LDAP configureren op UCS Manager - CIMC met Linux OpenLDAP- en 389-DS-servers

Inhoud

Inleiding

In dit document worden verschillende opties beschreven voor het configureren van LDAP als een verificatiemethode voor UCS Manager en CIMC met behulp van op Linux gebaseerde OpenLDAP- en 389-directoryservers.

Achtergrondinformatie

Vanwege de grote variabiliteit van OpenLDAP-serverconfiguraties valt een uitputtende behandeling buiten het bereik van dit document. In dit artikel wordt de nadruk gelegd op algemeen geïmplementeerde configuraties die meerdere Linux-distributies, LDAP-serverpakketten en attribuutschema's omvatten. Ter wille van de duidelijkheid en eenvoud behandelt dit document standaard LDAP-configuraties. Configuratie van Secure LDAP (LDAPS) wordt niet behandeld in dit document.

Voorwaarden:

Kennis van deze onderwerpen wordt sterk aanbevolen:

- UCS B-Series
- UCS C-Series
- Beheer Linux-server

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Firmwareversie van UCS Manager: 4.3(2c)
- Fabric Interconnect-model: UCS-FI-6454
- Standalone servermodel uit de UCS C-reeks: UCSC-C240-M5
- Standalone UCS C-reeks firmware versie: 4.3 (2.250045)
- Ubuntu 10 .04
- CentOS Stream 10

Instellingen gebruikt voor deze demonstratie:

- LDAP Server-hostnaam: test
- Serverdomein: xxxxxxxxx.com
- FQDN-server: test.xxxxxxxxx.com
- IP-adres Linux Server (Ubuntu en CentOS): X.X.X.19

- OpenLDAP-gebruikers: testgebruiker1, testgebruiker2
- OpenLDAP Groep(en): it
- OpenLDAP Bind-gebruikersaccount: bind_user

Opmerking: de Linux Nano teksteditor werd gebruikt in dit lab.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Scenario 1: Ubuntu - Debian

De configuratie van de LDAP-server kan worden uitgevoerd met een grafische interface, zoals LDAP Account Manager, of opdrachtregelprogramma's, afhankelijk van de beheerdersvoorkeur en het vereiste controleniveau. Dit scenario onderzoekt de configuratie met behulp van Linux-gebaseerde OpenLDAP, te beginnen met een GUI-gebaseerde implementatie en vervolgens over te schakelen naar command-line hulpprogramma's om geavanceerde mogelijkheden, waaronder overlay plugins (vaak gebruikt in integraties met Cisco UCS Manager) te verkennen.

Optie 1: OpenLDAP configureren met Ubuntu LDAP Account Manager (LAM)

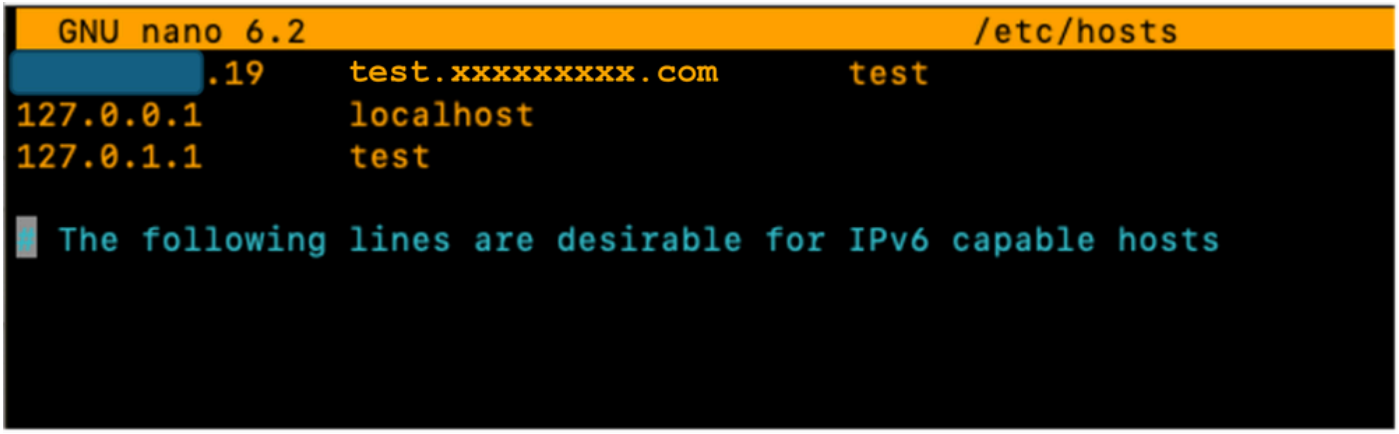
Stap 1: Initiële configuratie van de Linux server hostnaam en net-tools.

Update ubuntu en installeer het net-tools pakket voor toegang tot tools zoals ifconfig, netstat etc:

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

Gebruik de opdracht "ifconfig" om het IP-adres van de server te verifiëren en voeg dit samen met de domeinnaam van de server (bijvoorbeeld: "test.xxxxxxxxx.com" gebruikt in dit lab) en de hostnaam (bijvoorbeeld: "test") in de opgegeven indeling toe aan het bestand "/etc/hosts".

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



Werk daarnaast het bestand "/etc/hostname" bij door de inhoud ervan te vervangen door de hostnaam (test).

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

De server moet opnieuw worden opgestart voordat deze wijzigingen van kracht worden.

```
sudo reboot
```

Stap 2: Installeer SLAPD, Apache, PHP en hun afhankelijkheden

Installeer vervolgens Apache, PHP en hun afhankelijkheden. Deze worden gebruikt om GUI-interactie via een webpagina mogelijk te maken:

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

Open LDAP-serverpakket "slapd" en de afhankelijkheden ervan installeren (ldap-utils)

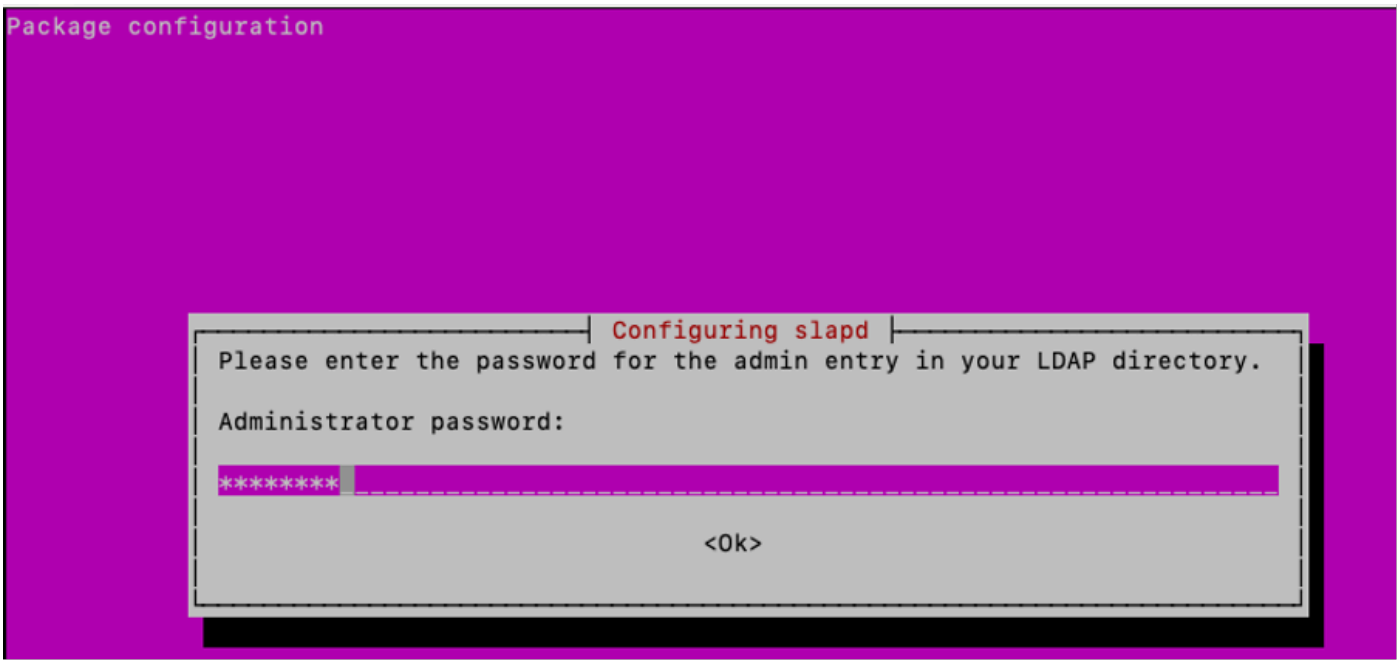
```
sudo apt install slapd ldap-utils -y
```

Tijdens de installatie van de SLAPD voert u in het pop-upvenster van de GUI de extra vereiste configuratie van het SLAPD-pakket in.

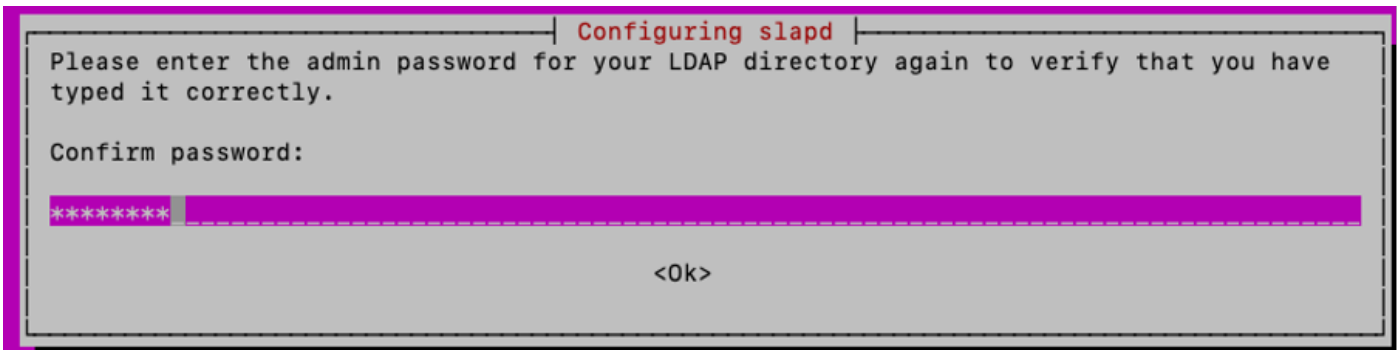
Opmerking: voor het verliezen van het wachtwoord moet de LDAP-server opnieuw worden geïnstalleerd.

De "beheerder" (admin) in deze context is een account dat wordt gebruikt om de OpenLDAP-service, -modules en -configuraties te beheren.

Voeg het LDAP pakket "administrator" wachtwoord toe en druk op enter op het toetsenbord om "OK" te selecteren.



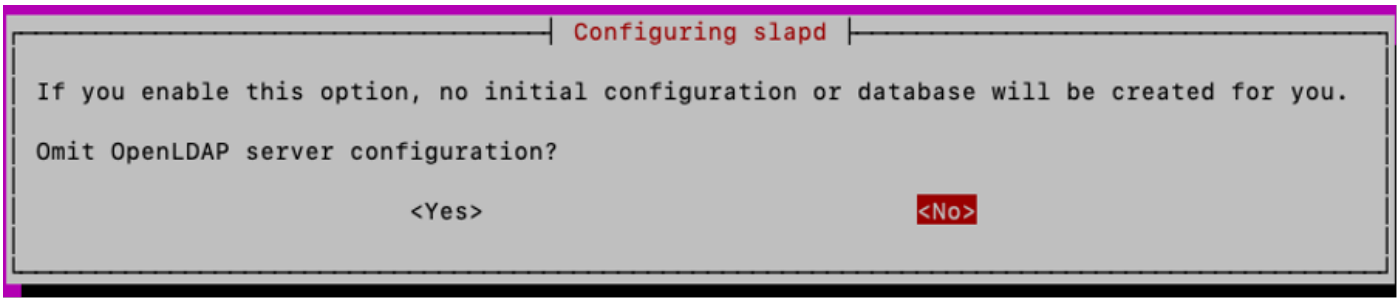
Het wachtwoord bevestigen:



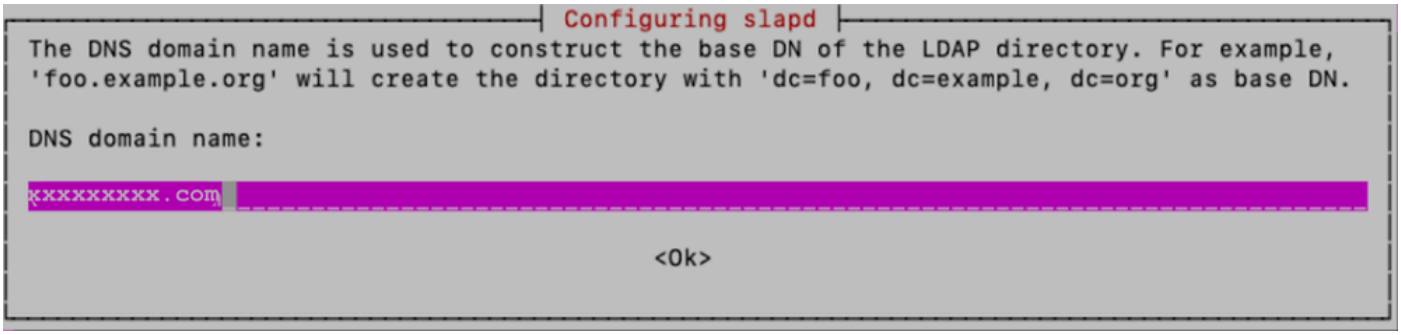
Nadat de installatie is voltooid, kunt u de opgegeven opdracht gebruiken om het SLAPD-pakket opnieuw te configureren en domeininformatie toevoegen:

```
sudo dpkg-reconfigure slapd
```

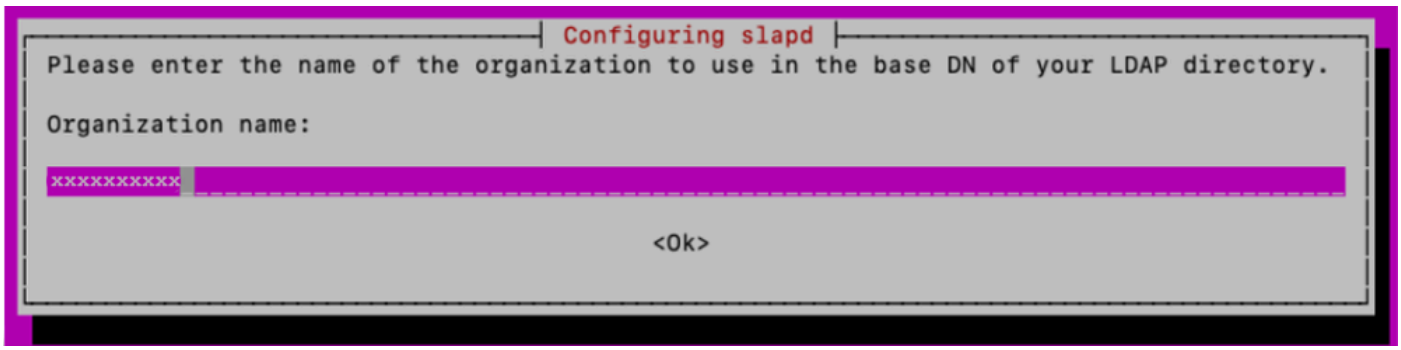
U kunt de standaardoptie "Nee" voor de "OpenLDAP-serverconfiguratie weglaten" accepteren en op enter drukken:



Typ de domeinnaam en druk op enter:



Voor dit lab wordt "xxxxxxxxx" gebruikt als "Organisatienaam":

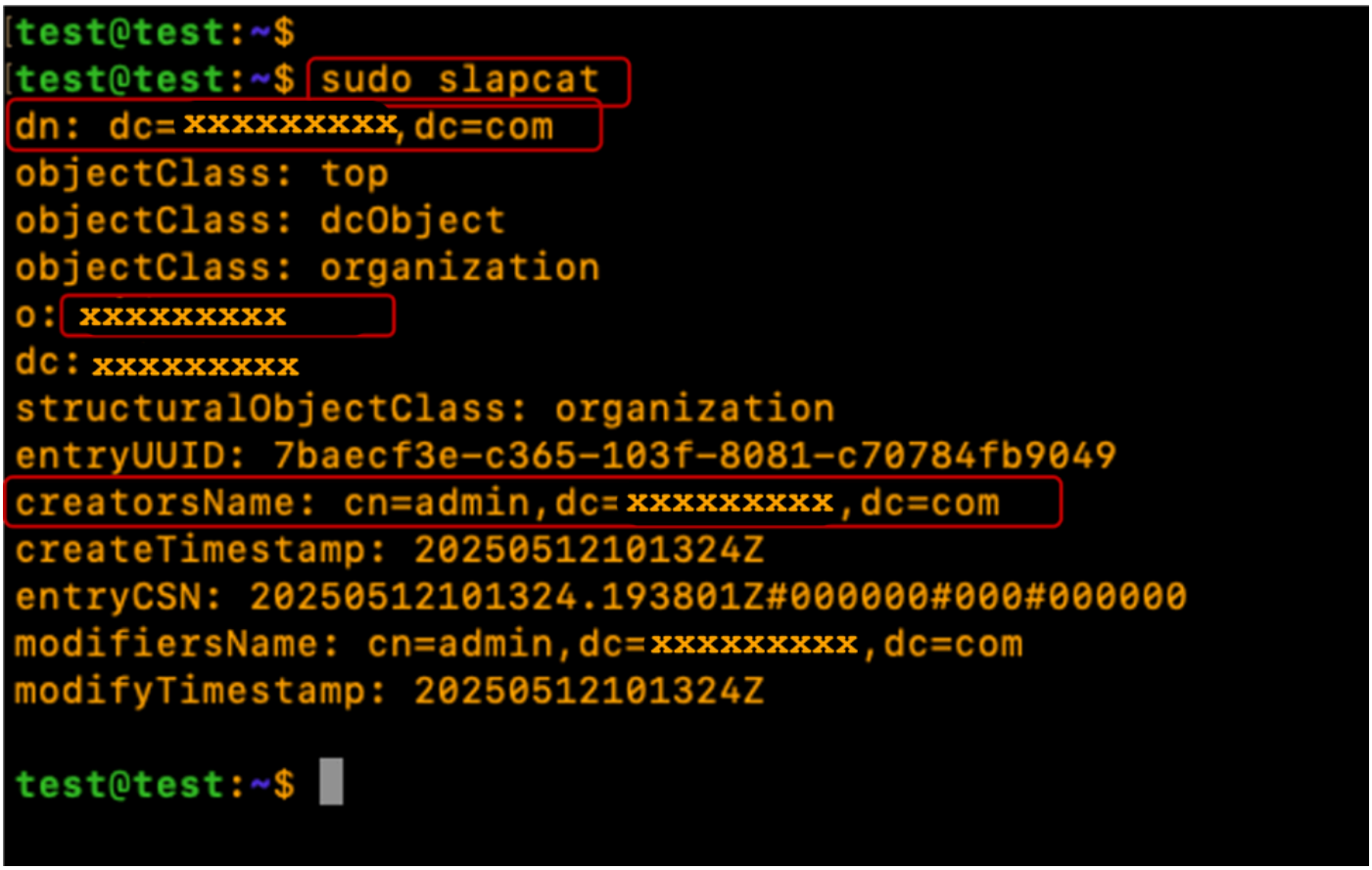


Typ vervolgens het "Beheerderswachtwoord" en bevestig het

Voor de andere configuratieopties houdt u de standaardinstellingen en drukt u op Enter op het toetsenbord om de configuratie te voltooien.

