LINUX NEW MEDIA
The Pulse of Open Source

UNIDOS PELO MIDDLEWARE p.24
Entrevista com o presidente do OW2

SOA A SÉRIO p.22
Entrevista com o criador do framework CoreBuilder

CEZAR TAURION p.28
Previsões para o SL/CA em 2008

#38 Janeiro 2008
LINUX MAGAZINE

LINUX MAGAZINE

A REVISTA DO PROFISSIONAL DE TI

#38 01/08
R$ 13,90
€ 7,50
9 771806 942009 00038

Acesso Remoto

ADMINISTRAR SERVIDORES REMOTAMENTE E APROVEITAR SUAS FÉRIAS NÃO É UM SONHO DISTANTE.

p.29

PARA QUEM SEU PINGÜIM TIRA O GORRO?
SÓ A F-SECURE TEM TODAS AS SOLUÇÕES DE SEGURANÇA EM UM ÚNICO PRODUTO.

Os sinos de Natal anunciam a proteção mais completa contra *phishing*, *spywares*, vírus, *worms*, tentativas de invasão, além de controle de conteúdo e trava de tempo para a web. É o **F-Secure Client Security**, a solução mais completa em um único sistema de segurança que deixa você, usuário Linux, realmente protegido contra ameaças virtuais.

Por que a **F-Secure** é a **mais indicada** para quem trabalha com Linux?

- Centralmente gerenciável (PMC mesmo estando na plataforma Windows)
- Verificação da integridade do sistema
- Prevenção do rootkit
- Firewall baseado no "host"
- Controle de Conteúdo

F-SECURE®

BE SURE.

Tel: (11) 2108.3300

f-secure@f-secure.com.br

www.f-secure.com.br

antivírus | anti-spywares | anti-rootkit | anti-spam | firewall | controle de conteúdo e aplicativos

Expediente editorial

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

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

Editor
Pablo Hess
phess@linuxmagazine.com.br

Revisão
Arali Lobo Gomes
agomes@linuxmagazine.com.br

Editor de Arte
Renan Herrera
rherrera@linuxmagazine.com.br

Assistente de Arte
Igor Daurício
isilva@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

Hubert Wiest (Alemanha, Áustria e Suíça)
anzeigen@linuxnewmedia.de

Brian Osborn (Outros países)
ads@linux-magazine.com

Assinaturas:
www.linuxnewmedia.com.br
assinaturas@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

Gerente de Circulação
Cláudio Guilherme dos Santos
csantos@linuxmagazine.com.br

Linux Magazine é publicada mensalmente por:

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

Distribuição: Distmag

Impressão e Acabamento: Parma

Atendimento Assinantes
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

Do nicho para o mundo

Prezados leitores da Linux Magazine,

Embora o mito da dificuldade em se ganhar dinheiro com Software Livre e de Código Aberto já tenha sido superado há tempos, ainda há partes do mercado em que suas raízes estão mais aprofundadas. Então, mesmo sob o risco de me repetir ou, pior ainda, repetir célebres defensores do SL/CA, vou expor mais uma vez um recente fenômeno da penetração do Linux.

O subnotebook fabricado pela Asus e equipado com Linux pela Xandros, o EeePC, ilustra como duas empresas que dependem primordialmente de software estão conseguindo atrair consumidores e gerar receita com base em SL/CA. Na realidade, "atrair consumidores" seria menosprezar o poder desse portátil de menos de um quilo. No último Natal, o EeePC foi um dos itens mais disputados, com os estoques acabando na maioria das lojas onde ele foi comercializado.

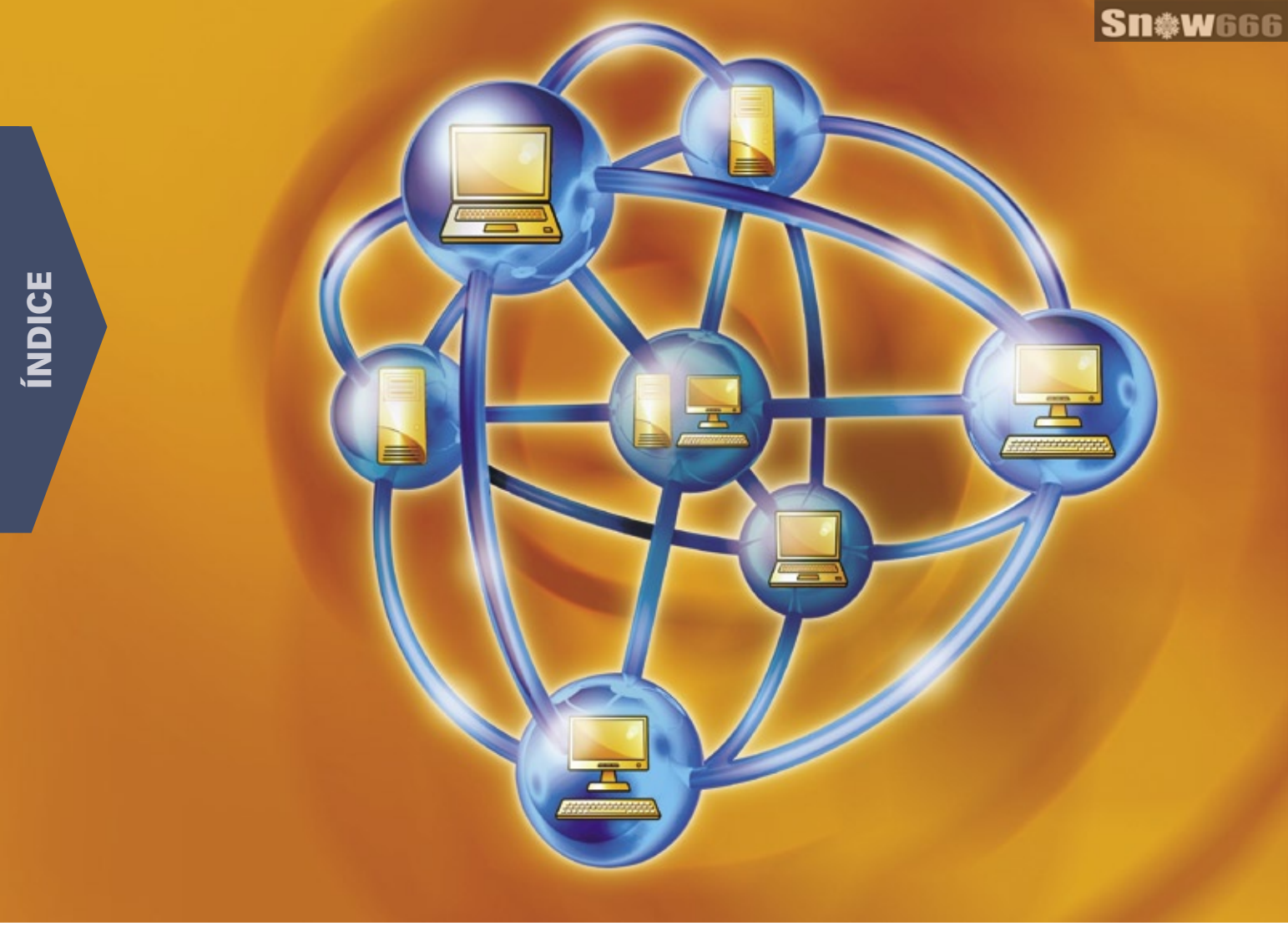
A surpresa, aqui, é ver o SL/CA embarcado num produto de consumo de massa, no qual ele fornece a base da interação com o usuário, provavelmente não técnico. Isso é diferente, por exemplo, dos dispositivos que utilizam um kernel Linux e, quando muito, alguns programas de Código Aberto na interação com o usuário. No EeePC, tudo o que se vê é de Código Aberto.

Nesse aspecto, é importante também salientar a rápida providência para sanar o problema de violação da GPL, tomada pela Asus ao disponibilizar, em pouco tempo, os trechos de código-fonte alterado incluídos no sistema operacional que equipa o EeePC.

E é assim que o Linux chega às massas. Numa ponta, partindo da ampla adoção em nichos específicos, como a computação de alto desempenho e os servidores web e de email. Na outra, ocupando uma fatia cada vez maior do mercado de sistemas embarcados, como telefones celulares e *Internet tablets*.

Se 2007 foi ou não o tão desejado "ano do Linux no desktop", não sei dizer. Mas parece que em dezembro tivemos o primeiro natal do Linux no notebook. ■

Pablo Hess
Editor



CAPA

COLUNAS

NOTÍCIAS

CORPORATE

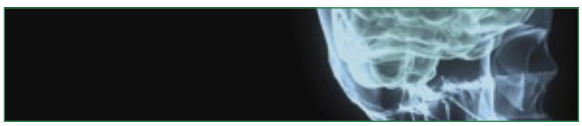
Tutorial

REDES

SEGURANÇA

ANÁLISE

PROGRAMAÇÃO



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 volume de correspondência, é 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.*

✎ Usuários de desktop

Tenho acompanhado a Linux Magazine desde seu lançamento, e tenho todos os números guardados, mas sinto falta de alguns artigos direcionados para desktops.

Apesar do lançamento da Easy Linux, que trata diretamente sobre o assunto, e que talvez seja o motivo para a Linux Magazine ter sido direcionada para o público corporativo, a revista citada acima não é mais encontrada nas bancas, deixando uma lacuna para os usuários domésticos da revista.

Creio que seria interessante algumas coisas mais, além das colunas já consagradas do Augusto, Charly, Klaus, Zack e Pablo (este último mais recentemente), pois as colunas do Edgar e Cezar são puramente corporativas, sendo interessantes para o leitor mediano apenas em partes.

Já que, pelo que me parece, a Easy Linux não mais deve ser editada, fica aqui meu pedido de ajustes na Linux Magazine, a fim de que, mais uma vez, não fiquemos órfãos de literatura apropriada para aqueles que simplesmente usam o Linux em suas casas pelo simples prazer de ter nas mãos um sistema robusto, livre das pragas digitais que assolam o sistema dominante, e para sentir a liberdade de instalar um software disponível, sem a necessidade de buscar os programas em sites de terceiros.

Ademais, parabéns por mais um ano de vida.

Saudações e recomendações,

Carlos Wagner

Resposta

Prezado Carlos, em primeiro lugar, muito obrigado pelos parabéns. De fato a Linux Magazine vem sendo progressivamente direcionada aos usuários técnicos e corporativos, como indica o novo slogan, "A revista do profissional de TI". Essa decisão foi tomada concomitantemente ao início da produção regular da Easy Linux, no início de 2006, que passou, então, a ser direcionada aos usuários domésticos e entusiastas de Linux.

Nosso desejo não é, nem jamais foi, eliminar a Easy Linux. A revista foi suspensa para reestruturação e reformulação de seu modelo de negócio, e tão logo esse objetivo seja atingido, a revista voltará a ser publicada no Brasil.

Esperamos sinceramente que isso aconteça o mais breve possível, e humildemente pedimos desculpas pela interrupção em nossa publicação. ■

Sua Revenda de Hospedagem já encheu?

A melhor hospedagem do Brasil agora com a melhor revenda Linux e Windows.

PLANOS DE REVENDA PLUGIN (com domínios ilimitados)

LINUX	Espaço em Disco	Taxa de Transf.	E-mails	BD My-SQL	Preço
PREMIUM *Páginas em PHP*	10 GB	250 GB	700 un.	80 un.	**R$ 500,00**

WINDOWS	Espaço em Disco	Taxa de Transf.	E-mails	BD Access	BD MS-SQL	Preço
STANDARD	500 MB	10 GB	40 un.	4 un.	2 un.	**R$ 98,00**
PREMIUM *Páginas em ASP*	10 GB	250 GB	700 un.	80 un.	40 un.	**R$ 800,00**

MISTA	Espaço em Disco	Taxa de Transf.	E-mails	BD Access	BD MS-SQL	BD My-SQL	Preço
STANDARD	1 GB	25 GB	70 un.	8 un.	4 un.	8 un.	**R$ 170,00**
PREMIUM *Páginas em ASP e PHP*	10 GB	250 GB	700 un.	80 un.	40 un.	80 un.	**R$ 890,00**

Planos intermediários consulte www.plugin.com.br

A Plug In tem vários motivos para ser a sua nova revenda de hospedagem: além de ter os pacotes mais atrativos do mercado, possui um grande diferencial, que é ter os serviços (sites, e-mail, base de dados e painel de controle) em servidores independentes, isso faz com que a Plug In garanta 99,9% de UPtime em suas aplicações de internet.

Contrate agora mesmo uma Revenda Plug In e abra espaço para novos clientes.

- *Revenda* - Linux e Windows
- *Streaming* - Conexões Ilimitadas
- *E-mail Marketing* - Ações Segmentadas

Ligue e contrate:
4003-1001

Contrate online:
www.plugin.com.br

Powered by UOL O MELHOR CONTEÚDO

Plugin

COLUNA

O que aprendi na aula de Biologia

Augusto Campos

Como lidar com a explosão de popularidade do Ubuntu, preservando a diversidade de distribuições.

por Augusto Campos

Nas aulas de Biologia, todos aprendemos sobre a importância da diversidade genética para o sucesso continuado de qualquer espécie e sobre os perigos associados à ausência dela. O professor de Sociologia também recorria a esse mesmo argumento para ajudar a explicar a decadência de dinastias ou grupos sociais que adotavam o costume de casar-se apenas ou principalmente entre si, eliminando assim a necessária diversidade. Nenhum geek, mesmo que tenha faltado a todas as aulas de Biologia, ignora o assunto, abordado até em um episódio (o segundo da quarta temporada) da série cult *Arquivo X*.

Mercados equilibrados também apresentam diversidade, e tanto para o consumidor quanto para a cadeia de valor é sempre mais saudável que haja diversidade do que concentração de opções.

Mesmo assim, estamos em um momento curioso: se as tendências permanecerem constantes, provavelmente logo teremos uma distribuição comunitária de Linux assumindo a posição de líder inconteste, sendo vista até mesmo como sinônimo de Linux no desktop.

Eu vejo vários aspectos positivos nisso, e certamente é mérito dos envolvidos na distribuição, por saber o que fazer para atingir uma fatia cada vez maior dos usuários e interessados em Linux no desktop. Sob o ponto de vista do crescimento do Linux no mercado, a consolidação também é positiva, mas creio que seria mais vantajosa se houvesse a dominância de dois ou três fornecedores, e não de apenas um. E note que não estou me referindo ao desktop corporativo, e sim ao meu e ao seu.

Infelizmente, não dispomos de grande riqueza estatística nos dados históricos que podem ser consultados publicamente. Mas a reflexão pode partir até mesmo da pouca informação isenta que se pode obter – uma das minhas preferidas é a do Google Trends, que mostra a popularidade das buscas por determinados temas ao longo dos anos. Visite e compare o interesse despertado pelas principais distribuições em anos recentes.

Outra fonte para análise é a pesquisa dos Favoritos da Comunidade Linux Brasileira, que promovo anualmente no BR-Linux.org[1]. Até 2005, havia alternância entre os vencedores na categoria *Distribuição desktop*, que obtinham sempre menos de 25% dos votos totais. Mas no final de 2005 foi lançado o Ubuntu, e a partir daí ele sempre ganhou – e em 2007 obteve a primeira maioria absoluta nessa categoria.

Tenho algo contra o Ubuntu? Não, pelo contrário. Aprecio e uso diariamente. Mas tenho visto cada vez mais reações por parte dos entusiastas das distribuições cujo percentual de participação está se reduzindo, e noto que essas reações freqüentemente apontam para o lado errado e impedem sua efetividade.

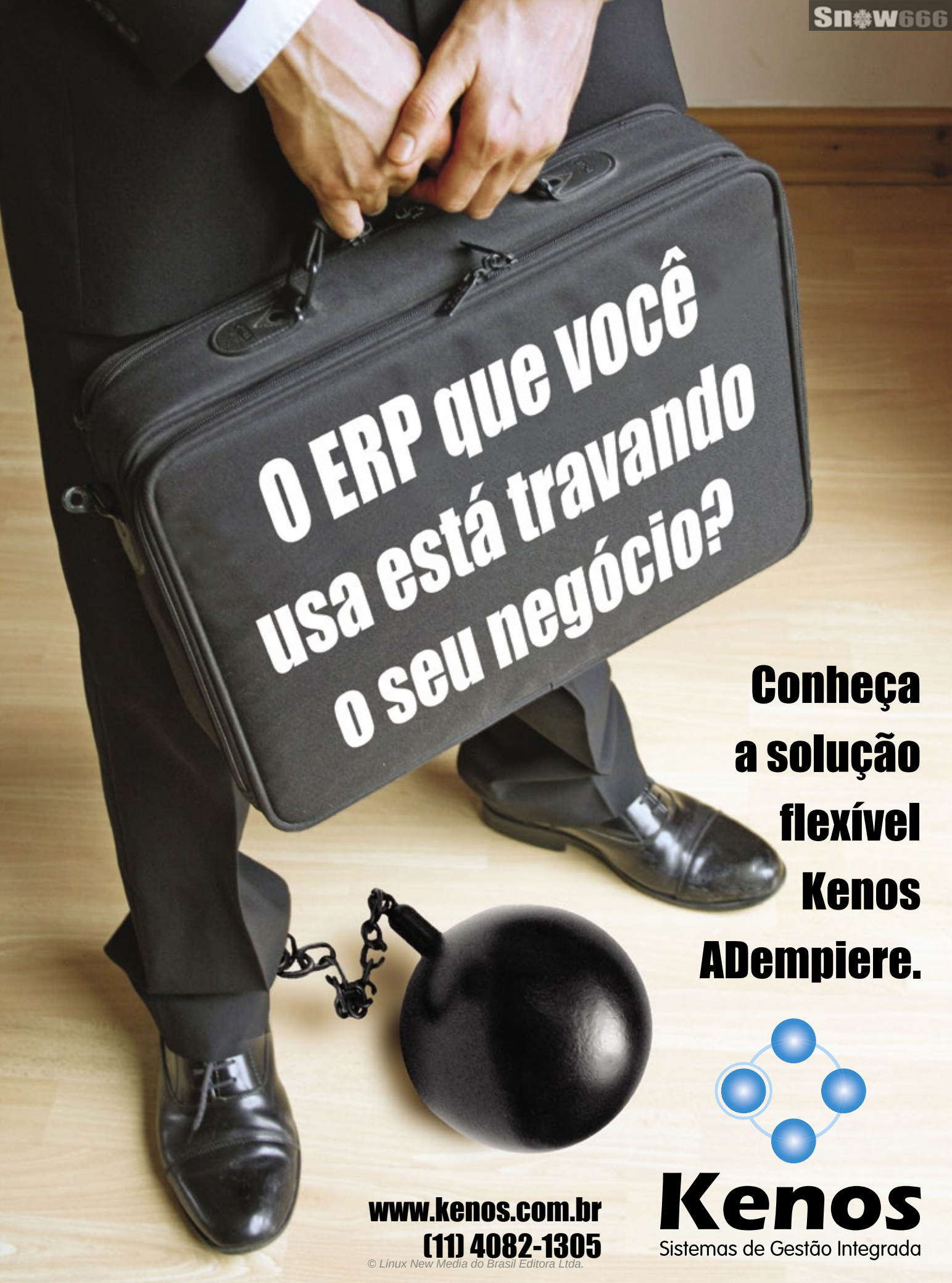
Fica, portanto, a minha dica: no meu entender, para reagir a essa expansão de uma forma que todos ganhem, é necessário promover e divulgar o uso de outras distribuições – e não fazer o oposto, que é combater ou criticar o sucesso da distribuição mais popular. Diversidade é bom, mas já temos adversários suficientes; não precisamos criar disputas adicionais entre nós mesmos. ■

Mais informações

[1] BR-Linux.org: http://www.br-linux.org/

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.



Conheça a solução flexível Kenos ADempiere.

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

Kenos
Sistemas de Gestão Integrada

COLUNA

Munin

Charly Kühnast

O verdadeiro cleptomaníaco entre as aves é o corvo. É bom os detentores dos dados conhecerem o Munin, uma ferramenta de monitoramento que homenageia um famoso corvo.

por Charly Kühnast

Desde que nos lembramos, os humanos convivem com animais domésticos. O deus nórdico Odin tinha um cavalo chamado Sleipnir, dois lobos, com os nomes Geri e Freki ("glutão" e "ganancioso"), e os corvos Hugin e Munin. Odin enviava os corvos para o mundo toda manhã, e à noite eles retornavam para relatar o que haviam observado – um tipo de *news ticker* primitivo, alado e com penas.

Memória

Enquanto Hugin representa o poder da imaginação e da fantasia, Munin significa memória, que é um nome apropriado para um software que coleta, processa e arquiva dados do sistema. O Munin[1] possui dois componentes: um servidor e vários nós. O software de cada nó coleta os dados a respeito de sua própria máquina e os serviços nela instalados.

O servidor obtém os dados periodicamente, e usa o *RRDtool* para processar os dados e gerar gráficos detalhados como o exibido na **figura 1**.

Configurando a ave

O minúsculo arquivo de configuração do servidor, `/etc/munin/munin.conf`, é semelhante a:

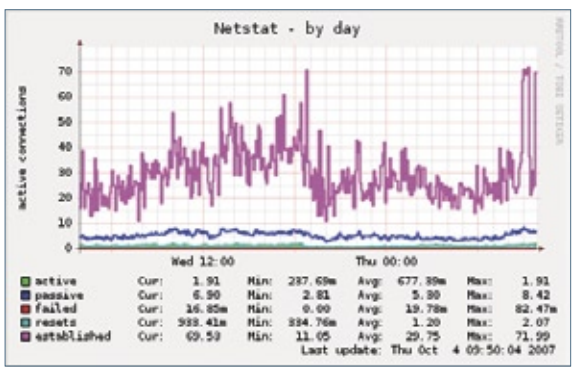


Figura 1 O servidor do *Munin* agrupa dados de sistema coletados dos nós, e usa a *RRDtool* para gerar a visualização.

```
dbdir   /var/lib/munin
htmldir /var/www/munin
logdir  /var/log/munin
rundir  /var/run/munin

[gw.kuehnast.com]
address 192.168.0.127
```

Esse exemplo possui somente um nó, *gw.kuehnast.com*. A configuração dos nós é bastante exaustiva, mas os padrões são muito úteis. Alterei apenas o usuário e as configurações de grupo:

```
user root
group root
setsid yes
```

É claro que é necessário permitir que o servidor acesse a porta 4949 do Munin, `allow ^192\.168\.0\.42$`. Mas como o Munin sabe quais serviços e estados de sistema devem ter seus dados coletados?

Nesse sentido, o software segue o exemplo de seu amigo emplumado – simplesmente relata tudo que acontece lá no grande mundo exterior, ou ao menos em seus próprios nós.

Antes de começar a alimentar seus amigos voadores, talvez seja uma boa idéia ler as FAQs do Munin, que mostram exemplos e respostas específicos a respeito de gráficos, plugins, configurações do servidor e outros. ■

Mais informações

[1] Munin: http://munin.projects.linpro.no

Sobre o autor

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

Guia de TI

Soluções em Tecnologias Abertas

LINUX NEW MEDIA
The Pulse of Open Source

Garanta já sua vaga para o Guia de TI 2008!

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

Assinatura:
11 4082-1300
assinatura@linuxnewmedia.com.br

COLUNA

Pergunte ao Klaus!

Klaus Knopper

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

por Klaus Knopper

NDISwrapper

Tenho um laptop antigo que gostaria de usar para navegar sem fio na Internet. Instalei o *Debian Etch* recentemente. O laptopt não tem uma placa de rede. Eu gostaria de usar o *NDISwrapper* para fazer funcionar um adaptador de rede sem fio USB Belkin.

Não uso Linux em desktops há muito tempo, e não sei como fazer isso. Eu agradeceria se você pudesse me dizer como instalar o NDISwrapper e pôr tudo para funcionar. Atualmente estou acessando a Internet por um PC com Windows® XP.

Resposta

O NDISwrapper é uma extensão do kernel Linux que permite o carregamento de um driver de rede do Windows como se fosse um módulo do kernel Linux. Com isso, é possível oferecer suporte a adaptadores de rede que não possuam suporte nativo no kernel Linux.

Os iniciantes enfrentam alguns obstáculos porque as extensões do kernel, como módulos, exigem conhecimentos básicos sobre o funcionamento do sistema operacional, e precisam que o código-fonte do kernel e o compilador C estejam instalados corretamente. Portanto, não posso prometer que as instruções a seguir vão funcionar precisamente caso você jamais tenha instalado um módulo do kernel ou trabalhado na linha de comando. Uma solução melhor seria instalar uma versão do kernel mais recente que suporte o adaptador de rede nativamente (com um driver do Linux, em vez de um driver para Windows com o NDISwrapper).

Se seu desejo for experimentar o NDISwrapper, as instruções abaixo devem ajudá-lo. Nesse exemplo, parto do princípio de que o pacote com o código-fonte do NDISwrapper, `ndiswrapper-1.49.tar.gz`, e o driver da sua placa de rede para Windows, `meudriver.inf`, estejam presentes numa partição do disco rígido ou em um pendrive montado em `/media/sdb1/`..

Obtenha o código-fonte mais recente do NDISwrapper em http://ndiswrapper.sourceforge.net/, normalmente distribuído como um arquivo compactado. Para resolver o problema de "ovo ou galinha", provavelmente será necessário outro computador para fazer o download, ou então você pode inicializar outro sistema operacional que já possua um driver funcional para a rede sem fio. Salve o arquivo baixado num pendrive ou numa partição do disco rígido que seja acessível a partir do Linux.

Após entrar no Linux, descompacte o código-fonte do NDISwrapper no diretório `home` do usuário e compile com o `make` o módulo do NDISwrapper. (Para isso funcionar, os fontes do kernel referentes ao kernel em execução precisam estar instalados).

Instale o módulo e seus utilitários com o comando `make install` (como root).

Entre no diretório onde estão os arquivos do driver para Windows (`cd /media/sdb1`, em meu exemplo) e carregue-os (novamente como root):

```
ndiswrapper -i minhaplaca.inf
```

Se o driver para Windows demandar outros arquivos de driver (`algo.sys` e possivelmente `firmware.bin`), eles precisarão estar presentes no mesmo diretório.

Com `ndiswrapper -l`, verifique se funcionou. A resposta deve ser: `driver present, hardware present`.

Carregue o módulo do NDISwrapper, caso ainda não o tenha feito (novamente como root):

```
modprobe ndiswrapper
```

Ao digitar `/sbin/ifconfig -a`, agora o adaptador deve aparecer como *wifio*. Pode-se configurá-lo com as ferramentas para redes sem fio fornecidas pela distribuição usada. ■

Sobre o autor

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

nova regra do mercado

dividir para multiplicar

DO BANCO DE DADOS À INTERFACE, O SOFTWARE LIVRE DO GOVERNO DO PARANÁ ESTÁ MULTIPLICANDO RESULTADOS

Independência tecnológica. Confiança. Segurança. Evolução permanente. Codificação auditável. Protocolos confiáveis. Sistemas robustos e escaláveis. Ampla rede de suporte técnico. Interoperabilidade. Personalização. Racionalização de custos.

Quando resolveu apostar no software livre o Governo do Paraná sabia o que estava fazendo. A parceria com a comunidade software livre tem produzido resultados de alto impacto social e econômico.

Do banco de dados à interface gráfica, as ferramentas e aplicações de código aberto utilizadas pela CELEPAR - Informática do Paraná estão multiplicando as soluções de TI no ambiente de governo e na sociedade. Avanços que são divididos com a comunidade através da liberação dos códigos fonte.

Compartilhar conhecimentos e somar esforços. Esta é a regra que o Paraná usa para crescer e criar oportunidades.

QUEM CONHECE, SABE. QUEM NÃO CONHECE, PRECISA VER.

Veja alguns exemplos das soluções desenvolvidas pela Celepar:

EXPRESSO sistema integrado de correio eletrônico, agenda, fluxos de trabalhos (workflow) e catálogos. Permite o compartilhamento e a busca de informações corporativas, independente da plataforma ou de limites geográficos, técnicos ou organizacionais.

PLATAFORMA PARANÁ (framework) conjunto de ferramentas, métodos e padrões para a produção de sistemas. Maior produtividade com arquitetura tecnológica pré-definida, organização de acervos e reutilização de componentes.

HABILITAÇÃO E VEÍCULOS (DETRAN-PR) sistemas de alta complexidade que gerenciam os processos de expedição, renovação, multas, pontos e situação de 3,5 milhões de condutores e igual número de veículos.

XOOPS - eXtensible Object Oriented Portal System, ferramenta dinâmica e interativa para a criação de portais, comunidade virtuais, sítios de notícias, intranets e weblogs de pequena e grande escala.

DIA-A-DIA EDUCAÇÃO portal colaborativo com recursos didáticos, banco de imagens, dicionários, sons e vídeos, tradutores e links desejáveis. Possui área para publicação de conteúdos e pesquisas nas diversas áreas do conhecimento.

Software Livre: o Paraná usa e abusa

*A Licença Pública Geral para a Adminsitração Pública é um decreto governamental que permite e dá cobertura legal para o uso, distribuição, adaptação, e distribuição de todos os softwares produzidos pelo Governo do Estado do Paraná.

central@celepar.pr.gov.br 55(41) 3350-5000 www.celepar.pr.gov.br

GOVERNO DO PARANÁ

COLUNA

Crônicas do kernel

Zack Brown

Empresas desenvolvem o kernel, enquanto programadores eliminam grande quantidade de lixo. Mas não sem dificuldades.

por Zack Brown

Trabalho com Linux?

Algumas pessoas têm se interessado em encontrar empregos em empresas para desenvolver o Linux, ou então em descobrir outras formas de se envolver nisso profissionalmente. Ao longo de um debate, na lista de discussão do kernel, Greg Kroah-Hartman postou suas estimativas da participação das empresas no desenvolvimento do kernel: http://lkml.org/lkml/2007/10/14/241.

As cinco principais empresas no desenvolvimento do Linux, segundo a lista feita por Greg, são um tanto previsíveis: Red Hat, IBM, Linux Foundation, Novell e Intel.

Padrões de código

Recentemente, alguns desenvolvedores começaram a aumentar o tamanho do arquivo `CodingStyle` para incluir boas práticas e recomendações para a escrita de código legível. Isso levou a um debate em que Linus Torvalds deixou claro que não queria forçar um padrão rigoroso em áreas nas quais houvesse espaço para individualidade. Ele queria que o `CodingStyle` fosse o menor possível, e contivesse apenas as grandes questões, como a obrigatoriedade da indentação correta. Outros aspectos, como a idéia de que não se deve usar parênteses em `printk()`, são considerados problemas menores de estilo que não devem ser exigidos de ninguém. Na verdade, ele já considera o arquivo `CodingStyle` atual preocupado demais com detalhes, quando seu propósito deveria ser explicar princípios mais gerais.

Alexander Viro também levantou a questão de que não importa quão draconianas fiquem as diretrizes de estilo de código, sempre será possível alguém aderir a elas estritamente e ainda conseguir escrever código ruim ou feio.

Os que apoiavam o arquivo `CodingStyle` expandido agora estão trabalhando num documento anexo que contenha apenas sugestões, e então o `CodingStyle` poderá focar-se no que deve ser obrigatório no kernel. Linus está de acordo com essa solução, contanto que os scripts usados para verificar erros de estilo nos *patches* enviados não acabe incomodando seus autores com infrações menores.

Remoção de código

Graças a Adrian Bunk, sempre há muito código saindo do kernel, e quando outros tentam retirá-los, geralmente descobrem que Adrian já esteve lá. Por exemplo, Robert P. J. Day recentemente tentou eliminar alguns códigos de suporte a *APUS* da arquitetura PowerPC; Adrian disse que já possuía um patch aguardando na fila.

O código de APUS já está listado como defeituoso há mais de dois anos, e alguns códigos de APUS foram eliminados no kernel 2.6.23. Robert havia descoberto os pedaços restantes através de um script feito por ele mesmo, que identifica segmentos de código mortos nos fontes do kernel.

Adrian ainda tentou mais uma vez livrar o kernel do driver *eepro100*. Esse driver foi substituído há muito tempo pelo *e100* e foi marcado para eliminação, mas como explicaram Jeff Garzik e Auke Kok antes, o e100 ainda tem problemas que dificultam a troca pelo eepro100.

Além disso, David Acker, que está trabalhando em melhorias no driver e100, precisou dedicar sua atenção a vários outros projetos, o que reduziu seus esforços no e100. Para piorar, algumas falhas do e100 são difíceis de testar, o que torna o processo inteiro ainda mais lento. Em virtude da vontade coletiva de eliminar o driver eepro100, no entanto, David disse que fará seu melhor para cumprir o prometido. Porém, por enquanto, o código de Adrian ainda precisará esperar. ■

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.

Coleção Pocket Pro já nas bancas!

A coleção Linux Pocket Pro é um lançamento da Linux New Media do Brasil, responsável pela publicação da conceituada revista Linux Magazine, especializada em Código Aberto e no universo do profissional de TI. O objetivo da coleção é trazer conhecimento confiável e de alto nível técnico para estudantes, técnicos e até mesmo administradores de sistemas experientes, sempre com enfoque prático e voltado para a utilização do sistema Linux e de outras tecnologias livres, hoje utilizadas ou reconhecidas como altamente competitivas por milhares de empresas, incluindo gigantes como IBM, Apple, Banco do Brasil, Casa Bahia e Microsoft.

LINUX NEW MEDIA
The Pulse of Open Source

Mais informações:
Site: www.linuxmagazine.com.br
Tel: 11 - 4082-1300

LINUX MAGAZINE

Mono

O *Mono* oferece o software necessário ao desenvolvimento e à execução de aplicativos *.NET* clientes e servidores em várias plataformas. A implementação *BigInteger* do Mono contém uma vulnerabilidade de estouro de *buffer* que poderia levar à execução de código arbitrário.

Um agressor remoto poderia explorar essa vulnerabilidade enviando dados especialmente criados a aplicativos Mono que usem a classe `BigInteger`, o que poderia acarretar a execução de código arbitrário sob os privilégios do usuário que estivesse rodando o aplicativo (possivelmente root), ou uma negação de serviço. (**CVE-2007-5197**) ■

Debian: DSA-1397
Gentoo: GLSA 200711-10
SUSE: SUSE-SR:2007:023

SiteBar

O *SiteBar* é um aplicativo em *PHP* que permite aos usuários armazenar suas páginas web favoritas num servidor web. Foram identificadas no SiteBar múltiplas falhas que poderiam permitir a execução de código arbitrário e a revelação de arquivos arbitrários. O módulo de tradução não trata corretamente o valor do parâmetro `dir`. (**CVE-2007-5491**, **CVE-2007-5694**) O módulo de tradução também não cuida dos valores de `edit` e `value` que ele passa para as funções `eval()` e `include()`. (**CVE-2007-5492**, **CVE-2007-5693**)

O comando de login não valida a URL à qual os usuários são redirecionados após o registro. (**CVE-2007-5695**)

O SiteBar contém ainda várias vulnerabilidades do tipo *cross-site scripting*. (**CVE-2007-5692**) ■

Gentoo: GLSA 200711-05

OpenSSL

Um erro do tipo *off-by-one* na implementação de *DTLS* do *OpenSSL* 0.9.8 anterior à versão 0.9.8f permite que agressores executem códigos arbitrários através de vetores não especificados. (**CVE-2007-4995**) ■

Fedora: Fedora-2007-725
Gentoo: GLSA 200710-30
Red Hat: RHSA-2007:0964
SUSE: SUSE-SR:2007:021
Ubuntu: USN-534-1

zope-cmfplone

O *Plone*, nas versões de 2.5 a 2.5.4, e 3.0 a 3.0.2, permite que agressores remotos executem código *Python* arbitrário através de dados de rede contendo

Postura das principais distribuições Linux quanto à segurança

Distribuição	Referência de Segurança	Comentários
Debian	Info: www.debian.org/security Lista: lists.debian.org/debian-security-announce Referência: DSA-... 1	Alertas de segurança recentes são colocados na homepage e distribuídos como arquivos *HTML* com links para os patches. O anúncio também contém uma referência à lista de discussão.
Gentoo	Info: www.gentoo.org/security/en/glsa Fórum: forums.gentoo.org Lista: www.gentoo.org/main/en/lists.xml Referência: GLSA: ... 1	Os alertas de segurança são listados no site de segurança da distribuição, com link na homepage. São distribuídos como páginas HTML e mostram os comandos necessários para baixar versões corrigidas dos softwares afetados.
Mandriva	Info: www.mandriva.com/security Lista: www1.mandrdrivalinux.com/en/flists.php3#2security Referência: MDKSA-... 1	A Mandriva tem seu próprio site sobre segurança. Entre outras coisas, inclui alertas e referência a listas de discussão. Os alertas são arquivos HTML, mas não há links para os patches.
Red Hat	Info: www.redhat.com/errata Lista: www.redhat.com/mailing-lists Referência: RHSA-... 1	A Red Hat classifica os alertas de segurança como "Erratas". Problemas com cada versão do Red Hat Linux são agrupados. Os alertas são distribuídos na forma de páginas HTML com links para os patches.
Slackware	Info: www.slackware.com/security Lista: www.slackware.com/lists (slackware-security) Referência: [slackware-security] ... 1	A página principal contém links para os arquivos da lista de discussão sobre segurança. Nenhuma informação adicional sobre segurança no *Slackware* está disponível.
Suse	Info: www.novell.com/linux/security Lista: www.novell.com/linux/download/updates Referência: suse-security-announce Referência: SUSE-SA ... 1	Após mudanças no site, não há mais um link para a página sobre segurança, contendo informações sobre a lista de discussão e os alertas. Patches de segurança para cada versão do *Suse* são mostrados em vermelho na página de atualizações. Uma curta descrição da vulnerabilidade corrigida pelo patch é fornecida.
Ubuntu	Ubuntu Info: www.ubuntu.com/usn Lista: lists.ubuntu.com/mailman/listinfo/ubuntu-security-announce Referência: USN-... 1 |	O *Ubuntu*, baseado no Debian, mantém um sistema de atualizações de segurança independente. Muitas notas do Debian podem ser aplicadas também ao Ubuntu. |

1 Todas as distribuições indicam, no assunto da mensagem, que o tema é segurança.

objetos *pickled* para as mensagens de status ou para o módulo *linkintegrity*, no qual o módulo faz um *unpickle* e executa. (**CVE-2007-5741**) ■
Debian: DSA-1405-1

phpMyAdmin

Várias vulnerabilidades foram encontradas no *phpMyAdmin*, um aplicativo que administra o *MySQL* pela *Web*. O phpMyAdmin permite que um agressor remoto injete um script web ou HTML no contexto da sessão de um usuário logado (*cross-site scripting*). (**CVE-2007-5589**)

Quando acessado por um navegador que não codifica as requisições na URL, o phpMyAdmin permite que agressores remotos injetem scripts web ou HTML arbitrários através da cadeia de consulta. (**CVE-2007-5386**) ■
Debian: DSA-1403-1

Nagios Plugins

Duas vulnerabilidades de estouro de buffer no pacote *Nagios Plugins* podem permitir a execução remota de código arbitrário. O Nagios Plugins é um conjunto oficial de plugins para o *Nagios*, um programa de Código Aberto para monitoramento de máquinas, serviços e rede.

