capítulo 1

Conceitos, Arquitetura e Design

1.1 – O que são os serviços de diretórios?

Segundo a Wikipédia:

"Um **serviço de diretório** é um software que armazena e organiza informações sobre os recursos e os usuários de uma rede de computadores, e que permite aos administradores de rede gerenciar o acesso de usuários e sistemas a esses recursos. Além disso, os serviços de diretório atuam como uma camada de abstração entre os usuários e esses recursos.

A palavra directory em inglês poderia ser melhor traduzida por catálogo, no sentido de uma lista ordenada com descrição curta dos itens, não necessariamente de arquivos."

A sua primordial diferença está na forma como os recursos são tratados. Entenda por recursos todos os componentes de uma rede de computadores, como compartilhamentos, configurações, usuários, senhas, permissões e mais.

1.2 – Qual sua utilidade?

Permitir a centralização de gestão dos recursos da rede, visando simplificar a administração, o backup e a replicação. Centralização é a palavra-chave de todas as facilidades encontradas no uso de um serviço de diretórios.

1.3 – O que é LDAP?

LDAP é um protocolo. Como todos os protocolos, sua função é definir a forma de funcionamento de um serviço de diretórios, especificando critérios, mecanismos e métodos para armazenar e fornecer informações. LDAP – "Lightweight Directory Access Protocol" ou Protocolo Leve de Acesso a Diretórios – é um conjunto de protocolos desenhados para acessar informação centralizada em uma rede. Esse conjunto de protocolos serve para interagir com o Serviço de Diretório. Assim, as regras de acesso ao diretório estão definidas no LDAP. O LDAP é definido para uso em sistemas Cliente-Servidor, permitindo a um cliente LDAP consultar ou alterar o diretório comunicando-se com o servidor LDAP. É multiplataforma.

O servidor LDAP tem a função de verificar as credenciais do cliente, verificar se as informações solicitadas estão armazenadas neste servidor e permitir ou não que o cliente realize consultas e modificações. As formas de armazenamento dos dados, o tipo de gerenciador de bancos de dados usado e o sistema operacional de base não fazem parte do protocolo. Fazem parte da implementação específica do LDAP.

A manutenção de um cadastro centralizado de usuários é um grande desafio para o administrador de TI. A rotatividade de colaboradores e a mobilidade na hierarquia tornam difícil a manutenção de informações coerentes sobre determinado recurso de uma organização.

O grande número de sistemas e a heterogeneidade de plataformas fazem com que a manutenção de senhas e identidades seja um grande desafio. É repetidamente motivo para escolha de senhas frágeis e vazamento de informações.

O uso do LDAP permite que colaboradores, aplicativos e recursos de rede possam usar informações armazenadas em um repositório central. Isso unifica os esforços de criação, manutenção da base de informações. O LDAP permite a consulta a informações cadastrais, o que permite sua utilização como agenda de contatos central da organização, um dos primeiros usos para o protocolo.

Como vantagens do LDAP podemos citar:

- Por ser um padrão aberto, a interoperabilidade entre os diversos fornecedores é facilitada. Um cliente LDAP baseado em OpenLDAP pode perfeitamente realizar consultas e atualizações em um servidor de outro fornecedor que siga os padrões LDAP. O LDAP é um protocolo. As implementações podem trazer novas interfaces e ferramentas de administração e consulta, mas os métodos básicos são definidos no protocolo;
- API ("Application Programming Interface", Interface para Programação) bem definida e com suporte para diversas linguagens de programação;
- Muito mais rápido que Sistemas de Bancos de Dados (considerando que atualizações são menos constantes que consultas);
- Esquemas (regras para o armazenamento de dados) padronizados existem para diferentes funções;
- Permite a consolidação de informações de várias fontes;
- Facilmente replicável e distribuível.

1.4 – Qual é a estrutura de uma base LDAP?

Uma base LDAP busca organizar as informações em forma de diretório, ou seja, em forma de "árvore". As partes que permitem essa formação são as especificações do protocolo.

Baseando-se em campos, chamados de atributos, e em seus conjuntos, chamados de schemas, é possível armazenar praticamente qualquer tipo de informação de forma estruturada, o que facilita sua administração.

Cada ramificação da "árvore" pode ser um departamento da organização, permitindo ter um efeito visual organizacional da base.

1.5 – Entendendo os diretórios

O primeiro passo para entender como uma base LDAP está estruturada é realizar um exercício mental para eliminar quaisquer outros conceitos pre-existentes. Um erro muito comum é tentar estabelecer elos com bases de dados SQL ou DB.

Bases LDAP têm uma estrutura muito singular e qualquer comparação servirá apenas para criar confusão, especialmente para os iniciantes. Portanto, evite as comparações e abra a mente para entender algo completamente novo.

Visando simplificar o entendimento, vamos utilizar a palavra diretório com o seu mais conhecido conceito: o de pasta de armazenamento de arquivos e outros diretórios.

Sabemos que um diretório no sistema de arquivos nada mais é do que uma divisão lógica que visa organizar os arquivos existentes no disco rígido. Pense no LDAP nos mesmos termos. Assim começa a ficar claro que a estrutura de uma base LDAP é completamente diferente de qualquer outra base de dados comum.

