UNASP

CENTRO UNIVERSITÁRIO ADVENTISTA DE SÃO PAULO

CAMPUS SÃO PAULO

CURSO DE CIÊNCIA DA COMPUTAÇÃO

FLÁVIO BURGARDT

INFRAESTRUTURA COM SAMBA 4

Trabalho de conclusão de curso apresentado ao Centro Universitário Adventista para obtenção do título de Bacharel em Ciência da Computação

São Paulo, SP, Junho de 2010.

FLAVIO BURGARDT

INFRAESTRUTURA COM SAMBA 4

Trabalho de conclusão de curso apresentado ao Centro Universitário Adventista para obtenção do título de Bacharel em Ciência da Computação

Área de Concentração
Ciência da Computação

Orientador:
Prof. MSc. Clodonil Honório Trigo

São Paulo, SP, Junho de 2010.

Dedico este trabalho à comunidade de software livre.

AGRADECIMENTOS

Agradeço a Deus por tudo. Agradeço também ao professor Clodonil por sempre ter paciência desde os primeiros semestres, o que me motivou a continuar estudando software livre e resultou neste trabalho.

RESUMO

O Active Directory trata-se de um serviço de diretório proprietário desenvolvido pela Microsoft no qual é possível gerenciar recursos de uma rede pertencente a um domínio. Domínio é uma estrutura lógica onde são armazenadas informações e recursos pertencentes a ele. Ainda não existe uma alternativa ao Active Directory, exceto a que está em desenvolvimento no projeto Samba 4, serviço de compartilhamento de arquivos da plataforma Linux. O nome samba foi dado por seu criador, o australiano Andrew Tridgell, baseado na sigla SMB, que era o protocolo utilizado para compartilhamento de arquivos em servidores Microsoft. Tridgell desenvolveu o Samba porque precisava utilizar um compartilhamento UNIX na sua máquina que utilizava o sistema DOS, mas não tinha a intenção de desenvolver o Samba. Anos depois, Tridgell descobriu o poder do que tinha feito, e aliado a documentação do SMB, o desenvolvimento do Samba pôde dar um salto muito grande. Desta forma, o objetivo do presente trabalho é pesquisar esta alternativa e comparar o serviço de diretórios da Microsoft com o serviço de diretórios desenvolvido em Linux. Trata-se do estudo dos protocolos envolvidos na construção do Active Directory, tendo como base principal os protocolos LDAP, DNS, Kerberos, SMB/CIFS, NTP, RCP e implementação no Samba 4. Embora a implementação do serviço de diretório para o Samba seja uma novidade, este servidor é muito utilizado para compartilhar dados entre redes Microsoft e Linux e por sua estabilidade e segurança. Mesmo com o Samba 4 ainda estando na versão de desenvolvimento, ele mostrou uma boa integração com o Active Directory e também poderá ser uma alternativa ao serviço de diretórios da Microsoft. Com o Samba 4 será possível criar domínios e gerenciar recursos, assim como no Active Directory, e também fazer integração com domínios Microsoft, além de herdar todas as características de suas versões anteriores.

ABSTRACT

Active Directory is about a directory service proprietor developed for the Microsoft in which it is possible to manage resources of a pertaining net to a domain. Domain is a logical structure where pertaining information and resources are stored it. Not yet an alternative to Active Directory exists, except that it is in development in the project Samba 4, service of sharing of archives of the Linux platform. The name samba was given by its creator, the Australian Andrew Tridgell, based on acronym SMB, that was the protocol used for sharing of archives in Microsoft servers. Tridgell developed the Samba because it needed to use an UNIX sharing in its machine that used the system DOS, but did not have the intention to develop the Samba. Years later, Tridgell he discovered the power of what he had fact, and ally the documentation of the SMB, the development of the Samba could give a very great jump. In such a way, the objective of the present work is to search this alternative and to compare the service of directories of Microsoft with the service of directories developed in Linux. One is about the study of the involved protocols in the construction of Active Directory, having as main base protocols LDAP, DNS, Kerberos, SMB/CIFS, NTP, RCP and implementation in Samba 4. Although the implementation of the service of directory for the Samba is a newness, this server is very used to share given between nets Microsoft and Linux and for its stability and security. Exactly with Samba 4 still being in the development version, it he showed a good integration with Active Directory and also he could be an alternative to the service of directories of Microsoft. With Samba 4 he will be possible to create domains and to manage resources, as well as in Active Directory, and also to make integration with domains Microsoft, beyond inheriting all the characteristics of its previous versions.

SUMÁRIO

Lista de Figuras

Lista de Tabelas

Lista de Abreviaturas

LDAP	*Lightweight Directory Access Protocol*
CTDB	*Cluster Trivial Database*
DC	*Domain Controller*
DHCP	*Dynamic Host Configuration Protocol*
DNS	*Domain Name System*
GPO	*Group Policy*
IIS	*Internet Information Services*
ISA	*Internet Security and Acceleration*
KDC	*Key Distribution Center*
MIT	*Massachusetts Institute of Technology*
MTA	*Mail Transfer Agent*
NTP	*Time Protocol*
PDC	*Primary Domain Controller*
SMB/CIFS	*Server Message Block/Common Internet File System*
SWAT	*Samba Web Administration Tool*
TGS	*Ticket Granting Server*
TGT	*Ticket Granting Ticket*

1 Introdução

O Active Directory é um serviço de diretórios desenvolvido pela gigante empresa de softwares Microsoft, utilizado para armazenar várias informações, como contas de usuários e contas de máquinas, centralizar e facilitar a administração de redes de computadores. Essa centralização é melhor definida como domínio. O Active Directory é uma implementação do protocolo LDAP, principal protocolo do deste serviço de diretórios, utilizado para o acesso rápido às informações de diretórios.

Além da administração centralizada disponibilizada pelo Microsoft Active Directory, serviços como compartilhamento de arquivos e acesso controlado à internet podem ser integrados a este serviço de diretório, tornando uma ferramenta quase que indispensável para administração de redes, independente do seu tamanho.

O Microsoft Active Directory é um sistema pago e com um custo relativamente alto, além de ser a única opção disponível neste seguimento e também oferecer suporte apenas para sistemas Microsoft. Porém, a versão 4 do Samba, serviço de compartilhamento de arquivos desenvolvido para Linux, também implementa um serviço de diretórios através do protocolo LDAP, que vai muito além do serviço de compartilhamento de arquivos.

Embora o Samba 4 esteja em sua versão de desenvolvimento, sendo sua estrutura baseada nos mesmo protocolos envolvidos no Microsoft Active Directory, este sistema poderá substituir o serviço de diretórios da Microsoft, o que incentivou o estudo deste sistema. Desta forma o objetivo principal será estudar o principais protocolos envolvidos no Microsoft Active Directory e a implementação o Samba 4, visando algumas de suas principais características e suas opções de integração com serviços de rede.

As implementações realizadas mostram recursos como autenticação de clientes Microsoft através do Samba 4, além de integrar a outros serviços, como compartilhamento de arquivos e e-mail.

2 Objetivos

2.1 Geral

Instalar e configurar o serviço de diretório do Samba 4 e comparar as opções oferecidas com as equivalentes no Microsoft Active Directory.

2.2 Específico

- Instalar o Samba 4 e o seu serviço de diretórios.
- Ingressar máquinas Windows XP Pro no domínio do Samba 4.
- Acessar o serviço de diretórios do Samba 4.
- Criação de usuários e grupos no domínio do Samba 4.
- Configuração de Políticas de Grupo para usuários do domínio do Samba 4.
- Configuração do serviço de compartilhamento de arquivos com autenticação no Samba 4.
- Configuração do serviço de Proxy no Linux para autenticação no Samba 4.
- Configuração do serviço de e-mail no Linux para autenticação no Samba 4.
- Configuração do serviço Web no Linux para autenticação no Samba 4.

3 Justificativa

Hoje em dia o único serviço de diretórios para controladores de domínio é o Active Directory de propriedade da Microsoft. A implementação do protocolo LDAP no Samba 4 para a criação do serviços de diretório, dará uma alternativa a este serviço de diretórios proprietário.

O custo pode ser considerado uma primeira vantagem. Ao passo que o Microsoft Active Directory tem um custo elevado de licenciamento, o serviço de diretórios para Linux, implementado no Samba 4, deverá ser totalmente gratuito.

A filosofia de software livre também pode ser considerada uma vantagem. Assim como em distribuições Linux e softwares voltados para estes sistemas, existem programadores espalhados pelo mudo todo que ajudam no desenvolvimento do Samba 4, que em breve poderá se tornar um concorrente à altura do Microsoft Active Directory.

Os sistemas desenvolvidos em Linux proporcionam também liberdade para ser alterados na medida de nossas necessidades, o que fatalmente irá contribuir para que o Samba 4 se torne cada vez melhor e seguro.

4 Referencial Teórico

4.1 Diretórios

De uma maneira geral, os diretórios servem para agilizar o processo de pesquisa de informações. Informações estas que podem ser dados de usuários ou informações sobre recursos de rede em geral. Segundo Trigo (2007), um diretório é um serviço de armazenamento hierárquico de informações otimizado para leitura, onde a pesquisa e busca destas informações se torna mais fácil e ágil e a inserção de itens no diretório ocorre de maneira ocasional.

Em outras palavras, diretório é um banco de dados que armazena informações as quais são encontradas mais rapidamente devido à sua estrutura hierárquica. Porém, no diretório não são realizadas operações complexas como em um banco de dados e as informações nele contidas são mais descritivas (detalhadas) do que um banco de dados comum. No diretório estas informações são baseadas em atributos e são organizadas em estrutura de árvores, e não em tabelas como em um banco de dados tradicional. (TRIGO, 2007)

A figura 1 mostra a estrutura de um diretório:

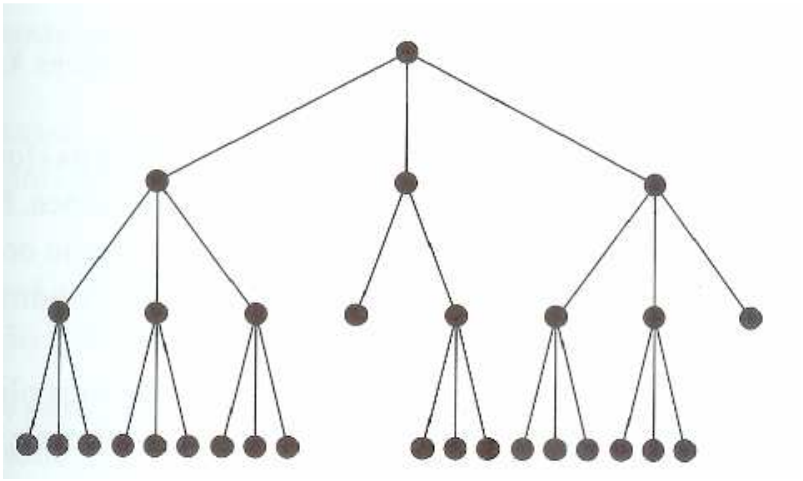


figura 1 - representação de um diretório (SCRIMGER.R. et al, 2002)

Os diretórios possuem nós, que são representados na figura 1 e são organizados em níveis. O nó no nível mais alto é a raiz. Os nós de nível mais baixo podem ou não conter outros nós, chamados respectivamente de nós-filhos e folhas. Desta forma é possível centralizar, manter e recuperar informações de maneira eficiente e padronizada.

Os diretórios são preparados para dar uma resposta rápida a um grande volume de consultas ou operações de busca (TRIGO,2007)

O DNS (*Domain Name System*), serviço de resolução de nomes utilizado na Internet, utiliza a estrutura de diretórios. (SCRIMGER.R. *et al.*, 2002)

4.2 Introdução ao Active Directory

Active Directory é um serviço de diretório da Microsoft, desenvolvido através da implementação do protocolo LDAP (*Lightweight Directory Access Protocol*), que é utilizado para acessar de maneira eficiente as informações contidas no diretório. Está presente desde a versão Windows Server 2000 e está disponível apenas para versões *server*, que são sistemas operacionais para servidores Microsoft. (MINASI *et al*, 2000)

Basicamente, o Active Directory é um banco de dados que armazena informações de usuários, máquinas e grande parte de informações administrativas. A base de dados do Microsoft Active Directory chama-se NTDS.DIT e armazena uma variedade muito ampla de informações de usuários e recursos. Esta base de dados é organizada em uma estrutura de diretórios, sendo otimizada para leitura, tendo em vista que bancos de dados de usuários são mais consultados do que gravados. (MINASI. M *et al*, 2000)

Um serviço de diretórios é um serviço de rede que identifica e mantém informações sobre todos os recursos disponíveis na rede. Estes recursos são chamados de objetos, que podem ser contas de usuários e computadores, grupos de usuários e grupos de computadores, políticas de segurança, impressoras, outros domínios, senhas, entre outros. Todos os objetos possuem propriedades que são chamadas de atributos. Todas estas informações dos objetos são armazenados na base de dados NTDS.dit. O Active Directory faz uso de *schemas*, que são arquivos que contém regras de como as informações são organizadas dentro da base LDAP, sendo o *Schema Master* o principal *schema* do Microsoft Active Directory. (MICROSOFT-2, 2009); (TRIGO, 2007).

