

BI EM NOVOS MERCADOS p.24
Com o SpagoBI, a Business Intelligence entra no radar de todos

NEGÓCIOS LIVRES p.26
Maddog apresenta modelos de negócios para Software Livre

ZIMBRA NO BRASIL p.28
Primeiro grande case de sucesso do groupware no país

53 Abril 2009



LINUX

MAGAZINE

A REVISTA DO PROFISSIONAL DE TI

rede em CRISE

ADMINISTRAR MÚLTIPLAS MÁQUINAS NÃO PRECISA SER UM PESADELO. BASTA USAR AS FERRAMENTAS CERTAS. p.31

- » Controle flexível com o poderoso Cfengine p.32
- » Cada máquina é diferente aos olhos do Bcfg2 p.42
- » Zenoss, de olho nos serviços e servidores p.48

exemplar de
Assinante
venda proibida



REDES: BIND PARA QUÊ? p.70

Em redes modestas, o Bind é desnecessário. O Dnsmasq é muito mais leve e simples, e ainda traz DHCP e TFTP.

SEGURANÇA: PROXY DO GOOGLE p.74

Se o Google encontra tudo na Internet, imagine como o seu Ratproxy pode ajudar a achar vulnerabilidades em qualquer aplicação web.

VEJA TAMBÉM NESTA EDIÇÃO:

- » Debian automatizado é com o FAI p.52
- » O melhor appliance Asterisk do mercado p.60
- » A Liberdade de Software em questão p.62
- » X2Go, SBC da próxima geração p.64

Promoção amigos do pinguim



LINUX
MAGAZINE

INDIQUE UM AMIGO
PARA ASSINAR A LINUX MAGAZINE.
ELE ASSINA E VOCÊ GANHA!

SEU AMIGO ASSINA A REVISTA POR UM ANO.
Você ganha um presente exclusivo e ele ganha
1 parcela paga da assinatura.



você

Além de receber conteúdo de qualidade todo mês, ganhará uma exclusiva mochila da Linux Magazine.



Mochila em poliéster preto, com bolso frontal e dois bolsos laterais.
Medidas: 40 x 30 cm.

seu amigo

Assina a Linux Magazine impressa por um ano (12 edições) + a versão digital (em PDF) e ganha uma parcela paga.

LINUX MAGAZINE + **LINUX** MAGAZINE ONLINE =

preço normal:

~~10 x 19,80~~

seu amigo paga:

9 x 19,80

Assine pela internet:

www.linuxmagazine.com.br/amigo

ou pelo telefone: **(11) 4082-1300**



O presente será enviado 35 dias após a confirmação do pagamento da segunda parcela. Ao ligar tenha em mãos seus dados, os do seu amigo e a forma de pagamento escolhida (cartão de crédito). Promoção válida até 30/06.

© Linux New Media do Brasil Editora Ltda.



11^o

ENCONTRO LOCAWEB DE PROFISSIONAIS DE INTERNET

**APROVEITE A CONEXÃO MAIS RÁPIDA QUE EXISTE:
TUDO DIRETO PRO SEU CÉREBRO.**

O maior encontro de profissionais de Internet do Brasil está esperando a sua inscrição. Acesse www.locaweb.com.br/encontro e saiba mais sobre o 11º Encontro Locaweb de Profissionais de Internet, que será realizado nas principais cidades do Brasil. Aproveite, outra transferência de dados em alta velocidade como esta só em 2010.

PALESTRAS

Tendências do Mercado de Internet	Gilberto Mautner
Agilidade e Qualidade de Projetos	Fabio Akita
O Google além das Buscas	Executivos do Google
A Internet além da Web	Executivos da Microsoft
O Novo Marketing para a Sociedade Digital	Marcelo Tripoli
Estratégias em Sites de Busca: SEO & SEM	Martha Gabriel

14 DE ABRIL: Belo Horizonte/MG • **6 DE MAIO:** Salvador/BA • **14 DE MAIO:** Curitiba/PR
21 DE MAIO: Porto Alegre/RS • **9 DE JUNHO:** Rio de Janeiro/RJ • **17 DE JUNHO:** São Paulo/SP

PATROCINADORES PLATINUM:

Microsoft

Google

REALIZAÇÃO:

LOCAWEB

PATROCINADOR GOLD:

info
EXAME

VEÍCULO OFICIAL:

Www.com.br

Expediente editorial

Diretor Geral

Rafael Peregrino da Silva
rperegrino@linuxmagazine.com.br

Editor

Pablo Hess
phess@linuxmagazine.com.br

Revisora

Aileen Otomi Nakamura
anakamura@linuxmagazine.com.br

Editora de Arte

Paola Viveiros
pviveiros@linuxmagazine.com.br

Centros de Competência

Centro de Competência em Software:

Oliver Frommel: ofrommel@linuxnewmedia.de
Kristian Kießling: kkiessling@linuxnewmedia.de
Peter Kreussel: pkreussel@linuxnewmedia.de
Marcel Hiltzinger: hiltzinger@linuxnewmedia.de

Centro de Competência em Redes e Segurança:

Achim Leitner: aleitner@linuxnewmedia.de
Jens-Christoph B.: jbreindel@linuxnewmedia.de
Hans-Georg Eßer: hgesser@linuxnewmedia.de
Thomas Leichtenstern: tleichtenstern@linuxnewmedia.de
Max Werner: mwerner@linuxnewmedia.de
Markus Fellner: mfellner@linuxnewmedia.de
Nils Magnus: nmagnus@linuxnewmedia.de

Anúncios:

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

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

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

Amy Phalen (Estados Unidos)
aphalen@linuxmagazine.com

Hubert Wiest (Outros países)
hwiest@linuxnewmedia.de

Gerente de Circulação

Claudio Bazzoli
cbazzoli@linuxmagazine.com.br

Na Internet:

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

Apesar de todos os cuidados possíveis terem sido tomados durante a produção desta revista, a editora não é responsável por eventuais imprecisões nela contidas ou por consequências que advenham de seu uso. A utilização de qualquer material da revista ocorre por conta e risco do leitor.

Nenhum material pode ser reproduzido em qualquer meio, em parte ou no todo, sem permissão expressa da editora. Assume-se que qualquer correspondência recebida, tal como cartas, emails, faxes, fotografias, artigos e desenhos, sejam fornecidos para publicação ou licenciamento a terceiros de forma mundial não-exclusiva pela Linux New Media do Brasil, a menos que explicitamente indicado.

Linux é uma marca registrada de Linus Torvalds.

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

Direitos Autorais e Marcas Registradas © 2004 - 2008:

Linux New Media do Brasil Editora Ltda.

Impressão e Acabamento: Parma

Distribuída em todo o país pela Dinap S.A.,

Distribuidora Nacional de Publicações, São Paulo.

Atendimento Assinante

www.linuxnewmedia.com.br/atendimento

São Paulo: +55 (0)11 3512 9460

Rio de Janeiro: +55 (0)21 3512 0888

Belo Horizonte: +55 (0)31 3516 1280

ISSN 1806-9428

Impresso no Brasil



INSTITUTO VERIFICADOR DE CIRCULAÇÃO

Mais do mesmo

Prezados leitores,

Praticamente todas as áreas do conhecimento humano estão sujeitas à moda. Não necessariamente no vestuário, mas em comportamento, produtos, metodologias e atitudes. E principalmente tecnologias. A partir do momento em que uma tecnologia se torna muito difundida – geralmente por mérito técnico, tecnológico e de marketing –, seu uso cresce de forma impressionante.

Entretanto, certas modas parecem recusar-se a passar. Tornam-se um hábito e passam a constituir parte de uma cultura estabelecida. Contestar tais culturas é saudável e desejável, mas quem o faz se passa no mínimo por iconoclasta e no máximo por reclamão.

A recente explosão de infecções de estações Windows pelo worm Conficker foi e continua sendo uma tragédia de grandes dimensões, e oferece um forte subsídio para contestarmos a cultura do uso indiscriminado desse sistema operacional, estabelecido há tantos anos.

É verdade que o sistema operacional, por si só, não foi o causador da disseminação da praga. Computadores com as últimas atualizações de segurança da Microsoft, compartilhamentos seguros, senhas fortes e antivírus em dia permaneceram imunes à ameaça. A crítica que deve ser feita, no entanto, cabe ao trabalho exigido do administrador ou usuário para tornar seu sistema seguro, e também à facilidade com que se compromete essa mesma segurança tão difícil de obter.

Gestores e outros profissionais de TI em todo o planeta perderam várias horas, senão dias de trabalho – e qualidade de vida, certamente – para solucionar infecções em suas redes ou apenas para evitá-las a qualquer custo.

A todos estes profissionais, pergunto: vale a pena insistir nesses sistemas operacionais proprietários? Há sistemas de código aberto para todas as necessidades, incluindo desktops, e seus usuários sequer foram atingidos pelo worm. Aliás, jamais tivemos uma infecção com tamanho sucesso atuando sobre sistemas de código aberto. Enquanto as companhias dependentes de sistemas Windows perdiam produtividade, aquelas que já adotaram amplamente o Código Aberto mantinham-se plenamente operacionais e funcionais.

Se os aspectos tecnológicos dos sistemas de código aberto, aliados à estabilidade e ao desempenho superiores, não são suficientes para desencadear a ampla adoção dessa plataforma, talvez a gota d'água caiba ao fator segurança – que se reflete diretamente na qualidade de vida dos administradores e gestores.

A indústria de TI já passou da época de sofrer com mais iterações das mesmas pragas de sempre. É hora de os administradores e gestores evitarem que suas empresas continuem vulneráveis aos mesmos males. ■



Pablo Hess
Editor

CAPA

Super máquina! 32

Automatize tarefas administrativas com a poderosa plataforma Cfengine.

O gerente 42

O poderoso Bcfg2 oferece um ambiente sofisticado para gerenciamento de configuração centralizado.

O observador 48

Veja como essa ferramenta boa, bonita, livre e gratuita pode ajudar no monitoramento de rede.



COLUNAS

Klaus Knopper	08
Charly Kühnast	10
Zack Brown	12
Augusto Campos	14
Insegurança	16
Pablo Hess	18

NOTÍCIAS

Geral	20
♦ O silverlight de código aberto	
♦ Linux New Media aplica provas LPI	
♦ Lançado o SUSE Linux Enterprise 11	
♦ Código aberto para automóveis	



CORPORATE

Notícias	22
♦ Crise favorece o Linux	
♦ A IBM vai adquirir a Sun?	
Entrevista: SpagoBI	24
Entrevista: M. Dias Branco	26
Coluna: Jon "maddog" Hall	28
Coluna: Cezar Taurion	30

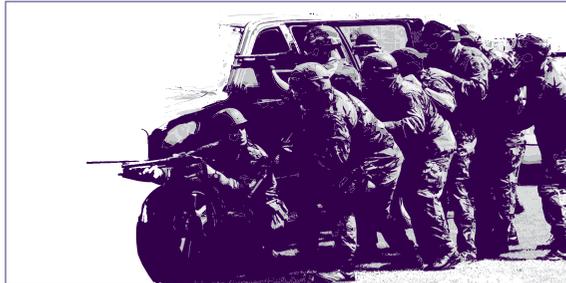
TUTORIAL

Turbilhão!	52
O FAI auxilia na automatização do processo de instalar e configurar novos sistemas Debian.	



ANÁLISE

Appliance para toda obra	60
O PIKA Warp é, além de um appliance VoIP completo baseado em Linux, uma plataforma para desenvolvimento de soluções customizadas.	
Flancos abertos por definição	62
O conceito do Software Livre é simples, mas ainda assim há quem se interesse em deturpá-lo para aproveitar suas vantagens sem se comprometer com a liberdade.	



REDES

Deixa com o servidor	64
Em sua versão 3, já quase pronta, o projeto livre X2Go traz funções como novos clientes e janelas sem decoração.	
DNS e muito mais	70
O Dnsmasq é uma alternativa prática para DNS em pequenas redes.	



SEGURANÇA

Tem rato na rede	74
O Ratproxy do Google é uma ferramenta gratuita que busca problemas de segurança em aplicações web.	



SERVIÇOS

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

Emails para o editor

Permissão de Escrita

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

Controle e balanceamento de banda

Primeiramente, meus parabéns pela ótima revista que é a Linux Magazine. Ela já me ajudou e está me ajudando muito no meu dia a dia.

