Configurar LDAP en UCS Manager & CIMC con servidores Linux OpenLDAP y 389-DS

Contenido

Introducción

Este documento describe una variedad de opciones para configurar LDAP como método de autenticación para UCS Manager y CIMC usando OpenLDAP basado en Linux y 389 Directory Servers.

Antecedentes

Debido a la amplia variabilidad de las configuraciones del servidor OpenLDAP, un tratamiento exhaustivo está más allá del alcance de este documento. En este artículo se hace hincapié en las configuraciones implementadas habitualmente que abarcan varias distribuciones de Linux, paquetes de servidor LDAP y esquemas de atributos. Para mayor claridad y simplicidad, este documento trata las configuraciones LDAP estándar. La configuración de LDAP seguro (LDAP) no se trata en este documento.

Requisitos previos:

Se recomienda conocer estos temas:

- UCS serie B
- UCS serie C
- Administración de Linux Server

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Versión del firmware de UCS Manager: 4.3(2 quater)
- Modelo de Fabric Interconnect: UCS-FI-6454
- Modelo de servidor independiente de la serie C de UCS: UCS C240-M5
- Versión de firmware independiente de UCS serie C: 4.3(2.250045)
- Ubuntu 20,04
- Flujo 10 de CentOS

Configuración utilizada para esta demostración:

- Nombre de host del servidor LDAP: prueba
- Dominio del servidor: xxxxxxxxx.com
- FQDN de servidor: test.xxxxxxxxx.com

- Dirección IP del servidor Linux (Ubuntu y CentOS): X.X.X.19
- Usuarios de OpenLDAP: testuser1, testuser2
- Grupos OpenLDAP: it
- Cuenta de usuario de enlace OpenLDAP: bind_user

Nota: en este laboratorio se utilizó el editor de texto linux Nano.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Escenario 1: Ubuntu - Debian

La configuración del servidor LDAP se puede realizar mediante una interfaz gráfica, como el Administrador de cuentas LDAP, o mediante herramientas de línea de comandos, en función de las preferencias administrativas y del nivel de control requerido. Este escenario examina la configuración mediante OpenLDAP basado en Linux, comenzando con una implementación basada en GUI y, posteriormente, realizando la transición a utilidades de línea de comandos para explorar funciones avanzadas, incluidos los complementos superpuestos (que se utilizan habitualmente en las integraciones con Cisco UCS Manager).

Opción 1: Configuración de OpenLDAP mediante Ubuntu LDAP Account Manager (LAM)

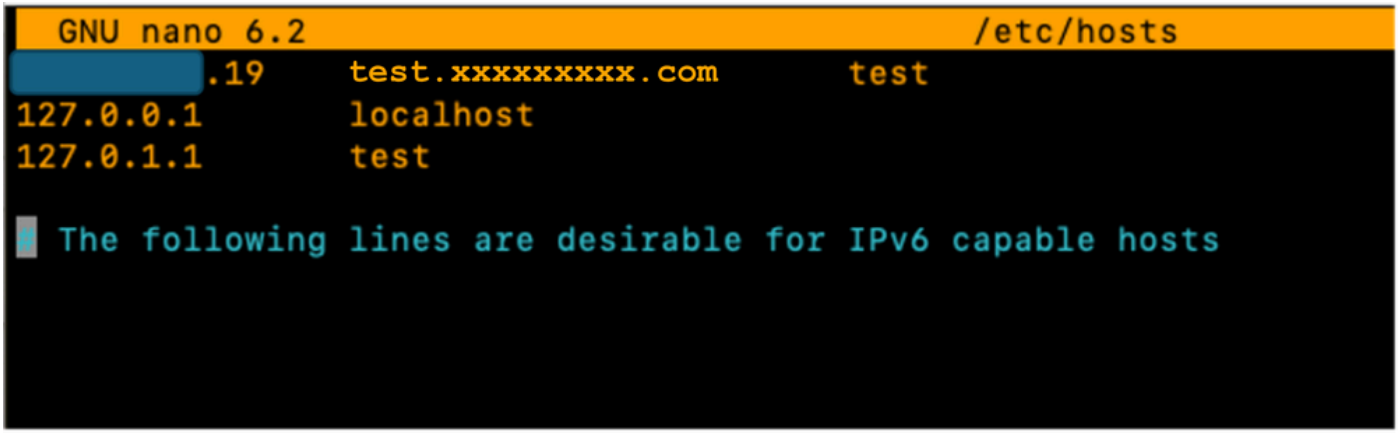
Paso 1: Configuración inicial del nombre de host del servidor Linux y net-tools.

Actualice ubuntu e instale el paquete net-tools para acceder a herramientas como ifconfig, netstat, etc:

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

Utilice el comando "ifconfig" para verificar la dirección IP del servidor y, a continuación, agréguela al archivo "/etc/hosts" junto con el nombre de dominio del servidor (por ejemplo: "test.xxxxxxxxx.com" utilizado en este laboratorio) y nombre de host (por ejemplo: "prueba") en el formato especificado.

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



Además, actualice el archivo "/etc/hostname" sustituyendo su contenido por el nombre de host (prueba).

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

Es necesario reiniciar el servidor para que estos cambios surtan efecto.

```
sudo reboot
```

Paso 2: Instalar SLAPD, Apache, PHP y sus dependencias

A continuación, instalar Apache, PHP y sus dependencias. Se utilizan para habilitar la interacción

de la GUI en una página web :

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

Instalar el paquete de servidor LDAP abierto "slapd" y sus dependencias (ldap-utils)

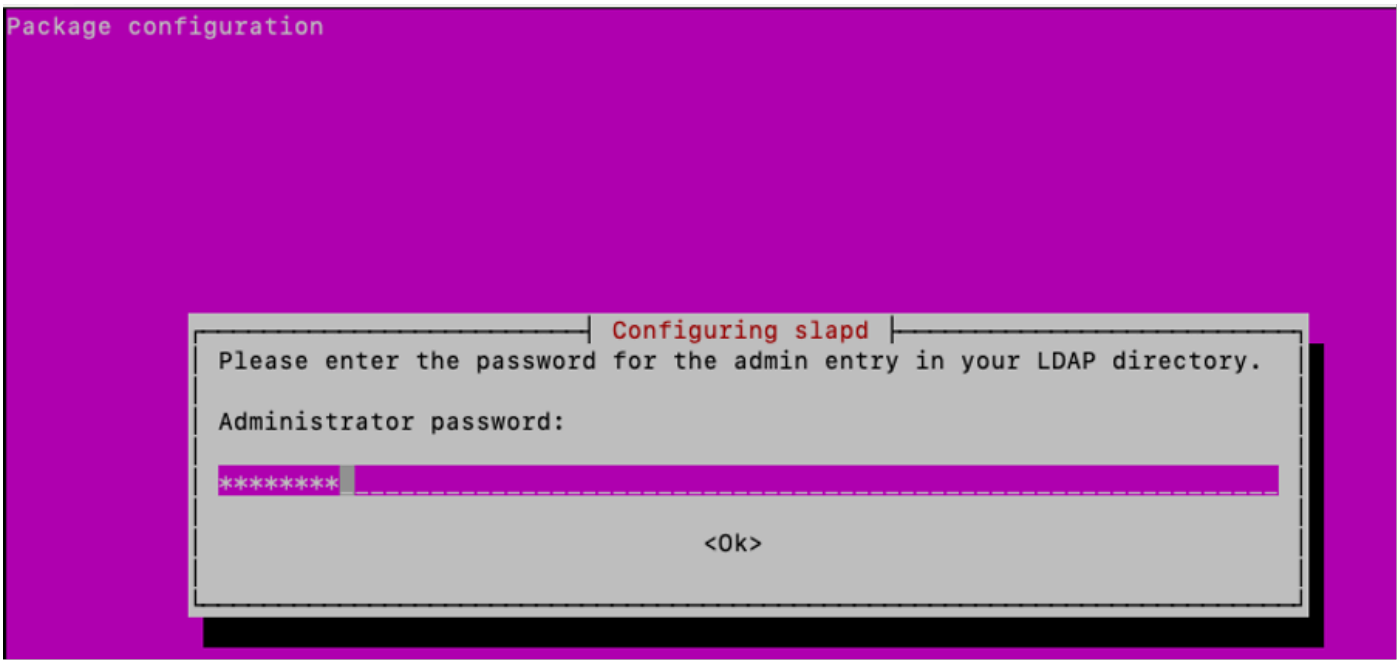
```
sudo apt install slapd ldap-utils -y
```

Durante la instalación de SLAPD, en la ventana emergente de la GUI que aparece, introduzca la configuración de paquete SLAPD adicional necesaria.

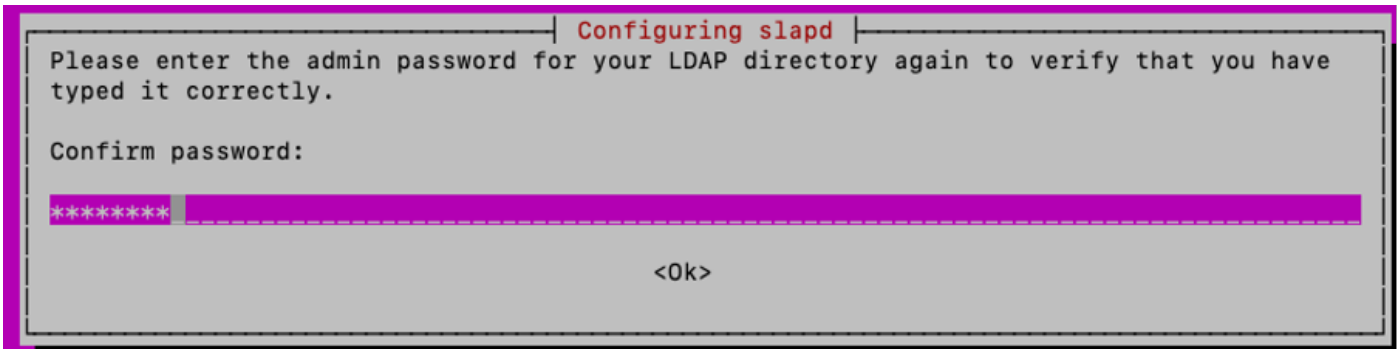
Nota: La pérdida de la contraseña requiere una reinstalación del servidor LDAP.

El "administrador" (admin) en este contexto es una cuenta que se utiliza para administrar el servicio OpenLDAP, los módulos y las configuraciones.

Agregue la contraseña de "administrador" del paquete LDAP y presione Enter en el teclado para seleccionar "OK".



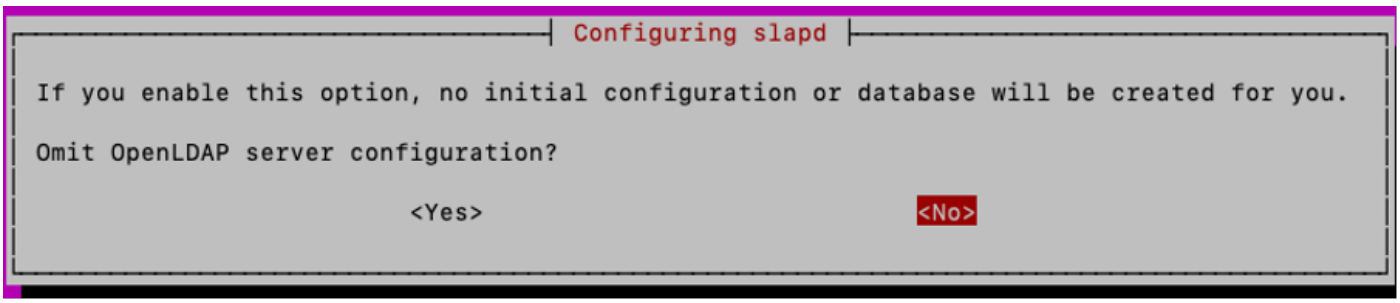
Confirme la contraseña:



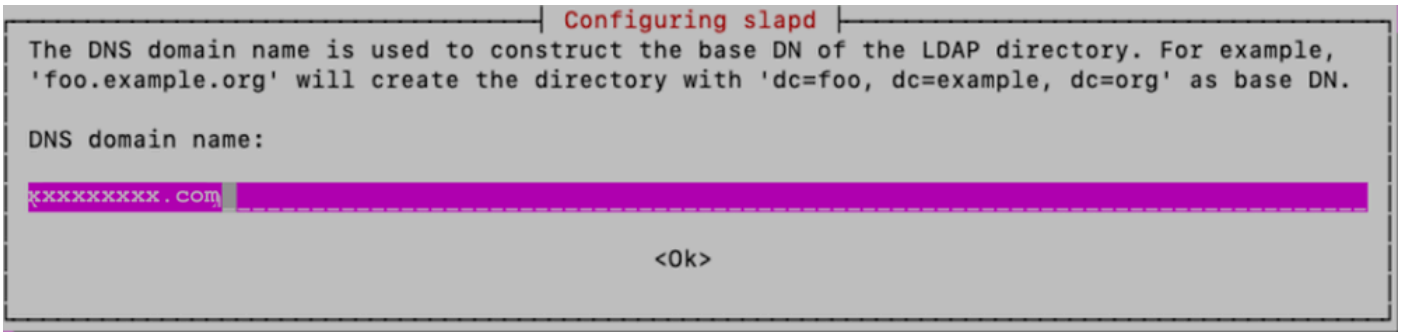
Una vez finalizada la instalación, puede utilizar el comando especificado para volver a configurar el paquete SLAPD, agregando información de dominio:

```
sudo dpkg-reconfigure slapd
```

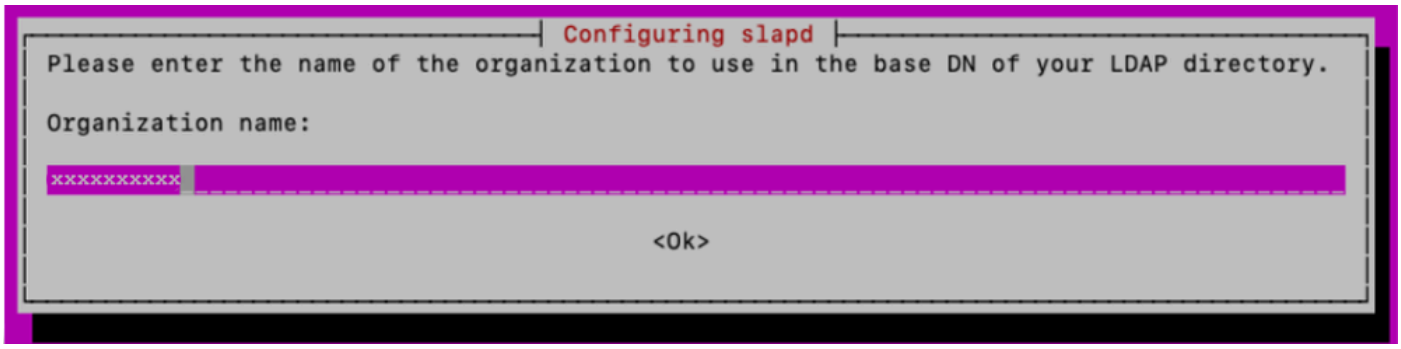
Puede aceptar la opción predeterminada "No" para "Omitir configuración del servidor OpenLDAP" y presionar Enter:



Escriba el nombre de dominio y pulse intro:



Para este laboratorio, "xxxxxxxxx" se utiliza como "Nombre de la organización":

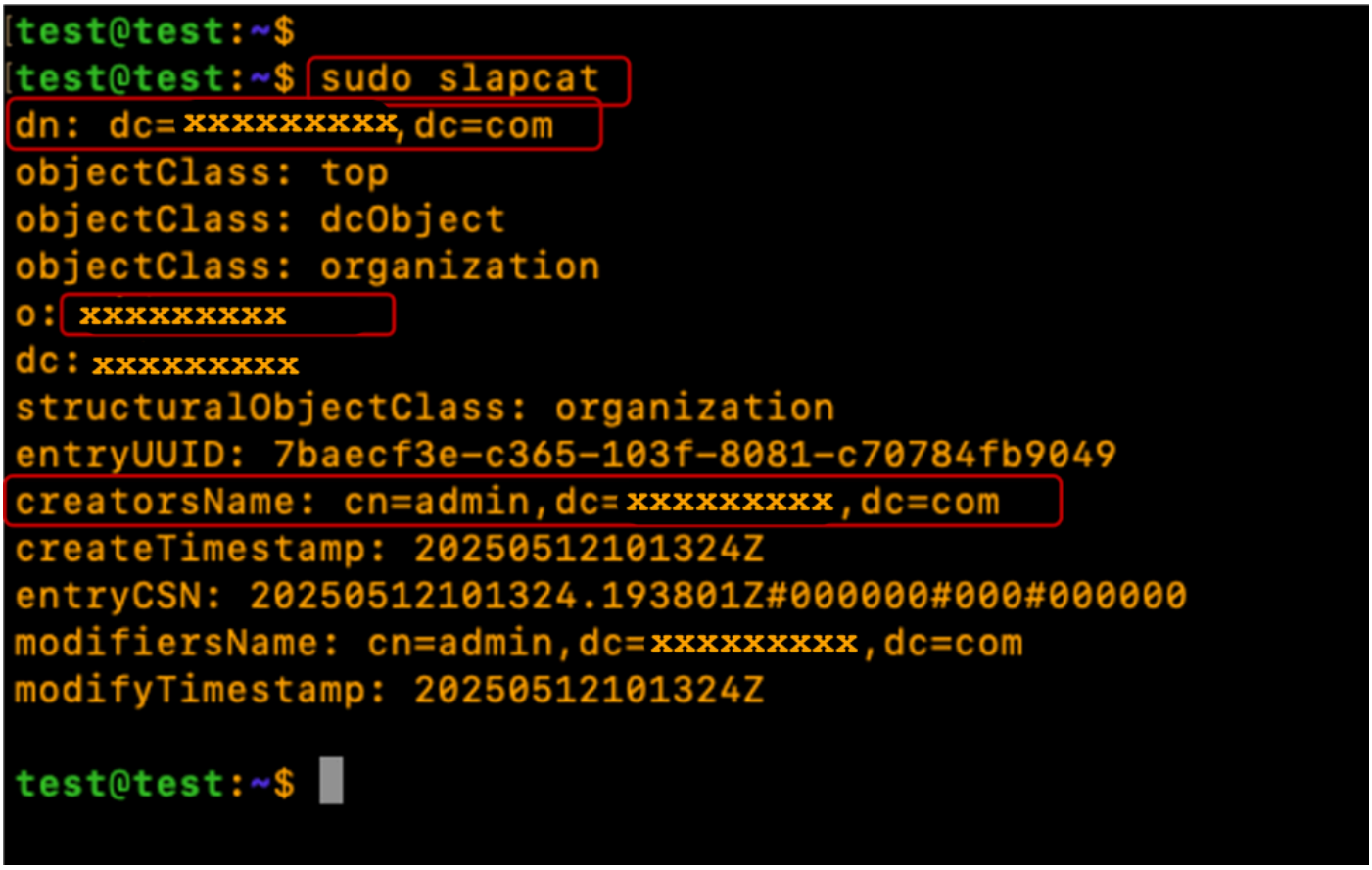


A continuación, escriba la "contraseña del administrador" y confírmela

Para las demás opciones de configuración, mantenga los parámetros predeterminados y pulse la tecla Intro del teclado para completar la configuración.

