Configura LDAP in UCS Manager & CIMC che utilizza server Linux OpenLDAP e 389-DS

Sommario

Introduzione

In questo documento viene descritta una serie di opzioni per configurare LDAP come metodo di autenticazione per UCS Manager e CIMC utilizzando i server delle directory OpenLDAP e 389

basati su Linux.

Premesse

A causa dell'ampia variabilità delle configurazioni dei server OpenLDAP, un trattamento completo esula dall'ambito di questo documento. In questo articolo vengono invece enfatizzate le configurazioni implementate comunemente che comprendono più distribuzioni Linux, pacchetti di server LDAP e schemi di attributi. A fini di chiarezza e semplicità, questo documento tratta le configurazioni LDAP standard. La configurazione di LDAP sicuro (LDAPS) non è descritta nel presente documento.

Prerequisiti:

Si raccomanda vivamente la conoscenza di questi argomenti:

- UCS serie B
- UCS serie C
- Amministrazione server Linux

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Versione firmware UCS Manager: 4.3 (2 quater)
- Modello Fabric Interconnect: UCS-FI-6454
- Modello di server standalone serie C UCS: UCSC-C240-M5
- Versione firmware standalone UCS serie C: 4.3(2.250045)
- Ubuntu 20.04
- Flusso CentOS 10

Impostazioni utilizzate per questa dimostrazione:

- Nome host server LDAP: test

- Dominio server: xxxxxxxxx.com

- FQDN server: test.xxxxxxxxx.com
- Indirizzo IP server Linux (Ubuntu e CentOS): X.X.X.19
- Utenti OpenLDAP: testuser1, testuser2
- Gruppi OpenLDAP: it
- Account utente di binding OpenLDAP: utente_associazione

Nota: in questo laboratorio è stato usato l'editor di testo linux Nano.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Scenario 1: Ubuntu - Debian

La configurazione del server LDAP può essere eseguita tramite un'interfaccia grafica, ad esempio Gestione account LDAP, o tramite strumenti della riga di comando, a seconda delle preferenze amministrative e del livello di controllo richiesto. In questo scenario viene esaminata la configurazione utilizzando OpenLDAP basato su Linux, a partire da un'implementazione basata su GUI e quindi passando alle utilità della riga di comando per esplorare funzionalità avanzate, inclusi i plug-in di overlay (comunemente utilizzati nelle integrazioni con Cisco UCS Manager).

Opzione 1: Configurare OpenLDAP utilizzando LAM (Ubuntu LDAP Account Manager)

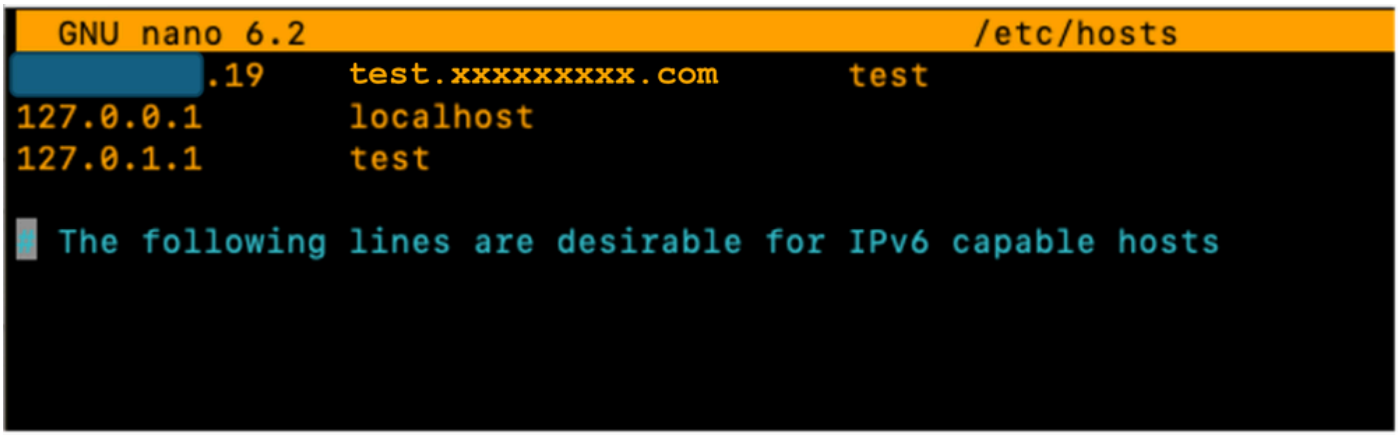
Passaggio 1: Configurazione iniziale del nome host e degli strumenti di rete del server Linux.

Aggiornare ubuntu e installare il pacchetto net-tools per accedere a strumenti come ifconfig, netstat, ecc:

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

Utilizzare il comando "ifconfig" per verificare l'indirizzo IP del server, quindi aggiungerlo al file "/etc/hosts" insieme al nome del dominio del server (ad esempio: "test.xxxxxxx.com" utilizzato in questa esercitazione e nome host (ad esempio: "test") nel formato specificato.

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



Inoltre, aggiornare il file "/etc/hostname" sostituendone il contenuto con il nome host (test).

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

Per rendere effettive le modifiche è necessario riavviare il server.

```
sudo reboot
```

Fase 2: Installare SLAPD, Apache, PHP e le relative dipendenze

Installare quindi Apache, PHP e le relative dipendenze. Queste interfacce vengono usate per abilitare l'interazione dell'interfaccia su una pagina Web:

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

Installa il pacchetto server LDAP aperto "slapd" e le relative dipendenze (ldap-utils)

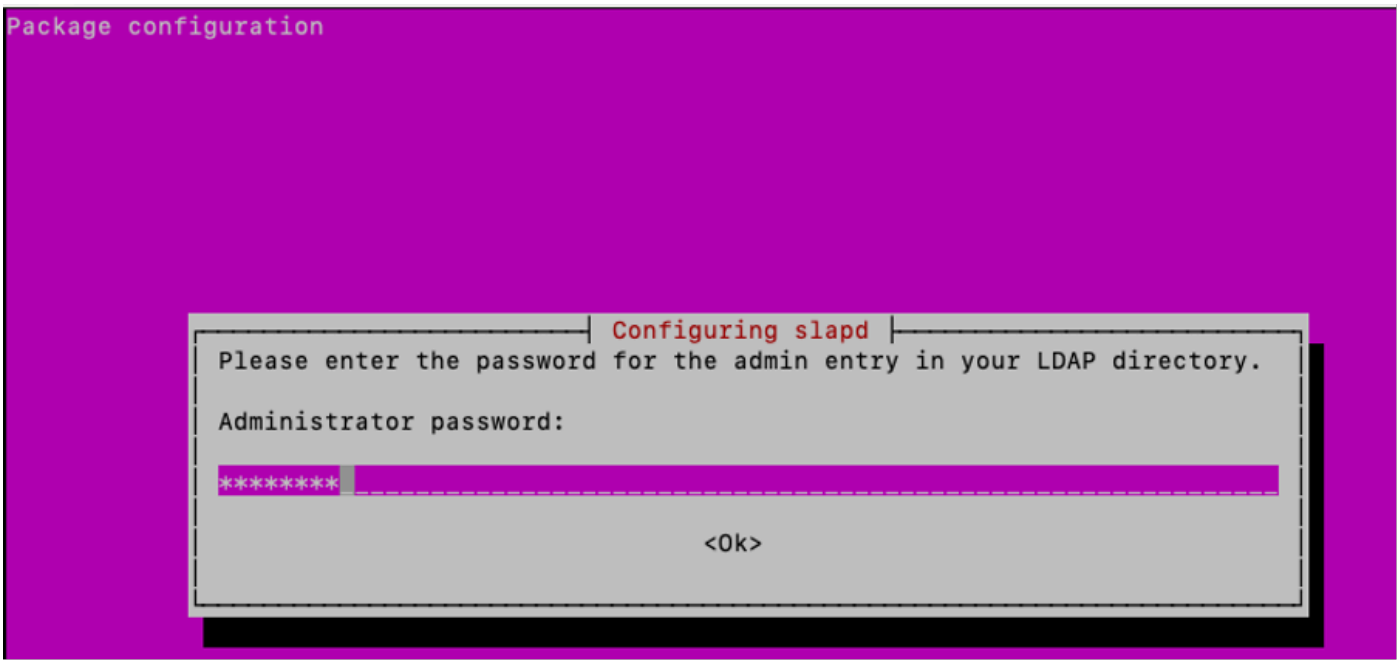
```
sudo apt install slapd ldap-utils -y
```

Durante l'installazione slapd, nella schermata di popup dell'interfaccia grafica visualizzata, immettere la configurazione aggiuntiva del pacchetto SLAPD richiesta.

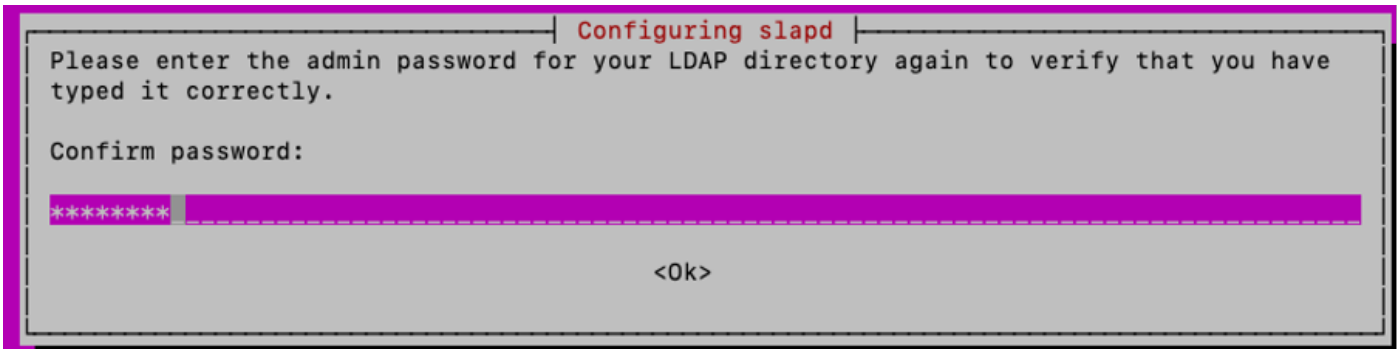
Nota: La perdita della password richiede la reinstallazione del server LDAP.

L'"amministratore" (admin) in questo contesto è un account utilizzato per gestire il servizio, i moduli e le configurazioni OpenLDAP.

Aggiungere la password dell'amministratore del pacchetto LDAP e premere Invio sulla tastiera per selezionare "OK".



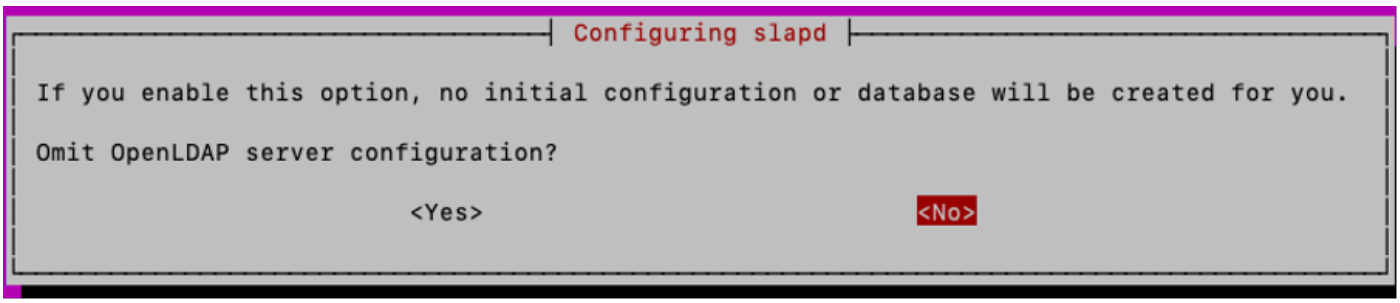
Confermare la password:



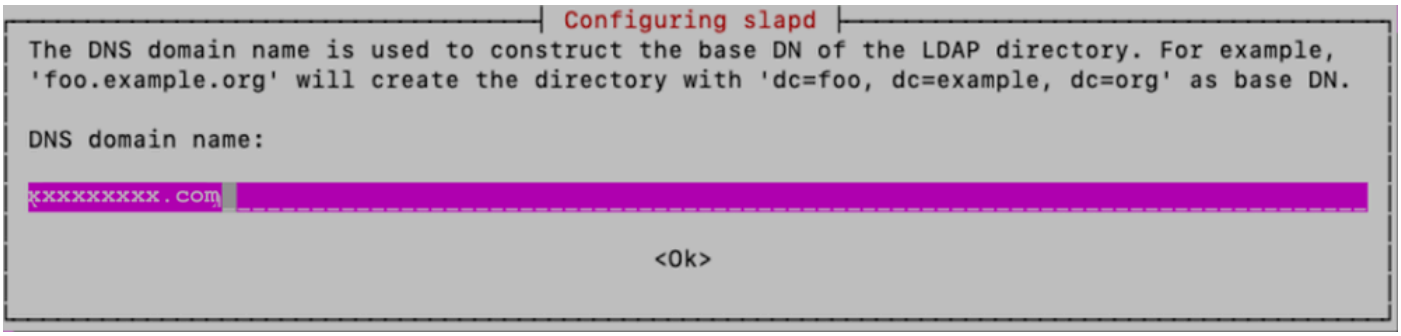
Al termine dell'installazione, è possibile utilizzare il comando specificato per riconfigurare il pacchetto SLAPD, aggiungendo le informazioni sul dominio:

```
sudo dpkg-reconfigure slapd
```

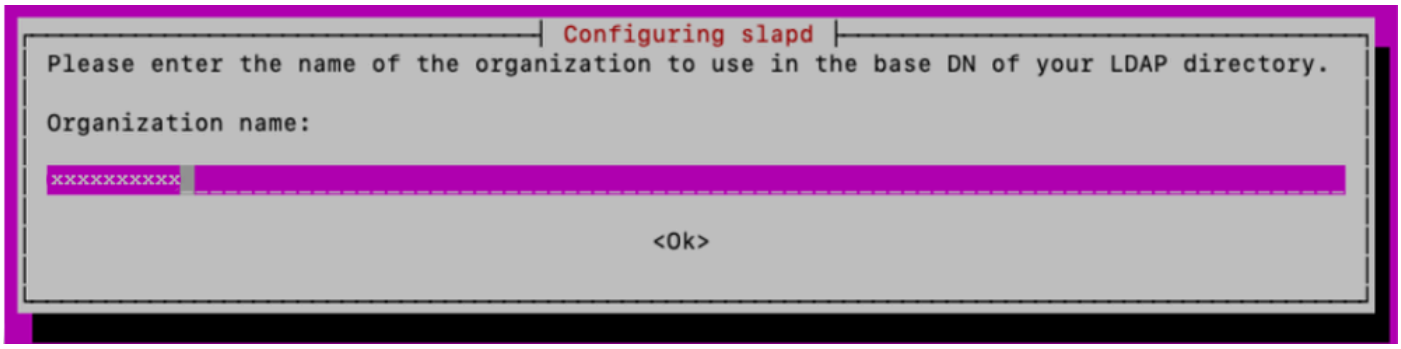
È possibile accettare l'opzione predefinita "No" per "Omit OpenLDAP server Configuration" (Ometti configurazione server OpenLDAP) e premere Invio:



Digitare il nome del dominio e premere Invio:



Per questa esercitazione, "xxxxxxx" viene utilizzato come "Nome organizzazione":

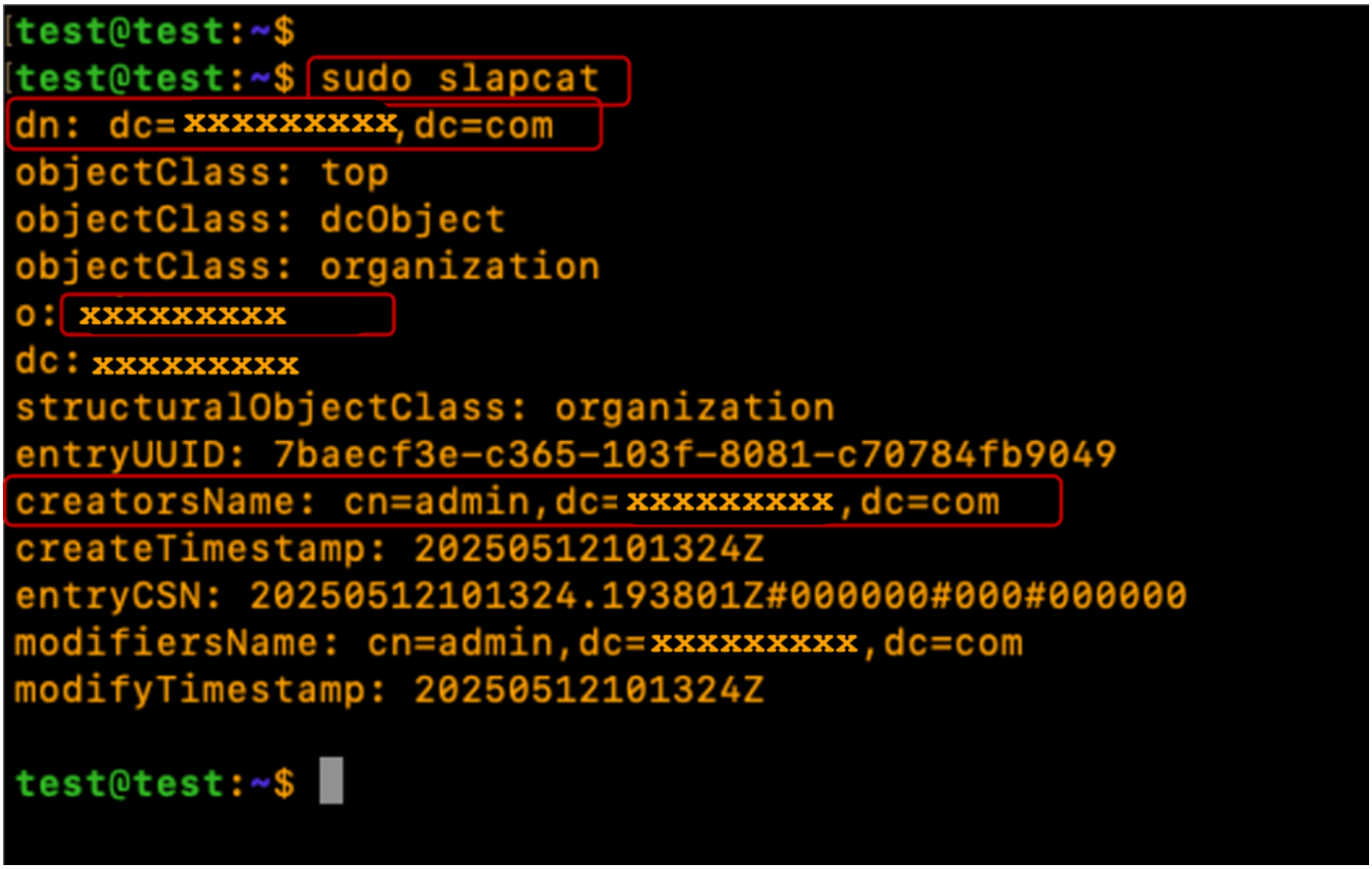


Quindi, digitare la "password amministratore" e confermarla

Per le altre opzioni di configurazione, mantenete le impostazioni predefinite e premete il tasto Invio sulla tastiera per completare la configurazione.

