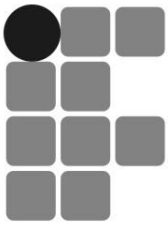


INSTITUTO FEDERAL DE
EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
FLUMINENSE
Campus Campos-Centro

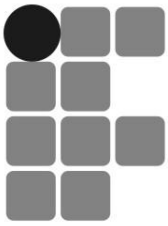
Secretaria de Educação
Profissional e Tecnológica

Ministério
da Educação

CURSO DE BACHARELADO SISTEMAS DE INFORMAÇÃO

SERVIDOR LINUX COM SAMBA - PDC (PRIMARY DOMAIN CONTROLLER). COMPARTILHAMENTO DE ARQUIVOS, IMPRESSORAS E CONTRALADOR DE DOMÍNIO EM MAQUINAS WINDOWS.

Campos dos Goytacazes/RJ
2012



INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA FLUMINENSE
Campus Campos-Centro

Secretaria de Educação Profissional e Tecnológica

Ministério da Educação

CURSO DE BACHARELADO SISTEMAS DE INFORMAÇÃO

SERVIDOR LINUX COM SAMBA - PDC (PRIMARY DOMAIN CONTROLLER). COMPARTILHAMENTO DE ARQUIVOS, IMPRESSORAS E CONTRALADOR DE DOMÍNIO EM MAQUINAS WINDOWS.

Trabalho de conclusão de curso apresentado ao Instituto Federal Fluminense como requisito parcial para conclusão do Curso de Bacharelado em Sistemas de Informação.

Orientador: Prof. Vinicius

Campos dos Goytacazes/RJ
2012

SERVIDOR LINUX COM SAMBA - PDC (PRIMARY DOMAIN CONTROLLER). COMPARTILHAMENTO DE ARQUIVOS, IMPRESSORAS E CONTRALADOR DE DOMÍNIO EM MAQUINAS WINDOWS.

Trabalho de conclusão de curso apresentado ao Instituto Federal Fluminense como requisito parcial para conclusão do Curso de Bacharelado de Sistema de Informação.

Aprovada em de Agosto de 2012

Banca avaliadora:

Prof. (Orientador)
Instituto Federal de Educação, Ciência e Tecnologia Fluminense

---

Prof.
Instituto Federal de Educação, Ciência e Tecnologia Fluminense

---

Prof.
Instituto Federal de Educação, Ciência e Tecnologia Fluminense

Aos meu amigos, professores e familiares ,

com amor. . .

AGRADECIMENTOS

Queremos agradecer a Deus, pois sem ele nada seria possível, nossas famílias que nos apoiam em todas decisões, nossos colegas de trabalho que sempre nos ajudam e ao IFF por nos proporcionar recursos financeiros e materiais para o desenvolvimento deste trabalho.

PDC.

Gabriel Rocha

RESUMO

PALAVRAS-CHAVE: Linux, Samba, PDC, Compartilhamento

ABSTRACT

KEYWORDS: Linux, Samba, PDC, Share

LISTA DE FIGURAS

SUMÁRIO

1 INTRODUÇÃO

1.1 Justificativa do trabalho

A implementação de um servidor de domínio no IFF – Campus Bom Jesus possibilitará um maior controle dos usuários que acessam o sistema, e assim será possível saber quem está logado no sistema, permitir ou bloquear o acesso à pastas e compartilhamentos pela rede, realizar a substituição mais fácil e ágil de equipamentos sem ter a necessidade do usuário ficar esperando a manutenção da máquina.

O servidor de impressão permite que todas as impressoras sejam mapeadas por setor possibilitando que mais de uma máquina possa imprimir no mesmo equipamento sem ter uma conexão física entre elas.

1.2 Objetivo

O foco deste trabalho é servir como base para estudo de servidores linux e implementar um serviço que busca melhorar o controle da rede no IFF – campus Bom Jesus, e também melhorar e proporcionar maior segurança digital e diminuir o tempo de manutenção dos incidentes.

1.3 Estrutura do trabalho

2 CONCEITOS E TÉCNICAS NECESSÁRIAS

O capitulo explica termos técnicos essenciais para o melhor entendimento do trabalho.

2.1 Samba

/* Samba é um software open source e reimplementa os protocolos SMB e CIFS para prover uma série de serviços para ambiente Windows, como servidor de arquivos e impressão e pode ser usado em um Servidor de Domínio como um Primary Domain Controller (PDC) ou como como um membro do domínio, e pode também ser usado como parte de um domínio Active Directory. */

Samba é um software open source que provê serviços a clientes nos protocolos SMB e CIFS. O samba permite a interoperabilidade entre servidores Linux/Unix e clientes baseados na plataforma Windows. O samba permite que um servidor linux seja apto a fornecer serviços como:

- **#Servidor de arquivos e impressão** Utilizando o protocolo Server Message Block para possibilitar o compartilhamento de arquivos, pastas volumes e impressoras na rede.
- **#Autenticação e autorização** Identifica um computador ou um usuário da rede e determina os direitos de acesso a arquivos que cada usuário possui, através de tecnologias como permissões de arquivos, diretivas de grupo e o serviço de autenticação Kerberos.
- **#Resolução e busca de nomes e diretórios** Compartilha as principais informações sobre computadores e usuários da rede através do Light Directory Access Protocol (LDAP) e o Microsoft Active Directory.
- **#Servidor de domínio como PDC** Funcionando como controlador de domínio ativo dentro de um domínio Windows.

2.2 Permissões no Linux

2.3 Permissões especiais no Linux

2.4 Seções

No Samba, as configurações de compartilhamentos, configurações de impressoras e todas as configurações gerais, são realizadas através de um unico arquivo de configuraçõa, o ”/etc/samba/smb.conf”. Esse arquivo para melhor organização, fica dividio em sessões, sendo a primeira sessão nomeada como [global], onde são definidas as configurações gerais do servidor. Também podem ser criadas sessões adicionais para cada compartilhamento, sendo nomeadas com o nome do mesmo. Se desejamos criar um compartilhamento com o nome ”arquivo”, a sessão que deve ser criada no arquivo de configuração deve ser [arquivo].

2.5 Parâmetro

2.6 Variáveis

2.7 Variáveis Especiais do Samba

2.8 PDC

2.9 Comandos Básicos do Samba3

2.10 SAMBA-TOOLS

2.11 SMBD

2.12 NMDB

2.13 NETBIOS

NETBIOS, Networking Basic Input/Outbut System, é uma API desenvolvida em 1984 pela IBM, que fornece serviços relacionados na camada de sessão do modelo OSI, permitindo a comunicação entre computadores na rede através de um nome NETBIOS correspondente a um hostname.

2.14 Domain Master

DOMAIN MASTER BROWSER Uma vez que o Local Master Browser é eleito no segmento de rede, uma consulta é feita ao servidor WINS para saber quem é o Domain Master Browser da rede para enviar a lista de compartilhamentos. A máquina escolhida como Local Master Browser envia pacotes para a porta UDP 138 do Domain Master e este responde pedindo a lista de todos os nomes de máquinas que o Local Master conhece e também o registra como Local Master para aquele segmento de rede.

2.15 Master Browser

2.16 WINS

2.17 BIND

2.18 Ldap

2.19 Kerberos

2.20 NTVFS

Sistema de arquivos que armazena os atributos do NTFS

2.21 GSSAPI

A GSSAPI é uma interface que permite desenvolvedores escreverem aplicações que aproveitam mecanismos de segurança tais como Kerberos, sem ter de programar explicitamente para qualquer mecanismo, ou seja, aplicações genéricas do ponto de vista de segurança. Programas que usam GSSAPI são, deste modo, altamente portáteis, não somente de uma plataforma para outra, mas de uma configuração de segurança a outra e de um protocolo de transporte a outro. A GSSAPI fornece vários níveis de proteção de dados, consistentes com os mecanismos de segurança subjacentes.

2.22 Referencias - Temporário

SAMBA: http://pt.wikipedia.org/wiki/Samba_(servidor)

http://en.wikipedia.org/wiki/Samba_(software)

http://www.samba.org/samba/docs/

http://www.samba.org/samba/what_is_samba.html

http://www.samba.org/samba/docs/SambaIntro.html

http://www.samba.org/cifs/docs/whatissmb.html

http://www.samba.org/cifs/

Using Samba (OREILLY)

NETBIOS:

http://pt.wikipedia.org/wiki/Netbios

Using Samba (OREILLY)

GSSAPI: http://www.gta.ufrj.br/grad/10_1/kerberos/gssapi.html

3 SAMBA 3

Este capítulo descreve como são feitas a instalação e a configuração de um servidor samba como controlador de domínio, servidor de impressão e servidor de dados, respeitando as regras de usuários e permissões.

3.1 Instalação do samba

O pacote samba pode ser instalado através do repositório de sistemas da distribuição em que está sendo usado (neste caso Ubuntu 11.04). Primeiro temos que atualizar a base de dados do repositório para que possamos instalar a versão mais atual do samba.

- **# apt-get update** - Atualiza a base de dados do repositório no Ubuntu.
- **# apt-get install samba** - Realiza a instalação do pacote samba.
- **# apt-get install smbclient** - Pacote que mostra as informações do servidor samba e permite acesso de compartilhamentos no windows ou linux a partir de uma máquina linux.

3.2 SWAT - Gerenciando o samba pelo browser

Com ele é possível compartilhar impressoras, arquivos, criar usuários, permitir ou restringir acessos, tudo em um ambiente gráfico.

- **# apt-get install swat** - Instala a ferramenta gráfica swat para o gerenciamento do samba.
- **$ firefox localhost:901** - Endereço de acesso no browser (neste caso o Firefox) para acessar o swat.

Informe o usuário root e sua senha. Como se pode ser na Figura 3.1

Na barra de ferramentas pode se observar as opções de configuração do swat. Da esquerda para direita vemos:

**FIGURA DO SWAT

- **Home** - Documentação do samba
- **Globals** - Variáveis globais de configuração do samba
- **Shares** - Ativar compartilhamentos de diretórios e arquivos
- **Printers** - Compartilhamento de impressoras
- **Wizard** - Escreve as modificações no arquivo smb.conf do samba
- **Status** - Status do servidor com usuário, compartilhamento dos ativos e arquivos abertos
- **View** - Mostra o arquivo smb.conf
- **Password** - Cadastrar o usuário, máquinas e mudar senha dos usuários no servidor

3.3 Iniciando Samba

Com todos os componentes instalados o servidor samba pode ser iniciado.

- **# /etc/init.d/smbd start** - Inicia o samba. Existem outras formas de inicia-lo, como:
  1. **# service smbd start** - Inicia o samba.
  2. **# service smbd stop** - Para o processo do samba.
  3. **# service smbd restart** - Finaliza o processo existente e cria outro para o samba.
  4. **# /etc/init.d/samba start** - Para iniciar o samba em computadores com Debian 6.
  5. **# /etc/init.d/samba restart** - Reiniciar no Debian 6.

3.4 Configuração do samba para ser um PDC

O arquivo de configuração se encontra no diretório /etc, onde está a maioria dos arquivos de configuração dos programas no linux.

- **# cp /etc/samba/smb.conf > /etc/samba/smb.conf.bkp** - Por motivo de segurança é recomendado fazer um backup do arquivo.
- **# gedit /etc/samba/smb.conf** - Para editar o arquivo e adicionar as seções, parâmetros e variáveis deve-se abrir o arquivo smb.conf.
- **# testparm -s /etc/samba/smb.conf.bkp > /etc/samba/smb.conf** - Removerá os comentário para melhor leitura do arquivo. Observação: o arquivo de origem não pode ser o smb.conf pois ele irá se rescrever e o arquivo só conterá a seção [global] vazia.

Agora é necessário inserir, modificar e remover alguns parâmetros na seção [global] para que o samba se comporte como um PDC.

[global]

workgroup = ”nome do servidor de domínio”

server string = ”Título”

security = user

netbios name = ”nome que será da netbios do servidor”

domain master = yes

domain logons = yes

enable privileges = yes

passdb backend = tdbsam

encrypt passwords = true

preferred master = yes

local master = yes

os level = 100

wins support = yes

map to guest = Bad User

panic action = /usr/share/samba/panic-action %d

Explicação das variáveis utilizadas:

- **workgroup** - Nome do servidor de domínio.
- **server string** - Descrição do servidor que aparece na barra de título das janelas do compartilhamento.
- **security** - Tipo de segurança do compartilhamento. Existem os tipos domain, user e share.
    1. share - É utilizado quando o compartilhamento será aberto, onde todos os usuários conectados serão guest e sem a necessidade de realizar login.
    2. user - Todos os usuários que tentarem se conectar terão que se identificar por meio de um login e uma senha.
    3. domain - Quando um servidor de domínio será responsável pela identificação e segurança dos usuários.

