

Relatório do Projeto

INTEGRAÇÃO DE REDE LINUX E WINDOWS COM SAMBA E LDAP



Responsável técnico

Pedro Delfino dos Santos Neto

e-mail: delfino@delfino.com.br

pedrod@passaura.com.br



Setor STI
IRMÃOS PASSAURA & CIA LTDA
Data: 25/02/2003

- **Objetivo**

Integrar informações da rede da PASSAURA para que as máquinas Windows 98, Windows XP e Windows 2000 possam fazer autenticação em um servidor de dados, assim centralizando as informações de arquivos e sistemas que rodam em rede. Toda estação de trabalho deverá ter a capacidade de compartilhar arquivos e impressoras com as devidas permissões de acesso, assim como seus usuários deverão ter a capacidade de fazer login em qualquer estação de trabalho.

- **Sistema implantado**

O sistema escolhido para fazer a integração da rede foi o LINUX na distribuição DEBIAN versão 3.0 utilizando o serviço **SAMBA ALPHA 3.0** e serviço de diretório LDAP com **OPENLDAP**.

Serviços implantados no servidor LINUX:

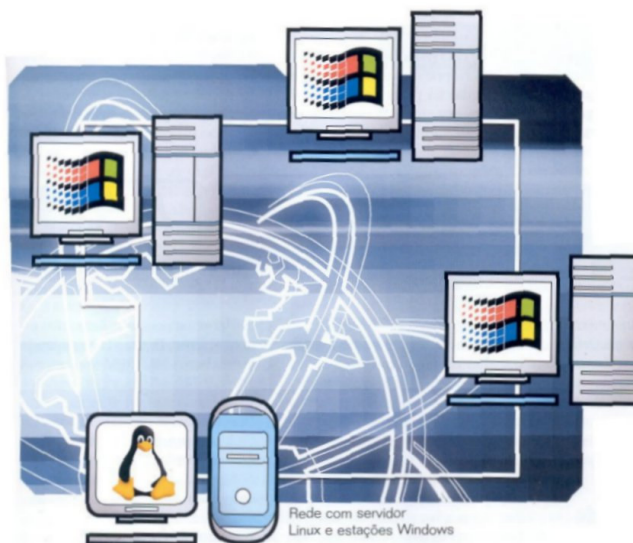
SAMBA: É o responsável por fazer a integração das estações de trabalho com o servidor de DADOS, assim **substituindo** a necessidade de um servidor de dados Windows 2000.

LDAP: O serviço do LDAP é o responsável pela centralização das informações da rede, assim todos os serviços instalados nos servidores iram fazer a autenticação através do LDAP.

- **Vantagens**

Usando o LINUX como sistema operacional em nosso servidor ganhamos não só com relação ao custo, mas também com a disponibilidade do servidor, já que o LINUX tem se mostrado um sistema operacional leve e estável e de simples manutenção, qualquer manutenção pode ser realizada remotamente.

Integrando o serviço do SAMBA + LDAP nossa rede esta compatível com qualquer estação de trabalho Windows 95, 98, 2000 e XP, essas estações poderão usar todas as vantagens de uma rede utilizando Windows 2002 Server como servidor de dados, na integração do LDAP com o SAMBA as informações da rede estão centralizadas, assim os usuários, as máquinas os endereços de e-mail, as autenticações para Proxy estão em uma única base de dados centralizada, permitindo que um servidor de e-mail por exemplo, autentique seus usuários na base do



DIRETÓRIO LDAP facilitando a administração dos usuário

Na questão de segurança o LINUX tem muitas opções para trabalhar com ACL (Access Control List) implementado em nosso servidor e também um sistema de arquivos moderno e rápido.

Custo: Não há um custo para a instalação de um sistema rodando o SAMBA + LDAP, já que esses dois sistemas assim como os sistemas operacionais LINUX estão sob licença GPL (GNU GENERAL PUBLIC LICENSE), sem restrições de uso e quantidade instalação.

Na tabela abaixo esta o custo para a mesma solução aplicada em nosso projeto porem utilizando software proprietário. (software comerciais)

PLANILHA DE CUSTO PARA IMPLANTAÇÃO DE SERVIDOR WINDOWS 2000				
ITEM	Produto	Quant.	Valor	Valor Total
1	Windows 2000 SERVER	1	2.939,00	2.939,00
2	Licença CAL para Windows 2000	74	129,00	9.546,00
Total Geral				12.485,00

Preços cotados em R\$ no dia 19/02/2003

- ***Desvantagens***

Falta de integração para listas de acesso em estações Windows 98, pode ser resolvido alterando configurações na estação de trabalho. Necessidade de edição do registro de Windows XP para liberar o acesso a rede SAMBA.

- ***Informações de hardware***

Abaixo estão as informações de hardware do servidor implantando.

Nome	Processador	Memória Ram	Área de troca	Rede
SDL	Intel(R) Pentium(R) 4 CPU 2.00GHz	512 MB	329 MB	10.1.1.2/255.255.255.0

- **Informações de Processador**

```
*CPU
processor      : 0
vendor_id     : GenuineIntel
cpu family    : 15
model         : 2
model name    : Intel(R) Pentium(R) 4 CPU 2.00GHz
stepping      : 4
cpu MHz       : 2018.001
cache size    : 512 KB
fdiv_bug      : no
hlt_bug       : no
f00f_bug      : no
coma_bug      : no
fpu           : yes
fpu_exception : yes
cpuid level   : 2
wp            : yes
flags         : fpu vme de pse tsc msr pae mce cx8 apic sep mtrr pge mca cmov pat
pse36 clflush dts acpi mmx fxsr sse sse2 ss ht tm
bogomips      : 4023.91
```

- **Pontos de montagem**

Filesystem	Size	Used	Avail	Use%	Mounted on
/dev/sda1	4.6G	521M	3.8G	12%	/
/dev/sda2	3.5G	211M	3.1G	7%	/var
/dev/sdb1	8.4G	449M	7.5G	6%	/home
/dev/sdc1	17G	3.3G	12G	21%	/dados

- **Particionamento de disco**

```
Disk /dev/sda: 255 heads, 63 sectors, 1111 cylinders
Units = cylinders of 16065 * 512 bytes

   Device Boot      Start         End      Blocks   Id  System
/dev/sda1   *           1           608    4883728+   83   Linux
/dev/sda2             609        1070    3711015   83   Linux
/dev/sda3          1071        1111    329332+    5   Extended
/dev/sda5          1071        1111    329301    82   Linux swap

Disk /dev/sdb: 255 heads, 63 sectors, 1111 cylinders
Units = cylinders of 16065 * 512 bytes

   Device Boot      Start         End      Blocks   Id  System
/dev/sdb1           1        1111    8924076   83   Linux

Disk /dev/sdc: 255 heads, 63 sectors, 2235 cylinders
Units = cylinders of 16065 * 512 bytes

   Device Boot      Start         End      Blocks   Id  System
/dev/sdc1           1        2235   17952606   83   Linux
```

• **Gerenciamento de memória RAM**

	total	used	free	shared	buffers	cached
Mem:	500	494	6	0	84	303
-/+ buffers/cache:		106	394			
Swap:	321	0	321			

• **Portas**

Starting nmap V. 2.54BETA31 (www.insecure.org/nmap/)		
Interesting ports on localhost (127.0.0.1):		
(The 1543 ports scanned but not shown below are in state: closed)		
Port	State	Service
22/tcp	open	ssh
25/tcp	open	smtp
80/tcp	open	http
111/tcp	open	sunrpc
139/tcp	open	netbios-ssn
389/tcp	open	ldap
445/tcp	open	microsoft-ds
587/tcp	open	submission
8080/tcp	open	http-proxy
10082/tcp	open	amandaidx
10083/tcp	open	amidxtape

• **Processos**

Nmap run completed -- 1 IP address (1 host up) scanned in 1 second				
PID	TTY	STAT	TIME	COMMAND
1	?	S	0:03	init
2	?	SW	0:58	[keventd]
3	?	SWN	0:01	[ksoftirqd_CPU0]
4	?	SW	0:00	[kswapd]
5	?	SW	0:00	[bdfld]
6	?	SW	0:00	[kupdated]
7	?	SW	0:00	[i2oevtd]
9	?	SW	0:00	[scsi_eh_0]
10	?	SW	0:00	[kjournald]
45	?	SW	0:00	[khubd]
80	?	SW	0:00	[kjournald]
81	?	SW	0:00	[kjournald]
82	?	SW	0:00	[kjournald]
105	?	SW	0:00	[eth0]
110	?	S	0:00	/sbin/portmap
188	?	S	0:00	/sbin/syslogd
191	?	S	0:00	/sbin/klogd
198	?	S	0:00	/usr/sbin/slaped
200	?	S	0:00	/usr/sbin/slaped
201	?	S	0:02	/usr/sbin/slaped
319	?	S	0:12	/usr/sbin/slaped
320	?	S	0:13	/usr/sbin/slaped
326	?	S	0:00	sendmail: MTA: accepting connections
335	?	S	0:00	/usr/sbin/sshd
356	?	S	0:00	/usr/sbin/cron
369	tty6	S	0:00	-bash
373	?	S	0:13	/usr/sbin/slaped

376	?	S	0:13	/usr/sbin/slapd
377	?	S	0:14	/usr/sbin/slapd
378	?	S	0:13	/usr/sbin/slapd
379	?	S	0:13	/usr/sbin/slapd
806	?	S	0:11	/usr/sbin/slapd
894	?	S	0:10	/usr/sbin/slapd
951	?	S	0:12	/usr/sbin/slapd
1026	?	S	0:08	/usr/sbin/slapd
1033	?	S	0:07	/usr/sbin/slapd
3674	?	S	0:00	/usr/local/samba-alpha-ldap/sbin/smbd -D
3676	?	S	0:02	/usr/local/samba-alpha-ldap/sbin/nmbd -D
3936	?	S	0:04	/usr/sbin/slapd
4313	tty6	S	0:43	iptraf
4658	?	S	0:00	/usr/sbin/squid -D -sYC
4661	?	S	0:09	(squid) -D -sYC
4667	?	S	0:00	(unlinkd)
14448	?	S	0:00	/usr/sbin/apache
16055	?	S	0:00	/usr/sbin/slapd
16057	?	S	0:00	/usr/sbin/slapd
16061	tty5	S	0:00	/sbin/getty 38400 tty5
16062	tty4	S	0:00	/sbin/getty 38400 tty4
16066	tty1	S	0:01	-bash
16444	tty3	S	0:00	/sbin/getty 38400 tty3
16749	?	S	0:00	/usr/sbin/inetd
16958	tty2	S	0:00	/sbin/getty 38400 tty2
18512	?	S	0:00	/usr/lib/squid/ldap_auth -b ou=People,dc=passaura,dc=com,dc=br localhost
18513	?	S	0:00	/usr/lib/squid/ldap_auth -b ou=People,dc=passaura,dc=com,dc=br localhost
18514	?	S	0:00	/usr/lib/squid/ldap_auth -b ou=People,dc=passaura,dc=com,dc=br localhost
18515	?	S	0:00	/usr/lib/squid/ldap_auth -b ou=People,dc=passaura,dc=com,dc=br localhost
18516	?	S	0:00	/usr/lib/squid/ldap_auth -b ou=People,dc=passaura,dc=com,dc=br localhost
18527	?	S	0:00	/usr/sbin/apache
18528	?	S	0:00	/usr/sbin/apache
18529	?	S	0:00	/usr/sbin/apache
18530	?	S	0:00	/usr/sbin/apache
18531	?	S	0:00	/usr/sbin/apache
18841	?	S	0:00	/usr/local/samba-alpha-ldap/sbin/smbd -D
18887	?	S	0:00	/usr/local/samba-alpha-ldap/sbin/smbd -D
18926	?	S	0:00	anacron -s
19040	tty1	R	0:00	ps ax

- **Porque o Debian ?**

A escolha da distribuição DEBIAN pesou muito quando analisamos as atualizações que devem ser feitas em um servidor, pesando sempre na segurança dos dados devemos manter nosso sistema operacional sempre atualizado, como o DEBIAN conta com a ferramenta APT (Advanced Package Tool) para gerenciamento de seus pacotes .deb, ferramenta essa que facilita muito a atualização do sistema operacional inteiro (referencias sobre o APT <http://www.debian.org>).

