ANDERSON VIGNATTI

IMPLANTAÇÃO E ESTUDO DE UM SISTEMA UTILIZANDO O ACTIVE DIRECTORY

Monografia de graduação apresentada ao Departamento de Ciência da Computação da Universidade Federal de Lavras como parte das exigências do curso de Ciência da Computação para obtenção do título de Bacharel em Ciência da Computação.

LAVRAS
MINAS GERAIS - BRASIL
2007

ANDERSON VIGNATTI

IMPLANTAÇÃO E ESTUDO DE UM SISTEMA UTILIZANDO O ACTIVE DIRECTORY

Monografia de graduação apresentada ao Departamento de Ciência da Computação da Universidade Federal de Lavras como parte das exigências do curso de Ciência da Computação para obtenção do título de Bacharel em Ciência da Computação.

Área de Concentração:
Redes de Computadores

Orientador:
Prof. Luiz Henrique Andrade Correia

LAVRAS
MINAS GERAIS - BRASIL
2007

Ficha Catalográfica preparada pela Divisão de Processos Técnicos da Biblioteca Central da UFLA

Vignatti, Anderson

Implantação e estudo de um sistema utilizando o Active Directory / Anderson Vignatti. Lavras – Minas Gerais, 2007

Monografia de Graduação –Universidade Federal de Lavras. Departamento de Ciência da Computação.

1. Redes de Computadores. 2. Windows Server 2003 (Active Directory). 3. O protocolo LDAP. 3. Modelo de redes Workgroups. 4. Modelo de redes Domínio. I. VIGNATTI, A. II. Universidade Federal de Lavras. III. Título.

ANDERSON VIGNATTI

IMPLANTAÇÃO E ESTUDO DE UM SISTEMA UTILIZANDO O ACTIVE DIRECTORY

Monografia de graduação apresentada ao Departamento de Ciência da Computação da Universidade Federal de Lavras como parte das exigências do curso de Ciência da Computação para obtenção do título de Bacharel em Ciência da Computação.

Aprovada em 30 de março de 2007

Profª. Marluce Pereira Rodrigues

Prof. Thiago de Souza Rodrigues

Prof. Luiz Henrique Andrade Correia
(orientador)

LAVRAS
MINAS GERAIS – BRASIL
2007

A Deus primeiramente, aos meus pais Angelo e Guanair, a minha noiva Vanessa, a minha irmã Andréia Vignatti e ao meu irmão Adriano Vignatti e meus amigos.

Agradecimentos

Agradeço primeiramente a Deus, que se não fosse pela tua vontade nada teria se realizado.

Aos amigos de turma, pelas alegrias e tristezas compartilhadas, mas que acima de tudo, os momentos inesquecíveis ficarão guardados para sempre.

Agradeço a todos que me apoiaram e ajudaram durante toda minha graduação, sem os quais eu não poderia ter realizado este trabalho.

Ao meu amor, Vanessa, por todo apoio e incentivo.

Aos meus pais e familiares, que sempre me incentivaram durante a minha jornada.

A todos meus amigos do Centro de Informática (CinUfla), companheiros de trabalho, especialmente aos meus chefes Luiz e Anderson.

Ao meu orientador Luiz Henrique Correia por me guiar durante a elaboração deste trabalho.

A todos os professores do DCC, que contribuíram para minha formação profissional.

IMPLANTAÇÃO E ESTUDO DE UM SISTEMA UTILIZANDO O *ACTIVE DIRECTORY*

RESUMO

A evolução no tratamento de informações veio a revolucionar o mundo em que vivemos, abrindo as fronteiras com novas formas de comunicação e permitindo maior eficiência dos sistemas computacionais.

As redes de computadores são uma realidade nesse contexto e também fazem parte de todo esse processo. Como resultado, os sistemas operacionais de rede se aperfeiçoaram e passaram a gerar muito mais que simples arquivos de rede e serviços de impressão. Eles agora necessitam de um gerenciamento transparente das relações entre os recursos de rede distribuídos e seus usuários.

Portanto, o aumento no tamanho das redes e as constantes mudanças pelas quais as mesmas estão inseridas, fizeram com que as pessoas e as organizações de modo geral, passassem a necessitar de serviços que disponibilizem um acesso cada vez mais transparente. Contudo, surge à necessidade de trabalhar com uma base de dados centralizada, possibilitando a simplificação do gerenciamento; fortalecendo a segurança; aumentando a interoperabilidade, dentre outros benefícios que tragam mais facilidade em criar e manipular essas informações.

Um problema bastante usual em empresas é o de criar um sistema unificado de autenticação. Com a interação do protocolo LDAP ao *Active Directory* pode garantir que todos os usuários dessa empresa possam ter suas contas de acesso unificadas em um domínio. Uma opção que pode ser disponibilizada ao usuário é permitir a interação entre um servidor Windows e um computador Linux (usuário), possibilitando um maior número de usuários na rede e maior utilização de softwares livres. Essa interação só é realizada mediante os dois sistemas operacionais utilizarem o mesmo padrão de protocolos, o LDAP. Este trabalho faz também uma breve descrição de outros softwares de rede que utilizam o protocolo LDAP.

Palavras-chaves: Redes de Computadores, Windows Server 2003 (Active Directory), O protocolo LDAP, Modelo de redes Workgroups, Modelo de redes Domínio.

IMPLANTATION AND STUDY OF A SYSTEM USING THE ACTIVE DIRECTORY

ABSTRACT

The evolution in the treatment of information came to revolutionize the world where we live, opening the borders with new forms of communication and allowing bigger efficiency of the computational systems.

The computer networks are a reality in this context and also they are part of all this process. As result, the operational systems of net if had perfected and started to generate much more that simple archives of net and services of impression. They now need a transparent management of the relations between the resources of net distributed and its users.

Therefore, the increase in the size of the nets and the constant changes for which the same ones are inserted, had made with that the people and the organizations in general way, started to need services that disponibilizem an access each more transparent time. However, it appears to the necessity to work with a database centered, making possible the simplification of the management; fortifying the security; increasing the interoperabilidade, amongst other benefits that bring more easiness in creating and manipulating these information.

A sufficiently usual problem in companies is to create a unified system of authentication. With the interaction of protocol LDAP to Active Directory it can guarantee that all the users of this company can have its unified accounts of access in a domain. An option that can be disponibilizada to the user is to allow to the interaction between a Windows server and a Linux computer (using), making possible a bigger number of users in the net and greater free use of softwares. This interaction alone is carried through by means of the two operational systems to use standard of protocols, the LDAP the same. This work also makes one brief description of others softwares of net that use protocol LDAP.

Key-Words: Computer networks, Windows Server 2003 (Active Directory), protocol LDAP, Model of Workgroups networks, Model of networks domain.

SUMÁRIO

ÍNDICE DE FIGURAS

LISTA DE SIGLAS

ACE- *Access Control Entries*

AD- *Active Directory*

DNS- *Domain Name System*

LDAP- *Lightweight Directory Access Protocol*

TCP- *Transmission Control Protocol*

IP- *Internet Protocol*

DAP- *Directory Access Protocol*

OSI- *Open Source Initiative*

ISODE- *International Organization for Standardization Development Environment*

ITU- *International Telecommunications Union*

IETF- *Internet Engineering Task Force*

ADSI- *Active Directory System Interface*

URL- *Universal Resource Locator*

UOs- Unidades Organizacionais

DHCP- *Dynamic Host Configuration Protocol*

DC- *Domain Controler*

SO- Sistema Operacional

WAN- *Wide Area Network*

LAN- *Local Area Network*

MSI- *Microsft Sistem Installer*

1 . INTRODUÇÃO

No mundo globalizado, as informações sobre pessoas, aplicações e recursos se espalham pela maioria dos sistemas de informação e continuam se ploriferando. Como resultado, os sistemas operacionais de rede precisam gerar muito mais que simples arquivos de rede e serviços de impressão. Agora, necessitam de um gerenciamento transparente dos recursos de rede distribuídos. O sistema operacional Microsoft Windows Server, com seu serviço integrado de diretório ativo (*Active Directory*), deixam as redes mais fáceis de usar, facilitam o gerenciamento da rede.

Em uma rede que utiliza como o software de rede Microsoft Windows Server, o *Active Directory* (AD) é o elemento central, fundamental, sobre o qual é planejada e implementada uma infra-estrutura de rede, sendo o seu elemento principal. O AD é utilizado para centralizar a administração da rede, devido a grande dificuldade que se tem de trabalhar com a base de dados de usuário descentralizado e por reconhecer que é indispensável um melhor gerenciamento dos recursos para os usuários.

Os sistemas distribuídos freqüentemente conduzem a uma administração demorada e redundante. Como as companhias acrescentam aplicações à sua infra-estrutura e contratam mais pessoal, eles precisam distribuir software adequadamente para a área de trabalho e administrar diretórios de aplicações múltiplas. O *Active Directory* permite às companhias baixar, significativamente, os custos com gerenciamento, gerando um único espaço para os usuários, grupos e recursos de rede, bem como distribuir software e administrar configurações da área de trabalho do usuário.

A segurança é integrada ao *Active Directory* através da autenticação de *logon* e controle de acesso a objetos no diretório. Com um único *logon* na rede, os administradores podem gerenciar a organização e os dados de diretório em suas redes. Desta forma, os usuários de rede autorizados podem acessar recursos em qualquer lugar da rede. A administração com base em diretivas facilita o gerenciamento até mesmo das redes mais complexas. As permissões de acesso serão atribuídas aos usuários e grupos do *Active Directory*. Esta abordagem de um diretório único tem inúmeras vantagens: O *logon* único e

o fato de que atualizações feitas no diretório já são feitas automaticamente em todas as aplicações, uma vez que o diretório é único.

Um problema bastante usual em empresas é o de criar um sistema unificado de autenticação. Com a interação do protocolo LDAP ao *Active Directory* pode-se garantir que todos os usuários dessa empresa terão suas contas de acesso cadastradas em um único servidor. Com a autenticação unificada, um conjunto de máquinas compartilham informações diversas para identificar e validar a identidade dos usuários, facilitando o trabalho de usuários e administradores de um sistema distribuído. Atualmente, programas e linguagens de programação têm suporte ao protocolo LDAP(*Lightweight Directory Access Protocol)*. O LDAP pode exercer um papel vital em redes de todos os tamanhos.

Este trabalho é um resultado de experiência prática, onde são mostrados todos os passos que foram efetuados, desde a instalação do AD, criando um DNS (*Domain Name System*), que será o nó raiz desta árvore e o domínio. A instalação de alguns serviços do Windows Server 2003, proporcionam maior eficiência ao administrador deste domínio. Dessa forma, apresentamos algumas características da principal ferramenta do Server 2003, que é o *Active Directory*. Neste trabalho abordamos a interação do protocolo LDAP com o *Active Directory*. No capítulo 2 mostraremos sua história, os serviços do *Active Directory*, citaremos outras ferramentas que utilizam o protocolo LDAP.

1.1 Objetivos

O principal objetivo deste trabalho é centralizar a administração da rede, utilizando a principal ferramenta do Windows Server 2003, o *Active Directory*; para gerenciar todos os computadores de um domínio.

- Apresentar os principais benefícios que o AD pode trazer para as redes, transformando um modelo de rede Workgroups para um modelo de rede Domínio.

Os objetivos secundários deste trabalho são:

- Estudar como é estabelecida a comunicação entre um computador cliente, utilizando um sistema operacional Linux, e um servidor, utilizando o sistema operacional Windows Server 2003, com a sua principal ferramenta *Active Directory*.

1.2 Motivação

Na migração das redes Windows *Workgroups* para domínio, apenas usuários autenticados podem *logar* neste domínio. Essa autenticação aumenta a segurança da rede, evitando que usuários não cadastrados venham a utilizar o sistema. Os usuários cadastrados no sistema têm a facilidade de *logar* em qualquer computador deste domínio. Entretanto, é necessário um *login* e uma senha para que o usuário tenha as permissões a ele concedidas pelo administrador.

Devido a grande dificuldade que se tem de trabalhar com a base de dados de usuários descentralizada e por reconhecer que é indispensável um melhor gerenciamento dos recursos da rede para os usuários, vislumbramos a solução de administrar a rede por meio do AD. Com a administração da rede centralizada, podemos criar grupos de usuários sendo que cada grupo possuirá diretivas ou políticas adotadas pela empresa. A administração do sistema pode permitir e fornecer acesso a esses grupos. Ao cadastrarmos o usuário em determinado grupo, ele passará a ter os privilégios deste determinado grupo, podendo ser cadastrado em mais de um grupo.

A implantação do AD irá permitir a interação entre os sistemas operacionais Linux e Windows, permitindo um número maior de usuários trabalharem no mesmo domínio, além da maior disseminação de softwares livres.

1.3 Estrutura do trabalho

Este trabalho é dividido em 5 capítulos, descritos a seguir.

No capítulo 2, descrevemos o principal protocolo que é utilizado pelo AD, protocolo LDAP. Apresentamos sua definição, vantagens, desvantagens e outras empresas que utilizam o padrão protocolo LDAP.

