UniCEUB – Centro Universitário de Brasília
FATECS – Faculdade de Tecnologia e Ciências Sociais Aplicadas
Curso de Engenharia da Computação
Projeto Final

CENTRALIZAÇÃO DOS SERVIÇOS DE INTRANET EM UMA REDE COM SISTEMAS OPERACIONAIS HETEROGÊNEOS

Aluna: Dayanna de Menezes Martins – RA: 2041632-8
Orientador: Prof. M. Sc. Antonio José Gonçalves Pinto

Brasília, DF - junho de 2009

DAYANNA DE MENEZES MARTINS

CENTRALIZAÇÃO DOS SERVIÇOS DE INTRANET EM UMA REDE COM SISTEMAS OPERACIONAIS HETEROGÊNEOS

Monografia apresentada ao Curso de Engenharia da Computação, como requisito parcial para obtenção do grau de Engenheira de Computação.

Orientador: Prof. Antonio José Gonçalves Pinto

BRASÍLIA/DF

1º SEMESTRE DE 2009

AGRADECIMENTOS

Primeiramente agradeço a Deus que permitiu e me deu força para passar por mais essa etapa em minha vida.

Ao meu pai José Gerado Martins, a minha mãe Dinair Menezes Alves Martins, a minha irmã Dyanna de Menezes Martins pelo apoio constante e por entender os momentos em que estive ausente durante todo esse tempo. Amo vocês.

Aos meus amigos Marcelo Moraes, George Rosa, Leonardo Taffner, Adriana Carretta e Paula Contijo. Pelo incentivo, pela amizade e por me proporcionarem alguns momentos de descontração.

Aos colegas de trabalho que em vários momentos de estresse me acalmaram.

Agradecimento especial ao meu namorado Thiago de Almeida Milhomem, pelo apoio, carinho, amor, dedicação, compreensão e tolerância. Pelos finais de semana em que ficamos em casa ao invés de sairmos. Com certeza essa vitória também é sua. Que Deus te ilumine e ajude a realizar todos os teus sonhos. Eu te amo.

Por fim, agradeço a todos que compreenderam a minha ausência durante a elaboração do projeto.

RESUMO

Este projeto apresenta uma proposta de centralização dos serviços de uma intranet em um servidor onde haverá um controlador de domínio, de acessos a Internet, de arquivos, de impressão, de inventários das máquinas e de políticas de acesso a diretórios e compartilhamentos. Para a criação do servidor serão utilizados softwares livres, o que fará com que a empresa não se preocupe com os custos relacionados a licenças de softwares. Essa rede interna irá se comunicar com máquinas que possuam sistemas operacionais GNU/Linux e Microsoft Windows.

Palavras-chave: linux, windows, intranet.

ABSTRACT

This project presents a proposal of centralization of the intranet's services in a server which will have a controller of domain, Internet access, files, print, machine's inventories and access policies to directories and sharing. For the creation of this server will be used free softwares, which will turn possible that the company do not worry with the costs from software's licenses. This intranet will communicate with machines which have GNU/Linux and Microsoft Windows operational systems.

Key-Words: linux, windows, intranet.

SUMÁRIO

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE SIGLAS E ABREVIATURAS

ACL – *Access Control List*

AD – *Active Directory*

BDC – *Backup Domain Controller*

CIFS – *Common Internet File System*

CUPS – *Common Unix Printing System*

DC – *Domain Controller*

DHCP – *Dynamic Host Configuration Protocol*

DNS – *Domain Name System*

GNU – *General Public License*

GPO – *Group Policy Object*

HP – *Hewlett Packard*

IP – *Internet Protocol*

ISA – *Internet Security and Acceleration*

LAN – *Local Area Network*

LDAP – *Lightweight Directory Access Protocol*

MAC – *Media Access Control*

NFS – *Network File System*

PDC – *Primary Domain Controller*

RAM – *Random Access Memory*

SARG - *Squid Analysis Report Generator*

SMB – *Server Message Block*

TI - *Tecnologia da Informação*

VPN – *Virtual Private Network*

WINS – *Windows Internet Name Services*

1. INTRODUÇÃO

1.1. Motivação

O sistema operacional que predominava nas estações de trabalho em grande parte das empresas eram os sistemas da família Microsoft. Para administrar essa rede, nada melhor do que o próprio software da Microsoft para controlar servidores. Esse software da família Microsoft responsável por controlar a rede interna das empresas, permite apenas administrar máquina com o sistema operacional também da Microsoft e, além disso, possui o custo de licenciamento. Atualmente, é possível encontrar várias empresas utilizando os sistemas operacionais GNU/Linux, principalmente em seus servidores.

Motivado pela situação apresentada, este projeto visa criar um servidor para controlar a rede interna de uma empresa todo em software livre. Onde esse permitirá o controle de um ambiente computacional com estação clientes que utilizam sistemas operacionais GNU/Linux e Microsoft Windows.

1.2. Objetivo

O objetivo deste projeto é apresentar um sistema alternativo ao Windows 2003 Server, software responsável por administrar a rede interna das empresas que utilizam o sistema operacional Microsoft Windows em suas estações de trabalho. O sistema proposto visa atender empresas pequenas, que estão entrando no mercado e que desejam utilizar uma rede com sistemas operacionais heterogêneos, ou seja, estações de trabalho que utilizem GNU/Linux e Microsoft Windows.

O servidor deste projeto possui os principais serviços de intranet como, controle de acesso a diretórios e impressoras compartilhadas no servidor, controlador de domínio, Proxy para controlar o acesso a Internet e, além disso, o

servidor controlará o inventário do hardware e do software de todas as máquinas da rede.

Por fim, serão apresentados dados que mostram as limitações ou melhorias do sistema implementado comparando-se com o Windows 2003 Server, para que assim as empresas que estão entrando no mercado possam saber se esse sistema criado pode atender as suas necessidades.

1.3. Organização da Monografia

Capítulo 1 - Introdução: Nesse capítulo são apresentadas as idéias que levaram a escolha do tema do projeto, os objetivos e a estrutura da monografia.

Capítulo 2 – Apresentação do Problema: Aqui é descrito o cenário existente e os problemas encontrados. Por fim é apresentada a proposta de solução.

Capítulo 3 – Serviços de Intranet: Esse capítulo possui todo o embasamento teórico para o melhor entendimento do projeto.

Capítulo 4 – Implementação do Projeto: Contém todos os procedimentos realizados para a implementação do sistema proposto. Também estão descritas todas as ferramentas utilizadas.

Capítulo 5 – Resultados Obtidos: Neste capítulo são descritos todos os testes realizados para a elaboração do projeto, as dificuldades encontradas na realização e por fim a funcionalidades obtidas.

Capítulo 6 – Conclusão: É apresentada a conclusão do projeto obtido. Também são sugeridas algumas propostas para a continuidade do projeto.

2. APRESENTAÇÃO DO PROBLEMA

Este projeto surgiu da necessidade de criar um sistema alternativo ao Windows 2003 Server para empresas pequenas. Essa idéia veio devido ao grande problema encontrado pelas pequenas empresas que estão começando a entrar no mercado. No momento de escolher um software para gerenciar a rede interna da organização, essas pequenas empresas não tem muita opção e acabam optando pelo sistema da Microsoft. Nos itens abaixo são mostrados os principais problemas encontrados por essas empresas e a proposta de solução deste trabalho de pesquisa.

2.1. Descrição do cenário existente

A maneira como as empresas trabalham tem mudado bastante com o crescimento das tecnologias da informação[1] (TI). As grandes empresas existentes hoje no mercado utilizam diversos recursos de tecnologia para facilitar e agilizar o seu trabalho.

As intranets baseiam-se nas mesmas tecnologias da Internet. Em essência, as intranets são pequenas versões da Internet, mas de caráter privado. A menos que você decida permitir o acesso público da Internet, somente as pessoas da empresa terão acesso aos computadores conectados com sua intranet

A tecnologia da informação dispõe de diversos recursos para a criação de uma intranet que atenda a qualquer tipo de empresa. A organização deve dispor de serviços que realizem o controle de armazenamento de arquivos, gerenciamento de acesso dos usuários aos compartilhamentos internos, as impressoras e a recursos externos da rede, como a internet. Esses serviços são essenciais para o controle de uma rede interna.

---

[1] Disponível em: <http://www.infowester.com/col150804.php>. Acesso em 05 de maio de 2009.

A intranet não foi criada apenas para grandes corporações, por mais que as empresas sejam pequenas e possuam poucos funcionários, é essencial criar uma rede interna onde possa ter maior controle dos acessos dos funcionários. Quando uma pequena empresa já começa utilizando grande parte dos recursos de TI existentes no mercado para facilitar e agilizar o seu trabalho, mais oportunidades ela tem para crescer.

Outro fator essencial no momento da criação de uma intranet para a empresa é a escolha do sistema operacional a ser utilizado. Os sistemas operacionais Microsoft são bastante procurados no mercado atual, mas os sistemas GNU/Linux[2] vêm ocupando seu espaço. Isso se deve ao fato do GNU/Linux ser um sistema livre de licenças de software, possibilitando ao administrador da rede configurar os servidores e estações de trabalho da maneira que ficar melhor para a organização. [Mandriva Conectiva, 2004]

Em 12 de fevereiro de 2008 a revista Linux Magazine publicou uma pesquisa feita pelo Instituto Sem Fronteiras do ano de 2007 até 2008 sobre a utilização de softwares livres em empresas. Nesses 12 meses de pesquisas 46% relataram ter aumentado seu uso e 51% informaram que mantiveram seu patamar, enquanto apenas 3% disseram estar usando menos Software Livre, conforme figura 1.

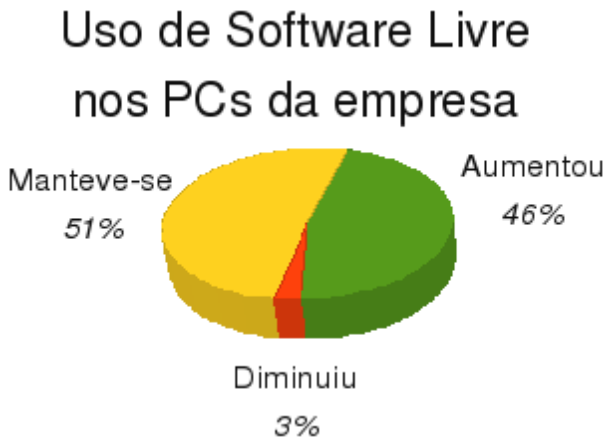


Figura 1: Uso de Software Livre em Empresas

Fonte: www.ldap.org.br

2 Disponível em: <http://www.debian.org/releases/stable/s390/ch01s02.html.pt>. Acesso em 05 de maio de 2009.

Mesmo sabendo que os sistemas operacionais livres estão crescendo muito, os sistemas operacionais Microsoft possui uma grande força no mercado, por isso a preocupação em sempre criar uma rede que consiga trabalhar com todos os tipos de sistemas operacionais.

Trabalhar com todos os sistemas da família Microsoft pode ser mais fácil, mas isso envolve um grande gasto com licenças de software, por tratarmos de um sistema proprietário. Por isso a idéia de utilizarmos sistemas livres, mas que seja compatível com os sistemas Microsoft que são bastante utilizados.

Quando se trata de administração desses sistemas, os softwares Microsoft são mais amigáveis, já que toda a configuração pode ser feita através de interfaces gráficas. Já nos sistemas GNU/Linux nem todas as configurações podem ser feitas de forma gráfica, grande parte das configurações são feitas via comando, principalmente em servidores.

A utilização de servidores com softwares livres vem crescendo no mercado atual. Um exemplo disso é que no dia 06 de janeiro de 2009 o Ministério Vietnamita de Informações e Telecomunicações emitiu uma resolução administrativa para o aumento do uso de produtos de software livre nos órgãos estatais. De acordo com essa nova norma 100% dos servidores do governo executarão Linux antes de 30 de julho de 2009. [VIETNAM NET, 2009]

Ainda assim, a rede interna da maioria das empresas é gerenciada através de servidores que utilizam o Windows 2003 Server por ser um software bastante conhecido e confiável. De acordo com uma pesquisa realizada pelo IDG NOW em 04 de junho de 2007, 65% dos servidores empresariais utilizam Windows Server, 31% Unix e família, sendo 17% Linux e 4% entre outros sistemas. [IDG NOW, 2007]

2.2. Problemas encontrados

O maior problema encontrado pelas empresas está relacionado à falta de opção de softwares que possam controlar a intranet das empresas. O software mais

utilizado hoje no mercado é o Windows Server, conforme pesquisa apresentada pelo IDG NOW no item 2.1. Esse software necessita de licença de software, motivo pelo qual nem todas as empresas podem ter acesso.

O Windows 2003 Server também não possui um software nativo que realize controle de inventário do hardware e dos softwares das máquinas utilizados na rede interna da empresa, evitando assim que possa ter um maior controle dos equipamentos. [VASCONCELOS, 2006]

Outro problema encontrado é com relação ao controle de uma rede com sistemas operacionais distintos dentro das organizações. O Windows 2003 Server não consegue controlar as máquinas que não possuem o sistema operacional Windows. Para que o Windows 2003 Server controle máquinas com diferentes sistemas operacionais é necessário a instalação do software livre Samba, que será utilizado na criação do sistema proposto.

2.3. Proposta de solução

A proposta para solução dos problemas apresentados seria a criação de um sistema alternativo ao Windows 2003 Server feito todo em GNU/Linux. Esse sistema proposto fará o controle da rede interna de uma empresa sem custos com licenças de softwares.

O produto final desse projeto fará com que máquinas Linux e Windows possam se comunicar de forma que sejam integrados os principais serviços de intranet, como controle de domínio, servidor de arquivos e impressão. Além disso, haverá um controle de inventários de todas as máquinas que estão na rede interna da empresa. Outro recurso que estará disponível no servidor proposto será o servidor de Proxy, que fará o controle de acesso a Internet dos usuários da rede interna, além de gerar registro de tudo o que foi acessado.

Por fim, será criado um cenário de comparação mostrando as diferenças entre o Windows 2003 Server e o sistema criado, realizando um comparativo das

limitações da implementação do projeto em relação ao Windows 2003 Server, bem como as limitações do Windows 2003 Server em relação à implementação do projeto.

3. SERVIÇOS DE INTRANET

Nesse capítulo serão apresentadas e descritas todas as características das principais tecnologias utilizadas para a elaboração do produto final desse projeto, como por exemplo, virtualização, sistema operacional, servidor de arquivo e impressão, controle de acesso a internet, inventário das máquinas. A visão geral de todas essas tecnologias auxiliará em um melhor entendimento da solução proposta.

3.1. Sistema de Virtualização

> Em uma definição livre, virtualização é o processo de executar vários sistemas operacionais em um único equipamento. Uma máquina virtual é um ambiente operacional completo que se comporta como se fosse um computador independente. Com a virtualização, um servidor pode manter vários sistemas operacionais em uso. [HP, 2009]

Na figura 2, podem ser visualizadas algumas diferenças entre a computação estática e virtualizada.

Figura 2: Computação Estática X Virtual

Fonte: www.microsoft.com

Empresas do mundo inteiro têm adotado sistemas de virtualização em seus servidores e estações de trabalho, para que possam aprimorar a capacidade de reação frente a condições que sofrem bastantes alterações. [Microsoft, 2009]

De acordo com a Microsoft, a máquina virtual é uma das tecnologias responsáveis por mudanças no custo da infra-estrutura de TI. [Microsoft, 2009]

Durante o processo de elaboração do projeto o servidor e as estações clientes foram criados através de um sistema de virtualização. O software utilizado para criação desses sistemas virtualizados foi o VMware Sever. Esse software foi utilizado apenas para permitir a criação do sistema.

3.2. Sistema Operacional

O sistema operacional é um programa que gerencia o hardware do computador. A sua principal função é controlar e coordenar o uso do hardware entre os diversos programas aplicativos para os diversos usuários, oferecendo assim,

meios para o uso adequado desses recursos na operação do computador. [SILBERSCHATZ, GALVIN, GAGNE, 2004]

A figura 3 apresenta uma visão abstrata dos componentes de um computador, onde é composto basicamente do hardware, sistema operacional e aplicativos.

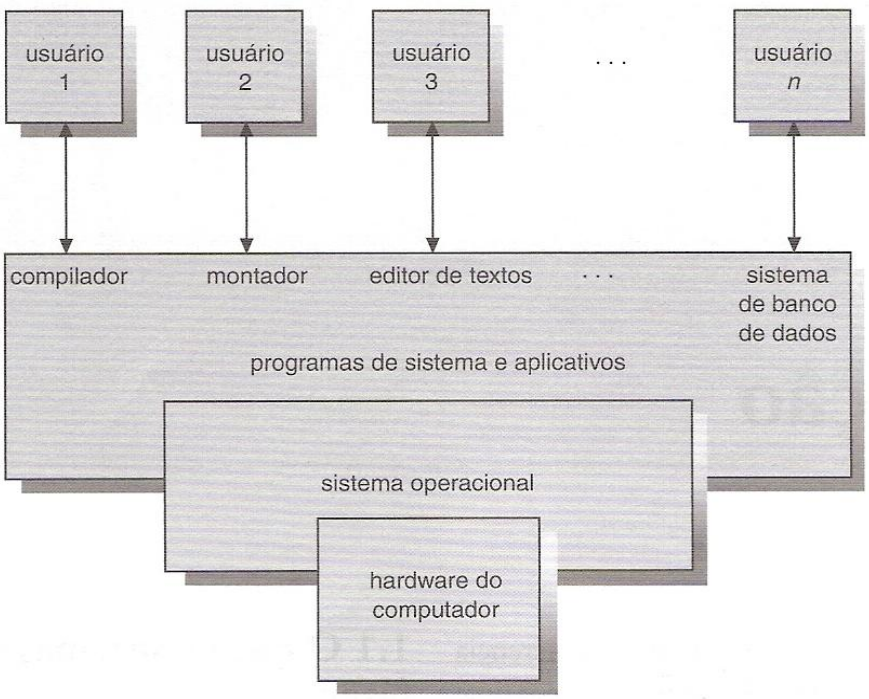


Figura 3: Visão abstrata dos componentes de um computador

Fonte: SILBERSCHATZ, GALVIN, GAGNE, 2004.

Os três sistemas operacionais mais conhecidos hoje são Microsoft Windows, Apple Macintosh e o Linux. [SILBERSCHATZ, GALVIN, GAGNE, 2004]

Para criação do servidor desse projeto, será utilizada a distribuição[3] Linux Mandriva, por ser estável e de fácil configuração.

[3] Disponível em: <http://www.conectiva.com/doc/livros/online/10.0/usuario/pt_BR/ch01s03.html>. Acesso em 18 de março de 2009.

3.2.1. Mandriva

O Mandriva é uma distribuição GNU/Linux criada em 2005 quando a antiga Mandrake Linux adquiriu o Conectiva.

Em 1998 os sistemas operacionais Linux eram conhecidos por exigir um grande conhecimento técnico dos usuários devido à grande utilização de linhas de comando.

Com o objetivo de tornar o Linux um sistema operacional que fosse mais fácil de utilizar a Mandrak Linux decidiu integrar os melhores ambientes de desktop e contribuir com a configuração dos utilitários através do modo gráfico. Após essa junção o Mandriva rapidamente se tornou famoso pela facilidade, funcionalidade e estabilidade. Todas essas características permitem com que esse sistema operacional possa ser utilizado tanto em servidores como em estações de trabalho. [distrowatch.com]

3.3. Lightweight Directory Access Protocol (LDAP)

LDAP é um protocolo leve para acessar serviços de diretórios, baseado no modelo cliente-servidor. Esse serviço é um banco de dados otimizado para ler, procurar e navegar, mas normalmente não suportam grandes volumes de dados, como nos bancos tradicionais. Os diretórios costumam ter um filtro sofisticado para busca de dados, pois são feitos para respostas rápidas devido ao grande número de operações de buscas.

No LDAP as informações são organizadas de forma hierárquica, como uma estrutura de árvore, diferente dos bancos de dados tradicionais. Esse protocolo possui um alto nível de segurança. A maioria dos administradores de rede tem escolhido utilizar esse protocolo e cada vez mais existe aplicações com suporte ao LDAP, como podemos destacar na figura 4. [LDAP, 2009]

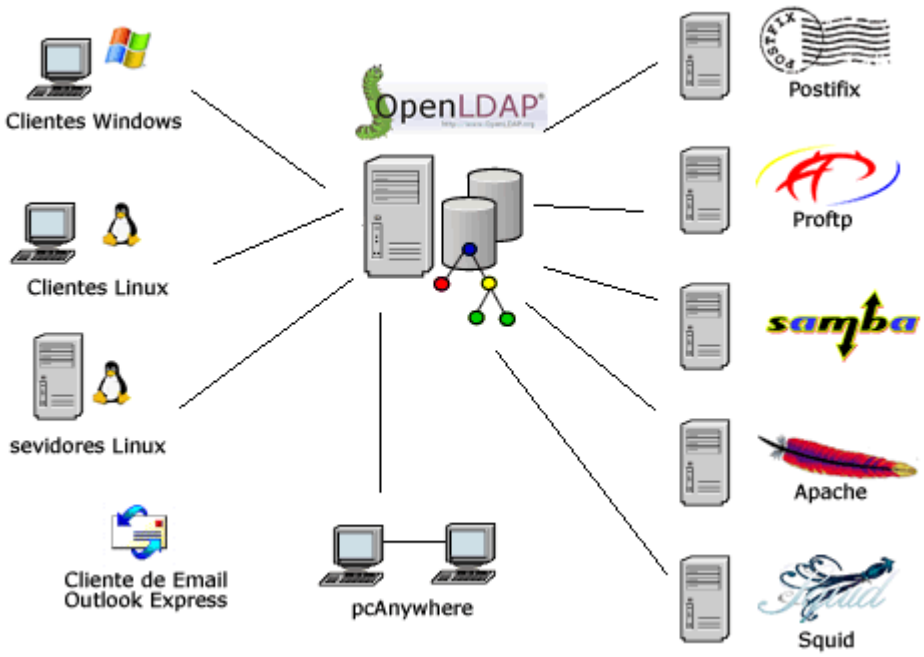


Figura 4: Utilização do LDAP

Fonte: www.ldap.org.br

Uma característica importante desse protocolo é que são centralizadas todas as informações evitando assim dados duplicados e trazendo grandes benefícios. Já a grande desvantagem é que raramente são efetuadas atualizações.

3.4. Servidor de arquivo e impressão

A função de um servidor de arquivos é oferecer a seus clientes alguns serviços como: armazenamento, acesso de informações e compartilhamento de discos. Esses servidores controlam também unidades de disco ou outras unidades de armazenamento e são capazes de aceitar pedidos de transações das máquinas clientes.

O servidor de arquivos pode ser dividido em três subsistemas funcionais:

- Subsistema de gerência de arquivos;
- Subsistema de cachê de disco;

- Subsistema de controle de acesso compartilhado e segurança.

O subsistema de gerência de arquivos faz o controle de todo acesso físico aos meios de armazenamento. Para que obtenha uma melhor eficiência e segurança, alguns servidores implementam o seu próprio subsistema de gerência de arquivos, enquanto outros utilizam os serviços do sistema operacional local. O subsistema de cachê de disco na tentativa de diminuir o número de acessos físicos às unidades de armazenamento e aumentar a eficiência do servidor, realizam o acesso ao disco em grandes blocos de dados, mantendo-os em memória RAM. O subsistema de acesso compartilhado e segurança realizam um controle de acesso simultâneo aos arquivos, permitindo que eles sejam compartilhados e utilizados da forma correta. [SOARES, LEMOS, COLCHER, 1995]

Já o servidor de impressão tem como finalidade oferecer serviço de impressão as máquinas clientes dispostas na rede, possuindo um ou mais tipos de impressoras. [SOARES, LEMOS, COLCHER, 1995]

Para o servidor proposto nesse projeto o software que fará o papel de servidor de arquivos, impressão e controlador de domínio será o Samba.

3.4.1. Samba

O Samba é o servidor responsável pelo controle no compartilhamento de alguns serviços como arquivos, diretórios e impressão. É uma solução livre capaz de interligar redes com sistemas operacionais heterogêneos.

Atualmente, o Samba é um servidor fundamental para a migração de pequenos grupos de trabalho a grandes domínios com diferentes clientes. Esse servidor proporciona uma grande flexibilidade de acesso para o compartilhamento arquivos e impressão em rede. [SILVA, 2009]

O Samba possui algumas características fundamentais para o funcionamento das redes com sistemas operacionais heterogêneos como, compartilhamento de arquivos entra máquinas Linux e Windows, controle de impressão das máquinas

Windows através do servidor com Linux e permite montar unidades mapeadas nos sistemas Windows e de outros servidores Linux, como se fosse um diretório do Linux.

Além de prover serviços de impressão e arquivos, o Samba também oferece serviços de controlador de domínio primário da rede. Esse serviço é oferecido pelo PDC (*Primary Domain Controller)*[4], que é responsável por validar os usuários do domínio através de consulta a uma base de dados.

3.4.1.1. Protocolo SMB/CIFS

O SMB/CIFS (*Server Message Block/Common Internet File System*) é um protocolo que possui grande utilização nos sistemas operacionais Microsoft Windows e em sistemas Unix via Samba.

Esse protocolo encontra-se na camada de aplicação e é utilizado para compartilhamentos de arquivos e impressoras, permitindo que o cliente faça a manipulação como se estivessem em sua máquina local.

O funcionamento consiste no envio de pacotes do cliente para o servidor. Quando o servidor recebe esse pacote, ele checa para saber se o cliente tem permissão para fazer aquele tipo de requisição e por fim executa a requisição e envia o pacote de volta ao cliente. Ao retornar o pacote para o cliente, o mesmo verifica se o pacote de resposta foi completado com sucesso. Após o estabelecimento de uma conexão, um cliente pode manusear arquivos, impressoras ou outros recursos. Esse protocolo é capaz de suportar múltiplas requisições. A figura 5 apresenta um esquema de comunicação entre cliente e servidor. [RODRIGUES, 2008]

---

[4] O'REILLY. Using Samba, 3rd Edition. Califórnia: O'Reilly Media, 2007.

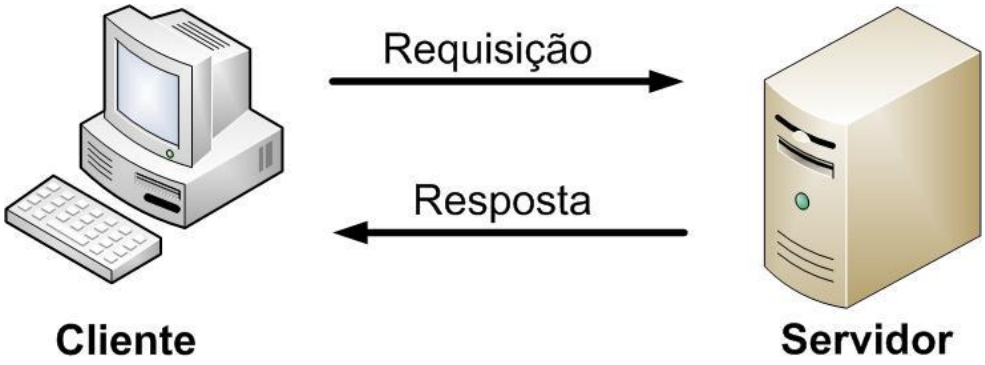


Figura 5: Requisição – Resposta

3.5. Controle de acesso a internet

O acesso a internet nas corporações tem sido inevitável devido ao grande avanço e dinamismo das novas tecnologias de comunicação. Para que as empresas realizem o acesso a internet de forma segura e eficiente, é necessário a implementação de servidores Proxy que funcione como um intermediador entre a rede interna da empresa e a internet.