- **netbios name** - Nome da netbios do servidor.
- **encrypt passwords** - Quando informado a variável ”true”as senhas informadas para o servidor serão criptografadas.
- **domain master** - Informa que o servidor samba será o domínio principal da rede.
- **domain logons** - O servidor samba passa a ser um controlador de domínio.
- **enable privileges** - Habilita alguns privilégios no samba. Alguns deles:
    1. SeAddUsersPrivilege - Adicionar usuários e grupos no domínio
    2. SeDiskOperatorPrivilege - Gerencia os discos compartilhados
    3. SeMachineAccountPrivilege - Adicionar maquinas no domínio
    4. SePrintOperatorPrivilege - Gerencia as impressoras
- **passdb backend** - Aceita valores smbpasswd ou tdbsam . Define qual será a forma de armazenagem dos registros dos usuários.
    1. smbpasswd - Segundo (http://www.hardware.com.br/tutoriais/samba-configuracao-avancada/pagina8.html) O smbpasswd é o backend mais simples. Nele, as senhas são salvas no arquivo ”/etc/samba/smbpasswd”e são transmitidas de forma encriptada através da rede, com suporte ao sistema NTLM, usado pelas versões contemporâneas do Windows. A vantagem do smbpasswd é que ele é um sistema bastante simples. Embora encriptadas, as senhas são armazenadas em um arquivo de texto, com uma conta por linha.
    2. tdbsam - Segundo (http://www.hardware.com.br/tutoriais/samba-configuracao-avancada/pagina8 O tdbsam, que usa uma base de dados muito mais robusta, armazenada no arquivo ”/var/lib/samba/passdb.tdb”(é justamente este arquivo que o script executado durante a instalação do pacote ”samba”no Debian pergunta se deve ser criado).
    3. Diferença entre smbpasswd e tdbsam - Segundo (http://www.hardware.com.br/tutoriais/samba-configuracao-avancada/pagina8.html) O tdbsam oferece duas vantagens sobre o smbpasswd: oferece um melhor desempenho em servidores com um grande número de usuários cadastrados e oferece suporte ao armazenamento dos controles SAM estendidos usados pelas versões server do Windows. O uso do tdbsam é fortemente recomendável caso seu servidor tenha mais do que algumas dezenas de usuários cadastrados ou caso você pretenda usar seu servidor Samba como PDC da rede (veja mais detalhes a seguir). Ele é também um pré-requisito caso você precise migrar um domínio NT já existente para o servidor Samba.
- **local master** - Define se o servidor será o Master Browser.

- **os level** - Valor que será passado na eleição para definir o mestre da rede. O valor máximo é 100, assim vencendo os valores padrões de ”os level”o servidores windows.
- **win support** - Se nmbd será um servidor WINS.
- **map to guest** - Tornar usuário guest todos que não conseguirem se identificar com um login e senha valido.
- **panic action** - Comando que será executado caso o smbd ou nmbd pararem de funcionar.

Com todas as variáveis devidamente adicionadas o servidor samba precisa ser reiniciado para que todas as modificações entrem em vigor.

- **# testparm** - Verifica se existe algum erro de sintaxe no arquivos de configuração no smb.conf
- **# /etc/init.d/smbd restart** - Reinicia o samba.
- **# /etc/init.d/nmbd restart** - Reinicia o servidor de nomes do samba.

**FIGURA DA SAIDA DO TESTPARM

3.5 Cadastro de Usuário

Os usuários que terão acesso e permissões de login no domínio devem ser criados no servidor linux, onde se encontra o samba. Antes da criação dos usuários normais o usuário root tem que ser cadastrado no samba.

- **# smbpasswd -a root** - Uma senha terá que ser informada e precisa ser a mesma do usuário no sistema.

Cada usuário no sistema deverá conter uma pasta com o nome de ”profile.pds”. Essa pasta irá conter informações das sessões de logon que o usuário fez no servidor de domínio.

Para automatizar a criação dessa pasta no diretório home dos usuários, cria-se o diretório no /etc/skel.

- **# mkdir /etc/skel/profile.pds** - O /etc/skel armazena todos os diretórios e arquivos que serão criados juntos com o usuário no sistema.

Antes de cadastrá-los no samba eles precisam ser criados no sistema.

- **# adduser --disabled-login usuario** - Comando para a criação mais completa de usuário no linux com nome completo, telefone , sem a permissão de login e entre outros dados.

Após o usuário ser criado no sistema, ele necessita ser cadastrado no samba.

- **# smbpasswd -a usuario** - Informe a mesma senha cadastrada no linux.

3.6 Cadastro de Máquinas

Da mesma forma que os usuário têm que ser cadastrados no sistema, as máquinas que poderão entrar no domínio também devem ser cadastradas.

As máquinas são cadastradas como usuários normais no linux antes de serem cadastradas no samba, porém sem pasta home e sem bash para login.

- **# groupadd machine** - Cria o grupo no qual serão adicionadas as máquinas cadastradas para melhor organização dos usuários no linux.
- **# useradd --home /dev/null --shell /bin/false --group machine computador1$** - Comando para a criação da máquina no sistema linux. Por padrão se adiciona o $ no final do nome pois é dessa forma que o samba irá identificar que o usuário na verdade é uma maquina.
- **# passwd -l computador1$** - Desativa a mudança da senha para o usuário/máquina.

Após a criação do usuário/máquina no sistema agora ele tem que ser cadastrado no samba.

- **# smbpasswd -a -m computador1$** - Cadastra o usuário como uma máquina no samba.

3.7 Script de Cadastro de Usuários e Máquinas

Para facilitar a criação e exclusão dos usuários no sistema e no samba, foi feito um script. Com ele é possível criar usuários e máquinas, adicionar usuários em grupos e também excluí-los do sistema.

Script smbmanager.sh

#!/bin/bash

#Gabriel Rocha

```
end=0

help="É NECESSÁRIO TER PERMISSÃO DE ROOT \nUSO: smbmanager [OPCAO] [VALOR] \n \nOpções gerais:\n -g [VALOR] Grupo no qual será adicionado a máquina ou usuário \n -m [VALOR] Nome da máquina a ser cadastrada \n -u [VALOR] Usuário a ser cadastrado no sistema e no samba \n -d [VALOR] Usuário a ser deletado do sistema \n -x [VALOR] Máquina a ser deletada do samba e do sistema"

AddMachine()

if [ -n "$machine"] ; then

if [ -z "$group"] ; then

useradd --disabled-login --home /dev/null --shell /bin/false $machine\$ 2>/dev/null && passwd -l $machine\$ && smbpasswd -a -m $machine

fi

if [ -n "$group"]; then

useradd --disabled-login --home /dev/null --shell /bin/false --group $group $machine\$

check=$(echo $?)

if [ $check -eq 0 ]; then

passwd -l $machine\$ 2>/dev/null && smbpasswd -a -m $machine fi

fi

fi

AddUser()

if [ -n "$user"] ; then

if [ -z "$group"] ; then

adduser $user 2>/dev/null

smbpasswd -a $user

fi

if [ -n "$group"] ; then

adduser $user 2>/dev/null

usermod -g $user $group

check=$(echo $?)
```

```
if [ $check -eq 0 ]; then
smbpasswd -a $user
fi
fi
fi
DelMachine()
if [ -n ”$delmachine”]; then
smbpasswd -x -m $delmachine
deluser $delmachine\$
fi
DelUser()
if [ -n ”$deluser”]; then
smbpasswd -x $deluser
deluser $deluser
fi
while getopts ”hg:m:u:d:x:”paramentro;
do
case $paramentro in
 h) echo -e $help;;
 g) group=$OPTARG ;;
m) machine=$OPTARG ;;
u) user=$OPTARG ;;
d) deluser=$OPTARG ;;
x) delmachine=$OPTARG ;;
*) echo -e $help; end=1;;
esac
done
if [[ ”$group”= *’-’* ]] || [[ ”$machine”= *’-’* ]] || [[ ”$user”= *’-’* ]] || [[ ”$deluser”=
```

’-’]] || [[”$delmachine”= *’-’*]]; then

echo -e $help

else

if [$end -ne 1] ; then

AddMachine

AddUser

DelMachine

DelUser

fi

fi

**FIGURA DO SCRIPT RODANDO

O script tem que ter a permissão de root para que possa ser iniciado.

- **# chmod +x smbmanger.sh** - Adiciona a permissão de execução ao script.
- **# cp smbmanager.sh /usr/sbin/** - Transferindo o script para a pasta /usr/sbin/ o script poderá ser iniciado em qualquer caminho que o usuário esteja.

3.8 Migração dos Usuários Administradores e Users do Linux para o Windows

Para que o Windows possa reconhecer um grupo de usuários administradores do linux como Power Users e Domain Users deve se mapear os grupos pelo RID dos mesmos.

Primeiro é necessário saber qual o ID dos principais grupos do Windows.

*****TABELA RID WIKI SAMBA*******

RID (Relative Identifier)

Domain Admins RID=512

Domain Users RID=513

Domain Guests RID=514

1. **# net groupmap list** - Liste os grupos existentes mapeados, caso não tenha o grupo siga o passo 2.

2. **# net groupmap add ntgroup=”Domain Admins”rid=512 unixgroup=admin** - Irá mapear o grupo admin para o grupo Domain Admins do windows.
3. **# net groupmap add ntgroup=”Domain Users”rid=513 unixgroup=users** - Mapea o grupo users com o Domain Users do windows.

- **# net groupmap delete ntgroup=”Domain Admins”** - Caso queira remover um mapeamento de grupo.
- **# net groupmap modify ntgroup=”Domain Admins”rid=512 unixgroup=admin** - Caso tenha necessidade de modificar um mapeamento.

Dessa forma, se o usuário logar com os usuários que estejam no grupo admin em algum terminal windows no domínio, ele terá permissões de administrador.

3.9 Perfis Moveis

Para que as configurações e personalizações do perfil do usuário no windows sejam salvas é necessário a criação de um perfil móvel no servidor samba. A vantagem de se utilizar um perfil móvel é que não existe a obrigatoriedade de se realizar backup na máquina do usuário, pois os arquivos são salvos no servidor, sendo assim é só o usuário fazer o login em outra máquina windows que o seu perfil e os seus dados serão migrados para o novo computador. Porém o perfil móvel tem um problema que é a quantidade de dados armazenados. Se o número de usuários e dados de cada um for muito grande, cria-se a necessidade de ter um servidor com muito espaço e uma rede muito bem estruturada.

Para ativar a configuração de perfil móvel no samba deve-se adicionar no [global]

logon path = \\%L\Profiles\%U

logon home = \\%L\Profiles\%U

logon drive = H:

- **logon path** - Serve para indicar o caminho onde vão ficar os perfis no Windows XP/Vista/7
- **logon home** - Indica o caminho para os perfis em versões mais antigas do Windows, como 95/98.
- **logon drive** - Unidade que será mapeada com o caminho \\servidor\profiles\”nome do usuário”no Windows.

Como a estrutura da rede do IFF Bom Jesus é composta por Windows XP/7 e Ubuntu 11.04 ou superior temos a opção de não adicionar a variável ”logon home”

Agora precisamos deletar todas as pastas do diretório home e trocar a sua permissão

- **# mkdir /var/samba/usuario**
- **# chmod 1777 -R /var/samba/usuario**

Todo usuário que fizer login no servidor irá criar automaticamente uma pasta com o seu nome e com toda a estrutura do perfil como Desktop, Meus documentos. Com a permissão 1777 o samba se encarrega de permitir somente acesso ao usuário logado, onde o 1 é uma permissão especial.

Os diretórios criados podem ficar em compartilhamento para o usuário que será mapeado na unidade H no windows.

[profiles]

path = /var/samba/usuario

writeable = yes

browseable = no

create mask = 0600

directory mask = 0700

available = yes

- **path** - Caminho da pasta que vai ser compartilhada.
- **writeable** - Permite a escrita no diretório e nos arquivos.
- **browseable** - Define se o compartilhamento poderá ser visto na pasta principal do compartilhamento ou somente pelo endereço completo.
- **create mask** - Força a criação dos arquivos com a permissão 0600, assim somente os donos do arquivo poderão alterar os arquivos.
- **directory mask** - Criação dos diretórios com permissão 0700.
- **available** - (Yes/No) Se o compartilhamento estará acessível ou não no servidor.

**FIGURA DO PERFIL MOVEL NO LINUX

3.10 Compartilhamento de Arquivos

O compartilhamento de arquivos é dado pela adição de seções no arquivo smb.conf.