Andei lendo em alguns blogs um assunto novo, que é o hardware Open Source. Seria bem interessante ver este assunto com mais detalhes e como podemos usufruir desse novo conceito em tecnologia.

Outro assunto interessante que gostaria de ver é o balanceamento de carga de banda larga com Linux. Já enfrentei um problema assim, mas acabei optando por um hardware específico, justamente por falta de conteúdos com clareza. Seria interessante também um assunto como esse. Creio que há pessoas que já passaram e passarão pelo mesmo problema que eu.

Edson Malta Soares Santos
São Paulo – SP

Resposta

Edson, muito obrigado pelas sugestões. Como de costume, fica a dica para autores que se interessarem pelo assunto, pois trata-se realmente de conteúdo muito importante.

Assim como hardwares específicos (appliances) resolvem perfeitamente a demanda por balanceamento de banda, distribuições Linux voltadas especificamente à tarefa de gateways ou roteadores também são bastante indicadas. Geralmente, contam com uma interface de gerenciamento via web que simplifica bastante a configuração e, dependendo da distribuição, até oferece gráficos bastante informativos.

Há também distribuições com esse fim baseadas em outros sistemas operacionais livres, como FreeBSD, por exemplo.

Fica a dica da redação para os demais leitores que enfrentarem a mesma necessidade.

Errata

Memri a distribu da

Na notícia "Xen Server agora é gratuito", à página 20 da edição 52 da Linux Magazine, o terceiro parágrafo diz equivocadamente que a ferramenta Storage Link permite a distribuição de memória virtual. O correto, no caso, era afirmar que a Storage Link permite a distribuição de dados, sejam eles arquivos ou imagens de sistemas.

O servidor ideal para o seu sistema open source. O servidor ideal para o futuro da sua empresa.



PENSAMENTO ALTERNATIVO EM OPEN SOURCE:

Escalabilidade, alta disponibilidade e baixo custo/performance.

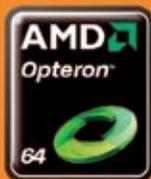
Os sistemas open source são a alternativa de muitas empresas que buscam administrar o ambiente de TI com menor investimento, além da consolidação e virtualização para otimizar a utilização dos recursos. E, para atender a essas demandas do seu negócio, agora você tem o servidor HP ProLiant DL785 G5. Ele proporciona uma infra-estrutura confiável para consolidar e virtualizar aplicações executadas em Linux RedHat® ou Suse® e Solaris10®. Atinge até 32 núcleos, fornece até 114 máquinas virtuais e é compatível com as tecnologias Xen® e VMware®, onde alcançou o mais alto desempenho em virtualização segundo o benchmark da VMark*. HP ProLiant DL785 G5. Entre alto desempenho ou baixo custo para sua empresa, fique com os dois.

Tecnologia para melhores resultados de negócios.



HP PROLIANT DL785 G5

- Até 8 processadores Quad-Core AMD Opteron®.
- Até 512 GB de memória.
- 11 slots de I/O PCI-e.
- Até 16 drivers SAS hot plug.



Para saber mais sobre o ProLiant DL785 G5, ligue para (11) 4689-2540





Coluna do Klaus

Pergunte ao Klaus!

O professor Klaus responde as mais diversas dúvidas dos leitores.

Instalei recentemente o Ubuntu 8.10 em meu laptop Medion MD 98300 na tentativa de me livrar do desastre do Windows Vista instalado no sistema. Quase tudo funciona perfeitamente, mas estou com alguns problemas. A maior dificuldade no momento é o som. Tocar músicas do disco rígido não é nenhum problema, mas a música só sai pelos alto-falantes embutidos. Com um cabo plugado ao meu aparelho de som, não sai som algum.

Tentei encontrar uma solução nas páginas de documentação do Ubuntu, mas as sugestões (atualizar para o driver ALSA mais recente) não surtiram efeito. Não consigo usar nem fones de ouvido.

Procurei em vários fóruns pessoas com problemas semelhantes, mas ainda não achei a solução. O chip de som é um Intel HDA com chip de áudio Realtek ALC 883.

Resposta

Seu chip de som talvez esteja sofrendo de má configuração do mixer interno. Já vi isso várias vezes nesse chipset. O problema é que independentemente do valor definido para o volume da saída de som, ele não muda nada. Na verdade, isso também acontece às vezes com as configurações *Master* e *PCM*.

A causa desse problema geralmente é a troca de canais. Em outras palavras, o canal *PCM* ou *line out* não está realmente fazendo o que o programa mixer diz. Em vez disso, algum outro controle do mixer lida com a função procurada. Frequentemente, *igain* ou *phone out* (sim!) definem o valor que se esperaria que o volume de *line out* definisse.

Para resolver o problema, primeiro inicie a sua ferramenta mixer preferida. Quanto mais botões e ajustes de canais diferentes houver, melhor. Eu costumo usar o *aumix* ou seu equivalente gráfico *aumix-gtk*, mas o *kmixer* do KDE deve funcionar tão bem quanto.

Agora reproduza um arquivo de áudio com o cabo ligado ao seu aparelho de som ou fones de ouvido (su-

ponho que você não tenha plugado o cabo nos conectores de microfone ou *line-in*). Defina os canais *Master*, *PCM* e *line out* com valores significativos (80 por cento deve ser suficiente), o que ainda não deve resolver o problema, e depois aumente também os valores de todos os canais de saída.

Tome cuidado com as configurações chamadas *monitor* e *feedback*, o que pode causar sons horrendos quando o microfone do laptop começar a captar o som vindo dos alto-falantes.

Se você tiver aumentado o volume de todos os canais de saída e nada de diferente tiver acontecido, experimente em seguida os canais *effect* e *amplifiers*. Um deles pode ser o verdadeiro controle de nível de saída que você procura. Como última tentativa, tente também o volume de *input level*, mas atente para os efeitos já mencionados de ressonância que podem surgir, principalmente ao desconectar seu cabo estéreo com o volume ainda no máximo e a música em andamento.

Se essas medidas não resolverem o problema da falta de som, talvez seja mesmo necessário um driver novo (ou um kernel novo) para esse chip de som; porém, é raro os alto-falantes embutidos funcionarem e a saída auxiliar não. Na maioria dos casos, os chips de áudio simplesmente não funcionam quando as interrupções e outros parâmetros são auto-detectados incorretamente.

Outra possibilidade é que o soquete esteja com defeito, mais isso causaria problemas em outros sistemas operacionais além do Linux.

Também é possível que outros dispositivos de áudio, como uma webcam com microfone, por exemplo, estejam confundindo as suas ações, pois talvez você esteja alterando os volumes desse outro dispositivo quando acha que está ajustando o chip de som do computador. ■

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



SUN OPEN-SOURCE UNIVERSITY MEETUP (OSUM) MUDE O MUNDO

Software Livre está Mudando Nosso Mundo (bom para a sociedade como um todo):

- SL promete um mundo de liberdades digitais
- Liberdade para participar, colaborar, criar, usar e distribuir
- Software Livre = Expansão de oportunidades
- Maior flexibilidade
- Novas comunidades
- Inovação contínua

Software livre está Mudando o Seu Mundo (bom para oportunidades de carreira para estudantes):

- Desenvolva habilidades para carreiras em TI
- Ótimo para projetos de estudantes
- Fortalece o aprendizado independente
- Comunidades criam oportunidades para colaboração
- Sem custo

A Sun é contribuinte líder em Software Livre. O suporte à Comunidade OSUM é parte do nosso comprometimento para assegurar que estudantes são capazes de perceber os benefícios do Software Livre para Mudar o Mundo.

Mude o Mundo.

> Sun.com/students

Participe de discussões com outros estudantes do mundo inteiro através do Sun Open-Source University Meet-Up (OSUM). OSUM (pronunciado "awesome") é a comunidade global para estudantes apaixonados por Software Livre e sobre como isso está Mudando O Mundo. Nós o chamamos de "Meet-Up" para encorajar colaboração entre grupos de estudantes criando uma comunidade de Software Livre ainda mais forte.

Através de atividades em campus, OSUMs patrocinados pela Sun receberão acesso a informações técnicas que podem ser compartilhadas com outros membros do OSUM por meio de demonstrações técnicas. Além disso, cursos online, através do programa Sun Academic Initiative estarão disponíveis ao OSUM para prover uma oportunidade de que seus membros possam ser Sun Certified.

A Sun fornecerá um website de rede social para todos os OSUMs registrados. Esta presença online possibilitará que a comunidade OSUM esteja conectada com desenvolvedores estudantes de todo o mundo. OSUMs podem colaborar online em forums e grupos de comunidades com outros desenvolvedores estudantes possuem os mesmos interesses técnicos.

Crie um OSUM na sua universidade e você ganhará acesso a:

- Treinamento Hands-On através de demonstrações técnicas e projetos estudantis
- Recursos livres e de baixo custo para estudantes, assim como o Sun Academic Initiative, contendo treinamentos sem custo e desconto em certificações
- Recursos que ajudam a organizar eventos OSUM

E, assim que uma universidade possuir um forum OSUM estabelecido, você e seus colegas poderão utilizar o patrocínio da Sun para encontros OSUM, incluindo:

- Palestrantes Sun para prover demonstrações técnicas em tecnologias open-source
- Patrocínio da Sun para encontros OSUM, incluindo brindes e ajuda de custo com alimentação
- Acesso à comunidade online Sun OSUM, que fornece uma rede social rica em recursos para OSUMs de desenvolvedore-estudantes

A Sun, uma empresa inovadora, lidera com ações e compartilha tecnologia para direcionar o progresso econômico e social ao redor do mundo, oferece aos estudantes a tecnologia, ferramentas e oportunidade para alcançar o sucesso – na escola, na carreira e na vida. A partir do nosso treinamento e últimos avanços obtidos pelos experts da indústria e a imensa comunidade, a Sun fornece aos estudantes ferramentas com as quais poderão compartilhar e desenvolver idéias e objetivos, mudando seu mundo.

Junte-se a essa rede social global e conecte-se a milhares de estudantes ao redor do mundo. Selecione seu idioma e registre-se.

Registrar-se é fácil – simplesmente visite <http://osum.sun.com> e clique através das poucas perguntas. E você já estará lá!

Se o seu clube de estudantes gostaria de utilizar o patrocínio Sun – registre-se seu clube em: <http://developers.sun.com/students/osum/index.jsp>



Sun Microsystems, Inc. 4150 Network Circle, Santa Clara, CA 95054 USA Phone 1-650-960-1300 or 1-800-555-9SUN Web sun.com

© 2008 Sun Microsystems, Inc. All rights reserved. Sun, Sun Microsystems, the Sun logo, and The Network is the Computer are trademarks, registered trademarks, or service marks of Sun Microsystems, Inc. in the United States and other countries. Other brand and product names are trademarks of their respective companies. Information subject to change without notice.

© Linux New Media do Brasil Editora Ltda.



Coluna do Charly

Conspiração dos mortos-vivos

A utilidade do uptime vai além de competições bobas. Hoje, suas estatísticas ajudam administradores a monitorar tarefas e a encontrar falhas.

Foi-se o tempo em que eu tirava vantagem dos meus colegas da área do Windows mostrando um uptime de 1.000 dias. Se eu for pego com um Matusalém desses hoje em dia, devo estar preparado para perguntas embaraçosas sobre meu suposto medo de atualizações do kernel (a resposta para elas é: sim, tenho medo. Uso controladoras RAID bem exóticas porque atirei no meu pé ao atualizar para o 2.6.27 – ai!).

Aficionados por segurança contam histórias assustadoras sobre os *exploits* que eles acham que funcionariam em sistemas que ninguém se incomodasse de reiniciar ao longo de um ano. Mas o orgulho não deve ser o único motivo para tantos administradores usarem o *Uptime* [1], um *daemon* que registra o uptime do sistema ao longo de um extenso período de tempo. Isso

faz a ferramenta restringir a lista de uptimes salvos a 20 itens legíveis.

```
LOG_MINIMUM_UPTIMED=12h
```

permite informar ao *daemon* para não começar a gravar entradas até que o computador atinja 12 horas de uptime. Isso é bom para suprimir os avisos entre duas reinicializações sucessivas, como seria o caso se precisássemos consertar ou recriar e experimentar um novo módulo de kernel (sim, você adivinhou: minhas controladoras RAID). Também é possível definir pontos específicos no arquivo de configuração para que o software notifique o administrador por email quando o servidor alcançar um deles.

