在UCS Manager上配置LDAP &使用Linux OpenLDAP和389-DS伺服器的CIMC

目錄

簡介

本文檔介紹各種選項，用於使用基於Linux的OpenLDAP和389目錄伺服器將LDAP配置為UCS Manager和CIMC的身份驗證方法。

背景資訊

由於OpenLDAP伺服器配置具有廣泛的可變性，詳盡的處理超出了本文檔的範圍。本文重點介紹跨多個Linux發行版、LDAP伺服器包和屬性架構的常見配置。為了清晰和簡單，本文檔介紹了標準LDAP配置。本文檔未介紹安全LDAP(LDAPS)的配置。

必要條件:

強烈建議瞭解以下主題：

- UCS B系列
- UCS C系列
- Linux伺服器管理

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- UCS Manager韌體版本：4.3(2c)
- 交換矩陣互聯型號：UCS-FI-6454
- UCS C系列獨立伺服器型號：UCSC-C240-M5
- UCS C系列獨立韌體版本：4.3(2.250045)
- Ubuntu 20.04
- CentOS流10

用於此演示的設定：

- LDAP伺服器主機名：測試
- 伺服器域：xxxxxxxxx.com
- 伺服器FQDN:test.xxxxxxxxx.com
- Linux伺服器（Ubuntu和CentOS）IP地址：X.X.19
- OpenLDAP使用者：testuser1、testuser2

- OpenLDAP組：它
- OpenLDAP繫結使用者帳戶：bind_user

附註：本實驗使用linux Nano文本編輯器。

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

案例 1:烏本圖 — 德比安

LDAP伺服器配置可以使用圖形介面（如LDAP帳戶管理器）或命令列工具執行，具體取決於管理首選項和所需的控制級別。本場景使用基於Linux的OpenLDAP檢查配置，從基於GUI的部署開始，然後過渡到命令列實用程式以探索高級功能，包括重疊外掛（通常用於與Cisco UCS Manager的整合）。

選項 1:使用Ubuntu LDAP帳戶管理器(LAM)配置OpenLDAP

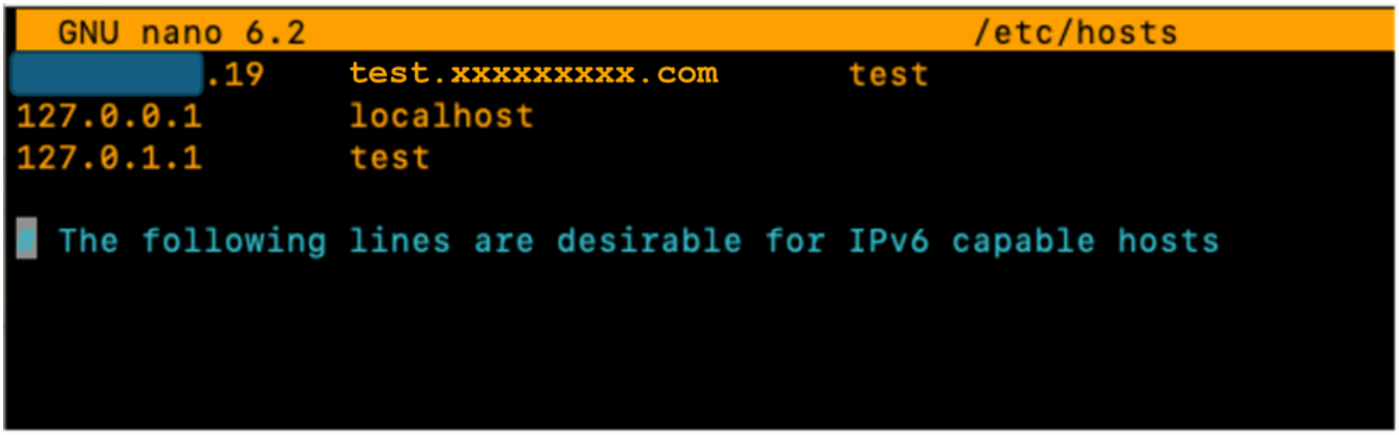
步驟 1:Linux伺服器主機名和網路工具的初始配置。

更新ubuntu並安裝net-tools軟體包以便訪問ifconfig、netstat等工具：

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

使用「ifconfig」命令驗證伺服器IP地址，然後將其與伺服器域名一起新增到「/etc/hosts」檔案中(例如：本實驗中使用的「test.xxxxxxxxx.com」和主機名(例如：「test」)。

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



此外，請更新「/etc/hostname」檔案，方法是將其內容替換為主機名（測試）。

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

需要重新啟動伺服器才能使這些更改生效。

```
sudo reboot
```

第2步：安裝SLAPD、Apache、PHP及其依賴項

接下來，安裝Apache、PHP及其依賴項。這些用於啟用通過網頁的GUI互動：

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

安裝Open LDAP伺服器軟體包「slapd」及其依賴項(ldap-utils)

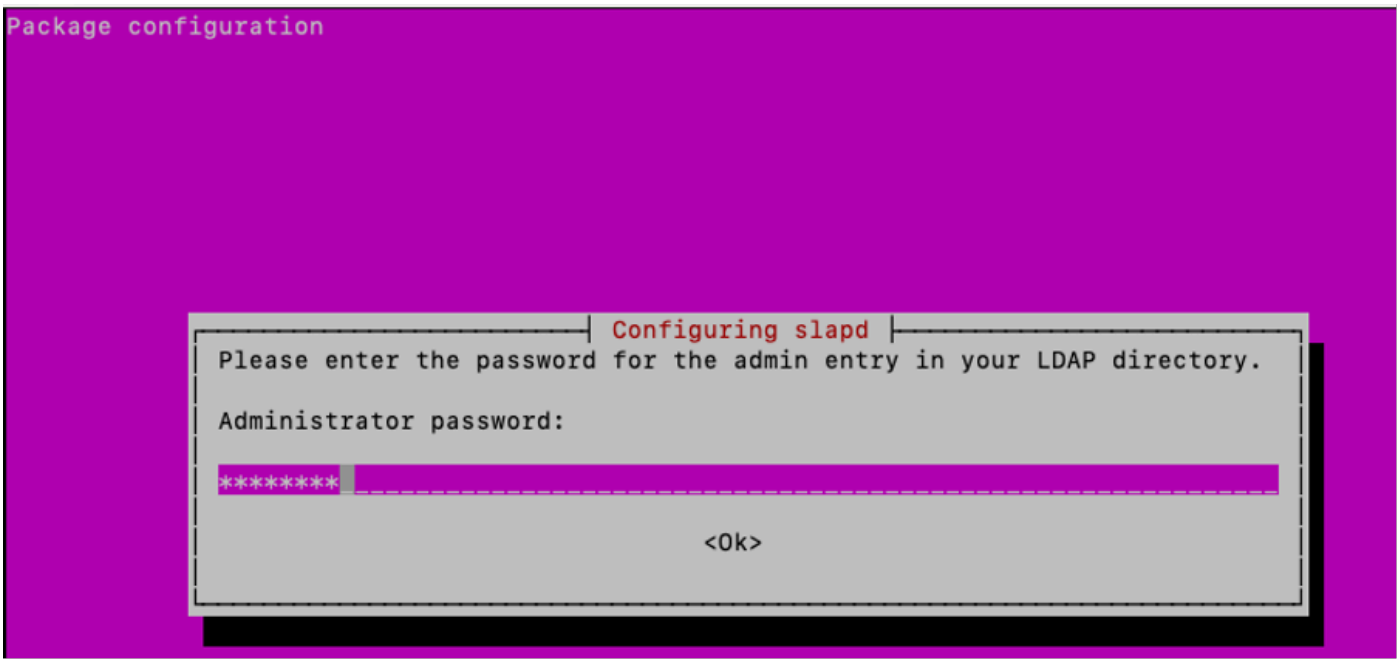
```
sudo apt install slapd ldap-utils -y
```

在安裝slapd的過程中，在顯示的GUI彈出視窗中 — 輸入額外的SLAPD軟體包配置。

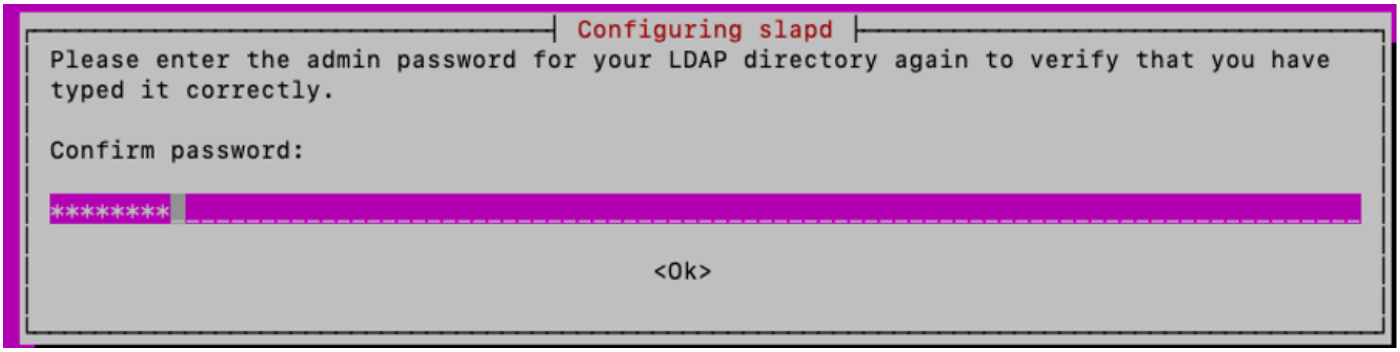
附註：丟失密碼需要重新安裝LDAP伺服器。

此上下文中的「管理員」(admin)是用於管理OpenLDAP服務、模組和配置的帳戶。

新增LDAP包「administrator」密碼，然後按鍵盤上的enter鍵選擇「OK」。



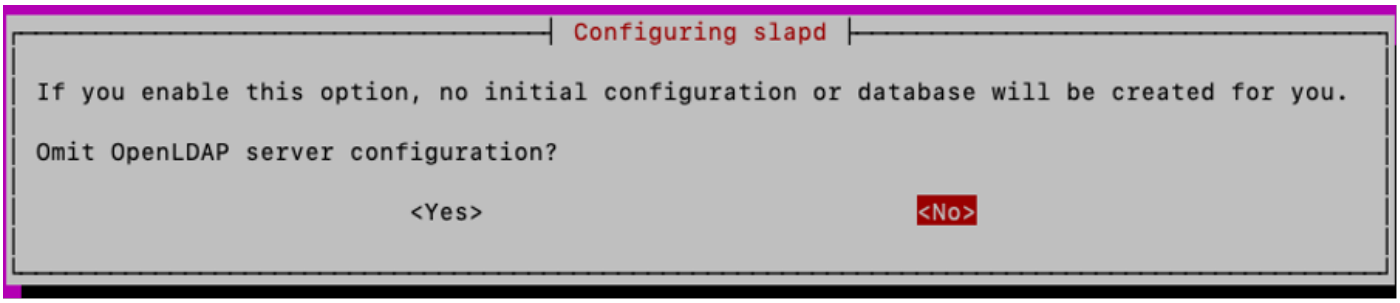
確認密碼：



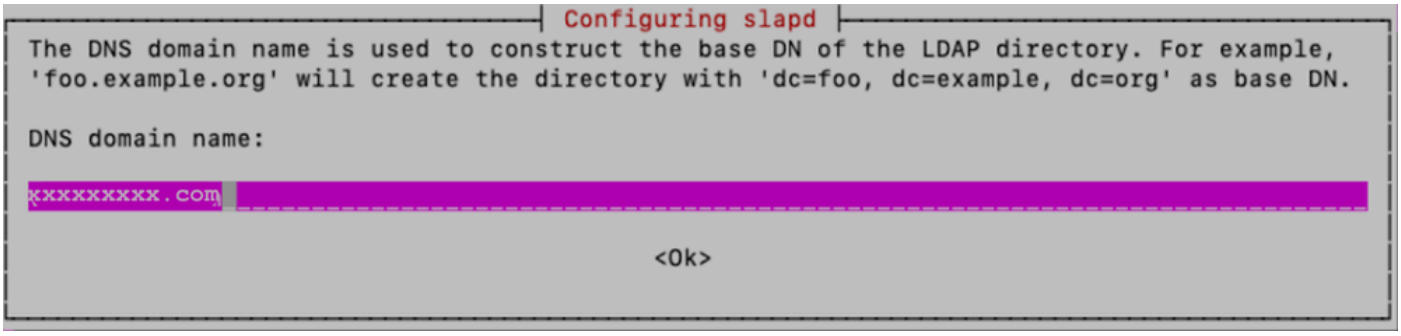
安裝完成後，可以使用指定的命令重新配置SLAPD軟體包，新增域資訊：

```
sudo dpkg-reconfigure slapd
```

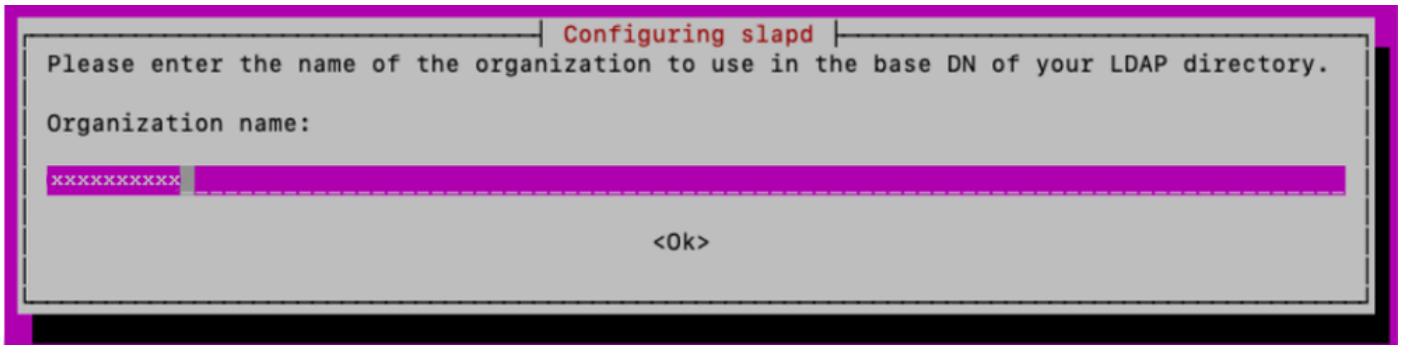
您可以接受「忽略OpenLDAP伺服器配置」的預設「否」選項，然後按下enter:



