



**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

CHAIANA LAYZA DO NASCIMENTO LIMA
FELIPE DA SILVA FERREIRA
GABRIEL NASCIMENTO MARCOS DA ROCHA

SAMBA 3 E 4 COMO CONTROLADOR DE DOMÍNIO, SERVIDOR DE
ARQUIVOS E DE IMPRESSÃO: UMA ALTERNATIVA LIVRE PERANTE
AS SOLUÇÕES PROPRIETÁRIAS.

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

CHAIANA LAYZA DO NASCIMENTO LIMA
FELIPE DA SILVA FERREIRA
GABRIEL NASCIMENTO MARCOS DA ROCHA

SAMBA 3 E 4 COMO CONTROLADOR DE DOMÍNIO, SERVIDOR DE
ARQUIVOS E DE IMPRESSÃO: UMA ALTERNATIVA LIVRE PERANTE
AS SOLUÇÕES PROPRIETÁRIAS.

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

CHAIANA LAYZA DO NASCIMENTO LIMA
FELIPE DA SILVA FERREIRA
GABRIEL NASCIMENTO MARCOS DA ROCHA

SAMBA 3 E 4 COMO CONTROLADOR DE DOMÍNIO, SERVIDOR DE
ARQUIVOS E DE IMPRESSÃO: UMA ALTERNATIVA LIVRE PERANTE
AS SOLUÇÕES PROPRIETÁRIAS.

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 22 Novembro de 2012

Banca avaliadora:

Prof. Vinicius Barcelos da Silva (Orientador)
Mestre em Engenharia de Produção / UENF
Instituto Federal de Educação, Ciência e Tecnologia Fluminense

Prof. Fernando Luiz de Carvalho e Silva
Mestre em Engenharia de Produção / UENF
Instituto Federal de Educação, Ciência e Tecnologia Fluminense

Prof. José Elias da Silva Justo
Mestre em Pesquisa Operacional e Inteligência Computacional / UCAM-CAMPOS
Instituto Federal de Educação, Ciência e Tecnologia Fluminense

Prof. Rogério Avelar
Mestre em Pesquisa Operacional e Inteligência Computacional / UCAM-CAMPOS
Instituto Federal de Educação, Ciência e Tecnologia Fluminense

Aos nossos 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.

"O começo de todas as ciências é o
espanto de as coisas serem o que são."

Aristóteles

RESUMO

Este trabalho sugere uma proposta de implantação de um servidor de compartilhamento de arquivos, impressoras e um controlador de domínio em uma instituição de ensino, com a missão de facilitar o compartilhamento dos recursos disponíveis de rede, tornando mais seguro e confiável o controle de acesso dos usuários a estes recursos. Mais especificamente, este trabalho implanta o software Samba, nas suas versões 3 e 4, como alternativa livre para soluções proprietárias, como o *Active Directory* da Microsoft, servindo os recursos supracitados tanto para clientes Windows tanto Linux. Também serão apresentados conceitos básicos para a compreensão das ferramentas utilizadas além de passo-a-passo e *scripts* necessários para realizar a implementação de toda a estrutura proposta neste trabalho. Será abordado no trabalho, um estudo de caso da utilização do Samba no Instituto Federal Fluminense de Bom Jesus do Itabapoana, mostrando a ferramenta sendo configurada em um caso real. Por final serão apresentadas as conclusões sobre a tecnologia utilizada e trabalhos futuros.

PALAVRAS-CHAVE: Samba 3, Samba 4, Primary Domain Controller, Servidor de Arquivos, Servidor de Impressão, Software Livre

ABSTRACT

This work suggests a proposal to implant a files and printers sharing server and a domain controller in an educational institution, with mission to facilitate the sharing of available network resources, making safer and reliable the control of user's access to these resources. More specifically, this work implants the Samba software, in versions 3 and 4, as a free alternative to proprietary solutions such as Microsoft Active Directory, serving the resources above to both Windows and Linux clients. Will also be presented basic concepts for the understanding of the tools used in addition to step-by-step instructions and scripts needed to carry out the implementation of the entire structure proposed in this work. Will be addressed in this work, a case study of the use of the Samba software in Instituto Federal fluminense in Bom Jesus do Itabapoana, showing the tool being configured in a real case. By the end we will present the findings on the technology and future work.

KEYWORDS: Samba 3, Samba 4, Primary Domain Controller, File Server, Print Server, Open Source

LISTA DE FIGURAS

2.1	Estrutura do funcionamento da NetBios (MICROSOFT, 2012a)	20
2.2	Estrutura do protocolo LDAP (THE OPENLDAP FOUNDATION, 2003) . . .	21
2.3	Estrutura hierárquica do DNS (MONTEIRO, 2007)	22
2.4	Autenticação Kerberos (ERICOM, 2012)	23
3.1	Tela do SWAT	25
3.2	Saída do testparm	31
3.3	Saída do smbmanager	33
3.4	Tela de um mapeamento	40
3.5	Tela do CUPS pelo Browser	41
3.6	Tela do Login no Windows localmente	44
3.7	IP do servidor de compartilhamento	44
3.8	Impressoras e aparelhos de fax compartilhados	45
3.9	Adicionar driver ao servidor de impressão	46
3.10	Selecionar o driver que será copiado para o servidor de impressão	47
3.11	Selecionar os Sistemas Operacional que o driver será compatível	48
3.12	Propriedade da impressora do compartilhamento	49
3.13	Opção para não instalar o driver naquele momento	49
3.14	Aba onde será feito o link da impressora com o driver	50
3.15	Logar no domínio	51
3.16	Selecionar a impressora que será mapeado no usuário logado	52
3.17	Impressora instalada no usuário	52
3.18	Tela de logon local	53
3.19	Alterando nome do micro	54
3.20	Incluir micro no domínio	55
3.21	Efetuando logon no domínio	56
4.1	Tela do fstab.	59
4.2	Tela para executar o DSA.	62
4.3	Tela do DSA.	62

4.4	samba-tool no terminal.	63
4.5	Tela do script para inserir maquinas linux no AD.	69
4.6	Acessando as Conexões de Rede	70
4.7	Acessando as propriedades da conexão ativa	71
4.8	Incluindo o IP do servidor Samba 4 no campo de DNS	71
5.1	Estrutura da rede do instituto	72

Lista de Tabelas

3.1	Tabela do RID (<i>Relative Identifier</i>) Windows (SAMBA.ORG, 2003)	34
-----	--	----

LISTA DE QUADROS

3.1	Exemplo de utilização das variáveis de substituição	27
3.2	Exemplo do que deve ser inserido no smb.conf	28
3.3	Variáveis necessárias para o perfil móvel	35
3.4	Variáveis para criação do compartilhamento profile	36
3.5	Criação de uma seção para compartilhamento de arquivos	37
3.6	Aplicação de algumas variáveis no Samba 3	38
3.7	Compartilhamento dos <i>scripts</i> de <i>logon</i>	39
3.8	Comando para mapeamento automático de uma pasta compartilhada	40
3.9	Variáveis para permitir impressão em impressoras compartilhadas	40
3.10	Variáveis para compartilhar impressoras	41
3.11	Variáveis para compartilhamento onde deverão ficar os <i>drivers</i> das impressoras	42
3.12	Arquivo smb.conf com as variáveis necessárias para fazer login em um domínio	49
3.13	Arquivo nsswitch.conf	51
3.14	Resultado quando a máquina é adicionada com sucesso no domínio	52
3.15	Exemplo de configuração do /etc/pam.d/login	53
3.16	Linhas do arquivo /etc/pam.d/login	54
3.17	Arquivo /etc/pam.d/gdm	55
4.1	FAZER	60
4.2	FAZER	64
4.3	FAZER	64
4.4	FAZER	65
4.5	FAZER	66
4.6	FAZER	67
4.7	FAZER	68
4.8	FAZER	68
4.9	FAZER	68
4.10	FAZER	68
5.1	FAZER	74

5.2	FAZER	76
-----	-----------------	----

SUMÁRIO

1	INTRODUÇÃO	15
1.1	Objetivo	15
1.2	Justificativa do trabalho	16
1.3	Estrutura do trabalho	17
2	TECNOLOGIAS EMPREGADAS	18
2.1	Samba	18
2.2	PDC	19
2.3	Permissões especiais no Linux	19
2.4	NETBIOS	20
2.5	<i>Active Directory</i>	20
2.6	LDAP	21
2.7	DNS	22
2.8	BIND	22
2.9	Kerberos	22
2.10	GSSAPI	23
3	SAMBA 3	24
3.1	Instalação do Samba 3	24
3.2	SWAT - Gerenciando o Samba 3 pelo browser	24
3.3	Iniciando Samba 3	26
3.4	Seções	26
3.5	Variáveis de substituição do Samba 3	26
3.6	Configuração do Samba para ser um PDC	28
3.7	Cadastro de Usuário	31
3.8	Cadastro de Máquinas	32
3.9	Script de Cadastro de Usuários e Máquinas	32
3.10	Migração dos Usuários Administradores e Users do Linux para o Windows	33
3.11	Perfis Móveis	35

3.12	Compartilhamento de Arquivos	37
3.13	Script Logon	39
3.14	Compartilhamento de Impressoras	40
3.15	Instalação automática dos driver da impressora	42
3.16	Ingressando o Windows XP no Domínio	47
3.17	Ingressando o Linux no Domínio	48
4	SAMBA 4	57
4.1	Instalação do SAMBA 4	57
4.2	Criação de Domínio com o Samba 4	58
4.3	Instalação do Kerberos	61
4.4	Gerenciando o Samba4 através do Windows e do Linux	62
4.5	Maquinas linux interagindo com o <i>Active Directory</i> do Samba4	63
4.6	Script para adicionar maquina linux no <i>Active Directory</i>	69
4.7	Compartilhamento de arquivos	69
4.8	Windows no domínio Samba 4	70
5	ESTUDO DE CASO	72
6	CONCLUSÕES	77
	REFERÊNCIAS BIBLIOGRÁFICAS	78
	Apêndice A – Scripts	80
A.1	smbmanager.sh	80
A.2	smbda.sh	82

1 INTRODUÇÃO

A organização lógica de uma rede é uma necessidade que se torna bem visível quando se possui um cenário com 110 computadores administrativos e entorno de 140 usuários, entre servidores e alunos bolsistas, e a implantação de um domínio se torna indispensável para o gerenciamento mais eficiente desse tipo de recurso. A implantação de um domínio na rede permite que se possa fornecer maior confiabilidade, facilidade de manutenção, controle de recursos e aumento da segurança da informação.

Esses recursos de gerenciamento de domínios são fornecidos através de PDC (*Primary Domain Controller*) e estão disponíveis para os sistemas operacionais mais atuantes do mercado, sendo o AD (*Active Directory*) da Microsoft considerada pelo senso comum a principal e mais utilizada ferramenta para essa finalidade. Pelo fato de ser um *software* proprietário, a solução da Microsoft acaba não sendo a melhor alternativa para muitas organizações pois possui alto custo de utilização e manutenção, e por não permitir a customização dessas ferramentas para que atendam melhor as necessidades de cada cenário distinto.

Recorrendo a ferramentas de *software* livre como o Samba 3 e 4 para obter a mesma solução, as organizações podem ter sem custo os recursos necessários para implantar e gerenciar um domínio em suas redes. Porém, percebe-se uma grande dificuldade na configuração dessas ferramentas, principalmente para usuários não “acostumados” ao Linux, devido ao fato delas apresentarem o terminal de comando e arquivos texto como as principais formas de configuração, não necessitando de interface gráfica para tal. Entretanto, após configurado, o Samba 3 e 4 se mostram capazes de substituir integralmente as ferramentas proprietárias existentes.

1.1 Objetivo

O objetivo deste trabalho é apresentar especificamente a implantação do *software* Samba, em suas versões 3 e 4, como tecnologias livres e viáveis para o gerenciamento de recursos de redes. Diferentemente do Samba 3 que já está estável há vários anos, o Samba 4 ainda esta em fase de desenvolvimento e amadurecimento, mas já demonstra ser promissor

e possivelmente se tornará uma excelente alternativa às principais ferramentas proprietárias existentes no mercado. Além de servir como base para estudo de servidores Linux, este trabalho visa implantar, através de um estudo de caso, um serviço que pretende melhorar o controle da rede no Instituto Federal Fluminense (IFF), especificamente do campus Bom Jesus do Itabapoana, proporcionando maior segurança digital e diminuindo o tempo de manutenção dos incidentes.

1.2 Justificativa do trabalho

A implantação de um servidor de domínio no IFF – Campus Bom Jesus do Itabapoana possibilitará um maior controle dos usuários que acessam o sistema, e assim será possível saber quem está logado, 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 permitirá 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.

O servidor de arquivos permitirá a centralização e compartilhamento de arquivos através da rede, além de aumentar a confiabilidade do armazenamento desses arquivos, possibilitando o fácil *backup* dos dados, e permitindo controle de acesso das informações. Da mesma forma, é possível criar perfis móveis, onde os dados e arquivos dos usuários ficam armazenados no servidor, possibilitando o acesso desses perfis em qualquer computador ligado na rede. Será possível também, embora não seja o foco deste trabalho, a utilização de programas de cotas de impressão, possibilitando definir a quantidade de páginas que um determinado usuário/setor poderá imprimir em um determinado espaço de tempo (diário, semanal, mensal, etc), ou simplesmente fazer o monitoramento das impressões realizadas nas impressoras compartilhadas pelo servidor.

Cabe ressaltar que a escolha do Samba para o campus foi motivada não só visando atender aos aspectos econômicos e legais da Instrução Normativa Nº 1, de 17 de janeiro de 2011, mas também pela história do projeto, pelo desempenho e estabilidade do *software*, por ser um *software* livre, garantindo assim as liberdades do usuário, no caso do campus e da equipe de TI (Tecnologia da Informação) em questão, além da grande comunidade entorno do projeto, que se mostra bastante ativa, disponibilizando bom suporte e grande quantidade de informações através de fóruns e sites especializados.

1.3 Estrutura do trabalho

Este trabalho está dividido em seis capítulos, incluindo a presente introdução. Os demais capítulos estão dispostos da seguinte forma:

O segundo capítulo apresenta uma breve explicação sobre as ferramentas e os termos técnicos utilizados para a implantação que é objetivo deste trabalho.

O terceiro capítulo descreve um passo-a-passo para instalação e configuração do servidor Samba 3, desde o momento do *download* do pacote até o cadastro de usuários, máquinas e a integração com o Windows e Linux.

No quarto capítulo é apresentado um passo-a-passo similar ao do terceiro capítulo, porém utilizando a versão 4 do Samba.

O quinto capítulo apresenta um estudo de caso descrevendo a estrutura da instituição tida como proposta para a implantação do servidor abordado neste trabalho.

O sexto capítulo apresenta as conclusões do estudo, além dos trabalhos futuros que poderão ser realizados a partir deste.

Além dos capítulos descritos acima há uma área destinada aos *scripts* utilizados nas configurações necessárias.

2 TECNOLOGIAS EMPREGADAS

Este capítulo faz uma introdução das tecnologias utilizadas, tais como o Samba, NetBIOS, *Active Directory*, DNS, LDAP, Kerberos, entre outros, além da apresentação de termos técnicos essenciais para o melhor entendimento deste trabalho.

2.1 Samba

Samba é um *software open source* que provê serviços a clientes utilizando os 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, com um controle de permissões de acessos a usuários e grupos juntamente com as permissões locais atribuídas as pastas compartilhadas. Algumas permissões de acesso local serão explicadas no tópico sobre permissões especiais no Linux.
- **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 *LightWeight Directory Access Protocol* (LDAP).
- **Servidor de domínio como PDC** - Funcionando como controlador de domínio ativo dentro de um domínio Windows. Para melhor entendimento ele será explicado no tópico sobre PDC.

Basicamente, o Samba é um servidor e um conjunto de ferramentas que permite o compartilhamento de arquivos e impressoras em sistemas Windows e Linux. Outra característica do Samba é poder atuar como um Controlador Primário de Domínio (PDC), armazenando perfis de usuários e realizar controle de acesso. (FOCA, 2012).