[Diretoria]

path = /media/diretoria

read only = no

valid users = +diretoria

force group = diretoria

create mask = 0770

directory mask = 0770

browseable = no

- **[Diretoria]** - Nome do compartilhamento que será mostrado no servidor.
- **path** - Caminho onde se encontra o diretório no servidor.
    1. $ mkdir - Cria uma pasta no servidor. Exemplo: mkdir pasta .
    2. # chmod - Define as permissões do arquivo. Exemplo: # chmod 774 /pasta_criada - Essas permissão definem que o usuário proprietário do diretório e todos os usuário do seu grupo terão acesso total ao mesmo e seus arquivos e que os outro usuário poderão apenas listar os arquivos que se encontram no diretório.
    3. # chown - Define qual será o usuário e grupo proprietário do diretório ou arquivo. Exemplo: # chown usuario.grupo /diretorio .
- **read only** - Define se o compartilhamento estará com permissão de somente leitura ou não.
- **Valid users** - Define quais usuários e grupos poderão acessar o compartilhamento. O símbolo de + define que o nome inserido esta se referindo a um grupo de usuários.
- **force group** - Força qual será o grupo proprietário dos arquivos criados no compartilhamento.
- **create mask** - Permissão dos arquivos que forem criados ou inseridos no compartilhamento
- **directory mask** - Permissão dos diretórios do compartilhamento

- **browseable** - Define se o compartilhamento poderá ser visualizado na janela do compartilhamento do servidor.

Existem outras variáveis que podem ser adicionadas em um compartilhamento de arquivos dependendo da necessidade.

- **invalid users** - Lista de usuários e grupos que não terão acesso.
- **guest ok** - Permite que qualquer usuário acesse a pasta.
- **veto files** - Impede que certos arquivos sejam transferidos para o servidor.
- **write list** - Lista dos usuários que poderão gravar e fazer alterações nos arquivos e diretórios compartilhados.
- **read list** - Lista dos usuários que só poderão ler e listar os arquivos e diretórios compartilhados.
- **host deny** - Ip‘s ou faixa de ips que não podem conectar ao servidor.
- **hosts allow** - Ip‘s ou faixas de ips que podem conectar ao compartilhamento.

Exemplo da aplicação de algumas delas

[Backup]

write list = usuario1 # Somente o usuario1 terá permissão de escrita no compartilhamento.

read list = usuario2 # O usuario2 só poderá ler e listas os arquivos e diretórios desse compartilhamento.

host allow = 192.168.1.2-192.168.1.20 # Somente os ip’s que estiverem entre 192.168.1.2 e 192.168.1.20 poderão acessar esse compartilhamento.

veto files = *.tmp/*.doc # Não será permitido inserir esses tipos de arquivos no compartilhamento. Essa variável aceita expressões regulares

**FIGURA DO COMPARTILHAMENTO NO SERVIDOR

3.11 Script Logon

Para que os mapeamentos de unidades e alguns códigos sejam executados de forma automática nos usuários logados o samba fornece a opção na seção [global].

- logon script = %G.bat - Com essa variável adicionada, o sistema irá buscar o script com o nome do grupo primário do usuário. Trabalhar com o grupo é mais fácil de se gerenciar pois o mesmo script serve para mais de um usuário. O uso do %U é um complicador, já que cada seria necessário criar um script para cada usuário do sistema.

  Exemplo:

  Usuário logado : usuário

  Grupo primário : grupo

  Script a ser procurado : grupo.bat

  Esse script precisa estar compartilhado no smb.conf para que possa ser executado.

  [netlogon]

  path = /var/samba/scripts

  read only = yes

  browseable = no

O local onde foi definido que irá conter os scripts e os arquivos (/var/samba/scripts), tem que ter a permissão 1775.

- **# mkdir -p /var/samba/scripts** - Cria a pasta onde estarão os scripts.
- **# chmod 1775 /var/samba/scripts** - Permissão de execução dos scripts.

  Exemplo de um dos scripts

  diretoria.bat

  net use x: \\servidor\diretoria

  **FIGURA DO MAPEAMENTO AUTOMÁTICO

3.12 Compartilhamento de Impressoras

O compartilhamento de impressora é a publicação das impressoras instaladas no servidor para que outras máquinas que estão na rede possam acessar e imprimir sem precisar da conexão local na impressora.

Para compartilhar as impressoras com o samba deve-se adicionar na seção [global]

[global]

printing = cups

load printers = yes

- **printing** - Define qual o programa será utilizado para gerenciar as impressões
- **load printers** - Carrega as impressoras

O samba utiliza o cups que é o gerenciador de impressoras mais comum para o linux.

- **#smbd -b | grep CUPS** - Para saber se o pacote samba instalado é compatível com o CUPS. A saída deve ser algo como ”HAVE CUPS”

Caso o cups não esteja instalado.

- **#apt-get install cups** - Instala todos os pacotes necessários para o funcionamento do cups.
- **$ firefox localhost:631** - Interface gráfica para gerenciar as impressoras.
- **# /etc/init.d/cupsys restart** - Reinicia o serviço do cups

FIGURA DO CUPS PELO BROWSER

Habilitando o compartilhamento de impressora

[printers]

print ok = yes

guest ok = yes

path = /var/spool/samba

browseable = yes

- **path** - Esse caminho é onde ficarão os spools de impressão. Esse diretório é criado automaticamente pelo samba e deve ter a permissão 777.

1. **chmod 777 -R /var/spool/samba**

Dessa forma ao acessar o servidor irão aparecer todas as impressoras instaladas.

3.13 Instalação automática dos drive da impressora

Para conectar-se a uma impressora compartilhada é necessário a instalação dos drivers da mesma.

Um problema é como esses drivers são armazenados e instalados, já que uma das formas de instalar esses drivers é ir até o computador com o instalador em cd ou pen-drive e realizar a instalação manualmente, porém em uma grande rede se perde muito tempo com a locomoção e instalação. A solução desse problema é a instalação automática dos drivers, e com a utilização do samba os drivers serão instalados assim que o usuário tentar conectar a impressora.

Adiciona no [global]

- **enable privileges = yes** - Permite privilégios a usuários

Criar um compartilhamento não visível onde ficará os drivers das impressoras.

[print$]

path = /var/lib/samba/printers

read only = yes

write list = root

inherit permissions = yes

- **path** - Local onde os drivers serão instalados
- **write list** - Usuários ou grupos que terão permissão de escrita
- **inherit permissions** - Se os arquivos irão herdar as permissões da pasta.

Se o caminho apontado pelo path não existir ele terá que ser criado com as permissões necessárias.

- **# mkdir -p /var/lib/samba/printers**
- **# cd /var/lib/samba/printers**
- **# mkdir WIN40 W32X86** - Essas pastas são os locais onde ficarão os drivers das impressoras, o WIN40 para sistemas Windows 95/98/ME e o W32X86 Windows NT/2000/XP.
- **# chmod 2775 WIN40 W32X86** - Permissões especiais para instalar os drivers nos usuários.

- **# net -S localhost -U root -W BATTOUSAI-SHARE rpc rights grant 'BATTOUSAI-SHARE\root' SePrintOperatorPrivilege** - Irá definir que o usuário root terá todas os privilégios necessários para gerenciar as impressoras.

Com as permissões, usuários e impressoras configuradas, os drivers têm que ser passados para o servidor.

1. **Acessar a maquina com um usuário local** - 3.2
2. **Informar o endereço do servidor** - 3.3
3. **Informar o usuario root e sua senha** - 3.4
4. **Acessar a pasta 'Impressoras e aparelhos de fax'** -3.5
5. **Clique na opção Arquivos ->> Propriedade do servidor** - 3.6
6. **Aba Driver ->> Adicionar** - 3.7
7. **Selecionar o driver da impressora que deve ser copiado para o servidor** - 3.8
8. **Selecionar os SO dos drivers** - 3.9
9. **Botão direito na impressora Propriedades** - 3.10
10. **Selecione a opção 'Não', se selecionar o SIM o driver será instalado somente na maquina local** - 3.11
11. **Aba Avançado** - 3.12
12. **Selecione o drive que será vinculado a impressora** - 3.12
13. **Logar com o usuário do domínio no qual será mapeada a impressora** - 3.13
14. **Selecione a impressora no servidor** - 3.14
15. **Impressora instalada no usuário** - 3.15

