

Zairo Afonso Balestrin

Migração para *Software Livre* no Ministério Público Federal. Estudo de caso sobre adoção do SAMBA, *Proxy Squid* e OpenOffice.org.

Monografia de Pós-Graduação “*Lato Sensu*” apresentada ao Curso de Administração em Redes Linux(ARL) da Universidade federal de Lavras como parte das exigências da disciplina Monografia para obtenção do título de Especialista em “Administração em Redes Linux”

Orientador

Professor Esp. Daniel Darlen Corrêa Ribeiro

Lavras
Minas Gerais - Brasil
2005

Zairo Afonso Balestrin

Migração para *Software Livre* no Ministério Público Federal. Estudo de caso sobre adoção do SAMBA, *Proxy Squid* e OpenOffice.org.

Monografia de Pós-Graduação “*Lato Sensu*” apresentada ao Curso de Administração em Redes Linux(ARL) da Universidade federal de Lavras como parte das exigências da disciplina Monografia para obtenção do título de Especialista em “Administração em Redes Linux”

Aprovada em *10 de Setembro de 2005*

Professor Doutor José Monserrat Neto

Professora MSc. Kátia Cilene

Professor Esp. Samuel Pereira Dias

Professor Esp. Daniel Darlen Corrêa Ribeiro
(Orientador)

Lavras
Minas Gerais - Brasil

Sumário

1	Introdução	1
2	Contextualização e Problematização	5
2.1	Ministério Público Federal(MPF)	5
2.1.1	Atuação do Ministério Público Federal(MPF)	6
2.1.2	Foco da Análise	7
2.2	Contextualização do Ambiente	8
2.3	Aspectos Legais	9
2.4	Segurança das Informações	10
2.5	Definição do Problema	10
2.6	Outras Considerações	11
3	Software Livre	13
3.1	Conceitos e filosofias	13
3.2	Software Livre na Administração Pública	16
4	Migração para Software Livre	19
4.1	Uma Visão Macro da Migração	19
4.2	Custo da Migração	20
4.3	Metodologias para Migração	20
4.4	Considerações Finais	21
5	Ferramentas Objeto da Migração	23
5.1	Samba	23
5.1.1	Um Pequeno Histórico do SAMBA	23
5.1.2	Instalação do Samba	24
5.2	Proxy Squid	24
5.3	OpenOffice.org	25
5.3.1	Instalação do OpenOffice.org	26

6	Migração para as ferramentas: SAMBA, Squid e OpenOffice.org	27
6.1	Considerações Iniciais	27
6.2	Ponto de Partida	28
6.3	Proposta de implementação	28
6.4	Apresentação e discussão da Proposta	29
6.4.1	Instalação e configuração do GNU/Linux	31
6.4.2	Considerações Sobre a Instalação e Configuração do Samba	31
6.4.3	Considerações sobre Instalação e Configuração do Squid .	32
6.4.4	Considerações sobre a migração para o OpenOffice.org . .	32
6.5	Resultados Obtidos	33
6.5.1	Resultados Obtidos com o SAMBA e Squid	33
6.5.2	Resultados Obtidos com migração para OpenOffice.org . .	34
6.6	Análise dos Resultados	34
6.7	Previsão para o futuro	36
7	Conclusão	37
8	Referências Bibliográficas	39
A	Apêndice A - Samba	43
A.1	Introdução	43
A.2	Instalação e Configuração do Samba	44
A.2.1	Configuração de <i>hardware</i>	44
A.2.2	Instalação	45
A.2.3	Configuração	46
A.2.4	Conhecendo os parâmetros	49
A.2.5	Testando o SAMBA	55
A.2.6	Acessando Servidores através de Estações Linux	55
A.2.7	Adicionando o SAMBA a um Domínio Windows NT	58
A.2.8	Adicionando estações NT Workstation ao Domínio SAMBA	58
A.2.9	Como migrar senhas do Domínio NT para o SAMBA	59
A.2.10	Exemplo de Login Script para estações Windows	60
A.2.11	Configurando o SAMBA Remotamente	61
A.3	Considerações	62
A.4	Créditos	64
B	Apêndice B - Servidor Proxy Squid	67
B.1	Introdução	67
B.2	Instalação do <i>Proxy Squid</i>	68
B.2.1	Roteiro de Instalação do Servidor <i>Proxy Squid</i>	68
B.2.2	Configuração do Servidor Proxy Squid	69
B.2.3	Configuração das estações Windows para utilizarem o Proxy	77
B.3	Gerador de Relatórios Html - SARG	78

B.4	Créditos	83
-----	--------------------	----

Lista de Figuras

2.1	Estrutura do MPF - Organograma	7
6.1	Estrutura antiga da PRM Franca	30
6.2	Estrutura atual da PRM Franca	35
A.1	Configuração de estação de trabalho winMe	61
A.2	Tela de Login do win98	61
B.1	Aba de configuração do Proxy no browser Mozilla Firefox	77
B.2	Página Principal - Index do SARG	81
B.3	Visualização do Relatório do Acesso a web, gerado pelo SARG	82
B.4	Relatório dos acessos Negados	82
B.5	Relatório das páginas mais acessadas - <i>topsites</i>	83

Lista de Tabelas

3.1	Quadro comparativo entre os modelos Cathedral e Bazar	16
6.1	Particionamento do Disco de Sistema - HD1	31
6.2	Particionamento do Disco HD2 home/ de compartilhamento . . .	31
6.3	Estrutura de arquivos, diretorios da PRM Franca	32
A.1	Particionamento do Disco de Sistema - HD1	44
A.2	Particionamento do Disco HD2 home/ de compartilhamento . . .	44
A.3	Serviços/componentes disponibilizados pelo SAMBA	46
A.4	Variáveis do SAMBA e seus significados	54

Dedico este trabalho às Comunidades Open Source, que brilhantemente vêm colaborando globalmente com a socialização e democratização do conhecimento tecnológico. Dedico também a toda equipe responsável pelo funcionamento do ARL, que com muita competência fez-nos perceber a grandeza do Software Livre, de maneira que o adotássemos em nosso dia a dia, transformando-nos em defensores dessas tecnologias

Agradecimentos

Primeiramente ao criador de tudo, Deus, que nos permitiu a realização de mais um sonho; à minha esposa Léia; aos filhos Lia e Íkaro; pelo apoio e força concedidos e principalmente pela compreensão diante do nosso trabalho, pois, por muitas vezes trocamos o afeto familiar pela árdua tarefa de autodidata, em função do curso 'Administração em Redes Linux'; à Professora Daniele Mattos pelo auxílio prestado na correção ortográfica deste trabalho; à Coordenação do ARL, por ter-nos proporcionado esta especialização e incentivado o aprendizado e a utilização de *Software Livre*; ao Professor Orientador Daniel Darlen Correa Ribeiro.

Resumo

A substituição de *Software Proprietário* por *Software Livre*, na Procuradoria da República no Município de Franca, está proporcionando uma grande economia de recursos, devido a ausência de taxas de licença sobre o uso de *Software*. Além do aspecto econômico as ferramentas *Software Livre* implementadas proporcionaram ganhos na qualidade e produtividade, além de propiciar a tão almejada **segurança**, no armazenamento e acesso aos arquivos e dados.

Este trabalho pretende abordar analiticamente, relatando os processos trilhados na migração para o *Software Livre*, na Procuradoria da República no Município de Franca, com ênfase para as ferramentas: Samba - Servidor de Arquivos ; Servidor *Proxy Squid* - Acesso a Internet e *cache*; *OpenOffice.org* - suíte para Escritório. Pretende-se sobretudo demonstrar que o uso das ferramentas *Software Livre*, estão contribuindo para o controle e segurança no acesso às informações, com aumento da qualidade e produtividade no trabalho executado.

Pretende-se ainda com esse trabalho: mostrar a outros órgãos da Administração Pública que é possível migrar, sem grandes traumas. O estudo realizado serve como um referencial para outros órgãos governamentais em futuras migrações.

Capítulo 1

Introdução

A evolução e a sofisticação das Tecnologias da Informação, cada vez mais acelerada, estão forçando as instituições a adotarem mecanismos de segurança no armazenamento dessas "informações"¹, com robustos mecanismos de controle, visando garantir a segurança e a integridade dessas "informações". Desta forma, as instituições necessitam de ferramentas capazes de implementar uma Política de Segurança. No estabelecimento de uma boa Política de Segurança deve-se segundo [UCHOA (2003b:10:11)] priorizar os aspectos inerentes a Segurança Física, Segurança Lógica, Privacidade e legalidade do *Software*, esclarecendo ainda importantes aspectos:

"É inútil elaborar uma política de segurança que sirva apenas de enfeite na parede. Assim, uma política de segurança deve possuir as seguintes características:

- ser implementável através de procedimentos de administração de sistema, regras de uso, ou outros métodos apropriados;
- ser reforçada com ferramentas de segurança e sanções;
- definir claramente as áreas de responsabilidade para usuários e administradores do sistema.

Na Administração pública, poucas instituições possuem uma política de uso para *Software* que embase uma possível escolha entre *Software proprietário* e ou *Software Livre*. Na maioria das instituições governamentais o principal fator que leva a adoção do *Software Livre*, é a dificuldade econômica/financeira reconhecida como falta de provisionamento orçamentário. Em contrapartida, temos um movimento de nível mundial em torno do *Software Livre*, principalmente entre os profissionais das áreas tecnológicas das empresas e instituições. Assim, vislumbra-se uma crescente mudança cultural, permitindo que o *Software Livre* tenha maior

¹Definição do autor para o termo Informações, no contexto desta monografia é: Arquivos ou dados armazenados em meio magnético.

aceitação, devido a seu amadurecimento contínuo e principalmente devido ao aumento do número de especialistas aptos a dar suporte a essas ferramentas.

Pesquisou-se objetivando buscar ferramentas *Software Livre* que pudessem proporcionar aos usuários a produção, armazenamento e acesso seguro aos arquivos e dados².

Dentre as várias ferramentas pesquisadas, destacaram-se os *Software Livre* desenvolvidas sob licença GPL³, dentre os quais cita-se:

- **SAMBA:** Servidor de Arquivos que permite a autenticação de usuários e controle de acesso a arquivos, além de integrar vários sistemas operacionais.
- **Proxy Squid:** O *Proxy Squid* é capaz de controlar o acesso a Internet, com alternativa de autenticar usuários, configuração de regras para o controle do acesso, além de realizar o *cache* das páginas visitadas.
- **OpenOffice.org:** Como o principal produto gerado pelo MPF⁴ são peças processuais em texto formatado, manteve-se um cuidado redobrado para escolher uma suíte⁵ que permitisse uma fácil adaptação dos usuários e manter ou elevar o nível de produtividade e qualidade do material produzido. Analisando os *Software*, acima mencionados, revelaram-se excelentes ferramentas, garantindo a produção, armazenamento e acesso seguro aos dados.

Dentro desse universo, nesta monografia, pretende-se avaliar a adoção do *Software Livre* na Procuradoria da República no Município de Franca, num estudo de caso envolvendo a utilização do SAMBA, *Proxy Squid* e OpenOffice.org, como solução para a produção, armazenamento e acesso seguro aos dados.

Na migração realizada na Procuradoria da República no Município de Franca, destaca-se o baixo custo de implementação, devido a utilização e reciclagem da estrutura antiga⁶.

Este trabalho está organizado de maneira a mostrar a migração ocorrida, especialmente na implementação do *Software Livre* Servidor de arquivos SAMBA,

²O termo arquivos e dados, aqui tratado, pode referir-se a: peças processuais em texto formatado, imagens digitalizadas, planilhas eletrônicas, relatórios e banco de dados e, que os usuários devam ter acesso com liberdade e autonomia para criação, alteração de acordo com as permissões que lhe são inerentes ao cargo.

³General Public License ou Licença Pública Geral.

⁴MPF é a sigla utilizada para designar Ministério Público Federal.

⁵Termo utilizado para designar ferramentas de escritório, agrupadas em uma única aplicação. Por exemplo o OpenOffice.org é uma suíte composta por várias ferramentas (planilha, editor de texto, etc.).

⁶Inicialmente treinou-se equipes técnicas que foram e são responsáveis pela migração. O treinamento dessas equipes técnicas foi o que viabilizou a migração no MPF, pois além de trazer o conhecimento para dentro da instituição, não demandou recursos para as tarefas de instalação, configuração, implementação e manutenção dos *Software*.

Servidor *PROXY SQUID* e a "suíte" OpenOffice.org. O Capítulo 2 trata da contextualização e problematização no Ministério Público Federal, colocando aspectos estruturais, organizacionais, aspectos legais e Segurança da informação. O Capítulo 3 trás uma conceituação de *Software Livre* e inserção deste na administração pública. No quarto Capítulo tem-se uma macro visão da Migração, tratando de custo e metodologia. O Capítulo 5 descreve as tarefas de instalação e configuração das ferramentas: Servidor SAMBA, Proxy Squid e OpenOffice.org. No Capítulo 6 tem-se uma análise evolutiva de todo o processo de migração até a análise de resultados. Por fim no Capítulo 8 apresenta-se a conclusão deste trabalho.

Capítulo 2

Contextualização e Problematização

2.1 Ministério Público Federal(MPF)

O Ministério Público é definido pela Constituição Federal como instituição permanente, essencial à função jurisdicional do Estado, incumbindo-lhe a defesa da ordem jurídica, do regime democrático e dos interesses sociais e individuais indisponíveis conforme preceituado nos artigos 127 a 135 [BRASIL (1988)]. No artigo 127, § 1º da Constituição Federal, atribui-se como princípios institucionais do Ministério Público a unidade, a indivisibilidade e a independência funcional [BRASIL (1998)].

O Ministério Público abrange:

1. O Ministério Público da União, que compreende:

- O Ministério Público Federal;
- O Ministério Público do Trabalho;
- O Ministério Público Militar;
- O Ministério Público do Distrito Federal e Territórios.

2. Os Ministérios Públicos dos Estados.

Como se vê, o Ministério Público Federal é parte do Ministério Público da União. Não se deve confundir assim, o Ministério Público Federal no Estado de São Paulo com o Ministério Público do Estado de São Paulo, regido por lei diversa. O Ministério Público Federal atua na Justiça Federal, enquanto o Ministério Público Estadual atua na Justiça Estadual.

2.1.1 Atuação do Ministério Público Federal(MPF)

A Procuradoria da República no Município de Franca vinculado ao Ministério Público Federal, que por sua vez integra o Ministério Público da União, tem por finalidade atuar na área de sua Jurisdição:

- Promovendo, privativamente, a ação penal pública, na forma da lei;
- Instaurando inquérito civil e outros procedimentos administrativos correlatos;
- Zelando pelo efetivo respeito dos Poderes Públicos e dos serviços de relevância pública aos direitos assegurados na Constituição Federal, promovendo as medidas necessárias à sua garantia;
- Promovendo o inquérito civil e a ação civil pública, para a proteção do patrimônio público e social, do meio ambiente e de outros interesses difusos e coletivos;
- Promovendo a ação de inconstitucionalidade ou representação para fins de intervenção da União e dos Estados, nos casos previstos na Constituição;
- Defendendo judicialmente os direitos e interesses das populações indígenas;
- Expedindo notificações nos procedimentos administrativos de sua competência, requisitando informações e documentos para instruí-los, na forma de lei complementar respectiva;
- Exercer o controle externo da atividade policial, na forma de lei complementar;
- Requisitando diligências investigatórias e a instauração de inquérito policial, indicados os fundamentos jurídicos de suas manifestações processuais;
- Exercendo outras funções que lhe forem conferidas, desde que compatíveis com sua finalidade, sendo-lhe vedada a representação judicial e a consultoria jurídica de entidades públicas.

Além da Constituição Federal, a definição das funções do Ministério Público da União, basicamente estão na [LEI COMPLEMENTAR 75 (1993)], que dispõe sobre a organização, as atribuições e o estatuto do Ministério Público da União.

2.1.2 Foco da Análise

Na base do Organograma mostrado na **Figura 2.1**, encontra-se a Procuradoria da República no Município de Franca, o foco desta análise. A PRM Franca¹, estava equipada com um parque computacional de 06 computadores, com sistema operacional Microsoft Windows 98 e operando em rede **sem servidor**², compartilhando arquivos e impressoras.

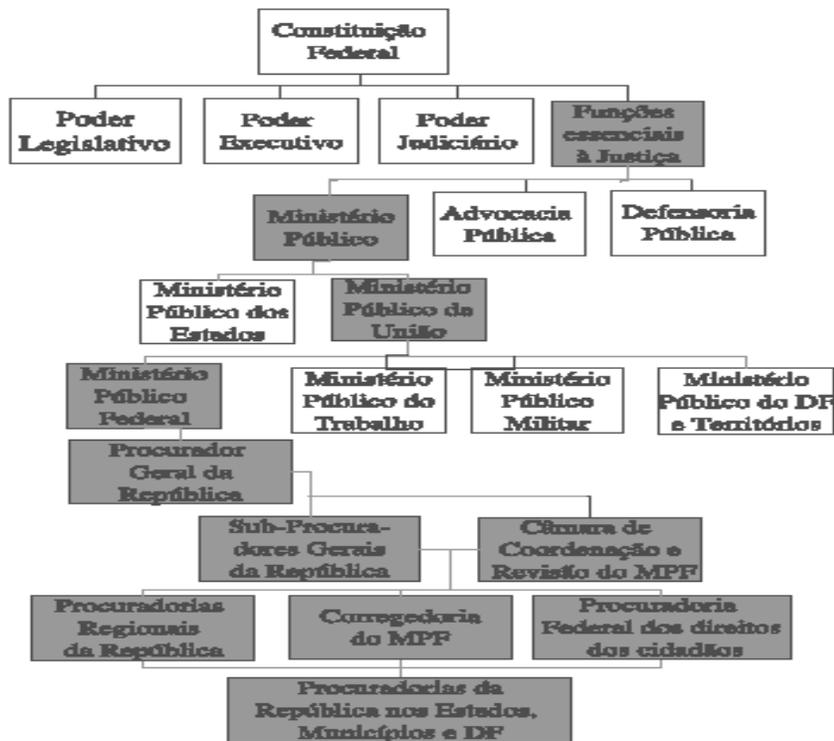


Figura 2.1: Estrutura do MPF - Organograma

¹PRM Franca é o termo abreviado para designar: Procuradoria da República no Município de Franca.

²A rede era composta por várias máquinas conectadas em rede através de um *hub*, compartilhando arquivos entre si, sem a presença de um Servidor de arquivos.

2.2 Contextualização do Ambiente

Situação Organizacional: Desde a sua criação em 1996, a PRM Franca convivia com necessidade de controlar a criação e o acesso aos arquivos e dados. Os computadores da PRM Franca já operavam em rede entretanto não se tinha qualquer tipo de controle de acesso ao compartilhamento de arquivos e dados.

