Ruy Minoru Ito Takata

Migração da rede da Fatec Ourinhos utilizando software livre: De Novell Netware para Samba + OpenLDAP

Monografia de Pós-Graduação "*Lato Sensu*" apresentada ao Departamento de Ciência da Computação para obtenção do título de Especialista em "Administração em Redes Linux"

Orientador
Prof. Ms. Denilson Vedoveto Martins

Lavras
Minas Gerais - Brasil
2009

Ruy Minoru Ito Takata

Migração da rede da Fatec Ourinhos utilizando software livre: De Novell Netware para Samba + OpenLDAP

Monografia de Pós-Graduação "*Lato Sensu*" apresentada ao Departamento de Ciência da Computação para obtenção do título de Especialista em "Administração em Redes Linux"

Aprovada em *21 de novembro de 2009*

Prof. Arlindo Follador Neto

Prof. Ms. Herlon Ayres Camargo

Prof. Ms. Denilson Vedoveto Martins
(Orientador)

Lavras
Minas Gerais - Brasil
2009

Agradecimentos

Agradeço aos amigos que fiz durante o curso e a todos os professores
do curso, em especial ao professor Denilson, meu orientador.

Sumário

Lista de Figuras

Lista de Tabelas

Resumo

Este trabalho tem por objetivo apresentar as técnicas utilizadas na migração da infra-estrutura lógica de rede da Faculdade de Tecnologia de Ourinhos (Fatec - Ourinhos), Faculdade do estado de São Paulo, gerida pela autarquia estadual Centro Estadual de Educação Tecnológica Paula Souza.

A migração foi motivada pela troca de hardware antigo, que apresentava problemas de desempenho. O software livre foi adotado para se alinhar com o posicionamento estratégico da direção da faculdade, que crê no crescimento da adoção de tecnologias livres, e em conseqüência, o aumento da escassez de mão-de-obra nesse segmento. Como formadora de mão-de-obra, a faculdade ve esse fato como uma oportunidade de formar profissionais capacitados para trabalharem nesse mercado.

O foco principal do trabalho foi a substituição do servidor de arquivos Novell Netware 4.11 pelo Samba com OpenLDAP, configurados como servidor de domínio (PDC). Também foram configurados os serviços de DHCP e DNS (DNS dinâmico). O proxy já estava configurado, sendo necessário somente trocá-lo de hardware.

Palavras-Chave: Linux; Samba; OpenLDAP; Xen; DNS; DHCP

Capítulo 1

Introdução

Atualmente a utilização de Software Livre vem crescendo muito, principalmente em servidores. Com isso, há uma vasta quantidade de documentação disponível.

Apesar dessa grande quantidade de documentação, ela é sobre alguma parte de um processo, e encontra-se muito pouco material sobre a migração inteira de uma infra-estrutura lógica de rede para software livre, o que dificulta muito tal tarefa.

O objetivo deste trabalho de conclusão de curso é documentar a migração da infra-estrutura lógica da rede da Faculdade de Tecnologia de Ourinhos.

A necessidade da migração surgiu devido a aquisição de novos servidores no início do ano de 2008. A atualização de hardware era realmente necessária, pois os servidores de arquivos utilizados anteriormente tinham mais de 10 anos, e além da capacidade de armazenamento muito pequena, eles também apresentavam problemas de desempenho.

Com a atualização do hardware foi necessário também atualizar o sistema operacional, pois era utilizado o Novell Netware 4.11, que apresenta incompatibilidade com o hardware. O custo de aquisição de uma nova licença do Novell Netware seria muito alto, e para isso seria necessário todo um processo burocrático para liberação de verba e para a abertura de um pregão para a aquisição do software. Isso tudo provavelmente atrasaria muito a migração, pois, nem todo ano há verba para aquisição de software, e todo o processo costuma demorar mais de 6 meses.

A administração da rede tem autonomia para decidir qual software utilizar caso este não tenha custos, por isso decidiu-se pela utilização de outro sistema operacional.

O Windows 2003 não foi utilizado por dois motivos:

- A Fatec Ourinhos adotou uma política de incentivo ao Software Livre, pois, vendo o crescimento da utilizacão de tal tecnologia, acredita em um conseqüente aumento na escassez da mão-de-obra nesse segmento. Como formadora de mão-de-obra, a faculdade ve isso como uma oportunidade de formar profissionais que podem atuar nessa área. Muitos alunos não vêem o software livre como uma alternativa, seja por falta de conhecimento técnico, seja pela preferência por softwares proprietários. Migrar toda a Administração da Rede foi uma maneira de mostrar aos alunos que além de possível, é também viável.

- A performance do Samba é superior quando comparada com o Windows 2003, conforme pode ser visto em (KEGEL, 2003) e em (KAVEN, 2001).

Pelos motivos citados acima, o servidor foi configurado com o sistema operacional Linux, e o servidor de arquivos Samba, configurado como PDC.

Outra necessidade suprida pelo controlador de domínios foi a melhoraria da segurança dos compartilhamentos de recursos entre as estações (prática utilizada pela secretaria acadêmica e pela administração), configurando compartilhamento através do domínio.

Os outros servidores tinham um desempenho bom, mas com o projeto de instalação de um link de Internet com IP público, existe a possibilidade de disponibilizar serviços para acesso externo, o que aumentará a utilização dos servidores.

A maior necessidade de acesso externo é para o sistema acadêmico, que disponibiliza os seguintes serviços:

- Consulta a notas e faltas;
- Lançamento de notas e faltas;
- Calendário escolar;
- Reserva de recursos multimídia.

A migração já vinha sendo planejada a muito tempo, por isso o administrador da rede já estudava o que seria necessário. Mesmo assim, durante todo o processo algumas dificuldades foram encontradas, mas todas foram superadas.

Este trabalho de conclusão de curso não tem o objetivo de instruir totalmente os leitores sobre todos os serviços configurados, mas sim oferecer uma orientação em alguns pontos que são importantes, e também indicar um pouco da documentação que foi utilizada pelo autor para conseguir realizar todo o trabalho.

A elaboração do trabalho baseou-se em consultas a livros, artigos, manuais técnicos e fóruns onlines mantidos pelos desenvolvedores das ferramentas. Foram efetuados diversos testes em laboratório para validar todas as configurações antes da implementação em produção.

No capítulo 2 há uma explicação sobre a infra-estrutura antiga e sobre a nova, e como configurar os servidores para poder utilizá-los.

O capítulo 3 fala sobre a configuração dos serviços e como integrá-los.

O capítulo 4 mostra como os serviços foram dispostos nos servidores, e uma sugestão de melhorias na infra-estrutura.

O capítulo 5 traz a conclusão do trabalho.

Capítulo 2

Ambiente

Neste capítulo será feita uma comparação entre a estrutura anterior e posterior ao processo de migração. Além de uma introdução sobre os conceitos utilizados para a configuração dos servidores.

2.1 Infra-Estrutura Antiga

A infra estrutura anterior era composta pelo seguinte:

Novell Netware 4.11: servidor de arquivos e impressão para os alunos. Servidor dual Pentium 3 de 450MHz com 256 MB de memória RAM e disco rígido SCSI de 8GB.

Novell Netware 4.11: servidor de arquivos e impressão para os professores. Computador Pentium 4 HT de 2,4GHz com 512 MB de memória RAM e disco rígido IDE de 40GB.

Debian GNU/Linux: servidor Proxy. Servidor dual Pentium 3 de 1GHz com 1GB de memória RAM e disco rígido SCSI[1] de 36GB.

Debian GNU/Linux: servidor de páginas e banco de dados para aulas. Computador Pentium 4 de 1,8GHz com 512MB de memória RAM e disco rígido SCSI de 36GB.

[1] sigla de Small Computer System Interface. Maiores detalhes podem ser encontrados em http://www.infowester.com/scsi.php

Gentoo: servidor de páginas e banco de dados para o sistema acadêmico. Computador Pentium 4 HT de 3,2 GHz com 2GB memória RAM e dois discos rígidos SATA2[2] em raid 0 de 120GB.

A figura 2.1 ilustra os servidores na estrutura antiga de rede.

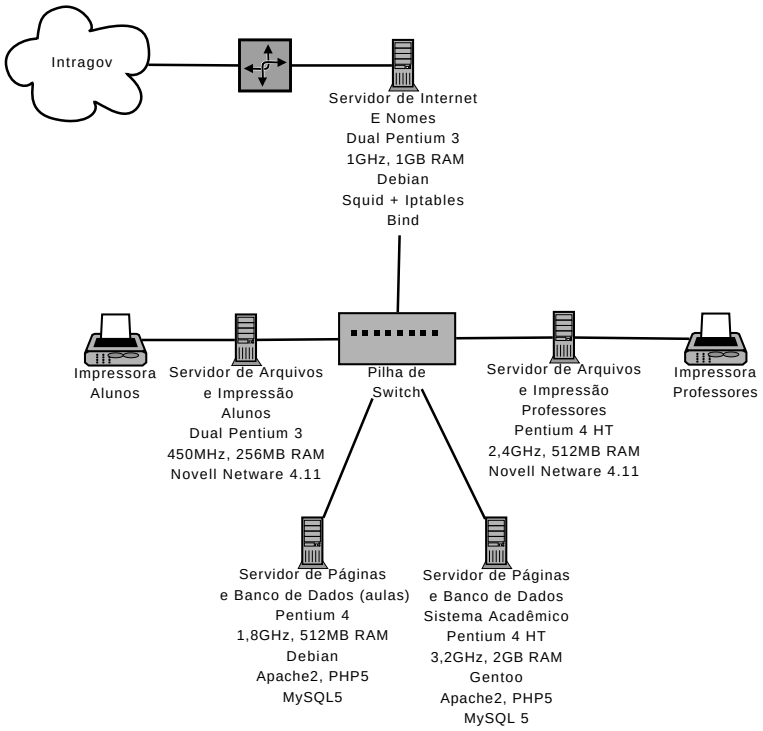

Figura 2.1: Diagrama da rede antiga

O servidor Novell Netware dos alunos estava em um hardware muito antigo, o que causava problemas de desempenho na rede. Era muito comum o servidor travar em momentos de pico de utilização.

Apesar do sistema Operacional Netware ser muito bom e oferecer muitos recursos, a versão utilizada não consegue utilizar muito bem o hardware atual, por isso havia a necessidade de atualizá-lo também.

[2]Serial Advanced Technology Attachment. Maiores detalhes em `http://www.infowester.com/serialata.php`

Na Fatec Ourinhos há um projeto de instalação de um novo link de Internet, o que irá possibilitar acesso externo aos serviços de Intranet. Para atender a nova demanda foi constatado também a necessidade de atualização do hardware dos servidores de Internet e de páginas.

2.2 Infra-Estrutura Nova

No início do ano de 2008 foram adquiridos três servidores Itautec dual Xeon de 1,6Ghz com 8GB de memória RAM e quatro discos rígidos SAS[3] de 140GB.

Um deles foi destinado inteiramente para o Samba, OpenLDAP e Cups. O segundo foi configurado com máquinas virtuais, tendo em uma o DNS e o DHCP e em outra o Proxy.

O terceiro foi reservado para configuração do servidor de páginas e banco de dados, sendo que a idéia inicial foi de configurar duas máquinas virtuais, uma para aulas e outra para o sistema acadêmico, mas isso ainda não foi feito.

A distribuição escolhida foi o Gentoo pela familiaridade do administrador da rede e pela possibilidade de compilar os pacotes otimizados para o hardware utilizado.

A figura 2.2 ilustra os servidores na nova estrutura.

2.3 Instalação dos servidores

Juntamente com os servidores foram adquiridos três no-breaks. Cada servidor tem três fontes redundantes, ou seja, se somente uma fonte estiver ligada, o servidor continua funcionando. Cada fonte foi ligada em um no-break para tentar garantir que eles nunca desliguem por problemas de energia.

Como dito anteriormente, os novos servidores têm quatro discos rígidos SAS, que foram configurados como RAID 5 por hardware. Quando configurado RAID por hardware, o sistema operacional detecta como se fosse um só disco rígido, ou seja, nenhuma configuração de software é necessária.

[3] Serial Attached SCSI. Maiores detalhes em http://en.wikipedia.org/wiki/Serial_Attached_SCSI

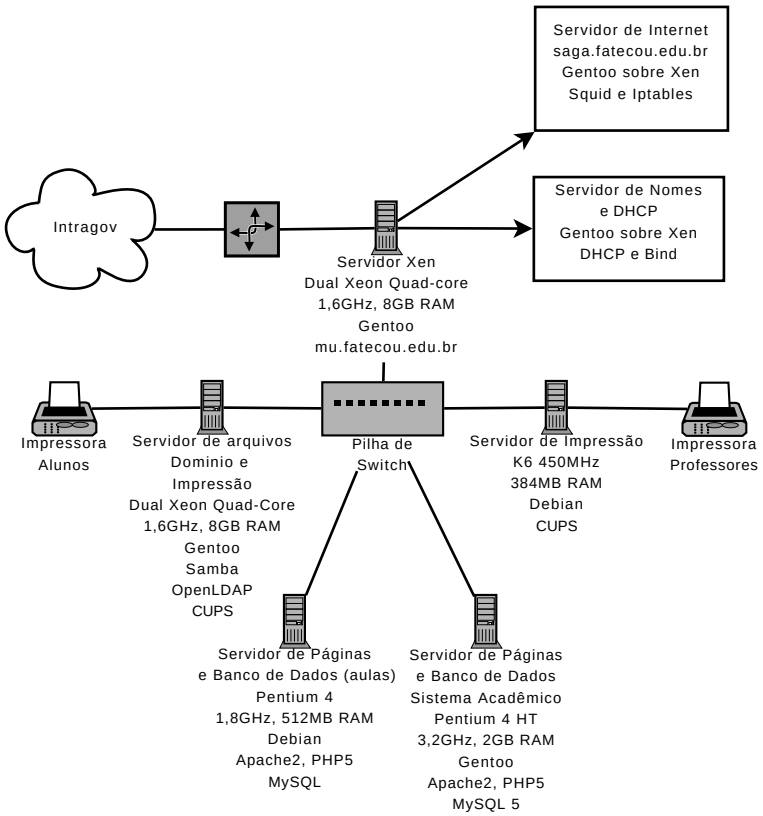

Figura 2.2: Diagrama da rede Nova

No RAID 5, os dados são gravados paralelamente em todos os discos, e o bit de paridade é gravado alternadamente entre os discos, conforme ilustra a figura 2.3[4]. Essa configuração foi escolhida pois o acesso de leitura é muito rápido. A capacidade dos discos é somada, mas perde-se a capacidade de um disco pela necessidade de gravação do bit de paridade.

Para configurar o RAID, logo após ligar o servidor, pressiona-se as teclas CTRL+H para entrar no utilitário SCSI da placa mãe. O utilitário é gráfico, e muito intuitivo, podendo ser operado facilmente.

[4]Disponível em http://pt.wikipedia.org/wiki/RAID

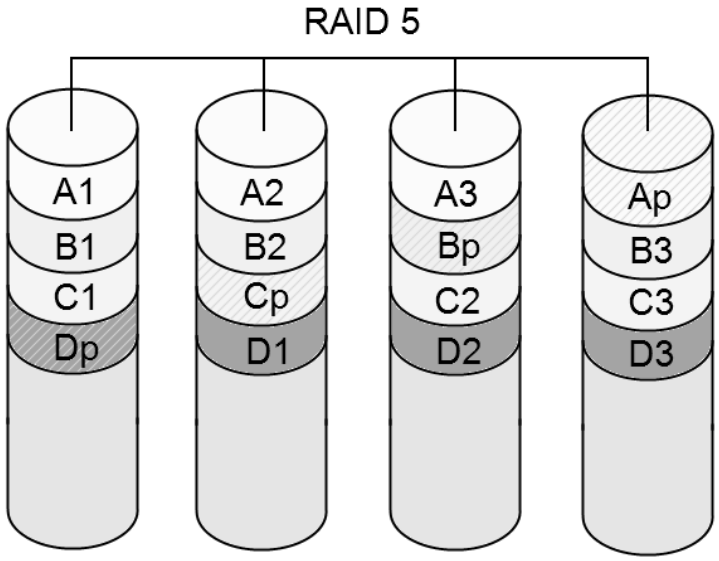

Figura 2.3: RAID 5: dados são divididos em todos os discos

2.4 Linux - Gentoo

Segundo (GENTOO.ORG, 2008), o Gentoo[5] é uma distribuição Linux que pode ser otimizada e customizada. Com a utilização do portage[6] pode-se adaptá-lo para ser utilizado como servidor, estação de trabalho, embarcado e outros. Por causa dessa adaptabilidade ele é considerado uma metadistribuição.

Além de um grupo de mais de trezentos desenvolvedores, o Gentoo tem um conselho global composto por 7 membros que decidem sobre questões globais, políticas e avanços do projeto.

A documentação é bem vasta e de boa qualidade. Além da documentação oficial disponível no site[7] há também o wiki[8] com várias dicas e tutoriais postados por usuários.

[5] http://gentoo.org
[6] Gerenciador de pacotes do Gentoo
[7] http://www.gentoo.org/doc/en/list.xml?desc=1
[8] http://gentoo-wiki.com/Main_Page

Para instalação estão disponíveis liveCD para várias arquiteturas[9].