Um dos servidores Proxy mais utilizados no mundo é o Squid. Trata-se de um Proxy bastante robusto e seguro. Esse software trabalha ouvindo requisições numa determinada porta padrão que pode ser configurada pelo administrador de rede. [SQUID-CACHE, 2006]

O Squid possui alguns recursos que o torna uma excelente alternativa. Um deles é o armazenamento do conteúdo já acessado em um *cache*, de forma que se houver um novo acesso a mesma informação já acessada, o Proxy fornece ao cliente a informação já armazenada com o propósito de se obter uma maior ganho de performance. Outra característica é a autenticação, para que somente os usuários autorizados possam acessar a internet. Esse software permite também a geração de um log onde serão registrados todos os acessos. E por fim, temos um recurso de segurança, pois a única máquina que está ligada diretamente a internet é o Proxy, sendo a única máquina potencialmente vulnerável. [SQUID-CACHE, 2006]

3.6. Sistema de Cota de Disco

Nas grandes empresas uma das maiores necessidades encontradas é a configuração da quantidade de disco que cada usuário pode ocupar. Para que haja esse controle é essencial a configuração do sistema de cota de disco.

> Cota de disco é o número de arquivos e blocos de dados definidos pelo administrador do sistema, que podem ser alocados para um usuário ou grupo, independentemente para cada sistema de arquivo (partição do disco rígido). [FERREIRA, 2003]

3.7. Dynamic Host Configuration Protocol (DHCP)

Antes de colocar uma nova máquina na rede de uma empresa é necessário escolhermos um endereço IP[5] que não esteja sendo utilizado por outra estação. Em pequenas empresas isso é possível de ser feito, mas nas grandes corporações isso se torna uma tarefa muito difícil e sujeita a bastantes falhas. Para evitar esse problema, foi criado o DHCP.

O DHCP é o servidor responsável em fornecer alguns dados para as máquinas clientes da rede interna como, por exemplo, o endereço IP. Esse servidor evita ter que realizar as configurações de rede manuais nos computadores. Assim, logo que uma máquina é configurada para receber os dados de rede automaticamente e entra em uma rede, a máquina envia um sinal para o servidor DHCP solicitando os dados para a sua configuração na rede. O servidor enviará os dados para a estação confirmando que a máquina poderá participar da rede em questão. Esse protocolo se preocupa em sempre evitar conflitos entre os seus clientes.

---

[5] Disponível em: <http://www.infowester.com/internetprotocol.php>. Acessado em 06 de maio de 2009.

3.8. Controle de inventário

É um software que permite ter um controle de todas as configurações de hardware e software das máquinas presentes em uma determinada rede. Para realizar o controle de inventários das estações clientes do sistema proposto, foi utilizados o software OCSng Inventory. A escolha se deu por ser o único software conhecido que consegue coletar dados de maneira correta de estações com os sistemas operacionais GNU/Linux e Windows.

3.8.1. OCSng Inventory

O OCSng Inventory (*Open Computer and Software Inventory Next Gerenetion*) auxilia bastante os administradores de rede das grandes empresas a ter um maior controle dos dispositivos da organização. O OCSng Inventory possui dois componentes, o módulo de gerenciamento fica instalado no servidor e os agentes nas máquinas clientes. [MUNIZ, 2007]

Após a instalação do software de inventário nas estações de trabalho iremos obter algumas informações fundamentais para o controle dos equipamentos da empresa como: processador, quantidade de memória, sistemas operacionais e programas instalados.

4. IMPLEMENTAÇÃO DO PROJETO

Neste capítulo são apresentadas as configurações e implementações realizadas para a montagem do projeto, descrevendo os softwares utilizados para a sua elaboração e as respectivas justificativas para seleção desses softwares.

4.1. Cenário proposto

Para elaboração desde projeto foi utilizado o cenário apresentado na figura 6:

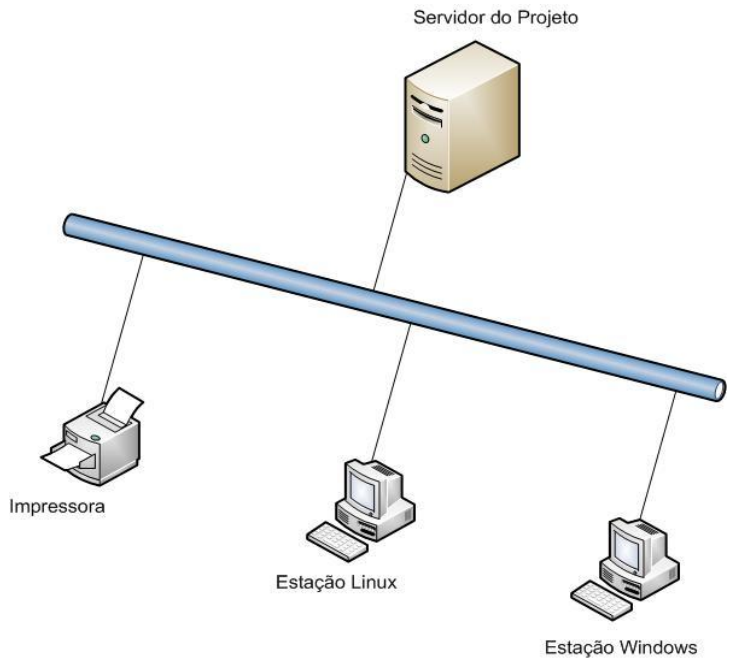


Figura 6: Cenário Proposto

A rede possui máquinas com sistemas operacionais diferentes. Uma máquina utiliza o sistema GNU/Linux e a outra Microsoft Windows XP. O servidor responsável por realizar o controle da rede utiliza o sistema operacional GNU/Linux. O mesmo atua como controlador de domínio, servidor de arquivos e impressão. Além disso, faz o controle de acessos a internet e inventário nas estações clientes. Esse modelo proposto é um sistema alternativo ao Windows 2003 Server.

Para criação do sistema proposto foram utilizadas as configurações abaixo:

- Nome do domínio utilizado: projeto.com
- IP do servidor: 172.16.5.10
- Hostname do servidor: servidor
- Gateway: 172.16.5.2
- Máscara: 255.255.255.0
- Intervalo de endereço IP para o DHCP: 172.16.5.200 a 172.16.5.250
- DNS: 208.67.222.222

A estação cliente com o sistema operacional Windows utiliza IP fixo. O IP fixado para esta estação é 172.16.5.150. Essa máquina recebe o nome de projeto-maq01. Já a estação com Linux pegar IP do servidor DHCP e recebe o nome de projeto-maq02.

Para facilitar o entendimento do sistema proposto, foram criados 5 usuários e 5 grupos. Os usuários são: dayanna, jose, dinair, thiago e dyanna. Os grupos criados foram: diretoria, financeiro, marketing, rh e shared. A usuária dayanna fará parte dos grupos diretoria e financeiro, o usuário jose do grupo financeiro, a usuária dinair do grupo rh, o usuário thiago do grupo marketing e por fim, a usuária dyanna faz parte também do grupo rh.

4.2. Sobre os softwares escolhidos

Para a implementação desse projeto são necessárias diversas ferramentas e softwares que integrem da melhor forma os sistemas. Para auxiliar na configuração

e integração desses sistemas é fundamental a criação de alguns scripts. Nos itens abaixo serão descritos todos os softwares utilizados na elaboração do projeto.

4.2.1. Software utilizado para virtualização

Para virtualização dos sistemas utilizados nesse projeto foi utilizado o software proprietário VMware Server, que é mundialmente difundido quando tratamos de virtualização de sistemas e por isso foi escolhido para implementação do projeto. A escolha da versão 2.0.0 foi por ser a mais atual no momento da elaboração do projeto, para trabalhar dentro de uma máquina GNU/Linux. Para utilizar o VMware Server é necessário adquirir licença, mas o mesmo não é obrigatório na solução deste projeto. Esse software foi utilizado apenas para demonstrar o sistema proposto.

4.2.2. Sistemas Operacionais

A distribuição Mandriva foi escolhida para utilização no servidor e na estação cliente desse projeto, por ser um sistema que combina estabilidade e atualidade. A distribuição Debian, por exemplo, é considerado um sistema bastante estável, porém seus programas são desatualizados.

A versão 2009.0 do Mandriva foi escolhida por ser a mais atualizada no momento da implementação do projeto.

A distribuição Mandriva também foi escolhida para a estação GNU/Linux em um dos clientes, por ser uma distribuição estável e de fácil configuração. A outra estação cliente desse projeto utilizará o Windows XP, por ser o sistema operacional mais comum nas estações de trabalho no momento da realização do projeto.

Na proposta do projeto foi citado que utilizaria a distribuição Ubuntu na estação GNU/Linux, mas foi alterado devida a distribuição Mandriva possuir recursos que facilitam a sua configuração para utilizar a base de dados do LDAP, facilitando assim para os administradores da rede nas empresas.

4.2.3. Aplicativo para controlar espaço em disco

O aplicativo quota foi escolhido, por permitir que os administradores das redes controlem a quantidade de espaço em disco que os usuários e grupos podem utilizar.

Foi escolhida a versão 3.16-3mdv2009.0, por ser a mais atual disponível na distribuição Mandriva utilizada no servidor desse projeto.

4.2.4. Softwares utilizados no servidor de arquivos, domínio e impressão

O Samba foi escolhido, pois possui todas as características necessárias para a implementação dos serviços de intranet. Esse software permite o controle de arquivos, diretórios e domínios na rede. A versão 4 do Samba, que encontra-se em desenvolvimento, oferecerá suporte ao *Active Directory* (AD) facilitando assim a administração de uma rede. O AD utiliza o protocolo LDAP para armazenar os dados relativos ao domínio de uma rede, tais como contas de usuários, grupos e políticas de segurança. A versão 4 do Samba seria ideal para a elaboração desse projeto, mas como ainda não está disponível, utilizaremos a versão 3.2.3 por ser a mais atual para o Mandriva no momento.

O serviço LDAP será utilizado na implementação desse projeto, pois é um protocolo robusto para armazenamento de base de dados de usuários. A versão 2.4.11-3mdv2009.0 foi em virtude de ser a mais atual para o Mandriva.

Para controlar as impressões será utilizado o CUPS. Esse software foi escolhido como servidor de impressão, pois é o padrão das distribuições GNU/Linux. Já a escolha da versão 1.3.9 deu-se ao fato de ser a mais atualizada compilada para o Mandriva.

4.2.5. Softwares utilizados no servidor Proxy

O servidor Proxy foi implementado com o Squid, pois esse é o software livre mais utilizado para este fim. A versão do Squid, 3.0, foi escolhida, pois é a versão mais atual compilada para o Mandriva.

Para ajudar no controle de acesso dos usuários a Internet foi utilizado o software FireUau, que é uma ferramenta desenvolvida em código aberto. Esse software possui a vantagem de permitir a realização de todas as configurações via gráfico, facilitando assim para os administradores da rede no momento da criação de uma política de acesso para os grupos e usuários. Outro motivo para a escolha desse software é por estar mais familiarizada com ele e por ser de fácil utilização.

4.2.6. Software utilizado para controle de inventário

O software livre OCSng Inventory foi escolhido por ser o único conhecido que consegue coletar dados de maneira correta de estações com os sistemas operacionais GNU/Linux e Windows. Ele possui suporte a diversas distribuições GNU/Linux, além de possuir suporte para os sistemas Microsoft Windows XP e Vista. A versão 1.02RC3 foi escolhida por ser a mais atualizada no presente momento. Não foi escolhida a versão padrão do Mandriva, pois essa está desatualizada.

4.3. Implementação da solução proposta

A maioria das configurações e instalações realizadas no servidor foi executada em um *prompt* de comando. Esses procedimentos foram realizados através de um comando que segue o seguinte formato:

```
# mkdir projeto
$ mkdir projeto
```

O símbolo # indica que para este comando está sendo utilizada a permissão de administrador do sistema (usuário root). Quando é executado um comando com o símbolo $, entende-se que terá apenas permissão de usuário normal.

Como este projeto não contempla a implementação de um servidor DNS, foi utilizado o DNS disponível no site do OpenDNS, para resolução de nomes ao realizar o download dos softwares de instalação necessários. Foi utilizado também pelo Proxy para resolver os nomes das requisições dos clientes que terão acesso a internet.

4.3.1. Servidor Samba

O Samba é responsável pelo controle dos arquivos, diretórios e domínio. Já o LDAP é responsável por armazenar os dados dos usuários, como: login, grupo pertencente e nome da máquina. E por fim, o SMBLDAP possui a finalidade de integrar o Samba e o LDAP, pois o mesmo é responsável por escrever os dados no LDAP.

A base de dados do LDAP funciona como se fosse uma árvore genealógica. A figura 7 apresenta um exemplo dessa árvore.

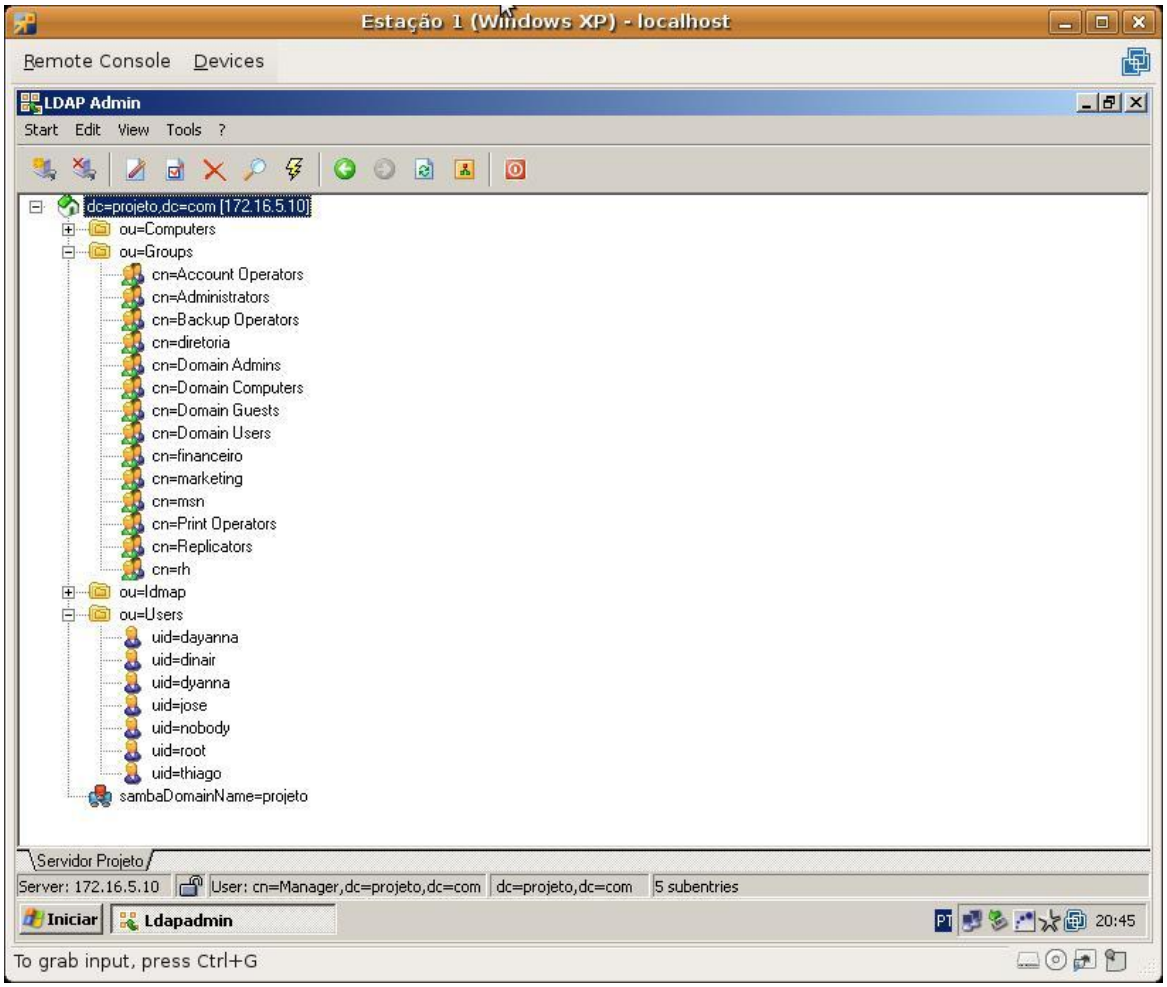


Figura 7: Árvore do LDAP

Para a criação desse servidor, foi instalado o Samba, o ldap e o smbladap que é responsável por integrar os dois aplicativos. O seguinte comando foi utilizado para realizar a instalação desses aplicativos:

```
# urpmi smbldap-tools openldap-servers Samba-server
```

4.3.1.1. Configurando o LDAP e o SMBLDAP

O arquivo de configuração do LDAP é o slapd.conf que fica localizado em /etc/openldap. As principais linhas configuradas foram:

/etc/openldap/sldap.conf:

```
suffix        "dc=projeto,dc=com"
```

```
rootdn          "cn=Manager,dc=projeto,dc=com"
rootpw          {SSHA}do5nHXnefAwzCzCm7xIC0ZEYGrD+LRJ8
```

O parâmentro *suffix* indica o sufixo do LDAP, que é base onde foram passadas todas as informações como usuários, grupos e nome das máquinas. Já o parâmetro *rootdn* indica o usuário que vai administrar a base criada. Por fim, o *rootpw* é a senha criptografada do usuário definido no rootdn. Para geração desse código criptografado foi executado seguinte comando:

```
# slappasswd
New password:
Re-enter new password:
{SSHA}jeKKIJnrZpODMuoX8bxQ5Ozlh/2ehWzf
```

Os arquivos de configuração do smbldap são smbldap_bind.conf e smbldap.conf que ficam localizados em /etc/smbldap-tools. As configurações realizadas no arquivo smbldap_bind.conf foram:

/etc/smbldap-tools/smbldap_bind.conf:

```
masterDN="cn=Manager,dc=projeto,dc=com"
masterPw="senha"
```

No parâmetro *masterDN* foi passado o usuário que tem privilégios para escrever na base do LDAP. Já no *masterPw* é passada a senha que irá autenticar o usuário.

As principais configurações realizadas no outro arquivo de configuração do SMBLDAP foram:

/etc/smbldap-tools/smbldap.conf:

```
sambaDomain="projeto"
masterLDAP="127.0.0.1"
masterPort="389"
suffix="dc=projeto,dc=com"
userHome="/home/%U"
userHomeDrive="H:"
```

userScript="%U.bat"

No parâmetro *sambaDomain* foi passado o domínio do servidor. Através desse domínio as máquinas se conectam na rede deste projeto. Já a linha de configuração *masterLDAP* informa onde está o servidor LDAP deste projeto. A linha seguinte, *masterPort* indica em qual porta o LDAP se conecta, nesse caso é a porta padrão 389. Logo abaixo, o parâmetro *suffix* informa qual o nome da base que é utilizada para criar a estrutura do LDAP. A linha de configuração *userHome="/home/%U"* informa o diretório no servidor onde fica a pasta pessoal do usuário, onde %U é o login do usuário está conectado no domínio do Samba. O parâmetro seguinte *userHomeDrive="H:"* informa o nome do drive onde é mapeada a pasta pessoal dos usuário na estação. Por fim, a última linha de configuração *userScript="%U.bat"* indica o formato do script que o usuário deve executar antes de logar no domínio, onde %U é o login do usuário na rede.

4.3.1.2. Configurando o Samba

O arquivo de configuração do Samba é o smb.conf, localizado em /etc/samba. Nesse arquivo foram definidas as funções que um servidor Samba deve desempenhar. O arquivo de configuração completo do Samba encontra-se no apêndice C.

A seção global é responsável por todas as configurações do servidor PDC. As principais configurações realizadas na seção global do arquivo de configuração do Samba foram:

/etc/samba/smb.conf:
[global]
workgroup = projeto
netbios name = servidor

O parâmetro *workgroup* informa qual o nome do domínio. Já a linha *netbios name* indica qual é o nome da máquina onde está o servidor deste projeto.

Além de controlador arquivos e diretórios, o Samba pode desempenhar também o papel de controlador de domínio, mas para isso devemos acrescentar algumas configurações ainda na seção global no arquivo de configuração do Samba.

/etc/samba/smb.conf:

```
[global]
os level = 255
preferred master = Yes
domain master = Yes
local master = Yes
domain logons = Yes
wins support = Yes
```

O parâmetro *os level=255* é utilizado caso seja configurado mais de um controlador de domínio na rede, então aquele que tiver maior os level é eleito e o outro fica como BDC (*Backup Domain Controller*). O intervalo vai de 0 a 255. Já o parâmetro *preferred master=Yes* faz com que o Samba tenha maior chance de ser eleito o controlador de domínio. O *domain master=Yes* define que o Samba é o controlador de domínio da rede. O *local master=Yes* habilita o Samba para ser um controlador de domínio. O *domain logons=Yes* define que o Samba é autenticador de domínio para o Windows 95/98. Por fim, a opção wins *support=Yes* faz com que o servidor Samba passe a trabalhar como um servidor WINS (Windows Internetworking Name Server) na rede. O WINS é um protocolo auxiliar dentro das redes Microsoft, responsável pela navegação na rede e listagem dos compartilhamentos e outros recursos disponíveis.

Realizadas essas configurações, o Samba torna-se um controlador de domínio.

É necessário também informar ao Samba, ainda na seção global, que ele utiliza a base de dados do LDAP. Para isso são configuras as seguintes linhas:

/etc/samba/smb.conf:

```
[global]
```

```
passdb backend = ldapsam:ldap://172.16.5.10/
ldap admin dn = cn=Manager,dc=projeto,dc=com
ldap suffix = dc=projeto,dc=com
ldap group suffix = ou=Groups
ldap user suffix = ou=Users
ldap machine suffix = ou=Computers
```

No primeiro parâmetro *passdb backend* é informado qual é o tipo de base de dados utilizada nesse projeto e o local onde está essa base de dados. Nesse caso foi passado que a base de dados é o LDAP e está no servidor. A próxima linha de configuração, a *ldap admin dn* informa qual o usuário tem permissão para escrever no LDAP, nesse caso é o usuário Manager. Logo a seguir o parâmetro *ldap suffix* nos informa qual a base onde é criada a estrutura do LDAP. Nas próximas linhas são informadas quais as pastas criadas dentro dessa estrutura. No caso deste projeto e conforme definido no arquivo de configuração, foram criadas as pastas *group*, *user* e *machine*, onde dentro de casa uma delas estão as informações de grupos, usuários e máquinas existentes na rede, respectivamente.

É também no arquivo de configuração do Samba que configuramos todos os compartilhamentos existentes. A seção homes identifica o diretório home de cada usuário, onde todas as informações são salvas e também onde o usuário tem permissão de escrita para salvar seus arquivos. Para que os usuários tenham acesso a sua pasta pessoal no servidor, foi configurada a seção homes no arquivo smb.conf.

/etc/samba/smb/conf:

```
[homes]
comment = Home Directories
browseable = no
writable = yes
```

O parâmetro *comment* é o local disponível para colocar comentários sobre essa seção. Como a seção homes é a responsável por compartilha a pasta pessoal dos usuários, o comentário utilizado foi diretório home. Na próxima linha de comandos, o parâmetro *browseable=no* fará com que esse compartilhamento seja

exibido apenas se o usuário digitar o caminho completo. E por fim, o parâmetro *writable=yes* indica que os usuários podem escrever nesse compartilhamento.

Outro compartilhamento criado nesse servidor foi do diretório profiles. Esse compartilhamento serve para armazenar as configurações de área de trabalho de cada usuário. Cada usuário tem uma pasta na raiz deste compartilhamento. As configurações realizadas para esse diretório foram:

/etc/samba/smb.conf:

```
[Profiles]
path = /var/lib/samba/profiles
browseable = no
writable = yes
```

O parâmetro *path* informa o caminho no servidor onde está o diretório profiles. As outras configurações conforme já informado anteriormente indicam que o diretório profiles só será exibido se for informado o caminho completo e os usuários podem escrever no diretório.

De acordo com o cenário proposto, a empresa é dividida em 4 setores. Para cada setor foi criado um compartilhamento e além desses foi criado um compartilhamento comum entre todos os setores da empresa. Esse compartilhamento comum a todos recebeu o nome de shared. E os outros compartilhamentos receberam o nome dos setores, que são: diretoria, financeiro, marketing e rh.

A seguir é apresentada a configuração realizada no arquivo de configuração do Samba para que esses diretórios fossem compartilhados:

/etc/samba/smb.conf:

```
[diretoria]
comment = Pasta compartilhada da diretoria
path = /var/lib/samba/shares/diretoria
valid users = @diretoria
public = no
writable = yes
```

```
create mask = 660
directory mask = 770
```

O parâmetro *comment*, conforme já informado, é apenas uma descrição sobre o compartilhamento. O *path* é o caminho no servidor onde fica o diretório a ser compartilhado. O parâmetro *valid users=@diretoria* indica que apenas os usuários que estiverem no grupo diretoria podem acessar o diretório compartilhado. A linha seguinte *public=no* informa que este diretório não está disponível para clientes que não tenham um login no servidor. O próximo parâmetro *writable=yes* faz com que os usuários consigam escrever nesse diretório. Por fim, os parâmetros *create mask=660* e *directory mask=770* indicam os tipos de permissões para arquivos e pastas criadas nesse compartilhamento.

Essas permissões são definidas por números e letras, de acordo com as tabelas 1 e 2.

Tabela 1: Permissão de leitura, escrita e execução

Permissão de Leitura	Permissão de Escrita	Permissão de execução
4	2	1

No caso do parâmetro *create mask=660* indica que este arquivo tem permissão de leitura e escrita, onde leitura corresponde a 4 e escrita 2. Somando as permissões, totalizamos 6. Já no *directory mask=770* além das permissões de leitura e escrita, soma-se a permissão de execução, pois trata-se de um diretório e para abrí-lo deve ser executado, portanto totaliza em 7.

A ordem em que são colocados os números influência nessas permissões, conforme pode ser verificado na tabela 2.

Tabela 2: Permissão a dono, grupo ou outros

Primeiro Campo	Segundo Campo	Terceiro Campo
Dono	Grupo	Outros

O primeiro campo indica que a permissão está associada ao dono do arquivo ou diretório. O segundo campo associa a permissão a um grupo. Por fim, o terceiro

campo dá permissão a outro usuário que não seja o dono e nem usuários do grupo associado no segundo campo.

Os demais compartilhamentos têm as mesmas configurações realizadas para o diretório diretoria.

Além desses compartilhamentos, foi criado o diretório shared e este, por sua vez, foi configurado com permissão de leitura e escrita para todos os usuários que fizerem login no domínio, assim todos os usuários podem compartilhar arquivos de interesse geral dentro da rede. Segue abaixo as configurações realizadas para esse compartilhamento:

/etc/samba/smb.conf:

```
[shared]
comment = Pasta compartilhada da shared
path = /var/lib/samba/shares/shared
public = no
writable = yes
create mask = 660
directory mask = 770
nt acl support = yes
inherit acls = Yes
```

A única diferença da configuração desse diretório para os demais, é que este não possui o parâmetro *valid users*, já que se trata de um diretório comum a todos os usuários da rede e também por possuir configurações que ativam as permissões especiais do Windows no arquivo. O parâmetro *nt acl support = yes* é responsável por ativar o uso de ACL's no Samba. Já o parâmetro *inherit acls = yes* faz com que o samba verifique as permissões de acl ao acessar os arquivos e diretórios.

Para facilitar a criação dos *scripts* de login dos usuários, diretivas de grupos e outras ferramentas que são necessárias durante o login dos usuários, foi instalado o Ntlogon. Essa ferramenta é responsável por criar o arquivo .bat dos usuários. A figura 8 ilustra o arquivo dayanna.bat da usuária Dayanna.

