MIGRAÇÃO E INTEGRAÇÃO DE SERVIÇOS DE *E-MAIL*, AUTENTICAÇÃO DE USUÁRIOS E SERVIDOR DE DIRETÓRIOS

CARLOS VINICIUS VASCONCELOS RODRIGUES

LAVRAS
MINAS GERAIS - BRASIL
2008

CARLOS VINICIUS VASCONCELOS RODRIGUES

MIGRAÇÃO E INTEGRAÇÃO DE SERVIÇOS DE *E-MAIL*, AUTENTICAÇÃO DE USUÁRIOS E SERVIDOR DE DIRETÓRIOS

Monografia apresentada ao Departamento de Ciência da Computação da Universidade Federal de Lavras, como parte das exigências do curso de Pós-graduação Lato Sensu em "Administração em Redes Linux", para obtenção do título de especialização.

Orientador
Prof. Herlon Ayres Camargo

LAVRAS
MINAS GERAIS - BRASIL
2008

CARLOS VINICIUS VASCONCELOS RODRIGUES

MIGRAÇÃO E INTEGRAÇÃO DE SERVIÇOS DE *E-MAIL*, AUTENTICAÇÃO DE USUÁRIOS E SERVIDOR DE DIRETÓRIOS

Monografia apresentada ao Departamento de Ciência da Computação da Universidade Federal de Lavras, como parte das exigências do curso de Pós-graduação Lato Sensu em "Administração em Redes Linux", para obtenção do título de especialização.

APROVADA em ___de_____de____

Prof. _____

Prof. _____

Prof. Herlon Ayres Camargo
(Orientador)

LAVRAS
MINAS GERAIS - BRASIL
2008

Dedicatória

Dedico este trabalho aos profissionais com interesse no assunto abordado, principalmente os colegas da Embrapa.

Agradecimentos

Agradeço a Deus, que sempre me ilumina em todos os momentos.

Agradeço a minha namorada pela tolerância e compreensão, nas vezes que tive que abrir mão da convivência para me dedicar ao ARL. A minha mãe, pai e irmãs pelo apoio, incentivo e orações.

Ao colega da Embrapa Jaime Mota, que sempre me ajudou nas configurações e dúvidas de funcionamento dos serviços de rede.

Ao meu orientador, professor Herlon Camargo pela experiência e dedicação na busca pela melhor solução; aos professores do ARL e a todos que direta ou indiretamente contribuíram para realização deste trabalho.

Índice de Figuras

Índice de Tabelas

Resumo

O objetivo deste trabalho é apresentar a migração e integração de serviços de redes de computadores em sistemas operacionais *FreeBSD* e/ou *Linux* utilizando as ferramentas *OpenLDAP*, *Samba*, *Smbldap-Tools*, *Postfix*, *Courier-Imap*. É apresentada uma metodologia para instalação e configuração dos serviços de *e-mail*, autenticação de usuários e servidor de diretórios, integrando-os. Além disso, mostra alguns benefícios para os administradores de rede e para os usuários.

Sumário

1 – Introdução

Integração de sistemas de informação é o objetivo de inúmeras empresas, principalmente quando o ambiente é heterogêneo, com diferentes plataformas computacionais. A diversidade de equipamentos, sistemas operacionais, programas e sistemas traz a preocupação com o gerenciamento das informações de forma que os dados não precisem ser duplicados ou que fiquem indisponíveis ou desatualizados. Dessa forma, o uso de ferramentas de integração está cada vez mais presente nos ambientes de tecnologia de informação das empresas. Sabendo que essa integração é passo fundamental, surgem algumas dúvidas, como: o que integrar, quais ferramentas utilizar e qual metodologia será utilizada?

Outra característica de empresas de médio e grande porte que minimiza os problemas relacionados a informática é a padronização. Visando melhorar seu gerenciamento na área de redes de computadores, a Embrapa – Empresa Brasileira de Pesquisa Agropecuária, com 40 filiais (chamadas Unidades) em todo o Brasil, resolveu padronizar o uso de ferramentas para os serviços de *e-mail*, servidor de arquivos e impressoras, e principalmente o serviço de diretórios, integrando-os e oferecendo serviços adicionais a partir dessa integração.

O objetivo deste trabalho é apresentar os conceitos e passos necessários para essa integração usando os *softwares OpenLDAP*, *Samba*, *Postfix* e *Courier-Imap*. Primeiramente será mostrado o ambiente anterior, ou seja, como a empresa estava estruturada e quais as ferramentas utilizadas. Depois, como a migração pode ser feita, quais os passos necessários para integrar todas as ferramentas e finalmente, quais os resultados obtidos e as perspectivas de novas funcionalidades para os serviços de redes de computadores.

A metodologia usada neste trabalho consistiu inicialmente de levantamentos bibliográficos sobre servidores de diretórios, *e-mail* e compartilhamento de recursos. É apresentado o que o administrador de sistemas precisa para a instalação e configuração das ferramentas *Postfix*, *Courier-Imap*, *Samba*, *Smbldap-Tools* e a integração com o *OpenLDAP*. Além disso, mostra como utilizar comandos ou a ferramenta gráfica P*hpldapadmin* para gerenciar a base de dados do servidor *OpenLDAP*.

O texto é composto de 6 capítulos, assim divididos: o Capítulo 2 é uma descrição do histórico da migração. O Capítulo 3 aborda os conceitos básicos e necessários para entender cada serviço. No Capítulo 4 é mostrado o que é necessário para fazer os serviços funcionarem e conversarem entre si. O Capítulo 5 apresenta os testes e resultados obtidos com a integração. E por fim, o Capítulo 6 apresenta a conclusão.

2 – Histórico da Migração

Antes de apresentar os conceitos e funcionalidades dos serviços, esse capítulo começa com um histórico da migração, como ela foi planejada e quais os objetivos específicos.

2.1 Migração

A Embrapa Tabuleiros Costeiros[1] é uma Unidade (neste documento chamada de filial) da Empresa Brasileira de Pesquisas Agropecuárias – EMBRAPA[2] - localizada na cidade de Aracaju-SE que tem sua estrutura de tecnologia voltada para soluções integradas, seguindo as políticas do Governo Federal, principalmente baseadas no documentos [GUIA LIVRE, 2005] e [E-PING, 2007].

Cada filial da empresa é independente no que diz respeito a soluções de tecnologia, porém é fundamental manter um mínimo de padronização em serviços de rede, como por exemplo, um servidor de diretórios, o qual armazenará informações de usuários, grupos de usuários, etc.

Historicamente, a empresa mantém uma solução baseada em produtos e serviços da *Sun Microsystem*[3], daí a escolha inicial pelo seu sistema operacional *Solaris*[4] e pelo servidor de informação e autenticação *NIS*[5].

Quando esse trabalho foi iniciado, a estrutura computacional da filial

1 www.cpatc.embrapa.br
2 www.embrapa.br
3 www.sun.com
4 www.sun.com/software/solaris
5 *Networking Information Service*

tinha dois servidores com *Solaris*, versões 7 e 8, ou seja, bem desatualizados, pois a versão atual já era a 10 e *OpenSolaris*[6] (versão aberta do *Solaris*) estava em seu lançamento. Além dos servidores, haviam clientes com *Windows98* e *XP*, sem controle de autenticação, mas com acesso a algumas pastas dos servidores, que eram compartilhadas via *Samba*[7].

Com o objetivo de atualizar a estrutura computacional da filial, implantando sistemas operacionais e serviços atualizados, seguros, abertos e integrados é que o trabalho de migração foi iniciado, o qual será abordado ao longo desse texto.

Além desse objetivo inicial, havia a necessidade de implantar uma autenticação centralizada, usando o *Samba* como controlador de domínio, gerenciando os usuários com o *OpenLDAP*[8] e integrados ao novo serviço de *e-mail*, substituindo o *Sendmail*[9] pelo *Postfix*[10].

2.1.1 Planejando a migração

É importante ter um planejamento antes de qualquer migração, principalmente se o legado é extenso, ou seja, se a empresa possui diversos sistemas e bases de dados em tecnologias ultrapassadas, que precisam de migração. Além do planejamento do que fazer, também é importante elencar as possíveis alternativas, caso algo dê errado, como por exemplo retornar para a situação original a partir de *backup*. A Tabela 2.1 mostra os passos necessários para realizar a migração.

6 www.opensolaris.com
7 www.samba.org
8 www.openldap.org
9 www.sendmail.org
10 www.postfix.org

Tabela 2.1: Planejamento da migração

Nº	***Tarefas***	***Observações***
1	*Backup de todos os servidores*	*Backup em fita e em disco*
2	*Instalação e atualização do FreeBSD*	*Dois novos servidores SUN, cada um com dois processadores 64bits, 4GB de RAM, discos SCSI 160GB*
3	*Instalação do Bind*	*Configurar domínio da filial*
4	*Instalação do DHCP*	*Configurar máquinas da rede local*
5	*Instalação do Apache*	*Configurar e copiar arquivos da intranet e do site da filial*
6	*Instalação do OpenLDAP*	*Migrar usuários do NIS*
7	*Instalação do Samba e Smbldap-Tools*	*Configurar autenticação, integrar ao OpenLDAP e compartilhar pastas dos usuários*
8	*Instalação do Postfix*	*Migrar usuários de mailbox para maildir*
9	*Instalação do Courier-Imap*	*Permitir Pop3 e Imap para os usuários*
10	*Instalação bancos de dados*	*PostgresSql e Mysql*
11	*Instalar anti-vírus e filtros*	*Clamav, Procmail, configurações adicionais no Postfix*
12	*Instalar aplicativos adicionais*	*Cacic, Mrtg, Isoqlog, Squirrelmail, OpenSSH*
13	*Implantar gerenciamento de impressão*	*Cups e Pykota*
14	*Reconfigurar firewall*	*Packet filter (PF)*
15	*Teste de serviços, páginas e acesso aos sistemas*	*Testes internos e externos*
16	*Implantar VPN*	*Comunicação filial-sede*

A escolha do sistema operacional foi um dos primeiros passos dessa migração da filial, que optou pelo *FreeBSD*[11] em virtude da padronização da sede da empresa e, conseqüentemente, suporte técnico.