Verifique la instalación de SLAPD mediante el comando:

```
sudo slapcat
```



Paso 3: Instalación del LDAP Account Manager

Instale el LDAP Account Manager (LAM) para la creación y administración de usuarios y grupos LDAP:

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

Habilite la extensión PHP PHP-CGI, requerida por LAM.

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

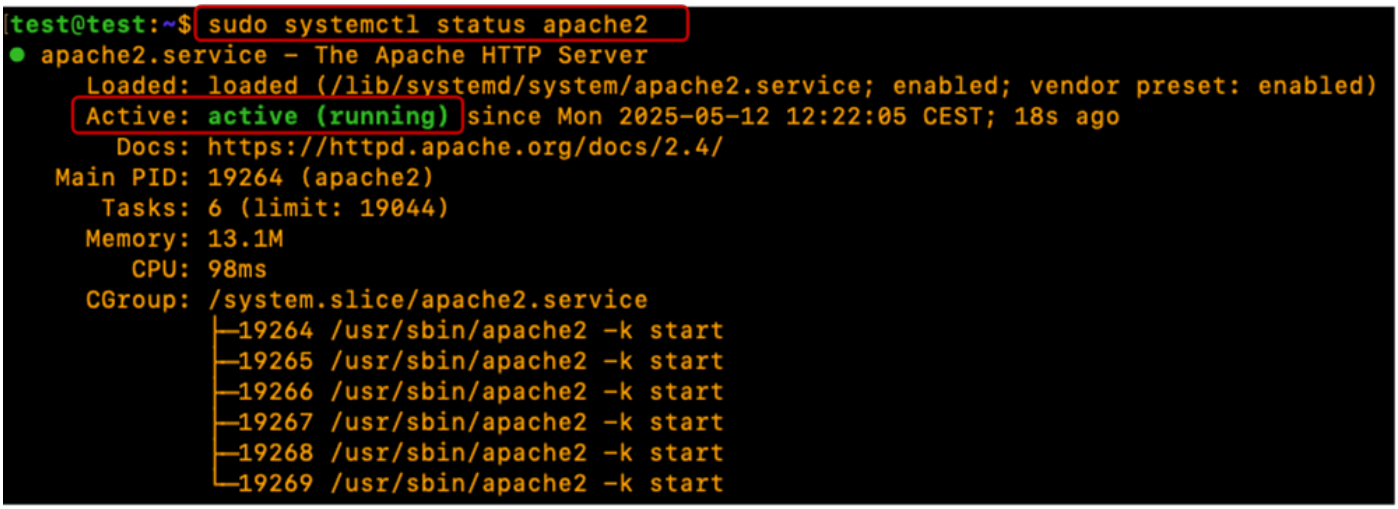
Vuelva a cargar Apache para activar la nueva configuración.

Reinicie y habilite el servicio Apache para que se inicie automáticamente al arrancar:

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

Compruebe que el estado del servidor Apache es "En ejecución" y "Activo"

```
sudo systemctl status apache2
```

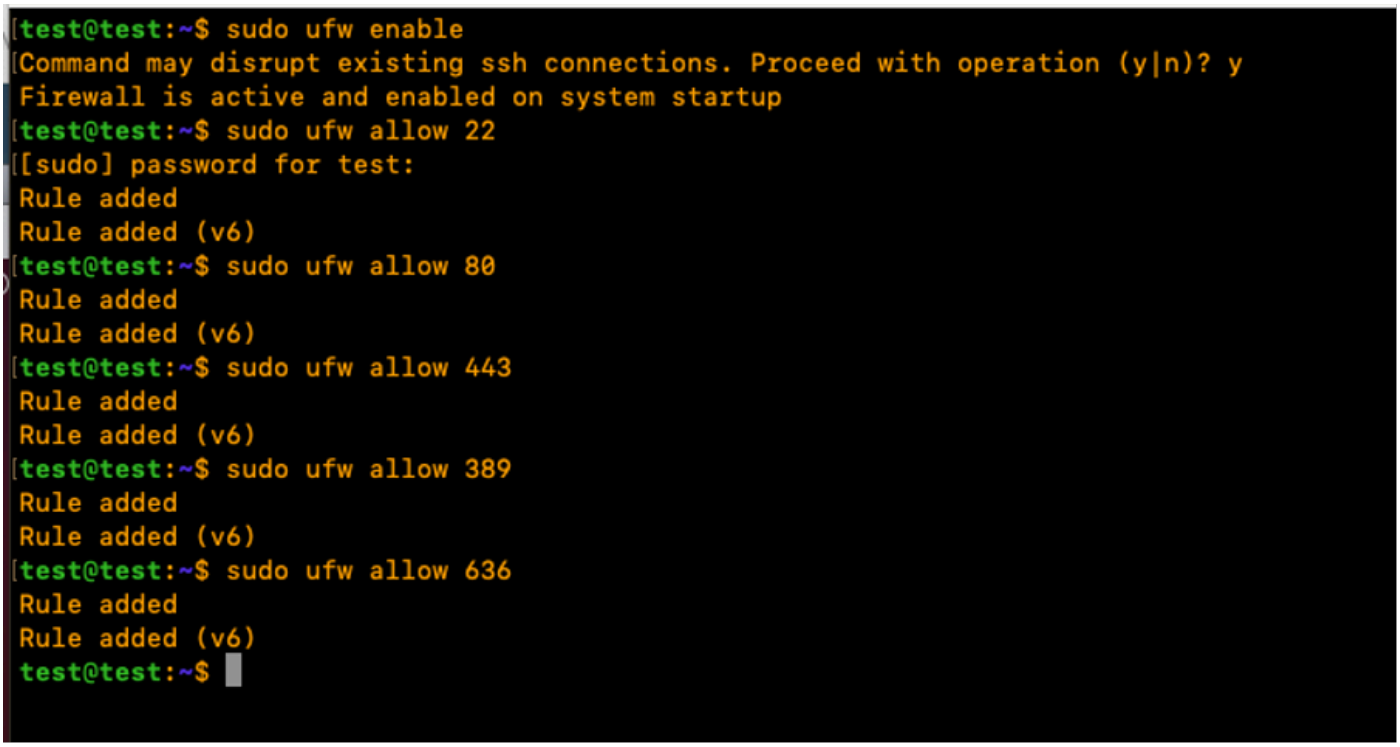


Configure el firewall de Ubuntu para permitir los puertos 80 (Web), 443 (Web segura), 389 (LDAP) y 636 (LDAP seguro si es necesario)

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

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

```
sudo ufw allow 636
```



Verifique el estado del firewall de Ubuntu:

```
sudo ufw status
```

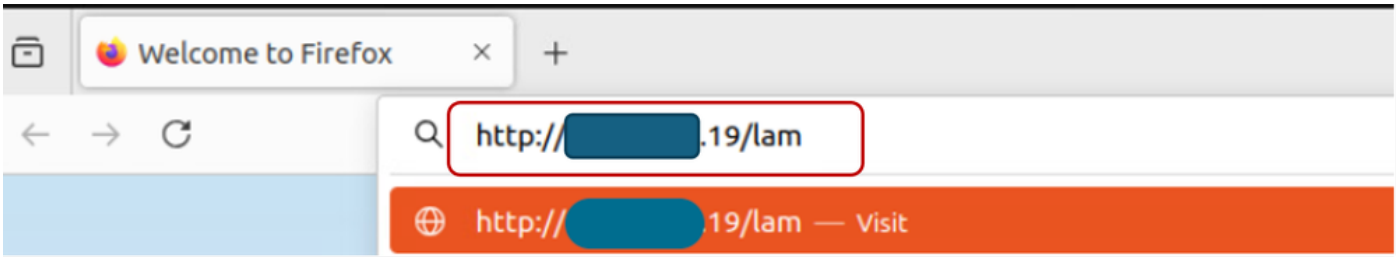
```
test@test:~$ sudo ufw status
Status: active

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)
```

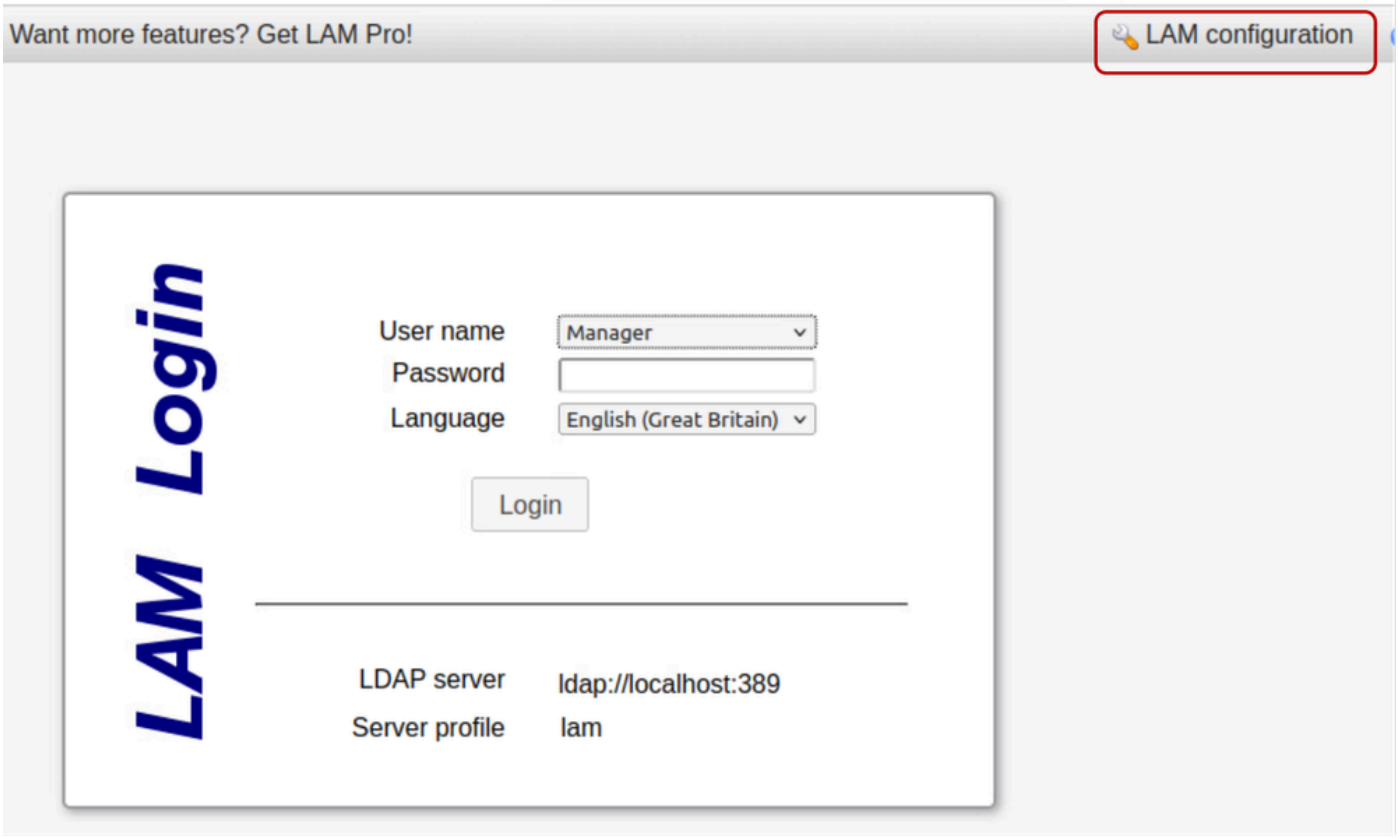
Paso 4: Configurar el administrador de cuentas LDAP

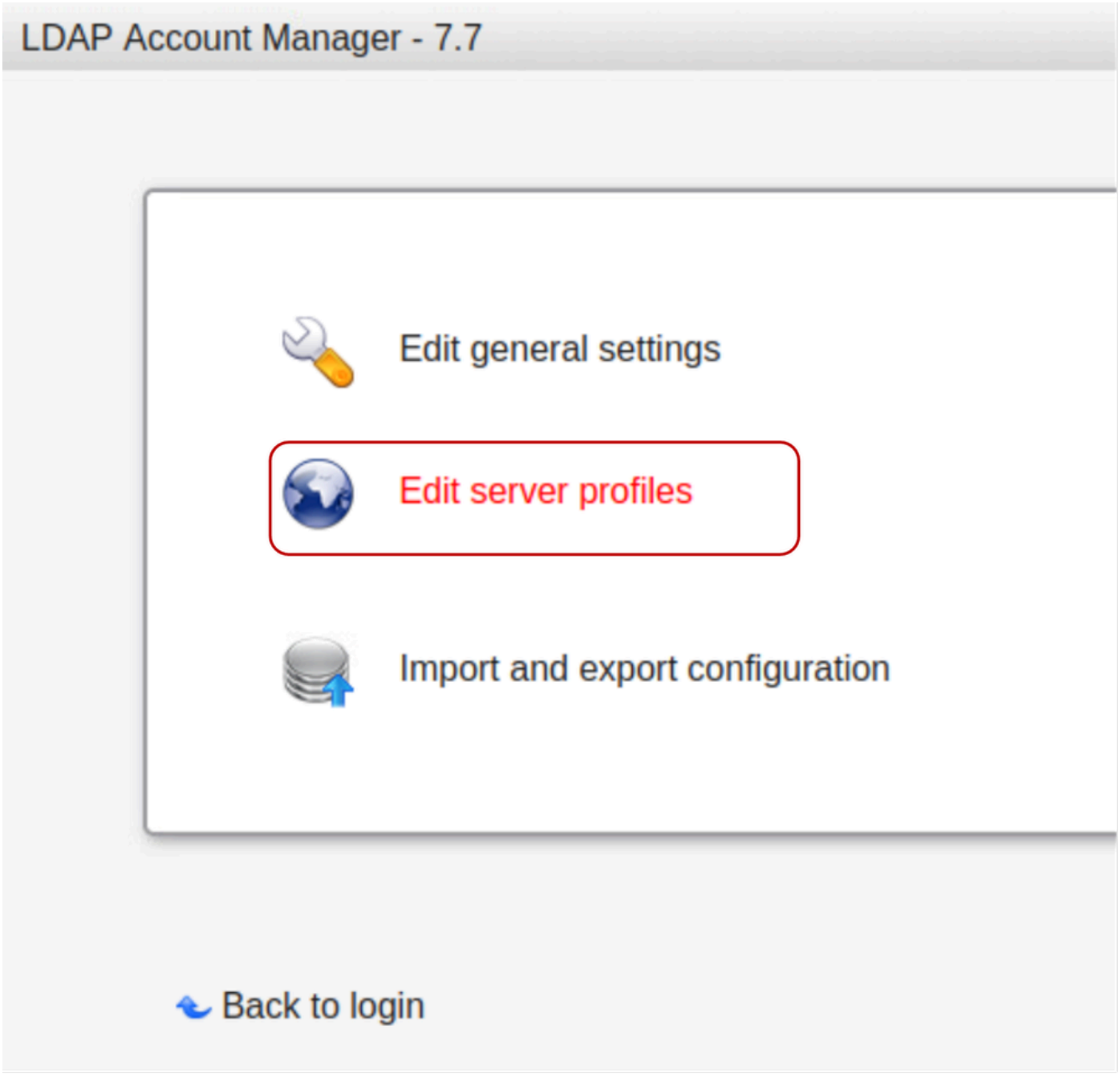
Para configurar el LDAP Account Manager (LAM) desde la GUI, abra un navegador web, ingrese la dirección IP del servidor Linux y agréguele la ruta 'lam' como se muestra:

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

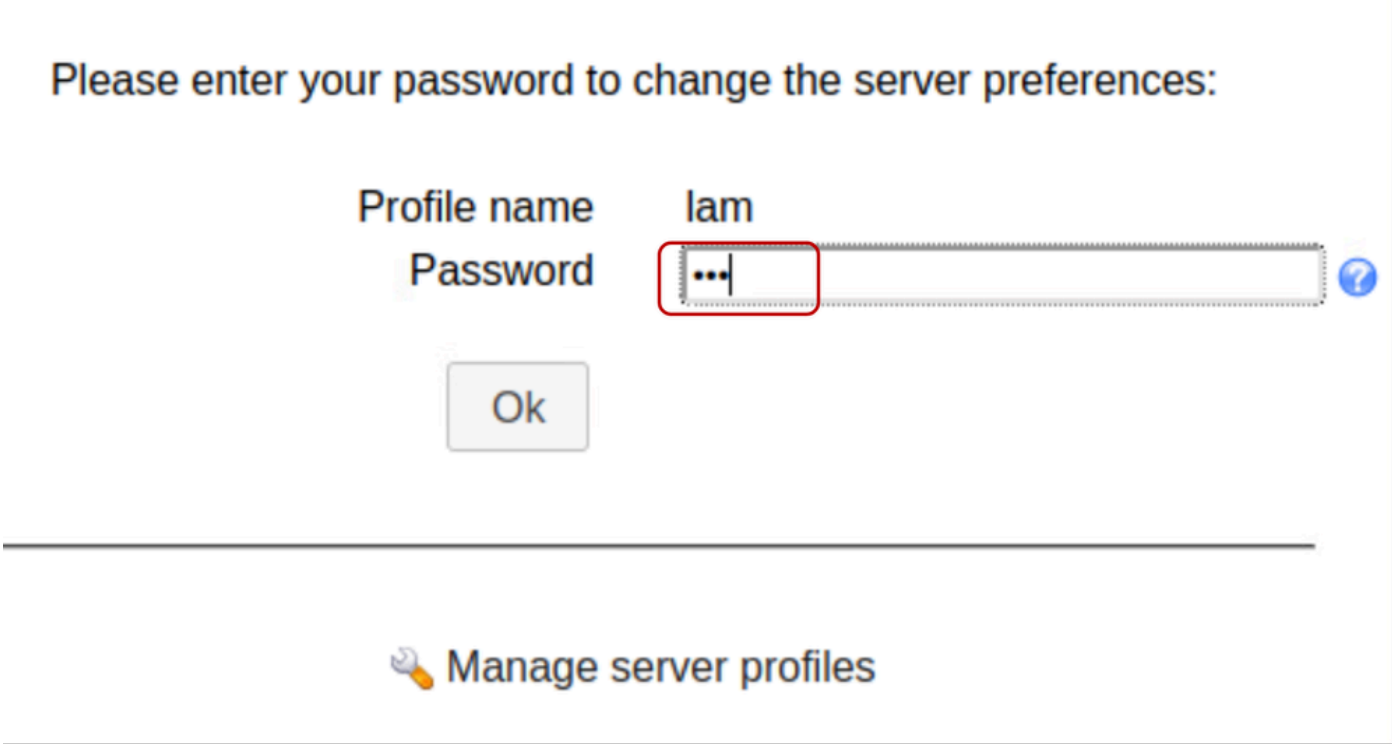


Haga clic en "Configuración de LAM" y seleccione "Editar perfiles de servidor".


