تكوين LDAP على UCS Manager & amp؛ CIMC باستخدام خوادم Linux OpenLDAP و 389-DS

المحتويات

المقدمة

يصف هذا المستند مجموعة متنوعة من الخيارات لتكوين LDAP كطريقة مصادقة ل UCS Manager و CIMC باستخدام OpenLDAP المستند إلى Linux و 389 خادم دليل.

معلومات أساسية

هذه الوثيقة تتجاوز المعالجة الشاملة لتكوينات خادم OpenLDAP، انظر للتغييرات الكبيرة في تكوينات خادم LDAP وتخطيطات السمات. والغرض من هذه الوثيقة هو توفير إرشادات واضحة وبسيطة، يتناول هذا المستند التكوينات القياسية لـ LDAP. تكوين LDAP الآمن (LDAPs) غير مغطى في هذا المستند.

المتطلبات الأساسية:

يوصى بشدة بمعرفة هذه الموضوعات:

- UCS B Series
- سلسلة UCS C
- إدارة خادم ليونكس

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج والمكونات المادية التالية:

- إصدار البرنامج الثابت UCS Manager: 4.3(2c)
- طراز اتصال البنية البيني: UCS-FI-6454
- نموذج الخادم المستقل UCS C Series: UCSC-C240-M5
- إصدار البرنامج الثابت المستقل UCS C Series: 4.3(2.250045)
- أوبونتو 20.04
- CentOS Stream 10

الإعدادات المستخدمة لهذا العرض التوضيحي:

- اسم مضيف خادم LDAP: إختبار
- مجال الخادم: xxxxxxxxx.com
- خادم FQDN: test.xxxxxxxxx.com
- عنوان IP لخادم Linux (نظام التشغيل Ubuntu و CentOS): X.X.X.19

- OpenLDAP: testuser1، testuser2 (ومدخدم) مستخدم
- OpenLDAP: تقنية معلومات (مجموعات) مجموعة
- OpenLDAP: bind_user حساب مستخدم ربط

ملاحظة: تم إستخدام محرر نصوص Linux Nano في هذا المختبر.

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. إذا كانت شبكتك قيد التشغيل، فتأكد من فهمك للتأثير المحتمل لأي أمر.

السيناريو 1: أوبونتو - دبيان

يمكن تنفيذ تكوين خادم LDAP باستخدام واجهة رسومية، مثل مدير حساب LDAP، أو أدوات سطر الأوامر، وقد يختلف هذا السيناريو. ويفحص الإداري ومستوى التحكم المطلوب. التكوين باستخدام برنامج OpenLDAP القائم على Linux، بدءا بالنشر القائم على واجهة المستخدم الرسومية (GUI) والانتقال بعد ذلك إلى أدوات مساعدة سطر الأوامر لاستكشاف الإمكانات المتقدمة، بما في ذلك المكونات الإضافية (المستخدمة بشكل شائع في عمليات التكامل مع مدير Cisco UCS).

الخيار 1: تكوين OpenLDAP باستخدام مدير حساب Ubuntu LDAP (LAM)

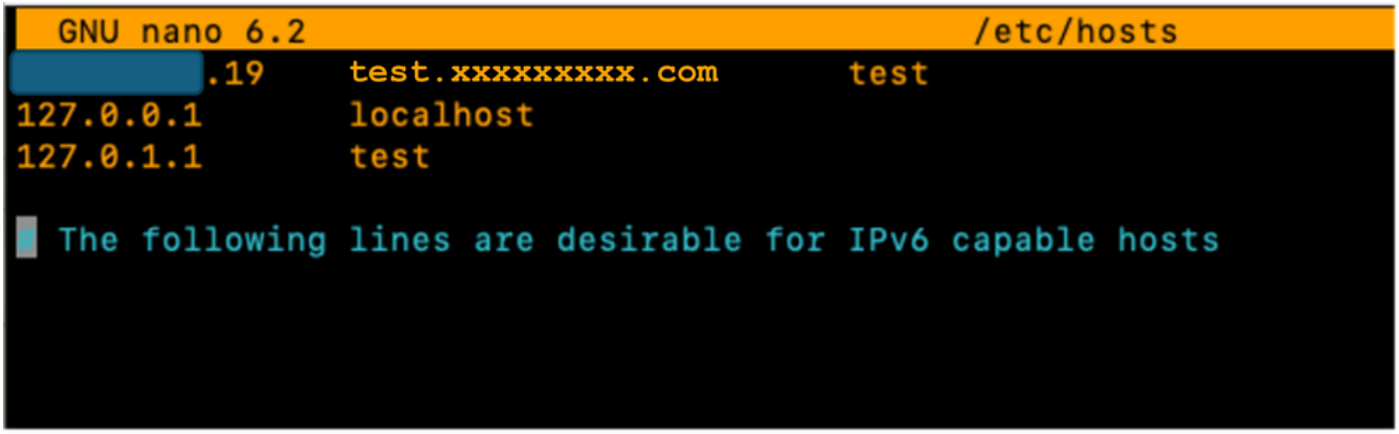
الخطوة 1: التهيئة الأولية لاسم مضيف خادم لينوكس وأدوات الشبكة.

قم بتحديث نظام التشغيل وتثبيت حزمة أدوات الشبكة للوصول إلى أدوات مثل ifconfig و netstat وما إلى ذلك:

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

أستخدم الأمر "ifconfig" للتحقق من عنوان IP الخاص بالخادم، ثم قم بإضافته إلى الملف "/etc/hosts" مع اسم مجال الخادم (على سبيل المثال: "test.xxxxxxxx.com") المستخدم في هذا المختبر) و hostname (على سبيل المثال: "إختبار") بالتنسيق المحدد.

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



بالإضافة إلى ذلك، قم بتحديث الملف "/etc/hostname" عن طريق إستبدال محتوياته باسم المضيف (إختبار).

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

يلزم إعادة تشغيل الخادم حتى تصبح هذه التغييرات نافذة المفعول.

```
sudo reboot
```

الخطوة 2: تثبيت SLAPD و Apache و PHP وتبعياتها

بعد ذلك، قم بتثبيت أباتشي، php وتبعياتهم. يتم إستخدام هذه العناصر لتمكين التفاعل مع واجهة المستخدم الرسومية (GUI) عبر صفحة ويب :

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

تثبيت حزمة خادم LDAP المفتوحة "slapd" وتوابعها (ldap-utils)

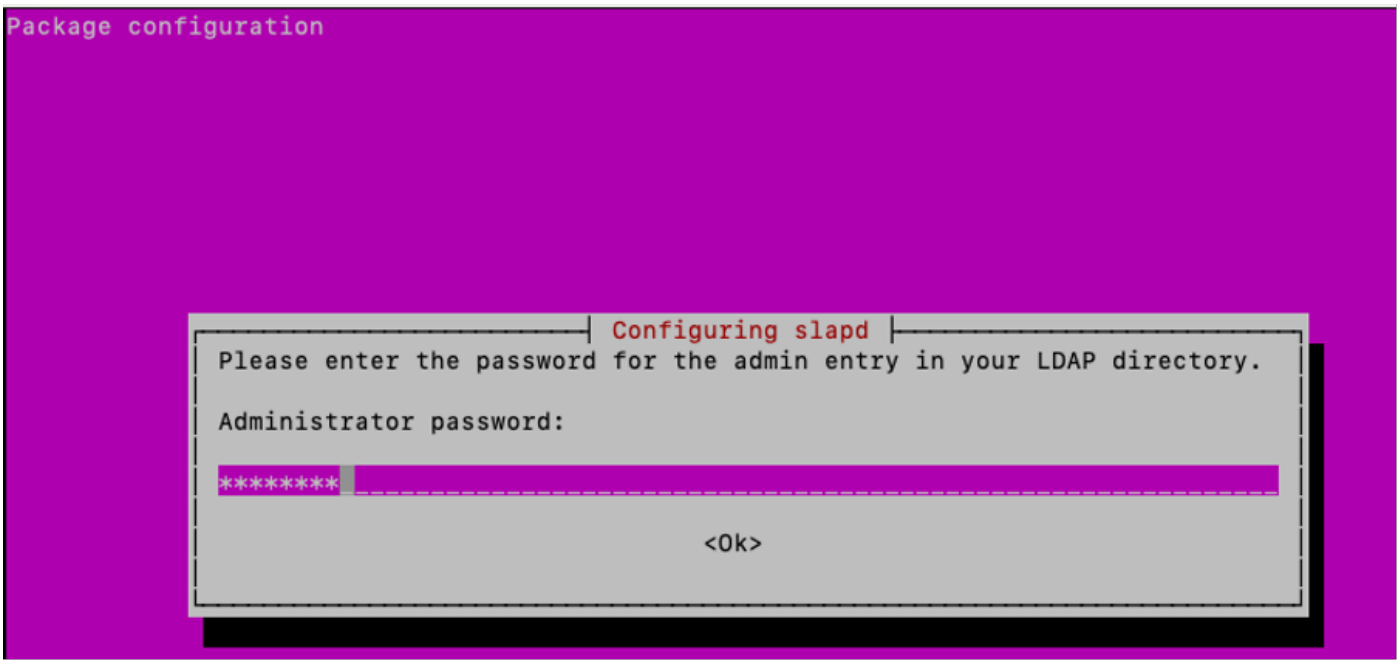
```
sudo apt install slapd ldap-utils -y
```

أثناء تثبيت SLAPD، في واجهة المستخدم الرسومية (GUI) التي تم تقديمها - أدخل تكوين حزمة SLAPD المطلوبة الإضافية.

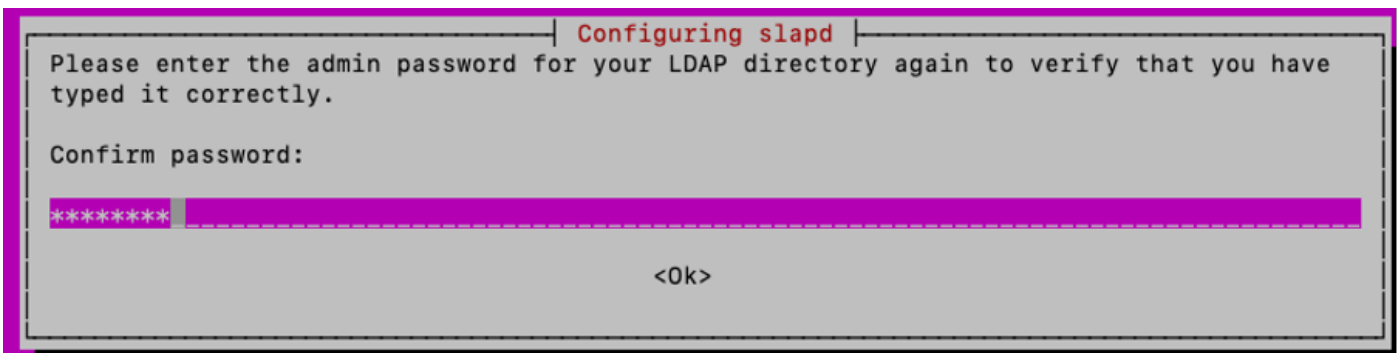
ملاحظة: يتطلب حل كلمة المرور إعادة تثبيت خادم LDAP.

يعد "administrator" (admin) في هذا السياق حسابا يتم إستخدامه لإدارة خدمة OpenLDAP والوحدات النمطية والتكوينات.

أضف كلمة مرور "administrator" لحزمة LDAP واضغط على مفتاح الإدخال Enter في لوحة المفاتيح لتحديد "ok".



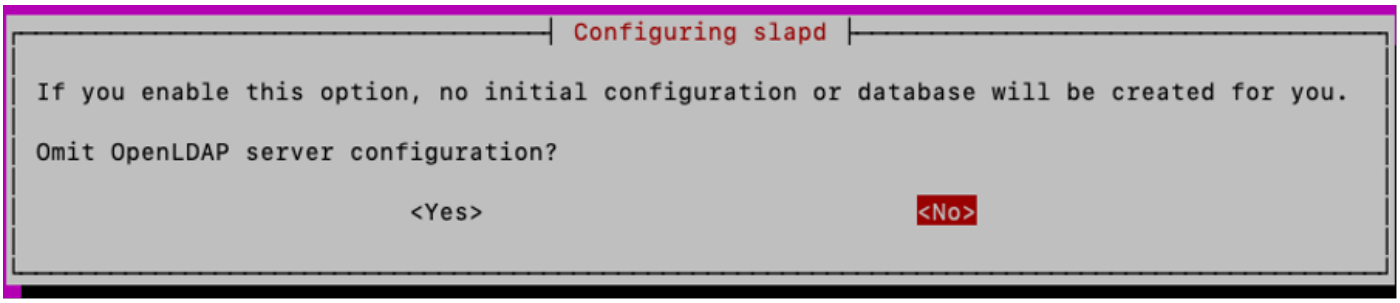
تأكيد كلمة المرور:



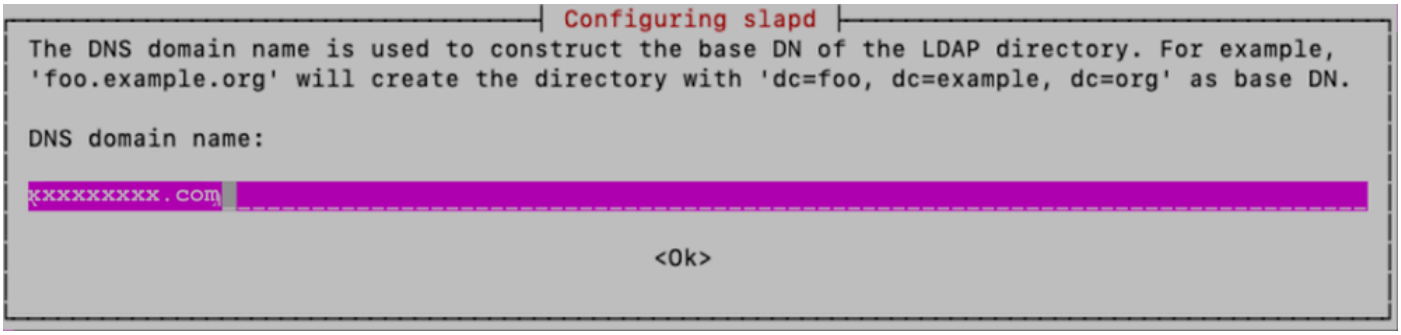
بمجرد اكتمال التثبيت، يمكنك إستخدام الأمر المحدد لإعادة تكوين حزمة SLAPD، وإضافة معلومات المجال:

```
sudo dpkg-reconfigure slapd
```

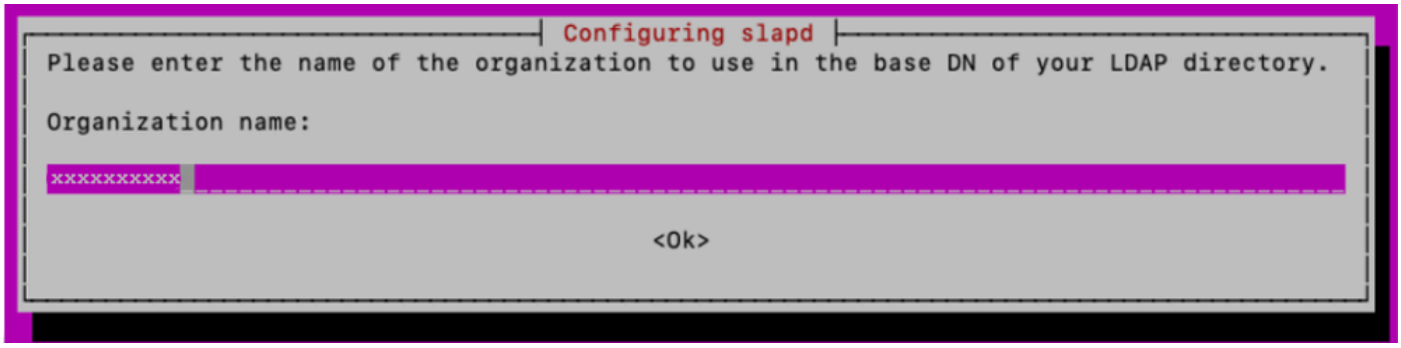
يمكنك قبول الخيار "لا" الافتراضي ل "حذف تكوين خادم OpenLDAP" وضغط مفتاح الإدخال:



اكتب اسم المجال واضغط مفتاح الإدخال:



يستخدم xxxxxxx" في هذا المختبر ك "اسم المؤسسة":



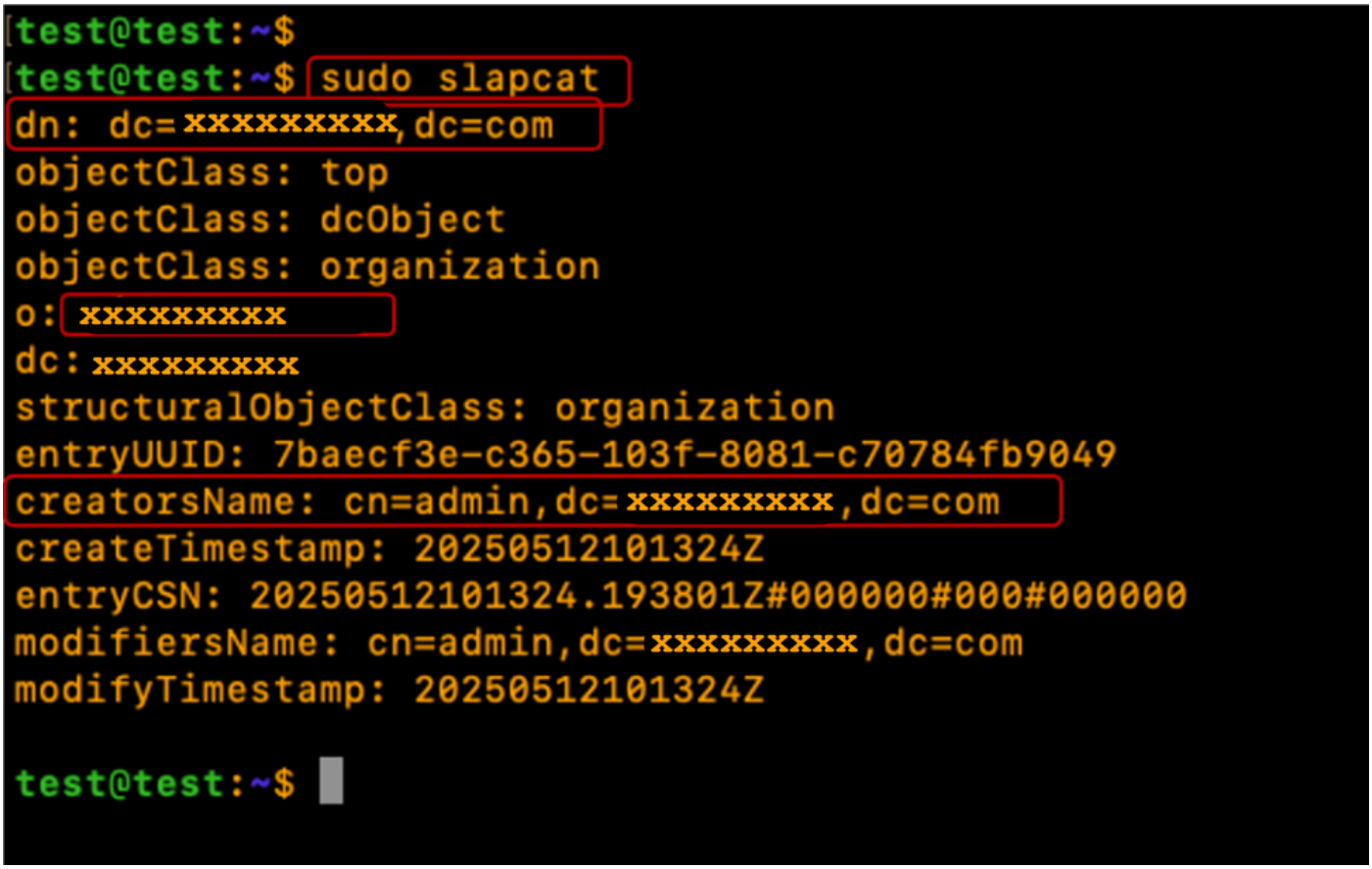
بعد ذلك، اكتب "كلمة مرور المسؤول"، وقم بتأكيدها

للحصول على خيارات التكوين الأخرى، ابق على الافتراضيات واضغط على مفتاح الإدخال

على لوحة المفاتيح لإكمال التكوين.