11 www.freebsd.org

Esse trabalho tem como objetivo explorar os itens 6, 7, 8 e 9 da Tabela 2.1 acima. Se o leitor desejar mais informações sobre outros itens pode consultar [LUCAS, 2003], um ótimo guia para configurações de sistemas e serviços em *FreeBSD* e em *Unix* de uma forma geral.

O planejamento da migração é importante não apenas para a migração em si, mas também para resolver muitas questões relacionadas à Tecnologia da Informação, como é citado em [GUIA LIVRE, 2005]. Outro fator importante na migração é a preocupação com os usuários, como bem evidenciado em [ABÍLIO, 2008]. E apesar desse documento tratar de *softwares* para servidores de redes, é mostrado no Capítulo 5 algumas vantagens para os usuários.

3 – *OpenLDAP, Samba, Smbldap-Tools, Postfix e Courier-IMAP*

Este capítulo aborda os conceitos necessários para entender as configurações dos serviços de *e-mail*, servidor de arquivos e servidor de diretórios.

3.1 O Servidor de Diretórios LDAP

Segundo [TRIGO, 2007], um diretório é algo usado para indicar direções, ou seja, algo que indica um caminho para se chegar aquilo que se procura. Ainda, define diretório como um serviço de armazenamento hierárquico de informações com o objetivo principal de facilitar a pesquisa e a recuperação dessas informações.

É nesse enfoque que os serviços de diretórios podem ser usados para diversas coisas na informática, como por exemplo: manter informações sobre autenticação de diversos servidores num só local, ou seja, sem duplicidade de informações; cadastro único de contas de usuários, grupos ou máquinas, conta de *e-mail*; etc. E para atender essas e outras demandas, foi criado o *LDAP*, que é um protocolo leve de acesso a diretórios (*Lightweight Directory Access Protocol*). A implementação mais conhecida do *LDAP* no mundo do *software* livre é o *OpenLDAP*.

O *LDAP*, que está atualmente na versão 3, foi padronizado em 1993, no *RFC*[12] *1487*. Pode ser considerado um "descendente leve" do protocolo *X.500*.

12 *Request for comment*

3.1.1 O que é necessário saber sobre Diretórios e *LDAP* para configurar o *OpenLDAP*

A melhor maneira de entender a estrutura de diretórios é saber que as informações são organizadas de forma hierárquica, semelhante a estrutura de árvore do *DNS – Domain Name System* (para saber mais sobre *DNS*, consulte [UCHÔA, 2004]). De acordo com [SUNGAILA, 2008], pode-se classificar a estrutura de um diretório em dois tipos: por localidade ou por domínio internet (dc), conforme apresentado nas Figuras 3.1 e 3.2.

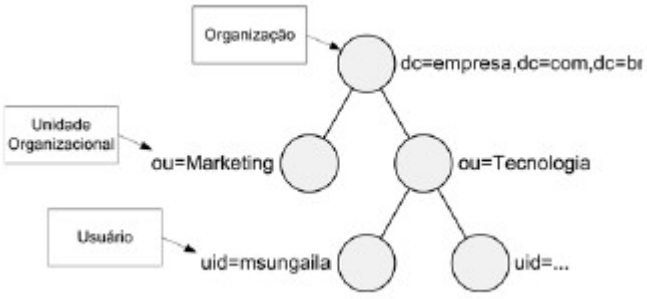

Figura 3.1: Modelo de Diretório baseado na estrutura dc

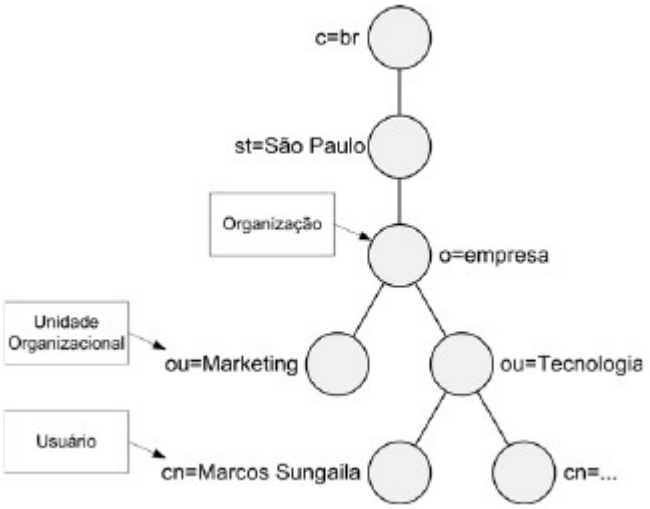

Figura 3.2: Modelo de diretório baseado na estrutura de localidade

O próximo passo para entender como implantar um serviço de diretórios é a criação de arquivos *ldif*, justamente a partir da estrutura definida anteriormente. O arquivo *ldif* é um arquivo texto contendo informações sobre a estrutura e os dados dos nós da árvore, ou seja, como o diretório será preenchido. Um exemplo com sua descrição será apresentado no Capítulo 5.

Os responsáveis por manter a estrutura do Diretório e definir sua padronização são os *schemas*, que são arquivos contendo definições de classes, tipos de dados e atributos. Por exemplo, um arquivo de *schema* de *e-mail* contém todas as definições para campos de *e-mail*, *login*, nome completo, sobrenome, quais os campos obrigatórios e opcionais, entre outros.

As listas de controle de acesso (*ACL - Access Control List*) servem para definir as permissões de acesso a base de dados. Nas *ACLs* é possível definir, por exemplo, quem tem permissões para leitura e escrita, usuários que acessam toda a base ou parte dela, usuários que podem alterar campos.

O servidor de diretórios tem uma característica que o diferencia do servidor de banco de dados que é o maior número de leituras (consultas) do que alterações em sua base. Para agilizar o processo de pesquisa na base, surgiu o conceito de índices, que nada mais são do que arquivos auxiliares que auxiliarão na busca dos resultados esperados.

O Capítulo 4 mostra o uso de todos os itens descritos aqui: *schemas*, índices e *ACLs*.

3.2 Samba e Smbldap-tools

Como visto em [BOAS, 2004] o *Samba* foi criado por Andrew Tridgell em 1992 porque precisava montar um volume *Unix* em sua máquina *DOS*. No mundo *Unix*, a opção existente para compartilhamento de arquivos era o *NFS*. O *Samba*, baseado no protocolo *SMB* (*Server Message Block)/CIFS(Common Internet File System*) é um servidor e um conjunto de ferramentas que permite que máquinas *Unix* e *Windows* compartilhem serviços entre si.

Esses serviços podem ser: compartilhamento de arquivos e impressoras, autenticação de usuários, resolução de nomes e anúncio de serviços. A maioria das funcionalidades do *Samba* é implementada por dois servidores: o *nmbd* e o *smbd*. O *nmbd* é responsável pelo anúncio de serviços e resolução de nomes. Já o *smbd* implementa compartilhamento de arquivos e impressoras, bem como autenticação e autorização [UCHÔA, 2004]. Essas funcionalidades podem ser melhor detalhadas com características como: pastas compartilhadas com acesso leitura/gravação por compartilhamento ou por usuário; suporte completo a controlador de domínio *Windows* (*Primary Domain Control - PDC*); uso de

ferramentas gráficas para configuração; autenticação criptografada através de *LDAP*, *PAM*, etc.

O *PDC* é uma máquina central (um servidor) que faz o controle das contas de usuários e permissões de acesso. É no PDC que tudo é controlado, ou seja, quais as máquinas que podem acessar o domínio, quais os usuários podem se autenticar, quais as permissões de acesso para usuários/grupos e onde as contas estão armazenadas. Sendo assim, graças ao *Samba*, clientes *Windows* podem se autenticar em servidores *Linux*, *FreeBSD*, etc.

Integrar *OpenLDAP* ao *Samba* é informar ao *Samba* onde está a base de autenticação do *OpenLDAP* e informar ao *OpenLDAP* sobre *schemas*, índices e *ACLs* do *Samba*. A vantagem dessa integração é que as mesmas senhas de autenticação para aplicações como *ssh* ou *e-mail*, também são usadas para acessar os compartilhamentos *Samba*. O Capítulo 4 detalha como acontece essa configuração.

O *Smbldap-Tools, d*esenvolvido pela empresa *IdealX*, atualmente *OpenTrust* (www.opentrust.com), é um pacote de *scripts* escritos em *Perl* que servem para gerenciar as contas de usuários, grupos e computadores armazenando as informações em bases *LDAP*.

3.3 Postfix e Courier-Imap

Segundo [TRIGO, 2007], o mecanismo que gerencia todo o fluxo da comunicação via internet entre pessoas e organizações é chamado de *MTA* (*Mail Transfer Agent* – Agente de Transferência de Correspondência). O *Postfix* é um *MTA* e utiliza o protocolo *SMTP* (*Simple Mail Transfer Protocol* – Protocolo Simples de Transferência de Correspondência), que é responsável por

armazenar, enviar e receber as mensagens de *e-mail*. Além do *MTA*, outros conceitos importantes sobre correio eletrônico são: *Mailbox*, local de armazenamento dos *e-mails* dos usuários; *MUA*, são os programas clientes, para que os usuários gerenciem seus *e-mails*; Agentes de Acesso, permitem baixar os *e-mails*, usando os protocolos *POP* ou *IMAP*.

O *Postfix* foi criado em 1998 por Wietse Venema e surgiu como uma alternativa ao *Sendmail*, que foi o servidor de *e-mail* mais usado na internet por muito tempo. Além de mais fácil de configurar, o *Postfix* também se tornou mais rápido e seguro que o *Sendmail*.

A integração ao *OpenLDAP* é de forma similar ao já descrito sobre *Samba*, ou seja, é informado ao *Postfix* onde está a base de autenticação do *OpenLDAP* e informado ao *OpenLDAP* sobre schemas e índices do *Postfix*. As explicações sobre configurações serão apesentadas no Capítulo 4.

