Konfigurieren von LDAP auf UCS Manager & CIMC unter Verwendung von Linux OpenLDAP und 389-DS Servern

Inhalt

Einleitung

In diesem Dokument werden verschiedene Optionen zur Konfiguration von LDAP als

Authentifizierungsmethode für UCS Manager und CIMC unter Verwendung von Linux-basierten OpenLDAP- und 389-Verzeichnisservern beschrieben.

Hintergrundinformationen

Aufgrund der großen Variabilität der OpenLDAP-Serverkonfigurationen wird in diesem Dokument auf eine erschöpfende Behandlung verzichtet. In diesem Artikel werden stattdessen häufig implementierte Konfigurationen betont, die mehrere Linux-Distributionen, LDAP-Serverpakete und Attributschemas umfassen. Aus Gründen der Übersichtlichkeit und Einfachheit werden in diesem Dokument die LDAP-Standardkonfigurationen behandelt. Die Konfiguration von sicherem LDAP (LDAPS) wird in diesem Dokument nicht behandelt.

Voraussetzungen:

Die Kenntnis dieser Themen wird dringend empfohlen:

- UCS B-Serie
- UCS C-Serie
- Linux Server-Administration

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- UCS Manager-Firmwareversion: 4,3 (2c)
- Fabric Interconnect-Modell: UCS-FI-6454
- Standalone-Servermodell der UCS C-Serie: UCSC-C240-M5
- Standalone-Firmware-Version der UCS C-Serie: 2,250045
- Ubuntu 20,04
- CentOS-Stream 10

Einstellungen für diese Demonstration:

- Hostname des LDAP-Servers: Test

- Serverdomäne: xxxxxxxxx.com

- Server-FQDN: test.xxxxxxxxx.com
- Linux Server (Ubuntu und CentOS) IP-Adresse: X,X,X,19
- OpenLDAP-Benutzer: testuser1, testuser2
- OpenLDAP-Gruppe(n): es
- OpenLDAP Bind-Benutzerkonto: bind_user

Anmerkung: In dieser Übung wurde der Text-Editor linux Nano verwendet.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Szenario 1: Ubuntu - Debian

Die LDAP-Serverkonfiguration kann entweder über eine grafische Benutzeroberfläche, wie den LDAP Account Manager, oder über Befehlszeilentools erfolgen, je nach den bevorzugten Verwaltungseinstellungen und der erforderlichen Kontrollebene. In diesem Szenario wird die Konfiguration mit Linux-basiertem OpenLDAP untersucht. Dies beginnt mit einer GUI-basierten Bereitstellung und der anschließenden Umstellung auf Befehlszeilen-Dienstprogramme, um erweiterte Funktionen, einschließlich Overlay-Plug-Ins (die häufig in Integrationen mit Cisco UCS Manager verwendet werden), zu erkunden.

Option 1: Konfigurieren von OpenLDAP mithilfe des Ubuntu LDAP Account Managers (LAM)

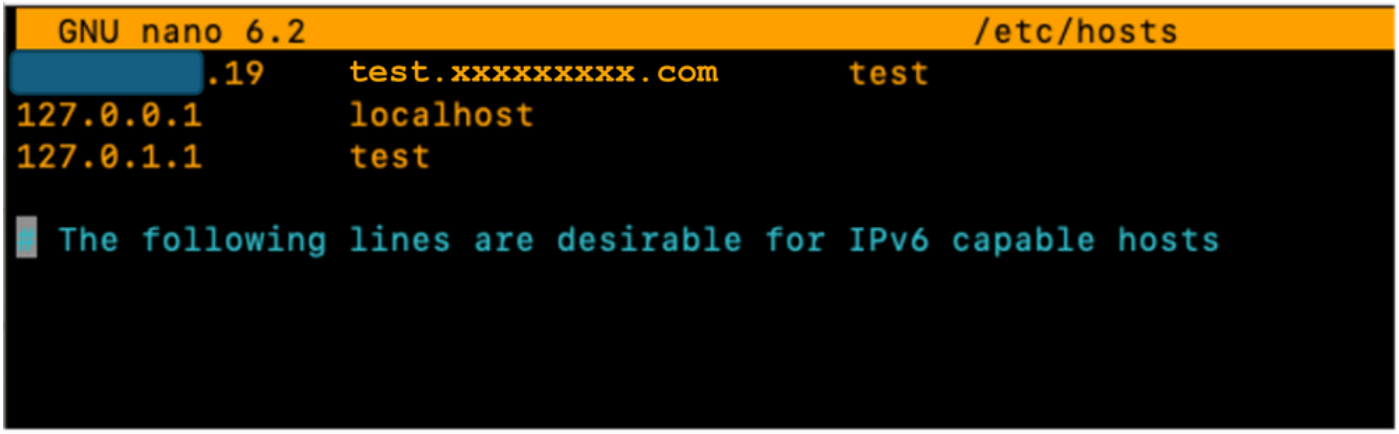
Schritt 1: Erstkonfiguration des Linux-Server-Hostnamens und der Net-Tools.

Aktualisieren Sie ubuntu und installieren Sie das net-tools Paket für den Zugriff auf Tools wie ifconfig, netstat etc:

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

Verwenden Sie den Befehl "ifconfig", um die IP-Adresse des Servers zu überprüfen, und fügen Sie sie zusammen mit dem Server-Domänennamen der Datei "/etc/hosts" hinzu (Beispiel: "test.xxxxxxx.com" in dieser Übung) und Hostname (Beispiel: "test") im angegebenen Format.

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



Aktualisieren Sie zusätzlich die Datei "/etc/hostname", indem Sie deren Inhalt durch den Hostnamen (test) ersetzen.

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

Damit diese Änderungen wirksam werden, muss der Server neu gestartet werden.

```
sudo reboot
```

Schritt 2: Installation von SLAPD, Apache, PHP und deren Abhängigkeiten

Als Nächstes installieren Sie Apache, PHP und ihre Abhängigkeiten. Diese werden verwendet, um

GUI-Interaktionen über eine Webseite zu ermöglichen:

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

Open LDAP-Serverpaket"slapd" und seine Abhängigkeiten (ldap-utils) installieren

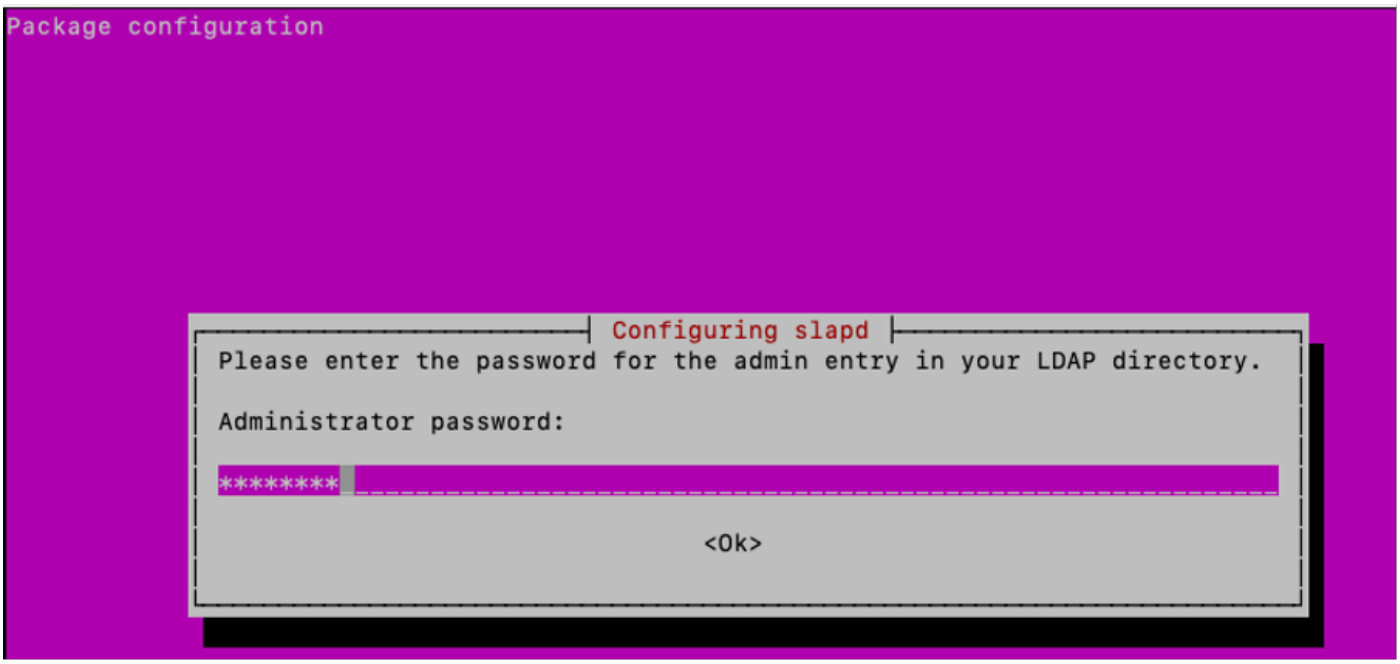
```
sudo apt install slapd ldap-utils -y
```

Geben Sie während der SLAPD-Installation in das angezeigte GUI-Popup die zusätzlich erforderliche SLAPD-Paketkonfiguration ein.

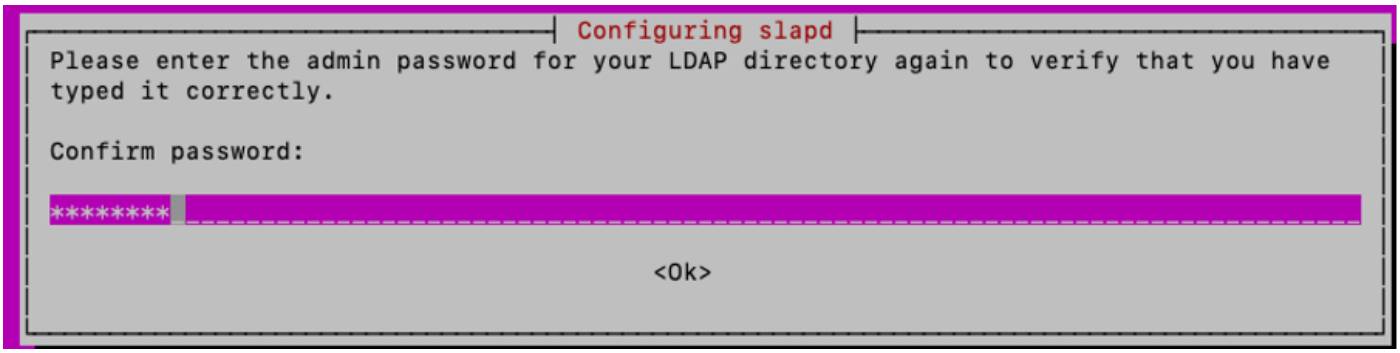
Anmerkung: Der Kennwortverlust erfordert eine Neuinstallation des LDAP-Servers.

Der "Administrator" (admin) in diesem Kontext ist ein Konto, das verwendet wird, um den OpenLDAP-Dienst, Module und Konfigurationen zu verwalten.

Fügen Sie das Kennwort des LDAP-Pakets "administrator" hinzu, und drücken Sie die Eingabetaste auf der Tastatur, um "OK" auszuwählen.



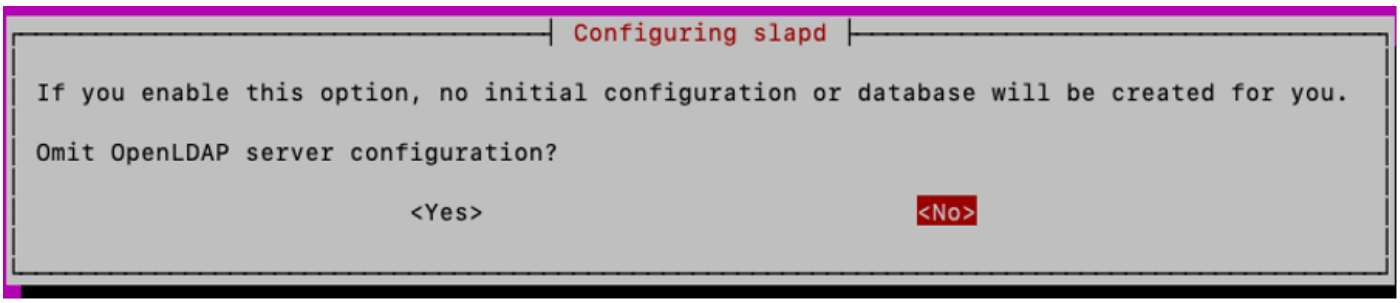
Passwort bestätigen:



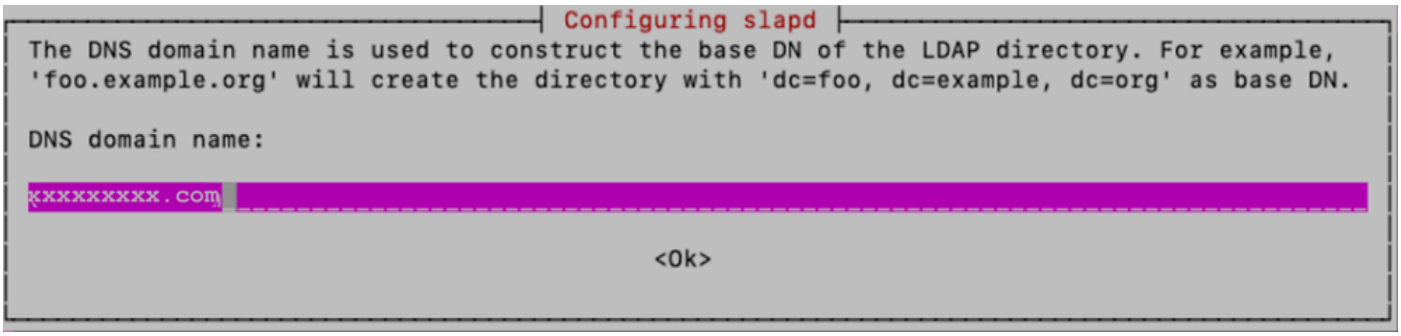
Nach Abschluss der Installation können Sie das SLAPD-Paket mit dem angegebenen Befehl neu konfigurieren und Domäneninformationen hinzufügen:

```
sudo dpkg-reconfigure slapd
```

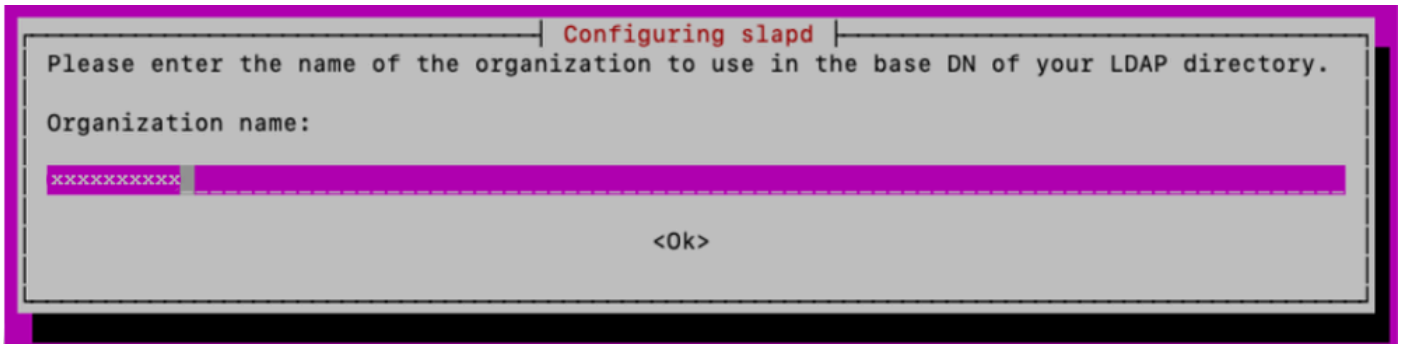
Sie können die Standardoption "Nein" für "OpenLDAP-Serverkonfiguration auslassen" akzeptieren und die Eingabetaste drücken:



Geben Sie den Domänennamen ein, und drücken Sie die Eingabetaste:



Für diese Übung wird "xxxxxxxxx" als "Organisationsname" verwendet:

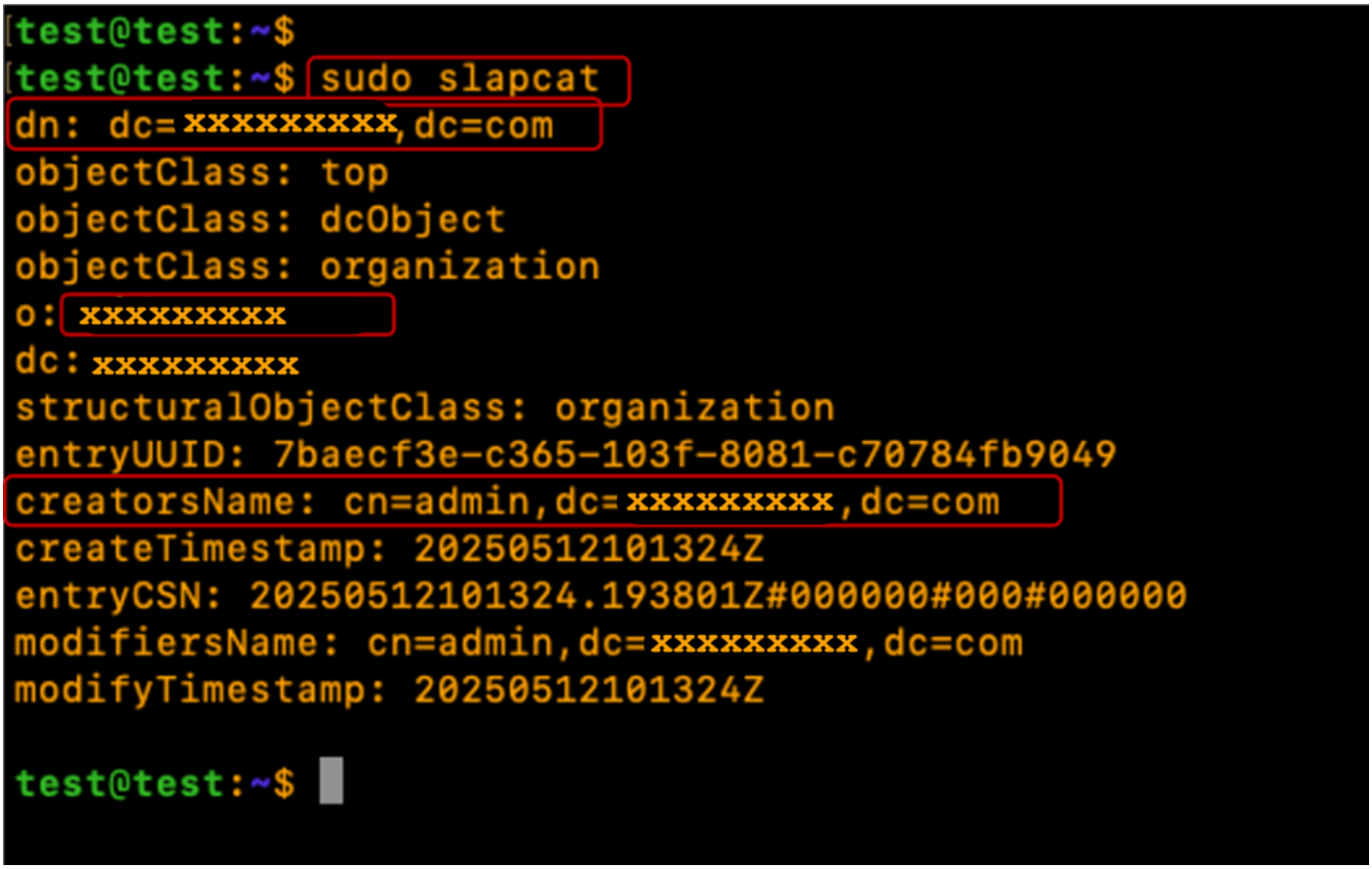


Geben Sie anschließend das "Administratorkennwort" ein, und bestätigen Sie es.