- **Instalação do OPENLDAP 2.0.23**

Na instalação do ldap estaremos utilizando o APT

```
apt-get source openldap2 --compile
```

Com esse comando estemos baixando os sources do openldap2 e já compilando. Ao fazer essa operação estaremos gerando os arquivos .deb que serão os responsáveis para fazer a instalação do LDAP, ao executar o comando acima o APT ira verificar dependências nos pacotes, caso ocorra alguma dependência teremos que resolver utilizando

```
apt-get install <nome>
```

Onde <nome> é o pacote que o APT encontrou dependência.
Após resolvido as dependências devemos repetir o comando

```
apt-get source openldap2 --compile
```

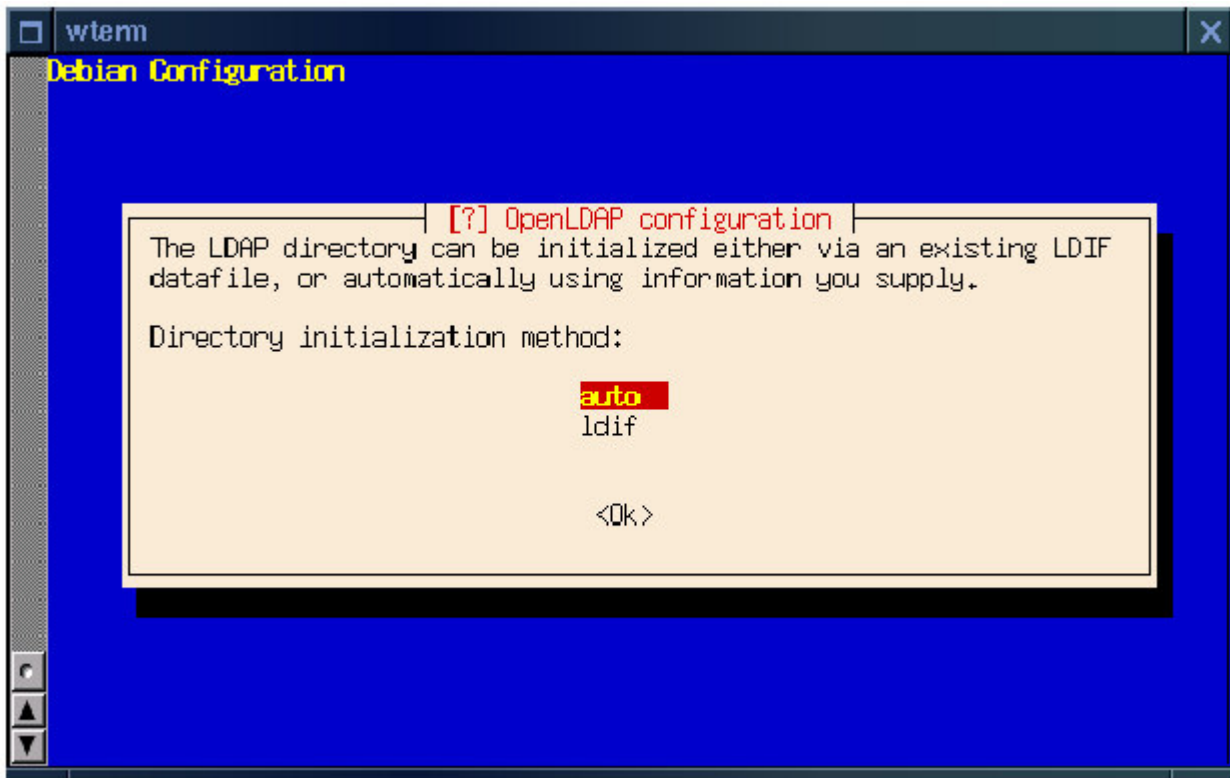
Serão gerados 5 arquivos:

ldap-gateways_2.0.23-6_i386.deb	-	Responsável pela comunicação
ldap-utils_2.0.23-6_i386.deb	-	Bibliotecas úteis
libldap2-dev_2.0.23-6_i386.deb	-	Bibliotecas para o cliente ldap
libldap2_2.0.23-6_i386.deb	-	Cliente ldap
slapd_2.0.23-6_i386.deb	-	Server ldap

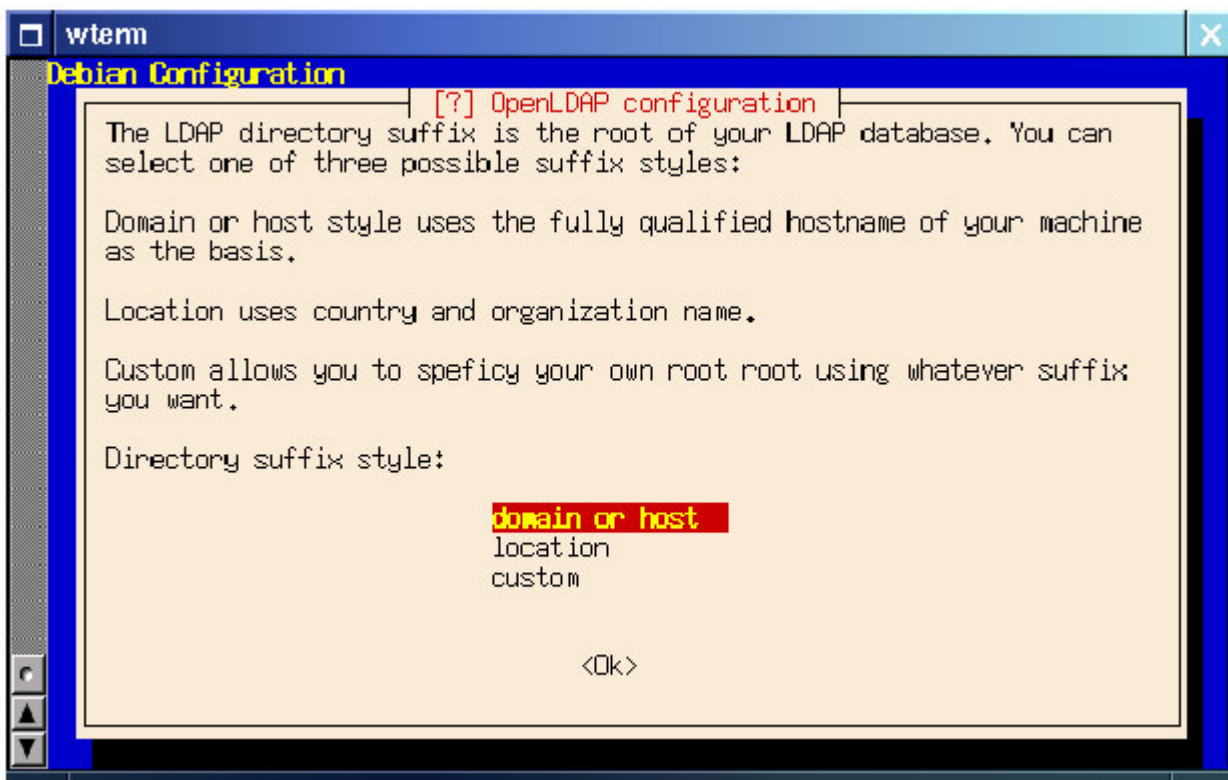
Para fazer a instalação do OPENLDAP comece pela bibliotecas e por fim o servidor

```
dpkg -i ldap-gateways_2.0.23-6_i386.deb
dpkg -i ldap-utils_2.0.23-6_i386.deb
dpkg -i libldap2-dev_2.0.23-6_i386.deb
dpkg -i libldap2_2.0.23-6_i386.deb
dpkg -i slapd_2.0.23-6_i386.deb
```

Após você instalar o slapd_2.0.23-6_i386.deb o debconf será chamado e a configuração do openldap:

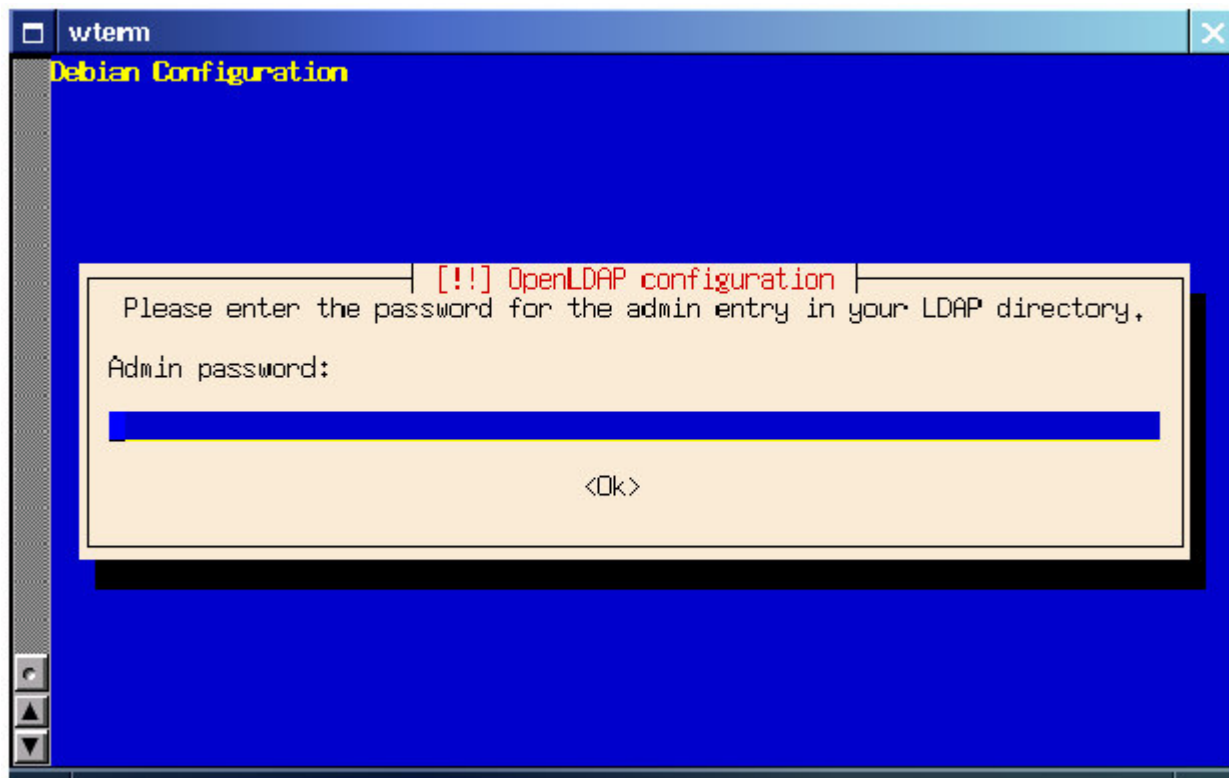


Deve-se escolher como a base de dados do LDAP será criada, podemos iniciar por um arquivo padrão LDIF, em nosso caso vamos escolher a opção AUTO para que o ldap gere automaticamente nossa base, o banco usado para gerar essa base será o ldbm.



