LINUX PARK 2008 p.26
No Rio de Janeiro, a praia é do Software Livre

HOBBY QUE DÁ DINHEIRO p.26
Entrevista com o criador do OSSEC

CAÇADOR DE VÍRUS p.24
Entrevista com o líder da F-Secure

LINUX NEW MEDIA
The Pulse of Open Source

45 Agosto 2008

LINUX MAGAZINE

A REVISTA DO PROFISSIONAL DE TI

Gerenciamento de PROJETOS

GERENCIAR PROCESSOS, PESSOAS E RECURSOS EXIGE TREINAMENTO E BOAS FERRAMENTAS p.33

» Métodos específicos para projetos de software p.34
» Workflow gerenciado com elegância pelo Bonita p.40
» Acompanhando tarefas de perto com o ClockingIT p.46

SEGURANÇA: SELinux p.66
O melhor sistema de segurança para Linux é muito eficaz, mas trabalhoso. Aprenda a usar, modificar e criar suas próprias regras

REDES: MONITORAMENTO p.60
Problemas de tráfego de rede? Com o MRTG, você ganha gráficos detalhados e também bonitos!

VEJA TAMBÉM NESTA EDIÇÃO:
» LPI nível 2: Autenticação LDAP e PAM p.50
» Ruby on Rails em cluster: monte o seu p.56
» PHP com Subversion no Eclipse p.74

Open Energy™

Open Access

Acesso a componentes de software validados e testados pela Bull

1

Open Service

Desenvolve e gerencia Projetos de Software Livre utilizando o ferramental Bull de Fábrica de Sistemas

3

2

Substitui suas tecnologias existentes nos atuais ambientes de desenvolvimento por alternativas de Software Livre

Open Exchange

4

Implementa processos empresariais utilizando com total segurança soluções de Software Livre

Open Enterprise

Nós implementamos um modelo industrial para o mundo do Software Livre

"Open Energy", a familia Bull de Serviços para Software Livre. Nossas soluções respondem a todas as necessidades para o desenvolvimento, integração, interoperabilidade e manutenção de sistemas requeridas por todos os tipos de organizações que tomam o rumo do Software Livre. Estabelecida sobre os fortes alicerces da ampla infraestrutura Bull de Integração, Serviços e Centros de Competência Internacionais, a "Open Energy" lhe da acesso aos melhores especialistas e comunidades de desenvolvimento.

BULL

Architect of an Open World™

www.bull.com

Expediente editorial

Diretor Geral
Rafael Peregrino da Silva
rperegrino@linuxmagazine.com.br

Editor-chefe
Tadeu Carmona
tcarmona@linuxmagazine.com.br

Editor
Pablo Hess
phess@linuxmagazine.com.br

Redator
Rodrigo Amorim
ramorim@linuxmagazine.com.br

Revisão
Aileen Otomi Nakamura
anakamura@linuxmagazine.com.br

Editora de Arte
Paola Viveiros
pviveiros@linuxmagazine.com.br

Assistente de Arte
Rafael Carvalho
rcarvalho@linuxmagazine.com.br

Centros de Competência
Centro de Competência em Software:
Oliver Frommel: ofrommel@linuxnewmedia.de
Kristian Kißling: kkissling@linuxnewmedia.de
Peter Kreussel: pkreussel@linuxnewmedia.de
Marcel Hilzinger: hilzinger@linuxnewmedia.de
Centro de Competência em Redes e Segurança:
Achim Leitner: aleitner@linuxnewmedia.de
Jens-Christoph B.: jbrendel@linuxnewmedia.de
Hans-Georg Eßer: hgesser@linuxnewmedia.de
Thomas Leichtenstern: tleichtenstern@linuxnewmedia.de
Max Werner: mwerner@linuxnewmedia.de
Markus Feilner: mfeilner@linuxnewmedia.de
Nils Magnus: nmagnus@linuxnewmedia.de

Anúncios:
Rafael Peregrino da Silva (Brasil)
anuncios@linuxmagazine.com.br
Tel.: +55 (0)11 4082 1300
Fax: +55 (0)11 4082 1302

Petra Jaser (Alemanha, Áustria e Suíça)
anzeigen@linuxnewmedia.de

Penny Wilby (Reino Unido e Irlanda)
pwilby@linux-magazine.com

Amy Phalen (Estados Unidos)
aphalen@linuxmagazine.com

Hubert Wiest (Outros países)
hwiest@linuxnewmedia.de

Gerente de Circulação
Mirian Domingues
mdomingues@linuxmagazine.com.br

Na Internet:
www.linuxmagazine.com.br – Brasil
www.linux-magazin.de – Alemanha
www.linux-magazine.com – Portal Mundial
www.linuxmagazine.com.au – Austrália
www.linux-magazine.ca – Canadá
www.linux-magazine.es – Espanha
www.linux-magazine.pl – Polônia
www.linux-magazine.co.uk – Reino Unido
www.linux-magazin.ro – Romênia

Linux Magazine é publicada mensalmente por:

Linux New Media do Brasil Editora Ltda.
Av. Fagundes Filho, 134
Conj. 53 – Saúde
04304-000 – São Paulo – SP – Brasil
Tel.: +55 (0)11 4082 1300
Fax: +55 (0)11 4082 1302

Distribuição: Distmag
Impressão e Acabamento: Parma

Atendimento Assinante

www.linuxnewmedia.com.br/atendimento
São Paulo: +55 (0)11 3512 9460
Rio de Janeiro: +55 (0)21 3512 0888
Belo Horizonte: +55 (0)31 3516 1280

ISSN 1806-9428 **Impresso no Brasil**

INSTITUTO VERIFICADOR DE CIRCULAÇÃO

As velhas falácias

Prezados leitores,

Por mais que sejam discutidas, explicadas e refutadas, algumas falácias parecem se perpetuar incompreensivelmente. A atração exercida por certas crendices ultrapassa o apelo da razão.

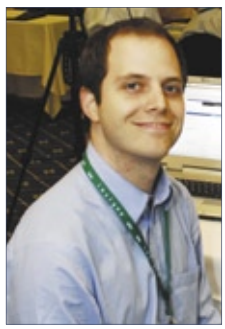
Mesmo sem qualquer evidência científica que demonstre os efeitos deletérios decorrentes da ingestão de manga com leite, diversas pessoas ainda propagam essa idéia. Nenhum dos incontáveis consumidores dos saborosos sorvetes de manga jamais morreu por conta dessa combinação, e há indícios de que o "mito" teria sido criado maquiavelicamente pelos escravocratas para evitar que seus escravos – com fácil acesso a mangas – consumissem o valioso leite que obtinham.

A questão dos motivos para a parca existência de vírus para sistemas baseados no Unix, em especial o Linux, também parece cercada de crendices e falácias. Comparado aos sistemas Windows, o Linux se parece com um deserto de vírus. Porém, esse deserto é habitado: a Wikipédia informa que em 2005 foram criados mais de 800 novos vírus para o sistema aberto, e acrescenta que o número vem crescendo anualmente.

A diferença entre os sistemas, como se conclui, é sua vulnerabilidade a ameaças. Apesar disso, ainda vemos profissionais altamente qualificados, muitos deles inclusive atuantes na indústria da segurança de TI, que provavelmente jamais experimentarão sorvete de manga, pois propagam a idéia de que há menos vírus para Linux porque as máquinas Windows são mais atraentes para os autores de vírus.

Difícil acreditar que servidores de bancos, lojas online ou qualquer site que comercialize produtos via Web – nos quais o Linux está maciçamente presente – sejam menos atraentes que simples desktops. Num ataque de sucesso a um desses servidores, o agressor obtém imediatamente algumas centenas ou milhares de informações valiosas; enquanto isso, cada desktop invadido precisa ser vasculhado independentemente em busca dos dados financeiros (que, aliás, ele pode nem ter armazenados) de uma única pessoa.

O Linux é, sim, mais seguro que o sistema da Microsoft. É positivo que a discussão sobre segurança comparativa de sistemas agora já parta desse princípio, questionando apenas os motivos da diferença. Porém, propagar a antiga falácia de que a razão para esse quadro é externa ao sistema de código aberto é, no mínimo, injusta – e, no máximo, ignorante. ■



CAPA

Precisa ser preciso 33

Para evitar que seus projetos excedam os custos e prazo acordados e alcancem a qualidade exigida, é necessário gerenciá-los com precisão.

Bom projeto, bom gerenciamento... bons resultados 34

Começar um projeto é fácil… difícil é conduzí-lo, com largas margens de sucesso, para a sua conclusão final.

Fluxo sincronizado 40

O sistema de workflow de código aberto Bonita é comparável às melhores alternativas comerciais e conta com o apoio de grandes empresas.

Na hora exata 46

O ClockingIT é uma solução de gerenciamento de projetos rica em recursos livres e com uma bela interface web. Basta optar entre as versões local e hospedada nos servidores do projeto e usar.

COLUNAS

Augusto Campos 08
Charly Kühnast 10
Klaus Knopper 12
Zack Brown 14
Notícias de Insegurança 16

NOTÍCIAS

Geral 18
- Lançado o ALSA 1.0.17
- MPX: Compiz com mais apontadores
- Novo comando na Gnome Foundation
- Workshop na Grande São Paulo
- Kolab 2 móvel
- São Paulo sedia IV SlackShow

CORPORATE

Notícias 20
- Intel recusa adoção do Vista
- Xandros adquire Linspire
- Para Sun, SL/CA dá mais lucro
- Linux domina supercomputadores
- Virtualização diferente na Red Hat
- ABNT contesta ISO

Entrevista: F-Secure 24
Entrevista: OSSEC 26
Artigo: Linux Park 28
Coluna: Cezar Taurion 32

TUTORIAL

LPI nível 2: Aula 14 50
Autenticação remota com os sistemas LDAP e PAM.

Cluster nos trilhos 56
O desenvolvimento de aplicações web com Ruby on Rails é bem ágil, mas isso não significa baixo desempenho.

REDES

Imagem é tudo 60
O MRTG gera gráficos simples para visualização rápida do desempenho da rede.

SEGURANÇA

Acesso restrito 66
O SELinux oferece um sistema mais seguro por meio do poderoso conceito dos controles obrigatórios de acesso.

PROGRAMAÇÃO

Eclipse controlado 74
O plugin PHPEclipse traz ao famoso IDE a capacidade de funcionar com o PHP, enquanto o Subclipse acrescenta o controle de versões.

SERVIÇOS

Editorial 03
Emails 06
Linux.local 78
Eventos 81
Índice de anunciantes 80
Preview 82

Emails para o editor

Permissão de Escrita

Se você tem dúvidas sobre o mundo Linux, críticas ou sugestões que possam ajudar a melhorar a nossa revista, escreva para o seguinte endereço: ***cartas@linuxmagazine.com.br****. Devido ao grande volume de correspondência, torna-se impossível responder a todas as dúvidas sobre aplicativos, configurações e problemas de hardware que chegam à Redação, mas garantimos que elas são lidas e analisadas. As mais interessantes são publicadas nesta seção.*

Aprovado!

Recentemente eu escrevi para a revista dizendo que usei no final da preparação da prova LPI 101 o conteúdo publicado na Linux Magazine e pude comprovar que muito do conteúdo lá informado caiu realmente na prova. E mais uma novidade: ontem prestei a prova LPI 102 e consegui êxito. Hoje é meu primeiro dia como LPIC2 e segui novamente o ritual que deu certo: estudei e, como final da preparação, li a Linux Magazine. Agora vou me dedicar a meu curso ITIL (também influenciado pelo mercado e pela última edição da LM). Obrigado à Linux Magazine Brasil pelo meu aperfeiçoamento profissional.

Fabricio Silva

Resposta

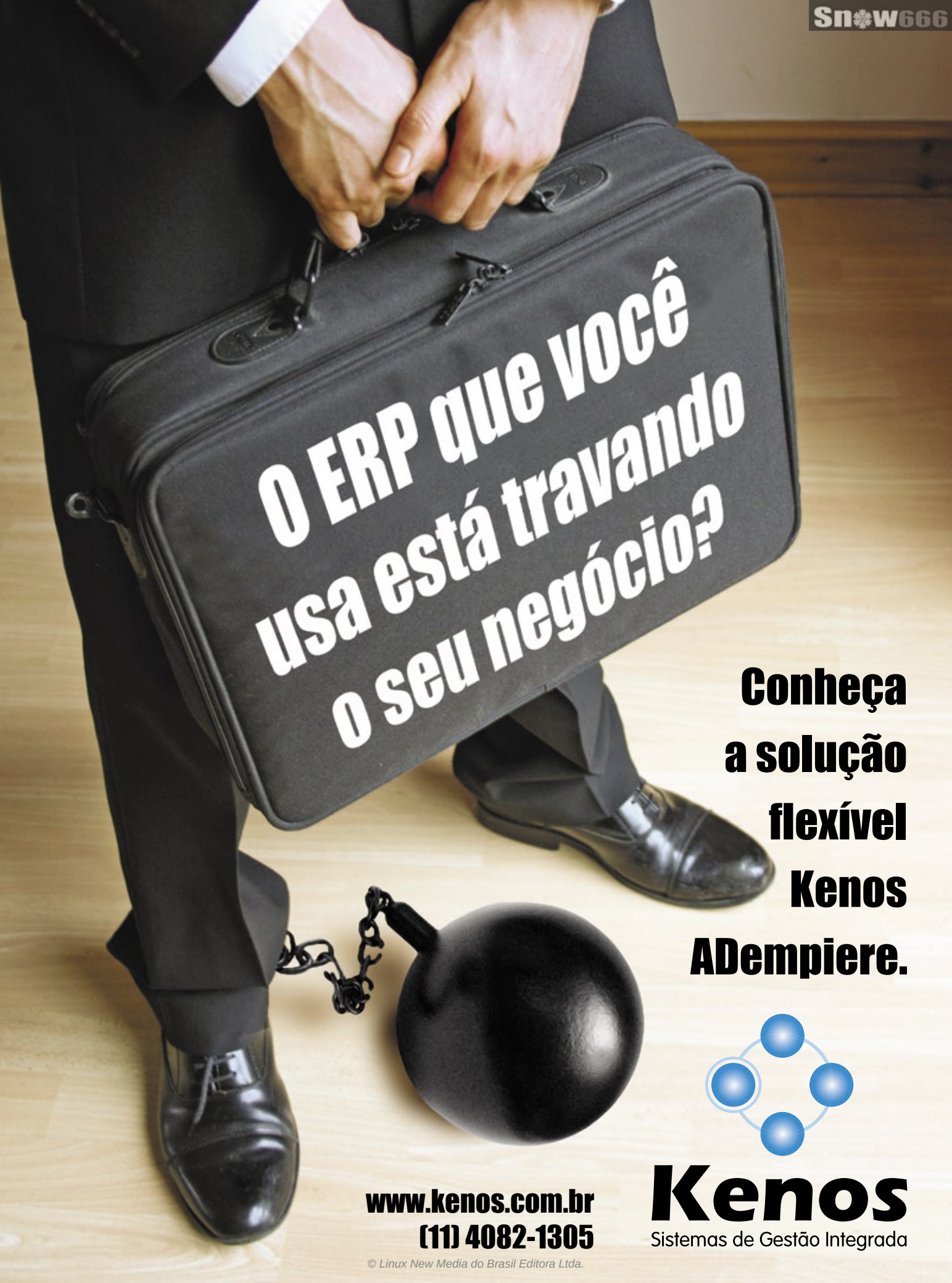
Parabéns mais uma vez, Fabricio. Reitero que é muito gratificante para a equipe da Linux Magazine contribuir para o sucesso profissional de nossos leitores. Esperamos sinceramente que possamos ajudar cada vez mais leitores a alcançar o sucesso.

Novamente, muito obrigado pelo depoimento, parabéns pela conquista e muito sucesso.

Errata

Na Linux Magazine 44, o índice das matérias de capa, na página 37, foi publicado incorretamente. O correto seria:

Boa e prática	pág. 39
Terceira versão	pág. 44



Conheça
a solução
flexível
Kenos
ADempiere.

www.kenos.com.br
(11) 4082-1305

Kenos
Sistemas de Gestão Integrada

COLUNA

O punk e o Software Livre

Augusto Campos

Há algumas semelhanças entre o Software Livre e o movimento punk. É interessante saber aproveitar o melhor lado disso.

por Augusto Campos

O movimento punk, do alto de seus mais de 30 anos de idade, influenciou em algum momento muitos de nós, seja diretamente – pela música, estética ou atitude punk – ou indiretamente, por intermédio de tantos formadores de opinião e figuras públicas que em algum momento estiveram mais perto do fenômeno.

É difícil definir o que é, em sua essência, o punk. Mas há alguns pontos que constam em todas as definições, e um deles é a ética do "Faça Você Mesmo" (*Do It Yourself*, ou DIY). Seguindo o DIY, bandas e grupos alcançaram seus objetivos e até mesmo o sucesso usando até onde possível os seus próprios meios – desde a metafórica fita demo gravada na garagem até os shows em porões, cartazes mimeografados e divulgação de manifestos por intermédio de fanzines que circulavam de mão em mão.

> ***Se você usufrui do software da comunidade livre, tire alguns minutos para refletir sobre qual tem sido seu papel.***

O Código Aberto, em seu sentido mais comunitário, tem muitos pontos de contato com o DIY conforme visto pelo movimento punk. Embora grande parte do desenvolvimento e disseminação ocorram hoje dentro de corporações e voltados para outras corporações, o espaço para os desenvolvedores "de garagem", seja em carreira solo ou em grupos, continua garantido e valorizado.

Os cartazes mimeografados foram substituídos pelos blogs, sites e wikis da comunidade, mantidos por indivíduos e grupos que dedicam tempo e recursos para divulgar as iniciativas da comunidade e as últimas novidades que lhes interessam, tendo o lançamento das novas versões de distribuições e projetos relevantes como o equivalente aos shows das maiores bandas, e os eventos comunitários no lugar dos festivais.

Os manifestos continuam circulando, mas agora nas listas de discussão e fóruns. Podem ser pura opinião recheada de espírito crítico, assim como podem assumir a forma de tutoriais ou compartilhamento de dicas sobre como realizar determinadas tarefas, e circulam livremente, às vezes literalmente de mão em mão.

Assim como no caso do punk, alguns integrantes e projetos eventualmente acabam atingindo o *mainstream*, às vezes até mesmo integrando-se a alguma corporação. Assim, uma parte do público comemora o sucesso e o aumento da visibilidade que a vitória proporciona, enquanto outra parte do mesmo público encara a situação como uma lástima e considera os envolvidos como vendidos ou até mesmo traidores do movimento – um fenômeno dual que provavelmente perdurará para sempre em todos os movimentos abertos.

Mas o que importa é continuar produzindo e disseminando, com fidelidade aos seus princípios e valores. Se você usufrui do software da comunidade livre, tire alguns minutos para refletir sobre qual tem sido seu papel.

Quantas linhas de código você disponibilizou, quantos bugs relatou aos autores, quantos documentos ajudou a traduzir ou revisar, quantas dúvidas de usuários ajudou a resolver nos últimos meses? Faça você mesmo a sua parte, e faça-a bem – é assim que a comunidade avança. ■

Sobre o autor

Augusto César Campos é administrador de TI e, desde 1996, mantém o site BR-linux.org, que cobre a cena do Software Livre no Brasil e no mundo.

Estar um passo à frente é ter hoje

VoIP

SUPORTE À TELECOM

SERVIDORES DE REDE

o que os outros só terão amanhã.

Surpreenda-se com a economia e confiabilidade dos nossos serviços VoIP, Suporte à Telecom e Servidores de Rede.

Conte com a Propus e deixe sua empresa sempre um passo à frente em TI.

Propus

Um passo à frente em TI

www.propus.com.br

info@propus.com.br
+55 51 3024.3568
+55 11 4063.8864

COLUNA

Combatendo ataques de dicionário com Sshutout e Fail2ban

Charly Kühnast

Serviços que exigem nome de usuário e senha para o login são alvos potenciais para ataques de dicionário. O Sshutout e o Fail2ban aplicam penalidades de tempo para tentativas inválidas.

por Charly Kühnast

O *Sshutout*[1] é um *daemon* escrito em C que procura logins SSH inválidos em intervalos freqüentes. Se descobrir um padrão de tentativas frustradas de login por um único cliente, ele bloqueia esse cliente de acordo com regras do Iptables. Após um intervalo configurável, a penalidade é automaticamente revogada.

Esteja banido

Para instalar o *tarball*, bastam os comandos padrão `make; make install`.

O daemon se localiza no diretório `/usr/local/sbin/` após a instalação e seu arquivo de configuração é `/etc/sshutout.conf`.

O arquivo de configuração permite a especificação de vários parâmetros. É extremamente importante especificar o nome correto do arquivo de log que se deseja que o Sshutout monitore. O padrão é `/var/log/messages`, mas muitas distribuições gravam as informações de login em outros arquivos. No Ubuntu, por exemplo, a configuração seria:

```
sshd_log_file = /var/log/auth.log
```

A opção de limite especifica o *LOS* (*level of stupidity*, ou nível de estupidez). Em outras palavras, ela define quantas tentativas de login são necessárias para um cliente ser bloqueado temporariamente. Caso haja muitas senhas ou pouca memória, talvez seja interessante aumentar esse valor (o padrão é `4`).

Tempo no xadrez

O tempo de bloqueio tem relação com o valor do limite. Por um lado, é necessário evitar ataques de força bruta com a maior eficácia possível; por outro, não é uma boa idéia bloquear os usuários durante horas simplesmente porque eles perdem a memória depois de uma noite de agito. O valor padrão, cinco minutos, é um bom meio-termo: `delay_penalty = 300`.

Esse valor dá ao usuário tempo suficiente para beber uma xícara de café e refrescar sua memória. Alternativamente, pode-se excluir esquecedores contumazes de senha do grupo sujeito à penalização. O arquivo de configuração possui uma linha para estabelecimento de uma "lista amiga" (`Whitelist`) a receber os nomes ou endereços IP das máquinas que jamais devem ser bloqueadas.

O Sshutout também atualiza essa lista de forma autônoma. Ao ser iniciado, ele exibe um panorama das configurações atuais, incluindo as seguintes linhas:

```
Whitelist:
    213.133.98.97
    10.0.0.254
    10.0.0.214
```

Isso significa que a lista amiga do Sshutout automaticamente exclui seu próprio endereço IP, o *gateway* padrão e o servidor DNS. Isso não deve representar perigo, mas administradores mais cuidadosos certamente vão preferir usar `auto_whitelist = no`.

O Sshutout também registra suas próprias atividades em `/var/log/sshutout.log` por padrão. Se um cliente for bloqueado, uma entrada relativa a ele é gravada no arquivo:

```
10.0.0.42 blocked on Sat Feb 02 15:32:32 2008
```

O comando `iptables -L` permite que se confira as regras do firewall relativas ao Sshutout. Uma função para tratamento de exceções lida com os casos em que um cliente inicia uma conexão SSH mas não cria uma entrada, o que geralmente é resultado de ataques de negação de serviço. Por padrão, o programa ignora esses tipos de conexão. A entrada `illegal_user = yes` ordena que o Sshutout trate esses casos como qualquer outra tentativa frustrada de login.

Fail2ban

O Fail2ban[2] usa basicamente a mesma técnica que o Sshutout; entretanto, ele não se restringe ao SSH. Na verdade, ele pode proteger qualquer serviço que

exija o login dos usuários. O Fail2ban toma decisões com base nas entradas do arquivo de log, mas usa uma técnica diferente.

A ferramenta é dividida em dois componentes: um servidor e um cliente. O servidor monitora os arquivos de log e as regras do Iptables. O administrador pode usar o cliente para enviar comandos ao servidor para alterar, por exemplo, o nível de log.

O arquivo de configuração `jail.conf` define vários serviços que o Fail2ban pode proteger, com o SSH encabeçando a lista:

```
[ssh]
    enabled  = true
    port     = ssh,sftp
    filter   = sshd
    logpath  = /var/log/auth.log
    maxretry = 6
```

As seções abaixo dessa contêm os parâmetros dos outros serviços. Cada uma dessas seções é um "jail", no jargão do Fail2ban. A entrada `filter = sshd`, por exemplo, é equivalente a um arquivo no diretório `/etc/fail2ban/filter.d/`. O arquivo contém uma expressão regular que o servidor Fail2ban procura no arquivo de log. Não é possível configurar a duração do bloqueio do usuário de forma específica para cada serviço, pois essa configuração é definida como 600 segundos na seção global `[DEFAULT]`. Se esse tempo for longo demais, pode-se acrescentar uma entrada `bantime = 300` na seção `[ssh]`.

Proteção contra DoS

O SSH possui dois *jails*: o já mencionado e o *sshd-ddos*. Esse jail não é projetado para impedir tentativas de adivinhação de senha, mas para resistir a ataques de negação de serviço (DoS) que abrem conexões com o daemon SSH sem fornecerem senha. Nesses casos, o arquivo de log exibe mensagens como:

```
ssh Did not receive identification string from
➥10.0.0.150
```

Apesar de ser possível configurar múltiplas expressões regulares por jail, muitos administradores preferem atribuir diferentes tempos de bloqueio para ataques DoS distribuídos (DDoS). Ou seja, dividir as regras entre as categorias `[ssh]` e `[sshd-ddos]` faz muito sentido.

O jail SSH é o único ativo por padrão; todos os outros – incluindo o sshd-ddos – precisam ser habilitados manualmente.

```
File  Edit  View  Terminal  Tabs  Help
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
fail2ban-ssh  tcp  --  anywhere             anywhere            multiport dports ssh,sftp
fail2ban-apache  tcp  --  anywhere             anywhere            multiport dports www,https

Chain fail2ban-apache (1 references)
target     prot opt source               destination
DROP       0    --  shetland.kuehnast.com        anywhere
RETURN     0    --  anywhere             anywhere

Chain fail2ban-ssh (1 references)
target     prot opt source               destination
RETURN     0    --  anywhere             anywhere
```

Figura 1 Regras do *Apache*: o *Fail2ban* pode proteger vários aplicativos diferentes.

Esquemão

Se um usuário digitar a senha errada múltiplas vezes, os resultados serão semelhantes aos resultados do Sshutout: uma regra do Iptables será acionada para bloquear todas as conexões a partir do computador suspeito pelos próximos cinco minutos.

A proteção de outros serviços segue o mesmo padrão (**figura 1**). Caso haja várias páginas web protegidas por senha no *Apache*, o Fail2ban oferece um jail para elas:

```
[apache]
     enabled  = false
     port     = http,https
     filter   = apache-auth
     logpath  = /var/log/apache*/*access.log
     maxretry = 3
```

que deve ser levemente modificado.

Após fazer alterações no arquivo de configuração do Fail2ban, a ativação das mudanças depende apenas da execução do comando:

```
fail2ban-client start apache
```

Esse comando faz o servidor adicionar a entrada `[apache]` à lista de jails ativos. Para experimentá-lo, basta tentar várias senhas incorretas com o cliente e verificar no servidor as regras do Iptables. ■

Mais informações

[1] Sshutout: http://www.techfinesse.com/sshutout/sshutout.html

[2] Fail2ban: http://www.fail2ban.org

Sobre o autor

Charly Kühnast é administrador de sistemas Unix no datacenter Moers, perto do famoso rio Reno, na Alemanha. Lá ele cuida, principalmente, dos firewalls.

COLUNA

Pergunte ao Klaus!

Klaus Knopper

O criador do Knoppix responde as mais diversas dúvidas dos leitores.

por Klaus Knopper

Disparidade em FTP

Estou impressionado com um efeito que tenho visto ao transferir arquivos de vídeo entre duas máquinas. Da máquina Windows XP para a máquina Linux, interligadas por Gigabit Ethernet, a transferência por FTP alcança mais de 600 MB/s, enquanto o sentido inverso só chega a 20 MB/s.

A taxa máxima ao copiar qualquer coisa da máquina Linux para um disco USB, por exemplo – ou até mesmo simplesmente duplicar um arquivo –, é de 20 a 28 MB/s. As leituras são feitas pelo diálogo de transferência do KDE.

Resposta

É difícil dizer o que causa a diferença, pois muitos componentes estão envolvidos em seu *benchmark*. Para um benchmark mais confiável, eu recomendaria algumas ferramentas de linha de comando presentes no Linux.

Primeiramente, eu verificaria as configurações da placa de rede com:

```
sudo ethtool eth0
```

No resultado desse comando, pode-se ver os modos de transferência de dados suportados. Por exemplo, a placa pode estar rodando a 10 MB/s, apesar de ser capaz de chegar a 100 MB/s. Isso pode estar relacionado à auto-negociação, em que o switch determina a velocidade considerada mais confiável. É possível desativar a auto-negociação e especificar a velocidade de 100 MB/s com:

```
sudo ethtool -s eth0 autoneg off
➥ speed 100
```

No seu caso, você deve experimentar a opção `speed 1000`. Para medir a velocidade bruta de transferência de dados, você pode usar a ferramenta *bing*:

```
sudo bing ip_da_máquina_local
➥ ip_ da_máq_remota
```

Isso envia dados e mede o tempo de resposta até serem pressionados **[Ctrl]+[C]**. Em seguida, depois mostra estatísticas sobre a transferência dos dados. Os números exibidos são a maior velocidade atingível com essa configuração da interface de rede, sem o *overhead* dos dados da aplicação.

Para medir a velocidade do FTP, pode-se usar o *wget*, por exemplo.

No caso de cópias para o disco (você disse que operações em disco parecem lentas na máquina Linux), por favor note que o Linux e o Windows usam o cache de disco de formas diferentes. Somente quando são copiados dados maiores do que a memória RAM disponível é possível verificar de fato o desempenho bruto do disco e, mesmo assim, em picos, pois os dados vão primeiro para a memória para depois serem gravados no disco de forma assíncrona.

Apesar de 20 a 28 MB/s ser o esperado em dispositivos USB 2.0, é lento demais para discos IDE ou SATA recentes. Por isso, vale a pena verificar com o *hdparm* se o DMA está ativado no disco em questão.

Escrever em discos flash USB é muito lento. Assim como ocorre com discos rígidos, as operações só "parecem" rápidas de gravação antes de mandar o sistema operacional desconectar o dispositivo e efetivamente gravar nele os dados.

Como a transferência pela rede entre seus dois computadores parece ser rápida, talvez o lado receptor seja lento para informar que recebeu dados. Ou, por algum motivo, ele pode estar tentando resolver nomes de máquinas em IPs locais ausentes no arquivo `hosts`. Você tentou subir arquivos nas duas direções? Ou o servidor FTP só está rodando em uma das máquinas? ■

Sobre o autor

Klaus Knopper é o criador do *Knoppix* e co-fundador do evento *Linux Tag*. Atualmente trabalha como professor, programador e consultor.

Sempre aparece alguém prometendo a solução para todos os seus problemas. A diferença é que a Itautec cumpre a promessa.

Segurança e Infra-estrutura. É-exatamente-o-que-eu-preciso.

Saiba tudo o que acontece na sua empresa com a Tecnologia Itautec. Para você ter mais segurança e integração, a Itautec dá aos seus clientes controle, monitoramento e gerenciamento com recursos administrados pela Tecnologia Itautec. Para dar tranqüilidade na gestão de seus negócios, oferece a você um serviço de infra-estrutura que fornece ferramentas de cabeamento, instalação, atualização e suporte. Se você precisa de segurança, integração e comodidade, conte com a **Tecnologia Itautec, a melhor tradução de TI.**

Acesse www.itautec.com.br ou ligue 0800 121 444.

COMPROMISSO COM A SUSTENTABILIDADE

Itautec

COLUNA

Crônicas do kernel

Zack Brown

Problemas dentro do kernel e infinitas possibilidades fora dele. Quem disse que amadurecer é fácil?

por Zack Brown

Big Kernel Lock

Linus Torvalds postou um *patch* para desfazer uma grande alteração no sistema de bloqueios (*locks*) do kernel. O *grande bloqueio do kernel* (BKL, para os íntimos) havia sido alterado a partir de um *spinlock*, com alguns problemas de latência, para um semáforo. Isso representou um grande avanço para quem desenvolvia monitores de saúde para hospitais (e também para quem aprecia jogos de tiro em primeira pessoa).

A solução do semáforo também ocasionou grandes problemas de desempenho em certos *benchmarks*, e as soluções para eles não resolveram tudo. Então, Linus decidiu que a forma simples seria voltar à forma antiga.

Linus também indicou que a única forma de contornar o problema do spinlock seria eliminar inteiramente o BKL. Ingo Molnar, auto-declarado "viciado em latência", não gostou disso, mas aceitou a colocação de que a solução seria cortar o BKL pela raiz. Acontece que eliminar o BKL é difícil! Foram necessários os talentos de Alan Cox (palavras de Ingo) para se aventurar no labirinto semântico e entender o que e como mudar nessa área. Segundo os cálculos de Ingo, até mesmo com desenvolvedores como Alan já mergulhados nessa tarefa, o ritmo atual exigiria mais de dez anos para remover o BKL. Ingo explicou o problema, dizendo que "suas dependências são totalmente desconhecidas e invisíveis e tudo está perdido nos últimos 15 anos de alterações no código. Tudo isso acabou criando uma espécie de medo, incerteza e dúvida relativas ao BKL: ninguém o conhece direito, ninguém se atreve a tocá-lo e o código pode quebrar silenciosa e sutilmente se o BKL estiver errado".

A solução de Ingo foi criar uma árvore *git* especificamente para receber as particularidades mais assustadoras do BKL, com o objetivo final de facilitar a remoção em massa do código. Um dos primeiros passos principais foi extraí-lo do código central do kernel e mover toda a sua feiúra para algum lugar em que possa ser completamente substituído (ao menos teoricamente) no futuro, mudando o comportamento ao longo de todo o kernel assim que se criar uma implementação melhor. Como disse Ingo, "uma vez que essa árvore se estabilize, a eliminação do BKL pode ser feita da forma normal de se eliminar grandes bloqueios – empurrando-os para os subsistemas, substituindo-os por bloqueios específicos de cada subsistema, dividindo-os e, finalmente, eliminando-os. Já fizemos isso várias vezes no passado e há muitos desenvolvedores capacitados que pode atacar tais problemas".

Andi Kleen gostou do plano, mas preferiu não esperar. Em vez de ter uma árvore git separada para todas as alterações, por que não efetuá-las no ramo oficial? Linus e vários outros hackers também gostaram de ver Ingo trabalhando nisso e ofereceram inúmeras sugestões.

Porte do Linux para... tudo?

Octavian Purdila, Stefania Costache e Lucian Adrian Grijincu estão essencialmente tentando portar o Linux para rodar em qualquer outro projeto de programação. Eles o chamam de *Linux Kernel Library Project*, e o objetivo é converter vários códigos, como o *Virtual File System* do Linux, por exemplo, em bibliotecas genéricas que permitam que qualquer pessoa as insira em seus projetos.

Caso os programadores tenham êxito, qualquer sistema operacional será nativamente capaz de suportar qualquer recurso do Linux, bastando usar essa biblioteca. A abordagem é criar a biblioteca como um porte direto do Linux para uma arquitetura virtual que depois poderá ser usada para qualquer objetivo.

Octavian, Stefania e Lucian já obtiveram algum progresso e estão procurando voluntários para ajudá-los a manter o porte atualizado em relação ao kernel. ■

Sobre o autor

A lista de discussão *Linux-kernel* é o núcleo das atividades de desenvolvimento do kernel. **Zack Brown** consegue se perder nesse oceano de mensagens e extrair significado! Sua *newsletter Kernel Traffic* esteve em atividade de 1999 a 2005.

NovaForge™

Nós conectamos nossos Clientes a nossos Centros de Competências de Software Livre

NovaForge, no centro da abordagem Industrial para Desenvolvimento de Sistemas da Bull.

O NovaForge é um poderoso conjunto de ferramentas e serviços amplamente testados e projetados para reduzir o esforço, otimizar custos de gestão e cronogramas, garantindo a qualidade dos produtos finais em Projetos de Desenvolvimento de Sistemas. O NovaForge foi concebido para ser utilizado em Projetos de Desenvolvimento e Atualização de Aplicações em ambientes J2EE, PHP e .net , na manutenção de aplicações desenvolvidas por terceiros e para o teste profissional e integrado dos sistemas.

BULL

Architect of an Open World™

www.bull.com

Caixa de areia

Insegurança

O mecanismo chroot não foi criado como ferramenta de segurança, mas algumas precauções em seu uso são importantes nessa área.

por Kurt Seifried

Se você é como eu, você adora testar novos softwares. Neles está uma das enormes vantagens do mundo do Código Aberto. Quase tudo está a um simples `wget; /configure; make; make install` de distância e não é preciso pagar, registrar-se, dar informações pessoais ou esperar uma semana pela chegada do CD.

Porém, como se pode ter certeza de que o software não vai interferir com seu sistema, sobrescrever algo ou simplesmente se comportar mal? E se você quiser rodar um *Web service* com histórico conhecido de problemas que permitem a execução remota de código no servidor web?

Sandbox

Uma técnica comum de programação e administração de sistemas é usar *sandboxes* (caixas de areia, literalmente), que são áreas restritas para o software (ou, em alguns casos, todo um sistema operacional ou grupo de sistemas) ser executado, na qual ele não pode interferir com sistemas em produção. Ao instalar uma área protegida para testes, você sabe que, se algo sair errado, é pouco provável que o programa cause problemas graves, como afetar os servidores de arquivos ou web. Além disso, é mais fácil observar e verificar o comportamento do software porque não há muitos eventos dentro de uma sandbox.

Felizmente, ao longo dos últimos anos, vários avanços na computação facilitaram muito o primeiro requisito para sandboxes (o isolamento). Processadores mais velozes, discos maiores e memória barata, em conjunto com a difusão dos softwares de virtualização, agora significam que quase qualquer um com um computador recente – pelo menos 1 a 2 GHz e 512 MB de RAM – pode facilmente executar pelo menos um sistema operacional inteiro sobre o sistema já presente.

Infelizmente, muitos desses produtos não ajudam muito no segundo requisito (monitoramento e controle), com alguns exigindo (i) que o sistema virtualizado seja modificado significativamente ou (ii) o uso de arquivos virtuais para abrigar o conteúdo do disco rígido do hóspede.

Sandbox com virtualização

Há inúmeras soluções de virtualização, como *Bochs*[1], *Xen*[2], *User-Mode Linux*[3], *VirtualBox*[4], *KVM*[5], *OpenVZ*[6], *Qemu*[7] e o gratuito, porém proprietário, *VMware Server* [8] – demais para cobrir nesta coluna.

A principal desvantagem desses produtos é que eles guardam as imagens dos discos hóspedes como arquivos no hospedeiro – então, examinar o "disco rígido" do sistema hospedeiro requer a parada ou suspensão do sistema, seguida da montagem da imagem do disco.

A vantagem é que é possível literalmente parar um sistema operacional no tempo, examinar um "instantâneo" seu e reativar o sistema ao final.

Sandbox com chroot

Às vezes, no entanto, colocar um sistema operacional inteiro em uma sandbox pode ser um exagero. E se você desejar apenas compilar algum software e instalá-lo sem afetar o sistema em execução, ou simplesmente permitir a remoção fácil do software? Estranhamente, esse é exatamente o mesmo desafio que Bill Joy enfrentou enquanto trabalhava com seu BSD nos anos 1980. Sua solução foi criar a chamada de sistema `chroot` e seu programa utilitário de mesmo nome.

