Gerenciamento automático de usuários de uma rede acadêmica

Daniel Cason[1], **Rodrigo Rocha**[1], **Antonio Terceiro**[1],
Amadeu Barbosa[1], **Eduardo Ramos**[1], **Humberto Galiza**[1]

[1]Departamento de Ciência da Computação
Universidade Federal da Bahia (UFBA)
Av. Adhemar de Barros, s/n - Campus Universitário de Ondina
Salvador - BA - Brazil

{cason,rodrigo,terceiro,amadeu,ihtraum,galiza}@dcc.ufba.br

Abstract. *This paper describes an application suite intended to automate administration tasks related to users and services in an academic computer network. We focus on the creation and removal of user accounts and on the integration of network services. Provided examples show the application suite the way it is used in a real network.*

Resumo. *Este artigo descreve uma suíte de ferramentas livres que automatiza tarefas de administração de usuários e serviços de uma rede acadêmica de computadores. É dado foco na criação e remoção de contas de usuários e na integração de serviços de rede. Os exemplos fornecidos mostram como as ferramentas são usadas em um ambiente real.*

1. Introdução

O objetivo de uma rede de computadores é servir às necessidades de cada um do seus diversos usuários e, especialmente em uma universidade, o conjunto de usuários e suas necessidades mudam constantemente. A cada semestre surgem alunos novos, outros tantos se formam e as disciplinas recebem novas turmas de alunos; colaboradores e responsáveis pelos grupos de pesquisa mudam, professores e outros funcionários assumem ou deixam cargos, ingressam ou se retiram do curso.

Os serviços oferecidos pela rede devem, então, acompanhar essas mudanças de cenário de maneira ágil, sem causar transtorno para os usuários. Ao mesmo tempo, é desejável que os administradores de rede se dediquem à implementação de novas configurações e serviços, evitando perder tempo com trabalhos burocráticos.

Com o crescimento do número de usuários e da quantidade de serviços oferecidos, tal cenário se torna mais complexo e mais difícil de administrar. Normalmente o resultado é uma base de contas de usuários desatualizada e descentralizada, que demanda grande esforço de manutenção.

Para facilitar a manutenção de contas de usuários é importante ter um servidor central robusto que, mediante a autenticação, forneça aos sistemas clientes o perfil do usuário requisitante. Tal solução pode ser implementada com a adoção um protocolo bem estabelecido, como o Lightweight Directory Access Protocol (LDAP)[J. Sermersheim 2006].

Infelizmente nem todos os serviços de nossa rede possuem suporte a LDAP e mesmo os que possuem freqüentemente precisam armazenar informações adicionais sobre cada usuário. Em vista disto, faz-se necessária uma solução para manter as diferentes bases de usuários em sincronia de forma automática.

Este artigo apresenta ferramentas livres que automatizam o gerenciamento de usuários em uma rede acadêmica. A seção 2 descreve como nossa base LDAP reflete a estrutura da universidade. A seção 3 lista os serviços oferecidos e as dificuldades que apresentam. Nossa solução é apresentada na seção 4. A seção 5 apresenta a conclusão do trabalho e perspectivas futuras.

2. Estrutura organizacional e o LDAP

A rede acadêmica em questão atende a um Instituto formado por três Departamentos. Ela fornece serviços prioritariamente para o Departamento de Ciência da Computação, mas temos um legado de usuários de outros departamentos, para os quais fornecemos uma gama mais limitada de serviços.

Dentro da comunidade acadêmica, independentemente de departamento, cada usuário assume um papel principal: aluno (graduação ou pós-graduação), professor ou convidado. É possível também que ele assuma dois papéis pois há, por exemplo, professores que também são alunos de pós-graduação.

A base LDAP leva em consideração a nossa organização estrutural, de modo que temos contas que representam nossos usuários, classes que representam seus papéis e grupos que permitem o acesso a uma série de serviços específicos.

A conta LDAP associa ao usuário vários atributos, dentre os quais um identificador único (uid) e senha usados para se autenticar nos serviços, informações pessoais (nome, telefone, email externo, etc.) e um campo que define a qual departamento o usuário pertence.

