Configurar LDAP no UCS Manager & CIMC usando Linux OpenLDAP e servidores 389-DS

Contents

Introdução

Este documento descreve uma variedade de opções para configurar o LDAP como um método de autenticação para o UCS Manager e o CIMC usando OpenLDAP baseado em Linux e 389 Diretory Servers.

Informações de Apoio

Devido à grande variabilidade das configurações do servidor OpenLDAP, um tratamento exaustivo está além do escopo deste documento. Em vez disso, este artigo enfatiza as configurações comumente implementadas que abrangem várias distribuições Linux, pacotes de servidor LDAP e esquemas de atributo. Para fins de clareza e simplicidade, este documento aborda as configurações LDAP padrão. A configuração do LDAP seguro (LDAPS) não é abordada neste documento.

Pré-requisitos:

O conhecimento sobre esses tópicos é altamente recomendado:

- UCS série B
- UCS C Series
- Administração do servidor Linux

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Versão do firmware do UCS Manager: 4.3 (2c)
- Modelo de interconexão de estrutura: UCS-FI-6454
- Modelo de servidor independente UCS C Series: UCSC-C240-M5
- Versão do firmware autônomo do UCS C Series: 4.3 (2.250045)
- Ubuntu 20,04
- Fluxo CentOS 10

Configurações usadas para esta demonstração:

- Nome de host do servidor LDAP: teste
- Domínio do servidor: xxxxxxxxx.com
- FQDN do servidor: test.xxxxxxxxx.com
- Endereço IP do servidor Linux (Ubuntu e CentOS): X X X 19

- Usuários do OpenLDAP: testuser1, testuser2
- Grupos OpenLDAP: o
- Conta de usuário OpenLDAP Bind: bind_user

Note: o editor de texto linux Nano foi usado neste laboratório.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Cenário 1: Ubuntu - Debian

A configuração do servidor LDAP pode ser realizada usando uma interface gráfica, como o Gerenciador de contas LDAP, ou ferramentas de linha de comando, dependendo da preferência administrativa e do nível de controle necessário. Este cenário examina a configuração usando o OpenLDAP baseado em Linux, começando com uma implantação baseada em GUI e, subsequentemente, fazendo a transição para utilitários de linha de comando para explorar recursos avançados, incluindo plug-ins de sobreposição (comumente utilizados em integrações com o Cisco UCS Manager).

Opção 1: Configurar o OpenLDAP usando o Ubuntu LDAP Account Manager (LAM)

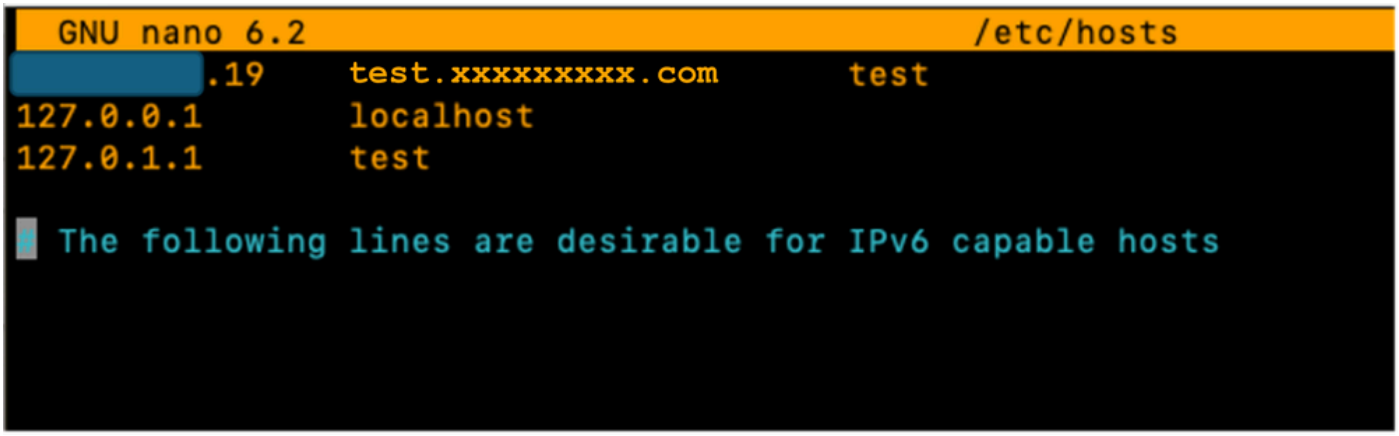
Passo 1: Configuração inicial do nome de host do servidor Linux e ferramentas de rede.

Atualize o ubuntu e instale o pacote net-tools para acessar ferramentas como ifconfig, netstat, etc:

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

Use o comando "ifconfig" para verificar o endereço IP do servidor e, em seguida, adicione-o ao arquivo "/etc/hosts" juntamente com o nome de domínio do servidor (Por exemplo: "test.xxxxxxxx.com" usado neste laboratório) e o nome do host (Por exemplo: "teste") no formato especificado.

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



Além disso, atualize o arquivo "/etc/hostname" substituindo seu conteúdo pelo nome do host (teste).

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

É necessário reinicializar o servidor para que essas alterações entrem em vigor.

```
sudo reboot
```

Etapa 2: Instalar SLAPD, Apache, PHP e suas dependências

Em seguida, instale o Apache, o PHP e suas dependências. Eles são usados para habilitar a interação da GUI em uma página da Web :

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

Instalar o pacote de servidor LDAP aberto "slapd" e suas dependências (ldap-utils)

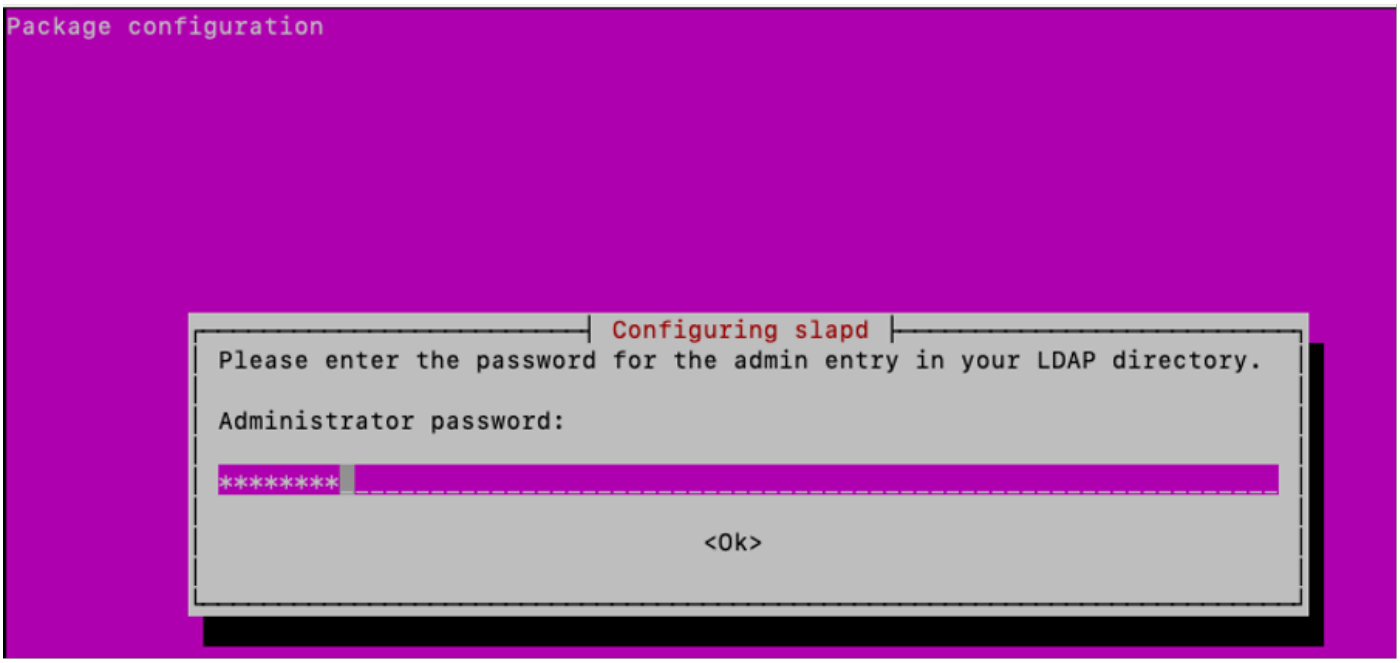
```
sudo apt install slapd ldap-utils -y
```

Durante a instalação do slapd, na janela pop-up da GUI apresentada, insira a configuração adicional necessária do pacote SLAPD.

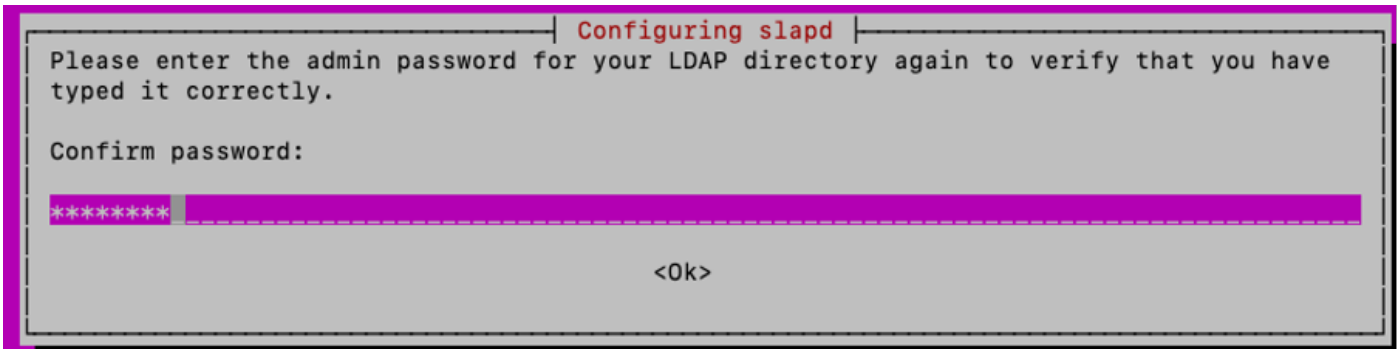
Note: Perder a senha exige a reinstalação do servidor LDAP.

O "administrador" (admin) nesse contexto é uma conta usada para gerenciar o serviço, os módulos e as configurações do OpenLDAP.

Adicione a senha de "administrador" do pacote LDAP e pressione Enter no teclado para selecionar "OK".



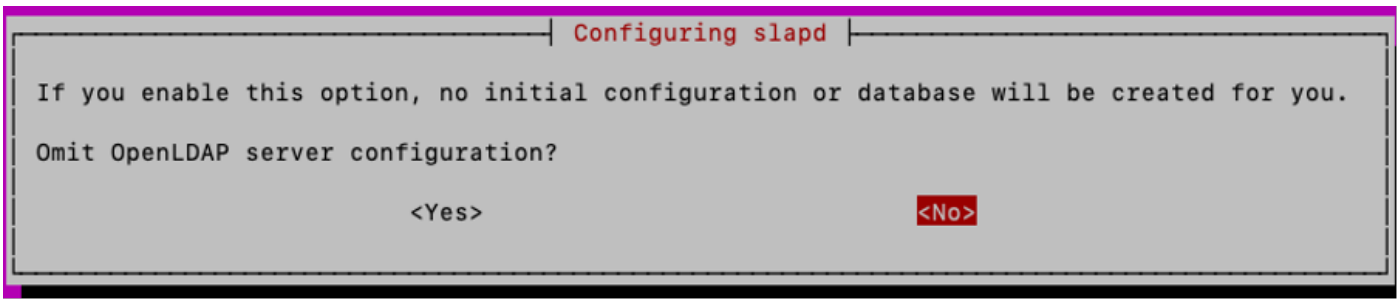
Confirme a senha:



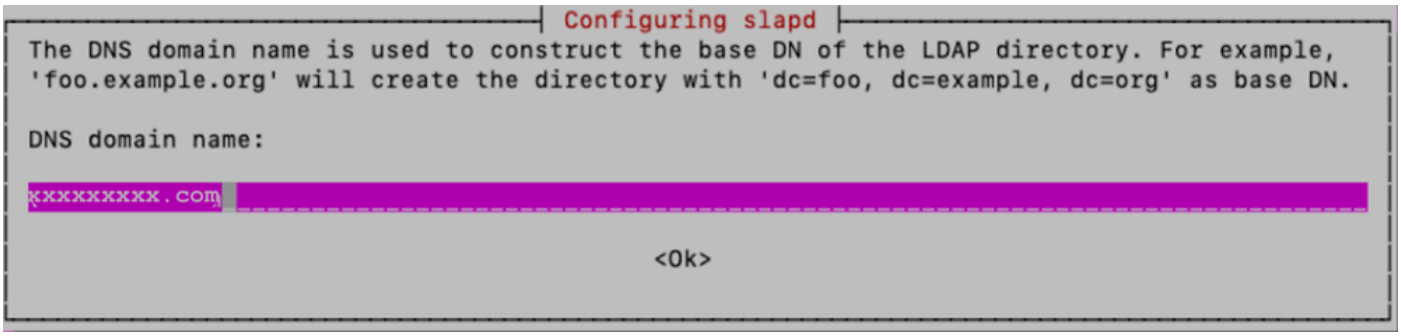
Quando a instalação estiver concluída, você poderá usar o comando especificado para reconfigurar o pacote SLAPD, adicionando informações de domínio:

```
sudo dpkg-reconfigure slapd
```

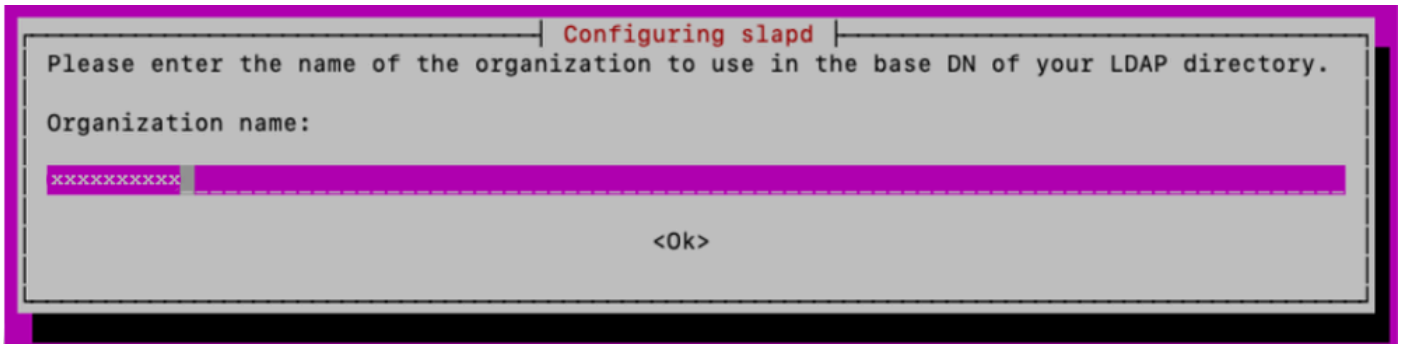
Você pode aceitar a opção padrão "No" para "Omit OpenLDAP server Configuration" e pressionar enter:



Digite o nome de domínio e pressione enter:



Para este laboratório, "xxxxxxxxx" é usado como "Nome da organização":

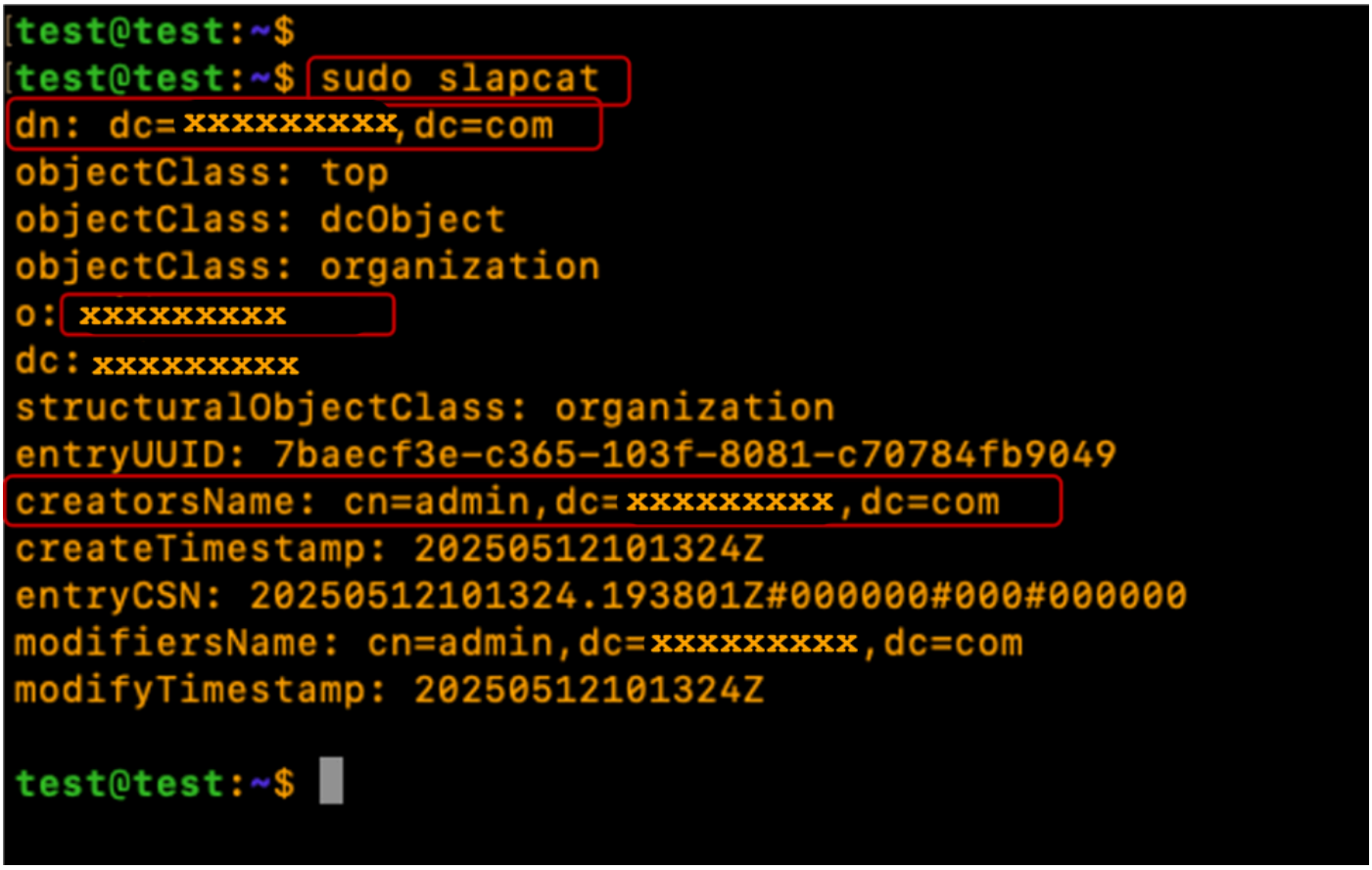


Em seguida, digite a senha do administrador e confirme-a.

