Servidor de Diretório

Sumário

Índice de tabelas

Índice de Figuras

Capítulo 1

Servidor de Diretório

- Prática dos comandos (slap...);
- Prática dos comandos (ldap...);
- Backup e restore da base.

1.1. Mãos a obra

O gerenciamento de um servidor de diretório pode ser feito através de comandos, obtidos através da instalação dos pacotes slapd e ldap-utils. A diferença de uso entre eles é definido quando o serviço do LDAP esta rodando ou esta parado. Neste caso termo comandos a “quente” e comandos a “frio”. Exemplo:

Para adicionar novas entradas ao servidor quando estiver rodando:
ldapadd (comando a quente)

Para adicionar novas entradas ao servidor quando estiver parado:
ldapadd (comando a frio)

Prática dos comandos (slap...)

Digite no terminal slap e tecle o Tab duas vezes para exibir os comandos que iniciam com ldap.

```
# slap (Tab 2x)
```

```
slapacl     slapauth    slapd       slapindex   slaptest
slapadd     slapcat     slapdn      slappasswd
```

Veja na lista comandos que são usados pelo sysadmin (root). Para ver na prática os comandos abaixo, pare o serviço Slapd.

```
# invoke-rc.d slapd stop
```

Slaptest

Testa a syntax no arquivo de configuração do Slapd. Exemplo:

```
# slaptest
```

```
config file testing succeeded
```

Slapcat

Lista o conteúdo da base de dados. Usado também para criar backup redirecionando a saída da lista para um arquivo. Exemplo:

 # slapcat | less

```
dn: dc=empresa,dc=com,dc=br
objectClass: top
objectClass: dcObject
objectClass: organization
o: empresa.com.br
dc: empresa
structuralObjectClass: organization
entryUUID: 79a08666-a6f0-102f-91c7-3b67a01c5ddc
creatorsName:
createTimestamp: 201012281705542
entryCSN: 20101228170554.331967Z#000000#000#000000
modifiersName:
modifyTimestamp: 201012281705542

dn: cn=admin,dc=empresa,dc=com,dc=br
objectClass: simpleSecurityObject
objectClass: organizationalRole
cn: admin
description: LDAP administrator
userPassword:: e2NyeXB0fVFxRTBYVHFoc2hBMms=
structuralObjectClass: organizationalRole
entryUUID: 79a2a5f4-a6f0-102f-91c8-3b67a01c5ddc
creatorsName:
createTimestamp: 201012281705542
:_
```

Opções de uso do comando:

-c → Continua a operação mesmo que tenha erros;

-v → Ativa o modo verbose;

-b → Especifica a base de dados a ser modificada;

-f → Especifica o arquivo de configuração do slapd;

-F → Especifica o diretório de configuração;

Slapindex

Realiza a indexação da base.

Use o comando grep para pesquisar intens não indexados no arquivo de log

```
# grep index /var/log/syslog
```

```
Dec 28 15:38:33 server slapd[3419]: <= bdb_equality_candidates: (cn) not indexed
Dec 28 15:38:39 server slapd[3419]: <= bdb_equality_candidates: (cn) not indexed
Dec 28 15:38:44 server slapd[3419]: <= bdb_equality_candidates: (cn) not indexed
```

Abra o arquivo de configuração do Slapd e adicione atributo cn para ser indexado

```
# vim /etc/ldap/slapd.conf
```

```
# Indexing options for database #1
index           objectClass     eq
index           cn              eq
```

Use o comando slapindex com a flag -v para acompanhar a indexação

```
# slapindex -v
```

```
WARNING!
Runnig as root!
There's a fair chance slapd will fail to start.
Check file permissions!

indexing id=00000001
indexing id=00000002
indexing id=00000003
indexing id=00000004
indexing id=00000005
indexing id=00000006
indexing id=00000007
indexing id=00000008
indexing id=00000009
indexing id=0000000a
indexing id=0000000b
indexing id=0000000c
indexing id=0000000d
indexing id=0000000e
indexing id=0000000f
indexing id=00000010
indexing id=00000011
indexing id=00000012
indexing id=00000013
indexing id=00000014
```

Ajuste as permissões dos arquivos

 # vim /etc/ldap/slapd.conf

Inicie o serviço do Slapd

 # invoke-rc.d slapd start

Slappasswd

Comando usado para gerar senhas para usuários da base Ldap. Com a flag -h é possível selecionar o tipo de algorítimo. Exemplos

CRYPT

 # slappasswd -h {CRYPT}

```
New password:
Re-enter new password:
{CRYPT}A2ZEE6kcGDspQ
```

MD5

```
# slappasswd -h {MD5}
```

```
New password:
Re-enter new password:
{MD5}4QrcOUm6Wau+VuBX8g+IPg==
```

SMD5

```
# slappasswd -h {SMD5}
```

```
New password:
Re-enter new password:
{SMD5}KtTNYbPdVn08ODo84TtBf1oMysI=
```

SSHA

```
# slappasswd -h {SSHA}
```

```
New password:
Re-enter new password:
{SSHA}ySKUDKrDoXkvUc8PY95AUEOQiONuiRoX
```

SHA

```
# slappasswd -h {SHA}
```

```
New password:
Re-enter new password:
{SHA}fEqNCco3Yq9h5ZUglD3CZJT4lBs=
```

Slapadd

Comando usado para adicionar dados off-line à base LDAP (quando o servidor não estiver rodando). Não esqueça de parar o serviço do Slapd. Exemplo:

```
# slapadd -v -l usuarios.ldif
```

Opções de uso do comando:

-c → Continua a operação mesmo que tenha erros;

-v → Ativa o modo verbose;

-b → Especifica a base de dados a ser modificada;

-f → Especifica o arquivo de configuração do slapd;

-F → Especifica o diretório de configuração;

-l → Especifica o arquivo .ldif com as informações que serão adicionadas na base LDAP.

Prática dos comandos (ldap...)

Digite no terminal ldap e tecle o Tab duas vezes para exibir os comandos que iniciam com ldap. Os comandos abaixo podem ser usados com o serviço em andamento. Exemplo:

```
# ldap (Tab 2x)
```

```
ldapadd      ldapdelete   ldapmodrdn   ldapsearch
ldapcompare  ldapmodify   ldappasswd   ldapwhoami
```

Ldapsearch

Realiza pesquisa na base LDAP. Exemplo:

```
# ldapsearch -x  -LLL -b dc=empresa,dc=com,dc=br uid=aluno
```

```
dn: uid=aluno,ou=People,dc=empresa,dc=com,dc=br
uid: aluno
cn: Aluno Linux
objectClass: account
objectClass: posixAccount
objectClass: top
objectClass: shadowAccount
shadowMax: 99999
shadowWarning: 7
loginShell: /bin/bash
uidNumber: 1000
gidNumber: 1000
homeDirectory: /home/aluno
gecos: Aluno Linux,,,
```

Opções de uso do comando:

-x → Autenticação simples, o método padrão é via SASL;

-ZZ → Autenticação que pede conexão segura (TLS);

-L → Formato de saída LDIF-v1;

-LL → Suprime comentários;

-LLL → Suprime o nome da versão;

-b → Base de pesquisa;

-h → Host onde o serviço esta rodando;

-p → Porta usado pelo servidor LDAP.

-s → Define o escopo da pesquisa. As opções são: base, one e sub

- base - Busca apenas na base DN

- one - busca no mesmo nível do “galho” definido em -b e em mais um sub-nível

- sub - opção padrão, busca recursivamente a partir do “galho”

Exemplo de uso pesquisando dois usuários

```
# ldapsearch -x  -LLL -b dc=empresa,dc=com,dc=br '(|(uid=aluno)(uid=joao))'
```

Operadores

& → “E” devem constar todas as condições no comando;

| → “OU” pode atender uma condição ou a outra;

! → Negação.

Ldapwhoami

Exibe o nome do usuário logado da base LDAP.

```
# ldapwhoami  -x -D cn=admin,dc=empresa,dc=com,dc=br -W
```

```
Enter LDAP Password:
dn:cn=admin,dc=empresa,dc=com,dc=br
```

Ldapadd

Adicione informações à base do LDAP com o servidor em funcionamento. Exemplo:

```
# ldapadd -x -D cn=admin,dc=empresa,dc=com,dc=br -f usuarios.ldif  -W
```

Opções de uso do comando:

-x → Autenticação simples, o método padrão é via SASL;

-ZZ → Autenticação que pede conexão segura (TLS);

-c → Continua a operação mesmo que tenha erros;

-D → Especifica o DN a ser usado;

-w → Especifica a senha do administrador do LDAP;

-W → Chama um prompt para digitar a senha do administrador do LDAP;

-f → Especifica o arquivo .ldif com as informações que serão incluídas na base LDAP;

-h → Host onde o serviço esta rodando;

-p → Porta usado pelo servidor LDAP.

Ldapdelete

Comando usado para excluir da base LDAP um objeto especificando o seu DN completo. Exemplo:

```
# ldapdelete -x -D cn=admin,dc=empresa,dc=com,dc=br
uid=aluno,ou=People,dc=empresa,dc=com,dc=br -W
```

Ldapmodrdn

Comando usado para renomear da base LDAP um objeto, atraves de um arquivo .ldif.