鍵入域名並按Enter鍵：



在本實驗中，「xxxxxxxxx」用作「組織名稱」：

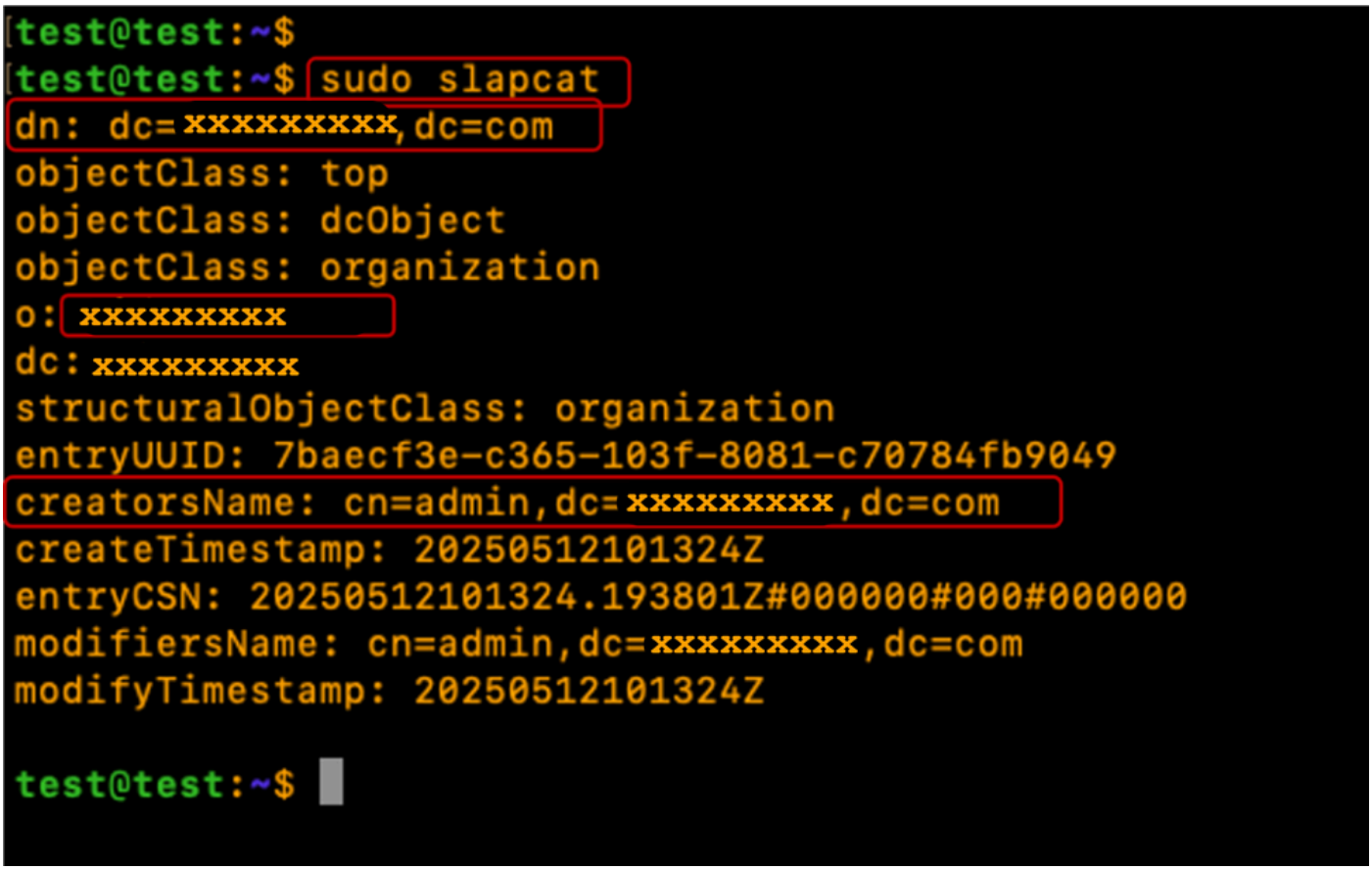


接下來，鍵入「管理員密碼」，確認它

對於其他配置選項，保留預設值並按鍵盤上的Enter鍵完成配置。

使用命令驗證SLAPD安裝：

```
sudo slapcat
```



步驟3：安裝LDAP帳戶管理器

安裝LDAP帳戶管理器(LAM)以建立和管理LDAP使用者和組：

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

啟用LAM所需的PHP-CGI PHP擴展。

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

重新載入Apache以啟用新配置。

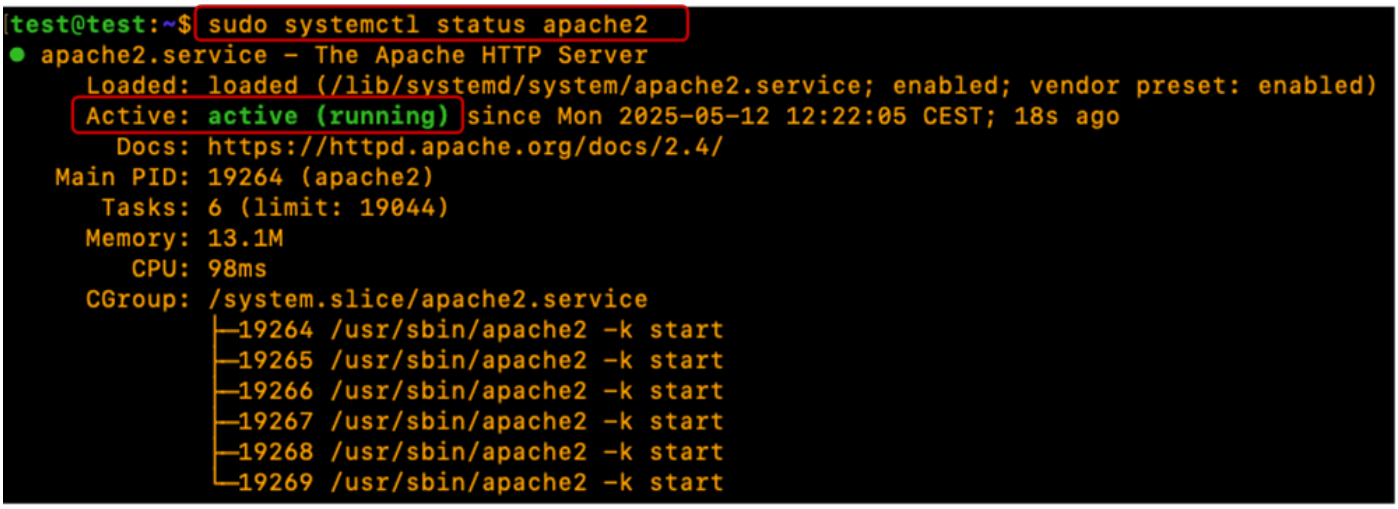
重新啟動並啟用Apache服務以在引導時自動啟動：

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

```
sudo systemctl enable apache2
```

驗證Apache伺服器的狀態為「Running」和「Active」

```
sudo systemctl status apache2
```



配置Ubuntu防火牆以允許埠80(Web)、443（安全Web）、389(LDAP)和636(如果需要，可保護LDAP)

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

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

```
sudo ufw allow 636
```

```
test@test:~$ sudo ufw enable
Command may disrupt existing ssh connections. Proceed with operation (y|n)? y
Firewall is active and enabled on system startup
test@test:~$ sudo ufw allow 22
[sudo] password for test:
Rule added
Rule added (v6)
test@test:~$ sudo ufw allow 80
Rule added
Rule added (v6)
test@test:~$ sudo ufw allow 443
Rule added
Rule added (v6)
test@test:~$ sudo ufw allow 389
Rule added
Rule added (v6)
test@test:~$ sudo ufw allow 636
Rule added
Rule added (v6)
test@test:~$
```

驗證Ubuntu防火牆狀態：

```
sudo ufw status
```

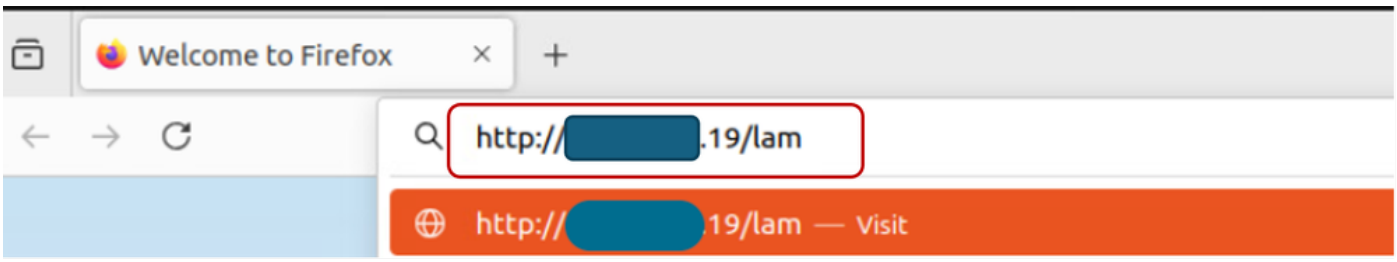
```
test@test:~$ sudo ufw status
Status: active

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)
```

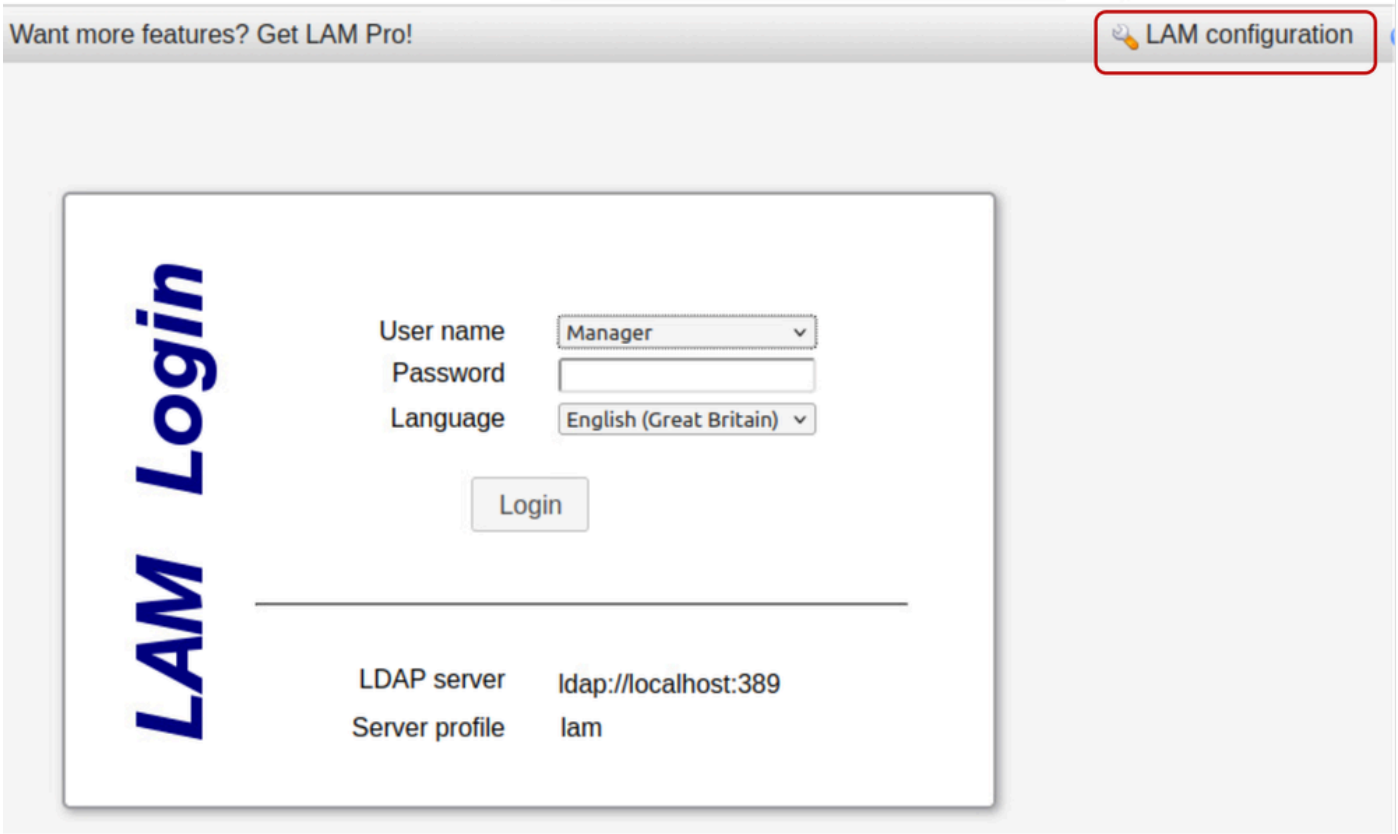
步驟 4: 配置LDAP帳戶管理器

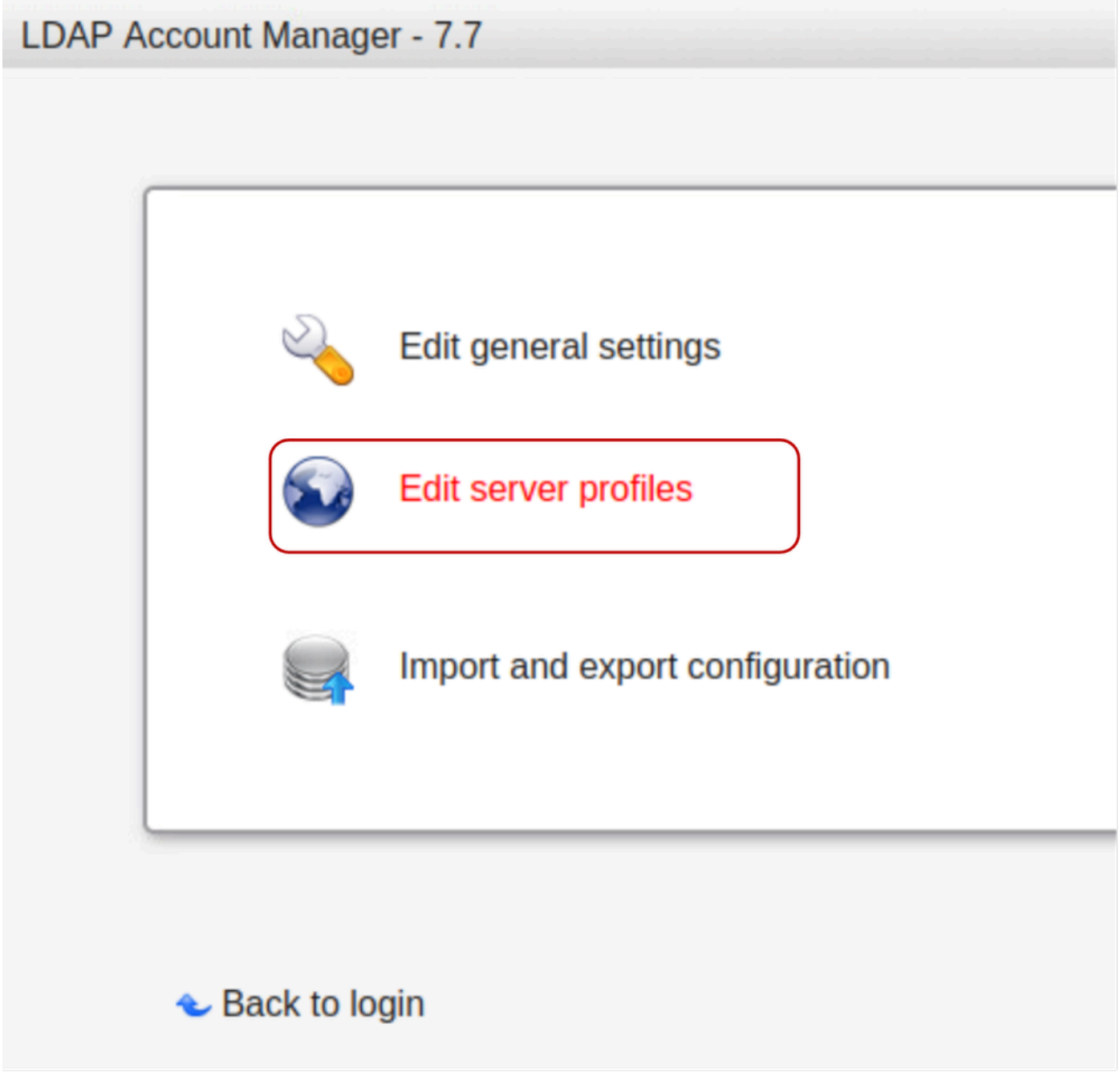
要從GUI配置LDAP帳戶管理器(LAM)，請開啟Web瀏覽器，輸入Linux伺服器IP地址並向其新增「lam」路徑，如下所示：

