LINUX NEW MEDIA
The Pulse of Open Source

SANEADA PELO LINUX P.22
Linux na Companhia de Águas do Maranhão

BOCA NO TROMBONE P.25
Maddog explica como fazer sua parte nas políticas públicas

LEI DOS CALL CENTERS P.26
Edgar Silva mostra como a nova lei requer TI

50 Janeiro 2009

LINUX MAGAZINE

A REVISTA DO PROFISSIONAL DE TI

Interoperabilidade

SUPORTANDO O VISTA

AS REDES ATUAIS SÃO AMBIENTES HETEROGÊNEOS. O BOM ADMINISTRADOR PRECISA SABER PROMOVER A INTEROPERABILIDADE ENTRE LINUX E WINDOWS p.27

» Conecte o Linux à VPN do Windows p.28
» MS AD e clientes Linux: a solução definitiva p.34
» Linux como servidor RDP p.40
» Agendamento de tarefas livre também no Windows p.44

SEGURANÇA: BIOMETRIA p.72
A autenticação por impressão digital já é realidade. Aprenda a implementá-la com um especialista

REDES: OPENID p.68
Uma única identidade para vários serviços na Web. Mas como fica a segurança?

VEJA TAMBÉM NESTA EDIÇÃO:

» MIDs: será que a moda pega? p.17
» Faça gráficos pelo Google p.50
» HA e PostgreSQL: uma ótima mistura p.54
» ETL muito competente com o Talend p.62

9 771806 942009 00050
#50 01/09
R$ 14,90
€ 7,50

Campus Party™

Inscrições Abertas

São Paulo, 19 a 25 de janeiro de 2009

Venha compartilhar su paixão pela tecnologia

Quatro mil computadores conectados em rede na maior festa da tecnologia e entretenimento digital que você já imaginou.

Venha à Campus Party e aproveite uma semana de intensa emoções. **Não fique fora dessa! Inscreva-se**

www.campusparty.com.br

Patrocinador Principal Realização Patrocinadores Institucionais

Telefônica Futura™ Networks PREFEITURA DA CIDADE DE SÃO PAULO GOVERNO DO ESTADO DE SÃO PAULO BRASIL UM PAÍS DE TODOS GOVERNO FEDERAL

Expediente editorial

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

Editor
Pablo Hess
phess@linuxmagazine.com.br

Revisora
Aileen Otomi Nakamura
anakamura@linuxmagazine.com.br

Editora de Arte
Paola Viveiros
pviveiros@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
Claudio Bazzoli
cbazzoli@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

Impressão e Acabamento: Parma
Distribuída em todo o país pela Dinap S.A.,
Distribuidora Nacional de Publicações, São Paulo.

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

Software natural

Prezados leitores,

Muitos de vocês provavelmente já tiveram a experiência de tentar explicar a outras pessoas o conceito de Software Livre. Recentemente, tomei conhecimento da iniciativa da Fundação Mozilla de adotar um novo nome – software natural – para designar os softwares produzidos por ela, e creio que essa pequena diferença pode facilitar significativamente a compreensão dos princípios do Software Livre pelo público em geral.

Para explicar a alguém do ramo técnico os preceitos do Software Livre, o maior desafio é esclarecer como uma empresa pode ganhar dinheiro sem vender seu software, e isso muitas vezes se mostra difícil o suficiente. Para interlocutores não técnicos, é difícil imaginar como liberdade pode ser associada a um programa, pois "software" e "livre", para essas pessoas, se relacionam tanto quanto "pedra" e "satisfeita", por exemplo.

Quando olho para essa tarefa por vezes tão complicada, lamento a infelicidade de quem tenta explicar o termo em inglês – "free software" – que traz à mente o sentido de gratuidade em vez de liberdade, e por isso exige a complementação "free as in freedom". Estranhamente, já ouvi de muitos executivos que pareciam entender o conceito de software livre frases como "aquele software é free", o que introduz um novo elemento de dúvida para quem escuta: trata-se de liberdade ou gratuidade?

Com o novo "software natural" da Fundação Mozilla, a compreensão do conceito por qualquer pessoa é muito mais prática. O termo "natural" traz, com facilidade, a idéia de uma fruta. Para colhermos uma laranja, precisamos plantar uma laranjeira antes. Embora colher a laranja até seja grátis – assim como o software natural –, isso não significa que o processo todo teve custo zero. No mínimo, levou tempo para se realizar, ainda que não se tenha gasto dinheiro com adubo, sementes, água ou manutenção da terra. Alternativamente, a laranja – ainda natural – pode ser comprada no mercado ou feira mais próximos.

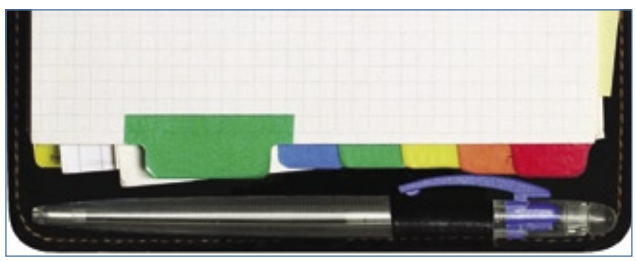
"Natural" também possui conotação positiva: alimentos naturais fazem bem à saúde e medicamentos naturais tendem a ter menos efeitos colaterais.

Quanto mais penso no adjetivo "natural" para o software, mais me convenço da escolha acertada da Fundação Mozilla. Minha lista de argumentos em favor do novo nome é infindável.

A quem questiona a relevância de um aspecto aparentemente tão inócuo quanto um nome, lembro que CIOs são pessoas, assim como usuários finais, e todos estamos sujeitos àquele primeiríssimo julgamento, por vezes completamente inconsciente, de qualquer objeto, pessoa ou fenômeno com base em seu nome. Naturalmente. ■

Pablo Hess
Editor

CAPA

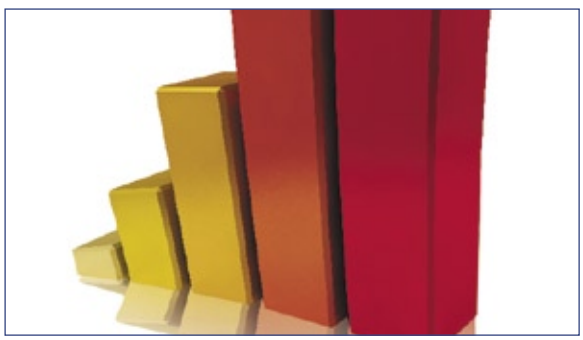


COLUNAS

NOTÍCIAS

CORPORATE

TUTORIAL



ANÁLISE

REDES

SEGURANÇA

SERVIÇOS

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.*

Gestão empresarial

Primeiramente gostaria de parabenizá-los pela revista, que possui ótimo conteúdo, poucas propagandas e é muito objetiva em suas matérias.

Já estive pesquisando, porém, é muito difícil encontrar sistemas para gerenciamento de empresas, como contas a pagar, a receber, controle de estoque etc. Este é, acredito eu, um dos maiores problemas para conseguirmos migrar os nossos clientes para a plataforma Linux.

Gostaria de pedir à Linux Magazine que, se possível, indicasse algumas opções de softwares (livres ou não) para gestão de empresas, para que pudéssemos analisá-los.

Ivan Moretto
Leme, SP

Resposta

Prezado Ivan, muito obrigado pelos elogios. É sempre muito gratificante receber o reconhecimento por parte de nossos leitores. Mas, por favor, não hesite em nos informar também o que poderia ser melhorado na Linux Magazine.

Sobre a sua questão, já publicamos duas edições (39 e 30) sobre esses sistemas, chamados ERP (do inglês "Enterprise Resource Planning" – Planejamento de Recursos da Empresa).

Como você pode conferir na listagem das matérias de capa dessas edições, há diversos sistemas ERP (proprietários ou de código aberto) para Linux, com destaque para Adempiere, Compiere e Openbravo – por sinal, todos os três têm o código aberto. ■

COLUNA

Pergunte ao Klaus!

Klaus Knopper

O professor Klaus responde as mais diversas dúvidas dos leitores.

Espaço na tela

Há uns dois anos eu comprei um PC bem básico com chip gráfico *onboard*. Pluguei nele um monitor LCD de 19 polegadas (1280x1024), mas troquei-o por um de 22 polegadas (1680x1050) um ano depois. No *Centro de Controle* do KDE, selecionei a resolução de 1680x1050, mas agora ele exibe e usa 1680x1200.

Como meu monitor não suporta essa resolução, é como se meu monitor estivesse "flutuando" sobre a área de trabalho: quando chego o mouse perto da base do monitor, ele desliza a imagem para baixo, mostrando a barra inferior do KDE e escondendo os 150 pixels lá de cima.

Eu gosto desse comportamento, pois os programas costumam ter seus menus na parte de cima da janela, então eu não preciso descer para a base com freqüência. Além disso, a base se torna um bom local para eu jogar janelas que não quero visualizar no momento.

Minha dúvida é se essa nova configuração é causada por um problema de driver ou se eu encontrei um recurso do X.org que é comum mas pouco usado.

Testei recentemente o Fedora 8 e ele reconhece automaticamente o tamanho do monitor. Às vezes eu sinto falta dos 150 pixels de altura que sobram para baixo. Existe alguma forma de recuperá-los?

Resposta

Os "150 pixels ocultos" de fato são causados por um recurso do servidor X. Se o tamanho da tela for configurado como 1680x1050, o Xorg entrará no modo de deslizamento (*scrolling mode*).

Novas versões do Xorg substituem esse recurso pela alteração da **resolução da área de trabalho** usando a extensão *randr*. A vantagem é que a área de trabalho ajusta seu tamanho automaticamente ao se alterar a resolução.

Além disso, alternar entre diferentes dispositivos de saída é mais fácil (por exemplo, conectar um projetor com uma resolução diferente ou usar no monitor interno a resolução do externo). O Xorg carrega automaticamente a extensão *randr* e depois as configurações de *Modes* no arquivo `/etc/X11/xorg.conf` são ignoradas em favor do que o monitor especifica como resolução favorita.

É possível fazer o Xorg alterar sua resolução dinamicamente usando o *krandtray* (no KDE) ou o comando `xrandr` (na linha de comando). Por exemplo:

```
# xrandr --output LVDS --auto
```

tentará alinhar automaticamente a resolução do servidor X à do monitor, enquanto:

```
# xrandr --output LVDS --mode 800x600
```

ou

```
# xrandr --output LVDS -s 800x600
```

usará o modo ou resolução para o tamanho de 800x600 especificado no comando, o que também faz certos ambientes desktop adotarem um tamanho de tela diferente.

```
# xrandr --output VGA --auto
```

deve ativar a porta VGA externa de um notebook e também fazer o desktop adotar a resolução preferida do monitor ou projetor ligado a essa porta.

No seu caso, para retornar ao comportamento original com 150 pixels "sobrando" (desativando o *randr* no Xorg), basta adicionar a seguinte seção ao seu arquivo `/etc/X11/xorg.conf`:

```
Section "ServerFlags"
    Option "RandR" "false"
EndSection
```

Escreva para o Klaus

Envie suas perguntas em português ou inglês para `klaus@linuxmagazine.com.br` e tire todas as suas dúvidas.

COLUNA

Siege

Charly Kühnast

O cerco a Tróia durou dez anos e terminou somente quanto Ulisses introduziu um cavalo de madeira dentro da cidade. Charly também está planejando um cerco, e o alvo é seu próprio servidor web. Naturalmente, ele não tem dez anos para completar essa tarefa, nem Ulisses como parte de sua equipe.

Estava checando meu servidor Apache e me lembrei do mito do monstro marinho Cila, que deu cabo de nada menos que seis homens de Ulisses voltando de Tróia a caminho de casa. O módulo de multi-processamento – *MPM worker* – do meu servidor também é capaz de devorar múltiplas requisições numa talagada só, mas até onde ele agüenta? Quantas *threads* eu preciso configurar para conseguir que ele entregue o máximo de desempenho? E a partir de quantas threads isso se torna um desperdício?

Teste de carga

Usando a ferramenta de ataque *Siege* [1], vou tentar responder essas questões por meio de um teste de carga. O programa contempla dois modos de ataque: o primeiro simula o comportamento de um ser humano navegando na Internet, o que explica o intervalo de três segundos entre cada dois acessos. No segundo, conhecido como modo *benchmark*, esses intervalos são eliminados e a ferramenta faz solicitações ao servidor ininterruptamente. Para fazer o servidor "suar", o Siege dispõe de um exército de usuários de contingente configurável – dez por padrão, mas é possível usar o parâmetro a seguir para aumentar o tamanho da tropa até que o servidor web peça misericórdia e nossos agressores consumam todos os recursos do sistema:

```
--concurrent=<número>
```

Como entrar em Tróia?

Como o Siege sabe qual servidor atacar? Há duas opções para isso: o parâmetro:

```
--url="http://<meu.site.com>/<index.html>"
```

permite que você forneça a URL que o programa solicitará repetidamente. Já a opção:

```
--file="/home/charly/siege-urls.txt"
```

é mais interessante, pois permite a criação de uma seqüência arbitrariamente longa de endereços web para o Siege atacar. O parametro `--reps=<número>` permite especificar quantas vezes o programa deverá repetir o teste de carga.

Também é possível usar o parâmetro `--internet` para dizer ao Siege para não realizar as requisições na ordem especificada no arquivo `siege-urls.txt`, mas fazê-lo de maneira aleatória, o que é muito mais próximo da realidade.

Fim da batalha

Para evitar que o teste de carga se estenda indefinidamente, é prudente utilizar o parâmetro `--time` para limitar seu tempo de execução. O ataque cessará ao final do tempo indicado, mesmo que a quantidade de execuções especificada pelo parâmetro `--rep` ainda não tenha sido atingida.

Após sua execução ter sido completada, o Siege mostra um resumo dos resultados encontrados (veja a **figura 1**). ■

```
File  Edit  View  Terminal  Tabs  Help
Transactions:                2566135 hits
Availability:                 100.00 %
Elapsed time:                1800.48 secs
Data transferred:           16593.17 MB
Response time:                  0.07 secs
Transaction rate:            1425.25 trans/sec
Throughput:                     9.22 MB/sec
Concurrency:                   99.40
Successful transactions:     2566014
Failed transactions:               0
Longest transaction:            9.01
Shortest transaction:           0.00

                                                14,0-1        Top
```

Figura 1 Após a batalha contra o servidor web, o Siege apresenta os resultados.

Mais informações

[1] Siege: http://www.joedog.org/JoeDog/Siege

QUER VENDER PELA INTERNET E NÃO SABE POR ONDE COMEÇAR?

a partir de R$ 49,00 por mês

FALE COM O UOL.

0800 723 6000
www.uol.com.br/host

LOJA VIRTUAL UOL HOST

Solução fácil e descomplicada para empresas de qualquer tamanho colocarem seus produtos à venda na internet.

UOL HOST
QUALIDADE EM SERVIÇOS WEB

COLUNA

Crônicas do kernel

Zack Brown

Os acontecimentos mais recentes na história do kernel.

Erradicação do Big Lock

Frederic Weisbecker criou o *Big Kernel Lock Tracer* (rastreador do *Big Lock* – grande bloqueio – do kernel), que rastreia os tempos de atraso causados pelo Big Kernel Lock, ou BKL. Isso pode ajudar a identificar áreas específicas nas quais o BKL deveria ser eliminado primeiro. Linus Torvalds sugeriu livrar-se do BKL e substituí-lo por estruturas de bloqueio mais simples. Entretanto, nem todas as situações podem ser resolvidas com um bloqueio genérico, e o código de bloqueio está espalhado por todo o kernel, o que dificulta qualquer tipo de esforço conjunto. Uma tentativa no momento é "empurrar" todo o código do BKL para sua própria parte da árvore do kernel para centralizá-lo de forma a tratá-lo de uma só vez. Os participantes de todo o espectro do desenvolvimento do kernel estão imbuídos da missão de procurar e destruir o BKL há meses, mas ainda falta bastante trabalho. A ferramenta de Frederic pode ajudar os desenvolvedores a concentrar sua atenção em áreas que beneficiariam a maioria.

> ***"Os participantes de todo o espectro do desenvolvimento do kernel estão imbuídos da missão de procurar e destruir o BKL há meses, mas ainda falta bastante trabalho."***

Redefinindo Load Average

Sena Senerviratne e David Levy estão preparando algumas mudanças para o cálculo do valor de *load average* (carga média) no Linux. Sua idéia é, em vez de calcular apenas um único número para representar toda a carga média do sistema, fornecer múltiplas estatísticas. Por exemplo, eles querem separar do resto do sistema a carga de I/O de disco, para visualizarem esse dado independentemente. Além disso, desejam ativar o cálculo de load average por usuário, para que cada usuário visualize os efeitos sobre o seu sistema. Arjan van de Ven pediu encarecidamente que eles apenas acrescentem estatísticas, sem alterar o comportamento dos números que o sistema já produz.

Mantenedores

Theodore (Ted) Y. Ts'o atualizou o arquivo `MAINTAINERS`, listando-se como mantenedor do sistema de arquivos *Ext4*, no lugar de Andrew Morton e Stephen Tweedie, embora isso não represente uma mudança real de mantenedor. De acordo com Ted, a entrada originalmente foi simplesmente copiada daquela do *Ext3* e jamais foi precisa, o que seu *patch* agora corrigiu.

Um detalhe interessante é que embora Andreas Dilger não esteja incluído como co-mantenedor no patch de Ted, a lista de emails para submissão de patches, relatórios de bug etc. inclui o email de Andreas junto com o de Ted. O email de Andreas também está listado junto com o de Andrew e Stephen na entrada original equivocada. Geralmente, isso significaria que ele dedica muito trabalho ao projeto e pode atuar como "tenente" de Ted, da mesma forma que Linus Torvalds confia em seus "tenentes" para facilitar seu trabalho de inclusão de códigos no kernel.

Mike Frysinger postou um patch para o arquivo `MAINTAINERS` listando a si mesmo e Subrata Modak como co-mantenedores do LTP (*Linux Test Project*). Esse projeto patrocinado pela SGI e IBM oferece um conjunto de aproximadamente 3 mil testes para avaliar a confiabilidade, robustez e estabilidade do sistema operacional Linux. ■

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.

Reduza os custos de comunicação usando Scalix

- aberto
- sem barreiras
- seguro
- flexível

O Scalix é uma solução completa para mensagens, que suporta múltiplos servidores e atende às necessidades de sua empresa. Não importa o tamanho dela. Baseia-se em uma Plataforma Colaborativa que serve de fundação para todas as edições desse produto.

Maiores informações: www.sentegrity.com.br
EUA 646-747-7648 | São Paulo 11 5105-9037 | Rio de Janeiro 21 3576-7282

SCALIX™

COLUNA

A quarta geração dos rootkits se baseia no hardware e é quase indetectável

Insegurança

Analisamos a história dos rootkits, incluindo a sua mais nova encarnação: o DR RootKit.

por Kurt Seifried

Originalmente eu pretendia escrever um artigo sobre o estado da arte dos rootkits e as ferramentas que poderiam ser usadas para detectá-los. Foi aí que acabei topando com um probleminha: os rootkits mais avançados e modernos tendem a ser realmente bons em evitar sua detecção. Com "realmente bons" quero dizer que será improvável para qualquer um detectá-los, a menos que se lance mão de técnicas como a análise detalhada de uma cópia (*dump*) da memória, por exemplo, comparando-se a partir daí a imagem real do kernel carregada na memória com aquela que seria de se esperar.

Lições históricas

Rootkits tradicionais são programas simples, geralmente rodando como um serviço isolado e fornecendo acesso a uma *backdoor*. Eles são relativamente fáceis de detectar, bastando para isso procurar novos processos ou programas recentemente instalados. Isso levou os agressores a começar a sobrescrever os programas executáveis do sistema. Via de regra, esses programas são substituídos por versões modificadas pelo agressor, tais como versões do OpenSSH com nome e senha do administrador embutidas diretamente no programa, com o intuito de escalar privilégios e obter direitos de root no sistema. O advento de ferramentas como o *Tripwire* e o uso cada vez mais comum de gerenciadores de pacotes com a capacidade de verificar a integridade dos arquivos instalados no sistema – tais como rpm e dpkg – acabou por facilitar a detecção desse tipo de rootkit também [1].

Rootkits para o kernel

Não demorou muito para que os agressores percebessem que métodos mais sofisticados de ocultação e subversão eram necessários para controlar um sistema, o que levou à criação de rootkits para o kernel. Assim, ao modificar a tabela de camadas do sistema, um agressor pode evitar facilmente a sua detecção, pois, em poucas palavras, ele controla o que é exibido e como seus programas estão sendo executados.

Tradicionalmente, um agressor usa um dos dois métodos para modificar o kernel do sistema: ou ele carrega um módulo com código malicioso no kernel (como o *heroin*, por exemplo) ou modifica o kernel carregado na memória, escrevendo no dispositivo especial `/dev/kmem` (como o *SucKIT*, por exemplo). A desvantagem dessa técnica é que, como esses ataques estão carregados apenas na memória do sistema, normalmente não sobrevivem a uma reinicialização.

Por mais difícil que possa parecer, esses rootkits podem ser detectados comparando-se a tabela atual de chamadas do sistema com a que seria de se esperar originalmente (isto é, examinando-se o arquivo `System.map`). Cópias da memória do sistema podem ser feitas e usadas para verificar se o kernel carregado na memória está intacto.

Quando chegam a esse nível, o que você acha que os agressores fazem? Vão mais fundo ainda, claro...

Hardware e virtualização

Lançado em 2006 durante a Black Hat Conference em Las Vegas, o primeiro rootkit desenvolvido para comprometer diretamente o hardware foi chamado de *Blue Pill* [2]. Os processadores modernos da AMD e da Intel dispõem de uma gama de recursos para suportar virtualização de sistemas operacionais. E como não é mais necessário que esses rootkits modifiquem o que quer que seja no sistema operacional para funcionar, eles são muito mais difíceis de detectar, de modo que somente verificar a integridade da tabela de chamadas do sistema não vai funcionar. Contudo, esses rootkits modificam a tabela de descritores de interrupção (IDT, na sigla em inglês), que é mantida em um dos registradores do processador (o IDTR) [3].

Como passam a existir dois IDTRs no sistema comprometido – um real e outro falso, que é apresentado ao sistema operacional –, este último vai ocupar uma posição de memória diferente da de costume. Felizmente, a instrução privilegiada *Store Interrupt Descriptor Table* (SIDT) pode ser executada a partir do espaço de usuário do sistema, retornando de forma confiável o conteúdo do IDTR

disponível para o sistema operacional (o que não serve para muita coisa, pois o sistema já foi comprometido), bem como – e o que é mais importante – a posição da memória em que o IDTR se encontra. Parece que chegamos a um beco sem saída: os agressores criaram novos métodos para esconder os rootkits e os defensores encontraram meios para detectá-los.

Tabela 1: Chamadas do sistema

`getdents64`	Lê entradas de diretório
`getdents`	Lê entradas de diretório
`chdir`	Muda o diretório de trabalho
`open`	Abre um arquivo ou dispositivo
`execve`	Executa um programa
`socketcall`	Chamadas de sistema via socket
`fork`	Cria um processo filho
`exit`	Encerra o processo atual
`kill`	Envia um sinal a um processo
`getpriority`	Obtém prioridade de escalonamento para um programa

A nova geração de rootkits

Lançados em setembro de 2008 pela Immunity Inc., o *DR RootKit* [4] implementa "ganchos" (*hooks*) para as chamadas de sistema no kernel Linux 2.6, sem modificar nem a tabela de chamadas do sistema nem a tabela de descritores de interrupção. Para fazer isso, ele introduz *breakpoints* de hardware no manipulador de chamadas do sistema. Isso corresponde à inclusão de um "vigia" na memória da tabela de chamadas do sistema, especificamente observando a entrada `__NR_syscall`, usada para exportar números de chamadas do sistema. Basicamente, o rookit se comporta como uma ferramenta de depuração de programas, esperando que determinadas chamadas do sistema sejam executadas e modificando-as quando isso acontece. Os ganchos do DR RootKit estão listados na **tabela 1**.

O DR RootKit dispõe de recursos tais como ocultação de processos e prevenção do término de execução de processos ocultos (o que significa que um agressor pode executar programas ocultos, e você não tem como terminá-los com o comando `kill`,

mesmo que você consiga descobrir a identidade – o *ID* – do processo). Se você usar os exemplos fornecidos com o pacote, é relativamente simples estender e criar outras chamadas de sistema modificadas. Por exemplo, você pode alterar o conjunto de recursos disponíveis para processos – o *capset*. O próprio rootkit é um módulo carregável no kernel, o que simplifica sua inserção em um sistema comprometido. Porém, da mesma forma que acontece com outros rootkits residentes na memória, a reinicialização do sistema irá removê-lo da memória.

Se você quiser estender o rootkit, pode por exemplo inserir suas próprias chamadas do sistema personalizadas. Forneci um exemplo para alterar a chamada de sistema `exit`. Em poucas palavras, o processo consiste em declarar seu próprio gancho para alterar uma chamada de sistema e então implementar uma chamada de sistema customizada – isso é realmente simples. O melhor lugar para começar é o código-fonte do kernel – mais especificamente no subdiretório `kernel/`, onde a maioria das chamadas do sistema são definidas. Por exemplo, se houver um sistema no qual os recursos em uso restringem o que programas podem ou não fazer, você pode simplesmente modificar a chamada de sistema `do_sys_capset_other_tasks` que sempre retorna todos os recursos de um ID de processo específico, como:

```
@@ -237,6 +237,9 @@
if (!capable(CAP_SETPCAP))
return -EPERM;
+ if (pid == 12345) /* magic
➥ process number */
+ return cap_set_all_
➥evil(effective, inheritable,
➥ permitted);
```

Como você pode notar, mesmo a menor das modificações pode ter um efeito significativo. Assim, de uma hora para outra, o processo com o ID *12345* terá sempre todos os recursos, o que permite a ele fazer praticamente tudo o que quiser. Assim, com apenas uma chamada de sistema, um agressor pode criar uma backdoor eficiente.

O único modo de detectar um rootkit desses é por meio da medição de atrasos ou de condições de corrida (*race conditions*) que sejam introduzidas pelo rootkit. Se um rootkit estivesse presente, o sistema deveria ficar mais lento do que de costume, mas a medição dessa variação não é uma tarefa simples. Além disso, o programa é relativamente simples e pode ser estendido facilmente, de modo a se esconder de maneira mais eficiente e tornando sua detecção ainda mais difícil.

Abordagem alternativa

Claro que você pode comprometer um sistema e manter o acesso de outras formas enquanto permanece escondido. Uma outra empresa que desenvolve software de verificação de invasão chamada Core Security [5] adotou uma abordagem de injetar código hostil em processos que já tenham sido atacados. Por exemplo, se você criar uma brecha no conhecido servidor web *Apache*, conseguirá injetar código nele que lhe garanta acesso remoto ao sistema. Essa técnica é algo limitado se comparada com um rootkit de kernel completo ou com um rootkit de hardware. A desvantagem dessa técnica são os mecanismos de proteção do sistema operacional, tais como o SELinux, que permanecem capazes de forçar uma política de segurança. Contudo, para agressores obstinados, isso não costuma ser um problema muito sério, pois eles podem usar um *exploit* local para comprometer ainda mais o sistema, ou mesmo permanecer dentro das condições impostas pela política definida pelo SELinux, mas ainda sim obter informações ou usar o sistema para realizar outros ataques maliciosos.

Conclusão

A boa notícia é que, chegando à camada de hardware, os agressores (pelo menos conceitualmente) atingiram a última camada passível de abuso. A má notícia é que um grande contingente de truques de hardware pode ser usado para manter o controle sobre um sistema comprometido. Por exemplo, uma placa de vídeo moderna tem acesso direto à memória (o que significa que ela pode fazer o que bem entender com a memória do sistema sem que o sistema operacional possa interferir significativamente no processo), dispõe de memória própria e de uma grande quantidade de poder de processamento (tanto que estão sendo usadas por muitos para criar clusters de baixo custo). Placas mais modernas têm seu firmware armazenado em memória flash, passível de atualização por software, e eu não tenho a mínima dúvida de que algum dia alguém vai criar algum método para abusar da placa de vídeo com o propósito de controlar um sistema comprometido. ■

Mais informações

[1] Amir Alsbih, "Passagem Secreta: Técnicas de criação de backdoors": http://www.linuxmagazine.com.br/article/passagem_secreta

[2] Blue Pill: http://bluepillproject.org/

[3] Red Pill: http://www.invisiblethings.org/papers/redpill.html

[4] DR RootKit: http://www.immunityinc.com/resources-freesoftware.shtml

[5] Core Security Technologies: http://www.coresecurity.com/

MID: mais um degrau na escadaria da mobilidade

Augusto Campos

Nem smartphone nem subnotebook: os MIDs chegam como uma nova categoria para facilitar nossas vidas.

Neste início de 2009 tive a oportunidade de segurar em minhas mãos um pedaço do futuro do desktop. Só que não se tratava propriamente de um desktop, ou pelo menos não daquele modelo que aprendemos a conhecer, com uma infinidade de arquivos gravados em um disco rígido ao meu alcance, um ambiente de trabalho cheio de aplicativos instalados localmente e a ocupação de uma vasta área em cima da escrivaninha.

Não era nem mesmo um daqueles notebooks pequeninos, estilo Eee PC, que foram se popularizando mundialmente ao longo de 2008. Era algo menor, mais singelo, mas com poder de processamento surpreendente: um Aigo MID, equipamento do qual provavelmente você ainda não ouviu falar – até porque ele parece estar bem distante do nosso mercado neste momento.

Os MIDs, ou *Mobile Internet Devices*, são dispositivos que parecem ficar entre os smartphones e os subnotebooks de hoje. Como em uma cadeia darwiniana, eu até apostaria que os mais bem-sucedidos entre eles vão acabar ficando no nicho exato que hoje é ocupado por um destes dois extremos (os smartphones ou os subnotebooks), até mesmo porque essas fronteiras vão ficando cada vez mais difusas com o passar do tempo. Mas hoje eles são uma categoria à parte, e torço para que suas características e possibilidades sejam logo herdadas pelos celulares (ou pelos subnotebooks).

O equipamento com o qual tive oportunidade de brincar um pouco tem características de um PC de pequeníssimo porte, com um display suficientemente grande para mostrar os sites da web 2.0 nossos de cada dia, um teclado escamoteável, câmera, microfone e acesso a redes Wi-Fi. Alguns modelos têm acesso à conectividade via redes mais amplas (CDMA, 3G etc.), mas não é o caso do meu. E eles permitem fazer o que eu mais faço no meu desktop diariamente: acessar a web, comunicar-me por IM, VoIP e email, consultar (ou editar levemente) documentos e textos, e até digitar esta coluna que você está lendo.

E o mais interessante: o aparelho que tenho em mãos, assim como tantos de sua categoria, roda Linux e uma série de aplicativos livres, como o Firefox e o Pidgin, entre vários outros. E nem é só pela questão do custo de aquisição: esses aplicativos livres são leves por natureza e ainda podem ser alterados de acordo com as especificações do aparelho no qual serão distribuídos, seja para ocupar menos disco, preencher menos memória RAM ou mesmo gastar menos bateria.

Hoje o acesso à Web é cada vez mais uma condição para que eu possa desempenhar bem as minhas atividades, e quanto mais rico esse acesso, melhor: a cada dia é necessário interagir, digitar textos, captar imagens, comunicar-se por vídeo e voz, conectar-se a redes de variadas tecnologias abertas. Acredito que em algum momento os celulares vão estar aptos a prover com conforto e economia esses recursos, e que vão estar rodando um sistema operacional livre quando o fizerem.

> ***O mais interessante: o aparelho que tenho em mãos, assim como tantos de sua categoria, roda Linux e uma série de aplicativos livres.***

Enquanto esse dia não chega, é interessante ver como a indústria avança nesta direção por vias oblíquas, que convergem em uma direção que muito nos interessa: softwares livres conectando-se a protocolos abertos e provendo serviços que facilitam as nossas vidas. ■

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.

Xen ganha recursos e promete integração

Keir Fraser, da Xensource (atualmente Citrix), anunciou na lista *xen-devel* a disponibilidade de uma árvore com o código-fonte para criação de um *domo* completo do Xen no kernel Linux 2.6.27.

Segundo Keir, "a intenção é fornecer uma árvore única para desenvolvimento e testes voltada aos desenvolvedores que precisarem de um kernel 2.6 mais moderno", e menciona o gerenciamento de energia como um dos motivos para isso.

O porte da funcionalidade de domo do Xen para o Linux atualmente depende da implementação final das *pv_ops* (operações para-virtualizadas), um conjunto de "ganchos de código" (*hooks*) no kernel que permitem sua operação mediante o uso da técnica de para-virtualização. Atualmente, o escopo de funcionalidade das pv_ops permite apenas o funcionamento do Linux como domU (ou seja, como máquina virtual), enquanto o kernel do domo ainda é restrito à versão 2.6.18 do Linux.

A expectativa é que os desenvolvedores da Novell que estão trabalhando nessa tarefa consigam incrementar as pv_ops de forma a permitir seu uso também como domo, o que permitiria o uso de versões mais recentes do kernel Linux (com todas as vantagens que trazem) no domo. Posteriormente, as novas pv_ops também devem ser incluídas na árvore principal do kernel, unindo definitivamente os projetos Xen e Linux. ■

Alta disponibilidade

Manter a sincronização perfeita de múltiplos servidores Xen, cada um com diversas máquinas virtuais, não é tarefa das mais fáceis. Atualmente, é preciso replicar arquivos de configuração entre os servidores e manter sincronizado todo o restante da estrutura.

Felizmente, tudo isso pode mudar para melhor com o projeto *Kemari*. Trata-se de um software de código aberto (GPL) descrito por seus autores como "um mecanismo de código aberto para sincronização de máquinas virtuais para tolerância a falhas. Oferece uma técnica utilizável para tolerância a falhas que não requer o uso de hardware específico ou a modificação dos aplicativos ou sistema operacional".

O objetivo do projeto é "manter as máquinas virtuais rodando transparentemente em caso de falhas de hardware". Para isso, ele "transfere o estado da máquina virtual primária para a secundária quando a primária está prestes a enviar um evento para dispositivos como armazenamento e rede", como descreve o anúncio do projeto.

Espera-se que o Kemari seja integrado ao Xen 3.4, a próxima versão estável do popular sistema de virtualização. ■

Lançado o Fedora 10

Seis meses após o lançamento do Fedora 9, o projeto livre lançou a versão 10 da popular distribuição Linux, codinome *Cambridge*.

