FACULDADE POLITEC

CURSO SUPERIOR DE TECNOLOGIA EM REDES DE COMPUTADORES

MARCEL HENRIQUE GOMES DOS SANTOS

RODRIGO LOURENÇO DE ARAÚJO

INFRAESTRUTURA COM SAMBA 4

Santa Bárbara d'Oeste

2013

MARCEL HENRIQUE GOMES DOS SANTOS
(unix.marcel@gmail.com)

RODRIGO LOURENÇO DE ARAÚJO
(rodrigo@dgnonline.net)

INFRAESTRUTURA COM SAMBA 4

Trabalho apresentado à Faculdade Politec, como exigência para a obtenção do grau de Tecnólogo em Redes de Computadores, sob a orientação do Prof. Esp. Mario Luiz Bernardinelli.

Santa Bárbara d'Oeste

2013

Aprovação

MARCEL HENRIQUE GOMES DOS SANTOS

RODRIGO LOURENÇO DE ARAÚJO

INFRAESTRUTURA COM SAMBA 4

Trabalho aprovado em: ____/____/____

Nota: ____ (_____)

_____ _____

Nome do primeiro examinador Nome do segundo examinador

_____

Prof. Esp. Mario Luiz Bernardinelli

Santa Bárbara d'Oeste

2013

Dedicatória

Dedico este trabalho a minha mãe e amigos. (Marcel Henrique Gomes dos Santos)

Dedico este trabalho aos meus pais, irmã, minha noiva, Deus e amigos. (Rodrigo Lourenço de Araújo)

Agradecimentos

Marcel Henrique Gomes dos Santos

Agradeço a minha mãe Rosemary Netto por sempre me apoiar e me ajudar em todos os momentos difíceis incentivando e dando força para que tudo isso fosse possível.

Agradeço aos meus amigos que são essenciais em todas as minhas vitorias.

Agradeço também ao orientador Mario Luiz Bernardinelli pelo apoio e preocupação com que foi concedido a nos nesse trabalho.

Rodrigo Lourenço de Araújo

A Deus, por sempre iluminar a minha trajetória para a realização de mais um sonho.

Aos meus pais Francisco e Maria, e minha irmã Thalita pelo apoio, dedicação e incentivo.

A minha noiva Gabriela, pelos conselhos e sua paciência.

Agradeço ao orientador e amigo Mario Luiz Bernardinelli, pela sua paciência, apoio, e por sempre ter compartilhado seu conhecimento.

E aos amigos, que de alguma forma contribuíram para a realização desse trabalho.

Software é como sexo: é melhor quando é de graça.
(Linus Torvalds)

Resumo

O *Active Directory* é um serviço de diretório desenvolvido pela *Microsoft*, que permite um gerenciamento de forma centralizada dos recursos e serviços na rede. O Samba é um servidor de arquivos que permite compartilhar recursos entre sistemas Linux, *Windows* e outros. Surgiu a partir de uma necessidade, onde o seu criador Andrew Tridgell, desenvolveu uma aplicação, que necessitava de suporte ao protocolo NetBIOS. O Samba em sua primeira versão permitiu que o computador de Andrew, com sistema operacional DOS, pudesse encontrar em sua rede a máquina UNIX como um servidor de arquivos. Desta forma, ele não utilizaria mais o protocolo NFS. A utilização do *Active Directory* da *Microsoft*, só é possível mediante ao pagamento de licenças. O Samba 4 permite sua utilização como *Active Directory*, e por ser um *software* livre, não tem custo adicional de licenças, ou seja, gratuito. Objetivo deste trabalho é explorar os protocolos envolvidos na implantação do *Active Directory*, tal como LDAP, Kerberos, DNS, SMB/CIFS e a implementação do Samba 4, bem como apresentar um cenário prático de aplicação do Samba 4 operando como *Active Directory* numa rede contendo clientes *Microsoft Windows XP, Microsoft Windows 7* e Linux.

Palavras-chave: *Active Directory,* LDAP, Samba e SMB/CIFS.

Abstract

Active Directory is a directory service developed by Microsoft that allows a centralized management of network resources and services. Samba is a file server that allows you to share resources between Linux, Windows and others. It emerged from a needed of its creator, Andrew Tridgell, that developed an application that needed to support the NetBIOS protocol. The first version of Samba allowed Andrew´s computer, with DOS operating system, to find an UNIX machine as a file server. Thus, he would not use the NFS protocol any more. The use of Microsoft's Active Directory is only possible through the payment of licenses. The Samba 4 allows its use as Active Directory, and because it´s an open source software, there is no additional license costs, it´s free. This study aims to explore the protocols involved in the deployment of Active Directory as LDAP, Kerberos, DNS, SMB/CIFS and the implementation of Samba 4, and it presents a practical scenario for implementing Samba 4 operating as an Active Directory in a network containing customers Microsoft Windows XP, Microsoft Windows 7 and Linux.

Keywords : *Active Directory, LDAP , Samba and SMB/CIFS .*

Lista de abreviaturas e siglas

AD	*Active Directory*
ARPANet	*Advanced Research Projects Agency Network*
AS	*Authentication Service (Kerberos)*
ccTLDs	*Country Code TLDs*
CIFS	*Common Internet File System*
DC	*Domain Controller*
DES	*Data Encryption Standard*
DNS	*Domain Name System*
DOS	*Disk Operating System*
FTP	*File Transfer Protocol*
GC	*Global Catalog*
GPO	*Group Policy*
HTTP	*Hypertext Transfer Protocol*
IP	*Internet Protocol*
ISP	*Internet Service Provider*
KDC	*Key Distribution Center*
KDC	*Kerberos Distribution Center*
LAN	*Local Area Network*
LDAP	*Lightweight Directory Access Protocol*
MIT	*Massachusetts Institute of Technology*
NTP	*Network Time Protocol*
OU	*Organizational Units*
PDC	*Primary Domain Controller*

SMB	*Server Message Block*
SNTP	*Simple Network Time Protocol*
SRV	*Service*
ST	*Session Ticket*
TCP	*Transmission Control Protocol*
TGS	*Ticket Granting Service*
TGT	*Ticket Granting Ticket*
TLD	*Top Level Domains*
UDP	*User Datagram Protocol*

Lista de Figuras

Lista de tabelas

Sumário

1 INTRODUÇÃO

O Samba 4 é um servidor para *Linux* que permite o gerenciamento e compartilhamento de recursos em redes heterogêneas. Como controlador de domínio, o Samba 4 é responsável por fazer a autenticação dos clientes *Microsoft Windows* e *Linux*, armazenando os perfis de usuários e permitindo acesso a seus arquivos na rede a partir de qualquer computador registrado no domínio.

Após dez anos de desenvolvimento, o LDAP foi implantado no Samba 4 permitindo a sua utilização no papel de *Active Directory (AD)* .

O *Active Directory* é uma base de dados de uso geral, utilizado principalmente para gerenciar atributos de recursos e serviços de forma centralizada. A base de dados do *Active Directory* é organizada de maneira hierárquica, assim como ocorre no LDAP. Presente a partir do *Microsoft Windows 2000 Server*, o *Active Directory* foi desenvolvido pela *Microsoft* com base no LDAP e é um produto com custo adicional de licenças, ou seja, o seu uso é permitido mediante a pagamento.

A implementação do protocolo LDAP diretamente no Samba 4 permite o seu uso como *Active Directory* reduzindo os custos relacionados às licenças, já que o Samba 4 é um *software* gratuito.

O objetivo desse trabalho é explorar o uso do Samba 4 como *Active Directory*, iniciando pelos conhecimentos básicos dos serviços e protocolos que formam a base do *Active Directory:* LDAP, DNS, Kerberos, SMB/CIFS, NTP e RCP, culminando com uma implementação prática do Samba 4, utilizando como servidor primário a distribuição *Linux openSUSE*, como servidor de replicação da base de dados a distribuição *CentOS* e estações de trabalho *Microsoft Windows 7, Microsoft Windows XP* e openSUSE.

2 ACTIVE DIRECTORY

O *Active Directory* é um serviço de diretório que armazena em seu banco de dados as informações sobre objetos da rede. Como em qualquer outro banco de dados o *Active Directory* tem índice, que aqui chamamos de *Global Catalog*, responsável em armazenar um subconjunto de informações de um objeto. Toda informação contida no *Global Catalog* é replicada para outros controladores de domínios.

Na prática o *Active Directory* serve a dois propósitos:

- Manter em seu banco de dados informações dos objetos da rede.
- Auto-replicação de dados.

2.1 Serviço de Diretório

> "Serviço de diretório é um conjunto de atributos sobre recursos e serviços existentes na rede, isso significa que é uma maneira de organizar e simplificar o acesso aos recursos de sua rede centralizando-os[...]" (LOSANO, 2003).

Os recursos disponíveis no serviço de diretório são denominados objetos no *Active Directory*, tais como contas de usuários, computadores, impressoras e pastas compartilhadas. Todos esses objetos são organizados em estruturas hierárquicas e são armazenados em seu banco de dados. Cada objeto armazenado no *Active Directory* possui um conjunto de características (ou parâmetros) que são chamados de atributos do objeto.

O objetivo principal do serviço de diretório é organizar e centralizar todas estas informações para agilizar as consultas e facilitar a atualização e gerenciamento.

2.2 Como o *Active Directory* é organizado?

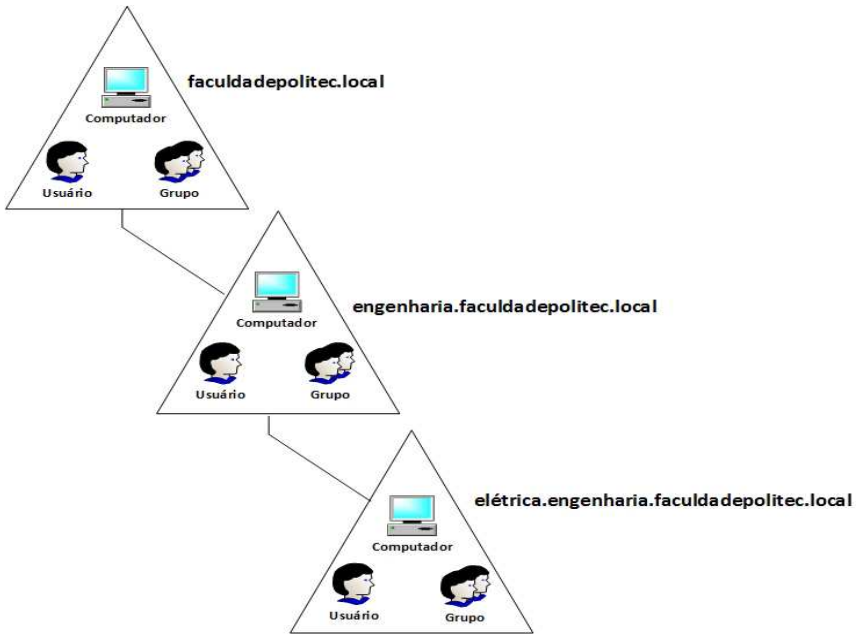
De acordo com (SEGUIS, 2008) quando se trata da organização do *Active Directory*, nos referimos a sua estrutura física e lógica. Fisicamente o *Active Directory* é armazenado em cada controlador de domínio como um conjunto de arquivos binários representando sua base de dados. Logicamente refere-se aos objetos internos do *Active Directory*, estruturados hierarquicamente sob a forma de uma árvore.

No *Active Directory,* um conjunto de objetos relacionados é chamado domínio. O *Active Directory* armazena estes objetos numa estrutura hierárquica em árvore.

O *Active Directory* possui recursos para armazenar e gerenciar mais de um domínio. Estes domínios podem estar num mesmo nível hierárquico ou podem estar hierarquicamente em níveis inferiores a outros domínios. Quando um domínio está no nível hierárquico inferior ao de outro domínio, chamamos este domínio de subdomínio.

Um domínio pode ter múltiplos subdomínios conforme ilustrado na Figura 1.

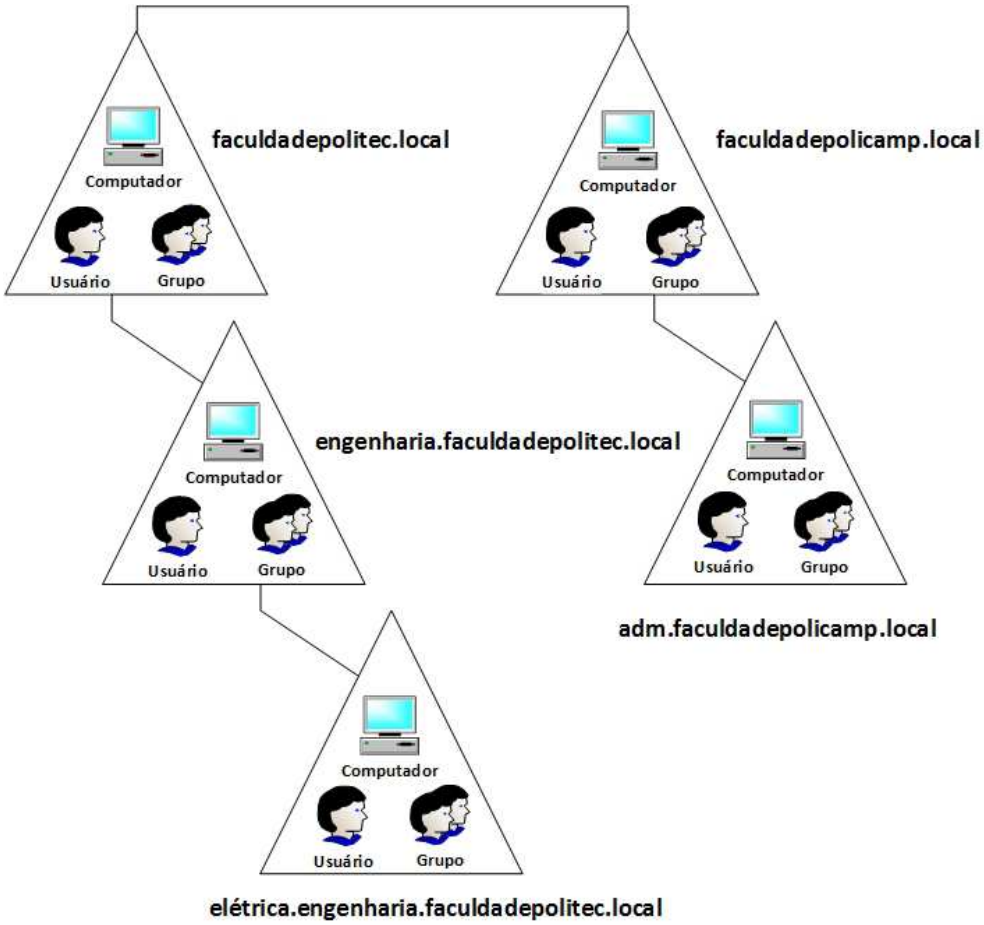
Figura 1: Representação de uma árvore *Active Directory.*



Fonte: Autoria própria, 2013.

A Figura 2 ilustra o conceito de floresta: faculdadepolitec.local e faculdadepolicamp.local. A vantagem do conceito de floresta é que os domínios podem compartilhar seus recursos desde que seja estabelecida uma relação de confiança entre eles.

Figura 2: Representação de uma floresta *Active Directory*.

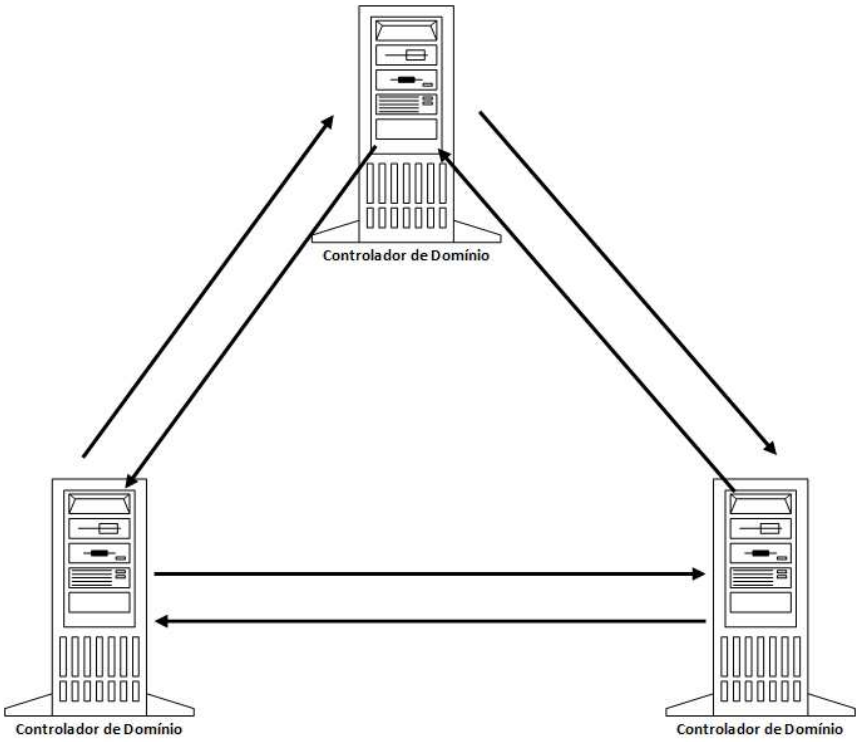


Fonte: Autoria própria, 2013.

2.2.1 Controlador de domínio

Um Controlador de Domínio, ou *Domain Controller* (DC), consiste fisicamente no servidor que é responsável por manter a base de dados do *Active Directory.* Uma solução muito comum para garantir a disponibilidade, consiste na utilização de mais de um DC, que mantém as bases de dados sincronizadas entre si, conforme ilustrado na Figura 3.

Figura 3: Representação de três Controladores de Domínios sincronizados.



Fonte: Autoria própria, 2013.

Quando criamos o primeiro domínio, estamos criando também o primeiro controlador de domínio, a primeira floresta e instalando o *Active Directory*. Quando utilizamos DC é importante pensar na quantidade de DC's necessários para manter a alta disponibilidade e a segurança física desses controladores.

> "Uma organização pequena que use uma única rede local (LAN) pode precisar somente de um domínio com dois controladores para obter alta disponibilidade e tolerância a falhas. Uma organização maior com vários locais de rede precisará de um ou mais controladores de domínio em cada site para garantir alta disponibilidade e tolerância a falhas". (MICROSOFT, 2003)

2.2.2 Unidade Organizacional

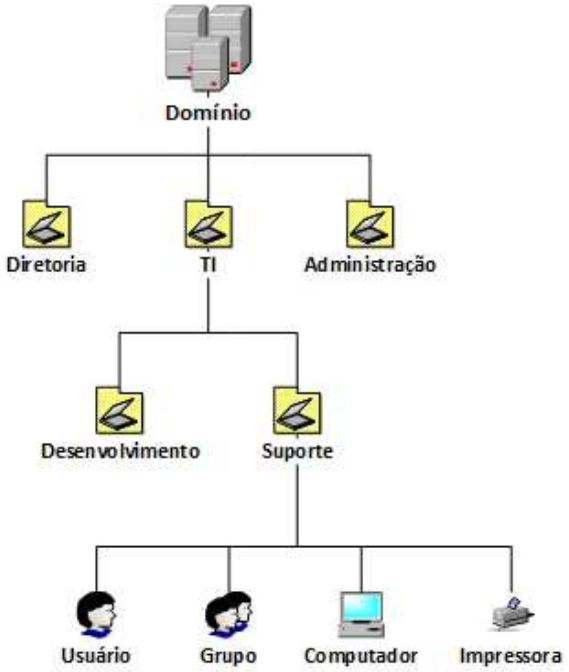
Segundo (SEGUIS,2008, p.97), uma Unidade Organizacional (*Organizational Unit* – OU), permite a divisão lógica de um diretório de forma a fazê-lo coincidir com a estrutura organizacional da empresa e com seu limites administrativos de uma forma mais direta.

Este recurso adiciona vários benefícios, sendo o principal deles a possibilidade de delegar autoridade.

A delegação de autoridade permite, por exemplo, que sejam concedidos privilégios administrativos a um determinado objeto, do *Active Directory*, de forma que ele possa gerenciar uma OU sem que ele precise ter privilégios administrativos sobre todo o domínio.

Conceito de OU é ilustrado na Figura 4.

Figura 4: Representação de Unidades Organizacionais



Fonte: Autoria própria, 2013.

2.2.3 GPO

Imagine uma residência onde tenha apenas um computador, e você decide modificar o papel de parede desse computador. Existem diversas maneiras para fazê-lo. A maioria das pessoas provavelmente abriria o Painel de Controle e em Personalização alteraria o Papel de Parede. Isso funcionaria bem para um usuário, agora vamos imaginar que você queira fazer essa alteração para toda a família isso pode ser tornar tedioso, teria que fazer essa mudança várias vezes, para cada usuário.

De acordo com (MICROSOFT, 2008, p.6-5), um *GPO (Group Policy* Object ou Objeto de Política de Grupo) é um *framework* dentro do *Windows* com componentes que residem no *Active Directory*, em controladores.

Um GPO é um conjunto de regras pré-configuradas, com a finalidade de facilitar o gerenciamento de forma centralizada, configurações de segurança, gerenciar configurações de *desktops* e aplicativos, implantar *softwares,* gerenciar redirecionamento de pastas e configurações de rede. Quando é utilizado essas regras, pode-se restringir ações dentro do domínio.

De acordo com (BRANDÃO,2013), outro conceito importante é saber que a hierarquia dos GPOs podem ser aplicadas em 3 níveis diferentes: *sites*, domínios e OUs.

- ***Sites:*** O mais alto nível. Todas as configurações feitas no *site* serão aplicadas a todos os domínios que fazem parte dele.

- **Domínios:** É o segundo nível. Configurações feitas aqui afetarão todos os usuários e grupos dentro do domínio.

- **OUs:** O que se aplica nas OUs afetarão todos os usuários dentro dela.

Existem dois tipos de GPOs que podem ser criados como:

- **Configuração do usuário:** Essa categoria afeta diretamente o usuário final.

- **Configuração do computador:** Essa categoria permite que o administrador customize as configurações do *Windows*.

A administração dos GPOs não é uma tarefa difícil, pois elas normalmente têm três opções a serem configuradas como:

- **Ativar:** Permite a ativação.

- **Desativar:** Permite a desativação.

- **Não Configurado:** Mantém a configuração padrão.

De acordo com (MICROSOFT, 2008, p.6-8), um GPO é utilizado para padronizar ambientes *desktops*, e todos os computadores em uma unidade organizacional ou toda uma organização. Em sua configuração avançada você pode fornecer um ambiente mais seguro.