No capítulo 3, mostramos a principal ferramenta do Windows Server 2003, AD. Apresentamos as vantagens da transformação de uma rede *Workgroups* para uma rede Domínio e a interação do DNS ao AD. Mostramos também as camadas de estrutura lógica do AD, a maneira como o AD é apresentado aos administradores e usuário e outros serviços que o AD utiliza para uma melhor administração da rede.

No capítulo 4, mostramos a utilização do protocolo LDAP no AD e algumas versões do protocolo LDAP que o AD tem suporte. Apresentamos como é feita a autenticação de um usuário Linux no Windows Server 2003, criando uma comunicação entre um computador cliente, utilizando um sistema operacional Linux, e um servidor, utilizando o sistema operacional Windows Server2003.

No capítulo 5, mostramos algumas aplicações práticas que o AD nos proporciona, como a criação e o gerenciamento de um laboratório institucional.

2 . O PROTOCOLO LDAP

O protocolo LDAP (*Lightweight Directory Access Protocol*) é empregado para acessar serviços de diretório, ou seja, é uma definição de protocolo para acesso a bancos de dados especializados nos chamados diretórios.

Segundo (Allem e Puckett, 2002), o LDAP pode ser usado em qualquer tipo de rede TCP/IP (*Transmission Control Protocol / Internet Protocol*) sendo um padrão aberto e que, permite que existam produtos para várias plataformas. O LDAP organiza os recursos da rede de forma hierárquica, como uma árvore de diretórios, na qual temos primeiramente um diretório raiz, em seguida a rede da empresa, o departamento e por fim o computador do funcionário e os recursos de rede (arquivos, impressoras e outros) compartilhados por ele.

2.1 Histórico

No início da década de 80 para criar um serviço de mensagens (a série X.400), ou seja, um protocolo que especifica serviços do tipo *store-and-forwar*d, houve a necessidade de desenvolver um protocolo que organizasse as entradas em um serviço de nomes de forma hierárquica, capaz de suportar grandes quantidades de informação e com uma enorme capacidade de procura de informação. Esse serviço criado pela Universidade de Michigan, com apoio do *Consortium* do ISODE (*International Organization for Standardization Development Environment*), foi apresentado em 1988. Ele especificava a comunicação entre o cliente e o servidor do Diretório que usava o DAP (*Directory Access Protocol)* e era executado sobre a pilha de protocolos do modelo OSI (*Open Source Initiative*). O DAP é um protocolo complexo, que roda sobre uma camada OSI completa, e precisa de uma quantidade significante de recursos computacionais para ser executado.

O X.500 é um Serviço de Diretório universal padronizado pela ITU (*International Telecommunications Union),* com o objetivo de definir a ligação entre Serviços de Diretórios locais para assim formar um diretório global distribuído. O fato do protocolo X.500 ser muito complexo e de custo incompatível, levou os pesquisadores da Universidade de Michigan a criar um servidor LDAP (*Lightweight Directory Access Protocol).*

Em 1993 o LDAP foi então apresentado como alternativa ao protocolo DAP para acesso a Diretórios baseados no modelo X.500. O LDAP roda diretamente sobre o TCP e fornece a maioria das funcionalidades do DAP, a um custo muito menor. Foi implementado pela primeira vez na própria universidade de Michigan. Esse grupo de pesquisadores disponibilizou o código fonte do protocolo LDAP na Internet e criou listas de discussão para divulgar e aperfeiçoar o novo serviço, sendo a sua evolução acompanhada por pessoas do mundo inteiro.

O LDAP foi reconhecido como um padrão da IETF (*Internet Engineering Task Force*), em Dezembro de 1997, o IETF lançou a versão três do LDAP como proposta padrão Internet para Serviços de Diretório.

2.2 Características

Conforme (Bialaski**,** 2000)**,** uma das principais vantagens do LDAP é a facilidade em localizar informações e arquivos disponibilizados. Pesquisando pelo sobrenome de um funcionário é possível localizar dados sobre ele, como telefone, departamento onde trabalha, projetos em que está envolvido e outras informações incluídas no sistema, além de arquivos criados por ele ou que lhes façam referência. Cada funcionário deve ter uma conta de acesso no servidor LDAP, para que possa cadastrar informações sobre si e compartilhar arquivos.

As informações do LDAP estão guardadas segundo uma estrutura em árvore e raramente se efetuam atualizações. O servidor está otimizado para responder a um grande número de pesquisas e tem um alto nível de segurança.

O LDAP centraliza toda a informação trazendo assim enormes benefícios, como por exemplo, um único ponto de administração e menor duplicação de dados. Além disso, utiliza um mecanismo de replicação que funciona de forma hierárquica, passando de pai para filho. O nó pai tem privilégios sobre o nó filho, logo, o nó pai pode conceder e remover privilégios. Ele fornece um mecanismo de segurança tanto para a autenticação, quanto para troca de dados.

Atualmente, várias aplicações têm suporte para LDAP, uma delas é a principal ferramenta do sistema operacional Windows Serve 2003. O LDAP vem sendo usado cada vez mais por administradores de rede porque as suas características e as suas vantagens em muitos casos compensam a sua complexidade. A prova disso é que cada vez mais aplicações e sistemas operacionais possuem suporte para LDAP. Apesar disso, o LDAP apresenta algumas restrições, como:

- Em alguns casos não substitui as Bases de Dados Relacionais.
- As atualizações são raramente efetuadas.
- Permite o armazenamento confiável somente de dados estáticos.
- Não é possível relacionar dois atributos, visto que não se trata de uma Base de Dados Relacionais, mas sim de uma base de dados estruturada hierarquicamente.

O LDAP pode ser utilizado em várias aplicações como mostrado a seguir.

2.3 Aplicações do LDAP

Segundo (Kanies, 2001), para compreender porque e como o LDAP está sendo uma ferramenta tão importante na vida de um administrador da rede, é necessário compreender como as dificuldades de administrar uma rede com uma base de dados descentralizada e

como o protocolo LDAP pode ser muito útil para uma eficiente administração da rede. Isto significa que, o LDAP pode ser visto como uma tecnologia e como uma ferramenta.

Várias grandes empresas participaram do desenvolvimento de aplicações que empregam o LDAP, entre elas:

- *Apache (através do Apache Directory Server)*
- *Apple (através do Open Directory/OpenLDAP)*
- *AT&T*
- *Banyan*
- *eB2Bcom (através do View500)*
- *Hewlett-Packard*
- *IBM/Lotus*
- *ISODE (através do M-Vault server)*
- *Microsoft (através do Active Directory)*
- *Netscape (agora em Sun Microsystems and Red Hat products)*
- *Novell (através do eDirectory)*
- *OctetString (através do VDE server)*
- *Oracle (através do Oracle Internet Directory)*
- *Radiant Logic (através do RadiantOne Virtual Directory Server)*
- *Red Hat (através do Red Hat Directory Server)*
- *Siemens AG (através do DirX server)*
- *SGI and*
- *Sun (através do iPlanet and Sun ONE directory servers)*
- *Symlabs (através do Directory Extender)*

Na figura 2.1, podemos ver alguns serviços e aplicações que o protocolo LDAP fornece suporte, entre elas duas em que utilizamos em nossas aplicações práticas, como a sua utilização nas redes Microsoft e Linux.

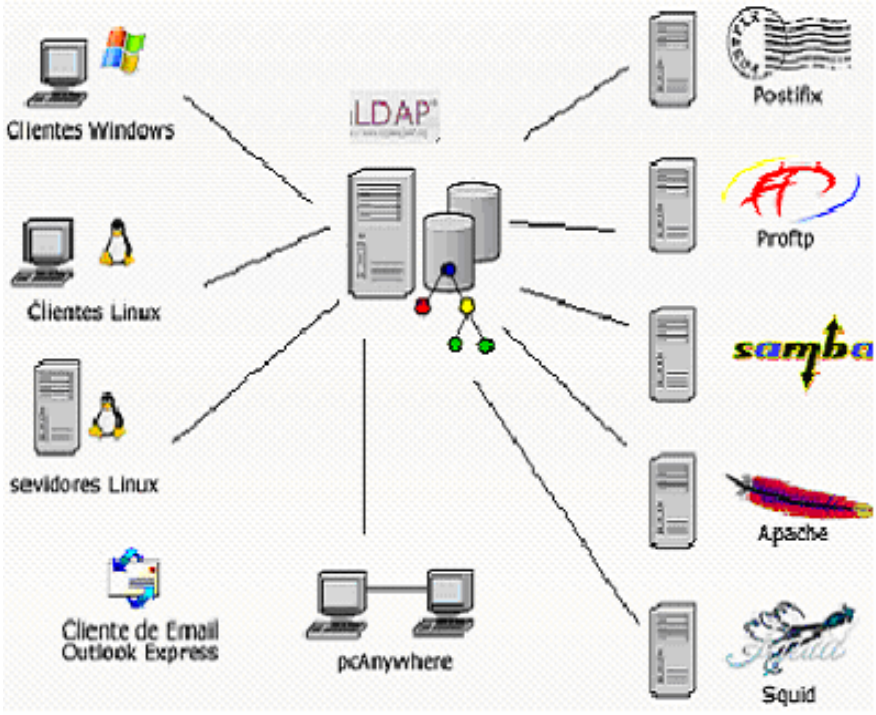

Figura 2-1 Alguns serviços que o protocolo LDAP fornece suporte. (Fonte: www.ldap.org)

O LDAP é usado atualmente pela maioria dos administradores de rede em detrimento das Bases de Dados Tradicionais, porque além das suas características já referidas, cada vez mais existem aplicações com suporte LDAP é uma das tecnologias mais difundidas e menos compreendidas da Internet o LDAP está em todo lugar, entretanto, é desconhecido da maioria dos profissionais.

Note que embora seja possível ter acesso à base de dados remotamente, o LDAP não é um protocolo freqüentemente usado na Internet, apenas em Intranets, sobretudo de grandes empresas, já que quanto maior é o número de usuários e de documentos disponíveis, maior é sua utilidade.

Neste capítulo vimos à teoria do protocolo LDAP, sua história, características, aplicações e algumas empresas que utilizam o protocolo, como a Microsoft (AD) e Linux.

O AD é umas das ferramentas que utiliza o protocolo LDAP para serviços de diretórios, mais características são apresentadas a seguir:

3 . ACTIVE DIRECTORY

Criado em 1996, o *Active Directory* foi implementado no Windows Server 2000. O *Active Directory* foi, sem dúvidas, a grande novidade do Windows Server 2000 em relação ao Windows NT Server 4.0. Algumas revisões para aumentar a funcionalidade e melhorar a administração foram necessárias para incorporar ao AD Windows Server 2003, sendo hoje, a sua principal ferramenta. O *Active Directory* também é o elemento central, fundamental, sobre o qual é planejada e implementada uma infra-estrutura de rede, sendo o elemento principal da Microsoft no Windows Server.

O *Active Directory* é o serviço de diretórios para os sistemas operacionais Windows Server 2003, *Standard Edition*, Windows Server 2003, *Enterprise Edition* e Windows Server 2003, *Datacenter Edition*. Ele armazena informações sobre objetos na rede, fazendo com que estas informações sejam fáceis de encontrar e utilizar por administradores e usuários. Possui um arquivo de dados estruturado como a base de uma organização lógica e hierárquica de informações de diretório.

Conforme (Picoto, 1999), o AD permite que qualquer controlador de domínio seja o único ponto de administração necessário para recursos publicados, os quais podem incluir periféricos, usuários, qualidade da ligação de rede para grupos de usuários e outros objetos.

Segundo (Anderson et al, 2001), o *Active Directory* é uma execução de serviços de diretório do protocolo LDAP pela Microsoft, para o uso em ambientes Windows. O *Active Directory* permite que os administradores atribuam políticas a grandes empresas, instalações de programas automaticamente, apliquem atualizações críticas a uma organização inteira. As redes do *Active Directory* podem variar de uma instalação pequena com alguns objetos, a uma instalação grande com milhões dos objetos.

Segundo (Param, 2001), o *Active Directory* é um serviço de diretório do Windows 2000 que permite as organizações mantenham as informações centralizadas dos recursos e usuários da rede. Uma característica significativa do *Active Directory* é a utilização do protocolo LDAP. Infelizmente, é ainda muito difícil utilizar o *Active Directory*, sem usar os serviços (ADSI) *Active Directory System Interface*.

Conforme (Schley, 2004), o *Active Directory* é um componente essencial da última geração da arquitetura de rede do Windows Server. Oferece um serviço de diretório que permite que as organizações controlem de maneira centralizada as informações dos recursos dos usuários da rede. Ele armazena também as informações de segurança da rede de Windows. O Windows faz com que o servidor de rede, utilize o *Active Directory* e um controlador de domínio em uma rede. Todos os objetos armazenados no *Active Directory* são acessíveis através do protocolo LDAP. O *Active Directory* suporta as versões LDAPv2 e LDAPv3.