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

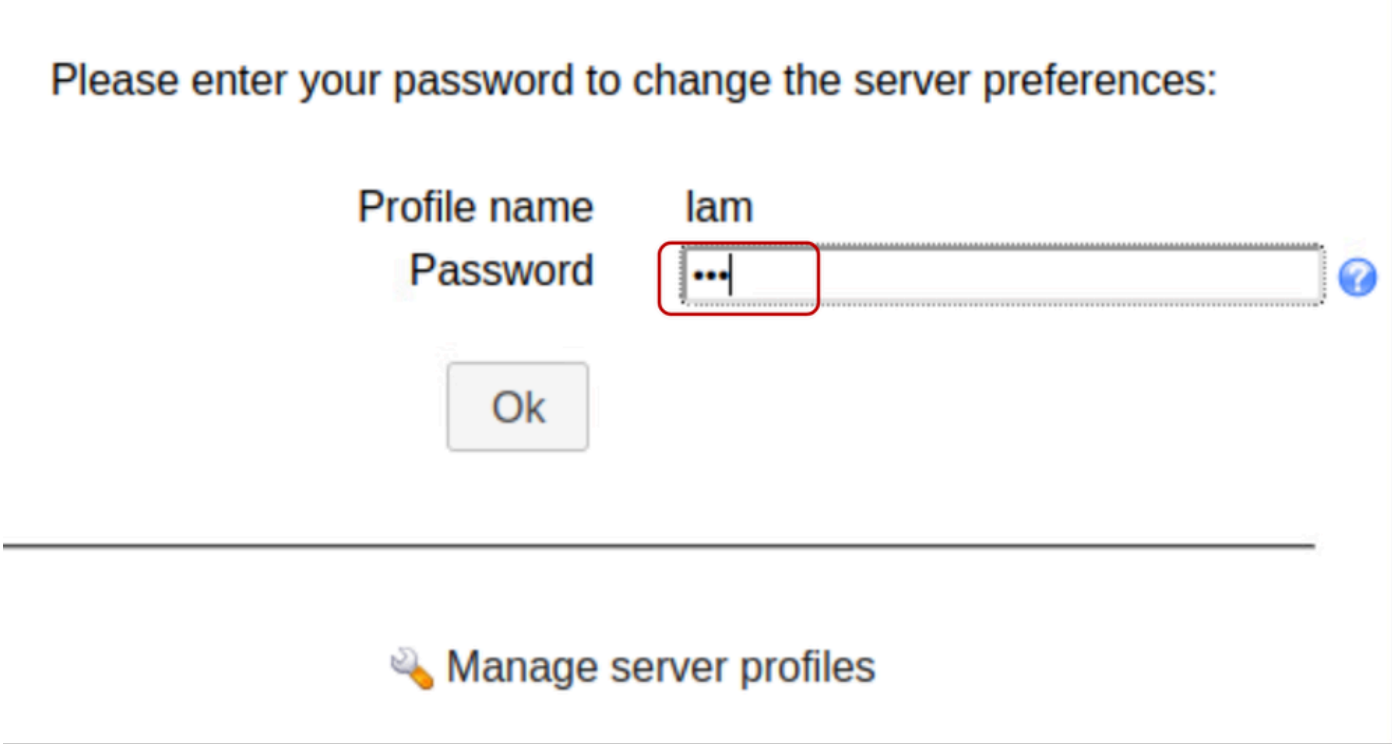


按一下「LAM配置」，然後選擇「編輯伺服器配置文件」。





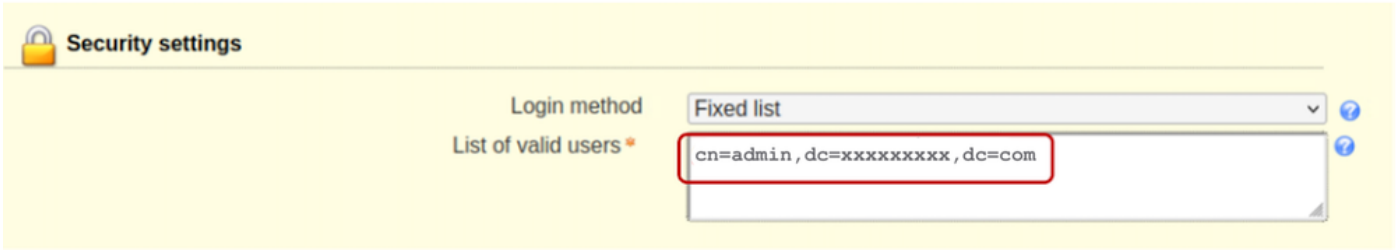
鍵入預設的lam密碼「lam」以登入。



在「常規設定」頁籤中，驗證伺服器設定「語言」和「時區」。

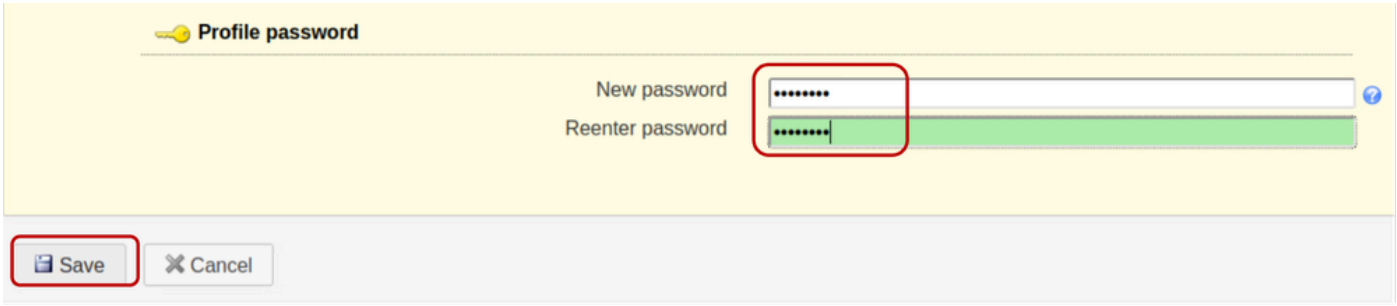
在「工具設定」(Tool settings)部分，編輯並在「樹字尾」(Tree suffix)欄位中新增所需的域名，如下所示：

編輯Security settings部分以包含用於管理SLAPD服務的「admin」使用者。



設定「配置檔案密碼」。此密碼用於後續登入LAM配置介面，例如，配置「cisco123」而不是預設的「lam」密碼。

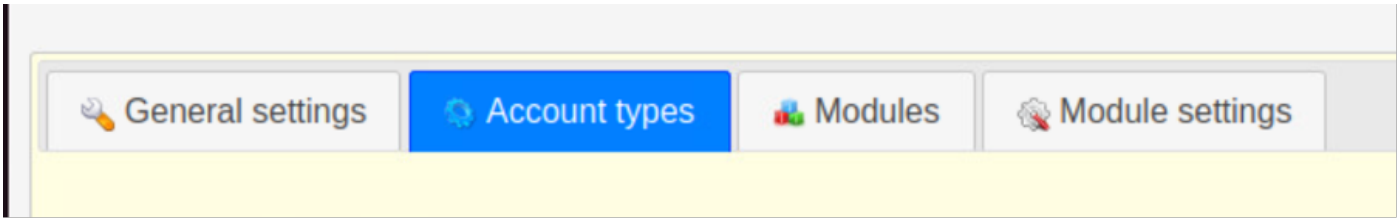
儲存組態：



然後，在LAM配置GUI介面上重新啟動會話。

使用建立的新密碼重新登入（LAM配置>>編輯伺服器配置檔案）。

點選「Account types」（帳戶型別），



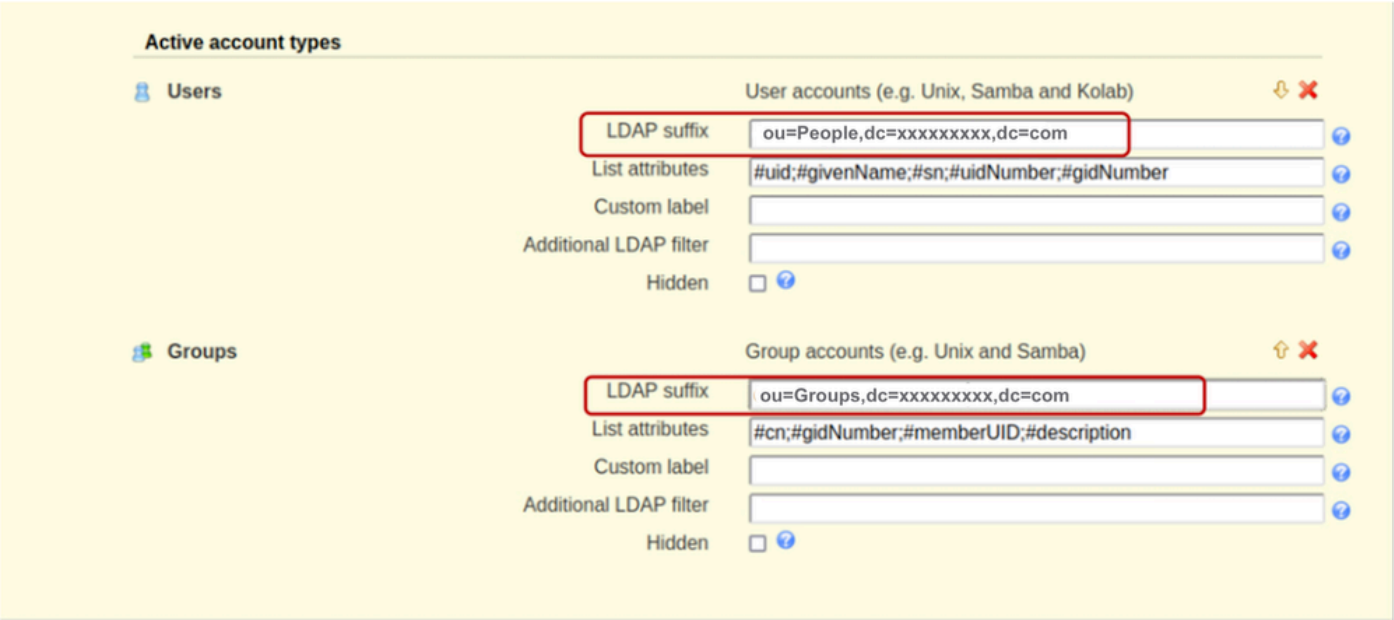
向下滾動並編輯LDAP字尾欄位中包含域名資訊的預設活動帳戶型別。例如，「LDAP字尾」欄位的預設內容顯示值為「ou=People，dc=my-domain，dc=com」。

如果需要建立新的組織單位，請替換「LDAP字尾」欄位的內容以包含組織單位的名稱。

格式顯示為「ou=<organizational_unit>,dc=xxxxxxxxx，dc=com」。

在本演示中，使用者的OU是「People」，組的OU是「Groups」。

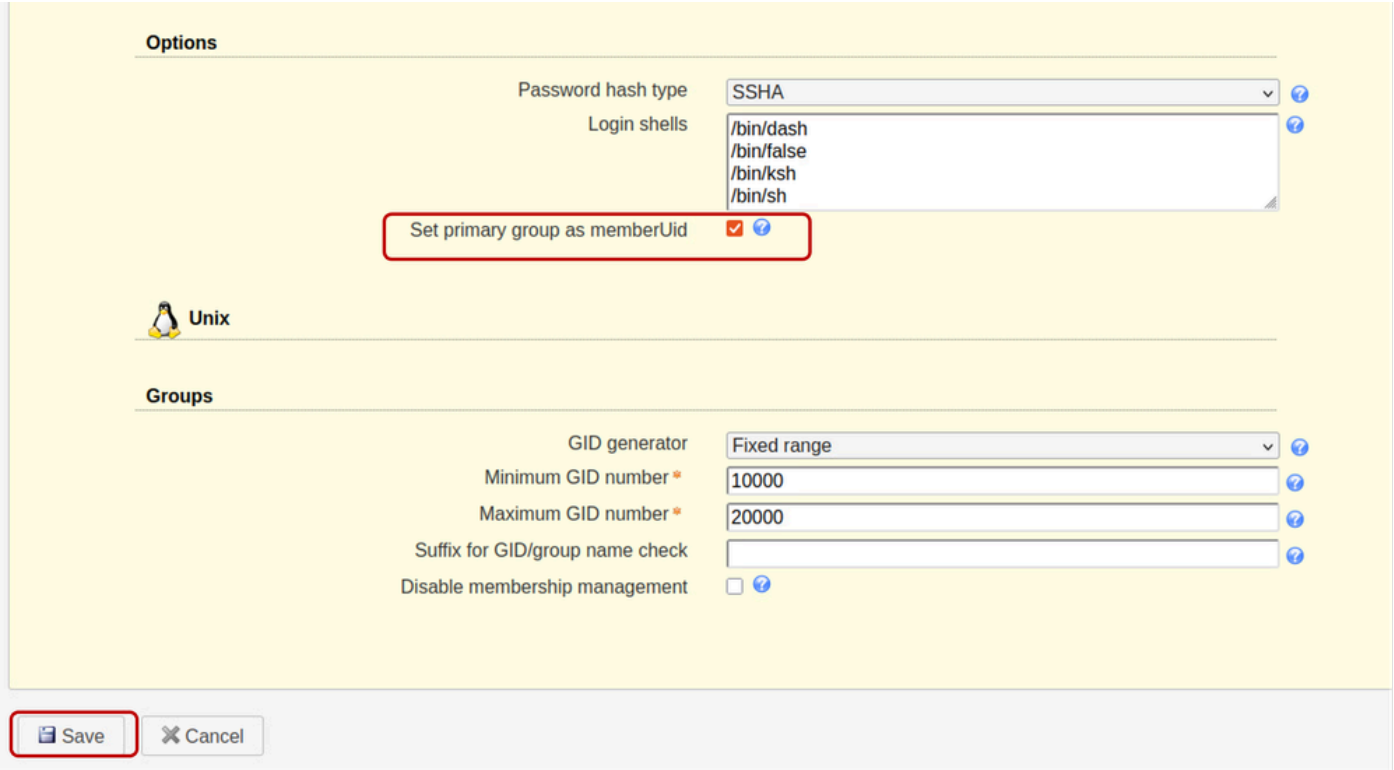
儲存組態。



向下滾動到「選項」部分，確保選中「將主組設定為memberUid」。

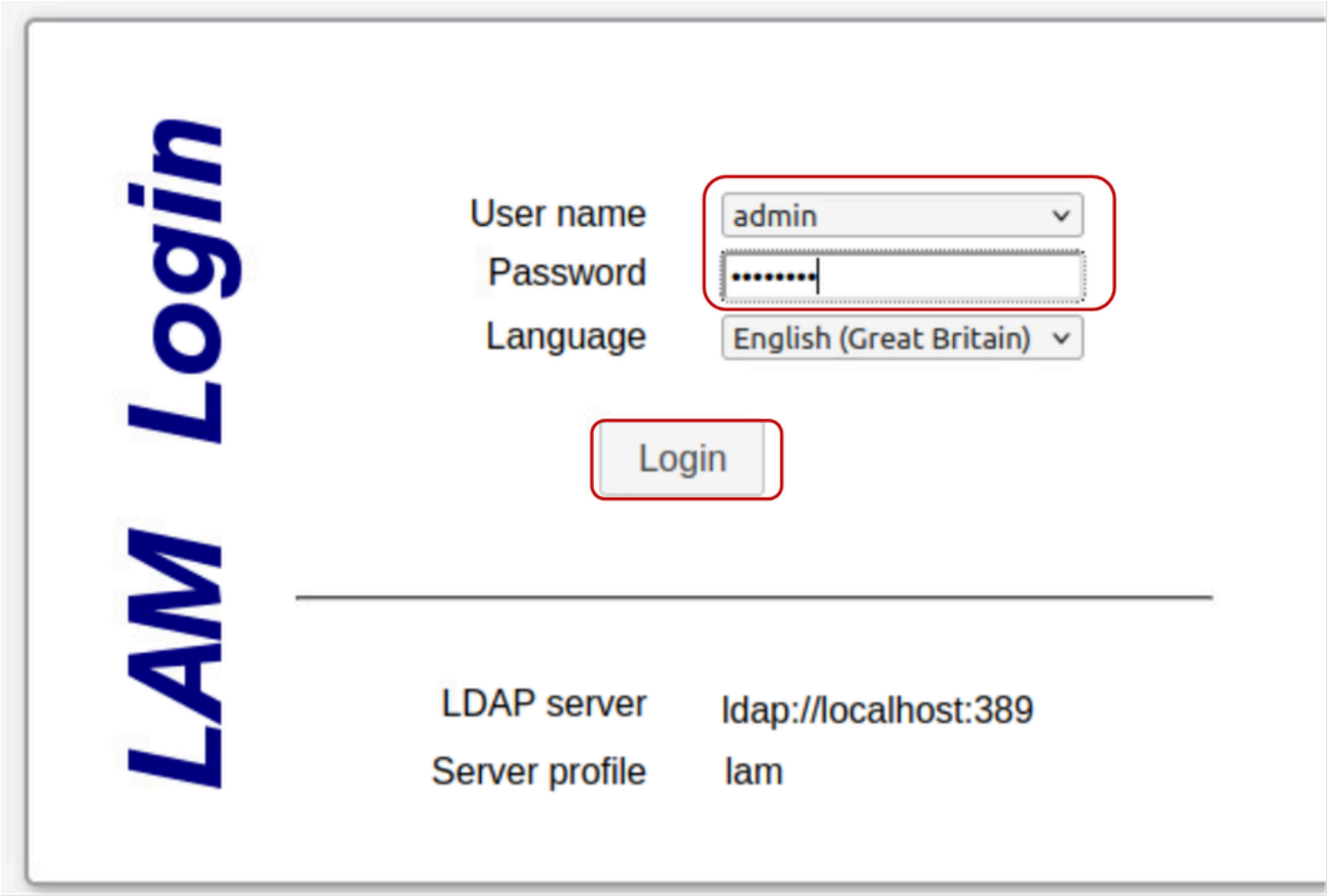
預設情況下，未對組對象設定「將主組設定為memberUid」選項。通過啟用此項，可以像標準LDAP組那樣使用OpenLDAP「主組」，在該組中可以引用「memberUid」(例如：在UCS C系列伺服器配置中)。 如果未選中此選項，則屬於任何主要組的使用者的登入將失敗。