De installatie van de SLAPD controleren met de opdracht:

```
sudo slapcat
```



Stap 3: Installeer LDAP Account Manager

LDAP Account Manager (LAM) installeren voor het maken en beheren van LDAP-gebruikers en -groepen:

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

PHP-CGI PHP extensie inschakelen, vereist door LAM.

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

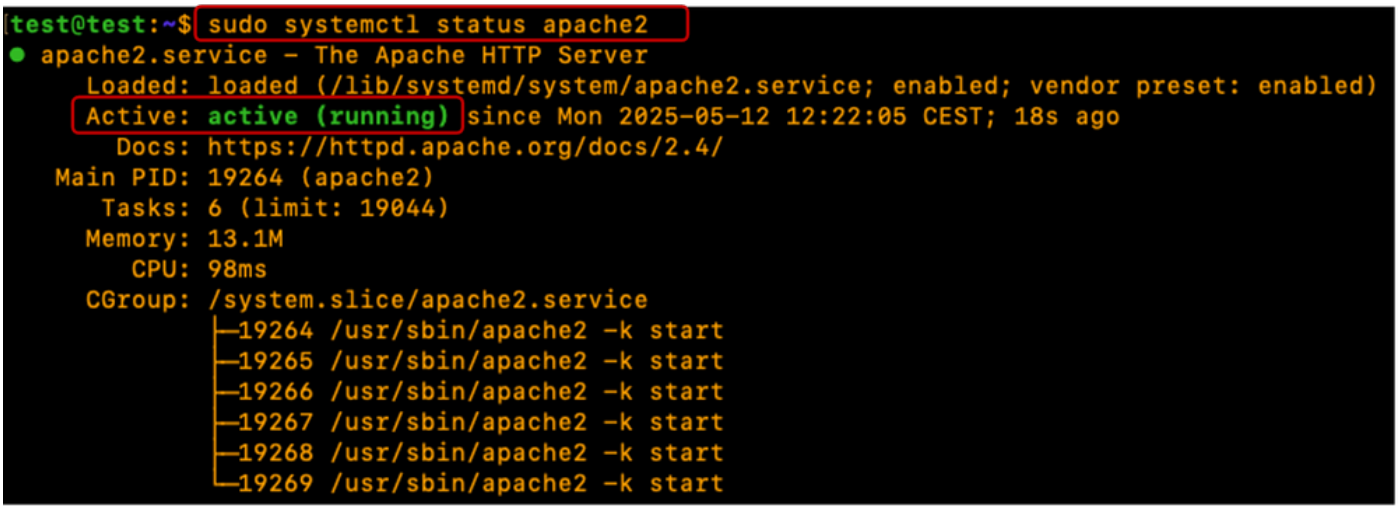
Apache opnieuw laden om de nieuwe configuratie te activeren.

Opnieuw opstarten en Apache-service inschakelen om automatisch op te starten bij opstarten:

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

Controleer of de status van Apache Server "Running" en "Active" is

```
sudo systemctl status apache2
```

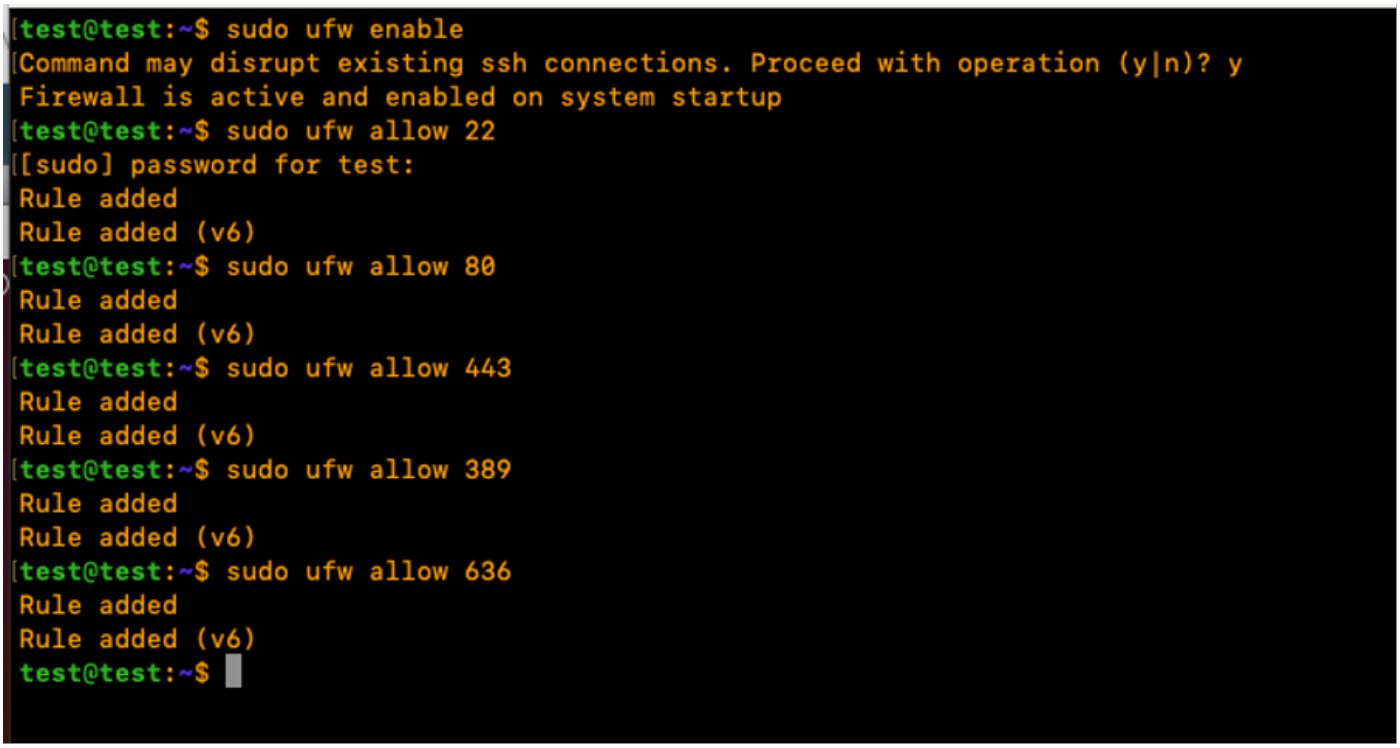


Configureer Ubuntu Firewall zodat poort 80(Web), 443 (beveiligd Web), 389(LDAP) en 636 (beveiligd LDAP indien nodig) mogelijk zijn

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

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

```
sudo ufw allow 636
```



Controleer de status van de Ubuntu Firewall:

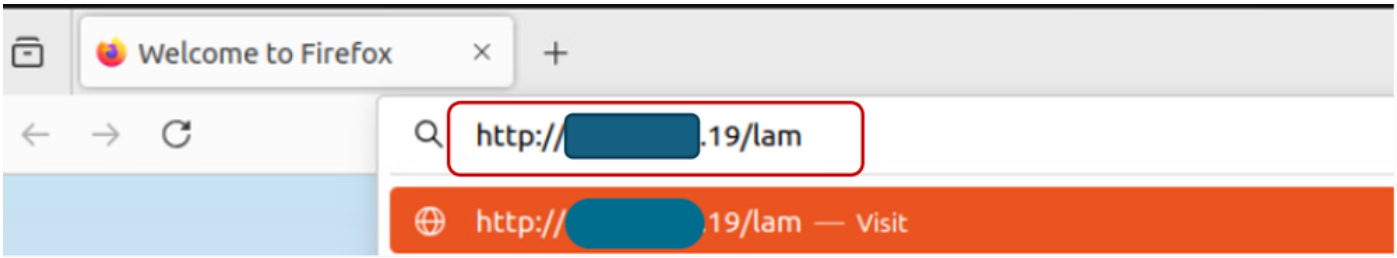
```
sudo ufw status
```

```
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)
```

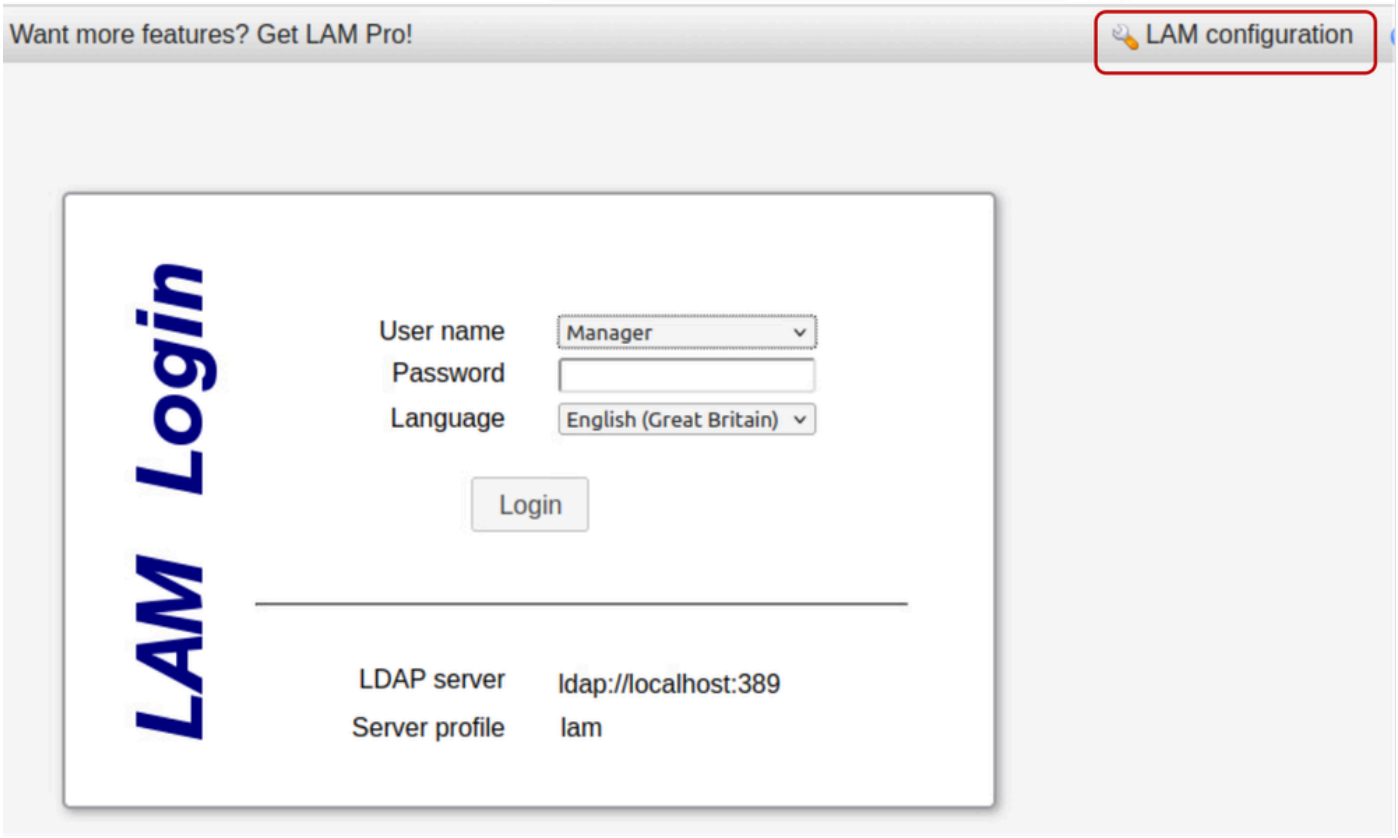
Stap 4: LDAP-accountbeheer configureren

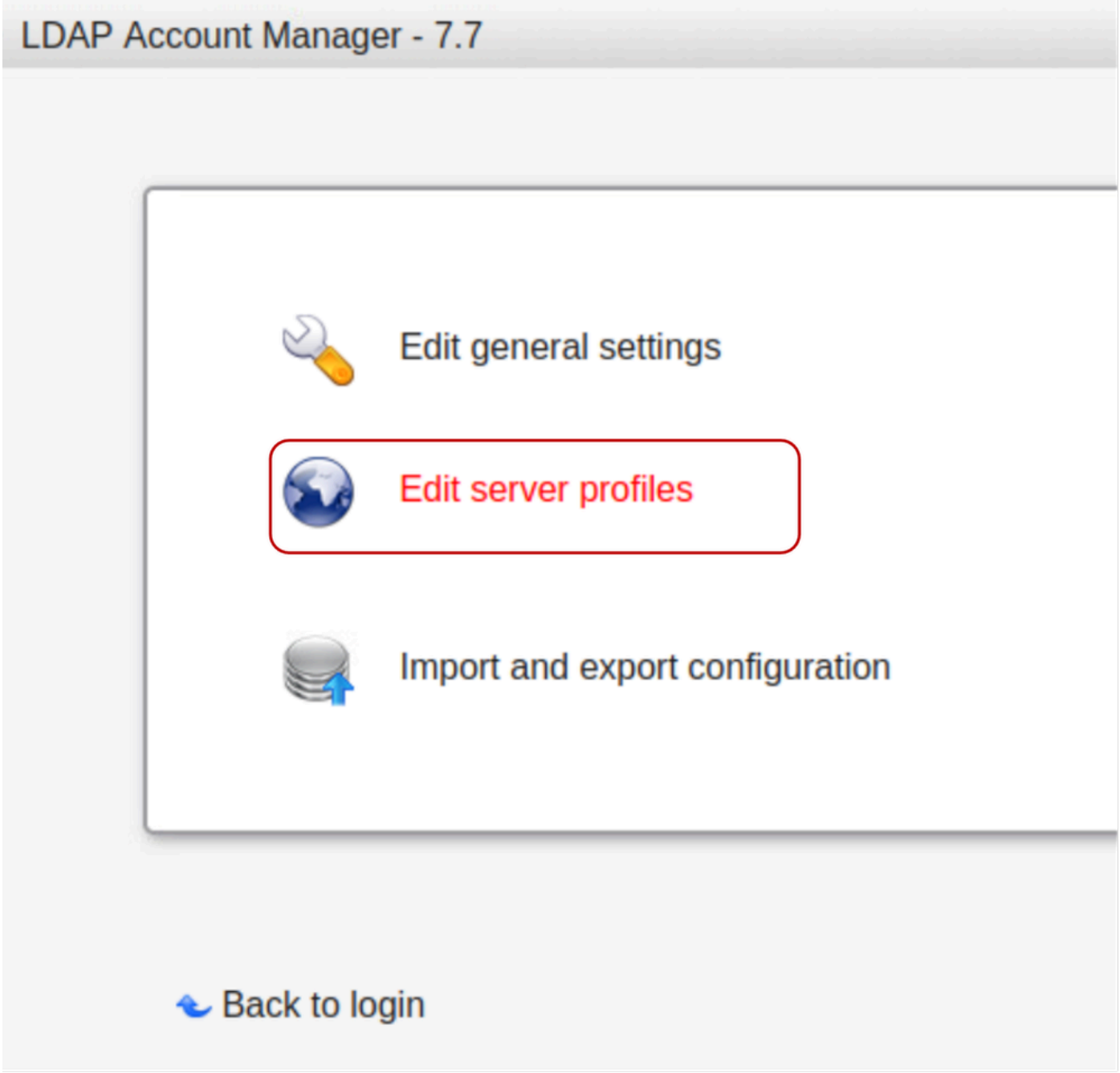
Als u LDAP Account Manager (LAM) vanuit de GUI wilt configureren, opent u een webbrowser, voert u het IP-adres van de Linux-server in en voegt u het 'lam'-pad toe zoals wordt weergegeven:

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

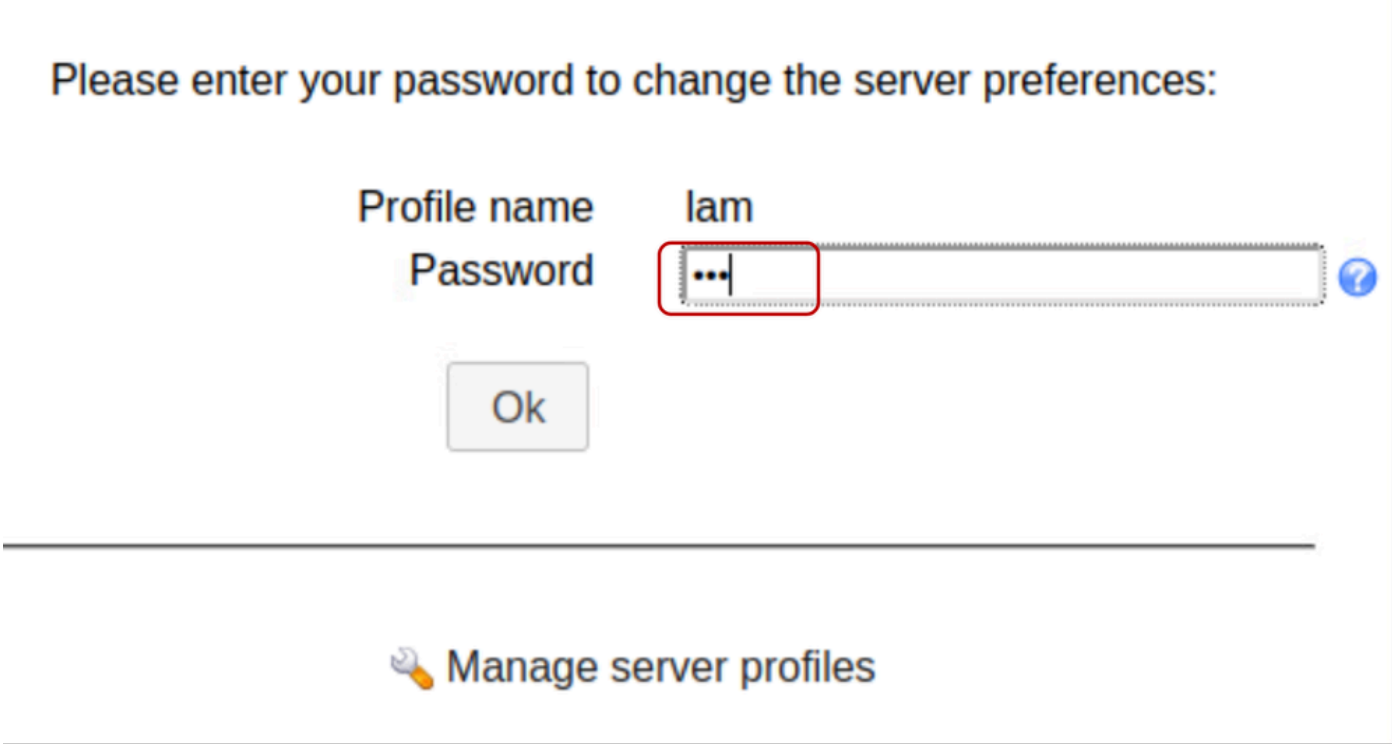


Klik op "LAM-configuratie" en selecteer "Serverprofielen bewerken".