Hora do show

O pacote do *Uptime* inclui o cliente *Upreords*, que exibe os dados obtidos numa lista cuidadosamente formatada no console. Para manter o resultado legível, eu restrinjo a saída de `uprecords -s -m3` às últimas três entradas. Existe um motivo para eu ter escolhido meu gravador de vídeo para isso – ele congela de tempos em tempos, e eu queria que o *Uptime* me ajudasse a descobrir algum método nessas quedas. Infelizmente, não havia nenhum: acho que o hardware está com defeito, exatamente como eu suspeitava. ■

Aficionados por segurança contam histórias assustadoras sobre os exploits que eles acham que funcionariam

faz sentido para dispositivos indisponíveis para monitoramento, por motivos de localização ou segurança – descobre-se exatamente quando faltou energia ou um componente de hardware falhou.

É possível usar o arquivo de configuração `/etc/uptime.conf` para controlar o comportamento do *Uptime*. O trecho:

```
LOG_MAXIMUM_ENTRIES=20
```

Mais informações

[1] *Uptime*: <http://podgorny.cz/moin/Uptime>

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

CAIXA

SOLUÇÕES BASEADAS EM
SOFTWARE LIVRE E PADRÕES ABERTOS.
ESSA É A MANEIRA DA CAIXA
SE CONECTAR AO FUTURO.

referência em inovação, criatividade e eficiência tecnológica no país.

SAC CAIXA 0800.726.0101 (informações, reclamações, sugestões e elogios)
0800.726.2492 (para pessoas com deficiência auditiva)



Coluna do Zack

Crônicas do kernel

Em tempos de bonança, os desenvolvedores se voltam para a manutenção do kernel e para o suporte a hardwares (muito) antigos.

Mensagem alarmista

Matt Mackall ficou um pouco preocupado ao descobrir uma mensagem de erro do kernel que dizia “Traição desmascarada!” (*Treason unclocked!*), informando em seguida que o código TCP detectara um interlocutor problemático. Matt achou a mensagem alarmante e enviou um *patch* para alterá-la. Herbert Xu respondeu lembrando da mensagem “impressora em chamas” (*printer on fire*), presente no kernel e integrante do folclore dos desenvolvedores. Em resposta a Xu, Alan Cox disse que essa mensagem já havia sido alterada há tempos por ser, de fato, confusa.

Porém, Herbert mostrou que Alan estava incorreto, pois encontrou a mensagem nos fontes do kernel, ao que Alan respondeu: “Interessante. Ela tinha sido alterada para ‘lpo relatou status de erro inválido (em chamas?)’ [*lpo reporter invalid error status (on fire, eh?)*]”.

Compatibilidade do Tux3

Daniel Phillips anunciou que seu sistema de arquivos Tux3 abandonou a compatibilidade com kernels mais antigos e somente será compilável em versões posteriores à 2.6.28.

Em seguida, Daniel anunciou que está prestes a embarcar na implementação das operações atômicas (*atomic commits*), deixando o código num período de instabilidade enquanto isso.

No momento, o Tux3 ainda é um projeto em desenvolvimento, e somente deve ser usado por quem realmente gosta de testar sistemas de arquivos.

Mais segurança de rede

Michael Stone propôs implementar um recurso no kernel para permitir que um processo abra mão irrevogavelmente da capacidade de realizar I/O irrestrito de rede, não apenas para si mesmo como para todos seus processos-filhos. Ele disse que isso permitiria que os usuários se protegessem de uma grande quantidade de softwares mal intencionados. Andi Kleen disse que

isso poderia ser feito parcialmente com uso do netfilter, mas Michael não gostou da ideia.

Após discussões entre os dois desenvolvedores sobre como conseguir isso com o netfilter, Alan Cox interveio e afirmou que, qualquer que fossem as restrições, haveria várias formas de um processo passar por cima delas e que, na verdade, o correto é usar soluções de segurança mais granulares como o SELinux.

Suporte a hardware

Adam Osuchowski estava embrenhando-se pelos cantos obscuros do kernel e esbarrou num código em *assembly* que usava a instrução *xadd*. Como o processador 386 não implementa essa instrução, Adam perguntou se o Linux ainda suportava o 386. No final, a instrução *xadd* era apenas um *bug*, mas o incidente disparou uma discussão sobre quais CPUs antigas ainda são suportadas pelo Linux.

Em termos de suporte a SMP (multiprocessamento simétrico), Alan Cox lembrou que o primeiro processador a suportar o padrão Intel MP foi o 486 com APIC externo – que já deve estar ausente da Terra há muito tempo, ele acredita.

Em relação ao 386, Jan-Benedict Glaw disse que tem um 386 velho que “...ainda liga e inicia uma versão secular do Debian. Usando um disco rígido de 20 GB (sim, gigabytes)”. Ele disse que poderia experimentar com kernels mais recentes para testar se funcionam. Vários outros desenvolvedores afirmaram que CPUs 386 ainda são usadas em sistemas embarcados, e Ingo Molnar disse que conhece uma pessoa que ocasionalmente inicia um 386 com kernels atuais. Então, aparentemente o 386 ainda funciona. ■

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.

Os melhores servidores – Os melhores preços

Oferta sedutora!

Por que SERVER4YOU?

- ★ 99% de disponibilidade garantida
- ★ Atendimento ao cliente e suporte 24x7 inclusos
- ★ Mais de 10 anos de experiência
- ★ Garantia de instalação imediata
- ★ Plesk 8 gratuito



Microsoft
GOLD CERTIFIED

Partner

Parallels

Gold Partner

SERVER4YOU

	POWER L	PREMIUM XL
Processador	▶ Intel Pentium IV, 2.8 GHz	▶ AMD Opteron 146
Memória RAM	▶ 512MB DDR2 RAM	▶ 2048 MB DDR2 RAM
Disco rígido	▶ 80GB SATA (7200 RPM)	▶ 2x 120GB SATA (7200 RPM)
Tráfego mensal	▶ 2000GB inclusos no pacote	▶ 4000GB inclusos no pacote
Infra-estrutura de software	▶ Grátis: Fedora 8, CentOS 5, Debian 4, Ubuntu 8 e PLESK 8! Windows 2003 Server Enhanced Edt. – gastos ad. \$12.00/mês	
Recursos adicionais	▶ Grátis: PowerFeatures: PowerReboot, PowerRecovery, PowerRestore etc.	
Suporte	▶ Grátis: 24x7 suporte técnico	
Preço por mês a partir	\$ 49 ⁰⁰	\$ 119 ⁰⁰

\$ 0 INSTALAÇÃO GRÁTIS

\$ 0 INSTALAÇÃO GRÁTIS

Servidores Dedicados Premium

Nossos servidores oferecem elevada qualidade e disponibilidade de serviços, garantindo acesso praticamente ininterrupto aos dados da sua empresa ou página pessoal. Utilizamos máquinas Dell Pentium IV e AMD Opteron, com armazenamento em RAID1, para garantir a integridade dos seus dados. A SERVER4YOU oferece suporte técnico 24x7, conexão de 100 Mbps e hardware de qualidade superior a preços reduzidos. Garantimos instalação imediata.



Preços em dólares.
Impostos incluídos.

WWW.SERVER4YOU.COM



Coluna do Augusto

Open Source é...

Você sabe mesmo o que é Open Source?

Open Source é um conceito definido com bastante detalhamento desde a década passada, mas mesmo assim todos os dias encontramos pessoas cometendo (e repassando – às vezes intencionalmente) erros comuns no seu uso, e em especial um equívoco muito comum: a ideia de que pode-se chamar de Open Source todo software cujo código-fonte esteja disponível para consulta (mesmo que sem possibilidade de livre modificação, ou de livre distribuição de versões modificadas).

Claro que nem sempre o uso equivocado é intencional. Até mesmo pela tradicional dicotomia percebida entre Free Software e Open Source, em que o primeiro coloca mais ênfase do que o segundo em uma série de aspectos relacionados ao livre uso, estudo, alteração e redistribuição, muitos entusiastas são levados a acreditar que o conceito de Open Source dispensa estas mesmas liberdades.

Assim, para surpresa de muitos usuários todos os dias, o conjunto dos softwares que podem ostentar a marca Open Source é praticamente igual ao dos que são considerados Free Software, e a lista de licenças consideradas como sendo Free Software é muito similar à lista de licenças reconhecidas como Open Source.

Assim, pode-se dizer (na ampla maioria dos casos, ao menos) que se um determinado software é livre, ele também é de código aberto, e vice-versa. Quando alguma entidade ou empresa afirma com propriedade que lançou um software sob licença Open Source, isso significa que seus usuários poderão usar, modificar e redistribuir livremente o produto.

A diferença essencial entre a Free Software Foundation e a Open Source Initiative, entidades proponentes de cada um dos dois conceitos, está nos objetivos, na filosofia e no modo de agir, e não nos softwares ou licenças. Ou, como diz o site da Free Software Foundation, “Nós discordamos nos princípios básicos, mas concordamos mais ou menos nas recomendações práticas. Assim nós podemos e de fato trabalhamos juntos em vários projetos específicos. Nós não pensamos no movimento Open Source como o inimigo”.

Exemplificando: softwares notáveis como o Linux, o ambiente gráfico KDE, o compilador GCC, o servidor web Apache, o OpenOffice.org e o navegador web Firefox, entre muitos outros, se qualificam simultaneamente como Free Software e como Open Source, ao mesmo tempo em que produtos disponibilizados juntamente com seu código-fonte mas sem permissão para livre alteração e redistribuição não se classificam em nenhum dos conceitos.

E da próxima vez que você encontrar alguém empregando mal os termos, está convidado a tentar esclarecer o equívoco! ■

Para um software ser considerado Open Source, sua licença tem que satisfazer dez condições.

Mas a definição de Open Source (usualmente traduzido para nosso idioma como Código Aberto) também exige estas liberdades. Para ser preciso, ela determina que, para um software ser considerado Open Source, sua licença tem que satisfazer dez condições, incluindo Livre Redistribuição, Acesso aos Fontes, Permissão de Trabalhos Derivados, Não Discriminação, Distribuição da Licença, e vários outros.

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.

COM O UOL HOST VOCÊ NUNCA ESTÁ SOZINHO.

NOVIDADE

PLANOS DE
HOSPEDAGEM
DE SITES

info
MELHOR RELAÇÃO
CUSTO/BENEFÍCIO

COM 10X MAIS ESPAÇO!

- ✓ Construtor de Sites
- ✓ Domínio Grátis!*
- ✓ E-mail Profissional
- ✓ Base de Dados MySQL Ilimitados

Plano Econômico

100GB transferência
5GB espaço • 25 E-mails **R\$14,90**
/mês

Conheça nossos planos:



PROGRAMA DE PARCERIAS UOL HOST

Entre em contato e saiba as vantagens.

REGISTRO DE
DOMÍNIOS

Domínio (.br)

R\$27,00
por ano

Domínio
(.com ou .net)

R\$9,00
por ano

- DELL R200 - Dual Core 2.0 GHz
- 1 GB de Memória RAM
- 2x250 GB (Serial Ata2) de Disco
- 2 Mbps de Banda

R\$490,00
por mês

SERVIDORES
DEDICADOS

0800 723 6000

PAINEL DE CONTROLE UOL HOST

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



UOL HOST

QUALIDADE EM SERVIÇOS WEB

www.uol.com.br/host



Coluna do Kurt

Segurança no navegador

Por mais feio e difícil de tornar seguro que seja o JavaScript, a situação poderia ser pior – poderíamos estar usando ActiveX.

O problema do JavaScript – impossível viver com ele, impossível viver sem ele. A Web moderna é incrível; consigo pagar minhas contas, comprar um laptop e pedir pizza a partir do meu navegador. Pra todas essas atividades, preciso de um navegador web com JavaScript ativado. Sem ele, não consigo ler meus emails, pagar minhas contas, comprar nada ou visualizar mais ou menos metade dos sites do planeta. Mas com ele ativado, os bandidos conseguem:

- ▶ descobrir quem eu sou por meio de códigos como o do Google Analytics;
- ▶ explorar vulnerabilidades de segurança do Firefox (mais de 120, e crescendo);
- ▶ redirecionar-me para sites hostis; e
- ▶ sequestrar ações, como teclas do teclado e cliques do mouse.