儲存組態。

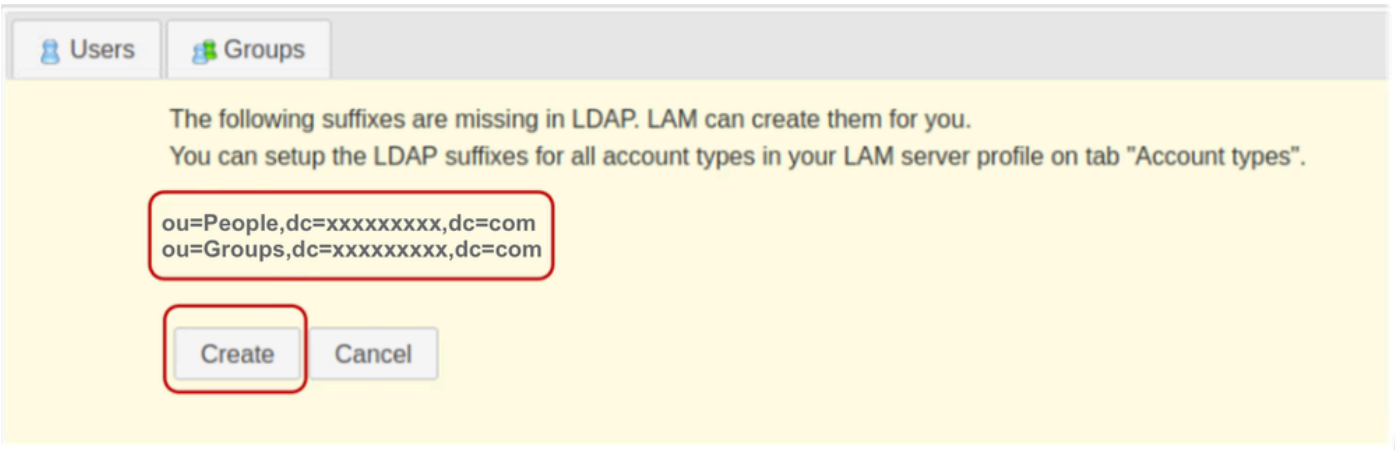


第5步：建立OU、組和使用者

以「admin」使用者身份登入LAM，使用在安裝期間建立的相同密碼，分別建立屬於先前建立的OU(People和Groups)的Users和Groups:

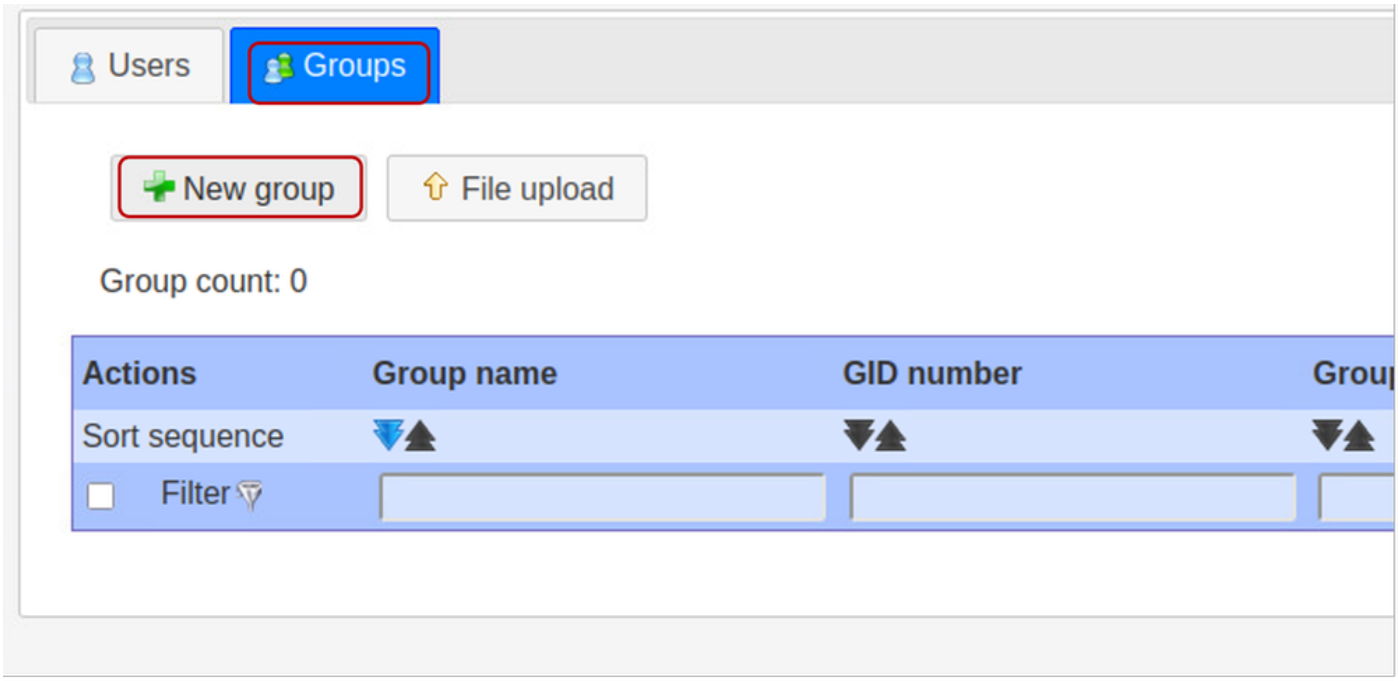


在LAM配置部分建立較早指定的OU。
按一下「建立」。



接下來，在LDAP客戶管理器中建立「it」組：

選擇「組」頁籤，然後按一下「新建組」

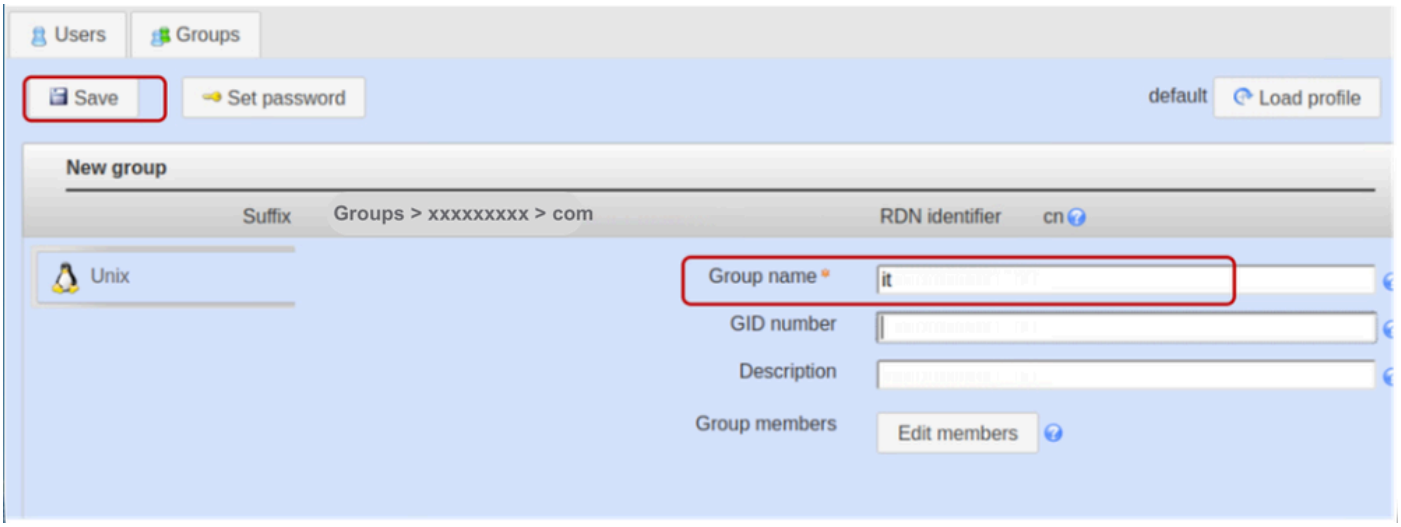


將組名稱設定為「it」。

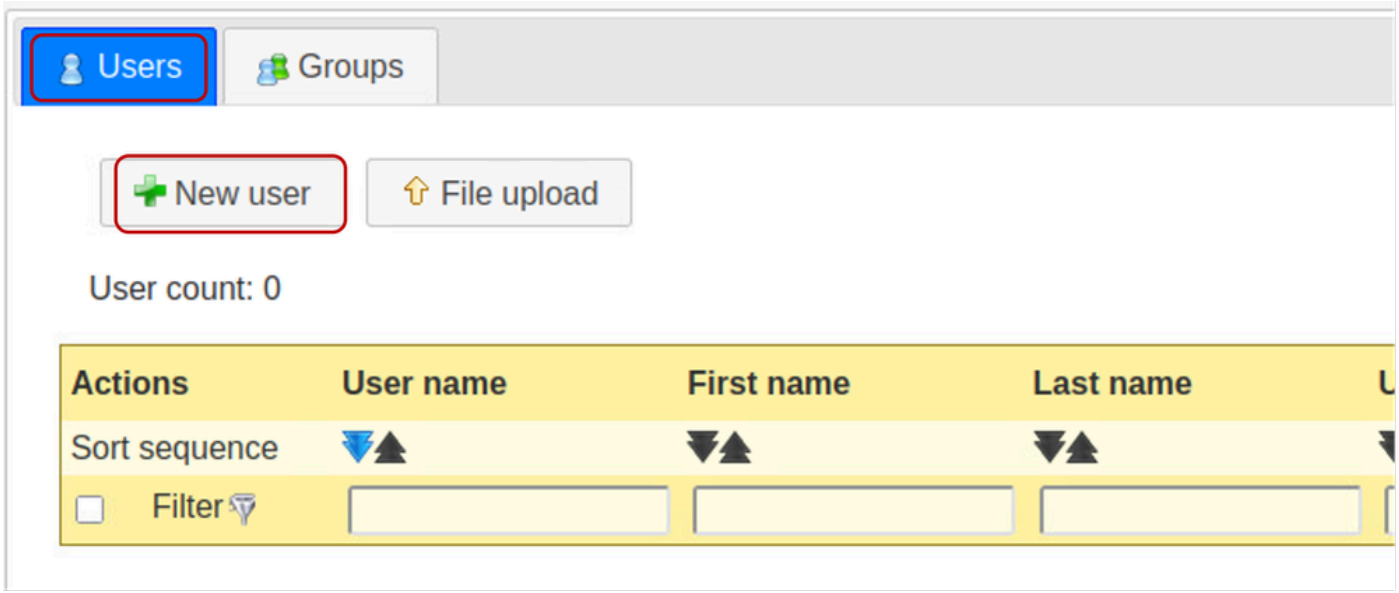
附註：儘管Cisco UCS系統通常可恢復大小寫變化，但保持小寫命名約定是確保不同LDAP伺服器基礎設施環境之間長期互操作性的最佳實踐。