Com o chroot, é preciso lembrar-se de algo muito importante: ele não foi criado como mecanismo de segurança. Em vez disso, o chroot foi projetado para facilitar e

tornar mais seguros o teste e a instalação de softwares. Um processo ou um usuário com privilégios de root consegue facilmente sair de um ambiente chroot e danificar o sistema operacional sob ele. Porém, esse risco pode ser bastante reduzido executando-se todos os softwares dentro de um chroot como usuário comum e retirando quaisquer binários *setuid* potencialmente inseguros que rodem como root ou com privilégios aumentados.

Criação de chroot

Em sistemas baseados em pacotes RPM e DEB, criar um ambiente chroot é relativamente fácil. O *Debian* já documentou adequadamente o processo de criação de um ambiente chroot [9], então, não preciso repeti-lo.

Para criar um ambiente chroot completo, são necessários vários itens básicos:

- um sistema de arquivos com diretórios básicos, como `/dev/` e `/proc/` (para que programas como o *ps* funcionem);
- quaisquer programas e bibliotecas necessários para executar o software que se deseje testar;
- opcionalmente, uma forma fácil de instalar ou atualizar softwares dentro da chroot, o que é especialmente importante se for desejável usar o chroot como ambiente para compartimentalizar softwares.

O **primeiro passo** é criar as entradas necessárias no sistema de arquivos. Para isso, execute (como root):

```
# mkdir /chroot
# mkdir /chroot/proc
# mkdir /chroot/dev
# mount -t proc proc /chroot/proc
# /sbin/MAKEDEV generic -D /
➥chroot/dev -d /chroot/dev
```

O **segundo passo** é a preparação do chroot para o uso pelo *yum*. Instalar o pacote *release* (*centos-release* ou *redhat-release*) no chroot permitirá que o yum funcione:

```
# rpm -Uvh --nodeps --root=/
➥chroot/centos-release-5-1.0.e15.
➥centos.1.x86|_64.rpm
```

O **terceiro passo** consiste na instalação dentro do chroot. O RPM também instala o software no chroot, mas o yum vai lidar com as dependências e simplificar bastante o processo:

```
# yum --installroot=/chroot/
➥install bash yum vim-minimal
```

Eu recomendo no mínimo uma *shell*, o yum, para instalar softwares, e o editor *vim* para modificar arquivos no chroot.

O **quarto passo** envolve os arquivos de configuração de rede. Se você desejar acessar a rede a partir do chroot, será necessário um arquivo `resolv.conf` e:

```
# mkdir /chroot/etc
# mkdir /chroot/etc/sysconfig
# cp /etc/resolv.conf /chroot/etc/
# cp /etc/sysconfig/network /
➥chroot/etc/sysconfig/
```

Entrando no chroot

Nesse ponto, você conseguirá acessar o chroot com um comando como `chroot /chroot/ bash`, que o colocará no diretório `/chroot/` e executará o *bash* de dentro dele.

Como eu disse antes, o chroot não é um método inerentemente seguro para isolamento de aplicativos. Ao usar um usuário sem privilégios para entrar no ambiente e também ao remover quaisquer binários que rodem com privilégios maiores, pode-se garantir que nada será executado como root a partir do ambiente chroot:

```
# find / -type f -perm +6000
```

Conclusão

Usar sandboxes hoje é mais fácil do que nunca, e seus benefícios jamais foram mais importantes. Isolar aplicativos web mal escritos do sistema operacional subjacente ou permitir que um administrador instale um programa sem afetar o sistema podem economizar tempo e dinheiro. Como em qualquer outro aspecto, prevenção e previsão podem reduzir significativamente a quantidade de trabalho necessária para manter e consertar um sistema a longo prazo, e o sandbox oferece uma ferramenta prática para alcançar isso. ■

Mais informações

[1] Bochs: http://bochs.sourceforge.net/

[2] Xen: http://www.xen.org

[3] User-Mode Linux: http://user-mode-linux.sourceforge.net/

[4] VirtualBox: http://www.virtualbox.org/

[5] KVM: http://kvm.qumranet.com/kvmwiki

[6] OpenVZ: http://openvz.org/

[7] Qemu: http://fabrice.bellard.free.fr/qemu/

[8] VMware Server: http://www.vmware.com/products/server/

[9] Instruções para chroot no Debian: http://www.debian.org/doc/manuals/reference/ch-tips.pt-br.html#s-chroot

Sobre o autor

Kurt Seifried é consultor de segurança da informação especializado em redes e Linux desde 1996. Ele freqüentemente se pergunta como a tecnologia funciona em grande escala mas costuma falhar em pequena escala.

Lançado o ALSA 1.0.17

Após três *release candidates* e centenas de linhas de código alteradas, os desenvolvedores do projeto ALSA finalmente lançaram a versão 1.0.17, que inclui grandes mudanças e vários drivers de som novos ou melhorados. Foi melhorado também o suporte a sistemas de 64 bits. Além disso os desenvolvedores resolveram um problema que ocorria na compilação dos drivers de áudio no kernel 2.6.25.

Agora há, também, suporte a placas de som de alto desempenho baseadas no chip CMI8788 Oxygen. O suporte a chips HDA Intel também foi otimizado, suportando até oito canais. Porém, nem todos os drivers foram migrados para a versão 1.0.17 do subsistema de áudio: os chips X-Fi, da Creative, por exemplo, ainda são uma lacuna a ser preenchida.

Houve ainda mudanças no pacote Alsa-utils, que compreende ferramentas de linha de comando para configuração e verificação do ALSA. Entre outros avanços, o gerador de sinais, o teste dos alto-falantes e a geração do chamado "ruído rosa" foram melhorados. Os utilitários Aplay e Arecord agora são capazes de usar o formato WAV "float".

A nova versão do ALSA pode ser baixada a partir do site oficial (`http://www.alsa-project.org`), mas os fabricantes de distribuições já devem incluí-la em suas próximas versões.

MPX: Compiz com mais apontadores

Aumentar janelas usando dois dedos em tela sensível ao toque enquanto se ajusta o volume ou então desenhar uma imagem com os dez dedos: isso será possível no futuro, garante o desenvolvedor Peter Hutterer, com o suporte a múltiplos apontadores no X (MPX).

Hutterer disse em seu blog que o código do Compiz já permite o uso de mais de um apontador no desktop 3D. Para conseguir isso, Hutterer reescreveu partes do código do gerenciador de janelas e do Compiz. Ele substituiu algumas funções de forma que os movimentos do mouse não gerassem mais *core events* do Compiz, mas X *Input Events*. O desenvolvedor afirma que, por falta de tempo, não conseguirá continuar o desenvolvimento do código, mas ficaria feliz em ajudar quem se interessar.

Novo comando na Gnome Foundation

A Gnome Foundation escolheu, neste último mês, Stormy Peters para o cargo de diretora executiva da fundação. Stormy será, a partir de agora, a responsável por promover o uso do ambiente Gnome e das tecnologias sobre as quais ele se baseia.

Antes de chegar a esse posto, Peters desempenhou papéis importantes na comunidade de Código Aberto, em especial como *Community Manager* na OpenLogic. Anteriormente, Peters trabalhou também como estrategista de código aberto na HP, uma importante patrocinadora do Gnome desde o ano de 2000.

Workshop na Grande São Paulo

Foi um sucesso o IV Workshop Software Livre, em Mauá, na Grande São Paulo. Realizado pela Solunix, empresa especializada em soluções em Software Livre, o evento ocorreu no dia 26 de junho no Teatro Municipal de Mauá e contou com a presença de representantes de inúmeras empresas em diversos segmentos, tais como contabilidade, prefeituras e câmaras municipais, metalúrgicas, transportes, logística, hospitais, tecnologia da informação e outros, além, é claro, de alunos universitários de várias instituições de ensino da região e autoridades públicas.

Durante o evento, cujo tema foi "Tecnologia de ponta e economia de recursos para sua empresa", foram apresentados diversos estudos de caso, finalizados com um fórum de discussões com intensa troca de informações e solução de dúvidas.

Kolab 2 móvel

O *Kolab* 2, pacote de colaboração de código aberto, em breve será capaz de lidar com o protocolo *SyncML* e, graças a isso, poderá sincronizar os dados armazenados no servidor com telefones celulares e PDAs. Em uma primeira versão, isso somente será possível para os dados armazenados no catálogo de endereços e entradas na agenda. A sincronização de dados relativos a tarefas e notas será disponibilizada apenas em versões posteriores. A adição desses recursos está planejada para a versão 2.2.1 do sistema (atualmente na versão 2.2.0).

A P@ardus, integradora de sistemas especialista em soluções groupware alemã com sede em Hamburgo, em parceria com a Univention, empresa alemã especialista em soluções de código aberto com sede em Bremen, integrou ao Kolab o suporte ao protocolo SyncML com base no *framework* desenvolvido pelo projeto *Horde*. A extensão assim desenvolvida será incorporada à solução de colaboração da Univention — o *Univention Groupware Server*, baseado no Kolab —, que disponibilizou uma versão de testes do sistema para download na página da empresa na Internet.

São Paulo sedia IV SlackShow

Pelo quarto ano consecutivo, será realizado em São Paulo, entre os dias 22 e 23 de agosto, o IV SlackShow, um evento voltado para técnicos, com palestras técnicas ministradas por técnicos, . Neste ano, o evento conta com a presença de palestrantes internacionais como Alan Hicks (autor do *The Book*, manual do Slackware), Eric Hameleers (responsável por boa parte da configuração de rede, das novidades do instalador e outras coisas) e Robby Workman (HAL, pacotes do KDE4 etc). Todos eles participam ativamente do desenvolvimento da distribuição e são *comitters* do Slackbuilds.org.

Intel recusa adoção do Vista

Paul McDougall, da americana **Information Week**, noticiou que, apesar de os computadores com Windows Vista freqüentemente virem acompanhados do selo "Intel Inside", a recíproca não é verdadeira.

Segundo uma fonte anônima dentro da Intel, a maior fabricante mundial de processadores que rodam o Microsoft Windows afirmou que não fará a atualização do Windows XP para o Vista nas máquinas utilizadas internamente por seus 80 mil funcionários. Em vez disso, o Windows XP será mantido até a comercialização do Windows 7, em 2010, pois, segundo a fonte anônima, não há "motivos convincentes" para a atualização.

Como Intel e Microsoft têm relações estreitas, essa decisão da fabricante de hardware pode ser embaraçosa para a empresa de Redmond. Um porta-voz da Intel informou apenas que a empresa está testando o Vista "em certos departamentos".

Apesar de estar no mercado há 18 meses e já contar com service packs, o Vista não tem apresentado ampla adoção pelo mercado corporativo – os motivos alegados pelas empresas vão desde o custo da licença até as exigências de hardware do sistema, incluindo a incompatibilidade com diversos softwares legados.

A empresa de Steve Ballmer parece reconhecer que seu mais novo sistema operacional está aquém do esperado. Seu vice-presidente sênior Bill Veghte afirmou, em carta enviada aos clientes da companhia, que o Vista sofre de vários problemas, decorrentes principalmente das "mudanças na arquitetura para aumentar a segurança e a confiabilidade" – as quais serão mantidas no Windows 7 justamente para não frustrar quem quer que tenha adquirido aplicativos e hardware compatíveis com o Vista.

Xandros adquire Linspire

Num jogo de xadrez, um dos movimentos mais imprevisíveis é o do cavalo que se joga no centro do tabuleiro: pode ser uma forma simples de controlar uma parte do jogo, ao menos durante certo tempo, mas pode ser também um prosaico "movimento louco".

Da mesma forma, não é possível saber o que está por trás do último movimento da canadense Xandros, dona da distribuição que roda no Eee PC da Asus: a compra da empresa americana Linspire. O negócio inclui a aquisição de produtos como as distribuições *Linspire* e *Freespire*, além da plataforma de instalação de desktops *CNR* (*Click 'N Run*). Segundo Kevin Carmony, antigo CEO da Linspire, a venda não foi recebida com entusiasmo pelos acionistas, tendo sido aprovada por meio de manobras de Michael Robertson, fundador da empresa e atual CEO. Em comunicado oficial à imprensa, Robertson afirmou que "os negócios com Linux estão atravessando uma consolidação saudável e necessária, que dará às empresas resultantes um maior tamanho e mais ativos para desenvolver maiores iniciativas para que o Linux alcance mais pessoas".

Já de acordo com Carmony, o resultado nada será além da "drenagem de recursos e dinheiro" e da "humilhação pública" da Linspire. Em relação à aquisição, valores oficiais e sólidos não foram revelados, limitando-se as empresas a falar em um aporte de valores, que ocorreria no decurso de vários anos.

Para Sun, SL/CA dá mais lucro

Segundo Simon Phipps, Chief Open Source Officer da Sun Microsystems, a abertura do código do sistema operacional *Solaris* valeu a pena. Em entrevista ao site alemão *Computerwoche*, Phipps afirmou que a venda de subscrições do *OpenSolaris* contribuiu com uma receita maior do que a venda de licenças jamais foi capaz de produzir – mas o executivo não mencionou valores. Enquanto o modelo tradicional de venda de licenças visa a transformar potenciais usuários em compradores, a mudança para o Código Aberto apresenta o desafio de transformar usuários em clientes e, por isso, levanta tantas dúvidas entre os executivos em geral.

Linux domina supercomputadores

Segundo noticiou o site *Linux Today*, a mais recente lista dos maiores supercomputadores do planeta, compilada semestralmente pela organização Top500, mostra o Linux presente em 427 (85,4%) dessas supermáquinas.

O sistema mais veloz, criado pelo Los Alamos National Laboratory, do departamento americano de energia, e chamado de "Roadrunner", alcançou a marca de 1,026 petaflops (mais de um quadrilhão de operações de ponto flutuante por segundo), tornando-se a primeira máquina a ultrapassar a barreira do petaflops. A notícia diz ainda que a máquina é, ao mesmo tempo, um dos sistemas mais eficientes da lista, em termos de energia.

Operating system Family

In addition to the table below, you can vie
page. A direct link to the charts is also ava

Operating system Family	Count	Share %	Rr (G
Linux	427	85.40 %	84
Windows	5	1.00 %	15
Unix	25	5.00 %	61
BSD Based	1	0.20 %	35
Mixed	40	8.00 %	23
Mac OS	2	0.40 %	28
Totals	**500**	**100%**	**11**

Virtualização diferente na Red Hat

Três iniciativas estratégicas em virtualização foram as estrelas durante a abertura do evento Red Hat Summit, em Boston, EUA. Segundo a empresa, as novas iniciativas representam mais opções em ferramentas de virtualização de código aberto e novos esforços para a segurança em ambientes virtualizados.

A novidade da Red Hat que provavelmente mais chama a atenção é o *hypervisor* embutido no kernel, batizado de *oVirt*. Trata-se de um hypervisor simples, rápido e incluído no kernel, que permite rodar máquinas virtuais com *Red Hat Enterprise Linux* e Microsoft Windows sobre o Linux. O que torna o oVirt diferente de outras soluções de virtualização é que ele possibilitará o transporte de máquinas virtuais personalizadas entre desktops e servidores dentro de um dispositivo USB.

ABNT contesta ISO

A ABNT, Associação Brasileira de Normas Técnicas, acaba de solicitar à ISO o cancelamento de todo o processo de elaboração da ISO/IEC DIS 29500 e seu retorno como um novo item de trabalho (NWIP) seguindo o processo normal de elaboração (sem *Fast-Track*) no âmbito do ISO/IEC/JTC1/SC34. Isso significa que o órgão brasileiro está solicitando o cancelamento da aprovação do formato de documentos digitais OOXML da Microsoft como padrão ISO/IEC.

Essa é considerada uma medida histórica. Após a aprovação da OOXML pela ISO, quatro países (África do Sul, Brasil, Índia e Venezuela) entraram com um pedido formal de apelação contra a aprovação da OOXML como padrão oficial. A apelação formal já ocasionou prejuízos consideráveis para a Microsoft, pois ocasionou o congelamento de todo o processo de homologação do novo padrão, impedindo sua conclusão.

A entrada da ABNT nessa briga pode virar definitivamente a balança em favor de todas as pessoas, instituições e entidades que foram contra esse processo de homologação. Muitos, inclusive, foram os questionamentos feitos à ISO durante todo o processo de avaliação da OOXML, apontando vários pontos considerados insatisfatórios e que, mesmo assim, permaneceram sumariamente ignorados pelo órgão internacional. Segundo o regulamento, apenas um único ponto negativo não solucionado é preciso para tornar inelegível um padrão. Se o pedido da ABNT for deferido, teremos então o retorno do padrão OOXML ao status de reavaliação perante a ISO. Com isso, todos os envolvidos devem esperar uma avaliação mais criteriosa e imparcial por parte da ISO na reconsideração do OOXML.

- **Multiempresa**
- **Multiplataforma**
- **Interface amigável**
- **Compatível com a legislação fiscal e tributária brasileira**
- **Independência do desenvolvedor do software**

- Gerenciamento de cadeia e fornecedores
- Análise de performance
- Contabilidade
- Financeiro
- Produção
- Logística
- Vendas
- MRP
- CRM

Flexibilidade e Confiabilidade

Solução de gestão integrada ADempiere:

a tecnologia utilizada por grandes empresas, agora acessível ao seu negócio, pelo melhor custo.

www.kenos.com.br • contato@kenos.com.br • (11) 4082-1305

Kenos
Sistemas de Gestão Integrada

Entrevista com Mikko Hypönnen, diretor de pesquisa da F-Secure

Problemas à vista

A indústria da segurança de dados está numa corrida constante contra os criadores de malware. Mikko Hypönnen oferece uma visão de dentro desse mercado.

por Pablo Hess

O mercado de soluções de segurança de dados é fundamental para a TI atual. Não faltam sistemas operacionais proprietários altamente vulneráveis a vírus, e os riscos de uma exposição dos dados das empresas por pragas virtuais são bastante reais.

Na área de emails indesejados, o quadro é ainda pior, levando à redução da velocidade geral de acesso à Web e ao desperdício de espaço de armazenamento.

Mikko Hyppönen é o diretor de pesquisa da F-Secure e acumula feitos marcantes no mercado de segurança, como a liderança da equipe que desativou a rede internacional usada pelo *worm Sobig.F* e por ter sido o primeiro a alertar o mundo sobre a disseminaçao do vírus *Sasser*, em 2004.

Após visitar o Brasil, Hyppönen concedeu à **Linux Magazine** uma entrevista a respeito do mercado de segurança da informação no Brasil e no mundo.

Linux Magazine» ***É comum ouvirmos que "um sistema só está seguro quando está desligado". Porém, muitos acham isso um exagero. Qual a sua opinião sobre essa questão?***

Mykko Hyppönnen» Não acho que seja um exagero. Sistemas desconectados da rede realmente não podem ser invadidos a distância. É claro que isso é altamente inconveniente. Porém, no caso de sistemas realmente críticos (infra-estrutura crítica, por exemplo), recomendo o uso de sistemas desconectados de redes públicas. Embora isso seja altamente inconveniente e doloroso, além de caro, é a opção segura.

Figura 1 Mikko Hypönnen, diretor de pesquisa da F-Secure.

LM» ***Muitas pessoas ainda acreditam que os fabricantes de antivírus são os verdadeiros criadores dessas ameaças. Você ainda ouve muito isso?***

MH» Se isso é uma piada, eu não acho engraçada. É isso que recebemos por tentarmos ajudar as pessoas. Eu costumava ouvir essa pergunta regularmente há muitos anos.

Na época, os vírus ainda eram escritos por hobby e diversão, e as pessoas freqüentemente eram incapazes de entender por que alguém criaria um vírus. Logo, sugeriam que seriam as próprias empresas fabricantes de antivírus as culpadas. Porém, não conheço um caso sequer em que uma empresa tenha escrito um vírus.

E não costumo mais ouvir essa pergunta. Hoje em dia, quase todos os vírus são criados por criminosos para ganharem dinheiro. Então, as pessoas vêem o motivo, entendem por que vírus estão sendo criados e não precisam mais suspeitar e culpar a indústria dos antivírus por sua criação.

LM» ***A quem ou o que você credita a existência de tantas ameaças de segurança atualmente?***

MH» É facílimo ganhar muito dinheiro com ameaças cibernéticas – milhões. Mesmo assim, quase nenhum cibercriminoso é capturado. Então, acho bastante óbvio entender por que essas ameaças existem.

LM» ***Com relação a sistemas operacionais, é possível afirmar que um sistema operacional é mais seguro que outro?***

MH» Há três motivos pelos quais existem menos vírus para Linux do que para Windows:

- o Linux tem menos usuários, principalmente no segmento de estações de trabalho. Portanto, os criminosos podem ganhar mais dinheiro infectando usuários de sistema Windows;
- os usuários de Linux não têm acesso de root ininterruptamente;
- motivos sociais: programadores Linux gostam desse sistema e também dos demais usuários do sistema, mas ninguém gosta do Windows.

LM» ***Dizem que o Brasil é um dos líderes mundiais no envio de spam e em redes tipo botnets. Por que um país é mais sujeito que outros a falhas de segurança?***
MH» O Brasil sempre teve um submundo hacker bastante ativo. Os motivos por trás desse desenvolvimento não são claros. A legislação e atividade locais da polícia brasileira provavelmente também têm importância nessa questão. Em geral, ambientes com muitos autodidatas em computação, fácil acesso à Internet para a população, mas sem emprego para todos, têm sido problemáticos nesse aspecto.

LM» ***A F-Secure oferece suporte a sistemas Linux? Qual das soluções é mais freqüentemente usada no sistema aberto?***
MH» Como a empresa é finlandesa, é claro que sempre oferecemos suporte ao Linux. A maioria dos nossos clientes Linux utilizam nossos produtos em servidores e gateways Linux para bloquear vírus para estações Windows.

LM» ***Quais as principais diferenças entre os produtos da F-Secure para os diferentes sistemas operacionais?***
MH» Nosso mecanismo de busca de vírus é o mesmo tanto para Windows quanto para Linux. Então, nossos softwares para um sistema também conseguem bloquear vírus do outro. É claro que há apenas poucas dezenas de vírus para Linux, comparados a meio milhão de ameaças para Windows.

LM» ***Especificamente no campo de antivírus, a alternativa mais popular de código aberto, o ClamAV, é competente na sua opinião?***
MH» O ClamAV é muito bom. Porém, como produto de hobby, ele não consegue competir com produtos profissionais nas taxas de detecção.

Um recente teste independente realizado pelo site av-test.org indicou que as soluções comerciais, como as das empresas F-Secure, Kaspersky e Symantec, alcançaram taxas superiores a 95% de detecção de vírus, enquanto o ClamAV detectou apenas pouco mais de 84% dos vírus.

LM» ***Como você vê o futuro da segurança em TI? Processadores mais poderosos e tendências como a computação quântica devem alterar o panorama dessa área?***
MH» Eu adoraria poder dizer que a situação está melhorando e que vamos vencer essa batalha. Porém, não acredito nisso. Acho que estamos vendo apenas o começo desses problemas. Se não implementarmos ações de execução internacional da lei e demorarmos em colocar esses criminosos atrás das grades, teremos grandes problemas. ■

Entrevista com Daniel Cid, desenvolvedor do OSSEC

Hobby seguro

Daniel Cid criou o OSSEC como hobby e agora é pago para continuar seu desenvolvimento em tempo integral. Confira as suas dicas de sucesso para projetos de código aberto.

por Pablo Hess

No último mês de junho, um projeto brasileiro de código aberto teve seu valor reconhecido – e adquirido – por uma empresa de segurança estrangeira. O sistema IDS e IPS OSSEC foi integralmente adquirido pela empresa Third Brigade, especializada em segurança da informação.

Daniel, criador e mantenedor do software e, agora, *Research Principal* do OSSEC na empresa canadense, trabalha integralmente no projeto que começou como hobby.

Confira a entrevista que o desenvolvedor concedeu com exclusividade à **Linux Magazine**.

> *Com o OSSEC, decidi dar o exemplo e ser bem educado e atencioso com todos.*

Linux Magazine» ***Qual foi a sua motivação para criar o OSSEC?***

Daniel Cid» O OSSEC começou em partes e bem devagar. Eu era administrator de sistemas de uma grande empresa com vários servidores Linux, AIX e Solaris. Na época, precisávamos realizar uma checagem periódica da integridade desses sistemas, ou seja, verificar se alguns arquivos de configuração ou binários dos sistemas tinham sido alterados.

As únicas soluções existentes na época (Tripwire e AIDE) não se adaptavam bem à nossa rede, que era muito grande, e não possuíam suporte centralizado, o que significava que teríamos que instalar esses softwares separadamente em cada máquina, além de fazer sua manutenção individualmente.

Por essa razão, iniciei o desenvolvimento do Syscheck no final de 2002. A finalidade desse programa era verificar a integridade de vários sistemas de modo centralizado. Todas as configurações, além do banco de dados e dos alertas, localizavam-se num servidor central, sendo fácil de manter e instalar em uma rede de grande extensão. Foi um trabalho bem interessante que deu muito certo na nossa empresa.

Alguns meses depois, lancei a primeira versão do Syscheck publicamente e com código aberto sob a GPLv2.

Depois disso, com o sucesso interno do Syscheck, quando surgiu a necessidade de centralizar os logs de todas essas máquinas, decidi colocar a mão na massa e criar o OS-HIDS, um programa de análise de logs, seguindo o mesmo modelo centralizado do Syscheck. Após algum tempo, fiz o mesmo com o Rootcheck, um programa de procura de Rootkits.

Todos esses projetos eram separados, mas no final de 2004 decidi juntá-los para criar o OSSEC HIDS, que combinaria análise de logs, checagem de integridade de arquivos e busca de rootkits em um único software, seguindo o mesmo modelo centralizado com um gerenciador e vários agentes. A primeira versão do OSSEC foi disponibilizada em meados de 2005 e, de lá pra cá, já tivemos mais de 15 versões diferentes.

LM» ***Até o momento da aquisição do software pela Third Brigade, como foi planejado o seu modelo de desenvolvimento?***

DC» O OSSEC sempre teve um modelo de desenvolvimento bem aberto e uma comunidade muito amigável. Nunca gostei de projetos cujos participantes tinham atitudes ruins nas listas e nos fóruns. Então, com o OSSEC, decidi dar o exemplo e ser bem educado e atencioso com todos, mesmo com aqueles que faziam perguntas simples que já presentes nas FAQ.

Isso permitiu uma fácil integração entre usuários novos ou sem muita experiência em segurança e nosso projeto. Muito deles, após algum tempo, passaram a contribuir de volta também. Nossa comunidade agora é bastante ativa, com aproximadamente 10 mil downloads do OSSEC por mês e mil pessoas nas nossas listas de email, além de muito amigável, exatamente como eu desejava desde o começo.

Além disso, sempre fui aberto a patches e sugestões, o que nos levou a receber muitas contribuições. A equipe ativa de desenvolvimento nunca foi muito grande, jamais ultrapassando três pessoas; porém, o número de patches, de pessoas

testando as versões beta e de tradutores sempre foi muito grande – hoje temos o OSSEC em mais de 12 línguas, o que é excelente para um projeto de segurança.

LM» ***Como foi o processo de aquisição do software? Já foi completado?***
DC» Eu sempre trabalhei no OSSEC como um hobby, durante as noites, os fins de semanas e os feriados. Eu o utilizava no meu trabalho como administrador de sistemas e engenheiro de redes, mas o desenvolvimento era feito à noite mesmo.

No fim de 2007, a Third Brigade me contactou com o interesse de fazer uma parceria com o projeto. Depois de várias conversas, me perguntaram sobre a possibilidade de virarem patrocinadores e bancarem meu trabalho em tempo integral. Além disso, também se ofereceram para comprar os direitos do projeto e virarem os mantenedores oficiais.

Depois de seis meses de discussões, nas quais minha maior preocupação era garantir que o projeto permaneceria com o código aberto, fechamos contrato em junho de 2008.

LM» ***Que atrativos a Third Brigade viu no OSSEC para adquiri-lo?***
DC» Vejo que a característica do OSSEC que mais chamou a atenção da Third Brigade foi sua capacidade de resolver problemas de várias empresas de um modo simples e elegante.

LM» ***O que mudará com a aquisição do projeto?***
DC» O projeto continuará com o código aberto sob a GPLv3 e voltado para a comunidade. Meu trabalho agora é continuar desenvolvendo-o e mantendo a comunidade unida e ativa. Já a Third Brigade vai oferecer suporte comercial e treinamentos sobre o OSSEC. Também estamos discutindo a criação de uma interface gráfica de gerenciamento, assim como a venda do produto pré-configurado em *appliances*, obviamente mantendo o código sob a GPLv3.

Em relação à colaboração com distribuidores Linux, nada vai mudar. Nosso interesse é que o projeto cresça cada vez mais e que seja incluído no maior número de distribuições possível.

LM» ***Na visão da Third Brigade, quais as vantagens do fato do OSSEC ter o código aberto? Eles vêem também alguma desvantagem?***
DC» Existem várias vantagens. Eles estão impressionados com a velocidade de atualização do projeto e com a quantidade de contribuições recebidas. Além disso, seria impossível ele ser suportado nos mais variados sistemas (Linux, FreeBSD, AIX, HP-UX, Windows, Mac OS etc.) e em tantas línguas se não fosse por esse modelo aberto que permite que qualquer pessoa colabore.

Em relação às desvantagens, não fui informado de nenhuma.

LM» ***Que sugestões você daria para quem está iniciando agora um projeto de Código Aberto na área de segurança? E em outras áreas?***
DC» Minha sugestão é que você interaja com a comunidade, se está começando um projeto agora, responda os emails e seja educado. Poste seu projeto em vários sites (Freshmeat, Sourceforge etc.) e deixe as pessoas participarem. Existem vários projetos pouco utilizados simplesmente por falta de divulgação.

Em segundo lugar, facilite a instalação do software. Isso é muito importante, pois poucas pessoas têm tempo e paciência de gastar várias horas apenas para testar um programa novo. Crie um instalador e facilite ao máximo a vida do usuário, pois isso vale a pena.

Para finalizar, faça algo de que você goste, sem pensar, a princípio, no retorno financeiro imediato. Leve o projeto como um hobby, divirta-se, mas trabalhe duro. ■

Edson Pires – www.sxc.hu

Linux Park 2008 no Rio de Janeiro

Linux Park 2008: A praia dos negócios

Continuando a edição 2008 dos seminários Linux Park, a cidade do Rio de Janeiro foi palco para as palestras sobre o ecossistema de negócios em Software Livre no Brasil.

por Pablo Hess

O ecossistema de negócios em Software Livre no Brasil está ganhando um novo impulso. Continuando sua trajetória itinerante pelo país, os seminários Linux Park, realizados pela editora Linux New Media e promovidos pela **Linux Magazine**, repetiram o sucesso do ano passado na cidade do Rio de Janeiro.

Na capital fluminense, o público (**figura 1**) contou com apresentações de empresas de diversas esferas, que informaram como fazem uso do Software Livre para ampliar suas oportunidades de negócios, sempre esclarecendo sua relação com o tema central dos seminários Linux Park deste ano, "O Ecossistema de Negócios em Software Livre no Brasil".

Abertura

Em seu tradicional *keynote* de abertura, Rafael Peregrino da Silva, Diretor Executivo da Linux New Media do Brasil, reafirmou a importância do evento no cenário nacional do Software Livre e de Código Aberto (SL/CA). Rafael exibiu também os resultados de uma pesquisa norte-americana realizada em 2005 com mais de 500 executivos de TI europeus e americanos pela empresa Chadwick Martin Bailey, apontando que os principais critérios para adoção de produtos e serviços Linux eram, na opinião dos executivos, em ordem decrescente, confiabilidade, segurança, desempenho e, apenas em quarto lugar, a redução de custos.

Peregrino reconheceu que a situação no Brasil é diferente, pois o aspecto dos custos tem uma importância maior no país.

Pesquisa nacional

Abordando justamente o panorama brasileiro do mercado do Software Livre, Álvaro Leal (**figura 2**), analista de mercado sênior da ITData, apresentou os resultados da pesquisa nacional realizada em parceria com o Instituto Sem Fronteiras[1] em 2007. Após consultar mais de 1.000 gerentes de TI de empresas brasileiras dos mais variados setores, tamanhos e receitas, a pesquisa chegou a algumas conclusões bastante impressionantes – em sua maioria, positivas para as empresas que investem ou usam SL/CA (um resumo dos resultados foi publicado na Linux Magazine Online em [2], [3], [4], [5] e [6]).

Álvaro apresentou suas motivações para realizar esse trabalhoso estudo e revelou também os critérios usados ao longo da empreitada, explicando por que o assunto interessa aos CIOs, maioria entre os participantes do evento no Rio.

O objetivo principal da pesquisa, nas palavras do analista, era "entender a adoção e a tendência de evolução dos investimentos em Software Livre pelas empresas brasileiras".

A distribuição das empresas pesquisadas em relação ao número de funcionários e ao segmento de atuação foi bastante homogêneo, diferentemente das regiões geográficas, que mostraram uma maior concentração no Sudeste (59% das empresas) e Sul (20%) – "para criar um pequeno modelo do que seria o universo de empresas do Brasil", segundo Álvaro, "e o Sudeste é realmente muito significativo no país".

Figura 1 Público altamente qualificado no Rio de Janeiro.

Figura 2 A pesquisa de Álvaro Leal, da ITData, revelou diversas surpresas do mercado nacional de SL/CA.

O primeiro resultado surpreendente apresentado pelo analista foi a presença do SL/CA em 59% das empresas do país, valor bem superior ao que os analistas em geral suporiam. Nos segmentos verticais, novamente surpresas: usa-se muito SL/CA para educação e comércio, contrariando as previsões conservadoras do público em geral. Os segmentos com barreiras à adoção dessa tecnologia, no entanto, seguem o que se previa: nos setores financeiro, de serviços e de agronegócio. Apesar disso, o primeiro demonstrou adoção de SL/CA em 49% das empresas pesquisadas, um cenário "impensável há cinco anos", de acordo com Álvaro. No setor de serviços, a adoção também cresceu, quebrando a barreira dos 50%; o analista revelou acreditar que esse valor ainda vá crescer bastante (de 9 a 11%) nos próximos 12 meses. No agronegócio, o problema é a maturidade do mercado, que sofre uma adoção tardia da tecnologia da informação e que, portanto, está focado, atualmente, em questões que não dizem respeito exatamente ao software.

O que mais marcou a pesquisa foi também o que deu "mais prazer para provarmos", como disse Álvaro. Trata-se da correlação entre o número de funcionários das empresas e a adoção de SL/CA, mostrando que nas empresas com mais de 1.000 funcionários usa-se mais SL/CA (73%) do que nas com menos de 99 (31%): "exatamente o oposto do que vem sendo divulgado na mídia", concluiu o analista.

TV digital

Luiz Fernando Gomes Sores (**figura 3**), representante da comunidade científica no Fórum de TV Digital brasileira, palestrou sobre a importância do Software Livre no *middleware Ginga*, desenvolvido por diversas entidades nacionais com a finalidade de equipar os decodificadores (os chamados *set-top boxes*) do sinal brasileiro de TV digital.

Luiz Fernando expôs o que se espera de um middleware nesse caso e mostrou toda a arquitetura interna da criação brasileira, informando também as possibilidades de expansão com linguagens de programação externas, como *Lua* e *Java*, entre outras, por meio da *NCL* (*Nested Context Language*).

Lojas Marabraz

Clóvis Alberto da Silva (**figura 4**), em seguida, falou a respeito da reestruturação da área de TI nas lojas Marabraz, com ênfase na implantação da tecnologia de virtualização. Clóvis descreveu as vantagens obtidas com a consolidação dos desktops como fruto do nível de maturidade da solução atual, toda baseada em SL/CA.

A adoção do SL/CA, na realidade, não foi uma novidade para a Marabraz, que já utilizava a tecnologia aberta em suas lojas há alguns anos,

Figura 3 O *middleware Ginga* foi desenvolvido como SL/CA desde o princípio, como mostrou Luiz Fernando.

Figura 4 Clóvis Alberto da Silva, das Lojas Marabraz, falou sobre virtualização e SL/CA.

como disse Clóvis. Porém, seu uso na fábrica, em conjunto com a tecnologia de virtualização, "ajudou a empresa a alcançar seus objetivos de negócios", afirmou o palestrante.

Eltek Valere

Após o almoço, Fabio Trambaioli, CFO da Eltek Valere apresentou sua palestra sobre o uso do sistema ERP e CRM de código aberto *ADempiere* pela empresa de energia. Presente em mais de 25 países e com 2 mil funcionários, a Eltek desenvolve e comercializa sistemas de energia para aplicação em telecomunicações e indústrias.

Fabio mostrou a dificuldade enfrentada pela filial brasileira, estabelecida em 2004, para administrar as finanças da empresa, emitir notas, faturar etc. Após a troca da solução ERP proprietária original pelo *Compiere*, que posterioremente deu origem ao ADempiere, o CFO afirmou que a empresa finalmente encontrou a ferramenta para suprir suas necessidades na área de gestão de recursos.

Fabio esclareceu ainda ter conhecimento das vantagens técnicas do SL/CA, enfatizando o uso conjunto do ADempiere com o sistema de banco de dados, também de código aberto, *PostgreSQL* e toda a flexibilidade que essa tecnologia oferece.

Globo.com

Jacques Varaschim (**figura 5**), da Globo.com, discorreu sobre o intenso uso de SL/CA no portal, um dos líderes de audiência na Internet brasileira. No datacenter com aproximadamente 1.500 servidores, Jacques afirma que "entre 70 e 80% da infra-estrutura roda sobre Código Aberto", servindo não apenas o portal, mas também todos os outros componentes das organizações Globo – como jornais, emissoras de TV etc.

Segundo o palestrante, a infra-estrutura de TI da empresa enfrenta um "desafio permanente de software e inteligência". Porém, há outros desafios, como a alta disponibilidade necessária para atender uma demanda que varia entre 840 Mbps, "quando o movimento é baixo", e 8,4 Gbps, nos picos, e o SL/CA é uma peça-chave para alcançar todos esses objetivos.

Figura 5 O SL/CA é uma peça-chave no sucesso operacional da Globo.com, como mostrou Jacques Varaschim.

Governança

Finalizando o evento, Eduardo Moura, Diretor de Serviços Profissionais da brasileira Qualityware, abordou a governança corporativa e sua relação com o modelo de desenvolvimento do Código Aberto. Eduardo demonstrou ter domínio do assunto, introduzindo conceitos de transparência na gestão da mesma forma como ocorre com projetos de Software Livre.

Eduardo concluiu sua apresentação sugerindo algumas formas de ação para empresas que desenvolvem SL/CA, tanto no aspecto da gestão quanto na produção e disponibilização de código.