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



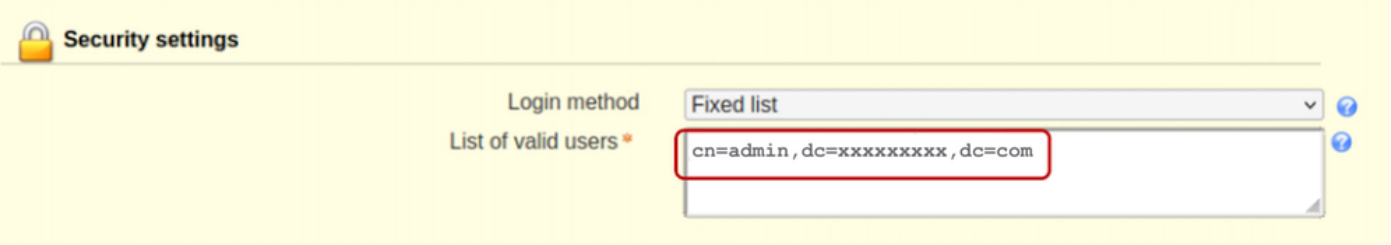
Escriba la contraseña de lam predeterminada "lam" para iniciar sesión.



En la ficha Configuración general, compruebe los parámetros del servidor, "Idioma" y "Zona horaria".

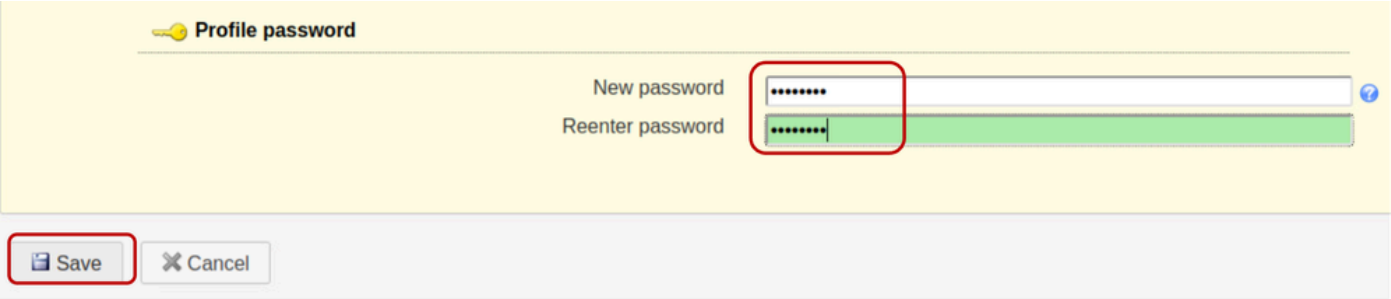
En la sección Configuración de herramientas, edite y agregue el nombre de dominio necesario en el campo Sufijo de árbol, como se muestra a continuación:

Edite la sección Configuración de seguridad para incluir un usuario "admin" utilizado para administrar el servicio SLAPD.



Establezca una "Contraseña del perfil". Esta contraseña se utiliza para los inicios de sesión subsiguientes en la interfaz de configuración de LAM; en este ejemplo, se configura "cisco123" en lugar de la contraseña "lam" predeterminada.

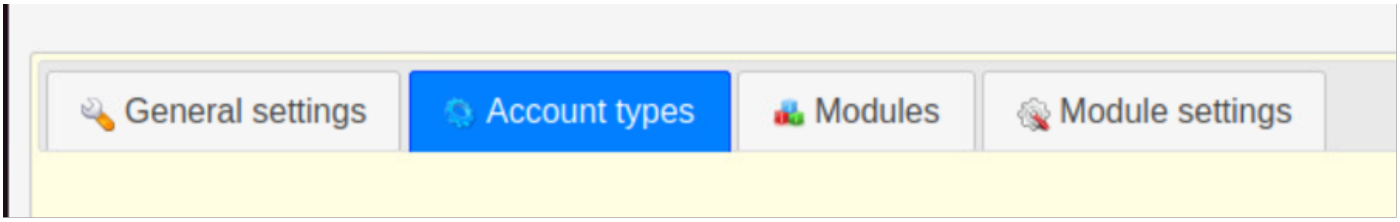
Guarde la configuración:



La sesión se reinicia en la interfaz GUI de configuración de LAM.

Vuelva a iniciar sesión (Configuración de LAM > Editar perfiles de servidor) con la nueva contraseña creada.

Haga clic en "Tipos de cuenta",



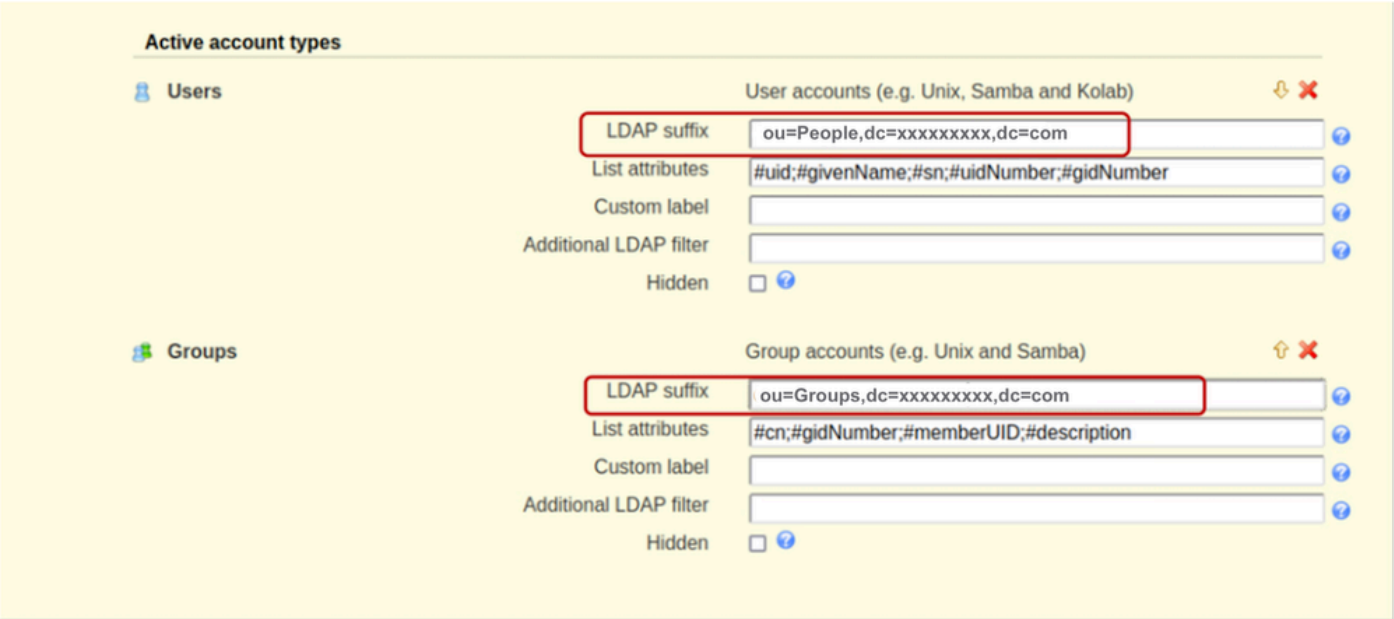
Desplácese hacia abajo y edite los tipos de cuenta activos predeterminados con la información de nombre de dominio en el campo de sufijo LDAP. Por ejemplo, el contenido predeterminado del campo "Sufijo LDAP" muestra un valor como "ou=Gente,dc=mi-dominio,dc=com".

En caso de que sea necesario crear nuevas unidades organizativas, sustituya el contenido del campo "Sufijo LDAP" para que contenga el nombre de la unidad organizativa.

El formato se muestra como "ou=<unidad_organizativa>,dc=xxxxxxxx,dc=com".

Para esta demostración, la unidad organizativa para usuarios es "Personas" y la unidad organizativa para grupos es "Grupos".

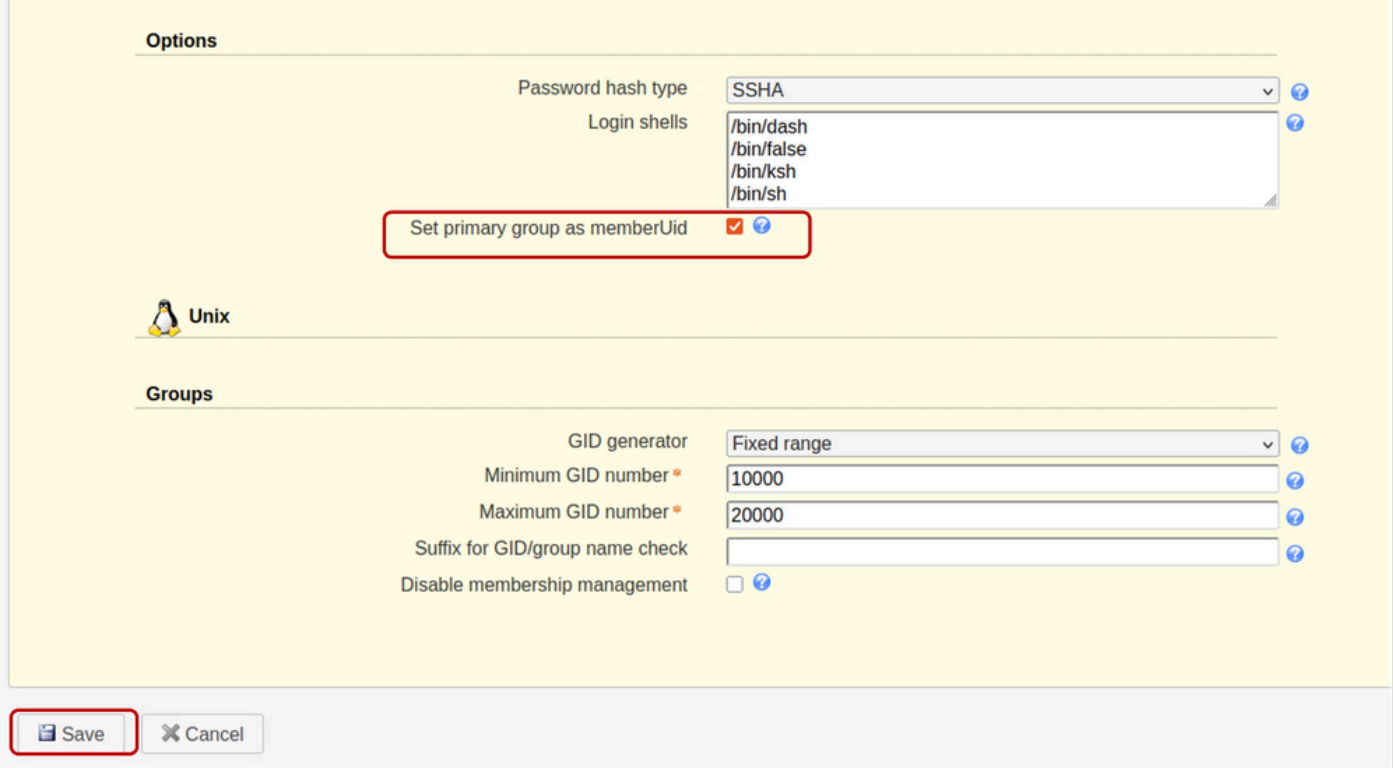
Guarde la configuración.



Desplácese hasta la sección Opciones y asegúrese de marcar la opción "Establecer grupo principal como memberUid".

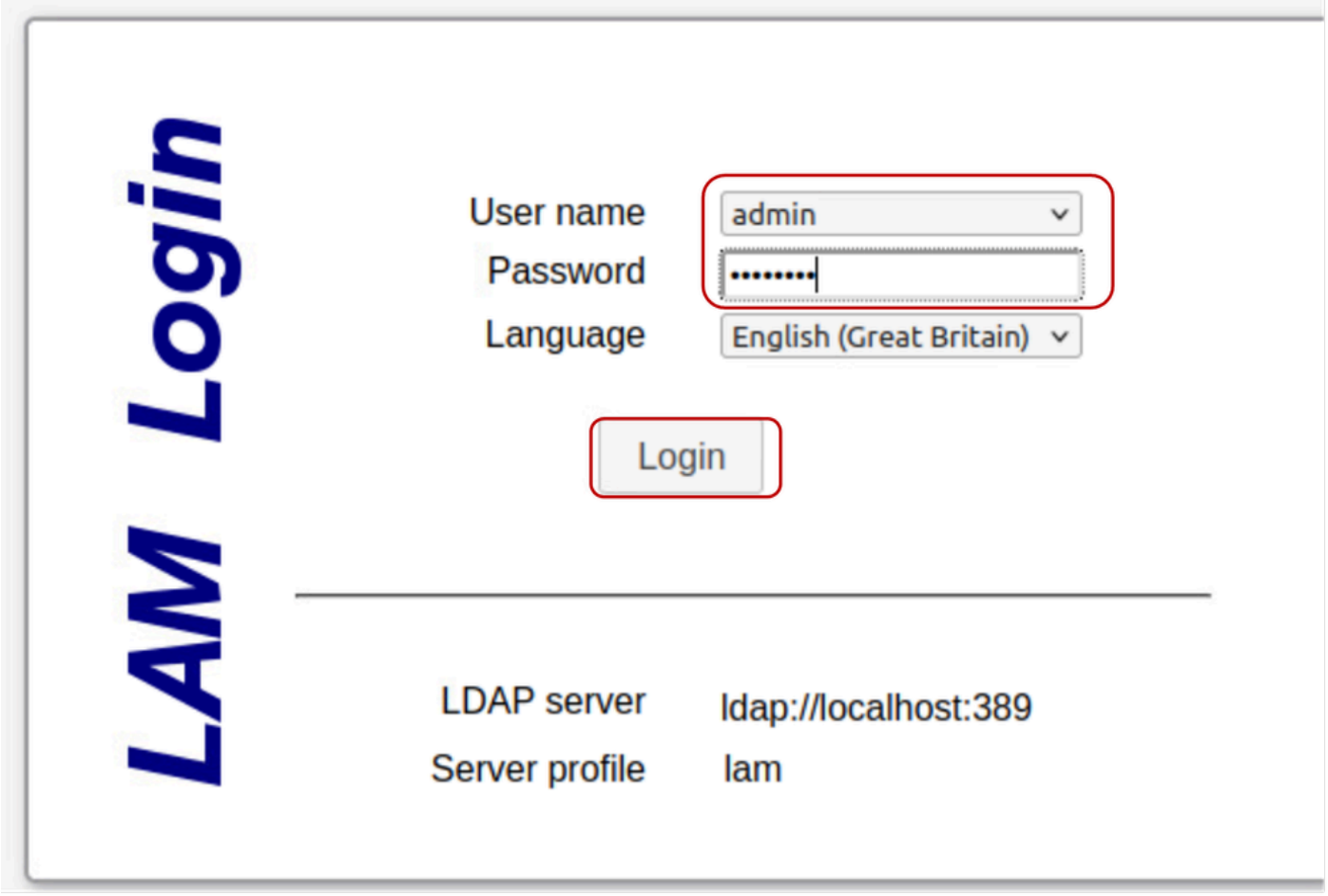
De forma predeterminada, la opción "Establecer grupo principal como memberUid" no está establecida en objetos de grupo. La activación de esto permite el uso de OpenLDAP "Primary group" como un grupo LDAP estándar, donde se puede hacer referencia al "memberUid" (por ejemplo: en la configuración del servidor de la serie C de UCS). Si esta opción no está marcada, el inicio de sesión de los usuarios que pertenezcan a cualquier grupo principal fallará.