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



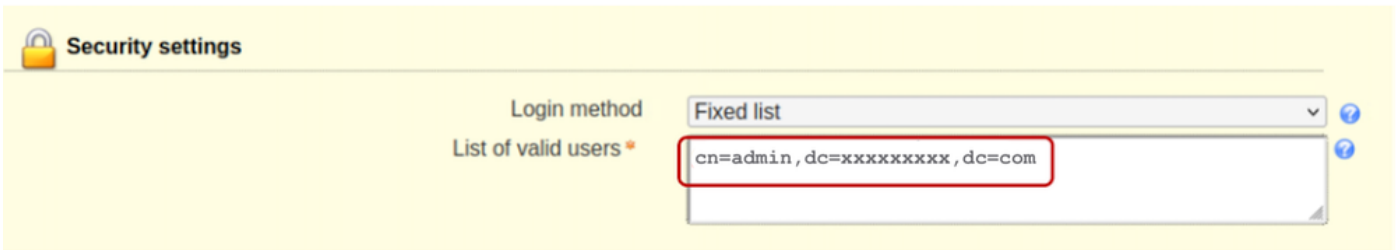
Typ het standaard lam wachtwoord "lam" om in te loggen.



Controleer op het tabblad Algemene instellingen de serverinstellingen, "Taal" en "Tijdzone".

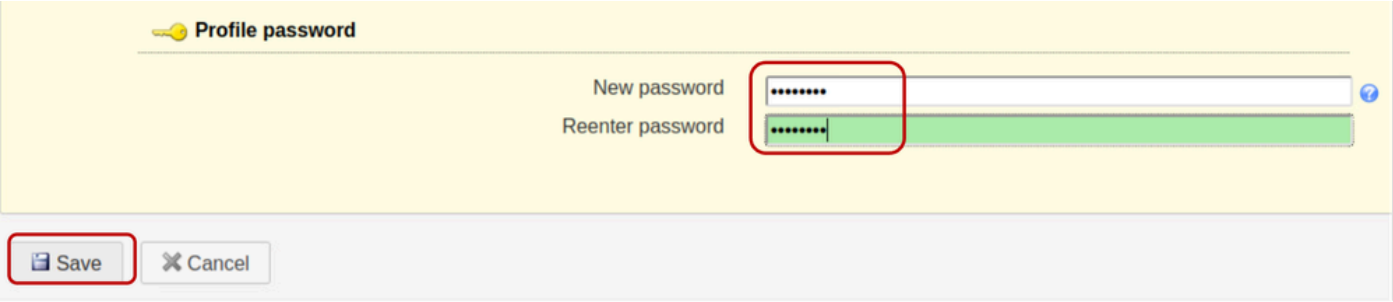
Bewerk en voeg de vereiste domeinnaam toe in het veld Structuurachtervoegsel in het gedeelte Gereedschapsinstellingen, zoals hieronder wordt weergegeven:

Bewerk de sectie Beveiligingsinstellingen om een "admin" -gebruiker op te nemen die wordt gebruikt om de SLAPD-service te beheren.



Stel een "Profielwachtwoord" in. Dit wachtwoord wordt gebruikt voor latere aanmeldingen bij de LAM-configuratie-interface, in dit voorbeeld is "cisco123" geconfigureerd in plaats van het standaard "lam"-wachtwoord.

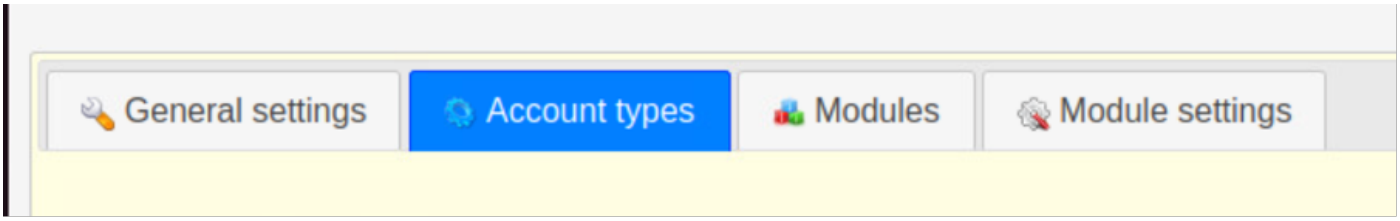
Sla de configuratie op:



De sessie wordt vervolgens opnieuw gestart via de interface van de LAM-configuratie-GUI.

Meld u opnieuw aan (LAM-configuratie >> Serverprofielen bewerken) met het nieuwe wachtwoord dat u hebt gemaakt.

Klik op de "Accounttypes",



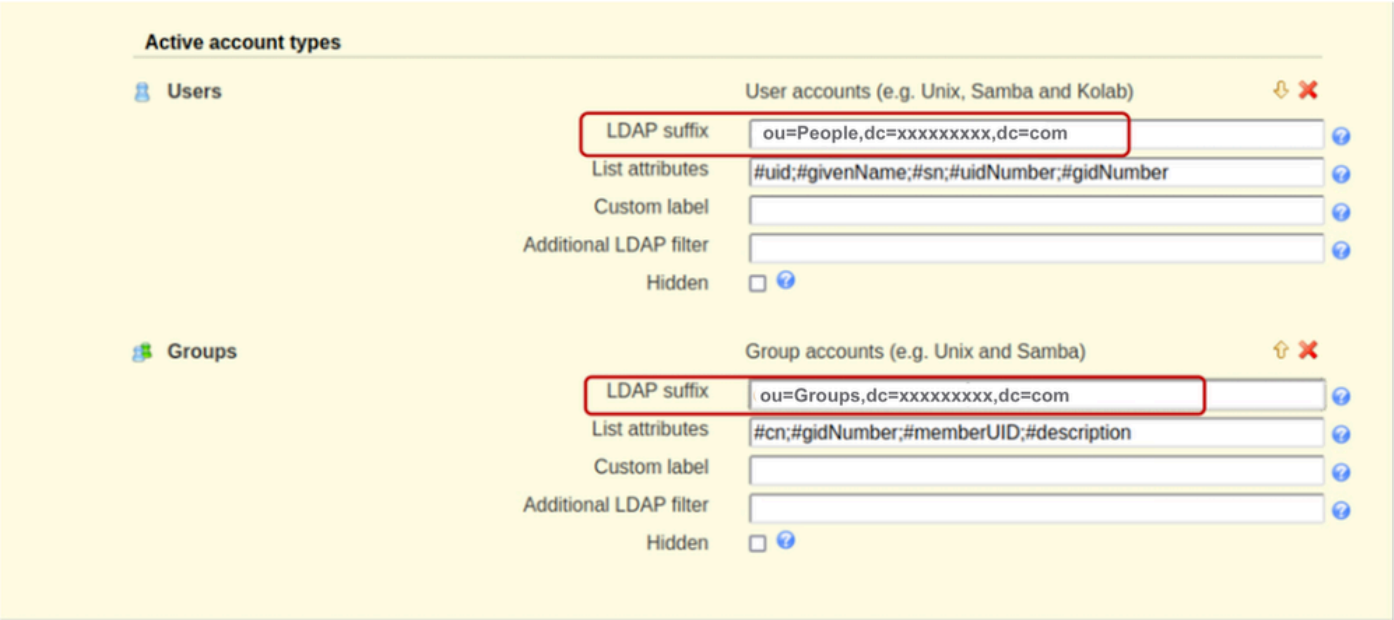
Blader omlaag en bewerk de standaard Active-accounttypen met de domeinnaaminformatie in het veld LDAP-achtervoegsel. De standaardinhoud van het veld "LDAP suffix" geeft bijvoorbeeld de waarde "ou=People, dc=my-domain, dc=com" weer.

In het geval dat er nieuwe Organisatorische Eenheden moeten worden gemaakt, vervangt u de inhoud van het veld "LDAP suffix" om de naam van de Organisatorische Eenheid te bevatten.

Het formaat wordt weergegeven als "ou=<organization_unit>, dc=xxxxxxxx, dc=com".

Voor deze demonstratie is de OU voor gebruikers "Mensen" en de OU voor groepen "Groepen".

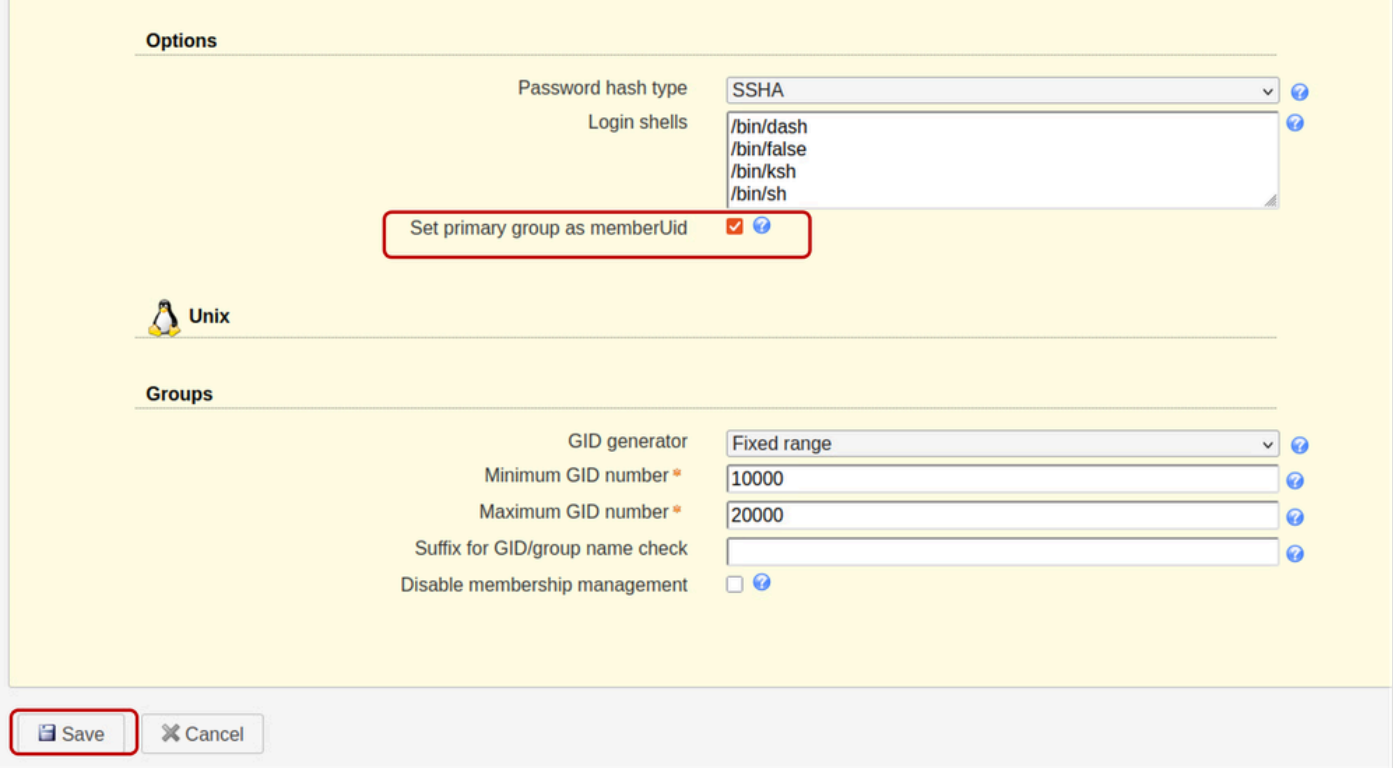
Sla de configuratie op.



Blader omlaag naar het gedeelte Opties en zorg ervoor dat u de optie "Primaire groep instellen als memberUid" selecteert.

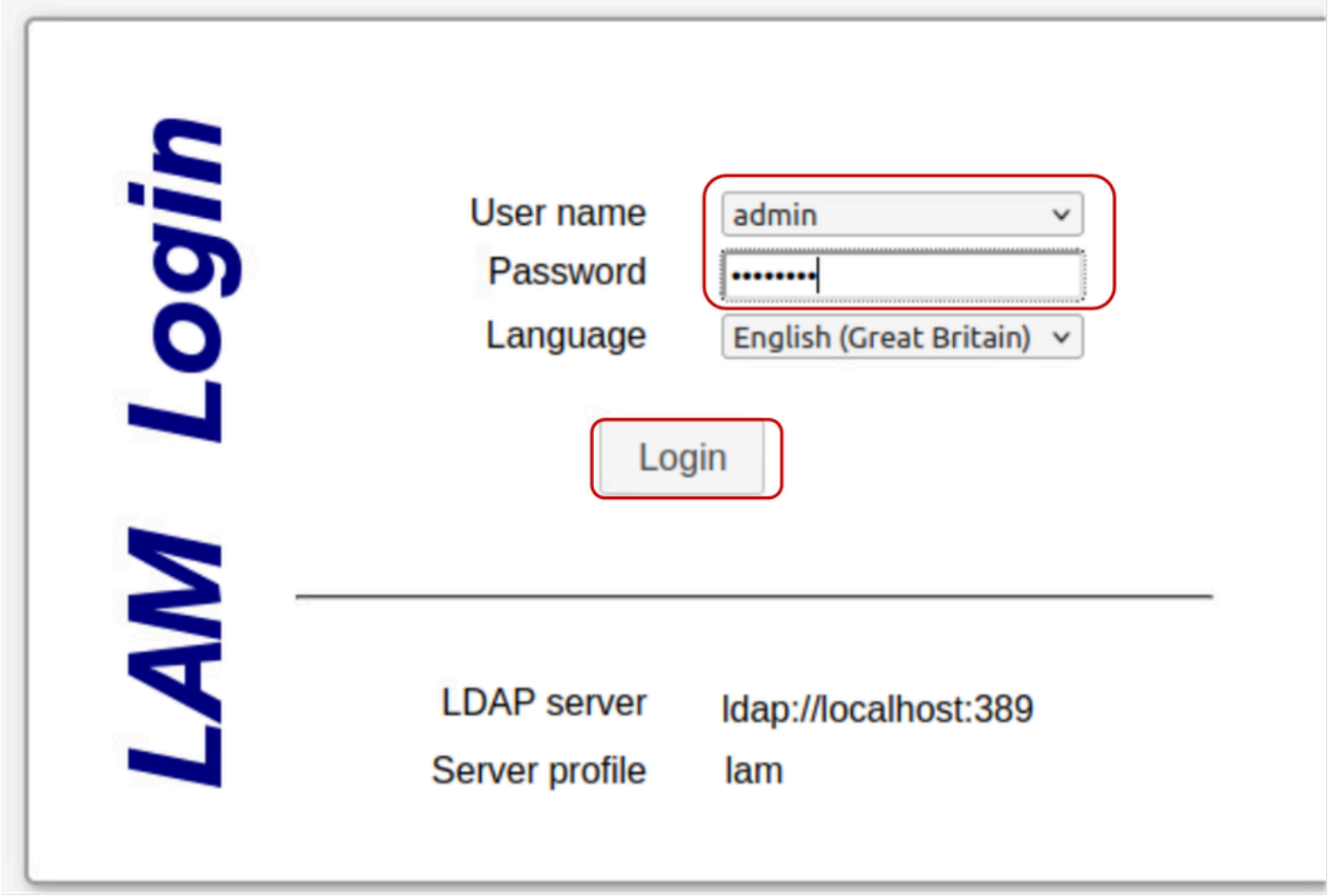
De optie "Primaire groep instellen als memberUid" is standaard niet ingesteld op groepsobjecten. Als u dit activeert, kunt u OpenLDAP "Primaire groep" gebruiken, zoals een standaard LDAP-groep, waar naar de "memberUid" kan worden verwezen (bijvoorbeeld: in de serverconfiguratie van de UCS C-reeks). Als deze optie niet is ingeschakeld, mislukt de aanmelding voor gebruikers die tot een primaire groep behoren.