O *Courier-Imap* é o servidor que faz o papel do agente de acesso, ou seja, possibilita acesso as mensagens tanto no formato *Mailbox*, onde as mensagens são armazenadas num único arquivo, como no formato *Maildir*, onde cada mensagem é um arquivo.

4 – Instalação e Configuração

Os passos apresentados neste documento foram executados inicialmente em servidores *FreeBSD* versão 6.3 e depois testados com *FreeBSD versão* 7. Também mostra os pacotes necessário para a instalação no *Linux* (usando a distribuição *Kubuntu*, derivada do *Debian*).

4.1 Pacotes necessários e instalação

No *FreeBSD,* a instalação de um pacote (chamado *port*) pode ser realizada através dos passos:

1. acesso ao diretório do *port* desejado, por exemplo:

```
cd /usr/ports/net/openldap23-server
2. make
3. make install
```

Caso algum *port* seja necessário, o próprio sistema de pacotes identifica a dependência e o instala automaticamente.

A Tabela 4.1 mostra os pacotes de cada serviço, suas dependências e/ou parâmetros necessários durante a instalação. Para este documento foi assumido que no *FreeBSD* o diretório que contém os pacotes para instalação é /usr/ports e no Linux, a instalação de pacotes foi feita usando o comando e gerenciador de pacotes *apt-get*.

Tabela 4.1: Pacotes necessários

Pacote	***Local***	***Opções***	***Em linux:***
openldap	*./net/openldap23-server*	*SASL, BDB, SLURPD*	*slapd, ldap-utils*
samba	*./net/samba3*	*LDAP, ADS, WINBIND, ACL_SUPPORT, UTMP, POPT*	*samba*
smbldap-tools	*./net/smbldap-tools*		*samba-doc*
postfix	*./mail/postfix*	*Make WITH_OPENLDAP_VER=23 SASL2, TLS, OPENLDAP*	*postfix*
courier-imap	*./mail/courier-imap*	*AUTH_LDAP*	*courier-imap*
nss_ldap	*./net/nss_ldap*		*libnss-ldap*
pam_ldap	*./security/pam_ldap*		*libpam-ldap*
phpldapadmin	*./net/phpldapadmin*		*phpldapadmin*
qmail-ldap	*./mail/qmail-ldap*		

O *nss_ldap* e o *pam_ldap* devem ser utilizados em todas as máquinas que necessitam fazer autenticação de usuários cadastrados em uma base *OpenLDAP*, inclusive no próprio servidor. O P*hpldapadmin* é uma ferramenta gráfica que ajuda no gerenciamento das contas. O *qmail-ldap* é usado apenas para copiar o arquivo de schema para integrar *Postfix* ao *OpenLDAP*.

Há dois passos importantes que devem ser realizados durante o processo de instalação do *Postfix*:

1. Antes da instalação do *Postfix*, parar o *Sendmail*:

```
/etc/rc.d/sendmail stop
```

2. No *make install* do *Postfix*, responder *y[yes]* para as duas perguntas que são para adicionar o usuário *postfix* ao grupo *mail* e ativar o *Sendmail* do *Postfix* em substituição do *Sendmail* padrão.

4.2 Configuração

Para os procedimentos de configuração, as definições da Tabela 4.2 foram adotadas.

Tabela 4.2: Definições de configuração

cpatc é o nome da filial (Unidade da Embrapa).
ldap.cpatc.embrapa.br é a máquina onde está instalado o servidor *OpenLDAP*
mailhost.cpatc.embrapa.br é a máquina onde está instalado o servidor de *e-mail*

4.2.1 *OpenLDAP*

Os passos necessários para a configuração do servidor *OpenLDAP* são apresentados nesta seção. O caminho para os arquivos de configuração é "/usr/local/etc/openldap". Os passos são os seguintes:

1. O comando "slappasswd" serve para criar a senha do *rootdn* (administrador) do servidor *LDAP*. É solicitado que o usuário digite uma senha e confirme. Essa senha é codificada e direcionada para o arquivo "segreto.txt", que é inserida no arquivo de configuração "slapd.conf".

```
slappasswd > /usr/local/etc/openldap/segredo.txt
```

2. Na Seção 3.1 foi explicado sobre o pacote *qmail-ldap*, que gera o esquema "qmail.schema", usado pelo *Postfix* e *Courier-Imap*. Os comandos necessários para gerar esse arquivo e copiar para o diretório de *schemas* do *OpenLDAP* são mostrados na Figura 4.1:

```
cd /usr/ports/mail/qmail-ldap
make
cd work
cp qmail-X.XX/qmail.schema /usr/local/etc/openldap/schema
make clean distclean
```

Figura 4.1: Comandos para gerar schema qmail

Onde "qmail-X.XX" deve ser substituído pelo nome do pacote, por exemplo "qmail-1.03".

3. Na Figura 4.2 são apresentados alguns parâmetros de configuração do arquivo "slapd.conf" do servidor *OpenLDAP (schemas, ACLs e índices)* e no Apêndice I, o arquivo completo, com as configurações desejadas e comentários explicativos de cada trecho do arquivo.

```
#Schemas
Include  /usr/local/etc/openldap/schema/core.schema
Include  /usr/local/etc/openldap/schema/cosine.schema
# Listas de Acesso ao Servidor (ACLs).
access to attrs=userPassword
    by anonymous auth
    by self write
    by * none
# Definição dos índices para melhorar as consultas
index  objectClass        eq
index  mail               pres,eq,sub
```

Figura 4.2: Configuração do arquivo slapd.conf

A senha criada com o comando “slappasswd” (que está no arquivo “segredo.txt”) deve ser inserida no “slapd.conf” na linha com a diretiva “rootpw**”**.

Ex.: `cat /usr/local/etc/openldap/segredo.txt`

```
rootpw      {SSHA}9XA1S9RDFGpoutiPyyxF7w/C/YjTFGT
```

4. Mudar a permissão de acesso ao arquivo de configuração “slapd.conf”:

```
chown ldap:ldap  slapd.conf
chmod 0600 slapd.conf
```

5. Criar o certificado da entidade certificadora (Apêndice V):
6. Para que seja possível ativar conexões seguras entre o servidor e os clientes *LDAP*, é necessário editar o arquivo “ldap.conf” e incluir as linhas:

```
TLS_CACERT /usr/local/etc/openldap/ssl/cacert.pem
HOST ldap.cpatc.embrapa.br
```

Esse exemplo serve para clientes que estão instalados no mesmo computador que o servidor. Caso o cliente esteja em outro computador, deve-se copiar o arquivo “cacert.pem” do servidor para o cliente e incluir as duas linhas de configuração descritas acima, onde “TLS_CACERT” indica o local do arquivo “cacert.pem” e “HOST” indica a máquina onde está o servidor *OpenLDAP*.

Os passos 7, 8 e 9 abaixo são para configuração e rotação do arquivo de *log* (arquivo que guarda mensagens de erros, avisos e problemas do servidor). E o passo 10 diz ao *FreeBSD* para iniciar o processo do servidor *OpenLDAP* na inicialização do sistema.

7. Editar o arquivo “/etc/syslog.conf” e incluir a linha:

```
local4.*  /var/log/ldap.log
```

8. Editar o arquivo “/etc/newsyslog.conf” e incluir a linha:

```
/var/log/ldap.log       644   5     100   *     J
```

9. Criar o arquivo “/var/log/ldap.log” e reiniciar o serviço “syslogd”, através dos comandos:

```
touch /var/log/ldap.log
killall -HUP syslogd
```

10. Editar o arquivo “/etc/rc.conf” e incluir as linhas conforme Figura 4.3:

```
slapd_enable="YES"
slapd_flags='-h "ldapi://%2fvar%2frun%2fopenldap
%2fldapi/ ldap://0.0.0.0/"'
slapd_sockets="/var/run/openldap/ldapi"
```

Figura 4.3: Opções de inicialização do OpenLDAP

Desta forma, a próxima vez que o computador reiniciar, o servidor *OpenLDAP* é carregado automaticamente. Para que o serviço seja executado imediatamente, após a inclusão das instruções no arquivo “rc.conf”, deve-se digitar o comando:

```
/usr/local/etc/rc.d/slapd start
```

4.2.2 *Samba* e *Smbldap-Tools*

Os passos necessários para a configuração do servidor *Samba* são apresentados nesta seção. O caminho para os arquivos de configuração é "/usr/local/etc". Os passos são os seguintes:

1. Copiar o *schema* do *Samba* para o diretório do *OpenLDAP*:

```
cd /usr/local/etc/openldap/schema
cp /usr/local/share/examples/samba/LDAP/samba.schema
```

2. Incluir as linhas no arquivo "openldap/slapd.conf" conforme Figura 4.4:

```
include /usr/local/etc/openldap/schema/samba.schema
index   sn                          pres,eq,sub
index   displayName                 pres,eq,sub
index   sambaSID                    eq
index   sambaPrimaryGroupSID        eq
index   sambaDomainName             eq
index   default                     sub
```

Figura 4.4: Integração Samba ao OpenLDAP

3. Reiniciar o *OpenLDAP*:

```
/usr/local/etc/rc.d/slapd restart
```

4. Verificar se foi criado ou criar o arquivo "/etc/pam.d/samba" com o conteúdo da Figura 4.5.

```
# Configuração PAM para o serviço Samba
auth        sufficient      pam_ldap.so
account     sufficient      pam_ldap.so
password required pam_ldap.so use_first_pass use_authtok
```

Figura 4.5: Configuração PAM

5. Integrar o Samba ao OpenLDAP configurando o arquivo "smb.conf" de acordo com os parâmetros da Figura 4.6. O Apêndice II apresenta o arquivo completo.

```
[global]
   ldap suffix             = dc=cpatc,dc=embrapa,dc=br
   ldap machine suffix     = ou=People
   ldap user suffix        = ou=People
   ldap group suffix       = ou=Group
   ldap passwd sync        = Yes
   ldap admin dn    = cn=root,dc=cpatc,dc=embrapa,dc=br
   ldap ssl         = start tls
   security         = user
   encrypt passwords= yes
   domain logons    = yes
   logon script     = logon.bat
   domain master    = yes
   preferred master = yes
   passdb backend   = ldapsam:ldap://localhost
```