Eu acabei de dizer que o Firefox tem mais de 120 vulnerabilidades de segurança exploráveis com JavaScript? Sim. E esse número não conta aquelas que ainda não foram oficialmente categorizadas ou solucionadas. Um exemplo perfeito de uma delas é o CVE-2009-0253; usando a ação `onmouseover` para colocar uma caixa de 2x2 pixels sobre um link clicável, um agressor consegue redirecionar o visitante para um site arbitrário. Qualquer evento de clique do mouse (ou seja, clicar no que parece um link ou imagem legítimos) num link resulta num evento `onmouseover` que redireciona o visitante para, bem, onde quer que o agressor deseje:

```
<div id="mydiv"
onmouseover="document.location='http://www.milw0rm.
com';"
style="position:absolute;width:2px;height:2px;
background:#FFFFFF;border:0px"></div>
<script>
function updatebox(evt) {
```

```
mouseX=evt.pageX?evt.pageX:evt.clientX;
mouseY=evt.pageY?evt.pageY:evt.clientY;
document.getElementById('mydiv').style.
left=mouseX-1;
document.getElementById('mydiv').style.top=mouseY-1;
}
</script>
```

Com esse código de exploit (e o Firefox 3.0.5), ao passar o mouse sobre o link, a barra de status mostrará o link da página web (porque o link em si não foi modificado de forma alguma), mas esse não é o que será levado em consideração quando você clicar nele.

Segurança difícil

Em resumo, JavaScript é uma linguagem Turing-completa, o que significa que ela pode realizar qualquer cálculo imaginável. Acrescente a isso uma gigantesca biblioteca padrão de métodos que podem interagir com o navegador web (como `onmouseover`, por exemplo) de formas potencialmente inesperadas e temos uma receita para o desastre. Os agressores também podem usar truques, como colocar o código JavaScript num arquivo em outro servidor e então chamá-lo com o método `document.write` para carregar o arquivo remotamente. Novamente, esse é um recurso legítimo que pode ser fortemente abusado por agressores.

Pelo lado bom, temos sites como o Google. Se você quiser usar seu serviço Analytics ou de anúncios, basta inserir um pequeno trecho de código JavaScript nas suas páginas, que por sua vez chamam programas JavaScript bem maiores dos sites do Google. As vantagens incluem: a possibilidade de clientes fazerem cache do JavaScript por vir da mesma URL (o que significa que as páginas serão carregadas mais rapidamente), o Google poder atualizar seus programas JavaScript de forma centralizada, as pessoas que o utilizam não precisarem atualizar suas páginas e as-

sim por diante. A desvantagem é que os agressores podem incluir JavaScript em páginas web e servi-las a partir de locais remotos. Dependendo das variáveis `document.referer`, `document.location` e `location.href`, elas podem servir código personalizado para cada site ou nenhum código. Portanto, se você tentar copiar e examinar a página web hostil numa *sandbox*, o código hostil não será carregado, ou uma versão inofensiva será enviada.

Desligar

Espero que você não goste de banco online, compras ou qualquer outro site “Web 2.0”, incluindo Gmail, Facebook e StackOverflow.

Ligar seletivamente

Não é uma má ideia. As extensões do Firefox como *NoScript* tornam essa experiência relativamente indolor (pelo menos depois que você permitir o JavaScript de todos os sites que costuma visitar e nos quais confia). Após instalar o *NoScript*, ao visitar uma página que tente carregar JavaScript (seja de seu próprio servidor ou de outro), você receberá um alerta no canto inferior direito do seu navegador. Quando isso acontecer, clique no botão *Opções* e permita que o site carregue scripts temporariamente (até o Firefox ser reiniciado) ou para sempre, ou bloqueie-os inteiramente.

Entretanto, não é possível permitir seletivamente certos scripts dentro de um domínio e bloquear outros com facilidade. Se um agressor conseguir realizar um ataque de *cross-site scripting* contra um site em que você confia, como seu banco, ele será capaz de executar seu JavaScript hostil na máquina do visitante sem qualquer alerta.

Política de segurança de conteúdo

Por que não permitir que os domínios especifiquem o que deve ser carregado a partir de seus sites? Essa ideia foi proposta como uma “Política de Segurança de Conteúdo” (*Content Security Policy*, [1]). Infelizmente, o projeto ainda é novo e não ganhou muita atenção (no lado positivo, existe uma especificação em funcionamento e uma extensão de exemplo para o Firefox implementar). No futuro, espera-se que esse projeto ganhe mais momento.

Aí vem o Linux

Se não for possível desativar JavaScript globalmente e se controlá-lo individualmente por domínio for impraticável, como se espera que você navegue na Web com segurança e tenha acesso a sites baseados em JavaScript? Usando o poder do Linux, é claro!

Se você está lendo esta revista, imagino que seja grande a probabilidade de você estar usando Linux (se não, impressione-se com a simplicidade para se resolver um problema).

SO multiusuário (Linux) + xhost

Se você usa o *X Window System*, seu desktop foi projetado para, entre outras coisas, permitir que diferentes usuários e até sistemas usem e exibam programas no desktop. O servidor X renderiza e exibe as informações no desktop. O cliente X executa o programa e envia os dados para exibição pelo servidor X. Para permitir que usuários locais e sistemas remotos interajam com o servidor X de forma segura numa dada máquina, são usados controles de acesso. Com o programa *xhost* é possível manipular esses controles de acesso. Se você quiser navegar na Web sem se preocupar se um site remoto executar código hostil e apoderar-se da sua máquina, simplesmente crie um novo usuário com o único propósito de executar o Firefox. O novo usuário terá permissão de executar e exibir programas no seu desktop:

```
(Como root, digite)
# adduser webuser
# passwd webuser
(E com seu próprio usuário)
$ xhost +SI:usuárioLocal:webuser
```

Esse código cria e define uma senha para o usuário *webuser* e, em seguida, emprega o *xhost* para permitir que essa nova conta use o seu monitor.

Então, faça login com o usuário *webuser* e execute o Firefox.

Para navegar na Web, você pode abrir um terminal, usar o comando *su* para adotar o usuário *webuser* e só então executar o Firefox, que usará o seu monitor.

Conclusão

Às vezes é mais fácil evitar problemas do que tentar solucioná-los de forma elegante. O Linux oferece muita flexibilidade; por exemplo, múltiplos usuários podem usar o mesmo sistema – na verdade, até a mesma tela, teclado e mouse. A longo prazo, definir contêineres para os aplicativos individuais serem facilmente restaurados é o melhor caminho. Certamente não podemos esperar que os softwares eliminem toda e qualquer falha. ■

Mais informações

[1] Política de Segurança de Conteúdo:
<http://people.mozilla.org/~bsterne/content-security-policy/>

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



Novidades do kernel 2.6.29

Linux 2.6.29

Novo kernel, novo recorde. Com mais de 1 milhão de novos trechos de código, o Linux 2.6.29 chega repleto de novidades para todos os usuários.

Treze semanas. Foi esse o tempo necessário para a equipe de desenvolvimento do kernel Linux partir da versão 2.6.28 e chegar à 2.6.29. Em 89 dias (quase 13 semanas), o “Erotic Pickled Herring” deu lugar ao “Temporary Tasmanian Devil” (você sabia que as versões do kernel têm apelidos como esses?).

Embora os 10.933 arquivos alterados desde 24 de dezembro último não sejam exatamente um recorde (as duas versões anteriores tiveram mais que isso), a verdadeira surpresa está nas mais de 1,3 milhões de inserções de código – essas sim constituem um novo recorde.

Tuz, novo mascote do Linux que substitui temporariamente o adorável pinguim Tux.

As novidades, como se pode imaginar, não são poucas: dois novos sistemas de arquivos (e avanços no ainda recente *Ext4*), o progresso do *mode-setting* de vídeo baseado no kernel (KMS, para os íntimos), o suporte a redes WiMAX e uma série de alterações que já começaram a reduzir significativamente o tempo de inicialização do kernel – essas são apenas as mais chamativas, mas há muitas outras, como o Tuz, novo mascote do Linux que substitui temporariamente o adorável pinguim Tux durante a inicialização do sistema.

Sistemas de arquivos

O acesso a disco ainda é um dos principais gargalos do desempenho na maioria dos sistemas, tanto desktops quanto servidores – e até em alguns sistemas embarcados. Com tempos de acesso bem maiores que o restante do sistema, o armazenamento em disco continuará atrasando a computação como um todo até encontrarmos uma forma barata para guardar nossos incalculáveis volumes de dados.

É por isso que, além dos avanços nas tecnologias de armazenamento, como discos *Flash* e discos rígidos giratórios mais velozes e confiáveis, os sistemas de arquivos têm uma importância tão fundamental.

O kernel 2.6.29 finalmente trouxe o suporte ao sistema de arquivos de próxima geração *Btrfs* (pronuncia-se “better FS” ou “butter FS”, à sua escolha). Seus recursos são baseados no poderoso ZFS da Sun e ele está sendo desenvolvido por uma grande equipe de programadores muito capazes. Porém, a má notícia é que ele ainda está em desenvolvimento, e sua inclusão na árvore principal do kernel servirá justamente para acelerar a estabilização do código para que o *Btrfs* amadureça o mais rápido possível. Por enquanto, ainda não é possível confiar nele para conservar seus dados.

O *SquashFS*, no entanto, já é conhecido por usuários de *Live CDs* há tempos, mas somente agora passa a integrar a árvore principal do kernel. Seu “concorrente” *CramFS*, outro sistema compactado e somente-leitura que já residia no kernel há algum tempo, não parece estar muito vivo, e o *SquashFS* é perfeitamente competente.

O recente *Ext4*, introduzido como sistema de arquivos estável na última versão do kernel, recebeu melhorias e correções que o tornam mais adequado para uso em discos *Flash*. Uma das mais interessantes

é a possibilidade de não utilizar o *journal*, introduzida por Ted Ts'o após o desenvolvedor descobrir que muitas pessoas utilizavam o venerável *Ext2* – com todas as suas importantes limitações – nessas mídias apenas por não quererem sobrecarregar seus discos Flash com as constantes atualizações do *journal*.

Além disso, o sistema de arquivos distribuído OCFS2 finalmente passa a contar com suporte a ACLs, atributos de segurança, cotas e verificação (*checksum*) de metadados.

Vídeo

Os trabalhos da transferência do mode-setting de vídeo para dentro do kernel (e para fora do driver do X.org) começaram há 21 meses, acompanhados pelo desenvolvimento da infraestrutura de gerenciamento de memória gráfica GEM, e agora esse recurso já pode ser usado com chips gráficos Intel. O KMS (*kernel-based mode setting*), além de trazer melhor desempenho e simplificar o uso de chips gráficos, também resolve vários problemas da suspensão do sistema para a memória.

Rede

As redes sem fio jamais serão as mesmas quando o WiMAX começar a ser comercializado. Com até 75 Mbps e alcance medido em quilômetros, o padrão encabeçado pela Intel e baseado no IEEE 802.16 finalmente chegou ao Linux, primeiramente apenas com drivers para os dispositivos Intel Link 5x50, que funcionam por meio dos barramentos SDIO ou USB.

Nas redes sem fio tradicionais (IEEE 802.11), o sistema do demônio da Tasmânia disfarçado de pinguim (temporariamente, lembre-se) agora ganha também a capacidade de trabalhar como ponto de acesso mediante a instalação do *hostapd*.

Inicialização rápida

Arjan van de Ven continua dedicado a acelerar o processo de inicialização do kernel. Após os avanços perceptíveis implementados na versão 2.6.28, a 2.6.29 torna o cenário ainda melhor, pois começa a paralelizar a inicialização de subsistemas que não sejam interdependentes.

Infelizmente, alguns problemas desse paralelismo adiaram sua estreia para a versão 2.6.30, embora toda a infraestrutura já esteja presente e possa ser ativada na configuração e em tempo de inicialização.

CPUs aos milhares

Se você estava feliz com seu computador de 4, 8 ou 16 núcleos – ou talvez 128, se você for uma pessoa influente –, saiba que o Linux agora suporta até 4.096

processadores. Para lidar com tantos processadores, são necessárias algumas alterações à forma como o sistema se refere a cada um deles, assim como o meio para se comunicar com eles. Então, junto com o novo limite superior, o kernel 2.6.29 traz o *Tree RCU*, um mecanismo hierárquico para acesso aos processadores que elimina graves problemas de desempenho enfrentados por sistemas com centenas de CPUs.

