UNIVERSIDADE CATÓLICA DO SALVADOR
CURSO DE BACHARELADO EM INFORMÁTICA
DISCIPLINA: REDES
PROF.: MARCO ANTÔNIO
ALUNA: IVANA CAMPOS BRITO

SERVIÇO DE DIRETÓRIO

SUMÁRIO

I. O que é um serviço de diretório?

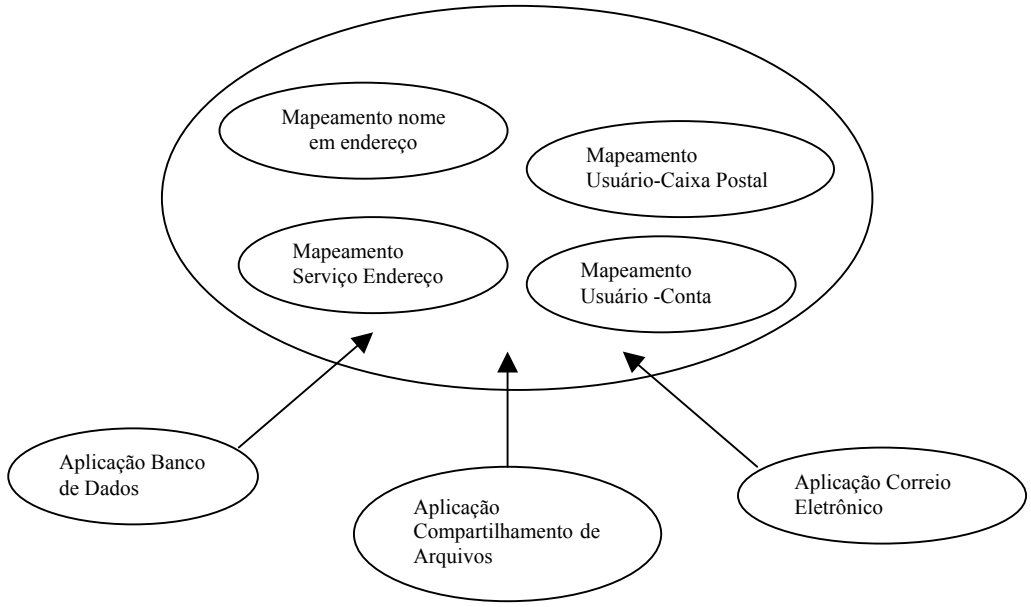
No contexto de uma rede, um diretório é uma estrutura hierárquica que armazena informações a respeito de itens(recursos) de uma rede. Um diretório pode ser composto pelos mais diferentes tipos de itens(objetos), como por exemplo, servidores, discos, impresoras, contas de usuários, arquivos compartilhados; ou ainda domínios de logon, aplicativos, políticas de segurança e de acesso, etc.

Cada item é um objeto e possue uma série de informações(atributos) associados a ele. Por exemplo, os atributos de um determinado objeto usuário podem ser nome, endereço, nome de usuário(login name), senha de acesso e grupos de que faz parte. O conceito de serviço de diretório é um conjunto de funções para criação, armazenamento e recuperação de informações de um diretório.

Diversos aplicativos precisam de informações para funcionar em rede:

- agendas de correio eletrônico: precisam localizar o endereço eletrônico do usuário a partir do nome;
- serviços para cadastro de contas de usuário: precisa localizar as informações de senha a partir do nome do usuário;
- etc.

A existência de múltiplos serviços de diretório cria dificuldades administrativas e incompatibilidade entre as aplicações.



Uma primeira tentativa de criar um serviço de diretório para suprir informações comuns a várias aplicações foi o X500. X500 é um conjunto de padrões definido pelo CCITT(atual ITU).

Características do X500:

- Banco de informações distribuído;
- Mecanismo de procura de informações flexível;
- Espaço de Nomes Homogêneo;
- Serviço padronizado e aberto.

1. Estrutura do X500

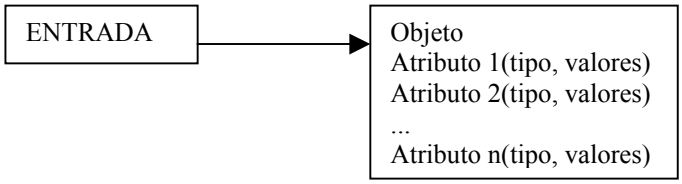
As informações de diretório do X500 estão armazenadas no DIB(Directory Information Base). X.500 é especificado como um serviço da Camada de Aplicação no mundo OSI, porem o seu projeto não depende significativamente das outras camadas OSI, e ele pode ser visto como um projeto de um Serviço de Diretório de propósito geral.

O padrão define o serviço como de acesso a informações sobre entidades do mundo real, porém ele também pode ser utilizado para acessar informações sobre serviços de hardware e software. Cada entrada do diretório aponta para um objeto.