2.3 Protocolos envolvidos no Active Directory

2.3.1 DNS

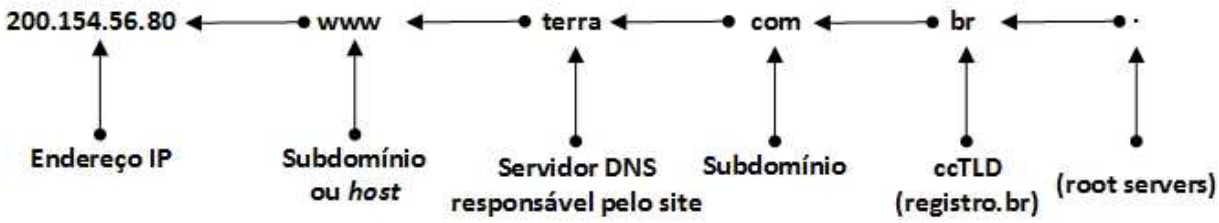
O *Domain Name System* (DNS) é um banco de dados distribuído, isso significa que o meu DNS armazena dados sobre os meus computadores. Essa tecnologia permite que se digite os nomes de domínios em seu navegador *web* ou na sua rede local e eles seriam automaticamente traduzidos para o endereço IP (*Internet Protocol*), do recurso a ser acessado.

Um elemento chave do DNS é uma coleção mundial de servidores DNS chamados *Root Servers*. Esses servidores estão espalhados pelo mundo e têm a função de responder a todas as requisições de resolução de domínio.

De acordo com (MORIMOTO, 2008) um nome de domínio é lido da direita para a esquerda como ilustrado na Figura 5. Os domínios primários são chamados de *Top Level Domains* (TLD) como .com, .net, .info, .cc, .biz etc e, em seguida, os domínios secundários

são chamados *Country Code TLDs* (ccTLDs) que recebem o prefixo de cada país, como .com.br ou .net.br. Nesse caso, o "com" é um subdomínio do domínio "br". Há, porém uma exceção, que é o Estados Unidos, que não usa o ccTLD .us.

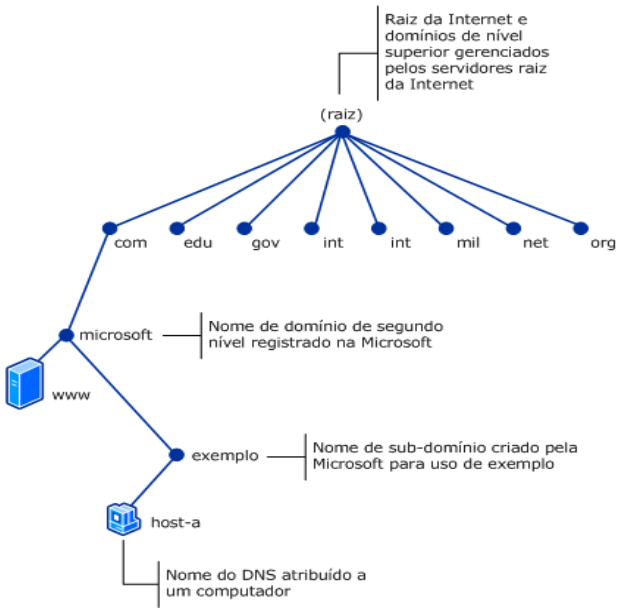
Figura 5: Como é feita uma consulta DNS.



Fonte: Autoria própria, 2013.

De acordo com (MICROSOFT, 2003) o DNS baseia-se no conceito de uma árvore em estrutura hierárquica, onde cada nível pode ser representado por uma ramificação ou uma folha das árvores conforme ilustrado na Figura 6. A ramificação é onde mais de um nome é utilizado para identificar uma coleção de recursos nomeados e a folha representa apenas um nome exclusivo.

Figura 6: Hierarquia DNS



Fonte: http://technet.microsoft.com/pt-br/library/cc737203(v=ws.10).aspx

A Tabela 1 apresenta o nome dos servidores de mais alto nível, os *root-servers*, bem como o endereço IP e a organização responsável pelo seu gerenciamento.

Tabela 1: *Root Servers*

Nome do host	Endereço Ip v4/v6	Gerenciado
a.root-servers.net	198.41.0.4, 2001:503:ba3e::2:30	VeriSign, Inc.
b.root-servers.net	192.228.79.201	University of Southern California (ISI)
c.root-servers.net	192.33.4.12	Cogent Communications
d.root-servers.net	199.7.91.13, 2001:500:2d::d	University of Maryland
e.root-servers.net	192.203.230.10	NASA (Ames Research Center)
f.root-servers.net	192.5.5.241, 2001:500:2f::f	Internet Systems Consortium, Inc.
g.root-servers.net	192.112.36.4	US Department of Defence (NIC)
h.root-servers.net	128.63.2.53, 2001:500:1::803f:235	US Army (Research Lab)
i.root-servers.net	192.36.148.17, 2001:7fe::53	Netnod
j.root-servers.net	192.58.128.30, 2001:503:c27::2:30	VeriSign, Inc.
k.root-servers.net	193.0.14.129, 2001:7fd::1	RIPE NCC
l.root-servers.net	199.7.83.42, 2001:500:3::42	ICANN
m.root-servers.net	202.12.27.33, 2001:dc3::35	WIDE Project

Fonte: http://www.iana.org/domains/root/servers

Para o correto funcionamento do DNS junto ao *Active Directory*, será utilizado o DNS interno do Samba 4, o mesmo deve oferecer suporte ao registro SRV e também ao protocolo de atualização dinâmica conforme as RFCs 2052 e 2136.

Em uma rede local (LAN) o servidor DNS terá a única e exclusiva função de interpretar todas as pesquisas de nomes de redes, controladas pelo *Active Directory* e se necessário direcionar todas as pesquisas externas para servidores externos.

2.3.2 LDAP

O protocolo LDAP (*Lightweight Directory Access Protocol)* em sua terceira versão definida pela RFC2251, é um protocolo que permite o acesso a informações centralizadas em uma rede.

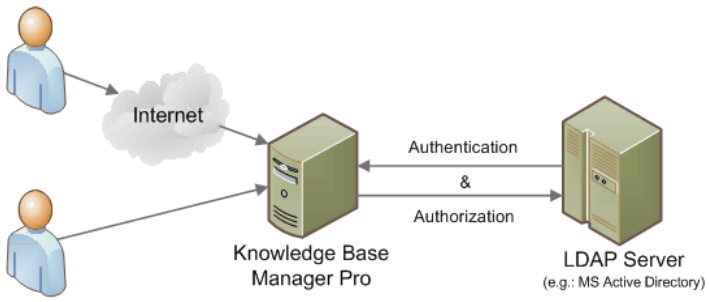
LDAP é um padrão cliente/servidor baseado em TCP/IP e tem sido utilizado por cerca de 15 anos. O padrão LDAP fornece métodos para acessar, pesquisar e modificar informações em seu diretório.

Atuando como um banco de dados, ele centraliza todas as informações de credenciais e acessos em uma única origem, facilitando a administração e manutenção dos registros.

O *Active Directory* nada mais é que a implementação do protocolo LDAP desenvolvida pela *Microsoft* que permite a autenticação e gerenciamento de usuários em ambiente *Microsoft Windows*.

Um exemplo de funcionamento do protocolo LDAP é ilustrado na Figura 7, que mostra um usuário via internet e local solicitando um acesso a um determinado servidor. Os dados do usuário são consultados na base de dados LDAP e o acesso pode ou não ser concedido.

Figura 7: Funcionamento LDAP



Fonte: http://www.web-site-scripts.com/images/blog/ldap-scheme.png

2.3.3 Kerberos

O Kerberos é um protocolo criado pelo MIT (*Massachusetts Institute of Technology*), capaz de oferecer segurança na autenticação em aplicações cliente/servidor utilizando criptografia.

De acordo com (MIT, 2013), a internet não é um lugar seguro, existem diversas ferramentas utilizadas por *hackers* mal-intencionados para rastrear senhas. O Kerberos foi criado como uma solução para esse tipo de problema de segurança, utilizando mecanismo

de criptografia forte, possibilitando que um cliente prove sua identidade através de uma rede insegura utilizando *Tickets*.

Um servidor de autenticação Kerberos, também conhecido como KDC (*Key Distribution Center*) compartilha sua chave com o cliente. Existem dois componentes no KDC:

- Serviço de Autenticação (AS) responsável pelo serviço inicial de *logon*.

- Serviço de Garantia de *Ticket* (TGS) que fornece os *tickets* para acessos dos recursos na rede após o usuário ter feito o *login*.

De acordo com (BANIN, 2010), conforme ilustrado na Figura 8:

1. Um usuário requisita a autenticação com o KDC no processo de *login*.

2. O componente AS do KDC recebe a requisição de autenticação e a valida para que possa ser decodificada com o *hash* da senha do usuário, acessada a partir do banco de dados do AD.

3. O cliente coloca o TGT em *cache* até que ele precise acessar um recurso de rede.

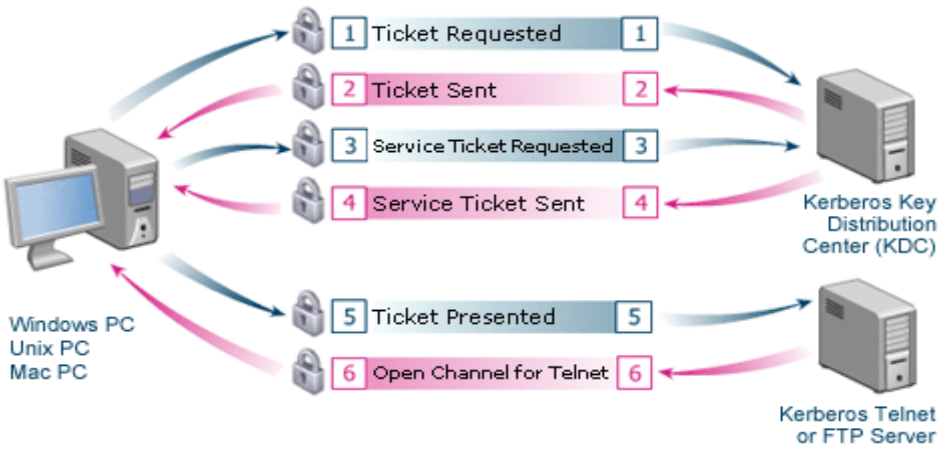
4. O KDC retorna um *Ticket* de Sessão (ST – *Session Ticket*) que contém um código em uma chave cifrada conhecida apenas por ele mesmo e pelo servidor de recurso.

5. O cliente apresenta o ST ao servidor do recurso.

6. O servidor do recurso examina o ST em busca do código da chave, conhecido apenas por ele e pelo KDC.

7. Se o código da chave for igual ao código da chave existente no servidor de recursos, o cliente receberá acesso ao servidor de recursos.

Figura 8: Autenticação Kerberos



Fonte: http://blogs.technet.com/b/gbanin/archive/2010/11/03/conhe-231-a-o-kerberos-o-c-227-o-de-guarda.aspx

No Kerberos as informações contidas em seus *tickets* são:

- Nome do cliente.
- Nome do servidor.
- Endereço IP do cliente.
- *Timestamp* (Data e hora do *ticket*).
- Tempo de vida.
- Chave de sessão cifrada gerada de forma pseudo-aleatória.

O *ticket* gerado pode ser utilizado diversas vezes até seu tempo de vida se esgotar. Quando o *ticket* vencer, deve ser realizada novamente uma solicitação de chave para o determinado serviço, e os autenticadores são ativados todas as vezes que um acesso ao servidor é realizado.

2.3.4 NTP

De acordo com (NTP, 2013) o NTP (*Network Time Protocol*) permite a sincronização dos relógios dos dispositivos em uma rede como servidores, estações de trabalho, e roteadores entre outros.

Para o correto funcionamento do servidor Samba 4, todas as estações de trabalho devem estar com seus relógios sincronizados.

As mensagens do NTP são baseadas no protocolo UDP. Na troca de mensagem entre cliente e servidor é possível descobrir qual é o intervalo tempo entre o cliente e servidor NTP através de seus algoritmos, e corrigir seu relógio numa forma precisa.

O SNTP (*Simple Network Time Protocol*) é uma versão simplificada e modificada pela *Microsoft*, e seu tempo de resposta é menor se comparado ao NTP, e é utilizado para sincronizar os relógios do *Microsoft Windows*.

2.3.5 SMB/CIFS

De acordo com (MORIMOTO,2008), a necessidade de se compartilhar arquivos entre computadores motivou o aparecimento das primeiras redes de computadores. O protocolo SMB (*Server Message Block*) surgiu junto com o *Windows* 3.11, e é um protocolo utilizado para realizar o compartilhamento entre estações de trabalho *Windows* numa rede local.

O protocolo SMB/CIFS (*Server Message Block/Common Internet File System*) é utilizado para compartilhar pastas, arquivos e impressoras em redes *Microsoft*. O CIFS é a nova versão do protocolo SMB, disponível a partir do *Windows* 2000.

2.4 Serviços de Rede

De acordo com (MORIMOTO,2006), as primeiras redes de computadores surgiram na década de 60, como uma forma de transmitir informações entre computadores. Nessa época o meio mais comum para transporte de dados eram os cartões perfurados.

Entre 1969 e 1973 foi criada a ARPANet *(Advanced Research Projects Agency Network*) precursor da Internet, uma rede responsável por interligar várias redes de universidade e órgãos militares.

A comunicação de dados não é possível sem uma linguagem padrão. Então em 1974 surgiu o protocolo TCP/IP que acabou se tornando o protocolo definitivo da ARPANet e em seguida da Internet.

A partir do momento em que um protocolo de comunicação (TCP/IP) foi definido, começaram a surgir os primeiros serviços de rede. Um serviço de rede é um *software* que fornece um serviço ou aplicação distribuída para os demais computadores na rede.

Numa infraestrutura de rede *Windows*, podemos ter os seguintes serviços:

- ***Active Directory:*** Responsável por armazenar e gerenciar recursos do domínio.
- **LDAP:** Protocolo utilizado para implementar o *Active Directory*.
- **DNS:** Responsável pela resolução de IP em nomes de máquinas.
- **Kerberos:** Permite uma autenticação segura utilizando criptografia.
- **SMB/CIFS:** Responsável pelo compartilhamento de arquivos.
- **NTP:** Responsável pela sincronização dos relógios entre os computadores.

2.5 Samba

O Samba é a implementação das funções de compartilhamento para sistemas Unix, Linux, BSD, Solaris, OS X, *Microsoft Windows* entre outros, que permite a manipulação de arquivos compartilhados na rede.

2.5.1 História

De acordo com (MAZIOLI,2010, p.300) o desenvolvedor do Samba Andrew Tridgell precisava montar um volume Unix em sua máquina DOS. Inicialmente ele utilizava o NFS (*Network File System*), mas seu aplicativo precisava de suporte NetBIOS. Andrew Tridgell desenvolveu então um *sniffer* para analisar e auxiliá-lo a interpretar o funcionamento do NetBIOS na rede.

Por volta de 1992 Andrew Tridgell escreveu seu primeiro código que fez com que seu servidor Unix aparecesse como um servidor de arquivos *Windows* para sua máquina DOS, satisfeito com o seu trabalho resolveu deixar de lado seu projeto.

Em 1994 quando a *Microsoft* disponibilizou a documentação do SMB e NetBIOS, Andrew resolveu voltar a seu projeto implementando novas funções no Samba e torná-lo público. Seu código vem sendo melhorado constantemente por *hackers*, melhorando sua transmissão e recepção de dados, segurança, melhorias em seu desempenho de rede, garantindo um controle mais rigoroso que a própria implementação no *Windows* NT utilizado na época, incluindo serviço de diretório e o mapeamento de IDs (*Identity*) de usuários *Windows* com Linux.

2.5.2 Principais características

De acordo com (MAZIOLI,2010,p.301) as principais funcionalidades do Samba são:

- Compartilhamento de arquivos entre máquinas *Windows* e Linux.
- Compartilhamento de impressora.

- Controle de acesso aos recursos compartilhados no servidor através de diversos métodos.

- Possibilidade de definir contas de ”Convidados“, que podem se conectar sem fornecer senha.

- Permite ocultar o conteúdo de determinados diretórios de forma que não sejam visíveis facilmente pelo usuário.

- Possibilita ajuste fino nas configurações de transmissão e recepção dos pacotes TCP/IP.

- Permite auditoria tanto dos acessos à pesquisa de nomes na rede, como dos acessos a compartilhamentos. Entre os detalhes salvos estão a data de acesso, IP de origem, etc.

2.5.3 Samba como servidor de arquivos

De acordo com (MORIMOTO,2006) o Samba é a solução mais completa quando se trata de servidor de arquivos, pois inclui várias opções de segurança e permite que os compartilhamentos sejam acessados a partir de clientes *Windows*, Linux e outros.

2.5.4 Samba como controlador de domínio

Manter as senhas dos usuários sincronizadas entre as estações de trabalho e servidor Samba, acaba consumindo uma boa parte do tempo do administrador da rede. Uma solução seria implantar o Samba como um Controlador de Domínio Primário (PDC), onde passa a assumir o papel de servidor de autenticação, permitindo assim utilizar suas credenciais em qualquer computador que faça parte do mesmo domínio.

Quando um novo usuário é cadastrado no servidor, automaticamente ele pode fazer *logon* em qualquer estação de trabalho. Isso possibilita o gerenciamento de todo o parque tecnológico, pois torna possível criar, remover ou bloquear contas de usuários de forma centralizada, isto é, de um único ponto.

2.6 Samba 4

Segundo (SAMBA, 2013), o Samba 4 além de fornecer todas a opções das versões anteriores, agora pode funcionar como um *Active Directory* (AD), onde qualquer versão atual do *Microsoft Windows* pode ingressar no domínio Samba. Nesse trabalho é referenciado o *Active Directory* inicialmente desenvolvido pela *Microsoft* como *Microsoft Active Directory* e o serviço desenvolvido para Linux como Samba 4 *Active Directory*.

Após dez anos de trabalho, a equipe responsável pelo desenvolvimento do Samba 4 criou a primeira implementação do *software* livre compatível com os protocolos do *Active Directory* da *Microsoft*.

O Samba 4 possui todos os serviços necessários para a implementação como o *Microsoft Active Directory*. O Samba 4 permite ingressar todas as versões de clientes *Microsoft Windows* atualmente suportados pelo *Microsoft Active Directory*, incluindo a sua mais nova versão *Microsoft Windows 8*. O Samba 4 permite a interoperabilidade entre um Microsoft *Active Directory* e o Samba 4 *Active Directory*.

2.6.1 Serviço de diretório do Samba 4

O Samba 4 sem a implementação do seu serviço de diretório, não seria diferente de suas versões anteriores. Portanto sua versão atual permite o gerenciamento de todos os recursos disponíveis na rede, chamados de objetos, como:

- Contas de usuários.
- Grupos de usuários.
- Grupos de computadores.
- Computadores.
- Políticas de segurança.
- Impressoras.

- Outros domínios.
- Entre outros.

Até o momento ainda não existem ferramentas desenvolvidas em Linux para o gerenciamento do Samba 4 *Active Directory*, mas existem ferramentas para gerencia-lo através de *softwares* desenvolvidos pela própria *Microsoft*.

2.6.2 Samba 4 – Integração com serviços

Após a implementação do *Active Directory* sobre o LDAP, é possível integrar diversos serviços de rede e também aplicações que suportam o mesmo. Alguns serviços para Linux como, servidores *proxy*, *e-mail*, Samba 4 e *web* podem ser configurados para utilizarem a base LDAP do *Active Directory*.

O objetivo de se utilizar esses serviços configurados para interagir com a base LDAP do *Active Directory*, é prover uma administração centralizada utilizando o mesmo usuário e senha cadastrada no *Active Directory*.

2.6.3 Recursos disponíveis no Samba 4

De acordo com (SAMBA, 2013) a equipe de desenvolvedores do Samba criou a primeira implementação do *software* livre compatível com o *Active Directory* da *Microsoft*. O Samba em sua nova versão inclui todos os recursos e procedimentos necessários para trabalhar como *Active Directory*.

O Samba 4 fornece suporte a:

- Ferramenta de administração do *Windows*.
- Pode ser associado a um *Active Directory Microsoft*.
- *Active Directory Microsoft* pode ser associar ao Samba 4.
- Clientes *Microsoft Windows*, até mesmo o recém-lançado *Windows* 8.

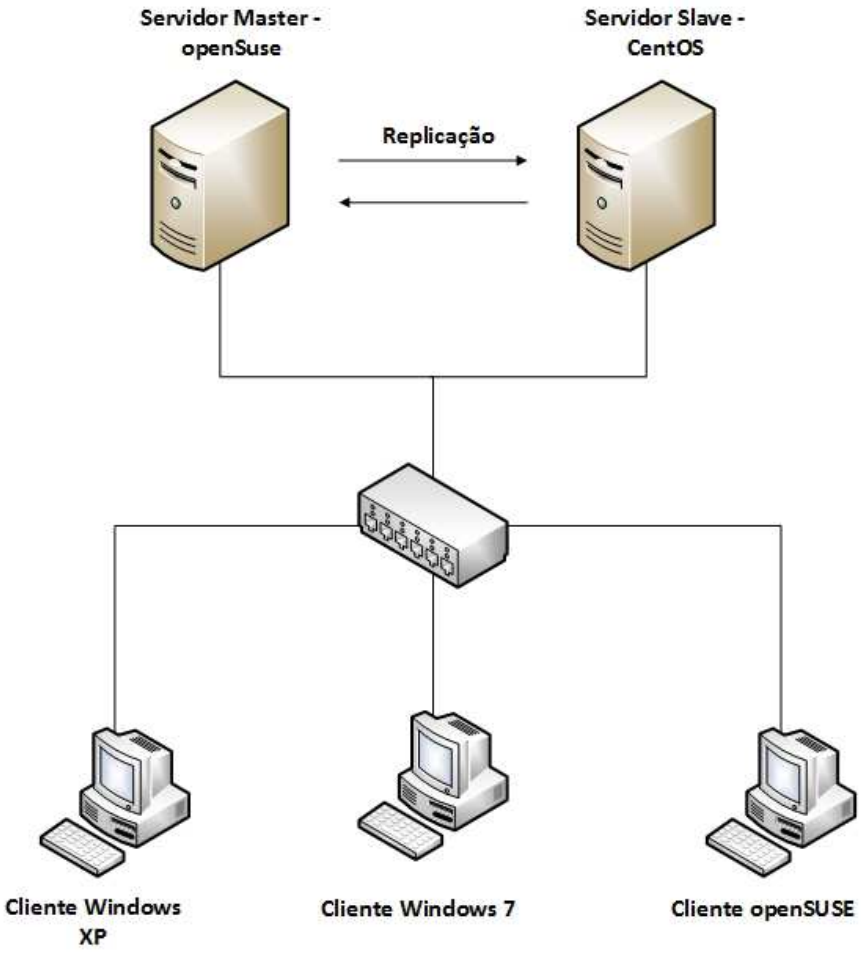
- Clientes Linux.
- Integração com diversos serviços como, *proxy*, *e-mail*, *web* etc.