3.14 Ingressando o Windows XP no Domínio

3.15 Ingressando o Linux no Domínio

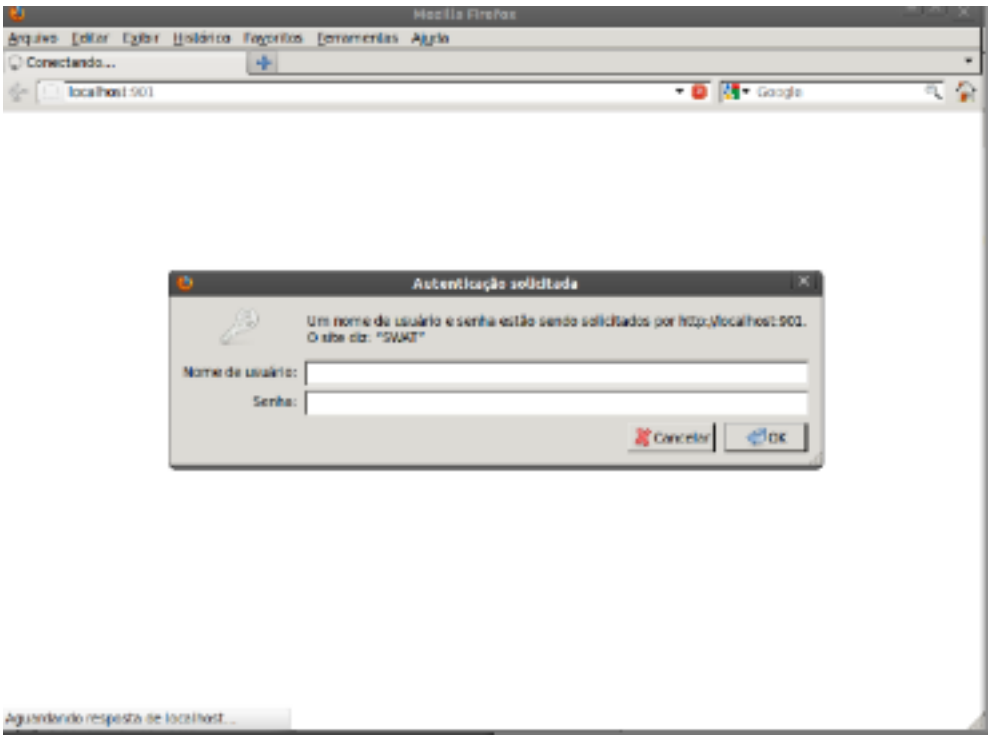


Figura 3.1: Tela do Login no Swat

Figura 3.2: Tela do Login no Windows localmente

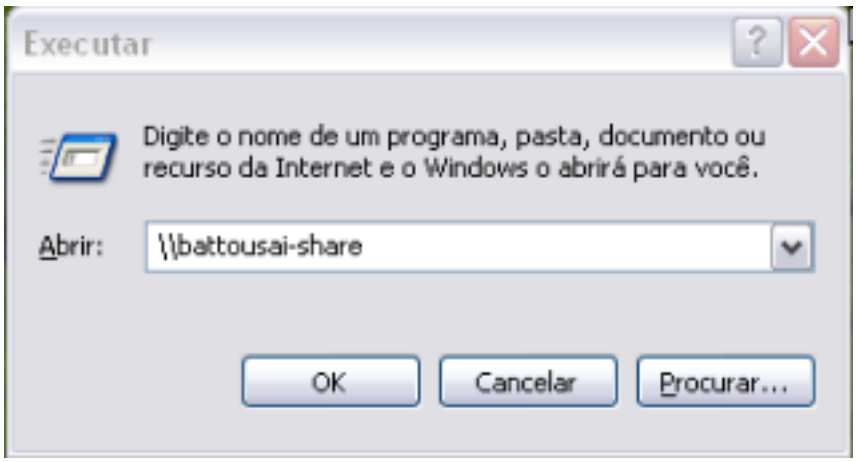


Figura 3.3: IP do servidor de compartilhamento

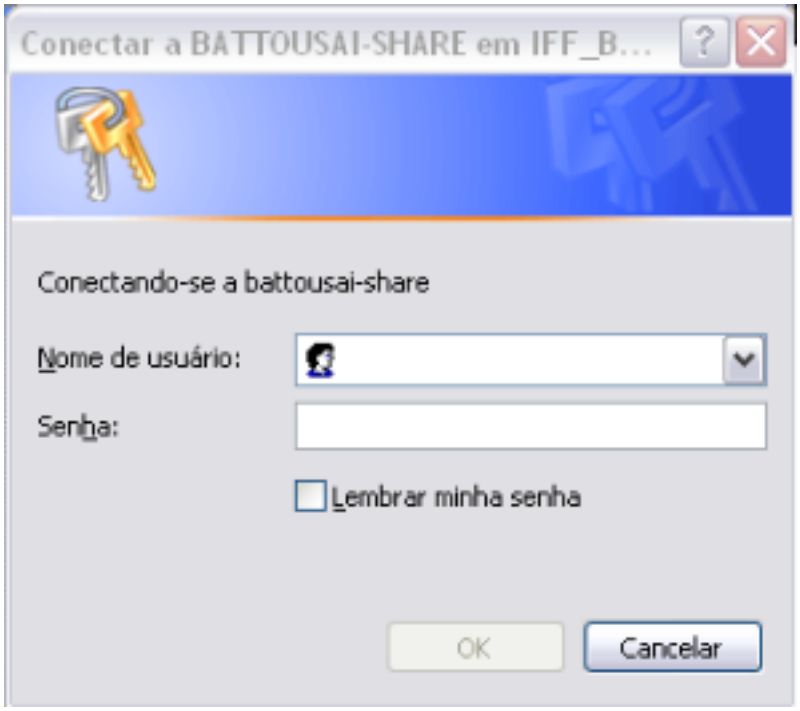


Figura 3.4: IP ou Netbios do servidor de compartilhamento

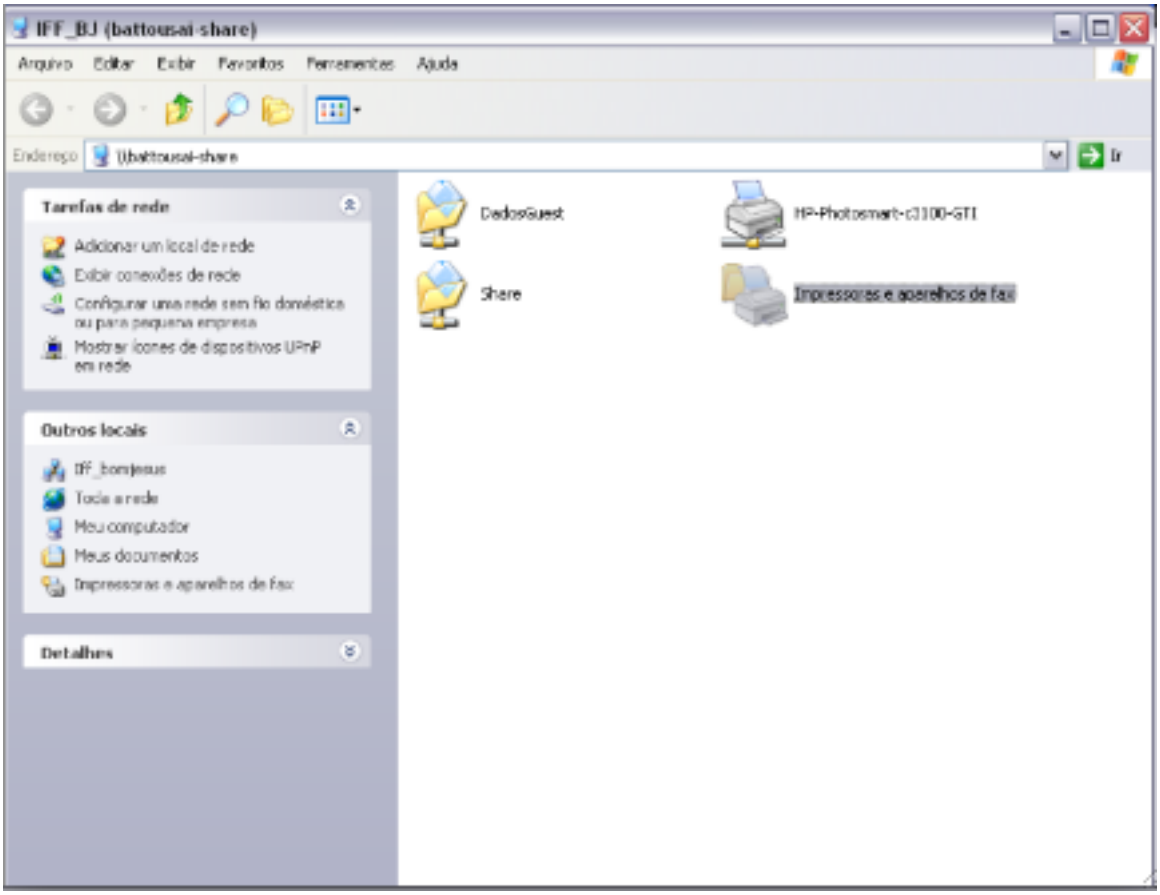


Figura 3.5: Impressoras e aparelhos de fax compartilhados

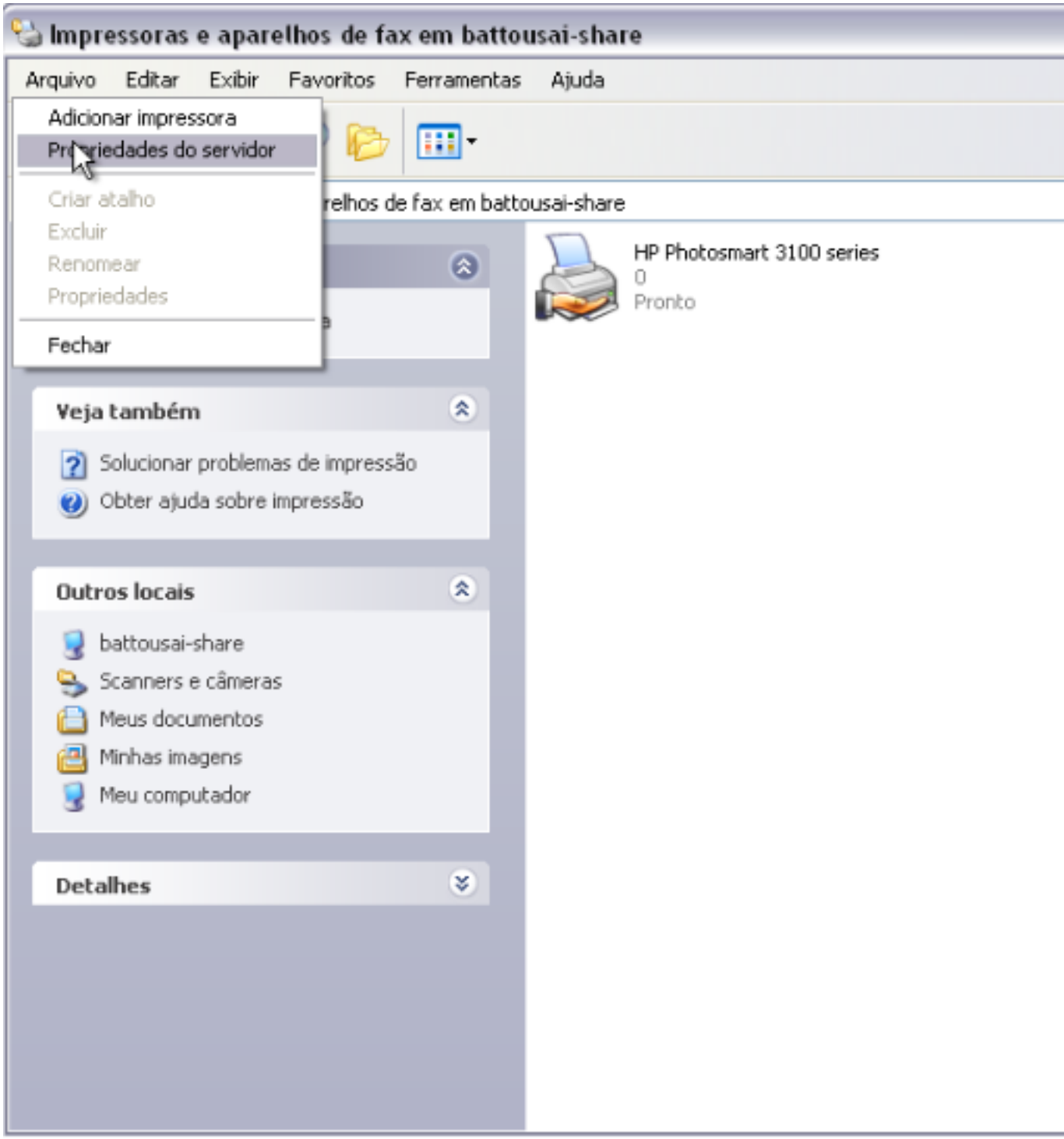


Figura 3.6: Propriedades do servidor de impressão

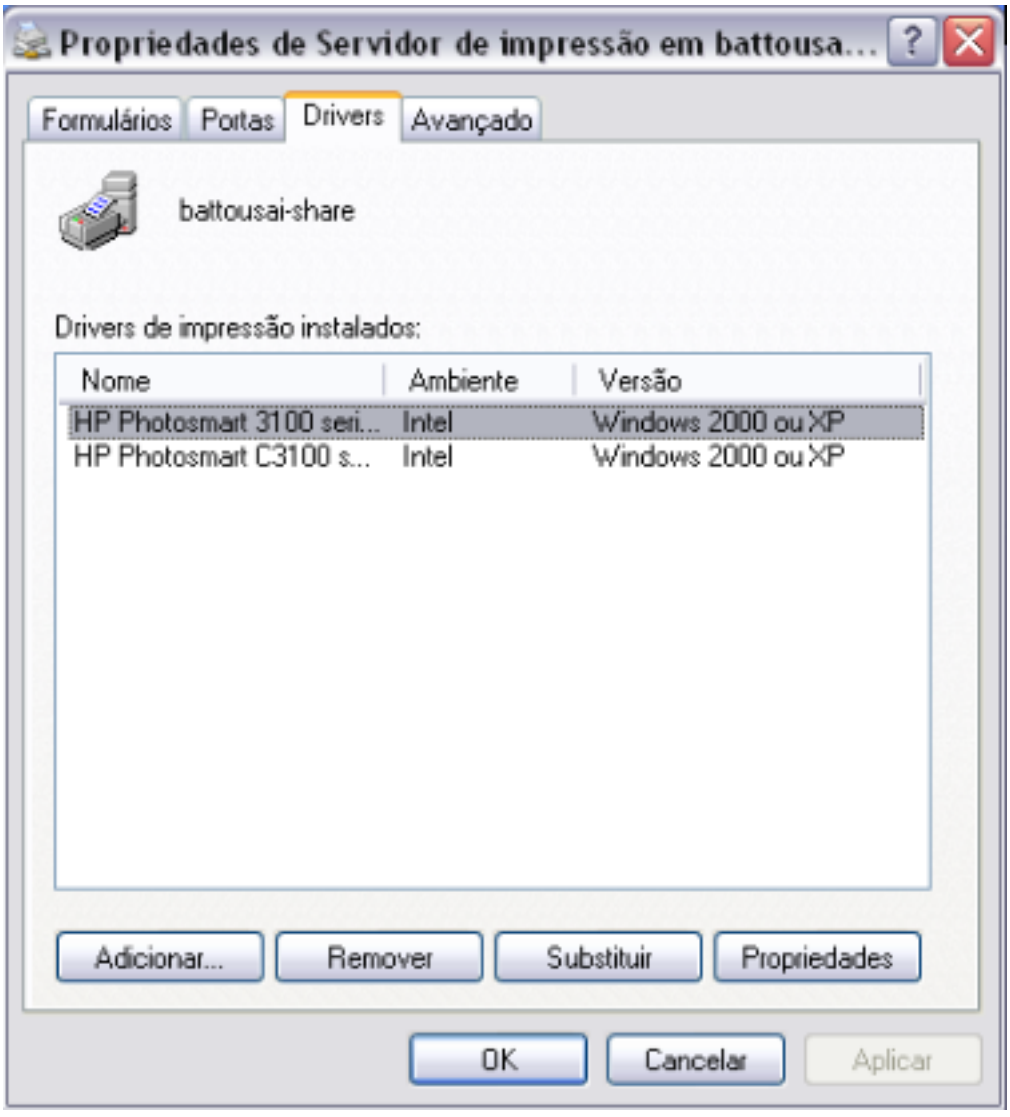


Figura 3.7: Adicionar driver ao servidor de impressão

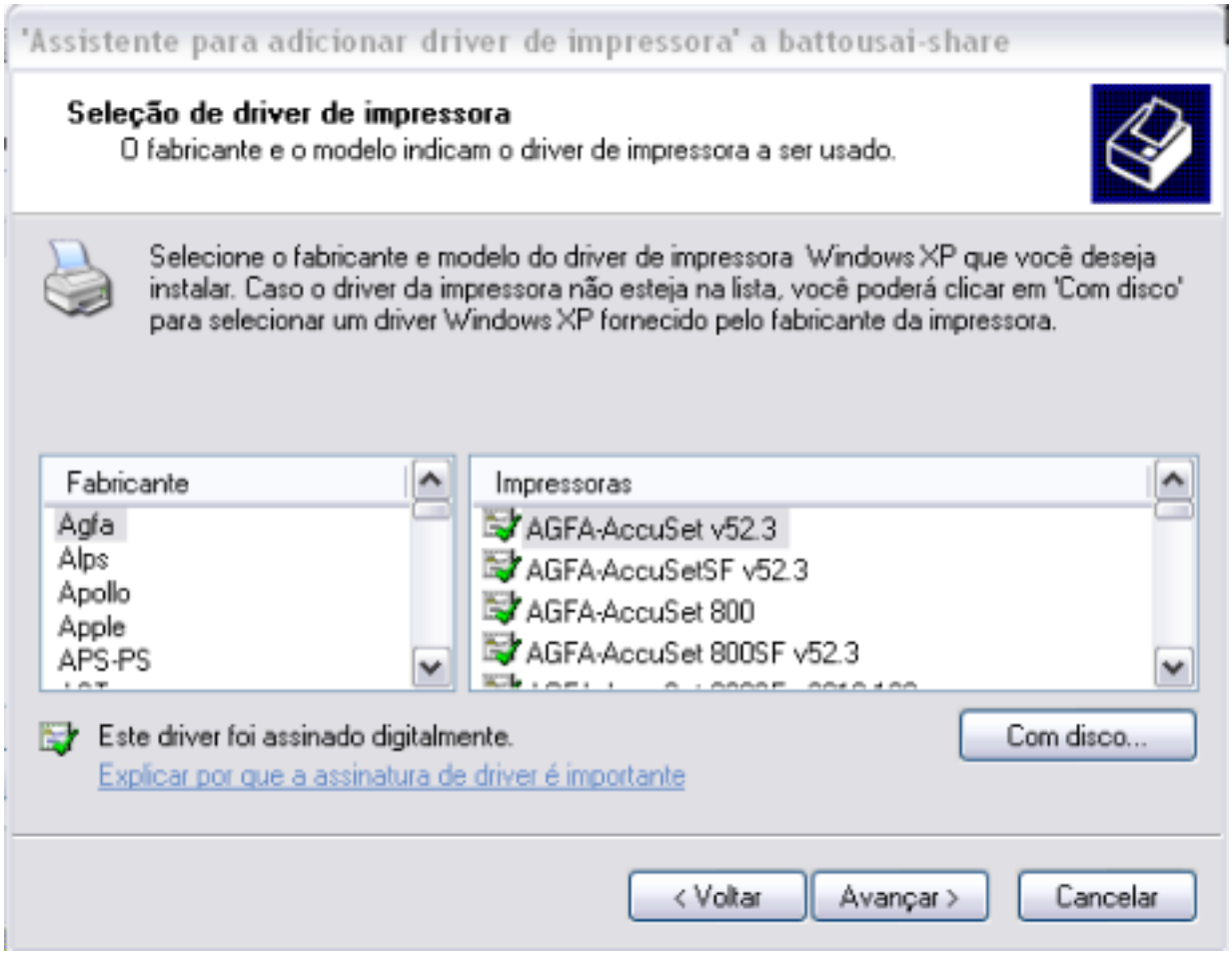


Figura 3.8: Selecionar o driver que será copiado para o servidor de impressão

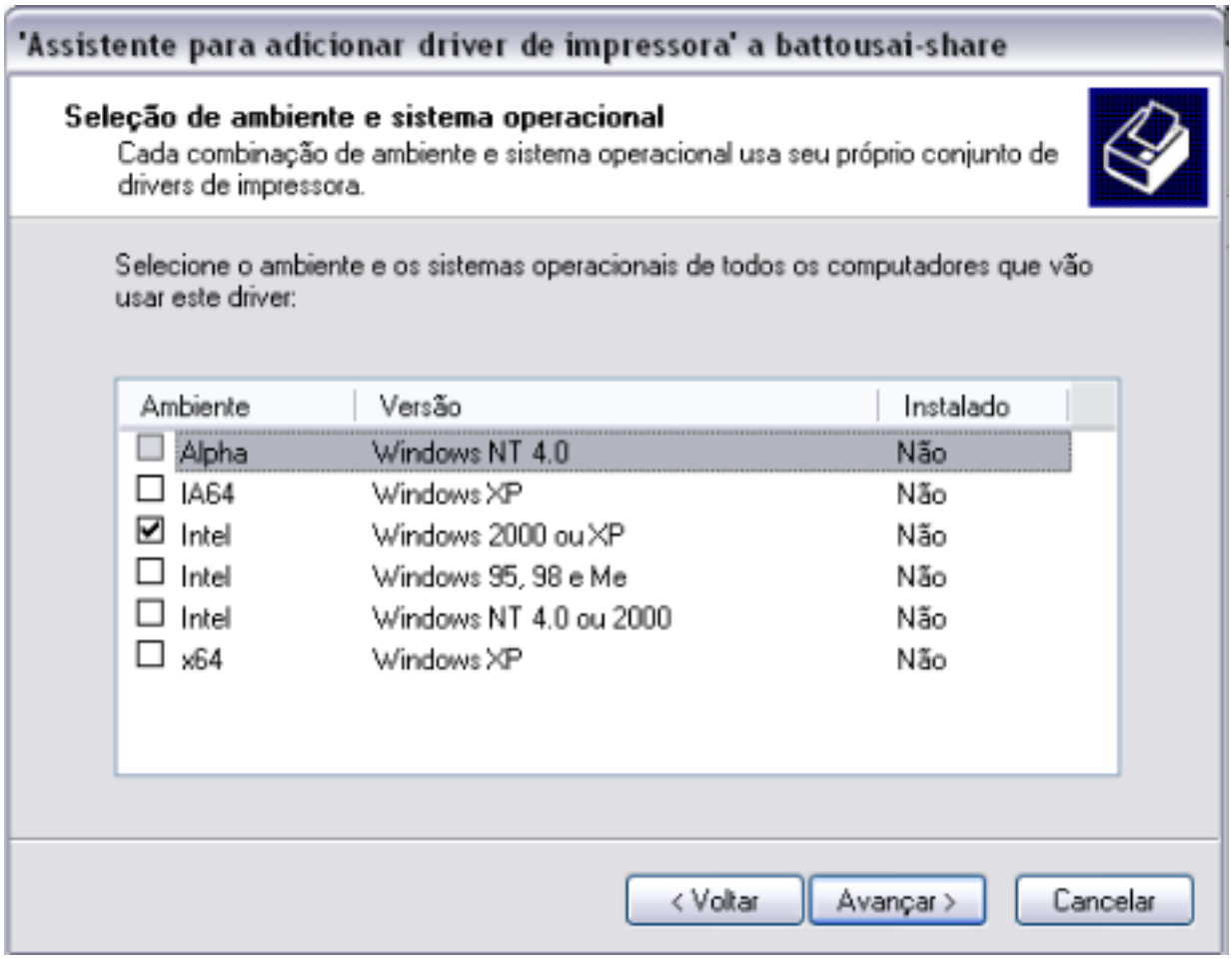


Figura 3.9: Selecionar os Sistemas Operacional que o driver será compatível

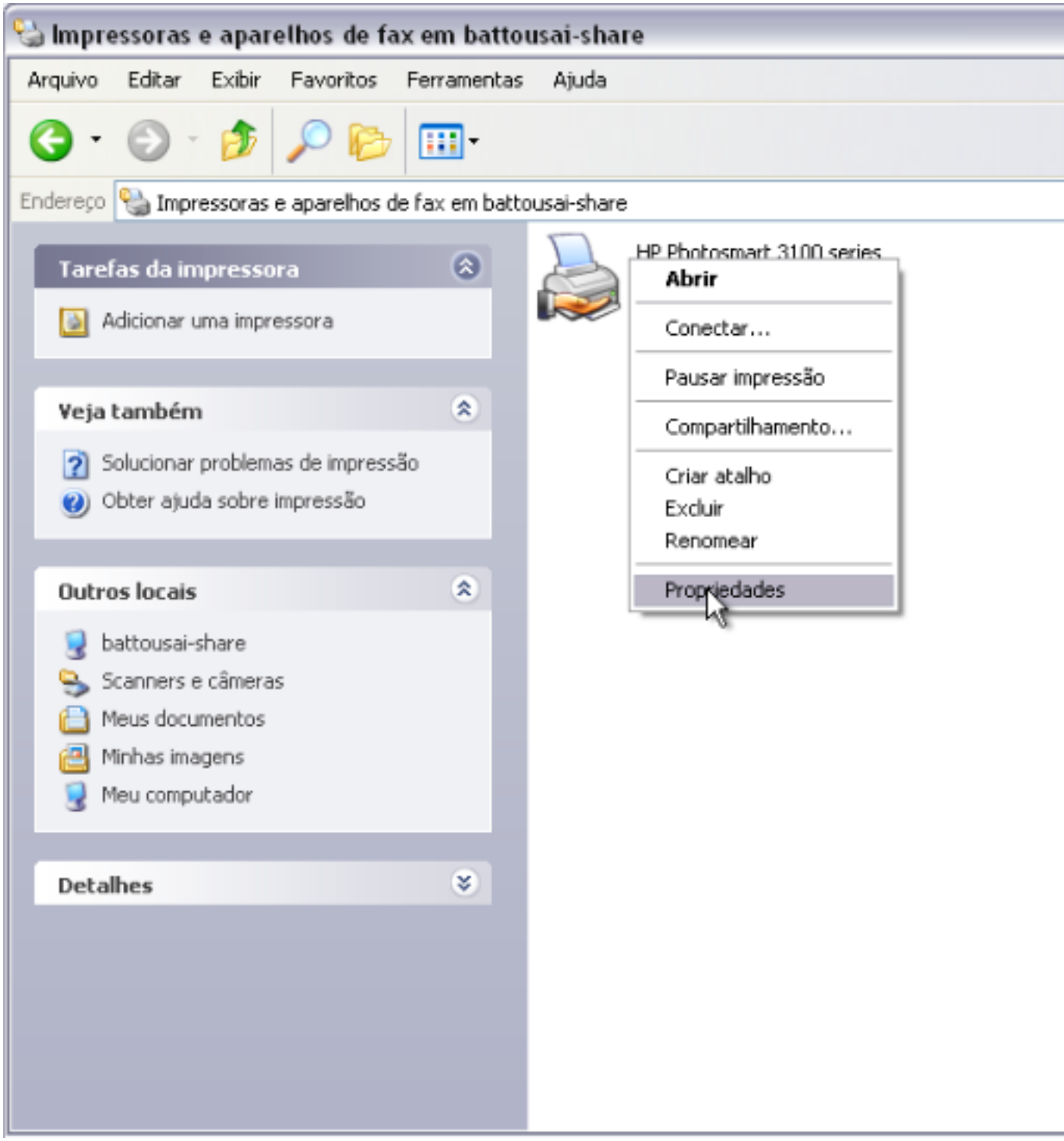


Figura 3.10: Propriedade da impressora do compartilhamento

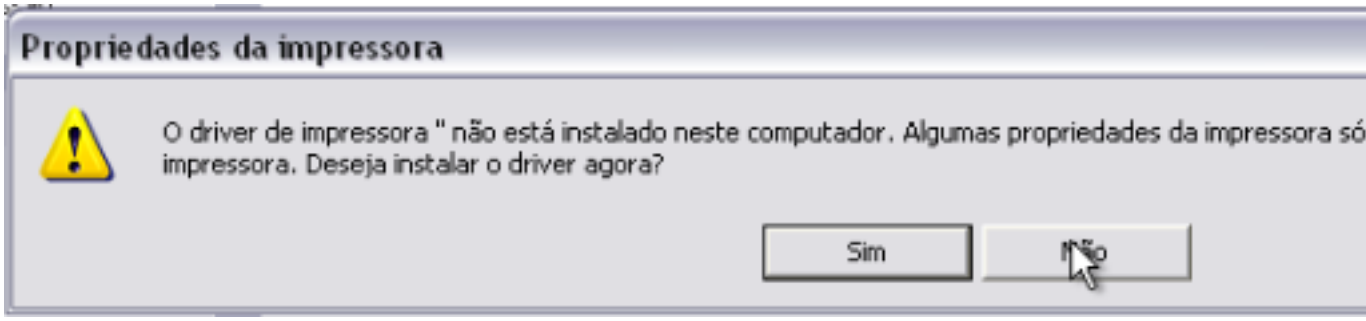


Figura 3.11: Opção para não instalar o driver naquele momento

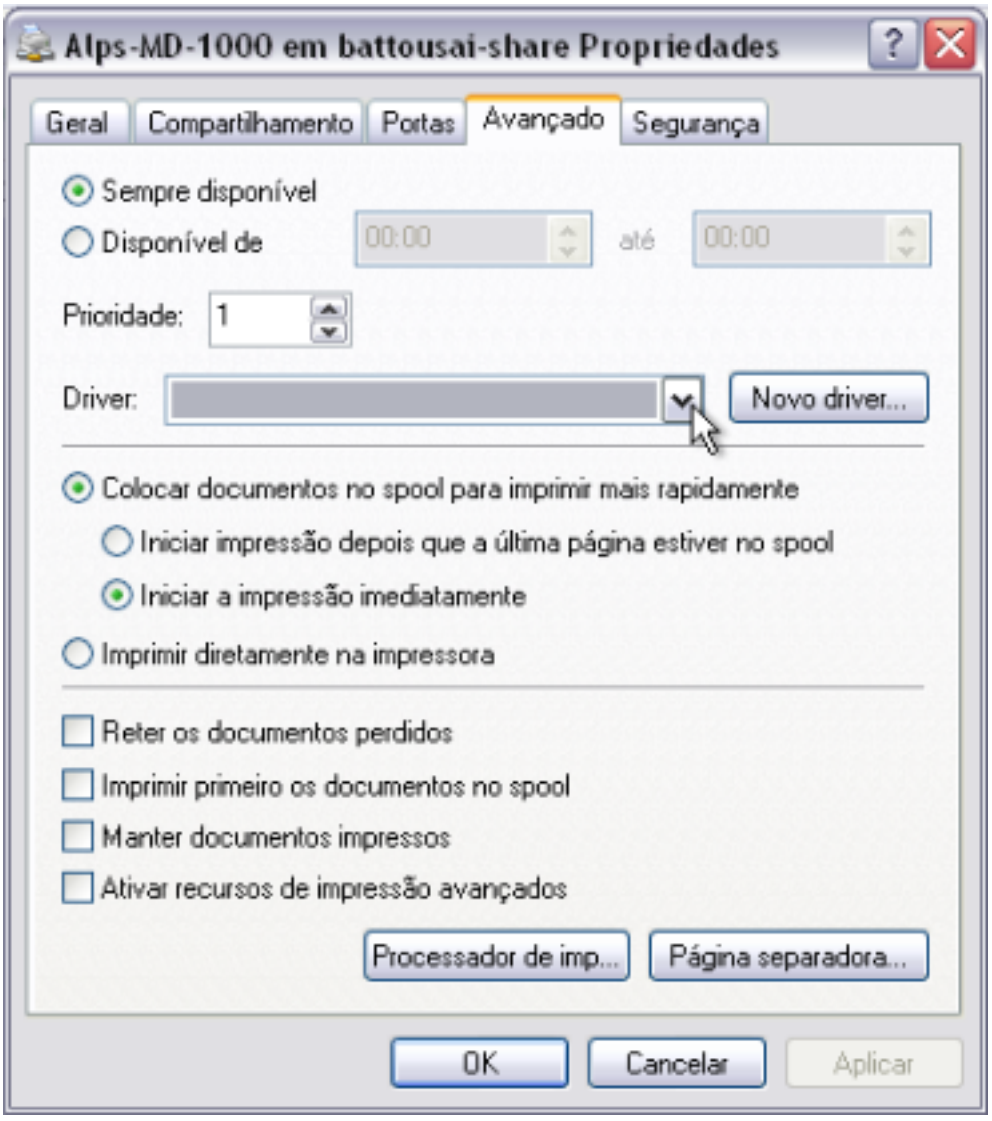