Sla de configuratie op.

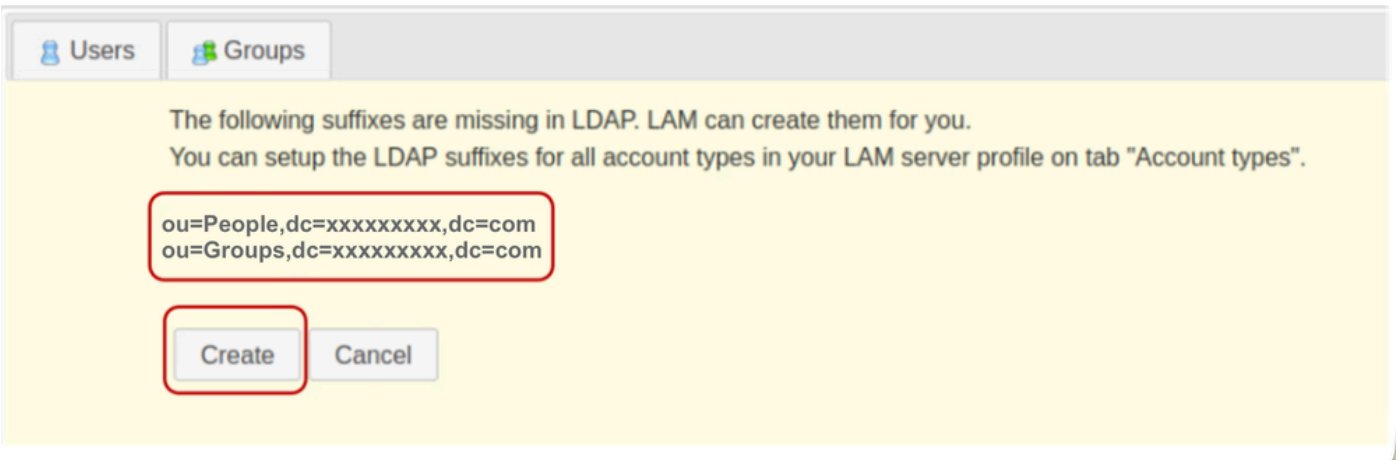


Stap 5: OU's, groepen en gebruikers maken

Meld u aan bij LAM als de "admin" -gebruiker met hetzelfde wachtwoord dat tijdens de installatie is gemaakt, om gebruikers en groepen te maken die behoren tot de eerder gemaakte OU's (mensen en groepen) respectievelijk:

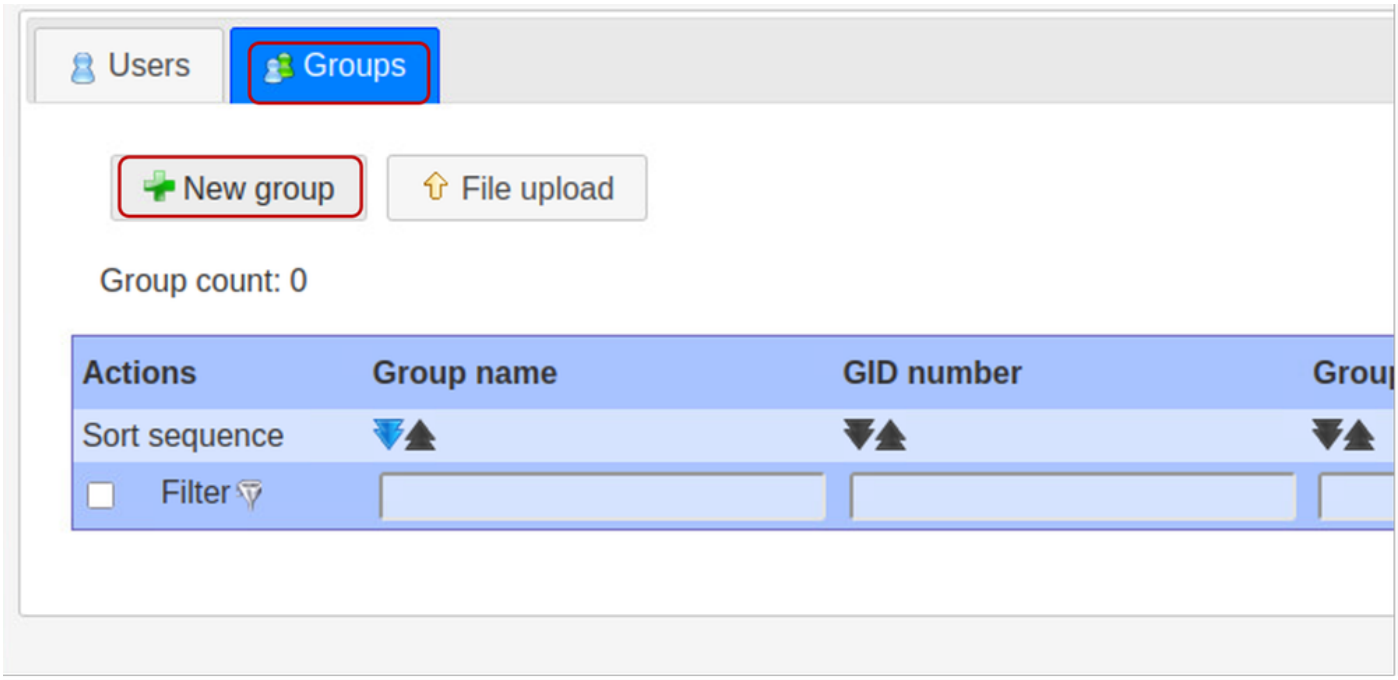


Maak de eerder opgegeven OU's aan in de sectie LAM-configuratie.
Klik op Aanmaken.



Maak vervolgens in LDAP Account Manager de "it" -groep aan:

Selecteer het tabblad Groepen en klik op Nieuwe groep

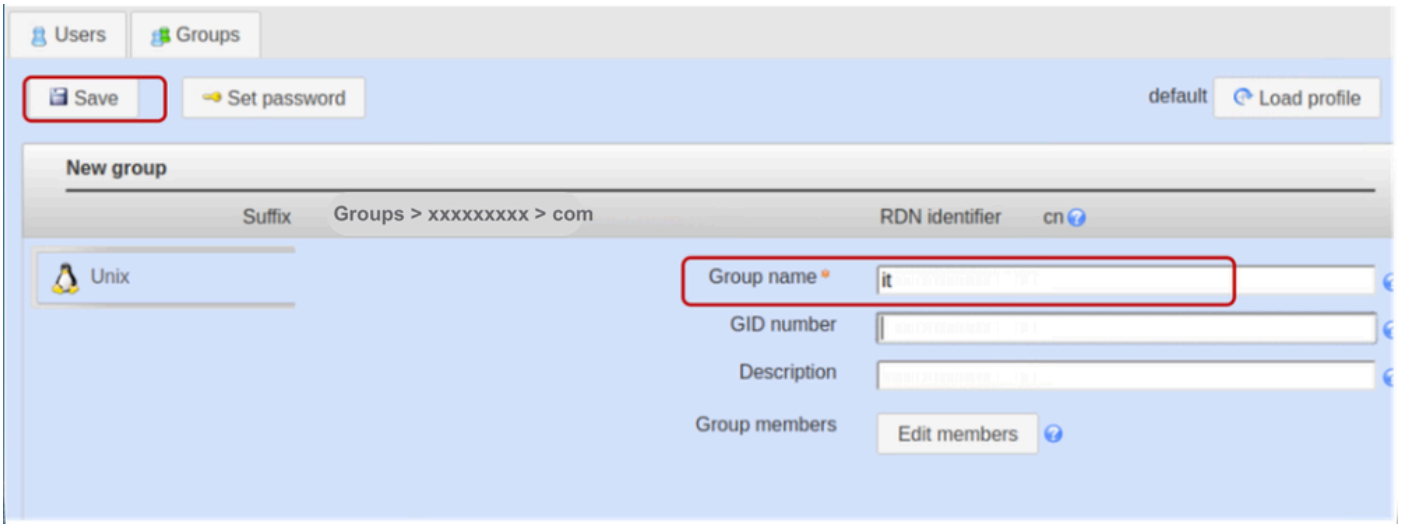


Stel de naam van de groep in als "it".

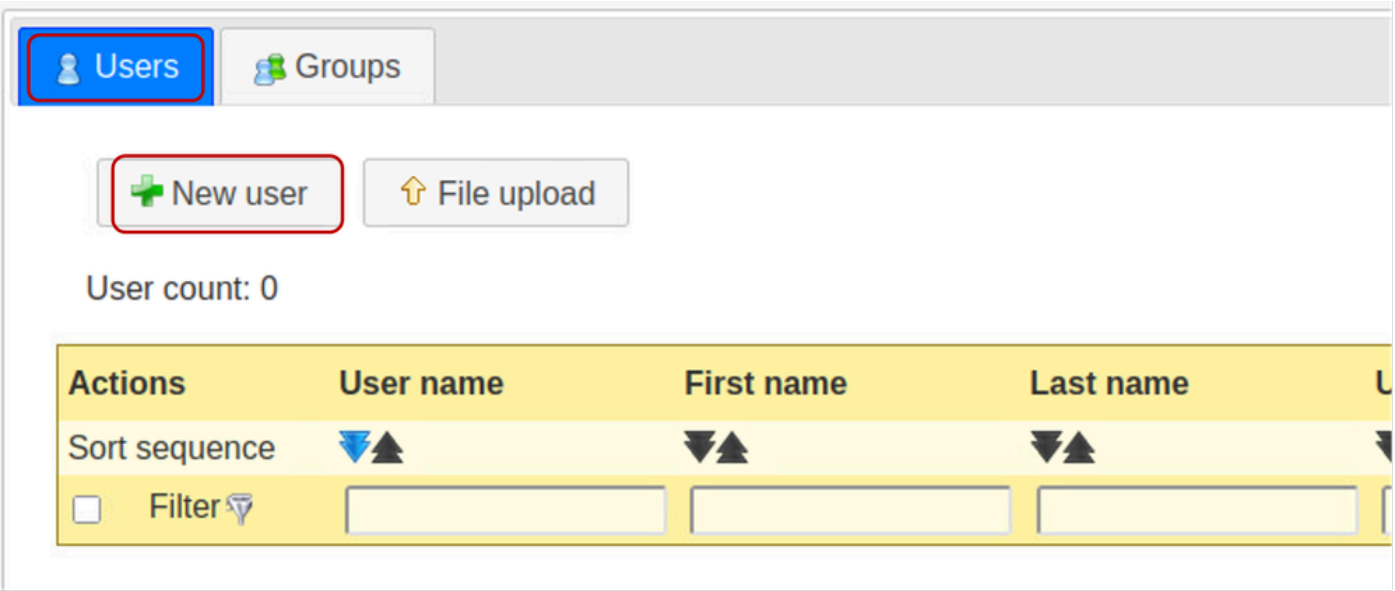
Opmerking: Hoewel Cisco UCS-systemen over het algemeen bestand zijn tegen variaties in casussen, is het handhaven van naamgevingsconventies in kleine letters een beste praktijk om interoperabiliteit op lange termijn te garanderen in verschillende LDAP-serverinfrastructuuromgevingen.

Laat het veld GID-nummer leeg. LDAP Account Manager (LAM) is ontworpen om dit veld automatisch te vullen met de volgende beschikbare waarde.

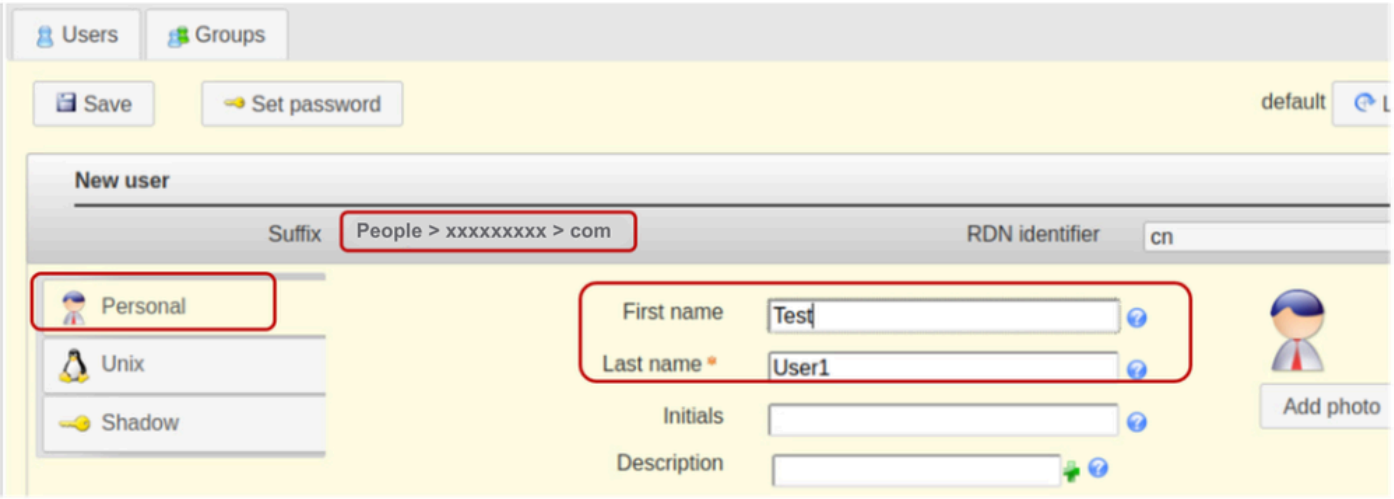
Geef desgewenst een beschrijving op en klik op Opslaan



Klik op het tabblad "Gebruikers" om gebruikersaccounts aan te maken en selecteer "Nieuwe gebruiker".



Vul de vereiste velden voor "testuser1" gebruiker in het tabblad Persoonlijk.

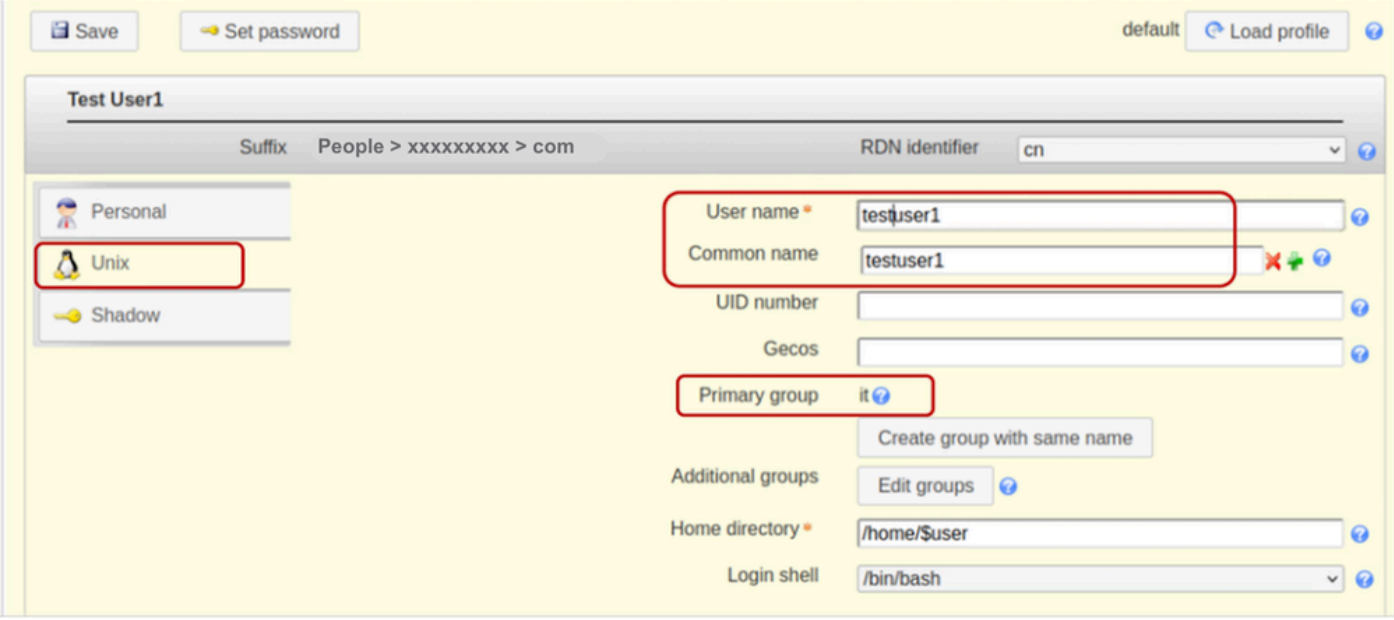


Selecteer het tabblad Unix en voeg testuser1 toe in het veld Gebruikersnaam. Voeg de gebruiker toe aan de groep "IT".

Voor deze demonstratie bestaat alleen de "it" -groep, dus deze is al voorbevolkt.

Handhaaf de RDN-id als de "Common Name" (cn). Hierdoor kan het systeem automatisch het veld "Algemene naam" invullen met de waarde die is opgegeven in het veld "Gebruikersnaam".

Laat het veld UID-nummer leeg omdat LAM het veld automatisch vult met beschikbare waarden.



