Universidade Federal do ABC

Centro de Matemática, Computação e Cognição

Uso do protocolo LDAP no Sistema de Reservas

Autor: Erick Alves Augusto

Santo André

2017

SUMÁRIO

1. INTRODUÇÃO

O protocolo LDAP (Lightweight Directory Access Protocol) é um protocolo usado para acessar diretórios distribuídos pela rede. Um sistema de diretórios permite que dados possam ser localizados dentro da rede interna da corporação que o utiliza. Diferente de um banco de dados, ele foi criado para suportar a uma grande quantidade de consultas simultâneas de registros e sofrendo poucas alterações como escrita e atualizações de registros dos dados armazenados.

O LDAP foi desenvolvido pela universidade de Michigan em 1993 para substituir o protocolo DAP que acessava o sistema de diretórios X.500. O DAP trabalhava com o padrão OSI e era extremamente pesado, já LDAP é mais leve e trabalha com o TCP/IP, o que o torna muito mais portável entre sistemas que fazem o acesso ao LDAP via rede.

A estrutura de armazenamento dos dados é hierárquica, o que também difere de um banco de dados, onde a distribuição é relacional. A estrutura do protocolo LDAP é caracterizada no formato de uma árvore, ou uma forma específica de grafo, chamada DIT (Directory Information Tree).

Um exemplo da estrutura da DIT pode ser observado na fugira 1.

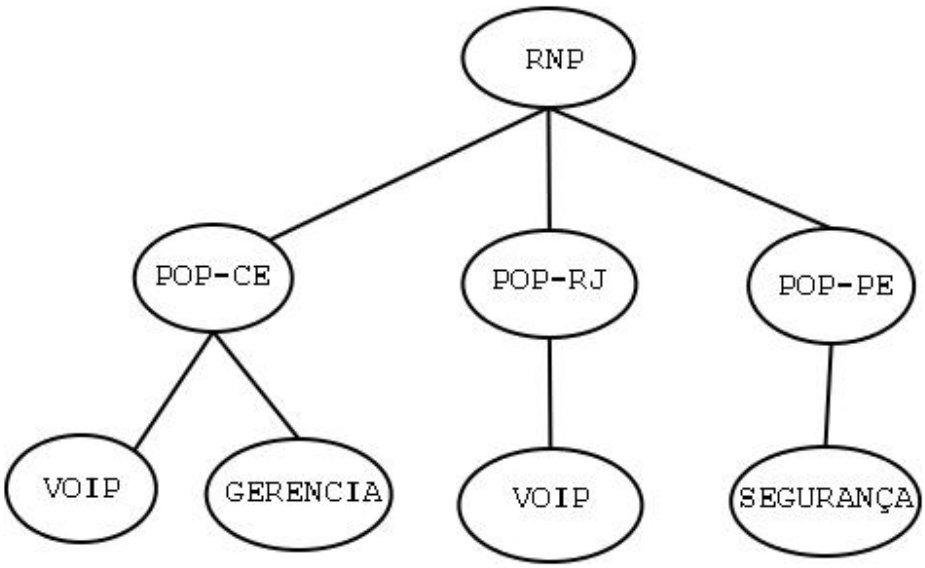

Figura 1 – Estrutura de uma Directory Information Tree

A DIT é uma árvore enraizada, então existe um diretório principal de onde os outros emergem por meio de arestas, ou relacionamentos, para poderem ser acessados. Na DIT cada vértice representa um registro, onde estão armazenadas as informações de determinado objeto. As informações armazenadas em um registro são determinadas por uma object class que define que atributos aquele registro deverá ter. Cada registro deve ter um único DN (distinguished name) para fazer a identificação e do registro e especificar o caminho a partir do diretório raiz.

2. FUNCIONAMENTO

A estrutura de diretórios é mantida centralizada dentro da rede onde ela está localizada, embora os diretórios sejam distribuídos fisicamente. Então a busca de dados é realizada pela hierarquia desses diretórios usando seus identificadores.