No Active Directory, além de fornecer o serviço de diretórios, existem ferramentas que complementam a implementação do protocolo LDAP. Serviços de rede como o DHCP (*Dynamic Host Configuration Protocol*) e DNS (*Domain Name System*), são utilizados respectivamente para gerenciar endereços de rede (IPs) e resolução de endereços de rede em nomes de máquinas e servidores. Além de protocolos fundamentais como o Kerberos, o qual se trata de um protocolo de autenticação que provê forte segurança. (MINASI. M *et al*, 2000)

O LDAP por ser largamente utilizado em outras plataformas, é utilizado como protocolo de acesso leve ao diretório, garantindo assim conectividade padronizada. O Active Directory faz uso de uma combinação do protocolo DNS do protocolo LDAP para encontrar e utilizar recursos na rede. (SCRIMGER.R. et al, 2002)

Além de prover um serviço de autenticação centralizada para contas de usuários, os objetos criados podem ser gerenciados para obedecer a políticas específicas ou globais, obrigatórias ou flexíveis.

A figura 2 mostra o Active Directory em um servidor com Microsoft Windows 2003 Server:

figura 2 – Microsoft Active Directory

O Active Directory possui *schemas*, necessários para definir os atributos dos objetos a ele pertencentes como nome, senha e e-mail. O *schema master* é o principal schema do Active Directory (MICROSOFT-3, 2009). Os Schemas não são requeridos pelo Active Directory em si, mas pelo protocolo LDAP.

O Active Directory é totalmente escalonável. Sendo assim pode ser organizado para suportar estruturas relativamente pequenas até grandes configurações. Essa estrutura lógica se dá através de Domínios, Árvores e Florestas, Unidades Organizacionais, e Grupos. (LOSANO.M, 2009)

Domínio é um agrupamento lógico de contas e recursos os quais compartilham políticas de segurança, serviços e diretórios. (MINASI. M. *et a.l*, 2000)

Em outras palavras, domínio são grupos de servidores, computadores e recursos e as informações sobre eles armazenadas dentro do diretório. Cada recurso de uma rede (impressoras, usuários, máquinas) faz parte de um único domínio apenas e cada domínio possui suas próprias políticas de segurança. As contas administrativas têm livre acesso a qualquer configuração do domínio, mas não de qualquer domínio, apenas dentro do seu próprio (MINASI. M. *et al.*, 2000).

Existem computadores configurados dentro do domínio, denominados Controladores de Domínio, os quais gerenciam o domínio.

Graças à administração centralizada proporcionada pelo Active Directory, os usuários podem usufruir dos recursos do domínio a partir de qualquer máquina na qual façam o login.

Árvores e Florestas de Domínios são o agrupamento de um ou mais domínios, de maneira hierárquica que compartilham o mesmo espaço de nomes.

A figura 3 ilustra uma árvore de domínio.

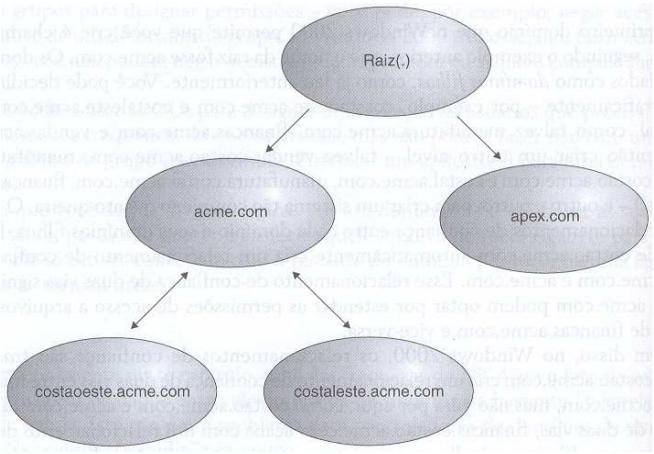


figura 3 - Árvores de domínio (MINASI. M. et al., 2000)

Abaixo do domínio raiz estão os subdomínios. Eles geralmente são criados quando há necessidade de delegar administração. Os recursos dos domínios são disponibilizados e transferidos para os demais através de relações de confiança transitiva Kerberos bidirecional, ou seja, novos domínios (domínios-filho) seguirão o caminho até o topo da hierarquia, herdando assim as suas permissões. (MINASI. M. *et al.*, 2000)

Existem também divisões feitas para delegar controles e realizar restrições a determinadas políticas de segurança. Estas divisões são denominadas Unidades Organizacionais. Com as Unidades Organizacionais é possível diminuir o número de domínios criados. Essas Unidades Organizacionais podem ser aninhadas, cada uma obedecendo a determinadas configurações Pai que são herdadas para as Unidades Organizacionais filhas, podendo estas ter suas próprias Políticas de Grupo ou *GPO - Group Policies*, que são exatamente as permissões que cada Unidade Organizacional terá. (MINASI. M. *et al.*, 2000)

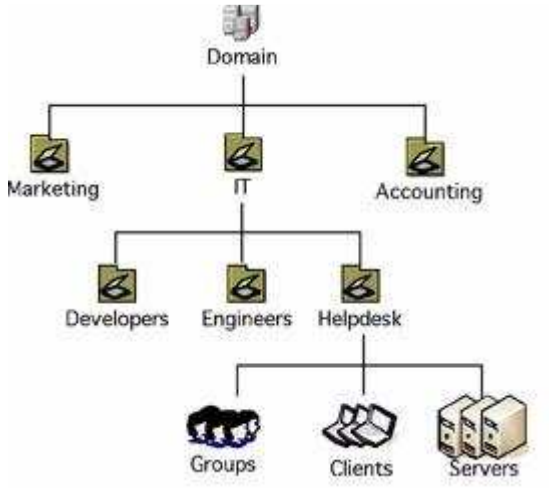


figura 4 - Unidades Organizacionais

No exemplo da figura 4, existem grupos de usuários, máquinas e servidores que pertencem à unidade organizacional HelpDesk, que é filha de IT, ou seja, herda suas políticas de segurança (GPO), que por sua vez herda da raiz do domínio.

Em resumo as Unidades Organizacionais servem para delegar tarefas administrativas sem o risco de dar permissão em todo um domínio.

É possível também a criação de Grupos, que é o simples agrupamento de objetos (usuários ou máquinas) visando uma melhor administração. (MINASI. M. *et al.*, 2000).

Em todo domínio deve existir pelo menos um controlador de domínio. Como o próprio nome diz, é ele que gerencia o domínio. Pode existir mais de um controlador de domínio, sendo o controlador primário conhecido como *PDC - Primary Domain Controller*. Os controladores de domínio compartilham a lista de usuários, grupos e políticas de segurança. Qualquer alteração feita em um controlador de domínio é replicada para todos os outros controladores do domínio. A instalação do Microsoft Active Directory é feita por utilitários amigáveis e considerada relativamente fácil. (MINASI. M. *et al*., 2000)

4.3 Protocolos Envolvidos no Active Directory

Protocolos são a maneira que os computadores utilizam para se comunicar, trocar informações. (SCRIMGER. R. *et al*, 2002)

Os principais protocolos envolvidos no Active Directory são mostrados na tabela 1 (MICROSOFT-2, 2009):

Tabela 1 - Principais protocolos envolvidos no Active Directory

Protocolo	Descrição
DNS	Protocolo responsável pela resolução de IP em nomes de máquina
LDAP	Principal protocolo utilizado para implementar o Active Directory
KERBEROS	Realizar autenticação de forma bastante segura utilizando criptografia
NTP	Protocolo utilizado para manter sincronização entre computadores
SMB/CIFS	Principal protocolo relacionado ao compartilhamento de arquivos
DHCP	Protocolo responsável pela distribuição de endereços IP

4.3.1 DNS

DNS (*Domain Name System*) é uma base de dados hierárquica e distribuída, usada para a resolução de nomes de domínios em endereços IP. É considerado como um banco de dados distribuído que converte nomes de hosts (máquinas) para endereços IP. É basicamente um mapeamento de endereços IP e seus respectivos nomes. A utilização mais comum é na internet. Todos os computadores da rede possuem um endereço IP. Os servidores DNS simplesmente transformam ou resolvem esse o número em um nome. Por exemplo, o endereço www.meudominio.com.br corresponde ao IP 10.0.0.1. (SCRIMGER.R. et al, 2002)

A resolução de nomes se dá da seguinte maneira:

- O nome do host é inserido (browser, ftp, prompt de comando, serviço);
- O sistema operacional verifica se o nome do host de destino é o mesmo configurado localmente (para agilizar o processo na pilha TCP);
- Se não houver correspondência o resolvedor (cliente) envia uma requisição ao servidor DNS que, se existir uma resposta, é enviado um número IP ao solicitante; e
- Se não houver resposta do servidor DNS, uma mensagem de erro irá ser exibida para o usuário.

A figura 5 mostra a estrutura do DNS que é baseada no conceito de espaços de nomes e árvore de domínios.

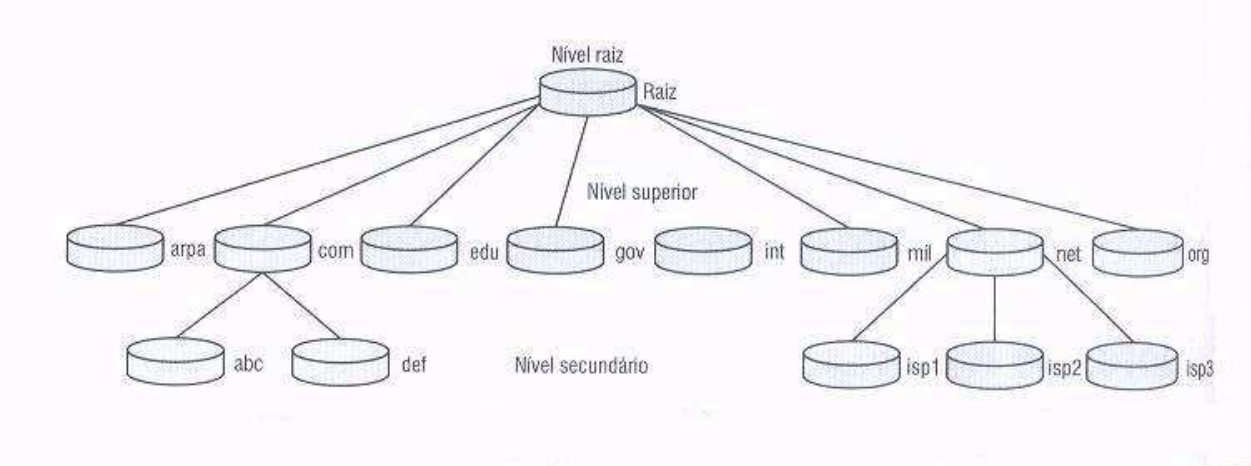


figura 5 - Estrutura hierárquica do DNS (SCRIMGER.R. et al, 2002)

O DNS composto por três elementos:

- Servidor de nome
- Resolvedor (um cliente)
- Espaço de nome

A raiz (root) é o domínio de mais alto nível, sendo representada por um ponto (.), seguido pelos domínios de níveis mais baixos (com, br, gov, org, etc.)

Na Internet, o DNS tenta retornar (resolver) um endereço tipo www.empresa.com.br em um número de IP. Se este não tiver sucesso, outros servidores DNS serão contatados num determinado espaço de tempo para efetuar a resolução do nome em endereço IP. (SCRIMGER.R. et al, 2002)

Já nas intranets os servidores DNS são utilizados para localizar recursos em geral (hosts, servidores, etc). Por exemplo, para se conectar ao endereço \\servidor01\pasta01, é feita uma consulta ao servidor DNS que retornará o endereço IP de servidor01. Se houver uma resposta com o endereço IP, a conexão é realizada com sucesso. (SCRIMGER.R. et al, 2002)

- Espaço de nome: Pode ser um espaço de nome de internet, como visto na figura 5, ou um espaço de nome interno definido conforme a necessidade.

- Servidor de nomes: É o computador possui um aplicativo do servidor DNS e que responde às solicitações dos clientes (resolvedores), retornando um nome de host ou endereço IP que estão dentro do espaço de nomes. Este servidor mantém as informações em um arquivo de zona ou na memória e também realiza tarefas de gerenciamento do banco de dados do arquivo de zona (atualizações do registro de recursos e transferência de zona).
- Resolvedores: São clientes de quem partem as solicitações para a resolução de nomes. Eles enviam ao servidor DNS as solicitações de conversão de endereços IP. Os resolvedores vão desde estações de trabalho até servidores.

4.3.2 LDAP

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

Além de oferecer acesso rápido e fácil a serviços de diretório, ele oferece suporte transparente ao TCP/IP, sendo então uma das melhores escolhas para o ambiente de internet e aceito como padrão para serviços de diretório (SCRIMGER.R. et al, 2002).

De forma resumida o LDAP é um protocolo utilizado para organizar as informações, visando à facilidade e agilidade na recuperação das mesmas. Estas informações são armazenadas em um banco de dados, mas sem especificar um banco de dados em particular. A organização é feita de forma hierárquica onde, a partir da raiz chegamos aos recursos, que podem ser computadores, servidores, usuários, etc. É uma árvore de nós, similar a forma como o DNS funciona (ERICH. S. M.).

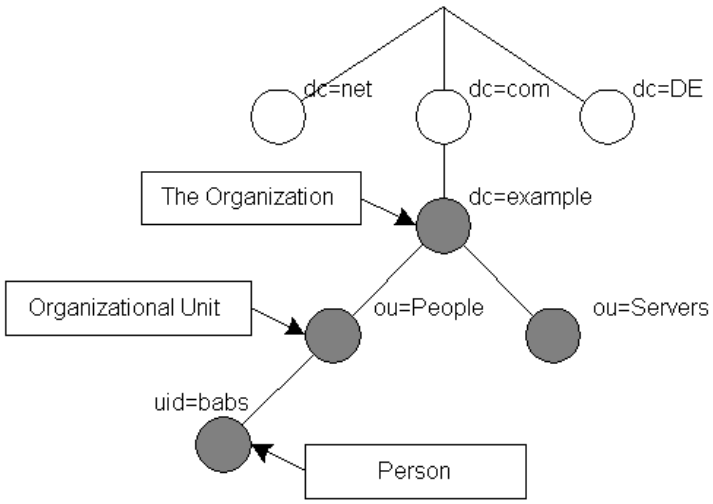


figura 6 - Estrutura do protocolo LDAP (OPENLDAP FOUNDATION, 2003)

A busca em uma estrutura em árvore inicia pela raiz e pára nas folhas (nós) onde estão as informações desejadas. Os diretórios são a raiz e os ramos e as entradas são as folhas.

