Carlos Fernando Papotti RA : 02131282
José Ricardo M. Bevilacqua RA : 02534626
Julio César Costa Marcondes RA : 02121069
Raul Baldin RA : 02088243

Lightweight Directory Access Protocol
LDAP

Tópicos em Engenharia de Computação A
Professor: Eduardo Nicola Ferraz Zagari

Campinas
2006

Introdução

LDAP é um protocolo (executado sobre o TCP/IP) cliente-servidor, utilizado para acessar um serviço de diretório. Ele foi inicialmente usado como uma interface para o X.500, mas também pode ser usado com autonomia e com outros tipos de servidores de diretório. Atualmente, vem se tornando um padrão, e diversos programas já têm suporte a LDAP. Livros de endereços, autenticação, armazenamento de certificados digitais (S/MIME) e de chaves públicas (PGP) são alguns dos exemplos onde o LDAP já é amplamente utilizado.

Mas, o que é um Diretório ?

Um Diretório é como um banco de dados, mas tende a conter mais informações descritivas, baseadas em atributos e é organizado em forma de árvore, não de tabela. A informação em um Diretório é, geralmente, mais lida do que escrita. Como conseqüência, Diretórios normalmente não são usados para implementar transações complexas ou esquemas de consultas regulares em bancos de dados, mas para realizar atualizações, tudo isso envolvendo apenas pequenas quantidades de dados.

Diretórios são preparados para dar resposta rápida a um grande volume de consultas ou operações de busca. Eles também podem ter a habilidade de replicar informações extensamente. Isso é utilizado para acrescentar disponibilidade e confiabilidade, enquanto reduzem o tempo de resposta.

Existem várias maneiras diferentes para disponibilizar um serviço de diretório. Métodos diferentes permitem que diferentes tipos de informações possam ser armazenadas no diretório, colocando requerimentos diferentes sobre como aquela informação poderá ser referenciada, requisitada e atualizada, como ela é protegida de acessos não autorizados, etc. Alguns serviços de diretório são locais, fornecendo o serviço para um contexto restrito (exemplo: o serviço finger em uma máquina isolada). Outros serviços são globais, fornecendo o serviço para um contexto muito maior (por exemplo, a própria Internet).

Serviços globais normalmente são distribuídos (conforme demonstra figura abaixo), ou seja, cada servidor é responsável por uma parte dos dados, apenas. O DNS (*Domain Name System*) é um exemplo. Ele é um tipo de serviço de diretório, embora bastante especializado.

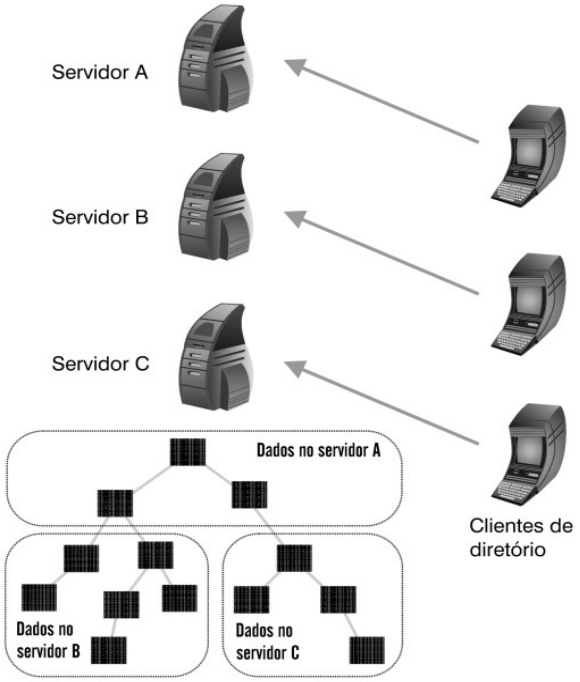

Figura 1 - Dados de um Diretório distribuídos em três servidores.

