

Redes de Computadores II

Aula 07 - Autenticação e Compartilhamento de arquivos – Parte II

Apresentação

Na aula passada entendemos como pode ser realizado o processo de autenticação e controle de acesso em computadores através de um protocolo de aplicação aberto e padrão para manter serviços de informação de diretório distribuído sobre uma rede TCP/IP.

Nesta aula iremos dar enfoque a parte prática, desde a instalação de um servidor LDAP no Linux, partindo para sua configuração e por fim na sua utilização. Para esta aula utilizaremos a implementação do LDAP conhecida como *OpenLDAP*.

Objetivos

Após estudar o conteúdo desta aula, você será capaz de:

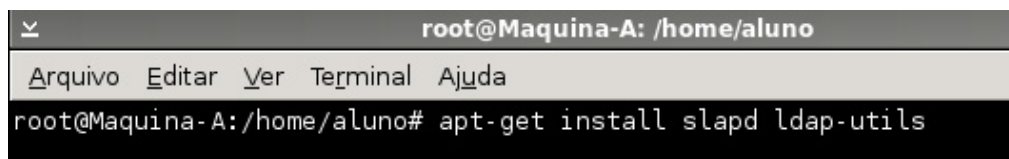
- Instalar e configurar um servidor LDAP no Linux.
- Inserir e consultar dados no servidor LDAP usando programas de linha de comando.
- Inserir e consultar dados no servidor LDAP usando um programa com interface gráfica.

LDAP na Prática

Vamos ver agora como instalar um servidor LDAP na prática. Usaremos o programa *Openldap*, que é uma implementação do LDAP de código aberto, e faremos a instalação em uma máquina Linux.

Para instalar o pacote Openldap no Linux, utilize o comando mostrado na Figura 11. O servidor ldap está contido no pacote slapd, mas o pacote ldap-utils contém vários programas para realizar operações no servidor. Portanto, ele será necessário, por exemplo, para inserirmos objetos no servidor.

Figura 01 - Instalando o Openldap no Linux.



```
root@Maquina-A: /home/aluno
Arquivo Editar Ver Terminal Ajuda
root@Maquina-A:/home/aluno# apt-get install slapd ldap-utils
```

Fonte: Autoria Própria

Para configurar o servidor precisaremos realizar três passos, que são:

- Informar ao servidor os *esquemas* que pretendemos suportar. Isso define quais tipos de objetos podem ser inseridos no servidor.
- Criar o arquivo de configuração e ativar a configuração.
- Criar os nós da árvore LDAP.

Após esses passos, as informações a serem armazenadas podem ser inseridas nos nós da árvore LDAP.

Antigamente, o LDAP era configurado através de um arquivo chamado slapd.conf. Embora esse método ainda possa ser usado, ele está obsoleto. A forma recomendada atualmente para configurar um servidor LDAP é a descrita nesta aula.

a. Informar ao servidor os esquemas suportados

É necessário avisar ao servidor quais esquemas são suportados. Naturalmente, isso vai depender de para que você vai utilizar o LDAP.

Vamos inserir três esquemas que já vem com o LDAP e são muito usados para armazenar informações dos usuários Linux. Os esquemas são: cosine.ldif, nis.ldif, e inetorgperson.ldif. A seguir, mostramos os três comandos (que devem ser executados como root) para instalar esses esquemas.

```
ldapadd -Y EXTERNAL -H ldapi:/// -f /etc/ldap/schema/cosine.ldif
```

```
ldapadd -Y EXTERNAL -H ldapi:/// -f /etc/ldap/schema/nis.ldif
```

```
ldapadd -Y EXTERNAL -H ldapi:/// -f /etc/ldap/schema/inetorgperson.ldif
```

LDAP na Prática

b. Criar o arquivo de configuração e ativar a configuração

Vamos agora criar o arquivo de configuração do servidor. Apesar de o arquivo possuir muitos parâmetros, você realmente só precisa alterar poucos desses parâmetros. Como um deles será a senha do administrador do LDAP, antes de alterarmos o arquivo, vamos gerar uma senha. Isso pode ser feito com o comando `slappaswd`, conforme mostrado na Figura 12. No exemplo, a senha informada foi `teste123`, o que gerou a senha criptografada `{SSHA}vVi6+5ZybDaVo90pIXg9XqF1pYkk67+s`.