Um erro de verificação de limites no plugin *check_snmp*, ao processar respostas *GET SNMP* pode levar a um estouro de buffer baseado na pilha. (**CVE-2007-5623**) Um erro de verificação de limites na função `redir()` do plugin *check_http* ao processar informações do cabeçalho `Location:` HTTP pode levar a um estouro de buffer. (**CVE-2007-5198**) ■
Gentoo: GLSA 200711-11

Perl

Foi descoberta uma falha no mecanismo de expressões regulares de *Perl*. Uma entrada especialmente criada para uma expressão regular pode fazer o Perl alocar memória inadequadamente, resultando na possível execução de código arbitrário com as permissões do usuário que estiver executando o Perl. (**CVE-2007-5116**) ■
Debian: DSA-1400-1
Mandriva: MDKSA-2007:207
Red Hat: RHSA-2007:0966-5, RHSA-2007:1011-3

Kernel Linux

Um *underflow* de inteiros na função `ieee80211_rx` em `net/ieee80211/ieee80211_rx.c` no kernel Linux 2.6.x anterior à versão 2.6.23 permite que agressores remotos causem uma negação de serviço (travamento) através de um valor de comprimento *SKB* num quadro IEEE 802.11 quando a *flag* `IEEE80211_STYPE_QOS_DATA` está ativada. (**CVE-2007-4997**) ■
Debian: DSA-1381-2
SUSE: SUSE-SA:2007:059

Arquivos PDF

Várias falhas foram descobertas no uso de arquivos PDF, e poderiam afetar aplicativos como *CUPS*, *gpdf*, *Poppler*, *Xpdf* e *TeTex*. Um agressor poderia criar um arquivo PDF malicioso para fazer esses aplicativos fecharem ou potencialmente executarem código arbitrário ao serem abertos. (**CVE-2007-4352**, **CVE-2007-5392**, **CVE-2007-5393**)

Uma falha foi encontrada na forma como o CUPS lida com a negociação SSL. Um agressor remoto capaz de se conectar ao *daemon* do CUPS poderia fazê-lo fechar. (**CVE-2007-4045**)

Foi descoberta também uma falha na biblioteca *t1lib*, usada no tratamento de fontes *Type 1*. Um agressor poderia criar um arquivo malicioso que faria o TeTex fechar, ou potencialmente executar código arbitrário ao ser aberto. (**CVE-2007-4033**) ■
Red Hat: RHSA-2007:1023-01, RHSA-2007:1025-01, RHSA-2007:1026-01, RHSA-2007:1027-6, RHSA-2007:1031-01

PCRE

Múltiplos estouros de inteiros na biblioteca *Perl-Compatible Regular Expressions* (*PCRE*) anterior à versão 6.7 permitem que agressores dependentes do contexto executem código arbitrário através de uma expressão regular que contenha um grande número de subpadrões com nomes (`name_count`), nomes longos de subpadrões (`max_name_size`), um subpadrão repetido com um nome longo ou um vetor não especificado envolvendo as variáveis `max`, `min` e `duplength` no cálculo de comprimento de *pcre_compile*. (**CVE-2006-7224**) ■
Red Hat: RHSA-2007:1052-4

OpenLDAP

Foi descoberta uma falha na forma como o daemon *slapd* do *OpenLDAP* lida com atributos mal formados de *objectClasses* LDAP. Um agressor poderia criar uma requisição LDAP para causar uma negação de serviço pela parada do slapd. (**CVE-2007-5707**) ■
Mandriva: MDKSA-2007:215
Red Hat: RHSA-2007:1037-3

Rails 2.0

Após mais de um ano de desenvolvimento, finalmente foi lançado, em dezembro de 2007, a versão 2.0 do *framework* web *Rails*. Segundo o anúncio oficial, a nova versão inclui diversos novos recursos, correções de falhas e bastante polimento. Segmentos de código também foram retirados, no intuito de tornar "o pacote mais coerente e leve", de acordo com David, líder no desenvolvimento do sistema.

O Rails 2.0 traz diversas incompatibilidades com recursos da versão anterior, após um longo tempo de avisos de que tais recursos já se tornavam obsoletos.

Feito na linguagem *Ruby*, com a qual compõe o sistema Ruby on Rails, o pacote recebeu grande atenção dos desenvolvedores web quando de seu lançamento, inspirando, inclusive, programadores de diversas outras linguagens a desenvolverem soluções semelhantes. ■

Novos centros de treinamento RH

A Red Hat inaugurou no final de 2007 novos centros de treinamento para atender o aquecido mercado de tecnologia. Os novos parceiros da empresa ministrarão os cursos nas cidades de Belo Horizonte, Brasília, Porto Alegre e Rio de Janeiro. Além desses centros, a Red Hat conta com seu próprio centro de treinamento e um parceiro, ambos na cidade de São Paulo.

"O mercado Linux no Brasil e na América Latina está em franca expansão e esperamos que a demanda por treinamento continue aumentando em toda a região", afirmou Mariano Fernandez, gerente regional de serviços da Red Hat para a América Latina e responsável pela área de treinamento. "Nossos novos parceiros de treinamento nos ajudarão a prover um melhor treinamento aos profissionais de Linux e expandir o entendimento e adoção da tecnologia de Código Aberto no Brasil".

Os cursos ministrados pelos parceiros abrangem desde o servidor de aplicações Java *JBoss* até aspectos específicos das distribuições Red Hat Enterprise Linux, como administração do sistema, implementação em empresas, desenvolvimento e segurança, e também as certificações da empresa, RHCE, RHCT e RHCA. ■

OpenVZ sobre Xen?

Máquinas virtuais dentro de máquinas virtuais. Isso é possível há tempos. Mas uma novidade é a liberação, pela equipe de desenvolvimento da tecnologia *OpenVZ*, de um kernel 2.6.18 para o Red Hat Enterprise Linux. Essa versão contém, além dos *patches* do OpenVZ, as alterações para viabilizar o funcionamento do *Xen*.

É muito interessante a possibilidade de se executar múltiplos sistemas sobre o OpenVZ numa máquina virtualizada sobre Xen, justamente por tratarem-se de tecnologias de virtualização radicalmente diferentes. Enquanto o Xen emprega a abordagem de controle das máquinas virtuais por um *hypervisor*, o OpenVZ compartilha um único kernel Linux por múltiplos aplicativos de espaço do usuário – como se fossem vários sistemas Linux rodando em paralelo sobre um único kernel.

Além do RHEL, o *Debian* também dispõe de versões do kernel com ambos os patches integrados, permitindo a mesma funcionalidade. ■

Criptografia no Windows quebrável

Pesquisadores da Universidade de Haifa, em Israel, descobriram uma séria falha de segurança no gerador de números pseudo-aleatórios do Windows. Ao descobrirem como funciona a geração desses números, os pesquisadores foram capazes de prever números passados e futuros que serviriam para a criação de chaves criptográficas, entre outros usos.

O uso de chaves criptográficas que possam ser descobertas põe em xeque toda a segurança derivada do uso de criptografia, uma vez que o usuário crê estar protegendo seus dados de olhos maliciosos quando na realidade o eventual agressor tem acesso integral aos dados trafegados.

O sistema investigado foi o Windows 2000, mas os pesquisadores presumem que o mesmo código tenha sido empregado nas versões seguintes do sistema, como Windows XP e Vista. A conclusão dos pesquisadores é de que a Microsoft precisa melhorar a forma como criptografa as informações, e que a liberação do código-fonte do gerador de números pseudo-aleatórios – associado ao código de outros segmentos relacionados à segurança – permitiria que especialistas em segurança externos à empresa implementassem tais melhorias no código. ■

Google pagará secundaristas

Seguindo o estrondoso sucesso das edições do Google Summer of Code, nas quais programadores recebem da gigante das buscas e anúncios online uma quantia para contribuírem no desenvolvimento de aplicativos de Código Aberto, agora os estudantes secundaristas também têm a chance de serem recompensados para desenvolver Software Livre.

Em comparação com o já tradicional Summer of Code, o Google Highly Open Participation Contest oferece um menor número de projetos e, em vez de salários temporários, premiações com camisas e outros objetos, incluindo pequenos prêmios em dinheiro. ■

SL nas escolas públicas

Corinto Meffe, gerente de inovações tecnológicas do Ministério do Planejamento, informou que o Governo Federal já começou a distribuir os 90 mil computadores equipados com Software Livre às escolas públicas. Somados às 50 mil máquinas já distribuídas, esses PCs devem ser distribuídos a escolas por todo o país, no intuito de promover e facilitar a inclusão digital dos alunos e também dos professores. ■

EeePC e a GPL

A variante comercial do laptop educativo Classmate PC da Intel, o EeePC, fabricado pela Asus, gerou polêmica no fim de 2007. Segundo um analista, o laptop necessita de drivers de dispositivos levemente alterados em relação ao código-fonte original. Porém, nem a fabricante do laptop nem a da distribuição, Xandros, haviam publicado as alterações realizadas sobre esse código-fonte, caracterizando uma violação da licença GPL.

Ao ser notificada a respeito da violação, a Asus procedeu à publicação do link para download dos códigos referidos em sua página de suporte. Em todo o ocorrido, chamou atenção a rapidez da resposta do fabricante. ■

Um ano do acordo MS-Novell

Em dezembro de 2007 Novell e Microsoft celebraram um ano da assinatura do acordo de cooperação entre as duas empresas. Seus objetivos iniciais, a colaboração na criação de uma conexão entre softwares proprietários e de Código Aberto, foram até superados, segundo anúncio da Novell à imprensa.

Jeff Jaffe, da Novell: "demanda por interoperabilidade".

As duas empresas "continuam enxergando uma importante demanda por interoperabilidade", informou o comunicado, "e mais tranqüilidade com relação a propriedade intelectual". Como forma de ampliação do acordo, as parceiras agora pretendem "criar um modelo de plataforma mista interligando Linux e Windows", com a meta de "ajudar deficientes a interagirem com computadores".

Jeff Jaffe, vice-presidente executivo e CTO da Novell, afirmou que, devido ao acordo, a fabricante do Suse Linux "está se tornando a melhor escolha de Linux para empresas integradas, resultado esse que se reflete no significativo crescimento das vendas".

Do outro lado, Bob Muglia, vice-presidente sênior da divisão de servidores e ferramentas da Microsoft, afirmou também: "Estamos muito interessados em trabalhar com a Novell para (...) ajudar um grande grupo de pessoas com deficiências no mundo todo a trabalhar com computadores".

Novos clientes

O anúncio comemorativo da Novell inclui também uma lista com 30 novos clientes – de setores diversos – que aderiram à solução conjunta proveniente do acordo, isto é, receberam da Microsoft certificados de três anos de suporte ao Suse Linux Enterprise Server.

A colaboração técnica nas áreas de virtualização, gerenciamento de padrões, diretórios, identidade e compatibilidade de documentos permanecem como parte importante do acordo. Em seus laboratórios conjuntos de interoperabilidade, nos EUA e na Alemanha, as duas vêm trabalhando para garantir a interoperabilidade do SLED 10 com as novas versões do Windows Server com uso do Xen. ■

Supercomputadores brasileiros

A francesa Bull, fornecedora de infraestrutura de TI, fechou com o Governo Federal a negociação para aquisição de dois supercomputadores. Cada uma das duas máquinas tem poder de processamento de 6,1 TFLOPS e é composta por 72 servidores Bull NovaScale com dois processadores Xeon quad-core, totalizando 576 núcleos, 1 TB de memória e 45 TB de espaço para armazenamento de dados.

Os supercomputadores estão sendo instalados nas Universidades Federais do Ceará (UFCE) e de Pernambuco (UFPE), e integram o Sistema Nacional de Processamento de Alto Desempenho (SINAPAD), que reúne centros (CENAPADS) de excelência em computação nas regiões Sul, Sudeste e Nordeste. Os dados processados pelo SINAPAD englobam áreas como simulação de reservatórios de petróleo, química computacional, oceanografia, recursos hídricos, clima e genômica.

Sobre a aquisição, Alberto Araújo, presidente da Bull no Brasil, afirmou: "Estamos muito orgulhosos pela Bull ter sido selecionada pelas Universidades Federais. Este negócio confirma que a Bull, responsável pelo desenvolvimento do mais poderoso Supercomputador da Europa, está pronta para desenvolver as melhores soluções de alto desempenho em todo o mundo, desde a Ásia até a América do Sul" ■

Processadores Power 6

No mesmo mês, a Bull apresentou também sua nova linha *Escala* de servidores *blade*. As novas supermáquinas vêm equipadas, em cada unidade, do modelo EL406B, com até dois processadores Power 6 de núcleo duplo e freqüência de 4 GHz. Esse modelo traz também um disco rígido SAS e duas portas Ethernet e conexões extras, como Ethernet 10 Gb, InfiniBand e Fiber Channel, podem ser adicionadas com placas opcionais.

Os sistemas operacionais oferecidos pelo fabricante são o AIX 6 e Linux. Além da oferta dos novos processadores Power 6, outro grande avanço nesses servidores blade é sua compatibilidade com chassis que comportam também servidores blade equipados com processadores x86. Isso significa que é possível unir, num mesmo chassi, as duas plataformas, da forma mais adequada ao processamento a ser realizado. ■

Valorização da Red Hat

A americana Red Hat, fabricante do Red Hat Enterprise Linux e da distribuição comunitária Fedora, foi eleita líder em satisfação na quarta edição do estudo intitulado "CIO Insight Vendor Value". Ziff Davis, autor do estudo, entrevistou 472 executivos de TI (mais da metade em cargos máximos de sua função) a respeito da confiança e do valor oferecidos pelos fornecedores de software, e mais uma vez a empresa de Raleigh ganhou a primeira colocação.

Este ano, além do ranking geral, a Red Hat ocupou o primeiro lugar em outras categorias da pesquisa, como satisfação do cliente e cumprimento de tempo e orçamento, por exemplo.

Nas três edições anteriores do estudo, a Red Hat ocupou a primeira posição em duas ocasiões, e em todos os estudos foi eleita como a empresa que oferece o maior valor entre os fornecedores de software. ■

Suporte para antivírus aberto

O sistema antivírus *ClamAV* é o mais utilizando dentre as alternativas de Código Aberto. No Brasil, até há pouco, ele não contava com suporte por nenhuma empresa. Porém, desde o final de novembro, a brasileira CLM Software mudou esse quadro, e passou a oferecer suporte de nível corporativo ao antivírus de Código Aberto.

A CLM é especializada em softwares de gestão de risco e segurança da informação, entre outras áreas, sendo também representante no Brasil da Sourcefire, que desenvolve o IDS/IPS *Snort* – também de Código Aberto – e que adquiriu o ClamAV em agosto de 2007.

Segundo a CLM, em 2008 devem começar a ser comercializados *appliances* contendo as soluções de segurança, como o Snort e as funcionalidades de antivírus, anti-spyware e anti-worms do ClamAV, sob a marca da Sourcefire. ■

SonicWALL com suporte a Linux

A SonicWALL, fabricante americana de soluções de segurança, anunciou o lançamento do produto SSL VPN para pequenas e médias empresas. O produto agora pode receber um módulo que permite acesso externo às máquinas gerenciadas por ele. O objetivo é possibilitar o suporte remoto, com o técnico acessando o computador sem precisar se deslocar até a máquina.

Outra importante novidade da versão 2.5 do firmware do SSL VPN é o suporte a sistemas Linux e Mac OS X. Com o SonicWALL Virtual Assist, o suporte técnico pode ser iniciado por qualquer um dos dois envolvidos: o usuário ou o técnico. O usuário pode enviar uma solicitação de suporte através do portal, ou o técnico pode indicar, por email, o link para o usuário acessar o portal e assim possibilitar o suporte remoto. ■

O mercado em 2008, segundo o IDC

O IDC divulgou suas previsões para o mercado global de TI no ano de 2008. Segundo o anúncio das previsões, os últimos anos foram marcados por inúmeros eventos disruptivos na área de TI, incluindo o desenvolvimento colaborativo de softwares, representado em grande parte pelo Software Livre e de Código Aberto. A atuação e o crescimento de empresas pouco convencionais no setor, como Google, Youtube e Facebook, também reforçam essa observação.

Em 2008, segundo o IDC, o mercado deve começar a entrar na fase chamada "pós-disrupção". Isso significa o estabelecimento e fortalecimento desses modelos e empresas até agora considerados heterodoxos, com representantes do mercado tradicional adotando as novas práticas. Evidentemente, isso inclui a abertura de modelos de negócios para a participação da comunidade, e também o crescimento dos investimentos para desenvolver esses modelos.

"O *status quo* está prestes a mudar", afirma Frank Gens, vice-presidente sênior de pesquisa do IDC. As tecnologias disruptivas serão o novo padrão e deixarão de receber essa denominação, enquanto mais e mais empresas adotarão os novos modelos de negócios e tecnologias. ■

Frank Gens, do IDC, afirma: "o *status quo* está prestes a mudar"

Entrevista com Marcelo Lombardo, Diretor de Tecnologia da NewAge Software

SOA sem suor

O CoreBuilder é um grande curinga no desenvolvimento de softwares para gestão empresarial. Conheça a visão de seu criador.

por Pablo Hess

A brasileira NewAge Software iniciou suas operações já em 1989. Em 1999, lançou o primeiro sistema *ERP* brasileiro em *Java*, e em 2002 criou o primeiro ERP em *.NET* da América Latina.

Com várias ofertas na área de gestão empresarial, a empresa desenvolve também sistemas especiais para alguns setores da indústria. Seu principal produto na área de desenvolvimento é o *CoreBuilder*, que, com o lema *Code once, run everywhere* (Programe uma vez, execute em qualquer lugar), possibilita o desenvolvimento de aplicativos para múltiplas plataformas sem necessidade de recompilação.

Figura 1 Marcelo Lombardo, Diretor de Tecnologia da NewAge Software.

Marcelo Lombardo, Diretor de Tecnologia da NewAge e criador do CoreBuilder, explica nesta entrevista de que forma esse sistema pode ajudar as empresas a adotarem SOA sem qualquer acréscimo de complexidade no desenvolvimento, manutenção ou portabilidade de seus sistemas mais críticos.

Linux Magazine» ***O que é o CoreBuilder, e quais as suas vantagens em relação a seus concorrentes?***

Marcelo Lombardo» O CoreBuilder é um *framework* de altíssima produtividade para o desenvolvimento de aplicações de gestão de negócio. Sua diferença básica em relação aos outros frameworks é isolar completamente a tecnologia das regras de negócio. Com isso, a "camada tecnológica" pode ser substituída sem necessidade de reescrever as regras de negócio, o que permite que sejam preservados os investimentos realizados no desenvolvimento contra rupturas tecnológicas.

> *O suporte ao Linux e a bancos de dados de Código Aberto fazem parte da linha mestre de nossa estratégia.*

LM» ***Como as tecnologias que formam a base do CoreBuilder o dife-***

renciam de um gerador de código-fonte comum?

ML» Nos últimos anos, as empresas desenvolvedoras de aplicativos vêm tendo a necessidade de escolher se vão entrar no mundo Microsoft – plataforma *.NET* – ou no mundo *Java*. Decisões como essa inevitavelmente levam a empresa a perder alguma fatia de mercado. A vantagem ao trabalhar com o CoreBuilder é que a aplicação é desenvolvida uma única vez, e no mesmo instante já pode ser executada em qualquer *front-end*, assim como em qualquer banco de dados do mercado, sem exigir a recompilação da aplicação.

O CoreBuilder se diferencia dos geradores de código-fonte por não necessitar de processos complexos de compilação e instalação. Uma vez criado um *form*, por exemplo, este já pode instantaneamente ser executado em Java, .NET ou *AJAX*. Além disso, nosso produto gerencia muito melhor as mudanças e trabalhos realizados por cada programador.

Em outras palavras, o CoreBuilder cuida não apenas do desenvolvimento do aplicativo, mas também gerencia o trabalho em equipe e a manutenção dos sistemas em ambiente de produção.

LM» ***Qual a importância estratégica de suportar o Linux e os bancos de dados de Código Aberto?***

ML» O suporte ao Linux e a bancos de dados de Código Aberto fazem parte da linha mestre de nossa estratégia, já que possuem a finalidade de disponibilizar soluções de baixo custo e alta confiabilidade. Prova disso é que cerca de 20% dos usuários finais dos aplicativos desenvolvidos já fazem sua instalação nessas plataformas abertas, ou estão migrando para elas.

Calculamos que existem hoje, em produção, aproximadamente 60 clientes nessa situação. Esse número engloba clientes de todos os portes, desde pequenas empresas até grandes redes de lojas com centenas de usuários simultâneos, fazendo uso de Linux tanto nos servidores quanto nas estações.

LM» ***Existe alguma plataforma preferida (entre Java e .NET) por seus clientes para a geração de seus softwares?***

ML» Existe uma clara preferência: percebemos que mais de 70% escolhem a plataforma Java, mesmo que seja em ambientes diferentes de Linux e mesmo que com bancos de dados de código fechado, como o *MSSQL Server*.

LM» ***De que forma a recente ênfase em SOA no Brasil pode ajudar a aumentar o uso de ferramentas como o CoreBuilder?***

ML» Ferramentas como o CoreBuilder assumem um papel decisivo nesse cenário de SOA, pois viabilizam o modelo na prática, já que as aplicações desenvolvidas podem rodar totalmente

> ***Nossa meta é que as software houses não fiquem dependendo da ferramenta de desenvolvimento ou do banco de dados da moda.***

Porém, nosso objetivo vai um pouco além desse fator. Nossa meta é que as software houses não fiquem dependendo da ferramenta de desenvolvimento ou do banco de dados da moda, e com isso seja possível minimizar os riscos no desenvolvimento de suas soluções.

LM» ***Quais as vantagens do modelo de negócios de software como serviço, adotado pelo CoreBuilder, com assinatura mensal, em comparação com o modelo de venda de licenças?***

ML» Na minha opinião, a maior vantagem é a segurança e não a simples redução de custos, como se costuma crer. É verdade que o custo total de propriedade no modelo *ASP* tende a ser menor que aquele visto no modelo tradicional. Porém, entendo que o tratamento profissional do gerenciamento do ambiente, do banco de dados, dos backups e da segurança dos dados garantem uma operação livre de falhas e sem preocupações de infraestrutura para o empresário.

desacompanhadas de um front-end. Isso é possível porque quaisquer componentes, sejam objetos ou forms, podem ser acessados como um *web service* automaticamente.

Acredito que, através da especialização das empresas produtoras de sistemas em setores específicos, podemos chegar ao tão sonhado *SOA Marketplace*, no qual aplicações – ou componentes, dependendo do caso – especializadas podem ser orquestradas por um *middleware* que automatiza as transações.

Entretanto, percebo que os aplicativos que estão sendo desenvolvidos no Brasil ainda tendem a ser preponderantemente monolíticos. Isso é negativo, pois esse mercado no futuro demandará granularidade, a qual não será atendida por sistemas monolíticos. Ainda há muito que aprender sobre SOA no Brasil. ■

Entrevista com Jean-Pierre Laisné, Presidente do OW2

Benefícios intercontinentais

O consórcio OW2 visa a desenvolver um middleware de Código Aberto e alta qualidade. Em sua visita ao Brasil, o presidente do OW2 nos explicou por que nosso país faz parte de sua estratégia para 2008.

por Pablo Hess

Linux Magazine» ***Como você descreveria o OW2? Qual seu propósito, e por que ele é importante para o mundo corporativo atualmente?***
Jean-Pierre Laisné» O OW2 descende da fusão entre a ObjectWeb e a OrientWare. A ObjectWeb foi fundada em 2002 por uma parceria entre o Instituto de Pesquisa em Informática da França (INRIA), a também francesa Bull e a France Telecom. Seu objetivo era desenvolver e abrigar um *middleware* de Código Aberto e distribuído, e antes da fusão, no fim de 2006, já havia alcançado relativo sucesso nisso. A chinesa OrientWare, mais recente, consistia também num consórcio de universidades e empresas chinesas, com o mesmo objetivo da ObjectWeb.

Figura 1 Jean-Pierre Laisné, Presidente do OW2

A união entre as duas iniciativas gerou o consórcio OW2, que agora engloba três continentes. A missão do OW2, portanto, permanece igual à de seus fundadores, e baseia-se na idéia de que o middleware deve ser aberto. Somente se o middleware for de Código Aberto, totalmente transparente e independente, poderemos evitar problemas com governos, instituições privadas e até mesmo com a vida das pessoas.

LM» ***Como está a evolução desses objetivos? Eles já foram alcançados?***
JL» O middleware já existe há vinte anos, e é uma tecnologia em constante modificação. Hoje, nossos esforços se destinam ao suporte a SOA, Business Intelligence e governo eletrônico (o *e-Gov*). Também estamos trabalhando numa plataforma completa e integrada e numa implementação de referência de todos os componentes do OW2, para fornecer serviços a empresas privadas, governos etc.

Nossa intenção é completarmos isso tudo em janeiro de 2008.

LM» ***O OW2 parece depender muito do servidor web Apache. Como é a sua relação com a Fundação Apache?***
JL» A relação é boa. Não utilizamos o mesmo modelo de licenciamento, ou as mesmas políticas de direitos autorais. Nós realmente não favorecemos a licença Apache. Porém, assim como nós utilizamos alguns de seus componentes, eles também utilizam alguns dos nossos. Há ocasiões em que competimos e outras em que colaboramos.

Isso é típico do Código Aberto, e é saudável. Como no OW2 somos pessoas de bem, assim como na Fundação Apache, nós não criamos problemas uns para os outros.

LM» ***E quanto ao Eclipse? A Fundação Eclipse tem o mesmo tipo de relação com a OW2?***
JL» Nossa relação com o Eclipse é mais próxima do que com o Apache. A Fundação Eclipse já participou da ObjectWeb, mais especificamente no projeto das *Webtools*. Alguns de nossos membros ainda colaboram de perto no projeto *Service Oriented Tools*.

Na realidade, nossa relação com o Eclipse é mais simples. O OW2 é especialista na plataforma de execução, e não existiria uma plataforma dessas sem as ferramentas de desenvolvimento. Então, não concorremos em nenhuma esfera.

LM» ***Na sua visão, qual a importância da adoção de uma licença de Código Aberto pelo Java da Sun?***
JL» A nosso ver, no OW2, é um movimento muito natural. Eles precisavam fazer isso, e ficamos muito contentes que de fato tenham feito. Mesmo antes desse movimento, a Sun sempre foi

muito amistosa com o OW2, assim a mudança do licenciamento do Java ainda não alterará nossa relação.

LM» ***Quais são os principais responsáveis por contribuições ao OW2? Empresas privadas, indivíduos ou governos?***
JL» Temos muitos participantes no consórcio, então apontar apenas um subconjunto deles como principais contribuidores não seria correto. Como somos compostos por empresas de todos os tamanhos e setores, que desenvolvem códigos voltados a suas próprias necessidades, realmente é impossível afirmarmos qual ou quais são mais presentes com seus códigos.

LM» ***Todo esse ecossistema certamente gera competição entre membros do OW2. Como o consórcio lida com esse aspecto?***
JL» Nós não forçamos qualquer tipo de competição. Para nós, os projetos surgem para preencher uma demanda tecnológica. Portanto, nós geralmente não incentivamos a existência de mais de duas respostas para uma mesma questão, tecnicamente falando.

LM» ***Como é feita a seleção de projetos para inclusão no OW2?***
JL» Temos um comitê, formado por desenvolvedores, representantes da OW2 e especialistas, que constrói a visão da arquitetura de nossas soluções. Além disso, esse comitê decide quais serão os projetos que comporão nossa base, fundamentados na adequação de cada candidato a essa mesma visão. Novos projetos cujo código não seja utilizável por outros projetos dentro do OW2 dificilmente terão chance de se juntar ao consórcio.

LM» ***Quais os modelos de negócio mais populares entre os projetos que compõem o OW2?***
JL» Como eu disse, nós englobamos diversos tipos de empresas, e cada uma tem seu próprio perfil. Há grandes integradores de sistemas, com forte base em serviços e especializados em seus mercados. Por outro lado, as *startups* costumam adotar uma mistura de modelos diferentes, como serviços e até OEM.

Cientistas e pesquisadores também têm usado nosso código, e publicam na comunidade acadêmica com base nele. Esse é mais um modelo de negócios que vem crescendo.

Por último, temos também empresas voltadas unicamente ao Código Aberto, como a Red Hat, por exemplo, que obtêm sua receita dentro desse modelo.

LM» ***Como é a política de licenciamento do consórcio?***
JL» Nós aceitamos o duplo licenciamento de nossos projetos. Com isso, a licença mais comum entre eles é a GNU GPL, com uma alternativa proprietária.

LM» ***Para uma empresa que ainda não faz parte do consórcio, quais as vantagens de vir a integrá-lo?***
JL» O OW2 é uma fonte reconhecida de componentes confiáveis e de Código Aberto. Somos a terceira geração do Código Aberto. As empresas que se juntam a nós são aquelas que compartilham nossa visão sobre a importância do desenvolvimento de componentes em Código Aberto para a formação de um middleware de alta qualidade e distribuído.

Além disso, como parte de um consórcio, todos os nossos projetos dispõem de uma espécie de marketing colaborativo.

Em resumo, juntar-se ao OW2 é bom para a imagem da empresa e oferece acesso a uma base de código de qualidade garantida e perfeitamente legalizada quanto à questão de licenças.

LM» ***Como você caracteriza o sucesso do OW2 em 2007, e quais os planos para 2008?***
JL» Disponibilizamos importantes porções de código sob a GPL, voltadas a todas essas áreas, e esse é exatamente o nosso objetivo.

Em nossa passagem pelo Brasil, a meta é preparar o terreno para a expansão do OW2 por todo o mundo. Desejamos criar uma verdadeira massa crítica de desenvolvedores e usuários de nosso código ao redor do planeta. Já estamos presentes na China e na Europa, assim nossa expansão deve continuar pelo Brasil e o restante da América Latina.

LM» ***Por que a América Latina?***
JL» Nossa motivação é a oportunidade que vislumbramos aqui, com diversas empresas e pessoas extremamente amigáveis e acolhedoras ao Código Aberto.

Se Ásia, Europa e América Latina unirem forças para construir em conjunto um middleware de Código Aberto e alta qualidade, conseguiremos mudar as regras do mercado desse segmento.

> ***Em nossa passagem pelo Brasil, a meta é preparar o terreno para a expansão do OW2 por todo o mundo.***

No Brasil, nosso primeiro associado é o Serpro, que já está altamente comprometido com a comunidade do OW2, e mostrou muito interesse em participar do desenvolvimento de um middleware de Código Aberto.

Outros órgãos federais, como o ITI e a Casa Civil, também mostraram interesse, e verificamos vários outros potenciais interessados entre universidades privadas e órgãos públicos estaduais e municipais. ■

Quando a educação tem Código Aberto

Edgar Silva

Iniciativas colaborativas para a educação técnica e superior.

por Edgar Silva

Com a chegada dos conteúdos colaborativos, wikis, fóruns e canais de IRC, a disseminação de cultura e conhecimento derrubou fronteiras geográficas e sociais. É a grande chance de encontrar talentos em todos os lugares do mundo, em todas as esquinas de uma cidade, e a chave para isso ainda é a educação. Como grande alternativa à indústria, a tecnologia da informação ganha alicerces em vários países que buscam desenvolvimento, como o Brasil. Neste artigo vou listar alguns movimentos interessantes que, com certeza, podem ser adaptados aqui.

A Educação Livre é uma iniciativa muito antiga; usemos como exemplo os grupos de usuários Java. Vamos pensar no projeto JEDI[1], que nasceu nas Filipinas para fomentar o aprendizado e o ensino de Java em vários países. No Brasil, ele é liderado pelo DFJUG (Grupo Java de Brasília), na figura de Daniel de Oliveira, que dirige o projeto visando ao alcance de todos os países de língua portuguesa. O objetivo é incentivar a profissionalização e, claro, propiciar oportunidades a uma legião de talentos escondidos no meio de tanta dificuldade nessa busca do aprendizado e do saber.

Como aplicativos do JEDI, destaco o uso do *Moodle*[2], uma ótima solução de ensino a distância, de custo zero e Código Aberto; como características mais importantes, a vontade de realizar e de fazer a diferença que os participantes demonstram no projeto. Pode-se acessar o site do JEDI e buscar informações para levar a solução à sua cidade ou instituições de ensino locais.

A segunda iniciativa vem do Rio Grande do Sul, do consultor e professor universitário Daniel Wildt. O projeto Fuja[3] transmite aos alunos muito mais que conhecimento sobre programação em *Java* e *Ruby*, e também os conceitos da cultura do Código Aberto, como o trabalho em equipe, a busca pela qualidade, a colaboração e, claro, o sucesso.

O Fuja fica hospedado no Java.Net, que fornece infraestrutura de controle de versão, fóruns, listas e homepage para diversos projetos de Código Aberto em Java, onde os alunos do professor Daniel aplicam toda a teoria das disciplinas na forma de desenvolvimento de software, cujos códigos ficam abertos para que qualquer pessoa possa conferir. Um resultado dessa iniciativa são as empresas do TecnoPuc de Porto Alegre, que começaram a consumir os recursos criados por esse projeto educacional.

Na minha época de faculdade, recursos como esses jamais foram disponibilizados. Talvez por isso eu tenha resolvido divulgar o admirável trabalho dessas pessoas, que têm o potencial de transformar realidades com criatividade, dedicação e coragem. Certamente são idéias a serem copiadas. Afinal, no mundo do Código Aberto, copiar é legal.

O Código Aberto oferece um meio de criar mais que tecnologia; cria a cultura colaborativa. Essa cultura já traz sinais de grandes transformações – tanto de cunho econômico quanto social – ao nosso País. Os projetos JEDI e Fuja podem ser replicados para qualquer tecnologia de padrão aberto, já que não influenciam em custos, mas na boa vontade e no trabalho colaborativo. Minha recomendação? Procure seus grupos locais de tecnologia; se não houver um em sua cidade, não desista, reúna os amigos e monte um. Assim como fizeram Oliveira e Wildt, você pode fazer a diferença! ■

Mais informações

[1] JEDI: http://www.dfjug.org/DFJUG/jedi/index.jsp

[2] Moodle: http://moodle.org/

[3] Fuja: https://fuja.dev.java.net/

Sobre o autor

Edgar Silva é *Solutions Architect* e *JBoss Sales Engineer* da Red Hat Brasil, além de também ministrar palestras no Brasil e no exterior sobre *Java*.

Cezar Taurion

Como será o Código Aberto em 2008?

por Cezar Taurion

Para mim está ficando claro que o Código Aberto é muito mais uma tecnologia social que simplesmente programação de software. Sua essência é a colaboração, criação de comunidades e redes sociais. Ele pode ser definido como um modelo técnico e social de desenvolvimento de artefatos de software baseado no desenvolvimento colaborativo.

Software é uma forma de representar conhecimento. E um novo sistema de riqueza baseado em conhecimento ainda é um território escassamente mapeado. Ao contrário dos recursos materiais, o consumo de conhecimento gera mais conhecimento.

Também está bem nítido que o discurso ideológico da fase inicial e romântica do Código Aberto está ficando em segundo plano. O Código Aberto não é antagônico ao software proprietário, mas permite uma coexistência entre os diversos e alternativos modelos de negócio.

O movimento do Código Aberto incentiva a criação de redes, inclusive a cooperação entre projetos. É muito comum partes de um mesmo software serem inseridas em outros projetos. Criam-se muitas vezes processos de co-evolução, com os projetos desenvolvendo-se de forma interdependente. O resultado dos projetos não beneficia apenas uma empresa ou indivíduo, mas toda uma comunidade interessada no uso daqueles softwares.

Para imaginar 2008, vamos criar um modelo de medição de maturidade de uso do Código Aberto, algo como o CMMi para Código Aberto, e inserir as empresas em determinados estágios evolutivos, considerando seu comprometimento com o Código Aberto. Quanto mais empresas estiverem nos estágios mais evoluídos, mais maduro estará o movimento.

O primeiro estágio é a negação, estágio no qual a empresa luta contra o Código Aberto, seja por desinformação ou por sentir-se ameaçada em seu modelo de negócio. Ainda há muitas empresas neste estágio.

No segundo estágio, não existe contribuição com a comunidade. A empresa é apenas usuária de programas abertos, às vezes até sem saber. Sua intenção é reduzir custos em relação às alternativas proprietárias. A grande maioria das empresas usuárias está neste estágio.

No próximo estágio, que chamaremos de colaborador, a empresa começa a usufruir mais intensamente dos conceitos de Código Aberto, fazendo modificações e melhorias em softwares e devolvendo-as à comunidade. Mas ainda não existe uma estratégia real de uso e exploração dos conceitos do Código Aberto. Algumas empresas usuárias e mesmo algumas produtoras de software encontram-se aqui.

O quarto estágio já mostra uma estratégia definida. A empresa assume um papel pró-ativo no desenvolvimento de uma comunidade, inclusive alocando profissionais de sua equipe ao projeto. O software não é mais desenvolvido ou evoluído dentro de casa, mas de forma independente, com a comunidade estruturada em fundações, por exemplo. A empresa incentiva o ecossistema em torno de seus softwares. Poucas empresas estão aqui, a maioria produtoras de software.

Finalmente, no quinto estágio a empresa participa ativamente de diversos projetos de Código Aberto, que se torna parte integrante e essencial da estratégia e modelo de negócios. A IBM, por exemplo, encontra-se nesse estágio.

Em 2008, o cenário do Código Aberto deve evoluir. Desejo que, nos eventos de nossa comunidade, além dos gurus sempre presentes, que certamente têm muito a dizer, tenhamos também representantes da Linux Foundation, Eclipse Foundation, Apache Software Foundation e diversas outras comunidades de grande reputação. Afinal, são esses projetos que estão disseminando o Código Aberto! ■

Sobre o autor

Cezar Taurion é gerente de novas tecnologias aplicadas da IBM Brasil. Seu blog está disponível em www.ibm.com/developerworks/blogs/page/ctaurion.

Controle remoto, compartilhamento de telas e serviço de terminais no Linux

Tranqüilo à distância

Se já é ruim ser obrigado a deixar um evento social devido a uma falha no servidor, imagine isso durante as férias. Melhor prevenir-se.

por Pablo Hess e Joe Casad

O controle de sistemas baseados em Unix, como o Linux, sempre foi fácil. Antigamente, ferramentas simples já permitiam ao usuário abrir uma conexão remota para acesso pela linha de comando. O surgimento e posterior desenvolvimento da interface gráfica, no entanto, ao mesmo tempo em que facilitaram várias tarefas antes entediantes, introduziram uma boa dose de complexidade a essa fórmula simples.

Nos anos recentes, os relatos de economia proveniente da adoção de *thin clients* lembraram o mundo das vantagens do modelo de serviços de terminal, e a virtualização também se concentrou em operar múltiplos sistemas com um único conjunto de teclado e mouse.