Figura 4.6: Parâmetros do Samba para integrar ao OpenLDAP

6. Testar o arquivo de configuração do *Samba* "smb.conf" para verificar se existe algum erro:

```
testparm
```

7. Criar o diretório "netlogon":

```
mkdir /usr/local/etc/netlogon
```

8. Editar o arquivo "/etc/rc.conf" e adicionar a seguinte linha:

```
samba_enable="YES"
```

9. Iniciar o *Samba*:

```
/usr/local/etc/rc.d/samba start
```

10. Criar a senha do *OpenLDAP* no arquivo "secrets.tdb" do *Samba*:

```
smbpasswd -w senha_do_ldap
```

11. Verificar se o *SID (Domain Security Identifier)* foi criado com sucesso no arquivo "secrets.tdb":

```
net getlocalsid
smbclient -L localhost -U%
```

12. Configurar *Smbldap-Tools*, acessando o caminho "/usr/local/etc/smbldap-tools" e alterar os parâmetros dos arquivos "smbldap.conf" e "smbldap_bind.conf", conforme Figuras 4.7 e 4.8.

```
# SID
SID="S-1-5-21-2834346363-453648026"
ldapTLS="1"

# Se estiver instalando o Samba num servidor diferente do
que está rodando o OpenLDAP, então copiar os 3 arquivos
abaixo do servidor OpenLDAP para o servidor do Samba
cafile="/usr/local/etc/openldap/ssl/cacert.pem"
clientcert="/usr/local/etc/openldap/ssl/servercrt.pem"
clientkey="/usr/local/etc/openldap/ssl/serverkey.pem"

suffix="dc=cpatc,dc=embrapa,dc=br"
usersdn="ou=People,${suffix}"
computersdn="ou=People,${suffix}"
groupsdn="ou=Group,${suffix}"
sambaUnixIdPooldn="sambaDomainName=CPATC,${suffix}"
hash_encrypt="CRYPT"
crypt_salt_format="%s"
userLoginShell="/bin/bash"
userHome="/home/%U"
defaultMaxPasswordAge="90"
userSmbHome="\\LDAP\%U"
userProfile="\\LDAP\%U\profile"
userHomeDrive="U:"
userScript="logon.bat"
mailDomain="cpatc.embrapa.br"
```

Figura 4.7: Arquivo de configuração smbldap.conf

```
slaveDN="cn=root,dc=cpatc,dc=embrapa,dc=br"
slavePw="secret"   # senha do administrador OpenLDAP
masterDN="cn=root,dc=cpatc,dc=embrapa,dc=br"
masterPw="secret"  # senha do administrador OpenLDAP
```

Figura 4.8: Arquivo de configuração smbldap_bind.conf

13. Retirar o direito de leitura para “todos” no arquivo que contém a senha:

```
chmod 400 smbldap_bind.conf
```

14. Gerar um *backup* da base do *OpenLDAP*:

```
/usr/local/etc/rc.d/slapd stop
tar -cvf /root/backup_ldap.tar /var/db/openldap-data
/usr/local/etc/rc.d/slapd start
```

15. Rodar o utilitário de criação de usuários/grupos do *Windows*:

```
/usr/local/sbin/smbldap-populate -u 2000 -g 2000
```

A opção -u vai setar o “id” do usuário a ser alocado quando da criação de um novo usuário, então coloque o valor do primeiro “id” disponível. A opção -g funciona da mesma maneira mas para os grupos.

4.2.3 Postfix

Os passos necessários para a configuração do servidor de correio *Postfix* são mostrados nesta seção. O caminho para os arquivos de configuração é “/usr/local/etc/postfix”. Os passos são os seguintes:

1. Criar o usuário “vmail”, que vai armazenar as mensagens no *Maildir*, conforme Figura 4.9:

```
pw groupadd vmail -g 240
pw useradd vmail -u 240 -g vmail -m
mkdir /var/spool/mail
chown -R vmail:vmail /var/spool/mail
```

Figura 4.9: Criação do usuário vmail

2. Editar o arquivo "main.cf", alterando ou acrescentando os parâmetros de integração ao *OpenLDAP* conforme Figura 4.10 abaixo. O Apêndice III mostra o arquivo completo "main.cf".

```
mailbox_transport = virtual:
mailbox_command_maps = ldap:accounts
virtual_maps = ldap:accountsmap
virtual_mailbox_base = /
virtual_mailbox_maps = ldap:accounts
accountsmap_server_host = ldap.cpatc.embrapa.br
accountsmap_search_base = dc=cpatc,dc=embrapa,dc=br
accountsmap_query_filter = (&(objectClass=qmailUser)
(mailAlternateAddress=%s))
accountsmap_result_attribute = mail
accountsmap_bind = no
```

Figura 4.10: Arquivo de configuração do Postfix

O *Postfix* é executado automaticamente no *boot* do servidor. Mas para iniciar o *Postfix* sem reiniciar a máquina execute:

```
/etc/rc.d/sendmail start
```

3. Verificar constante e regularmente os arquivos de *log* gerados:

```
more /var/log/maillog
more /var/log/ldap.log
```

4.2.4 Courier-Imap

Os passos necessários para a configuração do servidor de *Courier-Imap* são apresentados nesta seção. O caminho para os arquivos de configuração é "/usr/local/etc/". Os passos são os seguintes:

1. Editar o arquivo "authlib/authdaemonrc", alterando ou acrescentando os parâmetros conforme Figura 4.11:

```
authmodulelistorig="authldap"
authmodulelist="authldap"
version="authdaemond.ldap"
```

Figura 4.11: Configuração do arquivo authdaemonrc

2. Editar o arquivo "courier-imap/imapd", alterando ou acrescentando o parâmetro:

```
IMAPDSTART=YES
```

3. Editar o arquivo "courier-imap/pop3d", alterando ou acrescentando o parâmetro:

```
POP3DSTART=YES
```

4. Editar o arquivo “authlib/authldaprc”, alterando ou acrescentando os parâmetros da Figura 4.12:

```
LDAP_URI            ldap://ldap.cpatc.embrapa.br
LDAP_BASEDN         dc=cpatc,dc=embrapa,dc=br
LDAP_AUTHBIND       1
LDAP_PROTOCOL_VERSION     3
LDAP_GLOB_UID             240
LDAP_GLOB_GID             240
LDAP_TIMEOUT              5
# Filtro da pesquisa LDAP
LDAP_FILTER               (objectClass=qmailUser)
# Atributo utilizado para as pesquisas de login
LDAP_MAIL                 uid
LDAP_HOMEDIR              mailMessageStore
# Atributo da localização do Maildir
LDAP_MAILDIR               mailMessageStore
LDAP_DEFAULTDELIVERY      defaultDelivery
LDAP_FULLNAME              cn
# Atributo da senha do usuário
LDAP_CRYPTPW              userPassword
LDAP_DEREF                never
LDAP_TLS                  0
```

Figura 4.12: Arquivo de configuração authldaprc

5. Editar o arquivo “/etc/rc.conf” e acrescentar o conteúdo da Figura 4.13:

```
courier_imap_imapd_enable="YES"
courier_imap_imapd_ssl_enable="YES"
courier_imap_pop3d_enable="YES"
courier_imap_pop3d_ssl_enable="YES"
courier_authdaemond_enable="YES"
```

Figura 4.13: Inicialização do Courier-IMAP no arquivo rc.conf

6. Iniciar os serviços do *Courier-Imap* e de autenticação:

```
/usr/local/etc/rc.d/courier-imap-imapd.sh start
/usr/local/etc/rc.d/courier-imap-pop3d.sh start
/usr/local/etc/rc.d/courier-authdaemond.sh start
```

7. Teste do serviço de *Imap*:

```
telnet localhost 143
Deve aparecer:
Trying ::1...
Trying 127.0.0.1...
Connected to localhost.cpatc.embrapa.br.
Escape character is '^]'.
* OK [CAPABILITY IMAP4rev1 UIDPLUS CHILDREN NAMESPACE
THREAD=ORDEREDSUBJECT THREAD=REFERENCES SORT QUOTA IDLE
ACL ACL2=UNION STARTTLS] Courier-IMAP ready. Copyright
1998-2005 Double Precision, Inc.  See COPYING for
distribution information.

Digite então:
a login <usuario> <senha>
a OK LOGIN Ok.
a logout
```

Figura 4.14: Teste de Imap

8. Configurar um cliente de *e-mail* (*thunderbird*, por exemplo) para acessar o servidor através de *Imap* ou *Pop3*. O diretório "/var/spool/mail" deve existir e o usuário "vmail" deve ter direito de gravação nele.

9. Configuração do acesso ao *imapd-ssl* e *pop3d-ssl,* ou seja, *Imap* e *Pop3* seguros (com *SSL*):

a. Editar os arquivos “courier-imap/imapd.cnf.dist” e “courier-imap/pop3d.cnf.dist”, alterando as linhas conforme Figura 4.15.

```
[ req_dn ]
C=BR
ST=SE
L=Aracaju
O=Embrapa
OU=CPATC
CN=ldap.cpatc.embrapa.br
emailAddress=postmaster@ldap.cpatc.embrapa.br
```

Figura 4.15: Exemplo para arquivos imapd.cnf e pop3d.cnf

b. Copiar os arquivos:

```
cp pop3d.cnf.dist pop3d.cnf
cp imapd.cnf.dist imapd.cnf
```

c. Gerar os certificados:

```
/usr/local/sbin/mkimapdcert
/usr/local/sbin/mkpop3dcert
```

d. Iniciar os serviços do *Courier-Imap* com *SSL*:

```
/usr/local/etc/rc.d/courier-imap-imapd-ssl.sh start
/usr/local/etc/rc.d/courier-imap-pop3d-ssl.sh start
```

e. Testar se o protocolo *SSL* está funcionando:

```
openssl s_client -host localhost -port 993 -verify -debug
openssl s_client -host localhost -port 995 -verify -debug
```

f. No cliente de *e-mail*, marcar a opção para usar *SSL*. No *Thunderbird* por exemplo, *Edit – Account Settings – Server Settings – Use secure connection (SSL)*.