O *Active Directory* dá suporte aos sistemas operacionais Microsoft Windows 2000 Professional, Windows XP Professional, Windows 98 e Linux. Porém, a atualização do Win98 foi descontinuada em julho de 2006, impedindo assim sua atualização e não permitindo a migração de redes modelo *Workgroups* para modelos de domínio (ver seção 3.3).

O serviço de diretório do *Active Directory* pode ser instalado em servidores que executem o Microsoft Windows Server 2003. Ele armazena informações sobre objetos na rede e facilita o acesso de administradores e usuários a essas informações. Esse armazenamento de dados, também conhecido como diretório, contém informações sobre os objetos do *Active Directory*. Geralmente, os objetos incluem recursos compartilhados como servidores, arquivos, impressoras, contas de usuário e de computador da rede.

A segurança é integrada ao *Active Directory* através da autenticação de *logon* e controle de acesso a objetos no diretório. Com um único *logon* na rede, os administradores podem gerenciar a organização e os dados de diretório em suas redes e os usuários de rede autorizados podem acessar recursos em qualquer lugar da rede. A administração com base em diretivas facilita o gerenciamento até mesmo das redes mais complexas.

Segundo (Oliver, 2003) o *Active Directory*, sem sombra de dúvida, foi a principal ferramenta dos Windows Serves, sendo agora, uma ferramenta padrão em muitas empresas de todo mundo. Sua entrada no mercado foi marcada radicalmente no coração da plataforma dos usuários de Windows. Hoje, seria muito difícil administrar uma rede

Windows com a base de dados descentralizada, e com o *Active Directory*, a rede torna-se mais segura e mais fácil de ser administrada.

O *Active Directory* e o DNS são ligados por completo, não podendo instalar o *Active Directory* sem o DNS. De fato, o *Active Direcory* está construído no DNS (*Domain Name System*).

3.1 DNS

O sistema de nomes de domínios DNS (*Domain Name System*) oferece um serviço de nomes de computadores e redes organizado em uma hierarquia de domínios. Os nomes DNS são usados em redes TCP/IP, como a Internet, para localizar computadores e serviços por meio de nomes amigáveis para o usuário. Quando um usuário insere um nome DNS ou uma URL (*Universal Resource Locator*em) em um aplicativo, o serviço DNS pode resolver o nome para outra informação associada ao nome, como um endereço IP.

Por exemplo, a maioria dos usuários prefere um nome amigável, como a URL *labinst.ufla.br*, para localizar um computador como um servidor de correio ou da *Web* em uma rede. Um nome amigável pode ser mais fácil de aprender e lembrar do que um número. No entanto, os computadores se comunicam em rede usando endereços numéricos. Para utilizar os recursos da rede de maneira mais fácil, os sistemas de nomes como o DNS fornecem um modo de mapear o nome amigável do usuário de um computador ou serviço para seu endereço numérico conforme figura 3.1.

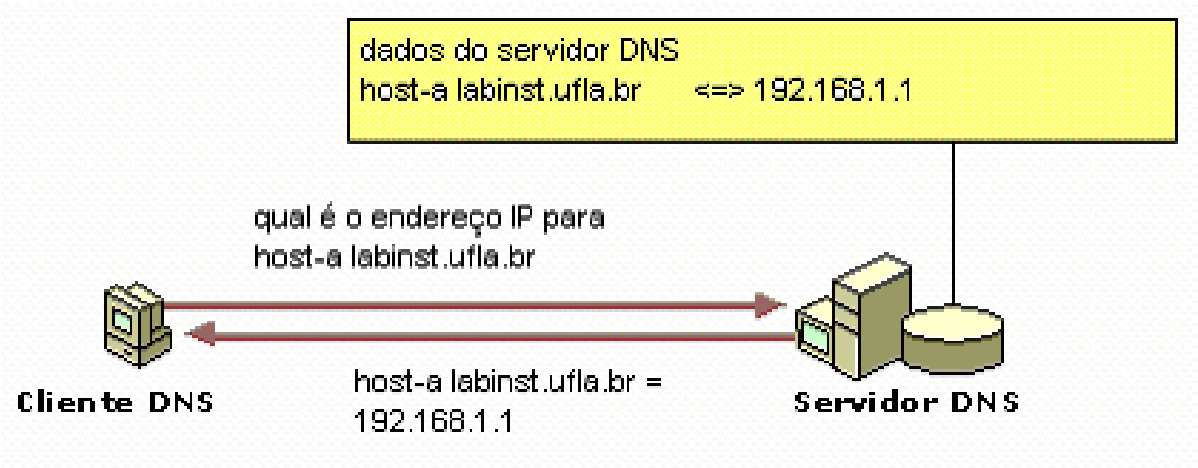

Figura 3-1Exemplo do funcionamento do DNS. (Fonte: Autor)

O exemplo da figura 3.1, um cliente consulta um servidor DNS, solicitando o endereço IP de um computador configurado para usar *host-a labinst.ufla.br* como nome de domínio DNS. Como o servidor DNS é capaz de responder à consulta com base no banco de dados local, ele envia com uma resposta que contém as informações solicitadas: um registro de recurso de *host* (A) que contém as informações de endereço IP para *host-a labinst.ufla.br*.

O sistema de nomes de domínios DNS foi projetado originalmente como um protocolo aberto e, conseqüentemente, vulnerável a invasores. O DNS do Windows Server 2003 melhorou a capacidade de impedir um ataque na infra-estrutura do DNS com a adição de recursos de segurança.

Em seguida mostraremos a camadas de estrutura lógica do AD, a maneira de como o AD é apresentado aos usuários e administradores deste domínio.

3.2 Camadas de estrutura lógica do Active Directory

Os elementos que compõem a estrutura do AD, são apresentadas ao administrador e aos usuários, quando estes utilizam as ferramentas de administração e pesquisa do AD.

A estrutura física determina onde são armazenadas as informações do *Active Directory*, como as informações são sincronizadas entre os diferentes DCs (controlador de Domínio). Por outro lado, a estrutura física pode ser diferente, e normalmente é, da estrutura lógica que é composta por: Domínios, Árvore, Floresta, Relação de Confiança, Objeto do AD, Unidades Organizacionais e Esquemas. Mostraremos agora cada uma delas nos próximas seções.

3.2.1 Domínios

Os domínios são unidades de replicação. Um domínio é a fronteira administrativa para gerenciar objetos, como usuários, grupos e computadores. Além disso, cada domínio possui diretivas de segurança individuais e relações de confiança com outros domínios. Todos os controladores de domínio em determinado domínio podem receber alterações e replicá-las em todos os outros controladores do domínio. Cada domínio do *Active Directory* é identificado por um sistema de nomes de domínios (DNS) e requer um ou mais controladores. Se a rede precisar de mais de um domínio, o administrador poderá criar facilmente vários domínios.

Para (Santos e Câmara, 2002) os domínios representam uma partição lógica do *Active Directory* que serve tanto para a segurança quanto para replicação de diretórios. Os administradores de domínio podem criar, excluir e gerenciar todos os objetos que residem no domínio pelo qual são responsáveis. Também podem atribuir e redefinir senhas, além de delegar uma autoridade administrativa para recursos de rede a outros usuários confiáveis.

O administrador não precisa criar domínios separados apenas para a organização de divisões e departamentos da sua empresa. Em um domínio, é possível usar unidades organizacionais para esse fim. A criação de um novo grupo facilita o gerenciamento das contas e os recursos existentes no domínio. Em seguida, o administrador pode atribuir configurações de diretiva de grupo e incluir usuários, grupos e computadores. O uso de um único domínio simplifica bastante a sobrecarga administrativa. Com a facilidade de criar diretiva por grupo (GPO) ele pode estabelecer a forma como os recursos de domínio são acessados, configurados e usados. Essas diretivas são aplicadas somente no domínio e não entre domínios.

Conforme (Shimonski, 2005), é importante saber controlar os níveis funcionais do usuário no Windows 2003 e podem ser de grande uso quando solicitado. Muitas vezes, é preciso adicionar a funcionalidade a seu domínio, e se estiver usando versões diferentes de Windows Server 2000/2003, têm que considerar os níveis funcionais, ajustando o seu domínio ou mesmo a floresta. Caso esteja utilizando outros servidores diferentes, transforme o seu Server 2000 para nível funcional do Server 2003, assim aumentará o nível funcional de seu domínio.

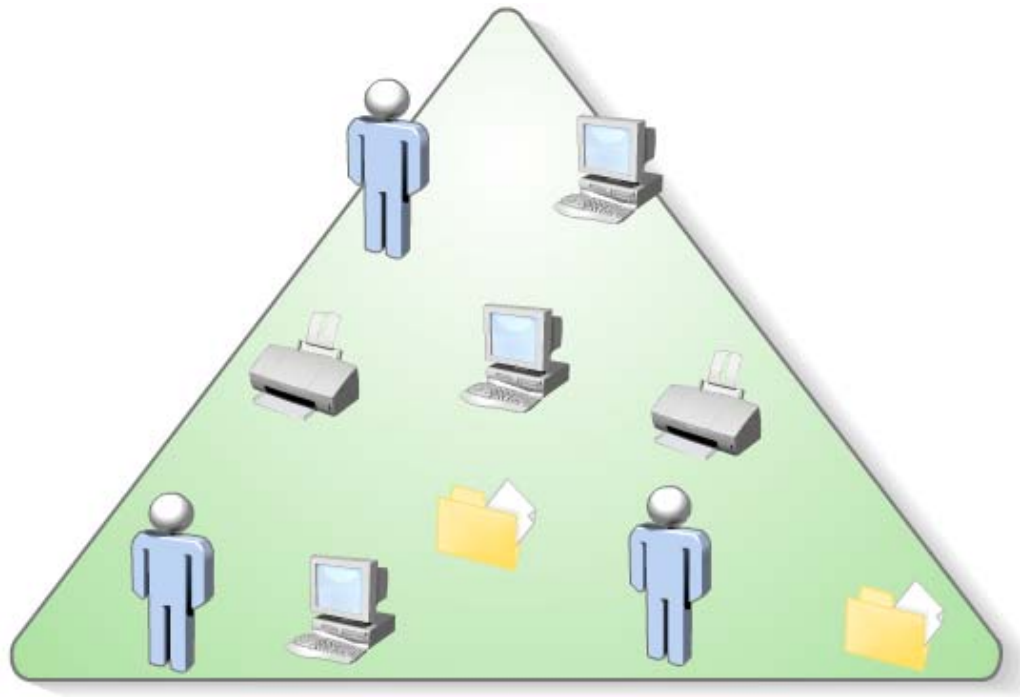

Figura 3-2 Exemplo de um domínio. (Fonte: Macromedia, Inc- Flash Player)

Pela figura 3.2, podemos ver claramente um domínio. Dentro de um domínio temos os objetos que são os usuários, computadores, grupos, impressoras, aplicativos, entre outros. Na próxima seção descrevemos os objetos do AD.

3.2.2 Objetos do Active Directory

Cada objeto representa uma única entidade, que pode ser um usuário, um computador, uma impressora, uma aplicação, ou dados compartilhados. Os objetos podem também ser recipiente de outros objetos. Por exemplo, os atributos de um objeto Arquivo incluem seu nome, localização e tamanho, enquanto os atributos de um objeto Usuário do *Active Directory* devem incluir o nome, sobrenome e endereço de *email* do usuário.

De acordo (Possey, 2006), quando criamos objetos no *Active Directory*, temos a possibilidade de incorporar a informação relacionada aos atributos de um número de objeto. Por exemplo, se estivermos criando um objeto do usuário devemos incorporar toda a informação usual tal como o *user_name* e a senha, mas podemos também incorporar a outra informação tal como o endereço do usuário e o número de telefone.

3.2.3 Unidades Organizacionais (UOs)

Algumas vezes um domínio é uma área grande demais para ter o acesso concedido. Por exemplo, suponha que precisamos contratar algumas pessoas para trabalharem com alguns serviços do *Active Directory* sem que esta pessoa tenha acesso a todo o domínio. Então criamos um novo usuário com certos privilégios, que por exemplo, ficará responsável pela folha de pagamento do grupo contabilidade, conforme mostrado na figura 3.3. Dessa forma, o administrador do domínio dará certos privilégios a este usuário “administrador”, podendo ter acesso total ou parcial da folha de pagamento. Pode criar um novo administrador para um grupo, como por exemplo, o gerente do setor Jurídico ter

controle total sobre o grupo jurídico, conforme mostrado na figura 3.3. A idéia é subdividir o domínio em unidades organizacionais ou UOs.

Figura 3-3Criação de unidades Organizacionais dentre de um Domínio. (Fonte: Macromedia, Inc-Flash Player)

Segundo (Anderson et al, 2001) o UO é responsável por dar o controle de um conjunto de contas de usuários e/ou máquinas para um conjunto de usuários, permitindo, por exemplo, definirmos um conjunto de pessoas que poderão redefinir senhas em um determinado departamento sem ter de torná-los administradores com mais poderes do que o desejável e, além disso, podemos restringir o grupo de pessoas em que as senhas possam ser alteradas.