Primeiro crie um arquivo para adicionar uma nova OU

```
# vim printers.ldif
dn: ou=Printers,dc=empresa,dc=com,dc=br
objectClass: organizationalUnit
ou: Printers
```

Adicione a nova entrada a base LDAP

```
# ldapadd -x -D cn=admin,dc=empresa,dc=com,dc=br -f printers.ldif -W
```

```
Enter LDAP Password:
adding new entry "ou=Printers,dc=empresa,dc=com,dc=br"
```

Realize a pesquisa da nova entrada

```
# ldapsearch -x -LLL -b dc=empresa,dc=com,dc=br ou=Printers
```

```
dn: ou=Printers,dc=empresa,dc=com,dc=br
objectClass: organizationalUnit
ou: Printers
```

Crie o arquivo .ldif usado para renomear a entrada na base.

```
# vim renomeia-printers.ldif
ou=Printers,dc=empresa,dc=com,dc=br
ou=Impressoras
```

Use o comando ldapmodrdn para renomear a entrada OU

```
# ldapmodrdn -x  -D cn=admin,dc=empresa,dc=com,dc=br -r -f  renomeia-printers.ldif -W
```

Realize a pesquisa e verifique a nova OU renomeada

```
# ldapsearch -x  -LLL -b dc=empresa,dc=com,dc=br ou=Impressoras
```

```
dn: ou=Impressoras,dc=empresa,dc=com,dc=br
objectClass: organizationalUnit
ou: Impressoras
```

Ldapmodify

Permite fazer alterações nos atributos de um objeto através de uma arquivo .ldif

Opções de uso do comando:

-x → Autenticação simples, o método padrão é via SASL;

-ZZ → Autenticação que pede conexão segura (TLS);

-c → Continua a operação mesmo que tenha erros;

-D → Especifica o DN a ser usado;

-w → Especifica a senha do administrador do LDAP;

-W → Chama um prompt para digitar a senha;

-h → Host onde o serviço esta rodando;

-p → Porta usado pelo servidor LDAP;

-f → Especifica o arquivo com as informações que serão alteradas na base.

Tipos de alterações usadas no arquivo .ldif:

add → Adiciona um novo o atributo;
dn: completo
ação: atributo
atributo: valor

Exemplo de um arquivo .ldif para adicionar atributos

```
# vim adiciona.ldif
dn: uid=maria,ou=People,dc=empresa,dc=com,dc=br
add: title
title: Gerente
```

Exemplo prático:

```
# ldapmodify -x -D cn=admin,dc=empresa,dc=com,dc=br -f adiciona.ldif -W
```

replace → Substitui um atributo existente
dn: completo
ação: atributo
atributo: valor

Exemplo de um arquivo .ldif para substituir atributos:

```
# vim substituir.ldif
dn: uid=maria,ou=People,dc=empresa,dc=com,dc=br
replace: loginShell
loginShell: /bin/sh
```

Exemplo prático:

```
# ldapmodify -x -D cn=admin,dc=empresa,dc=com,dc=br -f substituir.ldif
-W
```

delete → Exclui um atributo.

dn: completo

ação: atributo

atributo: valor

Exemplo de um arquivo .ldif para excluir atributos:

```
# vim deleta.ldif
dn: uid=maria,ou=People,dc=empresa,dc=com,dc=br
delete: title
```

Exemplo prático:

```
# ldapmodify -x -D cn=admin,dc=empresa,dc=com,dc=br -f deleta.ldif -W
```

Backup e restore da base

Backup

Para realizar o Backup utilize o comando Slapcat para redirecionar todo conteúdo da base para um arquivo ldif. Vamos a prática :

Primeiro pare o serviço Slapd

```
# invoke-rc.d slapd stop
```

Faça o backup da base com o comando Slapcat

```
# slapcat -v -l backup.ldif
```

Restore

Para realizar o Restore da base, vamos simular a perda total de todos os dados, para depois restaurar usando os dados do arquivo backup.ldif. Vamos a prática:

Acesse o diretório e remova todos os arquivos da base

```
# cd /var/lib/ldap
# rm *
```

Inicie o serviço Slapd e use o comando slapcat para ver que a base esta vazia

```
# invoke-rc.d slapd start
# slapcat
```

Para restaurar os dados pare o serviço Slapd, e use o comando Slapadd para adicionar os dados do arquivo backup.ldif

```
# invoke-rc.d slapd stop
# slapadd -v -l backup.ldif
```

```
added: "dc=empresa,dc=com,dc=br" (00000001)
added: "cn=admin,dc=empresa,dc=com,dc=br" (00000002)
added: "ou=Hosts,dc=empresa,dc=com,dc=br" (00000003)
added: "ou=Rpc,dc=empresa,dc=com,dc=br" (00000004)
added: "ou=Services,dc=empresa,dc=com,dc=br" (00000005)
added: "nisMapName=netgroup.byuser,dc=empresa,dc=com,dc=br" (00000006)
added: "ou=Mounts,dc=empresa,dc=com,dc=br" (00000007)
added: "ou=Networks,dc=empresa,dc=com,dc=br" (00000008)
added: "ou=People,dc=empresa,dc=com,dc=br" (00000009)
added: "ou=Group,dc=empresa,dc=com,dc=br" (0000000a)
added: "ou=Netgroup,dc=empresa,dc=com,dc=br" (0000000b)
added: "ou=Protocols,dc=empresa,dc=com,dc=br" (0000000c)
added: "ou=Aliases,dc=empresa,dc=com,dc=br" (0000000d)
added: "nisMapName=netgroup.byhost,dc=empresa,dc=com,dc=br" (0000000e)
added: "cn=root,ou=Group,dc=empresa,dc=com,dc=br" (0000000f)
added: "cn=daemon,ou=Group,dc=empresa,dc=com,dc=br" (00000010)
added: "cn=bin,ou=Group,dc=empresa,dc=com,dc=br" (00000011)
added: "cn=sys,ou=Group,dc=empresa,dc=com,dc=br" (00000012)
added: "cn=adm,ou=Group,dc=empresa,dc=com,dc=br" (00000013)
added: "cn=tty,ou=Group,dc=empresa,dc=com,dc=br" (00000014)
added: "cn=disk,ou=Group,dc=empresa,dc=com,dc=br" (00000015)
added: "cn=lp,ou=Group,dc=empresa,dc=com,dc=br" (00000016)
added: "cn=mail,ou=Group,dc=empresa,dc=com,dc=br" (00000017)
added: "cn=news,ou=Group,dc=empresa,dc=com,dc=br" (00000018)
added: "cn=uucp,ou=Group,dc=empresa,dc=com,dc=br" (00000019)
```

Ajuste as permissões dos arquivos

```
# chown openldap: /var/lib/ldap/*
```

Inicie o serviço Slapd e use o comando slapcat para ver que a base esta de volta

```
# invoke-rc.d slapd start
# slapcat
```

Capítulo 2

Gerenciando

2.1. Objetivos

•Trobleshooting: Instalação e configuração do GOSA no Debian.

2.1. Troubleshooting

Como posso gerenciar minha contas de usuários do LDAP?

Isso é possível através do GOSA (GOnicus System Administrator), que através de uma interface WEB você poderá gerenciar seus usuários, habilitando serviços de Samba, Proxy, Email, FTP e FAX. Vamos a pratica:

Abra o arquivo sources.list e adicione uma nova linha de repositório

```
# vim /etc/apt/sources.list
deb http://oss.gonicus.de/pub/gosa/debian-lenny/ ./
```

Atualize a lista de pacotes

```
# aptitude update
```

Instale os pacotes gosa, gosa-schema apache2 e php5-mhash

```
# aptitude install gosa gosa-schema apache2 php5-mhash
```

Pare o serviço do Slapd e abra o arquivo de configuração do LDAP. Adicione as linhas do schemas, atributos para indexação e ACLs. Feito isso grave o arquivo.

```
# invoke-rc.d slapd stop
# vim /etc/ldap/slapd.conf
```

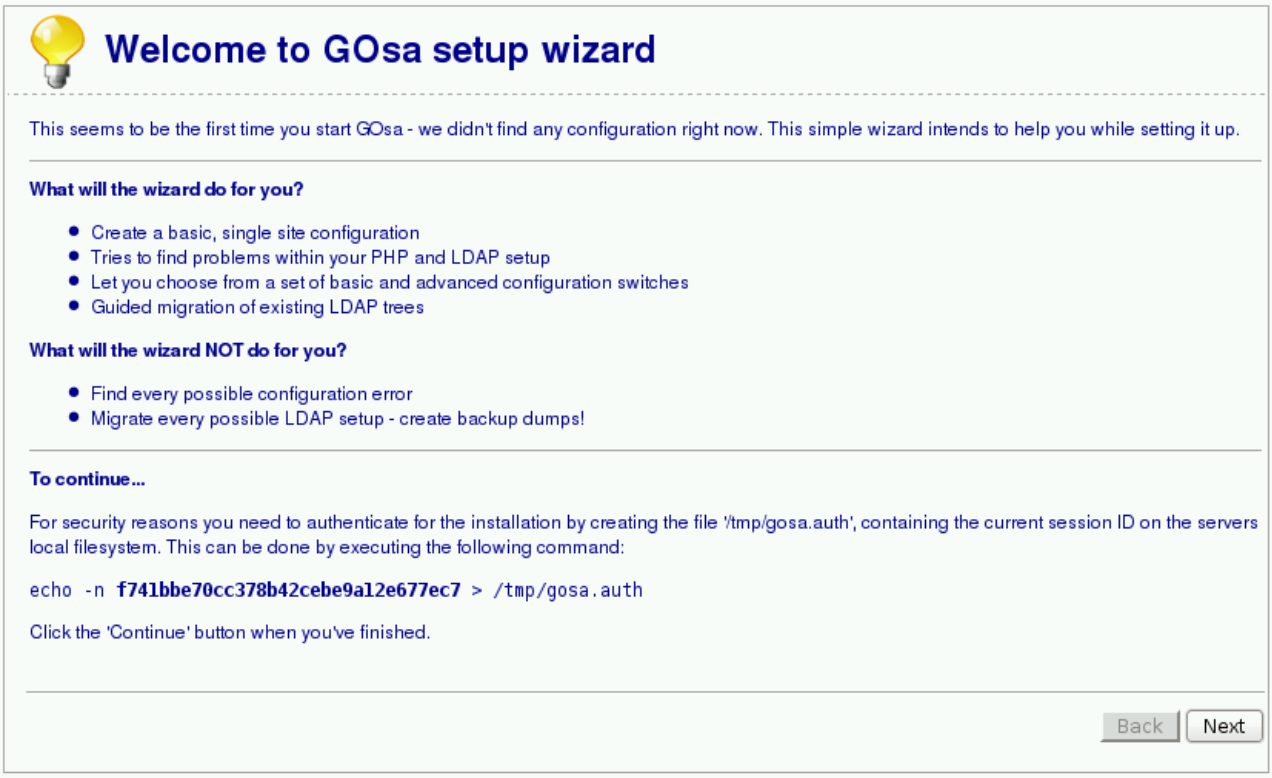
```
include         /etc/ldap/schema/gosa/samba3.schema
include         /etc/ldap/schema/gosa/trust.schema
include         /etc/ldap/schema/gosa/gosystem.schema
include         /etc/ldap/schema/gosa/gofon.schema
include         /etc/ldap/schema/gosa/goto.schema
include         /etc/ldap/schema/gosa/gosa-samba3.schema
include         /etc/ldap/schema/gosa/gofax.schema
include         /etc/ldap/schema/gosa/goserver.schema
include         /etc/ldap/schema/gosa/goto-mime.schema

index   default                                                 sub
index   uid,mail,gosaSnapshotDN                                 eq
index   gosaSnapshotTimestamp                                   eq,sub
index   gosaMailAlternateAddress,gosaMailForwardingAddress      eq
index   cn,sn,givenName,ou                                      pres,eq,sub
index   objectClass                                             pres,eq
index   uidNumber,gidNumber,memberuid                           eq
index   roleOccupant                                            eq
index   gosaSubtreeACL,gosaObject,gosaUser                      pres,eq
```

access to attrs=userPassword,shadowLastChange,sambaPwdLastSet,sambaPwdMustChange,sambaPwdCanChange,shadowMax,shadowExpire