Guarde la configuración.

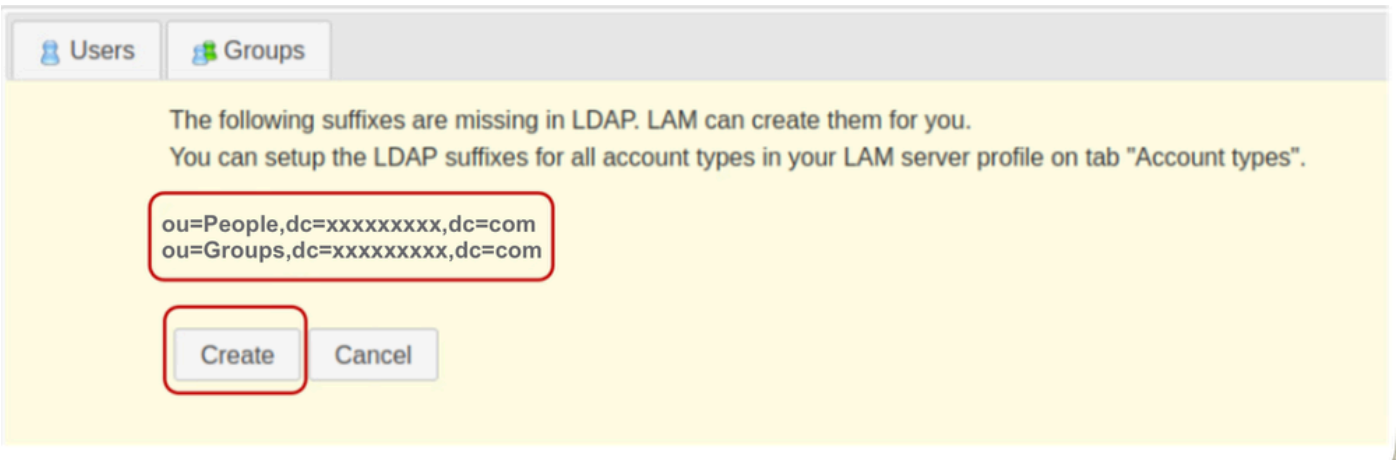


Paso 5: Crear unidades organizativas, grupos y usuarios

Inicie sesión en LAM como el usuario "admin" con la misma contraseña creada durante la instalación, para crear Usuarios y Grupos que pertenezcan a las OU creadas anteriormente (Personas y Grupos), respectivamente:

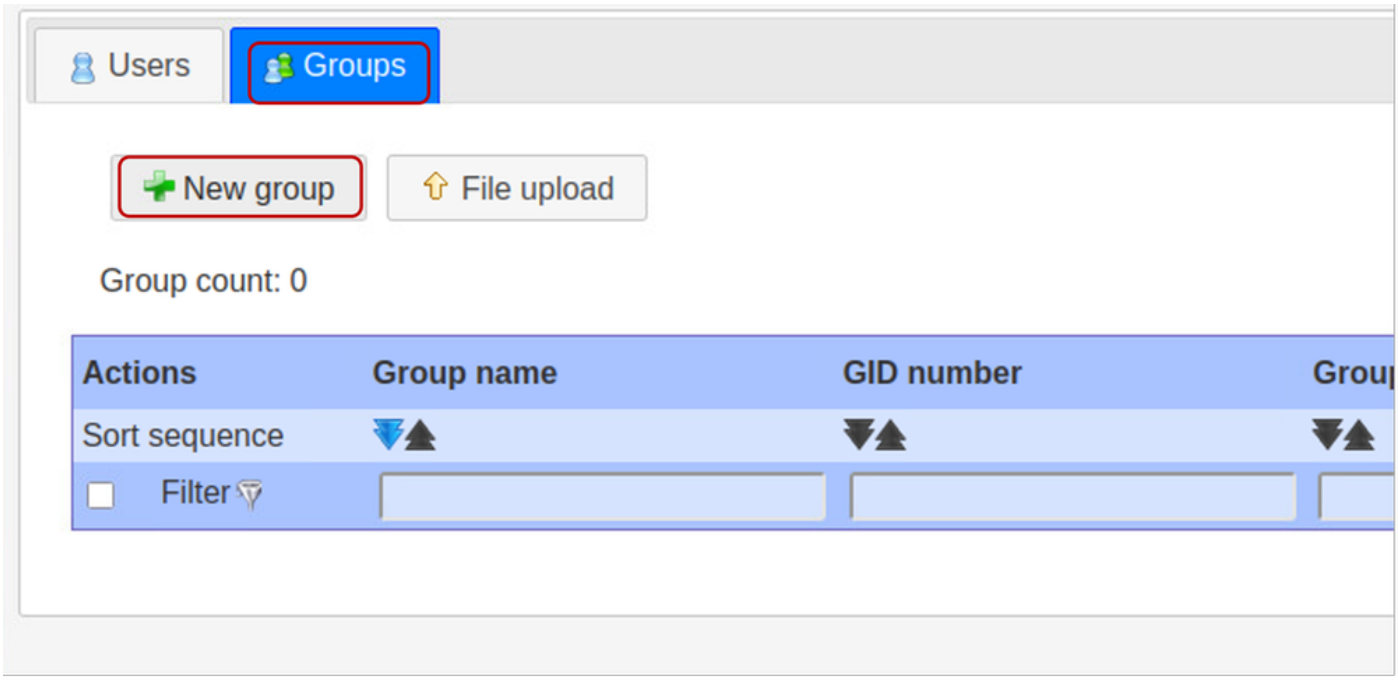


Cree las OU especificadas anteriormente en la sección Configuración de LAM.
Haga clic en Crear.



A continuación, en LDAP Account Manager, cree el grupo "it":

Seleccione la ficha Grupos y haga clic en Nuevo grupo

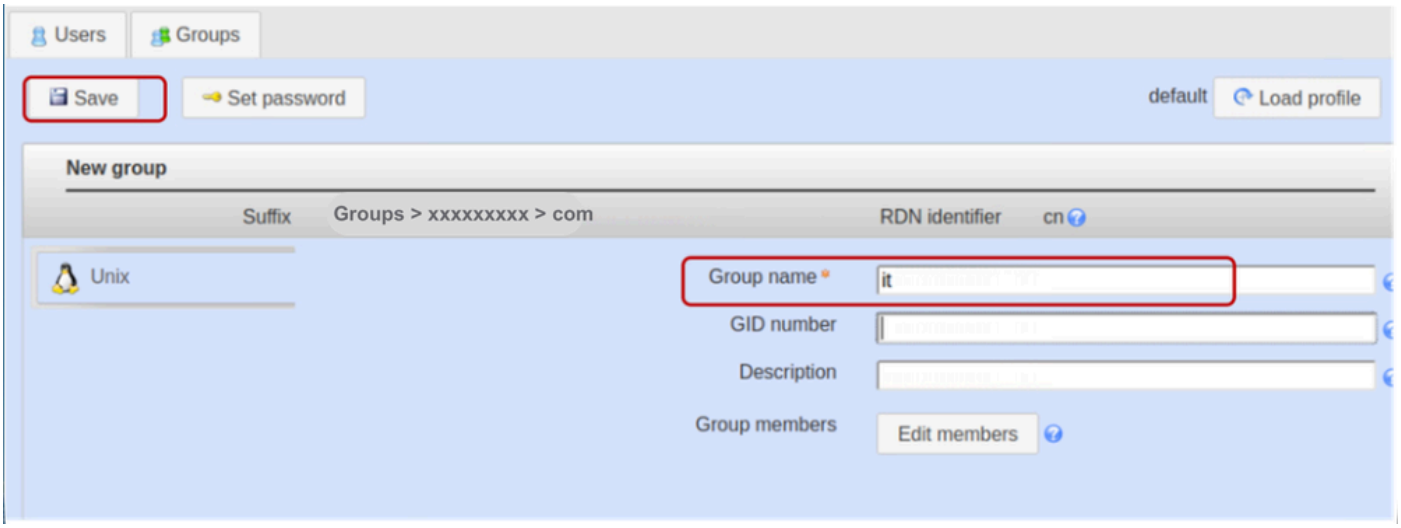


Establezca el nombre del grupo como "it".

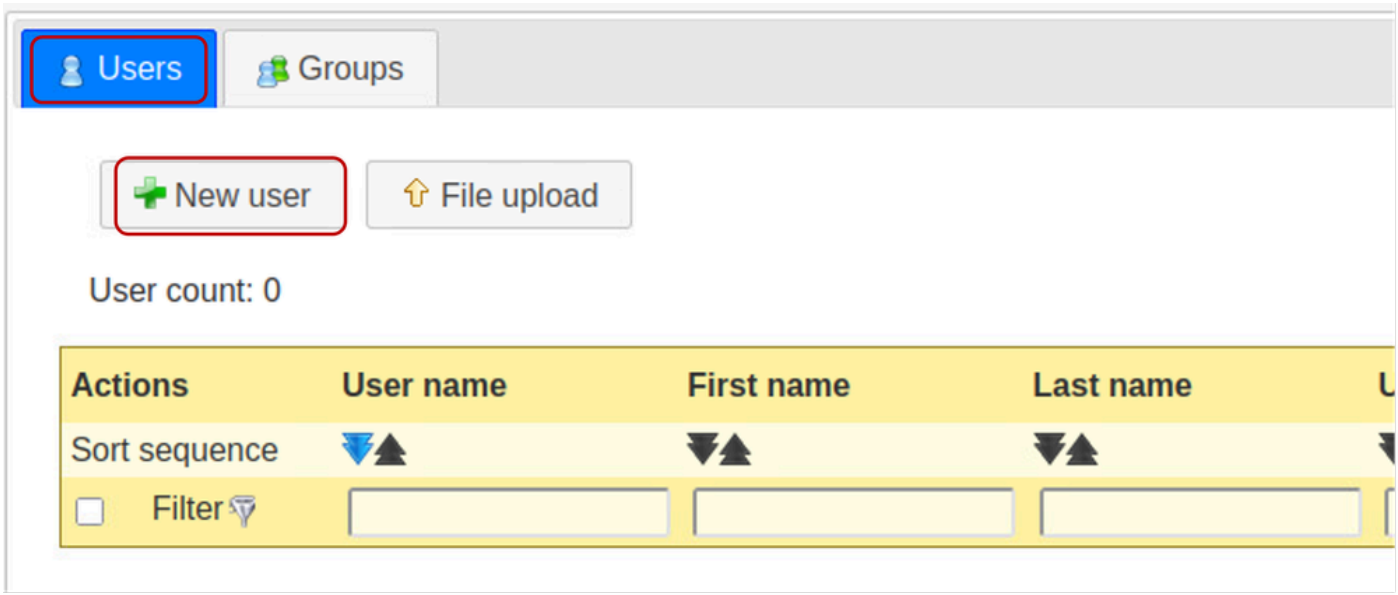
Nota: Aunque los sistemas Cisco UCS suelen ser resistentes a las variaciones de casos, el mantenimiento de las convenciones de nomenclatura en minúsculas es una práctica recomendada para garantizar la interoperabilidad a largo plazo entre los diversos entornos de infraestructura de servidores LDAP.

Deje el campo Número GID en blanco. LDAP Account Manager (LAM) está diseñado para rellenar automáticamente este campo con el siguiente valor disponible.

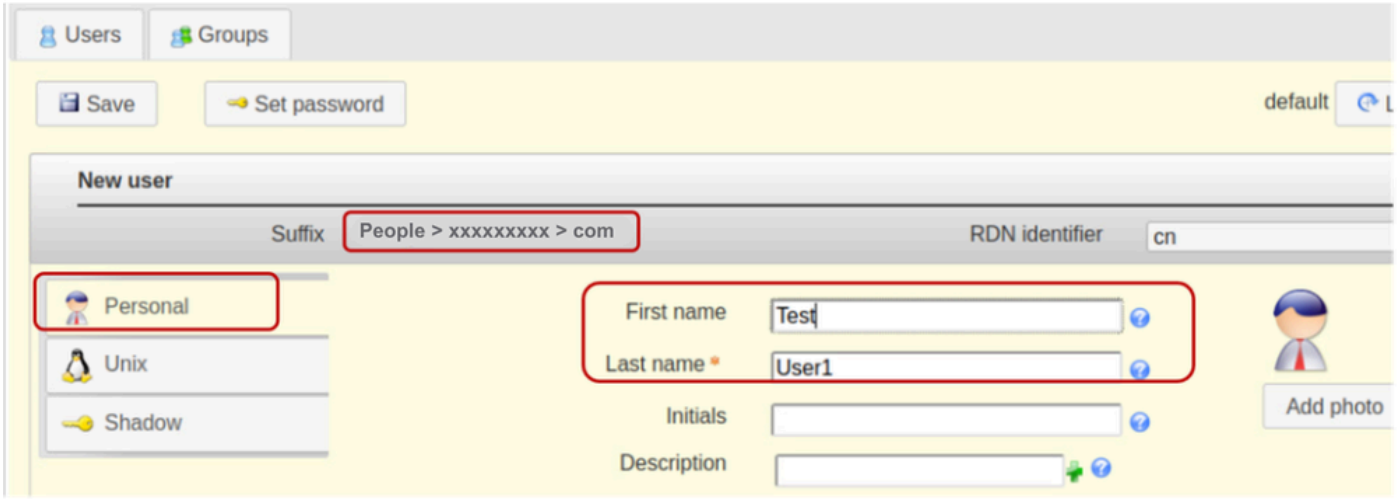
Proporcione una descripción si lo desea y haga clic en Guardar



Haga clic en la ficha "Users" (Usuarios) para crear cuentas de usuario y seleccione "New user" (Nuevo usuario).



Rellene los campos obligatorios para el usuario "testuser1" en la ficha Personal.



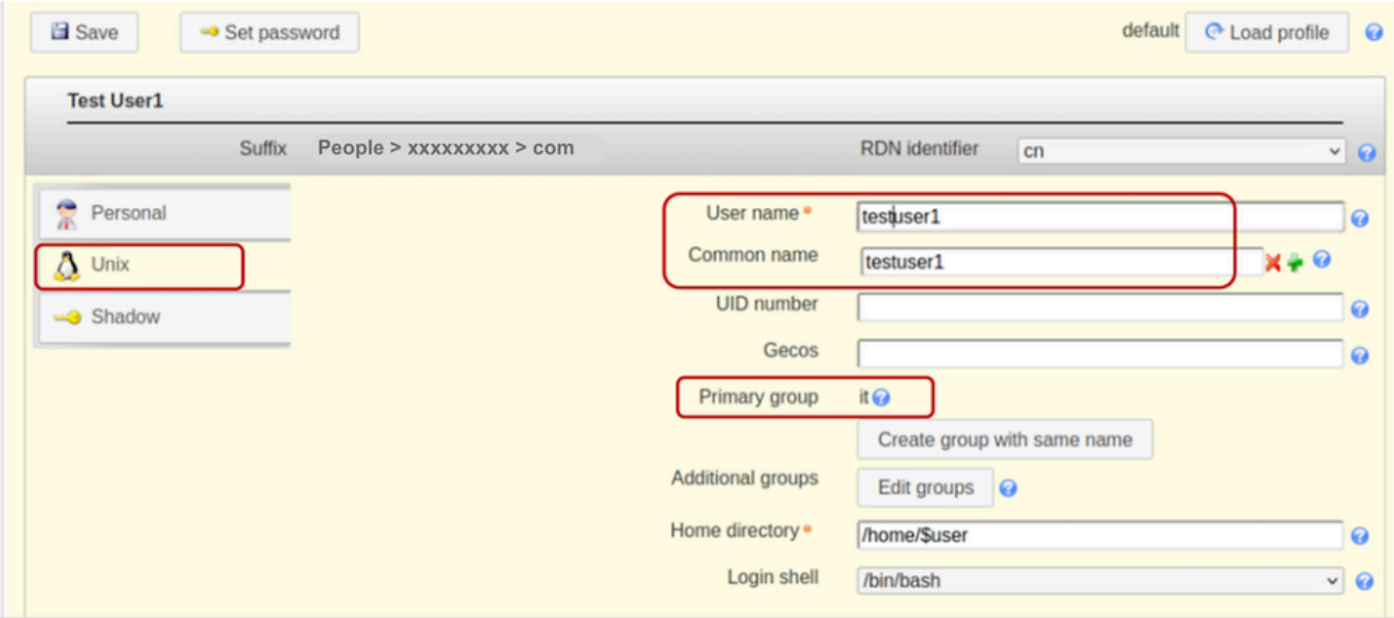
Seleccione la ficha Unix y agregue testuser1 en el campo User name (Nombre de usuario). Incluya al usuario en el grupo "it".

Para esta demostración, solo existe el grupo "it", por lo que ya se ha rellenado previamente.

Mantenga el identificador RDN como "Common Name" (cn). Esto permite al sistema rellenar automáticamente el campo "Nombre común" con el valor especificado en el campo "Nombre de usuario".

Deje el campo Número de UID en blanco, ya que LAM rellena automáticamente el campo con los

valores disponibles.