Aqui escolhemos o padrão para o SUFIXO do LDAP, esse sufixo será utilizado para as pesquisa e autenticação no diretório ldap. Escolha o opção domain or host para que o

sufixo seja criado com o padrão do seu endereço de DNS.



Indique uma senha para o administrador do diretório, ele será o usuário responsável por fazer as alterações no diretório.

O debconf estará fazendo toda configuração do diretório, que estará pronto para ser utilizado.

Arquivos de configuração do OPENLDAP.

/etc/ldap.scret	-	Senha do administrador do diretório
/etc/ldap/slap.conf	-	Configuração do servidor LDAP
/etc/ldap/ldap.conf	-	Configuração do cliente ldap
/var/lib/ldap	-	Diretório da base de dados

```
#####/etc/ldap/ldap.conf #####
# $OpenLDAP: pkg/ldap/libraries/libldap/ldap.conf,v 1.4.8.6 2000/09/05 17:54:38
kurt Exp $
#
# LDAP Defaults
#
# See ldap.conf(5) for details
# This file should be world readable but not world writable.
#### local do servido
host localhost
#### base principal do LDAP
base dc=passaura,dc=com,dc=br
#### User que sera padrao nas pesquisas
binddn cn=admin,dc=passaura,dc=com,dc=br
```

Relatório do Projeto
Integração de Rede LINUX e Windows com Samba e LDAP

```
#### Senha padrao para fazer as pesquisas
bindpw NOSSA_SENHA
#### Senha utilizando o MD5
pam_password md5
#### Define um filtro para as pesquisas
pam_filter objectclass=accout
#### Forca os usuarios a utilizar um determinado grupo
pam_groupdn cn=users,ou=Group,dc=passaura,dc=com,dc=br
### Habilita o SSL
ssl yes

#URI ldap://localhost
#ldap://ldap-master.example.com:666
#SIZELIMIT 12
#TIMELIMIT 15
#DEREF never
#####
```

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

# 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 para habilitar o samba no ldap
include /etc/ldap/schema/samba-alpha.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.pid

# List of arguments that were passed to the server
argsfile /var/run/slapd.args

# Where to store the replica logs
relogfile /var/lib/ldap/replog

# Read slapd.conf(5) for possible values
loglevel 0

#####
# ldbm database definitions
#####

# The backend type, ldbm, is the default standard
database ldbm

# The base of your directory
suffix "dc=passaura,dc=com,dc=br"

# Where the database file are physically stored
directory "/var/lib/ldap"

# Indexing options
```

```
index objectClass eq

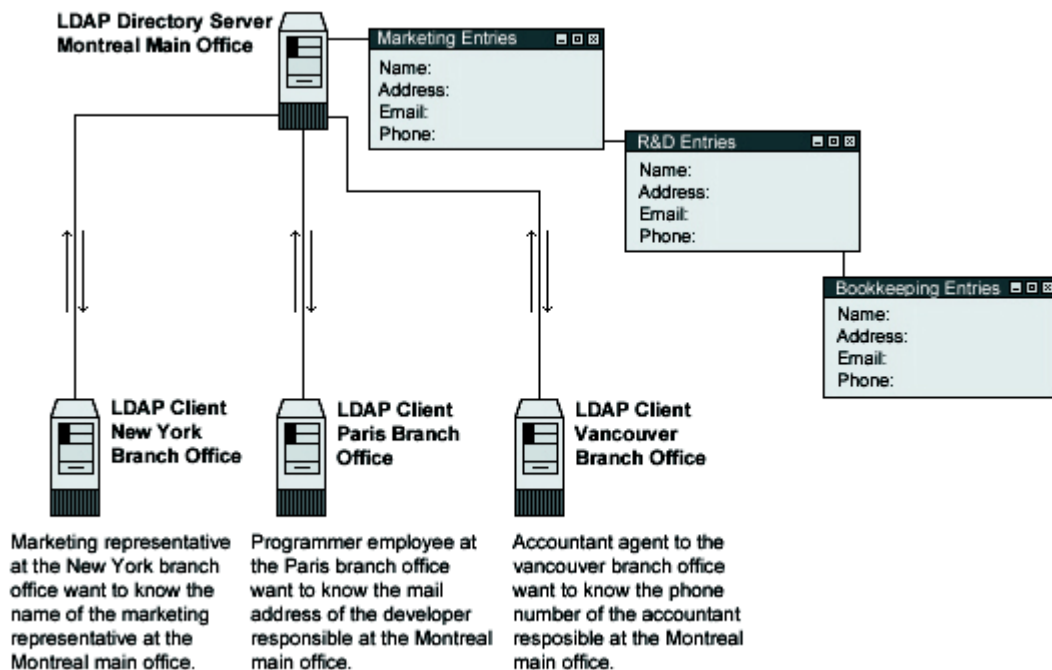
# Save the time that the entry gets modified
lastmod on

# The userPassword by default can be changed
# by the entry owning it if they are authenticated.
# Others should not be able to see it, except the
# admin entry below
access to attribute=userPassword
    by dn="cn=admin,dc=passaura,dc=com,dc=br" write
    by anonymous auth
    by self write
    by * none

# The admin dn has full write access
access to *
    by dn="cn=admin,dc=passaura,dc=com,dc=br" write
    by * read

# For Netscape Roaming support, each user gets a roaming
# profile for which they have write access to
access to dn="*.*,ou=Roaming,o=morsnet"
    by dn="cn=admin,dc=passaura,dc=com,dc=br" write
    by dnattr=owner write
```

```
#####/etc/ldap.secret #####
NOSSA_SENHA
#####
```



Estrutura de um diretório LDAP

- **Instalando o pacote do Migrationtools**

O pacote do migrationtools é o responsável por fazer a migração dos dados do LINUX para um arquivo padrão LDIF, esse pacote instala scripts perl que fazem as migrações.

Estaremos migrando os seguintes arquivos:

```
/etc/passwd  
/etc/group
```

Verificamos se o perl5 está instalado, caso não esteja instalamos

```
apt-get install perl5
```

Instalamos o migrationtools

```
apt-get install migrationtools
```

Agora acessamos o `/usr/share/migrationtools` e editamos o arquivo `migrate_common.ph`, esse arquivo é o responsável pela configuração básica dos demais scripts, altere conforme abaixo, localize as linhas.

```
##### /usr/share/migrationtools/migrate_common.ph #####  
# Default DNS domain  
$DEFAULT_MAIL_DOMAIN = "passaura.com.br";          # DNS do seu servidor de email  
  
# Default base  
$DEFAULT_BASE = "dc=passaura,dc=com,dc=br";        # SUFIXO base do LDAP  
#####
```

Migrando os usuários

Vamos migrar os usuários para um arquivo padrão LDIF, ainda dentro do diretório `/usr/share/migrationtools` execute.

```
./migrate_passwd.pl /etc/passwd /tmp/usuarios.ldif
```

Estaremos criando um arquivo `/tmp/usuarios.ldif` padrão para inserir na base ldap.

```
##### /tmp/usuarios.ldif #####  
dn: uid=ssh,ou=People,dc=passaura,dc=com,dc=br  
uid: ssh  
cn::c3NoLWxkYXA=  
objectClass: account  
objectClass: posixAccount  
objectClass: top  
objectClass: shadowAccount  
userPassword: {crypt}$1$u2Yc7v0D$hrIpIUHsiZeLuWbUjmnHd/
```

```
shadowLastChange: 12101
shadowMax: 99999
shadowWarning: 7
loginShell: /bin/bash
uidNumber: 1154
gidNumber: 100
homeDirectory: /home/ssh
#####
```

Migrando os grupos

Vamos migrar os grupos dos usuários para um arquivos padrão LDIF ainda dentro do diretório /usr/share/migrationtools execute.

```
./migrate_group.pl /etc/group /tmp/group.ldif
```

Estaremos criando um arquivo /tmp/group.ldif padrão para inserir na base ldap.

```
##### /tmp/group.ldif #####
dn: cn=smmssp,ou=Group,dc=passaura,dc=com,dc=br
objectClass: posixGroup
objectClass: top
cn: smmsp
userPassword: {crypt}x
gidNumber: 102
#####
```

Migrando a Base de Objetos

Quanto ao migrar a base de objetos, serve para que o diretório de ldap possa criar os "Objectos ou", a principio vamos criar apenas o "OU" People e Group.

```
./migrate_base.pl > /tmp/base.ldif
```

Executando o comando acima estaremos migrando os Objetos básicos para a criação do seu diretório. Vamos utilizar apenas o "OU" People que é responsável por guardar os usuários do diretório, e o group que o responsável por guardar os grupos. Portanto edite o /tmp/base.ldif delete as linhas que fazer referencias aos outros "OU", o arquivo deve ficar como indicado abaixo

```
##### /tmp/base.ldif #####
dn: ou=People,dc=passaura,dc=com,dc=br
ou: People
objectClass: top
objectClass: organizationalUnit

dn: ou=Group,dc=passaura,dc=com,dc=br
ou: Group
objectClass: top
objectClass: organizationalUnit
#####
```

- ***Adicionando as informações dos arquivos ldif no diretório LDAP***

Antes de executar o comando acesse o diretório /tmp.

Vamos utilizar o ldapadd para adicionar os dados base no ldap.

Adicionando o base.ldif

```
cd /tmp

ldapadd -x -D "cn=admin,dc=passaura,dc=com,dc=br" -f base.ldif -W
Enter LDAP Password:
```

Com isso acabamos criar os objetos "OU" People e Group, o básico para fazer a autenticação no ldap, os arquivos ldif são apenas um arquivo padrão de informação do ldap para que possamos gerar realmente a base do diretório. Estamos prontos para fazer a importação dos grupos e por fim os usuários.

Adicionando o group.ldif

```
cd /tmp

ldapadd -x -D "cn=admin,dc=passaura,dc=com,dc=br" -f group.ldif -W
Enter LDAP Password:
```

Adicionando o usuarios.ldif

```
cd /tmp

ldapadd -x -D "cn=admin,dc=passaura,dc=com,dc=br" -f usuarios.ldif -W
Enter LDAP Password:
```

Agora todos nossos grupos e usuários do sistema estão no diretório ldap .

Pedemos fazer um teste para saber se o LDAP esta funcionando, vamos utilizar o ldapclient para fazer isso, assim teremos que analisar as configurações do arquivo /etc/ldap/ldap.conf (já visto).

Para fazer a pesquisa simple no diretório LDAP.

```
ldapsearch -x
```

Esse comando ira retornar todos os objetos do seu diretório, ou seja usuários, grupos etc.

Quando essa pesquisa retornar seu resultado indica que o LDAP esta configurado corretamente.

• **Configuração sistema para administração do ldap.**

Agora que o LDAP esta rodando poderemos manipular nossos usuários via WEB utilizando fechamentas OpenSource, vamos utilizar o **DAVEDAP**.

Para baixar o davedap acessamos o site do *freshmeat.net* e pesquisamos por davedap. Escrito em php o davedap vai ajudar no compreender os objetos do LDAP, adicionar usuarios, grupos, membros de grupos etc.

Para que o davedap funcione corretamente teremos que instalar os seguintes pacotes:

PHP4

```
pt-get install php4
apt-get install php4-pear
apt-get install php4-ldap
```

APACHE:

```
apt-get install apache
```

Configuramos o apache para interpretar o php4, localizamos as linhas indicadas abaixo no arquivo /etc/apache/httpd.conf, e retiramos os comentários.