O Fedora 10 usa o kernel Linux 2.6.27.5 anunciado no último dia 7. O projeto também está buscando trazer seus softwares a um novo nível, e ele inclui o OpenOffice.org 3.0, Gnome 2.24.1, Eclipse 3.4 e RPM 4.6. O produto promete um melhor gerenciamento de impressoras e alguns interessantes recursos de virtualização. No momento, o KVM está disponível por padrão no Fedora 10, na versão 74-5 (no Fedora 9, o KVM era apenas uma opção). Certamente a aquisição da Qumranet, criadora e desenvolvedora do KVM, pela Red Hat, patrocinadora do Fedora, tem grande influência nisso. No entanto, o uso do KVM não implica a rejeição do "concorrente" Xen: o hypervisor tradicional está presente na versão 3.3.0-1. As ferramentas de virtualização de criação do próprio Fedora, como a libvirt e o virt-manager, também estão incluídas.

Outra importante novidade do Fedora 10 é seu tempo de inicialização, que foi reduzido graças ao novo sistema gráfico de inicialização *Plymouth*. ■

LPI lança provas 303 no Brasil

O Linux Professional Institute – órgão responsável pela certificação em Linux que mais cresce no mundo – realizou no Brasil a primeira aplicação das provas 303. Elas correspondem à categoria especialista do nível 3 da certificação e qualificam o profissional aprovado como "Security Specialist". As provas (grauitas) ocorreram na cidade de São Paulo no dia 20 de dezembro de 2008.

O Programa de Certificação LPI é composto por dois níveis básicos, com duas provas cada um. As provas do nível 1 (101 e 102) certificam o profissional como "Administrador Linux Júnior" e as do nível 2 (201 e 202), como "Administrador Linux Pleno".

O nível 3 da certificação LPI é focado no mercado corporativo. O profissional precisa se certificar obrigatoriamente na prova 301 (Core) e depois escolher uma das especialidades disponíveis. Atualmente a única disponível é a prova 302 (Mixed Environment) para profissionais que queiram se especializar em interoperabilidade em ambientes mistos (Linux, Unix, Netware e Windows). A prova '303 - Security' é a segunda especialidade a ser lançada pelo LPI. A prova 303 está sendo realizada em caráter de teste antes de ser lançada oficialmente. ■

Linux versus OpenSolaris e FreeBSD

O site dedicado a Software Livre e hardware Phoronix publicou um comparativo de velocidade (benchmark) na realização de diversas tarefas entre os sistemas operacionais mais famosos baseados em kernels de código aberto: Ubuntu, OpenSolaris e FreeBSD.

Os testes utilizaram a versão instável de 64 bits mais recente de cada um dos sistemas (com exceção do Ubuntu, cuja versão foi a 8.10 final) e se basearam no próprio pacote de benchmarks de código aberto desenvolvido pela equipe do Phoronix (e em rápida evolução), o *Phoronix Test Suite*.

Os autores concluem o artigo declarando o Ubuntu 8.10 como vencedor no desempenho, mas o representante do kernel Linux não foi o campeão em todas as categorias: venceu em oito dos 18 testes, contra sete vitórias do OpenSolaris e três do FreeBSD.

Poucos dias depois, os autores retornaram ao ambiente de testes e fizeram o comparativo entre o também recente Ubuntu 8.10 e o Fedora.

Foram usadas as versões de 32 e 64 bits de ambos os sistemas, e os testes empregados foram os mesmos do benchmark anterior, com o Phoronix Test Suite.

O resultado dessa comparação, no entanto, não foi conclusivo: as distribuições Linux se saíram praticamente igual com respeito ao desempenho nos testes. ■

Google Android no Openmoko

A Koolu, empresa canadense especializada no desenvolvimento de soluções de tecnologia ambientalmente corretas, disponibilizou o código-fonte da plataforma Android do Google adaptado ao telefone Openmoko FreeRunner, cujo desenvolvimento contou com esforço e total colaboração da comunidade internacional do Software Livre.

O anúncio foi realizado no IP Communications Brasil 2008, evento internacional sobre comunicações IP, por Jon 'maddog' Hall, CTO da Koolu, e Denis Galvão, presidente da paranaense iSolve. Durante o evento também foi anunciado o acordo nomeando a iSolve como canal master de distribuição do Openmoko FreeRunner no Brasil.

O Android foi lançado como um software livre no final de outubro de 2008, porém muito trabalho precisou ser realizado para que esse código pudesse funcionar em telefones de outros fabricantes. O FreeRunner, telefone com design aberto desenvolvido pela empresa taiwanesa Openmoko, demandou uma série de alterações no código-fonte do Android para que ele pudesse funcionar corretamente. A comunidade de Software Livre, com ajuda de várias pessoas ao redor do mundo, realizou as implementações necessárias e tornou possível a execução do Android no FreeRunner.

"Agora que o código-fonte já está rodando no FreeRunner, esperamos que os retoques finais estejam prontos rapidamente", disse Brian Code, diretor técnico da Koolu. "A criação do ambiente para compilação (toolchain), a criação dos patches necessários para tornar o código compatível com o telefone e a documentação de todo o passo-a-passo do processo de construção do software tomaram um bom tempo, mas agora está mais fácil para a comunidade do Software Livre desenvolver e realizar modificações nessa plataforma. Como um exemplo, as aplicações móveis Google Apps, bem como outra aplicações corporativas, podem ser instaladas e otimizadas para essa plataforma". ■

"O futuro é Open Source", diz ex-desenvolvedor MS

Keith Curtis, funcionário por vários anos da Microsoft, conclui em seu livro recém-lançado que o futuro do software está no modelo de desenvolvimento de código aberto. Curtis trabalhou para a Microsoft como desenvolvedor de software de 1993 a 2004, tendo participado do desenvolvimento dos produtos para bancos de dados da empresa, bem como na programação do Windows, do Office e do MSN, entre outros. No final de 2008, ele publicou o livro intitulado "After the Software Wars" (Depois das Guerras do Software), que descreve o processo de produção de software do ponto de vista de um desenvolvedor, analisa os possíveis avanços nesse processo no futuro e aborda desde tópicos como inteligência artificial, culminando no desenvolvimento de sistemas que possibilitem viagens espaciais.

A edição online do The New York Times fez uma resenha do livro e relatou a nova trajetória do ex-funcionário da gigante de Redmond: "Para o Sr. Curtis, a força do software de código aberto e o motivo pelo qual esse é o modelo de desenvolvimento do futuro estão no fato de que, por meio deste, a inteligência coletiva é estimulada". Segundo Curtis, "as diferenças entre Software Livre e software não-livre ou proprietário são comparáveis às diferenças existentes entre ciência e alquimia. Antes de a ciência se estabelecer, havia apenas alquimia, na qual as pessoas tentavam proteger suas idéias, pois elas desejavam dominar o mercado desenvolvendo um processo para transformar chumbo em ouro".

Curtis publicou seu livro usando a plataforma lulu.com, cujo fundador e diretor executivo é Bob Young, veterano da cena Open Source e ex-CEO da Red Hat. ■

MS: Windows é mais econômico

A Microsoft fez de novo: um estudo recente encomendado pela empresa "concluiu" que é mais barato para empresas usar o Windows como plataforma de software. A revista australiana iTWire analisou o estudo e fez algumas descobertas interessantes.

O que parece à primeira vista (com perdão do trocadilho) ser uma história de sucesso, na realidade não é — nem de longe: em primeiro lugar, não há economia alguma. O que há são apenas estimativas da Microsoft, segundo as quais a empresa britânica Speedy Hire deverá economizar 200 mil libras por ano em decorriencia da utilização do Windows.

A análise do estudo, disponível em artigo no site australiano iTWire.com, faz um raio-X da "economia" sugerida pela empresa de Bill Gates. Elas começam pelo hardware, já que no projeto foram utilizados terminais leves para Windows — que seriam inexplicavelmente mais baratos do que aqueles equipados com Linux. O estudo não menciona nem "en passant" que há alternativas bem mais baratas aos modelos V90 da empresa Wyse equipados com Windows, como os V50 pré-carregados com Linux. Nesse estilo, o artigo vai revelando de onde vieram as "reduções de custo" obtidas pela Microsoft, que vão transformam em vapor à medida que prosseguimos na leitura. Estamos curiosos para saber o que sobra da economia de 1 milhão de libras após os cinco anos. ■

Sun lança MySQL 5.1

Na nova versão do banco de dados de código aberto, os desenvolvedores se concentraram no desempenho, o que aumentou a velocidade do programa em surpreendentes 15%. Entre as novidades há cinco novos métodos de particionamento horizontal: *range*, *hash*, *key*, *list* e *composite*. Outros recursos novos são a replicação híbrida e o agendador de eventos (*event scheduler*), que permite a automatização de tarefas SQL repetitivas.

Os sistemas operacionais suportados são Red Hat Enterprise Linux, Suse Linux Enterprise, Windows, Mac OS X, FreeBSD, HP-UX, IBM AIX, IBM i5/OS e todas as distribuições Linux.

A Sun disponibiliza três versões do software para download: *Community Server*, sob a GPL, *Enterprise Server*, com base em subscrição (assinatura do serviço) e *Embedded Server*, esta com licença comercial proprietária. ■

VMware adquire Tungsten Graphics

A VMware adquiriu por um valor não revelado as operações da empresa Tungsten Graphics, fundada em 2001 e motor por trás do desenvolvimento da implementação de código aberto do OpenGL no Linux, a biblioteca *Mesa 3D*.

Além da Mesa 3D, a empresa também desenvolve o *Gallium 3D*, framework para desenvolvimento de drivers gráficos 3D. A Tungsten Graphics é formada por um grupo de desenvolvedores de aplicativos gráficos de código aberto. Segundo a FAQ no site da empresa, o desenvolvimento dos projetos de código aberto encabeçados por ela continuará, agora como parte das atividades da equipe de engenharia da VMware. A aquisição teria como objetivo melhorar o suporte a gráficos 3D em ambientes virtualizados. ■

Google e Red Hat firmam parceria

A Red Hat assinou em dezembro um acordo com o Google para trazer os principais desenvolvedores da empresa para a plataforma de construção de aplicações web *Google Web Tookit*. Com o acordo, estabelece-se também o suporte do servidor de aplicações da Red Hat, o JBoss, ao GWT.

Além da assinatura do acordo, a Red Hat também anunciou que já completou algumas integrações preliminares entre o GWT e o *JBoss Seam Framework*. Com a integração, a empresa alavanca o Seam para que os desenvolvedores possam combinar o poder do Java às modernas tecnologias view-layer, como GWT, *RichFaces* e *Spring* para desenvolver os *Rich Internet Applications*. ■

Insigne já planeja 2012

A fornecedora do Insigne Momentum 5.0 quer manter sua posição de liderança no Brasil e conquistar novos mercados, inclusive no exterior. O sucesso de sua participação no projeto de inclusão digital Computador para Todos fez com que a Insigne Free Software do Brasil conquistasse forte posição de liderança no mercado dos PC populares e também ficasse conhecida em outros países. Esse cenário positivo lhe permitiu iniciar negociações com fabricantes estrangeiros de PC para embarcar o Insigne Momentum 5.0, sistema operacional de código aberto, em microcomputadores fora das fronteiras nacionais.

Para atingir a meta de manter seu crescimento perante a perspectiva de elevação das vendas de PCs nos próximos anos, a empresa contratou o consultor de estratégia e professor de engenharia Carlos Roberto Lopes. As atividades envolvidas no planejamento estratégico incluem uma série de workshops com todas as equipes e departamentos da Insigne. O objetivo é coletar impressões dos colaboradores e lhes apresentar as mais recentes mudanças ocorridas no mercado global, incluindo a atual situação econômica mundial, que poderá alterar a correlação de forças entre os fornecedores de tecnologia nos próximos anos.

De acordo com João Pereira da Silva Jr., presidente da Insigne, esse planejamento incluirá não apenas o foco no seu cliente, que é o usuário do PC popular, mas também em toda a sua equipe de profissionais, envolvidos em todas as etapas de desenvolvimento de um sistema operacional de código aberto". ■

Mandriva demite dois desenvolvedores

A situação financeira da Mandriva parece estar ruim. Em dezembro, a empresa anunciou que, ao final de 2008, terminaria o contrato de dois de seus funcionários: Adam Williams (na prática, o Community Manager) e o mantenedor de pacotes Oden Eriksson.

Os dois desenvolvedores escreveram para a lista de emails do *Cooker* (Adam Williams, Oden Eriksson). Enquanto Adam Williams é considerado por muitos como a base da comunidade do Mandriva, Oden mantém aproximadamente 1.200 pacotes, principalmente na área de servidores, incluindo todos os pacotes do stack LAMP.

Entretanto, a comunidade do Mandriva não pretende esperar sentada a efetivação dessa decisão. Já há uma petição para tentar convencer a empresa a manter pelo menos Williams. ■

Entrevista com Armstrong Lemos, chefe do departamento de TI da CAEMA

Saneada pelo Linux

O Linux entrou com força na Companhia de Águas e Esgotos do Maranhão, proporcionando economia e ganhos fundamentais para a saúde da empresa.

por Pablo Hess

A Companhia de Águas e Esgotos do Maranhão (CAEMA) é uma sociedade de economia mista, com capital de investimento predominantemente do Estado do Maranhão. Fundada há 42 anos, a CAEMA atua no fornecimento de água, coleta e tratamento de esgotos. Atua em 146 municípios maranhenses com abastecimento de água, sendo que somente em três (São Luis, Imperatriz e Barreirinhas) faz a coleta de esgotos.

Linux Magazine» ***Como e por que a CAEMA começou a usar Linux?***

Armstrong Lemos» A CAEMA opera com déficit de quase R$ 5 milhões por mês, que são repassados pelo governo do estado para complementação das despesas. Isso muito se deve a sua função social, que é a de universalização do abastecimento de água no estado. Não é uma atividade meramente econômica, mas também social.

O sistema comercial já foi bloqueado por falta de pagamento. Quanto mais a CAEMA ampliava sua rede de atendimento, mais caro pagava pelo uso do sistema, sendo que a empresa prestadora mantinha relação de pouca paciência com os atrasos no pagamento, que deveriam ser realizados no dia cinco de cada mês. Como a companhia possuía e ainda possui dificuldades de arrecadação, esse prazo nem sempre era cumprido.

Outros fatores aliados a esse contribuíram para que no ínicio da gestão da atual diretoria se iniciasse um processo de diagnóstico geral da empresa. Com esse estudo, ficou clara a situação em que se encontravam diversos setores estratégicos da companhia, entre eles o de informática.

Tínhamos um parque de aproximadamente 500 máquinas com vários problemas, principalmente adwares, spywares e vírus. Havia ainda problemas de conectividade e processamento em função do Windows não se adequar ao perfil do hardware, fazendo com que o equipamento tivesse baixa performance. As atualizações com Windows tornavam-se inviáveis nos computadores com perfil padrão de dois ou mais anos.

O departamento não possuía outra função além do suporte de manutenção de computadores e impressoras, muitos já ultrapassados, uma vez que o último investimento feito em TI na companhia ocorreu no ano 2000.

A telefonia, as escolhas técnicas, o gerenciamento de contratos de sistemas e outras atividades não eram exercidas pelo departamento de informática. Não havia uma política definida de TI na empresa e não se dispunha de recursos para investimento. Muitos dos sistemas utilizados pela empresa eram piratas e não possuíam suporte. O banco de dados da companhia não dispunha mais de suporte de software, e o departamento de informática não tinha

Armstrong Lemos, chefe do departamento de TI da CAEMA.

conhecimento dos relacionamentos dos dados contidos nele.

Após o diagnóstico e reuniões, solicitou-se à diretoria administrativa da empresa, à qual a informática é subordinada, para que submetesse ao conselho de administração o restabelecimento das funções relativas à área de TI, incluindo telefonia.

Além dessas ações de retomada das atribuições, estruturamos uma equipe de programação, uma equipe de projetos estratégicos e reestruturamos a equipe de suporte técnico, tudo isso para viabilizar a política de Software Livre da CAEMA.

LM» ***Em que consiste essa política de Software Livre?***
AL» Estabelecemos várias etapas, como o desenvolvimento do Livre Linux e do sistema de protocolo via Web, a migração do sistema comercial (GSAN), a formação de monitores de treinamento e o treinamento dos usuários na solução completa (GSAN, Livre Linux, BrOffice.org e sistema de protocolo), seguida pela articulação do Movimento Software Livre Maranhão.

LM» ***Como foi a evolução do uso do Software Livre dentro da empresa?***
AL» Precisávamos resolver dois fatores que impediam o avanço da politica de Software Livre na empresa: o sistema de protocolo, em Windows, e o sistema comercial, também em Windows e com arquitetura cliente-servidor. Além disso, determinou-se a substituição deles por um novo sistema que permitisse a ampliação da nossa rede de atendimento e que ainda propiciasse a autonomia no gerenciamento dos dados da companhia.

O sistema de protocolo foi resolvido a partir do desenvolvimento do sistema livre *Balula*, feito pela equipe de programação e Software Livre da CAEMA. Hoje o protocolo está à disposição dos demais órgãos públicos para serem implementados sem qualquer custo adicional, através de parceria sem ônus entre a CAEMA e o órgão interessado.

Ainda em novembro todos os computadores de atendimento comercial das unidades da CAEMA passaram a utilizar o Livre Linux como sistema operacional.

LM» ***Como é a situação atual?***
AL» Hoje utilizamos o GSAN com banco de dados PostgreSQL. Com isso, estamos ampliando o atendimento aos municípios onde nosso sistema comercial antigo não funcionava, pois era inviabilizado pelo custo alto de contratação de serviços de transmissão de dados junto às operadoras locais. Atualmente, com uma simples conexão via rádio, que existe em todos os municípios onde a CAEMA atua, faremos a integração com o novo sistema.

Estão rodando na plataforma Linux todos os sistemas Web (comercial, protocolo, frotas, jurídico, cadastro, segunda via de contracheque) etc. Estamos com Livre Linux nos setores de atendimento, help desk, administrativo e em todos os servidores.

Vamos estender essa implantação para os demais setores, salvo máquinas que possuam aplicativos em Windows sem similares no mundo Linux (que são casos mais raros).

LM» ***Em quanto tempo a CAEMA espera obter o retorno do investimento em Software Livre?***
AL» O custo total foi de R$ 1,04 milhões para o sistema comercial e o banco de dados. Isso representa uma economia de R$ 3,60 milhões ao longo de quatro anos, somente nesses dois sistemas. Os levantamentos sobre a substituição do sistema operacional Windows por Linux, do proprietário Microsoft Office pelo BrOffice.org e programas pagos estão sendo levantados, o que poderá representar uma economia de aproximadamente meio milhão de reais.

LM» ***Quanto tempo durou a migração?***
AL» Aproximadamente oito meses, com um analista de sistemas da CAEMA e mais dois analistas de sistemas, quatro programadores e um analista de suporte e bancos de dados de nosso prestador de serviços (Domínio), além de quatro analistas de sistemas e um DBA do IPAD.

LM» ***Qual a opinião da direção da empresa sobre o Software Livre?***
AL» O convencimento junto à diretoria foi de estabilidade e custo financeiro, devido à situação em que estávamos. Hoje há o reconhecimento quanto às soluções implantadas e o estímulo para a descoberta de novas alternativas. A diretoria percebe as vantagens de total liberdade e autonomia de uso e configuração das ferramentas livres que tornaram a migração técnica e economicamente viável.

LM» ***E a sua opinião sobre o mercado de Software Livre?***
AL» O mercado de Software Livre no país está maduro. Muitas empresas estão habilitadas para a execução e a manutenção de projetos livres. Seguindo essa tendência, grandes empresas têm ações nesse foco. No entanto, temos carência de empresas privadas que prestem suporte a bancos de dados livres, assim como é carente o uso desses bancos em aplicações comerciais proprietárias.

LM» ***O movimento Software Livre Maranhão já rendeu frutos?***
AL» No dia 14 de novembro realizamos o I Encontro de Articulação de Software Livre Maranhão para apresentar aos demais gestores de TI do Estado a alternativa de uso de Software Livre pelo governo e articulação de um movimento independente para fortalecimento dessa política. ■

Como participar da comunidade Open Souce?

Cezar Taurion

Uma análise do desenvolvimento do kernel Linux.

Há alguns dias li um interessante artigo de Jonathan Corbet, "How to participate in the Linux Community"[1]. Ele descreve como funciona o processo de desenvolvimento do kernel Linux e é uma excelente fonte de referência para quem estiver interessado em colaborar com a comunidade ou mesmo conhecer como funciona por dentro o modelo de governança de um projeto de código aberto.

O kernel Linux tem mais de 6 milhões de linhas de código e aglutina mais de mil contribuidores ativos. É um dos maiores projetos de código aberto do mundo. Seu sucesso tem atraído muitos colaboradores, a maioria inclusive pertencendo a empresas que querem participar do projeto. A questão é: como entrar e ser um participante ativo da comunidade?

Cada comunidade Open Source tem suas próprias regras de conduta e modelos de governança. Entender como funciona a comunidade que desenvolve o kernel é essencial para ser um colaborador e também abre idéias para aprendermos como funciona um projeto Open Source.

A primeira seção do artigo mostra a importância de se inserir todo código na árvore principal do kernel para se evitar a proliferação de *forks* e futuras "bombas relógio". Por exemplo, um código inserido no kernel principal passa a ser visto, mantido e refinado por toda a comunidade, resultando em código de alta qualidade. Quando o código é mantido separado, não só não recebe contribuições externas como corre o risco de funcionalidade similar ser incorporada por outro desenvolvedor ao código principal, fazendo com que o código isolado fique cada vez mais difícil e custoso de ser mantido. Esse alerta é feito porque muitas empresas envolvidas em projetos de software embarcado tendem a acreditar que seu código, pela sua especificidade, deve ser mantido de forma isolada da árvore principal do kernel, o que é um grande erro. A seção também descreve as razões por que toda contribuição deve ser "assinada". É necessário para se evitar eventuais problemas de propriedade intelectual.

A seção dois é bem interessante, pois descreve como funciona o processo de desenvolvimento do kernel e a nomenclatura usada para designar as diversas versões. Explica também como é criado uma versão estável e o ciclo de vida dos *patches*. Descreve como um patch é inserido no kernel e cita alguns dados curiosos. A seção também descreve as regras de etiqueta da comunidade na troca de mensagens e o uso das listas de email.

As outras seções descrevem o processo de planejamento da evolução do kernel, debatendo as etapas de avaliação, as discussões com a comunidade para definir o que e como será feito, os estilos de escrita (que garantem a qualidade do código), as ferramentas de depuração usadas, a documentação que deve ser gerada e assim por diante.

A seção seis mostra como deve ser feito o trabalho em colaboração. Cada patch é revisado por desenvolvedores que você não conhece, o que muitas vezes pode gerar algum desconforto. Existem algumas recomendações de como se portar nessas situações meio desagradáveis e de como evitar discussões desgastantes. Trabalhar em colaboração é um exercício ao qual muitos desenvolvedores não estão acostumados. Para muita gente, ter um estranho revisando seu código e expondo as falhas em público é no mínimo desconfortável.

Enfim, a leitura desse documento é obrigatória para todos que estejam realmente interessados em conhecer mais a fundo o que é o movimento Open Source e os aspectos do desenvolvimento colaborativo que o caracterizam. ■

Mais informações

[1] Jonathan Corbet, "How to participate in the Linux Community": http://ldn.linuxfoundation.org/book/how-participate-linux-community.

Sobre o autor

Cezar Taurion (ctaurion@br.ibm.com) 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.

Argumentando em favor do Software Livre

Jon 'maddog' Hall

A comunidade do Código Aberto não dispõe de um séqüito de advogados e consultores de marketing e comunicação. Quando se trata de argumentar em favor do Software Livre, você provavelmente terá que assumir esse papel.

A "cena" jurídica envolvendo o Software Livre está sempre em movimento. Decisões de tribunais e ações governamentais estão sempre reformulando o panorama legal e têm efeitos bruscos na "temperatura" do desenvolvimento desse tipo de aplicação.

Uma lei proposta recentemente tinha por objetivo ajudar a eliminar a pornografia infantil, mas foi modificada para limitar todo e qualquer tipo de liberdade na Internet, a ponto de – nas palavras de um dos legisladores – dificultar o desenvolvimento de tecnologias como redes *mesh*.

No mês passado, escrevi sobre minha experiência em testemunhar perante uma assembléia nacional sobre uma lei considerada pioneira, relativa ao mundo *open source*. Muito embora oportunidades como essa não apareçam todos os dias, é surpreendente a freqüência com que os governos – em todos os níveis – são confrontados com tópicos relacionados à comunidade open source.

Seu governo local também gasta dinheiro com software. Algumas diretorias de escola gastam mesmo milhares de dólares em aplicativos proprietários, mesmo que suas contrapartes de código aberto estejam disponíveis a um preço muito inferior. A maioria dos governos locais e das diretorias das escolas dispõem, entretanto, de um tempo para ouvir o cidadão – e você poderia usar esse tempo para lhes dizer o que você pensa a respeito disso. Melhor ainda: você poderia reunir um grupo de amigos com os mesmos ideais para argumentar em favor do uso de Software Livre.

Se você for chamado para avaliar uma proposta de regulamentação ou orçamento, certifique-se de tê-la estudado profundamente. Não deixe de conhecer os políticos eleitos envolvidos no processo. Com freqüência, políticos locais estão dispostos a discutir esses tópicos com você diretamente. E se você marcar uma reunião, não se esqueça de "estar apresentável" (como sua mãe provavelmente diria) e de manter a calma, lançando mão de uma argumentação plausível.

A maneira mais simples de se envolver em nível nacional com esse tipo de legislação é por meio de uma carta. A maioria dos legisladores possui um email, mas eles recebem milhares de mensagens todos os dias, e a sua pode simplesmente "se afogar" nesse oceano, sem jamais ter sido lida. Uma carta tradicional, impressa e assinada, pode receber mais atenção do que um email, e uma carta enviada via portador, como encomenda expressa ou registrada, tem ainda maiores chances de ser notada. Não se esqueça de usar um corretor ortográfico ao escrever – nem de deixar alguém mais ler a carta antes de enviá-la, como medida para garantir que o conteúdo esteja inteligível.

Cartas para editores de publicações também são eficazes. Oficiais de governo – bem como cidadãos interessados que podem ser persuadidos por argumentos bem formulados – lêem jornais. Cartas concisas com argumentos claros são preferíveis a cartas longas sem um objetivo claramente definido. Evite criticar o caráter dos proponentes da legislação a que você se opõe. Em vez disso, concentre seus comentários no conteúdo.

Se você busca um modo simples de se envolver no movimento em torno do Software Livre, observe as oportunidades para dar a sua opinião sobre leis, regulamentações e decisões de compra que afetem de algum modo o ecossistema open source. O esforço é válido, já que manter os braços cruzados não é uma alternativa capaz de lhe dar voz ativa nesse tipo de processo. ■

Sobre o autor

Jon 'maddog' Hall é presidente da Linux International, instituição internacional dedicada a promover o Linux e o Software Livre e de Código Aberto. Maddog viaja o mundo ministrando palestras e debatendo com decisores sobre o uso do Software Livre em âmbito tanto corporativo quanto comunitário.

Nova lei de call center? Ótima oportunidade para TI

Edgar Silva

Há inúmeras tecnologias de código ou padrões abertos que podem ajudar a superar as dificuldades decorrentes da nova lei de call centers.

"O brasileiro, mesmo com todas as adversidades, é um povo criativo que, na dificuldade, cria oportunidades!" Essa afirmação cabe muito bem quando observarmos a nova lei para *call centers*. Afinal, quem nunca ficou esperando horas numa linha telefônica e repetindo número de documentos, nome da mãe, endereço etc. O decreto visa não só a melhorar a vida de todos que precisam dos serviços de empresas de telefonia fixa e móvel, TV a cabo e outros, mas também gerar novos empregos, assim como oportunidades de negócios, que é o tema deste artigo.

Certamente, em razão da tradicional morosidade dos atendimentos de call center, o comportamento padrão de nós consumidores é procurar alternativas. Uma delas foi a Internet, o que fez com que as empresas investissem em portais para evitar o gargalo no atendimento de suas redes e também porque representa um aumento no atendimento sem elevar os custos. Então, por que não criar novos canais de atendimento? A tecnologia Java e algumas especificações padrões e projetos open source fazem a diferença nessa indústria de atendimento.

Java, por exemplo, é extensamente utilizado. Dentre os inúmeros motivadores, destaco liberdade de escolha de seus fornecedores, a existência de padrões da indústria, que garantem maior ROI, bem como facilidade de obtenção e formação de profissionais. Java conta com alguns padrões de tecnologia que ajudam principalmente a aproveitar parte do legado, permitindo novos canais de interação com os clientes. Por exemplo: os componentes ou serviços que atendem um navegador web podem também atender uma chamada telefônica, uma interação SMS ou até mesmo um canal VoIP via *Skype*.

Entre as tecnologias disponíveis, cito as APIs padrões JSR116-SIP Servlets 1.0 [1] e JSR289-SIP Servlets 1.1 [2], que possibilitam a interação com servidores SIP (*Session Initiation Protocol*) , protocolo que, dentre inúmeras funcionalidades, estabelece chamadas de voz via Internet. O funcionamento do SIPServlet é similar ao do Servlet tradicional Java, entretanto, em vez de interagir com o protocolo HTTP, está apto a processar requisições e respostas do protocolo SIP. É por isso que seus componentes e serviços podem ser reaproveitados.

O *Mobicents* [3] também é uma solução que combina, além de SIP, vários outros serviços para o segmento de telecomunicações, que por sua vez é a implementação de referência do padrão JSLEE 1.0 , que em resumo é uma complementação do já conhecido JEE (J2EE para os mais antigos) específico para a comunicação de componentes existentes em arquiteturas que agrupam web, Voip, som e imagem.

Outro portal open source com soluções interessantes é o Ignite Real Time [4], que hospeda projetos como o *OpenFire*, servidor *Jabber* (XMPP) com inúmeros plugins, entre eles para chamadas SIP e comunicação com o legendário *Asterisk*. ■

Mais informações

[1] JSR116: http://jcp.org/en/jsr/detail?id=116

[2] JSR289: http://jcp.org/en/jsr/detail?id=289

[3] Mobicents: http://www.mobicents.org

[4] Ignite Real Time http://www.igniterealtime.org

Sobre o autor

Edgar A. Silva (edgar.silva@redhat.com) é Middleware Technology Lead da Red Hat no Brasil, com atuação desde 1998 em objetos distribuídos (Corba, COM+ e Java). Edgar vem nos últimos anos pesquisando, aplicando e ministrando palestras e treinamentos no Brasil e exterior sobre assuntos de alta tecnologia, entre eles JavaEE e SOA.

Dicas de especialistas para conviver com o Windows

Integração transparente

Sim, é possível fazer tudo com o Linux… Mas mesmo que você queira viver em um mundo de código aberto, ele ainda está cheio de Windows. A edição deste mês traz um apanhado de estratégias para facilitar o convívio com o sistema operacional da Microsoft.

por Joe Casad e Rafael Peregrino da Silva

As redes de hoje contam com um sortimento considerável de sistemas e dispositivos. Se todos esses componentes não precisassem se comunicar, não as chamaríamos de rede. Mesmo que você sonhe com um mundo sem Windows – e a IBM se esforce para tornar seu sonho realidade –, essa realidade ainda está um pouco distante. Por conta disso, a edição deste mês traz diversos artigos versando sobre interoperabilidade e integração de sistemas. No nosso primeiro artigo, examinamos algumas técnicas para conexão de clientes VPN para Linux a servidores Windows.

Também vamos mostrar alguns aplicativos Linux para gerenciamento de conexões a VPNs e descreveremos algumas técnicas de resolução dos problemas para fazer o sistema do pingüim funcionar com o protocolo PPTP usado em redes Windows. No artigo seguinte, abordamos a integração de sistemas Linux a um ambiente Windows usando o famoso (alguns diriam infame) *Microsoft Active Directory*, lançando mão, para tanto, do sistema de autenticação *Likewise Open*. O Likewise é uma ferramenta de código aberto que fornece uma configuração fácil para autenticação dos tipos *single sign-on* e *Kerberos*. O terceiro artigo da sessão mostra como configurar o Linux como um servidor de terminais para clientes Windows utilizando o *xrdp* – uma implementação de código aberto do *Remote Desktop Protocol* (RDP) da Microsoft. Nesse artigo, você vai entender por que o sistema das janelas não é necessário no servidor para criar um ambiente de terminais Windows e aprenderá como fazer os usuários desse sistema visualizarem um desktop Linux na sua área de trabalho, tudo isso em apenas alguns passos.

Por último, apresentamos um software de código aberto para agendamento de tarefas muito mais complexo que o venerável *Cron* e que tem como uma de suas maiores vantagens o fato de ser multiplataforma – o que facilita muito a administração de um ambiente heterogêneo de servidores.

Se você precisa conviver com o Windows, por que não viver em paz e com conforto? Se esse é o seu caso, esperamos tornar a sua vida um pouco menos atribulada com esta edição de integração com as tecnologias da gigante de Redmond. ■

Índice das matérias de capa

Configurando conexões VPN em clientes Linux

Rede fechada

Clientes Linux eventualmente precisam de uma mãozinha para se conectar a servidores VPN do Windows.

por James Stanger

Dois benefícios de se usar túneis VPN (*Virtual Private Networks*, ou redes virtuais privadas) são as conexões criptografadas e o acesso aos recursos localizados atrás do firewall. Quando a questão é interoperabilidade, entretanto, configurar essas conexões pode ser difícil em clientes Linux. As distribuições Linux freqüentemente têm problemas em estabelecer conexões a VPNs em servidores cuja tecnologia é baseada em outros sistemas operacionais, especialmente porque os aplicativos gráficos utilizados para configurar essas conexões normalmente não conseguem manter o mesmo ritmo de desenvolvimento do Linux, que está geralmente duas gerações à frente delas. Assim, pouco tempo após as distribuições terem sido lançadas, as bibliotecas usadas para a criação de VPNs são modificadas, e o aplicativo que você utilizava para fazer esse tipo de conexão simplesmente pára de funcionar em ambientes heterogêneos. Recentemente houve um avanço nessa situação, e este artigo dá algumas dicas sobre como estabelecer conexões a VPNs a partir de um desktop Linux.