التحقق من تثبيت SLAPD باستخدام الأمر:

```
sudo slapcat
```



الخطوة 3: تثبيت مدير حساب LDAP

تثبيت مدير حساب LDAP (LAM) لإنشاء مستخدمي LDAP والمجموعات وإدارتها:

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

تمكين امتداد PHP-CGI PHP، المطلوب من قبل LAM.

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

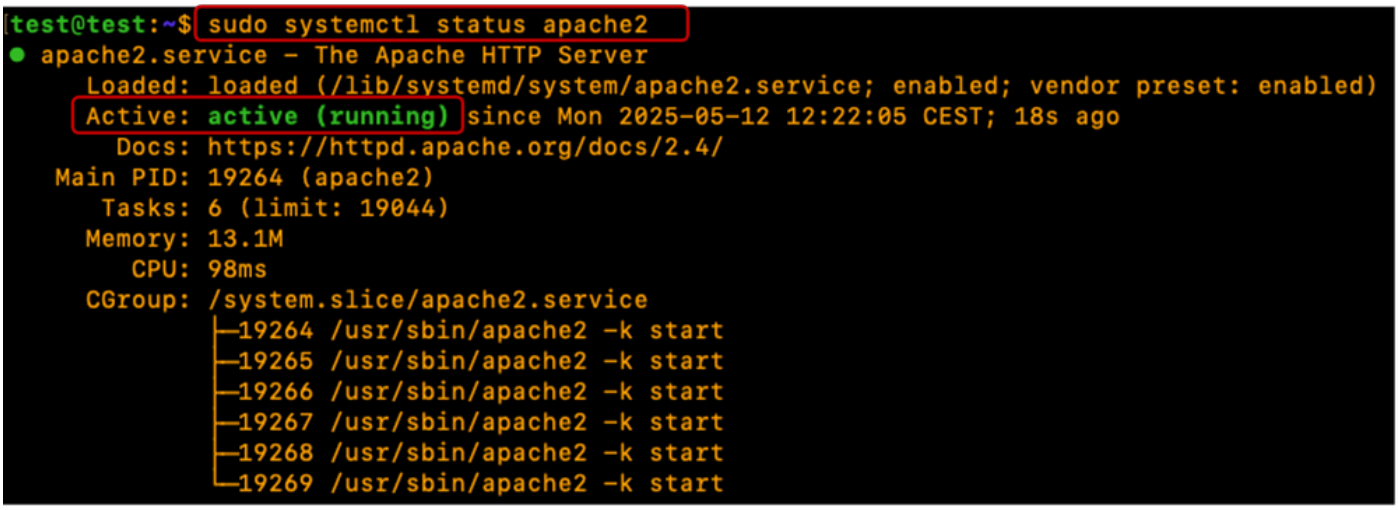
أعد تحميل Apache لتنشيط التكوين الجديد.

قم بإعادة تشغيل خدمة Apache وتمكينها من التشغيل التلقائي في وقت التمهيد:

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

تحقق من أن حالة خادم Apache "قيد التشغيل" و"نشط"

```
sudo systemctl status apache2
```

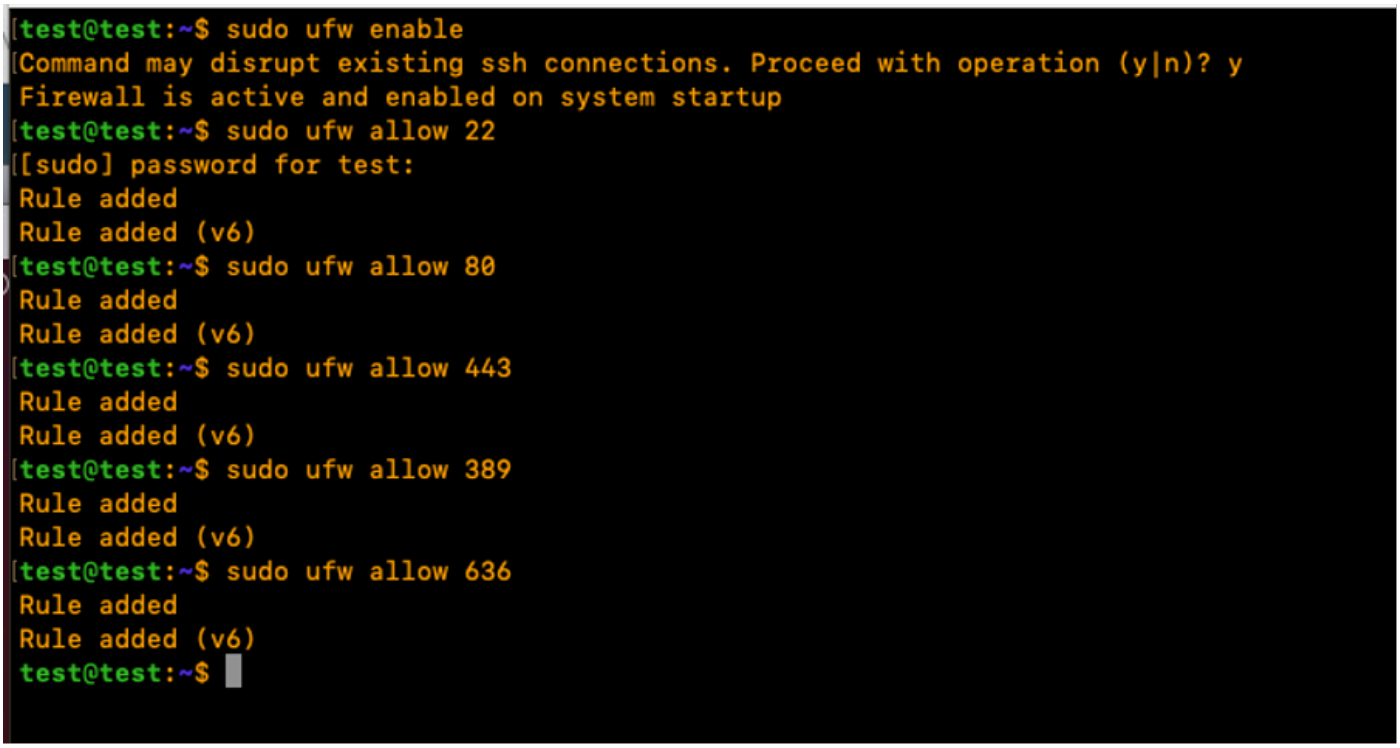


تكوين جدار حماية Ubuntu للسماح بالمنفذ 80(وب) و 443 (الويب الآمن) و 389(LDAP) و 636 (رمز الأمن الآمن إذا لزم الأمر لبروتوكول LDAP)

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

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

```
sudo ufw allow 636
```



التحقق من حالة جدار حماية Ubuntu:

```
sudo ufw status
```

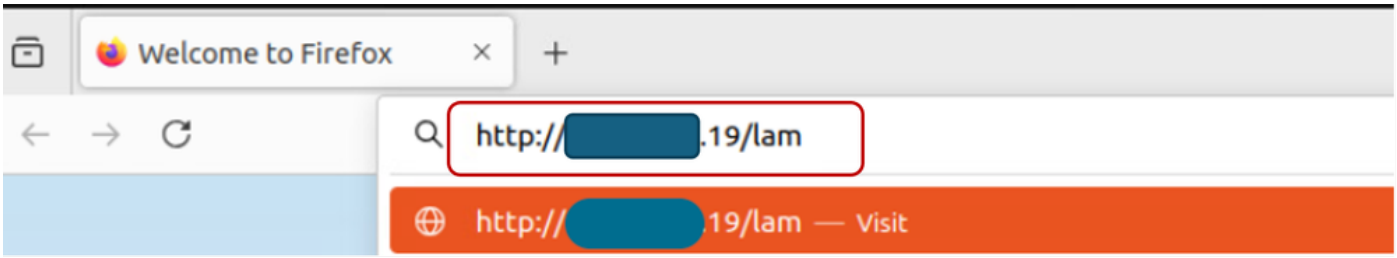
```
test@test:~$ sudo ufw status
Status: active

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)
```

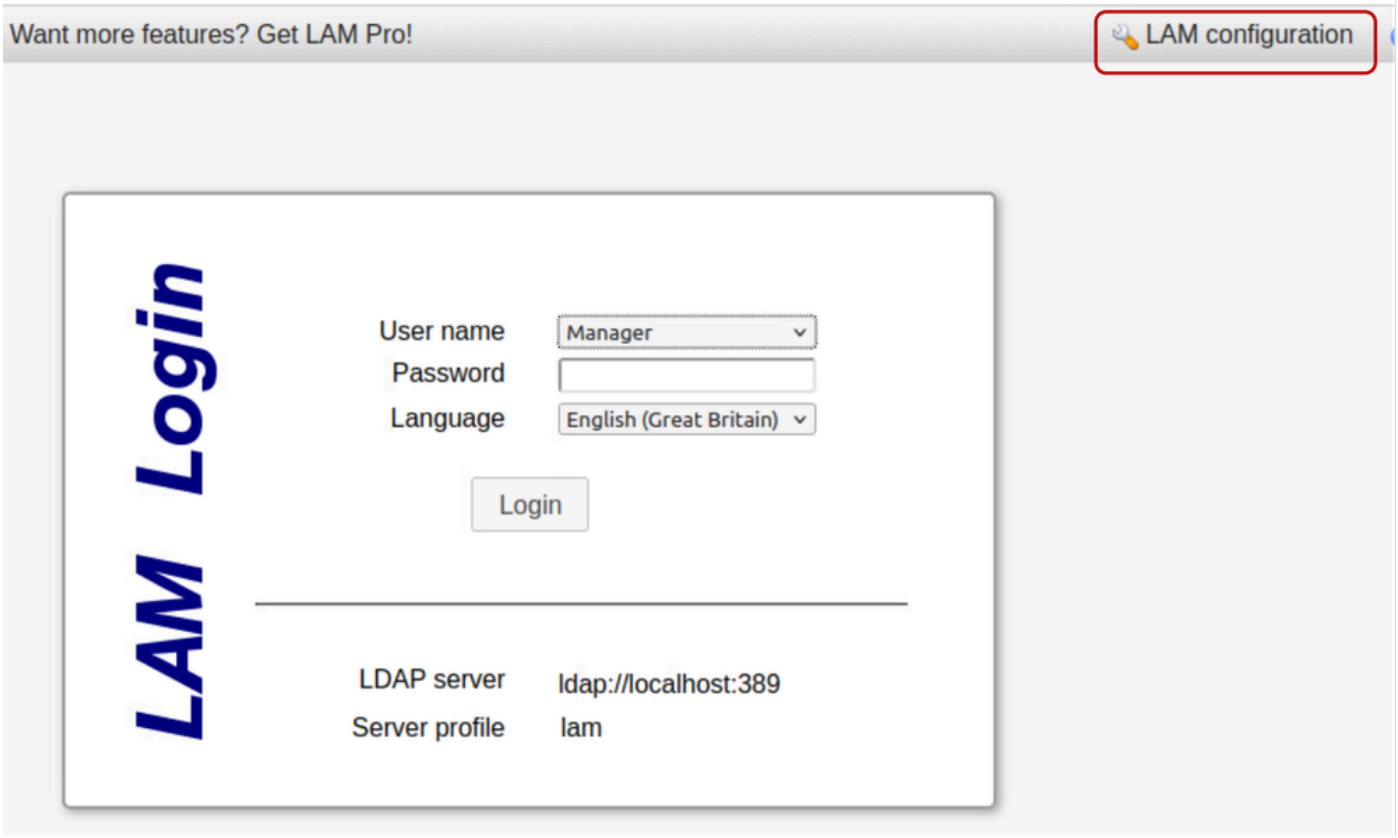
الخطوة 4: تكوين مدير حساب LDAP

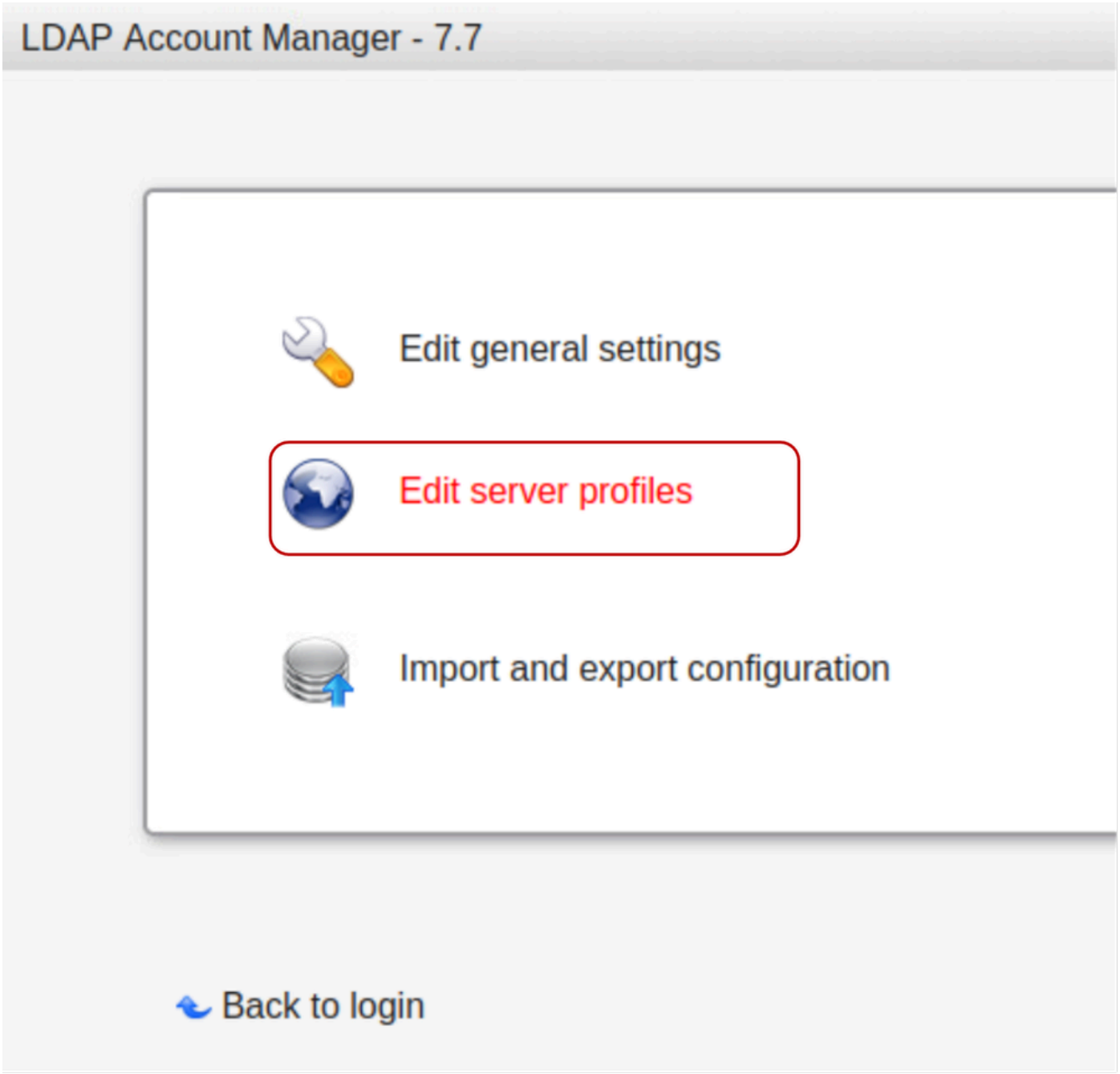
لتكوين مدير حساب LDAP (LAM) من واجهة المستخدم الرسومية، افتح مستعرض ويب، وأدخل عنوان IP الخاص بخادم Linux وأضف مسار 'lam' إليه كما هو موضح:

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

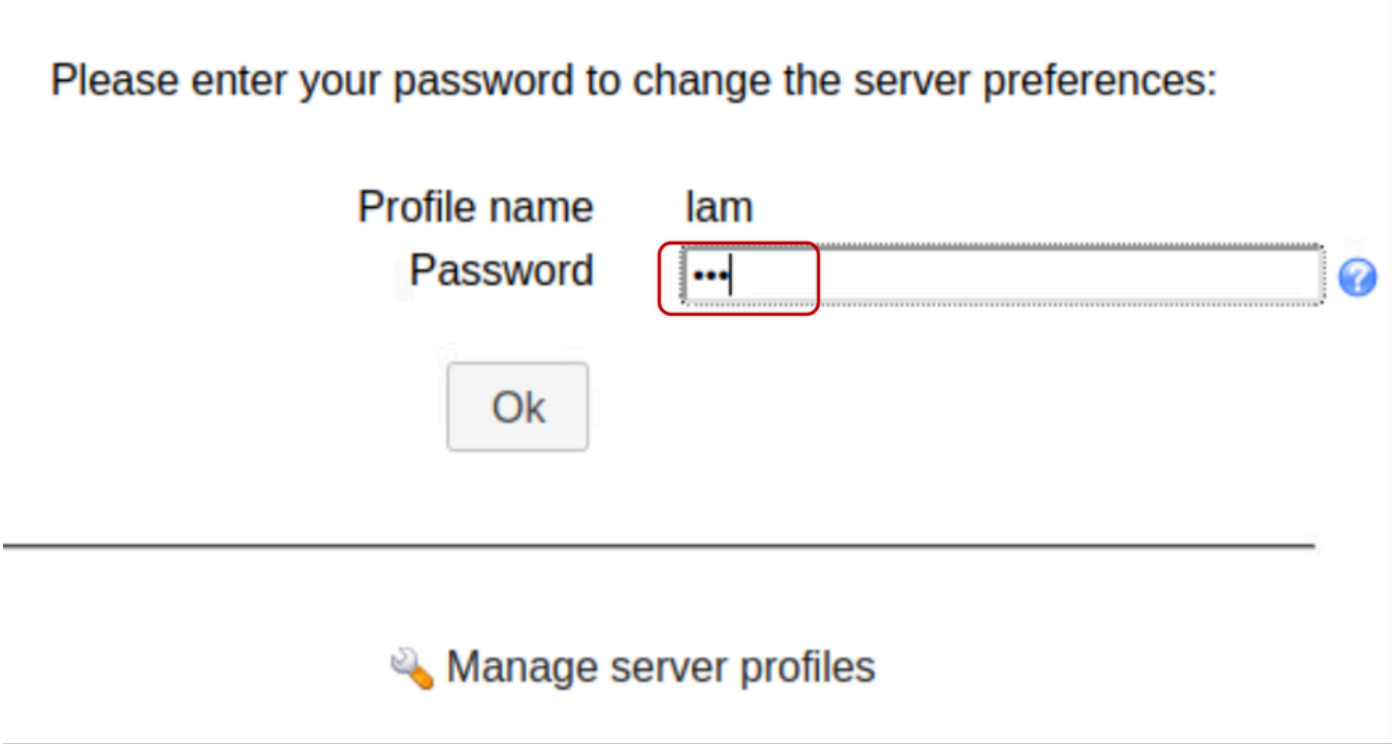


انقر على تكوين LAM" ثم حدد "تحرير ملفات تعريف الخادم".


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



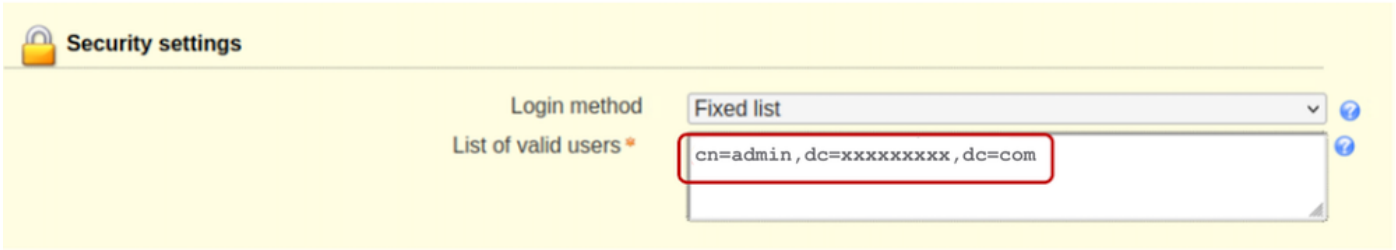
اكتب في كلمة المرور الافتراضية "lam" لتسجيل الدخول.



ضمن علامة التبويب "إعدادات عامة"، تحقق من إعدادات الخادم و"اللغة" و"المنطقة الزمنية".

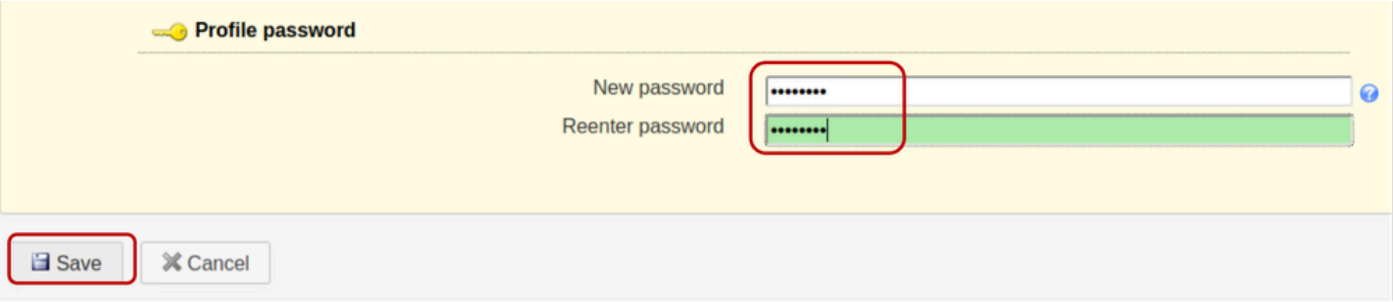
في قسم إعدادات الأداة، قم بتحرير وإضافة اسم المجال المطلوب في حقل لاحقة الشجرة كما هو موضح أدناه:

قم بتحرير قسم إعدادات الأمان لتضمين مستخدم "admin" المستخدم لإدارة خدمة SLAPD.



ضبط "كلمة مرور ملف التعريف". يتم إستخدام كلمة المرور هذه للإدخالات التالية على واجهة تكوين LAM، على سبيل المثال، يتم تكوين "Cisco123" بدل من كلمة المرور الافتراضية "lam".

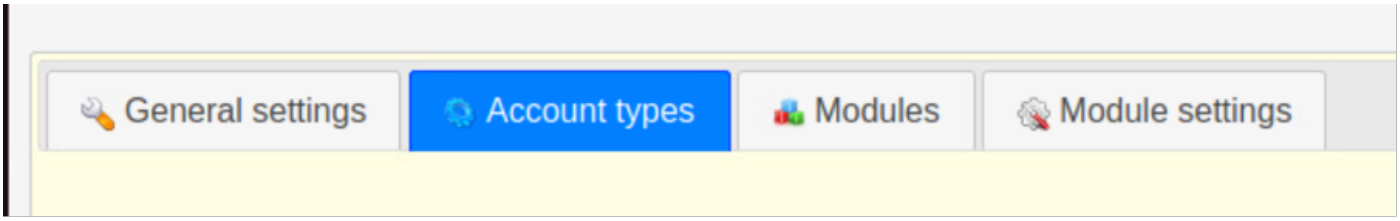
حفظ التكوين:



بعد ذلك، تتم إعادة تشغيل الجلسة على واجهة واجهة المستخدم الرسومية (GUI) الخاصة بتكوين LAM.

قم بتسجيل الدخول مرة أخرى (تكوين LAM > تحرير ملفات تعريف الخادم) باستخدام كلمة المرور الجديدة التي تم إنشاؤها.

انقر على "أنواع الحساب"،



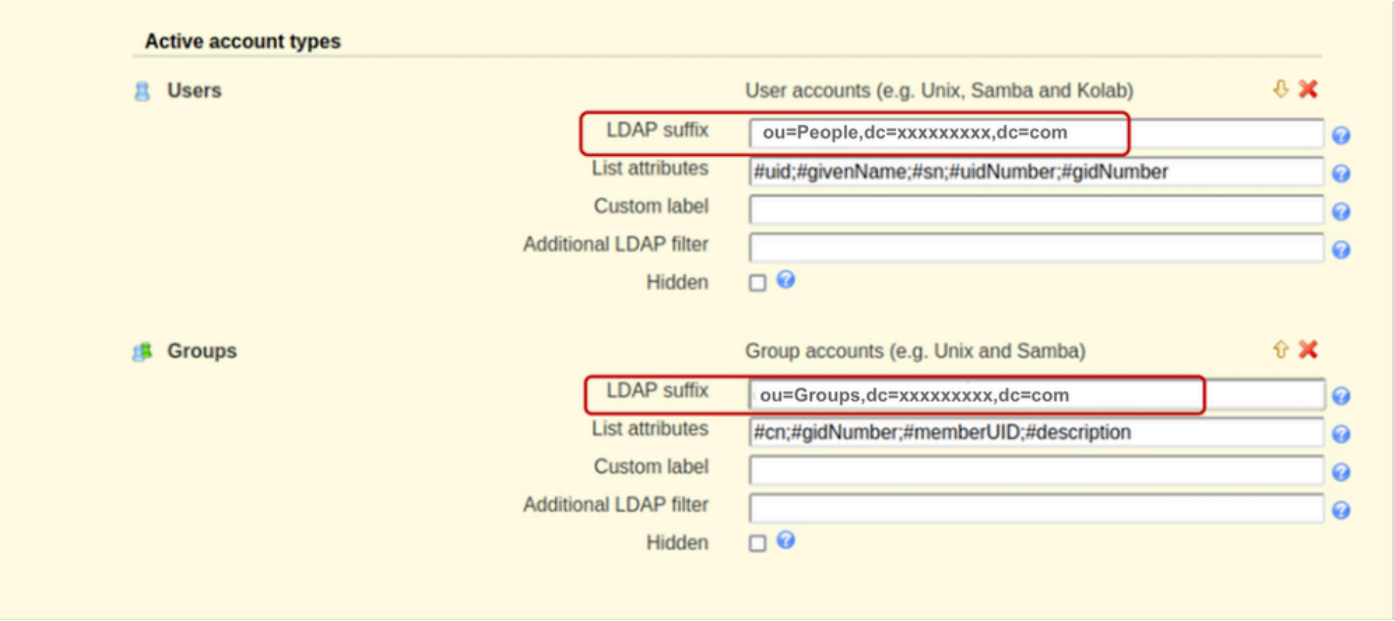
قم بالتمرير لأسفل وتحرير أنواع الحسابات النشطة الافتراضية باستخدام معلومات اسم المجال في حقل لاحقة LDAP. على سبيل المثال، يعرض المحتوى الافتراضي لحقل "لاحقة LDAP" قيمة على هيئة "ou=People،dc=my-domain،dc=com".

وفي حالة الحاجة إلى إنشاء وحدات تنظيمية جديدة، يستعاض عن محتوى حقل "لاحقة LDAP" لكي يحتوي على اسم الوحدة التنظيمية.

يتم عرض التنسيق على هيئة "ou=<organization_unit>، dc=xxxxxxx، dc=com".

وفي هذا العرض التوضيحي، فإن مذكرة التفاهم الخاصة بالمستخدمين هي "الناس"، أما كلمة المرور الخاصة بالمجموعات فهي "المجموعات".

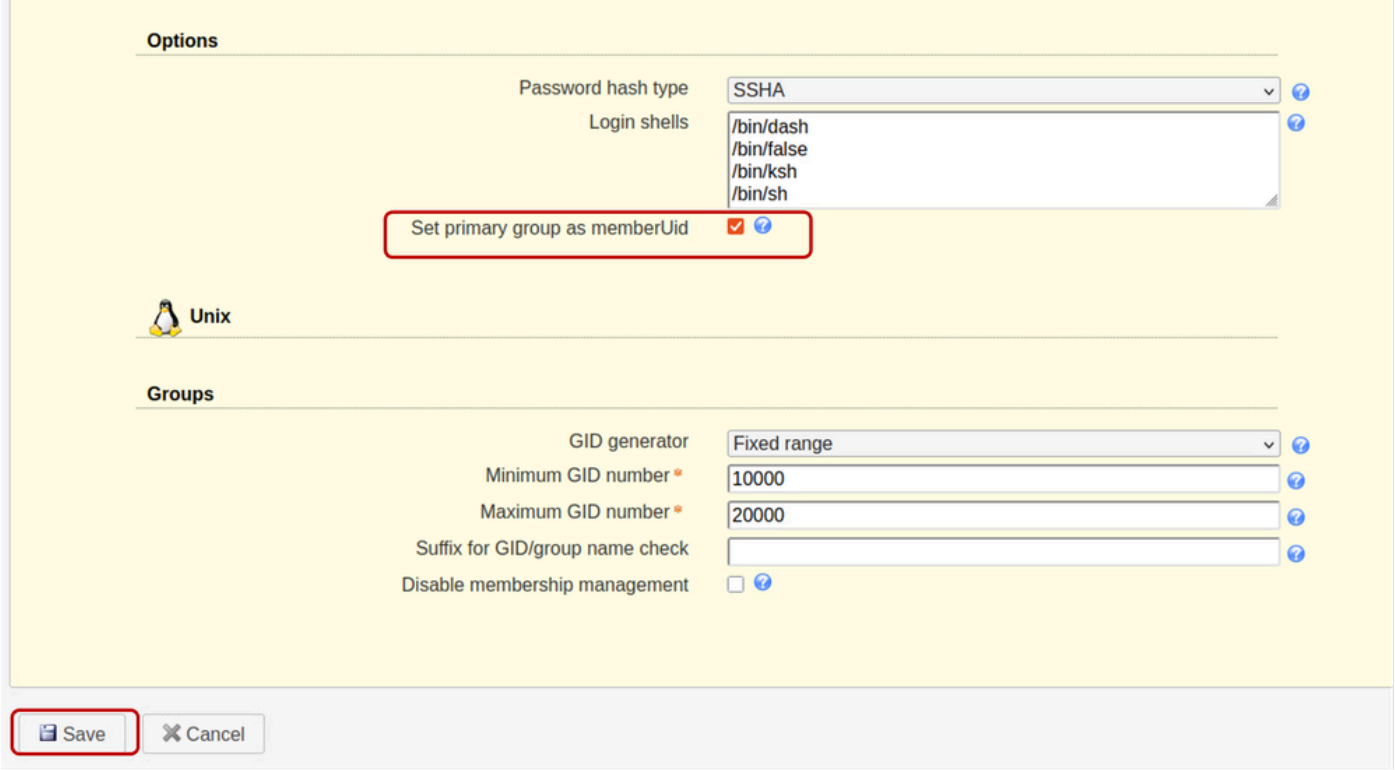
حفظ التكوين.



قم بالتمرير لأسفل إلى القسم "خيارات" وتأكد من التحقق من "تعيين المجموعة الأساسية ك memberUid".

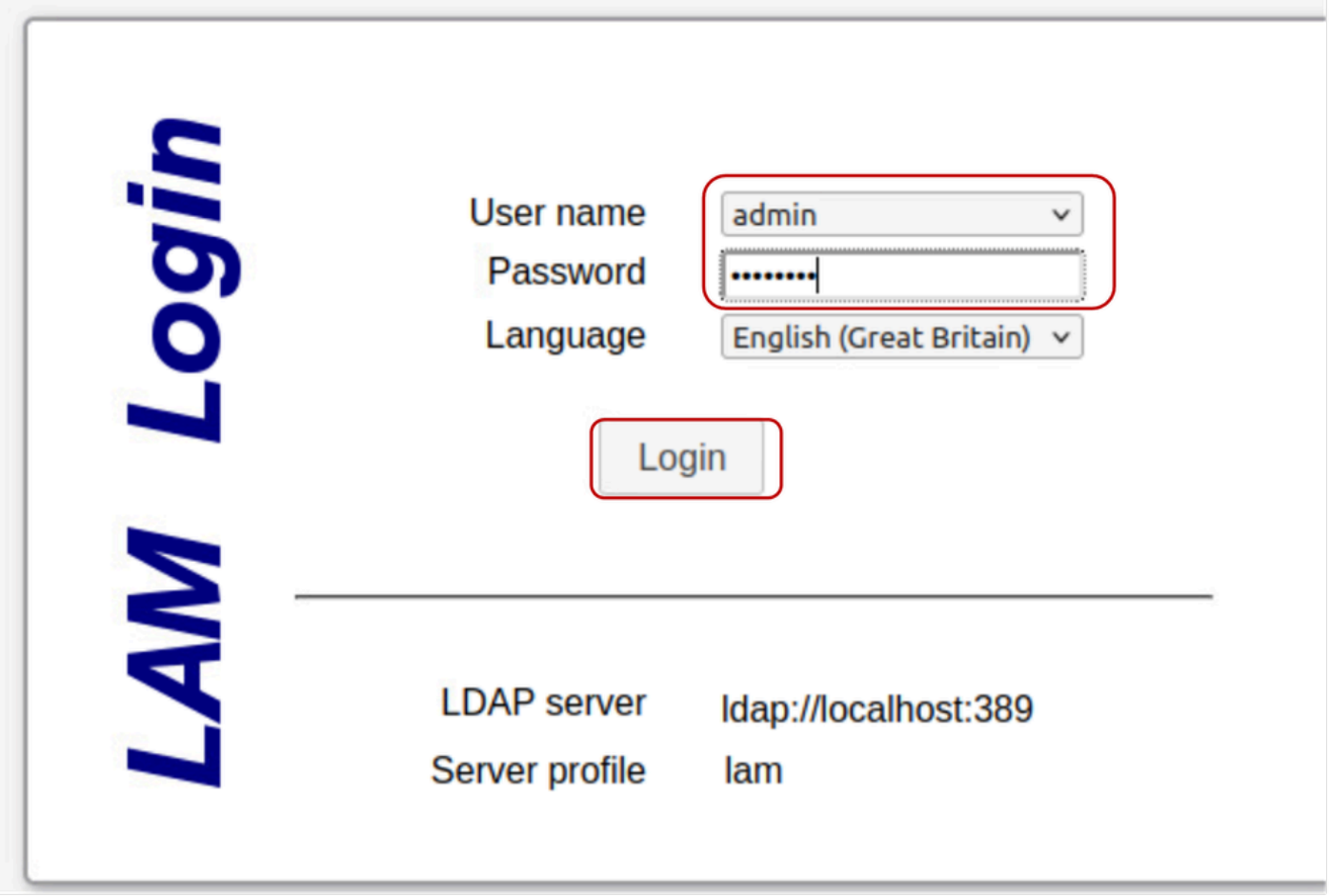
بشكل افتراضي ال يتم تعيين الخيار تعيين المجموعة الأساسية ك memberUid" على مثل OpenLDAP ل "المجموعة الأساسية" إستخدام هذا تنشيط يتيح. المجموعة كائنات مجموعة LDAP القياسية، حيث يمكن الإشارة إلى "memberUid" (على سبيل المثال: في تكوين خادم UCS C Series). في حالة إلغاء تحديد هذا الخيار، يفشل تسجيل الدخول للمستخدمين الذين ينتمون إلى أي مجموعة أساسية.