Behalten Sie für die anderen Konfigurationsoptionen die Standardeinstellungen bei, und drücken Sie die Eingabetaste, um die Konfiguration abzuschließen.

Überprüfen Sie die SLAPD-Installation mit dem folgenden Befehl:

```
sudo slapcat
```



Schritt 3: Installation des LDAP Account Managers

Installieren Sie den LDAP Account Manager (LAM) zum Erstellen und Verwalten von LDAP-Benutzern und -Gruppen:

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

Aktivieren Sie die PHP-CGI PHP-Erweiterung, die von LAM benötigt wird.

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

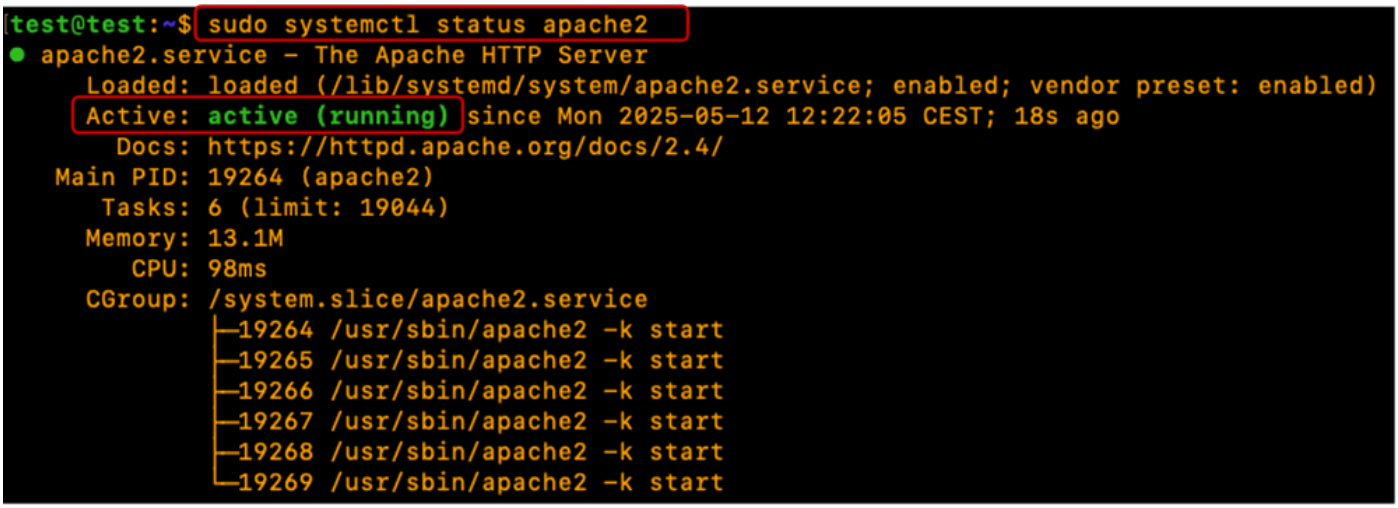
Laden Sie den Apache neu, um die neue Konfiguration zu aktivieren.

Starten Sie den Apache-Dienst neu, und aktivieren Sie ihn, um ihn beim Start automatisch zu starten:

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

Überprüfen Sie, ob der Apache-Serverstatus "Running" (Wird ausgeführt) und "Active" (Aktiv) lautet.

```
sudo systemctl status apache2
```



Konfigurieren Sie die Ubuntu-Firewall so, dass Port 80(Web), 443 (sicheres Web), 389(LDAP) und 636 (sicheres LDAP, falls erforderlich) zugelassen werden.

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

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

```
sudo ufw allow 636
```

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

Überprüfen Sie den Status der Ubuntu-Firewall:

```
sudo ufw status
```

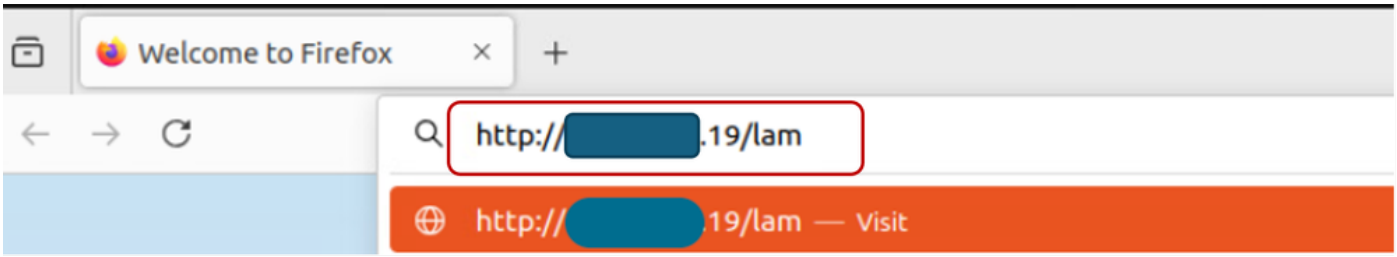
```
test@test:~$ sudo ufw status
Status: active

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)
```

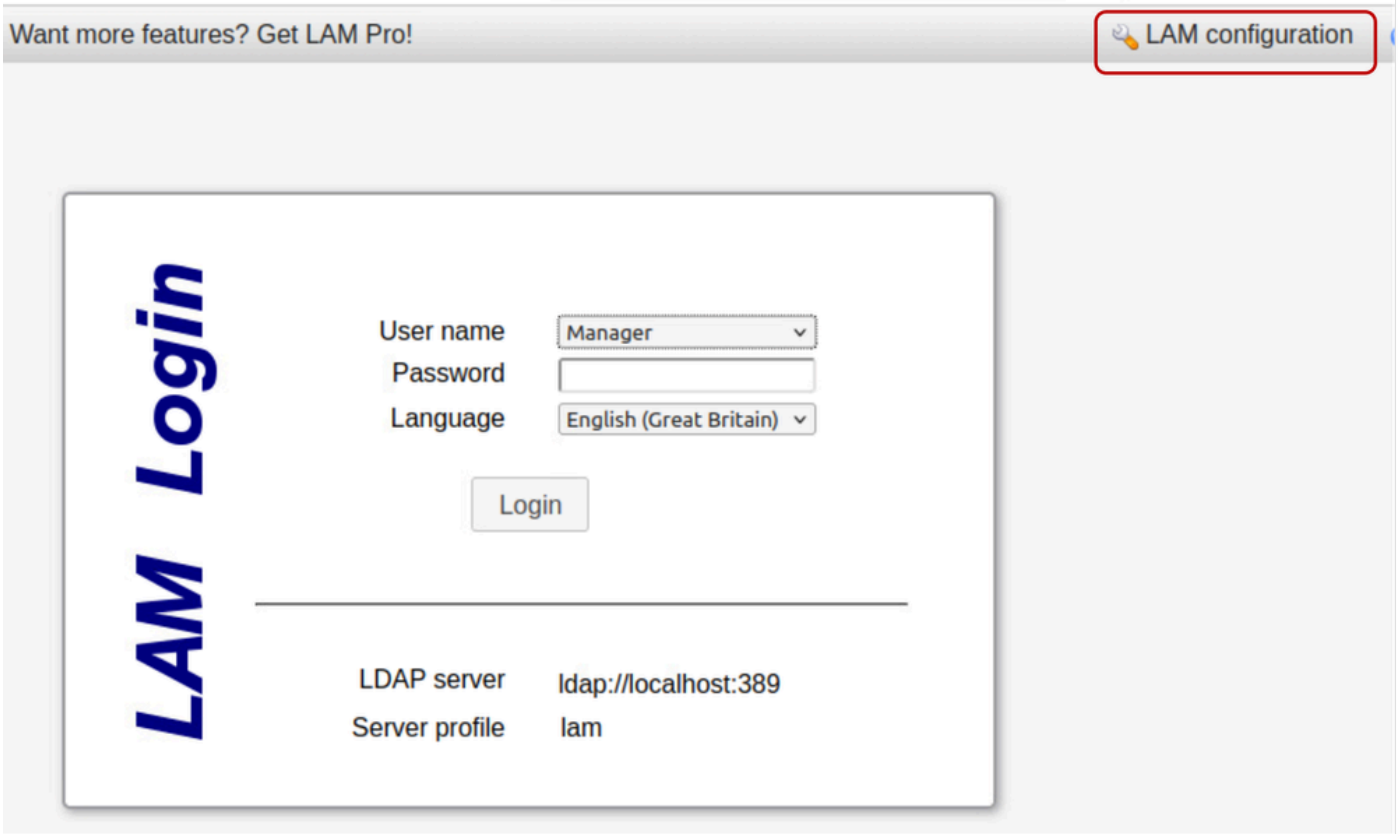
Schritt 4: LDAP-Kontomanager konfigurieren

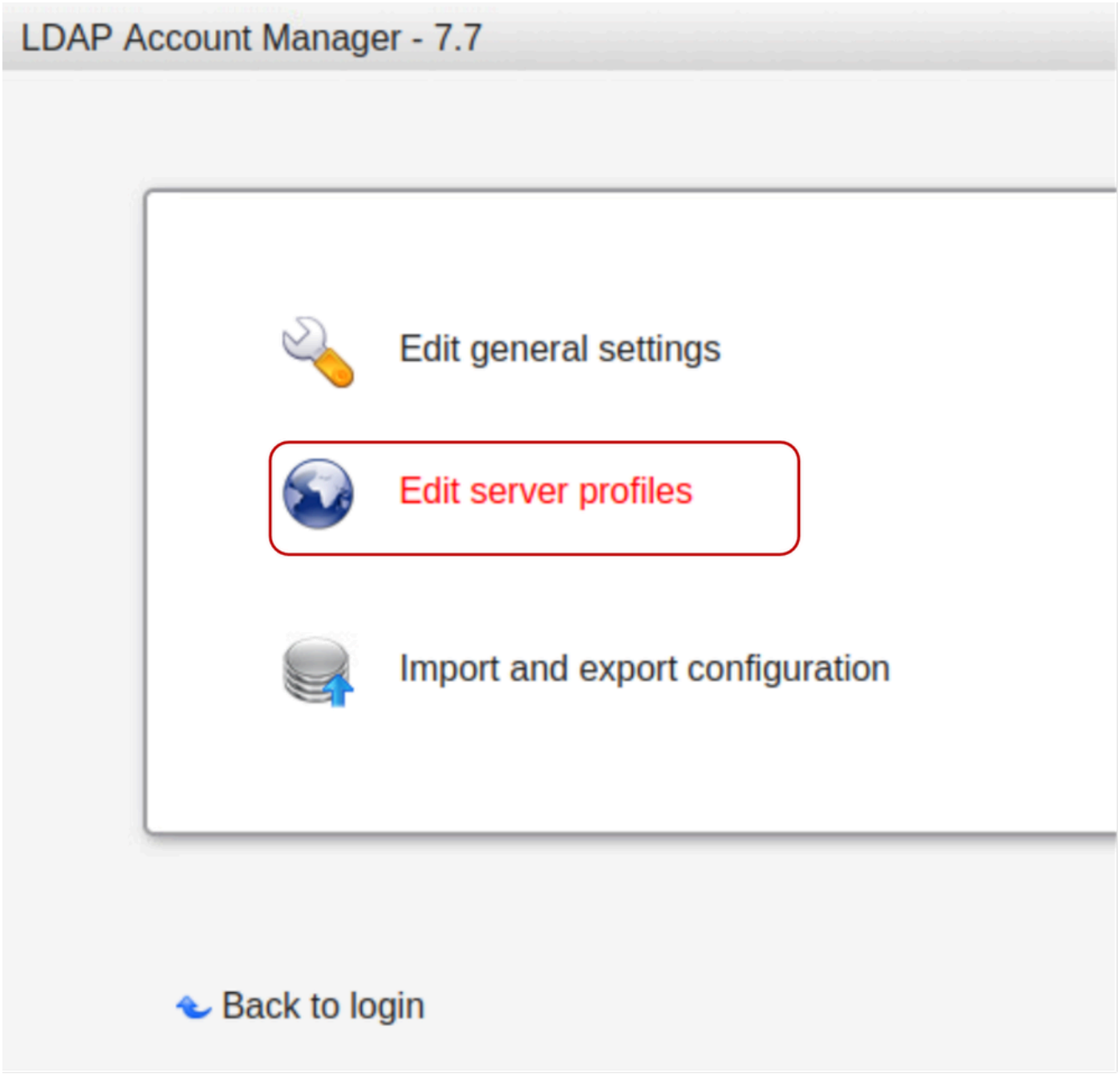
Um den LDAP Account Manager (LAM) über die GUI zu konfigurieren, öffnen Sie einen Webbrowser, geben Sie die IP-Adresse des Linux-Servers ein, und fügen Sie den Pfad "lam" wie folgt hinzu:

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

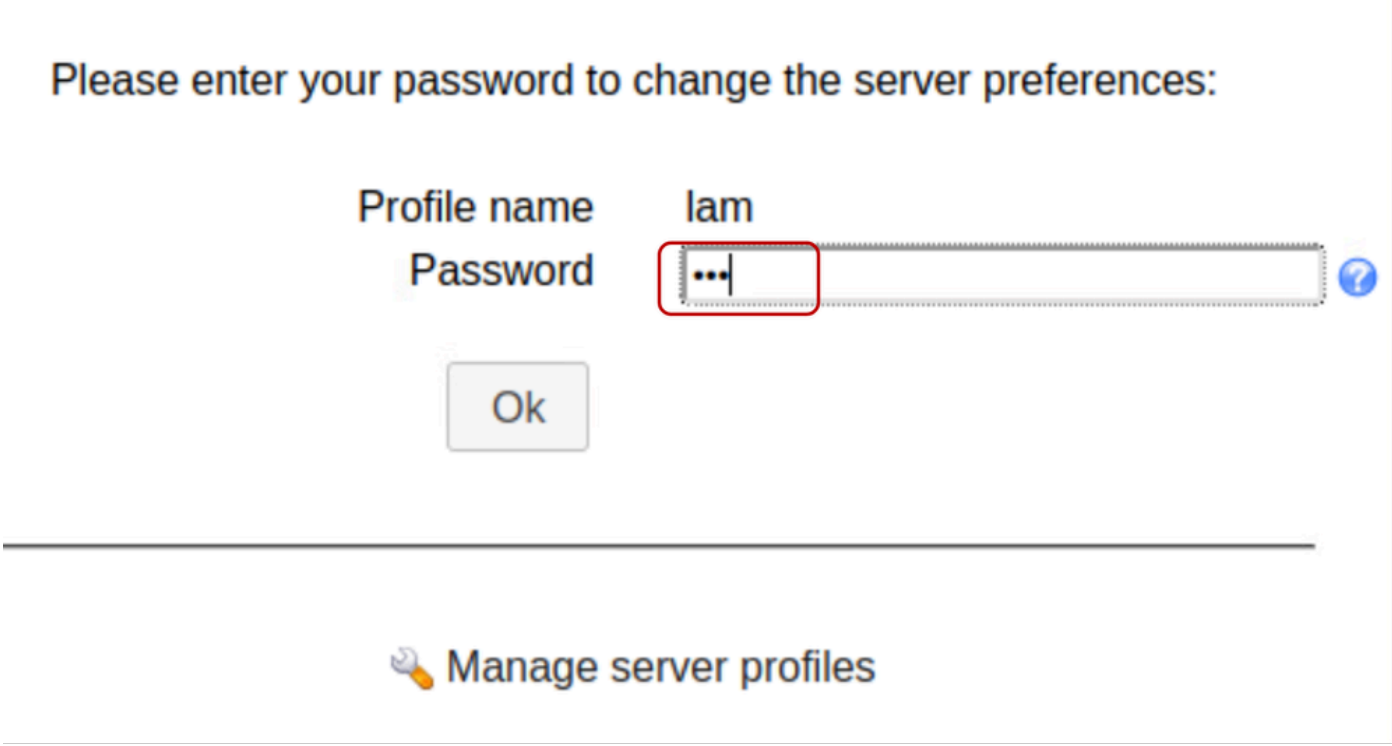


Klicken Sie auf "LAM-Konfiguration" und wählen Sie "Serverprofile bearbeiten".





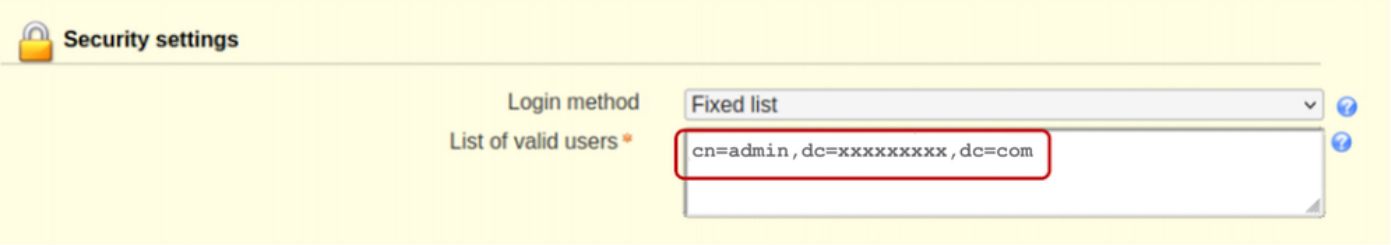
Geben Sie das Standard-LAM-Kennwort "lam" ein, um sich anzumelden.



Überprüfen Sie auf der Registerkarte General Settings die Servereinstellungen "Language" (Sprache) und "Timezone".