A instalação do Gentoo é, na opnião do autor, a mais difícil atualmente entre as várias distribuições de Linux. Mas também, na opnião do autor, é a melhor do ponto de vista didático, pois todos os passos seguidos pelos instaladores de outras distribuições devem ser feitos manualmente, e o manual de instalação explica todos eles muito bem.

A instalação foi feita seguindo o manual de instalação do Gentoo(WIKI GENTOO, 2008b). Foi utilizado o mesmo arquivo `/etc/make.conf` em todos os servidores. A única excessão foi a máquina host do Xen, que exige parâmetros para a variável USE, conforme explicado no wiki(GENTOO HANDBOOK, 2008). Arquivo utilizado na figura 2.4.

```
CFLAGS="-O2 -pipe -march=nocona -mno-tls-direct-seg-refs"
# a opcao nptlonly e necessaria para o funcionamento do Xen
USE="nptlonly bash-completion -ipv6 hardened -cups"
CHOST="x86_64-pc-linux-gnu"
MAKEOPTS="-j9"
ACCEPT_KEYWORDS=~amd64
GENTOO_MIRRORS="http://gentoo.osuosl.org/ ftp://distro.ibiblio.org
    /pub/linux/distributions/gentoo/"
SYNC="rsync://rsync.samerica.gentoo.org/gentoo-portage"
```

Figura 2.4: make.conf utilizado

2.5 Ferramenta de pacotes Portage

O portage é a ferramenta de pacotes do Gentoo. Conforme explicado no manual de instalação(WIKI GENTOO, 2008b), ela é escrita em Python e Bash.

Durante a instalação do gentoo, um dos passos necessários é fazer o download e descompactar a árvore do portage. Esta árvore é uma coleção de ebuilds, que são arquivos que contém todas as informações necessárias para a manutenção do software. Os ebuilds ficam em `/usr/portage` por padrão.

A atualização da árvore do portage é feita normalmente por rsync[10] usando o comando `emerge --sync`. Na época da configuração dos servidores, o link de

[9] Alpha, amd64, hppa, ia64, ppc/ppc64, sparc, i386 e i686

[10] Ferramenta para transferência de arquivos incremental

Internet era centralizado na Intragov[11], que libera poucos serviços de Internet, e um dos serviços restritos é o rsync. Por isso é necessário fazer a atualização da árvore utilizando o comando `emerge-webrsync`, que faz o download de toda a árvore compactada e descompacta-a sobre a árvore atual.

Outra observação importante é que, se for fazer a atualização em uma rede que passe por um proxy que não é transparente, é necessário especificar qual é o proxy. Isso pode ser feito no arquivo `/etc/make.conf` conforme mostrado na figura 2.5 ou por linha de comando com o comando export conforme a figura 2.6. Caso o proxy seja autenticado pode-se informar o usuário e a senha como na figura 2.7.

```
#/etc/make.conf
#Especificacao do proxy
http_proxy = http_proxy=http://proxy.fatecou.edu.br:3128
ftp_proxy = http_proxy=http://proxy.fatecou.edu.br:3128
RSYNC_PROXY = http://proxy.fatecou.edu.br:3128
```

Figura 2.5: Configuracão do proxy no arquivo /etc/make.conf

```
mu ~ #export http_proxy=http://proxy.fatecou.edu.br:3128
mu ~ #export ftp_proxy=http://proxy.fatecou.edu.br:3128
mu ~ #export RSYNC_PROXY=http://proxy.fatecou.edu.br:3128
```

Figura 2.6: Especificação do proxy por comando

.

```
mu ~ \#export http_proxy=http://usuario:senha@proxy.fatecou.edu.br
    :3128
mu ~ \#export ftp_proxy=http://usuario:senha@proxy.fatecou.edu.br
    :3128
mu ~ \#export RSYNC_PROXY=http://usuario:senha@proxy.fatecou.edu.
    br:3128
```

Figura 2.7: Especificação de proxy com autenticação

2.5.1 Procurando por um pacote

Para procurar por um pacote usa-se o comando `emerge --search`. Para procurar na descrição do pacote usa-se o comando `emerge --searchdesc`. Ambos podem ser vistos nas figuras 2.8 e 2.9. A saída do comando `emerge --searchdesc`

[11] Intranet que interliga órgãos do governo estadual. `http://www.intragov.sp.gov.br/`

foi editada para reduzir a quantidade de linhas, mas como pode-se ver, os dois comandos retornam pacotes diferentes.

```
mu ~ # emerge --search samba
Searching...
[ Results for search key : samba ]
[ Applications found : 4 ]

*  app-admin/system-config-samba [ Masked ]
      Latest version available: 1.2.35
      Latest version installed: [ Not Installed ]
      Size of files: 184 kB
      Homepage:      http://fedoraproject.org/wiki/SystemConfig/
          samba
      Description:   Samba server configuration tool
      License:       GPL-2

*  net-fs/samba
      Latest version available: 3.0.32
      Latest version installed: 3.0.30
      Size of files: 21,413 kB
      Homepage:      http://www.samba.org/
      Description:   A suite of SMB and CIFS client/server
          programs for UNIX
      License:       GPL-3 oav? ( GPL-2 LGPL-2.1 )

*  net-misc/sambasentinel [ Masked ]
      Latest version available: 0.1
      Latest version installed: [ Not Installed ]
      Size of files: 18 kB
      Homepage:      http://kling.mine.nu/sambasentinel.htm
      Description:   SambaSentinel is a GTK frontend to smbstatus
      License:       GPL-2

*  sec-policy/selinux-samba
      Latest version available: 20080525
      Latest version installed: [ Not Installed ]
      Size of files: 328 kB
      Homepage:      http://www.gentoo.org/proj/en/hardened/
          selinux/
      Description:   SELinux policy for samba
      License:       GPL-2
```

Figura 2.8: Usando o search

```
mu ~ # emerge --searchdesc samba
Searching...
[ Results for search key : samba ]
[ Applications found : 14 ]

*  app-admin/system-config-samba [ Masked ]
      Latest version available: 1.2.35
      Latest version installed: [ Not Installed ]
      Size of files: 184 kB
      Homepage:      http://fedoraproject.org/wiki/SystemConfig/
          samba
      Description:   Samba server configuration tool
      License:       GPL-2

*  net-fs/samba
      Latest version available: 3.0.32
      Latest version installed: 3.0.30
      Size of files: 21,413 kB
      Homepage:      http://www.samba.org/
      Description:   A suite of SMB and CIFS client/server
          programs for UNIX
      License:       GPL-3 oav? ( GPL-2 LGPL-2.1 )

*  dev-db/ctdb [ Masked ]
      Latest version available: 9999
      Latest version installed: [ Not Installed ]
      Size of files: 0 kB
      Homepage:      http://ctdb.samba.org/
      Description:   A cluster implementation of the TDB database
          used by Samba and other projects to store temporary data
          .
      License:       GPL-3

*  dev-perl/Crypt-SmbHash
      Latest version available: 0.12
      Latest version installed: 0.12
      Size of files: 8 kB
      Homepage:      http://search.cpan.org/~bjkuit/
      Description:   LM/NT hashing, for Samba's smbpasswd entries
      License:       GPL-2
```

Figura 2.9: Usando o searchdesc

2.5.2 Instalando um Pacote

O portage é uma ferramenta de pacotes que resolve dependências. Depois de localizado, pode-se ver quais são elas e outras opções com o comando `emerge -pv pacote` conforme pode ser visto na figura 2.10.

```
mu ~ # emerge -pv bind

These are the packages that would be merged, in order:

Calculating dependencies... done!
[ebuild  N    ] net-dns/bind-9.5.0_p2-r1  USE="berkdb ssl -dlz -
    doc -idn -ipv6 -ldap -mysql -odbc -postgres -resolvconf -sdb-
    ldap (-selinux) -threads -urandom" 6,472 kB

Total: 1 package (1 new), Size of downloads: 6,472 kB
```

Figura 2.10: Opções para o pacote bind

O pacote será instalado com ou sem suporte às opções que aparecem dentro de USE=“ ”. No exemplo, o bind será instalado com suporte a berkdb e ssl, mas não ao mysql, postgres, etc., ou seja, o pacote não terá suporte às opções que forem precedidas por um hífen (-mysql).

Para ativar tal suporte pode-se proceder de duas maneiras. Passando o parâmetro por linha de comando como visto na figura 2.11 ou adicionando ao arquivo como na figura 2.12. Com isso, a opção não aparece mais com o hífen como antes.

```
taiga ~ # USE="mysql" emerge -pv bind

These are the packages that would be merged, in order:

Calculating dependencies... done!
[ebuild  N    ] net-dns/bind-9.5.0_p2-r1  USE="berkdb mysql ssl -
    dlz -doc -idn -ipv6 -ldap -odbc -postgres -resolvconf -sdb-
    ldap (-selinux) -threads -urandom" 6,472 kB

Total: 1 package (1 new), Size of downloads: 6,472 kB
```

Figura 2.11: Passando parâmetro na linha de comando

Caso a opção adicionada necessite de algum pacote que não esteja instalado no sistema, ele será instalado também como pode ser visto em 2.13, onde o pacote unixODBC listado para instalação também.

```
echo "net-dns/bind mysql" >> /etc/portage/package.use
```

Figura 2.12: Adicionando ao `/etc/portage/package.use`

```
taiga ~ # USE="mysql ipv6 odbc" emerge -pv bind

These are the packages that would be merged, in order:

Calculating dependencies... done!
[ebuild  N    ] dev-db/unixODBC-2.2.12  USE="-gnome -qt3" 2,740 kB
[ebuild  N    ] net-dns/bind-9.5.0_p2-r1  USE="berkdb ipv6 mysql
    odbc ssl -dlz -doc -idn -ldap -postgres -resolvconf -sdb-ldap
    (-selinux) -threads -urandom" 6,472 kB

Total: 2 packages (2 new), Size of downloads: 9,212 kB
```

Figura 2.13: Pacote instalado como dependência

Depois de definidas as opções, a instalação é feita com o comando `emerge bind`, que irá fazer o download dos códigos fontes do pacote, de suas dependências e de patchs que tenham sido disponibilizados para eles, e depois irá compilá-los e instalá-los.

Tal procedimento pode demorar dependendo da velocidade do link e do pacote a ser instalado. Normalmente, enquanto um pacote é compilado, não é feito o download de outro até que a compilação não termine. Para resolver isto pode-se colocar a opção `FEATURES="parallel-fetch"` no arquivo `/etc/make.conf` conforme o wiki (WIKI GENTOO, 2008a).

Outra opção que é imprescindível no casos dos servidores utilizados é definir quantas compilações paralelas poderão ser feitas, alterando ou adicionando o parâmetro `MAKEOPTS="-j9"` também ao arquivo `/etc/make.conf` , onde 9 é o número de núcleos/processadores do computador mais um, conforme explicado em (WIKI GENTOO, 2008b).

Caso o servidor tenha bastante memória RAM, pode-se montar o diretório onde os pacotes são compilados em memória, conforme pode ser visto em (WIKI GENTOO, 2009). É possível montar por linha de comando (conforme pode ser visto na figura 2.14) ou adicionar ao `/etc/fstab` (conforme a figura 2.15). Em ambos os casos, o diretório `/var/tmp/portage` serão montados em memória e terão 7GB. Se o parâmetro `size` for omitido, o diretório utilizará metade da

memória RAM. Deve-se tomar cuidado caso tenha-se pouca memória disponível, pois se o diretório ficar sem espaço, a compilação falhará.

```
mount -t tmpfs -o size=7GB,nr_inodes=1M tmpfs /var/tmp/portage
```

Figura 2.14: Montando um diretório em memória

```
echo "tmpfs /var/tmp/portage  tmpfs size=7GB,mode=0777,noauto  0
    0" >> /etc/fstab
```

Figura 2.15: Adicionando ao `/etc/fstab`

2.6 Virtualização

Ao contrário do que alguns pensam, o conceito de virtualização é antigo, mas só chegou aos desktops recentemente por falta de poder computacional. Conforme (NAVARRO, 2009), a IBM já utiliza virtualização em mainframes a muito tempo. A virtualização consiste em um software que cria ambientes onde pode-se executar outros sistemas operacionais independente do sistema hospedeiro.

Além da virtualização, há também a paravirtualização, onde o sistema operacional hospedeiro e o hóspede devem ser modificados para o funcionamento.

A paravirtualização provê uma maior performance de I/O, CPU e memória comparado com a virtualização total. A desvantagem é que não é possível executar um sistema operacional diferente do sistema hospedeiro. Mais informações sobre paravirtualização podem ser vistas em (ALKALAY, 2007) e (MATTOS; CARLOS, 2008)

Entre as vantagens da virtualização temos:

Consolidação de servidores: A consolidação de servidores trás muitas vantagens (IBM, 2009):

Economia de espaço: Pode-se colocar vários serviços em um mesmo servidor, mas como se estivessem em máquinas separadas.

Melhor utilização do hardware: Atualmente o poder de processamento está muito alto, e na maior parte do tempo o processador fica ocioso. Em

sistemas x86, a taxa de utilização do processador fica entre 5 a 10%. Hoje em dia, com os processadores com mais de um núcleo a virtualização é ainda mais beneficiada, pois nem todos os programas são feitos para utilizar multiprocessamento.

Economia de energia: Colocando-se vários serviços em um mesmo servidor, o consumo de energia diminui.

Aquecimento: Apesar de uma maior taxa de utilização dos processadores, o aquecimento gerado é menor do que se fossem utilizados vários servidores.

Segurança: Quando é necessário configurar vários serviços em um mesmo servidor, uma invasão por um desses serviços pode indisponibilizar todos os outros. Se cada serviço for configurado em uma máquina virtual diferente, uma invasão por um dos serviços não irá afetar os outros, a não ser que a máquina hospedeira seja invadida.

Independência de hardware: Dentro da máquina virtual, o hardware é sempre o mesmo. Pode-se copiar sua imagem de um servidor para outro, e nenhum ajuste será necessário nela.

2.6.1 Xensource

O Xen é um sistema de máquinas virtuais que utiliza paravirtualização. Um breve resumo de como o sistema de paravirtualização funciona pode ser visto em (XEN SOURCE, 2008).

O XenSource é um software OpenSource que atualmente é mantido pela Citrix, que também tem outros softwares para virtualização.

A configuração do Xen é bem mais complicada do que de outras máquinas virtuais como o VmWare ou o VirtualBox. A documentação utilizada foi a do (GENTOO HANDBOOK, 2008) e (VERMEULEN, 2008).

Para configurar o Xen no Gentoo são necessárias algumas modificações no sistema. A biblioteca glibc deve ser recompilada com a FLAG *-mno-tls-direct-seg-refs* no arquivo make.conf (`CFLAGS="-mno-tls-direct-seg-refs"`), pois ela conflita com o Xen em ambientes 32-bit x86, causando perda de performance em aplicativos multi-thead. Em ambientes 32 bits, todo o sistema deve ser recompilado, mas em ambientes 64 bits, pode-se recompilar somente a glibc. É necessário também verificar se o glibc foi compilado com a opção nptonly (`emerge -pv`

glibc). Em caso negativo, habilita-se a opção na variável USE (USE="nptonly"). Feito isso, recompila-se a biblioteca glibc (emerge glibc), ou o sistema todo, se o ambiente for 32 bits (emerge -evat world).

É necessário instalar três pacotes: o xen, o xen-tools e o xen-source. Para que o Xen inicie junto com o sistema deve-se adicionar o xend ao runlevel default (rc-update add xend default).

Caso os pacotes estejam mascarados, é necessário desmascará-los, adicionando-os ao arquivo /etc/portage/package.keywords, como pode ser visto na figura 2.16.

```
#vi /etc/portage/package.keywords
app-emulation/xen
app-emulation/xen-tools
sys-kernel/xen-sources
```

Figura 2.16: Adicionando os pacotes em /etc/portage/package.keywords

Feito isso, é só efetuar a instalação dos pacotes com o comando emerge xen xen-tools xen-source.

Como dito anteriormente, o Xen utiliza paravirtualização, portanto, tanto o sistema operacional hóspede como o hospedeiro devem ser modificados. Para isso deve-se compilar o kernel xen-source duas vezes, uma para criar a imagem do hospedeiro e uma para a imagem do hóspede. A configuração do kernel deve ser feita como em um sistema normal, mas alguns pontos devem ser levados em consideração:

- Assim como em outros sistemas de virtualização, é possível configurar o Xen para funcionar como NAT ou como bridge. Se for configurar como bridge, o sistema hospedeiro deve ter suporte a tal recurso.
- Tanto para o sistema hóspede como para o hospedeiro deve-se habilitar a opção de compatibilidade com o Xen.
- Para o sistema hóspede deve-se habilitar a opção Privileged Guest.
- Para o sistema hospedeiro, deve-se habilitar a opção LoopBack Device Support.