Faça a indexação, ajuste as permissões e inicie o serviço do Slapd

```
# slapindex -v
# chown openldap: /var/lib/ldap/*
# invoke-rc.d slapd start
```

Acesse no Browser *http://localhost/gosa*

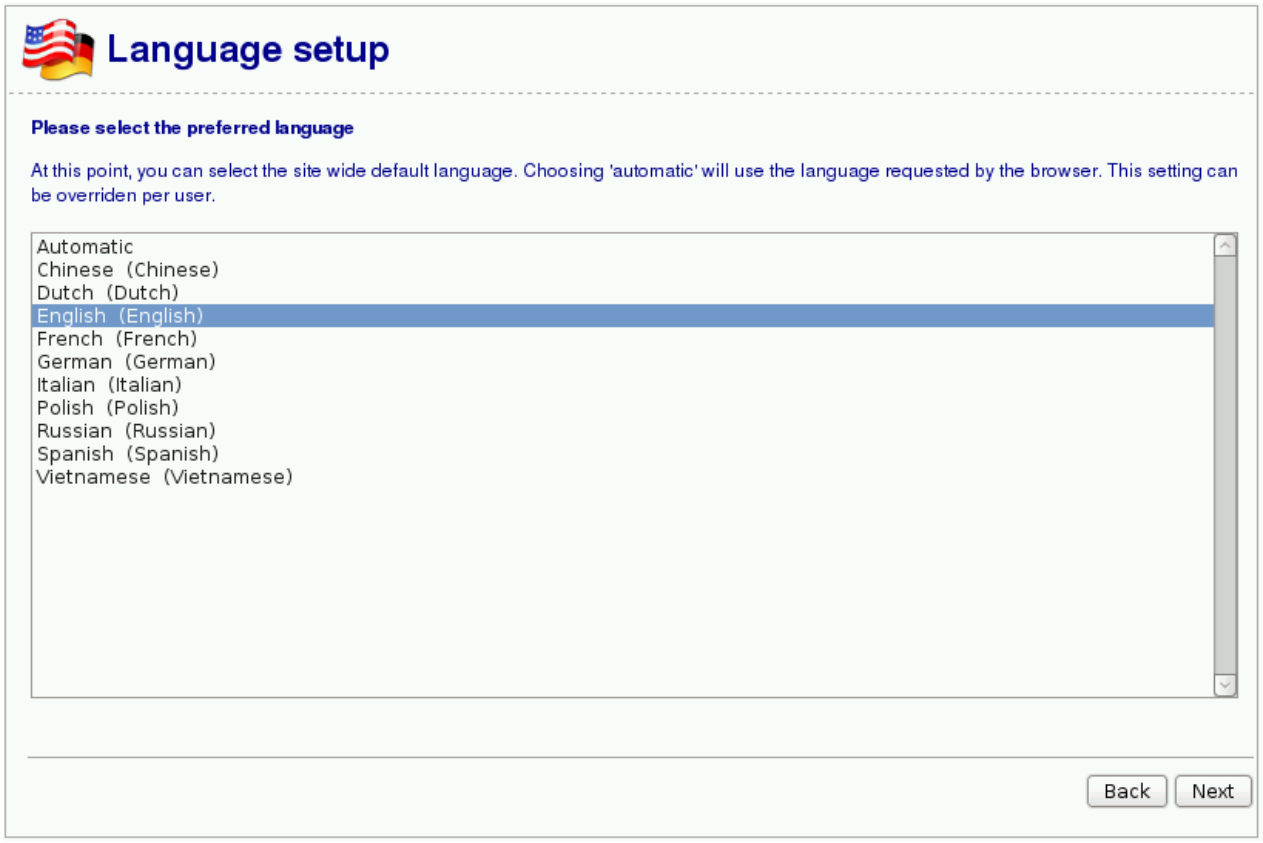


Por questão de segurança no assistente de instalação do GOSA, é necessário criar um arquivo temporário contendo a identificação da sessão.

```
# echo -n f741bbe70cc378b42cebe9a12e677ec7 > /tmp/gosa.auth
```

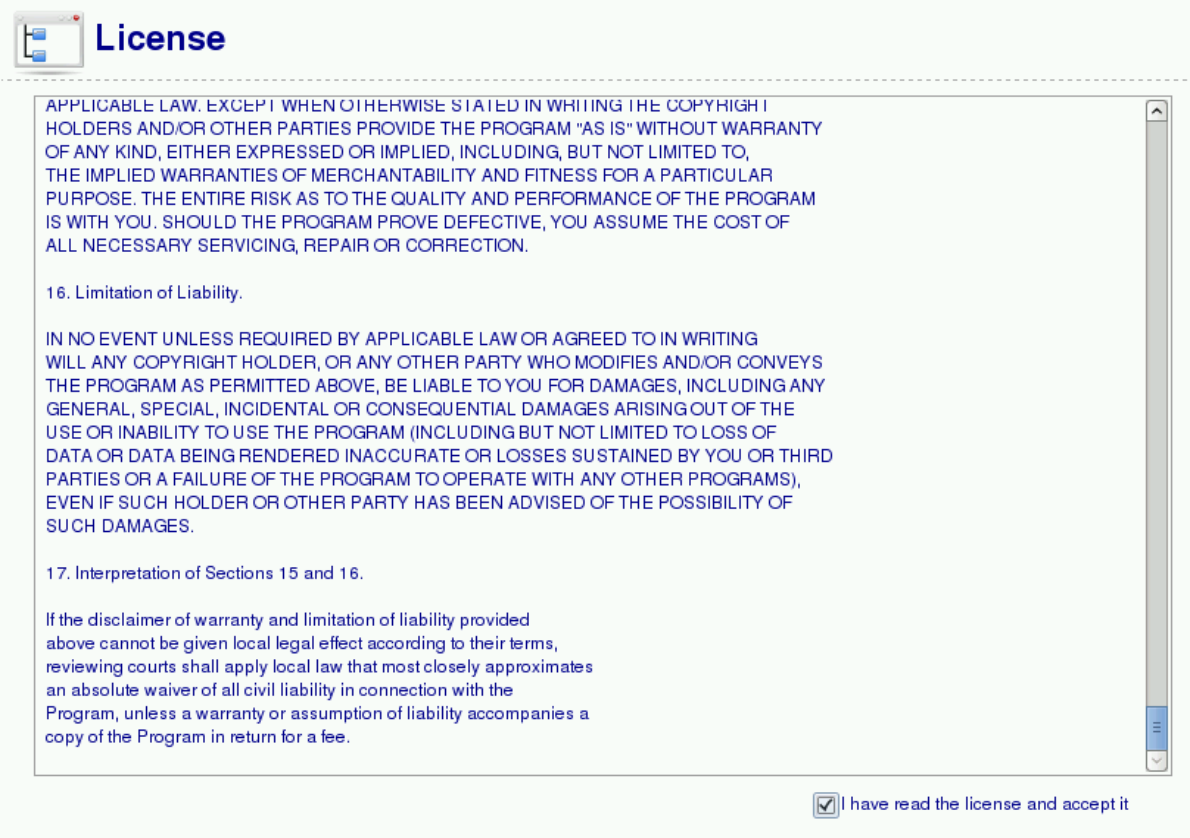
Clique no botão “Next” para continuar.

Na próxima etapa do assistente, escolha seu idioma e “Next” para continuar.

