



HELTTON ERICK BRANDÃO

**ESTÁGIO: IMPLANTAÇÃO DO SISTEMA
SAMBA4 NA REDE INSTITUCIONAL DO
CEFET-MG**

LAVRAS – MG

2014

HELTTON ERICK BRANDÃO

**ESTÁGIO: IMPLANTAÇÃO DO SISTEMA SAMBA4 NA REDE
INSTITUCIONAL DO CEFET-MG**

Monografia de graduação apresentada
ao colegiado do Curso de Bacharelado
em Sistemas de informação, para
obtenção do título de Bacharel.

Hermes Pimenta de Moraes Júnior (Orientador)

Franciscarlos N. Á. Pereira (Co-Orientador)

LAVRAS – MG

2014

HELTTON ERICK BRANDÃO

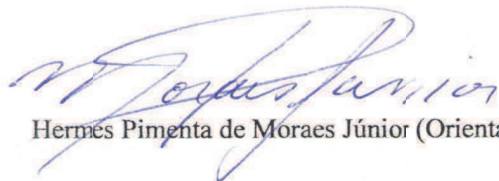
**ESTÁGIO: IMPLANTAÇÃO DO SISTEMA
SAMBA4 NA REDE INSTITUCIONAL DO CEFET-
MG**

Monografia de graduação apresentada ao
Colegiado do Curso de Bacharelado em
Sistemas de Informação, para obtenção
do título de Bacharel.

APROVADA em 9 de julho de 2014.

Neumar Malheiros

Rêmulo Maia Alves



Hermes Pimenta de Moraes Júnior (Orientador)

Franciscarlos N. A. Pereira (Co-Orientador)

**LAVRAS-MG
2014**

LISTA DE FIGURAS

Figura 1 Inclusão de cliente Windows XP no domínio	42
Figura 2 Windows XP inserido no Domínio	42
Figura 3 Inclusão de cliente Windows 7 no domínio	43
Figura 4 Inclusão de cliente Windows 8 no domínio	44
Figura 5 Windows 8 inserido no Domínio	45
Figura 6 Usuários e computadores do Active Directory	48
Figura 7 Criação de uma Unidade Organizacional	49
Figura 8 Cadastro de Usuário.....	50
Figura 9 Informações do novo usuário	50
Figura 10 Cadastrando senha para o Usuário	50
Figura 11 Inclusão de Usuário ao Grupo.....	51
Figura 12 Gerenciamento de Política de Grupo.....	52
Figura 13 Criação de GPO.....	53
Figura 14 Configuração de Políticas de Grupo.....	54
Figura 15 Bloqueio do Papel de Parede	55
Figura 16 Bloqueio do Painel de Controle.....	55
Figura 17 Painel de Controle Bloqueado	56
Figura 18 Bloqueio do <i>Prompt</i> de Comando.....	56
Figura 19 Bloqueio Editor de Registro	57
Figura 20 Teste de Bloqueio do Painel de controle.....	58
Figura 21 Teste de Bloqueio do <i>Prompt</i> de Comandos	58
Figura 22 Teste de Bloqueio do Editor de Registro	58

LISTA DE SIGLAS

AD	Active Directory
CEFET-MG IX	Centro Federal de Educação Tecnológica de Minas Gerais Unidade de Nepomuceno – MG
CEPROSUL	Centro de Educação Profissional do Sul de Minas
CN	Common Name
DAP	Directory Access Protocol
DC	Domain Controller
DN	Distinguished Name
DNS	Domain Name Server
FQDN	Fully Qualified Domain Name
FTP	File Transfer Protocol
GID	Group Identification
GPO	Group Policy Objects
KDC	Key Distribution Center
LDAP	Lightweight Directory Access Protocol
MIT	Massachusetts Institute of Technology
NetBIOS	Network Basic Input/Output System
NFS	Network File System
NTP	Network Time Protocol
OSI	Open Systems Interconnection
OU	Unidade Organizacional
PDC	Primary Domain Controller
SMB	Server Message Block
SMB/CIFS	Server Message Block/Common Internet File System
TGS	Ticket Granting Service
TI	Tecnologia da Informática
TKG	Ticket Granting Ticket
UFLA	Universidade Federal de Lavras

Sumário

1.	INTRODUÇÃO	7
1.1	Objetivos	9
1.2	Motivação	9
1.3	Metodologia	10
2.	REFERENCIAL TEÓRICO	12
2.1	Servidor Samba	13
2.2	Funcionalidades do Samba	14
2.2.1	Servidor de arquivos.....	14
2.2.2	Controlador de domínios.....	15
2.2.3	<i>Active Directory</i>	15
2.2.4	Autenticação de usuários	16
2.2.5	Resolução de nomes e IPs	19
2.2.6	Serviço de Diretório	20
3.	DESENVOLVIMENTO	23
3.1	Configuração do sistema operacional do servidor	23
3.2	Instalação do NTP (Network Time Protocol)	25
3.3	Instalação dos pré-requisitos	26
3.4	Instalação e configuração do Samba	26
3.4.1	Provisionamento do Samba4.....	27
3.4.2	Configuração do DNS.....	27
3.4.3	Configuração do Kerberos	29
3.4.4	Teste das configurações de DNS.....	30
3.4.5	Edição do arquivo de configuração do Samba	31
3.4.6	Criação das pastas compartilhadas	34
3.4.7	Criação dos compartilhamentos.....	35
3.4.8	Cadastro de usuário e grupo no Samba	35
3.4.9	Resolução de problemas com o comando <code>chown</code>	36

3.5	Inclusão de cliente Ubuntu no domínio	37
3.5.1	Configuração do sistema operacional do cliente	38
3.5.2	Instalação do NTP do cliente	38
3.5.3	Instalação do Samba.....	39
3.5.4	Edição de arquivos de configuração.....	39
3.6	Inclusão de cliente Windows XP no domínio	41
3.7	Inclusão de cliente Windows 7 no domínio	42
3.8	Inclusão de cliente Windows 8 no domínio	44
3.9	Administração do Samba a partir de um cliente Windows	45
3.9.1	Instalação e configuração do Windows 8.....	45
3.9.2	Windows 8 como administrador remoto do Samba	47
3.9.3	Cadastro de usuários com Windows 8	47
3.9.4	Aplicação de Políticas de Grupo	51
3.9.5	Configuração de Políticas de Grupo	53
3.10	Migração do Samba3 para o Samba4	59
4.	CONSIDERAÇÕES FINAIS	60
REFERÊNCIAS		60
ANEXO A – Arquivo: <code>ntp.conf</code>		64
ANEXO B – Arquivo: <code>campusix.cefetmg.br.zone</code> (DNS Master).....		66
ANEXO C – Arquivo: <code>128.16.172.in-addr.arpa</code> (DNS reverso)		68
ANEXO D – Arquivo: <code>logon.vbs</code>		69

1. INTRODUÇÃO

O presente trabalho de conclusão de curso foi realizado na forma de estágio na instituição CEFET-MG IX (Centro Federal de Educação Tecnológica de Minas Gerais *Campus* de Nepomuceno MG).

O CEFET-MG foi fundado em 23 de setembro de 1909, na cidade de Belo Horizonte em Minas Gerais, com o nome de Aprendizes Artífices de Minas Gerais. A partir dessa data, sua estrutura sofreu diversas transformações. No ano de 1942, impulsionado pela industrialização da cidade de Belo Horizonte, se tornou Escola Técnica de Belo Horizonte. Já em 1959, a Instituição foi federalizada e se tornou Escola Técnica Federal de Minas Gerais. Através de aprovação do Congresso Nacional, em 30 de junho de 1978, a Instituição se transformou em Centro Federal de Educação Tecnológica de Minas Gerais.

A transformação em Centro Federal de Ensino representou um grande avanço institucional, possibilitando a oferta de cursos de educação tecnológica em nível superior, incluindo graduação, pós-graduação *lato sensu* e licenciatura. A partir desse momento, o CEFET-MG teve unidades implantadas em várias cidades de Minas Gerais. A unidade de Nepomuceno-MG foi implantada no ano de 2007, por meio da transformação do CEPROSUL (Centro de Educação Profissional do Sul de Minas) em CEFET-MG IX.

O CEFET-MG IX possui aproximadamente 335 alunos, 44 professores e 34 servidores e colaboradores. Atualmente, a Instituição oferta três cursos: Mecatrônica, Eletrotécnica e Redes de Computadores. Esses cursos são ofertados em três modalidades, sendo elas: subsequente, integrada e com concomitância externa. A modalidade subsequente atende aos alunos que concluíram o ensino médio. A modalidade integrada atende os alunos que concluíram o ensino fundamental e a modalidade com concomitância externa atende os alunos que estão cursando o ensino médio em outras Instituições. Existem projetos de abertura de novos cursos, incluindo cursos

superiores na área tecnológica, um deles com o início previsto para o ano de 2015. O *campus* deverá expandir, e conseqüentemente, a estrutura de TI (Tecnologia em Informática) deverá acompanhar essa expansão.

Para manter a estrutura em pleno funcionamento, possibilitando expansões, o CEFET-MG IX necessita de uma rede de computadores bem estruturada e controlada. Atualmente, a estrutura da rede na Instituição é composta por quatro laboratórios de informática, 94 computadores, quatro impressoras, cinco *switchs* e sete servidores. A rede fornece aos usuários serviços de impressão, armazenamento, transferência e compartilhamento de dados. O CEFET-MG XI possui uma equipe de TI composta por dois técnicos em informática, um auxiliar administrativo e dois estagiários, e em parceria com essa equipe que o presente trabalho de estágio foi realizado.

As equipes de TI do *campus* estão subordinadas ao DRI (Departamento de Recursos de Informática) do CEFET-MG. Esse departamento está localizado em Belo Horizonte, no *Campus* I. O DRI controla tanto a liberação de recursos de informática, quanto às alterações na estrutura da rede dos diversos *campus*, com o objetivo de manter a padronização das atividades. Atualmente, um movimento de descentralização está ocorrendo, motivado pelo crescimento institucional. Por esse motivo, as atividades citadas neste trabalho, foram realizadas pela equipe de TI do CEFET-MG XI.

Os sistemas instalados nos servidores do CEFET-MG são Linux, podendo ser encontrados na internet de forma gratuita. O sistema que será instalado durante este trabalho, também possui as características supracitadas. Além de gratuitos, os sistemas Linux são altamente configuráveis e escaláveis, podendo ser adaptados para atender às necessidades das diversas redes onde são instalados.

1.1 Objetivos

Objetivos Gerais

O objetivo deste trabalho foi fazer com que o aluno utilize e aprimore os conhecimentos adquiridos nas disciplinas estudadas durante o curso de Sistemas de Informação e absorva experiências profissionais no ambiente ao qual foi inserido durante o estágio. A atividade principal prevista para ser cumprida durante o período do estágio foi a implantação de um sistema na rede de computadores do CEFET-MG IX, a fim de aprimorar e controlar o acesso aos computadores da rede e ainda manter a segurança e disponibilidade dos dados dos usuários.

Objetivos Específicos

Para a concretização dos objetivos gerais, durante o período de estágio foram realizadas as seguintes ações:

- a) a instalação, configuração e teste de um computador servidor com o sistema Samba4, com o intuito de centralizar a administração da rede;
- b) a configuração e inclusão de computadores clientes com os sistemas operacionais Ubuntu, Windows XP, Windows 7 e Windows 8 no domínio do servidor Samba4;
- c) a configuração e teste de um computador cliente Windows 8, para administrar o sistema Samba4 utilizando interface gráfica do cliente;

1.2 Motivação

A motivação deste trabalho foi baseada em um estudo realizado na rede de computadores do CEFET-MG IX. Com este estudo verificou-se que o Samba3, sistema em uso, possui muitas limitações em relação à sua nova versão o Samba4. O Samba é responsável por centralizar as informações dos usuários, fazer a autenticação desses usuários nos computadores da rede e

possibilitar o compartilhamento dos arquivos.

A configuração do Samba3, realizada por um dos técnicos há aproximadamente 7 anos, permite que apenas computadores com Windows XP, possam fazer parte do domínio. Assim, computadores com outros sistemas operacionais, não podem ser vinculados ao Samba. Para permitir a vinculação é preciso cadastrar contas diretamente nos computadores, para cada usuário que possivelmente faria uso do mesmo.

Já o Samba4 possibilita o uso de AD (*Active Directory*), uma funcionalidade nativa de servidores Windows que faz a centralização de informações de: usuários, impressoras, servidores, grupos de usuários, computadores, e políticas de segurança. Esses são chamados de objetos do AD. O Samba4 ainda permite o cadastro das versões mais recentes dos sistemas operacionais da Microsoft e dos sistemas operacionais Linux. Estes são os sistemas operacionais utilizados no *Campus IX*.

Outra vantagem que justifica a implantação do sistema Samba4 é que este possibilita ao administrador da rede gerenciar os objetos do AD, usando a interface gráfica de um cliente Windows. As limitadas funcionalidades do Samba3, ao contrário, são gerenciadas a partir do terminal do sistema operacional hospedeiro.

Assim, a implantação do Samba4 faz com que a administração dos recursos da rede seja feita de forma centralizada com o uso do AD e permite que computadores com os sistemas operacionais Windows 7, Windows 8 e Ubuntu, possam ser vinculados ao domínio.

1.3 Metodologia

O presente trabalho iniciou-se com uma análise e avaliação da rede de computadores do CEFET-MG IX. Este estudo foi realizado em conjunto com a equipe de TI, a fim de analisar os sistemas que auxiliam os administradores a monitorar e controlar a rede.

Verificou-se que as limitações do sistema Samba3, justificam a instalação do Samba4, mesmo que este esteja em fase de desenvolvimento.

Foi realizado um estudo sobre os serviços oferecidos pelo Samba4 e a forma como esses serviços são disponibilizados na rede. Em seguida, foi montado um ambiente de testes usando máquinas virtuais do Virtual Box para instalação do servidor Samba e de clientes com os sistemas operacionais Windows 7, Windows 8 e Ubuntu 12.10.