As opções extras de configuração do kernel do hospedeiro e do hóspede podem ser vistas na figuras 2.17 e 2.18 respectivamente.

```
Processor type and features  --->
      Subarchitecture Type (PC-compatible)  --->
                      Processor family (Intel EM64T)  --->
                  [*] Enable Xen compatible kernel

Networking --->
      Networking options --->
         TCP/IP networking
               <*> IP: tunneling
         <*> 802.1d Ethernet Bridging

Device Drivers  --->
      Block devices  --->
            <*> Loopback device support

XEN --->
      [*] Privileged Guest (domain 0)
      <*> Backend driver support
            <*>   Block-device backend driver
            <*>   Block-device tap backend driver
            <*>   Network-device backend driver
                  [  ]     Pipelined transmitter (DANGEROUS)
                  <*>     Network-device loopback driver
            <*>   PCI-device backend driver
                  PCI Backend Mode (Virtual PCI)  --->
                  [ ]     PCI Backend Debugging
            < >   TPM-device backend driver
      < > Block-device frontend driver
      < > Network-device frontend driver
      < > Framebuffer-device frontend driver
      [*] Scrub memory before freeing it to Xen
      [*] Disable serial port drivers
      <*> Export Xen attributes in sysfs
      Xen version compatibility (no compatibility code)  --->
```

Figura 2.17: Opções extras para a configuração do Hospedeiro

2.6.2 Instalando e configurando o Xen

O processo de instalação consiste na instalação dos pacotes (citados anteriormente), que são o xen, os fontes do kernel modificados para suporte ao Xen, e o xen-tools, que são as ferramentas para administração do serviço.

O kernel configurado para a máquina hospedeira (chamada de dom0) deve ser copiado dentro do diretório `/boot`, e o grub deve ser configurado para utilizá-lo,

```
Processor type and features  --->
      Subarchitecture Type (Xen-compatible)  --->

Bus options (PCI etc.)  --->
      [*] Xen PCI Frontend

XEN --->
      [ ] Privileged Guest (domain 0)
      < > Backend driver support
      <*> Block-device frontend driver
      <*> Network-device frontend driver
      <*> Framebuffer-device frontend driver
      <*>   Keyboard-device frontend driver
      [*] Scrub memory before freeing it to Xen
      [*] Disable serial port drivers
      <*> Export Xen attributes in sysfs
            Xen version compatibility (no compatibility code)
                --->
```

Figura 2.18: Opções extras para a configuração do Hóspede

conforme mostra a figura 2.19. O kernel compilado deve ser carregado como módulo, e o `xen.gz`, que é instalado junto com o pacote xen.

```
title  Xen 3.0 / Linux 2.6.x.y
root   (hd0,0)
kernel /boot/xen.gz
module /boot/vmlinuz-2.6.x.y-xen0 root=/dev/sda1
```

Figura 2.19: Configuração do menu.lst

A configuração do Xen é feita através do arquivo `/etc/xen/xend-config.sxp`. Nele é necessário definir qual script será usado para configurar a rede, como a rede será configurada (bridge ou nat), quanto de memória o hospedeiro irá utilizar e quantos CPU's serão utilizados pelas máquinas virtuais. Um exemplo dessas opções pode ser visto na figura 2.20.

O script network-multi foi criado para configurar as duas interfaces de rede. Conforme pode ser visto na figura 2.21, o script simplesmente executa o script network-bridge (que é instalado juntamente com o xend) passando como parâmetro cada uma das interfaces.

```
(xend-relocation-server yes)
(xend-relocation-hosts-allow '^localhost$ ^localhost\\.
    localdomain$')
(network-script 'network-route')
(vif-script vif-bridge)
(vif-script     vif-route)
(network-script 'network-multi')
# Dom0 will balloon out when needed to free memory for domU.
# dom0-min-mem is the lowest memory level (in MB) dom0 will get
    down to.
# If dom0-min-mem=0, dom0 will never balloon out.
(dom0-min-mem 196)
# In SMP system, dom0 will use dom0-cpus # of CPUS
# If dom0-cpus = 0, dom0 will take all cpus available
(dom0-cpus 0)
```

Figura 2.20: Arquivo de configuração xend-config.sxp

```
#!/bin/bash
sh /etc/xen/scripts/network-bridge start netdev=eth0
sh /etc/xen/scripts/network-bridge start netdev=eth1
```

Figura 2.21: Script de configuração network-multi

Após configurado, é necessário instalar o hóspede. Para isso deve-se criar o arquivo de imagem, formatá-lo, e iniciar o processo de instalação do Gentoo normalmente. Para ter acesso a imagem criada basta montá-la por loopback.

Para criar o arquivo de imagem utiliza-se o comando dd, definindo como parâmetro of, o arquivo que será criado. Por exemplo, para criar um arquivo chamado `image.img` dentro do diretório `/imagens`, com tamanho de 2GB, utiliza-se o comando `dd if=/dev/zero of=/imagens/image.img bs=1M count=2048`.

A formatação do arquivo é feita como em uma partição. Por exemplo, para formatar a imagem com o sistema de arquivos reiserfs, usa-se o comando `mkfs.reiserfs /imagens/image.img`. Qualquer parâmetro de formatação para alterar o desempenho do sistema de arquivos pode ser utilizado.

Para instalação do Gentoo, é necessário montar a partição e descompactar o stage e o portage. Para criar a máquina virtual isso também é feito, mas monta-se a imagem por loopback. Para montar a imagem criada acima no diretório `/mnt/gentoo`, usa-se o comando `mount -o loop /imagens/image.img /mnt/gentoo`.

Depois de descompactar o stage e o portage, é feito o chroot no diretório normalmente (`chroot /mnt/gentoo`), e todo o processo de instalação é feito como em um sistema normal. A diferença é o kernel, que deve ser compilado com as alterações citadas anteriormente, e ele não fica dentro da máquina virtual, ele é referenciado em seu arquivo de configuração.

No arquivo de configuração das máquinas virtuais é necessário definir o kernel que será usado, a quantidade de memória RAM, a quantidade de CPU's, as interfaces de rede, o nome do host, o tipo do disco rígido e onde ele está, em qual init a máquina irá iniciar. Um exemplo pode ser visto na figura 2.22.

```
kernel = "/xen/kernel/vmlinuz";
#ramdisk = "/xen/kernel/initrd.img";
memory = 512;
vcpus = 8;
vif = [ 'bridge=eth0', 'bridge=eth1' ];
name   = "aldebaran";
disk   = [ "file:/xen/imagens/gentoo_dns.img,xvda,w" ];
root   = "/dev/xvda ro";
extra = "3";
#vif = [ "ip=172.16.0.1" ];
#dhcp="dhcp";
on_poweroff = 'destroy'
on_reboot   = 'restart'
on_crash    = 'restart'
```

Figura 2.22: Exemplo de configuração da máquina virtual

2.7 Bonding

Conforme (DAVIS, 2000), o driver bonding permite que várias interfaces de rede sejam agregadas em uma única interface virtual. Essa agregação é feita para aumentar a velocidade e/ou disponibilidade e redundância do canal.

O bonding pode ser configurado de sete modos diferentes descritos abaixo:

balance-rr ou 0: Transmite pacotes em ordem sequencial, da primeira interface para a última. Este modo provê balanceamento de carga e tolerância a falhas.

active-backup ou 1: Apenas uma interface é ativada. Uma interface diferente é ativada se, e somente se, a interface atualmente ativa falhar. O MAC do

bond é visivel em apenas uma porta para evitar confundir o switch. Este modo provê tolerância a falhas.

balance-xor ou 2: Transmite baseado em um hash de política de transmissão, que pode ser alterado pela opção xmit_hash_police. Este modo provê balanceamento de carga e tolerância a falha.

broadcast ou 3: Transmite tudo em todas as interfaces. Provê tolerância a falhas.

802.3ad ou 4: IEEE 802.3ad Agregação dinâmica de link. Cria grupos de agregação que compartilham a mesma configuração de velocidade. O benefício oferecido depende da configuração.

balance-tlb ou 5: O tráfego de saída é distribuído de acordo com a demanda em cada interface. Tráfego de entrada é recebido pela interface atual. Se a interface que recebe falhar, outra interface recebe o MAC da interface receptora que falhou.

balance-alb ou 6: Inclui o balance-tlb mais balanceamento de carga na recepção.

Para a configuração do bonding é necessário a instalação do pacote ifenslave.

No arquivo de configuração da rede (`/etc/conf.d/net`) deve-se criar um bloco preup, e a interface que receberá endereço é a bond0, conforme pode ser visto na figura 2.23

```
#Arquivo de configuracao /etc/conf.d/net
#bloco que sera executado antes da configuracao da rede
preup() {
   if [[ ${IFACE} == "bond0" ]] ; then
      #especifica o modo em que o bond ira atuar
      BOND_MODE="balance-alb 6"
      #especifica a frequencia (em ms) de vefiricacao do link
      BOND_MIIMON="100"
      echo ${BOND_MODE} > /sys/class/net/bond0/bonding/mode
      echo ${BOND_MIIMON} > /sys/class/net/bond0/bonding/miimon
      einfo "Bonding mode is set to ${BOND_MODE} on ${IFACE}"
      einfo "MII monitor interval is set to ${BOND_MIINON} ms on $
          {IFACE}"
   else
      einfo "Doing nothing on ${IFACE}"
   fi
   return 0
}
#nao configura as interfaces eth0 e eth1
config_eth0=( "null" )
config_eth1=( "null" )
#define que as interfaces eth0 e eth1 farao parte da agregacao
slaves_bond0="eth0 eth1"
#define que a interface bond0 depende das interfaces eth0 e eth1
depend_bond0() {
   need net.eth0 net.eth1
   }
dns_domain="fatecou.edu.br"
#o restante da configuracao da rede e feito sobre a interface
    bond0
dns_servers_bond0="172.16.0.1"
config_bond0=( "172.16.0.4 netmask 255.255.0.0 broadcast
    172.16.255.255" )
routes_bond0=( "default via 172.16.0.2" )
```

Figura 2.23: Configuração da rede: arquivo `/etc/conf.d/net`

Capítulo 3

Configuração dos Serviços

Neste capítulo serão abordados os serviços que foram disponibilizados.

3.1 DHCP + DNS

Os serviços de DHCP[1] e o DNS[2] foram integrados para que funcionem como DNS dinâmico, ou seja, o DHCP atribui o endereço IP para a estação, e esta retorna o hostname para ser registrado no servidor DNS.

Para facilitar a depuração de erros deve-se ter certeza que ambos os serviços estejam funcionando corretamente antes de integrá-los.

3.1.1 DHCP

Segundo (WHATS, 2009), DHCP é um protocolo padrão de Internet com o qual um computador pode se conectar a uma rede local, pedindo as informações de configuração, e recebendo-a de um servidor, para se configurar como um membro daquela rede.

Como pode ser visto em (TLDP, 2009), pode-se configurar o servidor para atribuir IPs em determinada faixa, bem como a máscara de sub-rede, o endereço de

[1] Dinamic Host Configuration Protocol
[2] Domain Name System

broadcast, a rota padrão, o DNS, o domínio da rede, entre outras coisas, conforme pode ser visto na figura 3.1.

```
# Sample /etc/dhcpd.conf
default-lease-time 600;
max-lease-time 7200;
option subnet-mask 255.255.0.0;
option broadcast-address 172.16.255.255;
option routers 172.16.0.1;
option domain-name-servers 172.16.0.2;
option domain-name "fatecou.edu.br";
subnet 172.16.0.0 netmask 255.255.0.0
{
   range 172.16.1.0 172.1.255.254;
}
```

Figura 3.1: Arquivo de configuração dhcpd.conf

Para que o DHCP atualize a base do DNS, é necessário criar uma chave para que seja estabelecida uma relação de confiança entre os dois serviços. Além disso, é preciso adicionar infomações da zona DNS que será atualizada, e adicionar suporte a DDNS[3] na configuração. Um arquivo de exemplo pode ser visto na figura 3.2.

3.1.2 DNS Bind

Segundo (ALBITZ; LIU, 2001), DNS[4] é um banco de dados distribuído utilizado para traduzir nomes de domínio em endereços IP.

No início da ARPANET, o número de hosts era relativamente pequeno, por isso era possível guardar essa informação em um arquivo de hosts[5]. Mas com o rápido crescimento das redes, manter tais arquivos atualizados tornou-se praticamente impossível. Com isso criou-se um serviço com administração descentralizada, que permitisse que um administrador local atualizasse os dados relativos ao seu domínio. O DNS utiliza um sistema de árvore, que é dividida em sub-domínios, e cada sub-domínio é administrado por uma organização.

[3] Dinamic DNS
[4] Domain Name System
[5] `/etc/hosts`, no UNIX ou `c:\windows\system32\drivers\etc\hosts` no Windows

```
#Linhas adicinais para o DDNS
ddns-updates                on;
ddns-update-style           interim;
ddns-domainname             "fatecou.edu.br.";
ddns-rev-domainname         "in-addr.arpa.";
ignore                      client-updates;
include                     "/etc/bind/rndc.key";
# This is the communication zone
zone fatecou.edu.br.
{
    primary 127.0.0.1;
    key rndc-key;
}

zone    0.16.172.in-addr.arpa.
{
   primary 172.16.0.2;
   key             "rndc-key";
}
zone    fatecou.edu.br.
{
   primary 172.16.0.1;
   key             "rndc-key";
}
```

Figura 3.2: Arquivo de configuração dhcpd.conf com DDNS

O Bind[6] é uma implementação do protocolo DNS escrita para o sistema operacional Unix BSD 4.3 de Berkeley, e hoje é mantido pelo Internet Software Consortium[7].

A configuração do Bind é feita no arquivo `/etc/bind/named.conf`, onde deve-se especificar o(s) arquivo(s) de zona(s) que o servidor irá administrar. Um exemplo pode ser visto em 3.3.

Na configuração das zonas (`zone "16.172.in-addr.arpa."` e `zone "fatecou.edu.br."`) deve-se colocar a chave criptográfica, como na configuração do DHCP.

Também na configuração das zonas, as linhas que iniciam com `file` especificam os arquivos de zona. Na figura 3.3, temos a zona direta e a zona reversa para o domínio fatecou.edu.br.

[6]Berkeley Internet Name Domain

[7]https://www.isc.org/software/bind

```
include "/etc/bind/rndc.key";
logging
{
   category lame-servers{null;};
   category edns-disabled{null;};
};
options
{
   directory "/var/bind";
   listen-on-v6 { none; };
   pid-file "/var/run/named/named.pid";
};
zone "." IN {
   type hint;
   file "named.ca";
};
zone "localhost" IN {
   type master;
   file "pri/localhost.zone";
   allow-update { none; };
   notify no;
};
zone "127.in-addr.arpa" IN {
   type master;
   file "pri/127.zone";
   allow-update { none; };
   notify no;
};
zone "fatecou.edu.br." {
   type master;
   allow-update { key "rndc-key"; 127.0.0.1; };
   file "pri/fatecou.edu.br.db";
};
zone "16.172.in-addr.arpa." {
   type master;
   allow-update { key "rndc-key"; 127.0.0.1; };
   file "pri/fatecou.edu.br.rev.db";
};
```

Figura 3.3: Arquivo de configuração `/etc/bind/named.conf`

Os arquivos de zona direta e reversa podem ser vistos respectivamente em 3.4 e 3.5.

```
$ORIGIN .
$TTL 259200 ; 3 days
fatecou.edu.br    IN SOA   fatecou.edu.br. hostmaster.fatecou.edu.
    br. (
             2002031502 ; serial
             28800      ; refresh (8 hours)
             7200       ; retry (2 hours)
             604800     ; expire (1 week)
             86400      ; minimum (1 day)
             )
          NS aldebaran.fatecou.edu.br.
$ORIGIN fatecou.edu.br.
aldebaran       A  172.16.0.1
$TTL 3000   ; 50 minutes
aries        A  172.16.222.45
mu        A  172.16.222.44
```

Figura 3.4: Arquivo de zona direta `/etc/bind/pri/fatecou.edu.br.db`

```
$ORIGIN .
$TTL 259200 ; 3 days
16.172.in-addr.arpa  IN SOA   fatecou.edu.br. hostmaster.fatecou.
    edu.br. (
             2002031502 ; serial
             28800      ; refresh (8 hours)
             7200       ; retry (2 hours)
             604800     ; expire (1 week)
             86400      ; minimum (1 day)
             )
          NS aldebaran.fatecou.edu.br.
$ORIGIN 16.172.in-addr.arpa.
1.0          PTR   aldebaran.fatecou.edu.br.
$ORIGIN 222.16.172.in-addr.arpa.
$TTL 3000   ; 50 minutes
44        PTR   mu.fatecou.edu.br.
45        PTR   aries.fatecou.edu.br.
```

Figura 3.5: Arquivo de zona reversa `/etc/bind/pri/fatecou.edu.br.rev.db`

Uma observação importante deve ser feita ao configurar a zona reversa. No arquivo de zona, o endereço IP deve ser invertido caso a origem seja 16.172, como pode ser visto na figura 3.6, onde o host *aldebaran.fatecou.edu.br* tem o IP 172.16.0.1.

```
$ORIGIN 16.172.in-addr.arpa.
1.0         PTR   aldebaran.fatecou.edu.br.
$ORIGIN 222.16.172.in-addr.arpa.
$TTL 3000   ; 50 minutes
44        PTR   mu.fatecou.edu.br.
45        PTR   aries.fatecou.edu.br.
```

Figura 3.6: Trecho do arquivo e zona reversa

Após integrar os serviços, ambos os arquivos devem ser atualizados quando uma estação requisitar endereço IP. Em caso de estações linux, é necessário alterar o arquivo de configuração do cliente dhcp `/etc/dhcp3/dhclient.conf` e adicionar a seguinte linha: `send host-name "estacao-01";`.

3.2 LDAP

3.2.1 Serviço de diretórios

Segundo (OPENLDAP FOUDATION, 2008), um diretório é um banco de dados hierárquico otimizado para consulta. Nele pode-se armazenar vários tipos de objetos e seus atributos.