將GID編號欄位留空。LDAP Account Manager(LAM)設計為使用下一個可用值自動填充此欄位。

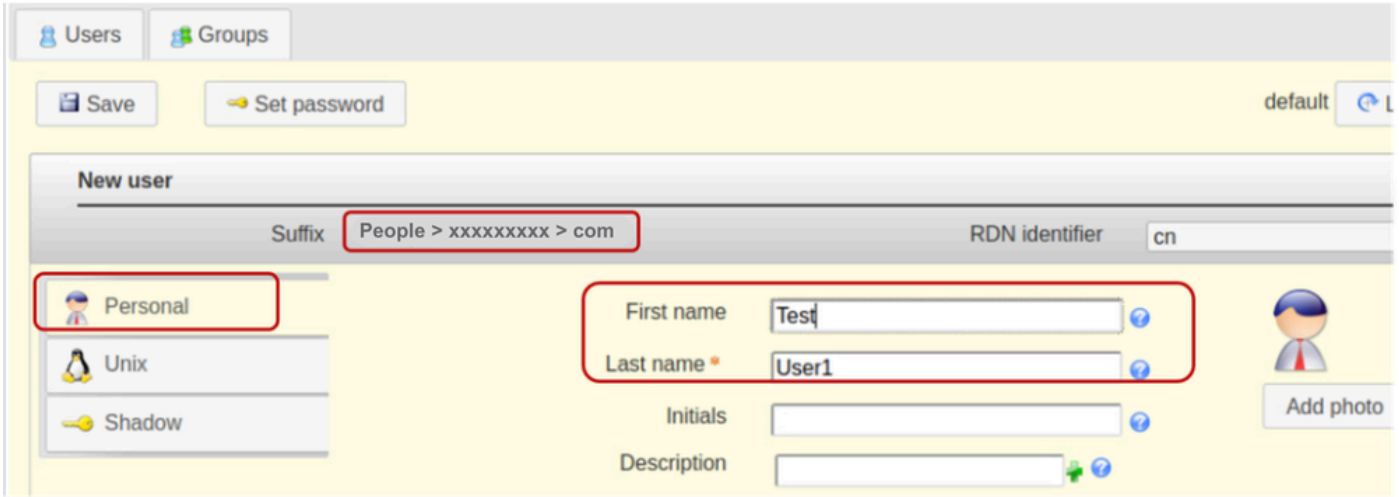
如果需要，請提供說明，然後按一下「儲存」



按一下「使用者」頁籤以建立使用者帳戶並選擇「新使用者」。



填寫「個人」頁籤中「testuser1」使用者所需的欄位。

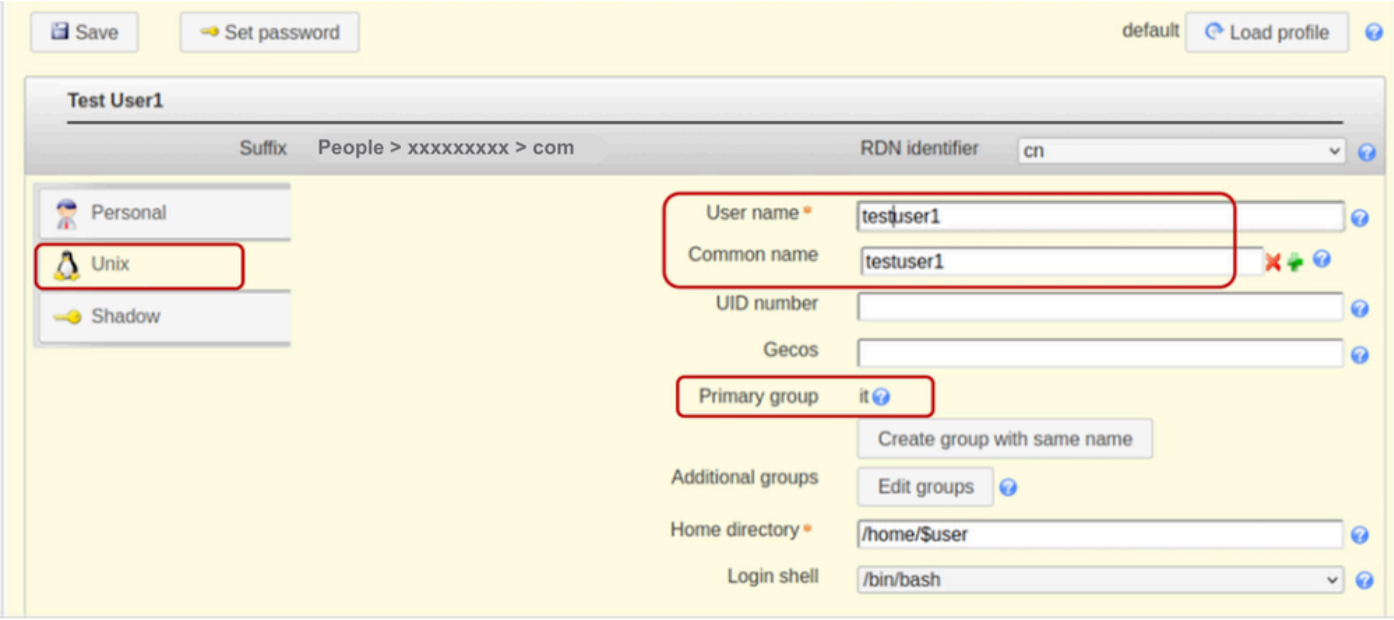


選擇Unix頁籤，在使用者名稱欄位中新增testuser1。在「it」組中包括使用者。

對於此演示，只有「it」組存在，因此它已預填充。

保留RDN識別符號作為「公用名」(cn)。 這使系統能夠使用「使用者名稱」欄位中指定的值自動填充「公用名」欄位。

將「UID編號」欄位留空，因為LAM會自動用可用值填充該欄位。



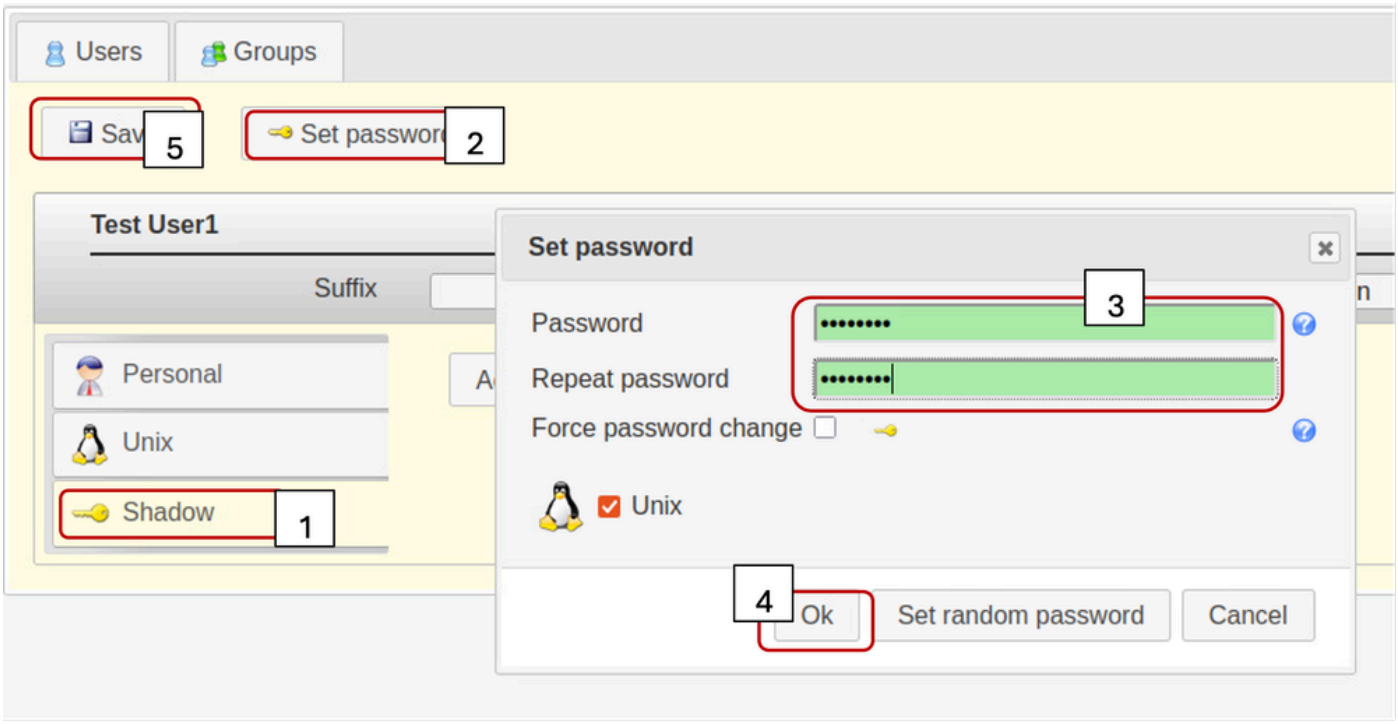
選擇「陰影」(Shadow)頁籤，

未使用影子帳戶擴展。

按一下「設定密碼」。

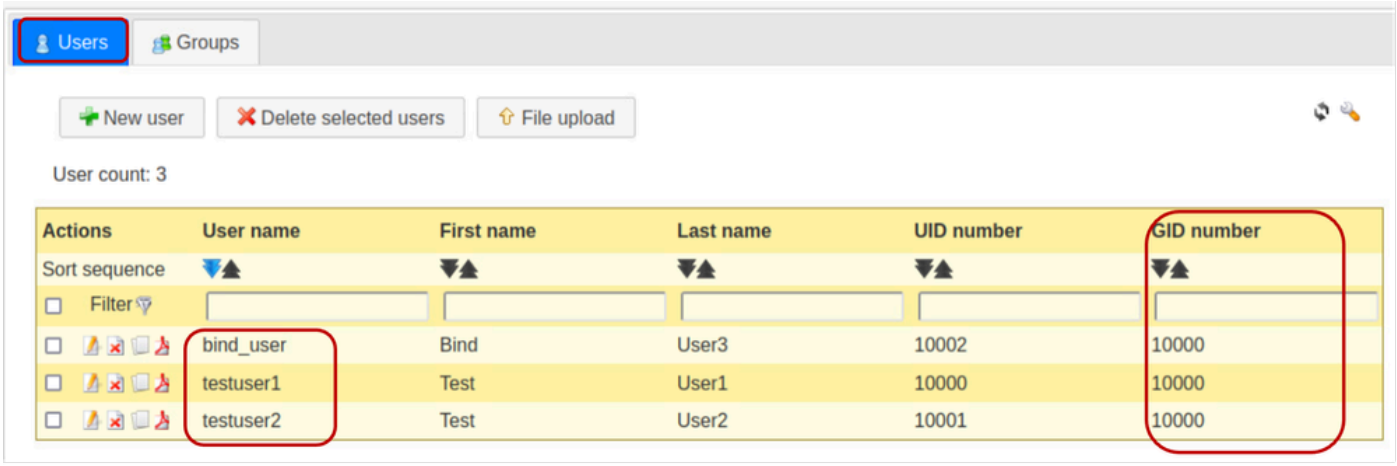
設定使用者密碼

按一下確定並儲存



重複前面所述的指定步驟，以建立「testuser2」使用者帳戶和「bind_user」帳戶。

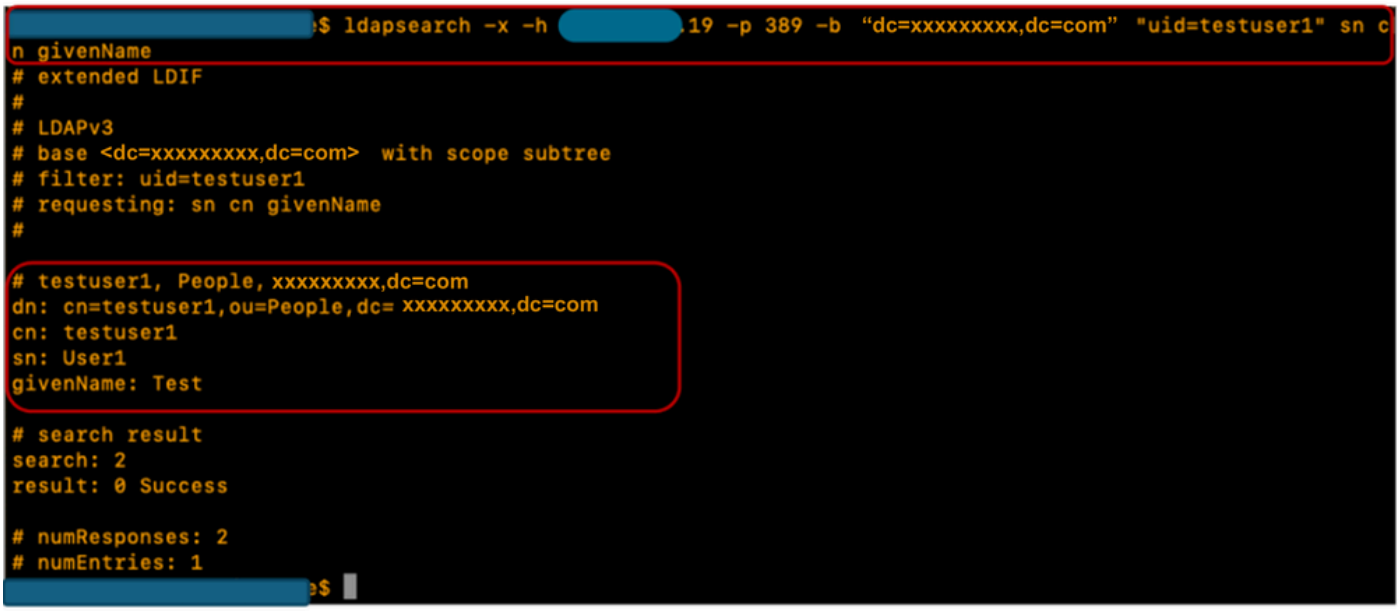
按一下「使用者」頁籤驗證所有所需使用者的建立。（在gidNumber列中有相同的值可確認建立的使用者屬於同一個組 — 它）



第6步：測試本地LDAP登入

登入到另一個基於Linux的系統，可以訪問OpenLDAP伺服器。
運行指定的ldapsearch命令以驗證LDAP是否正常工作：

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



CIMC上的配置引數

登入CIMC。

在「導航」窗格中，依次選擇管理員、使用者管理和LDAP。

如下所示填充LDAP配置引數：

- 啟用LDAP：已選中
- 基本DN:dc=xxxxxxx，dc=com

- 域：xxxxxxxxx.com

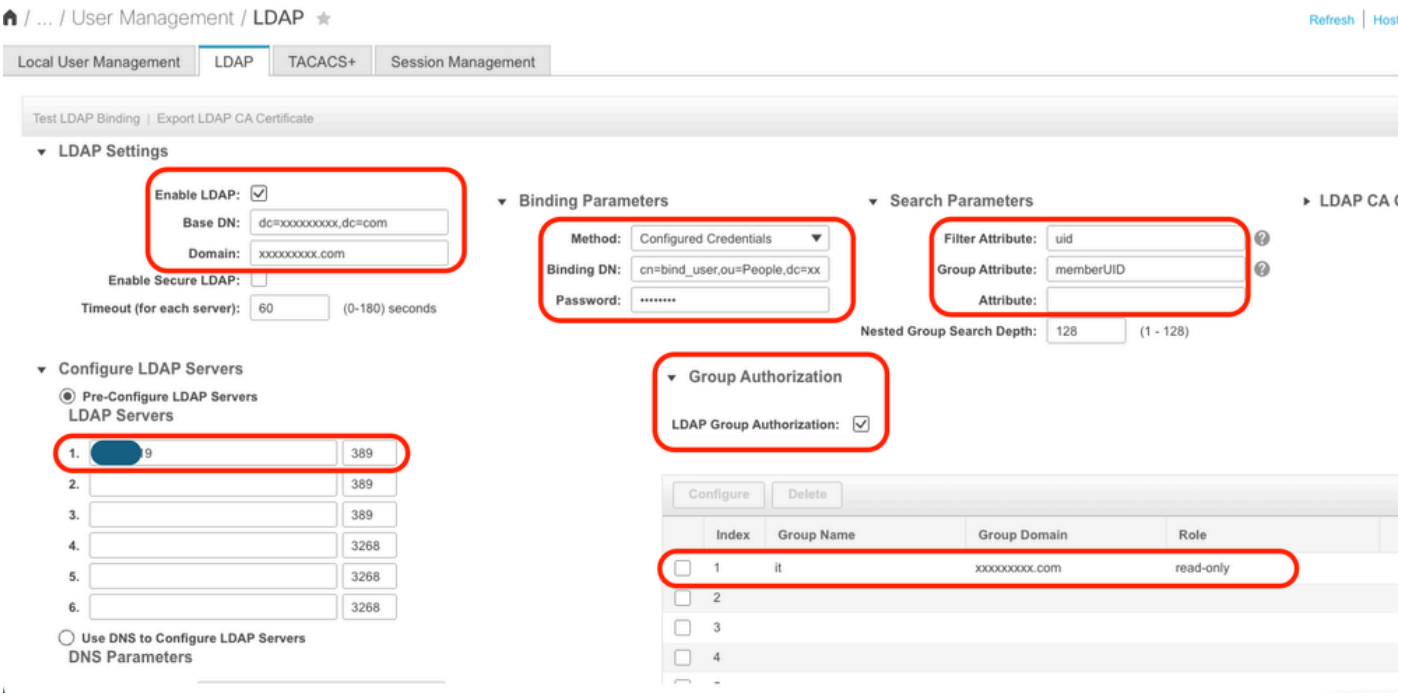
- LDAP 伺服器:<ldap_server_IP或FQDN> X.X.X.19

- 繫結引數："Login Credentials"或"Configured Credentials"
  - 使用已配置的憑據時，請完全按照在LDAP伺服器上配置的方法新增bind_user DN:
    - 例如：cn=bind_user，ou=People，dc=xxxxxxxxx，dc=com

- 搜尋引數：
  - 篩選器屬性："cn"或"uid"
  - 組屬性：memberUID

- LDAP組授權 — 已選中
  - 組名：它

- 組域：xxxxxxxxx.com
- 角色：只讀（任何所需的角色）



儲存配置並測試LDAP使用者登入。

UCS Manager上的配置引數

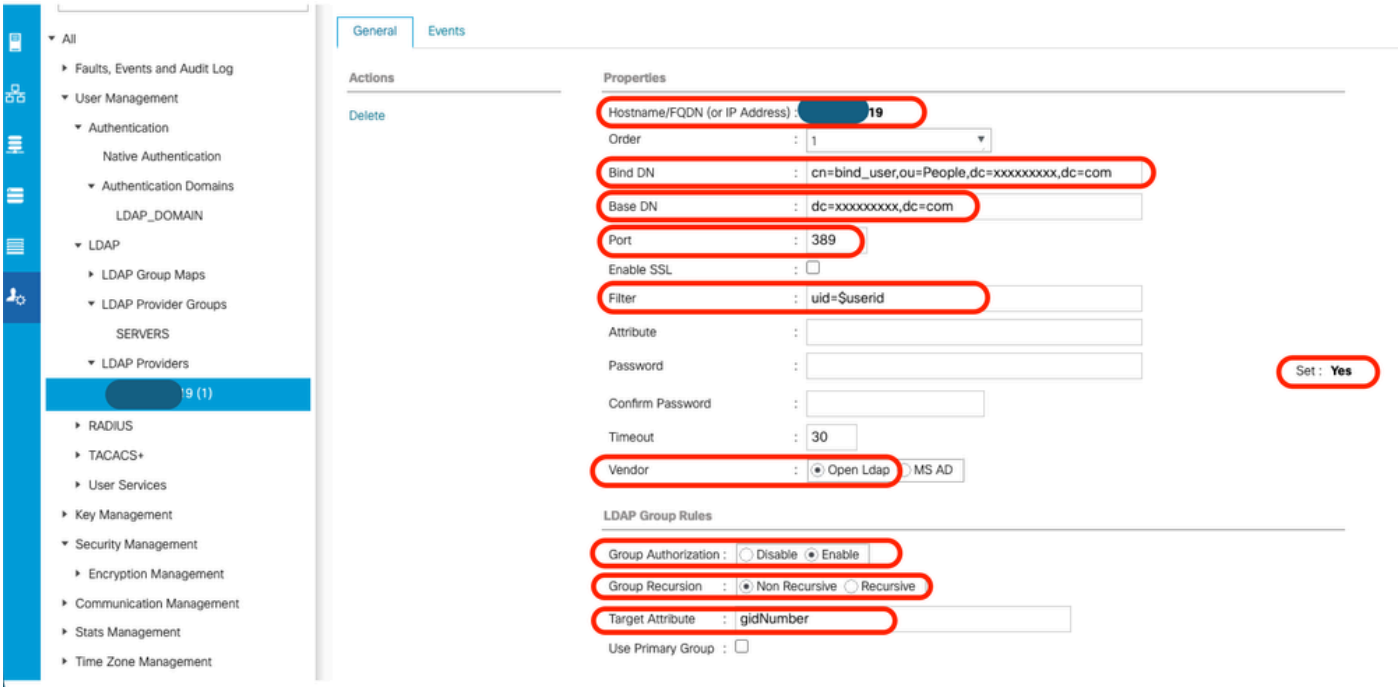
登入到UCS Manager。

在「導航」窗格中，依次選擇管理員、使用者管理和LDAP。

如下所示填充LDAP配置引數：

- LDAP提供程式：
  - 主機名： <LDAP伺服器的FQDN或IP地址>
  - 繫結DN:cn=bind_user，ou=People，dc=xxxxxxxxx，dc=com
  - 基本DN:dc=xxxxxxx，dc=com
  - 連接埠：389
  - 啟用SSL:已停用
  - Filter: (篩選條件：)uid=$userid
  - 組授權：已啟用
  - 組遞迴：非遞迴
  - 目標屬性：gidNumber
- LDAP組對映：