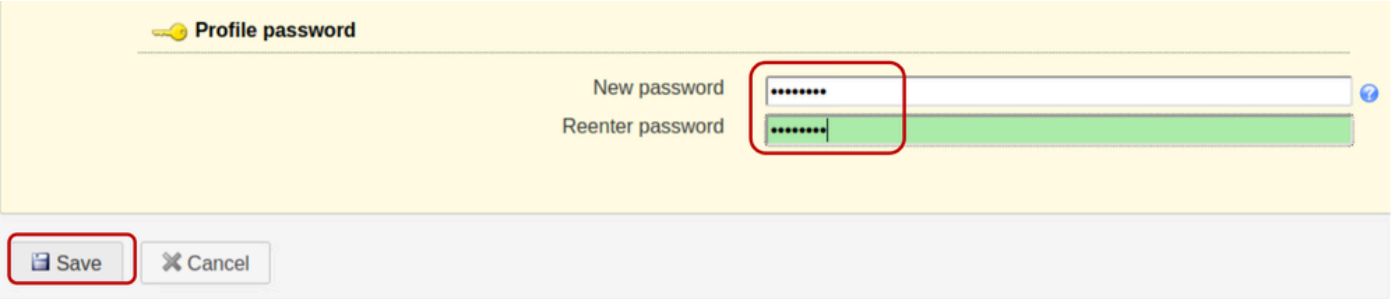
Bearbeiten und fügen Sie im Abschnitt "Tooleinstellungen" den erforderlichen Domänennamen wie unten gezeigt in das Baumsuffix-Feld ein:

Fügen Sie im Abschnitt "Sicherheitseinstellungen" einen Administrator hinzu, der für die Verwaltung des SLAPD-Dienstes verwendet wird.



Legen Sie ein "Profilkennwort" fest. Dieses Kennwort wird für spätere Anmeldungen an der LAM-Konfigurationsschnittstelle verwendet. In diesem Beispiel wird "cisco123" anstelle des Standardkennworts "lam" konfiguriert.

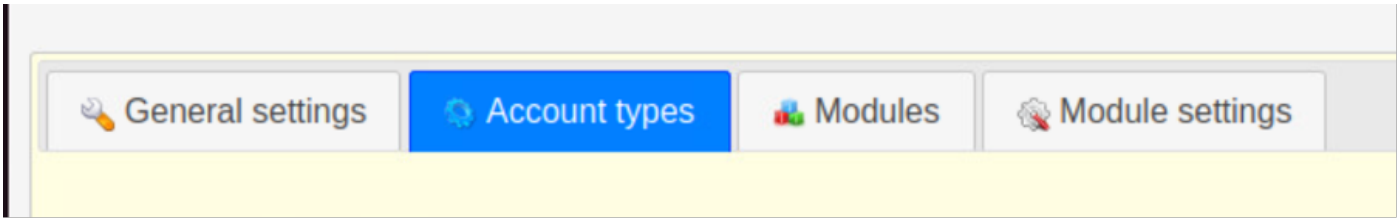
Speichern Sie die Konfiguration:



Die Sitzung wird dann auf der Benutzeroberfläche für die LAM-Konfiguration neu gestartet.

Melden Sie sich mit dem neu erstellten Kennwort wieder an (LAM-Konfiguration > Serverprofile bearbeiten).

Klicken Sie auf "Kontotypen",



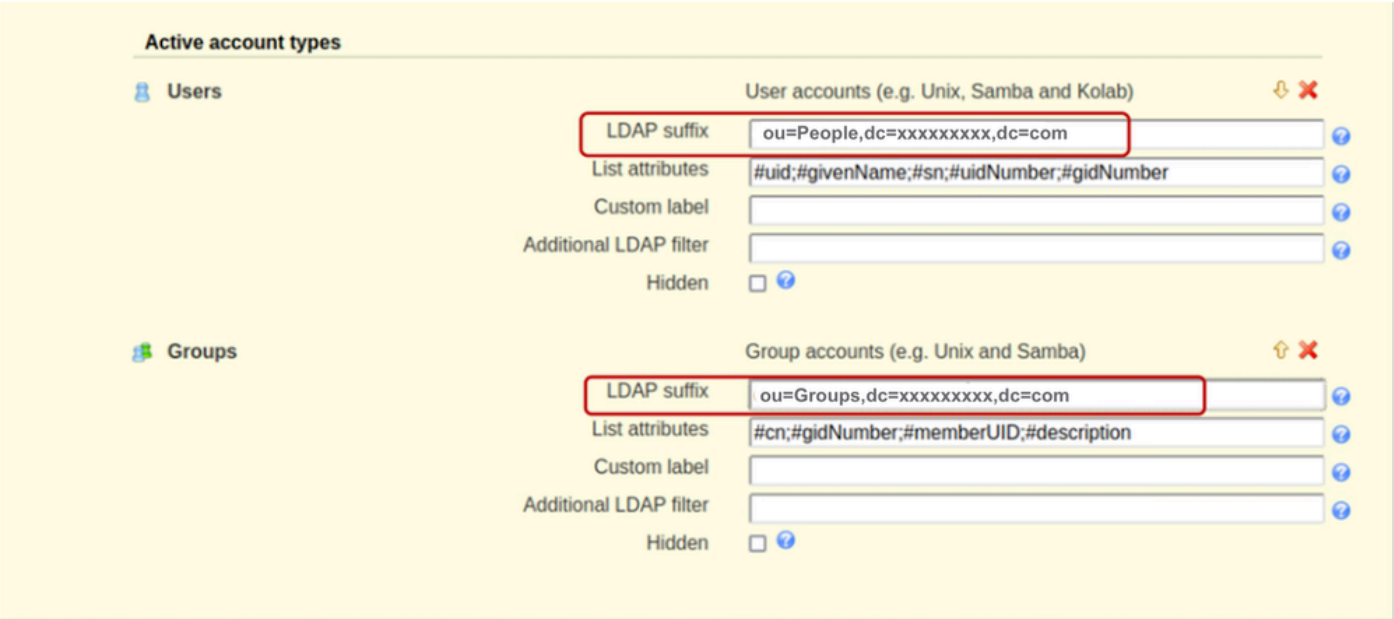
Blättern Sie nach unten, und bearbeiten Sie die Standardtypen für aktive Konten mit den Domänennameninformationen im LDAP-Suffix-Feld. Als Beispiel zeigt der Standardinhalt des Felds "LDAP suffix" den Wert "ou=People,dc=my-domain,dc=com" an.

Falls neue Organisationseinheiten erstellt werden müssen, ersetzen Sie den Inhalt des Felds "LDAP suffix", um den Namen der Organisationseinheit anzugeben.

Das Format wird angezeigt als "ou=<organisational_unit>,dc=xxxxxxxxx,dc=com".

In dieser Demonstration lautet die Organisationseinheit für Benutzer "Personen" und die Organisationseinheit für Gruppen "Gruppen".

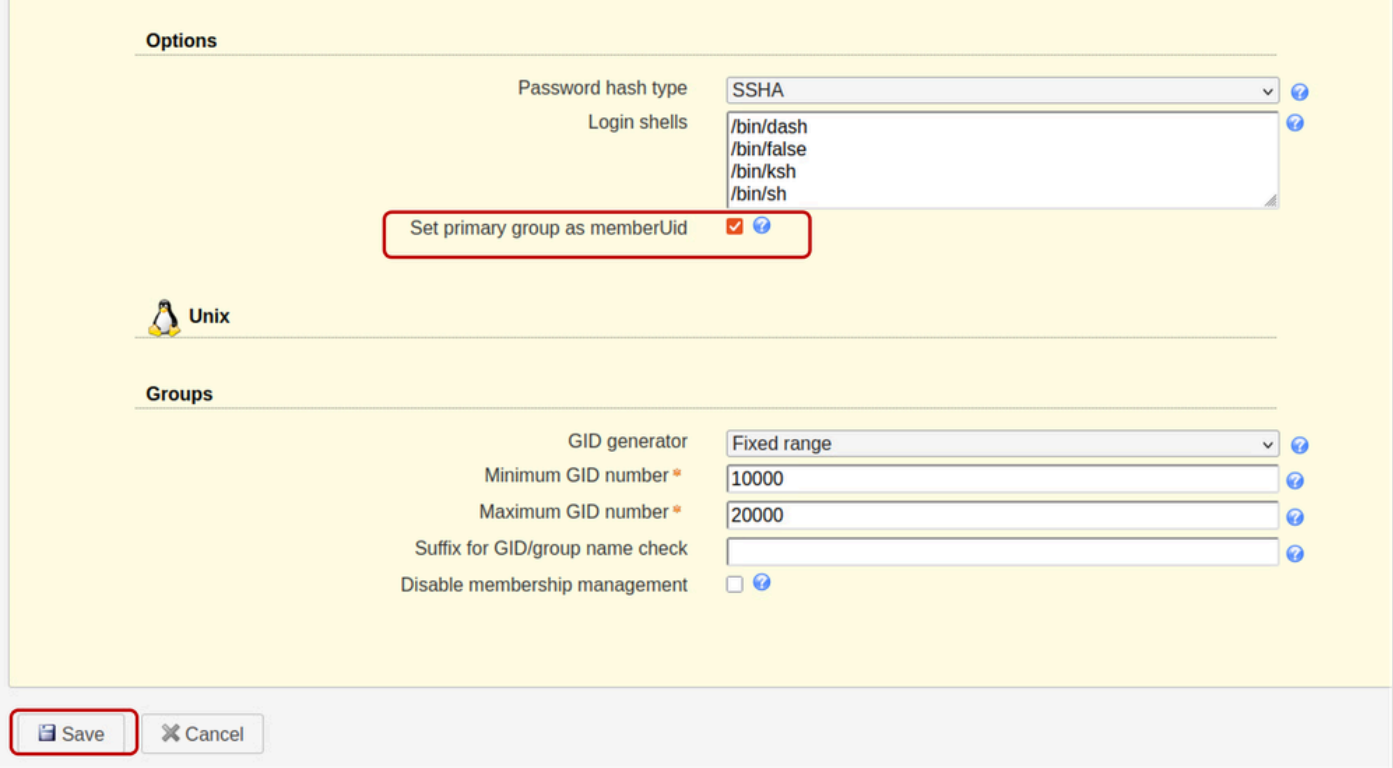
Speichern Sie die Konfiguration.



Scrollen Sie nach unten zum Options-Abschnitt und überprüfen Sie die Option "Set primary group as memberUid".

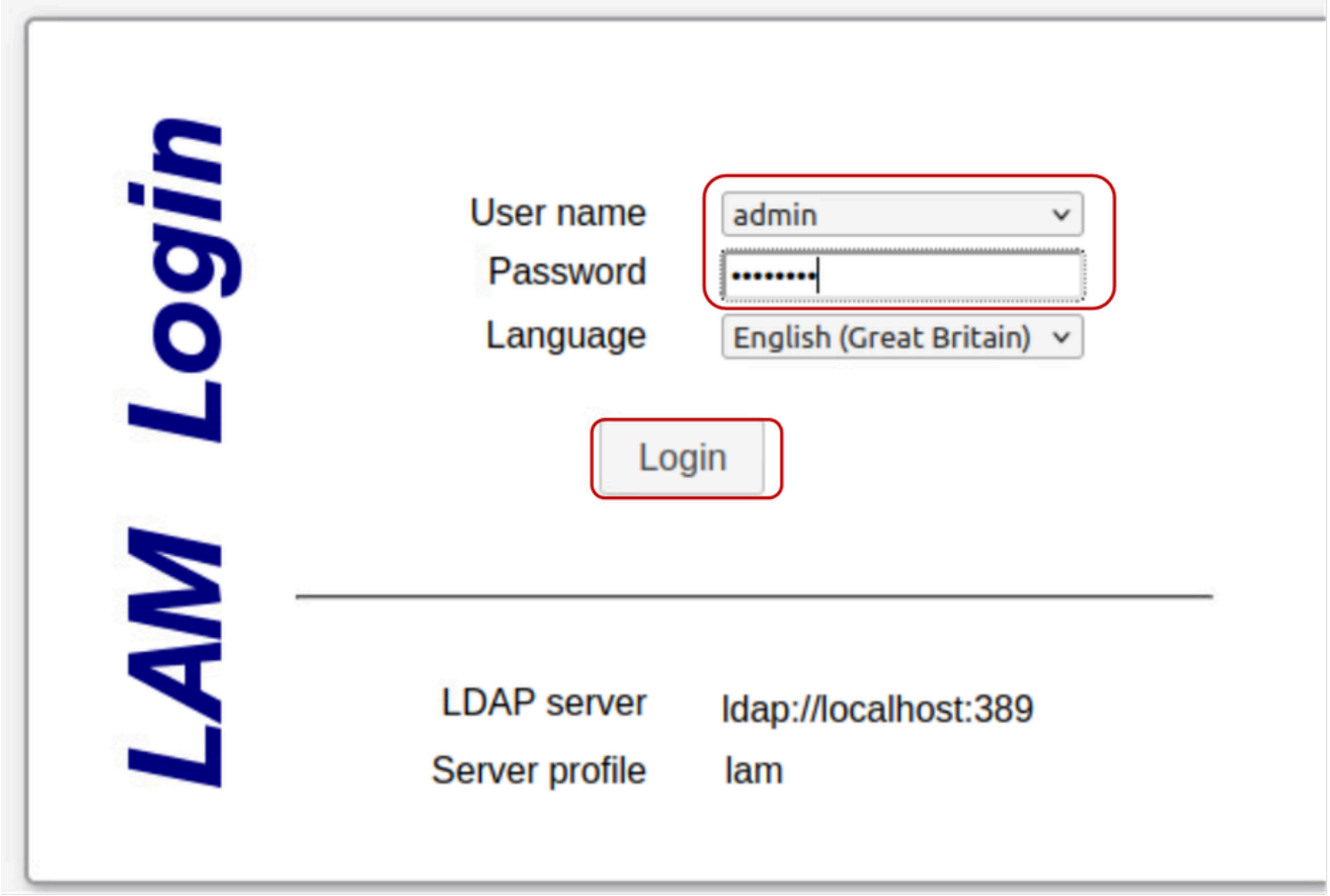
Standardmäßig ist die Option "Primäre Gruppe als memberUid festlegen" für Gruppenobjekte nicht festgelegt. Wenn Sie diese Option aktivieren, können Sie OpenLDAP "Primary group" (Primäre Gruppe) wie eine Standard-LDAP-Gruppe verwenden, auf die "memberUid" (Beispiel: In der UCS C-Serie (Serverkonfiguration). Wenn diese Option deaktiviert ist, schlägt die Anmeldung für Benutzer fehl, die zu einer primären Gruppe gehören.

Speichern Sie die Konfiguration.

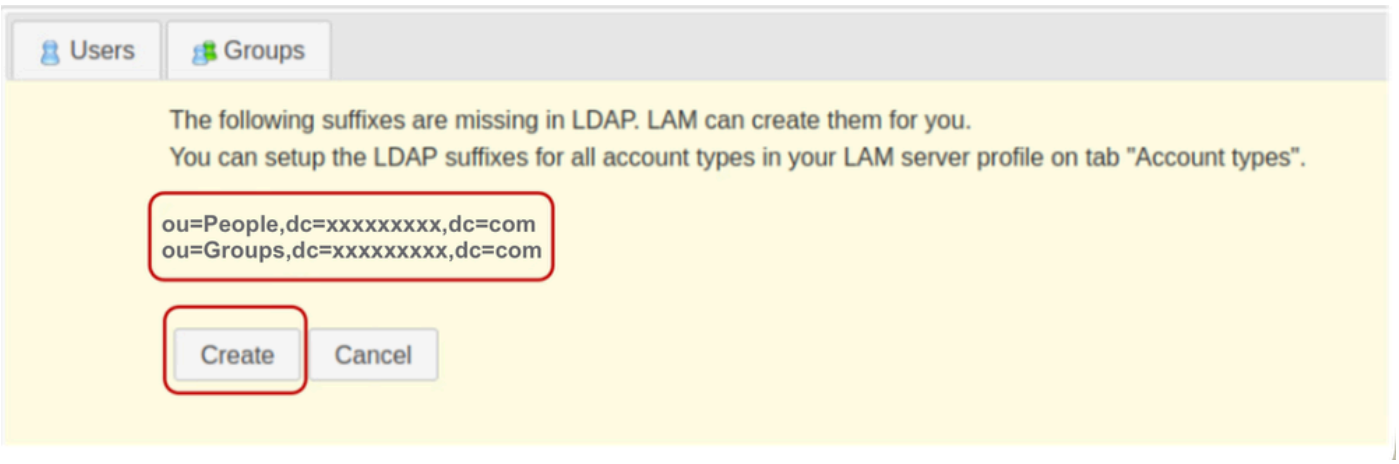


Schritt 5: Erstellen von Organisationseinheiten, Gruppen und Benutzern

Melden Sie sich beim LAM als "admin"-Benutzer mit demselben Kennwort an, das Sie während der Installation erstellt haben, um Benutzer und Gruppen zu erstellen, die zu den zuvor erstellten Organisationseinheiten (Personen und Gruppen) gehören:

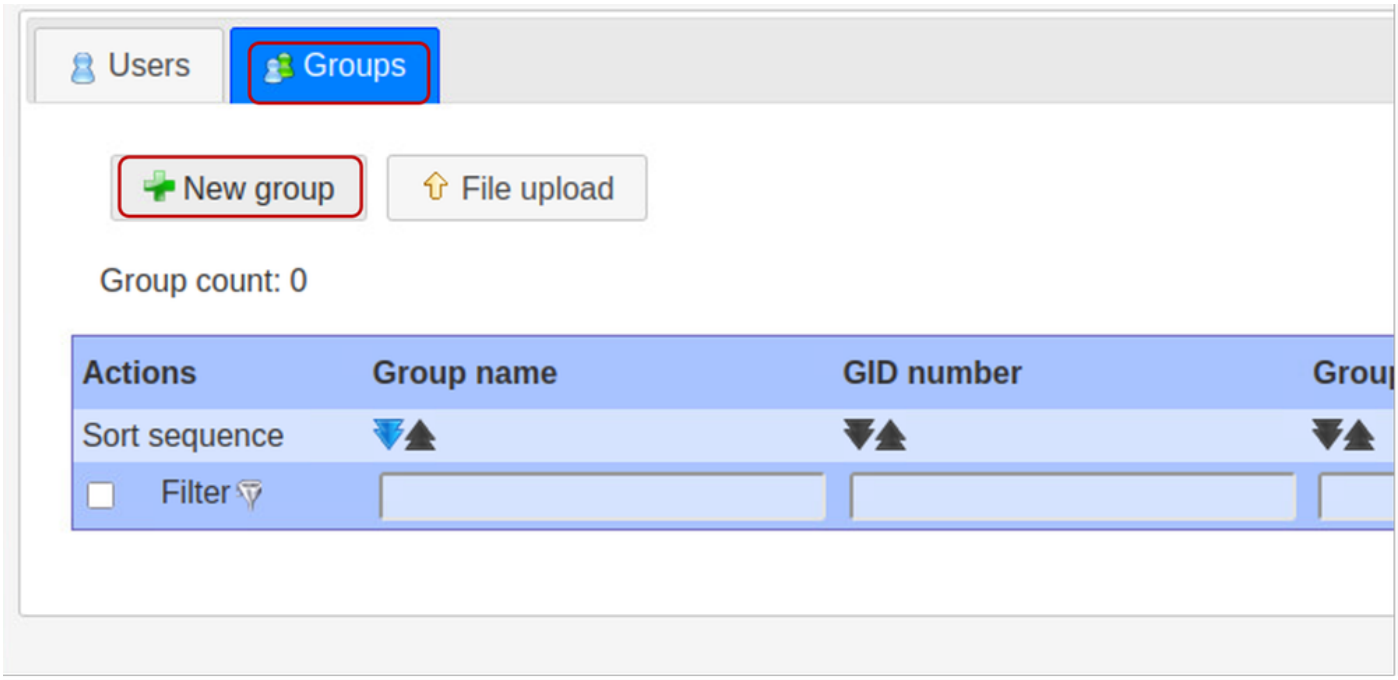


Erstellen Sie die zuvor im Abschnitt "LAM-Konfiguration" angegebenen OUs.
Klicken Sie auf Erstellen.