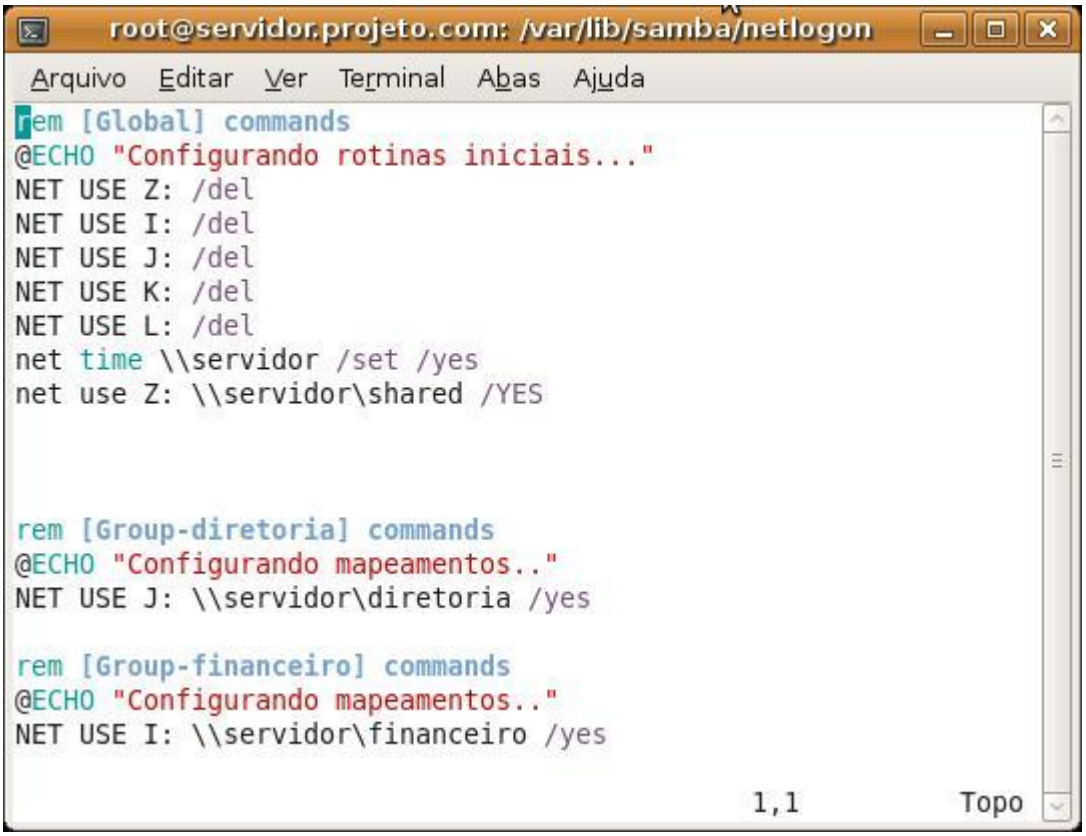


Figura 8: Arquivo dayanna.bat

O script acima informa que deverá ser montado para a usuária os diretórios diretoria e financeiro, pois essa usuária faz parte desses grupos.

Esses arquivos com a extensão bat devem ser compartilhados no diretório netlogon. Esse compartilhamento tem papel fundamental no suporte ao login e participação de usuário do domínio. Todos os controladores de domínio Microsoft possuem o compartilhamento netlogon. Para isso, foram acrescentadas mais algumas linhas no arquivo de configuração do Samba:

/etc/samba/smb.conf:

[netlogon]

comment = Network Logon Service

path = /var/lib/samba/netlogon

root preexec = /usr/local/samba/bin/ntlogon --user='%u' –dir=/var/lib/Samba/netlogon/

Conforme já informado, o primeiro parâmetro é um comentário sobre o compartilhamento. O segundo é o local onde o diretório está no servidor. E por fim, o

terceiro parâmetro é responsável por criar a bat, colocar no diretório netlogon. O arquivo de configuração do ntlogon é o ntlogon.conf. O arquivo de configuração completo encontra-se no apêndice D. A principais configurações realizadas nesse arquivo foram:

/etc/ntlogon.conf:

```
[Global]
net time \\servidor /set /Yes
net use Z: \\servidor\shared /YES
[Group-financeiro]
@ECHO "Configurando mapeamentos.."
NET USE I: \\servidor\financeiro /yes
[Group-diretoria]
@ECHO "Configurando mapeamentos.."
NET USE J: \\servidor\diretoria /yes
[Group-marketing]
@ECHO "Configurando mapeamentos.."
NET USE K: \\servidor\marketing /yes
[Group-rh]
@ECHO "Configurando mapeamentos.."
NET USE L: \\servidor\rh /yes
```

As linhas configuradas na seção global estão no arquivo .bat de todos os usuários. Já as linhas configuradas dentro das seções dos grupos estão apenas nos arquivos .bat dos usuários pertencentes a esses grupos. Por exemplo, a usuária dayanna pertence ao grupo diretoria. Portanto, no seu arquivo .bat aparecerá apenas as linhas da seção group-diretoria, conforme pode ser visualizado na figura 8.

A criação de usuários e grupos no LDAP é feito através da seguinte linha:

```
# smbldap-useradd –a –m –c “Dayanna Martins” dayanna
```

O parâmetro *smbldap-useradd* serve para criar um novo usuário. A opção *–a* faz com que o usuário seja criado na estrutura do LDAP. Já a opção *–m* é para que no momento da criação do usuário seja criado também o diretório pessoal dentro do

/home do servidor. A opção *–c* é para passar uma descrição do usuário, no caso seu nome completo. Por fim, dayanna é o login do usuário a ser criado no momento.

A definição de senha para este usuário é feito através do seguinte comando:

```
#smbldap-passwd dayanna
```

A criação dos grupos é feita através da seguinte linha de comando:

```
#smbldap-groupadd –a diretoria
```

O parâmetro *smbldap-groupadd* indica que vai ser criado um novo grupo. A opção *–a* é para que o grupo seja criado na base do LDAP. E por fim, diretoria é o nome do novo grupo a ser criado.

Para adicionar ou remover um usuário de um determinado grupo é executado seguinte comando:

```
#smbldap-usermod –g diretoria –G financeiro dayanna
```

O parâmetro *smbldap-usermod* serve para modificar a configuração de algum usuário da rede. A opção *–g* serve para adicionar um grupo primário para este usuário. Já a opção *–G* adiciona um grupo secundário para o usuário. Finalizando, deve ser adicionado no final da linha o login do usuário que deseja efetuar essas alterações.

4.3.1.3. Configurando o CUPS

Uma das ferramentas mais utilizadas para prover serviços de impressão é o software CUPS (Common Unix Printing System). O CUPS atua como um servidor de impressão recebendo requisições de impressões das estações clientes. Os documentos que as máquinas clientes enviam para impressão vão para o servidor, que se encarrega de organizá-los em fila para que possam sem enviados para a impressora da rede.

Uma grande vantagem desse software é por permitir a integração com o Samba. Assim, esse servidor de impressão torna-se um software compatível com as estações clientes que possuam o sistema operacional Microsoft Windows instalado. O compartilhamento de impressão, portanto é feito através do Samba.

Para criação do servidor de impressão foi necessário instalar o CUPS e alguns drivers para a impressora.

```
# urpmi cups task-printing-hp
```

A impressora foi instalada em um computador auxiliar, para simular uma impressora de rede. Essa impressora foi compartilhada na rede do projeto através do Samba.

As configurações do servidor de impressão são realizadas pelo administrador de rede, através da interface web do CUPS. O endereço para acesso é http://172.16.5.10:631, onde 172.16.5.10 é o IP do servidor e 631 é a porta de acesso a interface web do CUPS.

Realizadas todas as configurações, resta configurarmos o Samba, para que utilize a infra-estrutura do CUPS como servidor de impressão.

Para que as impressoras configuradas no CUPS possam ser compartilhadas na rede, foi necessário adicionar algumas linhas no arquivo de configuração do Samba.

/etc/samba/smb.conf:

```
[global]
printing = cups
load printers = Yes
```

Na seção global foram acrescentados os parâmetros printing=cups, que informa o servidor de impressão. E o outro parâmetro é o *load printers=yes*, que é responsável por carregar todas as impressoras presentes no CUPS.

Além da seção global, é necessário criar a seção printers no arquivo de configuração do Samba, pois é nesse diretório que vão estar as impressoras compartilhadas na rede.

/etc/samba/smb.conf:

```
[printers]
comment = All Printers
path = /var/spool/samba
browseable = yes
guest ok = yes
printable = Yes
```

No parâmetro *comment* é colocado um comentário sobre esse compartilhamento. Já no *path*, é informado o caminho completo onde está o compartilhamento no servidor. O *browseable=yes* indica que não é necessário digitar o caminho completo para visualizar esse compartilhamento. O parâmetro *guest ok=yes* é para que usuários convidados, que não possuam login no servidor, possam acessar o compartilhamento com as impressoras. E por fim, o *printable=yes* indica que tem permissão para imprimir com as impressoras compartilhadas na rede.

Na figura 9 pode ser visualizada a impressora do projeto configurada no CUPS.

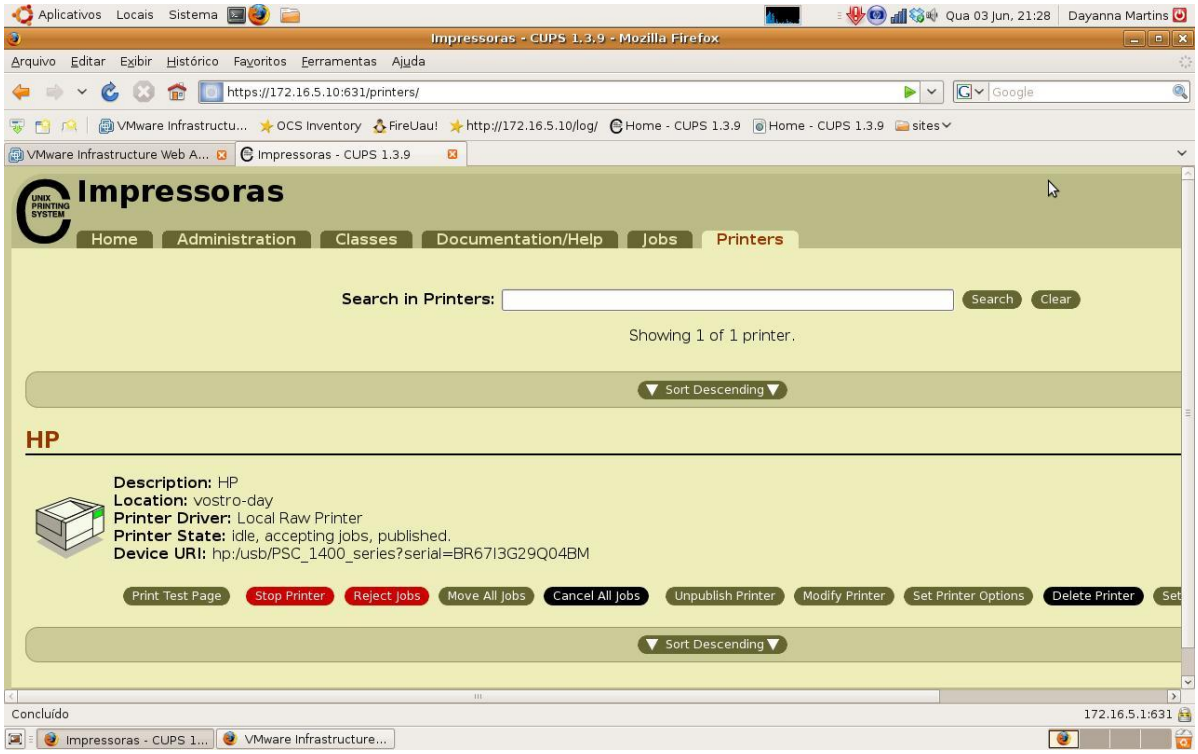


Figura 9: Interface web do CUPS

4.3.2. Servidor Proxy

O servidor *Proxy* é um intermediário nas requisições realizadas entre os clientes e o servidor. Para criamos o servidor Proxy, foi necessário instalar o software Squid. O controle de acesso a Internet e a criação de políticas de acesso foi realizado pelo software FireUau.

A instalação do Squid foi realizada através do comando urpmi que é padrão de instalação do mandriva.

```
# urpmi squid
```

Além do Squid, foi necessário realizar a instalação do software de banco de dados postgresql no servidor deste projeto, para que o FireUau possa armazenar todas as informações de políticas de acesso dos grupos e usuários. Foi criada uma estrutura do banco de dados para que o FireUau consiga guardar as informações necessárias.

```
# su – postgres
# cd /opt/fwl/pgsql
# sh mkdb.sh
# exit
```

No primeiro comando é realizado login com o usuário postgres, após isso foi realizado acesso no diretório pgsql e então é executado o *script* mkdb.sh do FireUau que é responsável por criar a estrutura do banco de dados.

Outros softwares essenciais para o funcionamento do servidor Proxy, foi a instalação do php e Apache, já que o FireUau é manipulado através de uma interface web, como podemos visualizar na figura 10.

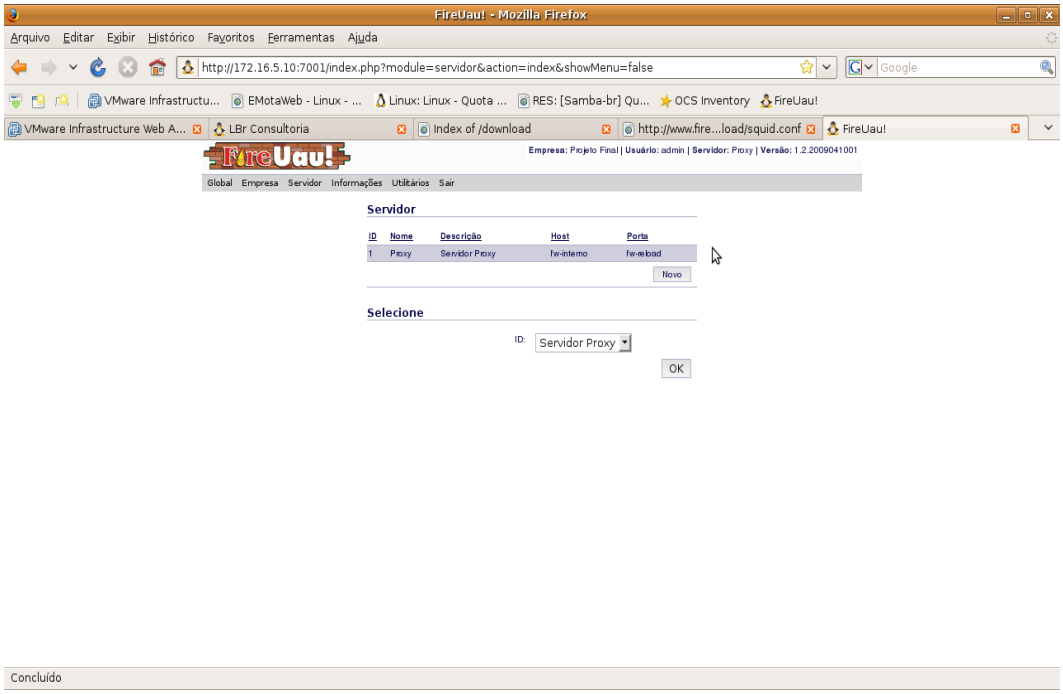


Figura 10: Tela inicial do FireUau

O arquivo de configuração do FireUau é o fwl.conf que encontra-se no diretório /etc/sysconfig/FireUau. O arquivo de configuração completo encontra-se no apêndice E. O arquivo foi configurado conforme as linhas abaixo:

/etc/sysconfig/FireUau/fwl.conf:

```
SERVER="172.16.5.10"
SQUID=1
```

O parâmetro *SERVER* indica qual o IP do servidor onde se encontra o FireUau. Já o parâmetro *SQUID* indica se o FireUau vai configurar o servidor Proxy. O valor 1 (um) indica que esse servidor foi ativado e 0 (zero) desativado.

Por fim, resta ao administrador da rede acessar a interface web do FireUau e definir as regras de bloqueio, de acordo com os grupos de usuários. O endereço para acesso a essa interface é http://172.16.5.10:7001, onde o 172.16.5.10 é o IP do servidor e 7001 é a porta de acesso da interface web do FireUau.

O servidor Proxy utiliza a base de dados do LDAP. Para isso, foi necessário realizar uma alteração no arquivo de configuração do Squid.

/etc/squid/squid.conf:

external_acl_type fwl children=10 ttl=600 %LOGIN %SRC /opt/fwl/acesso/scripts/ldapaccess.sh

Essa linha de configuração faz com que o FireUau carregue a base de dados do LDAP.

Para que o administrador da rede configure os sites que os setores da empresa podem ou não acessar, é necessário criar alguns filtros de conteúdo e algumas políticas de acesso para os grupos existentes. O FireUau já possui um filtro de conteúdo padrão, onde esse bloqueia o acesso a todos os sites. Dessa forma foram criados apenas alguns filtros permitindo acesso a determinados sites para os grupos existentes.

Ao criar um filtro de conteúdo devem ser passados os parâmetros apresentados na figura 11.

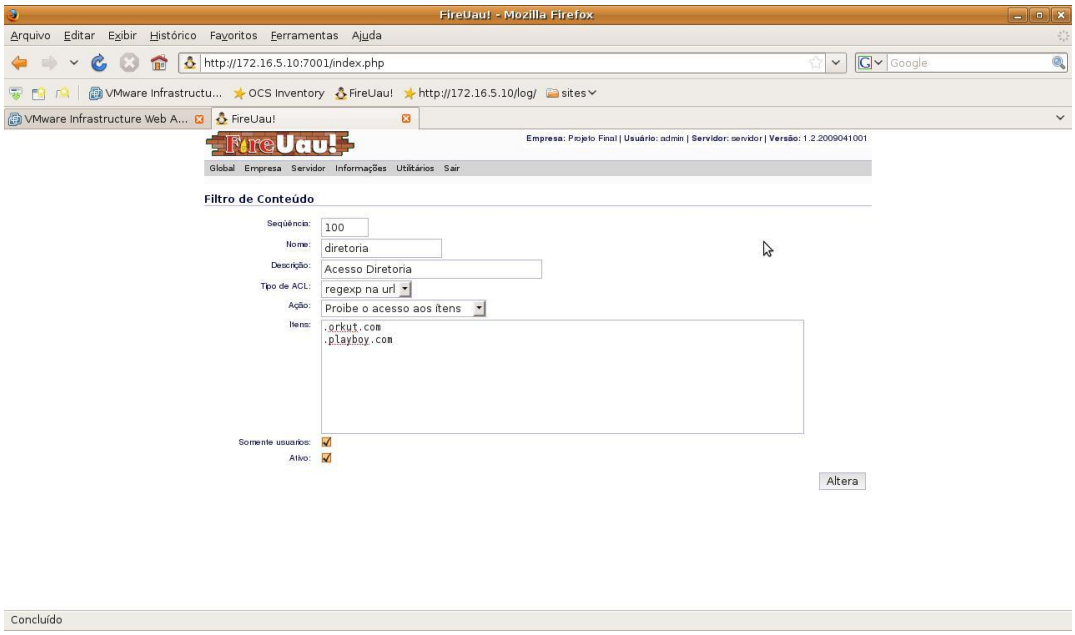


Figura 11: Criando filtro de conteúdo para o grupo Diretoria

O campo *sequência* indica exatamente a ordem que o FireUau vai ler os filtros de conteúdo. Por exemplo, se foi criada uma regra com a *sequência*=10 informando que bloqueia o acesso ao site www.google.com.br e logo após foi criado outro filtro com a *sequência*=11 informando que permite acesso a todos os sites. O sistema vai primeiro bloquear o acessso ao site do Google e liberar o acessos aos outros sites. Já em *nome*, é informado um título para o filtro de conteúdo. A seguir é feita uma descrição sobre o filtro que foi criado. No campo *tipo de ACL* temos 3 opções: *domínio*, *regexp na url* e *src*. O parâmetro *domínio* serve para indicar que foi realizado o filtro através do endereço completo, por exemplo, www.google.com.br. Já o parâmetro *regexp na url*, indica que o filtro foi através de palavras que aparecem no endereço, por exemplo, .google.com. O parâmetro *src* indica que o filtro foi feito através do IP. No campo *itens* que foram passados os endereços ou IP's para acesso ou bloqueio pelo FireUau. A opção *somente usuários* deve ser marcada para que esse filtro se aplique somente a usuários do grupo ao qual se refere o filtro, senão é aplicada a todos os outros usuários. Por fim, a opção *ativo* indica se esse filtro de conteúdo esta ativo ou não no FireUau.

Os filtros de conteúdo criados para o sistema proposto foram definidos de acordo com o setor da empresa que o usuário faz parte. A seguir serão descritas as regras para os grupos correspondentes:

- Grupo diretoria: Só não acesso o site www.orkut.com;
- Grupo financeiro: Só pode acessar os sites www.bancobrasil.com.br, www.bb.com.br e www.itau.com.br;
- Grupo marketing: Só pode acessar os sites www.terra.com.br, www.uol.com.br e www.globo.com;
- Grupo rh: Só pode acessar o site www.rh.com.br.

A figura 12 mostra esses filtros de conteúdo criados no FireUau.

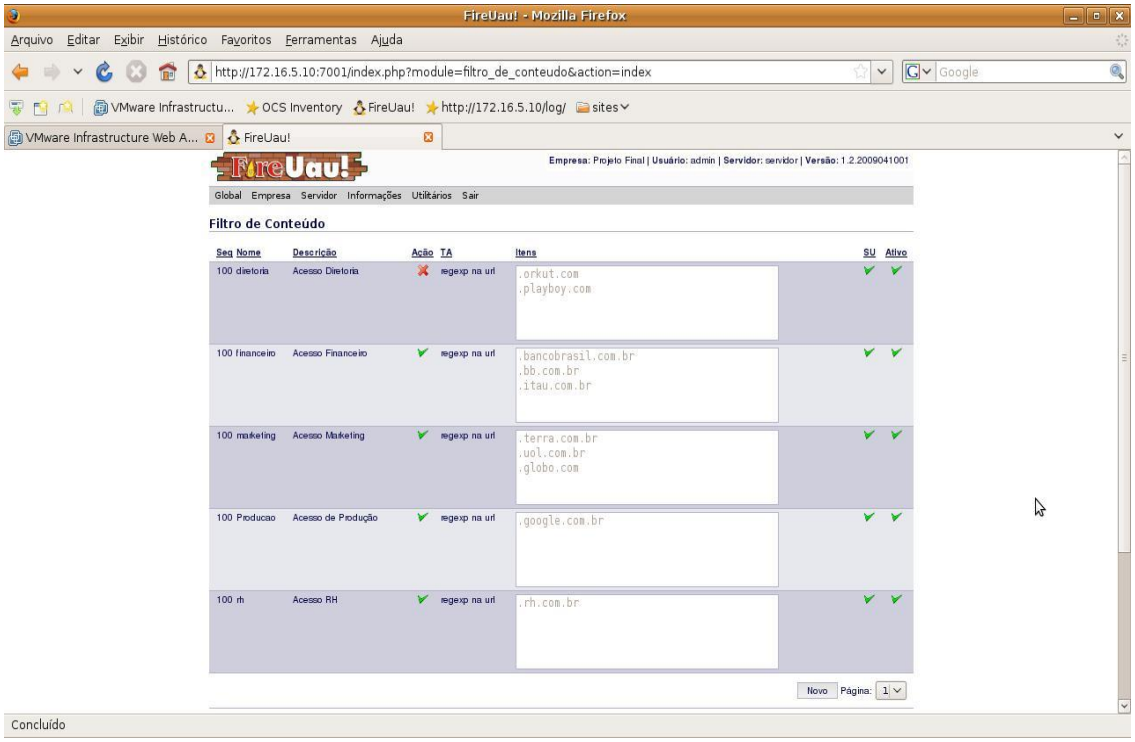


Figura 12: Lista com os filtros de conteúdo

Após criar todos os filtros de conteúdo necessários, foram configuradas as políticas de acesso. Nesse caso, foram informados os parâmetros conforme apresentado nas figuras 13 e 14.

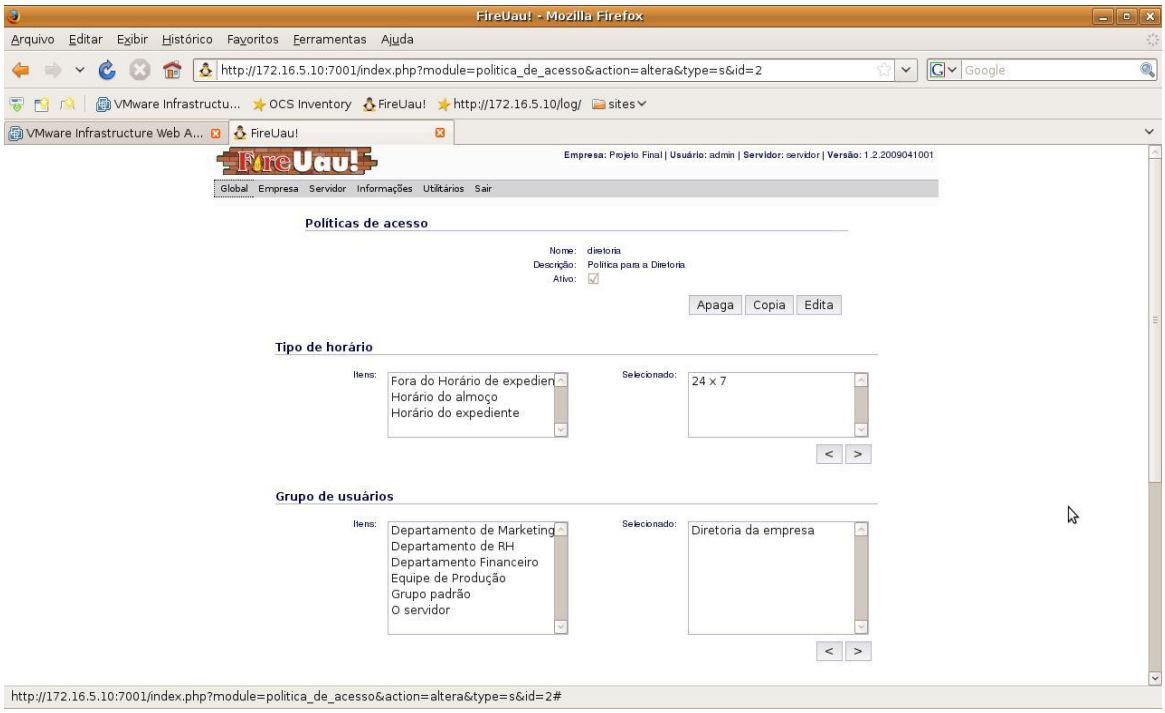


Figura 13: Configurando Politicas de acesso

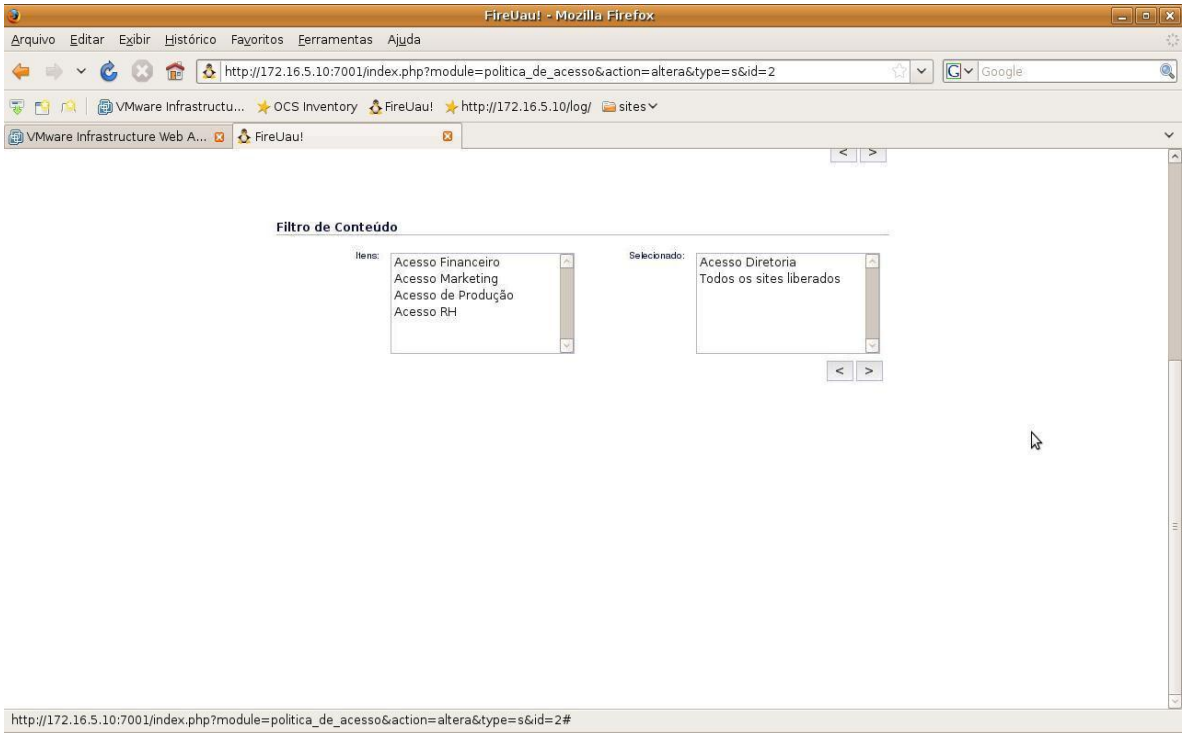


Figura 14: Configurando Politicas de acesso (Continuação)

No campo *Tipo de Horário* é informado em quais períodos essa política foi utilizada. As opções são: 24x7, fora do horário de expediente, horário do almoço,

horário do expediente. Já no campo *Grupo de Usuários* é informado a que grupo da empresa a política a ser configurada irá se aplicar. Por fim, no campo *Filtro de Conteúdo* são informados quais os filtros foram utilizados para essa política.