Uma VPN cria um túnel ponto-a-ponto por meio de uma rede pública. Vários protocolos oferecem suporte a conexões VPN, entre eles as seguintes alternativas bastante populares:

- L2TP via IPsec: Foi o primeiro protocolo desenvolvido pela Cisco para criação de túneis de acesso criptografados. L2TPv3 é a versão mais recente, mas certifique-se de escolher a versão apropriada para a sua rede. Lembre-se de que há duas implementações de *IPsec* principais no Linux. Por exemplo, sistemas mais antigos usam *FreeS/WAN* ou *Openswan* para IPsec. Sistemas mais recentes com qual-

Quadro 1: Problemas e soluções

Ao resolver problemas em conexões, certifique-se de estar com os módulos instalados e carregados. Por exemplo, num sistema Ubuntu 8.04.1, uma conexão PPTP precisa dos seguintes módulos:

```
ppp_mppe     8068  2
ppp_async   13312  1
crc_ccitt    3072  1 ppp_async
ppp_generic 29588  6 ppp_mppe ppp_async
slhc         7040  1 ppp_generic
ppdev       10372  0
```

A MTU (unidade máxima de transmissão) é outra configuração importante: pode ser necessário reduzir o valor de 1500 para algo menor, como 1490.

Em caso de problemas, lembre-se de ativar as opções de depuração no cliente – sempre é possível desativá-las depois. As opções de depuração podem incluir especificar pacotes ICMP para testar uma conexão, assim como determinar o tamanho do intervalo de eco.

Uma opção estranha, mas eventualmente útil, é desativar a criptografia. Obviamente, com isso perdem-se os benefícios da conexão VPN. A maioria dos servidores rejeita conexões sem criptografia, mas ainda assim essa opção pode ser de alguma ajuda para eliminar fontes de problemas.

O mascaramento de IP e outras formas de NAT também impõem alguns problemas para conexões VPN. Se estiverem sendo usados ESP ou AH (cabeçalhos de autenticação), por exemplo, haverá problemas com o NAT, pois o AH executa uma verificação que inclui valores como o endereço IP da conexão. Como o NAT modifica o endereço IP, a verificação falhará, e, portanto, também a comunicação.

quer versão do kernel da série 2.6 dispõem de suporte nativo a Ipsec;
- *Point-to-Point Tunneling Protocol* (PPTP): trata-se de um protocolo antigo que ainda é usado em diversos ambientes Microsoft;
- *Secure Sockets Layer/Transport Layer Security* (SSL/TLS): é um dos mais poderosos protocolos de interoperabilidade disponíveis atualmente, fornecendo suporte para muitos tipos de conexões VPN. O *OpenVPN* [1], por exemplo, é uma solução para criação de túneis de acesso criptografados baseada em SSL/TLS.

Com o passar dos anos, já houve muitas discussões sobre qual protocolo é o mais seguro ou qual seria mais favorável ao modelo de desenvolvimento de código aberto. Muitas dessas discussões chegaram a assumir um teor quase religioso. Porém, em vez de se envolver em tais discussões, é mais útil simplesmente descobrir qual dos protocolos funciona melhor para o seu tipo de rede em particular e então adotá-lo.

Qualquer que seja o protocolo usado para criar o túnel, é possível enviar pacotes através dele, os quais serão considerados pelo firewall como pacotes internos. A chave, como veremos a seguir, é se certificar de que os pacotes certos atravessem a interface correta do túnel.

O ambiente Linux dispõe de diversas ferramentas para configurar e gerenciar conexões VPN. O utilitário *KVpnc*, do projeto KDE, oferece suporte para várias tecnologias VPN (da Cisco, passando pela Microsoft e culminando no OpenVPN). O *vpnc* é um programa de linha de comando para sistemas Cisco. Muitas distribuições Linux passaram a usar o *NetworkManager* [2], desenvolvido pela Red Hat, que permite instalar extensões para redes Cisco e Microsoft. Dependendo da tecnologia VPN que você pretende usar, você terá que instalar a extensão apropriada.

O *pptpconfig* [3] é um aplicativo antigo que funciona especialmente bem para distribuições Linux da Red Hat e da Novell, bem como com BSDs e vários outros sistemas. Como o nome sugere, o pptpconfig é usado para gerenciar VPNs baseados em tecnologia Microsoft.

Quadro 2: Preso do lado de fora

Conforme são feitos experimentos com a conexão VPN, certifique-se de que sua conta não seja trancada do lado de fora. A maioria das VPNs tem dificuldade em diferenciar entre experimentos com a configuração e tentativas de invasão. Se você ficar trancado de fora, não conseguirá entrar, nem mesmo com as configurações corretas.

Se ficar impossível conectar-se, preste atenção ao arquivo de log e às mensagens de depuração para verificar se as mensagens de autenticação e conexão mudaram de alguma forma; uma mudança sutil pode indicar que se está, na verdade, trancado do lado de fora da conta. Se for esse o caso, será preciso esperar a conta ser desbloqueada. Com sorte, essa limitação será temporária. Caso contrário, será preciso contatar o administrador da rede cada vez que ocorrer esse imprevisto.

Criando um túnel

Independentemente de qual aplicativo ou protocolo for usado, é necessário obter algumas informações básicas para estabelecer uma conexão com sucesso. Por exemplo:

- Informações sobre autenticação: dependendo do que o administrador da rede exigir, será preciso fornecer informações específicas a respeito do usuário para se autenticar no servidor VPN. A alternativa menos segura (embora mais comum) é fornecer um nome de usuário e uma senha. Outras opções incluem chaves privadas e certificados. A Cisco dá preferência ao uso de chaves e certificados, por exemplo;
- *Gateway* (também conhecido popularmente como nome do servidor VPN): é o endereço IP ou nome do equipamento VPN que fornece o túnel depois da autenticação;
- Tipo de protocolo: como discutido acima, é necessário escolher entre os protocolos existentes, tais como L2TP, PPTP, OpenVPN etc. A ferramenta de configuração vai solicitar que sejam especificadas as opções adequadas para o(s) protocolo(s) escolhido(s)- pelo administrador da rede.
- Configurações gerais: qualquer que seja o protocolo de autenticação, será preciso fornecer informações específicas para a sua conexão. Por exemplo, algumas redes solicitam a configuração de uma unidade máxima de transmissão (do inglês *Maximum Transmission Unit*, o famigerado MTU) específica; o aplicativo permite que sejam realizadas as modificações específicas para a conexão em questão.
- Informações de roteamento: não importa os tipos de protocolo ou autenticação escolhidos, normalmente também é necessário assegurar-se de que os pacotes certos estão de fato sendo roteados através da interface correta.

Assim, é certo depender da ajuda de um administrador de redes compre-

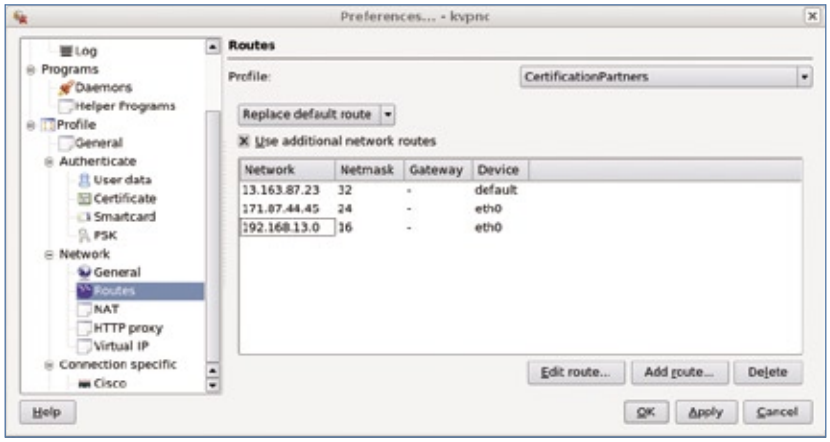


Figura 1 Criação de rotas no cliente *VPN KVpnc*.

ensivo para ajudar o usuário a obter as informações listadas acima.

PPTP com Microsoft

Mesmo que o protocolo PPTP seja considerado menos seguro que o da Cisco ou o OpenVPN, ele ainda é bastante popular. Para configurar uma conexão PPTP, há um grande rol de opções de autenticação, compressão e criptografia.

Um dos desafios é escolher o método de autenticação. Autenticação direta (*peer authentication*) significa que o servidor solicitará que o cliente se identifique. As opções para essa modalidade de autenticação incluem:

- *Challenge Handshake Authentication Protocol* (CHAP): protocolo padrão em conformidade com o RFC correspondente. Basta fornecer um nome de usuário e uma senha para se autenticar. MS-CHAP é a implementação do protocolo pela Microsoft. Se o administrador da rede não revelar o protocolo empregado, use o MS-CHAP no caso de servidores Windows.
- EAP: é uma extensão do protocolo de autenticação PPP original, que permite o uso de um certificado em vez de nome de usuário e senha. Menos comum do que MS-CHAP e CHAP.

Muitos clientes oferecem a opção de recusar todos esses métodos de autenticação. Para trabalhar bem com um servidor VPN remoto, talvez a melhor opção seja usar diretamente o *daemon* PPP do seu sistema.

- Compactar os dados para transmissão pela VPN também é uma boa idéia. Geralmente, há três opções de compressão:
- *Microsoft Point-to-Point Compression* (MPPC): protocolo antigo baseado no algoritmo LZ e geralmente reservado a clientes Windows antigos (Windows 95 e NT). Contudo, pode funcionar em outras VPNs.
- *Deflate compression*: protocolo similar ao MPPC, mas livre de patentes. É mais universal que o MPPC, mas raramente usado em VPNs Microsoft.
- *BSD compression*: descrito na RFC 1977, é o protocolo de compressão tradicional.

O tipo de compressão geralmente causa problemas nas conexões. Caso o administrador da rede não coopere, é melhor tentar primeiro uma conexão sem compressão.

A configuração da criptografia também é importante. O *Microsoft Point-to-Point Encryption* (MPPE) é um subconjunto do MPPC. Pode-se usar dois comprimentos de chave diferentes: 40 bits e 128 bits. Empresas de muitos países usam apenas chaves de 40 bits. Na configuração de clientes PPTP, o administrador deve informar o comprimento da chave. Senão, basta testar até descobrir.

Stateful MPPE geralmente é a melhor opção de criptografia, uma vez que fornece conexões de rede mais rápidas. Como veremos mais à frente, é necessário habilitar o módulo MPPE para qualquer uma dessas configurações.

DNS

A maioria dos clientes DNS pergunta se deve usar as informações de DNS em `/etc/resolv.conf` ou aquelas fornecidas pelo servidor VPN. A própria conexão VPN pode causar modificações na resolução de DNS, principal-

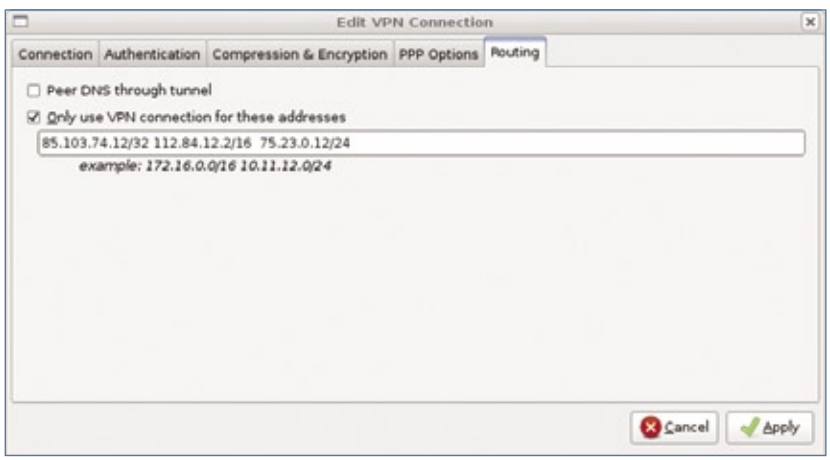


Figura 2 Criação de rotas no cliente *NetworkManager*.

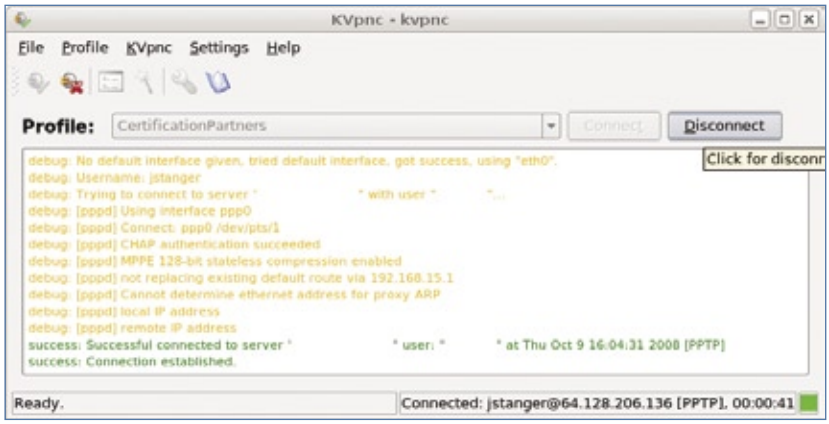


Figura 3 *KVpnc* com uma sessão PPTP legada.

mente porque o cliente VPN altera o conteúdo do arquivo `/etc/resolv.conf`, mesmo quando configurado explicitamente para não fazê-lo.

A melhor solução é usar um cliente VPN que funcione da forma que se espera. Na falta de tal solução, pode-se contornar o problema criando um script que faça uma cópia do arquivo `/etc/resolv.conf` correto. Quando o cliente VPN pergunta se deve "realizar acessos ao DNS através do túnel", geralmente o que ele realmente quer dizer é se pode alterar o arquivo `/etc/resolv.conf` com seus novos dados. A escolha correta depende de informações fornecidas pelo administrador da rede. Se o objetivo não for usar o DNS da VPN, será difícil o cliente acessar as outras máquinas detrás da VPN.

Suporte ao GRE

Para conectar um cliente a uma VPN Microsoft através de um firewall Linux, há um ajuste extra a ser feito nele para que tudo funcione: a ativação do protocolo *Generic Route Encapsulation* (GRE) para atravessar o firewall. Supondo o uso do *iptables* no firewall Linux e um servidor VPN com o endereço 189.44.45.3, é necessário executar o seguinte comando:

```
iptables -I FORWARD -p 47 -d
➥ 189.44.45.3 -j ACCEPT
```

Roteamento

Pode ser necessário rotear pacotes explicitamente através de uma interface específica. Muitos administradores de sistemas Windows consideram esse um dos maiores desafios do trabalho com clientes Linux.

A necessidade de rotear pacotes explicitamente é especialmente importante quando a rede remota utiliza IPs públicos. Mesmo que seja usado um túnel VPN, a interface de rede ainda pode tentar rotear pacotes pela Internet, em vez de simplesmente usar o túnel. São muito freqüentes problemas em conexões VPN cuja solução é simplesmente adicionar algumas rotas alternativas à tabela de roteamento padrão do sistema. Isso pode ser feito tanto com o aplicativo gráfico de configuração do VPN quanto pela linha de comando, com os utilitários `route` ou `iproute`:

```
route add -net 13.163.97.23
➥ netmask 255.255.255.255 dev ppp0
```

ou `iproute`:

```
ip route add 171.87.44.54/24 dev
➥ ppp0
```

Em alguns casos, sem essas rotas, não é possível fazer com que os pacotes que deveriam trafegar pela VPN realmente o façam, e eles acabam saindo pela placa de rede.

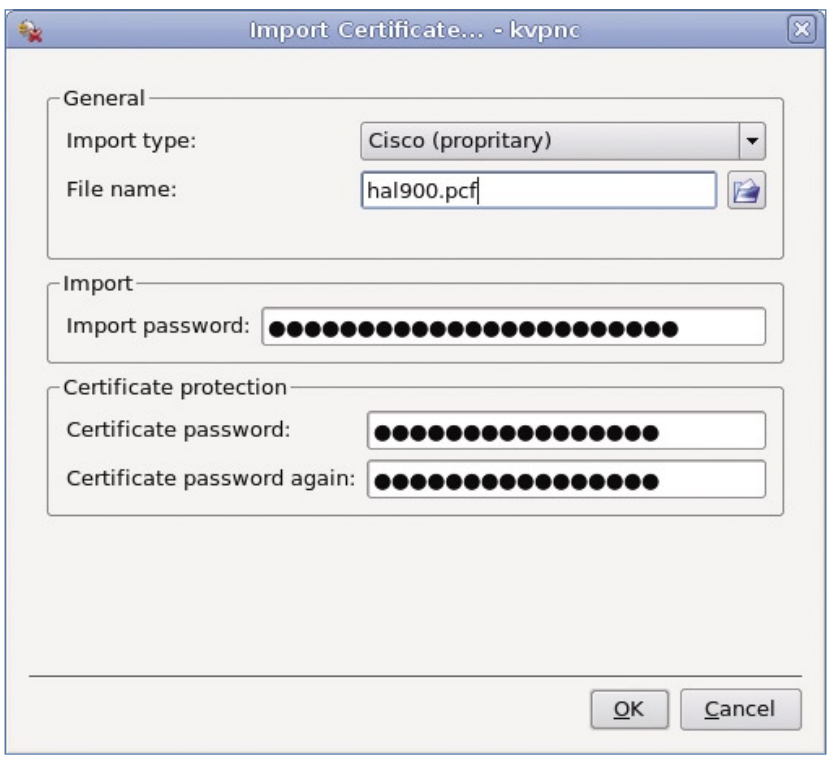


Figura 4 Importação de um certificado Cisco no *KVpnc*.

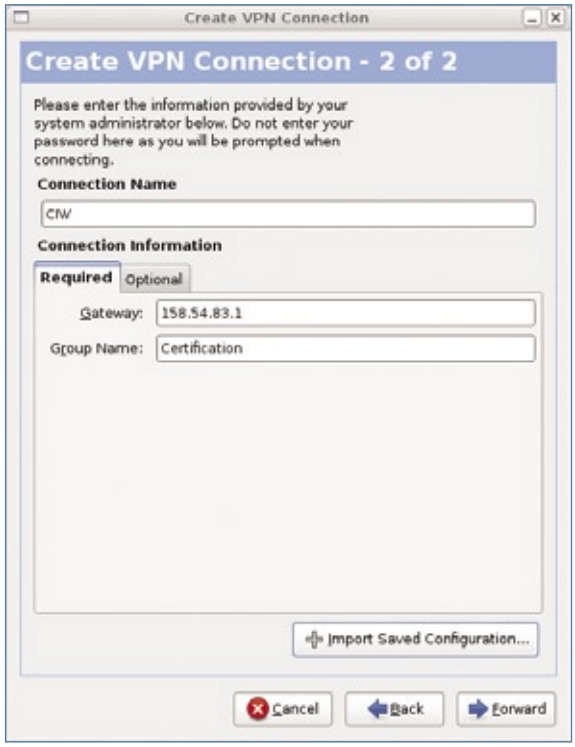


Figura 5 Configuração de *VPN Cisco* no *NetworkManager*.

Interface gráfica

Os aplicativos gráficos para configuração de VPNs estão ficando cada vez melhores quando se trata de adicionar as rotas necessárias automaticamente. A **figura 1** mostra as configurações para o *KVpnc*. A **figura 2** ilustra uma configuração similar no *NetworkManager*.

Assim como essas capturas de tela ilustram, pacotes que coincidam com o endereço IP e a máscara de rede definidos não serão enviados através da conexão de rede padrão, mas simpelo túnel VPN.

O KVpnc (**figura 3**), disponível em várias distribuições, talvez seja o mais versátil entre os clientes atuais, pois oferece suporte a L2TP, aos protocolos VPN tanto livres quanto proprietários da Cisco, ao OpenVPN e ao PPTP, da Microsoft. O KVpnc também permite a importação de certificados, conforme mostra a **figura 4**.

Apesar de os desenvolvedores da interface gráfica do programa terem cometido alguns deslizes ortográficos na interface, os desenvolvedores do KVpnc realmente criaram um produto que trabalha particularmente bem em conjunto com dispositivos Cisco.

O venerável `pptpconfig` também está disponível em muitas distribuições. O segredo para o sucesso no seu uso `pptpconfig` está na configuração da criptografia usada pelo programa, que precisa ser exatamente aquele previsto pelo administrador.

Com freqüência, é importante usar de criptografia MPPE e habilitar o modo stateful desse protocolo. No caso do `pptpconfig`, seria preciso selecionar *Require Microsoft Point-to-Point Encryption (MPPE)* e *Refuse Stateless Encryption* para conseguir isso.

O `pptpconfig` também tem capacidade de adicionar rotas automaticamente. Simplesmente clique na aba *Routing*, marque o botão *Client to LAN* e digite as rotas dos sistemas que devem ser conectados pela VPN.

Muitos usuários Linux preferem o NetworkManager por um simples motivo: ele costuma funcionar. Há plugins para ele que suportam vários protocolos, incluindo OpenVPN, Microsoft PPTP e L2TP. Após instalá-los, basta clicar no ícone de rede e selecionar as conexões VPN para começar a fornecer as informações apropriadas. A **figura 5** mostra as etapas para configurar uma conexão Cisco num sistema Ubuntu.

O NetworkManager suporta a criptografia por chave compartilhada quanto por certificado X.509. Para fazê-lo funcionar adequadamente é preciso instalar o daemon *racoon* para fazer a troca de chaves pela Internet. Depois, deve-se obter com o administrador da rede a chave compartilhada e os certificados assinados, caso eles sejam usados.

IPsec e kernel 2.6

Certifique-se de instalar os daemons certos para a conexão. Se o sistema utilizar alguma versão do kernel 2.6, ele já suporta nativametne o IPsec, mas se for usado o KVpnc ou o vpnc, ainda será preciso instalar o daemon racoon, que se encarrega da troca de chaves em implementações IPsec. Se o racoon não estiver disponível no repositório da distribuição em questão, basta conferir o site do projeto [4].

Para suportar o FreeS/WAN, o padrão antigo para o IPsec, é preciso instalar o daemon *ipsec*; caso contrário a implementação falhará, pois o sistema não conseguirá conduzir as trocas de senha necessárias ao estabelecer o túnel.

Conclusão

Estabelecer uma VPN hoje em dia é muito mais fácil, mas os clientes VPN gráficos ainda não fazem tudo pelo usuário. Apesar de ainda ser trabalhoso fazer a comunicação com servidores Microsoft, Cisco e OpenVPN, basta uma certa dedicação para se obter sucesso. ■

Mais informações

[1] OpenVPN: http://openvpn.net

[2] NetworkManager: http://www.gnome.org/projects/NetworkManager

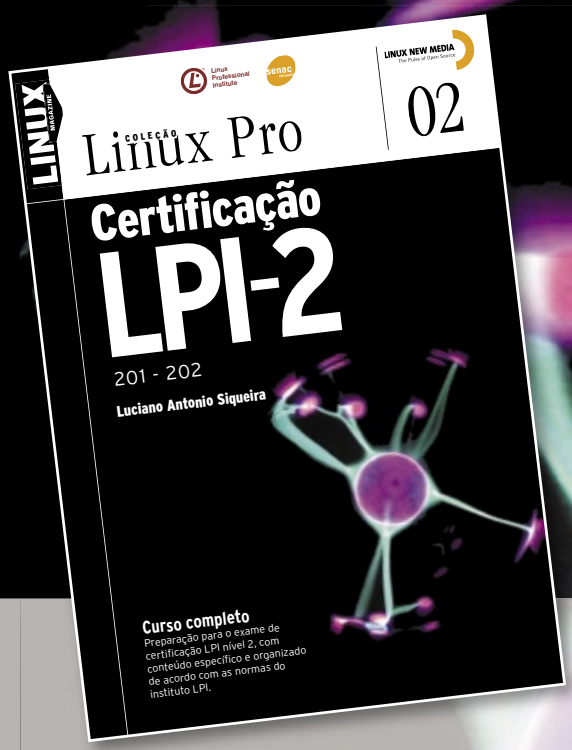
[3] pptpclient: http://pptpclient.sourceforge.net

[4] Rasvpn: http://www.netbsd.org/docs/network/ipsec/rasvpn.html

Coleção Linux Pro

Prepare-se para a principal certificação profissional do mercado Linux

Já em sua **2ª edição**



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

Integração fácil ao Active Directory com o Likewise Open

Na ativa

O Likewise Open oferece integração fácil a ambientes Active Directory. Mostramos como instalar e configurar o sistema de autenticação amigável para administradores.

por Walter Neu

O sistema de autenticação *Likewise Open* [1] integra clientes Linux ao ambiente *Active Directory*. Obviamente, também é possível configurar o Active Directory pelo *Samba* e seus atores coadjuvantes [2], mas a solução da Likewise oferece vários benefícios para facilitar a configuração e a administração.

A versão gratuita e GPL do Likewise suporta autenticação em diretórios AD, a autorização de serviços "kerberizados" e até o recurso de *single sign-on*. Isso pode se parecer bastante com o Samba, que faz as mesmas coisas; na verdade, o gerente de projetos da Likewise, Gerald Carter, é um antigo membro da equipe central de desenvolvimento do Samba. O Likewise Open se aproveita do trabalho do Samba, embora acrescente diversos recursos próprios.

Pacotes prontos

Há pacotes do Likewise para distribuições da Red Hat, Novell e Canonical, além de alguns sistemas Unix comerciais e do MacOS X.

O site do Likewise exibe a versão 5.0, embora os pacotes específicos por distribuição incluam a versão 4, usada neste artigo. Usuários do Ubuntu têm à disposição os pacotes *likewise-open* e *likewise-open-gui* no repositório *Universe*. Os pacotes do Likewise incluem várias dependências – primordialmente relacionadas ao *Kerberos*. O Likewise Open se baseia na versão MIT do Kerberos como *back-end* [3]. Durante a instalação no Ubuntu, o pacote pede para o administrador especificar os servidores Kerberos e administrativo (**figuras 1 e 2**).

Além de um servidor AD e uma estrutura de domínio gerenciada pelo Windows, o Likewise possui dois outros requisitos: um servidor de nomes funcional e um relógio do sistema sincronizado. Se os relógios do cliente e do servidor estiverem mais de cinco minutos fora de sincronia, o servidor Kerberos certamente se recusará a emitir tíquetes por medida de segurança, para evitar ataques.

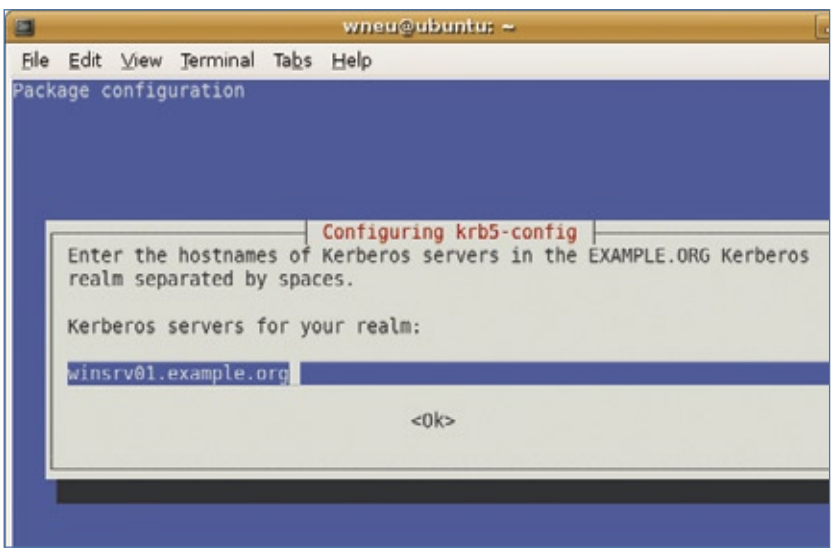


Figura 1 O gerenciador de pacotes do Ubuntu pede o nome do servidor Kerberos ao se instalar os pacotes do Kerberos.

Nova abordagem

Adicionar um sistema Linux "cru" a um domínio exige certo trabalho de configuração [2]. O *Likewise Agent* faz a maior parte desse trabalho, adicionando-se ao *Name Service Switch* (NSS) e aos *Pluggable Authentication Modules* (PAM) no cliente local.

No lado do servidor, o agente repassa as requisições de autenticação ao servidor Kerberos 5 e ao AD baseado em LDAP. Para permitir que isso aconteça, o pacote instala algumas bibliotecas e arquivos de configuração. Por exemplo, `/lib/libnss_lwidentity.so` integra o Likewise ao NSS, e `/etc/pam.d/pam_lwidentity.so` faz o mesmo para o PAM. O arquivo de configu-

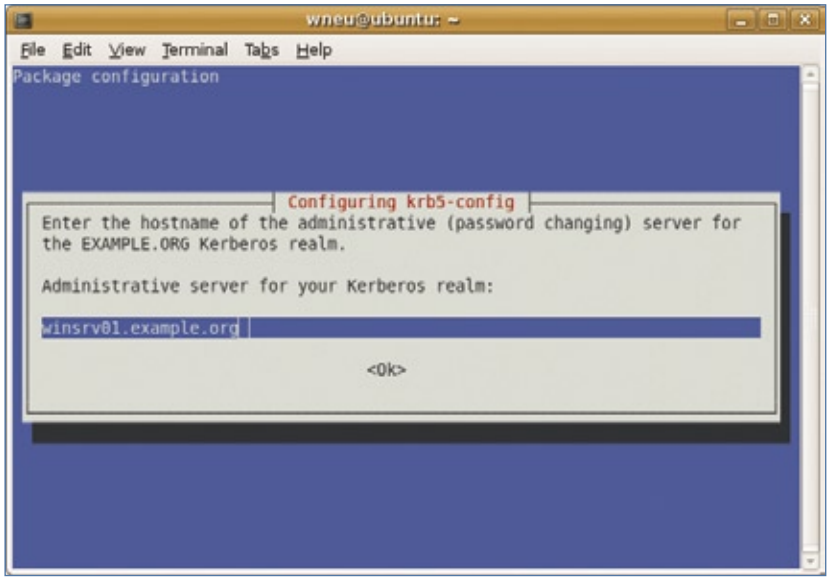


Figura 2 É preciso especificar o servidor administrativo para o domínio do Kerberos.

ração `/etc/security/pam_lwidentity.conf` configura o módulo, e a interface do controlador de domínio remoto é implementada pelo servidor Winbind do Likewise, o *likewise-winbindd*. O servior tem seu próprio arquivo de configuração, `/etc/samba/lwiauthd.conf`, semelhante ao arquivo `smb.conf` do pacote Samba.

O Likewise Open integra esses componentes para suportar um login de domínio transparente para os usuários. O processo de login repassa o nome do usuário e sua senha para o PAM. O módulo *pam_lwidentity.so* se comunica com o serviço de autenticação do Likewise, que gera uma chave secreta a partir do nome e da senha do usuário. O *daemon* do Likewise utiliza a chave secreta para solicitar um *tíquete para solicitação de tíquetes* (TGT, na nomenclatura do Kerberos) ao servidor de autenticação Kerberos, que roda como parte do *Key Distribution Center* (KDC) no servidor AD.

Ao apresentar o TGT, o serviço de autenticação do Likewise recebe tíquetes de serviço para outros serviços de rede, como SSH. Os usuários então já podem fazer logon nos servidores kerberizados sem digitar suas senhas novamente.

Configure o pacote de instalação do Likewise em cada máquina Linux que vai se tornar um membro do domínio AD (e ser gerenciada pelo Likewise). Se forem usados os pacotes de instalação fornecidos no site, o Likewise Open será instalado com uso de um *Bitrock Installer* – um executável cujo nome de arquivo termina com `installer`. Para executar o programa, é preciso tornar-se root e seguir as instruções na tela.

O instalador exibe informações sobre as licenças de código aberto dos componentes instalados antes de o Likewise instalar seus arquivos. Depois disso, o instalador leva o administrador ao `domainjoin-cli`, que se localiza no diretório `/usr/centeris/bin/` (violando assim as convenções do FHS [4]; os pacotes das distribuições e as versões mais recentes do Likewise corrigem esse erro). O agente armazena informações de log em `/var/log/lw-identity/` – se for usada a versão do repositório do Ubuntu – em `/var/log/likewise-open`.

Pode entrar

Um domínio AD precisa que os sistemas usuário e cliente tornem-se membros dele. O ato de criar uma conta de máquina no serviço de diretório da Microsoft é chamado, no idioma do AD, de "juntar-se ao domínio" (ou "Joining the domain", em inglês).

Há uma ferramenta de linha de comando chamada `domainjoin-cli` que permite que o usuário root se junte ao domínio AD, criando uma conta de máquina no diretório nesse processo. A ferramenta `domainjoin-cli` aceita a opção `join` e o domínio como argumentos. O argumento do domínio precisa ser especificado como um nome DNS completamente qualificado.

Além disso, o comando espera o nome de um usuário com autorização para criar contas de computador no ambiente AD. O **exemplo 1** mostra um computador chamado *ubuntu* se juntando ao domínio *exemplo.org*. A conta *Administrator* possui os privilégios necessários para essa etapa.

A segunda opção para se juntar a um domínio é a interface gráfica do Likewise Open (**figura 3**). Porém, a interface não está incluída no pacote básico do programa. Para acrescentá-la, simplesmente instale o pacote *likewise-open-gui* e inicie-o com privilégios de root digitando `domainjoin-gui`.

Manual e automático

Nos dois casos, o Likewise Open lida com a tarefa de configuração em segundo plano, eliminando a necessi-

Exemplo 1: Juntando-se a um domínio

```
01 # domainjoin-cli join example.org
➥ Administrator
02 Joining to AD Domain: example.org
03 With Computer DNS Name: ubuntu.example.org
04
05 Administrator@EXAMPLE.ORG's password:
06 Enter Administrator@EXAMPLE.ORG's
➥ password:
07 SUCCESS
```

dade de etapas manuais complexas. O software modifica as configurações para interação do usuário com o AD (figura 4), incluindo os arquivos necessários para a comunicação do Kerberos com o KDC `krb5.conf` e os arquivos do PAM em `/etc/pam.d/*`.

Para fazer login usando um domínio de cliente Linux, os usuários precisam de um diretório `home` no cliente. O Likewise cria o diretório localmente se for modificado o arquivo `/etc/security/pam_lwidentity.conf`.

O arquivo `/etc/nsswitch.conf` faz o Likewise Open retomar o controle e especifica o método `lwidentity`. O serviço de nomes do NSS verifica primeiro arquivos locais como `/etc/passwd`:

```
passwd: files lwidentity
group:  files lwidentity
```

Se ele não conseguir encontrar uma conta, ele acessa o AD em seguida. Isso significa que usuários locais ainda podem acessar a máquina local caso o AD falhe.