Operação

Para os administradores de sistemas, os recentes avanços significam uma grande ajuda nos raros momentos de ausência do escritório, como são os fins de semana ou as férias.

Se o local de lazer oferecer um computador com navegador web com *Java* ativado, talvez já seja possível solucionar eventuais problemas, mesmo a milhares de quilômetros de distância.

É pensando no sossego merecido que a **Linux Magazine**, neste mês, apresenta três importantes soluções para garantir a tranqüilidade do administrador nessas férias.

O já antigo *VNC* é tema do primeiro artigo. Nele, comparamos algumas alternativas livres para servidores e clientes VNC para Linux. Felizmente, há desenvolvedores criando servidores também para sistemas proprietários, permitindo o acesso remoto até mesmo a servidores Windows®.

Em seguida, o inovador *NX*, da NoMachine, é explicado em profundidade. Unindo funcionalidades do *X*, *SSH* e *VNC*, o produto da NoMachine tem uma versão proprietária gratuita (*NX Free Edition*) e a versão comunitária (*FreeNX*). Ambas são exploradas detalhadamente, para que você escolha o modelo mais adequado a suas necessidades.

Por último, a operação à distância de servidores Windows também é coberta, através do fabuloso *Rdesktop*, um software de Código Aberto que implementa o protocolo *RDP*, incluído em todos os sistemas da Microsoft.

Prepare seus servidores para a operação remota e divirta-se! ■

Índice

Acesso remoto e gráfico com VNC

Hora de compartilhar

O protocolo VNC oferece uma prática solução multiplataforma para compartilhamento de tela. Conheça as melhores soluções gratuitas para Linux.

por James Mohr

Há muitos administradores hoje em dia trabalhando em data centers espalhados por múltiplos prédios. Normalmente, a maioria das atividades de manutenção em sistemas Linux e Unix pode ser realizada via *SSH*; entretanto, em vários casos, a ferramenta usada pode não possuir uma interface em linha de comando, ou o sistema remoto pode estar rodando alguma versão do Windows® que exija acesso à interface gráfica.

O *Virtual Network Computing* (*VNC*) é uma alternativa popular para o compartilhamento de tela em redes heterogêneas. O comportamento do VNC é levemente diferente daquele do sistema X *Window*. Uma diferença é que o VNC **compartilha** o desktop inteiro. Um usuário em uma máquina consegue visualizar a área de trabalho de um usuário em outra máquina, e controlar o mouse e o teclado do sistema remoto. Esse recurso é útil em várias atividades, tais como acessar o computador do trabalho a partir de casa, trabalhar com estudantes num ambiente de treinamento, oferecer suporte técnico ou incomodar seu filho enquanto ele joga no computador.

No protocolo X, a máquina local é responsável por gerenciar a tela e as janelas. O VNC usa o protocolo *Remote Frame Buffer* (*RFB*), transmitindo os eventos do mouse e do teclado do cliente para o servidor, e depois enviando atualizações da tela de volta ao cliente.

O método mais simples para se atualizar a tela é enviar os dados brutos de pixels na ordem de formação da imagem (da esquerda para a direita, de cima para baixo). Assim que a tela inicial é desenhada, em vez de atualizar a tela inteira quando algo mudar, o protocolo VNC usa uma primitiva simples para desenhar um retângulo de dados num local particular. Dessa forma, somente as áreas alteradas precisam de atualização.

Como mais informação é enviada pela rede do que no X11, o VNC obviamente é mais lento; entretanto, nos testes que fiz, o VNC não causou qualquer problema de desempenho significativo.

Mesmo limitando os dados enviados dessa forma, ainda pode haver problemas de banda com conexões lentas com muitas atualizações. Portanto, inúmeras técnicas de compressão diferentes foram desenvolvidas para reduzir ainda mais a quantidade de informação transferida.

Como interage diretamente com o *frame buffer*, o protocolo RFB – e portanto o VNC – é independente de plataforma. Uma máquina Windows pode conectar-se ao Linux assim como a outro Windows. O VNC pode essencialmente trabalhar com qualquer sistema de janelas, e portanto é ideal para Windows e X11, assim como para sistemas Macintosh.

Conexão

Assim como o cliente para desktop Windows remoto, o servidor VNC guarda todas as informações de conexão e sessão. Portanto, pode-se desconectar um cliente numa localização, e depois reconectar de um ponto diferente, e retomar de onde se havia parado. Um cliente X11 geralmente não é capaz de se desligar do servidor e depois reconectar-se (embora haja alguns aplicativos X11 que fazem isso).

O aplicativo de controle, ou cliente, costuma ser chamado de visualizador, ou *viewer*, pois é usado para visualizar a máquina remota. Esse nome tem uma implicação muito mais profunda, pois na verdade pode-se até configurar o servidor para ser "somente leitura", ou "somente visualização". Ou seja, o usuário consegue visualizar a tela, mas não é possível realizar alterações. Pode-se usar esse recurso para monitoramento remoto de aplicativos nos quais não são permitidas mudanças, apenas para relatar qualquer evento observado.

Num ambiente de suporte, o técnico consegue visualizar os passos que o usuário toma, sem poder alterá-los. Em outros casos, pode-se configurar o VNC para exibir uma única tela em múltiplas máquinas, como num ambiente de treinamento quando o instrutor está demonstrando algo para um grande número de estudantes.

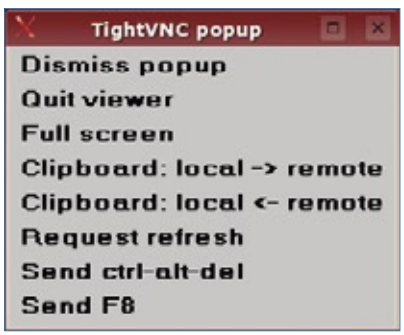


Figura 1 Opções de configuração do visualizador no Linux.

É importante lembrar-se de que o VNC precisa atualizar a tela local a cada alteração, como ao movimentar ou redimensionar uma janela. A janela não apenas deve ser redesenhada, como o fundo por trás da janela também precisa ser atualizado.

Fundos complexos levam mais tempo para serem atualizados. Além disso, quanto maior a resolução, mais dados são transmitidos, afetando também o desempenho.

Xvnc

Algumas versões do VNC oferecem não somente serviços VNC, mas também X11. O *Xvnc*, o verdadeiro aplicativo servidor no Linux, oferece X11 e VNC, suportando múltiplas sessões X11 simultâneas na mesma máquina remota, e inclui a conexão a sessões X11 pré-existentes, assim como a criação de novas sessões independentes. Isso significa que o que é mostrado pelo Xvnc no cliente não necessariamente é a mesma imagem exibida na máquina que está rodando o Xvnc.

Assim como o X11, o VNC cria telas virtuais, ou *screens*, para cada conexão. Por padrão, o VNC usa as portas 5900 a 5906, com cada porta correspondendo a uma dessas telas; então ao final tem-se as telas de :0 a :6. Note o sinal de dois-pontos à frente de cada número de tela, que é semelhante à notação usada pelas telas no X11.

VNC por dentro

Os pacotes costumam trazer cinco programas, mas o servidor e o visualizador VNC às vezes vêm em pacotes separados. Apesar de o comportamento geralmente ser o mesmo, podemos encontrar pequenas diferenças nas várias alternativas do VNC.

O script *vncserver* costuma ser usado para iniciar o servidor VNC. O script é simplesmente um *wrapper* para iniciar o programa *Xvnc*, que é o verdadeiro servidor. Esse script aceita bem menos opções do que o Xvnc, mas elas devem ser suficientes para a maioria dos usos. O programa cliente é o *vncviewer*.

Dois programas de suporte também são incluídos. O *vncpasswd* permite a configuração da senha para o usuário atual. As senhas precisam ter pelo menos seis caracteres. Note que na maioria dos casos apenas os oito primeiros caracteres são importantes, com os demais sendo ignorados.

Por padrão, o arquivo `$HOME/.vnc/passwd` é usado, mas é possível especificar um diferente. Por exemplo, um administrador que deseje criar um arquivo de senha para um usuário específico (ou seja, recriar uma senha) pode especificá-lo pela linha de comando, assim:

```
vncpasswd arquivo
```

Se, por exemplo, o diretório `home` do usuário estiver num sistema de arquivos compartilhado (isto é, *Samba* ou *NFS*) e se desejar garantir que o arquivo de senhas VNC seja local, é possível especificar a opção `-t` no *vncpasswd*, fazendo o aplicativo gravar as senhas em `/tmp/$USER-vnc/passwd`.

O programa *vncconnect* é usado para conectar um servidor VNC a um visualizador VNC numa máquina diferente. Alguns pacotes VNC também incluem o programa *vncconfig*, que oferece duas funções. A primeira é exibir ou estabelecer os parâmetros do Xvnc para um servidor em execução. A segunda função é auxiliar a transferência da área de trabalho de e para o visualizador VNC.

O uso do VNC não é garantido em todas as distribuições. Algumas têm problemas devido à configuração de seus firewalls, que bloqueiam as portas usadas pelo programa.

Em ação

O primeiro passo para executar o VNC é executar o script *vncserver* como qualquer usuário. Na primeira vez que se faz isso, é necessário fornecer uma senha para a conexão.

O script então cria os arquivos de configuração necessários, incluindo todos os aplicativos que devem iniciar automaticamente, que por sua vez são inseridos no diretório `$HOME/.vnc/`.

Depois de pedir a senha, ou caso já exista uma, o servidor VNC exibe as informações básicas a respeito da conexão, e qual arquivo ele está usando para iniciar algum aplicativo. Por padrão, os aplicativos são iniciados por `$HOME/.vnc/xstartup`. Na primeira vez que o navegador for iniciado, o visualizador geralmente vai criar um arquivo `xstartup` sozinho.

No Linux, por padrão, o script *xstartup* simplesmente configura o ambiente básico, e depois inicia um *Xterm* e o gerenciador de janelas *TWM*, que, apesar de exageradamente simples, é suficiente para a administração remota.

Como mostram as **figuras 1** e **2**, a interface gráfica do cliente Windows oferece muito mais opções que a do Linux, que só as disponibiliza pela linha de comando.

Dependendo da distribuição usada, o cliente *vncviewer* pode possuir uma interface gráfica para a execução, como o *Cliente do Terminal Server* do Gnome (**figura 3**).

Todos os servidores VNC avaliados neste artigo trazem um servidor HTTP embutido, que permite a conexão através de um navegador com Java habilitado. Apesar de a opção web ser útil em princípio, a velocidade da atualização da tela é sensivelmente pior do que todas as outras combinações experimentadas, e a qualidade gráfica não é boa. Ainda assim, essa é a única modalidade de acesso possível quando não se dispõe de um visualizador VNC.

Documentação

A documentação, por padrão, é esparsa e geralmente limitada às *manpages*, bem semelhantes para todos os produtos. Embora em geral os mesmos programas sejam fornecidos, seu comportamento pode variar, com alguns casos de diferenças eneromes.

Os produtos foram instalados em diferentes distribuições Linux e também no Windows, com várias combinações de servidores e clientes. Apesar do comportamento diferente entre diferentes produtos, não houve problemas de incompatibilidade entre componentes de pacotes diferentes.

Na rede de 100 Mbps em que foram realizados os testes, não houve grandes atrasos devidos à atualização de toda a área da tela, como ao abrir o menu *Iniciar* do Windows ou iniciar um novo gerenciador de arquivos. Entretanto, foi impossível jogar *World of Warcraft* através da conexão VNC.

TightVNC

O *TightVNC* se auto-intitula uma "versão melhorada do VNC", e alega incluir "vários novos recursos, melhorias, otimizações e correções de falhas", a maioria dos quais requer uma excursão pelos *changelogs*.

O TightVNC oferece o driver de vídeo espelhado *DFMirage*, que roda em Windows 2000, XP e mais recentes. Assim como o TightVNC, o driver é gratuito e oferece uma forma ainda mais prática de atualização das informações da tela. Mesmo sem o driver, não houve atrasos; entretanto, depois de instalar o driver, pelo menos um programa congelou completamente mesmo sem qualquer conexão de um cliente VNC.

Removido o driver, o programa voltou a funcionar, o que mostra que há certas restrições à forma como alguns programas para Windows reagem a esse driver.

Um aspecto interessante é que o servidor pode alterar a área de trabalho para uma cor sólida, em vez de transmitir o papel de parede. Também é possível desativar efeitos gráficos desnecessários da interface do Windows XP. Esses recursos aumentam a eficiência das atualizações da tela reduzindo a informação que é transmitida.

Uma eficiência ainda maior pode ser alcançada pela compressão *JPEG*. Segundo a documentação do TightVNC, essa codificação é otimizada para "conexões lentas e de média velocidade", mas não fica claro quais são essas velocidades.

RealVNC

Como a empresa RealVNC foi criada pelos desenvolvedores do VNC original, pode-se argumentar que o *RealVNC*[2] é o herdeiro do legado do VNC original. O RealVNC atualmente está disponível em três versões: *free*, *personal* e *enterprise*.

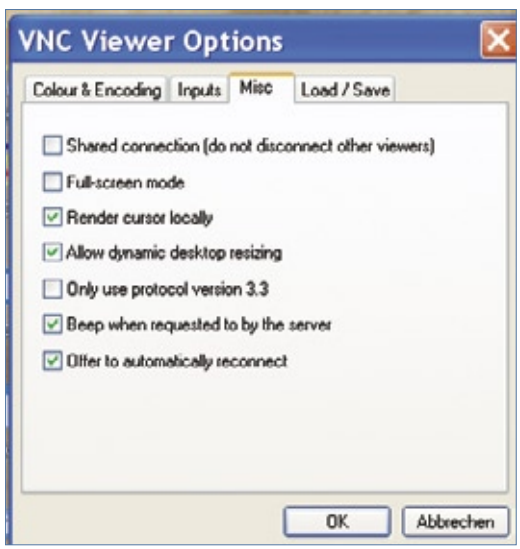


Figura 2 Opções de configuração do visualizador no Windows®.

Nos testes, foi usada a versão free 4.1.2, que parece ser uma versão restrita dos produtos de Código Aberto disponíveis. Por exemplo, o script *vncserver* não suporta um arquivo de senhas fora da localização padrão, `$USER/.vnc/passwd`.

Além disso, diferentemente dos outros produtos, o *vncpasswd* do RealVNC não pede uma senha para o modo "somente visualização". Na verdade, a versão do RealVNC nem parece suportar qualquer opção que os outros produtos suportam.

Outro inconveniente é que o programa não pede uma senha caso ainda não tenha sido fornecida alguma. Porém, o RealVNC sugere o uso do programa *vncpasswd*, que pedirá uma senha para visualização. O incômodo é ainda maior porque ele exibe uma mensagem de uso que indica a possibilidade de se especificar um arquivo de senhas com a opção `-t`; todavia, nenhum é suportado pelo script *vncserver*. Se o *vncpasswd* for executado com a opção `-t`, e depois se tentar iniciar o servidor, ele falhará novamente, pedindo que a senha seja configurada.

Além dos recursos suportados pela versão gratuita e aberta, a versão personal também suporta a autenticação RSA com 2048 bits, a criptografia da sessão com AES de 128 bits e a transferência de arquivos, entre outros recursos, mas não suporta Linux ou outras variantes de Unix.

A versão enterprise do RealVNC exige uma licença separada para servidores Windows e Linux, e também suporta o Mac OS X. Uma adição é a *Direct platform native authentication*, que significa que não é necessário criar um arquivo de senhas adicional para cada usuário para que este se conecte ao servidor. Em vez disso, a ferramenta usa os métodos de autenticação do próprio sistema operacional, exigindo assim uma única senha. Em servidores Windows, isso significa que se pode realizar a autenticação tanto com um domínio NT quanto com credenciais do Active Directory.

No Linux ou Unix, a autenticação é feita via NIS/NIS+. Como o sistema já consegue distinguir os usuários, esse mecanismo também significa que é possível criar ambientes separados para diferentes usuários.

Figura 3 O Gnome traz o *Cliente do Terminal Server*, que suporta alguns protocolos além de VNC.

MetaVNC

Em termos de escopo do produto e informação disponível, o *MetaVNC*[3] parece ser o mais exíguo. A versão 0.6.5, usada no teste, é baseada no TightVNC 1.3.9. A instalação no Windows funcionou sem dificuldade, mas no Linux a documentação só explica os procedimentos para o *Fedora*.

Em geral, o MetaVNC também parece ser o mais lento, independente de estar no servidor ou no cliente. Apesar da conexão com o MetaVNC nas duas pontas ainda ser aceitável, clientes diferentes operando junto com um servidor MetaVNC tiveram desempenho sofrível.

Os recursos dessa solução são quase idênticos aos do TightVNC. O cliente Windows tem várias novas opções, mas a documentação não informa o que elas fazem.

Conclusões

Apesar de algumas frustrações iniciais, o TightVNC oferece o melhor pacote e as informações mais facilmente acessíveis. A versão gratuita do RealVNC tem muito poucas funcionalidades. Apesar de o MetaVNC ter mais recursos que o TightVNC, a falta de documentação útil afasta os usuários, principalmente no ambiente corporativo. ■

Mais informações

[1] TightVNC: http://www.tightvnc.com/

[2] RealVNC: http://www.realvnc.com/

[3] MetaVNC: http://metavnc.sourceforge.net/

Sobre o autor

James Mohr é responsável pelo monitoramento de vários *datacenters* de um provedor de soluções corporativas em Coburg, Alemanha. Além de organizar o site *Linux Tutorial*, em http://www.linux-tutorial.info, James é autor de diversos livros e dezenas de artigos sobre grande número de tópicos.

Serviço de terminais veloz com NX

Velocidade máXima!

O NX oferece serviços de terminal velozes, mesmo em conexões lentas.

por Markus Feilner

Serviços gráficos de terminal de alta performance não passavam de sonho para os usuários de Linux. Agora, o *NX* da NoMachine[1] e o projeto independente *FreeNX*[2] oferecem a combinação de ferramentas necessárias para sessões gráficas de terminal no Linux. É possível até mesmo conectar-se por uma janela de terminal.

A NoMachine começou a desenvolver uma solução de servidor de terminais de alta performance em 2000. O anúncio de que a NoMacine havia liberado suas próprias bibliotecas sob a GPL em março de 2003 causou rebuliço, particularmente porque o NX suporta os principais protocolos, como o *RDP*, da Microsoft, o *VNC* (*Virtual Network Computing*) e o *X11*. A NoMachine também permite que os usuários controlem qualquer sessão do *KDE*, *Gnome* ou Windows® com apenas uma lenta conexão de modem, o que é ainda mais surpreendente frente ao fato de que o NX suporta criptografia por RSA e DSA.

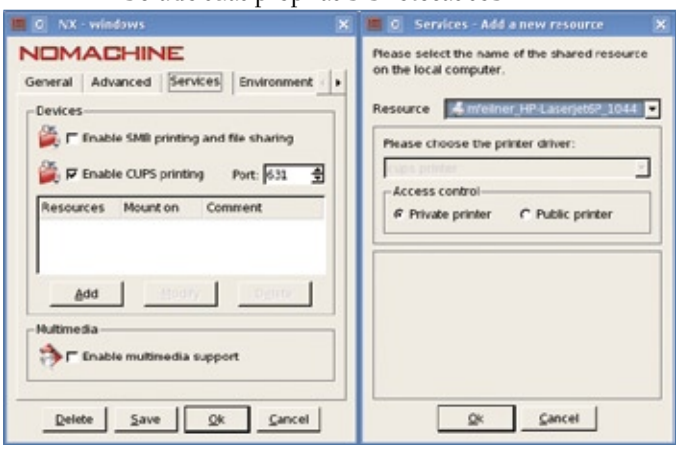


Figura 1 Uma HP Laserjet local está disponível na sessão de terminal. O *NX* depende do *CUPS* para ligar a impressora do cliente ao servidor de terminal.

Por que NX?

A tecnologia NX permite que os usuários contectem-se aos servidores de terminal Linux ou Windows, com um cliente Linux, Windows ou Mac, ou com qualquer outro navegador. Os usuários podem iniciar aplicativos individuais que o cliente exibe perfeitamente em janelas separadas. Os administradores Linux eventualmente forçados a trabalhar no Windows ficarão felizes ao verem seus terminais favoritos, como o *Gnome-terminal* ou o *Konsole*, na área de trabalho do Windows.

O suporte local a áudio, impressoras (veja a **figura 1**) e mídias de armazenamento está incluído, assim como o acesso a sessões VNC através de um proxy. Os usuários têm controle intuitivo do cliente, e os administradores também podem acessar ferramentas de linha de comando. A suspensão e recuperação de sessões também são suportadas, e a versão 3 da ferramenta acrescentou o suporte ao mascaramento e compartilhamento de desktop. O administrador precisa apenas abrir a porta 22 no firewall. A tecnologia do NX depende de X *Window*, *SSH*, *Rdesktop*, *VNC* e outros projetos livres.

O que torna as sessões muito mais velozes do que o encaminhamento convencional do X por comandos como `ssh -X -C usuário@máquina X programa` é uma combinação inteligente de *cache* e um proxy eficiente, assim como otimização com bibliotecas como *Zlib* e *JPG*.

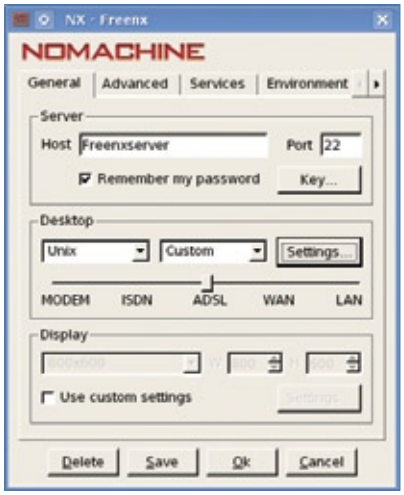


Figura 2 A barra define o nível de compressão. Nessa figura, o usuário configurou uma entrada personalizada para exibir um aplicativo individual.

O NX não apenas comprime todos os dados intercambiados entre o cliente e o servidor, como também tudo que ele guarda em seu cache local.

A maior parte da velocidade do NX vem do conhecimento exato do funcionamento do X Window. O desempenho ruim geralmente demonstrado por aplicativos X legados em conexões de banda estreita se deve, principalmente, à estrutura interna do desktop X11 Unix padrão, que é projetado para linhas velozes e com banda larga. O NX emprega vários truques para superar alguns desses problemas de desempenho associados ao X.

O NX substitui o X

Em vez de usar o X11, com suas várias desvantagens, para a transmissão de dados, o desenvolvimento da NoMachine se baseia no protocolo NX. O programa *nxserver* comunica-se com o programa *nxclient*. O *nxagent* do servidor lida com as requisições de aplicativos, o *nxclient* lida com a renderização no lado cliente, e o *nxproxy* comprime e otimiza.

Como tanto o cliente quanto o servidor fazem cache dos dados de X Window, o NX evita muita repetição. Sob condições ótimas, o aplicativo recebe uma resposta diretamente do processo local, que envia as modificações (*deltas*) ao servidor. Na média, o NX consegue carregar entre 60% e 80% dos dados diretamente a partir do cache, analisando o protocolo X. As taxas de acerto do cache costumam ficar pouco abaixo de 100% no caso de imagens, como ícones e *pixmaps*.

O NX começa verificando se consegue responder uma requisição diretamente a partir do seu próprio cache; se não, os passos de codificação do protocolo X com base em armazenamento de mensagens é iniciado. O NX analisa o protocolo X e disseca suas mensagens em duas partes: um componente de dados e uma identidade, ou *fingerprint*.

O fingerprint costuma ocupar apenas alguns bytes; o componente de dados é a parte interessante do tráfego. As fingerprints de duas mensagens são diferentes, mas a probabilidade de o componente de dados já ter sido transmitido cresce junto com a duração da sessão X. O NX consulta e armazena cada bloco de dados individual que transfere em seu armazém de mensagens. *Checksums MD5* aceleram a busca. Como o NX somente precisa calcular as checksums que vai codificar e a ponta que decodifica guarda apenas os dados, os requisitos de memória são comparativamente baixos. Graças a isso, o banco de mensagens é capaz de guardar até 3 mil mensagens.

Na primeira vez que um usuário abre um menu de aplicativos, o cliente NX pede todos os dados do servidor. Este comprime e criptografa os dados, e depois envia-os ao cliente. Quando uma segunda requisição é feita, quase todos os dados são obtidos da memória local. Isso ajuda o cliente a evitar a transmissão de dados, pois pode-se atender as requisições ao X diretamente do cache local.

O banco de mensagens é persistente; o usuário pode suspender e retornar a uma sessão sem se desfazer do conteúdo do banco. E como o NX salva o banco de mensagens ao final da sessão, este ficará disponível para uma segunda sessão idêntica – mesmo após reiniciar a máquina cliente. Esse método é eficaz, mas gera preocupações quanto à segurança. Um agressor conseguiria extrair dados críticos de sessão do cache do NX num laptop roubado ou comprometido? Essa pergunta requer uma investigação mais profunda.

Segurança

O NX comprime os dados restantes com uma técnica voltada ao suporte o que é ótimo ao protocolo X, chamada *differential X protocol encoding*, ou codificação diferencial do protocolo X. Como as mensagens do X transportam conteúdos muito diferentes, como imagens, fontes, texto e outras informações, e devido ao fato de o NX também "falar" RDP e VNC, assim como X, ele usa diferentes métodos de compressão, dependendo do objeto e do tipo de conexão: JPG, PNG, RDP, Tight ou Zlib. Combinações inteligentes ajudam o programa a alcançar taxas entre 20:1 e 2000:1 (veja também o **quadro 1**).

A biblioteca Zlib ainda atinge uma taxa de 4:1 com dados desconhecidos que não possuam um método de compressão específico, e o NX usa esse mesmo software para comprimir todo o tráfego entre o cliente e o servidor. As configurações do cliente definem um nível de compressão entre 1 (*WAN*) e 9 (*MODEM*) (veja a **figura 2**). De acordo com a NoMachine, esse último estágio reduz o volume de dados em mais 30%.

Streaming e priorização

O NX faz uso de *streaming* em casos como *GSM* (4 kbps), nos quais a transmissão de uma imagem de 12 KB levaria tempo demais. O servidor divide a imagem em segmentos, transmitidos

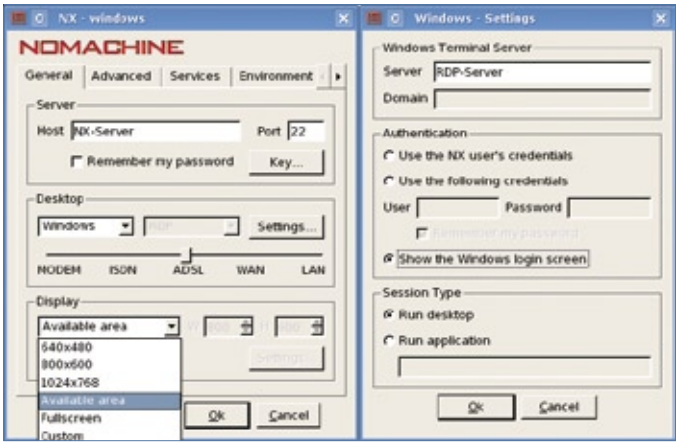


Figura 3 Configuração de um cliente *NoMachine* para acessar um servidor Windows. Os usuários podem redimensionar as sessões Linux dinamicamente, mas é melhor pré-selecionar a resolução exigida para as sessões Windows. O modo de autenticação é especificado no diálogo *Settings*.

com baixa prioridade após a aplicação da compressão JPG. Isso permite que o aplicativo continue respondendo às ações do usuário enquanto o NX carrega a imagem de fundo.

Genericamente falando, o NoMachine oferece aos aplicativos interativos uma prioridade maior do que aos programas dependentes de imagens, analisando os dados trafegados e adaptando vários parâmetros dinamicamente. Acima disso, controles internos de largura de banda, cotas e a compressão de tráfego são aplicados para reduzir o volume de dados transmitidos. Mais detalhes da compressão do protocolo X do NX estão disponíveis no site da NoMachine[4].

Esse esforço todo tem resultado. Dependendo do aplicativo, o NX suporta a operação suficientemente suave com bandas de 10 a 20 kbps e tempos de latência de décimos de segundo. Com uma banda de 30 ou 40 kbps e latências de 0,01 segundo, o desktop KDE ou Gnome fica tão rápido que parece que se está trabalhando localmente. Os múltiplos megabytes exigidos para a primeira execução do KDE são reduzidos a uns poucos kilobytes na próxima execução. Esse uso frugal de recursos significa que o NX economiza até 60% no volume de transmissão de dados em comparação com uma LAN.

Os clientes guardam dados comprimidos e descomprimem-nos dinamicamente – com resultados incríveis em alguns casos. Na segunda vez que se executa o *OpenOffice.org* num servidor NX remoto, o programa começa bem mais rápido que no disco local. As velocidades têm forte contraste com aquelas alcançadas nos sobrecarregados e mal configurados PCs Windows típicos da maioria dos ambientes de escritório.

Como as sessões de desktop geralmente incluem tarefas freqüentemente recorrentes (abrir o menu, abrir uma caixa de diálogo, mover uma janela), quanto mais o NX for usado, melhor será seu desempenho.

Exemplo 1: /usr/NX/etc/server.cfg

```
[...]
# (Des)ativar o BD de usuários NX:
#
# 1: Ativado. Somente os usuários no BD do NX podem
# fazer login no servidor
#
# 0: Desativado. Qualquer usuário autenticado pode fazer
# login.
# Se o BD de usuários do NX for desativado, qualquer
# usuário com uma senha válida no BD ou por autenticação
# SSHD conseguirá conectar-se ao sistema NX.
# Esse provavelmente é o padrão quando a autenticação
# por SSHD com PAM está ativada.
#
EnableUserDB = "1"
[...]
EnablePasswordDB = "1"
[...]
```

FreeNX ou NX?

Há várias versões do NX disponíveis, sendo a mais importante a *Free Edition*, da NoMachine[5], além dos pacotes fornecidos pelo projeto FreeNX. As duas implementações baseiam-se nas mesmas bibliotecas, mas a versão gratuita e aberta do NoMachine é mais nova, mais estável, mais rápida e tem mais recursos. A NoMachine oferece o cliente nos formatos Windows, RPM e DEB, além de arquivos com o código-fonte e softwares para Mac e Solaris.

Além disso, os desenvolvedores oferecem um gerenciador para o servidor e um recurso chamado *Web Companion*, que permite que os usuários acessem desktops Linux ou Windows a partir de um navegador web. Um cliente embarcado oferece a dispositivos portáteis, como Ipaqs com Linux ou o Zaurus, acesso a servidores NX.

O FreeNX fornece pacotes RPM e DEB, além de arquivos `tar.gz` da atual versão 0.7.0. Os usuários de Debian e Ubuntu podem acessar os repositórios[6] e executar `apt-get install freenx nxclient` para instalar a versão 0.6 e o Nxclient versão 2.1.0-17. O *OpenSuse* e o *Fedora* ainda funcionam com as antigas versões 0.4 e 0.5.

O FreeNX e o NX são compatíveis na maioria dos aspectos; de acordo com a lista de discussão[7], tanto o *applet Java* quanto o Web Companion funcionam com o FreeNX. Porém, as diferenças logo aparecem. O FreeNX é bem mais lento e não se aproxima da estabilidade demostrada pela versão gratuita do produto comercial. Apesar disso, o Nxclient das duas instalações roda com servidores do concorrente. Até mesmo sessões NX aninhadas respondem rapidamente à interação do usuário.

A experiência pode ser diferente em cada instalação do FreeNX, então os administradores podem

esperar alguns passos manuais. Há Howtos (para Ubuntu, por exemplo [8]) que ajudam a resolver várias dificuldades. Em contraste com isso, o software da NoMachine funciona sem dificuldade a partir da primeira execução, e o cliente é integrado ao firmware de vários *thin clients*.

Recursos e preços

Embora o FreeNX seja totalmente GPL, a NoMachine restringe sua Free Edition a dois usuários com sessões simlutâneas. A versão comercial suporta dez usuários (*NX Enterprise Desktop*) ou dez sessões simultâneas (*Small Business Server*). O *Enterprise Server* elimina essas restrições por aproximadamente US$ 1.500 e acrescenta a integração ao *LDAP* e *Active Directory*, um modo de quiosque e perfis de usuários.

O *Advanced Server* oferece sessões ilimitadas por um preço (por volta de US$ 3.500), adicionando possibilidades simples de criação de clusters e balanceamento de carga aos recursos oferecidos pela versão Enterprise Server. A NoMachine recomenda *Suse*, *Red Hat*, *Mandriva*, *Debian* ou Solaris como plataforma de sistema operacional, mas *Xandros* e outras distribuições também são suportados.

Configuração

Os arquivos de configuração do servidor FreeNX localizam-se em `/etc/nxserver/`; os binários ficam em `/usr/bin/` e `/usr/sbin/`, com as bibliotecas em `/usr/lib/nx/` e a documentação em `/usr/share/doc/freenx/`. Já a versão da NoMachine não respeita as recomendações da *FSB*, e instala tudo sob `/usr/NX/`, o que é comum na maioria dos softwares comerciais.

A configuração, os binários, as bibliotecas, os scripts e a documentação ficam todos disponíveis sob esse diretório. A pasta `/usr/NX/etc/` contém arquivos `.cfg`, modelos e arquivos de banco de dados de usuários e senhas. Após a instalação, o

Quadro 1: dxpc

Outra tecnologia conhecida como *Differential X Protocol Compressor* (*dxpc*[3]) funciona de forma semelhante ao NX. A técnica do dxpc inspirou os desenvolvedores da NoMachine, e eles fizeram bom uso das análises e ferramentas para codificação diferencial dos 160 diferentes tipos de mensagens do protocolo X. O dxpc ainda existe e, de acordo com seu site, o desempenho alcançado pela versão atual suporta o uso de um *Xterm* sobre uma conexão moderna. Mas ainda é praticamente impossível usar um navegador numa conexão de 28,8 kbps com o dxpc.

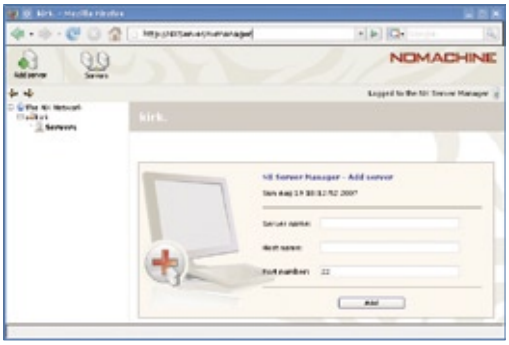


Figura 4 Gerenciamento de múltiplos servidores *NX* no *Firefox*. Os administradores de grandes redes com múltiplos servidores de terminal podem gerenciar seus bancos de dados de usuários e configurações dos servidores dessa forma.

NoMachine usa o *PAM* como fonte de autenticação, mas também pode utilizar um banco de dados de usuários completamente independente do sistema operacional do servidor. Caso seja necessário, é possível alterar as configurações através das entradas de `/usr/NX/etc/server.cfg`.

As opções do servidor para compartilhamento de arquivos e desktop, assim como o suporte a multimídia, também se localizam nesse diretório. Os bem documentados arquivos de configuração das duas variantes explicam todas as opções oferecidas pelo servidor.

A **figura 3** mostra como usar o cliente NX para acesso RDP a um servidor de terminais Windows. Nesse caso, é possível exportar aplicativos individuais; pode-se ver o NX exibindo aplicativos individuais num desktop Linux – uma ferramenta muito útil para acelerar o processo de migração.

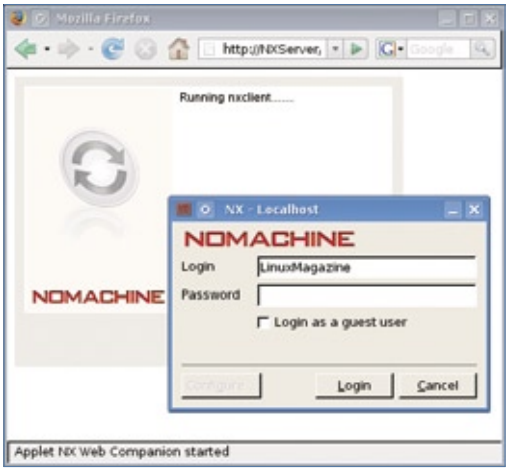


Figura 5 O *Web Companion* oferece acesso ao desktop pelo navegador. Um *applet Java* evita a necessidade de instalação de softwares no cliente.

O NX inicia o programa *rdesktop* e abre uma sessão. É importante que o servidor NX – não o cliente – estabeleça a conexão com o servidor Microsoft. A conexão entre o cliente o servidor NX é novamente criptografada utilizando SSH através da porta 22.

O *Server Manager* (**figura 4**) gerencia uma rede de servidores NX (por exemplo, um grupo de servidores num cluster com balanceamento de carga). A alta disponibilidade genuína não é suportada, e sessões ativas são perdidas se um servidor morrer. O Web Companion (**figura 5**) oferece o acesso pelo navegador web. Os administradores instalam um servidor *Apache* padrão no servidor NX, seguem alguns passos detalhados na documentação, e *voilà* – qualquer usuário com um navegador compatível com Java e as credenciais corretas é capaz de iniciar uma sessão no servidor NX.

O NoMachine esconde o plugin Java na versão `tar.gz`, e os pacotes RPM e DEB do Web Companion vêm sem o arquivo `nxapplet.jar`. Para ativar o acesso por navegador conforme descrito na documentação, é necessário baixar o `nxplugin-Versão.tar.gz`, descompactá-lo e salvar o arquivo em `/var/www/plugin/Java/nxapplet.jar`.

Conclusões

O NX redefine o serviço de terminais no Linux. Otimizado ao máximo e baseado num conhecimento profundo, o NX atinge desempenho incrível sem compometer a segurança. Os clientes estão disponíveis para qualquer sistema operacional atual, e os usuários podem acessar tanto servidores Windows quanto Linux. No modo de programas individuais, os administradores inteligentes podem possibilitar que seus usuários de Windows executem aplicativos do Linux, como *Firefox*, *Thunderbird* e *OpenOffice.org* – a única mudança que os usuários perceberão é que tudo roda mais rápido. O Web Companion significa que um desktop cliente precisa somente de um navegador, e há ainda um cliente móvel disponível. Profissionais de treinamento e suporte têm também a possibilidade de mascarar ou compartilhar os desktops dos usuários diretamente.