Para as outras opções de configuração, mantenha os padrões e pressione a tecla Enter do teclado para concluir a configuração.

Verifique a instalação do SLAPD usando o comando:

```
sudo slapcat
```



Etapa 3: Instalar o LDAP Account Manager

Instale o LDAP Account Manager (LAM) para a criação e o gerenciamento de usuários e grupos LDAP:

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

Habilite a extensão PHP PHP PHP-CGI, requerida pelo LAM.

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

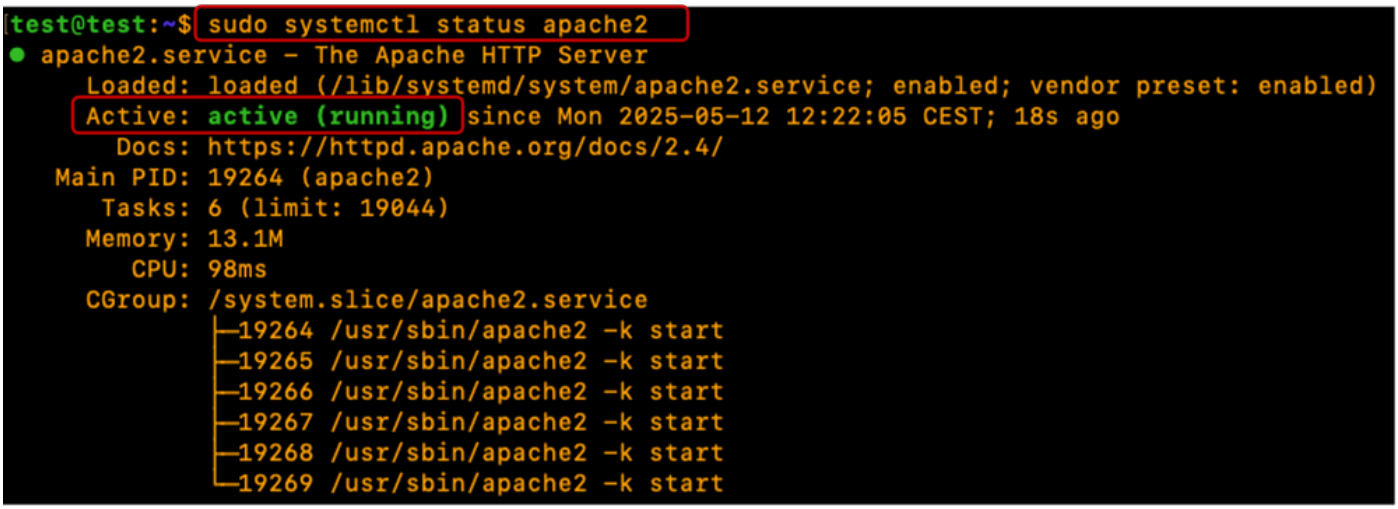
Recarregue o Apache para ativar a nova configuração.

Reinicie e ative o serviço Apache para iniciar automaticamente no momento da inicialização:

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

Verifique se o status do Apache Server é "Em Execução" e "Ativo"

```
sudo systemctl status apache2
```

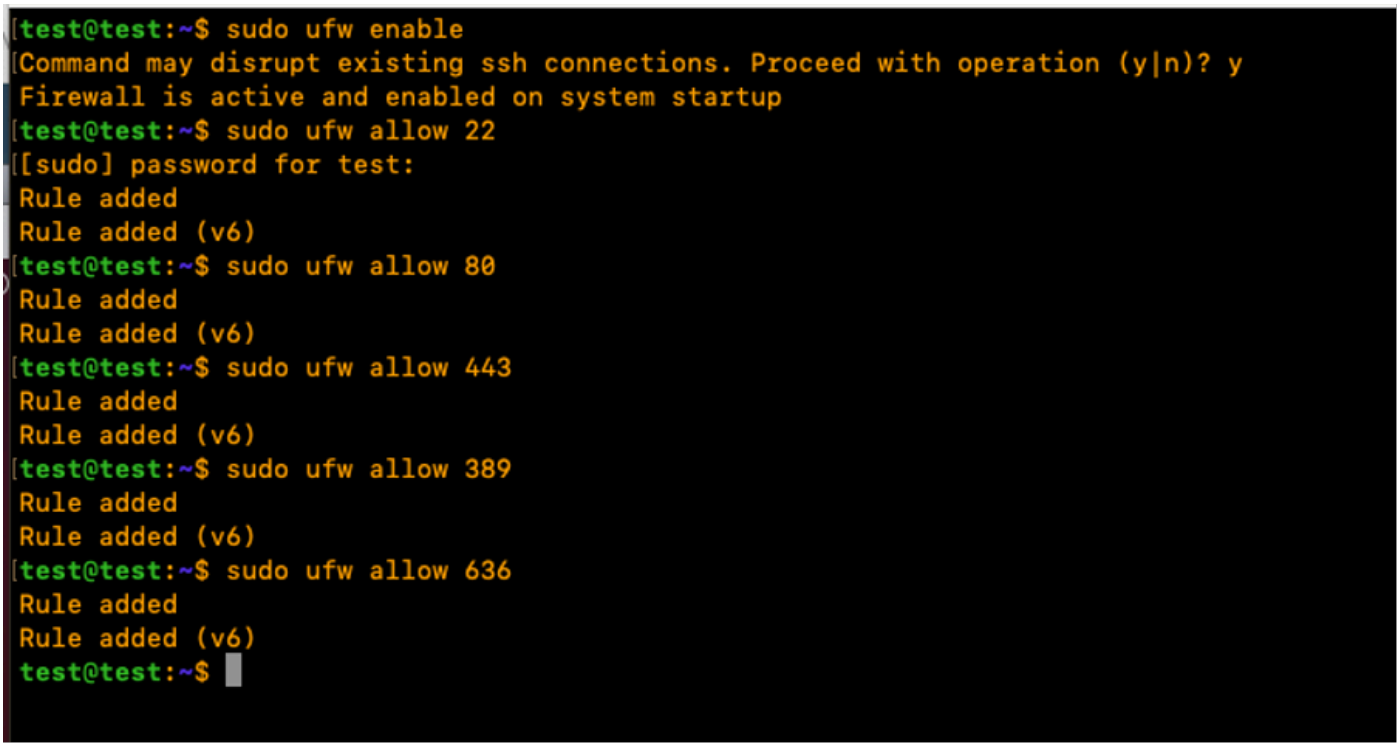


Configure o firewall do Ubuntu para permitir as portas 80(Web), 443 (Web segura), 389(LDAP) e 636 (LDAP seguro se necessário)

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

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

```
sudo ufw allow 636
```



Verifique o status do firewall do Ubuntu:

```
sudo ufw status
```

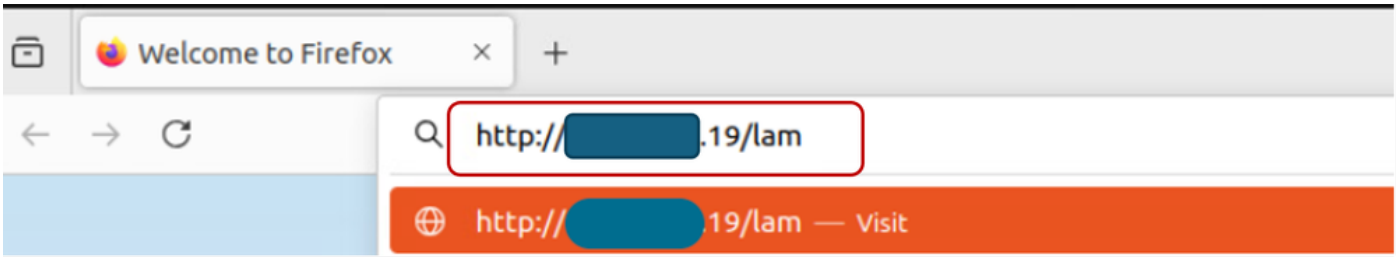
```
test@test:~$ sudo ufw status
Status: active

To                         Action      From
--                         ------      ----
22                         ALLOW       Anywhere
80                         ALLOW       Anywhere
443                        ALLOW       Anywhere
389                        ALLOW       Anywhere
636                        ALLOW       Anywhere
22 (v6)                    ALLOW       Anywhere (v6)
80 (v6)                    ALLOW       Anywhere (v6)
443 (v6)                   ALLOW       Anywhere (v6)
389 (v6)                   ALLOW       Anywhere (v6)
636 (v6)                   ALLOW       Anywhere (v6)
```

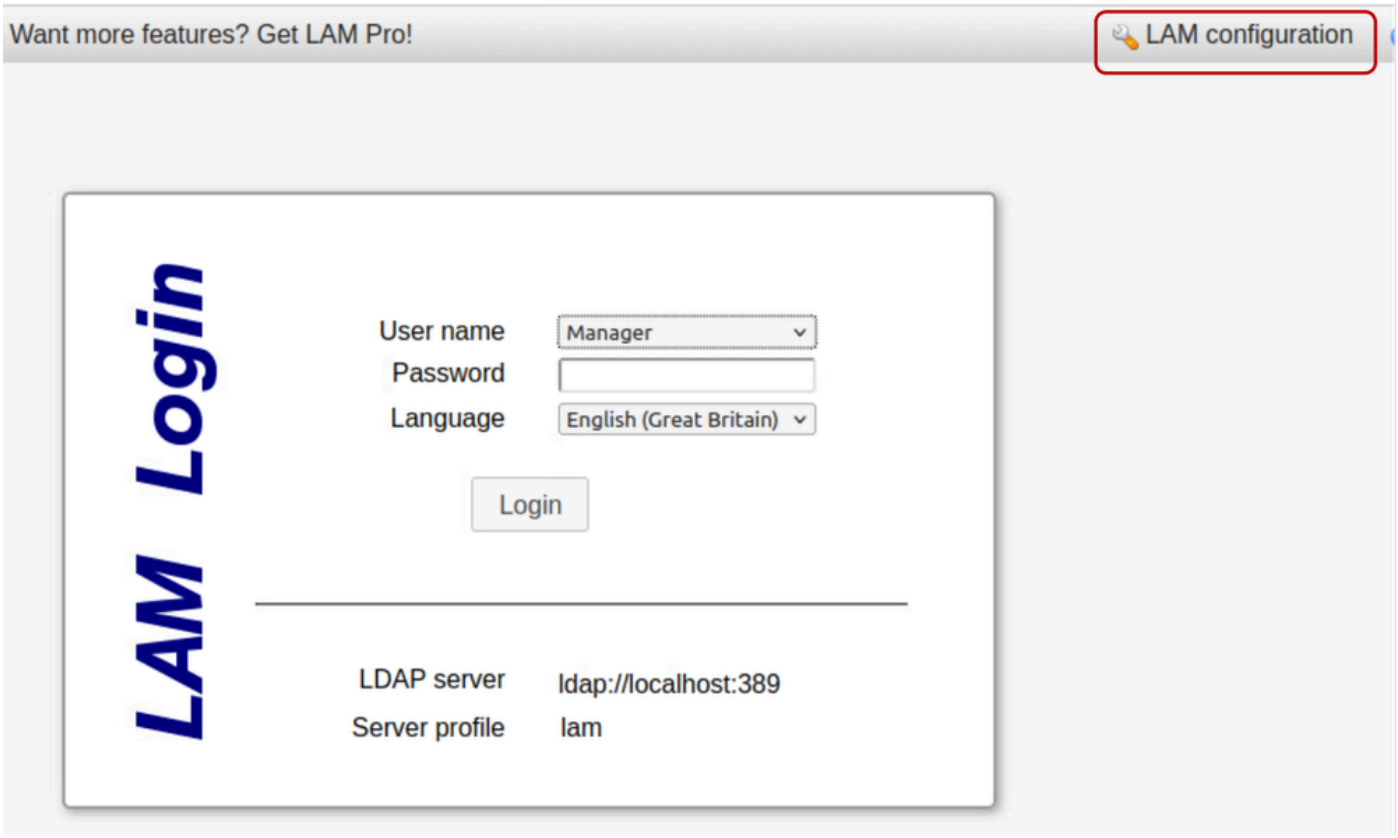
Passo 4: Configurar o Gerente de contas LDAP

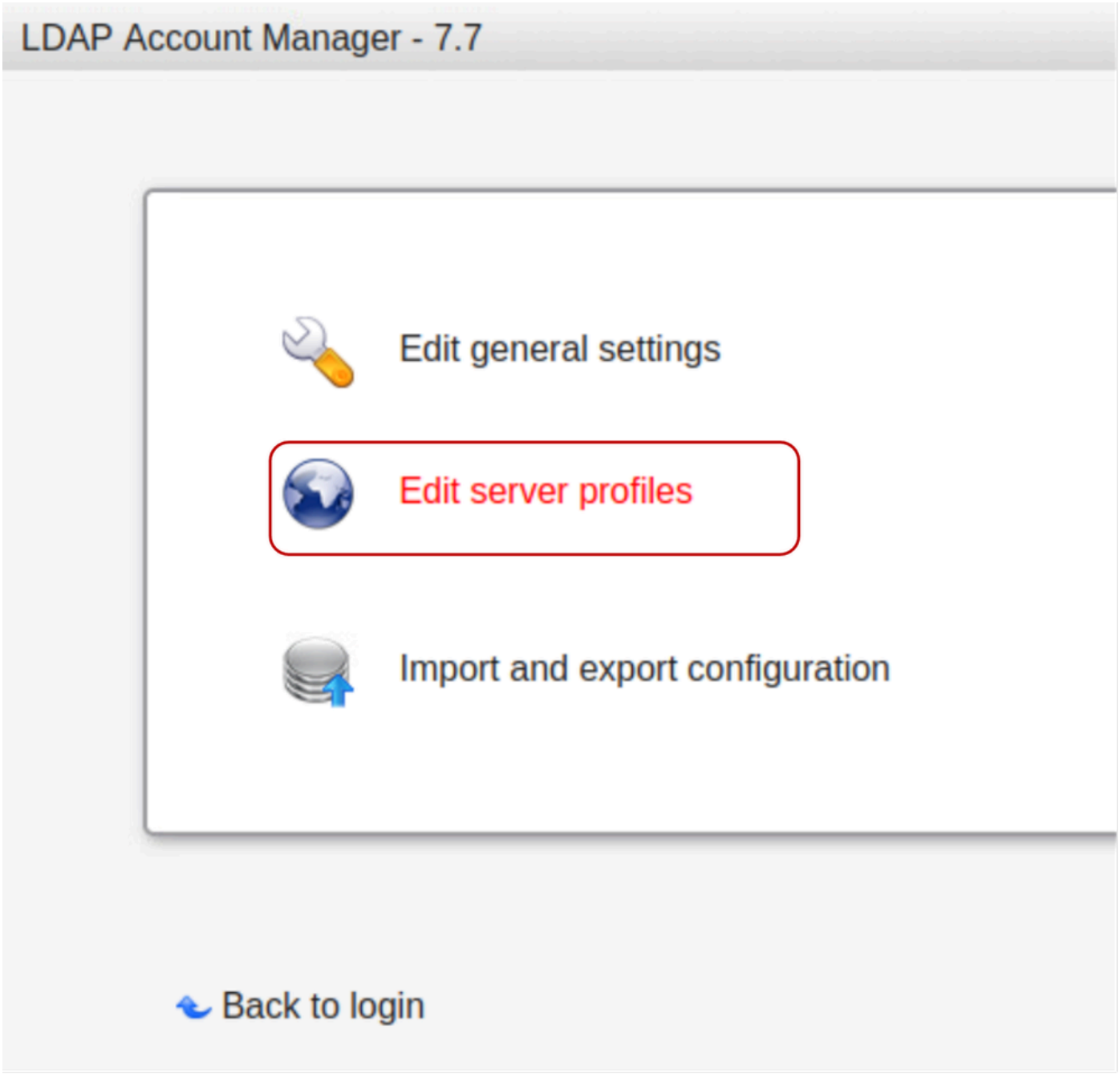
Para configurar o LDAP Account Manager (LAM) a partir da GUI, abra um navegador da Web, insira o endereço IP do servidor Linux e adicione o caminho 'lam' a ele como mostrado:

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

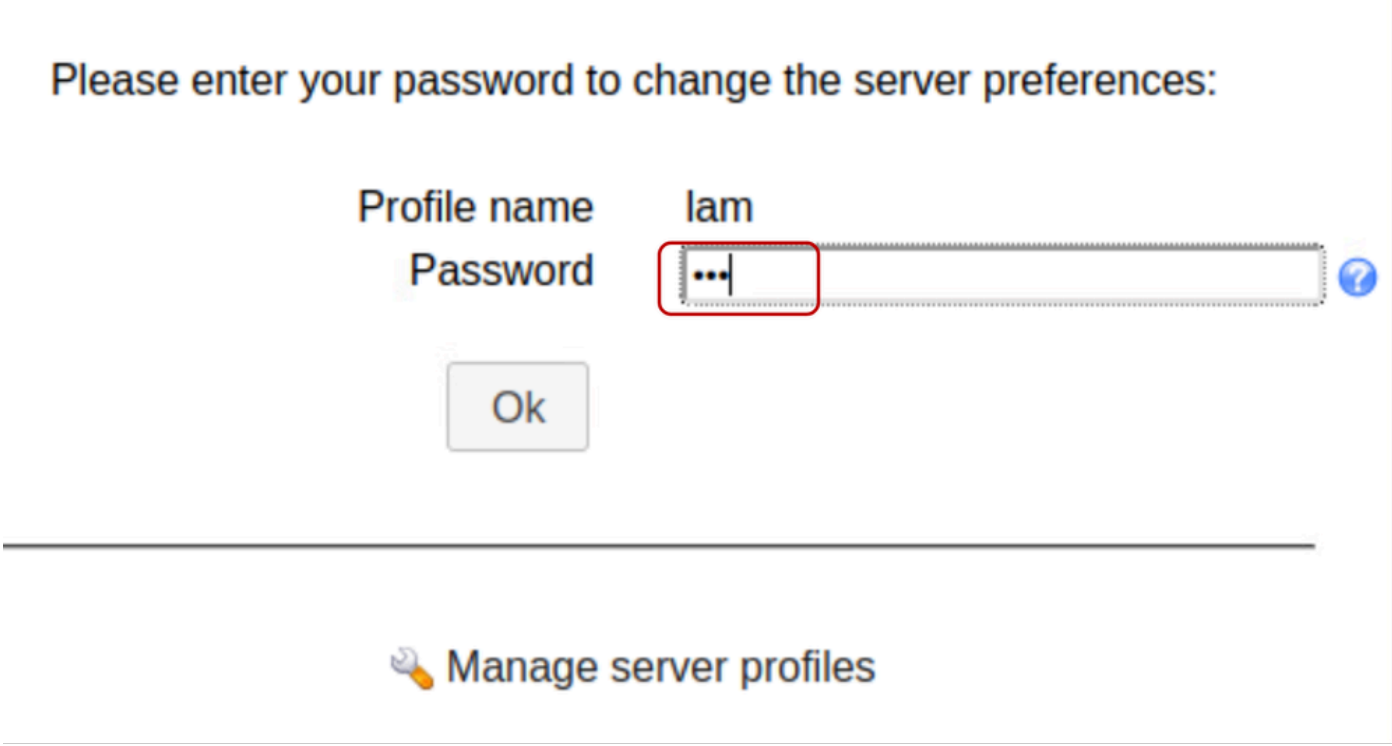


Clique em "LAM configuration" e selecione "Edit server profiles".


