PONTIFÍCIA UNIVERSIDADE CATÓLICA DE GOIÁS
DEPARTAMENTO DE COMPUTAÇÃO
CURSO DE ENGENHARIA DA COMPUTAÇÃO

SERVIÇOS DE DIRETÓRIO LDAP – ANÁLISE COMPARATIVA ENTRE O ACTIVE DIRECTORY E O OPENLDAP

MARCO TÚLIO RODRIGUES BRAGA

GOIÂNIA – GO
DEZEMBRO
2011

PONTIFÍCIA UNIVERSIDADE CATÓLICA DE GOIÁS
DEPARTAMENTO DE COMPUTAÇÃO
CURSO DE ENGENHARIA DA COMPUTAÇÃO

SERVIÇOS DE DIRETÓRIO LDAP – ANÁLISE COMPARATIVA ENTRE O ACTIVE DIRECTORY E O OPENLDAP

Trabalho de Projeto Final de Curso apresentado por Marco Túlio Rodrigues Braga à Pontifícia Universidade Católica de Goiás, como requisito parcial para obtenção do título de Bacharel em Engenharia da Computação, Orientadora –Prof. Ms. Angélica da Silva Nunes.

GOIÂNIA – GO
DEZEMBRO

SERVIÇOS DE DIRETÓRIO LDAP – ANÁLISE COMPARATIVA ENTRE O ACTIVE DIRECTORY E O OPENLDAP

MARCO TÚLIO RODRIGUES BRAGA

Trabalho de Projeto Final de Curso apresentado por Marco Túlio Rodrigues Braga à Pontifícia Universidade Católica de Goiás - Departamento de Computação, como parte dos requisitos para obtenção do título de Bacharel em Engenharia da Computação

Professora Angélica da Silva Nunes, Ms.	Professor Jeová Martins Ribeiro, Especialista.
Orientadora	Coordenador de Projeto Final de Curso

DEDICATÓRIA

Primeiramente a Deus, aos meus pais que tiveram a sabedoria de valorizar a formação de seu filho. Dedico-lhes esta conquista com gratidão.

“Entrega o teu caminho ao Senhor, confia Nele, e o mais Ele o fará.”

Salmos 37:5.

AGRADECIMENTOS

Ao Deus Todo Poderoso por sempre me dar sabedoria, força, determinação e discernimento em cada passo da minha vida.

A minha familia por sempre acreditar em mim e, mesmo em momentos difíceis, não me deixou desistir, sempre orando, apoiando, orientando e instruindo. Sei que sem eles não conseguiria conquistar essa vitória.

A professora Ms. Angélica da Silva Nunes, orientadora acadêmica, pelo empenho, dedicação, apoio durante a realização deste projeto.

Aos meus amigos(as) que muitas vezes deixei de sair ou me divertir para a construção deste trabalho, ou conclusão de diversas disciplinas cursadas durante a graduação ou mesmo a trabalho.

Aos profissionais que tive oportunidade de trabalhar e aprender muito em empresas como: RB (Laides dos Santos), ETERNIT (Michel Naressi, Marcelo Carvalho e Leonardo Arcuri), Palácio Pedro Ludovico Teixeira/Governo do Estado de Goías (Eliel Lima, Marcos Alves, Weber Miranda, Plinio Pierry, Denis Francis, Massahide Namba), SEFAZ-GO (Amilton, Rafael, Francis, Clodoaldo, Marcos), Minascom (Gustavo Lopes e Charbel Chalala), Politec Global IT (Jorge Eduardo e Weder Lima), Red & White IT (Fabiano Rocha e Wagner Kuramoto). Em especial aos profissionais Eliel Lima, Marcos Alves, Plinio Pierry, Weber Miranda, Amilton Rogerio, Weder Lima, Clodonil Trigo e Paulo Renato que me ajudaram a entender melhor o mundo Open Source e me fez ter a visão administrativa de uma rede em ambientes interoperaveis não deixando de lado a segurança e melhores práticas que, com toda certeza, ajudou a criar um profissional apaixonado pela tecnologia.

Aos meus amigos da faculdade que passamos por muitos momentos difíceis na faculdade, mas no fim conquistamos mais essa vitória. Também, aos veteranos amigos que me orientaram e aconselharam no inicio de minha graduação e me fizeram enxergar que realmente era a graduação em que pretendia fazer.

E por fim, aos Administradores de Redes que responderam a pesquisa cujo nome não citarei, pois, conforme prometido, manterei sigilo nas informações.

RESUMO

LDAP (*Lightweight Directory Access Protocol* - Protocolo Leve de Acesso a Diretórios) como o nome já diz é um protocolo de acesso a diretórios considerado e nomeado "leve" por ser implementado sobre a pilha TCP/IP. São apresentadas diversas ferramentas que o implementam. Foi elaborado um estudo de caso com Administradores de Redes com intuito de saber quais implementações são mais utilizadas. Foram detalhadas as ferramentas mais utilizadas em redes corporativas: Microsoft Active Directory e OpenLDAP, analisando e comparando com critérios de avaliação qualitativos entre as duas ferramentas levando em consideração questões vividas pelo administrador de redes. Por fim, foi abordada a instalação e configuração da estrutura de serviços de diretórios utilizando as ferramentas abordadas neste trabalho, tomando como referencia duas empresas fictícias de características semelhantes. Foram também desenvolvidos scripts em VB Script e Shell Script para automatizar a tarefa de criação da estrutura de diretórios proposta em cada implementação.

Palavras-chave: Serviços de Diretórios, LDAP, Active Directory, OpenLDAP, Shell Script, VB Script, TCP/IP

ABSTRACT

LDAP (Lightweight Directory Access Protocol) as the name implies is a directory access protocol considered and named "light" to be implemented over the TCP/IP. It presented several tools that implement them. It is made with a case study networks administrators with a view to know which are most widely used implementations. It will detail the most widely used in corporate networks: Microsoft Active Directory and OpenLDAP, analyzing and comparing with qualitative evaluation criteria between the two tools taking into account issues experienced by the network administrator. Finally, we discuss the installation and configuration of the structure of directory services using the tools discussed in this paper, taking as reference two fictitious companies with similar characteristics. Were also developed scripts in VB Script and Shell Script to automate the task of creating the directory structure proposed in each implementation.

Key-words: Directory Services, LDAP, Active Directory, OpenLDAP, Shell Script, VB Script, TCP/IP

SUMÁRIO

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

ACL	*Access Control List*
CAL	*Client Access License*
CCIT	*Consultative Committee for International Telegraphy and Telephony*
CIFS	*Common Internet File System*
DAP	*Directory Access Protocol*
DBM	*Database Manager*
DIT	*Directory Information Tree*
DN	*Distinguished Name*
DNS	*Domain Name System*
DSML	*Directory Services Markup Language.*
ERP	*Enterprise resource planning*
FRS	*File Replication Service*
GPO	*Groip Policy Objects*
HA	*High Availability*
IANA	*Internet Assigned Numbers Authority*
IETF	*Internet Engineering Task Force*
ISO	*International Organization Standardization*
LCUP	*LDAP Client Update Protocol*
LDAP	*Lightweight Directory Access Protocol*
LDBM	*Lightweight DBM*
LDIF	*LDAP Data Interchange Format*
LDUP	*LDAP Duplication/Replication/Update Protocols*
NSPI	*Name Service Provider Interface*
OSI	*Open Systems Interconnection*
OU	*Organizational Unit*
PDC	*Primary Domain Controler*
PDCA	*Plan, Do, Check, Act*
RDN	*Relative Domain Name*
RHEL	*Red Hat Enterprise Linux*
SASL	*Simple Authentication and Security Layer*
SMB	*Server Message Block*
SNMP	*Simple Network Managment Protocol*
SOAP	*Simple Object Access Protocol*
XML	*Extensible Markup Language*

Capítulo 1 - Introdução

Com o uso de uma grande variedade de tecnologias e aplicações no ambiente corporativo, começaram a surgir questões como redundância nos dados e controle de acesso a informações decorrentes de alterações na infraestrutura física da rede.

A partir dessas premissas, cria-se a necessidade de ter serviços de diretório, que advém do contraste entre a mudança da rede OSI (*Open Systems Interconnection* – Interconexão de Sistemas Abertos) como um todo e da necessidade de isolar (tanto quanto possível) o usuário da rede destas mudanças. Logo, um cliente de um serviço de diretório pode ver a rede OSI como uma entidade mais estável. Por exemplo, se o endereço fisico de um recurso na rede é alterado, o usuário daquele recurso não será afetado pela mudança, desde que esteja usando um nome para referenciá-lo e não um endereço físico.

Outra necessidade para um serviço de diretório advém do desejo de prover uma visão mais ergonômica da rede. Por exemplo, o uso de apelidos, o oferecimento de um serviço de "páginas amarelas", ajuda a minorar a dificuldade de encontrar e usar informação na rede [UFR11].

A CCITT (*Consultative Committee for International Telegraphy and Telephony*) e a ISO (*International Organization Standardization*) definiram um conjunto de padrões para o serviço de diretório de rede: (CCIa88) e (ISOa88) . Tais padrões especificam um sistema de diretório distribuído que atende a consultas sobre objetos da rede. O Sistema de Diretório assim definido engloba uma base de dados constituída de nomes e, para cada nome, um conjunto de propriedades a serem associadas com aquele nome. Por exemplo, dado o nome de uma pessoa, em forma apropriada, o serviço de Diretório pode devolver um endereço eletrônico ou número de telex. O serviço de diretório pode ser também usado para apoiar a definição de grupos de objetos, para autenticação de usuários e para funções de gerenciamento de redes, tais como registro da localização de aplicações [UFR11].

Quando se possui um número considerável de informações concentradas em servidores diferentes, é necessário utilizar um serviço de diretório. Tendo em vista essa necessidade, surgiram vários serviços de diretório, mas muitos eram de difícil implementação, ou não eram rápidos como um serviço de diretório deve ser.

O X.500[RFC1279] é um padrão de protocolos de serviços de diretórios, utilizados em redes de computadores, e foi elaborado para trabalhar sobre modelo OSI e incorporado ao pacote de protocolos ISO/IEC 9594[ISO01] Designado para dar suporte ao padrão X.400[RFC1405], que define a troca de mensagens eletrônicas entre os usuários da rede local,

a função do X.500 é prover serviços de diretórios para rede, centralizando a base de dados dos usuários da rede em um servidor X.500. O protocolo de acesso a diretórios DAP (*Directory Access Protocol*) faz parte das especificações do padrão X.500, e foi desenvolvido para trabalhar junto a todas as camadas do modelo OSI, com o objetivo definir o acesso de usuários aos serviços de diretórios que seu padrão provia [TEL01].

O LDAP foi criado como uma alternativa ao DAP, para prover acesso aos serviços de diretórios do X.500 pelos protocolos da pilha TCP/IP. O LDAP é mais fácil de ser implementado do que o DAP, além de exigir menos recursos da rede e de memória. Ele foi desenvolvido, e não adaptado como o DAP, para aplicações TCP/IP, obtendo, portanto, maior desempenho. Por esses motivos recebeu o nome *Lightweight Directory Access Protocol* (Protocolo Leve de acesso a Diretórios) [TEL01].

A partir daí surgem idéias das implementações dos serviços de manipulação do diretório para facilitar a administração do mesmo e adicionar novas funcionalidades que podem ser características e vantagens de cada aplicação.

A aceitação do LDAP e consequentemente a utilização foi tão grande que é um dos protocolos essenciais em redes de médio a grande porte podendo ser comparado ao uso do DNS e HTTP.

1.1. Pesquisa com Administradores de Redes

Para estudo de caso deste trabalho foi criada uma pesquisa e enviada para Administradores de Rede de empresas em Goiânia atuantes em diversos ramos de atividade com intuito de saber qual tecnologia de serviço de diretórios utilizada, suas vantagens, opiniões sobre outras implementações e complexidade de implantação, configuração e administração.

A pesquisa foi enviada por e-mail disponibilizando o Link para preenchimento do mesmo. Foram enviados para 62 Profissionais de Tecnologia da Informação sendo que apenas 12 responderam o questionário. A intenção de enviar para empresas de diversos ramos foi para expor as tendências em cada uma delas,

Nas respostas obtidas houve certa indefinição de que implementação seria melhor, pois muitos utilizavam ferramentas proprietárias, não descartando a opção de utilização para ambientes *opensource*.

Mais detalhes sobre a pesquisa é exibida a seguir.

Os ramos de atividades dos integrantes das pesquisas foram principalmente do setor governamental, conforme mostra na Figura 1.1 e na Tabela 1.1:

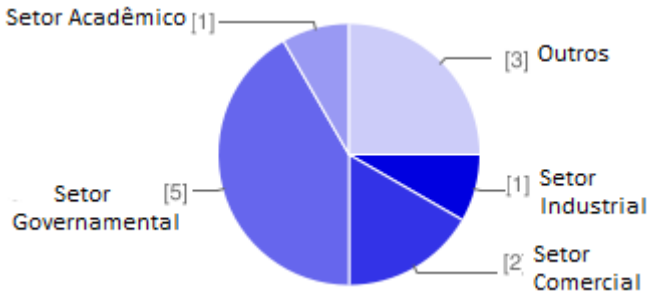

Figura 1.1 - Pesquisa - Ramo de atividade

Ramo de atividade	Respostas	Porcentagem
Setor Industrial	1	8%
Setor Comercial	2	17%
Setor Governamental	5	42%
Setor Acadêmico	1	8%
Outros	3	25%

Tabela 1.1- Pesquisa: Setor de Atuação

A quantidade média de usuários das entidades pesquisadas é apresentada na Figura 1.2 e na Tabela 1.2:

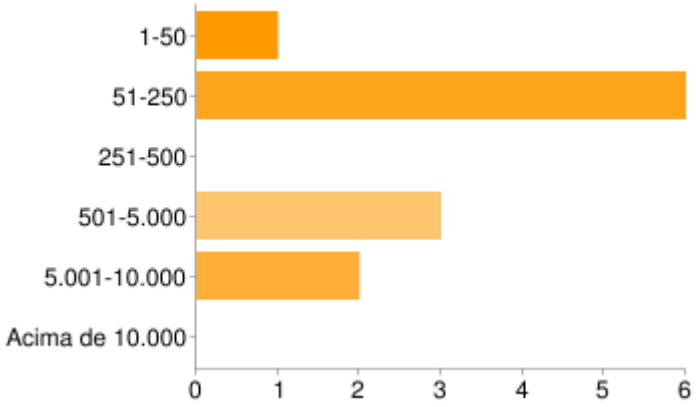

Figura 1.2 – Pesquisa: Quantidade de Usuários

Quantidade usuários	Respostas	Porcentagem
1-50	1	8%
51-250	6	50%
251-500	0	0%
501-5.000	3	25%
5.001-10.000	2	17%
Acima de 10.000	0	0%

Tabela 1.2 – Pesquisa: Quantidade de usuários

Baseado nessas informações foi questionado qual implementação de diretórios utilizada, podendo escolher dentre as principais ou informar manualmente caos não conste na lista. As respostas são apresentadas na Figura 1.3 e na Tabela 1.3:

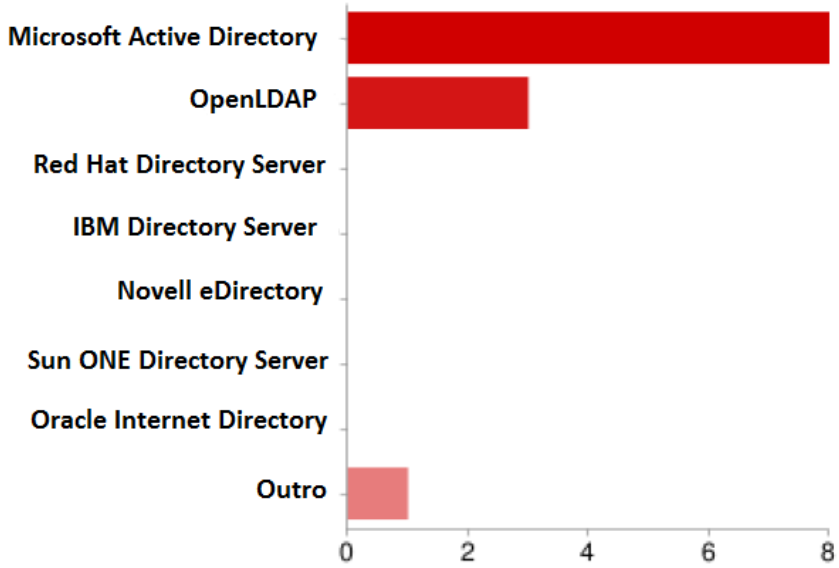

Figura 1.3 - Pesquisa - Serviços de Diretório

Implementação	Respostas	Porcentagem
Microsoft Active Directory	8	67%
OpenLDAP	3	25%
Red Hat Directory Server	0	0%
IBM Directory Server	0	0%
Novell eDirectory	0	0%
Sun ONE Directory Server	0	0%
Oracle Internet Directory	0	0%
Outros	1	8%

Tabela 1.3 – Pesquisa: Serviço de Diretório utilizado

Analisando as informações coletadas nas pesquisas pode-se verificar que a implementação mai utilizada no mercado é a da Microsoft, o Active Directory, e o OpenLDAP.

O Conteúdo desta pesquisa está disponível no Anexo I.

1.2. Motivação do Trabalho

A motivação deste trabalho foi a comparação das duas implementações de diretórios mais utilizadas no mercado. Para concretização dessa afirmação foi feito uma pesquisa com Administradores de rede, exibida no item 1.1, visando detalhar melhor as vantagens de grandes corporações utilizarem esses serviços de diretório, tanto como a possibilidade de convergência entre eles.

Existem controvérsias quanto a melhor solução de implementação de serviços de diretórios nas empresas. Fornecedores de software proprietários defendem que a sua solução é melhor porque oferece suporte 24 horas por dia enquanto os defensores do software livre defendem que não compensa investir grandes somas de dinheiro, se existem soluções equivalentes sem custo para as corporações.

Nos últimos anos, o Governo Federal tem sido um grande defensor da adoção do software livre, criando vários portais de apoio e disseminação do Software Livre, por exemplo o Portal do Software Livre[PSL01], o Guia Livre[PSL05] que oferece alternativas livres de softwares para servidores e desktops, inclusive para serviços de diretórios outro portal é o CDTC (Centro de Difusão de Tecnologia e Conhecimento)[PSL02] que oferece diversos

cursos para a comunidade [PSL03] e para funcionários públicos[PSL04] e por fim o portal de Softwares Publico do Governo Federal[PSL06], que oferece diversos softwares homologados pela comunidade brasileira e desenvolvido e utilizado em diversos órgãos públicos.

1.3. Objetivo do trabalho

O objetivo deste trabalho é apresentar os serviços de diretórios LDAP abordando e apresentando as funcionalidades de duas das principais implementações utilizadas em ambientes corporativos, educacionais, governamentais, dentre outros.

Serão instaladas e configuradas duas ferramentas de diretório, uma proprietária e outra livre, com intuito de comparação e apresentação de suas vantagens e funcionalidades. Também serão criadas duas empresas fictícias com características semelhantes para estes testes.

Para análise e comparação das ferramentas, serão definidos critérios para comparação qualitativa entre eles, levando em consideração questões vividas pelo administrador de redes. Esses critérios serão criados para comparação das duas ferramentas implantadas procurando determinar pontos positivos e negativos de cada uma.

1.4. Estrutura da Monografia

O trabalho está estruturado da seguinte forma:

No Capitulo 01 é apresentado a introdução sobre este trabalho, como também a motivação para estudo de serviços de diretório.

No Capitulo 02, são apresentados conceitos sobre serviços de diretório e em seguida apresentado detalhadamente o protocolo LDAP juntamente com suas características, vantagens e recursos do protocolo.

No Capitulo 03, são apresentados os serviços de diretórios mais comuns, detalhando as implementações de estudo de caso para este trabalho, OpenLDAP e Active Directory, apresentando as vantagens e recursos de cada implementação.

No Capitulo 04, descreve-se um ambiente fictício de exemplo de um diretório LDAP, e em seguida a implementação detalhada utilizando as aplicações OpenLDAP e Active Directory baseado-se no ambiente proposto.

Na conclusão são apresentados os resultados obtidos com os estudos de caso das implementações do LDAP e também a sugestão de trabalhos futuros.

No Anexo I contém a pesquisa feita com Administradores de redes sobre a utilização dos serviços de diretório.

No Anexo II, é apresentado a instalação do OpenLDAP e SAMBA. Este anexo é dividido em duas partes, sendo elas respectivamente: Instalação SAMBA e instalação OpenLDAP.

No Anexo III, é apresentado a configuração e integração do SAMBA e OpenLDAP. Este anexo é dividido em três partes: Configuração SAMBA como Controlador de Domínio, Instalação do OpenLDAP e populando a Base.

- A configuração do SAMBA foi adequado ao ambiente deste trabalho;
- A configuração do OpenLDAP foi adequado para o domínio abordado neste trabalho, porém com dicas de conversão para a nova funcionalidade do OpenLDAP utilizando *realtime*;
- Na população da base são abordadas ferramentas de visualização e administração da arvore para facilitar a administração.

No Anexo IV, são apresentados todos os pré-requisitos de configuração e boas praticas de preparação do ambiente, servidor, para instalação do Active Directory.

No Anexo V, é apresentado o script desenvolvido na linguagem VB Script para automatizar a tarefa de criar o ambiente para estudo de caso deste trabalho, porém este script não foi criado apenas para essa finalidade, a principal finalidade foi abordar outras maneiras, além das ferramentas administrativas da Microsoft, de manipular o serviço de diretório Active Directory, Muito útil, quando é necessário fazer inserções em massa, por exemplo, em migrações de diferentes plataformas de serviços de diretórios.

No Anexo VI, é apresentado o script desenvolvido na linguagem Shell Script que gera arquivos LDIF (*LDAP Data Interchange Format)* contendo a estrutura do Diretório no ambiente proposto, adicionando essas informações na Base e também gerando um *log* com informações de tempo de execução do mesmo.

Capítulo 2 - Serviços de diretórios LDAP

Este capitulo descreve o que é um serviço de diretório, serviços de diretórios existentes, o protocolo LDAP, conceitos e nomenclaturas e recursos oferecidos pelas implementações deste protocolo.

2.1. Conceitos de diretórios

O conceito de diretórios muitas vezes pode parecer confuso, mas basicamente ele pode ser entendido como uma “lista”.

Os diretórios são utilizados constantemente no dia a dia, muitas vezes sem perceber. Alguns exemplos desses diretórios são catálogos de lista de telefones, catálogos de compras, dicionário, etc. Esses diretórios são tipicamente chamados de diretórios *off-line*. Como exemplos de diretórios *on-line* temos o DNS, NIS, Catalogo de endereços de clientes de e-mail, arquivos de senhas e grupos (sistemas UNIX), arquivo *host* (sistemas UNIX e Windows).

Para um melhor entendimento do uso de diretórios nas listas telefônicas, elas são divididas em duas partes: páginas brancas (*white pages*) e páginas amarelas (*yellow pages*). As páginas brancas são utilizadas quando se tem um nome e deseja-se encontrar determinadas informações, no caso o numero de telefone e/ou endereço. Nas páginas amarelas deste exemplo, tem-se apenas um atributo especifico, o ramo de atividade, e deseja-se encontrar uma lista de pessoas ou empresas que estão organizadas por esse atributo.

2.2. Serviços de Diretório

Serviço de diretórios é um serviço de armazenamento de informações otimizado para busca e leitura. Eles também podem armazenar informações adicionais nos atributos para facilitar ou suportar alguns mecanismos de filtragem.

Os serviços de diretório *on-line* tem algumas vantagens em relação aos *off-lines*, as principais são: dinâmicos, flexíveis e também podem ser seguros e personalizados

Existem também diferentes tipos de diretórios, Timothy[HOW03] as dividiu nas seguintes categorias:

- Diretórios de aplicações especificas: Estes diretórios são criados para atender as necessidades de aplicações especificas. Por exemplo: Catálogos de endereços do Microsoft Exchange;

- Sistemas operacionais de redes (NOS) baseados em diretórios: Diretórios como eDirectory da Novell (atualmente chamado de NDS - *Netware Directory Services*), Microsoft *Active Directory*;
- Diretórios de propósitos específicos: Estes não são vinculados a aplicações e são projetados para propósitos específicos, eles também não são extensíveis. O DNS[RFC1034] e o SNMP[RFC1157] fazem parte dessa categoria;
- Diretórios de propósitos gerais: Estes são desenvolvidos para servir as necessidades de uma ampla variedade de aplicações. Exemplos são o LDAP, detalhado neste trabalho, e também os diretórios X-500.

Entendendo as diferenças de diretórios on-line e off-line como também os diferentes tipos de diretório é possível detalhar melhor os diferentes tipos de serviços de diretórios existentes.

2.3. Diversos serviços de diretórios atuais

Os RFCs (*Request for Comments*) são documentos que descrevem padrões de protocolos e são criados e disponibilizados pela comunidade da *Internet*.

Existem diversos RFCs que definem os serviços de diretórios e o protocolo LDAP, como por exemplo:

- RFC 1487 - X.500 Lightweight Directory Access Protocol [RFC1487];
- RFC 1777 - Lightweight Directory Access Protocol [RFC1777];
- RFC 2251 - Lightweight Directory Access Protocol (v3) [RFC2251];
- RFC 2252 - Lightweight Directory Access Protocol (v3): Attribute Syntax Definitions [RFC2252];
- RFC 2253 - Lightweight Directory Access Protocol (v3): UTF-8 String Representation of Distinguished Names [RFC2253];
- RFC 2254 - The String Representation of LDAP Search Filters[RFC2254];
- RFC 2255 - The LDAP URL Format [RFC2255];
- RFC 2256 - A Summary of the X.500(96) User Schema for use with LDAPv3 [RFC2256];
- RFC 3377 - Lightweight Directory Access Protocol (v3): Technical Specification [RFC3377];

Cada RFC descreve as funcionalidades e características que o serviço de diretório LDAP oferece.

Não é possível começar a falar de serviços de diretórios sem citar um dos serviços de diretórios mais bem sucedidos já implementados na *Internet*, o DNS. O DNS global compartilha muitas características que um serviço de diretório deve prover de maneira geral, são elas:

- Um serviço de diretório é eficaz para leituras;
- Um serviço de diretório implementa um modelo distribuído;
- Um serviço de diretório pode aumentar os tipos de informações que armazenam;
- Um serviço de diretório tem serviços de busca avançados.

O DNS é altamente otimizado para o seu objetivo principal, a maioria dos diretórios são de propósito geral. O DNS é um conjunto especializado de esquemas fixos; diretórios permitem esquemas extensíveis. Os servidores DNS tipicamente não permitem atualização de seus *schemas*; diretórios permitem. O DNS pode ser acessado através do protocolo de transporte não orientado a conexão; diretórios normalmente são acessados por protocolos de transporte orientados a conexão.

2.4. O que é o LDAP?

LDAP significa *Lightweight Directory Access Protocol* - Protocolo Leve de Acesso a Diretórios. Como o nome sugere, é um protocolo leve para acessar serviços de diretórios, mais especificamente serviços de diretórios baseados em X-500. LDAP roda em cima da pilha TCP/IP e outros serviços de transporte orientados a conexão [OPE01].

É comum ouvir alguém se referir a um servidor LDAP ou uma árvore LDAP. O LDAP, de fato, oferece uma visão dos dados em forma de árvore, e é a essa visão em forma de árvore que as pessoas se referem quando falam de um servidor LDAP. É suficiente pensar no LDAP como um protocolo cliente/servidor, baseado em mensagens que são definidas, principalmente, no RFC 2251[RFC2251]. O LDAP é assíncrono, o que significa que um cliente pode emitir solicitações múltiplas e respostas a essas solicitações podem chegar em uma ordem diferente da qual foram emitidas [CAR09].

O LDAP pode ser dividido em modelos que representam os serviços prestados pelo servidor, como visto por um cliente.

2.5. Modelos LDAP

Como descrito no item 2.4, os modelos descrevem ou representam os serviços prestados pelo servidor. O [RFC 2251] divide o protocolo em dois modelos: modelos de protocolo e modelos de dados:

- Modelos de Protocolo: Os clientes podem enviar mensagens ao servidor de forma assíncrona, o servidor recebe as mensagens, as processa e retorna a resposta contendo o resultado ou erros ao cliente solicitante;
- Modelos de Dados: Descreve como os dados devem ser organizados na árvore de informações do diretório (DIT – *Directory Information Tree*). Esta árvore contém diversas entradas que são chamadas de nomes distintos relativos (RDN - *Relative Domain Name*), eles são únicos em determinados pontos da árvore, que por sua vez pode ser identificado unicamente até a raiz. O atributo responsável por essa identificação é o DN (*Distinguished Name* - Nome Distinto).

Alguns autores também dividem esses modelos mais detalhadamente. Howes [HOW03] divide o protocolo em quatro modelos:

- Modelo de informação: Oferece as estruturas e os tipos de dados necessários para construir a árvore de um diretório LDAP. Uma entrada é uma unidade básica em um diretório LDAP. Uma entrada contém informações sobre uma ocorrência de uma ou mais Classes de objetos. Essas classes de objetos têm certos atributos exigidos ou opcionais. Os tipos de atributos definem as regras de codificação e comparação que controlam coisas como o tipo de dados que o atributo pode conter e como comparar esses dados durante uma busca;
- Modelo de nomes: O Modelo de nomes define como as entradas e dados na DIT e são referenciados de maneira única. Cada entrada tem um atributo que é único entre todos os irmãos no mesmo pai, chamado de RDN. É possível identificar de maneira única qualquer entrada em um diretório seguindo os RDNs de todas as entradas no caminho do nó desejado até a raiz da árvore. Esse fio criado pela combinação de RDNs para formar um nome único é chamado de nomes distinto do nó (DN);
- Modelo funcional: O modelo funcional é o protocolo LDAP em si. Esse protocolo fornece o meio para acessar os dados na árvore do diretório. O acesso é implementado por operações de autenticação (ligações), operações de consulta (pesquisa e lê) e operações de atualização (grava);

- Modelo de segurança: O modelo de segurança fornece um mecanismo para que os clientes se identifiquem (autenticação) e para que o servidor controle o acesso do cliente aos dados (autorização). O LDAPv3 oferece diversos métodos de autenticação não disponíveis em versões anteriores do protocolo. Alguns recursos, como as listas de controle de acesso, ainda não foram padronizados, deixando os fornecedores com seus próprios dispositivos.

Essa divisão do protocolo LDAP em módulos, facilita o entendimento, funcionamento e até o comportamento de ferramentas e aplicações que o implementam.

2.6. Protocolo LDAP

Como apresentado até a seção 2.5 dessa monografia, o protocolo LDAP oferece vários recursos na autenticação de usuários. Isso pode se explicar porque é um dos serviços de diretórios mais utilizados atualmente, conforme apresentado na Introdução. Nos itens a seguir são apresentadas algumas definições deste protocolo.

O 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 [TRI07].

Além de oferecer acesso rápido e fácil a serviços de diretório, o LDAP oferece suporte transparente ao TCP/IP, sendo então uma escolha adequada para o ambiente de *Internet* e, aceito como padrão para serviços de diretório [GUP02].

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.

A organização é feita de forma hierárquica onde, a partir da raiz podem-se chegar aos recursos: computadores, servidores, usuários, grupos, etc. É uma árvore de nós, similar a forma como o DNS funciona, conforme é apresentado na Figura 2.1[MAC06] e Figura 2.2.

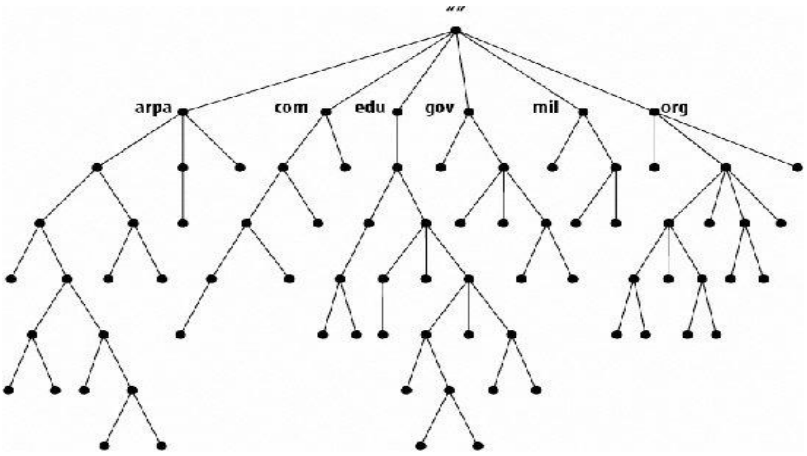

Figura 2.1 - Estrutura do espaço de nomes do DNS

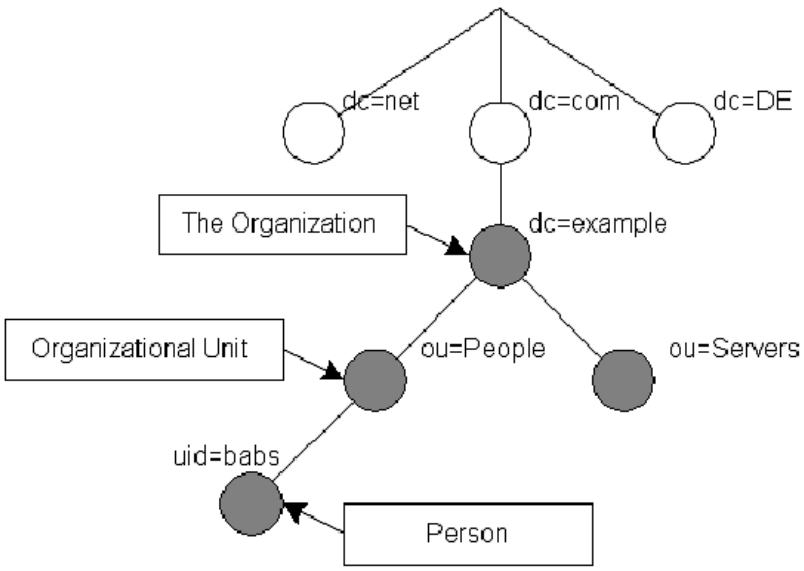

Figura 2.2 - Estrutura do Protocolo LDAP

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 mnemônicos para definir os nomes dos atributos e as entradas [TOP03].

Utilizando o protocolo LDAP é possível que uma serie de aplicativos de rede utilizar a mesma base, facilitando o papel do administrador de rede. Porém, também existe o outro lado,

se alguém descobrir a senha de outro usuário é possível ter acesso a diversos tipos de aplicativos, dependendo do nível de acesso deste e da habilidade do invasor é possível trazer diversos problemas a rede, como perdas de arquivos confidenciais e indisponibilidade de serviços.

2.7. LDIF e DSML

Como na maioria das bases de dados o LDAP também possui linguagens de manipulação dos dados na base, que são o LDIF e o DSML (*Directory Services Markup Language).*

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 [TRI07].

O formato LDIF é usado para transferir informações de diretório, ou uma descrição de um conjunto de alterações feitas às entradas de diretório. Um arquivo LDIF consiste de uma série de registros separados por linha. Um registro consiste em uma sequência de linhas descrevendo uma entrada de diretório, ou uma sequência de linhas que descrevem um conjunto de alterações em uma entrada no diretório. Um arquivo LDIF especifica um conjunto de entradas de diretório, ou um conjunto de mudanças a serem aplicadas às entradas de diretório[RFC 2849].