Os grupos LDAP são formados por usuários que pertencem a um mesmo grupo de pesquisa ou possuem privilégios de administradores, o que permite o acesso a pastas virtuais, login em máquinas de acesso restrito, edição de páginas, dentre outros. Além disto, os grupos Unix do usuário (que permitem acessar os dispositivos de sistema nos terminais) são importados da base LDAP.

Foi utilizada na rede uma implementação livre do protocolo LDAP, o OpenLDAP [Zeilenga et al. 2007]. A interface *web* phpLDAPadmin é usada para facilitar busca, visualização e modificação da base de usuários.

3. Serviços de rede oferecidos

Esta seção descreve os serviços fornecidos e potenciais necessidades de integração.

3.1. Laboratórios e pastas pessoais

O acesso aos laboratórios usa autenticação na base LDAP, que fornece às estações de trabalho as informações pessoais do usuário e os grupos aos quais ele está associado. Alguns laboratórios são de uso restrito e para acessá-los é preciso ser membro de determinados grupos, por exemplo, laboratórios de pesquisa só estão disponíveis para os usuários indicados como pesquisadores.

Nos laboratórios também são disponibilizados ao usuário os seus arquivos pessoais do servidor de arquivos. A quota máxima de espaço a ser utilizada por cada usuário está associada a diversos critérios armazenados na base LDAP, como classe e tempo de uso.

3.2. E-mail

Para fornecer um serviço de e-mail, mantemos um servidor de e-mail baseado no Postfix (agente de tranferência de mensagens), Courier (agente de entrega de mensagens), SpamAssassin (anti-spam), Amavis (anti-vírus) e SquirreMail (cliente webmail).

O webmail guarda as configurações específicas para cada conta na sua base de dados. A autenticação dos usuários é feita na base LDAP. A quota de espaço para mensagens é definida com base no perfil do usuário, assim como a quota de arquivos pessoais.

3.3. Sistema de controle de versão

Como sistema de controle de versão, utilizamos a solução livre Subversion, que é usada principalmente por grupos de pesquisa e desenvolvimento e em algumas disciplinas. Cada projeto, grupo ou disciplina possui o seu próprio repositório.

A autenticação do serviço é feita através do LDAP. Para alguns repositórios, a configuração de permissões de acesso (direitos de leitura e escrita) é mantida em sincronia com grupos na base LDAP.

3.4. Listas de discussão

O gerenciador de listas de discussão usado é o Mailman, que não tem um conceito bem definido de usuário. Ele agrega listas de discussão, cada uma delas contendo um conjunto de endereços de e-mail dos seus participantes, ao qual estão associadas as suas configurações pessoais.

Algumas listas são formadas apenas por usuários com características específicas, como por exemplo alunos de um curso, ou alunos matriculados em determinada disciplina. A participação nessas listas é compulsória, e é interessante que a base de usuários indique os usuários que devem participar de cada lista.

3.5. Reserva de salas

O MRBS é uma aplicação usada para reserva de salas do nosso Instituto. Certos usuários têm permissão de reservar uma sala para aula, palestra ou outro evento, além de alterar as reservas já feitas.

A partir de atributos do LDAP, é dado acesso aos usuários para reservar determinadas salas, por exemplo, restringindo salas por departamento do usuário. Para viabilizar isso foi feita uma modificação no MRBS, que na época não tinha suporte a filtros LDAP.

4. As ferramentas

Esta seção apresenta algumas tarefas de administração de rede e as ferramentas desenvolvidas para automatizá-las. Existem basicamente três tarefas importantes: criação e remoção de usuários, feita pelo sync-ldap-cpd e a manutenção das contas de usuários, feita pelo sync-groups. A figura 1 mostra como é feita a integração de alguns serviços.