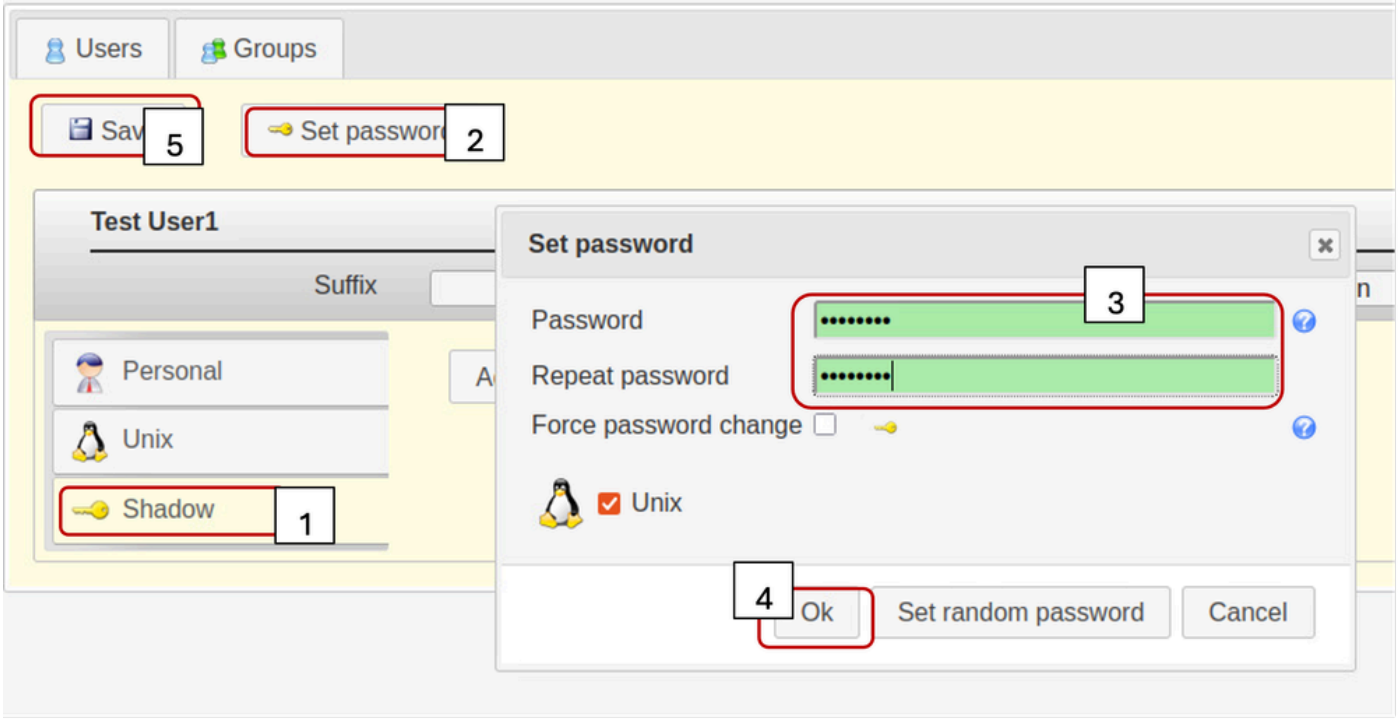
Selecteer het tabblad Schaduw,

De extensie van het schaduwaccount wordt niet gebruikt.

Klik op "Wachtwoord instellen".

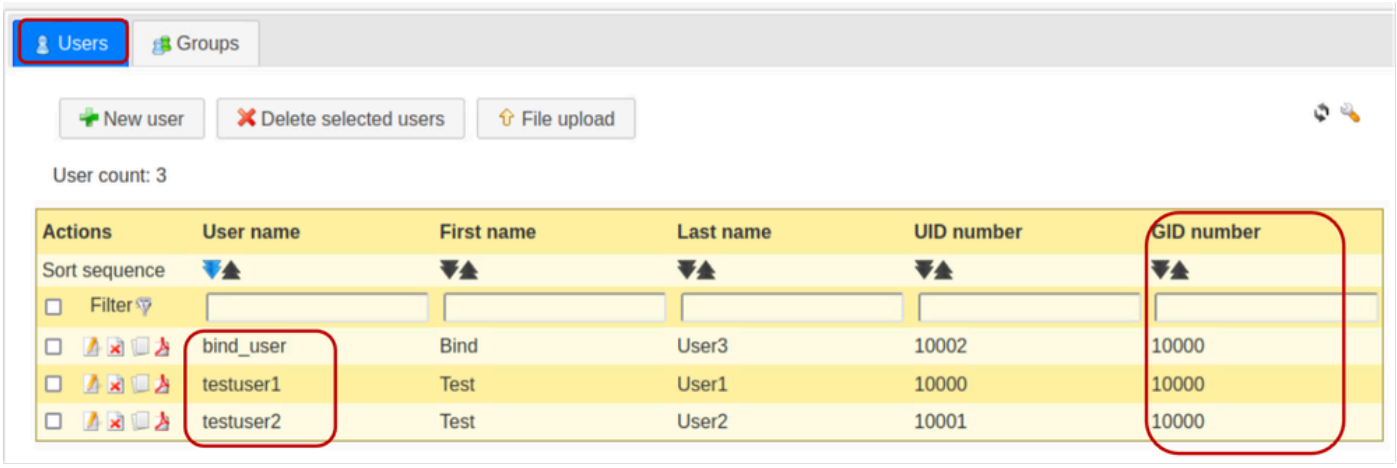
Stel het gebruikerswachtwoord in

Klik op OK en sla op



Herhaal de eerder beschreven stappen om een "testuser2" gebruikersaccount en de "bind_user" account aan te maken.

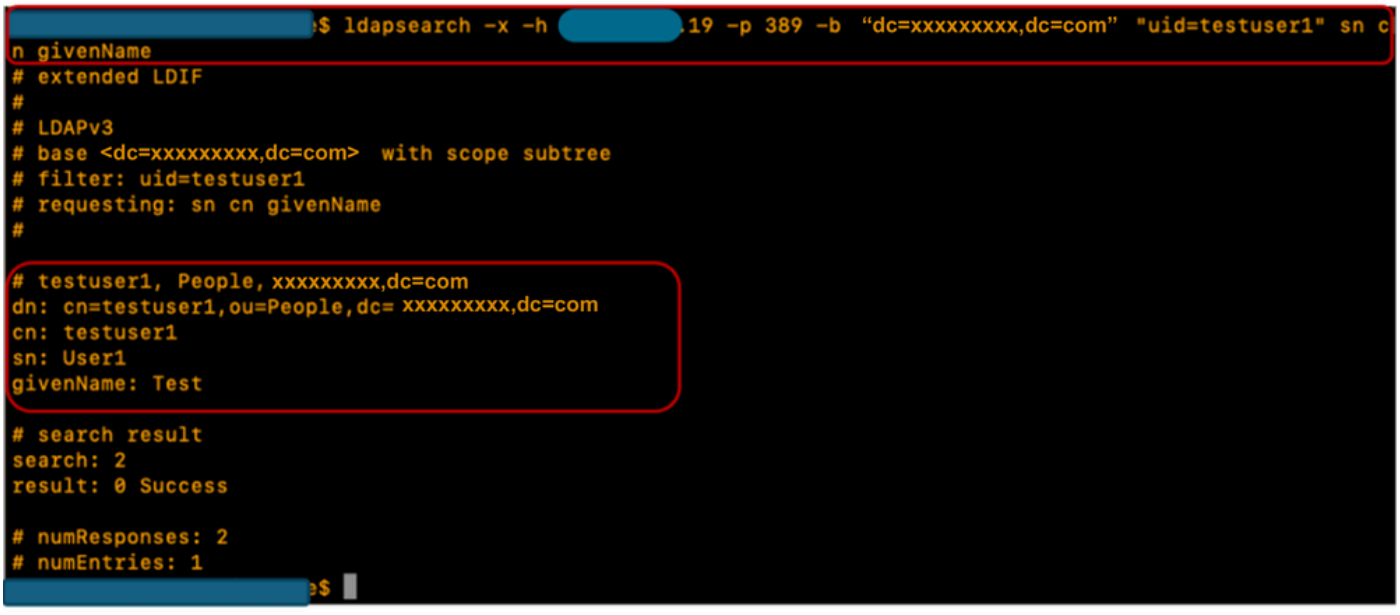
Klik op het tabblad "Gebruikers" om de creatie van alle gewenste gebruikers te verifiëren. (Als u dezelfde waarde hebt in de kolom gidNumber, wordt bevestigd dat de gemaakte gebruikers tot dezelfde groep behoren - het)



Stap 6: Lokale LDAP-aanmelding testen

Meld u aan bij een ander Linux-gebaseerd systeem dat toegankelijk is voor de OpenLDAP-server. Voer de opgegeven ldapsearch-opdracht uit om te controleren of LDAP werkt:

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



Configuratieparameters op CIMC

Log in bij CIMC.

Selecteer in het navigatiedeelvenster Beheer, Gebruikersbeheer en LDAP.

Vul de LDAP-configuratieparameters in zoals hieronder wordt weergegeven:

- LDAP inschakelen: ingeschakeld
- Basis-DN: dc=xxxxxxxx, dc=com

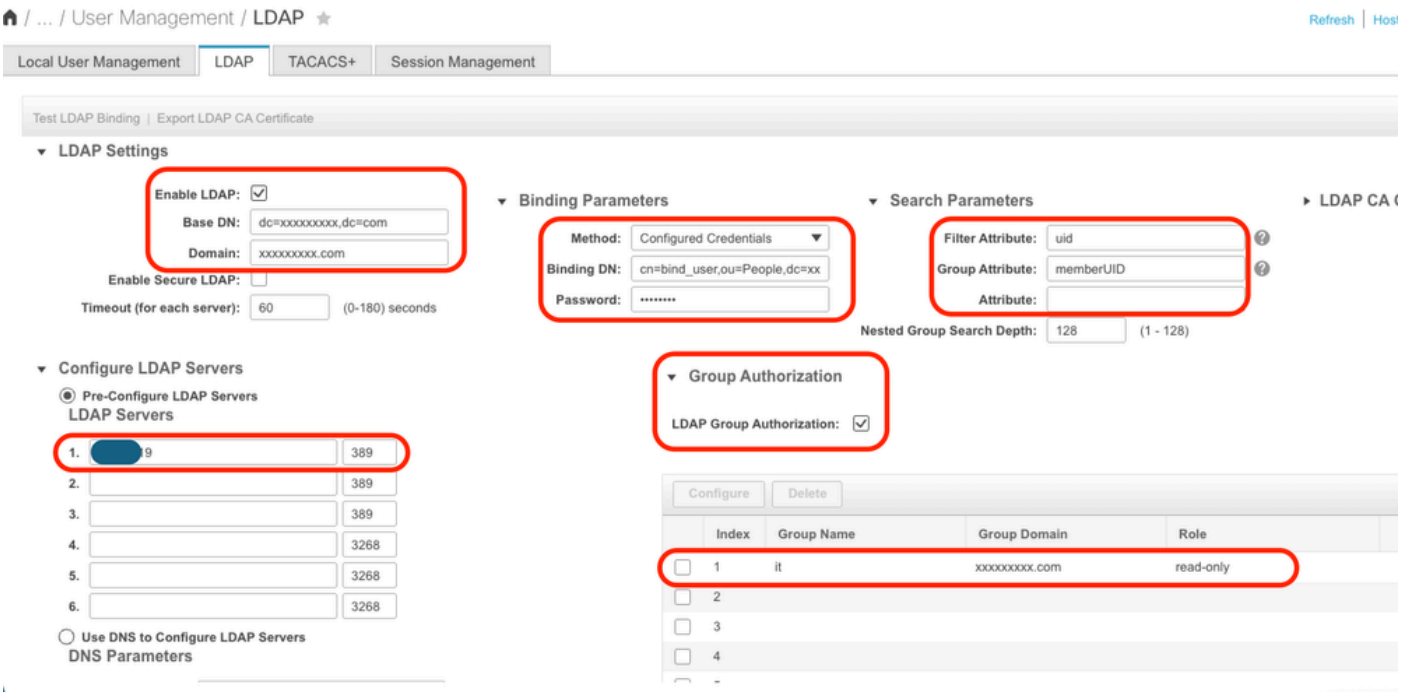
- Domein: xxxxxxxxx.com

- LDAP-server: <ldap_server_IP of FQDN> X.X.X.19

- Bindende parameters: "Inloggegevens" of "Geconfigureerde referenties"
    - Voeg bij het gebruik van geconfigureerde referenties de bind_user-DN precies toe zoals geconfigureerd op de LDAP-server:
        - Bijvoorbeeld: cn=bind_user, ou=People, dc=xxxxxxxxx, dc=com

- Zoekparameters:
    - Filterkenmerk: "cn" of "uid"
    - Groepsattribuut: memberUID

- LDAP-groepsautorisatie - gecontroleerd
    - Groepsnaam: it
    - Groepsdomein: xxxxxxxxx.com
    - Rol: alleen-lezen (elke gewenste rol)



Sla de configuratie op en test de aanmeldingsgegevens van de LDAP-gebruiker.

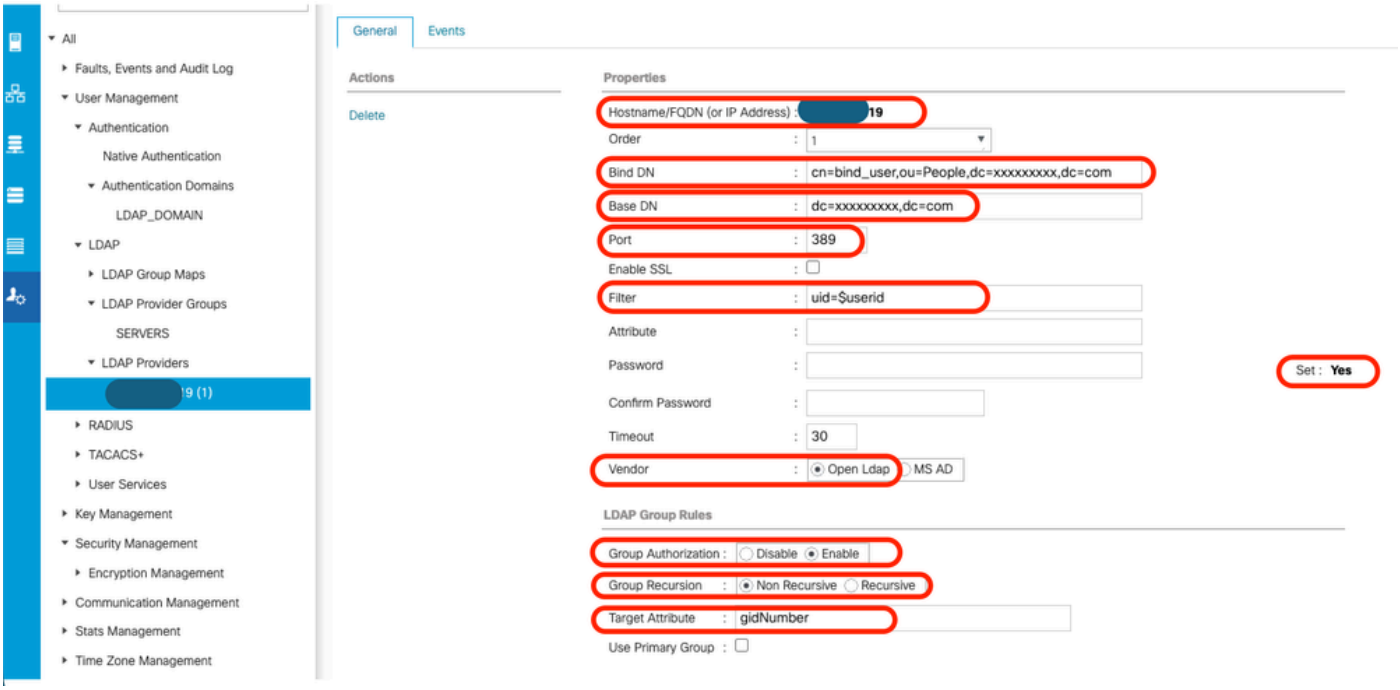
Configuratieparameters in UCS Manager

Meld u aan bij UCS Manager.

Selecteer in het navigatiedeelvenster Beheer, Gebruikersbeheer en LDAP.

Vul de LDAP-configuratieparameters in zoals hieronder wordt weergegeven:

- LDAP-providers:
  - Hostnaam: <FQDN of IP-adres van LDAP-server>
  - Bind DN: cn=bind_user, ou=People, dc=xxxxxxxx, dc=com
  - Basis-DN: dc=xxxxxxxx, dc=com
  - Poort: 389
  - SSL inschakelen: uitgeschakeld
  - Filter: uid=$userid
  - groepsautorisatie: ingeschakeld
  - Groepscorrectie: niet-recursief
  - Doelkenmerk: gidNumber
- LDAP Group Maps:
  - LDAP Group DN: 10000 <gidNumber for "it" group>

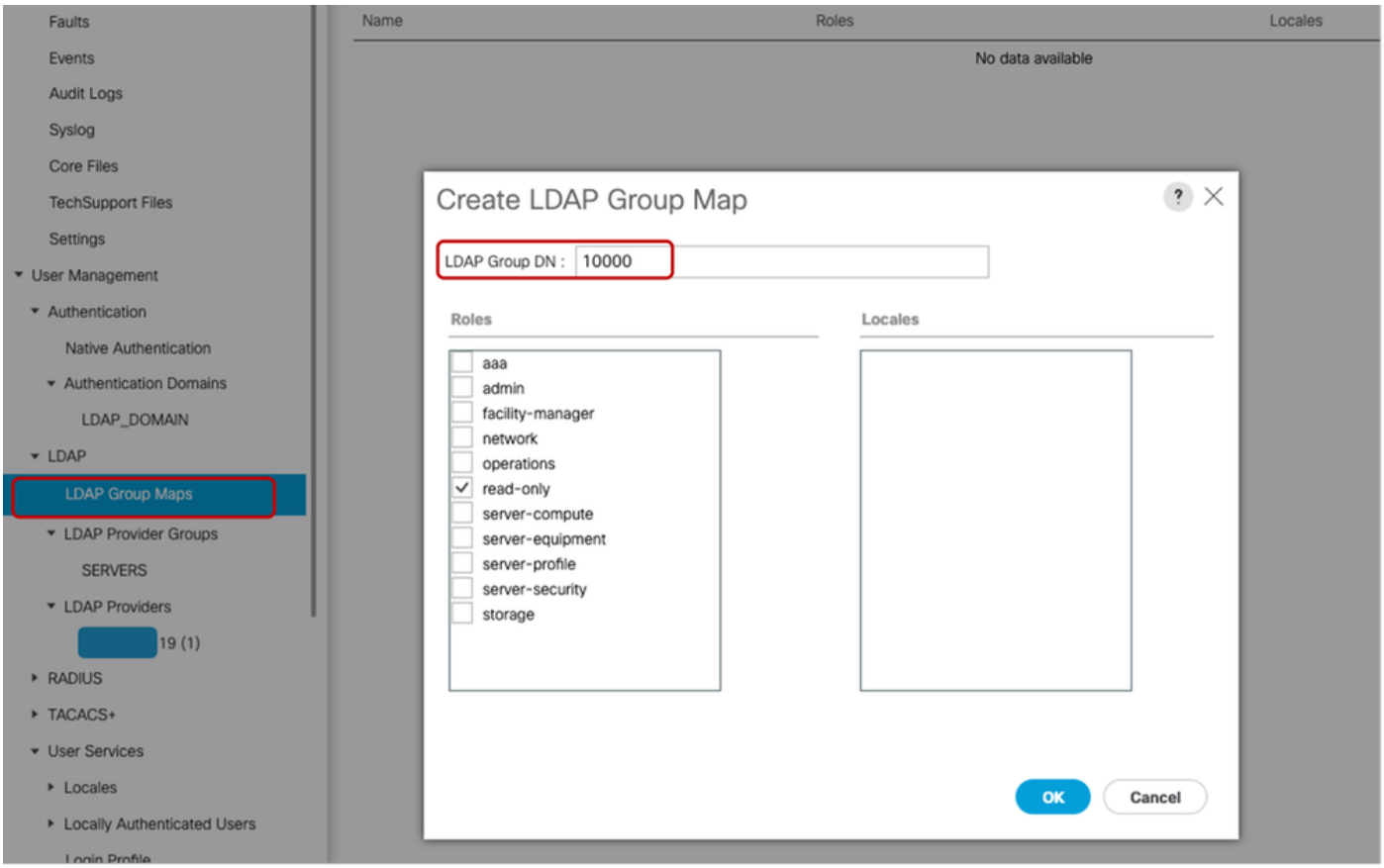


Onder Alle >> Gebruikersbeheer >> LDAP >> LDAP Providers>> LDAP Group Rules is het standaard doelkenmerk voor UCS Manager "memberOf". OpenLDAP-servers hebben dat attribuut standaard niet ingeschakeld, waardoor het instellen van de waarde voor het doelattribuut op "memberOf" (of leeg laten) ertoe leidt dat de aanmeldingen van gebruikers mislukken omdat de OpenLDAP-server de gevraagde waarde voor het attribuut niet herkent.