A NoMachine mostra a outros projetos como um modelo de desenvolvimento de sucesso baseado em Código Aberto pode ser, acrescentando produtos de nível corporativo e suporte com base em bibliotecas GPL. Para experimentar o NX, há dois servidores de teste disponíveis no site da NoMachine[1]. ■

Mais informações

[1] Página da NoMachine: http://www.nomachine.com

[2] FreeNX: http://freenx.berlios.de

[3] Compressor diferencial do protocolo X (dxpc): http://www.vigor.nu/dxpc

[4] Compressão do protocolo X do NX: http://tinyurl.com/d6abc

[5] Downloads do NoMachine: http://www.nomachine.com/download.php

[6] Repositórios do FreeNX para Ubuntu: http://tinyurl.com/ggg7f

[7] Lista de discussão do FreeNX: http://tinyurl.com/2nt2ve

[8] FreeNX no Ubuntu: http://tinyurl.com/yhos6o

CAPA

Serviço de terminais do Windows no Linux com Rdesktop

Cruzamento de terminais

O Rdesktop permite a abertura de uma sessão do Windows Terminal Server a partir do desktop Linux.

por Markus Klimke

O projeto *Rdesktop*[1], iniciado por Matthew Chapman, é um cliente de Código Aberto para os servidores de terminais Windows®. O Rdesktop implementa no Linux o mal documentado protocolo *RDP*, da Microsoft. Ele se adapta flexivelmente à largura de banda disponível, oferecendo aos usuários as mesmas opções para acessar os servidores de terminal que os sistemas Windows possuem. O *SeamlessRDP* da Cendio[2] leva essa solução um passo adiante, dando aos usuários a possibilidade de iniciar aplicativos individuais, como o *Word* ou o *Microsoft Management Console*, no Linux (**figura 1**).

O RDP é baseado no padrão *T.120 / T.128*[3] (originalmente chamado de *T.SHARE*) da International Telecommunications Union (ITU[4], **figura 2**). A Microsoft estendeu o protocolo e o introduziu na versão 4 do Windows NT, como *Windows Terminal Services*. O Windows Terminal Server possibilita a exibição de um desktop remoto nas máquinas de múltiplos usuários, e também a execução de aplicativos no servidor de termi-

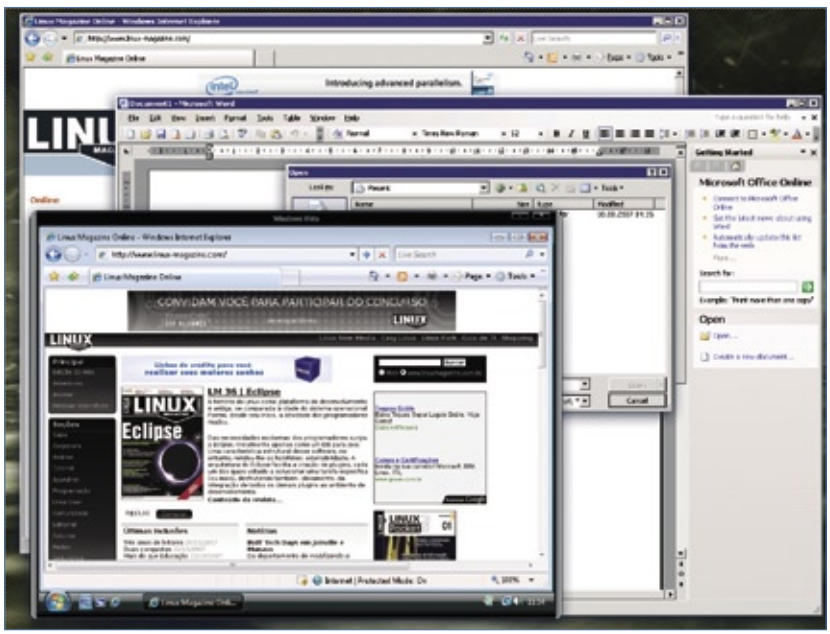


Figura 1 O *SeamlessRDP* permite a exibição de aplicativos Windows individuais no desktop Linux.

Quadro 1: Parâmetros do Rdesktop

- `-u usuário`: Nome de usuário para login no Windows.
- `-d Domínio`: Domínio de autenticação.
- `-s shell`: Substituir a shell padrão do Windows *(Explorer.exe)*.
- `-g geometria`: Dimensões da janela para a conexão remota (largura x altura). Também é possível especificar uma porcentagem da resolução da tela do cliente, como `80%`.
- `-f`: Modo de tela cheia (**figura 4**). Pode ser ativado ou desativado com **[Ctrl] + [Alt] + [Enter]**.
- `-K`: Manter os atalhos de teclado do gerenciador de janelas. Por padrão, o *Rdesktop* passa toda a entrada do teclado para o aplicativo Windows, se sua janela estiver ativa.
- `-r comport:número_de_porta_Windows`: Redireciona a porta serial.
- `-r disk:nome=/caminho/local`: Compartilhar `/caminho/local` como `nome` para acesso pelo servidor. Requer Windows XP ou mais recente.
- `-r lptport:número_de_porta_Windows`: Redireciona a porta paralela. Para operação bidirecional, é necessário Windows XP ou mais recente.
- `-r printer:nome_da_fila[=<driver>]`: Redireciona a impressora. O driver, se especificado, deve ser o mesmo da fila local. O Rdesktop usará a primeira impressora especificada como padrão.
- `-r sound:[local|off|remote]`: Redireciona a saída de som do servidor para o cliente.

nais, exatamente como o X *Window*. Os aplicativos de Windows sedentos por recursos podem rodar em poderosos servidores, em vez de se espremerem dentro das limitações dos desktops.

Além dos serviços de terminal integrados ao Windows, fabricantes como Citrix[5] e NoMachine[6] oferecem suas próprias soluções de servidores de terminal. As duas exigem a instalação de softwares clientes e servidores.

Se a única intenção for gerenciar um ou mais sistemas Windows remotamente, então esse problema não é necessário: embora a Microsoft cobre uma taxa de licenciamento para serviços de terminal multi-usuário, quase todas as variantes do Windows, seja para servidores ou desktops, incluem duas conexões gratuitas para gerenciamento. Dito isso, o sistema proprietário tem diferenças entre as versões do RDP: os Windows XP e Server 2003 falam RDP5, enquanto o Vista e o futuro Server 2008 falam RDP6. A versão atual do Rdesktop é a 1.5.0, usada nos exemplos deste artigo.

Por último, o VirtualBox[7], fabricado pela alemã Innotek, também faz uso do RDP. A Innotek inclui nas duas versões do Virtualbox – a de Código Aberto, chamada de *OSE*, e a proprietária, com recursos adicionais – a capacidade de acesso remoto via RDP para qualquer máquina virtual em execução sob o sistema, independente do sistema operacional hóspede.

Para ativar o acesso remoto a uma máquina virtual do VirtualBox, basta abrir as configurações da máquina virtual específica e selecionar o último item de configuração na lista à esquerda, *Tela Remota*. Após marcar a caixa *Habilita o servidor VRDP*, é possível configurar a porta a ser usada para acesso a essa máquina por RDP, o método de autenticação e o tempo máximo para esse procedimento (**figura 3**).

Acesso remoto

Para se conectar a um servidor Windows, simplesmente inicie o Rdesktop com o nome do servi-

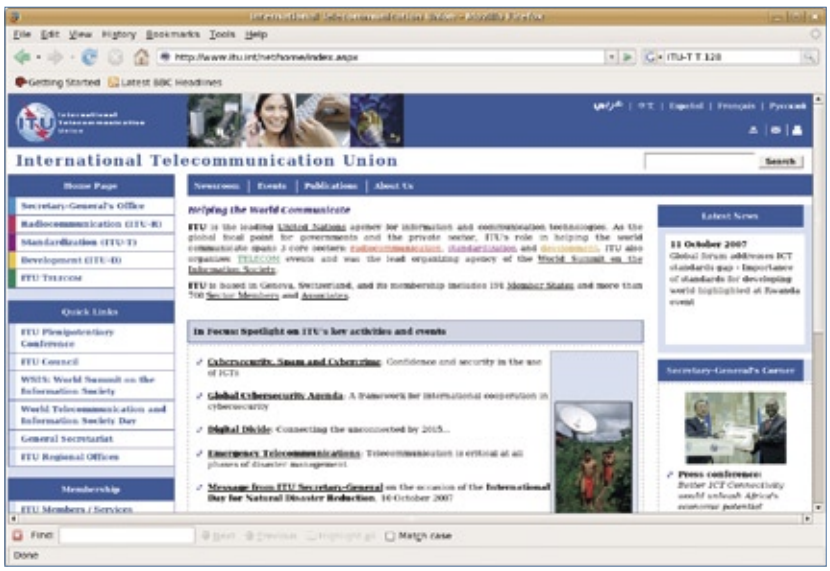


Figura 2 O *RDP* é uma extensão do protocolo *T.128* da ITU.

dor como parâmetro. O programa escolherá automaticamente a profundidade de cor e o layout de teclado adequados. Os usuários podem alterar essas configurações através de opções de linha de comando. O Rdesktop também aceita nomes de usuários e senhas, mas é importante considerar as implicações de segurança ao digitar uma senha na linha de comando. Uma típica linha de comando do Rdesktop é semelhante a:

```
$ rdesktop -a 16 -x l
➥ -g 1200x900 -u Administrador
➥ Windows_Terminal_Server
```

A opção `-a 16` seleciona a profundidade de cor de 16 bits. As políticas do Windows não permitem uma profundidade maior por padrão, mas é possível contornar essa restrição nas opções de grupo para seu domínio. A configuração se localiza no item *Computador | Serviços de Terminal | Rdesktop*. Como o Rdesktop usa uma resolução padrão de 800x600, e isso pode dificultar o trabalho com a máquina Windows remota, é bom especificar um valor mais alto com o parâmetro `-g`.

As interfaces gráficas, como *Grdesktop*[8], *TSClient*[9] e *KRDesktop*[10],eliminam a necessidade da linha de comando. Entretanto, não oferecem todos os recursos do Rdesktop, e por isso a ferramenta de linha de comando é preferida por muitos administradores.

Conexões lentas

Apesar das larguras de banda de menos de 100 MBps estarem tornando-se raras nas LANs atuais, ainda têm um importante papel como linhas de gerenciamento redundantes na infraestrutura profissional de TI. Devido às baixas taxas de transmissão, mecanismos que aglutinam o máximo de dados possível num pacote são tão importantes, nesse caso, quanto com linhas discadas ou ISDN.

A opção `-z` da linha de comando do Rdesktop comprime os dados como pré-requisito para conexões em redes lentas. Porém, o uso do parâmetro `-x` na conexão com os parâmetros `b`, `l` ou `m` para otimizar a conexão pode economizar muito mais largura de banda.

O parâmetro `-P` guarda no disco rígido bitmaps muito recorrentes, o que pode causar um atraso ao se estabelecer uma conexão. A opção `-b` evita operações baseadas em caracteres no lado cliente, forçando o servidor a atualizar a tela inteira como um bitmap.

O Rdesktop utiliza o que se conhece como *backing store* para armazenar seções de telas que já tenham sido renderizadas, acelerando assim o redesenho de telas.

A opção `-B` faz o software usar o backing store do servidor X em lugar do seu próprio; para isso funcionar, é preciso ativar a opção `"BackingStore" "true"` no arquivo `xorg.conf`.

Redirecionamento de dispositivos

O redirecionamento de dispositivos oferece ao servidor remoto acesso à impressora local, assim como às portas seriais e paralelas, saída de som e sistema de arquivos. Isso funciona perfeitamente com o Rdesktop no Linux: a opção `-r`, seguida de `disk`, `lptport impressora` ou `sound`, ativa o compartilhamento desses recursos. Por exemplo, `disk:share=/home/usuário/compartilhado` compartilha o diretório especificado, sob o nome *share*. Compartilhamentos são úteis caso se precise instalar, por exemplo, um *service pack* em múltiplas máquinas Windows, e o arquivo com este tenha sido baixado no cliente local (veja também o **quadro 1**).

SeamlessRDP

Como dito acima, o Rdesktop também permite a exibição de um aplicativo Windows individual, em vez

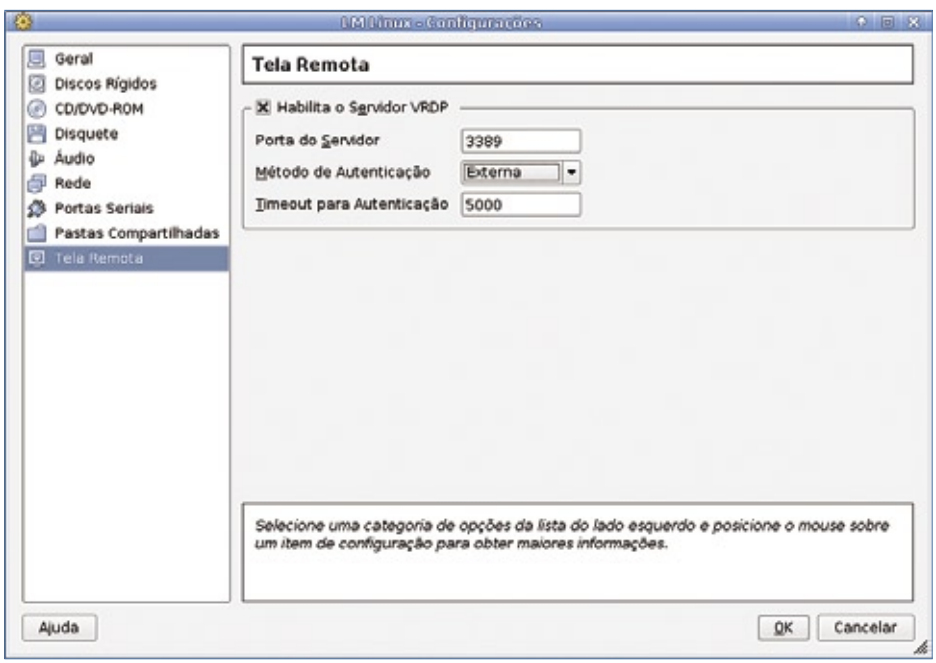


Figura 3 O VirtualBox oferece acesso remoto por RDP a qualquer máquina virtual hospedada por ele.

do desktop completo. Para isso, basta passar a opção `-s` para o Rdesktop e especificar o nome do aplicativo a ser iniciado no lugar do `Explorer.exe`. O aplicativo iniciado pelo SeamlessRDP é a shell GPL da Cendio[2].

Para instalar, descompacte o arquivo *ZIP*[11], copie seu conteúdo para um diretório do sistema Windows e lembre-se do caminho. O Rdesktop termina o trabalho no Linux, com o seguinte comando:

```
rdesktop -u Administrador
➥-A -s "C:\seamlessrdp
➥seamlessrdpshell.exe mmc.exe"
➥servidor
```

O `-A` informa ao Rdesktop tratar-se de uma conexão do SeamlessRDP. O `-u Administrador` dá privilégios administrativos. Antes de iniciar o Management Console, a tela de login do Windows aparecerá na janela do Rdesktop. Dessa forma, pode-se rodar qualquer executável proveniente do Windows.

Os arquivos *MSC* criados com o uso do Management Console, assim como arquivos `.doc`, não podem ser diretamente abertos por referência ao tipo de documento e aplicativo. Se o arquivo `.exe` não estiver no caminho de executáveis do Windows, será necessário especificar o caminho completo. Diferentemente do Windows, é importante usar letras maiúsculas para as unidades. Se a shell do SeamlessRDP não puder ser iniciada, a conexão entrará no modo desktop padrão. Ao acessar o Windows XP, note que a mudança rápida de usuários e a tela de boas vindas estão ativas na página inicial do Windows.

Substituições

O Rdesktop com ou sem SeamlessRDP pode facilitar a administração de máquinas Windows em ambientes heterogêneos: é fácil compartilhar arquivos guardados centralmente no cliente para tarefas em múltiplos servidores. O intercâmbio de dados pela área de transferência funciona bem até mesmo entre diferentes plataformas. Pode-se até redirecionar a saída da impressora ou do som, com a restrição de que somente duas conexões RDP estão disponíveis simultaneamente. O Rdesktop exibe quaisquer aplicativos Windows no Linux sem reduzir sua funcionalidade, embora se possa esperar alguns engasgos no modo de janela única ao usar o SeamlessRDP. ■

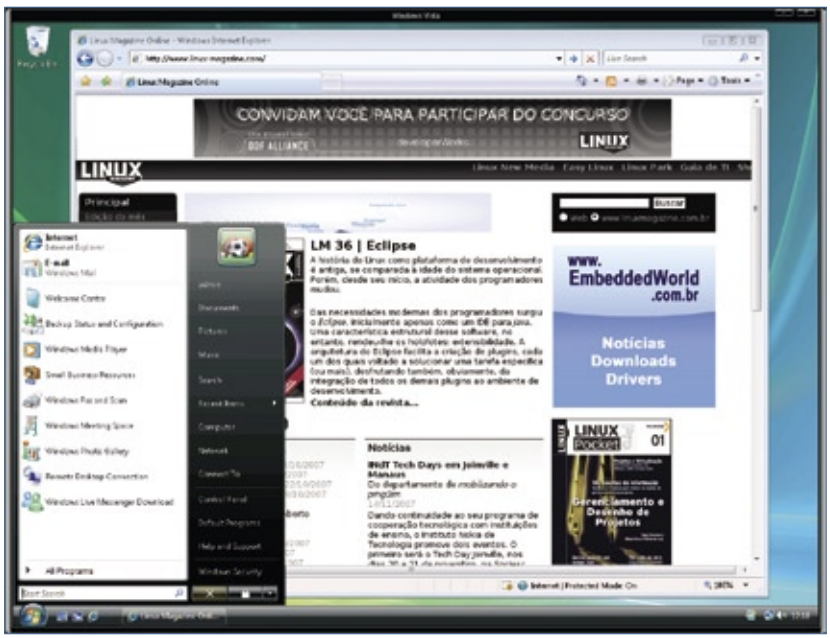


Figura 4 As aparências enganam: este não é um sistema Vista. O que se vê é o Rdesktop exibindo o Windows em modo de tela cheia no Linux.

Mais informações

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

[2] SeamlessRDP, da Cendio: http://www.cendio.com/seamlessrdp/

[3] T.120 (em inglês): http://en.wikipedia.org/wiki/T.120

[4] ITU: http://www.itu.int

[5] Citrix Terminal Server: http://www.citrix.com

[6] NX, da NoMachine: http://www.nomachine.com/

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

[8] Grdesktop: http://savannah.nongnu.org/projects/grdesktop

[9] TSClient: http://freshmeat.net/projects/tsclient/

[10] KRDesktop: http://krdesktop.sourceforge.net/

[11] Download do SeamlessRDP: http://tinyurl.com/293rcg

Sobre o autor

Markus Klimke é engenheiro de sistemas no Centro de Processamento de Dados da Universidade Técnica de Hamburgo-Harburgo, na Alemanha, e é responsável pela integração de sistemas.

Sexta aula da preparação LPIC-2

LPI nível 2: Aula 7

TUTORIAL

Tarefas rotineiras de manutenção, tanto no âmbito do hardware quanto do software.

por Luciano Siqueira

Tópico 214: Resolução de problemas

2.214.2 Criando discos de recuperação

Discos de recuperação são ferramentas indispensáveis para iniciar sistemas com o setor de boot danificado. Além de ser capaz de iniciar um sistema nesse estado, um disco de boot pode conter ferramentas para recuperá-lo.

Mesmo com a maioria dos kernels atuais não mais cabendo num disquete, ainda é possível criar um disquete de boot com o lilo.

Primeiro, o disquete deverá ser formatado e ter um sistema de arquivos:

```
# fdformat /dev/fd0h1440
```

Usando o sistema de arquivos `minix`:

```
# mkfs -t minix /dev/fd0
```

Montando o disquete:

```
# mount /dev/fd0 /mnt/floppy
```

É necessário criar um arquivo de configuração do lilo alternativo, como `/boot/lilo.floppy`, contendo as informações necessárias para criação do disquete de boot:

```
boot = /dev/fd0         # O
➥dispositivo de disquete
map = /mnt/floppy/map
compact
image = /boot/vmlinuz  #
➥Substituir para o kernel do
➥sistema
  root = /dev/hda1      # Partição
➥raiz do sistema
  read-only
```

Agora o Lilo pode ser instalado no disquete, usando o arquivo de configuração criado:

```
# lilo -C /boot/lilo.floppy
```

Desmontar o disquete:

```
# umount /mnt/floppy
```

O disquete de boot está pronto. É importante lembrar que disquetes de boot criados dessa forma só funcionarão na própria máquina onde foram feitos. Caso sejam feitas alterações no kernel ou localização da partição raiz, as configurações deverão ser adequadas e o Lilo reinstalado no disquete.

Geralmente é necessário alterar a seqüência dos dispositivos de boot no BIOS da máquina sempre que um dispositivo de boot alternativo for utilizado.

```
GRUB Loading stage1.5.

GRUB loading, please wait...
_
```

Figura 1 Mensagem exibida durante a execução do carregador GRUB.

Para fazer o backup da MBR, basta copiar os primeiros 512 bytes do disco, o que pode ser feito usando o comando `dd`:

```
# dd if=/dev/hda of=mbr.backup
➥bs=1b count=512
```

Este backup pode ser guardado num disquete e depois restaurado para o setor MBR:

```
# dd if=mbr.backup of=/dev/hda
```

2.214.3 Identificação dos estágios de boot

A inicialização de um sistema Linux pode ser dividida em quatro estágios principais:

1. Carregamento do kernel pelo Lilo ou Grub
2. Inicialização do kernel
3. Identificação de configuração do hardware
4. Disparo dos daemons

O primeiro estágio é o mais breve dos quatro. O BIOS do sistema executa as informações encontradas no setor de boot no dispositivo marcado como boot primário. Se o carregador de boot estiver instalado corretamente num dos dispositivos indicados, o mesmo será disparado (**figura 1**).

Neste caso, o carregador de boot utilizado é o GRUB. Em seguida, o kernel será carregado ou aparecerá um menu com as opções de kernels e outros sistemas operacionais porventura instalados no computador. Essa última é o comportamento padrão na maioria das distribuições Linux (**figura 2**).

Como descrito nas instruções do menu, basta pressionar **[Enter]** ou aguardar 5 segundos para que a primeira opção seja utilizada.

O carregador de boot, como o nome sugere, carregará o kernel, que passará a ter o controle sobre o computador. Algumas informações básicas passadas ao kernel pelo carregador de boot serão mostradas na tela e o processo de carregamento terá início (**figura 3**).

Neste momento o kernel será iniciado. A partir dessas informações podemos verificar que o dispositivo raiz indicado para o sistema será a primeira partição no primeiro disco (`hd0,0`), o sistema de arquivos identificado (`ext2fs`) e o tipo da partição (`0x83` - Linux). Também é mostrada qual imagem do kernel será utilizada (`/boot/vmlinuz-2.6.18-4-686`) e a imagem (se houver) initrd (`/boot/initrd.img-2.6.18-4-686`).

Assim que o kernel assume o controle, informações conseguidas junto ao BIOS e outras informações de hardware são mostradas na tela. É um processo muito rápido e dificilmente pode ser acompanhado (**figura 4**).

O hardware fundamental do sistema, como portas seriais, teclado e mouse, será então iniciado (**figura 5**).

Outros itens de hardware sendo identificados e minimamente configurados, como barramentos, discos rígidos e dispositivo de rede (**figura 6**).

Assim que a identificação inicial do hardware terminar e a partição raiz for montada, o `init` será disparado e as configurações mais avançadas de hardware e os daemons serão iniciados. Neste estágio, entre outros procedimentos, são montadas as demais partições, inclusive a partição swap, conforme constadas em `/etc/fstab` (**figura 7**).

Continuando a última etapa, demais daemons de serviços são disparados e o usuário poderá ingressar no sistema (**figura 8**).

2.214.4 Resolvendo problemas no carregador de boot

O carregador de boot pode deixar de funcionar corretamente por uma variedade de fatores, como remoção do kernel, defeito no sistema de arquivos, entre outros.

O processo de boot acontece em dois estágios. O primeiro estágio do Lilo consiste num único setor carregado pelo BIOS, que por sua vez carrega o segundo estágio do Lilo; o carregador Lilo multi-setor. O Lilo é capaz de informar ao administrador a natureza do erro ocorrido, sinalizando no momento em que é carregado.

Quando o primeiro estágio está ativo, é mostrada a letra "L". Assim que o primeiro estágio for invocar o segundo estágio, é mostrada a letra "I". Neste momento, caso ocorra al-

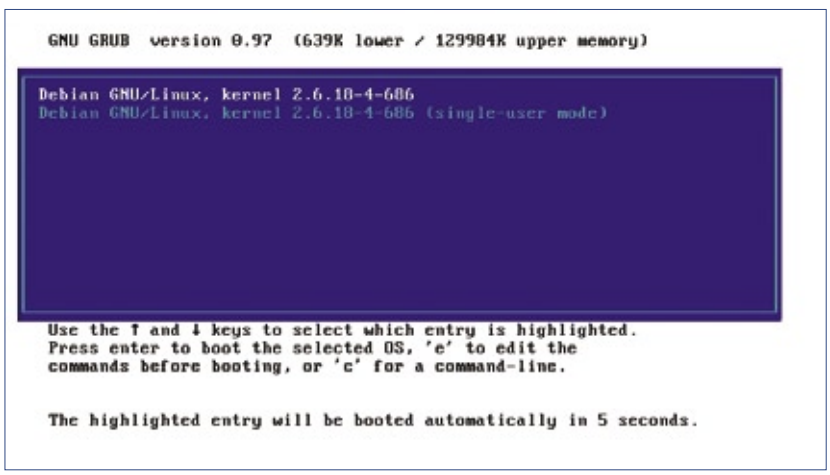


Figura 2 O menu do GRUB pode exibir múltiplas opções de kernels e sistemas operacionais.

```
  Booting 'Debian GNU/Linux, kernel 2.6.18-4-686'

root  (hd0,0)
 Filesystem type is ext2fs, partition type 0x83
kernel  /boot/vmlinuz-2.6.18-4-686 root=/dev/hda1 ro
   [Linux-bzImage, setup=0x1e00, size=0x131e9d]
initrd  /boot/initrd.img-2.6.18-4-686
   [Linux-initrd @ 0x7b18000, 0x4c7cb7 bytes]
savedefault

Uncompressing Linux... _
```

Figura 3 No processo de carregamento do kernel são mostradas algumas informações.

gum erro, um código hexadecimal é mostrado:

- 00: Nenhum erro
- 01: Comando de disco inválido
- 02: Indicador de endereço não encontrado
- 03: Disco protegido contra gravação
- 04: Setor não encontrado
- 06: Disquete removido
- 08: DMA overrun
- 0A: Setor defeituoso
- 0B: Trilha defeituosa
- 20: Falha no controlador
- 40: Falha no rastreio (BIOS)
- 40: Cilindro > 1023 (LILO)
- 99: Índice de setor inválido para o segundo estágio (LILO)
- 9A: Ausência de assinatura para o carregador de segundo estágio (LILO)
- AA: Drive não pronto
- FF: Falha geral

O erro 40 é gerado pelo BIOS ou pelo Lilo quando convertendo um endereço de disco linear (24bit) para um endereço geométrico (C:H:S). Os erros 99 e 9A geralmente ocorrem quando o arquivo de mapa não pôde ser lido. No caso de erro, o Lilo repetirá a operação, o que pode gerar o mesmo código de erro repetidas vezes.

Se o carregador de segundo estágio for carregado, será mostrada outra letra "L". Então, se a tabela de kernels e outros sistemas puder ser verificada, será mostrada a letra "O", completando a palavra "LILO", em maiúsculas. Mensagens de erro do carregador de segundo estágio são textuais.

Ainda, podem aparecer erros da seguinte forma:

- LIL?: O carregador de segundo estágio foi carregado num endereço incorreto;
- LIL-: A tabela de kernels está corrompida.

A maioria desses erros podem ser corrigidos simplesmente reinstalando o carregador de boot.

O carregador de boot GRUB proporciona recursos adicionais – em comparação ao Lilo – para a resolução de problemas de inicialização. O GRUB carrega na MBR um programa encarregado de ler, a partir de uma partição do disco rígido, as configurações de boot. Caso esse programa falhe, é iniciado um prompt que permite a execução de comandos para carregamento, por exemplo, de kernels ou discos RAM iniciais (initrd) alternativos, localizados em qualquer disco conectado ao sistema, contanto que use um sistema de arquivos legível pelo GRUB.

2.214.5 Resolução de problemas gerais

Apesar de existirem problemas realmente difíceis de diagnosticar e corrigir, a maioria das causas para uma interrupção de funcionamento do sistema são mais simples do que imagina. Muitas vezes, detalhes como um cabo mal conectado podem levar a crer que a configuração das rotas da rede ou o firewall estão com problemas.

Sempre que um problema surgir devem ser primeiro investigados os detalhes mais fundamentais do funcionamento do sistema, evitando embrenhar-se em configurações avançadas que podem não ser a causa dos problemas.

O primeiro passo é checar os logs e mensagens do kernel, buscando por possíveis avisos de erro. Dependendo do escopo da falha identificada, o log específico de um serviço em /var/log deve ser consultado. Mensagens do kernel, mostradas através do coman-

```
0MB HIGHMEM available.
127MB LOWMEM available.
DMI 2.3 present.
ACPI: PM-Timer IO Port: 0x4008
Allocating PCI resources starting at 10000000 (gap: 08000000:f7fc0000)
Detected 2134.743 MHz processor.
Built 1 zonelists.  Total pages: 32752
Kernel command line: root=/dev/hda1 ro
Found and enabled local APIC!
Enabling fast FPU save and restore... done.
Enabling unmasked SIMD FPU exception support... done.
Initializing CPU#0
PID hash table entries: 512 (order: 9, 2048 bytes)
Console: colour VGA+ 80x25
Dentry cache hash table entries: 16384 (order: 4, 65536 bytes)
Inode-cache hash table entries: 8192 (order: 3, 32768 bytes)
Memory: 121760k/131008k available (1544k kernel code, 8700k reserved, 577k data,
 196k init, 0k highmem)
Checking if this processor honours the WP bit even in supervisor mode... Ok.
Calibrating delay using timer specific routine.. 20353.96 BogoMIPS (lpj=40707928
)
Security Framework v1.0.0 initialized
SELinux:  Disabled at boot.
Capability LSM initialized
Mount-cache hash table entries: 512
```

Figura 4 As informações obtidas pelo kernel a partir da BIOS aparecem rapidamente no boot.

do dmesg, podem ajudar tanto no diagnóstico de problemas de hardware quanto de problemas de software.

Para verificar se dispositivos de hardware foram corretamente identificados pelo sistema, podem ser utilizados os comandos lspci e lsdev. Se o dispositivo suspeito de falha aparecer na listagem resultante, provavelmente trata-se de um erro de software.

Caso o dispositivo tenha sido corretamente identificado, mas ainda assim não funciona, o problema pode ser um módulo não existente ou não carregado. Com o comando uname -r é mostrada a versão do kernel utilizado. Verifique em /lib/modules se existe um diretório de módulos para a versão do kernel em questão. Este tipo de problema é comum quando se esquece de instalar os módulos após instalar um kernel.

Se o módulo do dispositivo não for carregado automaticamente, inclua nos scripts de inicialização o comando /sbin/modprobe nome_do_modulo. Consulte na documentação do kernel – /usr/src/linux/Documentation, se o código fonte do kernel estiver instalado – o nome do módulo para o dispositivo em questão.

```
Begin: Loading essential drivers... ...
Done.
Begin: Running /scripts/init-premount ...
Uniform Multi-Platform E-IDE driver Revision: 7.00alpha2
ide: Assuming 33MHz system bus speed for PIO modes; override with idebus=xx
PIIX3: IDE controller at PCI slot 0000:00:01.1
PIIX3: chipset revision 0
PIIX3: not 100% native mode: will probe irqs later
    ide0: BM-DMA at 0xc000-0xc007, BIOS settings: hda:DMA, hdb:DMA
    ide1: BM-DMA at 0xc008-0xc00f, BIOS settings: hdc:DMA, hdd:DMA
pcnet32.c:v1.32 18.Mar.2006 tsbogend@alpha.franken.de
hda: VBOX HARDDISK, ATA DISK drive
hdb: VBOX HARDDISK, ATA DISK drive
ide0 at 0x1f0-0x1f7,0x3f6 on irq 14
hdc: VBOX CD-ROM, ATAPI CD/DVD-ROM drive
hdd: VBOX HARDDISK, ATA DISK drive
ide1 at 0x170-0x177,0x376 on irq 15
ACPI: PCI Interrupt Link [LNKC] enabled at IRQ 11
ACPI: PCI Interrupt 0000:00:03.0[A] -> Link [LNKC] -> GSI 11 (level, low) -> IRQ
 11
pcnet32: PCnet/FAST III 79C973 at 0xc020, 08 00 27 28 92 5d assigned IRQ 11.
pcnet32: Found PHY 0000:0000 at address 0.
eth0: registered as PCnet/FAST III 79C973
pcnet32: 1 cards_found.
_
```

Figura 6 Identificação de outros itens de hardware do sistema, como barramento, discos rígidos e placa de rede.

Um erro pode ainda ser provocado por programas buscando recursos não disponíveis, como bibliotecas não instaladas. O comando strace é capaz de rastrear todas as chamadas de sistema feitas por um programa. Basta fornecer o nome do comando como argumento para strace e todas as chamadas de sistema feitas por ele serão mostradas na tela. Para rastrear um programa já em execução, utilize a opção -p PID, com o PID do programa em questão.

Com propósito parecido ao do strace, o ltrace intercepta e mostra todas as chamadas que um programa faz para bibliotecas dinâmicas. Também pode ser utilizada a opção -p para fornecer o PID de um processo existente.

Para investigar quem ou quais processos estão utilizando um determinado arquivo, é usado o comando lsof. Na medida que, em ambientes Unix, praticamente todos os recursos podem ser acessados através de arquivos ou pseudo-arquivos, o lsof é uma ferramenta de investigação bastante poderosa.

Por exemplo, é possível listar todos os arquivos abertos por um determinado processo utilizando o comando:

```
lsof -p PID
```

Onde PID representa o PID do programa em questão. Para verificar todos os arquivos sendo utilizados por processos disparados por um usuário em particular, utiliza-se a opção -u usuário. Para checar quais processos estão utilizando um arquivo, basta executar o comando lsof fornecendo como argumento o caminho completo para o arquivo:

```
# lsof /dev/net/tun
COMMAND    PID    USER   FD   TYPE
➥DEVICE SIZE NODE NAME
VBoxVRDP 25874 luciano   12u   CHR
➥10,200      7885 /dev/net/tun
VBoxVRDP 25922 luciano   12u   CHR
➥10,200      7885 /dev/net/tun
```

```
Activating ISA DMA hang workarounds.
isapnp: Scanning for PnP cards...
isapnp: No Plug & Play device found
Serial: 8250/16550 driver $Revision: 1.90 $ 4 ports, IRQ sharing enabled
RAMDISK driver initialized: 16 RAM disks of 8192K size 1024 blocksize
PNP: PS/2 Controller [PNP0303:PS2K,PNP0f03:PS2M] at 0x60,0x64 irq 1,12
serio: i8042 AUX port at 0x60,0x64 irq 12
serio: i8042 KBD port at 0x60,0x64 irq 1
mice: PS/2 mouse device common for all mice
PM-Timer running at invalid rate: 170% of normal - aborting.
TCP bic registered
NET: Registered protocol family 1
NET: Registered protocol family 17
NET: Registered protocol family 8
NET: Registered protocol family 20
Using IPI No-Shortcut mode
Time: tsc clocksource has been installed.
input: AT Translated Set 2 keyboard as /class/input/input0
ACPI: (supports S0 S5)
Freeing unused kernel memory: 196k freed
Loading, please wait...
Begin: Loading essential drivers... ...
Done.
Begin: Running /scripts/init-premount ...
_
```

Figura 5 Inicialização do hardware fundamental do sistema, como teclado, mouse e portas seriais.

A saída deste comando mostra várias informações úteis sobre o(s) processo(s) a acessar o arquivo `/dev/net/tun` (interface de rede TUN). Este uso é especialmente útil para checar processos bloqueando dispositivos ou pontos de montagem.

2.214.6 Problemas em recursos do sistema

Configurações mal feitas no ambiente do shell também podem causar falhas no funcionamento do sistema ou mesmo travamento total. Mesmo aplicações do modo gráfico, como navegadores e editores de texto, poderão não funcionar se algumas variáveis do shell não estiverem corretamente especificadas.

Variáveis de ambiente

As variáveis de ambiente principais do shell são utilizadas pela maioria dos programas. Os padrões para o sistema são especificados no arquivo `/etc/profile` e `/etc/bashrc`. As principais variáveis globais são:

- `PATH`: Lista de diretórios, separados por dois-pontos, onde programas requisitados serão procurados. A menos que o programa em questão possa ser encontrado num dos diretórios na variável, o mesmo só poderá ser executado fornecendo seu caminho completo na árvore de diretórios;
- `LANG`: Idioma padrão do sistema. Usado inclusive pelo seu ambiente gráfico;

```
Done.
INIT: version 2.86 booting
Starting the hotplug events dispatcher: udevd.
Synthesizing the initial hotplug events...done.
Waiting for /dev to be fully populated...input: PC Speaker as /class/input/input
1
Floppy drive(s): fd0 is 1.44M
FDC 0 is a S82078B
input: ImExPS/2 Generic Explorer Mouse as /class/input/input2
ACPI: PCI Interrupt Link [LNKA] enabled at IRQ 9
ACPI: PCI Interrupt 0000:00:05.0[A] -> Link [LNKA] -> GSI 9 (level, low) -> IRQ
9
ts: Compaq touchscreen protocol output
intel8x0_measure_ac97_clock: measured 25465 usecs
intel8x0: measured clock 87453 rejected
intel8x0: clocking to 48000
done.
Activating swap...Adding 321260k swap on /dev/hda7.  Priority:-1 extents:1 acros
s:321260k
done.
Checking root file system...fsck 1.40-WIP (14-Nov-2006)
/dev/hda1: clean, 10421/68272 files, 113284/273072 blocks
done.
EXT3 FS on hda1, internal journal
_
```

Figura 7 O processo *INIT* é iniciado após a identificação do hardware, e lança os *daemons* de serviço.

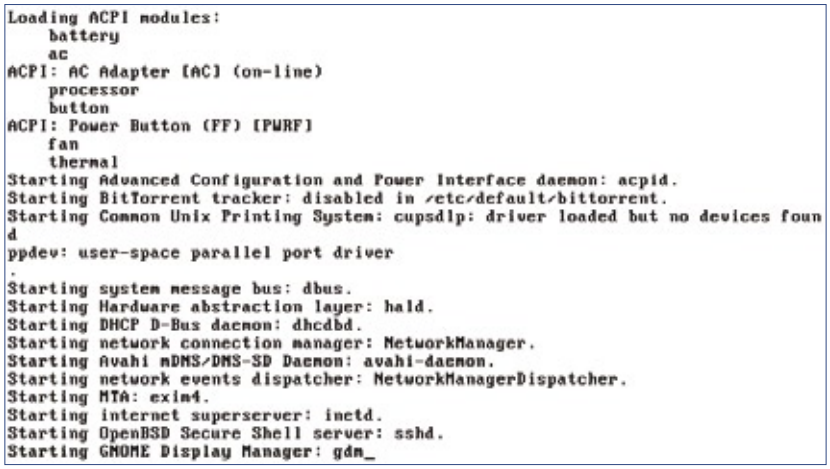


Figura 8 Mensagens emitidas pela execução dos *daemons* de serviço.

- `EDITOR`: Especifica qual é o editor de textos padrão utilizado no console;
- `PAGER`: O paginador usado no console, como o less ou more.