Conforme (Shimonski, 2005), durante a instalação *Active Directory* em uma organização, é sempre importante considerar o sistema desta organização e verificar que algumas configurações importantes estão sendo utilizadas. Uma das mais importante é o planejamento do sistema local do usuário, criando diretivas para usuários, restringindo assim seus acessos e permitindo alguns privilégios.

3.2.4 Árvore

Se vários domínios tiverem nomes de DNS contíguos, essa estrutura será chamada de árvore de domínio**.** No DNS, a estrutura de árvore hierárquica invertida é usada para indexar nomes de domínio. As árvores de domínio são semelhantes, quanto ao propósito e ao conceito, às árvores de diretórios usadas pelos sistemas de arquivamento do computador para armazenamento em disco. Por exemplo, quando houver vários arquivos armazenados em disco, os diretórios poderão ser usados para organizá-los em conjuntos lógicos. Quando uma árvore de domínio tiver uma ou mais ramificações, cada uma poderá organizar nomes de domínio usados no espaço para nome nos conjuntos lógicos.

Conforme (Santos e Camara, 2002) uma árvore é uma reunião hierárquica de domínios organizados em um espaço de nome contíguo. Uma árvore também constitui em um único domínio do Windows 2000. Podemos criar um espaço de nome contíguo maior, unindo diversos domínios em uma estrutura hierárquica. O primeiro domínio AD criado é chamado de raiz da árvore.

Neste trabalho, criamos um domínio chamado *labinst.ufla.br* e *drca.ufla.br*. Vale a pena ressaltar, porém, não colocamos em prática em nosso trabalho, o funcionamento dos domínios de forma hierárquica. O *Active Directory* cria relacionamentos de confiança automaticamente entre cada domínio e seus domínios filhos. Facilitando permissões aos seus domínios filhos, como por exemplo, serviço de impressão, entre outros.

Observe que é exibida uma árvore com 3 diretórios, conforme mostrado na figura 3.4. O domínio inicial, também conhecido como domínio pai ou domínio raiz, é *ufla.br*. Os domínios filhos seguintes são: *dcc.ufla.br* e *cin.ufla.br*.

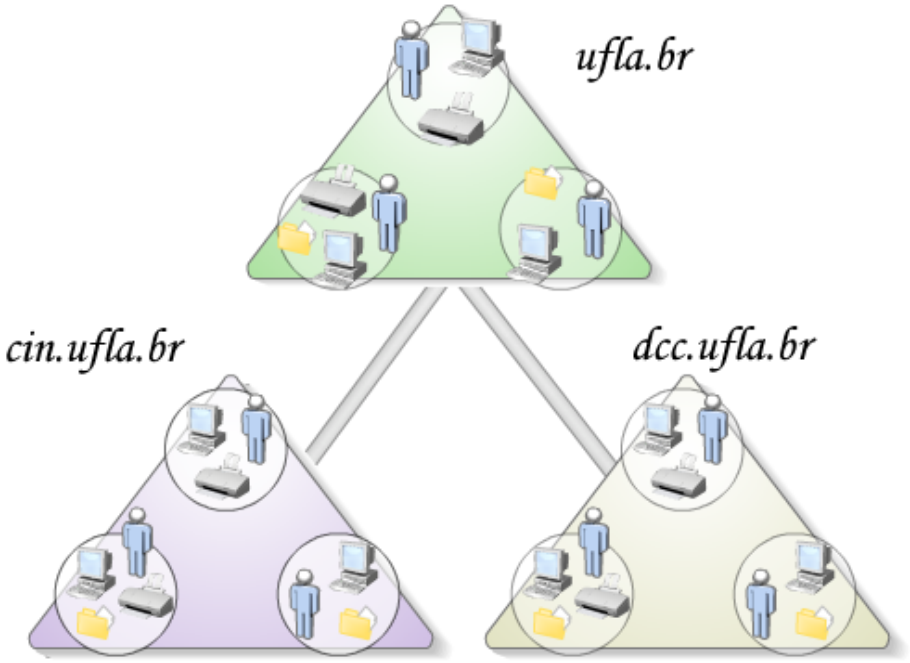

Figura 3-4 Exemplo de uma Árvore de Domínio compartilhando o mesmo nome.(Fonte: Macromedia, Inc- Flash Player)

Quando é formada uma hierarquia de diretórios, há um compartilhamento de nomes. Significa que os nomes dos objetos filho de segundo nível, por exemplo, *dcc.ufla.br* e *cin.ufla.br*, contêm o nome do objeto pai (*ufla.br*). Por exemplo, *dcc.ufla.br* contém *ufla.br*.

Com isso uma árvore de diretórios deste tipo forma um espaço de nomes contínuo, no qual o nome do objeto filho sempre contém o nome do objeto pai.

3.2.5 Floresta

Suponha, porém, que uma empresa esteja dividida em *ufla.br e ufes.br*, conforme figura 3.5. Suponha, ainda, que esta empresa resolveu continuar com uma empresa de domínios múltiplos e quer manter uma parte de sua firma como *ufla.br* e outra como *ufes.com.* Entretanto, é bastante provável que tenhamos dois domínios e esses dois domínios não caberão na mesma árvore.

Podemos optar por construir esses dois domínios do AD em uma mesma estrutura unificada, mas ela não poderá ser uma árvore devido aos nomes desiguais. Em vez disso,

optaremos pela criação de uma floresta. Uma floresta nada mais é do que um grupo de árvores, como podemos observar na figura 3.5.

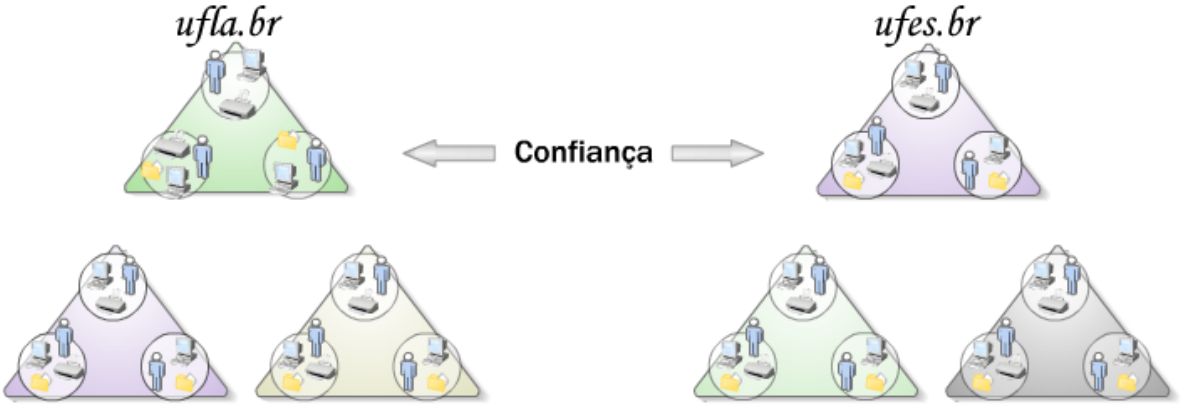

Figura 3-5 Exemplo de uma Floresta. (Fonte: Macromedia, Inc- Flash Player)

O primeiro domínio em uma floresta é chamado de domínio raiz da floresta. Para o DNS e o *Active Directory*, são nomes diretamente acima de outros nomes de domínio derivativos (domínios filho). Por exemplo, *ufla.br* poderia ser o domínio pai para *dcc.ufla.br* (um domínio filho).

3.2.6 Relação de confiança

Quando uma nova árvore de domínio é criada em uma floresta existente, ou mesmo um nó filho de mesma extensão, uma relação de confiança da raiz de árvore é estabelecida por padrão. No *Active Directory*, há uma estrutura hierárquica de um ou mais domínios. Várias árvores de domínio podem pertencer à mesma floresta. Em uma floresta, uma relação de confiança é criada automaticamente entre o domínio raiz de floresta e os domínios raiz de cada árvore.

Conforme (Santana, 2000), com a utilização de domínios, podemos fazer com que nossa rede reflita a estrutura de uma empresa. Quando utilizamos vários domínios temos o

conceito de relação de confiança. A relação de confiança permite que os usuários de ambos os domínios acessem os recursos localizados nesses domínios. No Windows 2000, as relações de confianças são bidirecionais e transitivas, ou seja, se o servidor X confia no servidor Y, e Y confia no servidor W, o servidor X também confia no servidor W, o servidor Y confia no servidor P, o servidor P confia no servidor M que este confia no servidor W, o servidor H confia no servidor P e T, e assim por diante, como mostra a figura 3.6.

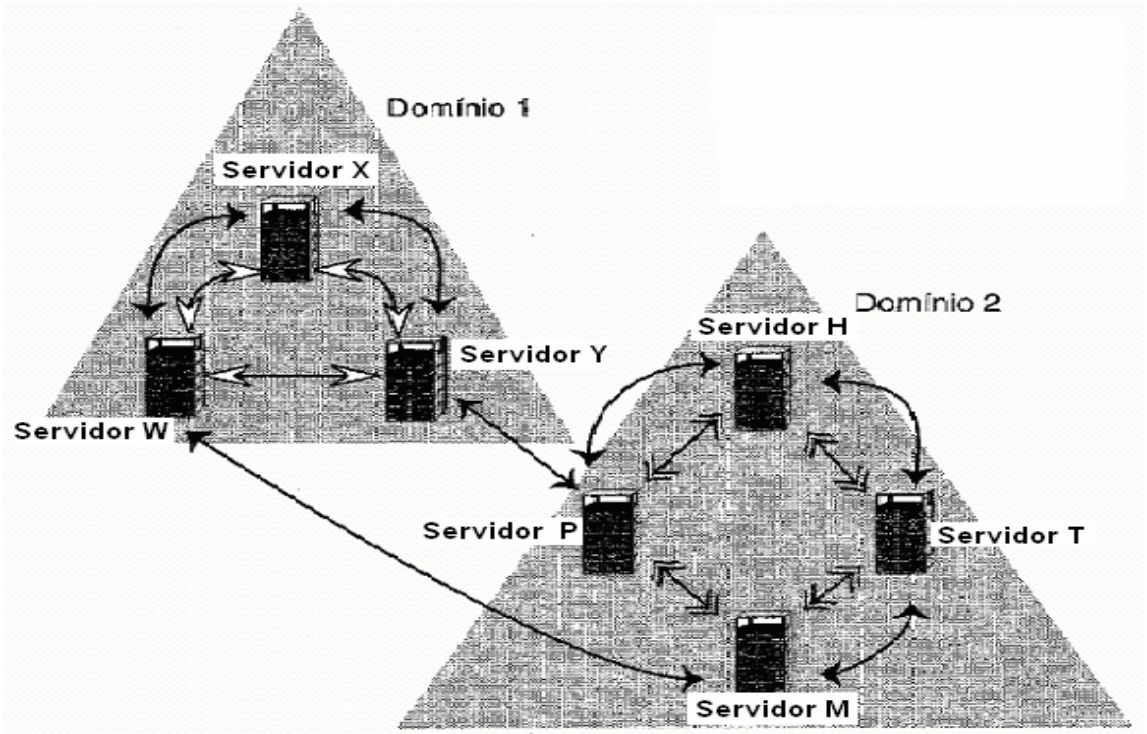

Figura 3-6Exemplo de uma relação de confiança. (Fonte Windows Server 2003 A Bíblia)

3.2.7 Esquema do AD

O Esquema do *Active Directory* é o conjunto de definições que estabelecem os tipos de objetos e os tipos de informações sobre estes objetos, que podem ser armazenados no *Active Directory*. As definições em si são armazenadas como objetos para que o *Active Directory* possa gerenciar os objetos do esquema com as mesmas operações de gerenciamento usadas para os demais objetos no diretório. Existem dois tipos de definições no esquema: atributos e classes, que também são chamados de objetos.

3.2.8 Integração do DNS ao Active Directory

Para (Posey, 2005), o *Active Directory* e o DNS possuem a mesma estrutura hierárquica, embora separados e implementados de diferentes formas para diversas finalidades. O nome do DNS é o mesmo usado para o *Active Directory* e possuem estrutura idêntica para mesma organização. Por exemplo, *microsoft.com* é um domínio DNS e um domínio *Active Directory.*

As zonas de DNS podem ser armazenadas no *Active Directory*. Se estivermos usando o serviço DNS do Windows Server 2003, os arquivos da zona primária poderão ser armazenados no *Active Directory* para replicação em outros controladores de domínio. O *Active Directory* usa o DNS como um serviço localizador, resolvendo o domínio, o site e os nomes de serviço do AD para um endereço IP.

O acesso do usuário ao domínio do AD, permite que o cliente do *AD* consulte seu servidor DNS configurado em busca do endereço IP do serviço LDAP que está sendo executado em um controlador de um domínio específico.

Conforme (Droubi, et al, 2003) quando a Microsoft começou o desenvolvimento do AD, criar uma compatibilidade com o DNS era a grande prioridade. O AD foi construído não apenas para ser inteiramente compatível com DNS, mas também para fazer com que os dois não possam ficar separados. Caso o DNS não estiver funcionando, o AD também não funcionará.