3 ESTUDO DE CASO

Neste estudo de caso é abordado a implantação do Samba 4 *Active Directory*, utilizando o Sistema Operacional Linux.

Conforme ilustra a Figura 9 é configurada a replicação do *Active Directory* entre o servidor *master* e *slave*. Serão ingressados ao domínio, os clientes *Microsoft Windows* XP/7 e openSUSE Linux.

Figura 9: Cenário proposto.



Fonte: Autoria própria, 2013.

Este estudo de caso tem como objetivo, demonstrar a eficiência do Samba 4 *Active Directory* tal como o *Microsoft Active Directory:*

- Gerenciando grupos e usuários.

- Criando e aplicando GPOs.
- Ingressando clientes *Windows* e Linux ao domínio.
- Demonstrando a replicação dos objetos entre os *Active Directory.*
- Comando para administração.

3.1 Implantação

A implantação é o passo onde todo o processo deve ser planejado cuidadosamente. É apresentado o processo da instalação de um servidor openSUSE Samba 4 *Active Directory* como *master* e um servidor *CentOS* Samba 4 *Active Directory* como s*lave*. Neste processo toda a base de dados do servidor *master* será replicada para o servidor *slave*.

A Tabela 2 apresenta as configurações básicas de cada elemento do cenário proposto na Figura 9.

Tabela 2: Configurações Servidores/Máquinas

Distribuição	Arquitetura	Hostname	Domínio	Endereço IP/Mascara
openSUSE 12.3	32 bits	master	enterprise.local	192.168.0.10/24
CentOS 6.4	32bits	slave	enterprise.local	192.168.0.20/24
Windows XP	32bits	cliente	enterprise.local	192.168.0.35/24
Windows 7	32bits	cliente1	enterprise.local	192.168.0.30/24
openSUSE	32bits	openSUSE-01	enterprise.local	192.168.0.31/24

Fonte: Autoria própria, 2013.

3.1.1 Preparando e instalando *Active Directory master*

1. Configure a interface de rede com endereço IP fixo, conforme ilustrado a seguir:

```
master:~ # vim /etc/sysconfig/network/ifcfg-eth0
BOOTPROTO='static'
BROADCAST=''
ETHTOOL_OPTIONS=''
IFPLUGD_PRIORITY='0'
IPADDR='192.168.0.10/24'
MTU=''
NAME='82540EM Gigabit Ethernet Controller'
NETMASK=''
NETWORK=''
REMOTE_IPADDR=''
STARTMODE='ifplugd'
USERCONTROL='no'
```

Onde:

- BOOTPROTO: *Static* indica que o endereço IP da interface é estático, isto é, fixo.

- IPADDR: Endereço IP da interface de rede.

2. Também deve ser configurado o arquivo *hosts* onde identificamos nome do nosso servidor e o seu domínio.

```
master:~ # vim /etc/hosts

127.0.0.1       localhost
127.0.0.1       master.enterprise.local master
192.168.1.10    master.enterprise.local master
```

3. No arquivo /etc/resolv.conf, configuramos o servidor DNS responsável pelas consultas do nosso servidor Linux. Após a instalação, a linha do arquivo '*nameserver* 8.8.8.8', poderá ser retirada, pois o serviço interno de DNS do Samba 4 já estará em funcionamento.

```
master:~ # vim /etc/resolv.conf

search enterprise.local
nameserver 192.168.0.10
nameserver 8.8.8.8
```

3.1.2 Instalando o Samba 4 master

1. Após toda a pré-configuração do servidor ter sido realizada, precisamos instalar os pacotes necessários para resolver as dependências da instalação do Samba 4.

```
master:~ # yast2 -i findutils readline glibc-devel findutils-locate gcc
flex lynx compat-readline4 db-devel wget gcc-c++ subversion make vim telnet
cron iptables iputils man man-pages nano pico sudo perl-TimeDate python
libacl-devel libblkid-devel gnutls-devel readline-devel python-devel gdb
pkgconfig  nss-pam-ldapd openldap2 cups-devel pam-devel  openldap2-client
krb5-client krb5-devel openldap2-devel  python-ldap
```

2. Em seguida baixe o pacote tar.gz do site samba e o descompacte-o.

```
master:~ # wget http://ftp.samba.org/pub/samba/stable/samba-4.1.0.tar.gz
master:~ # tar xvzf samba-4.1.0.tar.gz
```

3. Iniciando o processo de instalação do Samba 4: compile o Samba conforme o seguinte comando:

```
master:~ # cd samba-4.1.0/
master:~/samba-4.1.0 # ./configure --enable-debug --enable-selftest
…
Building with Active Directory support.
…
Checking configure summary
Checking compiler accepts -g
Checking compiler for PIE support
'configure' finished successfully (1m7.671s)
```

Os parâmentros *--enable-debug –enable-selftest* adicionam recursos para diagnostico de problemas e falhas na instalação.

4. No passo anterior foi gerado o arquivo Makefile. O comando *make* irá proceder a compilação do código do Samba 4 e o comando *make install* procederá a instalação do código recém compilado.

```
master:~/samba-4.1.0 # make
master:~/samba-4.1.0 # make install
```

5. Iniciando a instalação do *Active Directory*. O comando *samba-tool* deve ser utilizado para instalar o *Active Directory*, conforme apresentado a seguir:

```
master:~/samba-4.1.0 # /usr/local/samba/bin/samba-tool domain provision
Realm [SITE]: enterprise.local
 Domain [enterprise]:
 Server Role (dc, member, standalone) [dc]: dc
 DNS backend (SAMBA_INTERNAL, BIND9_FLATFILE, BIND9_DLZ, NONE)
[SAMBA_INTERNAL]:
 DNS forwarder IP address (write 'none' to disable forwarding) [127.0.0.1]:
8.8.8.8
Administrator password:
Retype password:
…
Server Role:           active directory domain controller
Hostname:              master
NetBIOS Domain:        ENTERPRISE
DNS Domain:            enterprise.local
DOMAIN SID:            S-1-5-21-321465293-1000093363-361710731
```

Serão solicitadas várias informações para a criação do *Active Directory*, a saber:

- *Realm*: Deve ser informado o nome do domínio enterprise.local.

- *Domain*: Confirme o nome do domínio.

- *Server Role* (*dc*, *member*, *standalone*) [dc]: Deve ser informado o tipo de domínio se é um *domain controler* ‘dc’, se será um membro de um controlador de domínio já existente ‘*member*’, ou *standalone* utilizado apenas para replicar os dados do *master*, mas não assume a função na rede como um controlador de domínio.

- *DNS backend* (SAMBA_INTERNAL, BIND9_FLATFILE, BIND9_DLZ, NONE) [SAMBA_INTERNAL]: Neste passo será configurado o *Active Directory* para utilizar o DNS interno do próprio Samba.

- *DNS forwarder IP address (write 'none' to disable forwarding) [127.0.0.1]:* Deve ser informado um DNS externo, para que as máquinas na rede possam fazer consultas de DNS externas através do *Active Directory*.

- *Administrator password*: Será definida a senha do usuário *Administrator* do *Active Directory*, a qual deve conter letras, números e caracteres especiais, em seguida a senha deve ser confirmada digitando-a novamente.

6. Criando os *links* para acesso direto ao *software* samba e smbclient. Este passo serve para adicionar os utilitários samba e smbclient no *PATH* do usuário *root*.

```
master:~ # ln -s /usr/local/samba/sbin/samba /sbin/samba
master:~ # ln -s /usr/local/samba/bin/smbclient /bin/smbclient
```

7. Criando o *script* para inicialização automática do Samba 4, para quando o servidor for reinicializado.

```
master:~ # vim /usr/lib/systemd/system/samba.service

[Unit]
Description=Samba AD Daemon
After=syslog.target network.target

[Service]
Type=forking
PIDFile=/usr/local/samba/var/run/samba.pid
LimitNOFILE=16384
EnvironmentFile=-/etc/sysconfig/samba
ExecStart=/usr/local/samba/sbin/samba $SAMBAOPTIONS
ExecReload=/usr/bin/kill -HUP $MAINPID

[Install]
WantedBy=multi-user.target
```

8. Em seguida crie o *link* e ative o *script* para sua inicialização automática. Isto fará com que o serviço Samba seja iniciado automaticamente quando o computador for ligado.

```
master:~ # ln -s /usr/lib/systemd/system/samba.service
/etc/systemd/system/samba.service

master:~ # systemctl enable samba
```

3.1.3 Testando o DNS

1. Em seguida deve ser realizado o teste do serviço DNS do *Active Directory*, através dos seguintes comandos:

```
master:~ # host -t SRV _ldap._tcp.enterprise.local
_ldap._tcp.enterprise.local has SRV record 0 100 389
master.enterprise.local.
```

```
master:~ # host -t SRV _kerberos._udp.enterprise.local
_kerberos._udp.enterprise.local has SRV record 0 100 88
master.enterprise.local.
```

```
master:~ # host -t A master.enterprise.local
master.enterprise.local has address 192.168.0.10
```

Observe que não há mensagens de erro nas respostas aos comandos.

3.1.4 Verificando as configurações do Kerberos

O arquivo de configuração do Kerberos foi gerado quando o *Active Directory* foi instalado. No cenário proposto, as configurações são as seguintes:

```
master:~ # vim /usr/local/samba/private/krb5.conf

[libdefaults]
        default_realm = ENTERPRISE.LOCAL
        dns_lookup_realm = false
        dns_lookup_kdc = true
```

3.1.5 Verificando as configurações do Samba

Todas as configurações do Samba 4 devem ser feitas no arquivo smb.conf, que é o mesmo arquivo utilizado nas versões anteriores do Samba. Esse arquivo é gerado na instalação do Samba 4 *Active Directory*. Como o Samba foi compilado com parâmetros padrões, o arquivo de configuração ficará localizado em /usr/local/samba/etc/smb.conf.

```
master:~ # vim /usr/local/samba/etc/smb.conf
# Global parameters
[global]
        workgroup = ENTERPRISE
        realm = ENTERPRISE.LOCAL
        netbios name = MASTER
        server role = active directory domain controller
        dns forwarder = 8.8.8.8
[netlogon]
        path =/usr/local/samba/var/locks/sysvol/enterprise.local/scripts
        read only = No

[sysvol]
        path = /usr/local/samba/var/locks/sysvol
        read only = No
```

Para que o *Active Directory* funcione, os compartilhamentos *netlogon* e *sysvol* devem estar criados, onde:

- *Netlogon*: É o compartilhamento, onde se localiza os scripts de mapeamento por exemplo.

- *Sysvol*: Esse compartilhamento contém informações sobre GPOs, *scripts* de *startup/shutdown* e *login/logoff*.

1. Testando os compartilhamentos. Para testar o funcionamento dos compartilhamentos, pode ser utilizado o comando *smbclient*, conforme o exemplo a seguir:

```
master:~ # /usr/local/samba/bin/smbclient -L localhost -U%
Domain=[ENTERPRISE] OS=[Unix] Server=[Samba 4.1.0]

        Sharename       Type      Comment
        ---------       ----      -------
        netlogon        Disk
        sysvol          Disk
        IPC$            IPC       IPC Service (Samba 4.1.0)
Domain=[ENTERPRISE] OS=[Unix] Server=[Samba 4.1.0]

        Server               Comment
        ---------            -------

        Workgroup            Master
        ---------            -------
```

2. Testando a autenticação no Samba 4. Para testar o mecanismo de autenticação do Samba 4, também deve ser utilizado o comando *smbclient*, conforme ilustrado a seguir:

```
master:~ # /usr/local/samba/bin/smbclient //localhost/netlogon -
Uadministrator%'Inicial2013@'
Domain=[ENTERPRISE] OS=[Unix] Server=[Samba 4.1.0]
smb: \> ls
  .                                   D        0  Tue Oct 29 10:29:10 2013
  ..                                  D        0  Tue Oct 29 10:29:21 2013

                40315 blocks of size 131072. 22822 blocks available
smb: \>
```

Observe que no parâmetro -Uadministrator%'Inicial2013@', deve ser fornecido o usuário e senha, no formato usuário%senha.

3.1.6 Testando autenticação no *Kerberos*

A validade do *ticket* de autenticação do Kerberos pode ser testado através do comando *kinit*, conforme ilustrado no comando a seguir:

```
master:~/samba-4.1.0 # kinit administrator@ENTERPRISE.LOCAL
Password for administrator@ENTERPRISE.LOCAL:
Warning: Your password will expire in 41 days on Tue Dec 10 13:01:39 2013
```

3.1.7 Comandos para gerenciamento de usuários e grupos do *Active Directory*

A seguir apresenta-se alguns comandos úteis para o gerenciamento de usuários e grupos no Samba 4.

1. Criar contas de usuários:

```
master:~/samba-4.1.0 # samba-tool user add USUARIO
```

2. Alterar senha das contas de usuários:

```
master:~/samba-4.1.0 # samba-tool user setpassword USUARIO
```

3. Apagar uma conta de usuários:

```
master:~/samba-4.1.0 # samba-tool user delete USUARIO
```

4. Listar todas as contas de usuários:

```
master:~/samba-4.1.0 # samba-tool user list
```

5. Desativar uma conta de usuário:

```
master:~/samba-4.1.0 # samba-tool user disable USUARIO
```

6. Ativar uma conta de usuário:

```
master:~/samba-4.1.0 # samba-tool user enable USUARIO
```

7. Expirar senhas de contas de usuários:

```
master:~/samba-4.1.0 # samba-tool user setexpiry USUARIO –-days=10
```

8. Cancelar a expiração de senha:

```
master:~/samba-4.1.0 # samba-tool user setexpiry USUARIO –-noexpiry
```

9. Criar grupo de usuário:

```
master:~/samba-4.1.0 # samba-tool group add GRUPO
```

10. Criar descrição do grupo:

```
master:~/samba-4.1.0 # samba-tool group add GRUPO –-description=”GRUPO
TESTE”
```

11. Adicionar usuário ao grupo:

```
master:~/samba-4.1.0 # samba-tool group addmembers GRUPO USUARIO
```

12. Adicionar um grupo dentro de outro grupo:

```
master:~/samba-4.1.0 # samba-tool group addmemebers GRUPO GRUPO1
```

13. Adicionar vários usuários a um grupo:

```
master:~/samba-4.1.0 # samba-tool group addmemebers GRUPO “USUARIO1,
USUARIO2”
```

14. Remover grupo:

```
master:~/samba-4.1.0 # samba-tool group delete GRUPO
```

15. Remover um usuário de um grupo:

```
master:~/samba-4.1.0 # samba-tool group removemembers GRUPO USUARIO
```

16. Remover membros de um grupo:

```
master:~/samba-4.1.0 # samba-tool group removemembers GRUPO “USUARIO1,
USUARIO2”
```

17. Listar todos os grupos:

```
master:~/samba-4.1.0 # samba-tool group list
```

18. Listar usuários pertencentes a um grupo:

```
master:~/samba-4.1.0 # samba-tool group listmembers GRUPO
```

3.1.8 Configurando o serviço NTP

Nesta etapa será configurado o serviço NTP para a rede local, onde todos os computadores atualizarão seus relógios através do servidor *Active Directory*. O servidor *Active Directory* irá sincronizar seu relógio com a.ntp.br ou b.ntp.br, que são servidores NTP disponíveis na Internet.

```
master:~/samba-4.1.0 # vim /etc/ntp.conf
server a.ntp.br  iburst prefer
server b.ntp.br  iburst prefer
driftfile /var/lib/ntp/ntp.drift
logfile /var/log/ntp
ntpsigndsocket /usr/local/samba/var/lib/ntp_signd/
restrict default kod nomodify notrap nopeer mssntp
restrict 127.0.0.1
restrict a.ntp.br  mask 255.255.255.255 nomodify notrap nopeer noquery
restrict b.ntp.br mask 255.255.255.255 nomodify notrap nopeer noquery
```

3.1.9 Preparando e instalando o *Active Directory Slave*

1. Configurando o *hostname*

```
[root@localhost ~]# vi /etc/sysconfig/network
NETWORKING=yes
HOSTNAME=slave.enterprise.local
```

Onde:

- NETWORKING: Parâmetro utilizado para ativação dos recursos de rede, na distribuição CentOS.

- HOSTNAME: Parâmetro utilizado para configuração do nome do servidor, na distribuição CentOS.

2. Configure a interface de rede com endereço IP fixo, conforme ilustrado a seguir:

```
[root@localhost ~]# vi /etc/sysconfig/network-scripts/ifcfg-eth0

DEVICE=eth0
HWADDR=08:00:27:99:49:0F
TYPE=Ethernet
UUID=aa50a3af-b417-473c-a543-a814e5112350
ONBOOT=yes
NM_CONTROLLED=yes
BOOTPROTO=static
IPADDR=192.168.0.20
NETMASK=255.255.255.0
GATEWAY=192.168.0.1
```

Onde:

- ONBOOT: Parâmetro utilizado "*yes*" para que a interface seja ativada na inicialização do sistema operacional.

- BOOTPROTO: *Static* indica que o endereço IP da interface é estático, isto é, fixo.

- IPADDR: Endereço IP da interface de rede.

- NETMASK: Máscara de rede.

- GATEWAY: *Gateway* da rede.

3. Desativando os recursos de *SELinux* do CentOS:

```
[root@slave ~]# vi /etc/sysconfig/selinux

SELINUX=disabled
```

4. Atualizando o CentOS:

```
[root@slave ~]# yum update –y
```

5. Após toda a pré-configuração do servidor ter sido realizada, precisamos instalar os pacotes necessários para resolver as dependências da instalação do Samba 4.

```
[root@slave ~]# yum install gcc libacl-devel libblkid-devel gnutls-devel
readline-devel python-devel gdb pkgconfig krb5-workstation zlib-devel
setroubleshoot-server libaio-devel setroubleshoot-plugins policycoreutils-
python libsemanage-python setools-libs-python setools-libs popt-devel
libpcap-devel sqlite-devel libidn-devel libxml2-devel libacl-devel
libsepol-devel libattr-devel keyutils-libs-devel cyrus-sasl-devel cups-
devel bind-utils cups ntp wget gcc* pam* fam* gamin* python* mlocate ntsysv
openldap xinetd rsync vim* openldap-devel openldap-clients -y
```

6. Em seguida baixe o pacote tar.gz do repositório oficial do Samba 4 e o descompacte-o:

```
[root@slave ~]# wget http://www.samba.org/samba/ftp/stable/samba-
4.1.0.tar.gz
[root@slave ~]# tar -xvzf samba-4.1.0.tar.gz
[root@slave ~]# cd samba-4.1.0
```

7. Iniciando o processo de compilação do Samba 4:

```
[root@slave samba-4.1.0]# ./configure --enable-debug --enable-selftest
…
Building with Active Directory support.
…
```

8. Compilando e instalando o Samba 4:

```
[root@slave samba-4.1.0]# make && make install

Waf: Leaving directory `/root/samba-4.1.0/bin'
'install' finished successfully (11m6.930s)
```

9. Criando os *links* para acesso direto ao *software* samba e smbclient.

```
[root@slave samba-4.1.0]# ln -s /usr/local/samba/sbin/samba /bin/samba
[root@slave samba-4.1.0]# ln -s /usr/local/samba/bin/smbclient
/bin/smbclient
```

3.1.10 Configurando o Kerberos no servidor slave

1. O conteúdo do arquivo /etc/krb5.conf deve ser substituído pelo conteúdo apresentado no quadro a seguir:

```
[root@slave samba-4.1.0]# vim /etc/krb5.conf

[logging]
 default = FILE:/var/log/krb5libs.log
 kdc = FILE:/var/log/krb5kdc.log
 admin_server = FILE:/var/log/kadmind.log

[libdefaults]
 default_realm = ENTERPRISE.LOCAL
 dns_lookup_realm = true
 dns_lookup_kdc = true
 ticket_lifetime = 24h
 renew_lifetime = 7d
 forwardable = true

[realms]
 ENTERPRISE.LOCAL = {
  kdc = master.enterprise.local #endereço do servidor de tickets
  admin_server = master.enterprise.local
 }

[domain_realm]
 .enterprise.local = ENTERPRISE.LOCAL
 enterprise.local = ENTERPRISE.LOCAL
```

2. Gerando o *ticket* para o usuário *administrator*.

Para gerar o *ticket* do *administrator*, necessário executar o comando *kinit* da seguinte forma:

```
kinit administrator@ENTERPRISE.LOCAL
Password for administrator@ENTERPRISE.LOCAL:
Warning: Your password will expire in 41 days on Mon Dec 16 16:44:53 2013
```

3. Verifique se o usuário *administrator* obteve seu *ticket* através do comando *klist*.

```
[root@slave ~]# klist
Ticket cache: FILE:/tmp/krb5cc_0
Default principal: administrator@ENTERPRISE.LOCAL

Valid starting     Expires            Service principal
11/04/13 17:01:52  11/05/13 03:01:52
krbtgt/ENTERPRISE.LOCAL@ENTERPRISE.LOCAL
        renew until 11/11/13 17:01:52
```

3.1.11 Configurando Samba como servidor slave

Para adicionar um servidor Samba 4 como *slave*, deve ser utilizado o comando *samba-tool*, com a opção "*domain join*", conforme ilustrado a seguir:

```
[root@slave ~]# samba-tool domain join enterprise.local DC -Uadministrator
--realm=enterprise.local
Finding a writeable DC for domain 'enterprise.local'
Found DC master.enterprise.local
Password for [WORKGROUP\administrator]:
workgroup is ENTERPRISE
realm is enterprise.local
checking sAMAccountName
Adding CN=SLAVE,OU=Domain Controllers,DC=enterprise,DC=local
Adding CN=SLAVE,CN=Servers,CN=Default-First-Site-
…
Replicating critical objects from the base DN of the domain
Partition[DC=enterprise,DC=local] objects[97/97] linked_values[23/0]
Partition[DC=enterprise,DC=local] objects[360/263] linked_values[23/0]
Done with always replicated NC (base, config, schema)
Replicating DC=DomainDnsZones,DC=enterprise,DC=local
Partition[DC=DomainDnsZones,DC=enterprise,DC=local] objects[40/40]
linked_values[0/0]
Replicating DC=ForestDnsZones,DC=enterprise,DC=local
Partition[DC=ForestDnsZones,DC=enterprise,DC=local] objects[18/18]
linked_values[0/0]
Partition[DC=ForestDnsZones,DC=enterprise,DC=local] objects[36/18]
linked_values[0/0]
Committing SAM database
Sending DsReplicateUpdateRefs for all the replicated partitions
Setting isSynchronized and dsServiceName
Setting up secrets database
Joined domain ENTERPRISE (SID S-1-5-21-1614055795-1312198854-1393802023) as
a DC
Setting up secrets database
Joined domain ENTERPRISE (SID S-1-5-21-1614055795-1312198854-1393802023) as
a DC
```

Observe que a execução deste comando deve ser realizado com o *Active Directory master* ativo, pois ocorrerá uma pesquisa na rede pelo DC mestre.