Demais

Outras novidades trazidas pelo Linux 2.6.29 incluem a criptografia de nomes de arquivos sob o *eCryptfs*, a capacidade de paralisar a atividade de determinados sistemas de arquivos para fins de backup ou *snapshots*, alterações na forma como o kernel lida com credenciais (usuário, grupo etc.) de processos e implementação do *Xenfs* para permitir a interação do Xen com o restante do sistema.

Adeus, velharia

Uma decisão particularmente polêmica dos desenvolvedores do kernel deu cabo da compatibilidade do Linux 2.6.29 com as versões 3.0, 3.1, 4.1.0 e 4.1.1 do compilador GCC – o único capaz de compilar o kernel na atualidade.

Futuro

Para a versão 2.6.30, já podemos esperar algumas novidades. O sistema de arquivos Ext4 certamente contará com alguns *patches* para resolver um problema de perda acidental de dados após quedas do sistema, em decorrência do recurso de adiamento da alocação de blocos. Outra novidade deve vir do novo (sim, mais um) alocador de páginas de memória, o SLQB, para substituir o antigo SLAB e o mais recente SLUB.

Na área da segurança, os desenvolvedores têm falado bastante na plataforma Tomoyo, que deve ser integrada ao kernel no futuro, embora dificilmente a tempo para o 2.6.30. ■

Mais informações

[1] Linux 2.6.29 no Kernel Newbies: http://kernelnewbies.org/Linux_2_6_29

Pablo Nehab Hess é editor da Linux Magazine, tem mestrado em genética e especialização em bioinformática. É autor de softwares de código aberto para computação científica e tem experiência em administração de sistemas.

▶ O silverlight de código aberto

A Novell anunciou o lançamento da versão 1.0 do Moonlight, implementação em código aberto da tecnologia Microsoft Silverlight. O Silverlight foi criado pela Microsoft com o objetivo de fornecer uma solução completa e robusta para criação e entrega de aplicações ricas para Internet (RIA, Rich Internet Applications) e experiências em mídia.

Assim como o Silverlight se baseia na plataforma .NET, também criada e desenvolvida pela Microsoft, o Moonlight tem como base o Mono, implementação em código aberto dessa plataforma.

O desenvolvimento do Moonlight é, em parte, resultado da atual colaboração técnica entre a Microsoft e a Novell com o objetivo de promover a interoperabilidade entre Linux e Windows.

“O Moonlight traz os benefícios do conteúdo multimídia do Silverlight para os espectadores que usam Linux”, afirmou Miguel de Icaza, fundador do projeto Mono (além de outros softwares célebres de código aberto, como Gnome e Midnight Commander) e vice-presidente de desenvolvimento de plataforma da Novell. “Esse primeiro lançamento tem como objetivo eliminar os obstáculos do conteúdo multimídia e criar igualdade na experiência de visualização do usuário, independentemente de ele usar Windows ou Linux”. □

▶ Linux New Media aplica provas LPI

Trazendo para o Brasil sua parceria mundial de longa data com o LPI (Linux Professional Institute), a Linux New Media passa agora a realizar provas de certificação LPI no país. Os leitores da Linux Magazine ganham descontos especiais de até 20%, bastando, para isso, acessar www.linuxnewmedia.com.br/cert.

Além disso, na aquisição de uma prova, o leitor será presenteado com uma assinatura digital de seis meses da Linux Magazine e os livros *Shell Script I* e *Shell Script II*, de Julio Neves, da série Linux Pocket Pro.

A aquisição de duas provas dá ainda mais presentes: um ano de assinatura digital da Linux Magazine e quatro livros da série Linux Pocket Pro, incluindo os dois títulos de Shell Script. ■

▶ Lançado o SUSE Linux Enterprise 11

A Novell anunciou hoje o lançamento de sua distribuição Linux corporativa SUSE® Linux Enterprise 11, descrito pela empresa como “o sistema operacional desenvolvido para os data centers de próxima geração”. O anúncio de lançamento informa que o sistema está pronto para todas as mais recentes tecnologias, como computação em nuvem e virtualização com hypervisors, assim como para redes heterogêneas e aplicações de missão crítica.

Uma novidade na oferta da Novell, com relação às versões anteriores do SUSE Linux Enterprise Server (SLES) e do SUSE Linux Enterprise Desktop (SLED) é a SUSE Linux Enterprise Mono® Extension, que oferece suporte comercial a aplicativos baseados na plataforma .NET da Microsoft. A segunda novidade nesse campo é a SUSE Linux Enterprise High Availability Extension, um produto para criação e administração de clusters de alta disponibilidade.

Os três objetivos principais do SUSE Linux Enterprise 11 são, de acordo com o anúncio de lançamento, disponibilidade, interoperabilidade e computação de missão crítica.

“À medida que a virtualização atinja a plenitude de seu potencial e a computação em nuvem comece a transformar os data centers, os sistemas operacionais precisam ser projetados para permitir essas novas soluções,” afirmou Matt Eastwood, vice-presidente de grupo no IDC, durante o lançamento. “A Novell, ao oferecer suporte completo para modelos físicos, virtuais, de dispositivos e computação em nuvem com o SUSE Linux Enterprise, pode auxiliar clientes em cada etapa da evolução dos data centers. Para os clientes que procuram um sistema operacional que trabalhe com sua infraestrutura de TI atual e ao mesmo tempo reduza o custo da computação corporativa, a Novell lançou o SUSE Linux Enterprise 11 e um conjunto completo de soluções para identidade, segurança e gerenciamento de sistemas”. ■

▶ Código aberto para automóveis

Em seu keynote no fórum de Código Aberto da CeBIT, Graham Smethurst, gerente geral de *infotainment* e sistemas de comunicação da BMW, apresentou uma nova plataforma de desenvolvimento de código aberto para a indústria automobilística. Sob o nome de GENIVI, os integrantes BMW, Delphi, General Motors Corp., Intel, Magnetti Marelli, PSA Peugeot Citroën, Visteon Corp. e Wind River vão desenvolver em conjunto softwares para infotainment com base no Linux.

O termo “IVI”, que faz parte do nome da iniciativa, GENIVI, significa “In-Vehicle Infotainment” (infotainment dentro do veículo) e descreve o objetivo conjunto dos parceiros, que fazem parte dos segmentos de fabricação de automóveis, TI e produtos eletrônicos. A força motriz da aliança cabe aos desenvolvedores de software da alemã BMW, que já trabalham há alguns meses com a fornecedora de Linux embarcado Wind River em softwares para produtos de consumo para automóveis, com base em Software Livre.

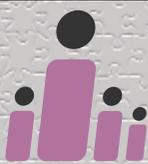
Sob o nome do GENIVI, a aliança da indústria desenvolverá uma arquitetura comum de hardware e software que deve favorecer OEMs, grandes fornecedores e outros. Os componentes da plataforma GENIVI incluirão serviços baseados em Linux, além de interfaces nas camadas de middleware e aplicações abertas. Com base na visão dos membros da aliança, a plataforma aberta deve ser o primeiro ponto de contato e base para todos os fabricantes de automóveis e seus fornecedores, que devem contribuir para o GENIVI a fim de

desenvolvê-lo e expandi-lo ainda mais com seus próprios produtos e serviços.

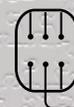
Smethurst promete a primeira versão da plataforma GENIVI já para o inverno de 2009 (verão no hemisfério norte). Ela deve ser baseada num protótipo automotivo que por sua vez se baseia no Wind River Linux e no processador Intel Atom que está em desenvolvimento há 18 meses. A implementação de referência será disponibilizada como código aberto “para incentivar a inovação entre os desenvolvedores”. ■



Congresso de



Governança de TI e ERM



12 e 13 de maio de 2009 - São Paulo

6ª Edição do Congresso de Governança de TI & ERM, aborda temas atuais e necessários para manter você a frente e conservar sua posição no mercado profissional!

CURSOS

Destacamos aqui alguns cursos que acontecem no período da manhã, para que você absorva totalmente o conteúdo e tenha subsídios para acompanhar as demais atividades do congresso.

Unindo CobIT e ITIL para avaliar como processos de TIC contribuem com o negócio

Ana Carolina Riekstin e Carlos Rodrigo Cordeiro Alves - PromonLogicalis

Análise e avaliação do risco a fraudes ocupacionais e computacionais

Mário Sérgio Ribeiro - Enigma Security

Outsourcing de TI em Tempos de Crise

Walter Ferrari Veras - Agnus Consulting

Sistemas de Mensageria Eletrônica: proteção, Controle e Registro de Uso

Duval A. Costa - Ideti Treinamento



Organização e Realização



Faça agora a sua inscrição:

www.governancati.com.br/sp/inscricao

Aguardamos pelo seu contato 11 5531-3899 ramal 213

ou pelo e-mail glucia@ideti.com.br

www.governancati.com.br/sp

© Linux New Media do Brasil Editora Ltda.

Crise favorece o Linux

A Novell anunciou os resultados de uma recente pesquisa de mercado patrocinada por ela e conduzida pelo IDC com mais de 300 executivos seniores de TI de setores como manufatura, serviços financeiros, varejo e agências governamentais de todo o mundo. O estudo revelou um aumento expressivo nas aquisições de Linux ocorridas em virtude da recessão econômica global. Quanto mais as empresas procuram cortar custos e agregar valor, mais são atraídas pela enorme economia que o Linux oferece. Mais da metade dos executivos de TI pesquisados planejam acelerar a adoção do Linux em 2009. Além disso, mais de 72% dos entrevistados disseram que estão avaliando seriamente ou já decidiram aumentar a adoção do Linux no servidor em 2009, com mais de 68% reivindicando o mesmo para o desktop.

Resultados

A principal razão que motivou os executivos a migrarem para Linux foi econômica e relacionada à redução contínua de custos de suporte. Como resultado, mais de 40% dos participantes da pesquisa disseram que planejam implantar novos fluxos de trabalho em Linux nos próximos 12 a 24 meses, e 49% indicaram que o Linux será sua principal plataforma nos próximos cinco anos. Notavelmente, entretanto, aqueles que continuam hesitantes em adotar Linux citaram falta de suporte por parte de aplicações e fraca interoperabilidade com Windows e outros ambientes como sua principal preocupação.

Além disso, 67% dos pesquisados afirmaram que interoperabilidade e gerenciamento entre Linux e Windows são dois dos fatores mais importantes na escolha do sistema operacional. O setor de varejo mostrou o maior potencial de aceleração na adoção de Linux, já que 63% dos pesquisados planejam aumentar seus desktops e 69% consideram o mesmo nos servidores. A área governamental ficou atrás.

Quase 50% dos pesquisados planejam acelerar a adoção de Linux no desktop, especialmente para funções de escritório básicas, usuários técnicos de estações de trabalho e educação superior. Aproximadamente metade dos entrevistados afirmou que sua migração para a virtualização está acelerando suas adoções de Linux. Destes, 88% planejam avaliar, implantar ou aumentar a utilização do uso de software de virtualização no sistema operacional Linux nos próximos 12 a 24 meses.

Do ponto de vista regional, o leste da Ásia é a região que mais adota Linux, onde 73% dos entrevistados disseram que gostariam de aumentar a implantação de Linux no servidor e 70% nos desktops. Nas Américas, 66% dos entrevistados afirmaram que estão avaliando ou já decidiram ampliar a adoção de Linux no desktop, e 67% no servidor.

Maior impacto

A crise econômica teve seu maior impacto nas Américas, nos serviços financeiros e governo. Mais de 62% dos entrevistados disseram que seus orçamentos sofreram cortes ou que estão apenas investindo no que é necessário.

“As recessões econômicas tendem a acelerar o uso de tecnologias emergentes, aumentar a adoção de soluções eficientes e punir soluções que não apresentam custo competitivo”, afirmou Al Gillen, vice-presidente de software e sistema do IDC. “Esta pesquisa confirma que usuários de Linux o enxergam favoravelmente, e essa percepção coloca o Linux em uma posição competitiva para emergir dessa recessão como uma solução mais fortalecida”.

Impacto da pesquisa

“As informações extraídas dessa pesquisa de mercado confirmam nossa crença de que, à medida que as empresas se esforçam para cortar custos e agregar valor nesse cenário econômico difícil, a adoção de Linux irá se acelerar”, afirmou Markus Rex, gerente geral e vice-presidente sênior para Soluções de Plataforma Aberta da Novell. “As empresas também afirmaram que a adoção do Linux será ainda maior com o fortalecimento do suporte a aplicações Linux, interoperabilidade, capacidades de virtualização e suporte técnico”.