Erstellen Sie anschließend im LDAP-Kontomanager die "it"-Gruppe:

Wählen Sie die Registerkarte Gruppen und klicken Sie auf Neue Gruppe

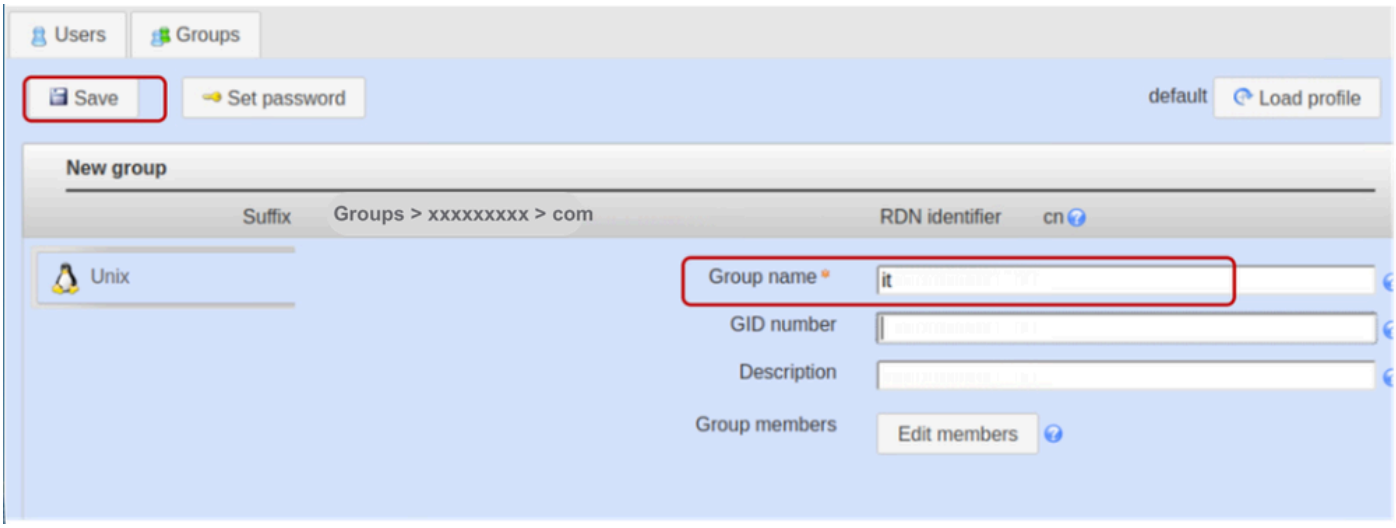


Setzen Sie den Gruppennamen auf "it".

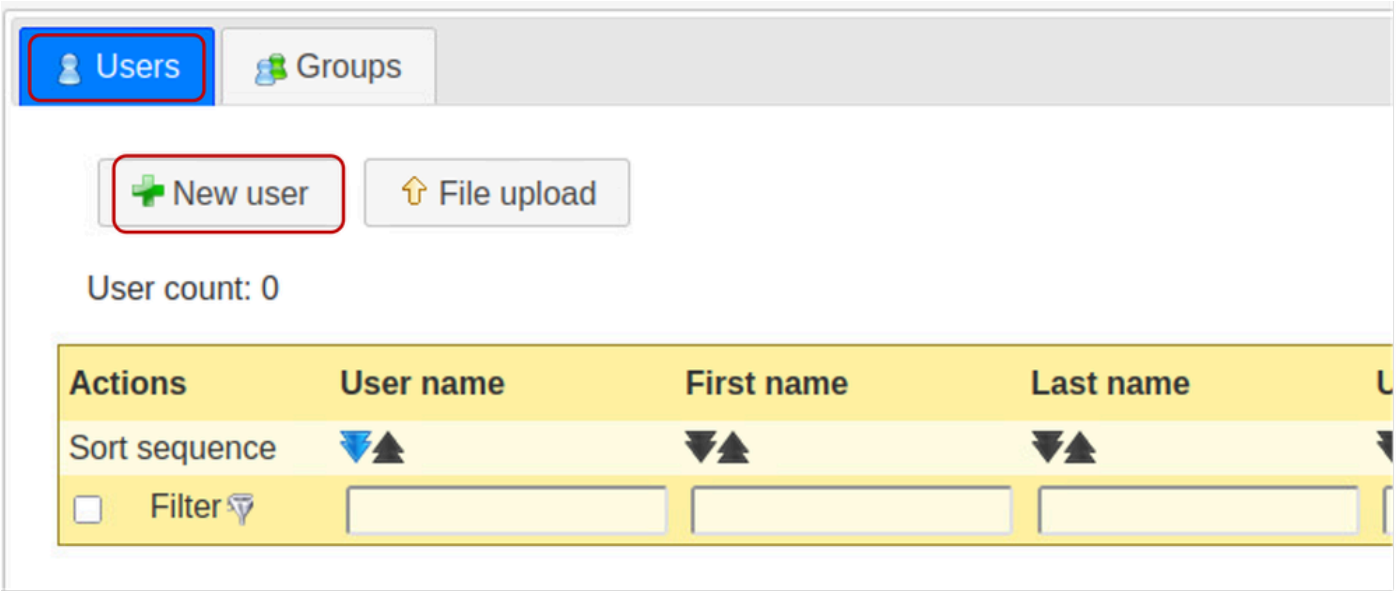
Anmerkung: Cisco UCS-Systeme sind im Allgemeinen ausfallsicher. Die Einhaltung von Namenskonventionen in Kleinbuchstaben ist jedoch eine Best Practice, um eine langfristige Interoperabilität zwischen verschiedenen LDAP-Serverinfrastrukturumgebungen sicherzustellen.

Lassen Sie das Feld "GID-Nummer" leer. Der LDAP Account Manager (LAM) wurde so konzipiert, dass in dieses Feld automatisch der nächste verfügbare Wert eingetragen wird.

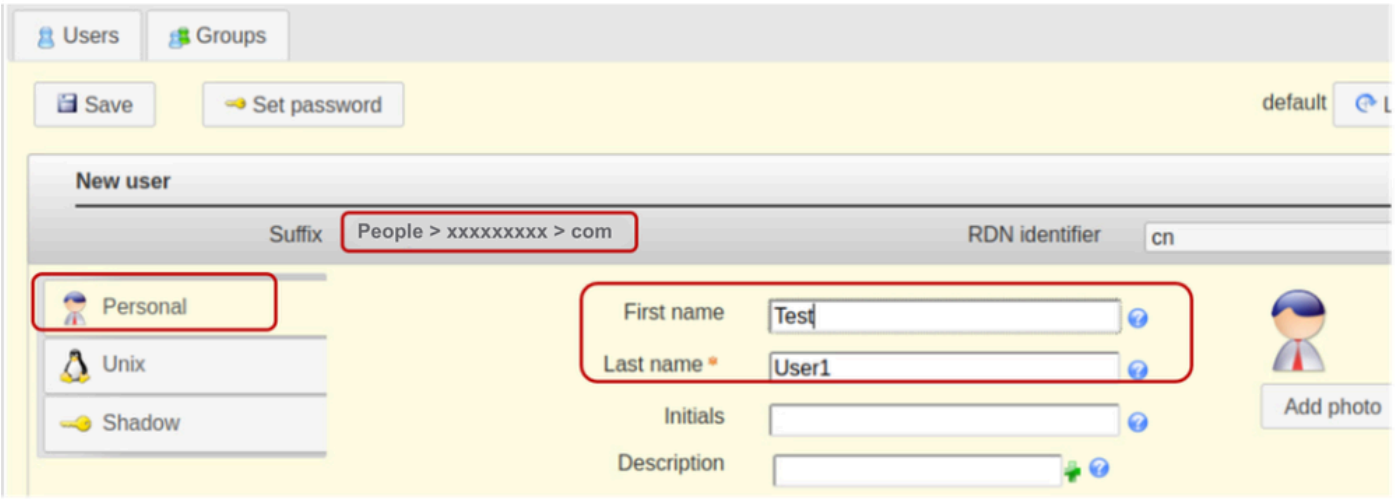
Geben Sie bei Bedarf eine Beschreibung ein, und klicken Sie auf Speichern.



Klicken Sie auf die Registerkarte "Benutzer", um Benutzerkonten zu erstellen, und wählen Sie "Neuer Benutzer" aus.



Füllen Sie die erforderlichen Felder für den Benutzer "testuser1" auf der Registerkarte "Personal" aus.

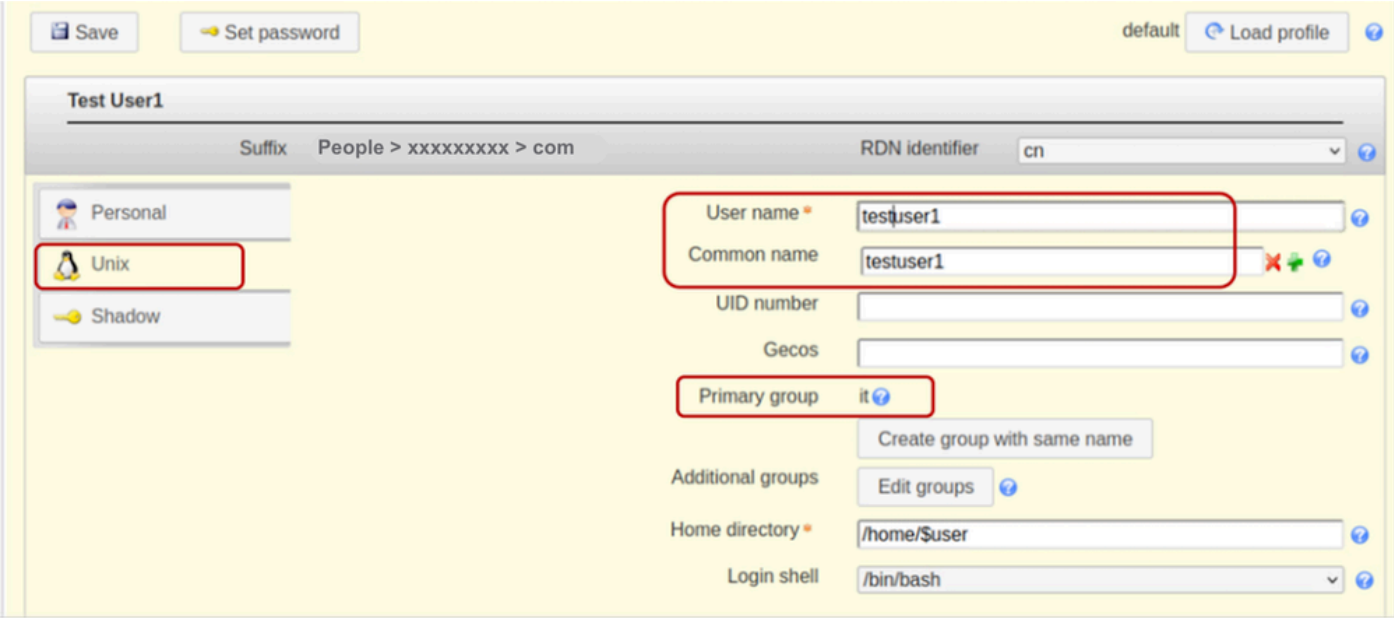


Wählen Sie die Registerkarte Unix aus, und fügen Sie testuser1 in das Feld Benutzername ein. Fügen Sie den Benutzer der Gruppe "it" hinzu.

Für diese Demonstration existiert nur die "it"-Gruppe, daher ist sie bereits vorausgefüllt.

Verwalten Sie die RDN-ID als "Common Name" (cn). Dadurch kann das System automatisch das Feld "Common Name" mit dem im Feld "User name" (Benutzername) angegebenen Wert ausfüllen.

Lassen Sie das Feld "UID-Nummer" leer, da LAM die verfügbaren Werte automatisch in das Feld einträgt.



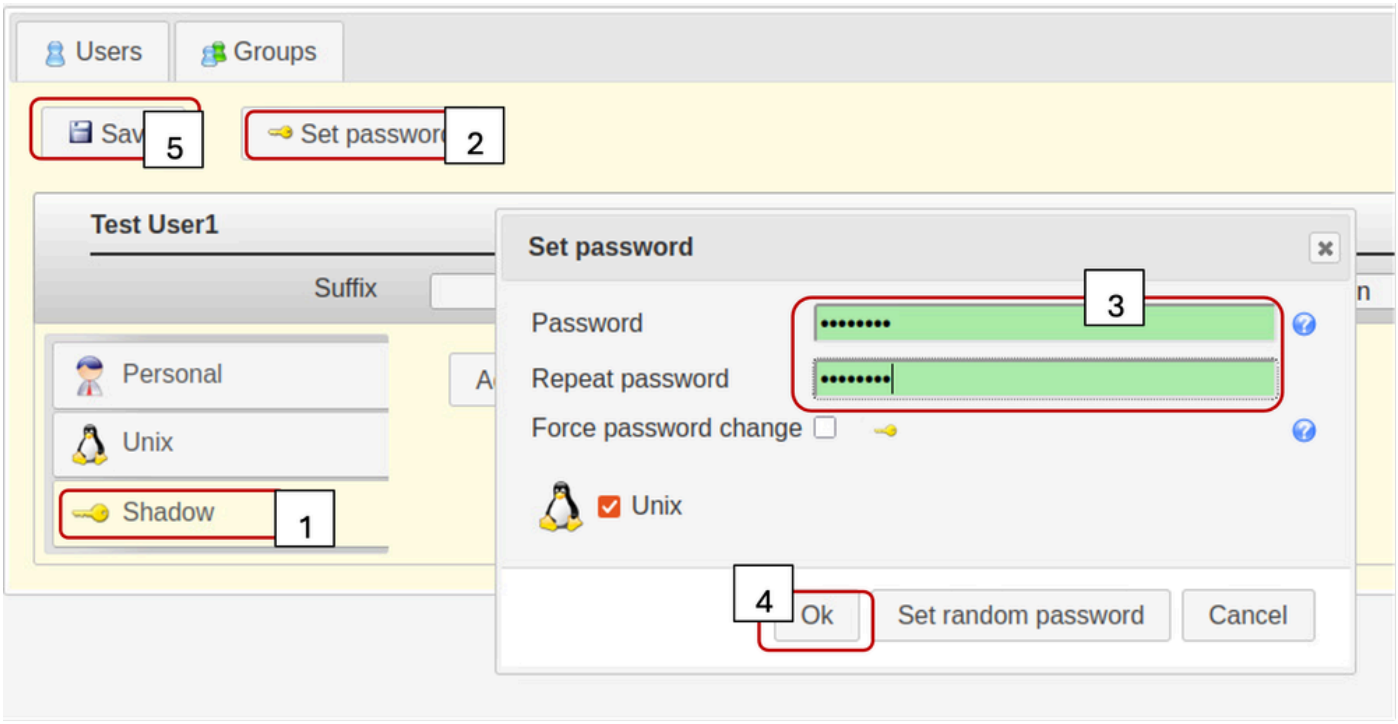
Wählen Sie die Registerkarte Schatten aus.

Die Schattenkontoerweiterung wird nicht verwendet.

Klicke auf "Passwort festlegen".

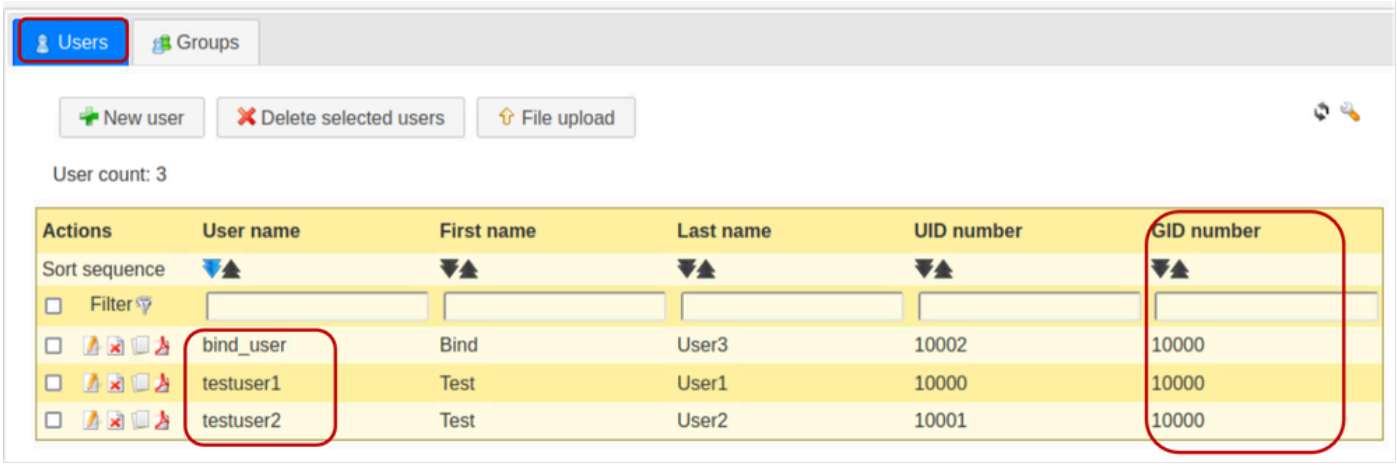
Benutzerkennwort festlegen

Klicken Sie auf OK und Speichern



Wiederholen Sie die zuvor beschriebenen Schritte, um das Benutzerkonto "testuser2" und das Konto "bind_user" zu erstellen.