Um arquivo LDIF é composto basicamente por:

- Um conjunto de entradas separadas umas das outras por linhas em branco;
- Um mapeamento de nomes de atributo a valores;
- Um conjunto de diretivas que instruem o analisador como processar a informação.

Esses arquivos no formato LDIF podem ser utilizados para importar, exportar, atualizar, excluir, dados no diretório de dados . A criação e atualização desses arquivos normalmente consome grande parte do tempo do administrador de redes. Por isso é importante tomar cuidado quanto à sintaxe do LDIF:

- Os comentários devem começar com símbolo “#” na primeira posição da linha que continuará até o final da linha em que está posicionado;
- Os atributos devem estar do lado esquerdo do sinal de dois pontos “:”, e os valores dos atributos do lado direito separado do sinal com espaço. Ex.: dn: dc=exemplo;
- O atributo dn identifica unicamente o DN da entrada.

O Exemplo 2.9.1, item 2.9, apresenta um exemplo de arquivos LDIF.

O LDAP também tem outra linguagem de marcação de dados, o DSML, descrita a seguir:

O DSML v2 é projetado para fornecer métodos para representar consultas, atualizações e as respostas do LDAP a essas operações em XML (*Extensible Markup Language*). Isso significa que é possível para dispositivos pequenos e integrados acessar os serviços LDAP sem confiar na biblioteca de clientes LDAP; eles só precisam da habilidade de analisar o arquivo XML[CAR09].

O DSML ainda não é muito utilizado, mas pode ser bem útil em aplicações para dispositivos que dispõem de menos poder de processamento [CAR09].

2.8. Schemas e atributos

2.8.1 Schemas

Cada elemento do esquema é identificado por um identificador exclusivo globalmente chamado de: *Object Identifier* (OID). OIDs são usados também para identificar outros objetos. Em particular eles são muito utilizados pelo protocolo SNMP (*Simple Network Managment Protocol*). Como os OID são hierárquicos, a organização pode obter um OID e ramo conforme necessário [TOP03].

Os *schemas* servem para definir os objetos e atributos e os tipos de dados que serão armazenados em cada atributo. Como dito anteriormente cada *schema* possui um número de controle, OID, identificado universalmente. Caso haja a necessidade de criar um novo *schema* que precise ser publicamente identificado, é preciso solicitar com a entidade responsável por manter esses identificadores, no caso a IANA (*Internet Assigned Numbers Authority*).

É possível fazer uma simples comparação com o DNS, por exemplo, para publicação de um dominio cujo escopo seja apenas a rede interna, basta criar no servidor de nomes esse domínio. Mas caso o escopo do domínio seja a *Internet*, é preciso adquirir um domínio em uma entidade responsável e reconhecida pela IANA.

2.8.2 Atributos

A raiz e os ramos da árvore são diretórios. Cada diretório pode conter outros diretórios ou elementos que são chamados de entradas; cada entrada possui um ou mais atributos que, por sua vez, podem ter um ou mais valores associados a eles, todos de acordo com um tipo de dado predefinido [TRI07].

Os atributos e regras de sintaxe são similares a declarações de tipo de variável ou de dados encontradas e diversas linguagens de programação. Mas a comparação não é tão parecida. Nas linguagens de programação quando uma variável recebe um valor diferente duas vezes, de forma geral é valida o último, no LDAP esse atributo é adicionado a uma lista de atributos disponíveis no objeto. É como se fosse atributos multivalorados, porém, vale lembrar que não são todos os atributos que permitem isto, por exemplo, o uid não permite, já o telephoneNumber tem esse recurso.

2.9. Espaço de Nomes (Nomenclatura)

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 mnemônicos para definir os nomes dos atributos e as entradas [TOP03].

O DN deve sempre indicar todos os ramos da árvore LDAP, desde a base até a parte final, a identificação do objeto propriamente dita. [SUN07].

Essa utilização de mnemônicos é herdada do padrão X.500. Para diretórios, por exemplo, são encontrados os seguintes atributos:

Atributo	***Descrição***
C	Para diretórios que representam países (*coutry*)
O	Para o nome da Empresa (*organization*)
Ou	Para departamento (*organizational unit*)

Tabela 2.1 – Atributos para diretórios

Para as entradas , por exemplo, os seguintes atributos são válidos:

Atributo	**Descrição**
Cn	Atributo de nome (*common name*)
Uid	Identificador do usuário, ou nome de usuário (*user ID*)
Gn	Para o nome próprio de uma pessoa (*given name*)
Sn	Para o sobrenome de uma pessoa (*surname*)
Mail	Para o e-mail de uma pessoa

Tabela 2.2 – Atributos para entradas

O conjunto desses atributos para entradas formam os nomes distintos relativos - RDN.

Se o DN é como o caminho absoluto entre a raiz de um sistema de arquivos e um arquivo, um nome distinto relativo (RDN) é como um nome de arquivo. Um DN é formado pela combinação de RDNs de toda entidade indo do elemento em questão à raiz da árvore de diretório [CAR09].

Neste sentido, um RDN funciona de maneira similar ao nome de arquivo. Entretanto, ao contrário do nome de arquivo, um RDN pode ser composto de múltiplos atributos. Isso é similar a um índice composto em um sistema de banco de dados relacional em que dois ou mais campos são utilizados em combinação para gerar uma chave única de índice [CAR09].

Segue abaixo o Exemplo 2.9.1 da criação de uma nova DIT:

```
dn: dc=mtulio,dc=eng,dc=br
objectClass: top
objectClass: dcObject
objectClass: organization
dc: mtulio
o: MTulio ENG
```

Note que o valor de DN identifica esse objeto em toda árvore, como dito anteriormente.

Todas as entradas de um diretório LDAP devem ter um atributo objectClass, e esse atributo deve ter pelo menos um valor. Múltiplos valores para o atributo objectClass são possíveis e comuns, dadas certas exigências. Cada valor de objectClass atua como um modelo para os dados a serem armazenados em uma entrada. Isso define uma série de atributos que precisam estar presentes na entrada e uma série de atributos opcionais que podem ou não estarem presentes [CAR09].

No exemplo anterior é possível notar também que o atributo objectClass tem mais de uma definição, isso é chamado de atributo multivalorado.

Os atributos podem ter um valor exclusivo ou valores múltiplos. Uma instância de um atributo de valor exclusivo só pode conter um único valor. Uma instância de um atributo multivalorado pode conter vários valores de sintaxe uniforme. Um atributo multivalorado não armazena informações sobre como ordenar os atributos que contém. Cada valor de um atributo multivalorado deve ser exclusivo [MIC11].

Todas as informações dentro de uma entrada de diretório são armazenadas como pares atributo-valor. O conjunto de atributos que podem aparecer em uma determinada entrada é estabelecido pelo seu objectClass. Alguns dos atributos são obrigatórios, mas a maioria são opcionais. Novos atributos podem ser definidos, se necessário, e novas classes de objeto também pode ser adicionado para permitir que os novos atributos apareçam em entradas. [FIN05]

Andrew [FIN05] divide os atributos em vários grupos, são eles:

- Atributos de nomes: estes definem os nomes dos objetos apresentados no mundo real e são constantemente utilizados para pesquisa;
- Atributos descritivos: fotos, textos descritivos;
- Atributos Postal: estes lidam com a localização física e entrega de objetos físicos;
- Atributos de telecomunicações: números de telefone, endereços de e-mail, etc;
- Atributos de autenticação: nomes de usuários, senhas, identificadores únicos, os dados do Samba e Kerberos, certificados X.509;
- Atributos de gerenciamento: os proprietários, gerentes, listas de controle de acesso.

A RFC2253 descreve um protocolo de acesso ao diretório que fornece leitura e atualização de acesso. As atualizações requerem acesso seguro e autenticado.

2.10. Autenticação

As aplicações de rede utilizam frequentemente o LDAP para suporte a autenticação. Na forma básica, é apresentado um usuário e senha para que seja feita uma operação de busca no LDAP: se a busca é executada com sucesso, então a senha está correta. *Schemas* mais seguros envolvem Kerberos ou também são suportados certificados X.509. A maioria das aplicações definem um conjunto de regras, cada uma com permissões para certas coisas, e atribuem usuários à estas regras. Isso pode ser representado utilizando-se atributos multi-valorados no diretório LDAP.

O processo de autenticação é utilizado para estabelecer os privilégios do cliente para cada sessão. Todas as pesquisas, consultas etc., são controladas pelo nível de autorização do usuário autenticado [CAR09].

A autenticação por um diretório LDAP é chamada de vinculação. A maioria dos usuários está acostumada a fornecer um nome de usuário e senha ao se conectar a um sistema. Ao se autenticar um cliente LDAP, o nome de usuário é especificado como um DN. As credenciais utilizadas para autenticar essa entrada são dadas pelo valor do atributo *userPassword* [CAR09].

Carter [CAR09] também apresenta as seguintes especificações do LDAPv3 que definem variados mecanismos para autenticação de clientes:

- Autenticação Anônima;
- Autenticação Simples

- Autenticação Simples sobre SSL/TLS
- Autenticação Simples e Camada de Segurança (SASL - *Simple Authentication and Security Layer*)

2.11. Pesquisa

As pesquisas são realizadas por meio de critérios de busca, podendo determinar em qual parte da árvore será realizada (com isso, o tempo de resposta do LDAP melhora consideravelmente). Também é possível pesquisar na árvore toda [TRI07].

As pesquisas nas bases LDAP podem ser realizadas de diversas formas; a mais comum é a consulta anônima, sem a identificação de quem está solicitando os dados [SUN07].

O protocolo LDAP define diversos tipos de filtros de pesquisa no servidor LDAP, esses filtros são detalhados no [RFC2254].

2.12. Replicação

Em uma empresa é comum a existência de mais de um servidor de autenticação ou de consulta de dados [SUN07].

A replicação da Base apresenta diversas vantagens e esse recurso é disponível nas principais implementações do LDAP.

Clodonil [TRI07], apresenta os dois principais programas para replicar a base de dados no OpenLDAP.

- O Slurpd:
    - Trabalha com o modelo *stateless*. Isto quer dizer que o servidor é responsável pela réplica. De acordo com o *status* da réplica e do arquivo de log;
    - Trabalha no modelo incremental. Apenas as mudanças feitas depois da última sincronização serão transmitidas;
    - O servidor que inicia a réplica;
    - Trabalha apenas com sincronização baseada em evento.
- O syncrepl:
    - Ttrabalha no modelo *stateful*. Neste modelo, a ação de replicar é baseada no status da réplica;
    - Trabalha no modelo de sincronização completo – é feita a réplica de todas as alterações e as diferenças entre o *master* e o *slave*;

- A réplica é iniciada pelo cliente (backup);
- Trabalha com períodos determinados de sincronização ou sincronização baseada em eventos.

Como o OpenLDAP, no Microsoft Active Directory Server também é possível efetuar réplicas. Existem basicamente dois tipos de réplicas [TFA11]:

- *Active Directory Intrasite Replication;*
- *Active Directory Intersite Replication;*

O Grupo de Trabalho de Protocolos de Duplicação/Replicação/Atualização do LDAP (LDUP - LDAP Duplication/Replication/Update Protocols) [LDU11] do IETF tentou definir um protocolo de replicação padronizado que permitiria a interoperabilidade entre todos os servidores em conformidade com o LDPAv3. No entanto, segundo Carter [CAR09]: "parece haver mais demanda por um protocolo de atualização de cliente LDAP (LCUP - *LDAP Client Update Protocol* [LCU00]) que permitirá os clientes sincronizar um cachê local de um diretório bem como ser notificado sobre atualizações.".

2.13. Importâncias de estruturação da base

Quando considerar a criação de uma base LDAP para servir mais do que uma aplicação, é importante obter a maior visão possível da organização e suas futuras necessidades. Isso é importante pois uma simples alteração na forma da DIT num determinado estágio de projeto pode ser difícil de ser implementada, uma vez que podem existir dados na DIT e aplicações funcionando [FIN05].

Em outras palavras, em certos casos, na construção de uma DIT é necessário conhecer as regras de negocio da instituição a qual se destina o serviço de diretórios desenhado.

Findlay [FIN05], apresenta três princípios básicos para projetos LDAP, são eles:

- Evitar renomear as coisas;
- Não modificar as definições dos esquemas padrões;
- Cuidado com as Classes de Objetos Estruturais.

Durante o processo de estruturação do diretório LDAP é importante que o administrador de redes considere todas as necessidades e o planeje cuidadosamente desde o início, pois uma reorganização posterior da DIT é muito difícil. Organizações sofrem alterações constantemente, e estas alterações devem ser possíveis de serem realizadas sem requerer grandes alterações no diretório [FIN05].

O maior benefício em compartilhar dados entre aplicações é colocá-los num diretório, mas um estudo cuidadoso é necessário e algumas ferramentas de gerenciamento provavelmente irão ser necessárias [FIN05].

Capítulo 3 - OpenLDAP e Active Directory (implementações LDAP)

3.1. Introdução

Esta seção explorará conceitos que podem ser encontrados também nas documentações do LDAP.

O LDAP além de ser protocolo de acesso que define um conjunto de mensagens para acessar certos tipos de dados, porém ele não diz nada a respeito de onde ou como os dados serão armazenados.

Um servidor LDAP é uma aplicação que implementa o lado servidor conforme as especificações do protocolo. Existem diversas implementações. Adiante será descrito o OpenLDAP, uma solução livre, e o Active Directory, solução proprietária. É esse servidor que fornece o serviço de diretório aos seus clientes. Um servidor LDAP está para o diretório assim como o SGBD (Sistema Gerenciador de Banco de Dados) está para o banco de dados.

O diretório é representado através de um *backend*, que é uma implementação de base de dados. O servidor pode usar qualquer *backend* para armazenar as informações, desde arquivos de texto até bancos de dados relacionais. O protocolo LDAP (e conseqüentemente o servidor LDAP) não suporta algumas características dos bancos de dados, pois o protocolo não possui as mensagens para usar essas características e, sendo assim, não requer que o *backend*, que armazena os dados, a tenha. A Figura 3.1 ilustra basicamente o funcionamento do servidor LDAP e o armazenamento das informações.

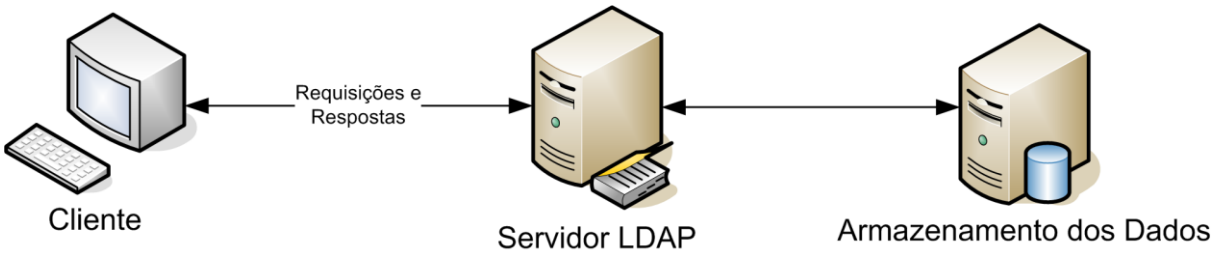

Figura 3.1 – Relacionamento entre o cliente LDAP, servidor LDAP e *backend*

O cliente não terá (ou pelo menos não deveria ter) informações a respeito do mecanismo de armazenamento que está sendo usado. Assim sendo, clientes e servidores LDAP podem se comunicar, independentemente da linguagem que foi desenvolvido ou plataforma operacional que está sendo executada.

Por exemplo, na utilização do servidor LDAP como *backend* para um servidor Web, todos os HTML's e os arquivos gráficos ficariam armazenados no diretório para serem lidos por vários outros servidores Web. Afinal, um servidor Web normalmente somente lê arquivos

e os manda para seus clientes; e esses arquivos não mudam com muita freqüência. Apesar de ser possível implementar um servidor Web que use LDAP, já existe um tipo especial de diretório para servir arquivos, chamado sistema de arquivo. Neste caso o sistema de arquivos seria o *backend* do servidor Web.

O LDAP foi criado para atender certa gama de problemas, não sendo destinado a substituir diretórios especializados, por exemplo o Sistemas de Arquivo e o DNS.

3.2. Implementações do protocolo LDAP

No mercado existem diversas implementações do LDAP, algumas livres e a maioria proprietária. Seguem alguns exemplos :

- Novell Directory Server (NDS) ou Novell eDirectory ;
- Microsoft Active Directory (AD);
- Red Hat Directory Server / Fedora Directory Server (FDS);
- OpenLDAP;
- IBM Directory Server;
- Sun ONE Directory Server;
- Oracle *Internet* Directory.

Existem inúmeras implementações e não seria possível detalhar todas aqui.

Como foi apresentado até aqui, o protocolo LDAP é flexível e extensível, possibilitando a criação e desenvolvimento de novas funcionalidades ou módulos ao LDAP que podem ser utilizados, por exemplo, para atender a necessidade de uma aplicação de uma empresa.

Este trabalho apresentará duas implementações são as mais utilizadas em redes de computadores: Microsoft Active Directory e OpenLDAP.

3.3. Interoperabilidade

Umas das maiores vantagens do LDAP é seu potencial em consolidar diretórios específicos de fornecedores ou de aplicativos. O LDAP minimiza problemas de interoperabilidade. As características principais do LDAP estão padronizadas, mas algumas coisas, como os esquemas, não estão. Existem muitas classes de objetos comuns e atributos que podem ser estendidos por um fornecedor. Não apenas esquemas podem ser estendidos: o protocolo pode ser estendido também com a criação de operações adicionais utilizando extensões e controles, os quais nem todos os fornecedores suportam.

Para cada serviço que pode ser consolidado em um diretório LDAP, deve haver um aplicativo correspondente do lado cliente que possa acessar as informações no novo diretório.

3.4. OpenLDAP

Idéias conceituais precisam de implementações concretas a fim de solidificar o entendimento sobre elas. Um protocolo de acesso de diretório é inútil sem uma implementação que permita colocar o protocolo em funcionamento para resolver problemas de informações reais em uma rede. O servidor OpenLDAP é atraente por várias razões:

- O código fonte do LDAP está disponível para download sob a licença OpenLDAP *Public License*. O código fonte pode fornecer uma grande quantidade de informações para suplementar a documentação existente;
- O OpenLDAP é compatível com as especificações principais do LDAPv3;
- O OpenLDAP está disponível para plataformas múltiplas, incluindo Linux, Solaris, Mac OS 10.2 e Windows (e suas várias variantes);
- O projeto do OpenLDAP é uma continuação do servidor de LDAP original da Universidade de Michigam;
- Suporte a IPv6 desde a implementação do LDAPv3;
- Autenticação e segurança com o serviço slapd (responsável pelo LDAP no servidor) que suporta serviços de forte autenticação através do uso do SASL[RFC4422]. A implementação SASL do slapd utiliza o software Cyrus SASL[CYR01] o qual suporta um grande número de mecanismos: DIGEST-MD5, EXTERNAL, GSSAPI;
- Segurança da Camada de Transporte com slapd fornecendo proteções de privacidade e integridade através do uso do TLS (ou SSL);
- O slapd contém diversas bases de dados backend disponíveis, permitindo a escolha da base que mais se adapta a solução pretendida. Entre os bancos alguns deles são:
    - Berkeley's Data Base (BDB) – A BDB é uma biblioteca de base de dados Open Source que provê escalabilidade, alta performance, transações protegidas por serviços de gestão de dados para aplicações [ORA11];
    - LDBM: O LDBM [IBM11] (*Lightweight DBM*), baseado em DBM (*Database Manager*), é um *backend* de propósito geral que pode

armazenar qualquer tipo de informações de diretório. Um banco de dados ldbm é implementado através do GNU Database Manager ou do pacote softaware Sleepycat Berkeley DB;

- Passwd: O *backend* passwd é um meio rápido e injusto de fornecer uma interface de diretório ao arquivo passwd do sistema Linux [CAR09];
- Shell: A diretiva de *backend* shell permite o uso de banco de dados alternativos e externos. A diretiva deixa especificar programas externos que são exigidos para cada uma das operações principais.

- O Slapd é altamente configurável através de um único arquivo de configuração (slapd.conf), a partir do qual é possível efetuar as alterações pretendidas e adaptar o Serviço ao sistema.

Outras funcionalidades do OpenLDAP é que ele foi projetado para trabalhar com threads, suportando pthreads do padrão POSIX e uma serie de outras variedades.[TOP03]

O *daemon* `slapd` suporta TCP Wrappers (filtros de controles de acesso a nível de IP), uma vez que o mesmo esteja pré-instalado. O uso de TCP Wrappers é recomendado para servidores que contém informações não publicas [UIS2011].

3.5. Microsoft Active Directory Domain Services

Muitos livros foram escritos sobre o planejamento, implementação e suporte do Active Directory. Stan [REI03], Jill [SPE06] [HOL03] são alguns deles.

O serviço de diretório Active Directory fornece um ponto único de serviços de gestão de rede, permitindo adicionar, remover, realocar usuários e recursos facilmente. O Active Directory fornece um método para um projeto de estrutura de diretórios que atenda as necessidades da organização [SPE06].

3.5.1 Características do Active Directory

Jill [SPE06] também descreve algumas características do Active Directory:

- **Armazenamento de dados centralizado:** Todos os dados no Active Directory estão presentes em um único repositório de dados, distribuído, permitindo aos usuários acesso fácil às informações de qualquer local. Um único repositório de dados distribuído requer menos administração e duplicação de esforços e assim melhora a disponibilidade e organização dos dados;

- **Escalabilidade**: O Active Directory permite a organização do diretório para atender aos requisitos de negócio e de rede através da configuração de domínios e árvores e a inserção de outros controladores de domínio. O Active Directory permite milhões de objetos por domínio ele utiliza a tecnologia de indexação e técnicas avançadas de replicação para o desempenho e velocidade;
- **Extensibilidade:** a estrutura do banco de dados do Active Directory (os esquemas) pode ser expandida para permitir tipos de informações personalizadas;
- **Gerenciamento:** A diferença para o modelo de domínio usado no *Windows NT*, o Active Directory é baseado em estruturas hierárquicas organizacionais. Estas estruturas organizacionais tornam mais fácil o direito de controles administrativos e outras configurações de segurança. Também facilita os usuários a localizar recursos de rede, como arquivos e impressoras;
- **Integração com o DNS – Sistema de Nomes de Dominios:** O Active Directory usa o DNS, um serviço padrão da *Internet* que traduz nomes de *host* de fácil leitura para endereço IP (*Internet Protocol*). Active Directory e DNS têm a mesma estrutura hierárquica. Os clientes do Active Directory usam o DNS para localizar controladores de domínio. Ao usar o Windows Server e o serviço de DNS, as zonas primárias DNS podem ser armazenadas no Active Directory, permitindo a replicação para outros controladores de domínio do Active Directory;
- **Gerenciamento de configurações do Cliente:** O Active Directory fornece novas tecnologias para gestão de configuração problemas de cliente, tais como a mobilidade do usuário e falhas no disco rígido, com um mínimo de administração e tempo de inatividade do usuário;
- **Política de administração:** No Active Directory, as políticas são usadas para definir as ações permitidas e configurações para usuários e computadores em um determinado site, domínio ou unidade organizacional;
- **Replicação de informações:** O Active Directory fornece a tecnologia de replicação de vários mestres para garantir a disponibilidade da informação, tolerância a falhas, balanceamento de carga, e os benefícios de desempenho;
- **Autenticação e autorização flexível e segura:** A autenticação do Active Directory e serviços de autorização fornecem proteção de dados, minimizando as barreiras à realização de negócios pela *Internet*. O Active Directory suporta múltiplos protocolos de autenticação, como o protocolo Kerberos versão 5, SSL (*Secure*

Sockets Layer) versão 3, e TLS (*Transport Layer Security*) usando certificados X.509 versão 3. Além disso, o Active Directory oferece grupos de segurança que abrangem domínios;

- **Integração segura:** o Active Directory é integrado com a segurança do Sistema Operacional, Windows Server. ACL (*Access Controle List* - Lista de Controle de acesso) pode ser definido para cada objeto no diretório e em cada propriedade de cada objeto. Políticas de segurança podem ser aplicados localmente ou unidade para um local especificado, domínio ou unidade organizacional;
- **Diretório habilitado para aplicativos e infraestrutura**: Esses são recursos no Active Directory criados para tornar mais fácil configurar e gerenciar aplicativos e outros componentes habilitado para diretórios de rede;
- **Interoperabilidade com outros serviços de diretório:** O Active Directory é baseado em protocolos diretório padrões de acesso, incluindo LDAP Versão 3, e do nome NSPI (*Service Provider Interface*), e pode interoperar com outros serviços de diretório utilizando estes protocolos. Como o LDAP é um protocolo de acesso de diretório padrão da indústria, os programas podem ser desenvolvidos usando o LDAP para compartilhar informações do Active Directory com outros serviços de diretório que também suportam LDAP. O protocolo NSPI, que é usado pelo Microsoft Exchange Server 4 e clientes 5.x, é suportado pelo Active Directory para fornecer compatibilidade com o diretório do Exchange;
- **Tráfego LDAP assinado e criptografado:** Por padrão, as ferramentas do Active Directory no Windows Server 2003 e superior assinam e criptografam todo o tráfego LDAP. A assinatura do tráfego LDAP garante que os dados compactados venham de uma fonte conhecida e que não foi adulterado.

3.5.2 Conceitos importantes utilizados no Active Directory

O administrador de redes no Ambiente Microsoft se depara com diversos conceitos importantes para administração deste ambiente. Nos parágrafos a seguir são explicados alguns conceitos básicos.

3.5.2.1 Redes, Serviços de Diretórios e Controladores de Domínio

As redes foram criadas para fornecer recursos remotamente. Esses recursos quase sempre incluem arquivos, pastas e impressoras. Ao longo do tempo, esses recursos passaram a

incluir muitas coisas, principalmente e-mail, banco de dados e aplicativos. Era preciso um mecanismo que controlasse esses recursos e fornecesse, no mínimo, um diretório de usuários e grupos para que os recursos estivessem seguros contra acesso indesejado.

As redes do Microsoft Windows suportam dois modelos de serviços de diretórios: grupos de trabalho e domínio. O modelo de domínio é o mais comum nas organizações que implementam o Windows Server 2003 ou superior.

O modelo de domínio caracteriza-se por um único diretório de recursos empresariais – Active Directory – que é um domínio confiável utilizado por todos os sistemas seguros que pertencem ao domínio. Assim, os sistemas podem utilizar as propriedades de segurança (contas de usuário, grupos e computadores) do diretório para segurança a seus recursos.

O Active Directory é mais do que apenas um banco de dados,é uma coligação de arquivos de suporte, incluindo os logs de transação e o volume de sistema, ou Sysvol, que contém os scripts de logon e as informações de diretiva de grupo. Seus serviços suportam e utilizam o banco de dados, incluindo o LDAP, o protocolo de segurança Kerberos, os processos de replicação e o FRS (*File Replication Service*).

O banco de dados e seus serviços são instalados em um ou mais controladores de domínio. Um controlador de domínio é um servidor que foi promovido com a execução do Assistente de Instalação do Active Directory e do DCPROMO na linha de comando, como mostrado no Anexo IV deste trabalho. Após um servidor ter se tornado um controlador de domínio, ele hospeda uma cópia, ou réplica, do Active Directory. As modificações no banco de dados de qualquer controlador de domínio são replicadas para todos os controladores dentro do domino.

3.5.2.2 Domínios, Árvores e Florestas

O Active Directory não pode existir sem pelo menos um domínio e vice-versa. Um domínio é a unidade administrativa principal do serviço de diretórios do Windows Server 2003 ou superior. Entretanto, uma empresa pode ter mais de um domínio em seu Active Directory. Vários modelos de domínio criam estruturas lógicas chamadas árvores ao compartilhar nomes DNS contíguos. A Figura 3.2 ilustra um domínio com diversos sub-dominios.

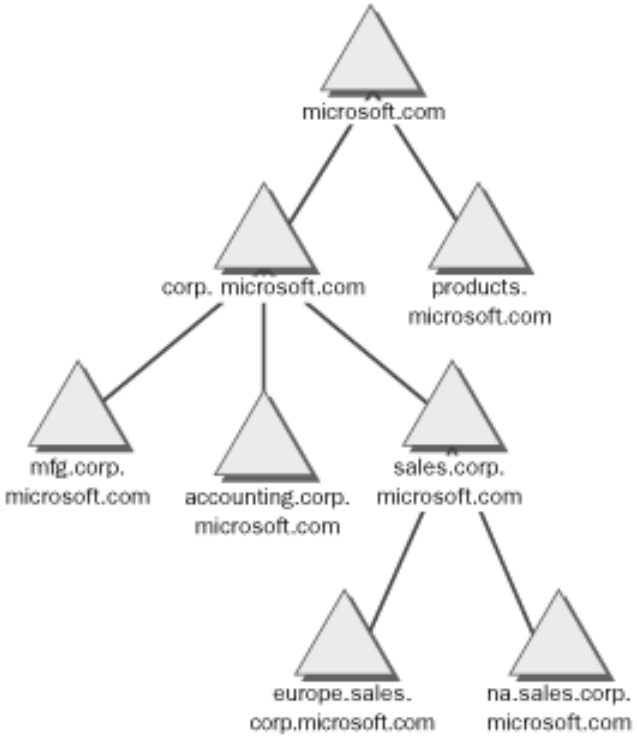

Figura 3.2 – Arvore de domínio

Se os domínios do Active Directory não compartilham de um dominio-raiz comum, eles criam várias árvores. Isso leva à estrutura maior de um Active Directory: a floresta. Uma floresta do Active Directory inclui todos os domínios dentro daquele Active Directory. Uma floresta pode conter vários domínios em múltiplas árvores, ou apenas um domínio. Quando há mais de um domínio, um componente do Active Directory chamado Catálogo Global torna-se importante, pois fornece informações sobre os objetos localizados em outros domínios da floresta. A Figura 3.3 ilustra um exemplo de floresta no Active Directory,

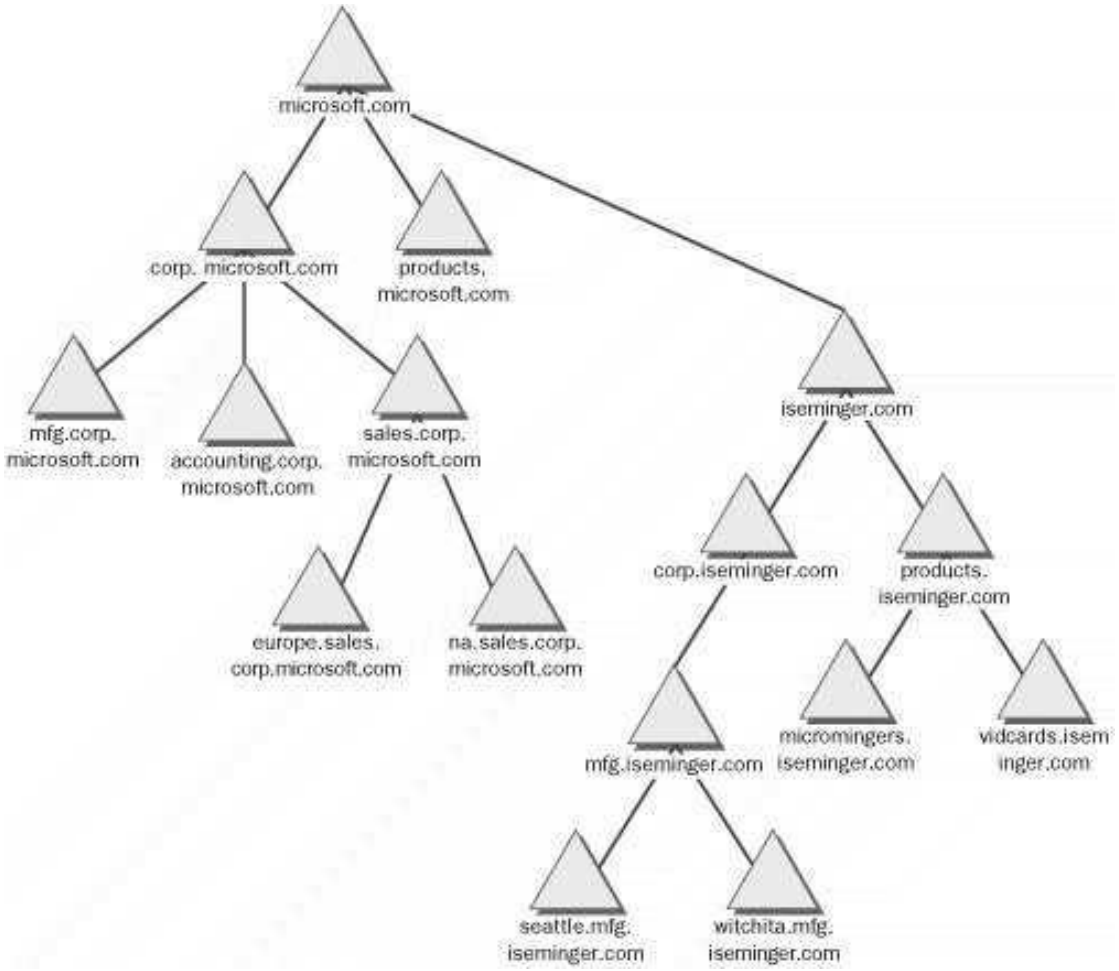

Figura 3.3 - Florestas

3.5.2.3 Objetos e Unidades Organizacionais (OUs)

No Active Directory, os recursos empresariais são representados como objetos, ou como registros do banco de dados. Cada objeto tem vários atributos, ou propriedades, que o definem. Por exemplo, um objeto de usuário inclui o nome de usuário e senha; um objeto de grupo inclui o nome do grupo e uma lista de seus membros.

O Active Directory pode hospedar milhões de objetos, incluindo usuários, grupos, computadores, impressoras,, pastas compartilhadas, sites, links de sites, Objetos de Diretiva de Grupo (GPO – *Group Policy Objects*), e até mesmo zonas DNS e registros de *host*.

A estrutura é função de um tipo especifico de objeto chamado unidade organizacional (OU – *Organizational Unit*). As OUs são *containers* dentro de um domínio que permitem agrupar objetos cuja administração ou configuração são compartilhadas. Mas elas fazem mais do que apenas organizar os objetos do Active Directory. Elas fornecem capacidades

administrativas importantes, uma vez que fornecem um ponto no qual as funções administrativas podem ser delegadas e aos quais as diretivas de grupo podem ser vinculadas.

3.5.2.4 Delegação

A delegação administrativa diz respeito à idéia de fazer com que um administrador de redes seja designado permissões para administrar uma determinada estrutura da árvore, por exemplo, alterar a senha de um subconjunto de usuários. Cada objeto do Active Directory permitem criar ACL que definem as suas permissões, assim como os arquivos em um volume de disco têm ACLs que definem acessos e permissões, aos mesmos. Por exemplo, uma ACL de objeto de usuário define quais grupos têm permissão para redefinir sua senha. Dependendo da organização seria inviável a atribuição ao administrador de redes permissões de alteração de senha individuais para cada usuário, sendo que é possível alocar todos esses usuários em uma única OU e designar ao administrador permissões a redefinição de senha neste Unidade Essa permissão será herdada por todos os objetos de usuário da pertencentes a OU, permitindo desta forma que o administrador modifique as permissões de todos os usuários contidos neste container.

