



**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 Bachare-  
lado 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

3.1	Tela do Login no Swat . . . . .	30
3.2	Tela do Login no Windows localmente . . . . .	30
3.3	IP do servidor de compartilhamento . . . . .	31
3.4	IP ou Netbios do servidor de compartilhamento . . . . .	31
3.5	Impressoras e aparelhos de fax compartilhados . . . . .	32
3.6	Propriedades do servidor de impressão . . . . .	33
3.7	Adicionar driver ao servidor de impressão . . . . .	34
3.8	Selecionar o driver que será copiado para o servidor de impressão . . . . .	35
3.9	Selecionar os Sistemas Operacional que o driver será compatível . . . . .	36
3.10	Propriedade da impressora do compartilhamento . . . . .	37
3.11	Opção para não instalar o driver naquele momento . . . . .	38
3.12	Aba onde será feito o link da impressora com o driver . . . . .	38
3.13	Logar no domínio . . . . .	39
3.14	Selecionar a impressora que será mapeado no usuário logado . . . . .	39
3.15	Impressora instalada no usuário . . . . .	40

# SUMÁRIO

<b>1</b>	<b>INTRODUÇÃO</b>	<b>11</b>
1.1	Justificativa do trabalho . . . . .	11
1.2	Objetivo . . . . .	11
1.3	Estrutura do trabalho . . . . .	11
<b>2</b>	<b>CONCEITOS E TÉCNICAS NECESSÁRIAS</b>	<b>12</b>
2.1	Samba . . . . .	12
2.2	Permissões no Linux . . . . .	13
2.3	Seções . . . . .	13
2.4	Parâmetro . . . . .	13
2.5	Variáveis . . . . .	13
2.6	Variáveis Especiais do Samba . . . . .	13
2.7	PDC . . . . .	13
2.8	Comandos Básicos do Samba3 . . . . .	13
2.9	SAMBA-TOOLS . . . . .	13
2.10	SMBD . . . . .	13
2.11	NMDB . . . . .	13
2.12	NETBIOS . . . . .	13
2.13	Domain Master . . . . .	13
2.14	Master Browser . . . . .	14
2.15	WINS . . . . .	14
2.16	BIND . . . . .	14
2.17	Ldap . . . . .	14
2.18	Kerberos . . . . .	14
2.19	NTVFS . . . . .	14
<b>3</b>	<b>SAMBA 3</b>	<b>15</b>
3.1	Instalação do samba . . . . .	15
3.2	Configuração do samba para ser um PDC . . . . .	16

3.3	Cadastro de Usuário . . . . .	18
3.4	Cadastro de Máquinas . . . . .	19
3.5	Script de Cadastro de Usuários e Máquinas . . . . .	20
3.6	Migração dos Usuarios ADM e Users do Linux para o Windows . . . . .	22
3.7	Perfis Moveis . . . . .	23
3.8	Compartilhamento de Arquivos . . . . .	25
3.9	Script Logon . . . . .	26
3.10	Compartilhamento de Impressoras . . . . .	26
3.11	Instalação automática dos drive da impressora . . . . .	28
3.12	Ingressando o Windows XP no Domínio . . . . .	29
3.13	Ingressando o Linux no Domínio . . . . .	29
<b>4</b>	<b>SAMBA 4</b>	<b>41</b>
4.1	Instalação do SAMBA4 . . . . .	41
4.2	Instalação e configuração do BIND9 . . . . .	42
4.3	Instalação do Kerberos . . . . .	44
4.4	Kerberos com Bind9 . . . . .	44
4.5	AD . . . . .	45
4.6	GPO . . . . .	45
4.7	Compartilhamento de arquivos e impressoras . . . . .	45
4.8	Perfil Móvel . . . . .	45
4.9	Gerenciando o Samba4 . . . . .	46
4.10	Maquinas linux e samba3 interagindo com o Active Directory do Samba4 . . .	46
4.11	Script para adicionar maquina linux no Active Directory . . . . .	51
4.12	Windows no domínio Samba 4 . . . . .	64
<b>5</b>	<b>CONCLUSÕES</b>	<b>65</b>
5.1	Objetivos alcançados . . . . .	65
5.2	Trabalhos futuros . . . . .	65

# **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 capítulo 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 um membro do domínio, e pode também ser usado como parte de um domínio Active Directory.

## **2.2 Permissões no Linux**

## **2.3 Seções**

## **2.4 Parâmetro**

## **2.5 Variáveis**

## **2.6 Variáveis Especiais do Samba**

## **2.7 PDC**

## **2.8 Comandos Básicos do Samba3**

## **2.9 SAMBA-TOOLS**

## **2.10 SMBD**

## **2.11 NMDB**

## **2.12 NETBIOS**

## **2.13 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.

## **2.14 Master Browser**

## **2.15 WINS**

## **2.16 BIND**

## **2.17 Ldap**

## **2.18 Kerberos**

## **2.19 NTVFS**

Sistema de arquivos que armazena os atributos do NTFS

## 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.
- **# 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.

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

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

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.

### 3.2 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.

- **# gedit /etc/samba/smb.conf** - Para editar o arquivo e adicionar as seções, parâmetros e variáveis deve-se abrir o arquivo smb.conf.
- **# cat /etc/samba/smb.conf > /etc/samba/smb.conf.bkp** - Por motivo de segurança é recomendado fazer um backup do arquivo.
- **# testparm -s > /etc/samba/smb.conf** - Muitas das linhas desse arquivo são comentários e podem ser removidos.

**\*\*Exemplo do smb.conf**

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

[global]