Figura 3.12: Aba onde será feito o link da impressora com o driver

Figura 3.13: Logar no domínio

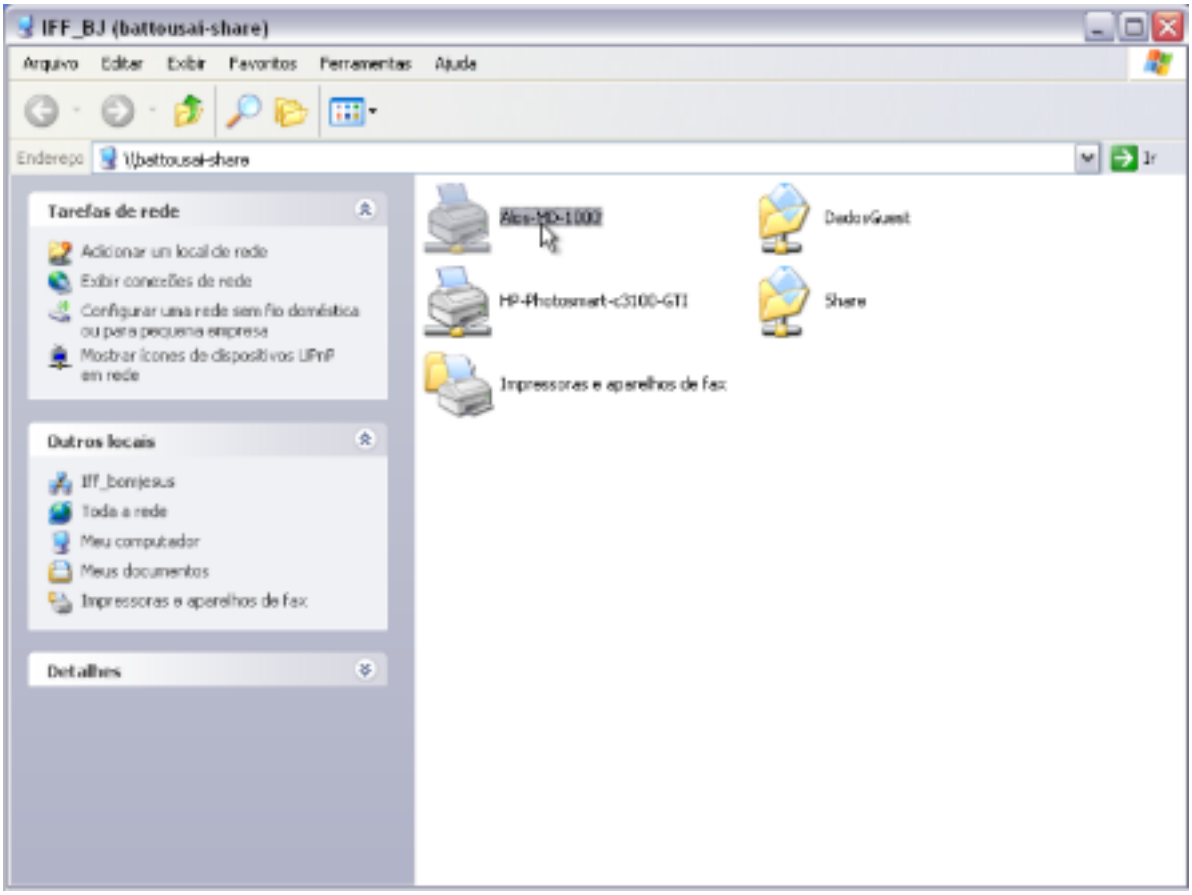


Figura 3.14: Selecionar a impressora que será mapeado no usuário logado

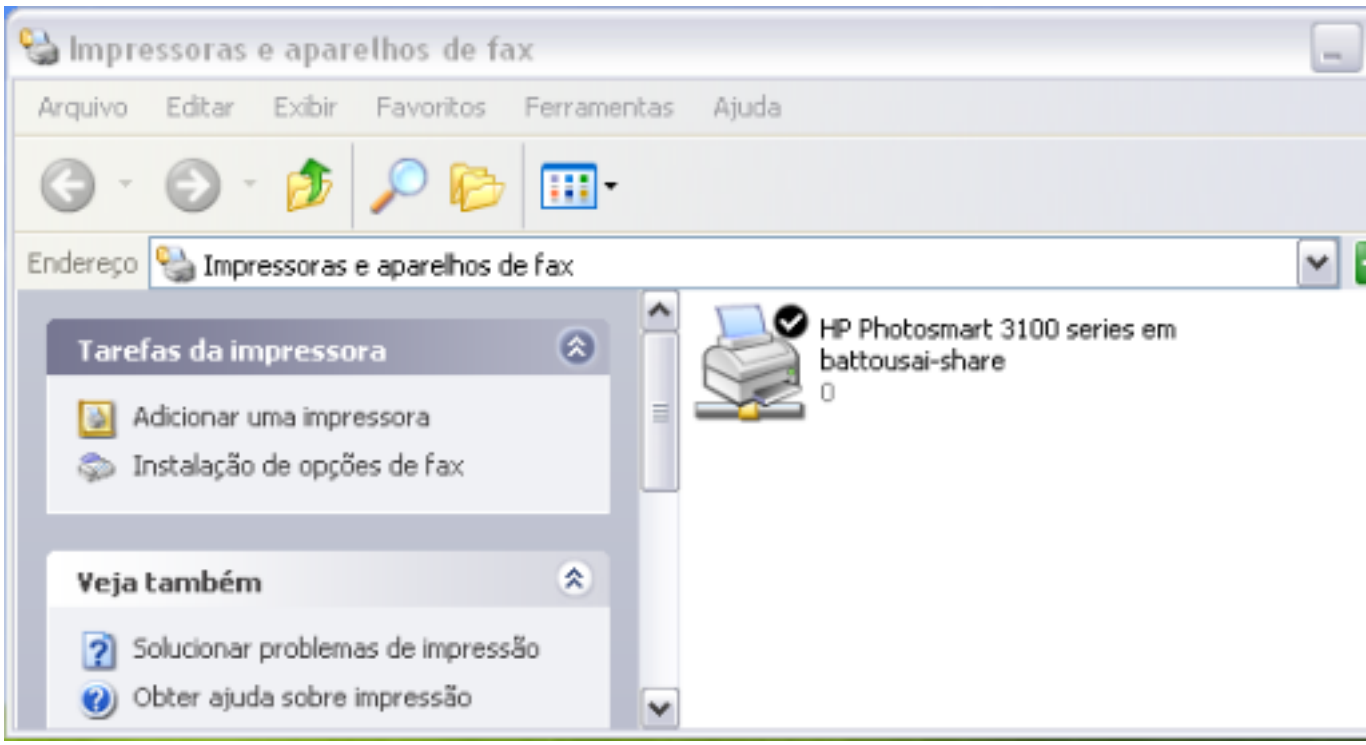


Figura 3.15: Impressora instalada no usuário

4 SAMBA 4

O samba 4 vem com a proposta de criar um Active Directory livre, utilizando o LDAP, Bind e Kerberos.

4.1 Instalação do SAMBA4

Por se tratar de um sistema ainda em fase de produção alguns erros podem aparecer ou alguns parâmetros deverão ser modificados. A instalação é realizada a partir do terminal, mas antes é necessário a instalação de algumas bibliotecas.

apt-get install build-essential libattr1-dev libblkid-dev libgnutls-dev python-dev autoconf python-dnspython git-core

Antes de começar a instalação o relógio do servidor tem que estar atualizado. O comando ntpdate deve ser usado para esse fim, onde um dos principais servidores é o br.pool.ntp.org.

ntpdate br.pool.ntp.org

O código fonte esta hospedado no servidor git dos desenvolvedores do samba, e o mesmo deve ser clonado para a maquina de destino.

git clone git://git.samba.org/samba.git samba-master; cd samba-master

