « memberOf » est installée

```
sudo ldapsearch -Q -LLL -Y EXTERNAL -H ldapi:/// -b cn=config '(olcModuleLoad=*)'
```



Pour installer la superposition « memberOf », créez un fichier .ldif nommé ldap.memberof.load.ldif

(utilisez n'importe quelle convention d'attribution de noms) et ajoutez la configuration spécifiée :

```
cat <

      ./ldap.memberof.load.ldif
dn: cn=module,cn=config
objectClass: olcModuleList
cn: module olcModuleLoad: memberof
EOF
```

Ajoutez la configuration du fichier ldap.memberof.load.ldif au profil LDAP à l'aide de la commande spécifiée :

```
sudo ldapadd -Q -Y EXTERNAL -H ldapi:/// -f ./ldap.memberof.load.ldif
```

Configure le module memberOf et l'entrée olcDatabase pour correspondre aux exigences de déploiement, selon les distributions Linux.

Deux valeurs d'attribut obligatoires sont "olcDatabase={1}mdb" et "groupOfNames", comme indiqué ci-dessous.

Créez le fichier ldap.memberof.config.ldif, renseignez ses attributs et importez son contenu dans le profil LDAP.

```
cat <

      ./ldap.memberof.config.ldif
dn: olcOverlay=memberof,olcDatabase={1}mdb,cn=config
objectClass: olcMemberOf
objectClass: olcOverlayConfig
olcOverlay: memberof
olcMemberOfGroupOC: groupOfNames
olcMemberOfMemberAD: member
olcMemberOfMemberOfAD: memberOf
olcMemberOfRefInt: TRUE
olcMemberOfDangling: ignore
EOF
```

```
sudo ldapadd -Q -Y EXTERNAL -H ldapi:/// -f ./ldap.memberof.config.ldif
```

Étape 4: Installer la superposition affinée sur le serveur LDAP

Ensuite, installez le raffinage sur openldap :

créez un fichier .ldif nommé ldap.rafft.load.ldif (utilisez n'importe quelle convention d'attribution de noms) et ajoutez la configuration spécifiée :

```
cat <

      ./ldap.refint.load.ldif
dn: cn=module,cn=config
objectClass: olcModuleList
cn: module
olcModuleLoad: refint
EOF
```

Importez la configuration dans le fichier ldap.rafft.load.ldif dans le profil LDAP en utilisant la commande spécifiée :

```
sudo ldapadd -Q -Y EXTERNAL -H ldapi:/// -f ./ldap.refint.load.ldif
```

Configurez la fonction Affiner, qui maintient l'intégrité référentielle entre les groupes et les utilisateurs.

Configure le module d'affinement et son entrée olcDatabase pour répondre aux exigences de déploiement.

Créez le fichier ldap.rafft.config.ldif et importez son contenu dans le profil LDAP.

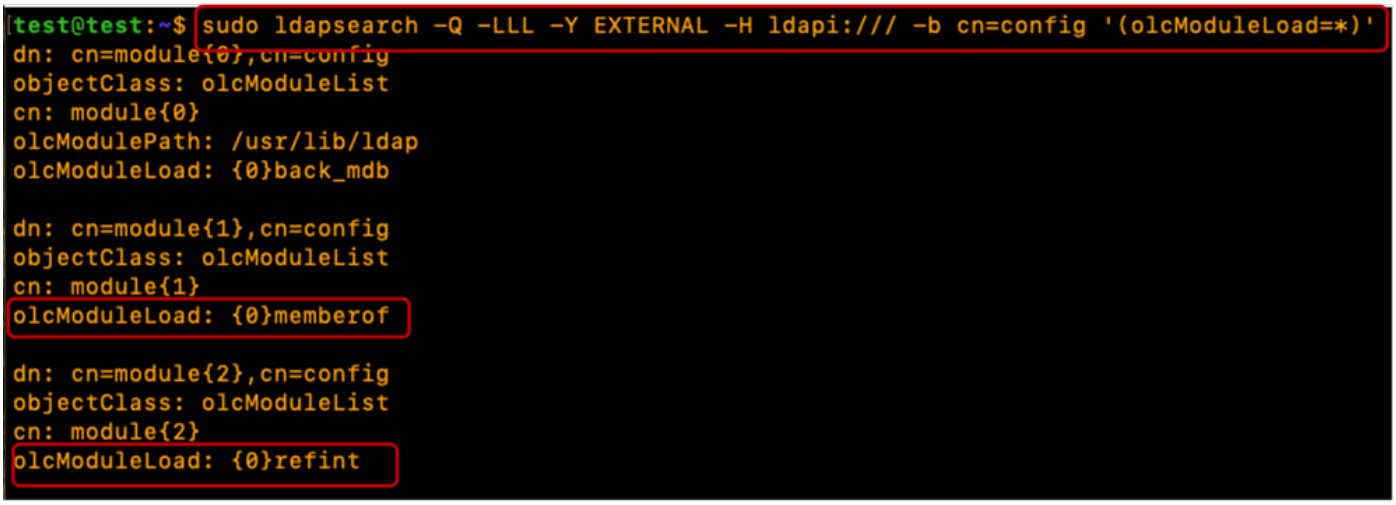
```
cat <
```

```
      ./ldap.refint.config.ldif
dn: olcOverlay=refint,olcDatabase={1}mdb,cn=config
objectClass: olcConfig
objectClass: olcOverlayConfig
objectClass: olcRefintConfig
olcOverlay: refint
olcRefintAttribute: memberOf member
EOF
```

```
sudo ldapadd -Q -Y EXTERNAL -H ldapi:/// -f ./ldap.refint.config.ldif
```

Lors de l'installation des deux plugins/extensions, le résultat de la commande ldapsearch spécifiée est similaire au résultat affiché ci-dessous :

```
sudo ldapsearch -Q -LLL -Y EXTERNAL -H ldapi:/// -b cn=config '(olcModuleLoad=*)'
```



Lorsque les deux plugins/extensions sont configurés, le résultat de la commande ldapsearch spécifiée est similaire au résultat affiché :

```
sudo ldapsearch -Q -LLL -Y EXTERNAL -H ldapi:/// -b cn=config '(olcOverlay=memberof)'
```

```
test@test:~$ sudo ldapsearch -Q -LLL -Y EXTERNAL -H ldapi:/// -b cn=config '(olcOverlay=memberof)'
dn: olcOverlay={0}memberof,olcDatabase={1}mdb,cn=config
objectClass: olcMemberOfConfig
objectClass: olcOverlayConfig
olcOverlay: {0}memberof
olcMemberOfDangling: ignore
olcMemberOfRefInt: TRUE
olcMemberOfGroupOC: groupOfNames
olcMemberOfMemberAD: member
olcMemberOfMemberOfAD: memberOf

test@test:~$
```

```
sudo ldapsearch -Q -LLL -Y EXTERNAL -H ldapi:/// -b cn=config '(olcOverlay=refint)'
```

```
test@test:~$ sudo ldapsearch -Q -LLL -Y EXTERNAL -H ldapi:/// -b cn=config '(olcOverlay=refint)'
dn: olcOverlay={1}refint,olcDatabase={1}mdb,cn=config
objectClass: olcConfig
objectClass: olcOverlayConfig
objectClass: olcRefintConfig
olcOverlay: {1}refint
olcRefintAttribute: memberOf member
```

Redémarrez le service slapd pour que les modules/plugins nouvellement installés soient utilisables :

```
sudo systemctl restart slapd
```

Étape 5: Créer des unités organisationnelles, des utilisateurs et des groupes

Créer des unités organisationnelles (pour les utilisateurs et les groupes), des utilisateurs et des groupes.