As informações armazenadas na base LDAP são baseadas em entradas, que são uma coleção de atributos que formam um nome distinto único, o DN. O LDAP faz uso de mnemônimos para definir os nomes dos atributos e as entradas. (THE OPENLDAP FOUNDATION, 2003)

A tabela 2 mostra atributos de diretórios:

Tabela 2 - Atributos de diretórios

Atributo	Descrição
C	Atributo de diretório que representam países
O	Atributo de nome da empresa
Ou	Atributo de nome de departamento

A tabela 2 mostra atributos de entradas

Tabela 3 - Atributos de entradas

Atributo	Descrição
Cn	Atributo de nome
Uid	Atributo de identidade de usuário
Gn	Atributo de nome próprio de pessoas
Sn	Atributo de sobrenome de uma pessoa

As entradas só podem ser adicionadas no banco de dados se forem válidas. O que define o que é válido ou não, são os *schemas*. Schemas são arquivos de configuração que definam o tipo de informação que poderá ser armazenada no diretório e quais atributos elas irão ter (ERICH. S. M).

As entradas são definidas em classes de objetos, onde alguns atributos são obrigatórios, como *uid* (identificação do usuário) e outros opcionais, como *displayname* (nome do usuário que será exibido) definido pela classe *person.*

As informações são inseridas na base LDAP através de arquivos específicos, chamados de *ldifs*. Eles são arquivos de texto puro, que possuem os atributos de entrada. (TRIGO, 2007)

Exemplo de um arquivo ldif:

- `dn: uid=pluto,ou=info,dc=empresa,dc=br`
- `objectClass: top`
- `objectClass: person`
- `objectClass: posixAccount`
- `objectClass: inetOrgPerson`
- `cn: pluto`
- `sn: cachorro`
- `mail: pluts@terra.com.br`
- `telephonenumber: 123-45-1000`
- `uid: pluto`
- `userPassword: 21`
- `homeDirectory: /home/pluto`
- `displayName: Pluto Cachorro`
- `loginShell: /dev/null`
- `uidNumber:103`
- `gidNumber:203`

O exemplo acima trata-se de um arquivo ldif, criado em texto puro. Os atributos propriamente ditos são os nomes antes dos dois pontos. Ou seja, conforme o exemplo acima, em *ObjectClass: top*. objectClass é atributo (vem antes dos dois pontos) e top indica o nível de entrada. Já o atributo *dn* indica um nome distinto, ou um nome inequívoco e único, que neste exemplo é composto pela identificação do usuáio (*uid=pluto*), unidade organizacional (*ou=info*) e o domínio do diretório (*dc=empresa, dc=br*).

Outros atributos também podem estar presentes, como *common name (cn)* que identifica o primeiro nome do usuário, o atributo *mail* que identifica o email do usuário, e assim por diante. Os atributos indicam o tipo de informação que será armazenada na base ldap. Os arquivos *ldif* são muito sensíveis a erros, como espaços em branco no final de cada linha ou pontuação incorreta. (TRIGO, 2007)

Os *schemas* não são utilizados apenas para atributos de usuários. Podem identificar também máquinas e serviços.

Exemplos de implementações do protocolo LDAP são o OpenLDAP e o Active Directory da Microsoft.

4.3.3 Kerberos

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

Foi criado pelo MIT na década de 80 e sua versão atual é a Kerberos 5 ou Kerberos V. Abaixo algumas características da autenticação do Kerberos (CONECTIVA, 2009):

- single sing-on: A senha é solicitada para o usuário somente uma vez. Se algum outro serviço que necessite de autenticação for solicitado, a senha não precisará ser informada novamente. Por exemplo, se for solicitada autenticação para o serviço de e-mail;
- senha criptografada: A senha sempre é codificada antes de ser transmitida pela rede;
- autenticação centralizada: Uma mesma senha pode ser utilizada para vários serviços tendo em vista a centralização na base de dados, o que facilita a memorização e definição de políticas de segurança globais;
- Redundância: A autenticação é feita utilizando-se mais de uma fonte.
- múltiplos domínios: Usuários de domínios diferentes podem ser autenticar entre si. Ex: empresa filial realizando autenticação na matriz;
- fácil configuração do cliente: A configuração é inserida no DNS, fornecendo na grande maioria a estrutura necessária para a utilização do Kerberos; e
- Padrão: Por ser padronizado, aplicações diferentes podem conversar, como Windows 2003 e o Linux, tendo em vista que ambos usam Kerberos, onde máquinas Windows podem obter tickets de máquinas Linux ou vice-versa (CONECTIVA, 2009).

O Kerberos não autentica o *host* no servidor, apenas a aplicação que oferece o serviço. Ele trabalha com *tickets*, servindo para provar a autenticidade de um usuário e garantir o acesso aos serviços e aplicações. (CONECTIVA, 2009).

Quando um usuário entra com as informações de *login*, considerando que seja um usuário cadastrado no KDC (é o servidor Kerberos), os dados são enviados para o servidor

Kerberos que recebe as informações e as confere com as que estão cadastradas no banco de dados. Estas informações são criptografadas com a própria senha do usuário e enviadas de volta para ele. Este é o ticket TGT (*Ticket-Grant-Ticket*). Se as informações do ticket TGT puderem ser descriptografadas, então o usuário é quem diz ser. O TGT é armazenado na máquina e, por segurança, tem um tempo de vida útil para o caso de ser interceptado na rede. (CONECTIVA, 2009)

O TGT servirá para solicitar serviços ao servidor. Quando um cliente solicita um serviço, ele utiliza o TGT para isso. Desta forma não será necessário fornecer os dados de login novamente, tendo em vista que o TGT foi criptografado com a senha do usuário e se foi descriptografado, significa que a senha fornecida no login confere com a do banco de dados do Kerberos (FILHO. M. M. C, 2009).

Desta forma, quando um serviço é solicitado, o cliente apresenta o TGT. O servidor Kerberos faz as verificações necessárias e responde com outro ticket, o TGS (*Ticket-Grant-Service*), que é o ticket necessário para solicitar serviços. O cliente então apresenta o novo ticket (TGS) para o servidor que pretende utilizar o serviço (por exemplo, um servidor de e-mail). (CONECTIVA, 2009).

É importante lembrar que para cada serviço utilizado pelo cliente, deverá ser gerado um novo ticket TGS, ou seja, se o cliente requisitar um serviço ao servidor web, o cliente enviará novamente o TGT para o Kerberos que responderá com outro ticket TGS específico para o serviço solicitado, no caso o serviço web. (FILHO. M. M. C, 2009)

A figura 7 ilustra o processo de autenticação pelo Kerberos.

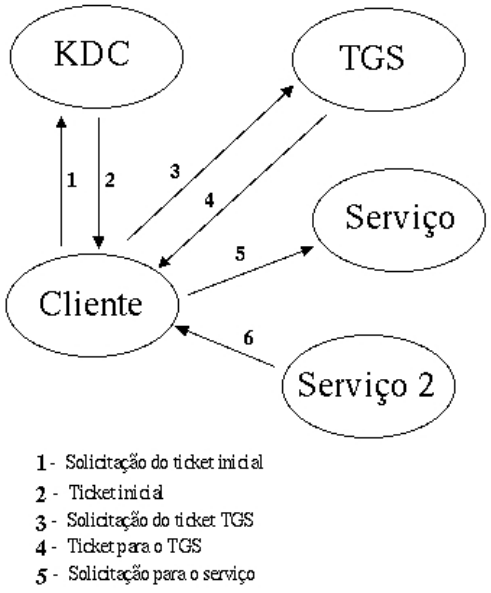


figura 7 - Autenticação Kerberos (CONECTIVA, 2009)

4.3.4 NTP

NTP (*Network Time Protocol*) é usado para sincronizar relógios de computadores na rede local ou na internet (RNP, 2009).

O não sincronismo dos relógios de uma rede pode causar problemas de administração em:

- servidores de controle de versão
- sistemas de backup
- transações de banco de dados
- erros no Active Directory
- análise de logs de vários servidores
- servidores de e-mail

O SNTP é uma adaptação do NTP feita pela Microsoft. Este protocolo é utilizado para manter o sincronismo entre as estações de trabalho e o servidor, onde a exatidão do NTP não é tão exigida (MICROSOFT-1, 2009).

4.3.5 SMB/CIFS

O protocolo SMB/CIFS (*Server Message Block / Common Internet File System*) é utilizado para realizar o compartilhamento de diretórios, arquivos e impressoras. É uma atualização do protocolo SMB, executado sobre NetBIOS originalmente desenvolvido IBM (UFRJ, 2009).

Desde 1996 foi reescrito pela Microsoft (baseado no original SMB) e hoje é conhecido apenas como CIFS (executado sobre TCP), ao passo que o termo SMB é usado quando referenciamos o compartilhamento de arquivos em si. O protocolo permite que o cliente manipule arquivos em rede, como se estivesse utilizando localmente. Qualquer ação (escrita, leitura, exclusão) é permitida, sendo que a única diferença é que o arquivo não está na máquina local, mas sim em um servidor. (UFRJ, 2009)

4.3.6 DHCP

O DHCP (*Dynamic Host Configuration Protocol*) permite que um dispositivo obtenha um endereço IP dinamicamente além de informações de configuração como, endereço de *gateway* e servidores DNS. Endereços IP definidos estaticamente têm um prazo de utilização. O DHCP gerencia a utilização destes endereços, liberando-os quando necessário. Este processo é chamado de concessão. (SCRIMGER.R. et al, 2002).

Um servidor DHCP mantém uma faixa de endereços IP válidos que podem ser distribuídos. Esta faixa de endereços é conhecida como *pool* e recebe o nome de escopo. Quando um cliente inicializa, ele emite uma mensagem de descobrimento na rede chamada de *DHCPDISCOVER*. Isso é conhecido como estado de inicialização.

O servidor DHCP recebe a mensagem de descobrimento e emite uma mensagem de oferecimento, chamada de DHCPOFFER. Esta mensagem de oferecimento contém um endereço IP válido para a rede e também informações relacionadas à configuração (existindo mais servidores DHCP na rede, o cliente entra no estado de seleção, para selecionar uma oferta). (SCRIMGER.R. *et al*, 2002)

O cliente entra então no estado de solicitação e envia uma mensagem de solicitação (DHCPREQUEST), solicitando a configuração oferecida pelo servidor. O servidor envia uma mensagem de reconhecimento positivo (DHCPPACK), respondendo à mensagem de solicitação enviada pelo cliente. Além do endereço IP e configurações, esta mensagem contém as informação da concessão. (SCRIMGER.R. *et al*, 2002).

Quando o cliente recebe o reconhecimento, ele entra no estado limite, onde utiliza *timers* controlando o vencimento, a renovação e a revinculação da concessão. Em geral, quando 50% do tempo de concessão é ultrapassado ou quando a concessão expira, o cliente emite uma mensagem DHCPREQUEST ao servidor que concedeu o endereço. (SCRIMGER.R. *et al*, 2002)

O cliente entra no estado de renovação, aguardando uma resposta do servidor, que responde aceitando a solicitação (DHCPPACK) ou rejeitando-a (DHCPNACK). Se for rejeitada o endereço libera o IP e volta para o estado de inicialização. O cliente não recebendo uma resposta, passando 87,5% do tempo de concessão, ele entra em estado de revinculação e retransmite a mensagem DHCPREQUEST para o servidor. Se o cliente receber a resposta, ele volta para o estado limite, caso contrário retorna para o estado de inicialização. (SCRIMGER.R. *et al*, 2002)

A figura 8 mostra o processo de concessão de DHCP.

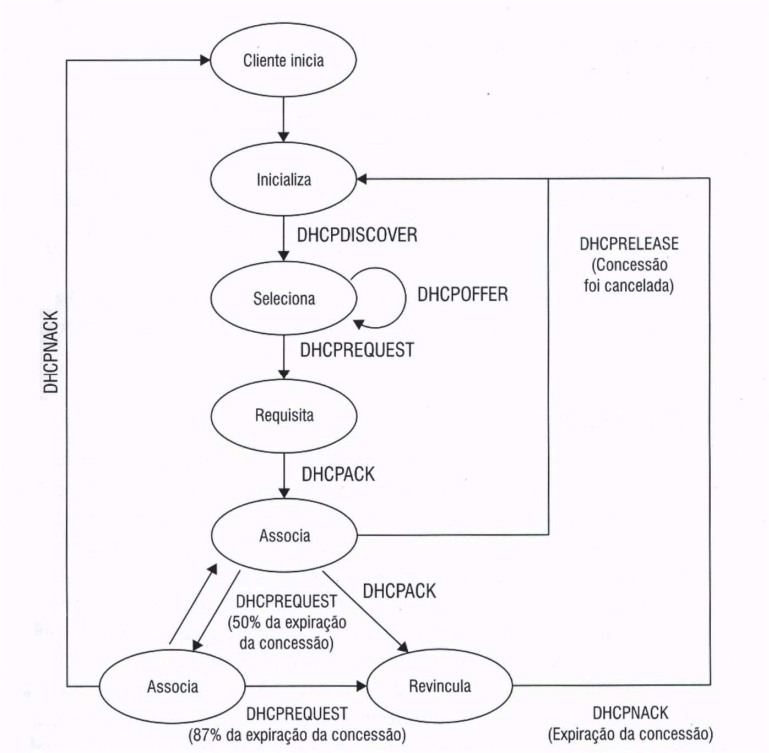


figura 8 – Processo de concessão DHCP - (SCRIMGER.R. et al, 2002).