Depois de realizadas todas as configurações necessárias no FireUau, essas foram gravadas no arquivo de configuração do Squid pelo FireUau. Isso acontece quando o administrador da rede clica no menu Utilitários e seleciona a opção Recarrega, conforme apresenta a figura 15.

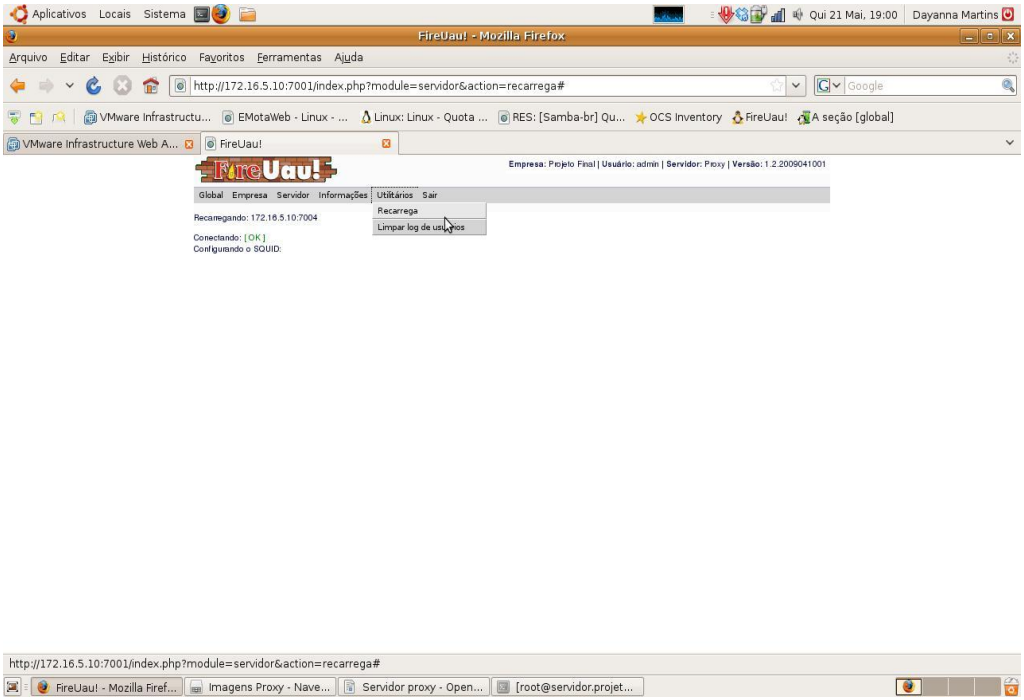


Figura 15: Escrevendo no arquivo de configuração do Squid

A figura 16 mostra o arquivo de configuração do Squid com as alterações realizadas pelo FireUau.

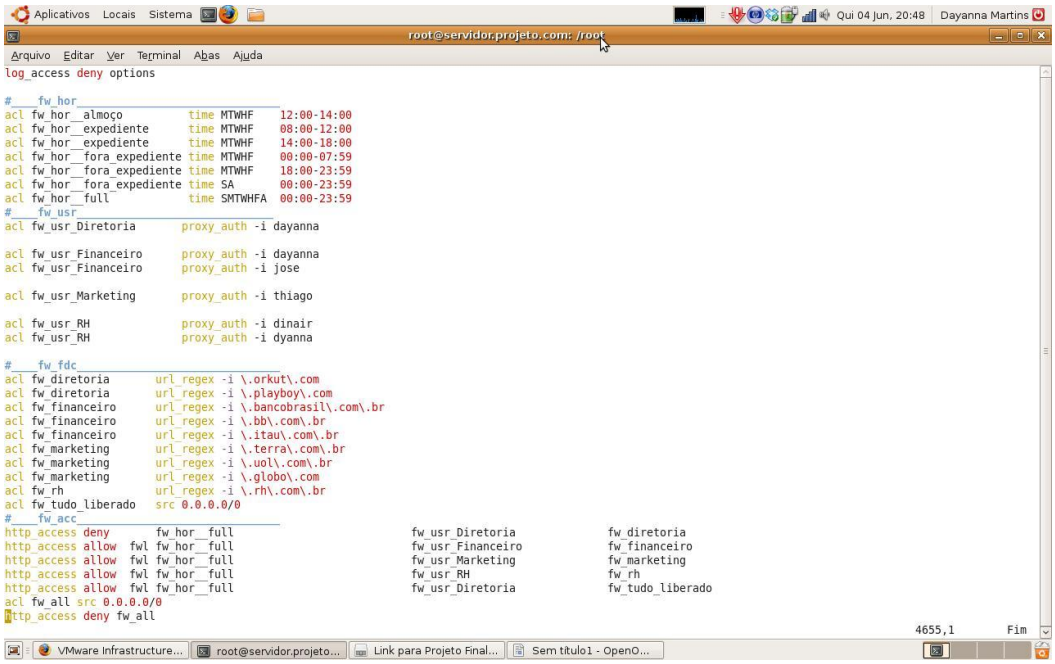


Figura 16: Arquivo de configuração do Squid

4.3.2.1. Sarg

O Sarg (*Squid Analysis Report Generator*) é um utilitário gerador de relatórios sobre os arquivos de log do Squid.

A instalação do Sarg foi realizada através do comando urpmi que é padrão de instalação do mandriva.

```
# urpmi sarg
```

O arquivos de configurações do Sarg é o sarg.conf, que fica localizado em /etc/sarg. As principais configurações realizadas nesse arquivo foram:

/etc/sarg/sarg.conf:

language Portuguese

access_log /var/log/squid/access.log

output_dir /var/www/html/log

resolve_ip yes

date_format e

O parâmetro *language Portuguese* informa que o idioma utilizado no Sarg é português. Já o parâmetro *access_log /var/log/squid/access.log* indica qual arquivo o Sarg retira as informações para gerar o relatórios. O parâmetro *output_dir /var/www/html/log* indica o diretório base onde foram gerados todos os relatórios. O parâmetro *resolve_ip yes* é responsável por tentar descobrir o nome da máquina que realizou o acesso a determinado site através do IP. Por fim, o parâmetro *date_format e* indica que o formato utilizado para datas é o Europeu (dd/mm/aaaa).

Além do Sarg foi necessário realizar algumas configurações no arquivo do Apache para que os relatórios fossem exibidos em uma página da web. Para isso foram adicionadas as seguintes linhas no arquivo httpd.conf.

/etc/httpd/conf/httpd.conf:

```
<Directory /var/www/html/log>
        AuthName “Relatório de Acesso.”
        AuthType Basic
        AuthUserFile /etc/Sarg/senha
        require valid-user
</Directory>
```

Essas linhas dentro do parâmetro Directory indicam que foram realizadas algumas configurações para o diretório de log onde são gravados os relatórios, que fica localizado em /var/www/html. No parâmetro AuthName é informado o título que aparece na tela de autenticação do Sarg, conforme apresenta a figura 17.

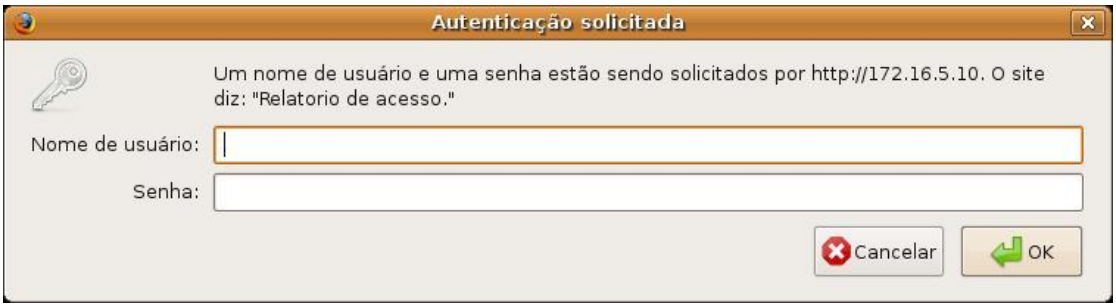


Figura 17: Autenticação do Sarg

Já o parâmetro *AuthType* indica que a autenticação realizada é do tipo Basic. O parâmetro *AuthUserFile* informa o arquivo onde fica a senha para acesso ao

diretórios onde ficam os logs. Por fim, o parâmetro *require valid-user*, indica que o Sarg exige autenticação para acesso ao diretório de log.

Realizadas essas configurações no arquivo do Apache, é necessário criar o usuário e a senha do diretório dos logs do Sarg. Para criar, é utilizado o comando *htpasswd*. O usuário criado para acesso a interface web do Sarg foi Admin.

Para que o Sarg gere um relatório, é preciso apenas chamá-lo quando quiser atualizar os relatórios, através do comando Sarg. Para que não seja necessário ficar digitando esse comando sempre que for necessário acompanhar o relatório, essa tarefa será automatizada através do cron.

O cron é um serviço carregado durante o boot do sistema. Esse serviço permite programar a execução de comando. Para executar as tarefas programadas o cron utiliza o crontab. O arquivo crontab fica localizado em /var/spool/cron. Para criar essas tarefas é utilizado o seguinte comando:

```
# crontab -e
```

O sistema proposto foi programado para executar o comando Sarg de 5 em 5 minutos. Para isso, foi criada essa regra no crontrab conforme apresenta a figura 18.

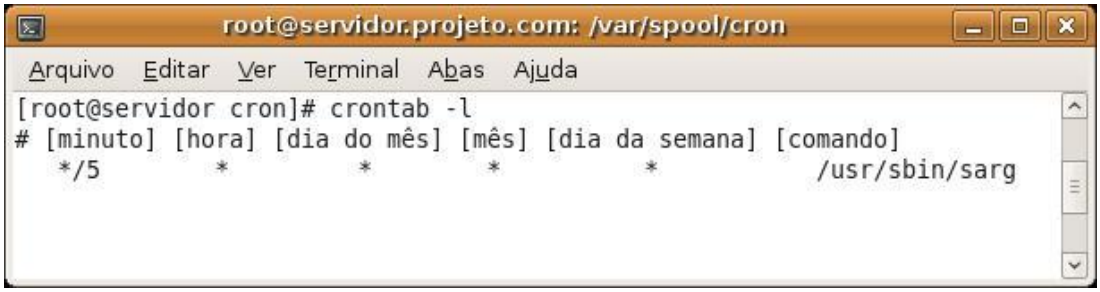
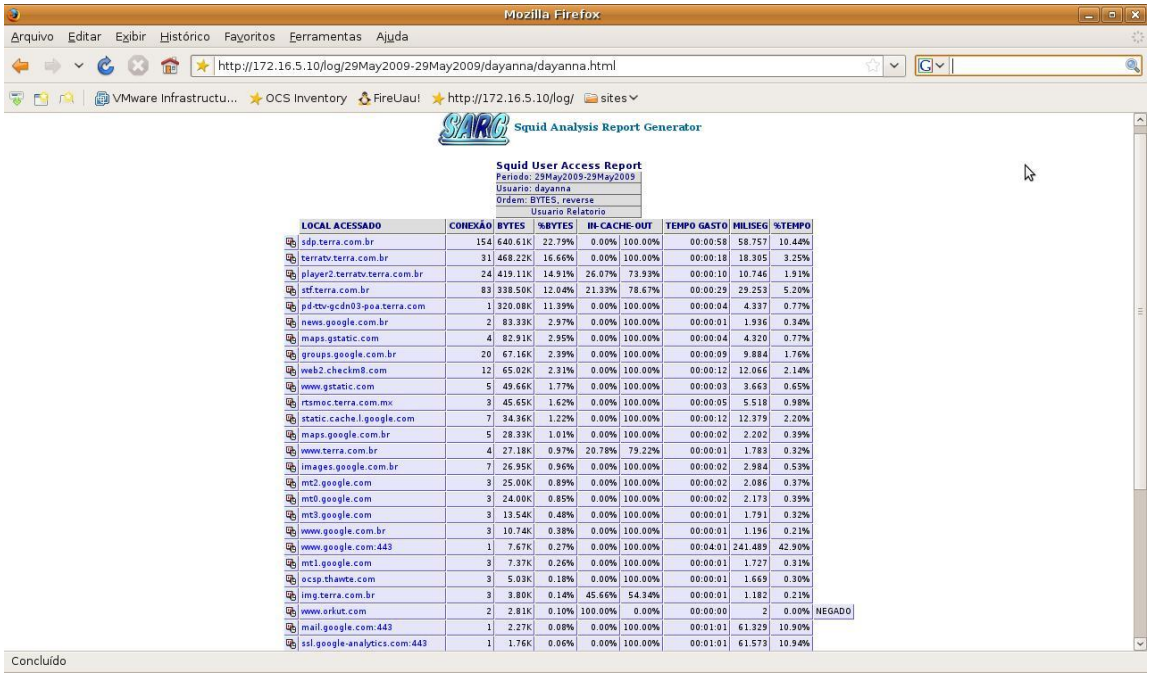


Figura 18: Tarefa programada no Crontab

O parâmetro **/5* indica que a tarefa é executada de 5 em 5 minutos de todas as horas, todos dias do mês, todo mês e todos dias da semana. Já no parâmetro *comando* é passado qual o comando que será executado nesse intervalo programado.

O endereço para acessar o Sarg via web é http://172.16.5.10/log. Através desse endereço é possível visualizar o dia em que foi gerado o log, o dia que foi feito o acesso, qual usuário realizou o acesso e por fim se o acesso foi liberado ou negado.

A figura 19 apresenta um log gerado pelo Sarg.



LOCAL ACESSADO	CONEXÃO	BYTES	%BYTES	IN-CACHE-OUT		TEMPO GASTO	MILISEG	%TEMPO	
sdp.terra.com.br	154	640.61K	22.79%	0.00%	100.00%	00:00:58	58.757	10.44%	
terratv.terra.com.br	31	468.22K	16.66%	0.00%	100.00%	00:00:18	18.305	3.25%	
player2.terratv.terra.com.br	24	419.11K	14.91%	26.07%	73.93%	00:00:10	10.746	1.91%	
stf.terra.com.br	83	338.50K	12.04%	21.33%	78.67%	00:00:29	29.253	5.20%	
pd-ttv-gcdn03-poa.terra.com	1	320.08K	11.39%	0.00%	100.00%	00:00:04	4.337	0.77%	
news.google.com.br	2	83.33K	2.97%	0.00%	100.00%	00:00:01	1.936	0.34%	
maps.gstatic.com	4	82.91K	2.95%	0.00%	100.00%	00:00:04	4.320	0.77%	
groups.google.com.br	20	67.16K	2.39%	0.00%	100.00%	00:00:09	9.884	1.76%	
web2.checkm8.com	12	65.02K	2.31%	0.00%	100.00%	00:00:12	12.066	2.14%	
www.gstatic.com	5	49.66K	1.77%	0.00%	100.00%	00:00:03	3.663	0.65%	
rtsmoc.terra.com.mx	3	45.65K	1.62%	0.00%	100.00%	00:00:05	5.518	0.98%	
static.cache.l.google.com	7	34.36K	1.22%	0.00%	100.00%	00:00:12	12.379	2.20%	
maps.google.com.br	5	28.33K	1.01%	0.00%	100.00%	00:00:02	2.202	0.39%	
www.terra.com.br	4	27.18K	0.97%	20.78%	79.22%	00:00:01	1.783	0.32%	
images.google.com.br	7	26.95K	0.96%	0.00%	100.00%	00:00:02	2.984	0.53%	
mt2.google.com	3	25.00K	0.89%	0.00%	100.00%	00:00:02	2.086	0.37%	
mt0.google.com	3	24.00K	0.85%	0.00%	100.00%	00:00:02	2.173	0.39%	
mt3.google.com	3	13.54K	0.48%	0.00%	100.00%	00:00:01	1.791	0.32%	
www.google.com.br	3	10.74K	0.38%	0.00%	100.00%	00:00:01	1.196	0.21%	
www.google.com:443	1	7.67K	0.27%	0.00%	100.00%	00:04:01	241.489	42.90%	
mt1.google.com	3	7.37K	0.26%	0.00%	100.00%	00:00:01	1.727	0.31%	
ocsp.thawte.com	3	5.03K	0.18%	0.00%	100.00%	00:00:01	1.669	0.30%	
img.terra.com.br	3	3.80K	0.14%	45.66%	54.34%	00:00:01	1.182	0.21%	
www.orkut.com	2	2.81K	0.10%	100.00%	0.00%	00:00:00	2	0.00%	NEGADO
mail.google.com:443	1	2.27K	0.08%	0.00%	100.00%	00:01:01	61.329	10.90%	
ssl.google-analytics.com:443	1	1.76K	0.06%	0.00%	100.00%	00:01:01	61.573	10.94%	

Figura 19: Relatório gerado pelo Sarg

4.3.3. Sistema de cota de disco

Esse sistema consiste em limitar a quantidade de espaço no disco que os usuários e grupos podem utilizar.

Inicialmente foi instalado o aplicativo quota:

```
# urpmi quota
```

Para que possa ser limitado o espaço em disco da pasta pessoal dos usuários, foi necessário criar o arquivo quota.user dentro da partição onde estão localizadas as pastas pessoais dos usuários, nesse caso no diretório /home. Além disso, foi preciso dá permissão de leitura e escrita a esse arquivo. Para limitar

espaço em disco para os grupos citados no cenário do projeto, foi criado o arquivo quota.group dentro do diretório /var/lib/samba, que é o diretórios raiz dos grupos.

Esses arquivos criados são binários e não podem ser editados diretamente por um editor de texto. O comando *edquota*, que será explicado posteriormente, é responsável por extrair as informações existentes nesses arquivos.

Outra configuração necessária no sistema de cota é a configuração do arquivo fstab que está localizado em /etc/fstab. O arquivo de configuração completo do fstab encontra-se no apêndice B. Assim, serão informadas as partições onde ficam os dados dos usuários e dos grupos, que devem respeitar as regras impostas pelo sistema quota. O parâmetro que foi acrescentado para cota de usuários é o *usrquota* e para grupos é o *grpquota*, conforme podemos visualizar abaixo:

/etc/fstab:
/dev/vg00/4 /home ext3 relatime,usrquota 1 2
/dev/vg00/a /var/lib/Samba ext3 relatime,acl,user_xattr,grpquota 1 2

Depois de realizadas essas configurações, vamos fazer uma checagem para saber se os arquivos de cotas estão funcionando e por fim habilitar o sistema de cota em disco.

4.3.3.1. Gerenciando cotas

O gerenciamento de cotas nesse aplicativo é realizado através do comando edquota. Dentro desse arquivo serão passadas as seguintes informações:

- Filesystem - partição que terá a quota editada;
- Blocks - número máximo de blocos (em Kbytes) que o usuário possui atualmente;
    - Soft – restrição mínima de espaço em disco utilizado;

- Hard – limite máximo aceitável de uso em disco para o usuário/grupo sendo editado;

- Inodes – número máximo de arquivos que o usuário possui atualmente na partição especificada;

  - Soft – restrição mínima do número de arquivos que o usuário/grupo possui em disco;

  - Hard – restrição máxima do número de arquivos que o usuário/grupo possui em disco.

Quando um usuário ou grupo atinge o limite configurado no soft é enviada uma mensagem de alerta, mas ainda assim é possível gravar informações nesse diretório por um prazo padrão de 7 dias (podendo ser alterado). Após esse prazo, as informações que estavam no espaço soft não ficarão mais disponíveis para o usuário ou grupo. Já quando o hard é atingido o usuário é automaticamente bloqueado para criar novos arquivos ou diretórios.

Na figura 20 pode ser visto um exemplo para o melhor entendimento de cota em disco, onde A corresponde ao espaço mínimo configurado para um determinado usuário/grupo e B corresponde ao espaço máximo que o usuário/grupo pode utilizar no disco.

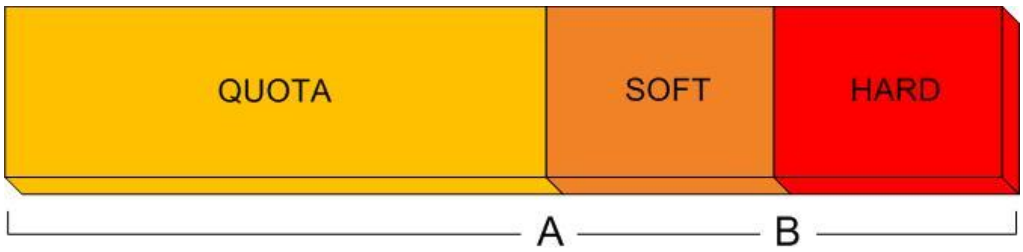


Figura 20: Cota em Disco

4.3.4. Configuração dinâmica dos clientes (DHCP)

Inicialmente foi instalada a versão do DHCP escolhida para o sistema proposto que é a 3.0.7.

```
# urpmi dhcp
```

O executável dhcpd foi instalado e utilizará o arquivo de configuração dhcpd.conf, que está localizado em /etc/dhcpd.conf. É neste arquivo que se define as principais funções do servidor DHCP.

É nesse arquivo de configuração que ficam descritas as funções que o servidor DHCP deve realizar, além de algumas informações sobre a topologia da rede. O arquivo de configuração para o ambiente proposto encontra-se nos apêndices desta monografia.

O arquivo de configuração do DHCP passa as informações necessárias para as estações clientes acessarem a rede. As configurações realizadas foram: o intervalo de endereço IP que as máquinas da rede podem utilizar, o tempo que cada estação pode utilizar esses endereços fornecido pelo servidor, a máscara da rede, o gateway e o servidor DNS utilizado. O arquivo de configuração completo do dhcp encontra-se no apêndice A.

Esse arquivo de configuração também permite configurar IP fixo para as estações clientes, caso haja necessidade. Para isso é necessário apenas colocar o endereço MAC da máquina e o IP que deseja fixar, conforme abaixo.

/etc/dhcpd.conf:

```
host windows {
        hardware ethernet 00:0c:29:9b:33:bc;
        fixed-address 172.16.5.150;
}
```

4.3.5. Controle de Inventário

O controle de inventário nas máquinas da rede foi realizado através do software OCSng Inventory. Primeiramente foi instalada a versão Server no servidor desse projeto e depois a versão para cliente nas estações.

No servidor, além de instalar o software para o controle de inventário, foi necessário instalar também o MySQL, que é o banco de dados utilizado pelo OCSng Inventory para armazenar o inventário coletado nas estações clientes. Para utilizar a interface web como forma de gerenciar o inventário, foi instalado no servidor o Apache e o php.

O relatório com o inventário das máquinas é gerado pelas estações clientes e enviado para o servidor, que por sua vez recebe esses dados e grava no banco de dados. Já o php busca os dados dos inventários das máquinas no bando de dados e exibe no navegador.

O controle do inventário das máquinas que estão na rede é realizado através do endereço http://172.16.5.10/ocsreports/index.php. A figura 21 nos mostra a tela inicial do software de controle de inventário.

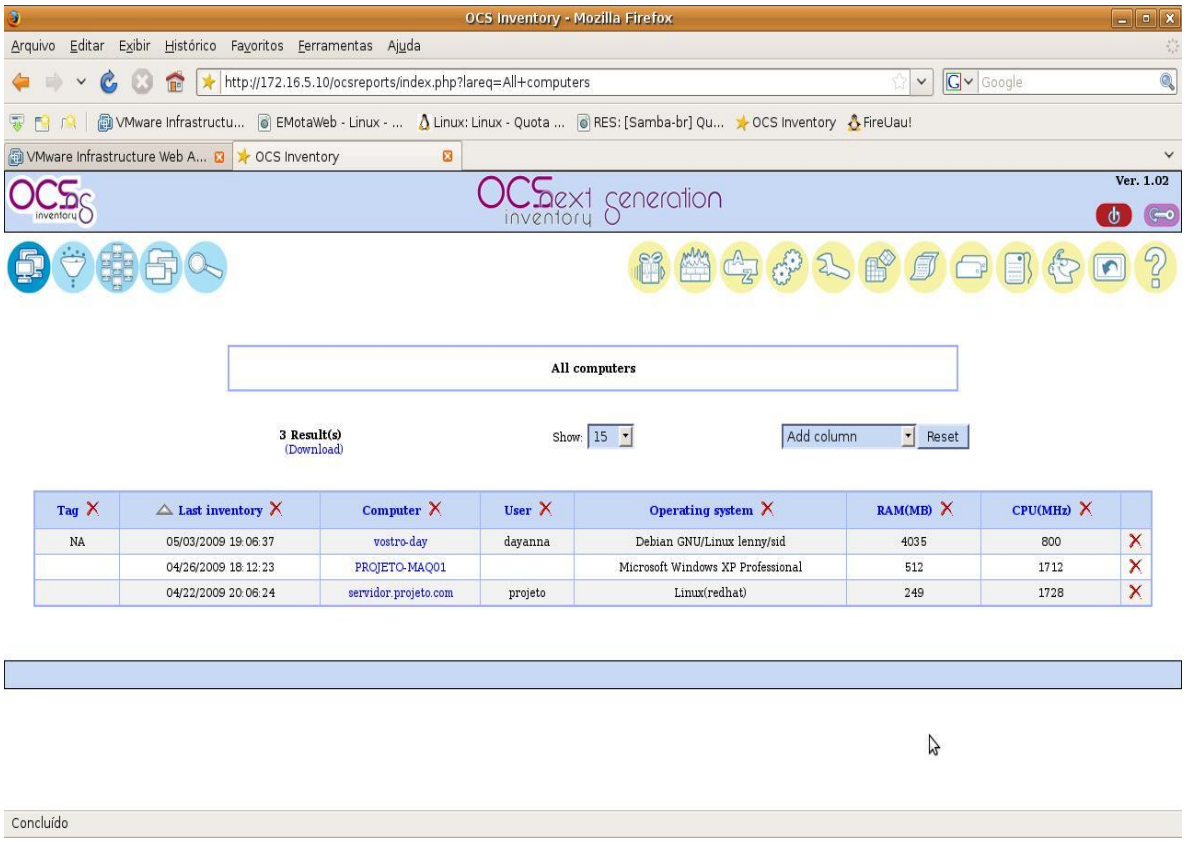


Figura 21: Tela Inicial OCSng Inventory

Nessa tela inicial do software, é possível visualizar algumas informações que já foram gravadas no banco de dados referente ao inventário das estações clientes da rede, como: nome da estação, usuários que estava conectado no momento em que foi retirado o relatório com o inventário, sistema operacional da máquina, quantidade de memória RAM, entre outras. Essas informações que aparecem na tela inicial podem ser alteradas de acordo com a necessidade de cada administrador da rede.

4.3.6. Configurando as Estações Clientes

A principal diferença na configuração das estações Windows e Linux é a forma como será realizado o acesso a base de dados dos usuários no LDAP. As máquinas com o sistema operacional da Windows XP realizaram o acesso ao LDAP através do Samba, já as máquinas com a distribuição Mandriva acessaram diretamente a base de dados do LDAP.

Nos subtítulos a seguir serão descritas as configurações quem foram realizadas nas estações clientes, para estas possam fazer parte da rede do projeto proposto.

4.3.6.1. Configurando a Estação Microsoft Windows

Conforme informado no cenário proposto, a estação Windows utiliza o IP fixo 172.16.5.150. Então, a primeira configuração realizada foi fixar esse IP na máquina.

Outras configurações realizadas na estação Windows XP foram:

- Colocar a máquina no domínio;
- Verificar se os compartilhamentos foram mapeados;
- Realizar teste de acesso a Internet através do Proxy;
- Instalar o driver da impressora na estação e testar se a máquina está imprimindo através da impressora configurada na rede do projeto.