Créez les unités organisationnelles Utilisateurs (Personnes) et Groupes (Groupes) et importez-les dans le profil LDAP. Cela nécessite le mot de passe du compte « admin » :

```
cat <
```

```
      ./ldap.ou.add.ldif
dn: ou=People,dc=xxxxxxxxx,dc=com
objectClass: organizationalUnit
ou: People
```

```
dn: ou=Groups,dc=xxxxxxxxx,dc=com
objectClass: organizationalUnit
ou: Groups
EOF
```

```
sudo ldapadd -xcWD cn=admin,dc=xxxxxxxxx,dc=com -f ./ldap.ou.add.ldif
```

Créez les utilisateurs (testuser1, testuser2 et bind_user), mappez-les à leurs unités organisationnelles respectives (People), ajoutez-les à leurs groupes à l'aide de la méthode gidNumbers (pratique recommandée) et importez les utilisateurs dans le profil LDAP.

```
cat <
```

```
      ./ldap.users.ldif
dn: uid=testuser1,ou=People,dc=xxxxxxxxx,dc=com
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: shadowAccount
uid: testuser1
sn: User1
givenName: Test
cn: testuser1
displayName: Test User1
gidNumber: 10000
uidNumber: 10000
userPassword: cisco123
gecos: Test User1
loginShell: /bin/bash
homeDirectory: /home/testuser1
```

```
dn: uid=testuser2,ou=People,dc=xxxxxxxxx,dc=com
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: shadowAccount
uid: testuser2
sn: User2
givenName: Test
cn: testuser2
displayName: Test User2
gidNumber: 10000
uidNumber: 10001
userPassword: cisco123
gecos: Test User2
loginShell: /bin/bash
homeDirectory: /home/testuser2

dn: uid=bind_user,ou=People,dc=xxxxxxxxx,dc=com
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: shadowAccount
uid: bind_user
sn: User3
givenName: Bind
cn: bind_user
displayName: Bind User3
gidNumber: 10001
uidNumber: 10002
userPassword: cisco123
gecos: Bind User3
loginShell: /bin/bash
homeDirectory: /home/bind_user
EOF
```

```
sudo ldapadd -xcWD cn=admin,dc=xxxxxxxxx,dc=com -f ./ldap.users.ldif
```

```
test@test:~$ cat <<EOF > ./ldap.users.ldif
dn: uid=testuser1,ou=People,dc=xxxxxxxxx,dc=com
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: shadowAccount
uid: testuser1
sn: User1
givenName: Test
cn: testuser1
displayName: Test User1
gidNumber: 10000
uidNumber: 10000
userPassword: cisco123
gecos: Test User1
loginShell: /bin/bash
homeDirectory: /home/testuser1

dn: uid=testuser2,ou=People,dc=xxxxxxxxx,dc=com
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: shadowAccount
uid: testuser2
sn: User2
givenName: Test
cn: testuser2
displayName: Test User2
gidNumber: 10000
uidNumber: 10001
userPassword: cisco123
gecos: Test User2
loginShell: /bin/bash
homeDirectory: /home/testuser2


dn: uid=bind_user,ou=People,dc=xxxxxxxxx,dc=com
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: shadowAccount
uid: bind_user
sn: User3
givenName: Bind
cn: bind_user
displayName: Bind User3
gidNumber: 10001
uidNumber: 10002
userPassword: cisco123
gecos: Bind User3
loginShell: /bin/bash
homeDirectory: /home/bind_user
EOF
test@test:~$ sudo ldapadd -xcWD  cn=admin,dc=xxxxxxxxx,dc=com -f ./ldap.users.ldif
Enter LDAP Password:
adding new entry "uid=testuser1,ou=People,dc=xxxxxxxxx,dc=com

adding new entry "uid=testuser2,ou=People,dc=xxxxxxxxx,dc=com

adding new entry "uid=bind_user,ou=People,dc=xxxxxxxxx,dc=com

test@test:~$
```

Créez les groupes (it), mappez-les à leurs unités organisationnelles respectives (Groupes), associez les membres du groupe (testuser1, testuser2) et importez-les dans le profil LDAP :

```
cat <


      ./ldap.group.create.ldif
dn: cn=it,ou=Groups,dc=xxxxxxxxx,dc=com
objectClass: groupofnames
cn: it
member: uid=testuser1,ou=People,dc=xxxxxxxxx,dc=com
member: uid=testuser2,ou=People,dc=xxxxxxxxx,dc=com
EOF
```

```
sudo ldapadd -xcWD cn=admin,dc=xxxxxxxxx,dc=com -f ./ldap.group.create.ldif
```

Remarque : Même si l'attribut memberOf n'est pas explicitement défini lors de la création d'utilisateurs ou de groupes, le système génère et gère automatiquement cette référence. Une fois que l'utilisateur est associé à un groupe, l'attribut memberOf reflète automatiquement ces appartenances, ce qui garantit que l'annuaire reste synchronisé avec la structure d'accès actuelle.

Étape 6 : Teste la connexion LDAP locale

Vérifiez la connexion de l'utilisateur au serveur LDAP à l'aide de la commande spécifiée (remplacez les paramètres de connexion en fonction de votre environnement) :

```
sudo ldapsearch -x -LLL -b uid=testuser1,ou=People,dc=xxxxxxxxx,dc=com memberOf
```

```
test@test:~$ sudo ldapsearch -x -LLL -b uid=testuser1,ou=People,dc=xxxxxxxxx,dc=com  memberOf
dn: uid=testuser1,ou=People, dc=xxxxxxxxx,dc=com
memberOf: cn=it,ou=Groups, dc=xxxxxxxxx,dc=com

test@test:~$
```

Paramètres de configuration sur CIMC

Connectez-vous à CIMC.

Dans le volet de navigation, sélectionnez Admin, User Management et LDAP.

Renseignez les paramètres de configuration LDAP comme indiqué ci-dessous :