Verificare l'installazione di SLAPD utilizzando il comando:

```
sudo slapcat
```



Passaggio 3: Installare Gestione account LDAP

Installare LDAP Account Manager (LAM) per la creazione e la gestione di utenti e gruppi LDAP:

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

Abilitare l'estensione PHP-CGI PHP, richiesta da LAM.

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

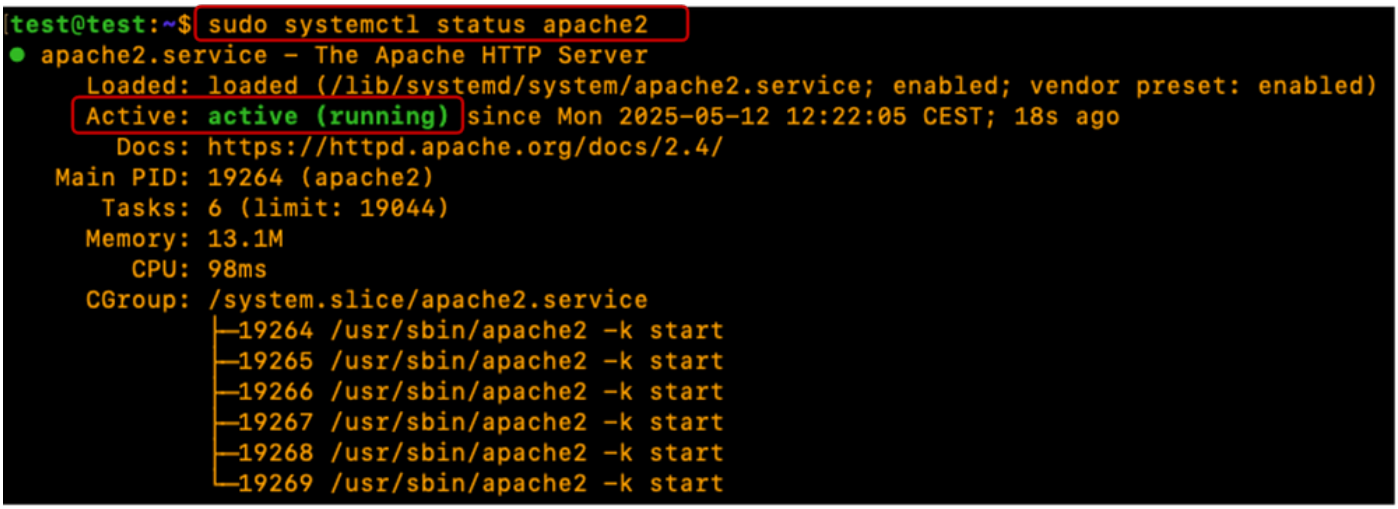
Ricaricare Apache per attivare la nuova configurazione.

Riavviare e abilitare il servizio Apache per l'avvio automatico all'avvio:

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

Verificare che lo stato del server Apache sia "In esecuzione" e "Attivo"

```
sudo systemctl status apache2
```

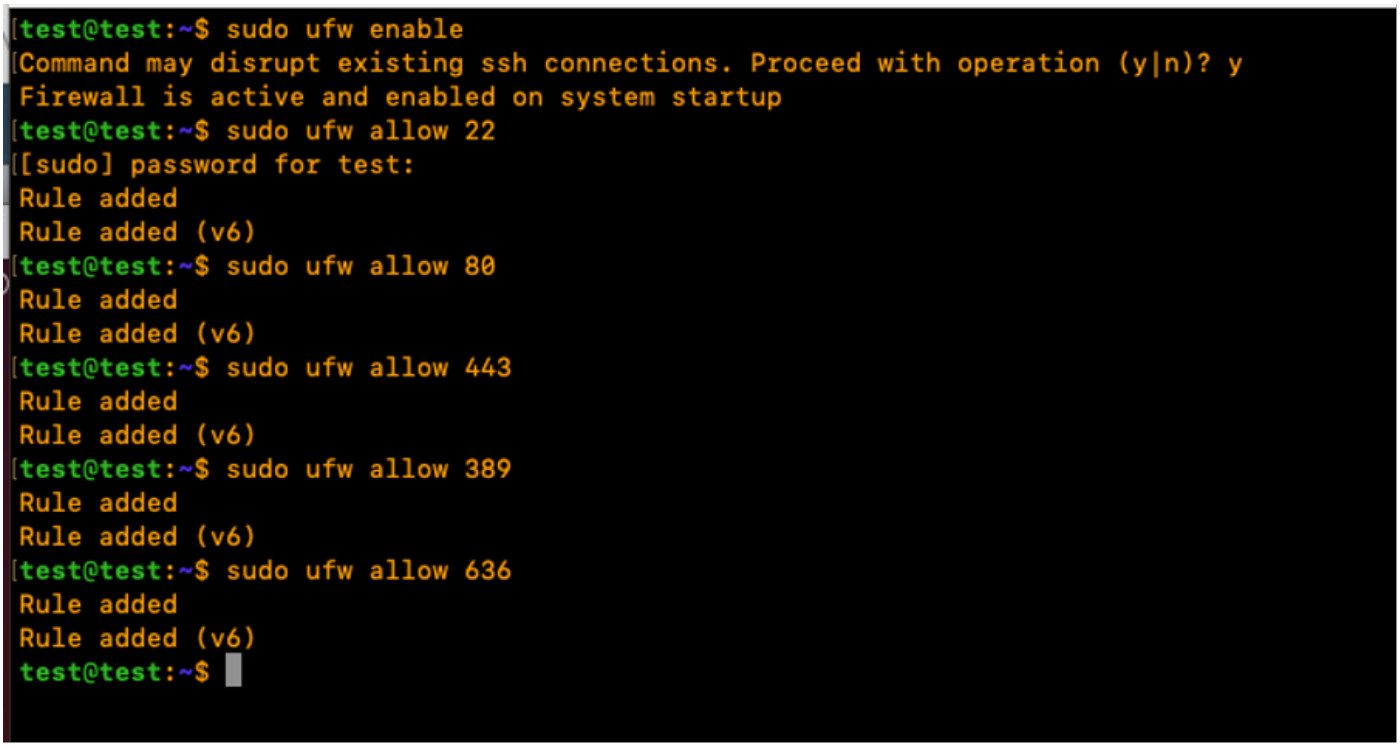


Configurare Ubuntu Firewall in modo da consentire le porte 80(Web), 443 (Web sicuro), 389(LDAP) e 636 (LDAP sicuro se richiesto)

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

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

```
sudo ufw allow 636
```



Verificare lo stato di Ubuntu Firewall:

```
sudo ufw status
```

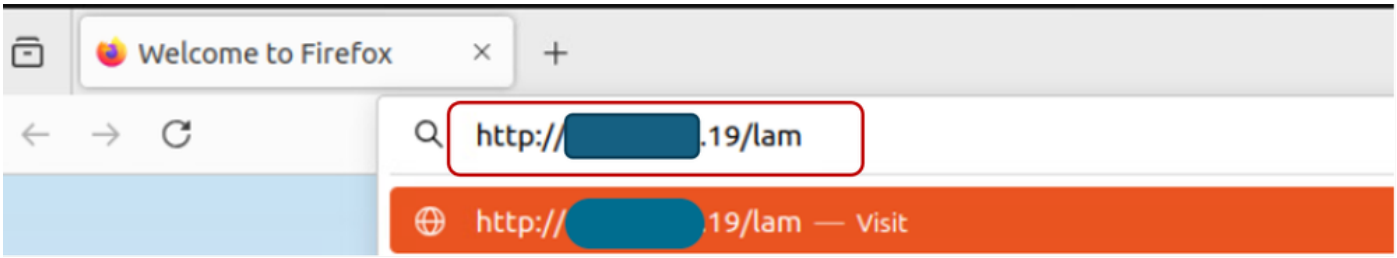
```
test@test:~$ sudo ufw status
Status: active

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)
```

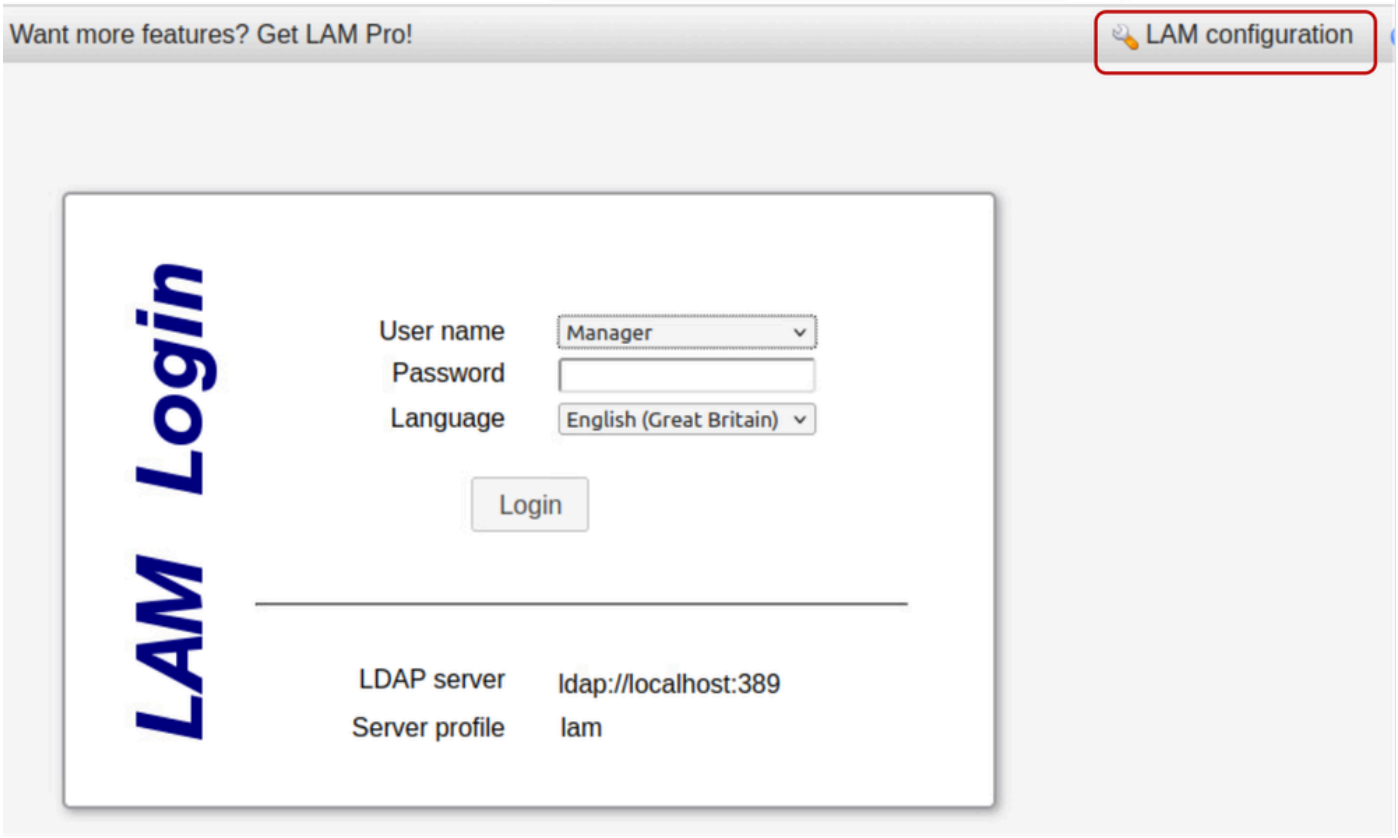
Passaggio 4: Configura Account Manager LDAP

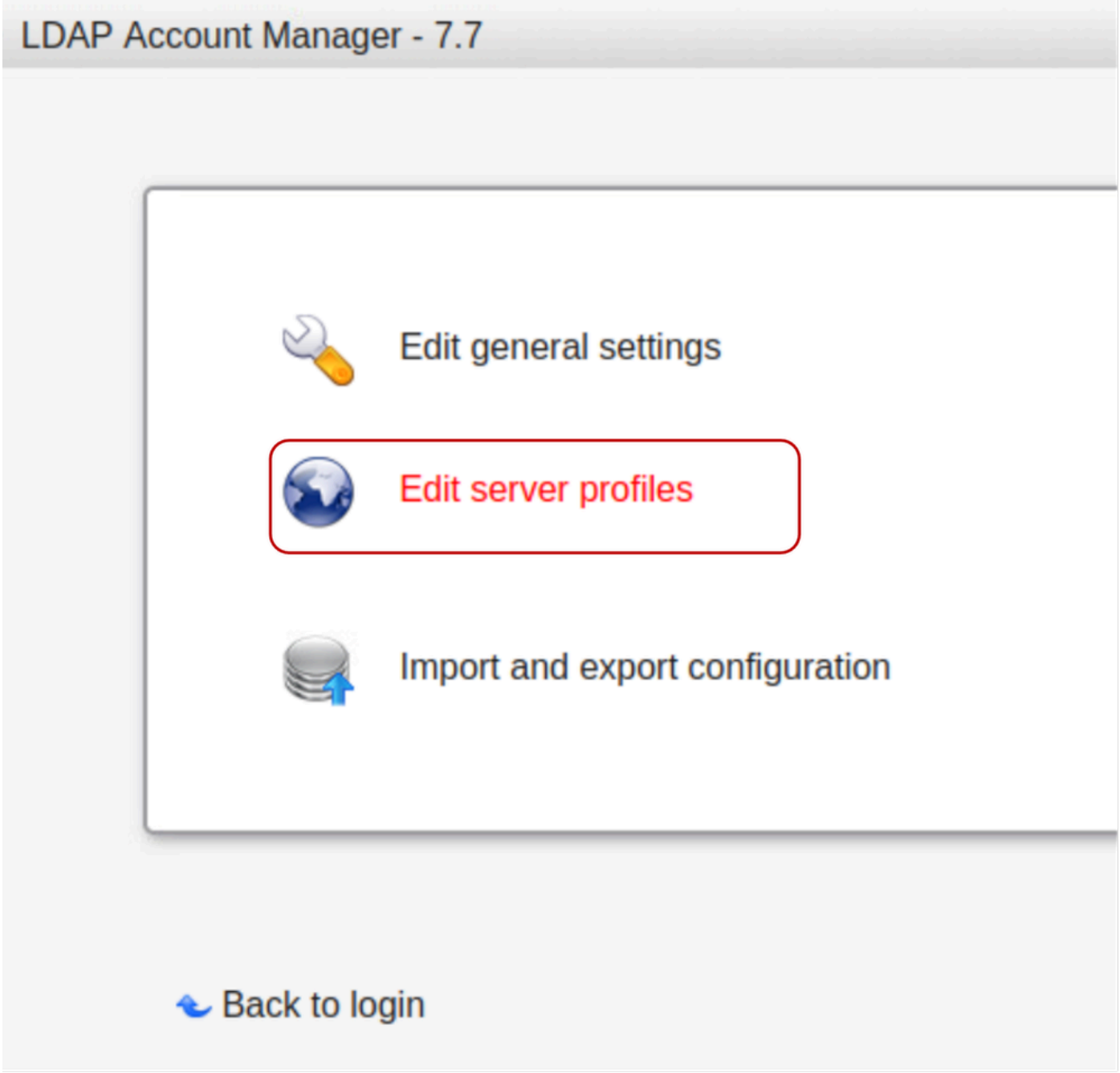
Per configurare LDAP Account Manager (LAM) dalla GUI, aprire un browser Web, immettere l'indirizzo IP del server Linux e aggiungervi il percorso 'lam' come mostrato:

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

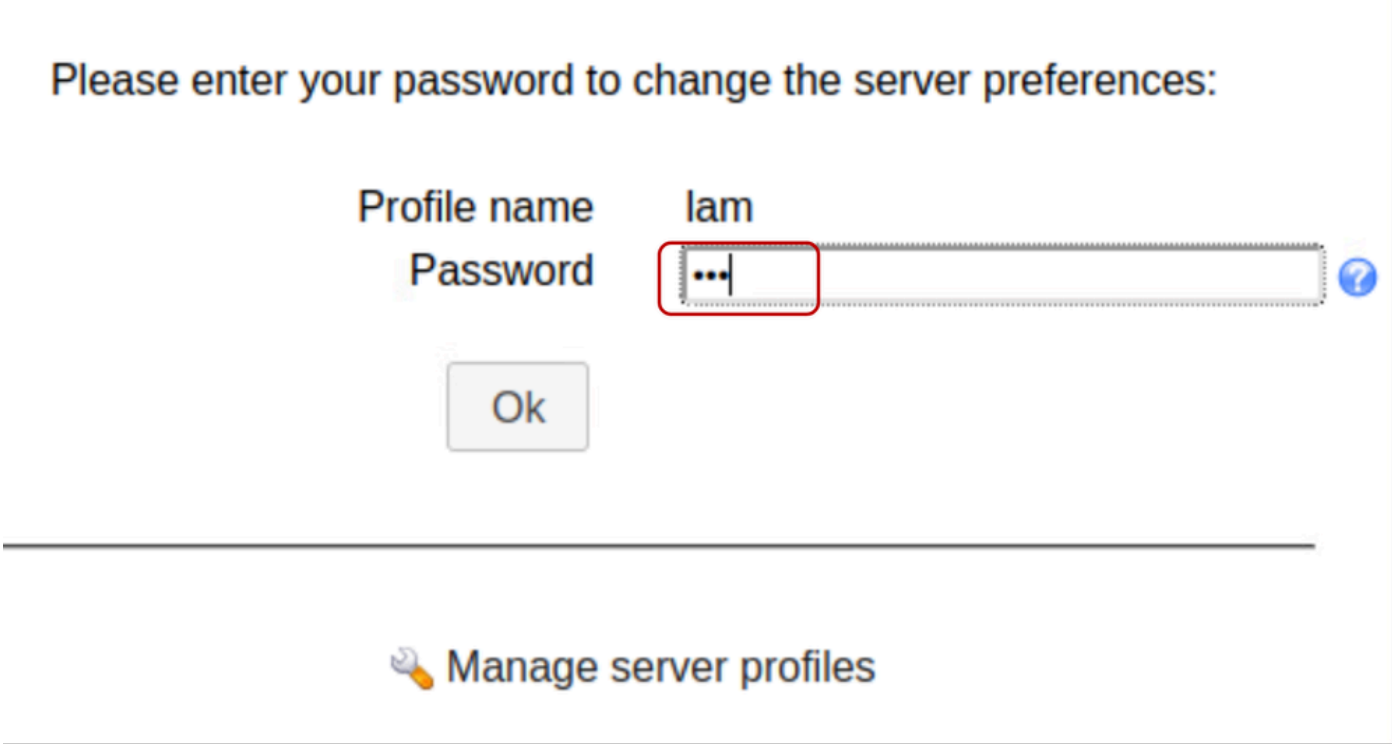


Fare clic su "Configurazione LAM", quindi selezionare "Modifica profili server".


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



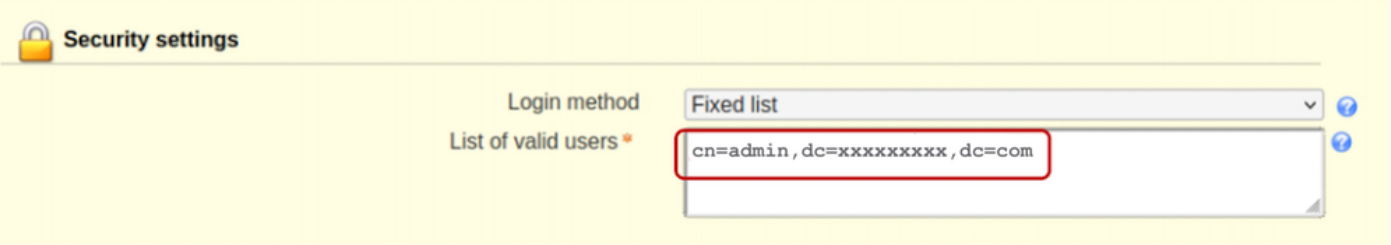
Digitare la password lam predefinita "lam" per eseguire l'accesso.



Nella scheda General Settings (Impostazioni generali), verificare le impostazioni Server, "Language" (Lingua) e "Timezone" (Fuso orario).

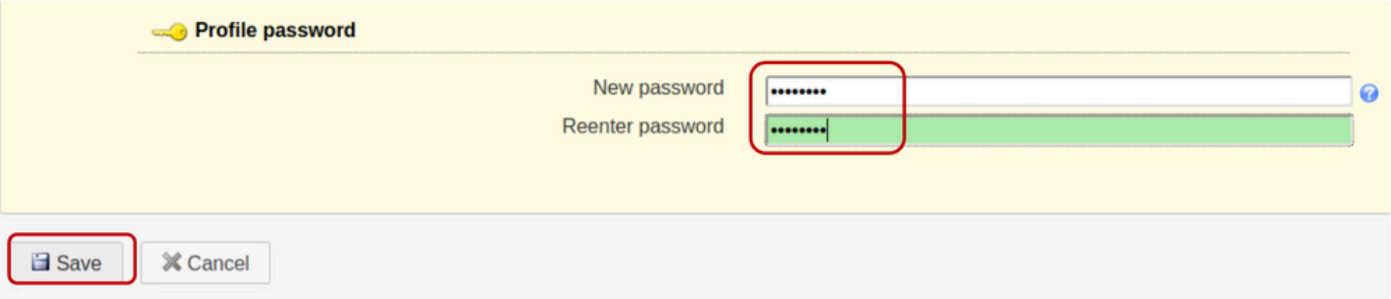
Nella sezione Impostazioni strumento, modificare e aggiungere il nome di dominio richiesto nel campo Suffisso struttura come mostrato di seguito:

Modificare la sezione Impostazioni protezione in modo da includere un utente "admin" utilizzato per gestire il servizio SLAPD.



Impostare una "Password profilo". Questa password viene utilizzata per i successivi accessi all'interfaccia di configurazione LAM. In questo esempio, viene configurato "cisco123" al posto della password predefinita "lam".

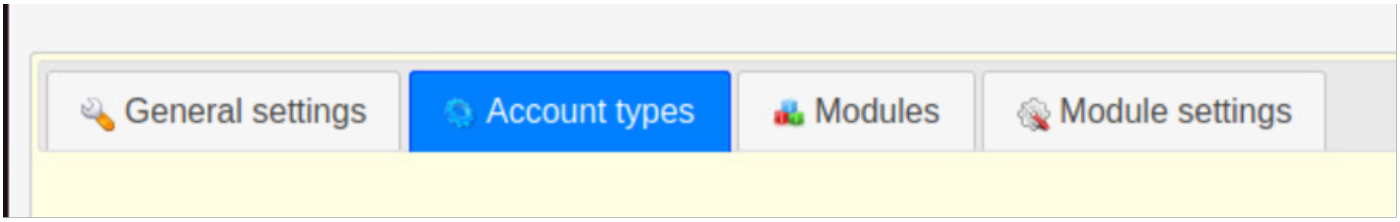
Salvare la configurazione:



La sessione viene quindi riavviata sull'interfaccia GUI di configurazione LAM.

Accedere nuovamente (configurazione LAM > Modifica profili server) utilizzando la nuova password creata.

Fare clic su "Account types" (Tipi di account),



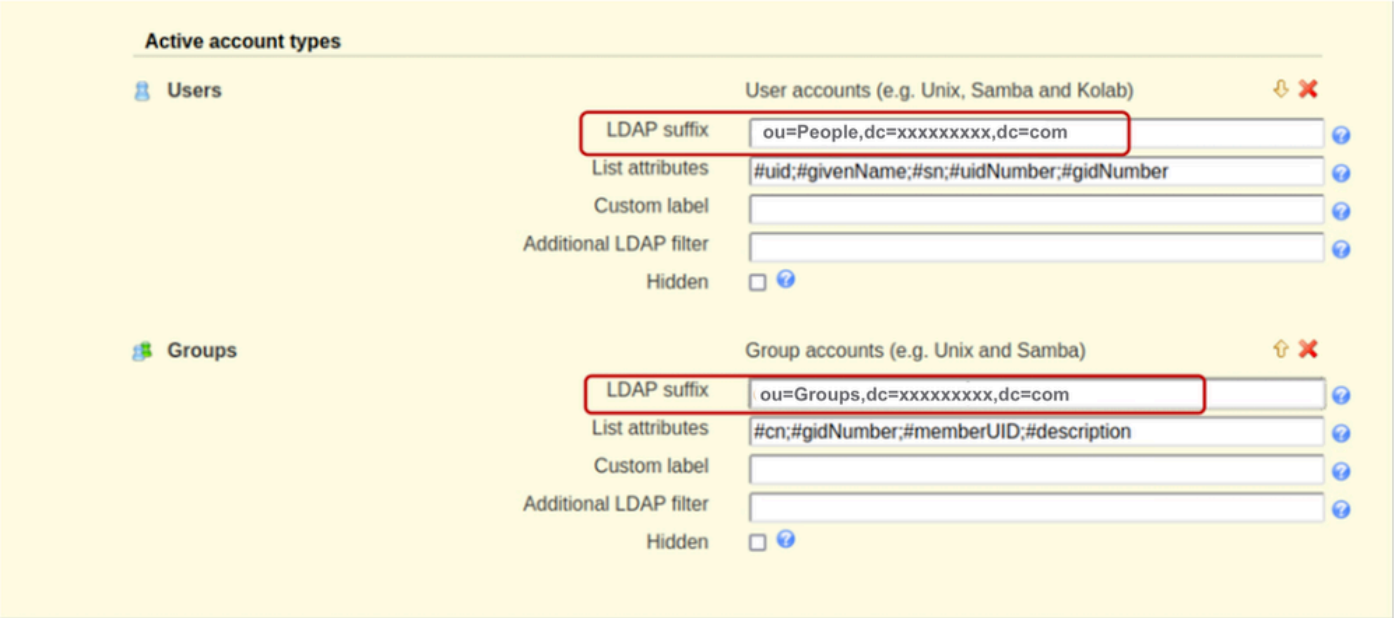
Scorrere verso il basso e modificare i tipi di account attivi predefiniti con le informazioni sul nome di dominio nel campo Suffisso LDAP. Ad esempio, il contenuto predefinito del campo "Suffisso LDAP" visualizza il valore "ou=People,dc=my-domain,dc=com".

Se è necessario creare nuove unità organizzative, sostituire il contenuto del campo "Suffisso LDAP" con il nome dell'unità organizzativa.

Il formato visualizzato è "ou=<unità_organizzativa>,dc=xxxxxxxxx,dc=com".

Per questa dimostrazione, l'OU per gli utenti è "Persone" e l'OU per i gruppi è "Gruppi".

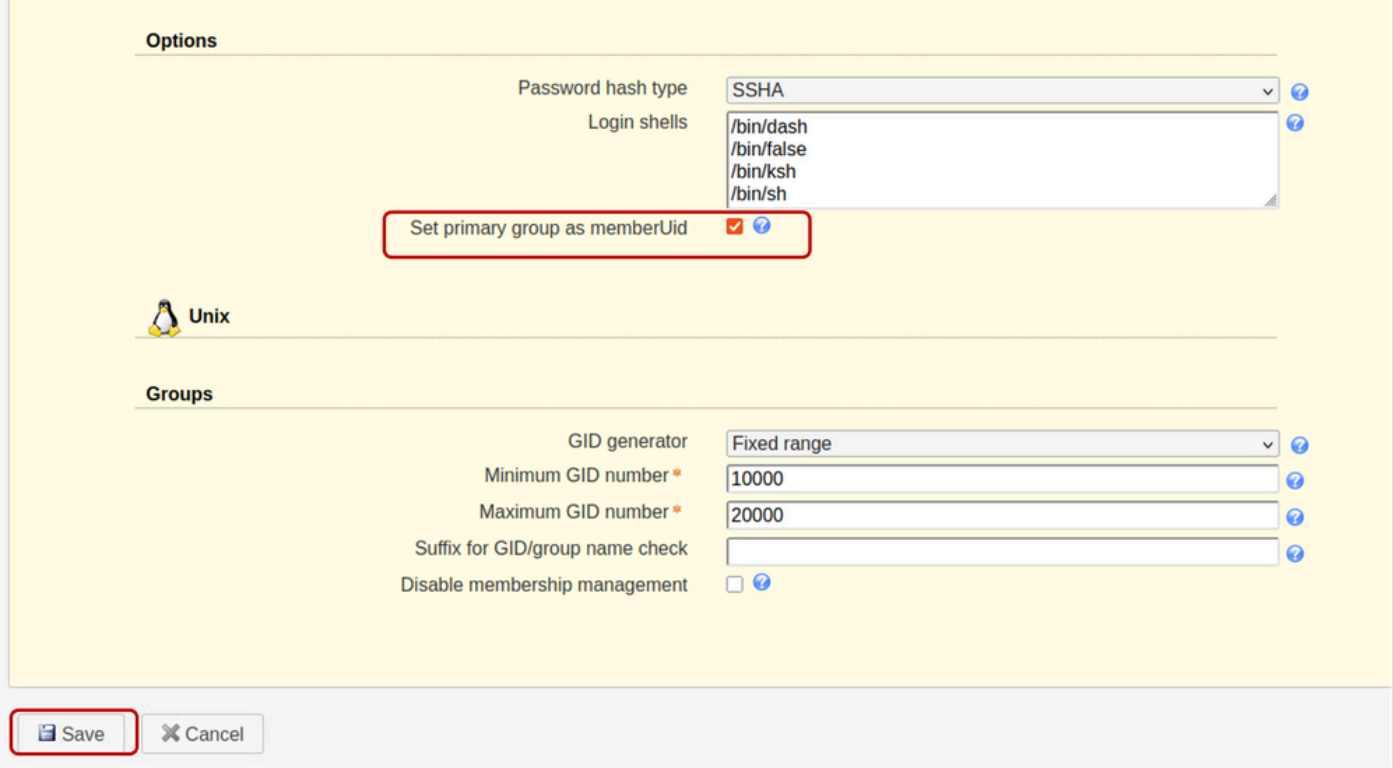
Salvare la configurazione.



Scorrere verso il basso fino alla sezione Options (Opzioni) e assicurarsi di selezionare "Set primary group as memberUid" (Imposta gruppo primario come memberUid).

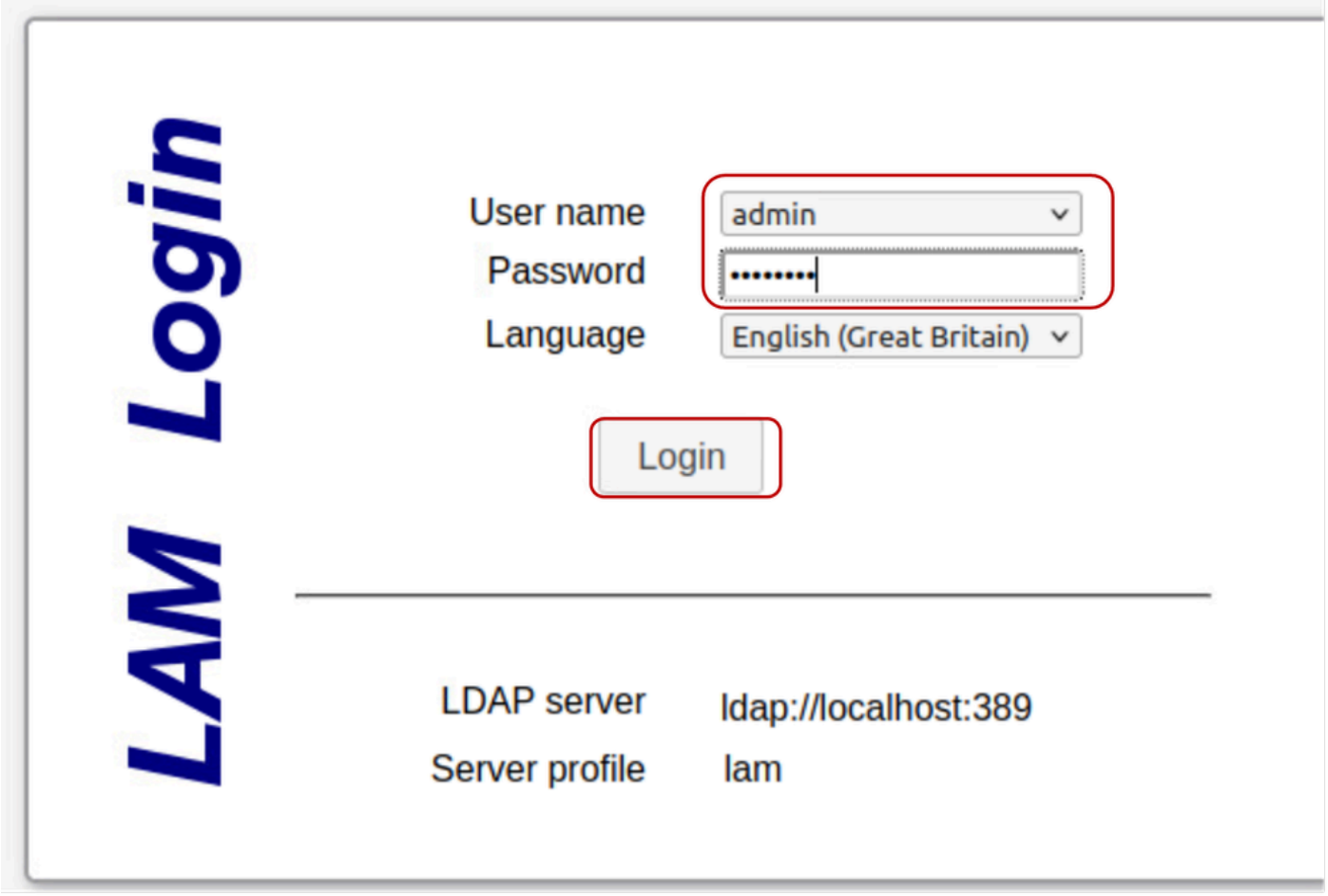
Per impostazione predefinita, l'opzione "Imposta il gruppo primario come memberUid" non è impostata sugli oggetti gruppo. L'attivazione di questa opzione consente l'uso di OpenLDAP "Gruppo primario" come un gruppo LDAP standard, dove è possibile fare riferimento a "memberUid" (ad esempio: nella configurazione del server UCS serie C). Se questa opzione è deselezionata, l'accesso per gli utenti che appartengono a un gruppo primario non riesce.