Nessa época a PRM Franca estava equipada com 06 computadores rodando sistema operacional Windows 95, ligados em rede via *hub*, sem a figura cliente-servidor. Os usuários tinham nas estações de trabalho sua ferramenta para confeccionarem peças processuais, no formato texto do Microsoft Word®. O acesso aos arquivos e dados era feito livremente, através dos compartilhamentos em cada estação. Não havia nenhum controle de acesso e nem *backup* de segurança.

Iniciando as atividades na PRM Franca em julho/2002, o autor desta obra, tomou posse da situação e iniciou estudos e análises para adequar a estrutura ao atendimento das necessidades da Procuradoria. Nesse instante o volume de arquivos e dados armazenados nos computadores da PRM Franca aumentara em volume de tal forma que inviabilizou a estrutura adotada até então³.

A partir desse ponto começou-se a pensar numa solução que fosse capaz de autenticar usuários, armazenar arquivos e dados de maneira centralizada e organizada. O problema chave, além da situação apresentada, residia na inexistência de dotação orçamentária (recursos financeiros escassos), impedindo a aquisição de *Software* ou ferramentas proprietárias, como por exemplo *Network File System* para Windows e a suíte para escritório Msoffice.

Objetivando começar a montagem de uma nova estrutura, organizada, que pudesse atender as necessidades da PRM Franca, ainda em Julho/2002 foi instalado um *gateway*, com roteador, permitindo que os usuários acessassem aplicações externas a sub-rede como por exemplo Banco de dados, servidor de *e-mail* e servidor HTTP, centralizados em São Paulo, na Procuradoria da República no Estado de São Paulo. Apesar da melhoria que esse fato significou aos usuários da sub-rede, sob o aspecto de segurança era mais um problema a resolver.

Assim em agosto/2002, separamos um *hardware* que servia como estação de trabalho, praticamente ociosa e instalamos o GNU/Linux, distribuição Conectiva 8.0. Inicialmente configuramos o Servidor SAMBA e o *Proxy Squid*. O servidor estava dotado de duas placas de rede, fato aproveitado, para isolar o tráfego da sub-rede com a *web*⁴.

O SAMBA foi configurado de maneira tal que autenticasse os usuários e os arquivos foram centralizados no Servidor Samba, obedecendo uma estrutura

³Os computadores estavam conectados em rede compartilhando arquivos em dados de maneira desorganizada distribuídos em todos os pontos de rede.

⁴Uma placa de rede ficava conectada diretamente ao roteador permitindo conexão externa inclusive com a *web* e a segunda placa de rede era conectada no *hub* para fazer a comunicação cliente-servidor.

de grupos e permissões. O Servidor *Proxy Squid*, foi configurado de maneira a compartilhar o acesso a *web* e para realizar o *cache* das páginas acessadas.

2.3 Aspectos Legais

A Constituição da República Federativa do Brasil prevê em seu Art. 37, que a Administração Pública direta, indireta ou fundacional, de qualquer dos Poderes da União, dos Estados, do Distrito Federal e dos Municípios obedecerá aos Princípios Administrativos de: legalidade, impessoalidade, moralidade, publicidade e eficiência [BRASIL (1988)].

Legalidade: Qualquer ação ou ato administrativo deve estar expressamente autorizado em lei. Nada pode ser feito sem que haja uma lei ou dispositivo equivalente que autorize ou normatize os atos da Administração Pública.

Impessoalidade: Princípio que regula o tratamento igual a todos os administrados, impedindo ou proibindo o favorecimento individual de um em detrimento de outrem. Com a observância desse princípio impede-se a auto-promoção das autoridades.

Moralidade: Exigência de observação dos preceitos éticos, objetivando impedir que administradores públicos pratiquem ações privilegiando interesses próprios. Dessa forma, a atuação do administrador deve seguir padrões éticos de probidade, decoro e boa-fé.

Publicidade: Trata-se neste princípio da transparência dos atos dos administradores, garantindo que os cidadãos exerçam seus direitos de fiscalização sobre os atos dos administradores públicos.

Eficiência: Prevê que os serviços prestados pelo "estado" devem ser de alta qualidade. É através da observância desse princípio que se obtém um melhor gerenciamento de recurso, maximizando resultados e minimizando custos. Obtem-se isso com a utilização de métodos racionais, modernas técnicas e tudo dentro das normas de especificação.

Os princípios constitucionais foram citados acima para demonstrar que o Administrador Público, quando da tomada de decisões, seja para migração do *Software Livre* ou para qualquer outra ação, deve obedecer principalmente a legislação vigente que normalmente está alinhada com os princípios constitucionais da administração pública acima, destacados.

2.4 Segurança das Informações

Na PRM Franca, a informatização vem sendo utilizada continuamente, auxiliando o trabalho dos Procuradores e dos Servidores.

Os computadores ligados em rede com acesso a *web*, tornaram-se sua principal ferramenta de trabalho, permitindo-lhe armazenamento, acesso, produção e alteração de arquivos e dados. Já, em agosto/2002, a PRM Franca contava com um parque computacional de 14 estações de trabalho e mais um *hardware* para servidor da rede.

A falta de segurança e controle provocados pelo acesso compartilhado, sem autenticação, permitia que usuários tivessem acesso a documentos sigilosos, alterassem documentos indevidamente, dentre outras ações possíveis e não desejáveis. Fazer *backup* dos arquivos e dados era uma tarefa quase impossível, pois nunca se sabia qual a última versão do documento e qual o local que estavam guardados.

No contexto relatado, percebe-se que a PRM Franca é extremamente dependente do parque computacional. Manter essa estrutura funcionando de maneira que não prejudicasse o sucesso da instituição passou a ser um fator crítico.

2.5 Definição do Problema

Segundo [UCHOA (2003b)], num **ambiente computacional**, sob a ótica da segurança, os elementos Confiança, Integridade e Confidencialidade tem de ser analisados⁵.

O fato de não existir ferramentas proprietárias instaladas na PRM Franca, que atendessem a esses quesitos de segurança e, ausência de previsões orçamentárias para realizar investimentos com *Hardware e Software*, geraram **os problemas motivadores desta monografia:** "Busca de Ferramentas *Software Livre* para implementação na Procuradoria da República no Município de Franca, sem ônus orçamentário e que proporcionasse aos usuários a satisfação do Princípios Administrativos: **confiabilidade, confidencialidade e integridade dos dados** e, como substituir a suíte de escritório proprietária por uma ferramenta *Software Livre*, que fosse capaz de garantir a manutenção ou melhorar a qualidade e a produtividade atual."

Outra alternativa para o estabelecimento de mecanismos de controle de acesso e garantia da segurança das informações armazenadas na PRM Franca⁶, seria o desenvolvimento de *Software* específico para essa finalidade. Como não havia possibilidade de desenvolver tal ferramenta, por demandar alto custo com

⁵Elementos já listados no Capítulo 1.

⁶Procuradoria da República no Município de Franca.

investimentos em Recursos Humanos, só restara a alternativa de encontrar as ferramentas necessárias dentre *Software Livre* disponíveis no mercado.

2.6 Outras Considerações

O contexto analisado permitiu a escolha de ferramentas capazes de resolver os problemas detectados, direcionando a escolha para *Software Livre*: o SAMBA, o *PROXY SQUID* e, especificamente para a produção de documentos o OpenOffice.org⁷, como a única alternativa viável, principalmente devido às limitações econômicas da PRM Franca.

⁷A escolha foi o Open Office.org por ser uma ferramenta semelhante ao pacote proprietário utilizado até então e atender a todas as necessidades da PRM Franca e, por ser um *Software Livre* mais difundido no mercado.

Capítulo 3

Software Livre

3.1 Conceitos e filosofias

O Principal líder e estudioso que participou ativamente do movimento *Software Livre*, foi Richard Stallman. Não satisfeito com a política de uso do *Software proprietário*, que restringia a liberdade dos usuários, fundou, em 1984, a *Free Software Foundation*, a qual propunha-se a estabelecer a filosofia de produção do *Software Livre*, destacada em [FSF (2003)]. Os pilares que sustentam essa nova filosofia estão fundamentados em quatro tipos de liberdades:

- **(0) A liberdade de executar o programa, para qualquer propósito;**
- **(1) A liberdade de estudar como o programa funciona e adaptá-lo às suas necessidades. Acesso ao código-fonte é um pré-requisito para esta liberdade;**
- **(2) A liberdade de redistribuir cópias de modo que outros usuários possam ser beneficiados;**
- **(3) A liberdade de aperfeiçoar o programa e liberar os seus aperfeiçoamentos, de modo que toda a comunidade se beneficie. Acesso ao código-fonte é um pré-requisito para esta liberdade.**

Junto com a *Free Software Foundation* nasceu o projeto GNU¹, cujo objetivo era criar um Sistema Operacional, utilitários e aplicativos baseados na filosofia *Software Livre*. O ambiente utilizado no desenvolvimento do projeto GNU foi o Unix².

¹GNU é uma sigla recursiva que significa GNU is Not Unix. "Curiosamente, essa sigla não explica o que é GNU, mas somente o que não é"[FERRAZ (2002)].

²"O ambiente de desenvolvimento do Projeto GNU era Unix porque este era o sistema tecnicamente mais avançado, estava disponível para várias plataformas, era distribuído mais livremente que os outros sistemas, sendo por essas razões o mais popular na academia e em setores da indústria de computação"[HEXSEL (2002)].

O projeto GNU, através de Stallman nos anos 90, desenvolveu o Editor de Textos EMACS e o Compilador GCC, dentre outras ferramentas e utilitários e, através de Linus Torvalds, via ação colaborativa desenvolveu o núcleo do sistema operacional Linux³, que teve o seu código disponibilizado na internet para que outros programadores ajudassem na tarefa de criação de um sistema estável e seguro.

"Quando Linus Torvalds escreveu o Linux, ele completou a última grande lacuna. Pessoas puderam então colocar o Linux junto com o sistema GNU para compor um sistema livre completo: um sistema GNU baseado em Linux (ou sistema GNU/Linux, para simplificar) [STALLMAN (2003)]."

Graças ao Projeto GNU/LINUX agora a comunidade *Software Livre*, dispõe de uma plataforma de trabalho isenta de restrições impostas pelo *Software Proprietário*, com um sistema operacional robusto e estável e vários aplicativos e utilitários.

O que é *Software Livre*?

Um *Software* só pode ser considerado livre se atender as quatro liberdades (a liberdade de executar, alterar, redistribuir e aperfeiçoar), enumeradas anteriormente. [HEXSEL (2002)], apresenta sua definição associada a essas liberdades:

"*Software Livre (Free Software)* é o *Software* disponível com a permissão para qualquer um usá-lo, copiá-lo, e distribuí-lo, seja na sua forma original ou com modificações, seja gratuitamente ou com custo. Em especial, a possibilidade de modificações implica em que o código fonte esteja disponível. Se um programa é livre, potencialmente ele pode ser incluído em um sistema operacional também livre. É importante não confundir *Software Livre* com *Software* grátis porque a liberdade associada ao *Software Livre* de copiar, modificar e redistribuir, independe de gratuidade."

Os Métodos de produção de *Software* Catedral e Bazar

Método Bazar: Segundo Eric Raymond, este método teve início quando Linus Torvalds colocou um anúncio no *news group* informando que havia desenvolvido o *kernel* básico de um sistema tipo Unix para arquitetura X86. O *kernel* foi baseado no Minix (um sistema operacional Unix para fins didáticos desenvolvido por

³<http://www.linux.org>.

Tanenbaum). No anúncio, Linus solicita colaborações no desenvolvimento deste *kernel*. Para tanto, ele disponibilizou, sob a licença GPL, os fontes do Linux.

A partir dos muitos retornos a mensagem de Linus, criou-se uma comunidade que passou a gerar novas versões do *kernel* muito rapidamente. Este método de organizar uma comunidade que trabalha cooperativamente no desenvolvimento do *Software* funciona como um bazar generalizado, descentralizado.

Alguns aspectos são fundamentais para que um projeto de *Software* desenvolvido pelo método bazar atinja a maturidade final e necessária, transformando-se em um bom *Software* estável:

- O projeto a ser desenvolvido deve representar para a comunidade um bom objetivo que deve ser claro e de fácil motivação;
- Ter boa liderança que mantenha a comunidade motivada, não deixando que o objetivo se perca, tomando as medidas necessárias para que tudo funcione;
- A comunidade deve ter um grande número de participantes;
- Boas ferramentas e meios de comunicação, como por exemplo a Internet com suas listas, grupos de trabalho, etc..

No modelo "bazar" a comunidade desenvolve *Software* num ambiente totalmente dinâmico, com a utilização de ferramentas como: *sites*, listas de discussão e *news groups*.

O líder desempenha um papel diferente do exercido pelo projetista chefe no método "catedral". No método do bazar, o líder não distribui tarefas e a dependência do projeto com relação a ele é menor. O principal papel do líder é manter a comunidade motivada e alinhada ao objetivo.

O que hoje é uma realidade na produção de *Software*, Eric Raymond, em [RAYMOND (1998)], pode constatar através de uma análise, a funcionalidade das duas metodologias de construção de *Software*.

Método Catedral: Método baseado na concepção tradicional de produção de *Software*, suas principais características são:

- Forma centralizada e controlada de se desenvolver *Software*;
- Amplamente utilizado na indústria de *Software* e no meio acadêmico;
- Necessariamente exige a figura do arquiteto centralizador.

No método Catedral, toda a responsabilidade no projeto de desenvolvimento de *Software* é assumida pelo arquiteto centralizador.

Nessa linha de pensamento,[RIBEIRO (2004)], na Tabela 3.1, construiu um quadro, estabelecendo uma comparação entre os principais pontos dos modelos:

Tabela 3.1: Quadro comparativo entre os modelos Catedral e Bazar

<i>Modelo Catedral</i>	<i>Modelo Bazar</i>
Trabalho controlado por um grupo de projetista.	Não há hierarquia entre os participantes.
Estabelecimento de metodologias, tarefas e prazos.	Projetos informalmente organizados ao redor de uma proposta inicial.
Demora para lançamento de atualizações.	Participação voluntária de interessados.
Dificuldade para atingir massa crítica.	Atualizações constantes.
Dificuldade para atingir qualidade esperada.	Massa crítica atingida rapidamente.

Além da comprovação acadêmica sobre a eficácia deste ou daquele método, é através da utilização nas empresas e nas instituições, que o *Software Livre* vêm ganhando largas fatias de mercado em função do seu bom desempenho.

3.2 *Software Livre* na Administração Pública

A viabilidade de implementação do *Software Livre* na administração pública, na atualidade é amplamente discutida e analisada. Hoje pode-se contar com um ótimo referencial de migração na Administração Pública, o [GUIA LIVRE(2004)], comprova a viabilidade através de estudos de caso. Com isso o autor deste trabalho, está convencido de que o *Software Livre* já encontrou um grau de amadurecimento suficiente para implementação em qualquer instituição pública ou privada, inclusive com argumentação suficiente para recomendar a utilização das seguintes ferramentas, na PRM Franca.

- O SAMBA para atender à necessidades de autenticação de usuários e controle de acesso aos arquivos de trabalho em meio magnético;
- O *Proxy Squid* para controle e compartilhamento de acesso a internet, bem como criação de *cache*, tornando a navegação mais rápida e;
- O OpenOffice.org como suíte de ferramentas para escritórios, destacando-se as ferramentas: processador de texto Writer⁴, planilha de cálculos CALC⁵,

⁴WRITER - É equivalente ao Microsoft Word: É uma ferramenta para criar documentos profissionais.

⁵CALC - Planilha eletrônica equivalente ao Microsoft Excel.

Gerador de Apresentações IMPRESS⁶ e o DRAW⁷.

No caso do MPF, a migração para *Software Livre* não representou custo adicional. Os profissionais responsáveis pelo planejamento e implementação da migração já trabalhavam na instituição. Constatou-se que no MPF ocorrera um readequação e melhor aproveitamento dos Recursos Humanos. Além de muitos valores agregados que foram adicionados com a migração, podemos quantificar a economia realizada, na proporção do valor de uma Licença do *Software* proprietário da Microsoft® (Msoffice-suíte de escritório), para cada estação existente no Ministério Público Federal. Como o preço de mercado de uma suíte de escritório proprietária custa em média R\$700,00 a PRM Franca economizou (14 estações x 700,00) R\$9.800,00 (nove mil e oitocentos reais).

Não se pretende aqui descartar a necessidade de realização de planejamento econômico/financeiro do projeto de migração, mas, reforçar a idéia de que a análise ou a pesquisa de custo do projeto deve ser feito caso a caso, com critérios bem definidos.

⁶IMPRESS ou Apresentação - É equivalente ao Microsoft Power Point: Para criar apresentações multimídia

⁷DRAW - É equivalente a Corel Draw: É a ferramenta para produzir desde um simples diagrama até ilustrações dinâmicas em 3D e efeitos especiais.

Capítulo 4

Migração para *Software Livre*

4.1 Uma Visão Macro da Migração

Migrar uma estrutura computacional de produção e armazenamento de documentos e dados, do *Software* proprietário para *Software Livre* está ficando cada dia mais comum, com adesão contínua de instituições públicas e empresas privadas. Abordando esse tema o [GUIA LIVRE (2004)] remete-nos a pensar na migração como um desafio:

A mudança para *Software Livre* deve ser vista como qualquer outro tipo de migração de sistemas de TI¹. Portanto, são aplicáveis a estas migrações, desafios e possibilidades já experimentadas por todo gerente de informática. Em especial, a migração de sistemas de TI proporciona a oportunidade de realizar a reengenharia dos mesmos, para satisfazer às novas demandas a eles propostas.

Ainda, o [GUIA LIVRE (2004)] mostra uma tarefa precedente a migração e de fundamental relevância no sucesso dos processos migratórios, o planejamento:

Muito do que precisa ser feito para migrar de um ambiente proprietário para um de *Software Livre*, é semelhante a qualquer migração. Até mesmo na migração de um ambiente tecnologicamente idêntico e/ou de um mesmo fornecedor, não se pode pressupor que os formatos dos arquivos serão compatíveis e sempre haverá necessidade de testes apropriados antes de proceder a qualquer mudança mais difundida. Todas as migrações precisam ser baseadas em um cuidadoso planejamento, [...]. As diretrizes aqui presentes não pretendem ser um manual sobre gestão de projeto e supõe-se que a Administração tenha habilidade para gerenciar a migração de forma apropriada.

¹Entende-se por TI a área de Tecnologia da Informação e/ou profissionais desta área.

Essa busca e preferência pelas ferramentas *Software Livre* está acontecendo devido ao trabalho sério desenvolvido pelas comunidades *Open Source*, difundindo essa tecnologia e produzindo *Software* de boa qualidade.