In dit voorbeeld is de waarde "Target Attribute" ingesteld op "gidNumber".

Voeg de geconfigureerde LDAP-provider toe aan een LDAP-providergroep. Voor deze demonstratie is de "SERVERS" LDAP Provider Group gemaakt.

Bij het configureren van de "LDAP Group Maps" in "All >> User Management >> LDAP >> LDAP Group Maps>>" wordt de waarde gidNumber (in dit geval "10000") gebruikt als de "Group DN Map" zoals weergegeven:



Configureer een LDAP-verificatiedomein (LDAP_DOMAIN) in "Alles >> Gebruikersbeheer >> Authenticatie >> Authenticatiedomeinen", verwijzend naar de LDAP-providergroepen en test de LDAP-gebruikersaanmelding.

Opmerking: Als het attribuut memberOf aan specifieke milieuvereisten moet voldoen of de functie "Groepsherhaling" moet implementeren, wordt aanbevolen om de tweede configuratieoptie hieronder te gebruiken, waarvoor LDAP met Overlay-extensies is ingeschakeld.

Hoewel LDAP Account Manager (LAM) overlay-configuratie ondersteunt, moet u er rekening mee houden dat voor deze functie de juiste licenties vereist zijn.

Raadpleeg de officiële documentatie van de LDAP-accountmanager voor meer informatie over het configureren van LDAP met behulp van LAM.

Optie 2: OpenLDAP configureren met behulp van Ubuntu CLI-tools en overlays

Om OpenLDAP te gebruiken voor UCS Manager-verificatie, zijn twee overlays vereist die ervoor zorgen dat de groepen worden gekoppeld aan gebruikers op een manier die het UCS-systeem (UCS Manager en CIMC) kan begrijpen.

De configuratie aan de OpenLDAP-zijde vereist:

- "member of" overlay: Deze overlay maakt mapping tussen gebruikers en groepen, zodat als een gebruikers-DN wordt opgevraagd, het attribuut memberOf kan worden opgevraagd als onderdeel van die query. Standaard geen attribuut voor gebruikers voor groepslidmaatschap, tenzij het lid van overlay is toegevoegd aan openLDAP
- "Refint"-overlay: deze overlay is geconfigureerd om te valideren dat items in het lidkenmerk in groepsobjecten gesynchroniseerd blijven met het lidkenmerk van gebruikersobjecten. Zonder deze service kunnen, als een gebruiker wordt verwijderd zonder ook de groep te wijzigen, verweesde DN's in het groepsobject blijven. De raffinageservice zorgt voor consistentie in beide richtingen.

Stap 1: Initiële nettools en configuratie van de hostnaam van de Linux-server

Herhaal stap 1 binnen optie 1.

Stap 2: SLAPD installeren

Herhaal stap 2 binnen optie 1. (Met uitzondering van PHP en Apache installatie als optie 2 vereist niet dat ze werken - geen LAM)

Zorg ervoor dat u de vereiste poorten toestaat via de Ubuntu Firewall.

Stap 3: Installeer 'memberOf' Overlay op de LDAP-server

Controleer of de "memberOf"-bedekking is geïnstalleerd

```
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
```

Om de "memberOf" overlay te installeren, maakt u een .ldif-bestand met de naam ldap.memberof.load.ldif (gebruik elke gewenste naamgevingsconventie) en voegt u de opgegeven

configuratie toe:

```
cat <

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

Voeg de configuratie in het bestand ldap.member.load.ldif toe aan het LDAP-profiel met de opgegeven opdracht:

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

Configureert de memberOf-module en de olcDatabase-vermelding om aan de implementatievereisten te voldoen, afhankelijk van de Linux-distributies.

Twee verplichte attribuutwaarden zijn "olcDatabase={1}mdb" en "groupOfNames" zoals hieronder weergegeven.

Maak het bestand ldap.member.config.ldif, vul de kenmerken ervan in en importeer de inhoud ervan in het LDAP-profiel.

```
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
```

Stap 4: Installeer 'Refint' Overlay op de LDAP-server

Installeer vervolgens opnieuw installeren naar openldap:

Maak een .ldif-bestand met de naam ldap.refint.load.ldif (gebruik elke gewenste naamgevingsconventie) en voeg de opgegeven configuratie toe:

```
cat <

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

Importeer de configuratie in het bestand ldap.refint.load.ldif naar het LDAP-profiel met de opgegeven opdracht:

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

Configureer de verfijning, die de referentie-integriteit tussen groepen en gebruikers behoudt.

Configureert de verfijningsmodule en de vermelding olcDatabase om aan de implementatievereisten te voldoen.

Maak het bestand ldap.refint.config.ldif en importeer de inhoud ervan in het LDAP-profiel.

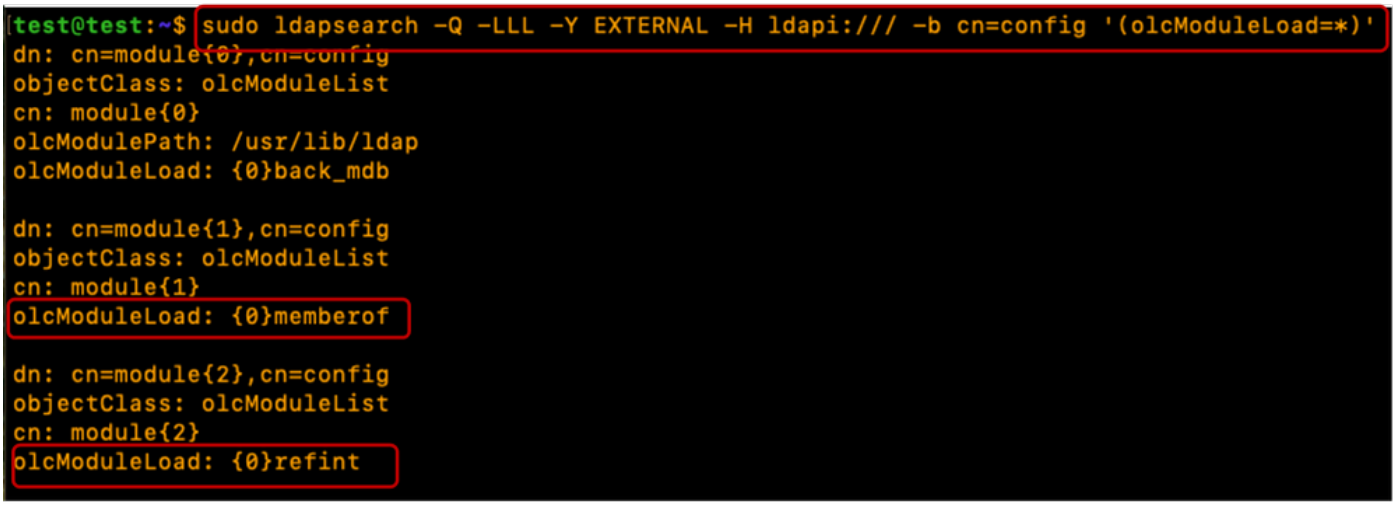
```
cat <

      ./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
```

Bij installatie van beide plug-ins/extensies is de uitvoer naar de opgegeven ldapsearch-opdracht vergelijkbaar met de uitvoer die hieronder wordt weergegeven:

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



Wanneer beide plug-ins/extensies zijn geconfigureerd, is de uitvoer naar de opgegeven ldapsearch-opdracht vergelijkbaar met de weergegeven uitvoer:

```
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
```

Start de slapd-service voor de nieuw geïnstalleerde plug-ins / modules opnieuw om bruikbaar te zijn:

```
sudo systemctl restart slapd
```

Stap 5: Maak OU's, gebruikers en groepen

Organisatorische eenheden (voor gebruikers en groepen), gebruikers en groepen maken.

Maak de gebruikers (mensen) en groepen (groepen) OU's en importeer ze in het LDAP-profiel. Hiervoor is het wachtwoord van de "admin"-account vereist:

```
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
```

Maak de gebruikers (testuser1, testuser2 en bind_user), wijs ze toe aan hun respectievelijke OU's (mensen), voeg ze toe aan hun groepen met behulp van gidNumbers (goede praktijken) en importeer de gebruikers in het LDAP-profiel.

```
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:~$
```

Maak de groepen (it), koppel ze aan hun respectievelijke OU's (groepen), associeer groepsleden (testuser1, testuser2) en importeer ze in het LDAP-profiel:

```
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
```

Opmerking: Zelfs als het kenmerk memberOf niet expliciet is gedefinieerd tijdens het maken van gebruikers of groepen, genereert en onderhoudt het systeem deze verwijzing automatisch. Zodra de gebruiker aan een groep is gekoppeld, weerspiegelt het kenmerk memberOf deze lidmaatschappen automatisch, zodat de directory gesynchroniseerd blijft met de huidige toegangsstructuur.

Stap 6: Lokale LDAP-aanmelding testen

Verifieer de aanmelding van de gebruiker bij de LDAP-server met behulp van de opgegeven opdracht (vervang aanmeldparameters afhankelijk van uw omgeving):

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

Configuratieparameters op CIMC

Log in bij CIMC.

Selecteer in het navigatiedeelvenster Beheer, Gebruikersbeheer en LDAP.

Vul de LDAP-configuratieparameters in zoals hieronder wordt weergegeven:

- LDAP inschakelen: ingeschakeld
- Basis-DN: dc=xxxxxxxx, dc=com

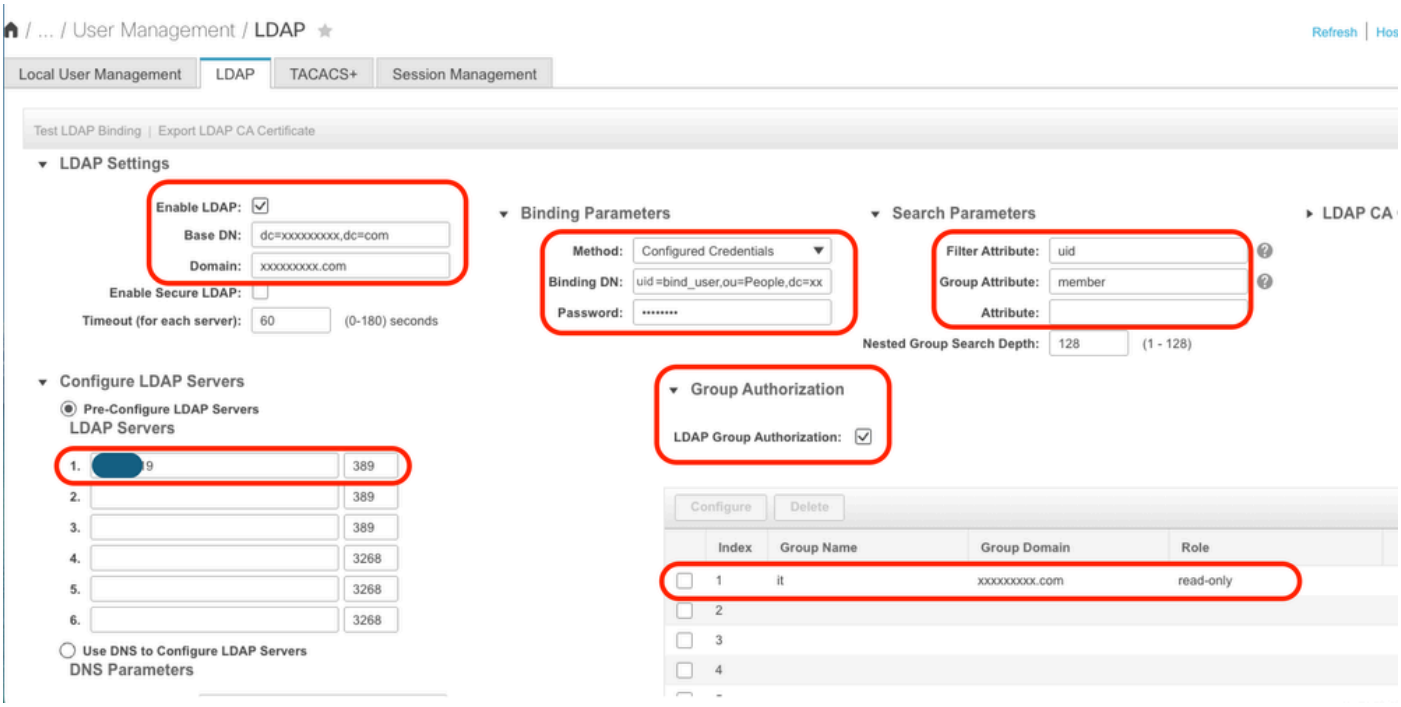
- Domein: xxxxxxxxx.com

- LDAP-servers: <ldap_server_IP of FQDN> X.X.X.19

- Bindende parameters: dit kunnen "inloggegevens" of "geconfigureerde referenties" zijn
  - Voeg bij het gebruik van geconfigureerde referenties de bind_user-DN precies toe zoals geconfigureerd op de LDAP-server:
  - Bijvoorbeeld: "cn=bind_user, ou=People, dc=xxxxxxxxx, dc=com" of "uid=bind_user, ou=People, dc=xxxxxxxxx, dc=com"

- Zoekparameters:
  - Filterkenmerk: "cn" of "uid"
  - Groepsattribuut: lid

- LDAP-groepsautorisatie - gecontroleerd
  - Groepsnaam: it
  - Groepsdomein: xxxxxxxxx.com
  - Rol: alleen-lezen (elke voorkeursrol)



Sla de configuratie op en test de aanmeldingsgegevens van de LDAP-gebruiker.

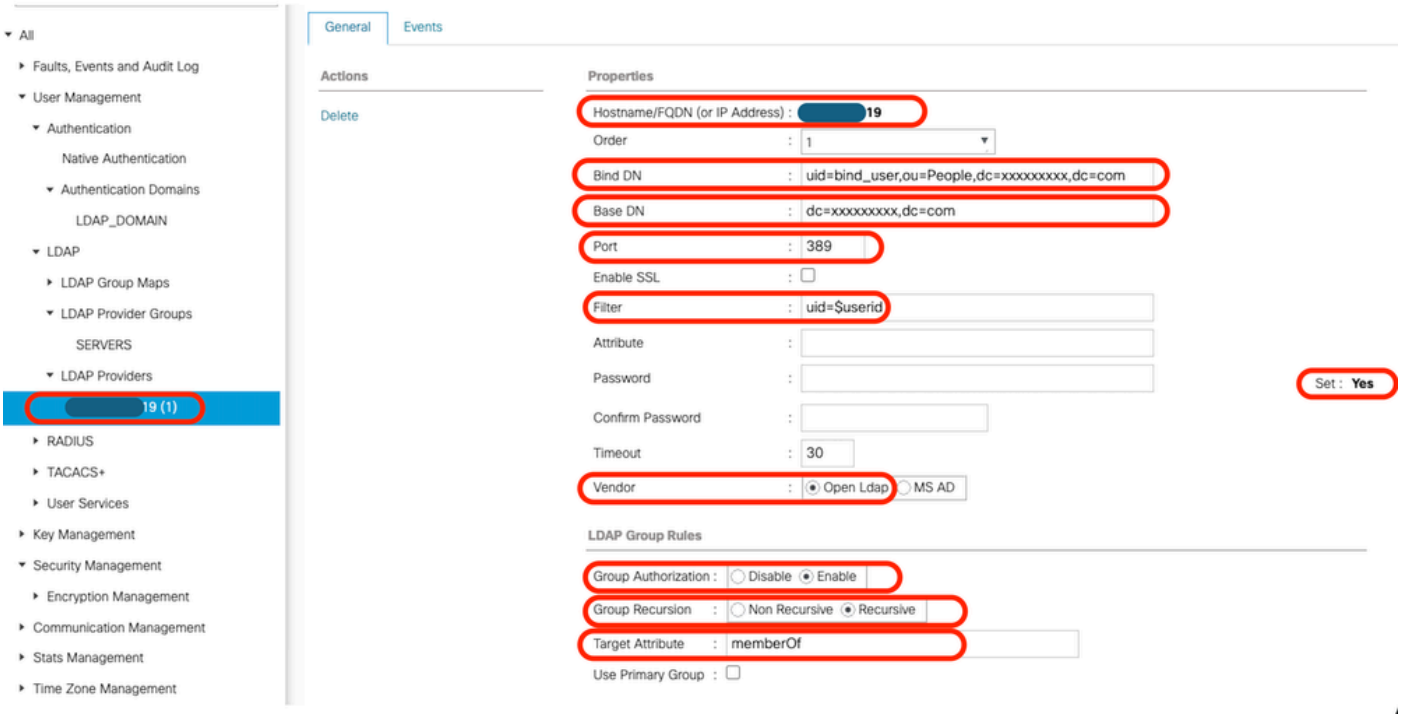
Configuratieparameters in UCS Manager

Meld u aan bij UCS Manager.