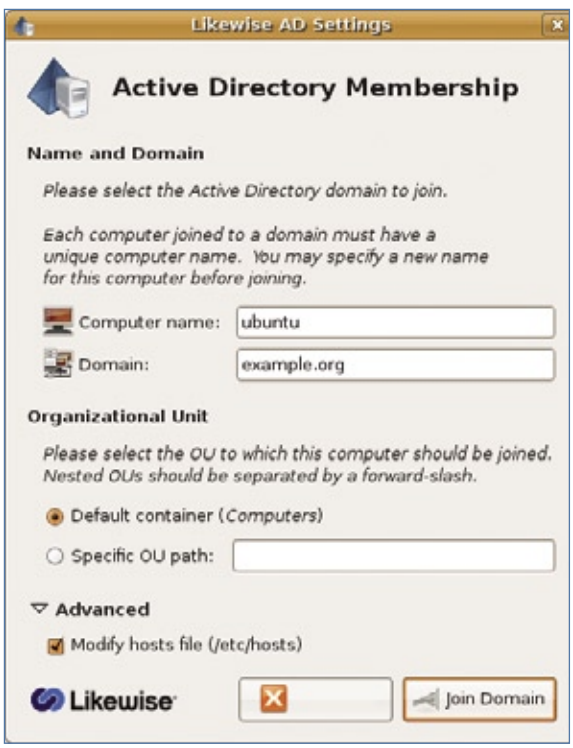


Figura 3 A interface do *Likewise Open* pede o nome DNS do domínio e os nomes das máquinas.

Exemplo 2: klist exibe os tíquetes locais

```
01 $ klist
02 Ticket cache: FILE:/tmp/krb5cc_1560282197
03 Default principal: wane000@EXAMPLE.ORG
04
05 Valid starting     Expires           Service principal
06 08/12/08 13:48:08  08/12/08 23:48:08  krbtgt/EXAMPLE.
➥ORG@EXAMPLE.ORG
07       renew until 08/19/08 13:48:08
08 08/12/08 13:48:08  08/12/08 23:48:08 SUSE$@EXAMPLE.ORG
09       renew until 08/19/08 13:48:08
```

Configuração cuidadosa

O Likewise é cuidadoso na configuração do sistema Linux. Ele cria becapes de todos os arquivos que modifica, acrescentando um sufixo `.lwid-entity.bak`, e por um bom motivo: executar `domainjoin-cli leave` como root na linha de comando ou na interface gráfica apaga a conta da máquina.

Nesse caso, o Likewise recupera todos os arquivos de configuração que tiverem sido alterados. Ele usa o arquivo `/etc/samba/lwiauthd.conf` para permitir que os administradores especifiquem opções de configuração para seu próprio sistema Winbind; essas configurações devem ser familiares àqueles que utilizam o Samba num ambiente AD.

Configuração individual

O parâmetro `template shell` define o shell de login para todos os usuários de forma centralizada. O diretório `home` do usuário não é definido no banco de dados de usuários do AD; portanto, é preciso especificar o caminho no arquivo de configuração com o parâmetro `template homedir` do Samba:

```
template shell = /bin/bash
template homedir = /home/%D/%U
```

O Likewise-Winbind substitui `%D` pelo nome de domínio curto e `%U` pelo usuário do domínio.

Para evitar colisões de nomes em relacionamentos de confiança, faz sentido adicionar o domínio ao caminho do usuário – e aplicar os padrões para diretórios dos usuários. Se a configuração não for alterada, o Likewise Open usará a contrabarra como separador de domínios e nomes de usuários. Obviamente, a contrabarra possui um significado especial em shells Unix. Os especialistas recomendam mudar isso para outro caractere em todos os clientes, usando a variável `winbind separator`. A sugestão é o sinal `+`.

Se houver apenas um domínio, é possível definir `winbind use default domain = yes` para evitar separar o domínio dos nomes de usuários. Se isso não for feito, os usuários do domínio fornecidos pelo Winbind não funcionarão, a menos que se adicione um prefixo de domínio. Reiniciar o Likewise Open por seu script de inicialização aplica as mudanças.

Verboso

O pacote *likewise-open* contém três ferramentas de diagnóstico – `lwinet`, `lwimsg` e `lwiinfo` – úteis para fins de depuração, entre outros.

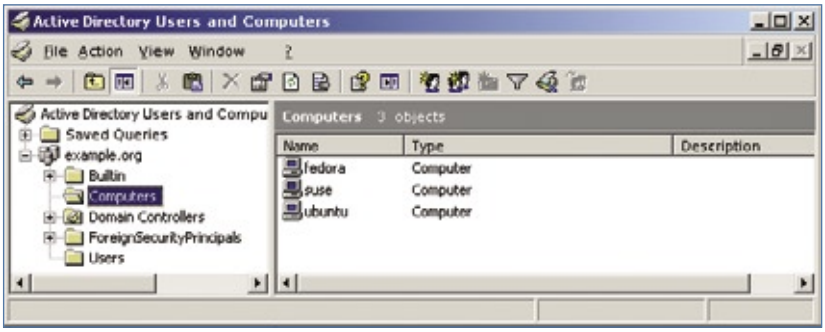


Figura 4 Depois de entrar no domínio, o Likewise cria uma conta de máquina para o computador Ubuntu no *Active Directory*.

Como o Likewise se baseia no código do *Winbindd* do Samba, as ferramentas vão lidar com as tarefas normalmente realizadas pelo daemon Winbind do Samba. Digitando `lwiinfo` é possível verificar a conexão ao controlador do domínio.

A ferramenta corresponde ao `wbinfo` do Samba. As duas consultam o daemon do Winbind. Por exemplo, o `lwiinfo -u` lista todos os usuários do domínio padrão:

```
EXAMPLE+mokr000
EXAMPLE+phkr000
EXAMPLE+wane000
```

O mesmo princípio se aplica a grupos no serviço de diretório, que são exibidos pela opção `-g`. Isso garante que o Linux saiba os nomes do AD. O comado `lwiinfo -g` lista os grupos conhecidos:

```
EXAMPLE+contas
EXAMPLE+marketing [...]
```

Novamente, o Likewise usa o caractere `+`, configurado em `lwiauthd.conf`, como separador no Winbind. A ferramenta `lwimsg` corresponde ao `smbcontrol` e é usada para controlar o Winbindd, definindo o nível de depuração, por exemplo. A contraparte da ferramenta `net` do Samba, usada para administração remota de um domínio, é o `lwinet`.

Após instalar o software, é uma boa idéia tentar fazer logon no AD. O formato do nome do usuário precisa corresponder àquele definido para o serviço de diretório. Por exemplo, se for mantida a configuração padrão para separação entre o domínio e o nome do usuário, mas o separador for alterado para o sinal de soma, os usuários precisarão digitar seus nomes como *DOMÍNIO+usuário* no login pelo console ou por um gerenciador de desktop (veja a **figura 5**):

```
ubuntu Login: EXAMPLE+wane000
Password:
EXAMPLE+wane000@ubuntu:~$
```

Conforme mencionado anteriormente, o Likewise autentica usuários pelo protocolo Kerberos por meio da requisição de um TGT ao KDC antes de prosseguir à instalação local do tíquete no cliente como `/tmp/krb5cc_UID` (veja o **exemplo 2**). O comando `klist` exibe os tíquetes válidos de um usuário.

O usuário que posuir um tíquete tem permissão para acessar serviços kerberizados na rede sem fazer logon separadamente no serviço de rede.

Single sign-on

Para permitir que um serviço de rede dê acesso sem senha a um usuário, o administrador precisa atribuir um *Service Principal Name* (SPN) ao serviço. O SPN identifica o serviço dentro do ambiente AD. O serviço pede um tíquete de serviço para o *Service Principal* ao KDC, identificando-se com seu TGT.

O SPN compreende uma definição de serviço seguida por uma barra e o hostname completamente qualificado do servidor, um símbolo de arroba e o domínio.

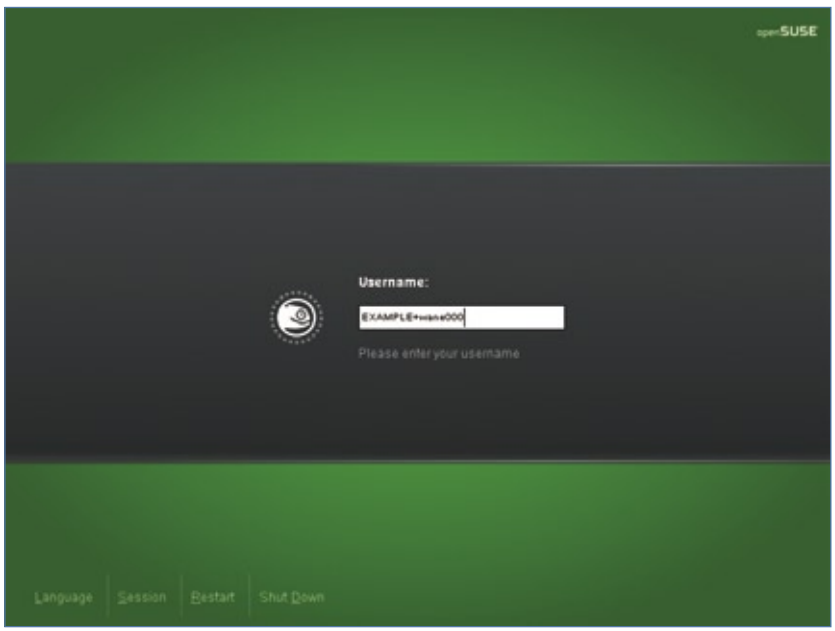


Figura 5 O *GDM* pede um nome para login na autenticação. Neste AD, o nome é composto pelo nome do domínio (*EXAMPLE*), um sinal + e o nome do usuário.

As definições de serviços incluem *host*, *ftp* ou *pop*. Se um usuário estabelecer uma conexão SSH com outro computador membro de um AD gerenciado pelo Likewise, o serviço kerberizado apresentará o TGT do usuário e pedirá um tíquete de serviço ao KDC para, por exemplo, o SPN `host/ubuntu.example.org@EXAMPLE.ORG` – isso pressupõe que o cache local de tíquetes ainda não tenha um tíquete. O tíquete de serviço contém o ID do usuário que faz a requisição e a chave da sessão. O Likewise Open criptografa isso com a chave do servidor e a armazena no cache de usuários como o TGT (**exemplo 3**).

O cliente SSH envia automaticamente o tíquete de serviço criptografado e um *timestamp* também criptografado para validar o *sshd* do autenticador. Isso garante que cada requisição de tíquete seja única, enquanto assegura que o cliente realmente não possui a chave da sessão. Sem o autenticador, seria mais fácil para um agressor capturar um tíquete no tráfego da rede e iniciar um ataque de repetição.

O servidor valida o tíquete de serviço apresentado a ele. Para isso, ele faz referência ao arquivo `/etc/krb5.keytab` local. Esse arquivo armazena a chave do servidor, que o usuário utiliza para decifrar o tíquete de serviço, revelando assim a chave da sessão. O autenticador se baseia na chave da sessão; caso tenha sucesso, o usuário é autenticado sem necessidade de senha (**figura 6**).

Exemplo 3: Tíquetes no cache de credenciais

```
01 $ klist
02 Ticket cache: FILE:/tmp/krb5cc_1560282197
03 Default principal: wane000@EXAMPLE.ORG
04
05 Valid starting     Expires            Service principal
06 08/13/08 15:48:29  08/14/08 01:48:30  krbtgt/EXAMPLE.ORG@
➥EXAMPLE.ORG
07         renew until 08/20/08 15:48:29
08 08/13/08 15:48:30  08/14/08 01:48:30  SUSE$@EXAMPLE.ORG
09         renew until 08/20/08 15:48:29
10 08/13/08 15:48:38  08/14/08 01:48:30  host/ubuntu.example.org@
11         renew until 08/20/08 15:48:29
12 08/13/08 15:48:38  08/14/08 01:48:30  host/ubuntu.example.
➥org@EXAMPLE.ORG
13         renew until 08/20/08 15:48:29
```

Exemplo 4: Montagem de compartilhamentos Samba

```
01 <?xml version="1.0" encoding="UTF-8"?>
02 <pam_mount>
03 <volume user = "*"
04    server = "SAMBASERVER"
05    mountpoint = "/home/EXAMPLE/%(USER)/Document"
06    path = "%(USER)"
07    fstype = "smbfs" />
08 </pam_mount>
```

Conexão

O Likewise Open configura automaticamente clientes SSH pré-existentes e outros clientes ao se juntarem ao domínio, permitindo que usem o Kerberos para se autenticarem no futuro. No lado do servidor, o Likewise adiciona as linhas:

```
GSSAPIAuthentication yes
GSSAPICleanupCredentials yes
```

ao arquivo de configuração `/etc/ssh/sshd_config`. O Likewise também acrescenta as seguintes linhas para um cliente SSH:

```
GSAPIAuthentication yes
GSSAPIDelegateCredentials yes
```

A instrução `GSSAPIDelegateCredentials` passa o TGT para o servidor de destino. Para todas as outras configurações, o software utiliza a *Generic Security Services API* (API de serviços genéricos de segurança, GSSAPI), uma interface genérica para serviços de segurança como o Kerberos.

Figura 6 O *Likewise* implementa o *single sign-on* por meio do Kerberos. Os usuários não precisam digitar uma senha para fazer logon.

Exemplo 5: Configuração do pam_mount

```
01 # /etc/pam.d/common-auth
02 auth    required   pam_mount.so
03 auth    sufficient /lib/security/pam_lwidentity.so
04 auth    requisite  pam_unix.so nullok_secure try_first_pass
05 auth    optional   pam_smbpass.so migrate missingok
06
07 # /etc/pam.d/common-session
08 session optional   pam_mount.so
09 auth    sufficient /lib/security/pam_lwidentity.so
10 session required   pam_unix.so
```

Local

Na primeira vez em que um usuário do domínio faz logon num cliente, o Likewise Open usa o PAM (*pam_lwidentity.so*) para criar diretórios locais para esse usuário. Alternativamente, o módulo *pam_mount* pode montar diretórios centrais do usuário num servidor remoto por SMB/CIFS [5]. Isso garante a todos os usuário o acesso a seus próprios arquivos, independentemente do cliente usado por eles no login. O compartilhamento é definido por uma linha no arquivo `/etc/security/pam_mount.conf` que usa a palavra-chave `volume`:

```
volume usuário sistema_de_arquivos
➥ servidor compartilhamento
➥ ponto_de_montagem opções algoritmo
➥ caminho
```

A presença de um curinga (`*`) no parâmetro `usuário` faz o módulo inserir o nome do usuário. `Sistema_de_arquivos` pode ser `smbfs` ou `cifs`. O `servidor` pode ser um IP ou um nome NetBIOS, e `compartilhamento` pode usar o `&` como curinga para o nome do usuário.

Os três últimos parâmetros geralmente não são necessários; traços são aceitáveis nesse caso: montar o diretório `Documentos` ou o diretório `home` completo é questão de gosto e depende de como a empresa organiza seus servidores centrais.

Caso o ponto de montagem não exista, o módulo *pam_mount* do PAM o cria, se sua opção `mkmountpoint 1` estiver presente. Na versão 0.29, o *pam_mount* armazena as configurações num formato XML equivalente, conforme mostra o **exemplo 4**.

Antes das linhas `sufficient` na seção `auth` de `/etc/pam.d`, é possível inserir uma linha para o módulo. O **exemplo 5** mostra uma configuração nos arquivos `common-auth` e `common-session` no Ubuntu. Para evitar a necessidade de os usuários digitarem suas senhas repetidamente, a linha `tr_first_pass = yes` do arquivo `/etc/security/pam_lwidentity.conf` ativa a opção para tentar novamente uma senha já digitada antes.

Versão comercial

Além da versão de código aberto do Likewise, a corporação americana Likewise Software oferece uma versão comercial de seu software o *Likewise Enterprise* [6]. A versão comercial possui suporte a políticas de grupo no AD além das funcionalidades oferecidas pela versão livre; o produto define aproximadamente 500 políticas padrão. O *Likewise Administrative Console* é capaz de usar uma máquina Linux ou Unix para gerenciar registros do AD.

Além disso tudo, o Likewise Enterprise suporta desktops Linux que fazem referência ao AD para obtenção de configurações e restrições. Isso ativa a implementação de políticas estritas de segurança. A variante corporativa está disponível gratuitamente para fins de avaliação, ou por US$ 250 na versão para servidores. A empresa oferece dois níveis de suporte comercial.

Nova cara

Uma vez configurado, o Likewise Open oferece o mesmo escopo funcional de uma combinação de Samba, Kerberos, PAM e NSS. Ele livra o administrador de várias tarefas monótonas e repetitivas de configuração e suporta o gerenciamento de usuários centralizado e independente de plataforma. O serviço de autenticação por tíquetes do Kerberos e o single sign-on são bônus.

Quem se interessar pelo Likewise Open pode apreciar os recursos adicionais oferecidos pela versão comercial, ou os benefícios do suporte profissional. O único trabalho manual que resta para o administrador é o gerenciamento centralizado dos diretórios dos usuários. ■

Mais informações

[1] Likewise Open: http://www.likewisesoftware.com/products/likewise_open/

[2] Walter Neu, "Domando os cães do inferno": http://lnm.com.br/article/2424

[3] Kerberos MIT: http://web.mit.edu/kerberos/

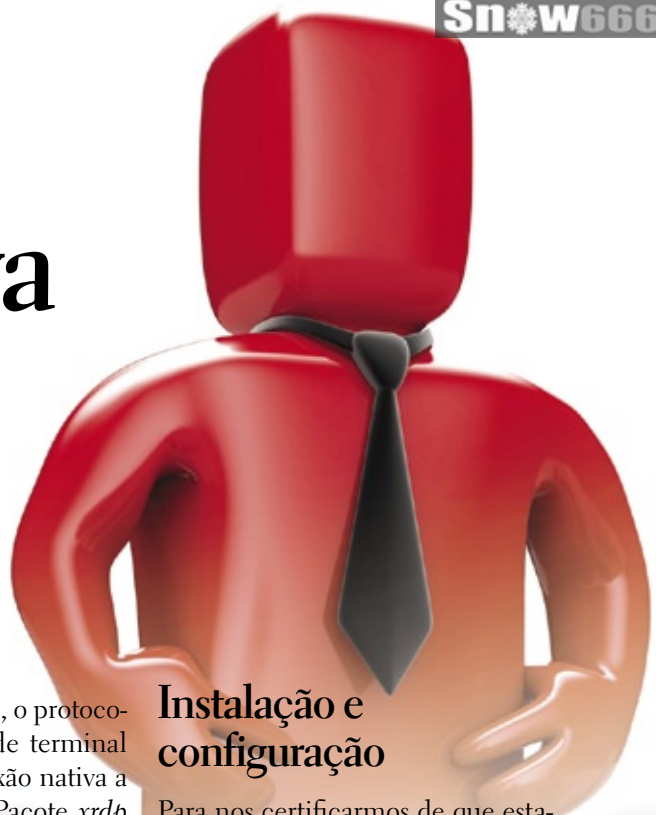
[4] Padrão Hierárquico de Arquivos (FHS): http://www.pathname.com/fhs/

[5] Montagem de diretórios home com PAM: http://pam-mount.sourceforge.net/

[6] Likewise Enterprise: http://www.likewisesoftware.com/products/likewise_enterprise

Serviço RDP Linux para clientes de terminal Windows

O manda-chuva do terminal



O xrdp ajuda os seus clientes de terminal Windows a se conectarem ao Linux.

por Kenneth Hess

A conexão de desktops remotos do Windows no Linux geralmente consome bastante banda da rede, é insegura e difícil de configurar. E se um sistema Windows pudesse se conectar a um sistema Linux tão facilmente quanto o faz com outro sistema Windows – utilizando, para isso, o mesmo aplicativo usado para conectar originalmente ao Windows?

O *xrdp* é uma implementação de código aberto do RDP (*Remote Desktop Protocol* – ou Protocolo de Ambiente de Trabalho Remoto, na tradução em português), o protocolo usado nos serviços de terminal do Windows para conexão nativa a desktops Windows. O Pacote *xrdp* fornece a funcionalidade RDP, bem como um servidor gráfico que seja capaz de aceitar conexões do *rdesktop* [1] e de clientes de serviços de terminais Windows.

Figura 1 Janela de conexão com o desktop remoto.

Figura 2 Forneça seu usuário e sua senha do sistema Linux.

Uma vez conectado e autenticado no servidor RDP Linux, o usuário remoto terá disponível um ambiente de trabalho Linux em modo gráfico. E o melhor é que não é necessário executar um servidor gráfico na máquina com Windows, nem é preciso exportar a tela do Linux para o computador com Windows.

Configurar o servidor RDP no Linux é fácil e leva apenas alguns minutos. Para os usuários novatos de Linux ou os administradores de sistemas Windows, segue a lista de requisitos necessários para fazer o sistema funcionar:

- uma conta de usuário padrão na máquina Linux;
- acesso remoto ou ao console do servidor Linux;
- acesso com privilégios administrativos (de root) no servidor Linux.

Também ajuda se você souber alguma coisa sobre RDP e sobre a otimização da configuração de um cliente RDP.

Instalação e configuração

Para nos certificarmos de que estamos usando a versão mais recente do xrdp, vamos instalá-lo a partir do código-fonte. Há pacotes do programa para algumas distribuições, o que pode facilitar a instalação e a integração à distribuição. Porém, o objetivo deste artigo é possibilitar a instalação em qualquer sistema. Assim, baixe o código-fonte do pacote *xrdp* [2], descompacte-o e compile-o:

```
$ tar zxvf xrdp-0.4.1.tar.gz
$ cd xrdp-0.4.1
$ make
```

Em seguida, instale-o usando privilégios de root:

```
# make install
```

Os arquivos executáveis, scripts e bibliotecas serão instalados no diretório `/usr/local/xrdp/`, e os arquivos de configuração no diretório `/etc/xrdp/`.

A documentação do aplicativo é um pouco obscura sobre o que fazer a seguir. Embora tenhamos decidido no começo não mudar nenhum dos parâmetros nos arquivos `sesman.ini` e `xrdp.ini` disponíveis em `/etc/xrdp/` e tenhamos abordado a situação

Tabela 1: Níveis de execução no Linux

0	Desligar
1	Modo monousuário
2	Multiusuário, sem NFS
3	Multiusuário, completo
4	Não utilizada
5	X11 (gráfico)

Detalhe: há distribuições que utilizam o nível 4 como ambiente gráfico, semelhante ao nível 5.

como um administrador de sistemas Windows, assumindo que as coisas iriam funcionar sem necessidade de muitos ajustes à configuração, nesse ponto essa abordagem começa a se tornar frustrante.

Uma vez com o sistema instalado, os seguintes comandos devem ser executados como root:

```
# cd /usr/local/xrdp
# cp xrdp_control.sh /etc/init.d/
➥xrdp_control
```

Em seguida, em distribuições derivadas do Red Hat, os seguintes comandos se aplicam:

```
# chkconfig --add xrdp_control
# chkconfig xrdp_control on
# service xrdp_control start
```

Já em distribuições derivadas do Debian, esses são os comandos:

```
# update-rc.d xrdp_control
➥defaults
# update-rc.d xrdp_control start
➥80 3 4 . stop 0 1 6 .
# /etc/init.d/xrdp_control start
```

O script `xrdp_control.sh` controla os serviços de ativação, desativação e reinicialização do programa. Ao copiar o script para o diretório `/etc/init.d/`, pode-se retirar a extensão `.sh` por motivos estéticos – nenhum outro script desse diretório possui essa extensão, embora todos sejam scripts de shell.

Em sistemas baseados em Fedora/Red Hat, o comando `chkconfig` é um utilitário para atualizar e buscar informações sobre o nível de execução para serviços de sistema, manipulando os vários links simbólicos em `/etc/init.d/`, para aliviar um pouco os administradores de sistema da tarefa tediosa de editar os links simbólicos e a necessidade de manipular esses serviços manualmente.

Há pacotes para esse aplicativo disponíveis para outras distribuições, como Debian e Ubuntu, mas o correto é usar a ferramenta adequada para a sua distribuição.

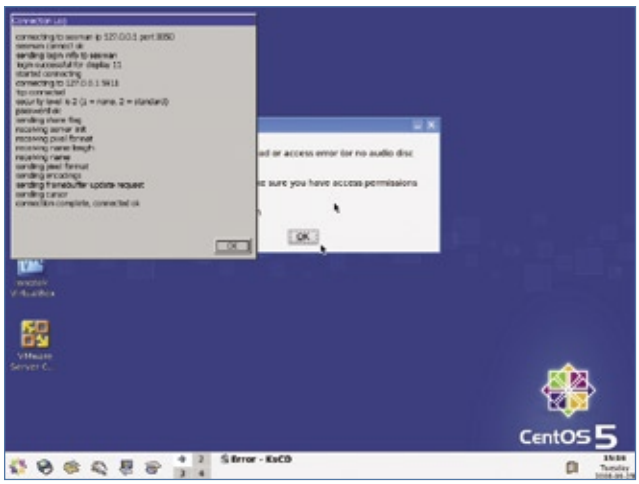


Figura 3 Registro do gerenciador de sessão da conexão xrdp.

Assim, para criar um novo serviço de inicialização, copie seu script de controle para `/etc/init.d/`, conforme mostrado acima, e então use o comando `chkconfig` para ativá-lo. A linha `chkconfig xrdp_control on` define os níveis de execução (*runlevels*) do serviço (ver **tabela 1**). Por exemplo, o comando `# chkconfig --level 35 xrdp_control` configura o `xrdp_control` para funcionar nos níveis de execução 3 e 5. O último comando na listagem acima inicia os serviços `sesman` e `xrdp`.

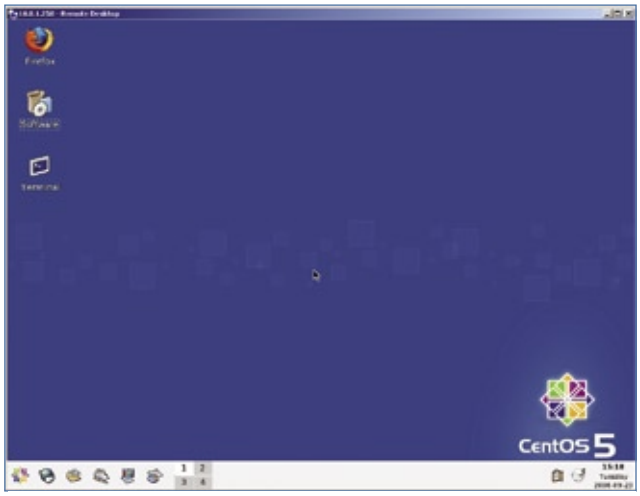


Figura 4 Uma conexão com o desktop pronta para usar.

Para se conectar ao serviço RDP no servidor Linux a partir de um PC com Windows, basta fazer exatamente como se faria com um servidor Windows, como mostra a **figura 1**.

O cliente RDP abre uma nova janela, conforme ilustrado na **figura 2**, solicitando o nome de usuário e a senha, que são aqueles configurados no servidor Linux. Forneça um nome e uma senha válidos e clique em *OK*. Mesmo que a máquina Linux esteja configurada para usar um domínio do serviço *Active Directory*, ainda será preciso adicionar cada usuário aos sistemas Linux que se desejar acessar via RDP. Para fazer isso, crie primeiramente um grupo para todos os usuários do serviço RDP:

```
# groupadd rdpusers
# useradd -g rdpusers fulano
# passwd fulano
```

Caso o usuário já exista no sistema, use o comando `usermod` para adicioná-lo ao grupo de usuários do serviço RDP:

```
# usemod -G rdpusers fulano
```

Embora não seja explicitamente necessário para o acesso, um grupo especial simplifica a administração do sistema. Forneça agora o nome do usuário criado e a sua senha, e então clique em *OK*.

A tela mostrada na **figura 3** deverá aparecer. Essa é a janela de registro do gerenciador de sessões da conexão, que ilustra a negociação entre o cliente e o servidor. Perceba que o gerenciador de sessões conecta primeiramente à porta associada ao serviço RDP e então à porta de um serviço VNC, para então apresentar o desktop Linux a você. A **figura 4** mostra um desktop CentOS 5.

Quando desconectando de uma sessão RDP em Linux, você verá a tela mostrada na **figura 5**. Perceba que somente duas ações estão disponíveis: *Encerrar sessão atual* e *Cancelar*, que são recursos padrão de conexões VNC remotas.

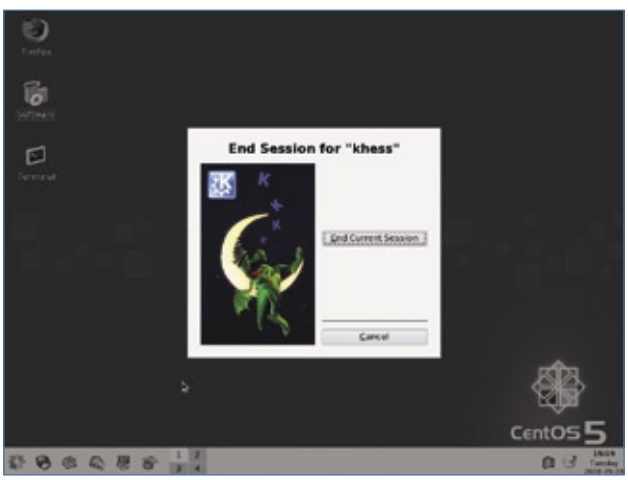


Figura 5 Janela de finalização de sessão do VNC.

O servidor Linux executa os programas `xrdp` e `sesman` e fica aguardando conexões RDP. Assim que um cliente de serviços de terminais Windows tenta se conectar ao servidor RDP, o servidor e o cliente negociam um nível de criptografia, trocam chaves e verificam quais recursos estão disponíveis. A partir daí, o cliente escolhe a quantidade de cores e a resolução da tela que será usada na sessão.

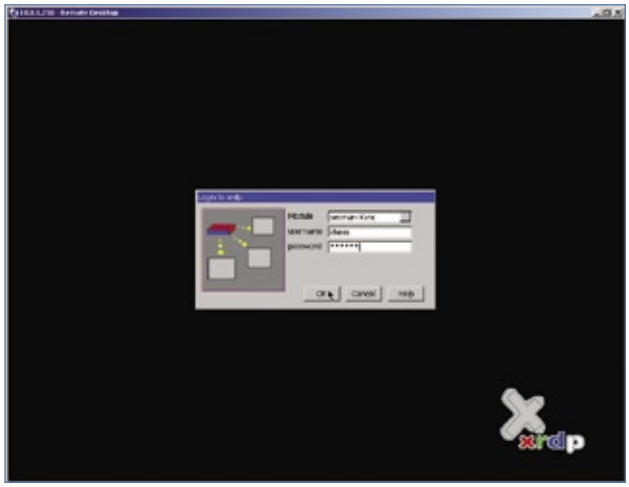


Figura 6 Tela de login do xrdp.

Se o usuário fornecer um nome e uma senha no aplicativo cliente, a autenticação é iniciada. Caso contrário, o usuário seleciona o módulo de uma lista do tipo *drop-down* e fornece um usuário e uma senha na tela de login, conforme ilustra a **figura 6**.

O módulo *libvnc* é carregado e uma conexão TCP é feita para o endereço 127.0.0.1 ou para o endereço IP especificado no arquivo `/etc/xrdp/xrdp.ini`. As credenciais de login do usuário, a resolução da tela e a quantidade de cores são fornecidas ao aplicativo `sesman` para fins de autenticação. Se o `sesman` encontrar uma sessão ativa com a resolução e a quantidade de cores especificadas, ele retorna essa tela ao usuário. Caso contrário, ele inicia uma nova instância *xvnc* com as especificações de ambiente do usuário.

Conclusões

O xrdp é fácil de instalar, configurar, customizar e usar. E – o que é melhor – não é necessário experiência em Linux para trabalhar com essa poderosa ferramenta. Como não há o que instalar no cliente Windows, não dá para se complicar com o xrdp.

Muito embora este artigo não mostre qualquer tipo de análise extensiva de desempenho de rede ou uso de banda com esse aplicativo, como se trata de RDP, é sabido que a performance começa a cair quando o número de usuários simultâneos conectados se aproxima da marca de 25. Contudo, vale a pena conhecer o xrdp e integrá-lo ao seu arsenal de ferramentas independentes de plataforma. ■

Mais informações

[1] rdesktop: http://www.rdesktop.org/

[2] xrdp: http://xrdp.sourceforge.net/

Sobre o autor

Ken Hess é editor de material técnico e jornalista freelance. Ele escreve sobre uma grande variedade de temas envolvendo sistemas de código aberto, entre eles Linux, bancos de dados e virtualização. Agradecimentos especiais a Jay Sorg, do projeto xrdp, e a Matt Chapman, do projeto rdesktop, pela ajuda no desenvolvimento deste artigo.

Complete a sua coleção

Mais informações

Site:

www.linuxmagazine.com.br

Tel: 11 4082-1300

LINUX MAGAZINE

LINUX NEW MEDIA
The Pulse of Open Source

O agendador Open Source Job Scheduler

Muito além do Cron

Planejar e agendar tarefas computacionais pode exigir muito trabalho, principalmente se abranger múltiplas máquinas. Conheça uma ferramenta que facilita muito essa área.

por James Mohr

A possibilidade de realizar uma certa tarefa num momento específico ou em intervalos regulares é obrigatória para administradores de sistemas. O *cron daemon* original oferece um método fácil para agendar tarefas em sistemas baseados em Unix. Embora o Cron tenha recebido diversas melhorias ao longo dos anos, suas versões mais recentes ainda são projetadas para agendamentos muito simples. Administradores que precisam de algo minimamente incomum são obrigados a criar scripts ou a incluir os recursos de que precisam em um dos scripts iniciados pelo Cron.

Imagine quanto tempo seria economizado se não fosse mais necessário criar e alterar esses scripts ou ter qualquer outro trabalho para fazer com que os programas reajam a condições de erro e sejam executados na exata hora em que deveriam. Vários produtos comerciais oferecem esse recurso, mas podem significar uma mordida no orçamento de TI. Felizmente o mundo do Código Aberto também oferece soluções de agendamento além do Cron.

Assim como em qualquer software de agendamento, a unidade primária é o *job*, ou tarefa, que geralmente é um script ou programa iniciado pelo software de agendamento. Em vários casos, o Cron é suficiente para suprir os requisitos mais básicos de agendamento, tais como executar uma tarefa uma vez por dia (becapes, por exemplo), ou tarefas que precisem ser executadas em intervalos mais freqüentes, menos freqüentes ou em datas específicas.