4.2 Custo da Migração

Considerando o tema central desta monografia estar focando a migração de um ambiente de rede com *Software* proprietários para *Software Livre*, há necessidade de esclarecer alguns aspectos que envolvem custo de migração. No Ministério Público Federal e principalmente na PRM Franca, a migração não representou custo operacional e investimento algum. Profissionais que atuavam na área tecnológica, eram adeptos da tecnologia *Software Livre* e, na sua maioria já tinham um bom contato com os ambientes colaborativos das comunidades *Open Source*, onde buscaram o conhecimento, alinhando-se com as novas culturas tecnológicas. Assim a discussão e o planejamento da migração para o *Software Livre* teve início em ambientes virtuais. Esses profissionais da área tecnológica, inclusive o autor dessa monografia, foram responsáveis pela difusão dessas novas tecnologias e principalmente, atuaram na instalação e configuração das ferramentas tecnológicas objeto de migração.

4.3 Metodologias para Migração

O projeto de Migração, deve ser concebido como qualquer outro projeto, seguindo todas as etapas: coleta e tabulação de dados, definição do projeto e por fim transferir o projeto do papel para a prática.

Em abordagem sobre o assunto o [GUIA LIVRE (2004)], destaca a necessidade de elaboração previa de projeto com alto nível de planejamento, detalhando todas as etapas do processo.

Na Procuradoria da República no Município de Franca o levantamento inicial de dados, mostrou que não existia nenhuma política de segurança no acesso e controle dos arquivos e dados. Percebeu-se ainda que qualquer ferramenta que se introduzisse no ambiente que proporcionasse melhorias, principalmente no armazenamento e, acesso seguro aos arquivos e dados, teriam uma ótima aceitação junto aos usuários finais.

No caso o Servidor Samba e Proxy Squid, na ótica dos usuários da PRM Franca so trariam benefícios. O problema residia na migração da ferramenta de escritório OpenOffice.org, pois os usuários acostumados a utilizar outro *Software* proprietário, inicialmente apresentariam certa resistência em absorver a substituição da ferramenta de longos anos de uso.

Normalmente a resistência à mudanças está intimamente relacionado com o

"NOVO", com o "DESCONHECIDO". Diante dessa situação a alternativa viável em qualquer processo migratório é transformar o "NOVO" e "DESCONHECIDO" em "ATUAL" e "CONHECIDO". Na PRM Franca o que veio a quebrar a resistência à mudanças nos usuários, foi o envolvimento destes com o planejamento inicial e com todo o processo de migração, através dos treinamentos e reuniões.

O treinamento ministrado aos usuários teve ênfase em *Software Livre* e foi ministrado através de reuniões, mensagens de correio eletrônico, debates em fórum especialmente montado para tal. Esse treinamento foi de fundamental importância para todo processo de migração, haja visto que proporcionou a quebra da resistência dentre os usuários para com o *Software Livre* em função destes terem entendido qual a diferença existente entre *Software grátis* e *Software Livre*. Entendimento este conseguido quando os usuários tomaram conhecimento dos princípios básicos que sustentam um *Software Livre* e dos métodos de desenvolvimento de *Software* "Bazar e Catedral".

4.4 Considerações Finais

A PRM Franca, conforme comentado em capítulos anteriores, não dispunha de servidor de arquivos² instalado, que garantisse o controle e acesso seguro aos arquivos e dados, bem como não tinha nenhuma política de segurança e autenticação de usuários. Além disso, precisava renovar as licenças corporativas da suíte de escritório proprietária. Entretanto o arrocho orçamentário impedia a renovação dessas licenças.

Na migração da PRM Franca, não foram feitos testes piloto, as análises limitaram-se a consulta de casos, publicações e artigos de ferramentas livres que se prestavam a finalidade buscada, no nosso caso: servidor de arquivos, servidor proxy e suíte de escritório.

O fator preponderante na escolha das ferramentas foi a questão econômica/financeira da PRM Franca, que não dispunha de provisão orçamentária para licenciamento de *Software*.

Assim ocorreu a escolha estratégica de ferramentas *Software Livres*, sendo que os estudos feitos indicaram viabilidade para utilização de um Servidor de arquivos e dados, mais Servidor Proxy, cujo sistema operacional deveria ser um GNU/Linux com as ferramentas SAMBA e Proxy Squid. Para suíte de escritório dentre as opções analisadas elegeram-se o OpenOffice.org por ser uma das suítes de escritório mais difundidas no mundo *Software Livre*, por ser uma ferramenta de excelente qualidade e, por ter uma semelhança muito grande com a ferramenta pro-

²A rede funcionava sem a figura cliente-servidor, os arquivos e dados eram compartilhados entre as estações de trabalho.

prietária até então utilizada, facilitando assim o processo de adaptação dos usuários à nova ferramenta.

As ferramentas SAMBA, *Proxy Squid* e OpenOffice.org, serão estudadas no capítulo que se segue.

Capítulo 5

Ferramentas Objeto da Migração

5.1 Samba

O SAMBA¹ é um conjunto de aplicativos *Software Livre*, desenvolvidos sob a licença GPL, rodando sob a plataforma GNU/Linux e tem por finalidade a autenticação de usuários, compartilhamento de arquivos. Este programa adaptou-se bem em redes mistas² permitindo que usuários de diferentes plataformas compartilhem informações na rede. Numa linha de pensamento semelhante [SILVA (2004)] define o SAMBA:

"Um servidor e conjunto de ferramentas que permite que máquinas Linux e Windows se comuniquem entre si, compartilhando serviços (arquivos, diretórios, impressão) através do protocolo SMB (Server Message Block)/CIFS³ (Common Internet File System), equivalentes à implementação NetBEUI⁴ no Windows. O SAMBA é uma das soluções em ambiente Unix capaz de interligar em redes heterogêneas."

5.1.1 Um Pequeno Histórico do SAMBA

Conforme vários autores já relataram, o SAMBA nasceu a partir da necessidade de Andrew Tridgell em montar um volume UNIX num Sistema operacional DOS. DARCI (2004) descreve muito bem esse fato:

"Andrew então utilizou um método muito avançado usado por admi-

¹O Site oficial do Samba é <http://www.samba.org>.

²O SAMBA pode ser utilizado em redes de plataforma, Windows, IBM-OS, Unix, Macintosh, Amiga OS, Netware.

³<http://www.webopedia.com/TERM/N/Netbeui.html>.

⁴<http://samba.org/cifs>.

nistradores para detectar problemas: escreveu um Sniffer⁵ de pacotes que atendesse aos requerimentos para ter uma única função: analisar e auxiliá-lo a interpretar todo o tráfego NetBIOS da rede. Aos poucos Andrew percebeu que sua ferramenta ganhava robustez e de fato, conseguia interagir com sistemas operacionais concorrentes, esse fato incentivou-o a disponibilizar seu código para aprimoramentos pela comunidade GNU/Linux."

Com a abertura do código do programa *Sniffer*, a comunidade *Open Source*, em pouco tempo consegue melhorá-lo, culminando com a entrega ao mercado do Programa Servidor SAMBA, com alta maturidade e estabilidade.

5.1.2 Instalação do Samba

Normalmente todas as distribuições GNU/Linux trazem os pacotes necessários para a instalação do SAMBA, que pode ser feito em conjunto com a instalação do Sistema Operacional GNU/Linux ou, posteriormente de acordo com a necessidade do administrador. O Apêndice A, trata do assunto com muita clareza, permitindo que o administrador siga a instalação passo a passo. Desta forma torna-se dispensável relatar aqui como proceder na instalação dos pacotes do SAMBA.

5.2 Proxy Squid

Básicamente um servidor Proxy serve para compartilhar o acesso a internet entre usuários de uma rede e realização de *cache* de páginas acessadas. O [GUIA LIVRE (2004)] cita-o da seguinte maneira:

Há disponível diversos servidores *proxy em Software Livre*. Dentre os servidores proxy para http, o Squid⁶ é o mais popular, possui elementos refinados para controle de acesso, banda, hierarquias de *caches*, proxy reverso etc. Ele possui um produto associado (squidguard), que evita o acesso a sítios indesejados, classificados por conteúdo.

O Dicionário [CaeteOnLine], define o termo Proxy da seguinte forma:

⁵Programas que permitem monitorar a atividade da rede registrando nomes (username, e senhas) sempre que estes acessam outros computadores da rede. Estes programas ficam monitorando o tráfego da rede para capturar acessos a serviços de redes, tais como: serviço de email remoto (IMAP, POP), acesso remoto (telnet, rlogin, etc), transferência de arquivos (FTP), etc. Acessos feitos, pacotes capturados. Sempre com o objetivo de pegar a identificação de acesso a conta do usuário.

⁶<http://www.squid-cache.org/>.

"Um servidor (programa) proxy (ou com capacidades de proxy) recebe pedidos de computadores ligados à sua rede e, caso necessário, efetua esses mesmos pedidos (de HTTP, Finger, etc.) ao exterior dessa rede (nomeadamente, ao resto da Internet), usando como identificação o seu próprio número IP e não o número IP do computador que requisitou o serviço. Útil quando não se dispõem de números IP registados numa rede interna ou por questões de segurança."

Com enfoque parecido, [MORIMOTO (2003)], define Proxy:

"O proxy serve como um intermediário entre os PCs de uma rede e a Internet. Um servidor proxy pode ser usado com basicamente três objetivos: 1- Compartilhar a conexão com a Internet quando existe apenas um IP disponível (o proxy é o único realmente conectado à *web*, os outros PCs acessam através dele). 2- Melhorar o desempenho do acesso através de um *cache* de páginas; o proxy armazena as páginas e arquivos mais acessados, quando alguém solicitar uma das páginas já armazenadas do *cache*, esta será automaticamente transmitida, sem necessidade de baixá-la novamente. 3- Bloquear acesso a determinadas páginas (pornográficas, etc.), como tipo passa pelo proxy é fácil implantar uma lista de endereços ou palavras que devem ser bloqueadas, para evitar por exemplo que os funcionários percam tempo em *sites* pornográficos em horário de trabalho.

Hoje em dia os servidores proxy são extremamente comuns, mesmo em redes domésticas, não é necessário um PC dedicado a esta função, basta instalar um dos vários programas de servidor proxy disponíveis no PC com a conexão à Internet: Wingate, Analog-X, etc."

Instalação do Servidor Proxy Squid: Atualmente a maioria das distribuições GNU/Linux trazem consigo os pacotes necessários para instalação do Servidor *Proxy squid*. No Apêndice B, encontra-se um roteiro bastante detalhado para instalar e configurar o Servidor *Proxy Squid*, além de permitir um aprofundamento nas funcionalidades desse servidor.

5.3 OpenOffice.org

O OpenOffice.org, na opinião do autor desta monografia, classifica-se como uma boa suíte de escritório existente no mercado, com uma vantagem adicional de ser de código aberto. O [GUIA LIVRE (2004)] faz uma abordagem histórica, destacando-se os seguintes pontos:

"O OpenOffice.org é um conjunto de aplicações para escritórios do *Software Livre* baseado no StarOffice, produzido por uma empresa alemã chamada StarDivision. A Sun Microsystems, comprou a StarDivision e franqueou o código à comunidade de *Software Livre*. Continua a colocar no mercado uma versão do OpenOffice.org, ainda chamada de StarOffice, que vende a um preço muito mais barato do que os pacotes proprietários correspondentes.[...]

Ambos os aplicativos são comparáveis às suítes de *Software* proprietário, porém alguns componentes destas suítes podem não estar contemplados, podendo ser obtidos à parte, também em *Software Livre*. Ambos os pacotes lidam com a maior parte dos arquivos de formato proprietário, até e inclusive as versões mais recentes destes, embora a compatibilidade possa piorar com as versões mais novas. Não lidam com arquivos protegidos por senhas (exceto para proteção de planilhas página a página) e tem alguns problemas com objetos gráficos com link com OLE. Ainda assim, têm algumas das melhores integrações de formatos de arquivos de outras ferramentas de Escritório.

Dentre as principais características do OpenOffice.org, podemos citar: ferramenta tecnológica confiável; funcional; flexível e; economicamente viáveis.

Inicialmente o OpenOffice.org atrai a atenção de empresas e instituições devido a este reunir num só pacote um conjunto de aplicativos como: editores de textos, planilhas eletrônicas, desenhos, apresentações, fórmulas matemáticas e acesso a dados; ter custo de licenciamento zero; possuir interface familiar; possibilitar a utilização em diversos sistemas operacionais (Windows, Solaris, GNU/Linux, FreeBSD e MacOS); ser compatível com formatos de arquivo de outros pacotes proprietários; estar disponível em vários idiomas inclusive em português do Brasil.

5.3.1 Instalação do OpenOffice.org

Em janeiro de 2004, instalou-se o OpenOffice.org versão 1.0 ptBR. Atualmente as estações da PRM Franca, estão com a versão 1.1.3 ptBR.

Quanto a instalação propriamente dita, dispensa-se qualquer comentário. Todas as distribuições para a plataforma Windows, vem com programa instalador "setup.exe", que automatiza todo o processo de instalação.

Atualmente encontra-se em fase de desenvolvimento e testes a versão Beta 2.0, inclusive na PRM Franca através do autor desta monografia. Preliminarmente essa versão Beta 2.0, está apresentando várias melhorias, com correção às versões anteriores e, sua interface está muito mais semelhante a concorrente ferramenta proprietária.

Capítulo 6

Migração para as ferramentas: SAMBA, *Squid* e OpenOffice.org

6.1 Considerações Iniciais

A PRM Franca¹, foi orientada pela administração central PGR², à migrar gradativamente seus aplicativos proprietários para aplicações não proprietárias.

A migração foi concebida devido a: necessidade de armazenar e permitir o acesso controlado e seguro, aos arquivos e dados; inexistência de verbas orçamentárias destinadas a aquisição de licenças; alinhamento às diretrizes para Política de *Software* na Administração Pública.

Objetivou-se buscar sem custos adicionais soluções para controlar e manipular arquivos em meio magnético, controle de acesso a Internet com realização de *cache* e, principalmente, substituir o pacote de escritório MsOffice para o OpenOffice.org, com ganho de produtividade e qualidade.

Convém salientar que a principal mercadoria gerada pela PRM Franca são peças processuais no formato texto, em que se utilizava o *Software* MsWord®. Sem a figura do servidor de arquivos, o armazenamento dessas peças era realizado de maneira desorganizada, sem nenhum controle de acesso, provocando um caos no ambiente. Quando necessitava-se consultar alguma peça já produzida, era uma tarefa quase impossível: a única maneira de localizá-la era fazer uma varredura em todas as máquinas da Procuradoria. Por consequência disso tudo, era impossível implementar uma política de *backup* segura que compreendesse todos os dados necessários a serem resguardados.

Apesar do quadro anteriormente descrito ser caótico, sabia-se da existência das ferramentas capazes de reverter a situação. Os recursos humanos do MPF enquadravam-se como servidores públicos, com certa resistência a mudanças e

¹Procuradoria da República no Município de Franca.

²PGR, sigla utilizada para designar: Procuradoria Geral da República.

acostumado a utilizar o pacote proprietário da Microsoft.

O que veio a provocar a quebra da resistência à mudanças nos usuários da PRM Franca, além dos benefícios provocados no ambiente de rede com o SAMBA e o Proxy, foi a conscientização para a tecnologia *Software Livre* introduzida através de treinamento e reuniões. Como resultado desse trabalho, obteve-se usuários comprometidos com o processo de migração e conscientes de que este processo não representaria apenas redução de custos para a PRM Franca, mas uma melhora na qualidade e produtividade dos serviços executados.

6.2 Ponto de Partida

Inicialmente desenvolveu-se um trabalho de treinamento da equipe técnica, através de cursos e autodidatismo, objetivando equipar as Unidades do MPF com o conhecimento tecnológico necessário para empreender a migração. Considerando que na estrutura antiga os usuários da PRM Franca não dispunham de nenhum mecanismo de controle de acesso e autenticação, o autor deste trabalho entendeu ser desnecessário discutir ou negociar as etapas da implementação das ferramentas: Servidor SAMBA e Servidor *Proxy Squid*. O que interessava ao usuário final era saber se as ferramentas exerceriam a função para o qual estavam sendo implementadas. Tomando por base estudos de casos, como por exemplo [GUIA LIVRE (2004)], [RIBEIRO (2004)], [DARCI (2004)], comprova-se que as ferramentas escolhidas cumprem a função desejada.

6.3 Proposta de implementação

O Projeto de migração contemplava basicamente as seguintes etapas:

1. Treinamento de Pessoal na área tecnológica, tornando-os aptos a administrarem as ferramentas;
2. Instalação e configuração do Sistema GNU/Linux;
3. Estruturação da PRM Franca em grupos por afinidades do trabalho executado;
4. Criação dos usuários e grupos de usuários de acordo com a estrutura de afinidades;
5. Instalação e configuração do Servidor SAMBA;
6. Implementar o acesso à internet via servidor *Proxy Squid*;

7. Criação das pastas e diretórios de acordo com a necessidade dos grupos e usuários;
8. Agrupamento dos arquivos e dados espalhados pelas diversas estações de trabalho, centralizando-os no servidor Samba de acordo com a estrutura de grupos e usuários criada anteriormente;
9. Criação dos *scripts* de *logon* e *profiles* dos usuários;
10. Configuração das estações Windows® (Windows 98);
11. Instalação da suíte de escritório OpenOffice.org;
12. Substituição do Sistema Operacional Windows®(Windows 98) por Sistema Operacional GNU/Linux.

6.4 Apresentação e discussão da Proposta

Antes de iniciar a migração na PRM Franca, foram feitas várias reuniões apresentando a todos os servidores como seria a nova estrutura. Os usuários da rede foram levados a pensar sobre os problemas que a estrutura antiga estava causando para a instituição, com ênfase nos seguintes itens:

- **Duplicidade de arquivos:** Pelo fato de não existir servidor de arquivos e frente à necessidade de compartilhamento de certos arquivos, utilizava-se a prática de compartilhamento destes entre todas as estações Windows 98, gerando duplicidade de arquivos, desperdício de tempo e de recursos, além de um total descontrole no armazenamento das informações.
- **Inviabilidade para realizar *backups*:** Não era possível manter uma rotina de *backup* geral dos dados dos usuários. Alguns usuários mantinham as informações ou dados mais importantes em disquetes, na sua maioria os dados eram armazenados no HD³ de cada estação e em pastas com denominação aleatória a gosto de cada usuário.
- **Falta de controle de acesso:** Devido a inexistência de servidor, não havia controle de acesso. Frequentemente deparava-se com problemas de perda de informações e ou alterações indevidas, sem poder identificar quem ou qual usuário teria sido responsável pela ocorrência.
- **Produtividade e Qualidade:** A Figura 6.1 representa a estrutura antiga da PRM Franca. Uma estrutura não planejada, provocando desorganização

³*hard disk*, disco rígido, *winchester* ou unidade de disco fixo de armazenamento de dados.

no ambiente de rede e contribuindo com a baixa produtividade e qualidade nos serviços. Devido à inexistência de monitoramento dos usuários e do sistema, perdia-se muito tempo em atividades não afins ao objetivo do MPF, como acessos indevidos à internet, leitura de *e-mails* particulares e etc..