A redefinição das senhas dos usuários é apenas um exemplo da delegação administrativa. Existem milhares de combinações de permissões que podem ser atribuídas a grupos que administram e dão suporte ao Active Directory. As OUs permitem que uma empresa crie uma representação ativa de seu modelo administrativo, e especifique quem pode fazer o que aos objetos do domínio.

3.5.2.5 Diretivas de Grupo

As OUs também são utilizadas para reunir objetos – computadores e usuários – que estão configurados de forma semelhante. Quase todas as configurações possíveis em um sistema Microsoft Windows podem ser gerenciadas centralmente por meio de recursos do Active Directory denominada Diretiva de Grupo. Uma Diretiva de Grupo permite especificar configurações de segurança, implantar software e configurar o sistema operacional e o comportamento de aplicativos remotamente.

Os GPOs são coleções de centenas de possíveis definições de instalação, desde os direitos privilégios de *logon* até o software que pode ser executado em um sistema. Um GPO está vinculado a um *container* dentro do Active Directory – em geral a uma OU, mas também

pode estar vinculado a domínios, ou até mesmo a sites – e todos os usuários e computadores abaixo dos conteiner são afetados pelas definições contidas na GPO.

Capítulo 4 - Implementação dos serviços de diretórios

Neste capitulo será definida uma empresa fictícia desenhada e organizada exclusivamente para estudo e aplicação nas implementações do protocolo LDAP deste trabalho. O desenho e organização da empresa fictícia foi embasada em experiências profissionais e algumas literaturas como por exemplo a de Andrew [FIN05]. Em seguida é apresentado a implementação do Active Directory e OpenLDAP e também é feita uma análise comparativa entre as duas implementações.

4.1. Descrição da corporação

A Empresa fictícia denominada MTulio foi criada para aplicação dos exemplos deste trabalho. MTulio é uma empresa com 5 unidades no Brasil. A sede é situada em Goiânia e as filiais estão instaladas em Anápolis, Uruaçu, Fortaleza e São Paulo.

4.2. Ambiente da Implementação

4.2.1 Hardware

O Ambiente de implementação sãos hosts virtualizados utilizando como hospedeiro o computador com Hardware conforme descrito abaixo:

- Partição raiz do sistema: 50 GB
- Memoria RAM: 4 GB DDR3
- Processador: Intel Core 2 Duo 2.6 GHZ 2MB
- Sistema Operacional: GNU/Linux CentOS 6 x86_64
- Sistema Virtualizador: Virtual Box 4.1
- Interface de rede: 2 NIC Gibabit Ethernet

As seguintes maquinas virtuais foram provisionadas com o mesmo recurso par aimplementação dos serviços de diretórios propostos:

- Virtual HD: 20 GB SATA
- Virtual RAM: 1024 MB
- Virtual CPU: 1
- Interface de Rede: 1 *Internal Network* e 1 *Bridge physical interface Ethernet*
- Memória de Video: 32 MB

4.2.2 Software

Os softwares escolhidos foram implementações proprietárias, Microsoft Active Directory e baseadas em condigo aberto, OpenLDAP. Foram simuladas as funcionalidades mais comuns das duas implementações.

4.2.2.1 Active Directory

- Sistema Operacional: Microsoft Windows Server 2003 Standard
- Versão do Software: Microsoft Active Directory Domain Services

4.2.2.2 OpenLDAP

- Sistema Operacional: GNU/Linux Debian 6 x86_64
- Versão Software: OpenLDAP 2.4

4.3. Estrutura do diretório LDAP

4.3.1 Estrutura Organizacional básica da estrutura de Diretórios

A Figura 4.1 descreve uma estrutura organizacional base para implementação do serviço de diretório LDAP deste trabalho. Essa estrutura foi desenhada para ser genérica para a organização proposta e expansível de acordo com as quantidades de unidades e de uma certa forma manter a organização e distribuição entre objetos em comum existentes em cada unidade criando assim uma estrutura única, gerenciamento centralizado e expansível a novas unidades por exemplo.

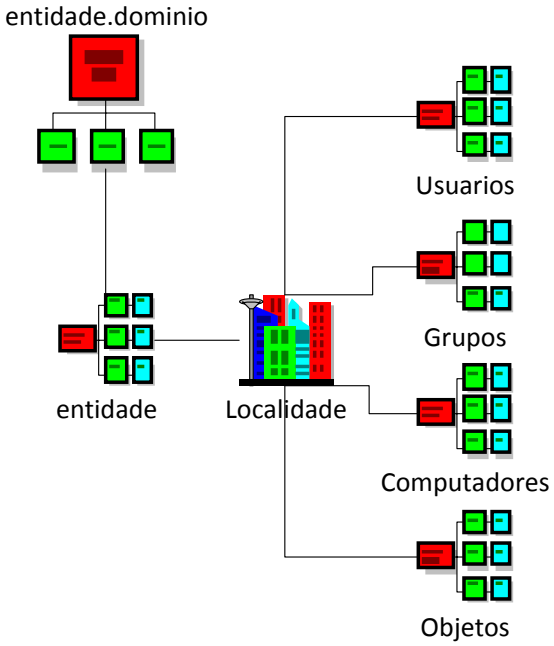

Figura 4.1 – Estrutura Lógica da Corporação

4.3.2 Estrutura das implementações

Para o estudo de caso deste trabalho são abordadas duas implementações do LDAP: Active Directory e OpenLDAP. Foram configurados no DNS a delegação dos dominios para os respectivos servidores visando o bom funcionamento do sistema autoritário. Mais detalhes sobre delegação DNS e esse protocolo podem ser obtidos em Paul [ALB01].

As implementações LDAP abordadas neste trabalho: foram escolhidas por serem consideradas as mais comuns de se implementar em um ambiente de produção. Cada uma delas tem suas características que foram discutidas no Capitulo 3. Visando complementar o design da estrutura, seguem as informações das duas implementações deste estudo.

4.3.3 Estrutura complementar básica das Empresas

As unidades organizacionais foram implementadas seguindo os padrões definidos na estrutura básica.

Os atributos DN das Empresas são:

- ou=entidade,dc=entidade,dc=mtulio,dc=eng,dc=br
- ou=Localidade,ou=entidade,dc=entidade,dc=mtulio,dc=eng,dc=br
- ou=Usuarios,ou=Localidade,ou=entidade,dc=entidade,dc=mtulio,dc=eng,dc=br
- ou=Grupos,ou=Localidade,ou=entidade,dc=entidade,dc=mtulio,dc=eng,dc=br

- ou=Computadores,ou=Localidade,ou=entidade,dc=entidade,dc=mtulio,dc=eng,dc=br

Conforme descrito no item 4.1 desse trabalho, são cinco unidades, sendo elas Goiânia, Anápolis, Uruaçu, Fortaleza e São Paulo. A seguir mais informações sobre a sub-estrutura Organizacional das Entidades e Unidades

4.3.3.1 Estrutura Organizacional das Entidades

4.3.3.1.1 Active Directory

Estrutura criada no Microsoft Active Directory:

- Nome da entidade: DOMAD MTulio ENG
- Domínio DNS: domad.mtulio.eng.br
- DN da entidade: dc=domad,dc=mtulio,dc=eng,dc=br
- OU da entidade: ou=domad,dc=domad,dc=mtulio,dc=eng,dc=BR

4.3.3.1.2 OpenLDAP

Estrutura criada no OpenLDAP:

- Nome da entidade: DOMOL MTulio ENG
- Domínio DNS: domol.mtulio.eng.br
- DN da entidade: dc=domol,dc=mtulio,dc=eng,dc=br
- OU da entidade: ou=domol,dc=domol,dc=mtulio,dc=eng,dc=BR

4.3.3.2 Estrutura Organizacional das Unidades

4.3.3.2.1 Unidade Goiânia

- Nome: Unidade Goiânia
- Localidade: Goiânia-GO
- Sigla: GYN
- DN raiz: ou=GYN,ou=entidade,dc=entidade,dc=mtulio,dc=eng,dc=BR

4.3.3.2.2 Unidade Anápolis

- Nome: Unidade Anápolis
- Localidade: Anápolis-GO
- Sigla: ANA
- DN raiz: ou=ANA,ou=entidade,dc=entidade,dc=mtulio,dc=eng,dc=BR

4.3.3.2.3 Unidade Uruaçu

- Nome: Unidade Uruaçu
- Localidade: Uruaçu-GO
- Sigla: URU
- DN raiz: ou=URU,ou=entidade,dc=entidade,dc=mtulio,dc=eng,dc=BR

4.3.3.2.4 Unidade Fortaleza

- Nome: Unidade Fortaleza
- Localidade: Fortaleza-CE
- Sigla: FOR
- DN raiz: ou=FOR,ou=entidade,dc=entidade,dc=mtulio,dc=eng,dc=BR

4.3.3.2.5 Unidade São Paulo

- Nome: Unidade São Paulo
- Localidade: São Paulo-SP
- Sigla: SPO
- DN raiz: ou=SPO,ou=entidade,dc=entidade,dc=mtulio,dc=eng,dc=BR

4.4. Configuração e Implementação

A instalação, configuração e implementação das ferramentas de serviços de diretórios, Active Directory e OpenLDAP, seguem conceitos diferentes por se tratarem de Sistemas Operacionais distintos, Microsoft Windows e GNU/Linux, por esse motivo serão abordados detalhes da pré-instalação, instalação, configuração e scripts para auxilio na manipulação (inserção, deleção e atualização) de registros na Base.

4.4.1 Implementação Active Directory

4.4.1.1 Instalação

O Microsoft Active Directory Domain Services foi instalado no Sistema Operacional Microsoft Windows Server 2003 Standard, detalhes da instalação deste não será abordada neste trabalho, por não ser o escopo do mesmo.

Os detalhes da preparação do ambiente, requisitos e instalação do Microsoft Active Directory está detalhada no Anexo IV.

4.4.1.2 Configuração

A estrutura organizacional no servidor Controlador de Domínio Active Directory seguirá conforme descrito no Item 4.1.

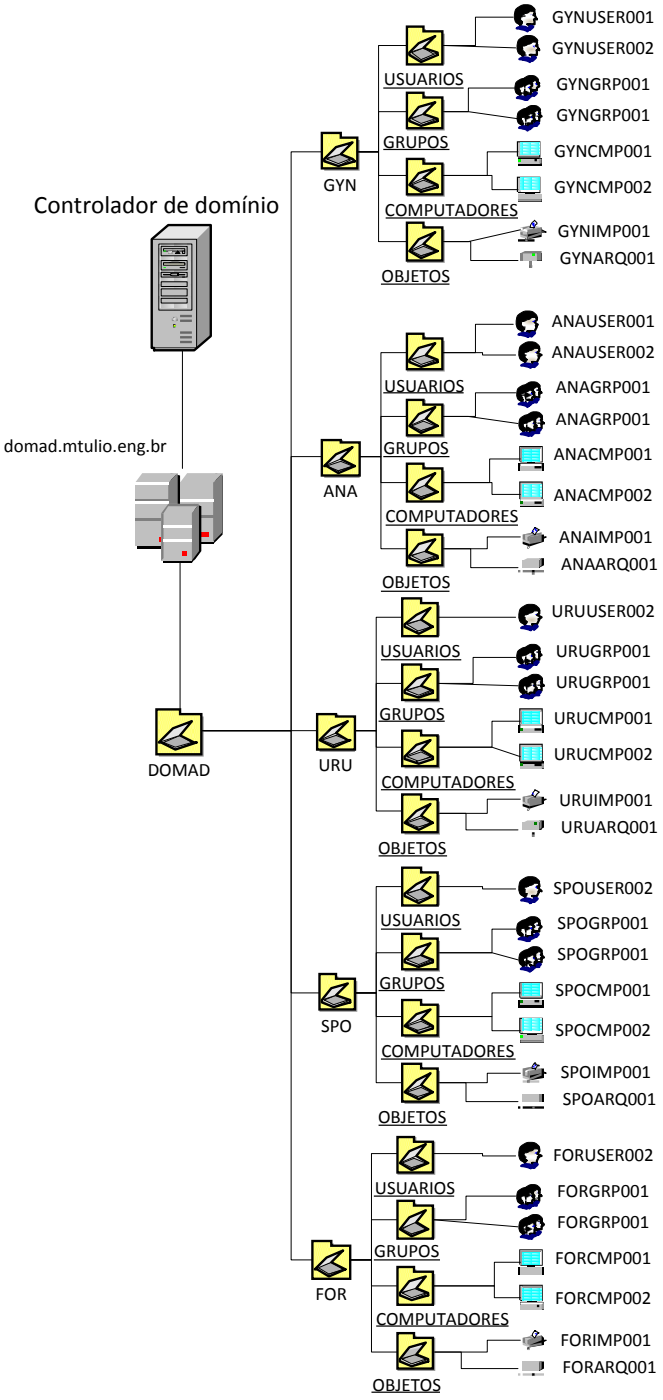

Figura 4.2 - Estrutura da Corporação no Active Directory

A Figura 4.2 ilustra a estrutura implementada no Active Directory. Como o protocolo LDAP é um diretório de propósitos gerais, as implementações adicionam recursos para facilitar e adequar ao ambiente. A Microsoft por sua vez, desenvolveu alguns recursos que caracterizam e adicionam maiores funcionalidades ao AD, alguns deles são:

- GPO – Group Policy Object: Políticas de grupos que são aplicadas nas Unidades Organizacionais em qualquer nível do diretório;
- Impressora: Objeto de impressora criado para consolidar objetos da rede no diretório;
- Compartilhamentos (volumes): criados para centralizar os compartilhamentos facilitando a manipulação e busca do mesmo;
- Rede e serviços : Possibilita desenhar a topologia da rede para fins de maximinizar o uso dos recursos de rede sem maior impacto na infraestrutura. Por exemplo: Aumento do tempo de Replicação de sites remotos interligados por links WAN de baixa velocidade.

4.4.1.3 Implantação e População do Diretório

Para muitos administradores, a fase que demanda mais tempo é a migração ou criação dos objetos no diretório. A popularização do diretório implementado neste trabalho foi automatizada utilizando script criado na linguagem Visual Basic Script. Este script e detalhes desta implementação segue no Anexo V.

4.4.2 Implementação OpenLDAP

4.4.2.1 Instalação

A distribuição GNU/Linux escolhida para instalação do OpenLDAP foi o Debian. Porém, não há problema em escolher outra distribuição para instalação do mesmo, basta conhecer os comandos e diretórios equivalentes, pois algumas distribuições têm suas particularidades.

O OpenLDAP assim como a maioria dos serviços no GNU/Linux tem o(s) arquivo(s) de configuração responsáveis por manter o serviço, mas a partir da versão 2.3 o OpenLDAP adicionou um novo recurso, opcional, em que a configuração pode ser realizada em tempo de execução, *runtime*, usando uma entrada na DIT chamada cn=config. Para os administradores que optarem por essa funcionalidade não mais utilizarão o tradicional arquivo slapd.conf. Com essa opção, toda e qualquer alteração na estrutura do servidor, tais como opções globais,

inclusão de *schemas*, definições de domínios, acls, módulos dentre outras terão que ser adicionadas a essa DIT utilizando um LDAP Browser ou o ldapadd. Essas alterações trouxeram grande evolução para o OpenLDAP, pois ao efetuar qualquer alteração no servidor LDAP, o serviço não precisa ser reinicializado, evitando *downtimes* que, dependendo das bases, pode trazer muitos transtornos e indisponibilidade nos serviços. Mais informações sobre *runtime* leia [ZYT11].

O OpenLDAP por si só é apenas um serviço de Diretório. Como o intuito deste trabalho é estudar as implementações LDAP e comparar o Active Directory, é necessário implementar o SAMBA integrando com o OpenLDAP tornando-o mais próximo do Microsoft Windows Domain Controler.

Samba é um software que utiliza o protocolo SMB/CIFS (*Server Message Block/Common Internet File System*) podendo ser executado em uma plataforma diferente do Microsoft Windows, por exemplo, UNIX, Linux, IBM System 390, OpenVMS e outros sistemas operacionais. O Samba utiliza o protocolo TCP/IP que é instalado no servidor host. Quando corretamente configurado, ele permite a interação do host com um cliente e/ou servidor do Microsoft Windows como se fosse um servidor de arquivos ou de impressão do Windows [SAM01].

A versão do OpenLDAP instalada foi a 2.4. A instalação do OpenLDAP, que é relativamente simples, tanto como a resolução das dependências é abordada no Anexo II, parte 02. A instalação do SAMBA é abordada na primeira parte do Anexo II.

4.4.3 Configuração e implantação do Diretório

A configuração da Base é um pouco mais complexa que ao Active Directory, porém, abordam os mesmo princípios: Definição (Design) da Base, criação da Base, Criação das Unidades Organizacionais e Criação dos Objetos. Como todos serviços de diretório, no OpenLDAP a inserção de objetos na Base pode ser feita de diversos modos como, por exemplo, utilizando clientes que se conectam a base do LDAP. Alguns deles são: Softerra LDAP Administrator, ldapaccount-manager, phpLdapAdmin, dentre outros. Para adicionar os registros na Base neste trabalho será utilizado os recursos que o OpenLDAP oferece por padrão, arquivos LDIF.

O design da estrutura implementada tem é apresentado na Figura 4.3:

Figura 4.3 - Estrutura OpenLDAP

A configuração do Controlador de Domínio utilizando o OpenLDAP, foram seguidos os seguintes passos:

- Configurar o SAMBA como PDC: Anexo III – Parte 01;
- Configurar o OpenLDAP com a Base (domínio) DOMOL: Anexo III – Parte 02;
- Criar as Unidades Básicas e população do diretório: Anexo III – Parte 03;
- Integração do Samba com OpenLDAP: Anexo III – Parte 04.

Para automatizar o desenvolvimento e estudo deste trabalho, foi desenvolvido um script que gera arquivos LDIF de toda a Base (Organização, Unidades, SYSTEM e entrada do SAMBA) definida na seção 4.3.3 de acordo com as variáveis constantes definidas no cabeçalho e em seguida esses registros são adicionados à base utilizando a ferramenta ldapadd. Este script e a utilização do mesmo estão no Anexo VI.

4.5. Critérios de comparação das duas implementações

4.5.1 Tempo

O tempo é um critério muito decisivo em ambientes corporativos, onde são exigidos maiores resultados no menor prazo, independente da equipe envolvida. Os critérios devem contabilizar desde o planejamento, migração (caso seja feita), desenho da estrutura, estudo de caso, instalação, configuração, implantação e com sistema em produção.

4.5.2 Facilidade de uso

A facilidade é um quesito relativo, pois a facilidade está ligada diretamente aos conhecimentos do administrativo e operacional da equipe envolvida no projeto de instalação e configuração do servidor de diretórios.

4.5.3 Descrição do Ambiente

Grandes corporações não têm uma estrutura organizacional bem definida ou tal estrutura é dinâmica o suficiente que dificultam no design da estrutura organizacional da empresa. Nestes casos devem-se definir uma estrutura genérica e que não fique completamente ligada a estrutura organizacional da entidade. Este recurso pode ser feito utilizando grupos.

4.5.4 Flexibilidade e adaptabilidade

Esses critérios podem ser divididos em algumas camadas/partes:

- Visão administrativa: Envolve muito a parte técnica e conhecimentos medianos e/ou avançados da tecnologia aplicada. Esse grau é medido pelo conhecimento do administrador de redes;
- Visão do Usuário: Para o usuário final, muitas vezes é transparente, ou até mesmo na migração pode ter alguns problemas, porém após uma migração/implantação de um serviço de diretórios o usuário será o mais satisfeito por manter uma "autenticação centralizada".
- Visão da Infraestrutura: A infraestrutura está ligada diretamente com o planejamento da nova estrutura de diretórios e com equipamentos que vão hospedar os novos serviços e o tamanho da corporação. É importante sempre estudar o pior caso para evitar gargalhos e alta latência em requisições de pesquisas no diretório.

4.5.5 Segurança

A segurança nos serviços de diretórios é um quesito essencial a ser considerado, pois, praticamente em todas as situações de implementação de serviços de diretório, o LDAP é usado para armazenamento de contas de usuário, sistemas, computadores e outros objetos essenciais para o bom funcionamento e gerencia da rede. Outro fator importante é que a estrutura de diretórios reflete a estrutura organizacional da empresa. Portanto se determinadas informações forem expostas sem necessidade, podem causar danos irreparáveis.

4.5.6 Estabilidade

A estabilidade e bom funcionamento estão ligados a diversos fatores tais como hardware, software recursos humanos, ou administradores de diretório, manutenção preventiva, segurança, dentre outros.

4.5.7 Manutenção

Este critério avalia a facilidade de administração e manutenção preventiva como corretiva, softwares de testes e monitoramento.

4.5.8 Tamanho da corporação

Conforme descrito neste trabalho é importante projetar a estrutura organizacional do diretório baseado na entidade e assim logo após iniciar a execução do projeto.

4.5.9 Tempo de resposta

O Diretório é o local onde são armazenados grande parte dos objetos da rede, e tem a sua finalidade a centralização da administração, incluindo neste a autenticação. Com isso, sistemas ERP (*Enterprise Resource Planning*), Banco de Dados, Usuários de sistemas, aplicações, hosts, dentre outros objetos podem ficar em um só lugar. Quanto maior a quantidade de objetos, consequentemente maior será maior o numero de requisições que o servidor receberá. Com isso, se a infraestrutura ou a configuração do diretório não estiverem atendendo o ambiente, o tempo de resposta será alto, e este é um dos quesitos mais visíveis ao usuário final, pois está ligado diretamente a sua jornada de trabalho. Existem algumas ferramentas de analise de desempenho (Benchmarks), uma delas é o DirectoryMark [DMA11].

4.5.10 Custo e Beneficio

O custo é levado em consideração em praticamente todos os setores de atuação: industrial, governamental, comercial, etc.. Porém, deve-se avaliar cada quesito de custos e benefícios, se houverem. Os custos podem ser divididos em algumas partes que são descritas abaixo.

4.5.10.1 Aplicação

O Custo da aplicação é um dos mais “visíveis” ou um dos primeiros a serem avaliados, talvez erroneamente pois existem ambientes críticos que necessitam, por exemplo de um suporte de uma falha na aplicação. Outro exemplo é a necessidade de desenvolvimento de novas funcionalidades, *schemas*, recurso, etc.

4.5.10.2 Treinamento, Suporte e Manutenção

Um serviço de diretórios consolidado é muito importante, mas só é possível chegar ao nível de estabilidade passando por diversas etapas. Um bom projeto de estrutura de diretórios passar por no mínimos as etapas de desenvolvimento e melhoria continua, o famoso PDCA (Plan, Do, Check Act – Planejamento, Execução, Verificação e Ação), disponível em diversas normas ABNT, gerenciamento de processos, projetos, dentre outros. Porém para obter esse ciclo, é importante que haja uma equipe com conhecimento da tecnologia a ser utilizada para poder resolver problemas que aparecerem e também criar possíveis melhorias e manutenção

no serviço de diretórios e a aplicação que a mantém. Para isso, é importante que tenha uma equipe “reciclada” ou atualizada. Por isso se o a implantação partir de uma equipe interna, deve-se disponibilizar treinamentos para equipe de suporte e administração da infraestrutura, todavia caso seja terceirizada devem ser avaliados níveis de conhecimentos e know-how da equipe a ser contratada.

4.5.10.3 Infraestrutura

A infraestrutura é um ponto muito importante na elaboração de um projeto. Algumas vezes só é projetado a infraesturtura para atender a demanda atual e do ambiente a ser implantado, sem estudo de caso para expansão, isso pode tornar um problema para uma possível expansão, ou chamada “upgrade”. Uma Infraestrutura bem projetada, como por exemplo, clusterização, H.A. (High Availability – Alta disponibilidade), sites remotos com réplicas é muito interessante. Para ambientes críticos praticamente essenciais a disponibilização desses recursos.

4.6. Análise comparativa

4.6.1 Tempo

A criação da estrutura deste serviço de diretórios não levou muito tempo, por se tratar de um ambiente fictício e sem muitas regras de negócios. É importante deixar claro que nesta fase deve-se gastar muito tempo por se tratar da projeção da estrutura organizacional da empresa num Serviço de Diretórios.

A instalação dos dois sistemas foi relativamente rápida, pois é necessário somente informar a estrutura da organização definidas no projeto. O Active Directory demandou mais tempo, pois além da promoção do Serviço de Diretórios foi feito também a instalação do DNS. A instalação do OpenLDAP e SAMBA foi mais rápida porque é relativamente mais simples por se tratar de um sistema GNU/Linux utilizando pacotes de instalação pré-compilados pelo gerenciador de pacotes utilizado pela distribuição, há vantagens de utilizar um gerenciador de pacotes, pois resolvem todas as dependências, caso contrário, o OpenLDAP demandaria mais tempo.

O tempo gasto pós-instalação foi maior, pois demandou a criação da estrutura lógica da Entidade, unidades organizacionais e população do diretório com os objetos específicos. Essa criação, neste trabalho, foi automatizada através de scripts que utilizam ferramentas fornecidas pelo Sistema Operacional (Microsoft Windows e GNU/Linux) e a aplicação

(OpenLDAP e Active Directory) desenvolvidos nas linguagens Visual Basic Script (utilizando plataforma .NET Famework) para o Windows e o Shell Script e LDIF no GNU/Linux. O tempo gasto para as duas plataformas foram relativamente os mesmos, pois demandou a adequação e estudo de funções especificas de cada linguagem.

4.6.2 Facilidade de uso

O quesito facilidade é bastante relativo, pois depende do conhecimento da equipe, necessidade de utilização determinada ferramenta disponível em um servidor de Diretório especifico, como por exemplo, GPO no Active Directory. Porém, apesar das particularidades de cada implementação, o Microsoft Active Directory é mais fácil devido a usabilidade do Microsoft Windows, podendo assim um administrador que não tenha tanta experiência criar uma nova estrutura a partir do zero sem ter muitos conhecimentos técnicos da ferramenta.

4.6.3 Descrição do ambiente

O ambiente criado, apesar de ser fictício, foi desenhado para que a simulação seja mais próxima de um ambiente real, utilizando recursos como objetos de usuários, volumes (compartilhamentos de redes, no Windows) e contas de máquinas. O Active Directory disponibiliza mais recursos, ambientes e ferramentas para manipulação do diretório com maior facilidade. O OpenLDAP fornece também diversas ferramentas sendo necessário a instalação a parte de cada uma, fica de acordo com o gosto e necessidade do administrador.

4.6.4 Flexibilidade e adaptabilidade

Analisando as mesmas questões descritas no item 4.5.4:

- Visão Administrativa: O Active Directory, trazendo as características do Windows, tem muito fácil instalação e administração, porém ele mal configurado pode ser uma dor de cabeça para o administrador. Já no OpenLDAP, a grande quantidade de *front-ends* torna a sua administração mais fácil, mas ainda é preciso que ele evolua para que tenha a mesma usabilidade da implementação da Microsoft. Portanto a ferramenta da Microsoft pode ser mais fácil de administrar;
- Visão do usuário: Para os usuários na maioria das vezes é transparente, porém depende de que aplicação ou sistema está sendo utilizado. Por exemplo, com a utilização de um servidor Exchange e um cliente Microsoft, a adaptabilidade do Active Directory é ideal. A maneira com as solicitações são feitas em grande parte

não são alteradas, pois a “conversação” entre o Cliente e o Servidor continua sendo pelo protocolo LDAP, apenas a manipulação, tratamento e armazenamento dos dados no servidor que são alteradas de acordo com a implementação instalada;

- Visão da Infraestrutura: Neste quesito, o OpenLDAP tem vantagem. Por ser um servidor “leve” e a plataforma a ser instalada pode ser otimizada apenas para este servidor. Podem ser instalados apenas os pacotes necessários para a execução do servidor de diretórios e controlador de domínio. Existem diversas distribuições GNU/Linux minimalistas que podem ser personalizadas, instalando apenas o kernel, ferramentas GNU, dependências e pacotes do servidor. Com isso, há ganho de desempenho no servidor instalado a ferramenta *opensource*. Já o Microsoft Windows consome muitos mais recursos de Hardware. Após a instalação do controlador de domínio da Microsoft, a utilização de recursos do servidor aumenta consideravelmente. Portanto, deve ser estudado bastante a estrutura física que este sistema será instalado, evitando problemas futuros de adaptabilidade, estabilidade e até indisponibilidade.

4.6.5 Segurança

Tanto o Active Directory como o OpenLDAP oferecem recursos de segurança como requisitos mínimo de tamanho, complexidade e troca de senha, recursos de ativação de LDAP sobre SSL/TLS, gerenciamento de certificados e outros. Esses recursos não foram abordados neste trabalho por se tratar de um assunto mais extenso. Para mais informações sobre estes recursos sugere-se que sejam consultadas a documentação do serviço de diretório utilizado.

Outros elementos básicos que podem ser implantados são: aplicar regras de acesso de acordo com usuários, grupos, departamentos ou toda organização. Tais regras podem conter restrições de acesso a diretórios de arquivos do servidor, restrição de alteração de configuração da maquina, tais como instalação de software, alteração do horário de maquina, registros, configurações de sistemas, dentre outros. Uma das grandes vantagens de se implantar um controlador de domínio com autenticação centralizada é essa administração, fortalecendo a aplicação das políticas de segurança da Entidade.

Os conceitos de segurança são relativos, pois depende até que nível a entidade deseja proteger seus dados. Também depende do ambiente computacional utilizado. Por exemplo, num parque computacional Microsoft Windows, o Active Directory terá mais ferramentas disponíveis para esse ambiente em comparação ao OpenLDAP integrado com SAMBA. Essas

restrições podem ser configuradas no Active Directory de forma bem eficaz utilizando as GPO's (Objetos de Políticas de Grupo). É possível "simular" as GPO's utilizando servidores SAMBA e recursos de ferramentas que criam tais políticas utilizando modelos administrativos, que são definições das configurações do cliente Windows. O SAMBA até a versão 3, esse método era "primitivo", que simulava o ambiente do Windows 2000 utilizando arquivos NTCONFIG que são arquivos de políticas de grupo gerada a partir da ferramenta POLEDIT, disponibilizada pela Microsoft para ambientes que não utilizam o Active Directory[MIC06]. Na versão 4, o SAMBA oferece recursos para simular grande parte (segundo a comunidade que a desenvolve) do ambiente Microsoft Windows Active Directory [SAM02]. Para mais informações sobre essa nova versão do SAMBA e todas as novas funcionalidades, entre no site oficial [SAM02].

4.6.6 Estabilidade

Este critério de avaliação não é possível mensurar em curto prazo, pois só depois de testes, correções, adequações e validações do ambiente um sistema pode alcançar estabilidade. Sistemas GNU/Linux em geral são conhecidos por ser mais "estáveis" e "confiáveis" em comparação aos sistemas da Microsoft, porém, ambos tem suas vantagens, o sistema *opensource* tem maior facilidade em uma recuperação de desastre ou upgrade para outra plataforma, pois são baseados em arquivos de configuração facilitando o *restore*. Já no Windows, existem algumas técnicas de recuperação, por exemplo *Backup* do *System State* [MIC07].

4.6.7 Manutenção

A manutenção em um servidor de diretórios LDAP pode ser feito utilizando diversas ferramentas disponíveis no mercado, grande parte já citadas neste trabalho. Vale também avaliar as ferramentas básicas fornecidas pela implementação escolhida, neste caso Active Directory e OpenLDAP. O Active Directory fornece duas ferramentas principais para administração. Na versão 2003 são chamadas "Usuários e Computadores do Active Directory" e "Gerenciar Sites e Serviços". Com essas ferramentas é possível gerenciar todo o controlador de domínio. No OpenLDAP essa administração não é tão amigável como o Active Directory. Por padrão o servidor disponibiliza as ferramentas ldaputils pela linha de comando. Para maior comodidade e visualização podem ser instalados alguns front-ends para administração do diretório, conforme citados no item 4.4.3 desse trabalho.

4.6.8 Tamanho da corporação

A corporação fictícia criada foi idêntica para as duas implementações, apenas no OpenLDAP foi criado uma Unidade Organizacional denominada SYSTEM para utilização por sistemas como SAMBA. Como foram criados scripts para criação automática dos objetos e unidades, não houve dificuldade, mas a expansão ou até alteração pode ser feita quando se tem um serviço de diretórios grande. O Administrador de redes deve tomar muito cuidado ao renomear ou realocar novas OU's, pois o identificador único do objeto, DN, está ligado a sua localização na arvore de diretórios. Como o Active Directory, por padrão, já fornece ferramentas para administração, neste quesito há mais vantagens em utilizá-lo.

4.6.9 Tempo de resposta

Para uma avaliação mais precisa deste quesito recomenda-se utilizar ferramentas de diagnósticos e testes de diretórios, conforme citado na seção 4.5.9. O DirectoryMark pode fazer essa sequência de testes. Neste trabalho foram inseridas trilhas de marcação de tempo no código de criação das Unidades, podendo mensurar os tempos de execução das operações no servidor. Deve-se levar em consideração no tempo da criação com o processamento de outros aplicativos instalados no servidor de diretórios. Para maior consistência nos dados, é aconselhavel evitar a utilização do sistema operacional no momento da execução do script. Com isso, os resultados poderão ser melhores. Foi gerado um *log* cujo caminho é informado no final da execução do script. Como não era um ambiente em produção e a quantidade de operações na base não foi o suficiente para tirar conclusões da melhor ferramenta.

4.6.10 Custo e Beneficio

Neste trabalho não foram analisados apenas os custos financeiros de cada quesito, mas sim os benefícios consquentes de tal investimento nas tecnologias avaliadas, Active Directory e OpenLDAP.

4.6.10.1 Aplicação

Analisando o custo da aplicação e de todos os custos envolvidos de se utilizar a tecnologia da Microsoft, o custo pode ficar elevado, pois se devem considerar as CAL (*Client Access License*). Neste trabalho não foram levados em considerações estes parâmetros, pois foram utilizados licença de uso acadêmico.

O OpenLDAP, é de código livre, licenciado pela OpenLDAP Public License que fornece o código fonte e permite alteração e a redistribuição de acordo com os termos de sua licença Publica. [OPE02].

4.6.10.2 Treinamento, Suporte e Manutenção

Para que se tenha um ambiente seguro é necessário estar sempre por dentro de novidades, atualizações do produto, implementação de novas funcionalidades e correção/resolução de problemas. Todas essas tarefas devem ser feitas pela equipe responsável pelo servidor de diretórios. Como as demandas de suporte e manutenção são imprevisíveis e também para melhorias continuas ou implementações de novas funcionalidades programadas exigem que a equipe se mantenha "reciclada" e com novas idéias e boas técnicas e praticas na resolução de problemas.

Com isso, tanto o Active Directory quanto no OpenLDAP é importante conhecer a tecnologia e o ambiente para ter um bom suporte e manutenção. Isso pode ser alcançado com qualidade da equipe e treinamento para os profissionais responsáveis pelo serviço de diretório é um diferencial.

4.6.10.3 Infraestrutura

A infraestrutura para suportar o Active Directory é relativamente maior que do OpenLDAP, devido aos requisitos mínimos exigidos do Sistema Operacional Microsoft. A Microsoft detalha mais sobre os Requisitos de Hardware para instalação do Sistema Operacional Windows Server 2003 no seu site [MIC03]. Nas versões atuais do Microsoft Windows Server foi embutida a opção de instalação do sistema sem ambiente gráfico, chamado Server Core [MIC04].