Figura 02 - Gerando senha para o arquivo de configuração do LDAP.

```
root@Maquina-A: /home/aluno
Arquivo Editar Ver Terminal Ajuda
root@Maquina-A: /home/aluno# slappasswd
New password:
Re-enter new password:
{SSHA}vVi6+5ZybDaVo90pIXg9XqF1pYkk67+s
root@Maquina-A: /home/aluno#
```

Na Figura 3, mostramos um arquivo de configuração que foi criado para a árvore mostrada na Figura 9, e você pode utilizar como base para o seu servidor LDAP. Os únicos valores que você precisa alterar estão marcados em vermelho e significam:

- *olcSuffix*: *o=ufrn*. O nome do nó raiz da sua árvore.
- *olcRootDN*: *cn=admin,o=ufrn*. O nome do usuário administrador do LDAP. Você usará esse nome sempre que for realizar operações no LDAP que precisem de privilégios de administrador. Basta alterar valor *o=ufrn* para o valor que tiver utilizado no campo *olcSuffix* (descrito no item anterior).
- *olcRootPW*: *{SSHA}vVi6+5ZybDaVo90pIXg9XqF1pYkk67+s*. A senha do usuário administrador do LDAP definido no item anterior. Coloque aqui o valor obtido com o comando *slappasswd*, conforme mostrado na Figura 2.
- *olcAccess*. São as permissões que o usuário administrador do LDAP tem. Portanto, onde aparece *dn="cn=admin,o=ufrn"*, coloque o mesmo valor que informou para o campo *olcRootDN*, explicado anteriormente.

```
1 # Load dynamic backend modules
2 dn: cn=module,cn=config
3 objectClass: olcModuleList
4 cn: module
5 olcModulepath: /usr/lib/ldap
6 olcModuleload: back_hdb
7 # Database settings
8 dn: olcDatabase=hdb,cn=config
9 objectClass: olcDatabaseConfig
10 objectClass: olcHdbConfig
11 olcDatabase: {1}hdb
12 olcSuffix: o=ufrn
13 olcDbDirectory: /var/lib/ldap
14 olcRootDN: cn=admin,o=ufrn
15 olcRootPW: {SSHA}vVi6+5ZybDaVo90pIXg9XqF1pYkk67+s
16 olcDbConfig: set_cachesize 0 2097152 0
17 olcDbConfig: set_ik_max_objects 1500
18 olcDbConfig: set_ik_max_locks 1500
19 olcDbConfig: set_ik_max_lockers 1500
20 olcDbIndex: objectClass eq
21 olcLastMod: TRUE
22 olcDbCheckpoint: 512 30
23 olcAccess: to attrs=userPassword by dn="cn=admin,o=ufrn" write by anonymous auth by self write
24 olcAccess: to attrs=shadowLastChange by self write by * read
25 olcAccess: to dn.base="" by * read
26 olcAccess: to * by dn="cn=admin,o=ufrn"
```

Figura 3 - Arquivo de configuração do servidor LDAP.

Salve esse arquivo (com suas modificações) no diretório `/etc/ldap` com o nome `ldapconfig.ldif`, e digite o seguinte comando (como *root*), para ativar suas configurações.

```
ldapadd -Y EXTERNAL -H ldapi:/// -f /etc/ldap/ldapconfig.ldif
```

LDAP na Prática

c. Criar os nós da árvore LDAP

Como última etapa para terminar a criação da nossa base LDAP vamos criar os nós da árvore. Posteriormente, as aplicações que forem utilizar essa base LDAP vão inserir os objetos contendo as informações a serem armazenadas dentro desses nós. Como exemplo, vamos criar os nós "ufrn", "Caicó", "Natal" e "Mossoró".

A criação desses nós também é feita utilizando um arquivo ldif, que está mostrado na Figura 4.

As primeiras quatro linhas definem o nó raiz (isso é indicado pelo campo `objectClass: top`). O campo `"objectClass: organization"` define que o nó é do tipo Organização ("o"). O campo "o" define o nome abreviado desse nó e o campo "dn", além de definir o nome completo do nó (que é único), indica em que posição da árvore o nó se encontra. Como o valor de dn (o=ufrn) é o próprio nome do nó, significa que não existe ninguém acima dele, como deve ser já que ele é o nó raiz.