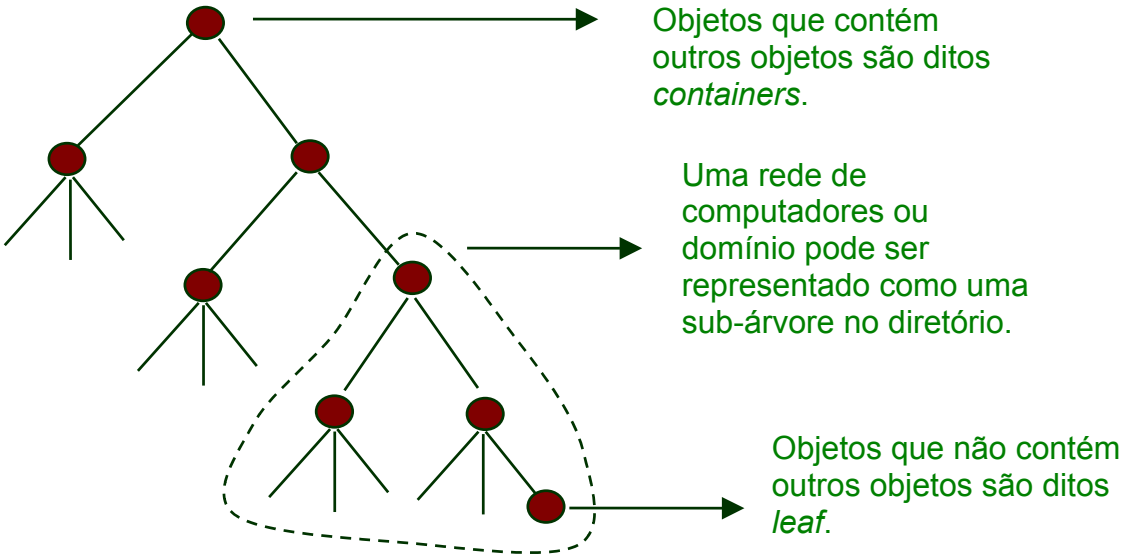
Objeto: Usuário

nome: Ivana
sobrenome: Campos Brito
e-mail: ivanacbrito@hotmail.com

} **Atributos**



Os objetos podem conter outros objetos constituindo uma estrutura hierárquica em forma de árvore.



O padrão X.500 define o Diretório como uma coleção de sistemas abertos que cooperam para manter sua base de dados lógica com informações sobre um conjunto de objetos do mundo real. Os usuários do Diretório, incluindo pessoas e programas, podem ler e modificar as informações, ou parte dela, se tiverem permissão para isto.
São também definidas regras para dar nome a objetos, uma base lógica de informações de Diretório para guardar informações sobre esses objetos e as entidades de protocolo que cooperam para prover o serviço de Diretórios.

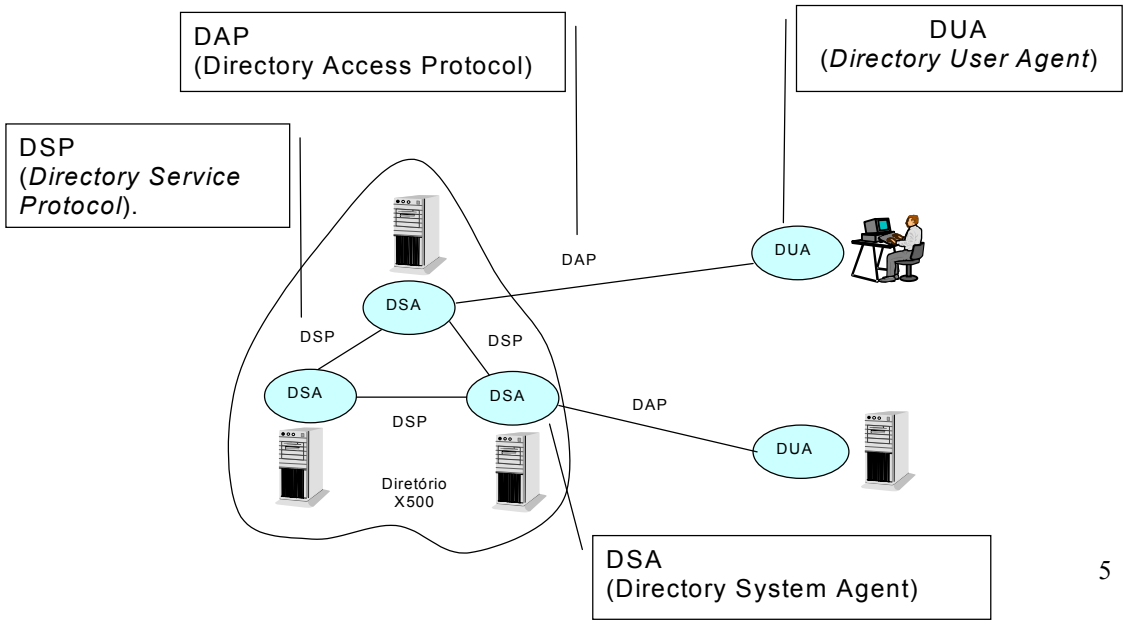
A recomendação X.500 é definida para suportar um diretório amplamente distribuído. Uma maneira de alcançar a distribuição é definir uma rede de processos clientes e servidores. Cada processo pode residir em um computador diferente e os processos se comunicam uns com os outros atraves de protocolos bem definidos. Processos clientes requisitam serviços dos servidores, que fornecem estes serviços.