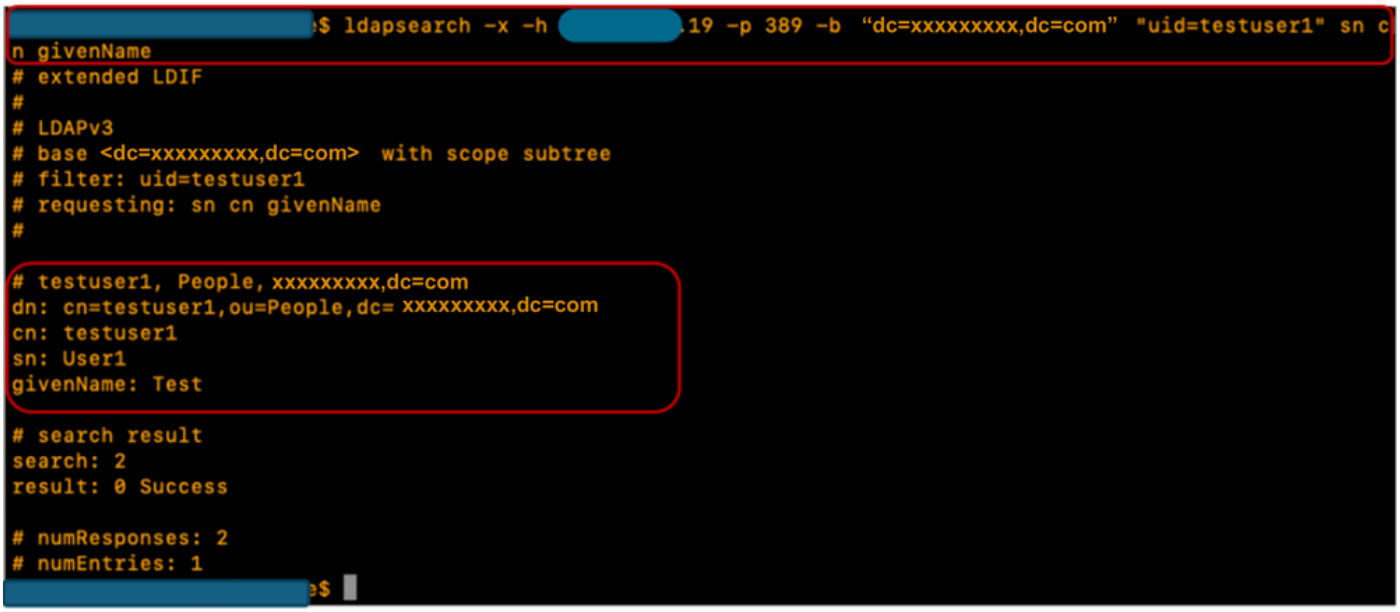
Klicken Sie auf die Registerkarte "Benutzer", um die Erstellung aller gewünschten Benutzer zu überprüfen. (Wenn Sie den gleichen Wert in der Spalte gidNumber haben, wird bestätigt, dass die erstellten Benutzer derselben Gruppe angehören.)



Schritt 6: Testet die lokale LDAP-Anmeldung

Melden Sie sich bei einem anderen Linux-basierten System an, das mit dem OpenLDAP-Server erreichbar ist.
Führen Sie den angegebenen ldapsearch-Befehl aus, um zu überprüfen, ob LDAP funktioniert:

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



Konfigurationsparameter auf CIMC

Bei CIMC anmelden

Wählen Sie im Navigationsbereich Admin, User Management und LDAP aus.

Füllen Sie die LDAP-Konfigurationsparameter wie folgt aus:

- LDAP aktivieren: Aktiviert
- Basis-DN: dc=xxxxxxxxx,dc=com

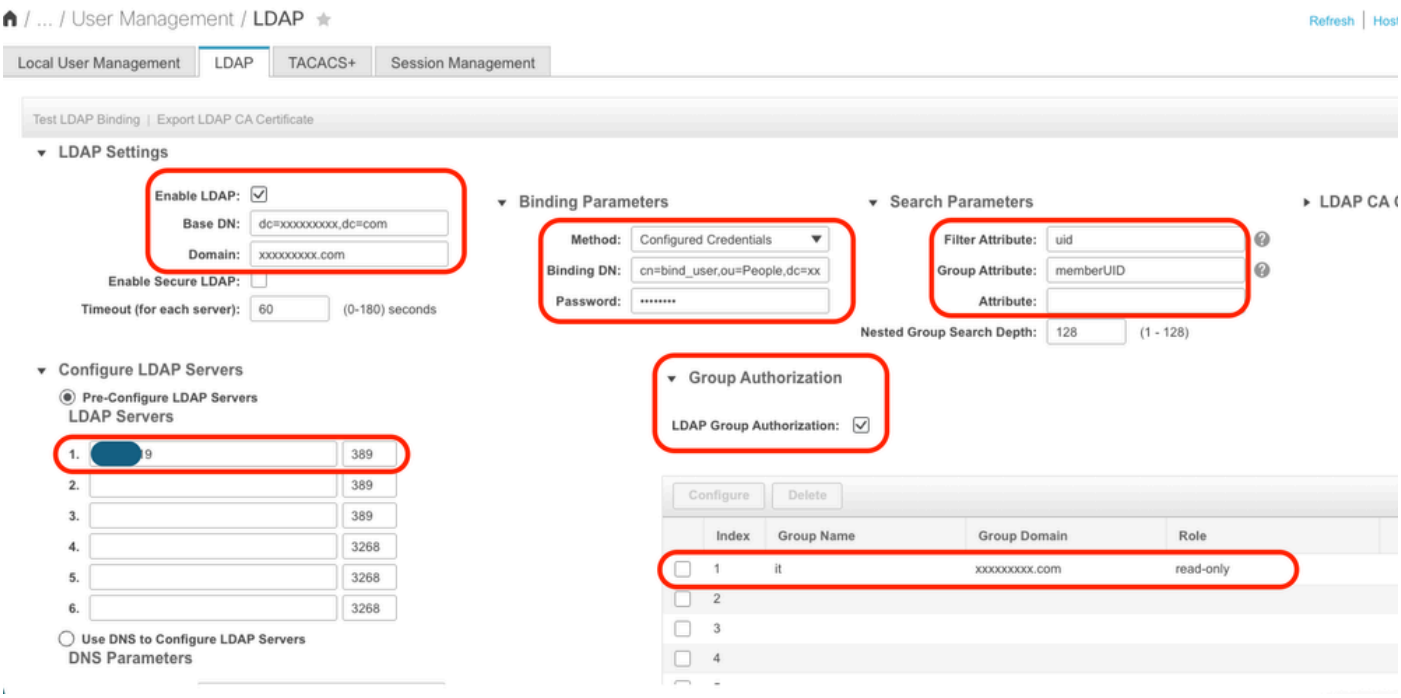
- Domäne: xxxxxxxxx.com

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

- Bindungsparameter: "Anmeldedaten" oder "Konfigurierte Anmeldedaten"
  - Wenn Sie die konfigurierten Anmeldeinformationen verwenden, fügen Sie die DN bind_user genau wie auf dem LDAP-Server konfiguriert hinzu:
    - Beispiel: cn=bind_user,ou=Benutzer,dc=xxxxxxxxx,dc=com

- Suchparameter:
  - Filterattribut: "cn" oder "uid"
  - Gruppenattribut: MitgliedUID

- LDAP-Gruppenautorisierung - Aktiviert
  - Gruppenname: es
  - Gruppendomäne: xxxxxxxxx.com
  - Rolle: schreibgeschützt (beliebige Rolle)



Speichern Sie die Konfiguration, und testen Sie die LDAP-Benutzeranmeldung.

Konfigurationsparameter in UCS Manager

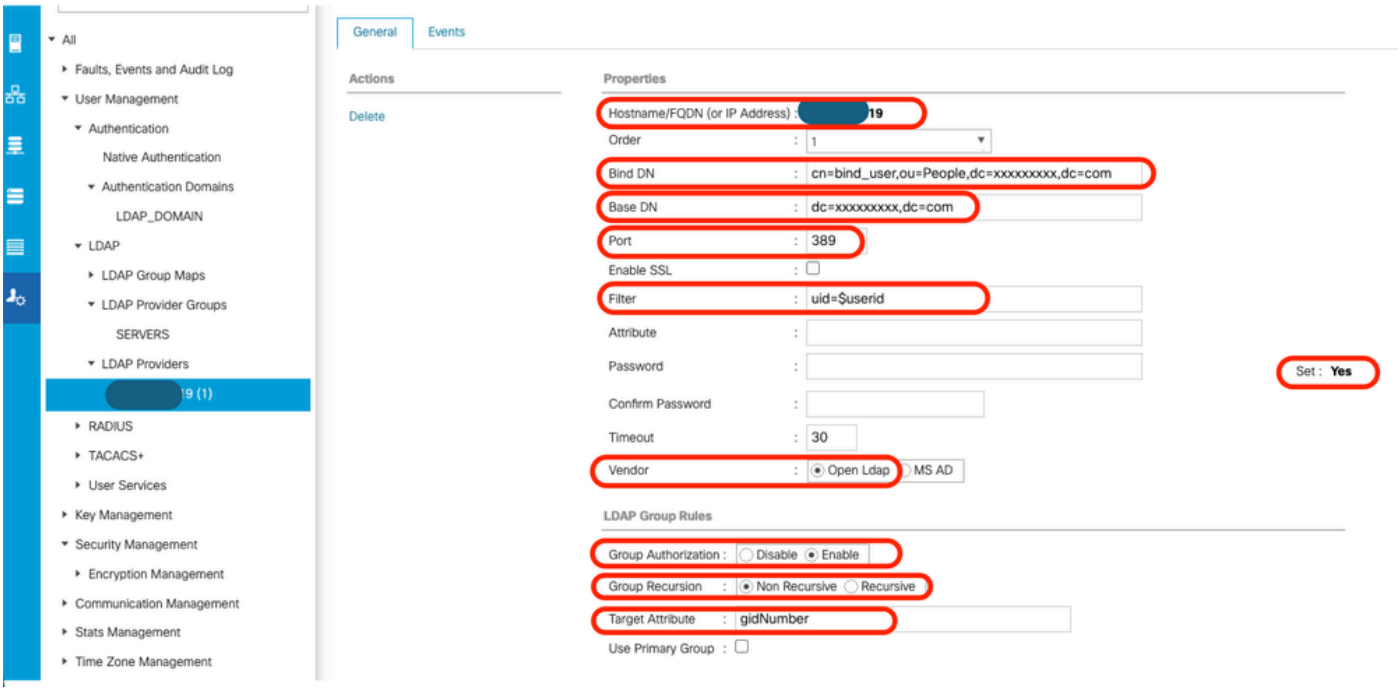
Bei UCS Manager anmelden

Wählen Sie im Navigationsbereich Admin, User Management und LDAP aus.

Füllen Sie die LDAP-Konfigurationsparameter wie folgt aus:

- LDAP-Anbieter:
  - Hostname: <FQDN oder IP-Adresse des LDAP-Servers>
  - Bind-DN: cn=bind_user,ou=Benutzer,dc=xxxxxxxxx,dc=com
  - Basis-DN: dc=xxxxxxxxx,dc=com
  - Anschluss: 389
  - SSL aktivieren: Deaktiviert
  - Filter: uid=$userid
  - Gruppenautorisierung: Aktiviert
  - Gruppenrekursion: Nicht rekursiv

    - Zielattribut: GIDummer
- LDAP-Gruppenzuordnungen:
    - LDAP-Gruppen-DN: 10000 <gidNumber für "it"-Gruppe>

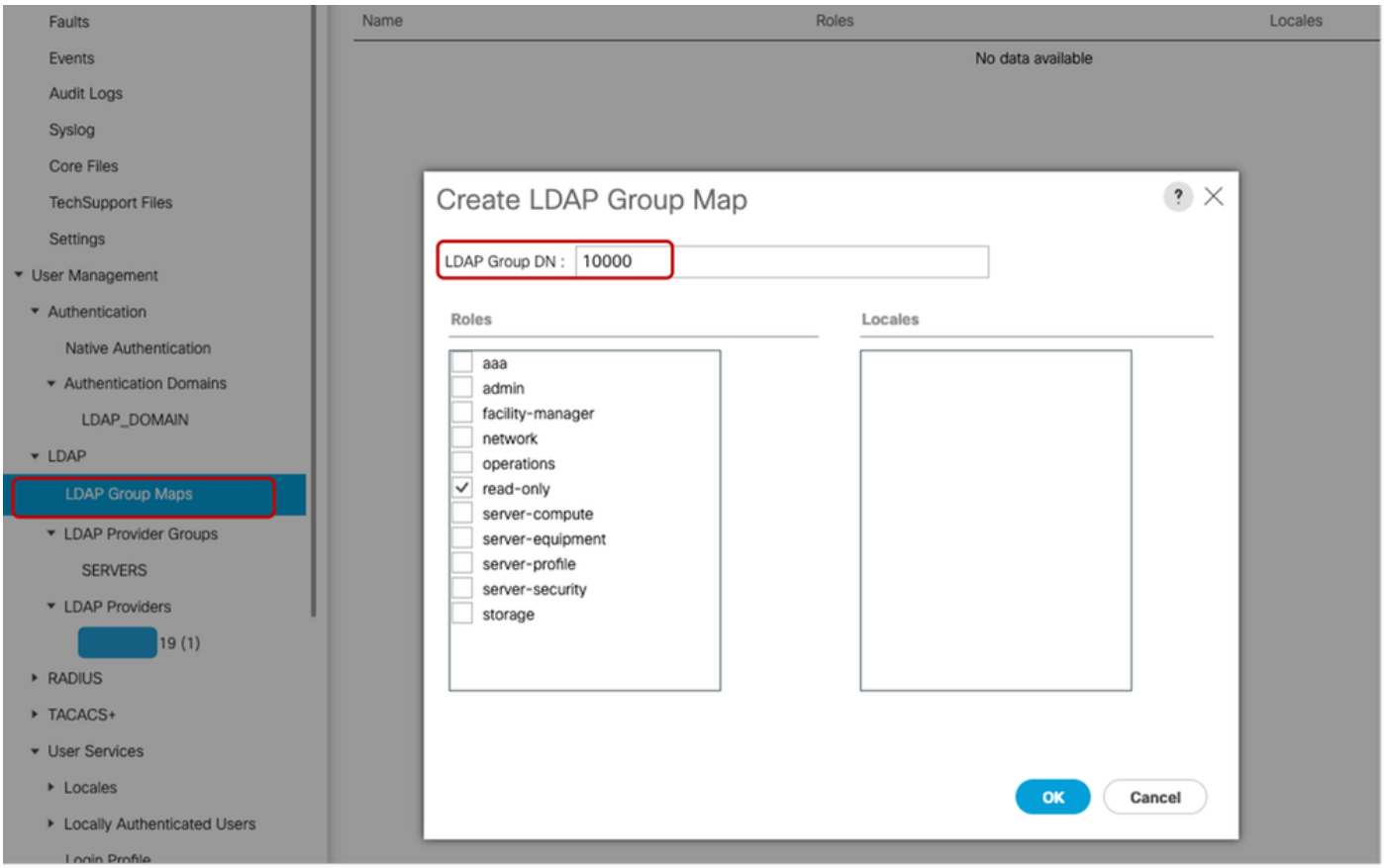


Unter Alle >> Benutzerverwaltung > LDAP >> LDAP-Anbieter >> LDAP-Gruppenregeln lautet das standardmäßige Zielattribut für den UCS Manager "memberOf". Standardmäßig ist dieses Attribut bei OpenLDAP-Servern nicht aktiviert. Wenn Sie daher den Wert für das Zielattribut auf "memberOf" setzen (oder leer lassen), können sich Benutzer nicht anmelden, da der OpenLDAP-Server den angeforderten Attributwert nicht erkennt.

In diesem Beispiel wurde der Wert "Target Attribute" auf "gidNumber" gesetzt.

Fügen Sie den konfigurierten LDAP-Anbieter einer LDAP-Anbietergruppe hinzu. Für diese Demonstration wurde die LDAP-Anbietergruppe "SERVER" erstellt.

Beim Konfigurieren der "LDAP Group Maps" in "All >> User Management >> LDAP >> LDAP Group Maps>" wird der gidNumber-Wert (in diesem Fall "10000") als "Group DN Map" verwendet, wie dargestellt:



Konfigurieren Sie eine LDAP-Authentifizierungsdomäne (LDAP_DOMAIN) unter "Alle >> Benutzerverwaltung >> Authentifizierung >> Authentifizierungsdomänen", und verweisen Sie dabei auf die LDAP-Anbietergruppen und testen Sie die LDAP-Benutzeranmeldung.

Anmerkung: Wenn das memberOf-Attribut für die Erfüllung bestimmter Umgebungsanforderungen oder zum Implementieren der Funktion "Gruppenrekursion" erforderlich ist, wird empfohlen, die zweite unten angegebene Konfigurationsoption zu verwenden. Hierfür ist LDAP mit aktivierten Overlay-Erweiterungen erforderlich.

LDAP Account Manager (LAM) unterstützt zwar die Overlay-Konfiguration, es ist jedoch eine entsprechende Lizenzierung erforderlich.

Weitere Informationen zum Konfigurieren von LDAP mithilfe von LAM finden Sie in der offiziellen LDAP Account Manager-Dokumentation.

Option 2: OpenLDAP mit Ubuntu CLI-Tools und Overlays konfigurieren

Um OpenLDAP für die UCS Manager-Authentifizierung verwenden zu können, sind zwei Overlays erforderlich, die sicherstellen, dass die Gruppen Benutzern auf eine für das UCS-System (UCS Manager und CIMC) verständliche Weise zugeordnet werden.

Die Konfiguration auf der OpenLDAP-Seite erfordert Folgendes:

- "member of"-Overlay: Dieses Overlay erstellt eine Zuordnung zwischen Benutzern und Gruppen, sodass das memberOf-Attribut im Rahmen dieser Abfrage angefordert werden kann, wenn eine Benutzer-DN abgefragt wird. Standardmäßig kein Attribut für Benutzer für die Gruppenmitgliedschaft, es sei denn, das Mitglied des Overlays wird zu openLDAP hinzugefügt
- Überlagerung "verfeinern": Dieses Overlay ist so konfiguriert, dass es überprüft, ob Einträge im Memberattribut in Gruppenobjekten mit dem memberOf-Attribut von Benutzerobjekten synchronisiert bleiben. Ohne diesen Dienst können verwaiste DNs im Gruppenobjekt verbleiben, wenn ein Benutzer gelöscht wird, ohne die Gruppe ebenfalls zu ändern. Der Raffinationsservice sorgt für Konsistenz in beide Richtungen.

Schritt 1: Erste Net-Tools und Konfiguration des Linux-Server-Hostnamens

Wiederholen Sie Schritt 1 in Option 1.