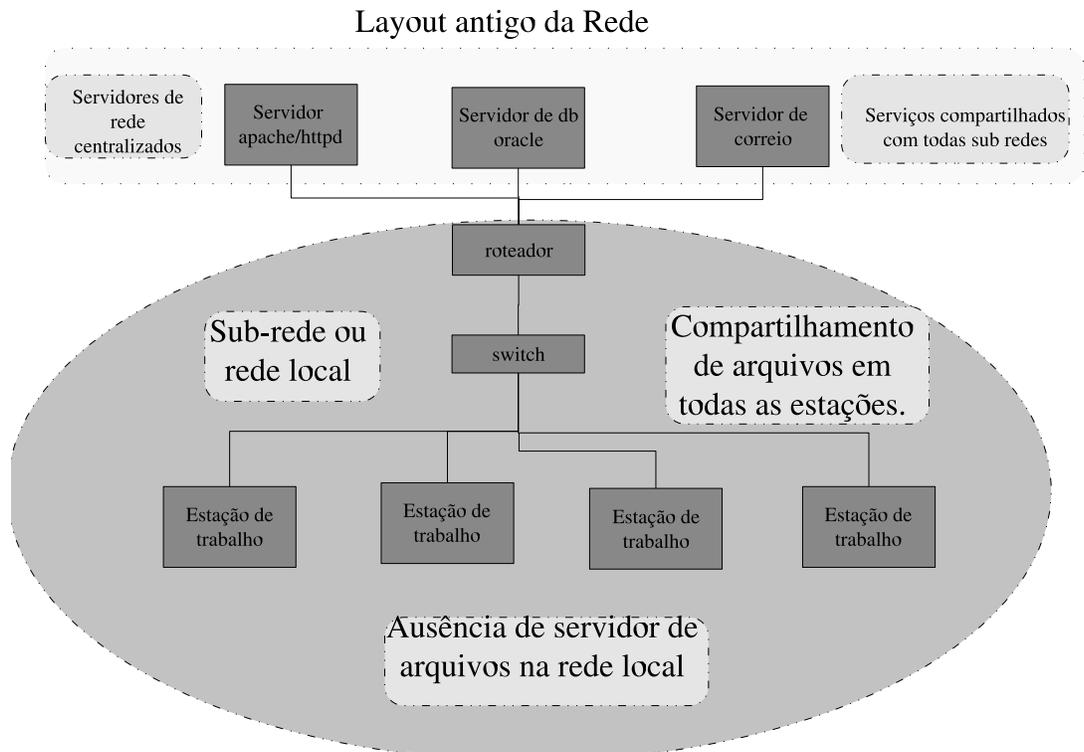


Figura 6.1: Estrutura antiga da PRM Franca

- **Acesso à Internet sem controle:** Cada estação acessava à Internet diretamente sem nenhum controle.
- **Sub utilização de periféricos:** Inexistia o compartilhamento de impressoras e periféricos.
- **Custo de Software:** Gastava-se muito com licenças de *Software proprietário*.
- **Aspectos Positivos:** Destacava-se um ponto positivo que era a boa estrutura física e de *hardware* das redes locais. A PRM Franca dispunha de cabeamento estruturado e um parque computacional atualizado e com uma boa política de *upgrade*.

6.4.1 Instalação e configuração do GNU/Linux

Após apresentação e discussão da proposta para migração e de posse da orientação superior para migrar, instalou-se o Genu/Linux, distribuição Conectiva 8.0. Nessa instalação, além do Sistema Operacional GNU/Linux, priorizou-se a instalação das ferramentas necessárias para a migração, como por exemplo o SAMBA e o Proxy Squid. O *hardware* utilizado nessa instalação foi um computador com a seguinte configuração: processador Intel, Pentium II de 350MHZ, com 256MB de memória RAM e 2Hds de 20GB cada. As Tabelas 6.1 e 6.2 mostram com detalhes o particionamento dos discos.

Tabela 6.1: Particionamento do Disco de Sistema - HD1

<i>Particao</i>	<i>Tamanho</i>
Swap	0,25GB
Raiz	3,00GB
/etc	3,00GB
/var	8,00GB
/log	6,75GB

Tabela 6.2: Particionamento do Disco HD2 home/ de compartilhamento

<i>Particao</i>	<i>Tamanho</i>
/home	20,0GB

6.4.2 Considerações Sobre a Instalação e Configuração do Samba

O SAMBA, por ocasião da instalação do GNU/linux, também foi instalado. Neste momento fez-se a configuração através da edição do arquivo */etc/smb.conf*.

O servidor Samba foi configurado para ser o controlador de domínio(PDC) e na seção global a *diretiva security = user*, atribuiu-lhe a função de autenticar usuários.

Iniciou-se a migração gradativa, visando minimizar os impactos ao usuário final. Implementou-se o servidor SAMBA, montando uma estrutura de diretórios e arquivos de acordo com a necessidade de cada setor. No **Apêndice A** temos um detalhamento completo para a configuração do SAMBA, especialmente para configuração de grupos e usuários.

A árvore de arquivos e diretórios do servidor SAMBA, foi desenhada dentro da partição */home* de maneira que pudesse atender as necessidades dos grupos e

usuários da PRM Franca. Sobre a criação dos grupos e dos usuários, temos no Apêndice A um detalhamento de como proceder na criação de grupos, usuários e diretórios. Na Tabela 6.3 mostra-se com clareza a estrutura montada.

Tabela 6.3: Estrutura de arquivos, diretorios da PRM Franca

<i>Recurso criado</i>	<i>Localização do recurso</i>	<i>Grupo</i>
Usuários	/home/usuarios	
Diretório Gabinetes	/home/gabinetes	gabinetes
Diretório Secretarias	/home/secretarias	Secretarias
Diretório Administrativo	/home/administrativo	administrativo
Diretório Informatica	/home/informatica	informatica
Diretório Processual	/home/processual	processual
Diretório Bases	/home/bases	
Diretório Procedimentos	/home/procedimentos	procedimentos
Diretório Público	/home/publico	publico

6.4.3 Considerações sobre Instalação e Configuração do Squid

A exemplo do SAMBA, o Proxy Squid, também foi instalado por ocasião da instalação do GNU/Linux. O principal ponto a destacar é o fato de que o Squid foi configurado para autenticar usuários através do SAMBA. Para que isso fosse possível foi inserido a seguinte diretiva no arquivo `/etc/squid/squid.conf`:

```
authenticate_program /usr/lib/squid/smb_auth -W prm-franca  
-U 200.222.11.33.
```

No **Apêndice B**, encontra-se uma abordagem completa, orientando a instalação e configuração. O referido Apêndice também contempla a instalação e configuração do SARG, implementado na PRM Franca para analisar os *logs* gerados pelo Proxy Squid.

6.4.4 Considerações sobre a migração para o OpenOffice.org

No início de 2004, iniciou-se a discussão em torno da proposta de migração do OpenOffice.org com os usuários. Na sequência instalou-se conjuntamente com a ferramenta proprietária a suíte OpenOffice.org, objetivando o auto-treinamento dos usuários. Nessa época, foi distribuída impressa, uma apostila que contemplava as ferramentas planilha eletrônica e editor de texto, disponível em [METRO (2004)].

Durante todo ano de 2004, os servidores da PRM Franca foram incentivados a conhecerem o OpenOffice.org, que já estava instalado em suas estações de trabalho.

Várias reuniões foram realizadas e, uma lista de discussão foi criada para

que os usuários pudessem interagir e expor suas dúvidas e medos. Em agosto/2004, os servidores da PRM Franca foram comunicados através de Circular interna de que a partir de janeiro/2005 as estações de trabalho seriam equipadas somente com a *suíte* de escritório OpenOffice.org e, informava ainda tal circular, que a troca de documentos entre setores e unidades deveriam ser feitos nos formatos nativos do OpenOffice.org ou no formato PDF.

Diante do fato que marcava data para a migração definitiva, intensificaram-se os trabalhos pré-migração, sendo que o autor desta monografia procurou maior interação com os usuários via lista de discussão e *e-mail*, buscando aprimorar o treinamento para com a ferramenta. A reação dos servidores da PRM Franca em relação ao fato de já terem data certa para a migração ocorreu dentro do esperado sem maiores percalços, pois já estavam familiarizados com a ferramenta.

Visando dar suporte à migração plena e sem imprevistos, iniciou-se desde agosto até dezembro/2004 uma análise rigorosa no banco de modelos e documentos da PRM Franca, convertendo-os para o padrão nativo do OpenOffice.org, corrigindo qualquer incompatibilidade encontrada. Houve vários modelos que não encontraram a compatibilidade necessária para serem convertidos automaticamente, tendo de ser reconstruídos por inteiro.

Em janeiro de 2005, no primeiro dia de expediente dos servidores da PRM Franca, não mais existia a *suíte* de escritório proprietária instalada. As estações de trabalho estavam agora equipadas somente com a *suíte* de escritório OpenOffice.org. O expediente de trabalho desse dia e dos dias que se seguiram foi normal, sem qualquer dificuldade para localizar ou salvar arquivos.

6.5 Resultados Obtidos

6.5.1 Resultados Obtidos com o SAMBA e Squid

Com a implementação do servidor SAMBA e SQUID, o acesso a arquivos, diretórios, dados e a *web* passou a ser controlado através da autenticação. Os usuários passaram a acessar arquivos e dados somente até o limite de suas permissões, que lhe foram concedidas pelo administrador da rede, quando da configuração do GNU/Linux e SAMBA.

No momento do acesso à rede a estação de trabalho executa automaticamente um *script*, contendo as informações necessárias para converter os acessos autorizados (pastas, arquivos e dados), em unidades mapeadas, melhorando o acesso e a manipulação desses recursos.

6.5.2 Resultados Obtidos com migração para OpenOffice.org

As licenças que a PRM Franca dispunha da suíte proprietária era limitado ao MsWord®, editor de texto da Microsoft. Com a migração além do ganho econômico tivemos uma melhoria acentuada na qualidade da *suíte de escritório*, devido à ausência de limitações quanto ao uso de suas ferramentas. Os usuários, de posse de uma suíte de escritório completa, passaram a ter mais recursos para produção de documentos, passando a produzir mais e melhor.

6.6 Análise dos Resultados

A implementação de *Software Livre* em substituição ao pacote proprietário (SAMBA, PROXY SQUID e OpenOffice.org), proporcionaram um bom controle de acesso às informações, aumento da produtividade e qualidade, maior dinâmica no acesso às informações, maior segurança no armazenamento de dados e redução do retrabalho. Algumas das melhorias trazidas pela migração podem ser assim descritas:

- **Compartilhamento de arquivos:** Os arquivos e dados são compartilhados utilizando a estrutura do servidor SAMBA.
- **Acesso a internet mais rápido e seguro:** O acesso a internet é realizado através da autenticação dos usuários via SAMBA, com utilização dos recursos do servidor *PROXY SQUID*, possibilitando aos usuários uma navegação mais segura e mais rápida, haja vista a utilização do recursos de *cache*⁴ e *ACLs*⁵
- **Controle de acesso aos dados:** A autenticação dos usuários feita pelo SAMBA, permitiu controlar o acesso aos arquivos e dados de acordo com a permissão dada a cada um, através do mapeamento de unidades feito pelo *script de logon* na inicialização da estação de trabalho. Esse mapeamento de unidades, permite ao usuário acessar arquivos ou dados no servidor como se estivesse acessando na sua própria estação de trabalho.
- **Possibilidade de backup de segurança:** Com arquivos e dados armazenados de maneira organizada e centralizada no servidor SAMBA, permitiu segurança e eficácia na realização de *backups*.

⁴É um recurso que permite aos navegadores de Internet armazenar páginas visitadas com frequência. Cada site visitado é guardado no *cache* do navegador, como um arquivo temporário, para que, na próxima visita, a página seja visualizada mais rapidamente.

⁵ACL's = Access Control List, traduzindo tem-se: Lista de Controle de Acesso. Nada mais são que regras permitindo ou negando determinados recursos.

- **Produtividade, qualidade** A estrutura de arquivos e dados montada através do SAMBA, proporcionou um ambiente mais organizado, permitindo inclusive monitoramento dos trabalhos executados. Os usuários da rede, sabendo da monitoração do sistema, passaram a concentrar seus esforços nas atividades inerentes aos seus cargos, onde se constatou melhora na qualidade e produtividade.

Com a migração implementada e reestruturação dos processos internos a rede de computadores da Procuradoria da República no Município de Franca passou a ter um *layout* demonstrado na Figura 6.2.

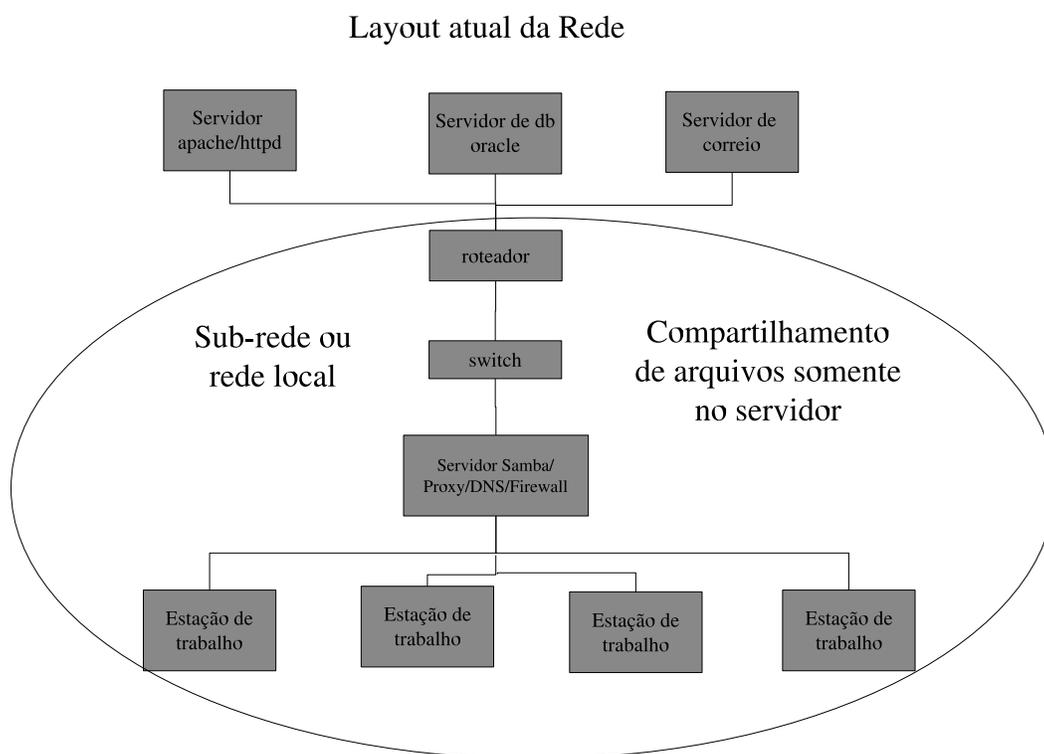


Figura 6.2: Estrutura atual da PRM Franca

O estudo realizado mostrou que as ferramentas SAMBA, Squid e OpenOffice.org, já estão bastante difundidas em instituições públicas. A migração na PRM Franca foi um sucesso, permitindo solucionar o problema motivador desta monografia:

"Busca por ferramentas *Software Livre* para implementação na Procuradoria da República no Município de Franca, sem ônus orçamentário

e que proporcionasse aos usuários a satisfação dos Princípios Administrativos: **confiabilidade, confidencialidade e integridade dos dados** e, como substituir a suíte de escritório proprietária por uma ferramenta *Software Livre*, que fosse capaz de garantir a manutenção ou melhorar a qualidade e a produtividade atual".

O princípio da confiabilidade foi garantido com a utilização ferramentas (SAMBA, SQUID e OpenOffice.org), que se apresentaram altamente estáveis. A confidencialidade está garantida desde o momento que foram criadas pastas individuais com acesso restrito para cada usuário e estabelecimento de permissões para acesso às demais pastas. A integridade dos arquivos e dados foi garantida com a implementação de um armazenamento estruturado e implementação de uma política de *backup*. A utilização das ferramentas *Software Livre* garantiram o atendimento do objetivo de migrar sem custos adicionais ou, gastos com licenciamento de *Software*. Com a implementação das ferramentas e a reestruturação do ambiente computacional, constatou-se que a PRM Franca já vem obtendo ganhos na qualidade e na produtividade, atendendo assim outra meta buscada com a migração.

6.7 Previsão para o futuro

A composição das estações de trabalho da PRM Franca, atualmente, utilizam o Sistema Operacional "Windows 98". Devido a previsão anunciada pela Microsoft, sobre a descontinuidade de suporte para o Sistema Operacional "Windows 98", já está em andamento um programa visando dar suporte e estrutura à migração das estações para o Sistema Operacional GNU/Linux.

Realizaram-se testes com uma distribuição masterizada pelo MPF, baseada nas distribuições DEBIAN e Kurumin. Testes foram feitos ainda, com base no Mandrake 10.0 e Conectiva 10.0.

Para as aplicações que utilizam banco de dados⁶, serão reescritas futuramente as interfaces de acesso com base em PHP e Java, visando tornar esse acesso ao Banco de Dados totalmente compatível com a *web/browser*, facilitando desta maneira a portabilidade dos aplicativos para qualquer plataforma ou Sistema Operacional.

Acredita-se que até o final do primeiro semestre de 2006 o MPF já tenha treinado os usuários e implementado o sistema operacional GNU/Linux nas Estações de Trabalho.

⁶No MPF os aplicativos utilizam : 90% Banco de dados Oracle 9.0 e 10% MySQL.

Capítulo 7

Conclusão

Com o advento e popularização da Internet o mundo tecnológico experimenta uma evolução acelerada, onde, num espaço de tempo cada vez mais curto, novos paradigmas surgem. Neste cenário, a *Informação*, destaca-se como um patrimônio muito valioso para as corporações, sejam elas públicas, ou privadas.

O *Software Livre* apresentou-se como uma dessas evoluções tecnológicas e, dentre as várias ferramentas existentes destacam-se o Servidor SAMBA, Servidor PROXY SQUID e a *suíte de escritório* OpenOffice.org, como ferramentas capazes de garantir a: produção, armazenamento, alteração e acesso seguro a essas informações.

O ambiente analisado apresentou problemas relacionados com o gerenciamento das *informações*, com disponibilidade de recursos financeiros. A partir dessa análise encontrou-se o problema motivador desta monografia: "Busca de Ferramentas *Software Livre* para implementação na Procuradoria da República no Município de Franca, sem ônus orçamentário e que proporcionasse aos usuários a satisfação dos Princípios Administrativos: **confiabilidade, confidencialidade e integridade dos dados** e, substituição da *suíte* de escritório proprietária por uma ferramenta *Software Livre*, que fosse capaz de garantir a manutenção ou melhorar a qualidade e a produtividade."