Cada grupo de três linhas define um nó abaixo da raiz. Cada nó é do tipo "ou", conforme indicado pelo campo `"objectClass: organizationalUnit"`. O valor do campo "ou" indica o nome abreviado do nó e o campo dn indica tanto o nome completo (que é único) quanto a posição na qual o nó se encontra na árvore. A posição é calculada retirando-se o valor do nome abreviado do valor do campo dn. Assim, para o nó "caico", que possui o nome abreviado "ou=caico", se retirarmos isso do valor do dn "ou=caico,o=ufrn", temos que esse nó fica abaixo do nó com o dn "o=ufrn", que é o nó raiz.

```

1 dn: o=ufrn
2 objectClass: top
3 objectclass: organization
4 o:ufrn
5 dn: ou=caico,o=ufrn
6 objectClass: organizationalUnit
7 ou: caico
8 dn: ou=natal,o=ufrn
9 objectClass: organizationalUnit
10 ou: natal
11 dn: ou=mossoro,o=ufrn
12 objectClass: organizationalUnit
13 ou: mossoro

```

Figura 4 - Arquivo LDIF para criar os nós da árvore.

Se quiséssemos inserir o nó “Medicina” abaixo do nó “Mossoró”, bastava inserir as linhas mostradas na Figura 15 no arquivo mostrado na Figura 4. Lembre-se que deve existir uma linha em branco entre a definição de dois nós da árvore.

```

1 dn: ou=medicina,ou=mossoro,o=ufrn
2 objectClass: organizationalUnit
3 ou: medicina

```

Figura 5 - Inserindo o nó “Medicina” abaixo do nó “Mossoró”.

Salve o arquivo mostrado na Figura 4 como `cria_arvore.ldif` na pasta `/etc/ldap`. Agora que o arquivo `ldif` está criado, basta executar o seguinte comando para que os nós da árvore sejam criados.

```

1 ldapadd -x -D cn=admin,o=ufrn -W -f /etc/ldap/cria_arvore.ldif

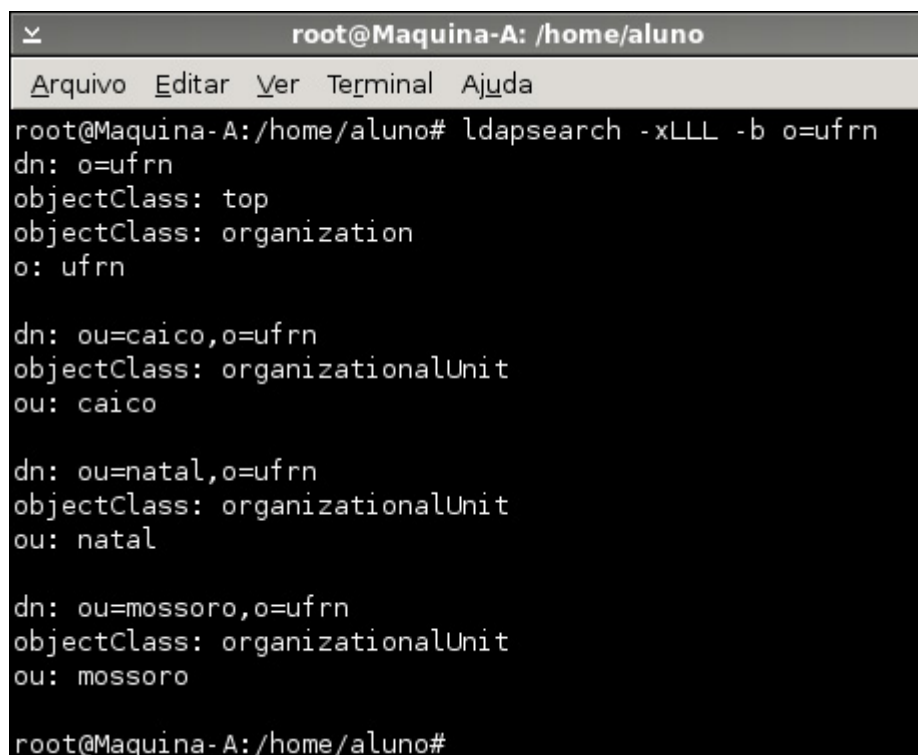
```

Será pedida a senha do usuário “`cn=admin,o=ufrn`”, que foi o usuário que você informou no arquivo de configuração do servidor LDAP (parâmetro `olcRootDN`), mostrado na Figura 3. Portanto, informe a senha colocada nesse mesmo arquivo (no parâmetro `olcRootPW`), que foi gerada com o comando `slappasswd`, mostrado na Figura 2.