O OpenLDAP por ser de código aberto e compatível com diversas distribuições GNU/Linux e Unix, ele pode ser customizado e/ou instalado em ambientes minimalistas, por exemplo Debian network instalation from minimal CD [DEB01] com instalação customizada. Essa opção é interessante, pois há maior aproveitamento de recursos hardware. Na implementação deste trabalho foi utilizada a distribuição Debian versão 6 na plataforma 64 bits.

4.7. Avaliação Geral

	Microsoft Active Directory	OpenLDAP
Tempo	Rápida e fácil instalação e configuração	Instalação completa demorada. Dependente de outros serviços
Facilidade de Uso	Administração Simples	Administração intermediaria. Bom por ter muitos front-ends para administração
Descrição do Ambiente	Ferramentas centralizadas de modelagem e administração do ambiente	Possui ferramentas front-ends para modelagem do ambiente ou para aplicações especificas. Ex.: LAM
Flexibilidade e Adaptabilidade: Administração	Fácil	Mediana
Flexibilidade e Adaptabilidade: Usabilidade	Transparente para usuários finais, quando configurado corretamente	Transparente para usuários finais, quando configurado corretamente
Flexibilidade e Adaptabilidade: Infraestrutura	Alto custo e utilização de recursos físicos	Baixo Custo, físico (hardware) e lógico (software)
Segurança	Seguro quando bem configurado.	Seguro quando bem configurado.
Estabilidade	Bom, quando configurado corretamente.	Bom, quando configurado corretamente.
Manutenção	Fácil administração e manutenção com ferramentas nativas da Aplicação.	Em sua instalação padrão, fornece a manipulação do diretorio pela linhda de comando, tornando um pocuo mais dificil a administrção. Porém, existem diversos front-ends para suprir esse problema
Tamanho da Corporação	Mais dinâmico a expansão. Cria por default estruturas com OU's e objetos para administração do dominio, facilitando e deixando organizado o diretório.	Mais limitado quanto a administração, porém há vantagem em ambientes que necessitam uma base personalizada ou para propositos específicos
Tempo de Resposta	Maior utilização da CPU na criação da base utilizando scripts desenvolvidos neste trabalho e o tempo de criação um pouco mais alto em relação ao OpenLDAP	Tempo de resposta mais rápido nos scripts da criação do domínio desenvolvidos neste trabalho. Pode ser vantagem quando se tratar de um numero mais elevado de objetos
Custo e Beneficio: Aplicação	Alto custo e diversos tipos de licenciamentos	Totalmente livre. Consequentemente não há custos
Custo e Beneficio: Treinamento, Suporte e Manutenção	Essencial para administradores das ferramentas	Essencial para administradores das ferramentas
Custo e Beneficio: Infraestrutura	Elevado custo pois o Sistema Operacional exige mais recursos computacionais	Baixo Custo, físico (hardware) e lógico (software)

Tabela 4.1 – Avaliação geral da análise comparativa

Capítulo 5 - Conclusão

O LDAP vem sendo cada vez mais utilizado pelos administradores de rede e de sistemas, pelas inúmeras vantagens que apresenta em relação aos demais serviços de diretórios.

Os problemas causados pela grande quantidade de informações que as organizações processam hoje são inúmeros: redundância nos dados, dificuldade ou impossibilidade de acesso às informações e dados de aplicações, acesso lento, ausência de um controle eficaz quanto a autenticação de usuários administradores e clientes, etc. Com tantos problemas, o LDAP é uma saída bastante eficaz, tendo se mostrado a frente de outros serviços similares de acesso a diretórios, além de apresentar poucas desvantagens, que podem ser irrelevantes.

Neste trabalho foram abordados desde os princípios básicos dos serviços de diretórios até as principais funcionalidades e características que o protocolo LDAP oferece. Como o LDAP é um protocolo aberto e mantido pelo IETF, ele está suscetível a modificações, na maioria das vezes adicionando novas funcionalidades e recursos para esse protocolo.

Além de estudo desse protocolo, este trabalho também abordou as ferramentas utilizadas como servidor do protocolo LDAP. A finalidade era desde buscar as "tendências" utilizadas pelos administradores de redes e com base nessas informações, coletadas pela pesquisa apresentada no Item 1.1, desenvolver ambientes fictícios e instalar e configurar as duas principais ferramentas nesses ambientes, em seguida aplicando critérios de avaliação e comparação. Analisando tais critérios e a implementação das ferramentas foi criado uma matriz de comparação baseando-se em tais ferramentas.

Embasado nas pesquisas e critérios de avaliação das ferramentas abordadas neste trabalho, podem surgir diversas indagações quanto a qual ferramentas realmente é a melhor. Foram abordados a importância de pontos que às vezes não são levados em consideração na implantação de serviços de diretórios como, por exemplo, o desenho e estruturação da base, treinamento e suporte, material sobre a ferramenta, dentre outros.

Com isso podem surgir alguns mitos, ou esclarecê-los, de que o Ambiente Operacional Microsoft Windows Server é fácil de instalar, configurar e administrar. Pode até ser, porém se uma estrutura não for desenhada, planejada, testada e a devida manutenção for dada, há grandes chances de esse ambiente passar por futuros problemas de expansão/reestruturação da base ocasionando a desorganização, descentralização, inconsistência nos dados, perda de informações e até lentidão devido a gargalhos que podem acontecer quando se há vários sites replicados.

Em controvérsia, o GNU/Linux, de certo modo, pode ser mais difícil de configurar e administrar, mas um ambiente bem planejado pode ser bem estável e também pode passar pelos mesmos problemas que o da Microsoft.

Para evitar esse tipo de problema a equipe responsável pelo planejamento/configuração/implantação deve ter um bom conhecimento da tecnologia a ser utilizada como também do ambiente operacional a ser instalado. Esse conhecimento dá-se através de treinamentos, e até do "suporte" a tecnologia. Esse suporte pode ser adquirido não só por empresas de software, mas como também da comunidade, no caso do GNU/Linux, livros, cursos, etc. Porém um dos grandes problemas enfrentado, neste trabalho, como na vida de administrador de redes é o acesso a informações de qualidade. Nem sempre na Internet há material de qualidade e em que se possa se embasar. Existem muitas bibliografias ou sítios que abordam apenas o "como fazer" e não a "importância" e até impactos de determinadas ações.

Analisando todas as informações coletadas e estudadas neste trabalho é possível verificar que há controvérsias em relação a que ferramentas utilizarem, todavia as ferramentas apresentadas neste trabalho são bastante poderosas e possuindo uma diversidade enorme de desenvolvedores e mantenedores dos projetos, para o Active Directory a Microsoft que traz mais recursos e funcionalidades a cada nova versão, e o OpenLDAP tem uma comunidade de desenvolvedores *opensource* que a mantém.

Com este trabalho foi possível entender melhor o funcionamento, princípios, conceitos, enfim, foi possível aprofundar o conhecimento em uma tecnologia que vem inovando e crescendo cada vez mais no que se diz respeito a acesso a informações. Tendo como base este estudo é possível evoluir e aplicar os conceitos aqui vistos nas aplicações e serviços em redes de computadores e em diversas outras áreas da computação..

5.1. Sugestão de Trabalhos Futuros

Como sugestão de trabalhos futuros propõe-se:

- Estudo de caso da replicação do Active Directory com o OpenLDAP ou vice-versa;
- Estudo de caso do Samba 4, que tem a finalidade de oferecer a maioria das implementações do Microsoft Active Directory;
- Criação de um "Compilador" (Analisador léxico, sintático e/ou semântico) para arquivos LDIF antes de inserção na BASE;

- Testes de desempenho entre os dois servidores de diretórios apresentados, e/ou com outros. A ferramenta utilizada pode ser o DirectoryMark[DMA11];
- Estudo de caso do desempenho (adicionar, remover, alterar, atualizar) de diversos backends disponíveis para o OpenLDAP: ldbm, bdb, passwd, dentre outros.

Bibliografia

[ALB01] ALBITZ, Paul, et. al. DNS and BIND, 4th Edition. Sebastopol, CA: O'Reilly, 2001.

[CAR09] CARTER, Gerald. LDAP, Administração de Sistemas. Rio de Janeiro:Alta Books,, 2009.

[CYR01] Project Cyrus. Na *Internet* em http://www.cyrusimap.org. Página acessada em Novembro de 2011.

[DEB01] Instalação via rede a partir de um CD mínimo. Na *Internet* em http://www.debian.org/CD/netinst . Pagina acessada em Novembro de 2011.

[DMA11] The LDAP Server Benchmarking Tool – DirectoryMark. Na *Internet* em http://www.mindcraft.com/directorymark. Pagina acessada em Outubro de 2011.

[FIN05] FINDLAY, Andrew. LDAP Schema Design. Na *Internet* em http://www.skills-1st.co.uk/papers/ldap-schema-design-feb-2005/ldap-schema-design-feb-2005.html. Página acessada em Junho de 2011.

[GUP02] GUPTA, Meeta, et al; TCP/IP A Biblia. Rio de Janeiro: Campus Elsevier, 2002.

[HOL03] HOLME, Dan, etc. al. Administração e Manutenção do Ambiente Microsoft Windows Server 2003. Washington: Microsoft Press, 2003.

[HOW03] HOWES, Timothy A., et.al; Understanding and Deploying LDAP Directory Services, Second Edition.Boston: Addison Wesley, 2003.

[IBM11] Setting up for LDBM. Na *Internet* em http://publib.boulder.ibm.com/infocenter/zvm/v5r4/index.jsp?topic=/com.ibm.zvm.v54.kill0/tivldbm.htm. Página acessada em Setembro de 2009.

[ISO01] ISO - International Organization for Standardization. Na *Internet* em http://www.iso.org/iso/home.htm. Página acessada em Setembro de 2011.

[LDU11] LDAP Duplication/Replication/Update Protocols (ldup) – Documents. Na Internet em http://datatracker.ietf.org/wg/ldup/charter. Página acessada em Novembro de 2011.

[LCU00] LDAP Client Update Protocol (LCUP). Na Internet em http://www.ietf.org/proceedings/47/slides/ldap-lcup-00mar/index.htm. Página acessada em Novembro de 2011.

[MAC06] MACHADO, Erich Soares. Autenticação Integrada Baseada no Serviço de Diretorio LDAP. Na *Internet* em http://www.linux.ime.usp.br/~cef/mac499-06/monografias/erich/html. Pagina acessada em Junho de 2011.

[MAN01] slapd.conf(5) - Linux man page. Na *Internet* em http://linux.die.net/man/5/slapd.conf. Página acessada em Novembro de 2011.

[MIC01] Microsoft Technet – Windows Server TechCenter, Requisitos e Recomendações para a instalação do Active Directory – Por: Artur Higashiyama. Na *Internet* em http://technet.microsoft.com/pt-br/library/cc668535.aspx. Página acessada em Outubro de 2011.

[MIC02] Microsoft Technet – Windows Server TechCenter, Instalando uma nova floresta usando um arquivo de resposta . Na *Internet* em http://technet.microsoft.com/pt-br/library/cc770303(WS.10).aspx. Pagina acessada em 10/10/2011.

[MIC03] Requisitos de Sistema, Windows Server 2003. Na *Internet* em http://technet.microsoft.com/pt-br/windowsserver/bb430827.. Página acessada em Novembro de 2011.

[MIC04] Instalação Server Core do Windows Server 2008. Na *Internet* em http://www.microsoft.com/brasil/servidores/windowsserver2008/servercore.mspx . Página acessada em Novembro de 2011.

[MIC05] Requisitos de instalação do AD DS. Na *Internet* em http://technet.microsoft.com/pt-br/library/cc771188(WS.10).aspx. Pagina acessada em Outubro de 2011.

[MIC06] Como implementar diretivas do sistema para computadores cliente baseados no Windows XP, com base no Windows 2000 e baseados em Windows Server 2003 em ambientes que não sejam do Active Directory. Na *Internet* em http://support.microsoft.com/kb/910203/pt-br. Pagina acessada em Dezembro de 2011.

[MIC07] Backing Up Your Server. Na *Internet* em http://technet.microsoft.com/en-us/library/cc753528.aspx. Pagina acessada em Dezembro de 2011.

[MIC11] Microsoft Technet - Windows Server TechCenter. Na *Internet* em http://technet.microsoft.com/pt-br/library/cc785254(WS.10).aspx. Pagina acessada em Junho de 2011.

[OPE01] OpenLDAP. Introduction to OpenLDAP Directory Services. Na *Internet* em http://www.openldap.org/doc/admin24/intro.html. Página acessada em Fevereiro de 2011.

[OPE02] OpenLDAP - Public License for 2.4.26. Na *Internet* em http://www.openldap.org/software/release/license.html. Página acessada em Outubro de 2011.

[OPE03] OpenLDAP, Main Page. Na *Internet* em http://www.openldap.org. Página acessada em Novembro de 2011.

[ORA11] What is Berkeley DB? . Na *Internet* em http://download.oracle.com/docs/cd/E17076_02/html/programmer_reference/intro_dbis.html. Pagina acessada em Setembro de 2011.

[ORA01] Oracle Berkeley DB Downloads. Na *Internet* em http://www.oracle.com/technetwork/database/berkeleydb/downloads/index.html. Página acessada em Novembro de 2011.

[PSL01] Portal do Software Livre. Na *Internet* em http://www.softwarelivre.gov.br. Página acessada em Novembro de 2011.

[PSL02] Centro de Difusão de Tecnologia e Conhecimento – CDTC. Na *Internet* em http://www.cdtc.org.br. Página acessada em Novembro de 2011.

[PSL03] Centro de Difusão de Tecnologia e Conhecimento – CDTC. Na *Internet* em http://cursos.cdtc.org.br.. Página acessada em Novembro de 2011.

[PSL04] Moodle da Comunidade – CDTC. Na *Internet* em http://comunidade.cdtc.org.br/. Página acessada em Novembro de 2011.

[PSL05] Guia Livre – Programa de Governo Eletrônico Brasileiro. Na *Internet* em http://governoeletronico.gov.br/acoes-e-projetos/guia-livre. Página acessada em Novembro de 2011.

[PSL06] Portal do Software Publico; Na *Internet* em http://www.softwarepublico.gov.br. Página acessada em Novembro de 2011.

[REI03] REIMER, Stan, et al; *Active Directory* for Microsoft Windows Server 2003 Technical Reference. Microsoft Press, 2003.

[RFC1034] DOMAIN NAMES - CONCEPTS AND FACILITIES. Na *Internet* em http://www.ietf.org/rfc/rfc1034.txt. Página acessada em Dezembro de 2011.

[RFC1157] A Simple Network Management Protocol (SNMP). Na *Internet* em http://www.ietf.org/rfc/rfc1157.txt. Página acessada em Dezembro de 2011.

[RFC1279] X.500 and Domains. Na *Internet* em http://www.ietf.org/rfc/rfc1279.txt. Página acessada em Dezembro de 2011.

[RFC1405] Mapping between X.400(1984/1988) and Mail-11 (DECnet mail). Na *Internet* em http://www.ietf.org/rfc/rfc1405.txt. Página acessada em Julho de 2011.

[RFC1487] X.500 Lightweight Directory Access Protocol. Na *Internet* em http://www.ietf.org/rfc/rfc1487.txt. Página acessada em Julho de 2011.

[RFC1777] Lightweight Directory Access Protocol. Na *Internet* em http://www.ietf.org/rfc/rfc1777.txt. Página acessada em Julho de 2011.

[RFC2251] Lightweight Directory Access Protocol (v3). Na *Internet* em http://www.ietf.org/rfc/rfc2251.txt. Página acessada em Julho de 2011.

[RFC2252] Lightweight Directory Access Protocol (v3): Attribute Syntax Definitions. Na *Internet* em http://www.ietf.org/rfc/rfc2252.txt. Página acessada em Julho de 2011.

[RFC2253] Lightweight Directory Access Protocol (v3): UTF-8 String Representation of Distinguished Names. Na *Internet* em http://www.ietf.org/rfc/rfc2253.txt. Página acessada em Julho de 2011.

[RFC2254] The String Representation of LDAP Search Filters. Na *Internet* em http://www.ietf.org/rfc/rfc2254.txt. Página acessada em Julho de 2011.

[RFC2255] The LDAP URL Format. Na *Internet* em http://www.ietf.org/rfc/rfc2255.txt. Página acessada em Julho de 2011.

[RFC2256] A Summary of the X.500(96) User Schema for use with LDAPv3. Na *Internet* em http://www.ietf.org/rfc/rfc2256.txt. Página acessada em Julho de 2011.

[RFC2849] The LDAP Data Interchange Format (LDIF) - Technical Specification. Na *Internet* em http://www.ietf.org/rfc/rfc2849.txt. Página acessada em Julho de 2011.

[RFC3377] Lightweight Directory Access Protocol (v3): Technical Specification. Na *Internet* em http://www.ietf.org/rfc/rfc3377.txt. Página acessada em Julho de 2011.

[RFC4422] Simple Authentication and Security Layer (SASL). Na *Internet* em http://www.ietf.org/rfc/rfc4422.txt. Página acessada em Novembroo de 2011.

[SAM01] What is Samba?. Na *Internet* em http://www.samba.org/samba/what_is_samba.html. Página acessada em Outubro de 2011.

[SAM02] Samba4 – SambaWiki. Na *Internet* em http://wiki.samba.org/index.php/Samba4. Página acessada em Outubro de 2011.

[SAM03] smb.conf(5) - Linux man Page. Na *Internet* em http://linux.die.net/man/5/smb.conf. Página acessada em Novembro de 2011.

[SAM04] Samba - opening windows to a wider world. Na *Internet* em http://www.samba.org. Página acessada em Novembro de 2011.

[SAM05] SambaWiki. Na *Internet* em http://wiki.samba.org. Página acessada em Novembro de 2011.

[SPE06] SPEALMAN, Jill, et. al. Planming, Implementing, and Maintaing a Microsoft Windows Server 2003 *Active Directory* Infrastructure. Washington: Microsoft Corporation, 2006.

[SSL01] OpenSSL: The Open Source Toolkit for SSL/TLS. Na *Internet* em http://www.openssl.org . Página acessada em Novembro de 2011.

[SUN07] SUNGALIA, Marcos. Autenticação Centralizada com o OpenLDAP. São Paulo: Novatec, 2007.

[TRI07] TRIGO, Clodonil Honório. OpenLDAP, Uma abordagem integrada. São Paulo: Novatec, 2007.

[TEL01] Origen do LDAP. Na *Internet* em http://www.teleco.com.br/tutoriais/tutorialldap1/pagina_3.asp. Página acessada em Novembro de 2011.

[TFA11] Active Directory Replication | Microsoft Active Directory | Asked and Answered. Na *Internet* em http://www.tech-faq.com/active-directory-replication.html. Página acessada em 01/08/2011.

[TOP03] The OpenLDAP Project. OpenLDAP 2.1 Administrator's Guide. Na *Internet* em http://www.bind9.net/manual/openldap/2.1/index.html. Pagina acessada em Junho de 2011.

[UIS2011] TCP Wrappers. Na *Internet* em http://itso.iu.edu/TCP_Wrappers. Pagina acessada em Setembro de 2009.

[UFR11] Serviços de Diretório. Na *Internet* em http://penta.ufrgs.br/aplicosi/x500/x5001.html. Pagina acessada em Novembro de 2011.

[ZYT11] Chapter 6: OpenLDAP using cn=config. Na *Internet* em www.zytrax.com/books/ldap/ch6/slapd-config.html. Página acessada em 03/11/2011.

[WIK01] Digest access authentication. Na *Internet* em http://en.wikipedia.org/wiki/Digest_access_authentication. Pagina acessada em Novembro de 2011.

ANEXO I – Pesquisa com Administradores de Sistemas

Foi criado o seguinte formulário e publicado na *Internet* em: http://www.mtulio.eti.br/tcc.html:

1.1 - Nome *

Digite seu nome.

_____

1.2 - Sobrenome *

Digite seu sobrenome.

_____

1.3 - E-mail *

Digite o seu e-mail que lhe foi enviado o convite para esta pesquisa.

_____

1.4 - Empresa / Instituição

Campo opcional. Apenas para integridade na pesquisa. Obs.: Esses dados não serão publicados.

_____

1.5 - Função

Campo opcional. Função ocupada na entidade.

_____

2 - Ramo de atividade da entidade *

- Setor Industrial
- Setor Comercial
- Setor Governamental
- Setor Acadêmico
- Outro:

_____

3 - Quantidade de usuários? *

- 1-50

- 51-250
- 251-500
- 501-5.000
- 5.001-10.000
- Acima de 10.000

---

4 - Qual implementação utilizada do serviço de diretório no protocolo LDAP ? *

- Microsoft Active Directory
- OpenLDAP
- Red Hat Directory Server
- IBM Directory Server
- Novell eDirectory
- Sun ONE Directory Server
- Oracle *Internet* Directory
- Outro:

---

5 - Porque escolheu esta implementação? *

Motivo que o levou, ou a instituição, a utilizar esta implementação, pode ser por facilidade ou particularidades quaisquer. Descreva-as aqui.

---

6 - Quais foram às principais dificuldades na elaboração de projetos da estrutura de diretórios? *

Descreva as dificuldades (se houveram) para projetar, organizar e estruturar toda árvore organizacional da estrutura de diretórios. Cada implementação é feita de acordo com as regras de negocio da empresa, por exemplo, a distribuição de Sites (ou Filiais) em diversas OU (Unidades Organizacionais) ou em subdomínios. Fale também sobre as experiências adquiridas neste projeto.

---

7 - Quais foram às principais dificuldades na implantação? *

Descreva as dificuldades na implantação da ferramenta.

_____

_____

8 - Escolheria outra ferramenta? Uma segunda opção! Por quê? *

Se a ferramenta não atendeu as expectativas, descreva quais os problemas encontrados. Se estudado a implantação de outra ferramenta, descreva logo abaixo os motivos.

_____

_____

9 - Você utilizaria o OpenLDAP? Por quê? *

Caso não utilize o OpenLDAP, mas o conheça, dê sua opinião sobre esta implementação. Com isso podemos saber as dificuldades de utilização/implementação/administração desta Ferramenta.

_____

_____

10 - Você utilizaria o *Active Directory*? Por quê? *

Caso não utilize o Active Directory, mas o conheça, dê sua opinião sobre esta implementação. Com isso podemos saber as dificuldades de utilização/implementação/administração desta ferramenta.

_____

_____

11 - Já foi necessário implementar um schema? Para atender a necessidade de alguma aplicação, por exemplo. *

Os Schemas definem os tipos de dados e elementos de informação que você pode armazenar em um diretório. Geralmente alguma aplicação com finalidade especifica necessita armazenar informações no LDAP no qual ele não suporta. Caso já tenha passado por essa experiência, por favor, descreva com detalhes logo abaixo.

_____

_____

12 - Alguma observação sobre esta pesquisa?

Descreva qualquer critica, sugestão, observação ou algum assunto que não foi abordado neste questionário. Fique a vontade.

_____

_____

ANEXO II - Instalação OpenLDAP e SAMBA

A isntalação dos servidores SAMBA e OpenLDAP será abordada de forma superficial, abordando os principais conceitos. Após a instalação será feito a inserção de diversos usuários no diretorio a partir de scripts desenvolvido neste trabalho para concretização do estudo dos mesmos.

Antes de iniciar a instalação dos serviços, o Sistema Operacional hospedeiro deverá atender alguns pré-requisitos de configuração e instalação de softwares para o bom funcionamento.

1) Pré-requisitos de compilação dos pacotes. Os seguintes utilitários devem ser instalados:
    a. GNU make
    b. Compilador C comparível com padrão ISO/ANSI
    c. Compactadores gzip e bzip2
    d. Utilitário tar
    e. Utilitário patch

Parte 1: Instalação do SAMBA

Embora não possa agir como o Active Directory Primary Domain Controller (PDC), o SAMBA até a versão atual estavél 3.6.1, é um servidor que pode ser configurado para atuar como um controlador de domínio Windows NT4. Uma grande vantagem desta configuração é a capacidade de centralizar as credenciais do usuário e máquina. O SAMBA também pode utilizar múltiplos backends para armazenar as informações do usuário.

1) Instalação dos pacotes

Será detalhada a instalação pelo código fonte, gerenciador de pacotes yum (distribuições Red Hat e derivados) e no gerenciador de pacotes apt (Debian e derivados).

a. Instalação a partir do código fonte

Para iniciar a instalação e configuração do Samba como PDC (*Primary Domain Controler* – Controlador de Domínio Primário) é necessário fazer o Download do código fonte no site oficial [SAM04].

O primeiro passo é descompactá-lo:

```
$ tar xfz samba.3X.tar.gz
```

No diretório que foi descompactado existe um diretório chamado *source*, este é o diretório que será compilado e logo após é chamado o script de configuração `configure` enviando argumentos parametrizando o sistema para compilação:

```
$ cd samba*/source
$ ./configure –prefix=/usr/local/samba –with-ldap –whith-
 ldapsam
```

NOTA: Os parâmetros –with-ldap e with-ldapsam definem que o Samba terá suporte ao LDAP. Para conhecer todos os parâmetros possíveis, execute o script configure com a opção –help.

O próximo passo é compilar e instale o SAMBA:

```
$ make
$ make install
$ make installbin
$ make installman
```

Instalação concluída pelo código fonte

b. Instalação pelo Gerenciador de Pacotes YUM

O Gerenciador de pacotes YUM, é utilizado principalmente em sistemas Red Hat Enterprise Linux, CentOS, Fedora e outros baseados no RHEL. Para instalação do samba, execute os seguintes comandos:

```
$ yum intall –y samba samba-client samba-common samba-
  winbind samba-doc ntp
```

c. Instalação pelo Gerenciador de Pacotes APT

O Gerenciador de pacotes APT, é utilizado principalmente em sistemas Debian, Ubuntu e outros baseados no Debian. Para instalação do samba, execute os seguintes comandos:

```
$ apt-get install samba smbclient samba-doc smbfs ntp
 smbldap-tools
```

2) Arquivos, comandos e diretórios.

Seguem algumas informações básicas sobre os arquivos de configuração e comandos:

- /etc/samba: Diretório padrão de configuração;
- /etc/samba/smb.conf: arquivo principal de configuração, dentro deste pode ser feito inclusões de outros arquivos ou pode-se informar outro arquivo na inicialização do servidor;
- /etc/init.d/smb: script que controla a inicialização/reinicializarão/desligamento do Servidor Samba;
- testparm: verifica a sintaxe do arquivo de configuração;
- smbclient: Acessa recursos do servidor SMB/CIFS pela linha de comando. Semelhante ao FTP;
- smbstatus: Exibe as conexões atuais;
- smbd: Comando principal do servidor SMB/CIFS.

Parte 2: Instalação OpenLDAP

Caso seja escolhida a opção de compilação dos pacotes a partir dos códigos fonte, será necessário ter os softwares listados como pré-requisitos no inicio desta seção confiugrados.. O OpenLDAP necessita também de pacotes para armazenamento dos dados, os backends, e bibliotecas para criptografia. Para isto, os seguintes softwares serão instalados:

- OpenSSL
- Berkley DB
- Cyrus-SASL
- OpenLDAP

1) Instalação OpenSSL

OpenSSL é a Biblioteca básica de criptografia para sistemas Linux. Faça o download dos pacotes em sua versão mais recente disponível no Site Oficial [SSL01].

a. Instalação a partir do código fonte

Copie os fontes para o diretorios /usr/src e execute os seguintes comandos:.

```
$ cd /usr/src;
$ tar xvfz openssl-1.0.tar.gz;
$ cd openssl-1.0;
```

```
$./configure –prefix=/usr –openssldir=/usr/lib/ssl shared;
$ make;
$ make test;
$ make install;
$ ldocnfig
```

b. Instalação pelo Gerenciador de Pacotes YUM

```
$ yum install openssl
```

c. Instalação pelo Gerenciador de Pacotes APT

```
$ apt-get install opensl libss10.9.8
```

2) **Instalação Berkley DB**

O Oracle Berkley DB é o gerenciador das informações armazenadas na base. . Faça o download dos pacotes em sua versão mais recente disponível no Site Oficial [ORA01].

a. Instalação a partir do código fonte

Copie os fontes para o diretorios /usr/src e execute os seguintes comandos:

```
$ cd /usr/src;
$ tar xzf db-4.8.tar.gz;
$ cd db-4.8/build_unix; .
$./dist/configure –prefix=/usr/local;
$ make;
$ make install;
$ ldconfig
```

b. Instalação pelo Gerenciador de Pacotes YUM

```
$ yum install db4 db4-devel
```

c. Instalação pelo Gerenciador de Pacotes APT

```
$ apt-get install db4.8-util
```

3) **Instalação Cyrus-SASL**

O SASL (*Simple Authentication and Security Layer*) define um método de prover autenticação segura para protocolos orientados à conexão, ela é utilizada como ferramenta de autenticação e comunicação criptografada. Faça o download dos pacotes em sua versão mais recente disponível no Site Oficial [CYR01].

a. Instalação a partir do código fonte

Copie os fontes para o diretorios /usr/src e execute os seguintes comandos:

```
$ cd /usr/src;
$ tar xfz cyrus-2.1.25.tar.gz;
$ cd cyrus-2.1.25x;
$./configure –prefix=/usr –enable-static –
mandir=/usr/share/man –infidir=/usr/share/info;
$ make;
$ make install
```

b. Instalação pelo Gerenciador de Pacotes YUM

```
$ yum install cyrus-sasl cyrus-sasl-lib cyrus-sasl-devel
cyrus-sasl-ldap
```

c. Instalação pelo Gerenciador de Pacotes APT

```
$ apt-get install sasl2-bin libsasl2-2 libsasl2-modules
libsasl2-modules-ldap
```

4) **Instalação OpenLDAP**

Para instalação do OpenLDAP em uma distribuição que não possua um pacote personalizado ou pré-compilado o primeiro passo é obter os códigos fontes a partir do site. Faça o download dos pacotes em sua versão mais recente disponível no Site Oficial [OPE03].

a. Instalação a partir do código fonte

Copie os fontes para o diretorios /usr/src e execute os seguintes comandos:

```
$ cd /usr/src;
$ tar xzf openldap-2.4.28;
$ cd openldap-2.4.28;
$ ./configure –with-threads –with-tls;
$ make depend;
$ make;
$ make install
```

b. Instalação pelo Gerenciador de Pacotes YUM

```
$ yum install openldap openldap-servers openldap-devel
```

c. Instalação pelo Gerenciador de Pacotes APT

```
$ apt-get install slapd ldap-utils
```

NOTA: A senha de administrador da Base LDAP será solicitada pelo instalador, informe-a.

Caso todos os procedimentos tenham ocorrido sem nenhum erro, o servidor OpenLDAP foi instalado com êxito.

ANEXO III - Configurando do SAMBA e OPENLDAP

Esta seção apresentará a configuração dos servidores SAMBA e OpenLDAP. Essa configuração será baseada na estrutura proposta para estudo de caso deste trabalho descrito no Item 4.3 e ilustrado na Figura 4.1 e Figura 4.3.

Este anexo é dividido nas seguintes partes:

1. Configurar o SAMBA como PDC
2. Configurar o OpenLDAP com a Base (domínio) DOMOL
3. Criar as Unidades Básicas e população do diretório
4. Integração do Samba com OpenLDAP

Parte 1 – Configurando SAMBA como PDC:

Agora com o servidor já instalado, é necessário fazer a configurá-lo para que ele opere como PDC. O arquivo principal de configuração basicamente deve estar basicamente conforme abaixo

1) /etc/samba/smb.conf

```
#=== Global Settings ===
[global]
        workgroup = DOMOL
        netbios name = DOMOL
        server string = DOMOL MTulio ENG

### Domains

        domain logons = Yes
        os level = 100
        preferred master = Yes
        domain master = Yes

        # Windows Internet Name Serving Support Section:
        ## Necessario habilitar o componente NMBD
        wins proxy = Yes
        wins support = Yes
        admin users = mtulio01 administrador root

### Authentication
        # Security = user requer uma conta Unix neste
    servidor
        security = user
        encrypt passwords = yes
        smb passwd file = /etc/samba/smbpasswd

        # Mantem sincrona a senha da Conta Samba com Unix
```

```
        unix password sync = yes

### Debugging
        log level = 1
        log file = /var/log/samba/%m.log
        max log size = 50

### Outras confs

        time server = Yes
        server signing = auto
        socket   options   =   TCP_NODELAY   SO_SNDBUF=8192
    SO_RCVBUF=8192

### LOGON OPTIONS

        add machine script = /usr/sbin/useradd  -c Machine
    -d /var/lib/nobody -s /bin/false %m$
        logon script = %U.bat
        logon drive = P:
        logon path =
        logon home =

#=== Share Definitions ===
[homes]
        path = /samba/home/%U
        comment = "Diretorio Home"
        browseable = no
        read only = yes
# Mascara para criacao de arquivos
        create mask = 0700
# Mascara para permissoes de diretorios
        directory mask = 0700
        valid users = %S

[netlogon]
        path = /samba/compartilhamentos/netlogon
        comment = "Servico de Logon de Rede"
        guest ok = no
        writeable = yes
        share modes = no
        browseable = no

[GERAL]
        path = /samba/compartilhamentos/GERAL
        comment = "DOMOL - Publico"
        writeable = yes
        browseable = yes
        valid users = %U
        write list = %U
```

```
        create mask = 0600
        directory mask = 0700
# Verifique se existe o modulo VFS no sistema
## Habilitando a Lixeira
        vfs objects = recycle
        recycle:repository = ### LIXEIRA ###

# Proibindo gravacao e deletando arquivos indesejados
        veto files = /*.cmd/*.exe/autorun.inf/
        delete veto files = yes
```

NOTA 1: As diretivas de configuração não serão explicadas, pois não é o escopo deste trabalho.

NOTA 2:Para obter ajuda visite o manual do arquivo de configuração digitando o comando:

```
$ man smb.conf [SAM03]
```

Ou a página oficial do SAMBA [SAM04] e no SambaWiki [SAM05].

2) Testando o arquivo de configuração

Para testar a sintaxe do configuração /etc/samba/smb.conf, digite o comando:

```
$ testparm
```

Caso não haja nenhum erro de sintaxe e/ou configuração, o servidor já pode ser iniciado.

3) Iniciando o servidor SAMBA

Obs.: Importante criar todos os diretórios referenciados no arquivo de configuração antes de inicializar o serviço.

O serviço é mantido pelo deamon smbd. Ele pode ser invocado com o seguinte comando:

```
$ smbd –D –s /etc/samba/smb.conf
```

-D : inicia o servidor como *daemon*

-s : especifica o arquivo de configuração

As principais distribuições GNU/Linux operam com scripts de inicialização que podem ser invocados manualmente conforme demonstrado abaixo:

A partir do diretorio principal dos scripts de inicialização /etc/init.d:

```
$ /etc/init.d/smb start
```

Nas distribuições Red Hat e derivados, esse script pode ser invocado com o seguinte commando:

```
$ service smb start
```

Nas distribuições Debian e derivados, pode ser invocado através do seguinte comando:

```
$ invoke-rc.d samba restart
```

Parte 2 - Configurando OpenLDAP

O OpenLDAP implementado neste trabalho terá suporte ao SAMBA sendo necessário carregar os schemas do mesmo em sua configuração. A instalação do samba foi feita antes da instalação do OpenLDAP, para configurar os módulos e *schemas* necessários para atenderem a demanda deste trabalho, porém, essa configuração pode ser feita dinamicamente de acordo com a expansão e necessidade do diretório, essa característica é possível pois o OpenLDAP é um servidor de diretórios flexível e de propósitos gerais .