A lista completa de variáveis globais pode ser obtida executando o comando `env`:

```
# env
SHELL=/bin/bash
TERM=xterm
USER=root
MAIL=/var/mail/root
PATH=/usr/local/sbin:/usr/local/
➥bin:/usr/sbin:/usr/bin:/sbin:/
➥bin
PWD=/root
LANG=pt_BR.UTF-8
PS1=\h:\w\$
SHLVL=1
HOME=/root
LANGUAGE=pt_BR:pt:en
LOGNAME=root
_=/usr/bin/env
OLDPWD=/etc
```

Semelhante a variável `PATH`, que determina onde são encontrados os comandos, a variável `LD_LIBRARY_PATH` pode ser utilizada para especificar onde podem ser encontradas as bibliotecas de sistema. Porém, essa variável não é utilizada por padrão (apenas em circunstâncias pontuais). Em seu lugar, os caminhos para as bibliotecas de sistema devem ser especificados no arquivo `/etc/ld.so.conf`:

```
/usr/local/lib
/usr/X11R6/lib
/opt/kde/lib
/usr/lib/qt/lib
```

Caso alguma alteração seja feita neste arquivo, é necessário executar o comando `ldconfig`, que regenerará o arquivo binário `/etc/ld.so.cache`, onde são armazenados os endereços das bibliotecas.

Opções do Kernel

O kernel também possui algumas opções que influem diretamente no funcionamento de programas. São opções como `ip_forward`, que determina se o sistema deve agir como um roteador de pacotes IP. Essas opções podem ser alteradas sem reiniciar o sistema, editando diretamente os arquivos sob o diretório `/proc/sys` ou através do comando `sysctl`. Este mesmo comando, `sysctl`, pode ser utilizado para mostrar todas as opções possíveis e seus valores, através do comando `sysctl -a`.

A sintaxe do comando `sysctl` para alterar parâmetros é:

```
sysctl -w net.ipv4.ip_forward=1
```

Deve ser fornecida a opção `-w` para alterar a opção indicada, caso contrário será mantido o valor atual. Esses valores podem ser mantidos incluindo as mudanças no arquivo `/etc/sysctl.conf`, no formato `nome_variável=valor`.

2.214.8 Configurações de ambiente

Alguns problemas de login podem ocorrer quando se editam os arquivos `/etc/passwd`, `/etc/shadow` ou `/etc/group` diretamente. Se um destes arquivos estiver corrompido, o login poderá não acontecer. Por esse motivo, estes arquivos devem ser editados através dos comando especializados `vipw` e `vigr`, que utilizam o editor padrão do sistema (na maioria das distribuições, o *vi* ou seu descendente *vim*) e evitam que o arquivo seja alterado por outro comando ou usuário durante a edição.

Usuários podem não conseguir entrar no sistema se suas contas estiverem bloqueadas. As contas de usuários podem ser bloqueadas se estiver presente a exclamação no lugar da senha em `/etc/shadow` ou se o shell padrão apontar para `/bin/false`, por exemplo.

Outras configurações referentes ao modo e à segurança do login podem ser feitas no arquivo `/etc/login.defs`. Por exemplo, valores padrão para validade de contas e número máximo de tentativas de login. Importante lembrar que algumas opções deste arquivo podem estar em desuso se for utilizado outro sistema de autenticação, como o PAM.

Considerações sobre o tópico

Saiba diferenciar as variadas mensagens da inicialização, de forma que falhas possam ser identificadas e corrigidas. Conheça a localização dos arquivos de log do sistema e a utilização dos diferentes carregadores de boot e scripts de inicialização. ■

O sistema de arquivos distribuído Lustre

Ilustres arquivos

Sistemas de arquivos comuns não são capazes de fornecer o alto desempenho exigido por algumas aplicações. O Lustre é um sistema de arquivos distribuído otimizado para HPC.

por Oliver Tennert

Francis Valadj - www.sxc.hu

A computação de alta performance é, ao que parece, uma luta constante contra a ineficiência. Inicialmente, o artigo em falta era o poder de processamento. Com a criação dos clusters de PCs, isso foi resolvido. Mas somente até ser descoberto o novo gargalo: a rede. A solução para esse novo problema está nas redes de alto desempenho, como Quadrics Elan[1], Rapid Array, Myrinet[2] da Myricom ou Infiniband [3]. Como de costume, o gargalo então é transferido a um outro ponto, o espaço de armazenamento.

Resultados de cálculos com terabytes de tamanho não são raros; na verdade, servidores de arquivo sobrecarregados são a regra. Como não apenas a entrada de dados cresce, mas também o tamanho de cada um dos arquivos, não adianta simplesmente exportá-los por NFS. É preciso que haja muito mais espaço livre disponível em um ou possivelmente alguns poucos sistemas de arquivos para evitar a exaustiva cópia de dados. Além disso, o sistema de arquivos precisa estar disponível em todos os nós do cluster, e deve utilizar as redes de alta velocidade para o transporte de dados.

A solução é o Lustre

Quem busca uma solução para esse problema dificilmente escapará do *Lustre*[4], um sistema de arquivos distribuído que a empresa norte-americana Cluster File Systems[5] comercializa e desenvolve, e que foi disponibilizado sob a Licença GPL. O nome do software corresponde apenas por acaso ao termo *lustre* em português. Na verdade, ele é uma brincadeira com as palavras *Linux* e *cluster* – caracterizado pelo sistema operacional predileto do sistema de arquivos compartilhado.

Entre os clusters da lista dos 500 supercomputadores mais poderosos[6] ele desfruta de grande aceitação. Até mesmo o Blue Gene/L, primeiro colocado, abriga seus dados com a ajuda do Lustre.

Mas não imagine que essa escolha dos fabricantes de supercomputadores é óbvia. A IBM, por exemplo, produz um sistema de arquivos concorrente, o *GPFS*[7], muito semelhante em projeto ao Lustre, mas com mais funções, como backup e uma administração de memória hierárquica. Os desenvolvedores do Lustre, no entanto, não têm em vista todos esses recursos, mas apenas o alto desempenho (**figura 1**).

Comunicação em LNET

Embora vise primordialmente ao mercado clusters, o Lustre não é um sistema de arquivos para clusters no sentido mais estrito. Esse termo costuma denotar sistemas de arquivos através dos quais vários computadores acessam simultaneamente um dispositivo de bloco comum, como

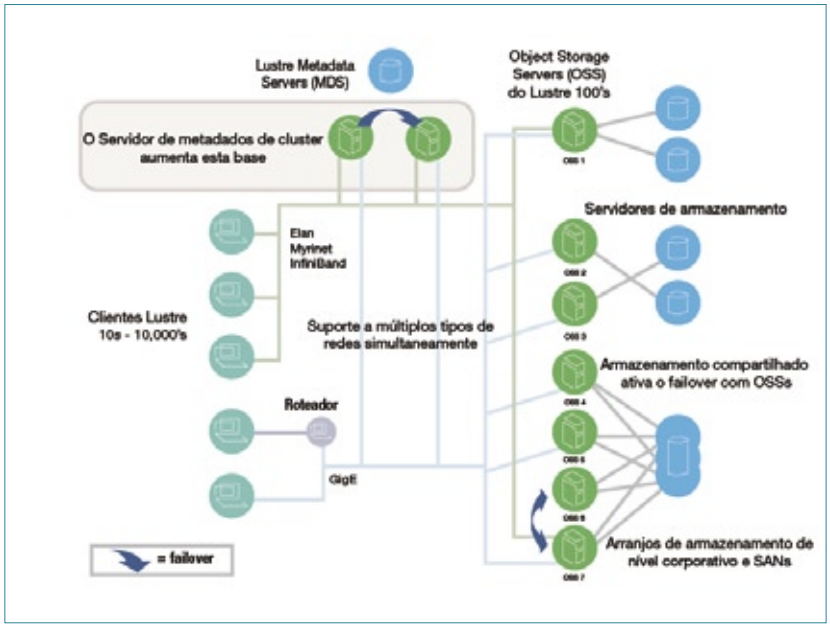


Figura 1 Construção esquemática de um cluster *Lustre* com as proteções contra falha necessárias.

em uma SAN por fibra óptica ou iSCSI, ou ainda a partir de várias máquinas virtuais.

Representantes dessa categoria, como o *GFS*[8] e o *OCFS2*[9] são freqüentemente empregados nos clusters de alta disponibilidade, e mais raramente em clusters de alto desempenho, uma vez que dispõem de escalabilidade limitada e custos elevados devido à exigência do canal de fibra óptica.

A arquitetura do Lustre, pelo contrário, segue o modelo de sistemas de arquivos compartilhados, como o *AFS*[10] ou o *pNFS*[11] (NFS paralelo). Eles reúnem localmente os dados existentes em vários computadores em uma única árvore de sistema de arquivos. Por último, um dispositivo de bloco armazena os dados, mas, diferentemente dos sistemas de arquivos para clusters, apenas um determinado computador acessa cada dispositivo de bloco. O acesso concorrente é regulado pelas camadas mais altas do software.

Para utilizar dados de um sistema Lustre, o cliente deve primeiro requisitá-los a um servidor de metadados, que informa onde os dados desejados se encontram, para que eles sejam obtidos numa segunda etapa. Todas as máquinas envolvidas empregam o protocolo especial do Lustre para essa finalidade, o *LNET*, que suporta não apenas o óbvio TCP/IP, mas também se comunica diretamente por meio de redes de alto desempenho, como as já citadas Infiniband, Quadrics ou Myrinet.

No jargão do Lustre, os drivers LNET para os diferentes tipos de rede em sua maioria chamam-se abreviadamente de *LND*. Os demais componentes do sistema Lustre também adotam diversas abreviações de três letras: o servidor de metadados costuma chamar-se *MDS* e os dados propriamente ditos residem em *Object Storage Servers* (*OSS*). Para isso, existe ainda um servidor de gerenciamento (*MGS*) que administra todas as informações de configuração de maneira centralizada (**figura 2**).

Para a tarefa de requisitar os dados aos servidores, cada um desses componentes possui também um software cliente: *MGCs*, *MDCs* e *OSCs*. Depois, a coisa fica um pouco mais complicada, pois o servidor, na terminologia do Lustre, é apenas o computador que oferece um determinado serviço. Os programas correspondentes em um servidor respondem pelo nome *Target*, ou, abreviadamente, *MGT*, *MDT* e *OST*. Partições de dados nos servidores de armazenamento chamam-se *Object Storage Devices* (*OSD*); um sistema de arquivos Lustre completo é chamado *Logical Object Volume* (*LOV*). Para se usar o Lustre, essas abreviações são inevitáveis.

Exemplo 1: Instalação de um sistema de arquivos de backend

```
01 root@metanode # mkfs.lustre --fsname ex1fs --mdt --mgs /dev/
➥sda1
02 Permanent disk data:
03 Target: ex1fs-MDT0000
04 Index: unassigned
05 Lustre FS: ex1fs
06 Mount type: ldiskfs
07 Flags: 0x75 (MDT MGS needs_index first_time update)
08 Persistent mount opts: errors=remount,ro,iopen_nopriv,
➥user_xattr
09 Parameters:
10 checking for existing Lustre data: not found
11 device size = 4096MB
12 formatting backing filesystem ldiskfs on /dev/sda1
13 target name examplefs-MDT0000
14 4k blocks 0
15 options -J size=160 -i 4096 -I 512 -q -O dir_index -F
16 mkfs_cmd = mkfs.ext2 -j -b 4096 -L ex1fs-MDT0000 -J \
17 size=160 -i 4096 -I 512 -q -O dir_index -F /dev/sda1
18 Writing CONFIGS/mountdata
```

Acesso de dois níveis

A princípio, o acesso a dados em um sistema de arquivos Lustre transcorre em dois níveis: primeiro o cliente realiza a conexão com o MDS. Com isso, obtém as informações sobre os metadados, como quais arquivos e diretórios estão disponíveis, ou quais seus direitos de acesso. Sobretudo, ele compartilha com o MDS quais são os nós OSS responsáveis pelo conteúdo de um arquivo desejado. O cliente então lê e escreve seus arquivos diretamente nos OSTs para o MDS sem demais rodeios.

O velho sistema AFS funciona da mesma forma. Diferentemente do AFS, no entanto, o Lustre armazena nos OSSs não os arquivos completos, mas os chamados objetos, que são fragmentos com apenas uma parte dos dados originais. Dessa forma, um arquivo pode ser dividido em mais de um OST.

O cliente busca os fragmentos dos OSTs e os recompõe na forma do arquivo original de maneira transparente para o usuário. O princípio é comparável ao de um arranjo *RAID* 0, que separa os dados dos *stripes* em diversos discos rígidos (**figura 3**). Com isso, o fluxo de dados aumenta e, além disso, esse princípio possibilita o armazenamento de arquivos maiores do que as partições de cada um dos OSTs.

O servidor de gerenciamento citado anteriormente não é propriamente uma parte do sistema Lustre, mesmo quando executado no mesmo computador que abriga um MDS. O MGS entra em jogo somente no início. Independentemente se o cliente é MDS, OSS ou Lustre, qualquer outro serviço primeiro assume o contato com o MGS, e então recebe todas as informações de configuração que faltam.

Caso um cliente deseje montar um sistema de arquivos Lustre, por exemplo, o comando de montagem conterá o nome do MGS. O comando então encaminha o cliente, por meio do nome do sistema de arquivos, junto com o processo de montagem propriamente dito, ao MDS responsável. O serviço de gerenciamento é um recurso da nova versão 1.6 do Lustre. Anteriormente, era preciso dividir um arquivo com as informações de configuração para todos os computadores envolvidos e mantê-los sincronizados.

Preparação e instalação

O Lustre consiste, em grande parte, em módulos e *patches* para o kernel Linux. A maioria dos patches se refere ao sistema de arquivos virtual.

Mesmo usuários experientes podem ter dificuldades com o uso do Lustre no kernel. Por isso, é aconselhável baixar um dos kernels já alterados do site do projeto, mesmo que isso signifique usar uma versão um pouco ultrapassada do Linux e nem sempre dispor dos patches aplicados por sua distribuição preferida. O fabricante do Lustre suporta somente esses kernels que distribui, além das versões oficiais do *SLES* 9 e 10, e *RHEL* 4 e 5 (veja a **tabela 1**). Fora essas distribuições, somente o *Debian* oferece pacotes próprios de suporte ao Lustre.

O Lustre necessita também de um moderníssimo pacote *e2fsprogs*, acrescentado recentemente ao *Ext3* / *Ext4*, e ainda suporta um recurso experimental para o endereçamento baseado em extensões. A versão 1.39 desse pacote contém as novidades necessárias, e há também pacotes RPM com os *e2fsprogs* na página do Lustre.

Outros pré-requisitos para o uso do sistema de arquivos são a sincronização do relógio de todos os computadores envolvidos e a unificação dos IDs de usuários e grupos para autenticação. As versões preliminares do futuro Lustre 1.8 oferecem a possibilidade de autenticação por *Kerberos* no lugar de IDs.

Como o Lustre é implementado em grande parte através de módulos do kernel, ele não consegue acessar automaticamente os arquivos de configuração no sistema de arquivos normal. Por isso, versões anteriores utilizam a ferramenta especial de linha de comando `lconf` para transmitir as informações ao kernel. Na versão 1.6 os desenvolvedores criaram um novo método que, embora seja mais fácil de utilizar, parece conceitualmente duvidoso. O chamado *mountconf* é uma extensão dos famosos programas `mkfs`, `tunefs` e `mount`, visto que todos podem estabelecer parâmetros para um sistema de arquivos Lustre.

ldiskfs como back-end

O uso do *ldiskfs* como *back-end* possibilita a proibição de acesso dos usuários a partes do sistema de arquivos. O ldiskfs é um aprimoramento do sistema de arquivos Ext3, e também já está contido no kernel como parte do Ext4.

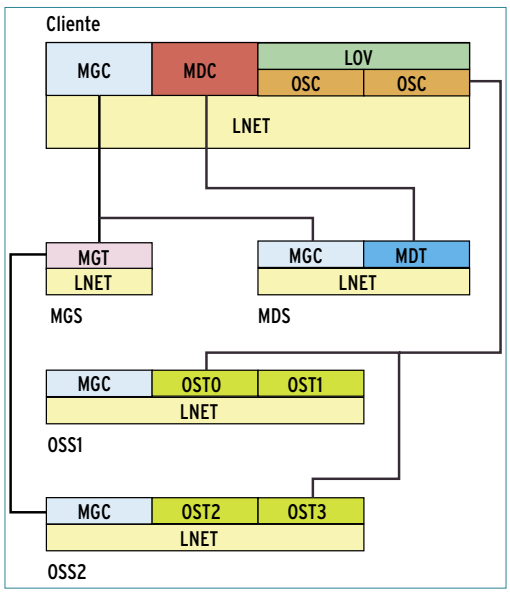


Figura 2 A interação dos diferentes componentes de servidor e respectivas clientes (LOV/OSC/LND, MDT/LND, OBD/OST/LND).

Quadro 1: LNET, o subsistema de rede do Lustre

Para desempenho de rede ótimo, o Lustre evita ao máximo a pilha TCP/IP do kernel. Para isso, utiliza recursos de *RDMA* de interconexões atuais para evitar, por meio do acesso direto à memória, a cópia desnecessária de dados e a sobrecarga da CPU.

Para isso, o Lustre implementa sua própria camada de abstração de rede *LNET*, que emprega LNDs (back-ends de drivers) para controlar os diferentes tipos de rede, como *Infiniband, Myrinet, Quadrics Elan, Rapidarray* e também o TCP/IP comum, tudo isso através da *Ethernet*. O LNET consegue rotear entre cada uma das redes, e assim, pode integrar, por exemplo, um cluster Myrinet a um sistema Infiniband.

IDs em vez de IPs

O Lustre não identifica um computador da maneira convencional, mas por meio de seu ID de rede de LNET (*NID*). Esse ID contém duas partes: a primeira se refere ao computador dentro da sub-rede, e a segunda é definida pela própria sub-rede. O formato exato depende do tipo de rede utilizada. Por exemplo, *42@elan0* é um nó com ID de sub-rede 42, conectado através da primeira interface Quadrics Elan, enquanto *192.168.16.21@tcp0* representa um nó com endereço IP 192.168.16.21.

O LNET utiliza o TCP como protocolo padrão caso o NID não contenha indicação da interface a usar, de forma que também se possa trabalhar facilmente com endereços IP e nomes de host. Nos exemplos deste artigo, o metanó 192.168.16.21 é abreviado para o NID `192.168.16.21@tcp0`.

Na parte de rede do NID, alguns LNDs usam uma convenção um pouco confusa: o driver *C2ib*, por exemplo, que controla placas Infiniband por meio da fila *OpenFabrics*, utiliza o endereço IP da interface *IPoIB*. Em virtude disso, o administrador precisa, em todo caso, ativar o *IP-over-Infiniband* nos nós envolvidos, mesmo que o Lustre não o utilize para comunicação, mas somente para identificar o computador e a porta IB desejados.

Configuração por módulo do kernel

A configuração LNET é feita totalmente por meio das opções dos módulos do kernel envolvidos. Nas configurações padrão, eles ativam somente o back-end TCP. Para se comunicar por redes de alta velocidade, é necessário fornecer os LNDs para o módulo *lnet* no parâmetro `networks`, como em `/etc/modprobe.conf`:

```
options lnet networks="tcp,o2ib"
```

Como alternativa, o administrador também pode fornecer ao módulo lnet, no parâmetro `ip2net`, uma tabela de modelos de endereço IP e os respectivos tipos de rede. O módulo verifica então os endereços IP disponíveis localmente e inicia os LNDs correspondentes. Com isso, pode ser utilizada uma configuração de módulo unificada para todos os nós.

Caso a sub-rede Ethernet possua, por exemplo, o IP 192.168.16.0/24 e tenha IP-over-Infiniband através da sub-rede 192.168.17.0/24, então a configuração terá o seguinte aspecto:

```
options lnet ip2nets="tcp 192.168.16.*; o2ib 192.168.17.*"
```

A opção `routes` determina quais nós devem transferir o fluxo de dados de um tipo de rede para outro:

```
options lnet routes="o2ib 192.168.16.42@tcp"
```

Com isso, o nó 192.168.16.42 transmite da Ethernet para a Infiniband. Caso ele também deva fazer o encaminhamento na direção contrária, é necessária mais uma entrada:

```
options lnet routes="o2ib 192.168.16.42@tcp; tcp 192.168.17.42@o2ib"
```

Para modificar informações de roteamento, é preciso desativar completamente o Lustre e o LNET, descarregar os módulos e recarregá-los com uma nova configuração. Não é possível realizar alterações com o serviço em execução.

Caso uma determinada partição deva agir como parte de um sistema de arquivos Lustre, é preciso primeiro que seja instalado o sistema de arquivos de back-end local. Isso costumava ser apenas um detalhe da implementação, mas agora o mountconf exige que o administrador crie a partição com o `mkfs` (**exemplo 1**).

O **exemplo 1** configura no computador *metanode* (veja o **quadro 1**) a partição `/dev/sda1` como back-end de MDT do sistema de arquivos Lustre `ex1fs`. Além disso, há um detalhe: como um MGS administra somente poucos dados, ele permite que o Lustre utilize uma partição simultaneamente para MDT e MGT. Para um LOV de Lustre adicional, é necessário então um novo MDT, porém pode-se utilizar o serviço de gerenciamento já existente. O comando adequado, portanto, é:

```
root@metanode # mkfs.lustre --
➥fsname ex2fs --mdt --
➥mgsnode=metanode /dev/sda2
```

Uma partição de dados no computador `node0` também pode ser preparada para utilização como OST, e de forma bem parecida. O MGS e o nome do respectivo sistema de arquivos são os únicos parâmetros obrigatórios necessários (**exemplo 2**).

Esse exemplo esconde uma chamada a `mkfs.ext2 -j`, que configura um ldiskfs na partição `/dev/sda1` e, definindo o tamanho de bloco, *hashes* para diretórios e ainda o tamanho do *journal* otimiza um pouco o desempenho.

O nome do sistema de arquivos Lustre é refletido no nome do sistema de arquivos do ldiskfs que lhe serviu de base: pode conter até 16 caracteres e tem o formato `lustrefs-Nome-MDTxxxx` para um MDT, ou `lustrefs-Nome-OST` para um OST. Os quatro últimos caracteres (`xxxx`) correspondem ao índice do OST atual, que o usu-

Tabela 1: Pacotes RPM do Lustre

Pacote	Descrição
kernel-smp-<release-version>.rpm	Kernel do Lustre corrigido dependente de distribuição (sem módulos do Lustre)
kernel-source-<release-version>.rpm	Kernel do Lustre corrigido como código-fonte (opcional)
lustre-modules-<release-version>.rpm	Módulos do Lustre adequados
lustre-<release-version>.rpm	Ferramentas de espaço de usuário do Lustre adequadas à versão do módulo
lustre-source-<release-version>.rpm	Ferramentas de espaço de usuário, correções do kernel e módulos como fontes

ário pode definir manualmente com a opção do `mkfs --index`. Do contrário, o Lustre atribui os índices seqüencialmente na primeira inicialização dos OSTs.

"mount" sem montagem

O comando `mount` é usado para iniciar o serviço do Lustre:

```
root@metanode # mount -t lustre
➥/dev/sda1 /lustre/ex1/mdt
```

Na verdade, esse comando não significa nada. Nesse exemplo, montou-se um sistema de arquivos Lustre no ponto `/lustre/ex1/mdt`. Isso significa que foram ativados os serviços ldiskfs em `/dev/sda1`. O último argumento, `/lustre/ex1/mdt`, não é usado pelo comando. Somente o comando `df` fornece saídas com algum sentido, e mostra o estado atual de preenchimento do respectivo MDT. Os OSTs são iniciados de maneira semelhante com o comando:

```
root@node0 # mount -t lustre
➥/dev/sda1/lustre/ex1/ost0
```

O comando do Lustre `lctl` mostra o estado atual do servidor. Por exemplo, ele pode exibir um panorama dos serviços atualmente em execução. Em um MDS:

```
root@metanode # lctl dl
0 UP mgs MGS MGS 5
1 UP mgc MGC192.168.16.21@tcp
➥bf0619d6-57e9-865c-551c-
➥06cc28f3806c 5
2 UP mdt MDS MDS_uuid 3
3 UP lov ex1fs-mdtlov ex1fs-
➥mdtlov_UUID 4
4 UP mds ex1fs-MDT0000 ex1fs-
➥MDT0000_UUID 3
```

E num OSS:

```
root@node0 # lctl dl
0 UP mgc MGC192.168.16.21@tcp
➥7ed113fe-dd48-8518-a387-
➥5c34eec6fbf4 5
1 UP ost OSS OSS_uuid 3
2 UP obdfilter ex1fs-OST0000
➥ex1fs-OST0000_UUID 5
```

Podem ser instalados até 1020 OSTs para um único sistema de arquivos Lustre. Do contrário, cada sistema de arquivos pode ser fixado em apenas um MDT. Entretanto, o fabricante CFS trabalha para que no futuro também possa oferecer clusters de servidores de metadados.

O tamanho do MDT limita o número de arquivos e diretórios com que o sistema de arquivos consegue lidar. Cada entrada ocupa até 4 KB a mais. O número de arquivos que o LOV pode armazenar resulta da soma dos tamanhos dos respectivos OSTs. Uma vez que foi conseguido espaço, o administrador pode inserir outros OSTs na operação em execução. No entanto, a CFS aconselha a não acessar o sistema durante esse período, pois ainda não foi testada a inserção de OSTs em condições de sobrecarga.

O cliente Lustre acessa normalmente o sistema de arquivos através de um comando `mount`. Para isso, precisa do ID de rede do MGS, bem como do nome do LOV:

```
root@cliente # mount -t lustre
➥/mnt/ex1fs
```

Esse comando funciona da forma convencional.

Lustre no dia-a-dia

Durante o funcionamento normal, o Lustre é simples. Como sistema de arquivos, ele suporta praticamente todas as exigências do padrão *POSIX*. Nas configurações padrão, ele não usa as funções de bloqueio `lockf()` e `flock()`. A opção de montagem `flock`, no entanto, exige o bloqueio explícito.

Com a opção `localflock`, o Lustre aloca os bloqueios eficientemente, porém eles perdem a consistência global entre todos os nós envolvidos. Isso é útil nos casos em que já tenha sido garantido de outra forma que somente os processos de uma máquina usarão um recurso. A opção de montagem `acl` fornece, além disso, o suporte a ACLs POSIX.

A ferramenta de linha de comando `lfs` oferece uma visão das entranhas do Lustre. O comando `lfs getstripe nome_do_arquivo`, por exemplo, mostra em quais OSTs e objetos um arquivo está dividido. Com `lfs setstripe`, também se pode definir o comportamento de distribuição de um novo arquivo alocado para um determinado servidor, ou dividir arquivos especialmente grandes em vários OSTs. Aplica-

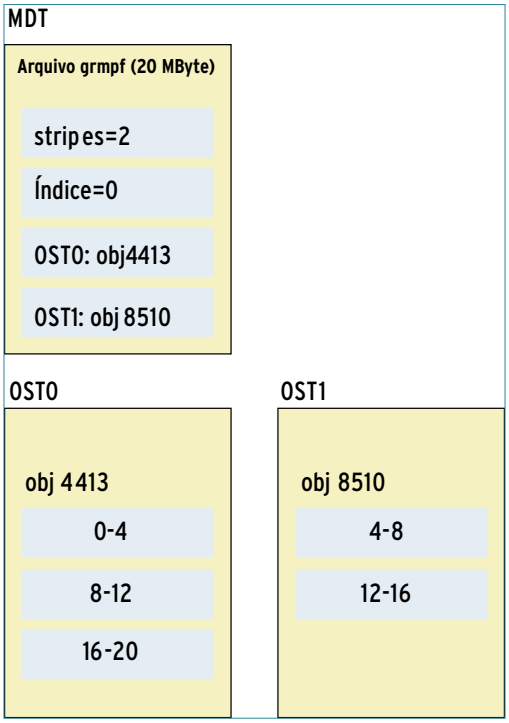


Figura 3 Segmentação de um arquivo em objetos, em vários OSTs.

do a um diretório, `lfs setstripe` define a configuração padrão para todos os novos arquivos e subdiretórios criados ali. Posteriormente, as configurações de um arquivo só podem ser modificadas por meio de cópia de seu conteúdo para um novo arquivo.

As cotas também são administradas com o `lfs` – os comandos são autoexplicáveis. O comando `lfs find` é muito importante no desligamento de um OSS. Com a opção `--pbd`, o comando detecta todos os arquivos de um determinado tipo – desde que o usuário ou o administrador não tenham utilizado anteriormente `lfs setstripe` para copiar os dados para outros OSTs.

Ajuste de desempenho

Geralmente os arranjos RAID agem como back-end de armazenamento para os serviços do Lustre. Porém, note que os níveis 5 e 6, que trabalham com paridade, não afetem pequenos blocos de dados durante a escrita, pois isso reduz drasticamente o desempenho.

O MDT, armazena *inodes* de poucos KB de tamanho, e por isso é aconselhável escolher um nível de RAID sem paridade, como 10, por exemplo. Os níveis 5 e 6 podem ser úteis para OSTs, mas é necessário levar em consideração o processo do *kjournald*. Novamente, para evitar maiores dores de cabeça, recomenda-se optar por RAID sem paridade.

Escalonamento e desempenho

O desempenho do Lustre depende fortemente da escolha do escalonador de I/O empregado. As versões mais recentes do kernel incluem quatro diferentes escalonadores: *Completely Fair Queueing* (*CFQ*), *Anticipatory*, *Deadline* e *NOOP*. O último é o mais simples: simplesmente não age sobre a ordem das requisições. Quando o controlador de armazenamento do servidor já se encarrega de escalonar adequadamente o fluxo de I/O, este é o mais indicado.

O CFQ é padrão na maioria das distribuições, mas não é indicado para aplicação em servidores de arquivo, já que seu algoritmo favorece uma operação bem diversificada, com poder de processamento excedente e pouca carga de I/O. O Anticipatory tem em vista a típica carga de I/O em estações de trabalho, e favorece o volume de dados em detrimento da latência, sendo muito pouco indicado para servidores de arquivos.

Finalmente, o escalonador Deadline minimiza a latência e é indicado para servidores com discos rígidos comuns, com RAID via software ou LVM. Portanto, dependendo do hardware dos nós do Lustre, NOOP ou Deadline são as melhores opções para os OSSs.

O escalonador de I/O pode ser especificado pelo parâmetro do kernel `elevator=Nome`, ou, dinamicamente, do sistema de arquivos `/sys`:

```
root@node0 # cat /sys/block/sda/
➥queue/scheduler
noop anticipatory deadline [cfq]
root@node0 # echo “noop” > /sys/
➥block/sda/queue/scheduler
root@node0 # cat /sys/block/sda/
➥queue/scheduler
[noop] anticipatory deadline cfq
```

Redundância e segurança

O desempenho é o fator mais importante no Lustre, e por isso ele é a primeira opção como diretório para velocidade em grandes clusters Linux. A segurança dos dados, ao contrário, é seu calcanhar de Aquiles, atualmente. A CFS vem se esforçando para evitar a perda de dados por falhas no Lustre, mas o sistema ainda implementa qualquer redundância, e por isso é vulnerável às menores falhas de hardware.

Portanto, é interessante utilizar RAID 1 (espelhamento completo) nos OSTs, fornecendo a redundância sem que o sistema de arquivos tenha de lidar com isso. Algo equivalente para os OSSs – suporte ao desligamento de OSSs – também está nos planos da CFS, e já tem o nome de *LAID* 1 (RAID 1 para Lustre). Esse recurso integrará o Lustre 2.0, mas ainda não está presente.

Armazenamento sem garantia

Na verdade, o Lustre não garante a segurança dos dados que armazena. Quando escrevemos dados num arquivo e depois de alguns minutos o abrimos novamente, talvez não encontremos os dados gravados, mesmo que nenhum erro ou falha tenha ocorrido nes-

Exemplo 2: Preparação de um OST

```
01 root@node0 # mkfs.lustre --fsname ex1fs --ost --
➥mgsnode=metanode /dev/sda1
02 Permanent disk data:
03 Target: ex1fs-OST0000
04 Index: unassigned
05 Lustre FS: ex1fs
06 Mount type: ldiskfs
07 Flags: 0x72 (OST needs_index first_time update)
08 Persistent mount opts: errors=remount-ro,extents,mballoc
09 Parameters: mgsnode=192.168.16.21@tcp
10 device size = 4096MB
11 formatting backing filesystem ldiskfs on /dev/sda1
12 target name ex1fs-OST0000
13 4k blocks 0
14 options -J size=160 -i 16384 -I 256 -q -O dir_index -F
15 mkfs_cmd = mkfs.ext2 -j -b 4096 -L ex1fs-OST0000 -J \
16 size=160 -i 16384 -I 256 -q -O dir_index -F /dev/sda1
17 Writing CONFIGS/mountdata
```

se intervalo. Às vezes, problemas temporários na rede podem desconectar alguns clientes, e então os ainda conectados conseguem alterar os dados, gerando quadros bizarros como esse. O NFS, por exemplo, contorna isso em sua versão 3, por meio do recurso *Sync on Close*.

Os desenvolvedores do Lustre recomendam o comando `sync` ou as chamadas de sistema `sync()` e `fdatasync()` para assegurar a integridade dos dados, mas isso exige trabalho de todos os desenvolvedores. A versão 1.6.2, publicada no final de agosto, oferece agora uma opção `sync` para montagem, que realiza todas as operações em arquivos de forma sincronizada – com significativa perda de desempenho.

Backup

Também falta ao software uma solução para backup. Embora soluções com o velho *tar* ainda possam ser usadas em cada cliente, todas as meta-informações específicas do Lustre, como o modelo de faixas, por exemplo, são perdidas. Caso um OST falhe, o administrador tem de reescrever uma grande quantidade de dados, já que o backup precisa restaurar cada arquivo por completo, mesmo quando são perdidos apenas segmentos específicos.

O trabalho extra pode prolongar significativamente o tempo de recuperação do sistema, pois sistemas de arquivos Lustre costumam reunir quantidades de dados de muitos TB ou até alguns PB. A CFS já planeja soluções de backup para salvar cada um dos OSTs como um *snapshot LVM*.

Recomendação

O uso de sistemas Lustre requer a redução de fontes de erro por defeitos de hardware de todas as espécies. O uso de RAID e bons no-breaks, portanto, é absolutamente obrigatório. O MDS deve contar com redundância, e os OSSs também precisam empregar pares de alta disponibilidade.

O Lustre oferece mecanismos de proteção contra falhas que permitem, com softwares como o *Heartbeat* ou *Cluster Manager*, transferir cada um dos serviços para outros computadores durante a operação. O preço disso é contabilizado no lado do hardware, pois, em vez de um disco rígido local e econômico, uma configuração como essa requer armazenamento compartilhado, como SANs ou iSCSI.

Como mostra a lista Top500, o Lustre é ótimo para abrigar um espaço temporário de armazenamento, tão necessário no caso de cálculos intensivos. No entanto, é importante evitar seu uso em sistemas de arquivo como `/home` ou raiz. ■

Mais informações

[1] Quadrics Elan: http://www.quadrics.com

[2] Myrinet: http://www.myri.com

[3] Infiniband: http://www.intel.com/technology/infiniband/

[4] Recursos do Lustre: http://wiki.lustre.org

[5] Cluster File Systems: http://www.clusterfs.com

[6] Top 500: http://www.top500.org

[7] GPFS: http://www-03.ibm.com/systems/clusters/software/gpfs.html

[8] GFS: http://www.redhat.com/software/rha/gfs/

[9] OCFS2: http://oss.oracle.com/ projects/ocfs2/

[10] OpenAFS: http://www.openafs.org

[11] pNFS: http://www.pnfs.com/

Sobre o autor

Oliver Tennert é Engenheiro de soluções sênior desde 1999 na prestadora de serviços de TI Science+computing AG de Tübingen, Alemanha.

Gerenciamento de tráfego de email com um proxy IMAP

Repasse a mensagem

Proxies IMAP ajudam a distribuir os emails a múltiplos servidores. Veja algumas opções de proxies IMAP para Linux.

por Jack Chongjie Xue e Markus Feilner

Sophie – www.sxc.hu

Cada vez mais servidores IMAP estão sofrendo sob o preso crescente do tráfego de email. Isso significa um problema para os administradores: criar um cluster de servidores IMAP não é uma tarefa trivial. Para assegurar a disponibilidade de um banco de dados compartilhado para as caixas de correio dos usuários, os administradores costumam apelar para caros SANs para armazenamento compartilhado ou mecanismos complexos de replicação.

O custo dos sistemas comerciais para criação de clusters, como o *Red Hat Cluster Suite*, podem deixar gerentes de TI nervosos, e a perspectiva de migrar um servidor IMAP antigo para um novo cluster e a complexidade técnica envolvida também pode prejudicar o sono de muitos administradores de sistema.

Os administradores de Linux que instalam seus sistemas com base em Software Livre geralmente se frustram com a medíocre capacidade de alta disponibilidade dos atuais servidores IMAP. Enquanto as soluções redundantes para os *MTAs* dos populares servidores SMTP atuais são facilmente implementadas por DNS ou técnicas de balanceamento de carga por IP, a qualidade do *back-end* de armazenamento determina o sucesso ou falha de um cluster IMAP.

Mais fácil que cluster

Um proxy IMAP é uma alternativa simples e flexível à solução de criação de um cluster. Os proxies IMAP fazem uma separação entre o transporte das mensagens e o armazenamento dos dados. Os clientes de email não usam IMAP nem POP para conversar com o servidor de email, simplesmente comunicando-se com o proxy. O proxy IMAP então verifica seu banco de dados, encontra o servidor IMAP responsável pelo usuário e encaminha a requisição para o servidor responsável (**figura 1**).

Fachada para o IMAP

Pode-se pensar no proxy IMAP como uma interface para o servidor de emails. O cliente se conecta ao proxy, que por sua vez se comunica com os servidores de email subjacentes para obter os dados de email dos usuários. Essa técnica adiciona uma flexibilidade inesperada, pois o cliente sempre se conecta à mesma máquina, mesmo que os dados do email sejam movidos para um local completamente diferente.

Os recursos padrão do protocolo IMAP oferecem diversas funções de encaminhamento e redirecionamento; entretanto, os vários projetos de software usam diferentes técnicas para realizar basicamente a mesma tarefa.