Um pouco de história

O LDAP foi originalmente desenvolvido como um cliente para o X.500, o serviço de Diretório OSI. O X.500 define o Protocolo de Acesso a Diretório (DAP) para os clientes usarem quando estiverem em contato com servidores de diretório. O DAP é um protocolo pesado, que roda sobre uma camada OSI completa, e precisa de uma quantidade significante de recursos computacionais para ser executado. Tendo isso em vista, pensou-se em criar um protocolo mais leve para que também fosse utilizado em máquinas de menor poder computacional, como em desktops convencionais. Então foram desenvolvidos dois protocolos, o Directory Assistance Service (DAS) e o Directory Interface to X.500 Implemented Efficiently (DIXIE), que foram os predecessores do LDAP, mas que ainda eram muito ligados ao X.500, pois precisavam de um servidor intermediário para efetuar a "tradução" desses protocolos para o DAP que se comunicaria com o Diretório X.500, como é demonstrado abaixo:

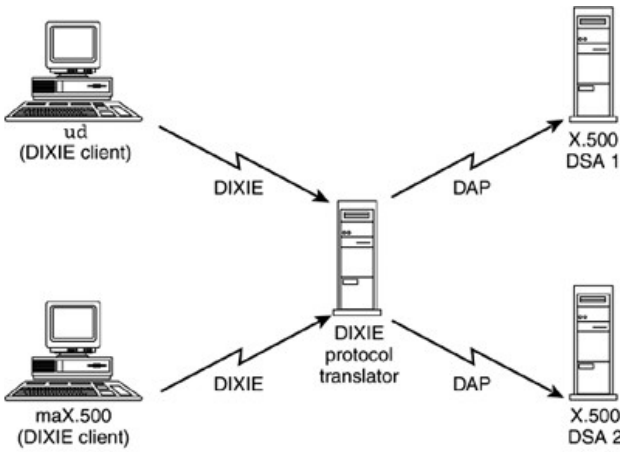

Figura 2 – Utilizando DIXIE para se comunicar com Diretórios X.500

Então, a união de forças da OSI-DS Working Group e da IETF resultou na construção de um novo protocolo, o Lightweight Directory Access Protocol (LDAP), que roda diretamente sobre TCP/IP e fornece a maioria das funcionalidades do DAP, a um custo muito menor, além de ser muito mais leve.

No princípio, a utilização do LDAP (LDAPv1) era similar ao DAS e ao DIXIE, utilizando um servidor intermediário e exigindo um serviço X.500 completo. A segurança dos dados que trafegavam também era uma preocupação, pois todos eram (e ainda são) em formato texto (*strings*). Então foi desenvolvido o LDAPv2, com autenticação utilizando o Kerberos v4. Mas ao passar dos anos percebeu-se que os complexos e pesados Diretórios X.500 poderiam ser substituídos por Diretórios mais leves e que não possuíssem tamanha complexidade que raramente era utilizada. Foi então que surgiu a ideía de desenvolver o lado servidor do LDAP, ou seja, Serviços de Diretórios LDAP, que são utilizados até hoje. E também foi desenvolvido o LDAPv3 (atual) que possui um suporte muito maior à autenticação (compatível com SASL e TLS) e várias outras extensões que permitem a adição de novas operações e controles.

Como funciona então o protocolo LDAP ?

Como já foi dito anteriormente, o serviço de diretório LDAP é baseado em um modelo cliente-servidor. Um ou mais servidores LDAP contém os dados residentes em uma árvore de diretório LDAP. Um cliente LDAP conecta-se a um servidor e faz uma requisição. O servidor responde com a requisição ou exibe um ponteiro para um local onde o cliente pode conseguir a informação (tipicamente, outro servidor LDAP). Pode-se até fazer uma comparação com o DNS, a diferença é que o servidor LDAP não faz buscas recursivas, ou seja, em nome do cliente. O cliente é que é encarregado de procurar pelo servidor até encontrar a informação desejada.

Quais são algumas das utilidades do protocolo LDAP ?

Antes de enumerarmos as diversas utiliades possíveis do LDAP, deve ser questionado que tipo de informação existe na rede. Se está de forma fragmentada ou desordenada e se não seria útil reunir estas informações num só lugar, dando uma nova formatação, reagrupando os itens, uniformizando estes dados de modo que estejam facilmente acessíveis por todas as estações de trabalho na rede.

Podemos agora indicar que o LDAP tem sido utilizado para os seguintes cenários:

- em substituição dos servidores NIS, fornecendo login/senha (autenticação) para usuários Linux/Unix;
- autenticação para usuários SAMBA;
- autenticação para serviços de email (POP3/IMAP);
- autenticação para aplicativos groupware (como o MoreGroupware);
- catálogo com os endereços de email, endereços, telefones, etc. de empregados ou clientes da empresa;
- solução de single sign on (SSO), permitindo acesso para vários ambiente e arquiteturas de software e sistemas operacionais.

