MAC 499 - Trabalho de Formatura Supervisionado

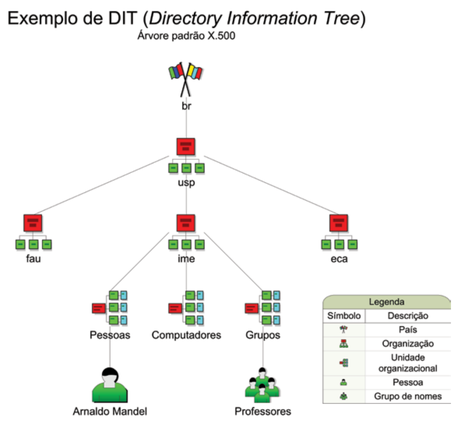
# Autenticação Integrada Baseada em Serviço de Diretório LDAP

Supervisor: Prof. Dr. Arnaldo Mandel
Erich Soares Machado e Flavio da Silva Mori Junior
Bacharelado em Ciência da Computação - IME - USP

## Introdução

Redes de computadores estão presentes na maioria das empresas atualmente, devido a grande necessidade de comunicação que as aplicações distribuídas exigem. Muitas dessas aplicações utilizam os mesmos dados para realizar as suas operações. Sendo assim, torna-se necessário buscar uma maneira de organizar essa informação de maneira clara e consistente, de forma a facilitar o acesso às mesmas, reduzir o custo de sua manutenção e por conseqüência aumentar a funcionalidade dos vários sistemas que a usam.

A necessidade de integração desse tipo de informação motivou o surgimento de um padrão aberto que possa atendê-la. Esse padrão chama-se LDAP (*Lightweight Directory Access Protocol*), e trata-se de um protocolo que define um método para o acesso e a atualização de informações em um diretório. Diretório é uma espécie de banco de dados, otimizado para leitura e busca.

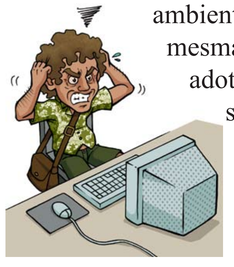


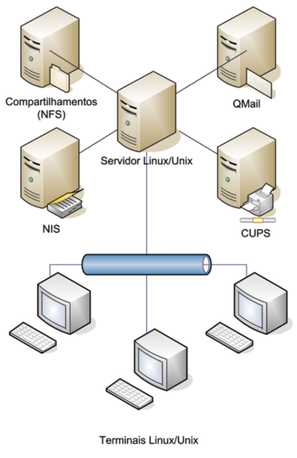

O LDAP define um protocolo de comunicação, ou seja, o transporte e o formato das mensagens utilizadas pelo cliente para acessar os dados que estão armazenados em um diretório do tipo X.500. O padrão X.500 organiza as entradas do diretório em um espaço de nomes hierárquico (uma árvore) capaz de incorporar grandes volumes de informação. O LDAP também define métodos de busca poderosos o suficiente para tornar a recuperação dessa informação fácil e eficiente. Ele não define o serviço de diretório em si. Com o LDAP o cliente não é dependente da implementação em particular do serviço de diretório que está no servidor.

## Problema

Todo ambiente de rede precisa armazenar informações para possibilitar o seu gerenciamento (autenticação, grupos de usuários, permissões, cotas de armazenamento e impressão, compartilhamentos e etc.). Hoje em dia, a maioria das grandes organizações possui ambientes de rede heterogêneos, com várias plataformas presentes (Unix, Windows, Solaris...) e com redes virtuais fisicamente conectadas, muitas vezes distribuídas geograficamente. Um exemplo de organização desse tipo é a Universidade de São Paulo, que possui uma grande rede de dados interconectando todos os seus campi, espalhados pelo estado.

Um problema decorrente desse tipo de implantação é que para cada plataforma ou para cada rede local virtual existente no ambiente de rede (a rede física), é necessário suprir essas mesmas informações de gerenciamento. Se não for adotada uma boa solução de gerenciamento, podem surgir problemas decorrentes da replicação desses dados. Os principais são: redundância, falta de sincronia nas informações, dificuldade de organização, maior custo no suporte e falta de segurança.

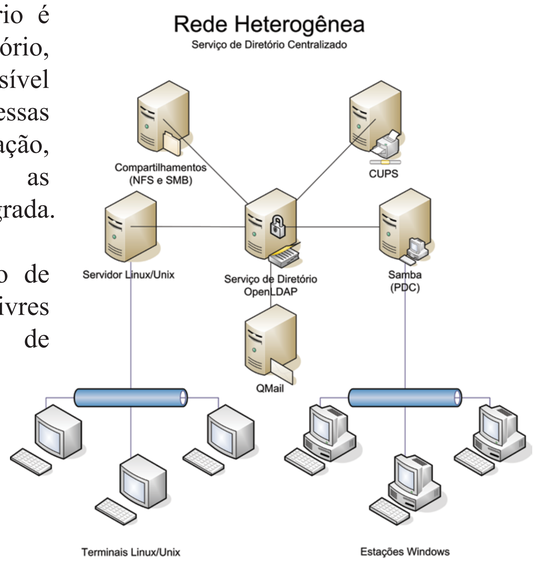





## Solução

Uma solução cada vez mais empregada para este cenário é armazenar as informações do ambiente de rede em um diretório, através de um serviço de diretório LDAP. Isso torna possível acessar de forma padronizada, ágil e segura, todas essas informações. Portanto todos os serviços da rede (autenticação, compartilhamento, impressão, email, etc.) buscarão as informações de que precisam nesse diretório, de forma integrada.

Uma maneira de disponibilizar um serviço de diretório LDAP é utilizando soluções livres disponíveis atualmente. Um exemplo de implantação desse tipo é instalar um servidor OpenLDAP, integrando-o ao PAM (*Pluggable Authentication Modules*) para realizar a autenticação dos clientes Linux/Unix, e integrando-o ao Samba para autenticar os clientes Windows. Toda a comunicação entre os serviços pode ser protegida através do suporte TLS (*Transport Layer Security*).




OpenLDAP é uma suíte de aplicativos LDAP open-source, que inclui todas as ferramentas necessárias para fornecer um serviço de diretório LDAP em um ambiente de rede (clientes, servidores, utilitários e ferramentas de desenvolvimento), disponível para várias plataformas. É uma solução considerada madura hoje em dia e possui amplo suporte, sendo largamente utilizada como alternativa às implementações comerciais existentes (Microsoft Active Directory, Novell eDirectory, SunOne Directory Server, etc.).

## Conclusão

O protocolo LDAP está sendo cada vez mais usado como método de acesso a diretórios na Internet, tornando-se a estratégia adotada por muitas redes corporativas. Muitas empresas de software o estão incorporando em seus produtos. Isso torna possível a criação de um diretório centralizado, que armazena toda a informação que precisa ser acessada por esses diferentes sistemas. Com essa centralização e pela facilidade de acesso à informação, existe a necessidade de implantar medidas de segurança de forma a evitar que esses dados caiam em mãos erradas. Sendo assim, a maioria dos serviços de diretório LDAP fornece meios de proteger as informações contidas no diretório através de um mecanismo de autenticação e de serviços de segurança dos dados (integridade e confidencialidade).