- LDAP組DN:10000 <it"組的gidNumber>

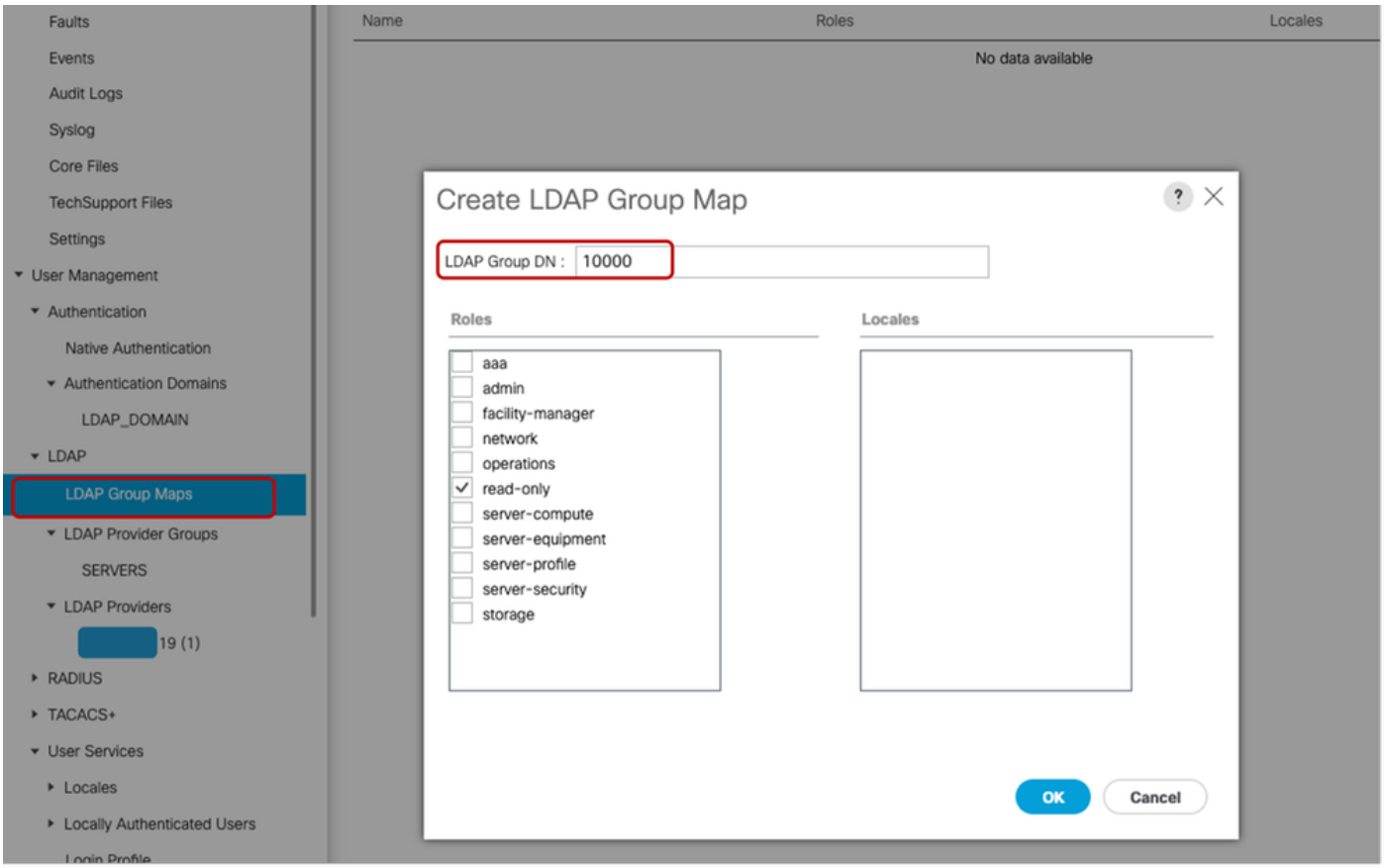


在All >> User Management >> LDAP >> LDAP Providers>> LDAP Group Rules下，UCS Manager的預設目標屬性為「memberOf」。預設情況下，OpenLDAP伺服器未啟用該屬性，因此將「目標屬性」值設定為「memberOf」（或將其留空）會導致使用者登入失敗，因為OpenLDAP伺服器無法識別所請求的屬性值。

在本示例中，「Target Attribute」值已設定為「gidNumber」。

將配置的LDAP提供程式新增到LDAP提供程式組。在本演示中，已建立「SERVERS」 LDAP提供程式組。

在「All >> User Management >> LDAP >> LDAP Group Maps>>」中配置「LDAP組對映」時，gidNumber值(在本例中為「10000」)將用作「組DN對映」，如下所示：



在引用LDAP提供程式組的「All >> User Management >> Authentication >> Authentication Domains」中配置LDAP身份驗證域(LDAP_DOMAIN),並測試LDAP使用者登入。

附註：如果要求memberOf屬性來滿足特定的環境要求或實施「組遞迴」功能，建議使用下面的第二個配置選項，該選項要求啟用覆蓋擴展的LDAP。

雖然LDAP客戶經理(LAM)支援重疊配置，但請注意，此功能需要適當的許可。

有關使用LAM配置LDAP的詳細資訊，請參閱官方LDAP客戶經理文檔。

選項 2:使用Ubuntu CLI工具和重疊配置OpenLDAP

為了使用OpenLDAP進行UCS Manager身份驗證，需要兩個重疊，以確保組以UCS系統（UCS Manager和CIMC）能夠理解的方式與使用者關聯。

OpenLDAP端上的配置要求：

- 「memberof」重疊：此覆蓋建立使用者和組之間的對映，以便查詢使用者DN時，可在該查詢中請求memberOf屬性。預設情況下，組成員資格的使用者沒有屬性，除非將重疊的成員新增

到openLDAP

- 「refint」覆蓋：此覆蓋配置為驗證組對象成員屬性中的條目是否仍與使用者對象的memberOf屬性保持同步。如果沒有此服務，如果刪除使用者時未同時修改組，則孤立DN可以保留在組對象中。精簡服務可確保兩個方向的一致性。

第1步：初始net-tools並配置Linux伺服器主機名

在選項1中重複步驟1。

第2步：安裝SLAPD

在選項1中重複步驟2。（PHP和Apache安裝除外，因為選項2不要求它們工作 — 無LAM）

確保允許所需埠通過Ubuntu防火牆。

步驟 3:在LDAP伺服器上安裝「memberOf」重疊

檢查「memberOf」重疊是否已安裝

```
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
```

要安裝「memberOf」覆蓋，請建立名為ldap.memberof.load.ldif的.ldif檔案（使用任何所需的命名約定）並新增指定的配置：

```
cat <

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

使用指定的命令將ldap.memberof.load.ldif檔案中的配置新增到LDAP配置檔案：

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

根據linux發行版配置memberOf模組和olcDatabase條目以符合部署要求。

兩個強制屬性值是「olcDatabase={1}mdb」和「groupOfNames」，如下所示。

建立ldap.memberof.config.ldif檔案，填充其屬性並將其內容匯入到LDAP配置檔案中。

```
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
```

步驟 4:在LDAP伺服器上安裝「精簡」覆蓋

下一步，安裝精簡到openldap:

建立名為ldap.refint.load.ldif的.ldif檔案（使用任何所需的命名約定）並新增指定的配置：

```
cat <


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

使用指定的命令將ldap.refint.load.ldif檔案中的配置匯入LDAP配置檔案：

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

配置refint，以維護組和使用者之間的引用完整性。

配置精簡模組及其olcDatabase條目以匹配部署要求。

建立ldap.refint.config.ldif檔案並將其內容匯入到LDAP配置檔案中。

```
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
```

安裝兩個外掛/擴展外掛時，指定的ldapsearch命令的輸出與下面顯示的輸出類似：

```
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
```

當兩個外掛/擴展都配置好時，指定的ldapsearch命令的輸出與顯示的輸出類似：

```
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
```

重新啟動slapd服務，使新安裝的外掛/模組可用：

```
sudo systemctl restart slapd
```

步驟 5:建立OU、使用者和組

建立組織單位（用於使用者和組）、使用者和組。

建立使用者（人員）和組（組）OU並將其匯入LDAP配置檔案。這需要「admin」帳戶密碼：

```
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:~$
```

建立使用者（testuser1、testuser2和bind_user），將它們對映到各自的OU(People)，使用gidNumbers將它們新增到其組（良好做法），然後將使用者匯入到LDAP配置檔案中。

```
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:~$
```

建立組（它），將它們對映到各自的OU（組），關聯組成員(testuser1、testuser2)，然後將它們匯入到LDAP配置檔案中：

```
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
```

附註：即使memberOf屬性在建立「使用者」或「組」期間未顯式定義，系統也會自動生成並維護此引用。一旦使用者與組相關聯， memberOf屬性就會自動反映這些成員身份，確保目錄保持與當前訪問結構的同步。

第6步：測試本地LDAP登入

使用指定的命令驗證使用者登入到LDAP伺服器（根據您的環境替換登入引數）：

```
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:~$
```

CIMC上的配置引數

登入CIMC。

在「導航」窗格中，依次選擇管理員、使用者管理和LDAP。

如下所示填充LDAP配置引數：

- 啟用LDAP：已選中
- 基本DN:dc=xxxxxxx，dc=com

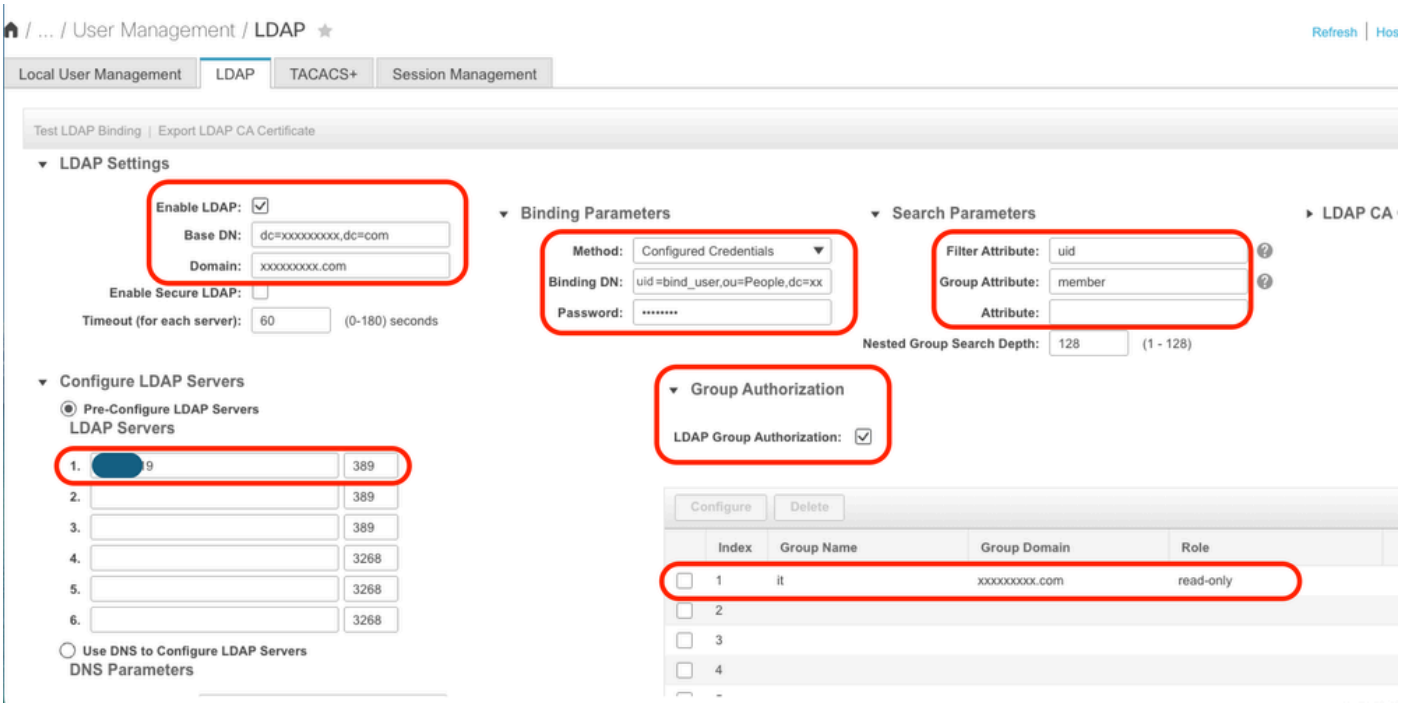
- 域：xxxxxxxxx.com

- LDAP伺服器：<ldap_server_IP或FQDN> X.X.X.19

- 繫結引數：可能是「登入憑證」或「配置的憑證」
  - 使用已配置的憑據時，請完全按照在LDAP伺服器上配置的方法新增bind_user DN:
  - 例如："cn=bind_user，ou=People，dc=xxxxxxxxx，dc=com"或"uid=bind_user，ou=People，dc=xxxxxxxxx，dc=com"