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



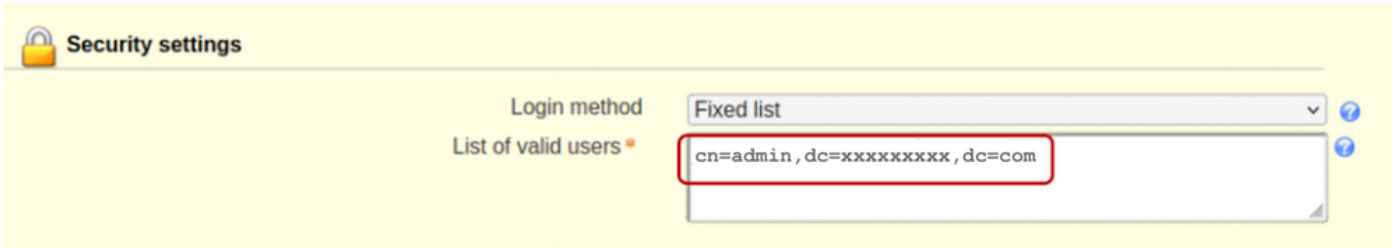
Digite a senha padrão "lam" para fazer login.



Na guia Configurações gerais, verifique as configurações do servidor, "Idioma" e "Fuso horário".

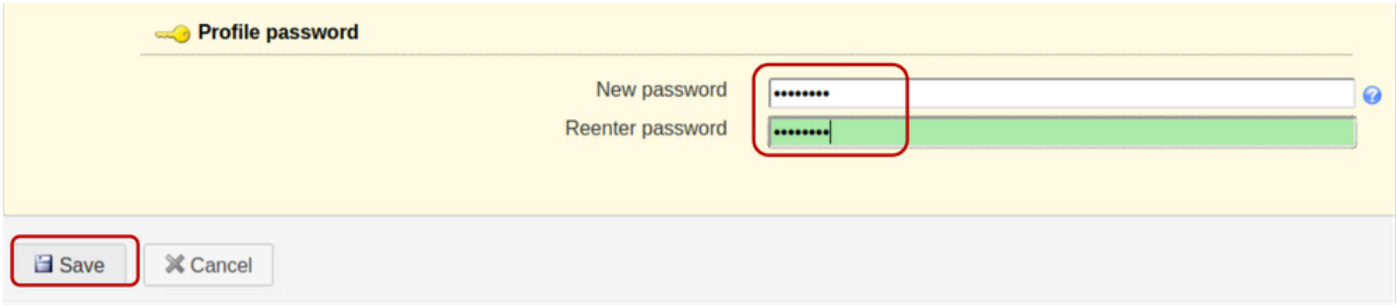
Na seção Configurações da ferramenta, edite e adicione o nome de domínio necessário no campo Sufixo de árvore como mostrado abaixo:

Edite a seção Configurações de segurança para incluir um usuário "admin" usado para gerenciar o serviço SLAPD.



Defina uma "Senha do perfil". Essa senha é usada para logins subsequentes à interface de configuração do LAM; para este exemplo, "cisco123" é configurado em vez da senha "lam" padrão.

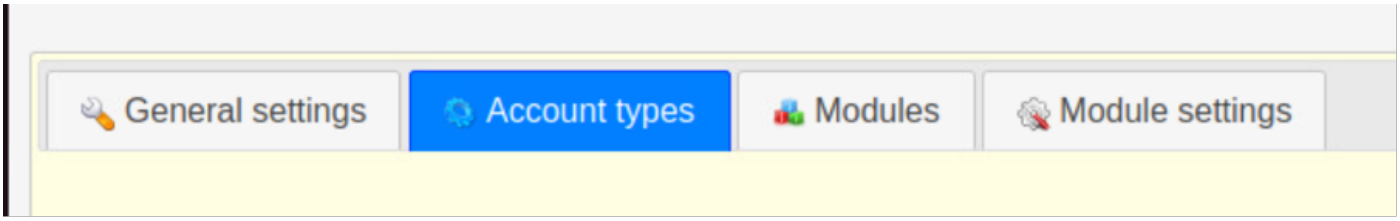
Salve a configuração:



A sessão é então reiniciada na interface GUI de configuração do LAM.

Faça login novamente (Configuração do LAM > Editar perfis do servidor) usando a nova senha criada.

Clique em "Tipos de conta",



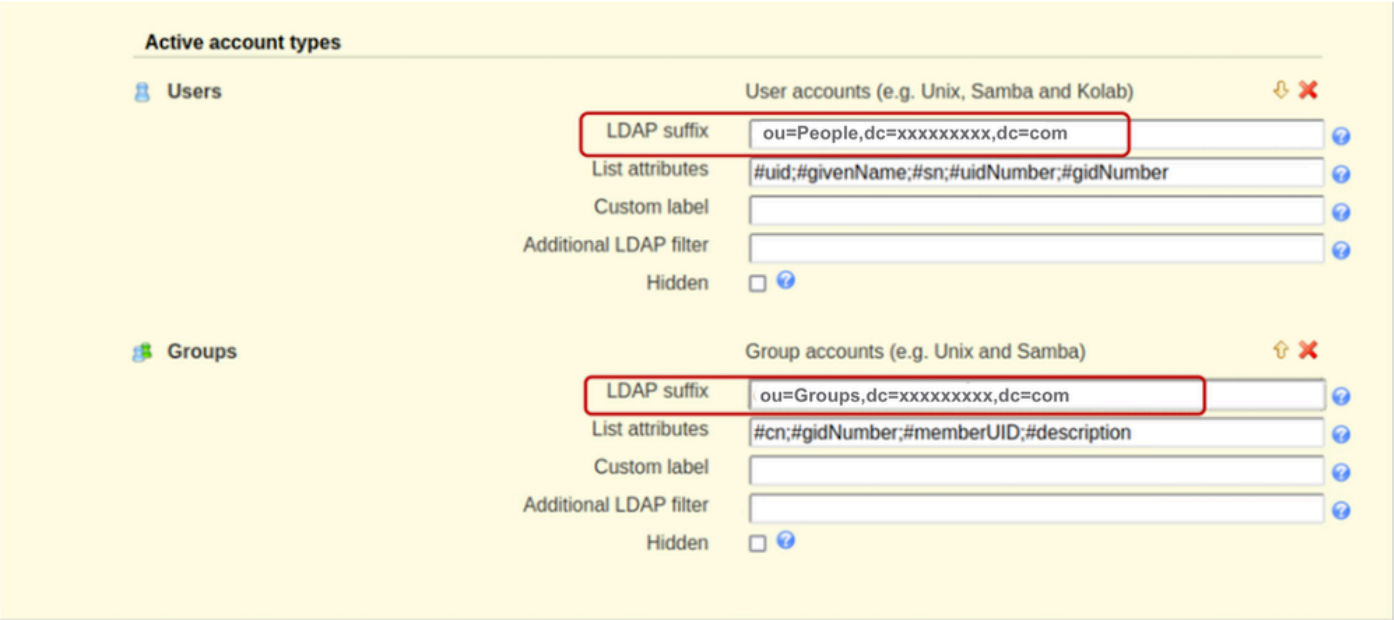
Role para baixo e edite os tipos de conta ativos padrão com as informações de nome de domínio no campo de sufixo LDAP. Por exemplo, o conteúdo padrão do campo "Sufixo LDAP" exibe um valor como "ou=People,dc=meu-domínio,dc=com".

Se houver necessidade de criar novas unidades organizacionais, substitua o conteúdo do campo "Sufixo LDAP" para que contenha o nome da unidade organizacional.

O formato é mostrado como "ou=<unidade_organizacional>,dc=xxxxxxxx,dc=com".

Para esta demonstração, a OU para Usuários é "Pessoas" e a OU para Grupos é "Grupos".

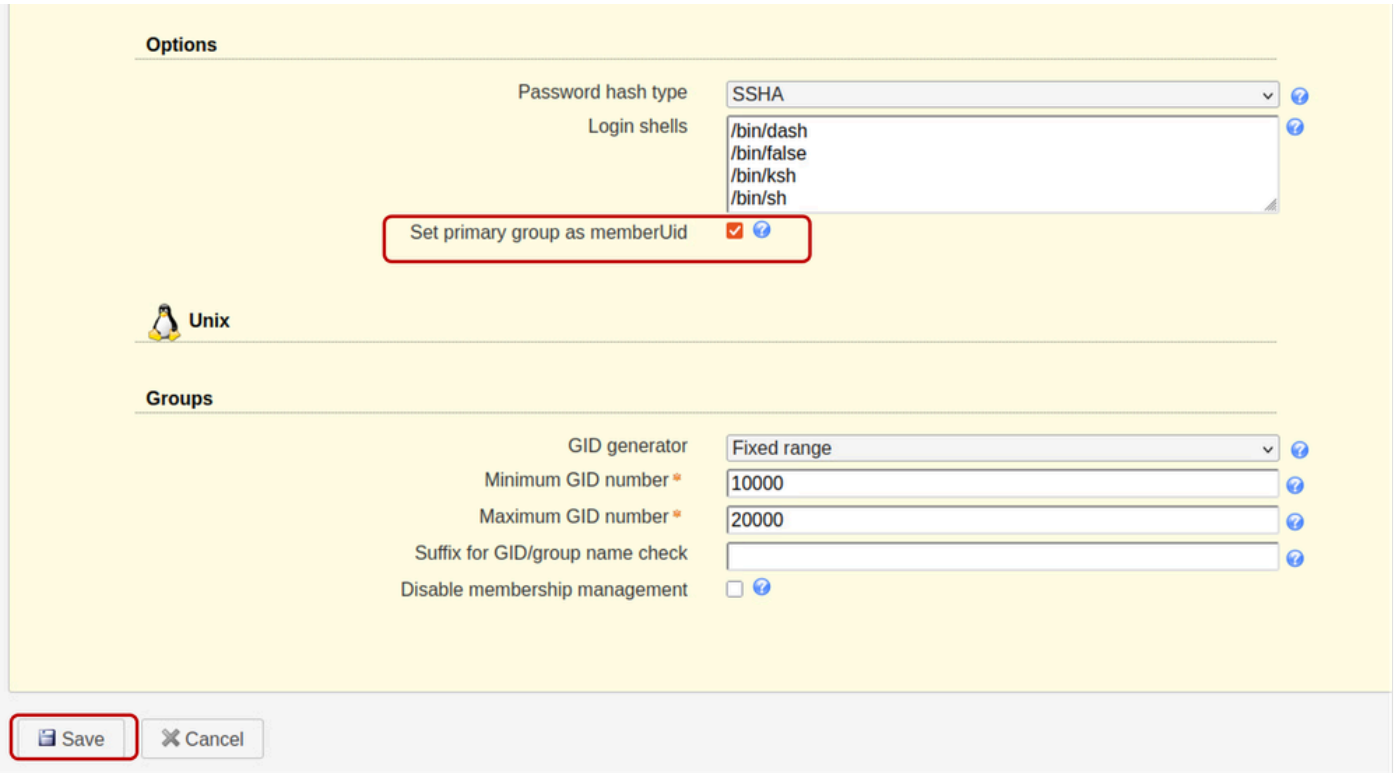
Salve a configuração.



Role para baixo até a seção Opções e verifique "Definir grupo primário como memberUid".

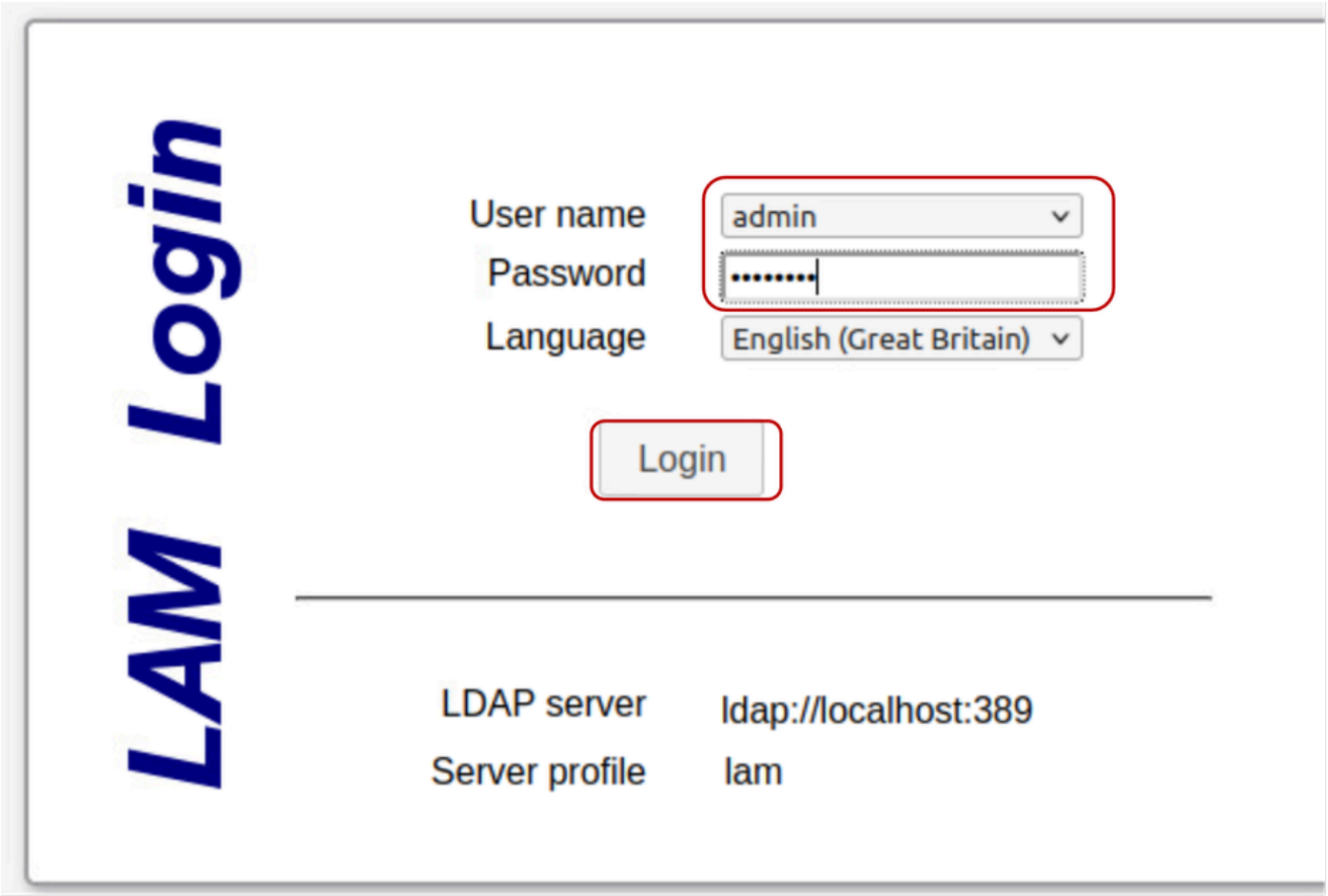
Por padrão, a opção "Definir grupo primário como memberUid" não está definida nos objetos do grupo. Ativar isso permite o uso do "grupo primário" do OpenLDAP, como um grupo LDAP padrão, onde o "memberUid" pode ser referenciado (Por exemplo: Na configuração do servidor UCS C Series). Se essa opção estiver desmarcada, ocorrerá uma falha no login dos usuários que pertencem a qualquer grupo Primário.

Salve a configuração.