Será abordado o OpenLDAP com a opção de *runtime*, discutido no Item 4.4.2.1. Porém, foi criado um arquivo de configuração "tradicional" e em seguida o mesmo foi convertido para inserções das entradas na DIT de configuração do servidor LDAP, cn=config.

1) Arquivo de configuração slapd.conf

Primeiramente foi criado o arquivo de configuração do OpenLDAP, slapd.conf, conforme detalhado abaixo. Detalhes das opções dos arquivos de configuração não irão além dos comentários no mesmo, para mais detalhes consulte o manual com o seguinte comando:

```
$ man slapd.conf [MAN01]
```

Arquivo slapd.conf:

```
# Arquivo de configuracao do OpenLDAP adaptado
# para utilizacao no Trabalho de Conclusao de Curso.
#
# Qualquer duvida consulte o manual: man slapd.conf
#
# Contato p/ Duvidas e sugestoes: admin@mtulio.eti.br
#
# Criado Por: Marco Tulio R Braga
#=== Global Settings ===

#### Schemas ####

include /etc/ldap/schema/core.schema
```

```
include /etc/ldap/schema/corba.schema
include /etc/ldap/schema/cosine.schema
include /etc/ldap/schema/inetorgperson.schema
include /etc/ldap/schema/misc.schema
include /etc/ldap/schema/nis.schema
include /etc/ldap/schema/openldap.schema

include /etc/ldap/schema/samba.schema

include /etc/ldap/schema/collective.schema
include /etc/ldap/schema/duaconf.schema
include /etc/ldap/schema/dyngroup.schema
include /etc/ldap/schema/java.schema
include /etc/ldap/schema/ppolicy.schema

#### Authentication ####

# This option configures one or more hashes to be used
# in generation of user passwords stored in the
userPassword
# attribute during processing
# of LDAP Password Modify Extended Operations (RFC 3062).
# Parameters: {SHA}, {SMD5}, {MD4}, {CRYPT}, {CLEARTEXT}
password-hash           {CRYPT}

# Search base
defaultsearchbase       dc=domol,dc=mtulio,dc=eng,dc=br

################################

# Verificacao do cliente nao eh requerida
# NOT SECURE: Only this case study
TLSVerifyClient never

################################

pidfile         /var/run/slapd/slapd.pid
argsfile        /var/run/slapd/slapd.args
loglevel        512

logfile         /var/log/ldap.log

# Where the dynamically loaded modules are stored
modulepath      /usr/lib/ldap
moduleload      back_hdb
moduleload      back_monitor

# Permissions

access to dn.base=""
```

```
        by * read

access to dn.subtree=cn=Monitor
        by * read

# The userPassword/shadow Emtries by default can be
# changed by the entry owning it if they are authenticated.
# Others should not be able to see it, except the admin
# entry below
access to
attrs=userPassword,sambaPwdLastSet,sambaPwdMustChange,samba
PwdCanChange,shadowMax,shadowExpire
        by
dn.regex="uid=[^/]+/admin\+(realm=GONICUS.LOCAL)?" write
        by anonymous auth
        by self write
        by * none

# Samba passwords by default can be changed
# by the entry owning it if they are authenticated.
# Others should not be able to see it, except the
# admin entry below
access to attrs=sambaLmPassword,sambaNtPassword
        by
dn.regex="uid=[^/]+/admin\+(realm=DOMOL.MTULIO.ENG.BR)?"
write
        by anonymous auth
        by self write
        by * none

# The admin dn has full write access
access to *
        by
dn.regex="uid=[^/]+/admin\+(realm=DOMOL.MTULIO.ENG.BR)?"
=wrscx
        by * read


#############################
# database definitions
#############################

# Monitor backend
database        monitor

# The backend type, ldbm, is the default standard
database        hdb
cachesize 5000
mode             0600
```

```
# The base of your directory
suffix          "dc=domol,dc=mtulio,dc=eng,dc=br"
checkpoint      512 720

# Sample password is "tester", generate a new one using the
mkpasswd
# utility and put the string after {crypt}
rootdn
"cn=administrador,dc=domol,dc=mtulio,dc=eng,dc=br"
rootpw          "123456"

# Indexing
index   default                         sub
index   uid,mail                        eq
index   cn,sn,givenName,ou              pres,eq,sub
index   objectClass                     pres,eq
index   uidNumber,gidNumber,memberuid   eq


# Indexing for Samba 3
index   sambaSID                        eq
index   sambaPrimaryGroupSID            eq
index   sambaDomainName                 eq

# Where the database file are physically stored
directory       "/var/lib/ldap/domol.mtulio.eng.br"

# Log modifications and write entryUUID
lastmod on
```

2) Importanto o schema do samba no OepnLDAP

Copie o arquivo de schema do samba para o diretorio do openldap:

```
$ cp /usr/share/doc/samba-
doc/examples/LDAP/samba.schema.gz /etc/ldap/schema/
$ gunzip /etc/ldap/schema/samba.schema.gz
```

3) Criando diretorio que ficará os arquivos do backend

Criar o diretório que ficará a base de dados - backend:

```
$ mkdir /var/lib/ldap/domol.mtulio.eng.br
```

Definindo permissões para o serviço openldap (usuário e grupo) neste diretorio:

```
$ chown openldap:openldap
 /var/lib/ldap/domol.mtulio.eng.br
```

4) Copiando o arquivo DB_CONFIG para o diretorio do backend

O slapd exige que tenha um arquivo DB_CONFIG no diretorio de cada base de dados, neste caso /var/lib/domol.mtulio.eng.br, para isso copie o arquivo padrão para o novo diretorio da nova base e defina as permissões corretas:

```
$ cp /var/lib/ldap/DB_CONFIG
 /var/lib/ldap/domol.mtulio.eng.br/
$ chown openldap:openldap
 /var/lib/ldap/domol.mtulio.eng.br/DB_CONFIG
$ chmod 644 /var/lib/ldap/domol.mtulio.eng.br/DB_CONFIG
```

5) Convertendo o arquivo slapd.conf

Conforme informado anteriormente, para execução do OpenLDAP em modo *runtime* é necessessário criar um servidor inserindo em sua arvore de configuração, cn=config, as configurações do servidor. Como já foi criado um arquivo slapd.conf para melhor entendimento deste trabalho, o mesmo será convertido em arquivos ldif para o servidor ser executado em modo *runtime*. A conversão para o novo formato é feita pela ferramenta slaptest, informando como argumento o arquivo de configuração e o diretório de destino, o seguinte comando ilustra esses passos:

```
$ mkdir /opt/slapd.d
$ slaptest –f /etc/ldap/slapd.conf –F /opt/slapd.d
```

O diretório /opt/slapd.d deve estar vazio. O utilitário fará a conversão gerando a estrutura de diretórios de acordo com as definições do arquivo de configuração, neste caso foram criados os seguintes arquivos e diretórios no /opt/slapd.d:

```
$ ls –la /opt/slapd.d/
-rw------- 1 openldap openldap  999 Nov  1 04:32 cn=config.ldif
drwxr-x--- 3 openldap openldap 4096 Nov  1 04:32 cn=config

$ ls –la /opt/slapd.d/cn\=config/*
-rw------- 1 openldap openldap   396 Nov  1 04:32 cn=module{0}.ldif
drwxr-x--- 2 openldap openldap  4096 Nov  1 04:32 cn=schema
-rw------- 1 openldap openldap 44844 Nov  1 04:32 cn=schema.ldif
-rw------- 1 openldap openldap   513 Nov  1 04:32 olcDatabase={0}config.ldif
-rw------- 1 openldap openldap  1131 Nov  1 04:32 olcDatabase={-1}frontend.ldif
-rw------- 1 openldap openldap   465 Nov  1 04:32 olcDatabase={1}monitor.ldif
-rw------- 1 openldap openldap  6153 Nov  1 04:32 olcDatabase={2}hdb.ldif

$ ls –la /opt/slapd.d/cn\=config/cn\=schema/*
-rw------- 1 openldap openldap 15428 Nov  1 04:32 cn={0}core.ldif
-rw------- 1 openldap openldap  1624 Nov  1 04:32 cn={10}dyngroup.ldif
-rw------- 1 openldap openldap  2520 Nov  1 04:32 cn={11}java.ldif
```

```
-rw------- 1 openldap openldap  3236 Nov  1 04:32 cn={12}ppolicy.ldif
-rw------- 1 openldap openldap  1212 Nov  1 04:32 cn={1}corba.ldif
-rw------- 1 openldap openldap 11290 Nov  1 04:32 cn={2}cosine.ldif
-rw------- 1 openldap openldap  2784 Nov  1 04:32 cn={3}inetorgperson.ldif
-rw------- 1 openldap openldap  1448 Nov  1 04:32 cn={4}misc.ldif
-rw------- 1 openldap openldap  6420 Nov  1 04:32 cn={5}nis.ldif
-rw------- 1 openldap openldap  1252 Nov  1 04:32 cn={6}openldap.ldif
-rw------- 1 openldap openldap 12492 Nov  1 04:32 cn={7}samba.ldif
-rw------- 1 openldap openldap  1450 Nov  1 04:32 cn={8}collective.ldif
-rw------- 1 openldap openldap  4414 Nov  1 04:32 cn={9}duaconf.ldif
```

O Utilitário já cria toda estrutura de diretórios com as respectivas permissões.

6) Iniciando o OpenLDAP Server

Após a conversão do arquivo slapd.conf, é necessário mover os arquivos resultantes para que os deamons inicie com as novas configurações. Por padrão o OpenLDAP busca as informações de configuração no diretorio /etc/ldap/slapd.d carregando-as para memória, caso esse diretorio não exista, o arquivo slapd.conf é lido. Neste caso, será movido as configurações convertidas do arquivo de configuração slapd.conf para o diretorio correto, executando os seguintes comandos:

```
$ mv /etc/ldap/slapd.d /etc/ldap/slapd.d-original
$ mv /opt/slapd.d /etc/ldap/slapd.d
$ chow openldap:openldap –R /etc/ldap/slapd.d
```

Agora o servidor já pode ser iniciado através do comando:

```
$ /etc/init.d/slapd restart
```

NOTA: Caso ocorra alguma problema na inicialização, ou necessite iniciar o diretorio com mais informações, pode ser feito em modo *debug*, utilizando o seguinte comando:

$ slapd –d 16

Quanto mais alto o nível, mais informações serão exibidas.

7) Visualizando a árvore de configuração

Após a execução do servidor, já é possível verificar através de um *Client* a estrutura da árvore de configuração. A Figura III.1 exibe o diretorio de configuração utilizando o software Softerra LDAP Administrator:

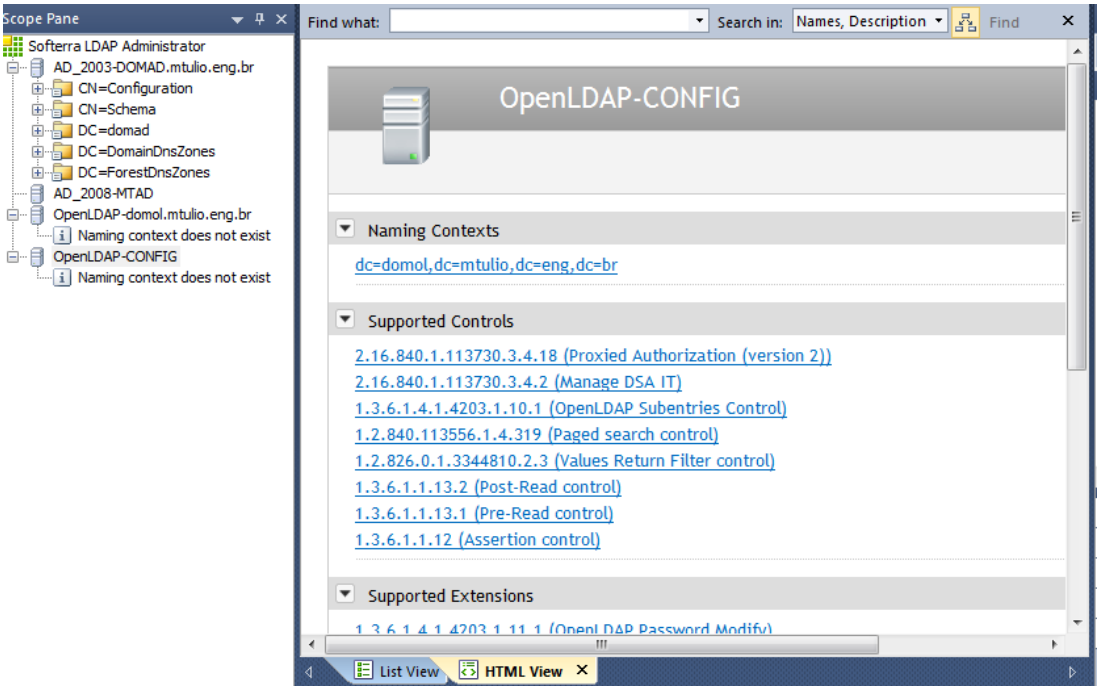

Figura III. 1 - Visualizando a base de configuração do OpenLDAP

Outros frontends de visualização e manipulação da base podem ser utilizados.

8) Adicionando bases de pesquisas, ou domínios, à base LDAP

NOTA: Este passo será executado para melhor entendimento do leitor, pois na Parte 3 desta seção será descrito um script que criará toda estrutura de diretórios proposta neste trabalho.

Até este ponto o servidor OpenLDAP está em execução e pronto para receber informações ou registros. Note que agora é preciso criar a estrutura de diretórios da empresa fictícia, os dados abaixo foram salvos no arquivo denominado, conforme arquivo abaixo denominado domol.mtulio.eng.br.ldif:

```
dn: dc=domol,dc=mtulio,dc=eng,dc=br
objectClass: top
objectClass: dcObject
objectClass: organization
dc: DOMOL
o: MTulio Dominio OpenLDAP
```

Adicione a estrutura da organização no diretorio LDAP através do seguinte comando:

```
$ ldapadd -f domol.mtulio.eng.br.ldif  -x -D
  cn=administrador,dc=domol,dc=mtulio,dc=eng,dc=br -w
  123456
```

Onde:

-f: arquivo *ldif*

-x : necessita de autenticação

-D: informa o adminsitrador da base (informado na definição da base, na árvore cn=config).

-w: informa a senha em texto plano

Visualizando o resultado na árvore:

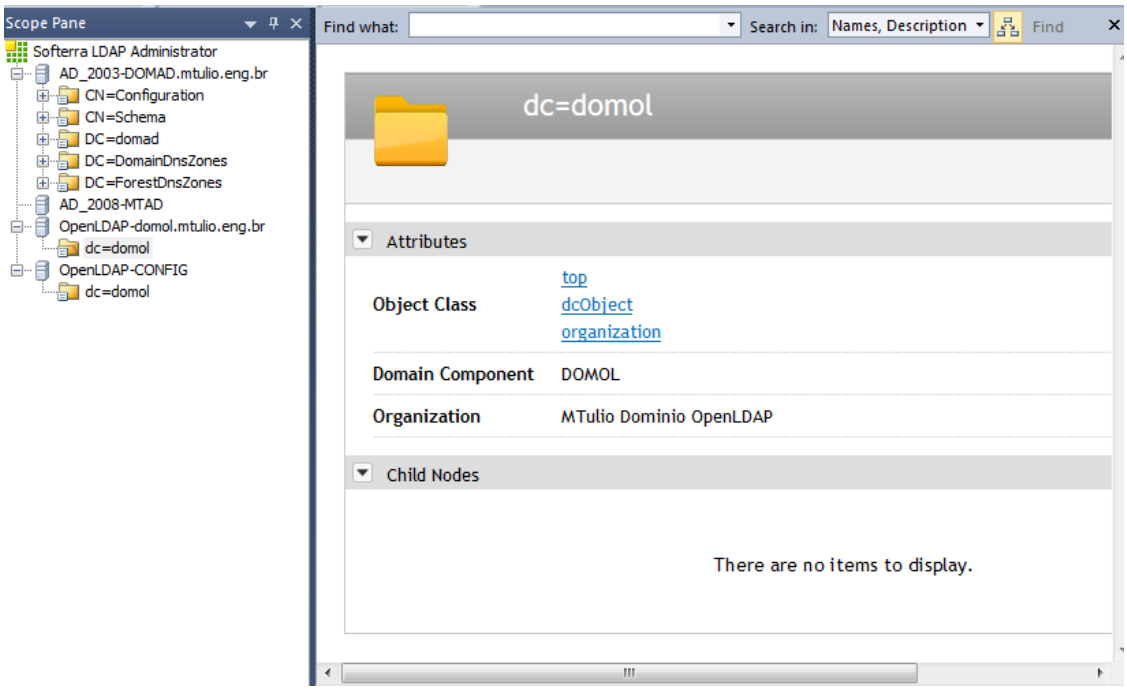

Figura III. 2 – Visualizando a base dc=domol no OpenLDAP

Agora que o servidor de diretórios OpenLDAP está apto a receber registros, já possível popular a base de acordo com a estrutura proposta neste trabalho.

Parte 3 – Populando a Base

Para automatização e melhor entendimento deste trabalho, foi criado uma empresa fictícia detalhada no Item 4.3 e para criação da estrutura da mesma foi desenvolvido um script que tem as seguintes finalidades:

- Criar a estrutura base da organização: domol.mtulio.eng.br;
- Criar as unidades organizacionais básicas descritas no Item 4.3.3.

O script completo está no Anexo VI. Para mais detalhes ou contribuição e adição de novas funcionalidades do script, basta entrar em contato o autor através do e-mail no cabeçalho do mesmo.

Detalhes sobre a execução do script.

Salvando o script no sistema de arquivos com o nome proposto, é possível executá-lo com uma das opções abaixo

1) Executando em um novo terminal bash:

```
$ bash DOMOL_criarEstrutura.sh
```

2) Executando no terminal atual:

```
$ ./DOMOL_criarEstrutura.sh
```

O Script executará os seguintes procedimentos:

- Criará os arquivos LDIF, de acordo com a estrutura prosposta;
- Adicionará ao LDAP os arquivos LDIF gerados;
- Informará o diretorio aonde foram armazenados os LDIF's para futuras consultas;

NOTA: A base não deve estar criada, senão o script retornará erro informando que o registro já existe.

Variaveis que podem ser ajustadas

Para melhor entendimento, testes de performance, ou adequação na quantidade de objetos a serem criados na base, as seguintes variaveis podem ser alteradas:

- countAllUsers : Quantidade de usuários a serem adicionados na Base LDAP.
- countAllComputers: Quantidade de computadores a serem adicionados a Base LDAP;
- countAllGroups: Quantidade de grupos a serem adicionados a Base LDAP.
- countAllObjects: Quantidade de objetos de compartilhamento a serem adicionados a Base LDAP.

Arquivos de logs gerados pelo Scrip:

No diretorio que foi armazenado os LDIF's, foram criados os seguintes arquivos de LOG:

- ldap_oper.log : Eventos de sucesso retornados pelo comando ldapadd;
- time.log: Informa o tempo das principais operações executadas pelo script;

Visualização da Estrutura resultante da execução do script

Para melhor visualização e manipulação da base existem diversos frontends. Alguns deles são:

1. Ldap Account Manager:

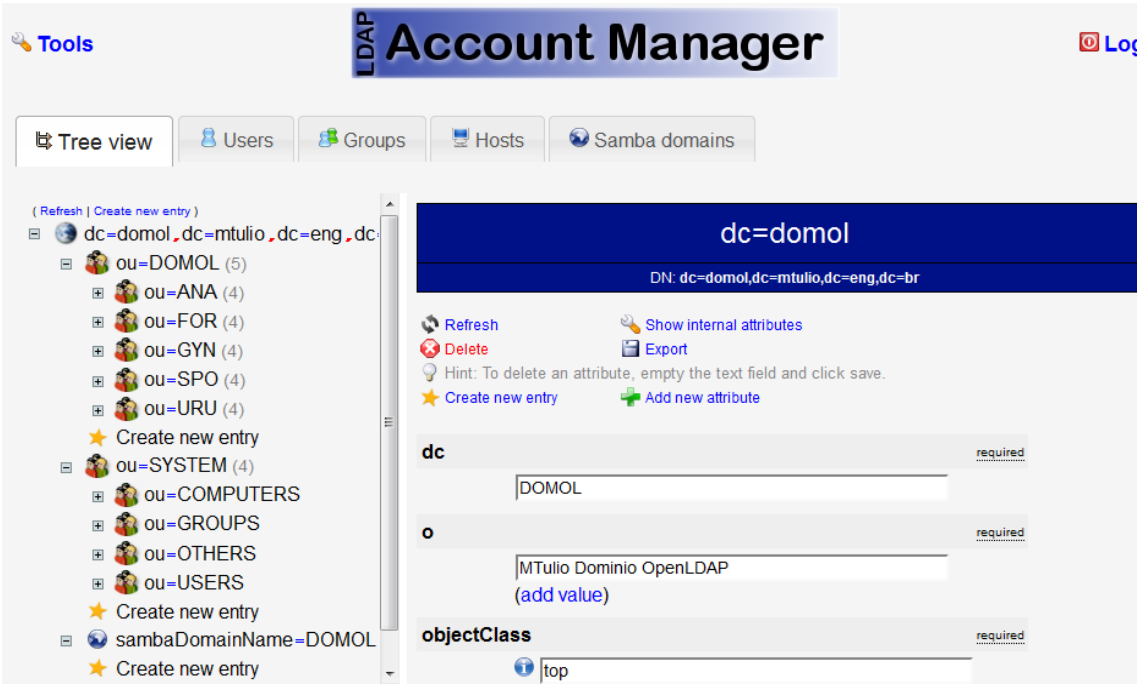

Figura III. 3 – Visualização da Base LDAP - LAM

2. LDAPExplorerTool 2

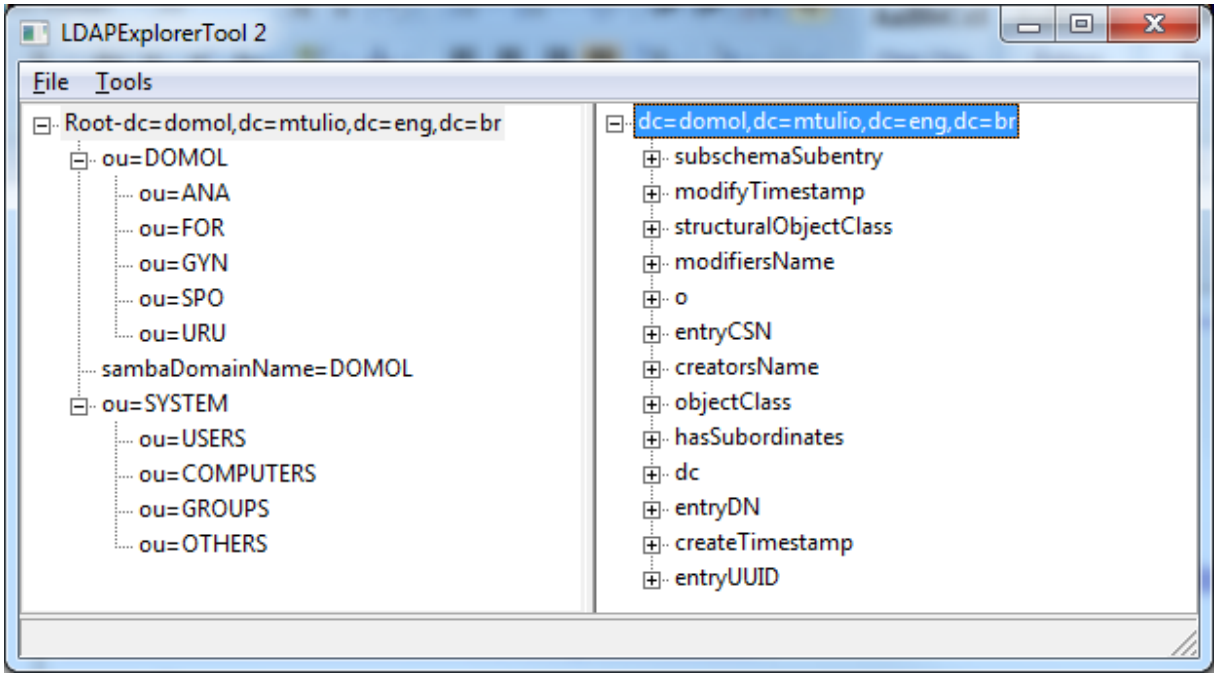

Figura III. 4 – Visualização da Base LDAP – LDAPExplorerTool

Parte 4 – Integrando com SAMBA

A integração do SAMBA com OpenLDAP é bem simples, basta alterar algumas diretivas na seção GLOBALdo arquivo principal de configuração do SAMBA.

NOTA: O schema de suporte ao SAMBA já deve estar disponível nas configurações do OpenLDAP, conforme Parte 2 desta seção, caso contrário a integração não ocorrerá corretamente.

As seguintes linhas devem ser adicionadas na seção global do arquivo de configuração principal do SAMBA, /etc/samba/smb.conf

```
# Base de Autenticacao LDAP
passdb backend = ldapsam:ldap://localhost
ldap admin dn =
cn=administrador,dc=domol,dc=mtulio,dc=eng,dc=br
ldap ssl = off
ldap delete dn = no
ldap user suffix = OU=USERS,OU=SYSTEM
ldap group suffix = OU=GROUPS,OU=SYSTEM
ldap machine suffix = OU=COMPUTERS,OU=SYSTEM
ldap suffix = dc=domol,dc=mtulio,dc=eng,dc=br
```

```
# Permite que usuarios membros do grupo “Domain Admins”
# insiram estações no domínio samba
enable privileges = Yes
```

Reinicie o SAMBA para que as novas configurações sejam aplicadas:

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

ANEXO IV - Instalando o Microsoft Active Directory Domain Services.

Pré-Requisitos:

A instalação do Active Directory, apesar de ser simples, é possível complicar caso não conheça alguns fundamentos básicos. É importante conhecer o design da estrutura do Active Directory.

Para esta implementação, é necessário que o Microsoft Windows Server, neste caso 2003 Standard Edition, esteja instalado em suas configurações padrões.

Segue abaixo alguns requisitos mínimos, boas praticas e algumas recomendações abordadas por Artur [MIC01]:

1) Nome do computador configurado

A escolha do nome NETBIOS do computador é de extrema importância por questões de segurança, padronização, organização e também não é possível fazer essa alteração depois que o servidor DC estiver configurado.

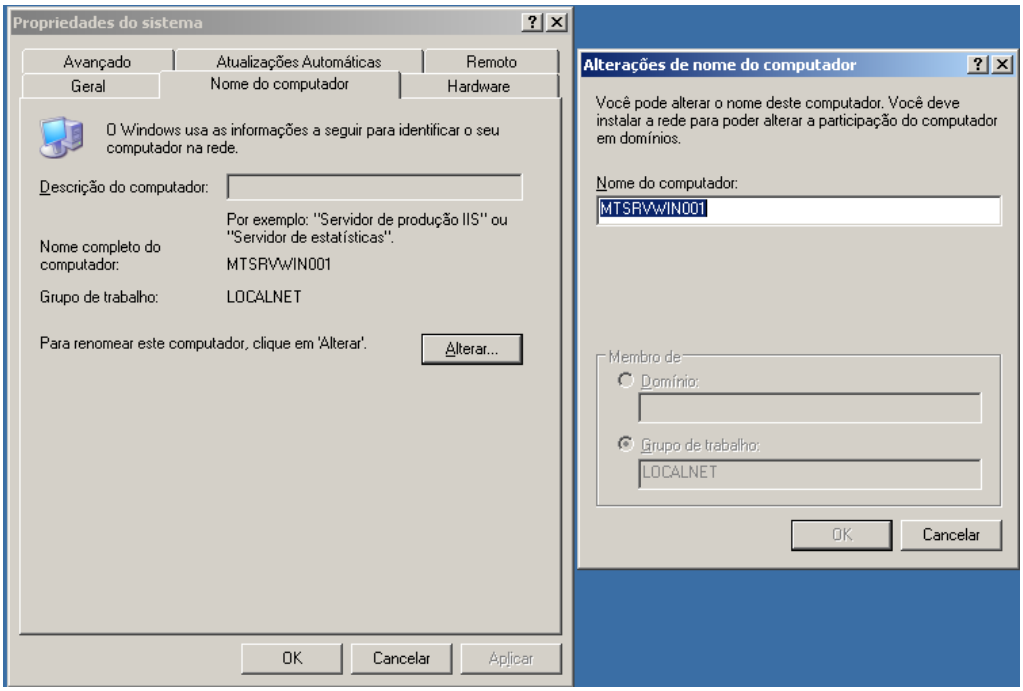

Figura IV. 1 – Alterando Hostname

2) Configurações de Data e Hora

É importante que a Data e Hora do computador esteja correta e sincronizada com servidores de tempos, pois geralmente, o controlador de domínio é um servidor de tempos interno da rede, com isso, se houver incompatibilidade com horário do(s)

servidor(es) com os clientes poderão ocorrer falhas no *logon*, em aplicações, inconsistências nos Banco de Dados e diversos outros problemas.

Para conferir basta abrir o gerenciador de Data e Hora no Painel de controle:

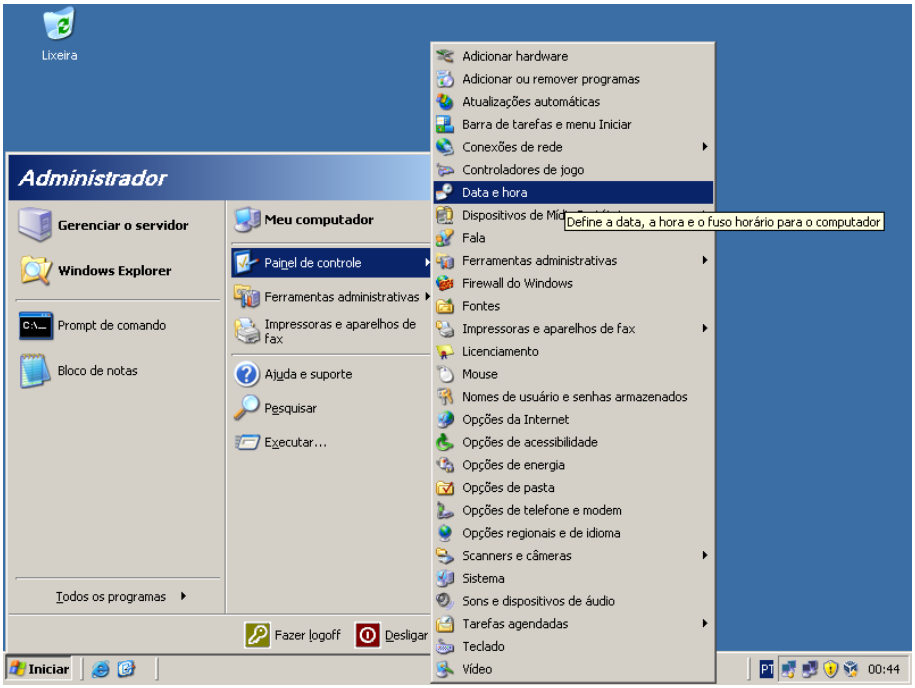

Figura IV. 2 – Alterando Data e Hora

Na tela de Propriedades de Data e Hora confira se está de acordo com a Hora legal de sua região (para conferir a hora legal de sua região entre em: http://ntp.br)

É altamente recomendável que seu servidor atualize o horário com um servidor de tempos especifico para esta finalidade, no Brasil temos os servidores do registro.br (a.ntp.br, b.ntp.br, c.ntp.br, dentre outros podendo verificar no site http://ntp.br), a Microsoft também fornece um servidor de tempos “default” do Sistema, basta que seu fuso-horario esteja bem configurado.

Configurando o Fuso Horário do Brasil:

Figura IV. 3 – Alterando Data e Hora - Timezone

Ajustando para atualização de hora automaticamente pela Internet:

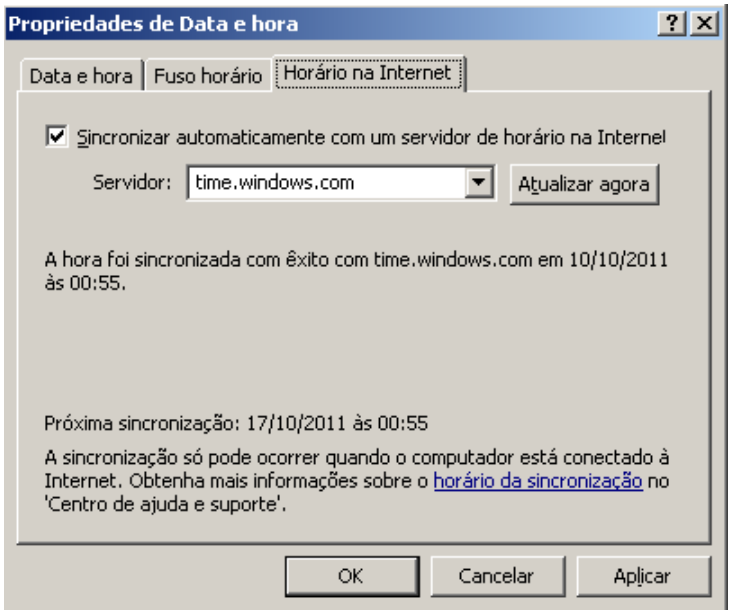

Figura IV. 4 – Alterando Data e Hora – Sincronização automatica

3) Uma partição NTFS com espaço livre suficiente

Para instalação do AD você deve ter pelo menos uma partição com formatação NTFS, preferencialmente a partição onde o Windows está instalado.

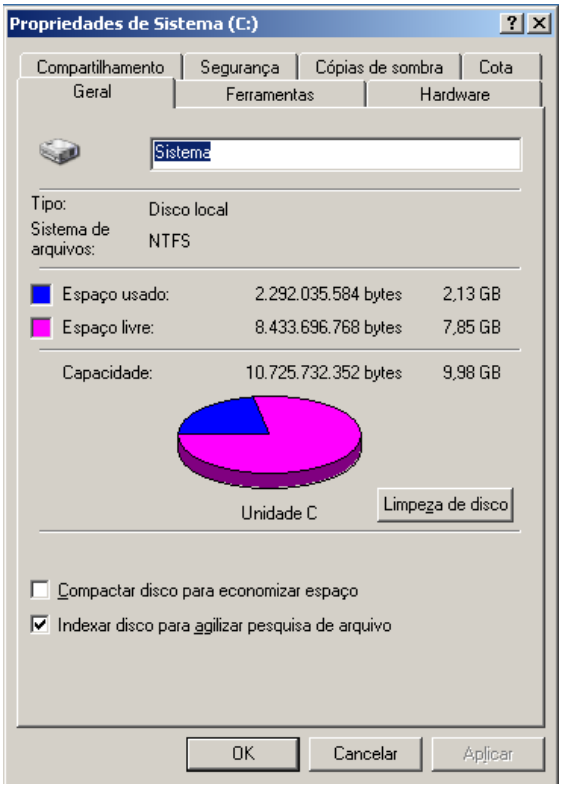

Figura IV. 5 – Verificando Partição

Caso a partição (C:) esteja em FAT, você pode converter a partição para NTFS com o seguinte comando:

```
convert C:/fs:ntfs
```

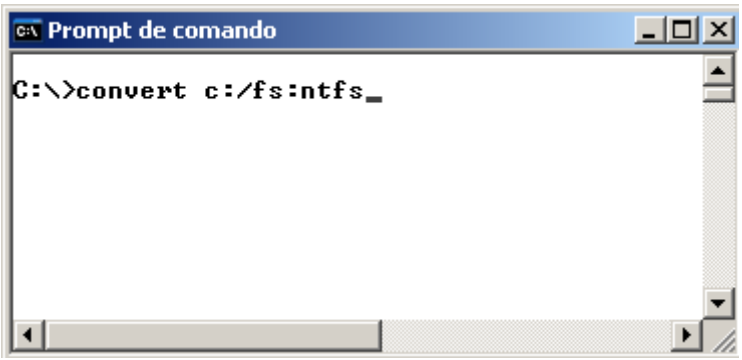

Figura IV. 6 – Convertendo Partição

A partição NTFS é necessária para a pasta SYSVOL.

