Instalação do

no Debian GNU/Linux (Sarge)

Antonio Carlos Feitosa Costa (antonio@cbpf.br)

Prefácio

Eu fiz este tutorial como material de apoio do minicurso: **LDAP – Conceitos e Aplicações**, que eu ministrei no *IV Fórum do Software Livre do Rio de Janeiro* realizado nos dias 16 a 20 de Outubro de 2006 na Unirio.

Site do evento:http://www.forumsoftwarelivre.org.br/

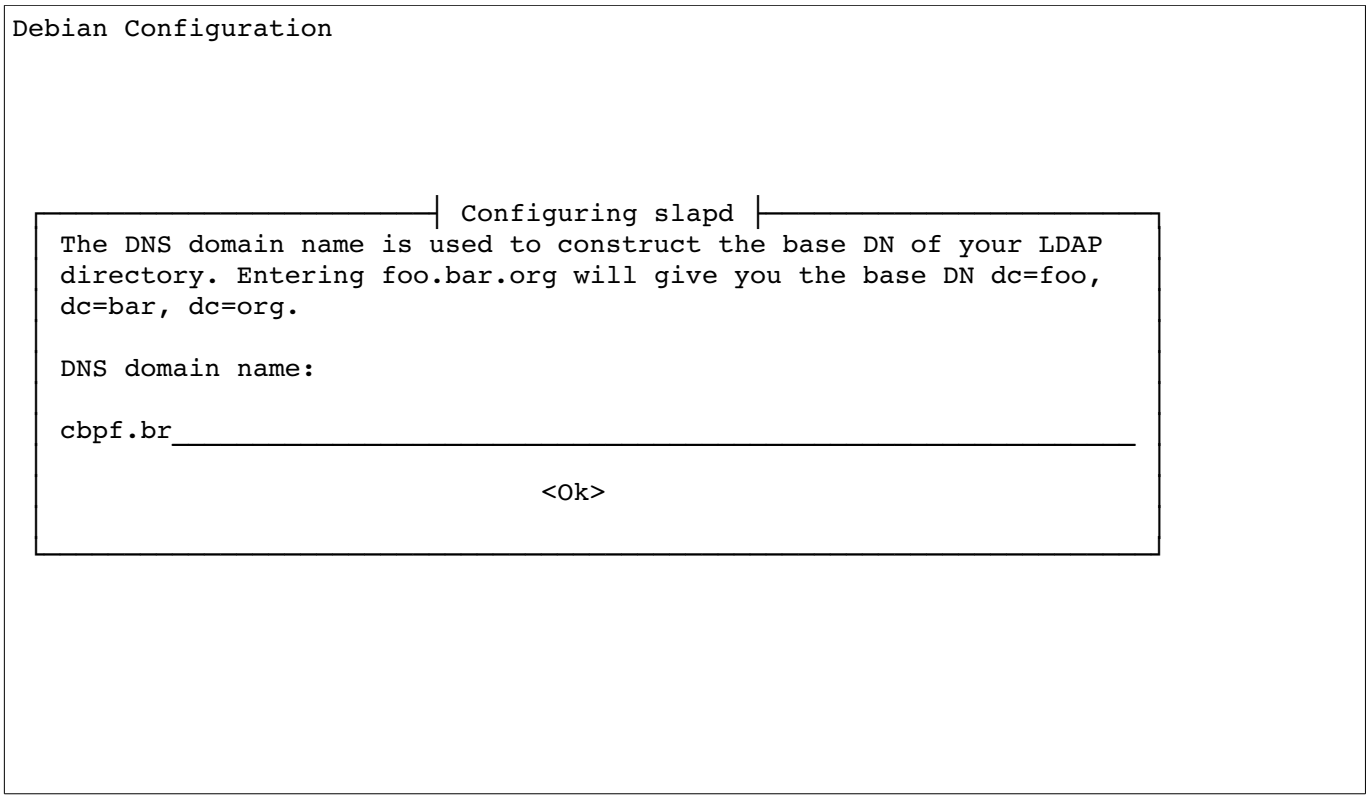
Instalação do OpenLDAP no Debian Sarge

Antes de começar a executar este tutorial, você precisa acrescentar algum repositório de pacotes remoto. Para isso digite `apt-setup` e escolha o repositório desejado.