```
##### /etc/apache/httpd.conf #####
LoadModule php4_module /usr/lib/apache/1.3/libphp4.so

<IfModule mod_dir.c>
    DirectoryIndex index.html index.htm index.shtml index.cgi index.php
</IfModule>

# And for PHP 4.x, use:
#
AddType application/x-httpd-php .php
AddType application/x-httpd-php-source .phps
#####
```

• **Instalando o davedap**

Descompactamos o davedap no diretório padrão do servidor apache

```
cd /var/www/
tar -xzf davedap-0.7.0.4.tar.gz
cd davedap-0.7.4
```

No diretório do davedap editamos apenas o config.inc.php onde estão as opção para acessar o diretório ldap.

```
ls
LICENSE
config.inc.php
htaccess
images
index.php
```

```
##### /var/www/davedap/config.inc.php #####
<?php

// Endereco do servidor de ldap
$ldap_server = "localhost";

// Porta do servidor de ldap
$ldap_port = 389;

// Diretorio root do servidor ldap
$base_dn = "dc=passaura,dc=com,dc=br";

// Where should I search?
// DN usado para fazer as pesquisas
$search_dn = "ou=admin,dc=passaura,dc=com,dc=br";

// Which attributes to include in the drop-down menu (comma-separated)
$search_attribute_names = "uid, givenname, sn, telephonenumber";

// Pretty names for the attributes above (you should have the same number here
as you have there)
$search_attribute_display_names = "user ID, first name, last name, phone";

// the search method in the drop down box (one for displaying, one for parsing
on the backend 1:1 )
$search_criteria_options = "starts_with, contains, ends_with, equals";
$search_criteria_options_display = "starts with, contains, ends with, is";

// The list of attributes to display in each vcard entry (all lower case)
$vcards_attribute_names = "cn, sn, address, telephonenumber";

// The attr name to display at the top of each vcard
$vcards_title_attribute = "uid";

// Unique ID for your LDAP server (uid is probably okay, but might be cn)
$unique_id = "uid";

// specify the authentication type. You can specify:
// 'config' means from the config file: you specify the login dn and password
right here (below)
// Realize that any other web-user can read this file
// 'form' means ask the user for a dn and password in a form (store them in a
cookie)
// this should be used only with https. Realize that your dn and password
will go back
// and forth in a cookie every page refresh
$auth_type = 'config';

// If you used auth_type 'form', you can adjust how long the cookie will last
(default is one hour, 3600 seconds )
```



```
$cookie_time = 3600;

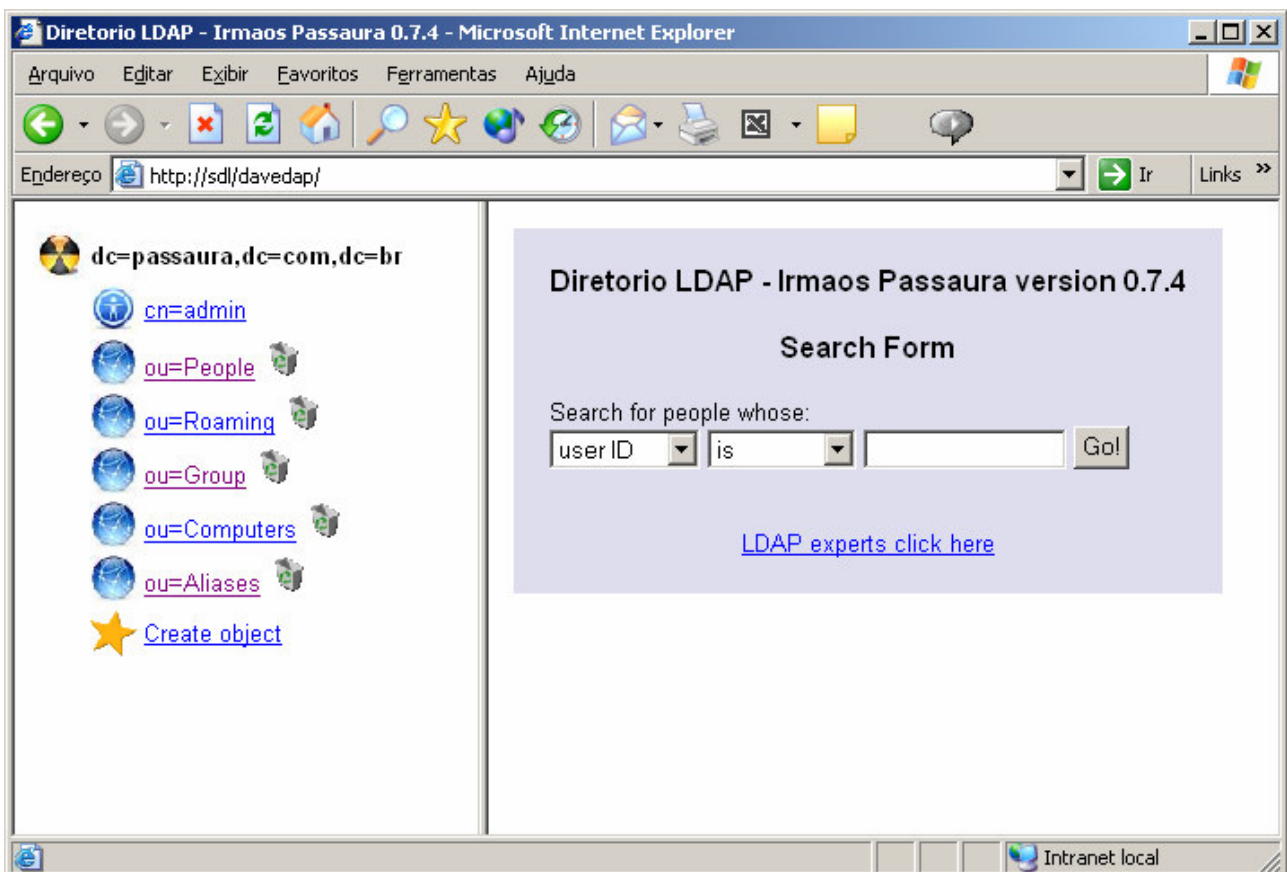
// LDAP admin login info (only fill this in if you specified 'config' for
$auth_type)
// Important: comment out these two lines if you used 'form' for your $auth_type
above
// Nome e Senha do Administrador
$admin_dn = "cn=admin,dc=passaura,dc=com,dc=br";
$admin_pw = "NOSSA_SENHA";

// Do you want to allow users to edit fields (ie, draw the Update! button)
$read_only = false;

// What name do you want to use as the name for this application?
// Nome do titulo do site
$appname = "Diretorio LDAP - Irmaos Passaura";

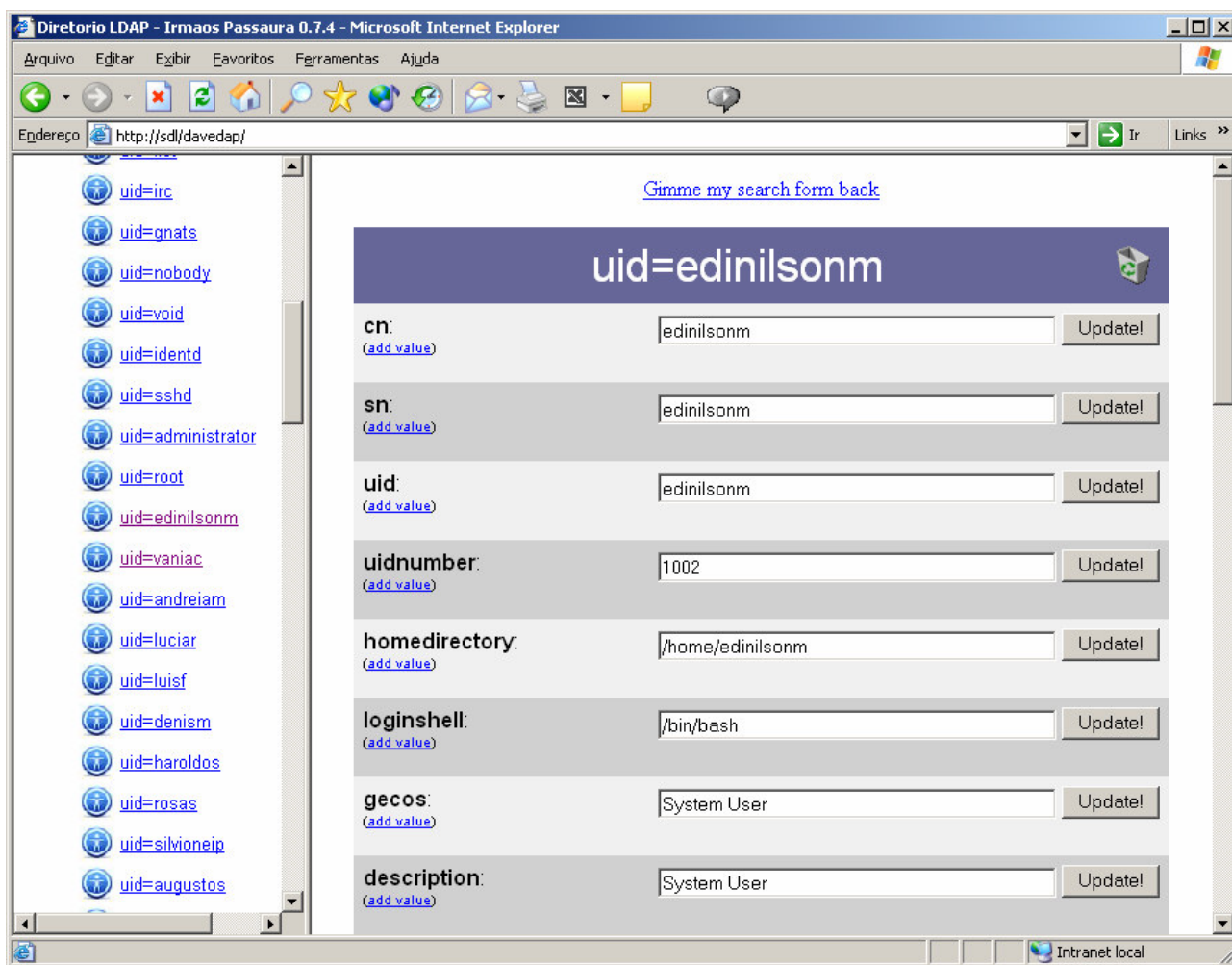
?>
```

Acessando <http://localhost/davedap/> teremos diretório LDAP, podendo fazer qualquer tipo de alteração, adicionar usuários, unix, samba, grupos etc.

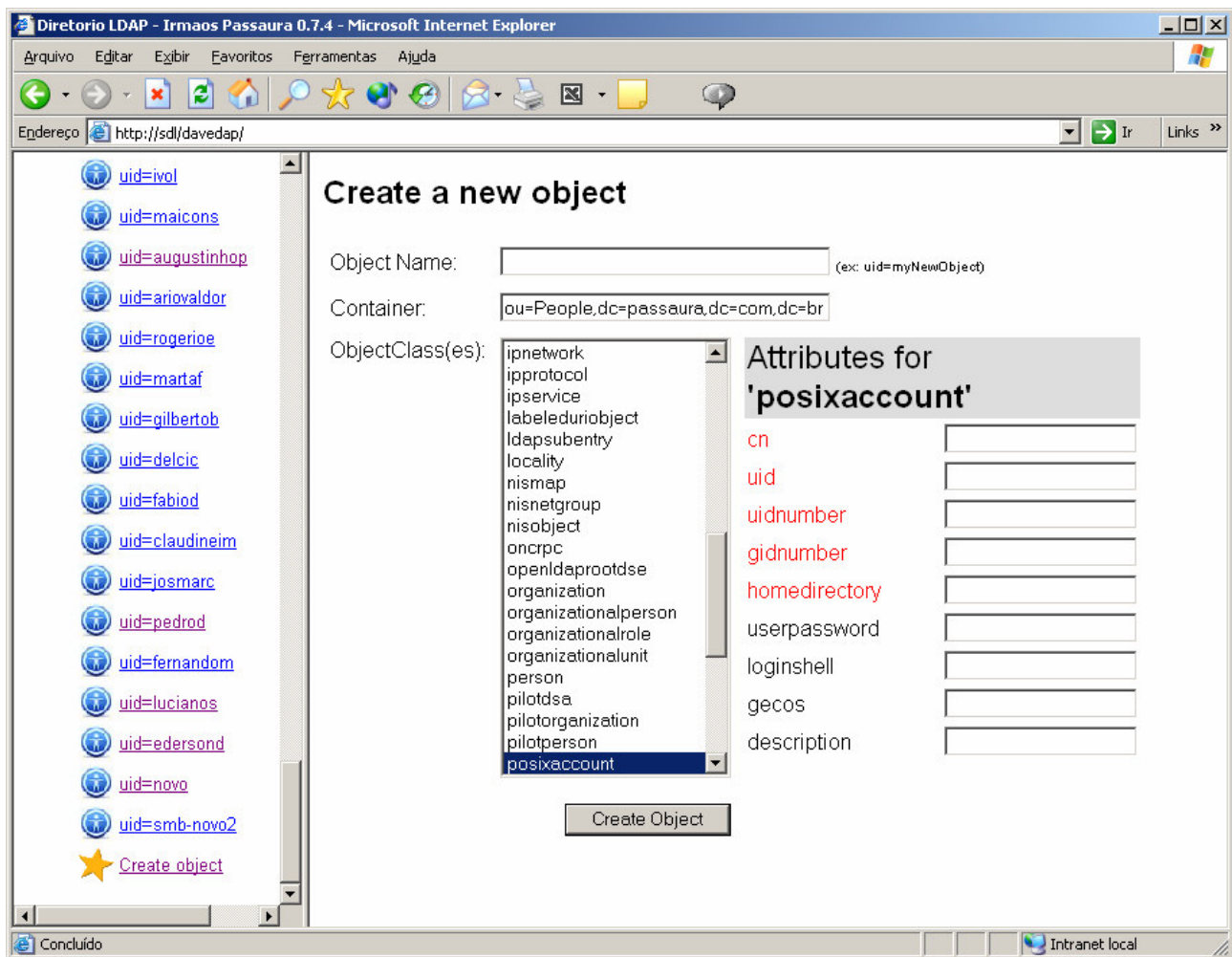


Interface do sistema web, davedap gerenciando o diretório ldap

Relatório do Projeto
Integração de Rede LINUX e Windows com Samba e LDAP



Interface do davedap alterando registro de usuários



interface do davedap criando novos registro e gerenciando objetos no diretório

• **Criando script PHP para adicionar usuários**

Com esse script php fica fácil criar os usuários para o padrão unix, devemos ter em mãos um uid e gid para atribuir ao usuário. Criamos os arquivos/scripts dentro de um diretório do servidor web, (ex.: /var/www/ldap).