E quais são os padrões que o LDAP segue?

O protocolo LDAP define quatro tipos básicos de modelos que definem como ele opera, que tipo de dados podem ser armazenados em seus Diretórios e o que pode ser feito com esse dados. Todos esses modelos estão publicados em RFCs disponíveis para consulta do público em geral. Os modelos são:

- **Modelo de Informação –** define os tipos de dados e as unidades básicas de informação que você pode armazenar no Diretório;
- **Modelo de Nomes –** define como você organiza e faz referência aos seus dados;
- **Modelo de Segurança –** define quais procedimentos podem ser tomados para se evitar o acesso não autorizado às informações do Diretório, como protocolos de encriptação e autenticação;
- **Modelo Funcional –** descreve as operações que você pode realizar no Diretório utilizando o protocolo LDAP;

E como são organizados as informações no LDAP ?

O elemento básico de informação de um Diretório é denominado *entrada*, que corresponde a uma coleção de informações de um determinado *objeto* que, por sua vez, possui diversos *atributos* que o descreve. Cada atributo possui um *tipo*, que define que tipo de informação está contida no atributo, e um *valor*, que contém o dado propriamente dito. Esses objetos podem corresponder a objetos do mundo real mesmo, como pessoas, impressoras, servidores, etc., mas não necessariamente precisam ser do mundo real, pode ser qualquer tipo de informação. É importante ressaltar também que cada entrada é identificada por um DN (*Distinguished Name*), que se trata de uma nome único que serve para se referir a uma determinada entrada no Diretório sem problemas de ambigüidade, por exemplo.

No LDAP, entradas de Diretório são organizadas em uma hierarquia de árvore invertida, semelhante, em alguns aspectos, à organização do sistema de arquivos Unix, porém com a diferença que na raiz estão armazenadas informações do servidor ao invés de um objeto. A estrutura desta árvore geralmente reflete limites políticos, geográficos e/ou organizacionais. O nó mais alto (**raiz**) é tipicamente o componente nome de domínio (**dc**) de um país, companhias ou organizações internacionais. Abaixo ficam as entradas representando estados ou organizações nacionais. Abaixo elas podem ser entradas representando pessoas, unidades organizacionais, impressoras, documentos ou qualquer outra coisa em que você possa imaginar. A figura abaixo mostra um exemplo de um Diretório LDAP em árvore:

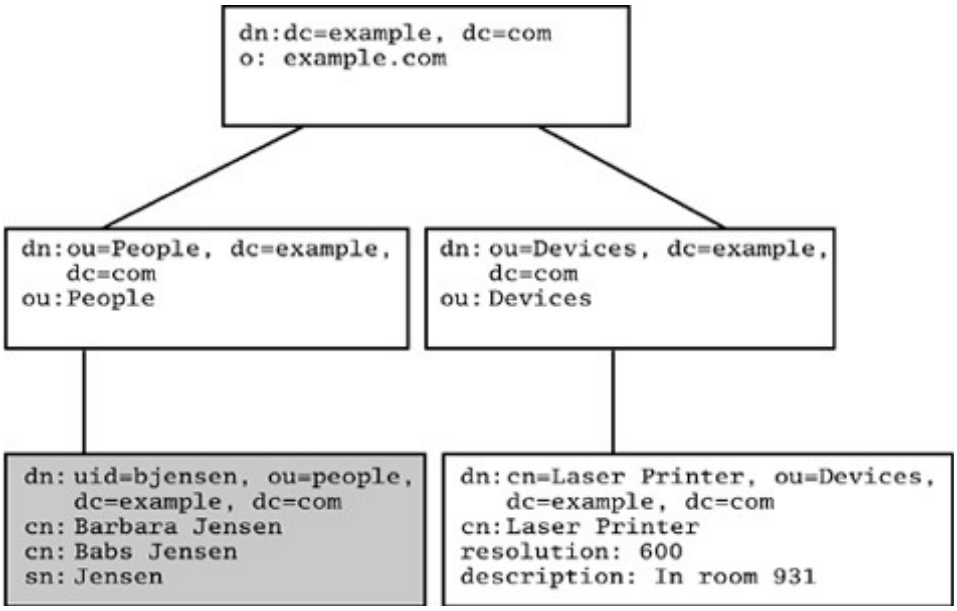

Figura 3 - Árvore de Diretório LDAP

Apesar de termos entradas para países, o diretório não possui uma entidade centralizadora como, por exemplo, o *root* do Unix. A separação por países, por exemplo, pode ser útil para empresas multinacionais. Uma outra vantagem de um serviço de diretórios é que os *ramos* da árvore podem estar em máquinas diferentes. No caso acima, a entrada de cor cinza pode estar em um outro computador, por exemplo. Note que esta característica também é típica de servidores DNS.

Como são organizados os atributos usando LDAP ?

Sabemos que alguns tipos de atributos usados nas entradas em um serviço de diretórios são: `mail`, `cn`, `telephoneNumber` e outros. Entretanto, pode-se criar qualquer outro tipo de atributo, mas isso não é recomendado. No LDAP existem diversas classes de objetos e cada classe contém uma lista de atributos obrigatórios e opcionais. Essa lista é tipicamente definida em uma RFC, mas empresas ou organizações também podem criar suas próprias classes, se necessário. O mais recomendado é tentar utilizar as classes e atributos já existentes.

Por exemplo, a classe *person* (RFC 2256) é definida da seguinte maneira:

```
objectclass ( 2.5.6.6 NAME 'person' SUP top STRUCTURAL
 MUST ( sn $ cn )
 MAY ( userPassword $ telephoneNumber $ seeAlso $ description ) )
```

O servidor LDAP pode ser configurado para verificar as classes (através da opção *`schemacheck`*) e forçar o uso correto dos atributos. Isso, geralmente, é uma boa idéia. Com a verificação das classes habilitada, será obrigatória a inserção dos atributos `objectClass`, `sn` e `cn`, por exemplo. Quando for definido que uma entrada do Diretório é da classe *person*, o atributo *description* será opcional. Entradas em diretórios podem ter várias classes diferentes, basta apenas observar os requisitos de atributos de cada classe.

E quanto a segurança e a consistência dos dados ? O que o LDAP oferece ?

Além de todo o serviço de organização de informações, o LDAP também oferece recursos para proteção dos dados que são manipulados, diferentemente de alguns serviços de diretório que não fornecem nenhum tipo de proteção, permitindo que qualquer pessoa possa interceptar as informações. O LDAP fornece métodos para autenticação de um cliente ou prova sua identidade para um servidor de diretório, protegendo as informações contidas no servidor.

Além disso, o LDAP oferece também recursos para a replicação de dados em caso das mesmas serem apagadas ou alteradas por intrusos. Um exemplo de um servidor para Linux que auxilia o LDAP (mais precisamente o SLAPD – servidor que pode ser executado em diversas plataformas), provendo a replicação do banco de dados é o SLURPD. O SLAPD e o SLURPD se comunicam através de um simples arquivo texto, que é utilizado para registrar as mudanças. A sintaxe deste arquivo lembra um pouco a sintaxe dos arquivos resultantes do *diff*, no sentido de que estão descritas as entradas ou atributos que devem ser removidos, adicionados ou modificados. Esse tipo de arquivo é identificado com o nome de LDIF.

Em um processo de replicação simples, o cliente insere, exclui ou modifica informações no servidor LDAP *master*, que se encarrega de realizar a replicação dos seus dados em outros servidores (os quais servem somente para operações de consulta). Esse processo de replicação ocorre continuamente em um determinado intervalo de tempo ou pode acontecer imediatamente, quando a atualização de dados for de alta prioridade ou crítica para o Diretório.