workgroup = IFFBOMJESUS

```

server string = IFFBJ
security = user
netbios name = battousai-share
encrypt passwords = yes
domain master = yes
domain logons = yes
enable privileges = yes
passdb backend = tdbsam
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.
  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 do usuário e dos dados.
- **netbios name** - Nome da netbios do servidor.
- **encrypt password** - Quando informado a variável "yes" 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 como osmbpasswd, tdbsam ou LDAP. Define qual será a forma de armazenagem dos registros dos usuários.
- **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**

### 3.3 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 usuario** - Comando para a criação mais completa de usuário no linux com nome completo, telefone , entre outros dados.

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

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

### 3.4 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.
- **# 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 máquina.
- **# 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.

### 3.5 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 smbmanager.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.

### 3.6 Migração dos Usuarios ADM e Users do Linux para o Windows

Para que o Windows possa reconhecer os usuários administradores do linux (grupo root) e definir quais grupos serão os 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.

Domain Admins RID=512

Domain Users RID=513

Domain Guests RID=514

RID (Relative Identifier)

- **# net groupmap list** - Lista todos os grupos mapeados no linux.
- **# net groupmap add ntgroup="Domain Admins"rid=512 unixgroup=root** - Irá mapear o grupo root para o grupo Domain Admins do windows.
- **# 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"** - Remove o mapeamento dos grupos.
- **# net groupmap modify ntgroup="Domain Admins"rid=512 unixgroup=root** - Caso tenha necessidade de modificar um mapeamento.

Dessa forma, se o usuário logar como root em algum terminal windows no domínio, ele terá permissões de administrador.

### 3.7 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

- **# rm -r /home/\***
- **# chmod 1777 /home**

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.

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

[profiles]

path = /home

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.

**\*\*FIGURA DO PERFIL MOVEL NO LINUX**

### 3.8 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.
- **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 usuarios.
- **force group** - Força o grupo dos arquivos criados no compartilhamento.
- **create mask** - Permissão dos arquivos que forem criados ou inseridos no compartilhamento
- **directory mask** - Permissão dos diretórios do compartilhamento

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 de usuário que podem escrever na pasta.