```
##### /var/www/ldap/index.html#####  
<html>  
<form name="criauser" action="ldapaddusr.php" method="post">  
<br> "Informe o Nome completo do Usuário"</br>  
<input type="text" name="usuario" size="50" maxlenght="60">  
<br>"Informe o login"</br>  
<input type="text" name="login" size="16" maxlenght="60">  
<br> "Informe a senha" </br>  
<input type="password" name="senha" size="16" maxlenght="60">  
<br> "Informe o UID" </br>  
<input type="text" name="uid" size="16" maxlenght="60">  
<br> "Informe o GID" </br>  
<input type="text" name="gid" size="16" maxlenght="60">  
<br>  
<input type="submit" name="enviar" value="enviar">  
</br>  
</form>  
</html>
```

```
##### /var/www/ldap/ldapaddusr.php #####

<?php
// Agradecimentos do void, Sr. André Santos email: void@onda.com.br
//Encripta a senha
$senhacripto = crypt($senha);

$ds=ldap_connect("127.0.0.1") // Define o host onde está o servidor LDAP
    or die ("Não foi possível conectar ao servidor LDAP");

if ($ds) {
    // Acessa o dn apropriado para obter permissões de escrita na base
    $r=ldap_bind($ds,"cn=admin,dc=passaura,dc=com,dc=br", "NOSSA_SENHA")
        or die ("Autenticação no Servidor LDAP falhou");

    // Prepara os dados em um array

    //Array para objectClass posixAccount
    $posix["uid"]="$login";
    $posix["cn"]="$login";
    $posix["userPassword"]="{CRYPT}$senhacripto";
    $posix["loginShell"]="/bin/bash";
    $posix["uidNumber"]="$uid";
    $posix["gidNumber"]="$gid";
    $posix["gecos"]="$usuario";
    $posix["homeDirectory"]="/home/$login/";
    $posix["objectClass"]="posixAccount";

    //Array para objectClass shadowAccount
    $shadow["shadowLastChange"]="11953";
    $shadow["shadowMax"]="99999";
    $shadow["shadowWarning"]="7";
    $shadow["objectClass"]="shadowAccount";

    // Array para objectClass account
    $account["objectClass"]="account";

    //Array para objectClass top
    $top["objectClass"]="top";

    // Adiciona os dados ao diretório (posix)
    $p=ldap_add($ds, "uid=$login,ou=People,dc=passaura,dc=com,dc=br", $posix);

    if ($p) {
        printf("<br>Usuário Adicionado com sucesso em posixAccount");
    }

    if (!$p) {
        printf("LDAP-Errno: %s<br>\n", ldap_errno($ds));
        printf("LDAP-Error: %s<br>\n", ldap_error($ds));
        die("Argh!<br>\n");
    }

    // Adiciona os dados ao diretório (shadow)
    $s=ldap_mod_add($ds, "uid=$login,ou=People,dc=passaura,dc=com,dc=br",
    $shadow);
}
```

```
if ($s) {
    printf("<br>Usuário Adicionado com sucesso em shadowAccount");
}

if (!$s) {
    printf("LDAP-Errno: %s<br>\n", ldap_errno($ds));
    printf("LDAP-Error: %s<br>\n", ldap_error($ds));
    die("Argh!<br>\n");
}

// Adiciona os dados ao diretório (account)
$a=ldap_mod_add($ds, "uid=$login,ou=People,dc=passaura,dc=com,dc=br",
$aaccount);

if ($a) {
    printf("<br>Usuário Adicionado com sucesso em account");
}

if (!$a) {
    printf("LDAP-Errno: %s<br>\n", ldap_errno($ds));
    printf("LDAP-Error: %s<br>\n", ldap_error($ds));
    die("Argh!<br>\n");
}

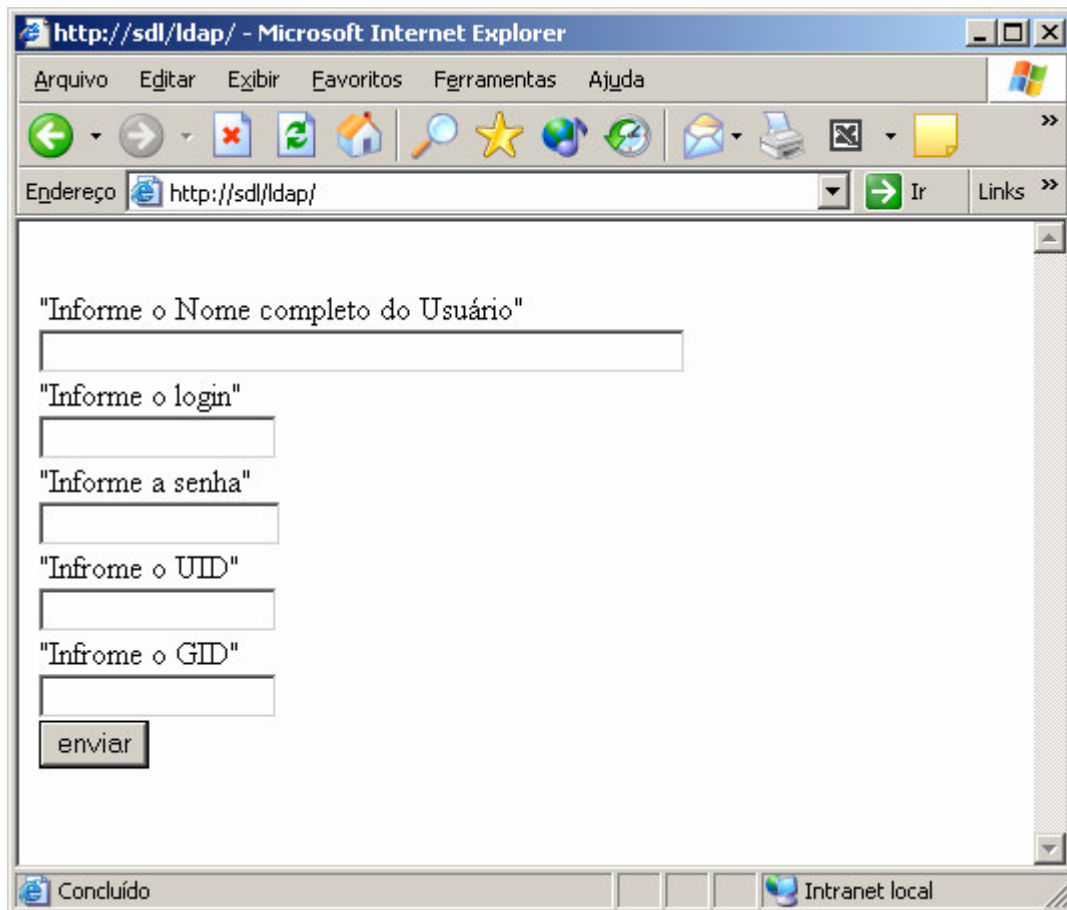
//Adiciona os dados ao diretório (top)
$t=ldap_mod_add($ds, "uid=$login,ou=People,dc=passaura,dc=com,dc=br", $top);

if ($t) {
    printf("<br>Usuário Adicionado com sucesso em top");
}

if (!$t) {
    printf("LDAP-Errno: %s<br>\n", ldap_errno($ds));
    printf("LDAP-Error: %s<br>\n", ldap_error($ds));
    die("Argh!<br>\n");
}

ldap_close($ds);

} else {
    echo "Não foi possível conectar ao servidor LDAP";
}
?>
#####
```



Esse script não ira criar o diretório home do usuário, podem automatiza muito o trabalho para adicionar usuários, para ver a nova entrada acessamos o DAVEDAP em People veremos as características do novo usuário.

- **Configurando autenticação com o LDAP**

Apos conferir e adicionar os usuários, já podemos configurar o novo servidor para que a autenticação de usuários seja feita pelo ldap.

Instalando os pacotes necessários:

```
apt-get install libnss-ldap  
apt-get install libpam-ldap
```

Edição de arquivos

```
#####/etc/ldap/ldap.conf #####  
# $OpenLDAP: pkg/ldap/libraries/libldap/ldap.conf,v 1.4.8.6 2000/09/05 17:54:38  
kurt Exp $  
#  
# LDAP Defaults  
#  
# See ldap.conf(5) for details  
# This file should be world readable but not world writable.  
#### local do servido  
host localhost
```

```
#### base principal do LDAP
base dc=passaura,dc=com,dc=br
#### User que sera padrão nas pesquisas
binddn cn=admin,dc=passaura,dc=com,dc=br
#### Senha padrao para fazer as pesquisas
bindpw NOSSA_SENHA
#### Senha utilizando o MD5
pam_password md5
#### Define um filtro para as pesquisa
pam_filter objectclass=accout
#### Forca os usuarios a utilizar um determinado grupo
pam_groupdn cn=users,ou=Group,dc=passaura,dc=com,dc=br
#### Habilita o SSL
ssl yes
```

```
##### /etc/nsswith.conf #####
# /etc/nsswitch.conf
#
# Example configuration of GNU Name Service Switch functionality.
# If you have the `glibc-doc' and `info' packages installed, try:
# `info libc "Name Service Switch"' for information about this file.