A migração com a implementação das ferramentas de *Software Livre* proporcionou a implantação de uma ótima Política de Segurança no acesso e armazenamento aos arquivos, dados e informações.

No estudo de caso realizado, além de comprovar a viabilidade técnica e econômica do uso das ferramentas *Software Livre*, concluiu-se que um dos melhores aliados no processo de migração de *Software* é a conscientização e treinamento das partes envolvidas, principalmente os usuários dos Software, proporcionando-

lhes conhecimento suficiente para compreenderem os conceitos básicos de *Software Livre* e como são desenvolvidos.

Sob todos os aspectos (econômico, técnico e administrativo), a migração na Procuradoria da República no Município de Franca foi um sucesso, entretanto saliente-se que neste caso especificamente, o sucesso econômico-financeiro veio devido a uma gestão dos recursos tecnológicos e humanos da estrutura existente, onde os recursos humanos foram insentivados a se auto-treinarem para o *Software Livre*.

Considerando o sucesso na implementação de *Software Livre* na Procuradoria da República no Município de Franca, pretende-se que este estudo de caso sirva como um referencial para futuras migrações, dentro do Ministério Público Federal e para outros órgãos.

Para o futuro, conforme consta da proposta de migração, pretende-se atingir um ambiente computacional 100% *Software Livre*, com a migração da plataforma Windows 98 para GNU/Linux, do banco de dados proprietário para **SGBD Livre** e, por fim, migrar o ambiente de servidor de correio e mensagens.

Capítulo 8

Referências Bibliográficas

[BRASIL (1988)] BRASIL. Constituição da República Federativa do Brasil, 1988. Disponível em <http://legis.senado.gov.br>
Último acesso: 15 de fevereiro de 2005.

[CaeteOnline] CaeteOnLine, Dicionário de termos técnicos disponível em <http://www.caeteonline.com.br/dicionario/dicionario.php>

[DARCI (2004)] DAMBRÓS, DARCI Junior, MIGRAÇÃO DE SERVIDOR DE ARQUIVOS MICROSOFT USANDO SAMBA - ESTUDO DE CASO SOBRE A ADOÇÃO DO SAMBA NO SERVIÇO NACIONAL DE APRENDIZAGEM COMERCIAL - SENAC CONCÓRDIA/SC. Monografia apresentada ao curso de Administração em Redes Linux (ARL) da Universidade Federal de Lavras como parte das exigências da disciplina Monografia para obtenção do título de Especialista em Administração em Redes Linux. Gentilmente disponibilizada pelo autor.

[DI PIETRO (2001)] DI PIETRO, Maria Sylvia Z. Direito Administrativo. São Paulo, Atlas, 13a. ed. 2001.

[FERRAZ (2002)] FERRAZ, Nelson Corrêa T. Vantagens Estratégicas do *Software Livre* para o Ambiente Corporativo. São Paulo, PUC-SP, 2002. Monografia de conclusão do curso Master Business Information Systems.

[FSF (2003)] FREE SOFTWARE FOUNDATION. O que é *Software Livre*. Disponível em: <http://www.gnu.org/philosophy/free-sw.pt.html>.
Atualizado em 11/02/2005. Último acesso em 14 de março de 2005.

[GUIA LIVRE (2004)] Guia Livre - Referência de Migração para *Software Livre* do Governo Federal- Versão Ipiranga. Último acesso em 16/03/2005, em:

<http://www.governoeletronico.gov.br>

[HEXSEL (2002)] HEXSEL, Roberto André. Propostas de Ações de Governo para Incentivar o Uso de *Software Livre*. Curitiba, UFPR 2002. Relatório Técnico RT-DINF 004/2002. Disponível em:

<http://www.inf.ufpr.br/~roberto>. Último acesso em 14 de março de 2005.

[LEI COMPLEMENTAR 75 (1993)] LEI COMPLEMENTAR, Lei Complementar 75 (1993), consultada em 24/03/05 - disponível em:

<http://www.senado.gov.br/sicon>.

[MEIRELLES (1996)] MEIRELLES, Hely Lopes. Direito Administrativo Brasileiro. Rio de Janeiro, Malheiros Editores, 21a. ed. 1996.

[MORIMOTO (2003)] MORIMOTO, Carlos E. Dicionário Termos Técnicos de Informática. 3a. ed. - versão e-book - Último acesso em 15/03/05, disponível em:

<http://www.guiadohardware.net>

[METRO (2004)] METRO, site de apostilas da suíte de escritorio OpenOffice.org, em:

<http://www.metro.sp.gov.br>

[RAYMOND (1998)] RAYMOND, Eric S. The Cathedral and the Bazaar. Último acesso em 14 de março de 2005, disponível em:

<http://www.catb.org/~esr/writings/cathedral-bazaar>

[RIBEIRO (2004)] RIBEIRO, Daniel Darlen Corrêa. Monografia : *Software Livre* na Administração Pública. Estudo de caso sobre adoção do SAMBA na Auditoria Geral do Estado de Minas Gerais. Monografia apresentada ao curso de Administração em Redes Linux (ARL) da Universidade Federal de Lavras como parte das exigências da disciplina Monografia para obtenção do título de Especialista em Administração em Redes Linux. . Último acesso 15/03/2005, disponível em www.rau-tu.unicamp.br/nou-rau/Softwarelivre

[SICA; UCHOA (2003)] SICA, Fernando Cortez; UCHOA, Joaquim Quinteiro. Administração de Sistemas Linux. Lavras, UFLA/FAEPE, 2003. Curso de Pós Graduação "Lato Sensu"(Especialização) à distância em Administração de Redes Linux.

[STALLMAN (2003)] STALLMAN, Richard. Linux e o Projeto GNU. Último acesso em 14 de março de 2005. Disponível em:

<http://www.gnu.org/gnu/linux-and-gnu.pt.html>

[UCHOA (2003b)] UCHOA, Joaquim Quinteiro. Segurança em Redes e Criptografia. Lavras, UFLA/FAEPE, 2003. Curso de Pós Graduação "Lato Sensu"(Especialização) à distância em Administração de Redes Linux.

Apêndice A

Apêndice A - Samba

A.1 Introdução

Neste Apêndice demonstra-se como foi realizada a configuração completa do SAMBA, possibilitando a integração com estações Windows. Segue abaixo um tutorial bem abrangente e muito detalhado, utilizado pelo pessoal da área tecnológica do MPF na configuração dos servidores de arquivos SAMBA.

O que é o Samba: Em uma rede é necessário compartilhar dados, por isso deve-se pensar em obter o máximo em qualidade do sistema ou aplicação que será o responsável por esta tarefa. Com o SAMBA é possível compartilhar diretórios, impressoras, acessar arquivos na rede exatamente como em redes Microsoft, somente com a diferença de que o servidor é um Linux rodando uma aplicação específica.

O Windows NT e o 2000 (assim como o NetWare e outros presentes no mercado) são reconhecidos mundialmente por sua segurança e escalabilidade, mas o SAMBA possui muitas vantagens que podem se transformar em soluções: permite compatibilidade com estações Windows e servidores WinNT, entre servidores e estações Linux (com Interface Gráfica por exemplo) a compatibilidade é total. O SAMBA é 100% configurável, com a grande vantagem de centralizar esta configuração em um único arquivo, o `/etc/smb.conf`.

Sem dúvida é muito interessante ter a possibilidade de restaurar toda a configuração que disponibiliza o Servidor de Arquivos, inclusive as permissões de acesso, através do *backup* de apenas 1 arquivo, em casos de desastre. Porém isso não quer dizer que não seja necessário o *backup* de outros arquivos de configuração.

Em se falando de economia não há o que discutir: o GNU/Linux e o SAMBA estão disponíveis para download na Internet sem ônus algum para qualquer usuário comum, órgãos governamentais ou empresas que se interesse em utilizá-lo, sem custos com licenças ou atualizações.

As mais recentes distribuições já trazem o SAMBA como padrão, mas seu down-

load e atualizações estão disponíveis em:

<http://us4.samba.org/samba/>. O suporte está disponível 24h por dia, o ano todo: além do próprio site do SAMBA existem milhares de *sites* e listas de discussão dedicadas ao assunto, entre outras documentações e artigos em *sites* de renome mantidos por Administradores e Engenheiros de Redes Linux. Muita coisa já está em nosso idioma facilitando os iniciantes e interessados em leitura. Muitos *sites* nacionais são especializados em Linux e Segurança para Linux.

A.2 Instalação e Configuração do Samba

A.2.1 Configuração de *hardware*

Utilizando-se o sistema Operacional GNU/Linux, tem-se um melhor aproveitamento de *hardware*, prolongando a vida útil de certos equipamentos. Para instalação do Servidor de Arquivos SAMBA, na PRM Franca não foram utilizadas máquinas novas, foram aproveitadas máquinas descartadas devido ao *upgrade* em alguns servidores. A configuração disponibilizada foi: processador Intel, Pentium II de 350MHZ, com 256MB de memória Ram e 2Hds de 20GB cada. Esses servidores foram dotados de sistema operacional GNU/Linux com a distribuição Conectiva 8.0 e com a seguinte especificação de particionamento dos discos, demonstrada nas Tabelas A.1 e A.2:

Tabela A.1: Particionamento do Disco de Sistema - HD1

<i>Particao</i>	<i>Tamanho</i>
Swap	0,25GB
Raiz	3,00GB
/etc	3,00GB
/var	8,00GB
/log	6,75GB

Tabela A.2: Particionamento do Disco HD2 home/ de compartilhamento

<i>Particao</i>	<i>Tamanho</i>
/home	20,0GB

Recomenda-se o particionamento físico dos itens acima por questões de segurança. As partições /log e /var são partições de muito acesso, ou seja de acesso continuado em função das características de nosso servidor (SAMBA e *Proxy Squid*), os logs e o *cache* e permanentemente atualizado e por consequência provocando também um acesso continuado ao disco, podendo provocar um desgaste maior nesses setores do disco. Outro ponto favorável a esse tipo de particionamento é a facilidade de recuperação da configuração original em função da reinstalação ou perda de alguma partição do disco - tudo isso é possível é claro, desde que se tenha um bom sistema de *backup* implementado.

A.2.2 Instalação

As distribuições do GNU/Linux mais recentes, já trazem o SAMBA incluído no seu sistema de pacotes¹, permitindo que a instalação do pacote ocorra a partir da mídia de instalação do Sistema Operacional GNU/Linux ou posteriormente, quando desejado.

Para instalação do SAMBA faz-se necessário antes de iniciar, saber se o pacote obtido está no formato RPM ou .tar (.tgz ou .tar.gz). Se o pacote for um RPM, **executa-se o comando abaixo:**

```
# rpm -ivh samba-2.0.x2-i386.rpm [enter]
```

Para atualizar o SAMBA atual, substitua a sintaxe -ivh por -Uvh.

Se o pacote está no formato tar.gz, execute-se o comando abaixo:

```
# tar -zxvf samba-2.0.x-i386.tar.gz
```

Um diretório será criado com o nome samba-2.0.x. Entrando-se neste diretório e em seguida no subdiretório source, inicia-se a instalação digitando-se:

```
# ./configure
```

Em seguida:

```
# make
```

Os binários do SAMBA serão criados. Quando terminar digita-se:

¹Conectiva, RedHat, Mandrake, Debian, TechLinux, Suse, praticamente todas.

²Substituindo o "x" pelo número relativo a versão do pacote ou o nome correto do pacote dependendo da sua distribuição.

```
# make install
```

Neste ponto os binários e páginas do man serão instalados. Aguarda-se o processo terminar, para então conferir o diretório `/usr/doc/samba-2.0.x/docs` onde estão as páginas de informações sobre o SAMBA.

A.2.3 Configuração

Recomenda-se realizar a configuração do SAMBA através da edição do arquivo "smb.conf", que na maioria das distribuições por padrão encontra-se no diretório `/etc` ou `/etc/samba`. Nele é que estão descritos os compartilhamentos, permissões de acesso, impressoras, dentre outras configurações disponíveis. A Tabela A.3, contempla os diversos serviços fornecidos pelo SAMBA.

Tabela A.3: Serviços/componentes disponibilizados pelo SAMBA

<i>Sigla</i>	<i>Descricao</i>
smbd	O servidor SAMBA.
nmbd	O Servidor de nomes NetBios
smbclient	Cliente SMB para sistemas Unix.
smbpasswd	Alterar senhas (encriptadas) de usuários smb.
smbprint	Cliente para envio de impressão a sistemas Linux.
smbstatus	Apresenta a situação atual das conexões SMB no Host.
testparm	Verifica o arquivo smb.conf (configuração do SAMBA).
testprns	Verifica a comunicação via rede com as impressoras.

O smb.conf é dividido basicamente em três partes:

1. Configuração do servidor SAMBA (parâmetros na seção [global]);
2. Configuração dos diretórios/pastas pessoais dos usuários (parâmetros na seção [homes])
3. Demais seções que correspondem aos diretórios compartilhados.

Cada seção é representada entre colchetes [seção], e os parâmetros são seguidos do sinal de igual (=) e o valor ou termo correspondente.

Na sequencia apresenta-se um exemplo do smb.conf para um servidor Samba como PDC da rede:

```
[global]
comment = Servidor SAMBA
workgroup = MPF_FRA
security = user
os level = 100
announce as = NT Server
domain logons = yes
logon script = %U.bat
logon path = //%L/Profiles/%U
domain master = yes
local master = yes
preferred master = yes
guest account = nobody
encrypt passwords = yes
wins support = yes
keep alive = 20
debug level = 3
winpopup command = csh -c 'xedit %s;rm %s' &
log file = /var/log/samba_log.%u
null passwords = no
unix password sync = yes
socket options = IPTOS_LOWDELAY TCP_NODELAY
printing = bsd
printcap name = /etc/printcap
load printers = yes
hosts allow = 200.XXX.0. 127.#colocar aqui a faixa de endereços IPs que terao
acesso, inclusive o localhost
hosts deny = 200.XXX.0.3 200.XXX.0.4
#Colocar aqui algum endereço cujo acesso seja negado

[homes]
comment = Pastas dos Usuarios
public = no
browseable = yes
writeable = yes
hosts deny = 200.XXX.0.25 #Usuário sem acesso ao Home.
```

```
[printers]
comment = Impressoras Linux
public = no
browseable = yes
printable = yes
read only = yes
create mode = 0700
path = /var/spool/samba
admin users = admin, usuario1
```

```
[netlogon]
comment = Scripts para Compartilhamento/mapeamento
path = /etc/scripts
public = no
browseable = yes
writeable = no
```

```
[Gabinete_A]
comment = Gabinete do Procurador A
path = /home/Gabinete_A
public = no
browseable = yes
valid users = @Gabinete_A
writeable = yes
write list = @Gabinete_A
force create mode = 0777
force directory mode = 0777
```

```
[processual]
comment = Grupo Processual
path = /home/processual
public = yes
browseable = yes
writeable = yes
write list = @processual
read list = @processual
force create mode = 0777
force directory mode = 0777
```

```
[protocolo]
comment = Grupo Protocolo
```

```
path = /home/protocolo
public = yes
browseable = yes
writeable = yes
write list = @protocolo
read list = @protocolo
force create mode = 0777
force directory mode = 0777
```

```
[administrativo]
comment = Grupo Administrativo
path = /home/administrativo
public = yes
browseable = yes
writeable = yes
write list = @administrativo
read list = @administrativo
force create mode = 0777
force directory mode = 0777
```

```
[admin$]
comment = Especifico do Admin
path = /home/admin
copy = homes
max connections = 1
```

A.2.4 Conhecendo os parâmetros

Seção [global]: Define as configurações globais do SAMBA. A relação abaixo apresenta a explicação dos parâmetros do exemplo:

comment: Comentário para este Host na Rede.

workgroup: Especifica o Domínio ou Workgroup a que o Host pertence na Rede.

security: Por padrão o SAMBA utiliza a segurança a nível de usuário (security = user), com opções:

security = share: Senhas de acesso serão solicitadas por cada recurso compar-

tilhado e não por usuário, ou seja, cada diretório ou impressora poderá ter uma senha única conhecida pelos usuários autorizados. Esta opção é geralmente usada p/ estações de trabalho Linux, onde em diversos casos simplifica o acesso a dados locais quando necessário.

security = user: As permissões são dadas de acordo com o login do usuário, ou através dos grupos (@grupo).

security = server: O SAMBA tentará validar a senha do usuário enviando os dados para outro servidor SMB, como outro servidor SAMBA ou um servidor Windows. Deve-se incluir o parâmetro `password server = x.x.x.x` na seção[global] do `smb.conf`.

security = domain: Usado se o Host for adicionado a um Domínio Windows através do comando `smbpasswd`. Neste caso as informações de usuário e senha serão enviadas para o PDC da rede, exatamente como o servidor NT faria. Note que é necessário que a conta do usuário exista tanto no Linux quanto no servidor primário (mais adiante isso será explicado de forma detalhada).

os level: Este parâmetro não é obrigatório se você não possui um servidor Linux ou Windows na rede, mas deve ser usado caso tenha um ou mais. A variável é um número de 1 a 255, onde 65 é a mesma variável utilizada pelo servidor Windows. Especifique um número maior que este (como 100 por exemplo) para garantir que o servidor SAMBA seja eleito na escolha de validação do login das estações.

announce as: Permite especificar o tipo de servidor NetBios (nmbd) que será divulgado na rede. As opções aceitas pelo SAMBA: "NT Server", "NT Workstation", "Windows 95" ou "WfW".

domain logons: Usado para validar o login na rede, apenas para estações Windows.

logon script: Indica qual arquivo de logon script será executado para os usuários. A variável %u corresponde ao usuário na rede. Deve também ser criado um compartilhamento de nome [netlogon] apontando para o diretório dos scripts.

logon path: Indica o caminho do perfil remoto do usuário. A variável %L corresponde ao nome do servidor NetBios (que pode ser o próprio SAMBA). O logon path é útil quando usuários costumam efetuar logon em mais de um Host na rede, pois seu perfil é trazido com o logon. No caso do exemplo, o diretório "Profiles" deve conter os scripts (em formato Microsoft usando NET USE e etc) e os scripts devem ser criados com o notepad do Windows por exemplo, a fim de con-

servar o formato do arquivo.

domain master: Indica se o Host será o Domain Master Browser da rede inteira (WAN).

local master: Indica se o Host será o Master Browser da rede local.

preferred master: Este parâmetro força a eleição do SAMBA como Master Browser para o workgroup. É recomendável utilizar este parâmetro em conjunto com o "domain master = yes" para garantir a eleição. Mas tome cuidado: se você possui uma rede com servidores Windows e SAMBA e já possui um servidor como Domain Master, não use esta opção e deixe o parâmetro "os level = 65" para haver equilíbrio.

guest account: O SAMBA trabalha melhor em redes Microsoft com a existência de uma conta guest (visitante em inglês). Por padrão a conta usada é nobody (a mesma utilizada pelo Apache).

wins server: Indica qual o servidor de Wins da rede. Se o próprio Host for o servidor de Wins então não utilize este parâmetro, pois haverá um loop e o sistema travará!

wins support: Permite ao SAMBA ser o servidor de Wins na rede. Isto significa que o SAMBA terá uma tabela com o ambiente completo da rede, garantindo que as estações tenham acesso a estas informações e ganho em velocidade para encontrar e acessar os compartilhamentos e impressoras. O Wins Server deve ser especificado na configuração de rede (TCP/IP) das estações, indicando o endereço IP do servidor.

keep alive: Como máquinas rodando Windows tendem a travar com o passar do tempo, este parâmetro é usado para verificar o estado da conexão, evitando tráfego desnecessário na rede. Também pode ser usado para estações Linux.

debug level: Parâmetro usado para dar flexibilidade a configuração do sistema. Permite ao SAMBA trabalhar corretamente com algumas situações de erro, por exemplo.

winpopup command: Especifica qual comando será executado quando o servidor receber mensagens Winpopup. Aqui, muitas opções podem ser usadas de acordo com a preferência do Administrador. Se sua rede utiliza mensagens deste tipo, é interessante definir um comando para o parâmetro, evitando assim possíveis mensagens de erro para quem enviou a mensagem ao servidor.

log file: Indica o arquivo de log do SAMBA. A variável %u corresponde ao nome de logon do usuário. O samba por padrão gera arquivos de log em /var/log/samba que indicam por exemplo os horários de logon dos usuários, quem acessou determinado arquivo, etc. Esteja atento para estas informações para consultas quando necessário.

null passwords: Indica se será ou não possível que usuários tenham senha nula de logon (logon sem senha). unix password sync. Se este parâmetro for ativado (= yes) então clientes SMB (como estações Windows) poderão trocar sua senha de login.

socket options: Este parâmetro permite configurações extras para o protocolo, possibilitando uma melhor performance do servidor em lidar com os pacotes na rede.

printing: Indica qual o sistema de impressão padrão utilizado pelo Linux.

printcap name: Indica o arquivo para busca das definições das impressoras.

load printers: Disponibiliza as impressoras para a rede.

hosts allow: Indica quais máquinas tem acesso ao servidor SAMBA. Pode-se utilizar o endereço IP ou o nome da máquina. Para garantir acesso a toda uma rede por exemplo, escreva: "hosts allow = 200.142.XX.". Este parâmetro deve ser usado preferencialmente nas demais seções, mas também pode ser usado na seção Global.

hosts deny: Como em "hosts allow", mas para restringir o acesso ao servidor SAMBA.