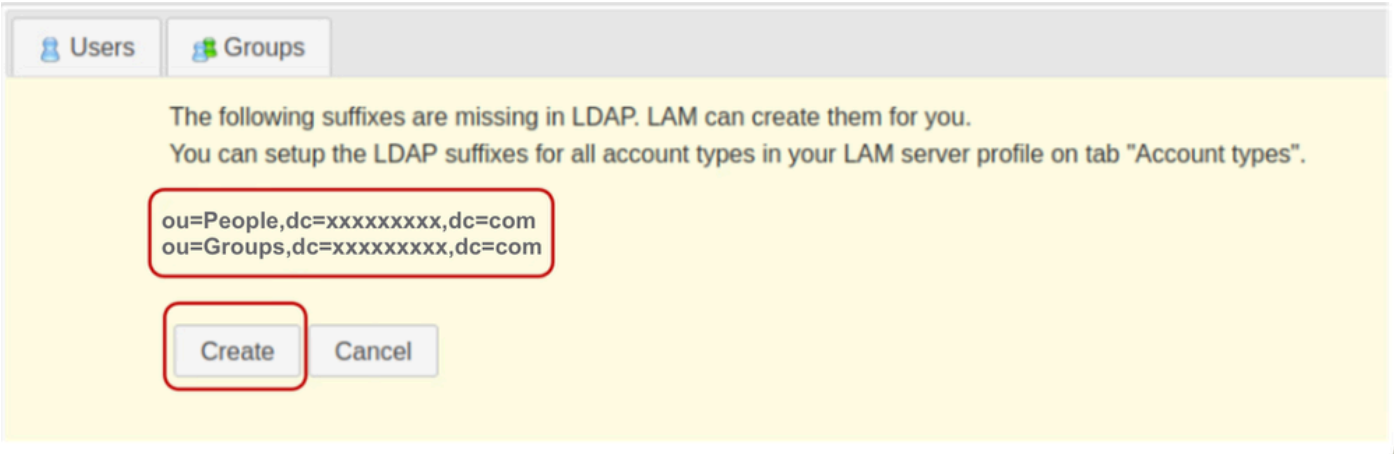


Etapa 5: Criar OUs, Grupos e Usuários

Faça login no LAM como o usuário "admin" com a mesma senha criada durante a instalação, para criar Users e Groups pertencentes às OUs criadas anteriormente (People e Groups), respectivamente:

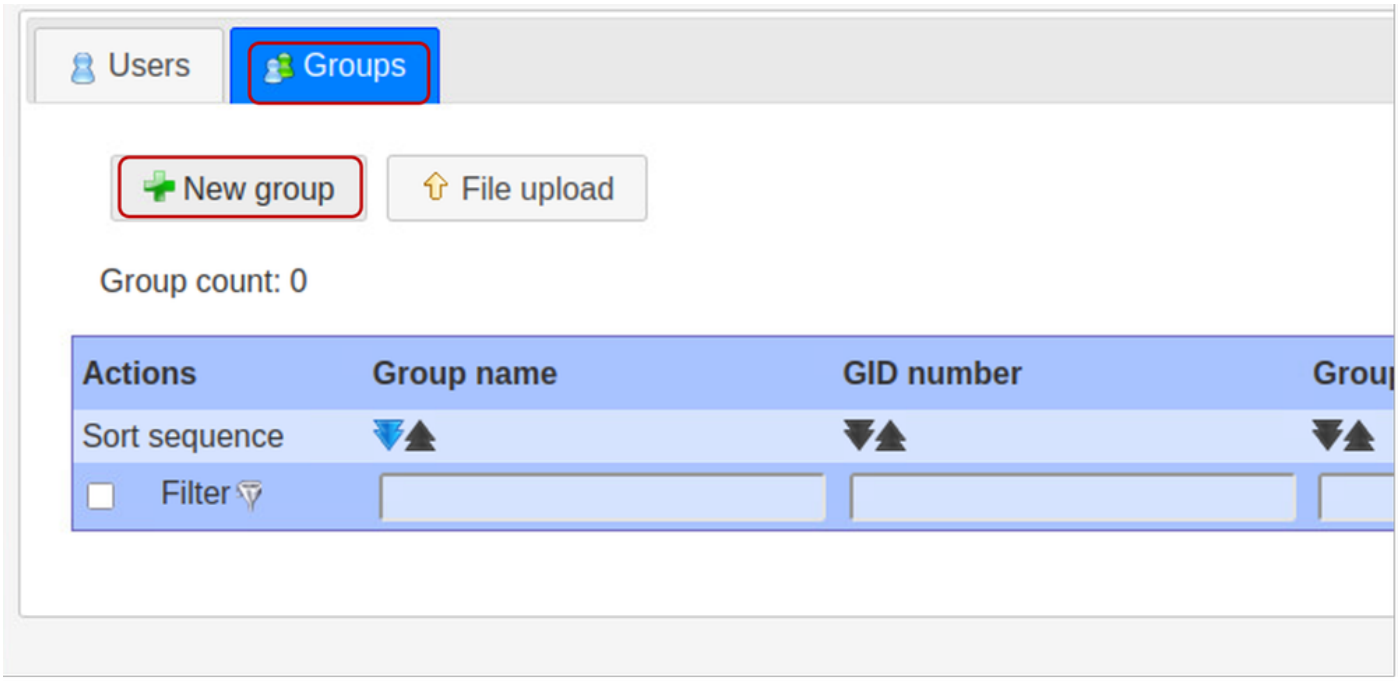


Crie as OUs especificadas anteriormente na seção Configuração do LAM.
Clique em Criar.



Em seguida, no Gerenciador de contas LDAP, crie o grupo "it":

Selecione a guia Grupos e clique em Novo grupo

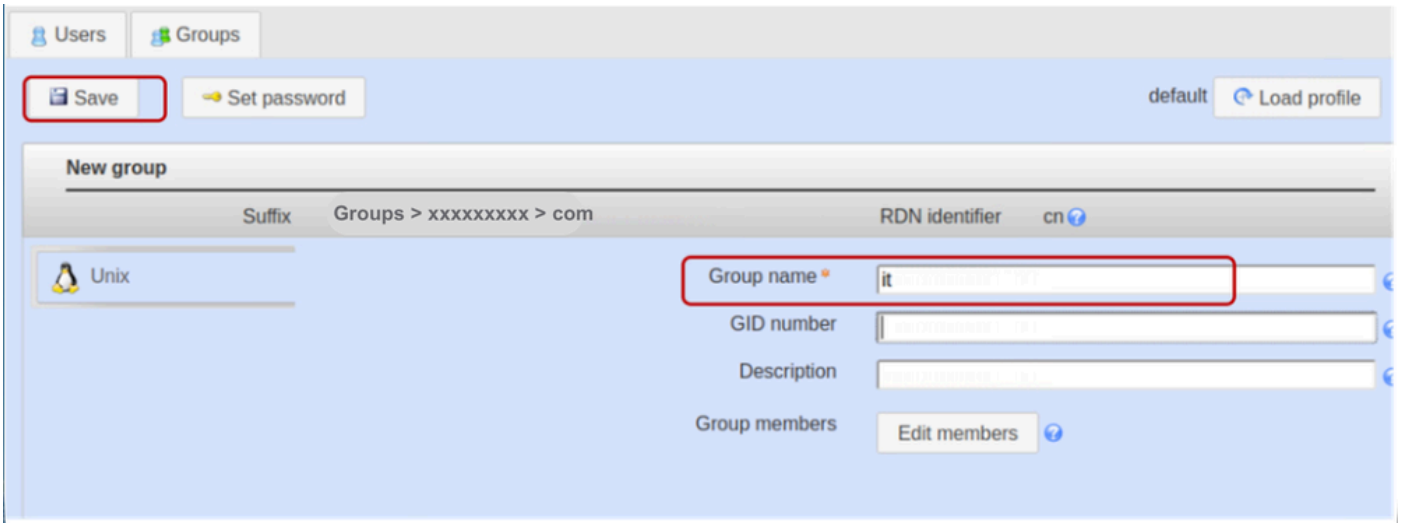


Defina o nome do grupo como "it".

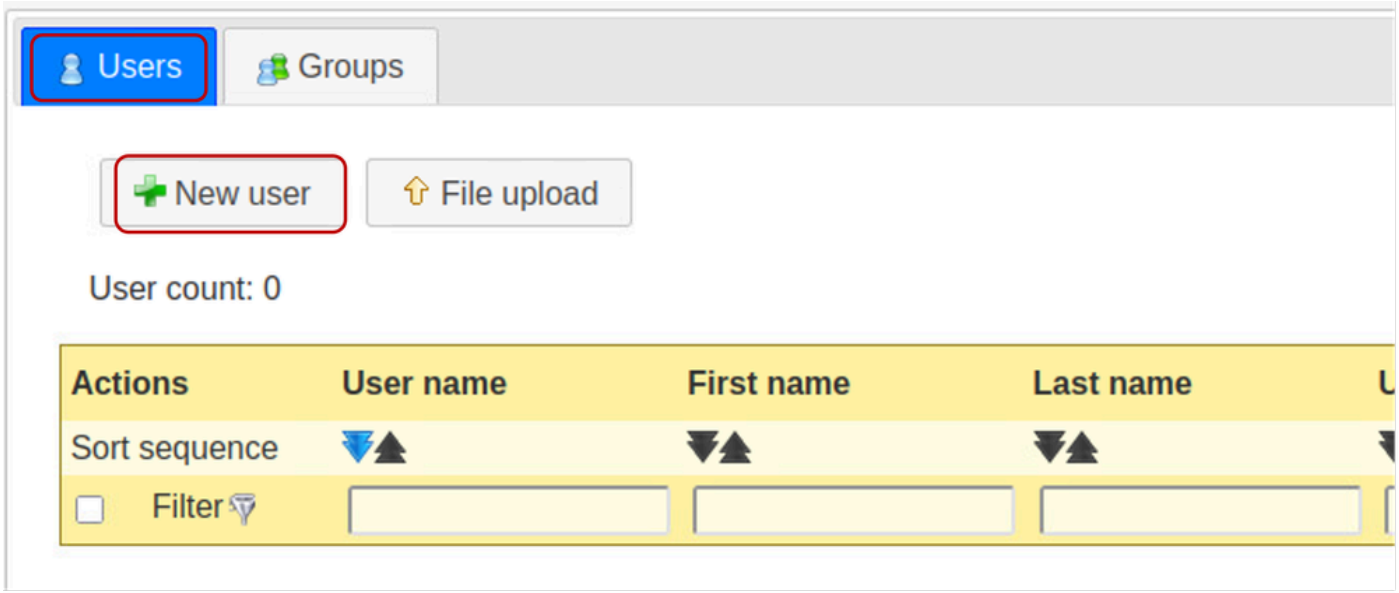
Note: Embora os sistemas Cisco UCS sejam geralmente resilientes a variações de casos, a manutenção de convenções de nomenclatura em minúsculas é uma prática recomendada para garantir a interoperabilidade de longo prazo em diversos ambientes de infraestrutura de servidor LDAP.

Deixe o campo Número GID em branco. O LDAP Account Manager (LAM) foi projetado para preencher automaticamente esse campo com o próximo valor disponível.

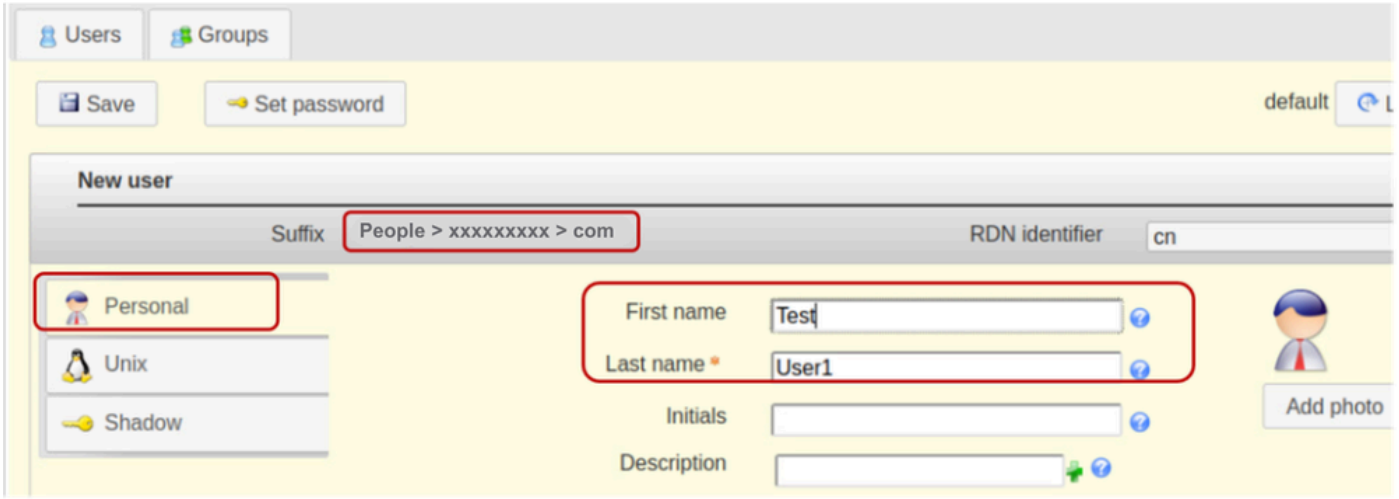
Forneça uma descrição, se desejar, e clique em Salvar



Clique na guia "Users" para criar contas de usuário e selecione "New user".



Preencha os campos obrigatórios para o usuário "testuser1" na guia Pessoal.

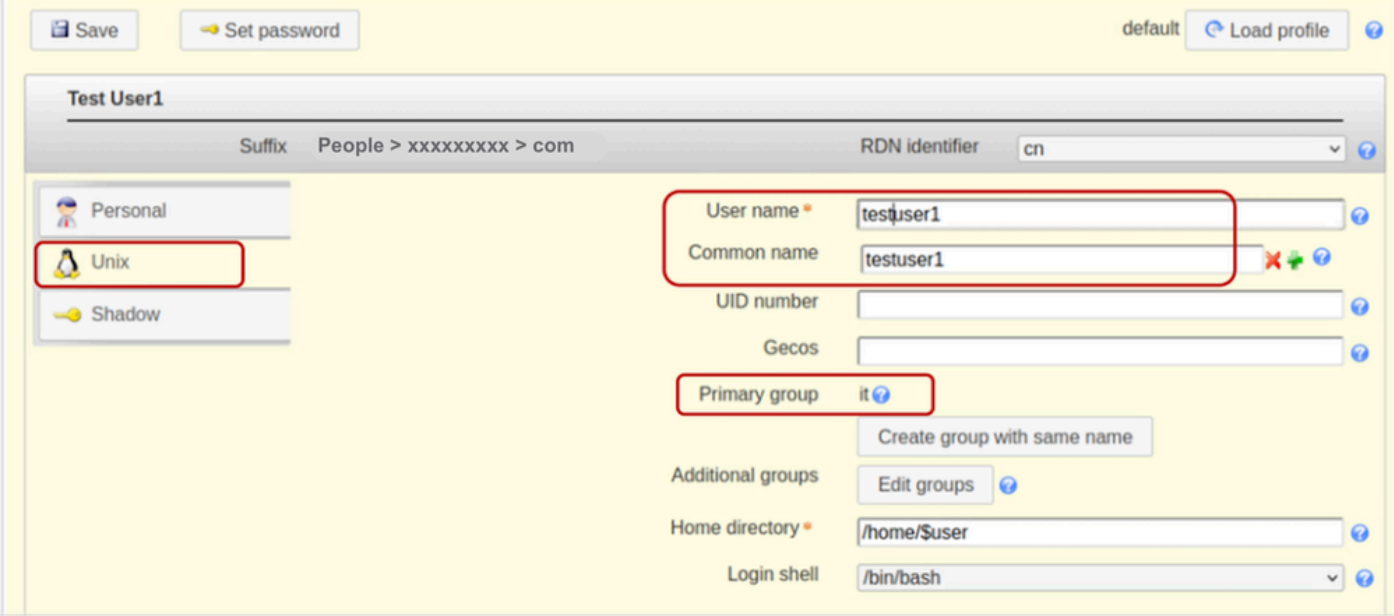


Selecione a guia Unix e adicione testuser1 no campo Nome de usuário. Inclua o usuário no grupo "ti".

Para esta demonstração, apenas o grupo "ti" existe, portanto, já está preenchido previamente.

Mantenha o identificador RDN como o "Common Name" (cn). Isso permite que o sistema preencha automaticamente o campo "Nome comum" usando o valor especificado no campo "Nome de usuário".

Deixe o campo Número UID em branco, pois o LAM preenche automaticamente o campo com valores disponíveis.



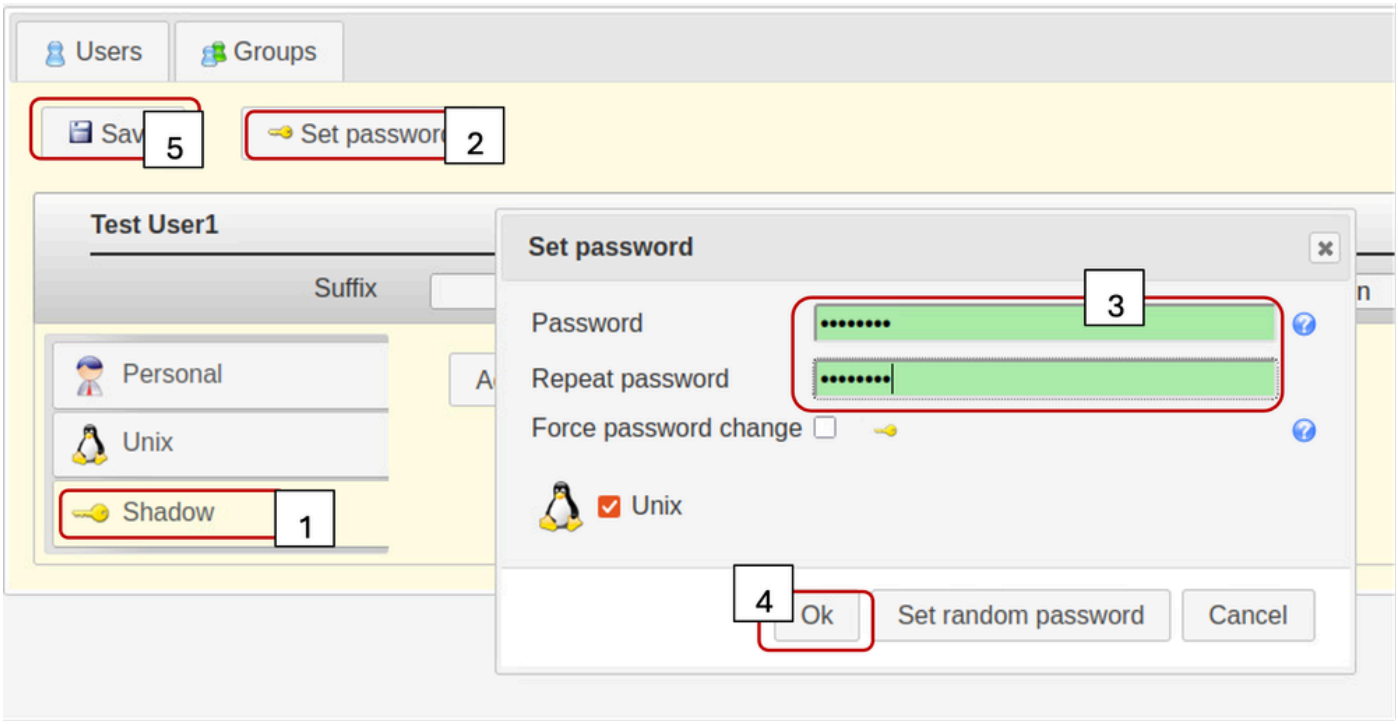
Selecione a guia Sombra,

A extensão da conta de sombra não é usada.