Além disso, também será solicitada a senha do *administrator* para adesão ao domínio.

1. Criando *script* de inicialização automática. No CentOS, o *script* de inicialização de serviços é diferente do utilizado no openSUSE. Veja o exemplo a seguir:

```
[root@slave ~]# vi /etc/init.d/samba
#!/bin/bash
. /etc/init.d/functions
. /etc/sysconfig/network
prog=samba
prog_dir=/usr/local/samba/sbin/
lockfile=/var/lock/subsys/$prog
start() {
        [ "$NETWORKING" = "no" ] && exit 1
#       [ -x /usr/sbin/ntpd ] || exit 5

                # Start daemons.
                echo -n $"Starting samba4: "
                daemon $prog_dir/$prog -D
        RETVAL=$?
                echo
        [ $RETVAL -eq 0 ] && touch $lockfile
        return $RETVAL
}
stop() {
        [ "$EUID" != "0" ] && exit 4
                echo -n $"Shutting down samba4: "
        killproc $prog_dir/$prog
        RETVAL=$?
                echo
        [ $RETVAL -eq 0 ] && rm -f $lockfile
        return $RETVAL
}

# See how we were called.
case "$1" in
start)
        start
        ;;
stop)
        stop
        ;;
status)
        status $prog
        ;;
restart)
        stop
        start
        ;;
reload)
        echo "Not implemented yet."
        exit 3
        ;;
*)
        echo $"Usage: $0 {start|stop|status|restart|reload}"
        exit 2
esac
```

2. Ajustando a permissão de execução no *script.* O *script* de inicialização deve ter permissões de execução. O comando *chmod* permite esta atribuição, conforme ilustrado no comando a seguir:

```
[root@slave samba-4.1.0]# chmod +x /etc/init.d/samba
```

3. Configurando o *script* para execução junto ao *boot* do servidor. Para que o serviço Samba seja executado na inicialização do sistema operacional, devemos adicioná-lo à inicialização do sistema, através do comando *chkconfig*, ilustrado a seguir:

```
[root@slave samba-4.1.0]# chkconfig samba on
```

3.2 Ingressando estações de trabalho no domínio Samba 4

Para ingressarmos qualquer cliente no domínio é necessário que seja identificado o nome do domínio "enterprise.local", os relógios devem estar sincronizados quase que precisamente com servidor Samba 4.

Para efeitos de teste do cenário, vamos adicionar 3 usuários ao *Active Directory*, a saber Morpheus, Apolo e Jupiter.

```
master:/ # samba-tool user add morpheus
New Password:
Retype Password:
User 'morpheus' created successfully

master:/ # samba-tool user add apolo
New Password:
Retype Password:
User 'apolo' created successfully

master:/ # samba-tool user add jupiter
New Password:
Retype Password:
User 'jupiter' created successfully
```

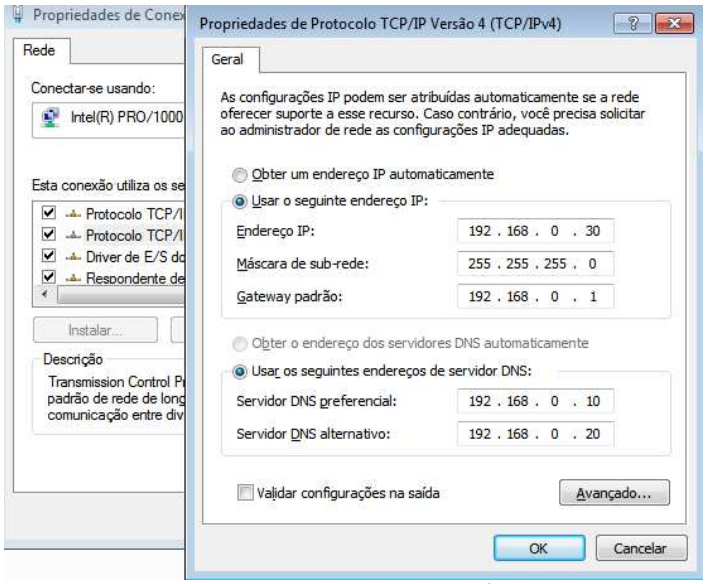
Observe que na execução do comando "*samba-tool user add*", é solicitado à senha do usuário.

3.2.1 Microsoft Windows 7

Para ingressar estações *Microsoft Windows 7* devem ser executados os seguintes passos:

1. Devemos primeiramente configurar a interface de rede do nosso cliente *Windows*. Localize o botão “Iniciar”, “Painel de Controle”, “Central de Rede e Compartilhamento” no menu a esquerda localize “Alterar as configurações do adaptador”. Clicar com o botão direito do mouse sobre “Conexão Local”, selecionar “Protocolo TCP/IP versão 4”, clicar em “Propriedades”. Nesse passo podemos definir o endereço IP da interface de rede, e também podemos fixar os endereços DNS, preferencial para o servidor *master*, secundário para *slave,* conforme ilustra a Figura 10.

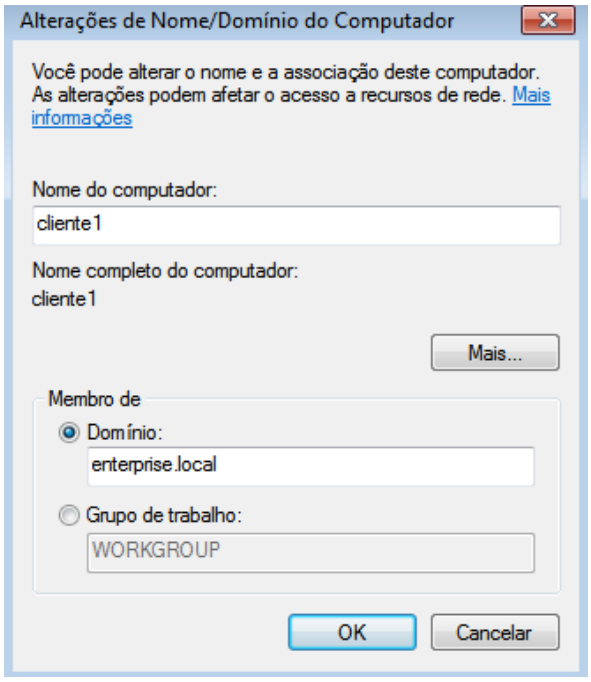
Figura 10: Propriedades da placa de rede.



Fonte: Autoria própria, 2013.

2. Para ingressar no domínio, clique com o botão direito do mouse sobre “Meu Computador”, localizar a opção “Propriedades”, em seguida “Sistema” localize e clique em “Alterar Configurações” na aba “Nome do computador”, clique em “Alterar” nesse passo devemos informar nome do domínio conforme ilustrado na Figura 11.

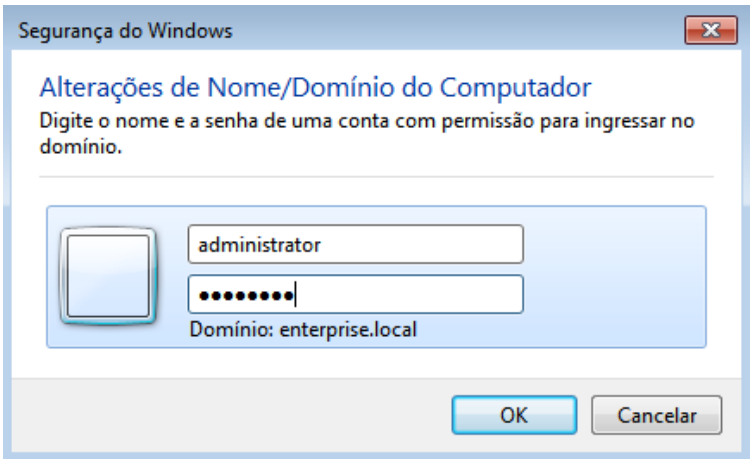
Figura 11: Alteração de nome e domínio do computador



Fonte: Autoria própria, 2013.

3. Agora será solicitado um *login* e senha para que a máquina ingresse no domínio. Este usuário deve ter permissões administrativas sobre o domínio, nesse caso será utilizado o usuário "*administrator*" do Samba 4 conforme ilustrado na Figura 12.

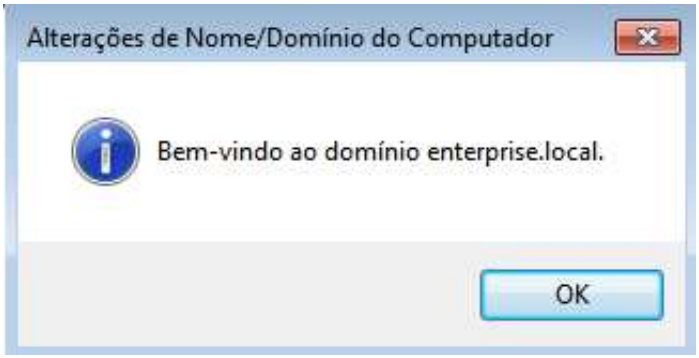
Figura 12: Autenticando com usuário do domínio



Fonte: Autoria própria, 2013.

4. Se tudo ocorrer bem, será aberta uma caixa de diálogo de bem-vindo ao domínio, conforme ilustrado na Figura 13.

Figura 13: Tela de boas vindas

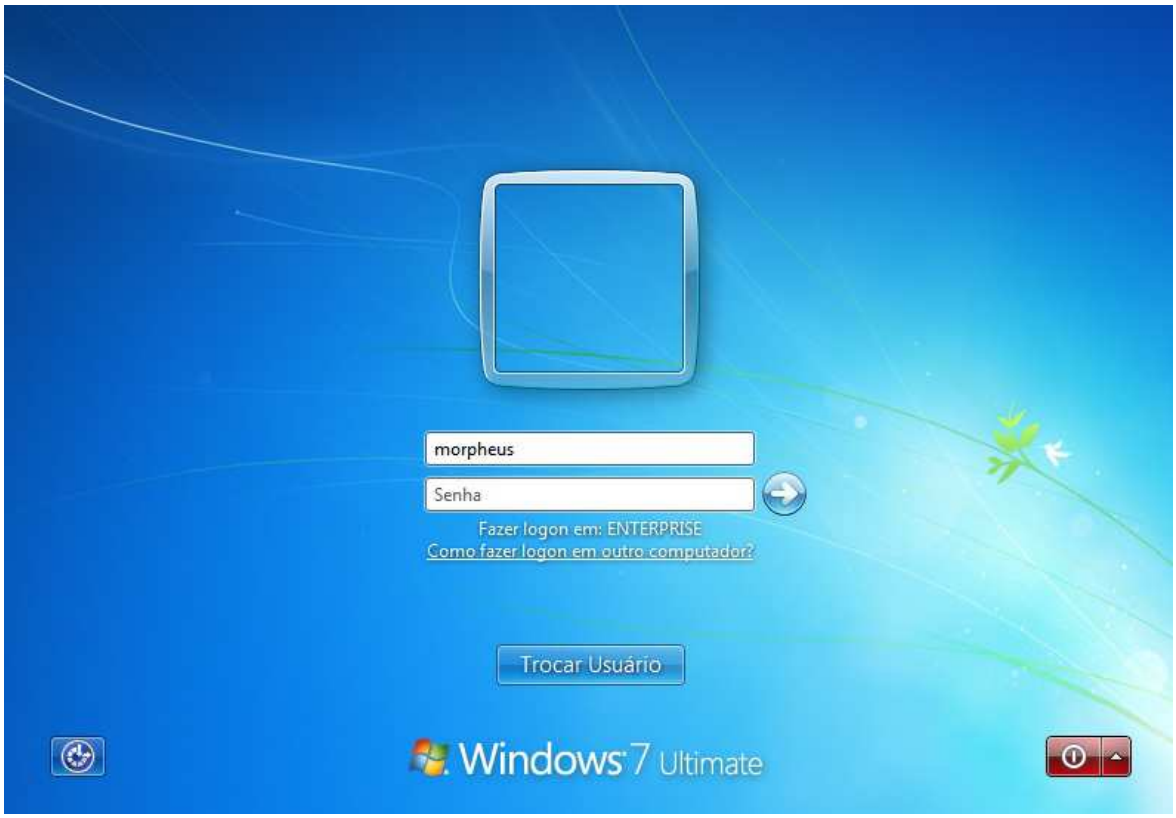


Fonte: Autoria própria, 2013.

5. Será solicitada a reinicialização do sistema operacional, para que sejam aplicadas as configurações do domínio.

6. Após o sistema ter sido reiniciado podemos utilizar as credencias de usuário criadas no servidor Samba 4 *Active Directory* conforme ilustrado na Figura 14.

Figura 14: Fornecendo credenciais.



Fonte: Autoria própria, 2013.

3.2.2 OpenSUSE *Desktop*

Também é possível ingressar ao domínio estações de trabalho com o sistema operacional Linux.

1. Altere o arquivo *hosts* onde identificamos nome do nosso servidor de domínio.

```
openSUSE-01:~ # vim /etc/hosts

127.0.0.1       localhost
192.168.0.30    openSUSE-01 openSUSE-01
127.0.0.1       openSUSE-01
192.168.0.10    master.enterprise.local master
```

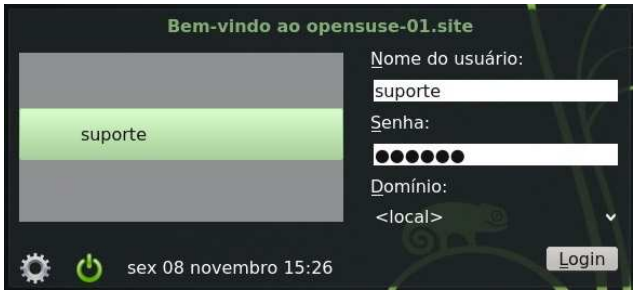
2. Em seguida altere o arquivo resolv.conf.

```
openSUSE-01:~ # vim /etc/resolv.conf

search enterprise.local
nameserver 192.168.0.10
```

3. Inicie o cliente openSUSE, e faça o *login* com o usuário criado na instalação do sistema operacional conforme ilustrado na Figura 15.

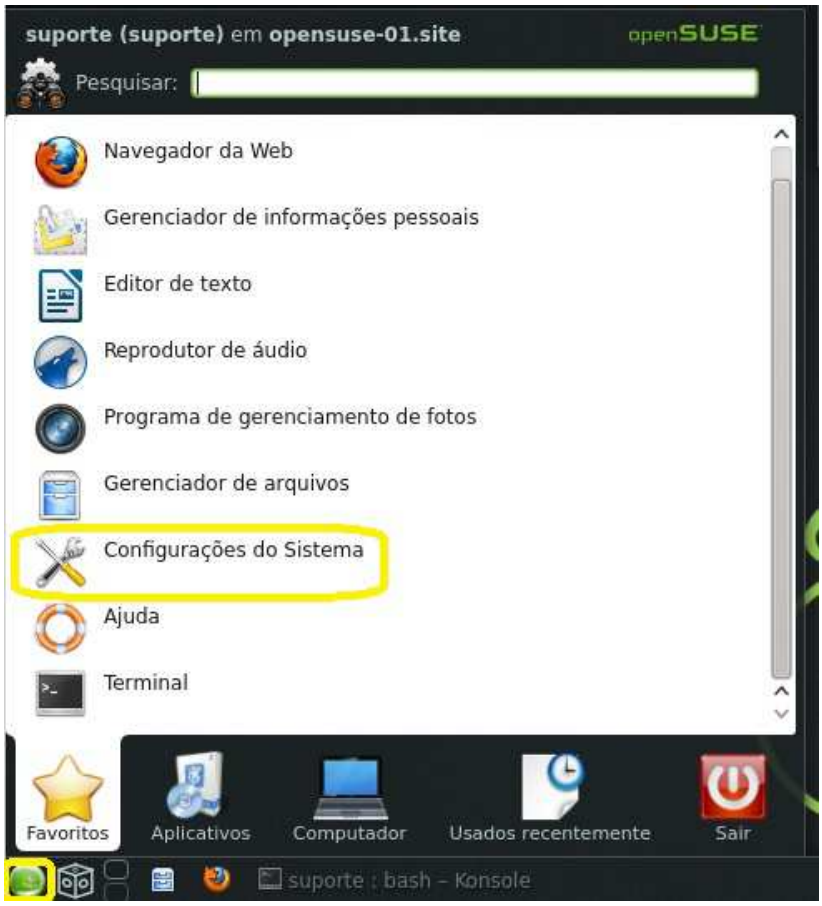
Figura 15: Tela autenticação openSUSE



Fonte: Autoria própria, 2013.

4. Em seguida vá até "Lançador de aplicativos *Kickoff*", em seguida "Configurações do Sistema" conforme ilustrado da Figura 16.

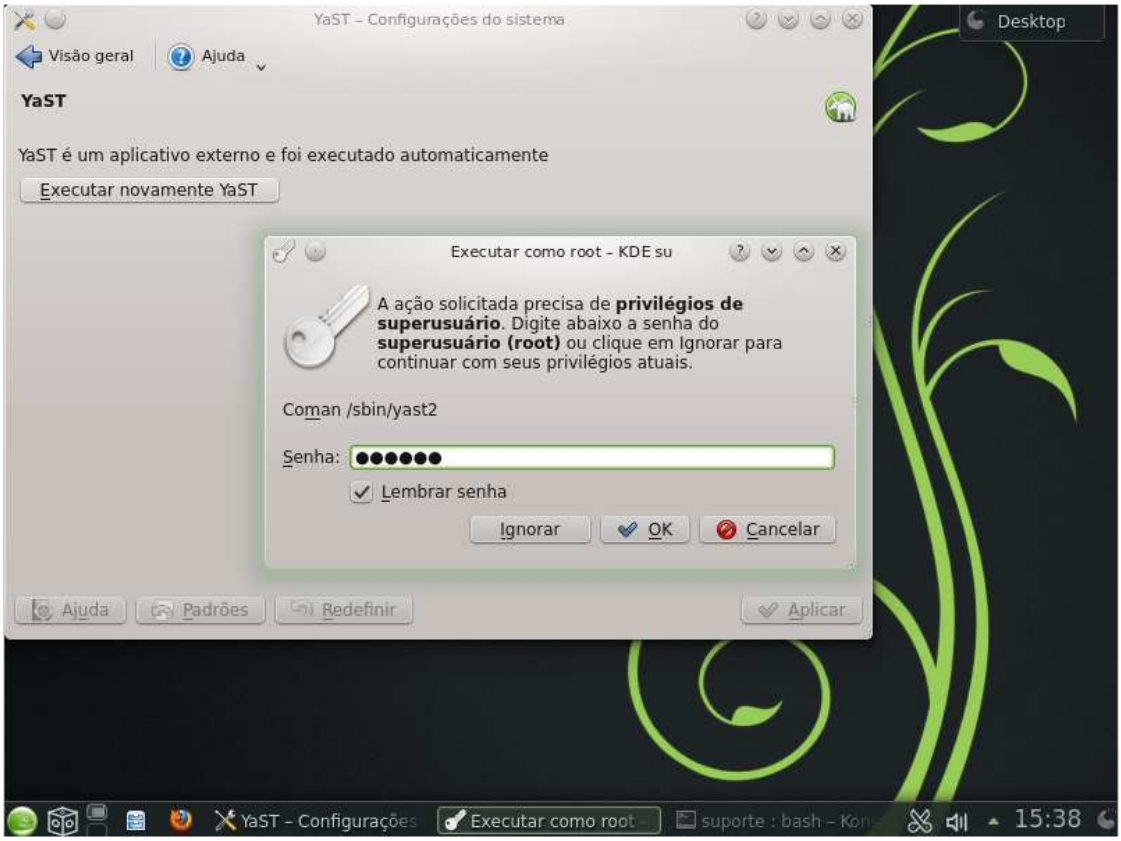
Figura 16: Lançador de aplicativos



Fonte: Autoria própria, 2013.

5. Na nova janela localize o ícone “YaST”, ao clicar em cima com o botão esquerdo do *mouse*, o mesmo vai solicitar que seja informada a senha do usuário *root* do sistema operacional, conforme ilustrado na Figura 17.