A partição deve ter pelo menos 250MB de espaço livre para o AD. Obviamente este espaço deve ser compatível com o tamanho da sua rede, de acordo com o número de usuários, grupos, etc. O recomendável para uma rede pequena (até 50 micros) é de 1 GB para o AD.

4) Nome e Senha para o Administrador

Somente o administrador local (ou equivalente) pode instalar o primeiro domínio e assim criar uma nova floresta.

Se você planeja criar outro Controlador de Domínio (DC - Domain Controller) para o domínio existente, você deve ser membro do Domain Admin no domínio que você quer ingressar.

Se você quer criar um domínio filho em um domínio existente ou outra árvore na floresta existente, você deve ser membro do Enterprise Admin.

5) Uma placa de rede

O AD necessita de pelo menos uma placa de rede instalada no computador, isto é, o driver da placa precisa estar corretamente instalado no Windows. Recomenda-se o uso de placas de rede do padrão Gigabit Ethernet que não estejam utilizando o mesmo IRQ com outro dispositivo.

A Figura IV.7 ilustra as interfaces de rede do servidor assim como outros dispositivos:

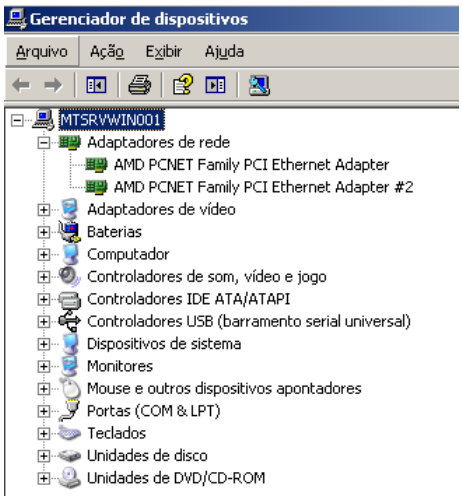

Figura IV. 7 – Configurando Interface de Rede (1)

A Figura IV.8 ilustra uma interface de rede Ativa:

Figura IV. 8 – Configurando Interface de Rede (2)

6) Configurações corretas de TCP/IP (endereço IP, máscara de subrede e gateway)

Você precisa de um endereço IP dedicado (fixo) para instalar o AD. Se você não usar um endereço fixo de IP, os registros DNS podem não funcionar e a funcionalidade do AD será perdida.

O DC do AD deve apontar para o próprio endereço IP na lista de servidores DNS para prevenir possíveis problemas de conexão. A Figura IV.9 ilustra um exemplo de configuração na interface de rede do Servidor DC:

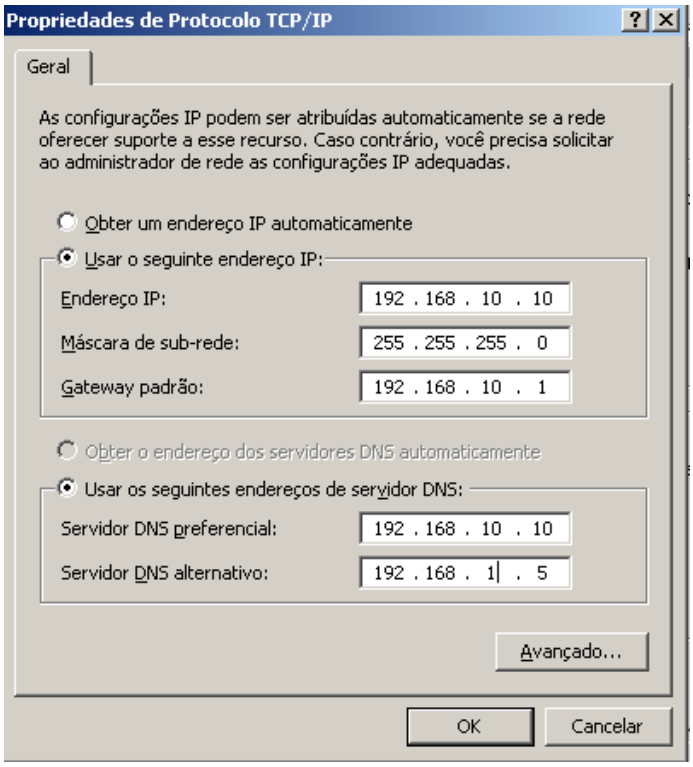

Figura IV. 9 – Configurando Interface de Rede (3)

7) Conexão de rede ativa (para um switch ou outro computador através de cabo crossover)

A instalação do AD requer uma conexão de rede ativa (cabo de rede conectado a um hub, switch, roteador, etc). Caso contrário, você pode receber o seguinte aviso de erro:

```
Active Directory Installation Failed
The operation failed with the following error
The network location cannot be reached. For further information about network troubleshooting,
see Windows Help.
```

Verifique o status da interface de rede não está como “desconectado”, semelhante a Figura IV.10:

Figura IV. 10 – Configurando Interface de Rede (4)

8) Um servidor DNS operacional (que pode ser instalado no controlador de domínio)

Um servidor DNS que suporte as entradas DNS do AD (registros SRV) precisa estar disponível para que as funções do AD operem normalmente. Você deve ter em mente que as seguintes configurações de DNS podem ser problemáticas: entradas Root Zone e DNS Forwarders.

- Root Zone

Requisições externas de DNS para a internet não funcionam se um Root Zone existir no servidor DNS. Para resolver o problema, remova a entrada de Root Zone. Esta entrada é identificada por um ponto (.) no gerenciador DNS na seção Forward Lookup Zones.

- DNS Forwarders (Recomendado)

Se você planeja ter conectividade internet então os DNS Forwarders são necessários para garantir que todas as entradas DNS são corretamente enviadas para o servidor DNS do seu ISP (Internet Service Provider - Provedor de Internet).

Você só pode configurar os DNS Forwarders se nenhum Root Zone estiver presente.

Caso seja o primeiro AD na rede e sua rede for pequena, a recomendação é deixar que o assistente de criação do AD faça a criação e configuração do servidor DNS.

9) Nome de domínio que você quer usar

Como regra geral, a Microsoft recomenda que você registre o domínio DNS (tanto interno quanto externo) nos órgãos controladores da Internet (Registro.br aqui no Brasil). Isso previne a possibilidade de duplicidade de nomes no registro do DNS.

10) Acesso à mídia de instalação (ou ao diretório i386)

Para a instalação do AD, o Windows necessita copiar arquivos do CD de instalação. Uma recomendação é deixar uma cópia do diretório i386 no HD do servidor, conforme a Figura IV.11.

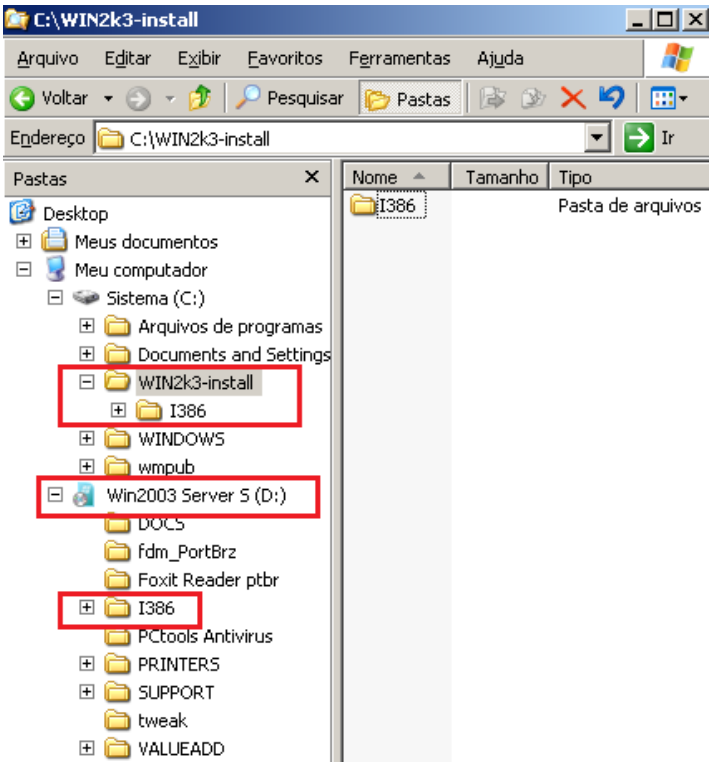

Figura IV. 11 – Arquivos de instalação

11) Não usar ICS (Recomendado)

Utilize sempre que possível o sistema NAT (Network Address Translator). O sistema ICS (Internet Connection Sharing) atrapalhará toda a funcionalidade DHCP e DNS da sua rede.

Depois que o servidor e a rede atenderem a todos os requisitos e recomendações acima, já é possível criar o primeiro DC do seu Active Directory.

Instalação do Active Directory

Importante: Esta instalação é voltada do primeiro DC (Domain Controller) em um novo AD (Active Directory), em uma nova Árvore, em uma nova Floresta.

1. Iniciando a promoção do Domain Controller

Existe duas maneiras de iniciar o "Assistente de Instalação do Active Directory": Assistente de Configuração do Servidor e executando o comando DCPROMO.

a) Assistente de Configuração do Servidor

i. Clique em “Iniciar”, “Ferramentas Administrativas” e “Gerenciar o Servidor”, conforme a Figura IV.12:

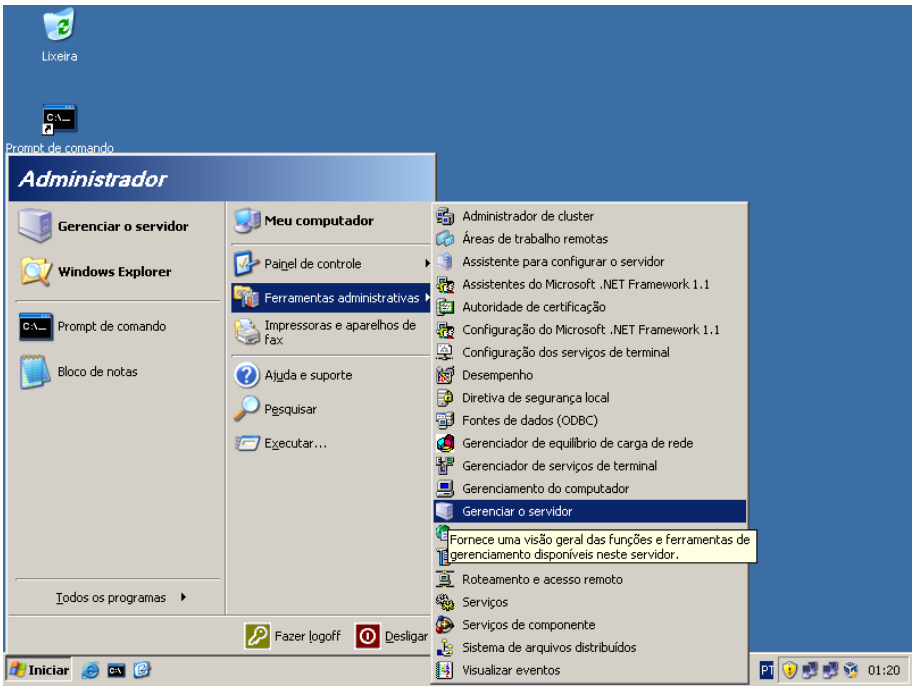

Figura IV. 12 – Gerenciando servidor

ii. Abrirá uma janela aonde contém todas as ferramentas administrativas do servidor. Para adicionar uma nova função clique no Link “Adicionar ou remover uma função”, conforme a Figura IV.13:

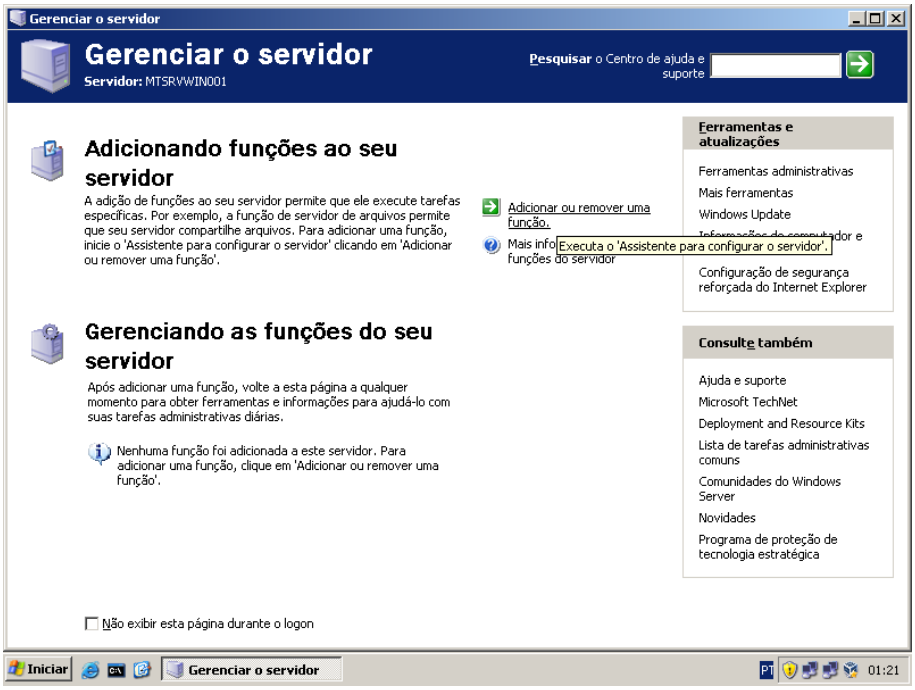

Figura IV. 13 – Gerenciar Servidor (1)

iii. Irá abrir o “Assistente para configurar o Servidor”, leia com atenção e clique em “Avançar”, conforme a Figura IV.14

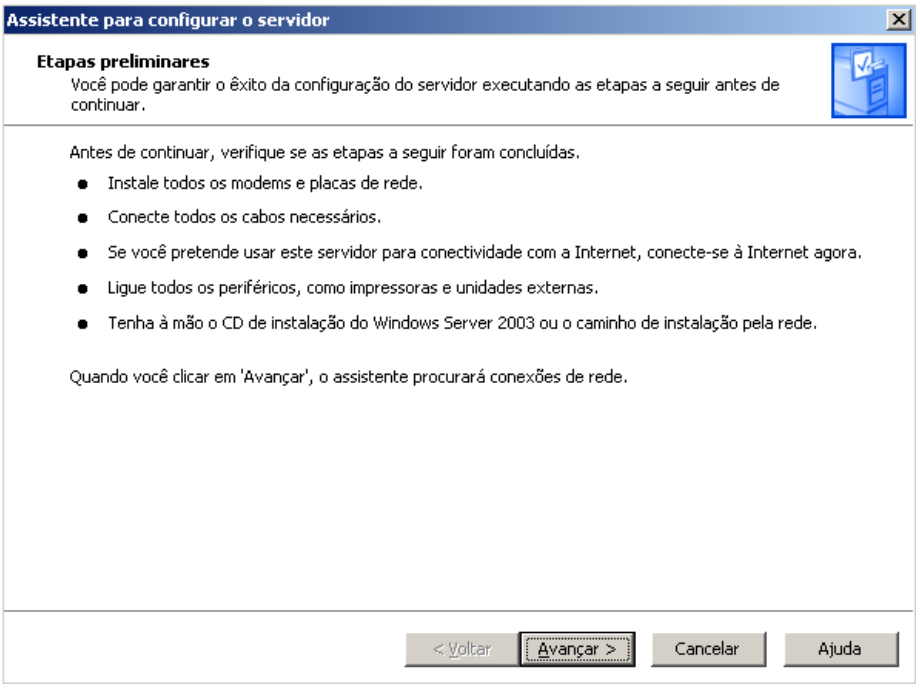

Figura IV. 14 – Gerenciar Servidor (2)

iv. Aguarde enquanto as configurações de rede estão sendo detectadas, conforme a , conforme a Figura IV.15

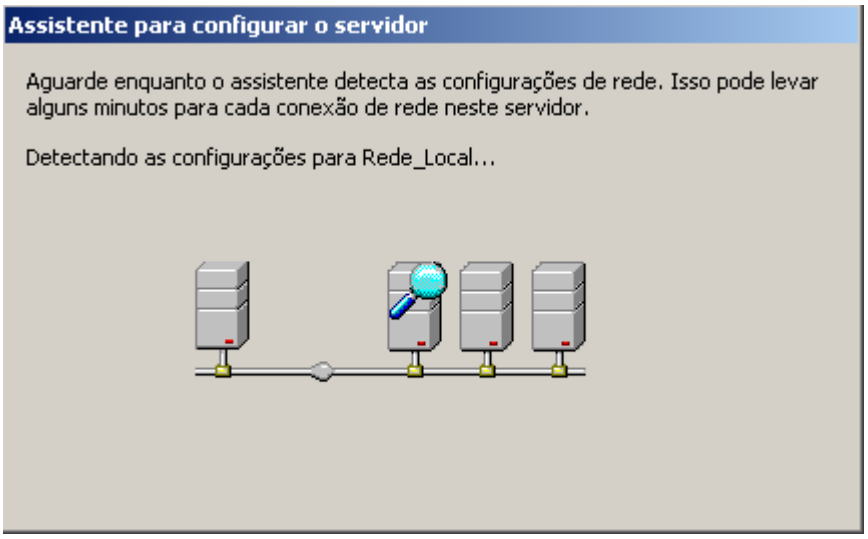

Figura IV. 15 – Gerenciar Servidor (3)

v. Na Janela de opções de configuração do Assistente para configurar o servidor, escolha “Configuração Personalizada” para instalação apenas do Active Directory, , conforme a Figura IV.16:

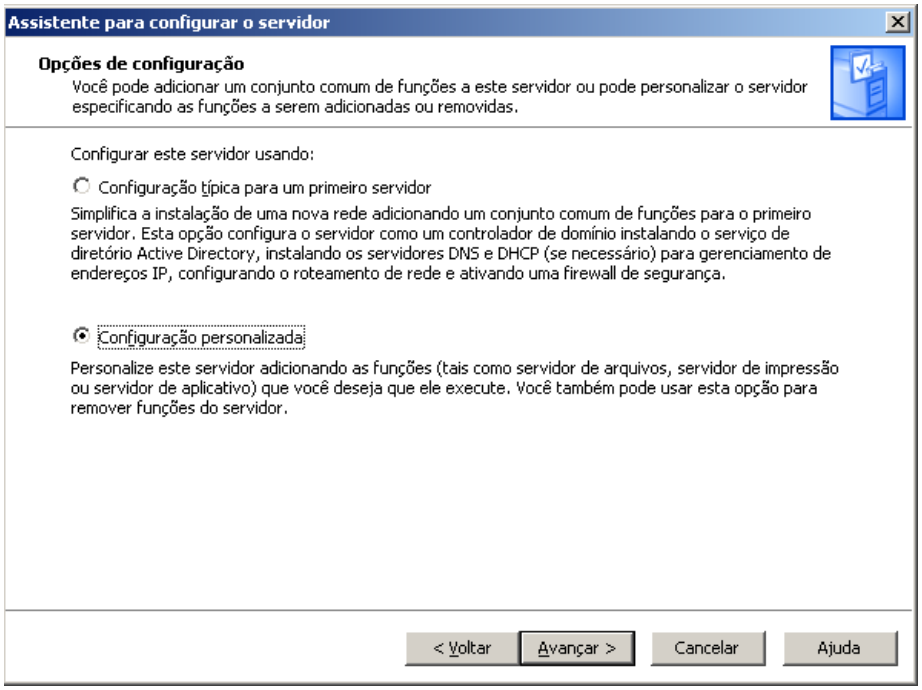

Figura IV. 16 – Gerenciar Servidor (4)

vi. O Assistente irá listar as funções disponíveis/instaladas neste servidor. Para instalação do AD, escolha a opção "Controlador de Domínio (Active Directory)" e clique em avançar, conforme a Figura IV.17.

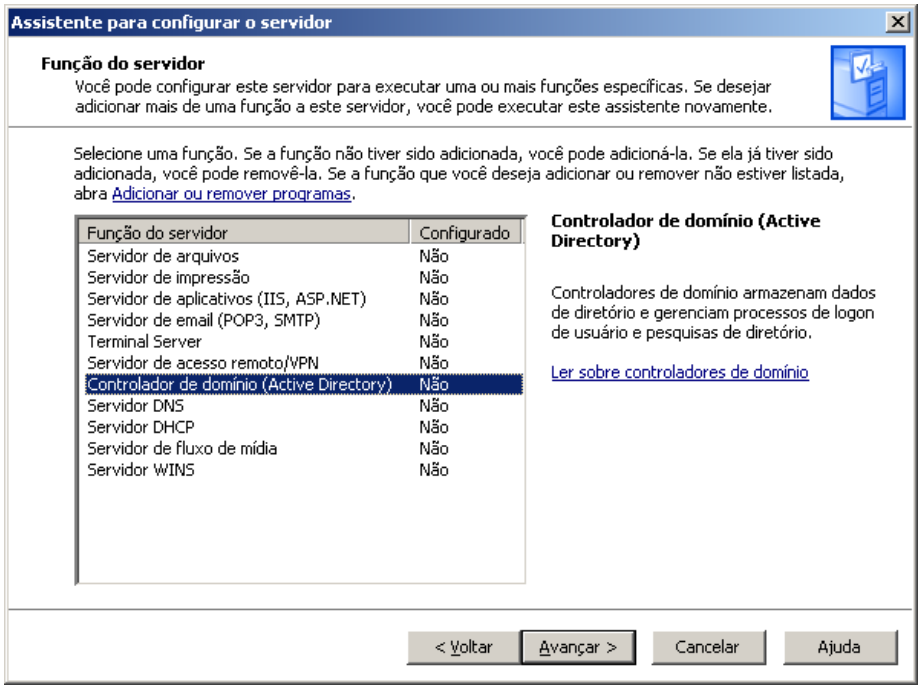

Figura IV. 17 – Gerenciar Servidor (5)

vii. O Assistente exibirá um resumo das instalações selecionadas e tarefas a serem executadas, leia atentamente e clique em “Avançar”, conforme a Figura IV.18:

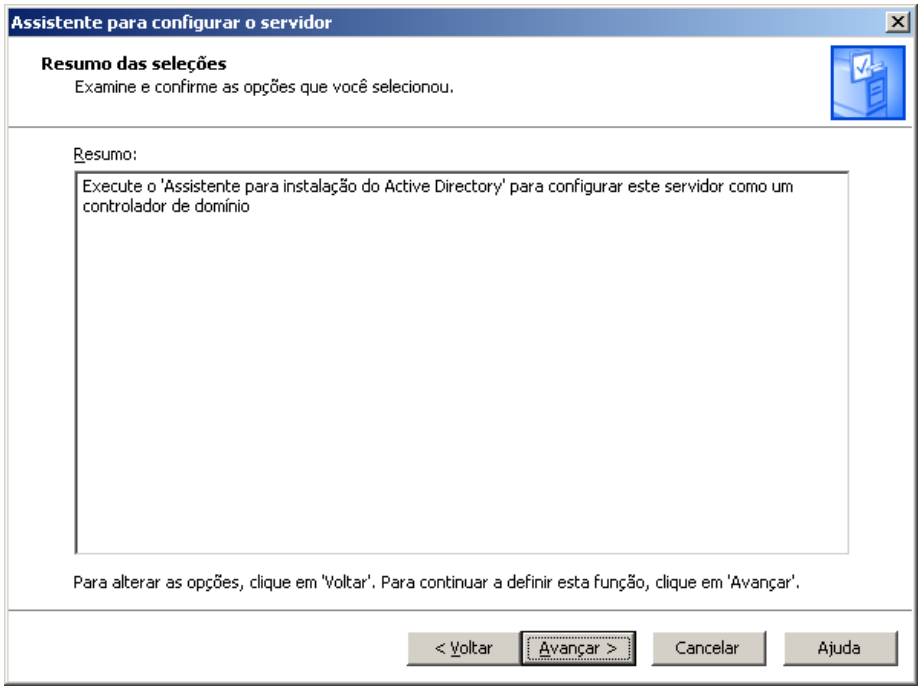

Figura IV. 18 – Gerenciar Servidor (6)

viii. O Assistente de instalação do Active Directory será iniciado, prosseguindo na Etapa 02.

b) Executando o DCPROMO

i. Para iniciar a instalação pelo DCPROMO, basta ir em “Iniciar”, “Executar” para abrir a janela de execução de comandos, conforme a Figura IV.19:

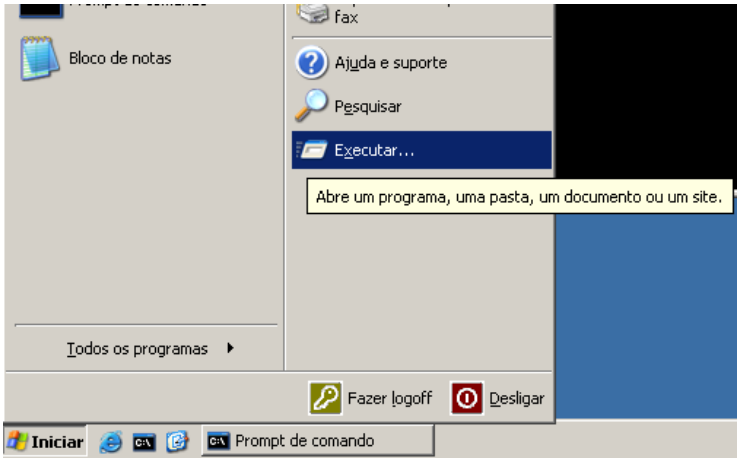

Figura IV. 19 – Executar comandos

ii. No Box de comandos do Windows, digite o comando DCPROMO e clique em ok, conforme a Figura IV.20

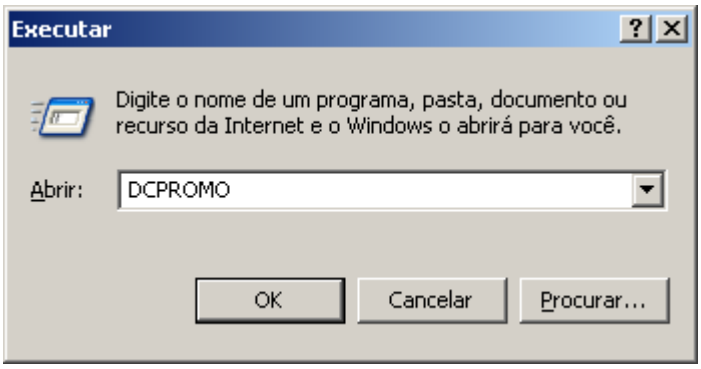

Figura IV. 20 – Executando DCPROMO

Observação importante: O Comando DCPROMO permite criar arquivos de "resposta", ou seja, permite a instalação pré-configurada através da leitura de um arquivo com as definições de instalação. Para mais informações sobre os parâmetros leia [MIC02]:

Os parâmetros aceitos pelo DCPROMO são exibidos na Figura IV.21:

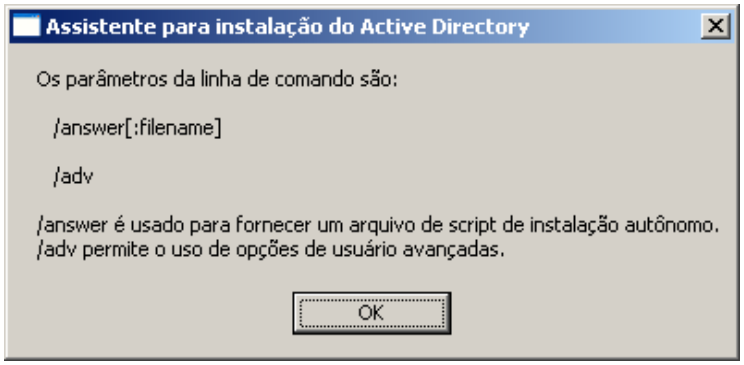

Figura IV. 21 – Opções de argumentos do DCPROMO

iii. O "Assistente de Instalação do Active Directory" será iniciado, prosseguindo na Etapa 02;

2. O Assistente para Instalação do Active Directory irá abrir, leia atentamente e clique em Avançar, conforme Figura IV.22:

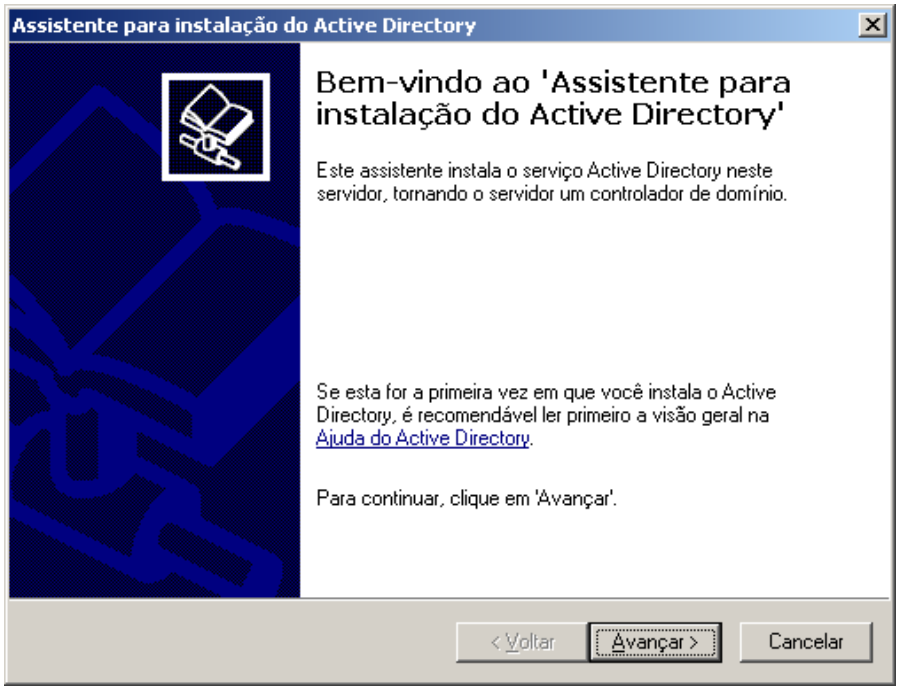

Figura IV. 22 – Assistente para instalação do Active Directory (1)

3. Na janela de "Compatibilidade de sistema operacional" leia os requisitos mínimos dos clientes do AD. A seguir, clique no botão "Avançar", conforme Figura IV.23:

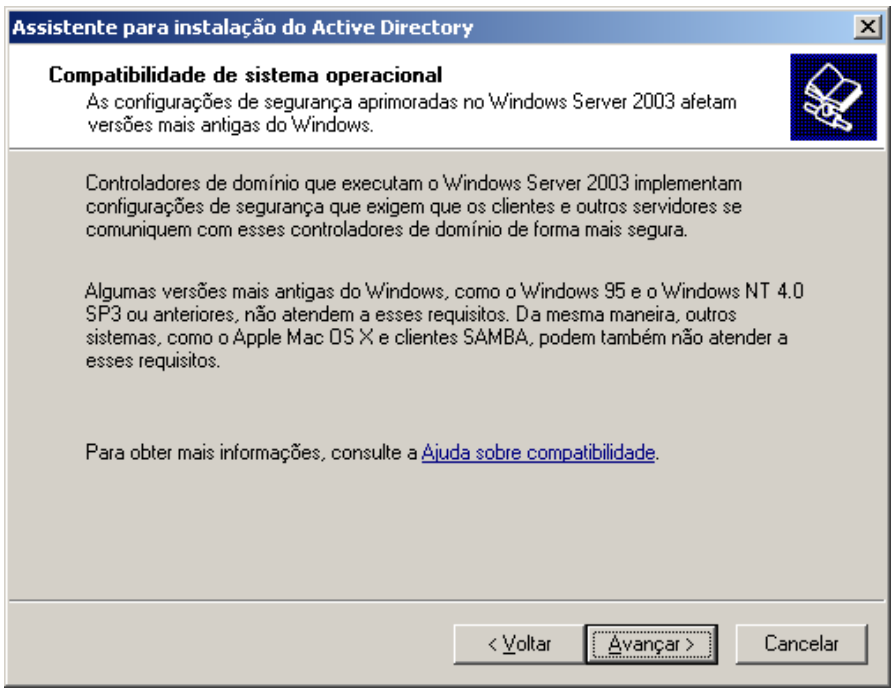

Figura IV. 23 – Assistente para instalação do Active Directory (2)

4. Na janela de "Tipo de controlador de domínio", selecione a opção "Controlador de domínio para um novo domínio" e clique no botão "Avançar", conforme Figura IV.24:

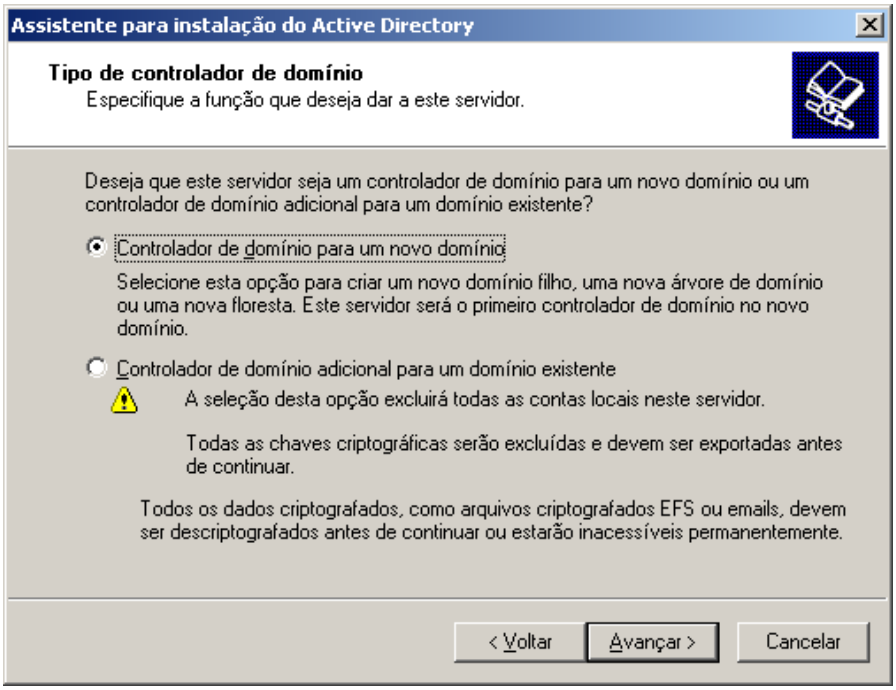

Figura IV. 24 – Assistente para instalação do Active Directory (3)

5. Na janela de "Criar novo domínio", selecione a opção "Domínio em uma nova floresta" e clique no botão "Avançar", conforme Figura IV.25:

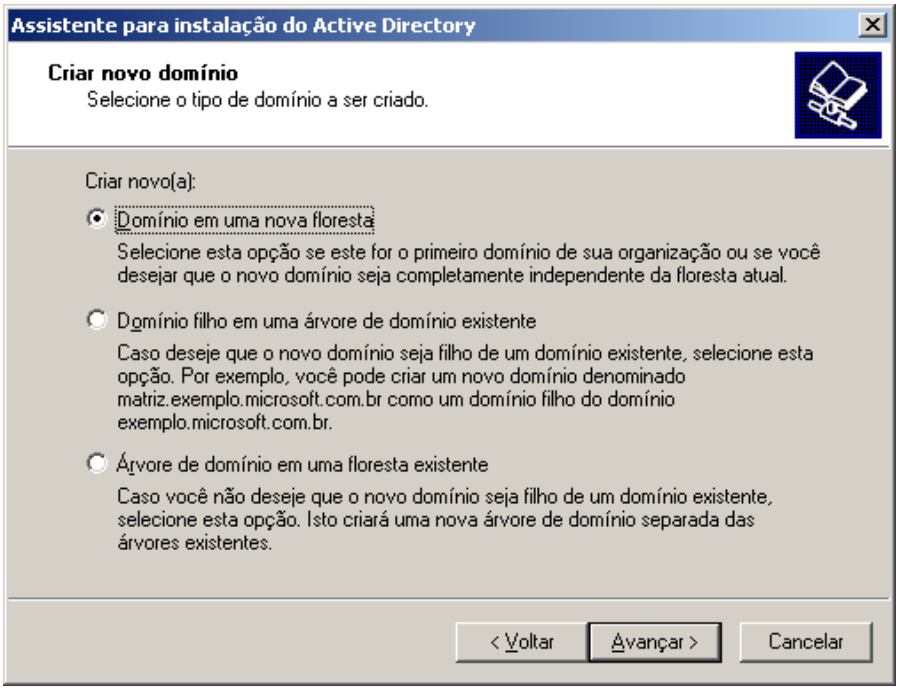

Figura IV. 25 – Assistente para instalação do Active Directory (4)

6. A janela de "Novo nome de domínio" é a opção mais importante na criação do AD. Como todo o sistema do AD é baseado no DNS, a criação do nome de domínio irá afetar toda a operação da rede. Entre com o nome DNS completo do domínio, neste caso: domad.mtulio.eng.br. Clique em “Avançar”, conforme Figura IV.26:

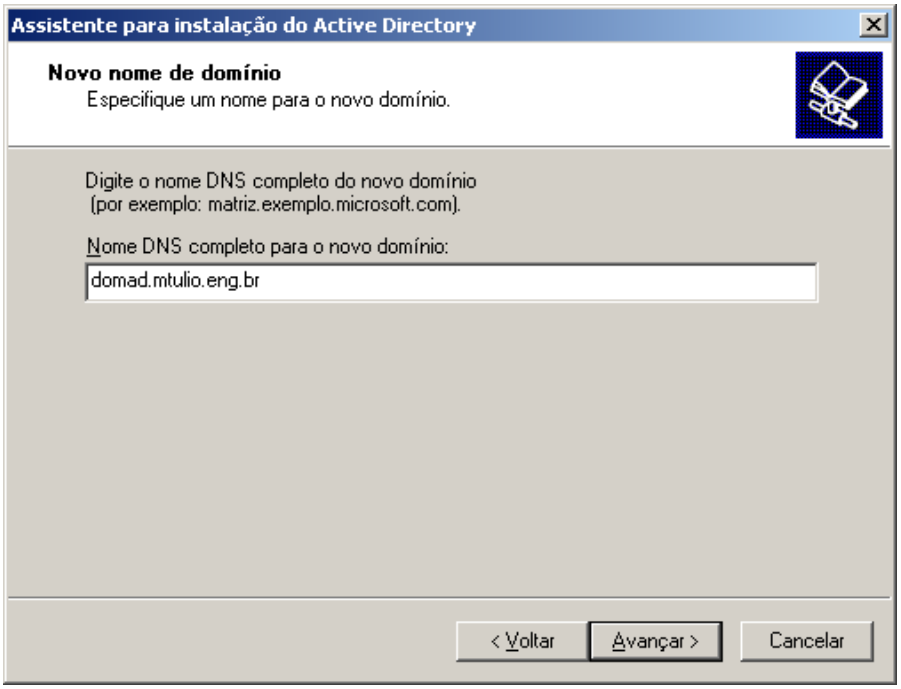

Figura IV. 26 – Assistente para instalação do Active Directory (5)

Obs.: Este parte poderá demorar alguns minutos, pois o sistema irá procurar pelo servidor DNS e verificar se o nome já existe.