Fechamento

Como de costume, o evento terminou com o sorteio de um Asus Eee PC entre os espectadores, seguido de um agradável show musical durante a confraternização do público e dos palestrantes. ■

Mais informações

[1] Instituto Sem Fronteiras: http://www.isf.org.br

[2] Tendências do SL no Brasil, parte 1: http://www.linuxmagazine.com.br/noticia/1525

[3] Tendências do SL no Brasil, parte 2: http://www.linuxmagazine.com.br/noticia/1528

[4] Tendências do SL no Brasil, parte 3: http://www.linuxmagazine.com.br/noticia/1531

[5] Tendências do SL no Brasil, parte 4: http://www.linuxmagazine.com.br/noticia/1538

[6] Tendências do SL no Brasil, parte 5: http://www.linuxmagazine.com.br/noticia/1547

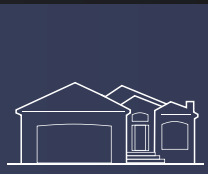
futurecom
SÃO PAULO • ANO 10

27 a 30 de outubro, 2008 • Transamerica Expo Center • **São Paulo**

Futurecom, o mais Qualificado evento de Telecom e TI da América Latina!

foto : Carlos Alkmin

Business Trade Show com aproximadamente **230 empresas,** demonstrando Serviços, Aplicações, Soluções, Sistemas e Tecnologia. A exposição abrangerá 3 pavilhões do Centro de Convenções Transamerica, com aproximadamente **20.000m² de área,** reunindo participantes de **mais de 35 países.**



mais de

10 Sessões Premium com presenças confirmadas de Presidentes de Operadoras.

85 Sessões de Marketing e Business visando o Desenvolvimento de Negócios e Relacionamento, no tradicional modelo de Palestras e Painéis Político-Estratégicos do Futurecom.

60 Sessões Técnicas abordando o mais moderno estado-da-arte em Tecnologia.

Faça já sua inscrição a preços promocionais!
www.futurecom.com.br

futurecom Organização e Promoção: Provisuale
(41) 3314-3200 • www.provisuale.com.br

Cezar Taurion

O livro "O Efeito Médici" sugere por que o Código Aberto altera toda a indústria do software.

por Cezar Taurion

Acabei de ler um livro excelente chamado "O Efeito Médici", de Frans Johansson. O livro já está traduzido para o português, mas pode-se fazer o download gratuito da versão em inglês em [1].

O livro reforça a idéia de que quando chegamos a uma interseção de domínios de conhecimento, disciplinas ou culturas, podemos combinar conceitos existentes em um grande número de inovações. Ele cita exemplos bem interessantes e curiosos.

Para Johansson, o surgimento de interseções se deve a três fatores.

O primeiro é a crescente movimentação de pessoas entre países: ele cita uma frase de Peter Drucker que diz que "as migrações em massa no século XIX ou eram para espaços vazios não habitados, como EUA, Canadá, Austrália e Brasil, ou eram do interior para as cidades dentro de um mesmo país. Em contraste, a imigração no século XXI é de estrangeiros (em nacionalidade, lingua e religião) que se mudam para países habitados".

O segundo fator seria a convergência das ciências. O autor cita uma frase de Alan Leshner, diretor da American Association for the Advancement of Science, que diz "a ciência disciplinar morreu. Acabou. A maioria dos grandes avanços envolve múltiplas disciplinas, sendo cada vez mais raro ver trabalhos científicos de um único autor. E, freqüentemente, os múltiplos autores são de disciplinas diferentes".

O terceiro e último fator, segundo Johansson, é o salto da computação.

O livro também defende a idéia de que criar uma cultura de inovação dá muito trabalho. Criatividade não é inovação, pois não basta ter uma idéia: ela precisa ser valiosa para uma sociedade e também ser realizada. Além disso, aceitar a diferença não é o mesmo que difundi-la e estimulá-la. Por exemplo, somente colocar áreas diferentes e repertórios de vida distintos na mesma sala não fará uma empresa inovar. É preciso estimular e ouvir, e muito.

Empresas e pessoas falam constantemente de inovação no sentido de revolução e quebra de paradigmas. Mas no dia-a-dia acabam aplicando a forma mais simples dela, a direcional, que, além de não ser nada revolucionária, é efêmera e envolve refinamentos e ajustes em processos e produtos, sem contar que isso os concorrrentes também fazem.

E o que isto tem a ver com Open Source e Linux? O autor cita o caso do Linux como um exemplo de como fazer as idéias intersecionais acontecerem. Linus Torvalds não pretendia, em princípio, desafiar todo o sistema da indústria de software, mas, embora tenha começado de forma não intencional, suas idéias estão transformando essa indústria. O que ele fez? Quebrou a cadeia de valor da indústria de software tradicional, envolvendo a comunidade e o modelo colaborativo no processo de desenvolvimento e usando a Internet como ferramenta de distribuição. Hoje, sem sombra de dúvidas, o Open Source nos permite pensar em novos e inovadores modelos de negócio.

Por exemplo, existe uma rede de pequenas empresas européias (Orixo) que se especializaram em desenvolver soluções de integração e customização de missão crítica baseadas em Apache e tecnologia Java/XML. A rede funciona com cada membro conquistando clientes em seu país de origem e desenvolvendo parcerias estreitas com os outros membros, que tenham experiência complementar, suportando uns aos outros. Essa é uma idéia que poderia ser adotada em países de grande extensão geográfica como o Brasil, onde pequenas empresas regionais, sem capital para se tornarem nacionais, podem se associar em rede para criar uma "empresa virtual" especializada e de abrangência nacional.■

Mais informações

[1] Download de "The Medici Effect": http://www.themedicieffect.com/

Sobre o autor

Cezar Taurion é gerente de novas tecnologias aplicadas da IBM Brasil e editor do primeiro blog da América Latina do Portal de Tecnologia da IBM developerWorks. Seu blog está disponível em http://www-03.ibm.com/developerworks/blogs/page/ctaurion.

Gerenciamento de projetos

Precisa ser preciso

Para evitar que seus projetos excedam os custos e prazos e alcancem a qualidade exigida, é necessário gerenciá-los com precisão.

por Pablo Hess

Projetos atrasados, custos excedidos, prazos não cumpridos, qualidade insatisfatória... Infelizmente, essa é a realidade de muitos projetos desenvolvidos e realizados em nosso país. Tomando como exemplo as obras de interesse público, não é incomum verificarmos viadutos, estradas e outras edificações que ultrapassam em muito os custos e prazos previstos inicialmente.

Esses são sintomas de projetos mal gerenciados, seja na fase do planejamento, na execução ou simplesmente no acompanhamento. O fato é que não existem motivos concretos para situações inexplicáveis em projetos bem gerenciados.

Seguir as regras

Isso não significa, no entanto, que gerentes de projetos precisem pertencer a uma estirpe de trabalhadores com capacidades sobre-humanas de controle, liderança, visão em múltiplas direções e tolerância à privação de sono. O bom gerente de projetos é simplesmente um profissional aplicado que segue da melhor maneira possível as orientações de alguma instituição de padronização do gerenciamento de projetos.

Experiência de trabalho na área do projeto também é sempre uma vantagem – quem jamais desenvolveu software, por exemplo, certamente terá dificuldade em planejar com precisão a divisão das tarefas no desenvolvimento de um novo sistema. Ainda assim, é importante reiterar que simplesmente conhecer as rotinas de uma determinada área não qualifica o profissional para gerenciar projetos nesta.

Formação e ferramentas

O bom gerente de projetos entende, além do fluxo de trabalho de sua área, as inter-relações das atividades pertinentes a cada projeto e de que forma cada uma delas pode influenciar – positiva ou negativamente – o desenrolar do projeto. O bom gerente de projetos sabe que, ao mesmo tempo em que cada projeto é diferente dos demais que já gerenciou, todo projeto possui diversas características em comum.

A formação em gerenciamento de projetos é uma das que vêm recebendo crescente atenção das empresas e profissionais de TI. Para obter uma certificação de gerente de projetos (PMP – Project Management Professional) do Project Management Institute[1], a instituição internacional de mais alto prestígio na área, são necessárias 4.500 horas e 36 meses de atuação nessa posição[2].

Quanto às ferramentas, espera-se que um bom profissional saiba escolher e usar boas ferramentas, e a **Linux Magazine** deste mês se empenha em mostrar justamente essa área do gerenciamento.

No primeiro artigo de capa desta edição, Flávia Jobstraibizer demonstra as características do gerenciamento de projetos aplicado ao desenvolvimento de software. Em seguida, Miguel de Lacy explora as potencialidades do Bonita no gerenciamento de *workflows* e o atraente software de gestão de projetos *ClockingIT* é apresentado por seu bem-humorado autor Erlend Simonsen.

Com essas ferramentas, todas de código aberto, um gerente de projetos é capaz de planejar e acompanhar as diferentes etapas e componentes de seus projetos, com todos os recursos que desejar e sem depender de programas proprietários.

Boa leitura e mãos à obra! ■

Mais informações

[1] PMI: http://www.pmi.org/

[2] Certificação PMP: http://www.pmisp.org.br/cert_pmp.asp

Índice das matérias de capa

Bom projeto, bom gerenciamento...
bons resultados **pág. 34**
Fluxo sincronizado **pág. 40**
Na hora exata **pág. 46**

Qual é a "receita" para os projetos de sucesso?

Bom projeto, bom gerenciamento... bons resultados

Começar um projeto é fácil. Difícil é conduzí-lo, com largas margens de sucesso, para a sua conclusão final. Mais do que formatar um documento bonito ou usar um software completo, no entanto, é preciso prestar atenção às especificações: o que se pode, quer e é preciso fazer?

por Flávia Jobstraibizer

A área de tecnologia da informação está em constante evolução, e as empresas constantemente incorporam novos avanços tecnológicos, seja para ganhar eficiência, seja para reduzir custos em todos os setores de um projeto. Com o avanço da velocidade de consumo da informação, usuários, administradores, coordenadores, desenvolvedores e gerentes da área de TI têm de garantir que as soluções de tecnologia utilizadas realmente sejam úteis para incrementar os níveis de serviços prestados, alcançar a redução de custo e proporcionar o aumento do desempenho planejado.

A organização de um projeto como um todo não pode ser reduzida apenas a um resumido documento de requisitos. É necessário visualizar todo o projeto de forma panorâmica, ter uma visão global – conhecer o *escopo* do projeto. Para estabelecer o escopo de projetos para sistemas de TI (alvo deste artigo), deve-se levar em conta a seguinte abordagem:

- estabelecer fases do projeto e versões, caso seja conveniente – e de acordo com o tipo de produto;
- ter controle sobre restrições de tempo e recursos;
- definir metas atingíveis e coerentes;
- definir prioridades e principais necessidades do cliente, além de analisar riscos.

Também é interessante definir quais serão os principais "entregáveis" do seu projeto, ou seja, itens de suma importância e de primeira necessidade, sem os quais todo o andamento do projeto pode ser comprometido.

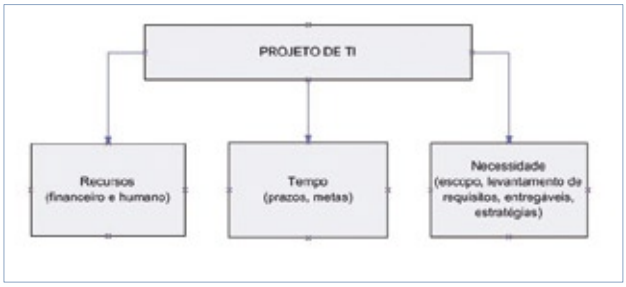


Figura 1 Pense sempre nos tripés do projeto: eles definem o que pode ou não ser feito de verdade...

Dá tempo?

Em se tratando da área de TI e, muito especialmente, dos projetos de TI, é normal haver mudanças de datas. Para o correto gerenciamento do projeto, no entanto, é importante formalizar essas mudanças caso afetem uma ou mais partes do escopo do projeto. Assim, é necessário avaliar quais alterações poderão ser incluídas, quando e como, sem que possam vir a afetar o andamento de todo o projeto.

É importante lembrar que projetos como um todo não são facilmente alteráveis: é necessário controle e planejamento. Sem isso, é comum o que vemos em diversas empresas, de qualquer porte: a falta de planejamento gerando atrasos, falhas na comunicação entre setores e erros na troca de informações importantes. Tudo isso, consequentemente, resulta no engavetamento de todo o projeto.

Estrategista

Os problemas dos projetos de TI são sempre os mesmos: prazo e recursos financeiros curtos, grandes necessidades, urgência em entregáveis, quantidade limitada de recursos humanos, dentre outros. O que falta para contornar tal situação é estratégia: ser estrategista é o principal mérito do gerente de projetos.

É importante lembrar que o tripé de um projeto é sempre: **recursos** (financeiros e humanos), **tempo** e **necessidade**. Além disso, capacitar todos os envolvidos a enxergarem o projeto com essa visão (**figura 1**) é de vital importância para o bom andamento de qualquer cronograma. É claro que seguir alguma metodologia de gerenciamento de projetos como ITIL, PMI ou IPMA, com todas as áreas de conhecimento respectivas, aumenta exponencialmente as chances de sucesso. Ainda que você não as siga ao pé da letra, é possível organizar-se e obter resultados logo na primeira tentativa.

Mas lembre-se: scripts, documentos e bibliotecas são ferramentas, e ferramentas precisam de matéria-prima para serem úteis e construírem algo belo ou útil. Um projeto de grandes proporções administrado por um gerente de projetos que cuida de outros projetos e que conta com uma equipe de duas pessoas trabalhando duas horas por dia, e que, além disso, tem prazo de finalização que já começou "no vermelho" do Gráfico de Gannt, tem tantas chances de obter sucesso seguindo as normas do IPMA quanto apostando no jogo de palitos.

Ajudantes bem-vindos

Para auxiliá-lo na árdua tarefa de gerenciar o seu projeto de TI, você pode fazer uso de alguma das diversas ferramentas existentes no mercado. Um bom exemplo de código aberto e online é o *DotProject* [1], com o qual pode-se gerenciar múltiplos projetos (**figura 2**), com acompanhamento de andamento, usuários e tarefas, tempo de execução, prazos e estimativas etc.

Outra boa ferramenta online com valor (em dólares) acessível é o *VPMI* [2], baseado na metodologia PMI de gerenciamento de projetos. Com uma interface mais amigável (**figura 3**), executa as mesmas tarefas do DotProject e de outras ferramentas proprietárias.

Estudo de caso

Na administração de empresas, é utilizado um famoso método, chamado POC3, que significa *Planejar*, *Organizar*, *Coordenar*, *Controlar* e *Comandar*. Pretendemos demonstrar, doravante, que essa fórmula também é válida no gerenciamento de projetos em TI, podendo ser aplicada em quaisquer cenários que se apresentarem, independendo de sua complexidade ou extensão.

Partiremos de um cenário formado por uma empresa de consultoria, cuja meta é a construção de um CRM online para um cliente externo. Nesse tipo de sistema, cujo principal foco é a automatização dos procedimentos de fidelização, interação e organização das informações dos seus clientes, é necessário organizar um projeto com quaisquer metodologias que se queira escolher, desde que se obtenha o máximo aproveitamento dos seus recursos (**figura 4**), atendendo no menor tempo essa necessidade (lembrando dos tripés do projeto, mencionados anteriormente).

Sendo assim e, nesse caso, seguindo a metodologia PMI, o primeiro passo é a organização do escopo do projeto. O gerenciamento do escopo considera a melhor forma de definir claramente o que se espera no final do projeto, ou seja, o entregável, o produto ou serviço, que, nesse caso, vem a ser o sistema de CRM. É necessário prever as expectativas do cliente, e um dos maiores problemas nessa fase do planejamento justamente é a dificuldade em abarcar totalmente os desejos do cliente, transformando-os em um planejamento coerente. É necessária uma boa dose de estratégia por parte do gerente de projetos para conseguir formalizar os desejos que o cliente não revelou diretamente no seu escopo do projeto.

A seguir, é necessário determinar as atividades que devem ser seqüenciadas e estimadas, com a finalidade de produzir um cronograma ao mesmo tempo realista e coerente. A etapa de gerenciamento dos prazos é aquela em que ocorrem os maiores conflitos, pois, geralmente, nos sistemas de TI, os prazos são curtos e é necessária uma grande integração entre as equipes envolvidas no projeto, a fim de não haver falhas que levem a atrasos. O ideal é que os gerentes de projeto conversem com a equipe que vendeu o sistema para o cliente, a equipe que o desenvolverá, a equipe que fará o suporte e assim por diante.

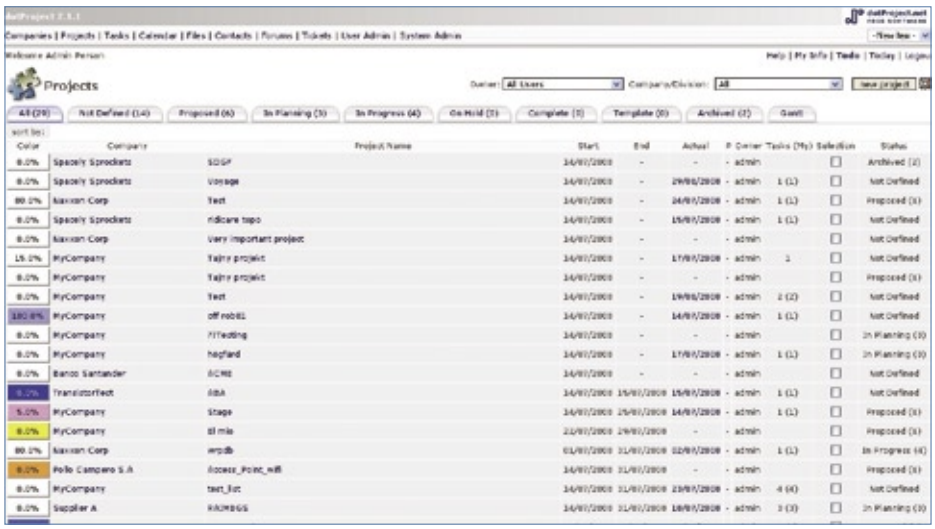


Figura 2 Interface de gerenciamento do *DotProject*.

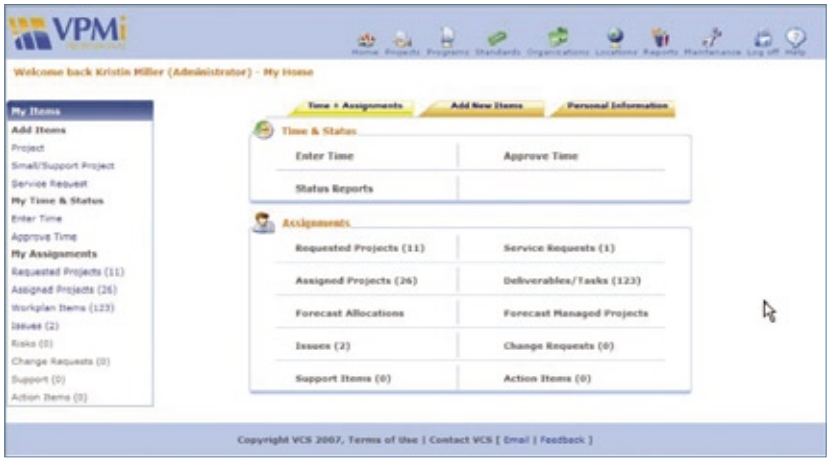


Figura 3 O *VPMI* obedece às normas PMI.

É primordial manter uma excelente comunicação entre as áreas responsáveis e, como isso nem sempre é tão simples, uma saída para o gerente de projetos é dividir o escopo do projeto em unidades menores, com a finalidade específica de manter na linha cada área envolvida em separado. Isso também torna mais fácil a organização e o acompanhamento das tarefas individuais, facilitando a visualização do progresso do projeto como um todo.

Quanto custa?

A parte mais crítica do projeto (se é que todas elas não o são) é o gerenciamento dos custos. Essa parte é constituída pelo acompanhamento dos custos individuais e totais de cada recurso necessário (bens, insumos, recursos humanos, serviços terceirizados, mercadorias em geral etc.) e a sua intenção é que o orçamento do projeto seja cumprido conforme aprovado.

É importante lembrar que o gerente de projetos deve comunicar-se constantemente com a área responsável por vender o sistema, visto que é comum que uma área comercial venda um sistema sem o real conhecimento dos valores que ele implica. Assim, acaba sendo usual o incremento de custos no decorrer do projeto. Dessa forma, será preciso fazer um levantamento individual de cada recurso necessário e agregado à solução, gerando novos orçamentos e levando-os até a aprovação do cliente. A solução para corrigir essas eventuais falhas de comunicação entre os setores é tratar todos os valores envolvidos de forma individual, discriminando-os elemento por elemento, mesmo que em uma planilha eletrônica comum. Essa prática torna mais simples a visualização dos custos gerais do projeto, tornando-a ao mesmo tempo mais precisa, inclusive abrindo a possibilidade de cálculo de uma pequena margem para imprevistos.

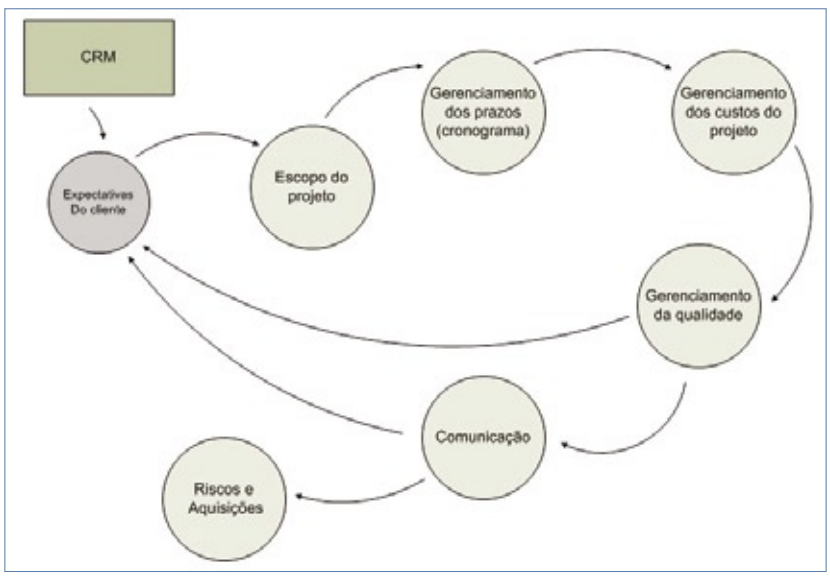


Figura 4 Cenário do projeto de construção de um aplicativo CRM.

Nessa etapa, deve-se ter especial cuidado com o gerenciamento dos riscos do projeto. Ao pôr o foco sobre ele, é necessário procurar a melhor tecnologia a ser utilizada, levando-se em consideração os custos com pessoal especializado, aquisição e gerenciamento de produtos ou mão-de-obra terceirizada.

Quem mandou?

Não menos importante é a satisfação do cliente. Nesse ponto da organização do projeto, é necessário atentar para o gerenciamento da qualidade. Sabemos que os clientes querem seu produto funcionando "para ontem", porém, é necessário permitir que ele acompanhe o andamento do projeto, preferencialmente com reuniões para que veja com seus próprios olhos o andamento do produto que está sendo produzido. Mantê-lo informado e manter-se continuamente em contato com ele evita reações inesperadas como o famoso: "Não foi isso que eu pedi".

Partindo para a organização prática do projeto de criação do sistema de CRM, levamos em conta:

- Tempo de desenvolvimento. Com base em um cronograma a ser desenvolvido e aprovado tanto pelas equipes envolvidas no desenvolvimento, quanto pelo cliente;

- Valor do desenvolvimento. Orçamento baseado na tecnologia empregada, recursos etc. e submetido à aprovação do cliente.
- Tecnologia a ser utilizada. Linguagem, banco de dados, estrutura de servidores, design de interfaces, etc.
- Recursos, sejam eles humanos, físicos (materiais, bens e insumos) ou mão-de-obra terceirizada.

Em se tratando de um projeto de TI, podemos esmiuçar um pouco mais o desenvolvimento do produto final – o CRM – e temos, então:

- Escolha do hardware;
- Escolha do sistema operacional de base;
- Modelagem do banco de dados;
- Desenvolvimento de módulos da aplicação;
- Testes;
- Implementação.

O ideal, já que o objetivo principal desse projeto parece assim demandar, é detalhar ainda mais o item de desenvolvimento dos módulos do CRM – afinal de contas, ele será o principal entregável do projeto em questão. Como exemplo, tenho os seguintes módulos:

- Controle de usuários;
- Cadastro de clientes;
- Suporte;
- Vendas;
- Pesquisas;
- Marketing e divulgação;
- Relatórios;.

A árvore de organização do projeto, com suas respectivas ramificações, termina por ser organizada de forma semelhante ao mostrado na **figura 5** – um excelente subsídio para que o gerente visualize como o projeto de fato deve transcorrer.

Baseando-se nesse resumo principal dos módulos, você pode começar a pensar no cálculo dos prazos, estimando cada tarefa individual de cada módulo em específico. É importante individualizar as tarefas, para melhor controle do prazo, recursos humanos e financeiros envolvidos, etc. Ao incluir qualquer tarefa individual no seu cronograma, é importante informar aos envolvidos e monitorar **continuamente** o progresso da tarefa.

Outro fator importante que deve ser levado em conta é evitar o uso de tarefas dependentes. Tais tarefas, que só podem ser executadas quando outra tarefa estiver concluída, são o "calcanhar de Aquiles" de um projeto, pois caso tais tarefas tenham problemas ou atrasos, o restante do projeto é comprometido. É possível evitar as tarefas dependentes caso você trabalhe com módulos, como já mencionado no exemplo anterior. Dessa forma, os módulos ficarão prontos paralelamente, o que proporciona melhor controle sobre o tempo e andamento do cronograma.

Caso seja necessário interligar esses módulos, crie uma nova fase do projeto, na qual cada módulo será interligado com outros módulos pela equipe por ele responsável. A adição dessa fase pode fazer com que todo o projeto seja concluído em prazo recorde, sem atrasos ou dependências impossíveis.

No caso de módulos que dependem de outros e dos quais não é possível "livrar-se", é necessário e importante prever que módulos se encaixam nessa característica, definir qual é o limite de atraso suportado sem engavetar todo o restante do projeto e, talvez, reforçar suas respectivas equipes. É provável que você tenha de definir rapidamente uma estratégia para gerenciar tais conflitos, e essas estratégias englobam reforço em recursos humanos, mão-

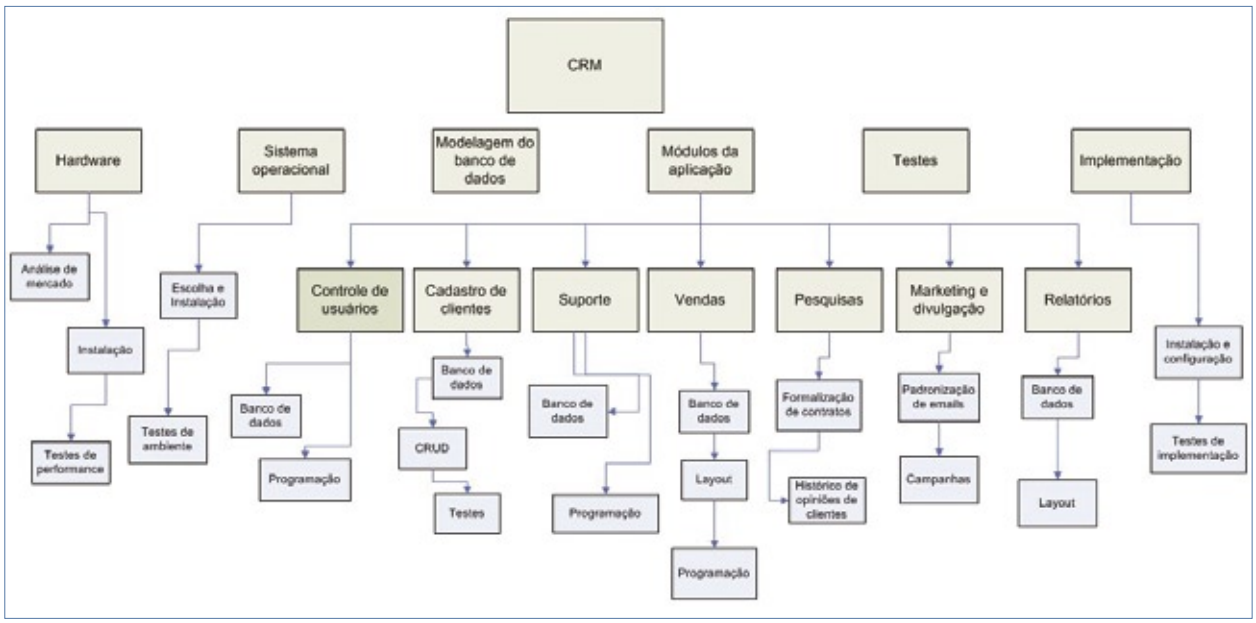


Figura 5 Árvore de organização do nosso projeto.

Tabela 1: Cálculo de tempo e custos de um recurso em sua tarefa

Recurso	Tarefa A	Tarefa B	Tempo total	Custo/h	Custo total
Analista	20	10	30	15,00	450,00
Testador	10	10	20	12,00	240,00
Desenvolvedor	10	35	45	24,00	1.080,00

de-obra terceirizada, horas extras trabalhadas etc.

Para calcular o tempo de *normatização* de cada módulo, o ideal é comunicar-se com os envolvidos. Um bom gerente de projetos jamais toma para si a premissa de que determinado membro da equipe deverá concluir sua tarefa em determinado tempo: o gerenciamento coerente das tarefas, unido à constante comunicação, é de suma importância. Veja um exemplo do cálculo de tempo e custos de um recurso em sua tarefa na **Tabela 1**.

Considerações finais

Algumas dicas para o bom andamento dos seus projetos:

- Caso seu projeto seja extremamente extenso, prefira dividi-lo em fases, com seus respectivos módulos e tarefas. Evite projetos intermináveis, pois é impossível prever os conflitos e contratempos em projetos que duram anos. Ao dividi-lo em fases, você pode até estar trabalhando com várias fases ao mesmo tempo, vários cronogramas e escopos, porém terá a visão global do projeto inteiro, o que facilitará ao se desenhar uma estratégia;
- Mantenha a motivação das equipes envolvidas. O esgotamento físico e mental dos membros da sua equipe pode, certamente, acarretar atrasos, falhas de comunicação e erros em tarefas. Evite utilizar os seus melhores membros de equipe (aqueles que mais se destacam na resolução de problemas) em diversos módulos ou tarefas, cortando o efeito de disputa entre recursos;
- Evite alocar membros em excesso para uma mesma tarefa ou então enxugar demais os prazos de uma tarefa.
- Use e abuse de consultores externos, caso haja necessidade. Sejam eles outros gerentes de projeto ou não, as opiniões de pessoas que estão fora do seu projeto podem ajudá-lo a ver de forma diferenciada algum problema, conflito ou estratégia empregada. Lembre-se de que o intuito é sempre maximizar o trabalho por tempo e custo;
- Dê poderes de decisão para sua equipe. Um bom gerente de projetos, que mantém os canais de comunicação sempre abertos, raramente vai se deparar com situações como recursos sem alocação por falta de pró-atividade. Deixe claro que cada um pode tomar à frente outra tarefa, ou mesmo auxiliar outro membro, a fim de garantir o bom andamento do cronograma. Outros poderes, como decidir layout, estrutura, metodologias de programação etc., também são bem vindas e amplamente aceitas por todos;
- Evite a qualquer custo o uso de "gambiarras" ou qualquer outro método temporário de solução de problemas. É melhor esticar o cronograma por algo bem feito... do que ter de ficar – e conseqüentemente exigir que os membros da equipe façam o mesmo – solucionando problemas "repentinos";
- Adote metodologias. Por mais que você dê poderes de decisão para os membros da sua equipe, adote metodologias, tanto para versionamento do código-fonte e modelagem do banco de dados quanto para a adoção de métodos de programação. Isso evitará a dependência de um membro da equipe, no caso de futuras manutenções, como também facilitará a documentação do projeto como um todo;
- Abra seus canais de comunicação. Mantenha-se aberto para que os membros de sua equipe possam vir apresentar problemas ou mesmo idéias. O gerente de projetos não sabe tudo e mesmo que saiba, um membro da equipe pode ter uma grande idéia que ninguém havia pensado. Use o potencial dos recursos que você possui para melhorar sempre!

Existe uma boa chance de que, com organização, olho crítico e acompanhamento constante, seu projeto seja um grande sucesso! ■

Mais informações

[1] DotProject: http://www.dotproject.net

[2] VPMI: http://www.vcsonline.com

Sobre a autora

Flávia Jobstraibizer é desenvolvedora PHP e DBA há seis anos, e trabalha com diversas tecnologias relacionadas a essas especializações. Atualmente atua como consultora de TI e programadora, sobretudo junto a empresas de comércio eletrônico, e se prepara para obter a certificação IPMA.

Com o **UOL HOST** você nunca está sozinho.

info
MELHOR RELAÇÃO CUSTO/BENEFÍCIO

Programa de Parcerias UOL HOST

Entre em contato e saiba as vantagens

Hospedagem de Sites

Plano Econômico:
- Hospedagem
- Registro de domínio*
- E-mail Profissional
- Atendimento Personalizado

R$ 14,90 /mês

Registro de domínios

Domínio Internacional ("*.com*" ou "*.net*")

R$ 15,00 /ano

Domínio Nacional ("*.br*")

R$ 30,00 /ano

Na compra de um plano de hospedagem, **GANHE** o registro de domínio GRÁTIS

*Na compra de um plano de hospedagem de sites para um novo domínio o UOL HOST paga a primeira anuidade do domínio.

Servidores dedicados

- DELL R200 - Xeon Dual Core 2.33 GHz
- 2 GB de memória RAM
- 2x250 GB (Serial Ata2) de Disco
- 4 Mbps de Banda

R$ 490,00 /mês

Painel de Controle UOL HOST

O painel mais moderno do mercado. Gerenciamento completo para as necessidades administrativas do dia-a-dia do seu website.

UOL HOST
QUALIDADE EM SERVIÇOS WEB

ASSINE 0800 723 6000

WWW.UOLHOST.COM.BR

Werner Braun – sxc.hu

O sistema de workflow e BPM Bonita

Fluxo sincronizado

O sistema de workflow de código aberto Bonita é comparável às melhores alternativas comerciais e conta com o apoio de grandes empresas.

por Miguel Koren O'Brien de Lacy

A execução de nossas atividades durante o horário comercial num dia de trabalho muitas vezes dá a impressão de falta de eficiência, falta de coordenação com outras pessoas ou mecanismos e falta de visão dos objetivos, resultados e etapas de nossas atividades. Hoje, a grande maioria das empresas e pessoas percebem as vantagens de se aumentar a eficiência, obter visibilidade sobre o estado das ações e estruturar a empresa focando-se nos fluxos de trabalho e processos. As empresas desejam capturar o conhecimento, aplicar as melhores práticas, incorporar decisões humanas nos fluxos de trabalho – ou *workflows* –, reutilizar a experiência adquirida e implementar as necessidades da forma mais simples possível.

"Workflow" é um termo amplo que pode ser definido como a formalização do modelo da seqüência de etapas que devem ser efetuadas por uma empresa, mecanismo, grupo ou indivíduo para realizar certa operação, que pode ser documentado e aprendido. Integra elementos tais como recursos, materiais, energia, funções e informações numa seqüência que forma um processo de trabalho. Por exemplo, podemos falar sobre o workflow para aprovação de pedidos recebidos na empresa. Os fluxos de trabalho são entidades que costumam ser usadas quando são tratadas organizações, projetos, equipes, funções e hierarquias. Além disso podem ser considerados como elementos de construção das organizações. Em TI, o termo "workflow" é usado para capturar, representar e desenvolver a interação entre pessoas e sistemas para realizar processos.

O termo "Business Process" (processo de negócio) é considerado por muitos como a extensão moderna do workflow, e entendemos que define o conjunto de etapas e fluxos nos quais interagem pessoas, sistemas, informações e regras para obtenção do resultado final desejado. Assim, BPM (*Business Process Management*) é a gestão dos processos de negócio.

Os workflows vêm da área de manufatura, com os trabalhos de Taylor e Gantt no começo do século 20.

Mais recentemente, as noções tradicionais de workflow sofreram críticas por considerar os atores humanos nas etapas como simples executores sem potencial de melhoramento, assim como pela idéia de que os fluxos desenhados engessavam a empresa e não permitiam uma resposta ágil a novas necessidades de mercado. Assim, começaram, nos anos 1980 e 1990, as noções de "Six Sigma", "reengenharia de processos" e outras técnicas para melhorar a qualidade dos resultados. Mais recentemente, especialmente nos últimos cinco anos, ganhou grande visibilidade o conceito de automação e orquestração de processos pequenos de forma automática. Hoje, a SOA (*Service Oriented Architecture*[1]) tem grande impacto em projetos de TI.

Com as novas possibilidades da TI, as etapas de capturar, implementar e monitorar os workflows e processos tendem a confluir para uma única ferramenta. Desse ponto de vista, os padrões ganham grande importância para implementar essa necessidade e são fundamentais para migrar as definições entre sistemas de diferentes fabricantes.

O histórico de evolução desse campo e os sistemas disponíveis tornaram íntimas as áreas de workflow e automação de processos. A crescente necessidade de consolidar sistemas faz com que cada empresa ou pessoa procure solucionar suas necessidades com a menor quantidade de sistemas possíveis. Claro que SOA atende à necessidade de integrar sistemas não relacionados, como os ERPs de parceiros de negócio, por exemplo, ou um sistema que integra gestão de documentos com aprovação de pedidos; mas todos queremos utilizar apenas uma plataforma, tanto para automação de processos executados por sistemas quanto para workflow (captura, implementação e monitoramento). A situação é similar à das ferramentas UML ou à modelagem de bancos de dados: o trabalho de modelagem é muito laborioso e ninguém quer repeti-lo para migrar para outra ferramenta. Em particular, pre-

cisam ser considerados os aspectos da notação para descrever o workflow, o suporte de TI para implementar essa notação, os padrões para situações distintas que devem ser consideradas e as linguagens para execução automática quando requeridas.

Bonita

O sistema *Bonita*[2] e seu complemento *Orchestra*[3] são membros do consórcio OW2[4], com forte apoio da Bull e da France Telecom. A missão do Bonita é gerenciar workflows de longa duração, orientados a processos com interação humana e com integração à automação de processos. O termo "longa duração", no caso, significa que o software não se foca exclusivamente em processos automáticos realizados por um sistema.

Um dos maiores destaques do Bonita é a participação de sua equipe em outras que desenvolvem esse tipo de soluções em Software Livre. Atualmente, o mercado está acostumado a soluções de workflow monolíticas, essencialmente fechadas e difíceis de expandir. São fechadas no sentido de que são elas que administram o processo e não interagem com outros sistemas semelhantes. Dificilmente, essas soluções facilitam o uso por parte de outros aplicativos de workflow.