2. Modelo Funcional X500

- DSP(Directory Service Protocol): protocolo que padroniza a comunicação entre servidores. Essa comunicação ocorre quando uma consulta não pode ser satisfeita pelo servidor local.
- DAP(Directory Access Protocol): protocolo de acesso, que padroniza a comunicação entre o cliente e o servidor de diretório.
- DUA(Directory User Agent): é o nome dado a parte do software do cliente que interage diretamente com o servidor de diretório.
- DSA(Directory Sustem Agent): é a denominação dada a porção do software do servidor responsável por atender as requisições dos clientes.

Um Agente do Usuário de Diretórios atua em benefício de um único usuário de Diretório. Quando uma pessoa ou processo deseja utilizar o Diretório interage com seu DUA. O DUA então desencadeia as ações apropriadas. O Agente de Usuário do Diretório está concentrado no primeiro nível de abstração e trata da maneira pela qual o usuário interage com o Diretório. A natureza desta interação entre os dois componentes foi padronizada, e envolve um conjunto de operações que pode ser executada no Diretório por um usuário do Diretório. Este protocolo é denominado Protocolo de Acesso ao Diretório (DAP).

Um Agente do Sistema de Diretório é um processo de aplicação OSI que é parte do Diretório é cujo papel é fornecer acesso a BID para Agentes de Usuário do Diretório e/ou para outros DSAs. Um DSA pode usar informações armazenadas em seu banco de dados local ou pode interagir com outros DSAs para responder a requisições. Alternativamente, o DSA pode redirecionar o pedido para outros DSA que pode realizar esta requisição. Os bancos de dados locais são inteiramente dependentes de implementação. Este protocolo de comunicação entre DSA é denominado Protocolo de Sistema de Diretório (DSP).



3. LDAP(Lightweight Directory Access Protocol)

Foi criado como uma alternativa mais simples ao protocolo padrão do X500(DAP-Directory Access Protocol).

O LDAP é baseado no modelo cliente-servidor. Um ou mais servidores LDAP contêm as informações. Os clientes LDAP conectam-se com os servidores para obter dados contidos no diretório e os servidores respondem às requisições.

Além de ser um padrão para internet, está sendo adotado por vários fabricantes de sistemas operacionais:

- Novell: LDAP está incluído na arquitetura NDS(Novell Directory Services);
- Microsoft: LDAP está incluído na arquitetura Active Directory do NT 2000;
- Lotus Notes/Domino: Vários produtos da Lotus são compatíveis com LDAP(Lotus Domino 4.6-Lotus Mail, Domino 5.0 e Lotus Notes Client);
- Nestscape Directory Server: Servidor de LDAP que pode ser integrado a sistemas operacionais da rede.

O LDAP define 4 modelos básicos que descrevem por completo a sua operação, que informações podem ser armazenadas em diretórios LDAP e o que pode ser feito com essas
informações. São eles:

Modelo de Informação: define o tipo de informação que pode ser armazenada em um diretório LDAP;

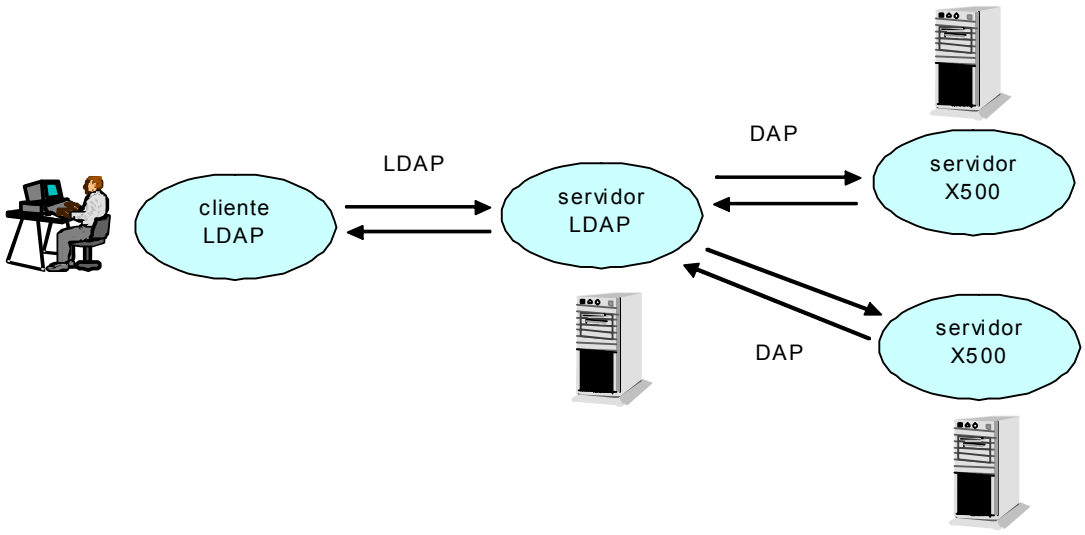
Modelo de Nomes: define como a informação no diretório LDAP pode ser organizada e referenciada;