7. Na janela de "Nome do domínio NetBIOS", aceite a opção padrão (que é o primeiro nome do domínio DNS) e clique no botão "Avançar, conforme Figura IV.27::

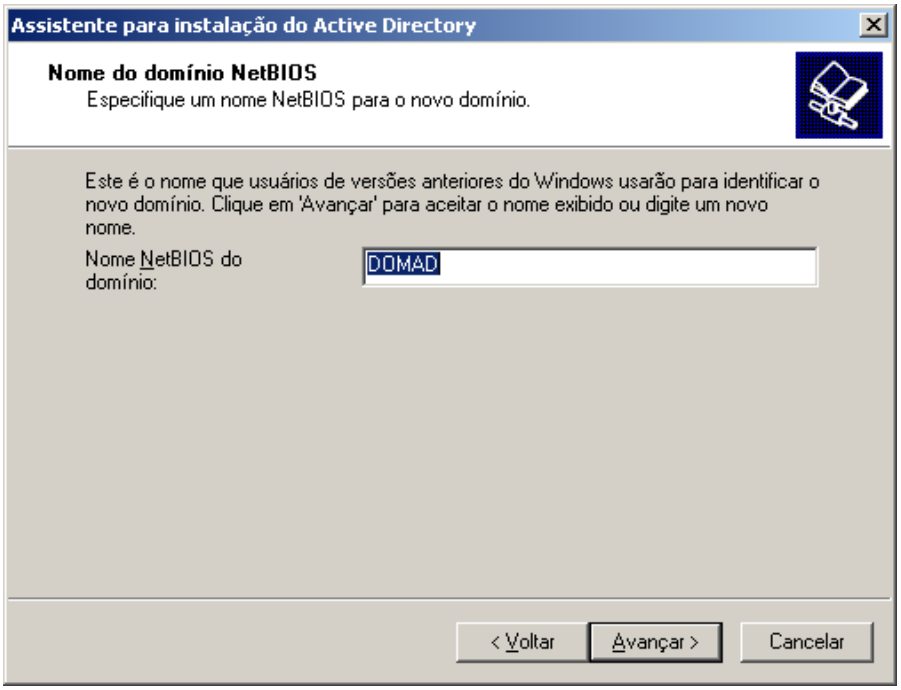

Figura IV. 27 – Assistente para instalação do Active Directory (6)

8. Na janela de "Pastas do banco de dados e log", lembre-se que a partição deverá ser NTFS e você somente deverá alterar os caminhos padrões por motivos de desempenho. O caminho "\Windows\NTDS" é o local onde serão armazenados os dados do AD. Aceite as opções padrões e clique no botão "Avançar", conforme Figura IV.28::

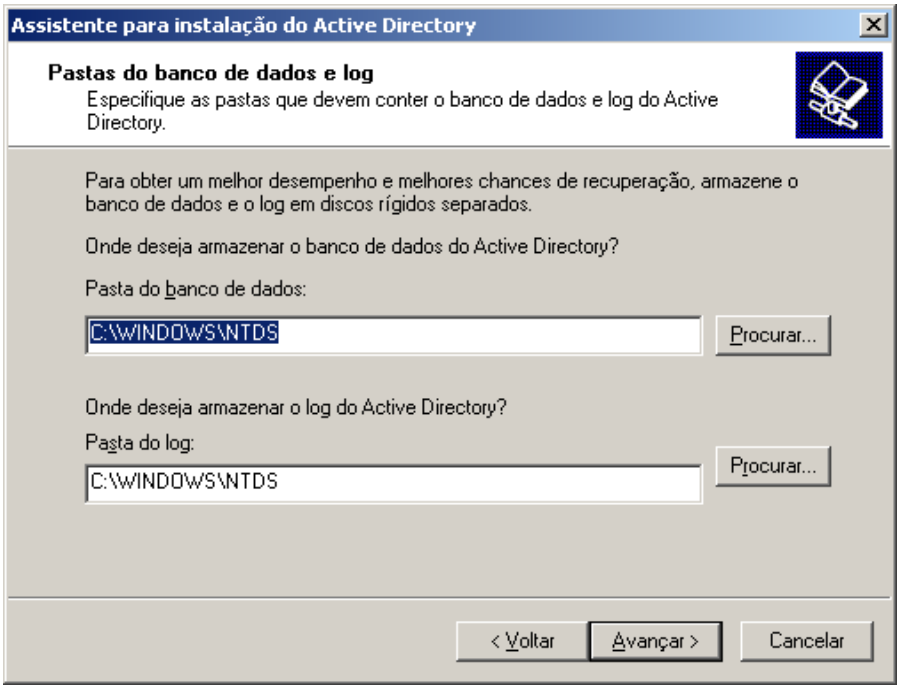

Figura IV. 28 – Assistente para instalação do Active Directory (7)

9. Na janela de "Volume de sistema compartilhado", a partição também deverá ser NTFS e somente deverá ser alterado caso haja problemas de desempenho. O caminho "C:\Windows\SYSVOL" é o local onde serão armazenados as GPOs e scripts do AD e esta pasta é replicada para todos os outros DC. Aceite a opção padrão e clique no botão "Avançar", conforme Figura IV.29::

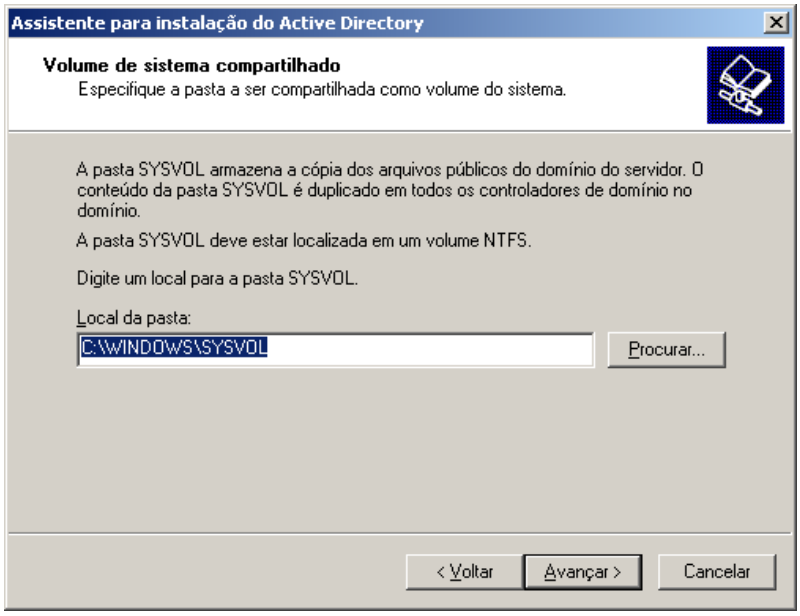

Figura IV. 29 – Assistente para instalação do Active Directory (8)

10. Servidor DNS

- Se o servidor DNS não estiver ativo ou configurado corretamente, será exibido o aviso de falha, conforme Figura IV.30:

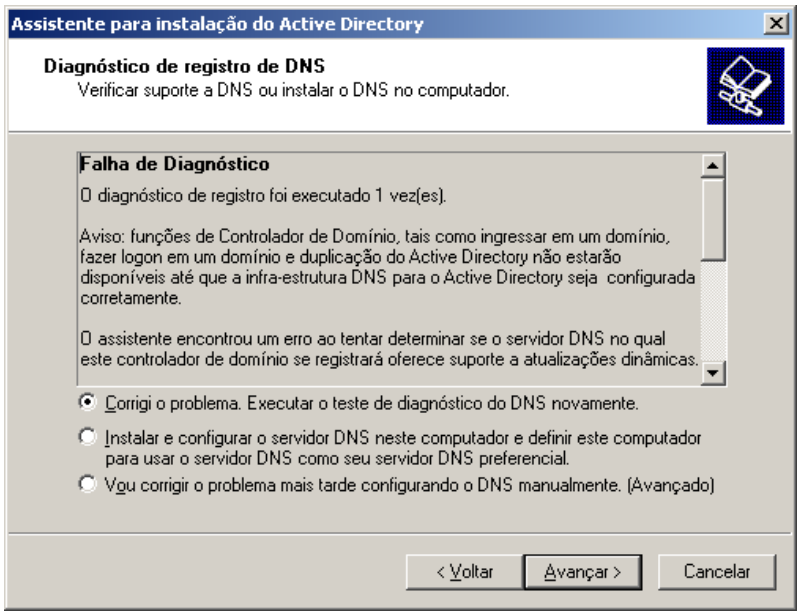

Figura IV. 30 – Assistente para instalação do Active Directory (9)

- Em geral, o primeiro DC do AD também é o servidor DNS. Lembre-se que o servidor DNS requerido pelo AD deve aceitar registro SRVs e atualizações dinâmicas. Portanto, o mais recomendável é utilizar o servidor DNS do Windows Server 2003 e deixar que o assistente faça a instalação e configuração do mesmo.
- Selecione a opção "Instalar e configurar o servidor DNS neste computador e definir este computador para usar o servidor DNS como seu servidor DNS preferencial" e clique no botão "Avançar", conforme Figura IV.31:

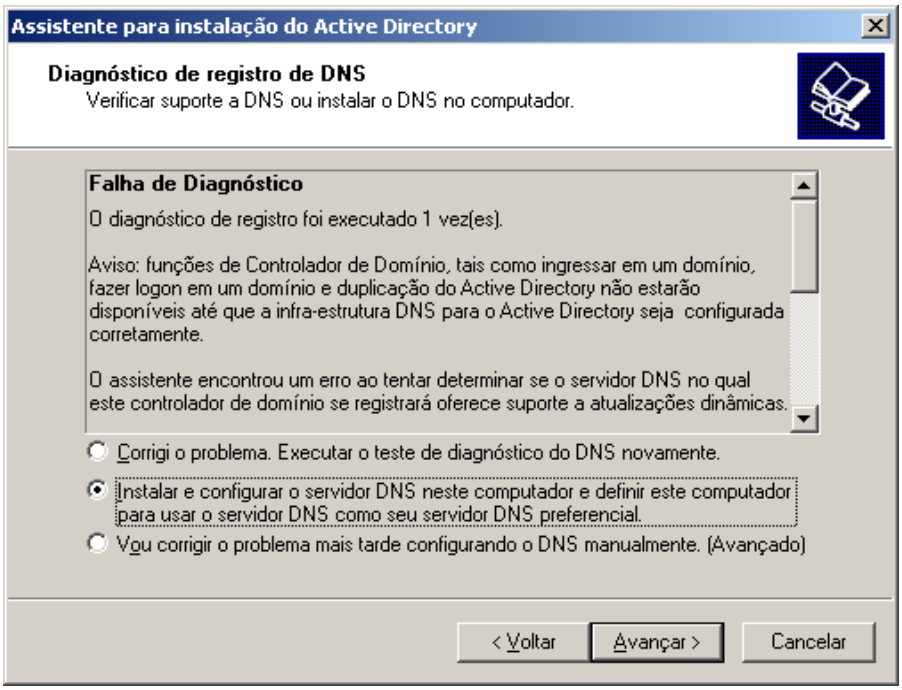

Figura IV. 31 – Assistente para instalação do Active Directory (10)

11. Na janela de "Permissões", selecione a opção "Permissões compatíveis somente com os sistemas operacionais de servidor Windows 2000 ou Windows Server 2003" e clique no botão "Avançar". , conforme Figura IV.32:
    - Esta opção somente deverá ser alterada caso você tenha DCs rodando em plataforma WindowsNT, o que não é o caso.

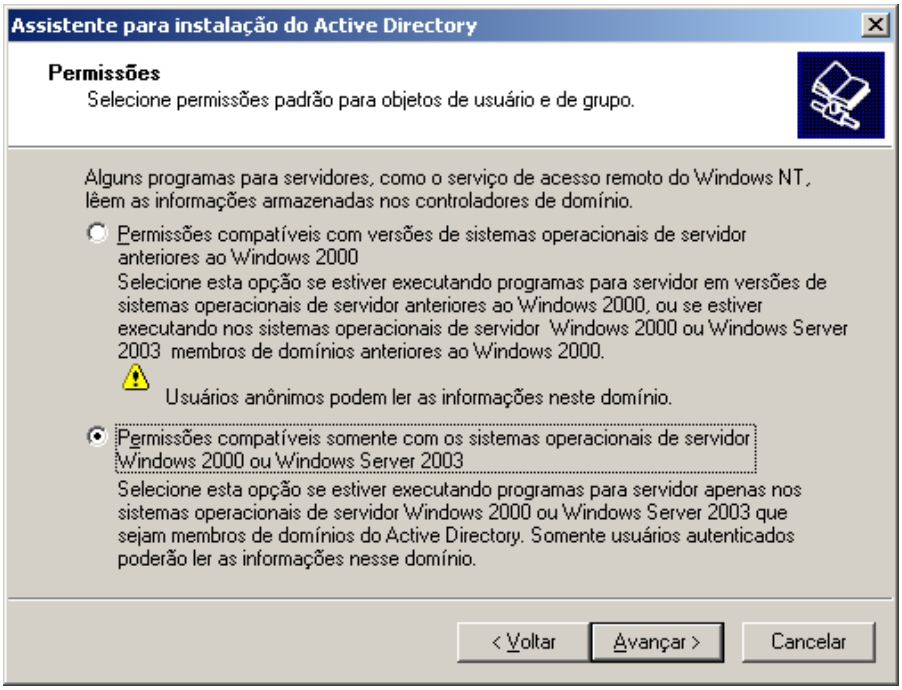

Figura IV. 32 – Assistente para instalação do Active Directory (11)

12. Na janela de senha, digite e confirme a senha de administrador do modo de restauração; clique no botão "Avançar", conforme Figura IV.33:
    - Esta senha é importante, pois ela não é a mesma senha do administrador do DC e deve ser usada quando houver problemas no DC ou quando o DC for removido do computador.

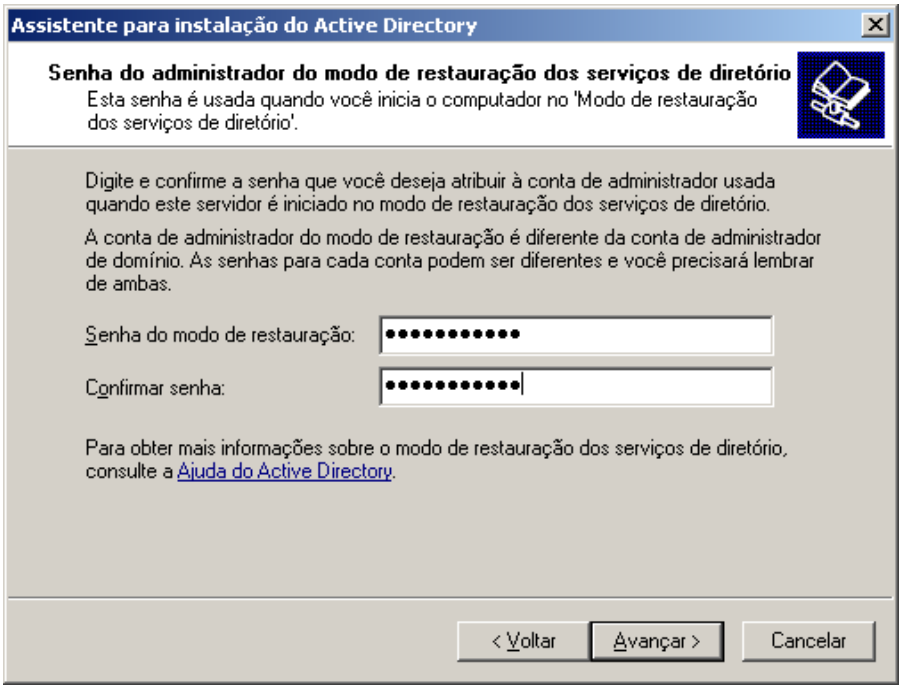

Figura IV. 33 – Assistente para instalação do Active Directory (12)

13. Na janela de "Resumo", verifique as opções selecionadas. Caso as opções estejam corretas, clique no botão "Avançar", conforme Figura IV.34::

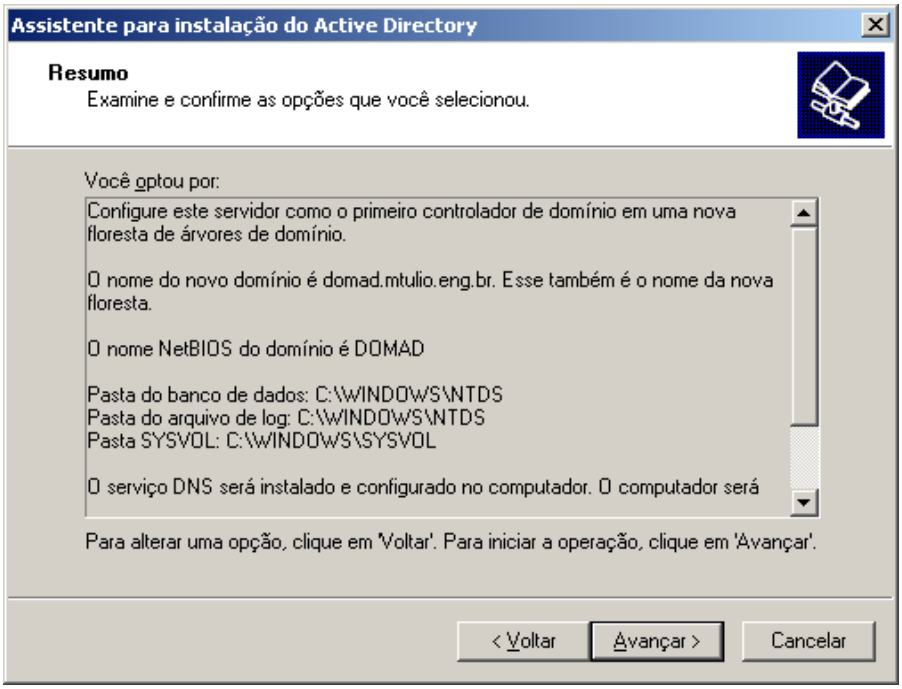

Figura IV. 34 – Assistente para instalação do Active Directory (13)

14. O Assistente executará as tarefas solicitadas exibindo-as na tela.
    - Nunca clique no botão "Cancelar", pois você irá estragar todo o computador!
    - Caso tenha cometido algum erro, aguarde o assistente finalizar e depois execute-o novamente para desfazer as alterações.

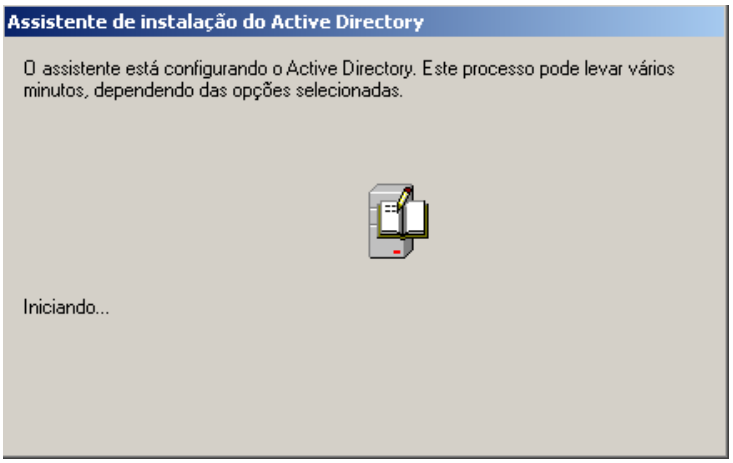

Figura IV. 35 – Assistente para instalação do Active Directory (14)

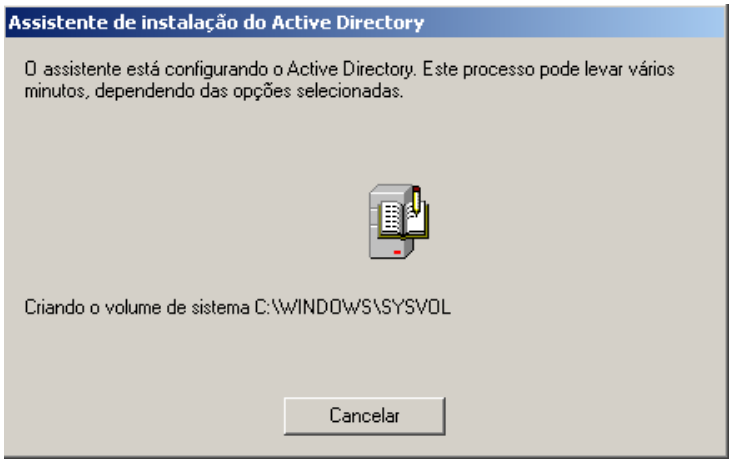

Figura IV. 36 – Assistente para instalação do Active Directory (15)

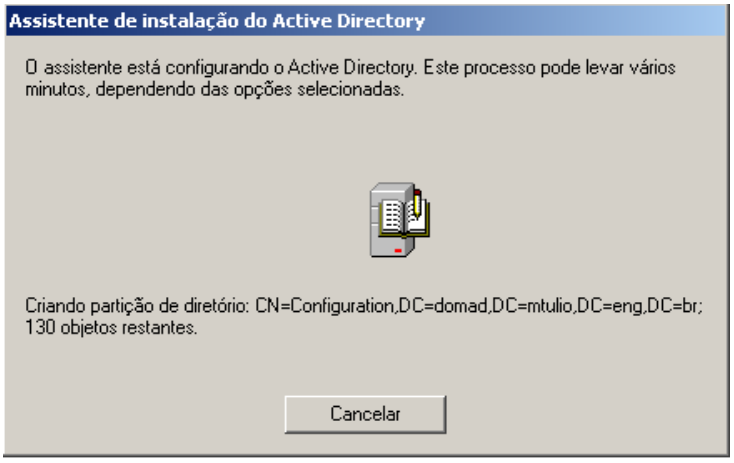

Figura IV. 37 – Assistente para instalação do Active Directory (16)

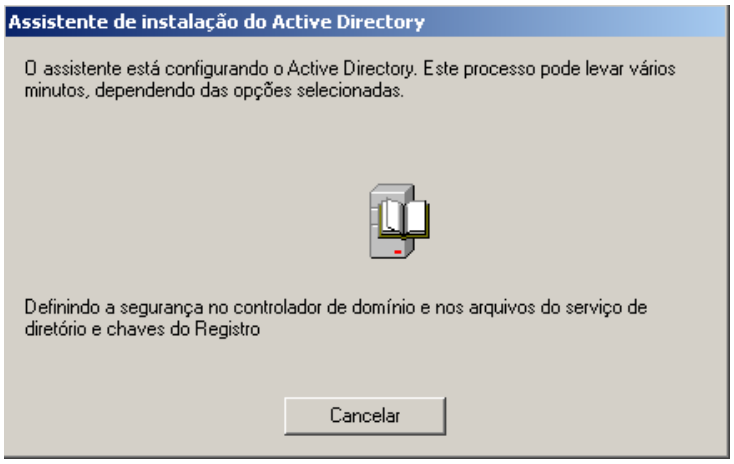

Figura IV. 38 – Assistente para instalação do Active Directory (17)

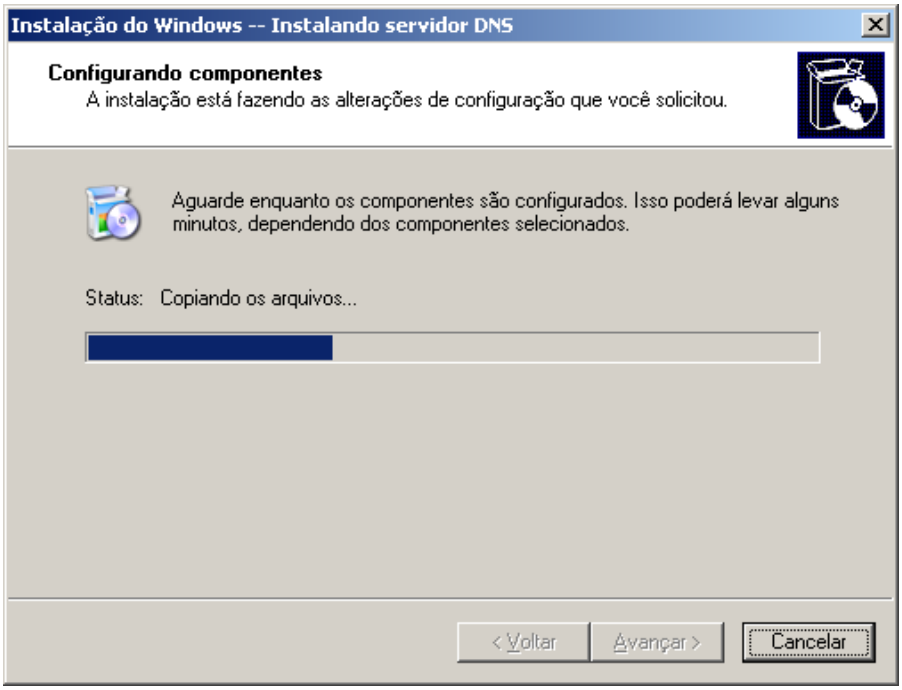

Figura IV. 39 – Instalando servidor DNS

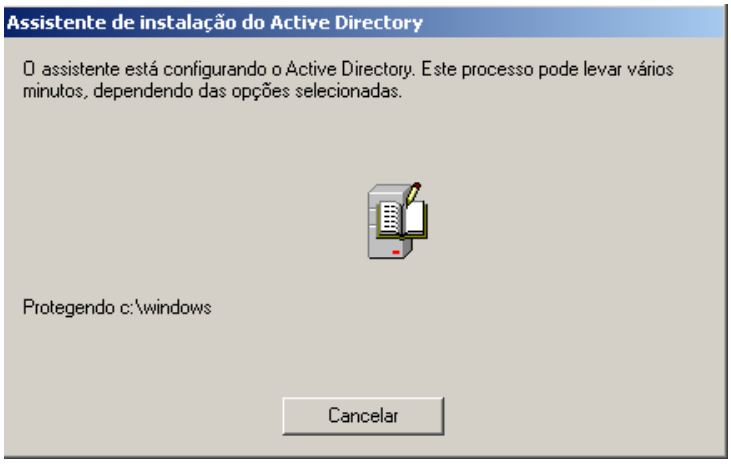

Figura IV. 40 – Assistente para instalação do Active Directory (18)

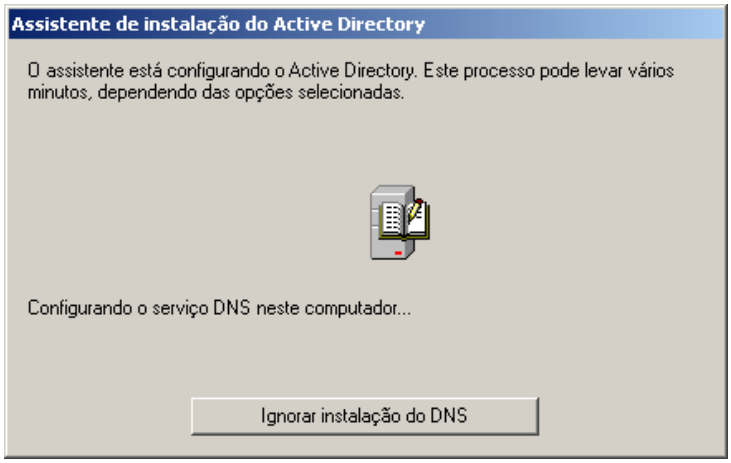

Figura IV. 41 – Assistente para instalação do Active Directory (19)

15. Caso as tarefas tenham sido realizadas com sucesso, um resumo da instalação será exibido informando que o Active Directory foi instalado com sucesso. Conforme Figura IV.42:

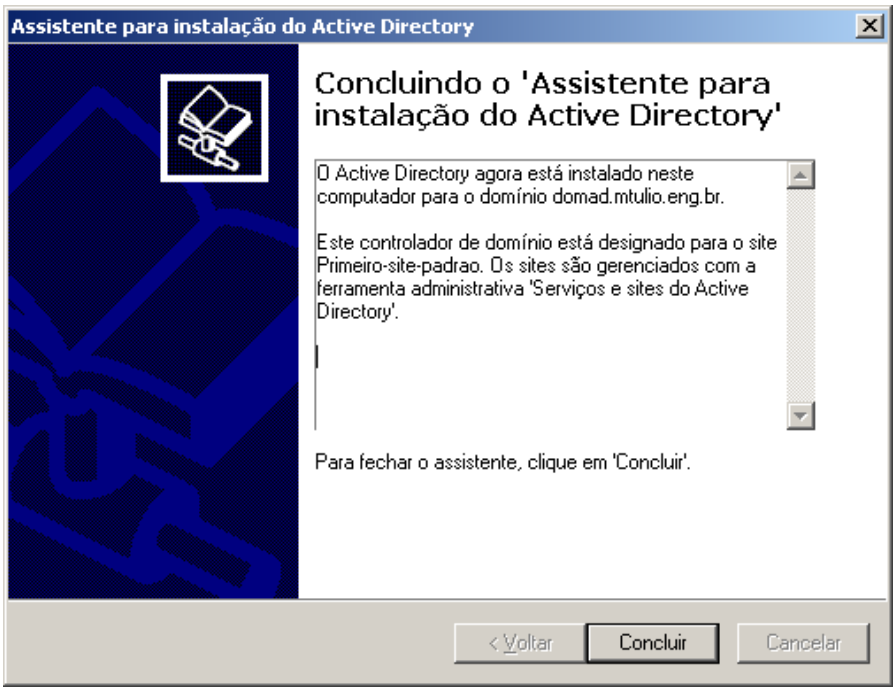

Figura IV. 42 – Assistente para instalação do Active Directory (20)

16. Clique no botão "Concluir".
17. Você precisará reiniciar o computador para que o sistema inicialize com o serviço do Active Directory. Clique no botão "Reiniciar agora". Conforme Figura IV.43.

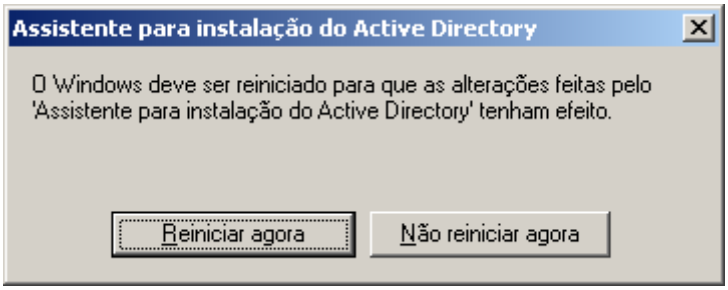

Figura IV. 43 – Assistente para instalação do Active Directory (21)

18. Após a reinicialização note que uma nova janela de logon aparecerá com a opção “Fazer logon em:”. Informe o Usuário, senha clique em “ok”. conforme Figura IV.44.

    Obs.: No Primeiro logon, deve ser informado o usuário e senha do usuário Administrador da Maquina, por questões de segurança, este usuário deve ser bloqueado após a conclusão da instalação.