Para a Microsoft, os serviços de workflow são tão importantes que a empresa criou a Windows Workflow Foundation para que qualquer aplicativo em Windows possa fazer uso dessa tecnologia. Na esfera do Software Livre, é o Bonita que oferece algo semelhante. Porém, a equipe do Bonita resolveu não trabalhar isoladamente e convidou outros grupos para participarem na definição de um novo conceito, chamado PVM (*Process Virtual Machine*, **figura 1**). Com isso, aproximou-se também a equipe do sistema *jBPM*[5], apoiada pela Red Hat. Em conjunto, definiram um mecanismo que possibilita a extensão do mecanismo de workflow, o que permite ser embarcado e estendido com diversas linguagens de execução, tais como BPEL e JPDL, que tem forte apoio na Red Hat; mas certamente outras ainda virão. É importante destacar que ambas as equipes colaboraram na definição do mecanismo, mas cada uma implementou a especificação de forma independente. A intenção é que um workflow que pode ser executado em Bonita também possa ser executado em jBPM sem alteração alguma.

Motores e aplicativos

No terreno de sistemas de workflow, devemos distinguir entre mecanismos ou "motores" (*engines*) de workflow e "aplicativos". Os motores são entidades mais simples que, por sua natureza, precisam ser integrados a aplicativos, pois sozinhos não resolvem o problema completo. Entre os motores para workflow, podem ser mencionados o próprio jBPM, *OpenWFE*[6], *OS Workflow*[7] e muitos outros que geralmente são incompatíveis entre si. Em termos de aplicativos, o Bonita tem como foco as mesmas necessidades de sistemas como o *OpenFlow*[8] e *Intalio*[9], porém, com a vantagem significativa de um forte suporte a padrões e uma modularidade interoperável com outros sistemas baseados na tecnologia PVM. Aplicativos de workflow oferecem um editor gráfico para definição dos fluxos, um editor para especificação das telas de interação com o usuário, segurança de acesso aos processos e etapas, um mecanismo de administração e de uso dos processos e formas de avaliar o estado dos processos para sugerir melhorias. No segmento de Software Livre, os aplicativos de workflow e o Bonita deixam algumas lacunas no aspecto de indicadores de processos, mas essa necessidade já pode ser compensada pelo fato de que o Bonita mantém todos os dados num banco de dados relacional.

Arquitetura

A arquitetura do Bonita (**figura 2**) permite seu uso como motor simples acessando a sua API, como aplicativo JSE ou como aplicativo JEE, dependo das necessidades da empresa. Atualmente, o Bonita está entre versões com grandes diferenças conceituais. A versão estável, 3.1, foi liberada em outubro de 2007. A nova versão, conhecida como "Nova Bonita", será liberada em setembro como Bonita 4. O Nova Bonita implementa a PVM e é o foco deste artigo. Assim como o SpagoBI[10], o Bonita pode rodar dentro do ambiente de portal *WebOS* da *Exo Platform*[11].

O WebOS é uma arquitetura revolucionária que apresenta um ambiente de trabalho com estilo "desktop" dentro de um navegador web. Os "apli-

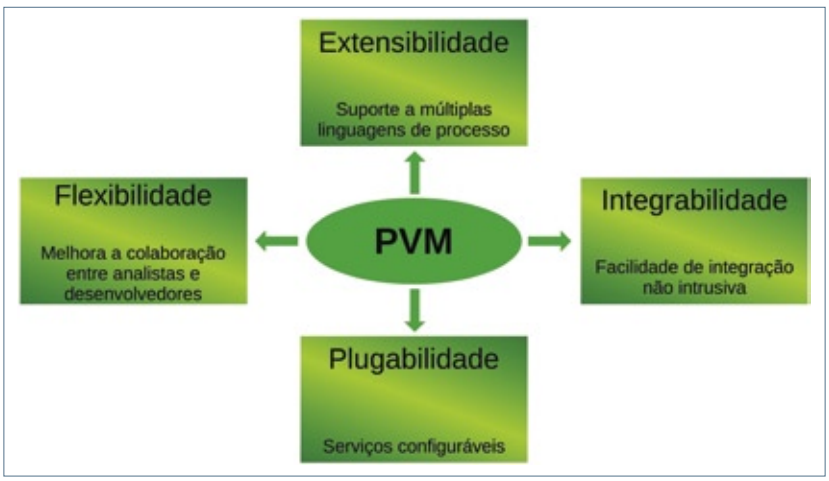


Figura 1 A *Process Virtual Machine*.

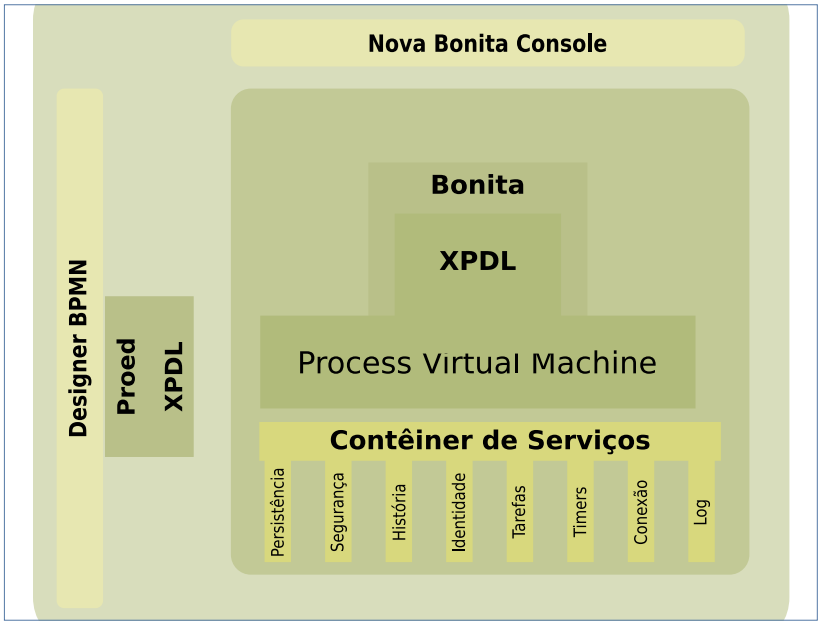


Figura 2 Diagrama funcional do *Bonita*.

cativos" do desktop são, na realidade, aplicativos web em *Java* que rodam como *portlets*, pois o WebOS é um portal com uma aparência distinta da convencional, implementada com uso avançado de tecnologia AJAX.

Na **figura 3**, o Bonita se encaixa no nível do WebOS como um portlet. A Exo Platform e, conseqüentemente, o Bonita, podem receber diversos aspectos visuais para melhorar a integração do Bonita ao restante do sistema.

Editor gráfico

O editor gráfico de workflow do Bonita é o *ProEd*, disponível em versão *stand-alone* e como plugin para a plataforma *Eclipse*. O ProEd é escrito em Java com *Swing*. A **figura 4** mostra o visual do ProEd na versão 3 do Bonita, também capaz de interagir com processos da versão 4. Em sua versão atual, o ProEd, que vem com o pacote RC2 do Nova Bonita, ainda não foi atualizada a interface de usuário para acompanhar todas as mudanças visuais do próprio Bonita.

Para o Eclipse, o ProEd é instalado simplesmente como um plugin, descomprimindo-se dentro do diretório de plugins e reiniciando-se o Eclipse. Aparece então um novo tipo de projeto dentro de "outros", com o nome de "ProEd".

Com o ProEd, podem ser capturados e documentados os processos que serão automatizados. O ProEd trabalha com o padrão XPDL para armazenar as informações dos processos. Trata-se de um padrão do WfMC que sofreu várias atualizações para ser adaptado às necessidades modernas. Atualmente, a versão 2 do XPDL é mais recente e o Bonita está evoluindo para suporte completo a essa versão ainda em 2008. No site do WfMC, existe uma lista de mais de 70 sistemas para workflow que implementam a XPDL. A interface entre o usuário e a etapa do processo pode ser desenhada dentro da janela administrativa do próprio Bonita.

Figura 3 Arquitetura da *Exo Platform*.

Integração

A integração dos workflows do Bonita com outros sistemas é feita por meio de *hooks*. Os hooks permitem incluir classes Java customizadas para ações relacionadas a diversos eventos da execução do workflow, tais como entrar numa etapa, sair da etapa etc. Praticamente qualquer situação pode ser tratada com os hooks. Um exemplo prático seria um processo de aprovação de despesas que deve estar integrado a um sistema de gerenciamento de projetos como o *Artemis*[12], por exemplo. Um hook especial (classe Java) é usado para mostrar uma lista de projetos na tela da etapa em que o funcionário solicita o reembolso da despesa. Um outro hook que atua na saída da etapa de aprovação poderia atualizar o valor aprovado da despesa diretamente a partir do sistema de gerenciamento de projetos. O documento de comprovação da despesa – por exemplo, uma nota fiscal digitalizada – poderia ser anexado a um sistema de gestão de documentos como o *Alfresco*[13], *Exo Platform ECM*[14] ou diretamente no sistema de gerenciamento de projetos que gerencie anexos, como o Artemis. Os hooks devem ser desenvolvidos como classes Java e não são definíveis pelo usuário que modela o processo com o ProEd. Uma característica importante do Bonita é seu suporte a sub-processos e datas de vencimento de etapas dos processos.

Outra característica muito útil na parametrização de etapas dos workflows é o *mapper* (mapeador). São mecanismos que executam classes Java especiais que podem selecionar quem tem acesso a determinada etapa do processo. Alguns mappers

especiais são o *InstanceInitiator* e o LDAP. O primeiro permite acesso ao usuário que iniciou esse processo. Por exemplo, numa etapa final de um processo que requer aprovação de uma solicitação, o próprio usuário que iniciou o processo é notificado sobre o resultado final. Nesse caso, o mapper a usar é InstanceInitiator. Os mappers customizados podem ser usados para qualquer situação de permissão de acesso.

O Bonita suporta diferentes situações de fluxos que são definidas pelos *workflow patterns*, boas práticas para workflow, equivalentes aos *design patterns* para programação. O suporte a essa tecnologia é comparável ao de outros sistemas livres e comerciais, como mostra o site dos workflow patterns. Infelizmente, o assunto não recebe muita atenção, assim como os design patterns na programação; porém, considerando-se a maturidade relativa da área de workflow, isso é esperado.

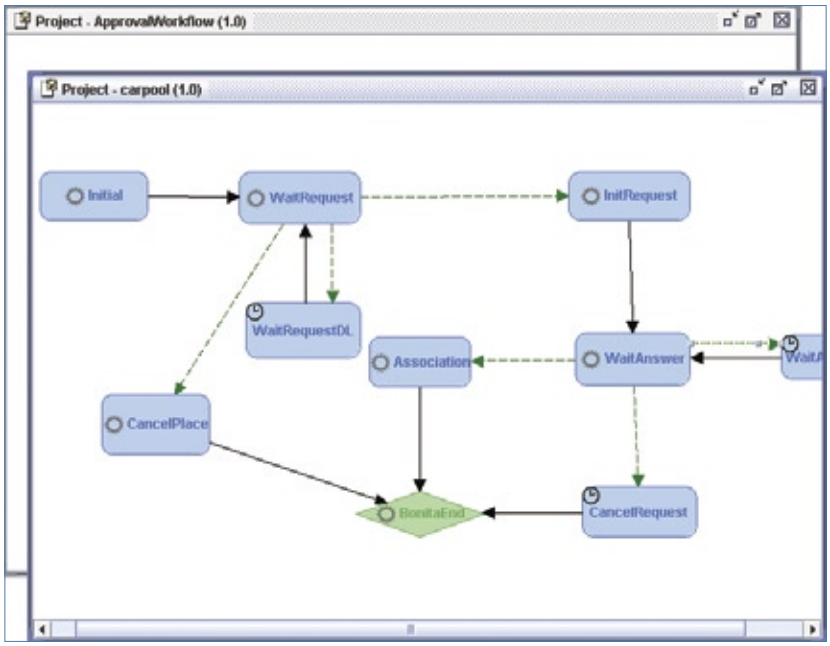


Figura 4 Editor *XDPL ProEd* em versão *stand-alone*.

Instalação e uso

A versão RC2 do Nova Bonita é a mais recente disponível para download. Ela inclui todos os elementos empacotados para implementação direta. Basta baixar o pacote correspondente à plataforma desejada e descompactá-lo. O software pode ser iniciado por meio do comando `bin/bpm.sh start`. O pacote RC2 inclui também o contêiner *Tomcat* na versão 6.0.x, que opera na porta TCP 8080. Antes de iniciar o Bonita, verifique a disponibilidade dessa porta. Para a instalação do pacote RC2, é importante que a variável de ambiente `JAVA_HOME` esteja definida e que as variáveis `CATALINA_HOME` e `CATALINA_BASE` **não** estejam definidas.

Em termos gerais, o sistema não será instalado dessa forma, pois precisa ser integrado à infra-estrutura de TI da empresa. A equipe do Bonita gera pacotes para instalação direta nos seguintes ambientes:

- Apache Tomcat;
- JBoss versões 4 e 5;
- JOnAS.

Um pré-requisito para a instalação do Bonita é o sistema *Ant*, cuja instalação é muito simples, assim como todas as demais instalações relacionadas ao Bonita. Para instalar com o Jboss, por exemplo, basta digitar `ant ear.jboss4` no diretório do pacote descompactado. O comando gera o arquivo `bonita.ear`, que pode ser copiado diretamente para o diretório de instalação do JBoss. Naturalmente, é necessário fazer a configuração antes de poder usar o software. Em virtude do suporte da Bull, existe documentação suficientemente completa para seguir todos os passos necessários; são poucos os sistemas livres com documentação tão apropriada.

No caso de instalação em conjunto com a Exo Platform, se não for usado o pacote completo já configurado, é preciso instalar a Exo Platform antes do Bonita. O mesmo vale também para JOnAS e JBoss.

Depois da instalação e configuração, o sistema já pode ser acessado. No caso do pacote completo RC2, a URL pré-configurada para acesso é `http://127.0.0.1:8080/portal`.

Figura 5 Portal *Exo Platform* com o *Bonita*.

Figura 6 Tela de login inicial da *Exo Platform*.

Esse endereço mostra o portal Exo Platform com o Bonita rodando como portlet (**figura 5**). Infelizmente, uma imagem estática não revela o poder da interface desse portal – é preciso experimentá-lo.

Administração

A tela de login (**figura 6**) não revela o importante detalhe de que o Bonita suporta LDAP para a autenticação, além de outras formas customizadas que podem ser definidas.

Após o login, aparece o "desktop" (**figura 7**) administrado pela Exo Platform, no qual podem ser abertos os portlets do Bonita selecionando-se os botões inferiores.

A administração de processos é feita pela janela do *Bonita Management*. Nela, podem ser incluídos processos novos definidos com uso do ProEd ou de outra ferramenta de modelagem aderente à XPDL. A aparência da tela de administração esconde seu poder: ela permite que se desenhe o aspecto visual das etapas de interação com o usuário.

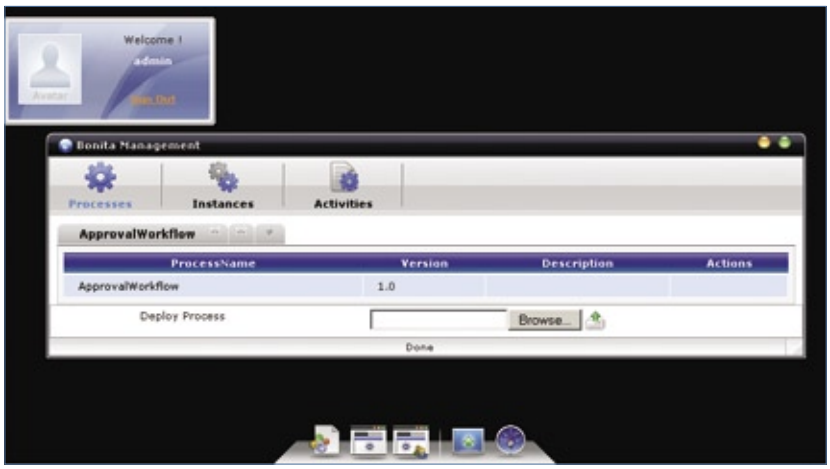


Figura 9 Novo *workflow* incorporado ao sistema.

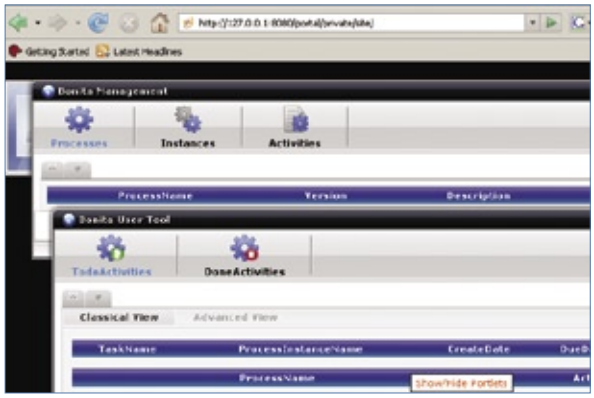


Figura 7 Ambiente de trabalho individual com *portlets Bonita* abertos.

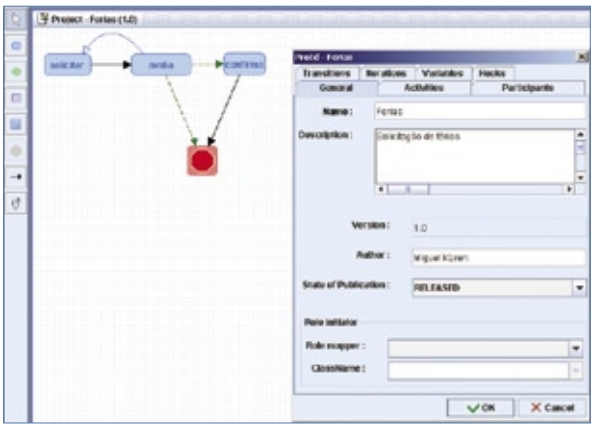


Figura 8 Desenho do processo de alocação de férias no *ProEd standalone*.

Um rápido exemplo

Para ilustrar o uso do sistema, definiremos um processo para solicitação de férias na empresa. Esse processo envolve uma solicitação que pode ser feita por qualquer funcionário da empresa (agrupados no grupo funcionários) e aprovada por alguém da área de Recursos Humanos. Existe uma interação entre RH e funcionário para solicitar maiores detalhes. Primeiramente, usaremos o ProEd para capturar e documentar o processo. O resultado do ProEd é um arquivo de extensão `xpdl` que pode ser incorporado ao Bonita usando a janela administrativa. A **figura 8** ilustra esse procedimento. Para iniciar o ProEd, basta entrar no diretório onde ele foi descompactado e digitar o comando `ant`.

Usando a janela administrativa do console BPM (**figura 9**), incorporamos esse processo ao repositório. Uma vez incorporado, ele fica disponível para os usuários que tenham permissão de iniciar esse processo.

O workflow é iniciado em estado instanciado. No caso do nosso exemplo, a primeira etapa já interage com o usuário. Pode haver workflows iniciados automaticamente por eventos monitorados pelo sistema ou pelo início de um processo solicitado pelo sistema externo. Um exemplo poderia ser a interação entre um sistema ERP e o Bonita. Pela API do Bonita, o sistema ERP solicitaria o início do workflow de aprovação do pedido. Também poderia ser pensado no caso de um sistema de gestão de documentos que solicita o início de um processo de aprovação. A **figura 10** mostra a interação entre o sistema e o usuário para a primeira etapa do processo de exemplo.

Com o uso do sistema, a tela do usuário e a tela administrativa começam a mostrar as instâncias de workflows iniciados, concluídos e em andamento.

Nosso exemplo simples mostra como a interface do usuário facilita o uso do sistema e esconde o poder deste. As atividades que devem ser realizadas estão disponíveis diretamente sem complicação e o administrador tem uma visão sobre o estado dos processos e o histórico. Essa informação pode ser usada para monitorar os processos e avaliar modificações

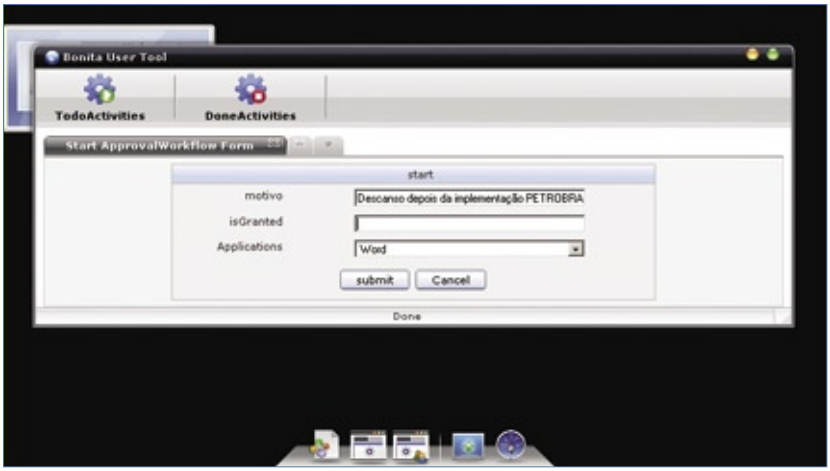


Figura 10 Tela padrão de interação entre a etapa do processo e o usuário.

para sua melhoria. O Bonita permite atribuir versões aos workflows e, por consultas feitas ao banco de dados onde são persistidos, podem ser feitas análises comparativas.

Conclusão

É difícil imaginar uma situação que requeira o serviço de workflow para a qual o Bonita não seja uma solução excelente. A empresa que implementa Bonita conta com uma plataforma relativamente completa, muito modular, com grande capacidade de expansão, aderente a padrões, adaptável a arquiteturas corporativas complexas ou simples e com o apoio de uma organizações como OW2 e Bull. Do ponto de vista do nosso mercado, falta ao sistema atualmente a interface de uso em português brasileiro para o console de uso e de administração, mas isso é facilmente solucionável durante a implementação. O uso do ProEd em versão stand-alone permite que as funções dentro da empresa sejam separadas. Analistas de negócio podem capturar e modelar os processos de negócio usando essa ferramenta visual, e os integradores ou programadores podem posteriormente incluir a lógica adicional na forma de hooks e mappers. Entretanto, o uso do ProEd dentro do Eclipse ajuda os desenvolvedores, pois podem tratar todos os aspectos do workflow e desenvolvimento dentro de um mesmo ambiente de trabalho.

O Bonita somente pode melhorar com o tempo. A partir da versão 4 (a versão 4.1 está planejada para liberação no final de 2008), haverá um esforço para tornar a interface do usuário ainda mas simples, direta e atraente. Porém, para uso corporativo, as seguintes melhorias (já planejadas) são as mais importantes:

- suporte completo à versão 2 da XPLD e à notação BPMN;
- console para BI, ou seja, relatórios de estados de processos, tempos etc.;
- console para BAM (*Business Activity Monitoring*). BAM é uma solução corporativa popularizada pelo Gartner Group para fornecer às áreas operacionais e à diretoria da empresa informações em tempo real sobre a situação dos processos de negócio.

As novas características completam o pacote com alguns elementos ainda ausentes para auxiliar na melhoria dos processos de negócio e maior suporte a padrões. ■

Mais informações

[1] Linux Magazine 42, "SOA": http://www.linuxmagazine.com.br/issue/lm_42_soa

[2] Bonita: http://wiki.bonita.objectweb.org

[3] Orchestra: http://orchestra.objectweb.org

[4] Consórcio OW2: http://www.ow2.org

[5] jBPM: www.jboss.org/jbossjbpm/

[6] OpenWFE: http://www.openwfe.org

[7] OS Workflow: http://www.opensymphony.com/osworkflow

[8] OpenFlow: http://www.openflow.it

[9] Intalio: http://bpms.intalio.com

[10] Miguel de Lacy, "Negócio Inteligente – SpagoBI": http://www.linuxmagazine.com.br/article/1747

[11] Exo Platform: http://wiki.exoplatform.com

[12] Artemis: http://www.aisc.com

[13] Alfresco: http://www.linuxnewmedia.com.br/article/documentos_fresquinhos

[14] Advanced ECM: http://wiki.exoplatform.com/xwiki/bin/view/ECM/Advanced+ECM

Sobre o autor

Miguel Koren O'Brien de Lacy (miguelk@konsultex.com.br) usa Software Livre desde 1997 e tem experiência de gerenciamento de projetos na América Latina, EUA e Europa. É diretor da Konsultex Informática (www.konsultex.com.br), representante da Artemis International Solutions Corporation (www.aisc.com), da Advanced Management Solutions (www.amsusa.com) e da Software Productivity Research (www.spr.com), além de ministrar palestras sobre Software Livre e participar em diversos fóruns de suporte ao Código Aberto.

Gerenciamento de projetos em código aberto com o ClockingIT

Na hora exata

Aggelos Fasoulis - www.sxu.hu

O ClockingIT é uma solução de gerenciamento de projetos rica em recursos e com uma bela interface web. Basta optar entre as versões local e hospedada e usar.

por Erlend Simonsen

O mercado de gerenciamento de projetos online está bastante cheio, ultimamente, com a maioria das soluções adotando modelos proprietários ou com alto custo, ou ambos. Entretanto há o *ClockingIT*[1], uma solução livre e gratuita disponível para todos.

O ClockingIT exibe uma longa lista de recursos que inclue o acompanhamento automático do tempo gasto em cada tarefa de um projeto, a verificação da forma como os envolvidos estão gastando seu tempo e quanto trabalho ainda precisam fazer, um RSS com as alterações mais recentes e um gráfico de Gantt que mostra todo o planejamento do projeto. O software tem interface Web e faz uso intenso de Ajax para permitir a atualização dos dados em tempo real.

Histórico

O software é fruto do trabalho do casal norueguês Erlend (que escreve este artigo) e Ellen Simonsen. Erlend o desenvolveu quando trabalhava numa pequena empresa de consultoria em 2004, onde tinha a sensação de que ele e seus colegas trabalhavam muito mais do que aquilo pelo qual os clientes lhes pagavam. Para conferir se sua sensação era verdadeira, eles precisavam verificar o que cada um deveria fazer, para quem e durante quanto tempo. A solução – um aplicativo de acompanhamento de tempo – parecia simples. Entretanto, encontrar o aplicativo certo se mostrou surpreendentemente difícil. Nenhum dos programas já existentes que encontraram apresentava a flexibilidade, o custo ou os recursos de que precisavam. Para conseguir o que queria, Erlend precisaria criar sua própria solução.

Após começar a desenvolver uma versão do sistema em C# e, posteriormente, em *Java*, o desenvolvedor se deparou com o vídeo "Criando um weblog em 15 minutos" (*Creating a weblog in 15 minutes*[2]), que mostra a agilidade de programação com uso do *Ruby on Rails*. O vídeo o convenceu da qualidade desse framework e ele baixou a versão 0.10 para testá-la. Uma semana mais tarde, surgia o ClockingIT.

Infelizmente, ainda não parecia uma solução profissional, pois seu visual realmente deixava a desejar. Por sorte, a esposa de Erlend, web designer, decidiu se envolver e fez uma verdadeira plástica no software. Com isso, o ClockingIT estava pronto para sua silenciosa estréia na Internet, em 2005, hospedado num velho desktop no escritório do casal desenvolvedor – hoje, ele roda num servidor apropriado e em um ambiente de hospedagem adequado.

O número de usuários cresceu rapidamente. Após algum tempo, os usuários pediram algum meio para instalar o programa em seus próprios servidores e, assim, o código-fonte foi liberado em abril de 2007. O autor gostaria muito de ver mais pessoas envolvidas no processo de desenvolvimento, pois continua desenvolvendo o software sozinho.

Recursos

Como a principal idéia por trás do ClockingIT é acompanhar o tempo gasto em tarefas, as funções de acompanhamento de tempo estão profundamente integradas à aplicação. Registrar tempos e horas requer apenas um clique ao iniciar e outro ao terminar a tarefa. Para conferir quanto tempo foi gasto numa tarefa, há vários relatórios disponíveis – incluindo um relatório pivô extremamente flexível e uma planilha de tempo pronta para impressão.

Uma vez criados alguns projetos e tarefas, pode-se usar o gráfico de Gantt interativo para facilmente agendar as tarefas e *milestones* (os pontos ou funções mais importantes do projeto, no jargão do gerenciamento de projetos) simplesmente arrastando os indicadores para as datas adequadas. Além disso, o calendário de eventos é atualizado automaticamente.

Dependências entre tarefas e a garantia de que todas as pessoas a receberem uma tarefa estejam livres também são tratadas automaticamente pelo calendário.

Todas as alterações feitas às tarefas são registradas e indexadas para busca, o que significa que é possível ver exatamente quando algo foi registrado, feito, completado, atualizado, reatribuído etc. Também é possível acrescentar comentários a uma tarefa e, quando seu email de notificação de mudanças é respondido, o conteúdo do email de resposta é adicionado ao histórico da tarefa.

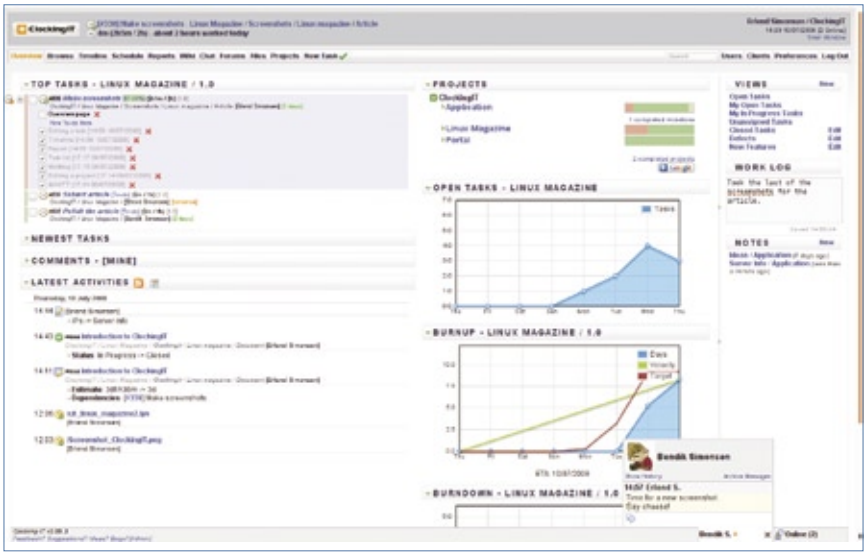


Figura 1 Visão geral de um projeto.

Há uma página de visão geral bastante customizável, com vários *widgets* à disposição, que podem ser configurados para exibir apenas as informações de interesse (**figura 1**).

Usuários do serviço *iGoogle* podem instalar o widget do ClockingIT e sempre ver suas próximas tarefas.

Cada projeto pode ter seu fórum privado integrado para facilitar discussões, assim como salas de *chat* privadas para colaboração em tempo real.

Atualmente, a interface está disponível em 14 idiomas e toda a tradução é feita de dentro do próprio software.

Arquitetura

Como já mencionado, o ClockingIT foi escrito usando a tecnologia Ruby on Rails, e a versão hospedada hoje está rodando sobre um sistema FreeBSD com um banco de dados MySQL.

Para manter a interface em sincronia ao longo de várias instâncias do navegador web, é usada uma versão fortemente modificada do *Juggernaut*[3] no servidor para fazer os navegadores clientes atualizarem as alterações sem que os usuários precisem recarregar as páginas.

O Juggernaut usa um *applet* em *Flash* que se conecta a um *push-server* personalizado e mantém um soquete aberto durante toda a visita, a fim de receber o código *Javascript* que atualiza as páginas dinamicamente. Essa tecnologia também está presente nas funcionalidades de mensagens instantâneas do ClockingIT, além de não sobrecarregar o servidor com requisições de *polling* a cada poucos segundos.

O Ruby on Rails tende a precisar de bastante memória para aplicações maiores, já que ele abre uma nova instância para cada requisição atendida em paralelo. Isso é uma conseqüência principalmente do fato de o Ruby on Rails não ser *thread-safe*. Para reduzir o uso de memória significativamente, é usada uma versão do Ruby com os *patches* do *Garbage Collector*[4] em conjunto com *Slim Attributes*[5] (atributos magros, literalmente), o que diminui a memória exigida pelo *ActiveRecord*, a camada de abstração de bancos de dados do Ruby on Rails.

Nas buscas, são usados o *Ferret*[6] e o *acts_as_ferret*[7] para lidar com a indexação e realizar as buscas propriamente ditas sem esforço.

Hora do teste

Para usar o ClockingIT, primeiramente é preciso criar uma conta em [8]. A primeira conta criada para a empresa será, obrigatoriamente, a do administrador, mas é possível dar direitos de administração a outros usuários. É preciso escolher um nome adequado para a empresa, juntamente com a URL privada que se deseje usar ao acessar a conta.

Após completar o registro, é possível adicionar usuários a partir da aplicação, mas apenas o administrador pode criar suas contas.

Depois de criar os usuários, já podemos começar a trabalhar. Primeiramente, é importante criar alguns clientes caso haja vários deles – isso ajudará a agrupar projetos relacionados para o mesmo cliente, o que facilita os relatórios e o acompanhamento do tempo.

Em seguida, vamos criar um projeto, atribuí-lo a um cliente, conferir-lhe um nome, uma breve descrição e um fórum, caso seja necessário um local para discutir problemas. Depois de criar o projeto, pode-se adicionar usuários a ele. Por padrão, o projeto é privado, mas é possível dar a outros usuários um acesso granular ao que for preciso (**figura 2**).

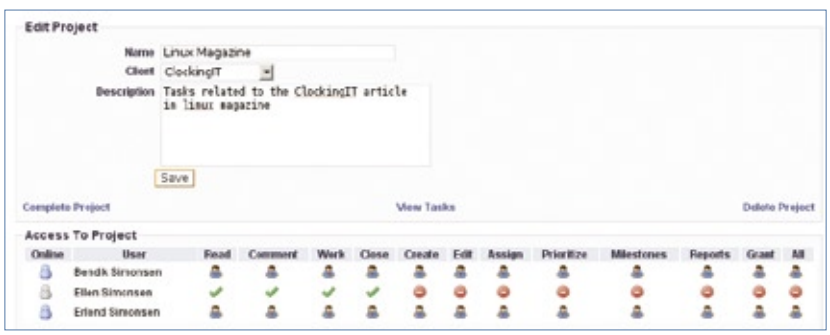


Figura 2 Atribuições de permissões num projeto.

Com o projeto criado e "configurado", podemos criar algumas tarefas relacionadas a ele e atribuir cada uma a múltiplas pessoas.

Conferir prioridades e pesos às tarefas permite que elas sejam ordenadas para que se faça o que realmente precisa ser feito, enquanto a estimativa de duração permite o acompanhamento do seu próprio progresso e o planejamento do calendário com mais detalhamento.

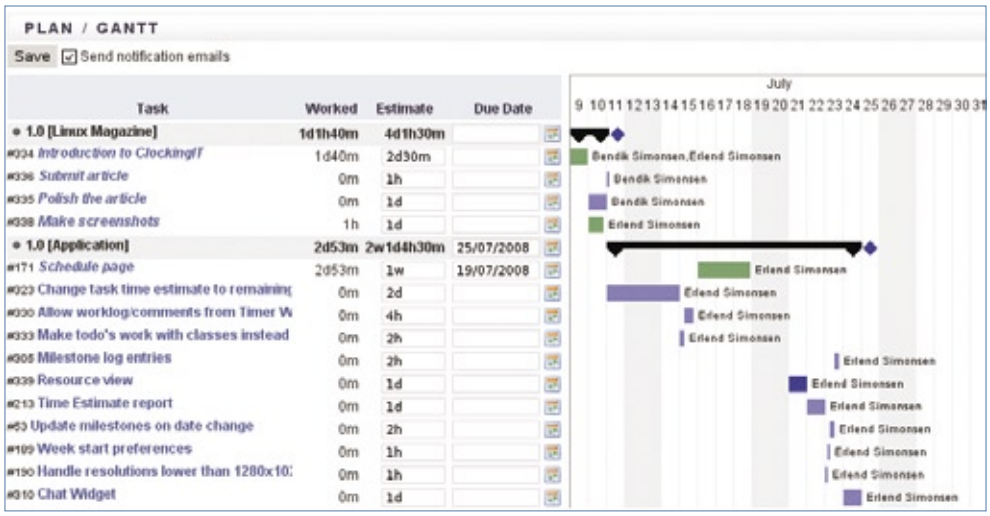


Figura 4 Gráfico de Gantt em *Ajax*.

Assim que a tarefa estiver definida, já se pode começar a trabalhar nela. Nas páginas *Overview* e *Browse*, ao procurar uma tarefa e clicar no relógio a seu lado, será iniciado o cronômetro da tarefa. Depois disso, o usuário pode fazer o que precisa, enquanto deixa notas na seção *Work Log*, à direita (**figura 3**).

Ao parar de trabalhar numa tarefa, basta clicar novamente no ícone e o tempo usado será salvo juntamente com as notas.

Fiscalizando

Isso é tudo de que se precisa para configurar um fluxo de trabalho diário no ClockingIT. Depois, todos os funcionários da empresa já podem trabalhar juntos em todos os projetos e tarefas. Com vários projetos e tarefas configurados, as funções de relatório e histórico de projetos se mostram muito úteis. A funcionalidade mais simples é a visão da linha de tempo, que permite a visão do que se passou nos projetos ao longo do tempo. Com o gráfico de Gantt, pode-se ter uma visão geral dos projetos ou, ainda, arrastar e soltar as tarefas para seus respectivos lugares (**figura 4**).

Para obter uma visão mais detalhada, a página de relatórios (chamada *Reports*) é o local certo. Pode-se ver o tempo gasto num projeto, numa tarefa, em um cliente específico ou por um usuário específico, a qualquer momento, exportando-se o resultado a qualquer programa de planilha, para manipulação dos dados (**figura 5**).

Fazendo upload do arquivo para o ClockingIT, todos os funcionários que precisarem acessá-lo podem obter uma cópia a qualquer momento, o que elimina a necessidade de um volume de rede compartilhado para os documentos pertinentes, por exemplo, a um único projeto.

Servidor próprio

A instalação do ClockingIT num servidor local não exige uma máquina poderosa. Além disso, o software geralmente não tem restrições quanto ao sistema operacional, desde que seja baseado em Unix, da mesma forma que o sistema de banco de dados – contanto que seja possível rodar o Ruby e o Rails, não há dificuldade. Se a demanda sobre o

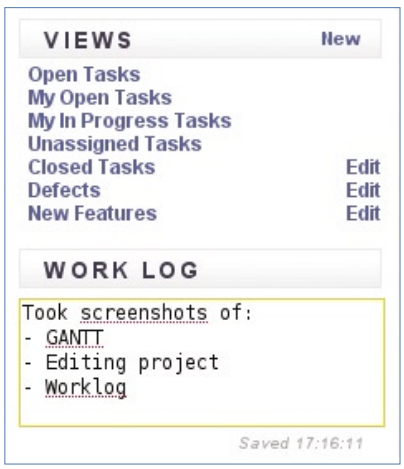


Figura 3 Anotações em uma tarefa de projeto.