Além da necessidade da interação com servidor DNS, se fez uma configuração automática do endereço IP, para facilitar e evitar problemas de conflito de IP. Numa rede de Arquitetura TCP/IP, todo computador deve possuir um endereço IP distinto. O DHCP (*Dynamic Host Configuration Protocol)* é o protocolo que provê um meio para alocar estes endereços dinamicamente.

Conforme (Araújo, 1997), para o perfeito funcionamento de um computador ligado a uma rede Internet, não apenas precisa-se configurar o seu endereço IP, mas também uma

série de outros parâmetros de rede. Um cliente DHCP busca encontrar um ou mais servidores DHCP que possam fornecer os parâmetros desejados, para que sua máquina possa ser configurada automaticamente.

Na próxima seção, mostramos a transformação de uma rede modelo *Workgroups* para uma rede modelo domínio a qual, terá uma base de dados centralizada.

3.3 Transformando uma Rede de Modelo *Workgroups* para Modelo Domínio

Nas redes Windows não existe domínio sem o *Active Directory*. Um domínio é criado quando o *Active Directory* é instalado no primeiro servidor. Ao instalar o *Active Directory*, o servidor torna-se um DC (*Domain Controler)*. O DC contém uma cópia da base de dados do *Active Directory*. Na base de dados do *Active Directory* ficam, dentre outras, informações tais como: contas e senhas de todos os usuários, grupos de usuários e membros de cada grupos, contas de computador e assim por diante. Um domínio pode ter vários DCs. Qualquer alteração feita nas informações do *Active Directory*, em qualquer um dos DCs será replicada, automaticamente, para todos os demais DCs do domínio. O resultado prático é que todos os DCs possuem uma cópia idêntica do AD. Em um domínio baseado no *Active Directory* e no Windows Server 2003 é possível ter dois tipos de servidores Windows Server 2003.

Quando os servidores Windows Server 2003 são configurados para trabalhar com *Workgroups*, não existe o conceito de domínio e nem de Controlador de Domínio. Cada servidor mantém uma lista separada para contas de usuários, grupos e políticas de segurança, conforme descrito anteriormente. Com isso se um usuário precisa acessar recursos em três servidores, por exemplo, será necessário criar uma conta para esse usuário nos três servidores diferentes. Uma rede *Workgroups* somente é recomendada para redes extremamente pequenas, não mais do que 10 estações clientes.

Em uma rede baseada no modelo de *Workgroups* cada servidor é independente do outro. Em outras palavras, os servidores do *Workgroups* não compartilham uma lista de usuários, grupos e outras informações. Cada servidor tem a sua própria lista de usuários e grupos, conforme mostrado na Figura 3.7.

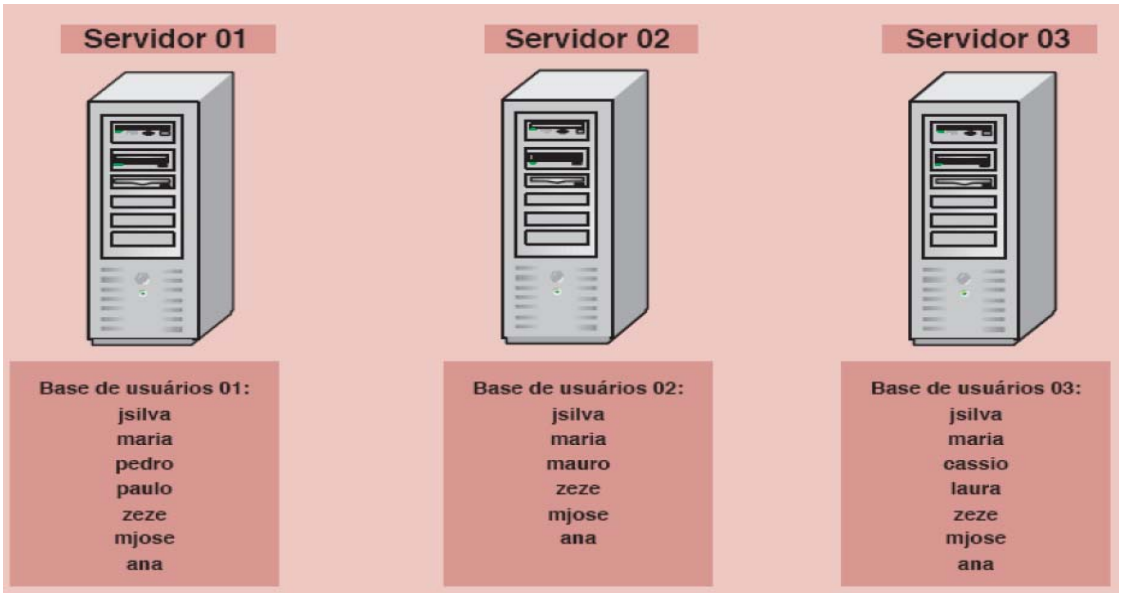

Figura 3-7Exemplo de uma rede baseada no modelo Workgroups. (Fonte : Julio Battisti, 2002).

Nesta rede temos três servidores (ver figura 3.7), onde cada servidor tem a sua própria base de usuários, senhas e grupos. Conforme pode ser visto na figura 3.7, as bases não estão sincronizadas, existem contas de usuários que foram criadas em um servidor, mas não foram criadas nos demais. Por exemplo, a conta Paulo somente existe no Servidor 01, a conta *Mauro* só existe no Servidor 02 e a conta *Cassia* só existe no servidor 03. Logo, se os três funcionários precisassem utilizar os três servidores, teriam que ter uma senha para cada servidor. Agora imagine o problema em uma rede de grandes proporções, com dezenas de servidores e milhares de funcionários. Fica fácil concluir que o modelo de *Workgroups* ficaria insustentável, impossível de ser implementado na prática, para redes de média a grande porte.

Agora mostraremos uma rede de modelo Domínio. Vamos iniciar considerando a figura 3.8 a seguir:

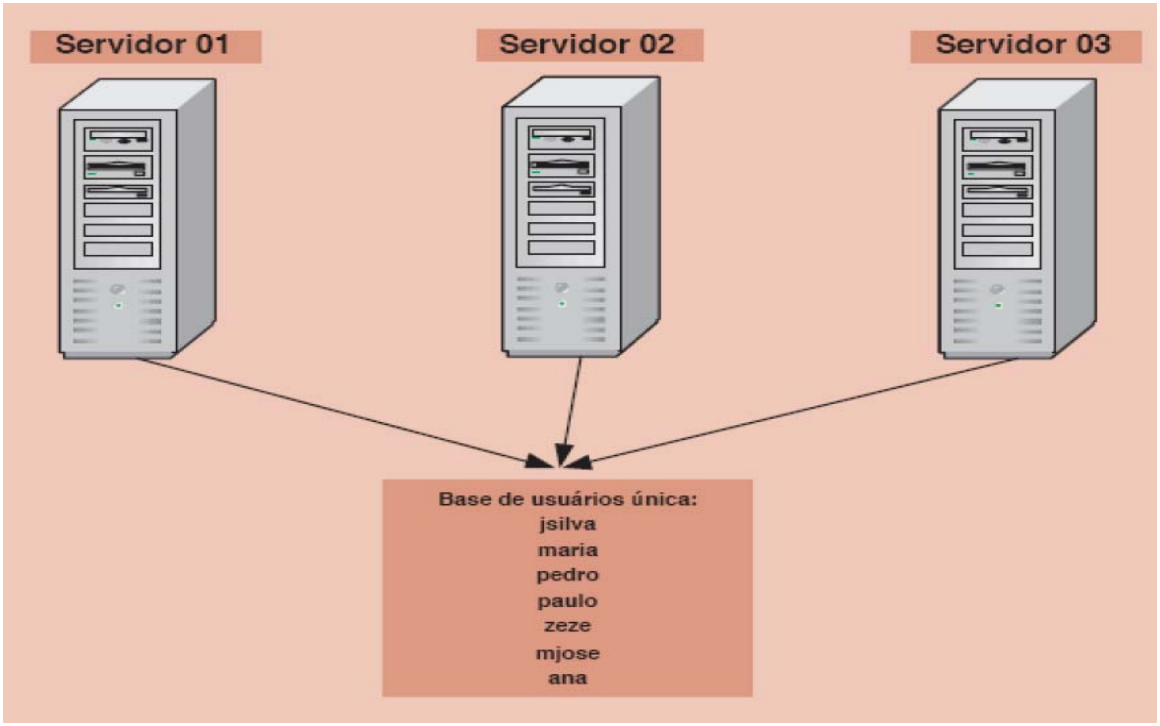

Figura 3-8Uma rede baseada no conceito de Diretório - Domínio. (Fonte: Julio Battisti, 2002)

No modelo baseado em diretório, temos uma base de usuários única, ou seja, todos os servidores da rede compartilham a mesma base de usuários. O que ocorre na prática, é que todos os servidores contêm uma cópia da base de informações do diretório. Alterações efetuadas em um dos servidores são repassadas para os demais servidores da rede, para que todos fiquem com uma cópia idêntica da base de dados do diretório. Esta sincronização entre os servidores do domínio é conhecida como Replicação do *Active Directory*.

3.4 Autenticação no AD

A autenticação é crucial para a comunicação segura. Os usuários devem comprovar suas identidades para as pessoas com quem se comunicam e verificar a identidade de outras pessoas. É difícil a comprovação de identidade em uma rede, pois as pessoas não se encontram fisicamente durante a comunicação, permitindo que um usuário mal-intencionado intercepte mensagens ou se faça passar por outra pessoa física ou jurídica.

O certificado digital é uma credencial comum que permite a verificação da identidade. Os certificados usam técnicas de criptografia para solucionar a falta de contato físico entre as partes em comunicação. O uso dessas técnicas diminui a possibilidade de uma pessoa mal-intencionada interceptar, alterar ou falsificar mensagens. Essas técnicas de criptografia dificultam a adulteração de certificados. Isso impede que uma entidade obtenha a identidade de outra pessoa.

Segundo (Melber, 2005), para uma boa administração de uma rede, a maioria dos administradores querem saber quem está utilizando o sistema, a que computador, quais recursos os usuários tem acesso, entre vários outros recursos da rede. Porém, não necessariamente qualquer usuário pode utilizar o sistema desta rede, apenas usuários autenticados no domínio terão o privilegio de *logar* no domínio desejado. Quando o usuário coloca seu *login* e sua senha, o *Active Directory* (controlador de domínio) verifica se o usuário tem permissões de acesso ao domínio pretendido. Com a autenticação de usuários, o AD torna essa rede mais segura e limitada à entrada de usuários não autenticados.

A seguir serão mostrados os benefícios de se trabalhar com usuários cadastrados em grupo, criando políticas por grupo e não para usuários individuais, assim, facilitando a administração da rede para o administrador.

3.5 Criando Grupos de Usuários e definindo diretivas por grupos.

Um grupo é um conjunto de contas de usuários e computadores, contatos e outros grupos que podem ser gerenciados como uma unidade. Os usuários e os computadores que pertencem a um grupo específico são chamados de membros do grupo. Os grupos são caracterizados pelo escopo e pelo tipo. O escopo de um grupo determina a extensão à qual o grupo é aplicado no domínio ou na floresta.

As configurações de Diretivas de Grupo definem os vários componentes do ambiente da área de trabalho do usuário que o administrador do sistema precisa gerenciar. Por exemplo, os programas que estão disponíveis para usuários, os programas que aparecem na área de trabalho do usuário e as opções do menu Iniciar. As configurações de Diretiva de Grupo especificadas estão contidas em um objeto de Diretiva de Grupo que, por sua vez, está associado aos objetos selecionados do *Active Directory*, como sites, domínios ou unidades organizacionais.

Usar grupos pode simplificar a administração ao atribuir um conjunto comum de permissões e direitos a várias contas simultaneamente, em vez de atribuir as permissões e os direitos a cada conta individualmente. Dessa forma pode simplificar a administração, atribuindo permissões sobre um recurso compartilhado a um grupo e não a usuários individuais. Isso atribui o mesmo acesso ao recurso compartilhado a todos os membros do grupo.

Segundo (Tulloch, 2005), o usuário é cadastrado em grupo ou grupos pelo administrador do domínio conforme necessidade de seu perfil, porém, este usuário pode a vir necessitar de algumas permissões especiais além das fornecidas pelo administrador. Por exemplo, conforme mostra figura 3.9 somente os usuários Bob Smith, Mary Jones, e Tom Lee receberem a política em execução, primeiramente são usados usuários e computadores do *Active Directory* para criar um grupo global chamado Sênior Venda e usuários introduzindo no mercado que tem somente estes três usuários como membros. Esses usuários terão algumas permissões especiais, além das que possuíam até mesmo um controle total do grupo.