Porém, quando começamos a lidar com dependências de algum tipo, rapidamente é possível perceber as limitações do Cron – por exemplo, se for necessário iniciar um programa específico após um certo evento. Há casos de verdadeiras séries de comandos que precisam ser executados em ordem e precisam todos ter sucesso – se um dos comandos falhar, a execução dos seguintes causaria grandes problemas. Nem as versões mais novas do Cron conseguem lidar com isso, principalmente se for necessário iniciar uma tarefa já no meio da cadeia de comandos.

Muitas tarefas precisam ser gerenciadas em múltiplas máquinas, então um bom software de agendamento permite que se gerencie todas as máquinas a partir de um ponto central, inicie tarefas remotamente e assim por diante. Para distribuir *crontabs* para essas máquinas remotas, pode-se usar o *Rsync*, mas isso rapidamente se torna um pesadelo administrativo quando a configuração é diferente ao longo das máquinas, ou quando as tarefas às vezes precisam ser iniciadas manualmente, ou ainda quando há

outras tarefas que não fazem parte do Cron.

Multiplataforma

Apesar de ser possível instalar versões abertas do Cron no Windows, lidar com diferentes sistemas operacionais causa ainda mais problemas. Por exemplo, alguns dialetos de Unix não suportam um arquivo `/etc/crontab` central, então é preciso criar um arquivo para cada usuário. O Cron era uma boa ferramenta nessa época, e geralmente ainda é, mas as necessidades de muitas empresas já superam suas funcionalidades.

As limitações do Cron não passaram despercebidas. Há produtos comerciais que custam pequenas fortunas e costumam ser licenciados com base no número de servidores ou de scripts a serem iniciados.

Por sua vez, os problemas dos produtos comerciais também não passaram despercebidos pela comunidade do Código Aberto. Uma solução surpreendente é o *Open Source Job Scheduler*, desenvolvido pela alemã SOS (*Software- und Organisations-Service*). Há versões para Linux, Solaris, HP-UX (PA-RISC, IA64), AIX e Windows. Ele também suporta vários bancos de dados, incluindo *DB2*, *Oracle*, *MS SQL Server*, *PostgreSQL* e *MySQL*.

O software adota um esquema de duplo licenciamento pela GPL e a *Guaranteed License* (Licença Garantida). Trata-se do mesmo código, com funcionalidades, atualizações e código-fonte idênticos.

A receita da SOS não provém da venda de seu produto, mas dos serviços e do suporte. Porém, estranhamente, a empresa não anuncia seu produto – nem seus serviços – da forma tradicional. Ao demonstrar o produto, o objetivo não é convencer clientes potenciais, mas mostrar-lhes o que o produto pode fazer e deixar que eles decidam se ele supre suas necessidades.

A versão comercial também oferece uma "pessoa responsável" para cada chamado de serviço, com tempos de resposta garantidos, e pedidos de recursos recebem maior prioridade de implementação. Além disso, essa versão não possui as restrições da GPL, então pode ser embutida em outros aplicativos (comerciais ou não) sem que este precise aderir à GPL.

Diferente da maioria dos softwares comerciais e de código aberto, a SOS oferece garantia limitada de dois anos e um acordo de indenização. Segundo seu diretor, a empresa se sente obrigada a fornecer ao cliente um retorno por seu pagamento, e isso também se estende a discrepâncias entre o produto e a documentação.

Estrutura

O componente central do pacote é o mecanismo de agendamento de tarefas, que roda em cada uma das máquinas que as **agendarão**. Esse método é diferente de **executar** a tarefa: pode-se ter um agendador em cada máquina, com todos agindo como escravos de um central, mas também é possível usar um agendador completo em cada uma delas. Esse mecanismo pode ser expandido para permitir o balanceamento de carga por meio de múltiplos servidores.

Um aspecto importante a ser considerado é chamado de *order* (pedido), que consiste em um sinal passado entre tarefas. Dependendo de suas configurações, as tarefas não têm permissão de iniciar até receberem seu pedido.

Na forma mais simples, pedidos são como o bastão numa corrida de revezamento, entregues por cada tarefa para a seguinte. Além disso, é possível configurar pedidos com horas específicas de início para que sejam gerados automaticamente pelo sistema no momento especificado e depois a cadeia respectiva possa se iniciar.

Note que, para conseguir reagir a um pedido, uma tarefa precisa ser configurada para aceitá-lo, mas o pedido só pode ser associado a uma

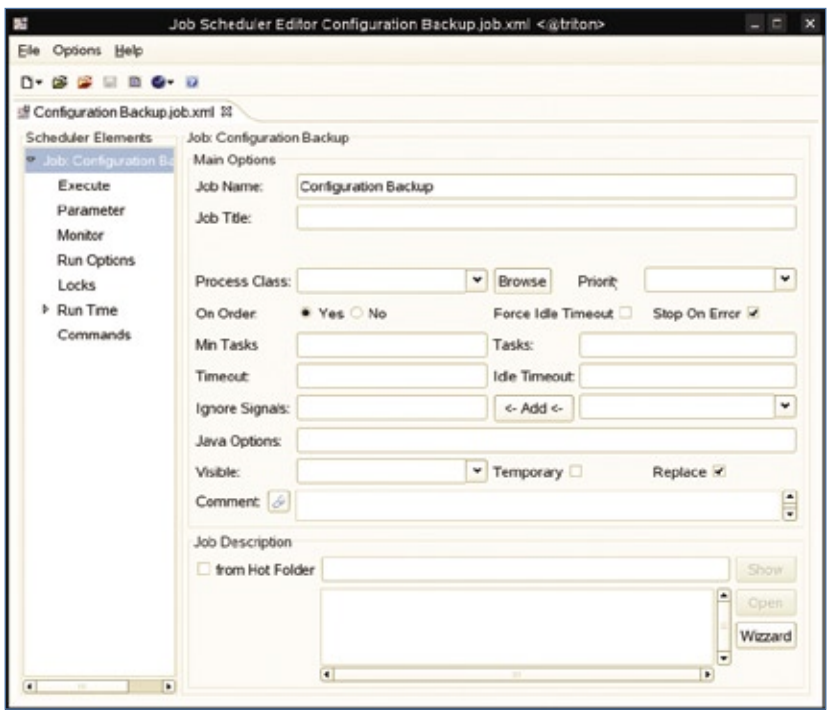


Figura 1 Janela do editor gráfico do agendador de tarefas.

cadeia de tarefas, e não a uma tarefa específica. Ou seja, o pedido é passado de tarefa para tarefa dentro da cadeia, mas é associado somente à cadeia. Se for desejável que uma única tarefa se inicie num momento específico, por exemplo, isso pode ser feito dentro da própria tarefa. Outro componente importante são os *Hot Folders* (pastas quentes), que seão diretórios monitorados pelo agendador em busca de alterações, tais como a alteração ou criação de tarefas.

Tarefas

Tarefas podem ser configuradas a partir da interface gráfica do editor do agendador (**figura 1**, chamado aqui de "editor de tarefas"), ou por arquivos XML editados manualmente. O editor de tarefas é um aplicativo em Java que configura várias tarefas, cadeias e outros aspectos do sistema. Todas as informações de configuração do sistema são armazenadas em arquivos XML, e basta abrir o arquivo XML respectivo no editor de tarefas para fazer alterações. Poder usar o *Vim* em arquivos de configuração é mais que uma bênção em casos de alterações em massa.

Os arquivos XML podem ser copiados para máquinas remotas e salvos via FTP diretamente a partir do editor de tarefas. Quando aterrissam num Hot Folder, os arquivos ficam imediatamente disponíveis para o mecanismo do agendador na máquina remota.

A interface gráfica do editor de tarefas não é tão intuitiva quanto poderia, e vários campos parecem misteriosos a princípio. Como a documentação deixa a desejar, faltam explicações sobre muitos desses campos. Em alguns casos a documentação dos arquivos XML ajuda a tirar as dúvidas.

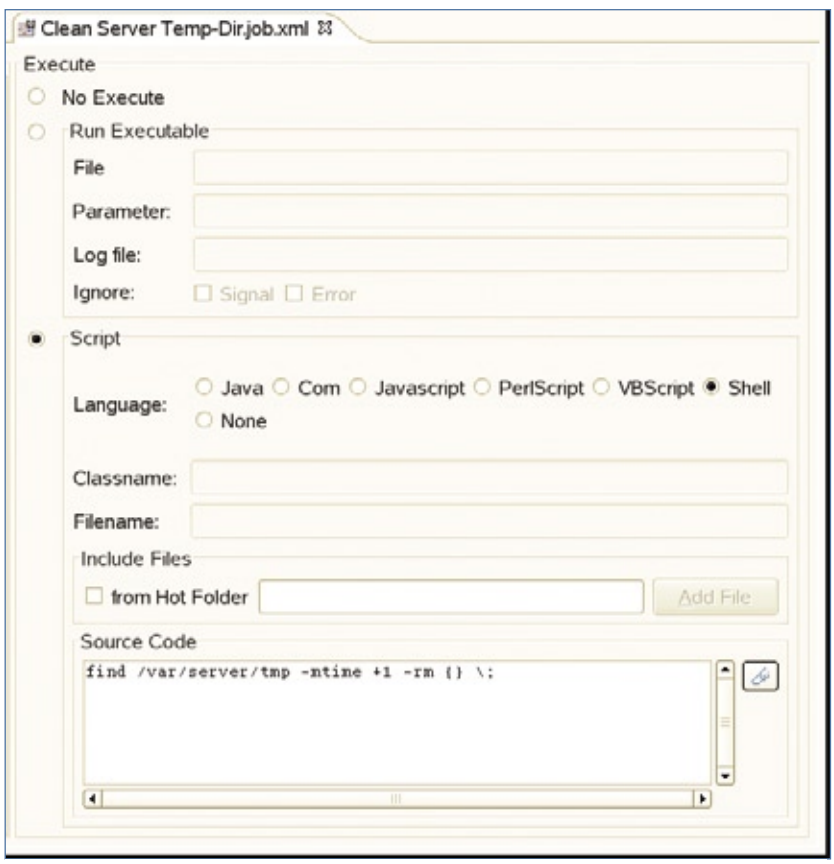


Figura 2 Digitação do código-fonte diretamente no editor de tarefas.

Apesar de as informações de configuração serem armazenadas em arquivos XML por padrão, é possível configurar o agendador para usar diversos bancos de dados diferentes. Essas tarefas são chamadas de "gerenciadas", e cada agendador instalado pode ser configurado para acessar as tarefas no banco de dados para não ser necessário copiar os arquivos manualmente.

A operação cotidiana do sistema é realizada pela sua interface gráfica (chamada neste artigo de "interface de operação"), que é acessada por um navegador e permite o gerenciamento das tarefas a partir de qualquer máquina. Com essa interface, é possível não apenas monitorar as tarefas, mas também iniciá-las, pará-las, tratar seus erros e muitas outras funções.

O agendador de tarefas também oferece uma API que permite o gerenciamento e o controle externos de tarefas. A API suporta várias linguagens, incluindo Perl, VBScript, JavaScript e Java. Surpreendentemente, não há suporte a PHP, apesar da possibilidade de se gerenciar tarefas a partir de um navegador web e da documentação de scripts PHP de exemplo.

Instalação

Os exemplos deste artigo foram feitos com a versão 1.3.4 para Linux, que pode ser baixada do site do Job Scheduler no SourceForge [1]. Se houver intenção de se usar um banco de dados MySQL como neste artigo, note que o programa não fornece um driver JDBC para esse banco, embora haja drivers para Oracle e outros bancos. O driver JDBC para MySQL pode ser baixado diretamente do site do MySQL [2]. Basta digitar o caminho do arquivo `.jar` apropriado durante a instalação.

Antes de começar, é recomendável ler o guia de instalação em

PDF incluído no pacote. Além disso, há vários outros PDFs no site da empresa [3] mais aprofundados em diversos tópicos. Fique ciente: até para obter as informações mais básicas na documentação é preciso ser um tanto familiarizado com a programação orientada a objetos e XML, pois a documentação não fornece qualquer introdução a esses tópicos. Além disso, ela não é bem organizada, então saiba que será preciso procurar bastante. Apesar de ser volumosa, a documentação não é fácil de usar, o que é algo que a empresa pretente melhorar.

No Linux, a instalação ocorre por meio de um instalador em Java e, se for feita por um usuário normal, o padrão é os arquivos serem abrigados em `$HOME/scheduler/`. Se for instalado como root, o diretório do programa é `/usr/local/scheduler/`. Após instalar o produto, há um arquivo `README` que recomenda que o programa não seja instalado como root, mas não há menção a isso no guia de instalação e configuração. Para evitar problemas potenciais, vamos instalá-lo como usuário normal.

Durante a instalação, são pedidos o tipo do banco de dados e informações da conexão. Não fica claro se o campo "database parameters" deve receber os parâmetros de conexão após o banco de dados estar em execução ou os parâmetros de conexão para criação do banco de dados. Infelizmente, recomenda-se criar um banco de dados e um usuário para o programa usar, mas isso só é mencionado **após** todas as etapas de instalação. Criar o banco de dados manualmente e conferir privilégios do banco antes de iniciar a instalação já resolve.

A instalação é relativamente intuitiva, mas leva alguns minutos para criar e preencher as tabelas do banco de dados. Para instalar o Scheduler em múltiplas máquinas com os mesmos parâmetros, há a opção de criar um script automaticamente ao final da primeira instalação.

Iniciando

Independentemente de a instalação ocorrer sob o root ou um usuário normal, é necessário iniciar o agendador manualmente. Seu controle é feito como num script *rc* comum:

```
$HOME/scheduler/bin/jobscheduler.
➥sh start
$HOME/scheduler/bin/jobscheduler.
➥sh stop
```

Para iniciar o Scheduler automaticamente na inicialização, recomenda-se criar um usuário específico para ele e depois um script rc que use o comando `su` para se tornar esse usuário e iniciar o programa. Se houver necessidade de tarefas serem executadas sob o root ou outro usuário com mais privilégios, é possível configurar um ambiente `sudo` apropriado.

Novas tarefas

Para criar tarefas, pode-se ou editar os arquivos XML diretamente ou pelo editor de tarefas. No Linux, execute o script `jobeditor.sh`, localizado por padrão em `/usr/local/scheduler/bin/` ou `$HOME/scheduler/bin/`.

Como exemplo, considere a tarefa típica de criação de um becape da configuração do sistema. Por ora, vamos supor que isso seja feito diariamente com o script `/usr/bin/becape.sh`.

Primeiramente, inicie o editor de tarefas e selecione *New* | *Hot Folder Element* | *Job* (**figura 1**). No primeiro formulário, comece digitando as informações básicas de sua tarefa. Para este exemplo, digite o nome `Becape das configurações`; no campo *Job Title*, adicione uma descrição ou deixe em branco.

No painel esquerdo, clique em *Execute* para digitar os detalhes sobre o programa ou script que se deseja iniciar. Como o objetivo é executar um script externo, selecione o botão

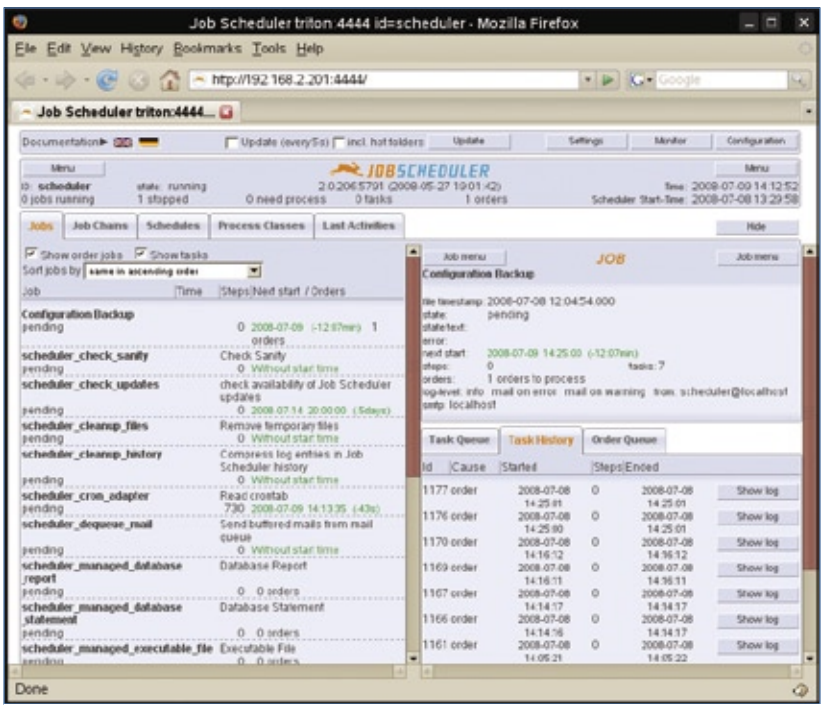


Figura 3 Interface de operação do *Job Scheduler*.

Run executable e digite o caminho completo do script referido. Nesse ponto também é possível definir masi parâmetros a ser passados para o script. Por exemplo, se o becape comprimir os arquivos armazenados, pode ser interessante acrescentar um `-c` a esse campo.

Além disso, pode-se incluir os passos individuais de execução selecionando-se o botão *Script* e o tipo de código do programa, depois digitando o código-fonte na caixa apropriada. Note que isso é mais que o nome de um script, e pode incluir estruturas de programação baseadas na linguagem selecionada (**figura 2**).

Para salvar a tarefa, pressione o botão *Save* ou escolha *Save* no menu *File*. Na primeira vez em que o arquivo é salvo é preciso digitar um nome para ele. Para isso, navegue até o diretório `../config/live/` e salve o arquivo como `becape`; assim, a extensão `.xml` será adicionada automaticamente.

Via navegador

Como o arquivo foi salvo no diretório `live/`, ele fica imediatamente visível para o sistema. Esse diretório é pré-definido como um *Hot Folder*, que o sistema lê regularmente. Nesse ponto, a tarefa não foi agendada, mas apenas adicionada ao sistema. Para iniciar a tarefa, é preciso executar a interface de operação apontando seu navegador para `http://localhost:4444`.

Em conexões pelo navegador, o Scheduler exibe uma interface semelhante à da **figura 3**. Para ver os detalhes da tarefa, dê um duplo clique na tarefa de becape na coluna à esquerda. Para executar a tarefa imediatamente, clique no botão *Job menu* e selecione *Start task now*.

Por ser muito fácil iniciar o script pela linha de comando, isso não é nada espetacular. É possível voltar ao editor de tarefas e clicar na entrada *Run Time* no painel esquerdo e selecionar uma hora para a execução da tarefa. Para isso, clique em *Everyday* (todos os dias) e defina um novo período clicando no botão *new Period*. Em *Start Time*, digite algo como `09:00` no campo *Single Start*. Depois, clique no botão *Save* e essa nova configuração será ativada – a tarefa terá início todos os dias às 9 horas.

Até agora, a única vantagem do programa sobre o Cron é uma interface amigável – mas isso é apenas o começo. Quando começamos a conhecer as cadeias de tarefas, vemos o poder do agendamento de tarefas.

Becape

Primeiro, suponha que você tenha criado uma segunda tarefa que faça um becape do banco de dados, que deve ser executada imediatamente após o fim do becape das configurações. Uma alternativa é criar um único script que faça primeiro o becape das configurações e imediatamente depois inicie o do banco de dados. Porém, cadeias de tarefas são úteis em várias situações mais complexas em que não é possível simplesmente lançar mão de um script shell, as quais serão discutidas mais adiante.

Assim como na primeira tarefa, crie um novo elemento no *Hot Folder*, mas selecione *Job Chains*. Digite o nome da cadeia (*Chain Name*) e, caso se deseje, também um título (*Title*). Como cada elemento de uma cadeia é chamado de nó (*Node*), é preciso adicionar um *New Chain Node* a seguir, clicando no botão respectivo. Caso o nome da tarefa seja conhecido, pode-se digitá-lo manualmente ou usar o botão *Browse* para procurá-la.

No campo *State* é possível definir um estado para essa etapa ou nó.

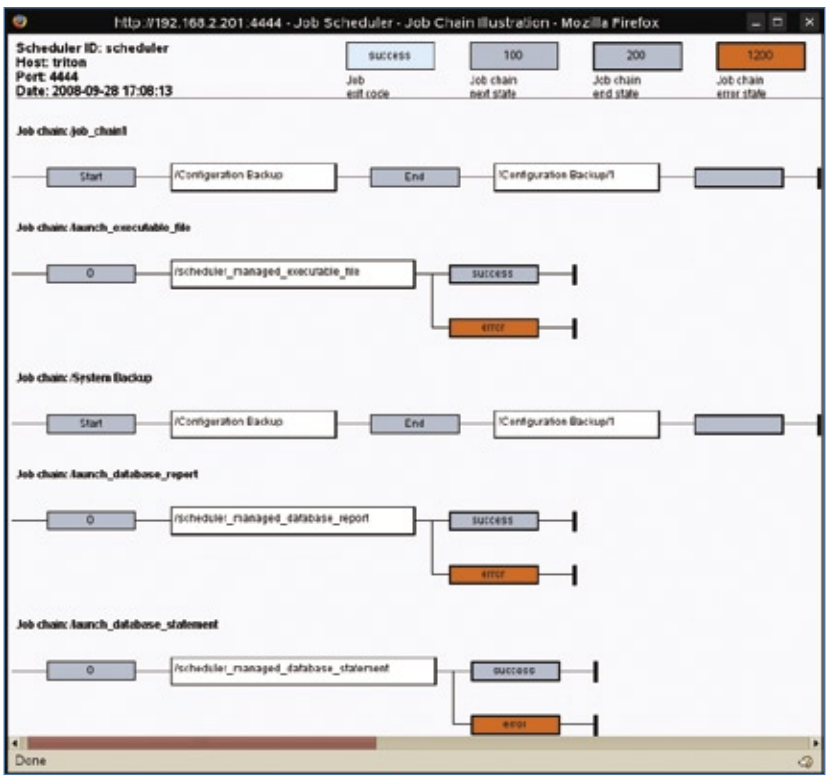


Figura 4 As dependências entre as tarefas podem ser exibidas com uso do *Job Chain Illustration*.

Definido estados, é possível criar um fluxo mais complexo para as tarefas. Por exemplo, pode-se criar um estado chamado *Erro* e, se alguma tarefa anterior apresentar um erro, pula-se imediatamente para a tarefa definida com esse estado, pulando todas as outras. Além disso, é possível executar diferentes tarefas de erro para cada uma das várias etapas.

Mais cadeias

Embora criar uma cadeia de tarefas que consista em apenas uma única tarefa possua certas vantagens, não pare nesse ponto. Como mencionado, é melhor uma tarefa de becape constituída por duas etapas, então vamos criar uma segunda cadeia com a tarefa de becape do banco de dados e configurá-la de forma semelhante à segunda tarefa. Em nosso exemplo, definimos o primeiro nó com o estado *Início* e o segundo com o estado *Fim*, embora isso não seja necessário.

Ao se clicar no botão *Save*, é mostrada a nova cadeia na aba *Job Chains* da interface de operação. Marcar a caixa *Show Jobs* exibe as tarefas individuais que compõem a cadeia. Um duplo clique na cadeia abre o painel de detalhes no lado direito, como ocorreu com a tarefa única.

Nesse ponto, a cadeia de tarefas ainda não será executada porque precisa de um pedido, que pode ser inserido manualmente no menu *Job | Add Order*. É mostrada uma nova janela que permite a definição de várias características do pedido, como ID, horário de início e até estado da cadeia. Neste exemplo, apenas deixe tudo em branco e o sistema criará sozinho uma ID de pedido.

Se não tiver sido definida uma condição, a cadeia inicia imediatamente; porém, pode ser definida uma fatia de tempo (*Time Slot*) para qualquer uma dessas tarefas, e o Scheduler esperaria a hora certa para iniciar a tarefa.

Note que as tarefas precisam ser capazes de aceitar pedidos para reagir a eles. Esta etapa é feita na janela de configuração para as tarefas individuais. Na janela *Main Options* há um botão *On Order* que precisa ser definido como *Yes*; caso contrário, o pedido não iniciará a tarefa.

Até aqui iniciamos tudo manualmente. Como precisamos definir um pedido para iniciar a cadeia de tarefas, obviamente é necessária uma forma de criar pedidos dinamicamente. Uma maneira seria criar um pedido numa hora específica, o que por sua vez aciona a cadeia de tarefas. Como se pode esperar, isso é feito pelo menu *New | Hot Folder Element | Order*. Após dar um nome ao pedido e selecionar a janela *Job Chains*, selecione a cadeia específica a ser associada a esse pedido. Note que um pedido só pode ser associado a uma única cadeia. Depois, defina um novo horário (*Time Period*) e um *Single Start* às 09:00. Para ativar imediatamente as alterações, é preciso armazená-la no diretório `config/live/`.

Ao retornar à interface de operação, pode-se ver que agora há um pedido associado à cadeia criada. Abaixo do pedido, uma entrada *next start* (próximo início) mostra a data e hora em que o pedido iniciará. Como já passou das 9:00 am neste exemplo, a data é amanhã. Se for usado outro horário de início, como o dia primeiro, o próximo início seria nessa data.

Controle

Para definir o período das tarefas, cadeias e pedidos, é possível estabelecer um horário para o início de uma tarefa, assim como um intervalo entre execuções (a cada 12 horas, por exemplo). Essa segunda opção não é útil no caso de cadeias em que as tarefas precisem seguir uma determinada ordem. Porém, é possível definir um pedido que seja iniciado diariamente às 7:00, que por sua vez inicie uma cadeia.

Há também definições de tempo como "segundo domingo de cada mês", "último dia do mês" ou "somente 8/janeiro e 16/fevereiro".

Horários e intervalos pré-estabelecidos são úteis, mas nem sempre é possível saber *a priori* quando uma tarefa precisará ser realizada. No caso daquelas que dependem da existência ou inexistência de algum arquivo, é possível definir *watch directories* (diretórios a ser observados), com regras que aceitam até expressões regulares (**figura 4**).

Pedido próprio

Depois de superar as dificuldades iniciais, nota-se que o Open Source Job Scheduler é um bom produto. Com intimidade, ele se torna fácil de configurar e administrar.

A SOS também presta um ótimo serviço. Identifiquei um bug e enviei um *patch* para um arquivo `.jar` que foi disponibilizado por eles no servidor em menos de um dia. Até em uma rede pequena o Open Source Job Scheduler oferece recursos muito úteis. Em instalações maiores, ele é quase indispensável. ■

Mais informações

[1] Open Source Job Scheduler: http://jobscheduler.sourceforge.net/

[2] Driver JDBC para MySQL: http://www.mysql.com/products/connector/

[3] Software- und Organisations-Service GmbH: http://www.sos-berlin.com/scheduler

TUTORIAL

Faça belos gráficos via navegador com a API do Google Chart

Gráficos via web

A API do Google Chart permite desenhar gráficos, planilhas, mapas e códigos de barras personalizados através de uma interface web simples.

por Martin Streicher

Se uma imagem vale mais que mil palavras, um gráfico deve ser algo semelhante a uma novela. Em apenas um piscar de olhos, um gráfico pode transmitir o estado do mercado de ações, a tendência de tráfego em um website, a distribuição dos eleitores por região, além de informar como a verba é distribuída em um orçamento familiar. Além disso, um gráfico é simplesmente mais compreensível do que uma enorme tabela cheia de números.

Porém, é estranho vermos que muito poucos sites utilizam gráficos em seu benefício. Isso acontece em grande parte porque a criação de gráficos requer um software especializado. Por exemplo, se o site é baseado em PHP, é preciso instalar o *pChart* [1], adicionar a biblioteca gráfica *GD* e escrever o código para produzir algum tipo de gráfico. Idealmente, qualquer um – um editor, escritor ou mesmo um usuário adicionando comentários – deve ser capaz de criar e embutir gráficos em suas páginas.

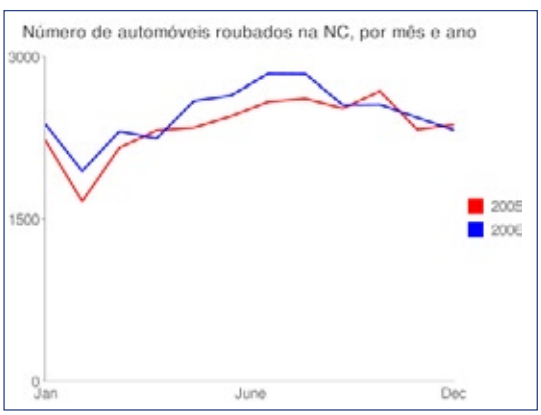


Figura 1 Um gráfico de linha simples produzido pela API do Google Chart.

Na verdade, o dinamismo, a simplicidade e a conveniência estão no cerne da interface de programação de aplicação (API) Google Chart [2], e talvez essa seja a descrição mais precisa para um Software como Serviço (SaaS). Simplesmente crie uma URL parametrizada como `http://chart.apis.google.com/chart?parâmetro1&parâmetro2&parâmetroN` e deixe o Google Chart fazer todo o trabalho pesado. O Google Chart permite que você renderize seis tipos de gráficos, um *Google-o-meter*, um *QR code* (espécie de código de barras) e mapas. Além disso, é possível usar praticamente um gugol de opções de personalização, tais como a barra de cores, a cor de fundo, a legenda e muito mais.

Este artigo ajuda nos primeiros passos no uso do Google Chart. Você aprenderá a desenhar gráficos e adicionar efeitos especiais para melhorar suas criações gráficas.

Elementos de gráficos

Para gerar um gráfico com o Google Chart, forneça o prefixo `http://chart.apis.google.com/chart?`, o tipo de gráfico (tal como torta ou de linhas), o tamanho do gráfico, seus dados e quaisquer parâmetros específicos, como as cores e os rótulos dos eixos, para adequá-lo ao resultado final.

Todas as opções do gráfico são associadas a pares de valores do tipo *chave=valor*. Algumas chaves são comuns para todos os gráficos, enquanto outras são exclusivas para um determinado tipo. Da mesma forma, a sintaxe para o valor especificado no par tende a variar de acordo com o tipo de gráfico.

O tamanho do gráfico é medido em pixels e especificado com o parâmetro `chs=`*LxA*, em que *L* é a largura e *A* é a altura. Por exemplo, `chs=200x100` gera um gráfico de 200 pixels de largura por 100 pixels de altura. A área de um mapa não pode exceder 440 pixels de largura por 220 de altura. Para todos os outros gráficos, nem a largura nem a altura podem exceder 1.000 pixels, e a área máxima é de 300.000 pixels quadrados.

O tipo de gráfico é escolhido com o par `cht=`*tipo*, em que *tipo* é uma das diversas constantes pré-definidas. Por exemplo, para desenhar um gráfico de linhas simples com pontos equidistantes do eixo *x*, especifique `cht=lc`. Para cada tipo de gráfico, pode-se consultar a constante apropriada na documentação do Google Chart.

Exemplo 1: Roubo de automóveis na Carolina do Norte

```
01  http://chart.apis.google.com/chart?
02  cht=lc&
03  chtt=Número de automóveis roubados
➥na NC, por mês e ano&
04  chs=400x300&
05  chd=t:2231,1658,2156,2318,2343,2450,
➥2583,2612,2522,2681,2326,2371|
06  2381,1939,2309,2242,2590,2642,2840,
➥2837,2555,2558,2437,2319&
07  chds=0,3000&
08  chco=FF0000,0000FF&
09  chdl=2005|2006&
10  chxt=x,y&
11  chxl=0:|Jan|June|Dec|1:|0|1500|30    00|&
12  chxp=0,0,50,100|1,0,50,100
```

Os dados de um gráfico podem ser fornecidos em vários formatos – a partir de uma lista de dados brutos simples até uma coleção de códigos alfanuméricos para mapear valores de uma escala pré-definida.

Normalmente, o conjunto de dados brutos é constituído por uma lista de valores separados por vírgulas, e um conjunto de dados codificados é uma seqüência contínua de caracteres alfanuméricos. Por exemplo, para fornecer dados como texto simples, utilize `chd=t:`*valores*, em que *valores* é uma lista de valores de ponto flutuante positivos entre 0 e 100 delimitados por vírgula. O caractere `_` (traço baixo) pode ser usado como um espaço reservado para a falta de um dado. Múltiplos conjuntos de dados são delimitados pelo caractere `|` (*pipe*, ou barra vertical).

Para demonstrar, abra um navegador e digite a URL `http://chart.apis.google.com/chart?cht=lc&chs=500x400&chd=t:7,3,9,2,0,7,9|15,15,18,11,0,16,12&chco=FF0000,00FF00` na barra de endereços. Como se pode adivinhar, o parâmetro `chco` lista os valores RGB para colorir cada grupo de dados.

A **figura 1** mostra o exemplo de um gráfico de linha incluindo seus elementos (eixos, títulos e legendas). A URL utilizada para gerar o gráfico é mostrada no **exemplo 1**. Cada URL mostrada nesse artigo abrange várias linhas de forma intencional, para melhor legibilidade.

De forma resumida, `chtt` fornece o título do gráfico. Os dados são fornecidos como valores brutos expressos em texto simples, mas como os valores são superiores a *100*, `chds` fornece um valor mínimo e um máximo para normalizar os dados para um percentual. Aqui, como os dois conjuntos de dados estão dentro do mesmo intervalo, bastam um valor mínimo e um máximo para ambos. No entanto, se cada um dos conjuntos de dados for traçado a partir de uma única série, é preciso fornecer um valor mínimo e máximo para cada conjunto. O parâmetro `chxt` é combinado com o `chxl` e com o `chxp` para criar e posicionar os rótulos dos eixos.

Acredite ou não, desenhar um gráfico é realmente simples. Para inserir um gráfico em um página web, use uma tag `img src` e defina seu atributo `src` para a URL do gráfico. Forneça uma descrição para o gráfico por meio do atributo `alt`.

Cartografia

Desenhar um mapa com o serviço Google Chart é tão simples quanto desenhar qualquer outro gráfico: primeiramente, especifique o mapeamento do gráfico, selecione uma região do mundo para desenhar e, em seguida, associe os dados a cada país, província ou estado encontrados no mapa. Os dados podem ser discretos – digamos, representar os estados azuis e vermelhos nos Estados Unidos – ou contínuos. Além disso, você pode associar uma cor com o mínimo e o máximo em um intervalo, e o Google Chart renderiza os valores intermediários em uma graduação de cores (degradê).

Por exemplo, o **exemplo 2** gera um mapa dos Estados Unidos, mostrando como os estados votaram na eleição presidencial de 2004. A **figura 2** apresenta os resultados.