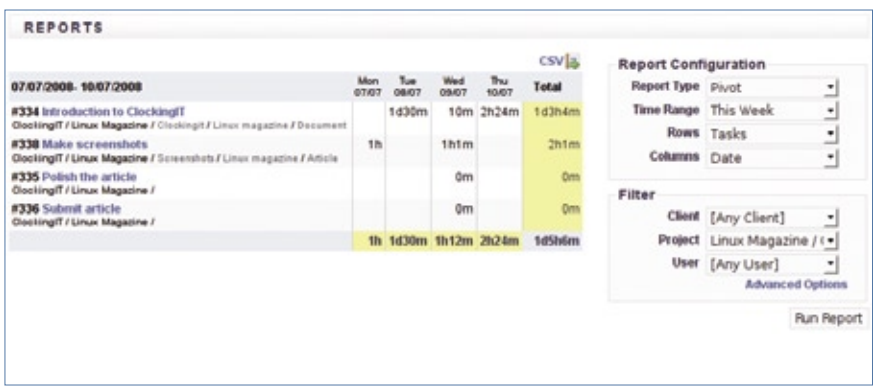


Figura 5 Exemplo de relatório pivô.

servidor for alta demais, é possível usá-lo num cluster de alto desempenho ou balanceamento de carga, mas isso geralmente não é necessário. Ainda assim, é importante saber que existe essa escalabilidade. Qualquer servidor comum suporta milhares de usuários simultâneos sem apresentar sinais de sobrecarga.

Como o ClockingIT está em intenso desenvolvimento atualmente, talvez seja melhor usar a versão do repositório Git:

```
$ git clone git://repo.clockingit.
➥com/cit.git
```

Alternativamente, para usar uma versão estável, basta baixar a última disponível em [9] e descompactá-la.

O ClockingIT requer a instalação dos pacotes do *Git*, *MySQL*, *ImageMagick* e *Ruby*, assim como suas dependências:

```
sudo apt-get install mysql-server
➥ mysql-client libmysqlclient15-
➥dev git-core libmagick9-dev
➥ ruby1.8-dev rubygems ri rdoc rake
```

Após baixar o código-fonte, já podemos começar a configurar o ClockingIT. Para isso, basta entrar no diretório criado (`cit/`) e executar o script de configuração `setup.rb`, procedendo conforme o **exemplo 1**. É importante se certificar de que a URL exibida por último no script de configuração possa ser resolvida para o IP do servidor, seja por meio do servidor DNS local ou pelo arquivo `/etc/hosts`. Com o navegador apontado para esse endereço, é possível fazer o login com o usuário e a senha da conta de administrador e começar a usar o ClockingIT. Em caso de dúvidas ou problemas, os fóruns do ClockingIT[10] contam com a presença do criador do sistema, que adora ajudar os usuários do software. Outra possibilidade é recorrer ao email `support@clockingit.com`. ■

Exemplo 1: Script de configuração

```
$ cd cit
$ ruby ./setup.rb
Verifying dependencies...
Dependencies verified...
(...)
Enter MySQL database name for ClockingIT [cit]:
Enter username for ClockingIT MySQL account [cit]:
Enter password for ClockingIT MySQL account [cit]:
(...)
Enter domain ClockingIT will be accessed from (for example projects.
mycompany.com): linuxmagazine.com.br
(...)
Enter name of initial company: LinuxMagazine
Enter name of initial user: Administrador
Enter username for initial user: adm
Enter password for initial user: s3gr3d0
Enter password (again) for initial user: s3gr3d0
Enter email address of initial user: adm@linuxmagazine.com.br
(...)
Enter port for push server [443]: 1443
(...)
Initialize database schema [n]: y
(...)
All done!
(...)
Access your installation from http://linuxmagazine.com.br:3000
```

Mais informações

[1] ClockingIT: http://www.clockingit.com/

[2] "Criando um weblog em 15 minutos": http://www.rubyonrails.org/screencasts

[3] Juggernaut: http://juggernaut.rubyforge.org

[4] Garbage Collector: http://lloydforge.org/projects/ruby/

[5] Slim Attributes: http://slim-attributes.rubyforge.org/

[6] Ferret: http://ferret.davebalmain.com

[7] acts_as_ferret: http://projects.jkraemer.net/acts_as_ferret

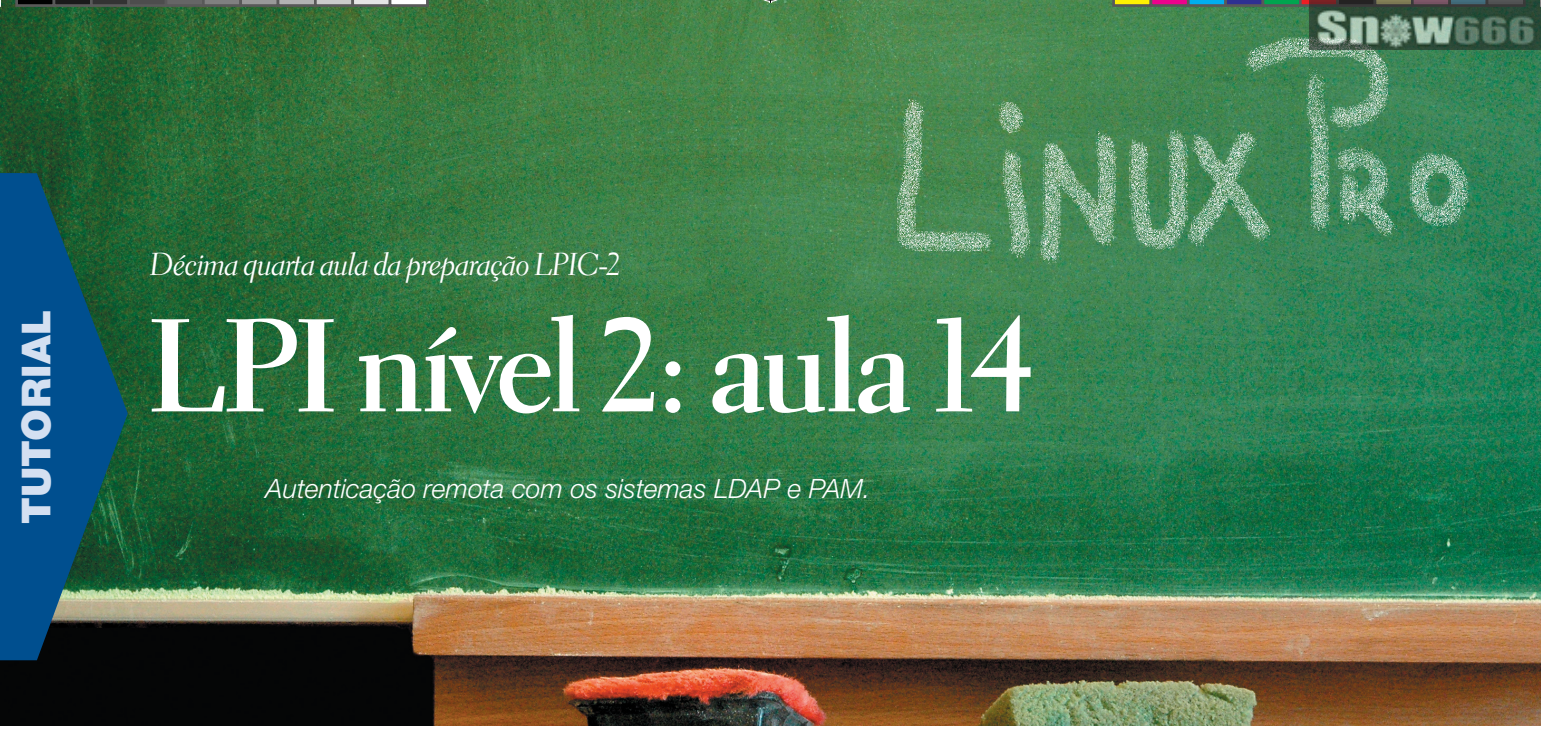
[8] Registro no ClockingIT: http://www.clockingit.com/signup

[9] Versões estáveis do ClockingIT: http://repo.clockingit.com/releases/

[10] Fóruns do ClockingIT: http://forum.clockingit.com

Sobre o autor

Erlend Simonsen é o criador e desenvolvedor do ClockingIT. O programador diz viver há 25 anos dentro de seu computador, saindo para o mundo quando sua família pede um pouco de atenção.



Décima quarta aula da preparação LPIC-2

LPI nível 2: aula 14

Autenticação remota com os sistemas LDAP e PAM.

Tópico 210: Administração de clientes da rede (continuação)

2.210.3 Configuração de LDAP

O LDAP (*Lightweight Directory Access Protocol*) é um protocolo utilizado para pesquisar e modificar serviços de diretório numa rede TCP/IP. Um diretório é um conjunto de informações – classes de objetos – com atributos e propriedades, organizadas de forma hierárquica e lógica, como num servidor DNS. Semelhante a um banco de dados, um serviço de diretório remoto fornece informações mediante um critério de solicitação. Porém, diferente de um banco de dados, um serviço de diretório é voltado para alta disponibilidade de leitura. Dados armazenados em um serviço de diretório são criados esporadicamente e pouco modificados. Uma utilização típica de um serviço de diretório é o armazenamento de contas de usuários. Neste caso, as informações ficam dentro de uma árvore hierárquica, na qual dados como departamento e empresa estão em níveis superiores, enquanto que dados pessoais, por exemplo, estão em níveis inferiores. Assim, um serviço de diretório pode substituir com vantagens o sistema clássico de contas de usuário em ambientes Unix.

A implementação do LDAP no Linux é o OpenLDAP. O daemon servidor do OpenLDAP é o `slapd`. A configuração do `slapd` é feita no arquivo `slapd.conf`, comumente localizado em `/etc/ldap/`.

O arquivo de configuração é dividido em três seções: global, funcionamento interno (*backend*) e configuração de banco de dados.

Configurando os servidores

Para ativar um servidor LDAP simples, poucas modificações precisam ser feitas no arquivo de configuração. O conteúdo do arquivo `slapd.conf` pode ser editado da seguinte forma:

```
include   /etc/ldap/schema/core.
➥schema
include   /etc/ldap/schema/cosine.
➥schema
include   /etc/ldap/schema/nis.schema
include   /etc/ldap/schema/
➥inetorgperson.schema
```

Incorpora os padrões de esquemas e definições de classes de objetos.

```
pidfile   /var/run/slapd/slapd.pid
```

Arquivo com o PID do processo servidor (`slapd`).

```
argsfile   /var/run/slapd/slapd.args
```

Arquivo contendo argumentos passados ao daemon.

```
backend          bdb
```

Define qual será o sistema de armazenamento de dados. Pode ser *bdb*, *config*, *dnssrv*, *hdb*, *ldap*, *ldbm*, *ldif*, *meta*, *monitor*, *null*, *passwd*, *perl*, *relay*, *shell* ou *sql*.

```
database         bdb
```

O início da seção de banco de dados deve ser correspondente a um valor definido numa entrada `backend`.

```
suffix   “o=lnm-br,c=BR”
```

O sufixo base para o diretório no banco de dados. A ordem é significante, os níveis são definidos da direita para a esquerda, do mais alto para o mais baixo.

```
rootdn   “cn=admin,o=lnm-➥br,c=BR”
```

Define o super-usuário (admin) para o banco de dados definido.

```
rootpw   {SSHA}rM7fwXjKoekcaVEKfBzn
➥+ovuGdr46Y3h
```

Exemplo 1: Arquivo LDIF simples

```
dn: o=lnm-br, c=BR
objectClass: organization
o: lnm-br
description: Editora Linux New Media do Brasil

dn: cn=Editor, o=lnm-br, c=BR
objectClass: person
cn: Editor
cn: Luciano Siqueira
sn: Siqueira
description: Editor Easy Linux
```

A senha pode ser digitada diretamente, mas é recomendável gerar uma senha criptografada, por meio do comando `slappasswd`.

Diretório onde serão armazenados os arquivos do banco de dados:

```
directory       "/var/lib/ldap"
```

Definição da indexação.

```
index           objectClass eq
```

Para testar a configuração, pode ser utilizado o comando `slaptest`:

```
# slaptest
config file testing succeeded
```

Feita a configuração, o daemon pode ser iniciado ou reiniciado. Provavelmente o `slapd` poderá ser executado por meio de um script de inicialização:

```
/etc/init.d/slapd start
```

Para verificar se o servidor está funcionando e respondendo, uma pesquisa simples é realizada com o comando `ldapsearch`, instalado por meio do pacote *ldapscripts*:

```
# ldapsearch -x -b '' -s base
➥'(objectclass=*)' namingContexts
(...)
dn:
namingContexts: o=lnm-br,c=BR
(...)
```

Arquivos LDIF

Outra diferença entre um diretório LDAP e bancos de dados é a maneira como os dados são gravados. Um diretório não possui uma interface de inserção como num banco de dados MySQL ou PostgreSQL. Em vez disso, o procedimento mais comum de inserção de dados num diretório LDAP é utilizar um arquivo LDIF (*LDAP Data Interchange Format*).

Basicamente, um arquivo LDIF contém os campos e valores necessários para fazer a inserção no diretório. Um exemplo de arquivo LDIF simples pode ser visto no **exemplo 1**.

Este arquivo define dois objetos: um da classe `organization` e outro da classe `person`. As siglas utilizadas representam propriedades dos objetos:

- `dn`: *distinguishedName*
- `o`: *organizationName*
- `c`: *country*
- `cn`: *commonName*
- `sn`: *surname*

Finalizada a edição do arquivo LDIF, os dados são incluídos no diretório com o comando `ldapadd`, no qual `exemplo.ldif` é o nome dado ao arquivo criado:

```
ldapadd -f exemplo.ldif -x -W -D
➥'cn=admin,o=lnm-br,c=BR'
```

A opção `-f` especifica o arquivo LDIF, `-x` indica autenticação simples (no lugar de SASL), com `-W` a senha será perguntada na seqüência e após `-D` são colocadas as informações do administrador do diretório, como configuradas em `slapd.conf`. São utilizadas aspas simples para evitar que o bash interprete algum caracter do trecho do comando.

A inclusão dos dados pode ser verificada com o comando `ldapsearch` mostrado no **exemplo 2**.

Grupos e usuários

Administração de usuários e grupos POSIX (padrão Unix) no LDAP é facilitada com as ferramentas do pacote LDAP scripts. Os principais comandos são:

- `ldapaddgroup`: Adiciona um grupo. Sua sintaxe é `ldapaddgroup <nome_do_grupo> [gid]`. Se não for fornecido um *gid*, este será gerado automaticamente;
- `ldapadduser`: Adiciona um usuário. Sua sintaxe é `ldapadduser <nome_do_usuário> <nome_do_grupo|gid> [uid]`. O nome do usuário e o nome do grupo/gid são obrigatórios. Se não for fornecido um *uid*. este será gerado automaticamente;
- `ldapaddusertogroup`: Inclui um usuário num grupo. Sua sintaxe é `ldapaddusertogroup <nome_do_usuário|uid> <nome_do_grupo|gid>`;
- `ldapaddmachine`: Cria uma conta de máquina. Sintaxe: `ldapaddmachine <nome$> <nome_do_grupo|gid> [uid]`;
- `ldapdeletegroup`, `ldapdeleteuser`: Remove um grupo ou um usuário;
- `ldapdeleteuserfromgroup`: Exclui um usuário de um grupo. Sintaxe: `ldapdeleteuserfromgroup <usuário> <nome_do_grupo|gid>`;
- `ldappasswd`: Altera a senha de um item no diretório LDAP. Sua utilização é semelhante à utilização do comando `passwd`.

2.210.4 Autenticação por PAM

PAM, ou *Pluggable Authentication Modules*, pode ser entendido como uma camada de abstração de autenticação de usuários. Dessa forma, diferentes programas e serviços podem autenticar usuários por meio de diferentes modelos de senhas e criptografias, sem necessidade de lidar com os meandros de funcionamento interno de cada um deles. O procedimento de autenticação é delegado ao PAM, que se encarregará de fazer os procedimentos necessários.

Grande parte das distribuições possui suporte a PAM. A instalação do PAM em uma distribuição que não possui suporte nativo é um processo pouco utilizado, pois envolve inúmeras adaptações no sistema, o que a torna pouco aconselhável. Portanto, assume-se aqui que a distribuição utilizada possua suporte nativo a PAM.

Exemplo 2: Comando ldapsearch

```
# ldapsearch -x -b 'o=lnm-br,c=BR'
➥'(objectclass=*)'
# extended LDIF
#
# LDAPv3
# base <o=lnm-br,c=BR> with scope
➥subtree
# filter: (objectclass=*)
# requesting: ALL
#

# lnm-br, BR
dn: o=lnm-br,c=BR
objectClass: organization
o: lnm-br
description: Editora Linux New Media do
➥Brasil

# Editor, lnm-br, BR
dn: cn=Editor,o=lnm-br,c=BR
objectClass: person
cn: Editor
cn: Luciano Siqueira
sn: Siqueira
description: Editor Easy Linux

# search result
search: 2
result: 0 Success

# numResponses: 3
# numEntries: 2
```

Exemplo 3: Diretório /etc/pam.d/

```
# ls -ll /etc/pam.d/
total 27
-rw-r--r-- 1 root root  182 2006-
01-03 05:15 atd
-rw-r--r-- 1 root root  384 2007-02-27 04:27 chfn
-rw-r--r-- 1 root root  581 2007-02-27 04:27 chsh
-rw-r--r-- 1 root root  392 2007-05-10 18:48 common-account
-rw-r--r-- 1 root root  436 2007-05-10 18:48 common-auth
-rw-r--r-- 1 root root 1097 2007-05-10 18:48 common-password
-rw-r--r-- 1 root root  372 2007-05-10 18:48 common-session
-rw-r--r-- 1 root root  289 2005-10-14 09:00 cron
-rw-r--r-- 1 root root   69 2007-02-02 11:18 cupsys
-rw-r--r-- 1 root root  263 2006-12-15 06:16 gdm
-rw-r--r-- 1 root root  270 2006-12-16 09:24 gdm-autologin
-rw-r--r-- 1 root root   21 2006-11-24 18:43 gnome-screensaver
-rw-r--r-- 1 root root 2843 2007-02-27 04:27 login
-rw-r--r-- 1 root root   38 2007-03-07 19:30 newrole
-rw-r--r-- 1 root root  520 2003-08-31 19:21 other
-rw-r--r-- 1 root root   92 2007-02-27 04:27 passwd
-rw-r--r-- 1 root root  168 2007-03-17 19:52 ppp
-rw-r--r-- 1 root root   38 2007-03-07 19:30 run_init
-rw-r--r-- 1 root root 1272 2007-03-05 13:36 ssh
-rw-r--r-- 1 root root 2305 2007-02-27 04:27 su
-rw-r--r-- 1 root root   56 2006-04-15 04:39 sudo
```

Configuração

Cada programa ou serviço que utiliza autenticação possui uma configuração individual no PAM. Existem duas possibilidades para a localização destes arquivos de configuração. Toda a configuração pode ser feita no arquivo `/etc/pam.conf` ou em arquivos individuais, no diretório `/etc/pam.d`.

O mais comum é que a configuração seja feita em arquivos individuais no diretório `/etc/pam.d`. Para cada serviço ou programa que utiliza autenticação via PAM, existe um arquivo que leva o nome do programa ou do serviço e é responsável por sua configuração. O conteúdo de `/etc/pam.d` varia conforme os serviços e programas instalados no sistema e quais deles utilizam PAM.

Conteúdo típico de `/etc/pam.d/` é exibido no **exemplo 3**.

A sintaxe interna de cada um dos arquivos de configuração é a mesma:

```
tipo controle módulo argumentos
```

Explicação dos termos:

`tipo`

Define o tipo de autenticação usado para o módulo. Módulos do mesmo tipo podem ser interligados, exigindo que a autenticação responda a vários critérios. Os tipos podem ser:

- `account`: verifica se o usuário pode acessar o serviço, se a senha não expirou etc.;
- `auth`: determina a autenticidade do usuário, geralmente via senha, mas pode utilizar outros meios, como biometria;
- `password`: mecanismo de alteração da autenticação (provavelmente a senha);
- `session`: procedimentos que devem ser realizados antes e depois que o usuário foi autenticado. Por exemplo, podem ser realizados a montagem/desmontagem do diretório pessoal ou restrição de serviços ao usuário.

`controle`

Especifica o que fazer caso a autenticação para o módulo falhe. Pode ser:

LINUX MAGAZINE ONLINE

CÓDIGO ABERTO PARA PROFISSIONAIS

www.linuxmagazine.com.br

O site da Linux Magazine está com novo visual e mais recursos. Além de reunir, em formato digital e de forma organizada, todo o conteúdo dos materiais da Linux New Media, o site oferece notícias em primeira mão e com a melhor cobertura na Web brasileira do cenário do Software Livre e de Código Aberto.

LINUX NEW MEDIA
The Pulse of Open Source

- `requisite`: autenticação é imediatamente negada;
- `required`: nega a autenticação, mas consultará os outros módulos para o serviço antes de negar completamente a autenticação;
- `sufficient`: se a autenticação para este módulo for bem sucedida, a autenticação será confirmada mesmo que módulos anteriores tenham negado a autenticação;
- `optional`: a aprovação ou negação neste módulo só fará diferença se for o único do tipo para o serviço.

`módulo`

Indica qual módulo utilizar e opcionalmente onde encontrá-lo. Se não for informada a localização, o PAM procurará no diretório padrão, `/lib/security` ou `/usr/lib/security`.

`argumentos`

Parâmetros opcionais. Representa os argumentos passados para o módulo. Cada módulo tem seus próprios argumentos.

Como exemplo, tomemos o conteúdo do arquivo `login` que pode ser visto no **exemplo 4**.

Caso as configurações do PAM no seu sistema sejam feitas inteiramente no arquivo `pam.conf`, as entradas serão um pouco diferentes. O nome do respectivo serviço deve ser incluído como primeiro termo para cada entrada. Por exemplo, entrada em `/etc/pam.d/login`:

```
auth  requisite  pam_securetty.so
```

Em `/etc/pam.conf`, é escrita da seguinte forma:

```
login  auth  requisite  pam_
➥securetty.so
```

```
auth    sufficient pam_ldap.so
➥auth    required   pam_unix.so
try_first_pass
account sufficient pam_ldap.so
account required   pam_unix.so
```

Exemplo 4: Arquivo login

```
# Bloqueia login de root, exceto
# em tty's listados em /etc/securetty
auth       requisite  pam_securetty.so

# Bloqueia login de usuários deferentes de root,
# caso o arquivo /etc/nologin exista
auth       requisite  pam_nologin.so

# Lê /etc/environment. Exige o argumento "readenv=1"
session       required   pam_env.so readenv=1

# Opções padrão de autenticação Un*x.
@include common-auth

# Configura limtes de usuário definidos em /etc/security/limits.conf
session    required   pam_limits.so

# Prints the last login info upon succesful login
# (Replaces the `LASTLOG_ENAB' option from login.defs)
session    optional   pam_lastlog.so

# Mostra a motd após um login bem sucedido
session    optional   pam_motd.so

# Padrões Un*x para contas e sessões
@include common-account
@include common-session
@include common-password
```

NIS e LDAP

A configuração do PAM para utilizar autenticação NIS ou LDAP requer módulos específicos, respectivamente `pam_nis.so` e `pam_ldap.so`.

Para que o login faça autenticação via NIS, o arquivo `/etc/pam.d/login` deve ser editado conforme o **exemplo 5**.

Para que o login faça autenticação via LDAP, o arquivo `/etc/pam.d/login` deve ser editado da seguinte forma:

Considerações sobre o tópico

A configuração básica de um servidor DCHP, como determinar um segmento de IPs oferecidos ou um IP específico relacionado ao endereço MAC (conforme visto na LM44), são todos os tópicos que serão exigidos.

A abordagem ao NIS, LDAP e PAM é ampla. Portanto, conheça bem os principais conceitos, arquivos e comandos por eles utilizados. ■

Exemplo 5: Arquivo /etc/pam.d/login

```
auth    sufficient pam_nis.so item=user sense=allow \
 map=users.byname value=compsci
auth    required   pam_unix.so try_first_pass
account sufficient pam_ldap.so item=user sense=deny \
 map=cancelled.byname error=expired
account required   pam_unix.so
```


Sobre o autor

Luciano Antonio Siqueira é editor e desenvolvedor da Linux New Media do Brasil. Escreveu os livros Certificação LPI-1, Certificação LPI-2 e outros títulos. Trabalha com Linux há mais de dez anos e é formado em psicologia pela Universidade Estadual Paulista.

Guia de TI

Soluções em Tecnologias Abertas

LINUX NEW MEDIA
The Pulse of Open Source

Garanta já sua vaga para o Guia de TI 2009!

Cadastre-se agora e apareça gratuitamente na maior e mais completa lista de empresas que oferecem soluções de TI baseadas em tecnologias abertas.

Cadastre a sua solução gratuitamente!
www.guiadeti.com.br

Cadastre-se:
11 4082-1300
guiadeti@linuxnewmedia.com.br

Publicidade:
11 4082-1300
anuncios@linuxnewmedia.com.br

TUTORIAL

Um servidor de alta disponibilidade para aplicações Ruby on Rails

Cluster nos trilhos

O desenvolvimento de aplicações web com Ruby on Rails é bem ágil, mas isso não significa baixo desempenho.

por Marcos Miras

A linguagem *Ruby*, que surgiu na mesma época que o Java, foi desenvolvido pelo japonês Yukishiro Matsumoto, também conhecido como Matz. Matsumoto decidiu, em meados em 1993, criar uma linguagem de programação que resolvesse suas próprias frustrações. O Ruby traz algumas inspirações com referências a outras linguagens populares, principalmente *Perl*, *SmallTalk* e *Python*. Na virada do milênio, a linguagem se aproximou do ocidente e conquistou diversos programadores.

Em paralelo, o dinamarquês David Heinemeier-Hansson, que estava desenvolvendo uma nova ferramenta web para gerenciamento de projetos, resolveu que ela seria produzida em Ruby. Foi a partir deste projeto que David elaborou o *framework* batizado como *Rails*.

O framework

Com o Rails, David trouxe o conceito *DRY* "Don't Repeat Yourself" ("não se repita") e "Convention over Configuration" ("Convenção é preferível a configuração"). O Rails não é uma nova tecnologia, mas apenas um pacote muito organizado. Não é um substituto para o *J2EE*, e sim mais uma alternativa. Quando se fala em Rails, não se fala de "alta tolerância a falhas" ou de outros grandes quesitos do J2EE, mas em desenvolver aplicações web com a programação ágil que ouvimos falar com relação à técnica de *Extreme Programming*. Já na maioria dos projetos J2EE, a promessa de agilidade demora a chegar.

Um fato muito interessante é que as ferramentas desenvolvidas em *Ruby on Rails* podem interagir com *Ajax*, *Flex* e outras ferramentas que trazem as facilidades do desktop para a web.

Muitos programadores têm adotado o Ruby on Rails como plataforma de desenvolvimento, já que, para adotar o *Java*, precisam empregar diversas ferramentas, como *Struts*, *Hibernate*, *Tomcat* etc.

Objetivo

O Ruby on Rails é uma plataforma livre. Logo, quem o adota, preferencialmente utilizará Linux. Este artigo tem o objetivo de mostrar como instalar, configurar e administrar um servidor de produção independente da sua distribuição.

Ruby on Linux

Para que seja possível ter um servidor de produção de alta disponibilidade para aplicações Ruby on Rails, são necessários alguns softwares instalados no sistema:

- Ruby;
- Gem;
- Rails;
- Mongrel;
- Mongrel Cluster;
- Apache;
- banco de dados;

A seguir, veremos a instalação, a configuração e a funcionalidade de cada um. Evidentemente, é fundamental que o servidor tenha as aplicações essenciais para compilação, como o compilador GCC e as *Autotools*, entre outros.

Ruby

O Ruby é o interpretador da linguagem que será responsável pela compilação dos pacotes *Gem*, *Mongrel*, *Mongrel Cluster*, *Rails* e outras funcionalidade destes.

Geralmente as distribuições trazem o Ruby entre suas ferramentas de programação. É necessária a desinstalação desse pacote para instalar a última versão do interpretador.

Após a desinstalação, pode-se baixar a última versão do Ruby (1.8.6, no momento da escrita deste artigo) em [1], descompactá-la e compilá-la:

```
# cd ruby-1.9.6
# ./configure
# make & make install
```

Após compilado, verifique se o Ruby está funcionando no servidor, criando um arquivo de nome `teste.rb` com o conteúdo de acordo com o **exemplo 1**. Após a sua execução (`ruby teste.rb`), deverá aparecer a mensagem `Teste do Ruby`, caso a instalação tenha funcionado.

Exemplo 1: Arquivo teste.rb

```
#!/usr/bin/ruby
puts "Teste do Ruby"
```

Gem

As distribuições têm diversos gerenciadores de pacotes, como *Apt* e *Yum*, por exemplo. O Ruby também possui um próprio, o Gem, cuja função é semelhante à dos demais gerenciadores, embora com um repositório restrito a aplicações que tenham interação com o Ruby on Rails.

Para instalar o Gem, baixe sua versão mais recente (1.1.1, na escrita deste artigo), descompacte-a e execute-a por meio do interpretador Ruby (o pacote é feito, ele próprio, em Ruby):

```
# wget http://rubyforge.org/frs/
➥download.php/35283/rubygems-
➥1.1.1.tgz
# tar zxvf rubygems-1.1.1.tgz
# cd rubygems-1.1.1
# ruby setup.rb
```

Rails

O Rails é o framework responsável por criar a aplicação e controlar os módulos *Active Record*, *Action View*, *Action WebServices*, *Action Mailer*, *Active Support* e *Action Pack*, como mostra a **figura 1**.

No caso do Rails, não será necessário fazer o download do código-fonte, pois o instalaremos a partir do Gem:

```
gem install rails
```

É importante lembrar-se de que o Gem sempre fará o download da última versão do software requisitado. Portanto, procure sempre saber com o desenvolvedor qual versão do Rails foi utilizada para o desenvolvimento da aplicação. Se for necessária uma versão diferente da mais recente, é possível especificar o número com o parâmetro `-v`.

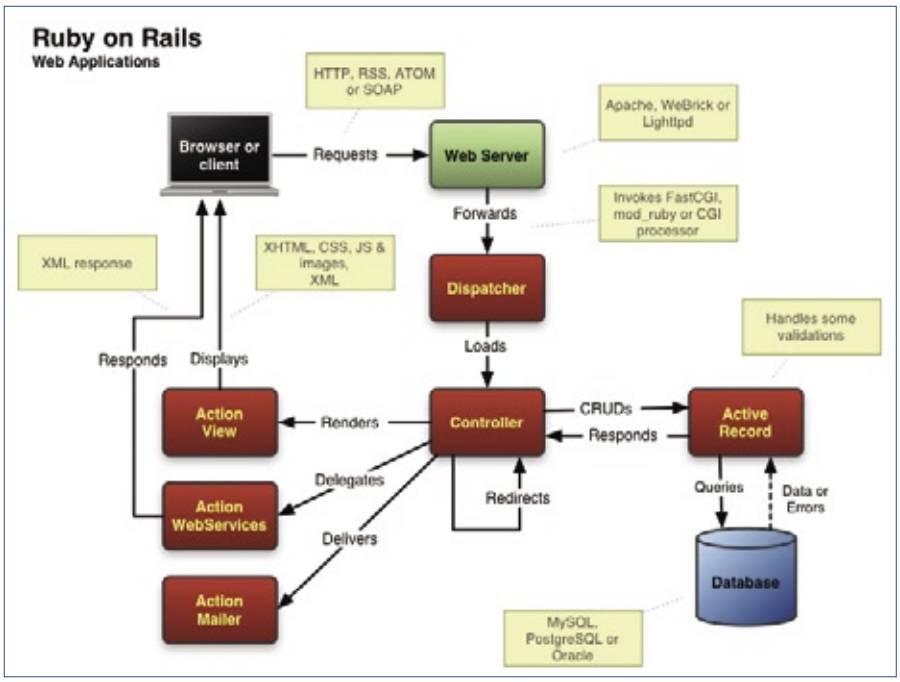


Figura 1 Arquitetura do *framework Rails*.

```
# gem install rails -v1.2.6
```

Ao instalar o Rails, serão instalados os seguintes pacotes:

- *Rake*, ou *Ruby Make*: uma série de scripts para configuração, instalação e limpeza, com finalidade semelhante à do popular *make*;
- *ActiveSupport*: responsável por recursos avançados, como *breakpoints*, cache, logs, plugins e outros;
- *ActiveRecord*: responsável pela integração com a base de dados, sua função lembra a do Hibernate do Java;
- *ActionPack*: responsável por controlar os componentes MVC (*Model*, *View*, *Controller*);
- *ActionMailer*: responsável por enviar e receber emails a partir da aplicação;
- *ActionWebService*: responsável pela integração entre sistemas;
- *Rails*: o componente de framework propriamente dito.

Banco de dados

Com aplicações Ruby on Rails, é possível usar vários bancos de dados, como *Oracle*, *PostgreSQL* e *MySQL*, entre outros. Porém, para concluir a instalação neste artigo, utilizaremos o MySQL por ser muito familiar para programadores voltados à Web.

O MySQL também será instalado a partir do Gem, com um simples:

```
# gem install mysql
```

Concluída a instalação, será preciso iniciar o MySQL e especificar a senha de root:

```
# mysqladmin -u root password
➥ 'senha_de_root'
```

Em seguida, entre no MySQL e crie os bancos de dados necessários para a aplicação:

```
# mysql -p
mysql> create database minhaapp_
➥production;
mysql> create database minhaapp_
➥development;
```

Obviamente, o termo `minhaapp` deve ser substituído por um que faça sentido para o uso do desenvolvedor.

Exemplo 2: Criação de senhas no MySQL

```
mysql> use minhaapp_
➥production;
mysql> grant all privileges
➥ on *.* to user@'localhost'
➥ identified by 'senha_
➥secreta';
mysql> flush privileges;
mysql> use minhaapp;
mysql> grant all privileges
➥ on *.* to user@'localhost'
➥ identified by 'senha_
➥secreta';
mysql> flush privileges;
mysql> quit
```

Ainda no MySQL, entre na nova base de dados e insira um usuário e uma senha para manipulação específica dos novos bancos de dados `minhaapp` (**exemplo 2**).

Feito isso, o banco de dados estará instalado e configurado, pronto para podermos testar a aplicação.

Primeiro teste

Para começarmos a usar a aplicação, primeiramente vamos precisar copiar o projeto para o diretório `/opt/` no servidor (pode-se usar qualquer outro diretório).

Caso ainda não exista uma aplicação, será possível criar um projeto Rails de teste com `rails /opt/minhaapp`. Em seguida, abra o arquivo `/opt/minhaapp/config/database.yml` e configure-o conforme o **exemplo 3**.

Exemplo 3: Arquivo database.yml

```
development:
    adapter: mysql
    database: minhaapp_development
    username: user
    password: senha_user
    host: localhost
    socket: /var/lib/mysql/mysql.sock

production:
    adapter: mysql
    database: minhaap_production
    username: user
    password: senha_user
    host: localhost
    socket: /var/lib/mysql/mysql.sock
```

Após a configuração da aplicação, vamos construir o banco segundo o desenvolvimento desta. É nesse momento que utilizaremos a ferramenta Rake:

```
# cd /opt/minhaapp
# rake db:migrate
```

Feito isso, já será possível executar sua aplicação com o *Webrick* (servidor para ambiente de desenvolvimento) e verificar suas funcionalidades junto ao banco de dados:

```
# ruby script/server
```

Em seguida, abra o navegador e acesse o endereço `http://localhost:3000` (**figura 2**).

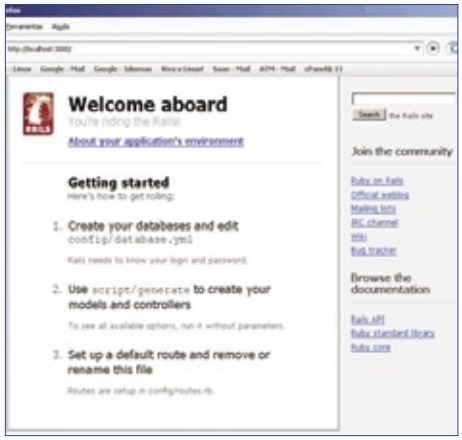


Figura 2 Página de apresentação do *Rails*.

Mongrel Cluster e Apache

Na parte final deste tutorial, vamos incluir o Mongrel como servidor para a aplicação Rails.

Pressione **[Ctrl]+[C]** no terminal para que o Webrick seja abortado. Depois disso, instalaremos o Mongrel e o Mongrel_Cluster:

```
# useradd mongrel
# gem install mongrel
# gem install mongrel_cluster
```

Instalados os pacotes necessários, criaremos a configuração do Mongrel Cluster:

```
# mongrel_rails cluster::configure
➥ -e production -p 9000 -a
➥ 127.0.0.1 -N 5 -c /opt/minhaapp
```

Os parâmetros utilizados têm os seguintes significados:

- `-e`: define se a aplicação está em produção ou em desenvolvimento;
- `-p`: determina a porta de comunicação em uso;
- `-a`: indica a máquina na qual está localizada a aplicação;
- `-N`: determina o número de instâncias do Rails;
- `-c`: local onde está sua aplicação.

Em seguida, vamos criar a pasta de configuração do Mongrel e adicionar a ela o arquivo de configuração criado anteriormente:

```
# mkdir /etc/mongrel_cluster
# ln -s /opt/minhaapp/config/
➥mongrel_cluster.yml /etc/
➥mongrel_cluster/minhaapp.yml
```

Com isso, o Mongrel está instalado e configurado. Chega a vez de instalarmos o poderoso servidor web Apache e habilitarmos o módulo `mod_proxy_balancer` (**exemplo 4**).

É necessário também editar o

Exemplo 4: Instalação do Apache

```
# wget http://apache.rmplc.
➥co.uk/httpd/httpd-2.2.6.tar.gz
# tar zxvf httpd-2.2.6.tar.gz
# cd httpd-2.2.6/
#./configure -prefix=/usr/local/
➥apache2 -enable-mods-shared=all
➥ -enable-deflate -enable-proxy
➥ -enable-proxy-balancer
➥ -enable-proxy-http
# make & make install
```

Exemplo 5: Arquivo httpd.conf

```
LoadModule proxy_module  modules/mod_proxy.so
LoadModule proxy_balancer_module modules/mod_proxy_balancer.so
LoadModule proxy_http_module  modules/mod_proxy_http.so
```

Exemplo 6: Configuração de hosts virtuais do Apache

```
01 <VirtualHost *>
02   ServerName minhaapp
03   ErrorLog /opt/minhaapp/log/errors.log
04   CustomLog /opt/minhaapp/log/apache.log combined
05
06   <Directory “/opt/minhaapp/public/”>
07     Options FollowSymLinks
08     AllowOverride None
09     Order allow,deny
10     Allow from all
11   </Directory>
12
13   RewriteEngine On
14
15   # Check for maintenance file and redirect all requests
16   #  ( this is for use with Capistrano’s disable_web task )
17   RewriteCond %{DOCUMENT_ROOT}/system/maintenance.html -f
18   RewriteCond %{SCRIPT_FILENAME} !maintenance.html
19   RewriteRule ^.*$ /system/maintenance.html [L]
20
21   # Rewrite index to check for static
22   RewriteRule ^/$ /index.html [QSA]
23
24   # Rewrite to check for Rails cached page
25   RewriteRule ^([^.]+)$ $1.html [QSA]
26
27   # Redirect all non-static requests to cluster
28   RewriteCond %{DOCUMENT_ROOT}/%{REQUEST_FILENAME} !-f
29   RewriteRule ^/(.*)$ balancer://mongrel_cluster%{REQUEST_URI}
➥[P,QSA,L]
30
31   # Deflate
32   AddOutputFilterByType DEFLATE text/html text/plain text/css
33   # ... text/xml application/xml application/xhtml+xml text/
➥javascript
34   BrowserMatch ^Mozilla/4 gzip-only-text/html
35   BrowserMatch ^Mozilla/4.0[678] no-gzip
36   BrowserMatch \bMSIE !no-gzip !gzip-only-text/html
37
38   <Proxy *>
39     Order allow,deny
40     Allow from all
41   </Proxy>
42
43   <Proxy balancer://mongrel_cluster>
44 # Irá variar de acordo com o número de instâncias desejadas na
➥configuração do mongrel cluster
45     BalancerMember http://127.0.0.1:9000
46     BalancerMember http://127.0.0.1:9001
47     BalancerMember http://127.0.0.1:9002
48     BalancerMember http://127.0.0.1:9003
49     BalancerMember http://127.0.0.1:9004
50   </Proxy>
51
52 </VirtualHost>
```

arquivo de configuração do Apache para habilitar os módulos de proxy:

```
# ln -s /usr/local/apache2/modules
➥ /usr/local/apache2/conf/modules
```

e acrescentar ao arquivo `httpd.conf` as linhas do **exemplo 5** na seção de configuração dos módulos do Apache.