Modelo Funcional: define o que pode ser feito com a informação no diretório LDAP e como ela pode ser acessada e alterada;

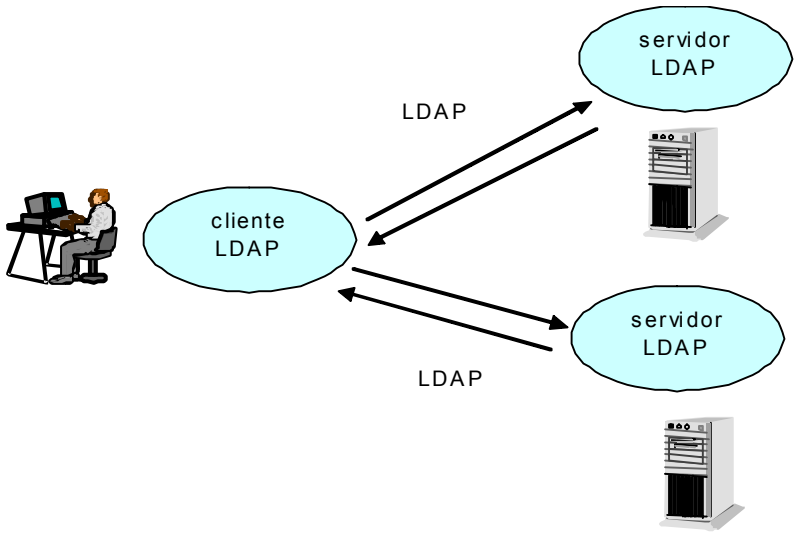
Modelo de Segurança: define como a informação no diretório LDAP pode ser protegida de acessos ou modificações não autorizadas.

O servidor LDAP pode ser de dois tipos:

- Fazer uma ponte com outro servidor de diretório(exemplo X500)



- Ser um servidor stand-alone.



Quando um servidor LDAP não conhece a resposta a uma pergunta do cliente, ele pode indicar um outro servidor LDAP(chamado referral) ou uma lista de servidores LDAP para o cliente consultar.

II. DNS(Domain Name System)

1. Introdução

O Domain Name System (DNS) é um sistema de banco de dados distribuído não genérico usado pelas aplicações Internet, pricipalmente, para conversão de um nome de máquina para seu endereço IP e também usado pelos programas que tratam correio eletrônico para pesquisar a máquina de recebe correio para determinado domínio. Antes de uma aplicação Internet, tais como um browser WWW ou um cliente FTP, abrir uma conexão com a máquina remota, um servidor de nomes DNS é consultado para a obtenção do seu endereço IP associado, caso o usuário use o seu nome na Internet.

2. Histórico

No ínicio da Internet, quando era chamada de Arpanet, a conversão entre o nome da máquina e o seu IP era realizada usando-se um arquivo denominado de hosts.txt. Os administradores enviavam via e-mail as alterações dos seus domínios e buscavam via FTP tal arquivo para atualizar-se.

Com o crescimeto da Internet tal mecanismo tornou-se completamente inviável, surgindo o DNS, um sistema descentralizado, fornecendo as características necessárias em relação aos problemas de carga gerada no tráfego na rede, de colisão de nomes e de consistência dos dados.

3. Como é formado o nome

O nome é formado por uma hierarquia de nomes que possui no primeiro nível referência de tipos de organizações nos Estados Unidos e as siglas dos países.

O primeiro nível dentro dos Estados Unidos possui as seguintes siglas:

- **edu**: instituições educacionias;
- **com**: organizações comerciais;
- **gov**: instituições governamentais;
- **mil**: agências militares;
- **net**: organizações da rede;
- **org**: organizações não comerciais;
- **int**: organizações internacionais.

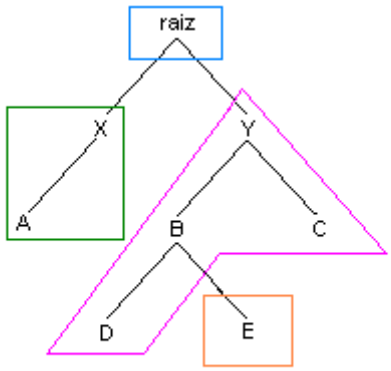
Além destes tem-se as siglas dos países, tais como **br** (Brasil), **fr** (França) e **ar** (Argentina). Também os Estados Unidos possuem a **us**, usada para o registro de nomes por disposição geográfica.

No Brasil, optou-se por seguir a estrutura inicial dos Estados Unidos, com exceção quanto à organizações educacionais que não possuem o **edu**. Exemplo de nomes:

- **ivana.ba.gov.br**: nome de uma máquina chamada ivana dentro do BA no GOV e no Brasil;
- **www.ucsal.br**: nome da máquina www na universidade do Brasil na Bahia ;
- **www.uba.ar**: nome da máquina www na Universidade de Buenos Aires na Argentina.