No **exemplo 2**, `cht=t` seleciona o gráfico de mapa, `chtm=usa` especifica os Estados Unidos como região e `chs=440x220` desenha o maior mapa

Exemplo 2: Estados vermelhos e azuis

```
01 http://chart.apis.google.com/chart?
02 cht=t&
03 chtm=usa&
04 chs=440x220&
05 chco=FF0000,0000FF,0000FF&
06 chld=CACTDEDCHIILMEMDMAMIMNNHNJNY
➥ORPARIVTWAWI&
07 chd=s:AAAAAAAAAAAAAAAAAAA
```

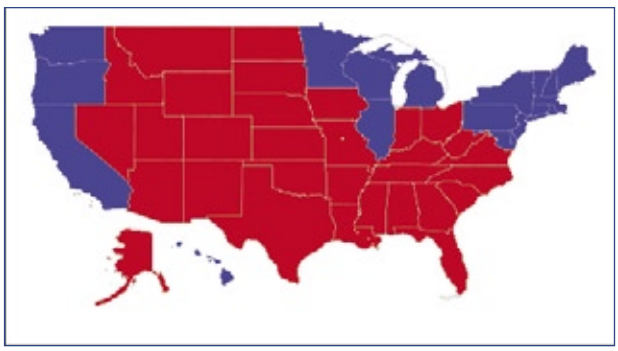


Figura 2 Divisão dos estados em vermelho (republicanos) e azuis (democratas) na eleição presidencial dos Estados Unidos em 2004.

Figura 3 O endereço do site da revista capturado num código QR.

possível. No gráfico de mapa, `chco=FF0000,0000FF,0000FF` define as cores padrão de cada estado (vermelho) e a cor de início e de final (ambas em azul) do gradiente.

O parâmetro `chld` contém o código de duas letras de cada um dos estados conquistados pelo candidato presidencial democrata. Finalmente, o parâmetro `chd=s:` seleciona o esquema de codificação simplificada de dados, em que todos os valores devem ser representados por um dos caracteres na seqüência de A-Z, *a-z* e *0-9*, sendo *A* o mínimo e *9* o máximo. Em outras palavras, o esquema de codificação simplificada fornece uma granularidade de 62 valores distintos. Tendo em conta que todos os estados são coloridos em vermelho por padrão, qualquer estado com outro valor – aqui, `A` – é colorido de azul.

Exemplo 3: Informações num código QR

```
01 http://chart.apis.google.
➥com/chart?
02 cht=qr&
03 chs=200x200&
04 choe=UTF-8&
05 chld=Q&
06 chl=http://www.
➥linuxnewmedia.com.br/lm/
```

Quadro 1: Dicas e truques do Google Chart

Essas dicas e truques tornarão seus gráficos mais legíveis:

- Certifique-se de que o tamanho de seu gráfico é suficiente para exibir o título, os rótulos e a legenda da imagem. Infelizmente, a determinação da largura mínima não tem uma forma algorítmica – pode ser preciso utilizar um pouco de tentativa e erro.
- Para alterar a cor e o tamanho do texto no título do gráfico, use `chts=color,fontsize`. Além disso, é possível alterar a cor e o tamanho da fonte de um eixo com o rótulo `chxs`. Infelizmente, não é possível especificar o tipo de fonte.
- Os quatro eixos são x, t, y e r, ou seja, a forma resumida para delimitar o eixo inferior x, o eixo superior x, o eixo à esquerda y e o eixo à direita y, respectivamente. Se você quiser vários rótulos para qualquer eixo, repita o nome do eixo no parâmetro `chxt` e especifique seus detalhes no `chxl`.
- Leia a documentação da API do Google Chart e dedique atenção especial à sintaxe de cada opção. Mesmo um erro de um caractere pode tornar um gráfico ilegível. Por exemplo, o parâmetro `chd` utiliza a barra vertical para separar cada conjunto de dados, diferentemente de `chds`. Infelizmente, essa não é a única inconsistência na API do Google Chart (o *clipping* do gráfico de barras é outro), portanto, mantenha o manual por perto.
- Antigamente, um gráfico de barras com valores negativos e positivos requeria truques para renderizar corretamente. Agora é possível usar o parâmetro `chp` e uma porcentagem para colocar a linha zero a partir de uma distância proporcional da origem sobre o eixo *y*. Os valores devem então ser interpolados para serem renderizados adequadamente. Por exemplo, suponha que o fluxo de caixa da empresa seja (em milhões) de -20, -5, 1, 3, 10. Para colocar a linha zero em `0.5`, ou na metade do caminho para cima do eixo *y*, valores menores que `50` serão desenhados "abaixo da linha" e todos os valores acima de `100` serão desenhados "acima da linha". Para normalizar os dados, adicione `50` a todos os valores e plote os novos valores.

```
http://chart.apis.google.com/chart?
cht=bvg&
chs=400x400&
chbh=40,5&
chd=t:30,45,51,53,60&
chp=.5&
chm=r,000000,0,.495,.5
```

- A **figura 5** mostra o gráfico final.
- O parâmetro `bvg` é a constante para o gráfico do tipo barra vertical, e o `chd` expressa o conjunto de dados normalizado. O parâmetro `chp` coloca a linha zero a meio caminho acima do eixo y, enquanto que o `chm` é uma opção para desenhar uma faixa de marcação no gráfico. Os seus parâmetros são (na ordem) `r` para um marcador horizontal; `000000` para desenhar o marcador em preto; `0`, que é ignorado; e `.495` e `.5` para expressar as margens inferior e superior da faixa de marcação em termos de proporção sobre o eixo-y. Isso porque a linha zero está colocada a `.0.5,.495` e `.5` desenha uma linha bem fina em zero.
- O parâmetro `chbh` especifica a largura de uma barra e o espaço entre cada uma barra. Diferentemente de outros tipos de gráficos, se `chbh` for grande demais e `chs` for muito pequeno, parte do gráfico será cortada. Certifique-se de ajustar o tamanho de um ou todos esses parâmetros quando estiver desenhando um gráfico de barras.

O Google Chart também oferece gráficos para África, Ásia, Europa, Oriente Médio, América do Sul e todo o globo.

Código de barras

No Japão moderno, jovens compartilham informações de uma forma digital verdadeiramente inovadora: eles trocam códigos de barras. E agora você também pode. O Google Chart fornece uma API para codificar até 4.296 caracteres em uma imagem bidimensional e monocromática chamado *QR code*, ou código QR.

Para começar, vamos codificar o email da **Linux Magazine** em um QR code. O **exemplo 3** mostra como a imagem na **figura 3** foi criada. Ao usar o gráfico QR, `choe` especifica a codificação do texto. O parâmetro `chld` dita o grau de correções de erros aplicado à imagem. O valor `Q` inclui informações duplicadas o suficiente a ponto de 25% da imagem poder ser destruída sem afetar a legibilidade. O parâmetro `chl` é o texto a ser codificado, geralmente fornecido como uma URL que é, então, interpretada por um aplicativo.

Se você tem um telefone celular, pode baixar gratuitamente o *BeeTagg* [3], tirar uma fotografia da **figura 3** e decodificar os resultados para entrar no site da revista.

Figura 4 Um vCard inteiro representado como código QR.

Como uma alternativa, o Google oferece gratuitamente uma biblioteca gratuita para leitura de códigos QR chamada *Zebra Crossing* [4][5] e um leitor de códigos de barras online experimental que interpreta as imagens recebidas.

Um código QR pode capturar até 4.296 caracteres. A **figura 4**, por exemplo, codifica um vCard (cartão de visitas) inteiro.

Como vai o coração?

A API do Google Chart é simples de usar e fácil de integrar em aplicações web.

Conforme mostrado, é possível usar a API imediatamente – basta inserir um link estático em sua página web e permitir que o navegador efetue a requisição e a renderização de um gráfico a cada vez que a página é desenhada.

Para acelerar a renderização da página, você pode solicitar e efetuar o cache da imagem do gráfico em seu próprio servidor, recriando o gráfico apenas quando os dados contidos nele forem alterados. Além de proporcionar melhor eficiência, essa técnica protege melhor os dados brutos. Um visitante do site não poderá "ver os fontes" e copiar a URL.

Naturalmente, também é possível misturar a API do Google Chart com técnicas AJAX para modificar os gráficos dinamicamente em resposta à requisição do usuário. O *Chart Maker* [6] é uma demonstração básica mas efetiva da dinâmica de gráficos; outros têm usado a API do Google Chart para implementar uma calculadora de empréstimos executiva.

Naturalmente, o Google Chart costuma ser mais lento que as ferramentas para geração de gráficos no desktop, como o *Apple Numbers* ou mesmo o *Microsoft Excel*. Estas utilizam mecanismos de renderização nativos e não requerem consultas à Internet para transmitir dados e baixar um grande gráfico na forma de uma imagem. No entanto, o Google Chart é um aplicativo gratuito que está disponível em qualquer lugar. Se você está realmente interessado em utilizar o Google Chart em ambiente de produção, o uso de cache pode melhorar o tempo de resposta. ■

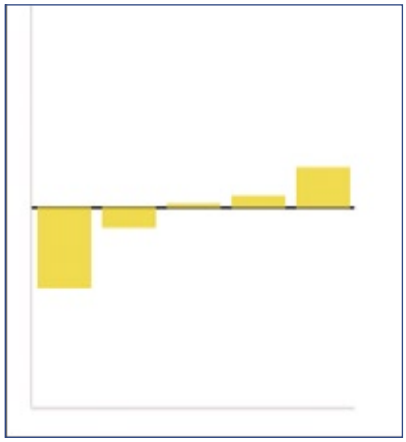


Figura 5 Renderização de valores positivos e negativos num gráfico de barras.

Mais informações

[1] pChart: http://pchart.sourceforge.net/

[2] Documentação do Google Chart: http://code.google.com/apis/chart/

[3] BeeTagg: http://www.beetagg.com/

[4] Zebra, biblioteca livre do Google para leitura de códigos de barra: http://code.google.com/p/zxing/

[5] Guia para codificação de dados em códigos QR: http://code.google.com/p/zxing/wiki/BarcodeContents

[6] Gerador simples para o Google Chart: http://almaer.com/chartmaker/

TUTORIAL

Alta disponibilidade em PostgreSQL

Banco cheio, mas disponível

O PostgreSQL não possui embutido um mecanismo para criação de clusters, mas essa tarefa é fácil com ferramentas externas. Conheça uma ótima estratégia.

por Fernando Ike

O tema alta disponibilidade, abordado na edição 43 da **Linux Magazine** [1], é abrangente e envolve várias áreas: desenvolvedores, administradores de sistemas, rede e banco de dados.

Geralmente, alta disponibilidade em bancos de dados é um objetivo mais complexo e crítico do que se costuma acreditar. Não é simplesmente pensar que uma solução como Oracle RAC garantirá disponibilidade de 100% do banco de dados. Para aumentar a disponibilidade, é necessário analisar uma série de variáveis, entre elas:

- Se o datacenter tem grupo gerador de energia elétrica;
- Se há conexão à Internet por mais de dois links;
- Servidores com fontes redundantes, discos etc.;
- Circuitos elétricos e rede redundantes;
- Se a aplicação suporta múltiplas instâncias de banco de dados;
- Se a aplicação suporta múltiplas instâncias dela mesma;
- Se a modelagem permite instâncias de banco de dados fisicamente distantes;
- Quanto se pode investir.

Tais variáveis dependem do projeto em questão, ou seja, variam de projeto para projeto. Em geral, a grande dificuldade para banco de dados é o sincronismo das bases de dados entre vários servidores, já que há a necessidade de garantir a consistência entre eles. Aplicações que usam banco de dados para operações somente leitura (como aplicações web, por exemplo) têm facilidade de trabalhar com vários servidores de banco de dados usando balanceamento de carga. Entretanto, o mesmo não acontece quando uma aplicação tem operações de leitura e escrita, pois não existe uma solução definitiva, uma vez que depende de como a aplicação foi projetada. Uma alternativa seria modelar a aplicação para acessar um servidor de banco de dados para operações de leitura/escrita e os outros servidores para operações de leitura.

Para *PostgreSQL*, essa tarefa é um pouco mais difícil – mas não impossível –, pois oficialmente existem poucas formas de aumentar sua disponibilidade sem que se use extensões ou aplicações de terceiros. Existe uma discussão [2] dentro do *PostgreSQL Global Development Group* para incorporar recursos de replicação *Master/Slave* na versão 8.4 (atualmente em desenvolvimento) e posteriores.

PostgreSQL hoje

Vejamos o que é possível fazer com o PostgreSQL sem ferramentas de terceiros.

Warm Standby usando PITR (*Point-In-Time Recovery*): um servidor primário envia para um ou mais servidores secundários os arquivos do WAL (*Write Ahead Log*), que contêm as modificações nas bases de dados do servidor primário. Tais arquivos, quando enviados, serão processados pelos servidores secundários. Esse método para o PostgreSQL não permite, por enquanto, que os servidores secundários sejam usados para leitura. Esses servidores não estarão disponíveis para nenhuma operação até que haja uma falha no servidor primário.

Em caso de falha no servidor primário, falhando a transmissão dos últimos arquivos do WAL para os servidores secundários, estes perderão as últimas alterações realizadas no servidor primário. Essa perda é pequena se comparada às estratégias de recuperação mais comuns para estes tipos de incidentes, as quais são: becape completo da última noite ou recuperação utilizando os arquivos do WAL. A comparação é de alguns segundos usando Warm Standby e de alguns minutos ou horas com recuperação de becape ou por arquivos do WAL.

Compartilhamento de disco: usando a mesma área num equipamento remoto (como storage), os servidores poderão ter a área montada nele, mas somente o servidor primário ou ativo poderá ter o serviço do PostgreSQL em execução. O servidor secundário só deve entrar em ação em caso de falha do primário; caso contrário, há o risco de corrompimento das bases de dados.

Neste método, numa eventual falha do servidor ativo, é praticamente nula a perda de dados, já que as bases de dados estão em um storage. Geralmente, usa-se NFS como forma de acesso ao storage. Uma recomendação importante ao usar NFS é montá-lo usando a opção `sync` (síncrono) desabilitar o cache e jamais usar a opção `async` (assíncrono), já que ela poderá corromper as bases de dados do PostgreSQL. O recomendável para esse método é o uso de SAN (iSCSI, AoE etc.) em vez de NAS (SMB, NFS, etc.), uma vez que a arquitetura SAN é projetada para situações de grande volumes de dados e menor tempo de recuperação em caso de incidente comparado com NAS.

Replicação por dispositivo de bloco: uma variação do compartilhamento de disco. Quando usado esse recurso, o dispositivo de bloco é a unidade de replicação. Assim como nos outros métodos, não pode haver dois servidores PostgreSQL em execução ao mesmo tempo. O DRBD é um software muito popular para essa finalidade.

Terceiros

Existe a possibilidade de se usar extensões ou aplicações de terceiros para aumentar a disponibilidade do PostgreSQL, em tarefas como replicação mestre-escravo, *middleware* de replicação orientado a sentença e replicação *multimaster* assíncrona ou síncrona.

Replicação mestre-escravo: esse método envia todas as consultas de modificações das bases de dados para o servidor mestre. Este envia as modificações que nele ocorreram para o servidor escravo. Essas modificações ocorrem por lote e de forma assíncrona, permitindo que se tenha múltiplos servidores escravos. O servidor escravo pode responder somente consultas de leitura, as quais são ideais para consultas do tipo *data warehouse*. O *Slony-I* é um exemplo desse tipo de replicação, com granularidade de tabela e suporte a múltiplos servidores escravos. Em caso de falha no servidor mestre, poderá haver perda de dados que ainda não foram replicados para o servidor secundário.

Middleware de replicação orientado a sentença: programa que intercepta cada consulta SQL e a envia para um ou todos os servidores. Cada servidor opera independentemente. Consultas de leitura e escrita são enviadas para todos os servidores, enquanto as consultas somente-leitura podem ser enviadas para qualquer um dos servidores, permitindo que o trabalho de leitura seja distribuído.

Se as consultas forem simplesmente transmitidas sem modificações, alguns valores específicos de cada servidor (como a função `random()` e os valores de `TIMESTAMP`) terão valores diferentes nos servidores. Isso ocorre porque cada servidor opera de forma independente e porque as consultas SQL são realizadas em *broadcast* (e não atuando na modificação das colunas). Se isso for inaceitável, o middleware ou aplicação deve consultar tais valores a partir de um servidor e depois usá-los para escrever as consultas. Exemplos desse tipo de replicação são o *pgpool-II* e *Sequoia*.

Replicação Multimaster Assíncrona: para os servidores que não estão regularmente ligados, como laptops e servidores remotos, manter os dados consistentes entre os servidores é um desafio. Usando replicação assíncrona multimaster, cada servidor trabalha com independência e periodicamente se comunica com os outros servidores a fim de identificar transações conflitantes. Os conflitos podem ser resolvidos pelos usuários

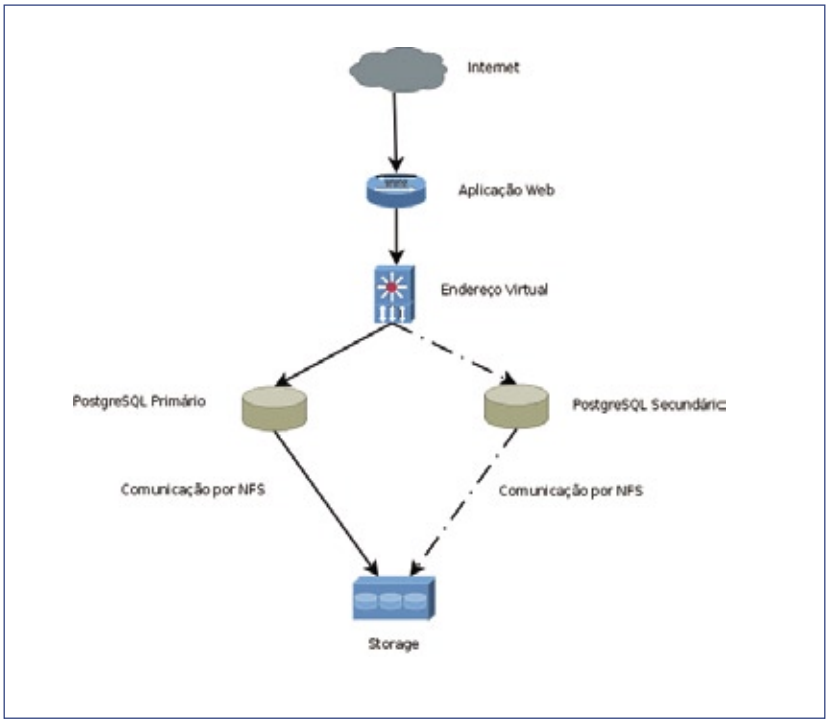


Figura 1 Solução de alta disponibilidade do banco de dados proposta.

ou por meio de regras. *Bucardo* é um exemplo desse tipo de replicação.

Replicação multimaster síncrona: em replicação multimaster síncrona, cada servidor pode aceitar conexões com transações de escrita (como `INSERT`, `UPDATE` e `DELETE`). Tais transações são transmitidas a partir do servidor de origem para todos os outros servidores antes de efetivar a transação. Em situações com muitas transações, isso poderá causar bloqueio dos registros, degradando consideravelmente a performance. Neste tipo de replicação, as transações com escrita geralmente são mais lentas do que as feitas em um servidor único. Além de dividir a carga de transações para leitura e escrita como na replicação mestre-escravo, a replicação multimaster síncrona é muito usada para balanceamento de carga, em alguns casos podendo haver problemas de consistência ao se usar funções como `random()`.

Solução simples

Uma solução muito comum e barata para alta disponibilidade em PostgreSQL é o uso de um dispositivo de storage comunicando-se com os servidores PostgreSQL via NFS (**figura 1**). A solução consiste em dois servidores, PostgreSQL e Heartbeat. Um deles será o primário e o outro o secundário. O secundário aguardará algum problema com o servidor primário e, caso ocorra, iniciará o serviço do PostgreSQL, assumindo o endereço de rede (VIP) usado para comunicação com a aplicação.

Essa solução não foi planejada para que o servidor primário assuma o controle novamente do ambiente caso retorne a operar, pois é recomendável verificar a razão do incidente, corrigir e retornar a operação ao ambiente num período de pouco uso do banco de dados.

Há alguns pontos importantes nessa solução. Sempre que ocorrer uma atualização de segurança no PostgreSQL, é recomendável aplicá-la a todos os servidores, pois não se deve executar uma versão diferente do binário em cada máquina. Além disso, nesse tipo de solução de alta disponibilidade não é possível haver dois servidores com o serviço PostgreSQL em execução. A disponibilidade é garantida pelo armazenamento dos dados no storage, sem necessidade de mecanismos de replicação de dados externos. Por último, políticas de backup devem continuar sendo usadas sem alterações. Caso aconteça algum incidente que indisponibilize os dados, haverá formas de recuperá-los.

Exemplo 1: Arquivo tuning.sh

```
01 #!/bin/bash
02
03 echo “2” > /proc/sys/vm/overcommit_memory
04
05 #kernel.shmmax = 4471775999
06 #25% do total da RAM
07 echo “17179869184” > /proc/sys/kernel/shmmax
08 ###kernel.shmmax = 4294967296
09 echo “17179869184” > /proc/sys/kernel/shmall
10 echo “300 32500 150 160” > /proc/sys/kernel/sem
11 echo “65536” > /proc/sys/fs/file-max
12 echo “deadline” > /sys/block/sda/queue/scheduler
13 echo “16777216” > /proc/sys/net/core/rmem_default
14 echo “16777216” > /proc/sys/net/core/wmem_default
15 echo “16777216” > /proc/sys/net/core/rmem_max
16 echo “16777216” > /proc/sys/net/core/wmem_max
```

Implementação

O procedimento de instalação será dividido por servidores: a primeira parte consiste na instalação do servidor primário, e a segunda parte trata do servidor secundário, considerando que um ponto de montagem foi disponibilizado previamente em ambos os servidores em `/var/lib/postgresql/storage`.

Depois de instalar o pacote do PostgreSQL 8.3 (versão estável mais recente) do Debian 5.0 (*Lenny*), o diretório padrão da instalação do cluster de base de dados[3] é o local em que está uma instância do PostgreSQL com seu catálogo de sistema. Esse diretório será movido para o storage usando uma partição NFS montada no servidor, o que exige uma parada no serviço do PostgreSQL.

Parado o serviço do PostgreSQL, mova o diretório com o cluster de base de dados armazenado localmente para o diretório NFS remoto. Depois disso, é necessário ainda criar um link simbólico para que o serviço inicie corretamente:

```
# mv /var/lib/postgresql/8.3 /var/
➥lib/postgresql/storage/
# ln -s /var/lib/postgresql/
➥storage/8.3 /var/lib/
➥postgresql/8.3
```

Feito isso, reinicie o PostgreSQL e crie um arquivo com ajustes de performance do PostgreSQL chamado `tuning.sh` em `/usr/local/sbin/` (**exemplo 1**). Esse arquivo conterá ajustes de parâmetros do kernel Linux para o PostgreSQL aproveitar melhor os recursos de hardware. Seria possível usar o arquivo `/etc/sysctl.conf`, mas ele não oferece

Exemplo 2: Arquivo postgresql.conf

```
data_directory = '/var/lib/postgresql/8.3/main'  # usar dados em outro diretório
hba_file = '/etc/postgresql/8.3/main/pg_hba.conf'  # arquivo de autenticação por máquina
➥(host-based authentication)
ident_file = '/etc/postgresql/8.3/main/pg_ident.conf'  # arquivo de configuração de ident
external_pid_file = '/var/run/postgresql/8.3-main.pid'  # gravar um arquivo extra com o PID
listen_addresses = '*'  # IP(s) para escutar
port = 5432  # porta (necessário reiniciar)
max_connections = 1000  # (necessário reiniciar)
unix_socket_directory = '/var/run/postgresql'  # (necessário reiniciar)
ssl = false  # (necessário reiniciar)
shared_buffers = 12GB  # mínimo=128 kB, máximo=max_connections*16kB
max_fsm_pages = 204800  # mínimo=max_fsm_relations*16, 6 bytes cada
fsync = on  # (des)ativa sincronização forçada
wal_sync_method = open_sync  # o padrão é a primeira opção
full_page_writes = on  # recuperar-se de gravações de página parciais
wal_writer_delay = 500ms  # 1-10000 milissegundos
commit_delay = 100  # 0-100000, em microssegundos
checkpoint_segments = 128  # em segmentos de logfile, mínimo=1, 16MB cada
checkpoint_timeout = 30min  # 30s-1h
checkpoint_completion_target = 0.7  # duração do alvo do checkpoint, 0.0 - 1.0
effective_cache_size = 48GB
datestyle = 'iso, dmy'
lc_messages = 'pt_BR.UTF-8'  # locale para mensagens de erro do sistema
lc_monetary = 'pt_BR.UTF-8'  # locale para formatação monetária
lc_numeric = 'pt_BR.UTF-8'  # locale para formatação numérica
lc_time = 'pt_BR.UTF-8'  # locale para formatação de tempo
default_text_search_config = 'pg_catalog.portuguese'
```

a possibilidade de alterar também o sistema de arquivos *sysfs*.

Entre os parâmetros a serem modificados, `shmmax` geralmente deverá ser de 25 a 50% do total da memória RAM, dependendo do tipo de aplicação e modelagem de dados. Nesse caso, usamos usamos 50% (16 GB) (**linha 7**).

Torne o script executável e crie um link simbólico para que ele seja carregado na inicialização:

```
# chmod 0755 /usr/local/sbin/
➥tuning.sh
# ln -s /usr/loca/sbin/tuning.sh /
➥etc/rcS.d/S99tuning.sh
```

Em seguida, execute-o para efetivar as alterações dos parâmetros do sistema operacional.

Ajuste do PostgreSQL

Com o sistema operacional pronto, é hora de ajustar o banco de dados. Para isso, comece editando o arquivo `postgresql.conf` de acordo com as determinações:

- `listen_adresses`: um asterisco permite que o PostgreSQL escute conexões vindas de qualquer rede. Ainda é necessário alterar o arquivo `pg_hba.conf` para que essa alteração tenha efeito.
- `max_connections`: número total de conexão simultâneas aceitas pelo PostgreSQL.
- `shared_buffers`: 20 a 25% do total da memória RAM.
- `wal_write_delay`: 500 milissegundos.
- `commit_delay`: 100.
- `checkpoint_segments`: 128.
- `checkpoint_timeout`: 30 min.
- `checkpoint_completion_target`: 0.7.

Exemplo 3: Arquivo pg_hba.conf

```
local   all         postgres                          md5
local   all         all                               md5
host    all         all         127.0.0.1/32          md5
host    all         all                 ::1/128       md5
host    intportal   portal  192.168.10.30/32          md5
```

- `effective_cache_size`: 75% da memória RAM.

Porém, tenha em mente que, conforme a base de dados cresce, esses e outros parâmetros do arquivo de configuração precisarão ser alterados.

O **exemplo 2** mostra o conteúdo do arquivo `postgresql.conf` após sua edição.

No arquivo `pg_hba.conf`, altere as políticas de acesso conforme a política da instituição, ativando ou desativando a criptografia, definindo quais redes podem acessar o banco etc. No **exemplo 3**, o arquivo permite que o usuário *portal* acesse a base de dados *intportal* com o endereço de rede 192.168.10.30/32 usando criptografia MD5.

Para efetivar as alterações, reinicie o PostgreSQL.

Exemplo 4: Arquivo ha.cf

```
logfacility daemon
logfile /var/log/ha.log
node pgprimario pgsecundario
keepalive 2
deadtime 10
bcast eth1
ping 192.168.10.5
auto_failback off
respawn hacluster /usr/lib/heartbeat/ipfail
```

Exemplo 5: Script PostgreSQL do heartbeat

```
01 #!/bin/bash
02
03 unset LC_ALL; export LC_ALL
04 unset LANGUAGE; export LANGUAGE
05
06 case $1 in
07   start)
08 /etc/init.d/postgresql-8.3 start
09 sleep 2
10 check_pgsql.sh &
11 exit 0
12 ;;
13
14   stop)
15 /etc/init.d/postgresql-8.3 stop
16 kill $(ps a|grep check_pgsql|awk '{ print
$1 }'|head -n 1)
17 exit 0
18 ;;
19   *)
20
21 esac
```

Heartbeat

O *hearbeat* é tido por muitos como sinônimo de alta disponibilidade, mas é apenas um meio para esse fim e a solução para alta disponibilidade de bancos de dados PostgreSQL proposta neste artigo o utiliza.

Após instalar o pacote do heartbeat na distribuição usada no servidor, adicione ao arquivo `/etc/hosts` os nomes e IPs dos servidores primário e secundário. No exemplo deste artigo, esses valores são:

```
192.168.10.10
➥pgprimario
192.168.10.11
➥pgsecundario
```

O arquivo de configuração do heartbeat pode se localizar em `/etc/ha.d/` ou em `/etc/heartbeat/`. O **exemplo 4** mostra o conteúdo do arquivo `ha.cf` que deve residir no diretório usado pela distribuição em questão, cujas opções têm os seguintes efeitos:

- `logfacility`: executar o heartbeat como serviço;
- `logfile`: local onde será gravado o registro de atividades do heartbeat;
- `keepalive`: intervalo de tempo de comunicação entre os nós;
- `deadtime`: intervalo de tempo para que heartbeat reconheça um nó como morto;
- `bcast`: forma de comunicação entre os servidores hearbeat, neste caso com uma placa exclusiva para comunicação (eth1);
- `ping`: checa se o IP virtual está no ar;
- `auto_failback`: caso o servidor primário saia do ar, quando voltar ele não tentará assumir como servidor principal no cluster;
- `respawn hacluster /usr/lib/heartbeat/ipfail`: serviço do heartbeat para trocar o IP Virtual em caso de falha no nó principal.

Ainda no diretório de configuração do heartbeat, crie o arquivo `haresources`. É nesse arquivo que o heartbeat procurará os serviços que precisam ser executados no cluster. Tais serviços são scripts que podem ou não ter parâmetros e estão localizados em `/etc/ha.d/resource.d/`. Acrescente ao arquivo `haresources` o seguinte conteúdo:

```
pgprimario IPaddr::192.168.10.5
pgprimario PostgreSQL
```

O parâmetro `IPaddr` adiciona o endereço de rede virtual (VIP) ao cluster, e `PostgreSQL` controla o PostgreSQL no heartbeat. Esse script não é distribuído oficialmente, e pode ser personalizado conforme a necessidade do ambiente.

Crie também o arquivo `authkeys` para abrigar a senha (criptografada com SHA1) necessária à comunica-

ção entre os nós do heartbeat. Para criar a senha, use algo como:

```
# echo "suasenha" | sha1sum
2fcaa24bc2673abbfb3d5ddcadccb7be2c
➥28fa53  -
```

Adicione esse hash ao arquivo `authkeys` da seguinte forma:

```
auth 1
1 sha1 2fcaa24bc2673abbfb3d5ddcadc
➥cb7be2c28fa53
```

Em seguida, altere as permissões do arquivo para *600* para que somente o usuário root possa ler e escrever nele.

No diretório `/etc/ha.d/resource.d/` ficam os scripts de interação dos serviços do heartbeat. Crie nele o script `PostgreSQL` referenciado no arquivo `haresources` que criamos antes, com o conteúdo mostrado no **exemplo 5**. Esse arquivo também precisará ter suas permissões alteradas, mas dessa vez para permitir que ele seja executado. Portanto, recomenda-se usar 755 como permissões.

Crie também um script (`/usr/local/sbin/check_pgsql.sh`) para verificar se o PostgreSQL continua no ar, de acordo com o **exemplo 6**. Esses são os significados das variáveis:

- `HOST`: endereço de rede do servidor;
- `USER`: usuário do PostgreSQL;
- `DB`: banco de dados a ser usado;
- `TEST`: tipo de consulta que servirá como teste;
- `REPEAT`: número de repetições do teste até considerar o servidor como inativo;
- `OTHER`: endereço de rede do servidor secundário.

Após tornar esse script executável, é necessário novamente reiniciar o PostgreSQL e o próprio heartbeat. Com isso, fica concluída a configuração do servidor PostgreSQL primário.

Servidor secundário

Para o servidor secundário, serão repetidos os mesmos passos da instalação e configuração do servidor primário, porém com certas diferenças.

Depois de instalar o pacote do PostgreSQL 8.3, pare o serviço deste e apague o diretório `/var/lib/postgre-`

Exemplo 6: Script check_pgsql.sh no servidor primário

```
01 #!/bin/bash
02
03 unset LC_ALL; export LC_ALL
04 unset LANGUAGE; export LANGUAGE
05
06 PSQL=$(which psql)
07 HOST=192.168.10.10
08 USER="postgres"
09 DB="postgres"
10 TEST="SELECT 1;"
11 REPEAT="5"
12 COUNTER="1"
13 OTHER=192.168.10.11
14
15 check()
16 {
17 while true;
18 $PSQL -U $USER -h $OTHER -c "$TEST" -d $DB 2>&1 > /dev/null
19 if [ $? -eq 0  ]
20 then
21    break
22 do
23 sleep 2
24
25     if [ $COUNTER -eq $REPEAT  ]
26     then
27           /etc/init.d/postgresql-8.3 stop
28           /etc/init.d/heartbeat stop
29     else
30           $PSQL -U $USER -h $HOST -c "$TEST" -d $DB 2>&1 >
➥/dev/null
31         if [ $? -eq 0  ]
32         then
33                 COUNTER="1"
34         else
35                 let  COUNTER=$COUNTER+1
36         fi
37     fi
38
39 done
40 fi
41 }
42
43 check
```

sql/8.3, pois ele usará, quando ativo, o mesmo cluster de base de dados do servidor primário que está armazenado no storage. Esse passo é o primeiro em que os procedimentos dos dois servidores diferem.