4.4 Serviços de Rede

Uma rede de computador é caracterizada por dois ou mais computadores que compartilham informações entre si. Essas informações são requisitadas por clientes, que são computadores os quais solicitam informações. Um exemplo seria o cliente solicitar informações de e-mail (consultar e-mails) ao servidor de e-mail, e este é quem gerencia o serviço. (SCRIMGER.R. et al, 2002).

As redes que possuem servidores, ou seja, computadores dedicados para fornecer serviços, são conhecidas como redes centralizadas. Existem vários tipos de serviços de rede, os quais requerem um servidor específico. Serviços como compartilhamento de arquivos, proxy, e-mail e web. (SCRIMGER.R. *et al*, 2002)

Abaixo são identificados os serviços de rede mais comuns.

- Serviço de compartilhamento de arquivos: Utilizado para compartilhar arquivos e impressoras. No Microsoft Windows o serviço de compartilhamento de arquivos é disponibilizado nativamente na instalação do Windows, bastando apenas pequenos ajustes para a disponibilidade do serviço. No Linux, o serviço de arquivos é disponibilizado pelo Samba, onde a disponibilidade depende da configuração do seu arquivo de configuração, o smb.conf

- Serviço DHCP: É utilizado para distribuir endereços IP, além de informações e configurações sobre a rede, como por exemplo o servidor DNS. (SCRIMGER.R. et al 2002). No Microsoft Windows o DHCP pode ser configurado em sistemas de servidor. No Linux o serviço de DHCP pode ser configurado pelo software dhcp3
- Serviço DNS: Serviço responsável por resolver nomes em uma rede. A resolução de nomes é feita pelo servidor DNS que recebe um nome de máquina (ou nome de host) e retorna o seu endereço IP. (SCRIMGER.R. et al 2002). No Microsoft Windows: É configurado na instalação do serviço de diretórios. No Linux o Bind9 é o software responsável pelo serviço de DNS.
- Serviço de Proxy: Faz a ligação de uma rede interna (intranet) com a rede externa (internet). Quando um cliente da intranet tenta acessar a internet, ele solicita ao Proxy, que por sua vez faz acessa o conteúdo e retorna para o cliente. (TRIGO, 2007). No Microsoft Windows o Microsoft ISA Server faz é um exemplo de servidor proxy. No Linux este serviço pode ser disponibilizado pelo proxy Squid.
- Serviço de e-mail: É uma aplicação de internet que possibilita a troca de mensagens por computador entre pessoas e organizações ao redor do mundo. O mecanismo que gerencia essa troca de informações e mantém o serviço de e-mail é chamado de MTA (*Mail Transfer Agent*), responsável por fazer o envio e recebimento de mensagens. (TRIGO, 2007). No Microsoft Windows o servidor Exchange fornece o serviço de e-mails. No Linux o servidor Postfix realiza esta função. (TRIGO, 2007)
- Serviço Web: Serviço fornecido pelo servidor Web, onde se trata de um computador que armazena páginas de internet e que contenha *software* (programa de computador) de servidor de Web. Este, por usa vez, aceita solicitações de clientes (quem está acessando a página) através de um navegador de internet e exibe os resultados para o cliente. Um exemplo de servidor Web para sistemas Microsoft é o IIS (*Internet Information Service*) e para sistemas Linux um exemplo é o Apache. (SCRIMGER.R. et al, 2002)

4.5 Samba

Basicamente, o Samba é um servidor e um conjunto de ferramentas que permite o compartilhamento de arquivos e impressoras sistemas Windows e Linux. Usando o Samba em um servidor Linux, ele se comporta exatamente como um servidor Windows, podendo inclusive autenticar usuários e compartilhar impressoras. Outra característica do Samba é que

ele pode atuar como um Controlador Primário de Domínio (PDC), armazenando perfis de usuários, realizar controle de acesso, sendo suas as configurações tão efetivas quanto às de um servidor Windows (FOCA, 2007).

4.5.1 História

O australiano Andrew Tridgell, desenvolvedor do samba, inicialmente precisava montar um espaço no disco do seu computador em um servidor UNIX. Porém ele precisava de suporte a NetBIOS (parecido com o DNS onde faz uso de nomes e endereços IP) para um aplicativo que pretendia utilizar, e como utilizava em seu computador o sistema de arquivos NFS (*Network File System*), que não suporta NetBIOS, Tridgell desenvolveu um *sniffer* (programa utilizado para capturar o tráfego dos dados em rede), que permitiu analisar e auxiliá-lo a interpretar o tráfego dos dados gerado pelo NetBIOS. Tridgell realizou engenharia reversa no protocolo SMB e implementou no UNIX, fazendo com que sua máquina rodando DOS respondesse às requisições como se fosse um servidor de arquivos Windows (ALECRIN, 2005).

Em 1992 ele disponibilizou o código publicamente, mas não levou o projeto adiante. Até que um dia resolveu testar a máquina Windows de sua esposa no seu computador Linux e ficou satisfeito com o resultado. Nesta mesma época obteve acesso à documentação do protocolo SMB, liberado pela Microsoft, e o projeto novamente foi retomado (ALECRIN, 2005).

Em 1994 a Microsoft disponibilizou a especificação do SMB e do NetBIOS, o que possibilitou um enorme salto no desenvolvimento do Samba. Hoje, mesmo a performance do Samba sendo considerada por muitos melhor do que a de um servidor Microsoft, esta percebeu que é vantajoso os sistemas trabalharem em conjunto, pois um servidor Linux pode funcionar perfeitamente como servidor para estações Windows. (ALECRIN, 2005)

Atualmente a versão estável do samba é a versão 3 e utilizada largamente. No entanto a versão 4 está no estágio alpha 11. Porém, por se tratar de uma versão de desenvolvimento, está disponível apenas para testes, não sendo aconselhável utilizá-la em um ambiente de produção.

4.5.2 Principais características

Toda a configuração do Samba é feita por um arquivo principal, o smb.conf. Neste arquivo estão as configurações globais do servidor, configurações de compartilhamento de arquivos e pastas, permissões, impressoras, entre outros. Ele pode ser modificado diretamente por um editor de textos ou usando um utilitário de configuração via interface Web (acessada

pelo navegador). Um exemplo de utilitário web é o SWAT, que facilita a administração remota quando não é possível estar fisicamente no servidor. A figura 8 mostra o arquivo de configuração smb.conf pelo editor de textos MC. Pode-se editar diretamente as configurações globais, diretórios dos usuários, impressoras e compartilhamentos.

A figura 9 mostra o arquivo de configuração do Samba, o smb.conf.

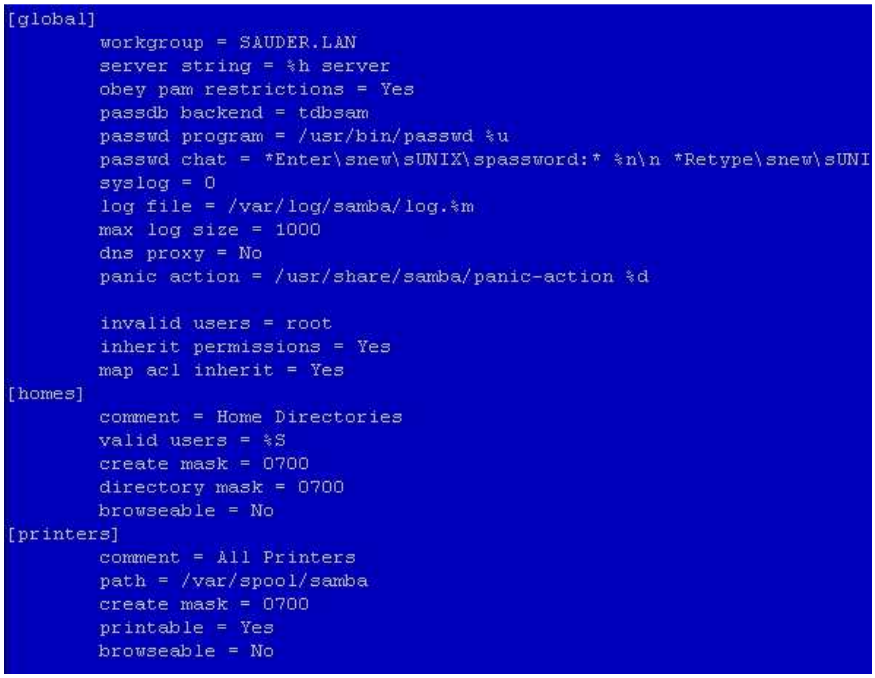


figura 9 - arquivo smb.conf.

Para utilizar a interface web é necessário instalar o SWAT, que proporciona algumas vantagens sobre a edição direta do arquivo de configuração, como interface gráfica, configuração individual das configurações globais, impressoras e compartilhamentos.

A figura 10 mostra a interface web para administração do arquivo smb.conf.

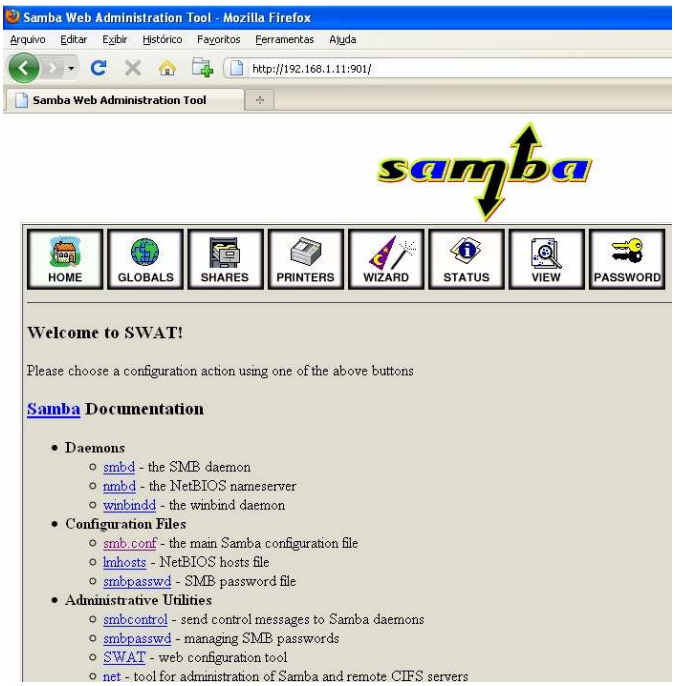


figura 10 - Interface web do Swat para configuração do arquivo smb.conf

4.5.3 Samba como Servidor de Arquivos

Como explicado anteriormente, o Samba pode ser usado como servidor de arquivos, pois conversa com rede Windows graças às implementações do protocolo SMB. Atualmente conhecido como CIFS (Common Internet File System) ou SMB/CIFS, que é uma melhoria do protocolo SMB feita pela Microsoft (FOCA, 2005).

4.5.4 Samba como Controlador de Domínio

Além da função de servidor de arquivos, o Samba pode ser usando também como Controlador de Domínio ou DC (*Domain Controller*), também conhecido como Controlador de Domínio Primário ou PDC (*Primary Domain Controller*) (MORIMOTO, 2005).

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

(da mesma rede) onde faz o login. Em contrapartida, bloqueando uma conta de usuário, automaticamente este estará bloqueado em todas as máquinas gerenciadas pelo Controlador de Domínio (MORIMOTO, 2005).

Para utilizar o Microsoft Active Directory é necessário tornar o servidor um Controlador de Domínio, ou seja, não é possível utilizar um servidor Windows Server como Controlador de Domínio sem utilizar o Active Directory. Porém, a função de controlador de domínio não necessariamente implica que este contém o Active Directory. Em outras palavras, Controlador de Domínio não é a mesma coisa que Active Directory. (MINASI. M. *et al.*, 2000)

4.6 CTDB

O CTDB é um recurso para sistema de arquivos em cluster. Desta forma o Samba passa a oferecer um sistema de arquivos distribuídos em múltiplos nós, aparentando um único servidor de alto desempenho. Embora os servidores Microsoft tenham suporta a cluster, estes são voltados para banco de dados e servidores de internet (servidores web), sendo o número de nós restrito apenas a oito. Portanto a característica de cluster para servidores de arquivos não é suportada por sistemas Windows. O CTDB é praticamente infinitamente escalável em relação ao número de nós (Linux Magazine, 2009).

CTDB significa *Cluster TDB*. Onde TDB (*Trivial Database*) é um banco de dados rápido e foi estendido para ser utilizado em clusters por suportar *locking* o que implica em escrita simultânea. *Locks* que são processos de bloqueio quando um nó-cliente acessa arquivos. As informações dos *locks* geradas pelo protocolo CIFS são armazenados neste banco de dados. Também é necessário sincronizar as tabelas de mapeamento de ID que mapeiam usuários e grupos do Windows aos do Unix (Linux Magazine, 2009).

O Samba utiliza o TDB internamente em vários locais, como caches, tarefas de manipulação de dados e mapeamento de memória para mapear áreas do TDB diretamente na memória. Logo, os TDBs podem ser tão rápidos quanto à memória compartilhada (Linux Magazine, 2009).

Os *daemons* (controladores de serviços de sistema) do CTDB possuem uma cópia do banco TDB, chamada de LTDB e reside na memória local.

O Samba utiliza bancos de dados voláteis (as informações residem na memória), e persistentes (são gravadas em disco). Para gerenciar os dados persistentes, cada nó possui uma cópia completa e atualizada. Cada alteração requer um bloqueio completo no banco. Terminado, as alterações são replicadas para todos os nós do CTDB (Linux Magazine, 2009).