- **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.

**\*\*FIGURA DO COMPARTILHAMENTO NO SERVIDOR**

### 3.9 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.

Exemplo:

**Usuário logado : gabriel**

**Grupo primário : dtic**

**Script a ser procurado : dtic.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**

### 3.10 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.

### 3.11 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

### **3.12 Ingressando o Windows XP no Domínio**

### **3.13 Ingressando o Linux no Domínio**

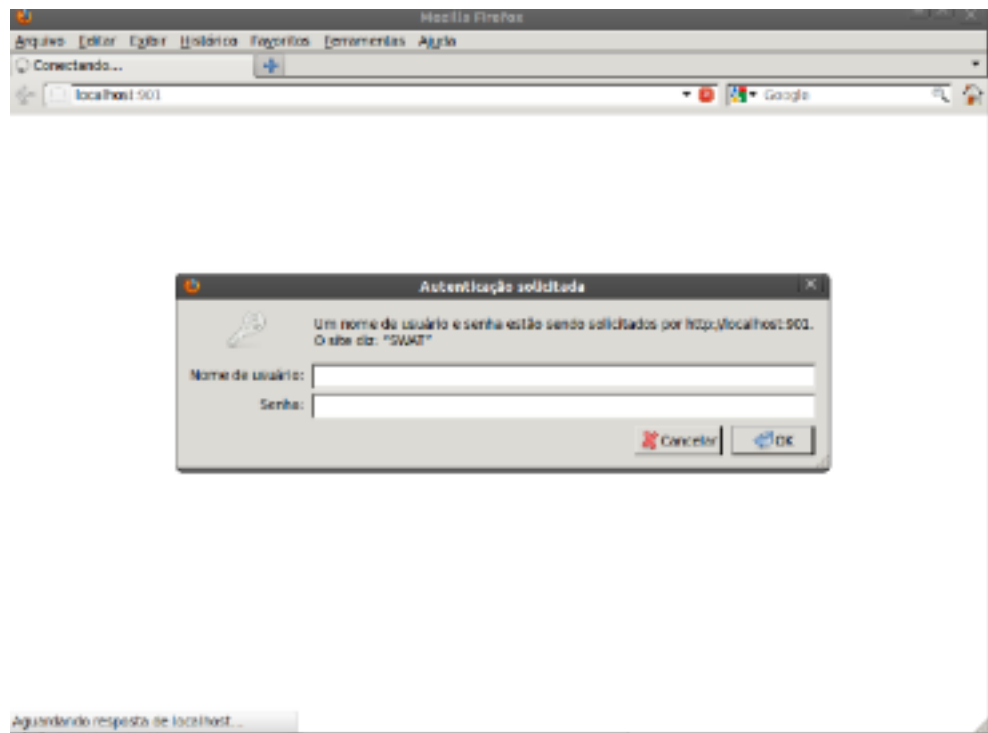


Figura 3.1: Tela do Login no Swat



Figura 3.2: Tela do Login no Windows localmente

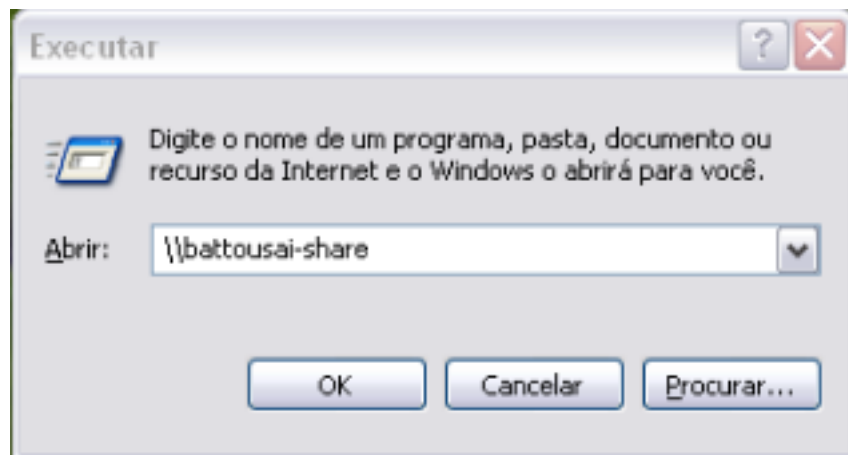


Figura 3.3: IP do servidor de compartilhamento



Figura 3.4: IP ou Netbios do servidor de compartilhamento



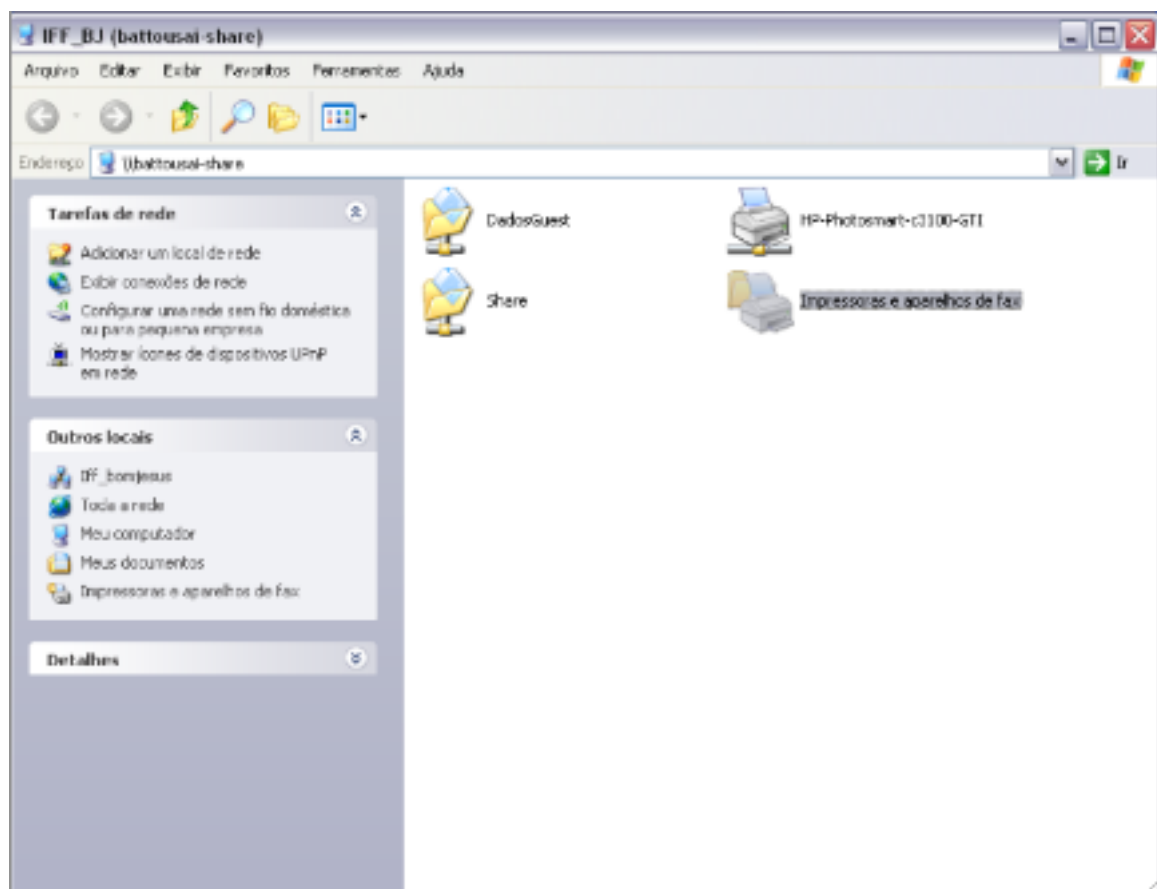


Figura 3.5: Impressoras e aparelhos de fax compartilhados

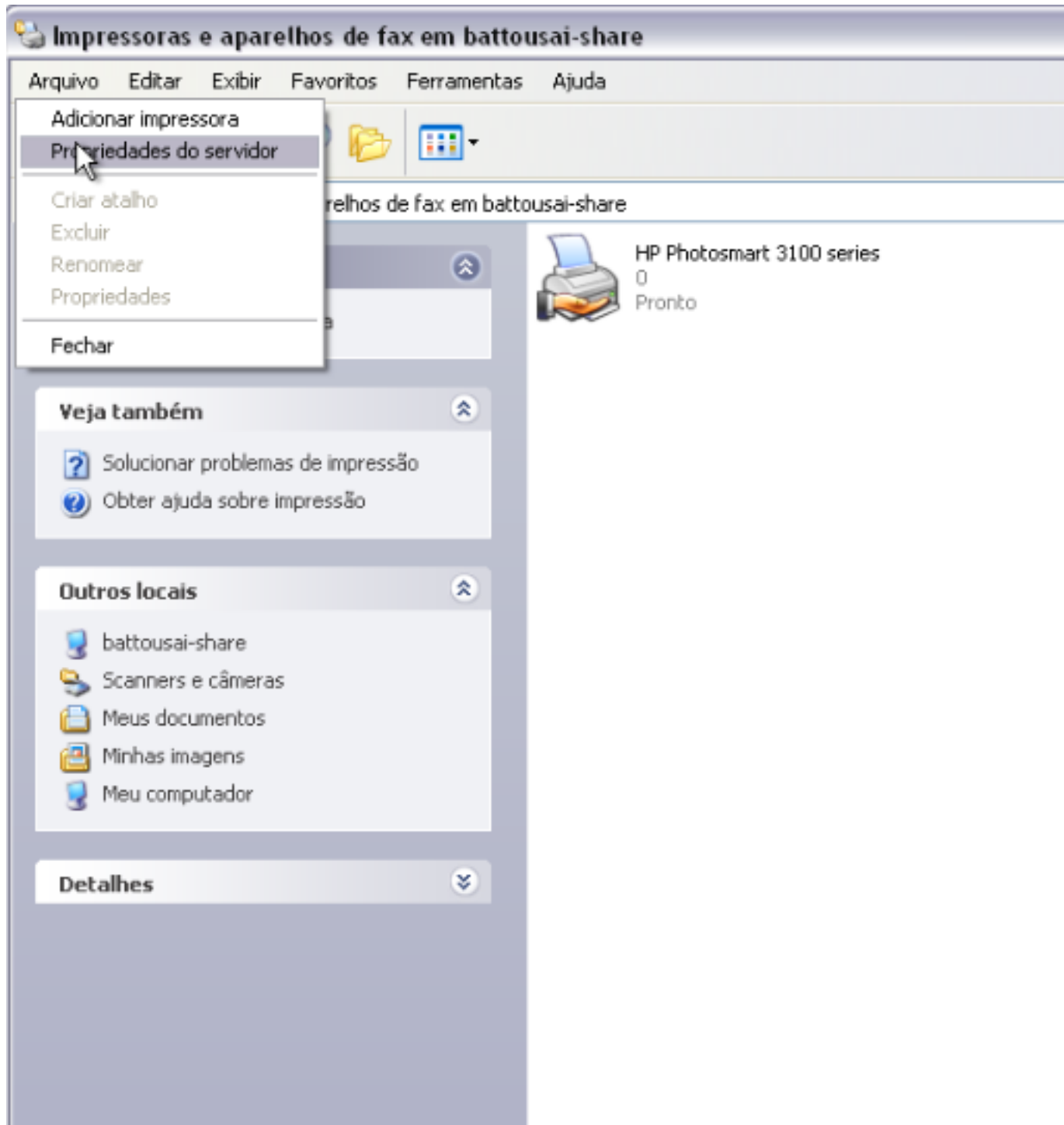


Figura 3.6: Propriedades do servidor de impressão

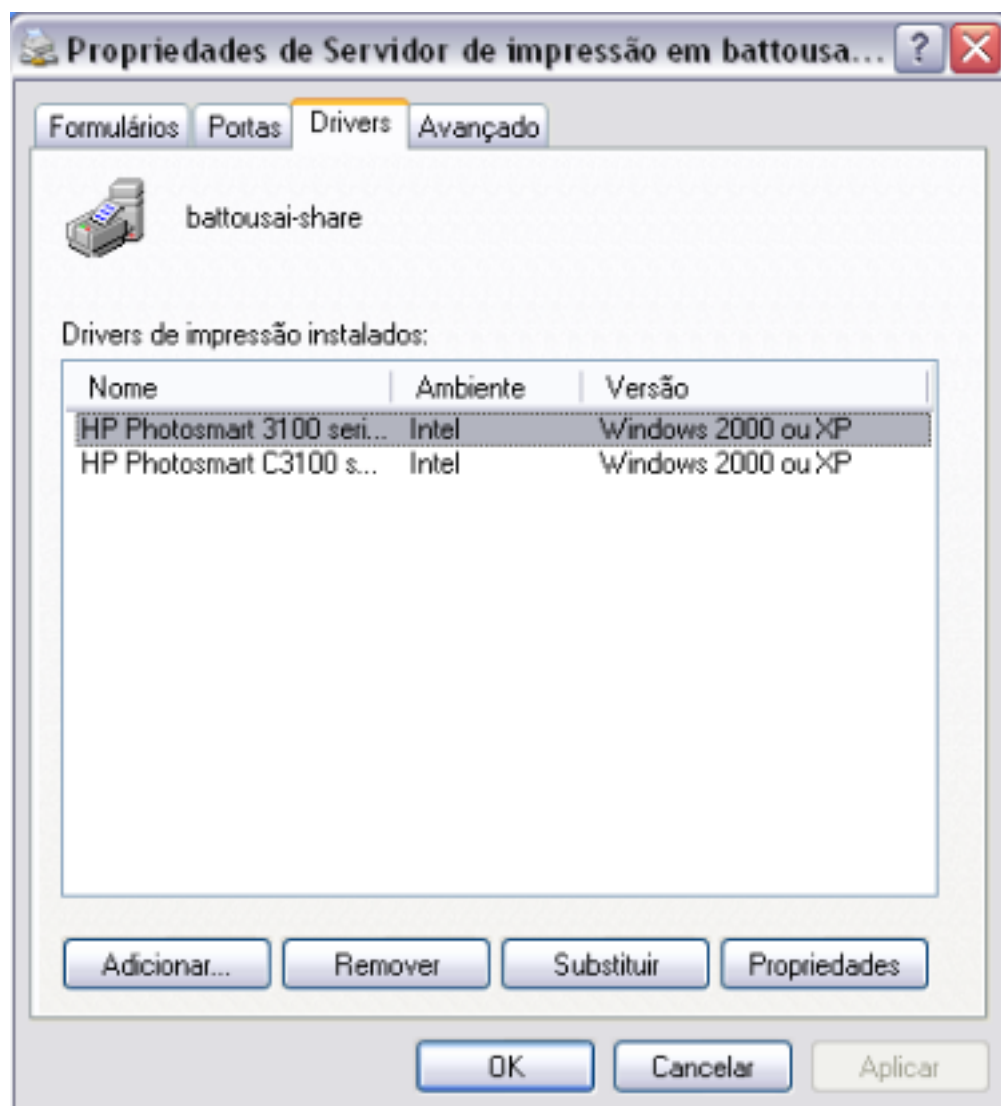


Figura 3.7: Adicionar driver ao servidor de impressão

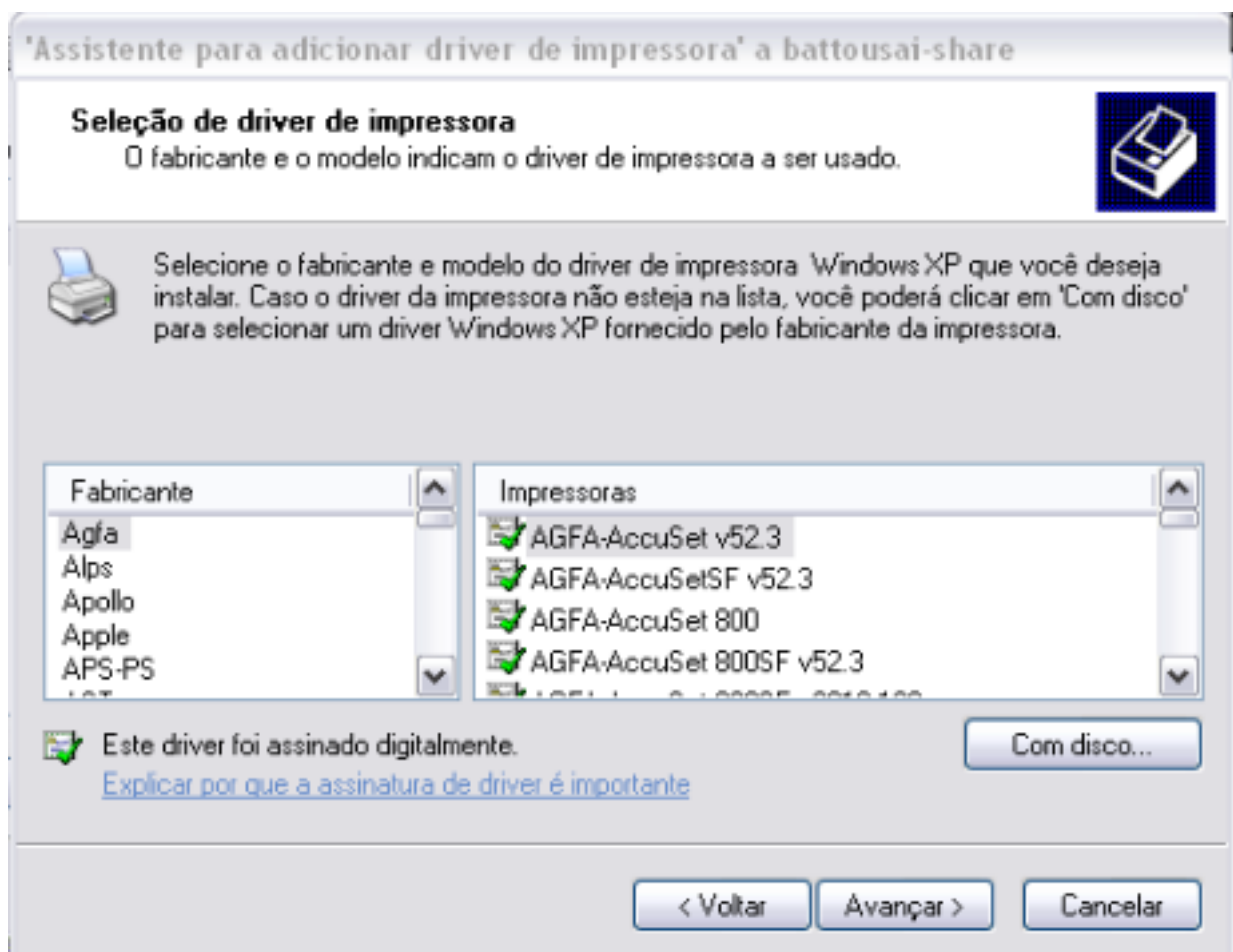


Figura 3.8: Selecionar o driver que será copiado para o servidor de impressão

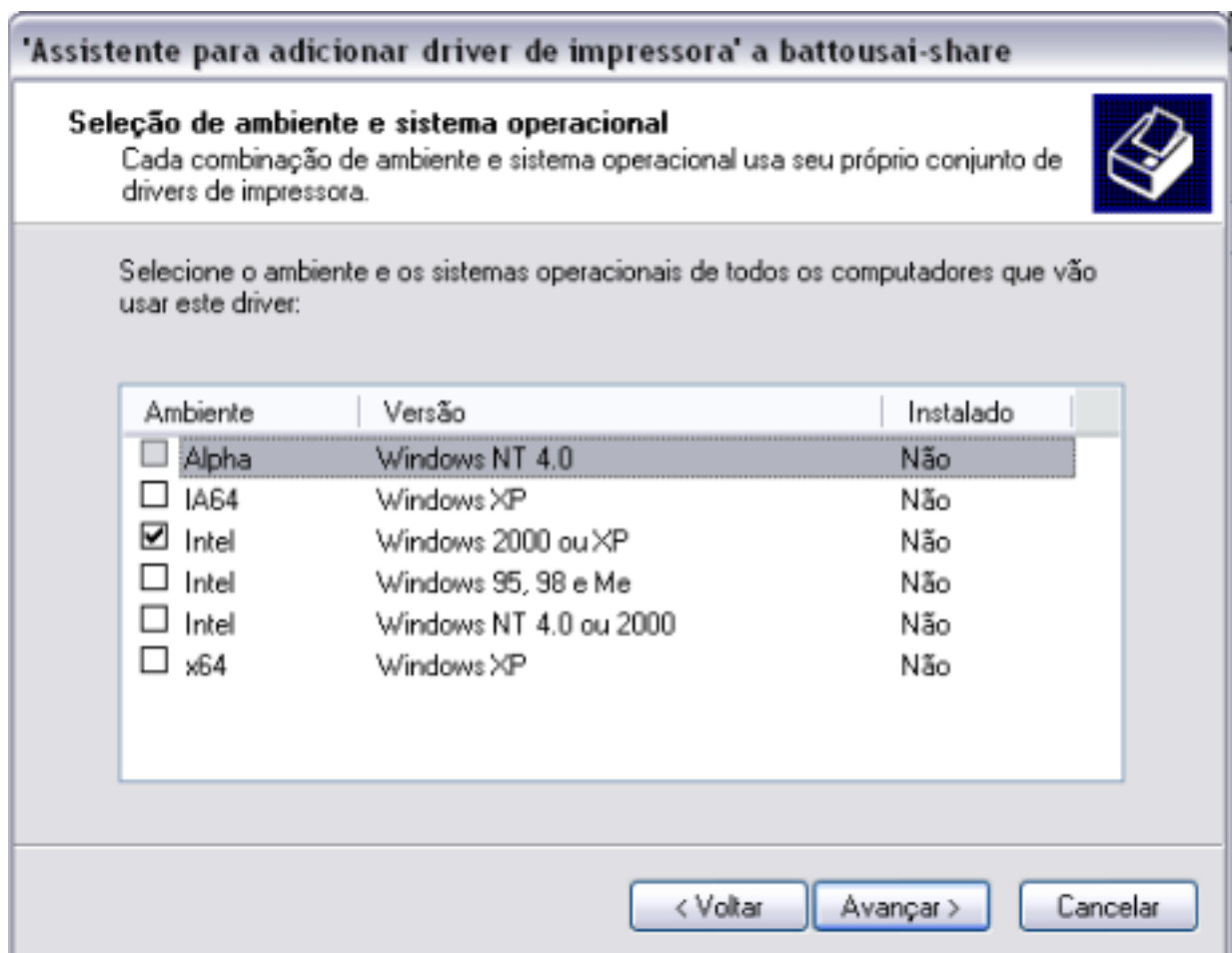


Figura 3.9: Selecionar os Sistemas Operacional que o driver será compatível

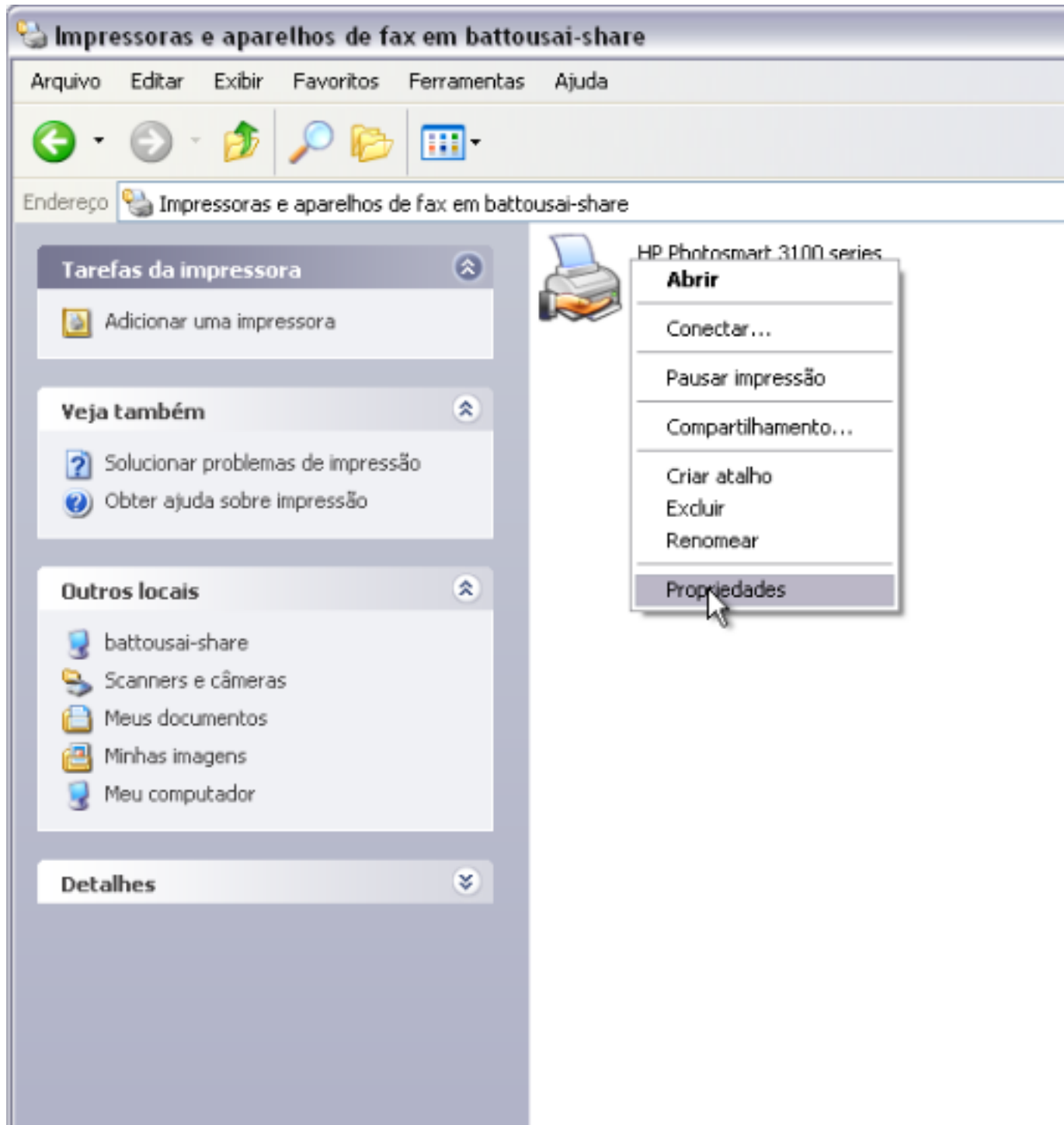