Salvare la configurazione.

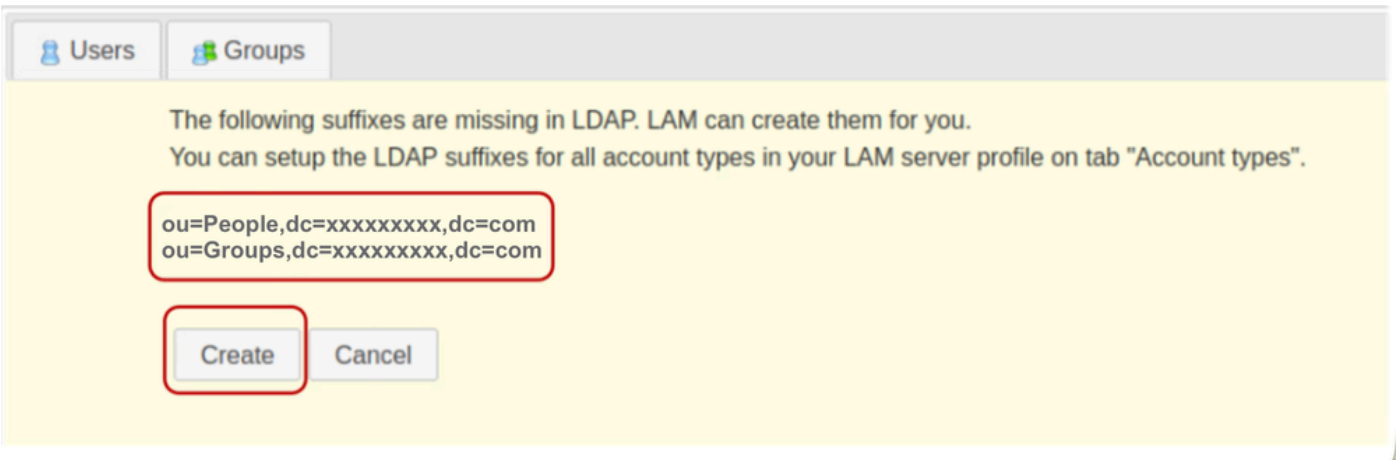


Passaggio 5: Creazione di unità organizzative, gruppi e utenti

Accedere a LAM come utente "admin" con la stessa password creata durante l'installazione, per creare utenti e gruppi appartenenti alle unità organizzative create in precedenza (Persone e Gruppi) rispettivamente:

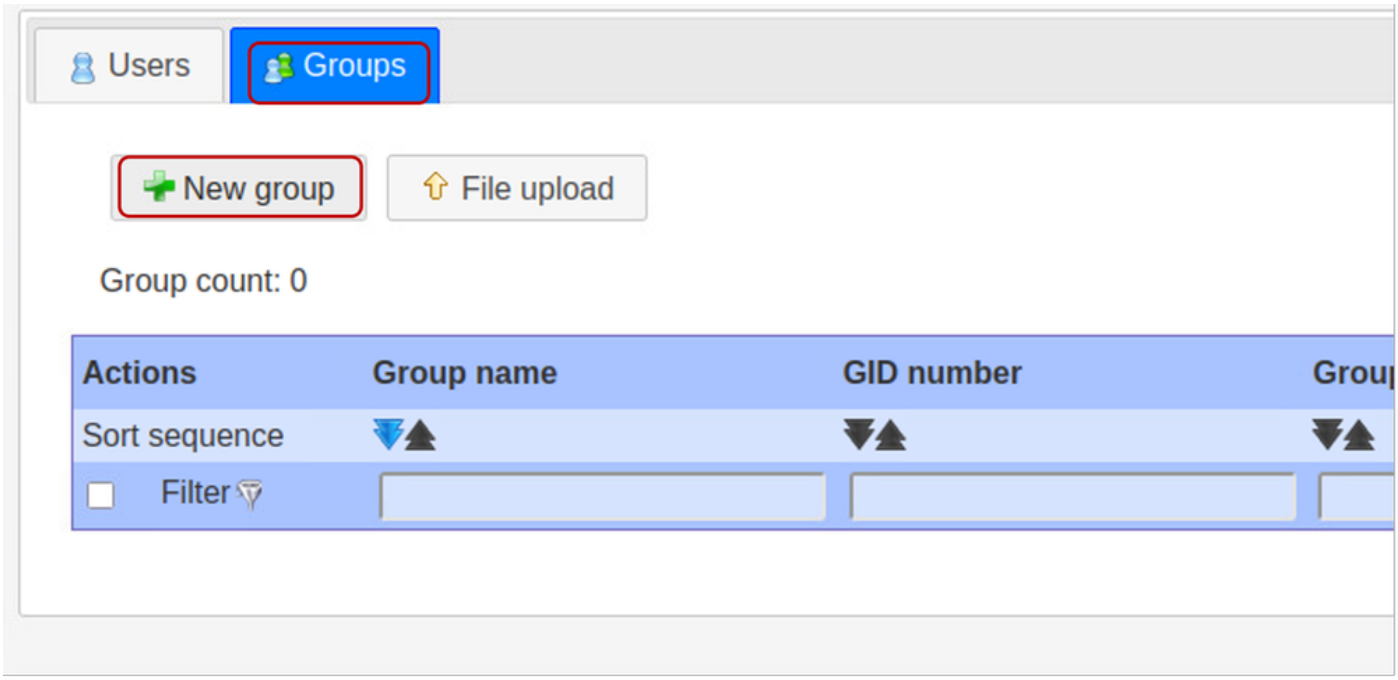


Creare le unità organizzative specificate in precedenza nella sezione Configurazione LAM.
Fare clic su Crea.



Quindi, in Gestione account LDAP, creare il gruppo "it":

Selezionare la scheda Gruppi e fare clic su Nuovo gruppo

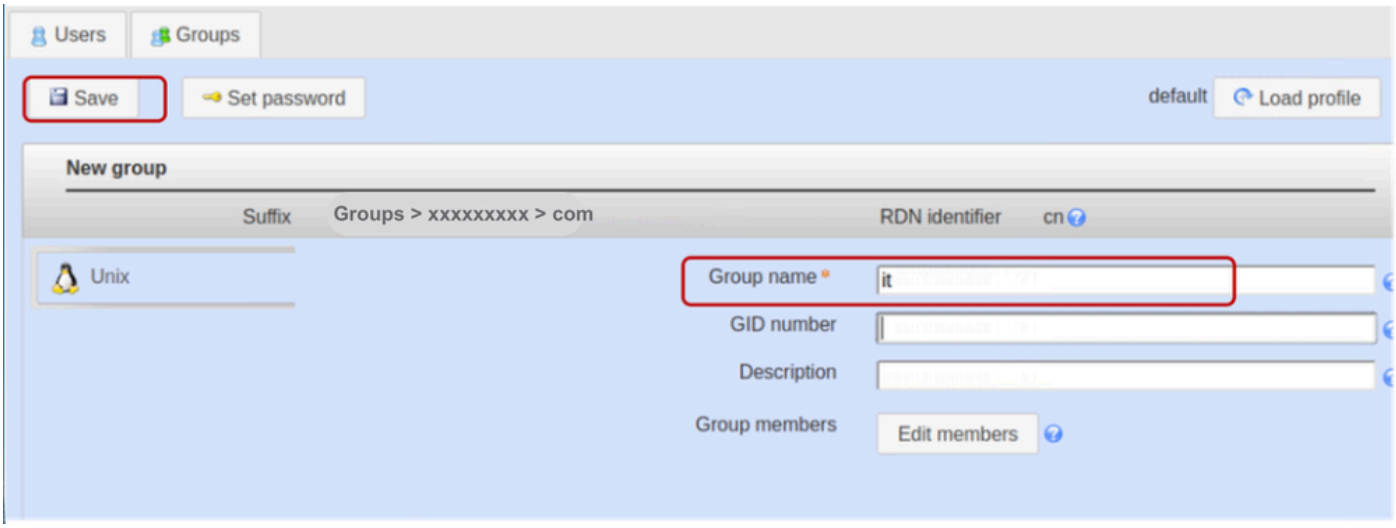


Impostare il nome del gruppo su "it".

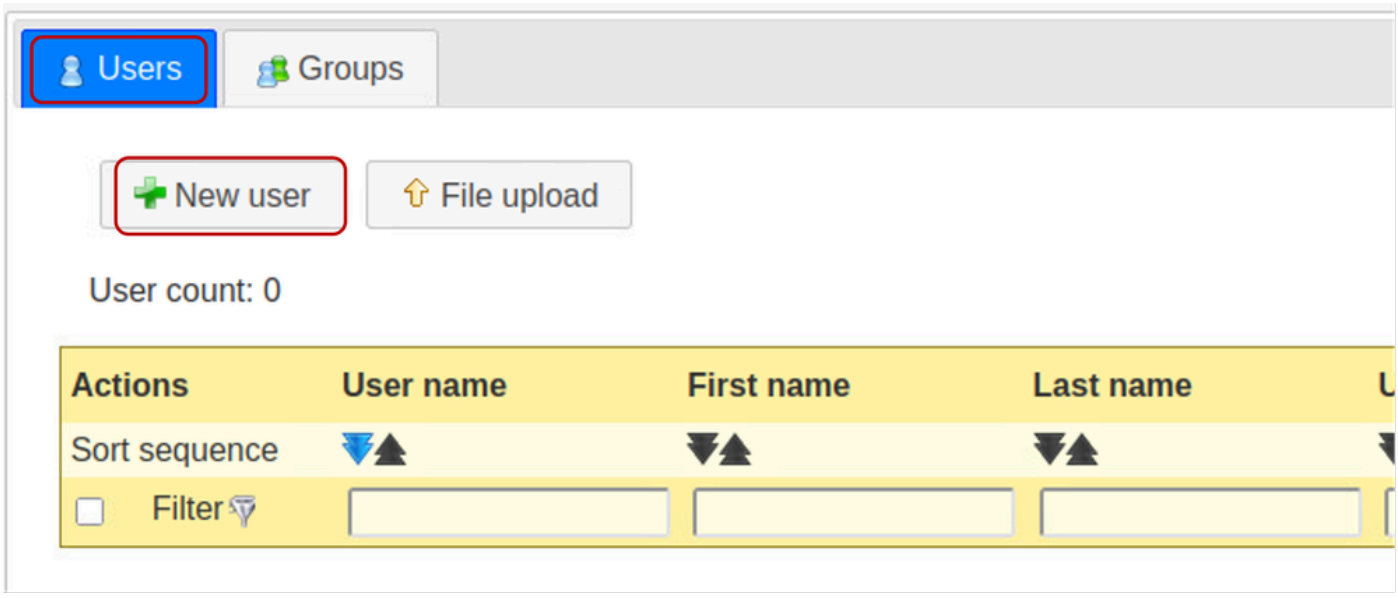
Nota: Mentre i sistemi Cisco UCS sono generalmente resistenti alle variazioni dei casi, il mantenimento delle convenzioni di denominazione minuscole è una procedura ottimale per garantire l'interoperabilità a lungo termine tra diversi ambienti di infrastrutture server LDAP.

Lasciare vuoto il campo Numero GID. Gestione account LDAP (LAM) è progettato per popolare automaticamente questo campo con il successivo valore disponibile.

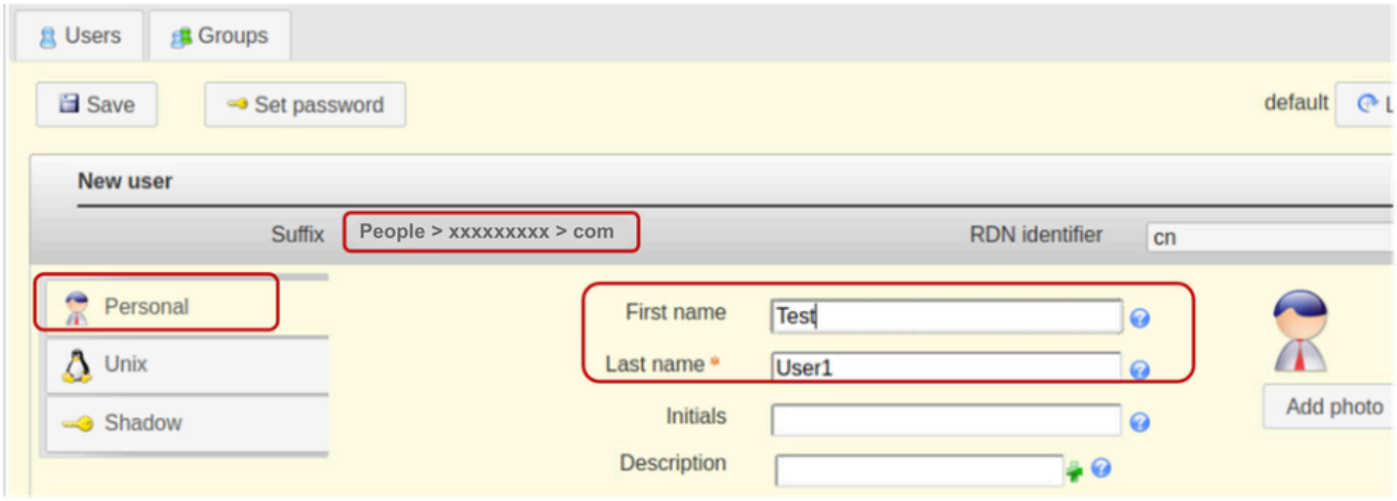
Fornire una descrizione, se desiderato, e fare clic su Salva



Fare clic sulla scheda "Utenti" per creare gli account utente e selezionare "Nuovo utente".



Compilare i campi obbligatori per l'utente "testuser1" nella scheda Personale.

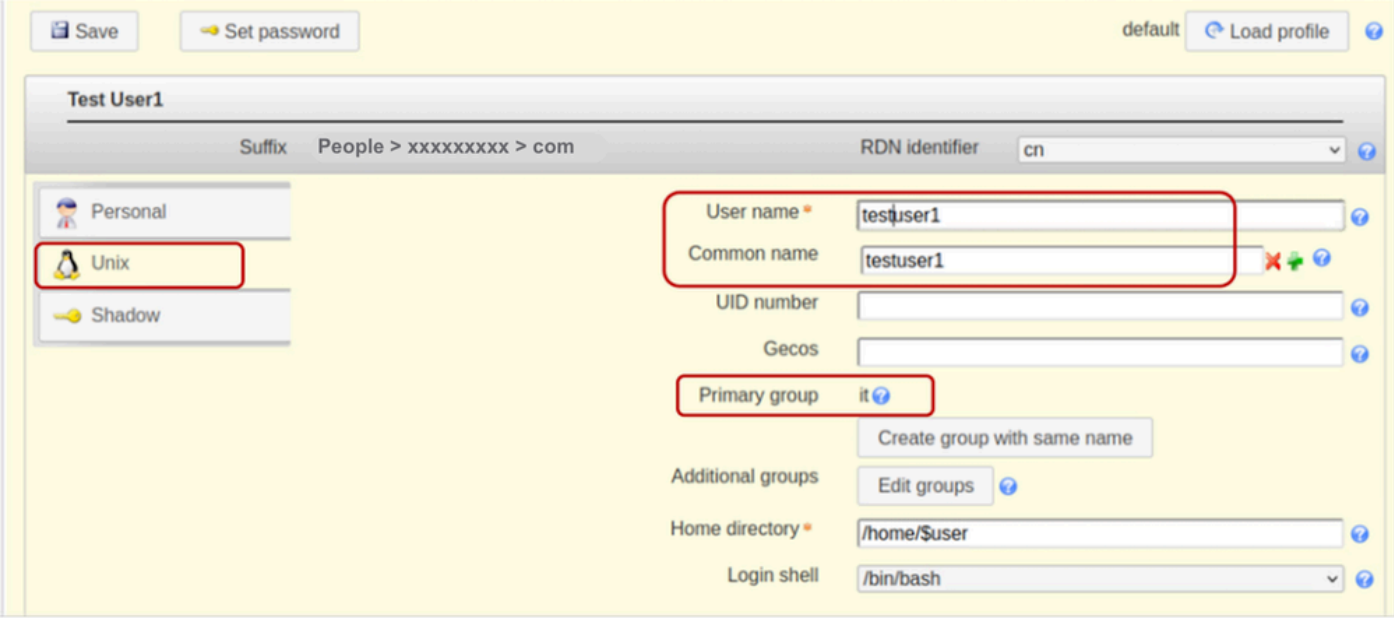


Selezionare la scheda Unix e aggiungere testuser1 nel campo Nome utente. Includi utente nel gruppo "it".

Per questa dimostrazione, esiste solo il gruppo "it" ed è già precompilato.

Mantenere l'identificatore RDN come "Nome comune" (cn). In questo modo il sistema può compilare automaticamente il campo "Nome comune" utilizzando il valore specificato nel campo "Nome utente".

Lasciare vuoto il campo Numero UID in quanto LAM compila automaticamente il campo con i valori disponibili.