حفظ التكوين.

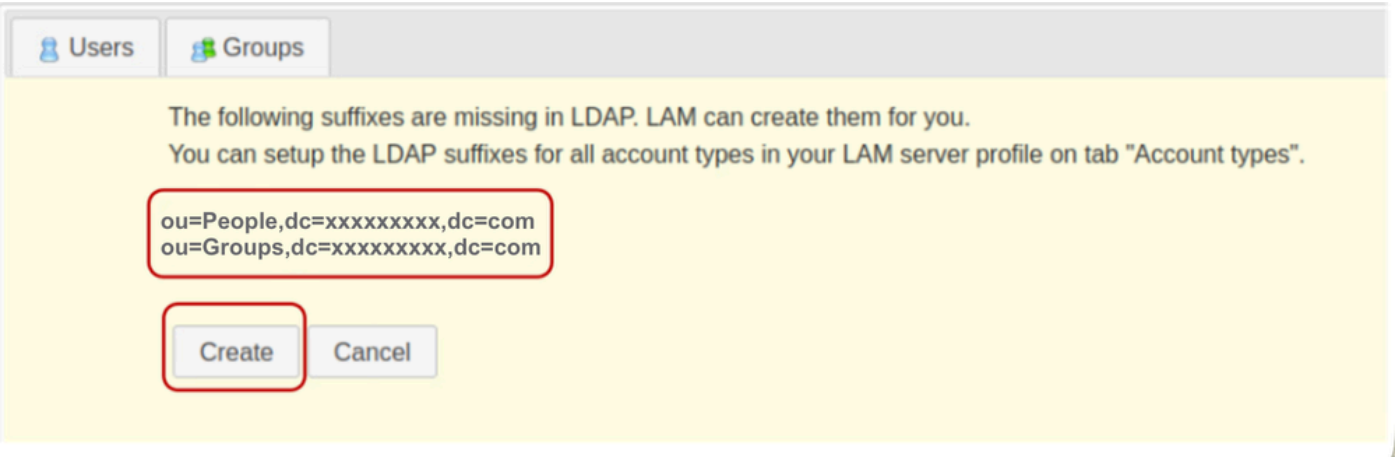


الخطوة 5: إنشاء ملحقات ومجموعات ومستخدمين

قم بتسجيل الدخول إلى LAM كمستخدم "admin" باستخدام كلمة المرور نفسها التي تم إنشاؤها أثناء التثبيت، لإنشاء مستخدمين ومجموعات تنتمي إلى وحدات التحكم في الوصول (OUs) التي تم إنشاؤها مسبقا (الأشخاص والمجموعات) على التوالي:

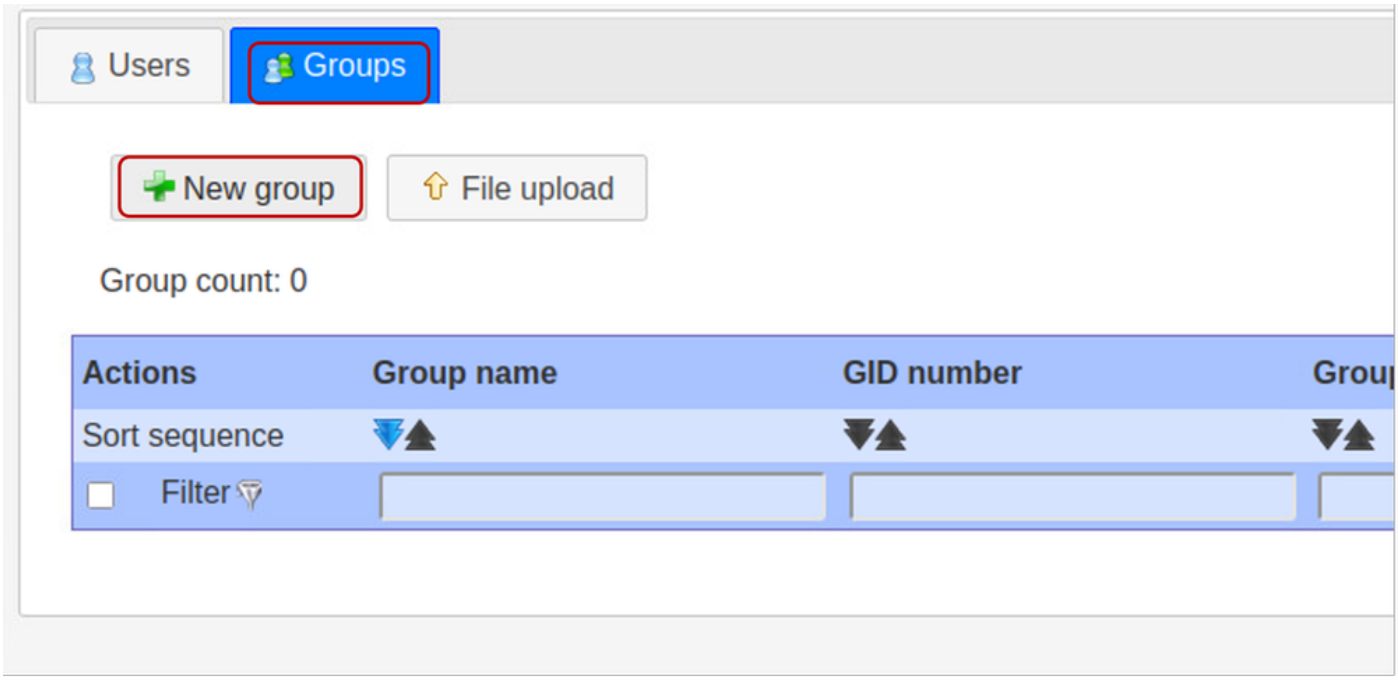


قم بإنشاء وحدات التحكم في الوصول (OUs) المحددة مسبقا في قسم تكوين LAM.
انقر فوق "إنشاء".



بعد ذلك، في مدير حسابات LDAP، قم بإنشاء مجموعة "it":

حدد علامة التبويب مجموعات وانقر فوق مجموعة جديدة

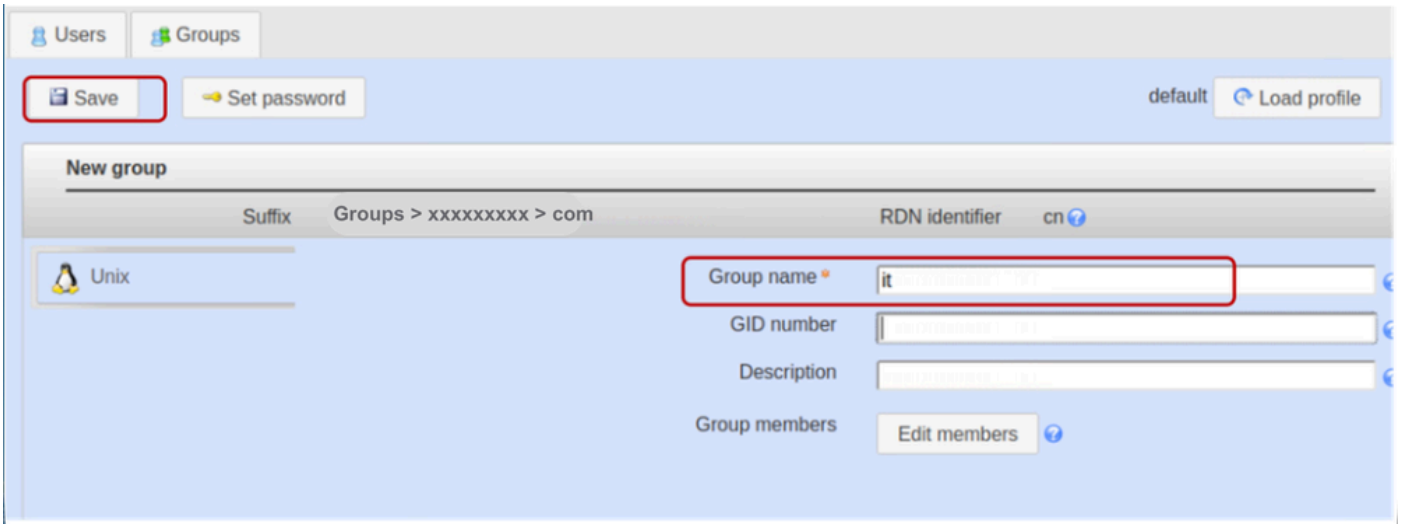


قم بتعيين اسم المجموعة على أنه وه".

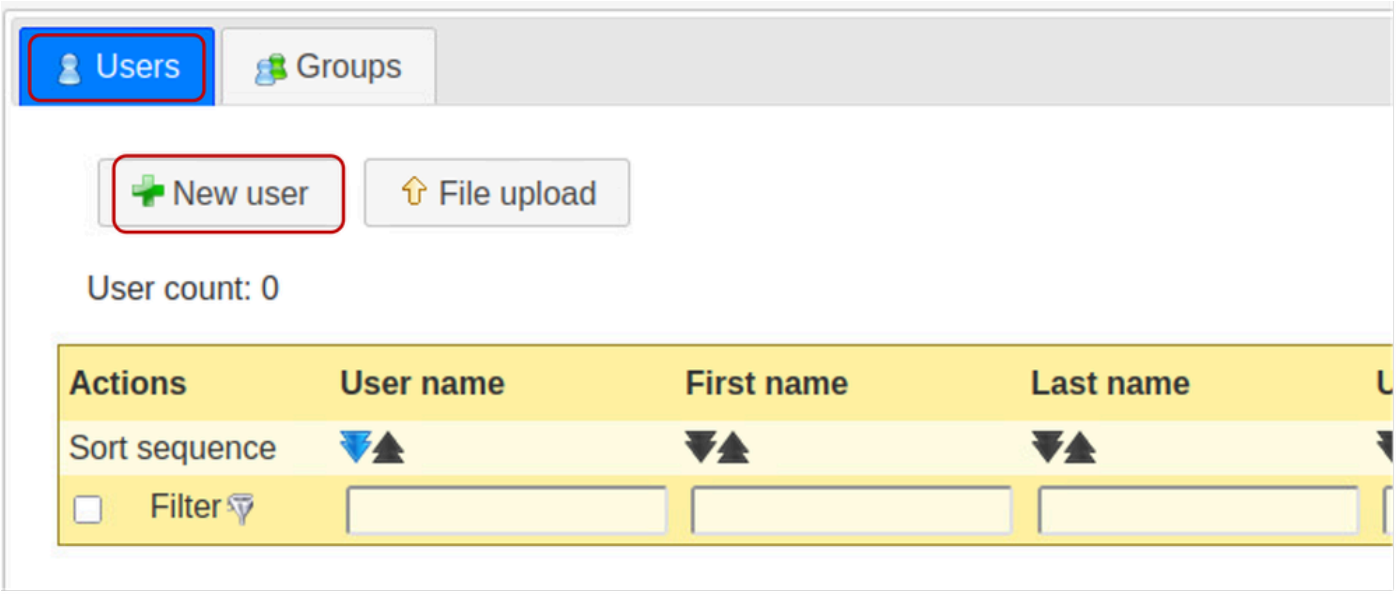
ملاحظة: بينما تكون أنظمة Cisco UCS مرنة بشكل عام لتنوعات الحالات، فإن أفضل ممارسة لضمان قابلية الحفاظ على اصطلاحات تسمية الحروف الصغيرة هو التشغيل البيني على المدى الطويل عبر بيئات البنية الأساسية لخادم LDAP المتنوعة.

أترك حقل رقم المعرف الفريد العمومي فارغا. تم تصميم مدير حسابات LDAP (LAM) لنشر هذا الحقل تلقائيا بالقيمة التالية المتاحة.

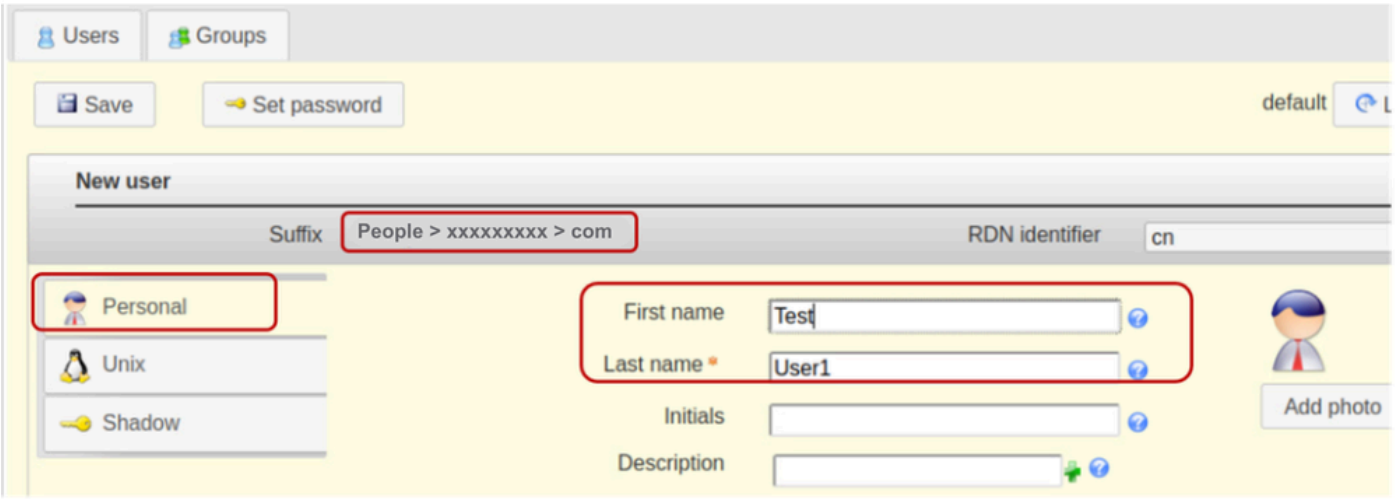
قم بتوفير وصف إذا كان ذلك مطلوبا وانقر فوق حفظ



انقر فوق علامة التبويب مستخدمون" لإنشاء حسابات مستخدمين وتحديد "مستخدم جديد".



ملء الحقول المطلوبة للمستخدم "testuser1" في علامة التبويب "شخصي".

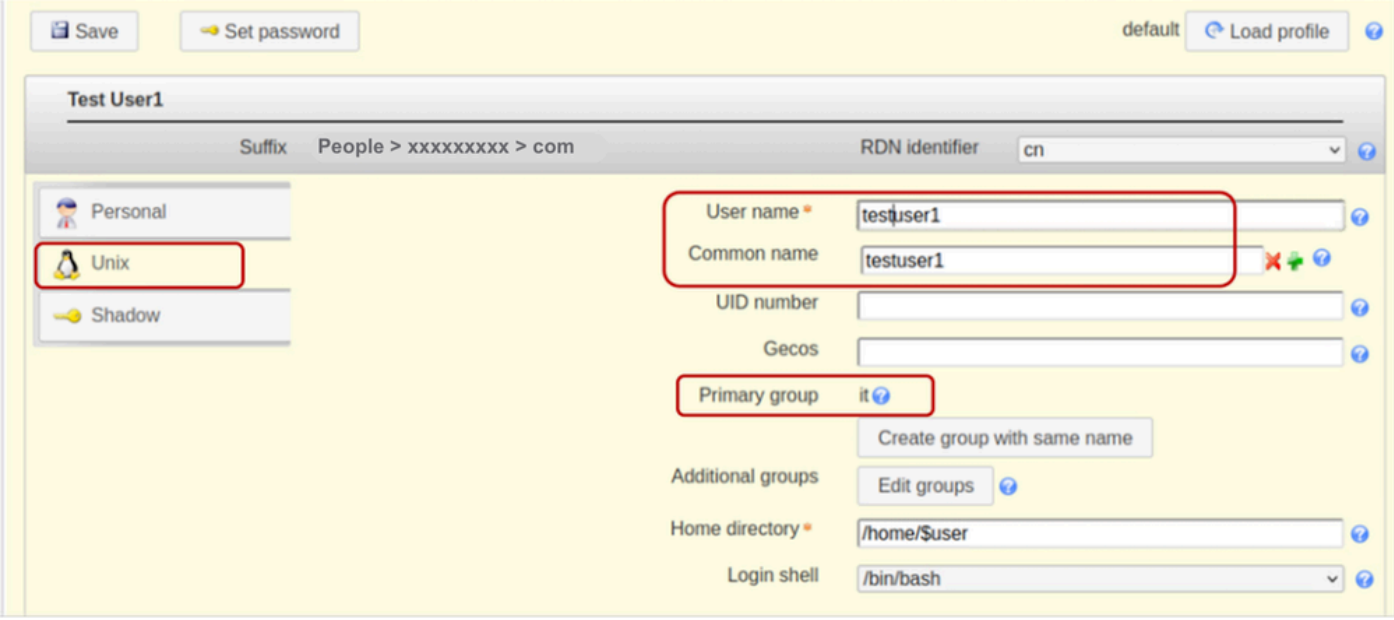


حدد علامة التبويب Unix، وقم بإضافة testuser1 في حقل اسم المستخدم. قم بتضمين المستخدم في مجموعة "it".