Para gerenciar os dados voláteis, cada nó mantém apenas os registros que já acessou. Isto implica que somente um nó detém as informações atualizadas dos registros, este é o mestre de dados. Se um nó quiser escrever ou ler um registro primeiramente ele verifica se é o mestre dos dados, caso sim executa a ação, caso contrário solicita os dados a partir do *daemon ctdbd* e assume o papel de mestre dos dados, escrevendo localmente (Linux Magazine, 2009).

O Samba também pode executar um processo de recuperação de dados caso algum nó falhar. Logo, o banco de dados volátil irá perder o mestre de dados dos seus respectivos registros. Neste caso é eleito um nó como mestre de recuperação que localiza as cópias mais recentes. O CTDB possui uma numeração seqüencial para registros em um campo do cabeçalho, comparado com o TDB padrão, onde este número é incrementado quando o registro é transferido para outro nó. Ao final do processo de recuperação, o nó eleito como mestre de recuperação passa a ser o mestre de dados para todos os registros de todos os TDBs (Linux Magazine, 2009).

A versão 3.3.0 do samba, lançada em janeiro de 2009, possui suporte completo a clusters.

4.7 Samba 4

Além de fornecer todas as opções de suas versões anteriores, uma implementação bastante interessante foi feita. Trata-se de um serviço de diretórios. Um exemplo bem conhecido de serviço de diretórios é o Active Directory da Microsoft. Porém, é incorreto afirmar que o Samba 4 tem o Active Directory, pois este foi o nome dado ao serviço de diretórios da Microsoft que também é uma implementação do protocolo LDAP. O correto, portanto, seria dizer que o Samba 4 também fornece um serviço de diretório assim como o Windows Server da Microsoft. No entanto, para fins didáticos, vou me referenciar ao serviço de diretório do Linux como **Active Directory do Samba 4** e o serviço de diretórios da Microsoft como **Microsoft Active Directory**.

O Samba 4 continua fornecendo toda a funcionalidade de servidor de arquivos, sendo necessária a edição de parâmetros no seu arquivo de configuração, smb.conf, da mesma forma que suas versões anteriores.

Com esta implementação do serviço de diretórios, é possível gerenciar todos os recursos e objetos disponibilizados pelo Active Directory do Samba 4, independentemente de qualquer ligação com o Microsoft Active Directory.

O foco do Active Directory é o gerenciamento de objetos e recursos. Através das políticas de grupo (GPO). Embora o Samba 4 esteja na versão Alpha (desenvolvimento), já é

possível usufruir deste recurso da mesma forma com é feito no Microsoft Active Directory, tendo em vista que este foi implementado sobre o protocolo LDAP e o Samba 4 utiliza os mesmos *schemas*. (SAMBA.ORG-1, 2009)

Porém, é imprescindível que a infra-estrutura esteja detalhadamente configurada. Boa parte desta estrutura inclui o serviço de DNS. Assim como no Microsoft Active Directory, é utilizado para resolução de nomes em endereços IP e uma configuração incorreta acarreta em falhas no serviço de diretório. O serviço de DNS do Linux chama-se Bind9.

Como o Samba 4 herda todas as características dos seus antecessores, também permanecem as compatibilidades com serviços. Um serviço muito útil é fornecido pelo protocolo DHCP. Trata-se do serviço de distribuição e gerenciamento de endereços IP. Assim como no Microsoft Active Directory, além da vantagem de fornecer endereços IP automaticamente, algumas informações adicionais podem ser enviadas, como o *Gateway* da rede e os servidores DNS.

Outro recurso, que é padrão no Microsoft Active Directory, é a junção em domínios, através de relações de confiança. Onde se o domínio A confia no domínio B, e o domínio B confia em C, automaticamente o domínio A confiará em C.

Além do gerenciamento de grupos e usuários, também é possível centralizar no Samba 4 a autenticação de usuários em vários serviços, como proxy, e-mail e web. O serviço de Proxy trata de fornecer acesso controlado à internet. Através do Proxy é possível definir permissões para usuário e grupos ao que se relaciona à internet. Da mesma forma que o serviço de proxy, os serviços de e-mail e web podem utilizar a base LDAP do Samba 4 para autenticar usuários.

4.7.1 Serviço de Diretórios do Samba 4

A grande novidade no Samba 4, é a implementação do serviço de diretório. Sem essa implementação, esta nova versão não seria diferente das anteriores. O foco principal é o gerenciamento de contas de usuários e máquinas. Alguns serviços como o DNS, são imprescindíveis para o serviço de diretório, pois está diretamente ligado ao domínio. Outros serviços, como o DHCP, complementam uma infra-estrutura mínima para a utilização do Active Directory no Samba 4. O DNS também é um requisito fundamental para a instalação do Microsoft Active Directory. Segundo Minasi (2002), sem o DNS o Active Directory não funciona.

O Active Directory do Samba 4 tem um comportamento muito similar ao Microsoft Active Directory por utilizar justamente os mesmos *schemas* que o serviço de diretórios da

Microsoft. Desta forma, os atributos do LDAP também deverão ser os mesmos, o que implica que será possível utilizar o Samba 4 como alternativa ao Microsoft Active Directory. (SAMBA.ORG-1, 2009)

Um ponto interessante, é que o gerenciamento do Active Directory do Samba 4 deve ser feito obrigatoriamente por ferramentas desenvolvidas para o Microsoft Active Directory. No próprio console de administração de uma máquina com Windows Server 2003 dentro do domínio do Samba 4 é possível gerenciar a base de dados do Active Directory do Samba 4. Até a data deste trabalho não existe ainda uma ferramenta nativa ou desenvolvida para o Linux voltada para a administração do serviço de diretório do Samba 4. (SAMBA.ORG-3, 2009)

Vários outros serviços podem se beneficiar de serviços de diretórios. O Microsoft Active Directory, por exemplo, pode ser integrado a Microsoft ISA Server e Microsoft Exchange, que respectivamente provêem acesso controlado à internet e acesso à serviços de e-mail, ambos mediante a nome e senha fornecidos pelo Active Directory. Linux também possui serviços de Proxy e Email, fornecidos respectivamente pelo Squid e Postifx.

Como os dois serviços de diretório (Microsoft e Linux) utilizam *schemas* compatíveis, o controle de recursos e permissões de usuários são idênticos. Os atributos que restringem a utilização de recursos em computadores Windows XP ficam armazenados na base de dados. Assim, a utilização do Active Directory para Linux é mais relevante quando as máquinas cliente forem Windows (SAMBA.ORG-2, 2009)

4.7.2 Samba 4 - Integração com Serviços

A tabela abaixo mostra alguns serviços e a equivalência entre os sistemas operacionais Microsoft e Linux:

Tabela 4 – Serviços de rede Microsoft x Linux

Serviço	Microsoft	Linux
Servidor de Arquivos	Windows Server	Samba 4
Servidor Proxy	ISA Server	Squid
Servidor de E-mail	Exchange Server	Postfix
Servidor Web	IIS	Apache

A intenção de se utilizar o Active Directory integrado a estes serviços é prover uma administração centralizada, onde independente do serviço, sendo necessário apenas um usuário e senha, cadastrados no Active Directory.

Diversos serviços disponíveis para Linux, como os apresentados na Tabela 4, podem ser configurados para utilizarem o protocolo LDAP. Sendo o Active Directory do Samba 4 uma implementação do protocolo LDAP, é possível integrar tais serviços para trabalharem em conjunto, assim como o Microsoft Active Directory integra seus serviços.

A figura 11 ilustra o Active Directory do Samba 4 integrando serviços, como e-mail, Proxy, arquivos e ao Microsoft Windows.

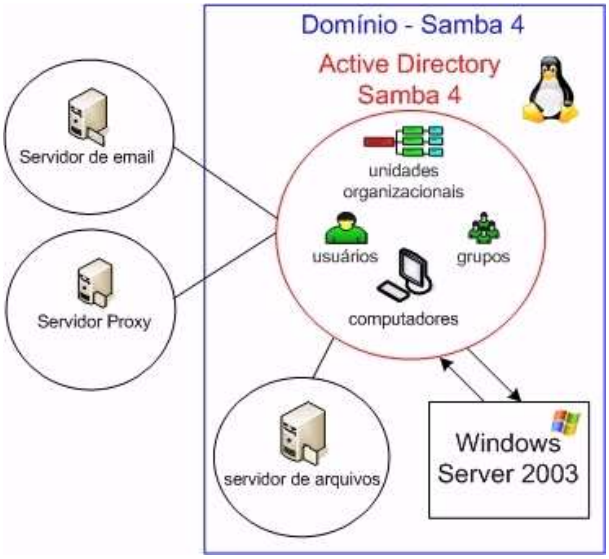


figura 11 – Esquema do Active Directory do Samba 4

A figura 12 ilustra o Microsoft Active Directory, identificando também a integração com serviços.

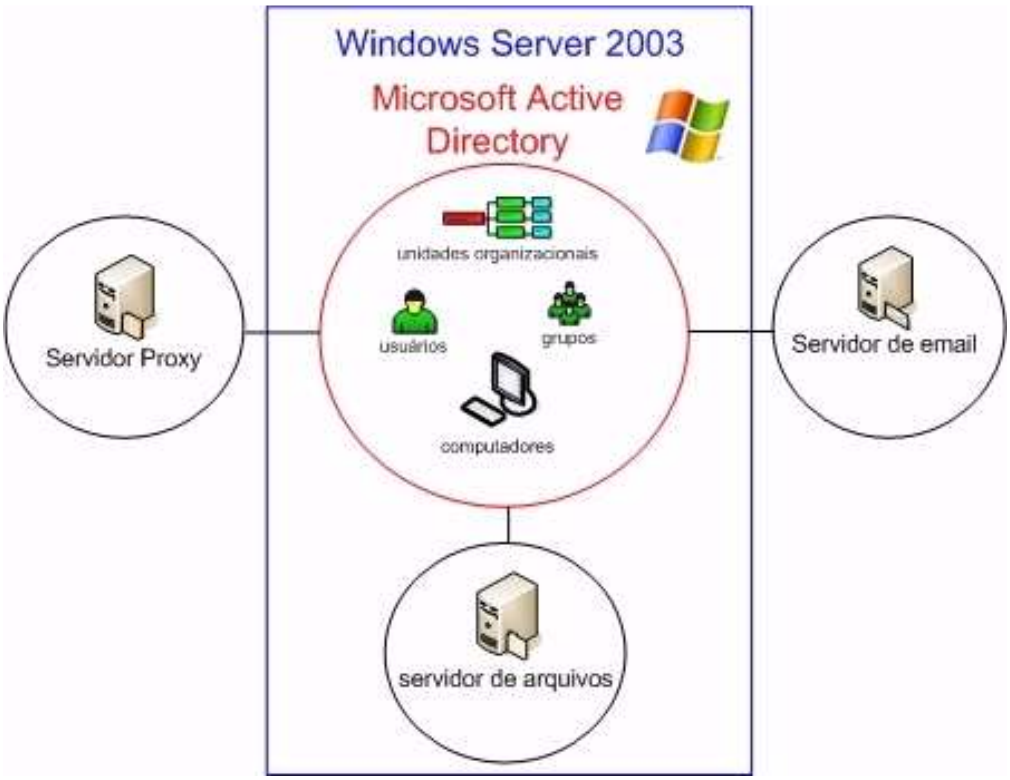


figura 12 – Esquema do Microsoft Active Directory

4.7.3 Recursos disponíveis no Samba 4

Por utilizar schemas compatíveis com os schemas do Microsoft Active Directory, o serviço de diretório do Samba 4 possui características equivalentes ao serviço de diretórios da Microsoft. Desta forma, o foco é o gerenciamento dos objetos do domínio, sendo eles máquinas, usuários e grupos. (SAMBA.ORG-1, 2009)

Embora a integração do Microsoft Active Directory com diversos serviços seja uma característica secundária, ou seja, existirá conforme a necessidade da rede, ela torna centralizada a administração de usuários em vários serviços, o que faz da integração uma ferramenta de trabalho. Desta mesma forma o Active Directory do Samba 4 também prevê a integração com diversos serviços, como: proxy, e-mail, web, etc.

5 Metodologia

Para o sucesso da implementação e obtenção dos dados necessários, será instalada uma estrutura de rede conforme mostrado na figura 13.

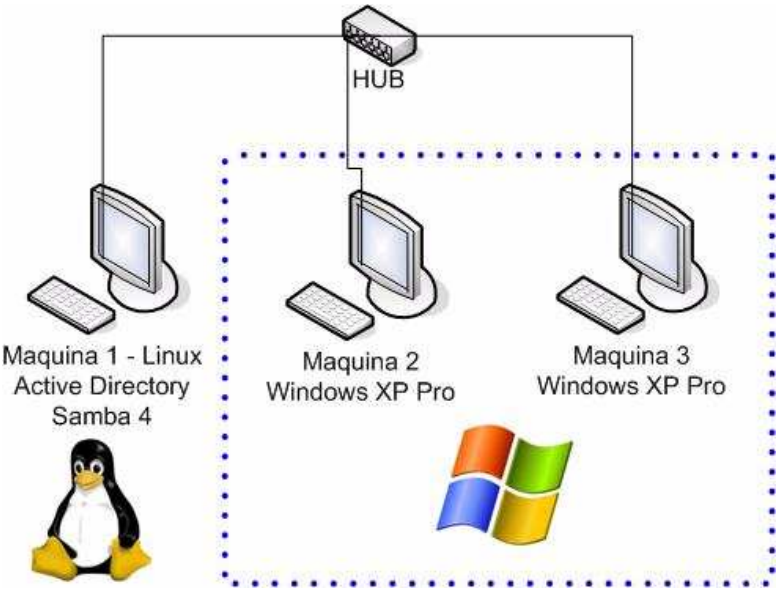


figura 13 – Infra-estrutura para a rede com Samba 4

Na máquina 1 será instalado o sistema operacional Linux, necessário para a instalação do Samba 4 e conseqüentemente, o seu Active Directory. Na máquina 2 será instalado o Windows XP Pro para ingresso no domínio do Active Directory do Samba 4 e também para sua administração. E na máquina 3 também instalado o Windows XP Pro que será utilizada como cliente e acesso a serviços de rede. As máquinas serão interligadas através de um HUB, formando uma rede.