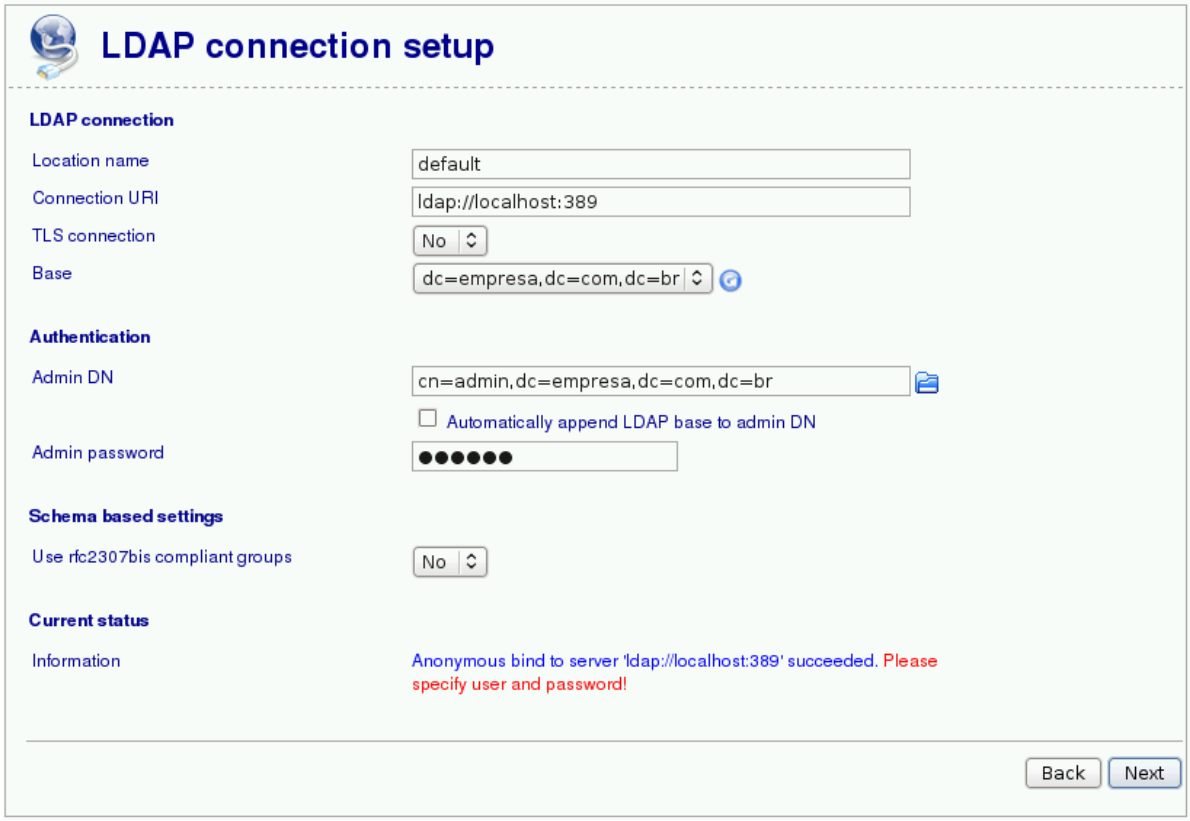


Na próxima etapa do assistente, é verificado se os módulos e extensões do PHP que o GOSa precisa para funcionar estão instalados. Caso o não tenha instale o pacote equivalente. Clique no botão “Next” para continuar.

Para continuar leia a licença de uso, selecione a opção “I have read license and accept it” e clique no botão “Next” para continuar.

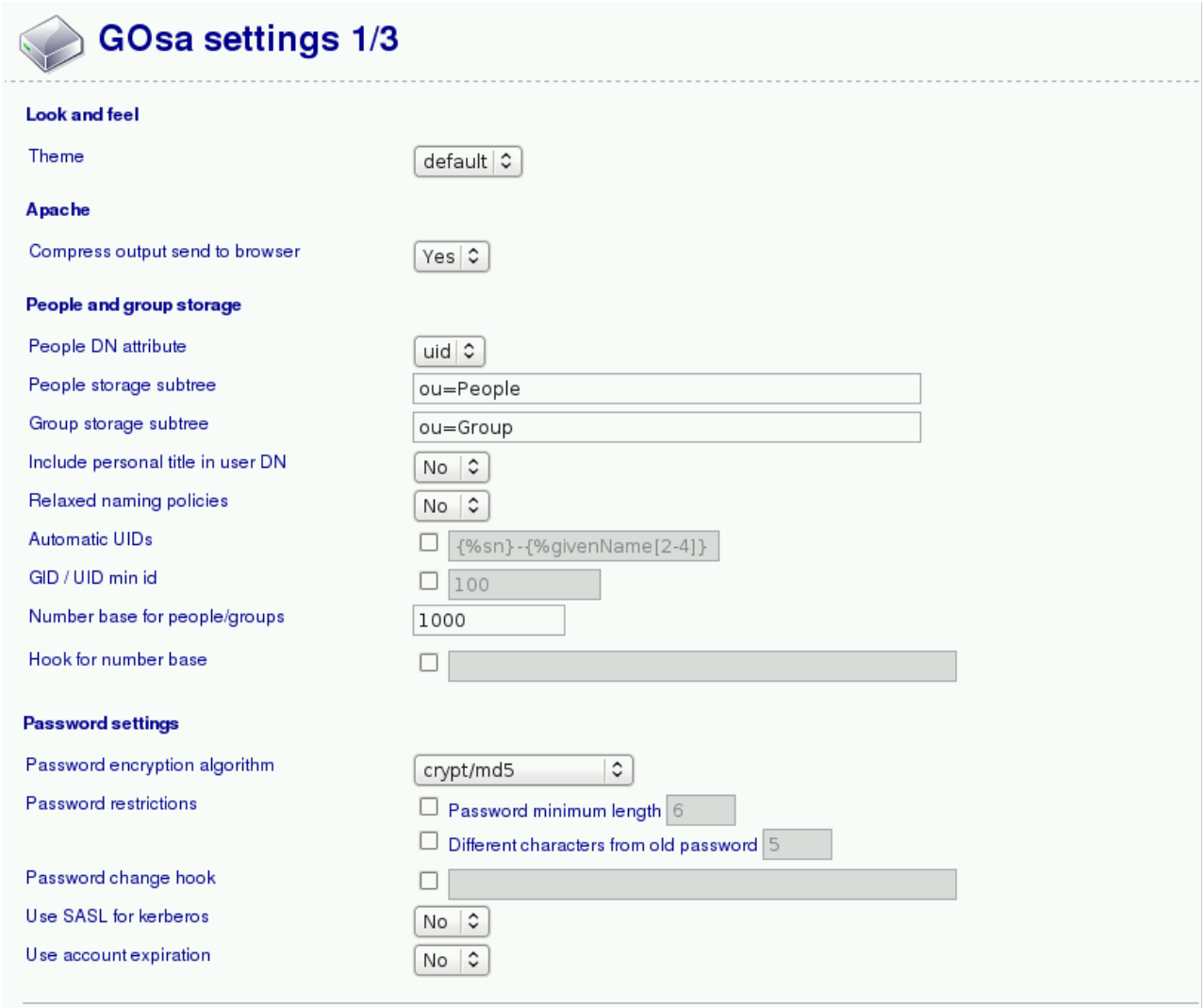


Preencha o DN do administrador da base e senha e “Next” para continuar

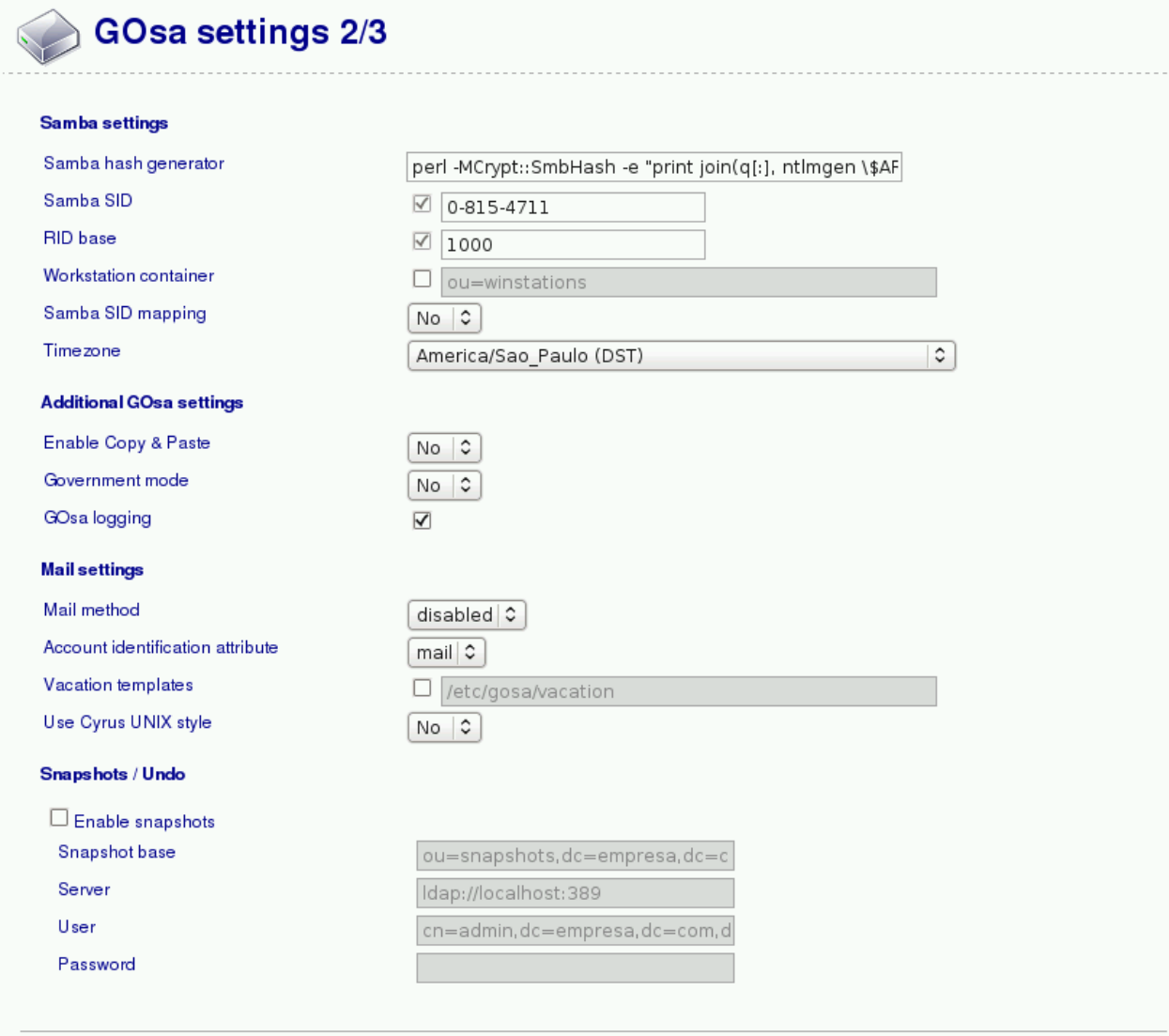


Na próxima etapa do assistente, será verificado se os schemas do GOSa estão inclusos em sua configuração do LDAP. Clique no botão “Next” para continuar.