4. Funcionamento

Abaixo é ilustrada uma hierarquia hipotética de nomes que seria o formato lógico da base de dados do DNS:



A hierarquia contém informações de oito domínios distribuídos em quatro processos servidores de nomes (PS - polígonos coloridos).

- PS azul
- PS verde

- PS violeta
- PS laranja

O PS azul é o servidor de nomes raiz, isto é, contém as referências para os servidores de nomes dos domínios do primeiro nível da hierarquia.

A base de dados do PS azul contém as seguintes informações:

- domínio X -> PS verde
- domínio Y -> PS violeta

Os processos servidores de nomes devem conter as referências aos processos dos domínios diretamente inferiores ao seus domínios, por exemplo, para a instalação do domínio X, é necessário a configuração prévia de sua referência no PS azul. Desta forma se dá o encadeamento dos diversos domínios na hierarquia.

O PS verde contém a base de dados dos domínios X e X.A. Por exemplo, poderia possuir o mapeamento da maquina **um.X.A** para endereço 143.54.1.7.

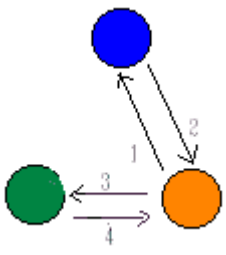
O PS violeta contém a base de dados contendo os domínios Y,Y.B,Y.B.D e Y.C. Cabe salientar que deve existir uma referência ao processo laranja que contém o sub-domínio Y.B.E.

O PS laranja contém informações do domínio Y.B.E.

5. Exemplo de Requisição

Uma cliente do DNS, chamado resolvedor, requisita ao PS laranja o IP do nome **um.X.A**. A seguinte comunicação entre processos servidores de nomes será efetuada:

1. Como o PS laranja nao possui a base de dados do domínio X.A, uma requisição é enviada para o PS azul, que é o raiz. A configuração do nome do PS raiz deve ser feita localmente.
2. Resposta com uma refência ao PS verde que possui a base de dados do domínio **X.A**.
3. Repasse da requisição original para o PS verde que contém a base de dados do domínio procurado.
4. Resposta do mapeamento do nome requisitado, 143.54.7.1.



Para resolver o nome pedido foi necessário quatro interações via rede dos processos servidores de nomes. O processo raiz é utilizado para localizar a informação desejada quando o processo que atende não a possui. Por exemplo, se o PS verde recebesse uma requisição para mapear um nome do domínio **Y.B.E**, então seria primeiro requisitado ao PS azul que responderia que o PS violeta atende o domínio Y, após o PS verde encaminharia o pedido ao PS violeta que responderia que o PS laranja contém a base de dados do domínio **Y.B.E**. Finalmente o PS verde enviaria a requisição ao PS laranja que responderia com a informação procurada. O DNS oferece FUNÇÕES ESPECIAIS para otimizar tal processo.

As funções especiais consideradas aqui são a replicação e o uso de cache.

A replicação permite que a base de dados, ou parte dela, de um processo servidor de nomes seja replicado em outro processo permitindo maior confiabilidade, pois caso um não esteja rodando haverá outro que fornecerá a informação, e otimização na utilização da rede, pois o pedido pode ser direcionado para um servidor mais perto.

O uso do mecanismo de cache permite a otimização do processo de atendimento de uma requisição DNS, pois as informações previamente consultadas são armazenadas por um período de tempo, desta forma tais informações são utilizadas ao invés de serem requisitadas via rede. Por exemplo, o PS verde poderia requisitar somente uma vez alguma informação do domínio **Y.B.E** e já teria na cache a refência que o PS laranja contém o bando de dados do domínio Y.B.E, não sendo mais necessário acessar o PS azul e violeta para pesquisar alguma informação desse domínio.

É possível também fazer pesquisas inversas, ou seja, fornecendo um número IP, o servidor devolve o domínio correspondente, e isso acontece porque, os servidores possuem uma zona de dados para resoluções inversas (Chamado de Reverso).

III. Active Directory(Microsoft)

O Active Directory tem o objetivo criar e manipular facilmente informações de um diretório.

O Active Directory implementa um espaço de nomes. Um espaço de nomes é uma área em que um determinado nome pode ser resolvido, isto é, transformado em um objeto ou nas informações que representa. Esse processo de transformação é denominado de resolução de nomes. Um exemplo de um espaço de nomes e de resolução é o guia telefônico. Nesse caso, os nomes dos assinantes são resolvidos para seus respectivos números de telefones. A estrutura do Active Directory é fortemente baseada em outro exemplo de espaços de nomes bastante comum no dia a dia de ambientes de redes: o DNS.

Entretanto, é importante observar que, apesar de empregar nomes idênticos, eles não compõem um único espaço de nomes, ou seja, em cada espaço de nomes(DNS ou Active Directory), os nomes são resolvidos para informações diferentes. Na realidade, o DNS é um serviço de resolução puro, isto é, um cliente DNS envia uma requisição a um servidor DNS para ”traduzir” um nome de máquina em IP. Já o Active Diretory é um serviço de diretório. A resolução do nome depende do tipo de objeto que o nome representa. Nesse procedimento, um cliente active directory realiza requisições a um servidor active directory(também denominado de controlador de domínio) através de um protocolo específico: o LDAP(Lightweight Directory Access Protocol).