Após a instalação do Samba na máquina virtual foram feitas configurações e testes até que o sistema funcionasse de acordo com o esperado. Assim, o sistema pôde ser instalado e configurado no servidor.

Computadores de clientes com os sistemas operacionais usados no *campus* foram configurados e cadastrados no Samba para testar as funcionalidades do sistema no ambiente de rede real. Com os testes realizados, o Samba ficou pronto para ser colocado em uso na rede.

A migração da versão 3 para a versão 4 do Samba ficou prevista para ser realizada no período de férias escolares, porque neste período o *campus* fica menos movimentado, e a migração prejudica um número menor de usuários.

2. REFERENCIAL TEÓRICO

A utilização de tecnologias em redes de computadores vem sendo cada vez mais explorada e, conseqüentemente, vem se tornando uma atividade importante para a sociedade. Com o avanço no uso da internet, por todos os ramos de atividades, se torna indispensável a ligação dos computadores em redes (MENDES, 2007). “Pouco a pouco, a internet se torna o verdadeiro computador e o seu PC passa a ser cada vez mais um simples terminal, cuja única função é mostrar informações processadas por servidores remotos” (MORIMOTO, 2006, p.14).

O gerenciamento consistente das redes tornou-se crucial para manter a estrutura em funcionamento, para atender às necessidades dos usuários e, no caso das empresas, atender às expectativas dos administradores (PINHEIRO, 2006).

Para o bom funcionamento de uma organização, é de extrema importância que a rede seja segura, e que os serviços prestados sejam contínuos. Para garantir esses requisitos, geralmente são utilizados servidores. Um servidor é uma máquina compartilhada, funcionando constantemente, com a finalidade de oferecer serviços aos clientes da rede. Como exemplos há servidores de arquivos, servidores de autenticação, servidores de impressão (MORIMOTO, 2006).

Outra questão importante é a segurança dos dados. Quando os dados estão disponibilizados na rede, deve-se adotar uma política rigorosa de permissões e restrições, fazendo com que o acesso a determinado arquivo ou diretório seja restrito a pessoas autorizadas. Para solucionar esses problemas, um personagem é imprescindível: o administrador da rede. Ele tem a responsabilidade de manter a rede em funcionamento e ainda atentar pela segurança da mesma. Para isso, ele necessita de ferramentas que o auxiliem a administrar e controlar o acesso à rede (KUROSE, 2010).

O sistema instalado supriu a demanda de alguns serviços da rede. Esses serviços estão ligados ao compartilhamento de arquivos, autenticação dos usuários e centralização das configurações dos computadores clientes. Para suprir essa demanda de serviços, será utilizado o Samba4, um sistema gratuito, disponibilizado na internet.

O sistema Samba4 foi escolhido, por ser um sistema gratuito, e já estar em funcionamento na Instituição, porém em uma versão mais antiga. No decorrer deste trabalho, será explicado o funcionamento desse sistema.

2.1 Servidor Samba

O Samba é um pacote de software distribuído gratuitamente. Possui um conjunto de ferramentas que permite a comunicação entre máquinas Windows e Linux. Ele permite que os administradores tenham flexibilidade e liberdade para escolha de sistemas e equipamentos para a infraestrutura da rede (FERRARI, 2009).

O criador do samba é Andrew Tridgell, um estudante da Universidade Nacional Australiana em Camberra. O sistema surgiu a partir de sua necessidade, em interligar um computador com sistema operacional da Microsoft, a uma estação de trabalho da Sun. Isso já seria possível usando NFS (Network File System), o problema é que Andrew precisava usar um aplicativo, que dependia de suporte a NetBIOS (Network Basic Input/Output System) (MORIMOTO, 2006).

Andrew então desenvolveu um sistema para capturar o tráfego de dados na rede e realizou engenharia reversa no protocolo de compartilhamento da Microsoft, o SMB (Server Message Block) e o implementou no sistema UNIX. Dessa forma, o UNIX foi reconhecido como um servidor de arquivos Windows em sua máquina (FERRARI, 2009).

Andrew publicou seu código em 1992, deixando assim seu projeto de lado por um período. Dois anos mais tarde resolveu conectar o

computador de sua esposa que possuía o sistema operacional Windows ao seu com Linux e tudo funcionou (FERRARI, 2009). Após sua conquista, Andrew começou a aprofundar-se no projeto e conseguiu fazer melhorias e implementar outras funções para seu programa.

Andrew precisou trocar o nome de seu programa, já que uma empresa entrou em contato alegando direitos sobre o referido nome escolhido. Com o intuito de encontrar um novo nome, teve a ideia de procurar no dicionário palavras que contivessem as letras S, M e B. Dentre as opções, escolheu “Samba”. A partir daí, o projeto cresceu e hoje conta com vários programadores e milhares de usuários em todo o mundo.

2.2 Funcionalidades do Samba

Um dos objetivos dos desenvolvedores do Samba é fazer com que os sistemas Windows e Linux possam compartilhar arquivos e serviços em uma rede mista. Dessa forma, diversas funcionalidades do samba estão ligadas à interação dos sistemas.

2.2.1 Servidor de arquivos

Existem várias formas de compartilhar arquivos na rede: NFS (network file system), FTP (File transfer protocol) (SMITH, 2003). O Samba também provê compartilhamento de arquivos, através do uso do protocolo SMB. Atualmente, conhecido como SMB/CIFS (server message block/commom internet file system) ele é considerado uma melhoria do SMB feita pela Microsoft. Esse protocolo é comumente utilizado em várias plataformas cliente/servidor (RICHARD, 2002).

É possível ler, escrever, editar, apagar e copiar os arquivos no diretório do servidor, tal como se faria em arquivos locais. Fazendo uso de um servidor, consegue-se uma centralização dos arquivos, uma melhor organização dos mesmos e, ainda, uma segurança maior sobre eles, visto que

o Samba faz controle de acesso (RICHARD, 2002).

2.2.2 Controlador de domínios

Outra funcionalidade do Samba é atuar como DC (Domain Controller), também conhecido como PDC (Primary Domain Controller). O controlador de domínio é responsável por centralizar as informações de contas dos usuários, assim um usuário cadastrado no domínio pode iniciar uma sessão em qualquer computador cadastrado no domínio, usando suas informações registradas no servidor. (MORIMOTO, 2006).

Um domínio pode ser dividido em partes conhecidas como componente de domínio ou DC. Os DCs são divisões lógicas de grupos de usuários e recursos da rede. Estes podem ser divididos de forma análoga à estrutura da organização (BATTISTI, 2006). Um desses recursos é a gestão de perfis móveis. Isso possibilita que o usuário que seja cadastrado tenha acesso à sua área de trabalho independente do computador utilizado, desde que o computador faça parte do domínio (MORIMOTO, 2006).

Considere domínio por um agrupamento lógico de usuários, computadores e impressoras, chamados objetos. Esses objetos são subordinados a políticas administrativas que podem ser implementadas em toda a organização através do domínio ou apenas para um departamento, representados pelos DCs (BADDINI, 2008).

A autenticação de usuários do Samba é feita de forma integrada com o serviço de diretórios baseado no protocolo LDAP (Lightweight Directory Access Protocol). De acordo com as notas de lançamento do Samba4 (2012), com a implementação desse serviço, é possível gerenciar os recursos e objetos com AD.

2.2.3 *Active Directory*

O AD é um serviço de diretório baseado no protocolo LDAP, nativo dos sistemas Windows Server oferecido desde a versão Windows Server

2000. O AD armazena informações de usuários, impressoras, servidores, grupos de usuários, computadores e políticas de segurança. Esses elementos são denominados objetos (BATTISTI, 2006).

O AD pode ser utilizado tanto em redes de pequenas organizações, como em grandes corporações. Uma rede onde o AD está instalado pode conter um ou mais domínios. Com o uso do AD, um usuário precisa ser cadastrado em apenas um dos domínios, podendo receber permissões para usar recursos em qualquer um dos domínios. A interoperabilidade entre os domínios é possível graças à relação de confiança entre eles (BATTISTI, 2006).

Para desfrutar do uso de AD no Samba, e deixá-lo no mesmo nível dos servidores da Microsoft em relação à centralização da administração de uma rede, a equipe de desenvolvimento do Samba trabalhou por vários anos na versão 4 desse sistema. Apesar de a Microsoft liberar algumas informações sobre suas tecnologias, o maior desafio para implementação do Samba4 está na arte de determinar o funcionamento de uma rede proprietária, examinando seus protocolos, como foi feito por Andrew Tridgell na concepção do Samba (BARTLETT, 2005). Em 2012, foi lançada a primeira versão estável do Samba4 já com o AD implementado.

O AD possibilita a aplicação de GPO (Group Policy Objects). GPOs ou diretivas de grupo são usadas para aumentar a segurança em um ambiente de rede corporativo. Com a aplicação destas, consegue-se restringir o que o usuário pode ou não fazer em sua estação de trabalho. As GPOs podem ser aplicadas tanto em nível de usuário como de computadores (SILVA, 2009).

2.2.4 Autenticação de usuários

“Kerberos é um protocolo de autenticação de usuário centralizado usa criptografia para a proteção contra varias formas de ataque” (SMITH,

2003, p. 121). Foi criado pelo MIT¹ (Massachusetts Institute of Technology) como uma solução para problemas de segurança de rede. O Kerberos é uma ferramenta responsável por centralizar a autenticação de usuários e serviços em uma rede. Ele permite que o usuário informe uma única vez suas informações de *login*, assim o Kerberos verifica se o usuário é quem diz ser e se ele tem permissão de usar o serviço da rede como FTP, Proxy ou outros que fazem autenticação (SMITH, 2003).

O uso dessa ferramenta tem três objetivos básicos, são eles: oferecer autenticação de rede; fazer proteção das senhas; e permitir que os usuários façam uso dos serviços da rede fornecendo suas senhas somente uma vez (SMITH, 2003).

A autenticação de rede é necessária para que somente usuários autorizados tenham acesso aos servidores. De outro lado, os usuários precisam confirmar a identidade dos servidores utilizados, isso impede que sistemas maliciosos tenham acesso às informações, fingindo ser um servidor da rede. No modelo de protocolo Kerberos, ocorre autenticação mútua entre as entidades. Cliente e servidor executam uma sequência de ações para verificar de uma ponta se a outra é quem diz ser. Isso é feito antes que se estabeleça uma conexão segura (WALLA, 2000).

A proteção de senhas é importante, pois existem vários serviços na rede que usam senhas sem criptografia, fazendo com que elas transitem pela rede de forma desprotegida. Alguns protocolos criptografam essas senhas para resolver o problema. O Kerberos, ao invés de criptografar as senhas, ele as utiliza como uma chave de criptografia. Essa chave é usada para codificar o pacote onde as informações de *login* estão. Isso evita que a senha transite na rede, mas garante que somente o usuário com a chave correta possa ter acesso aos dados do pacote (SMITH, 2003).

¹ MIT - Massachusetts Institute of Technology - <http://web.mit.edu/>

O serviço Kerberos é composto por três partes: por um KDC (Key Distribution Center), por um usuário cliente e por um servidor com a aplicação desejada. O KDC é instalado no servidor e executa duas funções: serviço de autenticação e serviços de distribuição de tíquetes. O usuário cliente é a parte que solicita a autenticação para ter acesso a um determinado serviço da rede. O servidor com a aplicação desejada é o responsável pela execução do serviço desejado pelo cliente (WALLA, 2010).

Passo a passo de uma autenticação Kerberos segundo Smith (2003):

- 1) usuário entra com suas informações de *login* em um cliente, a fim de usar uma aplicação;
- 2) o cliente (Kerberos) envia o nome de usuário, com uma solicitação para obter um TGT (Ticket Granting Ticket) ao KDC;
- 3) o KDC verifica se o nome de usuário está em sua base de dados. Se estiver correto, o KDC envia um TGT ao cliente. Nesse bilhete, há informações como nome do usuário válido, hora de envio e tempo de vida útil do bilhete. O KDC usa a senha do usuário armazenada em sua base de dados para codificar essas informações e, somente se o usuário possuir a senha correta terá como decodificar o bilhete;
- 4) o usuário recebe o TGT. Se conseguir decodificá-lo ele envia uma nova requisição de bilhete ao KDC, dessa vez um TGS (Ticket Granting Service), ou o KDC reconhece esse pedido como válido porque o cliente utiliza informações contidas no TGT, que estava criptografado tendo a senha como chave.
- 5) o servidor envia ao cliente o TGS. Esse bilhete é codificado com uma senha que somente o KDC e a aplicação em questão conhecem. Esse novo bilhete contém além das informações do TGT, o nome da aplicação solicitada. O tempo de validade desse bilhete

é curto, devendo ser renovado caso necessário;

6) o cliente envia então uma solicitação de conexão com a aplicação, usando o TGS. Se a aplicação conseguir decodificar o bilhete, ela é a aplicação válida, e concede a conexão ao cliente.

Como foi visto nesta sequência de passos, a conexão entre o usuário e a aplicação é feita de forma segura, as senhas não transitam na rede, evitando capturas indesejadas. As trocas de bilhetes entre o cliente Kerberos, servidor Kerberos e a aplicação solicitada, é feita de forma transparente para o usuário.

2.2.5 Resolução de nomes e IPs

Existem duas formas de se identificar um hospedeiro na internet na rede, uma é pelo nome do hospedeiro, outra pelo seu IP. Usuários preferem o uso de nomes para gravar como descrição de um hospedeiro, por exemplo, é mais fácil memorizar www.nepomuceno.cefetmg.br ao invés de 200.131.3.203. Já os roteadores trabalham com IPs, estes são padronizados e organizados hierarquicamente facilitando a localização dos mesmos na rede (KUROSE, 2010).

Para traduzir os nomes dos hospedeiros em IP e os IPs em nomes, existe o DNS (Domain Name Server). Esse é um serviço composto por um servidor de nomes, que na verdade é uma base de dados distribuída, implementada de forma hierárquica e um protocolo de camada de aplicação, usado pelos computadores de usuários para requisitar consultas aos servidores de nomes (KUROSE, 2010).

