Instalação do OpenLDAP com o esquema brEduPerson

> ⚠ **ATENÇÃO**
>
> Este roteiro deve ser executado apenas mediante orientação explícita do Service Desk da RNP.

1. Introdução

Este tutorial apresenta os passos necessários para se fazer a instalação do OpenLDAP com o esquema brEduPerson

2. Roteiro

2.1. Inicialmente deve ser efetuada a instalação do pacote slapd. Para tanto execute as linhas de comando a seguir:

```
debconf-set-selections <<-EOF
slapd slapd/no_configuration boolean true
EOF
apt-get -y install slapd
```

2.2. Para liberar o acesso as portas utilizadas para acesso remoto ao LDAP, adicione as linhas a seguir no final do arquivo de regras do firewall (/etc/default/firewall). Em seguida, reinicie o firewall.

```
# Liberação do LDAP                                    #LDAP
iptables -A INPUT -p tcp -m tcp --dport 389 -j ACCEPT #LDAP
iptables -A INPUT -p tcp -m tcp --dport 636 -j ACCEPT #LDAP
                                                       #LDAP
```

```
/etc/init.d/firewall restart
```

2.3. No escopo do projeto, foram definidas algumas configurações padrão, com o objetivo de uniformizar os servidores LDAP das instituições. Para aplicar essas novas configurações, é preciso inicialmente parar o serviço slapd. para tanto, execute a linha de comando a seguir:

```
/etc/init.d/slapd stop
```

2.4. Faça a criação da pasta que será utilizada pela base LDAP através do comando a seguir:

```
mkdir /var/lib/ldap
```

2.5. Faça download dos arquivos de configuração criados pela equipe do projeto com os comandos a seguir:

```
wget https://svn.rnp.br/repos/CAFe/conf/openldap/slapd -O /etc/default/slapd --no-check-certificate
wget https://svn.rnp.br/repos/CAFe/conf/openldap/slapd.conf -O /etc/ldap/slapd.conf --no-check-certificate
wget https://svn.rnp.br/repos/CAFe/conf/openldap/ldap.conf -O /etc/ldap/ldap.conf --no-check-certificate
wget https://svn.rnp.br/repos/CAFe/conf/openldap/DB_CONFIG -O /var/lib/ldap/DB_CONFIG --no-check-certificate
wget https://svn.rnp.br/repos/CAFe/schemas/openldap/eduperson.schema -O /etc/ldap/schema/eduperson.schema --no-
check-certificate
wget https://svn.rnp.br/repos/CAFe/schemas/openldap/breduperson.0.0.6.schema -O /etc/ldap/schema/breduperson.
0.0.6.schema --no-check-certificate
wget https://svn.rnp.br/repos/CAFe/schemas/openldap/schac-20061212-1.3.0 -O /etc/ldap/schema/schac-20061212-
1.3.0 --no-check-certificate
wget https://svn.rnp.br/repos/CAFe/schemas/openldap/samba.schema -O /etc/ldap/schema/samba.schema --no-check-
certificate
```

2.6. Após fazer o download dos arquivos deve-se atentar para a necessidade de fazer algumas breves alterações em alguns dos arquivos conforme segue:

slapd.conf: deve-se substituir as ocorrências de ${HOSTNAME} pelo hostname da máquina (ex.: servidor, não utilizar servidor.instituicao.br). Deve-se substituir ainda as ocorrências de ${RAIZ_BASE_LDAP} pelo valor correspondente a raiz da base LDAP de sua instituição, como por exemplo dc=instituicao,dc=br.
ldap.conf: deve-se substituir as ocorrências de ${RAIZ_BASE_LDAP} pelo valor correspondente a raiz da base LDAP como por exemplo dc=instituicao,dc=br.