O objetivo principal do Active Directory é facilitar a administração da rede. Essa abordagem mostrou-se prática para usuários e administradores, especialmente quando a rede apresentava uma certa complexidade pois forçava a sua subdivisão em vários domínios, o que dificultava a sua localização e o gerenciamento de sua recursos.

Os principais componentes que formam o Active Directory são: objeto, esquema, contêiner. Um objeto é qualquer usuário, sistema recurso ou serviço existente dentro do active directory. Os objetos são descritos por seus atributos, como por exemplo, nome de uma máquina e seu endereço IP. O conjunto de atributos para qualquer tipo particular de objeto é chamado de esquema. Um contêiner é um tipo especial de objeto utilizado para organizar o Active Directory. Sua idéia é similar a de pastas do Windows, isto é, se uma pasta contem arquivos e outras pastas, um contêiner armazena objetos e outros contêiners. Os três tipos possíveis de contêiners são domínios, sits e unidades organizacionais.

Um domínio é um grupo de usuários e computadores que formam uma unidade administrativa isolada. Um site consiste em uma localização geografica empregada para distinguir localizações remotas de localizações locais. Os sites podem ser comparados a subredes, isto é, uma estrutura pode ser empregada por aplicativos para localizar um determinado servidor mais próximo dessa subrede, reduzindo assim o tráfego em redes remotas. Uma unidade organizacional é um contêiner para agrupar objetos com políticas de acesso idênticas, podendo ser criadas com base em vários critérios, como função, localização, recursos, etc. As unidades organizacionais existem dentro de um domínio.

Uma característica das grandes organizações é a necessidade de criar vários domínios para controlar de forma mais apropriada os recursos de um determinado setor, departamento, filial e etc. O Active Directory permite que os domínios sejam organizados hierarquicamente na forma de uma árvore. Essa organização cria uma relação de filiação entre os domínios com uma relação de confiança, fazendo com que essa relação de confiança permita que recursos sejam compartilhados. Cada árvore possue um espaço de nome próprio. O conjunto de árvores, isto é, de espaços de nomes diferentes define o que se denomina de uma floresta.

Além de prover meios para armazenamento de dados e acesso a serviços de um diretório o Active Directory também integra mecanismos de segurança para evitar acessos não autorizados a objetos e mecanismos de replicação para garantir um certo grau de tolerância a falhas.

1. O que faz o Active Directory?

Imagine uma empresa de porte médio composta por divisões de administração, marketing, vendas, serviços e recursos humanos. A Microsoft explica que cada uma dessas divisões estaria contida no Active Directory, porque devido à sua construção hierarquica, as várias divisões teriam as sua arvores de rede, tal como uma estrutura tradicional de diretoria.

Suponha que o software da divisão de marketing precisa de atualizações. Como normalmente acontece em procedimentos normais de rede, um técnico teria que se deslocar a cada “workstation” para efetuar a mesma atualização, independentemente da localização. Com o Active Directory, isso deixou de ser um problema e uma perda de tempo, porque basta garantir o acesso ao pessoal de marketing ao software totalmente atualizado na sua máquina. O mesmo irá acontecer se garantir o acesso a drivers de disco, impressoras, e servidores de telecomunicação – ou qualquer dispositivo na sua rede. Não está limitado a software.

Ainda melhor, se alguma das pessoas do marketing transferir qualquer espécie de ficheiros, o Active Directory irá automaticamente instalar as aplicações e as permissões para o terminal que essa pessoa está a utilizar quando a mesma faz o login. Ninguém precisa de se deslocar ao site e fazer o processo de download manualmente. A rede encarrega-se de tudo automaticamente.

O Active Directory usa também, um sistema de segurança de rede. Não precisa estabelecer níveis de segurança separados para aqueles que acessem ao sistema, via Intranet. Uma vez que o utilizador faça o login na rede, a permissão e os níveis de segurança são garantidos a esse utilizador, independentemente do local onde ele se encontre. Sem essa autenticação de utilizador, as permissões implícitas ou explícitas não serão garantidas.

Isto significa que agora, mais do que nunca, o nome de utilizador e a password da Intranet deve ser pessoal e intransmissível.

2. Onde vai o Active Directory?

Se tem uma conta na internet, assim que se autenticar através do seu ISP independentemente do local onde se encontra, terá o mesmo nível de permissões disponíveis, mesmo que não se encontre no seu local habitual de utilizador. Pode acessar ao seu mail, ficheiros guardados na Internet, e caso tenha uma página personalizada na Web, a mesma irá aparecer da mesma forma em qualquer local que se desloque. Acontece que, com o Active Directory, a sua localização de login é transparente.