A pesquisa foi realizada em fevereiro de 2009. Foram entrevistados mais de 300 profissionais de TI que supervisionam as compras de Linux e outros sistemas operacionais para saber suas opiniões. Para participar, as organizações deveriam ter mais de 100 funcionários; a pesquisa procurou principalmente tomadores de decisão familiarizados com a utilização e planos de adoção de Linux. Dentre os participantes, 55% tinham Linux como sistema de servidor em uso, 39% Unix e 97% Windows. Os pesquisados tinham os cargos de CIOs, vice-presidentes, diretores, gerentes, funcionários e consultores de TI. Os entrevistados foram pré-avaliados por analistas locais e responderam a pesquisa pela Internet. A Novell não se envolveu no recrutamento, e os entrevistados não precisavam ser clientes da empresa.

Um white paper do IDC com o resumo dos resultados da pesquisa pode ser acessado em www.novell.com/id. □

► IBM vai adquirir a Sun?

Segundo artigo publicado no Wall Street Journal, a IBM estaria negociando a aquisição da rival Sun Microsystems. O jornal citou como fonte da notícia pessoas diretamente envolvidas na negociação. Apesar de a IBM ter manifestado interesse na aquisição, o estágio atual das negociações ainda é inicial, de modo que o negócio pode ser interrompido ou mesmo fracassar sem maiores consequências.

A motivação da *big blue* para a aquisição é o fortalecimento da sua posição em especial no mercado de infraestrutura de Internet e de soluções para o mercado financeiro e de telecomunicações. O valor do negócio seria de no mínimo 6,5 bilhões de dólares, o que representa o dobro do valor corrente da Sun Microsystems – que faturou 13,8 bilhões de dólares em 2008.

Estrategicamente, ambas as empresas têm como alvo companhias cujas estruturas de TI não são baseadas em tecnologia Microsoft, além de oferecerem hardware cujos processadores não são baseados em arquitetura x86. Essa independência do binômio “Wintel” seria in-

tenfificada por meio de uma fusão, o que poderia polarizar o mercado de hardware, colocando o Linux em uma posição privilegiada, como única plataforma operacional disponível para as duas arquiteturas.

Por outro lado, há sobreposição em diversos segmentos nas ofertas e tecnologias de hardware e software das duas empresas. Ademais, tanto a IBM quanto a Sun têm em seu portfólio de servidores máquinas equipadas com processadores de arquitetura x86 – predominantemente Intel, no caso da IBM, e AMD, no caso da Sun. No segmento de bancos de dados, a IBM dispõe de um rico leque de opções, como o Informix e o DB2, além de soluções específicas como o Red Brick Warehouse, UniData, UniVerse, além de ter aberto em 2007 o código do Cloudscape, tendo entregue o projeto nas mãos da Fundação Apache, que iniciou com ele o Apache Derby.

A Sun, por sua vez, adquiriu por 1 bilhão de dólares, há pouco mais de um ano, o MySQL, e ainda não conseguiu um retorno desse investimento. As duas empresas também oferecem tanto o Linux quanto suas próprias implementações de UNIX como sistemas operacionais para os seus servidores – lembrando que a Sun já abriu o código do OpenSolaris, base tecnológica para o Solaris, enquanto o AIX, da IBM, permanece proprietário e fechado. Um outro ponto importante é que a Sun é proprietária da tecnologia Java, muito utilizada pela IBM, e hoje uma das peças-chave para a infraestrutura de software de aplicações para a Internet. ■

Complete a sua coleção

O objetivo da coleção é trazer **conhecimento confiável** e de alto nível sempre com **ênfase prático** e voltado para a utilização do sistema **Linux** e de outras tecnologias livres.

Mais
informações

Site:

www.linuxmagazine.com.br

Tel: 11 4082-1300



Entrevista com Gabriele Ruffatti, diretor de arquiteturas e consultoria do Engineering Group

Modelo de negócio inteligente

O SpagoBI é um bom caso de estudo de uma grande empresa que abriu parte de seu código estratégico e vem tendo bons resultados com isso.

por Pablo Hess

O italiano Engineering Group é líder do mercado de serviços de TI na Itália. Há alguns anos a empresa abriu o código-fonte de uma parte estratégica de sua plataforma de desenvolvimento e lançou o software de *Business Intelligence* SpagoBI, proporcionando um interessante caso de estudo dessa tendência agora bem mais comum no mercado de TI.

Em visita ao Brasil, Gabriele Ruffatti, diretor de arquiteturas e consultoria do Engineering Group, contou à **Linux Magazine** mais detalhes da história da empresa, seu envolvimento com o Software Livre e de Código Aberto (SL/CA) e por que o modelo de negócios do SpagoBI tem dado tão certo.

Linux Magazine O que diferencia o modelo de negócios do SpagoBI daqueles usados por outros projetos abertos?

Gabriele Ruffatti O que diferencia nosso modelo de negócios é que produzimos Software Livre de qualidade corporativa. Esse é o melhor aspecto do Código Aberto. Muitas empresas produzem duas versões de seus softwares, com a versão aberta tendo menos recursos que a proprietária, e diversas empresas europeias estão empregando licenças específicas para forçar a contribuição.

Nossa escolha é diferente. Começamos com Software Livre porque já

tínhamos vínculos com a Free Software Foundation Europa. Porém, nós tínhamos algumas dúvidas sobre as licenças comerciais. Nossa escolha é oferecer o software de forma 100% livre sob a LGPL, para ser usada conforme a escolha do cliente (e inclusive linkada em outros softwares), e com qualidade corporativa. Não queremos produzir várias versões do mesmo software, principalmente porque somos uma empresa de integração de sistemas — múltiplas versões só iriam dificultar nosso trabalho.

Nosso maior mercado é na Itália. Temos mais de 6 mil pessoas lá trabalhando com a integração do nosso software e também com soluções proprietárias, mas nosso maior foco é atender às necessidades de nossos usuários, não decidir o que eles precisam.

Obviamente temos um planejamento, um *roadmap*, com propostas de novos recursos, mas basicamente nós coletamos as opiniões e demandas dos nossos usuários. E vendemos somente serviços: treinamentos, subscrições, integração.

As pessoas creem (de forma equivocada) que, com esse modelo, nosso retorno financeiro é menor. Nós podemos agir dessa forma porque somos uma grande empresa integradora, então temos os maiores projetos, nos quais usamos nossas soluções de forma a sustentar um modelo aberto.

LM Que parcela da receita da Engineering vem da integração de sistemas?

GR É muito difícil responder, porque nossos principais produtos são do ecossistema da própria Engineering. A empresa é subdividida em divisões de mercado, dedicadas a governo, finanças, indústria, telecomunicações... Nós somos uma divisão técnica que presta suporte para essas outras na entrega dos produtos.

Essa pergunta é difícil porque às vezes temos projetos totalmente baseados em nossas soluções, enquanto outras vezes são usadas soluções externas, mas que também se integram às nossas.

LM Quais são os principais concorrentes do SpagoBI no mercado de BI de código aberto?

GR Em resumo, nós começamos com a plataforma *Spago*, que é uma plataforma Java Enterprise que construímos em 2000 para um importante projeto interno da empresa. Em 2004, decidimos consolidar a plataforma e abrir seu código para aprender o que é o Código Aberto. Nós vendemos conhecimento e experiência, não folhetos.

Depois disso, decidimos começar outros projetos como código aberto. Em 2004, não existia nenhuma plataforma aberta para BI. Assim que lançamos o software, surgiu o Pen-

taho, nosso primeiro concorrente de código aberto.

Em BI de Código Aberto há três plataformas: SpagoBI, Pentaho e Jasper Reports.

LM *Qual a importância, nesse mercado, de ter parcerias com distribuidores de Software Livre, como a Engineering possui com a Red Hat?*

GR É importante para garantir que não apenas a plataforma Spago funcione para os clientes, mas também para mostrar que oferecemos suporte. Portanto, é para completar nossa oferta de código aberto. No Código Aberto, precisamos trabalhar em redes.

O distribuidor age como único ponto de contato entre toda a pilha de software de código aberto e o cliente. Então, nós somos o ponto de contato da Red Hat com nossos clientes e prestamos suporte de primeiro nível, enquanto temos um acordo para suporte a partir do segundo nível com todos os clientes da Red Hat.

LM *Nesse aspecto, qual a importância de integrar o consórcio OW2?*

GR O OW2 é um ótimo consórcio, mas eu gostaria de propor algumas mudanças. O princípio do consórcio é proporcionar um middleware – no sentido amplo – feito pela comunidade de empresas. O sentido de middleware realmente precisa ser esclarecido: o próprio SpagoBI pode ser considerado tanto como um produto quanto como parte do middleware. O que eu gostaria de mudar no OW2 é que deixássemos de depender tão fortemente da base de código do próprio consórcio. Nem sempre podemos afirmar que o código do OW2 é a melhor escolha. É o mercado que sabe qual é a melhor escolha.

O importante, então, é abrimos mais conexões, como estamos fazendo

neste momento com o Eclipse, por exemplo. Com base nessas conexões, queremos desenvolver o SpagoBI 3.0, com o objetivo de atender demandas reais de todo o mercado.

GR Nós tentamos atrair a comunidade para nosso projeto. É impossível. Muito poucos contribuíram algum código. O ramo de Business Intelligence pertence às empresas.



Graças ao Código Aberto, estamos inserindo BI em projetos que não o utilizariam de outra forma.

LM *Que parcela do mercado o SpagoBI detém na Europa?*

GR No mercado geral de BI, nossa participação é bem pequena, porque ainda estamos lidando com a dificuldade em promover o BI de código aberto. Geralmente, quando concorremos com soluções proprietárias, perdemos por causa de dois pontos: suporte local – frequentemente os clientes preferem trabalhar com empresas locais – e usabilidade, que os clientes costumam julgar pior nas soluções abertas.

LM *Se o próprio Código Aberto já tivesse uma maior aceitação, seria mais fácil promover BI de código aberto?*

GR Minha percepção é que, graças ao Código Aberto, estamos inserindo BI em projetos que não o utilizariam de outra forma. Isso ocorre porque muitos projetos não precisam de todos os recursos de BI, e somente com o Código Aberto esses clientes podem implementar apenas os recursos de que necessitam e pagar apenas pelo que vão, de fato, utilizar.

LM *Qual a diferença entre projetos livres direcionados por comunidades e aqueles direcionados por empresas?*

Assim que abrimos o código do SpagoBI, houve anúncios na comunidade de Software Livre italiana tratando do assunto, e uma das primeiras perguntas que surgiram era justamente “o que é Business Intelligence?”. Quando a resposta começava a deixar claro que era um software para uso em empresas, o interesse da comunidade simplesmente desaparecia.

LM *Para a Engineering, existe alguma desvantagem em depender de um ecossistema que ela não tem como controlar?*

GR Se você entra num ecossistema, automaticamente aceita entrar num ambiente que você não controla. Num ecossistema de verdade, as coisas simplesmente acontecem, e você precisa gerenciar para se adaptar a isso. É complexo.

No consórcio OW2, existe muita discussão. Às vezes discordamos e acontecem quebras e rompimentos internos. Mas todos do consórcio colhem os frutos da colaboração que realizam dentro dele. Ninguém tem o papel de controlar o ecossistema, mas de usar sempre o melhor que ele oferece para fornecer a melhor solução possível. E tudo depende da compreensão das empresas de como trabalhar em rede. ■

Entrevista com Daniel Simon, gerente corporativo de infraestrutura de TI da M. Dias Branco

Código Aberto que agrupa

A M. Dias Branco comparou e comprovou: o groupware de código aberto Zimbra é melhor e mais barato que seus concorrentes proprietários.
por Pablo Hess



O Grupo M. Dias Branco atua no ramo alimentício, é líder nacional nos segmentos de massas e biscoitos e atua também nos segmentos de farinhas, margarinas e gorduras hidrogenadas. Com 25 unidades espalhadas pelo Brasil, a empresa tem faturamento aproximado de R\$ 2,5 bilhões de reais ao ano e abrange várias marcas presentes em todo o país.

Em busca de um software de groupware, a empresa escolheu o Zimbra, de código aberto, e explicou à **Linux Magazine** os motivos de sua opção.