Selecteer in het navigatiedeelvenster Beheer, Gebruikersbeheer en LDAP.

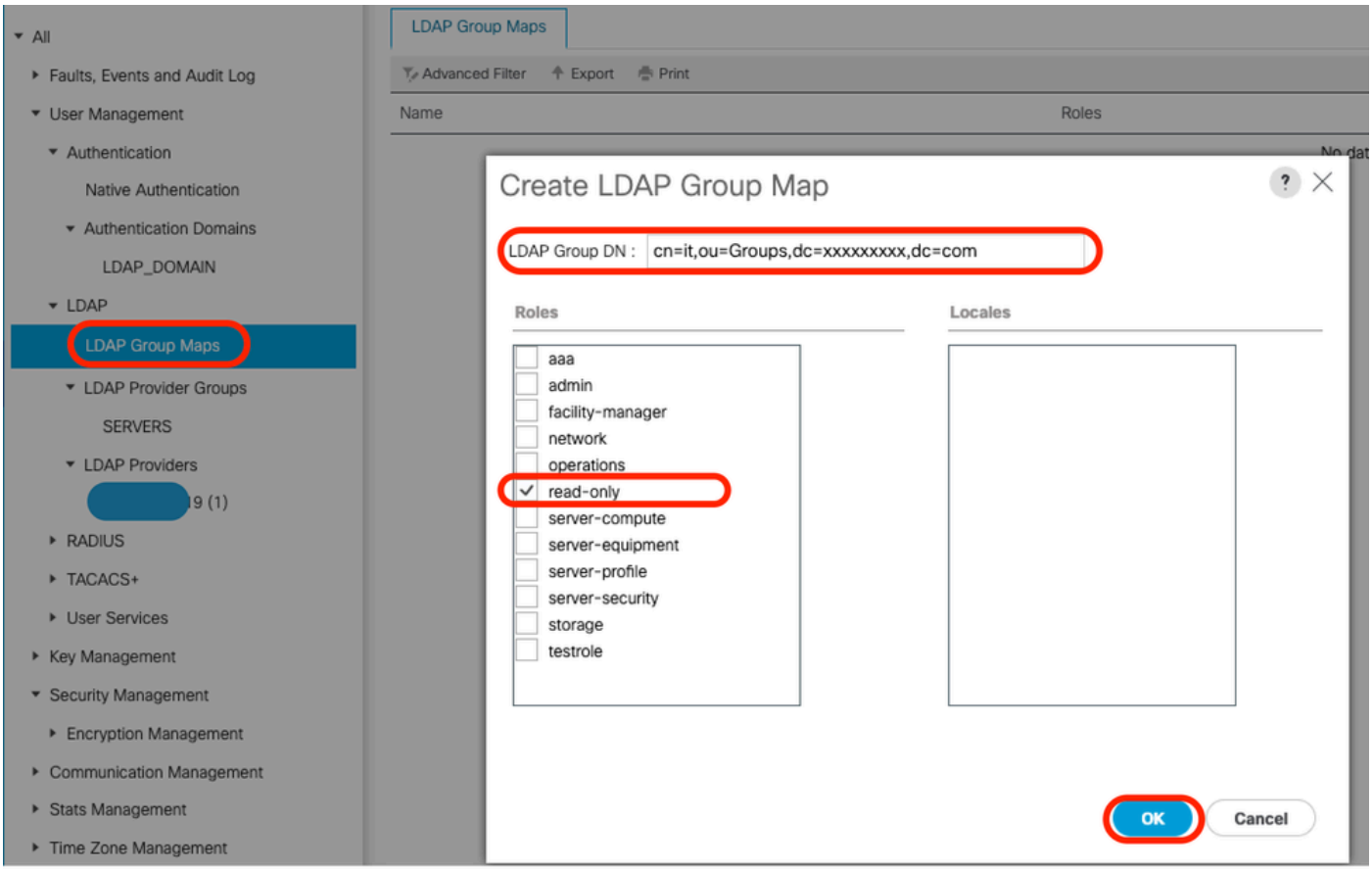
Vul de LDAP-configuratieparameters in zoals hieronder wordt weergegeven:

- LDAP-providers:
  - Hostnaam: <FQDN of IP-adres van LDAP-server>
  - Bind DN: uid=bind_user, ou=People, dc=xxxxxxxx, dc=com
  - Basis-DN: dc=xxxxxxxx, dc=com
  - Poort: 389
  - SSL inschakelen: uitgeschakeld
  - Filter: uid=$userid
  - groepsautorisatie: ingeschakeld
  - Groepscorrectie: recursief
  - Target Attribuut: lid van
- LDAP Group Maps:
  - LDAP Group DN: cn=it, ou=Groups, dc=xxxxxxxx, dc=com



Voeg de geconfigureerde LDAP-provider toe aan een LDAP-providergroep. Voor deze demonstratie wordt de "SERVERS" LDAP Provider Group gebruikt.

Configureer de LDAP Group Maps door een "LDAP Group DN" toe te voegen, opgehaald van de LDAP-server.



Configureer een LDAP-verificatiedomein (LDAP_DOMAIN) in "Alles >> Gebruikersbeheer >> Authenticatie >> Authenticatiedomeinen", verwijzend naar de LDAP-providergroepen (SERVERS) en test de LDAP-gebruikersaanmelding.

Laten we vervolgens kijken naar het instellen van hetzelfde (met Overlay) in een afzonderlijke Linux-distributie (CentOS 10)

Scenario 2: CentOS Stream 10 - Fedora

De configuratieprocedures voor Lightweight Directory Access Protocol (LDAP) variëren afhankelijk van de onderliggende versie van het besturingssysteem. Deze sectie richt zich op de implementatie van LDAP op CentOS Stream 10.

Hoewel veel Linux-distributies OpenLDAP gebruiken, gebruiken CentOS Stream 10 en hedendaagse op Fedora gebaseerde systemen de 389 Directory Server (389 DS) als de standaard LDAP-provider.

Opmerking: Hoewel 389 DS wordt beschouwd als de opvolger van OpenLDAP binnen de CentOS- en Red Hat-ecosystemen, zijn de twee oplossingen niet direct uitwisselbaar. Hun respectievelijke directorystructuren, configuratiebestanden en operationele omgevingen verschillen aanzienlijk.

Deze handleiding bevat de noodzakelijke stappen voor het succesvol configureren van LDAP met behulp van 389 DS in een CentOS Stream 10-omgeving.

Optie 1: LDAP configureren met 389 Directory Server op CentOS Stream 10

Stap 1: Eerste installatie

Herhaal stap 1 in scenario 1, optie 1.

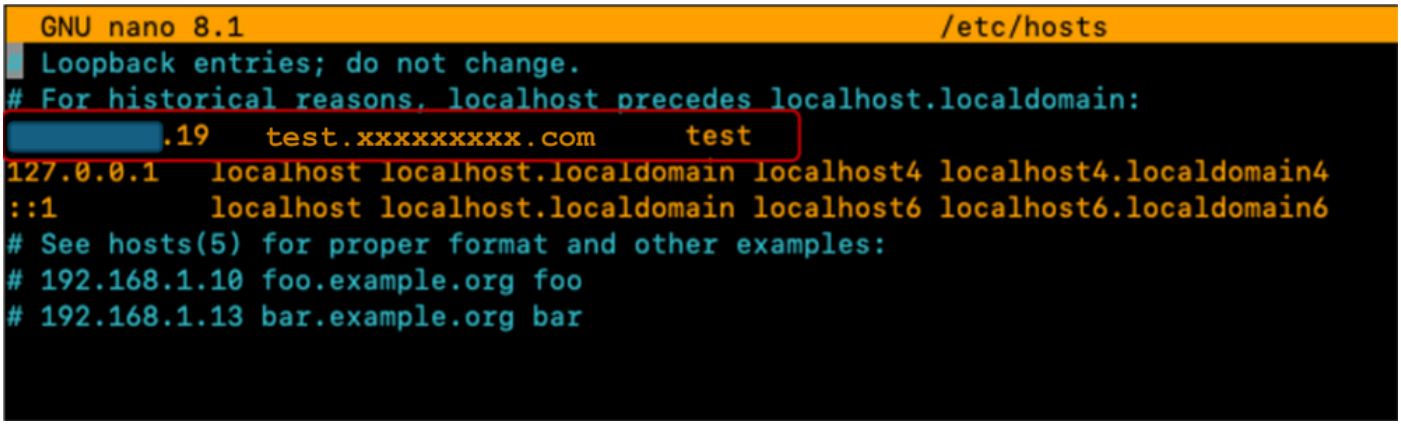
CentOS-systemen maken geen gebruik van de APT-pakketbeheersuite. Om de benodigde software-installaties op CentOS Stream 10 uit te voeren, gebruikt u de dnf (Dandified YUM) of yum package managers

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

Controleer het IP-adres van de server met de opdracht "ifconfig".

Voeg het IP-adres van de server toe aan het bestand "/etc/hosts", samen met de volledig gekwalificeerde domeinnaam van de server (bijvoorbeeld: test.xxxxxxxxx.com gebruikt in dit lab) en de hostnaam (bijvoorbeeld: test) in de hieronder gespecificeerde indeling:

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



Werk het bestand "/etc/hostname" bij door de inhoud ervan te vervangen door de hostnaam (test).

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

De server moet opnieuw worden opgestart voordat deze wijzigingen van kracht worden.

```
sudo reboot
```

Stap 2: EPEL repo en 389 Server pakket installeren

De EPEL-repository installeren en bijwerken.

Installeer het 389 Directory Server-pakket.

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

Maak een directory-sjabloonbestand met de gewenste parameters voor de LDAP-serverinstellingen:

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

Controleer de inhoud van het gemaakte sjabloonbestand (ldapconfig.conf)

```
sudo cat ldapconfig.conf
```

Bewerk het sjabloonbestand ldapconfig.conf.

```
sudo nano ldapconfig.conf
```

Voeg de opgegeven configuratiegegevens in het bestand in en sla de wijzigingen op.

Opmerking: er kunnen verschillende wijzigingen worden vereist op basis van de specifieke behoeften of vereisten van elke omgeving.

Dit voorbeeld behandelt de basislijnconfiguraties voor deze demonstratie.

```
[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
```

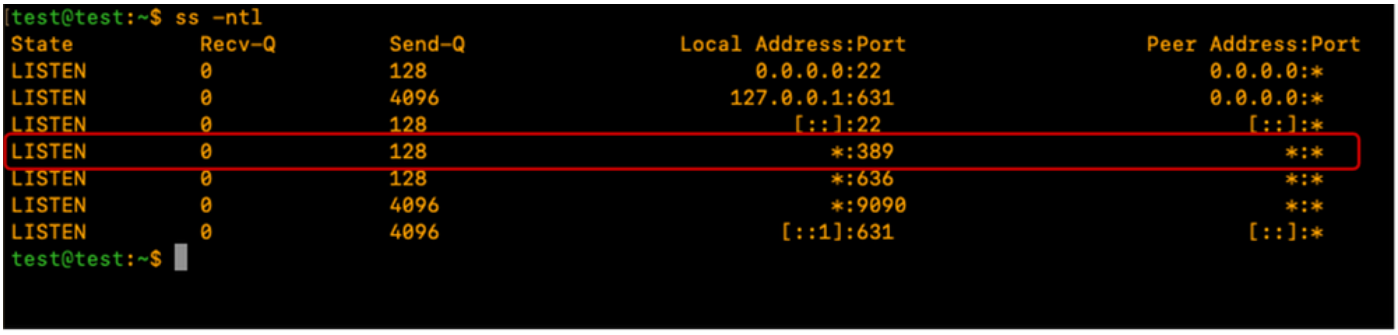
Het sjabloonbestand definieert de configuratieparameters voor de directory-instantie "localhost". Dit omvat het instellen van de beheerdersgebruiker ("admin"), het bijbehorende wachtwoord en de domeincontext ("xxxxxxxx.com").

Maak de "localhost" directory-instantie met behulp van de sjabloon die eerder is bewerkt. Met de opgegeven opdracht wordt de LDAP-directoryserver gemaakt en gestart:

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

Controleer of de LDAP-service op de server wordt uitgevoerd

```
ss -ntl
```



Pas de CentOS-firewall aan om de vereiste poort(en) voor LDAP (389 en/of 636) toe te staan.

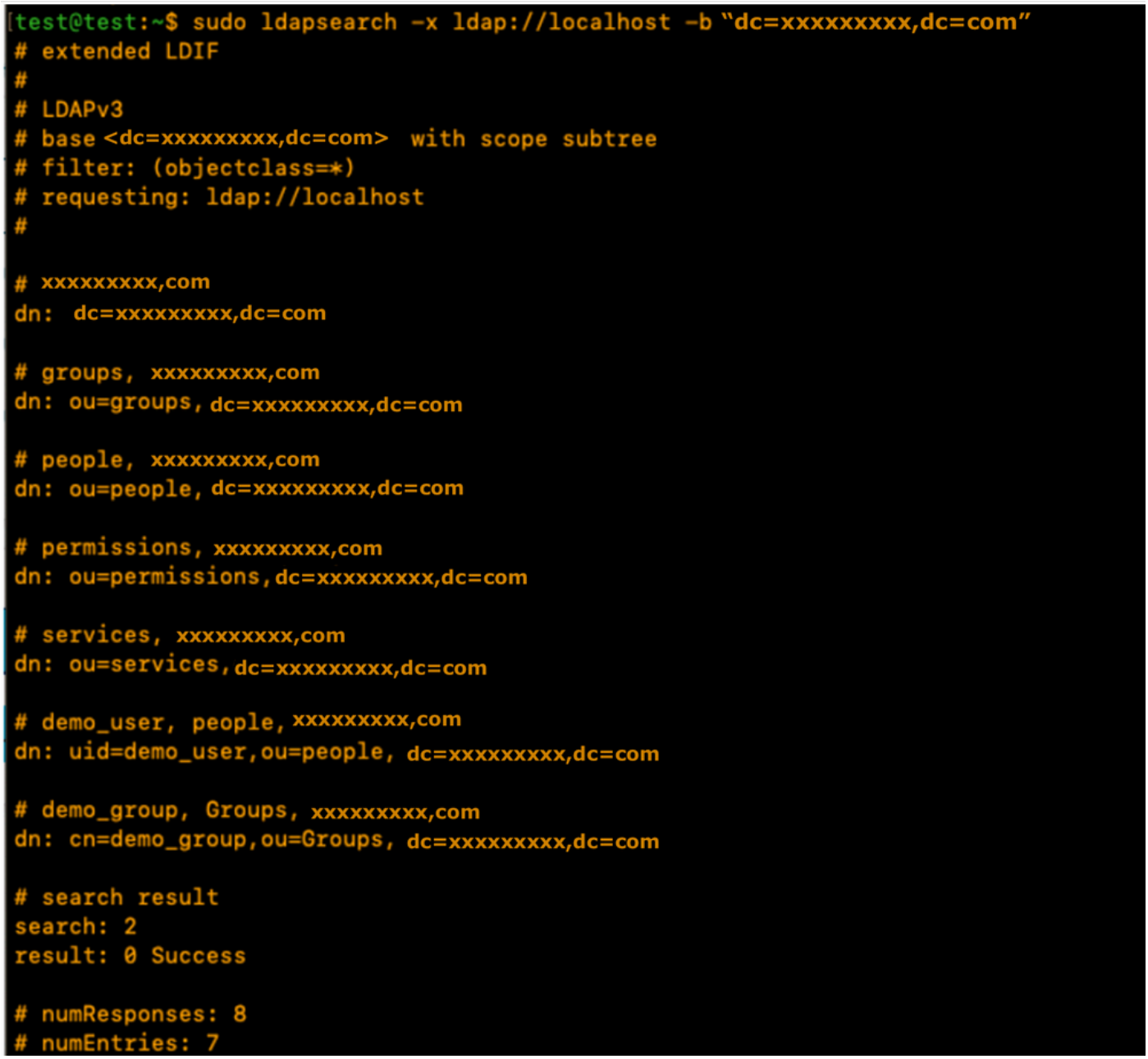
Voor deze demo is de firewall uitgeschakeld.

```
sudo systemctl stop firewalld
```

Controleer of LDAP lokaal op de LDAP-server werkt door de opgegeven opdracht uit te voeren en

zorg ervoor dat de LDAP-uitvoer wordt geretourneerd zoals wordt weergegeven:

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



De uitvoer bevat demo-accounts die zijn gemaakt door de 389DS-server. De LDAP-server maakt automatisch standaard-OU's.

De mensen OU voor gebruikers en de groepen OU voor groepen. Afhankelijk van de vereisten kunnen extra OU's worden gemaakt.

Voor deze demonstratie worden de standaard/automatisch gemaakte OU's gebruikt.