Nas redes locais, os servidores DNS são utilizados para localizar recursos, tais como *hosts*, servidores, impressoras da rede, entre outros. Funciona como na internet, um cliente envia uma requisição ao servidor DNS com o nome do *host* desejado, se o nome for válido o servidor responde com o IP desse *host* e a conexão é realizada com sucesso

(SCRIMGER, 2002).

O *Active Directory* é dependente do serviço prestado pelo DNS, pois este é responsável pela nomeação de servidores e recursos e pela resolução de nomes. Por esse motivo um dos requisitos indispensáveis, para que o AD funcione corretamente é o DNS instalado e configurado corretamente (BATTISTI, 2006).

2.2.6 Serviço de Diretório

“Um diretório é uma árvore de informações. Você começa na raiz e vai percorrendo os nós-filhos até chegar ao nó que contém a informação desejada.” (TRIGO, 2007, p. 20). Assim, diretório é análogo ao nome, ou seja, algo usado para direcionar, ou ainda um caminho para chegar às informações requisitadas.

Um serviço de diretório é responsável por gerenciar entradas e atributos em um diretório e disponibilizá-los para usuários e outras aplicações (MENDONÇA, BOAS, 2006). Logo, LDAP é um conjunto de regras responsável por controlar a comunicação entre um serviço de diretórios e seus clientes. Ele surgiu de uma evolução do DAP (Directory Access Protocol). O DAP foi desenvolvido baseado no modelo OSI (Open Systems Interconnection), que foi o antecessor do TCP/IP (TRIGO, 2007).

Com a proliferação da internet, o modelo OSI foi deixado de lado e a arquitetura TCP/IP ganhou força. Por esse motivo foi criado um protocolo de acesso aos diretórios que fossem compatíveis com os moldes do TCP/IP e colocou-se o nome de LDAP. Ele foi padronizado em junho de 1993, no RFC 1487 da Internet Engineering Task Force (IETF) (TRIGO, 2007).

A organização das informações é feita de forma hierárquica, como em árvores (estrutura de dados). A raiz onde começa a busca pelas informações e os nós intermediários são diretórios, os nós folhas são os elementos que são chamados de entrada. Cada diretório possui um atributo e

as entradas podem possuir um ou mais atributos (TRIGO, 2007). Trigo (2007) cita alguns exemplos de atributos.

Para os diretórios:

c – para diretórios que representam países (Country)

o – para nomes da empresa (organization)

ou – para departamentos (organization unit)

Para as entradas:

cn – como atributo de nome (common name)

uid – para identidade de usuários (user identification)

gn – para nome próprio de uma pessoa (given name)

sn – para sobrenome de uma pessoa (surname)

As entradas possuem um DN (distinguished Name), que é usado para identificação da entrada. Esse atributo geralmente é gerado pela concatenação do atributo CN (Common Name) da entrada com o nome dos diretórios (nó pai) até a raiz (TRIGO, 2007).

Os atributos que serão utilizados nas entradas devem ser definidos em um arquivo de configuração chamado *skema*. Esse arquivo define quais atributos serão inseridos na entrada e como ela será estruturada. Alguns atributos devem ser configurados como obrigatórios, ou seja, uma entrada só é inserida no diretório se os atributos obrigatórios forem inseridos (TRIGO, 2007).

Algumas características de um sistema de diretórios, começando pela centralização e organização dos dados. Isso evita redundância de informações e facilita o acesso de clientes às informações que ele precisa

(TRIGO, 2007).

Outra característica é que a forma hierárquica com que as informações são armazenadas facilita a pesquisa de informações, porém dificulta para inserir, alterar ou excluir registros.

3. DESENVOLVIMENTO

O presente trabalho foi desenvolvido no CEFET-MG IX. O estagiário desenvolveu durante o período de estágio, atividades ligadas ao monitoramento de uso de internet, atendimento aos usuários para esclarecer suas dúvidas e ainda auxílio aos técnicos em atividades eventuais ligadas à área de TI.

Por fim como atividade mais complexa realizada durante o período de estágio, foi instalado, configurado e testado no ambiente de rede do *campus*, o sistema Samba4.

A instalação e configuração do sistema Samba4 foram feitas pelo estagiário, em conjunto com um dos técnicos da equipe de TI do CEFET-MG IX, este técnico foi citado no presente relatório como co-orientador.

Após um estudo bibliográfico sobre os serviços ofertados pelo Samba4, iniciou-se a instalação e configuração do sistema. Num primeiro momento, a instalação, configuração e testes foram feitos em uma máquina virtual. Clientes também foram configurados no ambiente virtual para possibilitar os testes.

3.1 Configuração do sistema operacional do servidor

Para a instalação do sistema Samba4, foi usado o sistema operacional Debian wheezy. O disco rígido foi particionado de modo a atender às necessidades do Samba. Alguns subdiretórios foram instalados em partições diferentes da partição raiz do sistema, estratégia usada para facilitar a recuperação do sistema no caso de algum problema em uma partição isolada.

As partições criadas fora da partição raiz do sistema foram: `/home`, `/var`, `/boot`. A partição `/home` é onde ficam os dados dos usuários da rede, a partição `/var` é onde as bibliotecas e arquivos variáveis dos

processos que estão em execução e a partição `/boot` é a responsável por conter as configurações de inicialização do sistema operacional.

O sistema operacional foi instalado com interface gráfica, mas pode ser instalado apenas em modo texto, pois, a administração do servidor Samba4, é feita geralmente de forma remota usando um computador Windows cliente, facilidades proporcionada pelo AD. Abaixo segue as configurações feitas, antes da instalação do Samba4.

O arquivo `/etc/profile` deve ser editado, a linha 1 deve ser trocada pela linha 2:

1)

```
PATH="/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin"
```

2)

```
PATH="/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/opt/samba/bin:/opt/samba/sbin"
```

Essa alteração faz com que os comandos do Samba (arquivos binários) contidos em `/opt/samba/bin` e `/opt/samba/sbin`, sejam reconhecidos e executados em qualquer local da árvore de diretório. Após a alteração, para efetivá-la, é necessário executar o comando que faz o carregamento do arquivo `/etc/profile`, abaixo segue o comando:

```
#source /etc/profile
```

O arquivo `hostname` deve ser editado. Esse possui uma única linha que representa o nome do servidor. O nome escolhido é associado ao sistema a ser instalado. Segue abaixo o conteúdo deste arquivo.

```
samba-server
```

Outro arquivo é o `/etc/hosts`. Esse arquivo armazena os nomes que as interfaces do servidor irão responder podendo cada IP responder por

um ou mais nomes. O Debian utiliza este como método preferencial de resoluções de nome e IPs. Abaixo segue o conteúdo deste arquivo já configurado no servidor Samba.

```
127.0.0.1 localhost
127.0.1.1 samba-server
172.16.128.254 samba-server.campusix.cefetmg.br
samba-server

# The following lines are desirable for IPv6
capable hosts
::1 localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
```

O arquivo `/etc/resolv.conf` informa ao sistema operacional o domínio da rede e o IP do servidor DNS. Abaixo seguem as duas linhas que compõem esse arquivo. A primeira linha indica qual é o domínio padrão, e a segunda linha indica o IP do servidor DNS:

```
search campusix.cefetmg.br
nameserver 172.16.128.254
```

3.2 Instalação do NTP (Network Time Protocol)

O NTP é um protocolo para sincronização de relógios de um conjunto de dispositivos de uma rede, ele é importante porque os dispositivos podem atrasar ou adiantar seus relógios, em relação aos horários oficiais e isso gera alguns problemas. O mais comum deles é que a conexão segura entre um cliente e um servidor de internet pode ser recusada caso o cliente esteja com seu relógio fora de sincronia. Outro problema é na confiança dos *logs* gerados por determinados servidores da rede, a imprecisão do horário de um *log* pode atrapalhar na detecção da causa de um problema.

Para instalação do NTP servidor foram executados os comandos abaixo:

```
#aptitude install ntp
```

O arquivo de configuração do servidor NTP é o `/etc/ntp.conf`. Para que o servidor possa manter seu relógio atualizado, e assim padronize o relógios dos dispositivos da rede de acordo com o horário oficial, deve-se adicionar as seguintes linhas nesse arquivo:

```
server 127.127.1.0
fudge 127.127.1.0 stratum 10
:%s/debian/south-america/g
```

O arquivo com as configurações já realizadas pode ser visto no Anexo A. Após essas configurações reiniciar o serviço usando o comando:

```
#service ntp restart
```

3.3 Instalação dos pré-requisitos

Os pré-requisitos necessários para instalação do Samba foram disponibilizados na página oficial do sistema: https://wiki.samba.org/index.php/Samba_4/OS_Requirements, esses requisitos foram instalados com o comando abaixo:

```
# apt-get install build-essential libacl1-dev
libattr1-dev libblkid-dev libgnutls-dev
libreadline-dev python-dev python-dnspython gdb
pkg-config libpopt-dev libldap2-dev dnsutils
libbsd-dev attr krb5-user docbook-xsl libcups2-dev
acl
```

Com a instalação dos requisitos o próximo passo é a instalação do Samba4. O arquivo de instalação do Samba4 está disponível em: <https://ftp.samba.org/pub/samba/stable/>

3.4 Instalação e configuração do Samba

Após o *download*, o arquivo fonte foi copiado para a pasta `/src` que é o repositório onde os arquivos de programas ficam armazenados no Debian. A sequência de comandos abaixo foi executada e após segue a explicação de cada um:

```
#tar -zvxvf samba-4.1.5.tar.gz
# ./configure --prefix=/opt/samba
#make
#make install
```

O primeiro comando é responsável por descompactar o arquivo fonte do sistema. O segundo comando checa os pré-requisitos antes da instalação e define o local de instalação do Samba, o terceiro comando faz a compilação dos arquivos, e o último faz a instalação do sistema.

3.4.1 Provisionamento do Samba4

Para o provisionamento da base de dados do Samba foi executado o comando abaixo:

```
#samba-tool domain provision --domain=CAMPUSIX --
realm=CAMPUSIX.CEFETMG.BR --server-role=dc --
adminpass=cefetSPT328 --dns-backend=BIND9_DLZ --
use-rfc2307
```

Segue a explicação de cada item do comando:

-domain: define o nome do domínio usado na rede.

-realm: define o FQDN (Fully qualified domain name).

-server-role: define a função do servidor, no caso controlador de domínio.

-dns-backend: define como será feita a comunicação do Samba com o DNS no caso BIND9_DLZ.

-use-rfc2307: define as regras para autenticação de clientes linux e windows, obtendo uid e gid (Group identification) a partir dos atributos no AD.

3.4.2 Configuração do DNS

No provisionamento do Samba4, é gerado o arquivo `/opt/samba/private/named.conf`, este é o arquivo de

configuração do DNS interno. O carregamento de zonas do AD é feito dinamicamente. Abaixo segue o conteúdo desse Arquivo.

```
dlz "AD DNS Zone" {
    database "dlopen
/opt/samba/lib/bind9/dlz_bind9.so";
};
```

Este arquivo deve ser referenciado no arquivo de configuração do DNS no sistema operacional hospedeiro, `/etc/bind/named.conf`. O referenciamento foi feito adicionando uma linha no arquivo de configuração do Bind9_DLZ e dando ao `bind` (usuário *default* do DNS) permissões especiais, para que ele consiga fazer leitura e execução do arquivo `/opt/samba/private/named.conf`. Abaixo segue a sequência de comandos:

```
# echo 'include "/opt/samba/private/named.conf";'
>> /etc/bind/named.conf

# chown bind.bind /opt/samba/private/named.conf
```

O primeiro comando insere a informação `"/opt/samba/private/named.conf";` no arquivo `/etc/bind/named.conf` fazendo assim o referenciamento supracitado, e o segundo altera o usuário e grupo proprietário do arquivo, para `bind` dando as permissões especiais ao `bind`.

Outro arquivo que foi editado é o `/etc/bind/named.conf.option`. Abaixo seguem as linhas que foram inseridas nesse arquivo.

```
dnssec-validation auto;
allow-query {172.16.128.0/25;};
allow-recursion {172.16.128.0/25;};
tkey-gssapi-keytab "/opt/samba/private/dns.keytab";
```

O arquivo indicado na última linha inserida é o `/opt/samba/private/dns.keytab`, que possui informações do serviço DNS na base do Kerberos. Além dessas alterações é preciso alterar o usuário e grupo proprietário desse arquivo para o usuário padrão do DNS. O comando abaixo executa essa função.

```
#chown bind.bind /opt/samba/private/dns.keytab
```

Nos arquivos de zonas (DNS) `/var/cache/bind/campusix.cefetmg.br.zone` (DNS master) e `/var/cache/bind/128.16.172.in-addr.arpa` (DNS reverso) são configurados as entradas do servidor DNS interno do Samba, que responderam às requisições dos clientes. Esses arquivos podem ser visualizados respectivamente no Anexo B e C.

3.4.3 Configuração do Kerberos

O provisionamento do Samba gera o arquivo de configuração do Kerberos, o `/opt/samba/private/krb5.conf`. Esse arquivo deve ser copiado para a pasta `/etc`, do sistema operacional. Abaixo segue o conteúdo desse arquivo.

```
[libdefaults]
    default_realm = CAMPUSIX.CEFETMG.BR
    dns_lookup_realm = false
    dns_lookup_kdc = true
```

Para testar o Kerberos executa-se o comando `kinit` seguido do usuário administrador do Samba.

```
#kinit administrator@CAMPUSIX.CEFETMG.BR
```

O sistema solicita a senha do usuário, assim o Kerberos irá emitir um *ticket*. Caso algum problema ocorra, os arquivos que devem ser revisados

são o `resolv.conf` e o `krb5.conf`. Os detalhes do *ticket* gerado podem ser visualizados usando o comando abaixo:

```
#klist
```

Este lista os atributos do *ticket* gerado. Abaixo está o *feedback* gerado pelo comando:

```
Ticket cache: FILE:/tmp/krb5cc_0
Default principal:
administrator@CAMPUSIX.CEFETMG.BR
Valid starting Expires Service principal
10-04-2014      18:52:49      11-04-2014      04:52:49
krbtgt/CAMPUSIX.CEFETMG.BR@CAMPUSIX.CEFETMG.BR
renew until 11-04-2014 18:52:23
```

3.4.4 Teste das configurações de DNS

Após as configurações realizadas alguns testes foram realizados, garantindo que as configurações dos serviços do servidor Samba4 estão prontas e quaisquer problemas nesses serviços seriam identificados, pois, comprometeriam o sistema. Abaixo segue os comandos e uma explicação deles.