- 搜尋引數：
  - 篩選器屬性："cn"或"uid"
  - 組屬性：成員

- LDAP組授權 — 已選中
  - 組名：它
  - 組域：xxxxxxxxx.com
  - 角色：唯讀（任何首選角色）



儲存配置並測試LDAP使用者登入。

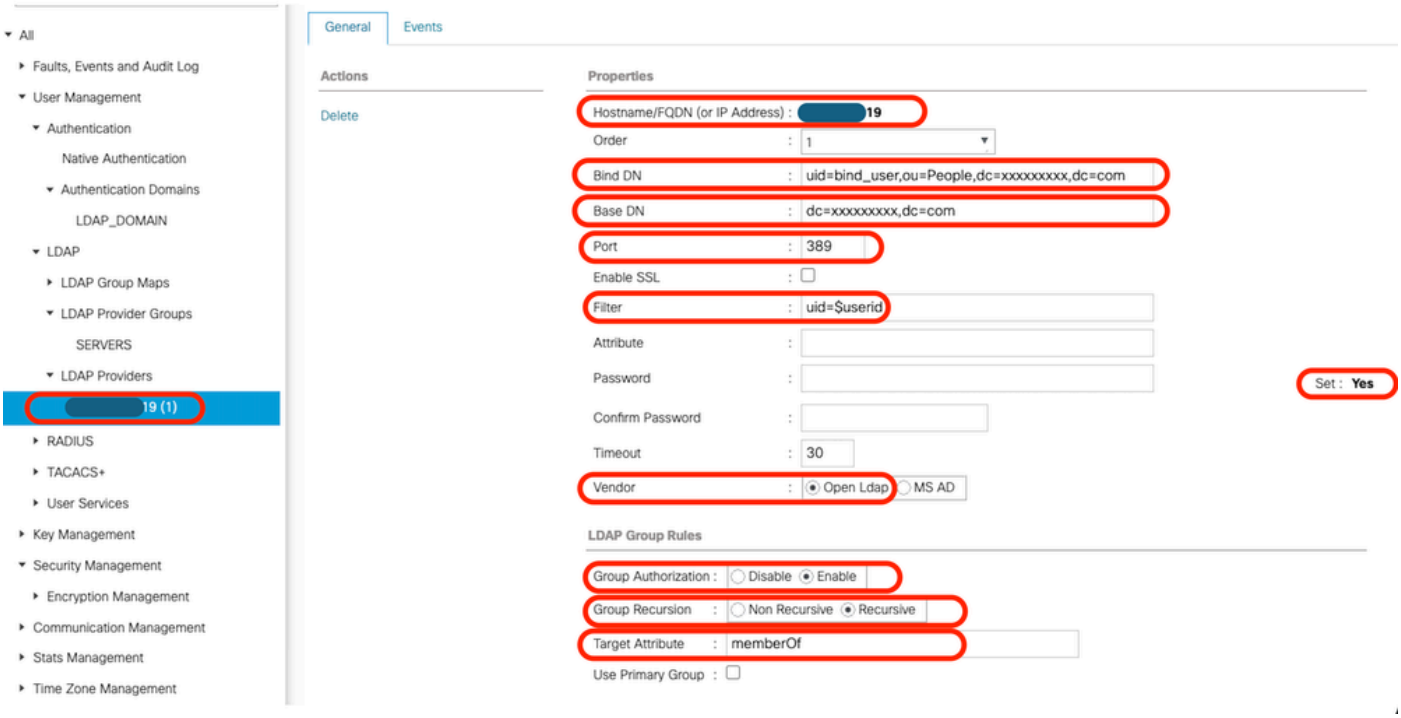
UCS Manager上的配置引數

登入到UCS Manager。

在「導航」窗格中，依次選擇管理員、使用者管理和LDAP。

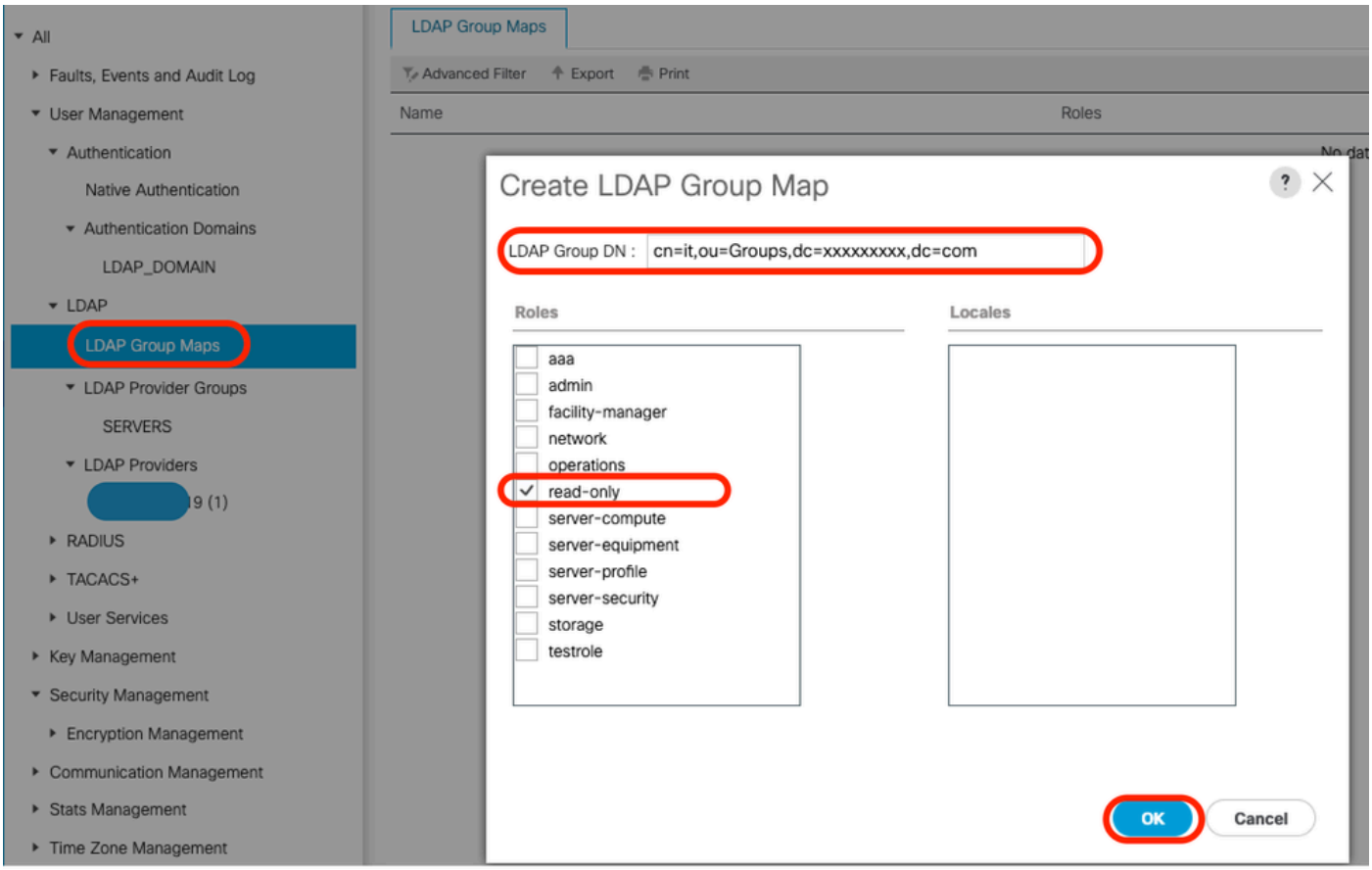
如下所示填充LDAP配置引數：

- LDAP提供程式：
  - 主機名： <LDAP伺服器的FQDN或IP地址>
  - 繫結DN:uid=bind_user，ou=People，dc=xxxxxxxxx，dc=com
  - 基本DN:dc=xxxxxxx，dc=com
  - 連接埠：389
  - 啟用SSL:已停用
  - Filter: (篩選條件：)uid=$userid
  - 組授權：已啟用
  - 組遞迴：遞迴
  - 目標屬性：memberOf
- LDAP組對映：
  - LDAP組DN:cn=it，ou=Groups，dc=xxxxxxx，dc=com



將配置的LDAP提供程式新增到LDAP提供程式組。在本演示中，使用「SERVERS」 LDAP提供程式組。

配置LDAP組對映，新增從LDAP伺服器檢索的「LDAP組DN」。



在All >> User Management >> Authentication >> Authentication Domains中，配置引用LDAP提供程式組(SERVERS)的LDAP身份驗證域(LDAP_DOMAIN)，並測試LDAP使用者登入。

接下來，我們考慮在單獨的Linux發行版(CentOS 10)中設定相同內容（使用重疊）

案例 2:CentOS串流10 - Fedora

輕量型目錄訪問協定(LDAP)的配置過程因底層作業系統版本而異。本節重點介紹在CentOS流10上實施LDAP。

雖然許多Linux發行版都使用OpenLDAP，但是CentOS Stream 10和基於Fedora的當代系統都使用389目錄伺服器(389 DS)作為預設的LDAP提供者。

附註：雖然389 DS被認為是CentOS和Red Hat生態系統中OpenLDAP的後繼者，但這兩個解決方案不能直接互換。它們各自的目錄結構、配置檔案和操作環境有很大不同。

本指南提供了在CentOS流10環境中使用389 DS成功配置LDAP的必要步驟。

選項 1:在CentOS流10上使用389目錄伺服器配置LDAP

步驟 1:初始設定

在場景1的選項1中重複步驟1。

CentOS系統不使用APT包管理套件。要在CentOS Stream 10上執行必要的軟體安裝，請使用dnf(Dandified YUM)或yum包管理器

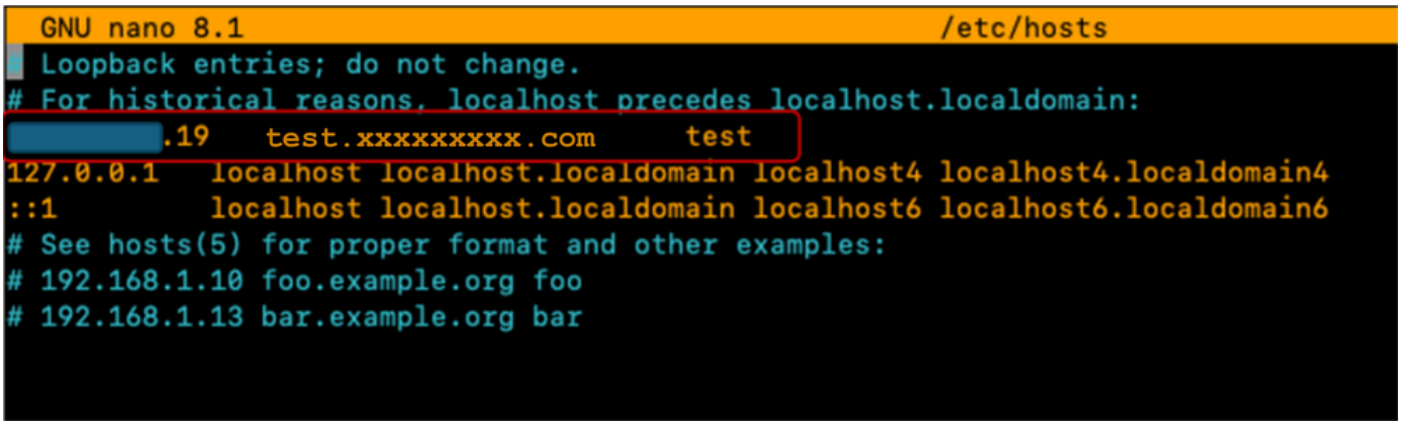
```
sudo yum update
sudo yum install net-tools
```

使用「ifconfig」命令驗證伺服器IP地址。

將伺服器IP地址與伺服器完全限定域名(例如：本實驗中使用的test.xxxxxxxxx.com)和主機名（例如

：test）一起新增到"/etc/hosts"檔案中，其格式如下：

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



通過用主機名（測試）替換檔案「/etc/hostname 」的內容來更新檔案。

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

需要重新啟動伺服器才能使這些更改生效。

```
sudo reboot
```

步驟 2:安裝EPEL回購和389伺服器軟體包

安裝和更新EPEL儲存庫。

安裝389 Directory Server軟體包。

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

建立包含所需LDAP伺服器設定引數的目錄模板檔案：

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

驗證建立的模板檔案(ldapconfig.conf)的內容

```
sudo cat ldapconfig.conf
```

編輯ldapconfig.conf模板檔案。

```
sudo nano ldapconfig.conf
```

將指定的配置條目插入檔案並儲存更改。

注意：根據每個環境的特定需求或要求，可能需要進行不同的修改。

此示例涵蓋此演示的基線配置。

```
[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
```

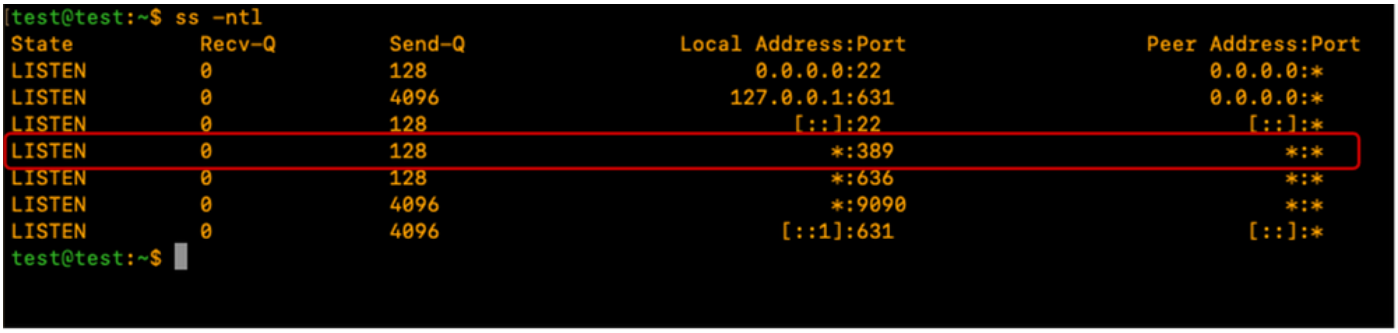
模板檔案定義「localhost」目錄例項的配置引數。這包括設定管理使用者(「admin」)、相關密碼和域上下文(「xxxxxxxxx.com」)。

使用以前編輯的模板建立「localhost」目錄例項。指定的命令建立和啟動LDAP目錄伺服器：

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

驗證LDAP服務是否正在伺服器上運行

```
ss -ntl
```



調整CentOS防火牆以允許LDAP所需的埠（389和/或636）。

在本演示中，防火牆關閉。

```
sudo systemctl stop firewalld
```

通過運行指定的命令，驗證LDAP在LDAP伺服器上本地正常工作，並確保它返回LDAP輸出，如下所示：

```
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
```

輸出包含由389DS伺服器建立的演示帳戶。LDAP伺服器會自動建立預設OU。

使用者OU和組OU。可根據要求建立其他OU。

在本演示中，使用預設/自動建立的OU。

請檢視389DS正式文檔，瞭解有關廣泛使用389DS軟體包的詳細資訊：

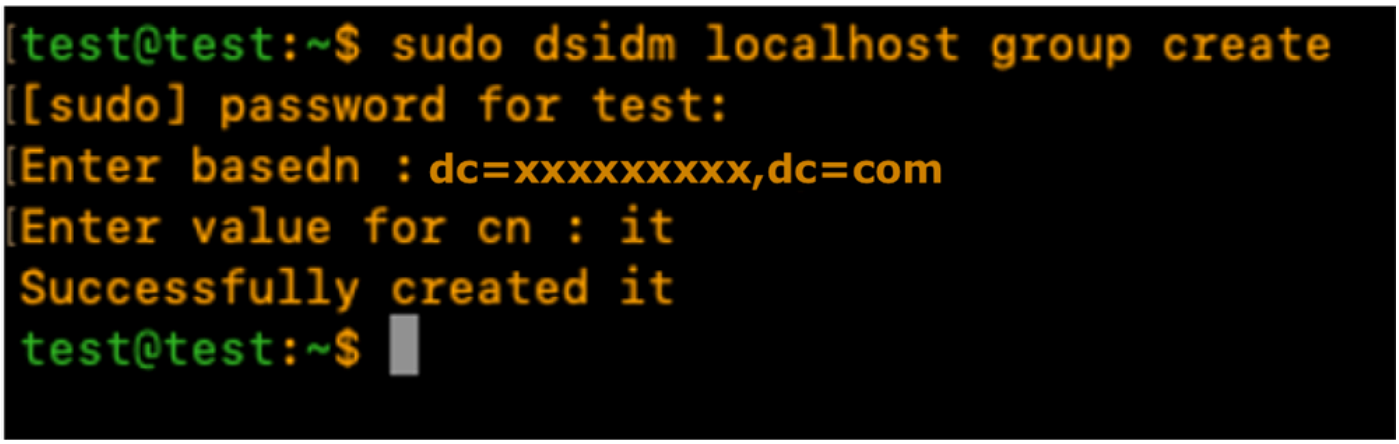
步驟 3:建立LDAP組和使用者

使用指定的命令建立組：sudo dsidm <instance_name> group create。

在本演示中，例項名稱為「localhost」。

```
sudo dsidm localhost group create
```

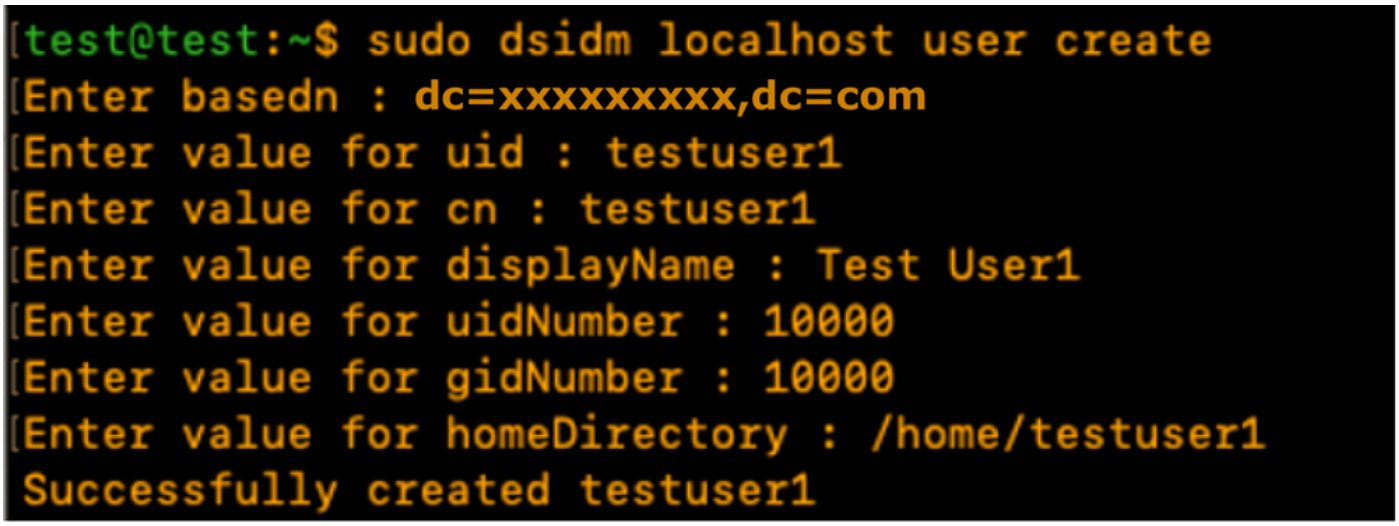
輸入終端提示以填充組詳細資訊，如下所示：



使用命令建立testuser1使用者帳戶：

```
sudo dsidm localhost user create
```

輸入終端提示以填充使用者詳細資訊，如下所示



使用指定的命令為testuser1建立口令，並輸入CLI提示：

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

使用指定的命令將使用者新增到組："sudo dsidm <directory_instance> group add_member <group_cn> <user_dn>"

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

重複使用者建立步驟以建立testuser2和bind_user。

注意：確保將每個使用者明確新增到其目標組。

忽略此步驟可能會導致訪問受限或授權失敗。

bind_user帳戶不需要是特定組的成員，因為它可以配置為獨立帳戶，從而靈活地管理目錄環境中的管理和服務級別訪問。

重新啟動Directory例項：

```
sudo dsctl localhost restart
```

步驟 4:安裝memberOf重疊

安裝「memberOf」外掛並重新啟動Directory例項：

```
sudo dsconf localhost plugin memberof status
```

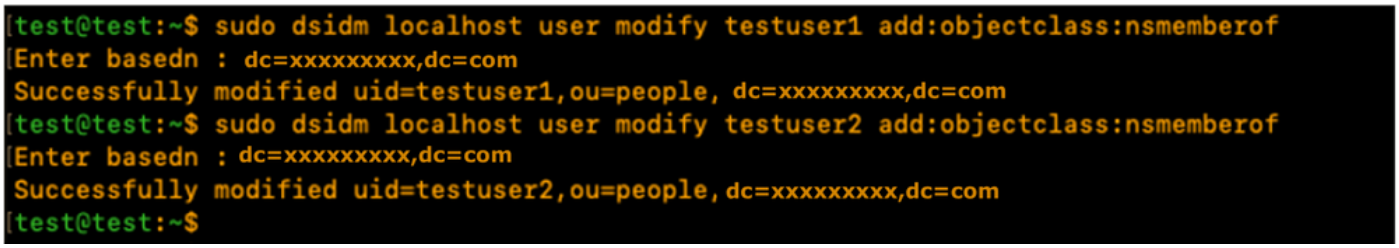
```
sudo dsconf localhost plugin memberof enable
sudo dsctl localhost restart
```

使用指定的命令配置「memberOf」外掛："sudo dsconf <directory_instance> plugin memberof set —scope <base_dn>"

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

使用指定的命令將使用者標籤為有效的「memberOf」目標："sudo dsidm <directory_instance> user modify <uid> add:objectclass:nsmemberof"