Linux Magazine Como a M. Dias Branco se aproximou do Software Livre?

M. Dias Branco Os primeiros testes com Software Livre na empresa ocorreram há cinco anos, quando

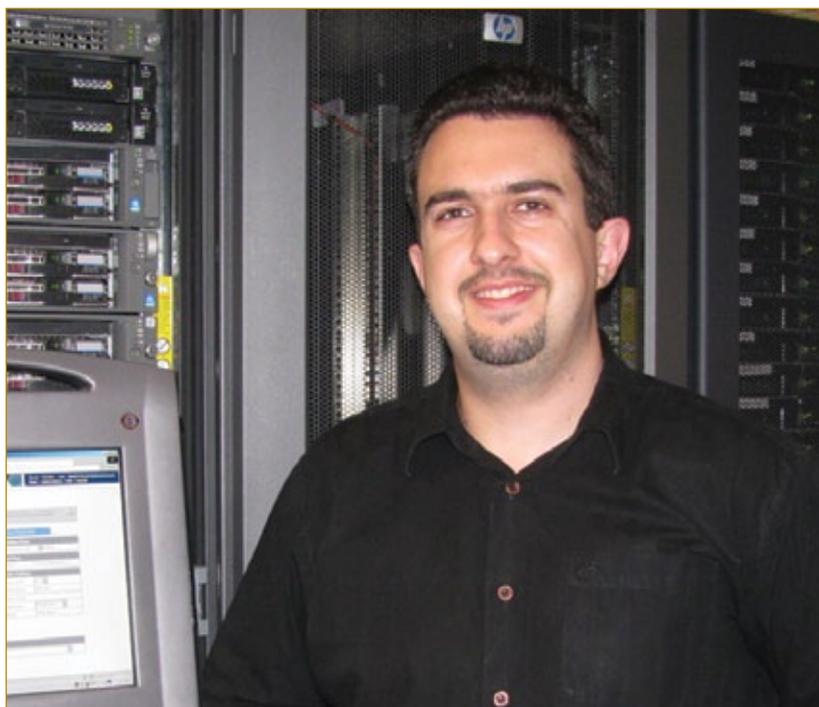
iniciamos os testes com o sistema operacional Linux. Em 2005, o Grupo optou por efetuar um *downsizing* de plataforma RISC UNIX para a plataforma x86 com Red Hat Linux, economizando aproximadamente US\$ 1 milhão na aquisição dessa solução.

LM O que levou a empresa a optar pelo Zimbra para a função de groupware?

MDB Antes de optarmos pelo Zimbra, avaliamos várias soluções de correio eletrônico, entre elas *Oracle Collaboration Suite* e *MS Exchange*. Ambas as soluções são muito boas, entretanto, se avaliarmos a utilização de seus recursos por parte do usuário, este não chega a 5% do que é oferecido.

Durante muito tempo, relutamos em utilizar soluções de código aberto, pois não havíamos encontrado uma solução que trouxesse os recursos de que necessitávamos com uma interface que agradasse aos nossos usuários.

O principal fator motivador foi o financeiro. Com a implementação do Zimbra, economizamos R\$ 500 mil reais apenas em licenças de software. Entretanto, não poderíamos admitir uma solução que deixasse a desejar com relação às soluções proprietárias que já conhecíamos.



Daniel Simon, gerente corporativo de infraestrutura de TI da M. Dias Branco.

LM *A abertura do Zimbra constitui alguma desvantagem ou vantagem na visão da M. Dias Branco?*

MDB O fato de o Zimbra possuir código aberto permitiu que efetuássemos algumas customizações e scripts. Estes, por sua vez, possibilitaram implementar particularidades de administração e integração com aplicativos desenvolvidos internamente, enquanto as soluções proprietárias não o permitiriam. Nesse aspecto, foi crucial o apoio dado pela empresa parceira, que focou nos entraves encontrados durante o processo de implementação.

LM *Qual o valor do investimento para a implantação do Zimbra?*

MDB O investimento não ultrapassou R\$ 30 mil, e o valor economizado possibilitou a implementação de diversos outros projetos que não estavam em pauta devido a restrições orçamentárias.

LM *Em quanto tempo se espera o retorno do investimento?*

MDB O Zimbra possui uma interface de administração simples. Isso permitiu que a equipe interna assimilasse seu uso facilmente, e por isso não houve aumento do TCO em decorrência da implementação dessa solução. Em outras palavras, o retorno do investimento foi imediato.

LM *Quanto tempo durou o processo de implantação?*

MDB O processo de implementação levou quatro meses, e o Zimbra já está em produção há seis meses. Após esse processo, implementamos também um anti-spam livre, e atualmente estamos, juntamente com a F13 Tecnologia, em fase de implementação de uma ferramenta de *web conference* integrada ao Zimbra.

A base de usuários que utiliza o zimbra hoje é de 3.200 usuários.

LM *Quantas pessoas se envolveram na implantação?*

MDB A equipe foi composta por apenas dois profissionais, sendo um técnico interno à M. Dias Branco e um profissional da F13 Tecnologia, que ficou completamente alocado durante o período da implementação.

LM *Que vantagens técnicas a nova solução oferece?*

MDB Tecnicamente, a solução é equiparável às concorrentes proprietárias, sendo sua principal vantagem a possibilidade de customização em função de necessidades específicas. No geral, a principal vantagem, sem dúvida, foi a economia promovida pelo Zimbra.

LM *A M. Dias Branco já tinha alguma opinião sobre softwares de código aberto antes da implantação?*

MDB A empresa não toma partido sobre ideologias. Nosso posicionamento é puramente profissional, alinhado com as necessidades da empresa. Buscamos o que melhor atende as nossas demandas.

Há bastante tempo já implementamos soluções baseadas em Software Livre, sempre após uma extensa avaliação técnica com o objetivo de verificar sua eficácia. A cada dia trocamos mais softwares proprietários por Software Livre, sempre por conta de sua qualidade superior e baixo custo.

LM *Existem planos de adotar outros softwares de código aberto no futuro?*

MDB Atualmente utilizamos amplamente o sistema operacional Linux. Aproximadamente 70% de nossos 120 servidores já rodam o sistema operacional do pingüim.

Além dele, utilizamos outros softwares de código aberto como o ASSP na prevenção de spam e o banco de dados MySQL em alguns sistemas, entre outros. ■

Ciclo de Palestras de Tecnologia da Informação

ROAD SHOW TI.09
SENAC
de março a maio



O Senac convida você para o ciclo de palestras que vai abordar os mais variados assuntos sobre Tecnologia da Informação. As novas tendências e as últimas novidades do mercado. Palestras com grandes profissionais e muito mais novidades. Não perca.

Em 32 unidades do Senac São Paulo (Capital e Interior).

Para mais informações sobre datas, locais de realização e inscrições:

0800 883 2000 ou www.sp.senac.br/roadshowti

Parceiros de conteúdo:



Apoio:

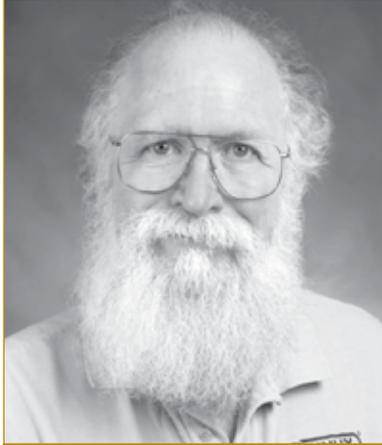


Realização:

senac
são paulo

Patrocínio:

Brasofware®



Coluna do maddog

Planos de negócios livres

Se tudo que você quer é ganhar dinheiro fazendo Software Livre, pode ser importante traçar um plano de negócios.

Recentemente uma pessoa chegou perto de mim numa conferência e disse que tivera uma empresa montada sobre um produto de software livre e a empresa havia falido. Eles tinham concebido um produto, contratado desenvolvedores, investido um monte de dinheiro no projeto e, quando chegou a hora de as pessoas comprarem o software, ninguém o fez. Ele perdeu todo o dinheiro investido. Perguntei qual era seu plano de negócios antes de começar a contratar os programadores. Ele disse que jamais chegara ao ponto de criar um plano de negócios. Essa era parte do problema, senão todo ele.

Quando chegou a hora de as pessoas comprarem o software, ninguém o fez. Ele perdeu todo o dinheiro investido.

Antes de escrever software livre, é preciso definir quais são os seus objetivos e como você planeja alcançá-los. Algumas pessoas escrevem software livre “só por diversão”, ou para aprender mais sobre a escrita de software para uma necessidade específica. Elas não precisam de incentivo para ganhar dinheiro com software. Mesmo que jamais ganhem um único real com o software, continuarão a escrevê-lo.

Outras pessoas têm interesse em campos como fotografia, astronomia ou administração de sistemas em geral, e precisam do software para ajudá-los nesse

campo. Frequentemente, elas criam um projeto para agrupar outros que também estejam interessados nesse campo para ajudá-los a melhorar o software.

Algumas pessoas escrevem software livre pelos motivos políticos ou sociológicos de “libertar a Internet” ou de “inclusão digital”. Elas acreditam (acho que corretamente) que a sociedade em geral seria melhor com a possibilidade de adequar o software às suas necessidades e dedicam suas horas livres e talentos para tornar isso verdade.

Por último, algumas pessoas enxergam no software livre uma chance para ganhar ou economizar dinheiro, tanto diretamente por meio da venda de serviços quanto pela aplicação de novas técnicas de software que agregam valor ao negócio do usuário.

Esse último grupo de pessoas geralmente não escreve o software para seu próprio uso, então uma maior parte da compensação por seu tempo e esforço é monetária. Portanto, é preciso saber a partir de onde e em que ponto do projeto a compensação vai vir.

O seu plano é ganhar dinheiro com base em serviços? Se sim, que tipo de serviço você vai oferecer? Integração? Treinamento? Personalização do software? A entrega do seu serviço conseguirá escalar direito? As pessoas vão perceber seu serviço como necessário e um “valor agregado” ao software?

Um amigo meu tinha uma empresa que oferecia treinamentos num certo pacote de software livre. Devido a uma alteração no direcionamento das comunidades, cada vez menos pessoas estavam usando esse software. Então, ele encontrou um software proprietário de uma empresa que não ia bem e adquiriu-a.

Reconhecendo que 60 por cento dos clientes que haviam comprado o software adquiriam também um contrato de suporte e treinamento, ele decidiu tornar

o software gratuito para download e pôs o código-fonte sob uma licença de Código Aberto. Imediatamente o número de empresas que usavam o software cresceu mais de 100 vezes, e (após um breve uso do software) 60 por cento das empresas que o baixaram compraram contratos de serviço e treinamento. Porém, meu amigo possuía os funcionários, recursos e experiência para alcançar e servir esse grande fluxo de pessoas, e então conseguiu obter a receita para fazer o negócio avançar. Ele ganhou muito mais dinheiro do que quando a empresa cobrava por licença.

Outro amigo tinha uma enorme quantidade de software que sua equipe de engenharia havia desenvolvido e que ele vendia e servia. Conforme aumentou a concorrência no mercado, ele foi forçado a cortar engenheiros e funcionários de verificação de qualidade. Ele decidiu tornar livre a maior parte do software e permitiu à comunidade baixá-lo, mantê-lo e melhorá-lo. Certas porções do software ele manteve proprietárias e alterou o foco de seu pequeno grupo de engenheiros para esse software, que apenas os maiores clientes achariam útil. Em segundo lu-

gar, ele cortou o custo das vendas ao comercializar apenas para os grandes clientes que haviam baixado o software livre. Com a redução de despesas e a alteração do foco da equipe de engenharia para novas funcionalidades que esses grandes clientes achariam úteis, ele manteve sua empresa.