5 – Testes e Resultados

A alimentação da base de dados pode ser feita através de arquivos *ldif* ou através de comandos ou ferramentas gráficas. Os testes apresentados nesta seção explora todas essas opções, começando com a criação da raiz da base *LDAP,* com exemplos de criação de usuários e grupos tanto através de arquivos *ldif* como também através de comandos do *OpenLDAP* e do *Smbldap-Tools*. Por fim, mostra o uso da ferramenta gráfica *Phpldapadmin*.

5.1 Criação da base e de contas de usuários

A criação dos usuários e grupos depende primeiramente da alimentação da árvore do servidor *OpenLDAP*. Nesta seção é apresentado como criar essa árvore e exemplos de usuário e grupo.

1. Criar um arquivo "/tmp/base_cpatc.ldif" conforme Figura 5.1:

```
dn: dc=embrapa,dc=br
dc: embrapa
o: Embrapa
objectClass: top
objectClass: dcObject
objectClass: organization

dn: dc=cpatc,dc=embrapa,dc=br
dc: cpatc
objectClass: top
objectClass: domain

dn: ou=People,dc=cpatc,dc=embrapa,dc=br
ou: People
objectClass: top
objectClass: organizationalUnit

dn: ou=Group,dc=cpatc,dc=embrapa,dc=br
ou: Group
objectClass: top
objectClass: organizationalUnit
```

Figura 5.1: Raiz do servidor OpenLDAP

2. Executar o comando para a criação da árvore *LDAP*:

```
ldapadd -Z -D "cn=root,dc=embrapa,dc=br" -W -f base_cpatc.ldif
```

3. Cadastrar usuários e grupos.

O cadastramento de usuários é feito manualmente, através de um arquivo que armazena seus dados. Esse arquivo é transferido ao servidor

OpenLDAP através do comando "*ldapadd"*, da mesma forma que a estrutura da árvore *LDAP* foi criada. A Figura 5.2 apresenta um exemplo de dados que devem estar contidos no arquivo para o cadastramento de grupos e o Apêndice IV mostra dados para cadastramento de usuários. Usou-se "gerentes" como nome de grupo e "usuteste" como nome de usuário.

```
dn: cn=gerentes,ou=Group,dc=cpatc,dc=embrapa,dc=br
objectClass: posixGroup
cn: gerentes
gidNumber: 3000
[memberUid: 4000]
```

Figura 5.2: Dados de grupo para arquivo ldif

Um arquivo pode conter dados de um ou mais usuários, um ou mais grupos, ou as duas situações. A senha do usuário armazenada em "userPassword" pode ser codificada externamente através do comando "slappasswd" utilizando a seguinte sintaxe:

```
slappasswd -h '{CRYPT}' -s <senha>
```

Outro modo de efetuar o cadastramento de senhas é eliminar a linha "*userPassword"* do arquivo de cadastro (*ldif*), e utilizar o comando "*ldappasswd"* para cadastrar/atualizar a senha do usuário. A sintaxe é:

```
ldappasswd -D "cn=root,dc=embrapa,dc=br" -W -S \
"uid=usuteste,ou=people,dc=cpatc,dc=embrapa,dc=br"
```

Ao executar o comando, é solicitada a nova senha do usuário e sua confirmação, em seguida é solicitada a senha do administrador *OpenLDAP*, ou seja, a mesma senha cadastrada para o "rootdn" no arquivo "slapd.conf".

4. Para excluir usuários ou grupos são mostrados os comandos da Figura 5.3:

```
ldapdelete -Z -D "cn=root,dc=embrapa,dc=br" -W \
"uid=ususteste,ou=people,dc=cpatc,dc=embrapa,dc=br"

ou

ldapdelete -Z -D "cn=root,dc=embrapa,dc=br" -W \
"cn=gerentes,ou=group,dc=cpatc,dc=embrapa,dc=br"
```

Figura 5.3: Exemplos de exclusão de usuários ou grupos

5.2 Manutenção da base de dados

Os comandos básicos para manutenção das contas do *OpenLDAP* usando o *Smbldap-Tools* são mostrados na Tabela 5.1.

Tabela 5.1: Comandos de manutenção

Criação de Usuário	/usr/local/sbin/smbldap-useradd -a -m login
Alteração de Senha	/usr/local/sbin/smbldap-passwd login
Exclusão de Usuário	/usr/local/sbin/smbldap-userdel login
Criação de Grupo	/usr/local/sbin/smbldap-groupadd -a nome_do_grupo
Remoção de Grupo	/usr/local/sbin/smbldap-groupdel nome_do_grupo
Mostrar info. do usuário	/usr/local/sbin/smbldap-usershow login
Mostrar info. do grupo	/usr/local/sbin/smbldap-groupshow nome_do_grupo

Além dos comandos da Tabela 5.1 acima, que são do pacote *Smbldap-Tools,* outro comando interessante é usado para fazer buscas (consultas) na base de dados. Para isso, utiliza-se o "*ldapsearch"*. Segue um exemplo:

```
ldapsearch -h nomedohost -b dc=cpatc,dc=embrapa,dc=br
'uid=usuteste'
```

Nesse caso, é feita uma pesquisa para saber os dados do uid=usuteste, no host nomedohost, com o domínio dc=cpatc,dc=embrapa,dc=br.

5.3 Melhorias no gerenciamento

Com o intuito de melhorar ainda mais a manutenção das contas, o *script "smbldap-useradd"* do *Smbldap-Tools* foi modificado pela empresa, acrescentando os seguintes campos:

-e – dados do empregado → matrícula, setor, tipo do empregado (estagiário ou funcionário).
-y – senha encriptada.
-p – *e-mail* alternativo.

O Apêndice VI mostra trechos do *script* "smblpdap-useradd". E logo depois, exemplo de uso do comando.

Para cadastrar um usuário com o *login* "usuteste", senha *crypt* "*7TyJBnoKGa526", uid* "4160", *gid* "514", matrícula "900160", *e-mail* alternativo "Usuario_Teste", usa-se o comando:

```
smbldap-useradd -a -p Usuario_Teste -u 4160 -g 514 -c "Usuario
teste" -e 900160,estagiario,"estagio" m -y 7TyJBnoKGa526
usuteste
```

5.4 Ferramenta Phpldapadmin

Muitas opções de comandos tanto do *OpenLDAP* como do *Smbldap-Tools* são mostradas ao longo deste documento e é interessante que um administrador de sistemas conheça essas opções e também opções gráficas, como é o caso do *Phpldapadmin*. Nas Figuras 5.4, 5.5, 5.6 e 5.7 são mostradas algumas funcionalidades dessa ferramenta.