Teste dos arquivos de zonas

```
# host -t SRV _ldap._tcp.campusix.cefetmg.br.
```

Esse comando testa o DNS. Ele verifica se o serviço está respondendo às entradas dos arquivos de zonas, o retorno desse comando pode ser conferido abaixo:

```
_ldap._tcp.campusix.cefetmg.br has SRV record 0 100
389 samba-server.campusix.cefetmg.br
```

Caso algum problema ocorra os arquivos `/var/cache/bind/campusix.cefetmg.br.zone` e `/var/cache/bind/128.16.172.in-addr.arpa` devem ser revisados.

Teste do serviço Kerberos

```
# host -t SRV _kerberos._tcp.campusix.cefetmg.br.
```

Esse comando testa o Kerberos, caso as configurações estejam corretas, o retorno para esse comando é:

```
_kerberos._tcp.campusix.cefetmg.br has SRV record 0
100 88 samba-server.campusix.cefetmg.br
```

Teste do hostname

```
# host -t A samba-server.campusix.cefetmg.br
```

Testa se o servidor responde pelo hostname configurado e abaixo segue o *feedback* deste comando, que confirma o hostname e o ip do mesmo:

```
samba-server.campusix.cefetmg.br has address
172.16.128.254.
```

3.4.5 Edição do arquivo de configuração do Samba

O `smb.conf` é o arquivo de configuração do Samba, este é gerado no provisionamento do sistema já com algumas configurações básicas. Esse arquivo é executado pelo servidor toda vez que um usuário inicia uma sessão, em um computador pertencente ao domínio do Samba.

O arquivo é dividido em seções, algumas alterações devem e foram feitas de acordo com as necessidades da rede, abaixo seguem as instruções da seção global, primeira seção do arquivo já configurado para a rede do CEFET-MG IX.


```
[global]
    workgroup = CAMPUSIX
    realm = CAMPUSIX.CEFETMG.BR
    netbios name = SAMBA-SERVER
    server role = active directory domain
controller
    server services = s3fs, rpc, nbt, wrepl, ldap,
cldap, kdc, drepl, winbind, ntp_signd, kcc,
dnsupdate
    idmap_ldb:use rfc2307 = yes
    allow dns updates = nonsecure
    dns forwarder = 172.16.128.254
    dns update command = nsupdate
    interfaces = eth0
    bind interfaces only = yes
    template shell = /bin/bash
    root preexec =
/opt/samba/var/locks/sysvol/campusix.cefetmg.br/scr
ipts/logon %U %D
```

As alterações mais importantes feitas nessa seção, foram a inclusão de duas linhas `/opt/samba/var/locks/sysvol/campusix.cefetmg.br/scripts/logon` e `script = logon.vbs`. Essas indicam *scripts* que foram criados, a fim de criar pastas para o usuário cadastrado no Samba e realizar o mapeamento destas, montando-as nos cliente Windows.

O *script* `/opt/samba/var/locks/sysvol/campusix.cefetmg.br/scripts/logon` é o responsável por criar uma pasta no servidor Samba para o usuário recém-cadastrado. No momento do carregamento do arquivo `smb.conf`, o sistema acessa o *script* `logon`, nele existem condições que verificam se o usuário está cadastrado no Samba e se ainda não possui uma pasta desse usuário no servidor. Se as duas condições forem satisfeitas será criada uma pasta no servidor samba que será onde os arquivos do usuário ficam armazenados no servidor. Abaixo segue o conteúdo do *script*:

```
#!/bin/bash

user=$1
```

```

dominio=$2

for usuarios in $(samba-tool user list |
egrep -v      "^Administrator|Guest|dns-
fileserver|krbtgt"); do
    if [ $usuarios = $user ] && [ ! -d
'/home/'$dominio/$user ]; then
        mkdir -p '/home/'$dominio/$user
        chown $user '/home/'$dominio
        chown -R $user '/home/'$dominio/$user
        chmod 770 -R '/home/'$dominio/$user

        net sam set homedir $usuarios \\.\pdc-
cix\\$usuarios
        net sam set homedrive $usuarios Z:
        net sam set logonscript $usuarios
logon.vbs

    fi
done

```

O

script

/opt/samba/var/locks/sysvol/campusix.cefetmg.br/scripts/logon.vbs é responsável por mapear as pastas do servidor e montá-las no lado cliente Windows. A extensão vbs do *script* refere-se a *Visual Basic Scripting Edition*, desenvolvida pela Microsoft, assim os clientes Windows conseguem reconhecer e executar o *script*. O arquivo *logon.vbs* pode ser visto no Anexo D.

O arquivo *logon.vbs* é responsável por fazer o mapeamento e montagem das pastas do usuário, do grupo e a pasta pública, no cliente windows. Isso é feito no momento em que este consegue iniciar uma sessão em um cliente Windows pertencente ao domínio.

As seções *netlogon* e *sysvol*, são compartilhamentos padrão do Samba, que também são criadas no momento do provisionamento. São necessários para a operação do servidor como AD.

[netlogon]

```

        path =
/opt/samba/var/locks/sysvol/campusix.cefetmg.br/scripts
        read only = No
        #browseable = No

[sysvol]
    path = /opt/samba/var/locks/sysvol
    read only = No
    #browseable = No

```

As demais seções do arquivo `smb.conf` devem ser criadas pelo administrador da rede, essas referem-se ao compartilhamento das pastas criadas no servidor para os grupos do AD.

3.4.6 Criação das pastas compartilhadas

No subdiretório `/home`, do sistema operacional foram criadas as pastas que serão compartilhadas na rede, para que os usuários possam armazenar seus arquivos. A pasta `admin` criada para que o grupo de usuários que se enquadrem no perfil administrativo é vinculada. Segue abaixo uma sequência de comandos que serão explicados logo a seguir:

```

#cd /home
#mkdir grupos
#cd /grupos
#mkdir admin

```

O primeiro comando navega o usuário do sistema até o subdiretório `/home`, o segundo comando cria a pasta `grupos` em `/home`, o terceiro comando faz com que o usuário do sistema entre na pasta criada e o quarto cria a pasta `admin` dentro de `grupos`. Assim o caminho absoluto da pasta `admin` é: `/home/grupos/admin` e é nessa pasta que os usuários que têm os perfis que enquadram no grupo `admin`, armazenam e acessam os arquivos comuns ao grupo.

Para os demais grupos foram executados os mesmos passos para a criação das pastas. Os grupos criados no CEFET-MG são: `publico`, `admin`, `biblioteca`, `estágio`, `eletrônica`, `direção`, `enfermagem`, `mecatrônica`, `ntic`, `nae`,

sae, ser, redes, formgeral, engeletrica. Os alunos serão alocados em outro domínio. Após a criação das pastas, executa-se o comando abaixo, alterando as permissões das subpastas da pasta /home/grupos:

```
#chmod 3770 /home/grupos/*
```

3.4.7 Criação dos compartilhamentos

O compartilhamento das pastas criadas no item anterior, com os usuários cadastrados no Samba é feito através das seções de compartilhamentos do arquivo `smb.conf`. São nessas seções que são colocadas as regras de compartilhamento dessas pastas com cada grupo.

Neste item será mostrado como foram feitas as regras de compartilhamento da pasta `admin`, os demais compartilhamentos seguem o mesmo padrão. O arquivo `/opt/samba/etc/smb.conf` com todas as seções e compartilhamentos, pode ser visualizado no Anexo E. Abaixo segue o compartilhamento `admin`:

```
[admin]
path = /home/grupos/admin
read only = No
force create mode = 0660
force directory mode = 0750
veto files = /*.mp3/*.mpg/*.mpeg/*.avi/*.jpg/
hide files = /*.ini/*.log/
browseable = No
```

O que está entre colchetes é o nome do compartilhamento, o qual recebe o mesmo nome do grupo para facilitar o entendimento. O que vem abaixo do nome são as regras do compartilhamento, essas regras são para a pasta do grupo criada no servidor Samba.

3.4.8 Cadastro de usuário e grupo no Samba

Após a criação dos compartilhamentos no arquivo de configuração do Samba e da pasta compartilhada no servidor foram criados os grupos

vinculados a essas pastas. O comando que cria um grupo no sistema Samba é:

```
#samba-tool group add admin
```

Esse comando criou o grupo admin, os usuários adicionados neste grupo terão acesso à pasta admin, no servidor. Para criar um usuário o comando é:

```
#samba-tool user add administrador
```

Após a criação do usuário administrador, o mesmo deve ser adicionado ao grupo admin, e para isso executou-se o comando:

```
# samba-tool group addmembers admin administrador
```

Para vincular o grupo admin à pasta admin do servidor, precisa-se alterar o usuário e grupo proprietário desta pasta para root e admin (root = usuário e admin=grupo).

O problema é que o usuário root é do sistema operacional e o grupo admin é do Samba. O comando chown é quem altera o dono de um arquivo ou pasta, para que ele consiga puxar informações de um grupo do samba e vinculá-lo a um arquivo ou pasta do sistema operacional, são necessárias algumas configurações, para essas configurações deve-se seguir as orientações do item 3.4.9

Após as configurações realizadas, o arquivo chown deve ser usado e assim vincular o grupo à pasta, para que os usuários do grupo tenham as devidas permissões sobre os arquivos. Abaixo segue o comando:

```
# chown root.admin /home/grupos/admin
```

3.4.9 Resolução de problemas com o comando chown

O winbind é o *daemon* que integra autenticação e mecanismos de serviços de diretórios no AD. As informações dos usuários e grupos do

Samba são acessadas pelos clientes Linux através do winbind. Os comandos abaixo são necessários para criar um *link* simbólico na pasta `/lib` do sistema operacional, para que ele reconheça o arquivo `libnss_winbind.so` da pasta `/lib` do Samba.

```
# cd /lib
# ln -s /opt/samba/lib/libnss_winbind.so
libnss_winbind.so.2
# ldconfig -v | grep winbind
```

Depois o arquivo `/etc/nsswitch.conf` foi editado indicando o winbind como fonte para busca de informações de usuários e grupos. Abaixo segue o conteúdo deste arquivo e as alterações feitas são na primeira e na segunda linha, com a inserção de winbind ao final das linhas.

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

hosts:           files mdns4_minimal
[NOTFOUND=return] dns mdns4
networks:        files

protocols:       db files
services:        db files
ethers:          db files
rpc:             db files
netgroup:        nis
```

Assim na execução do comando `chown`, o sistema consegue acesso as informações dos usuários e grupos cadastrados no servidor Samba.

3.5 Inclusão de cliente Ubuntu no domínio

Para inserir um computador cliente com Ubuntu, no domínio do samba4 é preciso: fazer algumas configurações em arquivos do sistema operacional, instalar o NTP, o Kerberos, o *Winbind* e o Samba. Nas seções abaixo segue instruções de como isso deve ser feito.

3.5.1 Configuração do sistema operacional do cliente

No sistema operacional do cliente, algumas configurações são semelhantes as do servidor. No arquivo `/etc/hostname` deve ser colocado o nome do computador. Como exemplo o primeiro computador configurado para instalação do Samba cliente se localiza na sala de TI, e seu *hostname* é NTI-01, assim o arquivo é composto por uma única linha:

```
NTI-01
```

O arquivo `/etc/hosts` deve ser editado inserindo uma linha que aponta qual o ip, nome totalmente qualificado e o aliás do servidor Samba.

```
127.0.0.1 localhost
127.0.1.1 NTI-01
172.16.128.1 gw-cix.campusix.cefetmg.br gw-cix

# The following lines are desirable for IPv6
capable hosts
::1 localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
```

O arquivo `/etc/resolv.conf` assim como no sistema servidor, informa ao sistema operacional o domínio padrão e o IP do servidores DNS. Observa-se abaixo as duas linhas que compõem este arquivo, e são idênticas a do servidor Samba.

```
search campusix.cefetmg.br
nameserver 172.16.128.1
```

3.5.2 Instalação do NTP do cliente

O NTP foi instalado no cliente para fazer a sincronização de relógio com o servidor, abaixo estão dois comandos, um para instalar o serviço e outro para indicar o endereço do computador onde o servidor do NTP está instalado:

```
# Apt-get install ntpdate
#ntpdate 172.16.128.254
```

3.5.3 Instalação do Samba

A instalação do Samba, como também suas dependências no cliente, é feita usando os seguintes comandos:

```
#aptitude update
#aptitude upgrade
#aptitude install samba smbcliente winbind kbr5-doc
kbr5-user kbr5-config
```

Os dois primeiros comandos são para atualização da lista de *softwares* do repositório, e o terceiro é para instalação do Samba, servidor winbind e do Kerberos. Porém a instalação do Kerberos feita dessa forma pode ocorrer algum problema (foi o caso de um computador cliente Ubuntu testado), isso é resolvido executando o comando abaixo para reinstalação:

```
#apt-get install kbr5-kdc kbr5-config kbr5-clients
libpam-kbr5 kbr5-user
```

Após a instalação do Kerberos o domínio por omissão será solicitado, como o domínio será configurado no arquivo do Kerberos, `krb5.conf`, essa solicitação pode ser ignorada.

3.5.4 Edição de arquivos de configuração

Arquivo `smb.conf`

O arquivo de configuração do cliente Samba, `/etc/samba/smb.conf` possui as mesmas características do servidor, centralizando as regras de funcionamento do sistema. No cliente ele possui apenas a seção `global`, nela encontram-se as entradas necessárias para que o usuário consiga iniciar uma sessão usando um cliente Linux. Abaixo segue o conteúdo do documento.