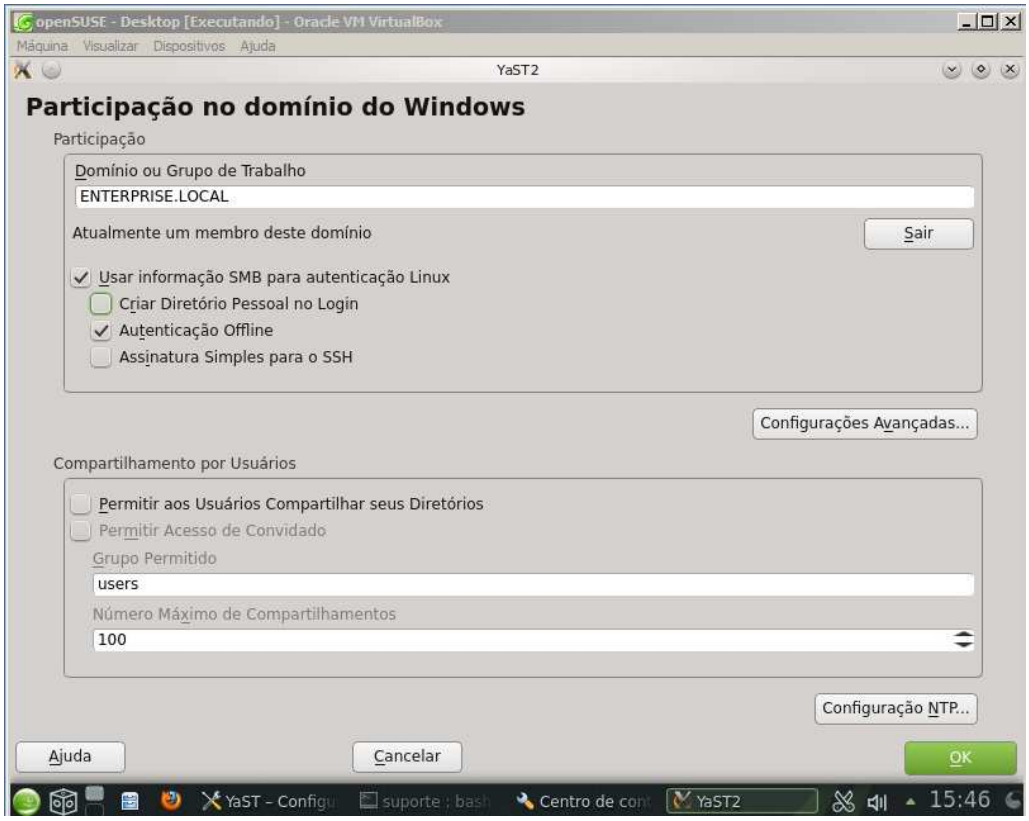
Figura 17: YaST



Fonte: Autoria própria, 2013.

6. Nessa nova janela vamos localizar “Sistema” e procurar por “Participação no domínio do *Windows*”, nessa etapa devemos informar os dados para que nosso cliente possa se autenticar. O próprio sistema vai verificar se o *winbind* e o Samba estão instalados. Após a verificação dessas dependências, podemos informar os dados para ingressarmos no domínio “ENTERPRISE.LOCAL” conforme ilustrado na Figura 18.

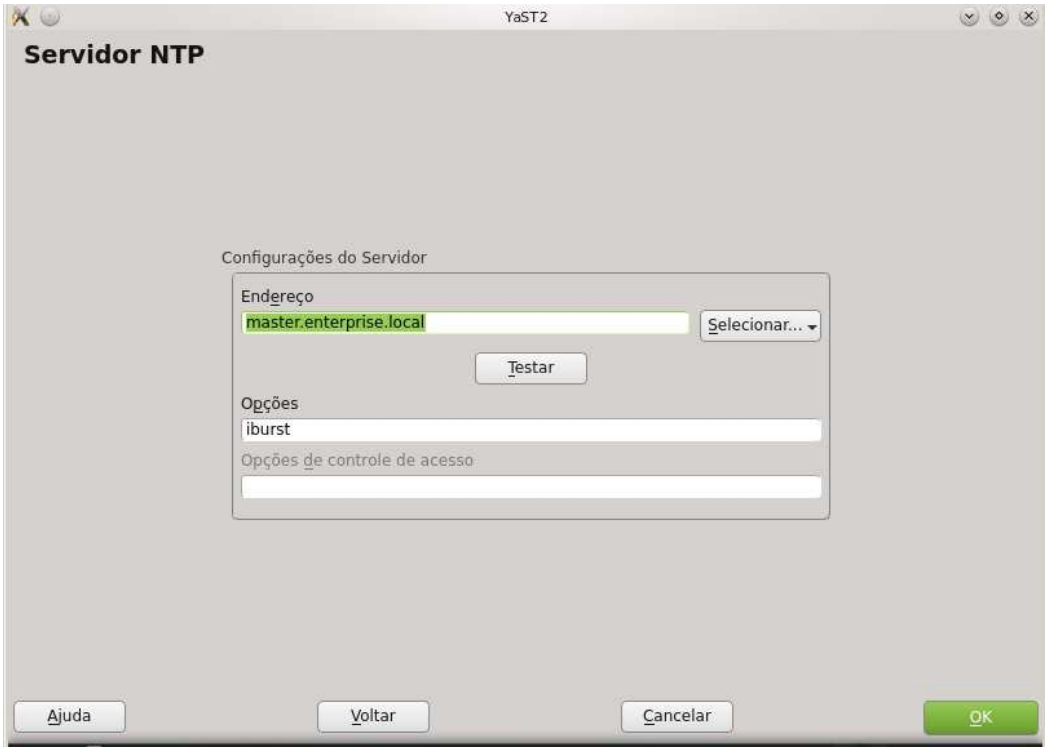
Figura 18: Autenticando no domínio.



Fonte: Autoria própria, 2013.

7. Na mesma janela do passo anterior, devemos configurar o serviço NTP, clicando em “Configuração NTP”, em seguida clique no botão “Adicionar”, em “Nova sincronização” selecione “Servidor”, e em seguida adicione o endereço do servidor Samba 4 *Active Directory* e clique no botão “OK”, conforme ilustrado na Figura 19.

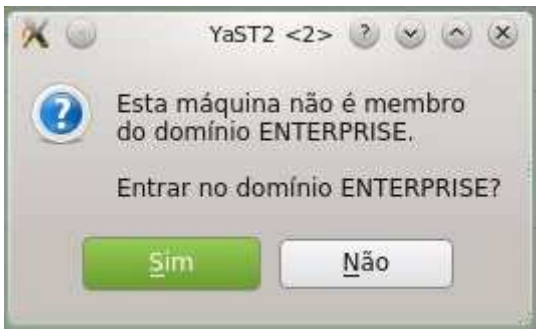
Figura 19: Servidor NTP



Fonte: Autoria própria, 2013.

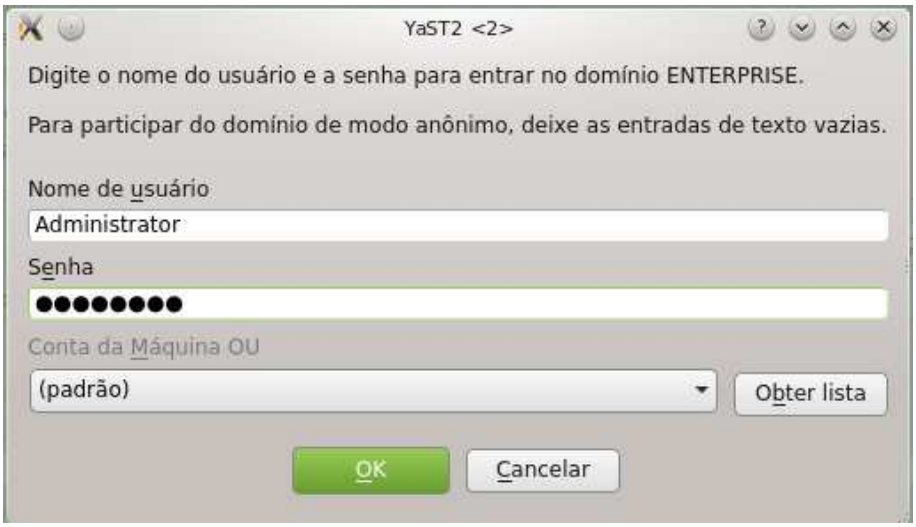
8. Após a configuração NTP ter sido realizada, clique novamente em “OK”, aparecerá uma nova caixa de diálogo informando que a máquina não faz parte do domínio, e se desejamos adicioná-la. Nesse passo clique em “Sim” e em seguida será solicitada a senha do usuário “*administrator*” do domínio, conforme ilustrado nas Figuras 20 e 21.

Figura 20: Ingressando no domínio 01.



Fonte: Autoria própria, 2013.

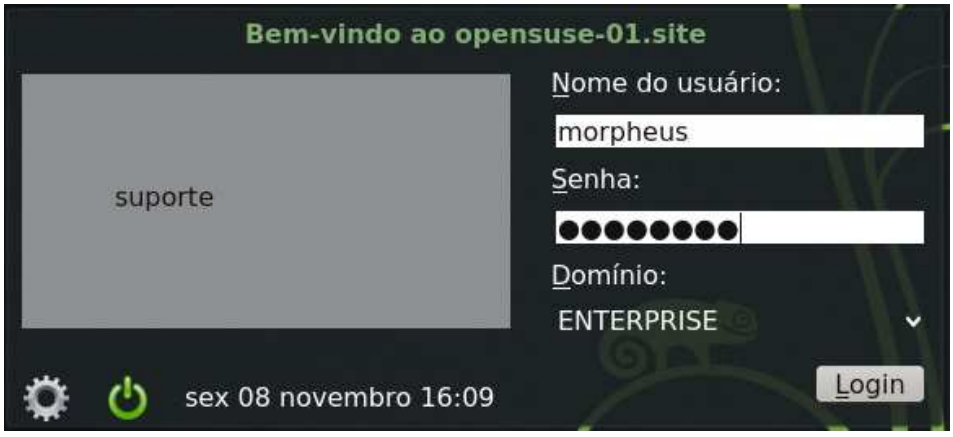
Figura 21: Ingressando no domínio.



Fonte: Autoria própria, 2013.

9. Devemos agora reiniciar o sistema operacional, para podermos autenticar com um usuário criado no *Active Directory*, conforme ilustrado na Figura 22.

Figura 22: Autenticando no *Active Directory*.



Fonte: Autoria própria, 2013.

10. Na próxima caixa de diálogo, o sistema irá perguntar se queremos que seja criado o diretório *home* do usuário Morpheus. Clique em “Sim”, conforme ilustrado na Figura 23.

Figura 23: Criando diretório *home* do usuário do domínio.

Fonte: Autoria própria, 2013.

11. Para termos certeza que o usuário Morpheus não é um usuário adicionado localmente, podemos fazer a leitura do arquivo passwd, onde ficam localizados todos os usuários locais do sistema operacional, conforme ilustrado a seguir.

Observe que, o usuário Morpheus não aparece na lista de usuários locais do Linux, ou seja, este usuário existe na base de dados do servidor *Active Directory*.

```
ENTERPRISE\morpheus@openSUSE-01:~> less /etc/passwd

at:x:25:25:Batch jobs daemon:/var/spool/atjobs:/bin/bash
avahi:x:494:492:User for Avahi:/var/run/avahi-daemon:/bin/false
bin:x:1:1:bin:/bin:/bin/bash
daemon:x:2:2:Daemon:/sbin:/bin/bash
dnsmasq:x:495:65534:dnsmasq:/var/lib/empty:/bin/false
ftp:x:40:49:FTP account:/srv/ftp:/bin/bash
games:x:12:100:Games account:/var/games:/bin/bash
lp:x:4:7:Printing daemon:/var/spool/lpd:/bin/bash
mail:x:8:12:Mailer daemon:/var/spool/clientmqueue:/bin/false
man:x:13:62:Manual pages viewer:/var/cache/man:/bin/bash
messagebus:x:498:496:User for D-Bus:/var/run/dbus:/bin/false
mysql:x:60:499:MySQL database admin:/var/lib/mysql:/bin/false
news:x:9:13:News system:/etc/news:/bin/bash
nobody:x:65534:65533:nobody:/var/lib/nobody:/bin/bash
ntp:x:74:498:NTP daemon:/var/lib/ntp:/bin/false
polkitd:x:492:491:User for polkitd:/var/lib/polkit:/sbin/nologin
postfix:x:51:51:Postfix Daemon:/var/spool/postfix:/bin/false
pulse:x:490:489:PulseAudio daemon:/var/lib/pulseaudio:/sbin/nologin
root:x:0:0:root:/root:/bin/bash
rtkit:x:491:490:RealtimeKit:/proc:/bin/false
sshd:x:497:494:SSH daemon:/var/lib/sshd:/bin/false
statd:x:493:65534:NFS statd daemon:/var/lib/nfs:/sbin/nologin
tftp:x:496:493:TFTP account:/srv/tftpboot:/bin/false
usbmux:x:499:65534:usbmuxd daemon:/var/lib/usbmuxd:/sbin/nologin
uucp:x:10:14:Unix-to-Unix CoPy system:/etc/uucp:/bin/bash
wwwrun:x:30:8:WWW daemon apache:/var/lib/wwwrun:/bin/false
suporte:x:1000:100:suporte:/home/suporte:/bin/bash
```

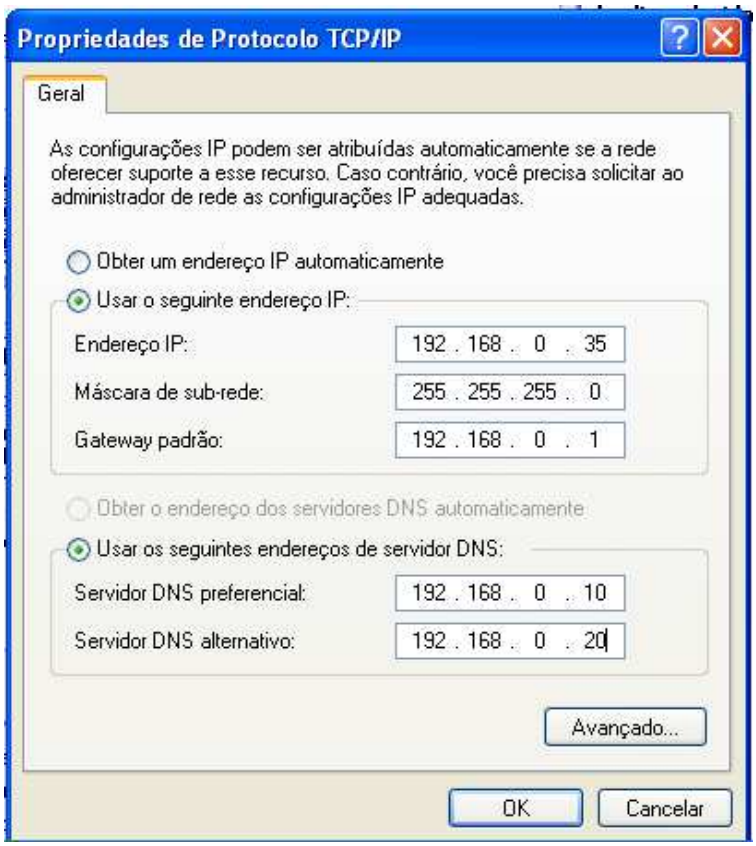
Com isto, está finalizada a inclusão de uma estação Linux openSUSE no domínio *Active Directory*.

3.2.3 *Microsoft Windows XP*

Para estações com *Microsoft Windows XP*, os seguintes passos devem ser realizados:

1. Devemos primeiramente configurar a interface de rede do nosso cliente *Windows*. Localize o botão “Iniciar”, “Painel de Controle”, “Conexões de rede e internet”, localize “Conexões de Rede”. Clique com o botão direito do *mouse* sobre “Conexão Local”, selecione agora “Protocolo TCP/IP”, e clique em “Propriedades”. Nesse passo podemos definir o endereço IP da interface de rede, e também podemos fixar os endereços DNS, preferencial para o servidor *master*, secundário para *slave,* conforme ilustrado na Figura 24.

Figura 24: Propriedades da placa de rede

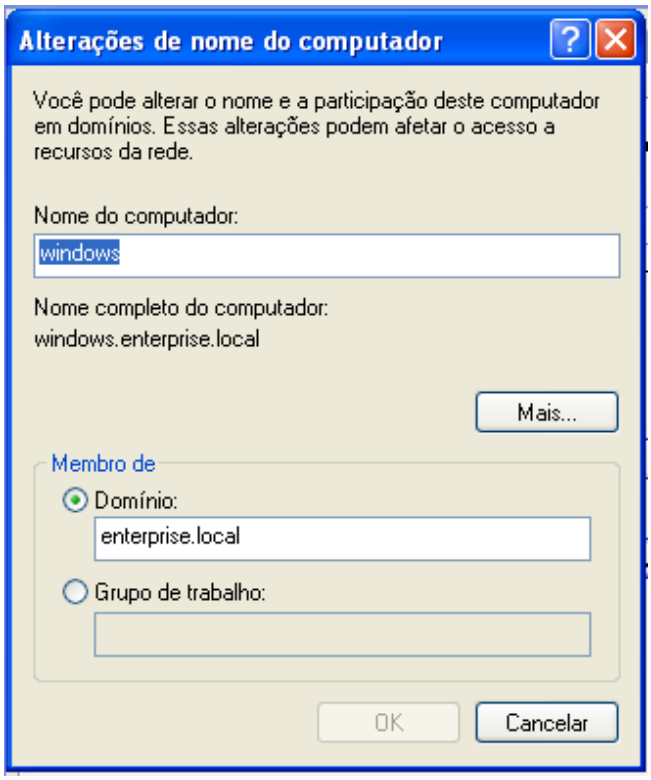


Fonte: Autoria própria, 2013.

2. Para ingressar no domínio, clique com o botão direito do *mouse* sobre “Meu Computador”, localize a opção “Propriedades” e, na aba “Nome do Computador”,

clique em “Alterar”. Nesse passo devemos informar nome do domínio conforme ilustrado na Figura 25.

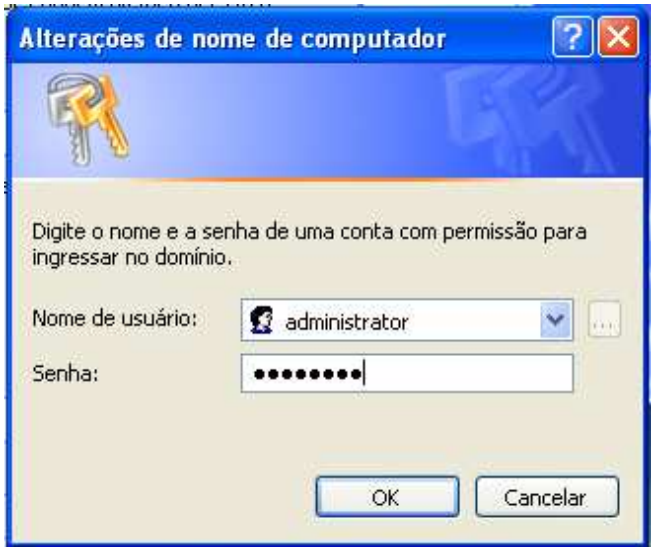
Figura 25: Alteração de nome e domínio do computador



Fonte: Autoria própria, 2013.

3. Agora será solicitado um *login* e senha para que a máquina ingresse ao domínio. Este usuário deve ter permissões administrativas sobre o domínio. Em nosso exemplo, será utilizado o usuário “*administrator*” do Samba 4 conforme ilustrado na Figura 26.

Figura 26: Autenticando com usuário do domínio



Fonte: Autoria própria, 2013.

4. Se houver falhas, irá aparecer uma caixa de diálogo dando as boas vindas ao domínio "enterprise.local". Após a reinicialização será possível efetuar o *login* com um usuário do Samba 4 *Active Directory* conforme ilustrado na figura 27.

Figura 27: Tela de *login* do *Windows* XP

Fonte: Autoria própria, 2013.

3.3 Ferramentas para gerenciamento do *Active Directory*

Para a realização de testes no *Active Directory,* utilizaremos uma ferramenta desenvolvida pela *Microsoft* para gerenciar o *Active Directory*. A ferramenta deve ser instalada no ambiente *Microsoft*, ou seja, no cliente *Microsoft Windows* 7 ou em qualquer outra versão a partir do *Microsoft Windows* XP.

Passos para a instalação da ferramenta:

1. Baixar as ferramentas "*Remote Server Administration Tools for Windows 7 with Service Pack 1 (SP1)*" e também "*Windows Server 2003 Service Pack 2 Administration Tools Pack for x86 editions*" a partir dos *links*:

- http://www.microsoft.com/downloads/details.aspx?FamilyID=7D2F6AD7-656B-4313-A005-4E344E43997D&displaylang=en

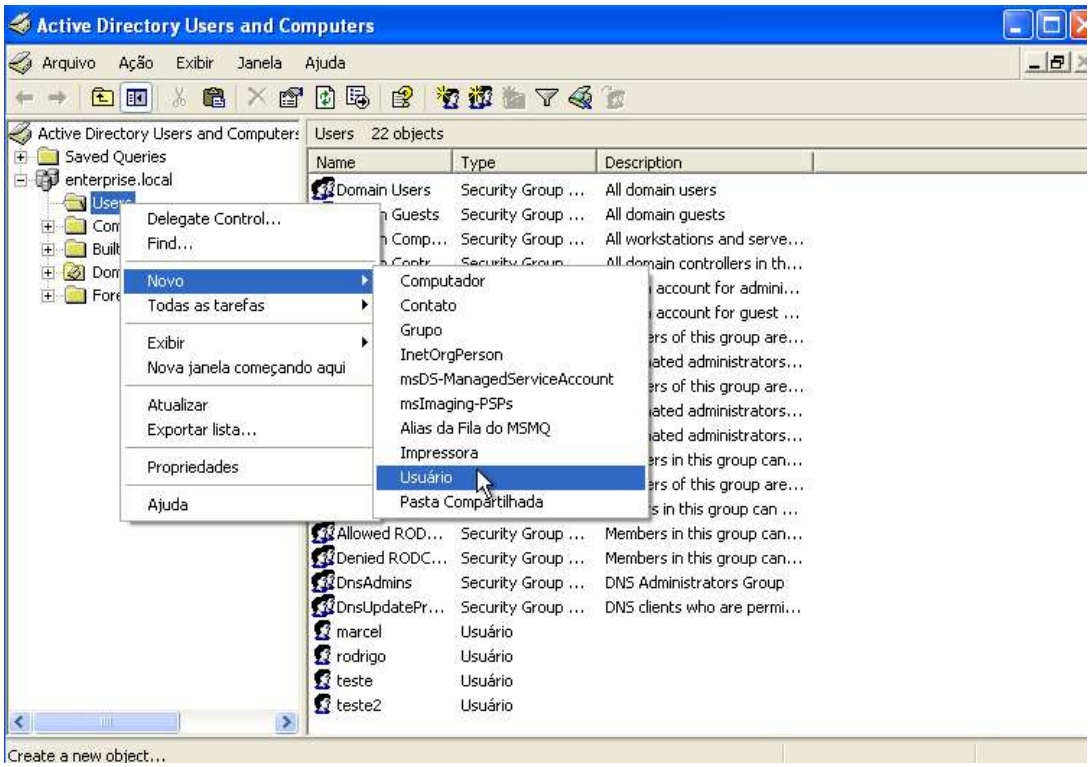
- http://www.microsoft.com/pt-br/download/details.aspx?id=19538

Essas ferramentas permitem a criação usuários, grupos e GPOs através do cliente. Cada objeto criado deve ser aplicado no servidor *Active Directory master* e replicado para o *slave*.