Se você informar a senha errada, aparecerá a mensagem “`ldap_bind: Invalid credentials (49)`”

Feito isso, seu servidor está pronto para ser utilizado! Se quiser verificar como está sua árvore, pode digitar o comando *ldapsearch*, conforme mostrado na Figura 6.

Figura 06 - Mostrando os nós criados.

A terminal window titled 'root@Maquina-A: /home/aluno' with a menu bar containing 'Arquivo', 'Editar', 'Ver', 'Terminal', and 'Ajuda'. The terminal shows the command 'ldapsearch -xLLL -b o=ufrn' and its output. The output lists four LDAP entries: the root organization 'o=ufrn', and three organizational units 'ou=caico', 'ou=natal', and 'ou=mossoro', all under the 'o=ufrn' domain. Each entry shows its 'dn' (distinguished name), 'objectClass' (top or organizationalUnit), and the specific value (o or ou).

```
root@Maquina-A:/home/aluno# ldapsearch -xLLL -b o=ufrn
dn: o=ufrn
objectClass: top
objectClass: organization
o: ufrn

dn: ou=caico,o=ufrn
objectClass: organizationalUnit
ou: caico

dn: ou=natal,o=ufrn
objectClass: organizationalUnit
ou: natal

dn: ou=mossoro,o=ufrn
objectClass: organizationalUnit
ou: mossoro

root@Maquina-A:/home/aluno#
```

O *ldapsearch* mostra o conteúdo do servidor incluindo os nós da árvore e os objetos armazenados nesses nós. No nosso caso, só apareceram os nós porque ainda não temos nenhum objeto armazenado dentro deles.

Além disso, observe que o *ldapadd* pode ser utilizado para inserir os objetos dentro dos nós. O que determina o tipo de informação inserida é o conteúdo do arquivo *ldif*!

Veja aqui a explicação em vídeo sobre a configuração do servidor ldap.



Vídeo 01 - Configuração LDAP



Vídeo 02 - LDAP Administração

Atividade 01

1. O que significam os parâmetros *olcRootDN* e *olcRootPW* no arquivo de configuração do servidor LDAP?
2. Na árvore LDAP criada, quantas e quais são as unidades organizacionais?

LDAP na Prática

d. Inserindo objetos dentro dos nós da árvore

Nós vimos até agora como criar uma árvore LDAP. Nesta seção, será mostrado o procedimento para inserir objetos dentro dos nós da árvore. Como poderemos ver, ele é semelhante ao procedimento de criar os nós: basta criar um arquivo *ldif* e executar o comando *ldapadd*.

Naturalmente, os dados contidos no arquivo *ldif* são referentes ao objeto que será incluído no diretório. Ou seja, os campos a serem informados dependem do esquema ao qual o objeto pertence. No arquivo *ldif* mostrado na Figura 8, o objeto a

ser criado pertence aos esquemas inetOrgPerson, posixAccount, shadowAccount. Sabemos disso, olhando os valores dos campos objectClass. Portanto, cada campo informado é de um desses esquemas.

Observe que o nome do campo que identifica o usuário não se chamará username, como usamos até aqui, mas sim uid, pois esse é o nome utilizado pelo Linux.

```
1 dn: uid=carlos,ou=direito,ou=natal,o=ufrn
2 objectClass: inetOrgPerson
3 objectClass: posixAccount
4 objectClass: shadowAccount
5 uid: carlos
6 sn: Silva
7 givenName: Carlos
8 cn: Carlos Silva
9 uidNumber: 1000
10 gidNumber: 10000
11 userPassword: password
12 loginShell: /bin/bash
13 homeDirectory: /home/carlos
14 shadowExpire: -1
15 shadowFlag: 0
16 shadowWarning: 7
17 shadowMin: 8
18 shadowMax: 999999
19 shadowLastChange: 10877
20 mail: carlos@metropoledigital.ufrn.br
21 homePhone: +55 (84) xx xx xx xx
```

Figura 7 - Arquivo LDIF para inserção de um objeto dentro de um nó da árvore.

