Redes de Computadores II

Aula 06 - Autenticação e Compartilhamento de Arquivos – Parte I

Apresentação

Com certeza você já está acostumado ao fato de que para utilizarmos um computador normalmente precisamos informar um nome de usuário e uma senha. Esse procedimento garante a nossa identificação e com isso permite que sejam aplicadas regras que controlam o que podemos fazer no computador, como, por exemplo, quais arquivos podemos acessar.

Nas redes das empresas, nas quais existem diversos computadores que podem ser acessados por diferentes pessoas, esses **mecanismos de autenticação** e **controle de acesso** são indispensáveis.

Além disso, como nessas redes uma pessoa pode usar diferentes computadores, é necessário que exista um mecanismo que disponibilize os arquivos desta pessoa na máquina onde ela estiver conectada em um dado momento.

Nesta aula, estudaremos um protocolo chamado **LDAP** que é muito utilizado para implementar os mecanismos de autenticação.

Vídeo 01 - Apresentação

Objetivos

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

- Entender como funcionam os serviços de autenticação e compartilhamento de arquivos.
- Aprender o funcionamento do protocolo aberto conhecido como *Lightweight Directory Access Protocol*, ou LDAP.

Autenticação de usuários e compartilhamento de arquivos

Nesta seção, vamos estudar como funcionam os serviços de autenticação de usuários e de acesso aos seus arquivos. Inicialmente, vamos ver como isso ocorre quando usamos uma única máquina, sem que ela esteja conectada em nenhuma rede. Depois veremos o que muda quando temos várias máquinas em rede.

Apenas uma máquina

Vamos entender agora como funciona a autenticação e o acesso aos arquivos quando usamos uma única máquina. Suponha que essa máquina é um computador que você tem na sua casa. Como provavelmente um irmão ou um de seus pais pode também querer usar o computador, é importante que cada pessoa tenha privacidade para seus arquivos, ou seja, cada pessoa só possa acessar seus próprios arquivos. Além disso, cada um pode querer personalizar a área de trabalho com papel de parede específico ou escolher os ícones que quer que apareçam na tela.

Para que isso seja possível é necessário primeiro ter como identificar cada pessoa (que é chamada de usuário), o que é feito através de um nome de usuário e uma senha.

Depois é necessário definir o que cada usuário pode fazer na máquina (permissões) e quais arquivos podem acessar. Você pode dizer, por exemplo, que um usuário não pode acessar o CD (ou DVD), ou que não pode usar a impressora, mas normalmente a principal restrição é se ele pode ou não instalar programas na máquina. No que diz respeito aos arquivos, por padrão, cada usuário só pode acessar seus próprios arquivos. Naturalmente um usuário pode liberar o acesso a um ou mais de seus arquivos para outro usuário.

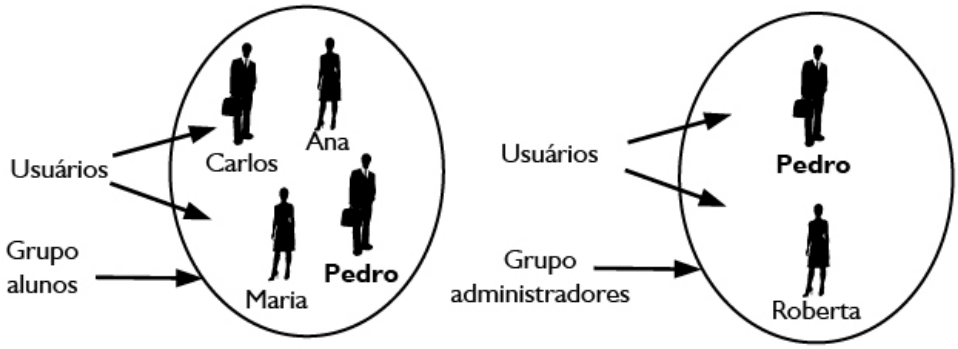
Um conjunto de permissões é chamado de **L**ista de **C**ontrole de **A**cesso, ou ACL.