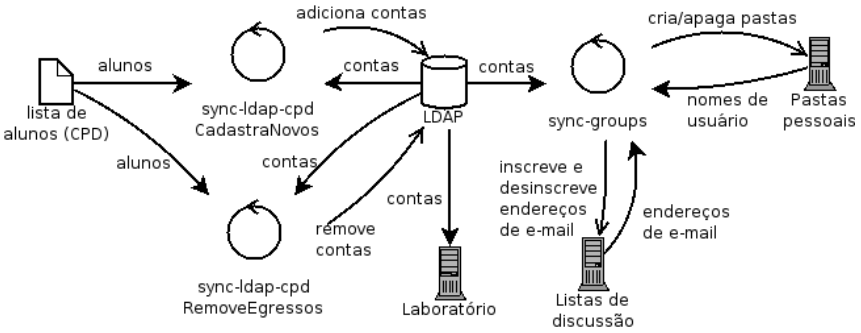

Figura 1. Relacionamento entre ferramentas e serviços

Todas as ferramentas foram escritas em Java e são executadas na linha de comando. À medida em que são executadas, as operações são mostradas na tela e gravadas num arquivo de log para posteriores consultas. A comunicação entre diferentes servidores é feita através do protocolo SSH[Ylonen and Lonvick 2006].

4.1. Criação de usuários

A participação de uma pessoa na rede acadêmica inicia-se com a criação de uma conta de usuário. No caso de novos professores, pesquisadores, funcionários e convidados utilizamos um procedimento manual para a criação de contas. Isso é feito através da interface *web* phpLDAPadmin. Ele permite a criação de modelos, ou *templates*, de acordo com o perfil do novo usuário. Os modelos determinam como são preenchidas informações comuns a toda uma categoria de usuários, como quota, departamento e o formato do endereço do e-mail institucional a ser criado.

A criação de contas de alunos é mais difícil, pois são um grupo maior e, a cada semestre, dezenas de novos alunos ingressam nos cursos. Para tal desenvolvemos um procedimento mais complexo e uma ferramenta para automatizar alguns dos passos: o sync-ldap-cpd.

Após o período de matrícula, recebemos do CPD (Centro de Processamento de Dados) da universidade uma planilha contendo informações sobre cada aluno matriculado, tais como nome, e-mail e número de matrícula. A ferramenta compara os números de matrícula da planilha com aqueles encontrados em nossa base LDAP e identifica os novos alunos.

Pode haver situações, no entanto, em que o novo aluno já possui uma conta no LDAP e desejamos mantê-la, apenas mudando algumas informações. É o caso de ex-alunos de graduação que ingressaram em um curso de pós-graduação. Para detectar esses casos, a ferramenta faz comparações aproximadas do nome da pessoa com nomes na base. Se a conta já existe, ela é mantida e o administrador de rede é informado sobre a necessidade de atualizar os dados.

Caso contrário, uma nova conta é criada com os dados presentes na planilha. Alguns outros dados são obtidos do modelo do phpLDAPadmin. Isso é muito importante, pois garante que usuários criados manualmente terão os mesmos dados iniciais daqueles criados automaticamente (como quota de disco). O nome de usuário e a senha são gerados automaticamente, caso não estejam especificados na planilha. No final do pro-

cesso o programa imprime um cartão para cada aluno contendo nome de usuário, senha e informações gerais.

4.2. Manutenção de usuários

Após a criação das contas, é preciso assegurar que os usuários têm acesso aos serviços apropriados. Dentro da universidade as pessoas se organizam naturalmente em grupos: alunos de graduação, alunos de pós-graduação, professores, membros de grupos de pesquisa e outros. Cada grupo possui necessidades específicas na rede. Uma pessoa pode se enquadrar em vários grupos.

Da mesma maneira os serviços formam grupos de usuários. Há o grupo de usuários que possuem conta de e-mail, o grupo de usuários inscritos na lista de discussão de alunos, o grupo de usuários que podem modificar um determinado repositório Subversion e muitos outros.

Nessa visão, inscrever usuários nos serviços apropriados é a mesma coisa que sincronizar grupos. Precisamos, por exemplo, fazer o grupo de usuários inscritos na lista de discussão de alunos coincidir com o grupo de alunos. A ferramenta sync-groups foi baseada nessa idéia.