O LDAP (Lightweight Directory Access Protocol) é o protocolo utilizado para acessar o serviço de diretórios baseados em X.500. O LDAP roda sobre a pilha TCP/IP e utiliza pouco recurso computacional, diferente de seu antecessor DAP, que rodava sobre a pilha OSI e utilizava muito recurso computacional.

Entre as várias implementações do LDAP temos:

- e-Directory[8] (antigo NDS), da Novell.
- Active Directory[9], da Microsoft.
- OpenLDAP[10], da OpenLDAP Foundation.
- Apache Directory Server[11], da Apache Software Foundation.

[8] http://www.novell.com/products/edirectory/

[9] http://www.microsoft.com/windowsserver2003/technologies/directory/activedirectory/default.mspx

[10] http://www.openldap.org/

[11] http://directory.apache.org/

- Red Hat Directory Server[12], da Red Hat.
- 389 Directory Server[13], do Fedora Project.
- Sun Java System Directory Server[14], da Sun Microsystem.

Atualmente muitos aplicativos aceitam a autenticação em bases LDAP. Com isso podemos centralizar o gerenciamento de usuários, o que facilita para o administrador e para o usuário, que só precisa decorar uma única senha.

O LDAP cria uma hierarquia em árvore, conforme pode ser visto na figura 3.7. Pode-se organizar as árvores de duas maneiras: no estilo X.500 ou no estilo DNS.

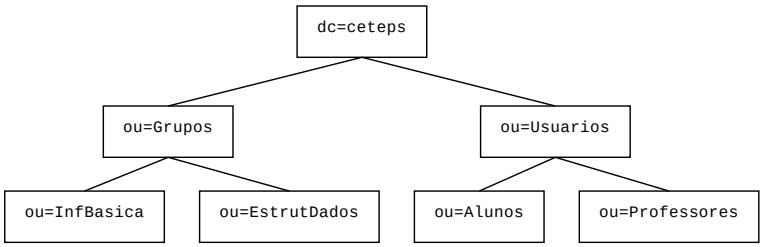

Figura 3.7: Exemplo de árvore de diretórios estilo DNS

O estilo X.500 é baseado em regiões, e os primeiros níveis da árvore referenciam-se ao país ou os estados, e depois as cidades, e só depois a organização e departamentos, conforme pode ser visto na figura 3.8.

Segundo (TRIGO, 2007), o padrão X.500 foi criado antes da Internet, e o formato de árvore X.500 não permite o correto funcionamento de um serviço de diretórios distribuído.

Para resolver este problema, criou-e a estrutura baseada em nomes domínio de DNS. Nesse formato, o primeiro nível da árvore é a organização, seguido de seus departamentos, conforme pode ser visto a figura 3.7.

3.2.2 OpenLDAP

A instalação do OpenLDAP tem algumas dependências, listadas abaixo:

[12] http://www.br.redhat.com/products/infrastructure/directory_server/
[13] http://directory.fedoraproject.org/
[14] http://www.sun.com/software/products/directory_srvr_ee/dir_srvr/index.xml

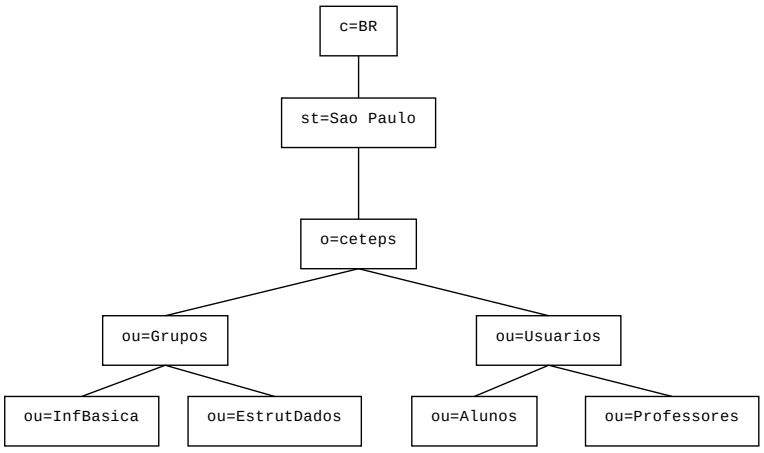

Figura 3.8: Exemplo de árvore de diretórios em estilo X.500

BerkeleyDB: O LDAP é apenas o protocolo de comunicação. Para armazenar as informações, deve-se utilizar uma base, chamada de backend. Esse backend pode ser até mesmo um banco de dados relacional. Nativamente, o OpenLDAP suporta o LDBM e o BerkeleyDB. Nesta solução, foi utilizado o BerkeleyDB.

OpenSSL: Utilizado para gerar as chaves criptográficas para criptografar a conexão entre o cliente e o servidor OpenLDAP.

Cyrus-Sasl : Mecanismo de autenticação que utiliza o OpenSSL para criptografar a conexão entre o cliente e o servidor OpenLDAP.

No Gentoo, o OpenLDAP irá criar o diretório `/etc/openldap`, onde ficam os arquivos do servidor e do cliente OpenLDAP. O arquivo do servidor é o slapd.conf, e o arquivo utilizado na solução pode ser visto na figura 3.9

Alguns parâmetros são obrigatórios, entre eles:

database hdb: Define o backend que será usado;

suffix "dc=ceeteps": Define qual será a raíz da árvore LDAP;

rootdn "cn=root,dc=ceeteps": Define o nome do usuário administrador da base LDAP;

rootpw: Define a senha do usuário administrador da base LDAP;

```
allow bind_v2
include     /etc/openldap/schema/core.schema
include     /etc/openldap/schema/cosine.schema
include     /etc/openldap/schema/nis.schema
include     /etc/openldap/schema/misc.schema
include     /etc/openldap/schema/inetorgperson.schema
include     /etc/openldap/schema/samba.schema
schemacheck on
pidfile     /var/run/openldap/slapd.pid
argsfile /var/run/openldap/slapd.args
loglevel 256
modulepath  /usr/lib64/openldap/openldap
moduleload  back_hdb.so
database hdb
suffix      "dc=ceeteps"
checkpoint  256   5 # <kbyte> <min>
rootdn      "cn=root,dc=ceeteps"
rootpw      {SSHA}qJMHzLA9hiQNa4pAOLNbFW+pcHVyRE
password-hash {SSHA}
directory   /var/lib/openldap-data
index cn,sn,uid,displayName            pres,sub,eq
index memberUID,mail,givenname         eq,subinitial
index objectClass,uidNumber,gidNumber        eq
index sambaSID,sambaPrimaryGroupSID,sambaDomainName   eq
index uniqueMember,entryCSN,entryUUID        eq
lastmod on
access to attrs=sambaLMPassword,sambaNTPassword,userPassword,
    sambaPasswordHistory,sambaPwdLastSet
   by dn="cn=root,dc=ceeteps" write
   by anonymous auth
   by self write
   by * none

access to dn.base="" by * read

access to *
   by dn="cn=root,dc=ceeteps" write
   by * read

TLSCipherSuite HIGH:MEDIUM:+SSLv2:RSA
TLSCertificateFile /etc/openldap/certs/servercrt.pem
TLSCertificateKeyFile /etc/openldap/certs/serverkey.pem
TLSCACertificateFile /etc/openldap/certs/cacert.pem
```

Figura 3.9: Arquivo de configuração `/etc/openldap/slapd.conf`

directory /var/lib/openldap-data: Define onde será criada a base LDAP;

Com o serviço configurado, é possível iniciá-lo. Para ver se ele está executando, pode-se utilizar o comando nmap, que deve mostrar a porta 389 aberta (e, se for configurado a criptografia, irá abrir também a porta 636).

3.2.3 LDIF

Após configurado serviço, é necessário povoar a base. É necessário criar pelo menos a raíz da árvore através de um arquivo LDIF (LDAP Data Interchange Format).

Segundo (RFC2849, 2000), LDIF é um formato usado para transferir informação para o diretório; ou uma descrição das alterações feitas nas entradas do diretório. O arquivo LDIF consiste em uma série de registros separados por uma linha em branco. Um registro consiste em uma sequência de linhas descrevendo uma série de alterações em uma entrada do diretório. Um arquivo LDIF especifica uma série de entradas no diretório ou uma série de alterações a serem aplicadas nas entradas do diretório, mas não ambas. O arquivo LDIF com a base utilizada na Fatec pode ser visto na figura 3.10.

```
dn: dc=ceeteps
objectClass: top
objectClass: dcObject
objectClass: organization
dc: ceeteps
o: Centro Estadual de Educacao Tecnologica Paula Souza
```

Figura 3.10: Arquivo ceeteps.ldif

Com a raíz da árvore criada pode-se povoar a base com alguma interface de administração como o PhpLDAPAdmin[15], ou pode-se criar um arquivo LDIF com as entradas necessárias. Um exemplo de um arquivo LDIF com um usuário pode ser visto na figura 3.11

[15] http://phpldapadmin.sourceforge.net/wiki/index.php/Main_Page

3.2.4 Comandos básicos

Para a administração do OpenLDAP, temos alguns comandos básicos que são importantes, entre os quais temos:

ldapadd: Usado para adicionar informações na base.

Ex.: ldapadd -f usuario.ldif -x -D “cn=Administrator,dc=ceeteps” -W

Onde:

-f usuario.ldif: especifica o arquivo que será incluído.

-x: Utiliza autenticação simples.

-D “cn=Administrator,dc=ceeteps”: Usuário utilizado para acesso a base.

-W: Chama um prompt para a digitação da senha.

ldapdelete: Usado para apagar registros da base.

Ex.: ldapdelete -x -v -W -D “cn=Administrator,dc=ceeteps” \
“uid=ruy.takata,ou=Docentes,ou=Usuarios,dc=ceeteps”

Onde:

-x: Utiliza autenticação simples.

```
dn: uid=ruy.takata,ou=Docentes,ou=Usuarios,dc=ceeteps
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: shadowAccount
cn: Ruy
sn: Takata
givenName: Ruy Takata
uid: ruy.takata
uidNumber: 1075
gidNumber: 513
homeDirectory: /home/ruy.takata
loginShell: /bin/bash
gecos: Ruy Minoru Ito Takata
mail: ruy.takata@email.com.br
userPassword: {SSHA}OCW8lXA8pUPUhTDBxzJMhQm7/BtDRT
```

Figura 3.11: Arquivo ldif com um usuário

-D “cn=Administrator,dc=ceeteps”: Usuário utilizado para acesso a base.

-W: Chama um prompt para a digitação da senha.

“uid=ruy.takata,ou=Docentes,ou=Usuarios,dc=ceeteps”: entrada que será apagada.

ldapmodify: Usado para alterar campos da base. A utilização é igual ao ldapadd, bastando apenas fazer as alterações necessárias no arquivo ldif.

ldappasswd: Para alterar a senha de um usuário que está na base LDAP.

Ex.: ldappasswd -x -W -D “cn=Administrator,dc=ceeteps” \
“uid=ruy.takata,ou=Docentes,ou=Usuarios,dc=ceeteps” -A -S

Onde:

-x: Utiliza autenticação simples.

-D “cn=Administrator,dc=ceeteps”: Usuário utilizado para acesso a base.

-W: Chama um prompt para a digitação da senha.

“uid=ruy.takata,ou=Docentes,ou=Usuarios,dc=ceeteps”: usuário cuja senha será alterada.

-A: Chama um prompt para a senha antiga. Pode-se utilizar o parâmetro -a seguido da senha.

-S: Chama um prompt para a senha nova. Pode-se utilizar o parâmetro -s seguido da senha.

ldapsearch: Para efetuar buscas na base LDAP.

Ex.: ldapsearch -x -D “cn=Administrator,dc=ceeteps” -W \
-b “dc=ceeteps” “(objectClass=*)”

Onde:

-x: Utiliza autenticação simples.

-D “cn=Administrator,dc=ceeteps”: Usuário utilizado para acesso a base.

-W: Chama um prompt para a digitação da senha.

-b “dc=ceeteps”: base onde será efetuada a busca. Caso saiba em que parte da árvore está o objeto a ser procurado, pode-se tornar a busca mais específica: “ou=Docentes,ou=Usuarios,dc=ceeteps”

“(objectClass=*)”: filtro utilizado na busca. Nesse caso, ele irá retornar tudo o que for encontrado. Outros tipos de filtros que podem ser utilizados:

atributo=valor: sn=Takata, ou uid=ruy.takata

atributo∼=valor: mail=ruy. Isso irá retornar todos os e-mails que contenham ruy.takata, podendo ser ruy@email.com, ruy.takata@email.com.br, ruy.takata@ufla.edu.br, takata.ruy@email.com.br

atributo<=valor: sn<=Takata, retornará todas as entradas cujo sn sejam alfabéticamente menores ou iguais a Takata.

atributo>=valor: sn>=Takata, retornará todas as entradas cujo sn sejam alfabéticamente maiores ou iguais a Takata.

***:** o asterisco é o coringa, e representa substrings. Uma buscar uid=ru-*.takata irá retornar ruy.takata, rui.takata. Mas como representa substring, também irá retornar rubens.takata, caso ela exista.

slapcat: Lista o conteúdo da base, e pode ser utilizado para fazer um backup da base.

Ex.: slapcat -b "ou=Usuarios,dc=ceeteps" -l backup.ldif

Onde:

-b "ou=Usuarios,dc=ceeteps": base que será listada. Se esse parâmetro for suprimido, toda a base será listada.

-l backup.ldif: arquivo onde será feito o backup. Se não for especificado, a base é listada na tela.

No comando slapcat não é necessário especificar o usuário que fará a consulta na base pois é um comando de superusuário, e essa consulta é feita como um usuário administrador do LDAP. O comando ldapsearch por sua vez, fará uma pesquisa anônima caso o usuário não seja especificado com o parâmetro -D, e caso o usuário seja especificado, fará uma consulta com a permissão desse usuário. Essas permissões podem ser alteradas utilizando-se ACL's, que serão tratadas mais adiante.

slapindex: Recria os índices da base de dados. Os índices são utilizados para otimizar as buscas, e devem ser recriados periodicamente caso a base sofra muitas alterações.

slappasswd: Usado para gerar uma senha criptografada. Pode-se especificar qual criptogafia será utilizada com o parâmetro -h. Esse comando pode ser utilizado para gerar a senha criptografada para arquivos ldif ou para o arquivo de configuração do servidor slapd.conf.

Ex:. slappasswd -h SSHA

Além desses, existem mais alguns comandos que podem ser encontrados em (TRIGO, 2007), e em (OPENLDAP FOUDATION, 2008).

3.2.5 SSL-TLS

Para aumentar a segurança pode-se configurar o OpenLDAP para aceitar conexões criptografadas. Isso é possível com o OpenSSL. O OpenSSL é uma implementação livre dos protocolos SSL[16] e TLS[17]. Segundo (VERISIGN, 2009), o protocolo SSL habilita criptografia durante as transações. Isso é feito usando duas chaves, uma pública (usada para criptografar os dados) e uma privada (usada para descriptografar). O protocolo TLS é baseado no SSL, mas eles não são compatíveis. A diferença está no handshake inicial, e também pelo TLS ser mais extensível.

3.2.5.1 Criando o certificado

O certificado utilizado pode ser auto-assinado, e pode-se usar qualquer ferramenta para criá-lo. A única atenção especial durante o preenchimento das informações é o Common Name, que deve ser igual ao resultado do comando `hostname` do servidor.

Abaixo um exemplo de como gerar a chave, criar uma CA[18] para assiná-lo, e assinar o certificado.

```
# openssl req -newkey rsa:1024 -nodes -out newreq.pem -keyout
newreq.pem -days 365

# /usr/lib/ssl/misc/CA.sh -newca

# /usr/lib/ssl/misc/CA.sh -sign
```

Serão necessários os arquivos cacert.pem, servercert.pem e serverkey.pem, que poderão copiados para o diretório do openldap para facilitar a configuração.

```
# mkdir /etc/openldap/certs

# cp demoCA/cacert.pem /etc/openldap/certs

# cp newcert.pem /etc/openldap/certs/servercert.pem
```

[16] Secure Sockets Layer
[17] Transport Layer Security
[18] Certificate Authority - Autoridade de Certificados

```
# cp newreq.peq /etc/openldap/certs/serverkey.pem

# chmod 400 /etc/openldap/certs/serverey.pem
```

O arquivo de configuração slapd.conf deve ser alterado, adicionando as linhas conforme a figura 3.12.

```
TLSCipherSuite HIGH:MEDIUM:+SSLv2:RSA
TLSCertificateFile /etc/openldap/certs/servercert.pem
TLSCertificateKeyFile /etc/openldap/certs/serverkey.pem
TLSCACertificateFile /etc/openldap/certs/cacert.pem
```

Figura 3.12: Linhas que devem ser adicionadas ao arquivo `/etc/openldap/slapd.conf`

Para que o slapd seja iniciado com suporte a SSL, deve-se alterar o arquivo `/etc/conf.d/slapd`, e alterá-lo conforme a figura 3.13. Feito isso, pode-se verificar se a porta 636 está aberta.

```
OPTS="-h 'ldaps:// ldap://'"
```

Figura 3.13: Linha que devem ser alterada em `/etc/conf.d/slapd`

3.3 Servidor de Domínio e de Arquivos

3.3.1 Samba

Segundo (TRIGO, 2007), o Samba foi desenvolvido por Andrew Tridgell, e tinha como objetivo compartilhar arquivos entre os sistemas operacionais DOS e UNIX.

Atualmente, com o Samba é possível construir servidores de domínio[19] para redes Windows. Com o domínio, o usuário deve autenticar-se na rede para ter acesso aos seus recursos.