4.3.6.2. Configurando a Estação GNU/Linux

Diferente da estação Windows, a máquina com o sistema operacional Linux vai pegar IP através do servidor DHCP.

Conforme informado no item 4.3.6, as estações com a distribuição Mandriva vão realizar acesso direto na base de dados do LDAP. Para isso, é necessário configurar o servidor NFS (Network File System).

O Sistema de Arquivo em Rede foi desenvolvido para permitir que se possam montar partições ou diretórios remotos como se fosse um disco local. A grande vantagem desse sistema de arquivos é que não há necessidade de usuários terem diretórios pessoais separados em cada máquina da rede, assim, os diretórios

pessoais podem ser configurados no servidor NFS e serem disponibilizados através da rede.

Para utilizarmos esse sistema de arquivos é necessário realizar a instalação no servidor e na estação cliente.

Para criação do servidor NFS foram instalados o *portmap*, que é utilizado por este servidor para gerenciar as requisições dos clientes e o *nfs-utils*.

```
# urpmi portmap nfs-utils
```

A configuração do NFS é feita através do arquivo de configuração exports que fica localizado em /etc. Nesse arquivo foram acrescentadas as seguintes linhas:

/etc/exports:

```
/home                172.16.5.0/24 (sync,rw)
/var/lib/samba/shares    172.16.5.0/24 (sync,rw)
```

A primeira linha indica que o diretório home dos usuários no servidor foi mapeado para as estações clientes que estão dentro da rede 172.16.5.0, que é a rede deste projeto. Já a segunda linha indica que foi mapeado o diretório shares, que é o diretório onde se encontram as pastas a serem compartilhadas pelo servidor. O parâmetro *sync* indica que a todo o momento novas informações são sincronizadas com o servidor. Já o parâmetro *rw* indica que esse compartilhamento tem permissão de leitura e escrita.

O diretório home do usuário no servidor foi montado no lugar do diretório home local do usuário. Assim, quando o usuário for salvar algum arquivo em sua pasta pessoal, estará salvando as informações automaticamente no servidor. Já os diretórios compartilhados do servidor que estão dentro da pasta shares foram montados no diretório /media/shares da estação do usuário. Para que os usuários não tenham que acessar o diretório media e depois o diretório shares para conseguir visualizar os compartilhamentos do servidor, foi realizada uma alteração no script de login e logout dos usuários, para que o diretório shares fossem montado dentro do diretório Empresa na pasta pessoal do usuário.

O script de login dos usuários é o *.bash_profile*. Esse arquivo fica localizado em /etc/skel. Foi acrescentada a seguinte linha no script:

/etc/skel/.bash_profile:

```
[ -L ~/Empresa ] || ln –s /media/shares ~/Empresa
```

A linha acima realiza um teste para saber se o link /home/usuário/Empresa já existe, caso não exista, cria o link do diretório /media/shares para /home/usuário/Empresa.

Já o script de logout dos usuários é o *.bash_logout*. Esse arquivo também fica localizado em /etc/skel. A linha acrescentada nesse script foi:

/etc/skel/.bash_logout:

```
[ -L ~/Empresa ] && unlink ~/Empresa
```

A linha acima realiza um teste para saber se o link /home/usuário/Empresa existe, caso sim, desmonta o link.

Dessa forma, sempre que o usuário fizer login nas estações Linux, é mapeado o diretório Empresa dentro da sua pasta pessoal, com todos os diretórios compartilhados no servidor.

Finalizadas as configurações do NFS no servidor do projeto, é necessário configurar o NFS na estação cliente com sistema operacional Linux. Para isso, é necessário instalar o *portmap* e o *nfs-utils* também na estação cliente.

```
# urpmi portmap nfs-utils
```

Uma das principais configurações necessárias na estação cliente foi realizada no arquivo fstab, que é responsável por montar os compartilhamentos de rede durante o boot do sistema. O arquivo fica localizado em /etc. As configurações realizadas foram:

/etc/fstab:

```
172.16.5.10:/home          /home          nfs      defaults0 0
```

```
172.16.5.10:/var/lib/Samba/shares        /media/shares    nfs        defaults0 0
```

A primeira linha indica que o diretório home do usuário no servidor foi mapeado no diretório home local do usuário a partir do sistema de arquivo NFS, onde a permissão utilizada é a default. A permissão default utiliza as seguintes opções: rw, exec, auto, nouser, e async. Onde:

- *rw*: monta o sistema de arquivo com permissão de leitura e escrita;
- *exec*: permissão de execução de arquivos;
- *auto*: habilita a montagem automática do diretório;
- *nouser*: somente o usuário root pode montar e desmontar o diretório;
- *async*: transferência de dados assíncrona, onde primeiramente a alteração é gravada na memória e só após confirmação o dado é gravado fisicamente.

Já a segunda linha adicionada no arquivo de configuração do fstab indica que o diretório que contém os compartilhamentos do servidor foi mapeado no diretório /media da estação cliente através do sistema de arquivo NFS com permissão default.

Por fim, a estação foi configurada para puxar a base de dados do LDAP.

Com a estação Linux configurada na rede, foram realizados os seguintes testes:

- Verificar se os compartilhamentos foram mapeados;
- Realizar teste de acesso a Internet através do Proxy;
- Instalar o CUPS e o drive da impressora na estação e testar se a máquina está imprimindo através da impressora configurada na rede do projeto.

5. RESULTADOS OBTIDOS

Este capítulo tem como objetivo apresentar os testes que foram realizados após a elaboração deste projeto, as dificuldades encontradas e por fim, as funcionalidades obtidas.

5.1. Testes realizados

Após a elaboração do sistema proposto, foram realizados diversos testes. A seguir serão apresentados os testes realizados com as estações clientes do projeto. As estações receberam os seguintes nomes: projeto-maq01 e projeto-maq02. Sendo que a primeira possui o sistema operacional Windows e a segunda Linux.

5.1.1. Estação com o Sistema Operacional Windows

Um dos principais testes realizados foi verificar se a estação estava no domínio deste projeto. A figura 22 mostra a estação Windows conectada no domínio.

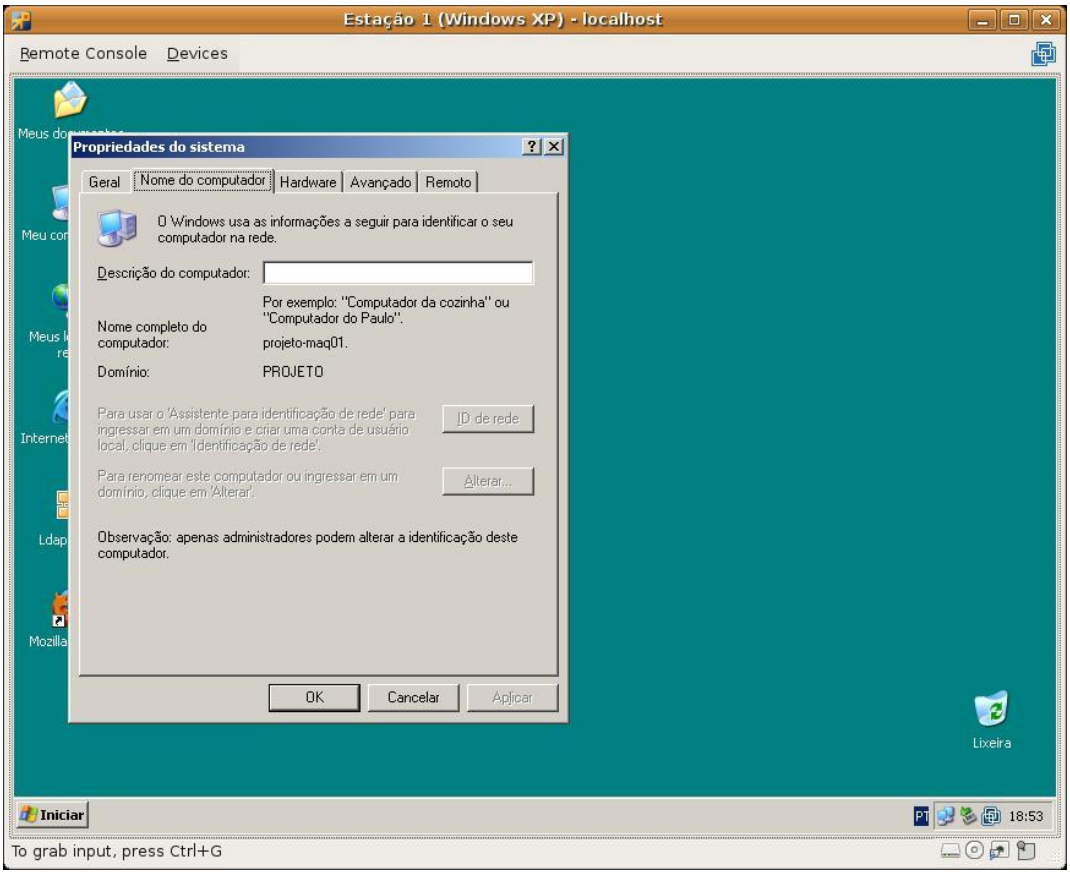


Figura 22: Estação Windows no domínio do projeto

Com a estação no domínio do projeto, foi realizada a configuração para colocar a máquina na rede. Para testar uma funcionalidade do servidor DHCP de fixar o IP através do MAC Address, a máquina Windows receberá um IP fixo, conforme destacado na figura 23.

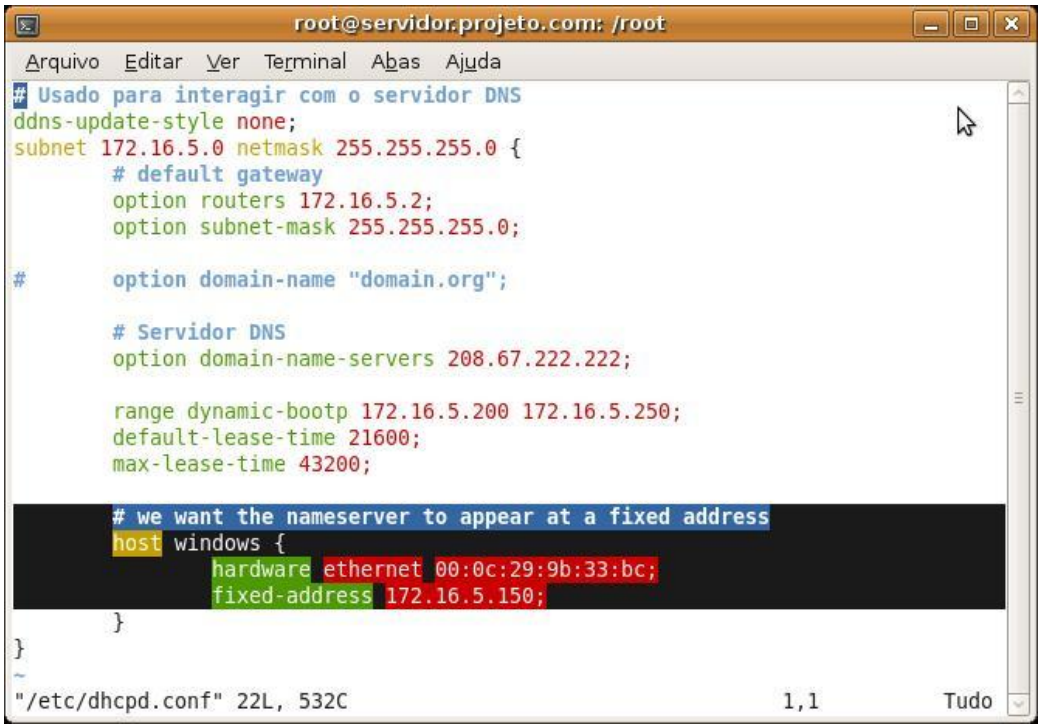


Figura 23: Fixando IP para estação Windows

A figura 24 mostra a configuração realizada na estação para utilização do IP (172.16.5.150) configurado para ela no servidor.

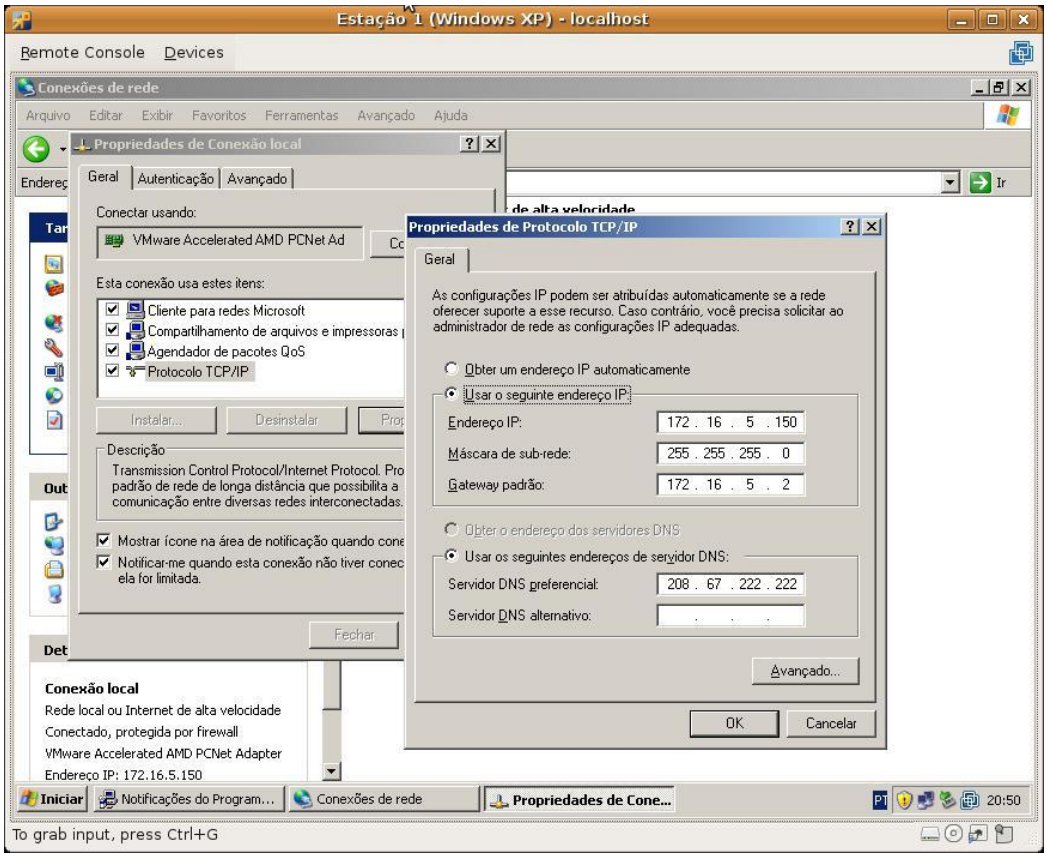


Figura 24: Configurando IP fixo no Windows XP

Outro teste realizado foi verificar se os compartilhamentos foram mapeados nessa estação. Foi feito login na máquina com o usuário “dayanna”. Este usuário faz parte dos grupos “diretoria” e “financeiro”, portanto devem ser mapeados para este usuário os seguintes diretórios: diretoria, financeiro, diretório pessoal do usuário no servidor (/home/dayanna) e por fim o diretório shared que deve ser mapeado para todos os usuários da rede. De acordo com a figura 25, todos esses diretórios foram mapeados corretamente.

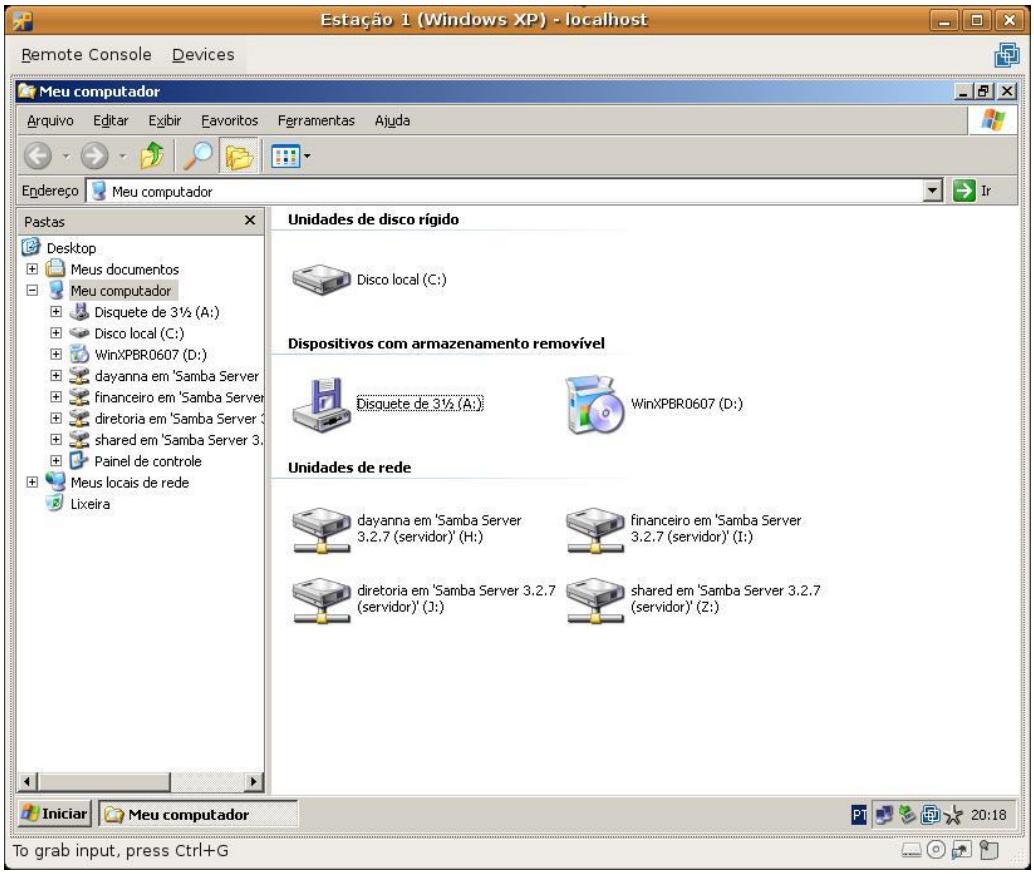


Figura 25: Compartilhamentos da estação Windows

O espaço em disco que os usuários e os grupos podem utilizar foi limitado através do uso de quotas. Essas configurações foram realizadas no servidor do projeto. Na figura 26 podem ser visualizadas as quotas configuradas para os usuários.

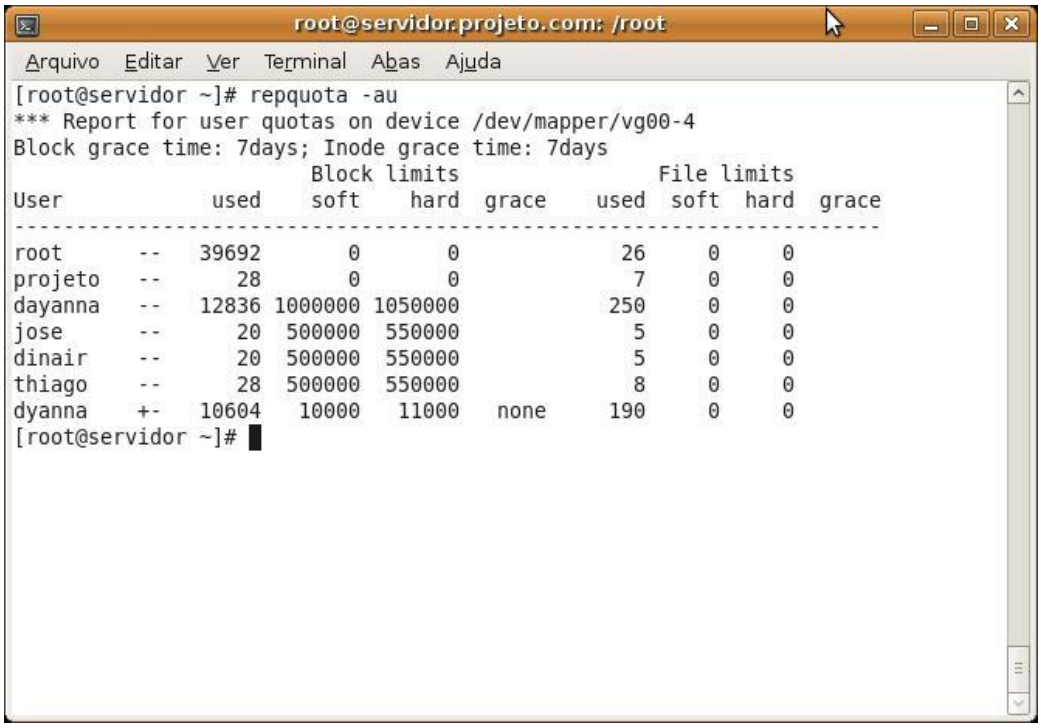


Figura 26: Configurando cota de usuário no servidor

Já na figura 27 são apresentadas as quotas de grupo.

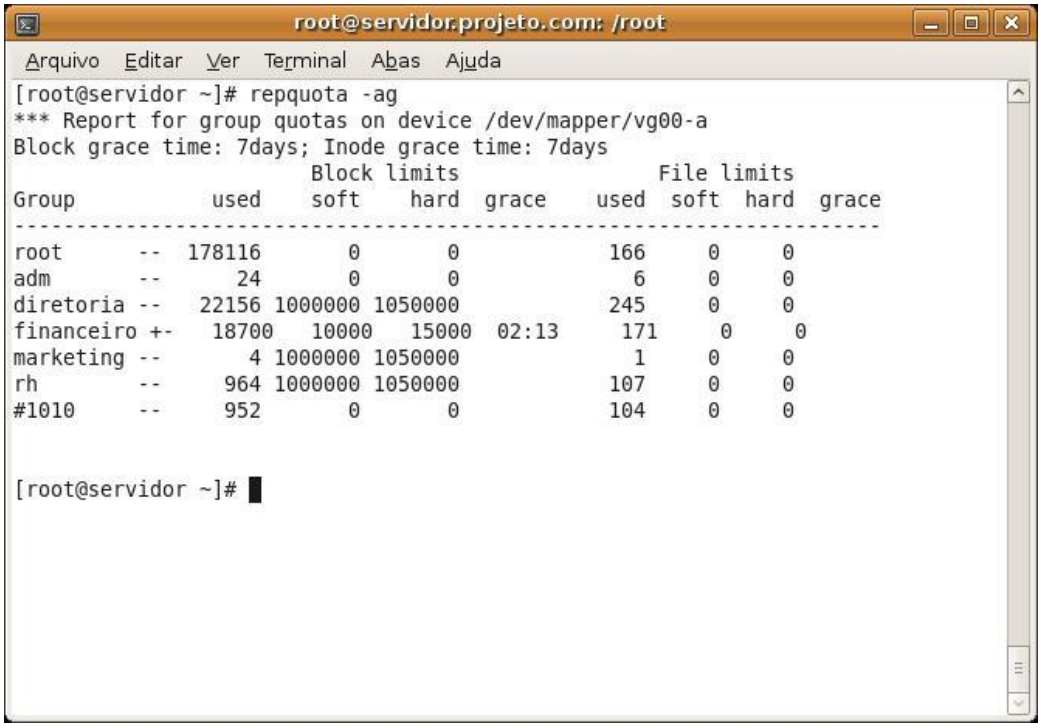


Figura 27: Configurando cota de grupo no servidor

De acordo com a figura 26 o servidor foi configurado para que a usuária “dyanna” possa utilizar 10 MB de espaço em disco.

Foi realizada uma tentativa de copiar arquivos maiores de 10 MB para o diretório pessoal da usuária. Na figura 28 pode ser visualizada a mensagem de erro apresentada ao copiar um arquivo com tamanho superior ao espaço alocado para esta usuária.

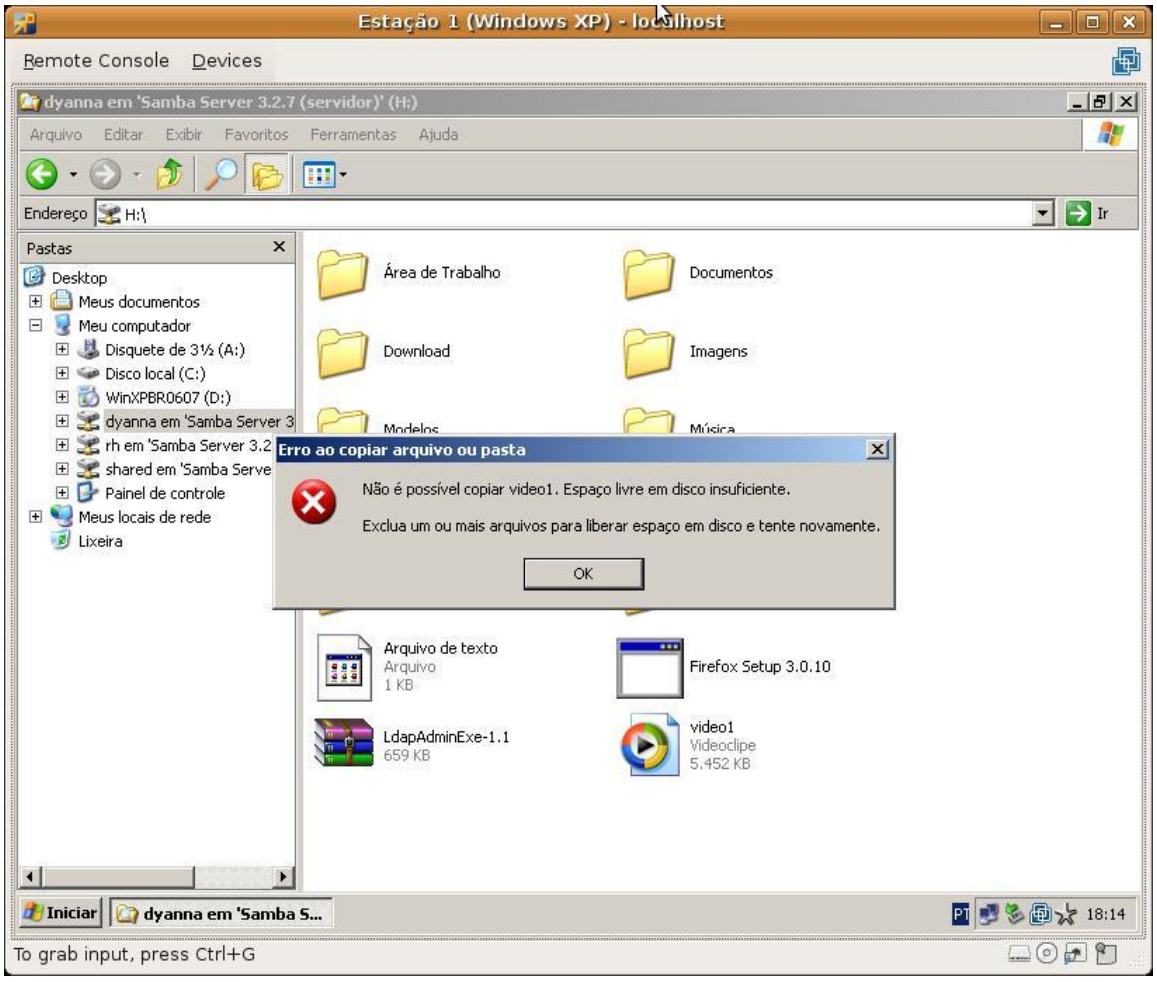


Figura 28: Erro cota de usuário no Windows

Outro teste de cota em disco realizado foi com o compartilhamento financeiro. Foi alocado um espaço de 10 MB para este diretório no servidor, conforme apresentado na figura 27. Ao tentar copiar um arquivo de tamanho superior para este diretório, apresenta a mensagem de erro da figura 29.