Normalmente, as ACLs são aplicadas a cada usuário individualmente. Para simplificar as coisas, são criados grupos e os usuários são inseridos nesses grupos. As ACLs são então definidas para os grupos e, consequentemente, são aplicadas a todos os usuários de cada grupo. Em uma máquina existem pelo menos dois grupos, um de usuários com direitos normais e outro para usuários com direitos de administrador. Os usuários desse último grupo normalmente têm acesso completo à máquina, ou seja, podem realizar qualquer operação.

Autenticação de usuários e compartilhamento de arquivos II

A Figura 1 mostra dois grupos, um chamado de “alunos” e outro de “administradores”. Observe que é possível um mesmo usuário pertencer a mais de um grupo, como é o caso do usuário “Pedro”. Naturalmente, nesse caso, os direitos dele serão obtidos considerando-se as permissões de todos os grupos aos quais ele pertence.

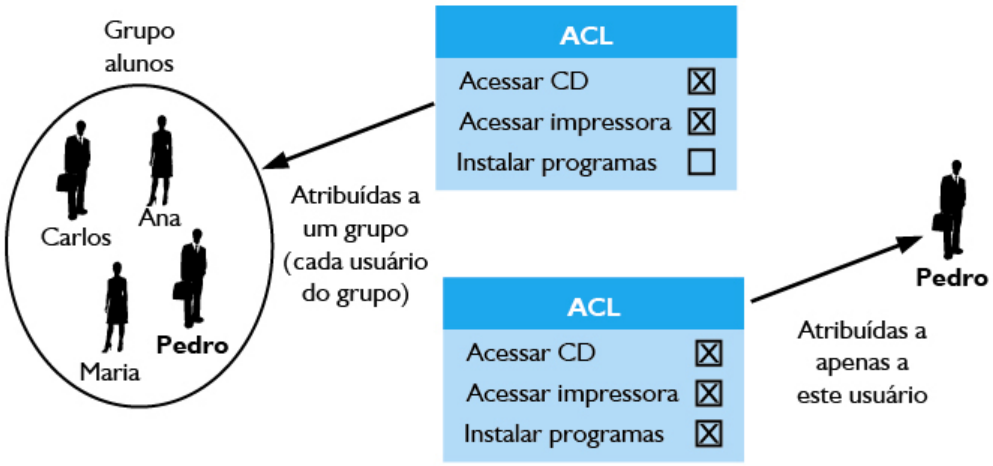
Figura 01 - Grupos de usuários: grupo comum e administradores.



Fonte: Autoria própria.

A Figura 2 mostra a aplicação de uma ACL para um grupo (alunos) e de outra ACL para um usuário individual.

Figura 02 - Atribuição de permissões a um grupo de usuários e a um único usuário.



Fonte: Autoria própria.

No primeiro caso, as regras de acesso contidas na ACL são aplicadas a cada usuário do grupo, mas de um modo muito mais fácil de fazer do que se fosse necessário fazer isso individualmente para cada um deles.

Observe que “Pedro” terá permissão de instalar programas, pois embora essa permissão não lhe tenha sido atribuída pelas permissões do grupo, lhe foi concedida pela atribuição das permissões individuais.

Observe que “Pedro” terá permissão de instalar programas, pois embora essa permissão não lhe tenha sido atribuída pelas permissões do grupo, lhe foi concedida pela atribuição das permissões individuais.

Sendo assim, após a pessoa que vai utilizar a máquina informar seu nome de usuário (username) e sua senha, o sistema operacional verifica se seu usuário existe e se a senha informada está correta.

No caso do Linux, as informações dos usuários, como seu username, por exemplo, estão no arquivo /etc/passwd, com exceção das senhas, que estão no arquivo /etc/shadow.

Atividade 01

1. O que é uma ACL?
2. O que acontece se uma ACL for atribuída a um grupo de usuários?
3. Suponha que você é casado e tem um filho de 8 anos que sabe mexer bastante no computador, mas você não quer que ele instale nenhum tipo de programa na máquina. No entanto, os outros membros da família podem continuar instalando o que quiserem. Indique o que fazer usando ACLs.