##### Como padrão esse arquivo ira procurar os usuarios nos arquivos do
sistema. Vamos adicionar o parametro ldap no fim da chamada do passwd, group,
shadow, para que o sistema procure os usuarios esses arquivos e tambem no
diretorio do ldap.

passwd:          compat ldap
group:           compat ldap
shadow:          compat ldap

##### Os outros parametro continuar inalterados
```

```
##### /etc/pam.d/login #####
#%PAM-1.0 PARA AUTENTICAR PELO LDAP
auth sufficient /lib/security/pam_ldap.so use_first_pass
account sufficient /lib/security/pam_ldap.so

### Caso ldap pare de funcionar voce poderá logar no sistema como root
normalmente, essa alteração faz com que o sistema autentique os usuarios
localmente, e caso consiga fazer isso ira "pegar" os usuarios do ldap
```

```
##### /etc/pam.d/passwd #####  
password sufficient /lib/security/pam_ldap.so  
##### Com essa alteracao, sera possivel trocar a senha o ldap pelo comando  
passwd  
#####
```

Para testar as configurações de autenticação

```
getent passwd  
getent group
```

Deve retornar os usuários e grupos que estão no diretório, após a resposta positiva, podemos logar no sistema, para testar pegamos outro console e logamos com o usuário e senha do do usuários de adicionamos no diretório LDAP.

• Configuração do Samba 3.0 Alpha.

Baixamos os fonte do samba 3.0 do site do www.samba.org e compilamos conforme abaixo.

```
tar -xzvf samba-3.0alpha21.tar.gz  
cd samba-3.0alpha21/source  
./configure --prefix=/usr/local/samba-alpha-ldap --with-ldap --with-ldapsam --  
with-tdbsam --with-syslog --with-quotas --with-acl-support --with-winbind
```

Caso tenha duvidas sobre essas opções use o:

```
./configure --help
```

Agora terminamos a compilação e instalação com o comando:

```
make  
make install
```

Copiamos o arquivo de configuração do samba que esta no samba-3.0alpha21/examples/smb.conf.default para o /usr/local/samba-alpha-ldap/lib/smb.conf

```
cp samba-3.0alpha21/examples/smb.conf.default /usr/local/samba-alpha-  
ldap/lib/smb.conf
```

Foi criado um link para facilitar o serviço de configuração.

```
ln -s /usr/local/samba-alpha-ldap/ /etc/samba
```



```
cd /etc/samba
ls -laF
total 44k
drwxr-sr-x    11 root      staff      4.0k Feb 14 13:32 ./
drwxrwsr-x    14 root      staff      4.0k Feb 19 08:01 ../
drwxr-sr-x     2 root      staff      4.0k Feb  7 15:21 bin/
drwxr-sr-x     2 root      staff      4.0k Feb 24 13:49 lib/
drwxr-sr-x     6 root      staff      4.0k Feb  7 15:17 man/
drwxr-xr-x     2 root      staff      4.0k Feb 14 13:32 ntlogon/
drwxr-sr-x     2 root      staff      4.0k Feb  7 16:36 private/
drwxr-sr-x     4 root      staff      4.0k Feb 20 14:04 profiles/
drwxr-sr-x     2 root      staff      4.0k Feb  7 15:17 sbin/
drwxr-sr-x     7 root      staff      4.0k Feb  7 15:17 swat/
drwxr-sr-x     3 root      staff      4.0k Feb 14 15:09 var/
```

Agora copiamos o schema do samba para o ldap:

```
cp samba-3.0alpha21/examples/LDAP/samba.schema /etc/ldap/schema/
```

Editar o arquivo de configuração do ldap para habilitar o schema do samba.

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

# 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 para habilitar o samba no ldap
include      /etc/ldap/schema/samba-alpha.schema
#####
```

Devemos restartar o ldap para validar a nova configuração.

• **Edição o arquivo de configuração do samba.**

```
##### /etc/samba/lib/smb.conf #####
===== Global Settings =====
[global]

# workgroup = NT-Domain-Name or Workgroup-Name, eg: REDHAT4

# CONFIGURACAO PARA O SAMBA LDAP
# DOMINIO PADRAO DA REDE
workgroup = IP

# server string is the equivalent of the NT Description field
# CONFIGURACAO PARA O SAMBA LDAP
# COMENTARIO DO SERVIDOR
server string = SAMBA ALPHA 3

# CONFIGURACAO PARA O SAMBA LDAP
# SCRIPT PADRAO PARA ALTERAR AS SENHAS DO SAMBA NO LDAP
passwd program = /usr/local/sbin/smbldap-passwd.pl -o %u
passwd chat = *new*password* %n\n *new*password* %n\n *successfully*
unix password sync = Yes
```

```
# CONFIGURACAO PARA O SAMBA LDAP
# CONFIGURACAO PARA O SAMBA AUTENTICAR SEUS USUARIOS NO DIRETORIO LDAP
# SUFFIX=RAIZ DO DIRETORIO, ADMIN=USUARIO ADMINISTRADOR DO LDAP,
# FILTER=FILTRO PADRAO PARA USUARIOS, PORT=PORTA PADRAO DO SERVIDOR,
# SERVER=IP DO SERVIDOR, SSL=NO PARA NAO USAR SSL NA SENHA
    ldap suffix = "dc=passaura,dc=com,dc=br"
    ldap admin dn = "cn=admin,dc=passaura,dc=com,dc=br"
    ldap filter = "(&(uid=%u)(objectclass=sambaAccount))"
    ldap port = 389
    ldap server = 127.0.0.1
    ldap ssl = no

# CONFIGURACAO PARA O SAMBA LDAP
# SCRIPT PARA INSERIR OS USUARIOS DO SAMBA NO LDAP
    add user script = /usr/local/sbin/smbldap-useradd.pl -w %u

# CONFIGURACAO PARA O SAMBA LDAP
# GRUPO DO ADMINISTRADOR
    domain admin group = @root

# CONFIGURACAO PARA O SAMBA LDAP
# USUARIO ADMINISTRADOR
    admin users = @root

# ALTERADO PARA O SAMBA LDAP
# ARQUIVO DE LOGS DOS USUARIOS - Devemos criar esse diretorio
    log file = /var/log/samba-alpha-ldap/log.%m

# Put a capping on the size of the log files (in Kb).
# ALTERADO PARA O SAMBA LDAP
# TAMANHO MAXIMO DOS LOGS DOS USUARIOS
    max log size = 50

# Security mode. Most people will want user level security. See
# security_level.txt for details.
# ALTERADO PARA O SAMBA LDAP
# AUTENTICACAO POR USUARIO NO SAMBA
    security = user

# You may wish to use password encryption. Please read
# ENCRYPTION.txt, Win95.txt and WinNT.txt in the Samba documentation.
# Do not enable this option unless you have read those documents
# ALTERADO PARA O SAMBA LDAP
# PARA RECEBER SENHAS ENCRYPTADAS
    encrypt passwords = yes

# OS Level determines the precedence of this server in master browser
# elections. The default value should be reasonable
# ALTERADO PARA O SAMBA LDAP
# ORDEM DE NIVEL DO PDC DA REDE
    os level = 80

# Domain Master specifies Samba to be the Domain Master Browser. This
# allows Samba to collate browse lists between subnets. Don't use this
# if you already have a Windows NT domain controller doing this job
# ALTERADO PARA O SAMBA LDAP
# INDICA SE SERA O DOMINIO MASTER PARA A REDE
    domain master = yes

# Enable this if you want Samba to be a domain logon server for
```

```
# Windows95 workstations.
# ALTERADO PARA O SAMBA LDAP
# PARA RECEBER OS LOGON DOS CLIENTES
    domain logons = yes

# Windows Internet Name Serving Support Section:
# WINS Support - Tells the NMBD component of Samba to enable it's WINS Server
# ALTERADO PARA O SAMBA LDAP
# HABILITA O WINS PARA O SERVIDOR SAMBA
    wins support = yes

#===== Share Definitions =====
# CONFIGURACAO PARA O DIRETORIO HOME O USUARIO
[homes]
    comment = Home Directories
    browseable = no
    writable = yes

# Un-comment the following and create the netlogon directory for Domain Logons

# CONFIGURACAO PARA O COMPARTILHAMENTO DO NETLOGON
[netlogon]
    comment = Network Logon Service
    path = /usr/local/samba-alpha-ldap/profiles/netlogon
    guest ok = yes
    writable = no
    share modes = no
    root preexec = /usr/local/samba-alpha-ldap/profiles/netlogon/login.pl %U
    root postexec = /usr/local/samba-alpha-ldap/profiles/netlogon/logout.pl %U

# CONFIGURACAO PARA O COMPARTILHAMENTO PADRAO O G:
[dados]
    comment = Directorio de dados
    path = /dados
    public = yes
    writable = yes
    printable = no
    create mask = 0765
# CONFIGURACAO PARA O COMPARTILHAMENTO PADRAO O X: DO SETOR DE RH
[bdf]
    comment = Directorio de dados
    path = /dados/bdf
    public = yes
    writable = yes
    printable = no
    create mask = 0765
#####
```

- ***Instalando e configurando o smbldap-tools para administração de usuários no LDAP.***

O smbldap-tools são scripts perl para fazer a administração dos usuários com acesso a samba via ldap, em resumo esses scripts perl criam as contas unix no ldap já com o objeto SambaAccount para o usuário ter acesso ao samba.

Baixamos o smbldap-tools do <http://samba.idealx.org/dist/smbldap-tools-0.7.tgz> ou acessamos o site <http://samba.idealx.org/>

Descompactamos o arquivo do smbldap-tools no diretório /usr/local/sbin

```
Cd /usr/local/sbin
tar -xzf smbldap-tools-0.7.tgz
ls -laF
total 184k
drwxrwsr-x    2 root    staff    4.0k Feb 17 15:07 ./
drwxrwsr-x   14 root    staff    4.0k Feb 19 08:01 ../
-rwxr-xr-x    1 root    staff    2.4k Feb  6 14:12 smbldap-groupadd.pl*
-rwxr-xr-x    1 root    staff    2.4k Feb  6 14:12 smbldap-groupdel.pl*
-rwxr-xr-x    1 root    staff    5.3k Feb  6 14:12 smbldap-groupmod.pl*
-rwxr-xr-x    1 root    staff    1.8k Feb  6 14:12 smbldap-groupshow.pl*
-rwxr-xr-x    1 root    staff    6.8k Feb  6 14:12 smbldap-migrate-
accounts.pl*
-rw-r--r--    1 root    staff    4.8k Feb  6 14:12 smbldap-migrate-
groups.pl
-rwxr-xr-x    1 root    staff    4.9k Feb  6 14:12 smbldap-passwd.pl*
-rwxr-xr-x    1 root    staff    7.1k Feb  6 14:12 smbldap-populate.pl*
-rwxr-xr-x    1 root    staff    13k Feb 11 11:49 smbldap-useradd.pl*
-rwxr-xr-x    1 root    staff    2.9k Feb  6 14:12 smbldap-userdel.pl*
-rwxr-xr-x    1 root    staff    10k Feb  6 14:12 smbldap-usermod.pl*
-rwxr-xr-x    1 root    staff    1.8k Feb  6 14:12 smbldap-usershow.pl*
-rw-r--r--    1 root    staff    6.9k Feb 11 11:51 smbldap_conf.pm
-rwxr-xr-x    1 root    staff    11k Feb  6 14:12 smbldap_tools.pm*
```

Esse script deve estar no diretório /usr/local/sbin somente nesse diretório ao executar, execute sempre dentro de path.