```
[global]
    security = ads
    realm = CAMPUSIX.CEFETMG.BR
    workgroup = CAMPUSIX
```



```

winbind enum users = yes
winbind enum groups = yes
template homedir = /home/%D/%U
template shell = /bin/bash
winbind refresh tickets = yes
idmap config * : backend = rid
idmap config *:range=100000-200000
idmap config *:backend = tdb
idmap config CAMPUSIX: default = yes
idmap config CAMPUSIX: range = 100000-200000
winbind use default domain = yes
obey pam restrictions = yes

```

Arquivo commom-session

O arquivo `/etc/pam.d/common-session` deve ser editado, para que o sistema possa criar a pasta local para o usuário, quando este fizer *login*. Abaixo segue o conteúdo desse arquivo:

```

session      [default=1]                pam_permit.so
session      requisite                  pam_deny.so
session      required                   pam_permit.so
session      optional                    pam_krb5.so
minimum_uid=1000
session      required   pam_unix.so
session      optional   pam_winbind.so
session      optional   pam_ck_connector.so
nox11
session      required   pam_mkhome.so   skel=/etc/skel/
umask=0077

```

Arquivo nsswitch.conf

Da mesma forma que no servidor o arquivo `/etc/nsswitch.conf` foi editado indicando o winbind como fonte para busca de informações de usuários e grupos. Abaixo segue o conteúdo deste arquivo e as alterações feitas são na primeira e na segunda linha, com a inserção de winbind ao final das linhas

```

passwd:      compat winbind
group:       compat winbind
shadow:      compat

```

```
hosts:                                files  mdns4_minimal
[NOTFOUND=return] dns mdns4
networks:                              files