2.2 PDC

O Controlador de Domínio é responsável por fornecer autenticação para os clientes, sejam sistemas Linux ou Windows. Ou seja, apenas centraliza contas de usuários e fornece recursos voltados para a administração de usuários, como a gestão de perfis móveis, que são as configurações de usuários que são lidas, independente de qual máquina o usuário utilize. Em uma rede com mais de 10 clientes a necessidade de ter um PDC é mais aparente, pois fica cada vez mais difícil gerenciar as contas de clientes e máquinas conforme o crescimento da mesma. Com o Controlador de Domínio também é possível fornecer acesso por perfis móveis onde o usuário pode ter acesso à sua área de trabalho independente da máquina (da mesma rede) onde faz o login. Em contrapartida, bloqueando uma conta de usuário, automaticamente este estará bloqueado em todas as máquinas gerenciadas pelo Controlador de Domínio (MORIMOTO, 2005)

2.3 Permissões especiais no Linux

Existe no Linux três permissões especiais, para dar segurança ao sistema, chamadas assim por somente serem atribuídas a arquivos específicos (arquivos executáveis e diretórios). Tais permissões são fornecidas pelos bits SUID, SGID e STICKY.

- **SUID** - O bit SUID (Set UID) é aplicável apenas a arquivos executáveis, fazendo com que estes rodem com as permissões de seu proprietário, independente de quem tenha executado-o. Pode ser útil para que usuários comuns possam executar arquivos permitidos apenas a administradores.
- **SGID** - O bit SGID (Set GID) pode ser aplicado a um arquivo executável e a um diretório. No primeiro caso ele tem a mesma função do SUID, porém rodando com as permissões de um grupo de usuários. No segundo, ele força os arquivos e diretórios criados dentro do diretório pai (o que obteve a permissão) a pertencerem ao mesmo grupo, independente do grupo de quem o tenha criado.
- **STICKY** - O bit STICKY é aplicável a diretórios e faz com que a exclusão de arquivos pertencentes a estes diretórios seja apenas permitida ao dono do arquivo e ao administrador do sistema. Tem vantagem sobre a permissão “Somente Leitura” no diretório pois faz com que outros usuários possam criar e editar qualquer arquivo, impedindo-os apenas de apagá-lo.

É importante ressaltar que de nada adiantará se os arquivos e diretórios possuírem determinadas permissões locais se as concedidas através do Samba não forem compatíveis às

permissões atribuídas. Por exemplo: de nada adiantará atribuir acesso de escrita a um arquivo no Linux se ele possui permissão “Somente Leitura” no Samba. A atribuição mais negativa, ou seja, a que concede menos permissões (neste caso a “Somente Leitura”) prevalecerá sobre a outra.

2.4 NETBIOS

Um nome NetBIOS é um endereço de 16 bytes usado para identificar um recurso NetBIOS na rede. Um nome NetBIOS é um nome único (exclusivo) ou de grupo (não exclusivo). Quando um processo de NetBIOS está comunicando-se com um processo específico em um computador específico, é usado um nome exclusivo. Quando um processo de NetBIOS está comunicando-se com vários processos em vários computadores, é usado um nome de grupo. A resolução de nomes NetBIOS significa o mapeamento bem-sucedido de um nome NetBIOS para um endereço IP. (MICROSOFT, 2012a)

O NetBIOS trabalha na camada sessão do modelo OSI (*Open Systems Interconnection*), e utiliza as portas de comunicação UDP (*User Datagram Protocol*) 137 e 138 para a resolução dos NetBios *names* e *datagrams* e 139 de comunicação TCP (*Transmission Control Protocol*) para NetBios *sessions*, conforme a Figura 2.1

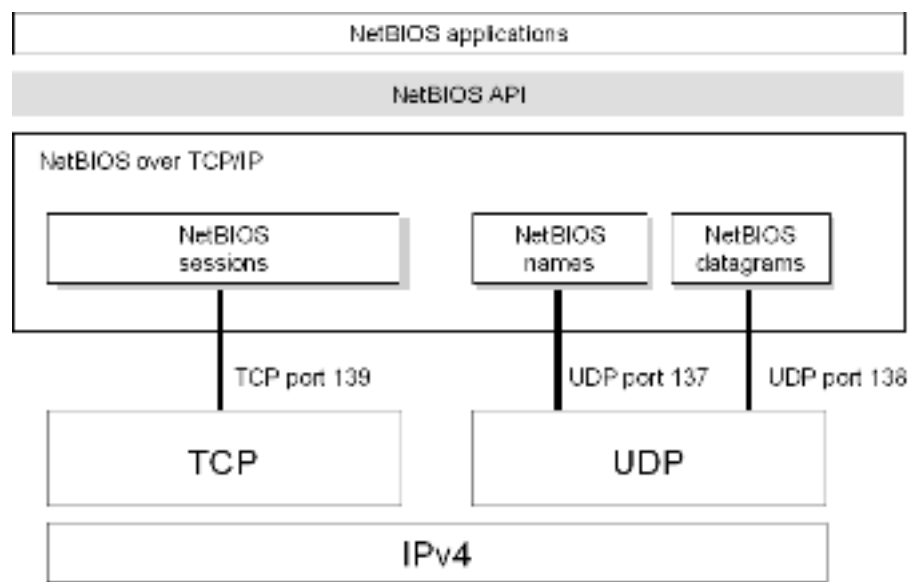


Figura 2.1: Estrutura do funcionamento da NetBios (MICROSOFT, 2012a)

2.5 Active Directory

O *Active Directory* (AD) é um serviço de diretório nas redes a partir do Windows 2000. Serviço de diretório é um conjunto de atributos sobre recursos e serviços existentes na

rede, isso significa que é uma maneira de organizar e simplificar o acesso aos recursos da rede, centralizando-os; bem como, reforçar a segurança e dar proteção aos objetos da base de dados contra intrusos, ou controlar acessos dos usuários internos da rede.

O *Active Directory* mantém dados como contas de usuários, impressoras, grupos, computadores, servidores, recursos de rede, etc. Ele pode ser totalmente escalonável, aumentando conforme a necessidade.(LOSANO, 2009)

2.6 LDAP

O LDAP (*Lightweight Directory Access Protocol*) é o protocolo responsável por fornecer Serviço de Diretórios a computadores Windows de forma similar ao *Active Directory* da Microsoft, que é baseado no LDAP. Tais serviços incluem conexões de computadores, grupos de computadores, usuários, administração de identidades, além de possibilitar uma maneira eficiente de descrever, localizar e administrar esses recursos. Essa estrutura do LDAP pode ser vista na Figura 2.2

LDAP é um protocolo para acessar informações contidas em um diretório. Por ser um protocolo cliente/servidor o LDAP permite navegar, ler, armazenar e pesquisar informações e realizar tarefas de gerenciamento em um serviço de diretórios. O serviço de diretório é um banco de dados otimizado para leitura, navegação e pesquisas (TRIGO, 2007).

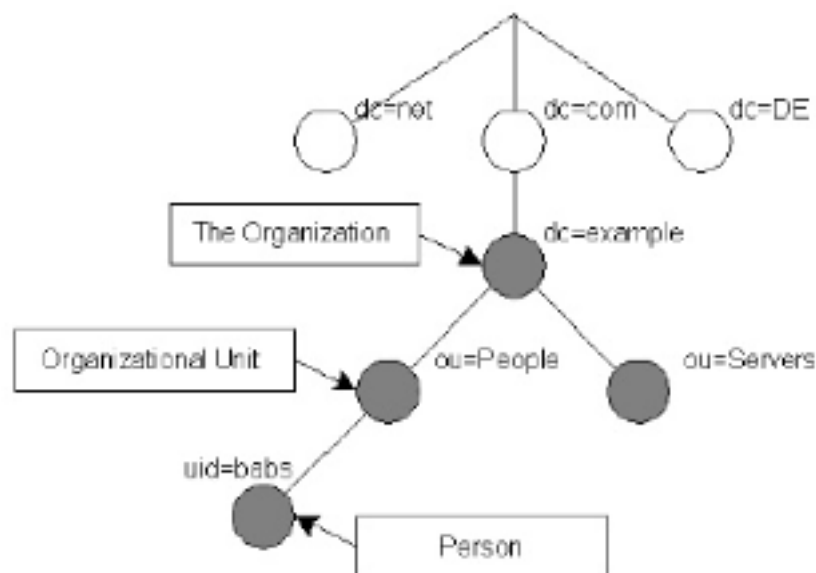


Figura 2.2: Estrutura do protocolo LDAP (THE OPENLDAP FOUNDATION, 2003)

2.7 DNS

DNS (*Domain Name System*) é uma base de dados hierárquica e distribuída, usada para a resolução de nomes de domínios em endereços IP (*Internet Protocol*). É considerado como um banco de dados distribuído que converte nomes de *hosts* (máquinas) para endereços IP. É basicamente um mapeamento de endereços IP e seus respectivos nomes. A utilização mais comum é na internet. Todos os computadores da rede possuem um endereço IP. Os servidores DNS simplesmente transformam ou resolvem esse número em um nome (SCRIMGER PAUL LASALLE, 2002). Por exemplo, o endereço `www.iff.edu.br` corresponde ao IP `200.143.198.110`. Exemplos de domínios DNS que podem ser visto na Figura 2.3

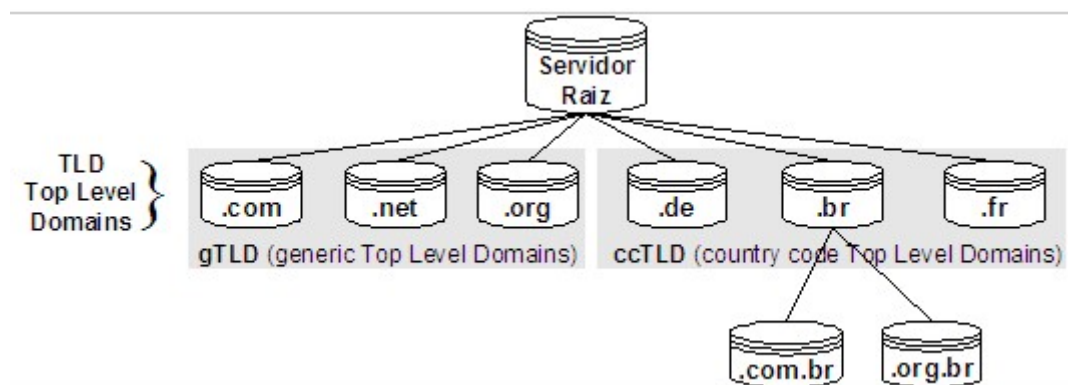


Figura 2.3: Estrutura hierárquica do DNS (MONTEIRO, 2007)

2.8 BIND

BIND é um *software* de código livre que implementa o Sistema de Nomes de Domínio (DNS) de protocolos para a internet. É uma referência em implementação desses protocolos, mas também possui uma produção em série de *software*, adequado para uso em aplicações de alto volume e de alta confiança. BIND está disponível para *download* gratuito sob os termos da Licença ISC, um estilo de licença BSD. (INTERNET SYSTEMS CONSORTIUM, 2012).

2.9 Kerberos

Kerberos é um protocolo de segurança de rede e fornece autenticação entre computadores e usuários através de um servidor centralizado que concede autenticações criptográficas a qualquer computador utilizando o Kerberos. Esse sistema de segurança e autenticação agrega diversos benefícios como autenticação mútua, autenticação delegada, interoperabilidade e gerência simplificada e confiável. O samba pode usar o Kerberos como um mecanismo autenticação de computadores e usuários.

O Kerberos é um protocolo que prevê forte autenticação entre aplicações cliente-servidor e usa criptografia de chave simétrica no qual servidores fornecem acesso aos serviços solicitados pelos clientes, caso provem que são eles mesmos. (FILHO, 2009)

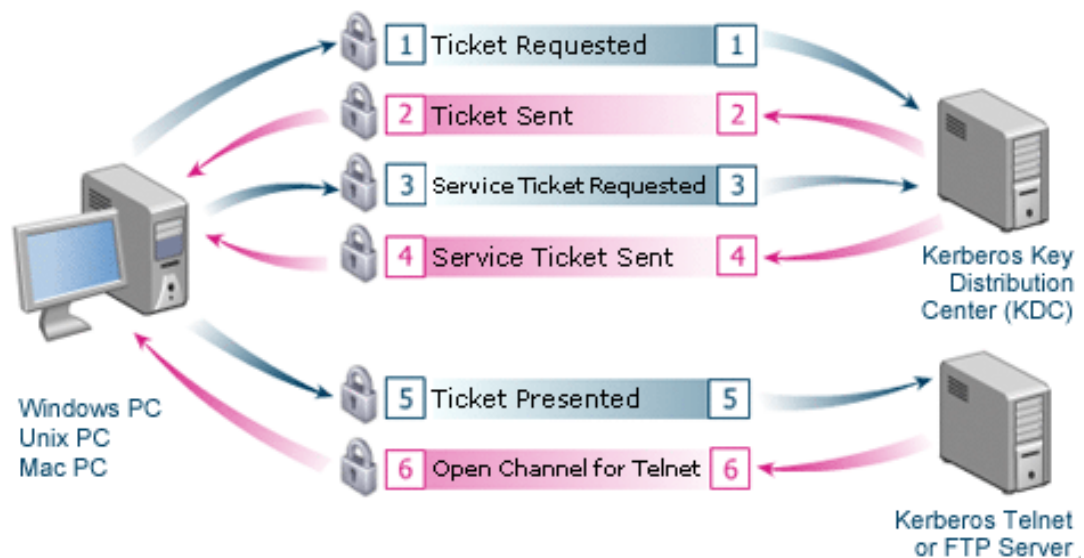


Figura 2.4: Autenticação Kerberos (ERICOM, 2012)

2.10 GSSAPI

A GSSAPI é uma interface que permite aos 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. (CUFFA, 2010)

3 SAMBA 3

Este capítulo descreve como são feitas a instalação e a configuração de um servidor Samba 3 como controlador de domínio, servidor de impressão e servidor de arquivos, respeitando as regras de usuários e permissões.

3.1 Instalação do Samba 3

O pacote Samba 3 pode ser instalado através do repositório de sistemas da distribuição Linux na qual será configurado (neste trabalho foram utilizadas as distribuições Ubuntu 11.04 e Debian 6.0.5). Antes da instalação é necessário atualizar a base de dados do repositório para que possa instalar a versão mais atual do Samba 3.

1. **# apt-get update** - Atualiza a base de dados do repositório no Ubuntu.
2. **# apt-get install samba** - Realiza a instalação do pacote Samba 3.
3. **# apt-get install smbclient** - Pacote que mostra as informações do servidor Samba 3 e permite acesso de compartilhamentos no windows ou linux a partir de uma máquina linux.

3.2 SWAT - Gerenciando o Samba 3 pelo browser

O SWAT é uma ferramenta para a edição do `/etc/smb.conf`, porém por meio de uma interface gráfica. Com ele é possível compartilhar impressoras, arquivos, criar usuários, permitir ou restringir acessos.

1. **# apt-get install swat** - Instala a ferramenta gráfica SWAT para o gerenciamento do Samba 3.
2. **\$ firefox localhost:901** - Endereço de acesso no *browser* (neste caso o Firefox) para acessar o SWAT.