Raadpleeg de officiële 389DS-documentatie voor meer informatie over het uitgebreide gebruik van het 389DS-pakket:

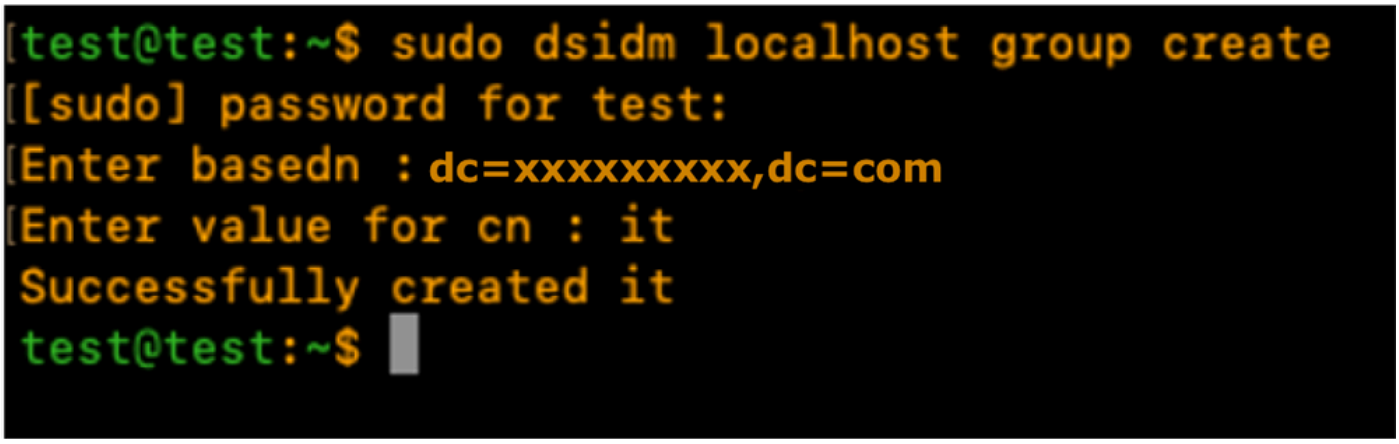
Stap 3: LDAP-groepen en -gebruikers maken

Maak een groep (it) met de opgegeven opdracht: sudo dsidm <instance_name> groep maken.

Voor deze demonstratie is de instantienaam "localhost".

```
sudo dsidm localhost group create
```

Voer de terminalprompt in om de groepsdetails in te vullen zoals wordt weergegeven:



Maak testuser1-gebruikersaccount aan met de opdracht:

```
sudo dsidm localhost user create
```

Voer de terminalprompt in om de gebruikersgegevens in te vullen zoals wordt weergegeven

```
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
```

Maak een wachtwoord voor testuser1 met de opgegeven opdracht en voer de CLI-prompt in:

```
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:~$
```

Voeg de gebruiker toe aan een groep met de opgegeven opdracht: "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
```

Herhaal de stappen voor het maken van de gebruiker om testuser2 en bind_user te maken.

Opmerking: Zorg ervoor dat elke gebruiker expliciet wordt toegevoegd aan de beoogde groepen.

Het weglaten van deze stap kan leiden tot beperkte toegang of mislukte autorisatie.

Het bind_user account hoeft geen lid te zijn van een specifieke groep, omdat het kan worden geconfigureerd als een zelfstandige account, waardoor flexibiliteit wordt geboden om toegang op beheer- en serviceniveau binnen de directory-omgeving te beheren.

Start de directoryinstantie opnieuw op:

```
sudo dsctl localhost restart
```

Stap 4: lid van overlay installeren

Installeer de plugin "memberOf" en start de Directory-instantie opnieuw op:

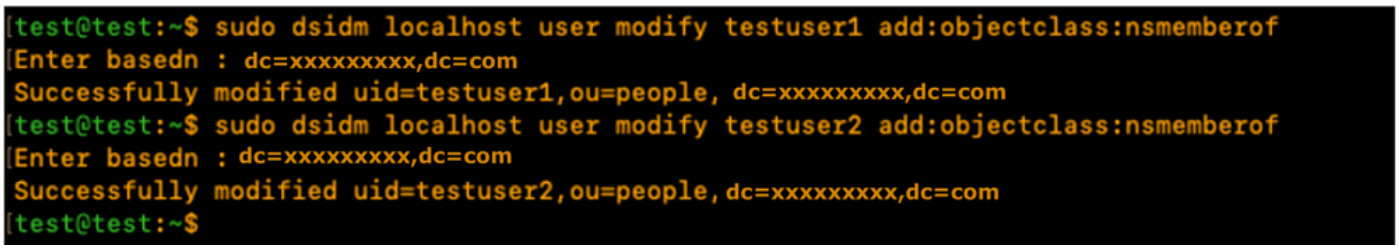
```
sudo dsconf localhost plugin memberof status
sudo dsconf localhost plugin memberof enable
sudo dsctl localhost restart
```

Configureer de plugin "memberOf" met de opgegeven opdracht: "sudo dsconf <directory_instance> plugin member of set --scope <base_dn>"

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

Markeer Gebruikers als geldige "memberOf"-doelen met de opgegeven opdracht: "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
```



Genereer "memberOf" fixup voor de basis DN: "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:~$
```

Controleer de gebruikersconfiguratie:

```
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:~$
```

De 389DS LDAP-server is geconfigureerd met de memberOf-plugin om het attribuut memberOf te ondersteunen.

Configuratieparameters op CIMC

Log in bij CIMC.

Selecteer in het navigatiedeelvenster Beheer, Gebruikersbeheer en LDAP.

Vul de LDAP-configuratieparameters in zoals hieronder wordt weergegeven:

- LDAP inschakelen: ingeschakeld
- Basis-DN: dc=xxxxxxxx, dc=com

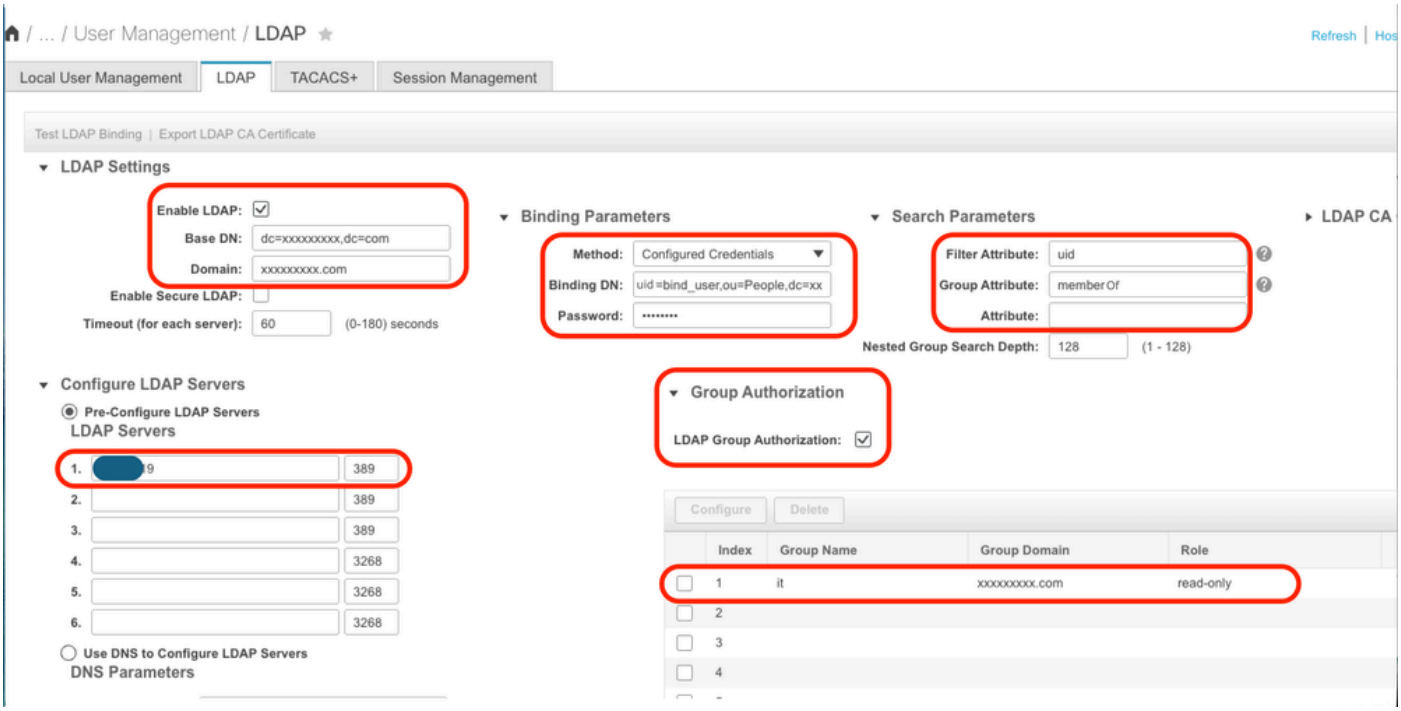
- Domein: xxxxxxxxx.com

- LDAP-servers: <ldap_server_IP of FQDN> X.X.X.19

- Bindende parameters: dit kunnen "inloggegevens" of "geconfigureerde referenties" zijn
  - Voeg bij het gebruik van geconfigureerde referenties de bind_user-DN precies toe zoals geconfigureerd op de LDAP-server:
    - Bijvoorbeeld: "cn=bind_user, ou=People, dc=xxxxxxxxx, dc=com" of "uid=bind_user, ou=People, dc=xxxxxxxxx, dc=com"

- Zoekparameters:
  - Filterkenmerk: "cn" of "uid"
  - Groepsattribuut: lid van

- LDAP-groepsautorisatie - gecontroleerd
  - Groepsnaam: it
  - Groepsdomein: xxxxxxxxx.com
  - Rol: alleen-lezen (elke voorkeursrol)



Sla de configuratie op en test de aanmeldingsgegevens van de LDAP-gebruiker.

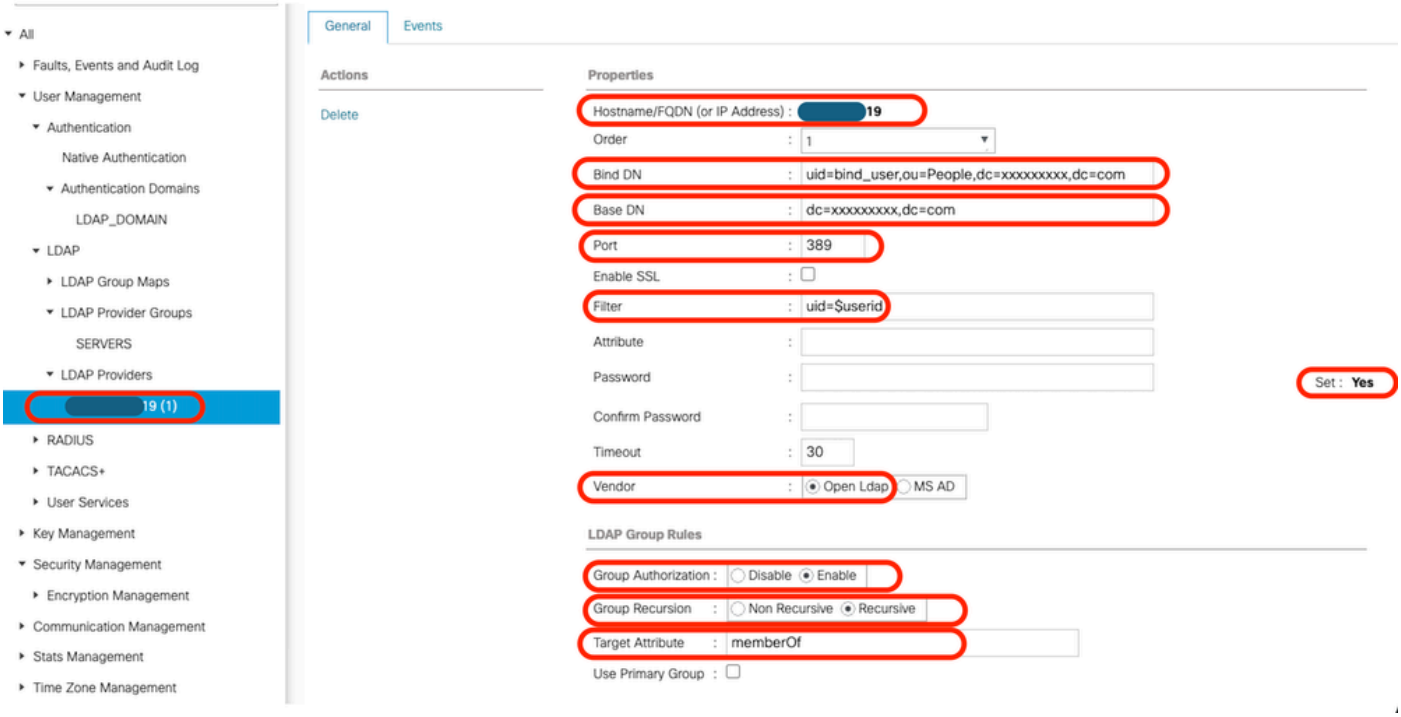
Configuratieparameters in UCS Manager

Meld u aan bij UCS Manager.

Selecteer in het navigatiedeelvenster Beheer, Gebruikersbeheer en LDAP.

Vul de LDAP-configuratieparameters in zoals hieronder wordt weergegeven:

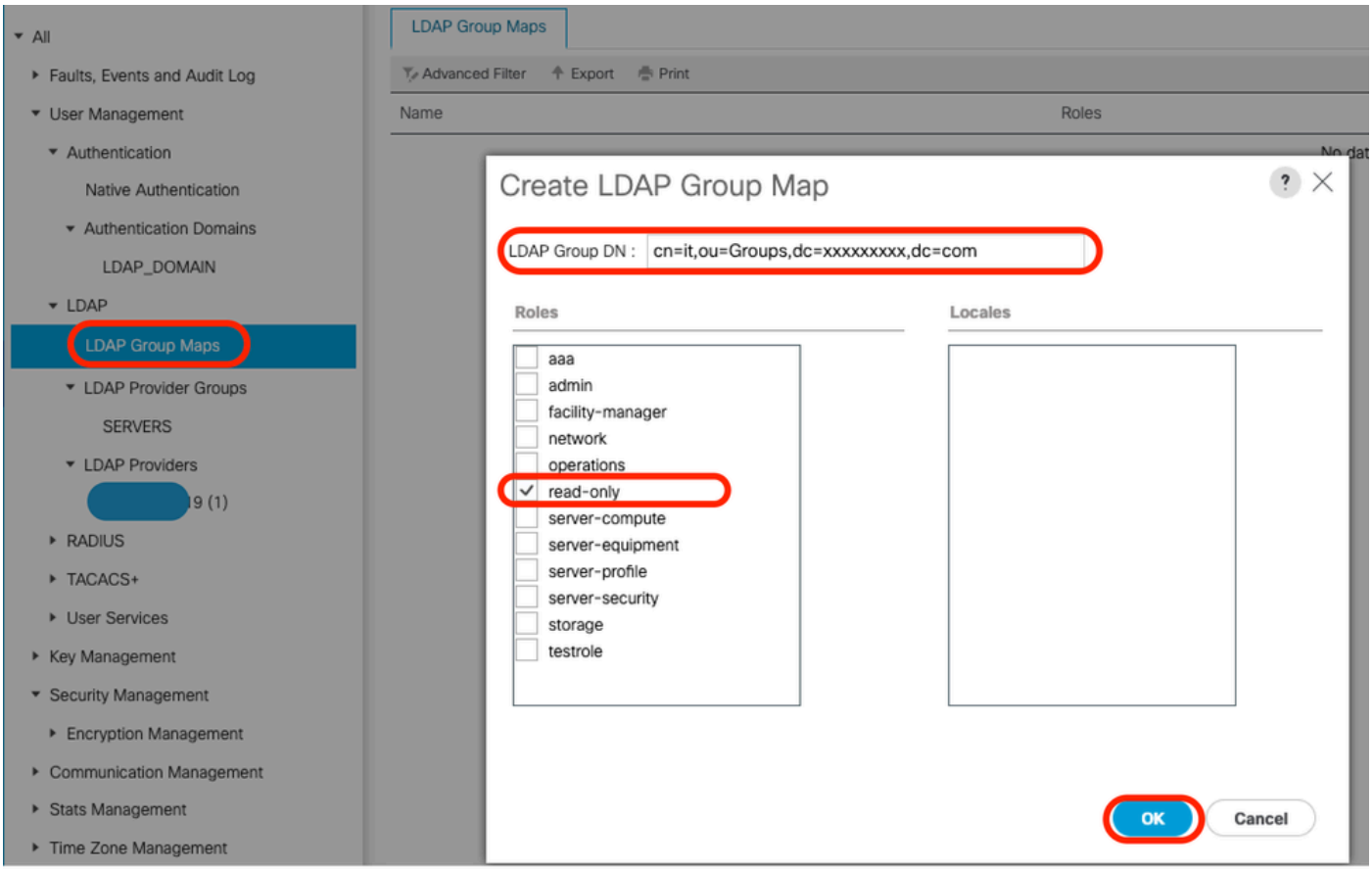
- LDAP-providers:
  - Hostnaam: <FQDN of IP-adres van LDAP-server>
  - Bind DN: uid=bind_user, ou=people, dc=xxxxxxxx, dc=com
  - Basis-DN: dc=xxxxxxxx, dc=com
  - Poort: 389
  - SSL inschakelen: uitgeschakeld
  - Filter: uid=$userid
  - groepsautorisatie: ingeschakeld
  - Groepscorrectie: recursief
  - Target Attribuut: lid van
- LDAP Group Maps:
  - LDAP Group DN: cn=it, ou=Groups, dc=xxxxxxxx, dc=com



Voeg de geconfigureerde LDAP-provider toe aan een LDAP-providergroep. Voor deze

demonstratie wordt de "SERVERS" LDAP Provider Group gebruikt.

Configureer de LDAP Group Maps door een "LDAP Group DN" toe te voegen, opgehaald van de LDAP-server.



Configureer een LDAP-verificatiedomein (LDAP_DOMAIN) in "Alles >> Gebruikersbeheer >> Authenticatie >> Authenticatiedomeinen", verwijzend naar de LDAP-providergroepen en test de LDAP-gebruikersaanmelding.

Conclusie

Hoewel deze gids essentiële implementatiescenario's behandelt, kan verdere verkenning van LDAP-mogelijkheden de directoryprestaties en -beveiliging aanzienlijk verbeteren.

Raadpleeg de opgegeven bronnen voor meer informatie, best practices en geavanceerde configuratiedetails:

- Officiële OpenLDAP-documentatie
- LDAP Account Manager - Handleiding

- 389 Directory Server-documentatie

- LDAP configureren in UCS Manager
- Beveiligde LDAP configureren op servers uit de UCS C-reeks

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.