No mesmo arquivo de configuração, criaremos um *host* virtual para acessar as instâncias do Mongrel Cluster, adicionando os parâmetros do **exemplo 6** ao final do arquivo.

Como o binário `mongrel_cluster` se encontra num longo caminho de diretório, é útil criar um link simbólico para ele num diretório mais próximo da raiz.

Feito isso, basta iniciar a aplicação após o Apache:

```
# /usr/local/apache2/bin/apachectl
➥ start
# /opt/minhaapp/mongrel_cluster
➥ start
```

Conclusão

O intuito deste artigo é mostrar aos administradores Linux que o Ruby on Rails é uma tecnologia que está se aproximando de diversas empresas e desenvolvedores. Para aproveitá-la, é necessário estar apto a instalá-la em diferentes cenários. ■

Mais informações

[1] Download do Ruby: http://ftp.ruby-lang.org/pub/ruby/1.8/ruby-1.8.6.tar.gz

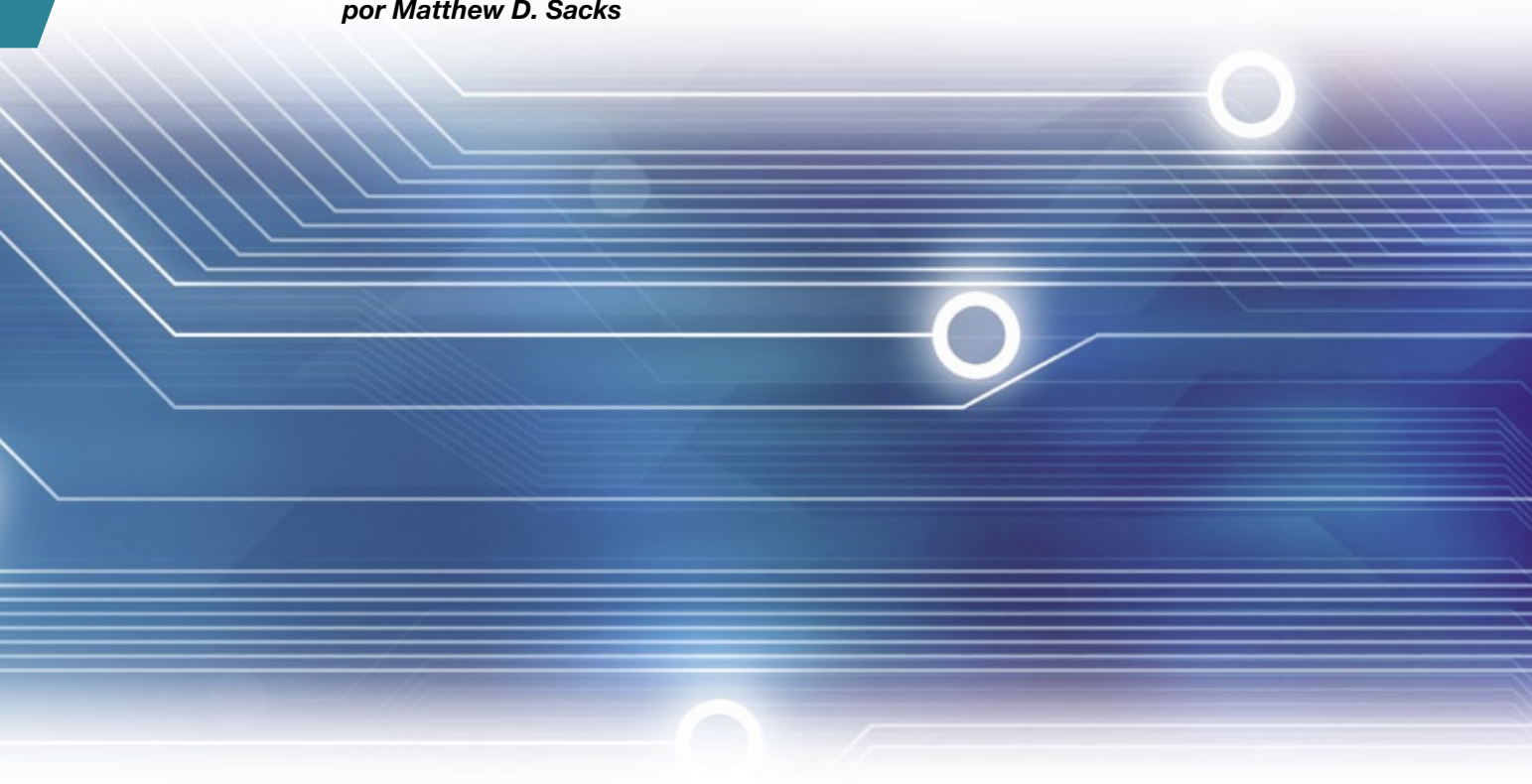
Sobre o autor

Marcos Miras (marcosmiras@atmsystem.com.br) é tecnólogo em redes de computadores e trabalha como administrador de redes da ATM System Sistemas e Internet, com foco em migração de ambientes Windows para Linux.

Imagem é tudo

O MRTG gera gráficos simples para visualização rápida do desempenho da rede.

por Matthew D. Sacks



Administradores Linux freqüentemente se beneficiam da captura de métricas do desempenho do sistema, como uso de disco, da CPU e da memória. Um gráfico de desempenho útil ajuda a diagnosticar problemas e a analisar questões de tráfego.

O *Multi-Router Traffic Grapher* (MRTG[1]) permite a coleta e a criação de gráficos de rede e dados de desempenho de máquinas Linux. O MRTG é uma ferramenta de código aberto que coleta e exibe estatísticas a partir de dispositivos de rede com base no protocolo SNMP.

Ferramentas comerciais como o *HP OpenView* ou o *IBM Tivoli*, assim como utilitários de código aberto como *Cacti*[2] e *Zenoss* (uma versão mais polpuda do MRTG), têm usos semelhantes, mas é difícil ultrapassar o nível do MRTG.

Instalação

Instalar o MRTG e o SNMP não é para os fracos de coração, principalmente quando se opta por compilar todos os pacotes necessários a partir dos fontes. É importante verificar se há pacotes do MRTG disponíveis nos repositórios da sua distribuição e, em caso negativo, o código-fonte está disponível no site do criador do programa, Tobi Oetiker[1].

SNMP

O SNMP é o protocolo por trás das imagens mágicas criadas pelo MRTG. Este artigo presume que o leitor tenha algum conhecimento básico do SNMP. Porém se não

Quadro 1: Pré-requisitos do MRTG

Para instalar o MRTG a partir de seu código-fonte, primeiramente é necessário fornecer os softwares dos quais ele depende:

- GCC: Como o programa é feito primariamente em *C*, o compilador[4] é necessário.
- Perl: Além de C, grandes partes do MRTG são escritas em *Perl*. É importante ter instalada no seu sistema uma versão recente do Perl (`perl -v` mostra a versão instalada). A versão 5.005 é a menor possível para usar o MRTG com sucesso. Se for usado o SNMPv3 e outros novos recursos, é preciso ao menos a versão 5.8.
- GD: A biblioteca *GD* para gerar desenhos foi criada por Thomas Boutell[5]. Todas as versões após a 1.3 criam somente imagens PNG. Thomas enfrentou problemas em razão do uso do formato GIF, que utiliza uma tecnologia de compressão patenteada pela Unisys. O MRTG é capaz de usar versões novas ou velhas da biblioteca GD.
- Libpng: A biblioteca GD exige essa biblioteca para conseguir produzir imagens PNG[6].
- Zlib: A biblioteca Zlib é necessária para que a Libpng consiga comprimir os arquivos de imagens gerados[7].

Exemplo 1: Problemas de configuração do MRTG

```
01 ** Ooops, one of many bad things happened:
02
03 a) You don't have the GD library installed.
04 Get it from http://www.boutell.com, compile it, and
05 use either --with-gd-lib=DIR or --with-gd-inc=DIR to specify
06 its location. You might also have to use --with-z-inc,
07 --with-z-lib and --with-png-inc, --with-png-lib for gd
08 versions 1.6 and higher. Check config.log for more
09 information on the problem.
10
11 b) You have the GD library installed, but not the gd.h
12 header file. Download the source (see above) and use
13 --with-gd-inc=DIR to specify where the file can be found.
14
15 c) You have the library and the header file installed, but
16 you also have a shared GD library in the same directory.
17 Remove the shared library files and/or links (e.g.,
18 libgd.so.2.0.0, libgd.so and libgd.so.2). This is especially
19 likely if you're using a recent (post 1.8.4) version of GD
20 and didn't configure it with --disable-shared.
21
22 d) You have the GD library installed and also its headers, butyou are
23 missing libpng (and headers) or freetype (and headers)
24 (MRTG does not use freetype, but if your copy of GD isprecompiled
25 against it, you have to install it ... )
```

for o seu caso, há muitas informações disponíveis na Internet sobre esse protocolo um tanto antigo, mas incrivelmente poderoso. Para mais informações sobre como configurar o SNMP em máquinas Linux, [3] é um bom ponto de partida.

Instalação

O **quadro 1** dá mais informações sobre os componentes necessários para o MRTG. Uma vez que estes estejam instalados, basta baixar o código-fonte em [1].

O comando `./configure, a opção --prefix` pode ser usado da seguinte forma para fazer a instalação de forma a facilitar futuras atualizações do software:

```
./configure --prefix=/usr/local/
➥mrtg-2.15.2
```

A criação de um link simbólico também é interessante para facilitar o uso da versão mais recente após uma atualização:

```
ln -s /usr/local/mrtg-2.15.2 /usr/
➥local/mrtg
```

Se o script de configuração do MRTG não conseguir encontrar alguma dependência, ele pode emitir uma mensagem de erro semelhante àquela do **exemplo 1**. Nesse caso, o ideal é sempre usar as versões mais recentes das bibliotecas usadas pelo MRTG, o que garantirá uma operação sem falhas.

Configuração

Se houver alguma dependência de biblioteca compilada a partir do código-fonte, será necessário modificar os parâmetros do script de configuração para incluí-las. Por exemplo, se for o caso da biblioteca gráfica *GD*, deve-se modificar o script de configuração da seguinte forma:

Tabela 1: Opções do comando cfgmaker

Opção	Descrição
`community`	Define o nome da comunidade SNMP.
`global`	Define os parâmetros globais de configuração para cada máquina configurada.
`Workdir`	Diretório onde as imagens e arquivos HTML devem ser criados.
`output`	Define onde o arquivo de configuração do MRTG será criado. Adicione os nomes de máquinas ou os IPs dos servidores a serem monitorados no fim do script `cfgmaker` separados por espaços. Em nosso caso, temos apenas uma máquina: *Tux*.

```
./configure --prefix=/usr/local/
➥mrtg-2.15 --with-gd-lib=/usr/
➥local/gd-2.0.34 --with-gd-inc=/
➥usr/local/gd-2.0.34/lib
make
make install
```

Modificação para desempenho

Este artigo utilizará duas máquinas Linux como exemplos: Tux e Grapher. A primeira é o servidor que será monitorado e o segundo é a máquina que executará o MRTG.

Os arquivos de configuração do MRTG são complexos e trabalhosos para editar, motivo pelo qual o MRTG traz um script de configuração fácil de usar, como o `cfgmaker`, que oferece várias opções. Ele cria o arquivo `mrtg.conf` com os dados necessários à geração de gráficos básicos. Os argumentos mais básicos de sua linha de comando são mostrados na **tabela 1**. Antes de executar o script, é importante criar um diretório para abrigar os arquivos de configuração do MRTG, pois é possível usar inúmeras configurações diferentes numa única máquina:

```
mkdir /usr/local/mrtg/cfg
```

O script `cfgmaker` deve ser executado da seguinte forma:

```
/usr/local/mrtg/bin/cfgmaker
➥--community=public --global
➥ Options[_]:growright,avgpeak,pri
➥ntrouter --global Workdir:/usr/
➥loca/apache2/htdocs --output=
➥/usr/local/mrtg/cfg/mrtg2.cfg Tux
```

Como já explicado, o MRTG recebe suas informações pelo protocolo SNMP. Esse protocolo organiza as informações de endereçamento de dispositivos numa estrutura hierárquica conhecida como *Management Information Base* (MIB). O exemplo a seguir presume que o MIB UCD-SNMP esteja carregado e que os dados possam ser consultados com o uso dessa definição de MIB. Para testar se o MIB UCD-SNMP está disponível e carregado, é necessário verificar a instalação do SNMP.

Teste do MIB

Uma forma rápida de testar se o MIB UCD-SNMP está disponível consiste em usar o seguinte comando no servidor monitorado:

```
snmpwalk -v1 -c public hostname
➥ ssCpuRawUser
```

Esse comando consulta o uso da CPU em relação ao tempo do usuário na máquina-alvo.

Se esse comando falhar, deve-se verificar se o *snmpd* na máquina monitorada está em execução e se o MIB UCD-SNMP foi compilado na instância do SNMP. A possibilidade de gerar gráficos do desempenho do servidor Linux depende fortemente desse MIB.

Monitor de CPU

Agora que o arquivo `mrtg2.cfg` padrão já foi gerado pelo script `cfgmaker`, é necessário editar manualmente esse arquivo de configuração para gerar gráficos das estatísticas de recursos como memória, disco e uso da CPU.

O site do MRTG possui ótima documentação cobrindo todos os diferentes parâmetros para configuração do programa.

Esse exemplo descreve como criar um modelo bem simples para criar gráficos do uso da CPU.

O MIB UCD-SNMP permite o monitoramento de uma grande variedade de configurações extras de desempenho. Para ver tudo que está disponível, a definição do MIB[8] é de grande ajuda.

Para adicionar um parâmetro como uso da CPU à configuração do MRTG, deve-se começar pela criação dos seguintes diretórios para abrigarem as novas configurações personalizadas:

```
mkdir /etc/mrtg
➥mkdir /etc/cron.mrtg
```

Depois, crie um arquivo `cpu.cfg` para monitorar a carga da CPU usando o conteúdo mostrado no **exemplo 2**. Crie um arquivo de *cron job* para o monitoramento da CPU com o seguinte conteúdo:

```
#!/bin/sh
env LANG=C /usr/local/mrtg/bin/
mrtg /etc/mrtg/cpu.cfg
```

Após tornar executável o comando para obtenção de dados da CPU, execute-o aproximadamente três vezes:

```
chmod +x /etc/cron.mrtg/cpu
sh /etc/cron.mrtg/cpu
```

Para visualizar os resultados, crie o arquivo de índice utilizando o script `indexmaker`:

```
indexmaker --output=/usr/local/
➥apache2/htdocs/mrtg/cpu_index.
➥html --title="CPU Usage" --
➥sort=name --enumerate /etc/mrtg/
➥cpu.cfg
```

Ao final, adicione um super cron contendo as OIDs personalizadas:

```
*/5 * * * * /bin/run-parts /etc/
➥cron.mrtg 1> /dev/null
```

Para gerar gráficos de qualquer outra métrica do sistema, como memória, número médio de usuários e uso de disco, consulte a definição do MIB UCD-SNMP[8] e simplesmente repita os passos anteriores, modificando o OID e os parâmetros de legenda do gráfico.

Consulta

Criamos um modelo para configurar gráficos personalizados específicos de recursos de sistema para dados de desempenho. O próximo passo é escolher um intervalo de consulta para a coleta dos dados. Isso pode ser feito informando-se o caminho do binário do MRTG e executando-o no intervalo desejado com o cron.

A linha a ser acrescentada ao crontab é:

```
0,5,10,15,20,25,30,25,40,45,50,55
➥* * * * env LANG=C /usr/local/
➥mrtg/bin/mrtg /usr/local/mrtg/
➥cfg/mrtg2.cfg
```

Essa entrada executará o binário do MRTG a cada cinco minutos, preenchendo os gráficos. Se um cron job não for configurado para executar o binário do MRTG, os dados do gráfico não serão preenchidos. É possível ajustar o intervalo de consulta conforme desejado, mas lembre-se de que quanto menor for a freqüência de consulta, menos preciso será o gráfico.

Conforme a configuração aplicada ao servidor web, pode ser necessário consultar o nome do arquivo que foi gerado pelos scripts do MRTG.

Nesse exemplo, o Apache foi utilizado e os arquivos foram gerados no diretório `WorkDir`.

Exibindo desempenho

A ferramenta *indexmaker* criou um arquivo de índice em `/usr/local/apache2/htdocs/mrtg/cpu_index.html`. O gráfico está presente nesse arquivo.

Exemplo 2: Arquivo cpu.cfg

```
01 ## Gráficos da CPU da máquina Tux ##
02 WorkDir: /usr/local/apache2/htdocs/mrtg
03 LoadMIBs: /usr/share/snmp/mibs/UCD-SNMP-MIB.txt
04 Target[Tux.cpu]:ssCpuRawUser.0&ssCpuRawUser.0:
   linux-magazine@Tux +
05 ssCpuRawSystem.0&ssCpuRawSystem.0:public@Tux +
06 ssCpuRawNice.0&ssCpuRawNice.0:public@Tux
07 RouterUptime[Tux.cpu]: public@Tux
08 MaxBytes[Tux.cpu]: 100
09 Title[Tux.cpu]: CPU Load
10 PageTop[Tux.cpu]: <H1>Active CPU Load %</H1>
11 Unscaled[Tux.cpu]: ymwd
12 ShortLegend[Tux.cpu]: %
13 YLegend[Tux.cpu]: CPU Utilization
14 Legend1[Tux.cpu]: Active CPU in % (Load)
15 Legend2[Tux.cpu]:
16 Legend3[Tux.cpu]:
17 Legend4[Tux.cpu]:
18 LegendI[Tux.cpu]: Active
19 LegendO[Tux.cpu]:
20 Options[Tux.cpu]: growright,nopercent
```

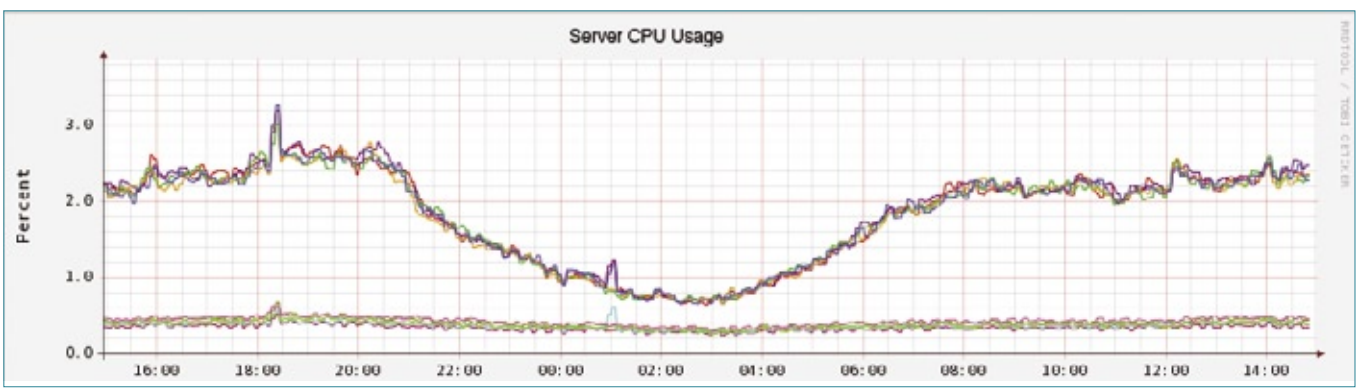


Figura 1 Gráfico de padrão normal no uso da CPU.

Exibindo banda

Nomes de arquivos às vezes são gerados automaticamente, portanto, é melhor primeiro procurar o arquivo no diretório de saída e só depois fornecer o nome do arquivo ao navegador web.

Depois de todo esse trabalho, os belos gráficos criados e uma visão global resumida do sistema são uma boa recompensa. É possível escalar a instalação do MRTG para incluir métricas e dados de desempenho, suprindo as necessidades tanto de pequenas quanto de grandes empresas. Para isso, basta executar novamente o *indexmaker* ou criar um portal para exibir imagens PNG criadas dinamicamente.

O *RRDtool*[9] oferece um desempenho maior e mais opções de customização do que os gráficos do MRTG. Use o RRDtool caso deseje monitorar um grande número de máquinas Linux.

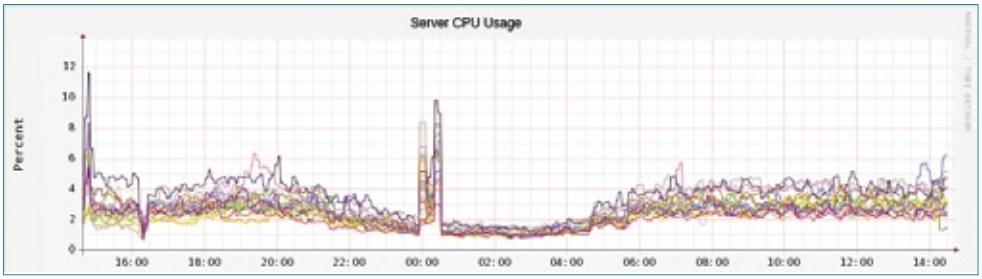


Figura 2 Um pico anormal aparece no gráfico de uso da CPU.

Interpretação de gráficos

Geralmente falando, os gráficos do MRTG são mais eficazes quando visualizados e interpretados com regularidade. É melhor gravar algum tipo de gráfico basal e usá-lo como comparação ao investigar e resolver problemas.

Por exemplo, a **figura 1** mostra um grupo de servidores sob carga normal. Na maioria das vezes, um padrão consistente se desenvolve ao longo do tempo. Note que a possibilidade de se agregar múltiplos servidores num único gráfico como esse é um recurso do RRDtool, que é um *add-on* do MRTG.

Se ocorrer um pico à meia-noite no gráfico de CPU do servidor (**figura 2**), uma explicação possível é alguma tarefa de becape agendada para esse horário. Outra possibilidade é que tenha ocorrido algum ataque aos servidores. Para decidir entre essas duas situações, pode-se comparar os gráficos de uso da CPU com os de tráfego de rede (**figura 3**).

O gráfico de rede não mostra pico algum no tráfego de rede no mesmo momento do pico no uso da CPU, então é seguro afirmar que não houve um ataque aos servidores. O passo seguinte seria investigar os logs do servidor em busca de indicações da execução de alguma tarefa agendada nesse horário.

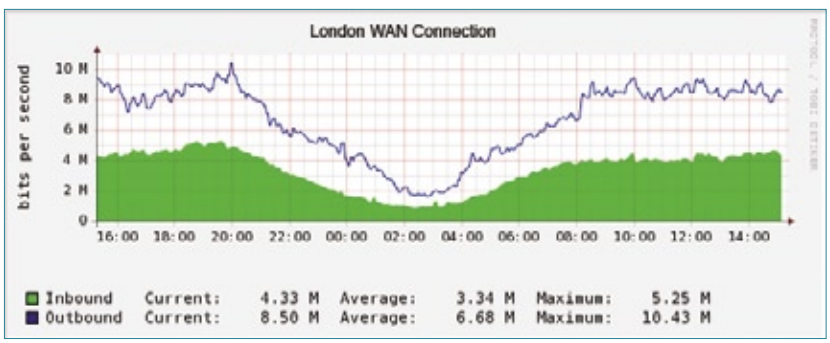


Figura 3 Uma rápida verificação do uso da rede mostra que o pico não foi causado pelo aumento do tráfego.

Conclusão

O MRTG permite que o administrador do sistema rapidamente detecte e investigue alterações em seu desempenho.

Este artigo mostrou uma pequena fração das possibilidades de criação de gráficos e resolução de problemas de desempenho do sistema com o MRTG. Diversas outras configurações são possíveis de acordo com as necessidades do administrador. ■

Mais informações

[1] MRTG: http://oss.oetiker.ch/mrtg/

[2] Adriano Matos Meier, "Monitorar é preciso": http://www.linuxmagazine.com.br/article/1154

[3] Net-SNMP: http://www.net-snmp.org

[4] GCC: http://gcc.gnu.org

[5] Biblioteca GD: http://www.boutell.com/gd/

[6] Libpng: http://www.libpng.org/pub/png/libpng.html

[7] Zlib: http://www.gzip.org/zlib

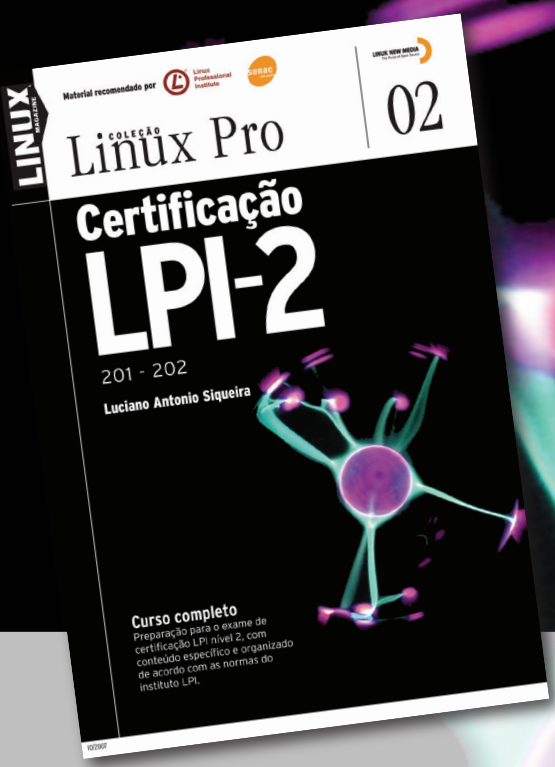
[8] Definição do MIB UCD-SNMP: http://www.oidview.com/mibs/2021/UCD-SNMP-MIB.html

[9] RRDtool: http://oss.oetiker.ch/rrdtool

Coleção Linux Pro

Prepare-se para a principal certificação profissional do mercado Linux

O primeiro volume traz informações referentes à LPI-1 e é o primeiro passo para a certificação. Estude para a prova de acordo com o conteúdo programático estabelecido pelo LPI.



Pautado conforme o roteiro estabelecido pelo próprio Linux Professional Institute e por este recomendado, o segundo volume é voltado à preparação do exame para a LPI-2.

Certifique-se para entrar em um mercado de trabalho em pleno crescimento no Brasil e no mundo.

Só a LPI garante a formação que o mercado espera para lidar com os ambientes mais diversos.
A qualidade destes volumes é atestada pelos selos do LPI e do SENAC, que os utilizam como material didático em seus cursos.

A venda nas melhores livrarias, no site www.linuxmagazine.com.br, ou pelo telefone (11) 4082-1300.

LINUX NEW MEDIA
The Pulse of Open Source

Controle obrigatório de acesso com o SELinux

Acesso restrito

O SELinux oferece um sistema mais seguro por meio do poderoso conceito dos controles obrigatórios de acesso.

por Thorsten Scherf

O Linux é um sistema operacional extremamente seguro, mas privilégios de acesso legados não oferecem proteção alguma contra a má configuração ou softwares mal escritos. Se um programa perder o controle porque o administrador se esqueceu de instalar o patch mais recente, ou se um usuário aumentar seus privilégios em decorrência de uma configuração incorreta, a segurança nativa do sistema não será capaz de oferecer qualquer proteção. O *SELinux* reduz esse perigo potencial, acrescentando níveis adicionais de controle por meio do nível chamado de *MAC*, ou *Mandatory Access Control* (controle de acesso obrigatório).

Há aproximadamente sete anos, a agência nacional de segurança dos EUA, NSA[1], lançou a primeira versão do SELinux. Com o objetivo de ser uma extensão do kernel 2.4 na época, os patches do kernel desde então ingressaram no kernel 2.6 oficial (**figura 1**). Em muitas distribuições, o SELinux faz parte da configuração padrão. Os exemplos apresentados neste artigo se baseiam na distribuição comunitária *Fedora Core* 8, mas são válidos em qualquer outra plataforma que suporte o SELinux. O importante é que o suporte necessário do kernel (`CONFIG_SECURITY_SELINUX`) e os pacotes *libselinux*, *policycoreutils* e *selinux-policy-targeted* estejam instalados. O SELinux também requer alguns pacotes padrão (*SysV-Init*, *pam*, *util-linux*, *coreutils* e outros).

O sistema legado de segurança do Linux se baseia em controles discretos de acesso (*Discretionary Access Controls* – DACs). Isso significa que o dono de um arquivo possui controle absoluto sobre o objeto que criou. Se um usuário conceder, desavisadamente, acesso global de escrita em um arquivo, não há um processo separado para validar essa etapa.

Se ainda um agressor conseguir executar códigos arbitrários no servidor web pela exploração de uma vulnerabilidade no software servidor web, o código do programa – uma shell, por exemplo – será executada com os privilégios da conta de usuário usada pelo servidor web. Se essa conta for o usuário *apache*, o agressor terá acesso a todos os arquivos que esse usuário possa acessar.

Na maioria dos casos, nenhum processo verifica se o servidor web realmente precisa acessar os arquivos que está acessando para realizar suas tarefas. Um agressor que venha a ganhar acesso ao sistema, nesse caso, pode conseguir aumentar seus privilégios na máquina. Recentemente, vários sistemas Linux foram comprometidos em virtude de uma falha no kernel que permitia que agressores explorassem a chamada de sistema

vmsplice(). Como conseqüência, os agressores ganharam controle completo de todo o sistema.

Em sistemas com o SELinux, todos os arquivos, ou todos os objetos, recebem um rótulo de segurança pelo MAC para um nível extra de controle. No caso de objetos de arquivo, o Linux guarda esse rótulo nos atributos estendidos. Ao mesmo tempo, cada processo, ou cada agente, também recebe o rótulo correspondente. Esse rótulo, conhecido como contexto de segurança, geralmente compreende três componentes: User:Role:Type/Domain (usuário, papel, tipo/domínio). Dois exemplos disso no arquivo de processo do servidor Apache /usr/bin/httpd são:

```
# ls -lZ /usr/sbin/http
➥-rwxr-xr-x  root root system_u:
➥object_r:httpd_exec_t  /usr/
➥sbin/httpd
```

e:

```
# ps -AZ|grep httpd
➥user_u:system_r:httpd_t  2571 ?
➥ 00:00:01 httpd
```

Exatamente da mesma forma como os rótulos de segurança, as ACLs Posix estendem os atributos de um arquivo. Neste exemplo, elas são assim:

```
# getfattr -d -m security /usr/
➥sbin/httpd
➥...
➥security.selinux="system_u:
➥object_
➥ r:httpd_exec_t\000"
```

Política SE

A política é outro componente importante. Uma política SE define o acesso entre objetos e agentes. A política especifica quais objetos o processo (como um processo do httpd com um papel específico) tem permissão para acessar. Se o acesso não for explicitamente permitido, ele será inicialmente registrado e finalmente proibido – ao menos no modo *enforcement* (**quadro 1**).

O servidor de segurança do kernel se assegura de que não ocorra infração alguma contra a política. Trata-se de uma entidade que faz referência à política e o rótulo de segurança define se o acesso é permitido. Para evitar *overheads* de desempenho, o servidor baseado no kernel usa o *Access Vector Cache* (AVC), ou cache de vetor de acesso.

Demo

Para uma pequena demonstração da forma como o *type enforcement* funciona, considere o seguinte: o administrador cria um arquivo chamado index.html no diretório /tmp/ (veja o **quadro 2**). Depois disso, o administrador move (não copia) o arquivo para a raiz de documentos

Quadro 1: Funções do SELinux

O SELinux possui três implementações distintas:

- Efetivação de tipo (TE, *Type Enforcement*);
- Controle de acesso baseado em papéis (RBAC, *Role-Band Acess Control*);
- Segurança multi-nível (MLS, *Multi-Level Security*).

O TE especifica qual agente tem permissão de acessar quais objetos – por exemplo, qual processo pode acessar quais arquivos. Entretanto, existe uma ampla gama de diferentes objetos, incluindo portas de rede e áreas de memória. O SELinux atribui um domínio a cada agente e um tipo a cada objeto. Para explicar de forma genérica, o reforço de tipo controla qual domínio tem permissão para acessar quais tipos. Tipos e domínios são identificados de formas semelhantes: sempre terminam com _T (por exemplo, httpd_t).

O RBAC emprega um modelo de usuário abstrato e atribui um papel a cada usuário, que, então, herdam os privilégios atribuídos ao papel. Portanto, é possível atribuir ao usuário root um papel que não possua privilégio administrativo algum. Para alternar para outro papel com maiores privilégios, o usuário primeiro precisaria se autenticar com uma senha. Esse é um recurso interessante caso se deseje configurar a máquina sem o onipotente usuário root. O usuário não pode, em momento algum, assumir mais de um papel; todavia, os usuários podem usar o comando newrole (semelhante ao su) para mudarem de papel, contanto que a política permita isso. Um nome típico de política é user_r (papéis sempre terminam em _r).

Russell Coker oferece na rede[2] uma máquina para se experimentar o SELinux. Nela, é utilizada a funcionalidade RBAC, e Coker publicou a conta de root para a máquina, permitindo o acesso de qualquer pessoa interessada em entrar como administrador. Testadores em breve descobrirão que o conjunto de comandos disponíveis para eles é extremamente restrito, pois o usuário de nome root não é o administrador nessas máquinas.

Finalmente, o MLS define diferentes níveis de segurança e é mais usado em ambientes de alta segurança, como aplicações militares. Objetos recebem níveis de segurança (confidencial, estritamente confidencial, secreto e assim por diante) e agentes recebem permissões para esses diferentes níveis de confidencialidade. Em todos os locais onde o MLS seja instalado, o rótulo de segurança é estendido acrescentando-se um quarto e um quinto componentes até se parecer com:

Usuário:Papel:Tipo/Domínio:Sensibilidade:Categoria

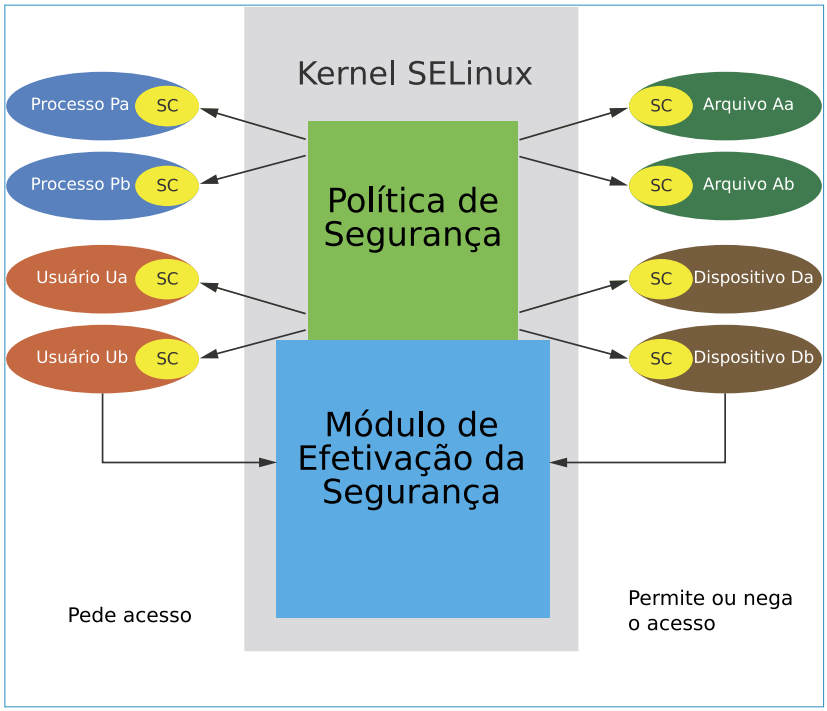


Figura 1 O servidor de segurança baseado no kernel decide o nível de acesso.

do servidor web, que, no Fedora, é `/var/www/html/`. Finalmente, o administrador inicia o servidor web (`/etc/init.d/httpd start`) e acessa a página recém-criada num navegador web (`http://localhost/index.html`). Se o modo enforcing do SELinux estiver ativo (padrão), o navegador web exibirá uma mensagem de erro, pois `index.html` foi criado em `/tmp/` e herdou seu rótulo de segurança:

```
# ls -l| /tm/index.html -rw-r--r--
➥ root root root:object_r:tmp_t /
➥tmp/index.html
```

Em contraste com isso, o processo do servidor web roda no domínio intitulado `httpd_t`:

```
# ps -AZ|grep httpd
user_u:system_r:httpd_t 2571
➥ ?00:00:02  httpd
```

A política precisa de uma regra que forneça ao domínio `httpd_t` acesso a arquivos do tipo `tmp_t`, mas essa regra não existe. O servidor web precisa acessar seus próprios arquivos de configuração, scripts CGI e outros conteúdos de seu diretório. Existem tipos específicos para todos esses arquivos, como, por exemplo, `httpd_config_t`, `httpd_log_t`, `httpd_sys@script_exec_t` e `httpd_sys_content_t`.

Os arquivos no diretório `/tmp/` geralmente não são os tipos de objetos que o servidor acessa; portanto, não há instrução de permissão para o tipo `tmp_t` no arquivo de política.