Ao acessar o SWAT pelo navegador, o usuário deve informar o usuário root e sua senha. Após o login no sistema, pode-se observar na barra de ferramentas as opções de configuração do SWAT, conforme Figura 3.1. A função de cada opção é detalhada a seguir:

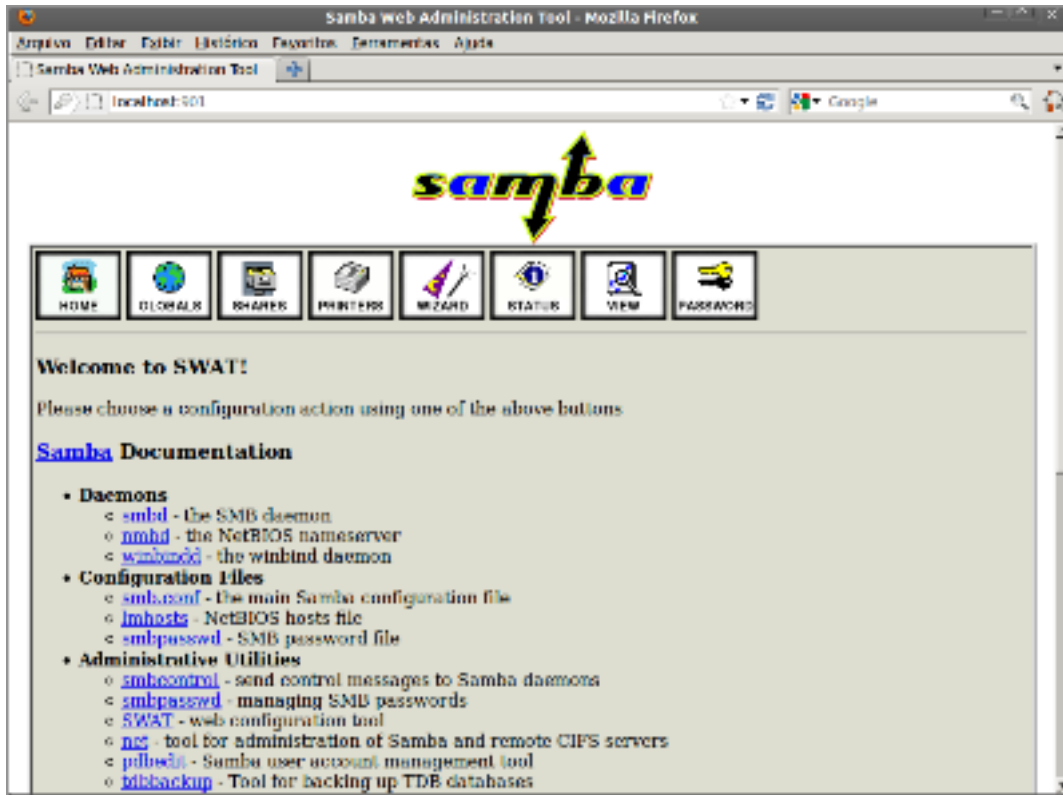


Figura 3.1: Tela do SWAT

- **Home** - Documentação do Samba 3
- **Globals** - Variáveis globais de configuração do Samba 3
- **Shares** - Ativar compartilhamentos de diretórios e arquivos
- **Printers** - Compartilhamento de impressoras
- **Wizard** - Escreve as modificações no arquivo smb.conf do Samba 3
- **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

Por se tratar de uma ferramenta gráfica o SWAT torna mais fácil a edição e adição de configurações no smb.conf, mas toda vez que as configurações são alteradas e salvas ele gera um novo arquivo smb.conf e com isso apaga todos os possíveis comentários existentes no

arquivo. Por se tratar de um arquivo com muitas variáveis, parâmetros e seções, nesse trabalho o foco será a edição através de editores de texto padrão como o “vim”, pois assim algumas configurações podem ser inseridas como comentários para fins de explicação ou como base para futuras modificações.

3.3 Iniciando Samba 3

Com todos os componentes instalados a aplicação pode ser iniciada. O Samba 3 trabalha com dois *daemon* principais, geralmente eles se encontram no `/usr/sbin/`, que são: SMBD e o NMBD

O SMBD permite compartilhamento de arquivos e impressoras em uma rede SMB e provê autorização e autenticação a usuários SMB. O NMBD cuida do *Windows Internet Name Service* (WINS) e auxilia com a navegação e resolução de nomes.(ECKSTEIN DAVID COLLIER-BROWN, 2003)

Existem varias formas de iniciar e parar os processos do Samba 3, que como:

- **# /etc/init.d/smbd start** - Inicia o Samba 3.
- **# service smb start** - Inicia o Samba 3.
- **# service smb stop** - Para o processo do Samba 3.
- **# /etc/init.d/samba start** - Para iniciar o Samba 3 em computadores com Debian 6.

3.4 Seções

No Samba 3, as configurações de compartilhamentos, impressoras e gerais, são realizadas através de um único arquivo de configuração, o “`/etc/samba/smb.conf`”. Esse arquivo para melhor organização, fica dividido 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 for necessário criar um compartilhamento com o nome “arquivo”, a sessão que deve ser criada no arquivo de configuração deve ser `[arquivo]`.

3.5 Variáveis de substituição do Samba 3

Existem variáveis especiais que podem ser usadas no arquivo de configuração do Samba 3 e são substituídas por parâmetros especiais no momento da conexão do usuário (FOCA,

2012). Um exemplo de utilização de variáveis de substituição seria mudar a localização do diretório home do usuário conforme no Quadro 3.1:

<pre>[home] comment = Diretorio home do usuario path = /home/usuarios/%u</pre>
--

Quadro 3.1: Exemplo de utilização das variáveis de substituição

Ao longo deste trabalho diversas variáveis de substituição serão utilizadas, principalmente nos scripts aqui propostos. Cada uma das variáveis são descritas em detalhes a seguir:

%S - O nome do serviço atual, se existir. Seu uso é interessante, principalmente no uso de diretórios homes.

%P - O diretório raiz do serviço atual, se existir.

%u - O nome de usuário do serviço atual, se aplicável. Esta variável é bastante útil para programação de scripts e também para criar arquivos de log personalizados, etc.

%g - O grupo primário do usuário **%u**.

%U - O nome de usuário da seção (o nome de usuário solicitado pelo cliente, não é uma regra que ele será sempre o mesmo que ele recebeu).

%G - O nome do grupo primário de **%U**.

%H - O diretório home do usuário, de acordo com **%u**.

%v - A versão do Samba.

%h - O nome DNS da máquina que está executando o Samba.

%m - O nome NetBIOS da máquina do cliente. Isto é muito útil para log de conexões personalizados e outras coisas úteis.

%L - O nome NetBIOS do servidor. Como o servidor pode usar mais de um nome no Samba (aliases), você poderá saber com qual nome o seu servidor está sendo acessado e possivelmente torna-lo o nome primário de sua máquina.

%M - O nome DNS da máquina cliente.

%N - O nome do seu servidor de diretórios home NIS. Este parâmetro é obtido de uma entrada no seu arquivo auto.map. Se não tiver compilado o SAMBA com a opção `-with-automount` então este valor será o mesmo de

%p - O caminho do diretório home do serviço, obtido de uma entrada mapeada no arquivo auto.map do NIS. A entrada NIS do arquivo auto.map é dividida na forma “%N:%p”.

%R - O nível de protocolo selecionado após a negociação. O valor retornado pode ser CORE, COREPLUS, LANMAN1, LANMAN2 ou NT1.

%d - A identificação de processo do processo atual do servidor.

%a - A arquitetura da máquina remota. Somente algumas são reconhecidas e a resposta pode não ser totalmente confiável. O Samba atualmente reconhece Samba, Windows for Workgroups, Windows 95, Windows NT e Windows 2000. Qualquer outra coisa será mostrado como “UNKNOWN” (desconhecido).

%I - O endereço IP da máquina do cliente.

%T - A data e hora atual.

%(var_ambiente) - Retorna o valor da variável de ambiente especificada.

3.6 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.

1. **# cp /etc/samba/smb.conf /etc/samba/smb.conf.bkp** - Por motivo de segurança é recomendado fazer um backup do arquivo. Ele contém exemplos comentados das possíveis configurações do Samba 3, auxiliando o profissional de TI no momento de sua configuração.
2. **# testparm -s /etc/samba/smb.conf.bkp > /etc/samba/smb.conf** - Removerá os comentários para melhor leitura do arquivo. Observação: o arquivo de origem não pode ser o smb.conf pois ele irá se sobrescrever e o arquivo só conterá a seção [global] vazia.
3. **# gedit /etc/samba/smb.conf** - Para editar o arquivo e adicionar as seções, parâmetros e variáveis.

Agora é necessário inserir, modificar e remover alguns parâmetros na seção [global] para que o Samba 3 se comporte como um PDC. Conforme o Quadro 3.2

```
[ global ]

workgroup = 'nome do servidor de dominio'

server string = 'Titulo'
```

```

security = user

netbios name = 'nome que sera 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

map to guest = Bad User

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

```

Quadro 3.2: Exemplo do que deve ser inserido no smb.conf

Explicação das variáveis utilizadas:

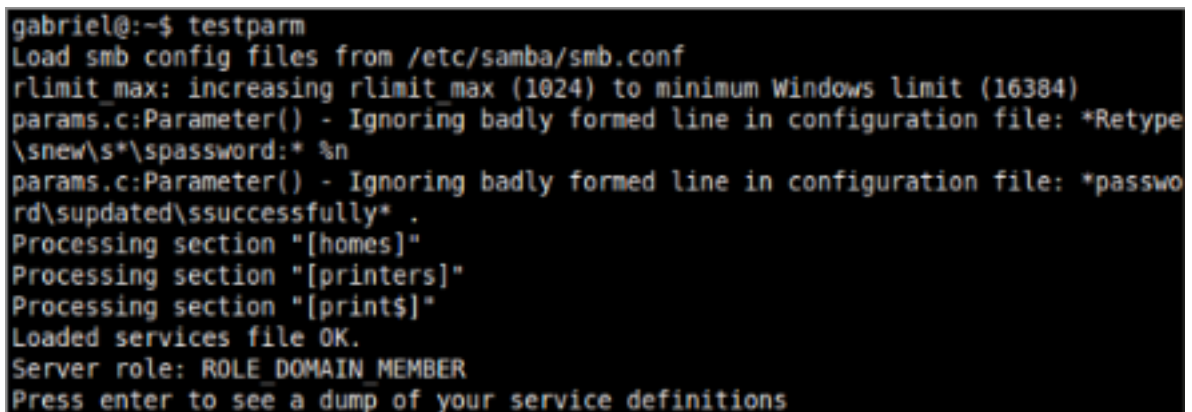
- **workgroup** - Nome do servidor de domínio.
- **server string** - Descrição do servidor que aparece na barra de título das janelas do compartilhamento.
- **security** - Tipo de segurança do compartilhamento. Existem os tipos domain, user e share.
 1. share - É utilizado quando o compartilhamento será 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 o valor "true" as senhas informadas para o servidor serão criptografadas.
- **domain master** - Informa que o servidor Samba 3 será o domínio principal da rede.
- **domain logons** - O servidor Samba 3 passa a ser um controlador de domínio.
- **enable privileges** - Habilita alguns privilégios no Samba 3. Alguns deles:
 1. SeAddUsersPrivilege - Adicionar usuários e grupos no domínio
 2. SeDiskOperatorPrivilege - Gerencia os discos compartilhados
 3. SeMachineAccountPrivilege - Adicionar máquinas 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 - 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. (MORIMOTO, 2008)
 2. tdbsam - O tdbsam usa uma base de dados muito mais robusta, armazenada no arquivo "/var/lib/samba/passdb.tdb". (MORIMOTO, 2008)
 3. Diferença entre smbpasswd e tdbsam - 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 (*Software Asset Management*) 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. Ele é também um pré-requisito caso você precise migrar um domínio NT já existente para o servidor Samba. (MORIMOTO, 2008)
- **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" os servidores windows.
- **map to guest** - Torna usuário guest todos que não conseguirem se identificar com um login e senha válida.

- **panic action** - Comando que será executado caso o `smbd` ou `nmbd` parem de funcionar.

Com todas as variáveis devidamente adicionadas o servidor Samba 3 precisa ser reiniciado para que todas as modificações entrem em vigor.

1. **# testparm** - Verifica se existe algum erro de sintaxe no arquivos de configuração no `smb.conf`. Exemplo de execução que pode ser visto na Figura 3.2
2. **# /etc/init.d/smbd restart** - Reinicia o Samba 3.
3. **# /etc/init.d/nmbd restart** - Reinicia o servidor de nomes do Samba 3.



```
gabriel@:~$ testparm
Load smb config files from /etc/samba/smb.conf
rlimit_max: increasing rlimit_max (1024) to minimum Windows limit (16384)
params.c:Parameter() - Ignoring badly formed line in configuration file: *Retye
\snew\s*\spassword:* %n
params.c:Parameter() - Ignoring badly formed line in configuration file: *passwo
rd\supdated\ssuccessfully* .
Processing section "[homes]"
Processing section "[printers]"
Processing section "[print$]"
Loaded services file OK.
Server role: ROLE DOMAIN MEMBER
Press enter to see a dump of your service definitions
```

Figura 3.2: Saída do testparm

3.7 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 3. O usuário `root` tem que ser cadastrado no Samba 3 antes de qualquer outro usuário, pois ele é o administrador da aplicação.

- **# 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 cadastrar os usuários no Samba 3 eles precisam ser criados no sistema.

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

Após o usuário ser criado no sistema, ele necessita ser cadastrado no Samba 3.

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

3.8 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 3, porém sem pasta home e sem bash para login.

1. **# groupadd machine** - Cria o grupo no qual serão adicionadas as máquinas cadastradas para melhor organização dos usuários no linux.
2. **# useradd --home /dev/null --shell /bin/false --disabled-login --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 3 irá identificar que o usuário na verdade é uma máquina.
3. **# 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 3.

- **# smbpasswd -a -m computador1\$** - Cadastra a máquina no Samba 3.

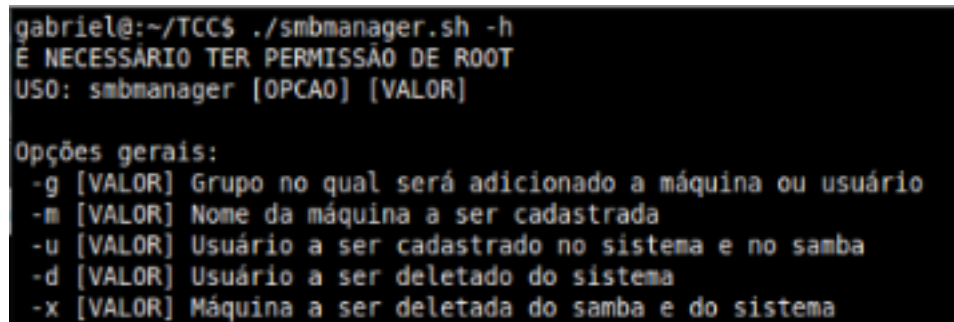
3.9 Script de Cadastro de Usuários e Máquinas

Para facilitar a criação e exclusão dos usuários no sistema e no Samba 3, foi feito o script **smbmanager.sh**¹ conforme o anexo no Apêndice A1. Com ele é possível criar usuários e máquinas, adicionar usuários em grupos e também excluí-los do sistema.

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

¹ Pode ser baixado em <https://github.com/GabrielRocha/Monografia/blob/master/latex/Scripts/smbmanager.sh>

1. **# chmod +x smbmanager.sh** - Adiciona a permissão de execução ao script.
2. **# 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. **# ./smbmanager.sh** - Execução do *script*. Figura 3.3



```
gabriel@:~/TCC$ ./smbmanager.sh -h
E NECESSÁRIO TER PERMISSÃO DE ROOT
USO: smbmanager [OPCAO] [VALOR]

Opções gerais:
-g [VALOR] Grupo no qual será adicionado a máquina ou usuário
-m [VALOR] Nome da máquina a ser cadastrada
-u [VALOR] Usuário a ser cadastrado no sistema e no samba
-d [VALOR] Usuário a ser deletado do sistema
-x [VALOR] Máquina a ser deletada do samba e do sistema
```

Figura 3.3: Saída do smbmanager

3.10 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. A Tabela 3.1 apresenta alguns dos grupos e seus respectivos RID (*Relative Identifier*). Os comandos a seguir devem ser utilizados para mapear esses grupos no Samba 3.

Tabela 3.1: Tabela do RID (*Relative Identifier*) Windows (SAMBA.ORG, 2003)

Well-Known Entity	RID	Type	Essential
Domain Administrator	500	User	No
Domain Guest	501	User	No
Domain KRBtgt	502	User	No
Domain Admins	512	Group	Yes
Domain Users	513	Group	Yes
Domain Guests	514	Group	Yes
Domain Computers	515	Group	No
Domain Controllers	516	Group	No
Domain Certificate Admins	517	Group	No
Domain Schema Admins	518	Group	No
Domain Enterprise Admins	519	Group	No
Domain Policy Admins	520	Group	No
Builtin Admins	544	Alias	No
Builtin users	545	Alias	No
Builtin Guests	546	Alias	No
Builtin Power Users	547	Alias	No
Builtin Account Operators	548	Alias	No
Builtin System Operators	549	Alias	No
Builtin Print Operators	550	Alias	No
Builtin Backup Operators	551	Alias	No
Builtin Replicator	552	Alias	No

- **# net groupmap list** - Liste os grupos existentes mapeados, caso não tenha o grupo siga os passos a seguir.
1. **# net groupmap add ntgroup='Domain Admins' rid=512 unixgroup=admin** - Irá mapear o grupo admin para o grupo Domain Admins do windows.
 2. **# net groupmap add ntgroup='Domain Users' rid=513 unixgroup=users** - Mapea o grupo users com o Domain Users do windows.
1. **# net groupmap delete ntgroup='Domain Admins'** - Caso queira remover um mapeamento de grupo.
 2. **# 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.

3.11 Perfis Móveis

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 3. 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 de armazenamento e uma rede muito bem estruturada.