Conforme citado na introdução, um dos motivos da escolha do Samba foi sua performance. Conforme pode ser visto na figura 3.14, a taxa de transferência do Windows 2003 para de aumentar depois que ultrapassa oito clientes.

Outra análise comparativa entre o Samba e o Windows 2003 pode ser visto em 3.15, onde o resultado mostra que o Samba tem um desempenho inferior.

[19] PDC - Primary Domain Controller, e BDC - Backup Domain Controller

Segundo (BARR, 2003), essa diferença de resultados deve-se ao fato de, no teste realizado pela Veritest, a configuração escolhida não é a melhor para o Linux. O servidor foi configurado com o sistema de arquivos ext3 e os discos foram dispostos em RAID0. A melhor opção seria sistema de arquivos XFS e RAID5.

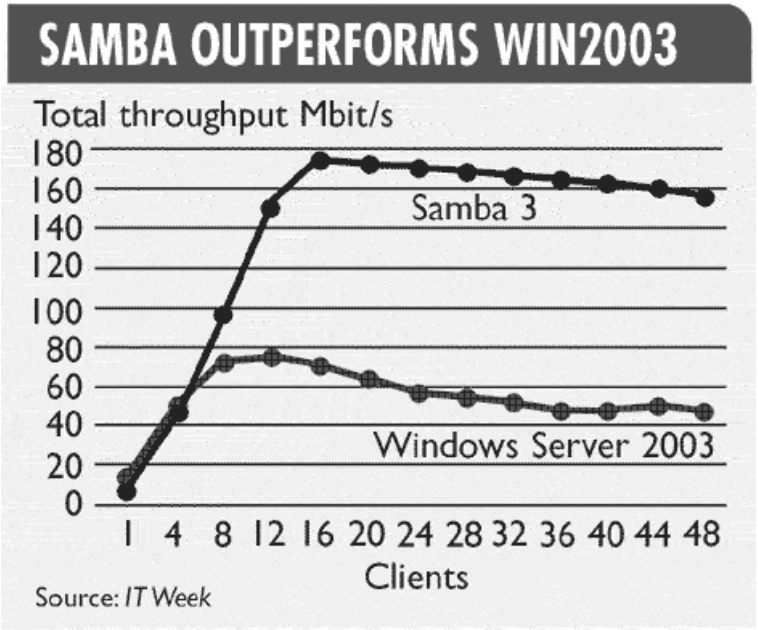

Figura 3.14: Taxa de transferência: Samba x Windows. Retirada de `http://www.kegel.com/nt-linux-benchmarks.html`

A integração com o LDAP facilita a replicação e a distribuição da base de senhas, segundo (VERNOIJ; TERPSTRA; CARTER, 2007).

A instalação do Samba foi feita usando o emerge, mas algumas USE's foram alteradas. Para facilitar as atualizações, o arquivo `/etc/portage/package.use` foi alterado conforme a figura 3.16. As principais alterações foram adicionar suporte a ldap, ao samba, ao ssl e ao sasl para alguns pacotes.

3.4 Servidor de Domínio

Conforme (VERNOIJ; TERPSTRA; CARTER, 2007), o samba pode ser configurado como servidor de domínios, substituindo do servidor Windows NT4.

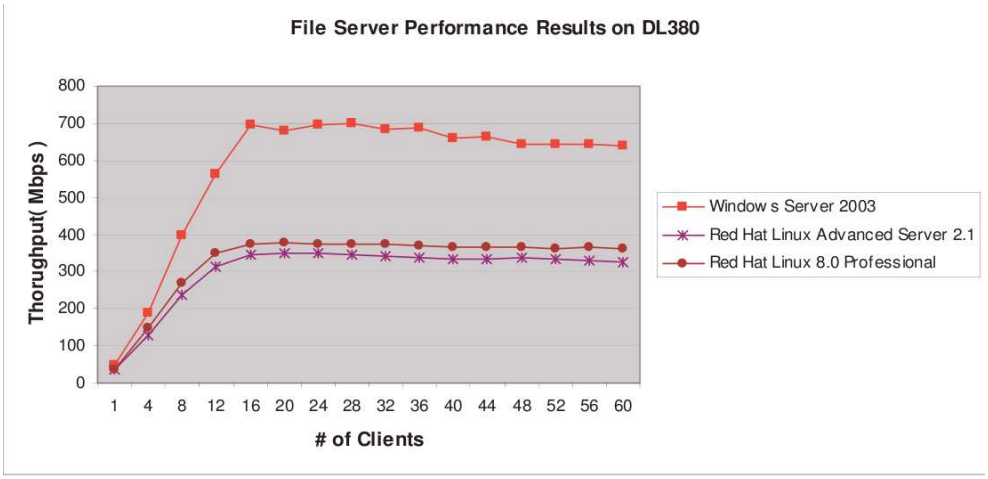

Figura 3.15: Taxa de transferência: Samba x Windows. Retirada de (VERITEST, 2003)

```
app-admin/eselect bash-completion -doc vim-syntax"
net-misc/openssh pam tcpd -X -X509 -hpn -kerberos ldap -libedit
media-libs/tiff zlib -jbig jpeg -nocxx
app-text/poppler zlib -cjk jpeg
net-print/cups acl nls pam perl python ssl -X -avahi -dbus java
    jpeg -kerberos ldap -php png ppds samba -slp -static tiff -
    zeroconf
app-text/ghostscript-gpl cups -X -bindist -cjk -djvu -gtk jpeg2k
net-fs/samba  acl cups pam python readline -ads async automount -
    caps doc examples -fam -ipv6 ldap quotas selinux swat syslog
    winbind LINGUAS="pt_BR"
net-nds/openldap  berkdb crypt gdbm perl ssl tcpd -debug -ipv6 -
    kerberos -minimal -odbc -overlays samba sasl selinux -slp -
    smbkrb5passwd
dev-perl/perl-ldap sasl
sys-auth/nss_ldap -debug -kerberos sasl
sys-auth/pam_ldap ssl sasl
```

Figura 3.16: Arquivo de `/etc/portage/package.use`

Para realizar tal configuração, basta adicionar algumas linhas ao arquivo de configuração do samba, conforme pode ser visto na figura 3.17.

Ao se configurar o samba como servidor de domínios, é possível armazenar na rede o perfil dos usuários, mas isso não foi implementado porque isso aumenta o tráfego na rede, e necessita de espaço em disco adicional no servidor.

```
[global]
   domain logons = Yes
   os level = 65
   local master = yes
   preferred master = Yes
   domain master = Yes
   wins support = Yes
```

Figura 3.17: Arquivo de `/etc/samba/smb.conf`

3.4.1 Integração com OpenLDAP

Para a integração com o OpenLDAP, foi utilizado o pacote smbldap-tools[20].

Após instalado, deve-se configurar os dois arquivos dentro de `/etc/smbldap-tools`. No arquivo smbldap.conf é necessário informar, além da localização do servidor LDAP, informações sobre o domínio Samba. No arquivo `smbldap_bind.conf`, é necessário informar qual o usuário administrador do LDAP.

O arquivo `/etc/openldap/slapd.conf` também deve ser alterado para que o esquema do samba seja carregado, e o servidor Ldap reconheça os campos necessários.

Uma informação obrigatória é o SID[21]. (MICROSOFT, 2008), define o SID como um valor exclusivo de tamanho variável que é usado em toda rede Windows. Segundo (VERNOIJ; TERPSTRA; CARTER, 2007), todos os computadores de uma rede Windows (servidores e estações de trabalho), usuários e grupos têm seu respectivo SID.

Para obter o SID, deve-se utilizar o comando `net getlocalsid`, conforme a figura 3.18

```
taiga:~# net getlocalsid
SID for domain TAIGA is: S-1-5-21-1654563363-510176204-240461965
```

Figura 3.18: Obtendo o SID

Além do SID, o sufixo da árvore Ldap deve ser informado corretamente para que a integração funcione. Feito isso, é possível utilizar os scripts disponibilizados pelo pacote.

[20] `https://gna.org/projects/smbldap-tools/`
[21] Security Identifier

O primeiro que deve ser executado é o `smbldap-populate`, que irá popular a base Ldap com os objetos necessários para o Samba. É recomendado gerar um arquivo ldif ao invés de adicionar diretamente no Ldap. Isso possibilita uma conferência do que será adicionado na base. Um exemplo pode ser visto na figura 3.19, que irá gerar o arquivo `base.ldif`.

```
taiga:~# smbldap-populate -e base.ldif
Populating LDAP directory for domain FATEC_OU (S
    -1-5-21-3226524203-2369515941-3762550674)
(using builtin directory structure)

exported ldif file: base.ldif
```

Figura 3.19: Comando smbldap-populate

Depois de portada a base, toda a gerência pode ser feita utilizando os comandos do pacote smbldap-tools. Alguns exemplos podem ser vistos abaixo:

smbldap-useradd: Adiciona um usuário na base. Para adicionar uma conta de computador, deve-se utilizar o parâmetro -w.

Ex.: smbldap-useradd -a -m -d /home/ruy -s /bin/bash -A -B ruy

onde:

-a: Adiciona uma conta com propriedades do Windows.

-m: Cria o diretório pessoal.

-d /home/ruy: especifica qual será home do usuário.

-s /bin/bash: especifica o shell do usuário.

-A: Define que o usuário pode mudar a senha.

-B: Define que o usuário deve mudar a senha no primeiro login.

smbldap-userdel: Remove uma conta de usuário.

Ex.: smbldap-userdel -r ruy

Onde:

-r: remove o diretório pessoal do usuário.

-R: remove o diretório pessoal do usuário recursivamente.

smbldap-passwd: Atribui uma senha para o usuário.

Além desses, existem mais alguns comandos que podem ser encontrados em (TRIGO, 2007).

3.4.2 Alterando o slapd.conf

Duas coisas devem ser feitas no arquivo de configuração do servidor OpenLDAP. Uma é criar os índices para alguns atributos utilizados pelo samba, e outra é criar ACLs para impedir que informações confidenciais sejam acessadas por qualquer usuário.

A criação de ACLs é feita adicionando algumas linhas ao arquivo `/etc/openldap/slapd.conf`, conforme pode ser visto na figura 3.20, onde foi definido que nos atributos *sambaLMPassword*, *sambaNTPassword*, *userPassword*, *sambaPasswordHistory* e *sambaPwdLastSet*:

- o usuário root pode gravar
- um usuário não autenticado pode se autenticar
- o próprio usuário pode gravar
- qualquer outro usuário não pode fazer nada.

```
access to attrs=sambaLMPassword,sambaNTPassword,userPassword,
    sambaPasswordHistory,sambaPwdLastSet
   by dn="cn=root,dc=ceeteps" write
   by anonymous auth
   by self write
   by * none
```

Figura 3.20: Criando ACLs

Na figura 3.21 há exemplos de criação de índices. Há uma linha com os atributos *sambaSID*, *sambaPrimaryGroupSID* e *sambaDomainName*. Nesse caso, foi criado índices para otimizar pesquisas buscando por valores iguais aos presentes nesses atributos.

```
index cn,sn,uid,displayName             pres,sub,eq
index memberUID,mail,givenname          eq,subinitial
index objectClass,uidNumber,gidNumber        eq
index sambaSID,sambaPrimaryGroupSID,sambaDomainName   eq
index uniqueMember,entryCSN,entryUUID        eq
```

Figura 3.21: Criando índices

Conforme (CARTER, 2003), os tipos de índices possíveis são:

approx (approximate): Indexa informações para buscas por uma aproximação do atributo.

eq (equality): Indexa informações para buscas de um valor exato do atributo.

pres (presence): Indexa informações para determinar se há algum valor entre os procurados.

sub (substring): Indexa informações para buscas por substring do atributos.

3.4.3 Alterando o arquivo /etc/samba/smb.conf

O arquivo smb.conf pode ser alterado para que o samba se integre com o OpenLDAP.

Além de informar que a base de senhas do samba é um servidor Ldap, pode-se também alterar comandos de administração de usuários, conforme pode ser visto na figura 3.22, todas na sessão GLOBAL.

```
passdb backend = ldapsam:ldap://localhost
add user script = /usr/sbin/smbldap-useradd -m "%u"
delete user script = /usr/sbin/smbldap-userdel "%u"
add group script = /usr/sbin/smbldap-groupadd -p "%g"
delete group script = /usr/sbin/smbldap-groupdel "%g"
add user to group script = /usr/sbin/smbldap-groupmod -m "%u" "%g"
delete user from group script = /usr/sbin/smbldap-groupmod -x "%u"
     "%g"
set primary group script = /usr/sbin/smbldap-usermod -g "%g" "%u"
add machine script = /usr/sbin/smbldap-useradd -w "%u"
ldap admin dn = cn=root,dc=ceeteps
ldap delete dn = Yes
ldap group suffix = ou=Grupos
ldap idmap suffix = sambaDomainName=FATEC_OU
ldap machine suffix = ou=Computadores
ldap passwd sync = Yes
ldap suffix = dc=ceeteps
ldap ssl = no
ldap user suffix = ou=Usuarios
idmap backend = ldap:ldap://localhost
idmap uid = 10000-20000
idmap gid = 10000-20000
```

Figura 3.22: Configurando o smb.conf

3.4.4 NFS

Para os clientes Linux, foi configurado o NFS, para exportar o home dos usuários, que são autenticados através do `pam_ldap`.

3.4.4.1 Configuração do servidor NFS

A configuração do servidor NFS é bastante simples. O pacote a ser instalado no servidor gentoo é o `nfs-utils`.

Após instalado, é preciso configurar o arquivo `/etc/exports`. Nele deve-se especificar qual diretório será exportado para qual rede, conforme pode ser visto na figura 3.23.

```
/home 172.16.0.0/255.255.0.0(rw,no_root_squash,sync)
```

Figura 3.23: /etc/exports

3.4.4.2 Configuração do cliente NFS

Para que o cliente monte o compartilhamento na inicialização é necessário editar o arquivo `/etc/fstab`, e adicionar a linha conforme a figura 3.24

```
mascaradamorte.fatecou.edu.br:/home /home nfs   rsize=8192,wsize
    =8192 0 0
```

Figura 3.24: /etc/fstab

Também é necessário configurar o PAM, para que ele autentique no servidor OpenLDAP. Conforme (POMEROY, 2009), isso é feito alterando os arquivos `/etc/pam_ldap.conf` (figura 3.25), `/etc/pam.d/common-account` (figura 3.26), `/etc/pam.d/common-auth` (figura 3.27), `/etc/pam.d/common-password` (figura 3.28) e `/etc/pam.d/common-session` (figura 3.29). Também é necessário colocar a senha do usuário administrador do OpenLDAP no arquivo `/etc/pam_ldap.secret`, e alterar sua permissão para 600.

Para a obtenção das informações de usuários e grupos do OpenLDAP é necessário cofigurar também o libnss-ldap. Segundo (JONG, 2009), é necessário confi-

```
base dc=ceeteps
rootbinddn cn=root,dc=ceeteps
```

Figura 3.25: /etc/pam_ldap.conf

```
account     required      pam_unix.so
account     sufficient    pam_succeed_if.so uid < 1000 quiet
account     [default=bad success=ok user_unknown=ignore] pam_ldap.
    so
account     required      pam_permit.so
```

Figura 3.26: /etc/pam.d/common-account

```
auth    sufficient      pam_unix.so nullok_secure
auth    requisite       pam_succeed_if.so uid >= 1000 quiet
auth    sufficient      pam_ldap.so use_first_pass
auth    required        pam_deny.so
```

Figura 3.27: /etc/pam.d/common-auth

```
password    sufficient    pam_unix.so md5 obscure min=4 max=8
    nullok try_first_pass
password    sufficient    pam_ldap.so
password    required      pam_deny.so
```

Figura 3.28: /etc/pam.d/common-password

```
session     required      pam_limits.so
session     required      pam_unix.so
session     optional      pam_ldap.so
```

Figura 3.29: /etc/pam.d/common-session

gurar os arquivos `/etc/libnss-ldap.conf` (figura 3.30) e `/etc/nsswitch.conf` (figura 3.31).

```
uri ldap://mascaradamorte.fatecou.edu.br
base dc=ceeteps
```

Figura 3.30: /etc/libnss-ldap.conf

```
passwd:      files ldap
shadow:      files ldap
group:       files ldap

hosts:          files dns ldap
networks:       files ldap
```

Figura 3.31: /etc/nsswitch.conf

3.4.5 Configuração do cliente Windows

Na Fatec Ourinhos há clientes Windows XP e Vista. Para adicioná-los ao domínio a configuração é muito parecida.

No Windows XP, deve-se abrir o *Painel de Controle*, depois *Sistema* e abrir a aba *Nome do Computador*. Ao clicar no botão *Alterar*, abrirá a janela *Alterações de nome do computador*. Deve-se selecionar a opção *Domínio* e escrever *FATEC_OU*. Irá abrir uma tela, onde deverá ser digitados o usuário administrador do domínio e sua senha. Caso tudo ocorra bem, irá abrir uma tela com a frase *Bem vindo ao domínio FATEC_OU*. Após reiniciar o computador, a tela de login irá mostrar a opção *Fazer logon em:*, onde pode-se escolher o domínio samba ou a própria máquina.

