Administração de Sistemas de Autenticação de Usuários*

Diego Luís Kreutz

[1]Laboratório de Sistemas de Computação — LSC
Núcleo de Ciência da Computação — NCC
Universidade Federal de Santa Maria — UFSM

kreutz@inf.ufsm.br

Resumo. *Ferramentas para o gerenciamento integrado de diferentes diretórios online são cada vez mais necessárias. Isso por que é comum a administração de uma rede local envolver o gerenciamento de bases de dados como o OpenLDAP, NIS e Samba. Nesse sentido, este trabalho apresenta um sistema simples para o gerenciamento integrado de diferentes diretórios online. Além disso, seu principal foco são ambiente acadêmicos, incluindo funcionalidades e recursos extras que podem agilizar e simplificar o controle das contas dos usuários de uma rede local.*

1. Introdução

O controle de acesso a máquinas e sistemas são partes críticas e comprometedoras em redes locais que prezem por segurança e disponibilidade. Esse controle de acesso é normalmente realizado através do uso de diretórios *online* como o LDAP[1], NIS[2] e Samba. Os dois primeiros são comumentemente utilizados para autenticar usuários em sistemas Unix, enquanto que o segundo serve de autenticador para ambientes Windows.

Atualmente existem vários utilitários e ferramentas de gerenciamento de diretórios *online*. Alguns desses utilitários são baseados em linha de comando enquanto outros fazem uso de interfaces gráficas. Cada um desses sistemas possui suas características e aplicações específicas. Uma característica mais geral das ferramentas disponíveis é a pouca simplicidade e facilidade de realizar um gerenciamento integrado de diferentes autenticadores de usuários em uma rede local.

A proposta deste trabalho é apresentar um sistema simples e adaptável para o gerenciamento integrado de diretórios como o LDAP, NIS e Samba. O projeto, desenvolvimento e implementação desse sistemas foi baseado em necessidades básicas da rede do Núcleo de Ciência da Computação (NCC) da UFSM. O sistema torna possível a administração simultânea de diferentes sistemas de autenticação de usuários, como o OpenLDAP e Samba. Além disso, ele disponibiliza funcionalidades como cadastro de usuários em massa, configuração de leitores de e-mail como o *pine*, criação de exemplos de páginas *html* e *php* nas contas dos usuários, envio de e-mail de boas vindas e controle de expiração de senhas.

Na próxima seção é brevemente apresentada a arquitetura do sistema. Na seqüência são abordadas algumas funcionalidades e particularidades do sistema. Na seção seguinte são apresentados alguns trabalhos relacionados. Por fim, aparecem a conclusão e as perspectivas de continuidade.

2. Arquitetura

A proposta de um sistema de gerenciamento integrado de diretórios *online* surgiu a partir de necessidades administrativas do NCC. Em meados de 2000 os servidores NT foram subs-

*Fomento CNPq: processo 380049/03-1

[1]Lightweight Directory Access Protocol (protocolo leve de acesso a diret´orios)

[2]Network Information Service (serviç o de informaç ˜ao de rede)

tituídos pelo Samba, rodando em GNU/Linux. Os servidores Solaris e AIX também foram migrados para GNU/Linux. A base de dados de usuários e máquinas (NIS) foi migrada para o OpenLDAP. No entanto, essa nova configuração da rede ainda requeria o gerenciamento de duas bases de informação, o OpenLDAP e o Samba. Como os dois sistemas estavam rodando em servidores GNU/Linux, muitas tarefas poderiam facilmente ser automatizadas e sincronizadas. Além disso, o cadastro de vários usuários a cada início de ano letivo, a configuração de leitores de e-mail por parte dos usuários e o controle mais rigoroso sobre as senhas dos usuários continuavam sendo tarefas pouco práticas. Por isso, decidiu-se pelo desenvolvimento de um sistema que fosse capaz de suprir as principais necessidades de gerenciamento da rede e ao mesmo tempo fosse legível, simples e modular a ponto de ser facilmente ajustável à diferentes ambientes e contextos.