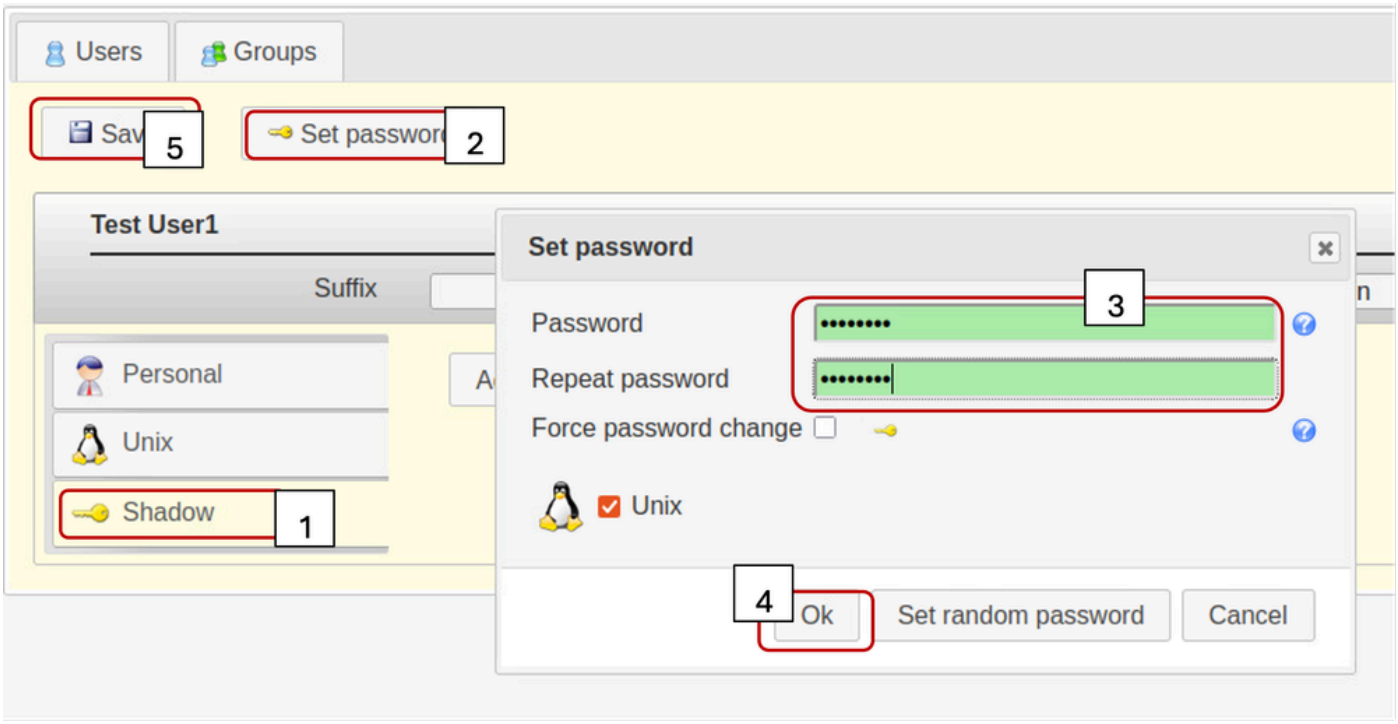
Seleccione la ficha Sombra,

No se usa la extensión de cuenta de instantáneas.

Haga clic en "Establecer contraseña".

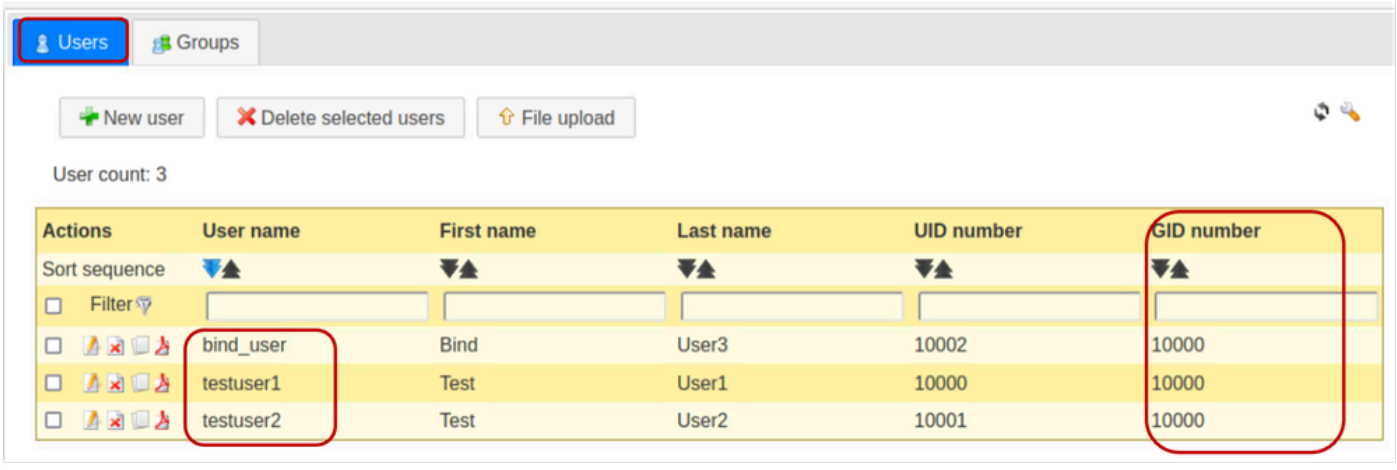
Establecer la contraseña de usuario

Haga clic en Aceptar y Guardar



Repita los pasos especificados descritos anteriormente para crear la cuenta de usuario "testuser2" y la cuenta "bind_user".

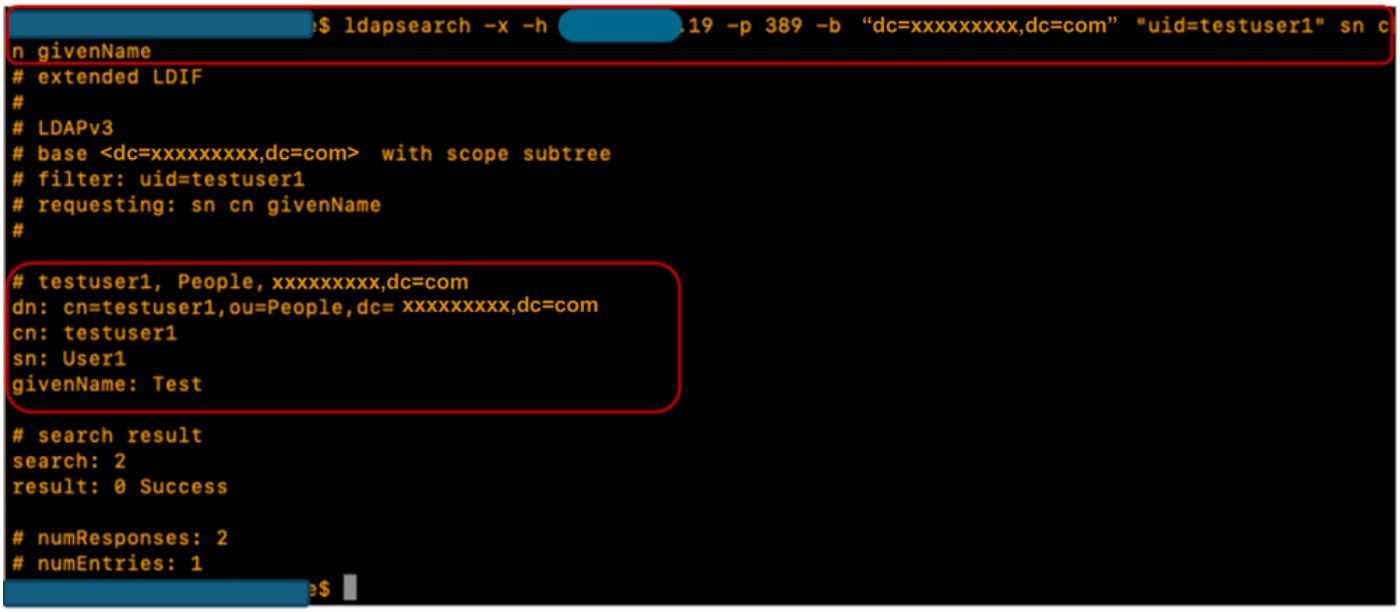
Haga clic en la ficha "Users" (Usuarios) para verificar la creación de todos los usuarios deseados. (Si tiene el mismo valor en la columna gidNumber, se confirma que los usuarios creados pertenecen al mismo grupo, es decir, el mismo grupo)



Paso 6: Prueba el inicio de sesión LDAP local

Inicie sesión en otro sistema basado en Linux, teniendo acceso al servidor OpenLDAP.
Ejecute el comando ldapsearch especificado para verificar que LDAP funcione:

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



Parámetros de configuración en CIMC

Inicie sesión en CIMC.

En el panel de navegación, seleccione Admin, User Management y LDAP.

Rellene los parámetros de configuración de LDAP como se muestra a continuación:

- Habilitar LDAP: activado
- DN base: dc=xxxxxxxxx,dc=com

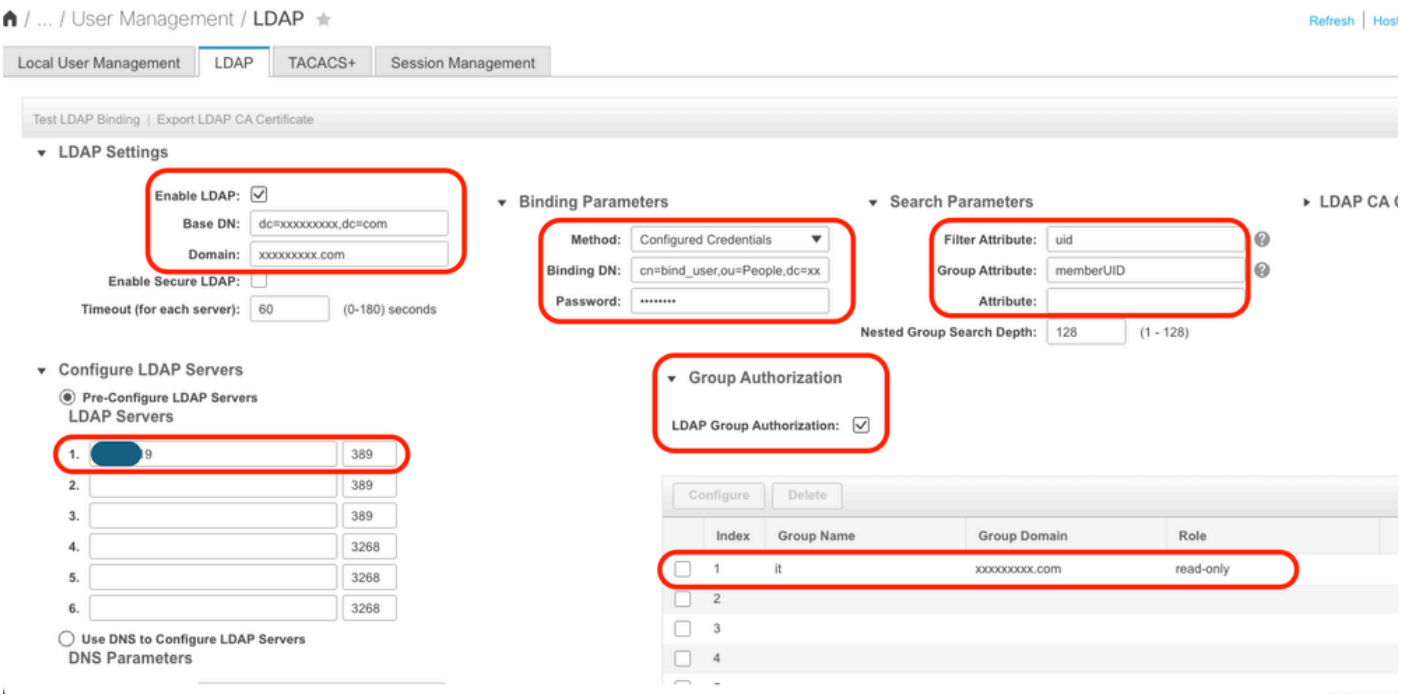
- Dominio: xxxxxxxxx.com

- Servidor LDAP: <ldap_server_IP o FQDN> X.X.X.19

- Parámetros de enlace: "Credenciales de conexión" o "Credenciales configuradas"
  - Cuando utilice las credenciales configuradas, agregue el DN bind_user exactamente como se configuró en el servidor LDAP:
    - Por ejemplo: cn=bind_user,ou=People,dc=xxxxxxxxx,dc=com

- Parámetros de búsqueda:
  - Atributo de filtro: "cn" o "uid"
  - Atributo de grupo: memberUID

- Autorización de grupo LDAP: activada
  - Nombre de grupo: it
  - Dominio de grupo: xxxxxxxxx.com
  - Función: sólo lectura (cualquier función que desee)



Guarde la configuración y pruebe el inicio de sesión de usuario LDAP.

Parámetros de configuración en UCS Manager

Inicie sesión en UCS Manager.

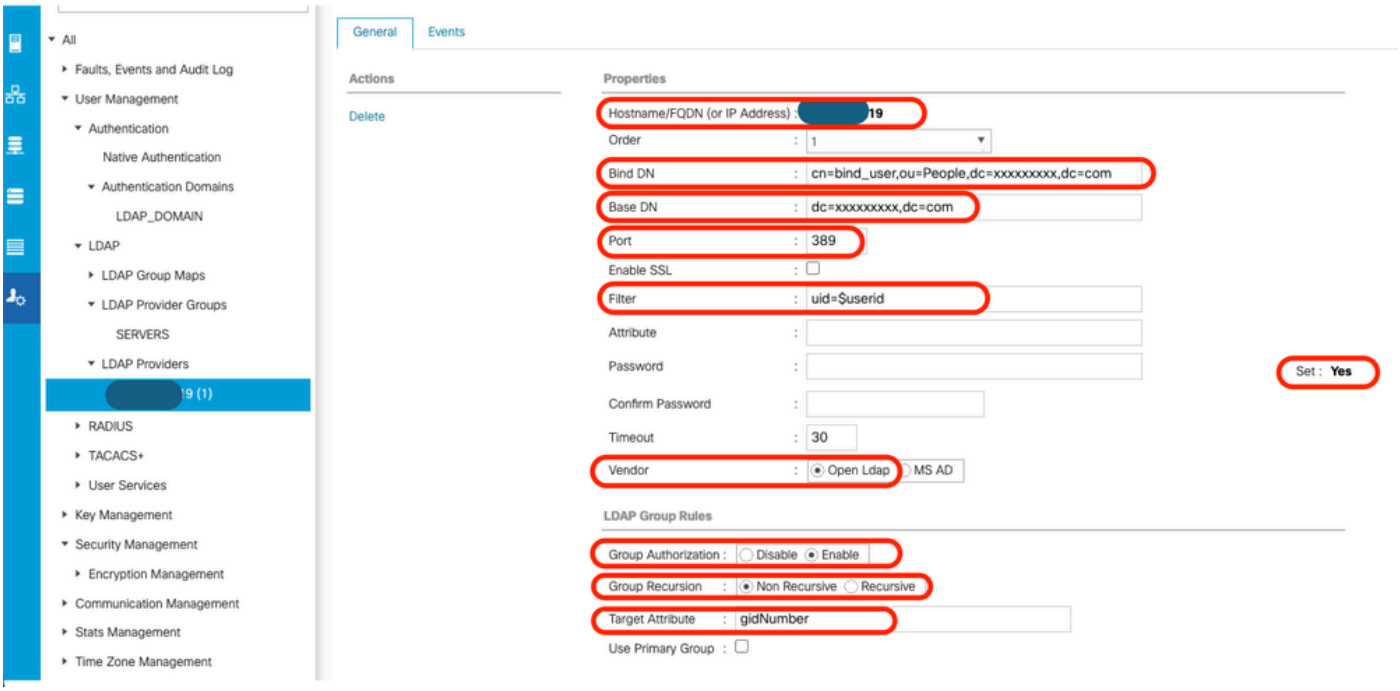
En el panel de navegación, seleccione Admin, User Management y LDAP.

Rellene los parámetros de configuración de LDAP como se muestra a continuación:

- Proveedores LDAP:
  - Nombre de host: <FQDN o dirección IP del servidor LDAP>
  - Enlazar DN: cn=bind_user,ou=People,dc=xxxxxxxxx,dc=com
  - DN base: dc=xxxxxxxxx,dc=com
  - Puerto: 389
  - Habilitar SSL: Inhabilitado
  - Filtro: uid=$userid
  - Autorización de grupo: Habilitado
  - Recursión de grupo: No recursivo

- Atributo de destino: gidNumber

- Mapas de grupo LDAP:
  - DN de grupo LDAP: 10000 <gidNumber for "it" group>

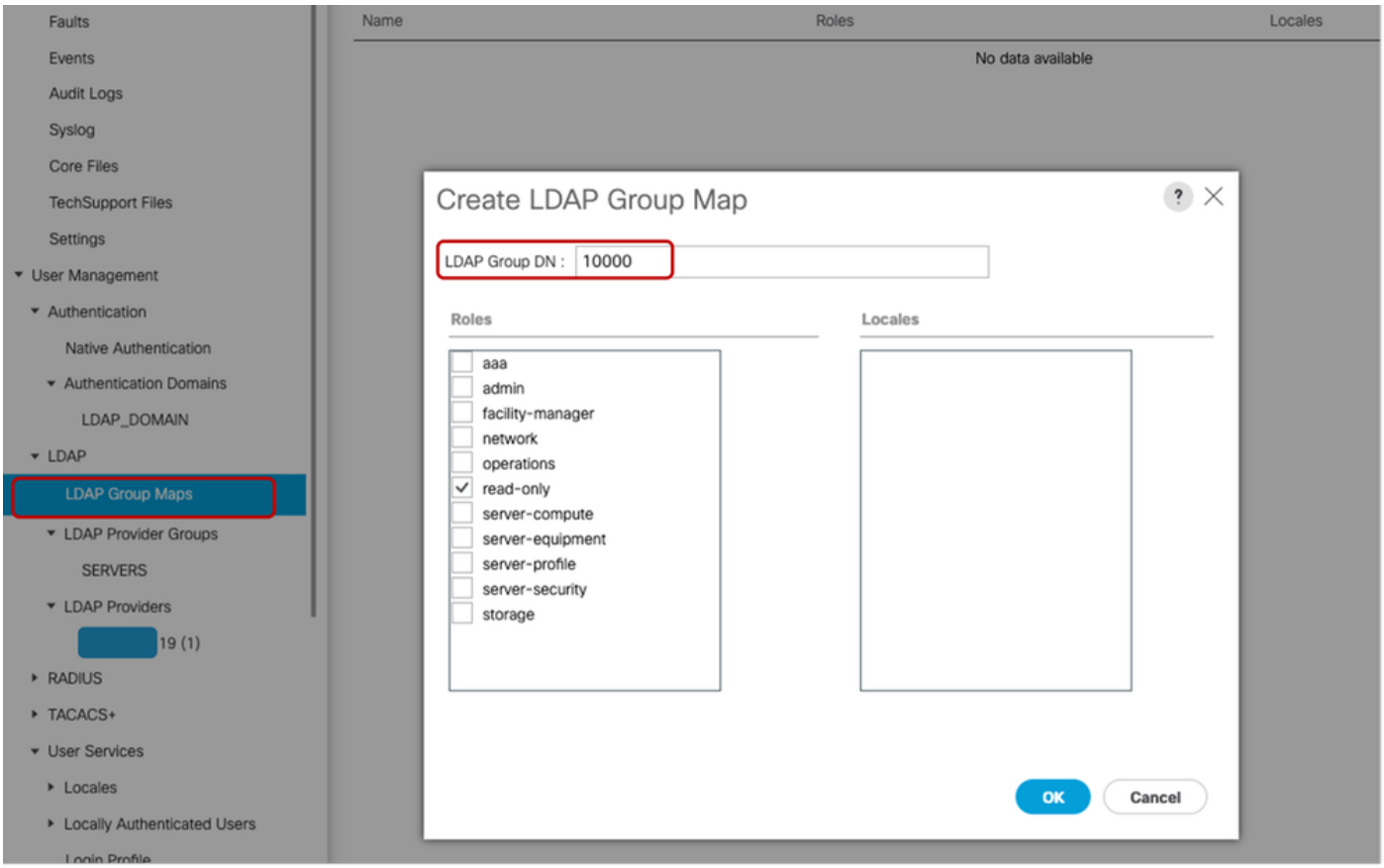


En Todas > Administración de usuarios > LDAP > Proveedores LDAP > Reglas de grupo LDAP, el atributo de destino predeterminado del UCS Manager es "memberOf". De forma predeterminada, los servidores OpenLDAP no tienen ese atributo habilitado, por lo tanto, si se establece el valor de Atributo de destino en "memberOf" (o se deja en blanco), los inicios de sesión de los usuarios fallarán porque el servidor OpenLDAP no reconoce el valor de Atributo solicitado.