Autenticação de usuários e compartilhamento de arquivos III

Veja aqui a explicação em vídeo sobre a autenticação e o controle de acesso em uma máquina isolada.

Vídeo 02 - Máquina Isolada

Máquinas em uma Rede

Vamos agora analisar o caso em que existem várias máquinas na rede que o usuário pode utilizar. Isso acontece em várias empresas. Pense em um laboratório de informática de uma escola, no qual os alunos vão estudar, por exemplo. Faça de conta que você é um desses alunos.

Evidentemente, em cada dia você poderia utilizar uma máquina diferente, não dá para ter as informações sobre os usuários (*username* e senhas), nem seus arquivos, gravadas em apenas uma máquina, como é feito para uma máquina que não está em rede. Veja que também não faria sentido gravar uma cópia dessas

informações em cada máquina, pois sempre que alguma informação fosse alterada na máquina que você estivesse trabalhando, todas as outras máquinas ficariam desatualizadas.

A solução é centralizar todas essas informações em uma única máquina (chamada *servidor*), e instalar um programa nas máquinas que os usuários vão utilizar (chamadas *clientes*) que dê a impressão de que tudo está acontecendo apenas na máquina local, na qual ele está trabalhando.

Vamos agora ver o que "dá a impressão de que tudo está acontecendo na máquina local" significa, em termos de autenticação e do acesso aos arquivos.

Autenticação

Os nomes dos usuários (*usernames*) e suas senhas ficam gravados em um arquivo no servidor. Nos clientes, o programa que verifica o username e senha dos usuários sabe disso e sempre que uma pessoa tenta utilizar a máquina, esse programa envia o username e a senha informados para o servidor. O servidor verifica no seu arquivo de usuários se a senha informada para aquele usuário está correta e envia uma mensagem de volta ao cliente liberando ou negando o acesso.

A Figura 3 mostra o que acontece quando o usuário Carlos (que possui a senha teste123) tenta se *logar* (entrar) em uma máquina da rede. Como ele informou a senha correta, no passo 4 o servidor envia uma mensagem informando que ele "autenticou com sucesso", pois a senha informada é a mesma existente no arquivo do servidor, e o acesso à máquina foi liberado.

Figura 03 - Esquema de autenticação de usuários em uma rede.

Fonte: Autoria própria.

Vídeo 03 - Autenticação e ACL

Compartilhamento de arquivos

Vamos agora ver como os arquivos do usuário que estão no servidor são acessados.

Do mesmo modo que existe o *software* de autenticação que é composto por uma parte que executa no servidor e outra que executa no cliente, existe também um *software* para acesso aos arquivos em rede, que é composto por uma parte que executa no servidor e outra que executa no cliente.

Observe que não estamos dizendo que o usuário vai ter que usar um programa especial para acessar seus arquivos. Nada disso! Esse programa faz parte do próprio sistema operacional e cria uma espécie de disco virtual na máquina cliente.

A Figura 4 mostra o que acontece quando o usuário Carlos tenta acessar um de seus arquivos (redes.doc) a partir de uma máquina cliente. Uma mensagem solicitando essa operação é enviada ao servidor (passo 2), que faz o acesso ao disco real (passo 3).