Para ativar a configuração de perfil móvel no Samba 3 deve-se adicionar no [global] as variáveis mostradas no Quadro 3.3

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

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

logon drive = H:
```

Quadro 3.3: Variáveis necessárias para o perfil móvel

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

No exemplo apresentado, o diretório profile criado fica compartilhado para que seja mapeado na unidade H do usuário no windows.

Após a definição dessas três opções na seção [global], deve-se criar uma seção [profiles] contendo alguns comandos que serão detalhados a seguir no Quadro 3.4.

```
[ profiles ]

path = / var / samba / % U

writeable = yes

browseable = no

create mask = 0600

directory mask = 0700

available = yes
```

Quadro 3.4: Variáveis para criação do compartilhamento profile

- **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.

3.12 Compartilhamento de Arquivos

O compartilhamento de arquivos é dado pela adição de seções no arquivo smb.conf. Como pode ser visto no Quadro 3.5

```
[Diretoria]

path = /media/diretoria

read only = no

valid users = +diretoria

force group = diretoria

create mask = 0770

directory mask = 0770

browseable = no
```

Quadro 3.5: Criação de uma seção para compartilhamento de arquivos

- **[Diretoria]** - Nome do compartilhamento que será mostrado no servidor.
- **path** - Nele devemos mapear diretórios que serão compartilhados na rede.

Cabe ressaltar que após a criação desses diretórios, é necessário o ajuste das permissões de acesso, do dono do diretório e do grupo do diretório, utilizando os programas `chmod` e `chown`, respectivamente. O ajuste varia caso a caso, e deve ser realizado com cautela, para não dar mais permissões que o necessário. Uma breve explicação sobre o `chmod` e `chown` é realizada a seguir:

`chmod` - Define as permissões do arquivo. Exemplo: # `chmod 774 -R /pasta_criada` - essas permissões definem que o usuário proprietário do diretório e todos os usuário do grupo do diretório terão controle total no diretório e em seus arquivos e que os outro usuário poderão apenas listar os arquivos que se encontram no diretório.

`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 criados dentro do diretório compartilhados.
- **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.

Aplicação de algumas das variáveis citadas acima que podem ser vista no Quadro

3.6

[Backup]

```
write list = usuario1 # Somente o usuario1 tera permissao de escrita no
compartilhamento.

read list = usuario2 # O usuario2 so podera ler e listas os arquivos e
diretorios 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 poderao acessar esse compartilhamento.

veto files = *.tmp/*.doc # Nao sera permitido inserir esses tipos de
arquivos no compartilhamento. Essa variavel aceita expressoes regulares

```

Quadro 3.6: Aplicação de algumas variáveis no Samba 3

3.13 Script Logon

Para que os mapeamentos de unidades e alguns códigos sejam executados de forma automática nos usuários logados o Samba 3 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 em um compartilhamento no smb.conf para que possa ser executado. Conforme descrito no Quadro 3.7

```

[netlogon]

path = /var/samba/scripts

read only = yes

browseable = no

```

Quadro 3.7: Compartilhamento dos *scripts* de *logon*

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

1. **# mkdir -p /var/samba/scripts** - Cria a pasta onde estarão os scripts.

2. # **chmod 1775 /var/samba/scripts** - Permissão de execução dos scripts.

Exemplo de um script `diretoria.bat` no Quadro 3.8 e seu resultado na Figura 3.4

```
net use x: \\servidor\diretoria
```

Quadro 3.8: Comando para mapeamento automático de uma pasta compartilhada

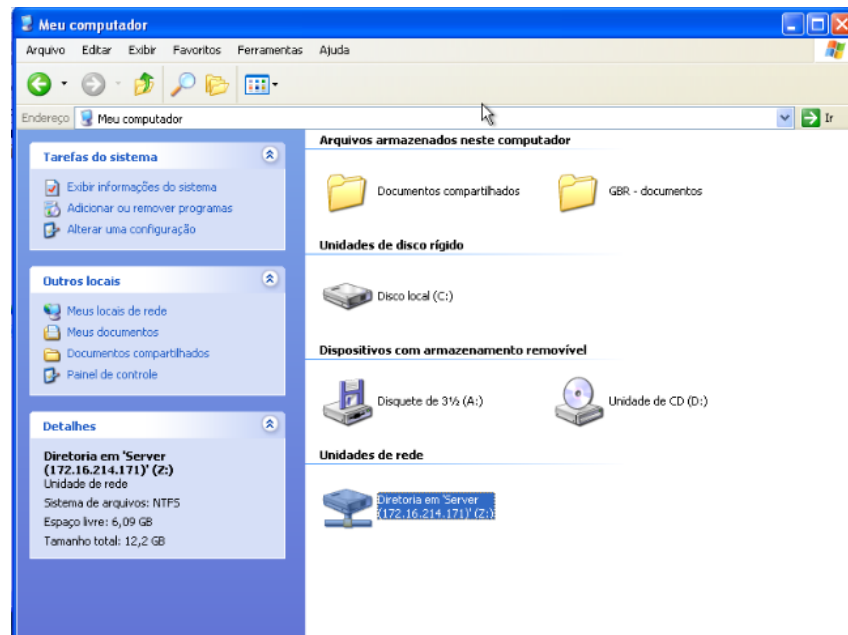


Figura 3.4: Tela de um mapeamento

3.14 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 3 deve-se adicionar na seção `[global]` as variáveis contidas no Quadro 3.9

```
[global]

printing = cups

load printers = yes
```

Quadro 3.9: Variáveis para permitir impressão em impressoras compartilhadas

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

O Samba 3 utiliza o cups que é o gerenciador de impressoras mais comum para o linux.

1. **#smbd -b | grep CUPS** - Para saber se o pacote Samba 3 instalado é compatível com o CUPS. A saída deve ser algo como "HAVE CUPS"

Caso o cups não esteja instalado.

1. **#apt-get install cups** - Instala todos os pacotes necessários para o funcionamento do cups.
2. **\$ firefox localhost:631** - Interface gráfica para gerenciar as impressoras. Figura 3.5.
3. **# /etc/init.d/cupsys restart** - Reinicia o serviço do cups

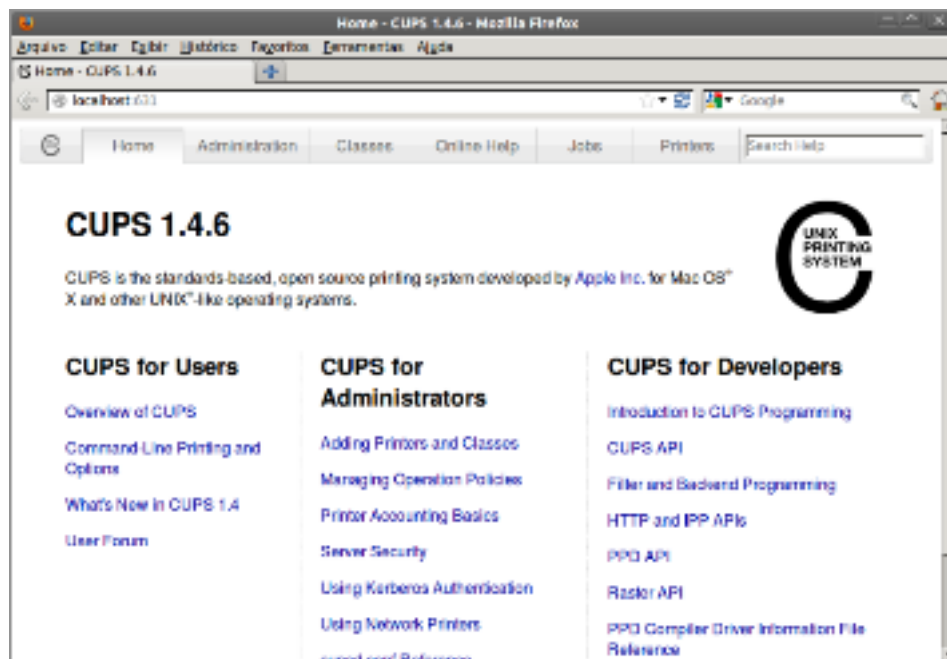


Figura 3.5: Tela do CUPS pelo Browser

Para habilitando o compartilhamento de impressora. Tem que adicionar as variáveis contidas no Quadro 3.10

```
[ printers ]

print ok = yes
```

```

guest ok = yes

path = /var/spool/samba

browseable = yes

```

Quadro 3.10: Variáveis para compartilhar impressoras

- **path** - Esse caminho é onde ficarão os spools de impressão. Esse diretório é criado automaticamente pelo Samba 3 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.

3.15 Instalação automática dos driver 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 3 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. Conforme mostrado no Quadro 3.11

```

[print$]