Após essas ferramentas terem sido devidamente instaladas vá até o botão "Iniciar", em seguida "Painel de Controle", "Ferramentas Administrativas" e "*Active Directory Users and Computers*".

2. Expandir árvore em "enterprise.local" clicando no sinal "+", assim podemos criar um usuário clicando com o botão direito do *mouse* em "Novo", "Usuário" como ilustrado na Figura 28.

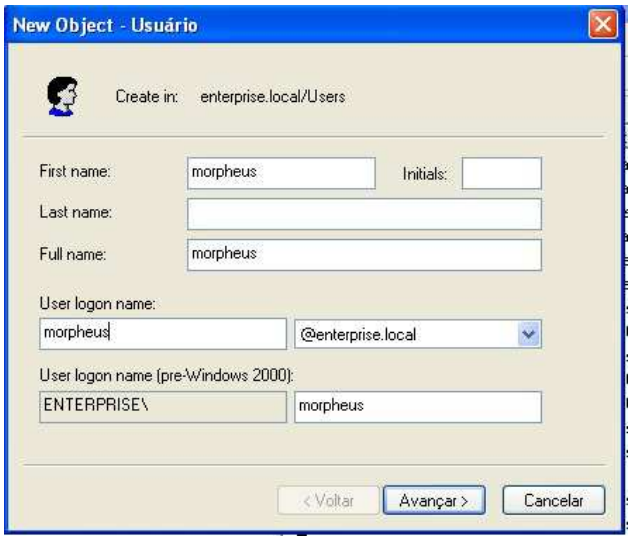
Figura 28: *Active Directory Users and Computers*



Fonte: Autoria própria, 2013.

3. Nessa caixa de diálogo devemos informar os atributos para a criação de um novo usuário conforme ilustrado na Figura 29.

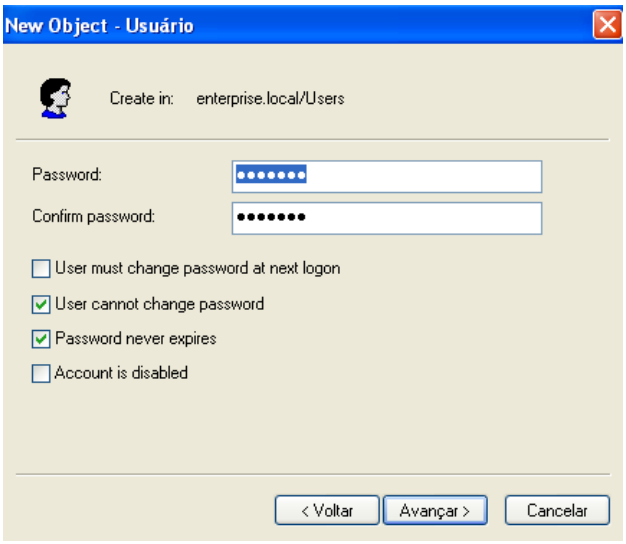
Figura 29: New Object



Fonte: Autoria própria, 2013.

4. Deve-se informar a senha do usuário, sendo que a mesma deve ter mais de sete caracteres, utilizando letras maiúsculas e minúsculas, números ou caracteres especiais, como ilustrado na Figura 30.

Figura 30: Definição da senha



Fonte: Autoria própria, 2013.

5. Em seguida clique em “Avançar” e “Concluir”.

3.3.1 Verificando usuários no *Active Directory master* e *slave*

1. Verifique no servidor *Active Directory master* se o usuário foi criado devidamente.

```
master:~ # wbinfo –u
Administrator
Guest
krbtgt
morpheus
apolo
jupiter
```

2. Agora verificamos com o mesmo comando no servidor *slave*.

```
[root@slave ~]# wbinfo –u
Administrator
Guest
krbtgt
morpheus
apolo
jupiter
```

Sendo assim podemos afirmar que a replicação dos dados entre o servidor *Active Directory master* e o servidor *slave*, está funcionando corretamente.

3.3.2 Criação de GPOs

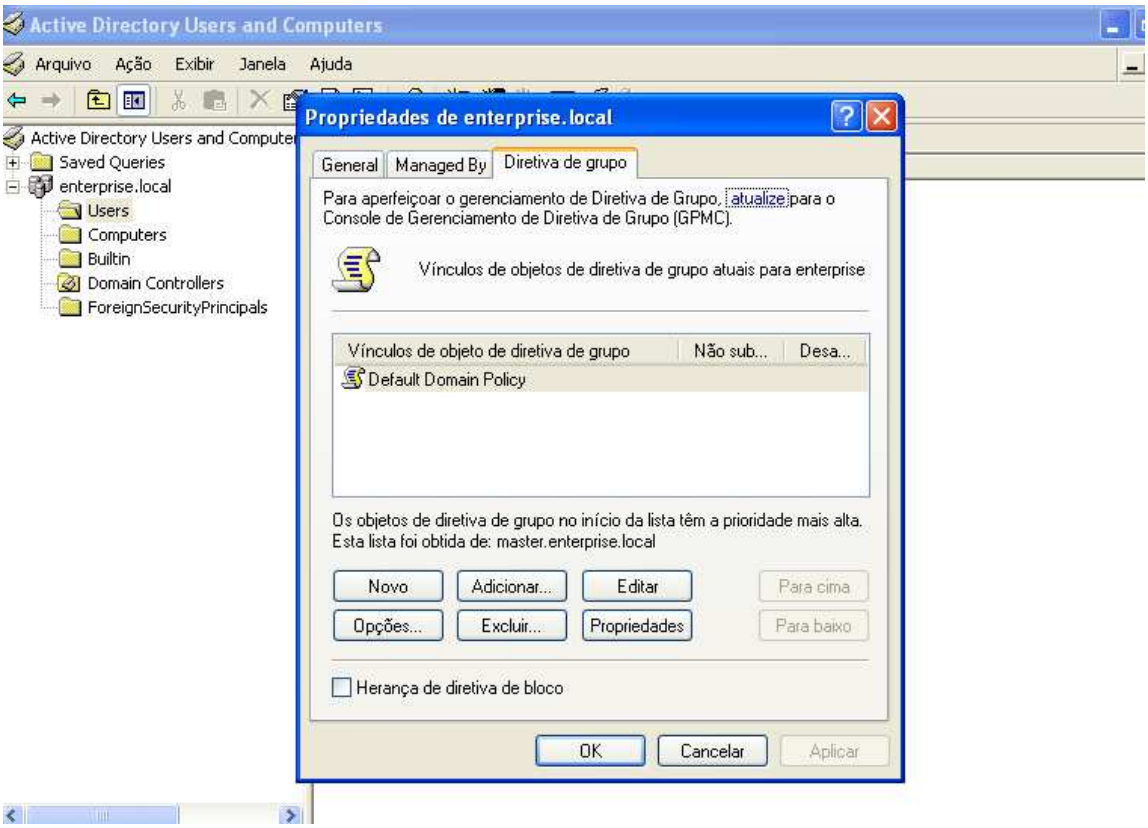
Para realizar a criação de GPO no Samba 4 *Active Directory*, será utilizada a ferramenta de gerenciamento do *Active Directory* desenvolvida pela *Microsoft*.

1. Vá até o menu “Iniciar”, “Painel de Controle”, “Ferramentas administrativas” e “*Active directory users and computers*”.

2. Clique com o botão direito do *mouse* sobre “enterprise.local”, e clique em propriedades.

3. Em propriedades, localize a aba “Diretiva de grupo”, conforme ilustrado na Figura 31.

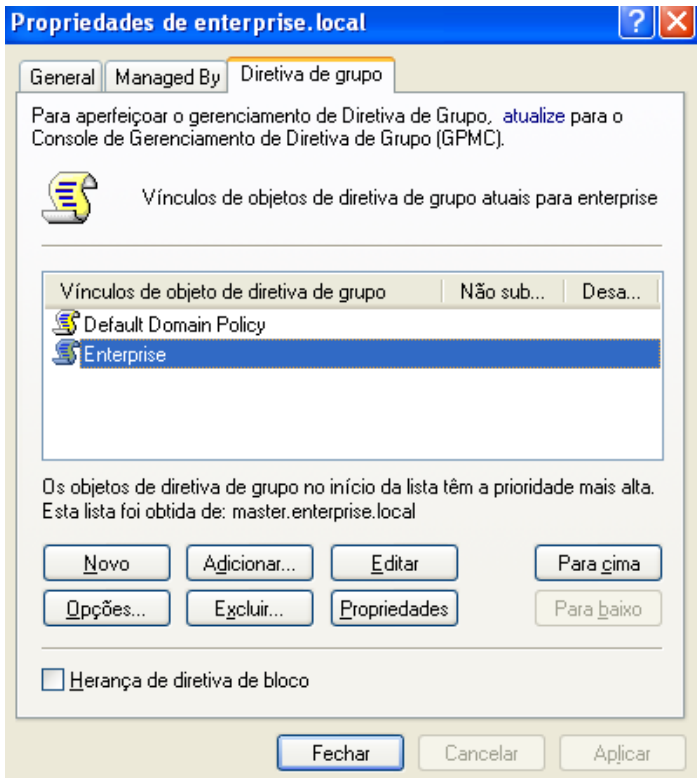
Figura 31: Criando GPO



Fonte: Autoria própria, 2013.

4. Clique no botão “Novo”, e defina um nome para o seu GPO como ilustrado na Figura 32 o nome “Enterprise”.

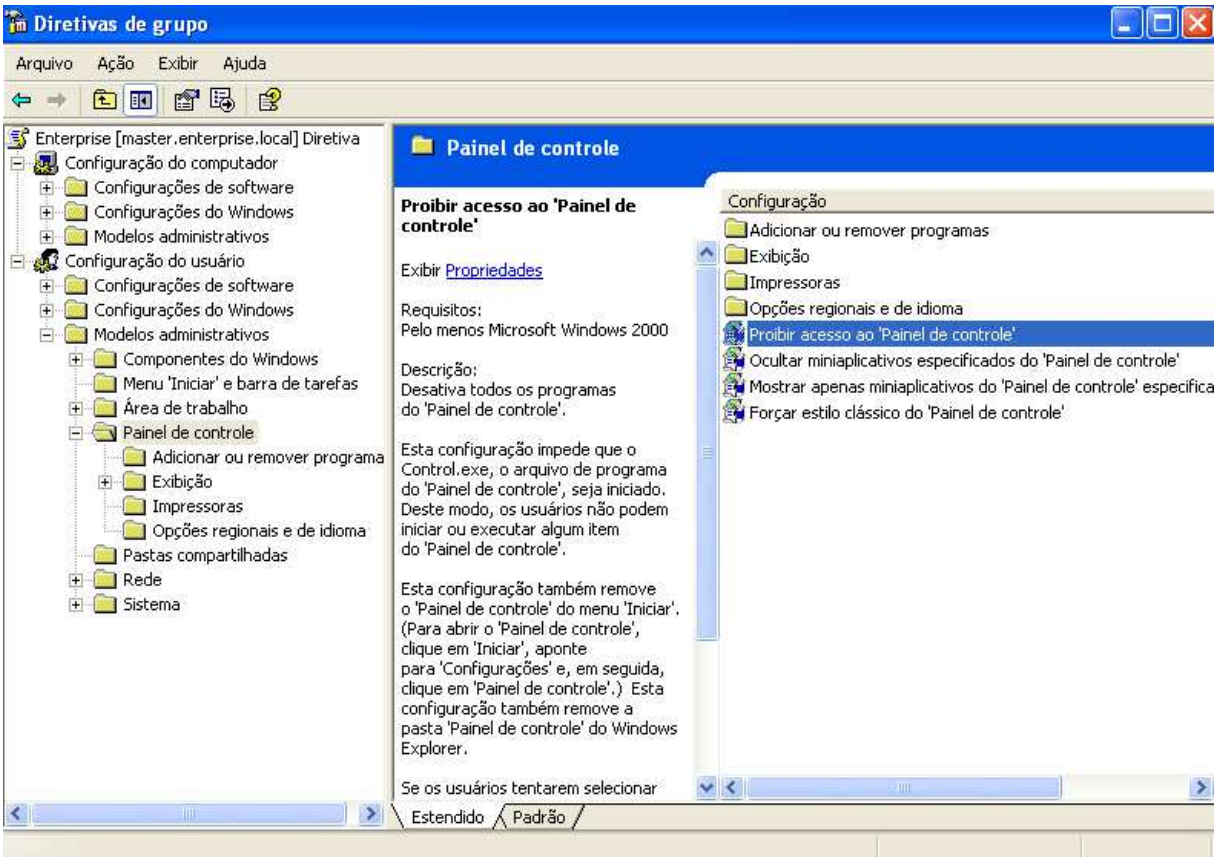
Figura 32: Definindo um nome para a GPO.



Fonte: Autoria própria, 2013.

5. Após o GPO ter sido criada, selecione-o e clique no botão “Editar”. O objetivo deste GPO será bloquear o acesso ao Painel de controle. Na próxima janela, conforme ilustrado na Figura 33, vá até “Configurações de usuário”, “Modelos administrativos”, “Painel de Controle”, nesta tela se encontra opção que queremos configurar, “Proibir acesso ao Painel de controle”. Clique duas vezes sobre essa opção e a ative selecionando a opção “Ativado”, e depois clique em “OK” conforme ilustrado na Figura 34.

Figura 33: Acesso as diretivas de grupo.



Fonte: Autoria própria, 2013.

Figura 34: Ativando GPO.

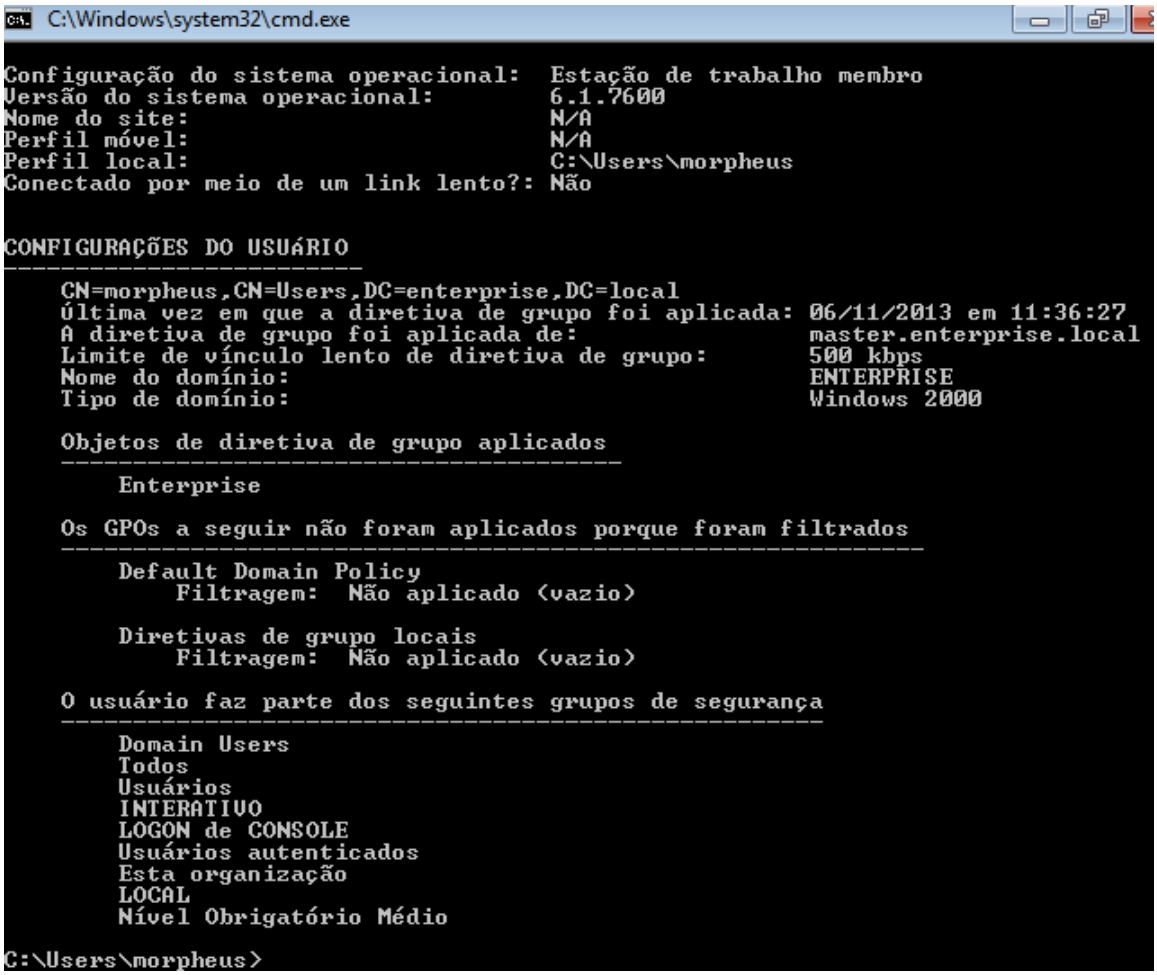
Fonte: Autoria própria, 2013.

6. Após o GPO ter sido aplicado, faremos um teste de replicação no cliente *Windows*, faça o *login* no cliente com o usuário “morpheus”, e execute o comando abaixo:

```
C:\Users\morpheus>gpresult /R
```

A saída do comando mostrará se as diretivas de grupos estão sendo aplicadas no cliente conforme ilustrado na Figura 35.

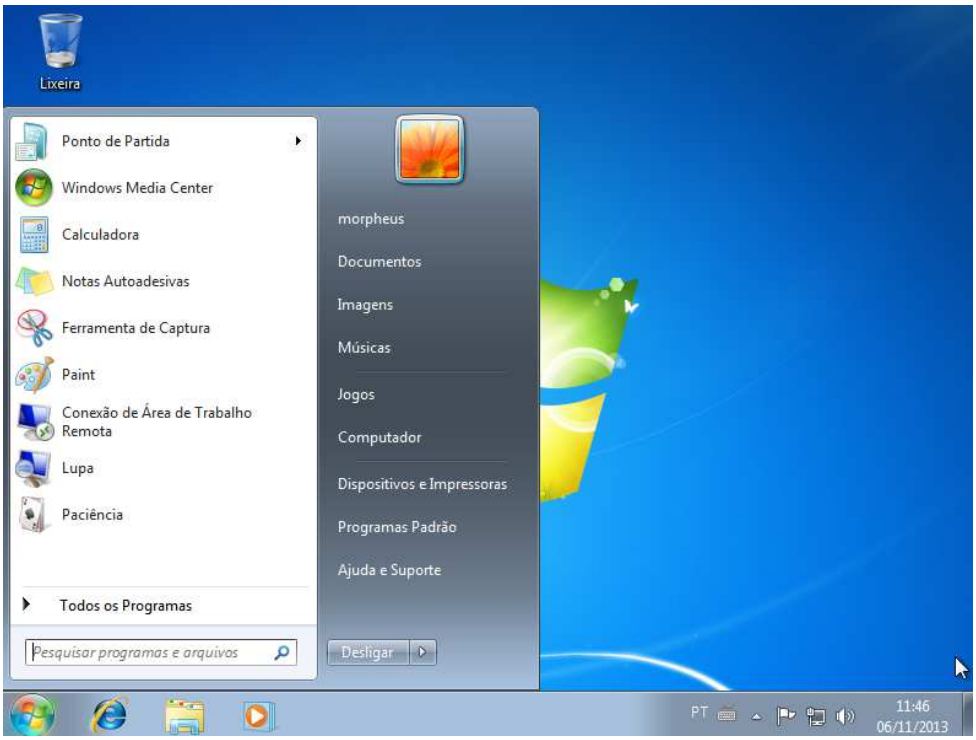
Figura 35: Resultado da diretiva de grupo.



Fonte: Autoria própria, 2013.

7. Podemos ver o resultado do GPO criado, na prática. Observe na Figura 36 que o menu “Painel de controle” não está mais acessível ao usuário Morpheus.

Figura 36: Demonstração da GPO aplicada.



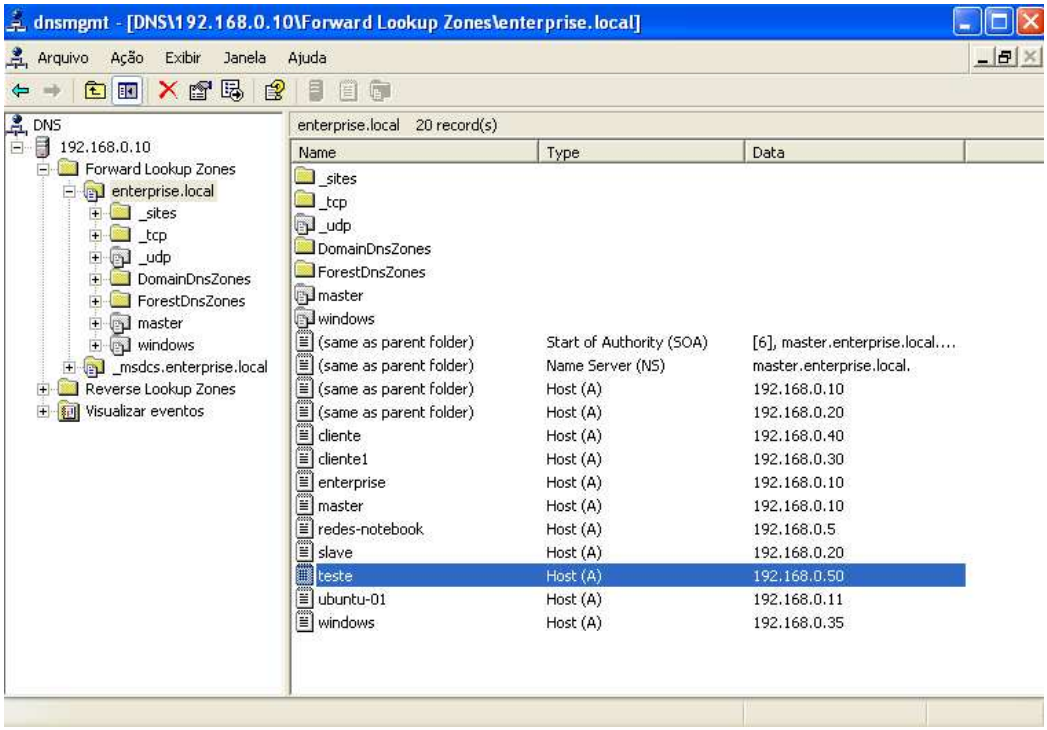
Fonte: Autoria própria, 2013.