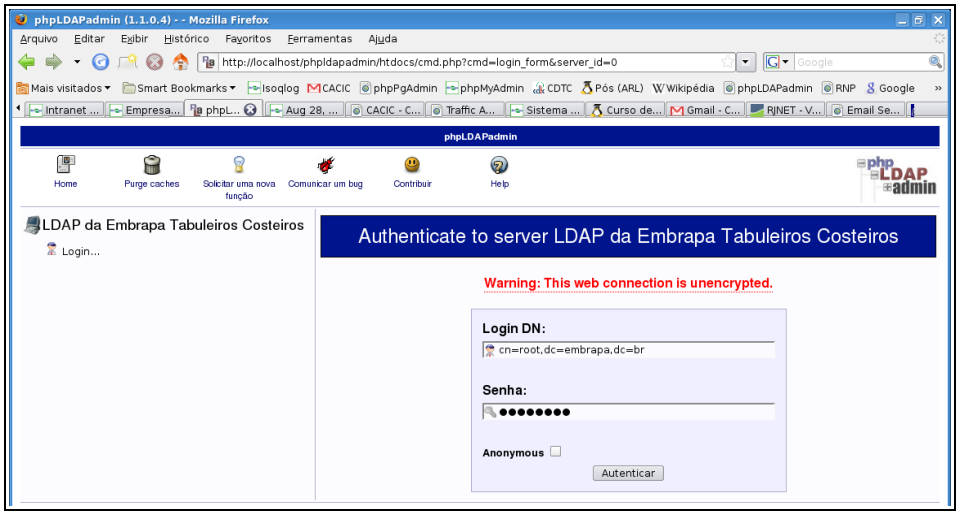

Figura 5.4: Phpldapadmin - Tela de login

Figura 5.5: Phpldapadmin - Dados de usuários

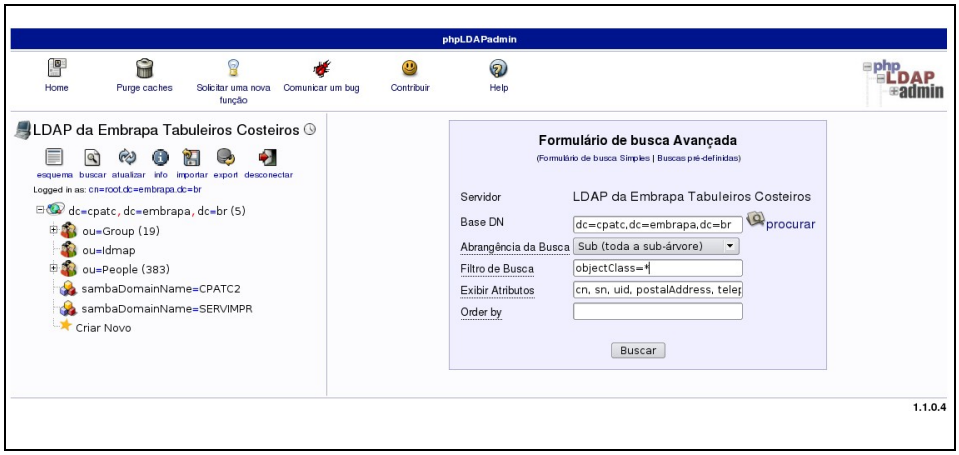

Figura 5.6: Phpldapadmin - Busca avançada

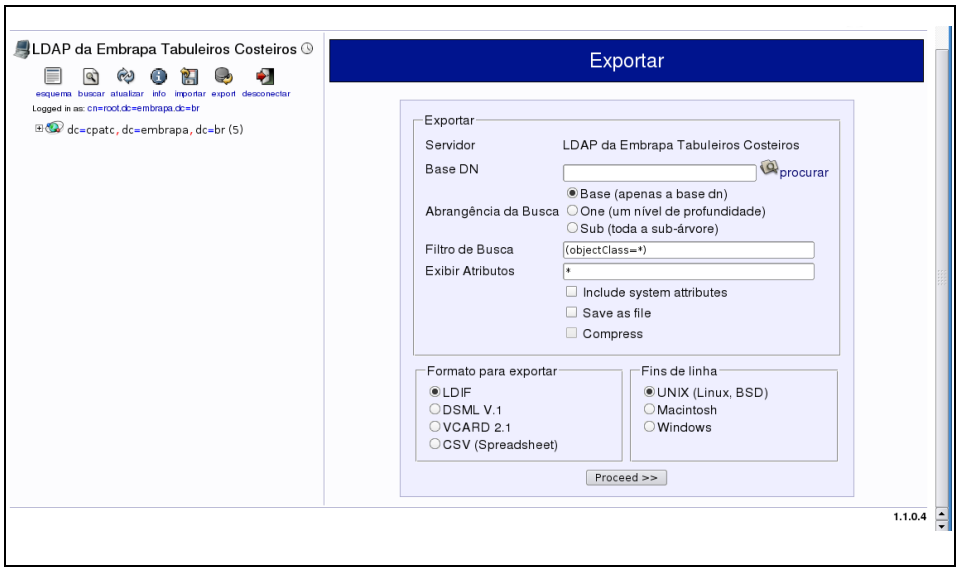

Figura 5.7: Phpldapadmin - Exportar dados

5.5 Melhorias para os usuários

A migração para as ferramentas mencionadas e o uso do *OpenLDAP* integrado ao *Samba* e ao *Postfix* trouxeram melhorias para os usuários da rede local de computadores da filial da empresa. Pode-se destacar:

1. *E-mail* alternativo:

O antigo uso do *Solaris* e do *NIS* nas versões usadas na empresa trazia limitações quanto a criação de contas de usuários e *e-mails* alternativos. Com o uso da solução apresentada, é possível criar usuários com *login* maior que 8 caracteres e um segundo *e-mail*, por exemplo, vinicius.rodrigues@cpatc.embrapa.br.

2. Catálogo de endereços no cliente de *e-mail*:

Quando a relação de empregados é muito extensa, é mais difícil mantê-la atualizada em todos os computadores, em todos os perfis de *e-mail* dos usuários. Mas com o uso do *OpenLDAP*, é necessário apenas configurar o cliente de *e-mail* para acessar a base, facilitando a vida dos usuários pela busca dos *e-mails* dos colegas de trabalho ou de qualquer lista armazenada do servidor.

3. Perfil móvel:

O perfil móvel é útil para usuários que mudam constantemente de computador, como é o caso de estagiários e técnicos de laboratórios da empresa. Com o uso do *Samba* como *PDC*, integrado ao *OpenLDAP* e com as facilidades do *Smbldap-Tools*, essa mobilidade é possível.

4. Uso do *Imap* em substituição ao *Pop3*:

Para os usuários que preferem manter suas mensagens no servidor(com o *Imap*) ao invés de "baixá-las" para o computador (*Pop3*), a instalação do *Courier-Imap* trouxe essa vantagem.

5. *Script* de *logon*:

O *Samba* como *PDC* também facilitou configurações automáticas de alguns serviços de rede, como por exemplo mapeamento de diretórios nos servidores, *backup* automático e atualização de programas em todos os computadores de forma automática, ou seja, de forma centralizada, tudo é feito em todos os computadores.

6 – Conclusão e Trabalhos Futuros

A migração para o ambiente tecnológico padronizado pela empresa proporcionou que os serviços de redes de computadores implantados atingissem a integração desejada, ou seja, serviços de *e-mail*, compartilhamento de recursos e autenticação de usuários mantidos por uma mesma base de dados. Essa integração das ferramentas *Postfix*, *Courier-Imap*, *Samba*, *Smbldap-Tools* ao *OpenLDAP* trouxe benefícios tanto para os administradores da rede como para os usuários. Estes, com *logins* e senhas únicos, *e-mail* alternativo e catálogo de endereços único, e aqueles, com melhoria no gerenciamento e manutenção de serviços e suporte técnico para a solução adotada.

A atualização tecnológica pretendida pela filial foi atendida nessa migração. O uso das ferramentas padronizadas pela empresa trouxe melhorias nos serviços de e-mail, compartilhamento de recursos e autenticação de usuários.

Para trabalhos futuros, outros serviços precisam ser integrados, como autenticação dos usuários de internet através da ferramenta *Squid*, sistema de atendimento a usuários (*Helpdesk*) e principalmente, ferramentas para aumentar a segurança da informação, no *firewall* e nos sistemas de acesso a bancos de dados. Também há motivação para o desenvolvimento de uma ferramenta gráfica que forneça todas as opções de cadastro dos comandos do *Smbldap-Tools*, já com as inclusões de campos feita pela empresa.

Referências Bibliográficas

ABÍLIO, R. S.; NETO, J. M. **Proposta de uma metodologia para Migração de Software Proprietário para Software Livre com Foco no Usuário**. FISL 9.0, 2008.

BOAS, T. V.; MENDONÇA, N. **Samba**. Rio de Janeiro: Brasport, 2004.

DOMINGUES, M. A.; UCHÔA, J. Q.; SCHNEIDER, B. O. **Autenticação em sistemas linux usando OpenLDAP**. Disponível em: http://www.ginux.ufla.br/~joukim/extensao/semac.pdf, 2001. Acesso em: 26/08/2008.

E-PING. **Padrões de Interoperabilidade de Governo Eletrônico**. Brasília, 2007. Disponível em: https://www.governoeletronico.gov.br/anexos/e-ping-versao-3.0. Acesso em: 26/08/2008.

GUIA LIVRE. **Referência de Migração para Software Livre do Governo Federal**. Brasília, 2005. Disponível em: https://www.governoeletronico.gov.br/anexos/guia-livre-versao-1.0. Acesso em: 26/08/2008.

LUCAS, M. **Dominando BSD**: o guia definitivo para o FreeBSD. Rio de Janeiro: Ciência Moderna, 2003.

SHEARER.org. **MTA Comparison**. Disponível em http://shearer.org/MTA_Comparison. Acesso em: 26/08/2008.

SUNGAILA, M. **Autenticação centralizada com OpenLDAP**: integrando serviços de forma simples e rápida. São Paulo: Novatec, 2008.

TRIGO, C. H.; **OpenLDAP**: uma abordagem integrada. São Paulo: Novatec, 2007.

UCHÔA, J. Q.; SICA, F. C.; SIMEONE, L. E. **Serviços de Redes em Linux**. Lavras: UFLA/FAEPE, 2004.

Apêndice I – Arquivo "slapd.conf"

```
#Schema Principal (base) do LDAP.
Include  /usr/local/etc/openldap/schema/core.schema
#Schemas utilizados pelo Posix.
Include  /usr/local/etc/openldap/schema/cosine.schema
include   /usr/local/etc/openldap/schema/inetorgperson.schema
include  /usr/local/etc/openldap/schema/nis.schema
#Schema utilizado pelo Postfix e Courier-Imap.
Include  /usr/local/etc/openldap/schema/qmail.schema

#Informações sobre os certificados para uso do ssl e tls
TLSCertificateFile  /usr/local/etc/openldap/ssl/servercrt.pem
TLSCertificateKeyFile /usr/local/etc/openldap/ssl/serverkey.pem
TLSCACertificateFile  /usr/local/etc/openldap/ssl/cacert.pem
TLSCipherSuite HIGH:MEDIUM:+SSLv2

modulepath   /usr/local/libexec/openldap
moduleload   back_bdb

# Arquivos necessários para o funcionamento do OpenLDAP.
pidfile      /var/run/openldap/slapd.pid
argsfile     /var/run/openldap/slapd.args

# Definição da Base de Dados (tipo, raiz, administrador e
senha).
database     bdb

# Raiz do LDAP.
suffix       "dc=embrapa,dc=br"

# Definição do Administrador.
rootdn       "cn=root,dc=embrapa,dc=br"
rootpw       <senha encriptada>
```

```
# Localização do Diretório LDAP.
directory    /var/db/openldap-data

## Listas de Acesso ao Servidor.
# Permite a alteração do campo "userPassword" pelo próprio
usuário e administrador do LDAP.
access to attrs=userPassword
    by dn.base="cn=root,dc=embrapa,dc=br" write
    by anonymous auth
    by self write
    by * none

# Qualquer um pode ter acesso ao "uidNumber e gidNumber,
mas apenas o Administrador pode modificar.
access to attrs=uidNumber,gidNumber
    by dn.base="cn=root,dc=embrapa,dc=br" write
    by * read

# Qualquer um pode alterar seus próprios dados. O
Administrador pode alterar os dados de qualquer um.
access to *
    by dn.base="cn=root,dc=embrapa,dc=br" write
    by self write
    by * read

# Definição dos índices para melhorar as consultas
index  objectClass         eq
index  uid                 pres,eq,sub
index  gidNumber           eq
index  uidNumber           eq
index  cn                  pres,eq,sub
index  memberuid           pres,eq,sub
index  mail                pres,eq,sub
index  mailAlternateAddress      pres,eq,sub
```