Schritt 2: SLAPD installieren

Wiederholen Sie Schritt 2 in Option 1. (Mit Ausnahme der PHP- und Apache-Installation, da Option 2 nicht erfordert, dass sie funktionieren - kein LAM)

Stellen Sie sicher, dass die erforderlichen Ports über die Ubuntu-Firewall zugelassen werden.

Schritt 3: 'memberOf' auf dem LDAP-Server installieren

Überprüfen, ob das Overlay "memberOf" installiert ist

```
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
```

Um das "memberOf"-Overlay zu installieren, erstellen Sie eine .ldif-Datei mit dem Namen

ldap.mitgliedof.load.ldif (verwenden Sie eine beliebige Namenskonvention), und fügen Sie die angegebene Konfiguration hinzu:

```
cat <

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

Fügen Sie die Konfiguration in der Datei "ldap.mitgliedof.load.ldif" mithilfe des angegebenen Befehls zum LDAP-Profil hinzu:

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

Konfiguriert das memberOf-Modul und den olcDatabase-Eintrag je nach Linux-Distributionen so, dass sie den Bereitstellungsanforderungen entsprechen.

Zwei obligatorische Attributwerte sind "olcDatabase={1}mdb" und "groupOfNames", wie unten gezeigt.

Erstellen Sie die Datei "ldap.mitgliedof.config.ldif", füllen Sie die Attribute aus, und importieren Sie den Inhalt in das LDAP-Profil.

```
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
```

Schritt 4: 'feint'-Overlay auf dem LDAP-Server installieren

Als Nächstes installieren und an openldap anpassen:

Erstellen Sie eine LDIF-Datei mit dem Namen ldap.rafft.load.ldif (verwenden Sie eine beliebige Namenskonvention), und fügen Sie die angegebene Konfiguration hinzu:

```
cat <


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

Importieren Sie die Konfiguration in der Datei ldap.rafft.load.ldif mithilfe des folgenden Befehls in das LDAP-Profil:

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

Konfigurieren Sie die Anpassung, die die referenzielle Integrität zwischen Gruppen und Benutzern aufrechterhält.

Konfiguriert das Anpassungsmodul und seinen olcDatabase-Eintrag, um die Bereitstellungsanforderungen zu erfüllen.

Erstellen Sie die Datei "ldap.rafft.config.ldif", und importieren Sie deren Inhalt in das LDAP-Profil.

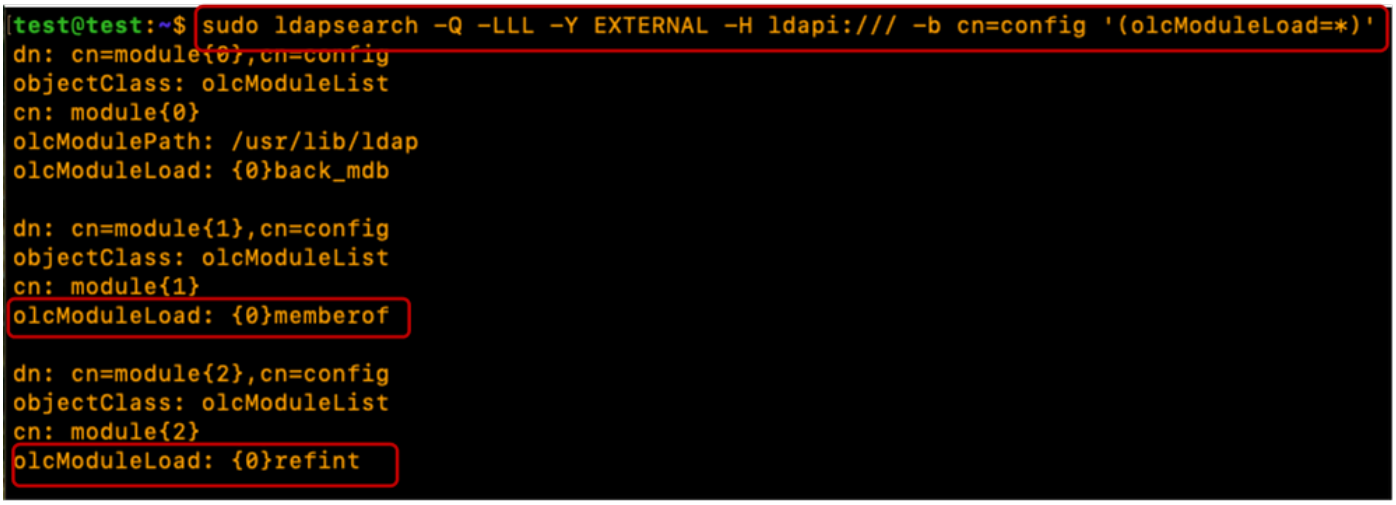
```
cat <
```

```
      ./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
```

Bei der Installation beider Plugins/Erweiterungen ist die Ausgabe des angegebenen ldapsearch-Befehls ähnlich der unten gezeigten Ausgabe:

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



Wenn beide Plugins/Erweiterungen konfiguriert sind, ist die Ausgabe des angegebenen ldapsearch-Befehls ähnlich wie die angezeigte Ausgabe:

```
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
```

Starten Sie den slapd-Dienst neu, damit die neu installierten Plugins/Module verwendbar sind:

```
sudo systemctl restart slapd
```

Schritt 5: Erstellen von Organisationseinheiten, Benutzern und Gruppen

Erstellen Sie Organisationseinheiten (für Benutzer und Gruppen), Benutzer und Gruppen.

Erstellen Sie die Benutzer- (Personen) und Gruppen- (Gruppen-) OUs, und importieren Sie sie in das LDAP-Profil. Hierfür ist das Kennwort des "admin"-Kontos erforderlich:

```
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
```

Erstellen Sie die Benutzer (testuser1, testuser2 und bind_user), ordnen Sie sie ihren jeweiligen OUs (People) zu, fügen Sie sie mithilfe von gidNumbers zu ihren Gruppen hinzu (Best Practice), und importieren Sie die Benutzer in das LDAP-Profil.

```
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:~$
```

Erstellen Sie die Gruppen (it), ordnen Sie sie ihren jeweiligen OUs (Gruppen) zu, ordnen Sie Gruppenmitgliedern (testuser1, testuser2) zu, und importieren Sie sie in das LDAP-Profil:

```
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
```

Anmerkung: Auch wenn das memberOf-Attribut bei der Erstellung von Benutzern oder Gruppen nicht explizit definiert wird, generiert und verwaltet das System diesen Verweis automatisch. Sobald der Benutzer einer Gruppe zugeordnet wurde, spiegelt das memberOf-Attribut diese Mitgliedschaften automatisch wieder, sodass sichergestellt ist, dass das Verzeichnis mit der aktuellen Zugriffsstruktur synchronisiert bleibt.

Schritt 6: Testet die lokale LDAP-Anmeldung

Überprüfen Sie die Benutzeranmeldung beim LDAP-Server mit dem angegebenen Befehl (je nach Umgebung müssen Sie die Anmeldeparameter ersetzen):

```
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:~$
```

Konfigurationsparameter auf CIMC

Bei CIMC anmelden

Wählen Sie im Navigationsbereich Admin, User Management und LDAP aus.

Füllen Sie die LDAP-Konfigurationsparameter wie folgt aus:

- LDAP aktivieren: Aktiviert
- Basis-DN: dc=xxxxxxxxx,dc=com

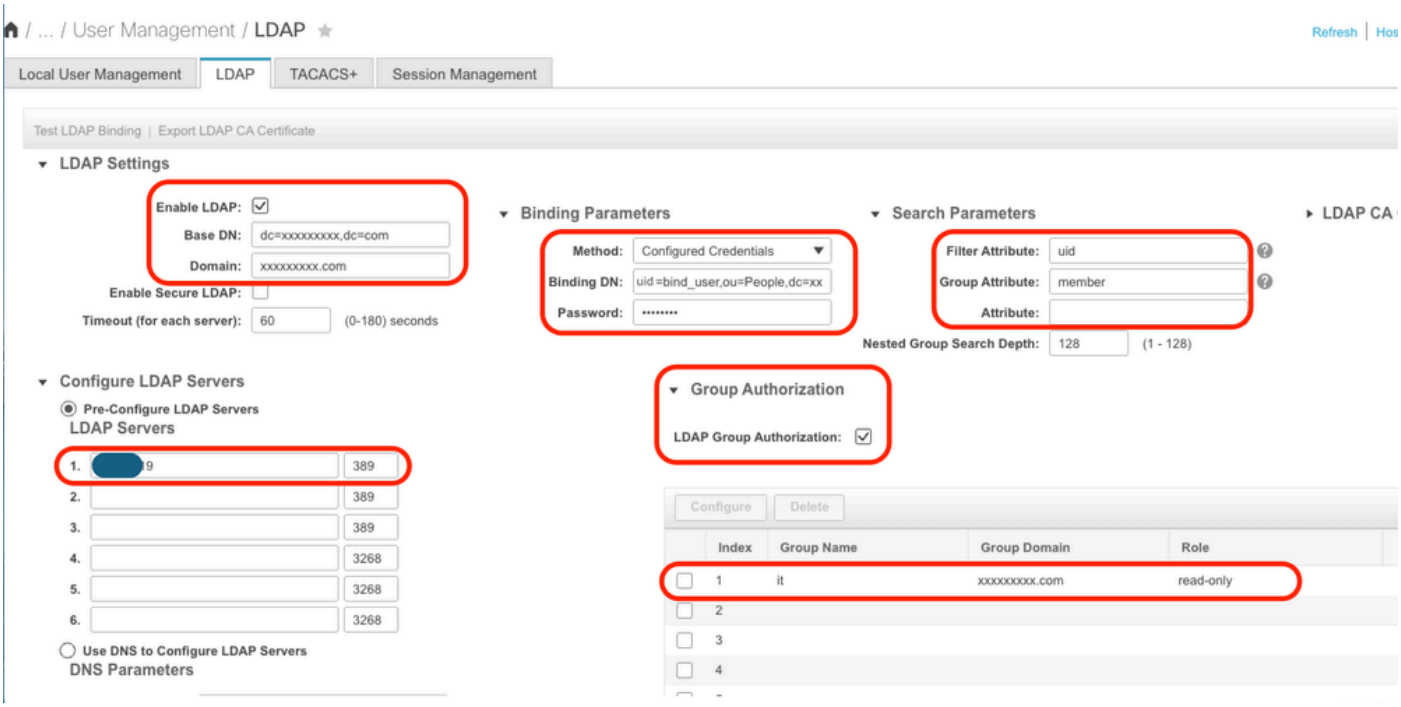
- Domäne: xxxxxxxxx.com

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

- Bindungsparameter: Möglicherweise "Anmeldeinformationen" oder "Konfigurierte Anmeldeinformationen"
    - Wenn Sie die konfigurierten Anmeldeinformationen verwenden, fügen Sie die DN bind_user genau wie auf dem LDAP-Server konfiguriert hinzu:
    - Beispiel: "cn=bind_user,ou=People,dc=xxxxxxxxx,dc=com" oder "uid=bind_user,ou=People,dc=xxxxxxxxx,dc=com"

- Suchparameter:
    - Filterattribut: "cn" oder "uid"
    - Gruppenattribut: Mitglied

- LDAP-Gruppenautorisierung - Aktiviert
    - Gruppenname: es
    - Gruppendomäne: xxxxxxxxx.com
    - Rolle: schreibgeschützt (jede bevorzugte Rolle)



Speichern Sie die Konfiguration, und testen Sie die LDAP-Benutzeranmeldung.

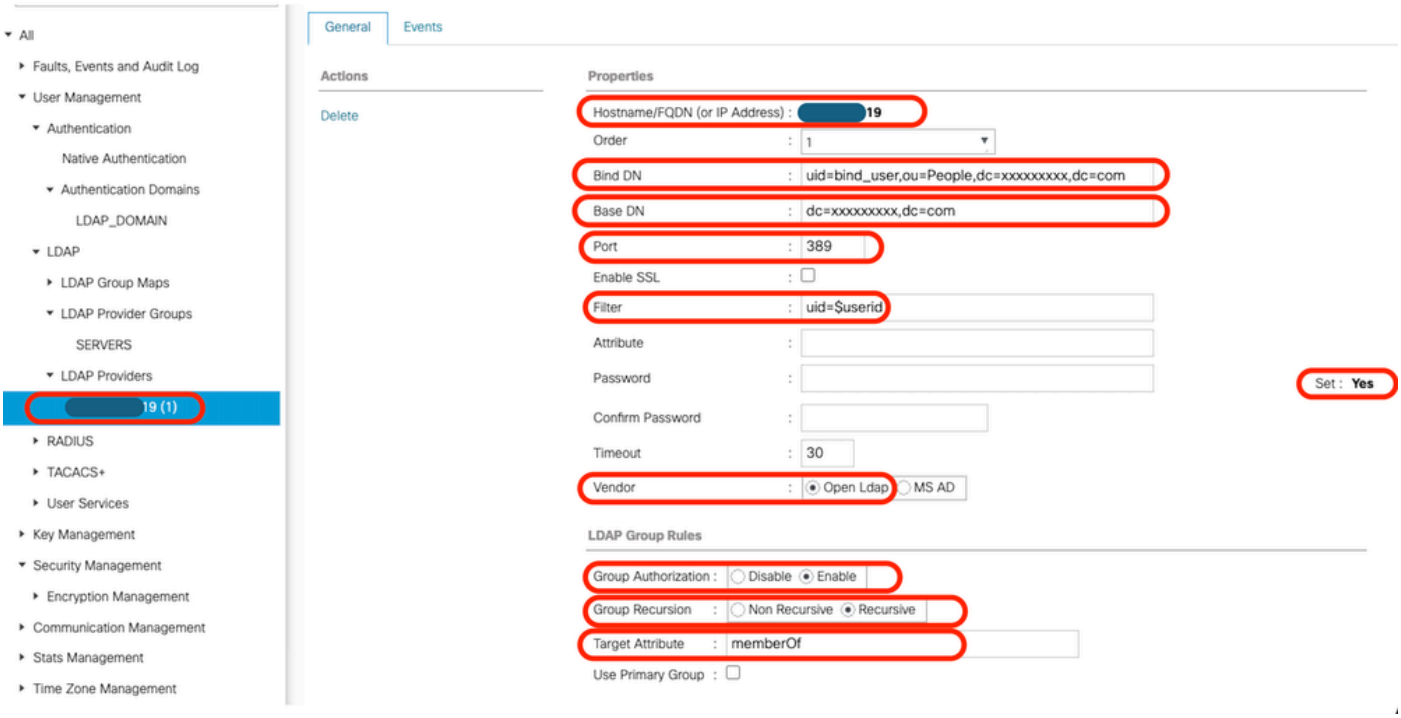
Konfigurationsparameter in UCS Manager

Bei UCS Manager anmelden

Wählen Sie im Navigationsbereich Admin, User Management und LDAP aus.

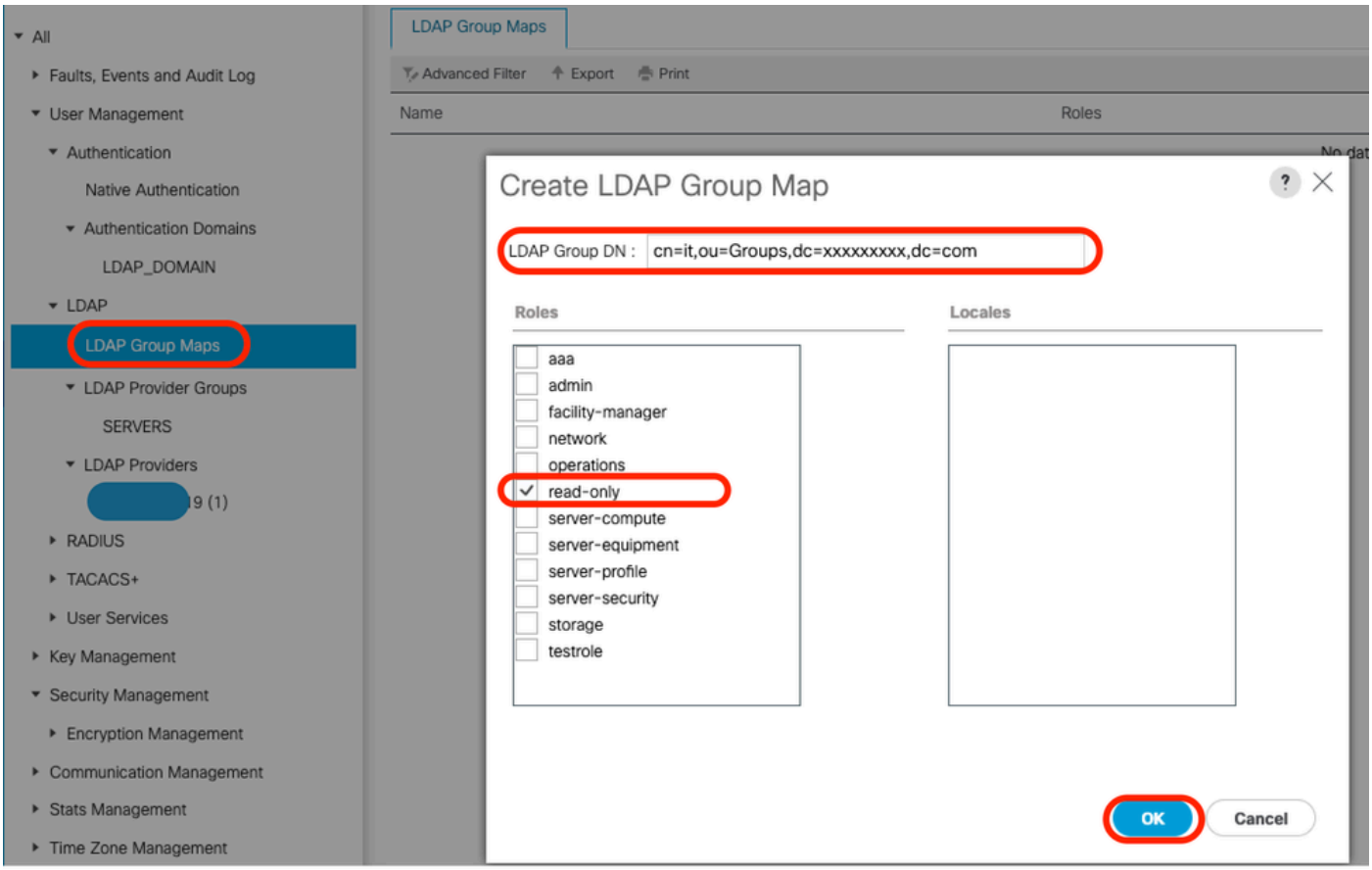
Füllen Sie die LDAP-Konfigurationsparameter wie folgt aus:

- LDAP-Anbieter:
  - Hostname: <FQDN oder IP-Adresse des LDAP-Servers>
  - Bind-DN: uid=bind_user,ou=Benutzer,dc=xxxxxxxxx,dc=com
  - Basis-DN: dc=xxxxxxxxx,dc=com
  - Anschluss: 389
  - SSL aktivieren: Deaktiviert
  - Filter: uid=$userid
  - Gruppenautorisierung: Aktiviert
  - Gruppenrekursion: Rekursiv
  - Zielattribut: MitgliedVon
- LDAP-Gruppenzuordnungen:
  - LDAP-Gruppen-DN: cn=it,ou=Groups,dc=xxxxxxxxx,dc=com



Fügen Sie den konfigurierten LDAP-Anbieter einer LDAP-Anbietergruppe hinzu. Für diese Demonstration wird die LDAP-Anbietergruppe "SERVER" verwendet.