No caso do LDAP as buscas de dados nos registros são feitas com base no caminho da raiz até o registro onde os dados estão armazenados, então umas busca seria da forma: raiz.diretório1.diretório2.informação.

Após ser localizado o diretório onde os dados desejados estão armazenados, os dados podem ser acessados pelo solicitante.

3. PROBLEMAS COM O SERVIDOR LDAP

A UFABC usa um servidor LDAP para armazenar os e-mails institucionais e logins dos alunos e funcionários da instituição. Isso possibilita que os usuários possam ter acesso a diferentes serviços oferecidos pela universidade sem ter que criarem diferentes contas. Todo o acesso dentro da rede interna da UFABC é feito através do LDAP.

Como o servidor LDAP da UFABC é uma conectada a rede interna. só é possível acessar o servido por meio de uma porta de rede. Para ter acesso a essa porta a máquina solicitante do serviço deve ter uma permissão de acesso que é concedida pelo NTI (Núcleo de Tecnologia da Informação).

O CMCC (Centro de Matemática, Computação e Cognição) possui aplicações que rodam em servidores internos da UFABC e que acessam o servidor LDAP para fazer autenticação dos seus usuários. Uma aplicação que precisa desse serviço é a aplicação de Reserva de Salas.

Essa aplicação é muito utilizada pelo CMCC para organizar o uso das salas de reunião e equipamentos disponíveis no setor. Para que apenas usuários credenciados possam ter acesso a essa aplicação de forma segura foi implementado dentro da aplicação o acesso ao servidor LDAP, assim cada usuário poderia utilizar o seu login institucional sem precisar memorizar um novo login e como as senhas não ficariam armazenadas na aplicação elas não correriam o risco de ser acessadas por meio de uma invasão do servidor onde a aplicação está armazenada.

Devido a falta de conhecimento sobre o funcionamento do servidor LDAP ocorreram problemas de acesso ao mesmo. Inicialmente, o acesso ao servidor foi impedido devido a mudanças nas configurações do firewall da rede interna da UFABC. Após a verificação da causa do problema foi feita a solicitação da reativação da permissão de acesso remoto ao servidor onde a aplicação estava armazenada.

Após o problema de acesso ao servidor ser resolvido a aplicação passou a não responder mais à solicitação de acesso dos usuários. Foram feitas alterações para que a

aplicação pudesse ser acessada por meio de um usuário primário que não precisasse ser autenticado via LDAP, esse usuário estava registrado diretamente no código do programa.

Foram feitas pesquisas sobre o funcionamento do LDAP para poder descobrir a origem do problema. Esse estudo abrangeu a estrutura de diretórios do LDAP e o seu funcionamento. Por fim, foi descoberto que para ter acesso ao LDAP em um servidor diferente ao da máquina que solicita o serviço era preciso acessar uma determinada porta que estava configurada para receber as solicitações de consulta do servidor LDAP.

A aplicação de reservas já estava configurada para direcionar as solicitações de consulta para a porta do servidor LDAP da UFACB, porém, o acesso não estava sendo realizado. O problema foi informado ao NTI que verificou que a permissão do servidor, onde a aplicação de reservas está alocada, havia sido restrita após as mudanças nas configurações do firewall. Então foi aberto um chamado para que o NTI pudesse habilitar novamente o acesso ao servidor LDAP para que a aplicação de Reserva de Salas pudesse voltar a operar usando os logins institucionais.

Após a correção desses problemas a aplicação de Reserva de Salas voltou a operar normalmente. Caso hajam futuros problemas com o servidor LDAP, já é conhecido que o problema pode decorrer da mudança nas permissões de acesso do servidor, sendo necessário abrir um chamado para que a permissão seja reabilitada.

4. BIBLIOGRAFIA

[1] F. J. R. Maia, "Entendendo o LDAP". Avaliable: http://www.vivaolinux.com.br/artigo/Entendendo-o-LDAP?pagina=1 Acessado em 26 de Novembro de 2015.