A figura 1 ilustra a arquitetura do sistema. Ele é basicamente constituído por três partes. A primeira é formada pelos dados de entrada, que podem ser estáticos ou interativos. Estáticos significa que existe um arquivo de entrada para ser processado. Esse arquivo de entrada contém conjuntos de registros que podem ser utilizados para proceder cadastros ou remoções em massa. Os dados interativos são utilizados quando o administrador deseja realizar de forma interativa apenas um cadastro, acompanhando os passos de geração e inclusão do novo registro e criação da *home* do usuário com dados e configurações padrão.

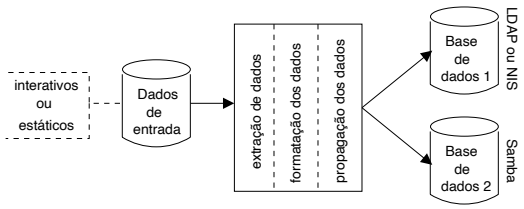

Figura 1: Ilustração da arquitetura do sistema

A segunda parte do sistema é constituída pelos módulos de gerenciamento e atualização. A primeira etapa, do funcionamento desses módulos, passa pela extração e classificação dos dados de entrada. Uma segunda fase consiste na formatação e preparação dos registros a serem incluídos ou manipulados. A etapa final é a propagação dos dados para as respectivas bases de informação.

O sistema é capaz de gerenciar simultaneamente uma ou mais bases de dados. Essa característica torna a ferramenta uma boa opção para o gerenciamento integrado de diferentes diretórios *online*, como o LDAP, NIS e Samba.

3. Características, Implementação e Manutenção do Sistema

O sistema foi planejado com o intuito de ser simples e adaptável. Um dos objetivos é permitir que administradores de redes ajustem facilmente o sistema para as suas necessidades ou situações particulares do dia-a-dia.

A primeira versão do sistema foi implementada utilizando *shell-scripts*. Uma característica marcante é a legibilidade, que torna a manutenção e extensão do sistema bastante simples. Outro fator que levou a essa opção esta relacionado aos usuários alvos, administradores de rede. Estes normalmente possuem ao menos algum conhecimento em linguagens *shell-script*. A maior parte dos gerenciadores de rede não são familiarizados com linguagens de programação como Perl, C e Java. Além disso, códigos nessas linguagens costumam ser menos legíveis e de difícil entendimento, pois as preferências de programação variam bastante de desenvolvedor para desenvolvedor. Não obstante a isso, a extensão ou adaptação do sistema demandaria mais trabalho caso o sistema fosse implementado em linguagens como Java ou C.

Apesar da simplicidade do sistema, os comandos de atualização e manipulação dos registros das bases de dados podem ser configurados para rodar sobre canais criptografados, utilizando SSL. O tráfego das senhas, por exemplo, é realizado com as mesmas criptografias e padrões de segurança utilizados pelos sistemas de autenticação para consultar e autenticar usuários na rede.

A praticidade e legibilidade do sistema permitem a fácil inclusão e manutenção de módulos. Uma outra característica é quanto a instalação do sistema. Ela é prática e fácil, bastando copiar o sistema para o local desejado, configurar algumas variáveis e o sistema estará funcional. Isso porque os comandos e módulos foram implementados utilizando caminhos relativos, ou seja, não há a necessidade de instalar o sistema (copiar os comandos) em local específico, como ocorre com sistemas como o *smbldap-tools* [Tournier, 2004].

As próximas seções apresentam algumas opções de configuração e funcionalidades do sistema.

3.1. Opções de configuração

Uma das características presentes no sistema é a possibilidade de configurá-lo para para diferentes ambientes. Ele pode ser utilizado para gerenciar simultaneamente diferentes bases de informação.

Na figura 2 são apresentadas algumas opções de configuração do sistema. No caso, o objetivo principal é trabalhar com OpenLDAP, NIS e Samba.

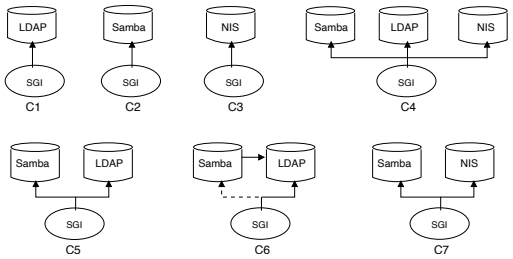

Figura 2: Ilustração de algumas possibilidades de configuração e utilização.