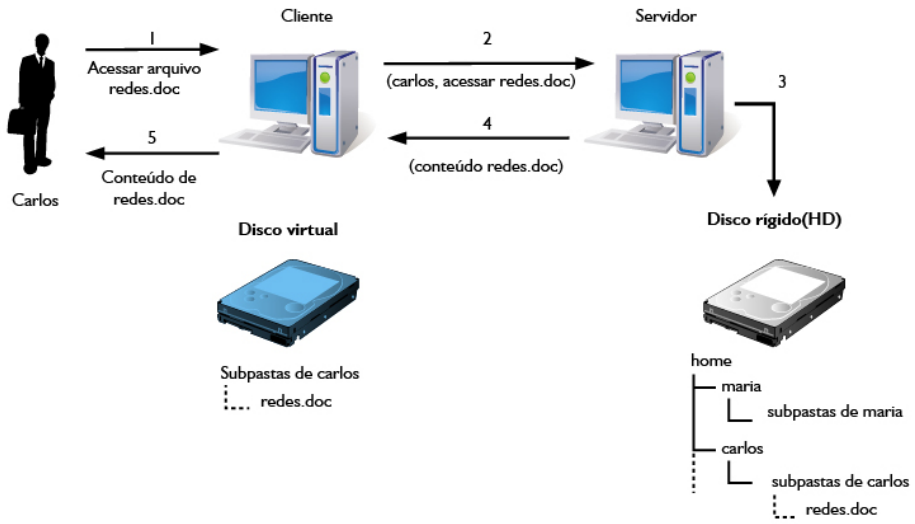
Nesse passo, as ACLs são verificadas para ver se o usuário Carlos tem permissão de acessar o arquivo. Caso tenha, no passo 4 o conteúdo do arquivo é enviado para a máquina cliente e finalmente passado para a aplicação (passo 5).

Veja, portanto, que para a aplicação que tentou ler o arquivo não existe nenhuma diferença se o arquivo estava na máquina cliente ou no servidor. É como se existisse realmente um disco na máquina cliente com os arquivos do usuário, mas na verdade ele não existe – daí o nome virtual.

Se a maquina cliente for Windows, realmente vai aparecer um novo disco, identificado com uma letra de *drive*, por exemplo, “D:”, ou “F:”. Se o cliente for um Linux, os arquivos e pastas do servidor vão aparecer dentro de alguma pasta existente na máquina local, que foi criada apenas para esta finalidade.

Observe que os arquivos (e pastas) de todos os usuários, incluindo os de Carlos, estão no disco rígido que existe no servidor, dentro da pasta *home*. Entretanto, o sistema operacional da máquina cliente mostra a relação de arquivos e pastas do servidor como se eles fossem locais.

Figura 04 - Compartilhamento de arquivos.



Fonte: Autoria própria.

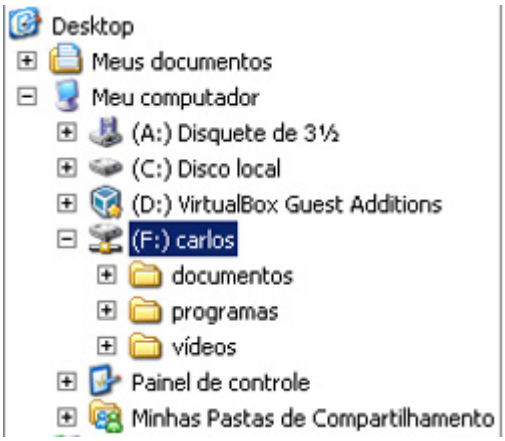
Atividade 02

1. Por que usar autenticação para ingressar (logar) nas máquinas da rede?
2. Explique qual a vantagem oferecida por uma rede que dispõe do serviço de compartilhamento de arquivos.

Compartilhamento de arquivos II

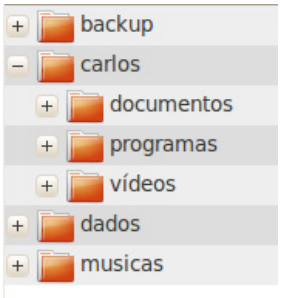
Como dissemos antes, a forma como as pastas de Carlos aparecem na máquina cliente depende se esta máquina é Linux ou Windows. Supondo que as pasta de Carlos no servidor fossem “documentos”, “músicas” e “vídeos”, a Figura 5 mostra um exemplo de como essas pastas apareceriam se a máquina cliente fosse Windows. Veja que foi criado um disco identificado pela letra “F:”, e as pastas aparecem dentro desse disco.

Figura 05 - Como as pastas remotas aparecem em um cliente Windows.



Assumindo as mesmas pastas de *Carlos* no servidor, a Figura 6 mostra como essas pastas apareceriam no cliente se a máquina fosse Linux. Observe que as pastas remotas aparecem dentro da pasta Carlos, que foi criada no cliente apenas para essa finalidade. Além disso, veja que nesse esquema as pastas remotas aparecem completamente integradas às pastas locais da máquina, que nesse caso, são: *“backup”*, “dados” e “músicas”.