path = /var/lib/samba/printers

read only = yes

write list = root

```

```
inherit permissions = yes
```

Quadro 3.11: Variáveis para compartilhamento onde deverão ficar os *drivers* das impressoras

- **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.

1. **# mkdir -p /var/lib/samba/printers**
2. **# cd /var/lib/samba/printers**
3. **# 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.
4. **# chmod 2775 WIN40 W32X86** - Permissões especiais para instalar os drivers nos usuários.
5. **# net -S localhost -U root -W NOME_DO_SERVIDOR rpc rights grant "NOME DO SERVIDOR\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* tem que ser passados para o servidor. Para tal, é necessária a utilização de uma máquina cliente com Windows instalado. Ela se conectará ao servidor que está compartilhando as impressoras, e através da senha de root desse servidor, irá passar os *drivers* através da rede. A sequência de figuras a seguir ilustra o passo-a-passo para a adição desses *drivers*.

1. **Acesse a maquina com um usuário local** - Figura 3.6
2. **Informe o endereço do servidor** - Figura 3.7



Figura 3.6: Tela do Login no Windows localmente

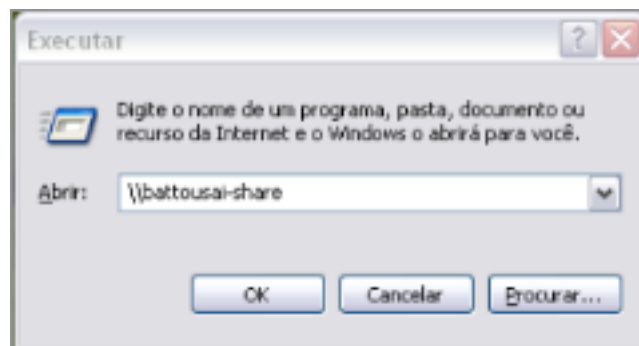


Figura 3.7: IP do servidor de compartilhamento

3. **Informe o usuario root e sua senha.**
4. **Acesse a pasta "Impressoras e aparelhos de fax" - Figura 3.8**
5. **Clique na opção Arquivos -> Propriedade do servidor.**
6. **Aba Driver -> Adicionar - Figura 3.9**

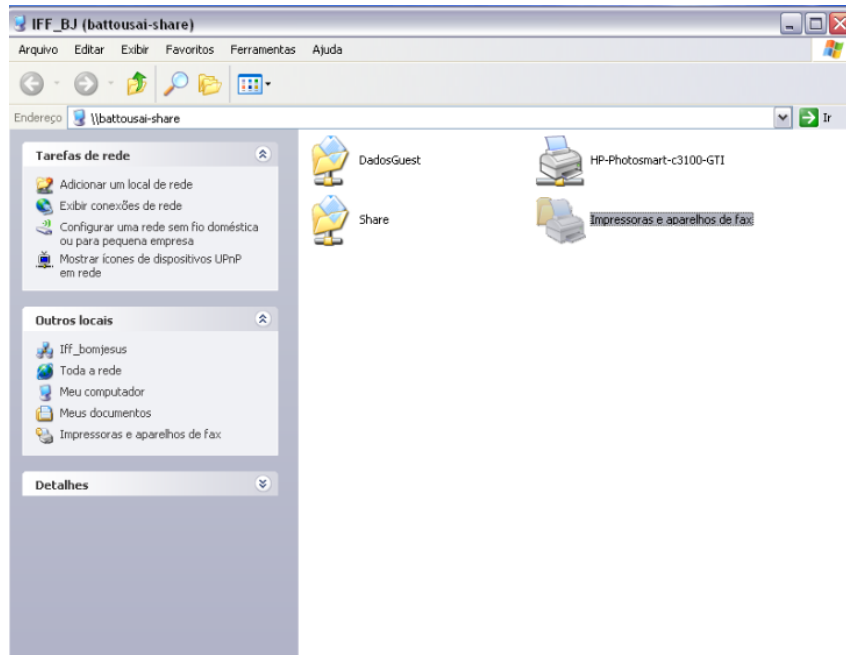


Figura 3.8: Impressoras e aparelhos de fax compartilhados

7. **Selecione o driver da impressora que deve ser copiado para o servidor** - Figura 3.10
8. **Selecione os sistemas operacionais dos *drivers* que serão instalados, e avance até concluir o assistente.** - Figura 3.11

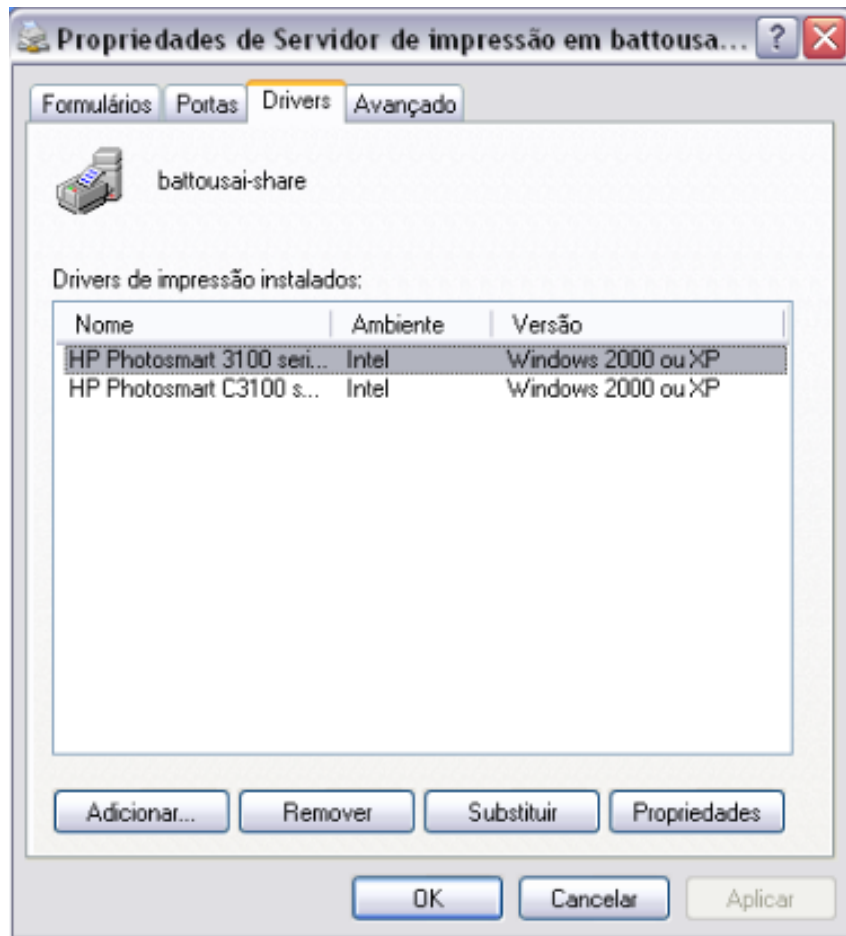


Figura 3.9: Adicionar driver ao servidor de impressão

9. Ao sair do assistente, clique com o botão direito na impressora desejada, e clique em **Propriedades**. - Figura 3.12
10. Na caixa de mensagem que irá aparecer, selecione a opção “NÃO”, pois caso selecione o sim o *driver* será instalado somente na maquina local. - Figura 3.13
11. Na guia avançado, selecione o *drive* que será vinculado a impressora e clique em OK. - Figura 3.14

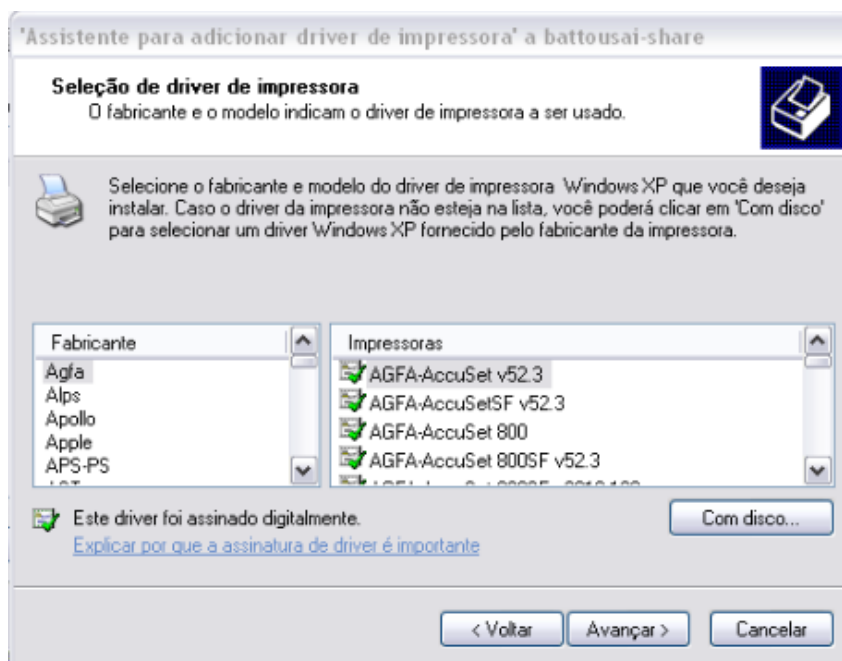


Figura 3.10: Selecionar o driver que será copiado para o servidor de impressão

12. Após esses passos, o *driver* da impressora já estará instalado no servidor de impressão. A partir desse momento, para instalar essa impressora, basta logar com o usuário do domínio no qual a impressora está compartilhada. - Figura 3.15
13. Acesse o servidor, conforme passo 2, e selecione a impressora que deseja mapear. - Figura 3.16
14. Após esses passos, a impressora será instalada automaticamente no computador cliente sem a necessidade de *drivers* adicionais, pois estes foram disponibilizados automaticamente pelo servidor através da rede. - Figura 3.17

3.16 Ingressando o Windows XP no Domínio

Para ingressar um computador Windows no domínio através do Samba 3 é necessário que primeiramente ele esteja devidamente cadastrado no servidor Samba 3. O windows deve estar com os drivers de rede instalados e respondendo na rede. Para ingressar o Windows XP no domínio deve-se realizar os seguintes passos:

1. Realize logon no windows com uma conta que possua privilégios administrativos. - Figura 3.18
2. Após o logon, deve-se abrir o programa Executar no menu Iniciar e acessar as Propriedades do Sistema através do comando "sysdm.cpl".
3. Acessar a aba "Nome do Computador". Deve-se clicar no botão "Alterar". - Figura 3.19

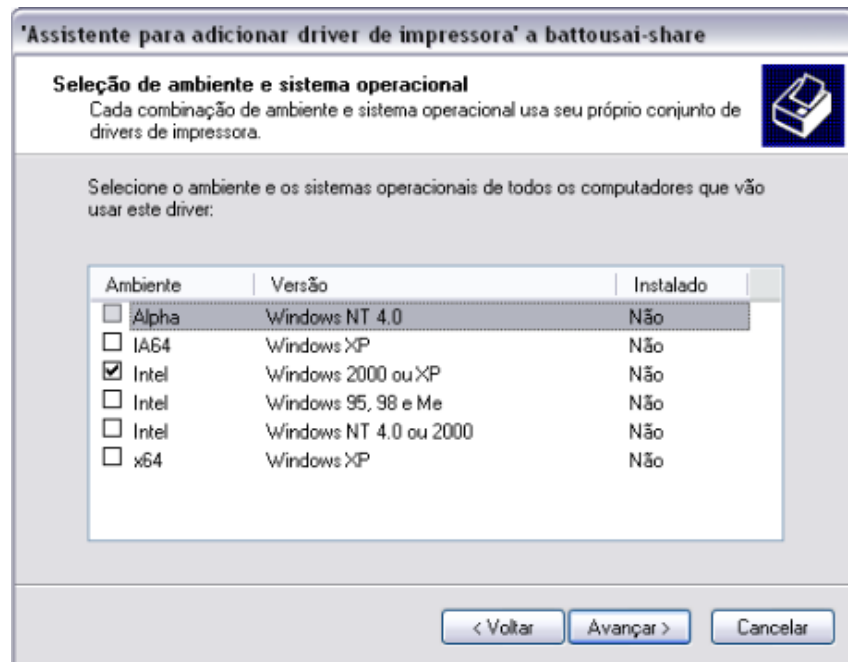


Figura 3.11: Selecionar os Sistemas Operacional que o driver será compatível

4. No menu de “Alterações de nome do computador”, certifique-se de que o nome definido para o computador é o mesmo que foi cadastrado no servidor Samba 3. No campo “Membro de”, selecione a opção “Domínio” e digite o nome do domínio definido na sessão [global] do Samba 3 e depois clique em OK. - Figura 3.20
5. Insira a senha de administrador do servidor para o micro ingressar no domínio. E aguarde a mensagem de confirmação.
6. Reinicie o micro quando for solicitado pelo sistema.
7. Após inicialização o micro, selecione o domínio para realizar o login e entre com um usuário e senha que esteja cadastrados previamente no servidor. - Figura 3.21

3.17 Ingressando o Linux no Domínio

Para ingressar um computador linux no domínio é necessário que primeiramente ele esteja devidamente cadastrado no servidor Samba 3. Para o linux realize login no servidor PDC é necessário a instalação de três pacotes essenciais. São eles o Samba, o Winbind e os módulos do PAM (libpam-modules).

A instalação desses pacotes na distribuição Ubuntu pode ser realizada através dos comando:

1. **#apt-get update** - Atualiza a base de dados do repositório.

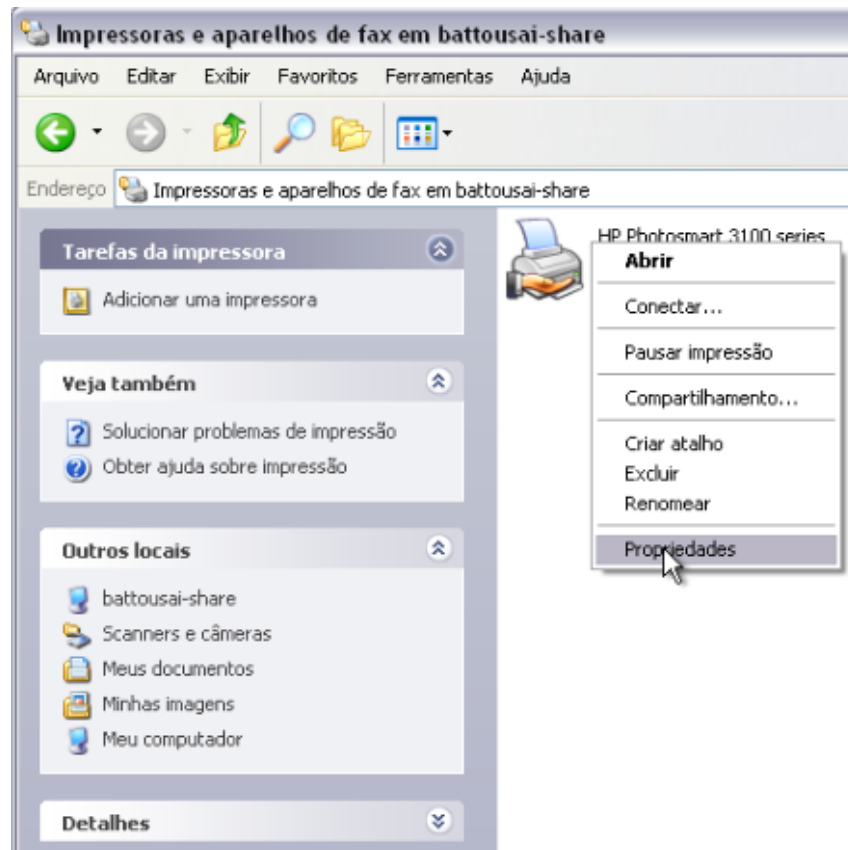


Figura 3.12: Propriedade da impressora do compartilhamento

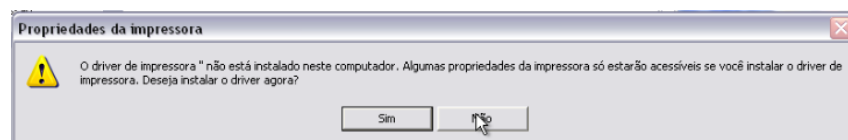


Figura 3.13: Opção para não instalar o driver naquele momento

2. **#apt-get install samba winbind libpam-modules** - Realiza a instalação dos pacotes Samba, Winbind e módulos do PAM.

Após a instalação é necessário realizar a configuração do micro para que possa fazer login no domínio. Começando pela configuração do Samba através do arquivo de configuração **/etc/samba/smb.conf**, que deve ser editado para que a seção [global] fique conforme o Quadro 3.12. Pode-se optar por adicionar essa configuração à configuração existente, ou pode manter apenas essa configuração básica:

```
[ global ]

workgroup = Dominio

netbios name = cliente1
```

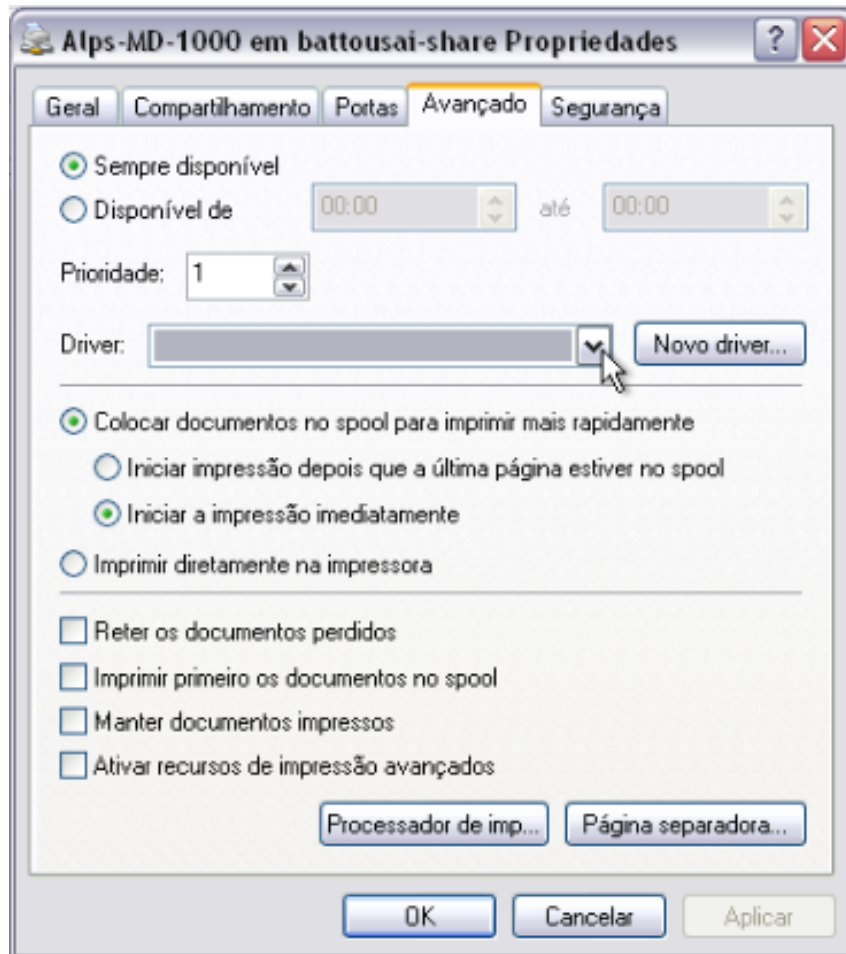


Figura 3.14: Aba onde será feito o link da impressora com o driver

```
winbind use default domain = yes

obey pam restrictions = yes

security = domain

encrypt passwords = true

wins server = 192.168.1.1

winbind uid = 10000-20000

winbind gid = 10000-20000

template shell = /bin/bash

template homedir = /home/\%U
```

Quadro 3.12: Arquivo smb.conf com as variáveis necessárias para fazer login em um domínio



Figura 3.15: Logar no domínio

Explicação de algumas variáveis importantes:

- **workgroup** - Nome do domínio configurado no servidor Samba 3.
- **netbios name** - Nome do computador cliente (/etc/hostname), que deve estar cadastrado no servidor.
- **wins server** - Ip do servidor PDC Samba 3.

Editado o arquivo `/etc/samba/smb.conf`, deve-se testar o arquivo de configuração para verificação de erros através do comando `#testparm`. Após a configuração do Samba, deve-se configurar o arquivo *Network Services Switch* (`/etc/nsswitch.conf`), que determina a ordem das buscas quando uma informação é solicitada. Esse arquivo deve ter as seguintes linhas do Quadro 3.13 alteradas:

```
passwd: compat winbind
group: compat winbind
shadow: compat winbind
```

Quadro 3.13: Arquivo nsswitch.conf

Foi incluído o **winbind** nas variáveis de busca **passwd**, **group** e **shadow** para que esses valores sejam buscados no servidor Samba 3.

Depois de concluídas as configurações, é necessário reiniciar o Samba e o Winbind.

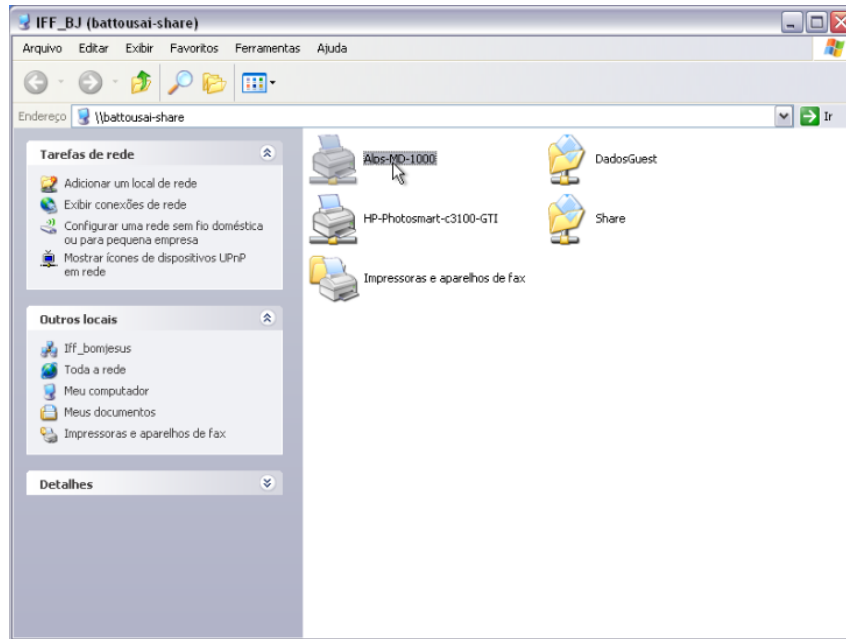


Figura 3.16: Selecionar a impressora que será mapeado no usuário logado

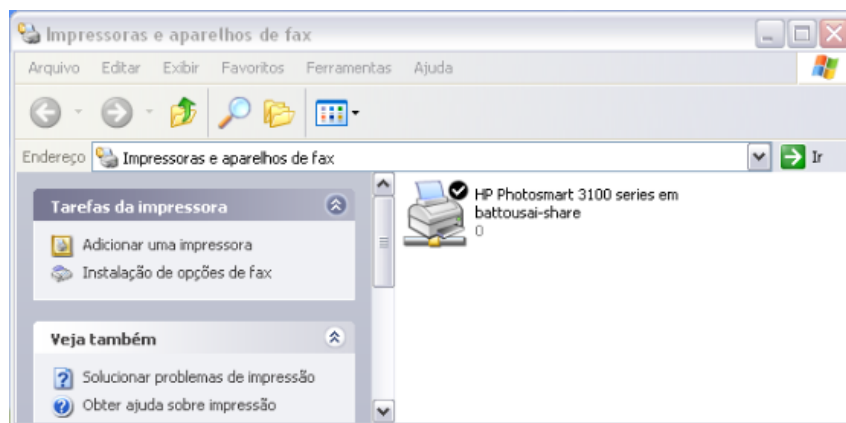


Figura 3.17: Impressora instalada no usuário

1. #service winbind restart
2. #service smbd restart
3. #service nmbd restart

Para testar a configuração realizada deve-se fazer o ingresso no domínio conforme abaixo. Será retornada uma mensagem de sucesso como a do Quadro 3.14.

- #net rpc join member -U root

Password :



Figura 3.18: Tela de logon local

Joined domain DOMINIO.

Quadro 3.14: Resultado quando a máquina é adicionada com sucesso no domínio

A senha solicitada é a senha de root do servidor PDC, cadastrada no Samba.

Os arquivos a serem alterados em seguida serão os arquivos de políticas de funcionamento do PAM. Essas políticas se encontram no diretório **/etc/pam.d**, onde estão contidos os arquivos de configuração para cada serviço que utilize os módulos de autenticação do PAM. O nome de um arquivo nesse diretório indica a qual serviço o arquivo de configuração se refere (portanto o arquivo **/etc/pam.d/login** fará referência ao serviço de *LOGIN* do Linux). Para definir políticas de autenticação a um serviço, deve-se acessar o arquivo do serviço desejado acrescentar as configurações desejadas seguindo a seguinte sintaxe do Quadro 3.15:

auth	required	pam_nologin.so	no_warn
------	----------	----------------	---------

Quadro 3.15: Exemplo de configuração do **/etc/pam.d/login**

Cada linha de configuração é formada por 4 campos. No exemplo temos os 4 campos na seguinte ordem: Nome instalação, tag de controle, nome do módulo, e argumentos do módulo. Campos adicionais serão interpretados como argumentos do módulo.

Após o teste de ingresso no domínio é necessário configurar o sistema de autenticação PAM para buscar os logins no servidor. Para isso é necessário modificar os arquivos **/etc/pam.d/login** e **/etc/pam.d/gdm**. O arquivo **/etc/pam.d/login** é responsável pelas configurações de autenticação de usuários no sistema, enquanto o arquivo **/etc/pam.d/gdm** é responsável pelas configurações de autenticação na interface de login do gnome. No arquivo **/etc/pam.d/login**, deve-se adicionar as linhas do Quadro 3.16 no início do arquivo:

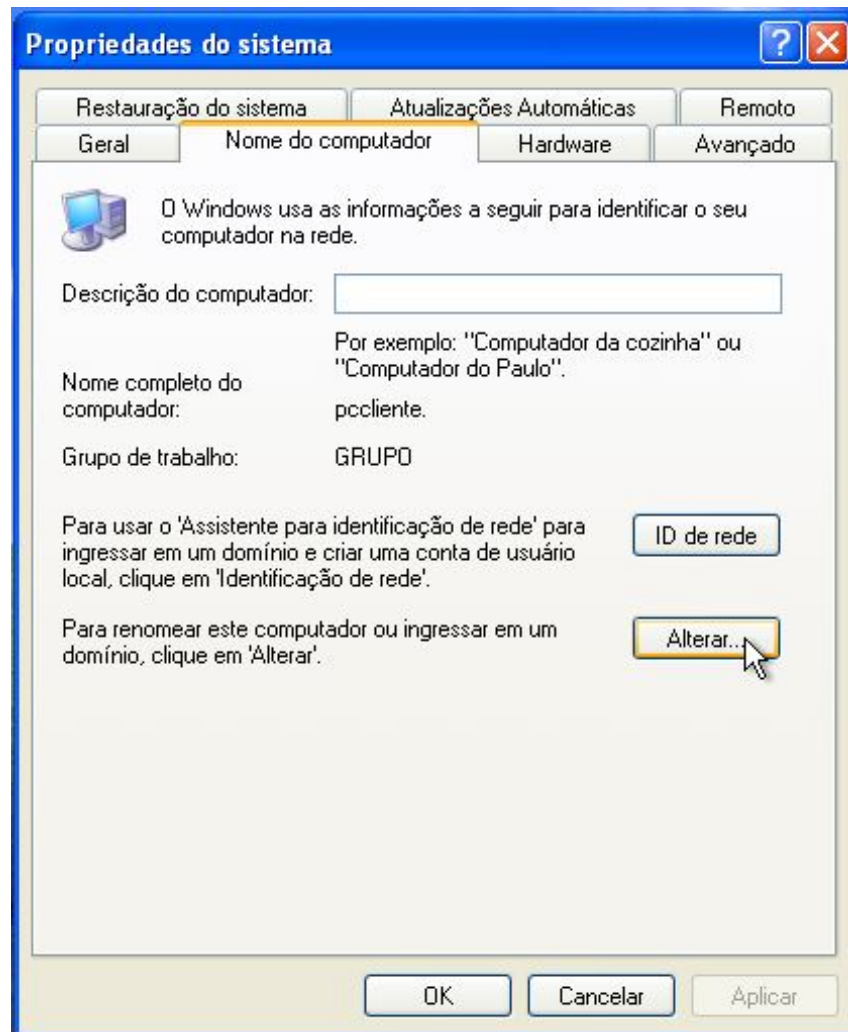


Figura 3.19: Alterando nome do micro

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

session optional pam_mount.so

auth sufficient pam_winbind.so

account sufficient pam_winbind.so

session required pam_winbind.so
```

Quadro 3.16: Linhas do arquivo /etc/pam.d/login

No arquivo **/etc/pam.d/gdm** deve-se comentar todo o seu conteúdo e adicionar as linhas contidas no Quadro 3.17 ao início do arquivo:

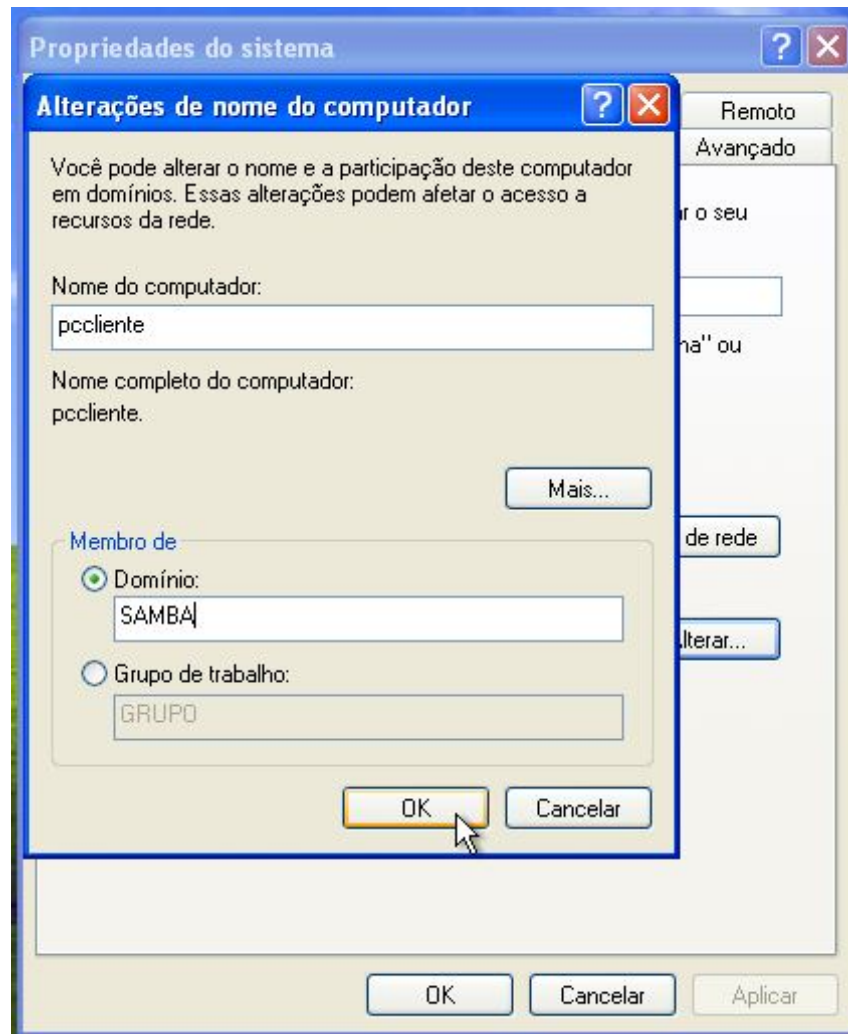


Figura 3.20: Incluir micro no domínio

```
auth required /lib/security/pam_securetty.so

auth required /lib/security/pam_nologin.so

auth sufficient /lib/security/pam_winbind.so

auth required /lib/security/pam_pwdb.so use_first_pass shadow nullok

account required /lib/security/pam_winbind.so

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

Quadro 3.17: Arquivo /etc/pam.d/gdm

As configurações acima fazem o GDM exibir os usuários disponíveis no servidor para login diretamente no domínio sem que haja autenticação local. Para as configurações acima funcionarem corretamente, a opção de Login Automático não pode estar ativada no computador.



Figura 3.21: Efetuando logon no domínio

4 SAMBA 4

O Samba 4 vem com a proposta de criar um *Active Directory* livre, combatendo as versões pagas da Microsoft, utilizando o LDAP, Bind (ou um DNS interno que o próprio Samba 4 possui) e Kerberos. Ele vem com a intenção de ser uma evolução do Samba 3. Com ele o administrador de rede é capaz de fornecer na rede serviços como, controle de usuários, máquinas, compartilhamento de arquivos, compartilhamento de impressoras, controle de acesso ao compartilhamento e entre outros. Com a adoção de um *Active Directory* no mesmo sistema que fornece o compartilhamento de arquivos e impressoras, o Samba 4 permite uma ligação nas configurações de permissões a usuários inseridas no compartilhamento com os usuários cadastrados no domínio, assim eliminando a divisão entre o servidor de domínio e o de compartilhamento.

O sistema ainda esta em desenvolvimento mas já passou por todas as suas fases de testes iniciais alpha e beta, atualmente esta na 4^o Release Candidate, mas sem data para o lançamento da versão estável.

4.1 Instalação do SAMBA 4

Todos os comandos foram testados no Ubuntu 11.04 e Debian 6, por isso algumas adaptações podem ser necessárias em outras distribuições Linux.

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 git-core autoconf python-dnspython ntpdate acl libacl1-dev**

Antes de começar a instalação o relógio do servidor tem que estar atualizado. O comando `ntpdate` atualiza a hora através do `ntp`², onde um dos principais servidores é o `pool.ntp.br`.

²Os servidores NTP permitem aos seus clientes a sincronização dos relógios de seus computadores e outros equipamentos de rede a partir de uma referência padrão de tempo aceita mundialmente, conhecida como UTC (*Universal Time Coordinated*). (RNP, 2010)

- **# ntpdate pool.ntp.br**

O código fonte do Samba 4 está hospedado no servidor git dos desenvolvedores do Samba, e o mesmo deve ser clonado para a máquina de destino.

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

O Samba 4 segue os procedimentos padrões de instalação de aplicativos no Linux através do terminal, que segundo (Långstedt, 2005) se segue com o `./configure`, `make` e `make install`. Nesse caso ao invés de se utilizar o `./configure` como padrão é utilizado o `./configure.developer`, pois o mesmo habilita alguns modos de debug.

- **# ./configure.developer**
- **# make**
- **# make install**

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

O Samba 4 trabalha com regras ACL e para que ele possa ser instalado tem que habilitar o modo `acl` nas unidades de disco.

- **# vim /etc/fstab**

Deve-se localizar a linha da unidade principal (`/`) e adicionar o parâmetro `acl` na coluna `options` da montagem desta unidade, conforme figura 4.1.

```
# /etc/fstab: static file system information.
#
# Use 'blkid' to print the universally unique identifier for a
# device; this may be used with UUID= as a more robust way to name devices
# that works even if disks are added and removed. See fstab(5).
#
# <file system> <mount point> <type> <options>        <dump> <pass>
proc                /proc              proc           defaults        0        0
# / was on /dev/sda1 during installation
UUID=853a5cd8-be6a-4623-83c0-e79500d02bf6 /                  ext4           acl,errors=remoun
t-ro 0            1
# swap was on /dev/sda2 during installation
UUID=86d40e2a-6c22-40c4-83fa-b1d4a587e2e1 none                swap           sw
0                0
/dev/scd0            /media/cdrom0       udf,iso9660    user,noauto      0        0
/dev/fd0             /media/floppy0      auto           rw,user,noauto   0        0
```

Figura 4.1: Tela do fstab.

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

- **# cd /usr/local/samba**

A instalação do Samba 4 é realizada através do samba-tools, uma ferramenta que acompanha o Samba 4, que fica localizado na pasta bin do Samba 4. Deve-se usar as opções “domain provision” e após inserir alguns parâmetros importantes para a configuração do domínio, conforme comando abaixo. Os parâmetros serão detalhados a seguir.

- **# bin/samba-tool domain provision --use-ntvfs --realm=NOME_DO_SERVIDOR --domain=NOME_DOMINIO --adminpass='Senha12' --server-role=dc**

1. **use-ntvfs** - Habilita o NTVFS³;
2. **realm** - Domínio do servidor Kerberos;
3. **domain** - Domínio do Samba;
4. **adminpass** - Senha do Administrator, por questões de segurança o samba-tool não permite a inserção de senhas consideradas fracas como senhas com menos de 7 dígitos e somente com números em sequência;
5. **server-role** - Regra do servidor.

Depois de instalado e configurado o Samba 4 pode ser iniciado.

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

³Sistema de arquivos que armazena os atributos do NTFS

Para facilitar a forma de ativar o Samba 4 podem ser feito dois procedimentos.

Criar um link do executável do Samba no /etc/init.d/

- **# ln /usr/local/samba/sbin/samba /etc/init.d/samba**

Mudar o caminho da variável de ambiente PATH para que os comandos possam ser acessados fora da sua pasta de origem.

- **# echo "export PATH=/usr/local/samba/sbin:/usr/local/samba/bin:\$PATH">> /root/.bashrc**

Por padrão o Samba 4 vem com uma servidor interno de DNS, facilitando a criação das zonas e dos mapeamentos. Para a resolução dos nome deve definir o ip da própria maquina como seu dns primário. Cabe resaltar que os micros clientes do domínio devem ser configurados para usar o servidor do Samba 4 como DNS primário.

- **# echo "domain NOME_DOMINIO nameserver IP_DO_SERVIDOR"> /etc/resolv.conf**

Mesmo contendo um servidor de dns interno o Samba 4 também trabalha com servidores externos, BIND9 versão 9.7 ou mais nova, onde alguns parâmetros de configuração são passados no named.conf.local e named.conf.options para a criação das zonas e atualização automática com o Kerberos.

- **#echo "include '/usr/local/samba/private/named.conf'"> /etc/bind/named.conf.local**
- **# vim /etc/bind/named.options**

Adicione as seguintes linhas:

```
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.

4.3 Instalação do Kerberos

Segundo Grassato (2009) a 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 o 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, com essas credenciais o DNS aceita atualizações GSS-TSIG assinadas e verifica as credenciais de correspondentes com as credencias cadastradas no Samba 4, 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-se 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 Gerenciando o Samba4 através do Windows e do Linux

É possível gerenciar o servidor Samba 4 através de um Windows XP mas para a realização do mesmo é necessário a instalação do AdminPack⁴ presente no Windows Server. Essa ferramenta permite gerenciar todos os usuários, grupos e máquinas presentes no *Active Directory*

Inicie a ferramenta pelo **Executar** -> **dsa.msc** 4.2.

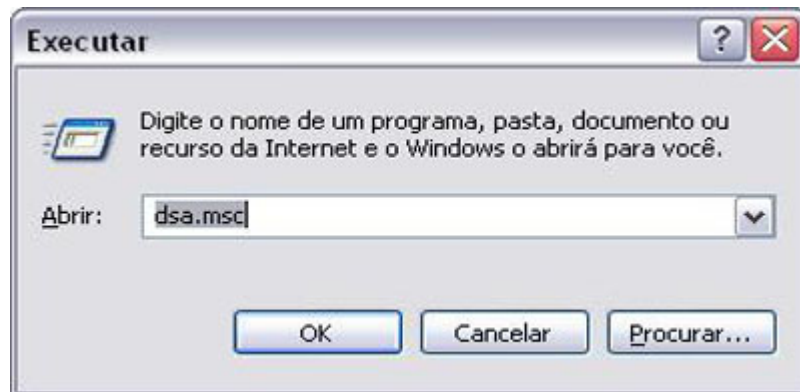


Figura 4.2: Tela para executar o DSA.