- Enable LDAP : coché
- DN de base : dc=xxxxxxx, dc=com

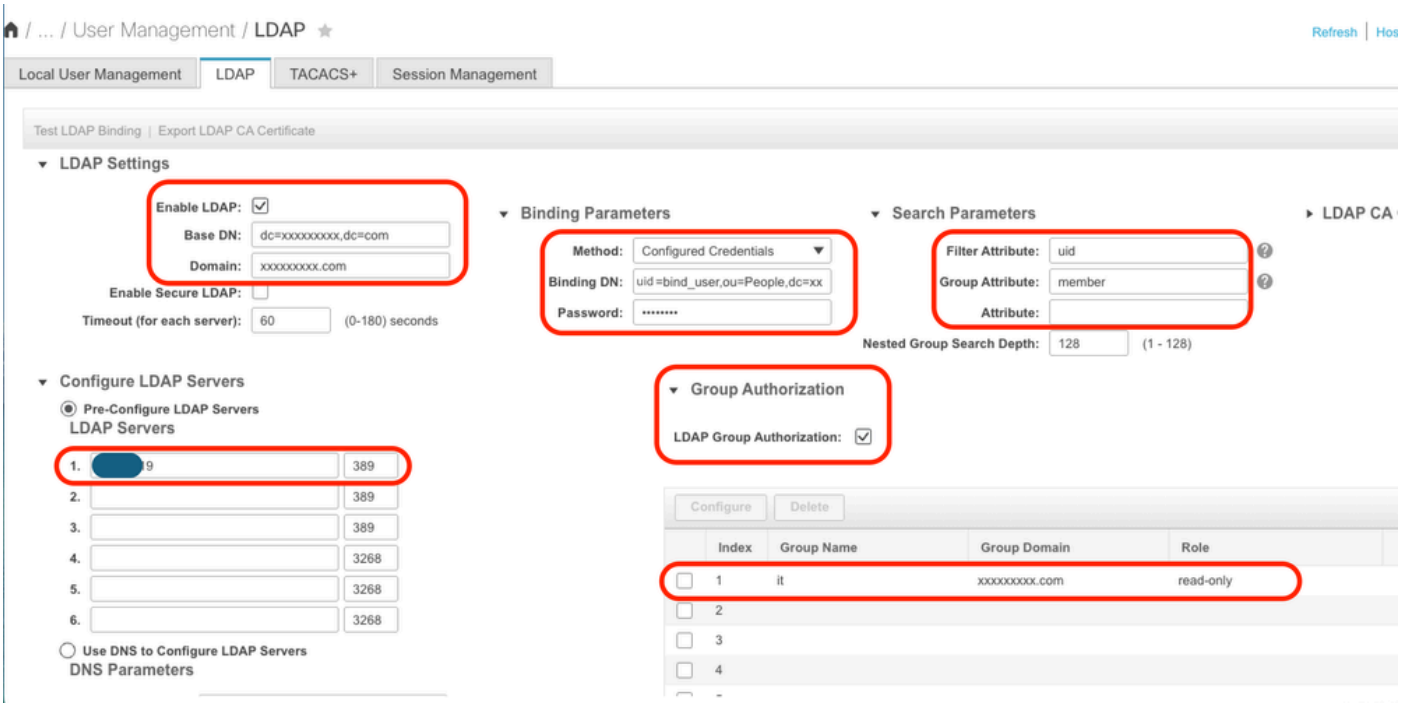
- Domaine : xxxxxxxxx.com

- Serveurs LDAP : <ldap_server_IP ou FQDN> X.X.X.19

- Paramètres de liaison : Peut être « Identifiants de connexion » ou « Identifiants configurés »
  - Lors de l'utilisation des informations d'identification configurées, ajoutez le DN bind_user exactement comme configuré sur le serveur LDAP :
  - Par exemple : "cn=bind_user, ou=People, dc=xxxxxxx, dc=com" ou "uid=bind_user, ou=People, dc=xxxxxxx, dc=com"

- Paramètres de recherche :
  - Attribut de filtre : « cn » ou « uid »
  - Attribut de groupe : adhérent

- Autorisation de groupe LDAP - Coché
  - Nom du groupe : il
  - Domaine du groupe : xxxxxxxxx.com
  - Rôle : lecture seule (tout rôle préféré)



Enregistrez la configuration et testez la connexion utilisateur LDAP.

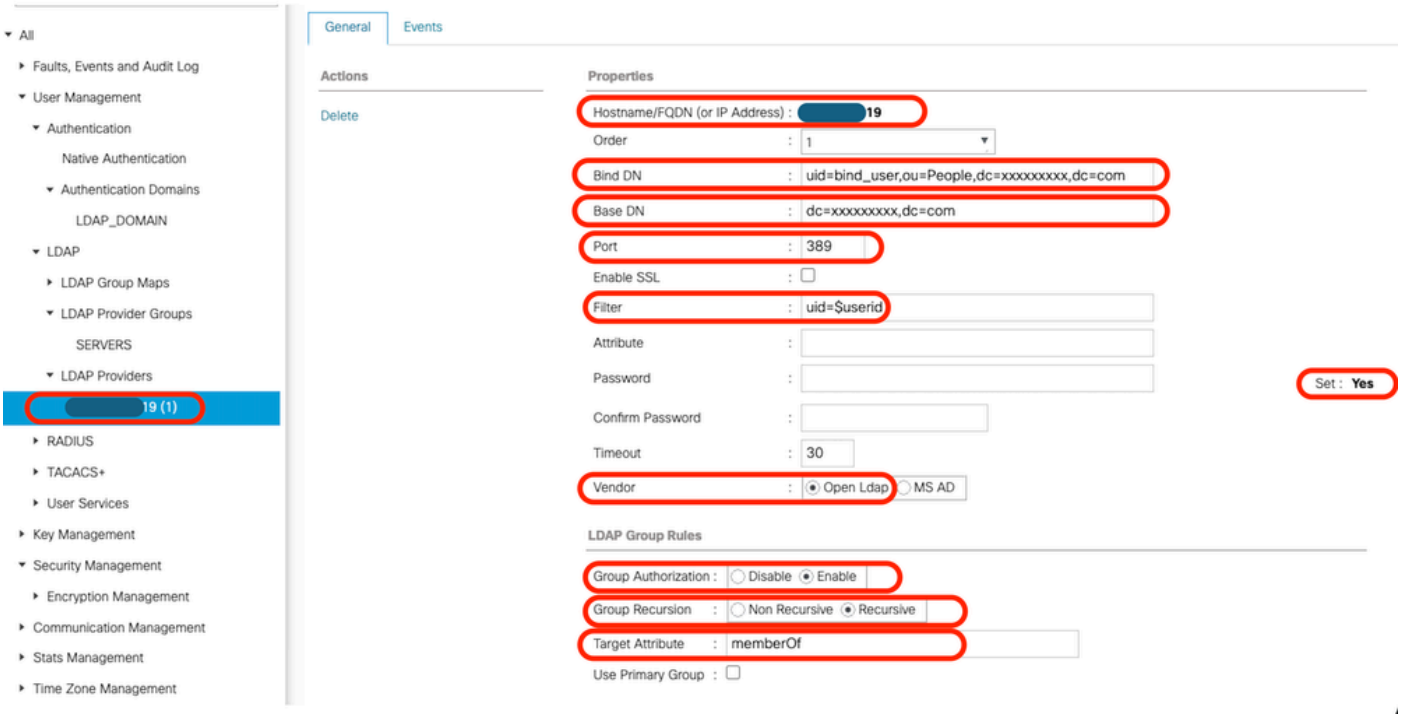
Paramètres de configuration sur UCS Manager

Connectez-vous à UCS Manager.

Dans le volet de navigation, sélectionnez Admin, User Management et LDAP.