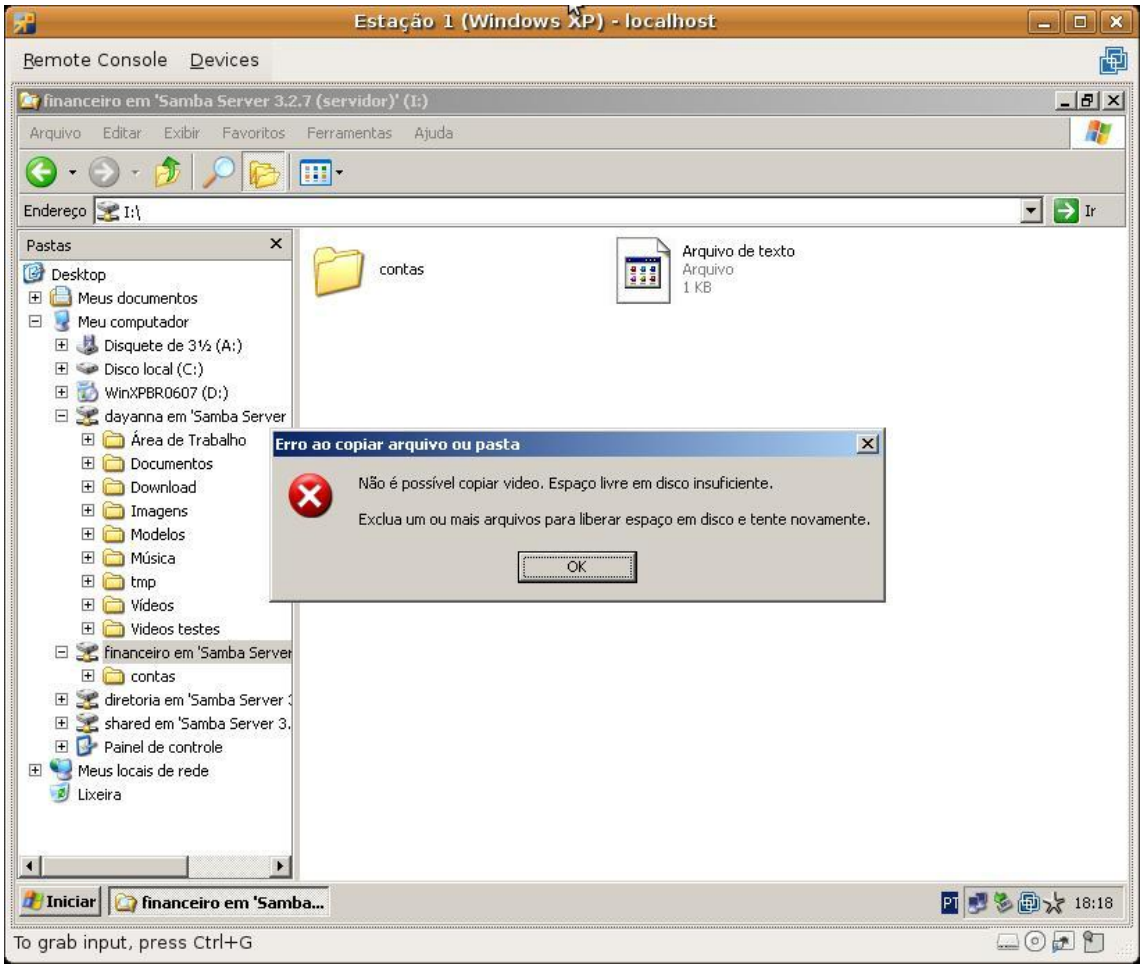


Figura 29: Erro cota de grupo no Windows

O acesso a internet pela estação cliente só poderá ser realizado caso as máquinas estejam configuradas para utilizar o Proxy implementado no servidor deste projeto. A figura 30 apresenta a configuração que foi realizada na estação.

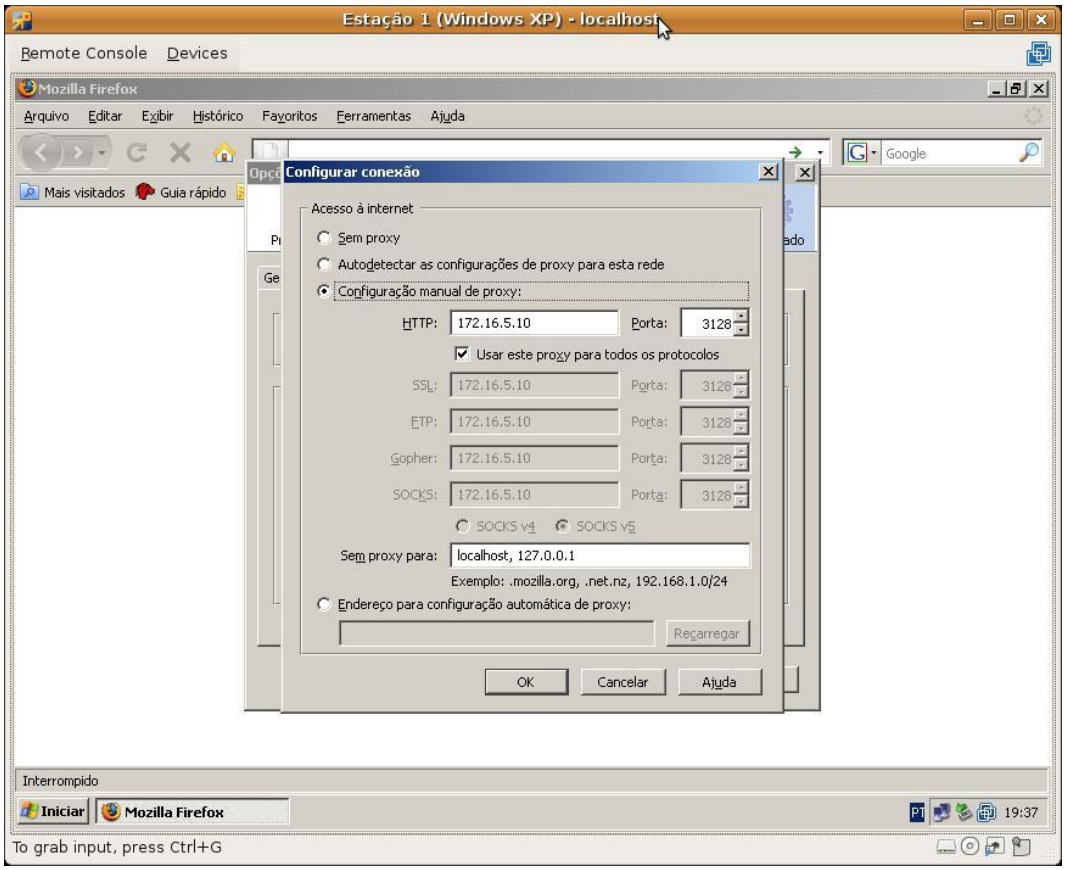


Figura 30: Configurando Proxy na estação Windows

Foram realizados testes de acesso a Internet com o login da usuária “dayanna” para verificar se o servidor Proxy está funcionando corretamente. De acordo com a política de acesso do Proxy, esta usuária só não pode acessar o endereço www.orkut.com.

A figura 31 mostra o servidor Proxy proibindo acesso do usuário ao sitio www.orkut.com, conforme o filtro configurado.

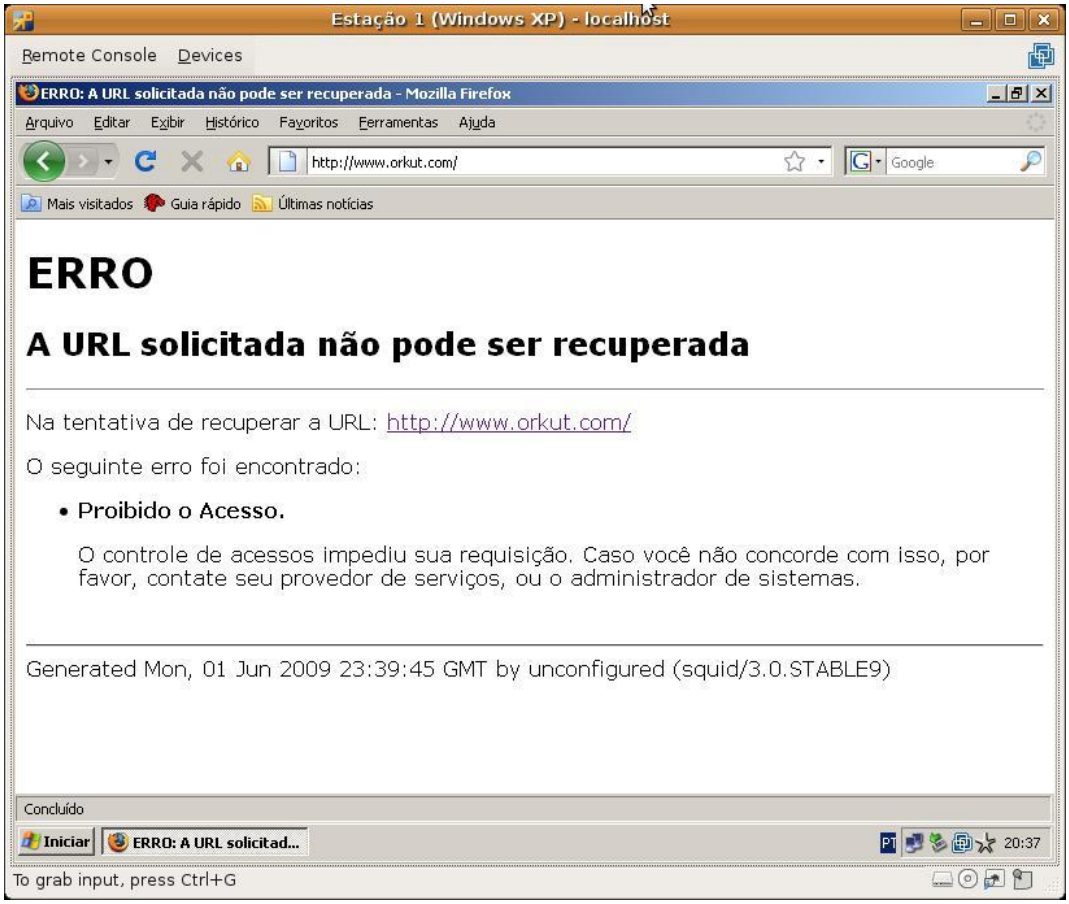


Figura 31: Proxy bloqueando acesso ao usuário dayanna

Já a figura 32 apresenta uma liberação de acesso do usuário ao endereço www.google.com.br de acordo com a política de acesso, configurada.

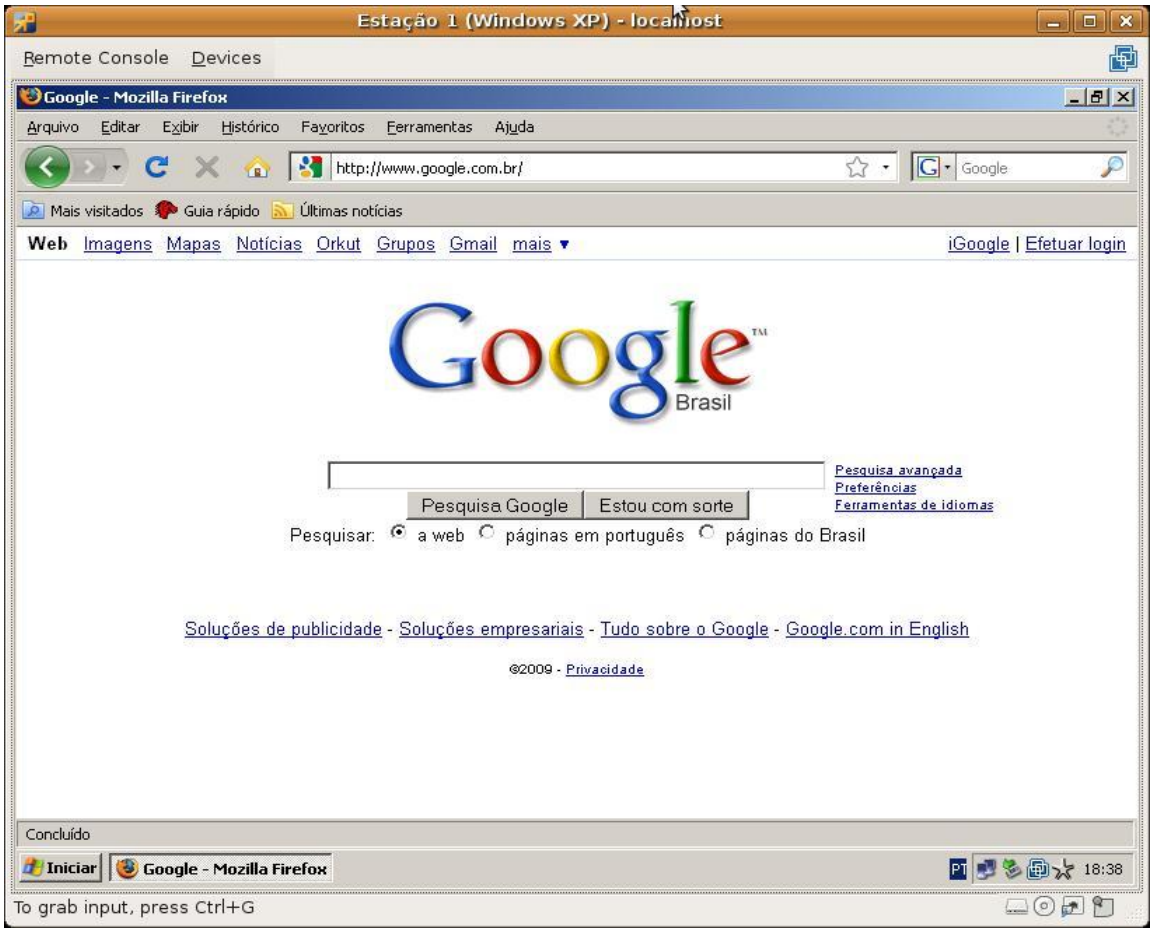


Figura 32: Acesso ao google através do Proxy

Outro teste realizado neste projeto foi verificar se a impressora compartilhada na rede estava disponível para a estação. Na figura 33 pode ser visualizada a impressora da rede disponível para a estação Windows.

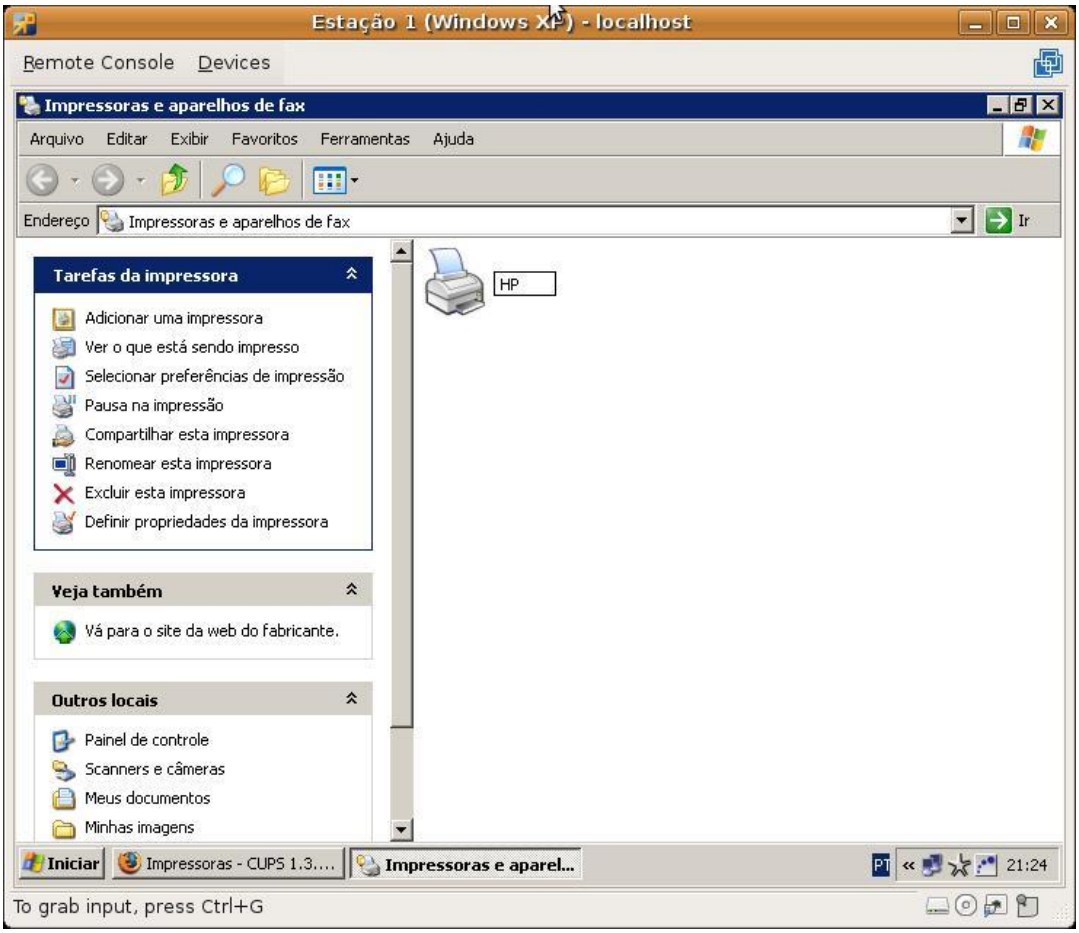


Figura 33: Impressora na estação Windows

Por fim, testamos se o software OCSng Inventory estava conseguindo emitir o relatório com o inventário da estação. As figuras 34 e 35 apresentam uma parte do relatório emitido pelo sistema com os dados referentes ao hardware e ao software da estação.

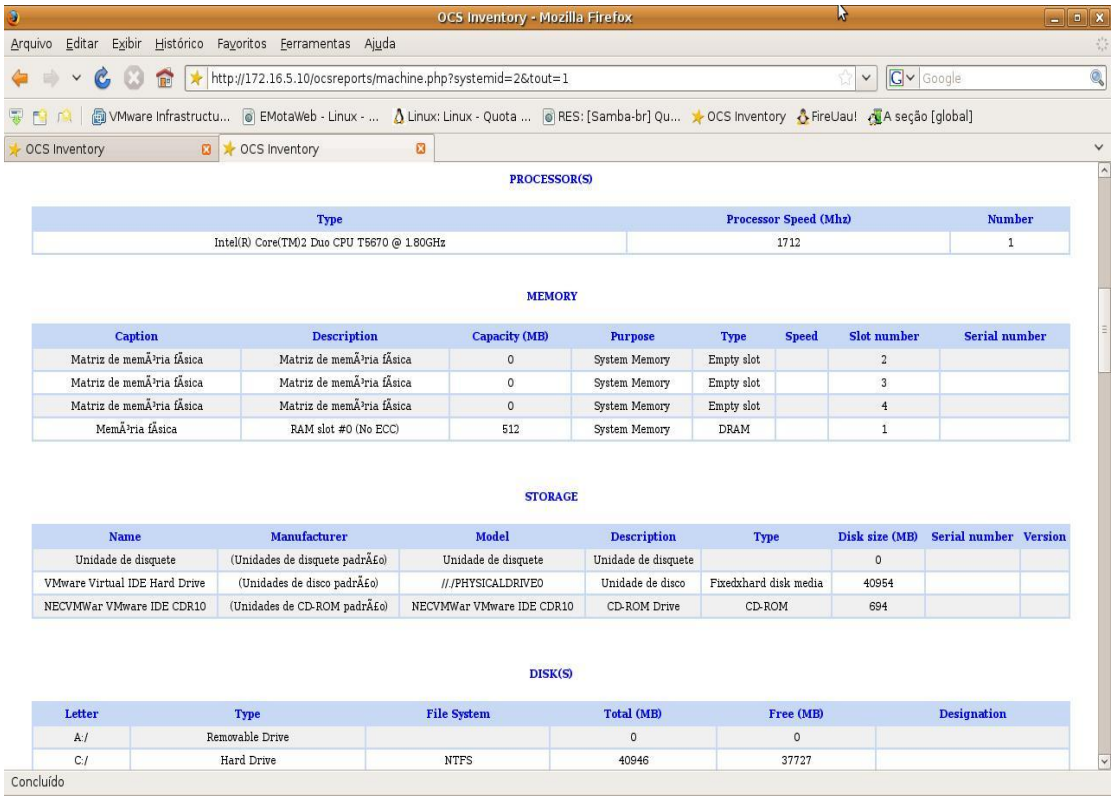


Figura 34: Inventário do hardware da estação Windows

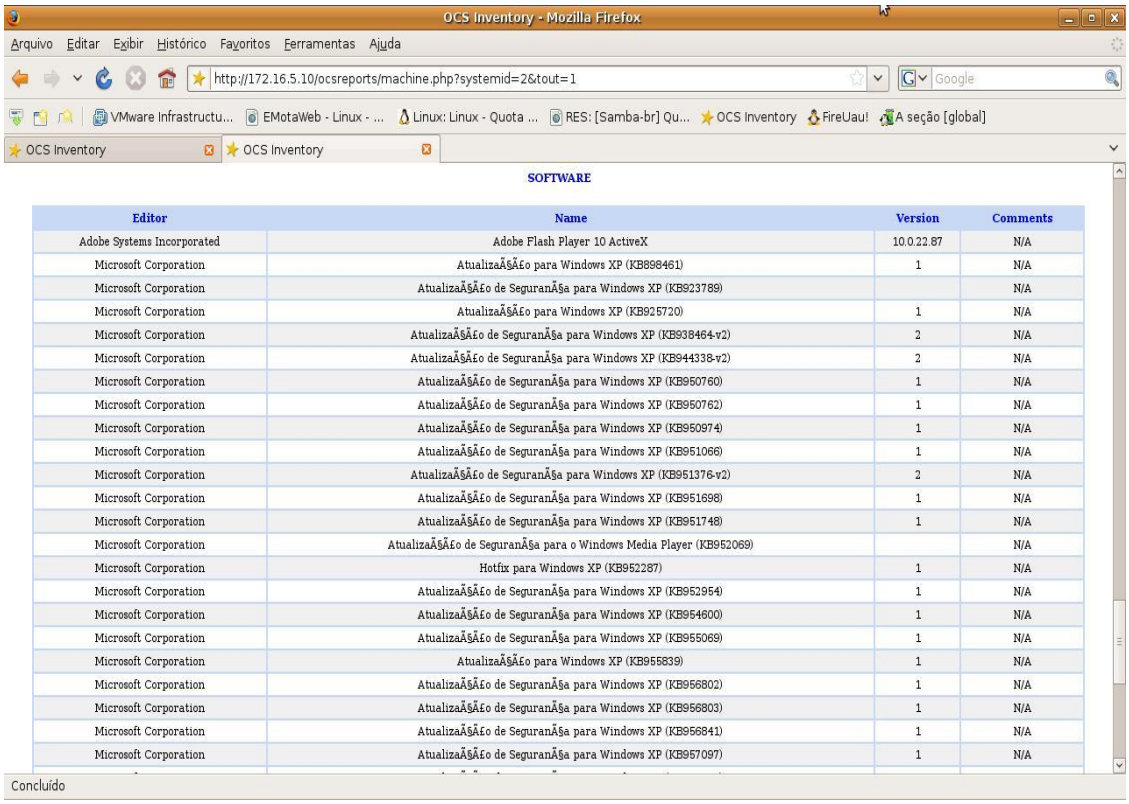


Figura 35: Inventário do software da estação Windows

5.1.2. Estação com o Sistema Operacional Linux

O primeiro teste realizado na estação Linux foi verificar se a máquina pegou um IP do servidor DHCP deste projeto. De acordo com a figura 36 a estação pegou o IP 172.16.5.250 Este endereço IP está dentro do intervalo configurado no servidor DHCP, conforme informado no cenário proposto.

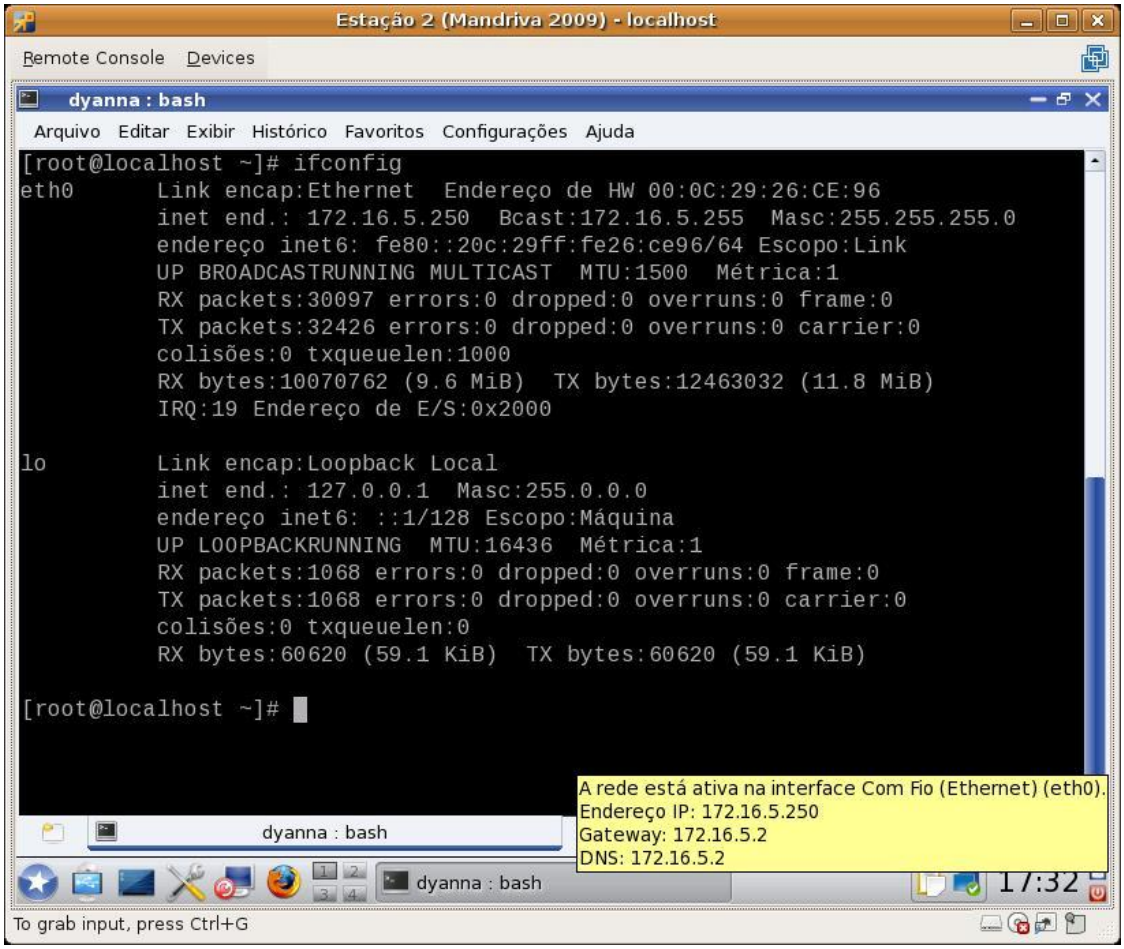


Figura 36: Estação Linux pegando IP via DHCP

Outro teste realizado foi verificar se os compartilhamentos foram mapeados nessa estação. Foi feito login na máquina com o. usuário “dayanna”. Este usuário faz parte do grupo “diretoria” e “financeiro”, portanto este usuário deve ter acesso os seguintes diretórios: diretoria, financeiro, diretório pessoal do usuário no servidor (/home/dayanna) e por fim o diretório shared que deve ser mapeado para todos os usuários da rede. Na figura 37 é possível visualizar os diretórios do servidor compartilhados em /media/shares.