Exemplo 7: Script check_pgsql.sh no servidor secundário

```
01 #!/bin/bash
02
03 unset LC_ALL; export LC_ALL
04 unset LANGUAGE; export LANGUAGE
05
06 PSQL=$(which psql)
07 HOST=192.168.10.11
08 USER="postgres"
09 DB="postgres"
10 TEST="SELECT 1;"
11 REPEAT="5"
12 COUNTER="1"
13 OTHER=192.168.10.10
14
15
16 check()
17 {
18 while true;
19 $PSQL -U $USER -h $OTHER -c "$TEST" -d $DB 2>&1 &gt; /dev/null
20 if [ $? -eq 0  ]
21 then
22    break
23 do
24 sleep 2
25
26     if [ $COUNTER -eq $REPEAT  ]
27     then
28           /etc/init.d/postgresql-8.3 stop
29           /etc/init.d/heartbeat stop
30     else
31           $PSQL -U $USER -h $HOST -c "$TEST" -d $DB 2>&1 &gt; /dev/null
32         if [ $? -eq 0  ]
33         then
34                 COUNTER="1"
35         else
36                 let  COUNTER=$COUNTER+1
37         fi
38     fi
39
40 done
41 fi
42 }
43
44 check
```

Com o diretório apagado, é necessário criar um link simbólico para que o serviço inicie corretamente quando for solicitado pelo heartbeat:

```
# ln -s /var/lib/
➥postgresql/storage/8.3 /
➥var/lib/postgresql/8.3
```

Assim como no servidor primário, crie um arquivo tuning.sh com ajustes de performance para o PostgreSQL em /usr/local/sbin/. Como os servidores têm hardwares semelhantes, usaremos os mesmos ajustes de performance (**exemplo 1**). Após salvar o script, crie um link simbólico para que ele seja carregado ao iniciar os serviços do servidor:

```
ln -s /usr/local/sbin/
➥tuning.sh /etc/rcS.d/
➥S99tuning.sh
```

Execute o script recém-criado para efetivar as modificações dos parâmetros do sistema operacional.

Diferentemente do servidor primário, não serão necessárias alterações aos arquivos postgresql.conf e pg_hba.conf, pois os arquivos usados serão os mesmos.

Assim como no servidor primário, instale o heartbeat e acrescente as seguintes linhas ao arquivo /etc/hosts:

```
192.168.10.11 pgprimario
192.168.10.10 pgsecundario
```

Note que os IPs são invertidos com relação ao conteúdo do arquivo no servidor primário.

Em seguida, crie o arquivo de configuração /etc/ha.d/

ha.cf de acordo com o **exemplo 4** e /etc/ha.d/haresources com conteúdo igual ao do servidor primário:

```
pgprimario IPaddr::192.168.10.5
pgprimario PostgreSQL
```

Todos os procedimentos com o arquivo /etc/ha.d/authkeys também devem ser repetidos, assim como os do script /etc/ha.d/resource.d/PostgreSQL (**exemplo 5**). O script diferente entre os servidores primário e secundário é o check_pgsql.sh, em /usr/local/sbin/ (**exemplo 7**), pois os valores das variáveis HOST e OTHER devem ter seus valores trocados entre si.

Ao final, no entanto, o mesmo procedimento do servidor primário é necessário: permitir a execução dos scripts criados e reiniciar o PostgreSQL e o heartbeat.

Considerações

As atualizações de segurança deverão ser realizadas em ambos os servidores, com diferentes procedimentos para cada. No servidor que estiver ativo no cluster deve-se atualizar conforme a liberação de novas versões do pacote do PostgreSQL e os procedimentos de atualização da distribuição em uso. É recomendável para ambos os servidores fazer a atualização em um horário de pouco uso ou numa parada programada para manutenção.

As atualizações de segurança no servidor secundário precisam de atenção, pois distribuições baseadas em Debian reiniciam o serviço do PostgreSQL. Nesse caso, esse reinício pode afetar o funcionamento do servidor primário. Para contornar esse problema, podemos alterar a permissão do arquivo /etc/init.d/postgresql-8.3 antes de atualizar o pacote do PostgreSQL:

```
# chmod 000 /etc/init.d/
➥postgresql-8.3
```

Quadro 1: Problemas no storage

Em caso de problemas no *storage*, o melhor é recriar o cluster de banco de dados com o comando initdb e restaurar seu conteúdo a partir do becape. Dependendo do incidente, pode-se optar por criar o cluster localmente ou em outro storage. Caso seja local, é possível criar um cluster provisório até que o storage volte a ficar disponível para o servidor.

O comando para isso é:

```
# pg_createcluster -u postgres -d /var/lib/postgresql/provisorio
➥ --start-conf=auto 8.3 provisorio
```

e suas opções são:

- -u: usuário que será usado pelo cluster;
- -d: diretório onde ficará o cluster;
- --start-conf=: opção para acrescentar a /etc/init.d/postgresq-8.3 o início do cluster que está sendo acrescentado;
- 8.3: versão instalada do PostgreSQL;
- provisorio: identificação do novo cluster.

Depois de atualizar o pacote, basta retornar o pacote às permissões anteriores (e corretas para a operação):

```
# chmod 755 /etc/init.d/
➥postgresql-8.3
```

O **quadro 1** oferece ajuda caso ocorra algum problema com o storage durante a operação do cluster.

Conclusão

Uma solução de alta disponibilidade como essa não elimina a necessidade de uma política de becape e procedimentos de melhora contínua de performance. O becape pode ser restaurado a partir de qualquer máquina na solução de alta disponibilidade, desde que elas estejam com o serviço do PostgreSQL em execução. Novos procedimentos de becape podem ser adotados, como armazenamento dos logs diários como complemento da política existente.

O aumento da disponibilidade do banco de dados não significa abandonar as políticas de contingência e becape. Também é necessário planejar o aumento da disponibilidade de todo o ambiente (aplicação e banco de dados). Não desconsidere o uso de storages com iSCSI ou fibra ótica para melhor performance. ■

Mais informações

[1] Linux Magazine 43: http://lnm.com.br/issue/lm_43_alta_disponibilidade

[2] Discussão no PGDG sobre replicação: http://archives.postgresql.org/pgsql-hackers/2008-05/msg00913.php

[3] Criação de clusters PostgreSQL: http://www.postgresql.org/docs/8.3/interactive/creating-cluster.html

Integração de dados com o ETL Talend

O talento do Talend

Quem procura uma solução ETL para Business Intelligence não deve deixar de conferir o Talend. Conectado a diversas fontes de dados, ele só não faz chover – ainda.

por Miguel Koren O'Brien de Lacy

Um dos componentes essenciais de uma solução para a inteligência de negócios (BI – *Business Intelligence*) é o módulo de integração de informações de diversas fontes de dados. Felizmente o mercado de Software Livre e de código aberto oferece algumas soluções bastante completas que são usadas dentro dos pacotes de BI ou em modo stand alone. As soluções de integração de dados são conhecidas como ETL (*Extract*, *Transform*, *Load*), pois a missão dessas soluções é integrar informações e prepará-las para a formação de tabelas no *data mart*. Normalmente os dados precisam ser manipulados depois de obtidos e logo inseridos nas tabelas dos bancos de dados em que reside o data mart. Ou seja, estamos falando em obter os dados, aplicar regras de negócios da empresa, facilitar as consultas posteriores ou validar a qualidade dos dados e entregá-los transformados ao destino final. Dentre as transformações normalmente aplicadas aos dados, podemos destacar a seleção de campos importantes para a análise, a filtragem dos registros necessários, a limpeza dos dados ("Sr." ou "Senhor" passam a valer "S"), a geração dos campos calculados (por exemplo, "valor nf = quantidade * valor unitário") etc. Mas essas soluções também podem ser consideradas integradores e manipuladores de dados para outras necessidades, podendo substituir muitos sistemas de "interfaces" de dados que são desenvolvidos pelas áreas de TI de grandes empresas.

Originalmente, os sistemas corporativos foram desenvolvidos de forma isolada para cumprir alguma função específica, não sendo parte do objetivo de projeto a necessidade de compartilhar dados. Quando a quantidade desses sistemas começou a ser mais importante dentro das empresas, surgiram as primeiras necessidades de integração de dados, como a carga de pedidos aos sistemas de estoque e faturamento. Tais necessidades de integração foram implementadas diretamente por programas ou scripts específicos. Com a crescente complexidade das integrações requeridas, iniciou-se um encarecimento do desenvolvimento desses processos. Os sistemas tinham manutenção complexa e as lógicas de integração difíceis de documentar, auditar e entender. Por isso, as empresas começaram a implementar ferramentas prontas ou semi-prontas para essa necessidade. Essa foi a origem dos sistemas ETL.

Esses sistemas, porém, não possuem a popularidade que merecem em razão de certos fatores que impedem sua adoção. Entre estes fatores devemos destacar:

- Custo inicial;
- Complexidade no uso com curva de aprendizado muito empinada;
- Escalabilidade a necessidades de integrações pequenas.

A empresa Talend é fabricante do Talend Open Studio [1], apresentado como "o sistema ETL mais abrangente no mercado de software livre e código aberto". O modelo de negócios da empresa é um dos clássicos para Software Livre. A empresa desenvolve um produto que licencia sem custo, usando licenciamento em modalidade livre, no caso a GPL [2], e oferece serviços e suporte comerciais. O software licenciado sob a GPL não possui todos os componentes que são oferecidos a clientes sob o licenciamento de subscrição do serviço, mas mesmo dessa forma é extremamente útil para as necessidades ETL de qualquer empresa. O *Talend Open Studio* foi liberado no mercado em 2005 pela empresa Talend, com bases na França, país com uma política oficial de apoio a Software Livre e Código Aberto. Analistas de TI como Forrester Research [3], IDC [4] e Bloor Research [5] posicionam o Talend como o melhor sistema para necessidades de integração de dados. O sistema BI em software livre *SpagoBI* [6][7] é um exemplo de uso do Talend como seu componente ETL padronizado.

O modelo de Software Livre é bem apropriado para esse tipo de solução, pois faz bom uso de desen-

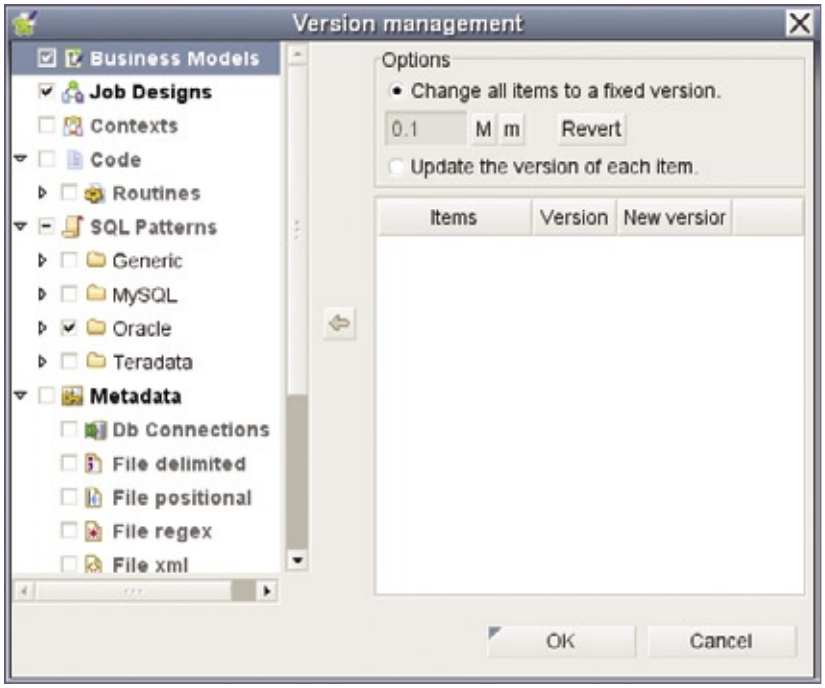


Figura 1 Gerenciamento de versões.

volvimento colaborativo, em que muitas pessoas contribuem com módulos para conexões a fontes de dados variadas. Mas o sucesso do Talend também mostra que o Software Livre não é apenas bem sucedido em soluções "comoditizadas", como sistemas operacionais e utilitários de infra-estrutura. O Talend mostra que uma solução livre pode ser muito atrativa num mercado novo em formação, competindo com sistemas proprietários de grandes empresas como IBM, SAS e SAP, as quais têm preços de licenciamento de nível corporativo. Empresas como Oracle e Microsoft também competem nesse mercado, porém com uma visão mais restrita, focada nos produtos de base de cada uma: banco de dados Oracle e *SQL Server*, respectivamente.

Um forte apelo do Talend é a disponibilidade de uma ferramenta abrangente em que os próprios usuários da informação podem modelar as regras de negócios (fontes de dados, campos requeridos, regras de transformação etc.) para a integração dos dados. Hoje a área de TI de qualquer empresa tem diariamente mais e mais dados, e os usuários têm necessidades de visualização que são mais urgentes a cada dia. Assim, é muito útil que os próprios usuários possam usar o sistema de forma não técnica para especificar as regras de integração.

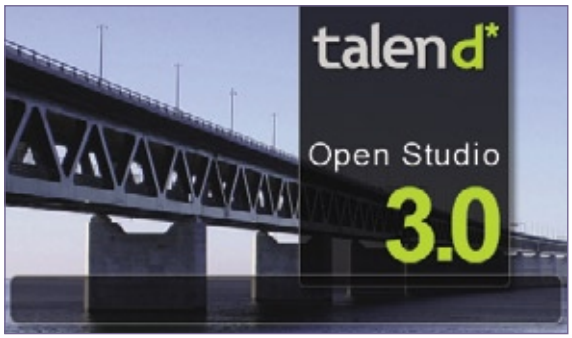


Figura 2 Tela de início do Talend.

Recurso e Tecnologia

O Talend é um sistema desenvolvido em Java que usa uma arquitetura modular formada por:

- Gerenciador gráfico de negócios (visão não técnica de necessidades de fluxo de dados);
- Gerenciador gráfico de processos ETL;
- Gerenciador de metadados (repositório para reutilização de objetos);
- Repositório de processos (módulo adicional da versão comercial);
- Interface web services a processos ETL;
- Monitor de processos;
- Componentes modulares (atualmente mais de 400). Usando a API do sistema podem ser desenvolvidos componentes personalizados.

O gerenciador gráfico de processos ETL roda dentro do ambiente *Eclipse* [8][9], seguindo a filosofia de integração de ferramentas dentro desse ambiente para desenvolvimento.

Normalmente os primeiros três módulos são usados na ordem listada. O gerenciador de negócios é usado pelos usuários do sistema, enquanto o gerenciador de processos ETL e o gerenciador de metadados são usados pelos programadores. Mesmo que o repositório de projetos ETL com apoio a equipes de trabalho seja um componente oferecido comercialmente, o Talend Open Studio inclui a possibilidade de versionamento do desenvolvimento dos processos. A **figura 1** mostra o uso desse recurso.

O Talend é um sistema "gerador de código", em oposição a um sistema de "caixa preta" – a qual é responsável pela execução dos processos ETL –, ou seja, o Talend não requer um servidor de execução de processos ETL. A vantagem da geração de código é que é mais simples integrar os processos ETL dentro de outros aplicativos e os modelos são de portabilidade muito mais flexível. Além de sistemas como SpagoBI, o

Talend é integrado em sistemas de empresas como Ingres, Teradata e JasperSoft. O mecanismo de geração de código permite a integração do código gerado pelo Talend dentro de outras soluções, além de ter maior portabilidade. Outra vantagem de mecanismos de geração de código é que mecanismos de integração "online", conhecidos hoje como "integração operacional", podem ser implementados com maior facilidade. O conceito de geração de código versus "caixa preta" de execução dos processos ETL é a maior diferença entre o Talend e muitos outros sistemas. O conceito de geração de código não foi popular no passado, possivelmente por causa do marketing das empresas comerciais destas soluções, mas as vantagens que o Talend apresenta usando este conceito são importantes.

No caso, o Talend gera código Java ou Perl e SQL para os processos ETL. Além de aplicar o conceito ETL, ele aplica também o conceito ELT (*Extract*, *Load*, *Transform*), o que significa que pode aproveitar a eficiência e performance nativas de bancos de dados SQL; ou seja, os dados são extraídos, carregados no destino e, somente depois, já dentro do banco de destino, é aplicada a lógica de transformação usando SQL e linguagem procedural de cada banco de dados. Para a funcionalidade ELT são suportados nativamente hoje os bancos de dados Oracle, MySQL e Teradata.

Figura 3 Definição de repositório local inicial.

Operação

O sistema está disponível em versões para Linux, Unix e Windows. Para todas as plataformas é necessário ter Java e Perl no equipamento, considerando seu conceito de desenho que é de geração de código, ou seja, que os processos do Talend são executados pela máquina virtual Java (JVM) ou pelo interpretador Perl.

Figura 4 Geração de um novo projeto.

O download do sistema ainda é relativamente pesado (235 MB), mas com conexões de banda larga cada dia mais confiáveis e rápidas pode ser feito em poucas horas. Neste artigo exploraremos o Talend Open Studio para Linux em ambiente gráfico Gnome rodando em OpenSUSE 10.2. No caso de usá-lo em Windows 2000, existe um pré-requisito adicional que é a instalação do GDI requerido pelo Eclipse [10]. A partir do Windows XP, essa biblioteca está incluída nativamente. Vale a pena fazer o download também do pacote completo de documentação. Referente ao produto e à documentação, o Talend apresenta as vantagens de suporte por uma empresa comercial, pois a documentação é bastante completa. Outro destaque importante do Talend é o acesso a um sistema de ajuda online muito completo. Infelizmente, isso ainda não é norma na maioria dos sistemas de código aberto. O site do Talend oferece um wiki e uma área de tutoriais.

Simplesmente descompacte o pacote obtido por download e atribua propriedades de executável ao binário de início do sistema:

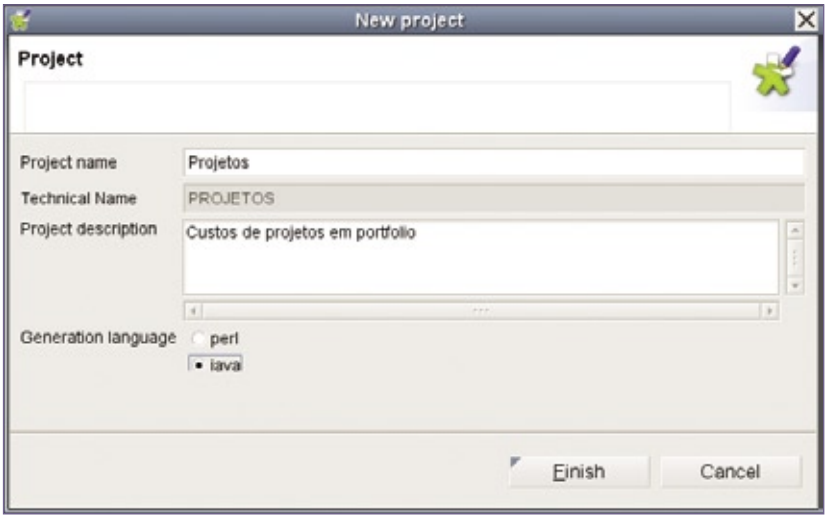


Figura 5 Detalhes de um novo projeto ETL.

```
chmod a+x TalendOpenStudio-linux-
➥gtk-x86
```

Selecione o binário de início apropriado para sua arquitetura de CPU. Para iniciar o gerenciador de processos, execute o binário:

```
./TalendOpenStudio-linux-gtk-x86 &
```

Isso exibirá a tela de abertura do sistema (**figura 2**).

Leia e aceite o contrato de licenciamento. Aparecerá finalmente a tela de conexão ao repositório de processos ETL (**figura 3**). No caso do Talend Open Studio, o repositório somente poderá ser local.

Com o repositório local definido, gere um projeto novo selecionando *Create a new local project* (**figura 4**).

Ao definir o título e a descrição do projeto, deve-se selecionar também a linguagem de geração do código. No exemplo para o artigo, escolhemos código em Java. A **figura 5** mostra as opções de definição do projeto.

Finalmente já se pode entrar no projeto escolhido pela tela principal, bastando selecionar nela o projeto e pressionar o botão *open*. Após alguns momentos aparecerá a tela principal do sistema. Na primeira vez, será pedido ao usuário que registre o uso digitando seu email e selecionando o país. Este passo não é obrigatório, mas é recomendado para receber notificações de novas versões do sistema.

Antes de usar o Talend Open Studio, deve ser configurada a lista de elementos disponíveis para o desenho. Isso pode ser feito modificando-se as propriedades do projeto na opção de "palette settings". A **figura 6** mostra a inclusão de conectores para MS SQL Server e PostgreSQL, que devem ser selecionados no caso de precisarmos desenhar um processo de integração de dados entre estes dois bancos de dados.

O desenho de um processo ETL requer várias etapas, incluindo desenho dos componentes de negócios, dos *jobs* de processamento, de conexões *JDBC*, acoplamento de módulos de processamento e outros elementos. A **figura 7** mostra um exemplo de configuração de conexão JDBC ao banco Microsoft SQL Server. O driver JDBC utilizado vem junto com a instalação do Talend, no caso, o excelente JTDS [11]. A **figura 8** mostra a tela do Talend Open Studio com a visão da paleta de ferramentas, componentes tratados e a edição de um elemento de negócios (*business object*).

Além das possibilidades de desenvolvimento lógico da solução dentro do ambiente gráfico, o Talend oferece

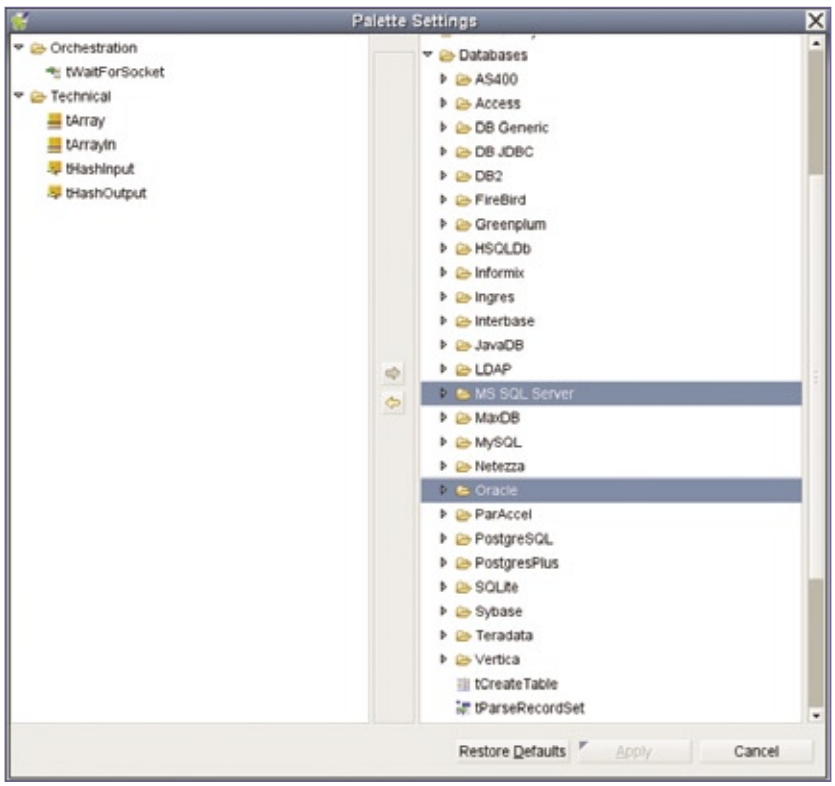


Figura 6 Formação da lista de ferramentas.

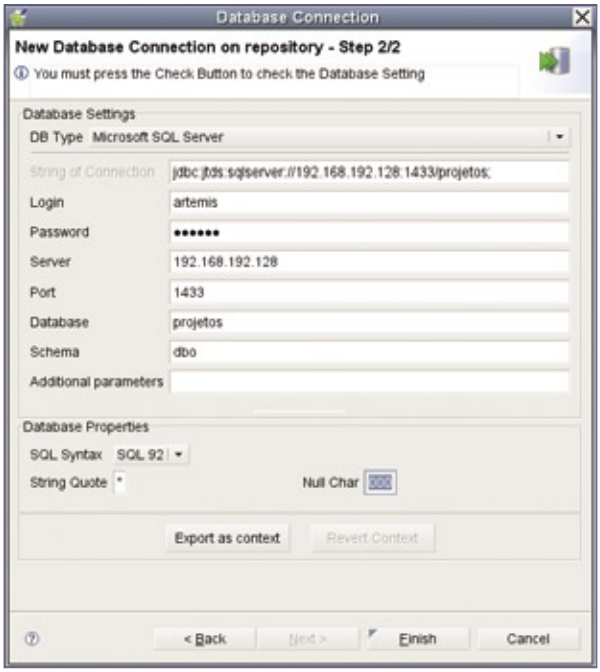


Figura 7 Definição de conexão JDBC.

ferramentas para preparar diagramas formatados para necessidades de documentação e apresentação. Por exemplo, podem ser escolhidas as fontes, as cores e os estilos de linhas para os objetos do diagrama, além de haver a possibilidade de alinhamento numa grade e a opção de layout automático dos componentes.

Entre as características que mais flexibilidade oferecem ao Talend está a biblioteca de componentes. Esses componentes estão divididos em grupos funcionais em que os de maior utilidade para uso corporativo podem ser os componentes preparados para acesso a outros sistemas, tais como *SugarCRM*, *Salesforce* e *SAP*. O Talend apresenta um destaque no mercado ao oferecer um conector ao SAP. A **figura 9** mostra alguns componentes do *Forge* do sistema que podem ser baixados e instalados para aumentar a funcionalidade padrão do Talend.

Um destaque do mecanismo de componentes do Talend é a possibilidade de publicar os processos automaticamente, por exemplo, no servidor de BI SpagoBI. Outro componente de uso geral e que incrementa em muito a complexidade de processos que podem ser definidos é o executor de scripts em *Groovy*. Além de poder desenvolver componentes específicos, a possibilidade de gerar scripts em Groovy para tratamento avançado dos dados permite que as transformações sigam regras muito especiais da empresa. A **figura 10** mostra a definição de integração com o SpagoBI.

Vale a pena destacar algumas características conceituais do editor gráfico que são importantes para uso corporativo do Talend:

- Os desenhos são versionados com a data de cada versão;
- Cada objeto dos modelos recebe um estado que pode ser "não verificado", "verificado" ou "validado" por default no caso dos business objects. Entretanto, podem ser definidos outros estados usados na empresa;
- Existe uma área em cada projeto para reunir a documentação que pode conter objetivos, justificativas, exemplos de resultados desejados etc. O Talend também gera documentação técnica e de processo automaticamente;
- Separação de papéis entre usuários de negócios que descrevem suas necessidades a nível macro (definindo business objects) e desenvolvedores (definindo jobs e outros elementos);
- Notificação ou atualização automática do sistema quando disponibilizadas novas versões Talend ou dos componentes;
- Facilidade para execução de testes individuais e integrados de componentes;
- Importação e exportação de projetos completos ou elementos.

O Talend é um sistema muito completo, com o apoio de uma empresa comercial, um ecossistema de componentes muito amplo e com um ambiente de definição

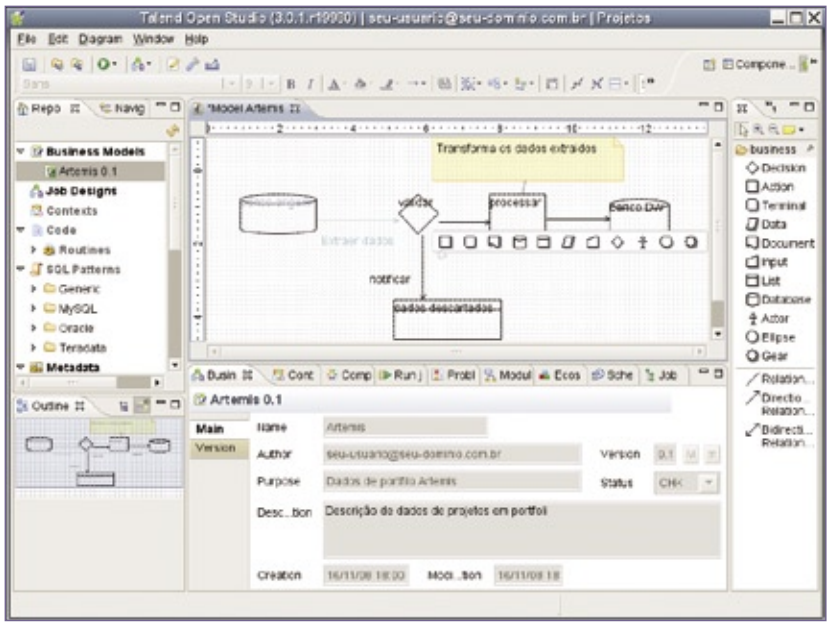


Figura 8 Tela do Talend Open Studio.

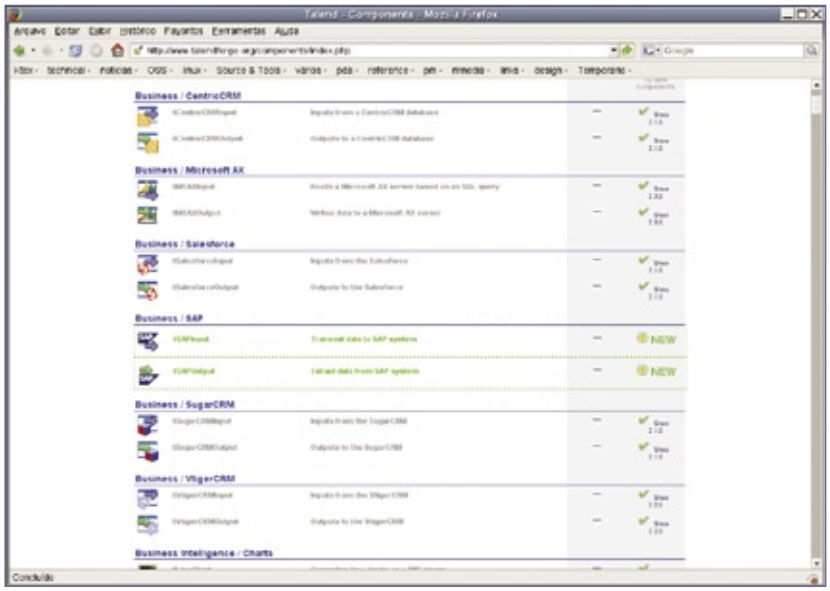


Figura 9 *Forge* de componentes mostrando aqueles específicos de algum sistema.

e desenvolvimento fácil de usar, além de poderoso e visualmente atraente. Assim, o projeto pode resolver a questão relatada no início do artigo sobre os motivos da falta de popularização de sistemas ETL no mercado.

Conclusão

Hoje, qualquer empresa tem necessidades de ETL e integração de dados, e em muitos casos é caro e complexo desenvolver soluções caseiras específicas. O Talend apresenta uma solução flexível com a qual estes processos podem ser modelados e executados de forma confiável. Podem ser definidos e documentados com a participação dos usuários que são os principais interessados no resultado final. Naturalmente, esse tipo de divisão de atividades ou responsabilidades requer que todos os usuários, independentemente do papel que desempenham no sistema, sejam devidamente treinados. Em TI, é cada vez mais comum haver situações em que os sistemas são simples e poderosos para usar, mas os usuários devem ser treinados nos princípios da tecnologia apresentada. Quem usa o Talend deverá estar ciente da documentação em inglês ou em francês, além do uso do sistema em inglês.

O uso do Talend dentro de uma empresa é facilitado pelas características corporativas do sistema que permitem, entre outras possibilidades, ter alta produtividade e visibilidade dos processos pelo apoio a componentes específicos, tais como conectores SAP, Salesforce ou customizados, e geração de documentação. Provavelmente será difícil encontrar um caso de uso que não possa ser atendido com comodidade pelo Talend. ■

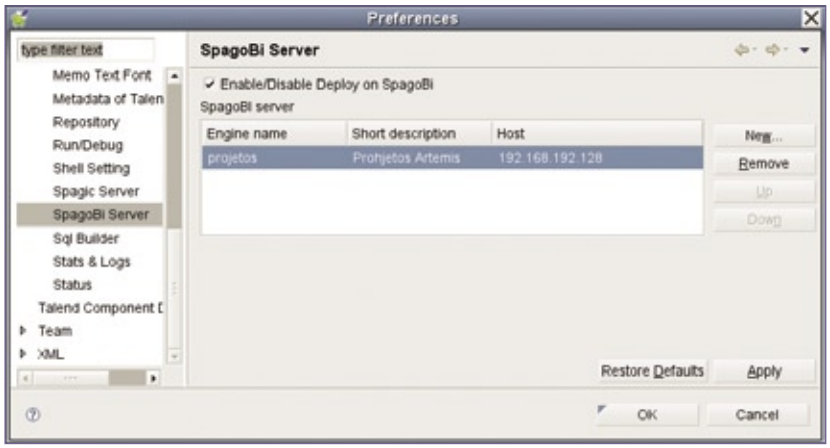


Figura 10 Integração com o *SpagoBI Server*.

Mais informações

[1] Talend: http://www.talend.com

[2] GPL versão 2: http://www.gnu.org/licenses/old-licenses/gpl-2.0.html

[3] Forrester Research: http://www.forrester.com

[4] IDC: http://www.idc.com

[5] Bloor Research: http://www.bloor-research.com

[6] SpagoBI: http://spagobi.eng.it

[7] Miguel K.O. de Lacy, "Negócio inteligente": http://www.lnm.com.br/article/1747

[8] Eclipse: http://www.eclipse.org

[9] Linux Magazine 36 – Eclipse: http://www.lnm.com.br/issue/1353

[10] GDI: http://www.eclipse.org/swt/faq.php#nographicslibrary

[11] JTDS: http://jtds.sourceforge.net

Gerenciamento de identidade na web com o Open ID

Identidade aberta, mas segura

O OpenID oferece um padrão aberto para login em websites fechados.

por Nils Magnus

A Web 2.0 é uma boa coisa, como todo mundo imagina. Um problema é a multiplicidade de sites protegidos por senha para acesso. Blogs pessoais, comunidades virtuais do Xing ao Orkut e Facebook e sites que gerenciam fluxo de trabalho, despesas, planejamento de férias, freqüentemente confiam em aplicações baseadas na web com o uso de contas de usuário privadas. Esse excesso de senhas de login está fazendo com que alguns usuários descontentes percam a paciência. Enquanto os usuários usam um dispositivo físico único e local, ferramentas como os gerenciadores de senhas oferecidos pela maioria dos navegadores e alternativas como o *KDE Wallet* são de grande ajuda.

Mas o paradigma da Web 2.0 supõe que o usuário tem a liberdade de se mover e efetuar login de diferentes locais.

Opção da comunidade

Soluções para o gerenciamento de identidades fornecem uma solução de maior mobilidade e flexibilidade para simplificar o login via web. Essas ferramentas muitas vezes empregam o princípio da idoneidade com terceiros. Alguns grandes *players* globais têm avançado com serviços que oferecem soluções de login confiáveis, desenvolvidas por terceiros, de uma única fonte. O sistema *Microsoft Passport* foi criado em sintonia com esse sentimento. Hoje, o mercado do Microsoft Passport é o "Windows Live ID" [1]. Muitos usuários, no entanto, estão receosos de se tornarem dependentes de aplicativos proprietários.