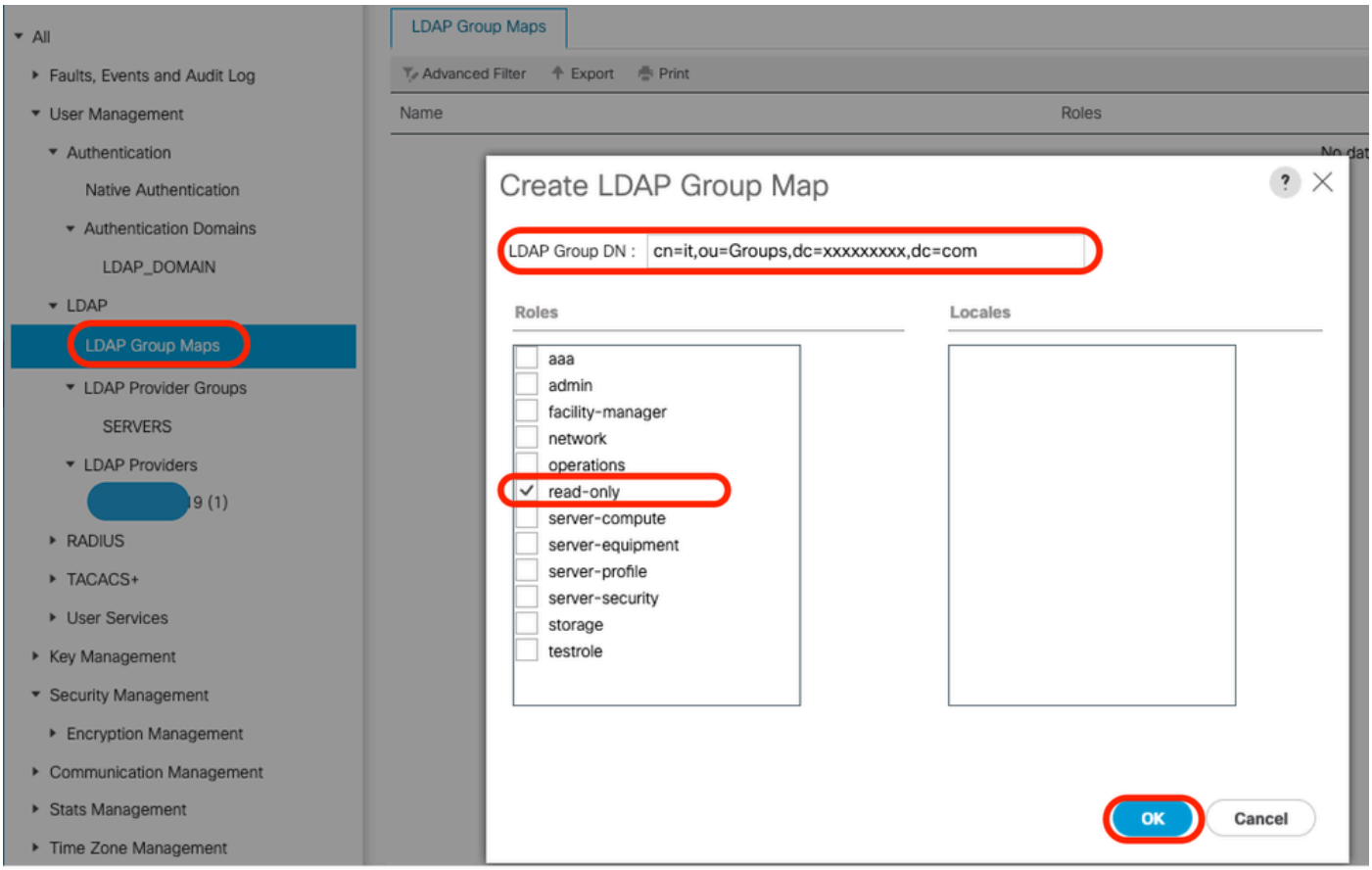
Renseignez les paramètres de configuration LDAP comme indiqué ci-dessous :

- Fournisseurs LDAP :
  - Nom d'hôte : <nom de domaine complet ou adresse IP du serveur LDAP>
  - DN de liaison : uid=bind_user,ou=Personnes,dc=xxxxxxxxx,dc=com
  - DN de base : dc=xxxxxxx, dc=com
  - Port : 389
  - Activer SSL : Désactivé
  - Filtre : uid=$userid
  - Autorisation de groupe : Activée
  - Récursivité du groupe : Récursif
  - Attribut cible : membreDe
- Mappages de groupes LDAP :
  - DN du groupe LDAP : cn=it, ou=Groups, dc=xxxxxxx, dc=com



Ajoutez le fournisseur LDAP configuré à un groupe de fournisseurs LDAP. Pour cette démonstration, le groupe de fournisseurs LDAP « SERVERS » est utilisé.

Configurez les mappages de groupe LDAP en ajoutant un « DN de groupe LDAP », récupéré à partir du serveur LDAP.



Configurez un domaine d'authentification LDAP (LDAP_DOMAIN) dans « Tous >> Gestion des utilisateurs >> Authentification >> Domaines d'authentification » faisant référence aux groupes de fournisseurs LDAP (SERVEURS) et testez la connexion des utilisateurs LDAP.

Examinons maintenant la configuration de la même (avec superposition) dans une distribution Linux distincte (CentOS 10)

Scénario 2 : CentOS Stream 10 - Fedora

Les procédures de configuration du protocole LDAP (Lightweight Directory Access Protocol) varient en fonction de la version du système d'exploitation sous-jacent. Cette section se concentre sur la mise en oeuvre de LDAP sur CentOS Stream 10.

Alors que de nombreuses distributions Linux utilisent OpenLDAP, CentOS Stream 10 et les systèmes Fedora actuels utilisent le serveur d'annuaire 389 (389 DS) comme fournisseur LDAP par défaut.

Remarque : Bien que 389 DS soit considéré comme le successeur d'OpenLDAP dans les écosystèmes CentOS et Red Hat, les deux solutions ne sont pas directement interchangeables. Leurs structures de répertoires, fichiers de configuration et environnements opérationnels respectifs diffèrent considérablement.

Ce guide présente les étapes nécessaires à la configuration réussie de LDAP à l'aide de 389 DS dans un environnement CentOS Stream 10.

Option 1: Configurer LDAP à l'aide du serveur d'annuaire 389 sur CentOS Stream 10

Étape 1: Configuration initiale

Répétez l'étape 1 dans le scénario 1, option 1.

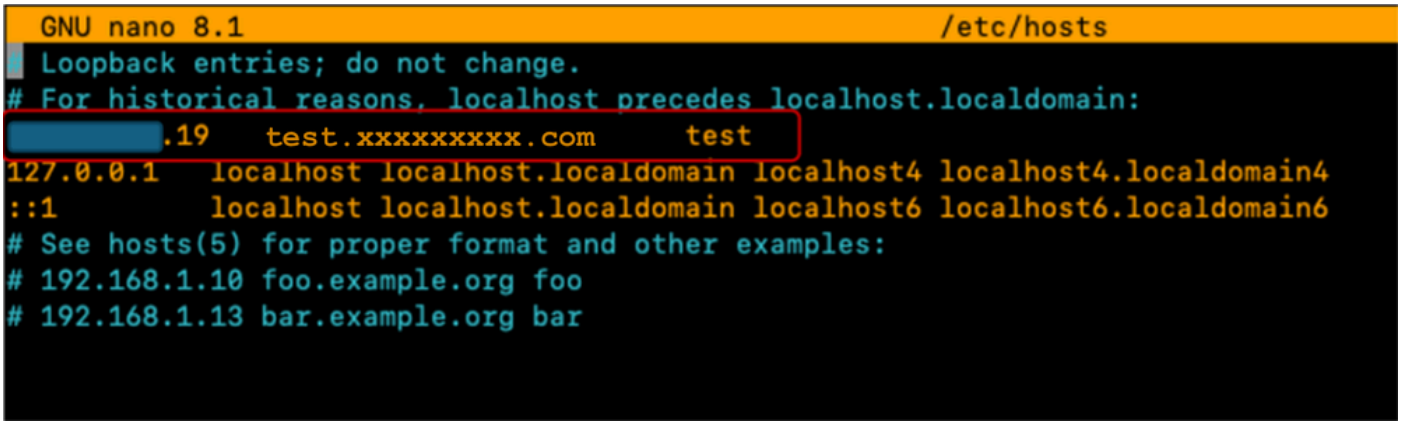
Les systèmes CentOS n'utilisent pas la suite de gestion des packages APT. Pour effectuer les installations logicielles nécessaires sur CentOS Stream 10, utilisez les gestionnaires de packages dnf (Dandified YUM) ou yum

```
sudo yum update
sudo yum install net-tools
```

Vérifiez l'adresse IP du serveur à l'aide de la commande « ifconfig ».