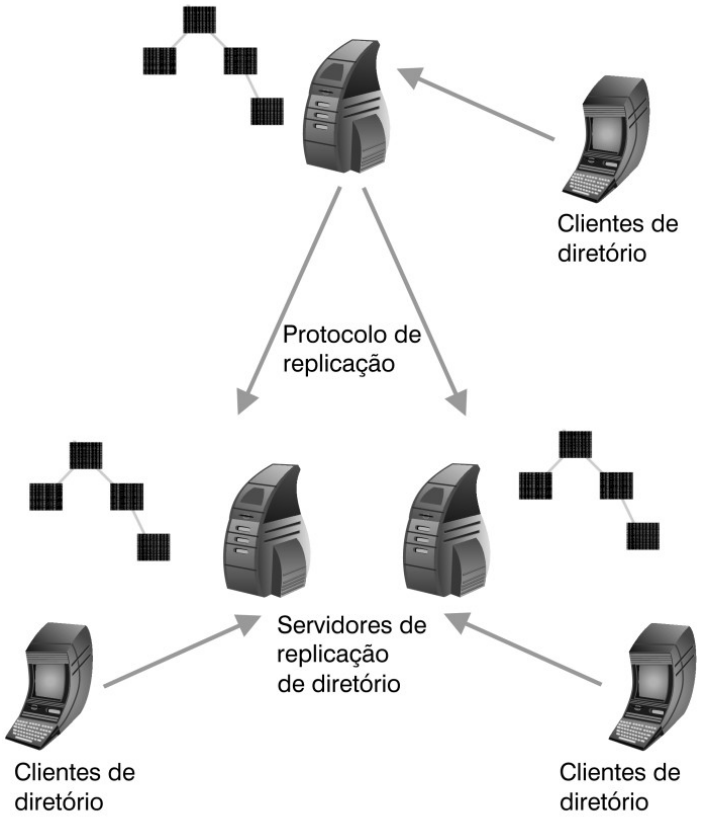

Figura 4 - Um Serviço de Diretório Replicado com Dados Distribuídos em Três Servidores

Do que é composto o arquivo LDIF?

O LDAP Data Interchange Format (LDIF), citado anteriormente, corresponde em inglês a: “Troca de dados entre diferentes formatos“ e é baseado em um formato de texto padrão utilizado para descrever diretórios, tendo sua estrutura definida pela RFC 2849.

Os arquivos LDIF permitem que você possa importar ou exportar os dados do seu servidor de diretório com outro, sem que os dois necessitem utilizar uma mesma base de dados. Com isso, é possível distribuir as mais diversas informações contidas em um servidor de diretório para outros servidores de diretório utilizando apenas comandos padronizados.

Atualmente existem dois tipos diferentes de arquivos LDIF. O primeiro tipo descreve um conjunto de entradas de diretórios (exemplo abaixo) que serve para ser diretamente agregado a um Diretório, enquanto que o outro tipo é uma série de comandos de atualização que descrevem as mudanças que devem ser aplicadas aos atributos das entradas de um Diretório.

```
version: 1
dn: uid=bjensen, ou=people, dc=example, dc=com
objectclass: top
objectclass: person
objectclass: organizationalPerson
objectclass: inetOrgPerson
cn: Barbara Jensen
cn: Babs Jensen
givenName: Barbara
sn: Jensen
uid: bjensen
mail: bjensen@example.com
telephoneNumber: +1 408 555 1212
description: Manager, Switching Products Division
dn: uid=ssmith, ou=people, dc=example, dc=com
objectclass: top
objectclass: person
objectclass: organizationalPerson
objectclass: inetOrgPerson
cn: Steve Smith
cn: Stephen Smith
givenName: Stephen
sn: Smith
uid:ssmith
mail: ssmith@example.com
telephoneNumber: +1 650 555 1212
description: Member of Technical Staff.
```

E quanto a autenticação ? O que o LDAP oferece ?

No LDAPv1 a autenticação era realizada de maneira simples, ou seja, não havia nenhum método de criptografia e o nome de usuário e senha eram enviados em formato de texto convencional, que poderia ser interceptado por qualquer outra pessoa no momento do envio. Como esse método de autenticação do LDAP era muito indesejável, pois introduzia uma grave vulnerabilidade no que diz respeito à sua segurança, foi desenvolvido uma nova versão do protocolo (LDAPv2) que tem como sua principal mudança a inclusão do suporte ao mecanismo Kerberos v4 como método de criptografia. Porém, o Kerberos v4 não foi comercialmente aceito e foi, posteriormente, substituído pela versão 5. Ainda assim, o Kerberos não estava amplamente

disponível nos servidores do LDAPv2, o que fazia com que os clientes adotassem o método básico de autenticação, ou seja, não-encriptado que era aceito por todos os servidores. Tendo isso em vista, foi desenvolvida uma nova versão do LDAP, o LDAPv3 (atual), que trata a autenticação baseada nos modos de como os servidores são acessados:

- Servidores LDAPv3 públicos somente-leitura – permitem login anônimo, sem senha;
- Servidores com autenticação usando senhas – usa mecanismo SASL DIGEST-MD5;
- Servidores com autenticação e criptografia de dados – usa StartTLS para camada de transporte segura e certificados com chaves públicas para autenticação de ambos os lados, proporcionando autenticidade, integridade e criptografia dos dados.