Todas as ferramentas para proxy IMAP possuem duas características em comum:

- O *front-end* e o back-end precisam oferecer as mesmas funcionalidades IMAP;

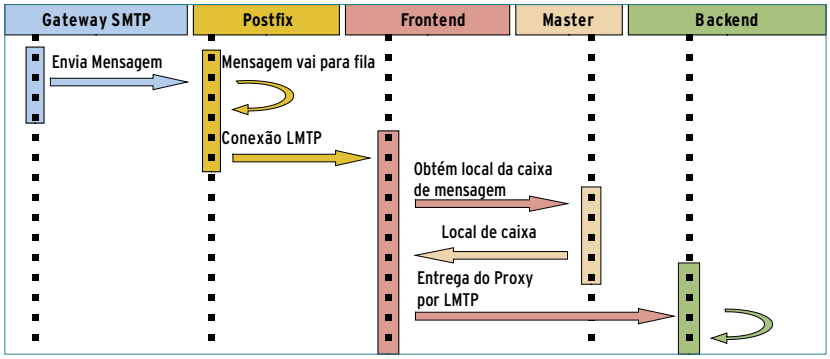


Figura 1 Os *gateways* de email entregam ao servidor *SMTP* a mensagem recebida. O servidor SMTP usa *LMTP* para encaminhar a mensagem ao servidor do *front-end*, e finalmente a mensagem é entregue ao *back-end* correspondente.

- O proxy usa um banco de dados para lidar com os mapeamentos usuário-servidor; o acesso é local ou através da rede.

Um dos proxies IMAP mais conhecidos e flexíveis é o *Perdition*[1]. Outro, chamado *Imapproxy*[2], se concentra no problema de clientes de webmail. Pacotes específicos de servidores, como o *Cyrus IMAP Aggregator*[3] oferecem uma grande gama de recursos, geralmente compatíveis somente para o servidor IMAP correspondente.

Perdition

O *Perdition* é um simples proxy de obtenção de email que suporta os padrões IMAP4 e POP3 tanto por conexões *SSL* quanto *TLS*. Ele entende somente os comandos IMAP necessários para a autenticação; de resto, ele simplesmente repassa os dados conforme são recebidos.

O artigo do Perdition (*Perdition Paper*, de Simon Horman)[4] dá mais detalhes dos recursos e funcionamento do programa para aqueles interessados numa visão aprofundada e em inglês. Mesmo tendo alguns anos de idade, esse documento ainda é considerado **a** referência para o uso do Perdition.

O proxy IMAP envia uma requisição para o banco de dados, e descobre o servidor correto para a conexão do cliente a partir da resposta.

Um recurso notável desse programa é seu suporte a múltiplas fontes de dados. O Perdition se comunica com back-ends *LDAP*, *ODBC*, *MySQL* e *PostgreSQL*, ou qualquer mistura deles. Outra vantagem é sua extensibilidade modular.

Instalação

É muito fácil instalar o Perdition. Os usuários de Linux podem optar por baixar o código fonte e compilá-lo ou usar os *RPMs* binários. Se houver interesse no logging detalhado, pode-se instalar também o *Vanessa Logger*[5]. O **exemplo 1** demonstra a configuração do Perdition com uma tabela de busca num banco de dados MySQL. Nesse exemplo, o banco se localiza na máquina local; o **exemplo 2** mostra seu conteúdo.

Durante a migração, scripts automatizados podem copiar as caixas de mensagens do servidor antigo para o novo, e em seguida atualizar as entradas necessárias do banco de dados. O proxy Perdition redireciona automaticamente para o novo servidor de back-end os usuários migrados. Não é necessário alterar qualquer configuração no cliente, e os usuários desfrutam de um serviço de email sem interrupções.

Exemplo 1: /etc/perdition/perdition.conf

```
01 connection_logging
02 connection_limit 1000
03 map_library /usr/lib/libperditiondb_mysql.so.0
04 map_library_opt "localhost:3306:dbPerdition:tblPerdition:
➥perdition:x:username:servername:port"
05 username_from_database
```

Imapproxy

O *Imapproxy* é projetado para a tarefa, altamente especializada, de acelerar o desempenho de servidores de webmail através do *cache* de dados de conexões POP e IMAP com o servidor de emails.

Servindo um cache IMAP, o Imapproxy reduz o número de conexões exigidas pelo programa de webmail. Normalmente, cada ação do cliente do webmail aciona uma operação de leitura ou escrita no servidor IMAP, demandando assim o intercâmbio de vários pacotes de dados. O cache do Imapproxy consegue lidar com várias requisições diretamente, acelerando o aplicativo do webmail.

Diferentemente do Perdition, o Imapproxy é mais uma ferramenta de otimização do que um verdadeiro proxy. Ele é útil sempre que os usuários precisarem de acesso via navegador ao servidor IMAP. Pode-se até combinar o Imapproxy com o Perdition (**figura 2**).

Alta performance: Cyrus

Outra solução de proxy IMAP é o *Cyrus IMAP Aggregator Proxy* (ou *Cyrus IMAP Proxy*, para abreviar). O proxy do Cyrus, é provavelmen-

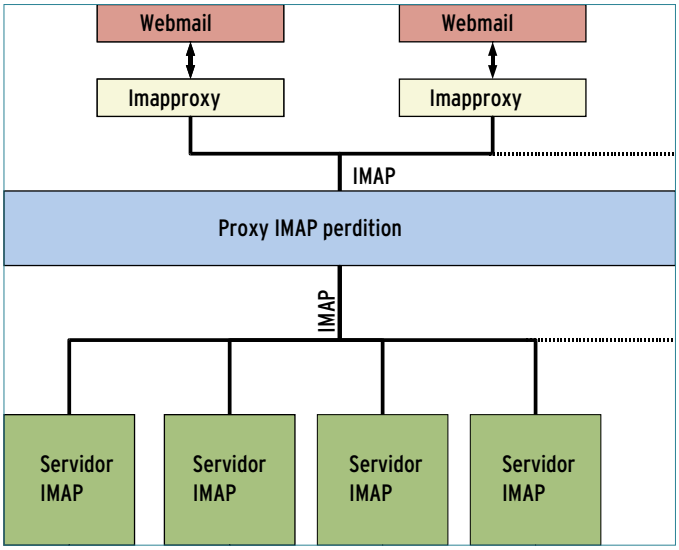


Figura 2 Enquanto o *Perdition* é uma solução completa para proxy *IMAP* e *POP*, o *Imapproxy* acelera os webmails através de um cache local de conexões IMAP.

te a ferramenta mais robusta de sua estirpe. O IMAP Aggregator Proxy suporta tanto a obtenção de emails (POP/IMAP) quanto sua entrega (*LMTP*), embora somente em parceria com o servidor de email Cyrus.

Assim como o *UW*, o *Courier* e o *Dovecot*, o IMAP Cyrus é um dos grandes servidores IMAP, e provavelmente é o que oferece a maior variedade de recursos.

O Cyrus armazena emails em seu próprio formato no servidor, ignorando completamente os formatos testados e aprovados, *mailbox* e *maildir*, e também funciona ao seu próprio modo em cenários multi-servidor. O *Cyrus Murder Aggregator* suporta clusters de alta performance com balanceamento de carga, criando servidores front-end para se comunicarem com os back-ends de armazenamento. A replicação em pares e o armazenamento compartilhado por sistemas de arquivos para clusters, como *GFS*, oferecem muitas possibilidades de exploração. Mas isso tudo requer tempo, tenacidade e algum dinheiro.

O Aggregator freqüentemente é usado como proxy IMAP para o popular servidor de email Cyrus. Nesse cenário, múltiplos back-ends compartilham o trabalho, e o front-end distribui as requisições. Os detalhes de qual conta de usuário do email reside em qual servidor são guardados numa máquina separada, chamada de servidor *Mupdate*. O servidor age como um tipo de nó mestre e usa o protocolo Mupdate para entregar os dados requisitados por SMTP, IMAP ou POP.

Proxy de entrega

Fora a entrega de emails, o Cyrus Aggregator é semelhante ao Perdition; porém, ele usa seu próprio servidor e um protocolo modificado. A grande vantagem do Aggregator é que também suporta SMTP e LMTP; assim, ele fornece um sistema completo de proxy de email em colaboração com o Cyrus (mas somente com o Cyrus).

Conclusões

Com muito pouco trabalho, um proxy IMAP pode adicionar funcionalidade a um ambiente já instalado que, sem isso, exigiria um cenário de cluster bem mais caro. Todos os programas descritos neste artigo facilitam o trabalho do administrador com uma enxurrada diária de emails.

As opções de proxy IMAP para Linux acrescentam conveniência e aumentam o desempenho de sistemas de email movimentados. Se você planeja migrar seu servidor e está procurando compatibilidade, o Perdition é a escolha certa.

O Imapproxy dá conta de seu trabalho como um cache para webmail; não é um concorrente do Perdition como solução completa, mas é uma extensão útil. O Cyrus Aggregator pode distribuir a entrega de emails por múltiplos servidores no back-end. ■

Exemplo 2: Tabela do MySQL

```
01 mysql> select * from dbPerdition.tblPerdition;
02 +------+--------------------+------+
03 | user | servername         | port |
04 +------+--------------------+------+
05 |nome1 | imap01.empresa.com | 143  |
06 +------+--------------------+------+
07 |nome2 | imap02.empresa.com | 143  |
08 +------+--------------------+------+
09 ...
```

Mais informações

[1] Perdition: http://www.vergenet.net/linux/perdition

[2] Imapproxy: http://www.imapproxy.org

[3] Cyrus IMAP: http://cyrusimap.web.cmu.edu/ag.html

[4] Perdition Paper: http://tinyurl.com/23jwlo

[5] Vanessa Logger: http://tinyurl.com/393k2x

Sobre o autor

"Jack" Chongjie Xue trabalha na Universidade Marshall, nos EUA, onde recentemente migrou o cluster de email usado por 30.000 alunos de OpenVMS para Linux sem interrupção no serviço.

De que forma um país poderia espionar seus cidadãos online?

Em nome da pátria

Alguns países têm feito investidas no monitoramento do tráfego de seus cidadãos, mas nem sempre de forma declarada. Conheça oito formas de combater esses espiões federais silenciosos.

por Nils Magnus

Com o pensamento nada gentil de que "os fins justificam a invasão", os governos de alguns países têm flertado com a idéia de instalar softwares espiões nos computadores pessoais dos cidadãos a fim de monitorar os dados trafegados para suposto benefício da segurança nacional.

O governo federal dos Estados Unidos, através do FBI, criou o software *Carnivore* na virada do século. Paradoxalmente destinado a proteger a segurança dos cidadãos através do monitoramento do conteúdo de pacotes de rede enviados por esses mesmos cidadãos, o programa foi amplamente atacado e, em poucos anos, retirado de operação. No entanto, há diversos outros programas semelhantes já em andamento nos EUA, e provavelmente, também, em muitas outras nações, violando a privacidade da população para fins nem sempre muito coerentes.

A Alemanha, outro país de grande importância no atual cenário mundial de TI, é um dos que recentemente integraram esse grupo. Sua agência federal de criminalística anunciou há poucos meses o desejo de legalizar a investigação online, e tem recebido duras críticas da população, em especial dos círculos de TI.

No caso da Alemanha, o objetivo do governo parece apontar para a instalação de cavalos-de-tróia nos computadores. Os usuários de Linux obviamente se deleitam com a teórica imunidade de seus sistemas operacionais a esse tipo de praga virtual. Porém, essa confiança é um tanto exagerada. Sistemas Linux são, sim, vulneráveis à ação de programas espiões.

Neste artigo, mostraremos como esses programas podem agir e, melhor ainda, como os usuários de Linux podem contra-atacar para manter sua privacidade intocada.

Ataque 1: Vírus e worms

O tipo clássico de construção de vírus (**figura 1**) ataca os arquivos disponíveis, modifica-os e espalha-os por meio do sistema de arquivos. *Worms* (em português, vermes) são um tipo semelhante de praga. A diferença entre eles é que, enquanto os vírus necessitam da ação do usuário, os worms são executados de forma autônoma, ou seja, sem programas hospedeiros, e utilizam a rede para sua propagação. Tanto vírus quanto worms possuem duas características básicas comuns: replicação e destruição. Com a primeira, infectam outros alvos, e com a segunda, apagam, por exemplo, o conteúdo do disco rígido, senhas e cartas de amor – ou espionam o plano de um próximo ataque suicida, como crêem os agentes federais.

Embora sejam conhecidos alguns worms para Linux, os vírus clássicos são praticamente inexistentes. O argumento da arquitetura de permissões é perfeitamente válido contra a ação de vírus, pois é bem difícil para um processo não privilegiado sobrescrever programas de outros e arquivos de sistema. Além disso, por ter seu código-fonte aberto, o Linux também não sofre o

Quadro 1: Panorama do malware

Softwares mal intencionados são chamados, na linguagem técnica, de malware. Os termos "vírus", "worm" ou "cavalo-de-tróia" referem-se a cada um dos aspectos do malware, cujos significados normalmente se confundem. Em resumo, vírus são programas que necessitam de um software hospedeiro para infectarem. Os vírus rodam como parte de seu hospedeiro, modificam suas funções e se difundem, injetando seus códigos também em outros programas. Os worms podem, além disso, rodar de forma independente e multiplicar-se e espalhar-se de maneira autônoma.

O termo cavalo-de-tróia se refere a funções ocultas (sempre com o intuito de causar danos) de um programa, as quais aparentemente inofensivas. Um cavalo-de-tróia é constituído de vários componentes, e alguns podem ser omitidos. Primeiro, o código invasor deve ser inserido no sistema alvo (vetor de ataque). Portanto, deve se acomodar (infecção) da forma mais resistente possível, para sobreviver, por exemplo, a uma reinicialização.

Para isso, alguns programas destrutivos chegam a se disfarçar (camuflagem), modificando programas do sistema que poderiam denunciar sua existência, e depois eliminam seus rastros. Eventualmente, do ponto de vista do invasor, o cavalo-de-tróia deveria rodar com privilégios abrangentes, de forma que obtivesse máximo acesso ao sistema hospedeiro (função destrutiva).

Desde que os cavalos-de-tróia trabalhem apenas localmente, sua utilidade para um agressor permanecerá limitada. Por isso, eles transmitem dados sensíveis do dispositivo afetado para um local da Internet (o chamado *drop host*, algo como máquina receptora). Exemplares mais aprimorados também assumem novas funções através das redes de comunicação, implementando backdoors por meio delas. Muitos programadores bloqueiam a comunicação externa, e às vezes também a memória temporária local de seu malware, para ocultar a existência ou o modo de funcionamento dos programas.

fenômeno do Windows® das cópias piratas contaminadas por vírus.

Restam os vírus de macro. Eles podem muito bem existir no Linux, mas nenhum deles foi visto no mundo livre até agora.

Probabilidade de êxito

Os worms para Linux parecem mais promissores. Eles não se limitam a programas hospedeiros, e também acessam computadores remotos por meio da Internet. Entretanto, como a maioria das distribuições ainda não iniciam muitos serviços de rede, esse caminho de invasão é mais complicado.

Ambas as formas clássicas de pragas são completamente imagináveis no Linux; no entanto, podem ser descobertas de forma relativamente fácil em situações normais. Os softwares antivírus, afinal, têm como função justamente descobrir esses molestadores e eliminá-los.

Efeito colateral

Como os vírus e worms, de acordo com os mecanismos de replicação de cada um, escondem o perigo de se multiplicarem de forma descontrolada e assim também afetarem infraestruturas críticas, parece menos provável que cavalos-de-tróia federais adotem esse caminho.

A melhor forma de um administrador se proteger contra ataques é através de um sistema com todas as atualizações de segurança, e também da atribuição correta de direitos e de um sistema de *checksums* como o *Aide* [1] ou a versão livre do *Tripwire* [2], que usa checksums criptográficos para todos os arquivos, e com isso reconhece modificações indesejadas, ou ainda como *lsof* (**figura 2** e **3**).

Ataque 2: Utilização de vulnerabilidades disponíveis

Independentemente da forma que a agência federal escolher para vigiar os cidadãos – seja por vírus, worm ou cavalo-de-tróia –, de alguma forma será preciso encontrar um caminho para entrar nos sistemas vigiados, ou seja, um vetor de ataque. Nesse caso, podem ser utilizadas as vulnerabilidades do software que está sendo utilizado.

Erros críticos de segurança não são raridade. A organização americana Mitre cataloga as vulnerabilidades conhecidas [3], e listou, somente na primeira metade de 2007, mais de 3 mil falhas em todos os sistemas operacionais e aplicativos. É lógico que o Linux também consta nessa lista, como se pode perceber pela seção de notícias de segurança da **Linux Magazine**.

A diferença mais óbvia entre o Software Livre e os proprietários, a disponibilidade do código-fonte, é usada tanto por invasores quanto por defensores. As vulnerabilidades são mais facilmente encontradas quando se tem acesso ao código-fonte, seja qual for a finalidade de quem as busca. Os engenheiros de segurança discutem se existem mais vantagens ou desvantagens, ou seja, se existem mais criminosos que exploram uma brecha do que especialistas em segurança que as corrigem. De maneira geral, todos estão convencidos de que vulnerabilidades desconhecidas ou secretas são mais problemáticas que as falhas já expostas.

Via de regra, a segurança pela obscuridade não funciona. Ocultar uma vulnerabilidade não im-

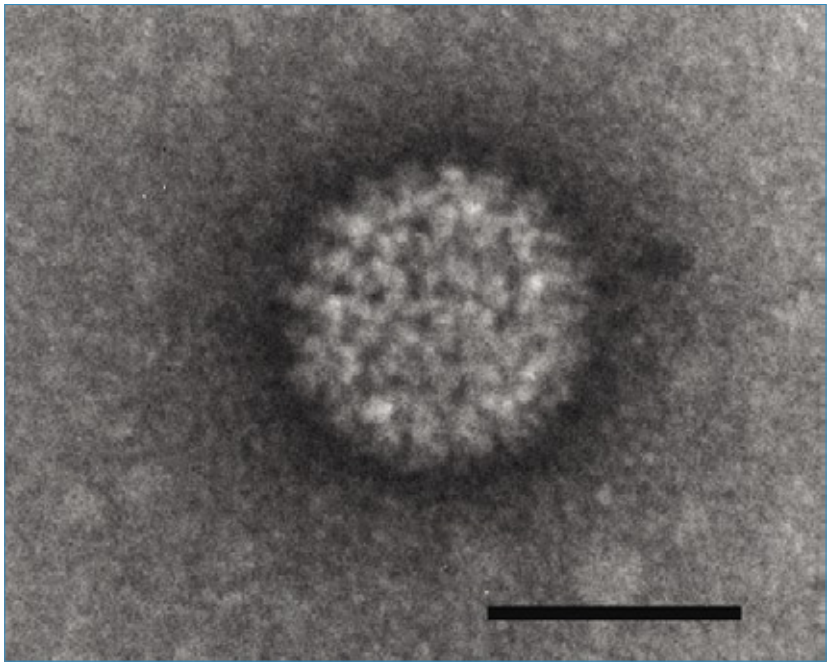


Figura 1 Assim como esse vírus biológico, os vírus de computador também infectam um portador, com ajuda do qual eles se espalham e perpetram danos.

pede que ela seja encontrada e explorada por outra pessoa. É um verdadeiro absurdo a tentativa de se proibir a busca de brechas de segurança, como a Alemanha fez recentemente com as "ferramentas para hackers", como o famoso *Nmap*. Pelo contrário, é importante solucionar rapidamente os pontos fracos que se tornam conhecidos.

No Software Livre, isso é feito, em geral, dentro de algumas horas, ou no máximo em poucos dias. No caso do software proprietário, geralmente demora mais, pois o gerenciamento do produto, os ciclos de lançamento e questões de marketing impedem a rápida publicação de correções.

Vulnerabilidades constituem um vetor de ataque perigoso para qualquer sistema, mas podem ser minimizadas pelo administrador através das atualizações regulares de segurança. A maioria das distribuições mais populares oferece correções em tempo real, e ajuda a executá-las de uma maneira simples. Quando tentam atuar contra a comunidade do Software Livre, os investigadores criminais dos governos dispõem apenas de um pequeno espaço de tempo para explorar as vulnerabilidades, e precisam de uma equipe de especialistas realmente eficiente, capaz de desenvolver rapidamente uma forma de explorar a falha do sistema.

Ataque 3: Backdoor em software proprietário

Há algum tempo, os espiões dos governos construiriam um cavalo-de-tróia clássico (veja o **quadro 1**). Nesse caso, seria possível esconder as funções de espionagem num software aparentemente inofensivo, que a vítima instalaria desavisadamente. Com isso, os investigadores infiltrariam seus próprios códigos em um aplicativo popular.

Para manter-se oculto, seria aconselhável escolher um aplicativo cujo código-fonte não estivesse disponível. Isso poderia ser desde um *plugin* multimídia para um navegador web, passando por um aplicativo VoIP, até um inocente driver de impressora. O cavalo-de-tróia obtém, com isso, todos os direitos que seu usuário possui. Do ponto de vista do invasor, a melhor das hipóteses seria ter o root como usuário. Para os investigadores dos governos, é relativamente complexo infiltrar-se nos processos de desenvolvimento de empresas privadas, e deve-se lembrar a grande indignação popular que surgiria caso algo assim fosse descoberto.

Ataque 4: Inserção no código-fonte

Inserir *backdoors* ou funções de cavalo-de-tróia num Software Livre é muito mais difícil em comparação com aplicativos proprietários, visto que a tramóia seria rapidamente descoberta por meio da revisão pública pelos desenvolvedores e especialistas em segurança.O bom funcionamento do trabalho de revisão, na prática, depende de muitos fatores. É claro que o tamanho e a complexidade do código-fonte desempenham um papel importante, somando-se a isso a preferência popular e a importância dos programas, bem como os potenciais danos.

Uma ferramenta aparentemente inofensiva, quase desconhecida, executada sem direitos especiais, atrai muito menos revisores do que o kernel Linux. Enquanto centenas de desenvolvedores trabalham no kernel, empregando um processo com vários níveis de revisão, um projeto menos proeminente que implemente funções primárias úteis poderia sucumbir diante de um grande *patch*.

As autoridades governamentais de fiscalização criminal precisariam discutir intensivamente com

os engenheiros específicos do projeto de cada um dos processos de desenvolvimento para realizar esse tipo de ataque com sucesso. Caso as alterações conseguissem passar despercebidas, os efeitos teriam um alcance muito maior.

Ataque 5: Ataque a repositórios

Um sucesso maior que o do ataque 4 pode ser alcançado optando-se pela manipulação direta do código-fonte de um aplicativo em seu repositório. Caso as alterações não surtam qualquer efeito real na funcionalidade do programa, poderiam permanecer ocultas por um período.

Entretanto, essas manipulações também correm o risco de serem descobertas pela revisão de um desenvolvedor interessado. Essa via de ataque já foi usada, por exemplo, contra o servidor de emails *Sendmail*.

Alvos de ataque especialmente recompensadores e por isso mesmo sob constante risco são as plataformas de desenvolvimento e repositórios como o *SourceForge* e o *BerliOS*. Uma vez realizada a invasão, o desenvolvedor de um cavalo-de-tróia federal poderia escolher dentre a ampla oferta de programas aqueles com perfil mais adequado a suas intenções.

Ataques bem sucedidos que empreguem esse modelo ainda não foram divulgados. Nesse caso, uma questão colocada aos investigadores de qualquer governo é se esse modelo de ataque pode ser articulado de forma legal, pois certamente cidadãos de outros países seriam igualmente afetados pela artimanha.

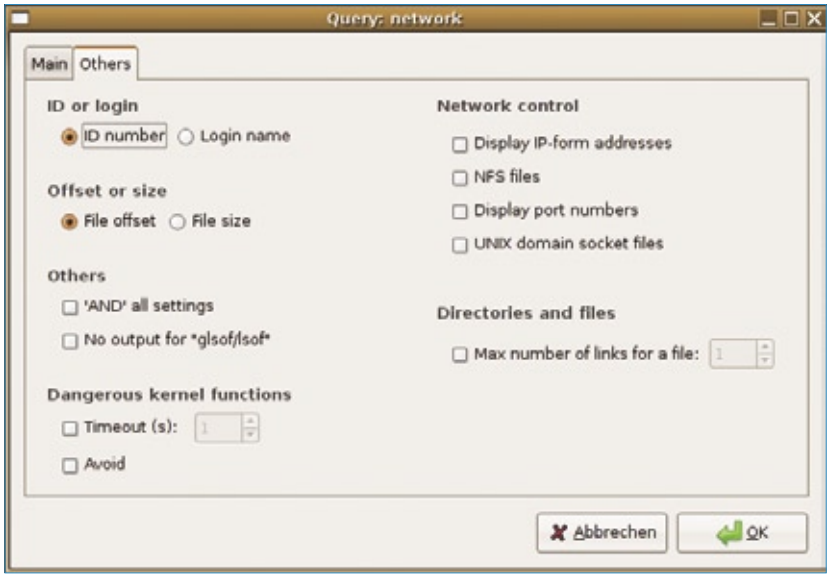


Figura 2 O *Glsof* é uma interface para o *lsof*, que permite descobrir o comportamento suspeito de programas.

Ataque 6: Virtualização

As modernas técnicas de virtualização funcionam tão bem que um usuário tem dificuldade para reconhecer, em um sistema hóspede, se ele se encontra de fato em um hóspede virtualizado ou no sistema de verdade. O órgão federal poderia introduzir uma camada de virtualização e lançar mão de ferramentas de monitoramento no sistema hóspede. A identificação do uso de virtualização é difícil, pois o sistema hóspede, ou seja, aquele operado pelo usuário, não teria indícios do problema, já que todos os arquivos permanecem intocados no ambiente virtualizado.

Por isso, tal ataque teria grande chance de sucesso, e vários projetos já o implementaram como prova do conceito. A combinação dessas técnicas de virtualização ainda está no início, e com certeza esse é um campo interessante para futuros desenvolvimentos.

Tabela 1: Técnicas de ataque

Ataque	Descrição	Complexidade	Eficácia	Medidas de defesa
1	Vírus e worms	média	alta	Antivírus, atribuição de direitos, *checksums*
2	Exploração de vulnerabilidades	média	alta	Atualizações de segurança
3	Backdoor	baixa	média	Melhores práticas de administração de sistemas
4	Modificação de código-fonte	alta	alta	Revisão do código
5	Ataque a repositórios	alta	alta	Segurança do sistema
6	Virtualização	alta	alta	Nenhuma
7	Manipulação de hardware	baixa	alta	Barreira física
8	Regulamentação por lei	baixa	baixa	Mudança para áreas não regulamentadas

Porém, resta um problema para os hospedeiros: eles precisam instalar seus softwares no sistema a ser monitorado. A solução mais funcional, nesse caso, seria usar um dos vetores de ataque já descritos.

Ataque 7: Monitoramento de hardware

É possível instalar hardwares para monitoramento. Sua função pode ser, por exemplo, a de um *keylogger*, registrando todas as ações do usuário. Apesar de tais dispositivos serem fáceis de instalar, eles requerem acesso físico ao dispositivo monitorado, e correm o risco de identificação por usuários técnicos.

Além disso, podem existir outros mecanismos de escuta no hardware. A BIOS da placa-mãe, por exemplo, costuma ser extensível. Seria possível por exemplo ter um mini *hypervisor* na bios, o qual faria os preparativos para o ataque 6. Controladores de disco rígido também seriam alvos interessantes para essa abordagem, assim como os firmwares de placas de rede ou de vídeo.

Assim, um chip de cavalo-de-tróia teria condições de buscar determinados dados ou, pelo menos, abrir um canal externo para permitir o download de outros softwares ou o upload de informações. Novamente, a maior barreira para as autoridades de investigação é que a instalação de um aparelho como esse exige acesso físico ao dispositivo.

Ataque 8: O poder do Estado

Um método inteiramente diferente, do ponto de vista conceitual, seria exigir legalmente a instalação de interfaces de observação em vez de realizar essa operação de forma furtiva. Em vários países isso já é válido em algumas áreas, como na escuta telefônica. Os fabricantes poderiam ser obrigados a instalar componentes que permitam rastrear dados, endereços IP e emails, por exemplo.

As tentativas de utilização de criptografia seguem uma tendência semelhante. O método *Key Escrow*, por exemplo, em vez de proibir o uso de criptografia de boa qualidade pelos cidadãos, como faz o governo americano, mantém as chaves criptográficas em poder de alguma autoridade. Com isso, todos se comunicam de forma segura, mas ainda é possível ceder as chaves a terceiros. A autoridade detentora das chaves, nesse caso, poderia ser o próprio governo, e seu uso seria obrigatório por lei.

A obrigatoriedade das interfaces físicas de monitoramento seria eficaz para as autoridades de investigação somente quando utilizadas em todo o país. Isso é viável para algumas centenas de provedores de acesso, mas supera todos os limites no caso dos muitos milhões de PCs. Seriam necessárias amplas modificações em toda a infraestrutura de TI, do projeto do PC às portas de comunicação.

Um bom resultado também poderia vir da introdução de interfaces ou funções de monitoramento em softwares mais baratos e comuns, como antivírus ou sistemas operacionais. Poderia ser estabelecido algum tipo de acordo entre o governo e os responsáveis pelas soluções antivírus, a fim de evitar conflitos posteriores quanto à privacidade dos usuários afetados.

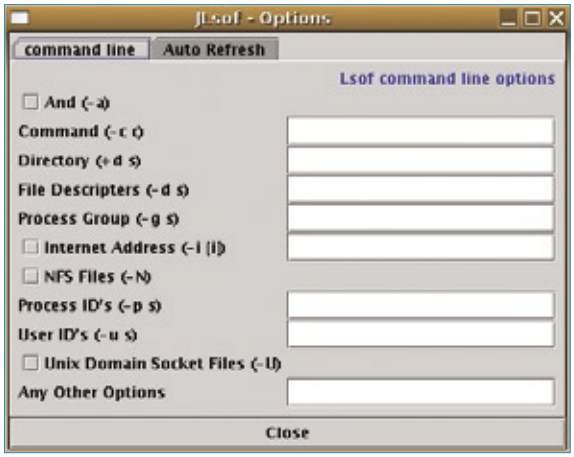


Figura 3 O *JIsof* é a interface em *Java* para o utilitário *lsof*.

Nesse ponto, as soluções antivírus proprietárias teriam maior probabilidade de adotar a obrigação, sobretudo se as negociações envolvessem grandes cifras, por exemplo, de aquisição de software. Já os projetos de Código Aberto, geralmente organizados internacionalmente, dificilmente sofreriam esse tipo de influência.

Conclusões

A **tabela 1** resume as diferenças entre os métodos de monitoramento online. Ela cita ainda os efeitos dos ataques e como proteger-se dos mesmos. Na verdade, essas mesmas formas de defesa devem ser empregadas para proteger os usuários de qualquer tipo de crime por praga virtual. ■

Mais informações

[1] Aide: http://sourceforge.net/projects/aide

[2] Tripwire: http://sourceforge.net/projects/tripwire/

[3] Lista de vulnerabilidades no Mitre: http://cve.mitre.org/cve/

Procedimentos para evitar a engenharia social

O lado analógico da segurança digital, parte 2

Michal Zacharzewski - www.sxc.hu

O primeiro artigo desta série mostrou como alguns fatores aparentemente inofensivos podem afetar sobremaneira a segurança digital de sua empresa. Veja agora como agir contra eles.

por Eduardo Moura

Em nosso artigo anterior[1][2], levantamos algumas questões, na forma de perguntas, com o objetivo de revelar os principais pontos com respeito à segurança da informação no ambiente corporativo.

É importante deixar claro que, embora esse seja um engano bastante freqüente, não há um tamanho de empresa mínimo ou máximo para a suscetibilidade de uma companhia a problemas de segurança. Nenhuma empresa é pequena demais para ter de se preocupar com essas questões. De forma semelhante, não é necessário que o mercado em que atua a empresa seja extremamente competitivo.

Esses descuidos proporcionam uma oportunidade de ouro para ataques de engenharia social. Sempre há uma recompensa que vale a pena para um atacante motivado. A cada dia mais invasores estão se arriscando na seara da engenharia social, e com isso os alvos de "menor visibilidade" também são interessantes. Pequenas empresas que atendem grandes corporações podem ser uma boa porta de entrada para um engenheiro social. Pensar segurança está mais relacionado à importância do negócio em um determinado mercado do que necessariamente ao seu poderio econômico.

A cultura vigente da empresa também não deve receber tanta confiança. Acreditar que todos os funcionários são bem informados quanto à segurança digital, ou que já estão cientes de todos os aspectos citados neste artigo ou no anterior é um perigo.

Todas as perguntas feitas no primeiro artigo desta série possuem um elemento em comum nas respostas: o elemento humano!

Segurança da informação depende da percepção das pessoas sobre ameaças. Percepção se adquire com treinamento e com processos de verificação claros e constantes. Não basta treinar as pessoas e não sensibilizá-las de forma adequada. Tampouco basta identificar incidentes de segurança e corrigi-los "sob demanda"; é necessário que o grupo de segurança da informação esteja sempre atento ao que chamamos de *quadro geral*, ou seja, as inter-relações possíveis entre os incidentes de segurança e o desfecho potencial de cada um dos cenários obtidos, além da percepção geral das pessoas sobre o assunto.

Iniciativas de treinamento com abordagens excessivamente técnicas espantam as pessoas que porventura tenham dificuldades com computadores. Abordagens excessivamente pirotécnicas ou hollywoodianas tendem a desacreditar o assunto, e o balanço entre forma e conteúdo deve ser buscado para obter uma correta motivação das pessoas.

Outra relação constantemente menosprezada é aquela entre o pessoal de TI e os integrantes da linha de negócios da empresa. Enquanto o assunto segurança da informação for tratado de forma fechada pelos profissionais técnicos, ele permanecerá suficientemente árido para que as pessoas na linha de frente não se interessem pelo mesmo. Um contato mais próximo entre essas duas áreas da companhia proporciona uma correta avaliação dos riscos a que todos estão expostos, e facilita, por conseguinte, a adoção de protocolos de segurança adequados.

Quadro 1: Risco e incerteza

É muito importante relembrar os conceitos de risco e incerteza, tão fundamentais à gestão da segurança da informação.

Risco é a chance de um evento não previsto ocorrer e trazer algum impacto para a organização, seja positivo ou negativo. O risco, normalmente, é tratado em uma escala quantitativa, do mais alto para o mais baixo.

Incerteza é o limite de visão dos desfechos de fatos que podem ocorrer com a organização. A incerteza pode ser:

- **conhecida**, ou seja, aquela na qual sabemos quais fatos podem ocorrer, porém não o seu desfecho;
- **desconhecida**, que é a presença de fatos que desconhecemos, mas cuja ocorrência pode ser simulada para fins de previsão de seus desfechos; e por fim
- a **imprevisibilidade**, que responde por fatos que não tinham como ser previstos.

Paranóia

Empresas que assimilaram a cultura da segurança mantêm-se atentas ao quadro geral, sem, no entanto desenvolverem uma paranóia de insegurança. Nesse ponto, é importante lembrar que a paranóia também tem efeito extremamente danoso. No estado de paranóia, uma empresa pode vir a ser explorada por engenheiros sociais que se passam por consultores de segurança e infiltram-se profundamente na organização, retirando dela vantagens maiores e mais rápidas do que aquelas que as obteriam por meio de um ataque "convencional". O equilíbrio correto nas percepções de risco e incerteza (veja o **quadro 1**) é fundamental para evitar esse tipo de paranóia.

Portanto, se os profissionais de segurança possuírem uma visão clara dos riscos, eventos e incertezas, o quadro de segurança fica mais definido. Essa clareza de visão é mais um elemento de reforço à segurança da informação.

Empresas que não possuem essa visão e entendimento certamente estão expostas ao risco de um ataque de alto nível, e com conseqüências devastadoras. A tecnologia e as normas – como a ISO:NBR 17799, por exemplo – ajudam o ambiente técnico a tornar-se "aderente" (do inglês *compliant*). Porém, sem uma estratégia global de segurança da informação que envolva fortemente o elemento humano, de nada adiantam os sofisticados recursos oferecidos pelas fabricantes de produtos de segurança ou pelos esforços implementados na comunidade de Software Livre. Sem esse composto, – o humano– as empresas continuarão a viver em um ambiente eminentemente inseguro. ■

Mais informações

[1] Eduardo Moura, "O lado analógico da segurança digital". Linux Magazine 37, dezembro de 2007, pág. 64.

[2] Eduardo Moura, "O lado analógico da segurança digital" (em PDF): http://www.linuxmagazine.com.br/lm/articles/o_lado_analogico_da_seguranca_digital

Sobre o autor

Eduardo Moura (eduardo.moura@telway.com.br) é consultor em segurança da informação e governança de TI. É entusiasta do Software livre e atua na Telway Tecnologia.

Copyleft

Para todos, os direitos preservados

Com o avanço do Software Livre, compreender o Copyleft torna-se ainda mais importante para exigir seus direitos e evitar más interpretações.

por Alexandre Oliva

Da tão conhecida frase "Copyright, all rights reserved" (Direitos autorais, todos os direitos reservados) surgiu o trocadilho "Copyleft, all rights reversed" (Esquerdos autorais, todos os direitos invertidos), que dá a impressão de que *copyleft* inverte a lógica das leis de direito autoral. Outros preferem "all wrongs reversed" (todos os erros corrigidos), que deixa ainda mais claro o propósito do copyleft: consertar a lógica anti-social que se tem aplicado ao direito autoral, usando a força da própria lei para restaurar e reforçar sua finalidade original: beneficiar a sociedade. No caso do software, para beneficiar especialmente seus usuários e desenvolvedores.

Lá vem história

Direito autoral é um monopólio temporário que a sociedade viu por bem conceder aos autores de certos tipos de obras, a título de incentivo à criatividade. Em troca do monopólio, um número supostamente maior de obras se torna disponível, ainda que com algum atraso, para toda a sociedade usar, aprimorar e compartilhar: o domínio público.

Ao contrário do domínio público, direito autoral é uma idéia relativamente recente. William Shakespeare não precisava se preocupar com a legalidade de adaptar obras anteriores e até contemporâneas suas. Não fosse assim, provavelmente hoje estaríamos privados de muito de sua genialidade.

Curiosamente, é outro William, mais conhecido como Bill Gates, quem vem suprimindo energicamente, em várias frentes, a possibilidade de usuários de software se comportarem da mesma maneira.

Na frente social, já em 1976, publicou a "carta aberta aos hobbistas"[1]; mais recentemente, apóia grupos que promovem o slogan "Pirataria é roubo", tentando levar a crer que o pilar moral do compartilhamento tem mais a ver com saquear um navio do que com usar a chama de uma vela para acender outra.

Na jurídica, utiliza licenças e contratos restritivos de direito autoral, patentes e segredo industrial, assim como *EULAs* (contratos de licenciamento para usuário final), *NDAs* (contratos de confidencialidade) e outras artimanhas de cunho legal.

Na tecnológica, utiliza mecanismos de controle de cópia, limitação artificial de funcionalidade de software e hardware, impedimento de instalação de software "não autorizado" e privação de acesso ao código-fonte, a forma ideal para entender como funciona e para modificar um programa, distribuindo apenas o código-objeto, incompreensível para meros mortais como nós.

Inversão de valores

Pela lógica original, fazer valer o monopólio pode até parecer sensato, mas a privação do código-fonte falha na contrapartida, pois impede[2] a reutilização e o aprimoramento da obra, mesmo após o término do monopólio de pelo menos 50 anos. Esse prazo mínimo descabido é imposto pela Organização Mundial de Comércio, e não sugerido pela Organização Mundial de Propriedade Intelectual[3] (um termo que só faz confundir) como seria de se esperar.