Ajoutez l'adresse IP du serveur au fichier « /etc/hosts », ainsi que le nom de domaine complet du serveur (par exemple : test.xxxxxxx.com utilisé dans ces travaux pratiques) et le nom d'hôte (par exemple : test) au format spécifié ci-dessous :

```
sudo nano /etc/hosts
```



Mettez à jour le fichier « /etc/hostname » en remplaçant son contenu par le nom d'hôte (test).

```
sudo nano /etc/hostname
```

Un redémarrage du serveur est nécessaire pour que ces modifications prennent effet.

```
sudo reboot
```

Étape 2: Installer la réparation EPEL et le package 389 Server

Installer et mettre à jour le référentiel EPEL.

Installez le package Directory Server 389.

```
sudo dnf install -y epel-release
sudo dnf update -y epel-release
sudo dnf install 389-ds-base
```

Créez un fichier de modèle d'annuaire contenant les paramètres de serveur LDAP souhaités :

```
sudo dscreate create-template ldapconfig.conf
```

Vérifiez le contenu du fichier modèle créé (ldapconfig.conf)

```
sudo cat ldapconfig.conf
```

Modifiez le fichier de modèle ldapconfig.conf.

```
sudo nano ldapconfig.conf
```

Insérez les entrées de configuration spécifiées dans le fichier et enregistrez vos modifications.

Remarque : différentes modifications peuvent être requises en fonction des besoins ou exigences spécifiques de chaque environnement.

Cet exemple présente les configurations de ligne de base de cette démonstration.

```
[general]
config_version = 2
selinux    = True

[slapd]
```

```
instance_name = localhost
root_dn = cn=admin
root_password = cisco123

[backend-userroot]
sample_entries = yes
suffix = dc=xxxxxxxxx,dc=com
```

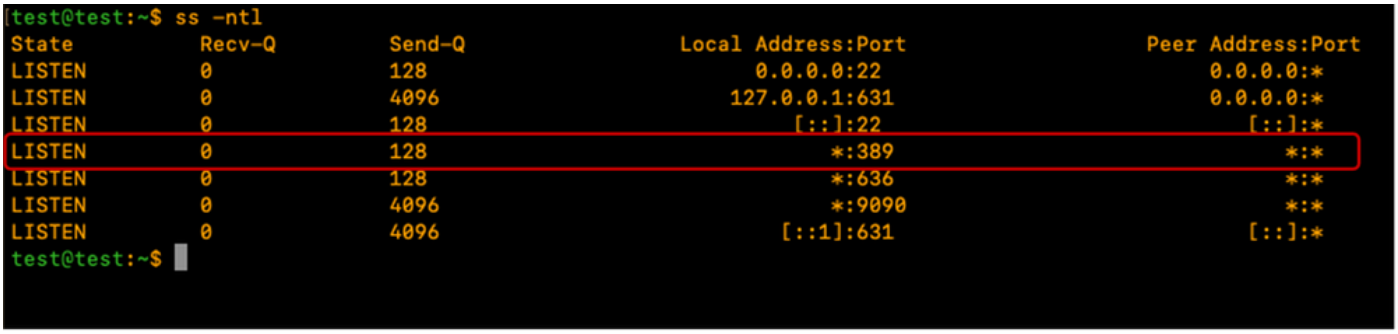
Le fichier modèle définit les paramètres de configuration pour l'instance de répertoire "localhost". Cela inclut la définition de l'utilisateur administratif (« admin »), du mot de passe associé et du contexte de domaine (« xxxxxxxxx.com »).

Créez l'instance d'annuaire "localhost" à l'aide du modèle modifié précédemment. La commande spécifiée crée et démarre le serveur d'annuaire LDAP :

```
sudo dscreate -v from-file ldapconfig.conf
```

Vérifiez que le service LDAP est en cours d'exécution sur le serveur

```
ss -ntl
```



Ajustez le pare-feu CentOS pour autoriser le ou les ports requis pour LDAP (389 et/ou 636).

Pour cette démonstration, le pare-feu est désactivé.

```
sudo systemctl stop firewalld
```

Vérifiez que LDAP fonctionne localement sur le serveur LDAP en exécutant la commande spécifiée et assurez-vous qu'il renvoie la sortie LDAP comme indiqué :

```
sudo ldapsearch -x ldap://localhost -b "dc=xxxxxxxxx,dc=com"
```

```
test@test:~$ sudo ldapsearch -x ldap://localhost -b "dc=xxxxxxxxx,dc=com"
# extended LDIF
#
# LDAPv3
# base <dc=xxxxxxxxx,dc=com> with scope subtree
# filter: (objectclass=*)
# requesting: ldap://localhost
#

# xxxxxxxxx,com
dn: dc=xxxxxxxxx,dc=com

# groups, xxxxxxxxx,com
dn: ou=groups,dc=xxxxxxxxx,dc=com

# people, xxxxxxxxx,com
dn: ou=people,dc=xxxxxxxxx,dc=com

# permissions, xxxxxxxxx,com
dn: ou=permissions,dc=xxxxxxxxx,dc=com

# services, xxxxxxxxx,com
dn: ou=services,dc=xxxxxxxxx,dc=com

# demo_user, people, xxxxxxxxx,com
dn: uid=demo_user,ou=people,dc=xxxxxxxxx,dc=com

# demo_group, Groups, xxxxxxxxx,com
dn: cn=demo_group,ou=Groups,dc=xxxxxxxxx,dc=com

# search result
search: 2
result: 0 Success

# numResponses: 8
# numEntries: 7
```

Le résultat contient des comptes de démonstration créés par le serveur 389DS. Le serveur LDAP a automatiquement créé des unités organisationnelles par défaut.

L'unité d'organisation des personnes pour les utilisateurs et les groupes pour les groupes. Des unités organisationnelles supplémentaires peuvent être créées en fonction des besoins.

Pour cette démonstration, les unités organisationnelles créées par défaut/automatiquement sont utilisées.