O samba 4 segue os procedimento padrões de instalação de aplicativos no linux através do terminal, que segundo (???) se segue com o ./configure, make e o make install. Explicação dos procedimentos. Nesse caso ao invés de se utilizar o ./configure como padrão é utilizado o ./configure.developer, pois o mesmo habilita alguns modos de debug.

Para verificar a versão instalada é só executar o seguinte comando:

/usr/local/samba/bin/smbclient --version

4.2 Criação de Domínio com o Samba 4

Por padrão o samba 4 é instalado no /usr/local/.

cd /usr/local/samba

A instalação é a partir da execução do comando provision que fica localizado no /sbin do samba e a inserção de alguns parâmetros.

sbin/provision --use-ntvfs --realm=NOME_SERVIDOR --domain=NOME_DOMINIO --adminpass= Senha12 --server-role='domain controller'

1. **use-ntvfs** - Habilita o NTVFS;
2. **realm** - Domínio do servidor Kerberos;
3. **domain** - Domínio do samba;
4. **adminpass** - Senha do Administrator, essa senha deve ter pelo menos uma letra maiúscula;
5. **server-role** - Regra do servidor.

Depois de instalado e configurado o servidor de Active Directory pode ser iniciado. Uma das forma é inicia-lo em modo debug para poder acompanhar melhor os processos realizados.