Supondo que esse arquivo foi salvo com o nome cria_usuario.ldif na pasta /etc/ldap, bastaria digitar o comando a seguir para que o objeto contendo os dados do usuário fossem inseridos no LDAP.

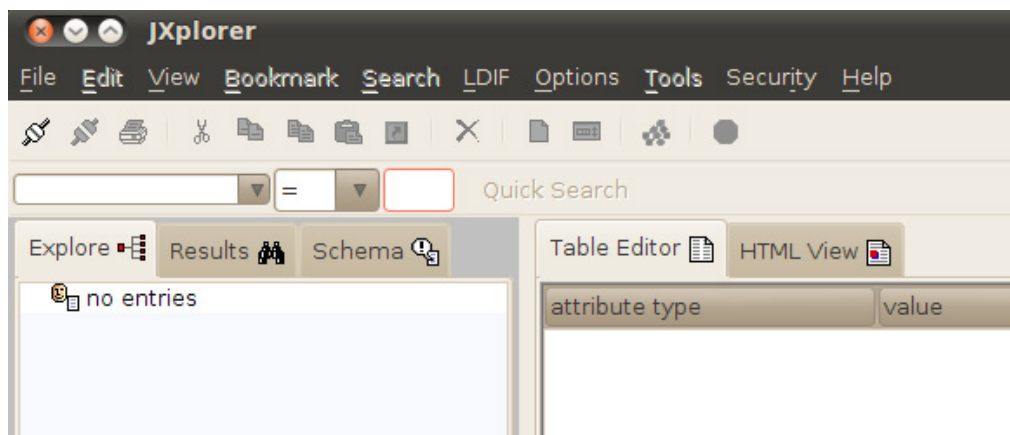
```
ldapadd -x -D cn=admin,o=ufrn -W -f cria_usuario.ldif
```

LDAP na Prática

e. Acessando o LDAP graficamente

Embora tenhamos mostrado que é possível utilizar a base LDAP através de comandos digitados no terminal, existem ferramentas gráficas (chamadas LDAP Browsers) para realizar todas as operações. Normalmente, o processo de criação da base de dados é realizado do modo que lhe mostramos, ou seja, através de comandos. Depois, usamos uma ferramenta gráfica, como o Jxplorer, cuja tela inicial é mostrada na Figura 8.

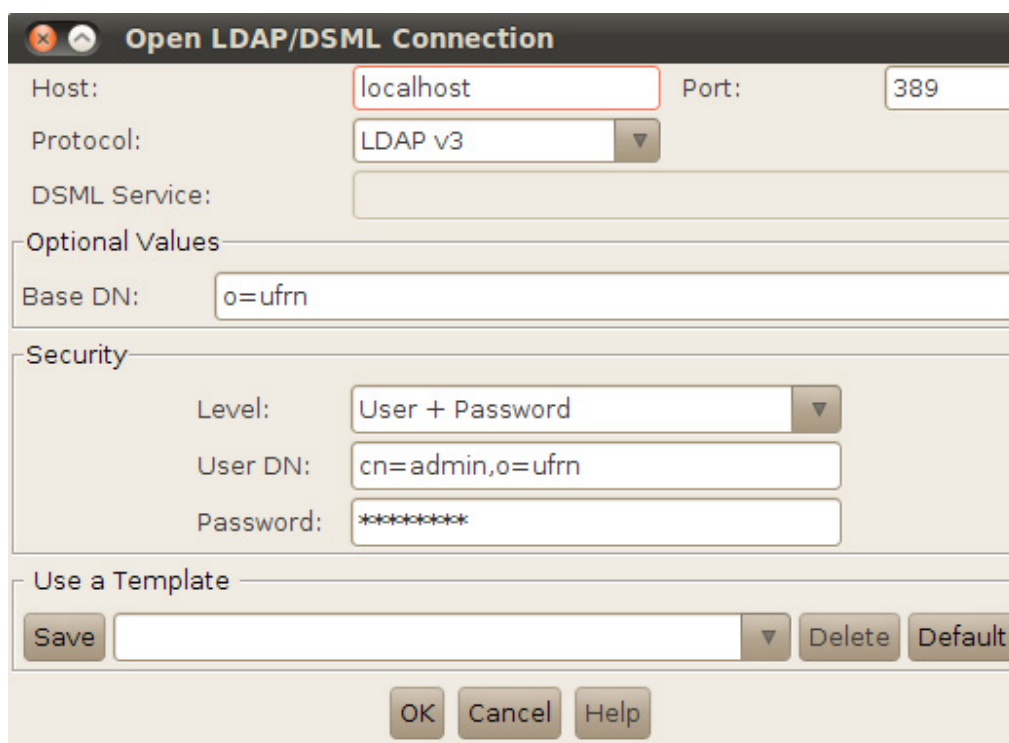
Figura 08 - Jxplorer: programa para administrar um servidor LDAP graficamente.