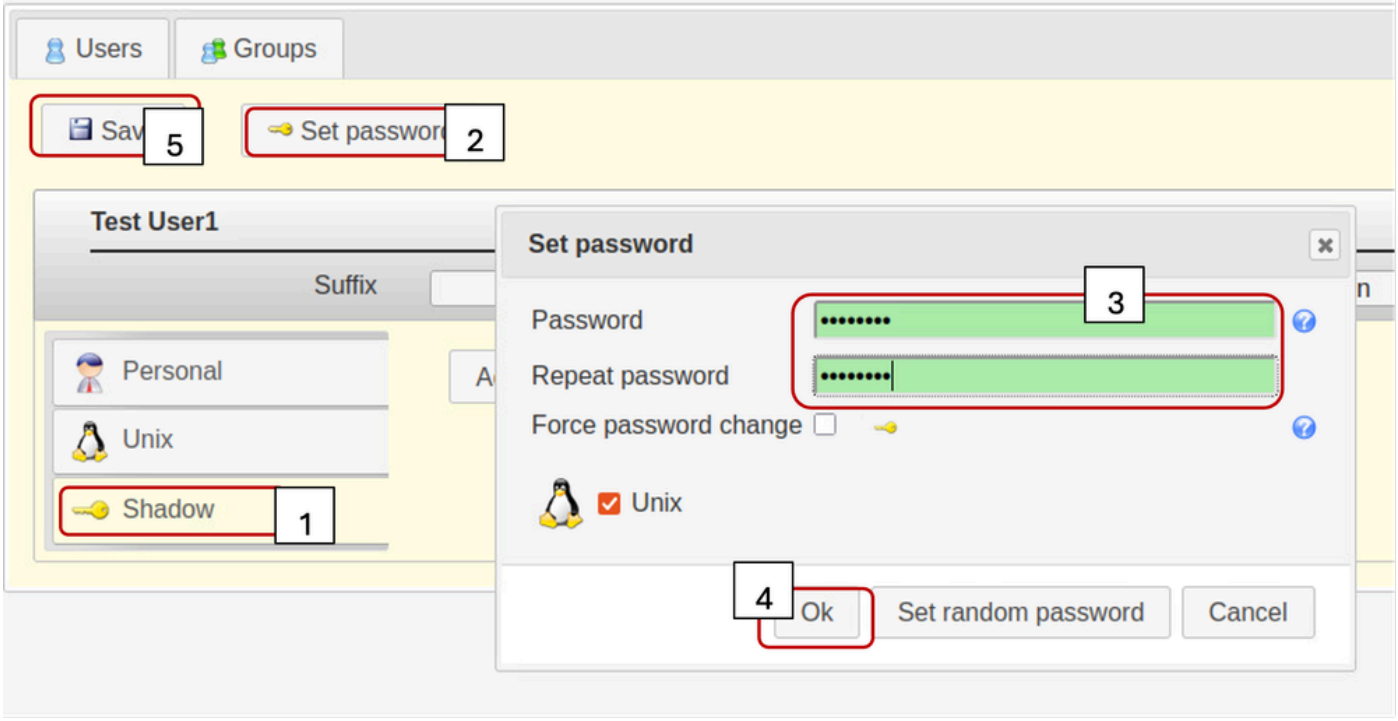
Selezionare la scheda Ombreggiatura,

L'estensione dell'account shadow non è utilizzata.

Fare clic su "Set Password".

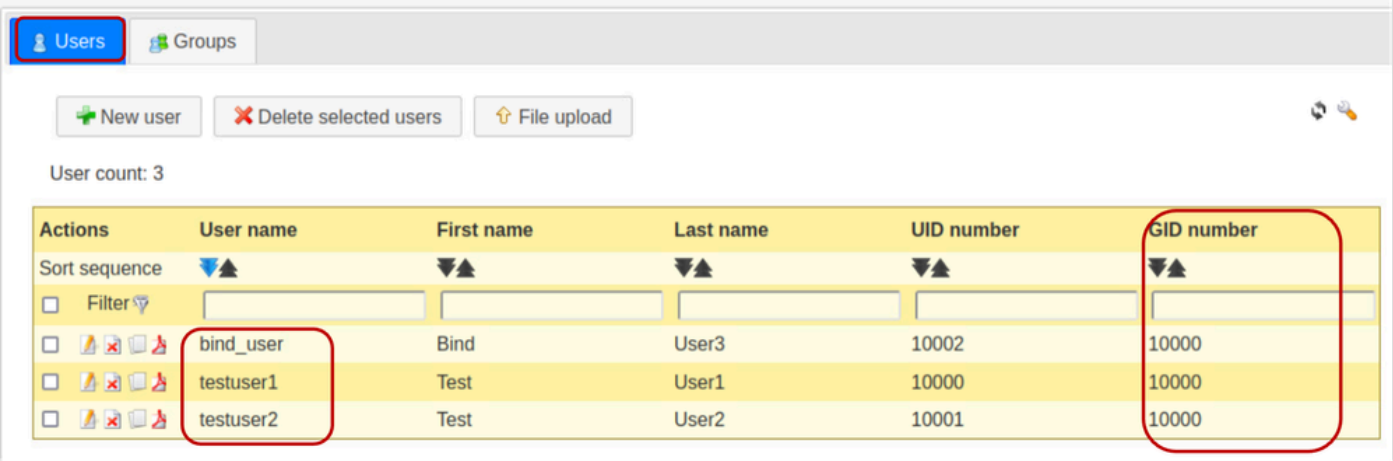
Impostazione della password utente

Fare clic su OK e su Salva



Ripetere i passaggi specificati descritti in precedenza per creare l'account utente "testuser2" e l'account "bind_user".

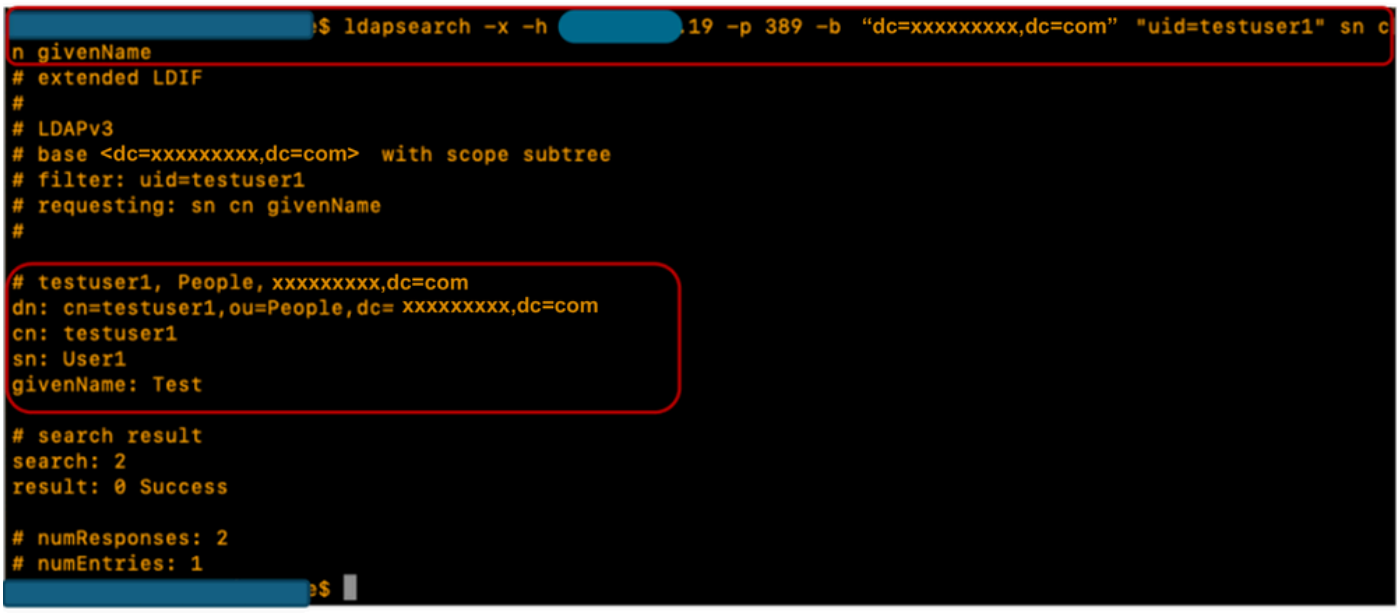
Fare clic sulla scheda "Utenti" per verificare la creazione di tutti gli utenti desiderati. (se nella colonna gidNumber è presente lo stesso valore, significa che gli utenti creati appartengono allo stesso gruppo - questo)



Passo 6: verifica dell'accesso LDAP locale

Accedere a un altro sistema basato su Linux, in modo da poter raggiungere il server OpenLDAP. Eseguire il comando ldapsearch specificato per verificare che LDAP funzioni:

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



Parametri di configurazione su CIMC

Accedere a CIMC.

Nel riquadro di navigazione, selezionare Amministrazione, Gestione utente e LDAP.

Inserire i parametri di configurazione LDAP come indicato di seguito:

- Abilita LDAP: selezionata
- DN di base: dc=xxxxxxxxx,dc=com

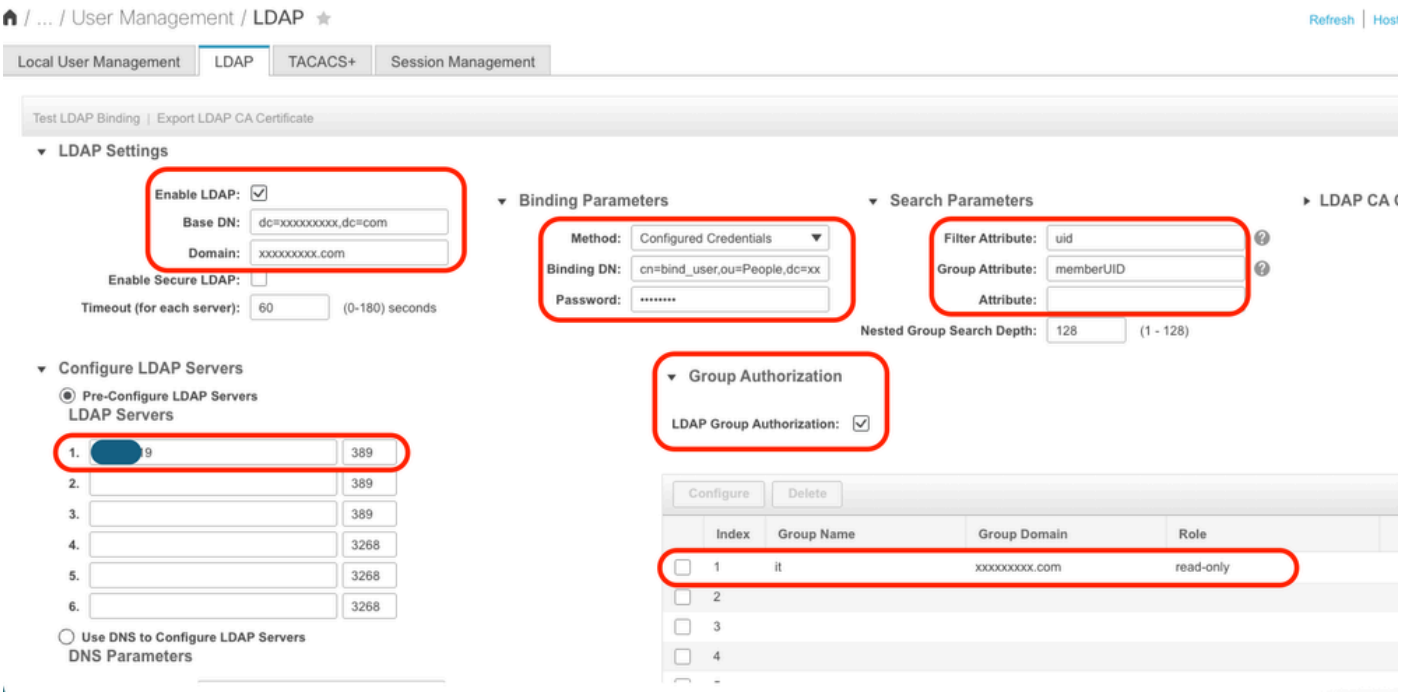
- Dominio: xxxxxxxxx.com

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

- Parametri di associazione: "Credenziali di accesso" o "Credenziali configurate"
    - Quando si utilizzano le credenziali configurate, aggiungere il DN bind_user esattamente come configurato sul server LDAP:
        - Esempio: cn=bind_user,ou=Persone,dc=xxxxxxx,dc=com

- Parametri di ricerca:
    - Attributo filtro: "cn" o "uid"
    - Attributo gruppo: memberUID

- Autorizzazione gruppo LDAP - Selezionata
    - Nome gruppo: it
    - Dominio gruppo: xxxxxxxxx.com
    - Ruolo: di sola lettura (qualsiasi ruolo desiderato)



Salvare la configurazione e verificare l'accesso utente LDAP.

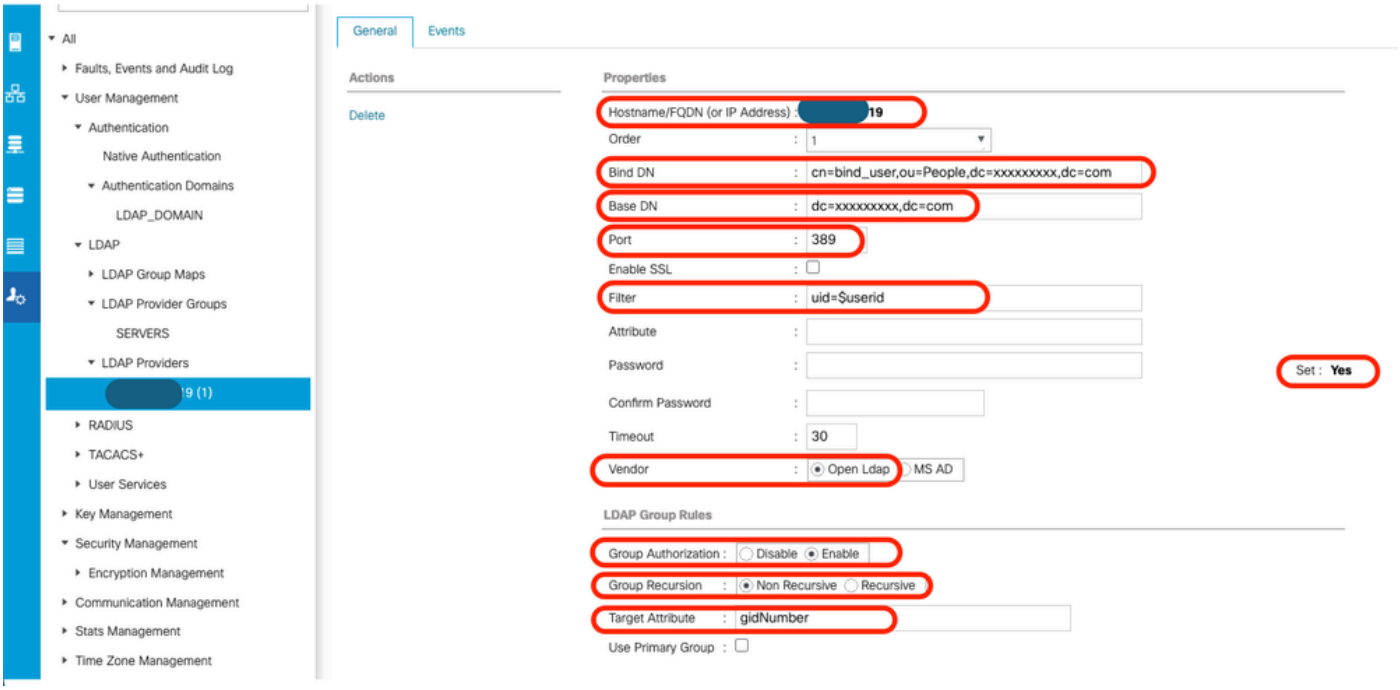
Parametri di configurazione in UCS Manager

Accedere a UCS Manager.

Nel riquadro di navigazione, selezionare Amministrazione, Gestione utente e LDAP.