Figura 06 - Como as pastas remotas aparecem em um cliente Linux.



Atividade 03

1. Onde ficam os arquivos com os nomes dos usuários e as senhas em uma rede?
2. Como as pastas remotas aparecem na máquina cliente se o usuário estiver utilizando Windows?

LDAP

Veja aqui a explicação em vídeo sobre os serviços de autenticação e compartilhamento de arquivos.

Vídeo 04 - Máquinas em Rede

Para realizar a autenticação dos usuários em uma rede, falamos que é utilizado um programa que é composto por uma parte que roda no cliente e outra que roda no servidor. Naturalmente, esses programas utilizam algum protocolo para se comunicarem. Existem diversos mecanismos de autenticação, que embora sigam o modelo que você acabou de estudar, utilizam protocolos diferentes.

É por isso que, a princípio, um cliente Windows só consegue se autenticar em um servidor Windows, e um cliente Linux em um servidor Linux. Felizmente, existem formas de reduzir essas limitações, fazendo, por exemplo, um cliente Windows se autenticar em um servidor Linux.

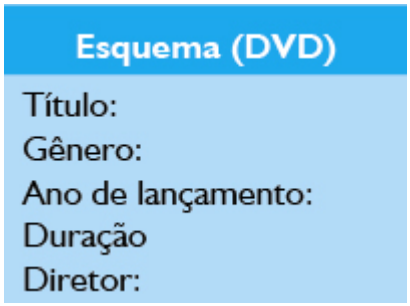
Na próxima aula iremos aprender a fazer a autenticação de um cliente Linux em um servidor Linux. Embora outros protocolos já tenham sido utilizados para realizar essa tarefa, como o NIS, por exemplo, atualmente a forma mais comum de fazer isso é utilizando o protocolo LDAP. Mas fique sabendo que o LDAP é um protocolo que

pode ser utilizado para diversas outras finalidades, além da autenticação. Por isso, nesta aula vamos falar sobre o LDAP de modo geral, para na próxima aula você aprender como utilizá-lo para a autenticação.

Definição e Esquemas

O LDAP (***L****ightweight* ***D****irectory* ***A****ccess* ***P****rotocol*) é um protocolo para acesso a informações remotas que são organizadas de forma estruturada. A melhor forma de entender o que se quer dizer com "estruturada" é através de um exemplo. Imagine que as informações que você quer disponibilizar sejam referentes aos filmes de uma locadora de DVDs. Para cada filme você iria estruturar as informações sobre ele mais ou menos do modo mostrado na Figura 7, criando uma espécie de modelo, ou formulário, que o LDAP chama de "Esquema".

Figura 07 - Esquema LDAP para informações sobre filmes.

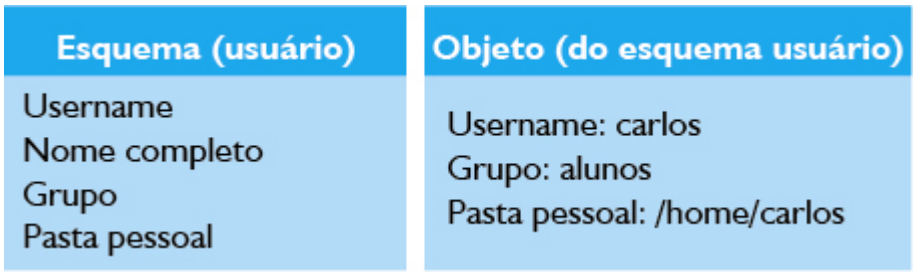


Fonte: Autoria própria.

Cada esquema, além dos nomes dos campos, define o tipo de cada campo. Um campo pode ser, por exemplo, uma *string*, e outro campo pode ser um inteiro. Além disso, um esquema pode dizer que alguns campos são opcionais e outros são obrigatórios. Assim, quando se vai inserir um objeto de um determinado esquema é necessário informar todos os campos obrigatórios. Por objeto, entenda o conjunto de informações referentes a um esquema. Para o esquema DVD, um objeto seria o conjunto de dados de um filme qualquer.