OBS.: Verificamos os módulos do perl antes de prosseguir com a configuração.

Configurando o smbldap_conf.pm

```
##### /usr/local/sbin/smbldap_conf.pm #####
#####
#
# General Configuration
#
#####

#
# UID and GID starting at...
#
# Numero do UID para inicio da criacao dos usuarios
$UID_START = 1000;

# Numero do GID para inicio da criacao dos grupos
$GID_START = 1000;

#####
#
# LDAP Configuration
#
#####

# Notes: to use to dual ldap servers backend for Samba, you must patch
# Samba with the dual-head patch from IDEALX. If not using this patch
# just use the same server for slaveLDAP and masterLDAP.
#
# Slave LDAP : needed for read operations
```

```
#
# Ex: $slaveLDAP = "127.0.0.1";
# Endereco do servidor LDAP SLAVE
$slaveLDAP = "127.0.0.1";

#
# Master LDAP : needed for write operations
#
# Ex: $masterLDAP = "127.0.0.1";
# Endereco do servidor LDAP master
$masterLDAP = "127.0.0.1";

#
# LDAP Suffix
#
# Ex: $suffix = "dc=IDEALX,dc=ORG";
# Suffixo do diretorio raiz do LDAP
$suffix = "dc=passaura,dc=com,dc=br";

#
# Where are stored Users
#
# Ex: $usersdn = "ou=Users,$suffix"; for ou=Users,dc=IDEALX,dc=ORG
$usersou = "People";

# OU onde estao os usuarios do LDAP
$usersdn = "ou=People,$suffix";

#
# Where are stored Computers
#
# Ex: $computersdn = "ou=Computers,$suffix"; for ou=Computers,dc=IDEALX,dc=ORG
$computersou = "Computers";

# OU onde serao criados os computadores da rede
$computersdn = "ou=Computers,$suffix";

#
# Where are stored Groups
#
# Ex $groupsdn = "ou=Groups,$suffix"; for ou=Groups,dc=IDEALX,dc=ORG
$groupsou = "Group";
# OU padrao para os grupos no LDAP
$groupsdn = "ou=Group,$suffix";

#
# Default scope Used
#
$scope = "sub";

#
# Credential Configuration
#
# Bind DN used
# Ex: $binddn = "cn=Manager,$suffix"; for cn=Manager,dc=IDEALX,dc=org
# Usuario administrador do LDAP
$binddn = "cn=admin,$suffix";
#
# Bind DN passwd used
# # Ex: $bindpasswd = 'secret'; for 'secret'
# Senha para o administrador do LDAP
```

```
$bindpasswd = "NOSSA_SENHA";

#
# Notes: if using dual ldap patch, you can specify to different configuration
# By default, we will use the same DN (so it will work for standard Samba
# release)
#
$slaveDN = $binddn;
$slavePw = $bindpasswd;
$masterDN = $binddn;
$masterPw = $bindpasswd;

#####
#
# Unix Accounts Configuration
#
#####

# Login defs
#
# Default Login Shell
#
# Ex: $_userLoginShell = q(/bin/bash);
# Shell padrao para o usuario
$_userLoginShell = q(/bin/bash);

#
# Home directory prefix (without username)
#
#Ex: $_userHomePrefix = q(/home/);
# Onde sera criado o diretorio home dos usuarios
$_userHomePrefix = q(/home/);

#
# Gecos
#
$_userGecos = q(System User);

#
# Default User (POSIX and Samba) GID
#
$_defaultUserGid = 100;

#
# Default Computer (Samba) GID
#
$_defaultComputerGid = 553;

#
# Skel dir
#
$_skeletonDir = q(/etc/skel);

#####
#
# SAMBA Configuration
#
#####

#
```

```
# The UNC path to home drives location without the username last extension
# (will be dynamically prepended)
# Ex: q(\\My-PDC-netbios-name\homes) for \\My-PDC-netbios-name\homes
# Endereco do diretorio home das manquinas Windows
$_userSmbHome = q(\\SDL\homes);

#
# The UNC path to profiles locations without the username last extension
# (will be dynamically prepended)
# Ex: q(\\My-PDC-netbios-name\profiles) for \\My-PDC-netbios-name\profiles
# Endereco do arquivo de configuracao
$_userProfile = q(\\SDL\netlogon\CONFIG.POL);

#
# The default Home Drive Letter mapping
# (will be automatically mapped at logon time if home directory exist)
# Ex: q(U:) for U:
# Endereco do drive padrao do usuario
$_userHomeDrive = q(U:);

#
# The default user netlogon script name
# if not used, will be automatically username.cmd
#
# Nome do script de login do usuario
#$_userScript = q(username.bat); # make sure script file is edited under dos

#####
#
# SmbLDAP-TOOLS Configuration (default are ok for a RedHat)
#
#####

# Allows not to use smbpasswd (if $with_smbpasswd == 0 in smbldap_conf.pm) but
# prefer mkntpwd... most of the time, it's a wise choice :-)
$with_smbpasswd = 0;
#### Caminho do programa para criar as senha smb
$smbpasswd = "/usr/bin/smbpasswd";

#### Caminho do programa para criar as senha NT
$mkntpwd = "/usr/local/sbin/mkntpwd";

#####
```

Agora com smbldap-tools configurado temos que compilar o mkntpwd que e muito simples, abaixo o arquivo mkntpwd.tar.gz.

• **Instalando o mkntpwd**

```
tar -xzf mkntpwd.tar.gz
Acesse o diretorio
make
```

Copie o mkntpwd que foi gerado para /usr/local/sbin , esse é o binário utilizado pelo smbldap-tools.

• ***Iniciando o samba***

Com nosso arquivo de configuração do samba já esta ok, sendo assim temos que gerar a senha para o samba conseguir se comunicar com o LDAP.

```
smbpasswd -w <senha>
```

Onde <senha> e a senha do administrador do LDAP, a senha será gerada em um arquivo /etc/samba/private/secrets.tdb

Depois devemos gerar a senha do root para ter acesso ao samba.

```
smbpasswd root
```

OBS.: Nunca esquecer que LDAP deve estar com o schema do samba para disponibilizar o ObjectClass SambaAccount.

Características do /etc/samba padrão da instalação do SAMBA 3.0

Em /etc/samba (nosso link para /usr/local/samba-alpha-ldap) estão todos os arquivos de configuração e binários do samba.

/etc/samba	
bin/	- Binários os sistema, utilitários etc
lib/	- Bibliotecas
man/	- Manuais
private/	- Diretorio onde estará a senha do adm do LDAP
profiles/	- Diretorio de profiles e netlogon
sbin/	- Binários dos DAEMONS
swat/	- Binário do swat
var/	- Diretorio padrão para logs

• ***Iniciando o Daemon do Samba***

Acesse o diretorio sbin do diretório.

```
pwd  
/etc/samba/sbin/  
./smbd &  
./nmbd &
```

Sempre verifique as mensagens do samba no syslog.

- **Script para iniciar o samba**

```
##### /etc/init.d/samba #####
#!/bin/sh
#
# samba
#
# This is from a Solaris box.  Proper links need to be made to it from the
# rcX.d directories.  For Linux, it goes into /etc/rc.d/init.d
#
# Lonnie

SAMBA=/usr/local/samba-alpha-ldap

case "$1" in
'start')
    echo "SMB Service starting."
    PATH="/usr/bin:/sbin:/usr/sbin:/usr/local/samba-alpha-ldap/sbin"
    export PATH
    ${SAMBA}/sbin/smbd -D
    ${SAMBA}/sbin/nmbd -D
    ;;
'restart')
    $0 stop
    $0 start
    ;;
'stop')
    echo "SMB Service stopping."
    for file in ${SAMBA}/var/locks/*.pid
    do
        if [ -r $file ]
        then
            kill `cat $file`
            rm $file
        fi
    done
    ;;
*)
    echo "Usage: /etc/init.d/samba { start | stop | restart }"
    ;;
esac
exit 0
#####
```

- **Administrando usuários samba e maquinas na rede**

Usando o smbldap-tools poderemos
Adicionar / remover / alterar
usuários
grupos
maquinas

```
cd /usr/local/sbin/
```

Adicionando usuários com acesso ao samba.

```
./smbldap-useradd.pl -a -m -c "Nome Completo" testel
```

Adicionando maquinas para acesso ao samba

```
./smbldap-useradd.pl -w novo-do-pc$
```

Dessa forma poderemos ingressar um Windows 2000 e XP domínio samba, colocamos sempre o nome do computador no samba e adicionamos o usuário normalmente.

Criando a senha para o usuário.

```
./smbldap-passwd.pl testel
```

• Criando o sistema de netlogon

Criamos o diretorio para dos scripts de netlogon.

```
mkdir /etc/samba/profiles/netlogon
```

Criando scripts perl

```
##### /etc/samba/profiles/netlogon/login.pl #####
#!/usr/bin/perl

$server="SDL";

sub ingroup($)
{
    my $group=shift;
    my $result=0;
    my $lcuser=lc($ARGV[0]);

    open (FD,"</etc/group");
    while (<FD>)
    {
        my $data=$_;
        if ($data =~ /$group/)
        {
            if ($data =~ /$lcuser/)
            {
                $result=1;
                last;
            }
        }
    }
    close FD;
    return $result;
}

# Inicio do login script

open (LOGON,">/etc/samba/profiles/netlogon/.$ARGV[0].bat");

print LOGON "\@ECHO OFF\r\n";
```

```
print LOGON "NET TIME \\\\$server /SET /YES\r\n";
print LOGON "NET USE U: /HOME\r\n";
print LOGON "NET USE G: \\\\$server\\dados\r\n";
print LOGON "NET USE X: \\\\$server\\bdf\r\n";
print LOGON "\\\\$server\\dados\\pdf\\avg.bat\r\n";
print LOGON "\\\\$server\\NETLOGON\\.logon.bat\r\n";
close LOGON;
#####
```

```
##### /etc/samba/profiles/netlogon/logout.pl #####
#!/usr/bin/perl
system("rm -rf /etc/samba/profiles/netlogon/.$ARGV[0].bat");
#####
```

```
##### /etc/samba/profiles/netlogon/.logon.bat #####
@echo off
CLS
CLS
EXIT
#####
```

Com essa configuração ao usuário fazer o login no sistema ele irá acessar o compartilhamento netlogon, e gerar através do script perl script .bat que será interpretado pelo Windows, conforme a configuração do samba no compartilhamento do netlogon.

- ***Adicionando Windows XP no domínio samba.***

Alterando o Registro para Windows XP logar no domínio do Samba

Adicione ao registro do WinXP

```
Windows Registry Editor Version 5.00
;
; This registry key is needed for a Windows XP Client to join
; and logon to a Samba domain. Note: Samba 2.2.3a contained
; this key in a broken format which did nothing to the registry -
; however XP reported "registry key imported". If in doubt
; check the key by hand with regedit.

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Netlogon\Parameters]
"requiresignorseal"=dword:00000000
```

Após alterar o registro do Windows adicione a máquina no ldap e depois o usuário.