Inserire i parametri di configurazione LDAP come indicato di seguito:

- Provider LDAP:
  - Nome host: <FQDN o indirizzo IP del server LDAP>
  - DN binding: cn=bind_user,ou=Persone,dc=xxxxxxx,dc=com
  - DN di base: dc=xxxxxxxxx,dc=com
  - Port: 389
  - Abilita SSL: Disabled
  - Filtro: uid=$userid
  - Autorizzazione gruppo: Attivato
  - Ricorsione gruppo: Non ricorsivo
  - Attributo di destinazione: numerogid
- Mapping gruppi LDAP:
  - DN gruppo LDAP: 10000 <gidNumber per il gruppo "it">

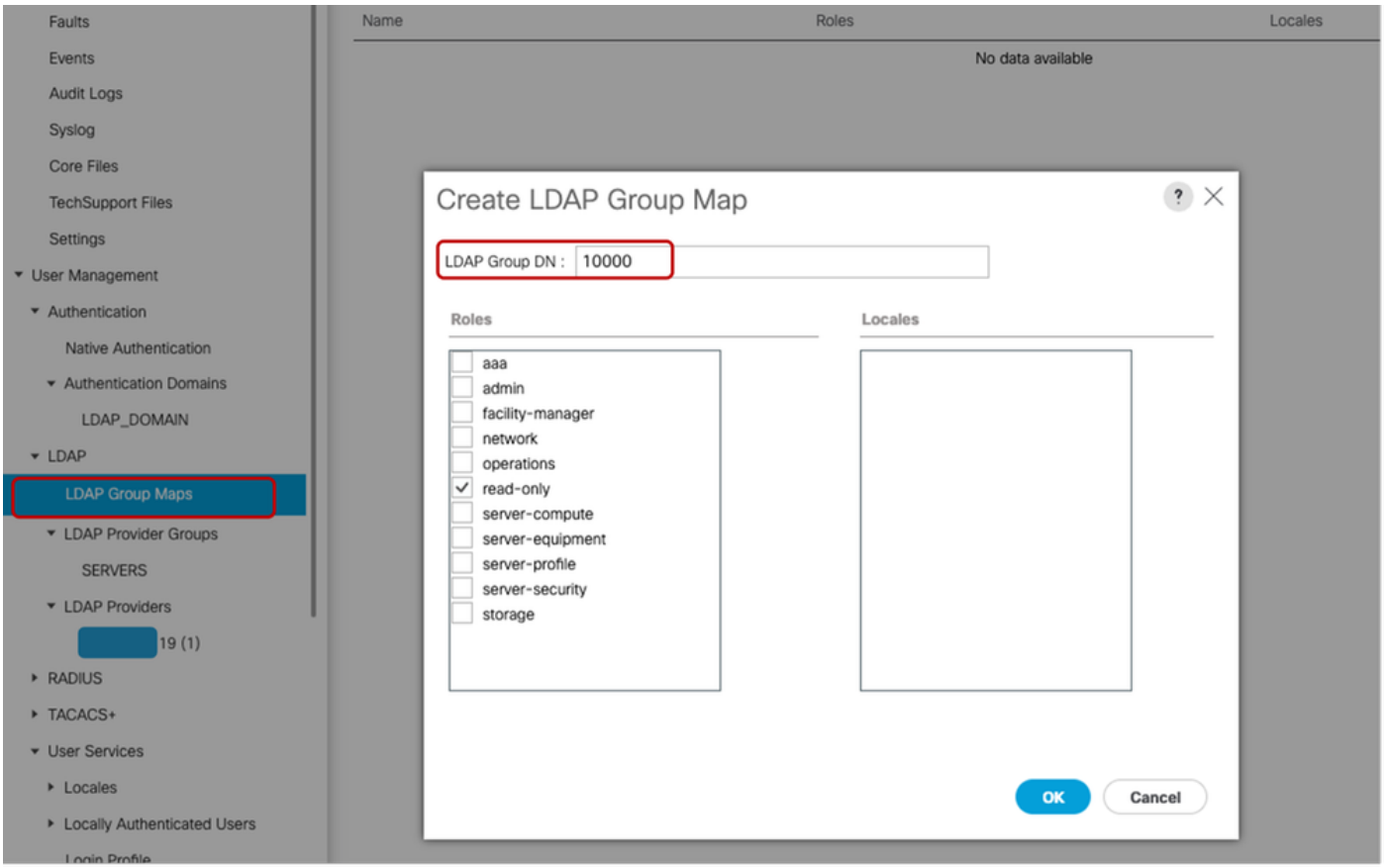


In Tutte >> Gestione utente >> LDAP >> Provider LDAP >> Regole gruppo LDAP, l'attributo di destinazione predefinito per UCS Manager è "memberOf". Per impostazione predefinita, nei server OpenLDAP tale attributo non è abilitato, pertanto l'impostazione del valore Attributo di destinazione su "memberOf" (o l'assenza di tale valore) impedisce il corretto accesso dell'utente, in quanto il server OpenLDAP non riconosce il valore Attributo richiesto.

In questo esempio, il valore "Target Attribute" (Attributo destinazione) è stato impostato su "gidNumber".

Aggiungere il provider LDAP configurato a un gruppo di provider LDAP. Per questa dimostrazione, è stato creato il gruppo di provider LDAP "SERVER".

Quando si configura "Mappe gruppo LDAP" in "All >> User Management >> LDAP >> LDAP Group Maps>>", il valore gidNumber (in questo caso "10000") viene utilizzato come "Mappa DN gruppo" come mostrato di seguito:



Configurare un dominio di autenticazione LDAP (LDAP_DOMAIN) in "All >> User Management >> Authentication >> Authentication Domains" facendo riferimento ai gruppi di provider LDAP e verificare l'accesso utente LDAP.

Nota: Se l'attributo memberOf è necessario per soddisfare requisiti ambientali specifici o per implementare la funzione "Group Recursion", si consiglia di utilizzare la seconda opzione di configurazione riportata di seguito, che richiede l'abilitazione di LDAP con estensioni di overlay.

Sebbene LDAP Account Manager (LAM) supporti la configurazione di sovrapposizione, si tenga presente che questa funzionalità richiede una licenza appropriata.

Per ulteriori informazioni sulla configurazione di LDAP mediante LAM, consultare la documentazione ufficiale di LDAP Account Manager.

Opzione 2: Configurazione di OpenLDAP mediante gli strumenti e le sovrapposizioni della CLI di Ubuntu

Per utilizzare OpenLDAP per l'autenticazione di UCS Manager, sono necessarie due sovrapposizioni che assicurino che i gruppi siano associati agli utenti in modo comprensibile per il

sistema UCS (UCS Manager e CIMC).

La configurazione sul lato OpenLDAP richiede:

- sovrapposizione "memberof": Questa sovrapposizione crea un mapping tra utenti e gruppi in modo che se viene eseguita una query su un DN utente, l'attributo memberOf può essere richiesto come parte della query. Per impostazione predefinita, nessun attributo per gli utenti per l'appartenenza ai gruppi a meno che il membro di overlay non venga aggiunto a openLDAP
- sovrapposizione "affinamento": Questa sovrapposizione è configurata per convalidare che le voci nell'attributo member negli oggetti group rimangano sincronizzate con l'attributo memberOf degli oggetti utente. Senza questo servizio, se un utente viene eliminato senza modificare anche il gruppo, i DN orfani possono rimanere nell'oggetto gruppo. Il servizio di ottimizzazione garantisce la coerenza in entrambe le direzioni.

Passaggio 1: Strumenti di rete iniziali e configurazione del nome host del server Linux

Ripetere il passaggio 1 nell'opzione 1.

Passaggio 2: Installare SLAPD

Ripetere il punto 2 all'interno dell'opzione 1 (ad eccezione dell'installazione di PHP e Apache come opzione 2 non richiede che funzionino - nessun LAM).

Verificare che le porte richieste possano passare attraverso il firewall Ubuntu.

Passaggio 3: Installa sovrapposizione 'memberOf' sul server LDAP

Verificare se la sovrapposizione "memberOf" è installata

```
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
```

Per installare la sovrapposizione "memberOf", creare un file con estensione ldif denominato ldap.memberof.load.ldif (utilizzare qualsiasi convenzione di denominazione desiderata) e aggiungere la configurazione specificata:

```
cat <


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

Aggiungere la configurazione nel file ldap.memberof.load.ldif al profilo LDAP utilizzando il comando specificato:

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

Configura il modulo memberOf e la voce olcDatabase in modo che soddisfino i requisiti di distribuzione, a seconda delle distribuzioni Linux.

Due valori di attributo obbligatori sono "olcDatabase={1}mdb" e "groupOfNames", come illustrato di seguito.

Creare il file ldap.memberof.config.ldif, popolare i relativi attributi e importarne il contenuto nel profilo 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
```

Passaggio 4: Installa 'affinamento' sovrimpressione sul server LDAP

Quindi, Installare il restringimento a openldap:

creare un file con estensione ldif denominato ldap.rafft.load.ldif (utilizzare qualsiasi convenzione di denominazione desiderata) e aggiungere la configurazione specificata:

```
cat <

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

Importare la configurazione nel file ldap.rafft.load.ldif nel profilo LDAP utilizzando il comando specificato:

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

Configurare la funzionalità affinamento ricerca, che mantiene l'integrità referenziale tra gruppi e utenti.

Configura il modulo Refint e la relativa voce olcDatabase in modo che soddisfino i requisiti di distribuzione.

Creare il file ldap.rafft.config.ldif e importarne il contenuto nel profilo LDAP.

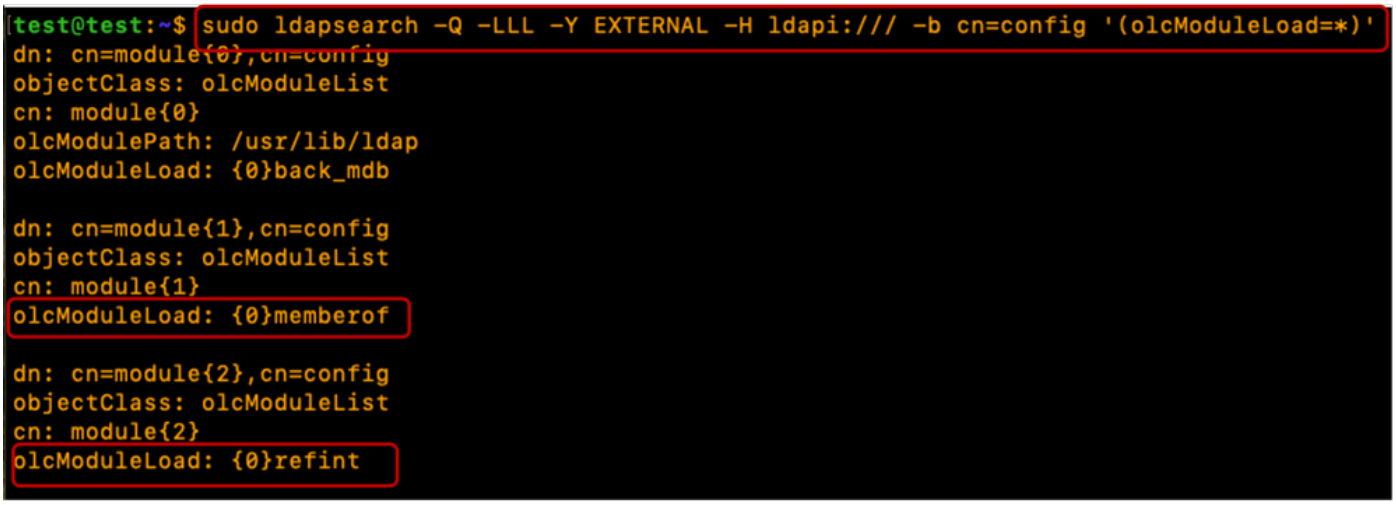
```
cat <


      ./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
```

Dopo l'installazione di entrambi i plug-in/estensioni, l'output del comando ldapsearch specificato è simile all'output mostrato di seguito:

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



Quando sono configurati entrambi i plug-in/estensioni, l'output del comando ldapsearch specificato è simile all'output mostrato:

```
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
```

Riavviare il servizio slapd per i plug-in/moduli appena installati per renderli utilizzabili:

```
sudo systemctl restart slapd
```

Passaggio 5: Creazione di unità organizzative, utenti e gruppi

Creare unità organizzative (per utenti e gruppi), utenti e gruppi.

Creare le unità organizzative Utenti (Utenti) e Gruppi (Gruppi) e importarle nel profilo LDAP. È necessaria la password dell'account "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
```

Creare gli utenti (testuser1, testuser2 e bind_user), mapparli alle rispettive unità organizzative (Persone), aggiungerli ai relativi gruppi utilizzando gidNumbers (procedura consigliata) e importare gli utenti nel profilo 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:~$
```

Creare i gruppi (it), eseguirne il mapping alle rispettive unità organizzative (Gruppi), associare i membri del gruppo (testuser1, testuser2) e importarli nel profilo 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: Anche se l'attributo memberOf non è definito in modo esplicito durante la creazione di Utenti o Gruppi, il sistema genera e mantiene automaticamente questo riferimento. Una volta che l'utente è associato a un gruppo, l'attributo memberOf riflette automaticamente queste appartenenze, garantendo che la directory rimanga sincronizzata con la struttura di accesso corrente.

Passo 6: verifica dell'accesso LDAP locale

Verificare l'accesso dell'utente al server LDAP utilizzando il comando specificato (sostituire i parametri di accesso in base all'ambiente):