No Windows Vista deve-se abrir o *Painel de Controle*, e depois *Sistemas*, *Configurações avançadas do sistema*. Na aba *Nome do Computador* deve-se clicar no botão *Alterar Nome*. Na tela que irá abrir, escolhe-se a opção *Domínio* e digita-se *FATEC_OU*. Na janela que abrir, deve-se digitar o usuário administrador do domínio e sua senha. Após reiniciar o computador, o login será feito no domínio.

No Windows Vista, caso seja necessário trocar o domínio onde se faz o login, é necessário clicar no botão *Trocar Usário* e especificá-lo.

3.4.6 Criação de Grupos

Na Fatec Ourinhos, a política de grupos é definida da seguinte maneira:

- Cada disciplina tem um diretório no servidor, onde os professores disponibilizam material para os alunos.

- Mais de um professor pode lecionar a mesma disciplina, portanto, mais de um professor deve poder gravar no mesmo diretório, mas não pode alterar conteúdo de outro professor.
- Os alunos só tem acesso as disciplinas nas quais estão matriculados.

Ou seja, somente as permissões básicas do Linux não são suficientes. Por isso foi utilizado ACL´s.

Para cada disciplina foi criado um diretório e dois grupos. Por exemplo, para a disciplina *Lógica de Programação*, foi criado o diretório */home/grupos/LogicaProgramacao*, e os grupos *LogicaProgramacao* e *LogicaProgramacao_profs*. Os alunos matriculados na disciplina fazem parte do grupo *LogicaProgramacao* e os professores que lecionam a disciplina fazem parte do grupo *LogicaProgramacao_profs*.

Neste diretório criado, foi dada a permissão 750, sendo seu dono o usuário root, e grupo *LogicaProgramacao*. Foi aplicada a ACL[22] para que o grupo *LogicaProgramacao_prof* possa ler, gravar e executar.

Também é importante que, o arquivo gravado dentro deste diretório seja desse grupo. Para isso foi utilizado o `chmod g+s` no diretório. Outra permissão especial[23] utilizada foi o `chmod +t`, para que, somente quem gerou o arquivo possa removê-lo.

Os grupos foram adicionados ao sistema através de um arquivo ldif, cujo modelo pode ser visto na figura 3.32.

Os comandos podem utilizados podem ser vistos na figura 3.33.

3.4.7 Adicionando usuários no domínio

Na Fatec Ourinhos, foi definido que o login do aluno seja seu registro de matrícula. Como dito anteriormente, o aluno tem acesso ao diretório das disciplinas nas quais está matriculado, portanto, ele deve fazer parte do grupo da disciplina.

Para adicionar usuários ao domínio foi pedido para a equipe de desenvolvimento do sistema acadêmico que fosse gerado um arquivo com os comandos `smbldap-useradd`.

[22] Mais informações sobre ACL podem ser obtidas em `http://acl.bestbits.at/`

[23] Mais informações sobre permissões especiais em `http://focalinux.cipsga.org.br/guia/intermediario/ch-perm.htm`

```
dn:cn=LogicaProgramacao,ou=FatecOU,ou=Grupos,dc=ceeteps
objectClass: top
objectClass: posixGroup
cn:LogicaProgramacao

dn:cn=LogicaProgramacao_profs,ou,Docentes,ou=FatecOU,ou=Grupos,dc=
    ceeteps
objectClass: top
objectClass: posixGroup
cn:LogicaProgramacao_profs
```

Figura 3.32: Criação de grupos

```
mkdir /home/grupos/LogicaProgramacao
chown root:LogicaProgramacao /home/grupos/LogicaProgramacao
chmod 750 /home/grupos/LogicaProgramacao
chmod g+s /home/grupos/LogicaProgramacao
chmod +t /home/grupos/LogicaProgramacao
setfacl -m g:LogicaoProgramacao_prof:rwx /home/grupos/
    LogicaProgramacao
setfacl -m g:LogicaProgramacao:rw /home/grupos/LogicaProgramacao
```

Figura 3.33: Criação de diretórios para os grupos

O formato do arquivo pode ser visto na figura 3.34.

```
smbldap-useradd -a -m -d /home/registro_matricula -n -c "
    Comentario, campo Gecos" -o ou=Alunos -G lista,de,disciplinas,
    separadas,por,virgula -g "Domain Users" -N "Primeiro Nome" -S
    "Sobrenome" -s /bin/bash -T email registro_matricula -P <
    arquivo_com_a_senha
```

Figura 3.34: Criação de usuários

Onde:

-a: Define que é um usuário do Windows.

-m: Cria o diretório home do usuário.

-d: Diretório home do usuário.

-n: Não cria um grupo com o nome do usuário.

-c: Campo GECOS do Linux.

-o: Adiciona o usuário dentro da organizational unit especificada

-G: Lista de grupos adicional.

-g: Grupo principal.

-N: Primeiro nome do usuário.

-S: Sobrenome do usuário.

-s: shell.

-T: endereço de e-mail.

-P < arquivo_com_a_senha: Lê a senha do arquivo.

3.4.8 Criando compartilhamentos através do domínio

Quando deseja-se compartilhar algum recurso com outros usuários, o ideal é que faça-se um compartilhamento com senha.

Caso tenha-se configurado um servidor de domínio, pode-se definir que tal compartilhamento só pode ser acessado por usuários do domínio, definindo quais permissões determinado usuário (ou grupo de usuários) terá.

Conforme pode ser visto em (MICROSOFT, 2004), após compartilhar o recurso, na guia *Compartilhamento*, deve-se clicar no botão *Permissões*. Na janela *Permissões*, clica-se no botão *Adicionar*. Na janela *Selecione Usuários ou Grupos*, o botão *Avançado...* abre outra janela de mesmo nome, onde deve-se clicar no botão *Localizar agora*, que irá listar todos os usuários e grupos disponíveis, tanto local quanto do domínio. Deve-se clicar no usuário ou grupo desejado e clicar no botão *OK*, e *OK* novamente. Depois basta definir quais permissões o usuário ou grupo terá.

Na lista aparece o usuário *Todos*, que deve ser removido.

3.5 Proxy

Quando temos uma rede com vários computadores, para que todos tenham acesso a Internet, na opnião deste autor, não é interessante que todas o façam diretamente.

Dois motivos podem ser citados para defender essa opnião:

- A quantidade de IP's reais que seriam necessários para toda a rede teriam um custo muito elevado.
- Tanto o controle de acesso quanto a segurança precisariam ser implementados em todos os computadores.

Para resolver esse problema, pode-se configurar um servidor proxy, que servirá de gateway para a rede.

O proxy utilizado foi o Squid. Segundo (SQUID, 2009), o squid é um cache proxy para Internet que suporta protocolos HTTP, HTTPS, FTP e outros. Ele reduz utilização de banda e melhora o tempo de resposta por cache e reutiliza páginas visitadas frequentemente.

3.5.1 Squid

A instalação do Squid foi feita por emerge, e sua USE foi alterada para habilitar suporte a LDAP, samba, sasl, proxy transparente e SSL. O arquivo `/etc/portage/package.use` pode ser visto na figura 3.35.

```
app-admin/eselect vim-syntax
sys-libs/glibc nptlonly
net-firewall/iptables -ipv6 extensions -imq -l7filter static
net-misc/openssh pam tcpd -X -X509 -hpn -kerberos ldap -libedit
net-proxy/squid pam ssl -icap-client ipf-transparent ldap
    logrotate -nis pf-transparent -radius samba sasl snmp
```

Figura 3.35: Arquivo de /etc/portage/package.use

Depois de instalado, ele foi configurado como proxy transparente. A parte de autenticação ainda não foi implementada.

Conforme pode ser visto em (SQUID, 2008), para configurar o Squid como proxy transparente basta alterar a linha conforme pode ser visto a figura 3.36.

Conforme (GHEORGHE, 2006) é necessário fazer um redirecionamento de portas usando o iptables, conforme pode ser visto na figura 3.37. Também é necessário fazer um mascaramento para requisições https, pois não é possível fazer redirecionamentos de conexões criptografadas. O mascaramento também pode ser visto na figura 3.37.

```
http_port 172.16.0.2:3128 transparent
```

Figura 3.36: Arquivo de `/etc/squid/squid.conf`

```
iptables -t nat -A PREROUTING -s 172.16.0.2 -p tcp -dport 80 -j
    REDIRECTT --to-port 3128
iptables -t nat -A POSTROUTING -o eth0 0s 172.16.0.2 - tcp --dport
     443 -j MASQUERADE
```

Figura 3.37: Regras do iptables para redirecionamento de portas e mascaramento

Capítulo 4

Organização Final

Este capítulo final explica como a nova rede foi organizada, definindo como os servidores foram instalados.

4.1 Servidor de máquinas virtuais

Um dos servidores (mu.fatecou.edu.br) foi configurado com o Xen. O esquema de particionamento pode ser visto no tabela 4.1.

Tabela 4.1: Esquema de particionamento: mu.fatecou.edu.br

Partição	Tamanho	Sistema de Arquivos	Função
/dev/sda1	2GB	Swap	swap
/dev/sda2	10GB	reiserfs	/var
/dev/sda3	40GB	reiserfs	/
/dev/sda4	420GB	xfs	/xen

A partição `/xen` foi criada para hospedar as imagens das máquinas virtuais. Não foi instalado nenhum outro serviço adicional neste servidor.

Foram criadas duas máquinas virtuais, uma para o proxy e outra para o DHCP-/DNS. Ambas as máquinas acessam as duas interfaces de rede. A intenção é que, quando houver um link com IP público, uma interface fique ligada na rede pública, e a outra a rede privada.

4.1.1 Servidor DHCP/DNS

A máquina virtual para os serviços de DHCP/DNS (aldebaran.fatecou.edu.br) foi criada com somente uma partição. A configuração pode ser vista na tabela 4.2.

Tabela 4.2: Configuração: aldebaran.fatecou.edu.br

Partição	5GB
Swap	1GB (em arquivo)
Memória RAM	512MB
IP interno	172.16.0.1/16
IP externo	10.66.30.3/23
Gateway	10.66.30.1

4.1.2 Servidor Proxy

Para a máquina virtual para o proxy (saga.fatecou.edu.br) foi criado dois arquivos de imagem, conforme a figura 4.3

Tabela 4.3: Configuração: saga.fatecou.edu.br

Partição /	5GB
Partição /var	5GB
Swap	2GB (em arquivo)
Memória RAM	3GB
IP interno	172.16.0.2/16
IP externo	10.66.30.4/23
Gateway	10.66.30.1

4.2 Servidor de Arquivos e domínio

O servidor de arquivos (mascaradamorte.fatecou.edu.br) foi configurado sem virtualização. Nele foi instalado o Samba, o OpenLDAP e o CUPS. Seu esquema de particionamento pode ser visto na tabela 4.4. As duas interfaces de rede foram

Tabela 4.4: Esquema de particionamento: mascaradamorte.fatecou.edu.br

Partição	Tamanho	Sistema de Arquivos	Função
/dev/sda1	4GB	Swap	swap
/dev/sda4	420GB	reiserfs	/home
/dev/sda2	10GB	reiserfs	/var
/dev/sda3	40GB	reiserfs	/

Tabela 4.5: Configuração de rede: mascaradamorte.fatecou.edu.br

IP	172.16.0.4/16
Gateway	172.16.0.2
DNS	172.16.0.1

configuradas em bonding nível 6 (explicado sessão 2.7), e os endereços podem ser vistos na tabela 4.5.

4.3 Outros serviços

Conforme dito anteriormente, foram comprados três servidores, mas somente dois foram utilizados. O outro foi reservado para a configuração do servidor de páginas e banco de dados.

Inicialmente foi-se pensado em criar duas máquinas virtuais, uma para o servidor de páginas e banco de dados do sistema acadêmico, e outra para o servidor de páginas e banco de dados para aulas.

Além disso, é possível criar cópias das máquinas virtuais do servidor mu.fatecou.edu.br para deixá-las em alta disponibilidade (e também fazer o inverso, criar cópias dos servidores de página no servidor mu.fatecou.edu.br).

O sistema de firewall também não foi configurado. O projeto inicial é de utilizar os servidores antigos para isso, e isolar os servidores do restante da rede utilizando DMZ[1], conforme a figura 4.1.

[1] Demilitarized Zone

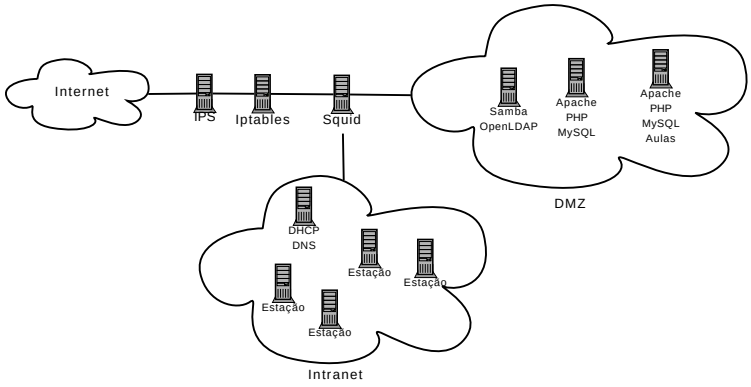

Figura 4.1: Projeto inicial a estrutura física de rede

Capítulo 5

Conclusão

O maior motivador para a migração foram os servidores antigos, que apresentavam um desempenho muito ruim devido ao hardware antigo. O Novell Netware é um sistema operacional fácil de ser operado, pois seus recursos já estão todos integrados, praticamente todas as soluções podem ser encontrados nos manuais do produto.

Mesmo com pontos positivos, ele não foi utilizado por não ser compatível com o hardware adquirido. Isso tornou a migração necessária, pois uma atualização da versão teria um custo muito alto, e o processo para aquisição levaria muito tempo.

Apesar de um dos motivos da utilização do software livre ter sido um alinhamento estratégico com a política de incentivo à adoção de software da direção da faculdade, ele mostrou-se tecnicamente viável, pois atende perfeitamente as necessidades da administração da rede.

O sistema operacional Linux mostrou-se completamente compatível com o hardware. Apesar de não ter sido possível uma comparação de desempenho entre o Novell Netware e o Linux (devido a incompatibilidade do Netware com o hardware), o Linux apresentou um desempenho muito bom nos novos servidores.

Outro fator positivo foi que, com a configuração do Samba como PDC, o login é feito somente no domínio. Com o Novell Netware, era necessário efetuar login no domínio e depois no Windows, o que causava confusão entre os novos alunos nas primeiras semanas, e demandava muita atenção por parte dos funcionários da administração da rede.

Todos os compartilhamentos locais foram configurados com autenticação no diretório, o que melhorou a segurança e facilitou a administração.

A administração de usuários, grupos, quotas e permissões são tarefas um pouco mais complicadas no Linux, mas ainda assim é possível treinar estagiários rapidamente para realizar as operações com maior incidência (como trocar e desbloquear senhas, adicionar usuários no sistema e em grupos).

Outras operações mais complexas necessitam de explicação mais aprofundada, mas também são operações que normalmente não trazem um impacto imediato, portanto podem ser adiadas para uma ocasião em que seja possível tal explicação.

Mesmo não tendo somente pontos positivos, a migração cumpriu seus três principais objetivos:

- Substituir o Novell Netware atendendo as necessidades da administração da rede;
- Mostrar aos alunos que o software livre é uma alternativa viável;
- Possibilitar a criação de um documento com uma implementação real de uma migração de uma infra estrutura lógica de rede para software livre.

Os dois servidores de página e banco de dados não foram migrados mas ainda atendem a demanda, por isso não havia tanta urgência. Há também a intenção de se implantar o Kerberos, a autenticação do proxy e a integração do sistema acadêmico com o diretório.

Como dito anteriormente, o Gentoo foi escolhido por ser uma distribuição altamente customizável, e pelo conhecimento do autor. Mas todos os serviços podem ser configurados em outras distribuições da mesma maneira, mudando muito pouca coisa. O autor recomenda sempre trabalhar com a distribuição com a qual se tenha maior conhecimento, pois o tempo desprendido para aprender as particularidades de cada uma é muito grande, e, independente da distribuição, o kernel é o mesmo.

Mesmo com a vasta documentação consultada, muitas dificuldades foram encontradas durante todo o processo, por isso recomenda-se que antes de se iniciar um processo de migração, tenha-se um bom conhecimento das ferramentas utilizadas, e que sejam realizados testes em laboratório.

Capítulo 6

Referências Bibliográficas

ALBITZ, P.; LIU, C. *DNS and BIND, 4th Edition*. 4. ed. [S.l.]: O'Reilly, 2001. ISBN 0-596-00158-4.

ALKALAY, A. Nos domínios da paravirtualização. Junho 2007. Disponível em: <http://www.ibm.com/developerworks/blogs/page-/tlcbr?entry=dominios_da_paravirtualizacao>.

BARR, J. Is windows 2003 server really faster than linux/samba? maio 2003. Disponível em: <http://linux.sys-con.com/node/32673>.

CARTER, G. *LDAP System Administration*. [S.l.]: O'Reilly, 2003. 308 p. ISBN 1-56592-491-6.

DAVIS, T. Net:bonding. 2000. Disponível em: <http://www.linuxfoundation.org-/en/Net:Bonding>.

GENTOO HANDBOOK. *Xen Gentoo Linux Wiki*. [S.l.], 09 2008. Disponível em: <http://gentoo-wiki.com/Xen>.

GENTOO.ORG. *Gentoo Linux - About Gentoo*. [S.l.], 2008. Disponível em: <http://www.gentoo.org/main/en/about.xml>.