En este ejemplo, el valor "Target Attribute" se ha establecido en "gidNumber".

Agregue el proveedor LDAP configurado a un grupo de proveedores LDAP. Para esta demostración, se ha creado el grupo de proveedores LDAP "SERVERS".

Al configurar "LDAP Group Maps" en "All >> User Management >> LDAP >> LDAP Group Maps>", el valor gidNumber (en este caso, "10000") se utiliza como "Group DN Map" tal como se muestra:



Configure un Dominio de Autenticación LDAP (LDAP_DOMAIN) en "All >> User Management > Authentication >> Authentication Domains" que hace referencia a los Grupos de Proveedores LDAP y pruebe el login de usuario LDAP.

Nota: Si se requiere el atributo memberOf para satisfacer requisitos ambientales específicos o para implementar la función "Recursión de grupo", se recomienda utilizar la segunda opción de configuración siguiente, que requiere LDAP con extensiones Overlay habilitadas.

Aunque el LDAP Account Manager (LAM) admite la configuración superpuesta, tenga en cuenta que esta función requiere las licencias adecuadas.

Para obtener más información sobre la configuración de LDAP mediante LAM, consulte la documentación oficial de LDAP Account Manager.

Opción 2: Configuración de OpenLDAP mediante herramientas y superposiciones de Ubuntu CLI

Para utilizar OpenLDAP para la autenticación de UCS Manager, se requieren dos superposiciones que garanticen que los grupos están asociados con los usuarios de una forma

que el sistema UCS (UCS Manager y CIMC) pueda comprender.

La configuración en el lado de OpenLDAP requiere:

- superposición "memberof": Esta superposición crea una asignación entre usuarios y grupos de modo que, si se consulta un DN de usuario, se puede solicitar el atributo memberOf como parte de esa consulta. De forma predeterminada, no hay ningún atributo para los usuarios de pertenencia a grupos a menos que el miembro de superposición se agregue a openLDAP
- superposición "refinada": Esta superposición se configura para validar que las entradas del atributo member en los objetos de grupo permanecen sincronizadas con el atributo memberOf de los objetos de usuario. Sin este servicio, si se elimina un usuario sin modificar también el grupo, los DN huérfanos pueden permanecer en el objeto de grupo. El servicio de refinamiento asegura la consistencia en ambas direcciones.

Paso 1: Net-tools inicial y configure el nombre de host del servidor Linux

Repita el paso 1 en la opción 1.

Paso 2: Instalar SLAPD

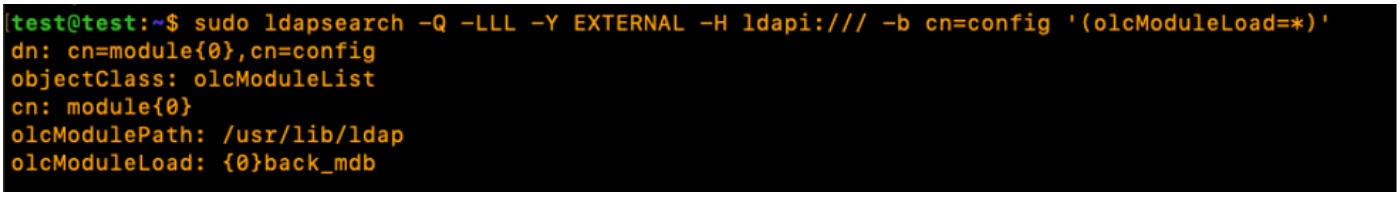
Repita el Paso 2 en la Opción 1. (Con la excepción de la instalación de PHP y Apache, ya que la Opción 2 no requiere que funcionen - no LAM)

Asegúrese de permitir los puertos necesarios a través del firewall de Ubuntu.

Paso 3: Instalar 'memberOf' Overlay en el servidor LDAP

Compruebe si la superposición "memberOf" está instalada

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



Para instalar la superposición "memberOf", cree un archivo .ldif denominado ldap.memberof.load.ldif (utilice la convención de nomenclatura que desee) y agregue la configuración especificada:

```
cat <



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

Agregue la configuración en el archivo ldap.memberof.load.ldif al perfil LDAP utilizando el comando especificado:

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

Configura el módulo memberOf y la entrada olcDatabase para que coincidan con los requisitos de implementación, dependiendo de las distribuciones de linux.

Dos valores de atributo obligatorios son "olcDatabase={1}mdb" y "groupOfNames", como se muestra a continuación.

Cree el archivo ldap.memberof.config.ldif, rellene sus atributos e importe su contenido en el perfil 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
```

Paso 4: Instale 'refint' Overlay en el servidor LDAP

A continuación, instale refint to openldap:

cree un archivo .ldif denominado ldap.refint.load.ldif (utilice la convención de nomenclatura que desee) y agregue la configuración especificada:

```
cat <

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

Importe la configuración del archivo ldap.refint.load.ldif al perfil LDAP mediante el comando especificado:

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

Configure refint, que mantiene la integridad referencial entre grupos y usuarios.

Configura el módulo refint y su entrada olcDatabase para que coincidan con los requisitos de implementación.

Cree el archivo ldap.refint.config.ldif e importe su contenido en el perfil LDAP.

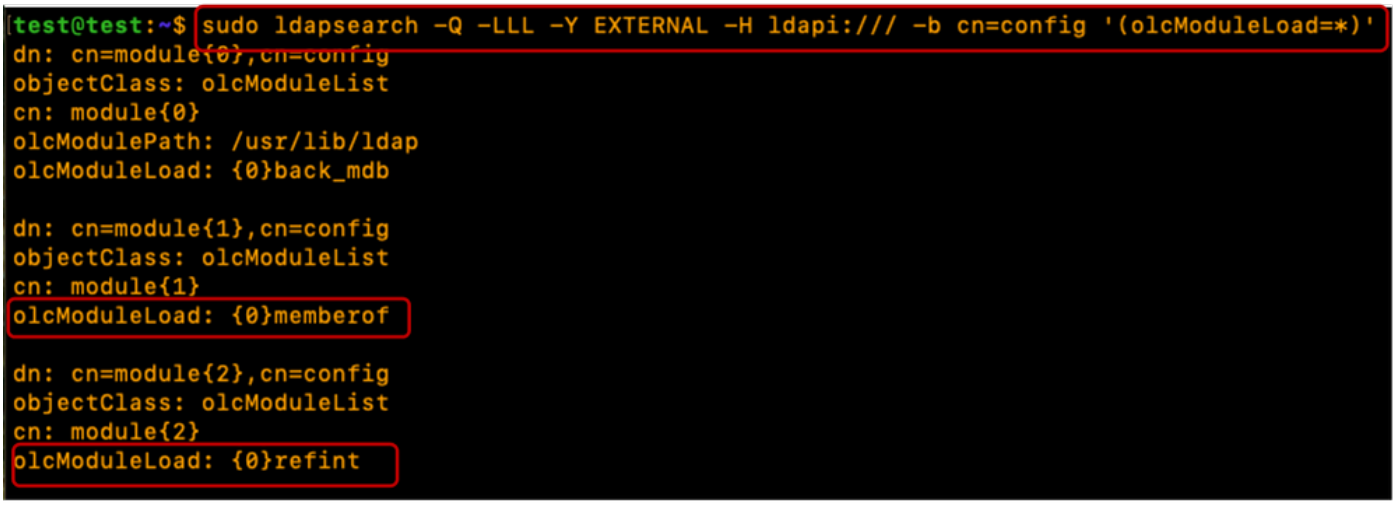
```
cat <
```

```
      ./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
```

Tras la instalación de ambos plugins/extensiones, el resultado del comando ldapsearch especificado es similar al resultado que se muestra a continuación:

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



Cuando se configuran ambos plugins/extensiones, la salida del comando ldapsearch especificado es similar a la salida mostrada:

```
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
```

Reinicie el servicio slapd para que los módulos/complementos recién instalados sean utilizables:

```
sudo systemctl restart slapd
```

Paso 5: Crear unidades organizativas, usuarios y grupos

Crear unidades organizativas (para usuarios y grupos), usuarios y grupos.

Cree las unidades organizativas de usuarios (personas) y grupos (grupos) e impórtelas al perfil LDAP. Esto requiere la contraseña de la cuenta "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
```

Cree los usuarios (testuser1, testuser2 y bind_user), asígnelos a sus respectivas OU (personas), agréguelos a sus grupos mediante gidNumbers (buena práctica) e importe los usuarios al perfil 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:~$
```

Cree los grupos (it), asígnelos a sus OU respectivas (Groups), asocie miembros del grupo (testuser1, testuser2) e impórtelos al perfil 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
```

Nota: Incluso si el atributo memberOf no se define explícitamente durante la creación de Usuarios o Grupos, el sistema genera y mantiene automáticamente esta referencia. Una vez que el usuario está asociado a un grupo, el atributo memberOf refleja automáticamente estas pertenencias, lo que garantiza que el directorio permanezca sincronizado con la estructura de acceso actual.

Paso 6: Prueba el inicio de sesión LDAP local

Verifique el inicio de sesión del usuario en el servidor LDAP mediante el comando especificado (reemplace los parámetros de inicio de sesión según su entorno):

```
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:~$
```

Parámetros de configuración en CIMC

Inicie sesión en CIMC.

En el panel de navegación, seleccione Admin, User Management y LDAP.

Rellene los parámetros de configuración de LDAP como se muestra a continuación:

- Habilitar LDAP: activado
- DN base: dc=xxxxxxxxx,dc=com

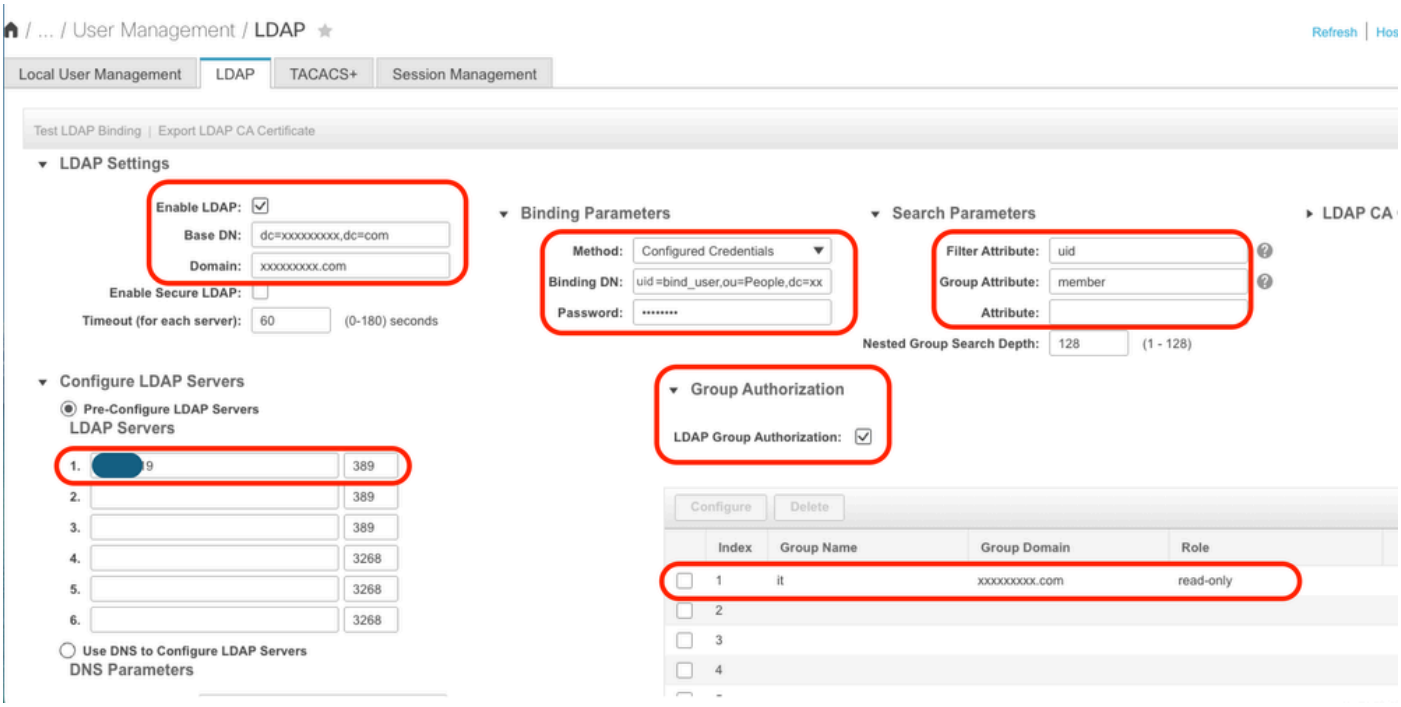
- Dominio: xxxxxxxxx.com

- Servidores LDAP: <ldap_server_IP o FQDN> X.X.X.19

- Parámetros de enlace: Puede ser "Credenciales de inicio de sesión" o "Credenciales configuradas"
    - Cuando utilice las credenciales configuradas, agregue el DN bind_user exactamente como se configuró en el servidor LDAP:
    - Por ejemplo: "cn=bind_user,ou=People,dc=xxxxxxxxx,dc=com" o "uid=bind_user,ou=People,dc=xxxxxxxxx,dc=com"

- Parámetros de búsqueda:
    - Atributo de filtro: "cn" o "uid"
    - Atributo de grupo: miembro

- Autorización de grupo LDAP: activada
    - Nombre de grupo: it
    - Dominio de grupo: xxxxxxxxx.com
    - Función: sólo lectura (cualquier función preferida)



Guarde la configuración y pruebe el inicio de sesión de usuario LDAP.

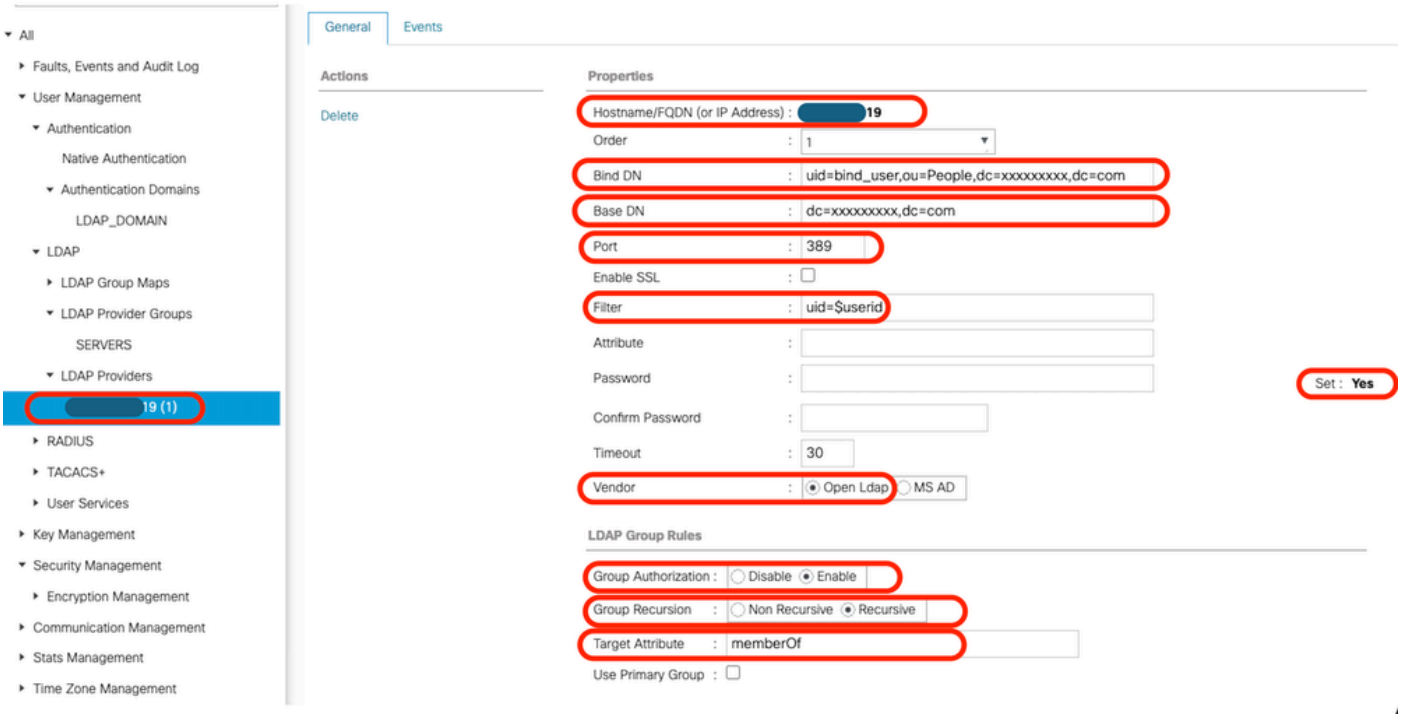
Parámetros de configuración en UCS Manager

Inicie sesión en UCS Manager.