Figura 3.10: Propriedade da impressora do compartilhamento

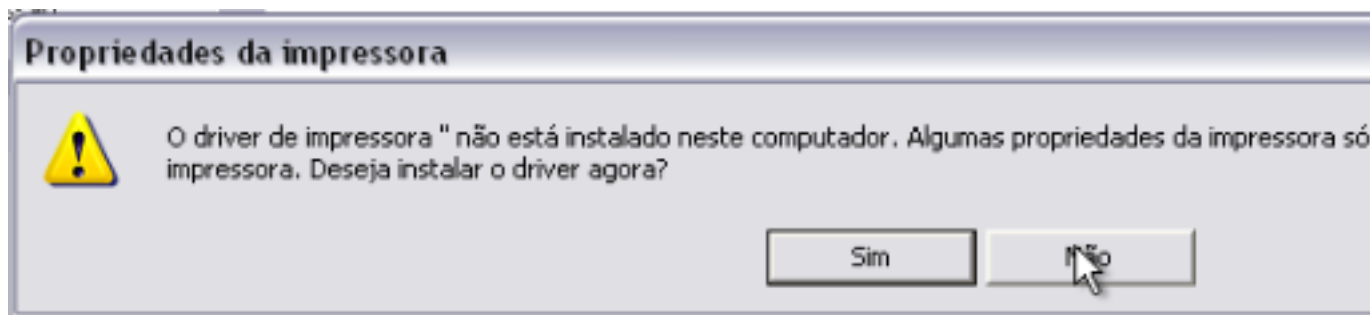


Figura 3.11: Opção para não instalar o driver naquele momento

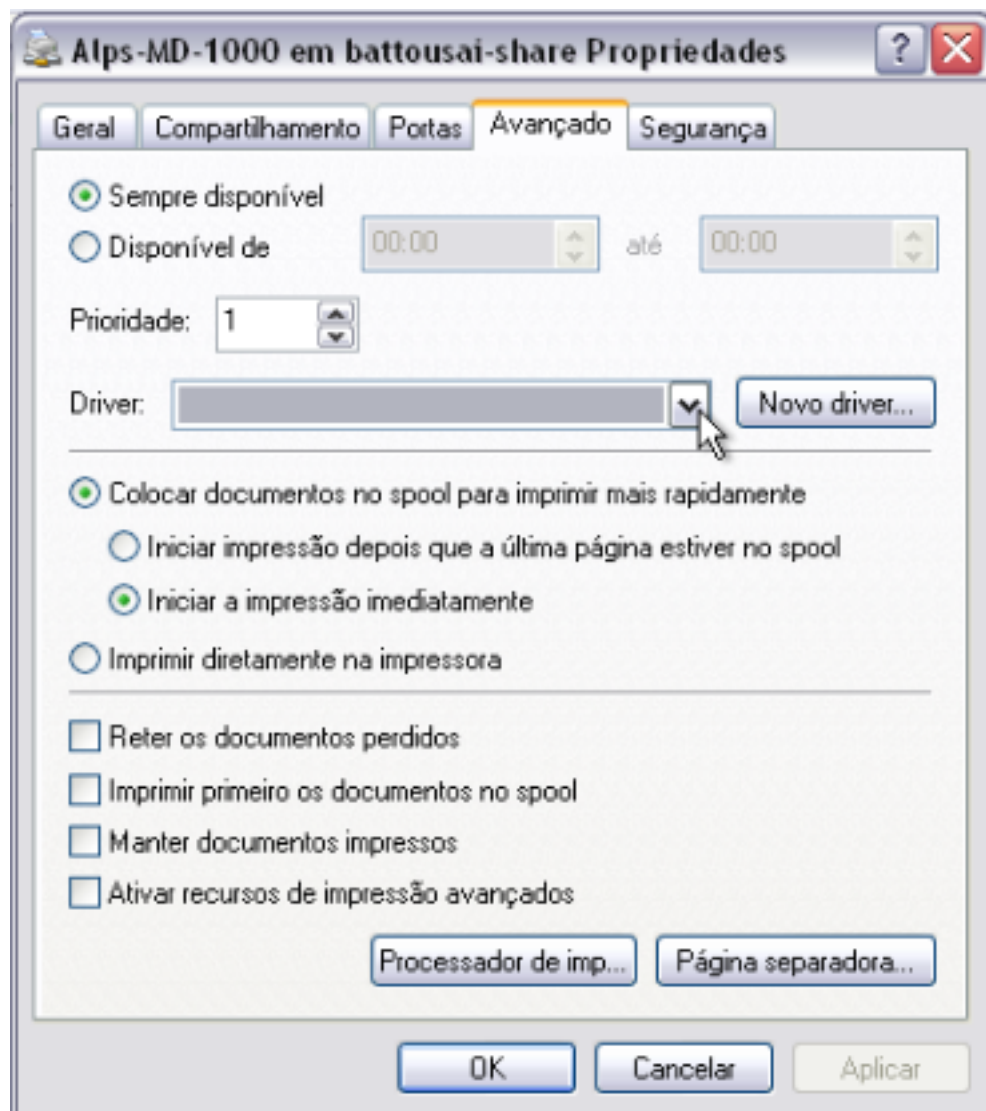


Figura 3.12: Aba onde será feito o link da impressora com o driver



Figura 3.13: Logar no domínio

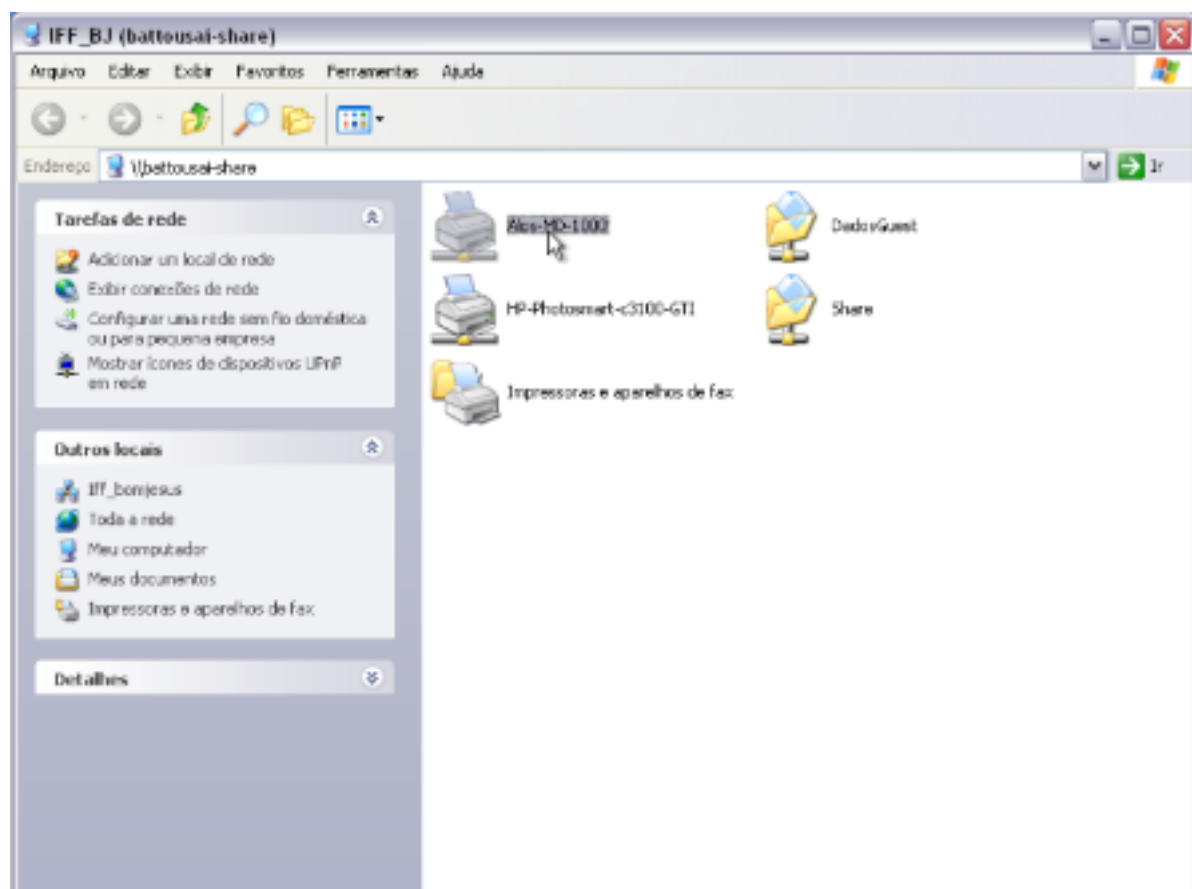


Figura 3.14: Selecionar a impressora que será mapeado no usuário logado



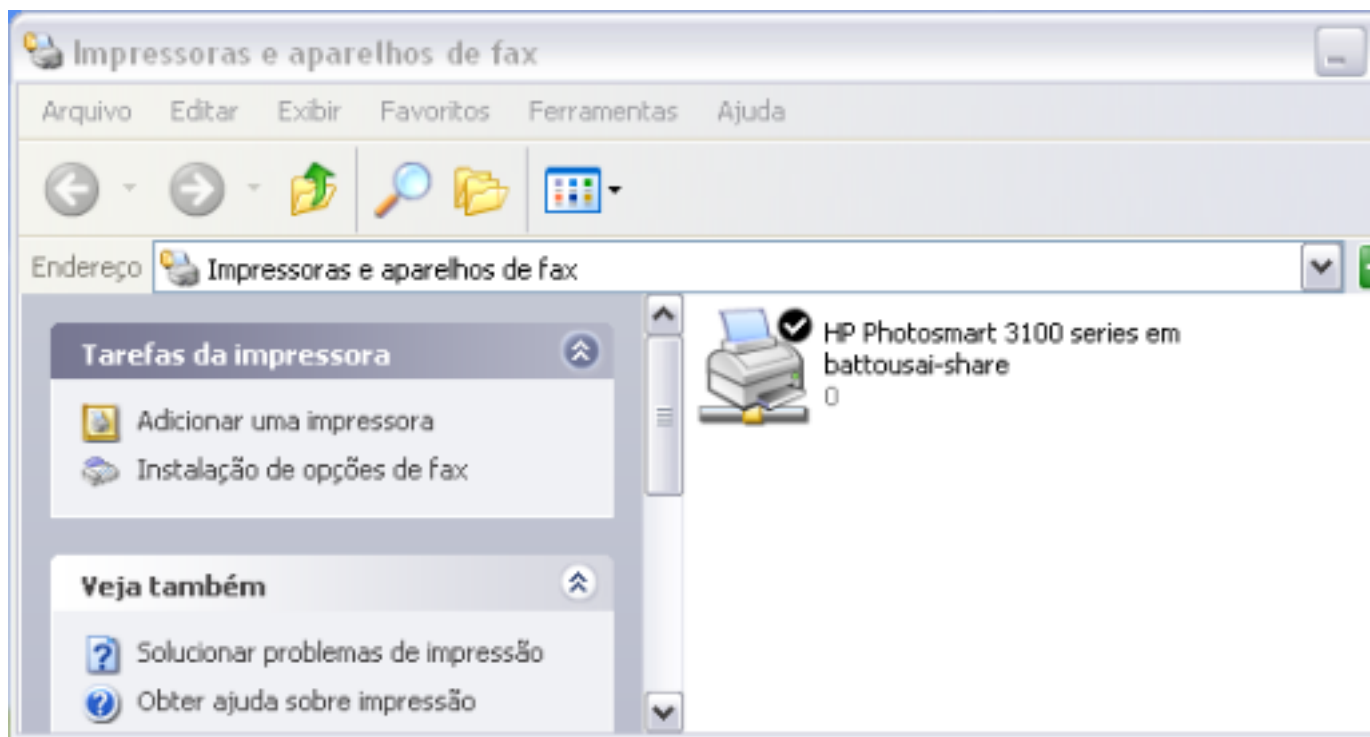


Figura 3.15: Impressora instalada no usuário

## 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

Antes de começar a instalação o relógio do servidor tem que estar atualizado.

- **# ntpdate br.pool.ntp.org** - Atualiza a hora do servidor a partir do servidor br.pool.ntp.org.

Por se tratar de um sistema ainda em fase de produção alguns erros podem aparecer ou alguns parâmetros devem ser modificados.

- **# apt-get install build-essential libattr1-dev libblkid-dev libgnutls-dev python-dev autoconf python-dnspython git-core** - Pacotes necessários para a compilação do samba 4 e download;
- **# git clone git://git.samba.org/samba.git samba-master; cd samba-master** - Faz um clone do samba 4 que esta no repositório para o servidor;
- **# ./configure.developer** - Configurar as bibliotecas com parâmetros de desenvolvedor. Habilitando alguns modos de debug;
- **# make** - Faz uma leitura do comando Makefile;
- **# make install** - Executa os comandos configurados para o parâmetro install do arquivo Makefile;