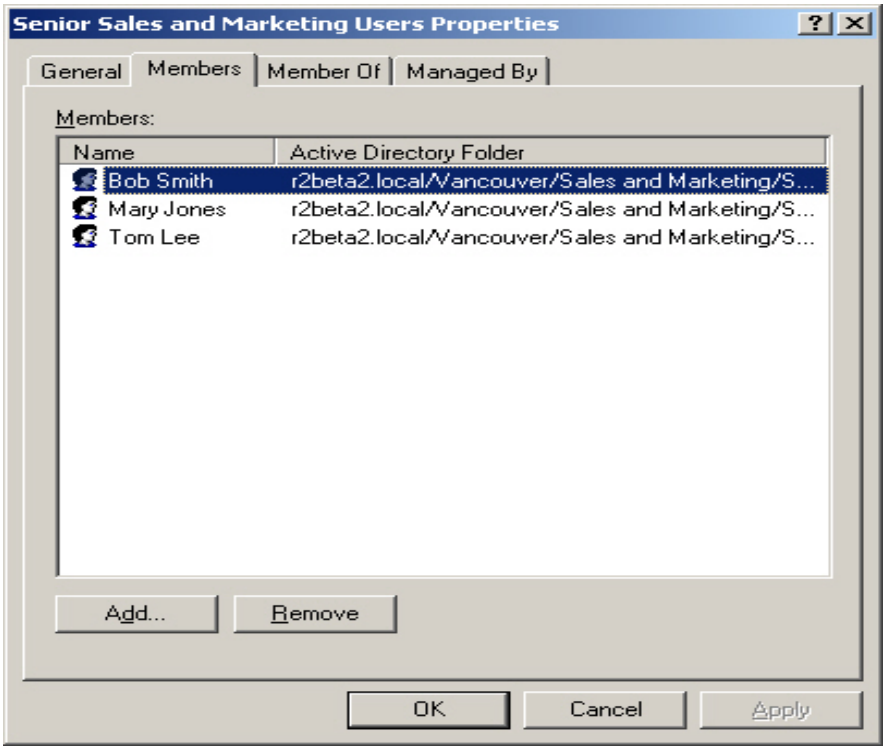

Figura 3-9Criando permissões especiais a usuário. (Fonte: Tulloch, 2005)

Conforme (Tulloch, 2005) um usuário pode ter permissões de grupo a ele concedido pelo administrador e além dessas permissões, o administrador pode dar a este usuário permissões especiais diretamente a sua conta, podendo também cadastrar em vários outros grupos.

Na figura 3.10**,** é apresentada uma ilustração do conceito de grupo de usuários. O grupo Contabilidade possui direito para um recurso compartilhado, o qual pode ser acessado através da rede. Todos os usuários que pertencem ao grupo Contabilidade, também possuem permissão para acessar o recurso compartilhado, com os mesmos níveis de acesso do grupo Contabilidade, uma vez que os usuários de um grupo, herdam as permissões do grupo.

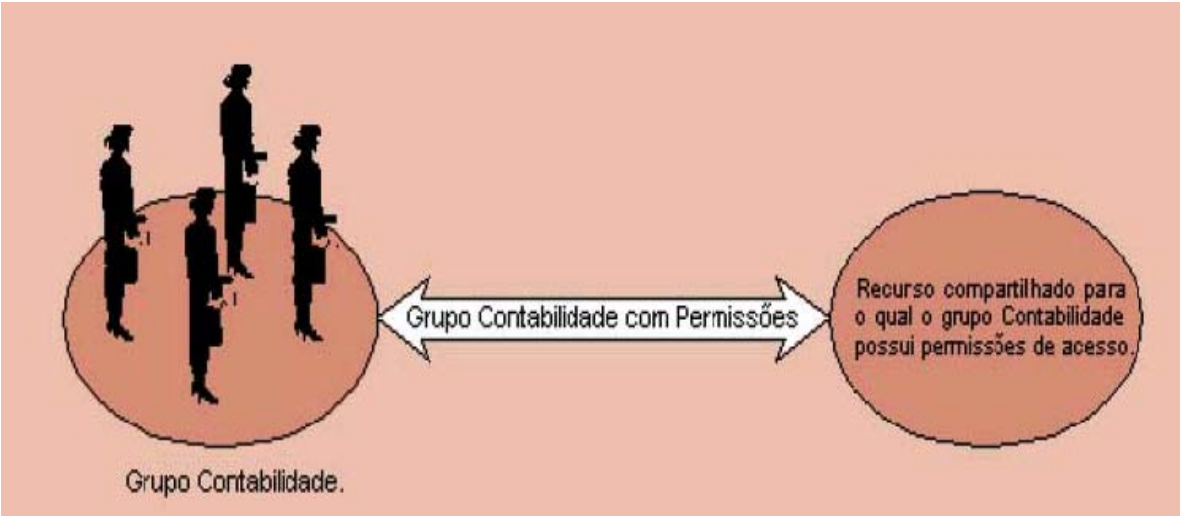

Figura 3-10 O usuário herda as permissões do grupo. (Fonte: Julio Battisti)

Para os grupos de usuários, podemos considerar alguns fatos a seguir:

- Grupos são coleções de contas de usuários.
- Os membros de um grupo herdam as permissões atribuídas ao grupo.
- Os usuários podem ser membros de vários grupos.
- Grupos podem ser membros de outros grupos.
- Contas de computadores podem se membros de um grupo.

A Diretiva de Grupo se aplica não apenas a usuários e computadores clientes, mas também a servidores membros, a controladores de domínio e a qualquer computador com o que esteja contido no domínio, dentro do escopo de gerenciamento.

Por padrão, a Diretiva de Grupo é aplicada a um domínio, ou seja, é aplicada no nível do domínio logo acima da raiz de Usuários e Computadores do *Active Directory*, o que afeta todos os computadores e usuários no domínio.

A Diretiva de Grupo inclui as configurações de diretiva para Configuração do usuário X, as quais afetam os usuários, e a configuração do computador X. Dessa forma, podemos colocar a diretiva por computador ou por usuário, isso dependerá também da

hierarquia de prioridade, conforme a política que adotaremos segundo cada departamento ou organização da empresa. Se colocarmos uma diretiva por computador e esta estiver em primeiro plano, no topo da diretiva adotada para aquele domínio, então todos os usuários seguirão a política adotada para este computador, seguindo assim as normas imposta pelo administrador deste domínio.

As diretivas por grupos facilitam o gerenciamento do administrador da rede. Um exemplo poderia ser a chegada de um novo funcionário, ao invés de colocar políticas para este usuário, basta analisar o que ele precisa ter acesso e colocá-lo em um determinado grupo ou grupos. Assim, conforme a necessidade deste usuário, ou mesmo uma promoção de um funcionário, podendo colocar e tirar acessos apenas sendo cadastrado nos grupos de diretivas.

Conforme (Tulloch, 2005), a política de grupo é muito importante e seria indispensável à criação de um projeto no *Active Directory* com um planejamento de diretiva de grupos. Caso os locais, domínios e OUs sejam criados de maneira errada, a política OU do grupo será difícil de se usar e de localizar problemas. Assim, a primeira etapa durante o planejamento, é criar regras para a política do grupo na rede, planejando como executar o próprio *Active Directory*. Tal planejamento inclui decisões como: Quantas florestas serão abertas (uma ou diversas)? Quantas árvores do domínio? Haverá quantos domínios filho? Que tipo de estrutura de cada domínio tem? E assim por diante. Cada uma destas OU de decisões deve sempre ser feita fazendo a pergunta: Que impacto sofrerá minhas decisões? Como a política do grupo será executada em minha empresa? Fazendo sempre essas perguntas, podendo assim gerenciar melhor as diretivas e grupos, evitando erros futuros e facilitando o gerenciamento do administrador da rede.

Computadores e Usuários são os únicos tipos de objetos do *Active Directory* que recebem a diretiva. Especificamente, a diretiva não se aplica a grupos de segurança. Em vez disso, por motivos de desempenho, os grupos de segurança são usados para filtrar a diretiva através de uma entrada de controle de acesso ACE (*Access Control Entries*) Aplicar Diretiva de Grupo, que pode ser definida como Permitir ou Negar, ou não ser configurada.

Em se tratando de diretivas, é necessário saber se um usuário pode ter acesso a qualquer computador deste domínio. Um usuário pode *logar* em qualquer computador dentro de um domínio, porém, se este computador estiver utilizando uma diretiva de computador para autenticação, apenas usuários locais têm acesso a estes computadores. Contudo, a diretiva de computador sobrepõe a diretiva de usuário.

Na próxima seção, será mostrado o compartilhamento de pastas por grupos, apenas usuários cadastrados no grupo, terão permissões de acesso às pastas compartilhadas pelo grupo.

3.6 Pastas Compartilhadas

As pastas compartilhadas são usadas para listar os recursos compartilhados disponíveis no computador. Em alguns casos, uma conexão à uma impressora é monitorada como uma conexão. Os recursos compartilhados podem ser uma pasta compartilhada, uma impressora compartilhada ou um recurso de tipo não reconhecido.

Um recurso compartilhado fornece acesso para aplicativos, informações ou dados pessoais de um usuário. O administrador pode conceder ou negar permissões para cada recurso compartilhado. Através de diversos métodos a atribuição de permissões a grupos simplifica o gerenciamento dos recursos compartilhados, com isso o administrador pode adicionar ou remover usuários nos grupos sem precisar retribuir as permissões.

Cada usuário poderá ter uma pasta para armazenar seus arquivos, sendo essa pasta uma pasta privada, e dependendo, esta mesma terá uma cota. Pode ser criada uma ou várias pastas compartilhadas, onde todos usuários deste domínio poderão ter acesso de leitura, controle total ou alteração, conforme política adotada pelo administrador da rede, ou apenas usuários de determinado grupo poderão ter acesso à determinada pasta.

Apresentamos nesse capítulo a principal ferramenta do Windows Server 2003. A ligação do DNS ao domínio do AD, onde o DNS tem o mesmo nome do Domínio. As

camadas de estrutura lógicas, que é à maneira de como o AD é apresentado aos usuários e administradores. A transformação de uma rede *Workgroups* para uma rede Domínio, na qual o AD só reconhece uma rede domínio. A importância da autenticação de usuários no domínio que, aumenta a segurança da rede.

Na próxima seção será mostrada a utilização do protocolo LDAP no AD, os serviços que o protocolo LDAP fornece ao AD, a interação entre o sistema operacional Windows Server 2003 e Linux, tendo assim um maior número de usuários e uma maior utilização de softwares livres.

4 . UTILIZAÇÃO DO PROTOCOLO LDAP NO ACTIVE DIRECTORY

Como está implícito em seu nome, o LDAP foi desenvolvido como um método eficaz para o acesso a serviços de diretório sem a complexidade de outros protocolos de serviços de diretório. O LDAP define as operações que podem ser executadas para consultar e modificar informações em um diretório e a forma como as informações em um diretório podem ser acessadas com segurança. Ele pode ser usado para localizar ou enumerar objetos de diretório e para consultar ou administrar o *Active Directory*.

Os clientes do *Active Directory* têm que se comunicar com computadores de domínio ao se conectarem à rede e ao procurarem recursos compartilhados. O acesso a controladores de domínio e catálogos globais é realizado com o protocolo de acesso a pastas (LDAP).

O protocolo LDAP define a forma como um cliente de diretório pode acessar um servidor de diretório e a forma como o cliente pode executar as operações de diretório e compartilhar dados de diretório.

4.1 Suporte do LDAP ao AD

O LDAP é um padrão aberto da Internet, ao utilizá-lo, o *Active Directory* permite a interoperabilidade com serviços de diretório de outros fornecedores. O suporte do *Active Directory* ao LDAP inclui um objeto de provedor LDAP como parte do recurso ADSI (*Active Directory* Service *Interfaces)*. O ADSI oferece suporte a interfaces de programação de aplicativos vinculadas à linguagem C para LDAP. Outros aplicativos de serviços de diretório podem ser facilmente modificados para acessarem informações no *Active Directory* usando ADSI e LDAP.

4.2 Autenticando um usuário Linux no Windows Server 2003

Segundo (Del, 2002) A autenticação LDAP é baseada em suportar os sistemas operacionais mais recentes da Microsoft, incluindo o Windows Professional 2000 e o Windows XP, e suporta também o sistema operacional Linux e outros sistemas Unix. Em qualquer um dos sistemas operacionais citados, faz-se um *logon* utilizando o *Active Directory*, porém, pode haver algumas limitações. Primeiramente, os clientes Microsoft nos Windows Professional 2000 e XP são específicos à autenticação, tendo um acesso a todos recursos a ele permitido fornecido pelo administrador do *Active Directory*.

O sistema operacional Linux implanta o serviço de diretório usando o LDAP, sendo conhecido como o *OpenLDAP*. Embora o *OpenLDAP* use o mesmo protocolo de LDAP, há outras características do *Active Directory* que o *OpenLDAP* não possui. Em geral, os clientes do *Active Directory* não necessariamente autenticam em uma máquina servidora utilizando o *OpenLDAP*. Mas, um cliente utilizando um sistema operacional Linux pode autenticar, configurar um domínio para que faça parte do "grupo".