A primeira coisa a fazer é conectar no servidor LDAP. Para isso, clique no menu “File” e depois em “Connect”. Será, então, mostrada a tela da Figura 9. O campo *Host* deve ser preenchido com o endereço IP do servidor ou seu nome de DNS.

O servidor LDAP utiliza o protocolo TCP e espera conexões na porta 389. Por isso, digite 389 no campo *Port*. *Base DN* é o nó da árvore a partir de qual queremos ver as informações após a conexão. *User Level* indica o tipo de autenticação utilizado para se conectar no servidor. Caso não esteja utilizando criptografia, informe “*User + Password*”. Nos campos *User DN* e *Password*, informe os dados do administrador do LDAP. Depois clique em OK para conectar ao servidor.

Figura 09 - Tela de login do Jxplorer.



The image shows a dialog box titled "Open LDAP/DSML Connection". It contains several input fields and buttons. The "Host" field is set to "localhost" and the "Port" field is set to "389". The "Protocol" dropdown is set to "LDAP v3". The "DSML Service" field is empty. Under the "Optional Values" section, the "Base DN" field is set to "o=ufrn". Under the "Security" section, the "Level" dropdown is set to "User + Password", the "User DN" field is set to "cn=admin,o=ufrn", and the "Password" field is masked with asterisks. At the bottom, there is a "Use a Template" section with a "Save" button, a dropdown menu, and "Delete" and "Default" buttons. At the very bottom are "OK", "Cancel", and "Help" buttons.

Host: localhost Port: 389

Protocol: LDAP v3

DSML Service:

Optional Values

Base DN: o=ufrn

Security

Level: User + Password

User DN: cn=admin,o=ufrn

Password: *****

Use a Template

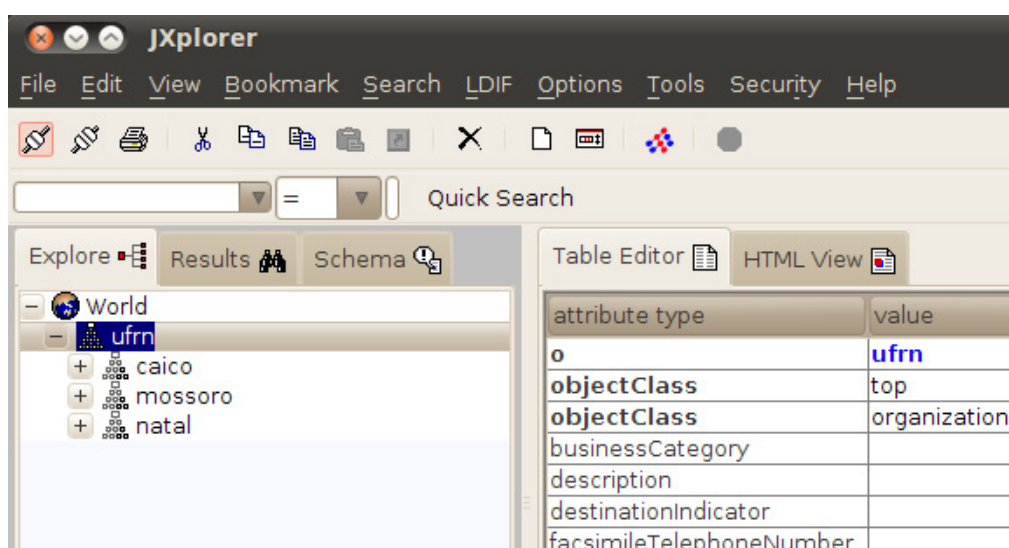
Save [dropdown] Delete Default

OK Cancel Help

Após isso, a conexão será mostrada na tela (Figura 10). Veja que para o nosso servidor de exemplo já aparecem os nós da árvore criada.