Uma recente alternativa conhecida como *Liberty Alliance Project* [2] ofereceu uma abordagem mais aberta, mas foi amplamente considerada como um exagero de especificações, e por isso ainda não obteve grande adoção, apesar de seus sete anos de esforço. O projeto *OpenID*, sob os auspícios da OpenID Foundation [3], se baseia na mais simples funcionalidade, podendo ser mais facilmente integrado a sistemas de autenticação online.

Os usuários que optaram pela alternativa do OpenID não inserem um nome de usuário, mas, em vez disso, identificam-se com uma URI que pode ser exibida em um navegador web. A URI pode ser um endereço web oferecido por um serviço OpenID, como `http://nilsmagnus.myopenid.com` no *MyopenID* [4]. O tipo de identidade não é importante, contanto que qualquer navegador consiga acessar a página. A página terá que adicionar uma *tag* que aponte para o provedor do serviço:

```
<link rel="openid.server"
➥ href="http://www.myopenid.com/
➥server" />
<link rel="openid.delegate"
➥ href="http://nilsmagnus.myopenid.
➥com/" />
```

O servidor do lado do provedor especifica a primeira relação; a segunda reafirma o nome da identidade. O provedor normalmente cria uma página para tornar essa informação disponível para os sites na Web que requisitem as informações de login. Contudo, um usuário poderia, de forma alternativa, integrar os detalhes necessários em uma página ou blog pessoal. Nesse caso, seu próprio endereço poderia servir como sua OpenID.

O login

Uma aplicação que suporte o OpenID exibirá um campo de login OpenID além da página de login tradicional. Por exemplo, a **figura 1** mostra a página de autenticação do OpenID no wiki do Amarok.

Quando um usuário digita seu ID baseado em uma URI, a aplicação web, que é conhecida como o

Figura 1 O wiki do Amarok permite que seus usuários efetuem login com o OpenID.

cliente na linguagem do OpenID, recupera a porção do servidor da URI. O OpenID se refere ao servidor como "provedor de identidade" (*identity provider*).

O cliente (o wiki do Amarok, neste caso) solicita ao provedor o nome associado à URI. Para fazer isso, ele redireciona a requisição para o provedor do site, e o provedor indica que foi emitida a solicitação. O usuário então concorda com o pedido, digitando uma senha. O provedor redireciona o navegador de volta para o site do cliente, onde o usuário está agora logado.

Uma prática característica do OpenID é a possibilidade de armazenar vários atributos para uma única identidade com um provedor; por exemplo, seu nome completo, seu idioma preferido ou sua data de nascimento (ver **figura 2**). O usuário que recebe um pedido do cliente pode especificar quais os dados que o prestador deve divulgar para o cliente e quais ele deve conservar como secretos.

Esse processo de aprovação é importante para evitar o mau uso de um parâmetro crítico, tal como o PIN de um banco, que na verdade até pode ser armazenado junto ao seu ID. Alguns provedores permitem que o usuário crie múltiplas identidades, cada uma com um conjunto distinto de atributos.

Essa abordagem também é conhecida como *Gerenciamento de Identidade Centrada no Usuário* (do inglês *User-Centric Identity Management*), em que cada usuário pode definir individualmente as informações fornecidas pelo provedor para os clientes que pedirem.

Alguns provedores de identidade associam-nas gratuitamente. Cabe ao usuário decidir em qual provedor confiar. Diferentemente da abordagem centralizada utilizada pelo Passport, um conjunto descentralizado de provedores OpenID competem entre si na oferta de serviços. Os usuários têm até mesmo a liberdade de criar seu próprio provedor.

Para quem se interessar pelo desenvolvimento de uma solução própria, há pacotes de código aberto em várias linguagens de programação, como *Perl*, *PHP*, *Ruby*, *Python*, e *Java* [5].

Tem segurança?

O OpenID pode gerar dúvidas sobre sua segurança, já que qualquer um pode atuar como provedor. Um agressor pode forjar (*spoof*) ou seqüestrar uma identidade? A primeira questão aponta para um clássico problema de segurança: se você pode manipular um site de terceiros, você pode redirecionar os visitantes para o seu próprio provedor de identidade ou escrever um para se adequar à demanda.

Em outras palavras, a segurança está nas mãos das pessoas responsáveis pelo site hospedeiro. Considerando-

Figura 2 O provedor especifica os detalhes que pretende enviar para o cliente.

Tabela 1: Provedores de identidade para aplicações web

Provedor	OpenID
AOL	http://openid.aol.com/nome_do_usuário
Blogger	http://nome_do_blog.blogspot.com
Flickr	http://www.flickr.com/photos/usuário
Livedoor	http://profile.livedoor.com/usuário
Livejournal	http://usuário.livejournal.com
Technorati	http://technorati.com/people/technorati/usuário
Wordpress	http://usuário.wordpress.com
Yahoo	http://openid.yahoo.com

se a qualidade do código dos muitos sites escritos nas populares linguagens de script, essa é uma preocupação real, mas não um argumento fundamental contra o OpenID.

A segunda pergunta é complicada: é possível que um hacker capture as comunicações entre o cliente e o provedor de identidade e com isso armazene as sessões? Afinal, o provedor envia uma confirmação de mensagem em caso de sucesso na autenticação. Um agressor poderia tentar apresentar uma sessão gravada na próxima tentativa de login. No entanto, isso pode ser evitado com a ativação do SSL ou do TLS no OpenID para proteger a conexão e adicionar um desafio para cada solicitação. Essa abordagem significa que qualquer resposta será válida apenas uma vez, o que exclui a reciclagem trivial.

Apesar disso, não é uma boa idéia subestimar a complexidade do gerenciamento de sessão baseado em estado (*stateful*) que trafega sobre um protocolo sem base em sessão (*stateless*) como o HTTP, que é a base do OpenID. O fato de várias aplicações web estarem sendo comprometidas é uma indicação clara dos perigos, supondo que você acredite em pesquisas e *whitepapers* [6].

Prático e aberto

O OpenID é um passo na direção certa para o gerenciamento de identidades. Como ele implementa o login único (*single sign-on*), também se torna mais conveniente para os usuários, reduzindo o número de senhas a serem lembradas. A capacidade de gerenciar atributos é muito mais poderosa do que parece à primeira vista.

O número de sites que usam OpenID continua crescendo vertiginosamente, mas algumas grandes aplicações continuarão precisando provar se preenchem todas as exigências operacionais e conceituais no que diz respeito à confiança e à disponibilidade. ■

Quadro 1: Gerenciamento de identidade e federação

O OpenID não é só um projeto de gerenciamento de identidade. O Feder ID [7], por exemplo, é um projeto de código aberto da França. Um dos financiadores do projeto, Oudot Clément, enfatiza a importância das identidades digitais para o acesso aos recursos da Web em uma recente entrevista com a Linux Magazine.

De acordo com Oudot, muitos usuários possuem uma identidade distinta para cada site. Isto é um grande problema para grandes empresas e organizações, já que os usuários precisam memorizar múltiplas senhas. O Feder ID fornece ferramentas para a sincronização de repositórios de identidade. Estes atributos não estão disponíveis apenas para uma única organização local; eles podem ser compartilhados por parceiros confiáveis.

As ferramentas do Feder ID são de código aberto e respeitam os padrões da IETF (*Internet Engineering Task Force*), OASIS (*Organization of Structured Information Standards*), e da Liberty Alliance para a gestão de identidades.

Mais informações

[1] Microsoft Passport: http://www.passport.net

[2] Projeto Liberty Alliance: http://www.projectliberty.org

[3] Projeto OpenID: http://openid.net

[4] MyOpenID: http://myopenid.com

[5] Bibliotecas abertas de OpenID: http://wiki.openid.net/Libraries

[6] Secure Computing, "Keeping Customers and Merchants Secure" (em inglês): http://www.securecomputing.com/webform.cfm?id=289&ref=pci

[7] Feder ID: http://federid.objectweb.org

[8] Extensões do Mediawiki para OpenID: http://www.mediawiki.org/wiki/Extension:OpenID

[9] Suporte a OpenID no Drupal: http://drupal.org/project/openid

Você está preparado para a TI virtualizada?

Aprenda a projetar e implementar infraestruturas de virtualização com Xen. Conheça outras soluções de Código Aberto, leia workshops profissionais, e maximize o desempenho em TI de sua empresa.

mais informações: www.linuxnewmedia.com.br

Coleção Linux Technical Review

LINUX NEW MEDIA
The Pulse of Open Source

Login no Linux pela impressão digital

Autenticação biométrica

A autenticação em sistemas Linux por meio da biometria já é uma realidade. Aprenda a instalar e a configurar esse recurso de segurança.

por Alessandro de Oliveira Faria (Cabelo)

Hoje a autenticação biométrica é imprescindível para elevarmos o nível de segurança computacional. Na **Linux Magazine** 48 foram mencionadas as principais tecnologias biométricas de código aberto. Agora, neste documento, veremos na prática o uso da biometria para autenticação de identidade. Esse recurso não faz parte apenas dos filmes de ficção científica; é uma realidade cada vez mais presente no nosso dia-a-dia em diversos segmentos do mercado.

Figura 1 Imagem extraída de um leitor de impressão digital U.Are.U da Digital Persona.

Com o crescimento dos equipamentos em redes abertas, surgiram problemas de segurança e confiabilidade de autenticação. Uma autenticação indevida fornece acesso privilegiado a pessoas não autorizadas, dando margem a roubo de informações, interrupções de serviços, fraudes sistemáticas, entre outros transtornos do século XXI.

Neste cenário surgiu a necessidade da autenticação biométrica, ou seja, verificação da autenticidade do usuário em operação. Esse mecanismo computacional é baseado em características ("o que você é"). A biometria aplicada à autenticação de usuários é um método automatizado para medir as características humanas e confrontá-las em uma base de dados, obtendo assim a autenticidade do usuário.

A eficácia da autenticação biométrica está diretamente relacionada à qualidade dos dados obtidos na fase de cadastramento da característica biométrica. Nessa etapa, a base de dados recebe o *template* matemático calculado pelo sistema, isto é, a representação binária da característica humana. Essa informação será utilizada posteriormente na comparação biométrica para autenticação do sistema, obtendo assim um resultado positivo ou negativo.

Este artigo apresenta um foco técnico e pouco teórico, assim obje-

Figura 2 Imagem binarizada (branco e preto).

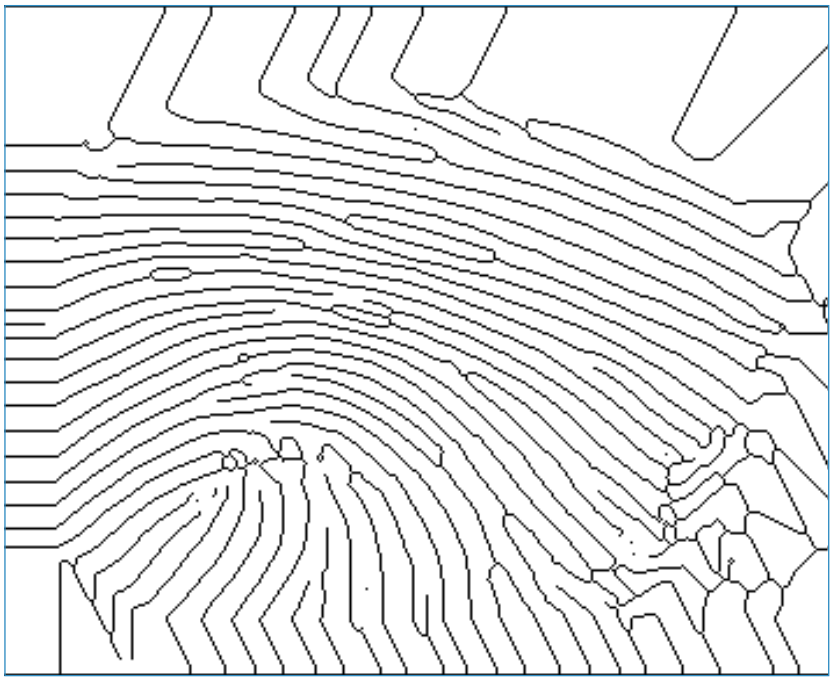


Figura 3 Linhas reduzidas para um único pixel.

tivando configurar ou acrescentar a autenticação biométrica como nível adicional de segurança ao login do sistema operacional Linux. Para tal operação, utilizaremos a tecnologia de impressão digital e pacotes de código aberto (biblioteca *fprint*).

A tecnologia utilizada para a confecção deste artigo foi:

- OpenSuse 10.3 – kernel 2.6.22.5-31-bigsmp;
- Notebook Dell Vostro 1510;
- 4 GB de memória RAM;
- Processador Core 2 Duo;
- Leitor de impressão digital U.are.U Digital Persona 4000B;
- Biblioteca fprint.

Fprint: conceitos

O pacote *fprint*[1] é o sonho de todo desenvolvedor de código aberto. O kit de integração permite o desenvolvimento de rotinas para identificação e verificação de impressões digitais do usuário. Um dos pontos fortes dessa solução livre é a compatibilidade com diversos modelos de sensores disponíveis no mercado. A lista de aparelhos compatíveis encontra-se em [2].

A impressão digital é composta por linhas formadas pelas elevações da pele. A comparação por impressão digital é um método utilizado há mais de mil anos como forma de identificação de usuários. É uma característica única entre os seres humanos, inclusive entre irmãos gêmeos univitelinos.

Formada ainda quando feto, a impressão digital acompanha a pessoa por toda a sua existência sem apresentar grandes mudanças. Extraindo os pontos característicos ou "pontos de minúcias" de uma impressão digital, um papiloscopista ou sistemas computadorizados podem identificar pessoas utilizando cálculos bastante confiáveis. Grande parte dos algoritmos trabalham com o princípio de extração desses pontos característicos. Após a extração, são calculados a relação entre as distâncias desses pontos. Cada algoritmo possui sua base de cálculo, seja por análise dos pontos entre si ou por agrupamentos de pontos para análise de semelhanças de triângulos com os ângulos internos.

A biblioteca fprint incorpora abstração de hardware para acesso ao leitor. Com esse recurso, não precisamos instalar qualquer módulo do kernel para o funcionamento de cada modelo de leitor de impressão digital.

Na primeira fase a biblioteca extrai a imagem do sensor (**figura 1**) e, logo a seguir, a linha da impressão digital é realçada com a cor preta (**figura 2**)

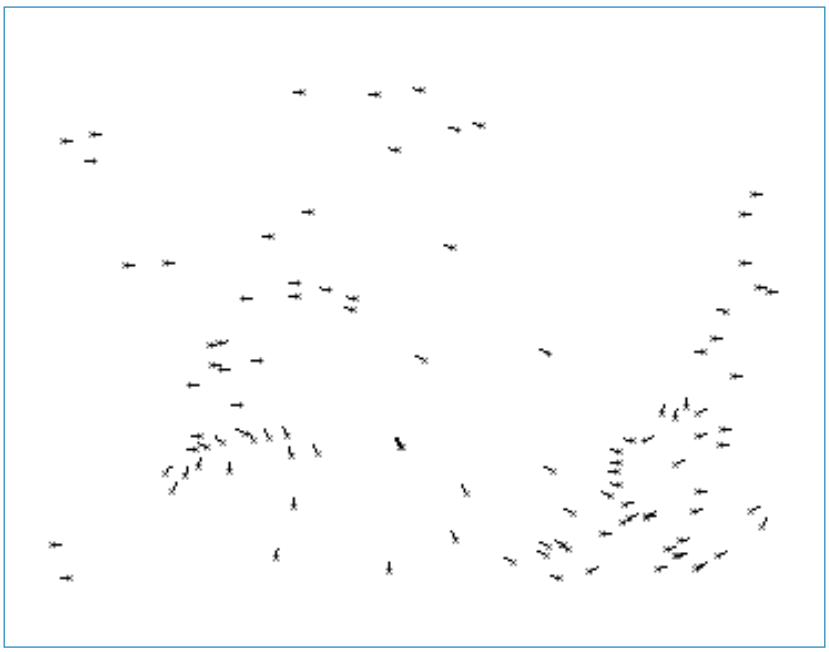


Figura 4 Pontos de bifurcação e terminadores.

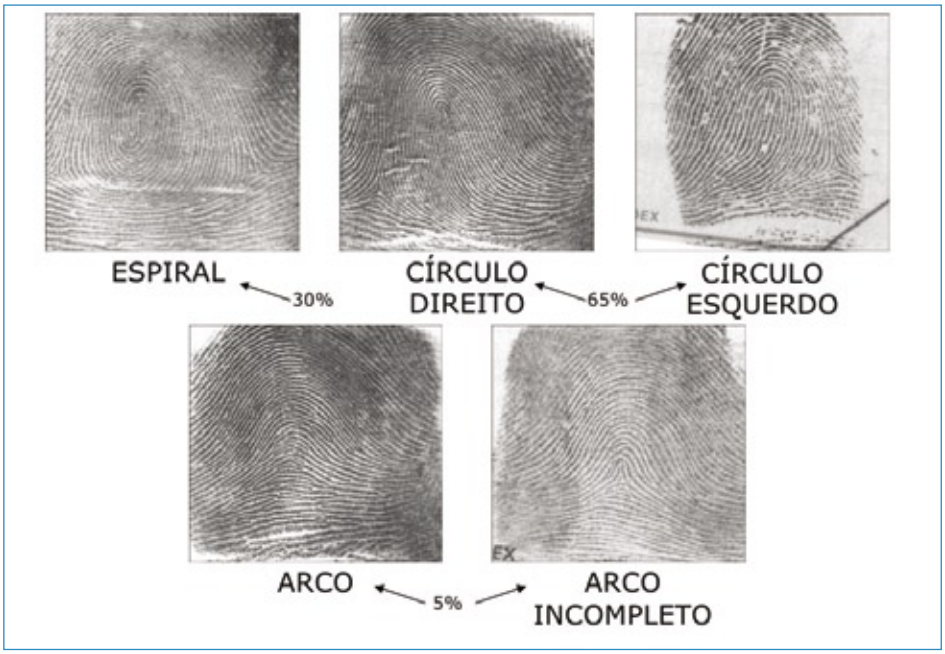


Figura 5 Os cinco grupos de impressões digitais.

As impressões digitais são classificadas em cinco grupos, conforme mostra a **figura 5**: círculo direito, círculo esquerdo, espiral, arco e arco incompleto. A estrutura de uma impressão digital é formada por cruzamentos das linhas, *core* (centro), bifurcações, terminações, ilhas, deltas (bifurcações inferiores) e poros. Os pontos terminais, assim como os pontos de bifurcações, são definidos em função da distância (coordenada relativa) para o core. Nos pontos terminais é comum calcular seu ângulo de inclinação.

utilizando algoritmos de extração com filtros. Na próxima etapa, a imagem já está *binarizada* (branco e preto, **figura 3**) e as linhas foram reduzidas a um único pixel de largura. Por último, a tarefa mais fácil, ou seja, detectar os pontos de minúcias. Fazendo um exame de cada pixel na imagem, se houver um pixel branco sem vizinhos, isso significa que encontramos um ponto terminal. Caso um ponto branco possua três pontos vizinhos, significa que encontramos uma bifurcação. Os pontos de minúcias são então destacados (**figura 4**) e compõem a verdadeira identidade da impressão digital.

Instalação

Há pacotes da biblioteca fprint pré-compilados para OpenSuse [3] e Ubuntu [4]. No entanto, este artigo sugere a compilação da biblioteca a partir de seu código-fonte, que pode ser obtido em [5]. Há também uma demonstração do software fprint que pode ser baixada a partir de [6].

Após o download, devemos descompactar os arquivos fontes. O **exemplo 1** detalha o procedimen-

Exemplo 1: Preparação da libfprint

```
$ tar -jxvf libfprint-0.0.6.tar.bz2
$ cd libfprint-0.0.6
$ ./configure
$ make
$ su
Senha:
# make install
# ldconfig
```

Exemplo 2: Compilação do pam_fprint

```
$ wget http://ufpr.dl.sourceforge.net/
➥sourceforge/fprint/pam_fprint-0.2.tar.
➥bz2
$ tar -jxvf  pam_fprint-0.2.tar.bz2
$ cd pam_fprint-0.2
$ ./configure
$ make
$ sudo make install
```

Exemplo 3: Arquivo de login do PAM

```
01 #%PAM-1.0
02 auth     requisite      pam_nologin.so
03 auth     [user_unknown=ignore success=ok ignore=ignore
➥ auth_err=die default=bad] pam_securetty.so
04 auth     include        common-auth
05 auth     requisite      pam_fprint.so
06 account  include        common-account
07 password include        common-password
08 session  required       pam_loginuid.so
09 session  include        common-session
10 session  required       pam_lastlog.so  nowtmp
11 session  required       pam_resmgr.so
12 session  optional       pam_mail.so standard
13 session  optional       pam_ck_connector.so
```

Exemplo 4: pam_fprint_enroll --help

```
# pam_fprint_enroll --help
Usage: ./pam_fprint_enroll options
     -h      --help                  Display this usage information.
     -f      --enroll-finger index   Enroll finger with index.

     Valid indexes are:
     1 - Left Thumb
     2 - Left Index Finger
     3 - Left Middle Finger
     4 - Left Ring Finger
     5 - Left Little Finger
     6 - Right Thumb
     7 - Right Index Finger
     8 - Right Middle Finger
     9 - Right Ring Finger
     10 - Right Little Finger
```

Exemplo 5: Cadastramento de digital

```
# pam_fprint_enroll --enroll-finger 7

This program will enroll your finger, unconditionally overwriting
any selected print that was enrolled previously. If you want to
continue, press enter, otherwise hit Ctrl+C

Found device claimed by Digital Persona U.are.U 4000/4000B driver
Opened device. It's now time to enroll your finger.

You will need to successfully scan your Right Index Finger 1 times
to complete the process.

Scan your finger now.
Enroll complete!
Enrollment completed!
```

Exemplo 6: Sucesso na autenticação biométrica

```
Welcome to openSUSE 10.3 (i586) - Kernel 2.6.22.5-31-bigsmp (tty1).
➥lapdell01 login: root
Senha:
Scan right index finger on Digital Persona U.are.U 4000/4000B
Último login:Dom Nov 16 23:15:01 BRST 2008em tty2

Have a lot of fun...
```


Exemplo 7: Falha na autenticação biométrica

```
Welcome to openSUSE 10.3 (i586)
➥- Kernel 2.6.22.5-31-bigsmp
➥(tty1).

lapdell01 login: root
Senha:
Scan right index finger on
➥Digital Persona U.are.U
➥4000/4000B
Login incorreto
```

to de configuração e compilação da biblioteca.

Execute o comando "make" convencional para efetuar a compilação na íntegra do código-fonte, a seguir transforme-se em super-usuário (root) para efetuar a instalação da biblioteca por meio do comando "make install", seguido do "ldconfig", conforme as instruções a seguir.

Autenticação: pam_fprint

O módulo biométrico que trabalha em conjunto com o sistema de autenticação PAM (*Pluggable Authentication Modules*) é o *pam_fprint*. Sua base tecnológica é a biblioteca fprint recém compilada e instalada. O pacote *pam_fprint* utiliza as funções biométricas para processar e verificar a autenticação do usuário. Em outras palavras, a sua impressão digital é utilizada para efetuar o login no sistema operacional.

Vale a pena mencionar que o PAM é um sistema para autenticação de usuários em ambientes Linux e Unix. Uma de suas principais vantagens é a centralização das chamadas e funções de login, assim facilitando a tarefa do desenvolvedor.

Continuando nossa jornada, vamos agora baixar, descompactar, compilar e instalar o pacote *pam_fprint* como no **exemplo 2**.

Configuração

No OpenSuse, é preciso modificar o arquivo de configuração para autenticação no modo console, `/etc/pam.d/login`. Esse arquivo pode ter nome diferente em outras distribuições. Seu conteúdo é mostrado no **exemplo 3**, e a **linha 5** deve ser acrescentada, pois é a responsável por requisitar o módulo pam_fprint.

É importante notar a utilização do modo `requisite` de autenticação no PAM. Para maiores informações sobre o tipo de autenticação, recomenda-se consultar a documentação do PAM.

Cadastramento

O próximo passo é efetuar o cadastramento biométrico da sua impressão digital. Se concluída com sucesso essa tarefa, no próximo login o usuário deverá fornecer, além da senha, sua impressão digital para ter acesso ao sistema.

O programa *pam_fprint_enroll* é responsável pelo cadastramento das impressões digitais. Para entender melhor sua sintaxe, digite `pam_fprint_enroll --help` e perceba (**exemplo 4**) que é preciso informar o número correspondente ao dedo utilizado para cadastro. A numeração começa em 1 no polegar esquerdo e segue até o dedo mindinho esquerdo (número 5), seguindo depois para o polegar direito (6) e terminando no mindinho direito (10).

No meu caso, utilizei o número 7, representando o dedo indicador da mão direita (**exemplo 5**). Ao executar o programa, pressione [**ENTER**], encoste o dedo no leitor de impressão digital e pronto! Nessa fase, ao efetuar o login, o sistema operacional solicitará a senha seguida da autenticação biométrica, como mostram os **exemplos 6** (sucesso na autenticação) e **7** (falha na autenticação biométrica).

Conclusão

A biblioteca fprint proporciona inúmeros recursos além dos mencionados neste artigo. Para um estudo detalhado sobre o assunto, sugiro algumas leituras no portal Viva o Linux [7] e também no site oficial do projeto. ■

Mais informações

[1] Fprint: http://reactivated.net/fprint/wiki/Main_Page

[2] Dispositivos compatíveis com a fprint: http://reactivated.net/fprint/wiki/Supported_devices

[3] Pacotes fprint para OpenSuse: http://download.opensuse.org/repositories/home:/dgege/

[4] Pacotes fprint para Ubuntu: http://www.madman2k.net/comments/105

[5] Download da biblioteca fprint: http://ufpr.dl.sourceforge.net/sourceforge/fprint/libfprint-0.0.6.tar.bz2

[6] Demo do fprint: http://ufpr.dl.sourceforge.net/sourceforge/fprint/fprint_demo-0.4.tar.bz2

[7] Portal Viva o Linux: http://www.vivaolinux.com.br

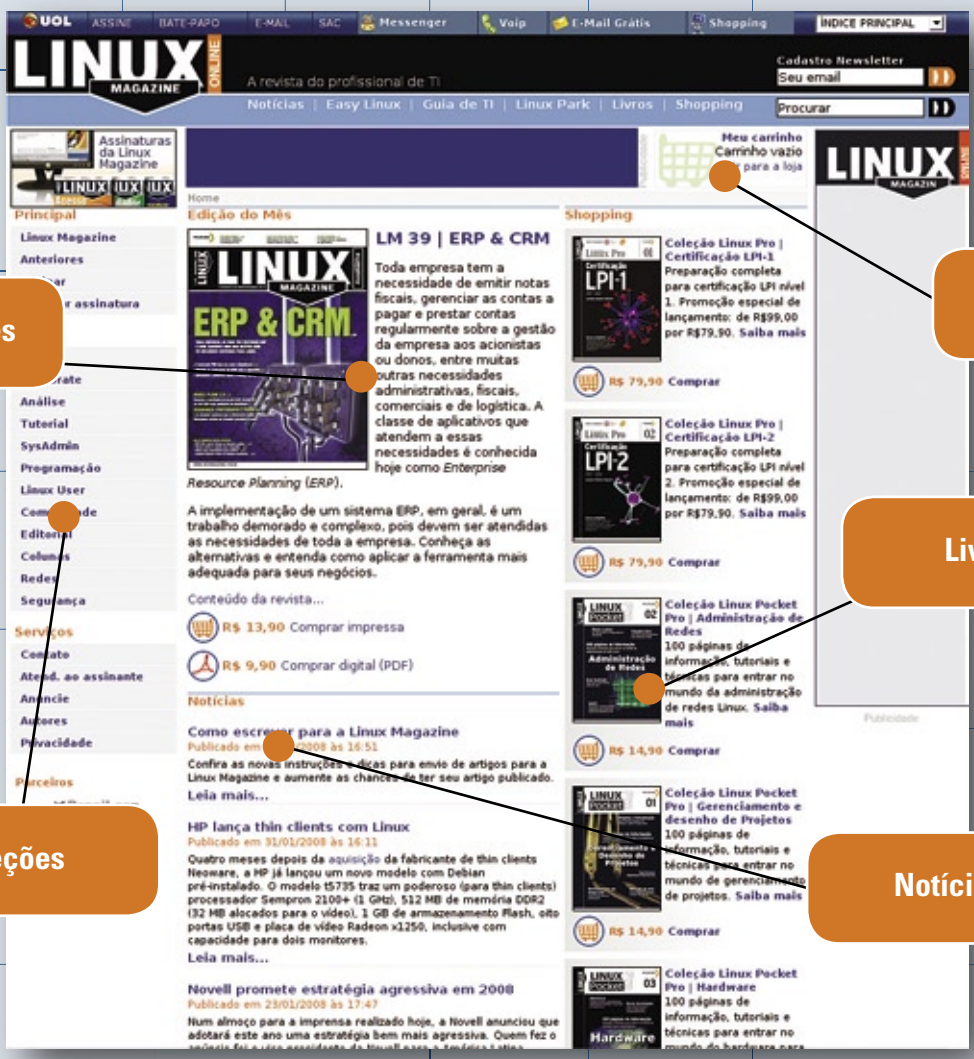
Sobre o autor

Alessandro Faria é sócio-proprietário da NETi TECNOLOGIA, fundada em Junho de 1996 (http://www.netitec.com.br), empresa especializada em desenvolvimento de software e soluções biométricas. Consultor Biométrico na tecnologia de reconhecimento facial, atua na área de tecnologia desde 1986, propiciando assim ao mercado soluções em software. Leva o Linux a sério desde 1998 com desenvolvimento de soluções open source, é membro colaborador da comunidade Viva O Linux e mantenedor da biblioteca open source de vídeo captura, além de participar entre outros projetos.

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

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	Carapicuíba	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	Av. Paulista, 2028 – CEP: 01310-200	11 3543-5543	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	✔	✔			✔	
2MI Tecnologia e Informação	Embu	Rua José Bonifácio, 55 – Jd. Independência – SP CEP: 06826-080	11 4203-3937	www.2mi.com.br		✔	✔		✔	✔

Calendário de eventos

Evento	Data	Local	Website
Campus Party	15 a 25 de janeiro	São Paulo, SP	www.campus-party.com.br
Bossa Conference	08 a 11 de março	Porto de Galinhas, PE	www.bossaconference.org
FISL	24 a 27 de junho	Porto Alegre, RS	www.fisl.softwarelivre.org
Interop	02 e 03 de setembro	São Paulo, SP	www.interopsaopaulo.com.br
Futurecom 2009	13 a 16 de outubro	São Paulo, SP	www.futurecom2009.com.br

Índice de anunciantes

Nerdson – Os quadrinhos mensais da Linux Magazine

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

PREVIEW

Na Linux Magazine #51

DESTAQUE

Segurança com VoIP

Verdadeiros administradores pensam em segurança o tempo inteiro. Mesmo que você seja um usuário comum, é importante saber o que os invasores podem fazer. Serviços que costumavam ser seguros se tornam brechas de segurança, a menos que você se mantenha atualizado com essas questões.

Na **Linux Magazine** 51 vamos examinar algumas estratégias de segurança recomendadas por especialistas. Você jamais terá a rede perfeita ou sequer as ferramentas perfeitas – o mundo da segurança de redes muda a todo tempo – e como é impossível descartar definitivamente os problemas, é melhor manter-se informado. ■

TUTORIAL

Deficientes visuais

O Linux possui muitos ambientes desktop belíssimos, incluindo cubos rotativos e janelas que balançam e queimam. Porém, considere, por exemplo, uma área de trabalho com ícones cuidadosamente organizados: você conseguiria utilizá-la com o monitor desligado?

Apesar das várias ofertas de softwares proprietários caríssimos para leitura da tela e teclados sofisticados que realmente possibilitam o uso do computador por deficientes visuais, a maioria das ferramentas e extensões necessárias para usuários cegos ou com visão prejudicada, além daqueles com dificuldades motoras ou mentais, já estão presentes nos repositórios da maioria das distribuições Linux. Veja como o projeto *Adriane* une todos esses recursos num único sistema desktop destinado a deficientes visuais. ■

Na EasyLinux #14

Monitores gigantes

Os monitores LCD de 19 polegadas já têm preços bem melhores que há um ano. Será que já chegou o momento de você comprar aquele monitor cinematográfico? Quais são as vantagens e desvantagens do LCD em relação aos antigos monitores de tubo? Até onde 21 polegadas valem mais que 19? Na Easy Linux 14, vamos comparar marcas, modelos e tecnologias de monitores à venda no Brasil para orientar suas compras. ■

A melhor parte de todos os sistemas

Empresas como Apple e Microsoft investem pesado em design para deixarem seus sistemas mais atraentes. Como resultado, tanto o Mac OS quanto o Windows Vista têm forte apelo visual. Porém, engana-se quem pensa que é impossível alcançar um grau de beleza semelhante no Linux. Na Easy Linux 14, vamos mostrar o caminho das pedras para deixar seu Linux com a cara do Mac OS X, do Vista e do Windows XP, seja por pura diversão ou para facilitar o uso do Linux por quem já está habituado a esses sistemas e tem dificuldade de adaptação ao pingüim. ■

Primeiro Super-Computador Híbrido da Europa

25 TB de Memória Principal, 1.000 TB de Armazenamento gerenciados através do Lustre®

O primeiro da Europa

Potência total acumulada de 295 Teraflops

Produção
8544 Núcleos (CPU's) Intel®
103 Teraflops

Pesquisa
46 080 Núcleos (CPU's) NVIDIA
192 Teraflops

BULL
Architect of an Open World™

Compacto
Design inovador
Alta performance

Apresentando uma linha totalmente nova de produtos Ubiquiti Networks liderados pelo dispositivo revolucionário, The Bullet. www.ubnt.com

BULLET
UBIQUITI NETWORKS

Transforme imediatamente qualquer antena em um sistema de rádio de categoria industrial. AP completo com conector tipo N à prova d'água! Basta plugar e usar!

NanoStation loco

Com até 10km de alcance e mais de 25Mbps de velocidade, o minúsculo NanoStation loco agrupa um poder louco.

PicoStation

O menor AP para ambientes externos no mundo também é o mais potente. Com até 1000mW de potência, o PicoStation fornece um alcance sem precedentes.

md brasil TELECOMUNICAÇÕES

md brasil telecom
Distribuidor Autorizado
www.mdbrasil.com.br
Tel: (17) 3344-7277

WDC Networks

WDC Networks
Distribuidor Autorizado
www.wdcnet.com.br
Tel: +55 (11) 3035-3777

UBIQUITI NETWORKS