Clique em "Definir senha".

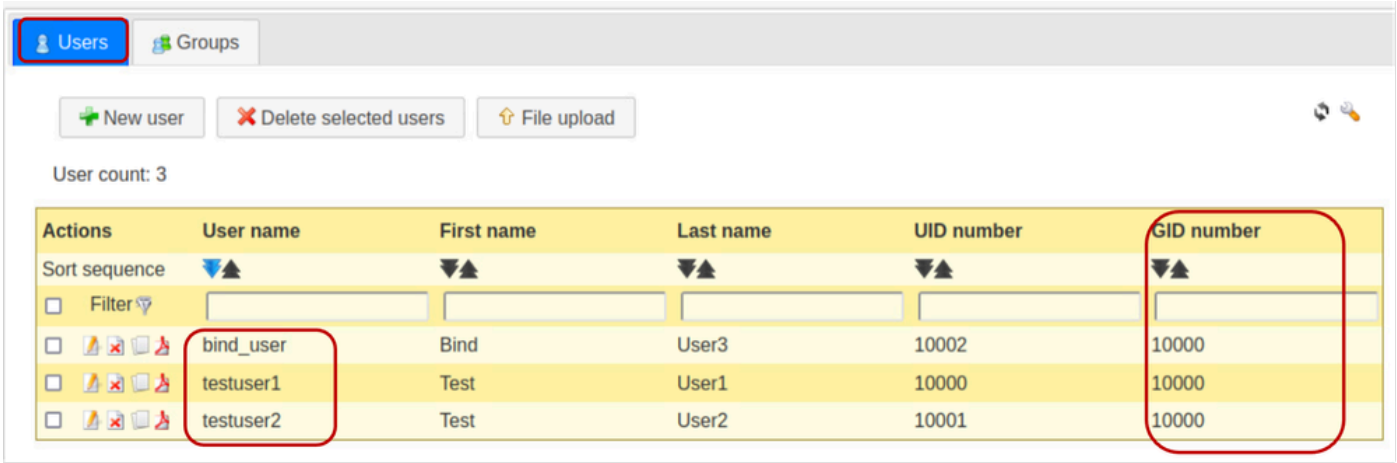
Definir a senha do usuário

Clique em OK e em Salvar



Repita as etapas especificadas descritas anteriormente para criar a conta de usuário "testuser2" e a conta "bind_user".

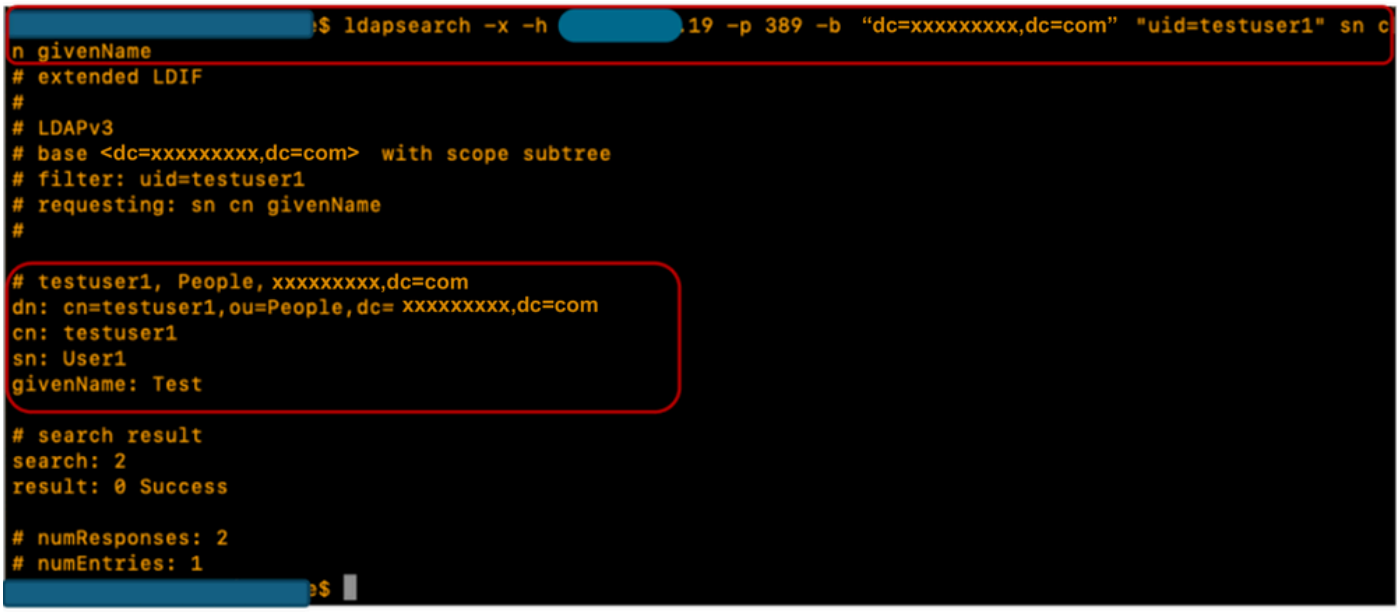
Clique na guia "Usuários" para verificar a criação de todos os usuários desejados. (Ter o mesmo valor na coluna gidNumber confirma que os usuários criados pertencem ao mesmo grupo - ele)



Etapa 6: Testa o login LDAP local

Efetue login em outro sistema baseado em Linux, tendo acesso ao servidor OpenLDAP. Execute o comando ldapsearch especificado para verificar se o LDAP funciona:

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



Parâmetros de configuração no CIMC

Faça login no CIMC.

No painel Navegação, selecione Admin, Gerenciamento de usuário e LDAP.

Preencha os parâmetros de configuração LDAP conforme mostrado abaixo:

- Habilitar LDAP: marcado
- DN base: dc=xxxxxxxx,dc=com

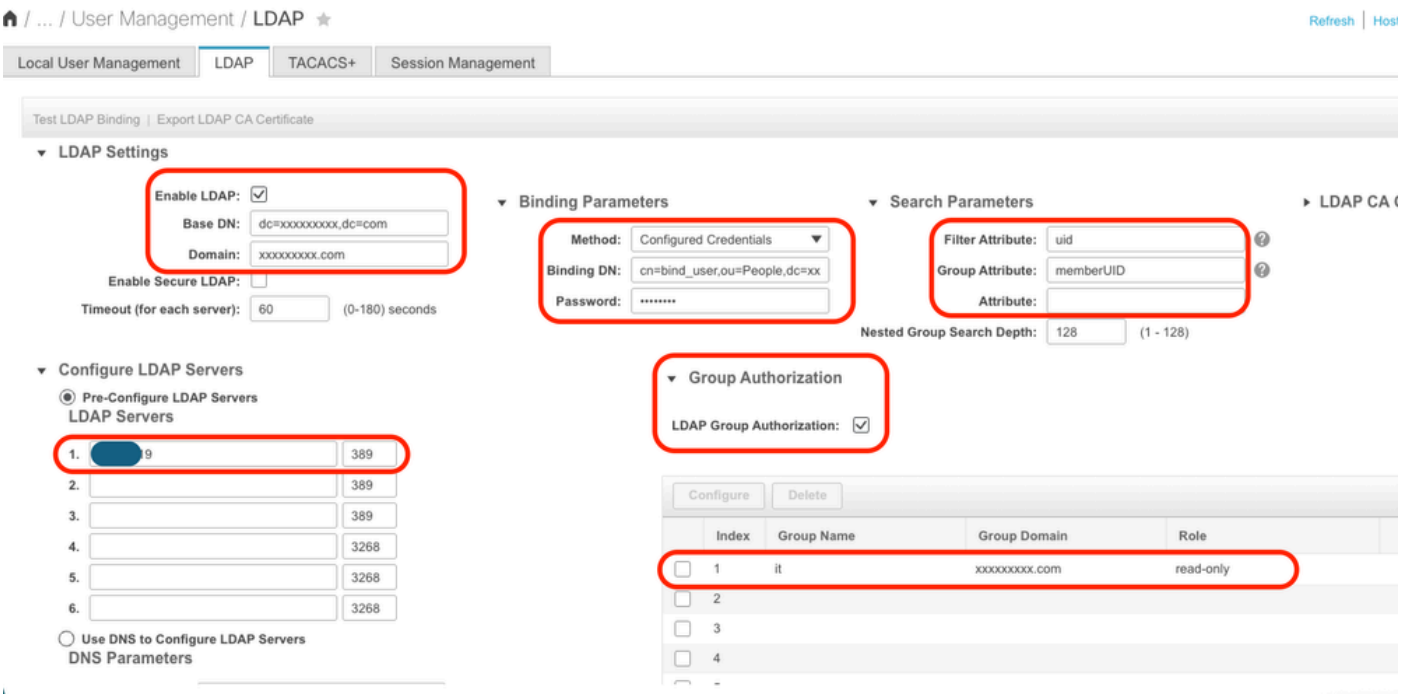
- Domínio: xxxxxxxxx.com

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

- Parâmetros de vinculação: "Credenciais de Logon" ou "Credenciais Configuradas"
  - Ao usar Credenciais configuradas, adicione o DN bind_user exatamente como configurado no servidor LDAP:
    - Por exemplo: cn=bind_user,ou=People,dc=xxxxxxxxx,dc=com

- Parâmetros de pesquisa:
  - Atributo de Filtro: "cn" ou "uid"
  - Atributo do grupo: memberUID

- Autorização de grupo LDAP - Verificada
  - Nome do grupo: o
  - Domínio do grupo: xxxxxxxxx.com
  - Função: somente leitura (qualquer função desejada)



Salve a configuração e teste o login do usuário LDAP.

Parâmetros de configuração no UCS Manager

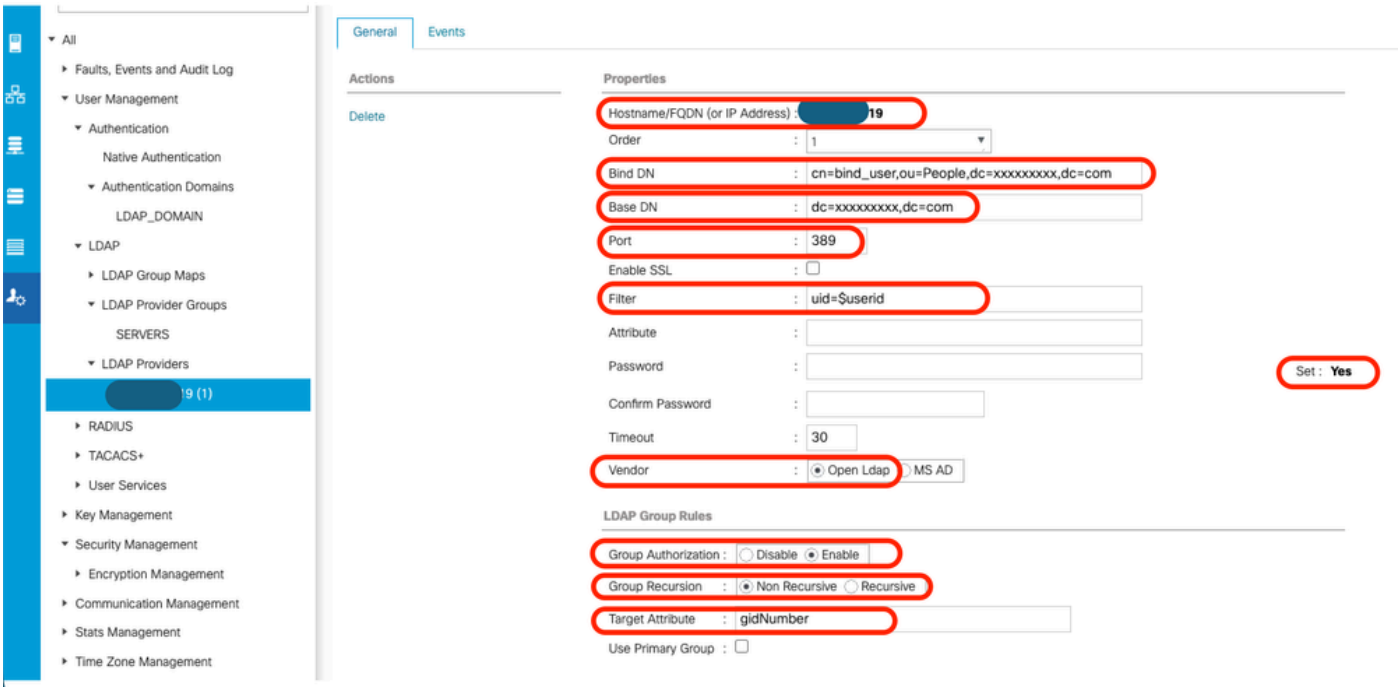
Faça login no UCS Manager.

No painel Navegação, selecione Admin, Gerenciamento de usuário e LDAP.

Preencha os parâmetros de configuração LDAP conforme mostrado abaixo:

- Provedores LDAP:
  - Nome do host: <FQDN ou endereço IP do servidor LDAP>
  - DN de vinculação: cn=bind_user,ou=People,dc=xxxxxxxxx,dc=com
  - DN base: dc=xxxxxxxx,dc=com
  - Porta: 389
  - Habilitar SSL: Desabilitado
  - Filtro: uid=$userid
  - Autorização do grupo: Habilitado
  - Recursão em grupo: Não Recursivo

    - Atributo de Destino: gidNumber
- Mapas de grupos LDAP:
    - DN do grupo LDAP: 10000 <gidNumber para "it" group>

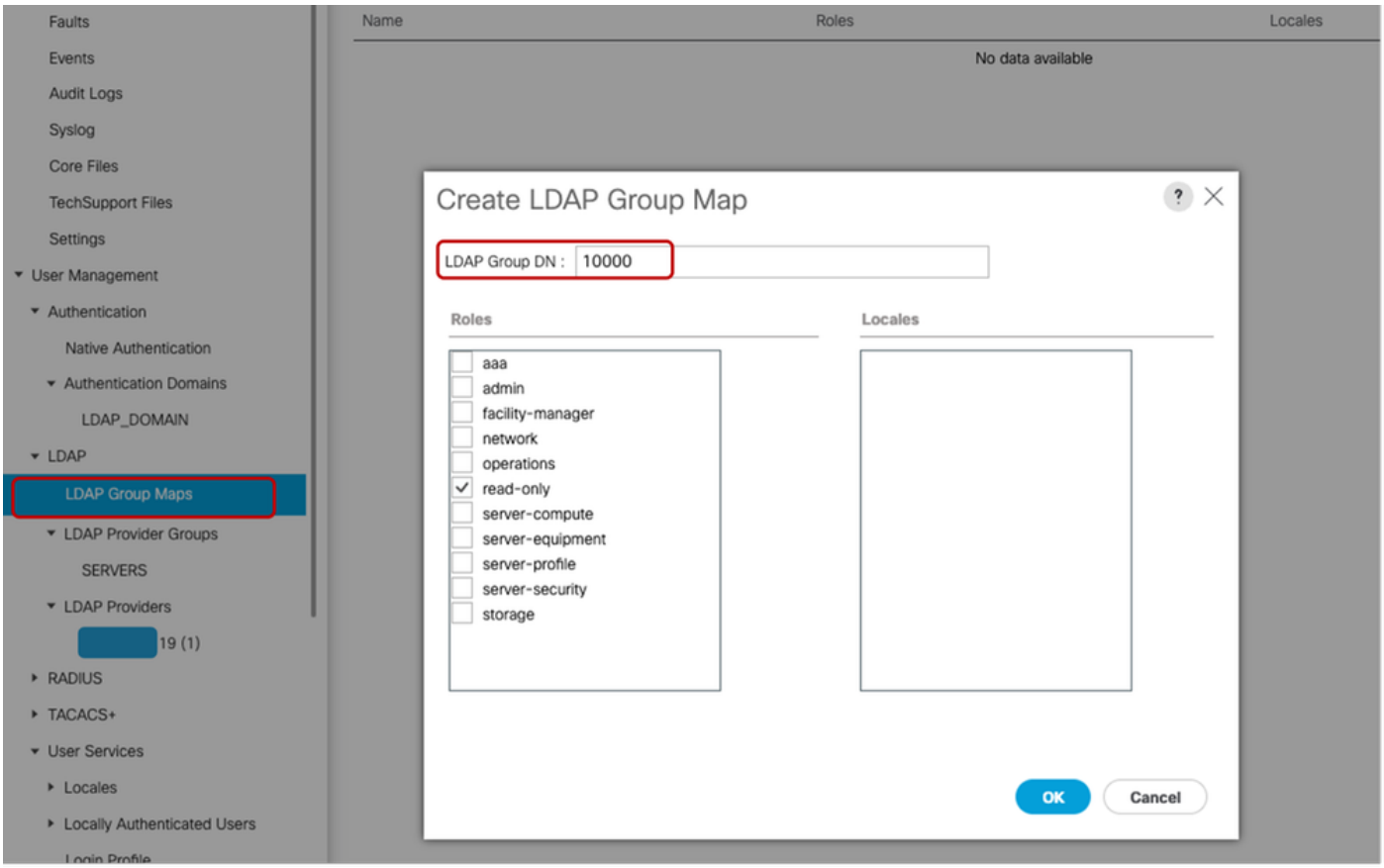


Em All >> User Management >> LDAP >> LDAP Providers>> LDAP Group Rules, o atributo de destino padrão do UCS Manager é "memberOf". Por padrão, os servidores OpenLDAP não têm esse atributo habilitado, portanto, definir o valor do atributo de destino como "memberOf" (ou deixá-lo em branco) faz com que os logons de usuário falhem porque o servidor OpenLDAP não reconhece o valor do atributo solicitado.