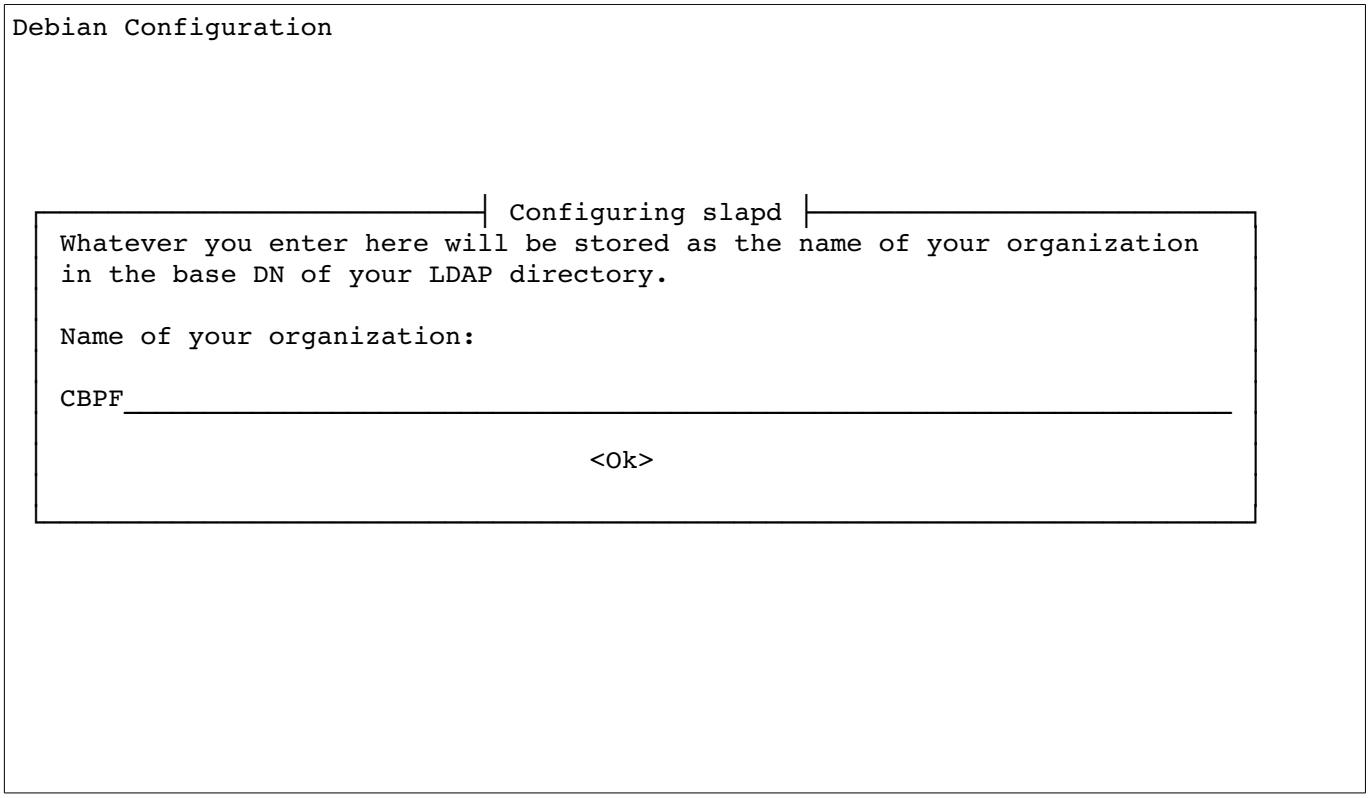
Para instalar o OpenLDAP, digite o comando abaixo com privilégio de root.

```
apt-get install slapd ldap-utils
```