En el panel de navegación, seleccione Admin, User Management y LDAP.

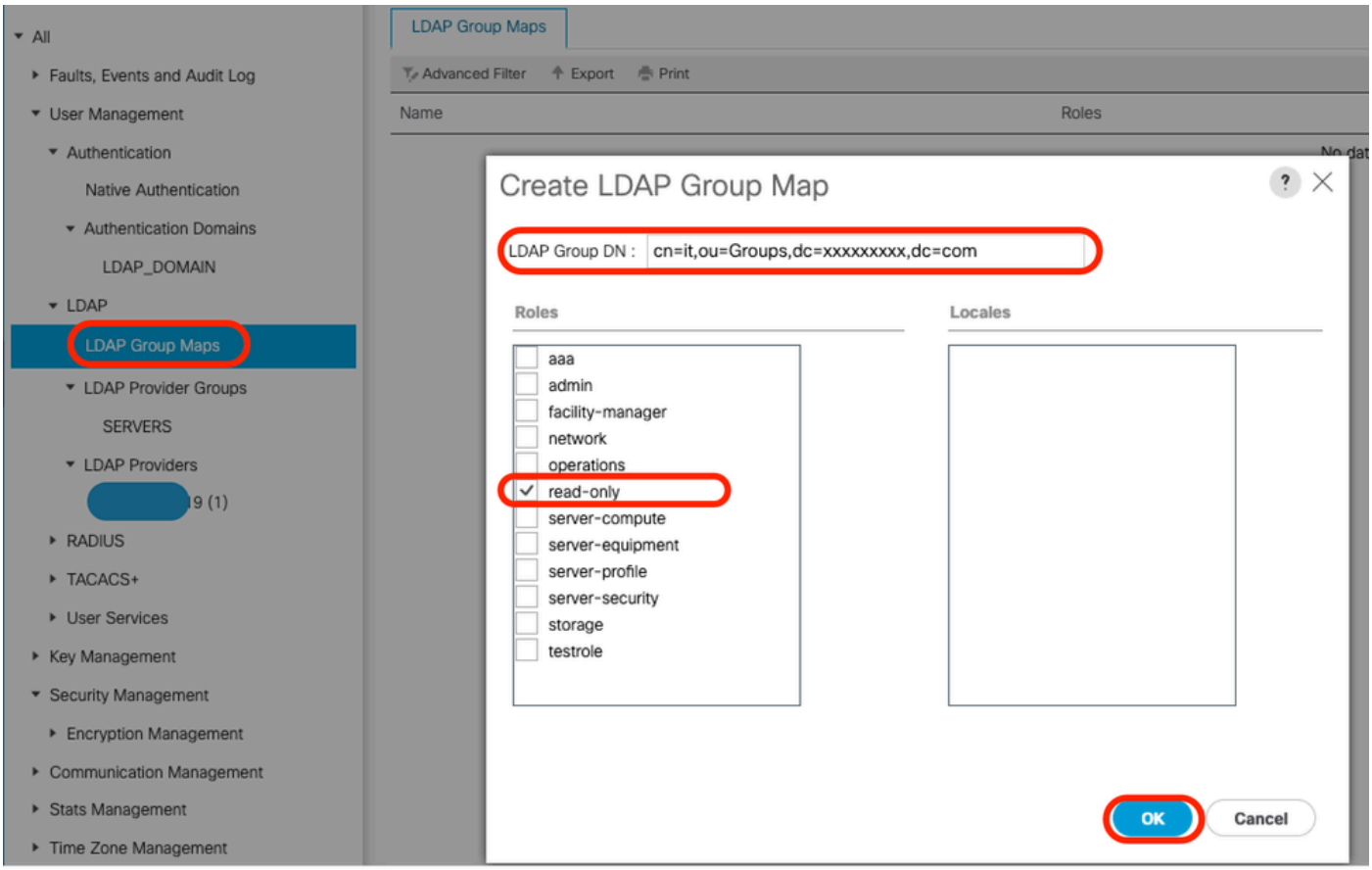
Rellene los parámetros de configuración de LDAP como se muestra a continuación:

- Proveedores LDAP:
  - Nombre de host: <FQDN o dirección IP del servidor LDAP>
  - Enlazar DN: uid=bind_user,ou=People,dc=xxxxxxxxx,dc=com
  - DN base: dc=xxxxxxxxx,dc=com
  - Puerto: 389
  - Habilitar SSL: Inhabilitado
  - Filtro: uid=$userid
  - Autorización de grupo: Habilitado
  - Recursión de grupo: Recursivo
  - Atributo de destino: memberOf
- Mapas de grupo LDAP:
  - DN de grupo LDAP: cn=it,ou=Groups,dc=xxxxxxxxx,dc=com



Agregue el proveedor LDAP configurado a un grupo de proveedores LDAP. Para esta demostración, se utiliza el grupo de proveedores LDAP "SERVERS".

Configure los Mapas de Grupo LDAP agregando un "DN de Grupo LDAP", recuperado del servidor LDAP.



Configure un Dominio de Autenticación LDAP (LDAP_DOMAIN) en "Todos >> Administración de Usuarios >> Autenticación >> Dominios de Autenticación" que haga referencia a los Grupos de Proveedores LDAP(SERVIDORES) y pruebe el login de usuario LDAP.

A continuación, veamos cómo configurar el mismo (con Overlay) en una distribución de Linux independiente (CentOS 10)

Escenario 2: CentOS Stream 10 - Fedora

Los procedimientos de configuración del protocolo ligero de acceso a directorios (LDAP) varían en función de la versión del sistema operativo subyacente. Esta sección se centra en la implementación de LDAP en CentOS Stream 10.

Mientras que muchas distribuciones Linux utilizan OpenLDAP, CentOS Stream 10 y los sistemas contemporáneos basados en Fedora utilizan 389 Directory Server (389 DS) como el proveedor LDAP predeterminado.

Nota: Aunque 389 DS se considera el sucesor de OpenLDAP dentro de los ecosistemas de CentOS y Red Hat, las dos soluciones no son directamente intercambiables. Sus respectivas estructuras de directorios, archivos de configuración y entornos operativos difieren significativamente.

Esta guía proporciona los pasos necesarios para configurar con éxito LDAP utilizando 389 DS dentro de un entorno CentOS Stream 10.

Opción 1: Configuración de LDAP mediante 389 Directory Server en CentOS Stream 10

Paso 1: Configuración inicial

Repita el paso 1 en el escenario 1, opción 1.

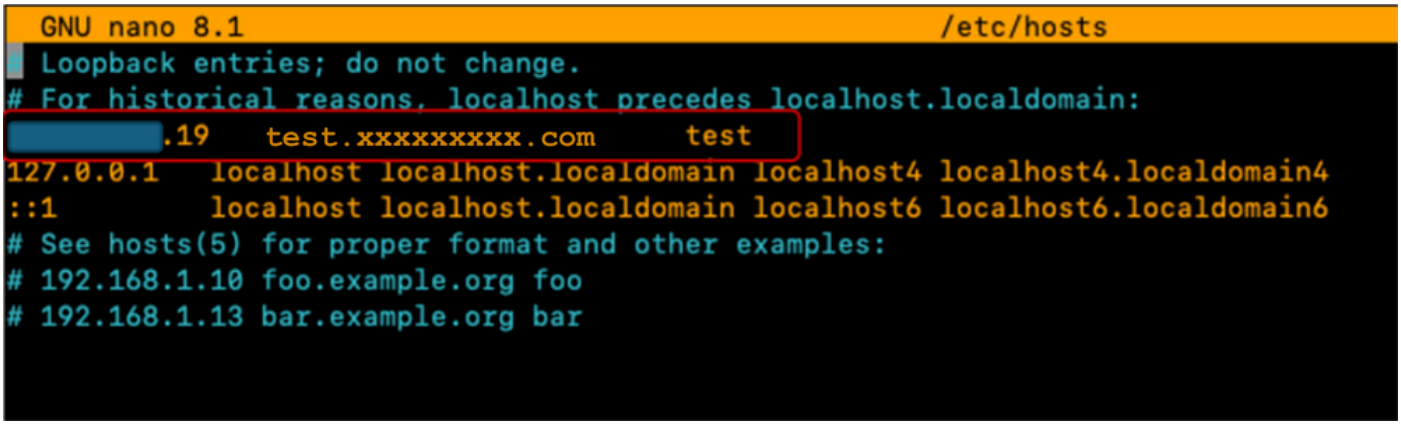
Los sistemas CentOS no utilizan la suite de gestión de paquetes APT. Para realizar las instalaciones de software necesarias en CentOS Stream 10, utilice los gestores de paquetes dnf (Dandified YUM) o yum

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

Verifique la dirección IP del servidor mediante el comando "ifconfig".

Agregue la dirección IP del servidor al archivo "/etc/hosts" junto con el nombre de dominio completo del servidor (por ejemplo: test.xxxxxxxx.com utilizado en este laboratorio) y el nombre de host (por ejemplo: test) en el formato especificado a continuación:

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



Actualice el archivo "/etc/hostname" sustituyendo su contenido por el nombre de host (prueba).

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

Es necesario reiniciar el servidor para que estos cambios surtan efecto.

```
sudo reboot
```

Paso 2: Instalar el paquete de repo EPEL y 389 Server

Instale y actualice el repositorio EPEL.

Instale el paquete 389 Directory Server.

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

Cree un archivo de plantilla de directorio que contenga los parámetros de configuración del servidor LDAP deseados:

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

Verifique el contenido del archivo de plantilla creado (ldapconfig.conf)

```
sudo cat ldapconfig.conf
```

Edite el archivo de plantilla ldapconfig.conf.

```
sudo nano ldapconfig.conf
```

Inserte las entradas de configuración especificadas en el archivo y guarde los cambios.

Nota:Pueden requerirse diferentes modificaciones según las necesidades o requisitos específicos de cada entorno.

En este ejemplo se describen las configuraciones básicas de esta demostración.

```
[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
```

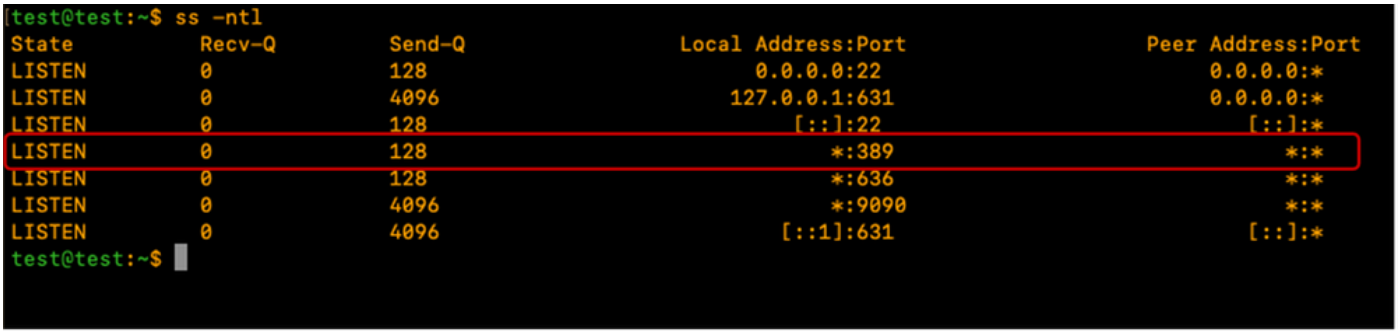
El archivo de plantilla define los parámetros de configuración para la instancia de directorio "localhost". Esto incluye la configuración del usuario administrativo ("admin"), la contraseña asociada y el contexto de dominio ("xxxxxxxxx.com").

Cree la instancia de directorio "localhost" utilizando la plantilla editada anteriormente. El comando especificado crea e inicia el servidor de directorio LDAP:

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

Verifique que el servicio LDAP se esté ejecutando en el servidor

```
ss -ntl
```



Ajuste el firewall de CentOS para permitir los puertos necesarios para LDAP (389 o 636).

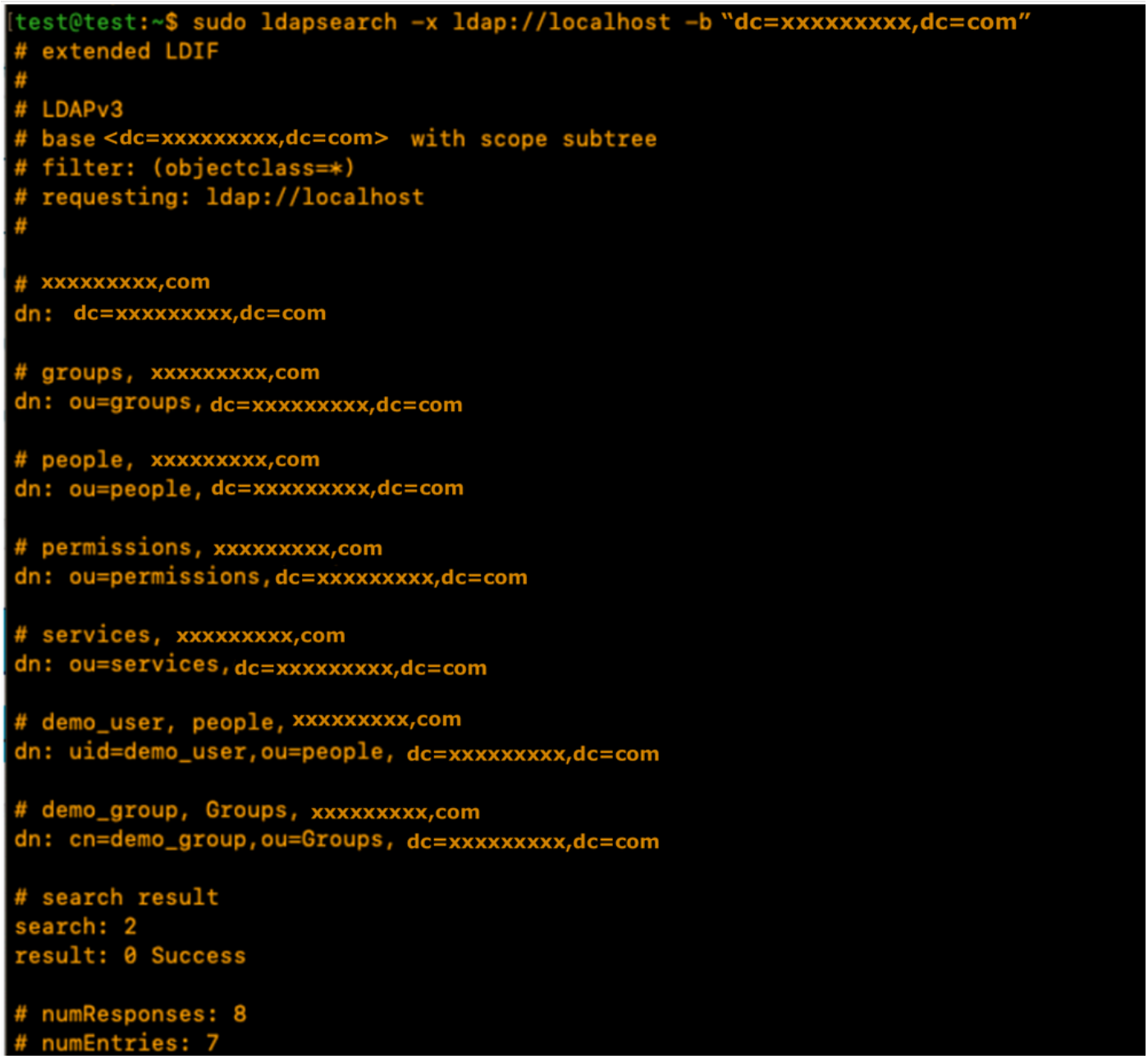
Para esta demostración, el firewall está desactivado.

```
sudo systemctl stop firewalld
```

Verifique que LDAP funcione localmente en el servidor LDAP ejecutando el comando especificado

y asegúrese de que devuelva el resultado LDAP como se muestra:

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



El resultado contiene las cuentas de demostración creadas por el servidor 389DS. El servidor LDAP crea automáticamente las OU predeterminadas.

La unidad organizativa para usuarios y la unidad organizativa para grupos. Se pueden crear unidades organizativas adicionales en función de los requisitos.

Para esta demostración, se utilizan las unidades organizativas creadas automáticamente o por

defecto.