Se você verificar o arquivo `/var/log/audit/audit.log`, verá uma mensagem informando que acaba de ocorrer uma tentativa não autorizada de abertura de um arquivo:

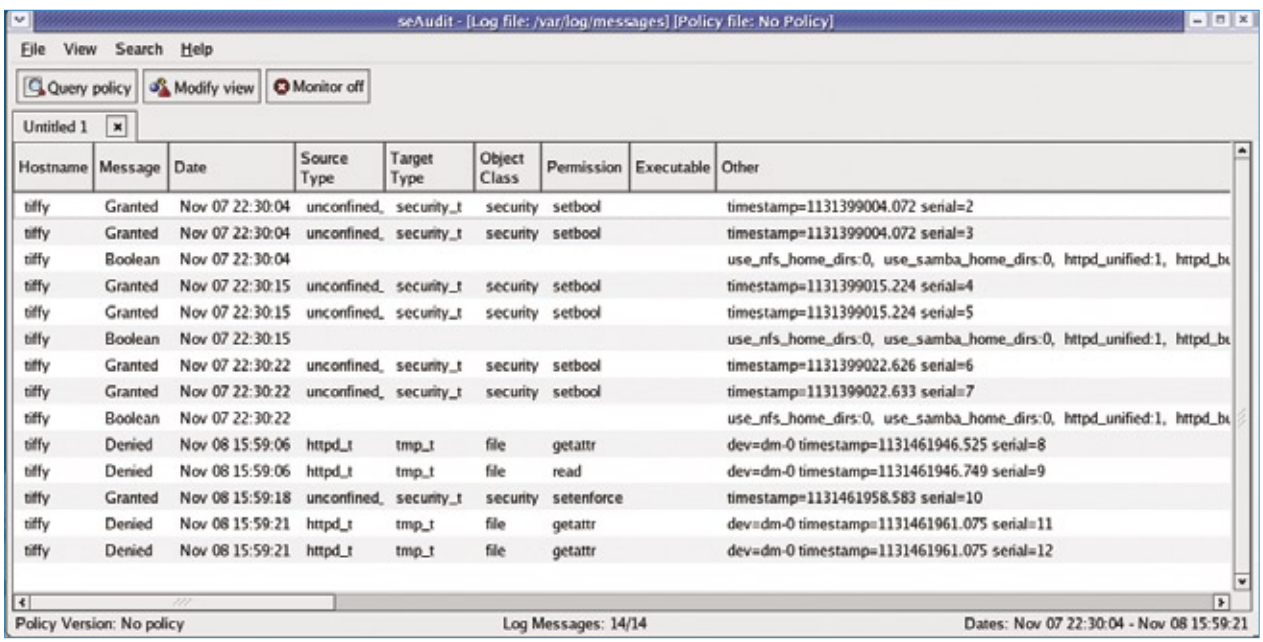


Figura 2 A ferramenta *seaudit* exibe todas as entradas do log do *SELinux* numa lista ordenada.

```
... audit(1202241301.521:12): avc>
➥ denied
➥ {getattr } for  pid=6608
➥ comm="httpd" name="index.html"
➥ dev=dm-0 ino=179881
➥ scontext=user_u:system_r:httpd_t
➥ tcontext=root:object_r:tmp_t
➥ tclass=file
```

Essa entrada no log revela que o processo com PID 6608 e nome *httpd* acabou de executar a chamada de sistema `getattr` (ou seja, tentou obter os atributos) sobre um arquivo de *inode* número 179881 e nome *index.html*. Os termos `scontext` e `tcontext` se referem ao rótulo de segurança para o processo de origem (`apache`) e o arquivo-alvo (`index.html`). Os termos `avc: denied` indicam que o servidor de segurança que está rodando no kernel impediu essa ação.

Se for preferível uma abordagem mais estruturada, pode-se usar o *seaudit* para visualizar arquivos de log (**figura 2**). Essa ferramenta exibe entradas individuais de log graficamente.

Chamando `seaudit-report --html arquivo`, é possível até gerar uma página HTML que exiba tanto os logs quanto várias estatísticas sobre o sistema SELinux (veja a **figura 3**).

Quadro 2: Rótulo de segurança do sistema de arquivos

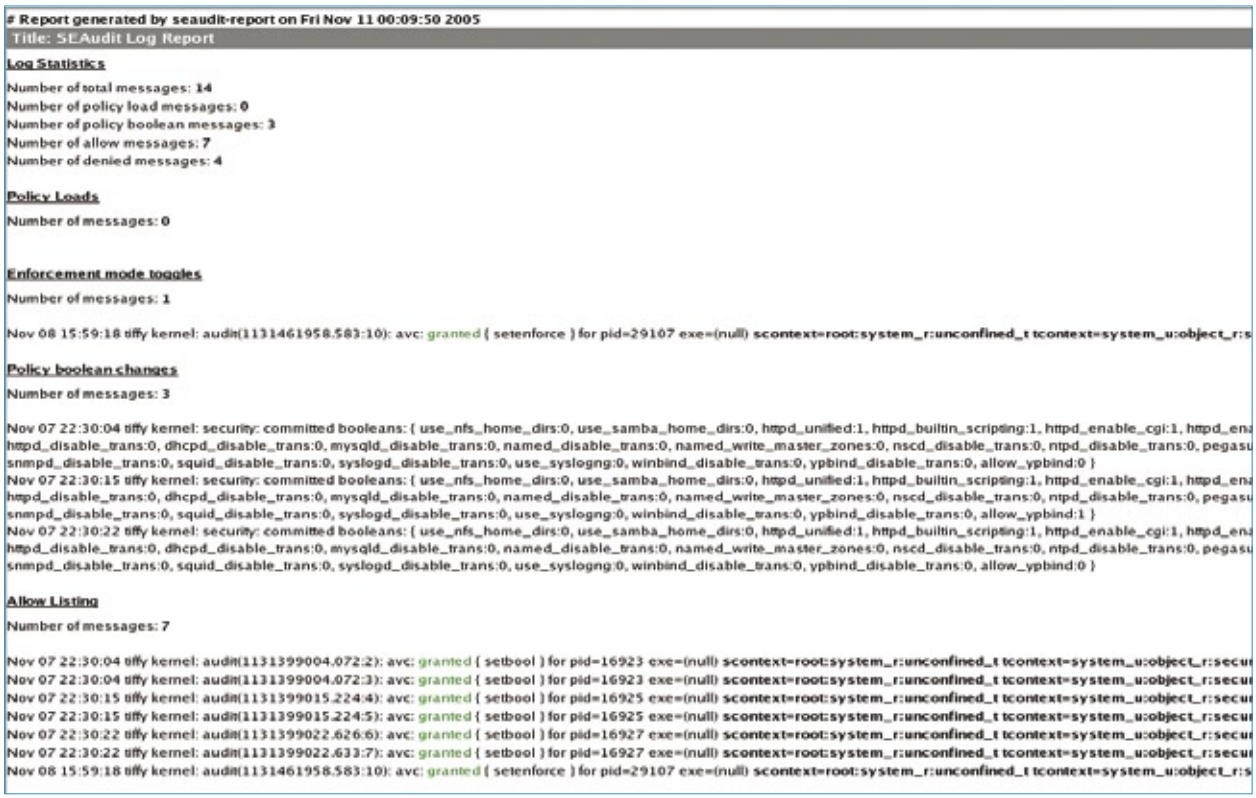
Embora o SELinux funcione em sistemas de arquivos sem suporte a atributos estendidos, como NFS ou ISO9660, os administradores precisam de macetes para fazer isso acontecer. O comando `mount` tem uma opção para lidar com isso: `context=<rótulo de segurança>`. Essa opção permite a especificação de um rótulo de segurança para todo o sistema de arquivos.

Achando problemas

Se o *setroubleshootd* estiver em execução, será mostrada a seguinte entrada extra no arquivo de log `/var/log/messages`:

```
setroubleshoot: #012 SELinux is
➥ preventing the /usr/sbin/httpd
➥ from using potentially
➥mislabeled files (/var/www/html/
➥index.html). #012 For complete
➥ SELinux messages
➥ run sealert -l 5e982b3b-3ae7-
➥4848-
➥b8bd-7d8553a07732
```

O *daemon* setroubleshoot foi desenvolvido há algum tempo para aumentar a legibilidade das mensagens levemente críticas emitidas pelo daemon de auditoria e para dar aos usuários dicas de solução de problemas. Se o usuário executar o comando especificado na entrada do log, ele verá a explicação exibida no **exemplo 1**.



Report generated by seaudit-report on Fri Nov 11 00:09:50 2005

Title: SEAudit Log Report

Log Statistics

Number of total messages: 14
Number of policy load messages: 0
Number of policy boolean messages: 3
Number of allow messages: 7
Number of denied messages: 4

Policy Loads

Number of messages: 0

Enforcement mode toggles

Number of messages: 1

Nov 08 15:59:18 tiffy kernel: audit(1131461958.583:10): avc: granted { setenforce } for pid=29107 exe=(null) scontext=root:system_r:unconfined_t tcontext=system_u:object_r:s

Policy boolean changes

Number of messages: 3

Nov 07 22:30:04 tiffy kernel: security: committed booleans: { use_nfs_home_dirs:0, use_samba_home_dirs:0, httpd_unified:1, httpd_builtin_scripting:1, httpd_enable_cgi:1, httpd_ena
httpd_disable_trans:0, dhcpd_disable_trans:0, mysqld_disable_trans:0, named_disable_trans:0, named_write_master_zones:0, nscd_disable_trans:0, ntpd_disable_trans:0, pegasu
snmpd_disable_trans:0, squid_disable_trans:0, syslogd_disable_trans:0, use_syslogng:0, winbind_disable_trans:0, ypbind_disable_trans:0, allow_ypbind:0 }
Nov 07 22:30:15 tiffy kernel: security: committed booleans: { use_nfs_home_dirs:0, use_samba_home_dirs:0, httpd_unified:1, httpd_builtin_scripting:1, httpd_enable_cgi:1, httpd_ena
httpd_disable_trans:0, dhcpd_disable_trans:0, mysqld_disable_trans:0, named_disable_trans:0, named_write_master_zones:0, nscd_disable_trans:0, ntpd_disable_trans:0, pegasu
snmpd_disable_trans:0, squid_disable_trans:0, syslogd_disable_trans:0, use_syslogng:0, winbind_disable_trans:0, ypbind_disable_trans:0, allow_ypbind:1 }
Nov 07 22:30:22 tiffy kernel: security: committed booleans: { use_nfs_home_dirs:0, use_samba_home_dirs:0, httpd_unified:1, httpd_builtin_scripting:1, httpd_enable_cgi:1, httpd_ena
httpd_disable_trans:0, dhcpd_disable_trans:0, mysqld_disable_trans:0, named_disable_trans:0, named_write_master_zones:0, nscd_disable_trans:0, ntpd_disable_trans:0, pegasu
snmpd_disable_trans:0, squid_disable_trans:0, syslogd_disable_trans:0, use_syslogng:0, winbind_disable_trans:0, ypbind_disable_trans:0, allow_ypbind:0 }

Allow Listing

Number of messages: 7

Nov 07 22:30:04 tiffy kernel: audit(1131399004.072:2): avc: granted { setbool } for pid=16923 exe=(null) scontext=root:system_r:unconfined_t tcontext=system_u:object_r:secur
Nov 07 22:30:04 tiffy kernel: audit(1131399004.072:3): avc: granted { setbool } for pid=16923 exe=(null) scontext=root:system_r:unconfined_t tcontext=system_u:object_r:secur
Nov 07 22:30:15 tiffy kernel: audit(1131399015.224:4): avc: granted { setbool } for pid=16925 exe=(null) scontext=root:system_r:unconfined_t tcontext=system_u:object_r:secur
Nov 07 22:30:15 tiffy kernel: audit(1131399015.224:5): avc: granted { setbool } for pid=16925 exe=(null) scontext=root:system_r:unconfined_t tcontext=system_u:object_r:secur
Nov 07 22:30:22 tiffy kernel: audit(1131399022.626:6): avc: granted { setbool } for pid=16927 exe=(null) scontext=root:system_r:unconfined_t tcontext=system_u:object_r:secur
Nov 07 22:30:22 tiffy kernel: audit(1131399022.633:7): avc: granted { setbool } for pid=16927 exe=(null) scontext=root:system_r:unconfined_t tcontext=system_u:object_r:secur
Nov 08 15:59:18 tiffy kernel: audit(1131461958.583:10): avc: granted { setenforce } for pid=29107 exe=(null) scontext=root:system_r:unconfined_t tcontext=system_u:object_r:s

Figura 3 O *seaudit-report* pode gerar estatísticas em HTML.

O desktop Gnome mostra um pequeno ícone (um escudo amarelo) na barra de tarefas sempre que é criada uma entrada no log do SELinux. Os usuários podem clicar no ícone para abrirem o navegador de solução de problemas do SELinux, que permite a navegação gráfica pelas mensagens processadas (**figura 4**). Essa ferramenta oferece aos usuários inexperientes uma forma de resolver problemas:

```
restorecon -v /var/www/html/index.
➥html
```

O comando usa uma política para especificar o rótulo correto para o arquivo `index.html`. De forma alternativa, o administrador pode especificar manualmente o tipo correto de arquivo:

```
chcon -t httpd_sys_content_t /var/
➥www/html/index.html
```

De qualquer forma, os resultados devem ser:

```
# ls -lZ /var/www/html/index.html
➥ -rw-r--r--  root root system_u:
➥object_r:httpd_sys_content_t  /
➥var/www/html/index.html
```

Da próxima vez que alguém tentar exibir um arquivo num navegador web, não deve haver obstáculos de segurança.

O exemplo acima mostra como o SELinux funciona. Independente de privilégios legados, o Linux permite o acesso somente se existir uma entrada correspondente na política do SELinux (MAC). O distribuidor ou administrador consciente da segurança só criará essa entrada se o acesso for realmente necessário.

Administração

Há várias ferramentas disponíveis para gerenciar um sistema SELinux. Por exemplo, um utilitário chamado *getenforce* exibe o modo atual do SELinux. `setenforce 0|1` permite que o administrador alterne o modo, com `0` representando o modo permissivo e `1` sendo o modo enforcing. O permissivo significa que ações não autorizadas são registradas, mas não proibidas, o que é útil quando se desenvolve um novo módulo de política. O servidor de segurança consulta suas entradas de política para decidir o que é permitido. Para mudar permanentemente um modo, é necessária uma entrada no arquivo `/etc/selinux/config` (**exemplo 2**).

Exemplo 1: sealert -l

```
Summary
    SELinux is preventing the /usr/sbin/httpd
from using potentially mislabeled files (/var/
www/html/index.html).
Detailed Description
    SELinux has denied /usr/sbin/httpd access
to potentially mislabeled file(s) (/var/www/
html/index.html). This means that SELinux will
not allow /usr/sbin/httpd to use these files.
It is common for users to edit files in their
home directory or tmp directories and then move
(mv) them to system directories. The problem is
that the files end up with the wrong file
context which confined applications are not
allowed to access.
Allowing Access
    If you want /usr/sbin/httpd to access this
files, you need to relabel them using
restorecon -v /var/www/html/index.html. You
might want to relabel the entire directory
using restorecon -R -v /var/www/html.
...
```

A ferramenta mais interessante para o SELinux é o *system-config-selinux* (**figura 5**). Ele permite que os administradores façam configurações básicas, como o modo do SELinux, enquanto suporta tarefas mais complexas como a criação de novos módulos de política. Também se pode configurar booleanos, que são simplesmente instruções que ativam regras de política que se tenha preparado sem precisar da linguagem de macro *m4* para fazer isso (a política inteira é baseada nessa linguagem).

Existe uma variedade de booleanos pré-definidos. Como exemplo, pode-se permitir que um servidor

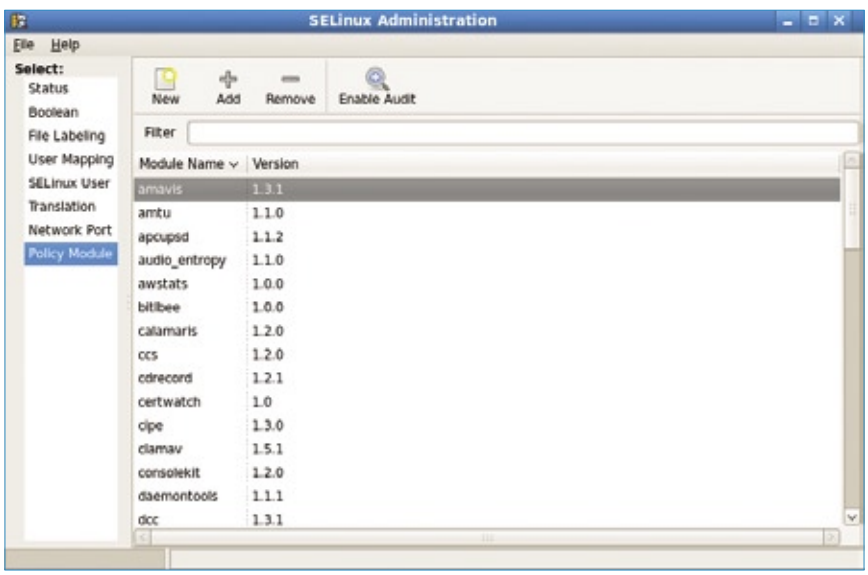


Figura 5 A ferramenta gráfica de configuração *system-config-selinux* garante uma administração conveniente aos sistemas *SELinux*.

Exemplo 2: /etc/selinux/config

```
# Este arquivo controla o estado
do SELinux no sistema.
# SELINUX= pode ter um dos
seguintes valores:
#     enforcing - A política de
segurança do SELinux é
efetivada.
#     permissive - O SELinux
imprime alertas em vez de
efetivar a segurança.
#     disabled - Nenhuma
política do SELinux é carregada.
SELINUX=enforcing
# SELINUXTYPE= pode receber um
dos dois valores:
#     targeted - Processos-alvo
são protegidos
#     mls - Proteção por
segurança multi-nível.
SELINUXTYPE=targeted
```

web acesse dados nos diretórios dos usuários (`UserDir`), ou que o servidor de nome realize mudanças no arquivo de zona (`DDNS`). Booleanos geralmente podem ser exibidos na linha de comando com o *getsebool*. O comando `getsebool -a | grep httpd`, por exemplo, lista todos os booleanos para o servidor web Apache (**exemplo 3**).

Várias *manpages* descrevem os booleanos para os serviços de rede mais populares. A página do *httpd_selinux* ajuda com o servidor web.

Exemplo 3: getsebool -a |grep httpd

```
allow_httpd_anon_write --> off
allow_httpd_dbus_avahi --> off
allow_httpd_mod_auth_pam --> off
allow_httpd_sys_script_anon_write --> off
httpd_builtin_scripting --> on
httpd_can_network_connect --> off
httpd_can_network_connect_db --> off
httpd_can_network_relay --> off
httpd_can_sendmail --> off
httpd_enable_cgi --> on
httpd_enable_ftp_server --> off
httpd_enable_homedirs --> on
httpd_ssi_exec --> off
httpd_tty_comm --> on
httpd_unified --> on
httpd_use_cifs --> off
httpd_use_nfs --> off
```

Além disso, pode-se alterar os booleanos na linha de comando com o *setsebool*. O seguinte comando permite que o servidor web execute scripts CGI:

```
setsebool -P httpd_enable_cgi 1
```

O *setstatus* é uma interessante ferramenta de linha de comando que resume a configuração atual do SELinux (**exemplo 4**).

Enquanto o RHEL 4 possuía uma política puramente monolítica, hoje são usadas as variantes modulares da política. Isso dá aos administradores várias vantagens. Por exemplo, um desenvolvedor de políticas não precisa mais se preocupar com as fontes completas de política para o sistema SELinux; basta desenvolver um único módulo para a aplicação que se deseje proteger e adicionar esse módulo ao sistema.

A política padrão,que faz parte do Fedora (política *targeted*), protege muitos aplicativos logo depois da instalação. Os programas protegidos pela política são chamados de *targeted programs* (programas objetivados), o que explica o nome da política. O comando `semodule` retorna todos os módulos de política disponíveis (**exemplo 5**).

Se os administradores quiserem remover um módulo junto com a proteção do SELinux para esse programa, eles podem simplesmente fornecer o nome do módulo com a opção `-r`:

```
semodule -r amavis
```

Isso remove permanentemente a permissão para o aplicativo especificado, mas é possível reintroduzir o módulo depois. O RPM de políticas armazena todos os módulos padrão disponíveis no diretório `/usr/share/selinux/targeted/`. O administrador pode recarregar o módulo do *Amavis* executando o `semodule` da seguinte forma:

```
semodule -i /usr/share/selinux/
➥targeted/amavis.pp
```

O comando recarrega o módulo do Amavis no servidor de segurança que roda no kernel. As regras do módulo então assumem a responsabilidade por negar ou permitir qualquer ação relacionada ao software Amavis. Se for necessário um panorama preciso de quais regras os módulos individuais incluem, pode-se instalar o SRPM da política em uso, ou pode-se simplesmente instalar a

Exemplo 4: sestatus -b

```
SELinux status:           enabled
SELinuxfs mount:         /selinux
Current mode:          permissive
Mode from config file: permissive
Policy version:                21
Policy from config file: targeted
Policy booleans:
allow_console_login           off
allow_cvs_read_shadow         off
allow_daemons_dump_core        on
allow_daemons_use_tty          on
allow_execheap                off
allow_execmem                  on
...
```

Exemplo 5: semodule -l

```
amavis          1.3.1
amtu            1.1.0
apcupsd         1.1.2
audio_entropy   1.1.0
awstats         1.0.0
bitlbee         1.0.0
calamaris       1.2.0
ccs             1.2.0
cdrecord        1.2.1
certwatch       1.0
cipe            1.3.0
clamav          1.5.1
...
```

ferramenta gráfica *apol*, que é capaz de exibir arquivos binários de política em formato de texto, permitindo assim a investigação da política instalada.

Se isso parecer complicado demais, ou se for necessário um panorama genérico da política que você instalou, o *seinfo* é a ferramenta que você procura (**exemplo 6**). É fácil verificar a complexidade do conjunto total de regras.

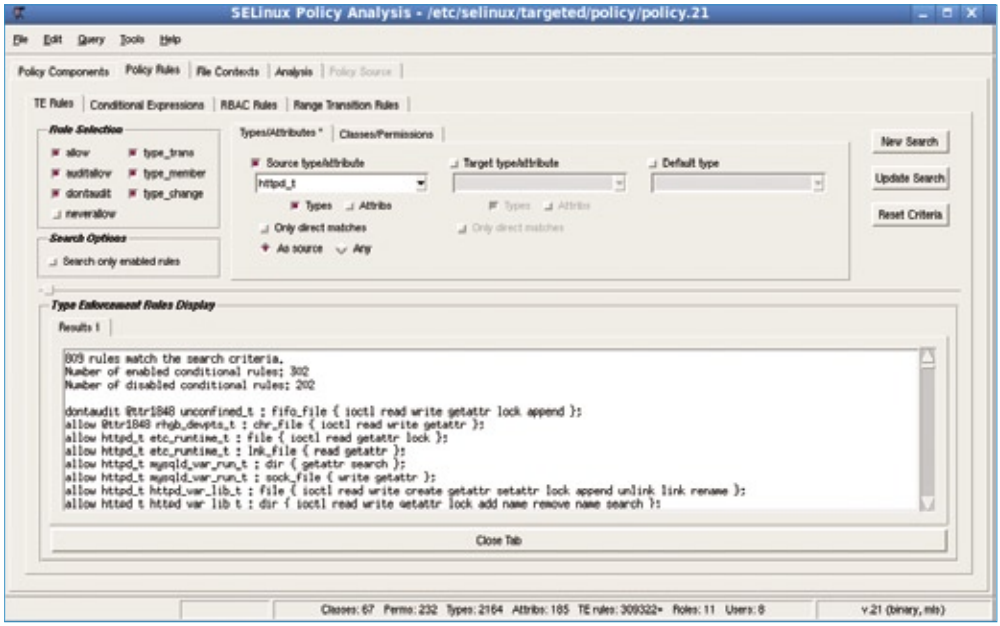


Figura 6 A ferramenta gráfica *apol* exibe a política binária em texto puro.

Um recurso da política do SELinux no Fedora 8 é que agora ele contém as propriedades da antiga política estrita. Para ser mais preciso, agora é possível usar a política targeted para restrir contas de usuários (ou seja, para implementar RBAC). Por exemplo, Dan Walsh liberou um módulo de política chamado *xguest*[3]. O módulo permite que o administrador converta rapidamente qualquer desktop Gnome num sistema de quiosque. O usuário tem permissão de fazer login com o usuário *xguest e* possui privilégios de acesso muito limitados, além de uma seleção de programas muito restrita. Por exemplo, o acesso à rede é restrito ao navegador web Firefox; nenhum outro aplicativo possui permissão de acesso à rede.

O módulo também proíbe modificações às configurações do Gnome (*gconf*). Esse é um ambiente ideal para sistemas de quiosque como aqueles geralmente encontrados em aeroportos e lobbies de hotéis. O módulo de política *xguest* também serve como ponto de partida para seu próprio desenvolvimento. Por exemplo, é possível acrescentar mais instruções às regras para suportar o acesso por SSH.

Exemplo 6: seinfo

```
Statistics for policy file: /etc/
selinux/targeted/policy/policy.21
Policy Version & Type: v.21 (binary,
mls)
Classes:      67  Permissions:  232
Sensitivities: 1  Categories:  1024
Types:      2166  Attributes:   185
Users:         8  Roles:         11
Booleans:    115  Cond. Expr.:  144
Allow:    171807  Neverallow:     0
Auditallow:   28  Dontaudit: 134379
Type_trans: 3286  Type_change:   88
Type_member:  14  Role allow:    16
Role_trans:    3  Range_trans:  158
Constraints:  59  Validatetrans:  0
Initial SIDs: 27  Fs_use:        17
Genfscon:     66  Portcon:      292
Netifcon:      0  Nodecon:        8
```

Desenvolvimento

Para quem preferir contribuir ativamente com o SELinux, em vez de apenas configurar políticas, o Fedora 8 possui várias ferramentas para isso. Por exemplo, pode-se modificar a política binária mesmo com ela em execução com a ferramenta *semanage* sem acessar os fontes. Obviamente, dessa maneira é possível mudar todas as propriedades, mas essa técnica geralmente é melhor para mudanças mais simples.

A política do SELinux oferece ao servidor web Apache a possibilidade de se ligar a portas de rede específicas. Essas portas são designadas como tipos `http_port_t` na política do SELinux. O comando `semanage` informa quais portas possuem um rótulo desse tipo:

```
# semanage port -l |grep http_
➥port_t tcp 80, 443, 488,
➥ 8008, 8009
```

O administrador que desejar aplicar esse rótulo a uma nova porta deve executar `semanage` da seguinte forma:

```
semanage port -a -t http_port_t -p
➥ tcp 777
```

A execução do comando `apol` na política para encontrar uma regra correspondente revela o seguinte:

```
allow httpd_t http_port_t : tcp_
➥socket { name_bind name_connect
➥};
```

A regra permite que os processos no domínio `httpd_t` acessem qualquer porta de rede que possua

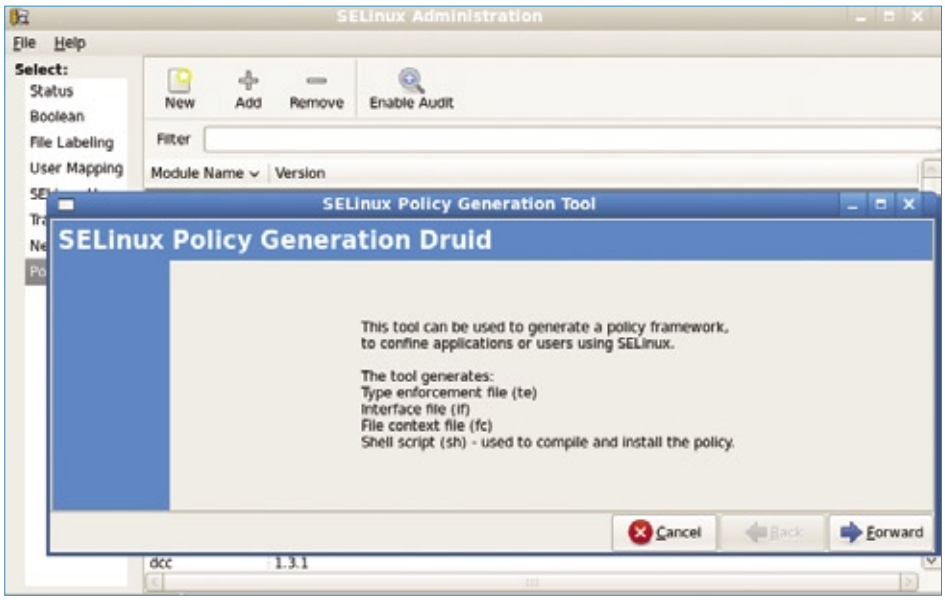


Figura 7 O *system-config-selinux* facilita a criação de novos módulos de política.

o rótulo `http_port_t`; agora, essas portas são 777, 80, 443, 488, 8008 e 8009.

É possível levar essa idéia um passo adiante e criar módulos completamente novos. Há duas ferramentas para isso: `system-config-selinux` e `policygentool`. O segundo faz parte do pacote *selinux-policy-devel*, localizado no diretório `/usr/share/selinux/devel/`. Ele ajuda na criação de arquivos necessários para gerar um módulo binário de política. Uma descrição dos passos individuais poderia facilmente encher um livro, por isso este artigo descreve apenas por alto as instruções necessárias.

Criação da política

Primeiramente, o administrador inicia uma ferramenta e informa o nome do aplicativo que deseja proteger, assim como o nome do módulo de política a ser criado:

```
./policygentool foo /usr/bin/foo
```

A ferramenta pede vários detalhes sobre o aplicativo, tais como se ele usa um script de inicialização, no qual armazena seus arquivos de log etc.

Após o administrador responder a todas essas perguntas, o programa cria três arquivos – `foo.fc`, `foo.if` e `foo.te` – que são, respectivamente, o contexto do arquivo, o arquivo de interface e o reforço de tipo. O arquivo de contexto de arquivo permite que o administrador vincule os arquivos do aplicativo a um rótulo do SELinux, enquanto que já o arquivo de reforço de tipo especifica as regras que coincidem com ele – ou seja, o que o aplicativo tem permissão para fazer. O arquivo de interface põe macros à disposição de outros módulos de política.

Após editar os arquivos, deve-se criar o módulo de política com a seguinte entrada:

```
make -f /usr/share/selinux/
➥devel/ Makefile
```

Após essa etapa, o arquivo `foo.pp` é criado no diretório atual. O comando `semoldule -i foo.pp` carrega o módulo no servidor de segurança do kernel.

Se esse processo todo parecer complexo demais, sempre é possível usar a interface gráfica *system-config-selinux* (**figura 7**) para criar um novo módulo de política. Há um extenso tutorial para isso disponível em [4].

Conclusões

O SELinux é uma extensão de segurança muito útil. Uma vez ativado, ele roda de forma mais ou menos transparente em segundo plano, monitorando o sistema em execução – contanto que o distribuidor tenha criado os meios, fornecendo uma política digna desse título. Durante a escrita deste artigo, o Fedora é a distribuição líder nesse aspecto.

As versões recentes melhoraram a usabilidade do SELinux; por exemplo, os logs agora são mais fáceis de ler do que antes, devido à ferramenta *setroubleshootd*. Até usuários inexperientes podem desenvolver seus próprios módulos de política para colocar novos programas sob o escudo protetor do SELinux, com alguma ajuda da interface gráfica *system-config selinux*. ■

Mais informações

[1] SELinux na NSA: http://www.nsa.gov/selinux

[2] Máquina de testes de Russell Coker: http://www.coker.com.au/selinux/play.html

[3] Dan Walsh, "Creating a Kiosk Account": http://danwalsh.livejournal.com/13376

[4] Guia para a criação de novos módulos de política, por Dan Walsh: http://tinyurl.com/2hn9nc

Programação em PHP com Subversion no IDE Eclipse

Eclipse controlado

O plugin PHPEclipse traz ao famoso IDE a capacidade de funcionar com o PHP, enquanto o Subclipse acrescenta o controle de versões.

por Alex Legler e Peter Kreussel

O popular ambiente de desenvolvimento livre *Eclipse*[1] oferece aos programadores um editor repleto de recursos, um gerenciador de controle de versões e um depurador de código numa única interface gráfica. O Eclipse foi criado como um IDE universal facilmente extensível para acomodar várias linguagens de programação. O plugin *PHPEclipse* converte o Eclipse num IDE completo para websites dinâmicos baseados em PHP. Outro plugin, chamado *Subclipse*[2], integra ao ambiente o controle de versões pelo sistema *Subversion*[3]. Este artigo descreverá como criar um ambiente de desenvolvimento para PHP com controle de versões pelo Subversion, tudo isso sobre o Eclipse.

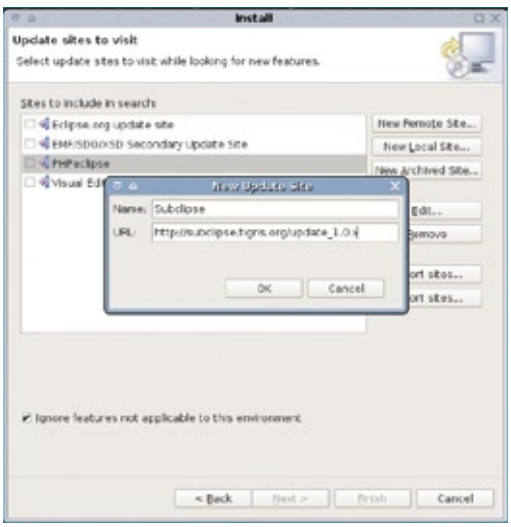


Figura 1 A interface de plugins do *Eclipse* pode ajudar a instalar o *Subversion* e várias outras extensões.

Quem desenvolve sites dinâmicos geralmente opta por instalar localmente um servidor web que ofereça suporte à linguagem de script escolhida. Este artigo utiliza essa abordagem, descrevendo uma configuração com todos os componentes necessários instalados localmente. Contudo, o sistema Subversion pode ser executado num servidor central para dar acesso a uma equipe de desenvolvedores.

A depuração exige um diretório para o projeto nos diretórios de documentos do servidor web. Para depurar, é necessário executar os arquivos no servidor web ou permitir que ele rode o código PHP embutido. Por outro lado, o depurador também precisa ter acesso direto ao código-fonte. Ao iniciar o Eclipse, selecione como *Workspace* o diretório raiz do servidor. Além disso, certifique-se de que o usuário que for rodar o Eclipse possua permissão de escrita.

A configuração descrita neste artigo requer os seguintes softwares:

- um servidor web na máquina local com suporte a PHP;
- o Subversion, com um servidor Subversion em execução: se a distribuição usada fornecer o servidor Subversion num pacote separado, será necessário instalá-lo também;
- o IDE Eclipse com os plugins Subclipse e PHPEclipse. O Eclipse exige a versão 1.4 ou mais recente do ambiente Java (JRE).

Instalação

O Subclipse está disponível sob a *Common Public License* e é fácil de instalar por meio da interface de plugins do Eclipse[4]. O menu *Help* | *Software updates* | *Find and install* abre a ferramenta de atualização (**figura 1**). É necessário ativar a opção *Search for new features to install* e clicar em *Next* antes de pressionar o botão *Add remote Site* e digitar a URL `http://subclipse.tigris.org/update_1.0.x/`. O usuário que for executar o Eclipse precisa ter permissão de escrita no diretório do programa.

No momento da escrita deste artigo, o Eclipse é incapaz de usar o sistema de arquivos para acessar diretamente repositórios locais, a menos que o Subversion seja compilado com os vínculos com *JavaHL* e que eles sejam usados por meio do menu *Preferences* | *Team* | *SVN*. O código-fonte do Subversion está disponível no site do projeto[5]. É fácil configurar o servidor SVN, assim como geralmente é fácil usá-lo, no caso de repositórios locais.

Para criar um repositório para o projeto, basta o seguinte comando:

```
svnadmin create --fs-type fsfs
➥ caminho/do/repositório
```

Em seguida, os arquivos `svnserve.conf` e `conf/passwd` (esse último no diretório do repositório) devem ser editados de acordo com os **exemplos 1** e **2**, respectivamente, para configurar o acesso ao servidor.

Para iniciar o servidor, basta um `svnserve -d -r caminho/do/repositório`. Para permitir que o Subclipse acesse o repositório, primeiro é necessário se registrar. Para isso, deve-se acessar o menu *Window* | *Open Perspective* e alternar para a perspectiva *SVN Repository Exploring*. O painel esquerdo possui uma janela intitulada *SVN Repository* que exibe todos os repositórios integrados. No canto direito da barra de ferramentas dessa janela está o botão *Add new SVN Repository*. Pressione-o e digite a URL `svn://localhost` no diálogo. Após o Subclipse pedir a senha, o novo repositório aparecerá na lista à esquerda da janela.

Caso o projeto em uso no Eclipse resida num repositório SVN, o Subclipse o ajudará a fazer o *check out* clicando em *File* | *New* | *Other...* para abrir uma seleção dos assistentes de projeto disponíveis. O menu *SVN* | *Checkout projects from SVN* permite a criação de um novo projeto no Eclipse a partir dos arquivos no repositório.

Se for necessário mexer em arquivos PHP já existentes, deve-se copiar o diretório raiz do projeto para o diretório de trabalho e criar no Eclipse um novo projeto com o nome do diretório do projeto. Para deixar o controle do gerenciador de versões com o Subclipse, agora basta clicar com o botão direito no diretório raiz do projeto e selecionar *Team* | *Share Project*.

Com um clique do botão direito no navegador de arquivos é possível criar um novo projeto. Selecione *New* | *PHP Project*. Se o item *PHP Project* estiver ausente, talvez ele esteja sob o item *Other...* Clicando com o botão direito em *Team* | *Share Project*, pode-se assinalar um novo projeto para ter as versões gerenciadas.

Terminada uma etapa de edição, pode-se fazer o *commit* das mudanças para o repositório com um clique direito no arquivo ou diretório e selecionando-se *Team* | *Commit* (**figura 2**). Um comentário pode ser adicionado a cada versão criada por um commit, opção essa de bom uso para uma melhor rastreabilidade no futuro.

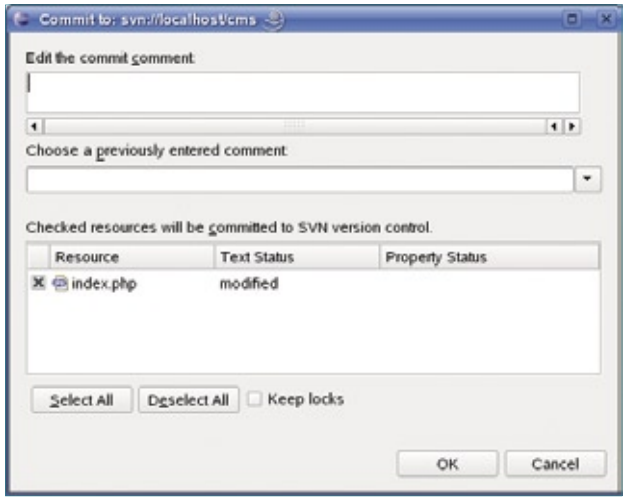


Figura 2 O diálogo de *commit* pede comentários.

Se tiver sido criado um novo arquivo, será preciso atribuir o controle explicitamente ao SVN. Para isso, marque a caixa à esquerda do nome do arquivo para alterar o estado para *added* (adicionado).

Conflitos

Caso múltiplos desenvolvedores editem o mesmo arquivo num mesmo momento, o SVN automaticamente fará a fusão das versões diferentes (*merge*), contanto que as alterações se apliquem a linhas diferentes do código. Caso contrário, o Subversion mostrará um conflito, o qual deverá ser resolvido manualmente, pois o SVN é obviamente incapaz de compreender mudanças no código-fonte.