Após a preparação da infra-estrutura, será feita a configuração do serviço de diretório, com o objetivo primário de autenticar usuários no domínio do Samba 4, ingressando a máquina 2 no domínio do Samba 4 e utilizar os recursos do serviço de diretórios, da mesma forma como é feito no Microsoft Active Directory.

Objetivos secundários, como a utilização da base de dados do Samba 4 para fornecer autenticação centralizada para outros serviços como arquivos, proxy, e-mail e web.

A metodologia seguirá os passos detalhados abaixo:

- Instalação do Samba 4 e infra-estrutura para o Active Directory (máquina 1)
- Ingressar a máquina 2 no domínio do Samba 4 e utilizá-la para administração do serviço de diretórios
- Ingressar a máquina 3 no domínio do Samba 4 e utilizá-la para demonstrar recursos fornecidos pelo serviço de diretórios.
- Adicionar usuários, grupos e configurar clientes a partir do Active Directory do Samba 4.
- Utilizar o software LDAP Browser para explorar estrutura da base LDAP do Active Directory do Samba 4 e do Microsoft Active Directory.
- Configurar serviços de rede para integração com o Samba4, equivalente aos serviços Microsoft integrados ao Active Directory.

As configurações das três máquinas são similares: Processador de 2Ghz, 1GB RAM, 80GB de disco rígido e placa de rede 10/100.

6 Implementação

Para a implementação do Active Directory do Samba 4, foram seguidos os principais passos de instalação e configuração mostrados a seguir.

Algumas informações utilizadas na configuração:

- Ip do servidor Samba 4: 192.168.1.230
- Nome do servidor Samba 4: note-debian
- Realm Kerberos: TESTE.LAN
- Domínio: TESTE
- Login administrativo: administrator
- Senha administrativa: 1010
- Máquina cliente Windows XP Pro: nomeada como NOTE

6.1 Instalando o Samba 4

Para a instalação foi necessário fazer o download dos fontes do samba 4 versão Alpha9, e o processo de compilação e instalação básicos. Estes arquivos são salvos no diretório *samba-master*, dentro no diretório raiz do sistema operacional Linux Debian. Neste diretório, ao executar o comando abaixo, é criada a estrutura básica do Active Directory do Samba 4 (SAMBA.ORG-3, 2009):

- `./setup/provision --realm=teste.lan --domain=teste --adminpass=1010 --server-role='domain controller'`

Uma estrutura de diretórios básica é criada, onde podem ser encontrados os arquivos de configuração do Samba4:

- `/usr/local/samba`

Os arquivos de configuração são instalados no diretório:

- `/usr/local/samba/sbin/`

Para iniciar o Samba 4, é necessário executar o comando abaixo, a partir do diretório raiz:

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

6.2 Instalação do serviço de DNS

A instalação e uma correta configuração do serviço de DNS é imprescindível para o funcionamento do serviço de diretório do Samba 4, não sendo possível a resolução de nomes sem o DNS, pois para ingressar no domínio, as máquinas precisam consultar o DNS para resolver o nome do domínio TESTE no endereço IP do servidor. (SAMBA.ORG-3, 2009). O servidor DNS do Linux que será instalado é o Bind9.

Foram configurados os arquivos do servidor DNS em:

- `/etc/bind`

Após configurar o servidor DNS, devemos garantir que ele esteja resolvendo nomes. O comando *ping* seguido pelo nome do domínio deverá retornar o endereço IP do Samba4. Com estas configurações, o servidor já será possível resolver nomes e as máquinas já podem ingressar no domínio.

6.3 Ingressando no Domínio do Samba 4

Para ingressar a máquina 2 e a máquina 3 no domínio do Samba 4, é necessário configurar endereços IP e DNS (SAMBA.ORG-3, 2009), conforme figura 14

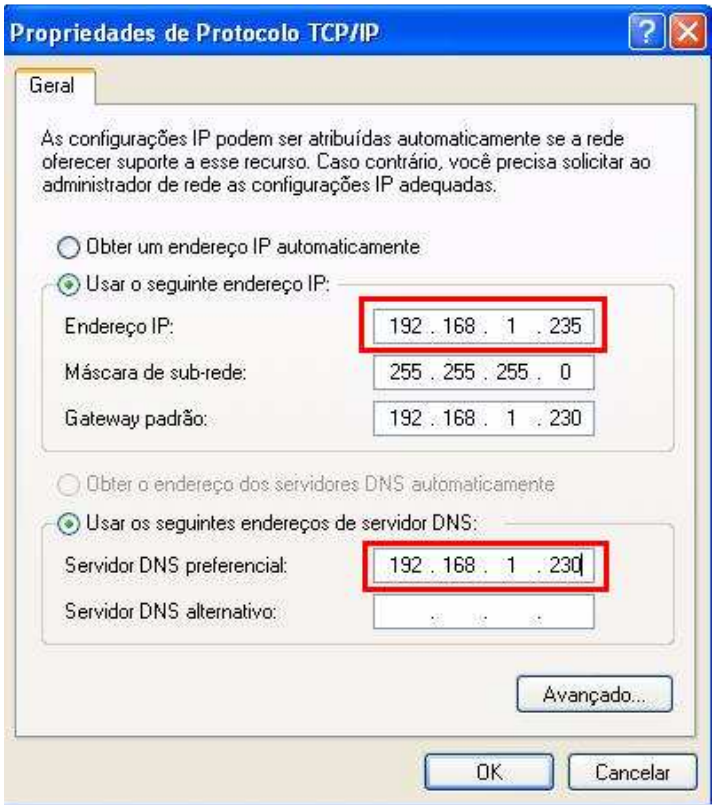


figura 14 - Configuração de rede do cliente Windows XP Pro

É importante observar a configuração do servidor DNS preferencial (IP do servidor Samba 4), que é fundamental para o sucesso do ingresso no domínio.

Também é requerido que as máquinas estejam com o relógio quase que sincronizado precisamente com o do servidor Samba 4. A diferença entre os horários não pode ser maior que 5 minutos. Com o comando *DATE*, executado no Linux Debian, o horário do servidor foi retornado e este foi aplicado manualmente nas máquinas cliente Windows XP Pro.

Para realizar o ingresso no domínio é necessário identificar o nome do domínio criado no Samba 4. As credenciais do administrador, também criadas no Samba 4, serão solicitadas.

A figura 15 mostra a configuração para o ingresso no domínio:

figura 15 - Ingresso no domínio do Samba 4

Após reiniciar a máquina, será possível fazer o login no domínio com a conta do administrador, criadas na instalação do Samba 4.

6.4 Recursos do serviço de diretórios do Samba 4

A administração do serviço de diretórios do Samba4 deve ser feita exclusivamente através das ferramentas utilizadas para administração Microsoft Active Directory, em um servidor Windows Server 2003.

A administração também é possível através do Sistema Operacional Windows XP Pro, utilizando as ferramentas abaixo: (SAMBA.ORG-3, 2009):

- Adminpak
- WindowsServer2003-KB892777-SupportTools-x86-ENU

Em ambos os sistemas operacionais Microsoft (cliente ou servidor), as máquinas devem fazer parte do domínio do Samba4. Para acessar o Active Directory do Samba 4 a partir de uma máquina Windows XP Pro com o software de administração devidamente instalado, é necessário executar o comando:

- `dsa.msc`

O resultado aparece na figura 16:

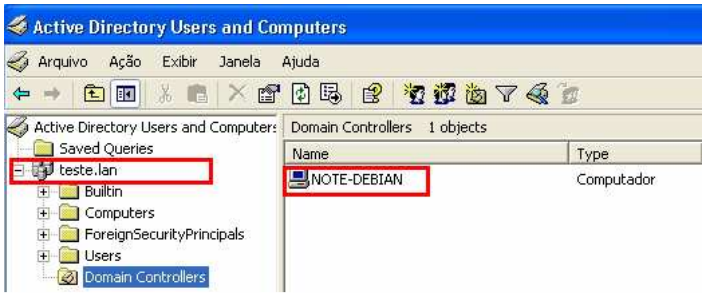


figura 16 - Samba 4 Active Directory

A figura 17 mostra o domínio criado *TESTE.LAN* e o nome do servidor Samba 4, *NOTE-DEBIAN*

Uma vez que o serviço de diretórios está instalado e operando, foram feitos os seguintes testes:

- Criar usuários e grupos

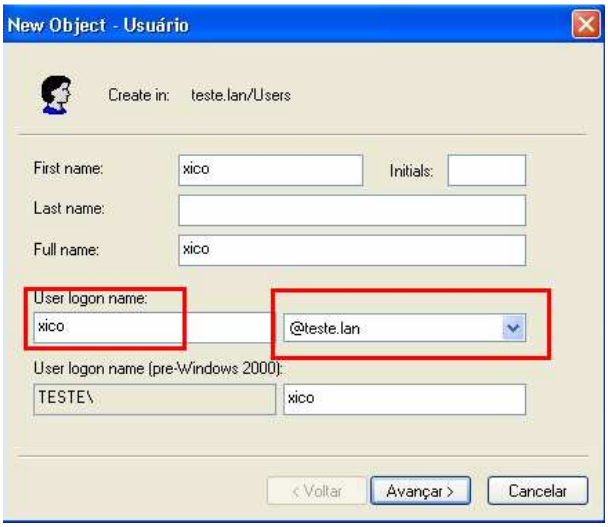


figura 17 - Criando um usuário no Active Directory do Samba 4

A figura 18 mostra a criação de grupos e usuários do Active Directory do Samba 4.

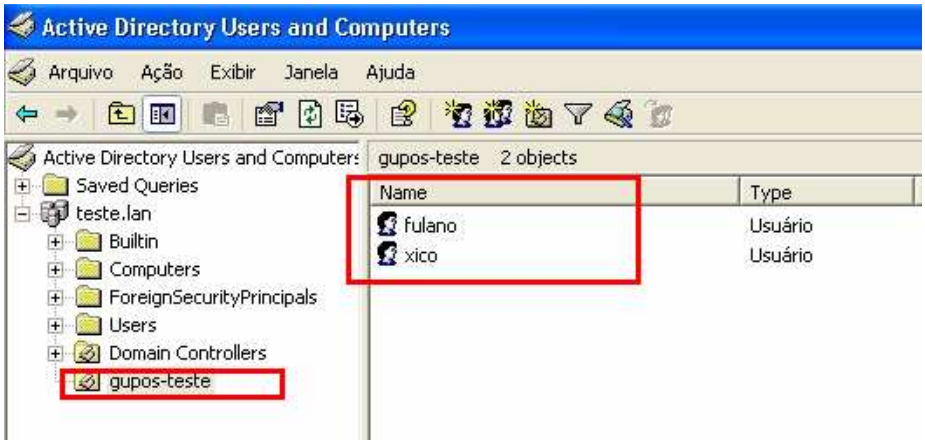


figura 18 - Grupos e Usuários do Active Directory do Samba 4

- Definir políticas de grupo (GPO)

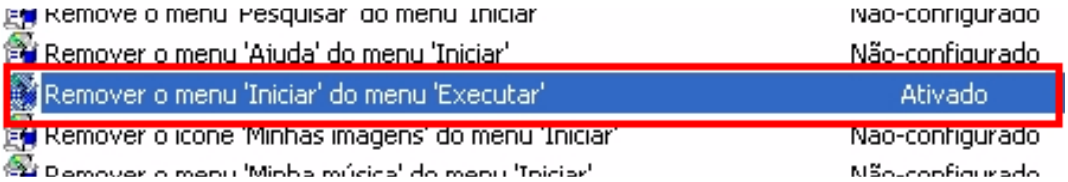


figura 19 - Configuração de políticas de grupo do Samba 4

A figura 20 mostra a política da figura 19 aplicada. O menu “executar” não está mais presente no menu “iniciar”.

figura 20 - Política aplicada

Depois de testar as funcionalidades do serviço de diretório Samba 4, foi notada uma dificuldade quanto à definição de permissões de usuários relacionadas a pastas e arquivos.

Mesmo configurando corretamente, ainda não é possível gerenciar corretamente as permissões para pastas e arquivos.

6.5 Estudo de Caso

Abaixo três cenários mostrando a implementação dos serviços de diretório do Samba 4, integrado a alguns serviços de rede, como de serviços de compartilhamento de arquivos, proxy, e-mail e web.

6.5.1 Serviço de Compartilhamento de Arquivos

Praticamente toda a rede de computador necessita de compartilhar arquivos. A característica de servidor de arquivos é mantida no Samba 4. Desta forma, este serviço é nativo, sem necessidade de instalação de outros softwares, bastando apenas configurar o arquivo de configuração do Samba 4, o smb.conf.

Dentre os serviços, provavelmente o mais simples de configurar é o próprio Samba para compartilhamento de arquivos. Basta apenas inserir as linhas abaixo no arquivo de configuração smb.conf do Samba 4, e que o diretório descrito em *path* exista:

```
[testes]
        path = /home/teste
        read only = no
```

Desta forma, deverá ser possível a qualquer usuário do domínio acessar o compartilhamento chamado “testes”, bastando apenas fornecer os seus dados de usuário e senha. As figuras 21 e 22 ilustram esta implementação.

figura 21 – Acesso ao servidor de arquivos mediante login e senha

A figura 22 mostra o recurso de compartilhamento de arquivos disponível.