- **# /usr/local/samba/sbin/provision - -use-ntvfs - -realm=iff.bomjesus - -domain=iff - -adminpass= Senha00 - -server-role='domain controller'** - Cria o domínio samba com AD;
  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.
- **# /usr/local/samba/bin/smbclient -v -version** - Mostra a versão do samba;
  - **# /usr/local/samba/sbin/samba -i -M single** - Inicia o samba 4 com o modo debug;
  - **# echo 'ip do servidor iff.bomjesus iff' >> /etc/hosts** - Define um nome para o ip do servidor.

## 4.2 Instalação e configuração do BIND9

O samba 4 já vem pré configurado para trabalhar com BIND9 para ser o servidor DNS.

- **# wget ftp://ftp.isc.org/isc/bind9/9.9.0/bind-9.9.0.tar.gz** - Download da versão 9.9 do bind9;
- **# tar xzvf bind-9.9.0.tar.gz** - Descompactar o pacote do bind9;
- **# cd bind-9.9.0** - Acessar o diretório do bind9 descompactado;
- **# ./configure --prefix=/usr/local/bind9 --sysconfdir=/etc/bind** - Configurar os parâmetros para a instalação do bind, tais como o local onde vai ser instalado e onde ficarão os arquivos de configuração;
- **# make** - Leitura do comando Makefile;
- **# make install** - Executa os comandos configurados para o parâmetro install do arquivo Makefile;
- **# cd /etc/bind** - Acessar o diretório onde se encontram os arquivos do bind;
- **# vim named.conf** - Cria e edita o arquivo. Adicione as linhas abaixo no arquivo;
  1. **include "/etc/bind/named.conf.options";**
  2. **include "/etc/bind/named.conf.local";**
- **# vim named.conf.options**

1. **Adicionar no arquivo** - options {
  - directory "/var/cache/bind";
  - auth-nxdomain no;
  - listen-on-v6 { any; };
  - };

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";**

Comentar as linhas conforme a versão do bind9

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

# 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;
- **# mkdir /var/cache/bind** - Cria a pasta onde ficarão os caches do bind;
- **# /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.

### 4.3 Instalação do Kerberos

O kerberos a ser instalado é o Heimdal

- **# 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**

### 4.4 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.

## 4.5 AD

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

## 4.6 GPO

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

## 4.7 Compartilhamento de arquivos e impressoras

SAMBA4 ainda não consegue compartilhar arquivos e impressoras, 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.

## 4.8 Perfil Móvel

Muito parecido com o samba3 criar um compartilhamento no samba e dar as devidas permissões a pasta. A diferença se da na hora de definir que será perfil movel.

\*\*\*FIGURA DO AD DEFININDO PERFIL MOVEL\*\*\*

## 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 *Ticketcache : 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

Edite o arquivo /etc/pam.d/common-account adicionando as seguintes linhas