protocols:                             db files
services:                              db files
ethers:                                 db files
rpc:                                    db files
netgroup:                               nis
```

Após estas configurações o sistema deve ser reiniciado e o próximo *login* já pode ser feito por usuários do AD.

3.6 Inclusão de cliente Windows XP no domínio

Para inserir um computador cliente com Windows XP no domínio do samba4 é preciso acessar as propriedades do sistema operacional. Isso é feito clicando-se no menu Iniciar e com o botão direito do mouse sobre a opção Meu computador, escolher a opção Propriedades.

Abre assim a janela Propriedades do sistema, nesta selecionar a aba Alterar nome e clicar no botão Alterar. Abrirá a janela, Alterações de nome do computador, nesta janela completar os campos de textos Nome do computador e Domínio. No caso do CEFET-MG o domínio é CAMPUSIX e o nome do computador é escolhido de acordo com o setor onde ele se encontra.

Clicar no botão Mais, que abrirá a janela Sufixo DNS e nome NetBIOS deste computador. No campo de texto desta janela digita-se o FQDN, no caso do CEFET-MG o FQDN é CAMPUSIX.CEFETMG.BR. Com essas configurações feitas clicar no botão OK.

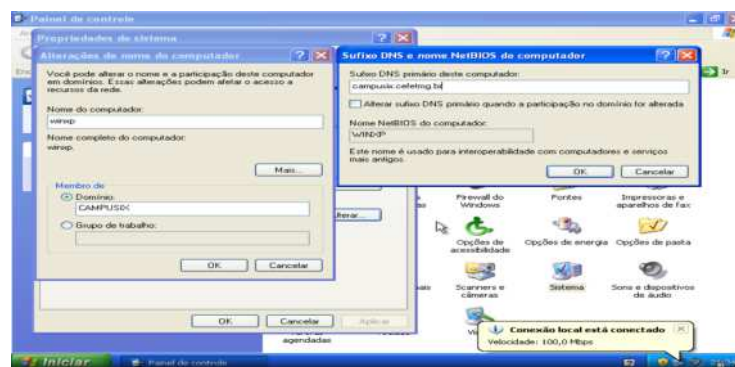


Figura 1 Inclusão de cliente Windows XP no domínio

O sistema irá requisitar o nome de usuário e senha do administrador do sistema Samba. Se o sistema reconhecer o usuário e a senha estiver correta será exibida uma janela de boas vindas.

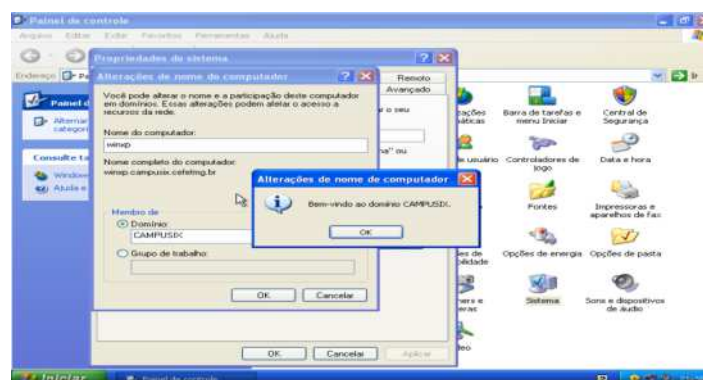


Figura 2 Windows XP inserido no Domínio

3.7 Inclusão de cliente Windows 7 no domínio

Para inserir um computador cliente com Windows 7 no domínio do samba4 é preciso acessar as propriedades do sistema operacional. Isso é feito clicando-se no menu Iniciar e com o botão direito do mouse sobre a opção Meu computador, escolhe-se a opção Propriedades. Abrirá a janela de informações básicas do computador, nesta clica-se em

Configurações avançadas do sistema, que se encontra na lateral esquerda da janela.

Abre assim a janela Propriedades do sistema, nesta seleciona-se a aba Nome do computador e clica-se no botão Alterar, abrirá a janela Alteração de nome/Domínio do computador, nesta janela completa-se os campos de textos Nome do computador e Domínio. No caso do CEFET-MG o domínio é CAMPUSIX e o nome do computador é escolhido de acordo com o setor onde ele se encontra.

Clica-se no botão Mais, abrirá a janela Sufixo DNS e nome NetBIOS do computador. No campo de texto desta janela digita-se o FQDN, CAMPUSIX.CEFETMG.BR. Com essas configurações feitas clica-se no botão OK.

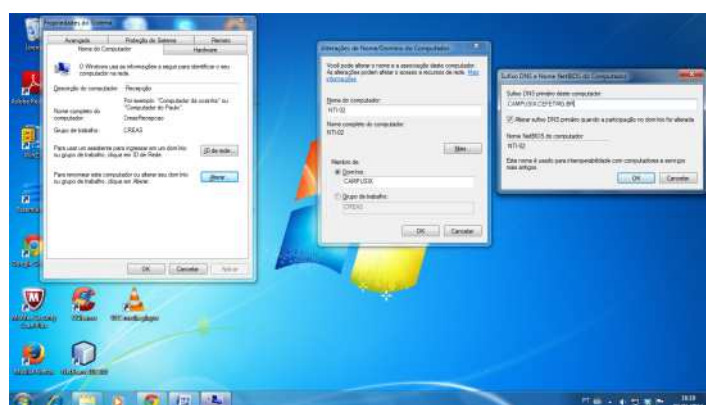


Figura 3 Inclusão de cliente Windows 7 no domínio

Assim como no Windows XP o sistema irá requisitar o nome de usuário e senha do administrador do Samba4, e se o sistema reconhecer o usuário e a senha estiver correta, também será exibida a janela de boas vindas.

3.8 Inclusão de cliente Windows 8 no domínio

Para inserir um computador cliente com Windows 8 no domínio do samba4 é preciso acessar as configurações avançadas do sistema operacional. Isso é feito clicando com o botão direito do mouse sobre a opção Meu computador, seleciona-se a opção Propriedades. Abrirá a janela Sistema, nesta clicar em Configurações avançadas do sistema, que se encontra na lateral esquerda da janela.

Abre assim a janela Propriedades do sistema, nesta seleciona-se a aba Nome do computador e clica-se no botão Alterar, abrirá a janela Alterações de nome/Domínio do computador, nesta janela completa-se os campos de textos Nome do computador e Domínio. No caso do CEFET-MG o domínio é CAMPUSIX e o nome do computador é escolhido de acordo com seu setor.

Clica-se no botão Mais, que abrirá a janela Sufixo DNS e nome NetBIOS do computador. No campo de texto desta janela digita-se o FQDN, CAMPUSIX.CEFETMG.BR. Com essas configurações feitas clica-se no botão OK.

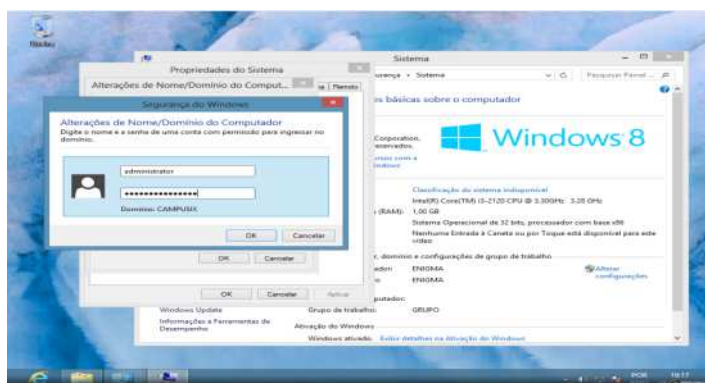


Figura 4 Inclusão de cliente Windows 8 no domínio

Assim como nas demais versões Windows o sistema requisitará o nome de usuário e senha do administrador do Samba4. Se o sistema

reconhecer o usuário e a senha estiver correta, será exibida a janela de boas vindas.

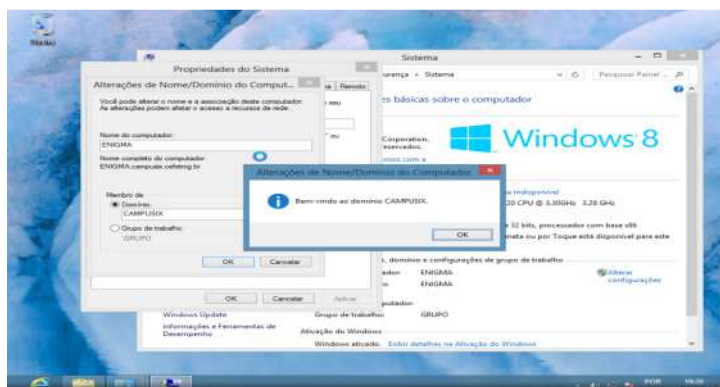


Figura 5 Windows 8 inserido no Domínio

3.9 Administração do Samba a partir de um cliente Windows

O Samba4 assim como o Windows Server versões 2008 e 2012, permitem ser gerenciados a partir de um cliente Windows. O cliente precisa apenas pertencer ao domínio do servidor e ter as ferramentas de administração para servidores remotos instalados. A seguir será explicado como um cliente com o Windows 8 pode gerenciar o AD e as GPOs do Samba4. O Windows 8 foi escolhido porque possui todas as ferramentas administrativas das versões anteriores a ele.

3.9.1 Instalação e configuração do Windows 8

No gerenciamento do sistema Samba, foi utilizada uma máquina virtual com sistema Windows 8. A justificativa do uso de uma máquina virtual para este fim, é que a equipe de TI, não possuía até o momento da realização do estágio, um computador com Windows 8 instalado que pudesse ser utilizado exclusivamente para gerenciamento do sistema .

O adaptador de rede da máquina virtual onde o sistema Windows 8 foi instalado, foi configurado no modo *bridge*. Dessa forma a máquina

virtual recebe IP dentro da faixa de IPs do servidor Samba, permitindo assim a comunicação entre eles.

A instalação do sistema operacional foi feita sem nenhuma particularidade, ou seja, da forma padrão, como se instala em um computador de usuário comum.

Para habilitar o Windows 8 como gerenciador remoto do Samba, foi preciso instalar as ferramentas de administração para servidores remotos. A instalação é feita usando o pacote Windows6.2-KB2693643-x64.msu, este pode ser baixado a partir da URL <http://www.microsoft.com/download/details.aspx?id=28972>.

O pacote deve ser instalado usando permissões de administrador do sistema operacional. Após a instalação, as opções de ferramentas de administração para servidores remotos estão disponíveis no painel de controle. Para habilitar estas ferramentas deve-se navegar até Painel de controle, clicar na opção Programas e acessar Ativar ou desativar recursos do Windows.

Irá abrir outra janela, nesta clica-se na opção Ferramentas de administração de servidor remoto, e seleciona-se todas as opções internas (todos os *checkbox* internos à opção devem ser selecionados), feito isso clica-se em Ok.

Para conferir se as ferramentas administrativas estão habilitadas, navega-se até Painel de controle, se a opção Ferramentas administrativa do Windows Server quando puder ser visualizada, implica que as configurações foram bem sucedidas.

3.9.2 Windows 8 como administrador remoto do Samba

Para administrar o Samba remotamente, com o sistema operacional Windows 8 é preciso que este esteja no domínio, e o *login* deve ser feito com o administrador do Samba.

Após o *login*, é preciso copiar a pasta PolicyDefinitions, que se encontra em `c:\windows\policyDefinition`, para o servidor Samba4. Esta deverá substituir a pasta `/opt/samba/var/locks/sysvol/campusix.cefetmg.br/PolicyDefinitions`.

Após a cópia, o Samba deve ser reiniciado, assim o sistema reconhece as configurações feitas no cliente Windows.

3.9.3 Cadastro de usuários com Windows 8

Existem duas formas de se cadastrar um usuário no Samba, uma é usando o terminal no servidor e outra usando a interface gráfica do cliente Windows com as ferramentas administrativas instaladas.

Ao cadastrar um usuário a partir do Windows 8 pode-se, além de vinculá-lo a um grupo, para que este tenha acesso aos arquivos remotos deste grupo, pode-se vinculá-lo também a uma GPO. A GPO é aplicada ao usuário e não ao grupo do usuário, porém uma forma de aplicar GPO a um conjunto de usuários é usando OU (unidade organizacional). As OUs são subdivisões da organização, nelas os usuários são agrupados de acordo com seu perfil dentro da empresa.

A GPO não é aplicada sobre o grupo, porque um usuário pode fazer parte de vários grupos, isso é determinado de acordo com a necessidade deste, em acessar documentos compartilhados. No CEFET-MG um usuário do grupo direção também faz parte do grupo administrativo, pois, ele precisa ter acesso aos documentos compartilhados nas duas pastas. Se a GPO fosse

aplicada no grupo, iria causar problemas, pois as configurações podem ser diferentes para cada grupo, e o usuário que estiver nos dois grupos teria duas GPOs aplicadas a ele, causando atritos entre elas.

Uma OU pode conter todos os usuários de uma organização, ou pode conter apenas alguns usuários, abaixo será explicado como foi criada uma das OUs do CEFETM-MG. Depois a explicação é sobre como cadastrar um usuário e vinculá-lo a um grupo e a uma OU.

Para criar uma OU, o primeiro passo é acessar Ferramentas administrativas do sistema, no Painel de controle. Dentro de Ferramentas administrativa do sistema acessa-se a opção Usuários e computadores do Active Directory, na janela que irá abrir clica-se em `campusix.cefetmg.br`, é neste diretório que estão os componentes do AD, como usuários, grupos, computadores e OUs, conhecidos também com objetos do AD.

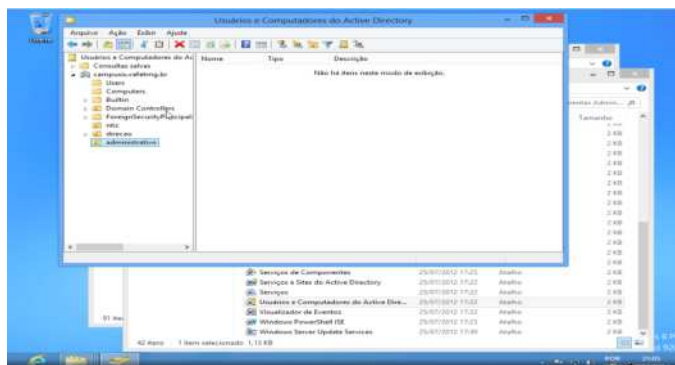


Figura 6 Usuários e computadores do Active Directory

Com o botão direito do *mouse* no diretório `campusix.cefetmg.br` seleciona-se a opção Novo, dentro desta opção, seleciona-se Unidade Organizacional. Abrirá uma nova janela, nesta digita-se o nome de OU desejado e seleciona-se o *checkbox*

Proteger contêiner contra exclusão acidental como o nome disse essa opção é para segurança, clica-se então no botão OK.

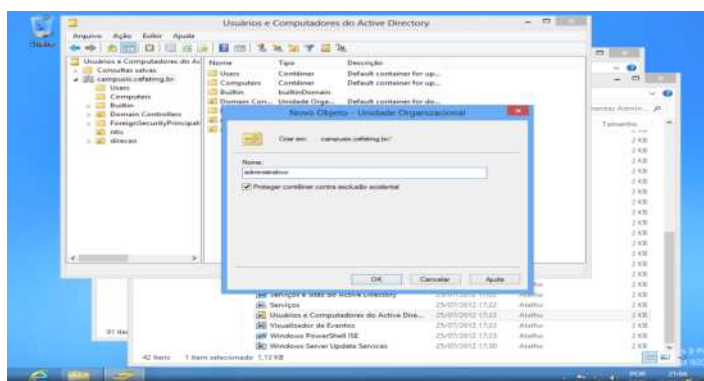


Figura 7 Criação de uma Unidade Organizacional

No CEFET-MG IX foram criadas três OUs: ntic, direcao e administrativo. Ntic é a OU que conterà os técnicos de TI, eles precisam ter acessos menos restritos às funcionalidades do sistema. A OU direção conterà os usuários da direção do CEFET-MG, estes não terão os mesmos privilégios dos técnicos de TI, mas terão mais privilégios que os demais usuários. Já a OU administrativo terá uma GPO mais restrita.

Criada a OU, o próximo passo é cadastrar o usuário. Seleciona-se a OU que o usuário será vinculado, com um duplo clique no *mouse*. Escolher a opção Novo> Usuário isso pode ser visto na Figura 8. Na nova janela, Novo Objeto - Usuário, preencher os campos com as informações do usuário a ser cadastrado, a criação do usuário Wagner pode ser vista na Figura 9. Clica-se então em Avançar, na nova janela, entrar com o nome e senha do usuário, e marcar os dois *checkboxes*: A senha nunca expira e O usuário não pode trocar a senha, esta janela pode ser vista na Figura10.

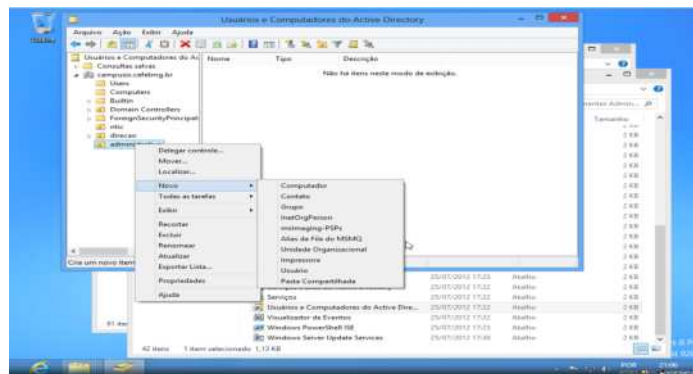


Figura 8 Cadastro de Usuário

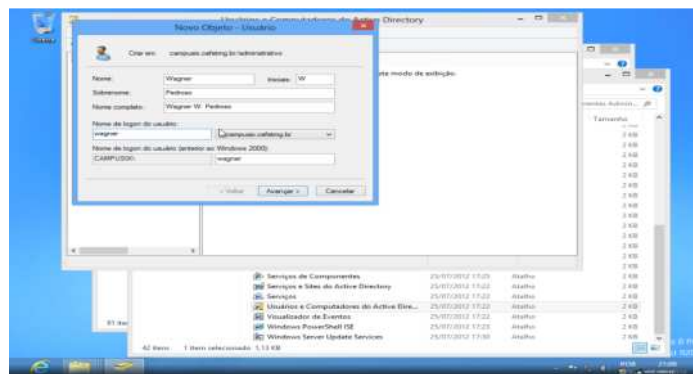


Figura 9 Informações do novo usuário

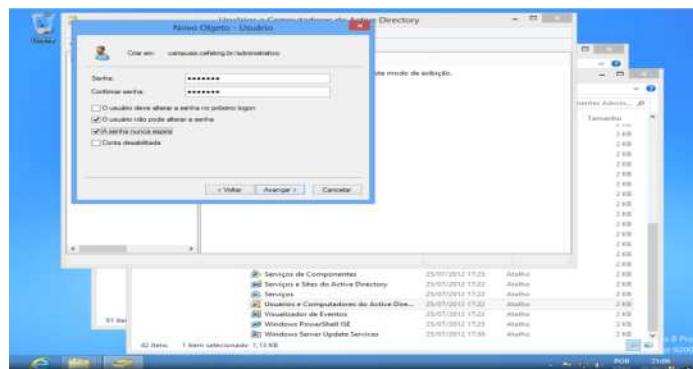


Figura 10 Cadastrando senha para o Usuário

O próximo passo é adicionar o usuário a um grupo. Ainda no diretório campusix.cefetmg.br, selecionar o subdiretório user. É

neste diretório que estão os usuário e grupos já cadastrados no Samba. O usuário criado, Wagner, foi adicionado ao grupo admin, para isso, deve-se selecionar o grupo com um duplo clique no *mouse*. Abrirá uma nova janela, propriedades de admin, clica-se em Avançar, abrirá então a janela Selecionar Usuários . . . , que pode ser vista na Figura 11. Nesta janela digita-se o nome do usuário cadastrado, e clica-se em Verificar Nomes, o sistema irá acessar a todas as informações deste usuário na base de dados do Samba, após isso clica-se em OK e o usuário é adicionado.