O sistema pode ser utilizado para gerenciar bases independentes, como é o caso das configurações C1, C2 e C3. As opções de configuração C4, C5, C6 e C7 buscam gerenciar simultaneamente mais de uma base de registros. Nestes casos, a manipulação dos dados de usuários é propagada para os diferentes diretórios *online*.

As configurações C4 e C6 representam dois casos especiais. A configuração C6 apresenta um leve diferencial em relação a arquitetura C5. Nela os dados do Samba são também armazenados no OpenLDAP, ou seja, existe apenas uma base de informação para ser gerenciada. Mas, por motivos de padronização, pode-se optar por continuar utilizando os comandos padrão do Samba. Neste caso, os comandos Samba terão seus efeitos propagados para o OpenLDAP pelo servidor Samba, o que torna o sistema mais compreensível e legível.

A configuração C4 é interessante para ambientes de transição, onde está sendo realizado o porte de sistemas. Neste contexto, manter temporariamente o NIS, Samba e LDAP pode ser uma boa opção, não necessitando portar e configurar de uma única vez todos os computadores da rede. Em uma situação desse gênero os três sistemas permanecerão ativos até que todas as máquinas e sistemas tenham sido devidamente configurados.

Permitir que o sistema facilmente seja configurado para alguma dessas configurações é relativamente fácil. A implementação pode seguir basicamente dois caminhos: utilização de vetores de comando ou módulos separados. No caso de vetores de comandos é executado o comando correspondente a cada configuração. Esta opção de configuração é indicada em um arquivo de configuração ou variável de ambiente do sistema. Uma alternativa é

a implementação de módulos independentes para as diversas configurações. Neste caso, quando o sistema for configurado, basta indicar o conjunto de módulos que serão utilizados. Essa segunda abordagem foi a escolhida na implementação da primeira versão do sistema.

3.2. Funcionalidades comuns

As funcionalidades padrão do sistema incluem: inclusão e remoção interativa de um usuário, alteração de dados cadastrais de um usuário, troca de senha, inclusão e remoção de grupos, listagem de usuários e grupos, listagem de dados específicos de um determinado grupo ou usuário, listagem dos usuários que pertencem a um determinado grupo (o que pode gerar mais de uma consulta a uma base OpenLDAP), bloqueio e liberação de usuários, troca de *login*, troca de *shell*, listagem de usuários bloqueados, listagem de usuários com senhas expiradas e inclusão e remoção de usuários em grupos. Muitas dessas funcionalidades estão presentes em praticamente qualquer sistema de gerenciamento de diretórios *online* como o OpenLDAP, NIS e Samba.

3.3. Funcionalidades complementares

Para facilitar o gerenciamento e cadastro de usuários o sistema possui algumas funcionalidades complementares. Entre elas podem ser citadas a inclusão de conjuntos de usuários, a geração de arquivos de configuração de leitores de e-mail, a inclusão de dados como arquivos de configuração e modelos de páginas pessoais (configuração e uso).

As *homes* dos usuários podem estar na máquina em que o sistema está rodando ou em uma máquina remota. Existem duas possibilidades de gerar os diretórios de usuários: 1) o servidor NFS[3] exporta o diretório raiz das *homes* para a máquina que roda o sistema; 2) utilizar comandos remotos para a geração dos diretórios dos usuários.

Uma característica interessante para laboratórios acadêmicos, por exemplo, é a possibilidade de gerar o cadastro simultâneo de um número qualquer de usuários a partir de um único arquivo de entrada. Na seqüência são apresentadas duas opções de configuração de um arquivo de entrada para o cadastro de vários usuários em massa.