A confusão de direito autoral, patentes e marcas num termo que alude a bens rivais se compara à da aplicação das mesmas regras a obras funcionais e artísticas.

Essas buscam proporcionar prazer estético, em suas muitas dimensões. Por mais especiais que sejam, não são insubstituíveis: prazer semelhante pode ser alcançável com outras obras.

Obras funcionais, particularmente software, são diferentes. Processos críticos de sua empresa podem ficar dependentes e engessados por um software específico que armazene informações essenciais em formatos secretos e que não possa ser adaptado de acordo com os interesses de quem o usa. Esse poder vai muito além do que se pretendia conceder aos autores através do direito autoral, e fica exa-

cerbado pela crescente importância do software em cadeias produtivas e no cotidiano das pessoas.

Livrai-nos do mal

Software Livre surgiu num movimento social que entende que negar a alguém as liberdades de executar um programa para qualquer propósito, estudar o programa, adaptá-lo para suas necessidades e distribuí-lo, com ou sem modificações é anti-ético e imoral, pois causa prejuízos financeiros e morais a quem é privado dessas liberdades e a toda a sociedade.

Escolher Software Livre para desempenhar uma determinada computação livra o usuário de monopólios de suporte, correções e aprimoramentos sobre esse software. Porém, alguém ter suas liberdades respeitadas com relação ao software não significa que todos as tenham. Um autor pode oferecer o software com liberdade para alguns e sem liberdade para outros. Pode inclusive autorizar quem receber o software de maneira livre a distribuí-lo, talvez modificado, de maneira não livre, pondo a perder as liberdades de quem mais importa: o usuário e potencial desenvolvedor do software.

Endireitando direitinho

Copyleft é uma técnica de licenciamento que evita essa ruptura. Valendo-se justamente do monopólio legal (no Brasil, as leis 9609/98, do Software, e 9610/98, de Direito Autoral), uma licença copyleft concede permissões que respeitam as liberdades do usuário, mas limitadas, de modo que o software, com ou sem modificações, só possa ser distribuído sob a mesma licença. Copyleft torna as liberdades parte integrante e inseparável do software.

Das várias licenças copyleft, algumas permitem a combinação com software sob outras licenças, mas a mais conhecida é a *GNU GPL*, que adota um copyleft forte: tanto a obra original quanto suas derivadas só podem ser distribuídas sob os mesmos termos e condições.

Há quem a chame de licença viral, querendo fazer parecer que a licença é uma doença cuja forma de contágio é o mero contato físico. Na realidade, as liberdades são uma herança que o software sob licença copyleft deixa para todos os seus descendentes, sem afetar obras que não sejam dele derivadas.

Com trato ou sem licença?

A GPL não cria obrigações contratuais, apenas condiciona as permissões que concede, deixando a lei prevalecer quando as condições não são respeitadas. Se eu digo: "pode estacionar seu carro na minha garagem", estou concedendo uma permissão legalmente necessária para alguém que não tinha o direito de sequer entrar no prédio onde moro, mas delimitada de tal forma que o acesso à minha residência continua não permitido. Da mesma forma, a GPL concede a permissão legalmente necessária para quem queira distribuir o software, mas delimitada de forma que a supressão do código-fonte e o uso de outros termos e condições continuem não permitidos.

As permissões são indiferentes a quem não tenha intenção de ir à garagem do prédio ou de distribuir o programa da forma especificada. Quem não quiser vir ao meu prédio e não quiser distribuir o programa não precisa delas. Já quem tenha as permissões acima mas invada minha residência ou distribua software GPL com restrições adicionais não está descumprindo obrigação para comigo, mas agindo fora do escopo das permissões que concedi. Na ausência de permissões adicionais, esses atos são ilegais: invasão de domicílio e infração de direito autoral, respectivamente.

Por isso é tão difícil subverter o copyleft, em particular o da GPL. Negar a validade da licença é confessar infração de direito autoral, enquanto reconhecê-la, com suas condições, não ajuda a quem tenha agido fora de seus limites.

Nasce torto mas endireita

Por contrariar a concepção mesquinha da lei de direito autoral e usá-la uma vez mais em prol da sociedade, diz-se que copyleft inverte os direitos. Como isso conserta várias distorções, diz-se que copyleft também corrige os erros do direito autoral. Por ser uma idéia de tamanho avanço social, faz sentido traduzi-lo como "esquerdos" autorais.

Copyleft usa a lei do direito autoral não para manter o monopólio legal, mas para evitar seu abuso, garantindo o respeito às liberdades de quem quer que receba a obra, impedindo a supressão desses direitos sobre ela. Daí dizer: para todos, os direitos preservados. ■

Mais informações

[1] Bill Gates, "Carta aberta aos hobbistas": http://en.wikipedia.org/wiki/Open_Letter_to_Hobbyists

[2] Boletim da FSFLA, editorial "Problemas com 'Propriedade Intelectual'": http://www.fsfla.org/?q=pt/node/129#1

[3] Richard Stallman, "Did You Say 'Intellectual Property'? It's a Seductive Mirage": http://www.gnu.org/philosophy/not-ipr.html

Sobre o autor

Alexandre Oliva é engenheiro, mestre em Ciências da Computação e trabalha na Red Hat, além de ser co-fundador e conselheiro da Free Software Foundation Latin America.

Virtude profunda

O KVM traz o kernel à era da virtualização. Saiba por que o universo do Linux tem tanto interesse nessa promissora alternativa de virtualização.

por Amit Shah

Em dezembro de 2006, Linus Torvalds anunciou que as novas versões do kernel Linux incluiriam a ferramenta de virtualização conhecida como *KVM* (*Kernel Virtual Machine Monitor*). O KVM surgiu há relativamente pouco tempo, e sua súbita chegada aos holofotes revela o poder do modelo de virtualização baseado no kernel. Esse modelo oferece várias vantagens potenciais, incluindo melhor desempenho e suporte mais uniforme a todo o ambiente Linux. Este artigo mostra como o KVM funciona e introduz a configuração de sistemas virtuais baseados nessa ferramenta.

O jeito do KVM

Num cenário comum de virtualização, um componente conhecido como *hypervisor* funciona como uma interface entre os sistemas hóspede e hospedeiro. O hypervisor se localiza sobre o sistema hospedeiro, lidando com as tarefas de escalonamento do processador e gerenciamento da memória para os hóspedes.

O KVM funde o hypervisor ao kernel, reduzindo a redundância e acelerando a execução. Um driver KVM comunica-se com o kernel e age como interface para uma máquina virtual no espaço do usuário. O escalonamento de processos e o gerenciamento da memória são realizados pelo próprio kernel. Um pequeno módulo do kernel Linux introduz o modo de hóspede, define as tabelas de página do hóspede e emula certas instruções chaves.

As versões atuais do KVM trazem uma versão modificada do emulador *Qemu*, que gerencia a entrada e saída, e opera como lar virtual para o sistema hóspede (**figura 1**). Este roda dentro do Qemu, que por sua vez roda como um processo comum no espaço do usuário. O ambiente resultante é semelhante ao cenário exibido na **figura 2**, em que vários processos de máquinas virtuais são executados lado a lado com outras tarefas de espaço do usuário gerenciadas diretamente pelo kernel. Cada hóspede consiste em duas partes: a de espaço do usuário (Qemu) e a do hóspede (o hóspede propriamente dito). A memória física do hóspede é mapeada no espaço de memória virtual da tarefa, e então os hóspedes também podem ir para a *swap*. Processos virtuais dentro de uma máquina virtual são simplesmente *threads* no processo do hospedeiro.

Esse modelo se encaixa perfeitamente no modo Unix de realizar somente uma tarefa, e realizá-la corretamente. O módulo do KVM trata apenas de criar e ativar o modo de hóspede e lidar com acessos virtualizados aos registradores. Da perspectiva do usuário, quase não há diferença entre rodar uma máquina virtual do Qemu com KVM desativado e uma com o KVM ativado, exceto, é claro, pela diferença significativa de velocidade.

O KVM segue o ideal de desenvolvimento e liberação do Linux: liberar cedo e freqüentemente. A versão estável mais recente é parte do Linux 2.6.x, com correções de falhas ocorrendo nas versões 2.6.x.y. O código-fonte do KVM é mantido numa árvore *git*. Para obter a versão mais recente, ou a árvore git mais recente, basta acessar o wiki do projeto[1] para os detalhes do download.

Using KVM

Como o KVM explora apenas os últimos avanços do hardware, é necessário assegurar a presença de um processador com suporte às extensões de virtualização. Para descobrir isso:

```
$ egrep '^flags.*(vmx|svm)' \
/proc/cpuinfo
```

Se for gerada alguma saída, então os recursos necessários estão presentes na CPU.

Nesse caso, meio caminho já está andado. É necessário ter uma versão recente do kernel 2.6. Se a versão do kernel for recente e já contiver o KVM, seja como módulo ou embutido, ele

já pode ser usado caso não se deseje compilar os módulos pessoalmente. Entretanto, o projeto KVM recomenda a versão mais recente disponível no site, pois ele recebe novos recursos e correções continuamente – para não mencionar as novas falhas, o que pode causar problemas ocasionais.

Baixe o código-fonte na página de download[1]. O *tarball* tem duas partes. O diretório `kernel/` contém os fontes dos módulos do kernel. Os outros arquivos são a porção de espaço do usuário, uma versão levemente modificada do Qemu. Se o suporte ao KVM já estiver presente, seja como módulo ou embutido no kernel, é importante impedir o programa de compilar os módulos.

Compilar os utilitários de espaço do usuário a partir do tarball requer algumas bibliotecas. A lista detalhada e as instruções estão disponíveis através do wiki do KVM[1].

É necessário usar a versão 3 do compilador GCC; parte do código do Qemu não se entende com o GCC 4, o compilador padrão das distribuições Linux recentes.

Depois de compilar e instalar o utilitário (e o módulo, se desejado), antes de começar a usar o KVM é necessário criar um arquivo para abrigar o sistema operacional hóspede:

```
$ qemu-img create -f qcow \
debian-etch.img 10G
```

Isso cria um arquivo `debian-etch.img` com 10 GB no formato *qcow*. São suportados alguns outros formatos, cada um com vantagens e desvantagens.

Assim que o arquivo de imagem é criado, já é possível instalar um sistema hóspede nele. Para isso, deve-se carregar os módulos do KVM, caso não estejam embutidos no kernel.

```
$ sudo modprobe kvm-intel
OU
$ sudo modprobe kvm-amd
$ qemu-system-x86_64 -boot d \
-cdrom /images/debian-cd.iso \
-hda debian-etch.img
```

Esse comando inicia uma sessão de máquina virtual. A janela exibe *QEMU/KVM* em seu título, o que significa que o KVM está ativo. Assim que a instalação termina, pode-se rodar o hóspede com:

```
$ qemu-system-x86_64 \
debian-etch.img
```

Também é possível passar o parâmetro `-m` para especificar a quantidade de memória RAM usada pela máquina virtual. O valor padrão é de 128 MB. As versões recentes do KVM possuem suporte à passagem da memória do hóspede para a swap, para que a RAM alocada ao hóspede não sobrecarregue o hospedeiro.

Pode-se ocasionalmente encontrar falhas ao rodar máquinas virtuais com o KVM. A saída nos logs do kernel do hospedeiro ajudam na busca de problemas semelhantes relatados antes, bem como de quaisquer sugestões disponíveis. A atualização para a última versão do KVM deve solucionar o problema.

Caso uma solução não seja encontrada, executar a máquina virtual com a opção `-no-kvm` inicia o Qemu sem suporte ao KVM. Se nem assim o problema for resolvido, isso significa que ele reside no Qemu, e não no KVM. Outra tentativa pode ser passar o parâmetro `-no-kvm-irqchip` ao iniciar a máquina virtual. Também se pode perguntar na amigável lista de discussão do KVM.

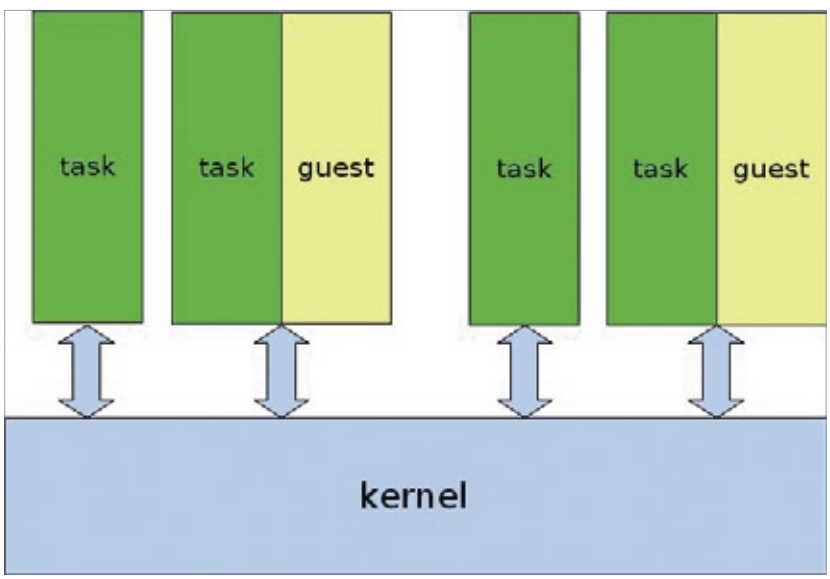


Figura 1 O *KVM* traz uma versão modificada do emulador *Qemu*.

Qemu monitor

O *Qemu monitor* é aberto com a combinação de teclas **[Ctrl]+[Alt]+[2]** quando a versão do Qemu é selecionada. O monitor dá acesso a alguns comandos de depuração e alguns comandos que podem auxiliar a inspeção do estado da máquina virtual. Por exemplo, `info registers` exibe o conteúdo dos registradores da CPU virtual. Também é possível conectar dispositivos USB a uma máquina virtual usando comandos do Qemu monitor.

Migração de máquinas virtuais

Migrar máquinas virtuais é muito importante para o balanceamento de carga e a redução do tempo de interrupção durante atualizações. O processo de migração inclui mover um hóspede de uma máquina física para outra. A vantagem da técnica do KVM é que os hóspedes não se envolvem na migração. Além disso, não são necessários

componentes especiais para realizar a migração através de um túnel SSH ou comprimir a imagem em migração. Pode-se até passar a imagem por um programa antes de ser transmitida à máquina alvo. A menos que estejam ativos recursos específicos de hardware ou da máquina, pode ser feita a migração entre duas máquinas. Além disso, hóspedes parados também podem ser migrados, assim como os ativos. A estrutura que permite isso é do próprio Qemu, então não são necessárias alterações no kernel para ativar o recurso. A sincronização do estado do dispositivo para efetuar a migração e o estado da máquina virtual são fornecidos e gerenciados transparentemente no espaço do usuário.

Na máquina de destino, pode-se executar o Qemu com as mesmas opções de linha de comando usadas para a máquina virtual na origem, mas com parâmetros adicionais para comandos específicos de migração:

```
$ qemu-system-x86 -incoming
➥<protocolo:parâmetros>
```

Por exemplo:

```
$ qemu-system-x86 -m 512
➥-hda /images/a.img
➥-incoming stdio
```

Na máquina de origem, a migração deve ser iniciada com o comando `migrate` do Qemu monitor, indicando o protocolo e seus parâmetros, como por exemplo:

```
(qemu) migrate
➥tcp://ipdestino:portadestino
```

O parâmetro de linha de comando para a migração no destino é:

```
-incoming tcp://0:porta
```

Se o comando de origem no Qemu monitor for:

```
(qemu) migrate ssh://ipdestino
```

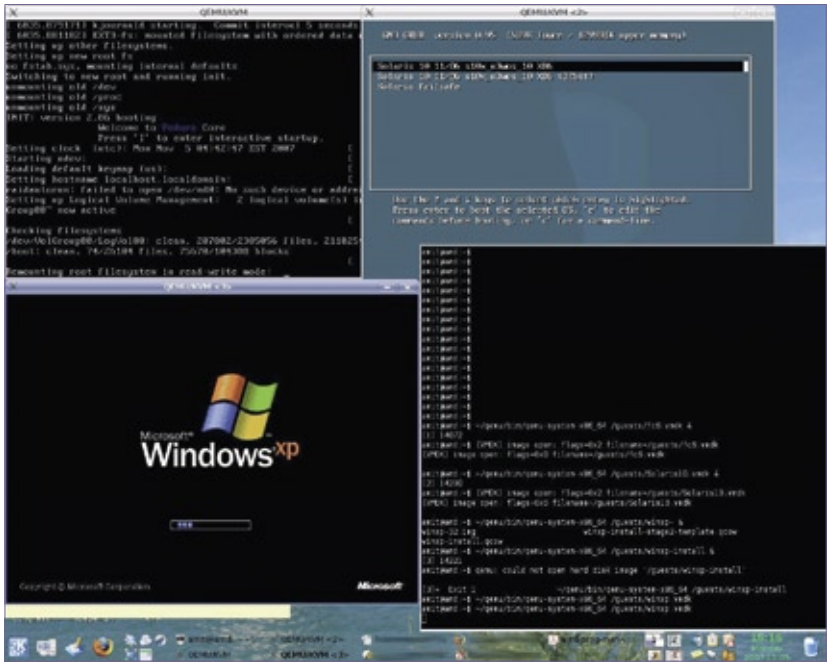


Figura 2 Um processo de máquina virtual roda ao lado de outras tarefas do espaço do usuário, e é gerenciado diretamente pelo kernel.

então o parâmetro para migração no destino será:

```
-incoming ssh://0
```

Há opções semelhantes para realizar a compressão por *Gzip* e a criptografia por *GPG*, e até mesmo para processar os dados num script antes de enviá-los.

Vantagens

A técnica do KVM oferece várias vantagens. Pode-se reutilizar todo o software e infraestrutura já existentes, e não é necessário aprender novos comandos. Por exemplo, *kill* e *top* funcionam como de costume na tarefa de hóspede do sistema hospedeiro.

O KVM foi projetado originalmente para suportar hospedeiros *x86*, e seu foco é na virtualização completa, sem modificações no sistema operacional hóspede. Entretanto, conforme ele foi ganhando mais desenvolvedores e casos de uso interessantes, começou a ser portado para outras arquiteturas e a ganhar suporte à paravirtualização. Se um hóspede conseguir comunicar-se com o hospedeiro, atividades como as de rede ou I/O podem ser mais velozes. Além disso, modificações no sistema operacional hospedeiro (Linux) para melhorar o escalonamento de processos e o uso da swap já foram propostas e aceitas.

O KVM funciona sem problemas em todos os tipos de máquinas – servidores, desktops, laptops e placas embarcadas – e é possível usar as mesmas ferramentas de gerenciamento e infraestrutura comuns do Linux.

O sistema KVM se integra ao escalonador, à camada de I/O e todos os sistemas de arquivos do Linux. Outros benefícios incluem a migração *ao vivo* e o suporte a *NUMA* e máquinas com 4096 processadores.

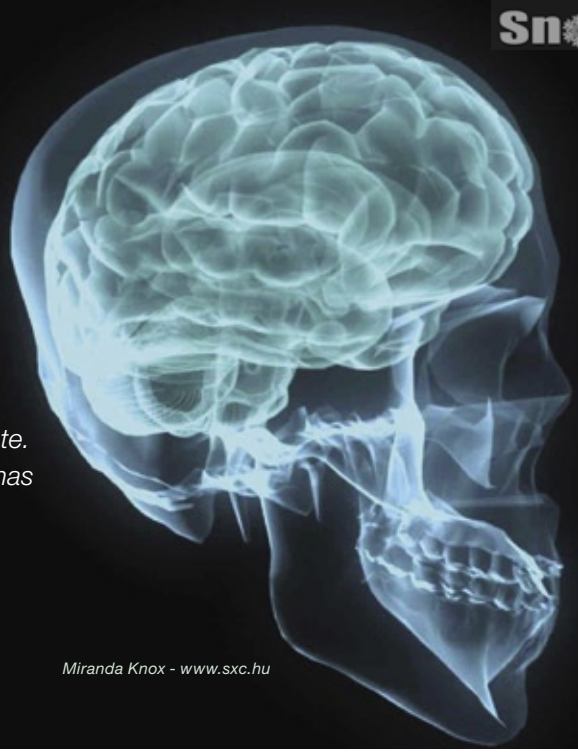
Se o objetivo for uma alternativa eficiente para virtualização bem integrada ao Linux, é hora de experimentar o KVM. ■

Mais informações

[1] KVM: http://kvm.qumranet.com

Programação de redes neurais com a Libfann

Jogos cerebrais



Miranda Knox - www.sxc.hu

3, 4, 8, 11… ? Uma rede neural consegue completar essa seqüência sem conhecer seu algoritmo subjacente. Veja como as redes neurais ajudam a resolver problemas simulando o comportamento de um cérebro.

por Andreas Romeyke

Ao procurar um caminho num mapa, seus olhos cairão diretamente numa solução eficiente. O cérebro humano é capaz de fazer julgamentos sem muita atenção a algoritmos de otimização ou cálculos de distância. Essa técnica intuitiva é totalmente alheia aos computadores digitais. Os programas de computador convencionais tendem a operar através de soluções matemáticas, tornando-os ineficientes em tarefas como predição e reconhecimento de padrões. Uma forma experimental de programa conhecida como *Rede Neural Artificial* (RNA, ou *ANN* na abreviação em inglês) resolve esse problema fazendo o computador funcionar de forma mais semelhante a um cérebro biológico.

Uma rede neural artificial simula um conjunto de células nervosas conectadas por caminhos ponderados. Um uso de sucesso para redes neurais é o campo do reconhecimento de faces. Uma rede neural consegue reconhecer um rosto com base num conjunto de pixels coloridos, apesar de ruído ou distorção, exatamente como um humano. Outras aplicações para a tecnologia de redes neurais incluem o reconhecimento óptico de caracteres ou previsões de manchas solares e preços de ações.

Neste artigo, veremos os princípios básicos das redes neurais, e introduziremos a biblioteca *Libfann*[1], que pode ser usada para criação de aplicações com uso de redes neurais.

Modelo natural

Uma rede neural simula a estrutura de um cérebro. Ela modela o efeito de um conjunto de neurônios que influenciam os estados uns dos outros através de um grande número de conexões. O peso diferencial das conexões neurais, que representam as fibras nervosas do cérebro, produz um valor de saída específico para um padrão específico de neurônios receptores. As conexões entre neurônios são ajustadas através de um processo análogo a um *treinamento*. Nesse processo, a rede neural aprende a associar padrões de entrada específicos a valores de saída específicos. Se o treinamento tiver sucesso, o cérebro artificial será capaz de descobrir soluções não especificamente apresentadas como exemplos.

A **figura 1** mostra uma célula nervosa, o modelo natural dos neurônios de uma RNA. A célula nervosa contém o corpo e dendritos que saem deste. Os dendritos transportam impulsos elétricos ao corpo da célula. Se a soma total desses impulsos exceder um valor limite pré-definido (potencial de ação), o neurônio torna-se ativo, enviando impulsos às células às quais está conectado.

Um neurônio artificial simula as propriedades de seu equivalente

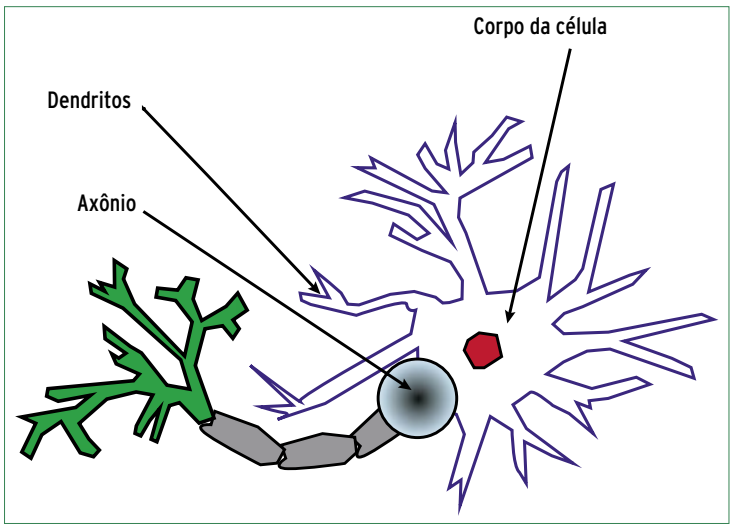


Figura 1 Os neurocientistas consideram as ramificações das células nervosas como a base do poder do cérebro para reconhecer padrões ou prever estados do sistema difíceis de calcular.

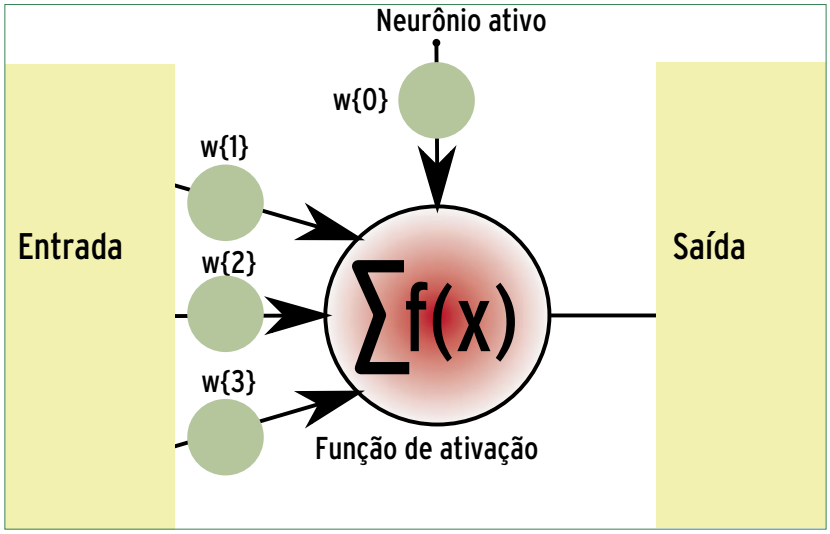


Figura 2 Assim como seus equivalentes biológicos, neurônios artificiais calculam a soma do potencial de ação dos neurônios conectados a eles, e repassam o sinal para outros neurônios através de conexões ponderadas.

natural: ele soma os potenciais de seus dendritos, aplica uma função fixa especial de ativação e passa os resultados a todas as células conectadas a ele (**figura 2**). As conexões com outros neurônios são ponderadas para atenuar ou amplificar o sinal ao longo de seu caminho.

A *função de ativação* define o limite no qual o neurônio será ativado. Abaixo desse valor, o neurônio não enviará sinais. Essa função freqüentemente é uma função simples de limite que retorna 1 se a soma de todas as saídas for superior a um valor específico. É comum representar a função de ativação num neurônio separado conhecido como *ativar neurônio* (*on neuron*). Então, pode-se ponderar a *ativar neurônio* como as conexões a outros neurônios.

Projeto

O processo de treinamento adapta a rede neural a uma situação específica; porém, na escala estrutural, o desenvolvedor também pode escolher uma topologia para a rede neural que reflita seu uso pretendido. Diferentes tipos de conexões entre neurônios levam a redes com características diferentes[2].

Uma das topologias de rede mais simples, bem explorada pela pesquisa científica, é o modelo de perceptron multicamada (*MLP*, na sigla em português) pró-alimentado[2]. Esse modelo divide a rede em camadas separadas. Essa rede não possui *feedback*; em outras palavras, o potencial de atuação simplesmente se propaga da esquerda para a direita (veja a **figura 3**).

As capacidades de uma rede neural, tais como a habilidade de reconhecer padrões ou prever valores, são um produto da estrutura interna da rede.

As operações a seguir modificam as características de uma RNA:

- adicionar novas conexões ou eliminar as já existentes;
- modificar os pesos das conexões entre neurônios;
- modificar os valores de limite dos neurônios;
- acrescentar ou eliminar neurônios.

O treinamento oferece os pesos adequados para resolver um problema específico. No caso do reconhecimento de caracteres, a entrada seria uma imagem ou um trecho de um texto e os respectivos códigos de caracteres. No caso do comportamento do mercado de ações ou da atividade das manchas solares, os dados históricos são usados para treinar a rede neural (**figura 4**). Uma função de aprendizado compara a entrada do exemplo com os valores de objetivo, e modifica as conexões neuronais, pesando até a reação da rede ser correspondente ao objetivo.

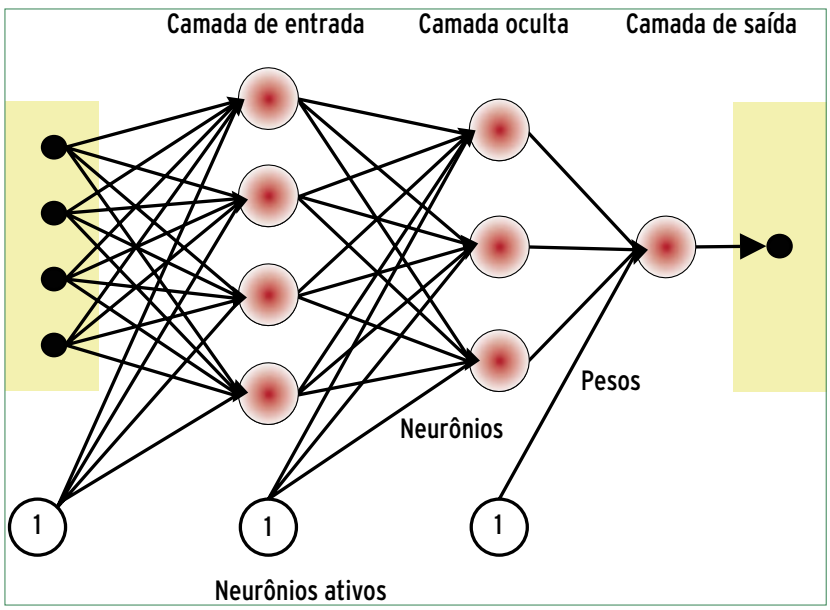


Figura 3 O perceptron multi-camada, que permite a propagação do potencial da entrada para a saída sem *loops* de retorno, é a rede neural artificial mais simples e melhor explorada.

Dentro da mente

Descreveremos agora, com um exemplo simples, o que acontece na fase de aprendizado de uma rede neural. Imagine que queiramos uma rede com quatro neurônios para prever o valor médio de dois números (veja a **figura 5**). No lado esquerdo da figura, os números `0,1` e `0,3` são entrados nos neurônios receptores. Inicialmente, as conexões neuronais possuem pesos aleatórios. A função de ativação, que define a forma como um neurônio reage à entrada, é $f(x) = x$. RNAs mais poderosas precisam de funções mais complexas, obviamente, mas esse exemplo simples é adequado para explicar o princípio subjacente.

Se os neurônios receptores possuem os valores de 0,1 e 0,3, pesar as conexões para os potenciais oferecem os seguintes valores: $(0{,}1*1{,}0 + 0{,}3*0{,}9 + 1{,}0*0{,}4) = 0{,}77$ para o primeiro neurônio $N(1,1)$, e $(0{,}1*0{,}2 + 0{,}3*0{,}3 + 1{,}0*0{,}7) = 0{,}81$ para o segundo neurônio $N(1,2)$. O neurônio entre as camadas de entrada e saída possui valor de $(0{,}77*0{,}5 + 0{,}81*0{,}1 + 1{,}0*0{,}2) = 0{,}666$. O neurônio de saída retorna o valor de $(0{,}666*0{,}2 + 1{,}0*0{,}3) = 0{,}433$, embora a média correta dos números 0,1 e 0,3 seja 0,2.

Em outras palavras, a rede não chegou muito perto do valor correto na primeira tentativa. Para permitir que a RNA ajuste sua matemática, é necessário modificar a pesagem das conexões neuronais. A contribuição do erro permite descobrir qual pesagem entre quais neurônios devem ser corrigidas. A contribuição do erro é o quadrado do valor de saída esperado menos o quadrado dos valores retornados nos neurônios de saída. O valor resultante é conhecido como erro quadrado médio (*MSE* ou *MQLE*, na notação em inglês).

Marcha a ré

Potenciais de ação geralmente movem-se adiante na rede a partir da entrada em direção à saída (sentido normal). Um método de ensino conhecido como propagação reversa (ou *back propagation*, como costuma ser chamado) inverte essa direção. Ele informa o valor de erro retornado na saída de volta, através da rede em direção à entrada, com base nos pesos das conexões individuais. A distribuição dos valores de erro sobre os nós da rede oferece a base para a modificação dos pesos. Os especialistas já desenvolveram vários outros métodos de ensino além desse, e alguns prometem resultados melhores para certas tarefas.

A **figura 6** mostra como a contribuição do erro se propaga para trás a partir da saída. O potencial do neurônio de saída é a soma de suas duas conexões: aquela com o neurônio ativo, com peso de 0,3, e a com o neurônio na camada abaixo, com peso de 0,2. Com base nisso, a contribuição do erro $(0{,}433 - 0{,}2 = 0{,}233)$ no neurônio de saída é distribuída pelas duas conexões. O caminho para o neurônio ativo tem uma fatia de $0{,}3/(0{,}2+0{,}3) = 60\%$, e o caminho para o neurônio abaixo tem a fatia de $0{,}2/(0{,}2+0{,}3) = 40\%$. Essa técnica possibilita o cálculo do potencial de erro total para cada conexão neuronal.

Ao final, um fator fixo de aprendizado estipula como uma contribuição de erro influencia o peso. Uma boa escolha de fator de aprendizado é um pré-requisito importante para o treinamento eficaz. Assim como vários outros parâmetros da rede, esse fator é desconhecido no início do treinamento. O treinamento completo de uma RNA sempre envolve um grande número de ciclos de propagações reversas, com pares de valores de entrada e saída para o problema que deve ser resolvido pela rede ao final.

Plano de treinamento

É óbvio que os pesos jamais devem ter valor zero, pois não haveria forma de traçar os erros. Pesos muito semelhantes ou com diferenças muito grandes teriam efeito negativo sobre o processo de aprendizado. Para uma RNA eficiente, é preferível que os sinais se propaguem através de toda a rede, exceto por áreas específicas, para lidar com padrões específicos.

Em aplicações práticas, a simples função de ativação $f(x) = x$ será substituída por uma tangente hiperbólica ou uma função sigmoidal. Isso aumenta o desempenho da rede neural, pois essas funções podem mapear

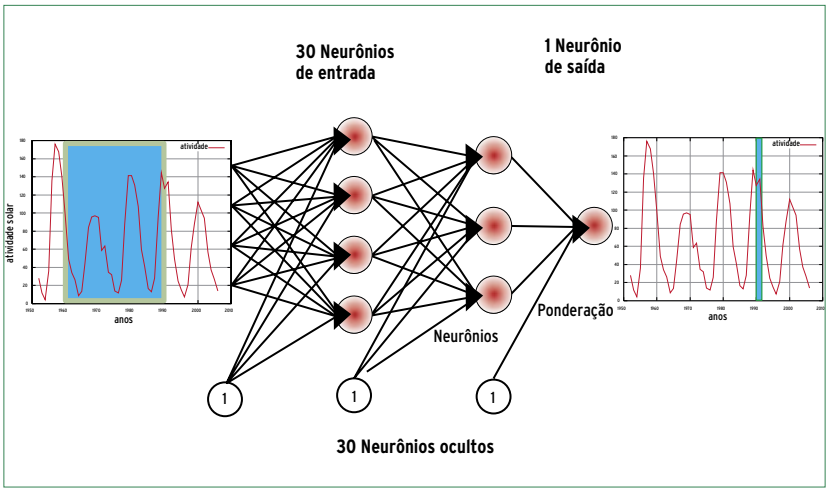


Figura 4 Uma rede neural com três camadas de neurônios prevê a atividade das manchas solares nos últimos 30 anos, e assim aprende a prever o fenômeno para o ano que vem.

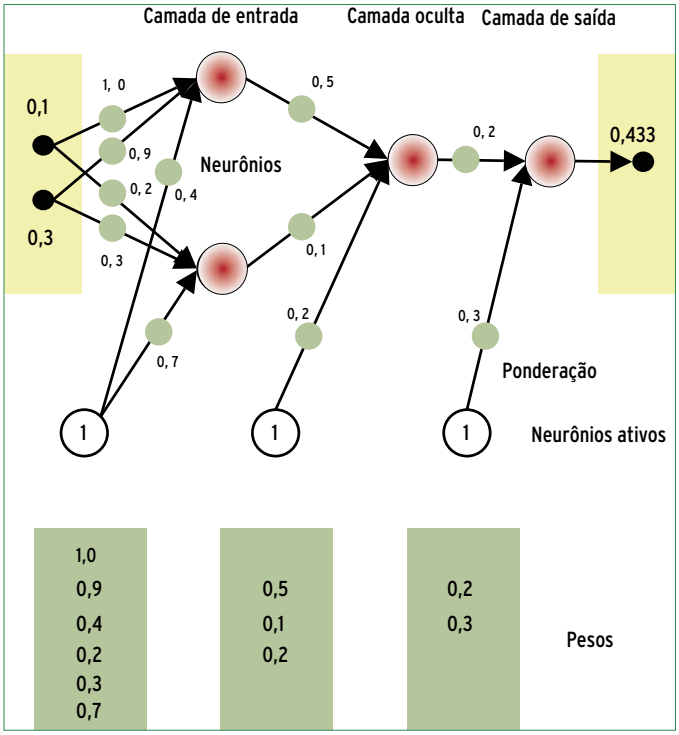


Figura 5 O comportamento da rede neural é definido pela ponderação das conexões neuronais e os neurônios ativos, que fixam o limite pelos quais os neurônios passarão estímulos para os outros.

uma faixa de entrada até o infinito com valores úteis. A back propagation também pressupõe que a função de ativação possa ser invertida. A vantagem desse esforço adicional é que os perceptrons de três camadas são capazes de aprender funções matemáticas arbitrárias, supondo que usem funções de ativação não lineares adequadas.

Libfann

A biblioteca *Fast Artificial Neural Network* (*FANN*) é uma biblioteca gratuita e de Código Aberto que fornece uma interface em C para implementar redes neurais multicamadas. A biblioteca foi desenvolvida em 2003 por Steffen Nissen, na Universidade de Copenhague, como parte de sua pesquisa científica, e ainda está em desenvolvimento ativo. A Libfann é fácil de usar e bem documentada, e roda em qualquer plataforma popular. A página do projeto também possui alguns exemplos práticos que facilitam a introdução a seu uso. Fora C, há ligações para todas as linguagens de programação mais comuns. No momento da escrita deste artigo, a Libfann é uma das implementações mais rápidas para simulações de redes neurais.

A maioria das distribuições Linux inclui a versão 1.2 da biblioteca. Um `aptitude install libfann1-dev` instala-a em qualquer distribuição derivada do *Debian*. O código-fonte, que pode ser compilado com os passos tradicionais, `configure; make; make install`, está disponível em [1].

Compilação

Todas as aplicações de redes neurais são diferentes, e é impossível explorar todas as sutilezas desse complexo campo num único artigo. O site do projeto Libfann inclui um manual de referência com descrições e notas de uso para as funções da biblioteca. O site da **Linux Magazine** contém em [3] um exemplo de programa em C que cria uma rede neural e a treina.