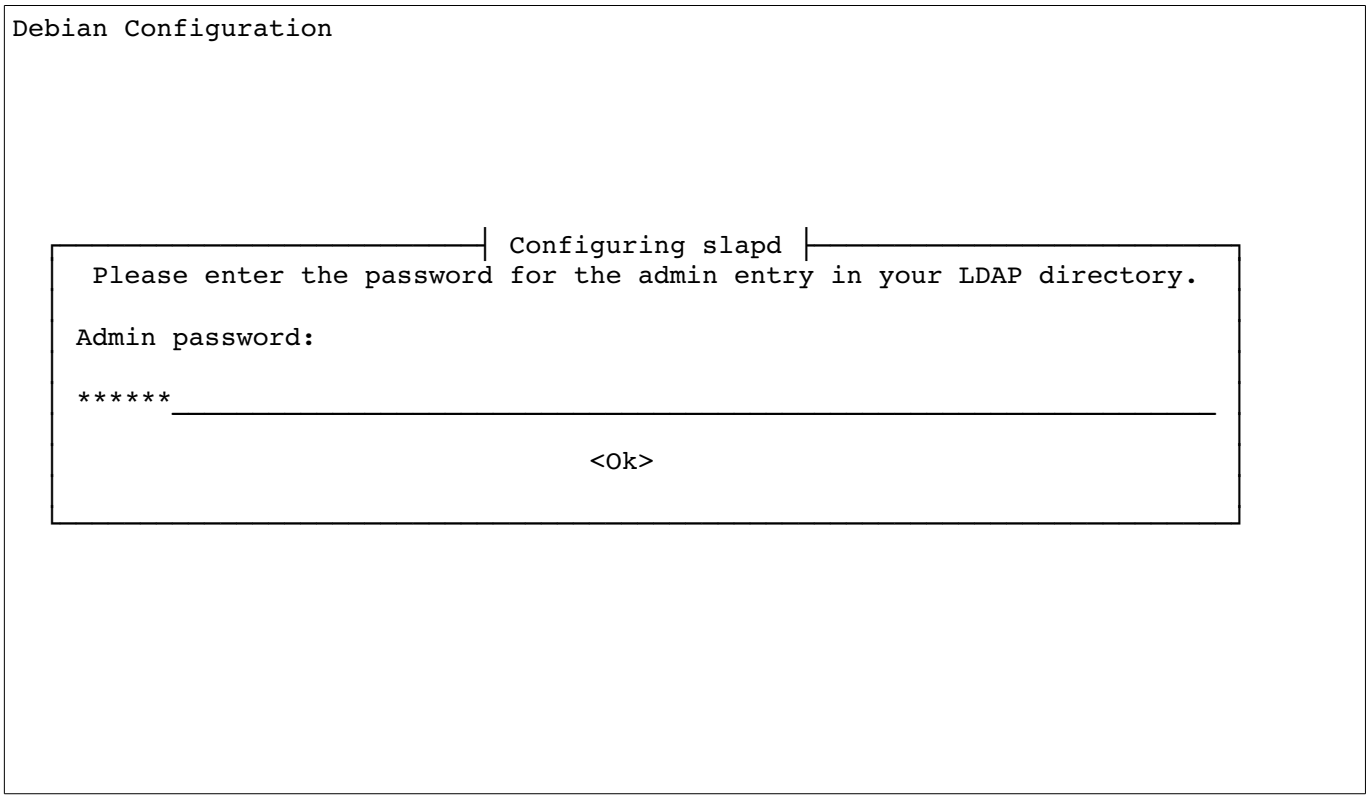
Digite o dn de sua base. De acordo com a entrada DNS na figura abaixo, a raiz da sua base será: `dc=cbpf,dc=br`