A rede TCP/IP e todos os destinos nela inseridos estão dispostos segundo um sistema de acesso hierarquico. (Assim como "A Internet" não é realmente um local preciso, mas sim um domínio gigante onde se encontra uma coleção de outros domínios no seu interior.) Voltando à explicação da Microsoft, é uma arvore de sistema invertida sendo o nome de acesso DNS, seguido de outros domínios preenchendo os espaços e deixando por exemplo, você entrar na www.zdnet.com e o Domain Name System (DNS) traduz essa nome para o seu endereço de Internet Protocol (IP), os quatro números separados que você normalmente encontra, e conecta-se à arvore da ZDNet – se está autorizado a isso.

Um sistema que corra num sistema operativo de um servidor de Windows 2000 é efetivamente um controlador de domínio. O Active Director usa os endereços de DNS e IP para permitir que corram processos em computadores de rede TCP/IP para identificar e conectar de uns para os outros. Cada um dos quatro números no endereço de IP representa o nome de um potencial domínio do Active Directory. E o Active Directory é baseado num diretório standard de protocolos de acesso (assim como o Lightweight Directory Acess Protocol – LDAP) – que significa que pode interoperar com outro diretório de serviços mostrando estes protocolos, o mesmo como se processa tudo na Internet.

Ainda vai despender muito tempo a desenvolver o seu site empresarial, mas quando terminar, será tudo muito mais fácil e acessível. As permissões de acesso para visitantes da Internet são construídas no Active Directory. Pode então definir os seus utilizadores com as respectivas permissões que tem de aplicar para os primeiros browsers, criar páginas Web pessoais, areas de arquivo, e mais – assim com se estivesse a administrar uma LAN graças ao Active Directory.

IV. E-Directory(Novel)

1. Sobre a Novell

Novell é a empresa líder em fornecimento de software de Serviços de Rede que fornecem os serviços que tornam todos tipos de redes, seguras e poderosas - Internet, intranets, extranets, cabeadas ou wireless, corporativas ou públicas, em sistemas operacionais líderes. Os software de Serviços de Rede da Novell, fornecem a base para uma Única Rede - uma rede global e unificada que integra novas aplicações e novas formas de negócios. Software de Serviços de Rede provêem às empresas de Tecnologia de Informação, uma forma de se adaptarem e acelerarem sua transformação para o e-business, simplificarem o gerenciamento e controle de todas as redes, criarem uma base segura para os negócios na rede global e ajudam no fornecimento de uma experiência consistente e de alto nível para os usuários em qualquer localidade. Os programas mundiais de canal, consultoria, treinamento e suporte técnico, em conjunto com as alianças estratégicas, combinam com os software de Serviços de Rede da Novell e produtos de terceiros e serviços, formando soluções completas de Serviços de Redes.

2. Visão geral do Novell eDirectory

Protege os recursos digitais dos clientes com a segurança com base em políticas. Essas políticas permitem que funcionários, clientes, parceiros e fornecedores acessem informações da rede, mas apenas as informações para as quais eles tiverem autorização. Com o eDirectory, é possível controlar o acesso, permitindo somente a entrada de pessoas bem-intencionadas. Por exemplo, os parceiros poderão ter um acesso mais amplo à sua rede do que os visitantes esporádicos. Seus clientes podem atribuir políticas para usuários individuais, grupos de usuários e a vários recursos da rede, como arquivos, aplicativos e servidores.

3. O Novell eDirectory 8.6.2

É um sistema de gerenciamento de identidade habilitado para LDAP (Lightweight Directory Access Protocol) e baseado em diretórios que centraliza o gerenciamento de identidades do usuário, privilégios de acesso e outros recursos de rede. O eDirectory ajuda empresas a comercializarem produtos e serviços mais rapidamente do que os concorrentes, fornecendo uma vantagem competitiva no mercado da Internet.

Como o eDirectory oferece suporte à funcionalidade de grupos dinâmicos, a pesquisas persistentes e ao backup contínuo ativo, ele reduz muito o overhead administrativo. Além disso, a versão 8.6.2 aumenta a escalabilidade e o desempenho da rede em um ambiente da Internet. Isso permite estender o suporte da rede a clientes e parceiros que utilizam a Web como canal principal para realizar negócios.

Além disso, o eDirectory permite que você utilize aplicativos habilitados para diretórios para criar relacionamentos personalizados e seguros entre sua rede e as redes implementadas pelos clientes e parceiros. Na verdade, você pode utilizar o eDirectory para estender a infra-estrutura da rede existente além do firewall e cultivar relacionamentos de eBusiness lucrativos. Os clientes podem preencher com segurança os diretórios que possam ser acessados por clientes. Parceiros comerciais podem se

comunicar diretamente com os diretórios uns dos outros e atualizá-los. Fornecedores podem obter informações imediatas sobre a quantidade e as datas de remessa de produtos. Alterações em reservas de companhias aéreas podem alertar automaticamente sistemas de reservas em hotéis e de aluguéis de carros. Dados importantes do mercado podem ser reunidos à velocidade da Internet.

O eDirectory também fornece a base para capturar, armazenar, organizar e otimizar informações de identidade importantes, como dados demográficos de clientes, interesse por produtos, padrões de compra, transações, feedback de produtos e níveis de satisfação. Com essas informações, você pode adaptar as experiências comerciais dos seus clientes, como as informações que eles vêem em uma página da Web, para cultivar um tipo de lealdade à sua empresa que permanecerá à medida que seu negócio mudar e se expandir.