3.3.3 Gerenciamento do DNS

Através da mesma ferramenta utilizada para gerenciar as diretivas de GPOs do *Active Directory*, podemos também administrar o DNS.

Para verificação dos registros no DNS basta ir até o menu “Iniciar”, “Ferramentas administrativas” e “DNS”. Basta agora expandir a árvore de diretório do DNS, clicando no símbolo “+”, até chegar ao “enterprise.local”, conforme ilustrado na Figura 37.

Figura 37: DNS *manager*.



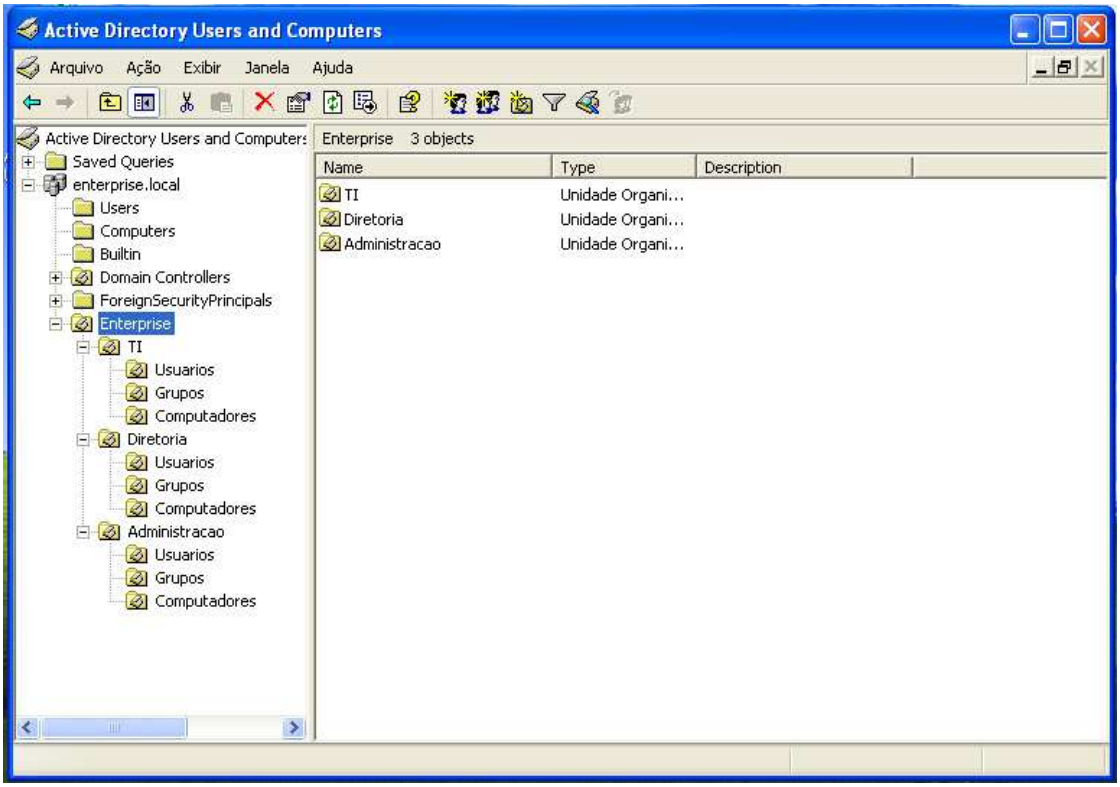
Autoria própria, 2013.

Esta ferramenta permite o gerenciamento de todos os registros do DNS, incluindo a adição e remoção dos mesmos.

3.3.4 Unidades Organizacionais

É muito importante à forma que vamos organizar nossas OUs, fazê-las de forma que coincida com a organização e seus departamentos, conforme ilustra a Figura 38.

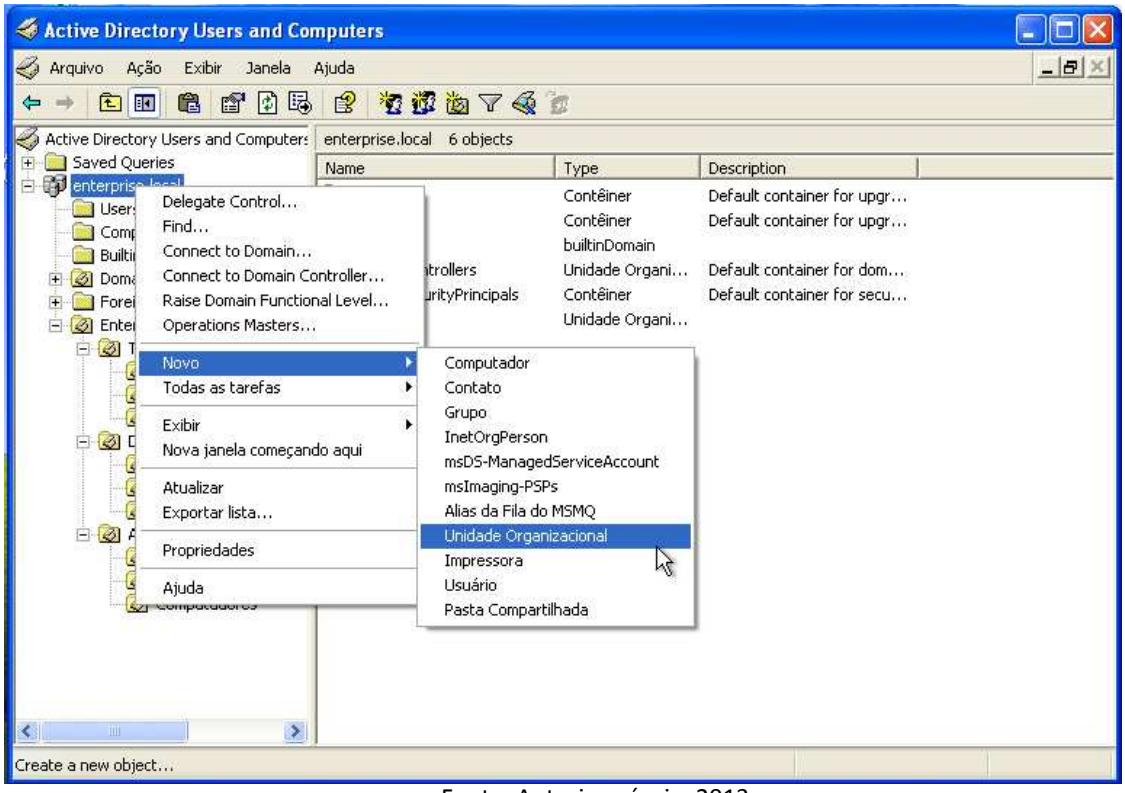
Figura 38: Organização OUs.



Fonte: Autoria própria, 2013.

1. Para criar uma Unidade Organizacional, bastas expandir a árvore do nosso domínio, clicando em “enterprise.local”, clique com o botão direito do *mouse*, vá em “Novo”, “Unidade Organizacional”, conforme ilustrado na Figura 39.

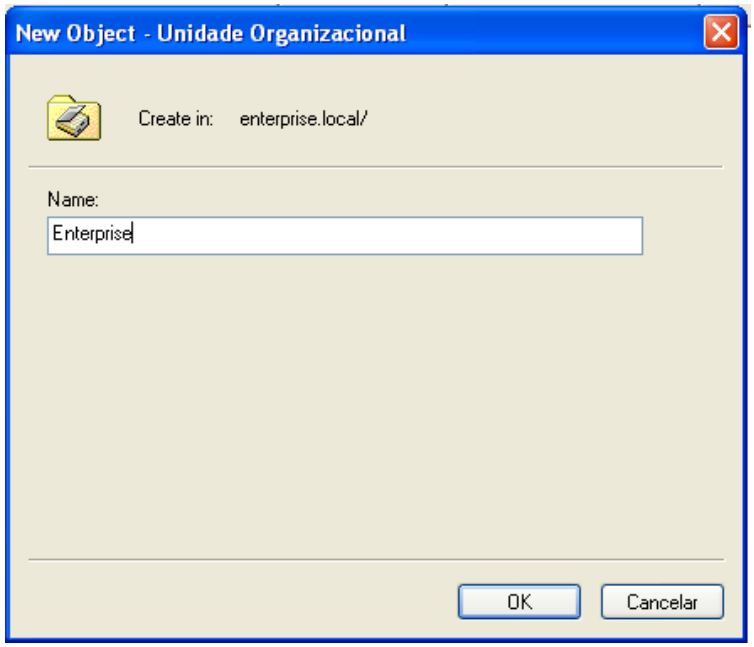
Figura 39: Criando OU.



Fonte: Autoria própria, 2013.

2. Na próxima caixa de diálogo, conforme ilustrado na Figura 40, basta informar o nome da nova Unidade Organizacional, e em seguida clique em “OK”.

Figura 40: Definindo nome da OU.



Fonte: Autoria própria, 2013.

3.4 Segurança e compartilhamento de dados

1. Para realizar um compartilhamento com o Samba 4, devemos configurar o arquivo smb.conf.

```
master:~ # vim /usr/local/samba/etc/smb.conf
[global]
        workgroup = ENTERPRISE
        realm = ENTERPRISE.LOCAL
        netbios name = MASTER
        server role = active directory domain controller
        dns forwarder = 8.8.8.8

[netlogon]
        path = /usr/local/samba/var/locks/sysvol/enterprise.local/scripts
        read only = No

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

[compartilhamento]
        comment = Compartilhamento
        path = /srv/storage/samba/compartilhamento
        read only = no
        guest ok = yes
        force create mode = 664
        force directory mode = 755
```

- ***comment*:** Define a descrição do compartilhado na lista de compartilhamentos em rede.

- ***path*:** Define o caminho do diretório que está sendo compartilhado.

- ***read only*:** Especifica se o compartilhamento terá acesso a leitura e escrita.

- ***guest*:** Define que nenhuma senha é necessária para se conectar ao compartilhamento.

- ***force create mode*:** Define as permissões para novos arquivos criados no compartilhamento;

- ***force directory mode*:** Define as permissões para novos diretórios criados no compartilhamento.

2. Após criar o compartilhamento no smb.conf, crie o diretório "compartilhamento", e aplique a permissão total. Após isso ser feito podemos ajustar as permissões através do *Active Directory*.

```
master:~ # mkdir -p /srv/storage/samba/compartilhamento
master:~ # chmod 1777 /srv/storage/samba/compartilhamento
```

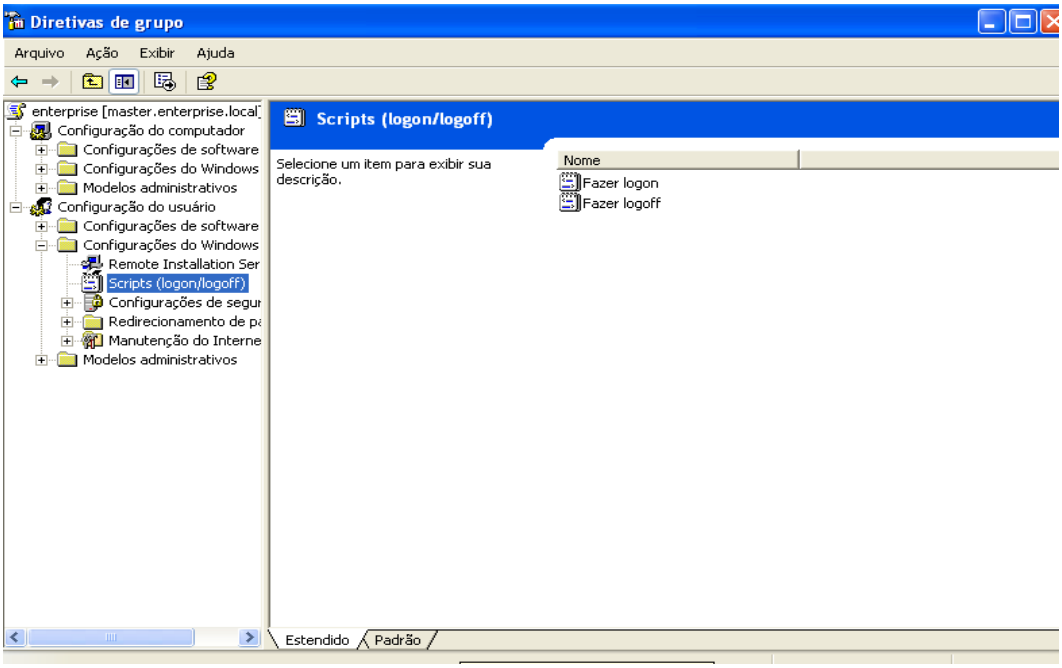
3. Podemos mapear as unidades de rede via GPO, basta criar um *script* com extensão .bat ou .cmd por exemplo, com o seguinte comando.

```
net use p: \\master\compartilhamento /yes
```

4. Acesse novamente o gerenciador do *Active Directory* através da estação *Windows*, clique com o botão direito do *mouse* sobre o domínio da empresa, e vá até "Propriedades". Nesta aba clique em "Diretiva de Grupo", e em seguida selecione o GPO já criado "ENTERPRISE", e clique em "Editar".

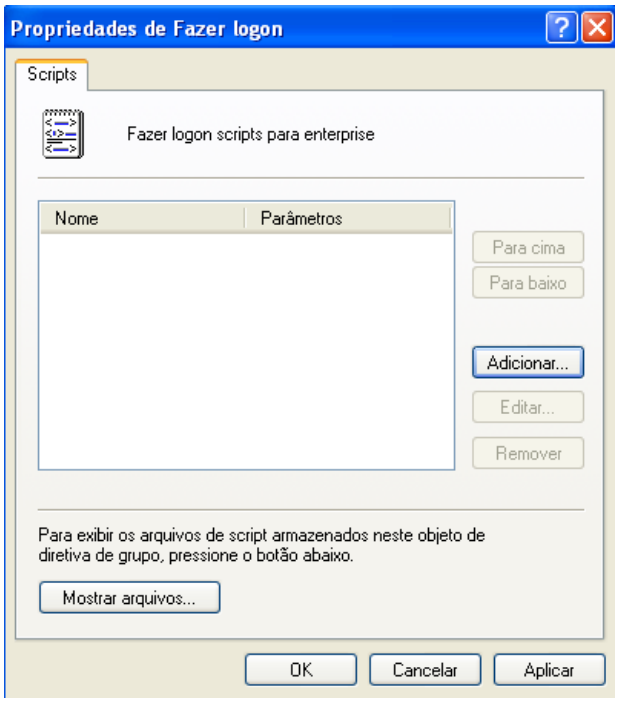
5. Localize em "Configuração do usuário", "Configurações do *Windows*", clique duas vezes com o *mouse* sobre "*Script (logon/Logoff)*". Em seguida com o botão direito do *mouse* clique sobre "Fazer *Logon*" no menu à direita, e em seguida em "Propriedades", conforme ilustrado nas Figuras 41 e 42.

Figura 41: Editando *script* de *logon*.



Fonte: Autoria própria, 2013.

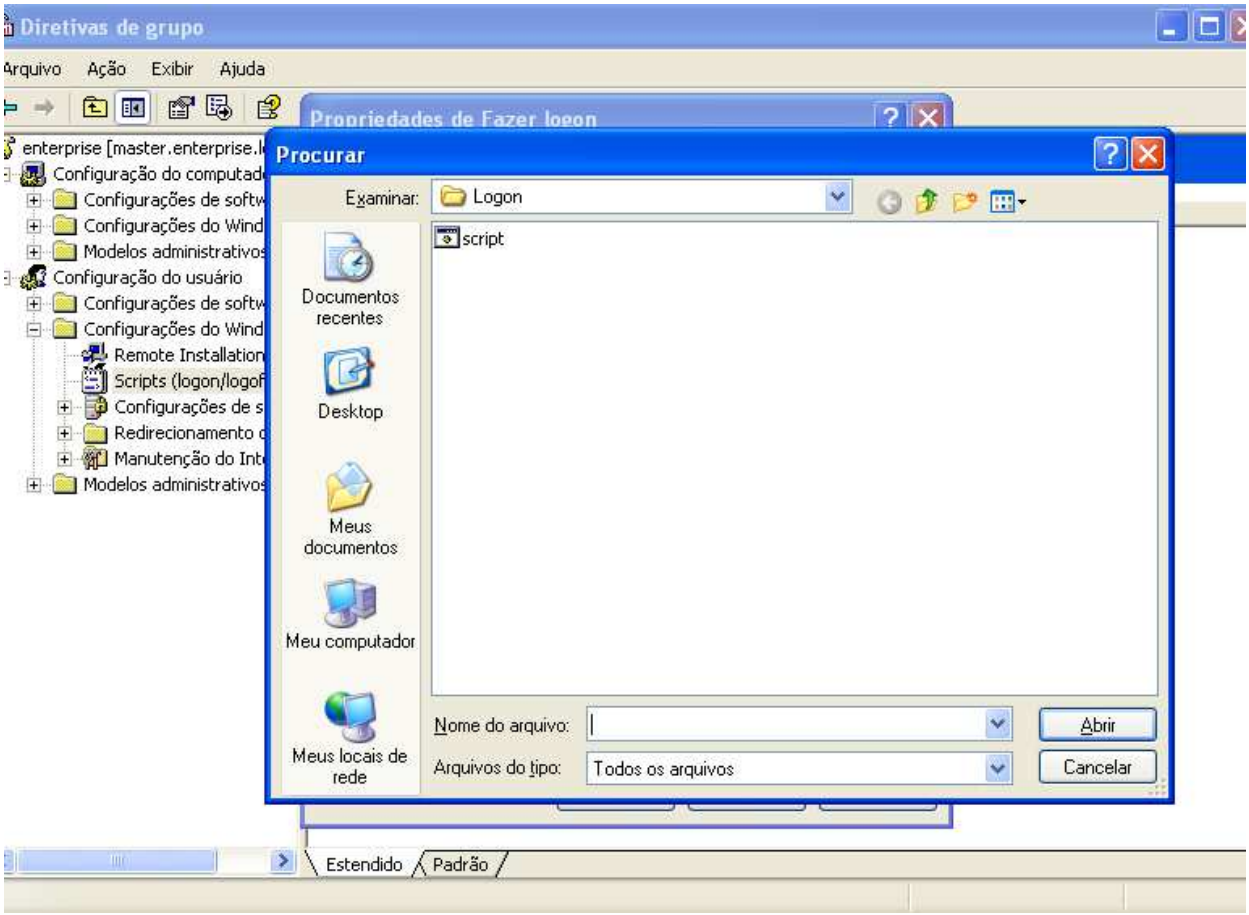
Figura 42: Propriedades da diretiva "Fazer *Logon*".



Fonte: Autoria própria, 2013.

6. Clique em adicionar e em seguida selecione o arquivo *script.bat.* Por padrão todos os *scripts* de compartilhamentos ficam em "\\master\netlogon" conforme ilustra a Figura 43.

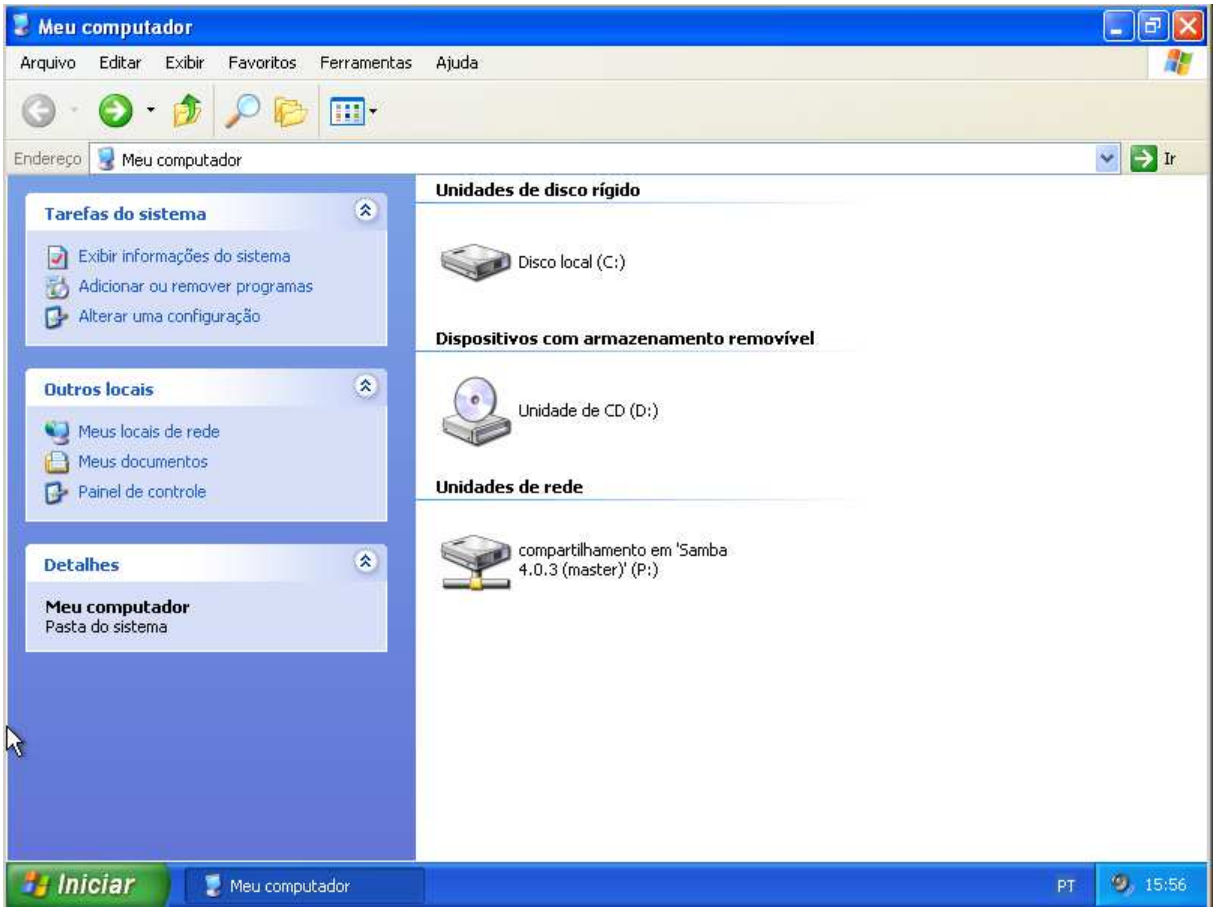
Figura 43: Script compartilhamento.



Fonte: Autoria própria, 2013.