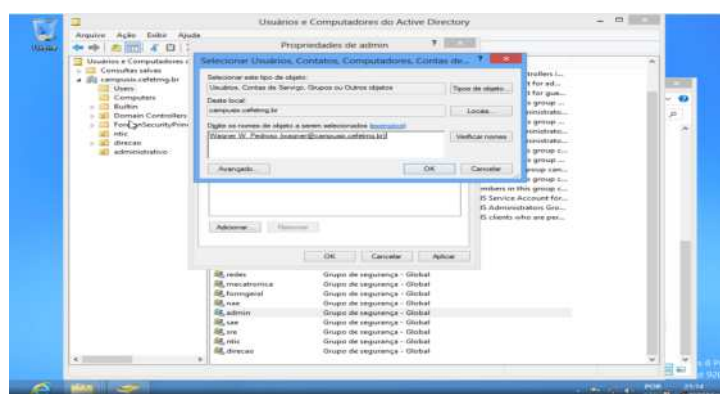


Figura 11 Inclusão de Usuário ao Grupo

3.9.4 Aplicação de Políticas de Grupo

O uso de GPO centraliza as configurações de políticas de grupos, essas configurações eram feitas nos computadores da rede de forma individual, ou seja, cada computador era configurado separadamente. Com a centralização, as políticas podem ser alteradas no servidor, de acordo com o perfil do usuário através da OU que este pertença, ou seja, alguns usuários podem ser restritos a algumas alterações do sistema operacional e outros usuários podem ter acesso a elas. Um exemplo prático disso é que, um usuário pode alterar o papel de parede do computador e outro usuário não. Abaixo segue explicações de como aplicar GPO em uma OU.

A aplicação de GPO é feita através das ferramentas administrativas no painel de controle. Dentro das ferramentas administrativas entra-se em Gerenciamento de Políticas de Grupo abre-se uma nova janela, esta pode ser vista na Figura 12. Na nova janela, deve-se navegar até o diretório administrativo, que é referente a OU criada no item anterior. Para chegar até este diretório segue-se o seguinte caminho: Floresta: campusix.cefetmg.br->Domínios->campusix.cefetmg.br->administrativo. Em administrativo, clicar com o botão direito do *mouse* e escolher a opção Criar um GPO neste Domínio ...

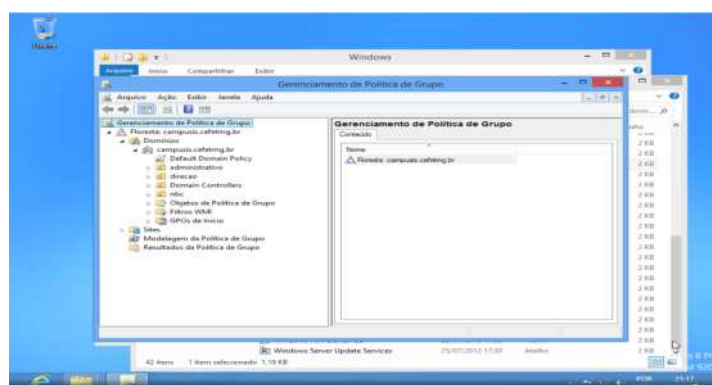


Figura 12 Gerenciamento de Política de Grupo

O próximo passo é escolher um nome para GPO criada, no CEFET-MG os nomes das GPOs são idênticos aos nomes das OUs, para facilitar o entendimento da ligação entre elas.

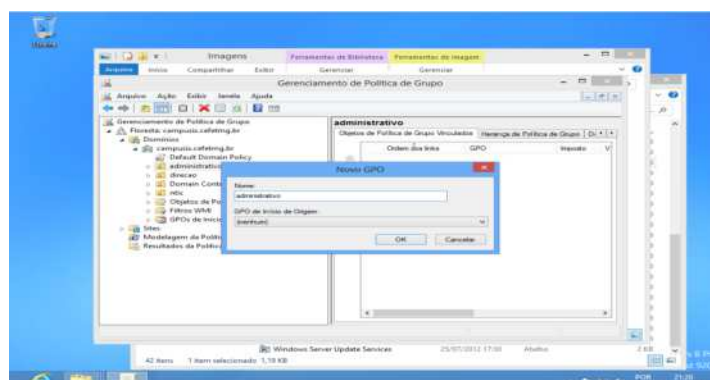


Figura 13 Criação de GPO

3.9.5 Configuração de Políticas de Grupo

As GPOs são criadas por padrão com as regras de bloqueio desabilitadas, ou seja, nenhuma restrição, assim para criar restrições aos usuários das OUs, é preciso configurar as diretivas de grupo.

Algumas restrições foram configuradas para os usuários da OU administrativo são elas: bloqueio do papel de parede, bloqueio do *prompt* de comando, bloqueio do painel de controle e bloqueio do regedit (editor de registro do sistema windows). Outras restrições ou até liberações podem ser configuradas, em cada OU, de acordo com as necessidades dos administradores da rede.

Para ter acesso as diretivas, seleciona-se a GPO na janela Gerenciamento de Políticas de Grupo, no quadro da direita, referente à GPO escolhida, deve-se selecionar a GPO com o botão de direito do *mouse*, escolher a opção Editar. Abre a janela Editor de Gerenciamento de Política de Grupo.

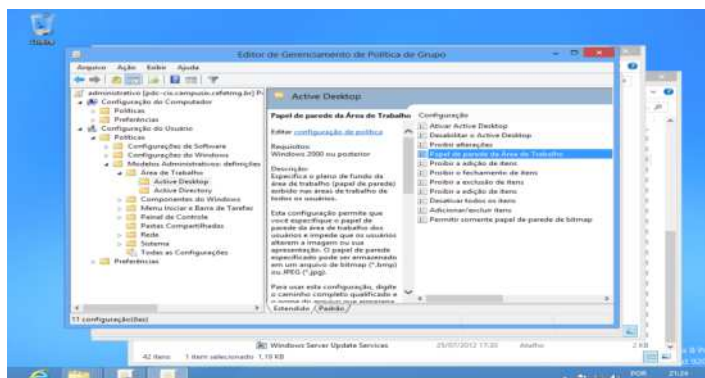


Figura 14 Configuração de Políticas de Grupo

Abaixo seguem algumas restrições que foram habilitadas na OU administrativo e como configurá-las:

1) Bloqueio de papel de parede: as diretivas referentes ao bloqueio do papel de parede da área de trabalho, estão no diretório *Active Desktop* e o caminho para chegar até este diretório é : Configuração do usuário->Políticas->Modelos Administrativos: definições->active Desktop. O caminho até o diretório também pode ser visto na figura 14.

No quadro da direita, seleciona-se a opção Papel de parede da Área de Trabalho com um duplo clique. Na nova janela, seleciona-se a opção habilitado. E dentro de Opções , no campo de texto Nome do papel e parede, digita-se o caminho absoluto de uma imagem que será padronizada como papel de parede, esta pode estar salva no servidor Samba.

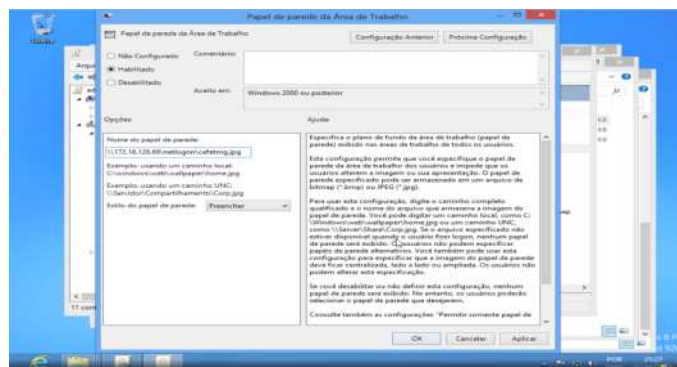


Figura 15 Bloqueio do Papel de Parede

2) Bloqueio do painel de controle: as diretivas referentes ao bloqueio do painel de controle estão no diretório Painel de controle, o caminho para chegar a este diretório é: configuração do usuário->Políticas->Modelos Administrativos: definições->Painel de Controle.

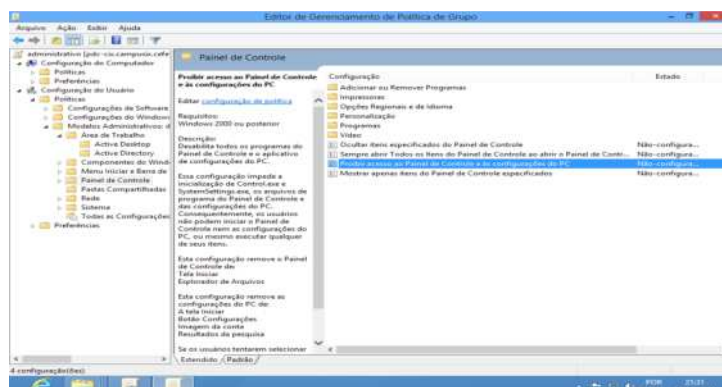


Figura 16 Bloqueio do Painel de Controle

No quadro da direita, seleciona-se a opção Proibir acesso ao Painel de Controle e às configurações do PC, com um duplo clique. Na nova janela, seleciona-se a opção habilitado.

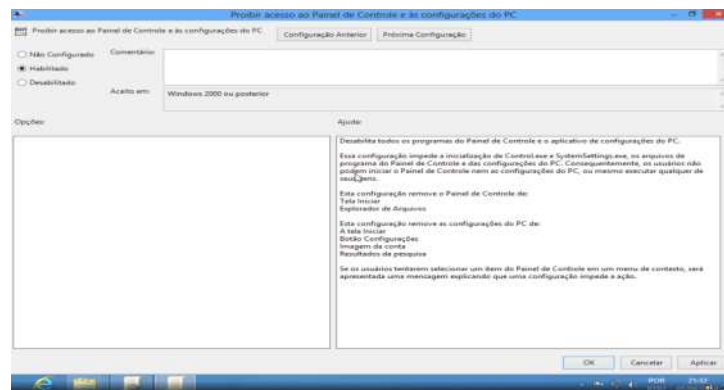


Figura 17 Painel de Controle Bloqueado

3) Bloqueio do *prompt* de comando: as diretivas relacionadas ao *prompt* de comando, estão no diretório Sistema, acessado partir de : Configuração do usuário->Políticas->Modelos Administrativos: definições->Sistemas.

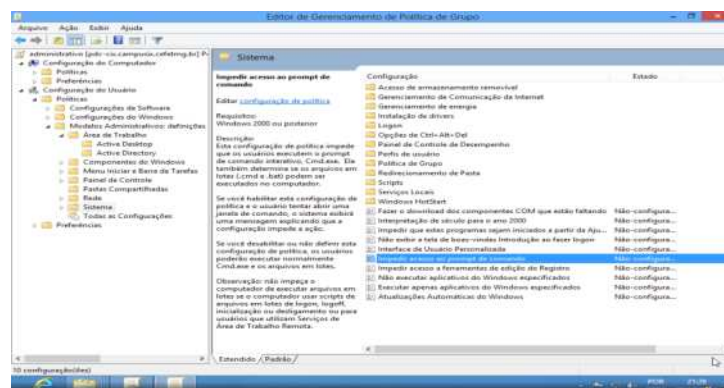


Figura 18 Bloqueio do Prompt de Comando

No quadro da direita, seleciona-se a opção *Impedir acesso ao prompt de comando*, com um duplo clique. Na nova janela, seleciona-se a opção *habilitado*, com essa opção selecionada o usuário não conseguirá ter acesso ao *prompt* de comando.

4) Bloquear o editor de registro do sistema: para acessar as configurações relacionadas ao regedit, navegar até impedir acesso as ferramentas de edição do registro, esta opção está abaixo da opção referente ao *prompt* de comando vista no tópico anterior. Com um duplo clique nesta opção, abrirá uma nova janela, nesta marcar a opção Habilitado.

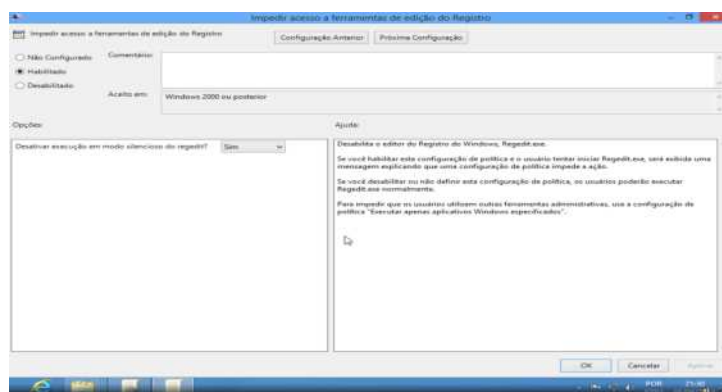


Figura 19 Bloqueio Editor de Registro

Com as diretivas de grupo configuradas, os usuários cadastrados na OU administrativo, que acessarem os computadores da rede, pertencentes ao domínio, não conseguiram trocar o papel de parede, nem ter acesso as configuração do painel de controle, nem acessar o editor de registro do sistema e nem mesmo terá acesso ao *prompt* de comando.

Para testar se a GPO está configurada aplica-se aos seus usuários uma sessão em um computador com windows7, usando uma conta de usuário, cadastrado e vinculado a OU administrativo. Assim verificou-se que ele não conseguia mais acessar os itens bloqueados. As janelas com as mensagens referentes aos testes executados podem ser vista nas figuras 20, 21, 22.

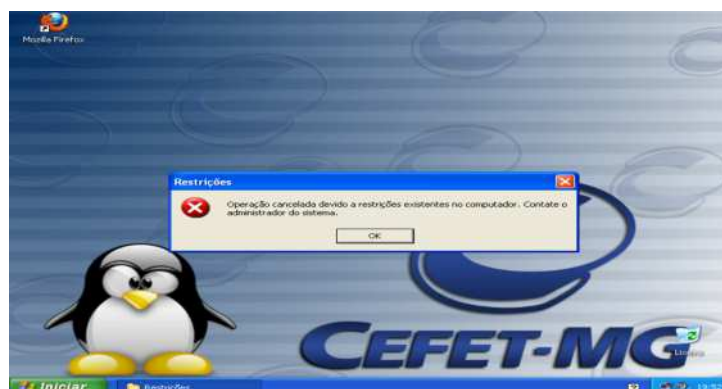


Figura 20 Teste de Bloqueio do Painel de controle



Figura 21 Teste de Bloqueio do *Prompt* de Comandos



Figura 22 Teste de Bloqueio do Editor de Registro

3.10 Migração do Samba3 para o Samba4

O sistema Samba4 foi instalado, configurado e devidamente testado, porém não foi colocado em uso na rede do CEFET-MG no período de estágio, devido ao fato de que essa implantação poderia trazer impactos ao funcionamento da rede em um momento impróprio. Desse modo, os técnicos de TI planejaram a migração do Samba3 para o Samba4, em um período em que os alunos se encontrassem de férias, dessa forma, os impactos da migração do sistema seriam minimizados.

O Samba4 permite a migração da base de dados do Samba3, porém isso não será feito. O retrabalho necessário para preencher a base de dados recadastrando os usuários, é justificado pela reorganização, pois muitos usuários que ainda estão cadastrados no Samba3, não são mais servidores ou colaboradores do CEFET-MG IX. Essa desorganização é justificada pela dificuldade de administrar uma base de dados dinâmica usando linha de comando, como é no Samba3.

4. CONSIDERAÇÕES FINAIS

O desenvolvimento deste trabalho proporcionou ao estagiário a oportunidade de conhecer um ambiente profissional, onde o mesmo pôde aplicar os seus conhecimentos adquiridos durante o curso de Sistemas de Informações, e do mesmo modo contribuiu para o melhor desenvolvimento de suas atividades futuras. O estagiário participou de diversas reuniões, juntamente com a equipe de TI do CEFET-MG IX, realizadas a fim de levantar problemas na rede que justificassem a realização do estágio, fato que proporcionou a aquisição de experiências ao estagiário.

Os estudos realizados sobre o sistema Samba revelaram que o sistema proposto para implantação agrega benefícios substanciais para a administração da rede. O uso de *Active Directory*, principal serviço disponibilizado pelo Samba, funciona centralizando as informações dos usuários, computadores, impressoras, grupos de usuários e políticas de segurança, fazendo com que o Sistema Samba trabalhe de forma parecida com os servidores da Microsoft.

Esses benefícios supracitados justificam as dificuldades que a implantação de um sistema ainda em desenvolvimento traz para os envolvidos nesta ação. Pode-se citar como exemplo, testes no sistema alterando arquivos de configurações para resolver problemas ainda não solucionados pela equipe de desenvolvimento do Samba4.

Alguns serviços são necessários para um melhor funcionamento da rede do CEFET-MG IX, porém ainda não foram instalados. No estudo realizado, verificou-se que outros sistemas poderiam ser instalados para sanar essas necessidades, a fim de auxiliar os técnicos de TI na administração e monitoramento da rede. Para tal alguns sistemas foram

propostos: o Cacti² para monitoramento da rede e o Bacula³ para *backups* dos arquivos dos usuários, e dos servidores da rede.

² Cacti - Software de monitoramento de rede – site oficial disponível em: <http://www.cacti.net/>.

³ Bacula - Conjunto de programas que permite administradores de redes gerenciarem: backups, restauração e verificação de dados- site oficial disponível em: <http://www.bacula.org/>.

REFERÊNCIAS

BADDINI, F. Gerenciamento de Redes com Microsoft Windows XP Profissional. São Paulo: Érica. 2008.

BARTLETT, A. Samba 4 - Active Directory. Disponível a partir do site oficial do samba. Disponível em: <http://www.samba.org/samba/news/articles/abartlet_thesis.pdf> acesso em 08/01/2014.

BATTISTI, J. Windows XP – Home & Profissional Para Usuários e Administradores. Rio de Janeiro: Axcel.2006.

FERRARI, S. R. Sambando com Linux. Rio de Janeiro: Alta Books. 2009.

KUROSE, J. F. Redes de computadores e a Internet - Uma abordagem top-down. São Paulo: Traduzido por Opportunity Translations. Revisado por Zucchi, Wagner L. 2010.

MENDES, D.R. Redes de Computadores –Teoria e Prática. São Paulo: Novatec. 2007.

MENDONÇA, N.; BOAS, Tiago V. Samba3 - Totalmente Reformulado para Samba. Rio de Janeiro: Brasport. 2006.

MORIMOTO.C.E. Redes e Servidores Linux - Guia Prático. Porto Alegre: Sul. 2006. Notas de lançamento do Samba4. Disponível em <<http://www.samba.org/samba/history/samba-4.0.0.html>>. Acesso em 23 de janeiro de 2014.

PINHEIRO, J.M.S. Gerenciamento de Redes de Computadores: Uma Breve Introdução. 2006. Disponível em: <http://www.projetoderedes.com.br/artigos/artigo_gerenciamento_de_redes_de_computadores.php>. Acesso em: 08 de janeiro de 2014.

RICHARD, S. Just what is SMB?. 2002. Disponível no site oficial do samba <www.samba.org>, ou no link direto: <http://www.samba.org/cifs/docs/what-is-smb.html>> Acesso em 20 de janeiro de 2014.

SCRIMGER.R.;LASALLE.P.;PARIHAR.M.;GUPTA.M. TCP/IP - A Bíblia. Rio de Janeiro: Campus. 2002.

SILVA, L.H.R. – Tecnologia em Redes de Computadores – Uso de GPO's na Segurança de Domínios Corporativos. Rio de Janeiro: Ciência Moderna.2009.

SMITH, R. W. Redes Linux Avançadas. Rio de Janeiro: Ciência Moderna. 2003.

TANENBAUM, A. S. Redes de Computadores - Rio de Janeiro: Campus, 2003.

TRIGO, C. H. – Openldap: Uma Abordagem Integrada. São Paulo: Novatec. 2007.

WALLA, M. Kerberos Explained. 2000. Disponível em: <<http://technet.microsoft.com/en-us/library/bb742516.aspx>>. Acessado em 15 de janeiro de 2014.

ANEXO A – Arquivo: ntp.conf