في هذا العرض، يوجد فقط مجموعة "it"، لذلك فهي بالفعل مأهولة مسبقا.

الاحتفاظ بمعرف RDN ك "الاسم الشائع" (cn). هذا يمكن النظام من ملء الحقل "الاسم الشائع" تلقائيا باستخدام القيمة المحددة في الحقل "اسم المستخدم".

أترك حقل رقم المعرف فارغا حيث تقوم LAM تلقائيا بملء الحقل بالقيم المتاحة.



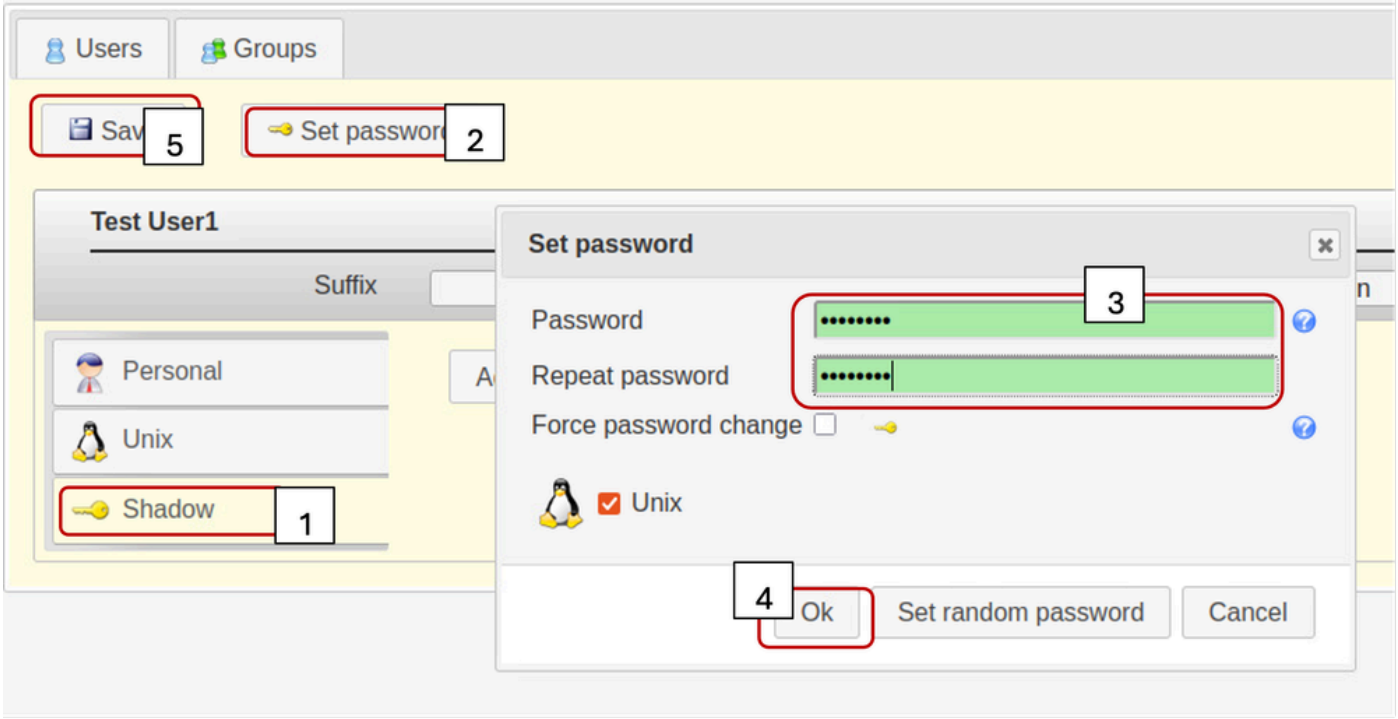
حدد صفحة الظل،

لم يتم إستخدام ملحق حساب الظل.

انقر على "تعيين كلمة المرور".

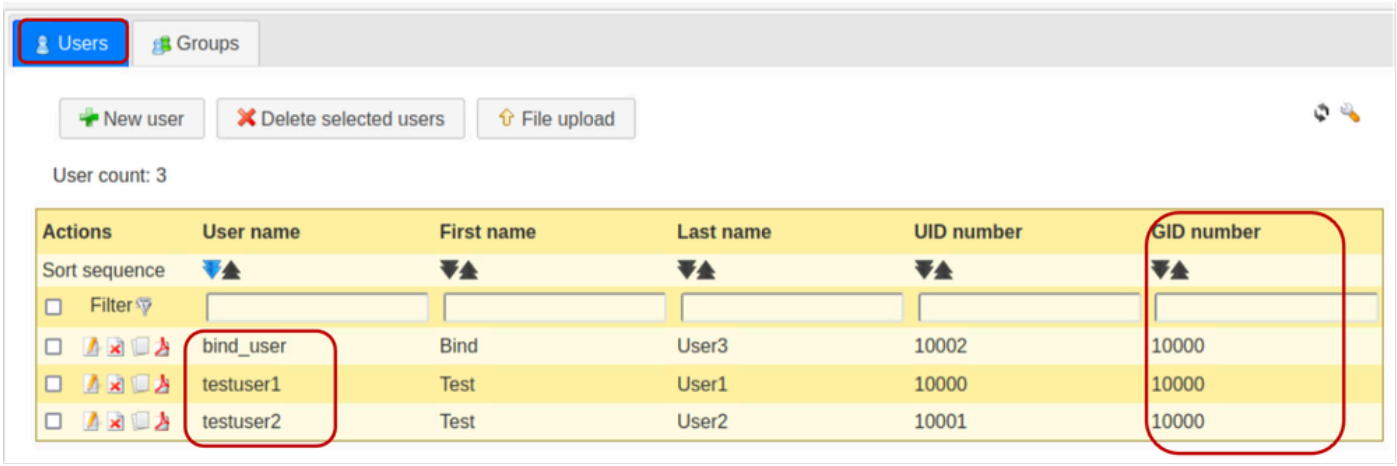
تعيين كلمة مرور المستخدم

ثم انقر فوق موافق واحفظ



كرر الخطوات المحددة الموضحة مسبقا لإنشاء حساب مستخدم "testuser2" وحساب "bind_user".

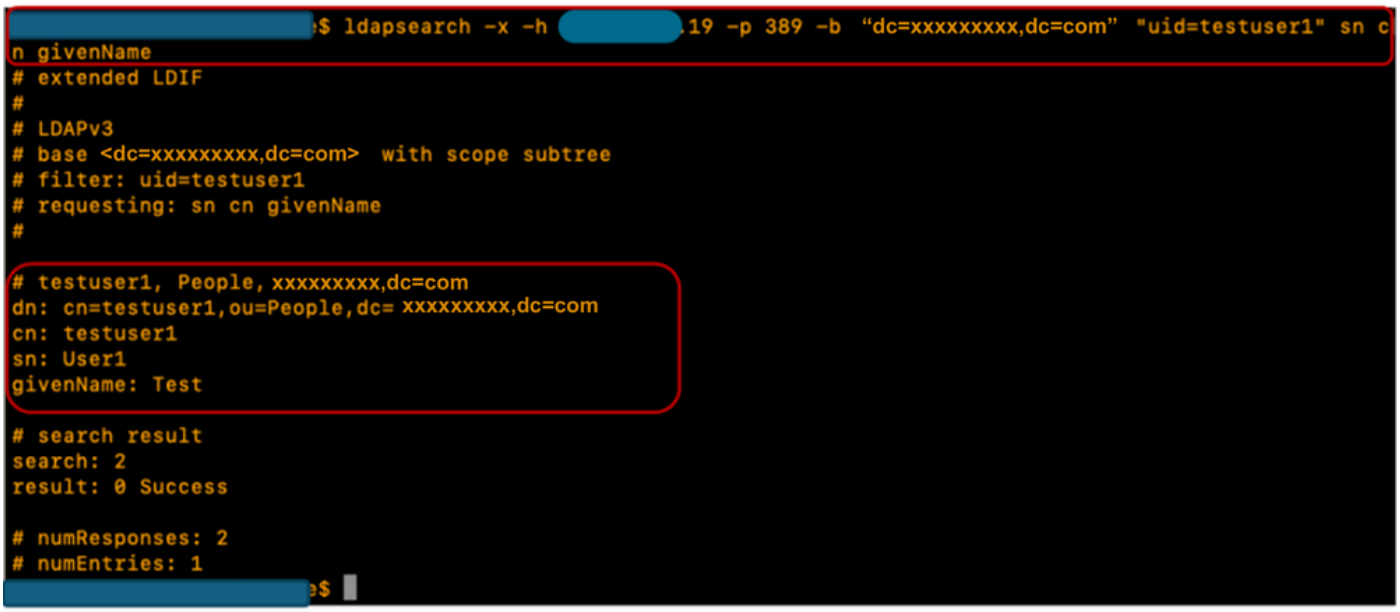
انقر فوق علامة التبويب "المستخدمون" للتحقق من إنشاء جميع المستخدمين المطلوبين. (الحصول على نفس القيمة في عمود gidNumber يؤكد أن المستخدمين الذين تم إنشاؤهم ينتمون إلى نفس المجموعة - وه)



الخطوة 6: إختبار تسجيل دخول LDAP المحلي

قم بتسجيل الدخول إلى نظام آخر يستند إلى Linux، مع إمكانية الوصول إلى خادم OpenLDAP.
قم بتشغيل الأمر ldapsearch المحدد للتحقق من عمل LDAP:

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



مع لمات التكوين عل CIMC

قم بتسجيل الدخول إلى CIMC.

في جزء التنقل، حدد Admin وإدارة المستخدم و LDAP.

مل ع معلمات تكوين LDAP كما هو موضح أدناه:

- تمكين LDAP: محدد
- شبكة DN الأساسية: dc=xxxxxxx،dc=com

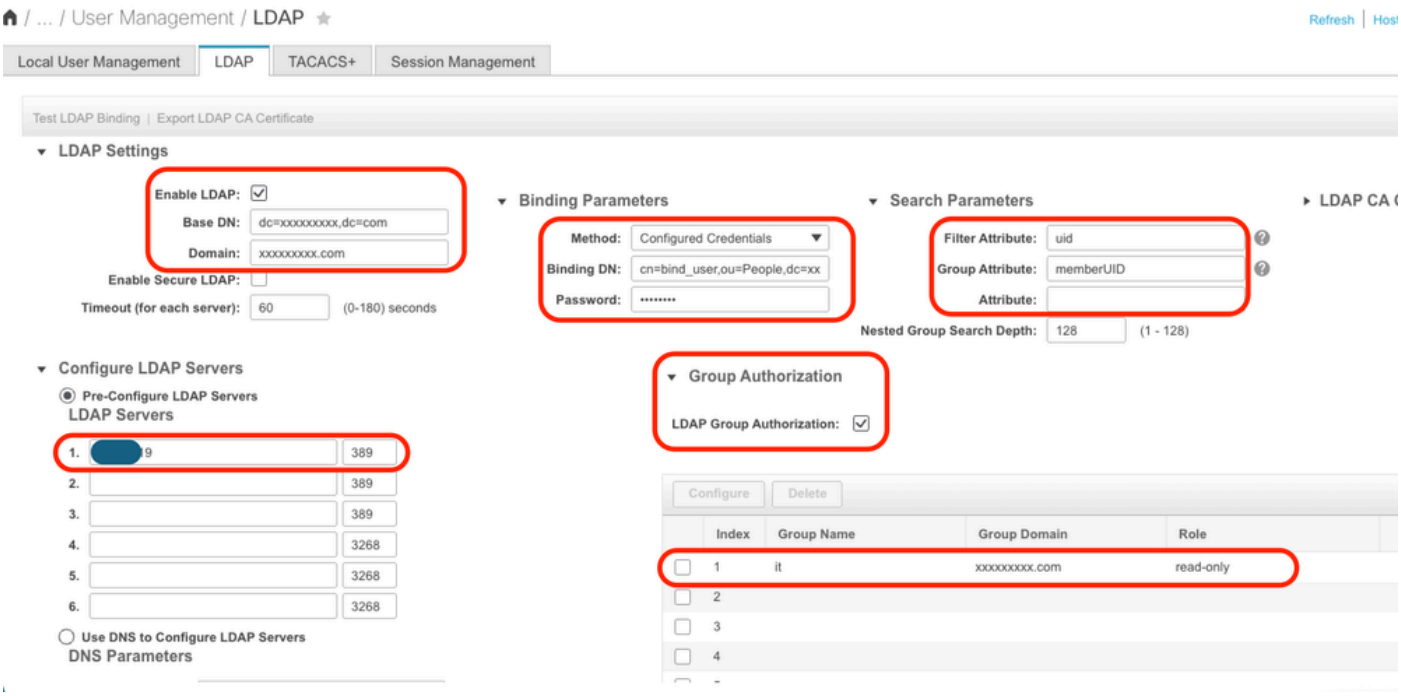
- المجال: xxxxxxxxx.com

- خادم LDAP: X.X.19 <ldap_server_ip أو FQDN>

- رب ط المعلمات: "بيانات اعتماد تسجيل الدخول" أو "بيانات الاعتماد المكونة"
  - عند إستخدام بيانات الاعتماد التي تم تكوينها، قم بإضافة DN bind_user كما تم تكوينه تماما على خادم LDAP:
    مثال: cn=bind_user، ou=People، dc=xxxxxxx، dc=com

- معلمات البحث:
  - سمة عامل التصفية: "cn" أو "uid"
  - سمة المجموعة: memberUID

- تفويض مجموعة LDAP - تم التحقق
  - اسم المجموعة: تقنية معلومات
  - مجال المجموعة: xxxxxxxxx.com
  - الدور: للقراءة فقط (أي دور مرغوب)



قم بحفظ التكوين واختبار تسجيل دخول مستخدم LDAP.

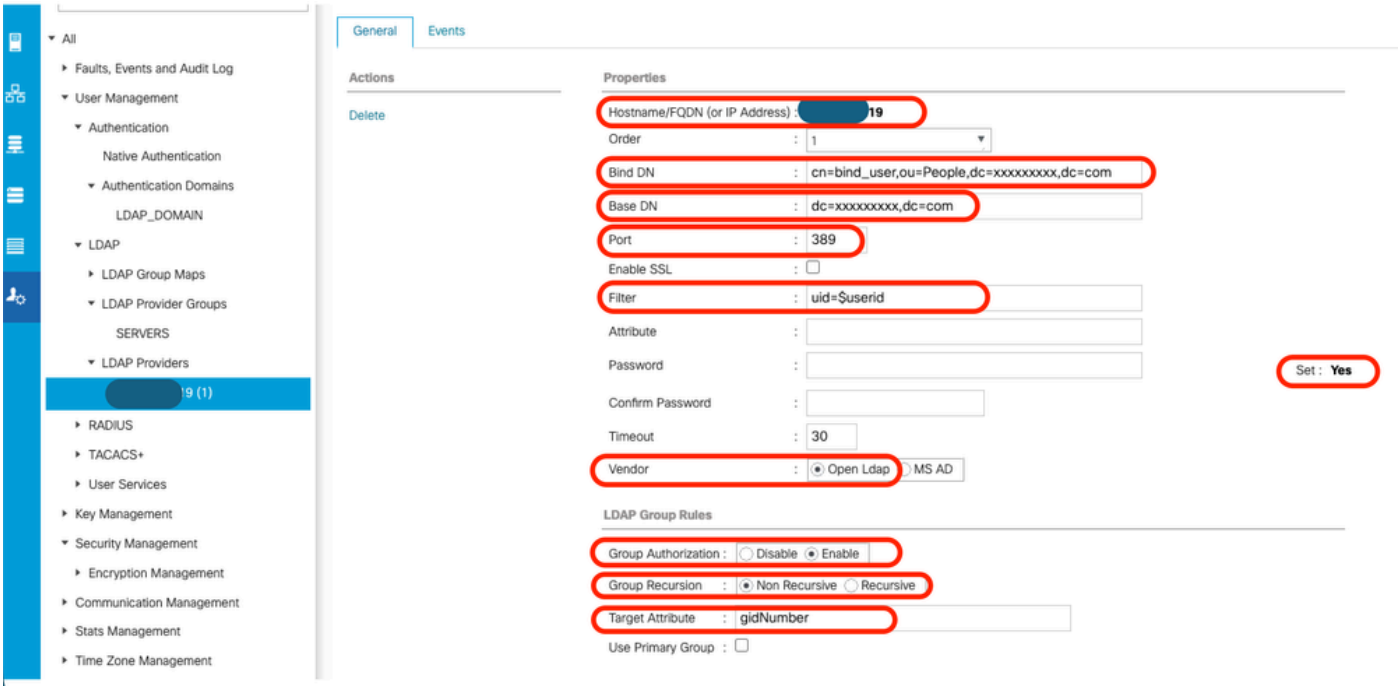
تعليمات التكوين على مدير UCS

قم بتسجيل الدخول إلى مدير UCS.

في جزء التنقل، حدد Admin وإدارة المستخدم و LDAP.