Figura IV. 44 – Efetuando Logon no Sistema

Mais informações:

- Microsoft Technet – Windows Server TechCenter, Requisitos e Recomendações para a instalação do Active Directory . [MIC01] ;
- Requisitos de instalação do AD DS . [MIC05]

ANEXO V – Script para criação da Organização no Active Directory – DOMAD_criarEstrutura.vbs.

```
'
'  Name: DOMAD_criarEstrutura.vbs
'  Copyright: DOMAD MTulio ENG
'  Author: Marco Túlio Rodrigues Braga
'  E-mail: admin@mtulio.eti.br
'  Date: 29/10/2011 02:40
'  Last Change: 30/11/2011
'  Description: Este script foi criado para criação
'da estrutura organizacional implementada no trabalho
'de Conclusão de Curso. Este script pode ser utilizado
'e distribuido de acordo com a necessidade.
'Sugestões e contribuições podem ser enviadas por e-mail.
'

' -> Impede que você use uma variável sem criá-la
Option Explicit

' -> Declarando variaveis

' Atributos do Objeto
Dim strDescription, userName, userNamePrefix, sAMAccountName

' Variaveis Auxiliares
Dim i, iItem, iTemSubOU
Dim strOU, strPath, strOUBase, strUnitSigla, strNameComp, strSn,
strCompany, strPrincipalName, userNamePart, strComputerNamePart
Dim strComputerName, strOS, strSP
Dim strCn, strCnPart, strName, struNCName, struNCNamePart,
strDescriptionPart

' Variaveis DN
Dim DNPai, DNPai2, DNUser, DNAtual, DNFilho, DNComp

' Variaveis de Objeto
Dim objDOMAD, objOU,  objOUPai, strOUOrg, objUser

' Quantidade de objetos a serem criados - INFORME
```

```
Dim countAllUsers, countAllComputers, countAllGroups, countAllObjects
countAllUsers = 99
countAllComputers = 60
countAllGroups = 80
countAllObjects = 30

' Valores para Testes
'countAllUsers = 9
'countAllComputers = 6
'countAllGroups = 8
'countAllObjects = 3

' Manipulacao de Arquivos
' Log File
Dim myFSO, objFileWrite, myLog
Dim DATE_AAAAMMDDHHmmss, DATE_DDMMAAAAHHmmss, HOUR_DD, HOUR_MM, HOUR_AAAA,
HOUR_HH, HOUR_min, HOUR_ss

' Essa funcao deve ser chamada sempre que seja
' necessario coletar a hora atual
Sub hourNow(HOUR_DD, HOUR_MM, HOUR_AAAA, HOUR_HH, HOUR_min, HOUR_ss)
 HOUR_DD = DatePart("d",Now())
 HOUR_MM = DatePart("m",Now())
 HOUR_AAAA = DatePart("yyyy",Now())
 HOUR_HH = DatePart("h",Now())
 HOUR_min = DatePart("n",Now())
 HOUR_ss = DatePart("s",Now())
End Sub

Sub getDateStr(dateStr)
 hourNow HOUR_DD, HOUR_MM, HOUR_AAAA, HOUR_HH, HOUR_min, HOUR_ss
 dateStr = HOUR_DD & "/" & HOUR_MM & "/" & HOUR_AAAA & "_" & HOUR_HH & ":"
& HOUR_min & ":" & HOUR_ss
End Sub

Sub getDateFilenameStr(dateStr)
 hourNow HOUR_DD, HOUR_MM, HOUR_AAAA, HOUR_HH, HOUR_min, HOUR_ss
 DATE_AAAAMMDDHHmmss = HOUR_AAAA & "-" & HOUR_MM & "-" & HOUR_DD & "_" &
HOUR_HH & "-" & HOUR_min & "-" & HOUR_ss
End Sub
```

```
' Arquivo p/ gravar o tempo de execucao
getDateFilenameStr DATE_AAAAMMDDHHmmss
myLog = "time_" & DATE_AAAAMMDDHHmmss & ".log"

' Criando arquivo
Set myFSO = CreateObject("Scripting.FileSystemObject")
Set objFileWrite = myFSO.OpenTextFile(myLog, 8, True)

' ####################################
' -> Iniciando o Programa

WScript.Echo "Certifique-se que as OU configuradas neste script não
existam, caso contrario este script falhará!"

objFileWrite.WriteLine("####################################")
objFileWrite.WriteLine("  DOMAD")

' Definindo a hora atual e gravando no arquivo:
getDateStr DATE_DDMMAAAAHHmmss
objFileWrite.WriteLine("Start Add to dir: " & DATE_DDMMAAAAHHmmss)
objFileWrite.WriteLine("Adicionando Estrutura no AD!")

' String de pesquisa.
' Bind to object.
strPath = "LDAP://dc=domad,dc=mtulio,dc=eng,dc=br"
Set objOUPai = GetObject(strPath)

' === OU=DOMAD
' Criando a OU Base

DNPai = "dc=DOMAD,dc=mtulio,dc=eng,dc=br"
Set objOUPai = GetObject("LDAP://" & DNPai)

strOU = "ou=DOMAD"
strDescription = "MTulio ENG - Dominio AD (DOMAD)"

' Criando a estrutura da Unidade
Set objOU = objOUPai.Create("organizationalUnit", strOU)
objOU.Put "description", strDescription
```

```
objOU.SetInfo

' Saida: Sucesso ou Erro.
If Err.Number <> vbEmpty Then
 WScript.Echo "Erro:   Falha na criação.\n" & Err.Number
End If

' === OU=UNIDADES,OU=DOMAD
' Quatro Unidades Organizacionais para 5 Filiais
' Matriz 2 X 5
Dim vetorOU(1,4)

vetorOU(0,0) = Array("ou=GYN", "Unidade Goiania-GO")
vetorOU(1,0) =
Array("ou=USUARIOS","ou=GRUPOS","ou=COMPUTADORES","ou=OBJETOS","ou=Departam
entos" )

vetorOU(0,1) = Array("ou=ANA", "Unidade Anapolis-GO")
vetorOU(1,1) =
Array("ou=USUARIOS","ou=GRUPOS","ou=COMPUTADORES","ou=OBJETOS" )

vetorOU(0,2) = Array("ou=URU", "Unidade Uruacu-GO")
vetorOU(1,2) =
Array("ou=USUARIOS","ou=GRUPOS","ou=COMPUTADORES","ou=OBJETOS" )

vetorOU(0,3) = Array("ou=FOR", "Unidade Fortaleza-CE")
vetorOU(1,3) =
Array("ou=USUARIOS","ou=GRUPOS","ou=COMPUTADORES","ou=OBJETOS" )

vetorOU(0,4) = Array("ou=SPO", "Unidade Sao Paulo-SP")
vetorOU(1,4) =
Array("ou=USUARIOS","ou=GRUPOS","ou=COMPUTADORES","ou=OBJETOS" )

' ===  Criando as unidades: ou=Unidade,ou=DOMAD
strPath = "LDAP://ou=DOMAD,dc=DOMAD,dc=mtulio,dc=eng,dc=br"

 For iItem=0 To UBound(vetorOU,2)
  DNPai = "ou=DOMAD,dc=DOMAD,dc=mtulio,dc=eng,dc=br"
  DNAtual = vetorOU(0,iItem)(0)
```

```
Set objOUPai = GetObject("LDAP://" & DNPai)

' Buscando a Unidade Organizacional no Vetor
strOU = DNAtual
strDescription = vetorOU(0,iItem)(1)

strOUOrg = strOU

'WScript.Echo "Criando:  " & strOU & "," & DNPai

' Criando a estrutura da Unidade
Set objOU = objOUPai.Create("organizationalUnit", strOU)
objOU.Put "description", strDescription
objOU.SetInfo

' Saida: Sucesso ou Erro.
If Err.Number <> vbEmpty Then
 WScript.Echo "Erro:   Falha na criação."
End If

DNPai = DNAtual & "," & DNPai
' Criando a estrutura Basica
For iTemSubOU=0 To UBound(vetorOU(1,iItem))
 DNFilho = lcase(vetorOU(1,iItem)(iTemSubOU))
 Set objOUPai = GetObject("LDAP://" & DNPai)
 strOU = lcase(vetorOU(1,iItem)(iTemSubOU))

 ' Criando a estrutura da Unidade
 Set objOU = objOUPai.Create("organizationalUnit", strOU)
 objOU.SetInfo

 ' Saida: Sucesso ou Erro.
 If Err.Number <> vbEmpty Then
  WScript.Echo "Erro:   Falha na criação."
 End If

 strCompany = "MTulio ENG"
 DNPai2 = DNFilho & "," & DNPai

 Set objOUPai = GetObject("LDAP://" & DNPai2)
```

```
' Populando a base com Usuarios
If strOU = "ou=usuarios" Then
 For i = 1 To countAllUsers
  If (i < 10) Then
   strSn = " User 0" & i
   userNamePart = "USER0" & i
  Else
   strSn = " User " & i
   userNamePart = "USER" & i
  End if
  If strOUOrg = "ou=GYN" Then
   strUnitSigla = "GYN"
   strNameComp = strUnitSigla & strSn
   DNUser = "cn=" & strNameComp
   userName = strUnitSigla & userNamePart
   strPrincipalName = userName & "@domad.mtulio.eng.br"
   Set objUser = objOUPai.Create("User", DNUser)
   objUser.sAMAccountName = userName
   objUser.givenName = strUnitSigla
   objUser.sn = strSn
   objUser.SetInfo
   objUser.userPrincipalName= strprincipalname
   objUser.displayName = strNameComp
   objUser.company = strCompany
   objUser.description = strNameComp
   objUser.userAccountControl = 512    ' Ativando a conta
   objUser.pwdLastSet = 0       ' Ativando a conta
   objUser.setPassword("" & "123@qwe" & "")' Definindo senha
   objUser.SetInfo
  End if

  If strOUOrg = "ou=ANA" Then
   strUnitSigla = "ANA"
   strNameComp = strUnitSigla & strSn
   DNUser = "cn=" & strNameComp
   userName = strUnitSigla & userNamePart
   strPrincipalName = userName & "@domad.mtulio.eng.br"
   Set objUser = objOUPai.Create("User", DNUser)
   objUser.sAMAccountName = userName
```

```
 objUser.givenName = strUnitSigla
 objUser.sn = strSn
 objUser.SetInfo
 objUser.userPrincipalName= strprincipalname
 objUser.displayName = strNameComp
 objUser.company = strCompany
 objUser.description = strNameComp
 objUser.userAccountControl = 512
 objUser.pwdLastSet = 0
 objUser.setPassword("" & "123@qwe" & "")
 objUser.SetInfo
End if

If strOUOrg = "ou=URU" Then
 strUnitSigla = "URU"
 strNameComp = strUnitSigla & strSn
 DNUser = "cn=" & strNameComp
 userName = strUnitSigla & userNamePart
 strPrincipalName = userName & "@domad.mtulio.eng.br"
 Set objUser = objOUPai.Create("User", DNUser)
 objUser.sAMAccountName = userName
 objUser.givenName = strUnitSigla
 objUser.sn = strSn
 objUser.SetInfo
 objUser.userPrincipalName= strprincipalname
 objUser.displayName = strNameComp
 objUser.company = strCompany
 objUser.description = strNameComp
 objUser.userAccountControl = 512
 objUser.pwdLastSet = 0
 objUser.setPassword("" & "123@qwe" & "")
 objUser.SetInfo
End if

If strOUOrg = "ou=FOR" Then
 strUnitSigla = "FOR"
 strNameComp = strUnitSigla & strSn
 DNUser = "cn=" & strNameComp
 userName = strUnitSigla & userNamePart
 strPrincipalName = userName & "@domad.mtulio.eng.br"
```

```
    Set objUser = objOUPai.Create("User", DNUser)
    objUser.sAMAccountName = userName
    objUser.givenName = strUnitSigla
    objUser.sn = strSn
    objUser.SetInfo
    objUser.userPrincipalName= strprincipalname
    objUser.displayName = strNameComp
    objUser.company = strCompany
    objUser.description = strNameComp
    objUser.userAccountControl = 512
    objUser.pwdLastSet = 0
    objUser.setPassword("" & "123@qwe" & "")
    objUser.SetInfo
   End if

   If strOUOrg = "ou=SPO" Then
    strUnitSigla = "SPO"
    strNameComp = strUnitSigla & strSn
    DNUser = "cn=" & strNameComp
    userName = strUnitSigla & userNamePart
    strPrincipalName = userName & "@domad.mtulio.eng.br"
    Set objUser = objOUPai.Create("User", DNUser)
    objUser.sAMAccountName = userName
    objUser.givenName = strUnitSigla
    objUser.sn = strSn
    objUser.SetInfo
    objUser.userPrincipalName= strprincipalname
    objUser.displayName = strNameComp
    objUser.company = strCompany
    objUser.description = strNameComp
    objUser.userAccountControl = 512
    objUser.pwdLastSet = 0
    objUser.setPassword("" & "123@qwe" & "")
    objUser.SetInfo
   End if
 Next
' Fim ou=usuarios
End if
' Populando a OU Grupos
If strOU = "ou=grupos" Then
```

```
strDescription = "Grupos - " & strDescription
For i = 1 To countAllGroups
 If (i < 10) Then
  strCnPart = "GRUPO0" & i
 Else
  strCnPart = "GRUPO" & i
 End if
 If strOUOrg = "ou=GYN" Then
  strUnitSigla = "GYN"
  sAMAccountName = strUnitSigla & strCnPart
  strCn = strUnitSigla & strCnPart
  Set objUser = objOUPai.Create("Group", "cn=" & strCn)
  objUser.cn = strCn
  objUser.sAMAccountName = sAMAccountName
  objUser.description = strDescription
  objUser.SetInfo
 ' End GYN
 End If

 If strOUOrg = "ou=ANA" Then
  strUnitSigla = "ANA"
  sAMAccountName = strUnitSigla & strCnPart
  strCn = strUnitSigla & strCnPart
  Set objUser = objOUPai.Create("Group", "cn=" & strCn)
  objUser.cn = strCn
  objUser.sAMAccountName = sAMAccountName
  objUser.description = strDescription
  objUser.SetInfo
 ' End ANA
 End If

 If strOUOrg = "ou=URU" Then
  strUnitSigla = "URU"
  sAMAccountName = strUnitSigla & strCnPart
  strCn = strUnitSigla & strCnPart
  Set objUser = objOUPai.Create("Group", "cn=" & strCn)
  objUser.cn = strCn
  objUser.sAMAccountName = sAMAccountName
  objUser.description = strDescription
  objUser.SetInfo
```

```
  ' End URU
  End If

  If strOUOrg = "ou=FOR" Then
   strUnitSigla = "FOR"
   sAMAccountName = strUnitSigla & strCnPart
   strCn = strUnitSigla & strCnPart
   Set objUser = objOUPai.Create("Group", "cn=" & strCn)
   objUser.cn = strCn
   objUser.sAMAccountName = sAMAccountName
   objUser.description = strDescription
   objUser.SetInfo
  ' End FOR
  End If

  If strOUOrg = "ou=SPO" Then
   strUnitSigla = "SPO"
   sAMAccountName = strUnitSigla & strCnPart
   strCn = strUnitSigla & strCnPart
   Set objUser = objOUPai.Create("Group", "cn=" & strCn)
   objUser.cn = strCn
   objUser.sAMAccountName = sAMAccountName
   objUser.description = strDescription
   objUser.SetInfo
  ' End SPO
  End If
 Next
' Fim ou=grupos
End if

' Populando a base com Computadores
If strOU = "ou=computadores" Then
 strOS = "Microsoft Windows 7 Professinal"
 strSP = "Service Pack 20"
 For i = 1 To countAllComputers
  If (i < 10) Then
   strComputerNamePart = "COMP0" & i
  Else
   strComputerNamePart = "COMP" & i
  End if
```

```
If strOUOrg = "ou=GYN" Then
 strUnitSigla = "GYN"
 strComputerName = strUnitSigla & strComputerNamePart
 DNComp = "cn=" & strComputerName
 Set objUser = objOUPai.Create("Computer", DNComp)   ' Criando objeto
 objUser.cn = strComputerName        ' Atributo Obrigatorio
 objUser.Description = strComputerName      ' Atributo Obrigatorio
 objUser.distinguishedName = DNComp & DNPai     ' Atributo Obrigatorio
 objUser.OperatingSystem = strOS         ' Atributo Opcional
 objUser.OperatingSystemServicePack = strSP     ' Atributo Opcional
 objUser.sAMAccountName = strComputerName & "$"   ' Definindo senha
 objUser.userAccountControl = 4096       ' Ativando a conta
 objUser.SetInfo
End If

If strOUOrg = "ou=ANA" Then
 strUnitSigla = "ANA"
 strComputerName = strUnitSigla & strComputerNamePart
 DNComp = "cn=" & strComputerName
 Set objUser = objOUPai.Create("Computer", DNComp)   ' Criando objeto
 objUser.cn = strComputerName        ' Atributo Obrigatorio
 objUser.Description = strComputerName      ' Atributo Obrigatorio
 objUser.distinguishedName = DNComp & DNPai     ' Atributo Obrigatorio
 objUser.OperatingSystem = strOS         ' Atributo Opcional
 objUser.OperatingSystemServicePack = strSP     ' Atributo Opcional
 objUser.sAMAccountName = strComputerName & "$"   ' Definindo senha
 objUser.userAccountControl = 4096       ' Ativando a conta
 objUser.SetInfo
End If

If strOUOrg = "ou=URU" Then
 strUnitSigla = "URU"
 strComputerName = strUnitSigla & strComputerNamePart
 DNComp = "cn=" & strComputerName
 Set objUser = objOUPai.Create("Computer", DNComp)   ' Criando objeto
 objUser.cn = strComputerName        ' Atributo Obrigatorio
 objUser.Description = strComputerName      ' Atributo Obrigatorio
 objUser.distinguishedName = DNComp & DNPai     ' Atributo Obrigatorio
 objUser.OperatingSystem = strOS         ' Atributo Opcional
 objUser.OperatingSystemServicePack = strSP     ' Atributo Opcional
```

```
    objUser.sAMAccountName = strComputerName & "$"   ' Definindo senha
    objUser.userAccountControl = 4096      ' Ativando a conta
    objUser.SetInfo
   End If

   If strOUOrg = "ou=FOR" Then
    strUnitSigla = "FOR"
    strComputerName = strUnitSigla & strComputerNamePart
    DNComp = "cn=" & strComputerName
    Set objUser = objOUPai.Create("Computer", DNComp)   ' Criando objeto
    objUser.cn = strComputerName        ' Atributo Obrigatorio
    objUser.Description = strComputerName      ' Atributo Obrigatorio
    objUser.distinguishedName = DNComp & DNPai     ' Atributo Obrigatorio
    objUser.OperatingSystem = strOS        ' Atributo Opcional
    objUser.OperatingSystemServicePack = strSP     ' Atributo Opcional
    objUser.sAMAccountName = strComputerName & "$"   ' Definindo senha
    objUser.userAccountControl = 4096      ' Ativando a conta
    objUser.SetInfo
   End If

   If strOUOrg = "ou=SPO" Then
    strUnitSigla = "SPO"
    strComputerName = strUnitSigla & strComputerNamePart
    DNComp = "cn=" & strComputerName
    Set objUser = objOUPai.Create("Computer", DNComp)   ' Criando objeto
    objUser.cn = strComputerName        ' Atributo Obrigatorio
    objUser.Description = strComputerName      ' Atributo Obrigatorio
    objUser.distinguishedName = DNComp & DNPai     ' Atributo Obrigatorio
    objUser.OperatingSystem = strOS        ' Atributo Opcional
    objUser.OperatingSystemServicePack = strSP     ' Atributo Opcional
    objUser.sAMAccountName = strComputerName & "$"   ' Definindo senha
    objUser.userAccountControl = 4096      ' Ativando a conta
    objUser.SetInfo
   End If
 Next
' Fim ou=computadores
End if

' Populando a base com Mapeamentos de Compartilhamentos
If strOU = "ou=objetos" Then
```

```
strDescription = "Compartilhamentos - " & strDescription
For i = 1 To countAllObjects
 If (i < 10) Then
  strCnPart = "SHARE0" & i
  struNCNamePart = "001\share0" & i
  strDescriptionPart = " - Compartilhamento 0" & i
 Else
  strCnPart = "SHARE" & i
  struNCNamePart = "001\share" & i
  strDescriptionPart = " - Compartilhamento " & i
 End if
 If strOUOrg = "ou=GYN" Then
  strUnitSigla = "GYN"
  strCn = strUnitSigla & strCnPart
  struNCName = "\\srv" & strUnitSigla & struNCNamePart
  strDescription = strUnitSigla & strDescriptionPart
  Set objUser = objOUPai.Create("Volume", "cn=" & strCn)
  objUser.cn = strCn
  objUser.uNCName = struNCName
  objUser.uNCName = strDescription
  objUser.SetInfo
 ' End GYN
 End If

 If strOUOrg = "ou=ANA" Then
  strUnitSigla = "ANA"
  strCn = strUnitSigla & strCnPart
  struNCName = "\\srv" & strUnitSigla & struNCNamePart
  strDescription = strUnitSigla & strDescriptionPart
  Set objUser = objOUPai.Create("Volume", "cn=" & strCn)
  objUser.cn = strCn
  objUser.uNCName = struNCName
  objUser.uNCName = strDescription
  objUser.SetInfo
 ' End ANA
 End If

 If strOUOrg = "ou=URU" Then
  strUnitSigla = "URU"
  strCn = strUnitSigla & strCnPart
```

```
      struNCName = "\\srv" & strUnitSigla & struNCNamePart
      strDescription = strUnitSigla & strDescriptionPart
      Set objUser = objOUPai.Create("Volume", "cn=" & strCn)
      objUser.cn = strCn
      objUser.uNCName = struNCName
      objUser.uNCName = strDescription
      objUser.SetInfo
     ' End URU
     End If

     If strOUOrg = "ou=FOR" Then
      strUnitSigla = "FOR"
      strCn = strUnitSigla & strCnPart
      struNCName = "\\srv" & strUnitSigla & struNCNamePart
      strDescription = strUnitSigla & strDescriptionPart
      Set objUser = objOUPai.Create("Volume", "cn=" & strCn)
      objUser.cn = strCn
      objUser.uNCName = struNCName
      objUser.uNCName = strDescription
      objUser.SetInfo
     ' End FOR
     End If

     If strOUOrg = "ou=SPO" Then
      strUnitSigla = "SPO"
      strCn = strUnitSigla & strCnPart
      struNCName = "\\srv" & strUnitSigla & struNCNamePart
      strDescription = strUnitSigla & strDescriptionPart
      Set objUser = objOUPai.Create("Volume", "cn=" & strCn)
      objUser.cn = strCn
      objUser.uNCName = struNCName
      objUser.uNCName = strDescription
      objUser.SetInfo
     ' End SPO
     End If
    Next
   ' Fim ou=objetos
   End if
  Next
Next
```

```
' Definindo a hora atual e gravando no arquivo:
getDateStr DATE_DDMMAAAAHHmmss
objFileWrite.WriteLine("Finish Add to dir: " & DATE_DDMMAAAAHHmmss)
objFileWrite.WriteLine("Estrutura adicionada com sucesso!")
objFileWrite.WriteLine("####################################")

WScript.Echo "Script executado com sucesso."

' Sugestões para melhoria deste script
' 1) Adicionar tratamento de excessões. Exemplo: Verificar se uma
determinada OU existe e não tentar criá-la
' 2) Criar funções e  separar melhor o codigo para maior organização
```

ANEXO VI – Script para criação da Organização no OpenLDAP – DOMOL_criarEstrutura.sh.

```
#!/bin/bash
#
#Name: DOMOL_criarEstrutura.sh
#Copyright: DOMOL MTulio ENG
#Author: Marco Tulio Rodrigues Braga
#E-mail: admin@mtulio.eti.br
#Date: 01/11/11 06:39
#Last Change: 29/11/2011
#Description: Este script foi desenvolvido para criacao
# da estrutura organizacional implementada no
# trabalho de Conclusao de Curso.
# Este script pode ser utilizado e distribuido
# de acordo com a necessidade desde que seja
# contribuido novamente para o autor.
#
#Details:
#
#Sugestões de melhorias:
# - ARQUIVOS LDIF: Criar um analisador Lexico dos
# arquivos LDIF's gerados para evitar falhas na
# insercao dos dados na base, podendo tambem
# ser criada uma analisador sintatico e semantico,
# criando um mini-compilador. Com isso eh possivel
# evitar erros na insercao de registros
# em arquivos LDIF grandes.
# - Pode-se adicionar a verificacao das strings
# validas em cada dn tanto como o tamanho de cada
# atributo.
#
#Problems: Implementar DoWhile(C++) no laco da populacao
# do diretorio

###################################
# 0 - Definindo VARIAVEIS
# Comandos
MOVE=`which mv`
LDAPADD=`which ldapadd`

LDAPADD_ADMIN_AUTH="-x -D
cn=administrador,dc=domol,dc=mtulio,dc=eng,dc=br -w 123456"

# Sera registrado o tempo de execucao para analise
# de performance
HOUR_NOW="date +%d/%m/%Y_%T"

# Definicao: Arquivos e Diretorios
DIR_NAME="/samba/compartilhamentos/GERAL/ldif/`date +%Y%m%d-%H_%M`"
FILE_LOG_TIME="$DIR_NAME/time.log"
FILE_LOG_LDAP_OPE="$DIR_NAME/ldap_oper.log"

# PREREQ

if [ ! -d $DIR_NAME ];then
```

```
 mkdir -p $DIR_NAME
fi

# Registrando:  Inicio do Script
echo "###################################" >> $FILE_LOG_TIME
echo " DOMOL" >> $FILE_LOG_TIME
echo "Iniciando script: `$HOUR_NOW`" >> $FILE_LOG_TIME

# Informacoes sobre a estrutura de Diretorio

DOMAINNAME="domol.mtulio.eng.br"
LDAP_BASE="dc=domol,dc=mtulio,dc=eng,dc=br"
LDAP_BASE_OU="ou=DOMOL,dc=domol,dc=mtulio,dc=eng,dc=br"
LDAP_BINDDN="cn=administrador,dc=domol,dc=mtulio,dc=eng,dc=br"

# OU Generica para usuarios de sistemas (LAM, phpldapadmin)
LDAP_BASE_SYSTEM="ou=SYSTEM,dc=domol,dc=mtulio,dc=eng,dc=br"

NM_ENTIDADE="DOMOL"
NM_ENTIDADE_DESC="MTulio Dominio OpenLDAP"
NM_UNIDADES_SIGLA="GYN ANA URU FOR SPO"
NM_UNIDADES_OU="USUARIOS GRUPOS COMPUTADORES OBJETOS"

# Sempre definir um objeto a mais, pois o laco
# verifica antes de sua execucao

countAllUsers=9
countAllComputers=6
countAllGroups=8
countAllObjects=3

###################################
# 0 - Definindo FUNCOES

fc_createOuUsuarios() {
 i=0
        until [ $i = $countAllUsers ];do
         USERNAME="${UNIDADE}USER${i}"
                cat << EOF >> $FILE_BASE

EOF
                echo "dn: cn=${USERNAME},$DNAtualSub
cn: ${USERNAME}
givenName: ${USERNAME}
mail: ${USERNAME}@${DOMAINNAME}
sn: $UNIDADE User
objectClass: top
objectClass: inetOrgPerson" >> $FILE_BASE
  i=`expr 1 + $i`
                # Fim usuarios
 done
# Fim funcao criar OU Usuarios
}

fc_createOuGrupos() {
 i=0
 until [ $i = $countAllGroups ];do
```

```
  GROUPNAME="${UNIDADE}GRUPO${i}"

 MEMBERSGROUP="cn=${UNIDADE}USER${i},ou=USUARIOS,ou=${UNIDADE},$LDAP_BA
SE_OU"
  cat << EOF >> $FILE_BASE

EOF
  echo "dn: cn=${GROUPNAME},$DNAtualSub
cn: ${GROUPNAME}
description: Group - ${GROUPNAME}
member: ${MEMBERSGROUP}
objectClass: groupofnames" >> $FILE_BASE
  i=`expr 1 + $i`
 done
# Fim funcao criar OU Grupos
}

fc_createOuComputadores() {
 i=0
 until [ $i = $countAllComputers ];do
  COMPUTERNAME="${UNIDADE}COMPUTER${i}$"
  cat << EOF >> $FILE_BASE

EOF
  echo "dn: cn=${COMPUTERNAME},$DNAtualSub
cn: ${COMPUTERNAME}
sn: Hostname: ${COMPUTERNAME}
objectClass: top
objectClass: inetOrgPerson" >> $FILE_BASE
  i=`expr 1 + $i`
  done
# Fim funcao criar OU Computadores
}

fc_createOuObjetos() {
 i=1
 until [ $i = `expr $countAllObjects + 1` ];do
  OBJECTNAME="${UNIDADE}OBJ-SHARE${i}"
  SHARENAME="\\\SERVER${UNIDADE}${i}\SHARED${i}"
               cat << EOF >> $FILE_BASE

EOF
  echo "dn: cn=${OBJECTNAME},$DNAtualSub
description: ${OBJECTNAME}
sn: \\servidor${i}\share${i}
objectClass: top
objectClass: inetOrgPerson" >> $FILE_BASE
  i=`expr 1 + $i`
  done
# Fim funcao criar OU Objetos
}

###################################
# 01 - Criando a BASE e a OU Padrao

echo "Inicio - Criar LDIF: `$HOUR_NOW`" >> $FILE_LOG_TIME
FILE_BASE="/tmp/01-$NM_ENTIDADE.ldif"
```

```
cat << EOF >> $FILE_BASE
dn: $LDAP_BASE
objectClass: top
objectClass: dcObject
objectClass: organization
dc: ${NM_ENTIDADE}
o: ${NM_ENTIDADE_DESC}
EOF

# Movendo o arquivo gerado para o diretorio correto
$MOVE $FILE_BASE $DIR_NAME

# 02 - Criando as OU da Entidade
FILE_BASE="/tmp/02-$NM_ENTIDADE.ldif"

cat << EOF >> $FILE_BASE
dn: ou=$NM_ENTIDADE,${LDAP_BASE}
ou: ${NM_ENTIDADE}
objectClass: top
objectClass: organizationalUnit
EOF

# Movendo o arquivo gerado para o diretorio correto
$MOVE $FILE_BASE $DIR_NAME

# 02 - Criando as OU para Sistemas
FILE_BASE="/tmp/02-SYSTEM.ldif"

cat << EOF >> $FILE_BASE
dn: ou=SYSTEM,${LDAP_BASE}
ou: SYSTEM
description: OU for Systems Objects
objectClass: top
objectClass: organizationalUnit

dn: ou=USERS,${LDAP_BASE_SYSTEM}
ou: USERS
description: OU for Systems Users
objectClass: top
objectClass: organizationalUnit

dn: ou=COMPUTERS,${LDAP_BASE_SYSTEM}
ou: COMPUTERS
description: OU for Systems Computers
objectClass: top
objectClass: organizationalUnit

dn: ou=GROUPS,${LDAP_BASE_SYSTEM}
ou: GROUPS
description: OU for Systems Groups
objectClass: top
objectClass: organizationalUnit

dn: ou=OTHERS,${LDAP_BASE_SYSTEM}
ou: OTHERS
description: OU for Others Systems Objects
```

```
objectClass: top
objectClass: organizationalUnit
EOF

# Movendo o arquivo gerado para o diretorio correto
$MOVE $FILE_BASE $DIR_NAME

# 02 - Criando a estrutura da SAMBA
FILE_BASE="/tmp/02-SAMBA.ldif"

SAMBA_DOMAIN="DOMOL"
# O SID da maquina pode ser obtido pelo comando:
# $ net getlocalsid
# A variavel pode ser utilizada:
# SAMBA_SID="`net getlocalsid |awk -F "is: " '{print$2}'`"
SAMBA_SID="S-1-5-21-3420771710-2698102504-902350248"

cat << EOF >> $FILE_BASE
dn: sambaDomainName=${SAMBA_DOMAIN},${LDAP_BASE}
sambaDomainName: ${SAMBA_DOMAIN}
sambaSID: ${SAMBA_SID}
sambaAlgorithmicRidBase: 1000
objectClass: sambaDomain
sambaMinPwdLength: 5
sambaPwdHistoryLength: 0
sambaLogonToChgPwd: 0
sambaMaxPwdAge: -1
sambaMinPwdAge: 0
sambaLockoutDuration: 30
sambaLockoutObservationWindow: 30
sambaLockoutThreshold: 0
sambaForceLogoff: -1
sambaRefuseMachinePwdChange: 0
EOF

# Movendo o arquivo gerado para o diretorio correto
$MOVE $FILE_BASE $DIR_NAME

###################################
# 03 - Criando as OU das Unidades

for iItem in $NM_UNIDADES_SIGLA; do
 UNIDADE=$iItem
 FILE_BASE="/tmp/03-$UNIDADE.ldif"
 DNAtual="ou=$NM_ENTIDADE,${LDAP_BASE}"

 echo "dn: ou=$UNIDADE,${DNAtual}
ou: ${UNIDADE}
objectClass: top
objectClass: organizationalUnit" >> $FILE_BASE

 for iItemSubOU in $NM_UNIDADES_OU; do
  SUB_OU=$iItemSubOU
  UNI_SUBOU="${iItemSubOU}"
  DNAtualSub="ou=${iItemSubOU},ou=${UNIDADE},${DNAtual}"
  cat << EOF >> $FILE_BASE
```

```
EOF
  echo "dn: ${DNAtualSub}
ou: ${SUB_OU}

objectClass: top
objectClass: organizationalUnit" >> $FILE_BASE

  case "$SUB_OU" in
   "USUARIOS") fc_createOuUsuarios;;
   "GRUPOS") fc_createOuGrupos;;
   "COMPUTADORES") fc_createOuComputadores;;
   "OBJETOS") fc_createOuObjetos;;
   *)echo "Erro desconhecido na criacao das OU's por unidade";;
  esac
 # Fim SubOU
 done
 $MOVE $FILE_BASE $DIR_NAME
# Fim Unidades
done

echo "Fim - Criar LDIF: `$HOUR_NOW`" >> $FILE_LOG_TIME
echo "Start Add to dir: `$HOUR_NOW`" >> $FILE_LOG_TIME

# Executando os scripts na ordem de que o "Pai" seja criado primeiro
que o "Filho"

for LDIF_LIST in $(ls -l $DIR_NAME/01-*.ldif | awk -F " "
'{print$9}');do
 $LDAPADD -f $LDIF_LIST $LDAPADD_ADMIN_AUTH >> $FILE_LOG_LDAP_OPE
done

for LDIF_LIST in $(ls -l $DIR_NAME/02-*.ldif | awk -F " "
'{print$9}');do
 $LDAPADD -f $LDIF_LIST $LDAPADD_ADMIN_AUTH >> $FILE_LOG_LDAP_OPE
done

for LDIF_LIST in $(ls -l $DIR_NAME/03-*.ldif | awk -F " "
'{print$9}');do
 $LDAPADD -f $LDIF_LIST $LDAPADD_ADMIN_AUTH >> $FILE_LOG_LDAP_OPE
done


echo "Finish Add to dir: `$HOUR_NOW`" >> $FILE_LOG_TIME
echo "####################################" >> $FILE_LOG_TIME

#cat $FILE_LOG_TIME

echo "LDIF's criados em: $DIR_NAME" |tee -a $FILE_LOG_TIME
```