Consultez la documentation officielle 389DS pour plus de détails sur l'utilisation étendue du package 389DS :

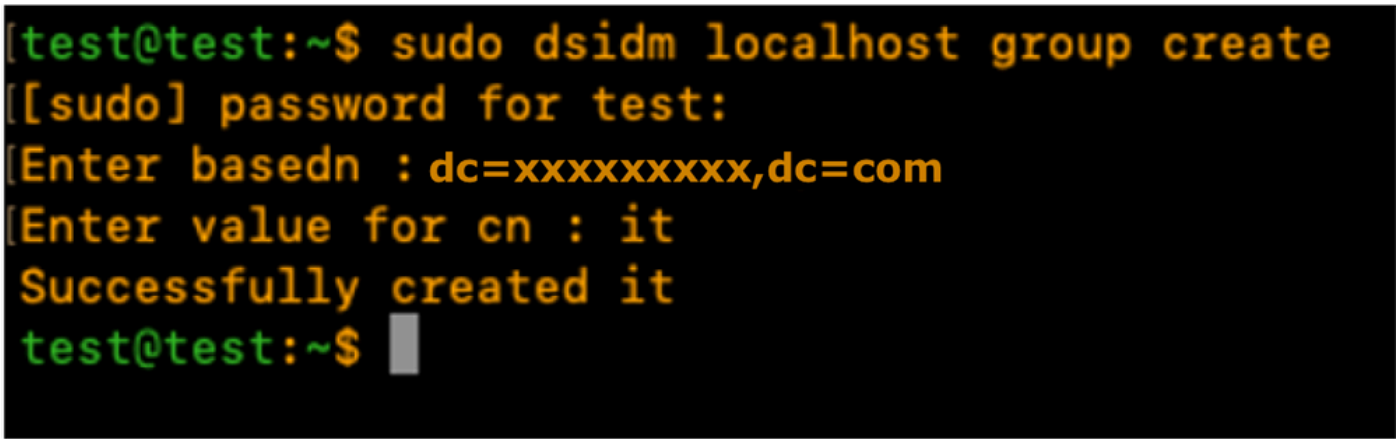
Étape 3: Créer des groupes et des utilisateurs LDAP

Créez un groupe (it) à l'aide de la commande spécifiée : sudo dsidm <nom_instance> group create.

Pour cette démonstration, le nom de l'instance est « localhost ».

```
sudo dsidm localhost group create
```

Entrez l'invite du terminal pour renseigner les détails du groupe comme indiqué :



Créez un compte utilisateur testuser1 à l'aide de la commande :

```
sudo dsidm localhost user create
```

Entrez l'invite du terminal pour renseigner les détails de l'utilisateur comme indiqué

```
test@test:~$ sudo dsidm localhost user create
Enter basedn : dc=xxxxxxxxx,dc=com
Enter value for uid : testuser1
Enter value for cn : testuser1
Enter value for displayName : Test User1
Enter value for uidNumber : 10000
Enter value for gidNumber : 10000
Enter value for homeDirectory : /home/testuser1
Successfully created testuser1
```

Créez un mot de passe pour testuser1 à l'aide de la commande spécifiée et entrez l'invite CLI :

```
sudo dsidm localhost account reset_password uid=testuser1,ou=people,dc=xxxxxxxxx,dc=com
```

```
test@test:~$ sudo dsidm localhost account reset_password uid=testuser1,ou=people, dc=xxxxxxxxx,dc=com
Enter basedn : dc=xxxxxxxxx,dc=com
Enter new password for uid=testuser1,ou=people, dc=xxxxxxxxx,dc=com :
CONFIRM - Enter new password for uid=testuser1,ou=people, dc=xxxxxxxxx,dc=com :
reset password for uid=testuser1,ou=people,dc=xxxxxxxxx,dc=com
test@test:~$
```

Ajoutez l'utilisateur à un groupe à l'aide de la commande spécifiée : "sudo dsidm <instance_répertoire> group add_member <group_cn> <user_dn>"

```
sudo dsidm localhost group add_member it uid=testuser1,ou=people,dc=xxxxxxxxx,dc=com
```

Répétez les étapes de création de l'utilisateur pour créer testuser2 et bind_user.

Remarque : assurez-vous que chaque utilisateur est explicitement ajouté à ses groupes.

L'omission de cette étape peut entraîner des échecs d'accès ou d'autorisation restreints.

Le compte bind_user n'a pas besoin d'être membre d'un groupe spécifique, car il peut être configuré en tant que compte autonome, offrant ainsi la flexibilité nécessaire pour gérer l'accès administratif et de niveau de service dans l'environnement d'annuaire.

Redémarrez l'instance de répertoire :

```
sudo dsctl localhost restart
```

Étape 4: Installer le membre de superposition

Installez le plug-in « memberOf » et redémarrez l'instance de répertoire :

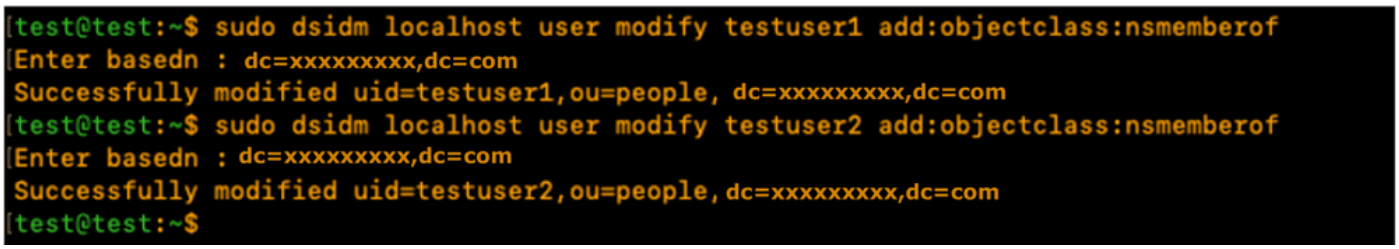
```
sudo dsconf localhost plugin memberof status
sudo dsconf localhost plugin memberof enable
sudo dsctl localhost restart
```

Configurez le plug-in « memberOf » à l'aide de la commande spécifiée : "sudo dsconf <instance_répertoire> plugin memberof set —scope <base_dn>"

```
sudo dsconf localhost plugin memberof set --scope dc=xxxxxxxxx,dc=com
```

Marquer les utilisateurs comme cibles « memberOf » valides à l'aide de la commande spécifiée : "sudo dsidm <instance_répertoire> user modify <uid> add:objectclass:nsmemberof"

```
sudo dsidm localhost user modify testuser1 add:objectclass:nsmemberof
sudo dsidm localhost user modify testuser2 add:objectclass:nsmemberof
```



Générez une correction « memberOf » pour le DN de base : "sudo dsconf <instance_répertoire> membre du plug-in de fixup <base_dn>"

```
sudo dsconf localhost plugin memberof fixup dc=xxxxxxxxx,dc=com
```

```
test@test:~$ sudo dsconf localhost plugin memberof fixup dc=xxxxxxxxx,dc=com
Adding fixup task entry...
Successfully added task entry "cn=memberOf_fixup_2025-05-13T14:54:11.926390,cn=memberOf task,cn=tasks,cn=config". Th
is task is running in the background. To track its progress you can use the "fixup-status" command.
test@test:~$
```

Vérifiez la configuration utilisateur :

```
sudo dsidm localhost user get testuser1
sudo dsidm localhost user get testuser2
```

```
test@test:~$ sudo dsidm localhost user get testuser1
Enter basedn : dc=xxxxxxxxx,dc=com
dn: uid=testuser1,ou=people, dc=xxxxxxxxx,dc=com
cn: testuser1
displayName: Test User1
gidNumber: 10000
homeDirectory: /home/testuser1
memberOf: cn=it,ou=Groups,dc=xxxxxxxxx,dc=com
objectClass: top
objectClass: nsPerson
objectClass: nsAccount
objectClass: nsOrgPerson
objectClass: posixAccount
objectClass: nsmemberof
uid: testuser1
uidNumber: 10000
userPassword: {PBKDF2-SHA512}100000$uJ+bQ9OAQ4L2uynoUBt+QeVlW0tj0KZJ$B/1yULxaE3F3wrE+Qo/+KPnynHgN5vWUzfM9MxpO1qeHq9gXs863u
rkAZakFSmLrZVduqN/TRNZE4W/ZbRmECw==


test@test:~$ sudo dsidm localhost user get testuser2
Enter basedn : dc=xxxxxxxxx,dc=com
dn: uid=testuser2,ou=people, dc=xxxxxxxxx,dc=com
cn: testuser2
displayName: Test User2
gidNumber: 10000
homeDirectory: /home/testuser2
memberOf: cn=it,ou=Groups,dc=xxxxxxxxx,dc=com
objectClass: top
objectClass: nsPerson
objectClass: nsAccount
objectClass: nsOrgPerson
objectClass: posixAccount
objectClass: nsmemberof
uid: testuser2
uidNumber: 10001
userPassword: {PBKDF2-SHA512}100000$efAcaYcRRHIU6OAIMeHxvHPAAhWX7yWc$tzeynBPPX6qXBXWpGe9nyq1sHetEsCq7ngwt+4lhSWY2syZ9tvcSd
ZCXZbo8RK8OhBSCoqTYpi1N5oOBqU6A1w==


test@test:~$
```

Le serveur LDAP 389DS est configuré avec le plug-in memberOf pour prendre en charge l'attribut memberOf.