Seção [homes]: Define os parâmetros para as pastas pessoais dos usuários na rede (home dir):

comment: Comentário para este compartilhamento.

public: Também conhecido como guest ok, permite ou não acesso de outros usuários.

browseable: Define se o compartilhamento será ou não visível para o Ambiente de Rede. Estações Windows95 versão 4.00.950-C não aceitam esta opção, onde uma possível solução é utilizar o nome do compartilhamento seguido de \$ (teste\$ por exemplo), como faz-se no Windows.

writable: Indica se o usuário poderá ou não escrever em sua pasta pessoal (home dir).

Seção [shares]:Correspondem aos compartilhamentos presentes na rede. Os parâmetros abaixo são apenas alguns dos possíveis que podem ser utilizados:

comment: Comentário para o compartilhamento.

path: Caminho do diretório compartilhado.

valid users: Este parâmetro é usado para destacar quem terá acesso ao compartilhamento na rede. É importante destacar que estações Windows 95/98/Me têm diferenças entre si que em muitas situações representam um problema para acesso e segurança. Acontece algumas vezes de você definir o *write list* e o *read list* corretamente mas mesmo assim usuários do *read list* conseguem escrever no compartilhamento (!). Para resolver este problema, inclua o *valid users* indicando os usuários que têm acesso e em seguida inclua o *write list* e o *read list* conforme sua necessidade.

writable: Indica se será ou não possível criar ou excluir arquivos ou diretórios do compartilhamento.

public / guest ok: Indica se será ou não permitido o acesso de outros usuários.

browseable: Define se o compartilhamento será ou não visível para o Ambiente de Rede do Windows (apresentado na rede).

write list: Define os usuários e/ou grupos com acesso de escrita no compartilhamento. Para mais de um usuário, separe os nomes por vírgula (user1, user2, etc) e para grupos utilize @ antes do nome do grupo.

read list: Como em *.write list.*, mas define quem terá permissão de apenas leitura.

force create mode: Diz ao SAMBA para forçar o tipo de permissão dos arquivos criados (o mesmo que usar o *chmod*). Esta permissão tem menor prioridade que os parâmetros *write list* e *read list*.

force directory mode: O mesmo que *force create mode*, mas para os diretórios criados no compartilhamento.

admin users: Indica quais são os usuários com permissão completa para o com-

partilhamento (permissão de root).

copy: Permite copiar os parâmetros de outra seção, como um template por exemplo, útil se utiliza compartilhamentos semelhantes. Para alterar parâmetros basta informá-los na seção atual.

hosts allow: Indica quais máquinas podem acessar o compartilhamento. Pode-se utilizar o endereço IP ou o nome da máquina. Para garantir acesso a toda uma rede classe C por exemplo, escreva: "hosts allow = 200.142.XX.XX".

hosts deny: Como em "hosts allow", mas para restringir o acesso ao compartilhamento.

max connections: Permite especificar o número máximo de conexões simultâneas ao compartilhamento.

max disk size: Permite especificar qual o limite de espaço em disco que o compartilhamento pode utilizar. Este valor é definido em Mb (megabytes).

O SAMBA possui variáveis de ambiente, muito úteis na administração e monitoração do servidor. É importante que os administradores de rede tenham conhecimento destas variáveis, para melhor gerirem suas redes. Na Tabela A.4 relacionam-se todas as variáveis do SAMBA com seu significado.

Tabela A.4: Variáveis do SAMBA e seus significados

<i>Variavel</i>	<i>Significado</i>
%S	Nome do Serviço (compartilhamento) atual
%u	Nome do usuário.
%g	Nome do grupo.
%H	Nome do diretório pessoal do usuário (home dir).
%m	Nome da máquina cliente fornecido pelo NetBios.
%L	Nome do servidor NetBios, permitindo que a configuração desejada seja alterada de acordo com o cliente que vai acessar o sistema.
%M	Nome Internet da máquina cliente.
%a	Sistema Operacional da máquina remota, onde os reconhecidos são WfW, Windows NT e Windows 95.
%I	O endereço IP da máquina cliente.
%T	Data e horário.

A.2.5 Testando o SAMBA

Após a configuração do SAMBA, através do `smb.conf`, sugere-se realizar um teste para verificar se está tudo correto, utilizando-se para isso o comando `testparm`:

```
# testparm > teste_config_samba
```

O comando acima gerará o arquivo `teste_config_samba`, registrando neste todo o teste realizado. Caso houver algum erro registrado no arquivos, indica que existe alguma inconsistência na configuração que precisa ser corrigida. Acertadas as configurações, deve-se ativar o SAMBA:

```
# /etc/rc.d/init.d/smb start
```

Querendo conferir se o SAMBA está realmente no ar, executa-se o comando acima substituindo o "start" por "status".

```
# /etc/rc.d/init.d/smb status
```

Para que o SAMBA seja iniciado sempre após a inicialização do servidor, deve-se inserir linha de "start" do smb no arquivo `/etc/rc.d/rc.local`, da seguinte forma:

```
# vi /etc/rc.d/rc.local.
```

Escreve-se a seguinte linha: `/etc/rc.d/init.d./smb start`

Nas estações Linux, é necessário que cada estação contenha um `smb.conf`, se diretórios locais precisarem ser compartilhados, sendo necessário dar um "start" exatamente como no servidor, onde o `smbclient` deve ser utilizado para acessar os compartilhamentos disponíveis no servidor.

A.2.6 Acessando Servidores através de Estações Linux

O `smbclient`: Da mesma forma que o SAMBA permite que o Linux atue como servidor para estações Linux e redes Microsoft, ele também permite atuar como estação de trabalho para acessar servidores de ambos sistemas, sem que nenhuma configuração seja necessária no servidor. Com o `smbclient` é possível acessar dados em um servidor Windows, podendo ser usado para receber e enviar arquivos, listar diretórios, navegar pelos diretórios, renomear

e apagar arquivos, entre outros.

Para verificar quais compartilhamentos estão disponíveis em um determinado Host, executa-se:

```
$ smbclient -L host_desejado
```

A resposta será uma lista de serviços, ou seja, nomes de dispositivos ou impressoras que podem ser compartilhados com os usuários na rede. A menos que o servidor SMB não tenha itens de segurança configurados, será solicitada uma senha antes de mostrar as informações. Exemplo:

```
$ smbclient -L servidor1
```

A resposta será semelhante a:

```
Server time is Fri Dec 22 15:58:02 2000
Timezone is UTC+10.0
Password:
Domain=[EMPRESA] OS=[Windows NT 4.0]
Server=[NT LAN Manager 4.0]
Server=[servidor1] User=[] Workgroup=[MPF_FRA] Domain=[]
Sharename Type Comment
ADMIN$ Disk Remote Administration
Public Disk Public
C$Disk Default Share
Print$ Disk Printer Control
```

Para acessar uma pasta compartilhada, basta especificar o caminho na rede, conforme abaixo:

```
$ smbclient //maquina/pasta1 senha
```

Onde "senha" é literalmente a senha de acesso. Se o caminho estiver correto a resposta será algo como:

```
Server time is Fri Dec 22 16:01:12 2000
Timezone is UTC+10.0
Domain=[EMPRESA] OS=[Windows NT 4.0] Server=[NT LAN Manager] smb:>.
```

O smbtar: Também é possível fazer *backup* (cópias de segurança) para o formato .tar de arquivos que estão em compartilhamentos na rede.

Esta operação é muito útil para garantir *backup* de arquivos em estações com pas-

tas compartilhadas mas que não pertencem ao Domínio da rede (por exemplo) ou em estações isoladas da rede. O comando utilizado é o `smbtar`:

```
$ smbtar -s HOST -p SENHA -x COMPARTILHAMENTO -d PASTA -t FITA (.tar)
```

Para que o *backup* seja guardado em fita deve-se mudar a sintaxe do comando, substituindo o nome do arquivo pela unidade de fita instalada (geralmente `/dev/st0`).

O `smbpasswd`: O SAMBA permite também que as estações troquem suas senhas de logon, utilizando o `smbpasswd`. Ele age de forma similar ao comando `passwd`, mas as senhas são armazenadas no arquivo `smbpasswd`. É possível ainda alterar a senha dos usuários em um servidor Primário de um Domínio NT (PDC). Se utilizado pelo superusuário, permite ainda, que contas sejam adicionados ou removidos e atributos sejam alterados. Para isso deve-se manter o "localhost" especificado no parâmetro "allow hosts" para seu perfeito funcionamento.

O `smbpasswd` é um arquivo em formato ASCII e contém o nome do usuário, identificação junto ao Linux, a senha encriptada, o indicador de como está a conta e a data de última alteração da senha do usuário. Vale destacar que o `smbpasswd` somente é útil quando o SAMBA está configurado para utilizar senhas criptografadas.

O `smbstatus`: Para saber a situação atual das conexões SAMBA, utilizamos o `smbstatus` (`$smbstatus`). Abaixo está a lista das opções aceitas:

- b -> Fornece uma resposta resumida.
- d -> Fornece uma resposta comentada.
- L -> Lista somente os recursos em uso.
- p -> Lista os processos `smbd` e finaliza em seguida. Útil quando utilizado em programas.
- S -> Lista todos os compartilhamentos definidos.
- s -> Permite utilizar outro arquivo de configuração (`smb.conf2` por exemplo), que deve ser especificado após a opção.
- u -> Lista as informações relevantes sobre o usuário, que deve ser especificado após a opção.

O `testprns`: O `testprns` verifica o nome da impressora junto ao `smbd`, a fim de determinar se há um nome válido (entrada encontrada em `printcap` para a impressora) sendo informado para uso pelo serviço de impressão. Pode ser ativado da seguinte forma:

```
# testprns nome_da_impressora nome_do_arquivo_printcap
```

Encontrada uma impressora válida, a mensagem "Valid Printer"(ou outra semelhante, dependendo da distribuição utilizada) será apresentada. O arquivo /etc/printcap define as impressoras.

A.2.7 Adicionando o SAMBA a um Domínio Windows NT

Possuindo um servidor PDC (WindowsNT) e desejando-se adicionar um servidor SAMBA, é necessário antes de tudo configurar o SAMBA: não utilizar o parâmetro "domain master" e "domain logons"(conforme o caso) e também manter o parâmetro "os level" inferior a 65.

O nome NetBios do servidor SAMBA deve também ser adicionado ao PDC do Domínio NT (através do Gerenciador de Servidores para Domínios). Assim, uma conta será criada para o SAMBA no PDC. Como exemplo, vamos citar um servidor SAMBA como o nome NetBios "Samba" e o Domínio chamado "MPF_FRA". O PDC terá o nome "File_Server". Para juntar-se ao Domínio, o servidor SAMBA deve executar o comando abaixo:

```
smbpasswd -j MPF_FRA -r File_Server
```

Se o comando for bem sucedido, aparecerá a mensagem:

```
# smbpasswd: Joined domain MPF_FRA
```

Se algo der errado, confere-se o nome NetBios dos servidores, se o SAMBA está ativado, os parâmetros do smb.conf e tenta-se novamente. O comando acima ativa o protocolo de mudança de senhas, gerando uma nova conta aleatória para o servidor SAMBA, normalmente guardada em: /usr/local/samba/private.

O nome do arquivo será semelhante a: Organizacao.Samba.mac. Em seguida, edita-se o smb.conf incluindo os seguintes parâmetros na seção [global]:

```
security = domain #Pois agora o SAMBA pertence a um Domínio existente.
```

```
workgroup = MPF_FRA #Este é o Domínio utilizado.
```

```
encrypt passwords = yes #Para logon encriptado.
```

```
password server = File_Server Backup1 Backup2 #Autenticação no domínio.
```

A.2.8 Adicionando estações NT Workstation ao Domínio SAMBA

Possuindo um PDC SAMBA e estações Windows NT Workstation, deve-se seguir o modelo abaixo para criar contas específicas para estas estações. Importante: só é necessário adicionar estações NT Workstations a um Domínio SAMBA se a encriptação de login estiver habilitada. Após o Service Pack 3 este padrão

foi adotado p/ o NT, e no SAMBA é necessário especificar o parâmetro `encrypt passwords = yes`.

Em primeiro lugar, não existindo o arquivo `smbpasswd` deve-se cria-lo, utilizando o comando abaixo especificado e dando-se a permissão apropriada:

```
# touch /usr/local/samba/private/smbpasswd
# chmod go-rwx /usr/local/samba/private/smbpasswd
```

Dependendo da distribuição o arquivo `smbpasswd`, pode estar no diretório `/etc` como link (ou não) para seu diretório original, guardando muitas vezes a configuração sem nada escrever em `/usr/local/samba/private/smbpasswd`. Antes de tudo confere-se a localização correta do arquivo e só então segue-se em frente.

Seguindo adiciona-se a conta NT, onde o exemplo abaixo utiliza o nome de usuário "login" e o grupo "dominio" (que deve ser criado manualmente com o comando `groupadd`), que não contém password, shell ou diretório home.

```
adduser -g dominio -c NTWorkstation -d /dev/null -s /bin/false -n login$
```

Adicionando a conta ao smbpasswd, digitando:

```
# smbpasswd -a -m login$
```

Para que a estação NT Workstation possa agora participar do Domínio, no Painel de Controle do NT seleciona-se Network -> Identification Tag. Mudar o Domínio para o especificado no `smb.conf` (`workgroup = ...`). Não se deve marcar a opção "Create a Computer Account in the Domain".

A.2.9 Como migrar senhas do Domínio NT para o SAMBA

Quando se deseja migrar de um servidor Windows NT para o SAMBA um dos problemas mais comuns é o fato de que as senhas de logon são perdidas, pois entre o NT e o SAMBA a criptografia está em formatos diferentes. Para resolver este problema existe um pequeno programa que converte todo o registro de "nome e senha" do Windows NT para um arquivo `smbpasswd` compatível com o SAMBA.

Vejamos um exemplo:

O primeiro passo é conectar-se ao ftp do Samba e baixar o utilitário `pwdump.exe`, em:

```
ftp://ftp.samba.org/pub/samba/pwdump/pwdump.exe.
```

Seguindo Efetua-se logon como usuário Administrator no servidor NT (que dispo-

nibiliza a autenticação). Na sequencia, abre-se um Command Prompt executando-se o comando pwdump da seguinte maneira:

```
C:> pwdump > smbpasswd
```

Será gerado um arquivo smbpasswd com as informações de autenticação (logon e senha) do Windows NT no formato criptografado utilizado pelo SAMBA. Finalmente copia-se o arquivo smbpasswd gerado para o servidor Linux no diretório /etc definindo as permissões para 600:

```
# chmod 600 /etc/smbpasswd
```

Para obter um perfeito funcionamento o ID dos usuários deve ser o mesmo, tanto no smbpasswd, quanto no passwd do Linux. Na verdade não é necessário ter a senha no passwd, apenas o login, ID, home e senha smbpasswd, para rodar o SAMBA e ele autenticar os usuários.

A.2.10 Exemplo de Login Script para estações Windows

O login script (ou logon script) é uma ferramenta muito útil para disponibilizar recursos na rede. O script abaixo é um exemplo que pode usado em redes com estações Windows. Note que a sintaxe do comando net é diferente para sistemas 95/98/Me e NT.

```
rem Logon script padrão para a rede.
net time servidor1 /set /yes
@echo off
if %OS%.==Windows_NT. goto WinNT
:Win95
net use X: servidor1pasta_01
net use Z: /HOME
goto end
:WinNT
net use X: servidor1pasta_01 /persistent:no
net use Z: /HOME /persistent:no
:end
```

textbfEstações Windows devem estar com o TCP/IP configurado corretamente (IP, Máscara de SubRede, Wins se existir, identificação, domínio e etc).