Konfigurieren Sie die LDAP-Gruppenzuordnungen, indem Sie eine vom LDAP-Server abgerufene "LDAP-Gruppen-DN" hinzufügen.



Konfigurieren Sie eine LDAP-Authentifizierungsdomäne (LDAP_DOMAIN) unter "Alle >> Benutzerverwaltung >> Authentifizierung >> Authentifizierungsdomänen", und verweisen Sie auf die LDAP-Anbietergruppen (SERVER), und testen Sie die LDAP-Benutzeranmeldung.

Als Nächstes betrachten wir die Einrichtung derselben (mit Overlay) in einer separaten Linux-Distribution (CentOS 10)

Szenario 2: CentOS Stream 10 - Fedora

Die Konfigurationsverfahren für das Lightweight Directory Access Protocol (LDAP) variieren je nach der zugrunde liegenden Betriebssystemversion. Dieser Abschnitt behandelt die Implementierung von LDAP in CentOS Stream 10.

Während viele Linux-Distributionen OpenLDAP verwenden, verwenden CentOS Stream 10 und moderne Fedora-basierte Systeme den 389 Directory Server (389 DS) als Standard-LDAP-Provider.

Anmerkung: Obwohl 389 DS als Nachfolger von OpenLDAP innerhalb der CentOS- und Red Hat-Ökosysteme gilt, sind die beiden Lösungen nicht direkt austauschbar. Die jeweiligen Verzeichnisstrukturen, Konfigurationsdateien und Betriebsumgebungen unterscheiden sich erheblich.

Dieses Handbuch enthält die erforderlichen Schritte, um LDAP mit 389 DS in einer CentOS Stream 10-Umgebung erfolgreich zu konfigurieren.

Option 1: LDAP mit 389 Directory Server auf CentOS-Stream 10 konfigurieren

Schritt 1: Erstinstallation

Wiederholen Sie Schritt 1 in Szenario 1, Option 1.

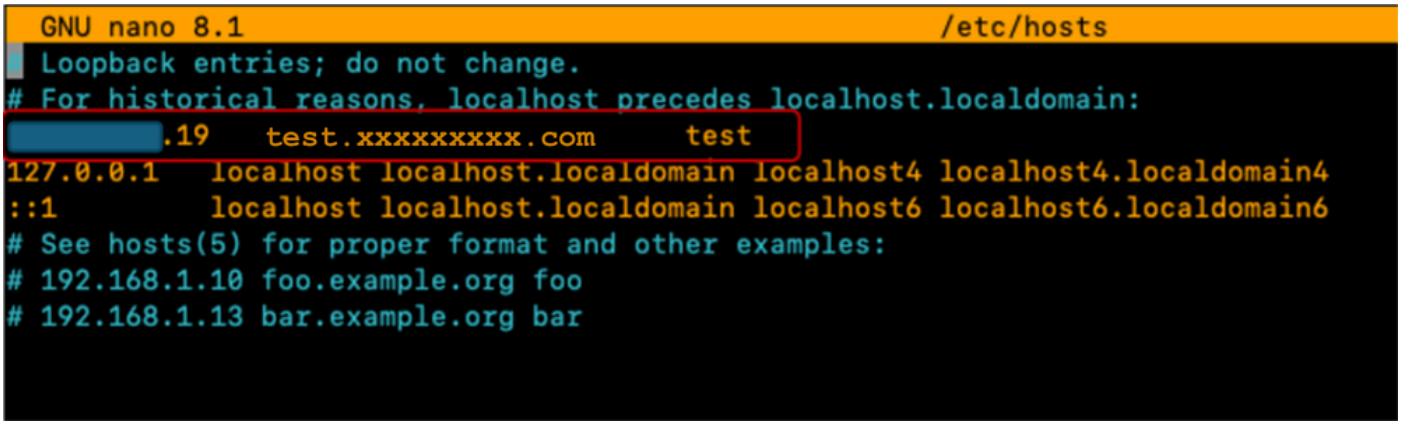
CentOS-Systeme verwenden die APT-Paketverwaltungs-Suite nicht. Um die erforderlichen Softwareinstallationen auf CentOS Stream 10 durchzuführen, verwenden Sie den dnf (Dandified YUM) oder yum Paketmanager

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

Überprüfen Sie die IP-Adresse des Servers mit dem Befehl "ifconfig".

Fügen Sie die Server-IP-Adresse der Datei "/etc/hosts" zusammen mit dem vollqualifizierten Domänennamen des Servers (z. B. test.xxxxxxxxx.com in dieser Übung) und dem Hostnamen (z. B. test) im unten angegebenen Format hinzu:

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



Aktualisieren Sie die Datei "/etc/hostname", indem Sie deren Inhalt durch den Hostnamen (test) ersetzen.

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

Damit diese Änderungen wirksam werden, muss der Server neu gestartet werden.

```
sudo reboot
```

Phase 2: Installation des EPEL repo- und 389 Server-Pakets

Installieren und Aktualisieren Sie das EPEL-Repository.

Installieren Sie das 389 Directory Server-Paket.

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

Erstellen Sie eine Verzeichnisvorlagendatei, die die gewünschten Parameter für die LDAP-Servereinstellungen enthält:

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

Überprüfen des Inhalts der erstellten Vorlagendatei (ldapconfig.conf)

```
sudo cat ldapconfig.conf
```

Bearbeiten Sie die Vorlage ldapconfig.conf.

```
sudo nano ldapconfig.conf
```

Fügen Sie die angegebenen Konfigurationseinträge in die Datei ein, und speichern Sie die Änderungen.

Hinweis: Je nach den spezifischen Anforderungen oder Anforderungen der jeweiligen Umgebung können verschiedene Änderungen erforderlich sein.

In diesem Beispiel werden die Basiskonfigurationen für diese Demonstration erläutert.

```
[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
```

Die Vorlagendatei definiert die Konfigurationsparameter für die "localhost"-Verzeichnisinstanz. Dazu gehört das Festlegen des Administrationsbenutzers ("admin"), des zugehörigen Kennworts und des Domänenkontexts ("xxxxxxxxx.com").

Erstellen Sie die Verzeichnisinstanz "localhost" mit der zuvor bearbeiteten Vorlage. Mit dem angegebenen Befehl wird der LDAP-Verzeichnisserver erstellt und gestartet:

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

Überprüfen, ob der LDAP-Dienst auf dem Server ausgeführt wird

```
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:~$
```

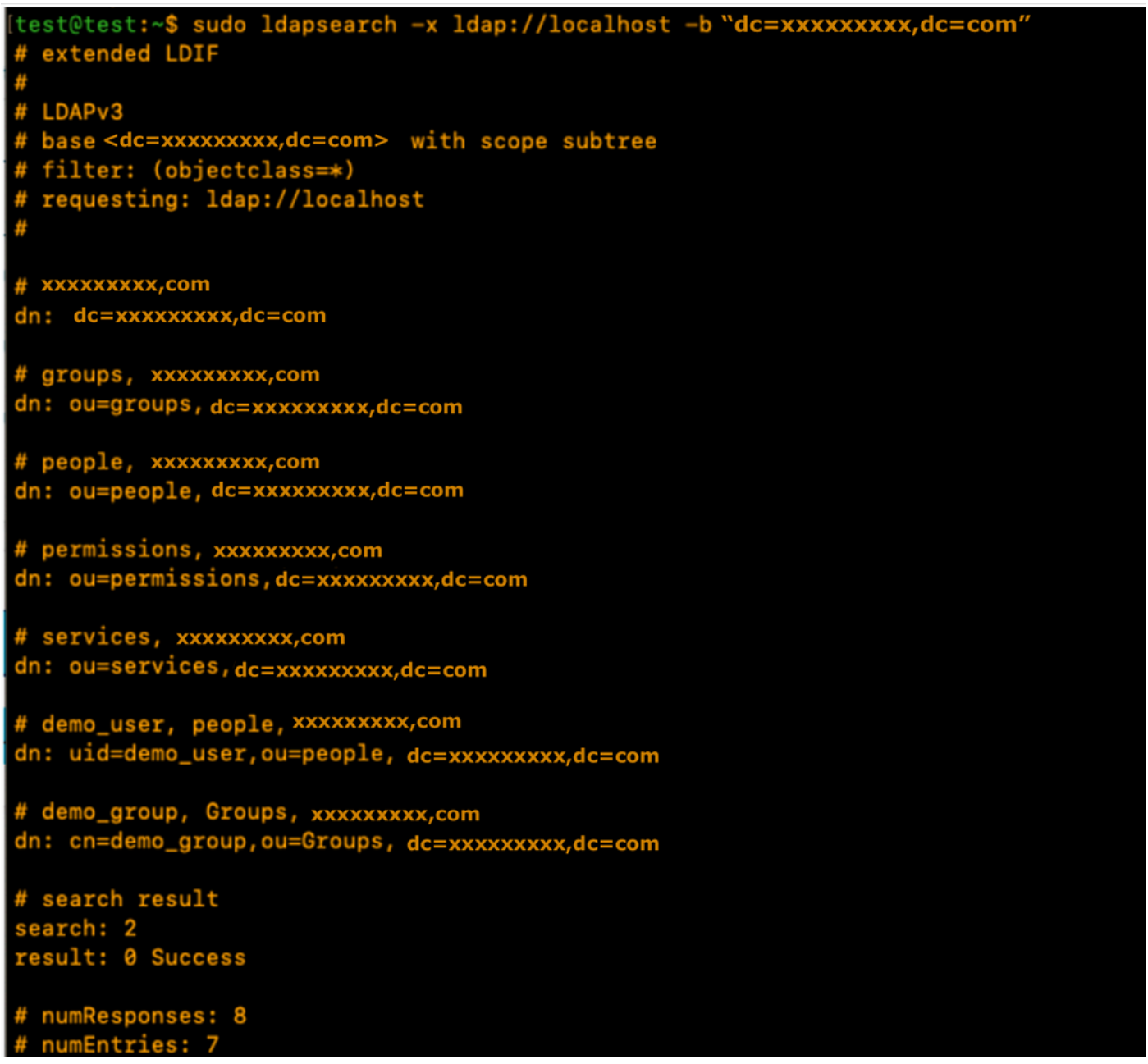
Passen Sie die CentOS-Firewall so an, dass die erforderlichen Ports für LDAP (389 und/oder 636) zugelassen werden.

Bei dieser Demo ist die Firewall deaktiviert.

```
sudo systemctl stop firewalld
```

Stellen Sie sicher, dass LDAP lokal auf dem LDAP-Server funktioniert, indem Sie den angegebenen Befehl ausführen und sicherstellen, dass die LDAP-Ausgabe wie folgt zurückgegeben wird:

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



Die Ausgabe enthält Demokonten, die vom 389DS-Server erstellt wurden. Der LDAP-Server hat automatisch Standard-OUs erstellt.

Die Personen-OU für Benutzer und die Gruppen-OU für Gruppen. Je nach Anforderung können weitere Organisationseinheiten erstellt werden.

Für diese Demonstration werden die standardmäßigen/automatisch erstellten Organisationseinheiten verwendet.

In der offiziellen 389DS-Dokumentation finden Sie Einzelheiten zur umfassenden Verwendung des 389DS-Pakets:

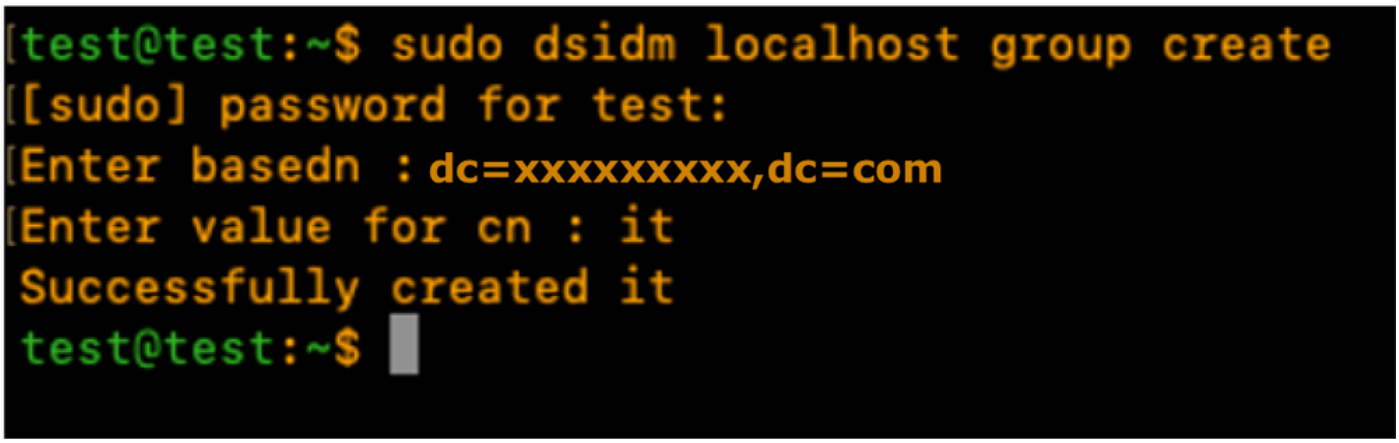
Schritt 3: LDAP-Gruppen und -Benutzer erstellen

Erstellen Sie eine Gruppe (it) mit dem angegebenen Befehl: sudo dsidm <instanzname> group create.

Bei dieser Demonstration lautet der Instanzname "localhost".

```
sudo dsidm localhost group create
```

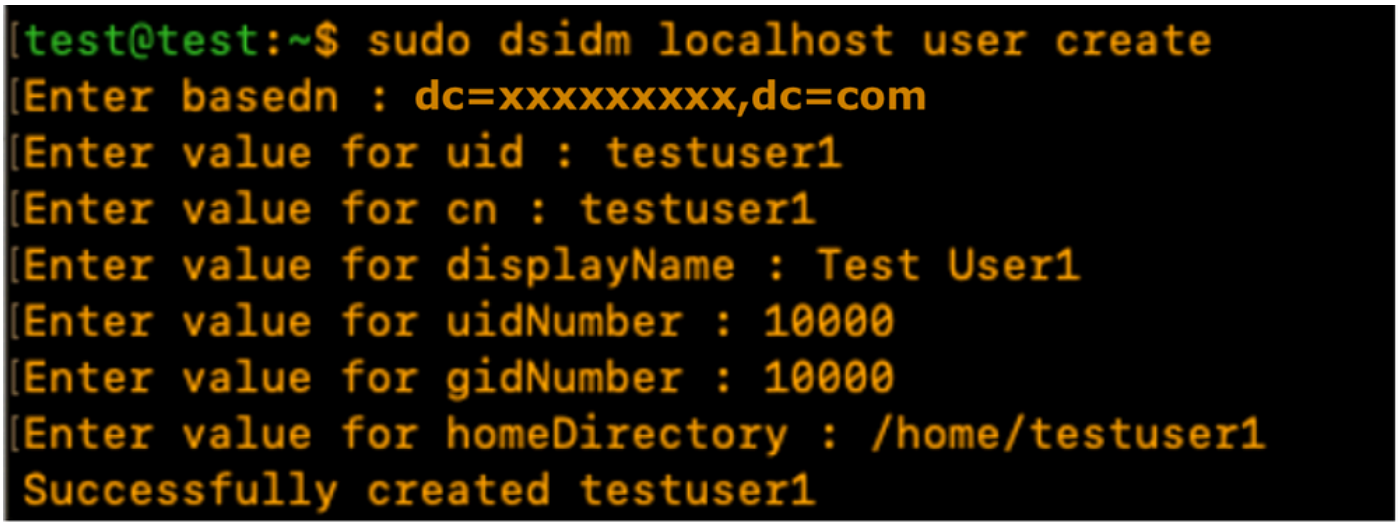
Geben Sie die Terminal-Eingabeaufforderung ein, um die Gruppendetails wie folgt aufzufüllen:



Erstellen Sie das Benutzerkonto testuser1 mit dem folgenden Befehl:

```
sudo dsidm localhost user create
```

Geben Sie die Terminal-Eingabeaufforderung ein, um die Benutzerdetails wie dargestellt einzugeben.