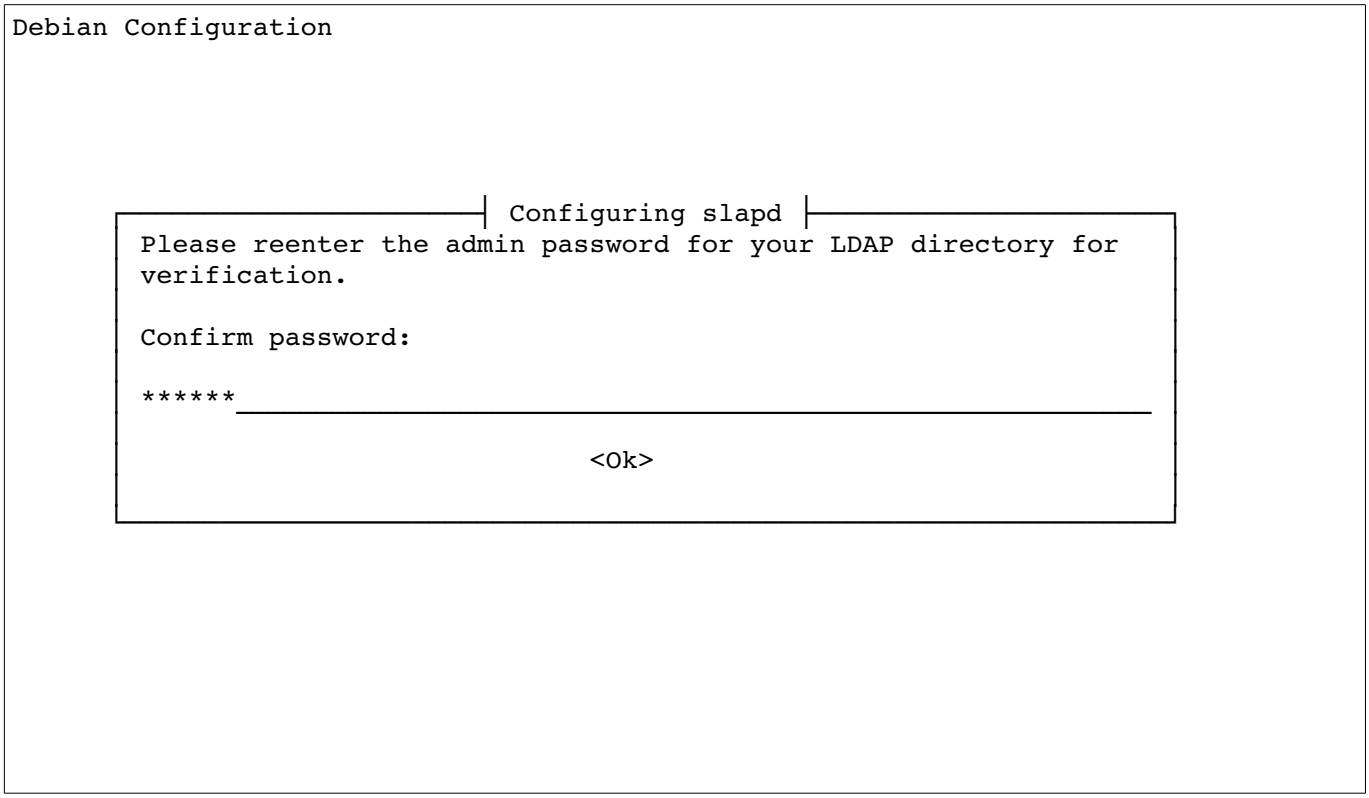
Agora digite o valor do Atributo “organization” , ou seja, o nome da empresa ou organização. Conforme o exemplo abaixo:



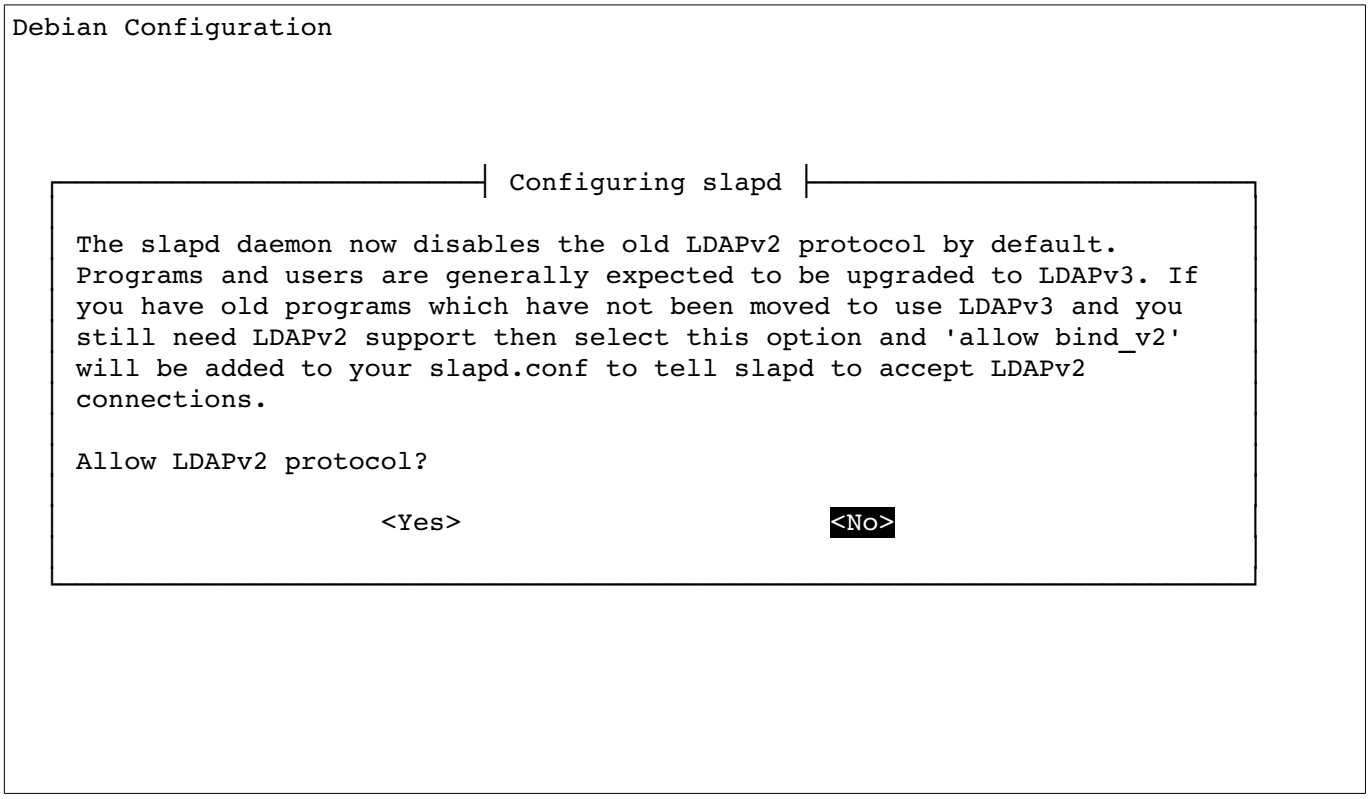
Agora digite a senha do rootdn padrão do Debian **cn=admin,dc=cbpf,dc=br** Exemplo:



Repita a senha:



Responda <No> a próxima pergunta para que NÃO seja habilitado o suporte a versão 2 do protocolo LDAP. Veja o exemplo abaixo:



O serviço agora será configurado e iniciado:

```
root@ldap01:~# apt-get install slapd
Reading Package Lists... Done
Building Dependency Tree... Done
Suggested packages:
  ldap-utils
Recommended packages:
  db4.2-util libsasl2-modules
The following NEW packages will be installed:
  slapd
0 upgraded, 1 newly installed, 0 to remove and 4 not upgraded.
Need to get 0B/817kB of archives.
After unpacking 2281kB of additional disk space will be used.
Preconfiguring packages ...
Selecting previously deselected package slapd.
(Reading database ... 19615 files and directories currently installed.)
Unpacking slapd (from .../slapd_2.2.23-8_i386.deb) ...
Setting up slapd (2.2.23-8) ...
  Creating initial slapd configuration... done.
  Creating initial LDAP directory... done.
Starting OpenLDAP: (db4.2_recover not found),  slapd.

root@ldap01:~#
```

Note que quando o serviço é iniciado, aparece a mensagem: `(db4.2_recover not found)`

Precisamos instalar os utilitários para manutenção de base do Berkeley DB.

```
apt-get install db4.2-util
```

Reinicie o Serviço e veja o que acontece...

```
/etc/init.d/slapd restart
```

```
Selecting previously deselected package slapd.
(Reading database ... 19615 files and directories currently installed.)
Unpacking slapd (from .../slapd_2.2.23-8_i386.deb) ...
Setting up slapd (2.2.23-8) ...
  Creating initial slapd configuration... done.
  Creating initial LDAP directory... done.
Starting OpenLDAP: (db4.2_recover not found),  slapd.

root@ldap01:~# apt-get install db4.2-util
Reading Package Lists... Done
Building Dependency Tree... Done
The following NEW packages will be installed:
  db4.2-util
0 upgraded, 1 newly installed, 0 to remove and 4 not upgraded.
Need to get 0B/58.4kB of archives.
After unpacking 188kB of additional disk space will be used.
Selecting previously deselected package db4.2-util.
(Reading database ... 19725 files and directories currently installed.)
Unpacking db4.2-util (from .../db4.2-util_4.2.52-18_i386.deb) ...
Setting up db4.2-util (4.2.52-18) ...
root@ldap01:~# /etc/init.d/slapd restart
```

```
Stopping OpenLDAP: slapd.
Starting OpenLDAP: running BDB recovery, slapd.
root@ldap01:~#
```

Digite `slapcat` para ver a base criada:

```
root@ldap01:~# slapcat
dn: dc=cbpf,dc=br
objectClass: top
objectClass: dcObject
objectClass: organization
o: cbpf
dc: cbpf
structuralObjectClass: organization
entryUUID: f2c41146-e80b-102a-8011-ee4af8243383
creatorsName: cn=anonymous
modifiersName: cn=anonymous
createTimestamp: 20061004155131Z
modifyTimestamp: 20061004155131Z
entryCSN: 20061004155131Z#000001#00#000000

dn: cn=admin,dc=cbpf,dc=br
objectClass: simpleSecurityObject
objectClass: organizationalRole
cn: admin
description: LDAP administrator
userPassword:: e2NyeXB0fXN2VVV0MlpvTmhKbDY=
structuralObjectClass: organizationalRole
entryUUID: f2d0b040-e80b-102a-8012-ee4af8243383
creatorsName: cn=anonymous
modifiersName: cn=anonymous
createTimestamp: 20061004155131Z
modifyTimestamp: 20061004155131Z
entryCSN: 20061004155131Z#000002#00#000000

root@ldap01:~#
```

Usando o comando abaixo para monitorar as consultas feitas no slapd.

```
tail -f /var/log/syslog
```

```
root@ldap01:~# tail -f /var/log/syslog
Oct  5 12:07:20 ldap01 -- MARK --
Oct  5 12:14:13 ldap01 slapd: slapd stopped.
Oct  5 12:14:13 ldap01 slapd: connections_destroy: nothing to destroy.
Oct  5 12:14:21 ldap01 slapd: slapd stopped.
Oct  5 12:14:21 ldap01 slapd: connections_destroy: nothing to destroy.
Oct  5 12:17:01 ldap01 /USR/SBIN/CRON[1155]: (root) CMD (   run-parts --report
/etc/cron.hourly)
Oct  5 12:27:20 ldap01 -- MARK --
Oct  5 12:47:20 ldap01 -- MARK --
Oct  5 13:07:20 ldap01 -- MARK --
Oct  5 13:27:20 ldap01 -- MARK --
```