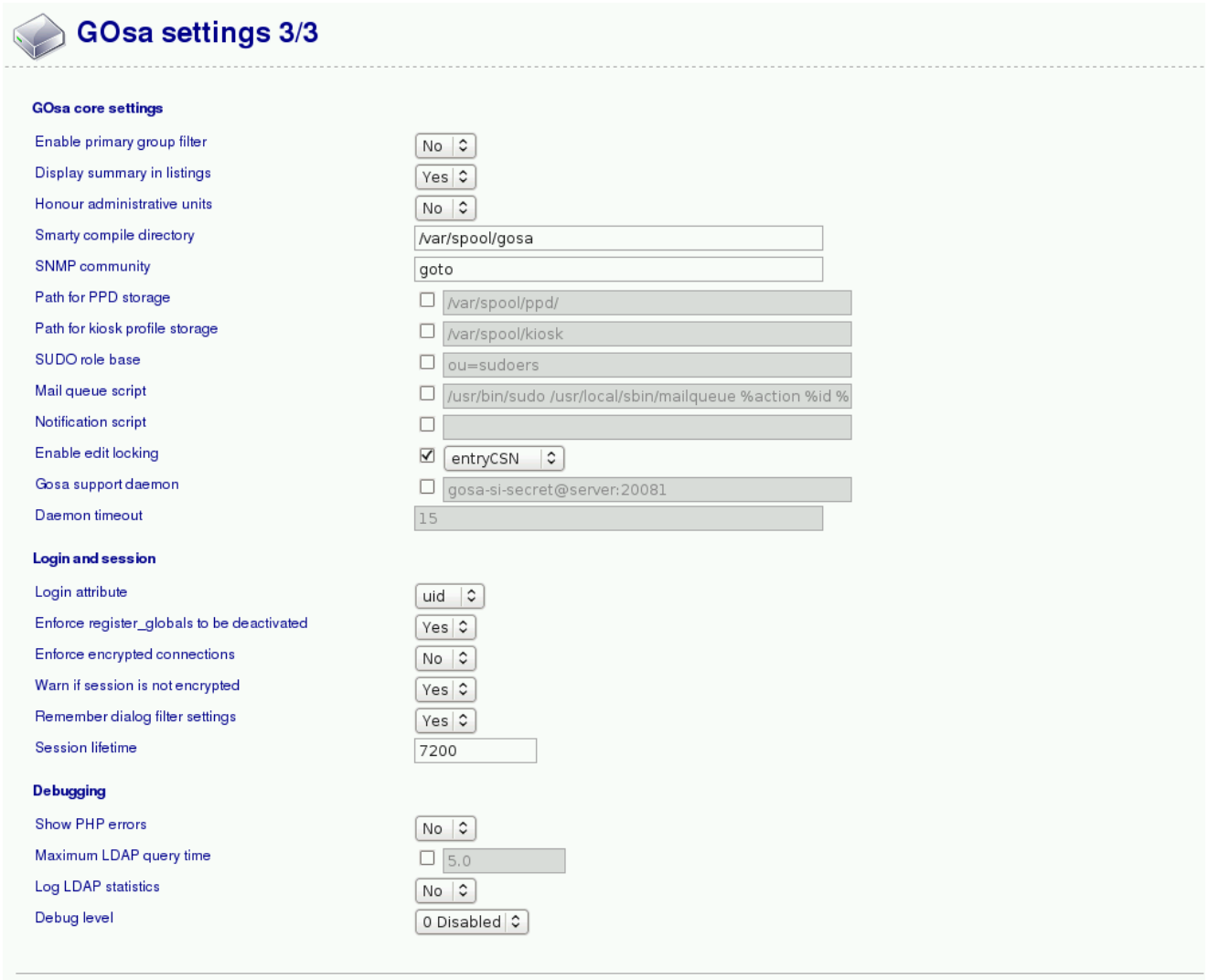
Na próxima etapa do assistente, configure o tipo de atributo usado para conta de usuário (UID), a OU de usuários (People) e a OU de grupos (Group). Clique no botão “Next” para continuar.



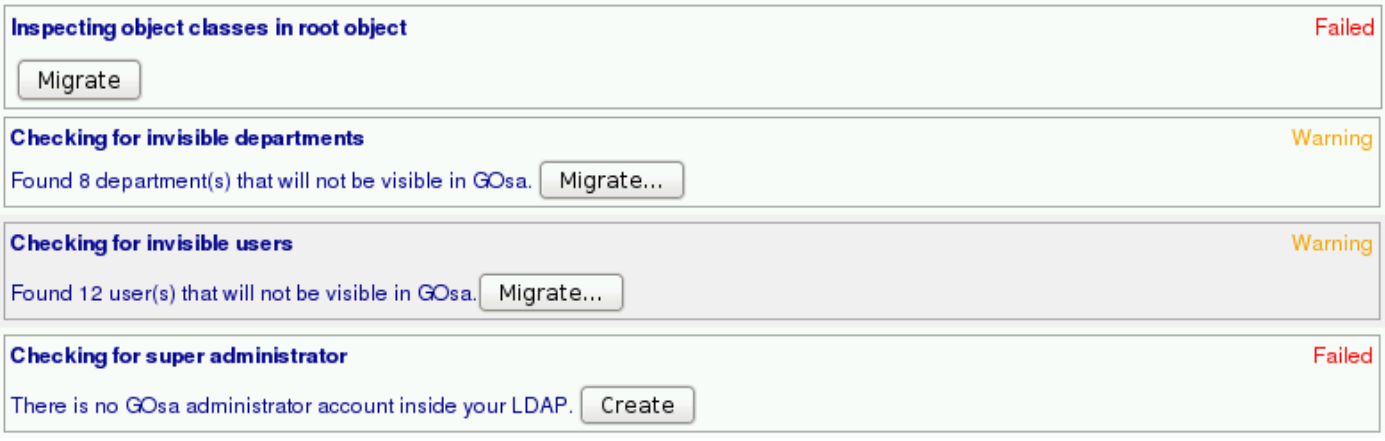
Na próxima etapa do assistente, configure as opções do Samba e email. Como este não é o nosso foco, apenas selecione o Time zone correto. Clique no botão "Next" para continuar.



Na próxima etapa do assistente, deixe a configuração padrão e clique no botão "Next" para continuar.

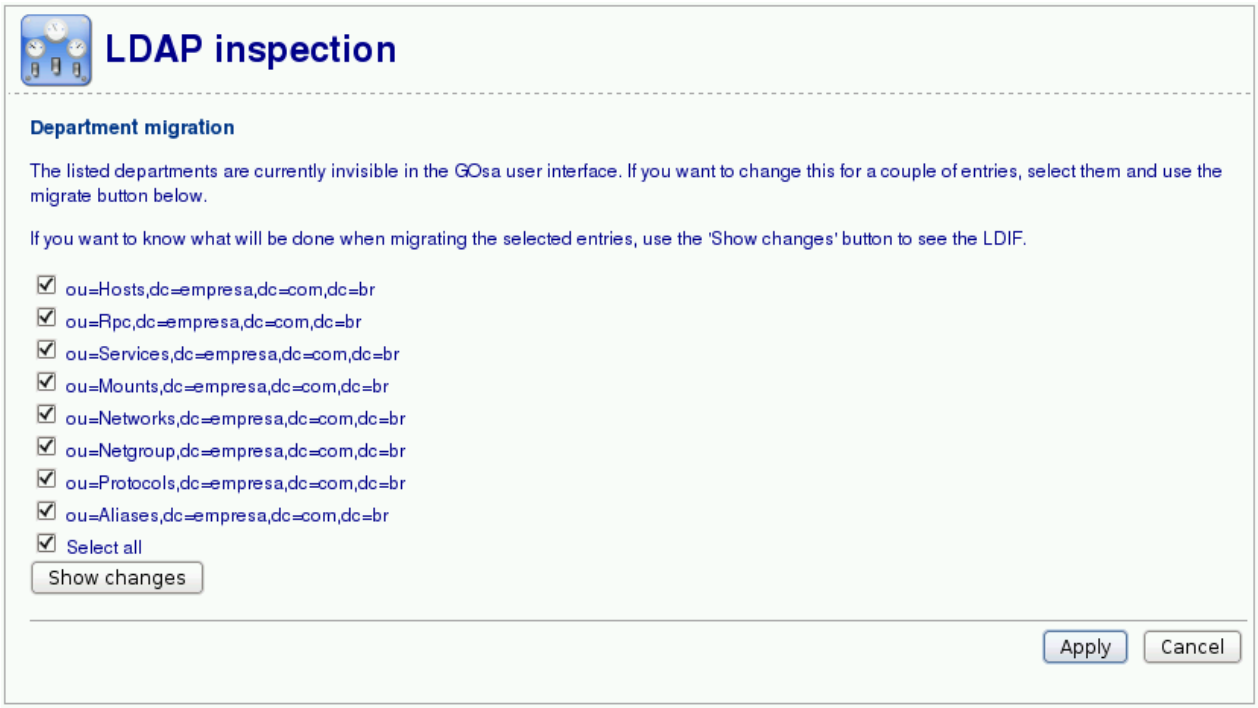


Agora o assistente ira verificar os objetos relacionados ao LDAP como grupos, usuários e a senha do administrador do GOSA. Para migrar os objetos clique no botão “Migrate”, o único que não será migrado são os 12 usuários encontrados que são usuários do sistema.