```
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:~$
```

Parametri di configurazione su CIMC

Accedere a CIMC.

Nel riquadro di navigazione, selezionare Amministrazione, Gestione utente e LDAP.

Inserire i parametri di configurazione LDAP come indicato di seguito:

- Abilita LDAP: selezionata
- DN di base: dc=xxxxxxxxx,dc=com

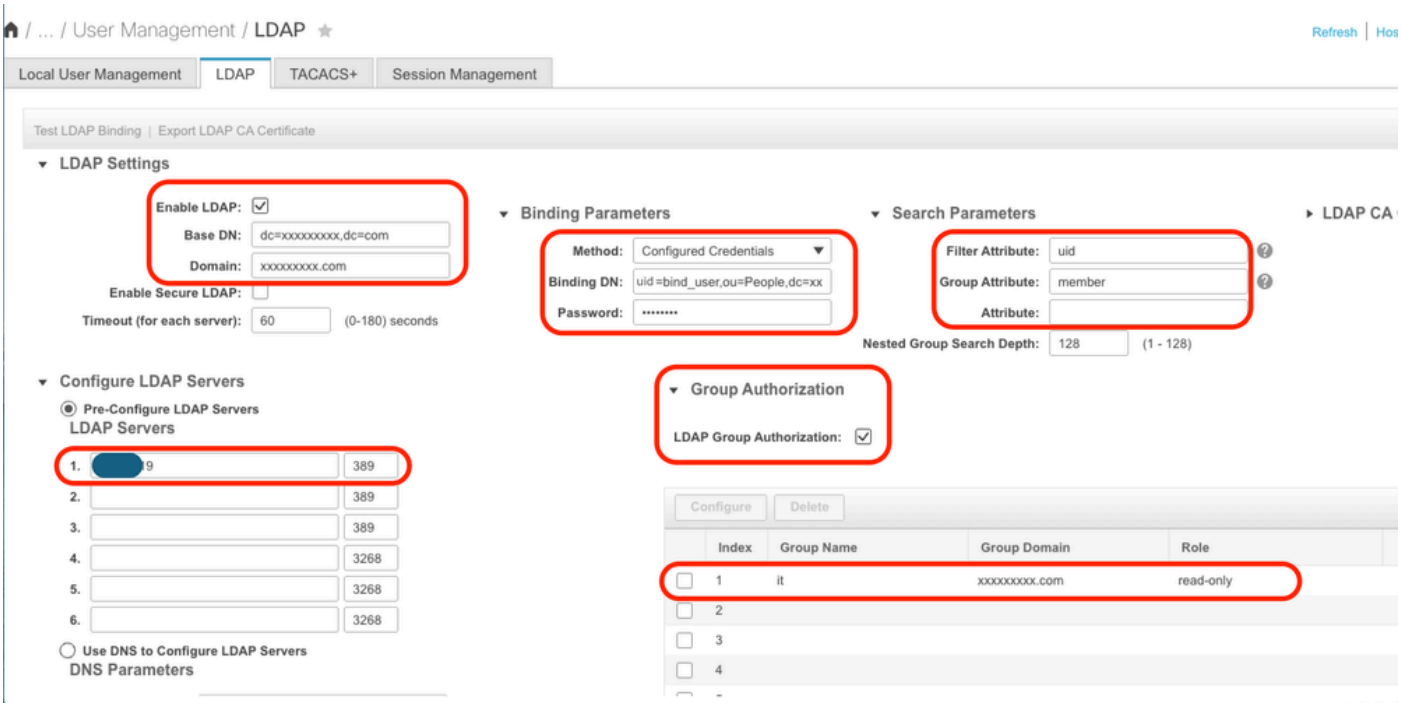
- Dominio: xxxxxxxxx.com

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

- Parametri di associazione: Può essere "Credenziali di accesso" o "Credenziali configurate"
  - Quando si utilizzano le credenziali configurate, aggiungere il DN bind_user esattamente come configurato sul server LDAP:
  - Esempio: "cn=bind_user,ou=People,dc=xxxxxxx,dc=com" o "uid=bind_user,ou=People,dc=xxxxxxxxx,dc=com"

- Parametri di ricerca:
  - Attributo filtro: "cn" o "uid"
  - Attributo gruppo: membro

- Autorizzazione gruppo LDAP - Selezionata
  - Nome gruppo: it
  - Dominio gruppo: xxxxxxxxx.com
  - Ruolo: di sola lettura (qualsiasi ruolo preferito)



Salvare la configurazione e verificare l'accesso utente LDAP.

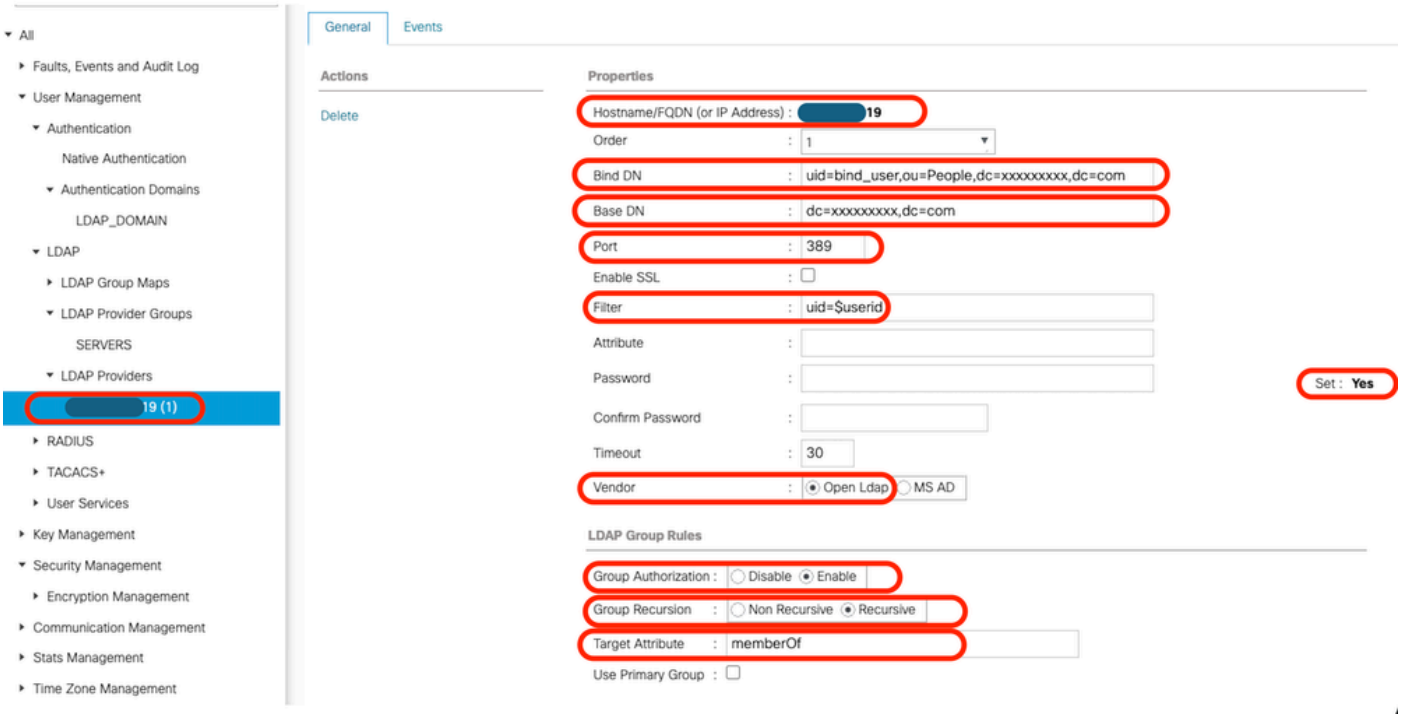
Parametri di configurazione in UCS Manager

Accedere a UCS Manager.

Nel riquadro di navigazione, selezionare Amministrazione, Gestione utente e LDAP.

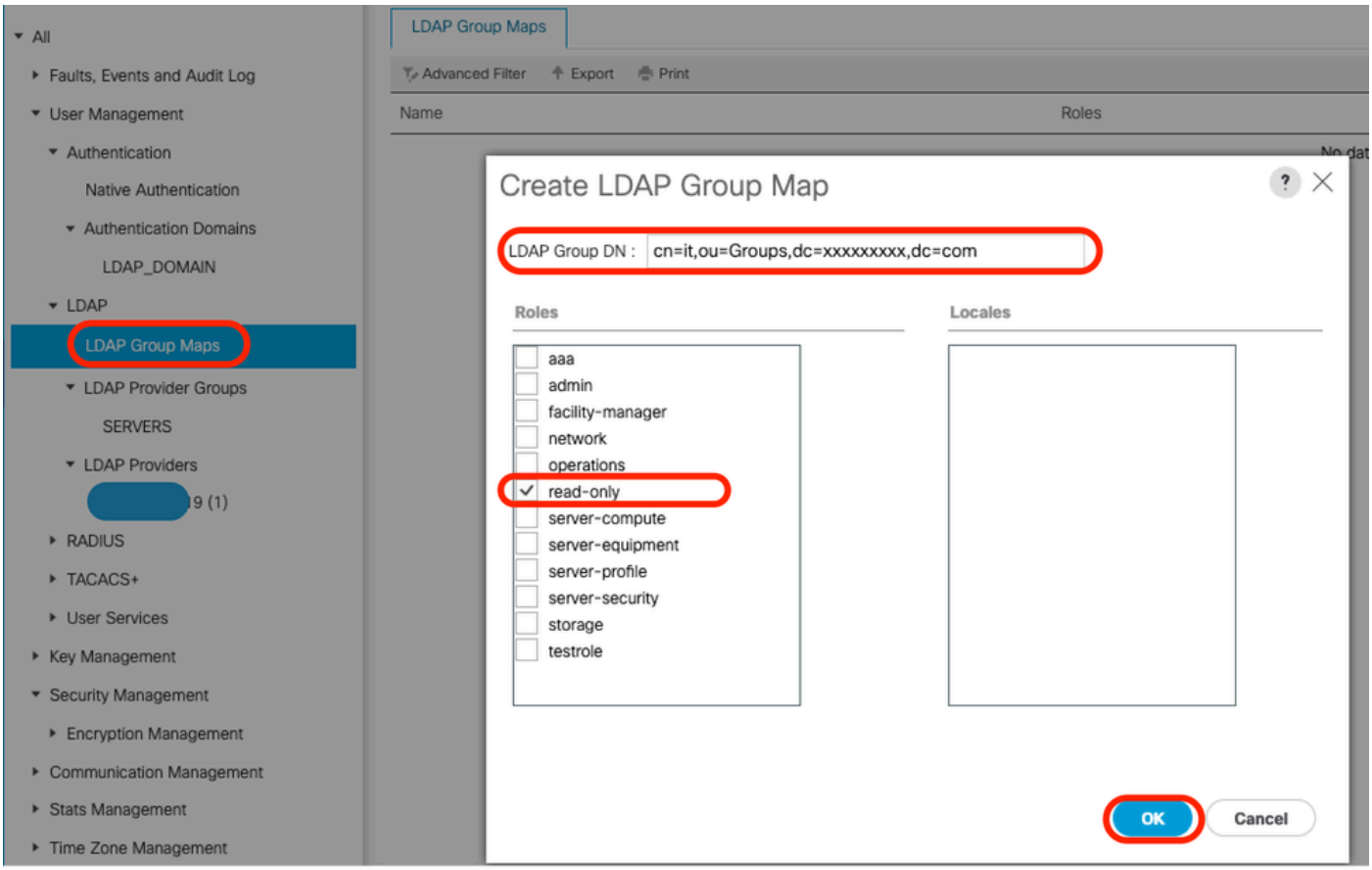
Inserire i parametri di configurazione LDAP come indicato di seguito:

- Provider LDAP:
  - Nome host: <FQDN o indirizzo IP del server LDAP>
  - DN binding: uid=bind_user,ou=Persone,dc=xxxxxxx,dc=com
  - DN di base: dc=xxxxxxxxx,dc=com
  - Port: 389
  - Abilita SSL: Disabled
  - Filtro: uid=$userid
  - Autorizzazione gruppo: Attivato
  - Ricorsione gruppo: Ricorsivo
  - Attributo di destinazione: memberOf
- Mapping gruppi LDAP:
  - DN gruppo LDAP: cn=it,ou=Groups,dc=xxxxxxxxx,dc=com



Aggiungere il provider LDAP configurato a un gruppo di provider LDAP. Per questa dimostrazione, viene utilizzato il gruppo di provider LDAP "SERVER".

Configurare le Mappe gruppo LDAP aggiungendo un "DN gruppo LDAP", recuperato dal server LDAP.



Configurare un dominio di autenticazione LDAP (LDAP_DOMAIN) in "All >> User Management >> Authentication >> Authentication Domains" (Tutti > Gestione utenti > Autenticazione > Domini di autenticazione) che fa riferimento ai gruppi di provider LDAP (SERVER) e verificare l'accesso utente LDAP.

Successivamente, esamineremo l'impostazione dello stesso (con overlay) in una distribuzione Linux separata (CentOS 10)

Scenario 2: CentOS Stream 10 - Fedora

Le procedure di configurazione per il protocollo LDAP (Lightweight Directory Access Protocol) variano a seconda della versione del sistema operativo sottostante. Questa sezione è incentrata sull'implementazione di LDAP su CentOS Stream 10.

Mentre molte distribuzioni Linux utilizzano OpenLDAP, CentOS Stream 10 e i sistemi basati su Fedora utilizzano il server di directory 389 (389 DS) come provider LDAP predefinito.

Nota: Sebbene 389 DS sia considerato il successore di OpenLDAP all'interno degli ecosistemi CentOS e Red Hat, le due soluzioni non sono direttamente intercambiabili. Le strutture delle directory, i file di configurazione e gli ambienti operativi sono notevolmente diversi.

Questa guida fornisce i passaggi necessari per configurare correttamente LDAP utilizzando 389 DS in un ambiente CentOS Stream 10.

Opzione 1: Configura LDAP utilizzando il server di elenchi in linea 389 in CentOS Stream 10

Passaggio 1: Impostazione iniziale

Ripetere il passaggio 1 nello scenario 1, opzione 1.

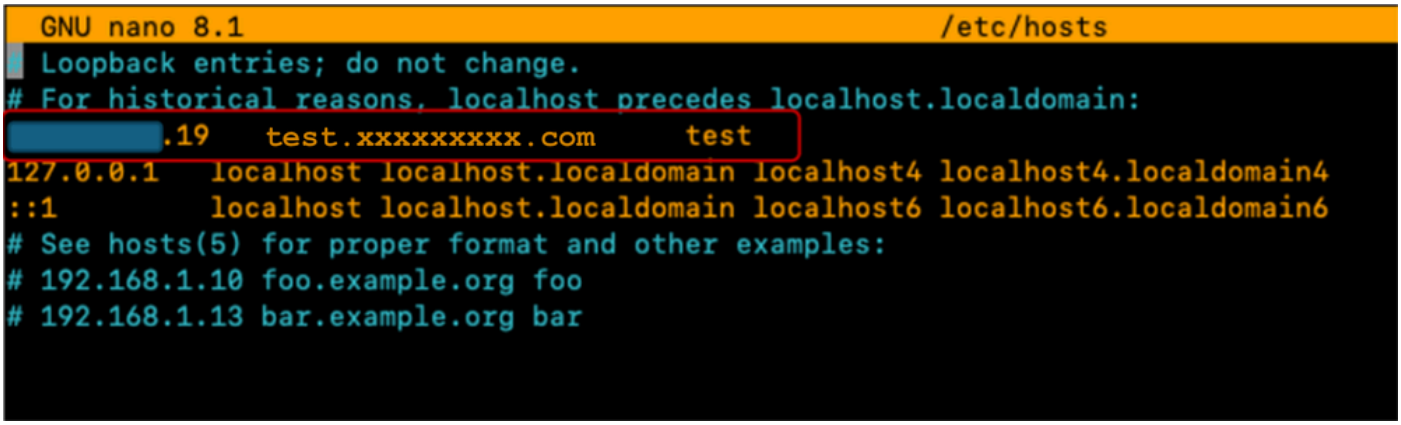
I sistemi CentOS non utilizzano la suite di gestione dei pacchetti APT. Per eseguire le installazioni software necessarie su CentOS Stream 10, utilizzare i package manager dnf (Dandified YUM) o yum

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

Verificare l'indirizzo IP del server utilizzando il comando "ifconfig".

Aggiungere l'indirizzo IP del server al file "/etc/hosts" insieme al nome di dominio completo del server (ad esempio: test.xxxxxxxxx.com utilizzato in questa esercitazione) e al nome host (ad esempio: test) nel formato specificato di seguito:

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



Aggiornare il file "/etc/hostname" sostituendone il contenuto con il nome host (test).

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

Per rendere effettive le modifiche è necessario riavviare il server.

```
sudo reboot
```

Passaggio 2: Installa il repository EPEL e il pacchetto server 389

Installare e aggiornare il repository EPEL.

Installare il pacchetto 389 del server delle directory.

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

Creare un file di modello di directory contenente i parametri delle impostazioni del server LDAP desiderati:

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

Verificare il contenuto del file modello creato (ldapconfig.conf)

```
sudo cat ldapconfig.conf
```

Modificare il file di modello ldapconfig.conf.

```
sudo nano ldapconfig.conf
```

Inserire le voci di configurazione specificate nel file e salvare le modifiche.

Nota:è possibile richiedere diverse modifiche in base alle esigenze o ai requisiti specifici di ciascun ambiente.

In questo esempio vengono illustrate le configurazioni di base per questa dimostrazione.

```
[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
```

Il file di modello definisce i parametri di configurazione per l'istanza della directory "localhost". Ciò include l'impostazione dell'utente amministrativo ("admin"), la password associata e il contesto del dominio ("xxxxxxxxx.com").

Creare l'istanza della directory "localhost" utilizzando il modello modificato in precedenza. Il comando specificato crea e avvia il server di directory LDAP:

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

Verificare che il servizio LDAP sia in esecuzione sul server

```
ss -ntl
```

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

Regolare il firewall di CentOS in modo da consentire le porte necessarie per LDAP (389 e/o 636).

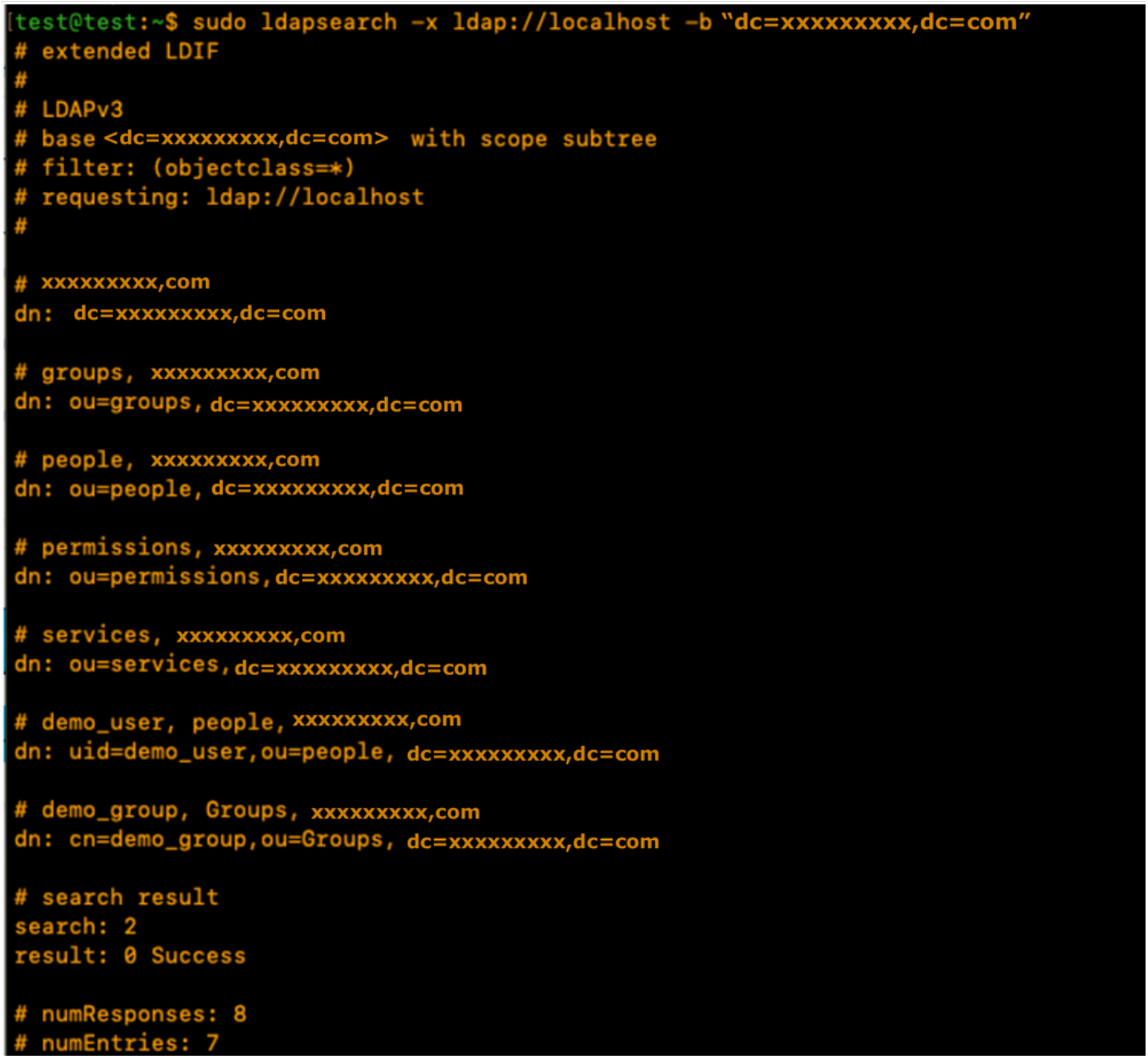
Per questa demo, il firewall è disattivato.

```
sudo systemctl stop firewalld
```

Verificare che LDAP funzioni localmente sul server LDAP eseguendo il comando specificato e che

restituisca l'output LDAP come mostrato di seguito:

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



L'output contiene account demo creati dal server 389DS. Il server LDAP ha creato automaticamente le unità organizzative predefinite.

OU utenti per utenti e OU gruppi per gruppi. È possibile creare unità organizzative aggiuntive a seconda dei requisiti.

Per questa dimostrazione vengono utilizzate le unità organizzative predefinite/create

automaticamente.

Consultare la documentazione ufficiale di 389DS per i dettagli sull'uso esteso del pacchetto 389DS:

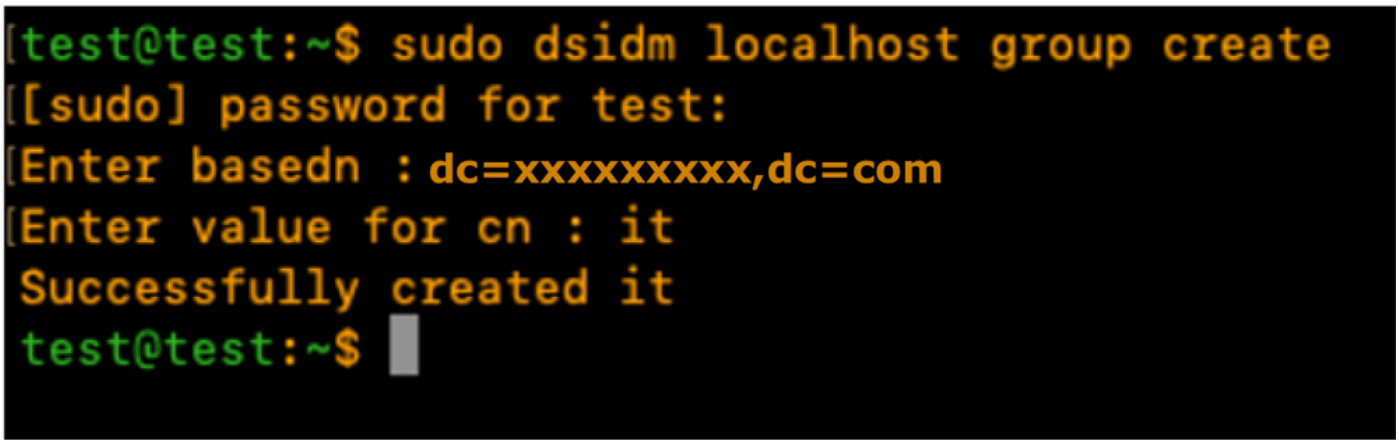
Passaggio 3: Creazione di utenti e gruppi LDAP

Creare un gruppo utilizzando il comando specificato: sudo dsidm <nome_istanza> group create.

Per questa dimostrazione, il nome dell'istanza è "localhost".