Agora faça uma consulta em outro terminal e note o que acontece no arquivo /vasr/log/syslog:

```
ldapsearch -x -b 'cn=admin,dc=cbpf,dc=br' '(objectclass=*)'
```

```
root@ldap01:~# ldapsearch -x -b 'cn=Admin,dc=cbpf,dc=br' '(objectclass=*)'
# extended LDIF
#
# LDAPv3
# base <cn=Admin,dc=cbpf,dc=br> with scope sub
# filter: (objectclass=*)
# requesting: ALL
#

# admin, cbpf.br
dn: cn=admin,dc=cbpf,dc=br
objectClass: simpleSecurityObject
objectClass: organizationalRole
cn: admin
description: LDAP administrator

# search result
search: 2
result: 0 Success

# numResponses: 2
# numEntries: 1
root@ldap01:~#
```

Note que não aparecerá nada no syslog relacionado com o slapd, para que isto aconteça, precisamos configurar o nivel de log do slapd para que sejam mostradas os acessos à base.

Edite o arquivo `/etc/ldap/slapd.conf` mude a linha "`loglevel 0`" para "**`loglevel 256`**".

```
# This is the main slapd configuration file. See slapd.conf(5) for more
# info on the configuration options.

########################################################################
# Global Directives:

# Features to permit
#allow bind_v2

# Schema and objectClass definitions
include         /etc/ldap/schema/core.schema
include         /etc/ldap/schema/cosine.schema
include         /etc/ldap/schema/nis.schema
include         /etc/ldap/schema/inetorgperson.schema

# Schema check allows for forcing entries to
# match schemas for their objectClasses's
schemacheck     on

# Where the pid file is put. The init.d script
# will not stop the server if you change this.
pidfile         /var/run/slapd/slapd.pid

# List of arguments that were passed to the server
```

```
argsfile        /var/run/slapd.args

# Read slapd.conf(5) for possible values
loglevel        256
```

Faça a mesma consulta à base usando o comando `ldapsearch`

```
ldapsearch -x -b 'cn=Admin,dc=cbpf,dc=br' '(objectclass=*)'
```

Veja como ficou o syslog...

```
tail -f /var/log/syslog
```

```
#

# search result
search: 2
result: 32 No such object
matchedDN: dc=cbpf,dc=br

# numResponses: 1
root@ldap01:~# tail -f /var/log/syslog
Oct  6 15:07:34 ldap01 slapcat: bdb_db_init: Initializing BDB database
Oct  6 15:17:01 ldap01 /USR/SBIN/CRON[1902]: (root) CMD (   run-parts --report
/etc/cron.hourly)
Oct  6 15:26:28 ldap01 slapcat: bdb_db_init: Initializing BDB database
Oct  6 15:38:21 ldap01 slapd[1861]: conn=1 fd=11 ACCEPT from IP=127.0.0.1:1048
(IP=0.0.0.0:389)
Oct  6 15:38:21 ldap01 slapd[1863]: conn=1 op=0 BIND dn="" method=128
Oct  6 15:38:21 ldap01 slapd[1863]: conn=1 op=0 RESULT tag=97 err=0 text=
Oct  6 15:38:21 ldap01 slapd[1864]: conn=1 op=1 SRCH base="dc=admin,dc=cbpf,dc=br"
scope=2 deref=0 filter="(objectClass=*)"
Oct  6 15:38:21 ldap01 slapd[1864]: conn=1 op=1 SEARCH RESULT tag=101 err=32
nentries=0 text=
Oct  6 15:38:21 ldap01 slapd[1863]: conn=1 op=2 UNBIND
Oct  6 15:38:21 ldap01 slapd[1863]: conn=1 fd=11 closed
```