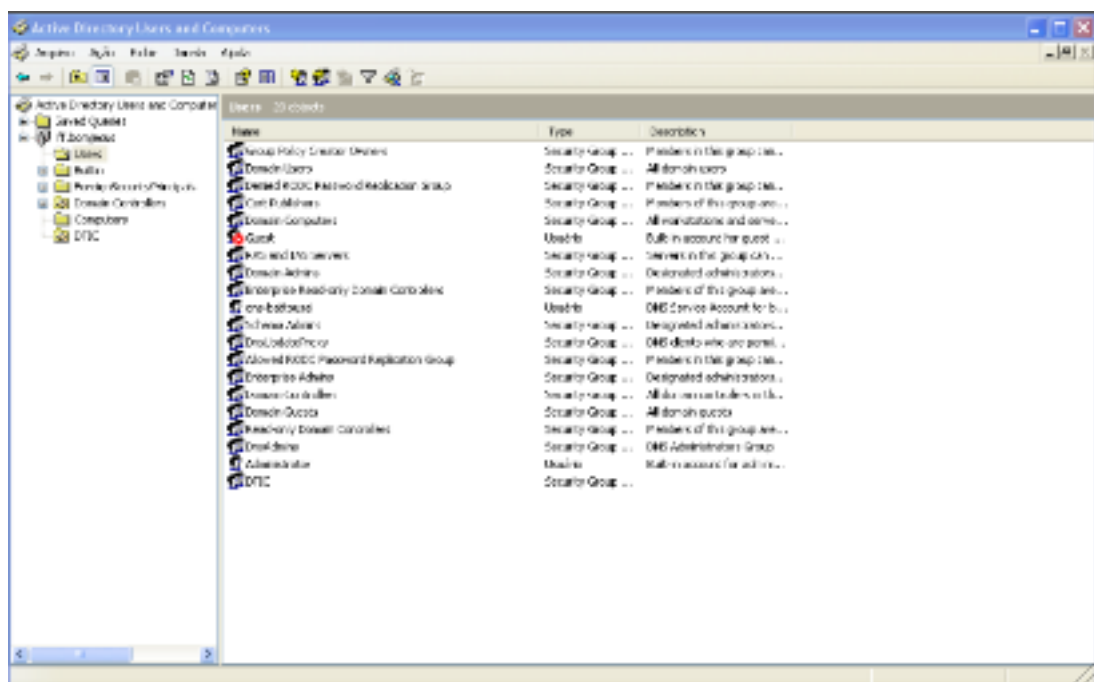


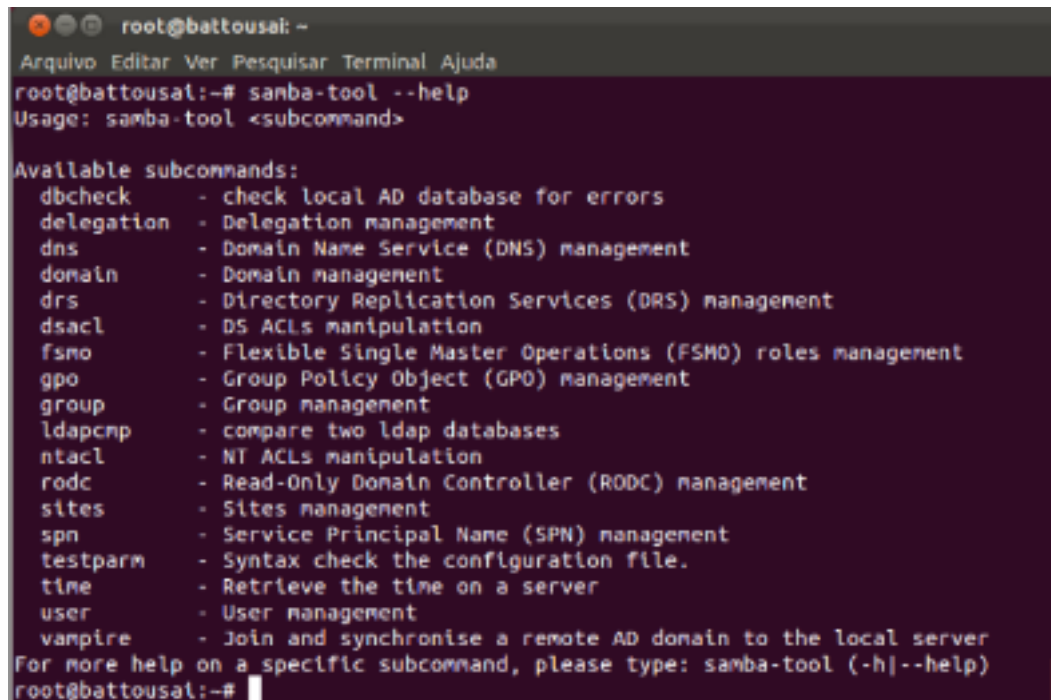
Figura 4.3: Tela do DSA.

Outra forma de gerenciar o servidor Samba 4 é utilizando o samba-tools, uma ferramenta que acompanha o Samba 4 e tem a finalidade de gerenciar as ações que podem ser feitas no no

⁴O AdminPack está disponível no site da Microsoft:

<http://www.microsoft.com/downloads/details.aspx?FamilyID=c16ae515-c8f4-47ef-a1e4-a8dcbaeff8e3&displaylang=en>

Active Directory. Com ele se poder criar usuários, grupos, gpo's, entre outras funções, porém através do terminal do linux, conforme figura 4.4.



```

root@battousai:~
Arquivo Editar Ver Pesquisar Terminal Ajuda
root@battousai:~# samba-tool --help
Usage: samba-tool <subcommand>

Available subcommands:
  dbcheck      - check local AD database for errors
  delegation   - Delegation management
  dns          - Domain Name Service (DNS) management
  domain       - Domain management
  drs          - Directory Replication Services (DRS) management
  dsacl        - DS ACLs manipulation
  fsmo         - Flexible Single Master Operations (FSMO) roles management
  gpo          - Group Policy Object (GPO) management
  group        - Group management
  ldapcmp      - compare two ldap databases
  ntaccl       - NT ACLs manipulation
  rodc         - Read-Only Domain Controller (RODC) management
  sites        - Sites management
  spn          - Service Principal Name (SPN) management
  testparm     - Syntax check the configuration file.
  time         - Retrieve the time on a server
  user         - User management
  vampire      - Join and synchronise a remote AD domain to the local server
For more help on a specific subcommand, please type: samba-tool (-h|--help)
root@battousai:~#

```

Figura 4.4: samba-tool no terminal.

4.5 Maquinas linux interagindo com o *Active Directory* do Samba4

Segundo (UBUNTU BR, 2011) a forma de incluir uma maquina Ubuntu no *Active Directory* é modificar alguns arquivos de configuração. A seguir será apresentado um passo-a-passo para inclusão do Ubuntu no domínio. Para tal, foi utilizado como exemplo de configuração do domínio as seguintes informações:

Descrição das variáveis que serão utilizadas na configuração e seus valores.

- **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.

1. Instalando os pacotes necessários

- `# aptitude install krb5-user libpam-krb5 winbind samba smbfs smbclient krb5-config libkrb53 libkadm5 vim`

2. Sincronizando a hora

- `# ntpdate 10.2.0.1`

3. 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
```

Quadro 4.2: FAZER

4. 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
```

Quadro 4.3: FAZER

5. 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

6. 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
```

Quadro 4.4: FAZER

7. 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

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
```

Quadro 4.5: FAZER

8. Reinicie os serviços.

1. # /etc/init.d/winbind stop
2. # /etc/init.d/samba restart
3. # /etc/init.d/winbind start

9. Adicione a conta ao domínio.

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

10. Configure a Autenticação.

- # vim /etc/nsswitch.conf

```
passwd:    compat winbind
group:     compat winbind
shadow:    compat
```

Quadro 4.6: FAZER

11. 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
```

12. Configure o PAM.

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

```
account sufficient pam_winbind.so
account required pam_unix.so
```

Quadro 4.7: FAZER

- # 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_denied.so
```

Quadro 4.8: FAZER

- # 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
```

Quadro 4.9: FAZER

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

```
auth sufficient pam_winbind.so
auth sufficient pam_unix.so use_first_pass
auth required pam_denied.so
@include common-account
```

Quadro 4.10: FAZER

13. Reinicie os serviços

1. # /etc/init.d/winbind stop
2. # /etc/init.d/samba restart
3. # /etc/init.d/winbind start

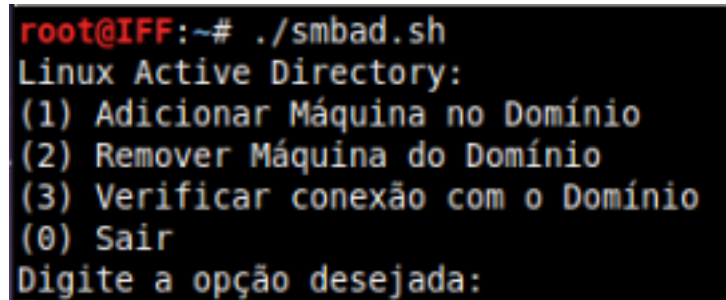
14. **Logando no domínio.** Vá para a console usando o comando CTRL+ALT+F1 e logue no sistema com o login e senha do domínio.

- login: nome_do_usuario
- Password: *****
- nome_do_usuario@gert: \$

4.6 Script para adicionar maquina linux no *Active Directory*.

O cadastro de maquinas no samba 4 se difere do samba 3 por não ser necessário o cadastramento do computador como usuário, com o \$ no final do nome, no servidor e depois cadastra-lo no Samba 4.

Para facilitar a inserção das maquinas linux no *Active Directory* do Samba 4 foi modificado um script e ele foi chamado de smbadd.sh⁴.



```

root@IFF:~# ./smbadd.sh
Linux Active Directory:
(1) Adicionar Máquina no Domínio
(2) Remover Máquina do Domínio
(3) Verificar conexão com o Domínio
(0) Sair
Digite a opção desejada:
  
```

Figura 4.5: Tela do script para inserir maquinas linux no AD.

4.7 Compartilhamento de arquivos

SAMBA4 tem um problema 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 ou grupo 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.

/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.

⁴Pode ser baixado em <https://github.com/GabrielRocha/Monografia/blob/master/latex/Scripts/smbadd.sh>

/usr/local/samba/bin/wbinfo --group-info Dtic - Mostra o gid do grupo e é a referência do grupo local com o do Samba 4.

chown 3000011.3000020 /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 Windows no domínio Samba 4

O procedimento para ingressar um computador Windows no domínio Samba 4 é o mesmo executado no Samba 3, porém o computador a ser ingressado não necessita ser cadastrado anteriormente, pois o mesmo será cadastrado automaticamente no Samba 4 através do Kerberos. Em adição aos procedimentos realizados no Samba 3, para ingressar o computador Windows no domínio pelo Samba 4, deve ser informado o IP do servidor no campo de DNS das configurações de Rede. Para configurar o IP de DNS deve-se:

- Acessar as conexões de rede através do Painel de Controle.4.6

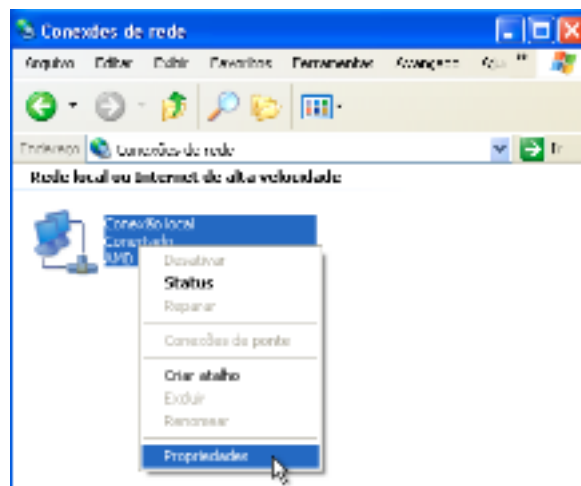


Figura 4.6: Acessando as Conexões de Rede

- Acessar as propriedades da conexão de rede ativa.4.7

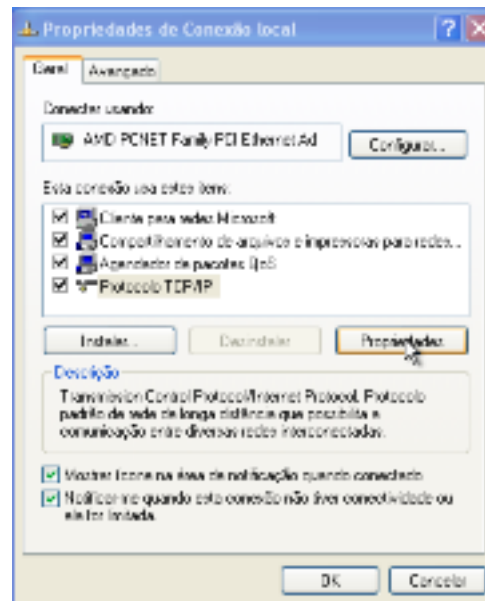


Figura 4.7: Acessando as propriedades da conexão ativa

- Incluir o IP do servidor no campo de DNS.4.8

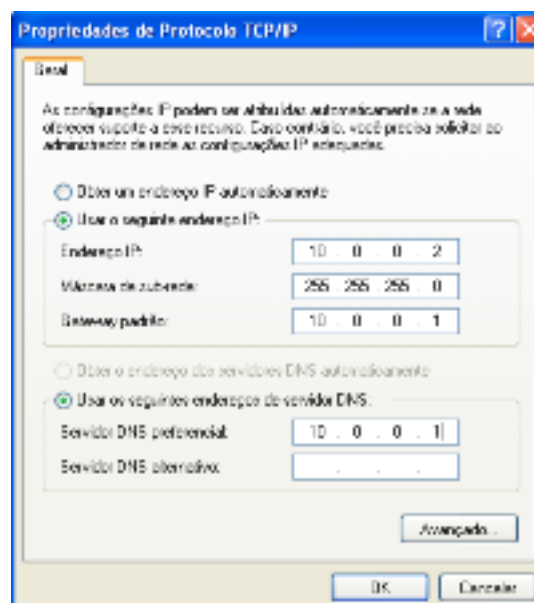


Figura 4.8: Incluindo o IP do servidor Samba 4 no campo de DNS

- Após salvo as configurações, o computador deve ser reiniciado.

5 ESTUDO DE CASO

Esta proposta de implementação foi motivada através de um cenário de uma instituição de ensino que necessitava de uma otimização na segurança e compartilhamento de seus recursos de TI. Para melhor gerenciamento e manutenção dos arquivos compartilhados e usuários na rede, seria necessário a implantação de um servidor que centralizasse todas essas tarefas.

Foi iniciada uma pesquisa para encontrar um software que atendesse a todos requisitos. O Windows Server é uma solução, mas é proprietário e o valor de uma licença da versão 2012 *Datacenter* custa em torno de 10 mil reais (MICROSOFT, 2012b). O alto valor da licença acaba inviabilizando a utilização em instituições de ensino e em pequenas empresas. Para solucionar esse problema da compra de licenças foi criada uma versão livre, o Samba 4, que faz as mesmas tarefas de um Windows Server, trabalhando com o mesmo protocolo, o LDAP. Pelo custo benefício, o Samba 4 foi utilizada neste trabalho. A instituição contém 110 computadores nos setores administrativos e 90 nos laboratórios de informática. Abaixo uma demonstração da estrutura da rede 5.1:

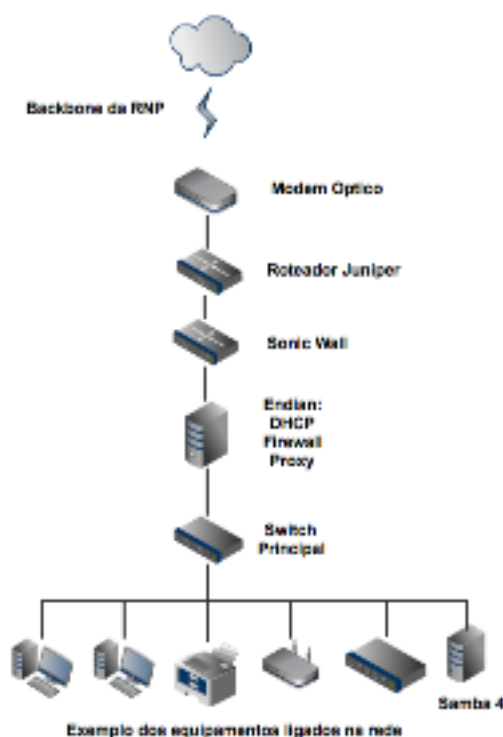


Figura 5.1: Estrutura da rede do instituto

Os setores são divididos conforme suas funções no organograma da instituição. Os principais são:

- * Diretoria do Departamento de Administração e Finanças
- * Diretoria do Departamento de Gestão de Pessoas
- * Coordenação de Registros Acadêmicos
- * Chefe de Gabinete

Com a proposta de implementação abordada neste trabalho, cada setor e usuário terá na rede um compartilhamento próprio, com suas permissões definidas. Um servidor foi inserido na rede com o sistema operacional Debian 6.0.5 e com as seguintes configurações:

- Processador Intel Core I7®
- 4GB de memória RAM
- Um servidor com 6 Tb de HD
- Placas de vídeo, áudio e rede Onboard

Antes da instalação do Samba 4 seus pré requisitos foram instalados e o Kerberos Heimdal com suas variáveis de ambiente. Após a configuração dos sistemas básicos, o Samba 4 foi configurado com os seguintes parâmetros.

1. **# cd /usr/local/samba/**
2. **# bin/samba-tool domain provision --use-ntvfs --realm=instituto.ensino
--domain=ensino --adminpass='Senha12' --server-role=dc**

Com o samba 4 as configurações básicas realizadas, foram feitas as modificações necessárias para que fosse utilizado o servidor de dns *default* do samba 4. Foi inserido no domínio do *Active Directory* todas as máquinas Windows XP, através do processo manual e as máquinas Linux, através do script *smbad.sh*, que se encontram na rede.

Por não ter uma ferramenta mais completa para o gerenciamento do Samba 4 pelo Linux, um computador com Windows XP foi designado para tal tarefa. Nele foram instalados o adminpack e o gerenciador de gpo do Windows. Por trabalharem com o mesmo protocolo como já foi dito anteriormente não houveram incompatibilidades na utilização das ferramentas.

Os usuários foram criados a partir da interface gráfica do adminpack no Windows, respeitando os requisitos de nome completo, ramal da sala, sala, entre outras informações

que auxiliam na identificação dos usuários no AD e inseridos nos respectivos grupos dos seus setores.

Com os usuários cadastrados e inseridos em seus grupos, foram criadas as GPO's com os scripts de inicialização e nelas foram definidos os mapeamentos automáticos dos compartilhamentos

Foram criados compartilhamentos com os nomes dos setores mais importantes da instituição afim de melhorar e garantir o melhor trabalho das pessoas no setor. Com a intenção de melhorar o controle dos recursos de armazenamento foram impostas regras de QUOTA com o EDQUOTA que consiste em um dos principais programas gerenciadores de cota de disco no linux.

- Pasta do usuário: 20Gb
- Pasta do setor: 100Gb

A seguir é apresentada uma parte do smb.conf do Samba 4, que corresponde as seções de compartilhamento de arquivos. As seções foram inseridas com a sigla dos setores. Foi decidido vetar arquivos de vídeo e áudio para não sobrecarregar o servidor.