```
sudo dsidm localhost group create
```

Immettere il prompt del terminale per inserire i dettagli del gruppo come mostrato:



Creare l'account utente testuser1 utilizzando il comando:

```
sudo dsidm localhost user create
```

Immettere il prompt del terminale per inserire i dettagli dell'utente come mostrato

```
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
```

Creare una password per testuser1 utilizzando il comando specificato e immettere il prompt 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:~$
```

Aggiungere l'utente a un gruppo utilizzando il comando specificato: "sudo dsidm <istanza_directory> group add_member <gruppo_cn> <nome_utente>"

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

Ripetere i passi di creazione Utente per creare testuser2 e bind_user.

Nota:assicurarsi che ogni utente sia aggiunto esplicitamente ai gruppi a cui è destinato.

Se si omette questo passaggio, è possibile che si verifichino limitazioni di accesso o errori di autorizzazione.

Non è necessario che l'account bind_user sia membro di un gruppo specifico, in quanto può essere configurato come account standalone, fornendo la flessibilità necessaria per gestire l'accesso amministrativo e a livello di servizio all'interno dell'ambiente di directory.

Riavviare l'istanza della directory:

```
sudo dsctl localhost restart
```

Passaggio 4: Installa sovrapposizione memberOf

Installare il plug-in "memberOf" e riavviare l'istanza della directory:

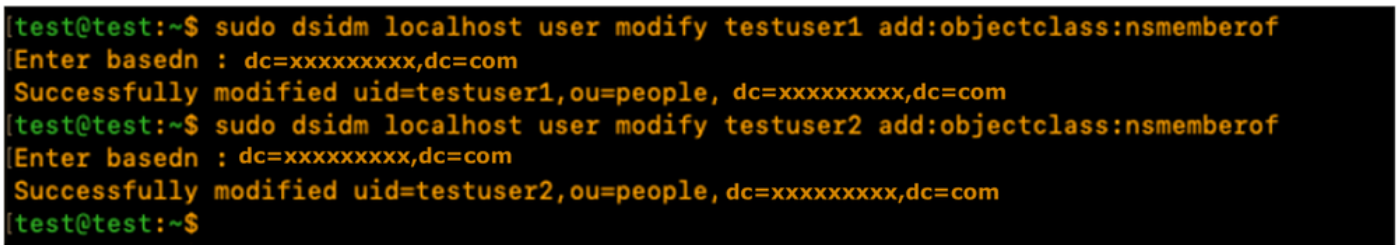
```
sudo dsconf localhost plugin memberof status
sudo dsconf localhost plugin memberof enable
sudo dsctl localhost restart
```

Configurare il plug-in "memberOf" utilizzando il comando specificato: "sudo dsconf <istanza_directory> plugin memberof set —scope <dn_base>"

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

Contrassegnare gli utenti come destinazioni "memberOf" valide utilizzando il comando specificato: "sudo dsidm <istanza_directory> user modify <uid> add:objectclass:nsmemberof"

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



Generare la correzione "memberOf" per il DN di base: "membro del plug-in sudo dsconf <istanza_directory> di correzione <dn_base>"

```
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:~$
```

Verificare la configurazione dell'utente:

```
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:~$
```

Il server LDAP 389DS è configurato con il plug-in memberOf per supportare l'attributo memberOf.

Parametri di configurazione su CIMC

Accedere a CIMC.

Nel riquadro di navigazione, selezionare Amministrazione, Gestione utente e LDAP.

Inserire i parametri di configurazione LDAP come indicato di seguito:

- Abilita LDAP: selezionata
- DN di base: dc=xxxxxxxxx,dc=com

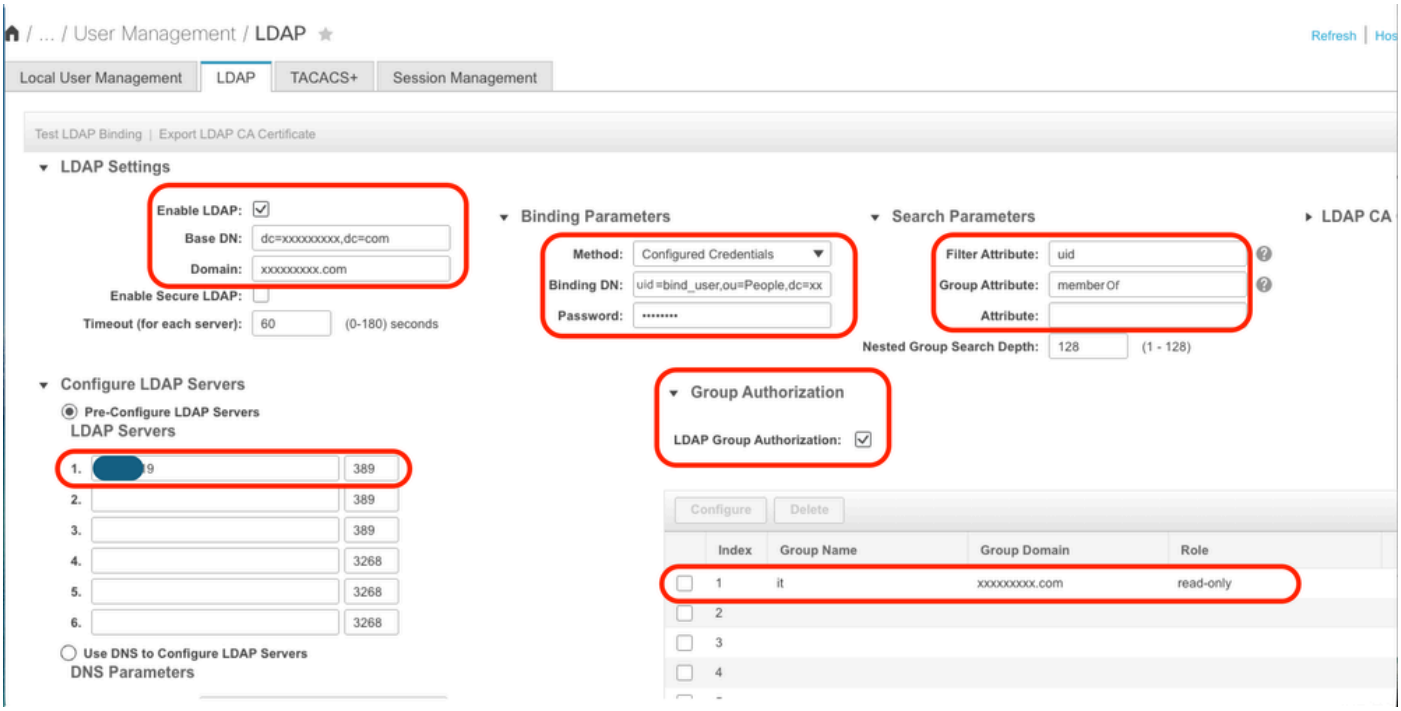
- Dominio: xxxxxxxxx.com

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

- Parametri di associazione: Può essere "Credenziali di accesso" o "Credenziali configurate"
  - Quando si utilizzano le credenziali configurate, aggiungere il DN bind_user esattamente come configurato sul server LDAP:
    - Esempio: "cn=bind_user,ou=People,dc=xxxxxxx,dc=com" o "uid=bind_user,ou=People,dc=xxxxxxxxx,dc=com"

- Parametri di ricerca:
  - Attributo filtro: "cn" o "uid"
  - Attributo gruppo: memberOf

- Autorizzazione gruppo LDAP - Selezionata
  - Nome gruppo: it
  - Dominio gruppo: xxxxxxxxx.com
  - Ruolo: di sola lettura (qualsiasi ruolo preferito)



Salvare la configurazione e verificare l'accesso utente LDAP.

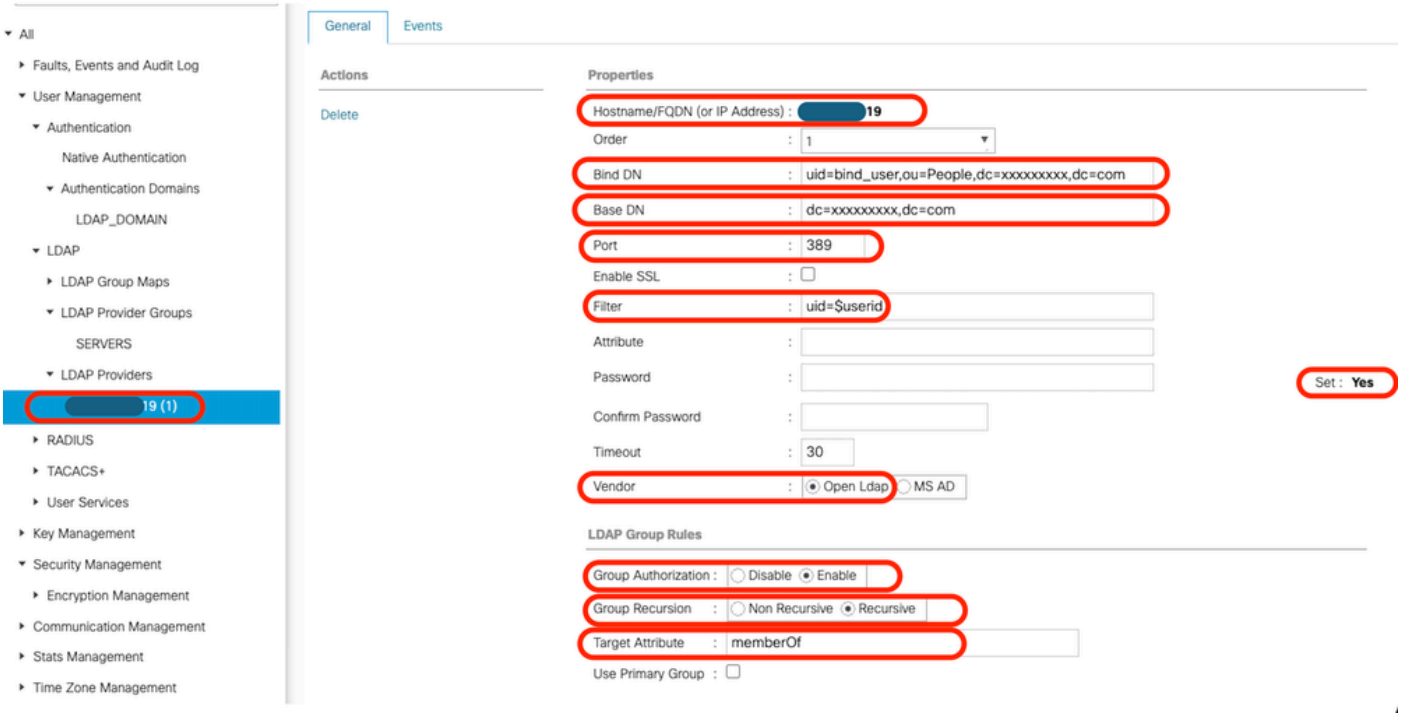
Parametri di configurazione in UCS Manager

Accedere a UCS Manager.

Nel riquadro di navigazione, selezionare Amministrazione, Gestione utente e LDAP.

Inserire i parametri di configurazione LDAP come indicato di seguito:

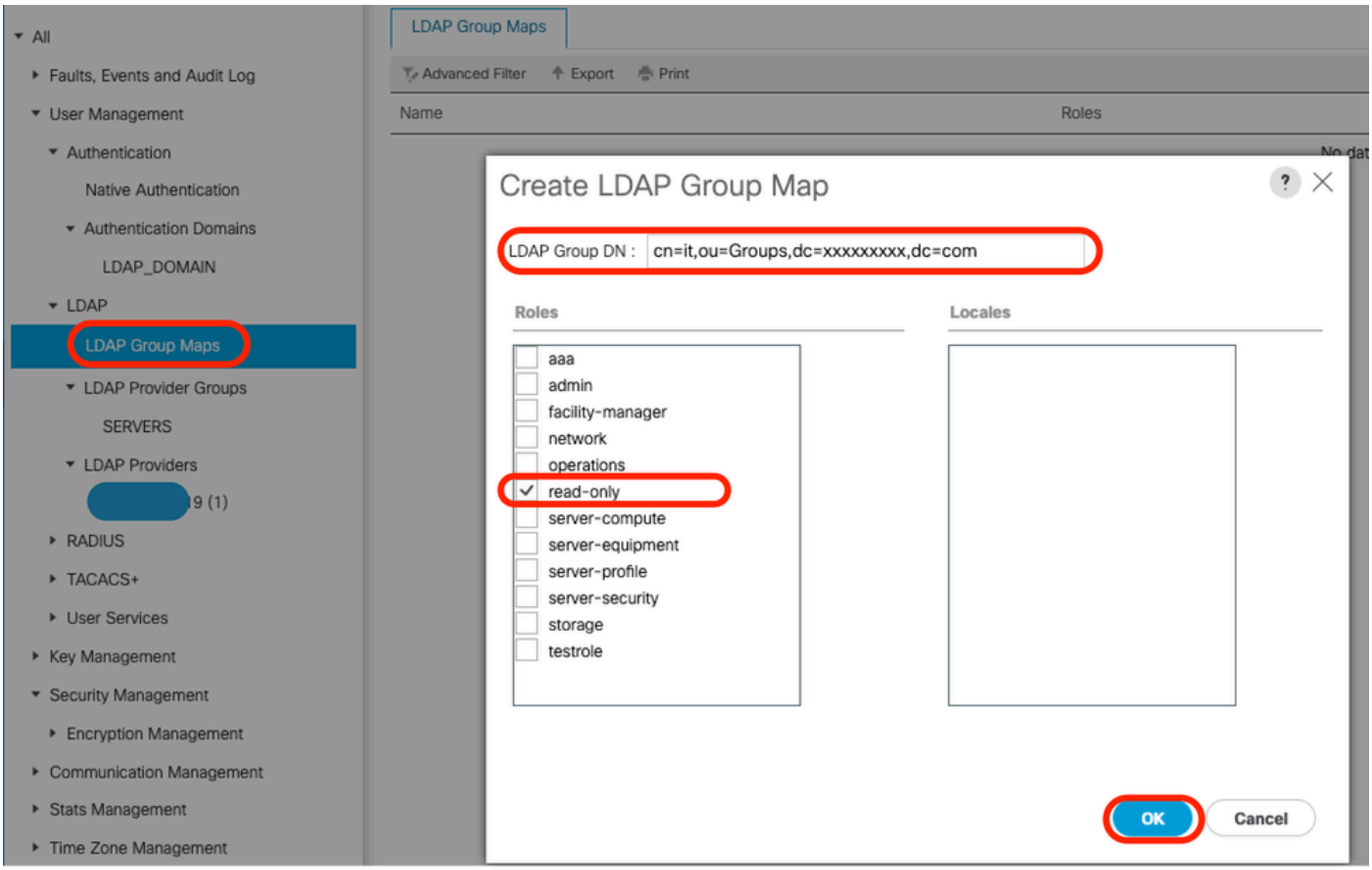
- Provider LDAP:
  - Nome host: <FQDN o indirizzo IP del server LDAP>
  - DN binding: uid=bind_user,ou=people,dc=xxxxxxxxx,dc=com
  - DN di base: dc=xxxxxxxxx,dc=com
  - Port: 389
  - Abilita SSL: Disabled
  - Filtro: uid=$userid
  - Autorizzazione gruppo: Attivato
  - Ricorsione gruppo: Ricorsivo
  - Attributo di destinazione: memberOf
- Mapping gruppi LDAP:
  - DN gruppo LDAP: cn=it,ou=Groups,dc=xxxxxxxxx,dc=com



Aggiungere il provider LDAP configurato a un gruppo di provider LDAP. Per questa dimostrazione,

viene utilizzato il gruppo di provider LDAP "SERVER".

Configurare le Mappe gruppo LDAP aggiungendo un "DN gruppo LDAP", recuperato dal server LDAP.



Configurare un dominio di autenticazione LDAP (LDAP_DOMAIN) in "All >> User Management >> Authentication >> Authentication Domains" (Tutti > Gestione utenti > Autenticazione > Domini di autenticazione) che fa riferimento ai gruppi di provider LDAP e verificare l'accesso utente LDAP.

Conclusioni

Anche se questa guida descrive gli scenari di distribuzione essenziali, un'ulteriore esplorazione delle funzionalità LDAP può migliorare significativamente le prestazioni e la sicurezza delle directory.

Per ulteriori informazioni, best practice e dettagli sulla configurazione avanzata, fare riferimento alle risorse specificate:

- Documentazione ufficiale di OpenLDAP

- Gestione account LDAP - Manuale
- Documentazione relativa a 389 Directory Server
- Configura LDAP in UCS Manager
- Configurazione di Secure LDAP sui server UCS serie C

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).