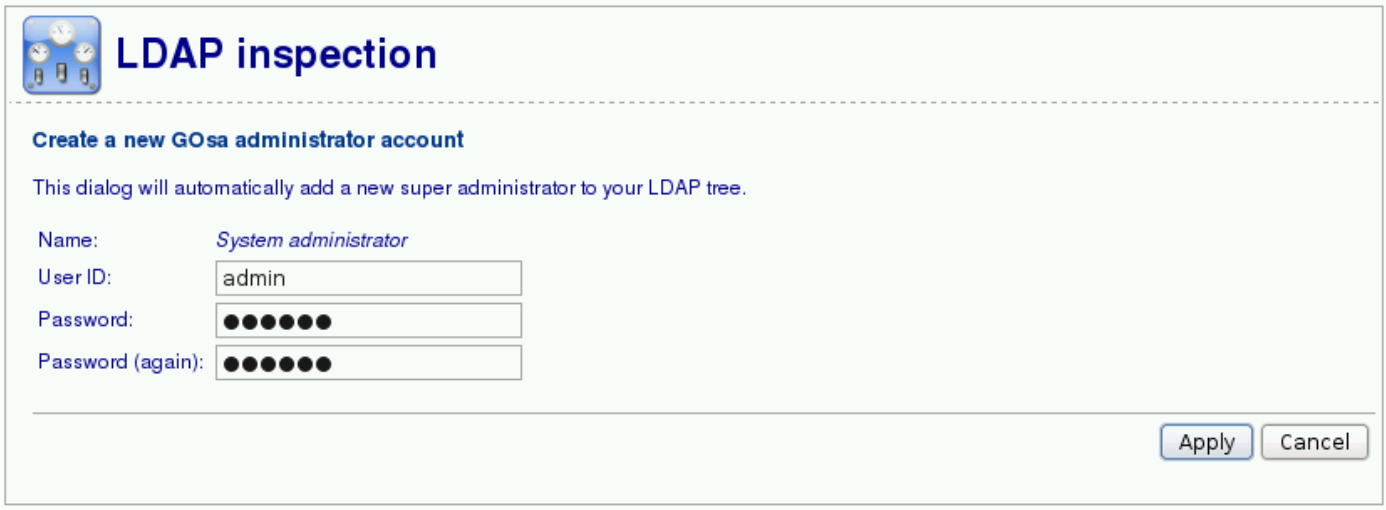


Clique no botão “Migrate” em “Inspecting object classes in root object” e novamente em “Migrate” para adicionar a nossa base o objectClass “gosaDepartment”

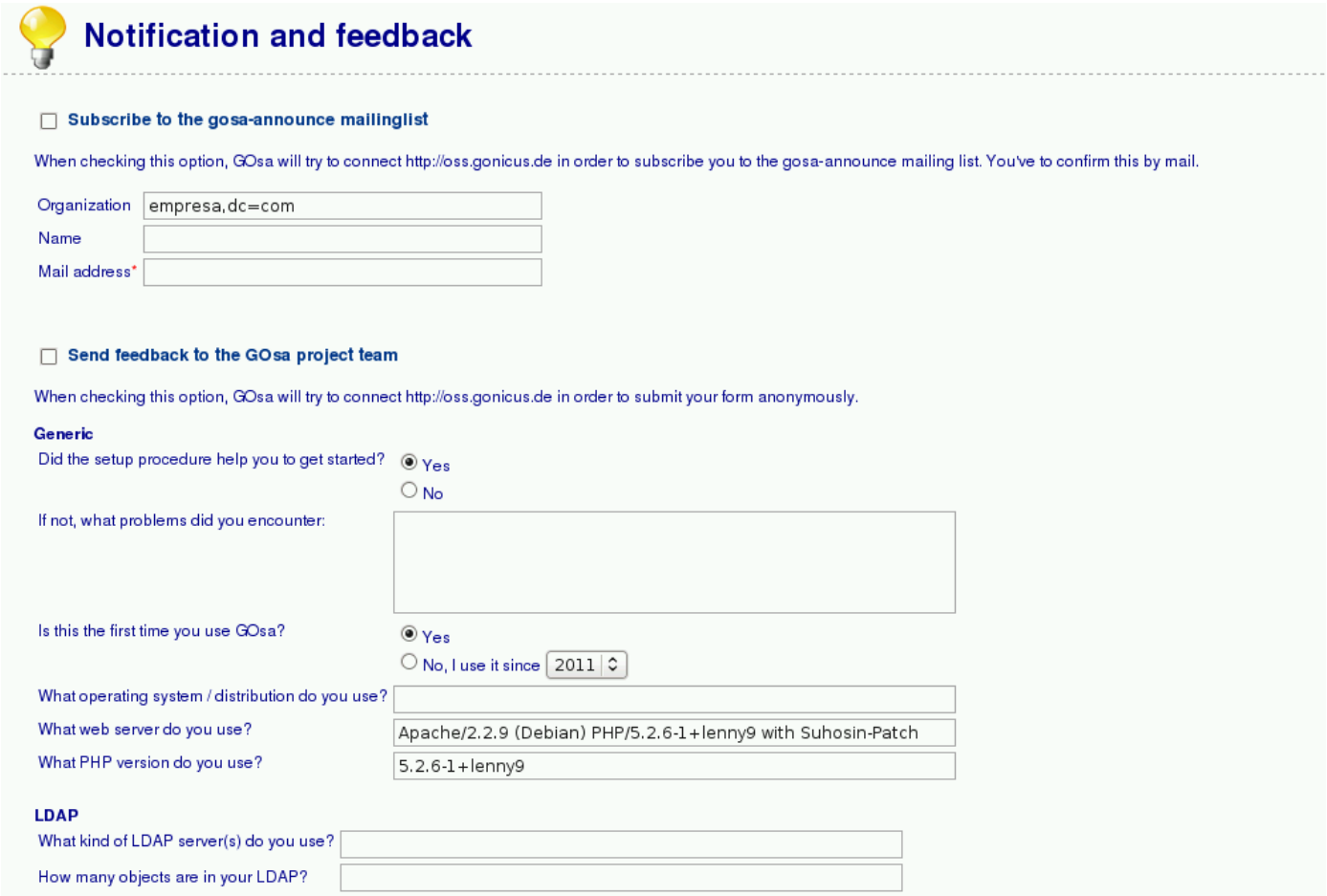
Clique no botão “Migrate” em “Checking for invisible departments”,e clique também em “Select all” para adicionar as OU selecionadas e no botão “Apply” para finalizar.



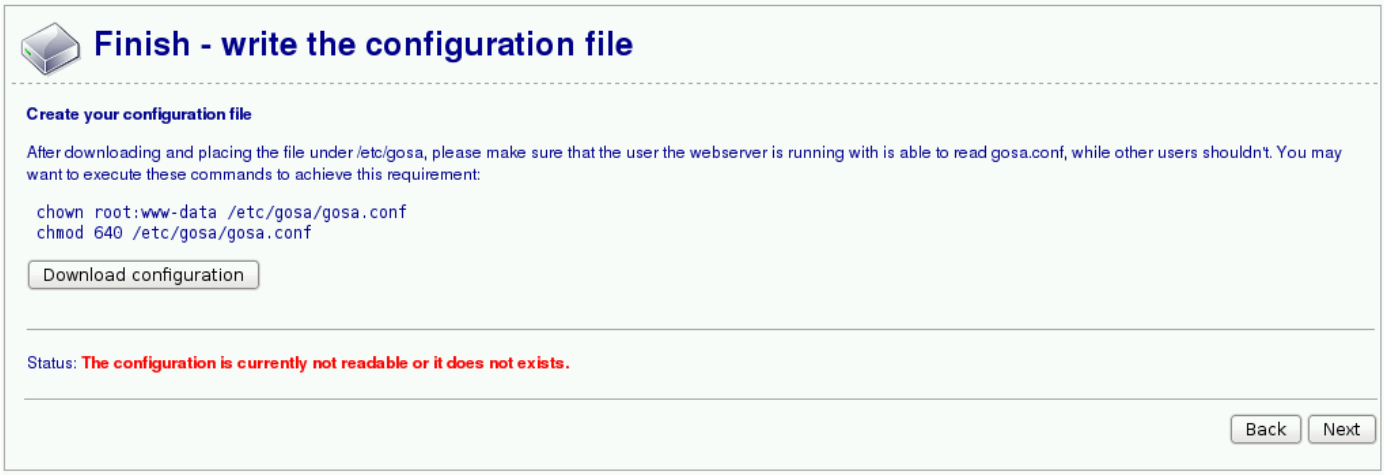
Clique no botão “Migrate” em “Checking for super adminstrator”, digite sua senha de administrador do GOSA e no botão “Apply” para finalizar.

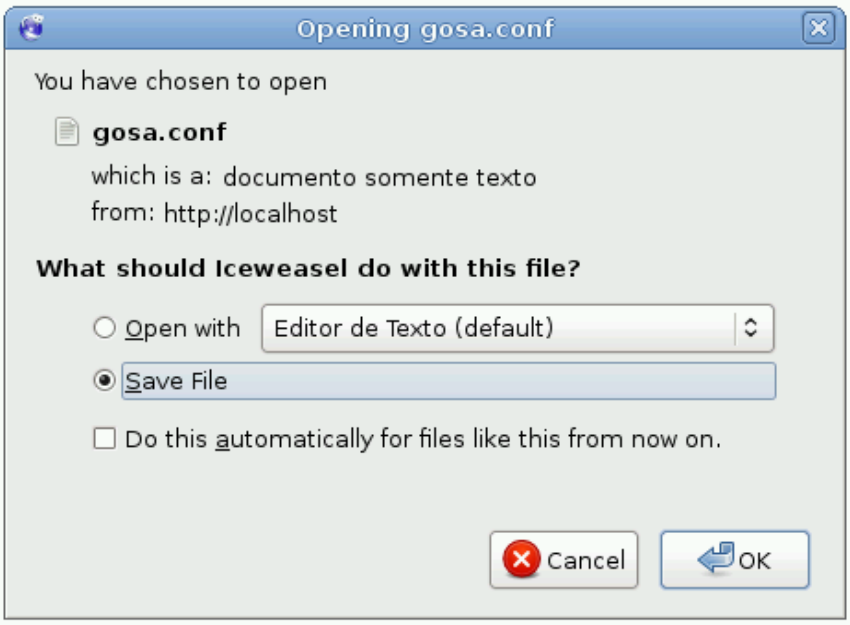


Para continuar clique no botão “Next”, preencha os formulários e novamente no botão “Next”



Para finalizar nosso assistente, faça download do arquivo de configuração do GOSA, copie para o /etc/gosa e ajuste as permissões.