O sync-groups possui um arquivo de configuração, o sync-groups.conf, que especifica as regras de sincronização dos grupos. A regra representada a seguir estabelece que todos os usuários da base LDAP rotulados como alunos de graduação, e somente estes, devem ser membros da lista todos-estudantes. Note que, para satisfazer a regra, pode ser necessário remover alguns usuários da lista.

```
list:todos-estudantes <- ldap:(objectclass=aluno-grad)
```

De maneira geral, cada regra é do tipo A $<-$ B, sendo A e B dois grupos. Ao executar a regra, o sync-groups obtém o conjunto de usuários de A e de B e os compara. Com o objetivo de tornar o grupo A idêntico ao grupo B, ele adiciona ao grupo A os usuários que estão exclusivamente em B e remove aqueles que estão exclusivamente em A. Os usuários pertencentes aos dois grupos não sofrem nenhuma manipulação.

Cada tipo de grupo reconhecido pelo sync-groups possui a implementação de três métodos: listar, remover e adicionar usuários. Isso permite estender o benefício do sync-groups a novos serviços. Todas as implementações devem identificar os usuários da mesma forma. Optamos por identificá-los através do nome de usuário utilizado na autenticação, ou *username*.

Tomemos o exemplo do "grupo de usuários que possuem pasta pessoal no servidor de arquivos". Seus métodos são implementados da seguinte forma:

- listar usuários: lista as pastas existentes dentro do diretório /home do servidor;
- adicionar usuário: cria uma pasta para o usuário contendo alguns arquivos de configuração padrão;
- remover usuário: faz uma cópia compactada de sua pasta pessoal e remove a original.

O invariante é que todos os usuários do grupo possuem pasta pessoal e ninguém mais. Portanto basta sincronizar esse grupo com o grupo de todos os usuários da rede para obter criação e remoção automática de pastas pessoais.

O sync-groups é configurado para ser executado periodicamente. O resultado disso é um sistema autogerenciável, em que o estado da rede sempre reflete as regras do arquivo de configuração.

4.3. Remoção de usuários

O módulo de remoção de usuários do sync-ldap-cpd desativa as contas de alunos egressos do curso. Para identificar essas contas ele utiliza a planilha do CPD de alunos matriculados, da mesma forma que o módulo de criação de usuários. Para cada pessoa identificada como egresso, o seguinte procedimento é realizado:

- a pessoa é marcada como egresso na base LDAP;
- a conta é configurada para ser desativada após 30 dias;
- é enviado um e-mail para a pessoa notificando a futura desativação de sua conta.

Eventualmente ex-alunos continuam desempenhando atividades dentro da universidade, e podem reivindicar a manutenção da conta. Se a justificativa for aceita, o administrador de rede desfaz as alterações no LDAP e atualiza os atributos do usuário para adequá-lo a sua nova situação. Caso contrário, a conta do usuário é removida na data prevista.

5. Conclusão

As ferramentas apresentadas têm se mostrado essenciais para simplificar a administração de rede, a partir do momento que automatizam a manutenção das contas de usuários e do modo como cada um deles acessa os serviços prestados. Dessa forma, o esforço empregado na sua elaboração e configuração é justificado pelo tempo que deixa-se de perder com operações manuais e repetitivas.

As ferramentas foram projetadas levando em consideração as necessidades específicas da nossa rede. Por não possuirem mecanismos de extensão, a única forma de adaptá-las a novos ambientes é através da modificação do código-fonte. Além disto, a intervenção humana, ainda necessária em alguns casos, pode ser reduzida com a implementação de novas funcionalidades.

Trabalhos futuros incluem o uso de técnicas de reengenharia, com intuito de facilitar ajustes e extensões das ferramentas, um estudo da viabilidade da implementação de uma arquitetura distribuída, além da elaboração de uma melhor documentação do código.

Mais informações sobre o projeto podem ser obtidas em `http://sync-users.dcc.ufba.br/`.

Referências

J. Sermersheim, E. (2006). Ldap: The protocol. Disponível em: http://tools.ietf.org/html/rfc4511. Último acesso em 1 de março de 2007.

Ylonen, T. and Lonvick, C. (2006). The secure shell (ssh) protocol architecture. Disponível em http://tools.ietf.org/html/rfc4251. Último acesso em 1 de março de 2007.

Zeilenga, K., Chu, H., and Masarati, P. (2007). Openldap. Disponível em: http://www.openldap.org/. Último acesso em 1 de março de 2007.