Paramètres de configuration sur CIMC

Connectez-vous à CIMC.

Dans le volet de navigation, sélectionnez Admin, User Management et LDAP.

Renseignez les paramètres de configuration LDAP comme indiqué ci-dessous :

- Enable LDAP : coché
- DN de base : dc=xxxxxxx, dc=com

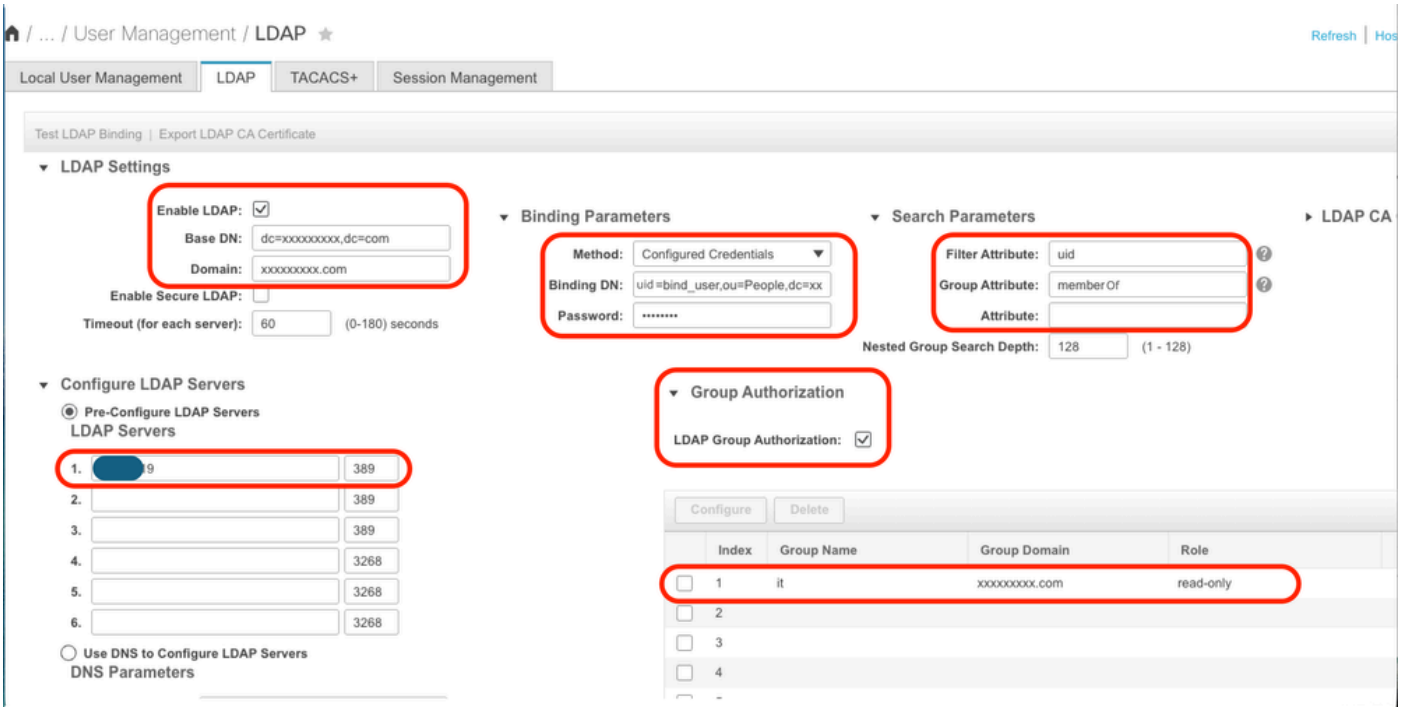
- Domaine : xxxxxxxxx.com

- Serveurs LDAP : <ldap_server_IP ou FQDN> X.X.X.19

- Paramètres de liaison : Peut être « Identifiants de connexion » ou « Identifiants configurés »
  - Lors de l'utilisation des informations d'identification configurées, ajoutez le DN bind_user exactement comme configuré sur le serveur LDAP :
    - Par exemple : "cn=bind_user, ou=People, dc=xxxxxxx, dc=com" ou "uid=bind_user, ou=People, dc=xxxxxxx, dc=com"

- Paramètres de recherche :
  - Attribut de filtre : « cn » ou « uid »
  - Attribut de groupe : membreDe

- Autorisation de groupe LDAP - Coché
  - Nom du groupe : il
  - Domaine du groupe : xxxxxxxxx.com
  - Rôle : lecture seule (tout rôle préféré)



Enregistrez la configuration et testez la connexion utilisateur LDAP.

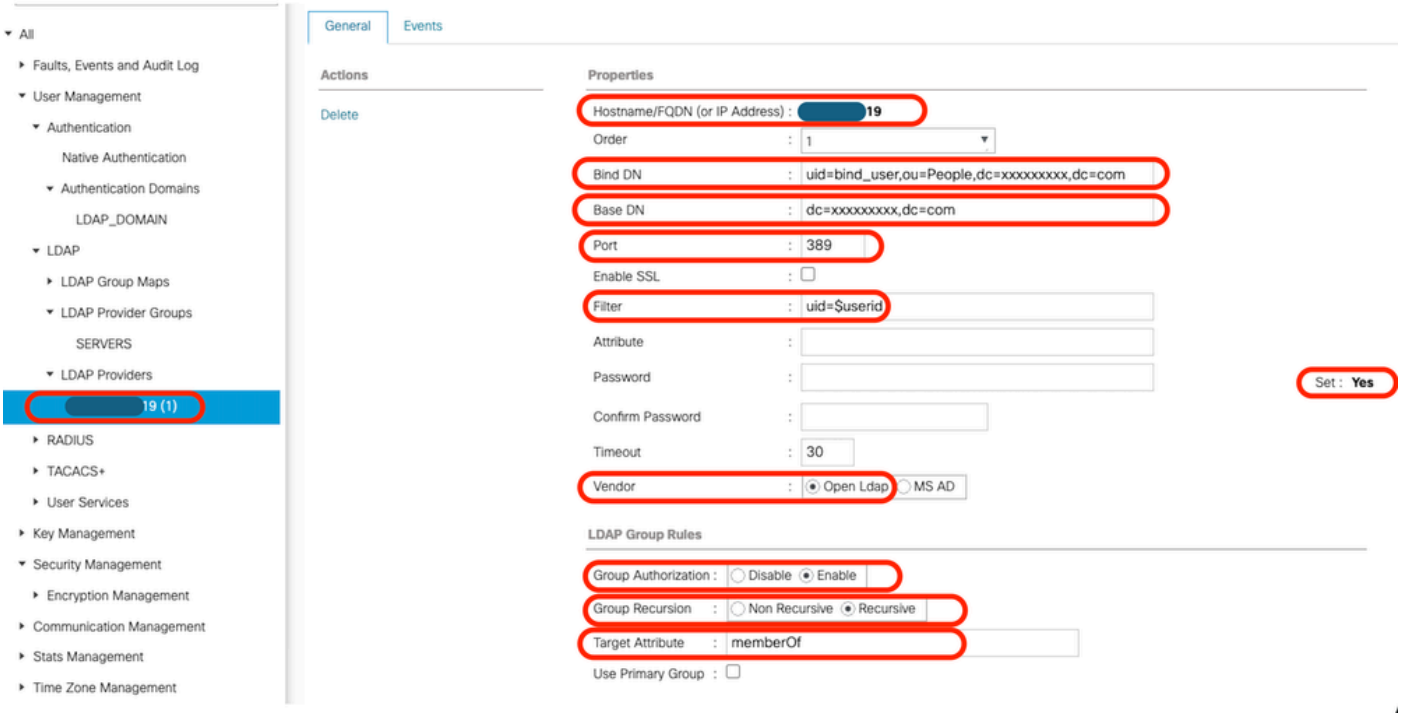
Paramètres de configuration sur UCS Manager