Neste exemplo, o valor "Atributo de destino" foi definido como "gidNumber".

Adicione o Provedor LDAP configurado a um Grupo de provedores LDAP. Para esta demonstração, o grupo de provedores LDAP "SERVIDORES" foi criado.

Ao configurar o "LDAP Group Maps" em "All >> User Management >> LDAP >> LDAP Group Maps>>", o valor gidNumber (nesse caso, "10000") é usado como o "Group DN Map", conforme mostrado:



Configure um Domínio de autenticação LDAP (LDAP_DOMAIN) em "All >> User Management >> Authentication >> Authentication Domains" (Todos > Gerenciamento de usuários > Autenticação >> Domínios de autenticação) referindo-se aos grupos de provedores LDAP e teste o login do usuário LDAP.

Note: Se o atributo memberOf for necessário para satisfazer requisitos ambientais específicos ou para implementar o recurso "Group Recursion", recomenda-se usar a segunda opção de configuração abaixo, que requer LDAP com extensões de sobreposição habilitadas.

Embora o LDAP Account Manager (LAM) suporte a configuração de sobreposição, lembre-se de que este recurso requer o licenciamento apropriado.

Para obter mais informações sobre a configuração do LDAP usando LAM, consulte a documentação oficial do Gerente de contas LDAP.

Opção 2: Configurar o OpenLDAP usando as ferramentas e sobreposições da CLI do Ubuntu

Para usar o OpenLDAP para autenticação do UCS Manager, são necessárias duas

sobreposições que garantam que os grupos estejam associados aos usuários de uma forma que o sistema UCS (UCS Manager e CIMC) possa entender.

A configuração no lado do OpenLDAP requer:

- sobreposição de "memberof": Essa sobreposição cria o mapeamento entre usuários e grupos de modo que, se um DN de usuário for consultado, o atributo memberOf possa ser solicitado como parte dessa consulta. Por padrão, nenhum atributo para usuários para associação de grupo, a menos que o membro da sobreposição seja adicionado a openLDAP
- sobreposição de "refinamento": Essa sobreposição é configurada para validar se as entradas no atributo de membro em objetos de grupo permanecem sincronizadas com o atributo memberOf de objetos de usuário. Sem esse serviço, se um usuário for excluído sem também modificar o grupo, os DNs órfãos podem permanecer no objeto do grupo. O serviço refinado garante consistência em ambas as direções.

Etapa 1: ferramentas de rede iniciais e configurar o nome de host do servidor Linux

Repita a Etapa 1 na Opção 1.

Etapa 2: Instalar o SLAPD

Repita a Etapa 2 na Opção 1. (Com exceção da instalação do PHP e Apache, pois a Opção 2 não exige que eles funcionem - sem LAM)

Certifique-se de permitir as portas necessárias através do firewall do Ubuntu.

Passo 3: Instalar a sobreposição 'memberOf' no servidor LDAP

Verifique se a sobreposição "memberOf" está instalada

```
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
```

Para instalar a sobreposição "memberOf", crie um arquivo .ldif chamado ldap.memberof.load.ldif (use qualquer convenção de nomenclatura desejada) e adicione a configuração especificada:

```
cat <


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

Adicione a configuração no arquivo ldap.memberof.load.ldif ao perfil LDAP usando o comando especificado:

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

Configura o módulo memberOf e a entrada olcDatabase para corresponder aos requisitos de implantação, dependendo das distribuições do linux.

Dois valores de atributo obrigatórios são "olcDatabase={1}mdb" e "groupOfNames", como mostrado abaixo.

Crie o arquivo ldap.memberof.config.ldif, preencha seus atributos e importe seu conteúdo para o perfil LDAP.

```
cat <


      ./ldap.memberof.config.ldif
dn: olcOverlay=memberof,olcDatabase={1}mdb,cn=config
objectClass: olcMemberOf
objectClass: olcOverlayConfig
olcOverlay: memberof
```

```
olcMemberOfGroupOC: groupOfNames
olcMemberOfMemberAD: member
olcMemberOfMemberOfAD: memberOf
olcMemberOfRefInt: TRUE
olcMemberOfDangling: ignore
EOF
```

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

Passo 4: Instalar a Sobreposição 'refint' no servidor LDAP

Em seguida, Instalar refint para openldap:

crie um arquivo .ldif chamado ldap.refint.load.ldif (use qualquer convenção de nomenclatura desejada) e adicione a configuração especificada:

```
cat <
```

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

Importe a configuração no arquivo ldap.refint.load.ldif para o perfil LDAP usando o comando especificado:

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

Configure o refinamento, que mantém a integridade referencial entre grupos e usuários.

Configura o módulo refint e sua entrada olcDatabase para corresponder aos requisitos de implantação.

Crie o arquivo ldap.refint.config.ldif e importe seu conteúdo para o perfil LDAP.

```
cat <


      ./ldap.refint.config.ldif
dn: olcOverlay=refint,olcDatabase={1}mdb,cn=config
objectClass: olcConfig
objectClass: olcOverlayConfig
objectClass: olcRefintConfig
olcOverlay: refint
olcRefintAttribute: memberOf member
EOF
```

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

Após a instalação de ambos os plug-ins/extensões, a saída para o comando ldapsearch especificado é semelhante à saída mostrada abaixo:

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

```
test@test:~$ sudo ldapsearch -Q -LLL -Y EXTERNAL -H ldapi:/// -b cn=config '(olcModuleLoad=*)'
dn: cn=module{0},cn=config
objectClass: olcModuleList
cn: module{0}
olcModulePath: /usr/lib/ldap
olcModuleLoad: {0}back_mdb

dn: cn=module{1},cn=config
objectClass: olcModuleList
cn: module{1}
olcModuleLoad: {0}memberof

dn: cn=module{2},cn=config
objectClass: olcModuleList
cn: module{2}
olcModuleLoad: {0}refint
```

Quando ambos os plug-ins/extensões estão configurados, a saída para o comando ldapsearch especificado é semelhante à saída mostrada:

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

```
test@test:~$ sudo ldapsearch -Q -LLL -Y EXTERNAL -H ldapi:/// -b cn=config '(olcOverlay=memberof)'
dn: olcOverlay={0}memberof,olcDatabase={1}mdb,cn=config
objectClass: olcMemberOfConfig
objectClass: olcOverlayConfig
olcOverlay: {0}memberof
olcMemberOfDangling: ignore
olcMemberOfRefInt: TRUE
olcMemberOfGroupOC: groupOfNames
olcMemberOfMemberAD: member
olcMemberOfMemberOfAD: memberOf

test@test:~$
```

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

```
test@test:~$ sudo ldapsearch -Q -LLL -Y EXTERNAL -H ldapi:/// -b cn=config '(olcOverlay=refint)'
dn: olcOverlay={1}refint,olcDatabase={1}mdb,cn=config
objectClass: olcConfig
objectClass: olcOverlayConfig
objectClass: olcRefintConfig
olcOverlay: {1}refint
olcRefintAttribute: memberOf member
```

Reinicie o serviço slapd para que os plug-ins/módulos recém-instalados possam ser usados:

```
sudo systemctl restart slapd
```

Passo 5: Criar OUs, Usuários e Grupos

Crie unidades organizacionais (para usuários e grupos), usuários e grupos.

Crie as OUs de Usuários (Pessoas) e Grupos (Grupos) e importe-as para o perfil LDAP. Isso exige a senha da conta "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
```

Crie os Usuários (testuser1, testuser2 e bind_user), mapeie-os para suas respectivas OUs (Pessoas), adicione-os a seus Grupos usando gidNumbers (boa prática) e importe os usuários para o perfil LDAP.

```
cat <
```

```
      ./ldap.users.ldif
dn: uid=testuser1,ou=People,dc=xxxxxxxxx,dc=com
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: shadowAccount
uid: testuser1
sn: User1
givenName: Test
cn: testuser1
displayName: Test User1
gidNumber: 10000
uidNumber: 10000
userPassword: cisco123
gecos: Test User1
loginShell: /bin/bash
homeDirectory: /home/testuser1

dn: uid=testuser2,ou=People,dc=xxxxxxxxx,dc=com
objectClass: inetOrgPerson
```

```
objectClass: posixAccount
objectClass: shadowAccount
uid: testuser2
sn: User2
givenName: Test
cn: testuser2
displayName: Test User2
gidNumber: 10000
uidNumber: 10001
userPassword: cisco123
gecos: Test User2
loginShell: /bin/bash
homeDirectory: /home/testuser2

dn: uid=bind_user,ou=People,dc=xxxxxxxxx,dc=com
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: shadowAccount
uid: bind_user
sn: User3
givenName: Bind
cn: bind_user
displayName: Bind User3
gidNumber: 10001
uidNumber: 10002
userPassword: cisco123
gecos: Bind User3
loginShell: /bin/bash
homeDirectory: /home/bind_user
EOF
```

```
sudo ldapadd -xcWD cn=admin,dc=xxxxxxxxx,dc=com -f ./ldap.users.ldif
```

```
test@test:~$ cat <<EOF > ./ldap.users.ldif
dn: uid=testuser1,ou=People,dc=xxxxxxxxx,dc=com
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: shadowAccount
uid: testuser1
sn: User1
givenName: Test
cn: testuser1
displayName: Test User1
gidNumber: 10000
uidNumber: 10000
userPassword: cisco123
gecos: Test User1
loginShell: /bin/bash
homeDirectory: /home/testuser1

dn: uid=testuser2,ou=People,dc=xxxxxxxxx,dc=com
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: shadowAccount
uid: testuser2
sn: User2
givenName: Test
cn: testuser2
displayName: Test User2
gidNumber: 10000
uidNumber: 10001
userPassword: cisco123
gecos: Test User2
loginShell: /bin/bash
homeDirectory: /home/testuser2


dn: uid=bind_user,ou=People,dc=xxxxxxxxx,dc=com
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: shadowAccount
uid: bind_user
sn: User3
givenName: Bind
cn: bind_user
displayName: Bind User3
gidNumber: 10001
uidNumber: 10002
userPassword: cisco123
gecos: Bind User3
loginShell: /bin/bash
homeDirectory: /home/bind_user
EOF
test@test:~$ sudo ldapadd -xcWD  cn=admin,dc=xxxxxxxxx,dc=com -f ./ldap.users.ldif
Enter LDAP Password:
adding new entry "uid=testuser1,ou=People,dc=xxxxxxxxx,dc=com

adding new entry "uid=testuser2,ou=People,dc=xxxxxxxxx,dc=com

adding new entry "uid=bind_user,ou=People,dc=xxxxxxxxx,dc=com

test@test:~$
```

Crie os grupos (ele), mapeie-os para suas respectivas OUs (Grupos), associe membros de grupo (testuser1, testuser2) e importe-os para o perfil LDAP:

```
cat <


      ./ldap.group.create.ldif
dn: cn=it,ou=Groups,dc=xxxxxxxxx,dc=com
objectClass: groupofnames
cn: it
member: uid=testuser1,ou=People,dc=xxxxxxxxx,dc=com
member: uid=testuser2,ou=People,dc=xxxxxxxxx,dc=com
EOF
```

```
sudo ldapadd -xcWD cn=admin,dc=xxxxxxxxx,dc=com -f ./ldap.group.create.ldif
```

Note: Mesmo que o atributo memberOf não seja explicitamente definido durante a criação de Usuários ou Grupos, o sistema gera e mantém automaticamente essa referência. Quando o usuário estiver associado a um grupo, o atributo memberOf refletirá essas associações automaticamente, garantindo que o diretório permaneça sincronizado com a estrutura de acesso atual.