Para (Henderson, 2004), o planejamento de integrar uma estação de trabalho Linux (usuário) a uma rede de Windows (servidor), um dos fatores que deveríamos nos preocupar é a autenticação e o encontro ao DNS (*domain name server*) do Windows. Isto é, fazer com que uma máquina Linux (usuário), possa ser configurada no domínio do *Active Directory* (Windows Server).

Qualquer Programa ou Sistema habilitado ao padrão LDAP, será capaz de acessar as informações do AD, ou seja, com o uso deste padrão é possível desenvolver sistemas integrado ao AD. Contudo, podemos concluir que, a utilização do SO Linux (cliente) em um servidor Windows só se concretiza mediante os dois SOs trabalharem com o mesmo protocolo, o protocolo LDAP por padrão.

Neste capítulo observamos o que o protocolo LDAP é o principal protocolo para o AD e seus serviços para o AD. A interação dos dois sistemas operacionais, mediante os dois SO trabalharem com o mesmo padrão que é o protocolo LDAP.

No próximo capítulo apresentamos como o AD possibilita implantar alguns serviços através das operações práticas na UFLA, como o *labinst.ufla.br* e o *drca.ufla.br*.

5 APLICAÇÕES PRÁTICAS

5.1 Objetivo

Neste trabalho, centralizaremos a administração da rede utilizando a principal ferramenta do Windows Server 2003, o *Active Directory*, para gerenciar todo os computadores deste domínio. Faremos uma comunicação entre diferentes sistemas operacionais utilizando *Active Directory*, em um servidor (Windows Server 2003) para usuários Linux.

5.2 Descrição do problema

Devido a grande dificuldade que se tem de trabalhar com a base de dados de usuários descentralizada e por reconhecer que é indispensável um melhor gerenciamento dos recursos da rede para os usuários, vislumbramos a solução de administrar a rede por meio do AD. Será feita uma instalação do SO Windows Server 2003 em um computador, sendo este computador um controlador de domínio (*Active Directory*), transformando assim uma rede de modelo *Workgroups* para uma rede de modelo domínio.

A implantação do AD irá permitir a interação entre os sistemas operacionais Linux e Windows, permitindo um número maior de usuários trabalharem no mesmo domínio, além da maior disseminação de softwares livres.

5.3 Instalação do AD

Em um servidor, foi instalado o Sistema Operacional Windows Server 2003. Antes de colocar o servidor em rede, foi instalado o antivírus *Norton Corporate (Symantec),* como servidor para dar suporte a todas as máquinas ligadas a seu domínio.

Foram feitas todas as atualizações do sistema operacional pelo Windows *update*. Com o término das atualizações, começou-se a utilizar a gerenciamento de serviço do Server 2003, onde se encontram várias ferramentas de servidor do SO. Iniciou-se pelo DHCP, e para que o servidor também funcionasse como servidor de DHCP, foi feita a instalação de duas placas de rede, uma para WAN e outra como LAN, funcionando como roteador.

Após a configuração dos computadores do laboratório para utilização de IP automático, empregando o mesmo servidor, foi feito um acesso remoto a um outro servidor do Campus da UFLA, um servidor de DNS, criando assim, um novo DNS, que por sua vez esse DNS será o domínio, nó raiz de uma nova árvore, indispensável à criação de DNS no servidor. Sem a instalação do DNS seria impossível utilizar os serviços do *Active Directory*. Na verdade o *Active Directory* nada mais é que um controlador de domínio.

Em seguida configuramos a principal ferramenta dos servidores, o *Active Directory*. Ao criarmos um domínio no AD, uma substituição ao Windows *Workgroups*, os computadores com os sistemas operacionais Windows 95, Windows 98 e Windows NT não poderão mais se conectar ao AD do Windows Server 2003. Esses sistemas operacionais que reconhecem apenas rede às de modelo *Workgroups*, logo, para utilizar uma rede de modelo domínio, precisam aderir normas para acesso ao domínio.

Esses sistemas operacionais mais antigos não dão suporte a instalação de um domínio, como podemos ver na figura 5.1. A Microsoft não oferece nenhum software que o faça suportá-lo; assim, simplesmente esses clientes não terão mais acesso. O Windows 98 pode acrescentar essa funcionalidade por meio de pequeno software cliente (*Active Directory Client* for Windows 98), portanto precisamos acrescentá-lo antes que qualquer sistema Windows 98 comunique-se com um domínio AD baseado no Server 2003.

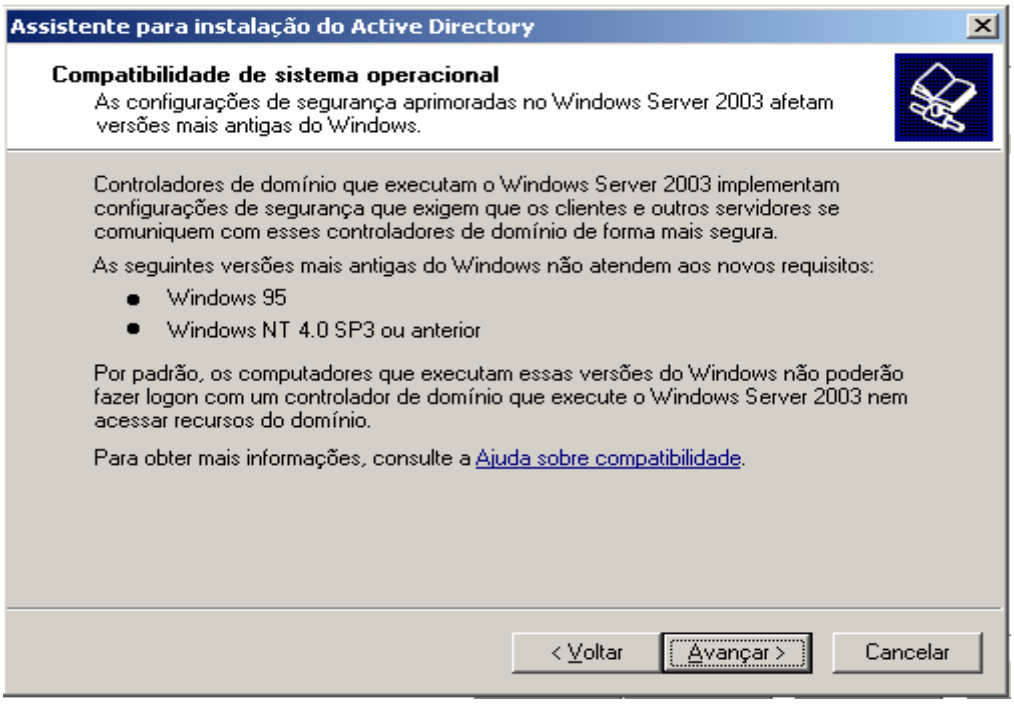

Figura 5-1 Compatibilidade de sistema operacional. (Fonte: instalação do AD no servidor)

Conforme (Anderson et al, 2002) é recomendável minimizar o número de domínio ao máximo, se possível apenas para um só domínio. Os domínios do *Active Directory* podem ser enormes, capazes de conter milhões de objetos, grandes o suficiente para a maior parte das empresas. A utilização de mais de um domínio por servidor, sobrecarrega a memória e a CPU. Além disso, ter muitos domínios por servidor significa ter muito tráfego na LAN, já que eles se mantêm atualizados quanto às alterações no AD.

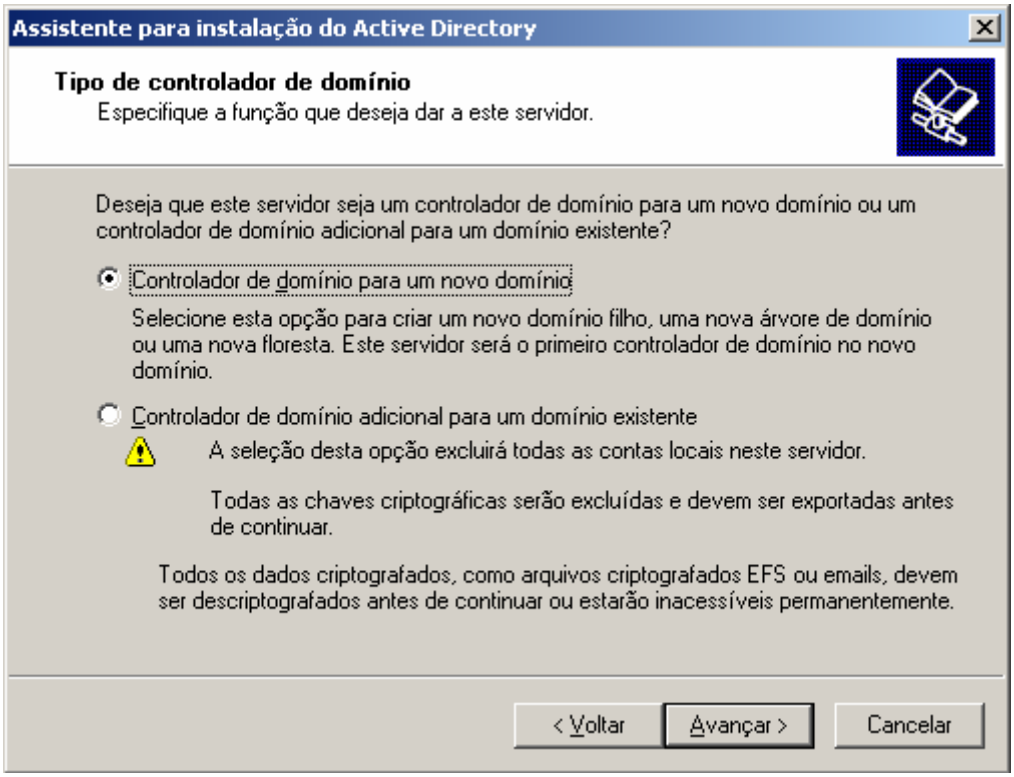

Figura 5-2 Controlador de domínio. (Fonte : instalação do AD no servidor)

No Laboratório Institucional e no departamento DRCA foi criado somente um domínio por servidor, o nó raiz, onde somente ele é a raiz, conforme mostrado na figura 5.2. Com apenas um domínio, ele é chamado de árvore. A segunda opção desta figura 5.2, domínio filho de uma árvore existente, precisa de um domínio raiz existente, um DNS controlador de domínio, criando-se, assim, um filho para este domínio. A partir do momento que é criado uma nova árvore e já existe um nó raiz chamado *ufla.br*, cria-se um outro nó chamado *dcc.ufla.br*. Esta árvore passa a ter uma relação de confiança, funciona como uma hierarquia, uma relação de pai para filho. Em nosso trabalho, foi criado apenas um domínio, conforme políticas adotadas pelo administrador da rede, mais vale lembrar que, podemos criar novos domínios, ou até mesmo uma floresta.

Após o término da instalação do *Active Directory*, utilizamos uma interface do AD para toda a administração dos usuários e computadores.

Ao cadastrar o usuário no *Active Directory*, a configuração da máquina cliente deve ser alterada do modelo *Workgroups* para o modelo de rede domínio. No entanto, algumas empresas utilizam um SO modificado para automatizar a conversão de *Workgroups* para domínio.

Após a troca de *Workgroups* para domínio, faz-se um *logoff* e ao fazer novamente um *login*, terá uma opção de domínio: máquina local ou domínio desejado, caso o administrador não tenha tirado a opção máquina local. Assim, o usuário entrará com sua senha e seu *login*, sendo que este usuário autenticado no domínio.

Muitas empresas, que utilizam o AD, adotam políticas onde apenas administradores podem instalar programas. Entretanto, usuários podem instalar programas apenas os que estão em sua área de trabalho, eles ficam em modo de espera, conforme necessidade do usuário instala ou não o programa.

O AD reconhece apenas programas do tipo MSI (*Microsft Sistem Installer*), que é uma extensão da Microsoft para instalações de programas para usuários do domínio, onde muitos programas fornecem uma instalação desses pacotes MSI. Porém, nem todos são fornecidos neste formato e devemos utilizar um software chamado *Veritas* que faz essa conversão. Por exemplo, um programa lanking.exe, é convertido para *lanking.msi*, sendo este programa *lanking.msi* reconhecido pelo AD. Neste programa cria-se um pacote de instalação que instala todos os programas solicitados pelo administrador do domínio.

5.3.1Exemplos de aplicação 1: DRCA

A primeira aplicação prática realizada foi no departamento do DRCA. Conforme a necessidade de compartilhamento e segurança no departamento DRCA, foi instalado o AD. Após a instalação do AD foi feito a troca dos computadores (cliente) de modelo *Workgroups* para um modelo de domínio. Entretanto, foi visto que, nem todos Sistemas Operacionais existentes no departamento não eram passíveis de realizar a troca de

Workgroups para domínio. Havia computadores utilizando o Sistema Operacional Win98 e outros utilizando WinXP. Segundo técnicos da Microsoft, pode-se baixar no *site www.microsoft.com*, um programa para transformar uma rede *Workgroups* para domínio, porém, a Microsoft forneceu esse serviço até o dia 11/07/2006 sendo descontínuo após esta data. Conforme política adotada pelos administradores do DRCA, só serão utilizado sistemas operacionais WinXP, no departamento DRCA.