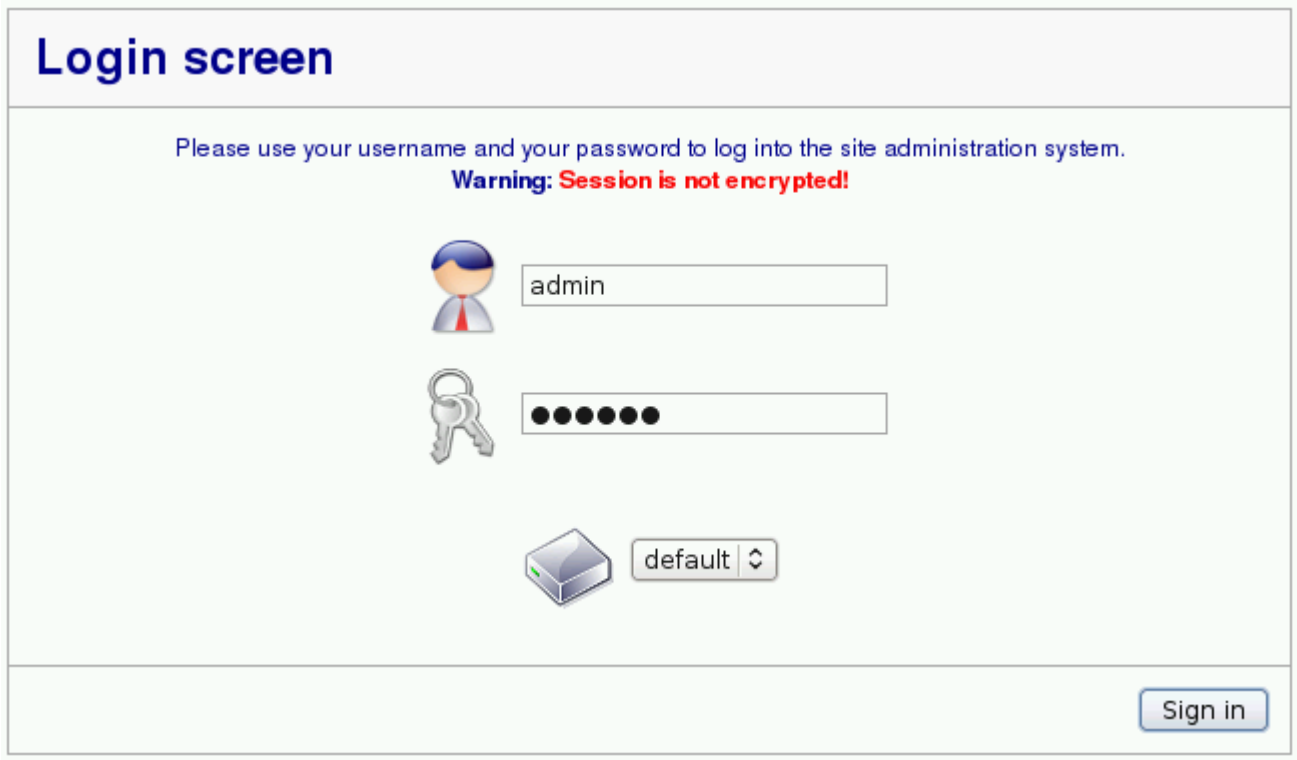


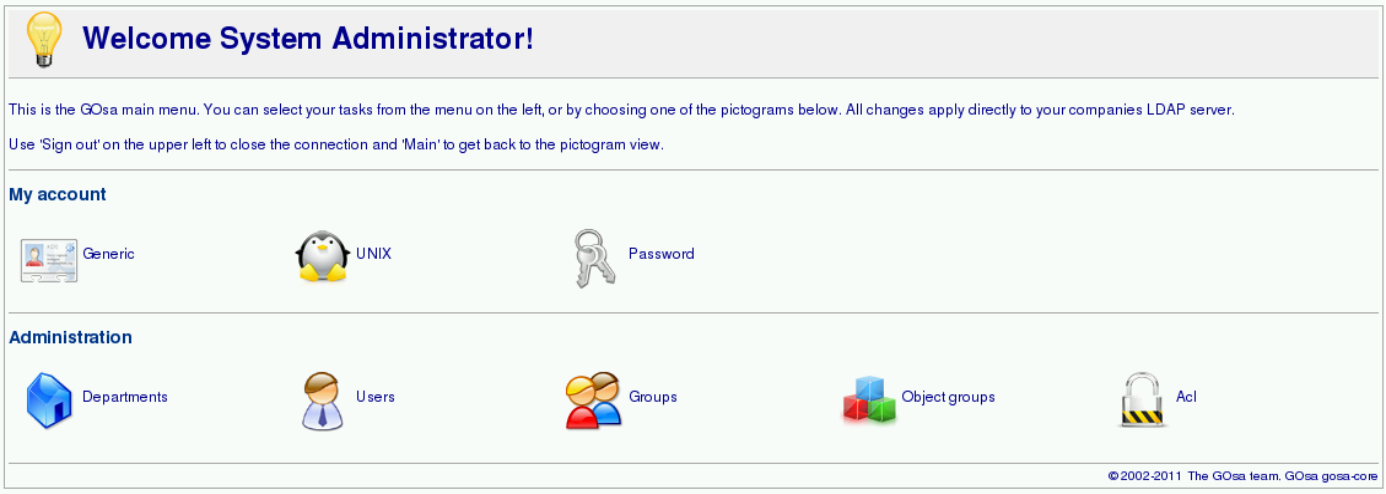


```
# cp gosa.conf /etc/gosa/
# chown root:www-data /etc/gosa/gosa;conf
# chmod 640 /etc/gosa/gosa.conf
```

Feito todos os passos acima, clique no botão “Next” e você tera um gerenciador via WEB para sua base LDAP.

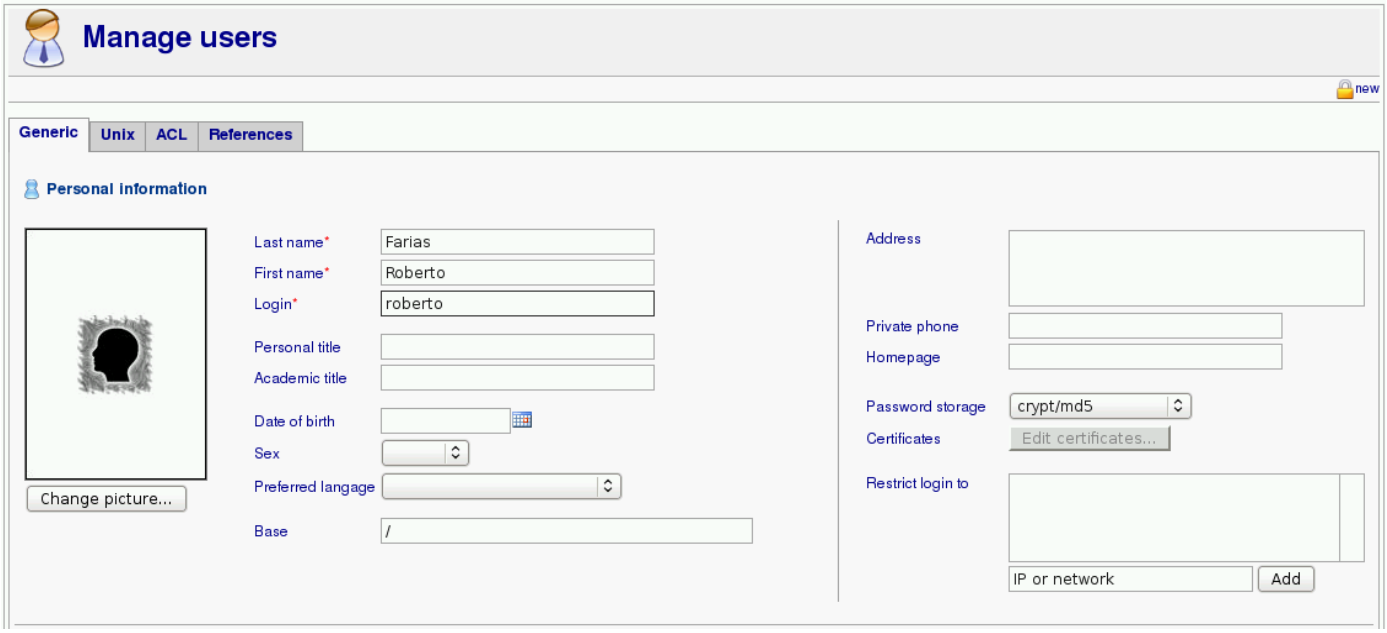
Entre com a senha que foi definida durante o assistente



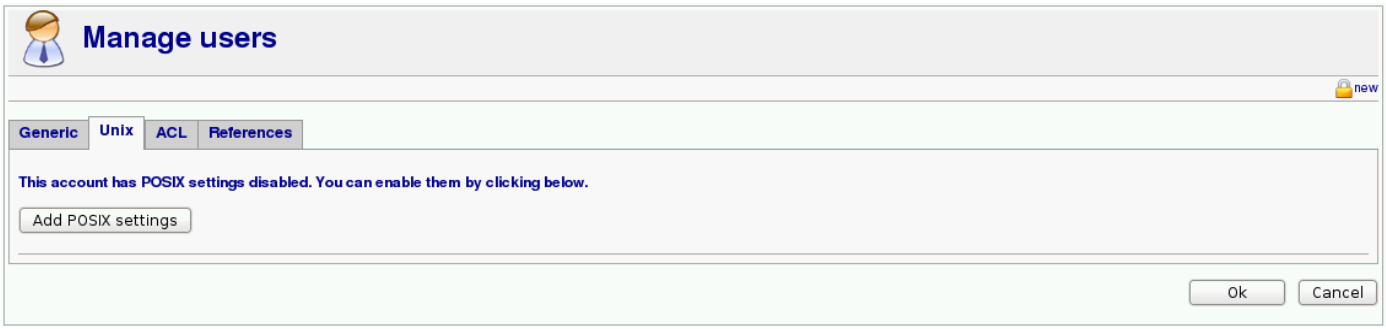


Adicionar nova entrada na base LDAP com login no Linux.