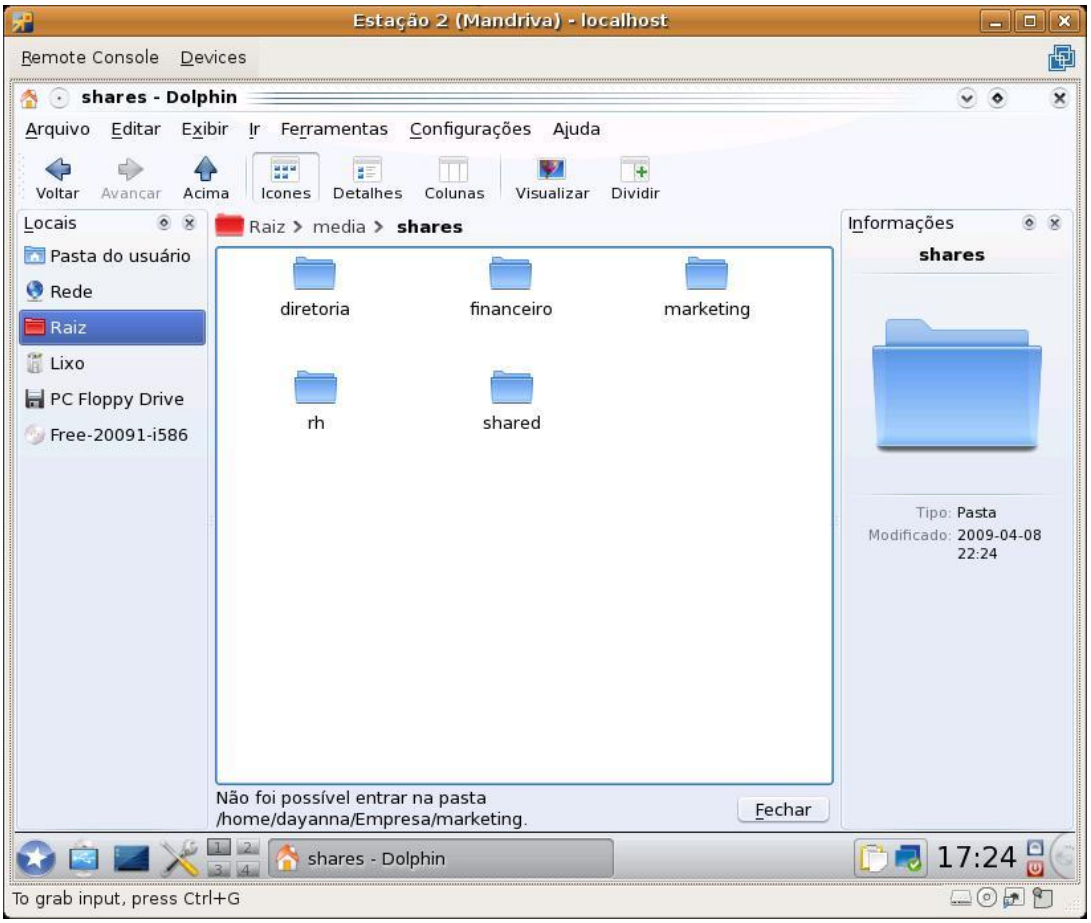


Figura 37: Acesso ao diretório /media/shares

Já na figura 38, pode ser verificado que o link Empresa de acesso ao diretório /media/shares foi criado quando o usuário logou na máquina.

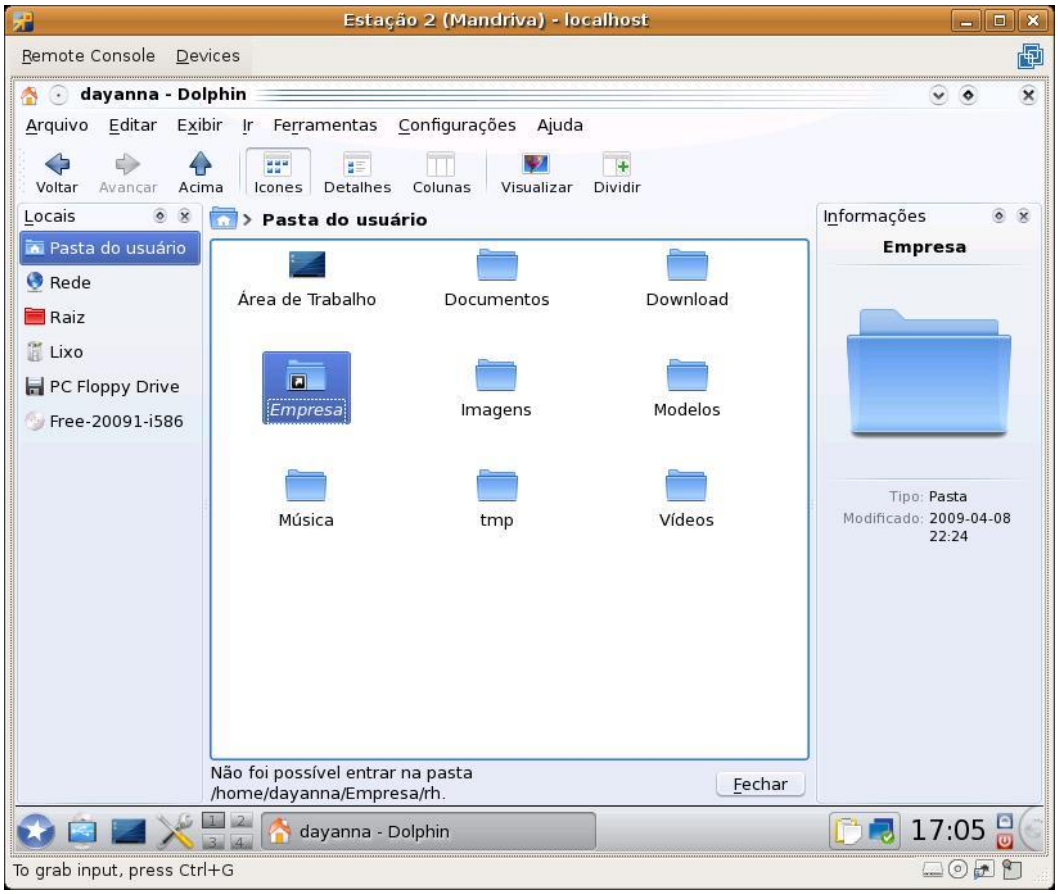


Figura 38: Link Empresa mapeado na pasta pessoal do usuário

Acessando o diretório Empresa, é verificado que os diretórios compartilhados no servidor estão disponíveis para o usuário, conforme figura 39.

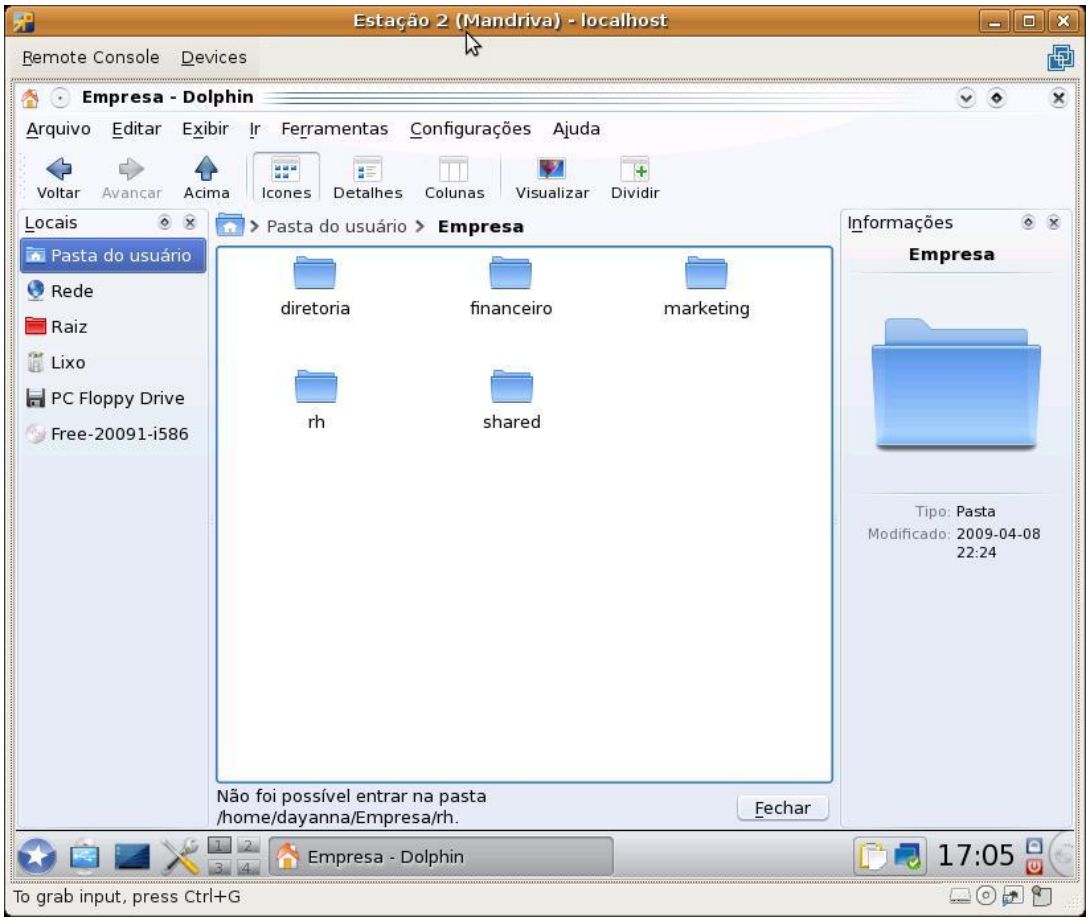


Figura 39: Compartilhamentos do Servidor mapeados na estação Linux

Caso o usuário tente realizar acesso a um diretório que não tenham permissão de acesso é exibida a mensagem “Não foi possível entrar na pasta /home/dayanna/Empresa/marketing”, conforme apresentada na figura 40.

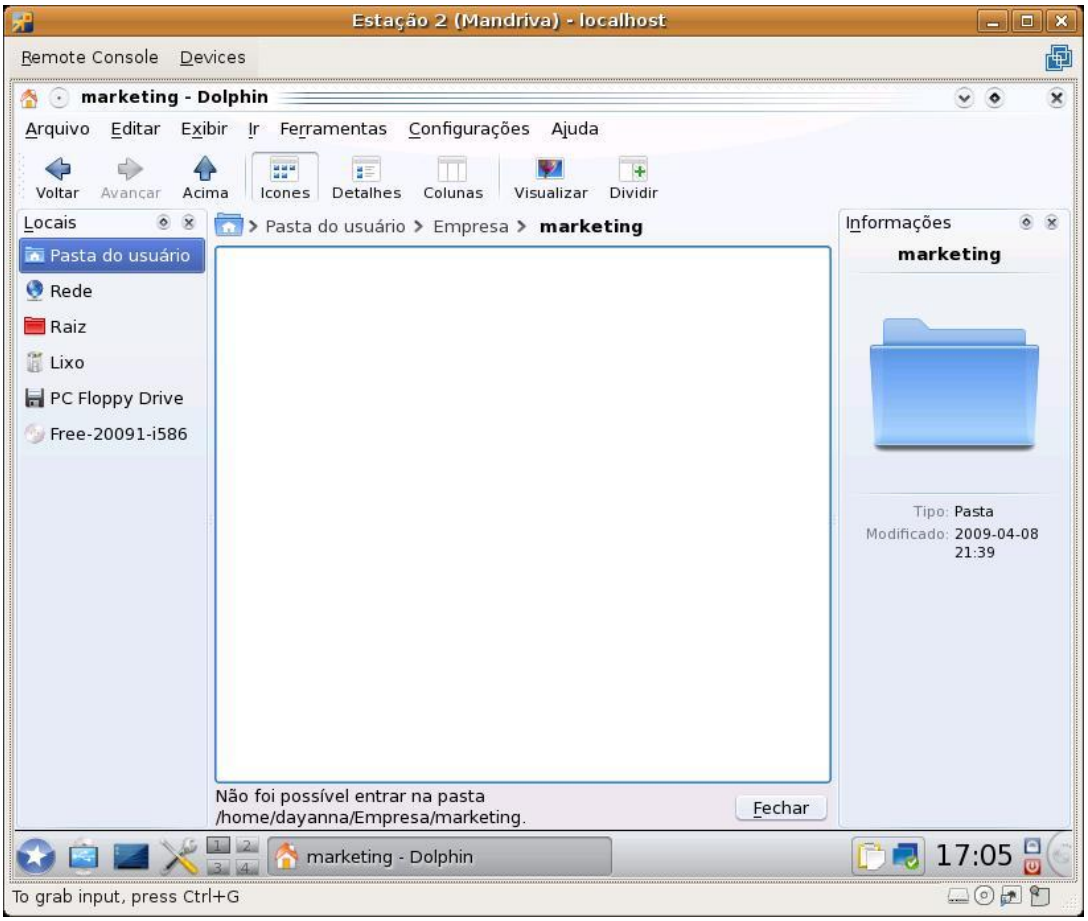


Figura 40: Negando acesso a diretório compartilhado no Linux

A usuária “dyanna” possa utilizar 10 MB de espaço em disco. Foi realizado uma tentativa de copiar arquivos maiores de 10 MB para o diretório pessoal da usuária também na máquina com Linux. Na figura 41 pode ser visualizada a mensagem de erro apresentada ao copiar um arquivo com tamanho superior ao espaço alocado para esta usuária.

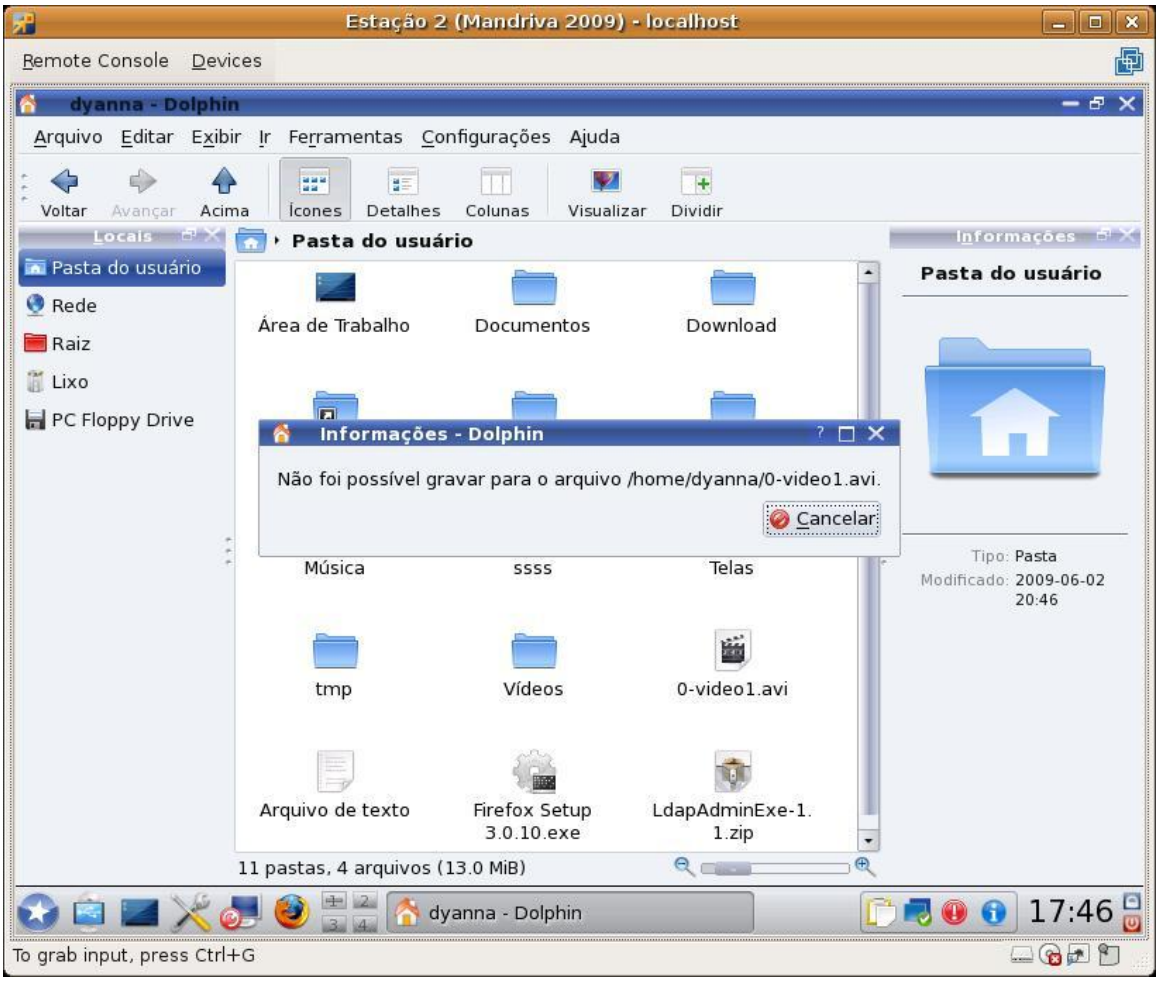


Figura 41: Erro de cota para usuário no Linux

Outro teste de cota em disco realizado na estação linux foi com o compartilhamento financeiro. Foi alocado um espaço de 10 MB para este diretório no servidor. Ao tentar copiar um arquivo de tamanho superior para este diretório, apresenta a mensagem de erro da figura 42.

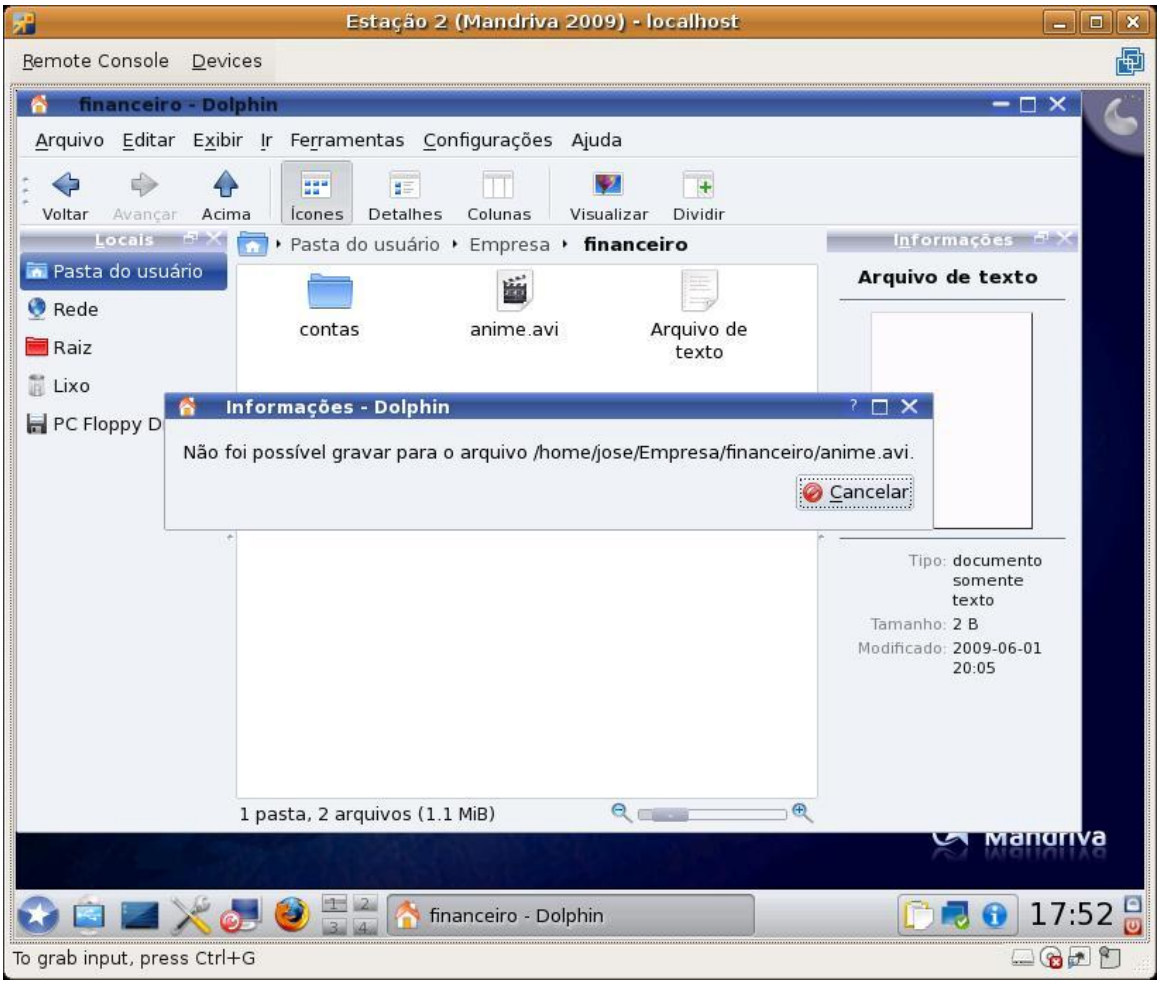


Figura 42: Erro de cota para grupo no Linux

A estação foi configurada para utilizar o servidor Proxy do projeto. A figura 43 apresenta a configuração realizada.

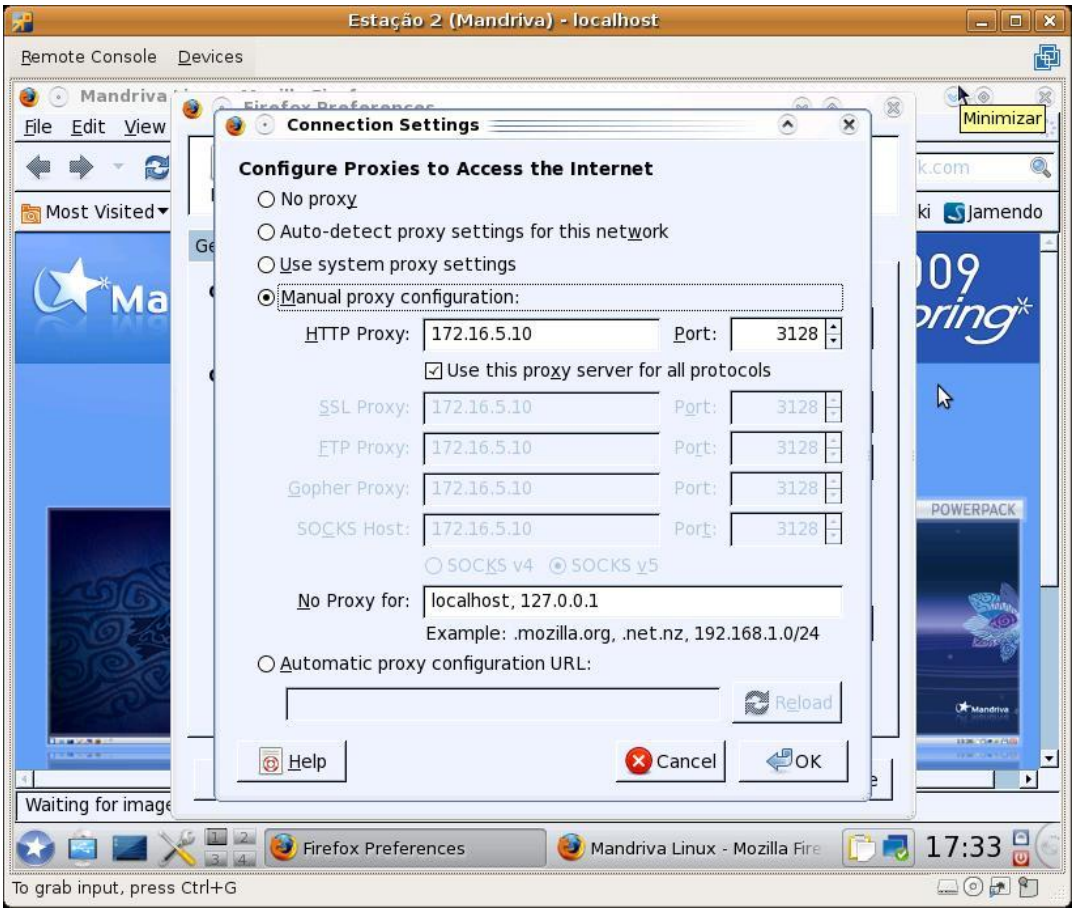


Figura 43: Configurando Proxy na estação Linux

Foram realizados testes de acesso a Internet com o login do usuário “jose” para verificar se o servidor Proxy está funcionando corretamente. De acordo com a política de acesso do Proxy, este usuário só pode acessar os endereços www.bancobrasil.com.br; www.bb.com.br e www.itau.com.br.

A figura 44 mostra o servidor Proxy proibindo acesso do usuário ao sitio www.google.com.br, conforme o filtro configurado.

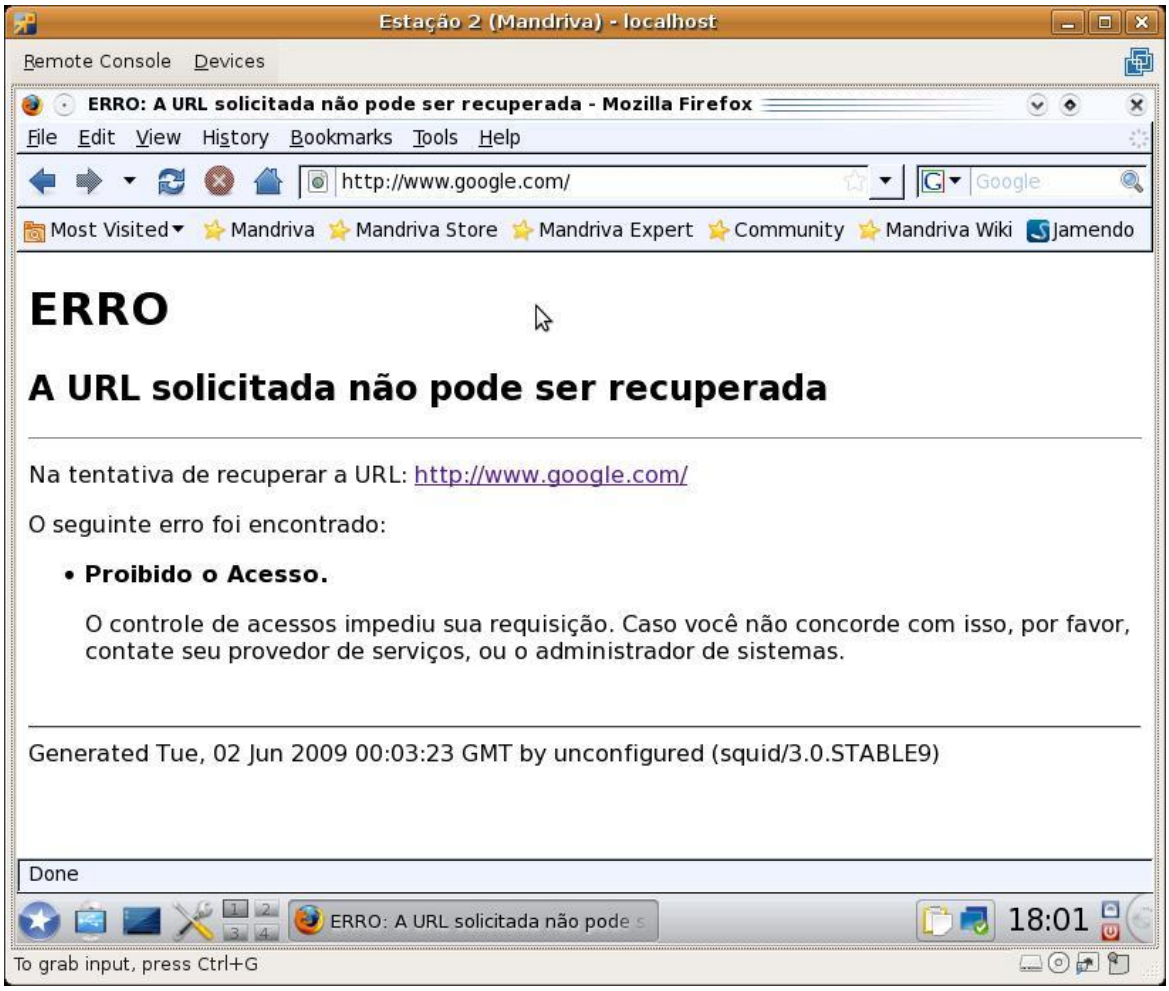


Figura 44: Servidor Proxy proibindo acesso do usuário Jose

Já a figura 45 apresenta o usuário acessando o endereço www.bb.com.br conforme permitido em sua política de acesso no servidor Proxy.