Erstellen Sie mit dem angegebenen Befehl ein Kennwort für testuser1, und geben Sie die CLI-Eingabeaufforderung ein:

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

Fügen Sie den Benutzer mit dem folgenden Befehl zu einer Gruppe hinzu: "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
```

Wiederholen Sie die Schritte zur Benutzererstellung, um testuser2 und bind_user zu erstellen.

Hinweis: Stellen Sie sicher, dass jeder Benutzer explizit zu den entsprechenden Gruppen hinzugefügt wird.

Wenn Sie diesen Schritt auslassen, kann es zu eingeschränktem Zugriff oder Autorisierungsfehlern kommen.

Das bind_user-Konto muss kein Mitglied einer bestimmten Gruppe sein, da es als

---

eigenständiges Konto konfiguriert werden kann. Es bietet die Flexibilität, den Administrator- und Service-Level-Zugriff innerhalb der Verzeichnisumgebung zu verwalten.

Starten Sie die Verzeichnisinstanz neu:

```
sudo dsctl localhost restart
```

Schritt 4: MemberOf Overlay installieren

Installieren Sie das "memberOf"-Plugin, und starten Sie die Verzeichnisinstanz neu:

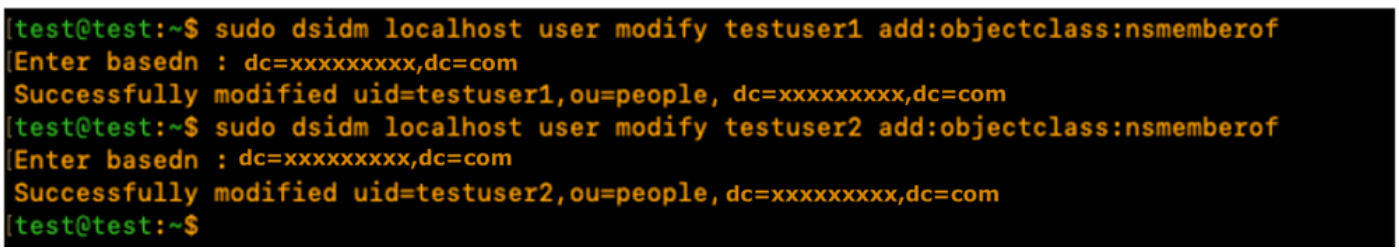
```
sudo dsconf localhost plugin memberof status
sudo dsconf localhost plugin memberof enable
sudo dsctl localhost restart
```

Konfigurieren Sie das "memberOf"-Plugin mit dem angegebenen Befehl: "sudo dsconf <directory_instance> plugin member of set —scope <base_dn>"

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

Benutzer mit dem angegebenen Befehl als gültige "memberOf"-Ziele markieren: "sudo dsidm <directory_instance> user modify <uid> add:objectclass:nsmitgliedof"

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

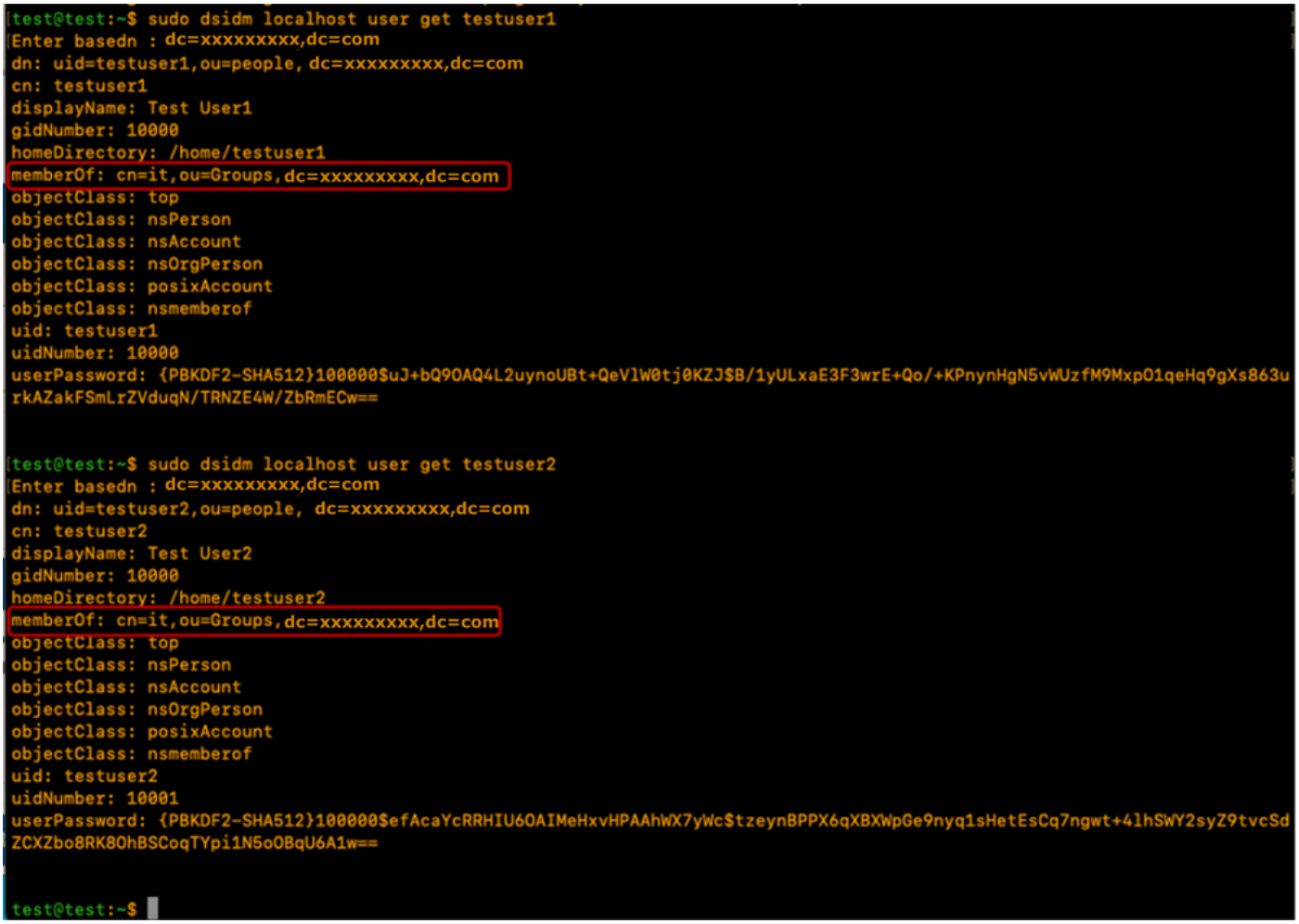


"memberOf"-Fixup für Basis-DN generieren: "sudo dsconf <directory_instance> plugin member of fixup <base_dn>"

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

Überprüfen Sie die Benutzerkonfiguration:

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



Der 389DS LDAP-Server wird mit dem memberOf-Plug-In konfiguriert, um das memberOf-Attribut zu unterstützen.

Konfigurationsparameter auf CIMC

Bei CIMC anmelden

Wählen Sie im Navigationsbereich Admin, User Management und LDAP aus.

Füllen Sie die LDAP-Konfigurationsparameter wie folgt aus:

- LDAP aktivieren: Aktiviert
- Basis-DN: dc=xxxxxxxxx,dc=com

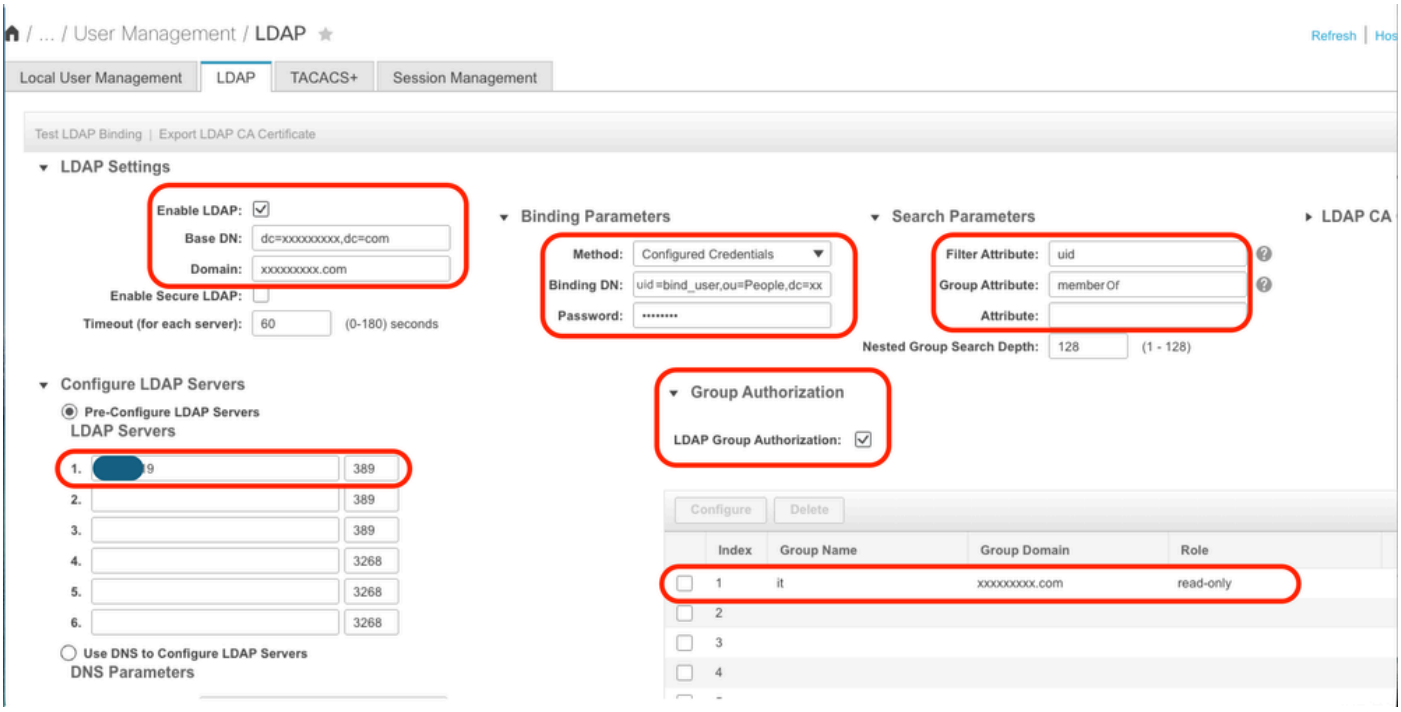
- Domäne: xxxxxxxxx.com

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

- Bindungsparameter: Möglicherweise "Anmeldeinformationen" oder "Konfigurierte Anmeldeinformationen"
    - Wenn Sie die konfigurierten Anmeldeinformationen verwenden, fügen Sie die DN bind_user genau wie auf dem LDAP-Server konfiguriert hinzu:
        - Beispiel: "cn=bind_user,ou=People,dc=xxxxxxxxx,dc=com" oder "uid=bind_user,ou=People,dc=xxxxxxxxx,dc=com"

- Suchparameter:
    - Filterattribut: "cn" oder "uid"
    - Gruppenattribut: MitgliedVon

- LDAP-Gruppenautorisierung - Aktiviert
    - Gruppenname: es
    - Gruppendomäne: xxxxxxxxx.com
    - Rolle: schreibgeschützt (jede bevorzugte Rolle)



Speichern Sie die Konfiguration, und testen Sie die LDAP-Benutzeranmeldung.

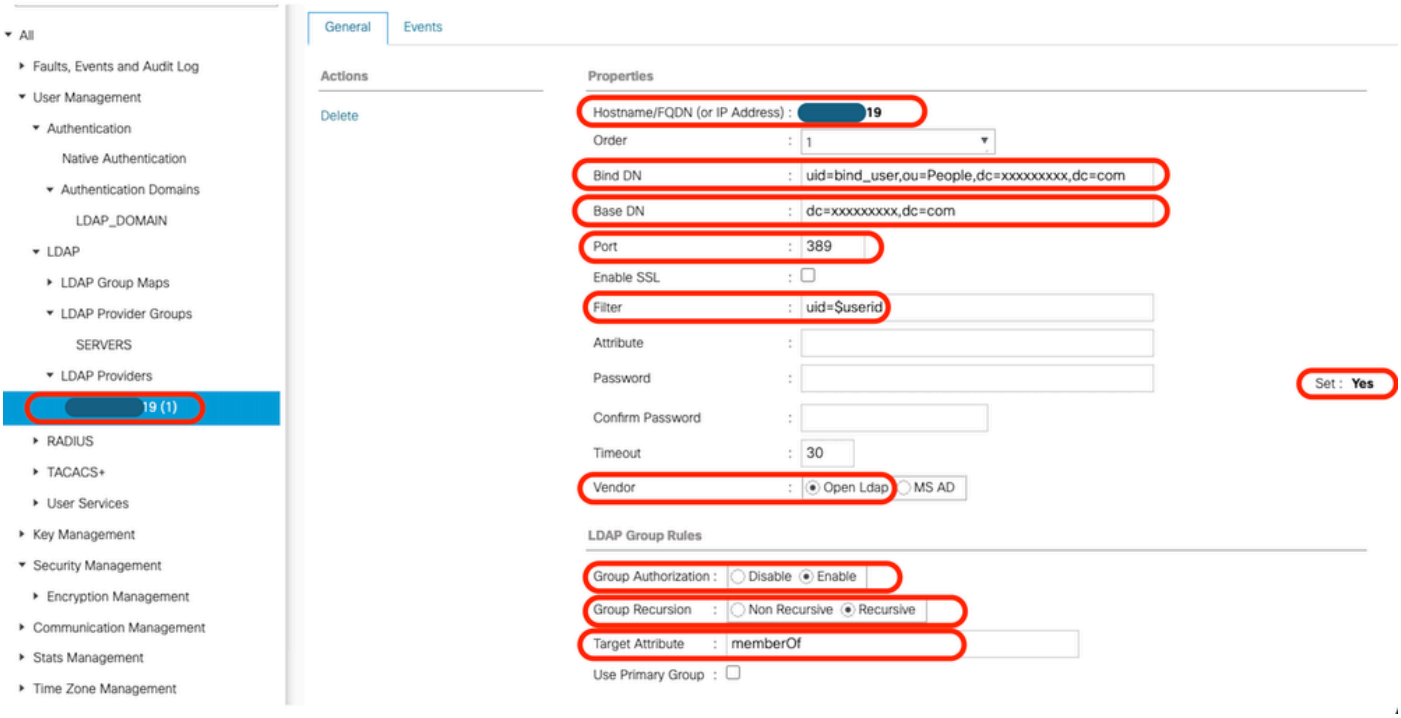
Konfigurationsparameter in UCS Manager

Bei UCS Manager anmelden

Wählen Sie im Navigationsbereich Admin, User Management und LDAP aus.

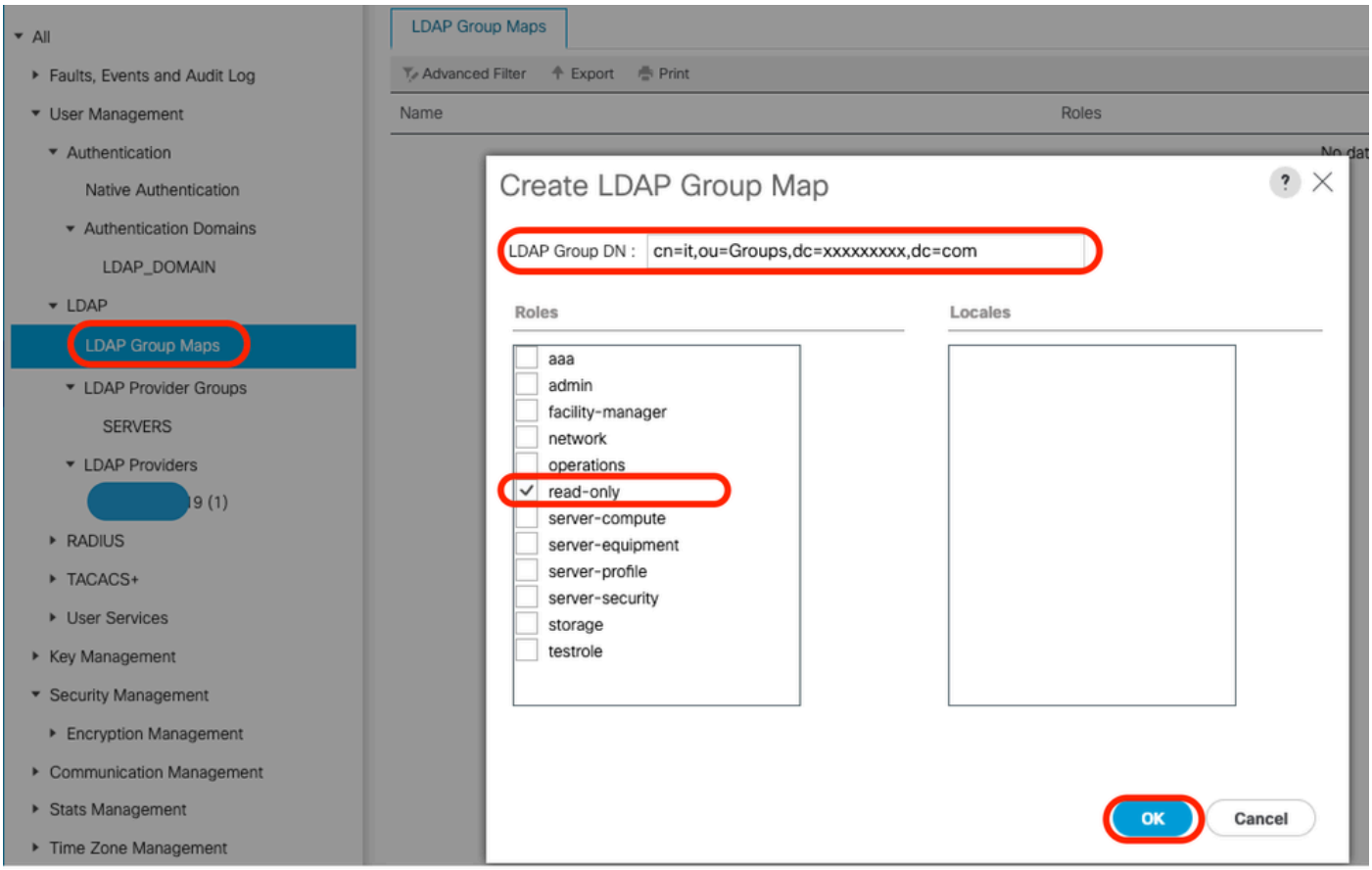
Füllen Sie die LDAP-Konfigurationsparameter wie folgt aus:

- LDAP-Anbieter:
  - Hostname: <FQDN oder IP-Adresse des LDAP-Servers>
  - Bind-DN: uid=bind_user,ou=people,dc=xxxxxxxxx,dc=com
  - Basis-DN: dc=xxxxxxxxx,dc=com
  - Anschluss: 389
  - SSL aktivieren: Deaktiviert
  - Filter: uid=$userid
  - Gruppenautorisierung: Aktiviert
  - Gruppenrekursion: Rekursiv
  - Zielattribut: MitgliedVon
- LDAP-Gruppenzuordnungen:
  - LDAP-Gruppen-DN: cn=it,ou=Groups,dc=xxxxxxxxx,dc=com



Fügen Sie den konfigurierten LDAP-Anbieter einer LDAP-Anbietergruppe hinzu. Für diese Demonstration wird die LDAP-Anbietergruppe "SERVER" verwendet.

Konfigurieren Sie die LDAP-Gruppenzuordnungen, indem Sie eine vom LDAP-Server abgerufene "LDAP-Gruppen-DN" hinzufügen.



Konfigurieren Sie eine LDAP-Authentifizierungsdomäne (LDAP_DOMAIN) unter "Alle >> Benutzerverwaltung >> Authentifizierung >> Authentifizierungsdomänen", und verweisen Sie auf die LDAP-Anbietergruppen, und testen Sie die LDAP-Benutzeranmeldung.

Schlussfolgerung

Dieser Leitfaden behandelt grundlegende Bereitstellungsszenarien. Eine eingehendere Betrachtung der LDAP-Funktionen kann jedoch die Leistung und Sicherheit von Verzeichnissen erheblich verbessern.

Weitere Informationen, Best Practices und erweiterte Konfigurationsdetails finden Sie in den angegebenen Ressourcen:

- Offizielle OpenLDAP-Dokumentation
- LDAP Account Manager - Handbuch
- 389 Directory Server-Dokumentation
- Konfigurieren von LDAP im UCS Manager
- Konfigurieren von sicherem LDAP auf Servern der UCS C-Serie

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.