Após todos os computadores (clientes) estarem configurado no domínio *drca.ufla.b*r, foram criados novos usuários, como por exemplo, funcionários do departamento DRCA, caracterizados por um *login*, como sobrenome e uma senha qualquer. Adota-se uma política, em que o usuário, ao *logar* pela primeira vez no domínio DRCA, deve criar uma nova senha com 8 dígitos e alfanumérica, com letras maiúsculas e minúsculas, aumentando o nível de segurança.

No DRCA, foi criada uma pasta particular onde este usuário (cliente) terá uma quota para que possa armazenar dados, arquivos pessoais, mas somente ele terá acesso a esta pasta. Já com a criação de uma outra pasta pública, todos os usuários deste domínio, *drca.ufla.br*, poderão armazenar dados e informações que sejam úteis a todos os usuários do grupo *drca.ufla.br*, facilitando a troca de informações. Um backup desta pasta pública é realizado diariamente, segundo política adotada pelo DRCA.

Notamos com a utilização do AD no DRCA, aumentamos a segurança do departamento, onde para utilizar o sistema tem que ser cadastrado no domínio, além da facilidade de compartilhamento entre os usuários do *drca.ufla.br*.

Mostraremos agora uma outra implantação em que o AD possibilitou na instituição UFLA, que é o Laboratório Institucional.

5.3.2Exemplo de aplicação 2: Laboratório Institucional

A segunda aplicação foi no Laboratório Institucional (*labinst.ufla.br).* Foi feita a instalação do AD no Pavilhão II, com cerca de 110 computadores e todos ligado no domínio *labinst.ufla.br*. Com a instalação do AD no *labinst.ufla.br*, adotamos políticas neste domínio para o uso dos alunos, onde cada aluno terá o seu *login* e sua senha para autenticação nos computadores. A instalação dos programas foi realizada usando-se pacotes MSI (*Microsft Sistem Installer*). A instalação desses pacotes MSI pode ser realizada apenas no *logon* do usuário na máquina, ou mesmo, ficar na área de trabalho para o usuário, caso este usuário venha a precisar.

Após instalarmos o AD (*Labinst.ufla.br*), foi criado usuários, porém, não colocamos em prática o cadastro de todos os alunos, colocamos uma senha e um *login* para cada computador, que ficam armazenadas no próprio computador. Entretanto, para o uso deste laboratório é necessário à apresentação de identificação para um funcionário da UFLA no Laboratório Institucional, não é a melhor maneira, mas foi a política adotada. Para isso seria preciso cadastrar todos os alunos, um processo mais lento, porém, mais eficiente.

Após uma solução temporária para a autenticação de alunos, será a preparação de diretivas de grupo por computadores ou usuários, como as instalações de programas para usuários do domínio *labinst.ufla.br*. Foram instalados programas que tinham pacotes prontos MSI e outros foram produzidos com o programa *Veritas,* transformando os softwares a serem instalados em MSI. Este pacote foi criado conforme necessidade do departamento e conforme a necessidade dos usuários deste domínio.

Foram instalados softwares utilizando política de grupo, após o usuário *logar* neste computador, aparecerá o ícone de instalação na barra de ferramentas, como se ficasse em espera, por exemplo, *Word, Excel, Power Point* e caso o usuário necessite utilizá-lo, clica a primeira vez no programa, que será instalado. Foi também instalado programas por diretiva de computador, sendo este computador desligado e ligado pela primeira vez após a ativação no AD de instalação, este programa será instalado automaticamente antes que o usuário venha a fazer *logon* neste computador.

Após a instalação de programas para os usuários, o sistema está pronto para ser administrado, permitindo acesso ou negando acesso ao usuário de seu computador ligado ao domínio. A política adotada pelo administrador em relação à diretiva do grupo do *labinst.ufla.br.*

Foram impressas todas as partes de diretivas de computador e de diretiva de usuário, totalizando mais de 100 páginas de diretivas. Poderão ser adotadas políticas de usuário ou mesmo de computador. Se colocarmos uma política de computador, apenas usuários deste domínio poderão *logar*, Por outro lado, se criarmos uma hierarquia de primeira ordem para computador, somente usuário o local terá acesso, um usuário global não terá como *logar* neste computador. Todas as diretivas são analisadas para uma melhor administração da rede, conforme necessidade do grupo de usuários.

Ao utilizarmos o AD no Laboratório Institucional, notamos um melhor gerenciamento dos usuários ao trabalhar com uma base de dados centralizada, maior facilidade na instalação de programas e um melhor gerenciamento dos recursos dos usuários, restringindo as permissões do usuário e permitindo apenas o essencial para uma utilização do sistema, conforme o perfil do usuário.

6 . CONCLUSÃO

Cada dia que passa aumenta a necessidade de uma rede mais segura e um melhor gerenciamento para os usuários de uma rede. Entretanto, com o aumento no tamanho das redes e as constantes mudanças pelas quais as redes passam, os usuários passaram a necessitar de um serviço que permitisse um acesso transparente aos recursos da rede. Com isso surge a necessidade de se trabalhar com uma base de dados centralizados, para um melhor gerenciamento de computadores e usuários.

Neste trabalho, mostramos os principais benefícios do serviço de modelo de rede domínio (*Active Directory),* permitindo um gerenciamento mais transparente das relações entre os recursos de rede distribuídos. Este é um fator de grande importância para as organizações, proporcionando maior segurança, redução de custos e melhorando a funcionalidade desejada. Dessa forma, o AD gera um único espaço para o gerenciamento dos usuários de gerenciamento, grupos e recursos de rede, bem como distribuir software e administrar configurações da área de trabalho.

Ao utilizarmos o AD, passou a ser obrigatório um *login* e uma senha para cada usuário. O AD forneceu serviços de segurança forte e consistente que são essenciais às redes incorporadas. Como o gerenciamento de autenticação de usuário e controle de acesso é, geralmente, propensa a erro, o *Active Directory* centralizou a administração e exigiu uma segurança baseada em regras consistentes com os processos empresariais da organização.

Em se tratando de ganho de tempo e maior segurança, a facilidade de cadastramento de usuários por grupo, adotou as permissões deste grupo. O administrador atribui as permissões ao grupo e não a usuário, como por exemplo, se tivesse uma rede de mais de 1000 usuários e colocar permissão a cada usuário, levaria muito tempo para uma rede de grande porte. Foram definidas políticas para o grupo de usuários, de acordo com o seu perfil. Essas políticas podem ser aplicadas ou removidas para cada grupo de usuários. Na instalação dos programas, onde existe um fácil acesso do usuário aos programas a ele fornecido pela diretiva de grupo, estes programas ficaram na área de trabalho do

computador do usuário. Eles podem ser instalados diretamente pelo administrador do domínio, apenas ligando a máquina na rede.

A interação entre os sistemas operacionais Linux e Windows, permitiu um número maior de usuários trabalhando no mesmo domínio, além da maior disseminação de softwares livres.

7 . TRABALHOS FUTUROS

Conforme aplicações de nosso trabalho, podemos constar que poderão ser realizadas outras tarefas, tais como:

- Criar um novo domínio, onde este domínio será o domínio pai, porém, utilizando outros domínios filhos, para que haja uma relação de confiança entre esses domínios.

- Fazer uma relação de confiança entre departamentos, fazendo com que usuários de locais diferentes possam *logar* em diferentes departamentos com um mesmo *login* e uma senha.

- Criação de UO, na qual será compartilhada a administração da empresa por outros administradores, sendo que o administrador do domínio, repassará a cada novo administrador uma nova tarefa, uma função a administrar.

- Fazer um cadastro dos alunos da Universidade Federal de Lavras no domínio Laboratório Institucional, à medida que esse usuário venha a utilizar o sistema, pois mediante seu cadastro, este usuário passará a ter um *login* e uma senha para utilização do domínio.

8 . REFERÊNCIAS BIBLIOGRÁFICAS

ALLEN, Robbie, PUCKETT, Richard. **Managing Enterprise Active Directory Services.** Disponível em <www.awprofessional.com>, 2002. Acessado em 19/ jan/ 2007

ARAUJO, Gorgonio. **DHCP: Por que Usar?** Disponível em: Dsponível em Rede Nacional de Ensino e Pesquisa (RNP), <www.rnp.br/newsgen/9705/n1-2.>. Acessado em 12/ fev/ 2007

BIALASKI, Tom. **Directory Server Security**. Disponível em <http://www.sun.com/blueprints>, 2000. Acessado em 11/ jan/ 2007

Del, David. **Active Directory and Linux.** Disponível em <http://www.securityfocus.com/static/submissions.>, 2002 . Acessado em 12/ out/ 2006

HENDERSON, Willian**. Authenticating Linux against Active Directory** Disponível em <www.windowsnetworking.com>, 2004. Acessado em 14/ out/ 2006

JURGENS, Tony**. Tive Directory Delivers Leading LDAP Performance.** Disponível em <http://www.microsoft.com/windows2000>, 2000. Acessado em 12/ nov/ 2006.

MARSHALL, Oliver. **Windows 2003 AD: An Overview**. Disponível em <www.windowsnetwork.com>, 2003. Acessado em 15 /dez /2006

MELBER, Derek. **Windows & Active Directory Auditing**. Disponível em <www.windows security.com>, 2005. Acessado em 24/ set/ 2006

PARAM, Kelvim**. Building a Bridge to the Active Directory.** Disponível em <www.perl.com/pub/a/2001/12/19/xmlrpc.> , 2001. Acessado em 19/ nov/ 2007

PICOTO, Carlos. **Microsoft Active Directory**. Disponível em: <http://www.fbnet.pt/red/0599/a03-01-00> Acesso em: 9/ out/ 2006.

POSSEY, Brien. **Introducing Windows Vista's Active Directory Search Tool.** Disponível em <www.windowsnetworking.com/articles_tutorials>, 2006. Acessado em 20/ nov/ 2006.

POSSEY, Brien. **Making Your DNS Service Fault Tolerant**. Disponível em <www.windowsnetwork.com>, 2005. Acessado em 26/jan/ 2007

SANTANA, Fabio. **AD-Active Directory**. Disponível em <http://www.juliobattisti.com.br>, 2000. Acessado em 2/ fev/ 2007

SCHLEY, Andrew. **Possible LDAP over SSI bug in OS 10, 10.4, 10.5, 10.6.** Disponível em: <http://www.utexas.edu/its/wes/kutz>, 2004. Acessado em 28/ set /2007

SHIMONSKI, R. **Determining the Funtional Level in Windows Server 2003**. Disponível em <www.windows network.com>, 2005. Acessado em 12/ fev/ 2007

SHIMONSKI, Robert**. File System Planning for Active Directory. Disponível em** <windowsnetworking.com/articles_tutorials>, 2005. Acessado em 20/ nov/ 2006

TULLOCH, Mitch**. How to Implement Group Policy Security Filtering**. Disponível em <www.windowsnetworking.com>, 2005. Acessado em 12/ nov/ 2006

TULLOCK, Mitch. **How to Implement Group Policy Security Filtering.** Disponível em <www.windows network.com>, 2005. Acessado em 10/ nov/ 2007

Active Directory and Linux**. Disponível em:** <www.securityfocus.com/infocus/1563 - 46k> Acessado 12/ fev/ 2007.

Active Directory - Wikipedia**, the free encyclopedia.** Disponível em: <www.wikipedia.org/wiki/Active_Directory > Acessado em 13/ out/ 2006

ANDERSON, Christa; MINASI, Mark ;SMITH, Brian; TOOMBS, Doug. **A Bíblia do Windows 2000 server.** São Paulo: Makron Books , 2001

APOSTILA WINDOWS 2000. **Introdução ao Active Directory.** Sao Paulo: 2002, p.1.

Apostila LDAP iniciantes. Disponível em <http://www.ldap.org.br/> Acessado em 1/ jul/ 2006

BRITO, Ivana Campos. **Serviço de diretório.** Salvador: UCS, 2002.

How to Install Active Directory on Windows 2003**. Disponível em:**
<www.petri.co.il/how_to_install_active_directory_on_windows_2003>
Acessado em 11/ out/ 2006

Protocolo LDAP. Disponível em: <http://www.ldap.org.br/> Acessado em 1/ jul/ 2006

SANTOS, Anderson; CAMARA, Fábio. **Implantando o Active Directory.** Florianópolis: Visual Books , 2002.

SENNA, Clovis. **LDAP Um Guia Prático**. Rio de Janeiro: Ciência Moderna, 2005.

SOARES, Luiz Fernando Gomes; LEMOS, Guido; COLCHER, Sérgio. **Redes de computadores.** 2 ed. Rio de Janeiro: Campus, 1995.

THOMPSON, Marco Aurélio. **Windows Server 2003:** Administração de Redes. São Paulo: Érica, 2003.

Windows Server 2003 Active Directory Disponível em:
<www.microsoft.com/windowsserver2003/technologies/directory/activedirectory>
Acessado em 11/ out/ 2006