Essas configurações podem ser incluídas ou alteradas acessando-se as propriedades da rede, conforme mostra a figura A.1

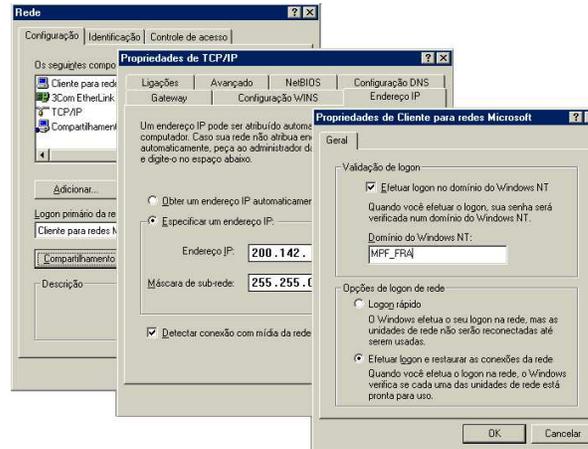


Figura A.1: Configuração de estação de trabalho winMe

Para acessar um compartilhamento samba de uma estação Windows, devidamente configurada, basta conectar-se, conforme login da Figura A.2

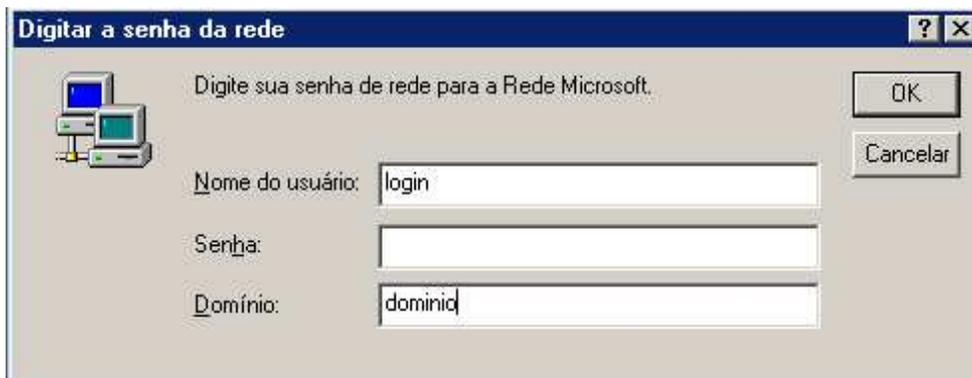


Figura A.2: Tela de Login do win98

A.2.11 Configurando o SAMBA Remotamente

Além de ser um *Software* de uso livre e compatível com redes existentes, o SAMBA ainda possui outra característica: permite ser administrado remotamente.

Para isso utilizam-se programas específicos que geralmente trabalha via http. É possível monitorar através de sua rede interna ou mesmo através da Internet. Os principais programas são o SWAT, Webmin e o LinuxConf, SSH, VNC entre outros. Neste trabalho não pretende-se demonstrar como instalar ou utilizar esses aplicativos, entretanto indicamos o link Linux:
<http://us4.samba.org/samba/GUI>, onde poderá ser encontrado vasto material para a finalidade.

A.3 Considerações

O SAMBA permite ainda muitas outras configurações que podem ser consultadas através do man do smb.conf. Uma documentação importante está em /usr/doc/samba-2.0.x/ com dicas e referências à segurança, navegação, compatibilidades, etc.

Uma característica das versões mais recentes do SAMBA é a possibilidade de um cliente WinNT usar sua interface nativa de configuração para ver e modificar permissões no Linux. O parâmetro *"nt acl support = yes"* deve ser adicionado na seção [global] do smb.conf.

É aconselhável reiniciar o SAMBA a cada modificação no smb.conf (embora não seja realmente necessário), principalmente em se tratando de parâmetros como "path", "logon master", e outros que definem acesso ou segurança.

Por padrão o SAMBA não utiliza autenticação encriptada na rede, mas sim "clear text". Versões mais atuais do Windows95/98/Me não utilizam o modo "clear text". Para resolver este problema seguem-se os passos a seguir:

Inserir os parâmetros "encrypt passwords = yes" e "smb passwd file = /etc/smb-passwd" na seção [global] do smb.conf e certificar-se de que todas as estações na rede utilizam autenticação encriptada no logon.

Para fazer o Windows trabalhar com senhas criptografadas, use o regedit e crie a seguinte chave:

Windows 95/98

HKEY_LOCAL_MACHINESystemCurrentControlSetServices
VxDVNETSUP

Adicione um novo valor DWORD:

Value Name: EnablePlainTextPassword e Data: 0x01.

Windows NT 4.0

HKEY_LOCAL_MACHINESystemCurrentControlSetServices
RdrParameters

Adicione um novo valor DWORD:

Value Name: EnablePlainTextPassword e Data: 0x01

Uma vez que as alterações no registro tenham sido feitas, reinicie a máquina Windows.

Para maiores detalhes, consultar os arquivos ENCRYPTION.txt, Win95.txt e WinNT.txt na documentação do Samba. Com isso, usando senhas criptografadas, não será possível visualizar compartilhamentos no servidor até que uma conexão inicial tenha sido feita com a autenticação apropriada. O SAMBA trás o arquivo .reg para cada versão do Windows com a chave modificada. Execute o arquivo correspondente para validar a mudança (eles estão em /usr/doc/samba-2.0.x/docs).

Não encontrando estes arquivos, abaixo estão as chaves que devem ser modificadas nas estações Windows para não utilizar o "clear text":

Windows 95/98

[HKEY_LOCAL_MACHINESystemCurrentControlSetServices
VxDVNETSUP]"

EnablePlainTextPassword"=dword:00000001

WindowsNT 4.0

[HKEY_LOCAL_MACHINESystemCurrentControlSetServices
RdrParameters]"

EnablePlainTextPassword"=dword:00000001

Windows 2000

[HKEY_LOCAL_MACHINESystemCurrentControlSetServices
LanmanWorkStatioParameters]"

EnablePlainTextPassword"=dword:00000001

Se a rede for "sniffada", os passwords que não estiverem encriptados serão des-

cobertos. Em alguns casos vale a pena tirar a criptografia de login e monitorar a rede com um anti-sniffer. Saliente-se entretanto que o Windows NT e o 2000 só conseguem se autenticar no servidor SAMBA através de senha encriptada. Mais ainda: o Windows 2000 vem com algumas dificuldades para entrar no Domínio de um PDC Samba.

Querendo que o SAMBA diferencie maiúsculas e minúsculas quando procurando por arquivos, adiciona-se "case sensitive = yes". Para utilizar como padrão letras maiúsculas ou minúsculas quando os arquivos são criados, adiciona-se "default case = lower (ou upper)". Para preservar maiúsculas e minúsculas para todos os nomes de arquivo, adiciona-se "preserve case = yes". Para preservar maiúsculas e minúsculas para nomes DOS (8.3), "short preserve case = yes".

Se o servidor possui mais de uma placa de rede, o smb.conf deve conter uma especificação para qual placa(s) será utilizada. Adicionando o seguinte parâmetro: "interfaces = xxx.xxx.x.x/24", onde o número depois da / é uma referencia à máscara de sub-rede. "24" é o valor a usar para uma rede Classe C não segmentada.

A.4 Créditos

Este roteiro para instalação e configuração é uma adaptação do Manual de Configuração do SAMBA escrito por Victor Zucarino/Atualização 7.0a - Agosto de 2002,

<http://geocities.yahoo.com.br/vffzbr/manual.html>, para os devidos créditos relatamos abaixo as principais fontes de pesquisas utilizadas na adaptação:

Site DicasLinux em:

<http://dicaslinux.linuxsecurity.com.br/>

Site Linuxunleashed.com em:

<http://www.linuxunleashed.com>

Site Linuxplace.com em: <http://www.linuxplace.com>

site Linux in Brazil em: www.linux.trix.net/sobre.htm

Dicas-L da Unicamp disponível em:

<http://www.dicas-l.unicamp.br>

LDP-BR - Projeto de Documentação do Linux no Brasil disponível em:
www.linorg.cirp.usp.br

Site Olinux disponível em: <http://www1.uol.com.br/olinux/>

Conectiva® Linux® em Redes Windows®, disponível em
www.zago.eti.br/samba/tutor10.tx

Site Oficial do SAMBA, disponível em: <http://www.samba.org>

Site Oficial da Conectiva, seção Suporte/perguntas e respostas, Último acesso em
18/03/2005, disponível em:
<http://www.conectiva.com.br>

Apêndice B

Apêndice B - Servidor *Proxy Squid*

Este Apêndice, contém um tutorial montado para subsidiar as equipes técnicas do MPF na instalação e configuração do Servidor *Proxy Squid*, bem como a implementação do SARG - utilitário gerador de relatórios no formato HTML, para monitoração de log de acesso dos usuários à web.

B.1 Introdução

A principal vantagem de se utilizar um servidor *Proxy Squid* é poder compartilhar uma conexão Internet entre os usuários da rede, além de possibilitar o *cache* de arquivos visitados e providenciar acesso local aos usuários, tornando assim o acesso mais rápido e descongestionando a banda. Além é claro de poder autenticar os usuários permitindo um acesso mais seguro.

O controle de acesso é feito por máquina (mais exatamente, por endereço IP). Entretanto, o Squid tem acesso a permissões por usuário, onde cada pessoa que tentar acessar a web é obrigada a fornecer login e senha (através do browser). A verificação pode ser feita de muitas maneiras: através de um arquivo *passwd* tradicional, ou no formato NCSA (geralmente associado ao utilitário *htpasswd*), ou ainda através de um servidor LDAP, um PDC de domínio Windows NT, ou módulos PAM.

B.2 Instalação do *Proxy Squid*

Descreve-se a seguir, procedimentos de instalação para distros baseadas no sistema de pacotes RPM¹.

B.2.1 Roteiro de Instalação do Servidor *Proxy Squid*

Inicialmente faz-se a verificação da existência do *squid* instalado no sistema GNU/Linux, através do comando:

```
$ rpm -qa |grep squid
```

A saída do comando acima poderá ser parecido com:

```
squid-(versão do pacote)  
linuxconf-squid-(versão do pacote)  
squid-doc-(versão do pacote)  
squid-auth-(versão do pacote)  
squid-templates-(versão do pacote)
```

Caso não se tenha obtido nenhuma saída com o comando acima, deve-se proceder a instalação, utilizando os pacotes que na maioria dos casos são encontrados no CD que acompanham às distros:

```
$ rpm -ivh /localdospacotes/squid*.*  
$ rpm -ivh /localdospacotes/linuxconf-squid-(versão do pacote).  
Outra alternativa de instalação, configuração e atualização, é a utilização do aplicativo apt-get.  
$ apt-get install squid* ou  
$ apt-get update squid*
```

Havendo necessidade de uma configuração específica, como, por exemplo, controle de banda, sugere-se instalar o squid via código-fonte, o qual pode ser obtido em (Verifique a versão mais recente):

<http://www.squidcache.org/Versions/v2/>.

Procedimento de instalação do fonte, após o download:

```
$ tar zxyf squid 2.5.STABLE1 src.tar.gz  
$ cd squid 2.5.STABLE1
```

¹RPM sigla utilizada para: RedHat Package Manager.

```
$ ./configure enable delay pools enable cache digests  
-enable poll disable ident lookups enable truncate  
-enable removal polices enable arp acl  
$ make all  
$ make install  
$ cd auth_modules/NCSA  
$ make  
$ make install
```

B.2.2 Configuração do Servidor Proxy Squid

A autenticação de usuários é um recurso bem interessante para controle pessoal de usuários. Isso permite que se crie ACLs individuais e gere Logs de qualidade bem superior. Existem diversos métodos de autenticação, sendo interessante averiguar exatamente o que se precise. Na maioria dos casos, o `ncsa_auth` resolve o problema. Ele está disponível junto com o `squid` e pode ser implementado rapidamente. É a solução ideal para pequenas e média instalações e redes com arquitetura de grupo de trabalho.

Antes de começar a edição do `/etc/squid/squid.conf` sugere-se que seja feita uma cópia do mesmo. Havendo necessidade de refazer a configuração desde o início por algum motivo de erro não será preciso reinstalar os pacotes.

Configuração do Proxy Squid utilizando o programa de autenticação de usuários, `ncsa_auth` que está no diretório `/usr/lib/squid`.

Copiando o arquivo para dentro do diretório `/usr/bin/` com o comando:

```
$ cp /usr/lib/squid/ncsa_auth /usr/bin/
```

Criando o arquivo de senha dos usuários *Proxy Squid*, com o comando:

```
$ htpasswd -c /etc/squid/squid_passwd usuário-1
```

Será pedida a senha e em seguida sua confirmação.

Para o cadastro dos demais usuários, utiliza-se o mesmo comando acima, retirando a opção `-c`". Em caso de redes grandes com muitos usuários sugere-se ao administrador que monte uma rotina simples num script, que crie os usuários e senhas.

Na PRM Franca optou-se por utilizar a estrutura de usuarios e senhas do samba para autenticação, para isso foi inserido algumas linhas ou ACLs no arquivo squid.conf:

Procura-se pela entrada:

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

# type:
# % make
# % make install
#
# Then, set this line to something like
#
# authenticate_program /usr/bin/ncsa_auth /usr/etc/passwd

authenticate_program /usr/bin/ncsa_auth /etc/squid/squid_passwd
<- para autenticação com NSA/AUTH insira a linha acima
authenticate_program /usr/lib/squid/smb_auth -W prm-franca -U 200.111.22.33
<- para autenticação com SAMBA insira a linha acima
```

As linhas acima indicam ao servidor squid qual programa irá autenticar os usuários, bem como o arquivo de senhas.

Agora se faz com que o *Proxy Squid* obrigue o navegador a pedir senha quando o usuário tentar se conectar na Internet. Utilizando-se da acl "acl password proxy_auth REQUIRED", conforme abaixo:

```
#Recommended minimum configuration:

acl all src 0.0.0.0/0.0.0.0
acl manager proto cache_object
acl localhost src 127.0.0.1/255.255.255.255
```

```
acl SSL_ports port 443 563
acl Safe_ports port 80 # http
acl Safe_ports port 21 # ftp
acl Safe_ports port 443 563 # https, news
acl Safe_ports port 70 # gopher
acl Safe_ports port 210 # wais
acl Safe_ports port 1025-65535 # unregistered ports
acl Safe_ports port 280 # http-mgmt
acl Safe_ports port 488 # gss-http
acl Safe_ports port 591 # filemaker
acl Safe_ports port 777 # multiling http
acl CONNECT method CONNECT
acl password proxy_auth REQUIRED <- insira esta linha.
```

Finalmente libera-se o acesso através de autenticação/senha. No squid.conf procura-se pela entrada abaixo:

```
# INSERT YOUR OWN RULE(S) HERE TO ALLOW ACCESS FROM YOUR
CLIENTS
#
# And finally deny all other access to this proxy
#http_access deny all <- comente esta linha.
http_access allow password <- insira esta linha.
```

Salvando o arquivo squid.conf, estão prontas as configurações para que o servidor *Proxy Squid* requisite senhas dos usuários.

Reinicia-se o serviço utilizando o comando:

```
$ service squid stop; service squid start
```

OBS: Se nenhum erro tiver sido cometido, quando o browser for carregado com alguma solicitação URL, será apresentada uma tela pedindo o login e a senha, somente os usuários cadastrados no servidor SAMBA² terão acesso.

Para melhorar a compreensão deste tutorial, coloca-se abaixo um exemplo completo de configuração do squid, via /etc/squid/squid.conf e demais arquivos que compõe a configuração. O exemplo que virá a seguir está em produção em um servidor controlado por este Autor, com modificações é claro, preservando aspectos inerentes à segurança e visando contemplar aspectos de configuração não implementados na PRM Franca. O script /etc/squid/squid.conf demonstra como

²Em função da PRM Franca ter utilizado a base de usuários do SAMBA e o arquivo de Senhas smbpasswd

controlar acesso a downloads, acesso de usuários a determinado site, separação por grupo, autenticação por senha.

A configuração do script, leva em consideração que já esteja configurado o acesso a Internet via ADSL ou qualquer tipo de banda larga, firewall instalado e configurado com direcionamentos .

No caso da PRM Franca foi utilizado uma estrutura de grupos específica, pois nem sempre as afinidades dos usuários do SAMBA coincidem com as do *Proxy Squid*.

Arquivos necessários:

- **useradm** - usuários administrativos (com acesso médio).
- **userctl** - usuários com acessos controlados.
- **userinf** - usuários com acessos livres (downloads, *sites*).
- **sites_proibidos** - arquivo com *sites* proibidos (pornografia, pedofilia, hackers, discriminação racial, *e-mail grátis (Hotmail, Yahoo)*).
- **palavras_proibidas** - arquivo com palavras proibidas, ou seja, todo tipo de palavras não convencionais).
- **palavras_permitidas** - arquivo com palavras permitidas como sexologia que não se refere à pornografia.
- **ip_permitidos_userctl** - este arquivo é para aqueles usuários restritos que podem acessar um endereço IP, por exemplo, um servidor com um aplicativo.
- **sites_permitidos_userctl** - este arquivo é para aqueles usuários restritos que podem acessar apenas os *sites* cadastrados.
- **download_proibidos** - este arquivo é para proibir downloads de arquivos como, por exemplo, *.EXE, *.ZIP, *.WAV entre outros evitando assim grandes problemas.
- **download_liberados** - este arquivo contém os arquivos liberados para downloads ou que serão liberados conforme solicitação do usuário. squid_passwd - arquivo com usuários e senhas. No caso da PRM Franca foi utilizado o `./smbpasswd`

Detalhamento do script /etc/squid/squid.conf:

```
http_port 3128 cgi-bin }?  
acl QUERY urlpath_regex cgi-bin }?  
no_cache deny QUERY
```

```
#Servidor usa 512Mb
```

```
cache_mem 256 MB
cache_swap_low 90
cache_swap_high 95
maximum_object_size 8192 KB
cache_dir ufs /var/cache/squid 300 16 256
cache_access_log /var/log/squid/access.log
cache_log /var/log/squid/cache.log
```

A linha abaixo, indica ao *squid* qual programa irá autenticar os usuários, bem como o arquivo de senhas:

```
authenticate_program /usr/lib/squid/smb_auth -W prn-franca -U 200.222.11.33
(autenticação via SAMBA)
```

Abaixo inicia-se o controle de acesso a usuários da rede, neste caso existem três grupos de usuários:

```
acl useradm proxy_auth "/etc/squid/useradm"
acl userctl proxy_auth "/etc/squid/userctl"
acl userinf proxy_auth "/etc/squid/userinf"
```

A seguir constrói-se um pequeno "firewall" pelo Squid:

```
acl sites_proibidos dstdomain "/etc/squid/sites_proibidos"
acl palavras_proibidas url_regex "/etc/squid/palavras_proibidas"
acl palavras_permitidas url_regex "/etc/squid/palavras_permitidas"
acl ip_permitidos_userctl url_regex "/etc/squid/ip_permitidos_userctl"
acl sites_permitidos_userctl dstdomain "/etc/squid/sites_permitidos_userctl"
acl download_proibidos url_regex -i "/etc/squid/download_proibido"
acl download_liberados url_regex -i "/etc/squid/download_liberados"
```

Observa-se que somente existe uma ACL para o grupo de usuários userctl que serão controlados ao extremo, também é bom verificar a existência de uma ACL com palavras_permitidas contendo aquilo que se queira liberar:

```
acl all src 0.0.0.0/0.0.0.0
acl manager proto cache_object
acl localhost src 127.0.0.1/255.255.255.255
acl SSL_ports port 443 563
acl Safe_ports port 80 # http
acl Safe_ports port 21 # ftp
acl Safe_ports port 443 563 # https, snews
acl Safe_ports port 70 # gopher
acl Safe_ports port 210 # wais
acl Safe_ports port 1025-65535 # unregistered ports
```

```
acl Safe_ports port 280 # http-mgmt
acl Safe_ports port 488 # gss-http
acl Safe_ports port 591 # filemaker
acl Safe_ports port 777 # multiling http
acl CONNECT method CONNECT
http_access allow manager localhost
http_access deny manager
http_access deny !Safe_ports
http_access deny CONNECT !SSL_ports
http_access allow userinf
```

Para usuários inscritos no arquivo userinf não há restrições allow libera tudo.

Os usuários do grupo userctl e useradm terão que executar os controles de acesso que seguem. O arquivo download_liberados serve para cadastrar os arquivos que podem ser baixados, isto é para usuários que necessitam e tem conhecimento para tal, mas para isso ele terá que solicitar qual arquivo deseja baixar, parece complicado, mas deve-se argumentar que este procedimento é para proteger a rede contra coisas indesejáveis como vírus, jogos, programas piratas e etc.:

```
http_access allow download_liberados
http_access deny download_proibidos
http_access allow useradm palavras_permitidas
http_access deny useradm sites_proibidos
http_access deny useradm palavras_proibidas
http_access allow useradm
http_access deny userctl sites_proibidos
http_access allow userctl sites_permitidos_userctl
http_access allow userctl ip_permitidos_userctl
http_access deny userctl palavras_proibidas
http_access deny all
```

No final das ACL sempre se deixa negando tudo, caso algum usuário passe pelas regras não passará pela última

```
icp_access allow all
proxy_auth_realm Servidor Proxy Squid PRM Franca #Nome que irá aparecer
na tela inicial de acesso
```

Sintaxe dos arquivos utilizados na configuração:

***/etc/squid/useradm* - contém os usuários do grupo useradm:**

marcos
joao

***/etc/squid/userctl* - contém os usuários do grupo userctl:**

karen
julia
vieira
jose
mauro

***/etc/squid/userinf* - contém os usuários do grupo userinf:**

ziro
carlos

***/etc/squid/sites_proibidos* - contém relação de *sites* proibidos:**

sexo.com.br
sexy.com.br
playboy.com.br
gostasas.com.br

***/etc/squid/palavras_proibidas* - contém relação de palavras proibidas:**

sexy
porno
playboy
eleela
SEX
gulosa
therun

***/etc/squid/palavras_permitidas* - contém relação de palavras permitidas:**

sexualidade
index.jsp

***/etc/squid/ip_permitidos_userctl* - contém os IPs. de onde o grupo userctl pode acessar a web:**

200.142.xx.xx

200.142.yy.yy 200.142.zz.zz

/etc/squid/sites_permitidos_userctl - Contém a relação dos *sites* permitidos ao grupo **userctl**:

www.prsp.mpf.gov.br

www.senado.gov.br intranet.prsp.mpf.gov.br

/etc/squid/download_proibidos - contém as restrições para download:

.*.mp3\$

.*.exe\$

.*.zip\$

.*.avi\$

.*.viv\$

.*.bmp\$

.*.mpeg\$

.*.jpeg\$

*Obs.: a sintaxe *.extensão\$ deste arquivo é muito importante para proibir o download somente no momento que o usuário clicar em download no site desejado.*

/etc/squid/download_liberados - Contém a lista de permissões para download:

atualiza.zip

receita.exe

darf.exe

OBS: Para usuários controlados normalmente os arquivos a que eles podem acessar, são arquivos relacionados ao trabalho e geralmente seus nomes são padronizados, facilitando a tarefa do administrador.

Caso não se queira utilizar a autenticação via SAMBA, exemplificamos a seguir a configuração através do NCSA_AUTH /etc/squid/squid_passwd

ziro:4TE0oMnbeo7Ec

carlos:uSoIbEzcKaHns

marcos:oa6lJb8zxL2e.

joao:M3BEUspc3.8LE

karen:eIrk3HWCnpQQ

julia:MsjIWfo38eLM

vieira:K9wqnCR5nm0Uc

jose:0Vcufrx.7UY

mauro:PwEb4tSjaFBGc

OBS: Os caracteres à frente do nome do usuário referem-se à senha criada pelo arquivo htpasswd

que é o responsável também pela criação do arquivo password com a sintaxe:

\$ htpasswd -c /etc/squid/squid_passwd usuário-1 (para criação)

#\$ htpasswd /etc/squid/squid_passwd usuário-1 (para adição).

B.2.3 Configuração das estações Windows para utilizarem o Proxy

Para configurar a estação de trabalho, cujo sistema operacional é win9x/2000/XP, deve-se proceder a configuração do browser. No caso do Internet Explorer, essa configuração está disponível na aba: Ferramentas/Opções da Internet/Conexões/Configurações da Lan e para o browser Mozilla na aba: Editar/preferências/Avançado/Proxy. Para melhorar o entendimento na figura B.1, ilustra-se como a configuração pode ser realizada.

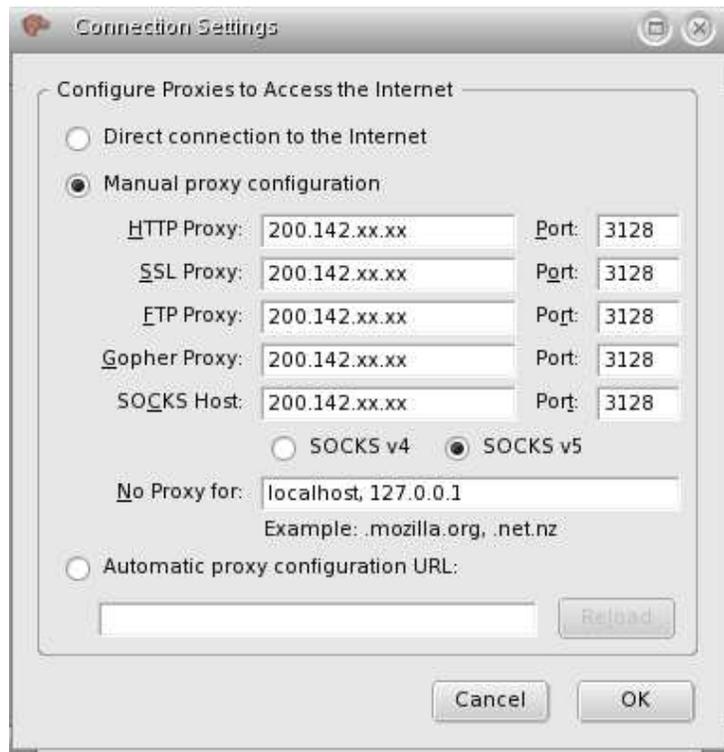


Figura B.1: Aba de configuração do Proxy no browser Mozilla Firefox

B.3 Gerador de Relatórios Html - SARG

O Sarg é uma ferramenta escrita principalmente para ser utilizada pelo Administrador de Redes. Através dela, pode-se controlar o que cada usuário acessa, o tempo gasto e a quantidade de bytes trafegados.

Como não existe nenhum servidor 100% seguro, sempre é bom estar verificando o que os nossos usuários estão fazendo na web. Para isso demonstra-se a seguir, como instalar, configurar e como gerar relatórios a partir do SARG(Squid Analysis Report Generator).

OBS: Assume-se que o serviço de *Proxy Squid* e web (apache) estão funcionando corretamente.

1° Passo - Acessando o sistema como root em um terminal:

Verificando se o pacote do sarg esta instalado:

```
$ rpm -qa |grep sarg
```

Caso não seja mostrado nenhum pacote instale o SARG através do aplicativo apt-get:

```
$apt-get install sarg
```

OBS: Assume-se que o leitor domine a ferramenta apt-get e esta esteja instalada adequadamente para trabalhar com os cds ou com os repositórios disponibilizados na Internet.

utilizando o comando RPM:

```
$ rpm -ivh /local/dos/pacotes/sarg*.*
```

2° Passo - Faça uma cópia de segurança do arquivo de configuração.

```
$cp /etc/sarg/sarg.conf /etc/sarg/sarg.conf
```

3° Passo - Edite o arquivo /etc/sarg/sarg.conf

```
$vi /etc/sarg/sarg.conf
```

4° Passo - Confira o arquivo /etc/sarg/sarg.conf, seguindo o exemplo abaixo:

Opção para cria o index.html principal

index yes

Opção que indica sobrescrever o relatório caso ele já exista

overwrite_report yes

Opção para registros sem nome de usuário opções:(ignore/ip/everybody)

records_without_userid ignore

Opção que indica a quantidade de *sites* mais acessados que será mostrada na página do relatório

topsites_num 100

Opção que indica critério de classificação no item *topsites* opções:CONNECT/BYTES A/D - Neste exemplo esta sendo utilizado o critério conexão em forma decrescente.

topsites_sort_order CONNECT D

Esta opção indica que os códigos HTTP deverão ser ignorados no relatório

exclude_codes /etc/sarg/exclude_codes

Tempo para checagem

max_elapsed 28800000

Opções que poderão ser escolhidas para gerar o relatório

topsites — Indica o site, conexão e bytes

sites_users — Indica quais usuários estavam acessando um determinado site

users_sites — Indica os sites acessados por cada usuário

date_time — Indica quantidade de bytes usados por dia e hora

denied — Indica os sites negados que foram negados com a URL completa

auth_failures — Indica problemas de autenticação

No arquivo *sarg.conf* as opções de geração de relatório são setadas com o Comando:

report_type *topsites sites_users users_sites date_time denied auth_failures*

Opção para exibir endereços completos.

long_url no

5º Passo - Criar um link /srv/www/default/html apontando para /var/www/html/squid:

```
$ cd /srv/www/default/html
$ ln -s /var/www/html/squid squid
```

6º Passo - Inserindo as entradas "Negado" e "Topsites" no final do arquivo /etc/sarg/languages/Portuguese, possibilitando gerar os relatórios de falhas de autenticação e de sites mais acessados:

```
$ vi /etc/sarg/languages/Portuguese
```

Faz-se a inserção das linhas abaixo no fim do arquivo:

```
"Negado"
"Topsites"
```

7º Passo - Automatizando a geração do Relatório diariamente via cron do usuário root:

```
$ crontab -e
Digita-se a linha abaixo, como exemplo, que será incluída no arquivo /etc/crontab
59 23 * * * /usr/sbin/sarg -f /etc/sarg/sarg.conf
```

8º Passo - Caso se queira gerar o relatório somente do dia corrente, cria-se o arquivo abaixo dentro do diretório /etc/sarg, utilizando o seguinte procedimento:

```
$ vi /etc/sarg/sargdia.sh
```

Digita-se as entradas abaixo:

```
#!/bin/bash
HOJE=$(date +%d/%m/%Y)
/usr/sbin/sarg -f /etc/sarg/sarg.conf -d $HOJE-$HOJE
exit 0
```

Dando permissão de execução ao script, digitando na linha de comando:

```
$ chmod a+x /etc/sarg/sargdia.sh
```

Inserindo a linha que chamará o script no crontab do usuário root:

```
$ crontab -e  
59 23 * * * /etc/sarg/sargdia.sh
```

Visualização do Relatórios Gerados pelo Sarg: O SARG gera os relatórios no formato HTML visualizados com qualquer browser disponível. O Relatório index.html, demonstrado na Figura B.2, contém um link para todos os relatórios gerados.

ARQUIVO/PERÍODO	DATA CRIAÇÃO	USUÁRIOS	BYTES	MÉDIA
18Mar2005-21Mar2005	Seg Mar 21 11:51:02 BRT 2005	11	99.511.138	9.046.467
07Jan2005-10Jan2005	Seg Jan 10 11:30:33 BRST 2005	6	22.011.958	3.668.659
07Jan2005-24Jan2005	Seg Jan 24 10:13:40 BRST 2005	9	664.406.538	61.600.726
07Jan2005-25Jan2005	Ter Jan 25 18:29:00 BRST 2005	9	717.578.915	79.720.990
25Jan2005-26Jan2005	Qua Jan 26 14:05:13 BRST 2005	8	44.734.817	5.591.852
25Jan2005-03Feb2005	Qui Feb 3 10:11:33 BRST 2005	10	653.435.868	55.343.586
03Feb2005-04Feb2005	Sex Feb 4 15:00:23 BRST 2005	10	70.998.031	7.099.803
04Feb2005-10Feb2005	Qui Feb 10 11:35:55 BRST 2005	9	92.197.822	10.244.202
10Feb2005-21Feb2005	Seg Feb 21 10:01:22 BRT 2005	10	424.747.617	42.474.761
21Feb2005-22Feb2005	Ter Feb 22 09:37:17 BRT 2005	10	60.905.404	5.090.540
22Feb2005-23Feb2005	Qua Feb 23 14:27:36 BRT 2005	10	146.154.674	14.615.467
23Feb2005-23Feb2005	Seg Feb 28 13:11:47 BRT 2005	10	185.551.408	18.555.140
28Feb2005-28Feb2005	Seg Feb 28 14:17:18 BRT 2005	9	8.181.364	909.040
28Feb2005-07Mar2005	Seg Mar 7 09:44:19 BRT 2005	11	244.496.896	22.226.990
07Mar2005-07Mar2005	Seg Mar 7 16:44:47 BRT 2005	11	60.347.980	4.577.089
07Mar2005-11Mar2005	Sex Mar 11 11:36:12 BRT 2005	11	275.532.284	25.048.389
11Mar2005-15Mar2005	Ter Mar 15 12:00:33 BRT 2005	10	184.862.034	18.486.203
15Mar2005-18Mar2005	Sex Mar 18 11:39:33 BRT 2005	11	173.932.350	15.812.031

Gerado por sarg-1.2.1.03Dez2001 em 21/Mar2005-11:51

Figura B.2: Página Principal - Index do SARG

O relatório demonstrado na Figura B.3, contém um resumo dos acessos realizados, com várias informações muito úteis para o administrador da rede.

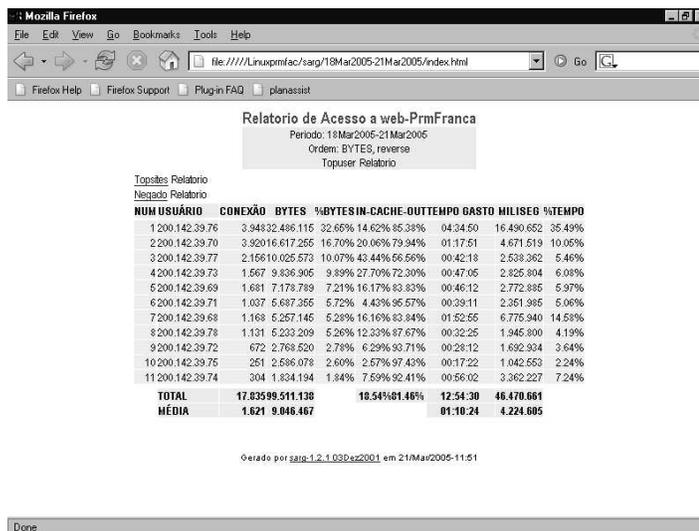


Figura B.3: Visualização do Relatório do Acesso a web, gerado pelo SARG

Outro relatório, visto na Figura B.4, também é de muita utilidade para o administrador, detectando usuários com tentativas de acesso não autorizado.

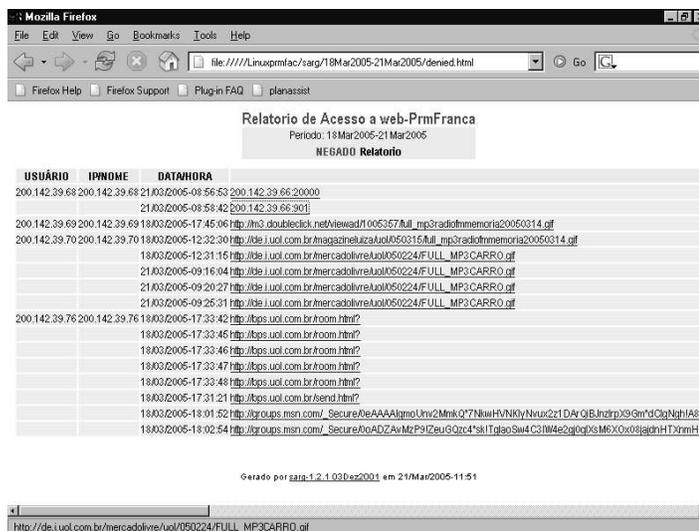


Figura B.4: Relatório dos acessos Negados

Por ultimo, a Figura B.5 mostra a visualização dos *sites* mais acessados. Com a análise desse relatório pode-se ter uma síntese dos conteúdos acessados e se for o caso, com base nas informações analisadas, readequar a configuração do servidor *SQUID*.

	LOCAL ACESSADO	CONEXÃO	BYTES
1	intranet.prsp.mpf.gov.br	1.219	2.861.011
2	img.terra.com.br	639	698.281
3	tp.uol.com.br	494	577.640
4	home.img.uol.com.br	487	627.271
5	www.atlantis.com	468	4.163.668
6	www.caixa.gov.br	398	963.989
7	producao.prsp.mpf.gov.br	374	420.513
8	www.msn.com.br	369	2.659.808
9	de.uol.com.br	361	848.597
10	www.bolcario.com.br	364	1.145.796
11	www1.caixa.gov.br	340	1.067.340
12	www.pgr.mpf.gov.br	310	1.112.254
13	www2.uol.com.br	303	175.241
14	www.temposgora.com.br	302	213.366
15	www.famerqo.com.br	292	2.271.768
16	www.virtuasexy.com	289	2.938.282
17	www.ivox.com.br	275	2.785.548
18	www2.zelo.com.br	274	1.807.188

Figura B.5: Relatório das páginas mais acessadas -topsites

B.4 Créditos

Na elaboração deste tutorial foram consultadas diversas fontes com leitura de artigos, apostilas, livros e outras publicações que ora são citados para os devidos créditos:

Documentação para *Proxy Livre* - Último acesso em 18/03/05, disponível em <http://www.Softwarelivre.gov.br>

Uso e configuração do Squid - acessado em 25/03/05, disponível em <http://www.linuxit.com.br>

Conectiva servidores/squid - Seção perguntas e respostas - Último acesso em 19/03/05,
em:

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

Atualização do Squid - acessado em 26/03/05, Disponível em:

<http://www.squid-cache.org/>

Artigo Autenticação no Squid - Último acesso em 18/03/2005, disponível em

<http://brlinux.linuxsecurity.com.br>

Configurando um Squid "Ninja- acessado em 27/03/05, disponível em

<http://www.linuxman.pro.br/squid/>