Apêndice II – Arquivo "smb.conf"

```
[global]
   workgroup = CPATC
   server string          = Servidor Samba com OpenLdap
   ldap suffix            = dc=cpatc,dc=embrapa,dc=br
   ldap machine suffix    = ou=People
   ldap user suffix       = ou=People
   ldap group suffix      = ou=Group
   ldap passwd sync       = Yes
   ldap admin dn    = cn=root,dc=cpatc,dc=embrapa,dc=br
   ldap ssl         = start tls
   security         = user
   encrypt passwords= yes
   os level         = 100
   domain logons    = yes
   logon script     = logon.bat
   domain master    = yes
   preferred master = yes
   logon drive      = u:
   logon path       = \\%N\%U\profile
   logon home       = \\%N\%U
   wins support     = yes
   netbios name     = LDAP
   passdb backend   = ldapsam:ldap://localhost
   smb ports        = 139 445
   hosts allow      = 10.10.   127.
   log file         = /var/log/samba/log.%m
   max log size     = 50
   socket options   = TCP_NODELAY
   dns proxy        = yes

[homes]
   comment          = Diretório Home
```

```
   writable         = yes
   browseable       = no
   create mask      = 0750
   directory mask   = 0750
   invalid users    = administrator

[netlogon]
   comment          = Diretório para profile de usuários
   browseable       = yes
   guest ok         = no
   path             = /usr/local/etc/netlogon
   writable         = no
   public           = yes
   create mask      = 0775
   directory mask   = 0775
   invalid users    = administrator

[public]
   comment          = Diretório Público
   path             = /tmp
   public           = yes
   writable         = yes
   printable        = no
```

Apêndice III – Arquivo "main.cf"

```
myhostname = mailhost.cpatc.embrapa.br
mydomain = cpatc.embrapa.br
myorigin = $mydomain
alias_maps = hash:/etc/mail/aliases
alias_database = hash:/etc/mail/aliases

# Configura o formato das caixas postais para Maildir
home_mailbox = Maildir/

# Define o método de transporte das caixas postais
mailbox_transport = virtual:
mailbox_command = /usr/local/bin/procmail
mailbox_command_maps = ldap:accounts

# Mapa de usuários locais
local_recipient_maps = $alias_maps $virtual_mailbox_maps

## Configuração Virtual

# Mapeia as contas de e-mail
virtual_maps = ldap:accountsmap

# Mailbox das contas de e-mail
virtual_mailbox_base = /
virtual_mailbox_maps = ldap:accounts

# Uid/Gid do usuário vmail que vai armazenar as mensagens
virtual_uid_maps = static:240
virtual_gid_maps = static:240
virtual_maildir_extended = yes

# Consulta aos dados no OpenLDAP
```

```
# O esquema qmail.schema já deve estar configurado no
arquivo "slapd.conf" e os usuários devem ter informações
para os atributos "mailAlternateAddress", "mail" e
"mailMessageStore"

# Pesquisa os endereços de e-mail dos usuários
(mailAlternateAddress) e retorna o endereço de e-mail de
roteamento (mail)
accountsmap_server_host = ldap.cpatc.embrapa.br
accountsmap_search_base = dc=cpatc,dc=embrapa,dc=br
accountsmap_query_filter = (&(objectClass=qmailUser)
(mailAlternateAddress=%s))
accountsmap_result_attribute = mail
accountsmap_bind = no

# Pesquisa o endereço de e-mail de roteamento (mail) e
retorna o local onde as mensagens vão ser armazenadas
(mailMessageStore)
accounts_server_host = ldap.cpatc.embrapa.br
accounts_search_base = dc=cpatc,dc=embrapa,dc=br
accounts_query_filter = (&(objectClass=qmailUser)(mail=%s))
accounts_result_attribute = mailMessageStore
accounts_bind = no
```

Apêndice IV – Dados para cadastro de usuário através de arquivo ldif

```
dn: uid=usuteste,ou=People,dc=cpatc,dc=embrapa,dc=br
uid: usuteste
cn: Usuario Fulano de Tal
objectClass: posixAccount
objectClass: shadowAccount
objectClass: inetOrgPerson
objectClass: qmailUser
objectClass: top
objectClass: sambaSamAccount
sn: Rodrigues
sambaLogonTime: 0
sambaLogoffTime: 2147483647
sambaKickoffTime: 2147483647
displayName: Usuario Fulano de Tal
sambaSID: S-1-5-21-2421889151-3335005291-3524197835-7006
sambaPrimaryGroupSID:
S-1-5-21-2421889151-3335005291-3524197835-513
sambaLogonScript: logon.bat
sambaProfilePath: \\intranet2\usuteste\profile
sambaHomePath: \\intranet2\usuteste
sambaHomeDrive: U:
employeeNumber: 299468
employeeType: funcionario
departmentNumber: Setor
sambaPwdCanChange: 1173910715
sambaPasswordHistory:
0000000000000000000000000000000000000000000000000000000000000000
sambaLMPassword: C9326367418E7CECAAD3B435B51404EE
sambaAcctFlags: [U]
sambaNTPassword: 6766DEF902D8827AC5209B839DC9A093
sambaPwdLastSet: 1204202845
```

```
sambaPwdMustChange: 1981802845
userPassword: {crypt}xxxxxxxxxx
loginShell: /bin/bash
uidNumber: 444
gidNumber: 222
homeDirectory: /home/usuteste
gecos: Usuario Fulano de Tal
description: Usuario Fulano de Tal
givenName: Usuario Fulano
sn: de Tal
mailAlternateAddress: usuteste@cpatc.embrapa.br
mailAlternateAddress: outro-email@cpatc.embrapa.br
mail: usuteste@mailhost.cpatc.embrapa.br
mailHost: mailhost.cpatc.embrapa.br
mailMessageStore: /var/spool/mail/usuteste/MailDir/
```

Apêndice V - Criação do Certificado da Entidade Certificadora

1. Executar os comandos abaixo para acessar o caminho (diretório) e gerar os arquivos dos certificados:

```
cd /etc/ssl
cp /usr/src/crypto/openssl/apps/CA.pl .
perl CA.pl -newca
```

Ao executar o comando, surgirá a pergunta:

```
CA certificate filename (or enter to create)
```

Pressionar ***<Enter>*** para criar um novo certificado.

Em "***Enter PEM pass phrase*:**" digitar senha e confirmação do certificador (essa senha será utilizada quando o certificado do servidor *OpenLDAP* for assinado).

Abaixo, estão todas as perguntas feitas pelo comando CA.pl:

```
Making CA certificate ...
Generating a 1024 bit RSA private key
......++++++
...........++++++
writing new private key to './demoCA/private/cakey.pem'
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:
-----
```

```
You are about to be asked to enter information that will be
incorporated into your certificate request.
What you are about to enter is what is called a Distinguished
Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:BR
State or Province Name (full name) [Some-State]:SE
Locality Name (eg, city) []:Aracaju
Organization Name (eg, company) [Internet Widgits Pty
Ltd]:Embrapa
Organizational Unit Name (eg, section) []:Tabuleiros Costeiros
Common Name (eg, YOUR name) []:root@cpatc.embrapa.br
Email Address []:root@ldap.cpatc.embrapa.br
```

Ao terminar o comando, tem-se um certificado da Autoridade Certificadora, ou seja, o certificado da entidade que garante a autenticidade do certificado *SSL* que é utilizado pelo servidor *OpenLDAP*.

2. Criar o certificado do servidor *OpenLDAP*:

```
openssl req -new -nodes -keyout newreq.pem -out newreq.pem


Generating a 1024 bit RSA private key
.....................................................
.++++++
.....................................++++++
writing new private key to 'newreq.pem'
-----
You are about to be asked to enter information that will be
incorporated into your certificate request.
```

```
What you are about to enter is what is called a Distinguished
Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:BR
State or Province Name (full name) [Some-State]:SE
Locality Name (eg, city) []:Aracaju
Organization Name (eg, company) [Internet Widgits Pty
Ltd]:Embrapa
Organizational Unit Name (eg, section) []:Tabuleiros Costeiros
Common Name (eg, YOUR name) []:ldap.cpatc.embrapa.br
Email Address []:root@ldap.cpatc.embrapa.br

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
```

Em **"*Common Name*"**, o nome informado deve ser o nome completo da máquina onde o servidor será executado.

3. Fazer a autenticação do certificado do servidor *OpenLDAP*:

```
perl CA.pl -sign
```

Durante a autenticação do certificado, é solicitado o "***PEM pass phrase***" criado para a autoridade certificadora.

4. Copiar o certificado para o diretório de configuração do servidor *OpenLDAP* e definir as permissões conforme comandos:

```
mkdir /usr/local/etc/openldap/ssl
cp demoCA/cacert.pem /usr/local/etc/openldap/ssl
mv newcert.pem /usr/local/etc/openldap/ssl/servercrt.pem
mv newreq.pem /usr/local/etc/openldap/ssl/serverkey.pem
chmod 0600 /usr/local/etc/openldap/ssl/serverkey.pem
chown ldap:ldap /usr/local/etc/openldap/ssl/serverkey.pem
```

Com isso, a geração dos arquivos que serão usados nas configurações do "slapd.conf" é finalizada. Esses arquivos são: "cacert.pem", "servercrt.pem" e "serverkey.pem", localizados no diretório "/usr/local/etc/openldap/ssl".