Opção 1: o administrador do sistema entra apenas com o nome completo dos usuários. Nessa opção o administrador tem a possibilidade de solicitar ao sistema a geração de *logins* para os usuários e cadastro dos mesmos. O processo pode ser feito em dois passos: a) geração dos registros de cadastro; b) inclusão dos registros nas bases de dados. A primeira fase não é necessária. Ela é interessante somente quando o administrador deseja visualizar os registros antes que eles sejam efetivamente cadastrados. Abaixo segue um exemplo de como seria o arquivo de entrada no caso da opção 1.

```
# nome completo do usuario
Galinha Caipira
Porco Espinho
```

Opção 2: o administrador entra com os detalhes do usuário, como *login*, grupo e diretório raiz da *home*. Abaixo segue um exemplo de um arquivo de configuração para essa opção. Esse arquivo é semelhante ao que seria o arquivo intermediário da opção 1, comentada anteriormente.

```
# usuario | nome | grupo | diretório base
gcaipira|Galinha Caipira|administrador|/home/admin
pespinho|Porco Espinho|grp2004|/home/usuarios
```

No processo de geração do cadastro será avaliado a validade de grupos e *logins*. Caso algum grupo ainda não esteja cadastrado, será indicado a necessidade de cadastro do mesmo. Se algum *login* estiver duplicado no sistema será alertado a necessidade de modificar o(s) *login(s)* problemático(s). Neste caso, o administrador pode optar por uma geração automática de *logins* (opção 1), indicando ao sistema para tentar formar um *login* a

[3]Network File System (sistema de arquivo de rede)

partir do sobrenome e das iniciais dos demais nomes. Caso ainda existam *logins* duplicados, podem ser escolhidas opções como gerar um *login* a partir das inicias do nome ou apenas com o primeiro nome ou o sobrenome.

Ambas as opções (1 e 2) irão gerar dados de saída semelhantes aos que seguem.

```
# identificador  |    senha randômica      | identificador  login    nome do usuário
-------------------------------------------------------------------------------------------
       01        |        YuI8JkH          |       01       gcaipira   NOME: Galinha Caipira
-------------------------------------------------------------------------------------------
       02        |        MTb32YA          |       02       pespinho   NOME: Porco Espinho
-------------------------------------------------------------------------------------------
```

O resultado final do cadastro será um arquivo *ps*[4], pronto para ser impresso. As senhas e *logins* devem ser separados. Para manter a relação entre senhas e usuários existem os identificadores. Cada usuário receberá a sua senha provisória. Para tanto, basta destacar a senha do identificador e entrega-lá ao usuário.

O sistema, além de gerar a conta de um usuário e uma senha randômica, gera também o diretório *home* com algumas configurações e dados padrão. São criados os arquivos de configuração básica do *shell*, com alguns exemplos de uso, o diretório *public_html* com exemplos simples e documentados de páginas em *html* e *php*, é enviado um e-mail de boas vindas e contendo também informações sobre o uso da rede e é ainda criada uma configuração automática para leitores de e-mail como o *pine*. Desta forma o usuário recebe instruções básicas e essenciais de utilização e normas de conduta da rede.

O sistema pode ainda ser programado para controlar a expiração de senhas. Isso pode ser feito através do agendamento do módulo de verificação de expiração no `crontab` do sistema GNU/Linux. Caso a senha esteja próxima de expirar (número x de dias) é enviado um e-mail ao usuário informando o fato.

Os usuários podem trocar suas senhas via uma página segura. A página principal, para a troca de senhas, propaga a nova senha para todas as bases de dados. No entanto, caso o usuário preferir ele poderá manter senhas distintas para os diferentes sistemas (exemplo: uma senha para o OpenLDAP e outra para o Samba). Isso pode ser feito pelas páginas CGI auxiliares.

4. Trabalhos relacionados

O gerenciamento de diretórios *online* é uma necessidade antiga entre administradores de redes. Ferramentas como o Swat[5] [Team, 2004], Webmin [Cameron and et. al., 2004], gerenciador de cadastros LDAP[6] [Duergner et al., 2003], o pacote *yp-tools* [Kukuk, 2003], ferramenta gráfica de configuração do Samba[7] [Sam, 2003], gsmb [Foucher@gch.iut-tlse3.fr, 1999], JXplorer [Betts, 2002] e *smbldap-tools* [Tournier, 2004] auxiliam os administradores de rede a realizar tarefas de manutenção em serviços como o Samba, NIS e LDAP. A maior parte destas ferramentas são gerenciáveis por interface gráfica. No entanto, elas carecem no que diz respeito a integração e ao gerenciamento de ambientes como os que comumentemente figuram em redes locais de laboratórios de computação.