/usr/local/samba/sbin/samba -i -M single

4.3 Instalação e configuração do BIND9

BIND (Berkeley Internet Name Domain ou, como chamado previamente, Berkeley Internet Name Daemon[1]) é o servidor para o protocolo DNS mais utilizado na Internet,[2] especialmente em sistemas do tipo Unix, onde ele pode ser considerado um padrão de facto. Foi criado por quatro estudantes de graduação, membros de um grupo de pesquisas em ciência da computação da Universidade de Berkeley, e foi distribuído pela primeira vez com o sistema operacional 4.3BSD. O programador Paul Vixie, enquanto trabalhava para a empresa DEC, foi o primeiro mantenedor do BIND. Atualmente o BIND é suportado e mantido pelo Internet Systems Consortium. Para a versão 9, o BIND foi praticamente reescrito. Ele passou a suportar, dentre outras funcionalidades, a extensão DNSSEC e os protocolos TSIG e IPv6.(http://pt.wikipedia.org/wiki/BIND)

O samba 4 já vem pré configurado para trabalhar com BIND9 para ser o servidor DNS nas versões 9.8 e 9.9. Atualmente a versão do Bind9 no repositório é a 9.7 e com isso é gerada algumas incompatibilidades e para resolver esses problemas é feita o download e a instalação manual da versão 9.9.

wget ftp://ftp.isc.org/isc/bind9/9.9.0/bind-9.9.0.tar.gz

Descompactazação do pacote baixado.

tar -xzvf bind-9.9.0.tar.gz

Entrar no diretório do bind9

cd bind-9.9.0

Configuração para a instalação, informando qual o local de instalação e onde ficarão os arquivos de configuração.

./configure --prefix=/usr/local/bind9 --sysconfdir=/etc/bind

*****EXPLICAR O MAKE*****

*****EXPLICAR MAKE INSTALL*****

Entrar no diretório onde se encontra os arquivos de configuração do bind

cd /etc/bind

Com esse procedimento de instalação os arquivos de configuração não são gerados automaticamente, com isso gerando a necessidade de cria-los manualmente.

vim named.conf.options

As seguintes configurações devem ser adicionadas.

options {

directory ”/usr/local/bind/var/run/named”;

tkey-gssapi-keytab ”/usr/local/samba/private/dns.keytab”;

tkey-domain ”nome_do_realm_samba”;

};

As variáveis adicionadas no arquivos são para:

- directory - É o caminho absoluto do seu servidor dns;
- tkey-gssapi-keytab - Local da chave do dns para conexão com o kerberos;
- tkey-domain - Nome do Domínio.

O comando provision gera os arquivos de configuração necessários para o funcionamento do samba com o servidor dns.

- **# vim named.conf.local** - Adicione a linha abaixo no arquivo;

    1. **include ”/usr/local/samba/private/named.conf”;**

Com os arquivos named.conf.local e named.conf.options devidamente criados e configurados, deve-se inclui-los no arquivos named.conf

vim named.conf

include ”/etc/bind/named.conf.local”; include ”/etc/bind/named.conf.options”;

Como o samba 4 já vem com configurações prontas do bind9 é necessário escolher qual a versão do dns que esta sendo utilizada.

- **# vim /usr/local/samba/private/named.conf**

  *****FIGURA DO ARQUIVO******

  # For BIND 9.8.0

  # database ”dlopen /usr/local/samba/lib/bind9/dlz_bind9.so”;

  Descomentar

  # For BIND 9.9.0

  database ”dlopen /usr/local/samba/lib/bind9/dlz_bind9_9.so”;

- **# groupadd named && useradd named -g named** - Cria o usuário responsável pelo bind e o insere no grupo named;
- # chown named:named /usr/local/samba/private/dns.keytab
- **# /usr/local/bind9/sbin/named -u named -g** - Inicia o bind com o usuário named;

O servidor samba tem que ter seu endereço DNS configurado para apontar para seu servidor DNS.

- **# echo ’nameserver ip_do_servidor’** $>>$ **/etc/resolv.conf** - Define o endereço do servidor de DNS que o computador irá enviar suas solicitações;

A partir de agora para acessar a internet através do servidor samba o bind deverá estar sendo executado.

4.4 Instalação do Kerberos

Segundo(http://samba4.wordpress.com/2009/09/25/instalacao-samba4) Autenticação Kerberos é um protocolo de rede. Foi concebido para fornecer autenticação forte para o cliente/servidores de aplicativos usando criptografia de chaves secretas, então um cliente pode

provar a sua identidade para um servidor (e vice-versa) em uma conexão de rede insegura. Em nosso caso utilizaremos BIND com suporte ao Heimdal Kerberos por causa do GSS-TSIG algoritmo de serviço de segurança genérico para autenticação de transação com chave secreta de DNS (GSS-TSIG) este mecanismo é utilizado para estabelecer relações TSIG para autenticação do tipo Kerberos, necessário para interagir BIND com Samba4, com essas credenciais o DNS aceita atualizações GSS-TSIG assinadas e verifica as credenciais de correspondentes com as credencias cadastradas no Samba4, isso permite aos usuários descarregar o DNS dos usuários do Microsoft Windows sem ter a segurança comprometida.

- **# apt-get install krb5-user krb5-kdc krb5-config kstart** - Instala todos os pacotes necessários e faz as referências necessárias.

Após instalar os pacotes, substitua o /etc/krb5.conf pelo arquivo criado e pré-configurado pelo samba que esta localizado em /usr/local/samba/private/krb5.conf

- **# cp /usr/local/samba/private/krb5.conf /etc/**

Teste para verificar se todos as configurações foram realizadas corretamente

- **# host -t SRV _ldap._tcp.”nome do realm sem aspas”.** - O resultado deve ser parecido : **_ldap._tcp.”nome do realm sem aspas”has SRV record 0 100 389 server.”nome do realm sem aspas”.**
- **# host -t SRV _kerberos._udp.”nome do realm sem aspas”.** - O resultado deve ser parecido : **_kerberos. _udp.”nome do realm sem aspas”has SRV record 0 100 88 server.”nome do realm sem aspas”.**
- **# host -t A ”nome do realm sem aspas”** - O resultado deve ser parecido : **”nome do realm sem aspas”has address ”ip do servidor**

4.5 Kerberos com Bind9

Configurar atualizações dinâmicas no DNS com o kerberos

Para o funcionamento das atualizações algumas variáveis necessárias de sistema devem ser criadas para o acesso do kerberos com bind

- **# KEYTAB_FILE=”/usr/local/samba/private/dns.keytab”**
- **# KRB5_KTNAME=”/usr/local/samba/private/dns.keytab”**

- **# export KEYTAB_FILE**
- **# export KRB5_KTNAME**

Mudar o dono e o grupo do dns.keytab para que o bind possa alterar o arquivo

- **# chown named:named /usr/local/samba/private/dns.keytab**
- **# /usr/local/samba/sbin/samba_dnsupdate --verbose** - Atualização automática do dns do samba.

4.6 AD

Pacotes necessários para gerenciar o AD no windows XP ou windows server.

4.7 GPO

Pacotes necessários para gerenciar as GPO's no windows XP ou windows server.

4.8 Compartilhamento de arquivos e impressoras

SAMBA4 ainda não consegue compartilhar arquivos e impressoras de forma fácil e simplificada como o samba 3, e tem problemas com a integração dos usuários e grupos do Active Directory com os locais, dificultando a definição das permissões a arquivos e diretórios.

Uma solução para tal problema é identificar o código do usuário no Active Directory e dar as devidas permissões a pasta desejada.

- **# /usr/local/samba/bin/wbinfo --name-to-sid USERNAME** - O resultado deve ser o sid do usuário no samba. Exemplo : S-1-5-21-4036476082-4153129556-3089177936-1005 SID_USER(1)
- **# /usr/local/samba/bin/wbinfo --sid-to-uid S-1-5-21-4036476082-4153129556-3089177936-1005** - Mostra o id do usuário e é a referência do usuário local com o do samba 4.
- **# chown 3000011 /pasta_que_será_compartilhada** - Mudando o usuário do diretório e as suas permissões, o usuário do AD irá ter o acesso aos arquivos.

4.9 Gerenciando o Samba4

O samba-tools - Gerência o samba. Com ele se poder criar usuários, grupos, gpo's e outras funções do Active Directory, porém um forma de texto.

FIGURA DO SAMBA-TOOLS

4.10 Maquinas linux e samba3 interagindo com o Active Directory do Samba4

Segundo (**??**) **??** a forma de incluir uma maquina Ubuntu no Active Directory é modificar alguns arquivos de configuração. Segue abaixo os arquivos e os procedimentos.

Informações

- **fja.br** - Domínio do Active Directory
- **fjadc01.fja.br** - Controlador de domínio
- **10.1.0.1** - IP do controlador de domínio
- **FJA.BR** - Kerberos Realm
- **gert** - Estação de Trabalho Ubuntu
- **gert.fja.br** - FQDN da estação de trabalho
- **fjadc01** - Servidor NTP

Instalando os pacotes necessários

- # aptitude install krb5-user libpam-krb5 winbind samba smbfs smbclient krb5-config libkrb53 libkadm55 vim

Sincronizando a hora

- # ntpdate 10.2.0.1

Edite o arquivo /etc/hosts adicionando o ip e o nome do DC de sua rede

- # vim /etc/hosts

127.0.0.1 gert.fja.br localhost gert

127.0.1.1 gert

The following lines are desirable for IPv6 capable hosts

::1 ip6-localhost ip6-loopback

fe00::0 ip6-localnet

ff00::0 ip6-mcastprefix

ff02::1 ip6-allnodes

ff02::2 ip6-allrouters

ff02::3 ip6-allhosts

10.2.0.1 fjadc01

10.2.0.2 fjadc02

Configurando o Kerberos

- # vim /etc/krb5.conf

[libdefaults]

default_realm = FJA.BR

[realms]

FJA.BR = {

kdc = fjadc01.fja.br

default_domain = FJA.BR

kpasswd_server = fjadc01.fja.br

admin_server = fjadc01.fja.br

}

[domain_realm]

.fja.br = FJA.BR

Testando a conexão com o Active Directory

- kinit <ENTER>
- Password for alex@FJA.BR: ****

- klist <ENTER>
- Ticket cache: FILE:/tmp/krb5cc_1000
- Default principal: alex@FJA.BR

Se o resultado for este o Kerberos está funcionando corretamente

Valid starting Expires Service principal 07/16/07 15:48:35 07/17/07 01:49:08

krbtgt/FJA.BR@FJA.BR renew until 07/17/07 15:48:35

Kerberos 4 ticket cache: /tmp/tkt1000

klist: You have no tickets cached

Acessando o Domínio

- # vim /etc/samba/smb.conf - Adicione as seguintes linhas

[global]

security = ads

realm = FJA.BR

password server = 10.2.0.1

workgroup = ADMINISTRATIVO

winbind separator = +

idmap uid = 10000-20000

idmap gid = 10000-20000

winbind enum users = yes

winbind enum groups = yes

template homedir = /home/%D/%U

template shell = /bin/bash

client use spnego = yes

client ntlmv2 auth = yes

encrypt passwords = yes

winbind use default domain = yes

restrict anonymous = 2

to avoid the workstation from

trying to become a master browser

on your windows network add the

following lines

domain master = no

local master = no

preferred master = no

os level = 0

Reinicie os serviços

- **# /etc/init.d/winbind stop**
- **# /etc/init.d/samba restart**
- **# /etc/init.d/winbind start**

Adicione a conta ao domínio

- **# net ads join**
- **Resultado** - Using short domain name – GERT Joined 'GERT' to realm 'FJA.BR'

Configure a Autenticação

- **# vim /etc/nsswitch.conf**

passwd: compat winbind

group: compat winbind

shadow: compat

Teste o winbind

- getent passwd

quiosque:*:10018:10000:Quiosque:/home/ADMINISTRATIVO/quiosque:/bin/bash

- getent group

__coordenação de enfermagem:x:10046:coordenf

__coordenação de design:x:10047:smarino,coorddes

Configure o PAM

- # vi /etc/pam.d/common-account - Adicione as seguintes linhas

  account sufficient pam_winbind.so

  account required pam_unix.so

- # vim /etc/pam.d/common-auth - Adicione as seguintes linhas

  auth sufficient pam_winbind.so

  auth sufficient pam_unix.so nullok_secure use_first_pass

  auth required pam_deny.so

- # vim /etc/pam.d/common-session Adicione as seguintes linhas

  session required pam_unix.so

  session required pam_mkhomedir.so umask=0022 skel=/etc/skel

- /etc/pam.d/sudo - Adicione as seguintes linhas

  auth sufficient pam_winbind.so

  auth sufficient pam_unix.so use_first_pass

  auth required pam_deny.so

  @include common-account

  Reinicie os serviços

- **# /etc/init.d/winbind stop**
- **# /etc/init.d/samba restart**
- **# /etc/init.d/winbind start**

Logando no domínio

Vá para a console usando o comando CTRL+ALT+F1 e logue no sistema com o login e senha do dominio