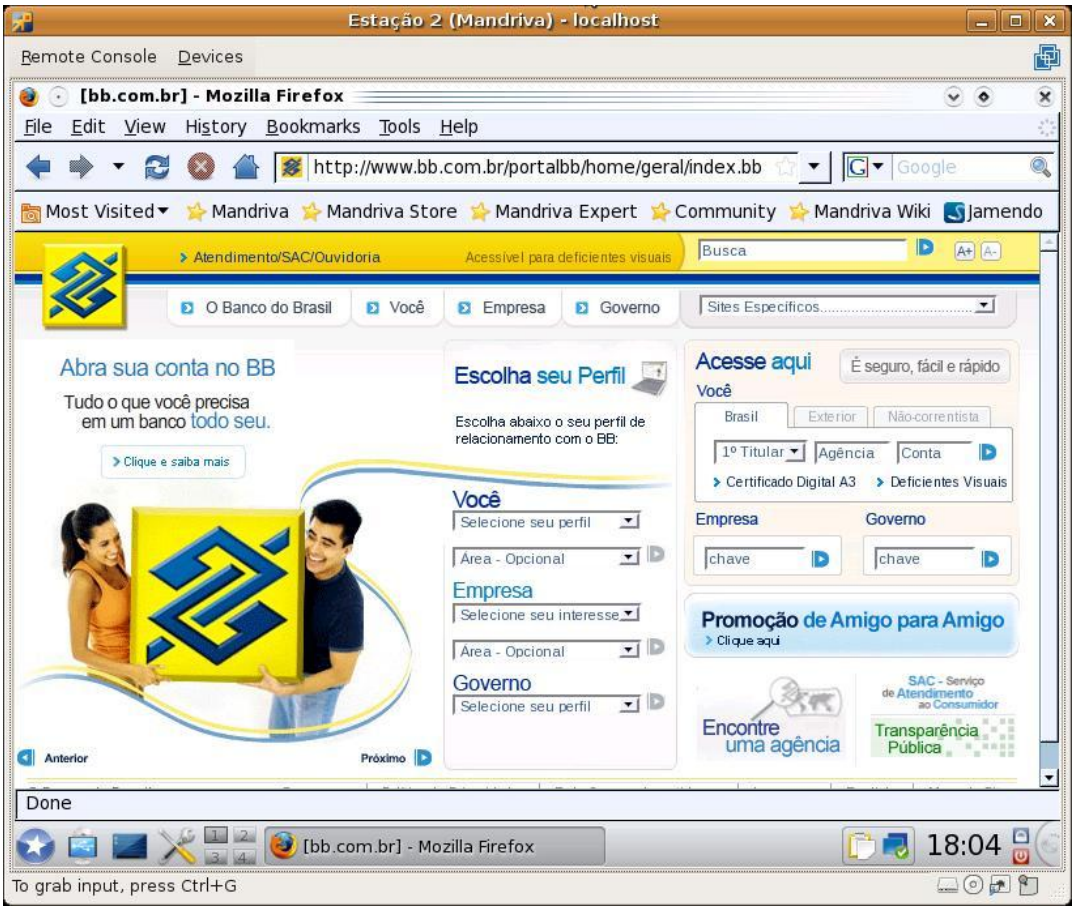


Figura 45: Servidor Proxy liberando acesso ao usuário Jose

Outro teste realizado neste projeto foi verificar se a impressora da rede estava compartilhada. Na figura 46 pode ser visualizada a impressora compartilhada para a estação Linux.

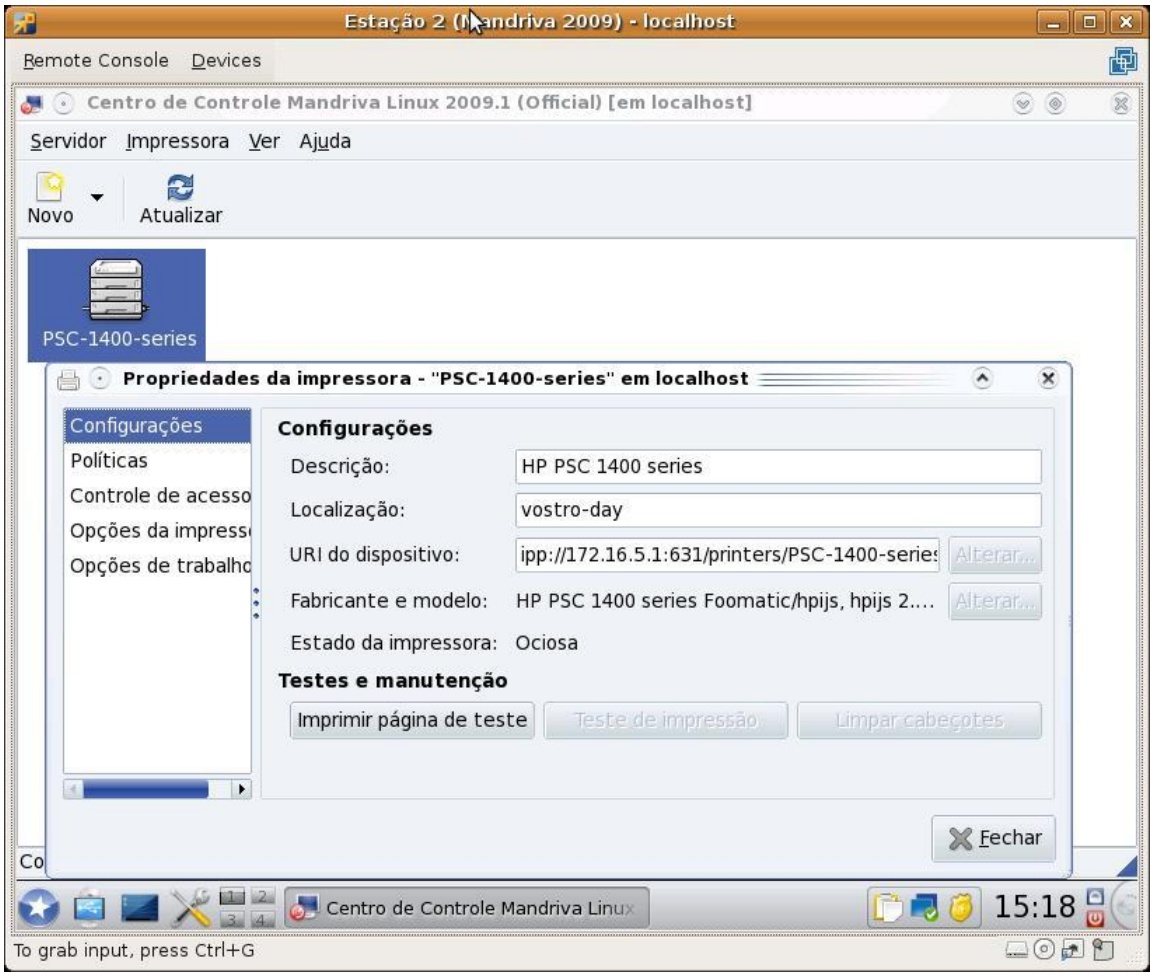


Figura 46: Impressora na estação Linux

Por fim, testamos se o software OCSng Inventory estava conseguindo emitir o relatório com o inventário da estação. As figuras 47 e 48 apresentam uma parte do relatório emitido pelo sistema com os dados referentes ao hardware e ao software da estação linux.

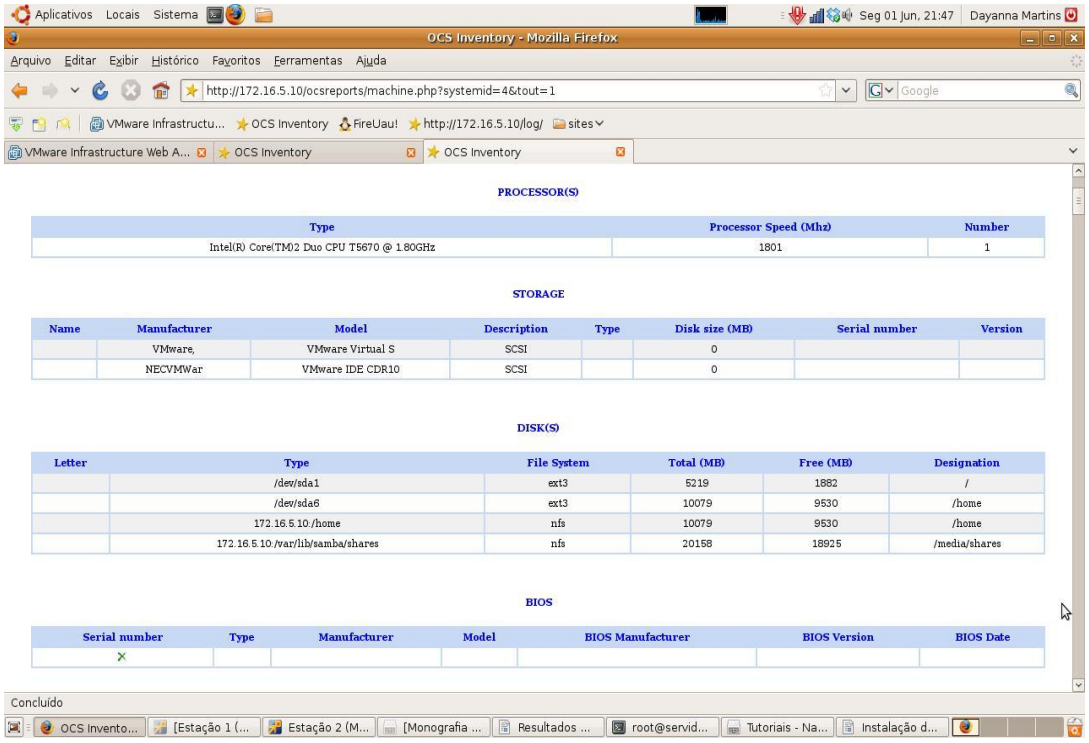


Figura 47: Inventário de hardware da estação Linux

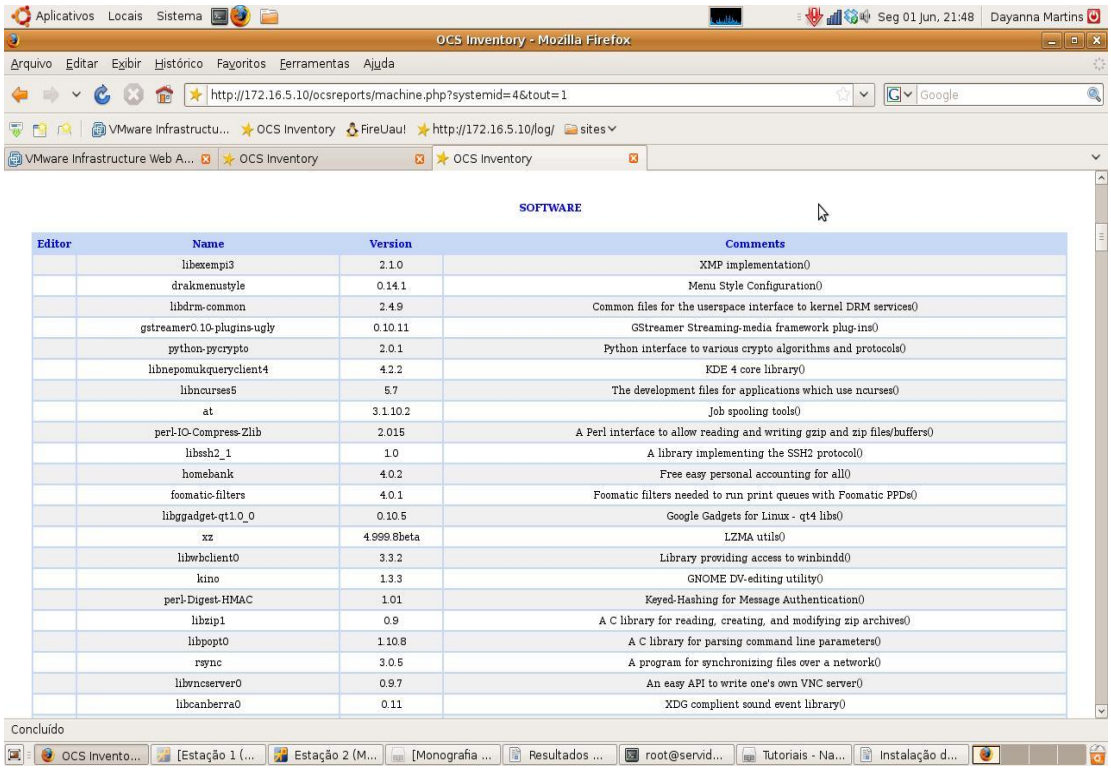


Figura 48: Inventário de software da estação Linux

5.2. Funcionalidades obtidas

Este projeto disponibilizou os principais serviços utilizados na intranet das empresas como controlador de domínio, compartilhamento de arquivos e impressão, controle de acesso a Internet, inventário do hardware e software das estações clientes.

Conforme proposto, é um sistema alternativo ao Windows 2003 Server com os principais serviços de intranet, servindo como uma solução para pequenas empresas. Serão apresentados alguns dados comparativos entre os dois sistemas para que essas empresas possam analisar se a escolha pelo sistema proposto é viável.

No sistema proposto pode ser encontrada grande parte dos serviços existentes na lista de funções do Windows 2003 Server conforme apresentado na tabela 3.

Tabela 3: Comparando o Sistema Proposto com o Windows 2003 Server

Serviços	Servidor	
	Windows 2003 Server	Sistema Proposto
Servidor de arquivos	Sim	Sim
Servidor de impressão	Sim	Sim
Servidor de web	Sim	Sim
Servidor de e-mail	Sim	Não
Servidor de acesso remoto	Sim	Não
VPN	Sim	Não
Controlador de domínio	Sim	Sim
Servidor DNS	Sim	Não
Servidor DHCP	Sim	Sim
Servidor de fluxo de mídia	Sim	Não
Servidor WINS	Sim	Sim
Servidor Proxy	Não	Sim
Inventário de Hardware e Software	Não	Sim

O sistema proposto não possui *Active Directory*, porém grande parte dos serviços pode ser feitos através do Samba como, o servidor de arquivos e o controlador de domínio deste projeto. Quando for lançado o Samba 4, ficará mais fácil realizar as configurações da rede interna, pois o mesmo terá um sistema que funcionará como o AD. O controle de impressões é feito pelo CUPS e as impressoras são compartilhadas na rede através do Samba. Foi criado também um servidor web para que o FireUau e o OCSng Inventory fossem gerenciados via browser.

A grande limitação do sistema proposto é não possuir objetos de políticas de grupo, mais conhecido como GPO (Group Policy Object), como o Windows 2003 Server. As GPO's permitem a configuração de diretivas de grupos, como por exemplo, configuração automática do Proxy, programas que estará disponíveis, os atalhos do menu iniciar que estarão disponíveis, configurações de rede e assim por diante. Para que o sistema proposto pudesse trabalhar com essas políticas, seria necessário criar scripts de logins com todas as políticas para os usuários da rede.

Existem alguns serviços que o Windows 2003 Server disponibiliza e que não foram desenvolvidos para este sistema proposto como servidor de e-mail, servidor de acesso remoto, servidor DNS, servidor de fluxo de mídia e Virtual Private Network[6] (VPN), pois não fazem parte do escopo do projeto. Para esses serviços citados, existem softwares livres com a mesma função. O servidor DNS pode ser criado através do Bind. Já o servidor de fluxo de mídia no pode ser disponibilizado no Linux através do software icecast. Por fim, o Virtual Private Network pode ser criado através do OpenVPN.

O sistema proposto disponibiliza alguns serviços extras como controle do inventário de hardware e software das máquinas através do software OCSng Inventory e servidor Proxy através do software Squid.

Ao adquirir a licença do Windows 2003 Server, o servidor Proxy não vem em sua lista de funções. Para que o servidor Windows administre também um servidor

[6] Disponível em: <http://www.novateceditora.com.br/livros/vpn/>. Acessado em 25 de maio de 2009.

Proxy, é necessário adquirir o Microsoft ISA Server, aumentando assim o custo com licenciamento.

São poucos os serviços que o sistema proposto não possui. Dessa forma, é possível atender a pequenas empresas sem ter que se preocupar com o custo das licenças de software.

6. CONCLUSÃO

Este projeto demonstra a possibilidade de um servidor com o sistema operacional GNU/Linux trabalhar e administrar uma rede com máquinas que utilizam sistemas operacionais distintos. O produto final pode ser utilizado por pequenas empresas que estão começando no mercado de trabalho e não tem condições de adquirir vários servidores e licenças de softwares.

O servidor apresentado neste projeto fornece os principais serviços disponíveis em uma intranet como controlador de domínio, servidor de arquivos, impressão, Proxy e DHCP, além de controlar todo o inventário das máquinas da rede. Portanto, esse ambiente fornece as funcionalidades básicas para os clientes Microsoft Windows e GNU/Linux, como gerenciamento de arquivos, contas, impressão, perfis e inclusive o controle de acesso à Internet.

A implementação deste projeto proposto apresentou diversos obstáculos. Uma das primeiras dificuldades encontradas foi encontrar uma ferramenta que criasse automaticamente os scripts de inicialização dos usuários. Foi encontrado o Ntlogon, que é o sistema responsável por criar esses scripts. A extensão desses arquivos é a .bat. Para todos os usuários é gerado um arquivo e esses são responsáveis por guardar informações de login dos usuários como, por exemplo, diretórios compartilhados que os usuários têm acesso, papel de parede que o usuários utilizar, entre outras.

Outro desafio desse projeto foi encontrar um software que integrasse com o Squid e que fosse de fácil manipulação para o administrador da rede. O software encontrado e que se encaixou nesse perfil foi o FireUau. Com ele, podemos definir todas as configurações necessárias para o Proxy de uma empresa em um ambiente com interface web e de fácil utilização. O próprio sistema se encarrega de escrever essas informações no arquivo de configuração do Squid e de guardar as informações passadas no banco de dados.

Apesar de o sistema proposto ter se apresentado como uma solução estável existe algumas limitações. Esse sistema não possui objetos de políticas de grupo, mais conhecido como GPO (Group Policy Object), como o Windows 2003 Server.

O projeto em questão possui os principais serviços de uma intranet, onde o foco são as pequenas empresas. Existem diversas melhorias que podem ser realizadas nesse sistema. Algumas dessas melhorias estão descritas abaixo como sugestões para futuras pesquisas:

- Utilizar um banco de dados para armazenar e centralizar as informações no lugar do LDAP;

- Aplicar critérios de segurança em todos os serviços apresentados nessa solução;

- Realizar testes de desempenho entre o sistema proposto e o Windows 2003 Server.

- Criar scripts que simule o funcionamento das GPO’s do Windows 2003 Server, além de acrescentar alguns serviços como o servidor DNS e VPN.

REFERÊNCIAS BIBLIOGRÁFICAS

BATTISTI, Júlio. **WINDOWS SERVER 2003 Curso Completo**. Rio de Janeiro: Editora Axcel, 2003.

DISTROWATCH. **Mandriva**. Disponível em: < http://distrowatch.com/?newsid=05369>. Acesso em 18 mar. 2009.

FERREIRA, Rubem E. **Linux: Guia do Administrador do Sistema**. São Paulo: Novatec Editora, 2003.

FILHO, João Eriberto Mota. **Descobrindo o Linux**. São Paulo: Novatec Editora, 2006.

HP. **O que é virtualização e o que ela pode fazer pela minha empresa?** Disponível em: <http://www.hp.com/latam/br/pyme/solucoes/apr_solucoes_01.html>. Acesso em 10 mar. 2009.

IDG NOW. Base instalada de Windows e Unix cresce em servidores no Brasil. Disponível em: <http://idgnow.uol.com.br/computacao_corporativa/2007/06/04/idgnoticia.2007-06-04.2314887372/>. Acesso em 15 jun. 2009.

INFOR WESTER. **Endereços IP**. Disponível em: <http://www.infowester.com/internetprotocol.php>. Acesso em 06 maio 2009.

LDAP. **Artigos sobre OpenLDAP**. Disponível em: < http://www.ldap.org.br/handler.php?module=ldap&action=view&sys_date=&dbname=ldap&section=4 >. Acesso em 23 mar. 2009.

LINUX MAGAZINE. **PCs com Software Livre cresceram 5,4% no Brasil**. Disponível em: <http://linuxmagazine.uol.com.br/noticia/1528>. Acesso em 09 mar. 2009.

MICROSOFT TECHNET. **TechCenter de Virtualização**. Disponível em: < http://technet.microsoft.com/pt-br/virtualization/default.aspx>. Acesso em 10 mar. 2009.

MICROSOFT. **A Promessa da Virtualização**. Disponível em: <http://www.microsoft.com/brasil/servidores/virtualizacao/promise.mspx>. Acesso em 10 mar. 2009.

MICROSOFT. **Escritórios Remotos**. Disponível em: < http://www.microsoft.com/brasil/servidores/virtualizacao/solution-issue-remote.mspx>. Acesso em 10 mar. 2009.

MUNIZ, David Barbosa. Trabalho de conclusão do Curso de Ciência da Computação da Universidade Federal da Bahia. **Estudo Comparativo de Aplicativos de Gerenciamento de Segurança da Informação para Conformidade com as Normas ISSO/IEC 17799 e ISO/IEC 27001**. Salvador 2007. Orientador Prof. Pablo Vieira Florentino.

NORTON, Peter; GRIFFITH, Arthur. **Guia Completo do Linux**. São Paulo: Editora Berkeley, 2000.

OLIVEIRA, Jefferson Martins de. Trabalho de conclusão do Curso de Sistemas de Informação da Universidade do Estado de Minas Gerais. **Linux como Alternativa de Sistema Operacional para Desktops**. Frutal 2008. Orientador Prof. Sérgio Carlos Portari Júnior.

OPEN IT, **Projeto de documentação do FreeBSD**. Disponível em: <http://www.openit.com.br/freebsd-hb/network-nfs.html>. Acessado em 01 jun 2009.

RODRIGUES, Leonardo Vítor Chaves. Trabalho de conclusão do Curso de Engenharia de Computação do Centro Universitário de Brasília. **Implementação de um Modelo de Ambiente Computacional Seguro para Gerenciamento de Clientes Microsoft**. Brasília 2008. Orientador Prof. Marco Antônio Araújo.

SARG, **Squid Analysis Report Generator**. Disponível em: <http://Sarg.sourceforge.net>. Acessado em 29 maio 2009.

SILBERCHATZ, Avi; GALVIN, Peter Baer; GAGNE, Greg. **Sistemas Operacionais com Java**. Rio de Janeiro: Editora Campus, 2004.

SILVA, Gleydson Mazioli da. **Samba**. Disponível em: <http://focalinux.cipsga.org.br/index.html>. Acesso em 14 mar. 2009.

SOARES, Luiz Fernando Gomes; LEMOS, Guido; COLCHER, Sérgio. **Redes de Computadores das LANs, MANs e WANs às redes ATM**. Rio de Janeiro: Editora Campus, 1995.

SQUID-CACHE. **Uso e Configuração do Squid**. Disponível em: <http://www.Squid-cache.org.br/index.php?option=com_content&task=view&id=81&Itemid=27>. . Acesso em 16 mar. 2009.

VASCONCELOS, **Laércio e Marcelo. Manual Prático de REDES**. Rio de Janeiro, 2006.

VIETNAM NET, **Vietnam to widely use open source software**. Disponível em: <http://english.vietnamnet.vn/tech/2009/01/822425/>. Acesso em 23 mar. 2009.

APÊNDICES

APÊNDICE A - ARQUIVO DE CONFIGURAÇÃO DO SERVIDOR DHCP

/etc/dhcpd.conf:

```
ddns-update-style none;
subnet 172.16.5.0 netmask 255.255.255.0 {
        option routers 172.16.5.2;
        option subnet-mask 255.255.255.0;
        option domain-name-servers 208.67.222.222;
        range dynamic-bootp 172.16.5.200 172.16.5.250;
        default-lease-time 21600;
        max-lease-time 43200;
        host windows {
                hardware ethernet 00:0c:29:9b:33:bc;
                fixed-address 172.16.5.150;
        }
}
```

APÊNDICE B - ARQUIVO DE CONFIGURAÇÃO DO FSTAB

/etc/fstab:

```
/dev/vg00/1 / xfs relatime 1 1
# Entry for /dev/sda1 :
UUID=e5c70804-62b7-4e37-ad2e-1c0481e6763a /boot xfs relatime 1 2
/dev/vg00/4 /home ext3 relatime,usrquota 1 2
/dev/cdrom /media/cdrom auto umask=0,users,iocharset=utf8,noauto,ro,exec 0 0
/dev/fd0 /media/floppy auto umask=0,users,iocharset=utf8,noauto,exec,flush 0 0
/dev/vg00/7 /mnt/backup xfs relatime 1 2
none /proc proc defaults 0 0
/dev/vg00/2 /tmp xfs relatime 1 2
/dev/vg00/3 /usr xfs relatime 1 2
/dev/vg00/5 /var xfs relatime 1 2
```

/dev/vg00/a /var/lib/Samba ext3 relatime,acl,user_xattr,grpquota 1 2
/dev/vg00/9 /var/lib/pgsql xfs relatime 1 2
/dev/vg00/8 /var/www xfs relatime 1 2
/dev/vg00/6 swap swap defaults 0 0

APÊNDICE C - ARQUIVO DE CONFIGURAÇÃO DO SAMBA

/etc/Samba/smb.conf:

```
[global]
workgroup = projeto
netbios name = servidor
load printers = yes
printing = cups

os level = 255
preferred master = Yes
domain master = Yes
local master = Yes
domain logons = Yes
wins support = Yes

passdb backend = ldapsam:ldap://127.0.0.1/
ldap admin dn = cn=Manager,dc=projeto,dc=com
ldap suffix = dc=projeto,dc=com
ldap group suffix = ou=Groups
ldap user suffix = ou=Users
ldap machine suffix = ou=Computers

[homes]
comment = Home Directories
browseable = no
writable = yes

[Profiles]
path = /var/lib/Samba/profiles
browseable = no
```

```
writable = yes

[printers]
comment = All Printers
path = /var/spool/Samba
browseable = yes
guest ok = yes
printable = yes

[diretoria]
comment = Pasta compartilhada da diretoria
path = /var/lib/Samba/shares/diretoria
valid users = @diretoria
public = no
writable = yes
create mask = 0660
directory mask = 0770

[financeiro]
comment = Pasta compartilhada da financeiro
path = /var/lib/Samba/shares/financeiro
valid users = @financeiro
public = no
writable = yes
create mask = 0660
directory mask = 0770

[marketing]
comment = Pasta compartilhada da marketing
path = /var/lib/Samba/shares/marketing
valid users = @marketing
public = no
writable = yes
create mask = 0660
directory mask = 0770

[rh]
```

```
comment = Pasta compartilhada da rh
path = /var/lib/Samba/shares/rh
valid users = @rh
public = no
writable = yes
create mask = 0660
directory mask = 0770

[shared]
comment = Pasta compartilhada da shared
path = /var/lib/Samba/shares/shared
public = no
writable = yes
create mask = 0660
directory mask = 0770
map acl inherit = yes
inherit acls = Yes
nt acl support = yes

[netlogon]
comment = Network Logon Service
path = /var/lib/Samba/netlogon
root preexec = /usr/local/Samba/bin/ntlogon --user='%u' --dir=/var/lib/Samba/netlogon/
```

APÊNDICE D - ARQUIVO DE CONFIGURAÇÃO DO NTLOGON

/etc/ntlogon.conf

```
[Global]
servername = servidor

@ECHO "Configurando rotinas iniciais..."
NET USE Z: /Del
NET USE I: /Del
NET USE J: /Del
NET USE K: /Del
```

```
NET USE L: /Del

net time \\%servername /set /Yes
net use Z: \\%servername\shared /YES

 [Group-financeiro]
@ECHO "Configurando mapeamentos.."
NET USE I: \\%servername\financeiro /yes
[Group-diretoria]
@ECHO "Configurando mapeamentos.."
NET USE J: \\%servername\diretoria /yes
[Group-marketing]
@ECHO "Configurando mapeamentos.."
NET USE K: \\%servername\marketing /yes
[Group-rh]
@ECHO "Configurando mapeamentos.."
NET USE L: \\%servername\rh /yes
# End configuration file
```

APÊNDICE E - ARQUIVO DE CONFIGURAÇÃO DO FIREUAU

/etc/sysconfig/FireUau/fwl.conf:

```
SERVER="172.16.5.10"
PORT_GETCONF="7002"
PORT_ACESSO="7003"
PORT_RELOAD="7004"
LOCK="/var/lock/fwl.lock"
#-------------------------------------------------------------
# se = 1 carrega as regras do iptables
IPTABLES=0
#-------------------------------------------------------------
# se = 1 carrega as regras do Squid
SQUID=1
```