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

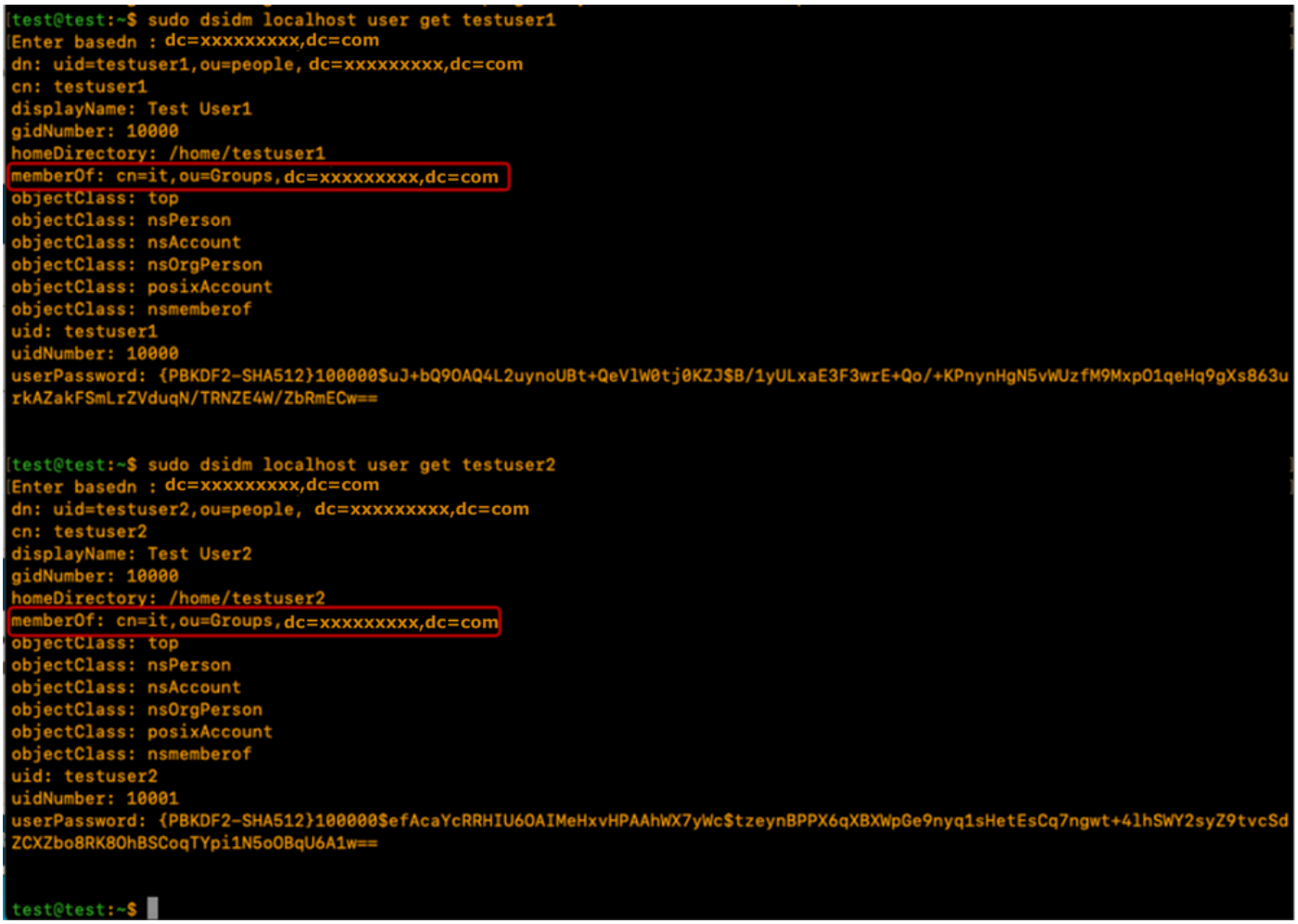


為基本DN生成「memberOf」修正："sudo dsconf <directory_instance> plugin memberof fixup <base_dn>"

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

驗證使用者設定：

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



389DS LDAP伺服器配置有memberOf外掛以支援memberOf屬性。

CIMC上的配置引數

登入CIMC。

在「導航」窗格中，依次選擇管理員、使用者管理和LDAP。

如下所示填充LDAP配置引數：

- 啟用LDAP：已選中
- 基本DN:dc=xxxxxxx，dc=com

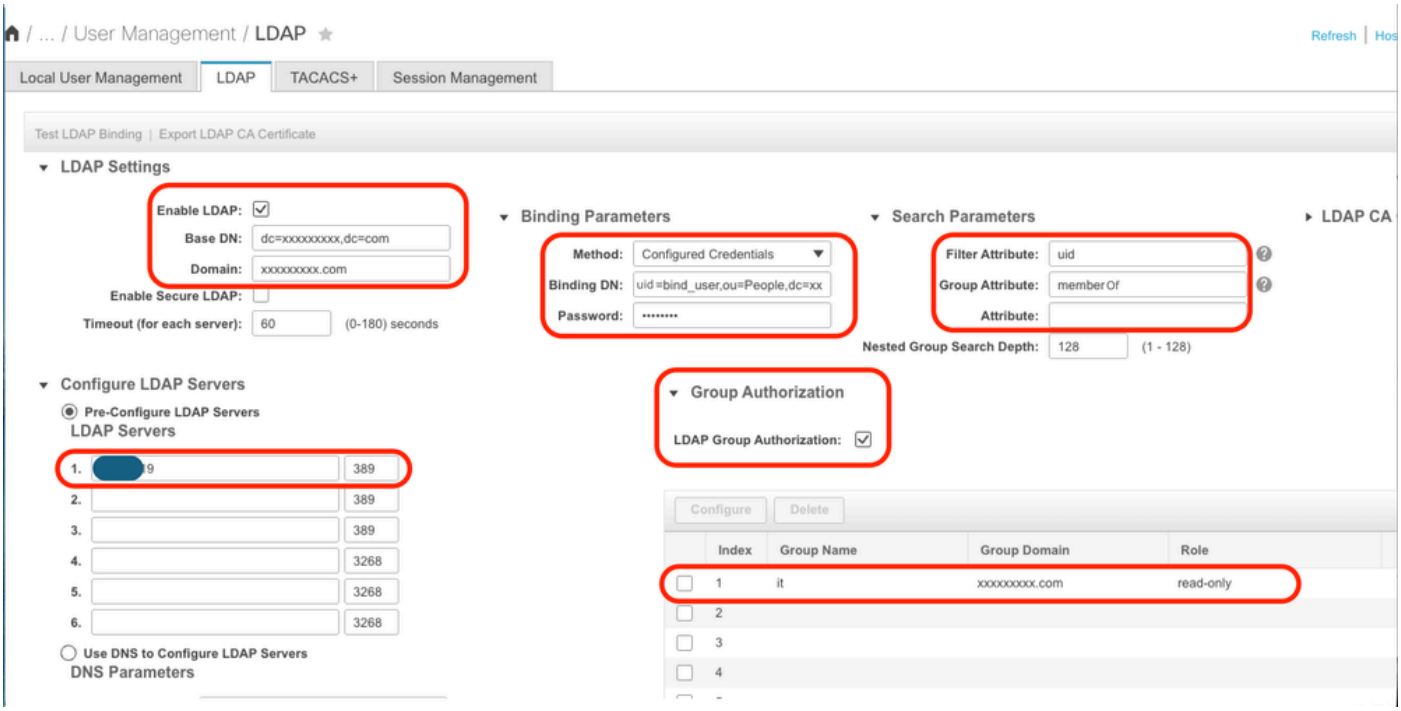
- 域：xxxxxxxxx.com

- LDAP伺服器：<ldap_server_IP或FQDN> X.X.X.19

- 繫結引數：可能是「登入憑證」或「配置的憑證」
  - 使用已配置的憑據時，請完全按照在LDAP伺服器上配置的方法新增bind_user DN:
    - 例如："cn=bind_user，ou=People，dc=xxxxxxxxx，dc=com"或 "uid=bind_user，ou=People，dc=xxxxxxxxx，dc=com"

- 搜尋引數：
  - 篩選器屬性："cn"或"uid"
  - 組屬性：memberOf

- LDAP組授權 — 已選中
  - 組名：它
  - 組域：xxxxxxxxx.com
  - 角色：唯讀（任何首選角色）



儲存配置並測試LDAP使用者登入。

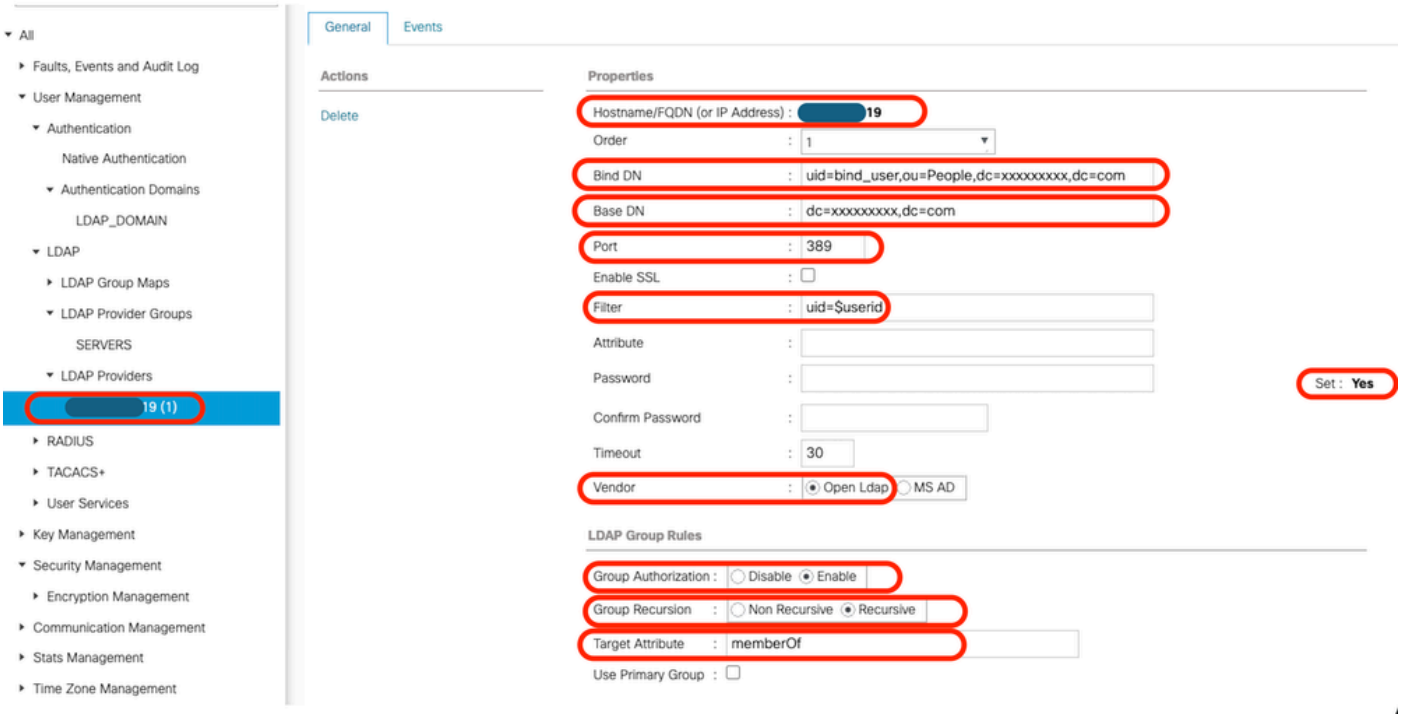
UCS Manager上的配置引數

登入到UCS Manager。

在「導航」窗格中，依次選擇管理員、使用者管理和LDAP。

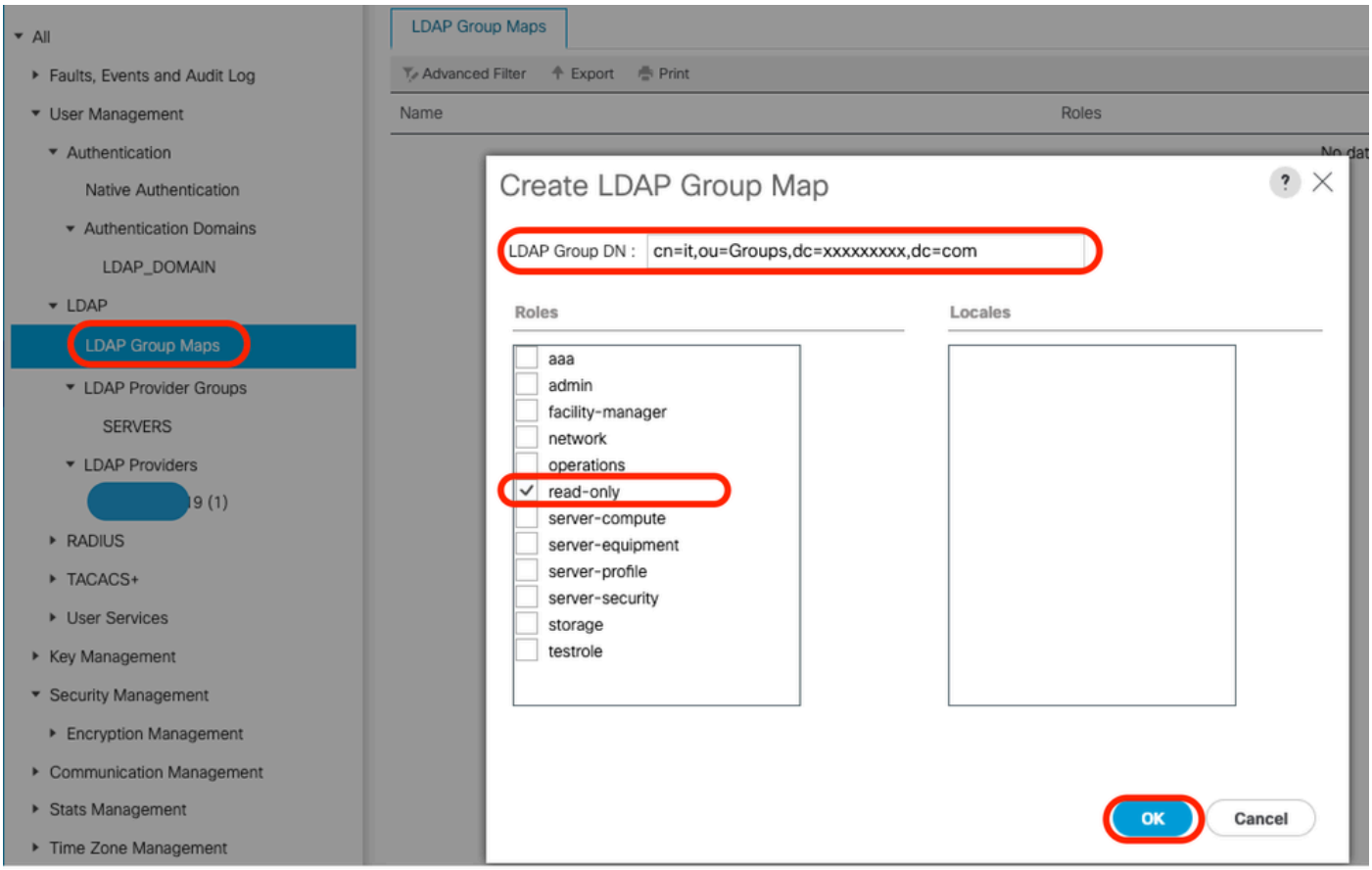
如下所示填充LDAP配置引數：

- LDAP提供程式：
  - 主機名： <LDAP伺服器的FQDN或IP地址>
  - 繫結DN:uid=bind_user，ou=people，dc=xxxxxxxxx，dc=com
  - 基本DN:dc=xxxxxxx，dc=com
  - 連接埠：389
  - 啟用SSL:已停用
  - Filter: (篩選條件：)uid=$userid
  - 組授權：已啟用
  - 組遞迴：遞迴
  - 目標屬性：memberOf
- LDAP組對映：
  - LDAP組DN:cn=it，ou=Groups，dc=xxxxxxx，dc=com



將配置的LDAP提供程式新增到LDAP提供程式組。在本演示中，使用「SERVERS」 LDAP提供程式組。

配置LDAP組對映，新增從LDAP伺服器檢索的「LDAP組DN」。



在引用LDAP提供程式組的「All >> User Management >> Authentication >> Authentication Domains」中配置LDAP身份驗證域(LDAP_DOMAIN)並測試LDAP使用者登入。

結論

雖然本指南涵蓋基本部署場景，但進一步探索LDAP功能可以顯著增強目錄效能和安全性。

有關其他資訊、最佳實踐和高級配置詳細資訊，請參閱指定的資源：

- OpenLDAP官方文檔
- LDAP客戶經理 — 手動
- 389目錄伺服器文檔
- 在UCS Manager上配置LDAP
- 在UCS C系列伺服器上配置安全LDAP

關於此翻譯

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