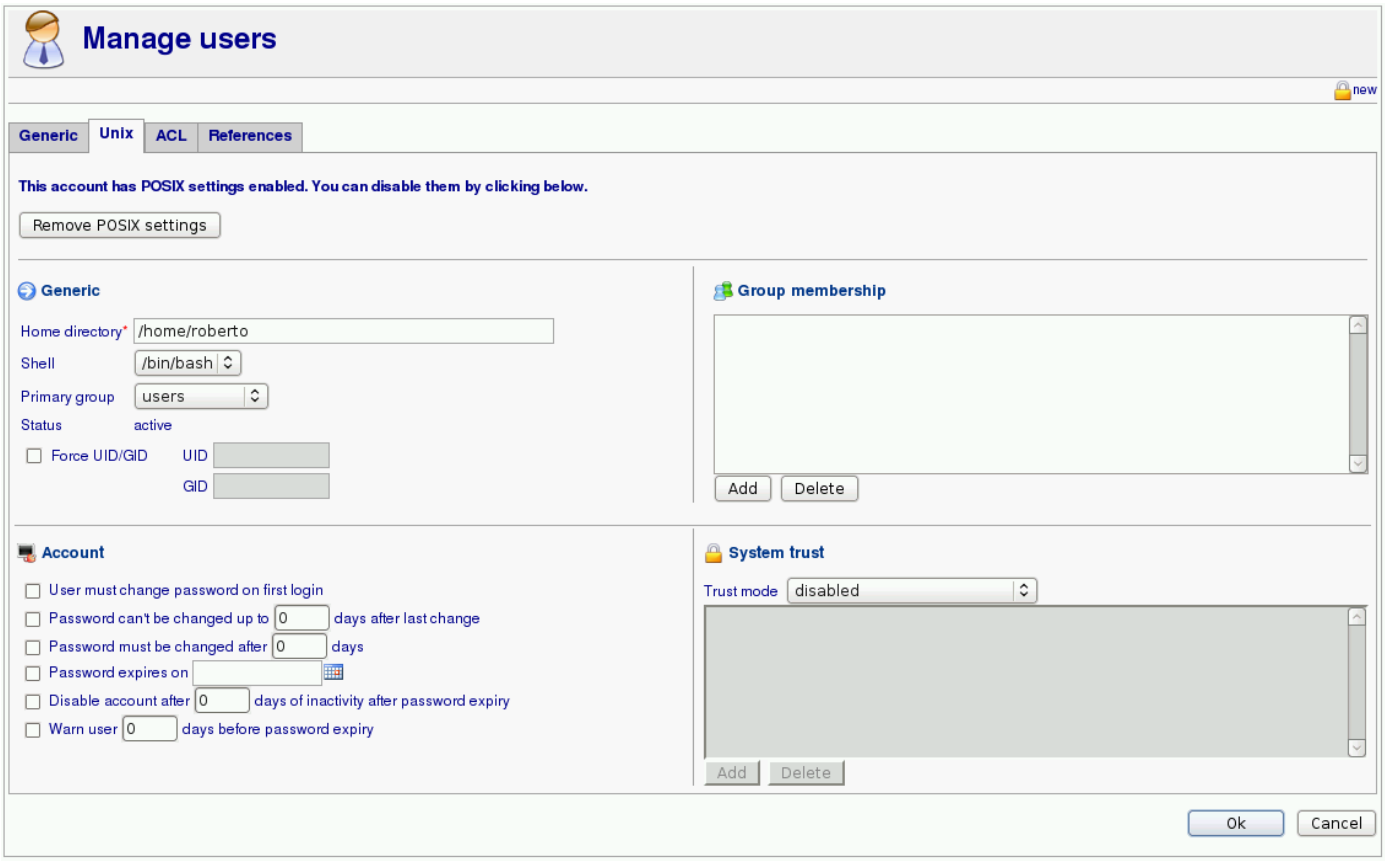
Clique no ícone Users → Actions → Create → User e preencha as informações sobre seu novo usuário.



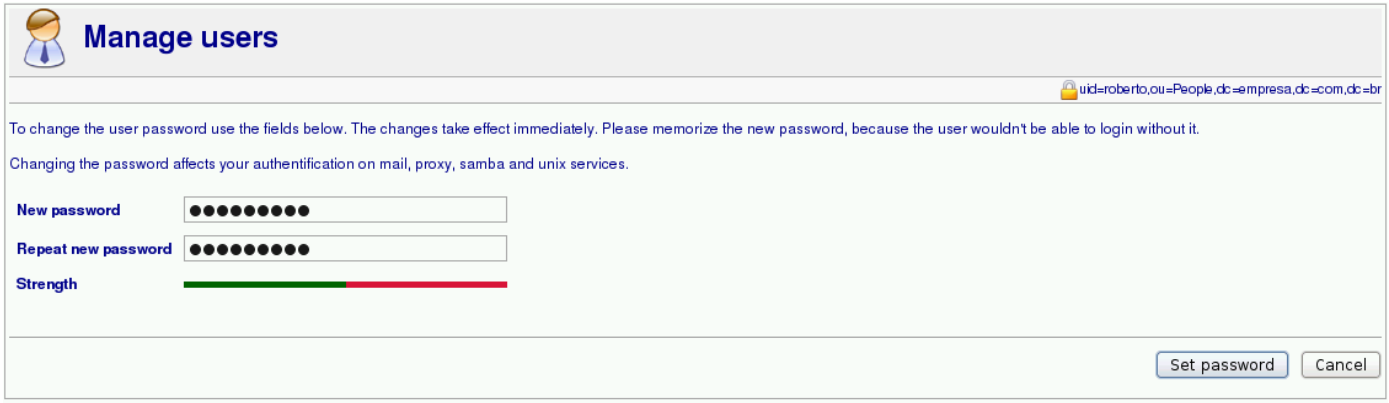
Para adicionar informações sobre a conta Linux, clique na aba “Unix” e no botão “Add POSIX settings”



Preencha a caixa “Home directory” com a path da home do usuário, e o grupo primário em “Primary group”. Clique no botão “OK” para continuar.



Na próxima etapa, preencha a nova senha do usuário e clique no botão “Set password” para adicionar o novo usuário.

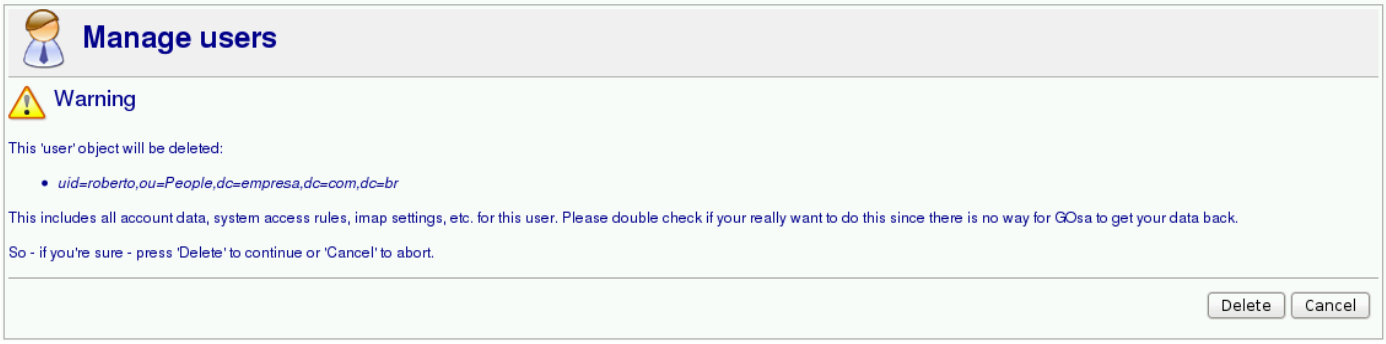


Clicando no icone “Users” sera listado os usuários cadastrados através do GOSA. Quando o usuário conter um “Tux” indica que o mesmo poder realizar login no Linux.

Para testar o login no Linux do novo usuário, configure sua instalação para autenticar via LDAP.

```
server login: roberto
Password:
Last login: Tue Jan  4 20:25:36 BRST 2011 on tty2
Creating directory '/home/roberto'.
roberto@server:~$ _
```

Para apagar o usuário da base, clique no ícone “Users” e na lista de usuários, clique no ícone do lixo ao lado direito referente ao usuário que você excluir.



Para ter acesso a novas finalidades no GOSA, instale o pacote referente ao serviço. Exemplo:

 # aptitude install gosa-plugin-samba

```
p   gosa-plugin-log                 - log plugin for GOsa
p   gosa-plugin-log-schema          - LDAP schema for GOsa plugin log
p   gosa-plugin-mail                - mail plugin for GOsa
p   gosa-plugin-mit-krb5            - mit-krb5 plugin for GOsa
p   gosa-plugin-mit-krb5-schema     - LDAP schema for GOsa plugin mit-krb5
p   gosa-plugin-nagios              - nagios plugin for GOsa
p   gosa-plugin-nagios-schema       - LDAP schema for GOsa plugin nagios
p   gosa-plugin-netatalk            - netatalk plugin for GOsa
p   gosa-plugin-opengroupware       - opengroupware plugin for GOsa
p   gosa-plugin-openxchange         - openxchange plugin for GOsa
p   gosa-plugin-openxchange-schema  - LDAP schema for GOsa plugin openxchange
p   gosa-plugin-opsi                - opsi plugin for GOsa
p   gosa-plugin-phpgw               - phpgw plugin for GOsa
p   gosa-plugin-phpgw-schema        - LDAP schema for GOsa plugin phpgw
p   gosa-plugin-phpscheduleit       - phpscheduleit plugin for GOsa
p   gosa-plugin-phpscheduleit-schem - LDAP schema for GOsa plugin phpscheduleit
p   gosa-plugin-pptp                - pptp plugin for GOsa
p   gosa-plugin-pptp-schema         - LDAP schema for GOsa plugin pptp
p   gosa-plugin-pureftpd            - pureftpd plugin for GOsa
p   gosa-plugin-pureftpd-schema     - LDAP schema for GOsa plugin pureftpd
p   gosa-plugin-rolemanagement      - rolemanagement plugin for GOsa
p   gosa-plugin-rsyslog             - rsyslog plugin for GOsa
p   gosa-plugin-samba               - samba plugin for GOsa
p   gosa-plugin-scalix              - scalix plugin for GOsa
p   gosa-plugin-squid               - squid plugin for GOsa
```

Automaticamente sera incluído um novo ícone sobre o serviço, em nosso exemplo você deve ter também instalado um servidor Samba.