```
# /etc/ntp.conf, configuration for ntpd; see
ntp.conf(5) for help
#driftfile /var/lib/ntp/ntp.drift

server 127.127.1.0
fudge 127.127.1.0 stratum 10

# Enable this if you want statistics to be logged.
#statsdir /var/log/ntpstats/

statistics loopstats peerstats clockstats
filegen loopstats file loopstats type day enable
filegen peerstats file peerstats type day enable
filegen clockstats file clockstats type day enable

# You do need to talk to an NTP server or two (or
three).
#server ntp.your-provider.example
# pool.ntp.org maps to about 1000 low-stratum NTP
servers. Your #server will
# pick a different set every time it starts up.
Please consider #joining the
# pool: <http://www.pool.ntp.org/join.html>
server 0.south-america.pool.ntp.org iburst
server 1.south-america.pool.ntp.org iburst
server 2.south-america.pool.ntp.org iburst
server 3.south-america.pool.ntp.org iburst

# Access control configuration; see
/usr/share/doc/ntp-#doc/html/acopt.html for
# details. The web page
#<http://support.ntp.org/bin/view/Support/AccessRes
trictions>
# might also be helpful.
# Note that "restrict" applies to both servers and
clients, so a #configuration
# that might be intended to block requests from
certain clients could #also end
# up blocking replies from your own upstream
servers.
```

```
# By default, exchange time with everybody, but
# don't allow #configuration.
restrict -4 default kod notrap nomodify nopeer
noquery
restrict -6 default kod notrap nomodify nopeer
noquery

# Local users may interrogate the ntp server more
# closely.
restrict 127.0.0.1
restrict ::1

# Clients from this (example!) subnet have
# unlimited access, but only #if
# cryptographically authenticated.
#restrict 192.168.123.0 mask 255.255.255.0 notrust

# If you want to provide time to your local subnet,
# change the next #line.
# (Again, the address is an example only.)
#broadcast 192.168.123.255

# If you want to listen to time broadcasts on your
# local subnet, de-#comment the
# next lines. Please do this only if you trust
# everybody on the #network!
#disable auth
#broadcastclient
```

ANEXO B – Arquivo: campusix.cefetmg.br.zone (DNS Master)

```

$ORIGIN campusix.cefetmg.br.
$TTL 1W
@           IN SOA    pdc-cix.campusix.cefetmg.br.
root.campusix.cefetmg.br. (
    2014042301    ; serial
    2D           ; refresh
    4H           ; retry
    6W           ; expiry
    1W )         ; minimum

                IN NS pdc-cix.campusix.cefetmg.br.
                IN A   172.16.128.254
;

pdc-cix         IN A     172.16.128.254
gc._msdcs       IN A     172.16.128.254

3ad3f63c-4b9e-4bf5-91ad-c1085887c739._msdcs      IN
CNAME pdc-cix
;
; global catalog servers
_gc._tcp        IN SRV 0 100 3268      pdc-cix
_gc._tcp.Default-First-Site-Name._sites      IN SRV 0
100 3268      pdc-cix
_ldap._tcp.gc._msdcs IN SRV 0 100 3268      pdc-cix
_ldap._tcp.Default-First-Site-Name._sites.gc._msdcs
                IN SRV 0 100 3268 pdc-cix
;
; ldap servers
_ldap._tcp      IN SRV 0 100 389pdc-cix
_ldap._tcp.dc._msdcs IN SRV 0 100 389pdc-cix
_ldap._tcp.pdc._msdcs IN SRV 0 100 389pdc-cix
_ldap._tcp.11526eb2-dda1-4044-b085-
9e2d8f2929bc.domains._msdcs      IN SRV 0 100
389 pdc-cix
_ldap._tcp.Default-First-Site-Name._sites      IN
SRV 0 100 389 pdc-cix
_ldap._tcp.Default-First-Site-Name._sites.dc._msdcs
                IN SRV 0 100 389 pdc-cix
;
; krb5 servers
_kerberos._tcp      IN SRV 0 100 88      pdc-cix
_kerberos._tcp.dc._msdcs IN SRV 0 100 88 pdc-cix
_kerberos._tcp.Default-First-Site-Name._sites      IN
SRV 0 100 88      pdc-cix

```

```
_kerberos._tcp.Default-First-Site-  
Name._sites.dc._msdcs IN SRV 0 100 88 pdc-cix  
_kerberos._udp          IN SRV 0 100 88      pdc-cix  
; MIT kpasswd likes to lookup this name on password  
change  
_kerberos-master._tcp    IN SRV 0 100 88  
      pdc-cix  
_kerberos-master._udp    IN SRV 0 100 88  
      pdc-cix  
;  
; kpasswd  
_kpasswd._tcp            IN SRV 0 100 464 pdc-cix  
_kpasswd._udp            IN SRV 0 100 464      pdc-cix  
;  
; heimdal 'find realm for host' hack  
_kerberos                IN TXT          CAMPUSIX.CEFETMG.BR
```


ANEXO D – Arquivo: logon.vbs

On Error Resume Next

```
set objNetwork= CreateObject("WScript.Network")
```

```
objNetwork.MapNetworkDrive "X:", "\\pdc-  
cix\publico"
```

```
strDom = objNetwork.UserDomain  
strUser = objNetwork.UserName
```

```
Set objUser = GetObject("WinNT://" & strDom & "/" &  
strUser & ",user")
```

```
For Each objGroup In objUser.Groups
```

```
    Select Case ucase(objGroup.Name)
```

```
        Case "ADMIN"
```

```
            objNetwork.RemoveNetworkDrive "F", "true"
```

```
            objNetwork.MapNetworkDrive "F:", "\\pdc-  
cix\admin", "true"
```

```
        Case "BIBLIOTECA"
```

```
            objNetwork.RemoveNetworkDrive "G", "true"
```

```
            objNetwork.MapNetworkDrive "G:", "\\pdc-  
cix\biblioteca", "true"
```

```
        Case "ESTAGIO"
```

```
            objNetwork.RemoveNetworkDrive "H", "true"
```

```
            objNetwork.MapNetworkDrive "H:", "\\pdc-  
cix\estagio", "true"
```

```
        Case "ELETRONICA"
```

```
            objNetwork.RemoveNetworkDrive "I", "true"
```

```
            objNetwork.MapNetworkDrive "I:", "\\pdc-  
cix\eletronica", "true"
```

```
        Case "MECATRONICA"
```

```
            objNetwork.RemoveNetworkDrive "J", "true"
```

```
            objNetwork.MapNetworkDrive "J:", "\\pdc-  
cix\mecatronica", "true"
```

```
        Case "DIRECAO"
```

```
            objNetwork.RemoveNetworkDrive "L", "true"
```

```
        objNetwork.MapNetworkDrive          "L: ", "\\pdc-
cix\direcao", "true"

        Case "ENFERMAGEM"
            objNetwork.RemoveNetworkDrive "M", "true"
            objNetwork.MapNetworkDrive     "M: ", "\\pdc-
cix\enfermagem", "true"

        Case "NTIC"
            objNetwork.RemoveNetworkDrive "N", "true"
            objNetwork.MapNetworkDrive     "N: ", "\\pdc-
cix\ntic", "true"

        Case "NAE"
            objNetwork.RemoveNetworkDrive "O", "true"
            objNetwork.MapNetworkDrive     "O: ", "\\pdc-
cix\nae", "true"

        Case "SAE"
            objNetwork.RemoveNetworkDrive "P", "true"
            objNetwork.MapNetworkDrive     "P: ", "\\pdc-
cix\sae", "true"

        Case "SRE"
            objNetwork.RemoveNetworkDrive "Q", "true"
            objNetwork.MapNetworkDrive     "Q: ", "\\pdc-
cix\sre", "true"

        Case "FORMGERAL"
            objNetwork.RemoveNetworkDrive "R", "true"
            objNetwork.MapNetworkDrive     "R", "\\pdc-
cix\formgeral", "true"

        Case "ENGELETRICA"
            objNetwork.RemoveNetworkDrive "S", "true"
            objNetwork.MapNetworkDrive     "S", "\\pdc-
cix\engeletrica", "true"

        Case "REDES"
            objNetwork.RemoveNetworkDrive "T", "true"
            objNetwork.MapNetworkDrive     "T", "\\pdc-
cix\redes", "true"
        End Select
    Next
```

ANEXO E – Arquivo: smb.conf

```

# Global parameters
[global]
    workgroup = CAMPUSIX
    realm = CAMPUSIX.CEFETMG.BR
    netbios name = PDC-CIX
    server role = active directory domain
controller
    server services = s3fs, rpc, nbt, wrepl, ldap,
cldap, kdc, drepl, winbind, ntp_signd, kcc,
dnsupdate
    idmap_ldb:use rfc2307 = yes
    allow dns updates = nonsecure
    dns forwarder = 172.16.128.254
    dns update command = nsupdate
    interfaces = eth0
    bind interfaces only = yes
    logon script = logon.vbs
    logon drive = Z
    logon path =
/opt/samba/var/locks/sysvol/campusix.cefetmg.br/scripts
    #winbind enum users = yes
    #winbind enum groups = yes
    template shell = /bin/bash
    #template homedir = /home/%U
    root preexec =
/opt/samba/var/locks/sysvol/campusix.cefetmg.br/scripts/logon %U %D

[netlogon]
    path =
/opt/samba/var/locks/sysvol/campusix.cefetmg.br/scripts
    read only = No

[sysvol]
    path = /opt/samba/var/locks/sysvol
    read only = No

[homes]
    path = /home/%D/%S
    browsable = no
    read only = no

[publico]

```



```

comment = Publico
path = /media/dados/samba/publico
read only = no
guest ok = yes
force create mode = 664
force directory mode = 755
veto files = /*.mp3/*.mpg/*.mpeg/*.avi/*.jpg/
hide files = /*.ini/*.log/

```

```

[admin]
    path =
/media/dados/samba/grupos/administrativo
    read only = no
    force create mode = 660
    force directory mode = 750
    veto files = /*.mp3/*.mpg/*.mpeg/*.avi/*.jpg/
    hide files = /*.ini/*.log/
    public = no
    browseable = no

```

```

[biblioteca]
    path = /media/dados/samba/grupos/biblioteca
    read only = No
    force create mode = 660
    force directory mode = 750
    veto files =
/*.mp3/*.mpg/*.mpeg/*.avi/*.jpg/
    hide files = /*.ini/*.log/
    browseable = No

```

```

[estagio]
    path = /media/dados/samba/grupos/estagio
    read only = No
    force create mode = 660
    force directory mode = 750
    veto files =
/*.mp3/*.mpg/*.mpeg/*.avi/*.jpg/
    hide files = /*.ini/*.log/
    browseable = No
    public = No

```

```

[eletronica]
    path = /media/dados/samba/grupos/eletronica
    read only = No
    force create mode = 660

```

```

        force directory mode = 750
        veto                files           =
/* .mp3/* .mpg/* .mpeg/* .avi/* .jpg/
        hide files = /* .ini/* .log/
        browseable = No
        public = No

```

```

[direcao]
        path = /media/dados/samba/grupos/direcao
        read only = No
        force create mode = 660
        force directory mode = 750
        veto                files           =
/* .mp3/* .mpg/* .mpeg/* .avi/* .jpg/
        hide files = /* .ini/* .log/
        browseable = No
        public = No

```

```

[enfermagem]
        path = /media/dados/samba/grupos/enfermagem
        read only = No
        force create mode = 660
        force directory mode = 750
        veto                files           =
/* .mp3/* .mpg/* .mpeg/* .avi/* .jpg/
        hide files = /* .ini/* .log/
        browseable = No
        public = No

```

```

[mecatronica]
        path                                     =
/media/dados/samba/grupos/mecatronica
        read only = No
        force create mode = 660
        force directory mode = 750
        veto                files           =
/* .mp3/* .mpg/* .mpeg/* .avi/* .jpg/
        hide files = /* .ini/* .log/
        browseable = No
        public = No

```

```

[ntic]
        path = /media/dados/samba/grupos/ntic

```

```
    read only = No
    force create mode = 660
    force directory mode = 750
    veto          files          =
/* .mp3/* .mpg/* .mpeg/* .avi/* .jpg/
    hide files = /* .ini/* .log/
        browseable = No
        public = No
```

```
[nae]
    path = /media/dados/samba/grupos/nae
    read only = No
    force create mode = 660
    force directory mode = 750
    veto          files          =
/* .mp3/* .mpg/* .mpeg/* .avi/* .jpg/
    hide files = /* .ini/* .log/
        browseable = No
        public = No
```

```
[sae]
    path = /media/dados/samba/grupos/sae
    read only = No
    force create mode = 660
    force directory mode = 750
    veto          files          =
/* .mp3/* .mpg/* .mpeg/* .avi/* .jpg/
    hide files = /* .ini/* .log/
        browseable = No
        public = No
```

```
[sre]
    path = /media/dados/samba/grupos/sre
    read only = No
    force create mode = 660
    force directory mode = 750
    veto          files          =
/* .mp3/* .mpg/* .mpeg/* .avi/* .jpg/
    hide files = /* .ini/* .log/
        browseable = No
        public = No
```

```
[redes]
    path = /media/dados/samba/grupos/redes
    read only = No
    force create mode = 660
    force directory mode = 750
```

```

    veto                files                =
/* .mp3/* .mpg/* .mpeg/* .avi/* .jpg/
    hide files = /* .ini/* .log/
    browseable = No
    public = No

[formgeral]
    path = /media/dados/samba/grupos/formgeral
    read only = No
    force create mode = 660
    force directory mode = 750
    veto                files                =
/* .mp3/* .mpg/* .mpeg/* .avi/* .jpg/
    hide files = /* .ini/* .log/
    browseable = No
    public = No

[engeletrica]
    path                =
/media/dados/samba/grupos/engeletrica
    read only = No
    force create mode = 660
    force directory mode = 750
    veto                files                =
/* .mp3/* .mpg/* .mpeg/* .avi/* .jpg/
    hide files = /* .ini/* .log/
    browseable = No
    public = No
```