قم بتعليم تكوين LDAP كما هو موضح أدناه:

- موفر LDAP:
  - اسم المضيف: <FQDN أو عنوان IP الخاص بخادم LDAP>
  - ربط DN: cn=bind_user، ou=People، dc=xxxxxxx، dc=com
  - شبكة DN الأساسية: dc=xxxxxxx،dc=com
  - المنفذ: 389
  - تمكين SSL: معطل
  - عامل التصفية: uid=$userID
  - تفويض المجموعة: ممكن
  - تكرار المجموعة: غير متكرر
  - السمة الهدف: gidNumber
- خرائط مجموعة LDAP:
  - مجموعة LDAP DN: 10000 <gidNumber لمجموعة "it">

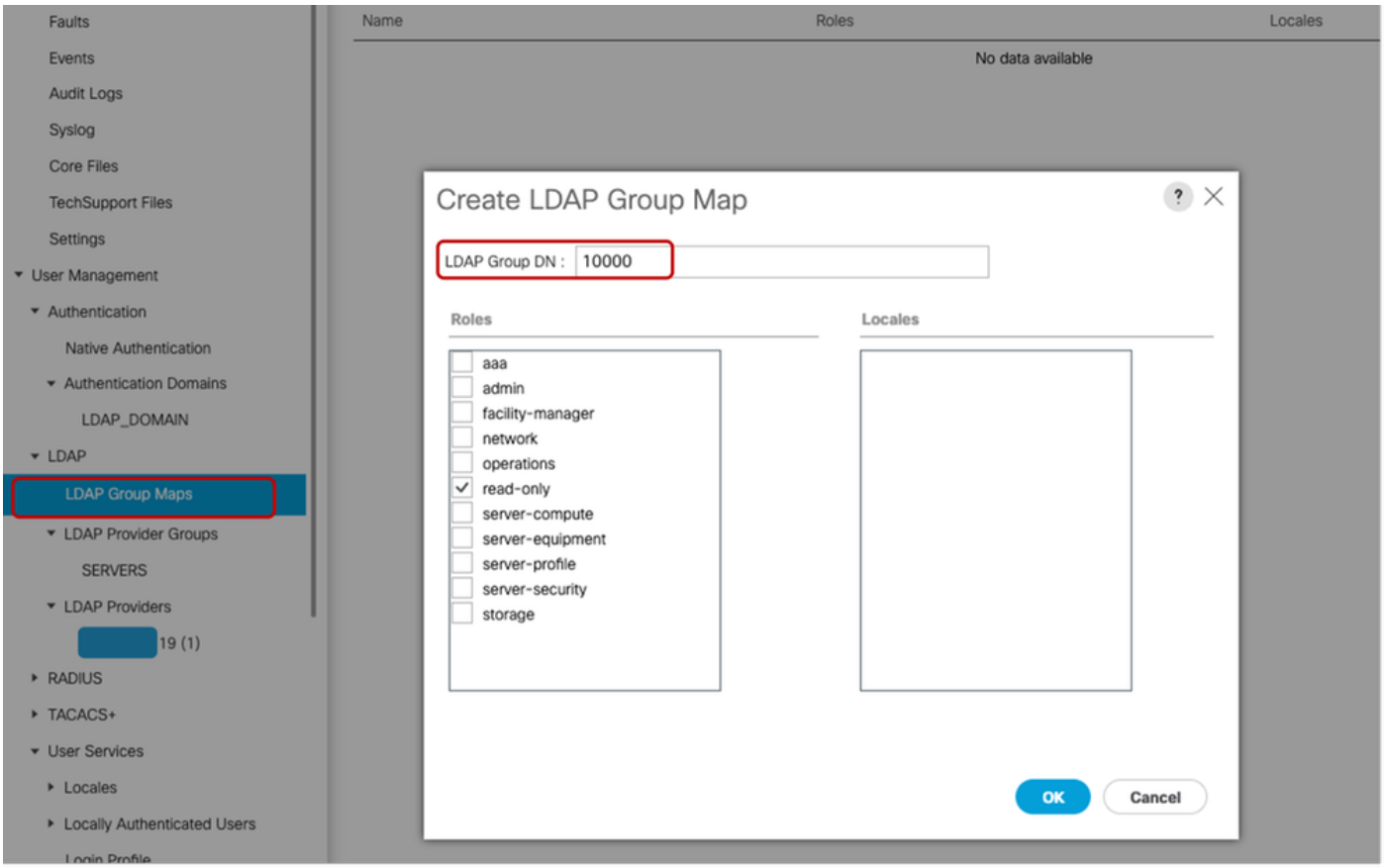


تحت الكل >> إدارة المستخدم >> LDAP> LDAP Providers>> LDAP مجموعة القواعد، السمة الهدف الافتراضية لإدارة UCS هي "memberOf". بشكل افتراضي، لا تحتوي خوادم OpenLDAP على هذه السمة المعكنة، وبالتالي فإن تعيين قيمة السمة الهدف على "memberOf" (أو تركها فارغة) يؤدي إلى فشل عمليات تسجيل دخول المستخدم لأن خادم OpenLDAP لا يتعرف على قيمة السمة المطلوبة.

في هذا المثال، تم تعيين قيمة "السمة الهدف" على "gidNumber".

إضافة موفر LDAP الذي تم تكوينه إلى مجموعة موفري LDAP. تم إنشاء مجموعة موفري LDAP ل "الخوادم" لهذا العرض التوضيحي.

عند تكوين "خرائط مجموعة LDAP" في "الكل > > إدارة المستخدم >> LDAP >> خرائط مجموعة LDAP>"، يتم إستخدام قيمة gidNumber (في هذه الحالة "10000") على أنها "خريطة DN المجموعة" كما هو موضح:



قم بتكوين مجال مصادقة LDAP (LDAP_DOMAIN) في "All>User Management>Authentication>> Authentication Domain (إدارة المستخدم)> Authentication Domain" مشيرا إلى مجموعات موفر LDAP واختبار تسجيل دخول مستخدم LDAP.

ملاحظة: إذا كانت السمة memberOf مطلوبة لتلبية متطلبات بيئية معينة أو لتنفيذ ميزة "تكرار المجموعة"، يوصى باستخدام خيار التكوين الثاني أدناه، والذي يتطلب LDAP مع تمكين ملحقات التغشية.

بينما يدعم مدير حساب LDAP (LAM) تكوين التضمين، الرجاء إعلامك بأن هذه الميزة تتطلب ترخيصا منا سبا.

لمزيد من المعلومات حول تكوين LDAP باستخدام LAM، ارجع إلى وثائق مدير حساب LDAP الرسمي.

الخيار 2: تكوين OpenLDAP باستخدام أدوات واجهة سطر الأوامر من Ubuntu والتغشيات

من أجل إستخدام OpenLDAP لمصادقة مدير UCS، يلزم وجود تغليفين يتأكدان أن المجموعات مقترنة بالمستخدمين بطريقة يمكن لنظام UCS (مدير UCS و CIMC) فهمها.

يتطلب التكوين الموجود على جانب OpenLDAP:

- شفاف "عضوي": يقوم هذه التغشية بإنشاء تعيين بين المستخدمين والمجموعات بحيث يمكن طلب سمة memberOf كجزء من هذا الاستعلام في حالة الاستعلام عن DN للمستخدم. بشكل افتراضي، لا توجد سمة للمستخدمين لعضوية المجموعة ما لم تتم إضافة تغشية إلى OpenLDAP
- تغشية "التحسين": يتم تكوين هذا التغشية للتحقق من أن الإدخالات في سمة العضو في كائنات المجموعة تبقى متزامنة مع سمة memberOf لكائنات المستخدم. بدون هذه الخدمة، إذا تم حذف مستخدم بدون تعديل المجموعة أيضا، يمكن أن تبقى شبكات DN المعزولة في كائن المجموعة. تضمن خدمة التحسين التناسق في كلا الاتجاهين.

الخطوة 1: أدوات الشبكة الأولية وتكوين اسم مضيف خادم Linux

1. كرر الخطوة 1 ضمن الخيار 1.

الخطوة 2: تثبيت SLAPD

كرر الخطوة 2 ضمن الخيار 1. (باستثناء تثبيت PHP و Apache كخيار 2 لا يتطلب مهمة العمل - لا توجد LAM)

تأكد من السماح بالمنافذ المطلوبة من خلال جدار حماية Ubuntu.

الخطوة 3: تثبيت "memberOf" على خادم LDAP

التحقق من تثبيت تغشية "memberOf"

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

```
test@test:~$ sudo ldapsearch -Q -LLL -Y EXTERNAL -H ldapi:/// -b cn=config '(olcModuleLoad=*)'
dn: cn=module{0},cn=config
objectClass: olcModuleList
cn: module{0}
olcModulePath: /usr/lib/ldap
olcModuleLoad: {0}back_mdb
```

لتثبيت تغشية "memberOf"، قم بإنشاء ملف .ldif باسم ldap.memberOf.load.ldif (استخدم أي اصطلاح تسمية مرغوب فيه) وأضف التكوين المحدد:

```
cat <
```

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

قم بإضافة التكوين في ملف ldap.member.load.ldif إلى ملف تعريف LDAP باستخدام الأمر المحدد:

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

يقوم بتكوين إدخال وحدة MemberOf و olcDatabase لمطابقة متطلبات النشر، حسب برامج لينوكس.

.هو موضح أدناه. olcDatabase={1}mdb" و"مجموعة GroupOfNames هي سمة إجبارية لقيمات

قم بإنشاء ملف ldap.memberOf.config.ldif، وملء السمات الخاصة به واستيراد محتوياته إلى ملف تعريف 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
```

الخطوة 4: تثبيت التغشية 'Refint' على خادم LDAP

بعد ذلك، قم بتثبيت التحسين إلى openLDAP:

قم بإنشاء ملف .ldif باسم ldap.refint.load.ldif (أستخدم أي اصطلاح تسمية مطلوب) وأضف التكوين المحدد:

```
cat <

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

إستيراد التكوين في ملف ldap.refint.load.ldif إلى ملف تعريف LDAP باستخدام الأمر المحدد:

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

تكوين التحسين، الذي يحافظ على التكامل المرجعي بين المجموعات والمستخدمين.

تكوين وحدة التحسين النمطية وإدخال OLCdatabase الخاص بها لمطابقة متطلبات النشر.

قم بإنشاء ملف ldap.refint.config.ldif واستيراد محتواه في ملف تعريف 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
```

عند تثبيت كل من الملحقات/الملحقات، يكون إخراج الأمر ldapsearch المحدد مماثل للإخراج المبين أدناه:

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

```
test@test:~$ sudo ldapsearch -Q -LLL -Y EXTERNAL -H ldapi:/// -b cn=config '(olcModuleLoad=*)'
dn: cn=module{0},cn=config
objectClass: olcModuleList
cn: module{0}
olcModulePath: /usr/lib/ldap
olcModuleLoad: {0}back_mdb

dn: cn=module{1},cn=config
objectClass: olcModuleList
cn: module{1}
olcModuleLoad: {0}memberof

dn: cn=module{2},cn=config
objectClass: olcModuleList
cn: module{2}
olcModuleLoad: {0}refint
```

عندما يتم تكوين كل الملحقين/الملحقين، فإن الإخراج إلى الأمر ldapsearch المحدد يماثل الإخراج المعروض:

```
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
```

إعادة تشغيل خدمة SLAPD لكي تكون الإضافات/الوحدات النمطية المثبتة حديثا قابلة للاستخدام:

```
sudo systemctl restart slapd
```

الخطوة 5: إنشاء ملحقات ومستخدمين ومجموعات

إنشاء وحدات تنظيمية (للمستخدمين والمجموعات) والمستخدمين والمجموعات.

قم بإنشاء أوامر المستخدمين (الأشخاص) والمجموعات (المجموعات) واستيرادهم إلى ملف تعريف LDAP. يتطلب هذه كلمة مرور حساب "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
```

```
test@test:~$ cat <<EOF > ./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
test@test:~$
test@test:~$ sudo ldapadd -xcWD  cn=admin,dc=xxxxxxxxx,dc=com  -f ./ldap.ou.add.ldif
Enter LDAP Password:
adding new entry "ou=People,dc=xxxxxxxxx,dc=com

adding new entry "ou=Groups,dc=xxxxxxxxx,dc=com

test@test:~$
```

قم بإنشاء المستخدمين (testuser1، testuser2 و bind_user)، وتخطيطهم إلى وحدات التحكم (مهارسة جيدة)، gidNumber باستخدام مجموعاتهم وإضافتهم إلى (People)، الخاصة بهم. واستيراد المستخدمين إلى ملف تعريف 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:~$
```

قم بإنشاء المجموعات (وه)، وتخطيطه إلى وحدات التحكم الخاصة به (المجموعات)، وأعضاء المجموعة المشاركة (testuser1، testuser2)، واستيراده إلى ملف تعريف 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
```

ملاحظة: حتى إذا لم يتم تعريف السمة memberOf بشكل صريح أثناء إنشاء المستخدمين أو المجموعات، فإن النظام يقوم تلقائيا بإنشاء هذا المرجع والاحتفاظ به. بمجرد اقتران المستخدم بمجموعة ما، تعكس سمة عضو Of هذه العضويات تلقائيا، مما يضمن بقاء الدليل متزامنا مع بنية الوصول الحالية.

الخطوة 6: إختبار تسجيل دخول LDAP المحلي

تحقق من تسجيل دخول المستخدم إلى خادم LDAP باستخدام الأمر المحدد (إستبدال معلمات تسجيل الدخول حسب البيئة الخاصة بك):

```
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:~$
```

مع‌لمات الت‌كوي‌ن ع‌لى CIMC

قم بت‌سجي‌ل الدخول إلى CIMC.

في جزء الت‌نق‌ل، حدد Admin وإدارة الم‌س‌تخدم و LDAP.

م‌لء مع‌لمات ت‌كوي‌ن LDAP ك‌ما ه‌و م‌وض‌ح أدن‌اه:

- ت‌مك‌ي‌ن LDAP: م‌حدد
- ش‌بك‌ة DN الأس‌اس‌ي‌ة: dc=xxxxxxx،dc=com

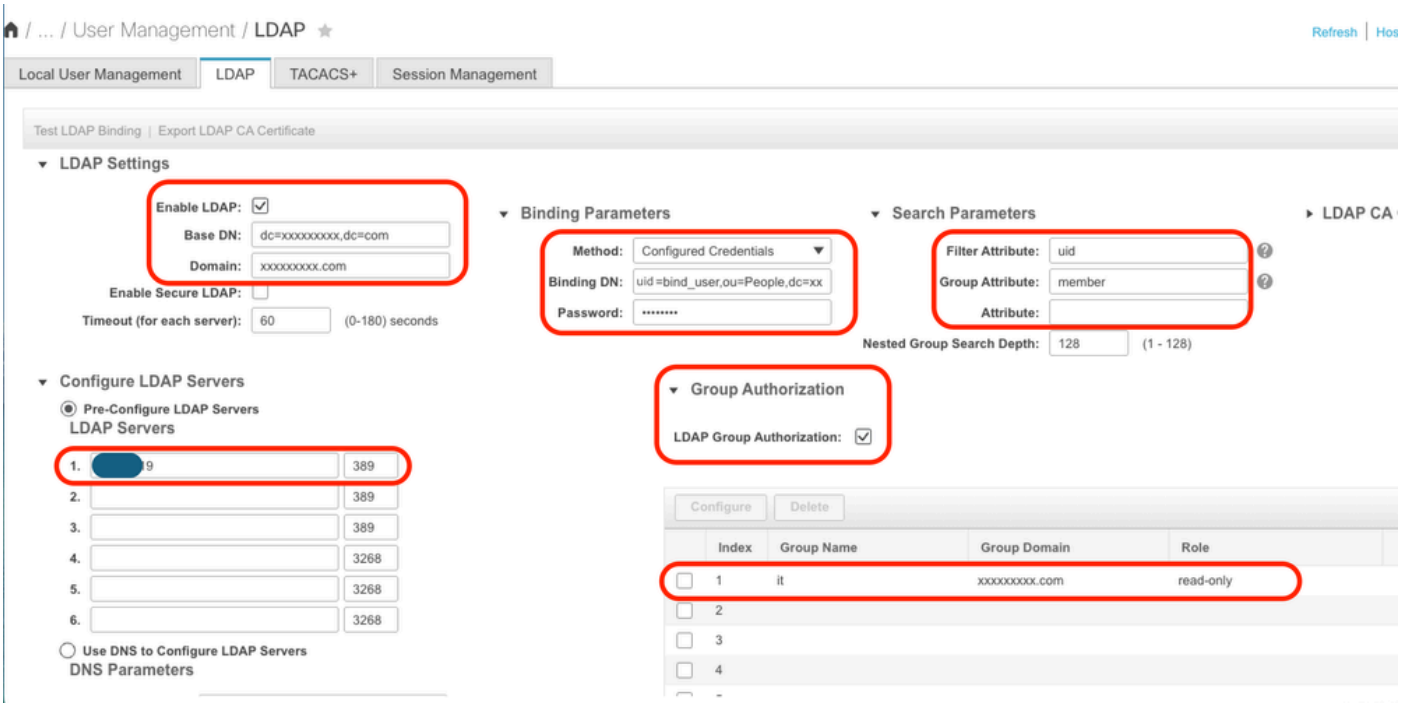
- الم‌جال: xxxxxxxxx.com

- خ‌وادم LDAP: <ldap_server_ip أو FQDN> X.X.19

- ربط الم‌ع‌لمات: ق‌د ت‌ك‌ون "ب‌ي‌ان‌ات اع‌ت‌م‌اد ت‌س‌جي‌ل الدخول" أو "ب‌ي‌ان‌ات اع‌ت‌م‌اد ت‌م ت‌كوي‌ن‌ه‌ا"
  - عند إس‌ت‌خ‌دام ب‌ي‌ان‌ات الاع‌ت‌م‌اد الت‌ي ت‌م ت‌كوي‌ن‌ه‌ا، ق‌م بإض‌اف‌ة DN bind_user ك‌م‌ا ت‌م ت‌كوي‌ن‌ه ت‌م‌ام‌ا ع‌لى خ‌ادم LDAP:
  - م‌ث‌ال: "cn=bind_user، ou=People، dc=xxxxxxx، dc=com" أو "uid=bind_user، ou=People، dc=xxxxxxx، dc=com"

- مع‌لمات الب‌ح‌ث:
  - س‌م‌ة ع‌ام‌ل الت‌ص‌في‌ة: "cn" أو "uid"
  - س‌م‌ة الم‌جم‌وع‌ة: ع‌ض‌و

- ت‌ف‌وي‌ض م‌جم‌وع‌ة LDAP - ت‌م الت‌ح‌ق‌ق
  - اس‌م الم‌جم‌وع‌ة: ت‌ق‌ن‌ي‌ة مع‌ل‌وم‌ات
  - م‌جال الم‌جم‌وع‌ة: xxxxxxxxx.com
  - الدور: ل‌لق‌راءة ف‌ق‌ط (أي دور م‌ف‌ض‌ل)



قم بحفظ التكوين واختبار تسجيل دخول مستخدم LDAP.