- login: nome_do_usuário
- Password: *****
- nome_do_usuário@gert: $

4.11 Script para adicionar maquina linux no Active Directory

```
#!/bin/sh
#####################################################################
# Copyright (C) 2011 - Fabio Antonio Ferreira                       #
# http://fantonio.wordpress.com — fantonios@gmail.com               #
# Este trabalho está licenciado sob uma Licença Creative Commons    #
# Atribuição-Compartilhamento pela mesma Licença 2.5 Brasil. Para ver a copia #
# desta licença, acesse: http://creativecommons.org/licenses/by-sa/2.5/br/ #
# ou envie uma carta para Creative Commons, 171 Second Street, Suite 300, #
# San Francisco, California 94105, USA.                             #
# Modificações em 27 de Julho de 2012 por Gabriel Rocha (GBR)       #
# email: gabriel.rocha.gbr@gmail.com                                #
#####################################################################
# == FUNCOES ================================================
USUARIO=‘whoami‘
if [ ”$USUARIO”!= ”root”]; then
echo
echo ”=====================================================”
echo ”ESTE PROGRAMA PRECISA SER EXECUTADO COM PERMISSOES DE SUPERUSUARIO!”
echo ”Abortando...”
echo ”=====================================================”
echo
exit 1
```

```
fi
_HEAD () {
‘which clear‘
echo ”============================================================”
echo ”SISTEMA PARA ADICIONAR MAQUINA LINUX AO DOMÍNIO WINDOWS OU LINUX”
echo ”============================================================”
}
_PACOTES () {
echo ”Instalando os pacotes necessários”;
apt-get install krb5-user libpam-krb5 winbind samba smbfs smbclient krb5-config lib-krb53 libkdb5-4 libgssrpc4 -y > /dev/null;
check=$(echo $?)
if [ $check -eq 0 ]; then
echo ”Pacotes instalados com sucesso”
else
echo ”Falha ao instalar os pacotes”
fi
}
_HORA () {
echo ”Atualizando data e hora”;
ntpdate br.pool.ntp.org > /dev/null;
echo ”Horario atual:”‘date‘
echo ”Hora alterada com sucesso”
}
_BACKUP_ORIG () {
# Rotina de Backup dos arquivos de configurações.
if [ ! -e /etc/krb5.conf_backup ]; then
cp /etc/krb5.conf /etc/krb5.conf_backup > /dev/null;
```

```
fi
if [ ! -e /etc/resolv.conf_backup ]; then
cp /etc/resolv.conf /etc/resolv.conf_backup > /dev/null
fi
if [ ! -e /etc/samba/smb.conf_backup ]; then
cp /etc/samba/smb.conf /etc/samba/smb.conf_backup > /dev/null
fi
if [ ! -e /etc/nsswitch.conf_backup ]; then
cp /etc/nsswitch.conf /etc/nsswitch.conf_backup > /dev/null
fi
if [ ! -e /etc/pam.d/common-account_backup ]; then
cp /etc/pam.d/common-account /etc/pam.d/common-account_backup > /dev/null
fi
if [ ! -e /etc/pam.d/common-auth_backup ]; then
cp /etc/pam.d/common-auth /etc/pam.d/common-auth_backup > /dev/null
fi
if [ ! -e /etc/pam.d/common-session_backup ]; then
cp /etc/pam.d/common-session /etc/pam.d/common-session_backup > /dev/null
fi
if [ ! -e /etc/pam.d/sudo_backup ]; then
cp /etc/pam.d/sudo /etc/pam.d/sudo_backup > /dev/null
fi
check=$(echo $?)
if [ $check -eq 0 ]; then
echo ”Rotina de Backup executada com sucesso!”
else
echo ”Falha ao fazer o Backup.”
fi
```

```
}
_RETURN_BACKUP () {
# Rotina de Recuperação do Backup de configurações.
mv /etc/krb5.conf_backup /etc/krb5.conf > /dev/null
mv /etc/resolv.conf_backup /etc/resolv.conf > /dev/null
mv /etc/samba/smb.conf_backup /etc/samba/smb.conf > /dev/null
mv /etc/nsswitch.conf_backup /etc/nsswitch.conf > /dev/null
mv /etc/pam.d/common-account_backup /etc/pam.d/common-account > /dev/null
mv /etc/pam.d/common-auth_backup /etc/pam.d/common-auth > /dev/null
mv /etc/pam.d/common-session_backup /etc/pam.d/common-session > /dev/null
mv /etc/pam.d/sudo_backup /etc/pam.d/sudo > /dev/null
check=$(echo $?)
if [ $check -eq 0 ]; then
echo ”Recuperação do Backup executada com sucesso!”
else
echo ”Falha na recuperação do Backup.”
fi
}
_NOME_DOMINIO () {
#Entrada do nome do dominio ao qual deseja engreçar.
#No caso do linux temos dois servidores um do KDC e outro do dominio
#No windows informamos o servidor kdc
read -p ”Entre com o nome do Domínio:”var1
dominio=$(echo $var1 — tr a-z A-Z)
read -p ”Entre com o seu KDC (key Distribution Center):”var2
kdc=$(echo $var2 — tr A-Z a-z)
}
_IP_DNS ()
```

```
#IP do servidor de dns
read -p ”Entre com o IP do servidor de DNS:”ip
echo ”nameserver $ip”> /etc/resolv.conf
}
_SO_SERVIDOR () {
#Sistema Operacional do AD
read -p ”Entre com o S.O. do servidor (Linux ou Windows): ”so
so=$(echo $so — tr a-z A-Z)
workgroup=
if [ $so = ”LINUX”] ; then
read -p ”Informe o Domain do Samba4: ”workgroup
workgroup=$(echo $workgroup — tr a-z A-Z)
else
workgroup=$(echo $var1)
fi
}
_KRB5 () {
echo ”[libdefaults]
default_realm = $dominio
# The following krb5.conf variables are only for MIT Kerberos.
krb4_config = /etc/krb.conf
krb4_realms = /etc/krb.realms
kdc_timesync = 1
ccache_type = 4
forwardable = true
proxiable = true
# The following libdefaults parameters are only for Heimdal Kerberos.
v4_instance_resolve = false
```

```
v4_name_convert = {
host = {
rcmd = host
ftp = ftp
}
plain = {
something = something-else
}
}
fcc-mit-ticketflags = true
[realms]
$dominio = {
kdc = $kdc
admin_server = $kdc
}
[domain_realm]
.$var1 = $kdc
[login]
krb4_convert = true
krb4_get_tickets = false”> /etc/krb5.conf
echo ”Configuração alterada com sucesso!”
}
_TESTEAD () {
read -p ”Entre com um usuário para testar sua conexão com o Active Directory:”user
kinit $user@$dominio
check=$(echo $?)
if [ $check -eq 0 ]; then
echo ”Sua máquina conectou com sucesso!”
```

```
else
echo ”Falha ao se conectar com o Active Directory”
fi
}
_SMB () {
maquina=$(hostname)
echo ”# Sample configuration file for the Samba suite for Debian GNU/Linux.
#======================= Global Settings =======================
[global]
workgroup = $workgroup
netbios name = $maquina
realm = $var1
server string = % h Server
dns proxy = no
log file = /var/log/samba/log.%m
max log size = 1000
syslog = 0
panic action = /usr/share/samba/panic-action %d
security = ADS
password server = $kdc
encrypt passwords = true
passdb backend = tdbsam
obey pam restrictions = yes
unix password sync = yes
passwd program = /usr/bin/passwd %u
pam password change = yes
idmap uid = 10000-20000
winbind gid = 10000-20000
```

```
winbind enum users = yes
winbind enum groups = yes
winbind use default domain = yes
template homedir = /home/%D/%U
template shell = /bin/bash
[homes]
comment = Home Directories
browseable = no
read only = yes
create mask = 0700
directory mask = 0700
valid users = %S ”> /etc/samba/smb.conf
echo ”Configuração alterada com sucesso!”
}
_FUNC_RESTART() {
# Stop Winbind
/etc/init.d/winbind stop > /dev/null
check=$(echo $?)
if [ $check -eq 0 ]; then
echo ”Winbind Stop!”
else
echo ”Falha ao parar o Winbind”
fi
# Restart Samba
/etc/init.d/smbd restart > /dev/null
check=$(echo $?)
if [ $check -eq 0 ]; then
echo ”Samba restart com sucesso!”
```

```
else
echo ”Falha no restart do Samba!”
fi
# Start Winbind
/etc/init.d/winbind start > /dev/null
check=$(echo $?)
if [ $check -eq 0 ]; then
echo ”Winbind start!”
else
echo ”Falha ao fazer iniciar o Winbind!”
fi
}
_ADDDOMINIO () {
echo ”++++++++++++++++++++++++++++++++++++++++++++++”
echo ”++ Adicionando a Máquina no Domínio ++”
echo ”++++++++++++++++++++++++++++++++++++++++++++++”
# Adicionando a máquina ao domínio
read -p ”Entre com um usuário administrador de Domínio:”user
net ads join -U $user;
check=$(echo $?)
clear
# Validação da conexão com o domínio
if [ $check -eq 0 ]; then
echo ”Sua máquina foi adicionada no Domínio!”
else
echo ”Falha ao adicionar a máquina no Domínio”
fi
}
```

```
_TESTDOMINIO () {
# Teste de requisição ao dominio
wbinfo -t > /dev/null
check=$(echo $?)
if [ $check -eq 0 ]; then
echo ”Teste de Domínio!”
else
echo ”Falha ao testar o Domínio”
fi
}
_FUNCAUTENTICACAO () {
# Configurando o arquivo nsswitch.conf
echo ”passwd: compat winbind
group: compat winbind
shadow: compat”> /etc/nsswitch.conf
# Teste de configuração do Winbind
check=$(echo $?)
if [ $check -eq 0 ]; then
echo ”Winbind testado com sucesso!”
else
echo ”Falha ao testar o Winbind”
fi
# PAM - common-account
echo ”account sufficient pam_winbind.so account required pam_unix.so”> /etc/pam.d/common-
account
# PAM - common-auth
echo ”auth sufficient pam_winbind.so
auth sufficient pam_unix.so nullok_secure use_first_pass
```

auth required pam_deny.so”> /etc/pam.d/common-auth

PAM - common-session

echo ”session required pam_unix.so

session required pam_mkhomedir.so umask=0022 skel=/etc/skel”> /etc/pam.d/common-session

PAM - sudo

echo ”auth sufficient pam_winbind.so

auth sufficient pam_unix.so use_first_pass

auth required pam_deny.so

@include common-account”> /etc/pam.d/sudo

Teste de configuração do PAM

check=$(echo $?)

if [$check -eq 0]; then

echo ”PAM configurado com sucesso!”

else

echo ”Falha ao configurar o PAM”

fi

}

_FUNC_HOMEDIR () {

HOME_DIR=$var1

if [-d /home/$HOME_DIR]; then

echo ”Já existe este diretório !”

else

echo ”Este diretório não existe !”

echo ”Criando o diretório $HOME_DIR”

mkdir /home/$var1

sleep 2

fi

```
}
_FUNC_DEL_MAQ_DOMINIO () {
maquina=$(hostname)
echo ”++++++++++++++++++++++++++++++++++++++++++++++”
echo ”++ Removendo a Máquina no Domínio ++”
echo ”++++++++++++++++++++++++++++++++++++++++++++++”
# Remover a máquina ao domínio
read -p ”Entre com um usuário administrador de Domínio:”user
net ads status -U $user
check1=$(echo $?)
clear
# Validação se a máquina está no domínio
if [ $check1 -eq 255 ]; then
echo ”A máquina $maquina não está no dominio”
else
# Validação de remoção de máquina do domínio
net ads leave -U $user;
check=$(echo $?)
clear
if [ $check -eq 0 ]; then
echo ”Sua máquina foi removida do Domínio!”
else
echo ”Falha ao remover a máquina no Domínio”
fi
fi
}
# ====================================================
# Menu de seleção
```

```
echo ”Linux Active Directory:”
echo ”(1) Adicionar Máquina no Domínio”
echo ”(2) Remover Máquina do Domínio”
echo ”(3) Verificar conexão com o Domínio”
echo ”(0) Sair”
echo ”Digite a opção desejada:”
read resposta
case ”$resposta”in
1)
_HEAD
_PACOTES
_HORA
_BACKUP_ORIG
_NOME_DOMINIO
_IP_DNS
_SO_SERVIDOR
_KRB5
_TESTEAD
_SMB
_FUNC_RESTART
_ADDDOMINIO
_TESTDOMINIO
_FUNCAUTENTICACAO
_FUNC_RESTART
echo ”++++++++++++++++++++++++++++++++++++++++++++”
echo ”++ Bem vindo ao dominio $dominio ++”
echo ”++++++++++++++++++++++++++++++++++++++++++++”
;;
```

```
2)
_FUNC_DEL_MAQ_DOMINIO
_RETURN_BACKUP
;;
3)
_TESTDOMINIO
;;
0)
exit
;;
)
echo 'Opção Inválida!'
esac
```

4.12 Windows no domínio Samba 4

5 CONCLUSÕES

5.1 Objetivos alcançados

5.2 Trabalhos futuros