Como outro exemplo de esquema, vamos pegar algumas informações que o sistema operacional precisa manter sobre um usuário. O esquema do LDAP para armazenar essas informações é mostrado na Figura 8. Veja que o campo "Nome Completo" não foi informado no novo objeto sendo inserido. Isso é possível caso esse campo seja declarado como opcional na definição do esquema usuário.

Figura 08 - Esquema LDAP para informações dos usuários e um objeto exemplo.



Fonte: Autoria própria.

O programa que armazena as informações do LDAP é chamado de “Diretório”, mas como esse nome pode não ser muito claro, é melhor você pensar no LDAP como uma base de dados, ou seja, algo que armazena um conjunto de informações. Todas as informações armazenadas devem ser de um dos tipos de esquemas suportados pelo servidor. Cada servidor define os esquemas que quer suportar. Existem vários esquemas pré-determinados, mas é possível criar novos esquemas com os campos que desejarmos.

Veja aqui a explicação em vídeo sobre os esquemas do LDAP.

Vídeo 05 - LDAP Esquemas

Estrutura em árvore

Até aqui você já sabe que o LDAP é um protocolo para acessar informações e que elas são organizadas de acordo com algum esquema. Assim sendo, sabe também que um servidor LDAP contém vários objetos de diversos esquemas diferentes. Vamos agora descrever mais uma característica do LDAP que o torna extremamente interessante.

Uma base LDAP é organizada em árvore e os objetos podem ser inseridos em qualquer nó da arvore. Além disso, cada nó tem um nome, que é único na árvore.

A característica descrita acima trás duas grandes vantagens.

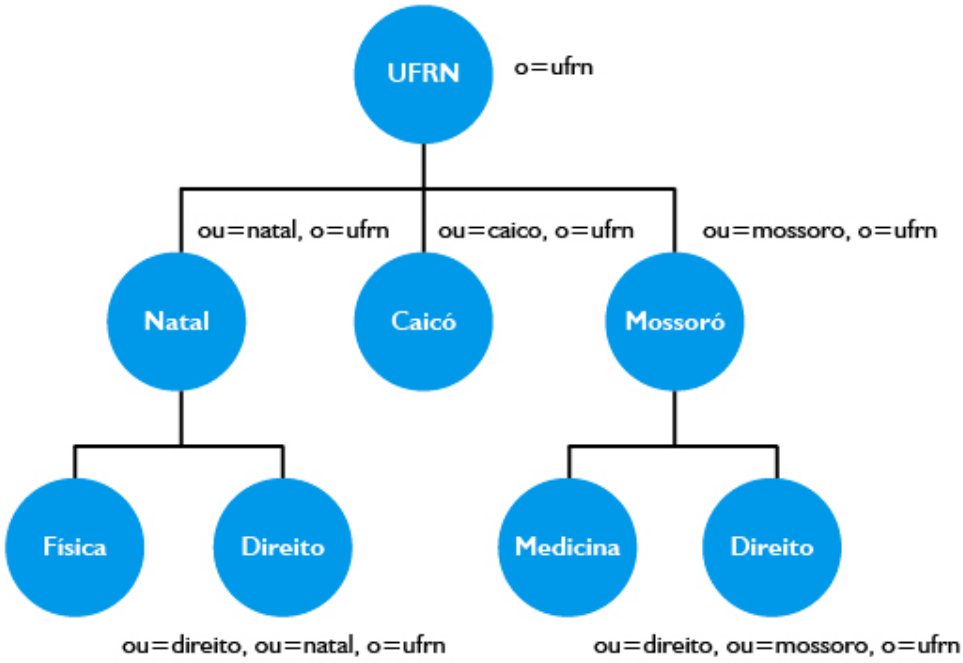
- Eficiência nas pesquisas. Quando se deseja procurar um objeto pode-se fazer a busca apenas em um nó específico, ou em uma subárvore (iniciando em um determinado nó).

- Descentralização. Cada parte da árvore pode ser armazenada em uma máquina diferente, mas todos continuam vendo a árvore inteira.