Em um sistema de arquivos o diretório principal chama-se raiz e isso deve-se a sua estrutura em forma de "árvore". O LDAP mantém essa mesma ideia, ou seja, a partir da "raiz da árvore" estão suas ramificações, que permitem a organização lógica dos arquivos.

Assim como em uma estrutura de diretórios, o LDAP permite a existência de outros diretórios dentro de um diretório já existente. Portanto, cada novo diretório é raiz em si mesmo para todo o seu conteúdo.

Em um diretório não é permitido ter arquivos com o mesmo nome e isso faz sentido, afinal, é fundamental ter apenas um nome que identifique cada arquivo.

Uma vez compreendido que a base LDAP funciona como um diretório de um sistema de arquivos, basta fazer a relação entre arquivos e recursos. Em uma base LDAP não se armazenam arquivos, mas sim recursos de rede, como usuários e senhas, por exemplo.

Assim como em alguns sistemas de arquivos existem regras para a criação de arquivos, a base LDAP também possui regras para o armazenamento de recursos. Estas regras são muito mais complexas do que simplesmente limitar o número de caracteres no nome de um arquivo, afinal trata-se do armazenamento de dados.

Estas regras (ou limites) são impostas pela definição do protocolo e elas têm que ser respeitadas. Caso contrário, a base simplesmente negará a adição de informações.

Qual informação e qual conteúdo podem ser adicionados são definidos pelos atributos e seus conjuntos, as ObjectClasses. Portanto, quanto mais schemas sua base LDAP tiver, mais flexível ela será, permitindo o armazenamento de mais recursos. O conjunto de ObjectClasses e atributos é chamado de “schemas”.

1.6 – Registros em uma base LDAP

Como foi visto antes, as regras para adicionar um registro em uma base LDAP são muito mais complexas do que para criar um arquivo em um diretório comum, em um sistema de arquivos.

Entretanto, a similaridade está no fato de que não pode haver dois registros iguais em um mesmo diretório. Para garantir essa unicidade para todos os registros utiliza-se o identificador DN (Distinguished Name).

Um registro único pode conter diversos objetos e atributos, de acordo com sua finalidade. Aqui vemos um exemplo de registro único:

```
cn=”Anahuac de Paula Gil”,ou=Usuarios,dc=kyapanel,dc=com
```

É importante entender o que está descrito. Esta é uma descrição do formato padrão que deve ser utilizado em nome da compatibilidade com os diversos serviços que oferecem suporte a bases LDAP. Portanto, não é obrigatório, mas extremamente desejável.

Quando uma base LDAP é criada é necessário definir a raiz da "árvore" do diretório. Esta raiz normalmente é definida pelo atributo "domainComponent", também conhecido como "dc", com o nome do domínio da internet da organização.

Neste exemplo: `dc=kyapanel,dc=com`

Dentro da raiz foi criado um outro "galho" da "árvore" chamado Usuarios, cujo atributo é ou (Organizational Unit).

Neste exemplo: `ou=Usuarios`

Finalmente, dentro do "galho" Usuarios foi criado um usuário cuja identificação única está sendo feita pelo atributo cn (Common Name).

Neste exemplo: `cn="Anahuac de Paula Gil"`

Pode-se também referenciar um usuário utilizando o atributo uid em vez de cn, entretanto o padrão é usar o cn.

O objeto final, que é o usuário, poderá e deverá conter diversos atributos para atender às exigências de diversos servidores. Por exemplo:

```
dn: cn="Anahuac de Paula Gil",ou=Usuarios,dc=kyapanel,dc=com
uid: anahuac
sn: anahuac
objectClass: top
objectClass: person
objectClass: qmailUser
homeDirectory: /home/anahuac
userPassword::e1NTSEF9MGNjcXJKTEVOQU9nTSswR2l4TVRtelhBWERObng5cFU=
cn: Anahuac de Paula Gil
mail: anahuac@anahuac.org
```

Perceba que o primeiro registro contém o identificador único: "dn:"

Para efeito de comparação, teríamos o usuário anahuac dentro do diretório Usuarios que está dentro da raiz kyapanel.com. Visualizando:

```
dc=kyapanel,dc=com
|
--------> ou=Usuarios
     |
     --------> cn="Anahuac de Paula Gil"
```

O objetivo de manter as informações assim é simplesmente para facilitar a localização e, consequentemente, facilitar a administração dos recursos.

1.7 – Resumindo

1. A base LDAP tem um funcionamento similar aos diretórios dos sistemas de arquivos. Portanto, não há nenhuma relação direta com bases de dados SQL.
2. A base LDAP armazena recursos e não arquivos.
3. A base LDAP utiliza um conjunto de objetos e atributos para fazer esse armazenamento.
4. O conjunto de objetos e atributos é chamado de schema e não passa de um arquivo texto que deve ser lido pela base LDAP para que possa ser usado.
5. Um objeto é chamado de ObjectClass e ele é composto de atributos obrigatórios e atributos opcionais.
6. Um atributo é uma definição de campo, contendo a definição de que tipo de valor ele pode armazenar.
7. Dentro de uma base LDAP cada registro é único, ou seja, não é permitido dois registros iguais em um mesmo diretório.