Cada uma dessas ferramentas possibilita o gerenciamento de alguns serviços. Elas possuem características distintas e particulares. Utilitários como o JXplorer e o LDAP Account Manager possibilitam o gerenciamento de hierarquias e contas de usuários em diretórios LDAP. Ferramentas como o Swat e o gsmb facilitam a manipulação de contas em servidores Samba. O pacote *yp-tools* inclui ferramentas para gerenciar o NIS. Com excessão

[4]PostScript (linguagem de descriç ˜ao em alto n´ıvel de p´aginas/telas/imagens impressas)
[5]Samba Web Administration Tool (ferramenta Web de administraç ˜ao do Samba)
[6]LDAP Account Manager (gerenciador de registros LDAP)
[7]Samba GUI Confi guration Tool (ferramenta gr´afi ca de confi guraç ˜ao do Samba)

do *yp-tools* e do *smbldap-tools*, as demais ferramentas possuem interfaces gráficas simples e amistosa. Porém, dependendo do tipo de operação desejada, essas interfaces tornam-se pouco práticas e flexíveis.

O conjunto de aplicativos do *smbldap-tools* demonstra ser o mais flexível e útil. Eles possibilitam o gerenciamento de bases de informação LDAP e Samba simultaneamente. Além de poder migrar dados de bases NT para LDAP. No entanto, para redes acadêmicas essa ferramenta carece de recursos auxiliares. Além disso, seu código é relativamente fixo, o que pode tornar a manutenção ou instalação pouco flexível.

É nesse sentido que surgiu a idéia, aqui apresentada, de um sistema de gerenciamento integrado de contas de usuários do LDAP, NIS e Samba. Simplicidade e organização estão entre suas características. Devido a isso, esse sistema também é facilmente extensível e adaptável a variados tipos de ambientes e especificidades de domínios administrativos.

5. Conclusão e Trabalhos Futuros

Muitas vezes o gerenciamento de sistemas de informação e autenticação de redes locais é uma tarefa pouco prática, pois é comum existir mais de uma base de dados de usuários para ser gerenciada. Isso por que normalmente são utilizados sistemas como o NIS, ou o OpenLDAP, e o Samba para a autenticação de sistemas Unix e Windows, respectivamente. Logo, um sistema que possibilite um gerenciamento síncrono e integrado é interessante em um ambiente desse gênero.

Este artigo apresentou um sistema simples e prático para realizar o gerenciamento integrado de diferentes bases de informação, como o OpenLDAP, NIS e Samba. Além disso, foram mostradas algumas características que podem ser interessantes e facilitar a vida de administradores de laboratórios de computação. Entre elas podem ser citadas o cadastro de usuários em massa, a configuração automática de leitores de e-mail como o pine, a geração de modelos de páginas *html* e *php* nas contas dos usuários e o controle de expiração das senhas.

Trabalhos futuros. Entre os trabalhos futuros estão a integração das diferentes configurações do sistema (seção 3.3), produção de uma documentação e disponibilização do sistema. Além disso, implementar e disponibilizar opções de personalização de comandos, ou seja, o usuário poderá definir o nome e o modo que melhor lhe convier para utilizar as funcionalidades do sistema.

Referências

(2003). Samba GUI Configuration Tool 1.0 Beta. `http://www.eatonweb.com/samba/`.

Betts, C. (2002). JXplorer - Java LDAP Browser. `http://jxplorer.org`.

Cameron, J. and et. al. (2004). Webmin. `http://www.webmin.com/`.

Duergner, M., Gruber, R., Lutz, T., and Walchshäusl, L. (2003). LDAP Account Manager. `http://lam.sourceforge.net/`.

Foucher@gch.iut-tlse3.fr (1999). Gsmb - simplified management of smbpasswd. `http://www.culte.org/projets/developpement/gsmb/`.

Kukuk, T. (2003). Linux NIS Tools: yp-tools. `http://www.linux-nis.org/nis/yp-tools/`.

Team, S. (2004). Swat - Samba Web Administration Tool. `http://us2.samba.org/samba/samba.html`.

Tournier, J. (2004). Smbldap-tools User Manual (Release: 0.8.4). `http://docs.biostat.wustl.edu/smbldap-tools/html/index.html`.