Agora todo acesso feito ao slapd será registrado no syslog

Para adicionar uma OU na base, crie um arquivo .ldif com o conteúdo abaixo.

```
#teste.ldif
#
dn: ou=INFO,dc=cbpf,dc=br
objectClass: top
objectClass: organizationalUnit
ou: INFO
```

Use o comando `ldapadd` para incluir a OU na base.

```
#ldapsearch -x -D “cn=admin,dc=cbpf,dc=br” -f teste.ldif -W
Enter LDAP Password:
adding new entry "ou=INFO,dc=cbpf,dc=br"
```

Para adicionar uma entrada na base, crie um arquivo .ldif com o conteúdo abaixo.

```
#usuario.ldif
dn: uid=usuario,ou=INFO,dc=cbpf,dc=br
objectClass: inetOrgPerson
objectClass: organizationalPerson
objectClass: Person
givenName: Usuario
uid: usuario
cn: Usuario da Silva
sn: da Silva
mail: usuario@cbpf.br
ou: INFO
title: Tecnico
telephoneNumber: 0000-0000
```

Use o comando `ldapadd` para incluir a OU na base.

```
root@ldap01:~#ldapsearch -x -D “cn=admin,dc=cbpf,dc=br” -f usuario.ldif -W
Enter LDAP Password:
adding new entry "ou=INFO,dc=cbpf,dc=br"
```

Digite `slapcat` para ver a base criada:

```
root@ldap01:~# slapcat
dn: dc=cbpf,dc=br
objectClass: top
objectClass: dcObject
objectClass: organization
o: CBPF
dc: cbpf
structuralObjectClass: organization
entryUUID: b9b3d4f0-3067-102b-9f3f-fdae02671108
creatorsName: cn=anonymous
modifiersName: cn=anonymous
createTimestamp: 20070104174952Z
modifyTimestamp: 20070104174952Z
entryCSN: 20070104174952Z#000001#00#000000

dn: cn=admin,dc=cbpf,dc=br
objectClass: simpleSecurityObject
objectClass: organizationalRole
cn: admin
description: LDAP administrator
userPassword:: e2NyeXB0fWNoWHM1WGZSZGlGemM=
structuralObjectClass: organizationalRole
entryUUID: b9ba4858-3067-102b-9f40-fdae02671108
creatorsName: cn=anonymous
modifiersName: cn=anonymous
createTimestamp: 20070104174952Z
modifyTimestamp: 20070104174952Z
entryCSN: 20070104174952Z#000002#00#000000

dn: ou=INFO,dc=cbpf,dc=br
objectClass: top
objectClass: organizationalUnit
```

```
ou: INFO
structuralObjectClass: organizationalUnit
entryUUID: 966bc1b4-3068-102b-8edc-9a9015eef7b3
creatorsName: cn=admin,dc=cbpf,dc=br
createTimestamp: 20070104175603Z
entryCSN: 20070104175603Z#000001#00#000000
modifiersName: cn=admin,dc=cbpf,dc=br
modifyTimestamp: 20070104175603Z

dn: uid=usuario,ou=INFO,dc=cbpf,dc=br
objectClass: inetOrgPerson
objectClass: organizationalPerson
objectClass: person
givenName: Usuario
uid: usuario
cn: Usuario da Silva
sn: da Silva
mail: usuario@cbpf.br
ou: INFO
title: Tecnico
telephoneNumber: 0000-0000
structuralObjectClass: inetOrgPerson
entryUUID: 1bc9a75c-306b-102b-8ede-9a9015eef7b3
creatorsName: cn=admin,dc=cbpf,dc=br
createTimestamp: 20070104181405Z
entryCSN: 20070104181405Z#000001#00#000000
modifiersName: cn=admin,dc=cbpf,dc=br
modifyTimestamp: 20070104181405Z
```