O estabelecimento de uma conexão cliente-servidor LDAP acontece, basicamente, em três passos, onde o cliente:

1. Abre uma conexão TCP com o servidor;
2. Envia uma operação StartTLS, em que os protocolos de camada mais baixa negociam a encriptação e a autenticação segundo a especificação do TLS;
3. Realiza o *bind* utilizando um mecanismo SASL EXTERNAL caso um certificado tenha sido fornecido durante a negociação TLS, ou outro mecanismo SASL como o DIGEST-MD5, por exemplo.

E como são acessadas as informações desejadas nos diretórios usando LDAP ?

O LDAP possui três tipos de operações que são definidas abaixo:

- **Operações de Interrogação:** search e compare – permite que você faça requisições de consulta ao Diretório;
- **Operações de Atualização:** add, delete, modify, modify DN (rename) – permite que você faça atualizações no Diretório;
- **Operações de Controle e Auteticação:** bind, unbind e abandon – o bind permite identificar o cliente enviando credenciais de autenticação (que pode ser um simples password), o unbind serve para terminar uma sessão estabelecida com o servidor e o abandon serve para indicar que o cliente não está mais interessado nas repostas que chegarem até ele.

As operações LDAP de consulta podem abranger a árvore toda (uma busca com escopo *subtree*) ou apenas um ramo, sem *descer* ou *subir* para os demais. Além de especificar com filtros quais entradas se deseja encontrar, também é possível especificar quais atributos destas entradas estão sendo procurados. Se os atributos não forem especificados, todos serão retornados.

Por exemplo, na figura 3 nós poderíamos querer pesquisar toda a sub-árvore de diretório abaixo da entrada *Devices*, procurando por impressoras com o nome *Laser Printer*, recuperando a resolução para cada entrada encontrada. O LDAP permite que você faça isso facilmente.

Como ocorre a troca de mensagens no protocolo LDAP ?

Como em qualquer outro protocolo de comunicação, o protocolo LDAP permite a comunicação entre dois servidores de diretório ou entre o servidor e seus clientes utilizando, para isso, a troca de mensagens. A troca de mensagens no protocolo LDAP consiste em três estágios :

1 – Abrindo a Conexão

2 – Fazendo uma ou mais pesquisas

3 – Fechando a conexão

No primeiro estágio, o cliente LDAP abre uma conexão TCP com o servidor LDAP utilizando um arquivo texto encriptado por TLS, por exemplo. O cliente, então, utiliza algum método de autenticação (exemplo: SASL) para se identificar, fornecendo as informações necessárias para a autenticação (normalmente nome de usuário e senha). Isso é chamado de *binding*. Em alguns casos a conexão não é realmente autenticada, mas anônima, então, a mensagem de *bind* é enviada sem identificação de usuário e senha. Após realizado o *bind* e as consultas, o cliente deve enviar uma mensagem de *unbind* para indicar o término da sessão. Note que apenas enviando um *unbind*, a conexão ainda permanece aberta e deve ser encerrada posteriormente com um fechamento de socket TCP, e os servidores também devem tratar situações onde não é enviado o *unbind* e a conexão é perdida ou propositalmente fechada. Um exemplo dessa troca de mensagens é demonstrado na figura abaixo:

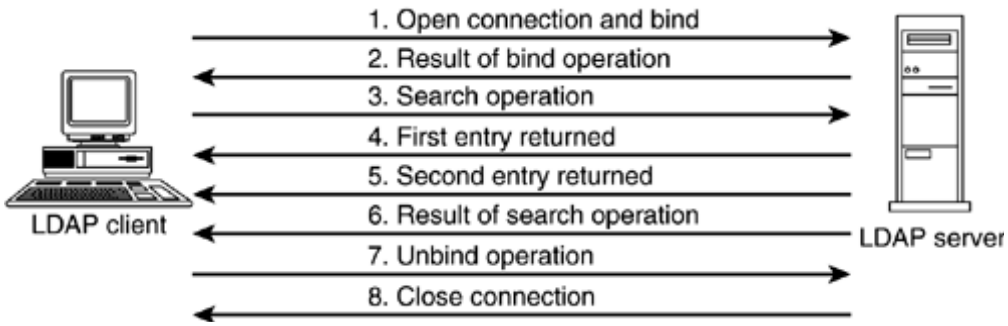

Figura 5 - Estabelecimento de conexão, consulta e fechamento de uma conexão LDAP

Na segunda etapa, o cliente envia uma mensagem de consulta, contendo um DN para cada consulta. E para cada mensagem, o cliente também gera um ID diferente, o qual o servidor utiliza como uma das informações de resposta, para que o cliente possa identificar a qual requisição de consulta aquela determinada resposta corresponde.

O servidor responde enviando o resultado da pesquisa, com uma mensagem por dado encontrado. Se não forem fornecidos dados a serem pesquisados ou se houver algum erro na pesquisa, o servidor pode não enviar as informações sobre a solicitação desejada. Por fim, o servidor envia uma mensagem indicando que a pesquisa foi concluída (*Result code*) que inclui a relação dos resultados obtidos, como é mostrado abaixo:

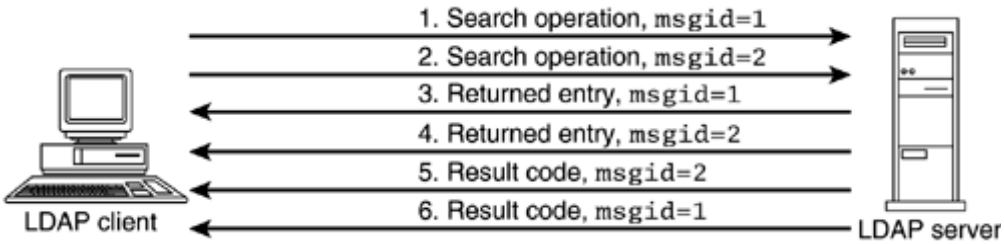

Figura 6 – Uma simples pesquisa LDAP

Note que se o cliente tiver enviado uma outra solicitação de pesquisa sem aguardar pela finalização da primeira solicitação, não há problema algum, pois todas as mensagem são devidamente identificadas, tornando o LDAP um protocolo ainda mais ágil na pesquisa de informações, pois com uma mesma conexão aberta pode-se realizar várias consultas ao invés de ter que abrir uma conexão para cada consulta.

Conclusão

Percebe-se que o LDAP possui inúmeras áreas onde pode ser aplicado, pois se trata de um protocolo leve que não exige muitos recursos computacionais e pode ser utilizado desde pequenas empresas até grandes corporações para integração de seus inúmeros serviços. Além de possuir uma grande escalabilidade, isto é, podem ser adicionadas várias expansões tanto na linha de operações funcionais quanto em comandos de controle, o LDAP ainda possui várias opções para a segurança de dados, pois adota, atualmente, um dos *frameworks* mais utilizados e flexíveis da Internet (SASL). Porém, o LDAP deve ser escolhido como solução e projetado com muito cuidado, pois ele não se trata de uma substituição definitiva a bancos de dados ou outros serviços, como servidores FTP, servidores WEB ou sistemas de arquivos. Deve-se analisar muito bem quais são os requisitos do serviço onde se pretende empregar o LDAP, pois, talvez, essa não seja a melhor solução. Pode até funcionar, mas não com uma eficiência satisfatória.

Bibliografia :

Timothy A. Howes - Ph.D., Mark C. Smith, Gordon S. Good – **Understanding and Deploying LDAP Directory Services, Second Edition –** 2003 – Ed. Addison Wesley Professional.

Lightweight Directory Access Protocol – Wikipedia
http://en.wikipedia.org/wiki/Lightweight_Directory_Access_Protocol

Understanding LDAP - IBM redbook
http://www.redbooks.ibm.com/pubs/pdfs/redbooks/sg244986.pdf

Sys Admin Guide for Directory Services
ftp://docs-pdf.sun.com/816-4856/816-4856.pdf

Introduction to OpenLDAP Directory
http://www.openldap.org/doc/admin21/intro.html