O Subclipse transfere a saída da ferramenta de linha de comando para o ambiente gráfico Eclipse; nos arquivos com alterações conflitantes, um ponto de exclamação será exibido à esquerda do nome do arquivo na lista. Ao abrir um dos arquivos, é possível ver que o SVN inseriu marcadores como `<<<<<<<.meu` ou `>>>>>>> .r7` (veja o **exemplo 3**).

No **exemplo 3**, as linhas acima dos sinais de igual refletem o conteúdo do arquivo local, enquanto que as linhas abaixo dele mostram o conteúdo da versão do repositório. O Eclipse oferece uma forma de visualização que justapõe linhas conflitantes, acessível em *Team* | *Edit conflicts* (**figura 3**). Os botões entre as duas janelas do editor com versões diferentes do código permitem a escolha de uma das duas versões. Após modificar o código,

Exemplo 1: Configuração do servidor

```
01 ### conf/svnserve.conf
02 [general]
03 password-db= senha
04 realm = exemplo de realm ### um tipo de “namespace”
05 anon-access = none ### ou ➥“read” para leitura anônima
06 auth-access = write
```

Exemplo 2: Dados de acesso

```
### conf/passwd
[users]
usuário_de_teste = senha ###
➥Usuário / Senha
```

Exemplo 3: Conflito no SVN

```
01 $nome = $_GET[‘nome’];
02 <<<<<<< .mine
03 $idade = $_GET[‘idade’];
04 =======
05 $pais = $_GET[‘pais’];
06 >>>>>>> .r7
07
08 <<<<<<< .meu
09 print “<h1>Ola, $nome. Voce
➥tem $idade anos de idade.
➥</h1>”;
10 =======
11 print “<h1>Ola, $nome. Voce
➥eh de $pais</h1>”;
12 >>>>>>> .r7
```

pode-se selecionar *Team* | *Mark as resolved* para informar ao SVN que o conflito já foi resolvido.

A função de atualização economiza o trabalho de fazer checkout do repositório inteiro sempre que for necessária uma alteração. Os arquivos só são baixados se a versão no repositório for mais nova que a cópia local em uso. Assim como na função *commit*, é possível realizar uma atualização por meio do menu no diretório que se desejar atualizar: *Team* | *Update* mostra o status mais recente. A janela *Console*, na metade inferior da janela do Eclipse, lista os arquivos alterados.

Agora, PHP

A extensão PHPEclipse, que pode ser acrescentada por meio da interface de plugins, transforma o Eclipse num ambiente de programação para PHP. Para iniciar a ferramenta de atualização, acesse o menu *Help* | *Software updates* | *Find and install*, selecione *Search for new features to install* e clique em *Next*. Depois, selecione *Add remote Site* para criar uma nova URL de download, `http://phpeclipse.sourceforge.net/update/nightly/`.

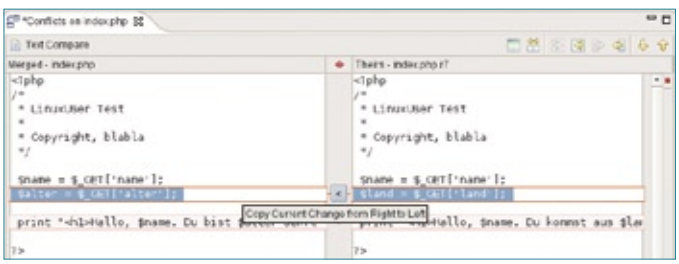


Figura 3 A visualização de conflitos auxilia na sua resolução rápida destes.

Figura 4 O *PHPEclipse* ajuda os desenvolvedores a escreverem código PHP exibindo a descrição de cada comando.

O PHPEclipse oferece tudo que um desenvolvedor precisa para a programação rápida em PHP: **[Ctrl] + [Espaço]** completa os comandos PHP (**figura 4**). Ao mesmo tempo, o Eclipse exibe um panorama dos parâmetros e valores de retorno, assim como uma curta descrição do comando. Esse recurso também funciona com variáveis anteriormente usadas. Pontos de exclamação e parênteses são fechados automaticamente. O Eclipse indenta blocos de código com instruções `if` para loops `for-next`.

O Eclipse realça comandos, funções, variáveis, cadeias de caracteres e outros elementos do código com diferentes cores. Em *Preferences* | *PHPEclipse Web Development*, é possível personalizar o esquema de cores. Esse também é o local onde se ativa a numeração de linhas. O Eclipse marca com um sinal azul as linhas que já foram editadas desde a última vez em que o arquivo foi salvo.

Sujeito a erros

Ao contrário dos erros de sintaxe, que são indicados por mensagens de erro do PHP, incluindo as linhas onde ocorrem, erros de lógica são difíceis de encontrar. O depurador interrompe o fluxo do programa em pontos pré-definidos, os *breakpoints*. O navegador mostra a saída gerada pelo script até o ponto atual e o depurador exibe os valores de todas as variáveis. É possível manipular variáveis para alterar o fluxo do programa.

Além disso, o cursor de depuração aponta diretamente para a linha do código, dando ao desenvolvedor uma ótima visão do fluxo do script. Além dos breakpoints, o depurador também suporta vários modos de uma etapa nos quais o cursor segue a seqüência de execução.

O Eclipse suporta o depurador PHP *Dbg*, disponível na forma de arquivo binário[6]. Selecione os `dbg_modules` correspondentes à versão do PHP em uso; os módulos também costumam funcionar com versões mais recentes.

Para instalar o módulo de PHP `dbg.so`, modifique o arquivo de configuração `php.ini`. Para descobrir onde o arquivo reside, crie um arquivo `teste.php` com `phpinfo()` como conteúdo e chame-o no navegador web. Em `php.ini`, encontre a variável `extension_dir`, que informa o diretório que contém os módulos de extensões PHP no sistema. Em seguida, descompacte o arquivo baixado e mova para o diretório referido o arquivo `dbg.so-x.x.x` correspondente à versão do PHP instalada, renomeando-o para simplesmente `dbg.so`.

Em `php.ini`, acrescente as seguintes linhas abaixo da posição recém-descoberta:

```
extension=dbg.so
[debugger]
debugger.enabled = true
debugger.profiler_enabled = true
debugger.JIT_host = clienthost
debugger.JIT_port = 7869
```

Depois disso, desative a extensão *Eaccelerator* (`eaccelerator.enable="0"`), caso ela exista, e comente a entrada do *XDebug* (`;zend_extension=/usr/lib/php4/20020429/xdebug.so`). Outras extensões PHP incompatíveis estão disponíveis em [7].

Mude o valor da variável `implicit_flush` para `On`. Isso faz o PHP passar conteúdo gerado dinamicamente para o servidor web antes que o script termine de rodar. A vantagem disso para a depuração é óbvia; porém, não é desejável usar essa configuração em sistemas em produção, pois ela afeta seu desempenho. Após reiniciar o ser-

vidor web, execute novamente `teste.php`. Se a saída de `phpinfo()` listar o `dbg` como uma das extensões instaladas (**figura 5**), isso significa que a instalação do depurador teve êxito.

Ainda é necessário configurar a ferramenta de depuração no Eclipse. Para isso, deve-se abri-la no menu *Run | Debug*. No painel de configurações, selecione a entrada *PHP DBG Script* e clique em *New*. São necessárias algumas configurações básicas na aba *PHP Environment*.

Na aba *Remote Debug*, marque *Remote Debug*; isso fará o depurador utilizar o servidor web para acessar as páginas. Essa é a única forma de interpretar páginas que contenham código PHP com scripts. A opção *Remote Debug* deve ser usada mesmo que o servidor esteja rodando na mesma máquina que o Eclipse. *Remote Sourcepath* precisa apontar para o diretório do projeto. Na aba *Interpreter*, digite o caminho do binário do PHP. Se ele não estiver presente, será necessário instalar o componente CGI do PHP ou compilar o PHP com suporte a CGI.

Agora selecione o projeto e o arquivo que deseja depurar na aba *File*; clique em *Apply* e feche a ferramenta de depuração, que já está totalmente configurada. Confira o código-fonte do arquivo PHP que deseja depurar e decida onde se deve investigar o processo de interpretação mais a fundo. Um duplo clique no canto esquerdo da janela do editor define um breakpoint.

Os breakpoints funcionam apenas em linhas com comandos PHP. Agora, inicie novamente o depurador (*Run | Debug*) e comece a depuração clicando em *Debug*.

No navegador web, abra o arquivo a ser depurado. Para executar o depurador, adicione `?DBGSESSID=1@cliente:10001` à linha de endereço no navegador. Essa ação é necessária apenas na primeira execução do depurador, pois ele armazenará um *cookie*. O navegador web, em seguida, deverá exibir uma página incompleta conforme os breakpoints interrompam o processamento do arquivo. Se seu gerenciador de janelas permitir, a janela do Eclipse subirá para a frente das outras. Para visualizar a saída do depurador, basta acessar o menu *Window | Open Perspective* e conferir a sessão de depuração ativa na subjanela.

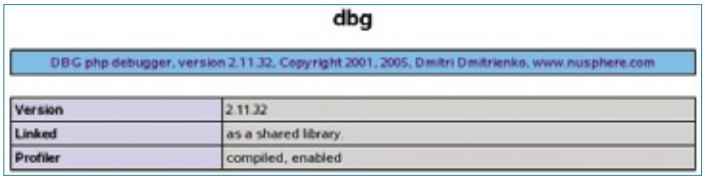


Figura 6 A saída da função `phpinfo()` mostra que o módulo do depurador foi corretamente instalado.

A janela *Variables* na perspectiva de depuração exibe todas as variáveis. Na parte de baixo da janela, pode-se conferir o conteúdo da variável e manipulá-lo se for necessário executar o resto do script com valores diferentes. Em relação a vetores, é possível visualizar os elementos e seus valores. A subjanela *Breakpoints* lista todos os breakpoints e permite que sejam temporariamente desativados.

Com um clique do botão direito na janela de depuração, é possível parar ou reiniciar uma sessão.

Caso não haja mais uma sessão ativa, o navegador exibirá uma página de erro ao serem chamadas páginas do servidor web local. Para resolver isso, basta apagar o cookie chamado *DBGSESSID*.

O depurador precisa de ao menos um breakpoint por arquivo. Caso contrário, o script de depuração será executado infinitamente. Se o objetivo for simplesmente acompanhar o funcionamento de cada etapa do código, não será necessário incluir um breakpoint em cada linha: a tecla **[F5]** executará o script linha por linha após o primeiro breakpoint. Um cursor verde mostra qual comando está em execução atualmente. Ao acompanhar o script, o depurador abre automaticamente todos os arquivos `include`. A tecla **[F6]** faz o depurador pular subestruturas para se concentrar na parte central do código. Em cada etapa, a janela *Variables* dá acesso de leitura e escrita a todas as variáveis.

Conclusões

A possibilidade de verificar o que um programa está fazendo, etapa por etapa, é muito útil para encontrar erros lógicos. Programadores excepcionais podem dizer que preferem usar suas mentes a um depurador, mas qualquer um que conheça o martírio de passar a noite inteira procurando um erro trivial ficará satisfeito com alguma ajuda.

A possibilidade de usar o controle de versões diretamente a partir da interface gráfica facilita o desenvolvimento de código. Finalmente, um editor absolutamente rico em recursos também oferece uma visão clara de sua estrutura e ajuda na escrita de código legível. ■

Mais informações

[1] Download do Eclipse: http://www.eclipse.org/downloads/

[2] Subclipse: http://subclipse.tigris.org/

[3] Livro do SVN (em inglês): http://svnbook.org/

[4] Plugins do Eclipse: http://eclipseplugincentral.com/

[5] Subversion: http://subversion.tigris.org/

[6] Dbg: http://dd.cron.ru/dbg/downloads.php

[7] Extensões do PHP incompatíveis com o Dbg: http://tinyurl.com/62a9mh

Linux.local

O maior diretório de empresas que oferecem produtos, soluções e serviços em Linux e Software Livre, organizado por Estado. Sentiu falta do nome de sua empresa aqui? Entre em contato com a gente: **11 4082-1300** *ou* **anuncios@linuxmagazine.com.br**

Fornecedor de Hardware = 1
Redes e Telefonia / PBX = 2
Integrador de Soluções = 3
Literatura / Editora = 4
Fornecedor de Software = 5
Consultoria / Treinamento = 6

Empresa	Cidade	Endereço	Telefone	Web	1	2	3	4	5	6
Ceará										
F13 Tecnologia	Fortaleza	Rua Coronel Solon, 480 – Bairro de Fátima Fortaleza - CE - CEP: 60040-270	85 3252-3836	www.f13.com.br		✔	✔		✔	✔
Espírito Santo										
Linux Shopp	Vila Velha	Rua São Simão (Correspondência), 18 – CEP: 29113-120	27 3082-0932	www.linuxshopp.com.br	✔	✔		✔	✔	
Megawork Consultoria e Sistemas	Vitória	Rua Chapot Presvot, 389 – Praia do Canto – CEP: 29055-410 sl 201, 202	27 3315-2370	www.megawork.com.br			✔		✔	✔
Spirit Linux	Vitória	Rua Marins Alvarino, 150 – CEP: 29047-660	27 3227-5543	www.spiritlinux.com.br			✔		✔	✔
Minas Gerais										
Instituto Online	Belo Horizonte	Av. Bias Fortes, 932, Sala 204 – CEP: 30170-011	31 3224-7920	www.institutoonline.com.br				✔		✔
Linux Place	Belo Horizonte	Rua do Ouro, 136, Sala 301 – Serra – CEP: 30220-000	31 3284-0575	corporate.linuxplace.com.br		✔	✔		✔	✔
Microhard	Belo Horizonte	Rua República da Argentina, 520 – Sion – CEP: 30315-490	31 3281-5522	www.microhard.com.br	✔	✔	✔		✔	✔
TurboSite	Belo Horizonte	Rua Paraíba, 966, Sala 303 – Savassi – CEP: 30130-141	0800 702-9004	www.turbosite.com.br	✔				✔	✔
Paraná										
iSolve	Curitiba	Av. Cândido de Abreu, 526, Cj. 1206B – CEP: 80530-000	41 252-2977	www.isolve.com.br		✔	✔			✔
Mandriva Conectiva	Curitiba	Rua Tocantins, 89 – Cristo Rei – CEP: 80050-430	41 3360-2600	www.mandriva.com.br			✔	✔	✔	✔
Telway Tecnologia	Curitiba	Rua Francisco Rocha 1830/71	41 3203-0375	www.telway.com.br					✔	✔
Rio de Janeiro										
Múltipla Tecnologia da Informação	Rio de Janeiro	Av. Rio Branco, 37, 14° andar – CEP: 20090-003	21 2203-2622	www.multipla-ti.com.br	✔		✔		✔	✔
NSI Training	Rio de Janeiro	Rua Araújo Porto Alegre, 71, 4º andar Centro – CEP: 20030-012	21 2220-7055	www.nsi.com.br				✔		✔
Open IT	Rio de Janeiro	Rua do Mercado, 34, Sl, 402 – Centro – CEP: 20010-120	21 2508-9103	www.openit.com.br				✔		✔
Unipi Tecnologias	Campos dos Goytacazes	Av. Alberto Torres, 303, 1ºandar – Centro – CEP: 28035-581	22 2725-1041	www.unipi.com.br			✔	✔	✔	✔
Rio Grande do Sul										
4up Soluções Corporativas	Novo Hamburgo	Pso. Calçadão Osvaldo Cruz, 54 sl. 301 CEP: 93510-015	51 3581-4383	www.4up.com.br		✔	✔		✔	✔
Definitiva Informática	Novo Hamburgo	Rua General Osório, 402 - Hamburgo Velho	51 3594 3140	www.definitiva.com.br	✔		✔		✔	✔
Solis	Lajeado	Av. 7 de Setembro, 184, sala 401 – Bairro Moinhos CEP: 95900-000	51 3714-6653	www.solis.coop.br		✔	✔	✔	✔	✔
DualCon	Novo Hamburgo	Rua Joaquim Pedro Soares, 1099, Sl. 305 – Centro	51 3593-5437	www.dualcon.com.br	✔		✔		✔	✔
Datarecover	Porto Alegre	Av. Carlos Gomes, 403, Sala 908, Centro Comercial Atrium Center – Bela Vista – CEP: 90480-003	51 3018-1200	www.datarecover.com.br	✔		✔			
LM2 Consulting	Porto Alegre	Rua Germano Petersen Junior, 101-Sl 202 – Higienópolis – CEP: 90540-140	51 3018-1007	www.lm2.com.br			✔		✔	✔
Lnx-IT Informação e Tecnologia	Porto Alegre	Av. Venâncio Aires, 1137 – Rio Branco – CEP: 90.040.193	51 3331-1446	www.lnx-it.inf.br	✔		✔		✔	✔
Plugin	Porto Alegre	Av. Júlio de Castilhos, 132, 11º andar Centro – CEP: 90030-130	51 4003-1001	www.plugin.com.br	✔		✔		✔	
TeHospedo	Porto Alegre	Rua dos Andradas, 1234/610 – Centro – CEP: 90020-008	51 3286-3799	www.tehospedo.com.br	✔	✔				
São Paulo										
Ws Host	Arthur Nogueira	Rua Jerere, 36 – Vista Alegre – CEP: 13280-000	19 3846-1137	www.wshost.com.br	✔		✔		✔	
DigiVoice	Barueri	Al. Juruá, 159, Térreo – Alphaville – CEP: 06455-010	11 4195-2557	www.digivoice.com.br	✔	✔	✔		✔	✔
Dextra Sistemas	Campinas	Rua Antônio Paioli, 320 – Pq. das Universidades – CEP: 13086-045	19 3256-6722	www.dextra.com.br			✔		✔	✔
Insigne Free Software do Brasil	Campinas	Av. Andrades Neves, 1579 – Castelo – CEP: 13070-001	19 3213-2100	www.insignesoftware.com			✔		✔	✔
Microcamp	Campinas	Av. Thomaz Alves, 20 – Centro – CEP: 13010-160	19 3236-1915	www.microcamp.com.br				✔		✔
PC2 Consultoria em Software Livre	Carapicuiba	Rua Edeia, 500 - CEP: 06350-080	11 3213-6388	www.pc2consultoria.com	✔					✔
Savant Tecnologia	Diadema	Av. Senador Vitorino Freire, 465 – CEP: 09910-550	11 5034-4199	www.savant.com.br	✔	✔	✔			✔
Epopéia Informática	Marília	Rua Goiás, 392 – Bairro Cascata – CEP: 17509-140	14 3413-1137	www.epopeia.com.br						✔
Redentor	Osasco	Rua Costante Piovan, 150 – Jd. Três Montanhas – CEP: 06263-270	11 2106-9392	www.redentor.ind.br	✔					
Go-Global	Santana de Parnaíba	Av. Yojiro Takaoca, 4384, Ed. Shopping Service, Cj. 1013 – CEP: 06541-038	11 2173-4211	www.go-global.com.br			✔		✔	✔
AW2NET	Santo André	Rua Edson Soares, 59 – CEP: 09760-350	11 4990-0065	www.aw2net.com.br			✔		✔	✔
Async Open Source	São Carlos	Rua Orlando Damiano, 2212 – CEP 13560-450	16 3376-0125	www.async.com.br	✔				✔	✔

Empresa	Cidade	Endereço	Telefone	Web	1	2	3	4	5	6
São Paulo (continuação)										
Delix Internet	São José do Rio Preto	Rua Voluntário de São Paulo, 3066 9º – Centro – CEP: 15015-909	11 4062-9889	www.delixhosting.com.br	✔		✔		✔	
4Linux	São Paulo	Rua Teixeira da Silva, 660, 6º andar – CEP: 04002-031	11 2125-4747	www.4linux.com.br					✔	✔
A Casa do Linux	São Paulo	Al. Jaú, 490 – Jd. Paulista – CEP: 01420-000	11 3549-5151	www.acasadolinux.com.br			✔		✔	✔
Accenture do Brasil Ltda.	São Paulo	Rua Alexandre Dumas, 2051 – Chácara Santo Antônio – CEP: 04717-004	11 5188-3000	www.accenture.com.br			✔		✔	✔
ACR Informática	São Paulo	Rua Lincoln de Albuquerque, 65 –Perdizes – CEP: 05004-010	11 3873-1515	www.acrinformatica.com.br	✔					✔
Agit Informática	São Paulo	Rua Major Quedinho, 111, 5º andar, Cj. 508 – Centro – CEP: 01050-030	11 3255-4945	www.agit.com.br	✔	✔				✔
Altbit - Informática Comércio e Serviços LTDA.	São Paulo	Av. Francisco Matarazzo, 229, Cj. 57 – Água Branca – CEP 05001-000	11 3879-9390	www.altbit.com.br	✔		✔		✔	✔
AS2M -WPC Consultoria	São Paulo	Rua Três Rios, 131, Cj. 61A – Bom Retiro – CEP: 01123-001	11 3228-3709	www.wpc.com.br			✔		✔	✔
Big Host	São Paulo	Rua Dr. Miguel Couto, 58 – Centro – CEP: 01008-010	11 3033-4000	www.bighost.com.br	✔				✔	✔
Blanes	São Paulo	Rua André Ampére, 153 – 9º andar – Conj. 91 CEP: 04562-907 (próx. Av. L. C. Berrini)	11 5506-9677	www.blanes.com.br	✔	✔	✔		✔	✔
Commlogik do Brasil Ltda.	São Paulo	Av. das Nações Unidas, 13.797, Bloco II, 6º andar – Morumbi – CEP: 04794-000	11 5503-1011	www.commlogik.com.br	✔	✔	✔		✔	✔
Computer Consulting Projeto e Consultoria Ltda.	São Paulo	Rua Vergueiro, 6455, Cj. 06 – Alto do Ipiranga – CEP: 04273-100	11 5062-3927	www.computerconsulting.com.br	✔		✔		✔	✔
Consist Consultoria, Sistemas e Representações Ltda.	São Paulo	Av. das Nações Unidas, 20.727 – CEP: 04795-100	11 5693-7210	www.consist.com.br			✔	✔	✔	✔
Domínio Tecnologia	São Paulo	Rua das Carnaubeiras, 98 – Metrô Conceição – CEP: 04343-080	11 5017-0040	www.dominiotecnologia.com.br	✔					✔
EDS do Brasil	São Paulo	Av. Pres. Juscelino Kubistcheck, 1830 Torre 4 - 5º andar	11 3707-4100	www.eds.com		✔	✔			✔
Ética Tecnologia	São Paulo	Rua Nova York, 945 – Brooklin – CEP:04560-002	11 5093-3025	www.etica.net	✔		✔		✔	✔
Getronics ICT Solutions and Services	São Paulo	Rua Verbo Divino, 1207 – CEP: 04719-002	11 5187-2700	www.getronics.com/br			✔		✔	✔
Hewlett-Packard Brasil Ltda.	São Paulo	Av. das Nações Unidas, 12.901, 25º andar – CEP: 04578-000	11 5502-5000	www.hp.com.br	✔		✔	✔	✔	✔
IBM Brasil Ltda.	São Paulo	Rua Tutóia, 1157 – CEP: 04007-900	0800-7074 837	www.br.ibm.com	✔		✔		✔	✔
iFractal	São Paulo	Rua Fiação da Saúde, 145, Conj. 66 – Saúde – CEP: 04144-020	11 5078-6618	www.ifractal.com.br			✔		✔	✔
Integral	São Paulo	Rua Dr. Gentil Leite Martins, 295, 2º andar Jd. Prudência – CEP: 04648-001	11 5545-2600	www.integral.com.br	✔				✔	
Itautec S.A.	São Paulo	Rua Santa Catarina, 1 – Tatuapé – CEP: 03086-025	11 6097-3000	www.itautec.com.br	✔	✔	✔		✔	✔
Kenos Consultoria	São Paulo	Av: Fagundes Filho, 13, Conj -53 – CEP: 04304-000	11 40821305	www.kenos.com.br					✔	✔
Konsultex Informatica	São Paulo	Av. Dr. Guilherme Dumont Villares, 1410 6 andar, CEP: 05640-003	11 3773-9009	www.konsultex.com.br			✔		✔	✔
Linux Komputer Informática	São Paulo	Av. Dr. Lino de Moraes Leme, 185 – CEP: 04360-001	11 5034-4191	www.komputer.com.br	✔		✔		✔	✔
Linux Mall	São Paulo	Rua Machado Bittencourt, 190, Cj. 2087 – CEP: 04044-001	11 5087-9441	www.linuxmall.com.br	✔			✔	✔	
Livraria Tempo Real	São Paulo	Al. Santos, 1202 – Cerqueira César – CEP: 01418-100	11 3266-2988	www.temporeal.com.br				✔	✔	✔
Locasite Internet Service	São Paulo	Av. Brigadeiro Luiz Antonio, 2482, 3º andar – Centro – CEP: 01402-000	11 2121-4555	www.locasite.com.br	✔				✔	✔
Microsiga	São Paulo	Av. Braz Leme, 1631 – CEP: 02511-000	11 3981-7200	www.microsiga.com.br			✔		✔	✔
Novatec Editora Ltda.	São Paulo	Rua Luis Antonio dos Santos, 110 – Santana – CEP: 02460-000	11 6979-0071	www.novateceditora.com.br				✔		
Novell América Latina	São Paulo	Rua Funchal, 418 – Vila Olímpia	11 3345-3900	www.novell.com/brasil			✔		✔	✔
Oracle do Brasil Sistemas Ltda.	São Paulo	Av. Alfredo Egídio de Souza Aranha, 100 – Bloco B – 5º andar – CEP: 04726-170	11 5189-3000	www.oracle.com.br					✔	✔
Proelbra Tecnologia Eletrônica Ltda.	São Paulo	Av. Rouxinol, 1.041, Cj. 204, 2º andar Moema – CEP: 04516-001	11 5052- 8044	www.proelbra.com.br	✔		✔			✔
Provider	São Paulo	Av. Cardoso de Melo, 1450, 6º andar – Vila Olímpia – CEP: 04548-005	11 2165-6500	www.e-provider.com.br			✔		✔	✔
Red Hat Brasil	São Paulo	Av. Brigadeiro Faria Lima, 3900, Cj 81 8º andar Itaim Bibi – CEP: 04538-132	11 3529-6000	www.redhat.com.br			✔		✔	✔
Samurai Projetos Especiais	São Paulo	Rua Barão do Triunfo, 550, 6º andar – CEP: 04602-002	11 5097-3014	www.samurai.com.br			✔		✔	✔
SAP Brasil	São Paulo	Av. das Nações Unidas, 11.541, 16º andar – CEP: 04578-000	11 5503-2400	www.sap.com.br			✔		✔	✔
Simples Consultoria	São Paulo	Rua Mourato Coelho, 299, Cj. 02 Pinheiros – CEP: 05417-010	11 3898-2121	www.simplesconsultoria.com.br			✔		✔	✔
Smart Solutions	São Paulo	Av. Jabaquara, 2940 cj 56 e 57	11 5052-5958	www.smart-tec.com.br		✔	✔		✔	✔
Snap IT	São Paulo	Rua João Gomes Junior, 131 – Jd. Bonfiglioli – CEP: 05299-000	11 3731-8008	www.snapit.com.br			✔		✔	✔
Stefanini IT Solutions	São Paulo	Av. Brig. Faria Lima, 1355, 19º – Pinheiros – CEP: 01452-919	11 3039-2000	www.stefanini.com.br			✔		✔	✔
Sun Microsystems	São Paulo	Rua Alexandre Dumas, 2016 – CEP: 04717-004	11 5187-2100	www.sun.com.br	✔		✔		✔	✔
Sybase Brasil	São Paulo	Av. Juscelino Kubitschek, 510, 9º andar Itaim Bibi – CEP: 04543-000	11 3046-7388	www.sybase.com.br					✔	✔
The Source	São Paulo	Rua Marquês de Abrantes, 203 – Chácara Tatuapé – CEP: 03060-020	11 6698-5090	www.thesource.com.br			✔		✔	✔
Unisys Brasil Ltda.	São Paulo	R. Alexandre Dumas 1658 – 6º, 7º e 8º andares – Chácara Santo Antônio – CEP: 04717-004	11 3305-7000	www.unisys.com.br	✔		✔		✔	✔
Utah	São Paulo	Av. Paulista, 925, 13º andar – Cerqueira César – CEP: 01311-916	11 3145-5888	www.utah.com.br			✔		✔	✔
Visuelles	São Paulo	Rua Eng. Domicio Diele Pacheco e Silva, 585 – Interlagos – CEP: 04455-310	11 5614-1010	www.visuelles.com.br			✔		✔	✔
Webnow	São Paulo	Av. Nações Unidas, 12.995, 10º andar, Ed. Plaza Centenário – Chácara Itaim – CEP: 04578-000	11 5503-6510	www.webnow.com.br	✔		✔		✔	
WRL Informática Ltda.	São Paulo	Rua Santa Ifigênia, 211/213, Box 02– Centro – CEP: 01207-001	11 3362-1334	www.wrl.com.br	✔		✔		✔	
Systech	Taquaritinga	Rua São José, 1126 – Centro - Caixa Postal 71 – CEP: 15.900-000	16 3252-7308	www.systech-ltd.com.br	✔	✔			✔	

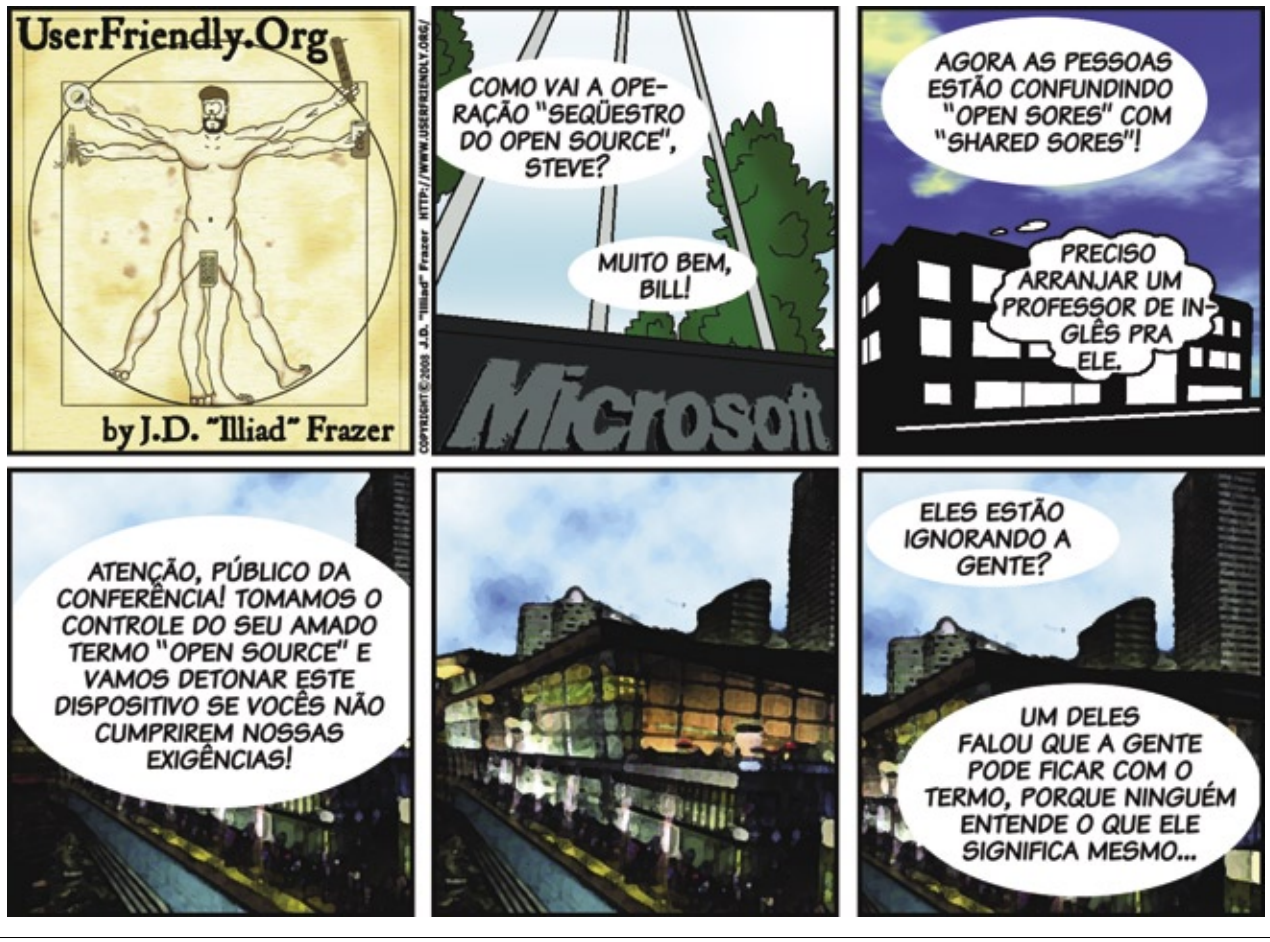
Calendário de eventos

Evento	Data	Local	Website
CESol	19 a 23 de agosto	Fortaleza, CE	www.cesol.ufc.br
PyConBrasil 2008	18 a 20 de setembro	Rio de Janeiro, RJ	www.pyconbrasil.com.br
Conisli	18 e 19 de outubro	São Paulo, SP	www.conisli.org
Futurecom 10	27 a 30 de outubro	São Paulo, SP	www.futurecom2008.com.br

Índice de anunciantes

Empresa	Pág.
Bull	2, 15
Itautec	13
Kenos	7, 22
Senac	83
Futurecom	31
Linux Pro	65
LPI	19
Linux Technical Review	81
Propus	9
Plugin	39
Locaweb	84
Planeta Digital	27
Guia de TI	55
Pocket Pro	25
CESol	21

User Friendly – Os quadrinhos mensais da Linux Magazine



PREVIEW

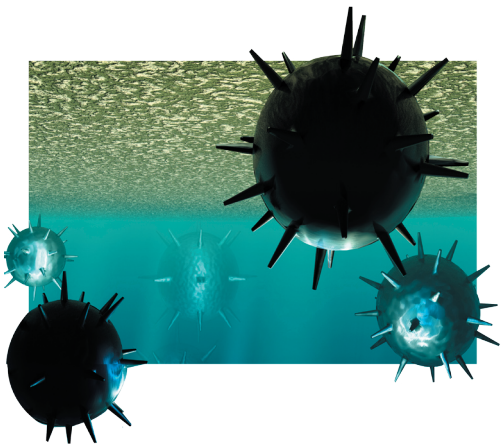
Na Linux Magazine #46

DESTAQUE

Invasores

Cena do crime: a sala dos servidores. O ladrão não precisa de chave ou crachá, nem mesmo da proteção da noite – um invasor pode usar a Internet para ir e vir. Porém, apesar da entrada secreta, o invasor ainda deixa um rastro. Encontrar e interpretar essas provas deve ser a maior prioridade de investigadores criminais.

Na próxima edição da Linux Magazine, vamos explorar o campo da computação forense. Mostraremos algumas ferramentas usadas pelos especialistas para encontrar vestígios, recuperar dados apagados e descobrir provas ocultas. Quem desejar se embrenhar nessa área terá a ajuda de várias ferramentas de código aberto, como a *Open Computer Forensics Architecture* e o conjunto de ferramentas *Sleuth Kit*, por exemplo.



Porém, se você deseja apenas realizar uma ação pontual sem grande importância, provavelmente essas ferramentas de investigação são um exagero. Nesse caso, mostraremos também como solucionar mistérios menos sofisticados com o uso de ferramentas comuns do Linux. ■

SEGURANÇA

ACLs

O sistema legado de permissões de arquivos do Linux são antigos. Isso, por si só, não é intrinsecamente ruim. Porém, as necessidades atuais de ajustes finos nas permissões do sistema de arquivos impõem dificuldades que o sistema legado não tem capacidade de transpor.

Um exemplo simples envolve a necessidade de se conceder permissão de escrita para um arquivo a um único usuário do sistema (além do dono do arquivo, obviamente). É claro que poderíamos incluir o usuário no grupo do dono do arquivo, mas isso implicaria a concessão da permissão de escrita a esse mesmo usuário para qualquer outro arquivo com um `w` na posição do grupo.

Ainda nesse caso, um grupo temporário pode resolver, mas essa solução não é prática no contexto de uma empresa.

As ACLs, ou *Access Control Lists*, são a solução mais promissora. Elas acrescentam flexibilidade ao sistema de permissões do Unix e permitem uma regulagem muito mais precisa sobre os privilégios de acesso dos usuários a arquivos. ■

Na EasyLinux #13

DESTAQUE

Portáteis!

Os laptops e os notebooks sempre deram aos seus possuidores um certo glamour, status de pessoas antenadas e, claro, fama de gente que tinha "grana" – afinal, um bom portátil, até dois anos atrás, não custava nada barato. Com o passar do tempo, no entanto, fabricantes foram criando uma nova geração de notebooks: menores, sem partes mecânicas quebráveis em boa parte de suas versões e mais baratos. Esses aparelhinhos, chamados de sub-notebooks, vêm ganhando espaço, tanto entre os clientes "tradicionais" dos laptops quanto entre pessoas que jamais imaginaram ter um portátil. ■

OFICINA

Com jeito de cinema

A qualidade de aúdio e vídeo da TV digital, recentemente iniciada no Brasil, é um atrativo para quem deseja assistir a programas em alta resolução e até gravar alguns de seus preferidos. Se os receptores de TV ainda estão muito caros, receptores USB para computador oferecem a imagem de cinema e qualidade de som de DVD. E, o que é melhor, usando Linux. ■

Rails Summit Latin America

by LOCAWEB

OS MAIORES NOMES DO MUNDO EM RAILS ESTARÃO AQUI.

A Locaweb realiza no Brasil o Rails Summit Latin America, que completa o calendário de eventos Rails no mundo. São mais de 10 palestrantes internacionais e os melhores especialistas brasileiros reunidos durante dois dias para trocar informações e novidades sobre Ruby on Rails.

DAVID HEINEMEIR HANSSON - videoconferência
Criador do Ruby on Rails e sócio da 37signals, Hansson mudou a forma de pensar o desenvolvimento de aplicações em web, definindo a essência de produtos Web 2.0 com Ruby on Rails.

CHAD FOWLER
Responsável pelas atuais conferências RubyConf nos Estados Unidos, Fowler é um dos fundadores da organização RubyCentral e ajudou efetivamente a elevar a qualidade da comunidade Ruby.

OBIE FERNANDEZ
Participante ativo da comunidade Rails on Ruby, Fernandez foi consultor da renomada ThoughtWorks e criou recentemente a HashRocket. Também lançou o livro *The Rails Way*, um dos melhores sobre o assunto.

FABIO AKITA
Escritor do primeiro livro original em português sobre Rails, Akita é Gerente de Produtos Rails na Locaweb e um dos maiores difusores do tema no país.

CHARLES NUTTER E THOMAS ENEBO
Criadores do projeto JRuby, Nutter e Enebo são engenheiros da Sun e com seu trabalho alcançaram um nível de produtividade e integração sem precedentes no mundo Java.

SÃO PAULO, 15 E 16 DE OUTUBRO – ANHEMBI – AUDITÓRIO ELIS REGINA

VAGAS LIMITADAS. INSCREVA-SE JÁ.

Realização: LOCAWEB

www.locaweb.com.br/rails