2.7. Edite o arquivo /etc/default/slapd e altere a entra SLAPD_CONF= para:

```
SLAPD_CONF=/etc/ldap/slapd.conf
```

2.8. Crie o arquivo `/tmp/openssl.cnf` com o conteúdo a seguir não esquece de substituir a variável `$HOSTNAME` pelo hostname máquina (ex.: servidor, não utilizar servidor.instituicao.br).

```
[ req ]
default_bits = 2048 # Size of keys
string_mask = nombstr # permitted characters
distinguished_name = req_distinguished_name

[ req_distinguished_name ]
# Variable name   Prompt string
#---------------------   ----------------------------------
0.organizationName = Nome da universidade/organização
organizationalUnitName = Departamento da universidade/organização
emailAddress = Endereço de email da administração
emailAddress_max = 40
localityName = Nome do município (por extenso)
stateOrProvinceName = Unidade da Federação (por extenso)
countryName = Nome do país (código de 2 letras)
countryName_min = 2
countryName_max = 2
commonName = Nome completo do host (incluíndo o domínio)
commonName_max = 64

# Default values for the above, for consistency and less typing.
# Variable name   Value
#------------------------------   ------------------------------
#0.organizationName_default =
organizationalUnitName_default = CPD
#localityName_default = Porto Alegre
#stateOrProvinceName_default = Rio Grande do Sul
countryName_default = BR
commonName_default = $HOSTNAME
```

É possível fazer o download do arquivo acima através da seguinte linha de comando:

```
wget https://svn.rnp.br/repos/CAFe/conf/ssl/openssl.cnf -O /tmp/openssl.cnf --no-check-certificate
```

2.9. Para gerar o par chave/certificado para o OpenLDAP, utilize os comandos no bloco abaixo:

```
openssl genrsa -out /etc/ldap/$HOSTNAME.key 2048 -config /tmp/openssl.cnf
openssl req -new -key /etc/ldap/$HOSTNAME.key -out /etc/ldap/$HOSTNAME.csr -batch -config /tmp/openssl.cnf
openssl x509 -req -days 730 -in /etc/ldap/$HOSTNAME.csr -signkey /etc/ldap/$HOSTNAME.key -out /etc/ldap
/$HOSTNAME.crt
```

2.10. O LDAP que foi instalado encontra-se vazio, ou seja, não há nenhum elemento em sua base da dados. Através dos passos a seguir, será possível fazer a carga inicial de dados na base LDAP. Para se fazer a carga inicial de dados no LDAP deve-se inicialmente fazer o download do script responsável por tal etapa. Para tanto, execute a linha de comando a seguir:

```
wget https://svn.rnp.br/repos/CAFe/scripts/openldap/popula.sh -O /tmp/popula.sh --no-check-certificate
```

2.11. Após fazer download do popula.sh, edite-o substituindo as valores das variáveis SENHA_ADMIN e SENHA_LEITOR_SHIB. Tais variáveis encontram-se nas linhas 7 e 8, respectivamente. Uma vez feita a substituição do valores, execute o script através das seguintes linhas de comando:

```
/etc/init.d/slapd stop
sh /tmp/popula.sh
/etc/init.d/slapd start
```

2.12. Por fim, faça um teste de conexão utilizando o Apache Directory Studio. Em Tutorial Básico Apache DS há informações sobre a utilização desse software.

3. Homologação Parcial

3.1. Para garantir que os passos descritos acima foram corretamente seguidos é necessário a execução de um script de homologação. Para fazer download desde script utilize a linha de comando abaixo:

```
wget https://svn.rnp.br/repos/CAFe/scripts/homologacao/clientes/cafe-homolog-ldap.sh -O /tmp/cafe-homolog-ldap.
sh --no-check-certificate
```

3.2. Após fazer download, execute este script com permissão de root.

```
/tmp/cafe-homolog-ldap.sh
```

3.3. Se todas as checagens forem bem sucedidas você deverá receber a mensagem abaixo. Envie o arquivo de log gerado pelo script para o Service Desk e aguarde instruções para continuidade do processo de adesão.

```
OK - Nao foram encontrados pontos impeditivos para o processo de adesao.
     Envie o arquivo de log gerado (cafe-homolog-ldap.sh.log) para o Service
     Desk da RNP para dar continuidade ao atendimento.
```

3.4. Se ocorrer alguma falha na checagem você deverá receber a mensagem abaixo. Identifique qual/quais checagem não foram bem sucedidas e faça a devida correção. Após isto retorne para o item 3.2. Em caso de dúvidas entre em contato com o Service Desk.

```
ERRO - Foram encontrados pontos impeditivos para o processo de adesao.
       Solucione os erros e execute novamente este script.
```

4. FAQ

A seção de FAQ está disponível aqui.