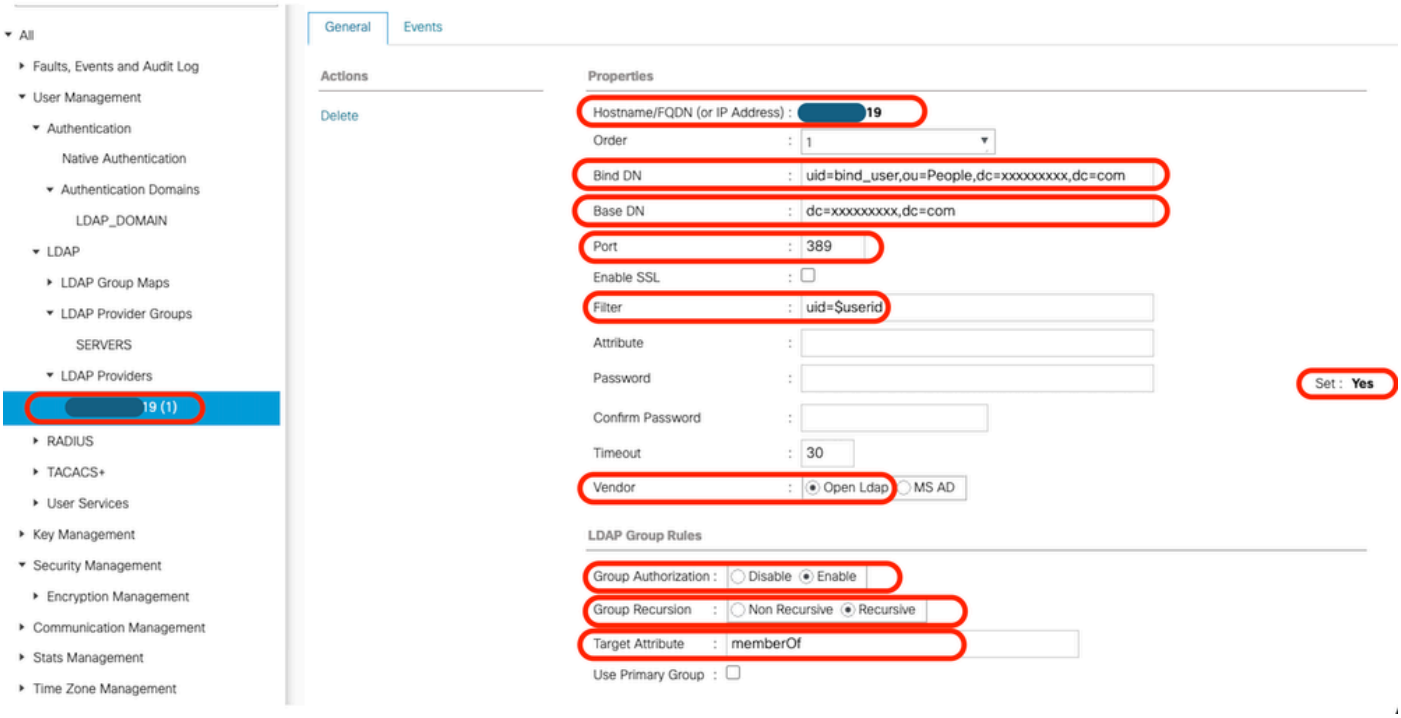
معلمات التكوين على مدير UCS

قم بتسجيل الدخول إلى مدير UCS.

في جزء التنقل، حدد Admin وإدارة المستخدم و LDAP.

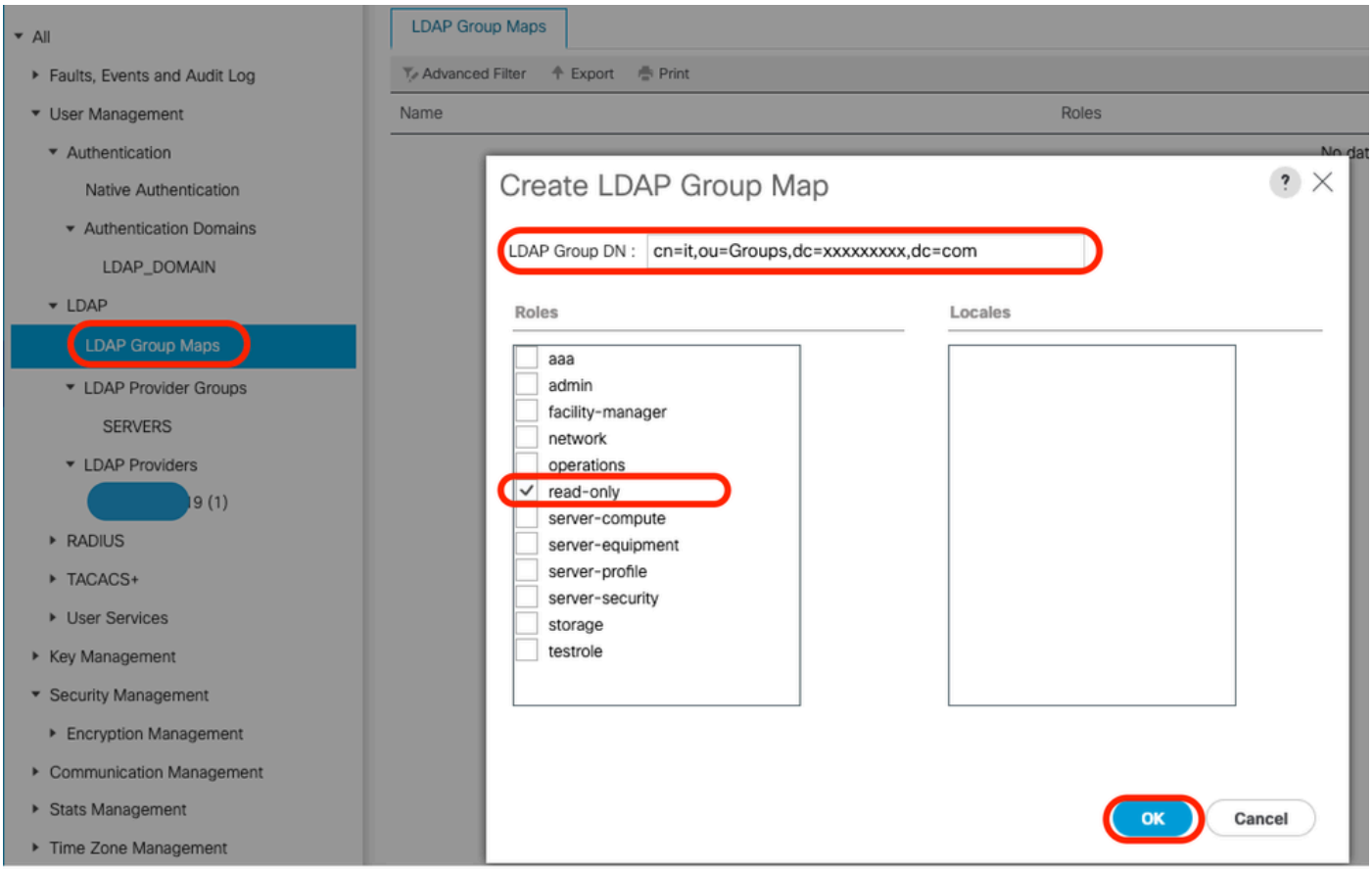
لملء معلمات تكوين LDAP كما هو موضح أدناه:

- موفر LDAP:
  - اسم المضيف: <FQDN أو عنوان IP الخاص بخادم LDAP>
  - ربط DN: uid=bind_user، ou=People، dc=xxxxxxx، dc=com
  - شبكة DN الأساسية: dc=xxxxxxx،dc=com
  - المنفذ: 389
  - تمكين SSL: معطل
  - عامل التصفية: uid=$userID
  - تفويض المجموعة: ممكن
  - تكرار المجموعة: مكرر
  - السمة الهدف: عضو
- خرائط مجموعة LDAP:
  - LDAP Group DN: cn=it،ou=groups،dc=xxxxxx،dc=com



إضافة موفر LDAP الذي تم تكوينه إلى مجموعة موفري LDAP. في هذا العرض التوضيحي، يتم إستخدام مجموعة موفري LDAP "الخوادم".

قم بتكوين خرائط مجموعة LDAP بإضافة "DN لمجموعة LDAP"، التي تم إستردادها من خادم LDAP.



قم بتكوين مجال مصادقة LDAP (LDAP_DOMAIN) في "All>User Management>Authentication>Authentication>Domain (إدارة المستخدم)> Authentication Domain" مشيرا إلى مجموعات موفري LDAP (المداوخ) واختبر تسجيل دخول مستخدم LDAP.

بعد ذلك انظر إلى وضع نفسه (مع التغشية) في توزيع لينوكس مستقل (CentOS 10)

السيناريو الثاني: CentOS Stream 10 - Fedora

تختلف إجراءات تكوين البروتوكول الخفيف للوصول للدليل (LDAP) بناء على إصدار نظام التشغيل الأساسي. يركز هذا القسم على تنفيذ برنامج العمل LDAP على CentOS Stream 10.

على الرغم من أن العديد من برامج لينوكس تستخدم تطبيق OpenLDAP، فإن أنظمة 389) 389 لدليل مداخ تستخدم Fedora إلى المستندة المعاصرة الأنظمة وال CentOS Stream 10 كمزود LDAP الافتراضي (ds.

ملاحظة: على الرغم من أن 389 ديسيبل يعتبر خلفا ل OpenLDAP في نظام Red Hat و CentOS، فإن الحلين ليسا قابلين للتبادل المباشر. وتختلف بنى كل منها في الدليل وملفات التكوين والبيئات التشغيلية إختلافا كبيرا.

يوفر هذا الدليل الخطوات اللازمة لتكوين LDAP بنجاح باستخدام 389 DS داخل بيئة CentOS Stream 10.

الخيار 1: تكوين LDAP باستخدام خادم الدليل 389 على CentOS Stream 10

الخطوة 1: الإعداد الأولي

1. كرر الخطوة 1 في السيناريو 1، الخيار 1.

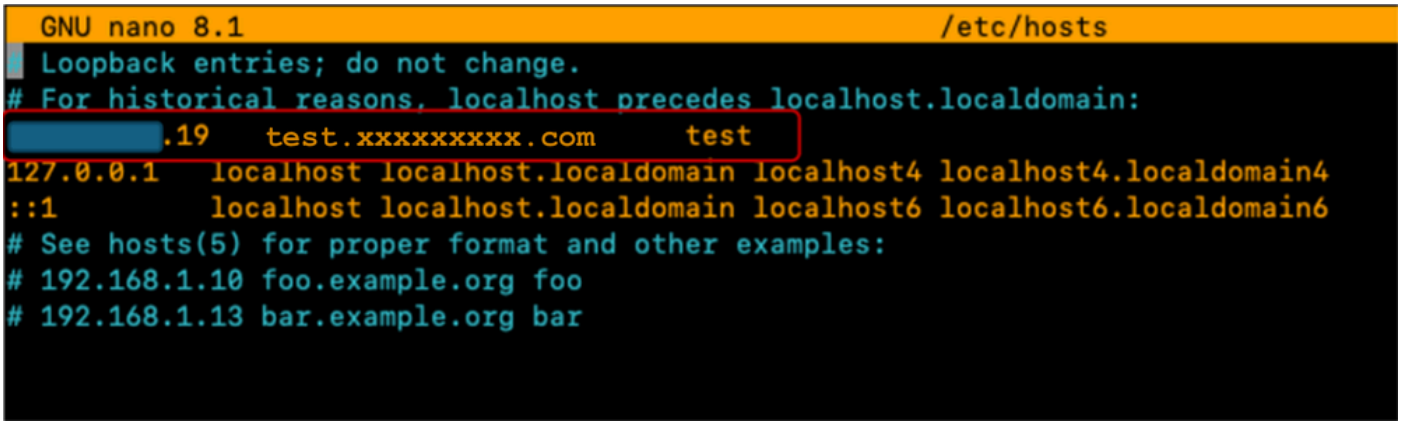
تستخدم أنظمة CentOS مجموعة إدارة حزم APT. لتنفيذ التثبيتات البرمجية الضرورية ال YUM وأ (صالمرقق) DNF (YUM مدير حزم مستخدم، أ CentOS Stream 10 على

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

تحقق من عنوان IP الخاص بالخادم باستخدام الأمر "ifconfig".

قم بإضافة عنوان IP للخادم إلى الملف "/etc/hosts" مع اسم المجال للخادم المؤهل بالكامل (على سبيل المثال: test.xxxxxxxx.com المستخدم في هذا المختبر) واسم المضيف (على سبيل المثال: test) بالتنسيق المحدد أدناه:

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



قم بتحديث الملف "/etc/hostname" عن طريق إستبدال محتوياته باسم المضيف (إختبار).

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

يلزم إعادة تشغيل الخادم حتى تصبح هذه التغييرات نافذة المفعول.

```
sudo reboot
```

الخطوة 2: تثبيت EPEL repo وحزمة الخادم 389

قم بتثبيت مستودع EPEL وتحديثه.

قم بتثبيت حزمة 389 Directory Server.

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

قم بإنشاء ملف قالب دليل يحتوي على معلمات إعدادات خادم LDAP المطلوبة:

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

التحقق من محتوى ملف القالب الذي تم إنشاؤه (ldapconfig.conf)

```
sudo cat ldapconfig.conf
```

قم بتحرير ملف قالب ldapconfig.conf.

```
sudo nano ldapconfig.conf
```

قم بإدراج إدخالات التكوين المحددة في الملف ثم احفظ التغييرات التي أجريتها.

ملاحظة: يمكن طلب تعديلات مختلفة وفقا للاحتياجات أو المتطلبات المحددة لكل بيئة.

يغطي هذا المثال تكوينات خط الأساس لهذا العرض التوضيحي.

```
[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
```

يحدد ملف القالب معلمات التكوين لمثيل الدليل "localhost". ويتضمن ذلك تعيين المستخدم الإداري ("admin") وكلمة المرور المقترنة وسياق المجال ("xxxxxxxx.com").

قم بإنشاء مثيل الدليل "localhost" باستخدام القالب الذي تم تحريره مسبقا. يقوم الأمر المحدد بإنشاء خادم دليل LDAP وتشغيله:

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

التحقق من تشغيل خدمة LDAP على الخادم

```
ss -ntl
```

```
test@test:~$ ss -ntl
State          Recv-Q         Send-Q                 Local Address:Port                  Peer Address:Port
LISTEN         0              128                          0.0.0.0:22                         0.0.0.0:*
LISTEN         0              4096                       127.0.0.1:631                        0.0.0.0:*
LISTEN         0              128                             [::]:22                            [::]:*
LISTEN         0              128                              *:389                              *:*
LISTEN         0              128                              *:636                              *:*
LISTEN         0              4096                             *:9090                             *:*
LISTEN         0              4096                         [::1]:631                          [::]:*
test@test:~$
```

ضبط جدار حماية CentOS للسماح بالمنفذ (المنافذ) المطلوب ل LDAP (389 و/أو 636).

لهذا العرض التوضيحي، تم إيقاف تشغيل جدار الحماية.

```
sudo systemctl stop firewalld
```

تحقق من عمل LDAP محليا على خادم LDAP من خلال تشغيل الأمر المحدد وضمان إرجاعه إخراج LDAP كما هو موضح:

```
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
```

يحتوي الإخراج على حسابات توضيحية تم إنشاؤها بواسطة خادم 389DS. قام خادم LDAP تلقائيا بإنشاء وحدات OUs الافتراضية.

الأشخاص الذين تم إستخدامهم للمستخدمين والمجموعات التي تعمل بها للمجموعات. يمكن إنشاء وحدات ذاكرة مؤقتة إضافية وفقا للمتطلبات.

في هذا العرض التوضيحي، يتم إستخدام وحدات التحكم الافتراضية/التي تم إنشاؤها تلقائيا.