```
[Chefia_de_Gabinete]

comment = Chefia de gabinete

path = /srv/samba/chefia

valid users = usuario1 , usuario2 # Usuarios do setor

read only = no

browseable = no

veto files = *.wmv / *.avi / *.wma / *.mp? / *.flv

[DDAF]

comment = Diretoria do Departamento de Administracao e Financas

path = /srv/samba/ddaf

valid users = usuario3 , usuario4 # Usuarios do setor

read only = no
```

```
browseable = no

veto files = *.wmv / *.avi / *.wma / *.mp? / *.flv

[DDGP]

comment = Diretoria do Departamento de Gestao de Pessoas

path = /srv/samba/ddgp

valid users = usuario5 , usuario6 # Usuarios do setor

read only = no

browseable = no

veto files = *.wmv / *.avi / *.wma / *.mp? / *.flv

[CRA]

comment = Coordenacao de Registros Academicos

path = /srv/samba/cra

valid users = usuario7 , usuario8 # Usuarios do setor

read only = no

browseable = no

veto files = *.wmv / *.avi / *.wma / *.mp? / *.flv


[HOME]

comment = Pasta dos usuarios

path = /srv/samba/%U

valid users = %U

read only = no

browseable = no

veto files = *.wmv / *.avi / *.wma / *.mp? / *.flv
```

Quadro 5.1: FAZER

Com as sessões criadas no samba, as pastas foram criadas no /srv e atribuídas as permissões 770 com o proprietário root e o GID do grupo criado no *Active Directory* com o nome do setor que foi designada a pasta:

1. **# mkdir /srv/samba/ddgp**
2. **# chmod 770 -R /srv/samba/ddgp**
3. **# chown root.3000020 -R /srv/samba/ddgp**

Todas as impressoras foram colocadas na rede, mapeadas no servidor do Samba 4 e compartilhadas para os demais computadores com a instalação dos drives automática.

```
[ printers ]

print ok = yes

guest ok = yes

path = /var/spool/samba

browseable = yes

[ print$ ]

path = /var/lib/samba/printers

read only = yes

write list = root

inherit permissions = yes
```

Quadro 5.2: FAZER

Tendo realizado todo este estudo com base na rede já existente da instituição de ensino foi constatado que a implementação sugerida neste trabalho é a mais adequada para atender os objetivos já explicitados anteriormente sobre otimização e segurança.

6 CONCLUSÕES

Neste trabalho foi apresentada uma proposta de implementação de um servidor de modo a otimizar o acesso dos usuários da instituição de ensino aos recursos disponíveis na rede e ainda assegurar a disponibilidade destes recursos, independente do equipamento utilizado.

Além disso, foi possível mostrar que, ao realizar esta implementação, o administrador de rede terá um maior controle dos acessos dos usuários, podendo permitir ou negar recursos, por exemplo.

Foi possível ainda apresentar ferramentas disponíveis para a realização da implementação da proposta, de forma simples e objetiva, focada na estrutura abordada para receber o servidor, além de configurações e *scripts* criados para otimizar o processo.

O Samba 3 é mais estável, e portanto é mais recomendado em redes de médio porte, porém não se comporta como *Active Directory* e não permite *policies*, mas realiza a autenticação dos usuários, compartilhamento de arquivos e impressoras. O Samba 3 e Samba 4 não podem ser instalados e configurados no mesmo servidor por trabalharem com os mesmos daemons de inicialização, um serviço quando iniciado anula o outro. Por ainda terem funções distintas a melhor forma de se trabalhar com os dois na mesma rede é trabalhando em servidores distintos porém interligados.

O Samba 4 funcionou perfeitamente no que se propõe a fazer, mesmo sendo uma versão Release Candidate e com o lançamento de uma versão estável o Samba 4 irá tornar o Samba 3 desnecessário.

Como em qualquer trabalho que envolve ferramentas em evolução, neste trabalho serão necessárias melhorias e novas pesquisas, não permitindo que o mesmo fique ultrapassado e não seja compatível com as ferramentas em constante atualização.

REFERÊNCIAS BIBLIOGRÁFICAS

CUFFA, H. de. *Interface de Programação de Aplicações de Serviços de Segurança Gerais*. Rio de Janeiro, 2010.

ECKSTEIN DAVID COLLIER-BROWN, P. K. R. *Using Samba*. Sebastopol, CA: OREILLY, 2003.

ERICOM. *Kerberos in PowerTerm Solutions*. 2012. Disponível em <http://www.ericom.com/kerberos.asp>. Acesso em Outubro de 2012.

FILHO, M. M. C. *Kerberos*. Rio de Janeiro, 2009.

FOCA. *Guia Foca GNU/Linux Capítulo 18 - SAMBA*. 2012. Disponível em <http://www.guiafoca.org/guia/avancado/ch-s-samba.htm>. Acesso em Outubro de 2012.

GRASSATO, D. P. *Instalação Samba4*. 2009.

INTERNET SYSTEMS CONSORTIUM. *BIND*. 2012. Disponível em <https://www.isc.org/software/bind>. Acesso em Novembro de 2012.

LOSANO, M. *Introdução ao Active Directory - Parte 1*. 2009.

LÂNGSTEDT, N. *Installing software from source in Linux - 1.2*. 2005.

MICROSOFT. *Resolução de nomes NetBIOS*. 2012. Disponível em [http://technet.microsoft.com/pt-br/library/cc738412\(v=ws.10\).aspx](http://technet.microsoft.com/pt-br/library/cc738412(v=ws.10).aspx). Acesso em Outubro de 2012.

MICROSOFT. *Windows Server 2012 How to Buy*. 2012. Disponível em <http://www.microsoft.com/en-us/server-cloud/windows-server/buy.aspx>. Acesso em Outubro 2012.

MONTEIRO, R. V. *O que é DNS (e DNSSEC) bem explicadinho*. 2007. Disponível em <http://webinsider.uol.com.br/2007/10/13/o-que-e-dns-e-dnssec-bem-explicadinho/>. Acesso em Novembro de 2012.

MORIMOTO, C. E. *Redes e Servidores Linux - Guia Prático*. Porto Alegre: Sulina, 2005.

MORIMOTO, C. E. *Servidores Linux, Guia Prático*. Porto Alegre: GDH Press e Sul Editores, 2008.

RNP. *Serviço NTP*. 2010. Disponível em <http://www.rnp.br/ntp/>. Acesso em Outubro de 2012.

SAMBA.ORG. *Samba HOWTO Collection*. 2003. Disponível em <http://www.samba.org/samba/docs/man/Samba-HOWTO-Collection/groupmapping.html>. Acesso em Outubro de 2012.

SCRIMGER PAUL LASALLE, M. P. R. *TCP/IP - A Bíblia*. Rio de Janeiro: Campus, 2002.

THE OPENLDAP FOUNDATION. *OpenLdap 2.1 Administrator's Guide*. 2003. Disponível em <http://www.bind9.net/manual/openldap/2.1/intro.html>. Acesso em Outubro de 2012.

TRIGO, C. H. *OpenLDAP - Uma Abordagem Integrada*. São Paulo: Novatec, 2007.

UBUNTU BR. *Autenticando AD*. 2011. [Http://wiki.ubuntu-br.org/AutenticandoAD](http://wiki.ubuntu-br.org/AutenticandoAD). Acesso em: 10/08/2012.

APÊNDICE A – Scripts

A.1 smbmanager.sh

```
#!/bin/bash
#Gabriel Rocha
end=0
help="NECESSARIO TER PERMISSAO DE ROOT \nUSO: smbmanager [OPCAO] [VALOR] \n
      \nOpcoes gerais:\n -g [VALOR] Grupo no qual sera adicionado a maquina
      ou usuario \n -m [VALOR] Nome da maquina a ser cadastrada \n -u [
      VALOR] Usuario a ser cadastrado no sistema e no samba \n -d [VALOR]
      Usuario a ser deletado do sistema \n -x [VALOR] Maquina 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\$ 2>/dev/null &&
            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
            2>/dev/null
        fi
    fi
fi
}

AddUser() {
if [ -n "$user" ] ; then
    if [ -z "$group" ] ; then
        adduser $user 2>/dev/null
        smbpasswd -a $user
    fi
fi
}
```

```

        fi
        if [ -n "$group" ] ; then
            adduser $user 2>/dev/null
            usermod -g $group $user
            check=$(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
    fi
fi

```

```

        DelUser
    fi
fi

```

A.2 smbda.sh

```

#!/bin/sh
# Copyright (C) 2011 – Fabio Antonio Ferreira
# http://fantonio.wordpress.com | fantonios@gmail.com
# Este trabalho esta licenciado sob uma Licenca Creative Commons
# Atribuicao-Compartilhamento pela mesma Licenca 2.5 Brasil. Para ver a
# copia
# desta licenca , 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.
# Modificacoes em 27 de Julho de 2012 por Gabriel Rocha (GBR)
# email: gabriel.rocha.gbr@gmail.com
# Versao 1.1

# == FUNCOES ==
USUARIO='whoami'
if [ "$USUARIO" != "root" ]; then
    echo
    echo "=====
    echo " ESTE PROGRAMA PRECISA SER EXECUTADO COM PERMISSOES DE SUPERUSUARIO
    echo " !
    echo " Abortando ..."
    echo "=====
    echo
    exit 1
fi

_HEAD () {
    'which clear '
    echo "=====
    echo "SISTEMA PARA ADICIONAR MAQUINA LINUX AO DOMINIO WINDOWS OU LINUX"
    echo "=====
}

_PACOTES () {
    echo "Instalando os pacotes necessarios";
    apt-get install krb5-user libpam-krb5 winbind samba smbfs smbclient
        krb5-config libkrb53 libkdb5-4 libgssrpc4 -y > /dev/null;
    check=$?
}

```

```

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 configuracoes.
    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 Backup dos arquivos de configuracoes.
    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 "Recuperacao do Backup executada com sucesso!"
    else
        echo "Falha na recuperacao do Backup."
    fi
}

_NOME_DOMINIO () {
    #Entrada do nome do dominio ao qual deseja engrekar.
    #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 Dominio:" 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 dominio
    read -p "Entre com o IP do servidor de DNS:" ip
    echo "nameserver $ip" > /etc/resolv.conf
}

_SO_SERVIDOR () {

```

```

#SO 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
        #kdc = $kdc2
        #kdc = $kdc3
        admin_server = $kdc
    }

[domain_realm]
    . $var1 = $kdc

```

```

[login]
    krb4_convert = true
    krb4_get_tickets = false" > /etc/krb5.conf

echo "Configuracao alterada com sucesso!"
}

_TESTEAD () {
    read -p "Entre com um usuario para testar sua conexao com o Active
        Directory:" user
    kinit $user@$dominio

    check=$(echo $? )
    if [ $check -eq 0 ]; then
        echo "Sua maquina 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
        passwd chat = *Enter\snew\s*\spassword:* %n\n *Retype\snew\s*\
            spassword:* %n\n *password\supdated\ssuccessfully* .

```

```

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

[printers]
comment = All Printers
browseable = no
path = /var/spool/samba
printable = yes
guest ok = no
read only = yes
create mask = 0700

[print$]
comment = Printer Drivers
path = /var/lib/samba/printers
browseable = yes
read only = yes
guest ok = no " > /etc/samba/smb.conf

echo "Configuracao 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
}

_ADDDDOMINIO () {

    echo "+++++"
    echo "++  Adicionando a Maquina no Dominio  ++"
    echo "+++++"
    # Adicionando a maquina ao dominio
    read -p "Entre com um usuario administrador de Dominio:" user
    net ads join -U $user;
    check=$(echo $?)
    clear
    # Validacao da conexao com o dominio
    if [ $check -eq 0 ]; then
        echo "Sua maquina foi adicionada no Dominio!"
    else
        echo "Falha ao adicionar a maquina no Dominio"
    fi
}

_TESTDOMINIO () {
    # Teste de requisicao ao dominio
    wbinfo -t > /dev/null
    check=$(echo $?)
    if [ $check -eq 0 ]; then
        echo "Teste de Dominio!"
    else
        echo "Falha ao testar o Dominio"
    fi
}

_FUNCAUTENTICACAO () {

```

```

# Configurando o arquivo nsswitch.conf
echo "passwd:          compat winbind
      group:          compat winbind
      shadow:         compat" > /etc/nsswitch.conf

# Teste de configuracao 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 configuracao 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 "Ja existe este diretorio !"
    else
        echo "Este diretorio nao existe !"
        echo "Criando o diretorio $HOME_DIR"
        mkdir /home/$var1
    fi
}

```

```

        sleep 2
    fi
}

_FUNC_DEL_MAQ_DOMINIO () {

    maquina=$(hostname)
    azul="{FONTE}33[0;34m"
    echo "+++++"
    echo "++  {FONTE}33[0;34m Removendo a Maquina no Dominio  ++"
    echo "+++++"

    # Remover a maquina ao dominio
    read -p "Entre com um usuario administrador de Dominio:" user
    net ads status -U $user
    check1=$(echo $?)
    clear
    # Validacao se a maquina esta no dominio
    if [ $check1 -eq 255 ]; then
        echo "A maquina $maquina nao esta no dominio"
    else
        # Validacao de remocao de maquina do dominio
        net ads leave -U $user;
        check=$(echo $?)
        clear
        if [ $check -eq 0 ]; then
            echo "Sua maquina foi removida do Dominio!"
            _RETURN_BACKUP
        else
            echo "Falha ao remover a maquina no Dominio"
        fi
    fi
fi

}

echo "===== "
# Menu de selecao
echo "Linux Active Directory:"
echo "(1) Adicionar Maquina no Dominio"
echo "(2) Remover Maquina do Dominio"
echo "(3) Verificar conexao com o Dominio"
echo "(0) Sair"

echo "Digite a opcao 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
;;
3)
 _TESTDOMINIO
;;
0)
 exit
;;
*)
 echo 'Opcao Invalida!'
esac

```