GHEORGHE, L. *Designing and Implementing Linux Firewalls and QoS using netfilter, iproute2, NAT, and L7-filter*. 1. ed. [S.l.]: Packt Publishing Ltd., 2006. ISBN 1-904811-65-5.

IBM. Tornar-se mais eficiente em relação aos custos. *www.ibm.com*, 2009. Disponível em: <http://www.ibm.com/br/systems/optimizeit/cost_efficiency-/energy_efficiency/services.phtml>.

JONG, A. D. Configuring ldap authentication. junho 2009. Disponível em: <http://wiki.debian.org/LDAP/NSS>.

KAVEN, O. Performance tests: File server throughput and response times. Novermbro 2001. Disponível em: <http://www.pcmag.com/article2-/0,2817,2313307,00.asp>.

KEGEL, D. Windows 2003 vs. linux file server benchmarks. Outubro 2003. Disponível em: <http://www.kegel.com/nt-linux-benchmarks.html>.

MATTOS, D. M. F.; CARLOS, O. Virtualizaçã. junho 2008. Disponível em: <http://www.gta.ufrj.br/grad/08_1/virtual/index.html>.

MICROSOFT. *Compartilhar arquivos e pastas na rede (domínio)*. Microsoft - Ajuda e Suporte, 3 2004. Disponível em: <http://support.microsoft.com/kb-/301198/pt-br>.

MICROSOFT. Identificadores de segurança conhecidos nos sistemas operacionais windows. mar. 2008. Disponível em: <http://support.microsoft.com/kb/243330>.

NAVARRO, A. C. Virtuzalização. *IBM*, 2009. Disponível em: <http://www.ibm-.com/expressadvantage/br/articles_etips/virtualization.phtml>.

OPENLDAP FOUDATION. *OpenLDAP Software 2.4 Administrator's Guide*. [S.l.], 2008. Disponível em: <http://www.openldap.org/doc/admin24/index-.html>.

POMEROY, S. Configuring ldap authentication. Julho 2009. Disponível em: <http://wiki.debian.org/LDAP/PAM>.

RFC2849. [S.l.], Junho 2000. Disponível em: <http://www.faqs.org/rfcs/rfc2849-.html>.

SQUID: Optimising Web Delivery. 2009. Disponível em: <http://www.squid-cache.org/>.

SQUID, W. Transparent caching/proxy. Setembro 2008. Disponível em: <http://www.deckle.co.za/squid-users-guide% -/Transparent_Caching/Proxy>.

TLDP. *DHCP Server Setup*. [S.l.], 2009. Disponível em: <http://tldp.org-/HOWTO/DHCP/x369.html>.

TRIGO, C. H. *OpenLDAP: Uma Abordagem Integrada*. 1. ed. [S.l.]: Novatec Editora Ltda., 2007. ISBN 978-85-7522-128-0.

VERISIGN. Secure sockets layer (ssl): How it works. 07 2009. Disponível em: <http://www.verisign.com/ssl/ssl-information-center/how-ssl-security-works-/index.html>.

VERITEST. Microsoft windows server 2003 vs. linux competitive file server performance comparison. abr. 2003. Disponível em: <http://download.microsoft-.com/download/0/7/1/0715a190-70f5-4b0d-8ced-f9d1e046aa6a/netbench.pdf>.

VERMEULEN, S. *Configuring Gentoo with Xen*. [S.l.], 08 2008. Disponível em: <http://www.gentoo.org/doc/en/xen-guide.xml>.

VERNOIJ, J. R.; TERPSTRA, J. H.; CARTER, G. *The Official Samba 3.2.x HOWTO and Reference Guide*. O'Reilly, 2007. Disponível em: <http://us1.samba.org/samba/docs/Samba3-HOWTO.pdf>.

WHATS is ISC DHCP nd what does t do? 2009. Disponível em: <https://www-.isc.org/software/dhcp>.

WIKI GENTOO. *Downloading dependencies while compiling*. [S.l.], 2008. Disponível em: <http://gentoo-wiki.com-/TIP_Downloading_dependencies_while_compiling>.

WIKI GENTOO. *Gentoo Linux AMD64 Handbook*. [S.l.], 2008. Disponível em: <http://www.gentoo.org/doc/en/handbook/handbook-amd64.xml?style=printable\&full=1>.

WIKI GENTOO. Portage tmpdir on tmpfs. Julho 2009. Disponível em: <http://en.gentoo-wiki.com/wiki/Portage_TMPDIR_on_tmpfs>.

XEN SOURCE. *Xen Paravirtualization*. [S.l.], 2008. Disponível em: <http://www.xen.org/about/paravirtualization>.

Apêndice A

Arquivos de configuração

A.1 Arquivos do Xen, no servidor mu.fatecou.edu.br

A.1.1 /etc/xen/xend-config.sxp

```
# -*- sh -*-
# Xend configuration file.
(xend-relocation-server yes)
(xend-relocation-hosts-allow '^localhost$ ^localhost.localdomain$
    ')
(network-script 'network-multi')
(network-script 'network-route')
(vif-script vif-bridge)
(vif-script     vif-route)
(dom0-min-mem 196)
# In SMP system, dom0 will use dom0-cpus # of CPUS
# If dom0-cpus = 0, dom0 will take all cpus available
(dom0-cpus 0)
```

A.1.2 /etc/xen/scripts/network-multi

```
#!/bin/bash
sh /etc/xen/scripts/network-bridge start netdev=eth0
sh /etc/xen/scripts/network-bridge start netdev=eth1
```

A.1.3 /xen/vms/gentoo_proxy

```
kernel = "/xen/kernel/vmlinuz";
memory = 3072;
vcpus = 8
vif = [ 'bridge=eth0', 'bridge=eth1' ];
name   = "saga";
disk   = [ "file:/xen/imagens/gentoo_proxy_root.img,xvdb1,w", "
    file:/xen/imagens/gentoo_proxy_var.img,xvdb2,w" ];
root   = "/dev/xvdb1 ro";
extra = "3";
on_poweroff = 'destroy'
on_reboot   = 'restart'
on_crash    = 'restart'
```

A.1.4 /xen/vms/gentoo_dns

```
kernel = "/xen/kernel/vmlinuz";
memory = 512;
vcpus = 8
vif = [ 'bridge=eth0', 'bridge=eth1' ];
name   = "aldebaran";
disk   = [ "file:/xen/imagens/gentoo_dns.img,xvda,w" ];
root   = "/dev/xvda ro";
extra = "3";
on_poweroff = 'destroy'
on_reboot   = 'restart'
on_crash    = 'restart'
```

A.2 Arquivos de configuração do servidor DNS + DHCP, aldebaran.fatecou.edu.br

A.2.1 /etc/dhcp/dhcpd.conf

```
server-identifier aldebaran;
ddns-updates on;
ddns-update-style interim;
ddns-domainname "fatecou.edu.br";
ddns-rev-domainname "in-addr.arpa";
# option definitions common to all supported networks...
option domain-name "fatecou.edu.br";
```

```
option domain-name-servers 172.16.0.1;
#option netbios-name-servers 172.16.0.1;
default-lease-time 6000;
max-lease-time 72000;
log-facility local7;
allow client-updates;
include "/etc/dhcp/rndc.key";
option subnet-mask 255.255.0.0;
use-host-decl-names on;
subnet 172.16.0.0 netmask 255.255.0.0 {
  range 172.16.1.0 172.16.255.254;
  option routers 172.16.0.1;
  option broadcast-address 172.16.255.255;
}
zone fatecou.edu.br {
   primary 127.0.0.1;
   key rndc-key;
  }
zone 16.172.in-addr.arpa {
   primary 127.0.0.1;
   key rndc-key;
  }
```

A.2.2 /etc/bind/named.conf

```
include "/etc/bind/rndc.key";
logging
  {
     category lame-servers{null;};
     category edns-disabled{null;};
  };
options
{
  directory "/var/bind";
  forwarders
  {
    200.176.2.10;
  };
 listen-on-v6 { none; };
  pid-file "/var/run/named/named.pid";
};
zone "." IN
{
  type hint;
  file "named.ca";
};
```

```
zone "localhost" IN
{
  type master;
  file "pri/localhost.zone";
  allow-update { none; };
  notify no;
};
zone "127.in-addr.arpa" IN
{
  type master;
  file "pri/127.zone";
  allow-update { none; };
  notify no;
};
zone "fatecou.edu.br."
{
  type master;
  allow-update { key "rndc-key"; 127.0.0.1; };
  file "pri/fatecou.edu.br.db";
};
zone "16.172.in-addr.arpa."
{
  type master;
  allow-update { key "rndc-key"; 127.0.0.1; };
  file "pri/fatecou.edu.br.rev.db";
};
```

A.2.3 /etc/bind/rndc.key

```
key "rndc-key"
{
  algorithm hmac-md5;
  secret "d0eUGk/svtVmpNUXK/fgKw==";
};
```

A.3 Arquivos de configuração do servidor de arquivos e diretório, mascaradamorte.fatecou.edu.br

A.3.1 /etc/samba/smb.conf

```
# Date: 2008/05/31 00:14:32
[global]
```

```
unix charset = ISO8859-1
workgroup = FATEC_OU
netbios name = PDC
server string = PDC
passdb backend = ldapsam:ldap://localhost
username map = /etc/samba/smbusers
log level = 1
syslog = 0
log file = /var/log/samba/%m.log
max log size = 0
name resolve order = lmhosts host wins bcast
time server = Yes
socket options = TCP_NODELAY SO_RCVBUF=8192 SO_SNDBUF=8192
show add printer wizard = No
add user script = /usr/sbin/smbldap-useradd -m "%u"
delete user script = /usr/sbin/smbldap-userdel "%u"
add group script = /usr/sbin/smbldap-groupadd -p "%g"
delete group script = /usr/sbin/smbldap-groupdel "%g"
add user to group script = /usr/sbin/smbldap-groupmod -m "%u" "%
    g"
delete user from group script = usr/sbin/smbldap-groupmod -x "%u
    " "%g"
set primary group script = /usr/sbin/smbldap-usermod -g "%g" "%u
    "
add machine script = /usr/sbin/smbldap-useradd -w "%u"
logon script = kixtart.exe
logon path =
logon home =
domain logons = Yes
os level = 65
local master = yes
preferred master = Yes
domain master = Yes
wins support = Yes
ldap admin dn = cn=root,dc=ceeteps
ldap delete dn = Yes
ldap group suffix = ou=Grupos
ldap idmap suffix = sambaDomainName=FATEC_OU
ldap machine suffix = ou=Computadores
ldap passwd sync = Yes
ldap suffix = dc=ceeteps
ldap ssl = no
ldap user suffix = ou=Usuarios
utmp = Yes
idmap backend = ldap:ldap://localhost
idmap uid = 10000-20000
idmap gid = 10000-20000
map acl inherit = Yes
```

```
  hide unreadable = Yes
  veto files = /*.eml/*.nws/*.{*}/
  veto oplock files = /*.doc/*.xls/*.mdb/
  strict locking = Yes
  load printers = yes
  printing = cups
  printcap name = cups

[netlogon]
  comment = Servico de Logon em Rede
  path = /home/samba/netlogon

[home]
  comment = Diretorio Pessoal
  path = /home/%u
  read only = No
  create mask = 0600
  directory mask = 0700
  browseable = No

[grupos]
  comment = Grupos
  path = /home/grupos/
  read only = No
  browseable = No

[dados]
  comment = Sistemas e Dados de Usuarios [ F:\ ]
  path = /home/samba/dados
  read only = No
  force create mode = 0660
  force directory mode = 02770

[temp]
  comment = Dados Temporarios [ T:\ ]
  path = /home/samba/temp
  read only = No
  force create mode = 0666
  force directory mode = 02777

[printers]
  comment = Impressora
  path = /var/spool/samba
  browseable = no
  guest ok = yes
  public = yes
  writable = no
  printable = yes
```

```
  read only = yes
  printer admin = root

[print$]
  comment = Printer Drivers
  path = /home/samba/drivers
  browseable = yes
  guest ok = no
  read only = yes
  write list = root
```

A.3.2 /etc/smbldap-tools/smbldap.conf

```
##############################################################
# General Configuration
##############################################################
# Put your own SID. To obtain this number do: "net getlocalsid".
# If not defined, parameter is taking from "net getlocalsid"
# return SID="S-1-5-21-3226524203-2369515941-3762550674" Domain
#name the Samba server is in charged. If not defined, parameter
# is taking from smb.conf configuration file
sambaDomain="FATEC_OU"
##############################################################
# 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.
# Those two servers declarations can also be used when you have
# one master LDAP server where all writing operations must be done
#one slave LDAP server where all reading operations must be done
#   (typically a replication directory)
# Slave LDAP server
slaveLDAP="127.0.0.1"
# Slave LDAP port
slavePort="389"
# Master LDAP server: needed for write operations
masterLDAP="127.0.0.1"
# Master LDAP port
masterPort="389"
# Use TLS for LDAP
# If set to 1, this option will use start_tls for connection
# (you should also used the port 389)
# If not defined, parameter is set to "1"
ldapTLS="0"
# How to verify the server's certificate (none, optional or
```

```
# require) see "man Net::LDAP" in start_tls section for more
# details
verify="require"
# CA certificate
# see "man Net::LDAP" in start_tls section for more details
cafile="/etc/smbldap-tools/ca.pem"
# certificate to use to connect to the ldap server
# see "man Net::LDAP" in start_tls section for more details
clientcert="/etc/smbldap-tools/smbldap-tools.pem"
# key certificate to use to connect to the ldap server
# see "man Net::LDAP" in start_tls section for more details
clientkey="/etc/smbldap-tools/smbldap-tools.key"
# LDAP Suffix
suffix="dc=ceeteps"
# Where are stored Users
usersdn="ou=Usuarios,${suffix}"
# Where are stored Computers
computersdn="ou=Computadores,${suffix}"
# Where are stored Groups
groupsdn="ou=Grupos,${suffix}"
# Where are stored Idmap entries
#(used if samba is a domain member server)
idmapdn="ou=Idmap,${suffix}"
# Where to store next uidNumber and gidNumber
#available for new users and groups
# If not defined, entries are stored in sambaDomainName object.
sambaUnixIdPooldn="sambaDomainName=${sambaDomain},${suffix}"
# Default scope Used
scope="sub"
# Unix password encryption (CRYPT, MD5, SMD5, SSHA, SHA, CLEARTEXT
    )
hash_encrypt="SSHA"
# if hash_encrypt is set to CRYPT, you may set a salt format.
# default is "%s", but many systems will generate MD5 hashed
# passwords if you use "$1$%.8s". This parameter is optional!
crypt_salt_format="%s"
##############################################################
# Unix Accounts Configuration
##############################################################
# Login defs
# Default Login Shell
userLoginShell="/bin/bash"
# Home directory
userHome="/home/%U"
# Default mode used for user homeDirectory
userHomeDirectoryMode="700"
# Gecos
userGecos="System User"
```

```
# Default User (POSIX and Samba) GID
defaultUserGid="513"
# Default Computer (Samba) GID
defaultComputerGid="515"
# Skel dir
skeletonDir="/etc/skel"
# Default password validation time (time in days) Comment the
#next line if you don't want password to be enable for
#defaultMaxPasswordAge days (be careful to the sambaPwdMustChange
#attribute's value)
defaultMaxPasswordAge="180"
#####################################################################
# SAMBA Configuration
#####################################################################
# The UNC path to home drives location (%U username substitution)
# Just set it to a null string if you want to use the smb.conf
#'logon home' directive and/or disable roaming profiles
userSmbHome=""
# The UNC path to profiles locations (%U username substitution)
# Just set it to a null string if you want to use the smb.conf
# 'logon path' directive and/or disable roaming profiles
userProfile=""
# The default Home Drive Letter mapping
userHomeDrive=""
# The default user netlogon script name (%U username substitution)
# if not used, will be automatically username.cmd
# make sure script file is edited under dos
userScript=""
# Domain appended to the users "mail"-attribute
# when smbldap-useradd -M is used
mailDomain=""
#####################################################################
# SMBLDAP-TOOLS Configuration (default are ok for a RedHat)
#####################################################################
# Allows not to use smbpasswd (if with_smbpasswd == 0 in
# smbldap_conf.pm) but prefer Crypt::SmbHash library
with_smbpasswd="0"
smbpasswd="/usr/bin/smbpasswd"
# Allows not to use slappasswd (if with_slappasswd == 0 in
# smbldap_conf.pm)  but prefer Crypt:: libraries
with_slappasswd="0"
slappasswd="/usr/sbin/slappasswd"
# comment out the following line to get rid of the default banner
# no_banner="1"
```

A.3.3 /etc/smbldap-tools/smbldap_bind.conf

```
############################
# Credential Configuration #
############################
# Notes: you can specify two differents configuration if you use
# a master ldap for writing access and a slave ldap server for
# reading access. By default, we will use the same DN (so it will
# work for standard Samba release)
slaveDN="cn=root,dc=ceeteps"
slavePw="senha_ldap_texto_simples"
masterDN="cn=root,dc=ceeteps"
masterPw="senha_ldap_texto_simples"
```