Vamos analisar melhor essas questões. Imagine uma universidade como a UFRN, que tem milhares de alunos e possui várias unidades, em diversas cidades, como Natal, Caicó e Mossoró, por exemplo. Em cada uma dessas unidades existem diversos cursos. Para armazenarmos as informações dos usuários da UFRN numa base LDAP, seria interessante organizarmos essas informações em uma árvore LDAP, como a mostrada na Figura 9.

Cada nó possui um nome abreviado, que se encontra mostrado dentro de cada círculo na Figura 9, e um nome completo, que para alguns nós está mostrado próximo ao círculo. Veja que o nó raiz é nomeado com “o=ufrn”, no qual esse “o” significa organização. Os demais nós se chamam “ou=XXX”, em que XXX é o nome abreviado do nó. A sigla “ou” significa *Organization* ***U****nit* (Unidade Organizacional). A regra é que você deve nomear o nó raiz da sua árvore com “o” e todos os demais abaixo dele com “ou”. Veja também que o nome de cada nó inclui o nome de todos os nós a partir dele até a raiz.

Figura 09 - Árvore LDAP.



Fonte: Autoria própria.

Essa árvore pode então ser utilizada para armazenar objetos do esquema "usuários", contendo as informações dos seus alunos. O objeto referente a cada aluno pode ser armazenado no nó do curso que o aluno pertence. Por exemplo, um aluno do curso de direito da unidade Natal seria armazenado no nó "ou=direito,ou=natal,o=ufrn" enquanto um aluno do curso de direito de Mossoró seria armazenado no nó "ou=direito,ou=mossoro,o=ufrn".

Desse modo, quando se deseja pesquisar por um aluno, sabendo que curso ele faz, basta realizar a busca indicando em que nó da árvore ela deve ocorrer. Caso não se saiba a qual curso o aluno pertence, a busca pode ser feita a partir do nó raiz da árvore (o=ufrn), passando por todos os nós filhos.

No que diz respeito à descentralização, cada unidade poderia manter seu próprio servidor LDAP, sendo responsável por manter a subárvore que inicia com o nó que possui o nome da unidade, mas todos os servidores veriam a árvore como ela é mostrada na Figura 9.

Veja aqui a explicação em vídeo sobre a árvore LDAP.

Vídeo 06 - LDAP

Vídeo 07 - LDAP Árvore

Atividade 04

1. Qual é o nome completo do nó “Medicina” na Figura 9?

Identificação única de cada objeto

Cada esquema LDAP pode definir os campos que desejar, mas todos possuem obrigatoriamente um campo chamado “dn” (*Distinguished **N**ame* – Nome Distinto), que é uma forma de identificar unicamente o objeto em toda a árvore. Portanto, o valor do campo dn de cada objeto na árvore deve ser diferente.

Para garantir isso, normalmente o valor utilizado nesse campo é o nome e valor de algum campo que é único dentro do nó da árvore em que o objeto está armazenado, concatenado com o nome do nó. Para as informações dos alunos que usam o esquema “usuários”, o valor desse campo que precisa ser único dentro de cada nó, poderia ser o campo “*username*”. Desse modo, o campo dn do usuário Carlos, do curso de direito de Natal, seria “username=carlos,ou=direito,ou=natal,o=ufrn”.

Arquivos LDIF

As operações em um servidor LDAP podem ser feitas utilizando aplicações que manipulam arquivos textos que possuem um formato especial, chamado LDIF. Embora o formato exato do um arquivo LDIF dependa do tipo de operação que se deseje realizar, a Figura 10 mostra um exemplo de um arquivo para alterar o e-mail do usuário Carlos.

```
1 dn: username=carlos,ou=direito,ou=natal,o=ufrn
2 changetype: modify
3 replace: mail
4 mail: carlos@metropoledigital.ufrn.br
```

Figura 10 - Arquivo LDIF.

Veja aqui a explicação em vídeo sobre o atributo dn e o formato LDIF.

Vídeo 07 - Apresentação

Referências

JXPLORER. 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.