Clicando sobre um nó, aparecerão na parte direita os campos que compõem o nó. Não entraremos em maiores detalhes sobre a interface desse programa, mas em "Schema" você pode ver todos os esquemas que esse servidor suporta, além dos campos que existem em cada um. Veja por exemplo o esquema *posixAccount*, que será usado para a autenticação dos usuários.

Figura 10 - Dados do servidor LDAP exemplo.



The image shows the JXplorer application interface. The top menu bar includes File, Edit, View, Bookmark, Search, LDIF, Options, Tools, Security, and Help. Below the menu is a toolbar with various icons. A "Quick Search" bar is present. The main interface is divided into two panes. The left pane, titled "Explore", shows a tree view of the LDAP hierarchy. The root is "World", and under it is "ufrn". Under "ufrn" are three nodes: "caico", "mossoro", and "natal". The right pane, titled "Table Editor", shows a table with two columns: "attribute type" and "value". The table contains the following data:

attribute type	value
o	ufrn
objectClass	top
objectClass	organization
businessCategory	
description	
destinationIndicator	
facsimileTelephoneNumber	

LDAP x bancos relacionais (SQL)

Caso você já saiba o que é um banco de dados relacional (um banco SQL), pode estar se perguntando qual a diferença entre ele e o LDAP. Resumidamente, podemos ressaltar três pontos principais:

- Um banco SQL armazena suas informações em tabelas, enquanto que no LDAP elas são armazenadas em forma de árvore.
- Embora um diretório LDAP suporte atualizações, ele é otimizado para operações de leitura. Portanto, se o número de modificações na sua base de dados é muito alto seria mais indicado utilizar uma base SQL que uma LDAP.
- Várias aplicações já suportam LDAP e existem esquemas criados especificamente para essas aplicações. Cada vez mais o LDAP está se tornando o padrão para o armazenamento de dados de diversas aplicações, como, e-mail, *browsers*, DNS, entre outras. Um browser, por exemplo, pode guardar sua lista de sites favoritos em um servidor LDAP.

Atividade 02

1. Após aprender as duas formas de efetuar e inserir informações no LDAP, com qual delas vocês se familiarizou mais? Quais as vantagens de cada uma em relação a outra?

Resumo

Nesta aula, você aprendeu que em uma rede é necessário que existam os serviços de autenticação de usuários e de compartilhamento de arquivos para que o usuário possa utilizar qualquer máquina da rede de modo transparente. Viu que esses serviços utilizam um programa no cliente e outro no servidor e que esses programas se comunicam usando algum protocolo. No caso da autenticação, aprendeu que o LDAP é um dos protocolos mais usados para essa finalidade. Você aprendeu, ainda, que o LDAP pode ser usado também para qualquer outra finalidade em que seja necessário armazenar e consultar informações de modo centralizado. Aprendeu a instalar e configurar o servidor Openldap no Linux e a usar ferramentas, em modo texto e com interface gráfica, para manipular a base LDAP.

Autoavaliação

1. O que significa o campo/atributo *Distinguished Name* (dn) de um objeto?
2. Qual o comando para ativar um esquema cuja definição do esquema se encontra no arquivo meuesquema.ldif?
3. Supondo que o usuário administrador do LDAP se chame `cn=admin,o=ufrn`, responda:
 - a. Qual o comando para processar o arquivo usuarios.ldif, que contém informações dos usuários a serem inseridos na LDAP?
 - b. Qual o comando para excluir o nó que possui o dn `"ou=medicina,ou=natal,o=ufrn"`?

Referências

JXPLOER. Disponível em: <<http://jxplorer.org/>>. Acesso em: 12 set. 2012.

KUROSE, J.; ROSS, K. **Redes de computadores e a internet**. 5. ed. São Paulo: Addison Wesley, 2010.

OPENLDAP SERVER. <<http://doc.ubuntu.com/ubuntu/serverguide/C/openldap-server.html>>. Acesso em: 12 set. 2012.

SENA, C. **LDAP: Um Guia Prático**. [Rio de Janeiro]: Ciência Moderna, 2005.