```
sudo vi /etc/pam.d/common-account
```

```
account sufficient pam_winbind.so
```

```
account required pam_unix.so
```

Edite o arquivo /etc/pam.d/common-auth adicionando as seguintes linhas

```
sudo vi /etc/pam.d/common-auth
```

```
auth sufficient pam_winbind.so
```

```
auth sufficient pam_unix.so nullok_secure use_first_pass
```

```
auth required pam_deny.so
```

Edite o arquivo /etc/pam.d/common-session adicionando as seguintes linhas

```
sudo vi /etc/pam.d/common-session
```

```
session required pam_unix.so
```

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

Edite o arquivo /etc/pam.d/sudo adicionando as seguintes linhas

```
sudo vi /etc/pam.d/sudo
```

```
auth sufficient pam_winbind.so
```

```
auth sufficient pam_unix.so use_first_pass
```

```
auth required pam_deny.so
```

```
@include common-account
```

Criando o HOMEDIR do dominio

```
sudo mkdir /home/ADMINISTRATIVO
```

Reinicie os serviços

```
sudo /etc/init.d/winbind stop
```

```
sudo /etc/init.d/samba restart
```

```
sudo /etc/init.d/winbind start
```

Logando no dominio

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

login: alex

Password: \*\*\*\*\*

alex@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

_HEADERS () {
    '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_mkhome.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**