Etapa 6: Testa o login LDAP local

Verifique o login do usuário no servidor LDAP usando o comando especificado (substitua os parâmetros de login dependendo do seu 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:~$
```

Parâmetros de configuração no CIMC

Faça login no CIMC.

No painel Navegação, selecione Admin, Gerenciamento de usuário e LDAP.

Preencha os parâmetros de configuração LDAP conforme mostrado abaixo:

- Habilitar LDAP: marcado
- DN base: dc=xxxxxxxx,dc=com

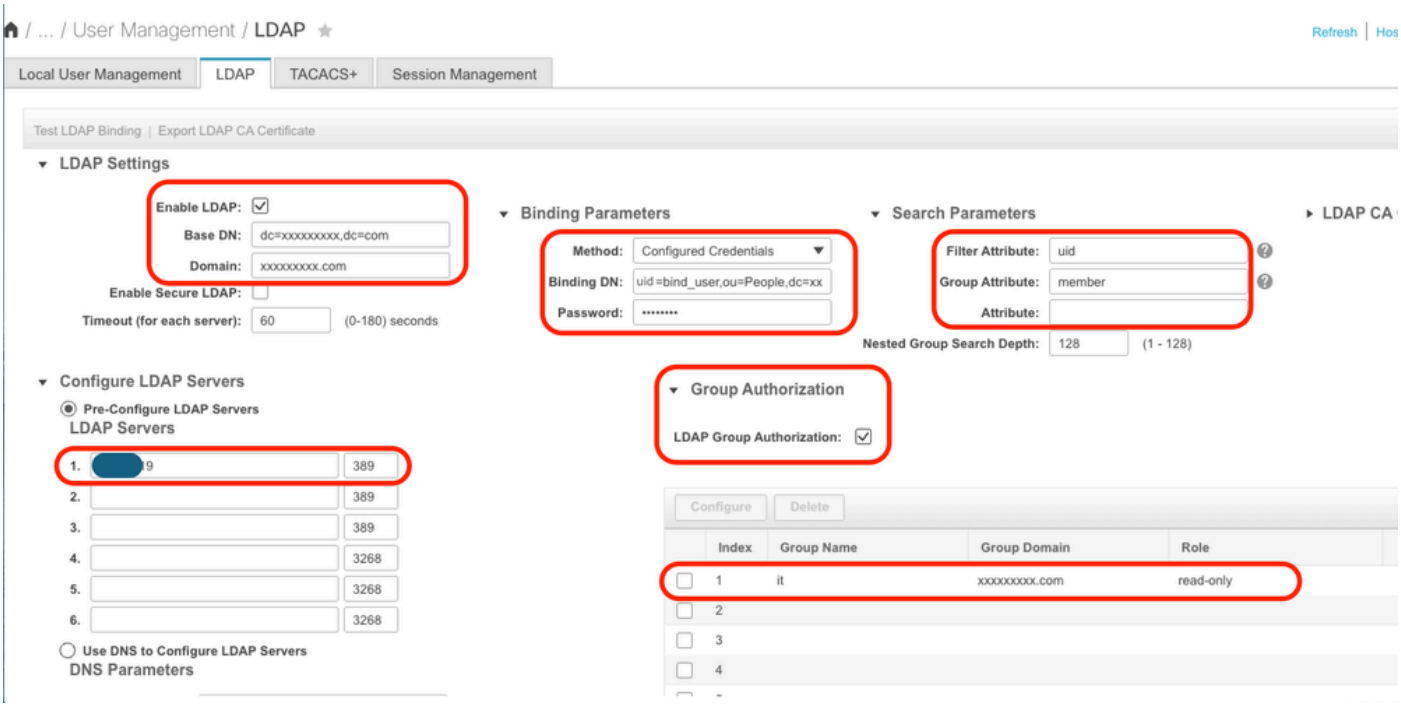
- Domínio: xxxxxxxxx.com

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

- Parâmetros de vinculação: Pode ser "Credenciais de login" ou "Credenciais configuradas"
  - Ao usar Credenciais configuradas, adicione o DN bind_user exatamente como configurado no servidor LDAP:
  - Por exemplo: "cn=bind_user,ou=People,dc=xxxxxxxx,dc=com" ou "uid=bind_user,ou=People,dc=xxxxxxxx,dc=com"

- Parâmetros de pesquisa:
  - Atributo de Filtro: "cn" ou "uid"
  - Atributo do grupo: membro

- Autorização de grupo LDAP - Verificada
  - Nome do grupo: o
  - Domínio do grupo: xxxxxxxxx.com
  - Função: somente leitura (qualquer função preferencial)



Salve a configuração e teste o login do usuário LDAP.

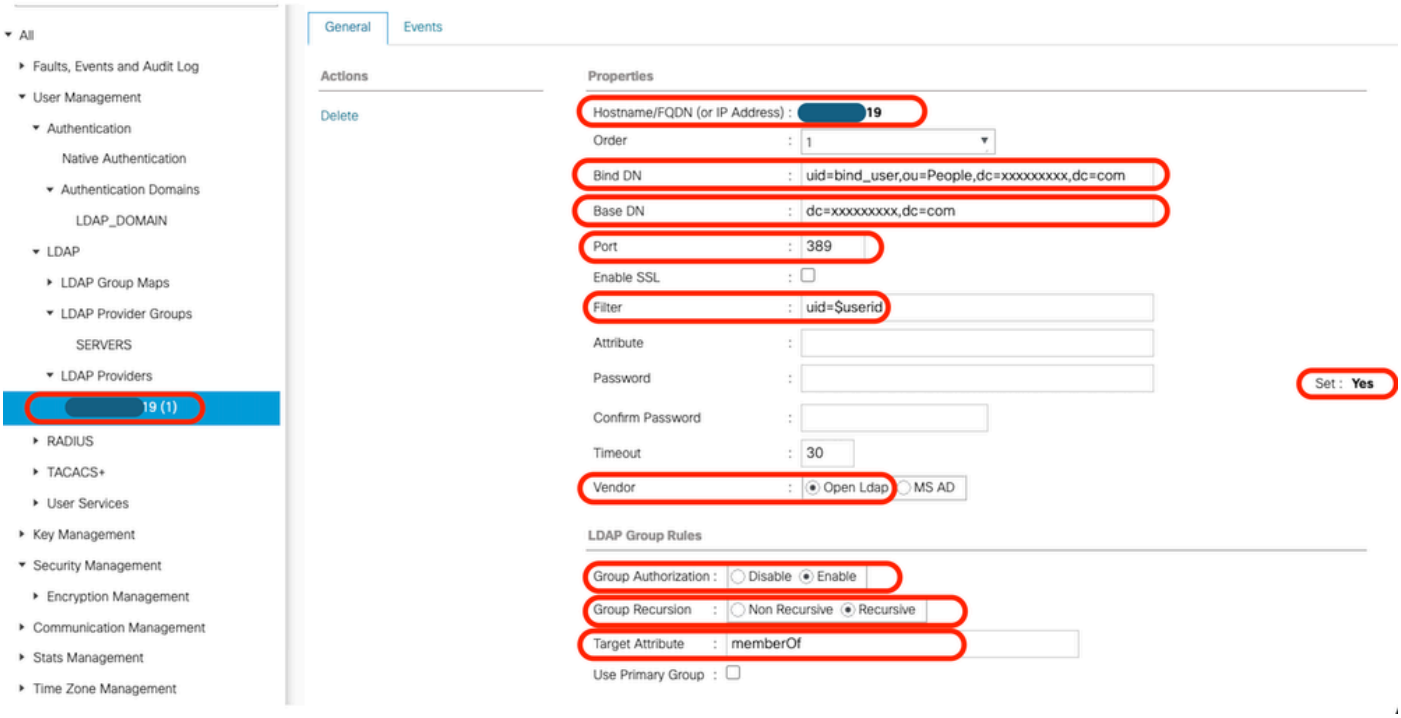
Parâmetros de configuração no UCS Manager

Faça login no UCS Manager.

No painel Navegação, selecione Admin, Gerenciamento de usuário e LDAP.

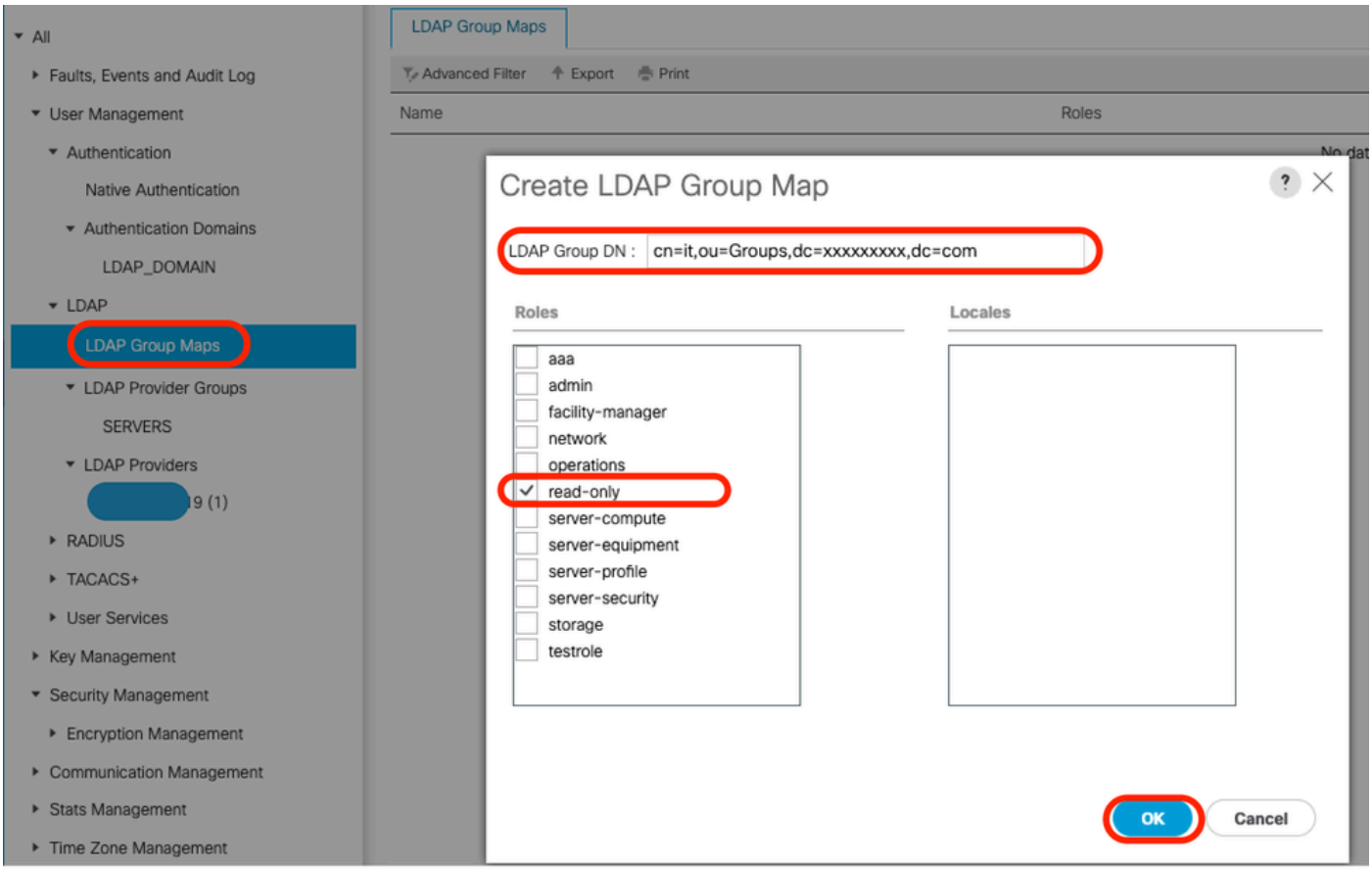
Preencha os parâmetros de configuração LDAP conforme mostrado abaixo:

- Provedores LDAP:
  - Nome do host: <FQDN ou endereço IP do servidor LDAP>
  - DN de vinculação: uid=bind_user,ou=Pessoas,dc=xxxxxxxxx,dc=com
  - DN base: dc=xxxxxxxx,dc=com
  - Porta: 389
  - Habilitar SSL: Desabilitado
  - Filtro: uid=$userid
  - Autorização do grupo: Habilitado
  - Recursão em grupo: Recursivo
  - Atributo de Destino: membroDe
- Mapas de grupos LDAP:
  - DN do grupo LDAP: cn=it,ou=Groups,dc=xxxxxxxxx,dc=com



Adicione o Provedor LDAP configurado a um Grupo de provedores LDAP. Para esta demonstração, o grupo de provedores LDAP "SERVIDORES" é usado.

Configure os mapas de grupo LDAP adicionando um "LDAP Group DN", recuperado do servidor LDAP.



Configure um domínio de autenticação LDAP (LDAP_DOMAIN) em "All >> User Management >> Authentication >> Authentication Domains" (Todos >> Gerenciamento de usuários >> Autenticação >> Domínios de autenticação) referindo-se a LDAP Provider Groups(SERVERS) (Grupos de provedores LDAP) e teste o login do usuário LDAP.

Em seguida, vamos analisar a configuração do mesmo (com Sobreposição) em uma distribuição Linux separada (CentOS 10)

Cenário 2: Fluxo 10 do CentOS - Fedora

Os procedimentos de configuração do Lightweight Diretory Access Protocol (LDAP) variam de acordo com a versão do sistema operacional subjacente. Esta seção se concentra na implementação de LDAP no CentOS Stream 10.

Enquanto muitas distribuições Linux utilizam OpenLDAP, CentOS Stream 10 e sistemas contemporâneos baseados no Fedora utilizam o 389 Diretory Server (389 DS) como o provedor LDAP padrão.

Note: Embora o 389 DS seja considerado o sucessor do OpenLDAP nos ecossistemas CentOS e Red Hat, as duas soluções não são diretamente intercambiáveis. Suas respectivas estruturas de diretório, arquivos de configuração e ambientes operacionais são significativamente diferentes.

Este guia fornece as etapas necessárias para configurar com êxito o LDAP usando 389 DS em um ambiente CentOS Stream 10.

Opção 1: Configure o LDAP usando o 389 Diretory Server no CentOS Stream 10

Passo 1: Configuração inicial

Repita a Etapa 1 no Cenário 1, Opção 1.

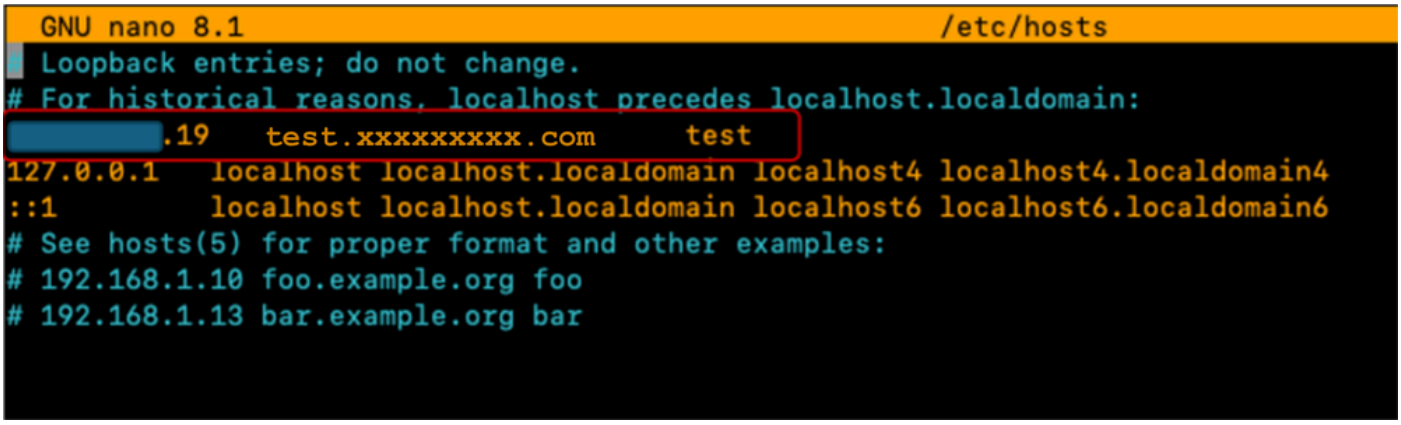
Os sistemas CentOS não utilizam o pacote de gerenciamento APT. Para executar as instalações de software necessárias no CentOS Stream 10, use os gerenciadores de pacotes dnf (Dandified YUM) ou yum

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

Verifique o endereço IP do servidor usando o comando "ifconfig".

Adicione o endereço IP do servidor ao arquivo "/etc/hosts", juntamente com o nome de domínio totalmente qualificado do servidor (Por exemplo: test.xxxxxxxx.com usado neste laboratório) e o nome do host (Por exemplo: test) no formato especificado abaixo:

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



Atualize o arquivo "/etc/hostname" substituindo seu conteúdo pelo nome do host (teste).

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

É necessário reinicializar o servidor para que essas alterações entrem em vigor.

```
sudo reboot
```

Passo 2: Instalar pacote EPEL repo e 389 Server

Instalar e atualizar o repositório EPEL.

Instale o pacote 389 Diretory Server.

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

Crie um arquivo de Modelo de Diretório que contenha os parâmetros de configuração do Servidor LDAP desejados:

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

Verificar o conteúdo do arquivo de modelo criado (ldapconfig.conf)

```
sudo cat ldapconfig.conf
```

Edite o arquivo de modelo ldapconfig.conf.

```
sudo nano ldapconfig.conf
```

Insira as entradas de configuração especificadas no arquivo e salve suas alterações.

Nota:Podem ser necessárias diferentes modificações de acordo com as necessidades específicas ou os requisitos de cada ambiente.

Este exemplo aborda as configurações de linha de base para esta demonstração.

```
[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
```

O arquivo de gabarito define os parâmetros de configuração para a instância do diretório "localhost". Isso inclui a configuração do usuário administrativo ("admin"), a senha associada e o contexto de domínio ("xxxxxxxx.com").

Crie a instância de diretório "localhost" usando o gabarito editado anteriormente. O comando especificado cria e inicia o servidor de Diretório LDAP:

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

Verifique se o serviço LDAP está em execução no servidor

```
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:~$
```

Ajuste o firewall CentOS para permitir as portas necessárias para LDAP (389 e/ou 636).

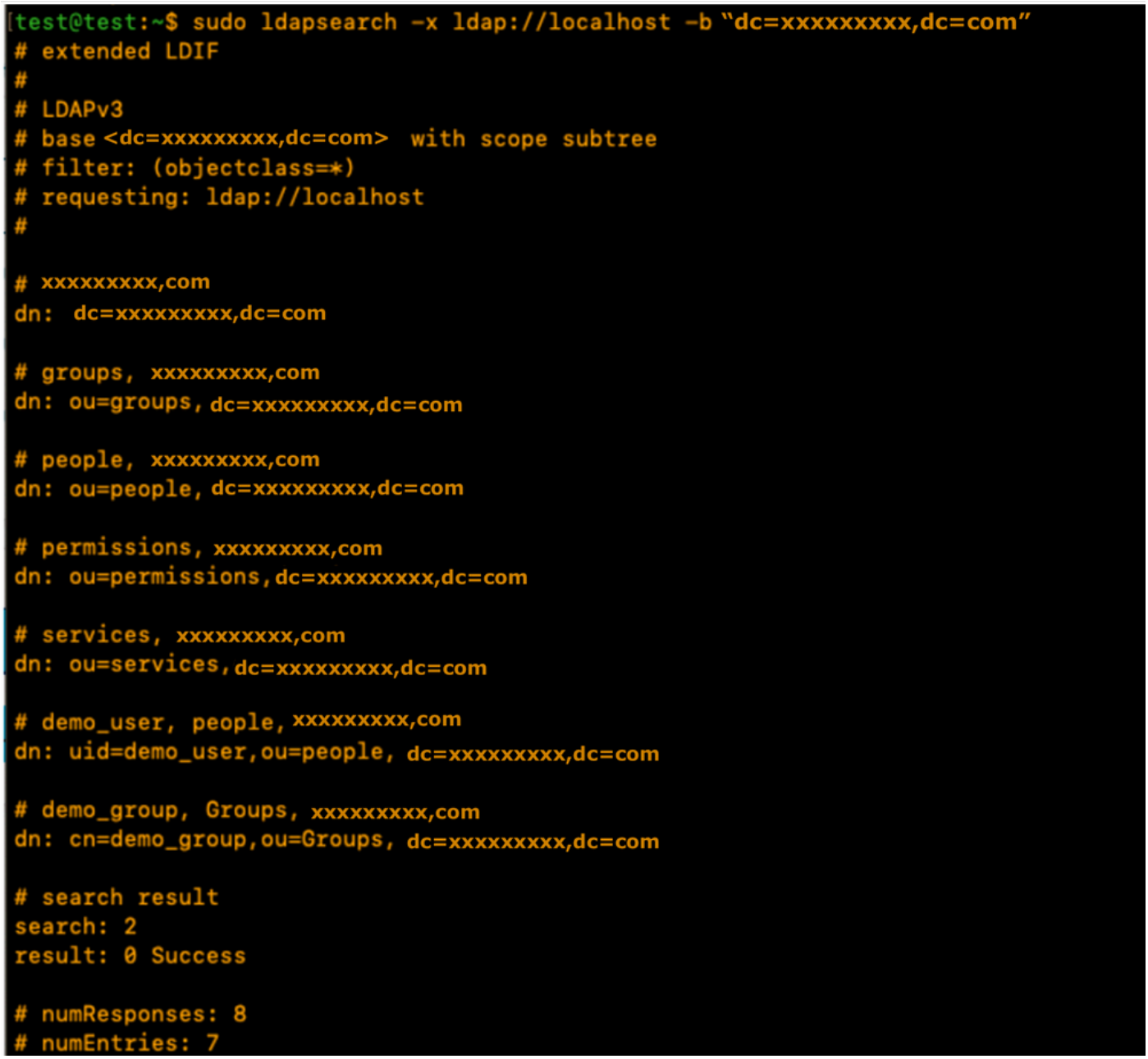
Para esta demonstração, o firewall está desligado.

```
sudo systemctl stop firewalld
```

Verifique se o LDAP funciona localmente no servidor LDAP executando o comando especificado

e certifique-se de que ele retorne a saída LDAP como mostrado:

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



A saída contém contas de demonstração criadas pelo servidor 389DS. O servidor LDAP criou automaticamente OUs padrão.

A OU de pessoas para Usuários e a OU de Grupos para Grupos. UOs adicionais podem ser criadas dependendo do requisito.

Para esta demonstração, são usadas as OUs padrão/criadas automaticamente.

Consulte a documentação oficial do 389DS para obter detalhes sobre o uso extensivo do pacote do 389DS:

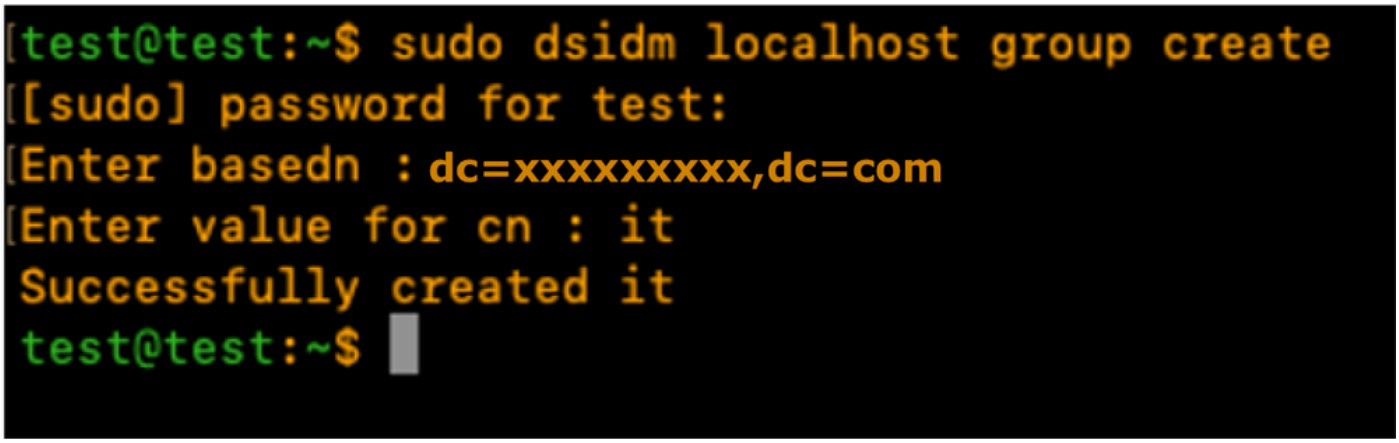
Passo 3: Criar grupos e usuários LDAP

Crie um grupo (ele) usando o comando especificado: sudo dsidm <nome_da_instância> group create.

Para esta demonstração, o nome da instância é "localhost".