Apêndice VI – *Script smbldap-useradd* (modificado)

```
#!/usr/bin/perl -w

# $Id: smbldap-useradd,v 1.25 2005/01/29 15:00:54 jtournier Exp $
#
#  This code was developped by IDEALX (http://IDEALX.org/) and
#  contributors (their names can be found in the CONTRIBUTORS file).
#
#                 Copyright (C) 2002 IDEALX
#
#  This program is free software; you can redistribute it and/or
#  modify it under the terms of the GNU General Public License
#  as published by the Free Software Foundation; either version 2
#  of the License, or (at your option) any later version.
#
#  This program is distributed in the hope that it will be useful,
#  but WITHOUT ANY WARRANTY; without even the implied warranty of
#  MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.  See the
#  GNU General Public License for more details.
#
#  You should have received a copy of the GNU General Public License
#  along with this program; if not, write to the Free Software
#  Foundation, Inc., 59 Temple Place - Suite 330, Boston, MA 02111-1307,
#  USA.

# Purpose of smbldap-useradd : user (posix,shadow,samba) add

use strict;

use FindBin;
use FindBin qw($RealBin);
use lib "$RealBin/";
use smbldap_tools;
use Crypt::SmbHash;
######################


use Getopt::Std;
my %Options;

my $DOMINIO_EMAIL_COMPOSTO = "cpatc.embrapa.br";
my $MX_HOST = "mailhost";

my $ok = getopts('o:anmwiPG:u:g:d:s:p:e:y:c:k:A:B:C:D:E:F:H:M:N:S:T:?', \%Options);

if ( (!$ok) || (@ARGV < 1) || ($Options{'?'}) ) {
  print_banner;
  print "Usage: $0 [-awmugdsckABCDEFGHMNPST?] username\n";
  print "  -o    add the user in the organazional unit (relative to the user
suffix)\n";
  print "  -a    is a Windows User (otherwise, Posix stuff only)\n";
  print "  -p    is a Postfix User - Postfix AlternateMail address (email
composto),mx host \n";
  print "  -e    Employee information -
employeeNumber,employeeType,departmentNumber \n";
  print "  -w    is a Windows Workstation (otherwise, Posix stuff only)\n";
  print "  -i    is a trust account (Windows Workstation)\n";
  print "  -u    uid\n";
  print "  -g    gid\n";
```

```
  print "  -y    Crypt password\n";
  print "  -G    supplementary comma-separated groups\n";
  print "  -n    do not create a group\n";
  print "  -d    home\n";
  print "  -s    shell\n";
  print "  -c    gecos\n";
  print "  -m    creates home directory and copies /etc/skel\n";
  print "  -k    skeleton dir (with -m)\n";
  print "  -P    ends by invoking smbldap-passwd\n";
  print "  -A    can change password ? 0 if no, 1 if yes\n";
  print "  -B    must change password ? 0 if no, 1 if yes\n";
  print "  -C    sambaHomePath (SMB home share, like '\\\\PDC-SRV\\homes')\n";
  print "  -D    sambaHomeDrive (letter associated with home share, like 'H:')\n";
  print "  -E    sambaLogonScript (DOS script to execute on login)\n";
  print "  -F    sambaProfilePath (profile directory, like '\\\\PDC-SRV\\profiles\\
foo')\n";
  print "  -H    sambaAcctFlags (samba account control bits like
'[NDHTUMWSLKI]')\n";
  print "  -N    canonical name\n";
  print "  -S    surname\n";
  print "  -M    local mailAddress (comma seperated)\n";
  print "  -T    mailToAddress (forward address) (comma seperated)\n";
  print "  -?    show this help message\n";
  exit (1);
}

my $ldap_master=connect_ldap_master();

...
...
...


# Alterado para em sn colocar o sobrenome e em givenName o primeiro nome
my @words = split(/ /, $config{userGecos});
my $givenName = $words[0];
my $last = @words - 1;
$userSN = $words[$last];
my $cryptpass = "x";

# Se passou a senha criptografada então grava no LDAP
if (defined($Options{'y'})) {
        $cryptpass = $Options{'y'};
}

# Adicionadas as informações:

my $add = $ldap_master->add ("uid=$userName,$config{usersdn}",
                             attr => [
                                      'objectclass' =>
['top','inetOrgPerson','posixAccount','shadowAccount','phpgwAccount'],
                                      'cn'   => "$userCN",
                                      'uid'   => "$userName",
                                      'uidNumber'   => "$userUidNumber",
                                      'gidNumber'   => "$userGidNumber",
                                      'homeDirectory'   => "$userHomeDirectory",
                                      'givenName'   => "$givenName",
                                      'sn'   => "$userSN",
                                      'loginShell'   => "$config{userLoginShell}",
                                      'gecos'   => "$config{userGecos}",
                                      'description'   => "$config{userGecos}",
                                      'phpgwAccountExpires'   => "-1",
                                      'phpgwAccountStatus'   => "A",
                                      'phpgwAccountType'   => "u",
                                      'userPassword'   => "{crypt}$cryptpass"
                                     ]
                            );
```

```
$add->code && warn "failed to add entry: ", $add->error ;


#if ($createGroup) {
#    group_add($userName, $userGidNumber);
#}

group_add_user($userGidNumber, $userName);

my $grouplist;
# adds to supplementary groups
if (defined($grouplist = $Options{'G'})) {
  add_grouplist_user($grouplist, $userName);
}

...
...
...

# Add Postfix user infos
if (defined($Options{'p'})) {

  my $domain = $config{mailDomain};
  my $altermail;
  my @postfixopt = &split_arg_comma($Options{'p'});
  my $mailhost = $MX_HOST;

  $altermail = $postfixopt[0];

  # Se passou o host de correio entao recupera o mx host
  if (@postfixopt > 1) {
    $mailhost = $postfixopt[1];
  }

  my $modify = $ldap_master->modify ( "uid=$userName,$config{usersdn}",
                                      changes => [
                                                  add => [objectClass =>
'qmailUser'],
                                                  add => [mailAlternateAddress =>
"$userName\@$mailhost\.$domain"],
                                                  add => [mailAlternateAddress =>
"$altermail\@$DOMINIO_EMAIL_COMPOSTO"],
                                                  add => [mail =>
"$userName\@$domain"],
                                                  add => [mailHost => "$mailhost\.
$domain"],
                                                  add => [mailMessageStore =>
"/var/spool/mail/$userName/MailDir/"],
                                                 ]
                                    );

  $modify->code && die "failed to add entry: ", $modify->error ;
}

# Add Employee informations
if (defined($Options{'e'})) {

  my $employeeNumber;
  my $employeeType = '';
  my $department = '';
  my @employeeopt = &split_arg_comma($Options{'e'});

  $employeeNumber = $employeeopt[0];

  if (@employeeopt > 0) {
    $employeeType = $employeeopt[1];
```

```
  }

  if (@employeeopt > 1) {
    $department = $employeeopt[2];
  }

  my $modify = $ldap_master->modify ( "uid=$userName,$config{usersdn}",
                                      changes => [
                                                  add => [employeeNumber =>
"$employeeNumber"],
                                                  add => [employeeType =>
"$employeeType"],
                                                  add => [departmentNumber =>
"$department"],
                                                 ]
                                    );

  $modify->code && die "failed to add entry: ", $modify->error ;
}


$ldap_master->unbind;             # take down session


if (defined($Options{'P'})) {
  exec "$RealBin/smbldap-passwd $userName"
}

exit 0;

######################################

=head1 NAME

smbldap-useradd - Create a new user

=head1 SYNOPSIS

smbldap-useradd [-o user_ou] [-c comment] [-d home_dir] [-g initial_group] [-G
group[,...]] [-m [-k skeleton_dir]] [-s shell] [-u uid [ -o]] [-P] [-A canchange]
[-B mustchange] [-C smbhome] [-D homedrive] [-E scriptpath] [-F profilepath] [-H
acctflags] login

=head1 DESCRIPTION

Creating New Users
  The smbldap-useradd command creates a new user account using  the values
specified on the  command  line  and  the default  values from the system and from
the configuration files (in  /etc/smbldap-tools directory).

For Samba users, rid is '2*uidNumber+1000', and sambaPrimaryGroupSID  is
'$SID-2*gidNumber+1001', where $SID is the domain SID.  Thus you may want to use :
  $ smbldap-useradd -a -g "Domain Admins" -u 500 Administrator
 to create an domain administrator account (admin rid is 0x1F4 = 500 and grouprid
is 0x200 = 512).

Without any option, the account created will be an Unix (Posix)  account. The
following options may be used to add information:

-o
The user's account will be created in the specified organazional unit. It is
relative to the user suffix dn ($usersdn) defined in the configuration file.

-a
The user will have a Samba account (and Unix).

-p
```

```
The user will have a Postfix account (and Unix).

-w
 Creates an account for a Samba machine (Workstation), so that it can join a
sambaDomainName.

-i
 Creates an interdomain trust account (machine Workstation). A password will be
asked for the trust account.

-c "comment"
 The new user's comment field (gecos).

-d home_dir
 The new user will be created using home_dir as the value for the user's login
directory.  The default is to append the login name      to userHomePrefix (defined
in the configuration file) and use that      as the login directory name.

-g initial_group
  The group name or number of the user's initial login group. The  group  name must
exist.  A group number must refer to an already  existing group.  The default group
number is defined in the  configuration file (defaultUserGid="513").

-G group,[...]
 A list of supplementary groups which the user is also  a  member of. Each  group
is separated to the next by a comma, with no intervening whitespace.  The groups
are  subject  to  the  same restrictions as the group given with the -g option.
The default is for the user to belong only to the initial group.

-m
The user's home directory will be created if it does not  exist. The  files
contained in skeletonDir will be copied to the home directory if the -k option is
used,  otherwise  the  files  contained  in /etc/skel will be used instead.  Any
directories contained in skeletonDir or  /etc/skel  will  be  created  in  the
user's  home  directory as well.  The -k option is only valid in conjunction with
the -m option.  The default is  to  not  create the directory and to not copy any
files.

-s shell
 The name of the user's login shell.  The  default  is  to  leave this  field
blank, which causes the system to select the default login shell.

-u uid
  The numerical value of  the  user's  ID.   This  value  must  be unique,  unless
the  -o option is used.  The value must be nonnegative.  The default is to use the
smallest ID  value  greater than 1000 and greater than every other user.

-P
 ends by invoking smbldap-passwd

-A
 can change password ? 0 if no, 1 if yes

-B
 must change password ? 0 if no, 1 if yes

-C sambaHomePath
 SMB home share, like '\\\\PDC-SRV\\homes'

-D sambaHomeDrive
 letter associated with home share, like 'H:'

-E sambaLogonScript
 relative to the [netlogon] share (DOS script to execute on login, like 'foo.bat'

-F sambaProfilePath
 profile directory, like '\\\\PDC-SRV\\profiles\\foo'
```

```
-H  sambaAcctFlags
  spaces and trailing bracket are ignored (samba account control bits like
'[NDHTUMWSLKI]'

-M  local mail aliases (multiple addresses are seperated by spaces)

-N  canonical name
 defaults to gecos or username, if gecos not set

-S  surname
 defaults to username

-T  mailToAddress (forward address) (multiple addresses are seperated by spaces)

-n  do not print banner message

=head1 SEE ALSO

       useradd(1)

=cut

#'
```