Adicionando usuários com acesso ao samba

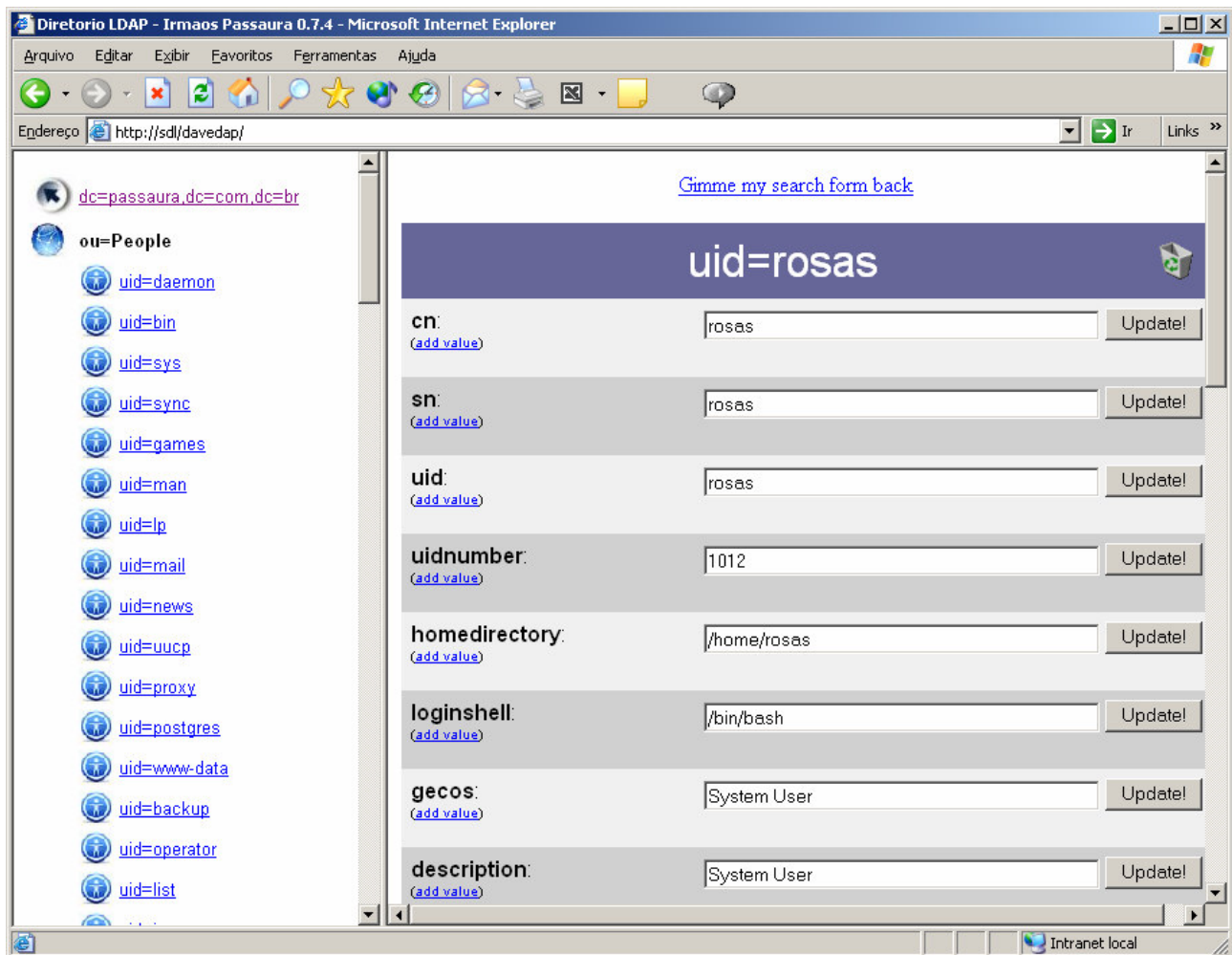
```
./smbldap-useradd.pl -a -m -c "Nome Completo" user1
```

Adicionando a maquina para acesso ao samba

```
./smbldap-useradd.pl -w nome-do-computador$
```

OBS.: Para conseguir adicionar as maquinas no ldap, teremos que inserir o objeto "OU" Computers, como já foi mostrado nesse relatório.

Depois dessas alterações poderemos logar com o WinXp no dominio Samba.



Alterando o registro do usuário no ldap

Relatório do Projeto
Integração de Rede LINUX e Windows com Samba e LDAP

Diretorio LDAP - Irmaos Passaura 0.7.4 - Microsoft Internet Explorer

Arquivo Editar Exibir Favoritos Ferramentas Ajuda

Endereço <http://sdl/davedap/> Ir Links

[Gimme my search form back](#)

dc=passaura.dc=com.dc=br

ou=Group

- [cn=root](#)
- [cn=daemon](#)
- [cn=bin](#)
- [cn=sys](#)
- [cn=adm](#)
- [cn=ttty](#)
- [cn=disk](#)
- [cn=lp](#)
- [cn=mail](#)
- [cn=news](#)
- [cn=proxy](#)
- [cn=kmem](#)
- [cn=dialout](#)
- [cn=fax](#)
- [cn=voice](#)
- [cn=cdrom](#)

cn=SPE

objectclass:

cn:

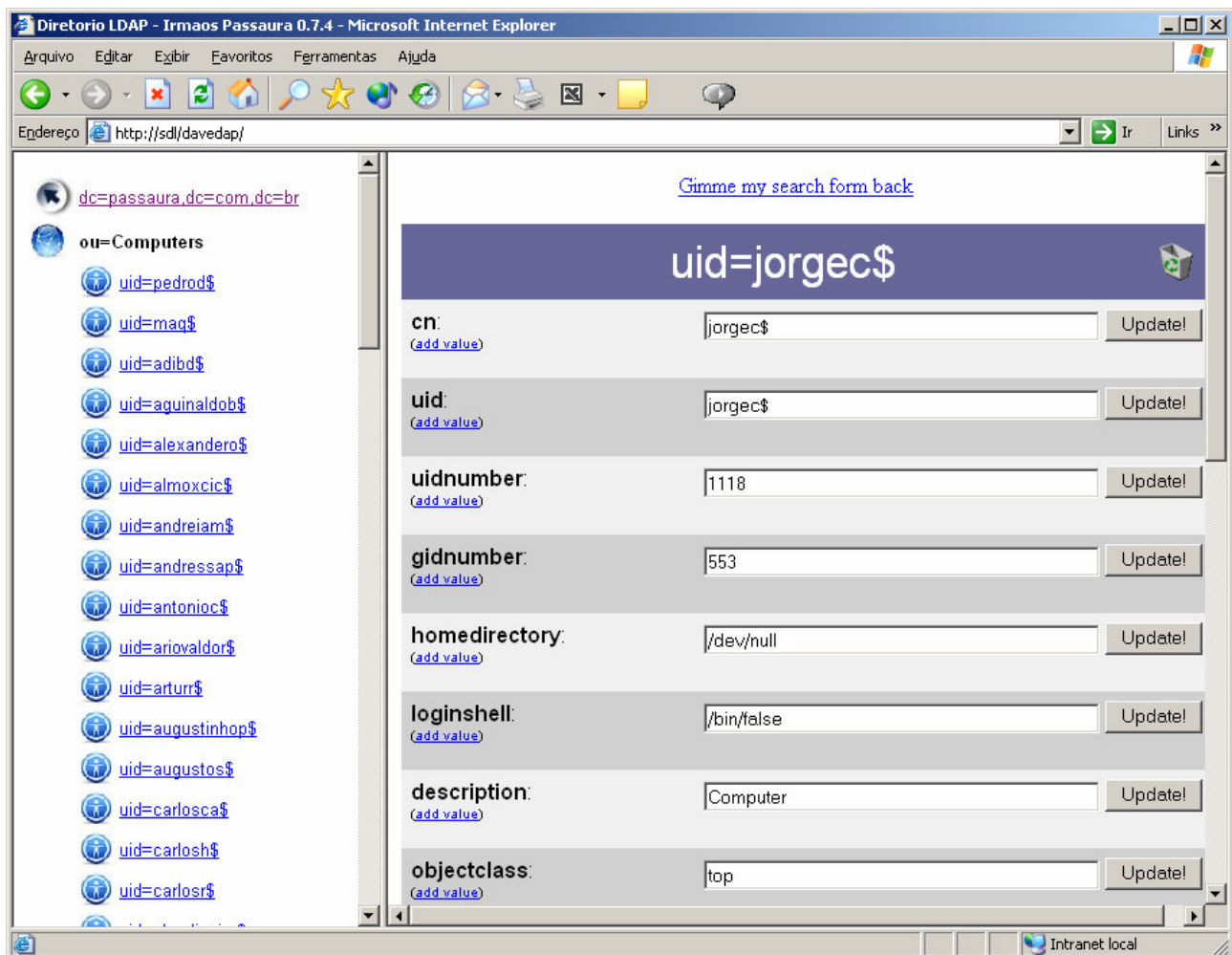
gidnumber:

memberuid:

New attribute:

Intranet local

Alterando os grupos no ldap



Alterando os registros das maquina no ldap

- **Configurando o Squid para usar o LDAP**

Para o squid autenticar no diretorio do LDAP temos que passar um parâmetro na chamada do authenticate_program. Para isso criamos um simples script para passar esses parâmetros.

```
##### /usr/lib/squid/ldap_auth.sh #####
#!/bin/sh
exec /usr/lib/squid/ldap_auth -b "ou=People,dc=passaura,dc=com,dc=br" localhost
#####
```

```
##### /etc/squid.conf #####
# TAG: authenticate_program
# Specify the command for the external authenticator. Such a
# program reads a line containing "username password" and replies
# "OK" or "ERR" in an endless loop. If you use an authenticator,
# make sure you have 1 acl of type proxy_auth. By default, the
# authenticator_program is not used.
#
# If you want to use the traditional proxy authentication,
# jump over to the ../auth_modules/NCSA directory and
# type:
#
# % make
```

```
#           % make install
#
#       Then, set this line to something like
#
#       authenticate_program /usr/bin/ncsa_auth /usr/etc/passwd
#
#Default:
# none
#   Aqui a chamada para o script que passa os parametros para o
#   ldap
#   authenticate_program /usr/lib/squid/ldap_auth.sh
#####
```

• **Conclusão**

Utilizando Software Livre, estaremos disponibilizando serviços modernos em nossa rede sem custo com compra desses softwares, assim usando tecnologias como os diretórios do LDAP, padrão para centralização de informações em rede, seja essa LINUX ou Windows, e claro poderemos ter estações de trabalho Windows e também Linux.

• **Implementações**

Estará sendo estudado a implementação para o nosso servidor de email fazer o autenticação no ldap, assim centralizando essa autenticação em uma única base ldap, para fazer isso devem entrar em fase de testes o qmail como servidor de email padrão da rede, substituindo o sendmail.

• **Referencias**

<http://www.samba.org>

<http://www.openldap.org>

<http://samba.idealx.org>

<http://www.linux.matrix.com.br>

<http://www.underlinux.com.br>

http://www.rnp.br/newsgen/0211/linux_samba_windows.shtml

<http://www.firenze.linux.it/~piccardi/ldap/>

<http://www.redhat.com/mirrors/LDP/HOWTO/LDAP-HOWTO>

- ***Versão da documentação***

Essa documentação visa atribuir ao setor de TI da Irmãos Passaura & Cia Ltda maior controle sobre as alterações e implementações feitas nos servidores da empresa, sendo que qualquer modificação e implementação será documentada com revisões e novas versões este relatório. Versão atual do documento 1.0.

Pedro Delfino dos Santo Neto
Responsável técnico do projeto
E-mail: delfino@delfino.com.br
pedrod@passaura.com.br
Fone: (41) 2141-7046