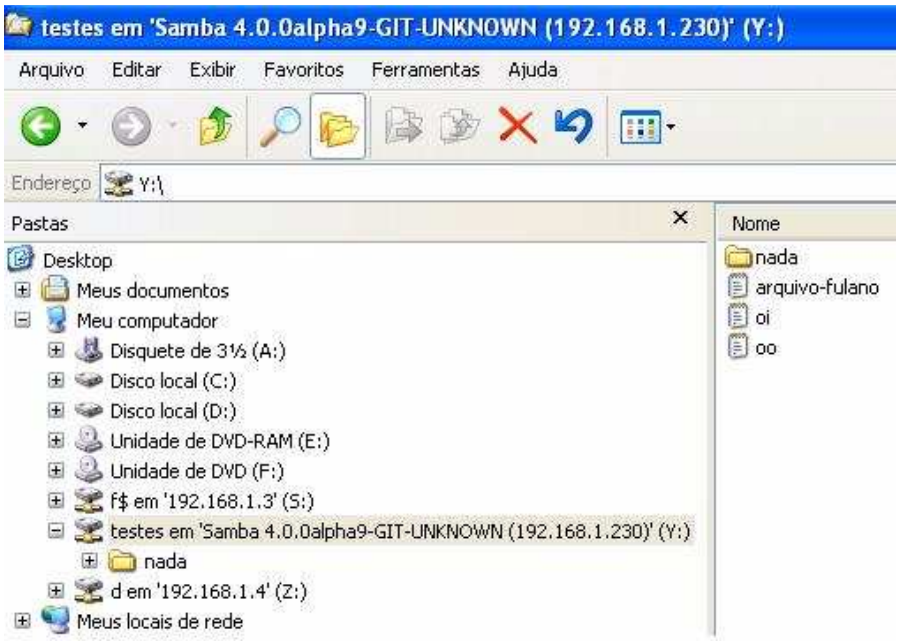


figura 22 – Servidor de Arquivos

6.5.2 Serviço de Proxy

O serviço de Proxy do Linux é fornecido pelo software Squid. Através do Proxy é possível definir permissões de acesso a usuários em diferentes níveis, como o bloqueio de sites indesejados, permissões individuais ou por grupos. (MORIMOTO, 2005)

O controle de acesso à internet, definido pelo Proxy integrado ao Samba 4, permite o gerenciamento de usuários de forma centralizada. Este serviço normalmente é utilizado em redes que necessitam de um controle mais rigoroso no acesso à internet.

Assim como as redes Microsoft podem utilizar serviço de Proxy fornecido pelo ISA Server, e este pode estar integrado ao Microsoft Active Directory para realizar autenticação, no Linux, através Squid integrado ao Active Directory do Samba 4, os usuários poderão se autenticar no navegador para acessar a internet.

O Squid não requer um *schema* específico. Os *schemas* padrão são suficientes para realizar a autenticação, pois requerem somente os atributos uid e senha, atributos comuns.

Primeiro é necessário instalar o squid, com o comando:

- `apt-get install squid`

Desta forma, o arquivo de configuração do squid deverá estar localizado em:

- `/etc/squid.conf`

Com alguns ajustes pontuais neste arquivo de configuração o serviço de Proxy já está disponível, porém para que seja integrado ao Samba 4 é necessário inserir um linha de código responsável por fazer a autenticação, podendo ser por usuários ou por grupos.

Abaixo a autenticação por usuários individuais:

- `auth_param basic program /usr/lib/squid/ldap_auth -D "cn=administrator,cn=users,dc=teste,dc=lan" -w senha -b "ou=internet,dc=teste,dc=lan" -f sAMAccountName=%s -h 192.168.1.230`

A seguir a configuração para autenticação por grupos:

- `external_acl_type ldap_group %LOGIN /usr/lib/squid/squid_ldap_group -R -b "dc=teste,dc=lan" -D "cn=proxy_user,ou=internet,dc=teste,dc=lan" -w senha -f "(&(objectclass=person)(sAMAccountName=%v)(memberof=cn=%a,ou=internet,dc=teste,dc=lan))" -h 192.168.1.230`

Na autenticação por grupos é necessário criar um usuário dentro do Samba 4 para fazer o link entre o Squid e a base LDAP. Neste caso o usuário criado foi *proxy_user*. No Active Directory este processo não é necessário, bastando apenas informar os dados do administrador.

Ainda no arquivo de configuração, é necessário utilizar um recurso do squid chamado de ACL (Listas de Controle de Acesso), para implementar o controle de permissões, conforme se segue:

- `acl AcessoPadrao external ldap_group LdapAcessoPadrao`

De forma que *AcessoPadrao* é o nome da ACL e *LdapAcessoPadrao* é o nome do grupo o qual o usuário pertence.

Assim, todos os usuários do grupo *AcessoPadrao*, criados no Samba 4, poderão ter acesso à internet através do servidor Proxy.

A figura 23 ilustra a utilização do servidor proxy integrado ao Samba 4.

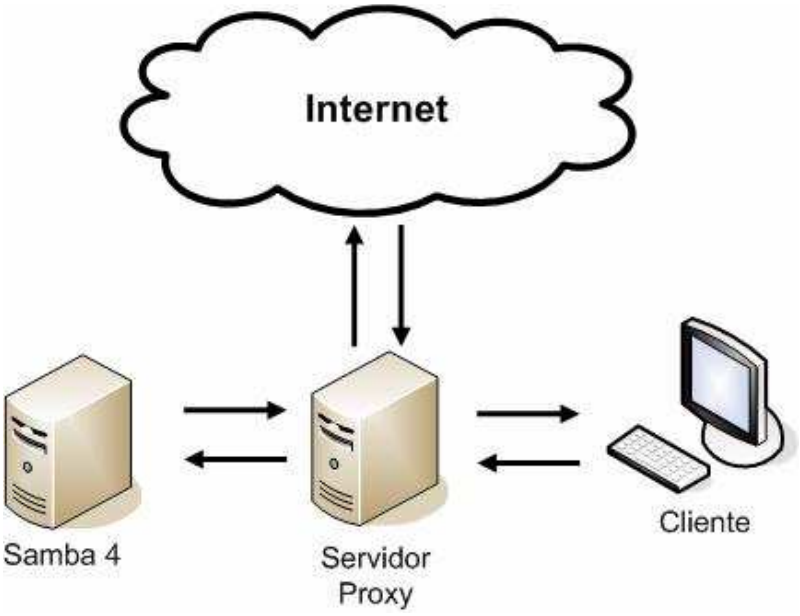


figura 23 - Autenticação com servidor Proxy

6.5.3 Serviços de E-mail

Um serviço de e-mail em um servidor interno, torna-se útil para um controle de arquivos que entram e saem da empresa, controlando assim seus interesses.

O serviço de e-mail utilizado para fazer a integração com o Samba4 será o Postfix, que equivale ao Microsoft Exchange.

Após instalar o Postfix existe a necessidade de utilizar um *schema* para acessar atributos específicos. Desta forma será utilizado o *qmail.schema* de outro servidor de e-mail, o Qmail (LDA.ORG.BR, 2009)

Deve-se fazer uma referência ao *qmail.schema* dentro do arquivo de configuração do LDAP (o *slapd.conf)*, desta forma:

```
include /etc/ldap/schema/qmailuser.schema
```

No arquivo de configuração do Postfix, as seguintes linhas devem ser adicionadas:

```
alias_maps = hash:/etc/aliases, ldap:accounts
accounts_server_host = ldap://ldap.teste.lan
accounts_search_base = ou=usuarios,dc=teste,dc=lan
accounts_query_filter = (&(uid=%u)(accountStatus=0))
accounts_result_attribute = uid
```

```
accounts_version = 3
```

Desta forma o Postfix irá consultar a base LDAP para fornecer acesso às caixas postais. (POSTFIX.ORG.BR, 2009)

O acesso às caixas postais depende de outros programas e configurações os quais não são o foco deste trabalho.

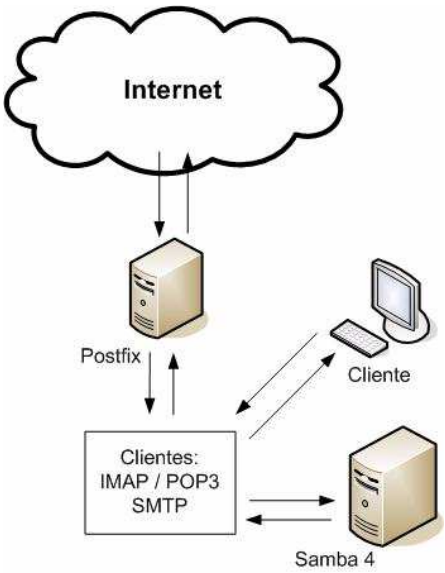


figura 24 – Postfix com autenticação via Samba4

6.5.4 Serviços de Web

Serviços como Proxy podem ter algumas ferramentas para geração de relatórios, as quais necessitam de um servidor web para funcionar, uma vez que a interface de acesso é o *browser* (navegador de internet). Desta forma, é necessário ter o serviço de web, no Linux provido pelo Apache.

Com o servidor Apache instalado, deve-se alterar o arquivo de configuração, localizado em:

```
/etc/apache2/sites-enabled/default
```

E acrescentar as seguintes linhas:

```
AuthBasicProvider ldap
AuthzLDAPAuthoritative off
AllowOverride None
Order allow,deny
Allow from all
```

```
AuthName "Acesso restrito."
AuthType Basic
```

A configuração abaixo é necessária para acessar a base LDAP:

```
AuthLDAPURL
ldap://192.168.1.230/ou=apache,ou=geral,dc=teste,dc=lan?sAMAccountNam
e?sub?(ObjectClass=*)
AuthLDAPBindDn administrator@teste.lan
AuthLDAPBindPassword 1010
require valid-user
```

Assim, para acessar determinados domínios do servidor web Apache, será necessário fornecer credenciais para autenticação, armazenadas na base LDAP do Samba 4.

O acesso aos relatórios gerados pelo servidor proxy por usuários do Samba4 é um exemplo dessa integração. Os relatórios podem ser acessados por qualquer navegador de internet. A figura 25 ilustra o processo de autenticação mediante ao login baseado nos dados cadastrados no Samba4.

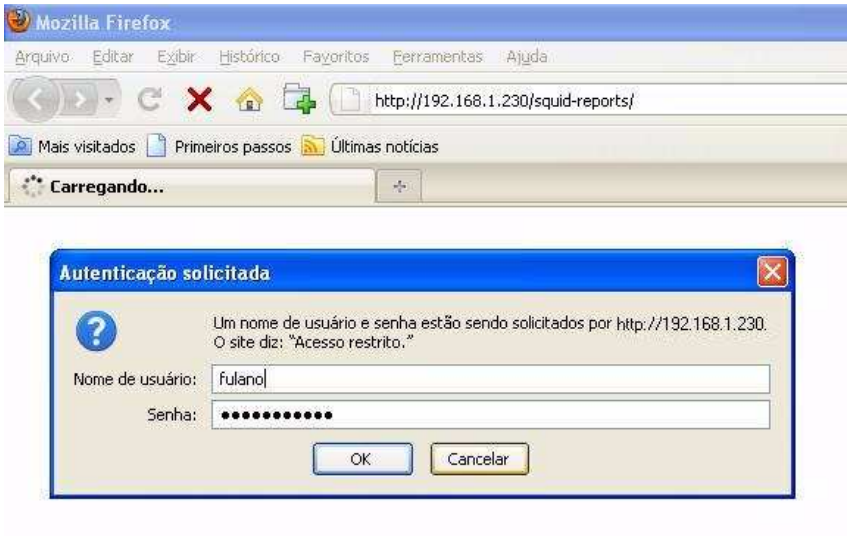
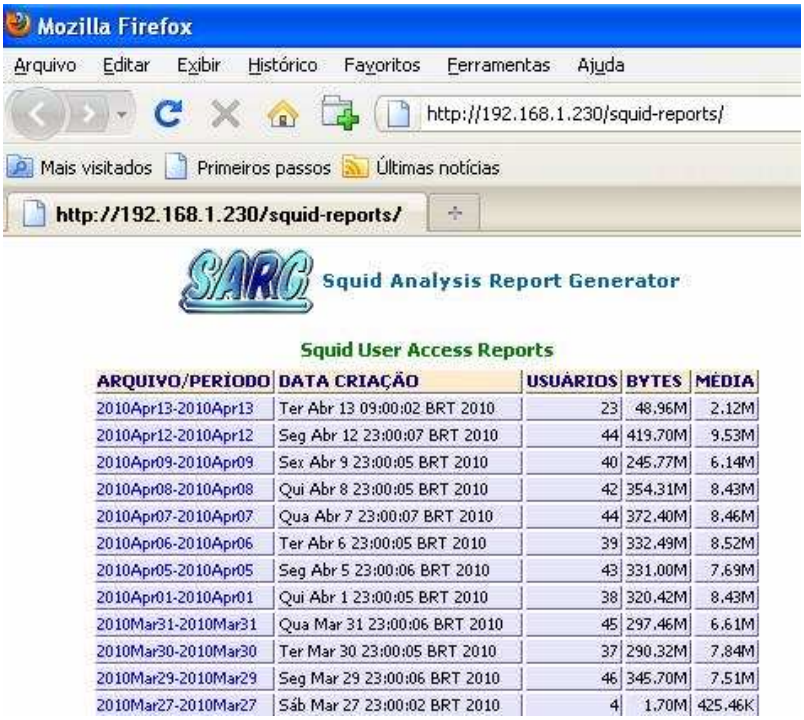


figura 25 – Autenticação na base LDAP do Samba4

A figura 26 mostra relatórios fornecidos após a autenticação do usuário pelo Samba 4.