Com o eDirectory, você também pode ter certeza de que os recursos estão seguros. Os recursos de segurança superiores do eDirectory incluem a Novell® International Cryptographic Infrastructure, senhas criptografadas por SSL (Secure Sockets Layer), criptografia de chaves privadas/públicas RSA, Servidores de Autenticação Seguros, cartões inteligentes e certificados X.509v3. Você poderá indicar com exatidão quem terá acesso a determinadas informações: a concessão de direitos a um diretório não fornecerá direitos de acesso a toda a rede ou mesmo a todas as informações desse diretório.

Além disso, o eDirectory inclui o Novell iMonitor, que permite gerenciar o eDirectory usando um browser da Web e a federação DNS, que permite gerenciar objetos de usuários nas árvores do eDirectory de parceiros e vice-versa. O suporte mais forte a aplicativos LDAP (incluindo SSL) e a replicação filtrada também são novidade.

O eDirectory 8.6.2 é executado em um servidor PC Intel Pentium ou em uma estação de trabalho UNIX e requer 64 MB de RAM (recomenda-se 128 MB). O eDirectory está disponível para NetWare® 5.x ou superior, Windows 2000, Windows NT, Solaris, Linux ou como uma atualização de servidores NetWare.

V. Comparativo entre Active Directory e E-Directory

Laboratório de Testes Certificado pela Microsoft Comprova que o NDS eDirectory da Novell é o Mais Rápido em Desempenho na Web com Taxa Zero de Falhas. Especialistas da Internet e Educacionais Destacam o Desempenho e a Confiabilidade do NDS eDirectory em Implementações de Missão Crítica.

A Novell, Inc. anunciou os resultados dos testes que demonstram o poder de seu NDS eDirectory; multiplataformas nos ambientes de mundo real da Internet. A KeyLabs Inc., uma empresa independente de testes e um Microsoft Certified Solution Partner, descobriu que o NDS eDirectory superou o desempenho do Microsoft Active Directory e do iPlanet (anteriormente Netscape) Directory Server em ambientes reais, simulando cargas comuns de diretório e solicitações de busca.

"Esta é a primeira vez que fomos contratados para elaborar testes que simulassem vários tipos de buscas de diretório simultaneamente," disse Matt Mace, diretor de qualidade da KeyLabs. "Em cada um dos testes baseados em LDAP que realizamos com diferentes tipos de buscas simultâneas, o NDS eDirectory da Novell superou o desempenho do Active Directory executado no Windows 2000 Server."

Os testes foram elaborados para simular o uso de diretórios em ambientes reais, onde a maioria dos usuários realizam buscas básicas e complexas na

Internet. Como a disponibilidade consistente de um Web site é o aspecto mais crítico dos serviços aos clientes, o teste também apontou falhas e sucessos na conclusão das buscas.

Os resultados dos testes do Active Directory e do NDS eDirectory mais recentes feitos pela KeyLabs são:

- Em várias buscas simultâneas simulando situações do mundo real, o NDS eDirectory foi consistentemente 250 porcento mais rápido do que o Active Directory. Qualquer pessoa que use a Web conhece a frustração de esperar por uma resposta. Fornecer respostas a uma variedade de consultas de usuários usando diversos critérios de pesquisa é considerado um requisito básico para manter a satisfação do cliente.

- Nos testes de pesquisa de nomes de usuários no diretório quando somente uma parte do nome era fornecida como critério de busca, o NDS eDirectory teve um desempenho de 1.250 vezes mais rápido do que o Active Directory, e nenhuma falha. No mesmo teste, o Active Directory falhou 715 vezes num total de 6000 pesquisas - uma em cada oito. Os usuários tendem a fazer buscas usando nomes parciais porque o esforço é menor. Um diretório de Internet deve ser capaz de acomodar o comportamento do usuário típico.

- Quando a KeyLabs aumentou de 2 para 100 clientes em sua busca comum por nomes parciais, o Active Directory foi incapaz de retornar um único resultado. Isto eqüivale a conectar-se ao seu mecanismo de busca preferido, fazer a busca de um tópico e jamais obter uma resposta.

VI. Conclusão

Com o aumento no tamanho das redes e as constantes mudanças pelas quais as redes passam, os usuários passam a necessitar um serviço que permita um acesso transparente ao usuário aos recursos da rede. Um Serviço de Diretórios é responsável por permitir que o usuário possa consultar ou navegar em diretórios de usuário, organizações ou recursos, sem ter a necessidade de conhecer detalhes sobre os objetos armazenados nestes diretórios.

Indivíduos e organizações podem usar um serviço de diretórios para tornar disponível um amplo conjunto de informações sobre eles próprios e sobre os recursos que desejam oferecer para uso na rede. Usuários podem pesquisar o diretório em busca de informações específicas, tendo somente conhecimento parcial sobre o seu nome, estrutura ou conteúdo.

VII. Bibliografia

www.keylabs.com/results/novell/nds/index.htm
www.novell.com
www.ppgia.pucpr.br
www.inf.ufrgs.br