```
sudo dsidm localhost group create
```

Insira o prompt do terminal para preencher os detalhes do grupo como mostrado:



Crie a conta do usuário testuser1 usando o comando:

```
sudo dsidm localhost user create
```

Insira o prompt do terminal para preencher os detalhes do usuário como mostrado

```
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
```

Crie uma senha para testuser1 usando o comando especificado e digite o 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:~$
```

Adicione o usuário a um grupo usando o comando especificado: "sudo dsidm <diretory_instance> group add_member <group_cn> <user_dn>"

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

Repita as etapas de criação do usuário para criar testuser2 e bind_user.

Nota:Certifique-se de que cada usuário seja explicitamente adicionado aos grupos desejados.

Omitir essa etapa pode resultar em falhas de autorização ou acesso restrito.

A conta bind_user não precisa ser membro de um grupo específico, pois pode ser configurada como uma conta autônoma, fornecendo flexibilidade para gerenciar o acesso administrativo e de nível de serviço no ambiente de diretório.

Reinicie a instância do Diretory:

```
sudo dsctl localhost restart
```

Passo 4: Instalar sobreposição memberOf

Instale o plug-in "memberOf" e reinicie a instância do Diretório:

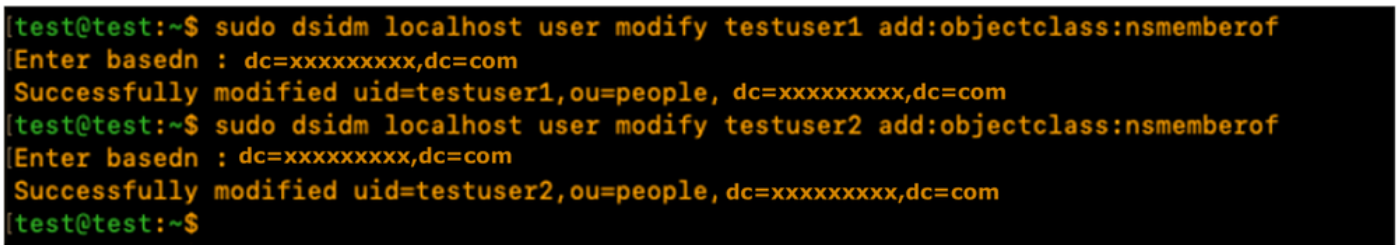
```
sudo dsconf localhost plugin memberof status
sudo dsconf localhost plugin memberof enable
sudo dsctl localhost restart
```

Configure o plug-in "memberOf" usando o comando especificado: "sudo dsconf <instância_de_diretório> plugin memberof set —scope <base_dn>"

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

Marque Usuários como destinos "memberOf" válidos usando o comando especificado: "sudo dsidm <instância_de_diretório> user modify <uid> add:objectclass:nsmemberof"

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



Gerar ajuste "memberOf" para o DN base: "sudo dsconf <instância_de_diretório> membro plugin de fixup <base_dn>"

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

```
test@test:~$ sudo dsconf localhost plugin memberof fixup dc=xxxxxxxxx,dc=com
Adding fixup task entry...
Successfully added task entry "cn=memberOf_fixup_2025-05-13T14:54:11.926390,cn=memberOf task,cn=tasks,cn=config". Th
is task is running in the background. To track its progress you can use the "fixup-status" command.
test@test:~$
```

Verifique a configuração do usuário:

```
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:~$
```

O servidor LDAP 389DS é configurado com o plug-in memberOf para suportar o atributo memberOf.

Parâmetros de configuração no CIMC

Faça login no CIMC.

No painel Navegação, selecione Admin, Gerenciamento de usuário e LDAP.

Preencha os parâmetros de configuração LDAP conforme mostrado abaixo:

- Habilitar LDAP: marcado
- DN base: dc=xxxxxxxx,dc=com

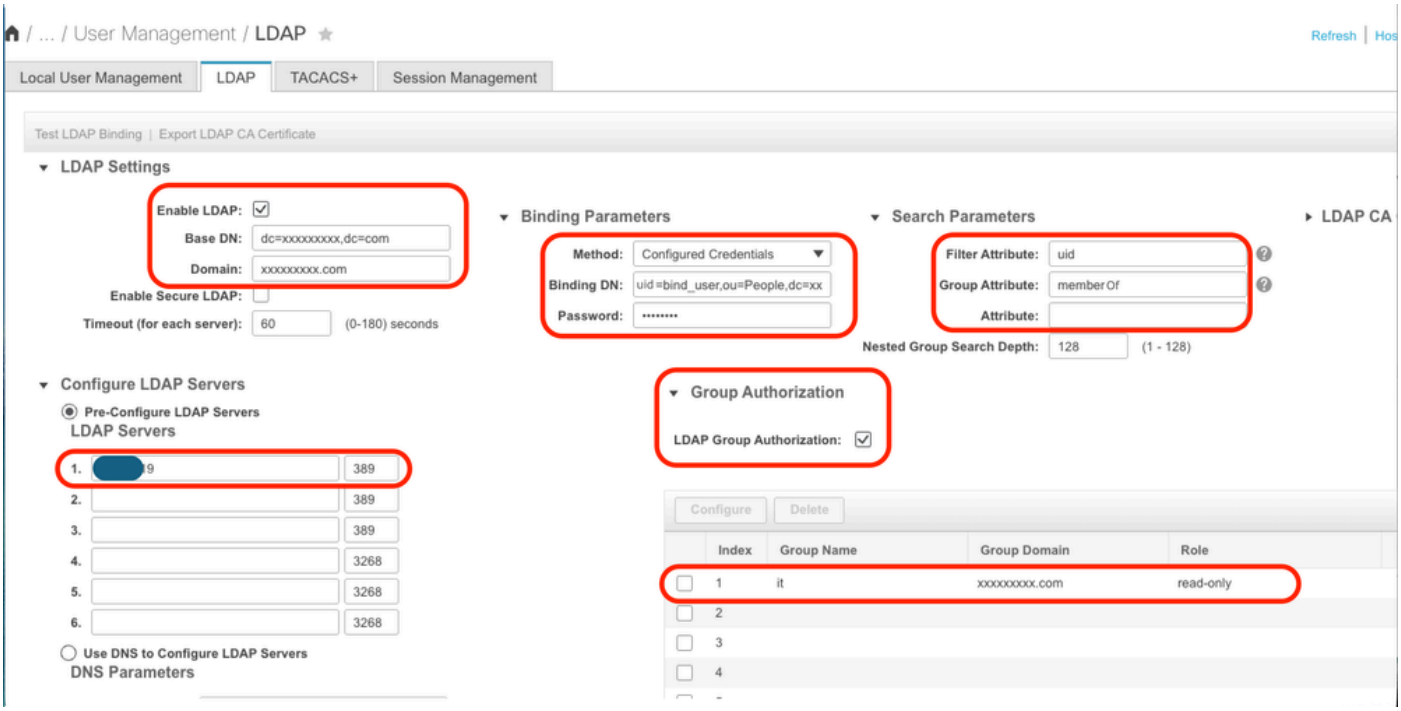
- Domínio: xxxxxxxxx.com

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

- Parâmetros de vinculação: Pode ser "Credenciais de login" ou "Credenciais configuradas"
  - Ao usar Credenciais configuradas, adicione o DN bind_user exatamente como configurado no servidor LDAP:
    - Por exemplo: "cn=bind_user,ou=People,dc=xxxxxxxx,dc=com" ou "uid=bind_user,ou=People,dc=xxxxxxxx,dc=com"

- Parâmetros de pesquisa:
  - Atributo de Filtro: "cn" ou "uid"
  - Atributo do grupo: membroDe

- Autorização de grupo LDAP - Verificada
  - Nome do grupo: o
  - Domínio do grupo: xxxxxxxxx.com
  - Função: somente leitura (qualquer função preferencial)



Salve a configuração e teste o login do usuário LDAP.

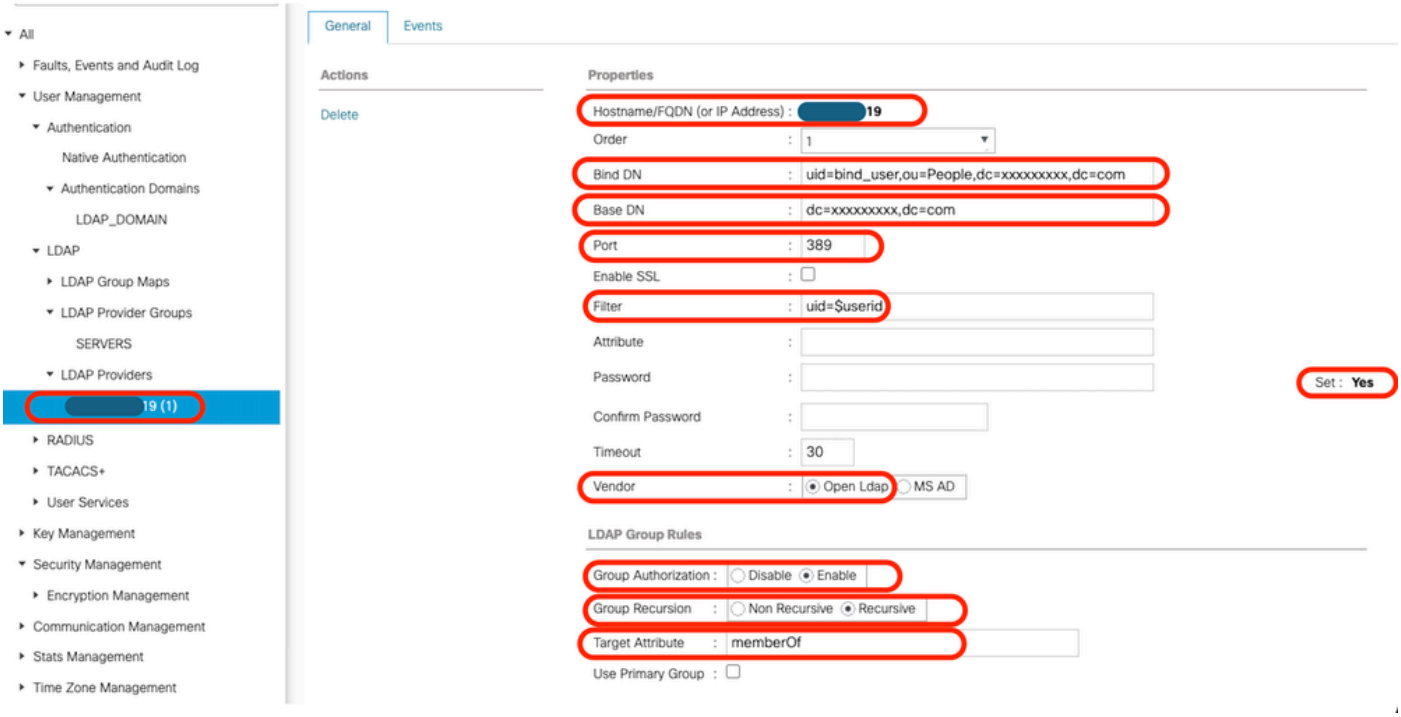
Parâmetros de configuração no UCS Manager

Faça login no UCS Manager.

No painel Navegação, selecione Admin, Gerenciamento de usuário e LDAP.

Preencha os parâmetros de configuração LDAP conforme mostrado abaixo:

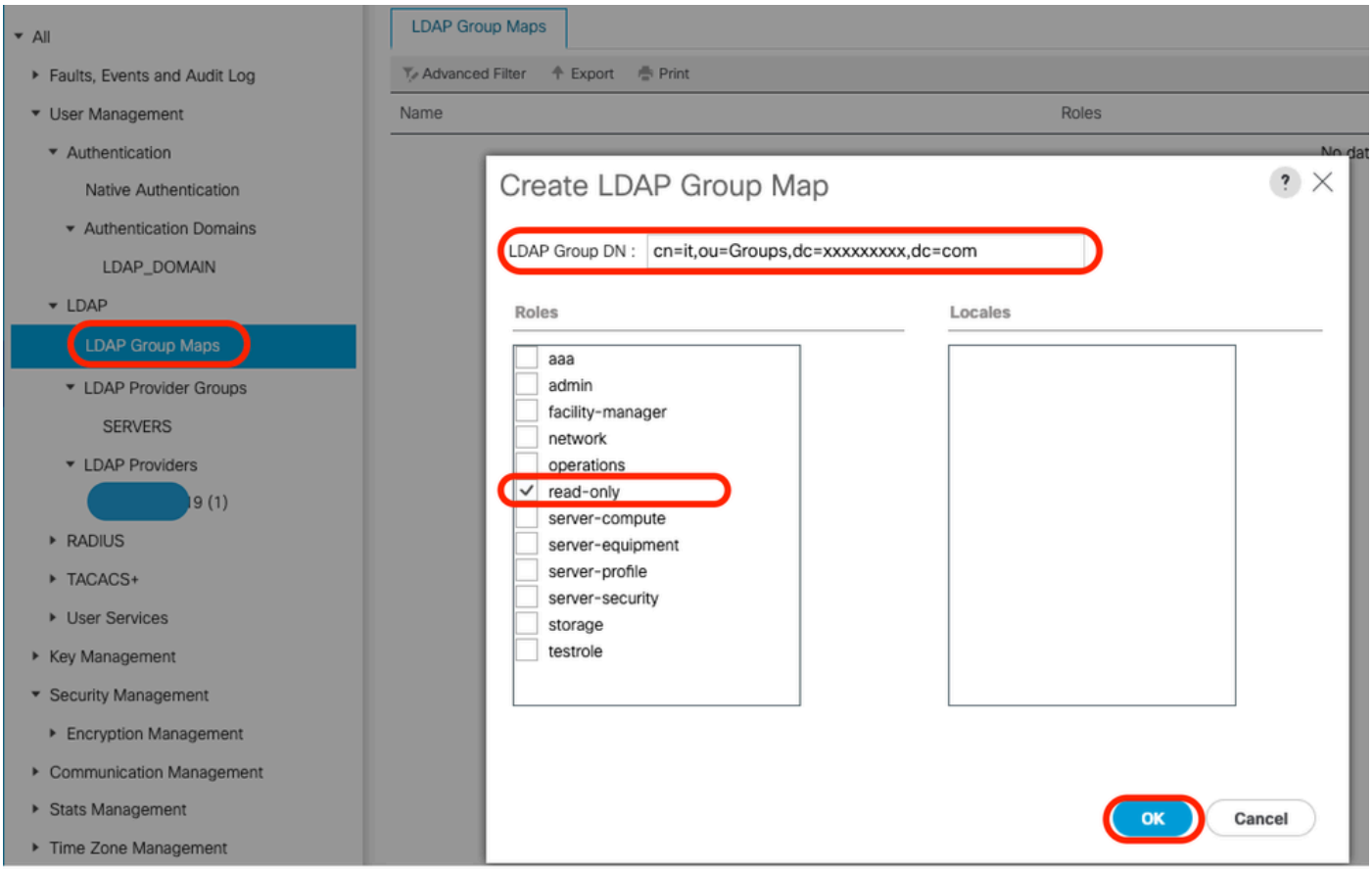
- Provedores LDAP:
  - Nome do host: <FQDN ou endereço IP do servidor LDAP>
  - DN de vinculação: uid=bind_user,ou=pessoas,dc=xxxxxxxx,dc=com
  - DN base: dc=xxxxxxxx,dc=com
  - Porta: 389
  - Habilitar SSL: Desabilitado
  - Filtro: uid=$userid
  - Autorização do grupo: Habilitado
  - Recursão em grupo: Recursivo
  - Atributo de Destino: membroDe
- Mapas de grupos LDAP:
  - DN do grupo LDAP: cn=it,ou=Groups,dc=xxxxxxxxx,dc=com



Adicione o Provedor LDAP configurado a um Grupo de provedores LDAP. Para esta

demonstração, o grupo de provedores LDAP "SERVIDORES" é usado.

Configure os mapas de grupo LDAP adicionando um "LDAP Group DN", recuperado do servidor LDAP.



Configure um domínio de autenticação LDAP (LDAP_DOMAIN) em "All >> User Management >> Authentication >> Authentication Domains" (Todos >> Gerenciamento de usuários >> Autenticação >> Domínios de autenticação) referindo-se aos LDAP Provider Groups (Grupos de provedores LDAP) e test LDAP user login (Testar login do usuário LDAP).

Conclusão

Embora este guia aborde cenários de implantação essenciais, a exploração adicional de recursos LDAP pode melhorar significativamente o desempenho e a segurança do diretório.

Para obter informações adicionais, práticas recomendadas e detalhes de configuração avançados, consulte os recursos especificados:

- Documentação oficial do OpenLDAP

- Gerenciador de contas LDAP - Manual
- Documentação do 389 Diretory Server
- Configurar LDAP no UCS Manager
- Configurar LDAP seguro em servidores UCS C Series

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.