ARQUIVO/PERÍODO	DATA CRIAÇÃO	USUÁRIOS	BYTES	MÉDIA
2010Apr13-2010Apr13	Ter Abr 13 09:00:02 BRT 2010	23	48.96M	2.12M
2010Apr12-2010Apr12	Seg Abr 12 23:00:07 BRT 2010	44	419.70M	9.53M
2010Apr09-2010Apr09	Sex Abr 9 23:00:05 BRT 2010	40	245.77M	6.14M
2010Apr08-2010Apr08	Qui Abr 8 23:00:05 BRT 2010	42	354.31M	8.43M
2010Apr07-2010Apr07	Qua Abr 7 23:00:07 BRT 2010	44	372.40M	8.46M
2010Apr06-2010Apr06	Ter Abr 6 23:00:05 BRT 2010	39	332.49M	8.52M
2010Apr05-2010Apr05	Seg Abr 5 23:00:06 BRT 2010	43	331.00M	7.69M
2010Apr01-2010Apr01	Qui Abr 1 23:00:05 BRT 2010	38	320.42M	8.43M
2010Mar31-2010Mar31	Qua Mar 31 23:00:06 BRT 2010	45	297.46M	6.61M
2010Mar30-2010Mar30	Ter Mar 30 23:00:05 BRT 2010	37	290.32M	7.84M
2010Mar29-2010Mar29	Seg Mar 29 23:00:06 BRT 2010	46	345.70M	7.51M
2010Mar27-2010Mar27	Sáb Mar 27 23:00:02 BRT 2010	4	1.70M	425.46K

figura 26 – Página fornecida pelo servidor web

6.6 Explorando bases LDAP

Na figura 22 é possível visualizar os atributos do diretório do Samba 4 e Microsoft com o software LDAP Browser (LdapBrowser, 2004).

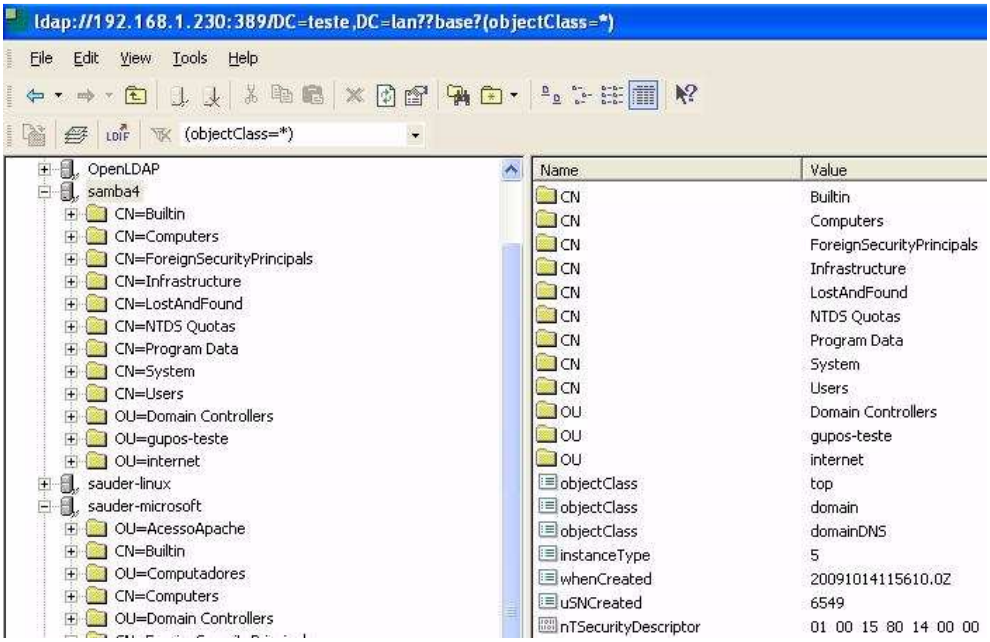


figura 27 – Base LDAP vista pelo software LDAP Explorer

A base LDAP, tanto no Microsoft Active Directory quanto no Active Directory do Samba 4, está configurada na porta padrão 389. Para realizar a conexão com o programa, é necessário indicar o endereço IP do computador onde está a base LDAP e a porta, além do DN referente ao administrador.

Todos os atributos dos objetos podem ser consultados através deste programa.

7 Resultados

Após implementar o Samba 4, foi possível determinar semelhanças e diferenças entre os dois serviços de diretórios, começando pela instalação. Por estar na versão de testes (Alpha), o Samba 4 requer um conhecimento avançado em Linux. Embora no site oficial do Samba exista um tutorial de instalação, muitos erros acontecem durante o processo e um conhecimento além do mínimo é fundamental. Ao passo que na instalação do Microsoft Active Directory existe um utilitário que guia o processo de instalação, apontado erros e os corrigindo se possível.

Ainda no processo de instalação e preparação, o conceitual é da instalação do Active Directory do Samba 4 é basicamente o mesmo do Microsoft Active Directory. É necessário ter o serviço DNS instalado corretamente para que o serviço de diretórios funcione adequadamente. Porém no Samba 4 todo o processo ainda é quase que totalmente manual, sendo no Microsoft Active Directory o processo ocorre por meio de utilitários.

Após a instalação do serviço de diretórios do Samba 4, é possível criar usuários e grupos assim como no serviço de diretórios da Microsoft. Alguns recursos como diretiva de segurança de senhas ainda não estão operando corretamente, pois mesmo que sejam definidas diretivas, estas não são aplicadas. Essa diretiva por padrão força a criação de senhas fortes para os usuários. Este recurso pode ser desativado no Microsoft Active Directory, mas no Samba 4 não foi possível.

Outro recurso que ainda precisa ser melhorado é a definição de permissões de acesso a pastas e arquivos. No Microsoft Active Directory é possível definir o nível de permissão (basicamente escrita, leitura, acesso negado) e refiná-las com permissões atômicas. No Samba 4 estas opções ainda não respondem corretamente quando configuradas.

Um recurso muito interessante são as Políticas de Grupo. Tanto no Active Directory do Samba 4 quanto no Microsoft Active Directory é possível gerenciar os computadores do domínio, moldando os recursos da máquina de acordo com cada Unidade Organizacional ou Usuário/Grupo.

A criação de Unidades Organizacionais também está presente em ambos os serviços de diretório e se mostrou bem efetiva no Samba 4. Um usuário do Samba 4 que pertence a uma Unidade Organizacional devidamente configurada para fornecer restrições a máquinas Windows XP Pro, efetivamente foi restringido a utilizar os recursos previamente definidos.

Em relação aos demais serviços, o Samba 4 se comportou exatamente como o Microsoft Active Directory autenticando os usuários em serviços de rede. Pelo fato destes serviços utilizarem *schemas* compatíveis, a configuração é praticamente idêntica.

Nas implementações o Active Directory do Samba 4 se mostrado tão estável e rápido quanto o Active Directory, mesmo estando em uma versão de desenvolvimento.

A tabela 5 mostra uma lista de serviços que podem ser integradas ao serviço de diretórios do Linux.

Tabela 5 – Serviços de Rede Microsoft x Linux

Serviços	Microsoft	Linux
Controlador de domínio	Active Directory	Samba 4
Servidor de arquivos	Windows Server 2003	Samba 4
Proxy	ISA Server	Squid
Servidor WEB	IIS	Apache

8 Conclusão

Nos dias de hoje o gerenciamento centralizado de recursos de uma rede deixou de ser uma opção. Recursos administrativos como os fornecidos pelo Microsoft Active Directory, se tornou imprescindível.

O serviço de diretórios da Microsoft ainda é a única alternativa. Desta forma a implementação do protocolo LDAP para criação de um serviço de diretório para Linux através do Samba 4 realmente foi uma boa iniciativa. Embora a instalação do Samba 4 ainda seja muito técnica, com muitos detalhes, exija um conhecimento relativamente avançado em Linux e ainda seja considerada difícil em comparação com a instalação Active Directory da Microsoft, pelos testes realizados este servidor poderá se tornar uma boa alternativa para controlador de domínio e serviços de diretório.

Embora com funcionalidades ainda reduzidas, o Samba 4 por utilizar como base os mesmo protocolos do Active Directory, sendo alguns já estáveis como KERBEROS, LDAP, DHCP e DNS, já fornece uma boa estrutura. O Samba 4 mostrou-se eficiente em algumas características, como a definição de políticas de grupo e o gerenciamento de usuários. Mas em outras, como controle de permissões e ingresso no domínio, ainda deverão ser melhoradas.

Desta forma, ainda não é recomendável utilizar o Samba 4 em um ambiente de produção, tendo em vista que por ele ainda está na versão de desenvolvimento. Portanto, não é um sistema estável. No entanto, as implementações mostraram-se estáveis e atingiram os objetivos as quais foram submetidas, mostrando assim que o Samba 4 está no caminho certo, porém ainda existe muito a ser feito.

Pode-se explorar para futuros trabalhos, os seguintes temas: Virtualização com Samba 4 e Disaster Recovery (recuperação de desastres) de domínios geridos pelo Samba 4.

9 Referências

ALECRIN. E. **Servidor Samba: o que é**. Disponível em: http://www.infowester.com/linuxsamba.php. Acesso em dezembro de 2009.

CONECTIVA. **Kerberos**. Autenticação do Sistema. Disponível em: http://www.conectiva.com/doc/livros/online/10.0/servidor/pt_BR/ch13s04.html. Acesso em outubro de 2009

ERICH. S. M. **Autenticação Integrada Baseada em Serviço de Diretório LDAP**. Apresenta estudo do protocolo LDAP. Disponível em http://www.linux.ime.usp.br/~cef/mac499-06/monografias/erich/html/ch01s05.html. Acesso em dezembro de 2009

FILHO.M.M.C. **Kerberos.**. Apresentação do protocolo Kerberos. Disponível em: http://www.gta.ufrj.br/grad/99_2/marcos/kerberos.htm. Acesso em julho de 2009

FOCA GNU/Linux**. Samba**. Disponível em: http://www.guiafoca.org/guia/avancado/ch-s-samba.htm. Acesso em novembro de 2009.

LDAP.ORG.BR **Como instalar um PDC Samba+OpenLDAP**. Disponível em: http://www.ldap.org.br/modules/ldap/files/files///samba+openLDAP+qmail.pdf. Acesso em setembro de 2009.

Linux Magazine. São Paulo. Linux New Media do Brasil Editora Ltda. 2009. Mensal. ISSN 1806-9428.

LOSANO.M. **Introdução ao Active Directory**. Apresenta visão geral do Active Directory. Disponível em: http://technet.microsoft.com/pt-br/library/cc668412.aspx. Acesso em agosto de 2009.

MICROSOFT-1. **Simple Network Time Protocol.** Apresenta detalhes do protocolo SNTP. Disponível em: http://msdn.microsoft.com/pt-br/library/aa919019.aspx. Acesso em agosto de 2009

MICROSOFT-2. **Descrição dos protocolos do Active Directory**. Disponível em: http://technet.microsoft.com/pt-br/library/cc961766%28en-us%29.aspx. Acesso em setembro de 2009.

MINASI. M; ANDERSON. C.;SMITH. B.M;TOOMBS.D. **Dominando o Windows 2000 Server**. São Paulo. Pearson Education do Brasil. 2001. 1275 p.

MICROSOFT-3. **Apresenta as operações mestres do Active Directory**. Disponível em http://technet.microsoft.com/pt-br/library/cc716426.aspx. Acesso em dezembro de 2009.

MORIMOTO.C.E. **Redes e Servidores Linux - Guia Prático**. Porto Alegre. Sul. 2005. 302p.

POSTFIX.ORG.BR. Disponível em: http://www.postfix.org/LDAP_README.html# config. Acesso em dezembro de 2009.

RNP - REDE NACIONAL DE ENSINO E PESQUISA. **Apresenta descrição do protocolo NTP**. Disponível em: http://www.rnp.br/ntp/. Acesso em outubro de 2009.

SAMBA.ORG-1. **Samba4 / Active Directory**. Disponível em: http://wiki.samba.org/index.php/Samba4/ActiveDirectory. Acesso em: dezembro de 2009

SAMBA.ORG-2. **Apresenta informações sobre schemas e ldap**. Disponível em: http://wiki.samba.org/index.php/Samba4/LDAP_Backend. Acesso em dezembro de 2009.

SAMBA.ORG-3. **Instalação e configuração do Samba 4**. Disponível em: http://wiki.samba.org/index.php/Samba4/HOWTO#Step_1:_download_Samba4. Acesso em outubro de 2009.

SCRIMGER.R.;LASALLE.P.;PARIHAR.M.;GUPTA.M. **TCP/IP - A Bíblia**. Rio de Janeiro. Campus. 2002. 642 p.

THE OPENLDAP FOUNDATION. **OpenLdap 2.1 Administrator´s Guide**. Disponível em: http://www.bind9.net/manual/openldap/2.1/intro.html. Acesso em dezembro de 2009.

TRIGO.C.H. **OpenLDAP - Uma Abordagem Integrada**. São Paulo. Novatec. 2007. 239 p.

UFRJ. **Apresenta funcionamento do protocolo CIFS**. Disponível em: http://www.gta.ufrj.br/grad/01_2/samba/smbcifsinternamente.htm. Acesso em outubro de 2009.

Ldap Browser. Versão 2.6. Softerra. 2004.