Consulte la documentación oficial del 389DS para obtener detalles sobre el uso extensivo del paquete del 389DS:

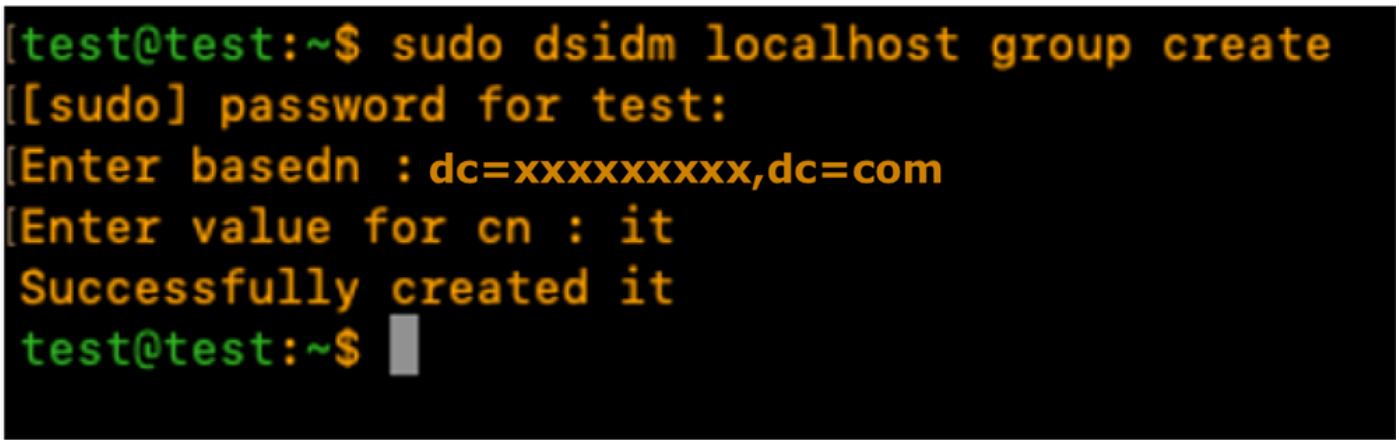
Paso 3: Crear grupos y usuarios LDAP

Cree un grupo (it) utilizando el comando especificado: sudo dsidm <nombre_instancia> group create.

Para esta demostración, el nombre de instancia es "localhost".

```
sudo dsidm localhost group create
```

Ingrese el prompt de terminal para llenar los detalles del grupo como se muestra:



Cree la cuenta de usuario testuser1 mediante el comando:

```
sudo dsidm localhost user create
```

Ingrese el prompt de terminal para llenar los detalles del usuario como se muestra

```
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
```

Cree una contraseña para testuser1 utilizando el comando especificado e ingrese el prompt de 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:~$
```

Agregue el usuario a un grupo mediante el comando especificado: "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
```

Repita los pasos de creación de usuario para crear testuser2 y bind_user.

Nota: asegúrese de que cada usuario se agrega explícitamente a sus grupos deseados.

Si se omite este paso, pueden producirse errores de acceso restringido o de autorización.

No es necesario que la cuenta bind_user sea miembro de un grupo específico, ya que se puede configurar como una cuenta independiente, lo que proporciona flexibilidad para administrar el acceso administrativo y de nivel de servicio dentro del entorno de directorio.

Reinicie la instancia del directorio:

```
sudo dsctl localhost restart
```

Paso 4: Instalar miembro de superposición

Instale el complemento "memberOf" y reinicie la instancia de Directory:

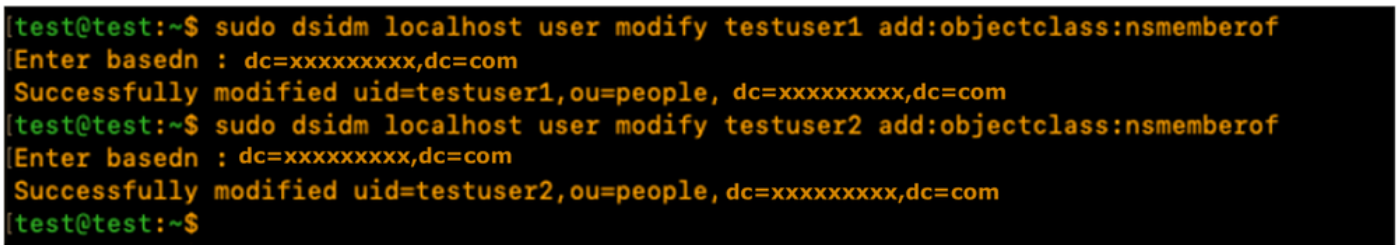
```
sudo dsconf localhost plugin memberof status
sudo dsconf localhost plugin memberof enable
sudo dsctl localhost restart
```

Configure el complemento "memberOf" mediante el comando especificado: "sudo dsconf <directory_instance> plugin member of set —scope <base_dn>"

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

Marcar usuarios como destinos "memberOf" válidos mediante el comando especificado: "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
```



Generar corrección "memberOf" para el DN base: "sudo dsconf <directory_instance> plugin member of 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:~$
```

Verifique la configuración del usuario:

```
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:~$
```

El servidor LDAP 389DS se configura con el complemento memberOf para admitir el atributo memberOf.

Parámetros de configuración en CIMC

Inicie sesión en CIMC.

En el panel de navegación, seleccione Admin, User Management y LDAP.

Rellene los parámetros de configuración de LDAP como se muestra a continuación:

- Habilitar LDAP: activado
- DN base: dc=xxxxxxxxx,dc=com

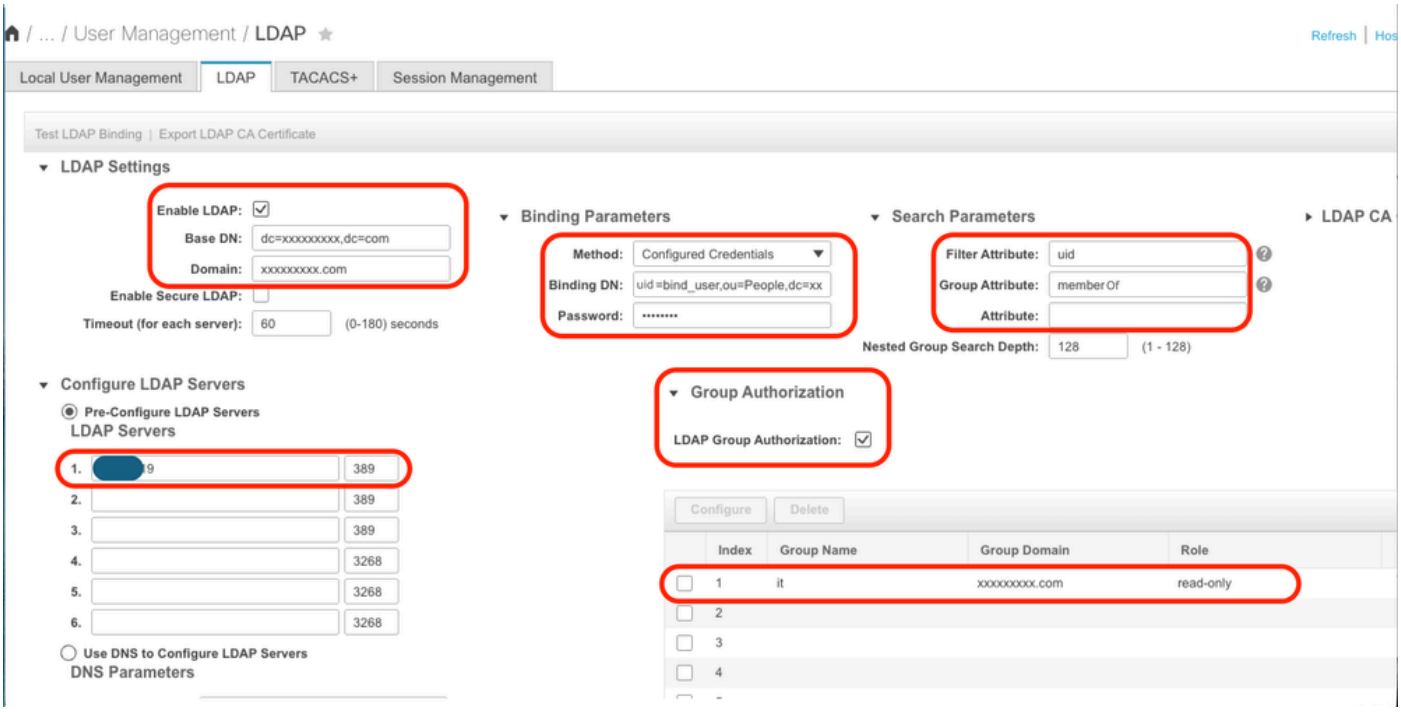
- Dominio: xxxxxxxxx.com

- Servidores LDAP: <ldap_server_IP o FQDN> X.X.X.19

- Parámetros de enlace: Puede ser "Credenciales de inicio de sesión" o "Credenciales configuradas"
    - Cuando utilice las credenciales configuradas, agregue el DN bind_user exactamente como se configuró en el servidor LDAP:
        - Por ejemplo: "cn=bind_user,ou=People,dc=xxxxxxxxx,dc=com" o "uid=bind_user,ou=People,dc=xxxxxxxxx,dc=com"

- Parámetros de búsqueda:
    - Atributo de filtro: "cn" o "uid"
    - Atributo de grupo: memberOf

- Autorización de grupo LDAP: activada
    - Nombre de grupo: it
    - Dominio de grupo: xxxxxxxxx.com
    - Función: sólo lectura (cualquier función preferida)



Guarde la configuración y pruebe el inicio de sesión de usuario LDAP.

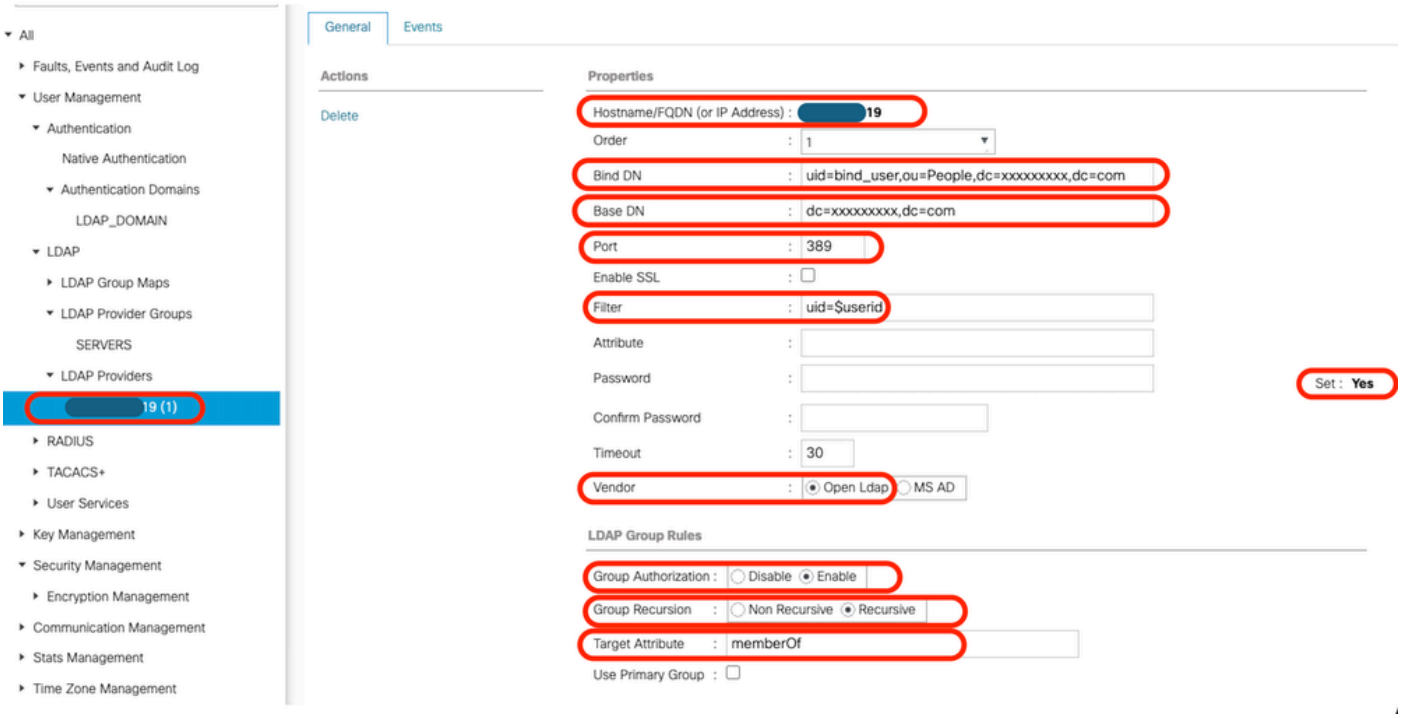
Parámetros de configuración en UCS Manager

Inicie sesión en UCS Manager.

En el panel de navegación, seleccione Admin, User Management y LDAP.

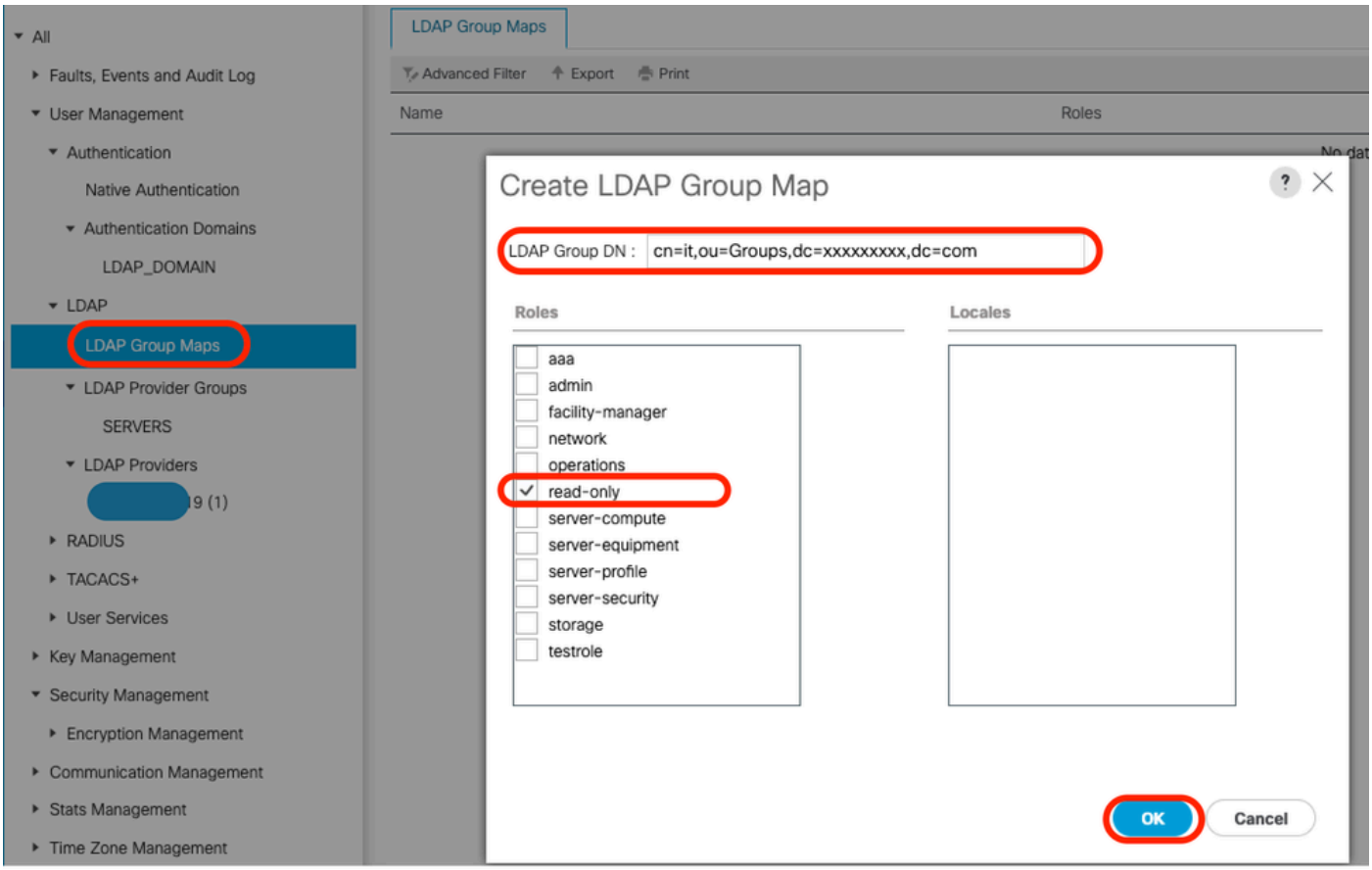
Rellene los parámetros de configuración de LDAP como se muestra a continuación:

- Proveedores LDAP:
  - Nombre de host: <FQDN o dirección IP del servidor LDAP>
  - Enlazar DN: uid=bind_user,ou=people,dc=xxxxxxxxx,dc=com
  - DN base: dc=xxxxxxxxx,dc=com
  - Puerto: 389
  - Habilitar SSL: Inhabilitado
  - Filtro: uid=$userid
  - Autorización de grupo: Habilitado
  - Recursión de grupo: Recursivo
  - Atributo de destino: memberOf
- Mapas de grupo LDAP:
  - DN de grupo LDAP: cn=it,ou=Groups,dc=xxxxxxxxx,dc=com



Agregue el proveedor LDAP configurado a un grupo de proveedores LDAP. Para esta demostración, se utiliza el grupo de proveedores LDAP "SERVERS".

Configure los Mapas de Grupo LDAP agregando un "DN de Grupo LDAP", recuperado del servidor LDAP.



Configure un Dominio de Autenticación LDAP (LDAP_DOMAIN) en "All >> User Management > Authentication >> Authentication Domains" que hace referencia a los Grupos de Proveedores LDAP y pruebe el login de usuario LDAP.

Conclusión

Aunque en esta guía se tratan los escenarios de implementación esenciales, una exploración más detallada de las capacidades de LDAP puede mejorar significativamente el rendimiento y la seguridad del directorio.

Para obtener información adicional, prácticas recomendadas y detalles de configuración avanzada, consulte los recursos especificados:

- Documentación oficial de OpenLDAP
- Administrador de cuentas LDAP: manual
- Documentación de 389 Directory Server
- Configuración de LDAP en UCS Manager
- Configuración de LDAP seguro en servidores UCS serie C

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).