Para os que desejarem experimentar, algumas das funções mais importantes da Libfann são `fann_train()`, `fann_run()` e `fann_test()`. A função `fann_train()` espera uma *struct* de rede, `struct fann * ann;`, como seu primeiro parâmetro. Pode-se chamar `ann=fann_create(taxa_conexão, taxa_aprendizado, num_camadas, num_entrada, num_neurônios_ocultos, num_saída);` para criar a struct. `taxa_conexão` especifica a força das conexões entre os neurônios. O valor correto normalmente é `1.0`. `taxa_aprendizado` deve ficar entre `0.7` e `0.00001`. O parâmetro `num_camadas` e os valores após ele informam à Libfann o número de camadas da rede e o número de neurônios em cada uma delas.

Treino e pensamento

Paralelos com o pensamento humano são úteis para entender o que se passa durante o treinamento e descobrir a fonte de quaisquer problemas numa rede neural – afinal, elas emulam a estrutura do cérebro. Se a sessão de treinamento informar os dados históricos em ordem cronológica, a rede talvez desenvolva visão em túnel. Isso afetaria a capacidade da RNA de lidar com novos dados.

Uma ordem aleatória evita a generalização prematura, e portanto a necessidade de treinar novamente a rede neural após uma estrutura inválida ser estabelecida nas conexões neuronais. Por isso, o script em *Perl*[3] garante uma ordem aleatória aos dados.

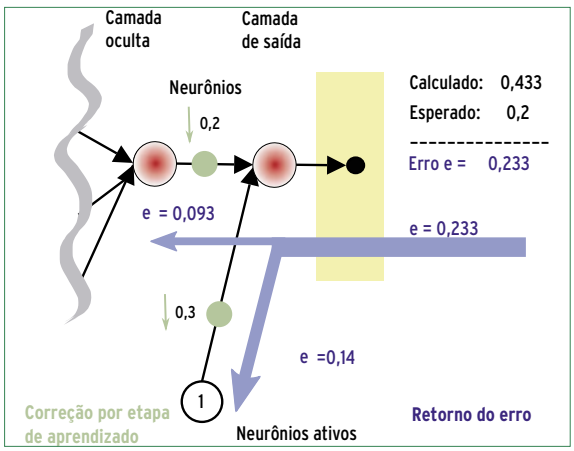


Figura 6 Redes neurais aprendem cometendo erros de previsão de valores específicos, rastreando esses erros de volta por sua estrutura e re-pesando as conexões entre neurônios que contribuíram para esses erros.

Dados que a rede não tenha visto durante o treinamento ajudam a julgar a eficácia com que a RNA consegue lidar com abstrações no estado atual do treinamento. O script em Perl divide os dados em dois subconjuntos. O erro que ocorre nesse caso é chamado de erro médio quadrado de generalização, ou *MQGE*. Junto com o *MQLE* (erro médio quadrado de aprendizado), ele informa se a rede neural está pronta para prever o futuro ou se é necessário mais treinamento. A Libfann injeta os dois valores através das funções `fanntest(rna, vetor_entrada, vetor_saídaesperada)` e `fann_get_MSE()`. Por último, `fann_save(rna,arquivo)` armazena a estrutura da rede e os pesos atuais para uso futuro.

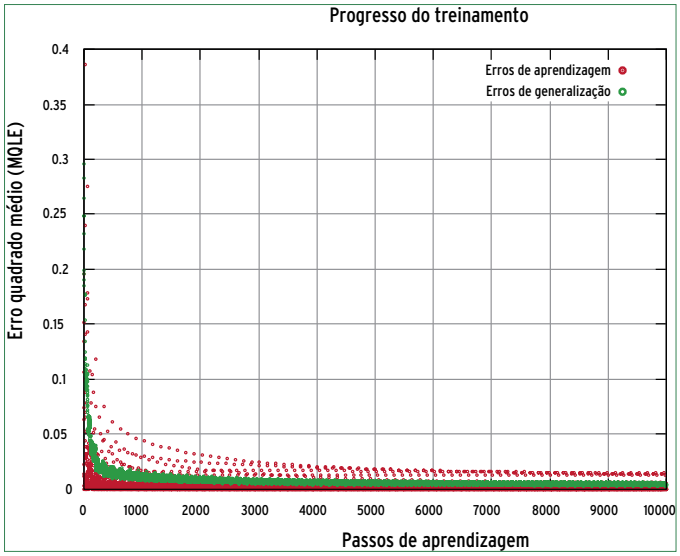


Figura 7 Num treinamento de sucesso, o *MQLE* cai continuamente, e a rede vai melhorando seu desempenho.

Vida real

O sucesso do treinamento depende não apenas dos dados, mas também da adequação da estrutura da rede à tarefa em questão – a começar pela função de ativação.

A Libfann usa a função sigmóide por padrão, e isso não é um problema para prever a atividade das manchas solares e outros fenômenos que se encaixam numa faixa positiva. Porém, no caso de preços de ações e outras séries temporais com valores negativos, é necessária a função de tangente hiperbólica `fann_set_activation_function_output(rna, FANN_SIGMOID)`.

O fator de aprendizado também influencia fortemente o sucesso ou fracasso do treinamento, pois especifica qual o efeito dos erros de aprendizado sobre os pesos das conexões entre neurônios, e sobre o número de neurônios da rede. O número de neurônios na camada intermediária deveria manter-se num mínimo, inicialmente. Três ou um máximo de 15 neurônios são suficientes para a maioria das aplicações. A tentativa e erro também oferecerão uma medida dos números adequados. Para essa sessão de treinamento, 500 mil passos de aprendizado devem ser um número suficiente.

Se o número de erros de aprendizado não cair continuamente, a rede fica parada num mínimo local, e seu desempenho dificilmente melhora, não importa a duração do treinamento. Nesse caso, é necessário reiniciar o treinamento com um fator de aprendizado menor, e possivelmente alterando a estrutura da rede.

Inspecionar o arquivo `fann_save` pode revelar o motivo do baixo desempenho da rede simplesmente pelo treinamento: neurônios individuais com pesos excessivos freqüentemente interferem no processo de aprendizado.

Se a curva de aprendizado continuar caindo, como mostrado na **figura 7**, então é hora de consultar o erro de generalização: se a curva for suave, não se deve esperar grande capacidade de previsão. A rede aprendeu os valores de treinamento e receberá valores de entrada desconhecidos. Para alterar isso, é necessário reduzir o número de neurônios ocultos.

Se o erro de generalização estiver num nível consistentemente alto, o número de nós ocultos está pequeno demais, ou a sessão de treinamento não foi suficientemente intensa.

A função `fann_load` da Libfann carrega uma rede armazenada anteriormente com `fann_save()`. A função `fann_run(rna, entrada)` retorna a saída da rede treinada. O script em Perl automatiza o teste do cérebro artificial. Nesse teste, a saída de uma rede treinada com sucesso foi bastante próximo às previsões.

Conclusão

A Libfann facilita a criação, treinamento e uso de RNAs. Os usuários não precisam preocupar-se com detalhes matemáticos como a inversão da função de ativação.

Escolher parâmetros como a taxa de aprendizado e o número de neurônios intermediários realmente demanda experiência e paciência. Os erros de aprendizado e generalização, além de um conhecimento da saturação de neurônios individuais, fornecem indicações dos motivos de falha de uma rede específica. A Libfann ajuda a precisar esses valores.

A versão atual (2.0) da Libfann estende seu escopo funcional, acrescentando novos algoritmos de aprendizado e tipos de neurônios. ■

Mais informações

[1] Libfann: http://fann.sourceforge.net

[2] Redes neurais artificiais: http://pt.wikipedia.org/wiki/Rede_neural

[3] Programa de treinamento: http://www.linuxmagazine.com.br/

[4] Warren Sarle, FAQ sobre RNAs: http://www.faqs.org/faqs/ai-faq/neural-nets/

Construindo interfaces com PHP-GTK

Hora de construir

Enquanto o uso das classes de PHP-GTK cria interfaces rápidas, o Glade pode tornar a tarefa ainda mais fácil.

por Pablo Dall'Oglio

No primeiro artigo desta série[1], conhecemos o *PHP-GTK*, extensão da linguagem de programação *PHP*, que nos permite desenvolver aplicações gráficas *standalone*. Neste segundo artigo, iremos estudar as diversas formas de se construir uma interface.

Exemplo 1: Janela subdividida

```
01 <?php
02 // cria a janela
03 $janela = new GtkWindow;
04 $janela->set_size_request(300,200);
05 $janela->set_border_width(20);
06 $janela->set_title('Título da
➥Janela');
07
08 // cria boxes
09 $caixa_vert= new GtkVBox;
10 $caixa_horz= new GtkHBox;
11
12 // adiciona caixa horizontal na
➥janela
13 $janela->add($caixa_horz);
14
15 // adiciona elementos na caixa
➥horizontal
16 $caixa_horz->pack_start(new
➥GtkLabel('elemento1'));
17 $caixa_horz->pack_start($caixa_
➥vert);
18 $caixa_horz->pack_start(new
➥GtkLabel('elemento2'));
19
20 // adiciona elementos na caixa
➥vertical
21 $caixa_vert->pack_start(new
➥GtkLabel('elementoA'));
22 $caixa_vert->pack_start(new
➥GtkLabel('elementoB'));
23 $caixa_vert->pack_start(new
➥GtkLabel('elementoC'));
24
25 // exibe a janela
26 $janela->show_all();
27
28 Gtk::Main();
29 ?>
```

A biblioteca *GTK* é formada por um conjunto de classes, organizadas hierarquicamente e que disponibilizam uma interface totalmente orientada a objetos. Isso permite o reaproveitamento de código através de mecanismos como a herança. A grande maioria das classes descende da superclasse `GtkObject`. Toda classe-filha herda automaticamente o comportamento (métodos e propriedades) da classe pai. Para exemplificarmos, todas as classes descendentes de `GtkBin` são contêineres que podem conter um elemento em seu interior. Já as classes descendentes de `GtkBox` podem conter vários.

Empacotamento

A primeira forma de construirmos a interface gráfica é através do empacotamento de objetos, ou seja, colocando uns objetos dentro de outros. Para tal, é necessário entender quais objetos permitem que se adicione conteúdo (contêineres) e quais não.

Em princípio, objetos descendentes da classe `GtkContainer` podem conter outros elementos dentro de si. No **exemplo 1**, iremos construir uma janela (`GtkWindow`) e adicionar uma caixa horizontal em seu interior. Dentro da caixa horizontal, vamos adicionar três objetos, conforme a **figura 1**: dois rótulos de texto (`GtkLabel`), sendo um em cada extremidade, e uma caixa vertical no centro, sendo que essa caixa vertical contém outros três objetos do tipo `GtkLabel` (rótulos de texto).

Observe que podemos construir a interface recursivamente, colocando objetos dentro de objetos.

Posições Fixas

Quem considera complexo demais projetar o visual do aplicativo com base no empacotamento pode dispor da construção baseada em posições fixas. O GTK possui um contêiner chamado `GtkFixed`, que proporciona uma área na qual os objetos podem ser ancorados em coordenadas absolutas definidas em pixels. No **exemplo 2**, criamos um objeto chamado `$fixed_area`, que é justamente um objeto do tipo `GtkFixed` dentro da janela. A partir disso, colocamos vários objetos em seu interior (**figura 2**), sempre definindo a posição em termos de coluna e linha, por meio do método `put()`.

Glade

Até o momento, construímos o visual do aplicativo via programação. Essa forma de desenvolvimento melhora o desempenho do aplicativo, mas, por outro lado, não é tão produtiva para programadores acostumados com ambientes *RAD*. Para situações em que precisamos de maior agilidade no desenvolvimento visual do aplicativo, podemos utilizar o *Glade*.

Figura 1 Uma janela com três elementos dispostos horizontalmente.

Figura 2 Uma janela com múltiplos elementos, usando localização fixa.

O Glade é uma ferramenta criada especialmente para desenho visual de aplicativos GTK. Ele pode ser utilizado em conjunto com todas as linguagens que suportam o GTK.

Essa ferramenta disponibiliza ao programador uma paleta de componentes e uma janela de propriedades que propiciam a construção de interfaces por meio de recursos como clicar-e-arrastar, entre outros. O resultado final do arquivo salvo pelo Glade é um documento *XML* com a extensão `.glade`.

Exemplo 2: Janela com múltiplos elementos

```
01 <?php
02 // cria a janela
03 $janela = new GtkWindow;
04 $janela->set_size_request(300,200);
05 $janela->set_border_width(20);
06 $janela->set_title('Título da Janela');
07
08 // cria fixed
09 $fixed_area= new GtkFixed;
10
11 // adiciona área fixa na janela
12 $janela->add($fixed_area);
13
14 // instancia diversos objetos
15 $rotulo1 = new GtkLabel('elemento1');
16 $rotulo2 = new GtkLabel('elemento2');
17 $botao   = new GtkButton('clique aqui');
18 $check   = new GtkCheckButton('checkbutto
➥n');
19 $radio   = new GtkRadioButton(null,
➥'radiobutton');
20 $combo   = new GtkCombo;
21
22 // coloca objetos na área fixa
23 $fixed_area->put($rotulo1, 10,  10);
24 $fixed_area->put($rotulo2, 140, 10);
25 $fixed_area->put($botao,   10,  50);
26 $fixed_area->put($check,   120, 50);
27 $fixed_area->put($radio,   120, 80);
28 $fixed_area->put($combo,   0,  120);
29
30 // exibe a janela
31 $janela->show_all();
32
33 Gtk::Main();
34 ?>
```

No **exemplo 3**, utilizamos uma interface criada no Glade. Veja que para interpretar o documento Glade precisamos fazer uso da classe `GladeXML`. Essa classe retorna um objeto `$glade`, que disponibiliza acesso a todos os objetos contidos dentro do documento. Para obtermos tais objetos, precisamos executar o método `get_widget()`, que recebe o nome do objeto (exibido na janela de propriedades) e retorna o objeto correspondente, como se ele fosse instanciado naquele momento.

Exemplo 3: Uso de arquivo .glade

```
01 <?php
02 //realiza leitura do documento glade
03 $glade  = new GladeXML('exemplo.
➥glade');
04
05 //obtém a janela contida no glade
06 $janela = $glade->get_
➥widget('window1');
07
08 //obtém o campo para digitação do
➥nome da pessoa
09 $nome   = $glade->get_widget('nome_
➥pessoa');
10
11 //joga um texto dentro do campo
12 $nome->set_text('digite o nome
➥aqui...');
13
14 //exibe a janela
15 $janela->show_all();
16
17 Gtk::Main();
18 ?>
```

Conclusão

Neste artigo, apenas vimos como construir uma interface inanimada. No próximo artigo da série, vamos estudar como se dá a programação de eventos, que nos permitirá escrever funções que reagem às ações tomadas pelo usuário frente à aplicação. ■

Mais informações

[1] Pablo Dall'Oglio, "Sempre Nativo". Linux Magazine 37, dezembro de 2007, pág. 70.

[2] PHP-GTK Brasil: http://www.php-gtk.com.br

[3] Site do autor: http://www.pablo.blog.br

[4] Livro PHP-GTK: http://www.php-gtk.com.br/book

Sobre o autor

Pablo Dall'Oglio (pablo@php.net) é graduado em Análise de Sistemas, autor de um livro sobre PHP-GTK e programa em PHP-GTK desde sua criação em 2001. É membro da equipe de documentação e criador da comunidade brasileira de PHP-GTK. Atualmente, é diretor de tecnologia e proprietário da Adianti Solutions, onde atua como consultor de tecnologia e engenheiro de software.

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										
NSI Training	Rio de Janeiro	Rua Araújo Porto Alegre, 71, 4ºandar 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			✔			✔
Solis	Lajeado	Rua Comandante Wagner, 12 – São Cristóvão – CEP: 95900-000	51 3714-6653	www.solis.coop.br		✔	✔	✔	✔	✔
DualCon	Novo Hamburgo	Rua Joaquim Pedro Soares, 1099, Sl. 305 – Centro	51 3593-5437	www.dualcon.com.br	✔		✔		✔	✔
Datarecover	Porto Alegre	Av. Carlos Gomes, 403, Sala 908, Centro Comercial Atrium Center – Bela Vista – CEP: 90480-003	51 3018-1200	www.datarecover.com.br	✔		✔			
LM2 Consulting	Porto Alegre	Rua Germano Petersen Junior, 101-Sl 202 – Higienópolis – CEP: 90540-140	51 3018-1007	www.lm2.com.br			✔		✔	✔
Lnx-IT Informação e Tecnologia	Porto Alegre	Av. Venâncio Aires, 1137 – Rio Branco – CEP: 90.040.193	51 3331-1446	www.lnx-it.inf.br	✔		✔		✔	✔
Plugin	Porto Alegre	Av. Júlio de Castilhos, 132, 11º andar Centro – CEP: 90030-130	51 4003-1001	www.plugin.com.br	✔		✔		✔	
TeHospedo	Porto Alegre	Rua dos Andradas, 1234/610 – Centro – CEP: 90020-008	51 3286-3799	www.tehospedo.com.br	✔	✔				
São Paulo										
Ws Host	Arthur Nogueira	Rua Jerere, 36 – Vista Alegre – CEP: 13280-000	19 3846-1137	www.wshost.com.br	✔		✔		✔	
DigiVoice	Barueri	Al. Juruá, 159, Térreo – Alphaville – CEP: 06455-010	11 4195-2557	www.digivoice.com.br	✔	✔	✔		✔	✔
Dextra Sistemas	Campinas	Rua Antônio Paioli, 320 – Pq. das Universidades – CEP: 13086-045	19 3256-6722	www.dextra.com.br			✔		✔	✔
Insigne Free Software do Brasil	Campinas	Av. Andrades Neves, 1579 – Castelo – CEP: 13070-001	19 3213-2100	www.insignesoftware.com			✔		✔	✔
Microcamp	Campinas	Av. Thomaz Alves, 20 – Centro – CEP: 13010-160	19 3236-1915	www.microcamp.com.br				✔		✔
PC2 Consultoria em Software Livre	Carapicuiba	Rua Edeia, 500 - 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	✔				✔	✔
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	✔		✔		✔	

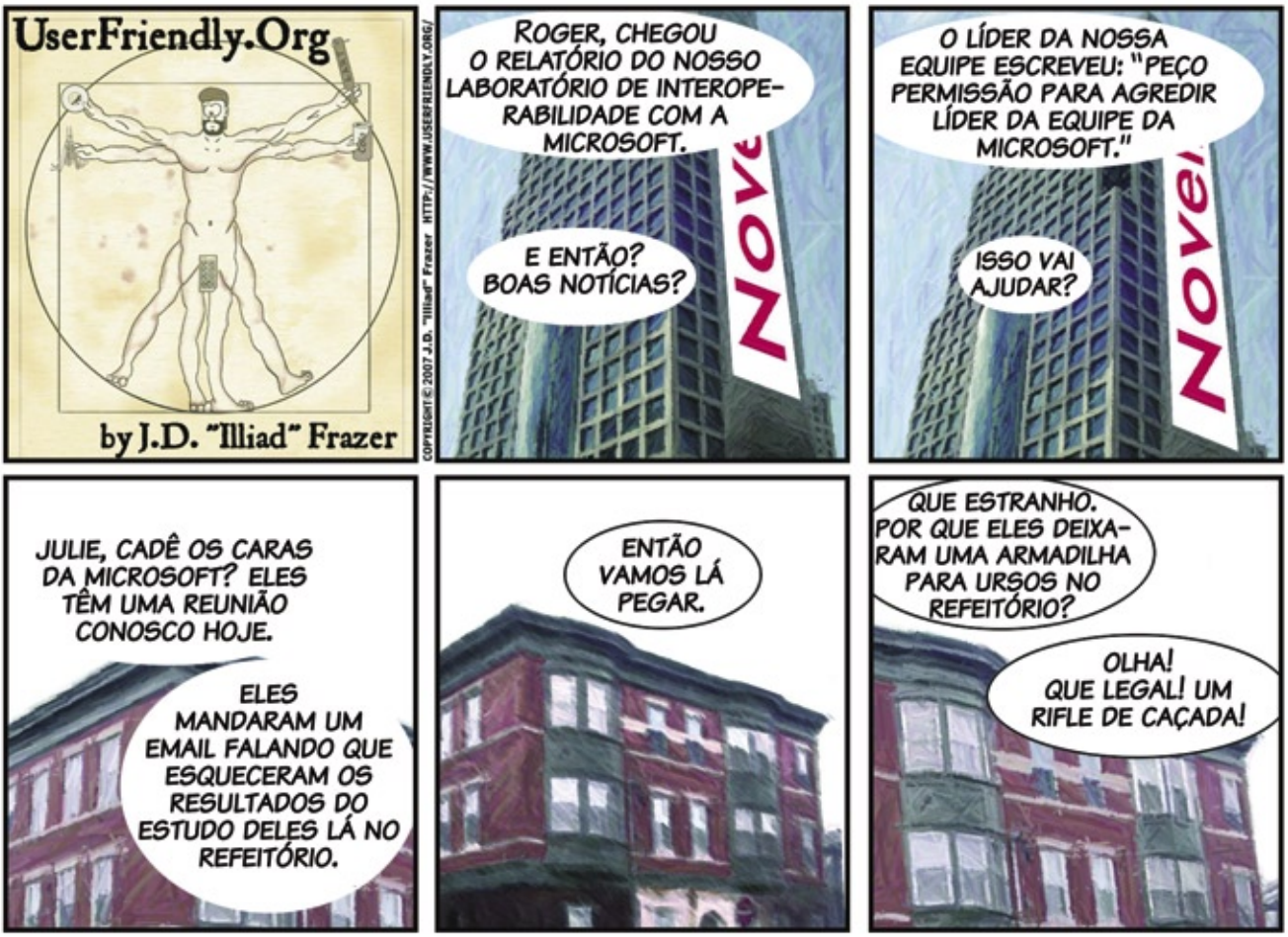
Empresa	Cidade	Endereço	Telefone	Web	1	2	3	4	5	6
São Paulo (continuação)										
4Linux	São Paulo	Rua Teixeira da Silva, 660, 6º andar – CEP: 04002-031	11 2125-4747	www.4linux.com.br					✔	✔
A Casa do Linux	São Paulo	Al. Jaú, 490 – Jd. Paulista – CEP 01420-000	11 3549-5151	www.acasadolinux.com.br			✔		✔	✔
Accenture do Brasil Ltda.	São Paulo	Rua Alexandre Dumas, 2051 – Chácara Santo Antônio – CEP: 04717-004	11 5188-3000	www.accenture.com.br			✔		✔	✔
ACR Informática	São Paulo	Rua Lincoln de Albuquerque, 65 –Perdizes – CEP: 05004-010	11 3873-1515	www.acrinformatica.com.br	✔					✔
Agit Informática	São Paulo	Rua Major Quedinho, 111, 5º andar, Cj. 508 – Centro – CEP: 01050-030	11 3255-4945	www.agit.com.br	✔	✔				✔
Altbit - Informática Comércio e Serviços LTDA.	São Paulo	Av. Francisco Matarazzo, 229, Cj. 57 – Água Branca – CEP 05001-000	11 3879-9390	www.altbit.com.br	✔		✔		✔	✔
AS2M -WPC Consultoria	São Paulo	Rua Três Rios, 131, Cj. 61A – Bom Retiro – CEP: 01123-001	11 3228-3709	www.wpc.com.br			✔		✔	✔
Big Host	São Paulo	Rua Dr. Miguel Couto, 58 – Centro – CEP: 01008-010	11 3033-4000	www.bighost.com.br	✔				✔	✔
Blanes	São Paulo	Rua André Ampére, 153 – 9º andar – Conj. 91 CEP: 04562-907 (próx. Av. L. C. Berrini)	11 5506-9677	www.blanes.com.br	✔	✔	✔		✔	✔
Commlogik do Brasil Ltda.	São Paulo	Av. das Nações Unidas, 13.797, Bloco II, 6º andar – Morumbi – CEP: 04794-000	11 5503-1011	www.commlogik.com.br	✔	✔	✔		✔	✔
Computer Consulting Projeto e Consultoria Ltda.	São Paulo	Rua Vergueiro, 6455, Cj. 06 – Alto do Ipiranga – CEP: 04273-100	11 5062-3927	www.computerconsulting.com.br	✔		✔		✔	✔
Consist Consultoria, Sistemas e Representações Ltda.	São Paulo	Av. das Nações Unidas, 20.727 – CEP: 04795-100	11 5693-7210	www.consist.com.br			✔	✔	✔	✔
Domínio Tecnologia	São Paulo	Rua das Carnaubeiras, 98 – Metrô Conceição – CEP: 04343-080	11 5017-0040	www.dominiotecnologia.com.br	✔					✔
EDS do Brasil	São Paulo	Av. Pres. Juscelino Kubistcheck, 1830 Torre 4 - 5º andar	11 3707-4100	www.eds.com		✔	✔			✔
Ética Tecnologia	São Paulo	Rua Nova York, 945 – Brooklin – CEP:04560-002	11 5093-3025	www.etica.net	✔		✔		✔	✔
Getronics ICT Solutions and Services	São Paulo	Rua Verbo Divino, 1207 – CEP: 04719-002	11 5187-2700	www.getronics.com/br			✔		✔	✔
Hewlett-Packard Brasil Ltda.	São Paulo	Av. das Nações Unidas, 12.901, 25º andar – CEP: 04578-000	11 5502-5000	www.hp.com.br	✔		✔	✔	✔	✔
IBM Brasil Ltda.	São Paulo	Rua Tutóia, 1157 – CEP: 04007-900	0800-7074 837	www.br.ibm.com	✔		✔		✔	✔
iFractal	São Paulo	Rua Fiação da Saúde, 145, Conj. 66 – Saúde – CEP: 04144-020	11 5078-6618	www.ifractal.com.br			✔		✔	✔
Integral	São Paulo	Rua Dr. Gentil Leite Martins, 295, 2º andar Jd. Prudência – CEP: 04648-001	11 5545-2600	www.integral.com.br	✔				✔	
Itautec S.A.	São Paulo	Rua Santa Catarina, 1 – Tatuapé – CEP: 03086-025	11 6097-3000	www.itautec.com.br	✔	✔	✔		✔	✔
Kenos Consultoria	São Paulo	Av: Fagundes Filho, 13, Conj -53, Cep: 04304-000	11 40821305	www.kenos.com.br					✔	✔
Konsultex Informatica	São Paulo	Av. Dr. Guilherme Dumont Villares, 1410 6 andar, CEP05640-003	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 – 02460-000	11 6979-0071	www.novateceditora.com.br				✔		
Novell América Latina	São Paulo	Rua Funchal, 418 – Vila Olímpia	11 3345-3900	www.novell.com/brasil			✔		✔	✔
Oracle do Brasil Sistemas Ltda.	São Paulo	Av. Alfredo Egídio de Souza Aranha, 100 – Bloco B – 5º andar – CEP: 04726-170	11 5189-3000	www.oracle.com.br					✔	✔
Proelbra Tecnologia Eletrônica Ltda.	São Paulo	Av. Rouxinol, 1.041, Cj. 204, 2º andar Moema – CEP: 04516-001	11 5052- 8044	www.proelbra.com.br	✔		✔			✔
Provider	São Paulo	Av. Cardoso de Melo, 1450, 6º andar – Vila Olímpia – CEP: 04548-005	11 2165-6500	www.e-provider.com.br			✔		✔	✔
Red Hat Brasil	São Paulo	Av. Brigadeiro Faria Lima, 3900, Cj 81 8º andar Itaim Bibi – CEP: 04538-132	11 3529-6000	www.redhat.com.br			✔		✔	✔
Samurai Projetos Especiais	São Paulo	Rua Barão do Triunfo, 550, 6º andar – CEP: 04602-002	11 5097-3014	www.samurai.com.br			✔		✔	✔
SAP Brasil	São Paulo	Av. das Nações Unidas, 11.541, 16º andar – CEP: 04578-000	11 5503-2400	www.sap.com.br			✔		✔	✔
Simples Consultoria	São Paulo	Rua Mourato Coelho, 299, Cj. 02 Pinheiros – CEP: 05417-010	11 3898-2121	www.simplesconsultoria.com.br			✔		✔	✔
Smart Solutions	São Paulo	Av. Jabaquara, 2940 cj 56 e 57	11 5052-5958	www.smart-tec.com.br		✔	✔		✔	✔
Snap IT	São Paulo	Rua João Gomes Junior, 131 – Jd. Bonfiglioli – CEP: 05299-000	11 3731-8008	www.snapit.com.br			✔		✔	✔
Stefanini IT Solutions	São Paulo	Av. Brig. Faria Lima, 1355, 19º – Pinheiros – CEP: 01452-919	11 3039-2000	www.stefanini.com.br			✔		✔	✔
Sun Microsystems	São Paulo	Rua Alexandre Dumas, 2016 – CEP: 04717-004	11 5187-2100	www.sun.com.br	✔		✔		✔	✔
Sybase Brasil	São Paulo	Av. Juscelino Kubitschek, 510, 9º andar Itaim Bibi – CEP: 04543-000	11 3046-7388	www.sybase.com.br					✔	✔
The Source	São Paulo	Rua Marquês de Abrantes, 203 – Chácara Tatuapé – CEP: 03060-020	11 6698-5090	www.thesource.com.br			✔		✔	✔
Unisys Brasil Ltda.	São Paulo	R. Alexandre Dumas 1658 – 6º, 7º e 8º andares – Chácara Santo Antônio – CEP: 04717-004	11 3305-7000	www.unisys.com.br	✔		✔		✔	✔
Utah	São Paulo	Av. Paulista, 925, 13º andar – Cerqueira César – CEP: 01311-916	11 3145-5888	www.utah.com.br			✔		✔	✔
Visuelles	São Paulo	Rua Eng. Domicio Diele Pacheco e Silva, 585 – Interlagos – CEP 04455-310	11 5614-1010	www.visuelles.com.br			✔		✔	✔
Webnow	São Paulo	Av. Nações Unidas, 12.995, 10º andar, Ed. Plaza Centenário – Chácara Itaim – CEP: 04578-000	11 5503-6510	www.webnow.com.br	✔		✔		✔	
WRL Informática Ltda.	São Paulo	Rua Santa Ifigênia, 211/213, Box 02– Centro – CEP: 01207-001	11 3362-1334	www.wrl.com.br	✔		✔		✔	
Systech	Taquaritinga	Rua São José, 1126 – Centro - Caixa Postal 71 – CEP: 15.900-000	16 3252-7308	www.systech-ltd.com.br	✔	✔			✔	

Calendário de eventos

Evento	Data	Local	Website
Lançamento do KDE 4.0	17 a 19 de janeiro	Mountain View, EUA	http://dot.kde.org/1191409937
Campus Party Brasil 2008	11 a 17 de fevereiro	São Paulo, SP	www.campusparty.com.br
PyCon	13 a 20 de março	Chicago, EUA	us.pycon.org
II Encontro Software Livre da Paraíba	2 a 4 de maio	João Pessoa, PB	ensol.org.br

Índice de anunciantes

User Friendly – Os quadrinhos mensais da Linux Magazine



LinuxWorld Conference & Expo – Worldwide Series

Seoul	June 20 – 23, 2007	www.linuxworldkorea.com
San Francisco	August 6 – 9, 2007	www.linuxworldexpo.com
Beijing	September 3 – 7, 2007	www.linuxworldchina.com
Stockholm	September 5, 2007	www.linuxworldsummit.se
London	October, 24 – 25, 2007	www.linuxworldexpo.co.uk
Utrecht	October 30 – November 1, 2007	www.linuxworldexpo.nl

LINUXWORLD® CONFERENCE & EXPO

World's leading Trade Event for Linux and Open Source in business

LINUX MAGAZINE

INTERNATIONAL MEDIA SPONSOR

PREVIEW

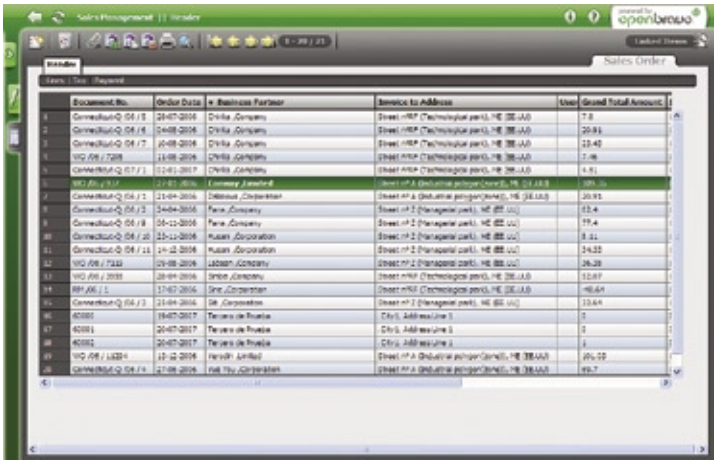
Na Linux Magazine #39

DESTAQUE

ERP e CRM em Linux

Se a palavra de ordem nas corporações atualmente é o controle, os aplicativos do momento são o ERP e o CRM. Para aumentar a eficiência de sua empresa, é fundamental reduzir os custos e aumentar a receita. Na busca desse objetivo, somente o controle das finanças e, em última instância, dos processos internos, pode ajudar.

Os softwares de *Enterprise Resource Planning* (Planejamento de Recursos da Empresa) e *Customer Relationship Management* (Gerenciamento de Relacionamento com o Cliente) oferecem a possibilidade de integrar as diversas fontes de informação, processos de produção, fluxos de dados e informações financeiras, entre outros, em um único sistema, de forma a possibilitar a consulta unificada desses dados pelos responsáveis, assim como a geração de relatórios e o acompanhamento dos processos.



Na **Linux Magazine** 39, apresentaremos o sistema de gestão empresarial *Openbravo*. Totalmente baseado na Web e de Código Aberto, o Openbravo é destinado às pequenas e médias empresas, e adota o modelo de software como serviço. Acessado por meio de qualquer navegador web, o Openbravo inclui as funcionalidades de ERP, partes de um CRM e ainda recursos de *Business Intelligence*. Sua arquitetura unificada elimina a falta de integração de diferentes módulos, oferecendo maior desempenho e flexibilidade.

Com arquitetura semelhante, o *ADempiere* também será apresentado na **Linux Magazine** 39. Criado como um *fork* do *Compiere*, o ADempiere introduziu o suporte ao banco de dados de Código Aberto *PostgreSQL*, além de aperfeiçoar alguns recursos de seu antecessor.

A arquitetura do ADempiere tem características em comum com a do Openbravo, como a ausência de modularidade, oferecendo grande flexibilidade e velocidade de execução. ■

TUTORIAL

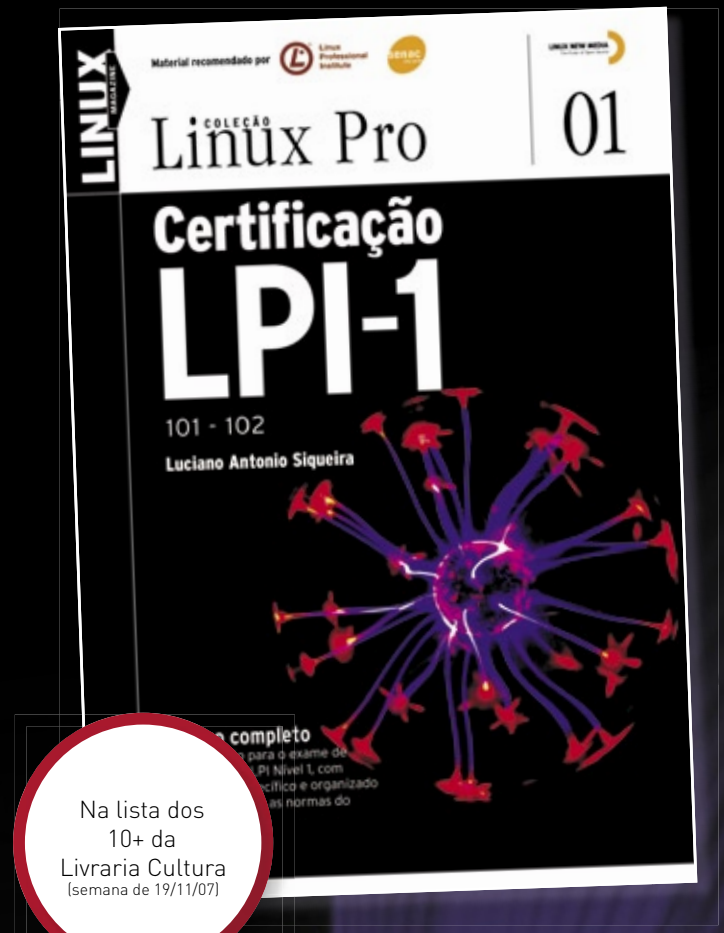
Curso LPI

A oitava aula do curso preparatório para a certificação LPIC-2 ensina a configuração de redes no Linux. Além da simples configuração das onipresentes redes Ethernet, serão apresentados temas como a configuração do protocolo *ARP*, a configuração de conexões discadas, *ISDN* e redes sem fio, assim como a manipulação da tabela de rotas do kernel.

Para isso, serão explorados os comandos `ifconfig`, `route`, `netstat`, `tcpdump`, `netcat` e `lsof`, com aprofundamento em sua sintaxe e suas múltiplas utilidades na administração de sistemas e redes.

Por último, será abordada a configuração de redes pessoais privadas (*VPNs*, na sigla em inglês) através do aplicativo *OpenVPN*. ■

Quer (re)conhecimento em Linux?



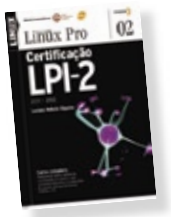
Só a LPI garante a formação que o mercado espera para lidar com os ambientes mais diversos.

Certifique-se para entrar num mercado em pleno crescimento no Brasil e no mundo!

Não se prenda a uma distribuição: o LPI certifica seus conhecimentos no Linux como um todo!

Prepare-se para a principal certificação profissional do mercado.

Leia também Certificação LPI-2:



Nas melhores livrarias ou no site www.linuxmagazine.com.br

LINUX MAGAZINE

LINUX NEW MEDIA

"A melhor conferência que
eu tive o prazer de participar."
Zack Rusin, *KDE/Mesa/Gallium3D*

"BOSSA Conference foi um evento impressionante.
Para mim, foi a melhor conferência de Open
source em 2007. Não perca a de 2008."
Marcel Holtmann, *Bluez Mainteiner*

"A melhor conferência que eu já participei.
Não perca a de 2008."
Carsten 'The Rasterman' Haitzler, *OpenMoko GUI/Enlightenment*

"Areia, sol e aparelhos móveis.
Bossa foi a conferência perfeita para discutir
o futuro do linux em sistemas embarcados."
John 'J5' Palmieri, *Red Hat/OLPC/DBus*

www.bossaconference.org

BOSSA'08 CONFERENCE

16 a 19 de Março
Conferência Internacional sobre
SOFTWARE OPEN SOURCE
para Aparelhos Móveis de Plataformas Embarcadas

Summerville Resort
Muro Alto - Pernambuco
Brasil