تحقق من [وثائق 389DS الرسمية](#) للحصول على تفاصيل حول الاستخدام الموسع لحزمة 389DS:

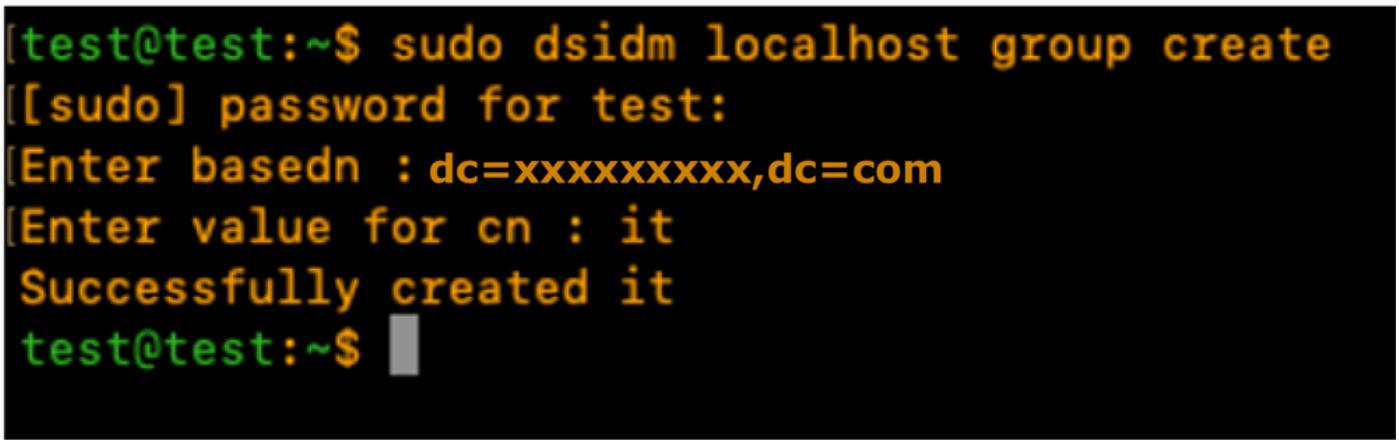
الخطوة 3: إنشاء مجموعات LDAP والمستخدمين

قم بإنشاء مجموعة (ه) باستخدام الأمر المحدد: إنشاء مجموعة SUDO dIDm <instance_name>.

بالنسبة لهذا العرض التوضيحي، اسم المثيل هو "localhost".

```
sudo dsidm localhost group create
```

أدخل مطالبة الوحدة الطرفية لنشر تفاصيل المجموعة كما هو موضح:



خلقت testuser1 مستعمل حساب يستعمل الأمر:

```
sudo dsidm localhost user create
```

أدخل مطالبة الوحدة الطرفية لنشر تفاصيل المستخدم كما هو موضح

```
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
```

قم بإنشاء كلمة مرور لـ testuser1 باستخدام الأمر المحدد وأدخل مطالبة 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:~$
```

إضافة المستخدم إلى مجموعة باستخدام الأمر المحدد: "sudold <directory_instance> group add_member <group_cn> <user_dn>"

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

كرر خطوات إنشاء المستخدم لإنشاء testuser2 و bind_user.

ملاحظة:تأكد من إضافة كل مستخدم بشكل صريح إلى مجموعاتهم المقصودة.

قد يؤدي حذف هذه الخطوة إلى تقييد الوصول أو فشل التخويل.

لا يلزم أن يكون حساب bind_user عضوا في مجموعة معينة، حيث يمكن تكوينه كحساب مستقل، مما يوفر المرونة لإدارة الوصول الإداري والوصول على مستوى الخدمة داخل بيئة الدليل.

إعادة تشغيل مثيل الدليل:

```
sudo dsctl localhost restart
```

الخطوة 4: تثبيت تغشية العضو

قم بتثبيت المكون الإضافي "memberOf" ثم أعد تشغيل مثيل الدليل:

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

قم بتكوين الوظيفة الإضافية "memberOf" باستخدام الأمر المحدد: "عضوية الوظيفة الإضافية ل Sudo dsconf <directory_instance> مجموعة —scope <base_dn>"

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

وضع علامة على "المستخدمين" كأهداف "memberOf" صالحة باستخدام الأمر المحدد: "يقوم SudoSidm بواسطة add:objectclass:nsmemberOf <uid> لتعديل المستخدم <directory_instance>

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

```
[test@test:~$ sudo dsidm localhost user modify testuser1 add:objectclass:nsmemberof
[Enter basedn : dc=xxxxxxxxx,dc=com
Successfully modified uid=testuser1,ou=people, dc=xxxxxxxxx,dc=com
[test@test:~$ sudo dsidm localhost user modify testuser2 add:objectclass:nsmemberof
[Enter basedn : dc=xxxxxxxxx,dc=com
Successfully modified uid=testuser2,ou=people,dc=xxxxxxxxx,dc=com
[test@test:~$
```

إنشاء إصلاح "memberOf" ل DN الأساسي: "عضو الوظيفة الإضافية ل <directory_instance> من الإصلاح <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:~$
```

التحقق من تكوين المستخدم:

```
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:~$
```

تم تكوين خادم 389DS LDAP باستخدام المكون الإضافي للعضو لدعم السمة memberOf.

معلمات التكوين على CIMC

قم بتسجيل الدخول إلى CIMC.

في جزء التنقل، حدد Admin وإدارة المستخدم و LDAP.

مثال على معلومات تكوين LDAP كما هو موضح أدناه:

- تمكين LDAP: محدد
- شبكة DN الأساسية: dc=xxxxxxx،dc=com

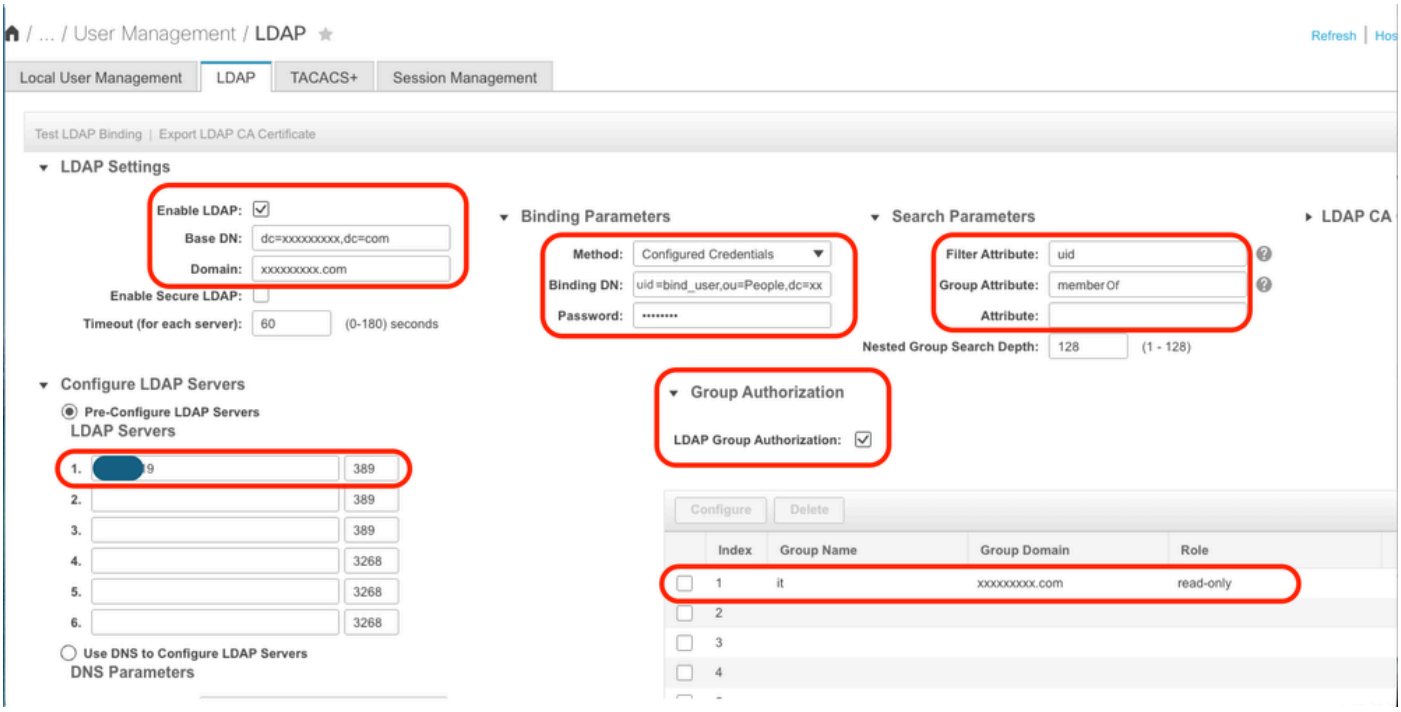
- المجال: xxxxxxxxx.com

- خوادم LDAP: <ldap_server_ip أو FQDN> X.X.19

- ربط المعلومات: قد تكون "بيانات اعتماد تسجيل الدخول" أو "بيانات اعتماد تم تكوينها"
  - عند إستخدام بيانات الاعتماد التي تم تكوينها، قم بإضافة DN bind_user كما تم تكوينه تماما على خادم LDAP:
    - مثال: "cn=bind_user، ou=People، dc=xxxxxxx، dc=com" أو "uid=bind_user، ou=People، dc=xxxxxxx، dc=com"

- معلومات البحث:
  - سمة عامل التصفية: "cn" أو "uid"
  - سمة المجموعة: عضو

- تفويض مجموعة LDAP - تم التحقق
  - اسم المجموعة: تقنية معلومات
  - مجال المجموعة: xxxxxxxxx.com
  - الدور: للقراءة فقط (أي دور مفضل)



قم بحفظ التكوين واختبار تسجيل دخول مستخدم LDAP.

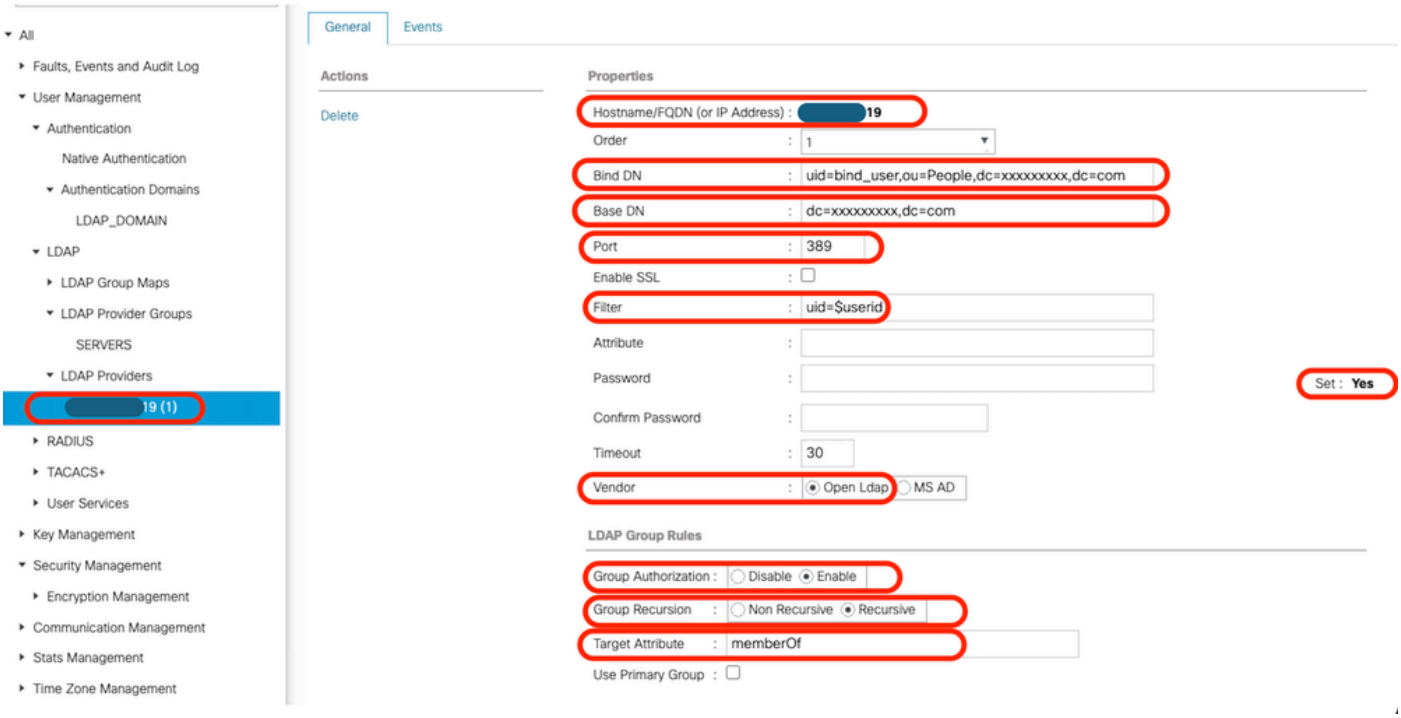
مع المات التكوين على مدير UCS

قم بتسجيل الدخول إلى مدير UCS.

في جزء التنقل، حدد Admin وإدارة المستخدم و LDAP.

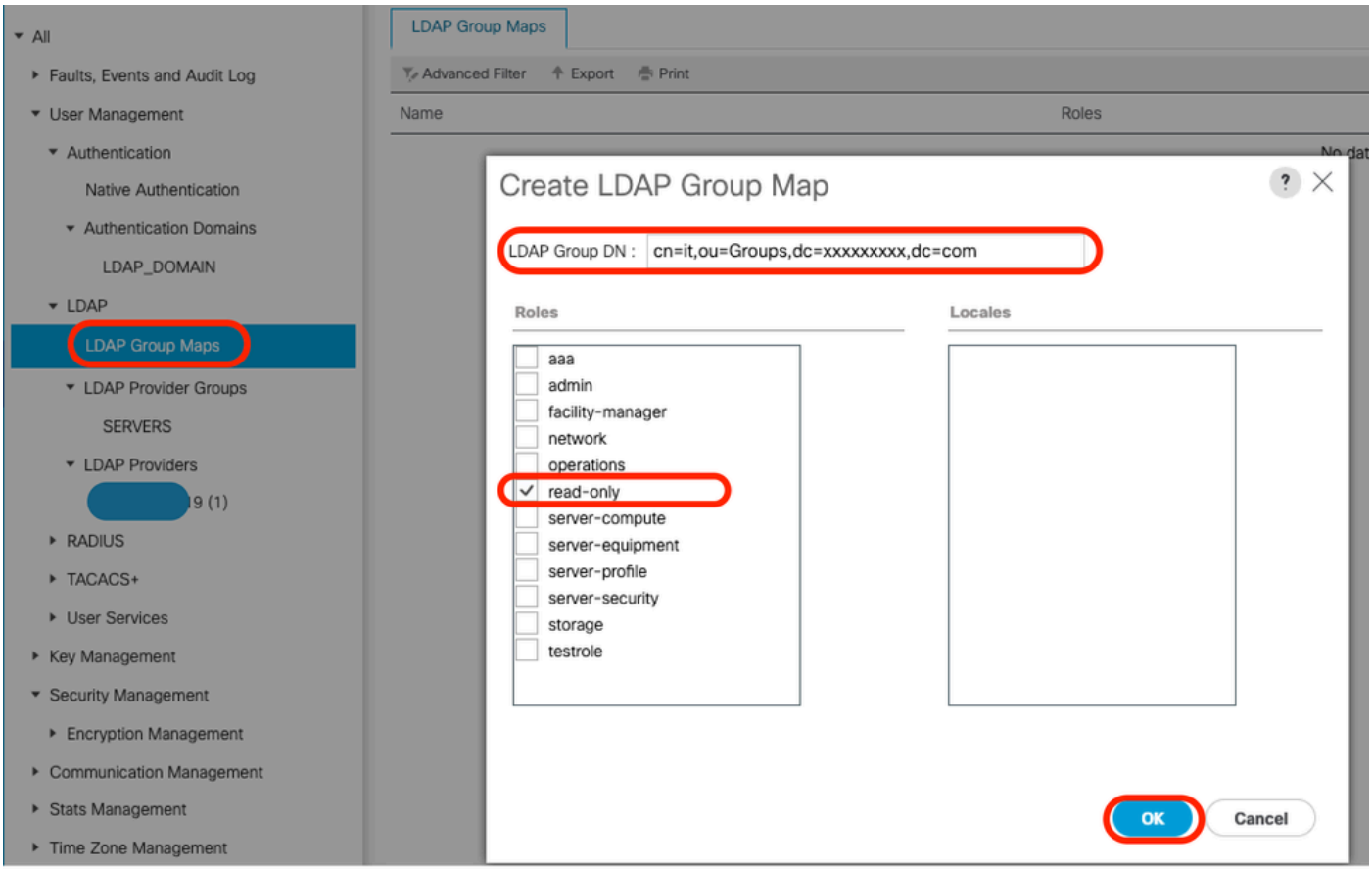
مل مع المات تكوين LDAP كما هو موضح أدناه:

- موفرو LDAP:
  - اسم المضيف: <FQDN أو عنوان IP الخاص بخادم LDAP>
  - ربط DN: uid=bind_user، ou=people، dc=xxxxxxx، dc=com
  - شبكة DN الأساسية: dc=xxxxxxx،dc=com
  - المنفذ: 389
  - تمكين SSL: معطل
  - عامل التصفية: uid=$userID
  - تفويض المجموعة: ممكن
  - تكرار المجموعة: مكرر
  - السمة الهدف: عضو
- خرائط مجموعة LDAP:
  - LDAP Group DN: cn=it،ou=groups،dc=xxxxxx،dc=com



إضافة موفر LDAP الذي تم تكوينه إلى مجموعة موفري LDAP. في هذا العرض التوضيحي، يتم إستخدام مجموعة موفري LDAP "الخوادم".

قم بتكوين خرائط مجموعة LDAP بإضافة "DN لمجموعة LDAP"، التي تم إستردادها من خادم LDAP.



قم بتكوين مجال مصادقة LDAP (LDAP_DOMAIN) في "All>User Management>Authentication>> Authentication Domain (إدارة المستخدم)> Authentication Domain" مشيرا إلى مجموعات موفر LDAP واختبار تسجيل دخول مستخدم LDAP.

القرار

وفي حين أن هذا الدليل يغطي سيناريوهات النشر الأساسية، فإن المزيد من أستكشاف قدرات LDAP يمكن أن يعزز بشكل كبير أداء الدليل وأمنه.

للحصول على معلومات إضافية وأفضل الممارسات وتفاصيل التكوين المتقدمة، ارجع إلى الموارد المحددة:

- وثائق OpenLDAP الرسمية
- مدير حساب LDAP - الدليل
- وثائق 389 Directory Server
- تكوين LDAP على مدير UCS
- تكوين LDAP الآمن على خوادم UCS C Series

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).