Uma visão geral do OpenLDAP e Active Directory para autenticação de usuários em sistemas heterogêneos e distribuídos

Guilherme M. Macedo, Rafael Bohrer Ávila e Philippe O. A. Navaux
Instituto de Informática/UFRGS
Caixa Postal 15064
91501-970 Porto Alegre – Brasil
Email: {gmmacedo, avila, navaux}@inf.ufrgs.br

Resumo

The OpenLDAP and Active Directory are the most used implementations of the LDAP protocol (Lightweight Directory Access Protocol) for querying and modifying directory services. It is used, nowadays, more than ever, for being a communication protocol that makes easy for heterogeneous and distributed systems to access information common to many systems quick and painlessly. This paper will explain briefly what is the OpenLDAP and Active Directory and how they can be used to make user authentication between different systems easier and simpler.

1. Introdução

Com a disseminação das redes de computadores e de sistemas distribuídos e heterogêneos, a necessidade de se manter informações em vários pontos e comuns a vários sistemas de uma rede cresceu. Para solucionar tal problema, na década de 1980 a ITU (International Telecommunication Union) e a ISO (International Organization for Standardization) definiram o padrão X.500 para diretórios de serviços [1].

Um diretório de serviços é muito parecido com um banco de dados, no entanto, ao contrário deste aquele visa à disponibilizar resultados de buscas de forma extremamente eficiente, já que os dados contidos nele são, na maioria da vezes, atualizados menos frequentemente. Fato que permite que os mesmos possam estar espalhados por vários computadores de uma rede, e que não haja a necessidade de mecanismos de transação e *rollback* [1], o que diminui a complexidade do sistema.

1 Mecanismo utilizado em Bancos de Dados aonde uma transação, caso falhe, pode ser desfeita

Atualmente existem várias implementações de diretórios de serviços, sendo o OpenLDAP e o Active Directory as mais utilizadas. Ambas as implementações serão explicadas a seguir. Além disto, este artigo citará como elas podem ser utilizadas para a autenticação de usuários em sistemas distribuídos.

2. OpenLDAP

O OpenLDAP é uma implementação livre e de código fonte aberto do protocolo LDAP (Lightweight Directory Access Protocol) desenvolvido pelo projeto OpenLDAP.

O OpenLDAP inclui um servidor e várias ferramentas para auxiliar nas consultas, adição e remoção de informações, entre outros utilitários.

2.1. O protocolo LDAP

O LDAP é um protocolo para consulta e modificação de informações em diretórios de serviços. Um exemplo clássico de diretório é uma lista telefônica, onde as informações possuem atributos em comum e são organizadas lógica e hierarquicamente. Esta implementação do protocolo LDAP, baseada originalmente no protocolo X.500, foi criada por Tim Howes, Steve Kille e Wengyik Yeong.

2.2. Estrutura de Diretório

Conforme pode ser visto em [2] um diretório é uma árvore de entradas de diretórios, cada entrada é composta por um conjunto de atributos, cada um possui um nome e um conjunto de valores. Cada entrada no diretório possui um identificador único, o seu *Distinguished Name* (DN), que é composto por um *Relative Distinguished Name* (RDN) – um atributo da entrada – e o DN

da entrada pai. Na figura 1 há o exemplo de uma entrada em um diretório.

```
dn: cn=John Doe,dc=example,dc=com
cn: John Doe
fn: John
sn: Doe
phone: 1 2345 6789
mail: john@example.com
```

Figura 1. Exemplo de uma entrada em um diretório

No exemplo acima, o RDN da entrada é “cn=John Doe”, o DN da entrada pai é “dc=example,dc=com”, e o DN da entrada em sí é: “dn: cn=John Doe,dc=example,dc=com”; que é formada pelo RDN e pelo DN da entrada pai.

3. Active Directory

O Active Directory (AD) é a implementação do protocolo LDAP, feita pela Microsoft Corp., e que é utilizada para a autenticação de usuários para o ambiente Windows. Uma diferença em relação a outras implementações é que se pode utilizar o AD para distribuir e realizar atualizações de programas em uma organização de acordo com [3].

A organização de diretórios no AD é basicamente a mesma utilizada pelo OpenLDAP, já que ambos se baseiam no padrão LDAP.

Um fator importante do Active Directory para a autenticação de usuários em sistemas distribuídos e heterogêneos, é o fato de o AD possuir interoperabilidade com plataformas UNIX através do “Services for UNIX” (SFU). Que é um conjunto de programas comumente encontrados nas plataformas UNIX e que permite ao administrador do diretório de serviços se comunicar com outros diretórios em sistemas UNIX. Maiores informações sobre o SFU podem ser obtidas em [4]

4. Autenticação de usuários

O OpenLDAP e o Active Directory, com o auxílio do “Services for UNIX”, permitem que se possa realizar a autenticação de usuários de diferentes sistemas rodando sobre arquiteturas heterogêneas, conforme apresentado em [5].

Para realizar tal tarefa, é necessário criar entradas em um diretório na máquina servidora, que irá conter os dados de cada usuário, no caso, os logins e as senhas. Feito isto, a próxima parte é configurar cada máquina cliente com os dados da máquina servidora e do diretório, para que cada uma possa efetuar a autenticação no servidor de diretório de serviços. Liberada a autenticação, cada pessoa possuirá agora acesso aos recursos disponibilizados pelo servidor.

Embora os passos tenham sidos simplificados, a configuração e a administração de usuários, com o auxílio de um diretório de serviços, torna-se relativamente fácil em um ambiente distribuído e heterogêneo. Já que permite padronizar e centralizar, caso se deseje, as informações sobre os usuários. Possibilitando que a autenticação se torne mais segura e independente da plataforma que cada um utiliza para o acesso aos recursos dos sistemas.

5. Conclusões

Com a proliferação de sistemas distribuídos, manter informações essenciais e comuns aos mesmos se torna cada vez mais difícil. Devido ao fato de muitos sistemas serem heterogêneos, a complexidade da tarefa aumenta. Para resolver este problema, um diretório de serviços é a solução mais simples, pois informações em diferentes sistemas podem ser acessadas de maneira simples, rápida e segura. Tal fato, torna o diretório a solução ideal para a autenticação de usuários a um servidor, pois permite que as informações necessárias, no caso os dados dos logins de cada usuário, sejam mantidas de forma independente de cada um e de modo que todos os sistemas da rede possam acessar.

Referências

[1] Wikimedia Foundation, Inc., http://en.wikipedia.org/wiki/Directory_service, acessado em Julho/2007.

[2] Wikimedia Foundation, Inc., http://en.wikipedia.org/wiki/Ldap, acessado em Julho/2007.

[3] Wikimedia Foundation, Inc., http://en.wikipedia.org/wiki/Active_directory, acessado em Julho/2007.

[4] Microsoft Corporation, technet.microsoft.com/en-us/interopmigration.aspx, acessado em Julho/2007.

[5] Núcleo de Desenvolvimento Open Source e Interoperabilidade, www.codeplex.com/NDOS, acessado em Julho/2007.