7. Após a criação do GPO de mapeamento, toda vez que o usuário efetuar o *login* no domínio, uma nova unidade de rede será mapeada automaticamente conforme ilustrado na Figura 44.

Figura 44: Mapeamento automático.



Fonte: Autoria própria, 2013.

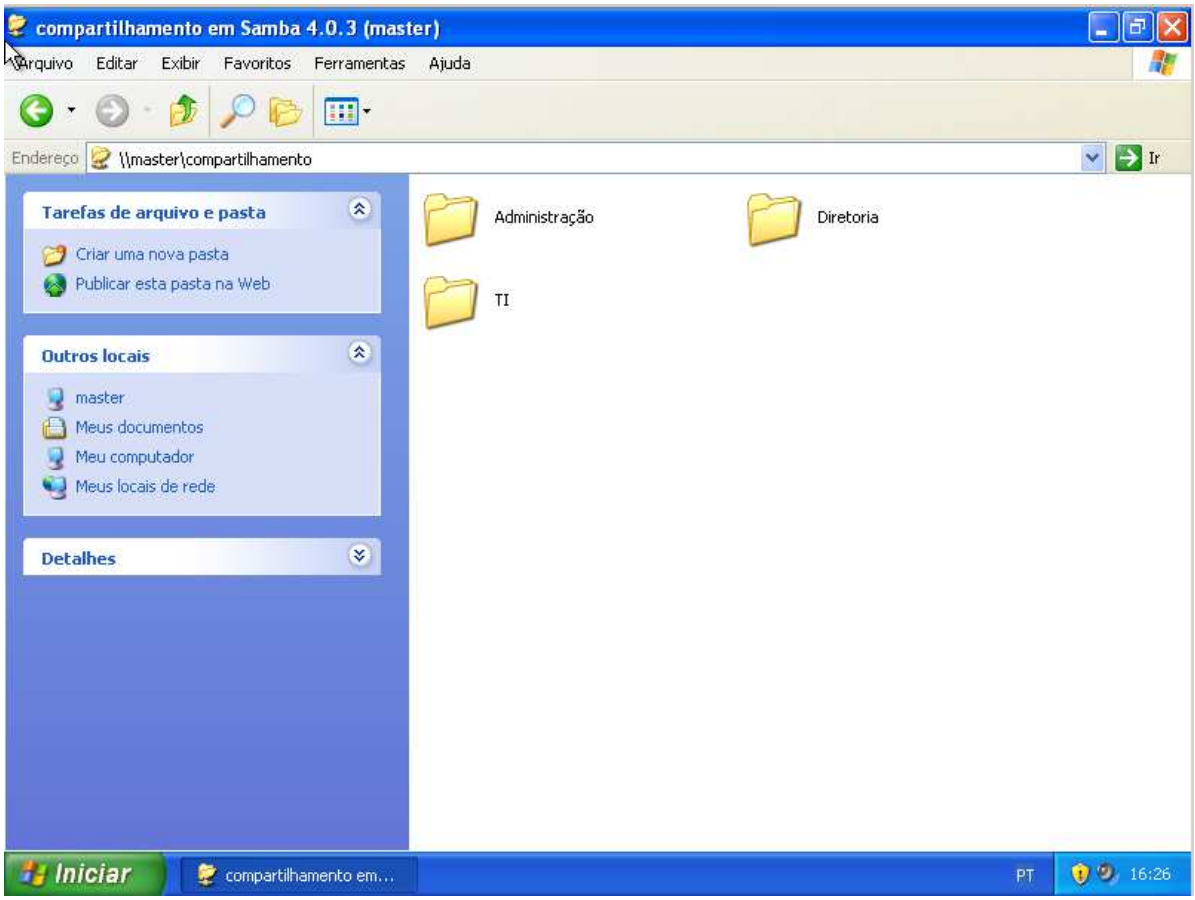
8. A titulo de exemplo, vamos criar 3 diretórios em nosso compartilhamento, 3 usuários e 3 grupos, com a finalidade de ilustrar o emprego de permissões de acesso à grupos de usuários.

   8.1. Autentique com o usuário "*administrator*", através de uma máquina *Windows*.

   8.2. Acesse o compartilhamento \\master\compartilhamento, conforme ilustrado na Figura 45.

   8.3. Crie 3 diretórios: TI, Administração e Diretoria.

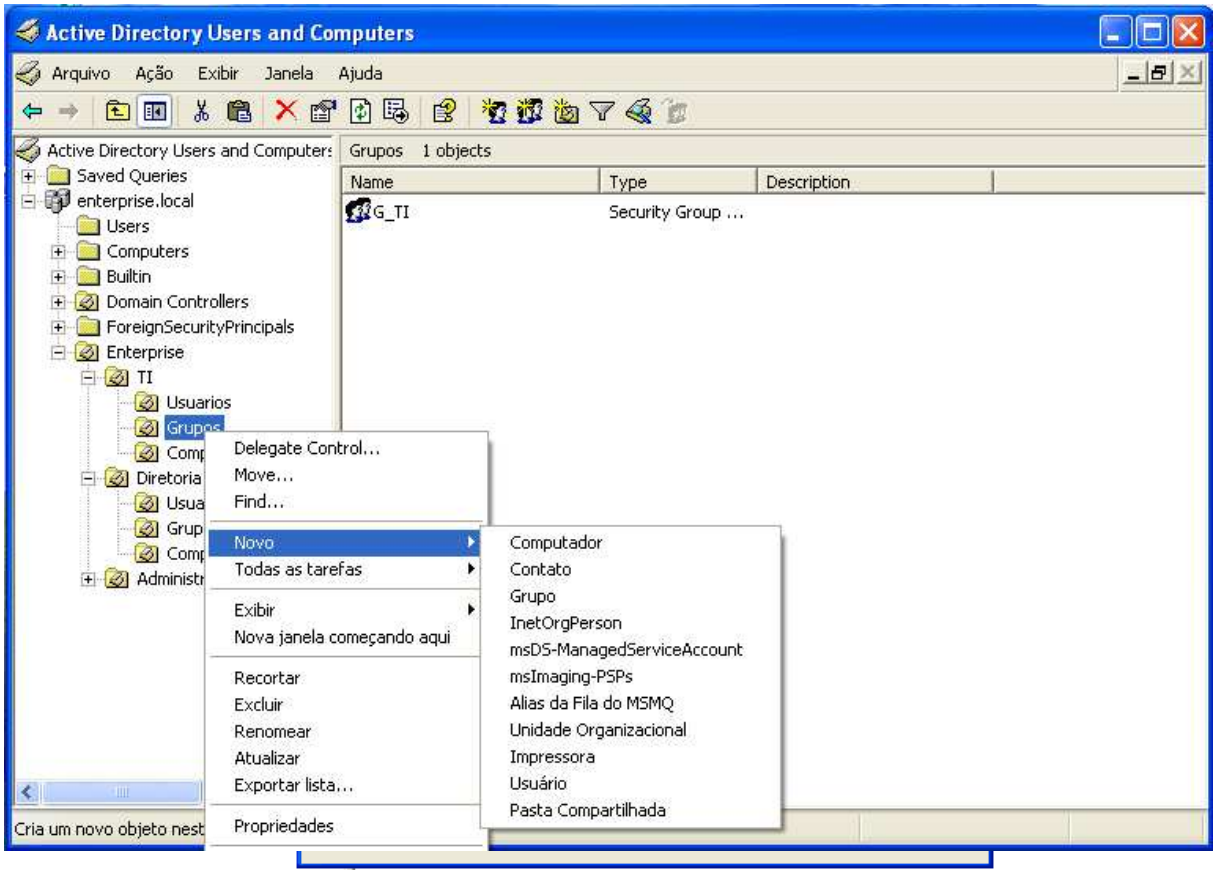
Figura 45: Acesso ao compartilhamento.



Fonte: Autoria própria, 2013.

9. Crie 3 grupos de trabalho, a saber: G_TI, G_Diretoria e G_Administração. Para criar um grupo basta acessar o "*Active Directory users and computers*", com o botão direto do *mouse* clique sobre a unidade organizacional que o usuário pertence, em seguida clique em "Novo", "Grupo", conforme ilustrado nas Figuras 47 e 48. Preencha o campo "*Group Name*" com o nome do grupo e clique em "*OK*".

Figura 46: Criando grupo de trabalho.

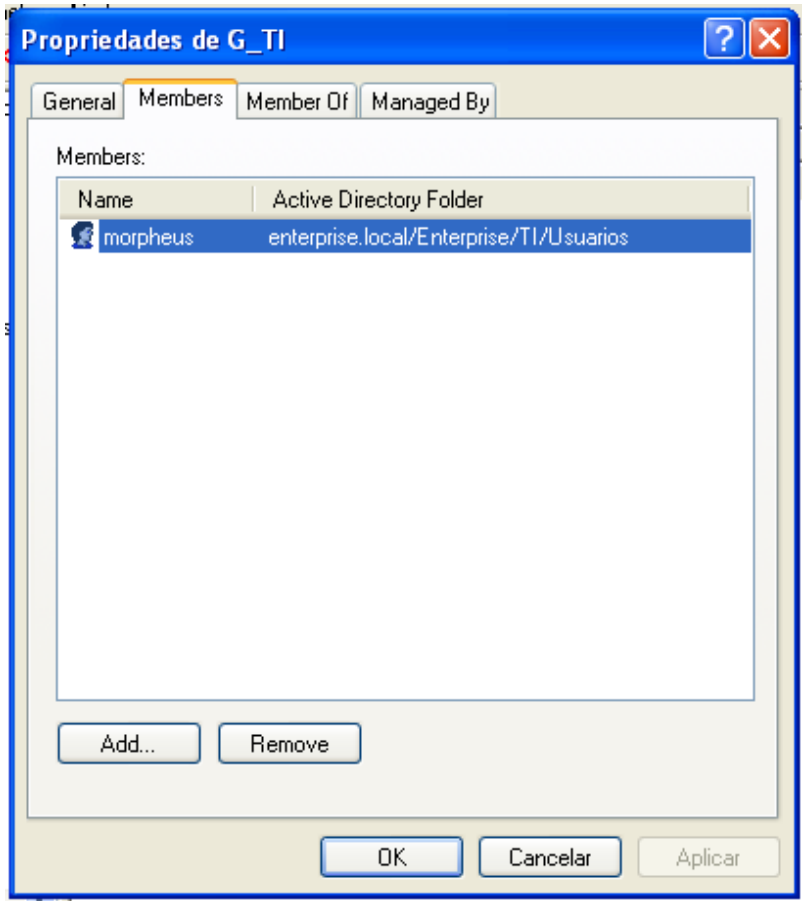


Fonte: Autoria própria, 2013.

10. Vamos adicionar o usuário Morpheus ao grupo G_TI. Clique duas vezes sobre o grupo G_TI, na Aba "*Members*", clique no botão "*Add*", e localize o usuário Morpheus, conforme ilustrado na figura 48.

11. Adicione o usuário apolo no grupo G_Diretoria e o usuário jupiter ao grupo G_Administração repetindo o passo anterior.

Figura 47: Adicionando um membro ao grupo.

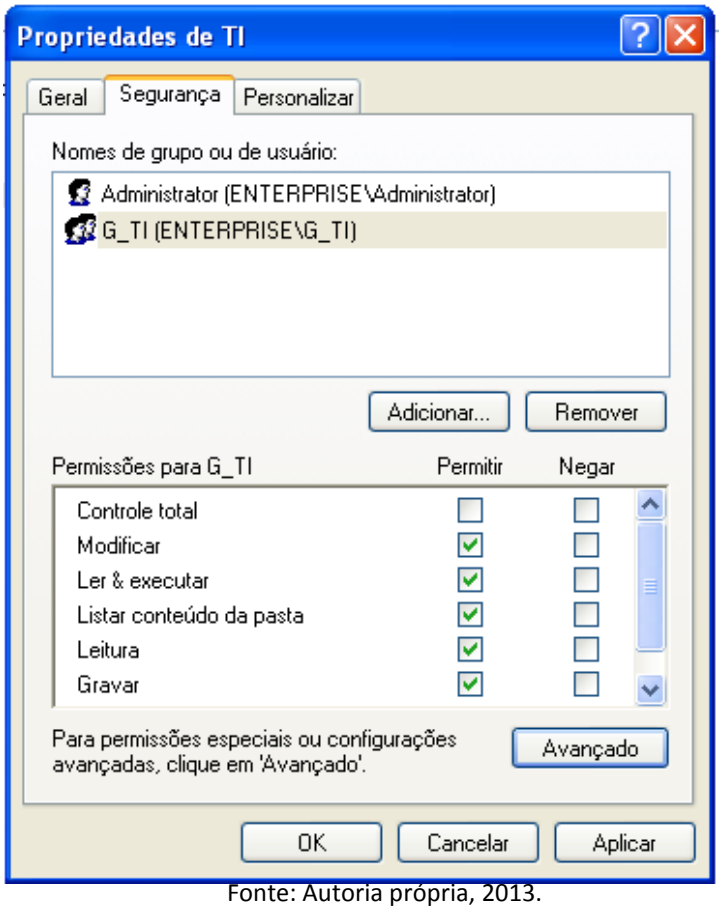


Fonte: Autoria própria, 2013.

12. Volte para o compartilhamento \\master\compartilhamento, e altere as permissões de acesso, conforme descrito a seguir:

    12.1. Clique com o botão direto do *mouse* sobre o diretório TI, localize “Propriedades”, “Segurança”, nessa aba clique em “Adicionar” e localize o grupo “G_TI”. O usuário *administrator* deve ter permissão total, e o grupo G_TI, deve ter todas as permissões, exceto “Controle total”, conforme ilustrado na Figura 48.

Figura 48: Permissão G_TI.

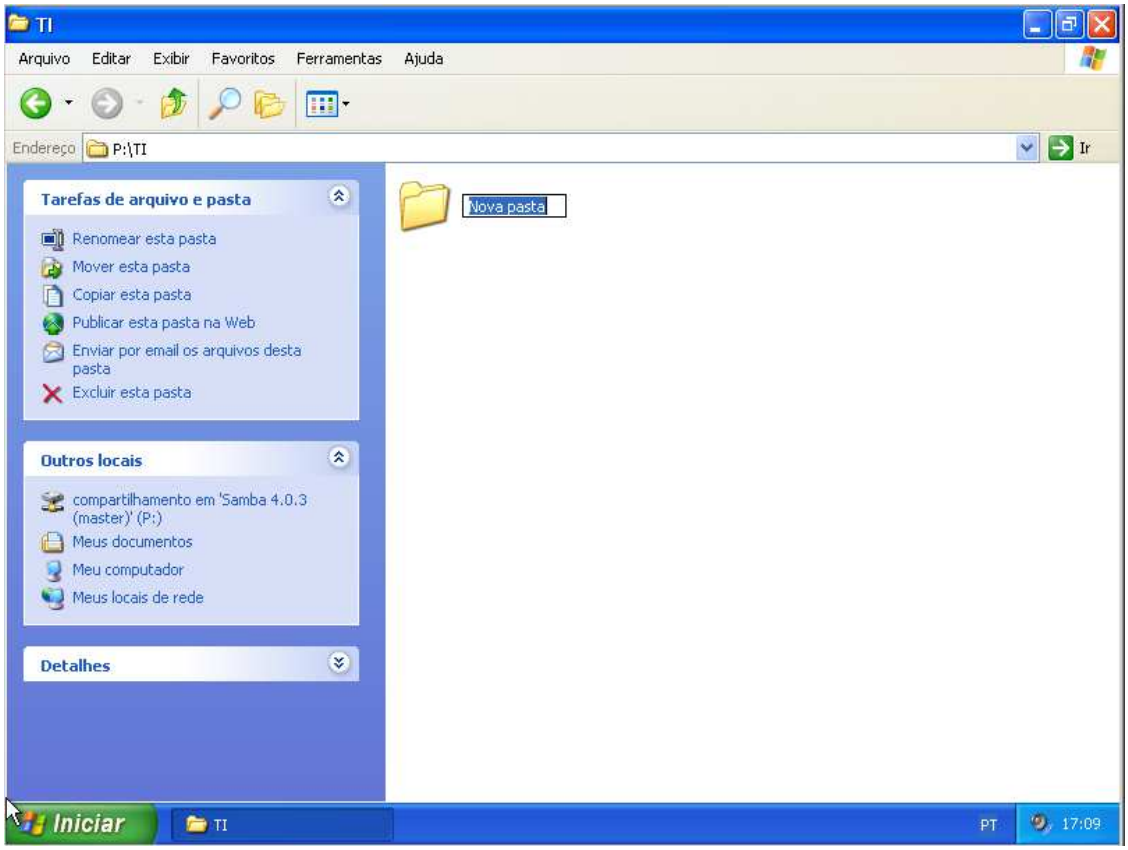


Fonte: Autoria própria, 2013.

13. O mesmo passo deve ser realizado nos demais diretórios, adicionando o acesso para o grupo pertencente à pasta.

14. Agora faça o *logoff* na estação de trabalho, e em seguida efetue o *login* novamente com o usuário “morpheus”, que deve apenas ter acesso ao diretório TI. Na Figura 49 é apresentada a criação de uma pasta na pasta TI, à qual o usuário morpheus possui acesso. Já a Figura 50 ilustra uma tentativa de acesso do usuário morpheus à pasta Administração, à qual ele não tem acesso por não fazer parte do grupo G_Administração.

Figura 49: Acessando diretório TI.



Fonte: Autoria própria, 2013.

Figura 50: Acessando o diretório Administração.

Fonte: Autoria própria, 2013.

O Samba 4 *Active Directory* nos permite gerenciar todo o domínio “enterprise.local”, através de sua ferramenta administrativa. Esse gerenciamento também é possível via linha de comando para, criar ou apagar usuários, grupos e aplicar permissões, como sempre foi feito nas versões anteriores do Samba. No entanto, para o gerenciamento e aplicações dos GPOs ainda é necessário à utilização das ferramentas da *Microsoft* instaladas numa estação de trabalho *Windows*.

4 CONSIDERAÇÕES

Após anos de desenvolvimento, o Samba 4 tornou-se uma alternativa viável, confiável e segura para a implantação de um *Active Directory*. Embora sua instalação exija conhecimentos relativamente avançados em Linux, por necessitar instalação a partir do código fonte, isto deve melhorar quando as distribuições Linux passarem a fornecer pacotes do Samba 4 personalizados e pré-configurados.

Em nossos testes, o Samba 4 mostrou-se muito eficiente em relação ao gerenciamento de contas de usuários, grupos, permissões, criação de GPOs etc. Desta forma, podemos concluir que o Samba 4 atendeu a todas expectativas propostas no estudo de caso.

Embora ainda não exista uma ferramenta desenvolvida para Linux para administração do Samba 4, a ferramenta de administração *Microsoft* é totalmente compatível com ele.

Para administradores de redes, acostumados com os ambientes *Active Directory* da *Microsoft*, não haverá dificuldade alguma em administrar um ambiente com Samba 4. Sua administração mostrou-se muito parecida como a de um *Microsoft Windows Server 2003*.

Além disso, deve-se considerar também a questão do custo de implantação de uma solução de *Active Directory* com o Samba 4: não há custo relacionado a licenças, já que o Samba 4 é um *software* gratuito e de código aberto. Talvez seja necessário contratar uma consultoria especializada, para que seja feita a implantação e manutenção do Samba 4 *Active Directory,* caso não haja profissionais capacitados dentro da empresa.

5 REFERÊNCIAS

BANIN. G. **Conheça o Kerberos, o cão de guarda.** Ano: 2010. Disponível em http://blogs.technet.com/b/gbanin/archive/2010/11/03/conhe-231-a-o-kerberos-o-c-227-o-de-guarda.aspx Acesso em: 23 out. 2013.

BRANDÃO, R. **Introdução a Group Policy (GPO).** Ano: 2013 Disponíveis em http://technet.microsoft.com/pt-br/library/cc668545.aspx Acesso em: 17 set. 2013.

LOSANO, M. **Introdução ao Active Directory.** Ano: 2003. Disponível em http://technet.microsoft.com/pt-br/library/cc668412.aspx Acesso em: 11 set. 2013.

MAZIOLI, G. S. **Guia Foca GNU/LINUX.** Ano: 2010. Disponível em http://www.guiafoca.org/?page_id=242 Acesso em: 02 out. 2013. 524p.

MICROSOFT. **Nomes de domínios DNS.** Ano 2003. Disponível em http://technet.microsoft.com/pt-br/library/cc737203(v=ws.10).aspx Acesso em: 23 out. 2013.

MICROSOFT. **Configuring and Troubloshooting Windows Server 2008 Active Directory Domain Services. Volume 1.** Brazil: Cargraphics Gráfica e Editora Ltda, 2011. 14-66p.

MICROSOFT. **Controladores de domínio.** Ano: 2003. Disponível em http://technet.microsoft.com/pt-br/library/cc759623(v=ws.10).aspx Acesso em: 27 set. 2013.

MICROSOFT. **Fundamentals of Windows Server 2008 Active Directory.** Brazil. Cargraphics Gráfica e Editora Ltda, 2008. 9-39p.

MICROSOFT. **Understanding Active Directory Domain Services Integration.** Ano: 2008. Disponível em http://technet.microsoft.com/en-us/library/cc726034.aspx Acesso em: 03 out. 2013.

MIT. **Kerberos: The Network Authentication Protocol.** Ano: 2013. Disponível em http://web.mit.edu/kerberos/#what_is Acesso em: 23 out. 2013.

MORIMOTO, E. C. **A origem do Samba.** Ano: 2008. Disponível em http://www.hardware.com.br/artigos/origem-samba/ Acesso em: 15 out. 2013.

MORIMOTO, E. C. **Entendendo o DNS e o registro de domínios.** Ano: 2008**.** Disponível em http://www.hardware.com.br/artigos/dns-registro/ Acesso em: 27 set. 2013.

MORIMOTO, E. C. **Redes e Servidores Linux, 2ed.** Ano: 2006 . Disponível em http://www.hardware.com.br/livros/linux-redes/introducao.html Acesso em: 02 out. 2013.

NTP. **O NTP.** Ano: 2013. Disponível em: http://www.ntp.br/NTP/MenuNTPNtp#O_Funcionamento_do_NTP Acesso em: 11 out. 2013.

SAMBA. **Samba Team Releases Samba 4.0.** Ano: 2013. Disponível em https://www.samba.org/samba/news/releases/4.0.0.html Acesso em: 08 out. 2013.

SEGUIS, S. **Microsoft Windows Server 2008 Administration.** New York: McGraw Hill, 2008. 514p.