Connectez-vous à UCS Manager.

Dans le volet de navigation, sélectionnez Admin, User Management et LDAP.

Renseignez les paramètres de configuration LDAP comme indiqué ci-dessous :

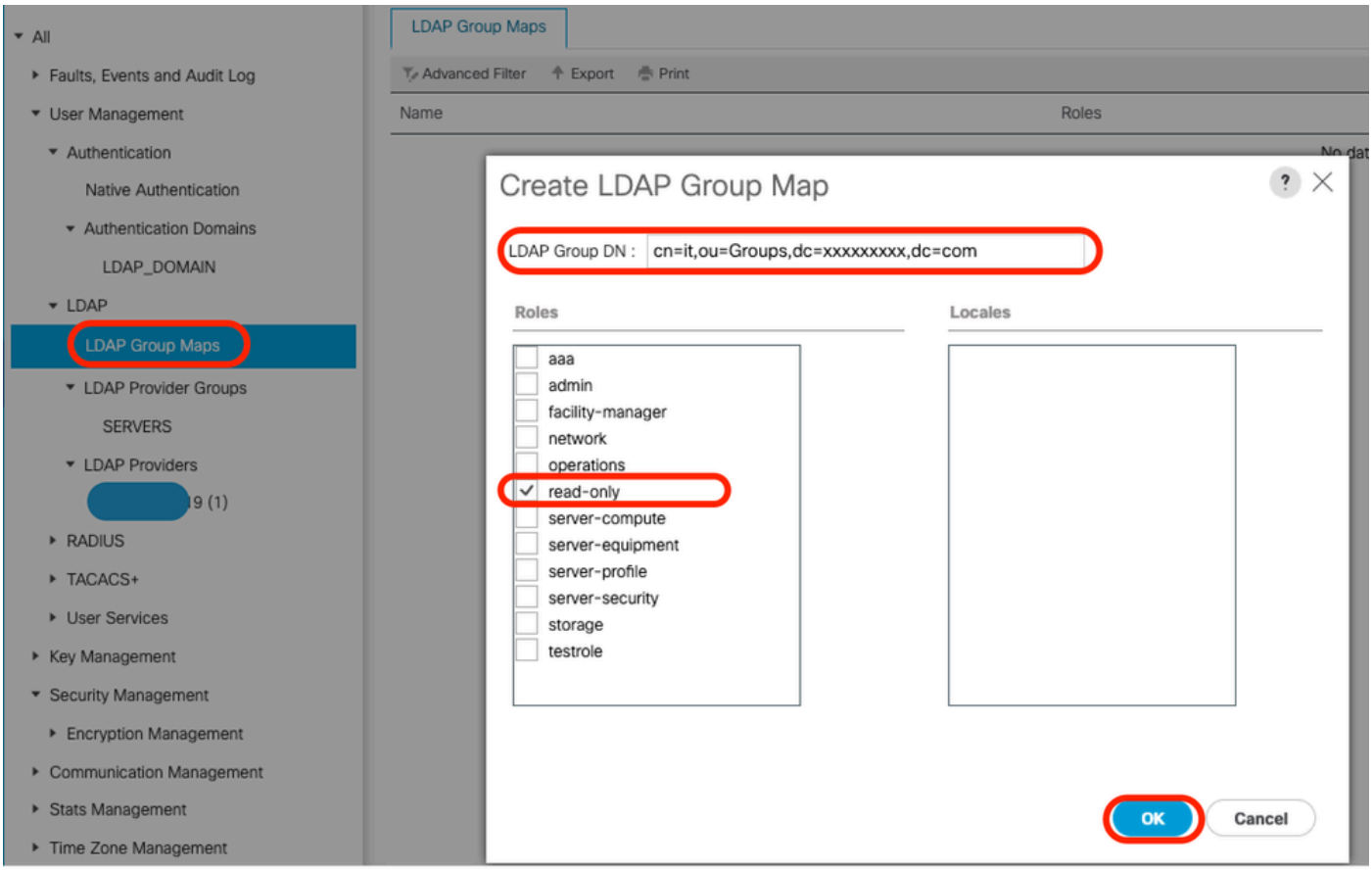
- Fournisseurs LDAP :
  - Nom d'hôte : <nom de domaine complet ou adresse IP du serveur LDAP>
  - DN de liaison : uid=bind_user,ou=people,dc=xxxxxxxxx,dc=com
  - DN de base : dc=xxxxxxx, dc=com
  - Port : 389
  - Activer SSL : Désactivé
  - Filtre : uid=$userid
  - Autorisation de groupe : Activée
  - Récursivité du groupe : Récursif
  - Attribut cible : membreDe
- Mappages de groupes LDAP :
  - DN du groupe LDAP : cn=it, ou=Groups, dc=xxxxxxx, dc=com



Ajoutez le fournisseur LDAP configuré à un groupe de fournisseurs LDAP. Pour cette

démonstration, le groupe de fournisseurs LDAP « SERVERS » est utilisé.

Configurez les mappages de groupe LDAP en ajoutant un « DN de groupe LDAP », récupéré à partir du serveur LDAP.



Configurez un domaine d'authentification LDAP (LDAP_DOMAIN) dans « Tous >> Gestion des utilisateurs >> Authentification >> Domaines d'authentification » faisant référence aux groupes de fournisseurs LDAP et testez la connexion des utilisateurs LDAP.

Conclusion

Bien que ce guide couvre des scénarios de déploiement essentiels, une exploration plus approfondie des fonctionnalités LDAP peut considérablement améliorer les performances et la sécurité des annuaires.

Pour plus d'informations, de meilleures pratiques et de détails sur la configuration avancée, reportez-vous aux ressources spécifiées :

- Documentation officielle OpenLDAP

- Gestionnaire de compte LDAP - Manuel
- 389 Documentation du serveur d'annuaire
- Configurer LDAP sur UCS Manager
- Configuration de Secure LDAP sur les serveurs 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.