A.3.4 /etc/openldap/slapd.conf

```
# See slapd.conf(5) for details on configuration options.
# This file should NOT be world readable.
allow bind_v2
include     /etc/openldap/schema/core.schema
include     /etc/openldap/schema/cosine.schema
include     /etc/openldap/schema/nis.schema
include     /etc/openldap/schema/misc.schema
include     /etc/openldap/schema/inetorgperson.schema
include     /etc/openldap/schema/samba.schema
schemacheck on
# Define global ACLs to disable default read access.
# Do not enable referrals until AFTER you have a working directory
# service AND an understanding of referrals.
#referral   ldap://root.openldap.org
pidfile     /var/run/openldap/slapd.pid
argsfile /var/run/openldap/slapd.args
loglevel 256
# Load dynamic backend modules:
modulepath  /usr/lib64/openldap/openldap

moduleload  back_hdb.so
# moduleload   back_dnssrv.so
#moduleload back_bdb
# BDB database definitions
#####################################################################
database hdb
suffix      "dc=ceeteps"
#checkpoint. Apos 256KB escritos ou 5 minutos passados
checkpoint  256   5 # <kbyte> <min>
rootdn      "cn=root,dc=ceeteps"
# Cleartext passwords, especially for the rootdn, should
# be avoid.  See slappasswd(8) and slapd.conf(5) for details.
```

```
# Use of strong authentication encouraged.
rootpw      {SSHA}qJMHzLA9hiQNaT4pAOLNb
password-hash {SSHA}
# The database directory MUST exist prior to running slapd AND
# should only be accessible by the slapd and slap tools.
# Mode 700 recommended.
directory   /var/lib/openldap-data
# Indices to maintain
#index   objectClass eq
index cn,sn,uid,displayName            pres,sub,eq
index memberUID,mail,givenname         eq,subinitial
index objectClass,uidNumber,gidNumber        eq
index sambaSID,sambaPrimaryGroupSID,sambaDomainName   eq
index uniqueMember,entryCSN,entryUUID        eq
lastmod on
## Os campos sambaLMPassword,sambaNTPassword,userPassword,
## sambaPasswordHistory e sambaPwdLastSet podem ser alterados
## pelos prorios usuarios - se tiverem se autenticado.
## Outros usuarios nao podem Ver estes campos.
access to attrs=sambaLMPassword,sambaNTPassword,userPassword,
    sambaPasswordHistory,sambaPwdLastSet
    by dn="cn=root,dc=ceeteps" write
    by anonymous auth
    by self write
    by * none
access to attrs=sambaPwdCanChange,sambaPwdMustChange,
    sambaPwdLastChange
    by self read
    by dn="cn=root,dc=ceeteps" write
    by self read
    by anonymous auth
    by * none
access to dn.base="" by * read
## O dn administrador tem acesso completo, o restante
## podem apenas Ler.
access to *
    by dn="cn=root,dc=ceeteps" write
    by * read
TLSCipherSuite HIGH:MEDIUM:+SSLv2:RSA
TLSCertificateFile /etc/openldap/certs/servercrt.pem
TLSCertificateKeyFile /etc/openldap/certs/serverkey.pem
TLSCACertificateFile /etc/openldap/certs/cacert.pem
```

A.3.5 /etc/conf.d/net

```
# This blank configuration will automatically use DHCP for any net
    .*
# scripts in /etc/init.d.  To create a more complete configuration
    ,
# please review /etc/conf.d/net.example and save your
    configuration
# in /etc/conf.d/net (this file :]!).
preup() {
if [[ ${IFACE} == "bond0" ]] ; then
  BOND_MODE="balance-alb 6"
  BOND_MIIMON="100"
  echo ${BOND_MODE} > /sys/class/net/bond0/bonding/mode
  echo ${BOND_MIIMON} > /sys/class/net/bond0/bonding/miimon
  einfo "Bonding mode is set to ${BOND_MODE} on ${IFACE}"
  einfo "MII monitor interval is set to ${BOND_MIINON} ms \
   on ${IFACE}"
else
  einfo "Doing nothing on ${IFACE}"
fi
   return 0
}
config_eth0=( "null" )
config_eth1=( "null" )
slaves_bond0="eth0 eth1"
depend_bond0() {
   need net.eth0 net.eth1
}
dns_domain="fatecou.edu.br"
dns_servers_bond0="172.16.0.1"
config_bond0=( "172.16.0.4 netmask 255.255.0.0
            broadcast 172.16.255.255" )
routes_bond0=( "default via 172.16.0.2" )
```

A.3.6 /etc/exports

```
/home 172.16.0.0/255.255.0.0(rw,syn,o_root_squash)
```

A.4 Arquivos de configuração dos clientes Linux

A.4.1 /etc/fstab

```
mascaradamorte.fatecou.edu.br:/home/home  nfs   rsize=8192,wsize
    =8192 0 0
```

A.4.2 /etc/pam.d/common-account

```
account required  pam_unix.so
account sufficient  pam_succeed_if.so uid < 1000 quiet
account [default=bad success=ok user_unknown=ignore] pam_ldap.so
account required  pam_permit.so
```

A.4.3 /etc/pam.d/common-auth

```
auth    sufficient      pam_unix.so nullok_secure
auth    requisite       pam_succeed_if.so uid >= 1000 quiet
auth    sufficient      pam_ldap.so use_first_pass
auth    required        pam_deny.so
```

A.4.4 /etc/pam.d/common-password

```
password sufficient pam_unix.so md5 obscure min=4 max=8 nullok
    try_first_pass
password sufficient pam_ldap.so
password required pam_deny.so
```

A.4.5 /etc/pam.d/common-session

```
session     required      pam_limits.so
session     required      pam_unix.so
session     optional      pam_ldap.so
```

A.4.6 /etc/pam_ldap.conf

```
base dc=ceeteps
rootbinddn cn=root,dc=ceeteps
```

A.4.7 /etc/libnss-ldap.conf

```
base dc=ceeteps
rootbinddn cn=root,dc=ceeteps
```

A.4.8 /etc/nsswitch.conf

```
passwd:         files ldap
group:          files ldap
shadow:         files ldap

hosts:          files dns ldap
networks:       files ldap
protocols:      db files
services:       db files
ethers:         db files
rpc:            db files

netgroup:       nis
```

A.4.9 /etc/dhcp/dhclient.conf

```
option rfc3442-classless-static-routes code 121 = array
   of unsigned integer 8;
request subnet-mask, broadcast-address, time-offset, routers,
        domain-name, domain-name-servers, domain-search, host-name
            ,
        netbios-name-servers, netbios-scope, interface-mtu,
        rfc3442-classless-static-routes;
send host-name "estacao-01";
```

Apêndice B

LDIF

B.1 Raiz

```
dn: dc=ceeteps
objectClass: top
objectClass: dcObject
objectClass: organization
dc: ceeteps
o: Centro Estadual de Educacao Tecnologica Paula Souza
```

B.2 PDC

```
# extended LDIF
#
# LDAPv3
# base <dc=ceeteps> with scope subtree
# filter: (objectclass=*)
# requesting: ALL
#

# ceeteps
dn: dc=ceeteps
objectClass: top
objectClass: dcObject
objectClass: organization
dc: ceeteps
o: Centro Estadual de Educacao Tecnologica Paula Souza
```

```
# FATEC_OU, ceeteps
dn: sambaDomainName=FATEC_OU,dc=ceeteps
sambaAlgorithmicRidBase: 1000
sambaNextUserRid: 1000
sambaMinPwdLength: 5
sambaPwdHistoryLength: 0
sambaLogonToChgPwd: 0
sambaMaxPwdAge: -1
sambaMinPwdAge: 0
sambaLockoutDuration: 30
sambaLockoutObservationWindow: 30
sambaLockoutThreshold: 0
sambaForceLogoff: -1
sambaRefuseMachinePwdChange: 0
gidNumber: 1000
sambaDomainName: FATEC_OU
sambaSID: S-1-5-21-3226524203-2369515941-3762550674
sambaNextRid: 1000
uidNumber: 1000
objectClass: top
objectClass: sambaDomain
objectClass: sambaUnixIdPool

# Usuarios, ceeteps
dn: ou=Usuarios,dc=ceeteps
objectClass: top
objectClass: organizationalUnit
ou: Usuarios

# Grupos, ceeteps
dn: ou=Grupos,dc=ceeteps
objectClass: top
objectClass: organizationalUnit
ou: Grupos

# Computadores, ceeteps
dn: ou=Computadores,dc=ceeteps
objectClass: top
objectClass: organizationalUnit
ou: Computadores

# Idmap, ceeteps
dn: ou=Idmap,dc=ceeteps
objectClass: top
objectClass: organizationalUnit
ou: Idmap
```

```
# root, Usuarios, ceeteps
dn: uid=root,ou=Usuarios,dc=ceeteps
cn: root
sn: root
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: inetOrgPerson
objectClass: sambaSamAccount
objectClass: posixAccount
objectClass: shadowAccount
gidNumber: 0
uid: root
uidNumber: 0
homeDirectory: /home/usr/root
sambaLogonTime: 0
sambaLogoffTime: 2147483647
sambaKickoffTime: 2147483647
sambaPwdCanChange: 0
sambaPrimaryGroupSID: S-1-5-21-2348235823-75777502-2747241662-512
sambaSID: S-1-5-21-2348235823-75777502-2747241662-500
loginShell: /bin/false
gecos: Netbios Domain Administrator
sambaAcctFlags: [U]
sambaPwdMustChange: 1230138608
shadowLastChange: 14057
shadowMax: 180

# nobody, Usuarios, ceeteps
dn: uid=nobody,ou=Usuarios,dc=ceeteps
cn: nobody
sn: nobody
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: inetOrgPerson
objectClass: sambaSamAccount
objectClass: posixAccount
objectClass: shadowAccount
gidNumber: 514
uid: nobody
uidNumber: 999
homeDirectory: /dev/null
sambaLogonTime: 0
sambaLogoffTime: 2147483647
sambaKickoffTime: 2147483647
sambaPwdCanChange: 0
sambaPwdMustChange: 2147483647
```

```
sambaPrimaryGroupSID: S-1-5-21-2348235823-75777502-2747241662-514
sambaAcctFlags: [NUD        ]
sambaSID: S-1-5-21-2348235823-75777502-2747241662-2998
loginShell: /bin/false

# Administradores do Dominio, Grupos, ceeteps
dn: cn=Administradores do Dominio,ou=Grupos,dc=ceeteps
objectClass: top
objectClass: posixGroup
objectClass: sambaGroupMapping
gidNumber: 512
cn: Administradores do Dominio
memberUid: root
description: Netbios Domain Administradores
sambaSID: S-1-5-21-2348235823-75777502-2747241662-512
sambaGroupType: 2
displayName: Administradores do Dominio

# Usuarios do Dominio, Grupos, ceeteps
dn: cn=Usuarios do Dominio,ou=Grupos,dc=ceeteps
objectClass: top
objectClass: posixGroup
objectClass: sambaGroupMapping
gidNumber: 513
cn: Usuarios do Dominio
description: Netbios Usuarios do Dominio
sambaSID: S-1-5-21-2348235823-75777502-2747241662-513
sambaGroupType: 2
displayName: Usuarios do Dominio

# Convidados do Dominio, Grupos, ceeteps
dn: cn=Convidados do Dominio,ou=Grupos,dc=ceeteps
objectClass: top
objectClass: posixGroup
objectClass: sambaGroupMapping
gidNumber: 514
cn: Convidados do Dominio
description: Netbios Convidados do Dominio Users
sambaSID: S-1-5-21-2348235823-75777502-2747241662-514
sambaGroupType: 2
displayName: Convidados do Dominio

# Computadores do Dominio, Grupos, ceeteps
dn: cn=Computadores do Dominio,ou=Grupos,dc=ceeteps
objectClass: top
objectClass: posixGroup
objectClass: sambaGroupMapping
gidNumber: 515
```

```
cn: Computadores do Dominio
description: Netbios Computadores do Dominio accounts
sambaSID: S-1-5-21-2348235823-75777502-2747241662-515
sambaGroupType: 2
displayName: Computadores do Dominio

# Administradores, Grupos, ceeteps
dn: cn=Administradores,ou=Grupos,dc=ceeteps
objectClass: top
objectClass: posixGroup
objectClass: sambaGroupMapping
gidNumber: 544
cn: Administradores
description: Netbios Domain Members can fully administer the
    computer/sambaDomainName
sambaSID: S-1-5-32-544
sambaGroupType: 5
displayName: Administradores

# Operadores de Contas, Grupos, ceeteps
dn: cn=Operadores de Contas,ou=Grupos,dc=ceeteps
objectClass: top
objectClass: posixGroup
objectClass: sambaGroupMapping
gidNumber: 548
cn: Operadores de Contas
description: Netbios Usuarios do Dominio to manipulate users
    accounts
sambaSID: S-1-5-32-548
sambaGroupType: 5
displayName: Operadores de Contas

# Operadores de Impressao, Grupos, ceeteps
dn: cn=Operadores de Impressao,ou=Grupos,dc=ceeteps
objectClass: top
objectClass: posixGroup
objectClass: sambaGroupMapping
gidNumber: 550
cn: Operadores de Impressao
description: Netbios Domain Operadores de Impressao
sambaSID: S-1-5-32-550
sambaGroupType: 5
displayName: Operadores de Impressao

# Operadores de Backup, Grupos, ceeteps
dn: cn=Operadores de Backup,ou=Grupos,dc=ceeteps
objectClass: top
objectClass: posixGroup
```

```
objectClass: sambaGroupMapping
gidNumber: 551
cn: Operadores de Backup
description: Netbios Domain Members can bypass file security to
    back up files
sambaSID: S-1-5-32-551
sambaGroupType: 5
displayName: Operadores de Backup

# Duplicadores, Grupos, ceeteps
dn: cn=Duplicadores,ou=Grupos,dc=ceeteps
objectClass: top
objectClass: posixGroup
objectClass: sambaGroupMapping
gidNumber: 552
cn: Duplicadores
description: Netbios Domain Supports file replication in a
    sambaDomainName
sambaSID: S-1-5-32-552
sambaGroupType: 5
displayName: Duplicadores

# Domain Admins, Grupos, ceeteps
dn: cn=Domain Admins,ou=Grupos,dc=ceeteps
objectClass: top
objectClass: posixGroup
objectClass: sambaGroupMapping
gidNumber: 512
cn: Domain Admins
memberUid: root
description: Netbios Domain Administrators
sambaSID: S-1-5-21-3226524203-2369515941-3762550674-512
sambaGroupType: 2
displayName: Domain Admins

# Domain Users, Grupos, ceeteps
dn: cn=Domain Users,ou=Grupos,dc=ceeteps
objectClass: top
objectClass: posixGroup
objectClass: sambaGroupMapping
gidNumber: 513
cn: Domain Users
description: Netbios Domain Users
sambaSID: S-1-5-21-3226524203-2369515941-3762550674-513
sambaGroupType: 2
displayName: Domain Users

# Domain Guests, Grupos, ceeteps
```

```
dn: cn=Domain Guests,ou=Grupos,dc=ceeteps
objectClass: top
objectClass: posixGroup
objectClass: sambaGroupMapping
gidNumber: 514
cn: Domain Guests
description: Netbios Domain Guests Users
sambaSID: S-1-5-21-3226524203-2369515941-3762550674-514
sambaGroupType: 2
displayName: Domain Guests

# Domain Computers, Grupos, ceeteps
dn: cn=Domain Computers,ou=Grupos,dc=ceeteps
objectClass: top
objectClass: posixGroup
objectClass: sambaGroupMapping
gidNumber: 515
cn: Domain Computers
description: Netbios Domain Computers accounts
sambaSID: S-1-5-21-3226524203-2369515941-3762550674-515
sambaGroupType: 2
displayName: Domain Computers

# Administrators, Grupos, ceeteps
dn: cn=Administrators,ou=Grupos,dc=ceeteps
objectClass: top
objectClass: posixGroup
objectClass: sambaGroupMapping
gidNumber: 544
cn: Administrators
description: Netbios Domain Members can fully administer the
    computer/sambaDomainName
sambaSID: S-1-5-32-544
sambaGroupType: 5
displayName: Administrators

# Account Operators, Grupos, ceeteps
dn: cn=Account Operators,ou=Grupos,dc=ceeteps
objectClass: top
objectClass: posixGroup
objectClass: sambaGroupMapping
gidNumber: 548
cn: Account Operators
description: Netbios Domain Users to manipulate users accounts
sambaSID: S-1-5-32-548
sambaGroupType: 5
displayName: Account Operators
```

```
# Print Operators, Grupos, ceeteps
dn: cn=Print Operators,ou=Grupos,dc=ceeteps
objectClass: top
objectClass: posixGroup
objectClass: sambaGroupMapping
gidNumber: 550
cn: Print Operators
description: Netbios Domain Print Operators
sambaSID: S-1-5-32-550
sambaGroupType: 5
displayName: Print Operators

# Backup Operators, Grupos, ceeteps
dn: cn=Backup Operators,ou=Grupos,dc=ceeteps
objectClass: top
objectClass: posixGroup
objectClass: sambaGroupMapping
gidNumber: 551
cn: Backup Operators
description: Netbios Domain Members can bypass file security to
    back up files
sambaSID: S-1-5-32-551
sambaGroupType: 5
displayName: Backup Operators

# Replicators, Grupos, ceeteps
dn: cn=Replicators,ou=Grupos,dc=ceeteps
objectClass: top
objectClass: posixGroup
objectClass: sambaGroupMapping
gidNumber: 552
cn: Replicators
description: Netbios Domain Supports file replication in a
    sambaDomainName
sambaSID: S-1-5-32-552
sambaGroupType: 5
displayName: Replicators

# search result
search: 2
result: 0 Success

# numResponses: 27
# numEntries: 26
```