Algumas pessoas argumentarão que o último exemplo de software não era completamente livre para os grandes clientes. Porém, as ações tomadas pelo meu amigo permitiram que pequenas empresas usassem e mantivessem o software (livre) para seu próprio uso, em vez de fazerem o software desaparecer de vez. Existem muitos projetos técnicos ótimos. As pessoas que esperam algum dia sustentar-se escrevendo software livre devem começar com um bom plano de negócios. ■

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



CNASI - VI Congresso de Auditoria de Sistemas, Segurança da Informação e Governança

18 e 19 de maio - Brasília/DF

www.cnasi.com.br/df

A 6ª Edição do CNASI - Brasília, acontece nos dias 18 e 19 de maio e aborda temas atuais e necessários para manter você a frente. São cursos, palestras técnicas, casos de sucesso e painéis de debates que abordarão temas instigantes. Algumas atividades confirmadas:

- Gestão de Riscos: E agora?? O que eu deveria ter feito? O que posso fazer?
Edson Kowask Bezerra - Gerente de Segurança da Informação - CPqD

- Como Padronizar Automatizar e controlar um processo seguro de análise Forense
Sandro Surffert - Consultor em Computação Forense- TechBiz Forense Digital

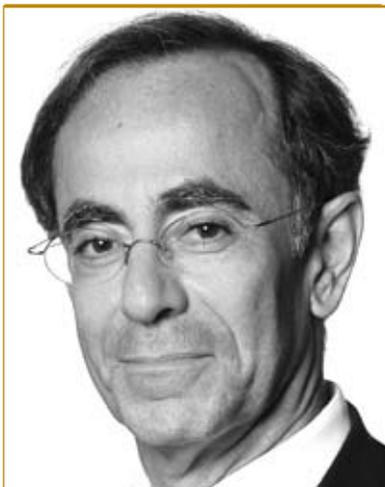
- Monitoração de Uso de Aplicações: Como Parar a Fraude Interna - Antes que Ela Pare Você!
Astor Calasso - Gerente Consultor - Governança, Auditoria e Segurança de TI - CONSIST - Business Information Technology

Faça agora a sua inscrição:
www.cnasi.com.br/df/inscricao

Aguardamos pelo seu contato 11 5531-3899 ramal 213
ou pelo e-mail glaucia@ideti.com.br
www.cnasi.com.br/df

Organização
e Realização:





Coluna do Taurion

O crescimento do ODF

Com o amplo apoio em diversas partes do planeta, o ODF continua no caminho para se tornar o formato padrão (e aberto) de documentos.

Há alguns dias li o relatório anual da ODF Alliance de 2008. O relatório mostra o avanço do ODF no mundo e, vou aqui fazer um pequeno extrato dele. O relatório, na sua íntegra, pode ser acessado em <http://www.odfalliance.org/resources/Annual-Report-ODF-2008.pdf>.

É indiscutível que o ODF está ganhando espaço no mercado, à medida que mais e mais governos requerem ou recomendam seu uso. Atualmente já são 16 os governos nacionais adotando ODF. Entre eles temos o Brasil (recentemente foi assinado o Procolo de Brasília, marco importante no contexto do ODF), Alemanha, Holanda, Bélgica, França, Japão, Rússia, Suíça, África do Sul, Uruguai e Venezuela. Interessante observar que, mesmo após o OpenXML ter sido aprovado pela ISO – de forma conturbada –, o ODF continua crescendo. E a própria Microsoft reconhece isso, ao afirmar que implementará o ODF em seu *Office 2007* por meio de um *Service Pack*. Além disso, no evento Red Hat Summit, em junho de 2008, Stuart McKee, National Technology Officer da Microsoft, disse: “O ODF claramente venceu”.

Claro, a Microsoft ainda insiste em dois padrões, ao tentar manter o OpenXML vivo, embora respirando por aparelhos. Bem, será que precisamos de mais de um padrão para a mesma coisa? Será que dois padrões nos dão o dobro de valor que um único?

A proposta do OpenXML aprovada pela ISO não é a especificação que está implementada atualmente no Microsoft Office 2007. Assim, os arquivos gerados no formato *docx* não serão necessariamente compatíveis com a nova especificação do OpenXML, ainda em discussão. E esta nova especificação ainda não tem data marcada para ser implementada! O resultado é que todo usuário do Microsoft Word ainda usa o velho e proprietário (e fechadíssimo) formato binário *.doc!* Aumenta-se a cada dia o acervo de arquivos em formato proprietário, aumentando o tamanho da bomba relógio...

O *business value* do ODF também continua a crescer, tendo hoje mais de 50 aplicativos que o suportam, como os pacotes *OpenOffice.org*, *StarOffice*, *Symphony* da IBM, *Word Perfect* e os que trabalham em nuvem como o *Google Docs*, *Zoho Office Suite* e *Adobe Buzzword*. A lista atualizada pode ser vista em <http://www.opendocumentfellowship.com/applications>.

Também o recente anúncio do *ODF Toolkit* permite aos desenvolvedores criar novas aplicações baseadas em ODF. Olha aí uma boa oportunidade para desenvolvedores brasileiros, uma vez que o próprio governo federal já colocou o ODF como padrão adotado no ePING v4.0.

Mas a luta continua... O ODF ainda tem muito a evoluir (a versão 1.2 já vai ser submetida à aprovação como padrão OASIS) e, no Brasil, sua adoção por governos estaduais e municipais poderia ser bem mais acelerada. Também ainda não vimos nenhuma manifestação por parte das bibliotecas públicas com relação à adoção de um formato aberto de documentos, como recentemente fez a Associação Canadense de Bibliotecas, como antes o fizeram o Arquivo Nacional da Austrália e a Biblioteca do Congresso dos EUA. Também os cursos de biblioteconomia deveriam ser mais ativos nessa discussão. É um assunto que lhes interessa diretamente.

A preocupação com padrões abertos já chegou inclusive à Casa Branca, com o discurso do novo presidente americano, Barack Obama, na sede do Google, em Mountain View, Califórnia, quando ele disse “Deixarei online os dados do governo em formatos acessíveis universalmente”.

Enfim, vamos usar documentos abertos! ■

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

Ferramentas flexíveis para configurar e gerenciar seus sistemas

Gerenciamento de rede

Administradores de sistemas profissionais com verbas de TI apertadas estão sempre à procura de novas ferramentas que os ajudem a fazer mais com menos. Conheça alguns aplicativos de código aberto populares para instalar, configurar, atualizar e monitorar sistemas e softwares pela rede.

Por Joe Casad

CAPA

Você já está cansado de ter de fazer o seu trabalho duas vezes – ou uma dúzia de vezes? Já não aguenta mais “rodar” pela empresa carregando um CD de instalação? Então esta edição é para você: este mês vamos apresentar ferramentas para automatizar e simplificar o desafio de configurar e gerenciar sistemas através da rede. É claro que ferramentas de gerenciamento de redes têm um longo histórico e a maioria dos profissionais de TI tem alguma experiência com os utilitários de gerenciamento mais comuns. Entretanto, o ambiente de rede de uma empresa é um cenário em constante mutação e nem sempre é simples manter o passo com os progressos mais recentes dos aplicativos. As últimas versões das ferramentas de código aberto nesta edição oferecem novos recursos para gerenciar configurações complexas de maneira sofisticada.

Nosso primeiro artigo, “Super máquina”, aborda de maneira detalhada a ferramenta de administração

de sistemas *Cfengine*. Começando com um simples exemplo do tipo “Olá mundo!”, vamos construir uma solução completa para instalar e gerenciar um serviço de software. O artigo é finalizado com um estudo de caso que descreve como usar o *Cfengine* para instalar um servidor web Apache.

No artigo seguinte, apresentamos uma outra ferramenta de código aberto tão prática quanto poderosa: o *Bcfg2*, desenvolvido pelo Argonne National Laboratory do departamento de energia norte-americano. Vamos mostrar como usar a arquitetura avançada do *Bcfg2* como uma plataforma flexível para configuração de aplicativos em máquinas clientes através da rede.

Em nosso último artigo de capa, apresentamos o *Zenoss*, uma ferramenta versátil de monitoramento de redes que fornece recursos de análise e monitoramento de estado e desempenho de serviços para redes grandes e pequenas. O *Zenoss* oferece suporte para uma variedade de

protocolos e tecnologias, incluindo SNMP, SSH e infraestrutura WMI (*Windows Management Instrumentation* – Instrumentação de Gerenciamento do Windows). Uma arquitetura modular e uma variedade de opções de interface auxiliam no ajuste do *Zenoss* às suas necessidades. Além de mostrar como instalar e configurar o sistema, vamos descrever também como usá-lo para monitorar tanto clientes equipados com Windows® quanto com Linux.

As ferramentas abordadas nesta edição são excelentes alternativas em redes corporativas, mas não deixam de ser igualmente úteis para redes de menor escala. Esperamos que o leitor aprecie o material que preparamos para tirar a sua rede da crise. ■

Índice das matérias de capa

Super máquina!	pág. 32
O gerente	pág. 42
O observador	pág. 48

Gerenciando redes com o Cfengine

Super máquina!

Automatize tarefas administrativas com a poderosa plataforma Cfengine.
por **Brendan Strejcek**

O Cfengine [1] é uma poderosa plataforma de automatização das tarefas de administração de sistemas. Com ela, o administrador pode gerenciar desde uma máquina até uma rede heterogênea inteira. A primeira versão do Cfengine foi lançada há mais de 15 anos por Mark Burgess, um professor da Universidade de Oslo, Noruega. De acordo com as estimativas de uso, o Cfengine já gerenciou mais de um milhão de computadores em todos esses anos. A terceira versão da plataforma Cfengine traz alguns recursos novos e abole todas as velhas camadas históricas. Os desenvolvedores chegaram até a reinstrumentar a linguagem usada pela plataforma, de modo que

agora todos os seus elementos são manipulados de maneira uniforme.

Para ilustrar o que é possível fazer com o Cfengine 3, vamos introduzir vários componentes do sistema em um exemplo funcional. Para que o leitor possa seguir esse procedimento, são necessárias duas máquinas Linux em rede, que chamaremos aqui *PolicyServer* e *Client*. Nosso objetivo final é ter um servidor web *Apache* totalmente configurado, funcional e gerenciado, rodando na máquina cliente, sem que seja necessária qualquer configuração manual além da instalação do próprio Cfengine.

O modelo básico usado neste artigo deverá armazenar e distribuir todo o código de política de gerenciamento

(o *policy code*) a partir de um único servidor central. O Cfengine pode ser usado de diversas maneiras, já que é uma plataforma muito flexível, mas o modelo sugerido é bastante comum, além de ser suficiente para a maioria dos administradores de redes e sistemas. O *PolicyServer* vai armazenar e disponibilizar o repositório central de código do Cfengine, e a máquina *Client* vai receber dele a configuração do Apache.

Instalação

Primeiro, vamos instalar o Cfengine tanto no servidor quanto no cliente. Há pacotes disponíveis para muitas distribuições Linux populares, ou pode-se simplesmente compilar o programa a partir do código-fonte.

O Cfengine 3 tem muito poucas dependências em seu processo de compilação – e ainda menos dependências depois de compilado (somente as bibliotecas *libcrypto*, do projeto *OpenSSL*, e a *libdb*, do projeto *Berkley DB*). Muito embora não seja imprescindível, a biblioteca de manipulação de expressões regulares compatíveis com Perl (a *libpcre*) também contribui de modo significativo para o funcionamento do Cfengine.

Se o programa for compilado a partir do código-fonte, é necessário primeiramente obter os pacotes tipo *TAR.GZ* das versões 2 e 3 do Cfengine, disponíveis na presença web do projeto [2]. Adicionalmente, vamos precisar ter instaladas para a compilação do Cfengine as ferramentas *Flex*, *Bison* e *Make*, além da biblioteca estática *libcfengine* do Cfengine 2. Uma vez que todas essas dependências estejam disponíveis, vamos compilar o Cfengine 2 em primeiro lugar, compilando o Cfengine 3 na sequência (usar o mesmo procedimento a seguir para ambos):

```
$ ./configure
$ make
$ sudo make install
```

Por padrão, os arquivos são instalados em */usr/local*, mas pode-se modificar isso acrescentando o argumento *--prefix=algum/outro/diretório* ao comando *configure*, embora seja necessário se certificar de que o processo de compilação seja capaz de encontrar a biblioteca *libcfengine*. Todos os binários serão instalados em *sbin* sob o prefixo escolhido (por padrão, */usr/local/sbin*). A próxima versão do Cfengine – a 3.0.1 – com data de lançamento prevista para o final de 2009, não vai mais necessitar da *libcfengine*, de modo que essa dependência é apenas uma situação provisória.

Olá mundo!

Uma vez que o programa esteja instalado apropriadamente no servidor e no cliente, estamos prontos para dar uma primeira olhada no Cfengine em ação. Um simples exemplo, ao estilo “Olá mundo!”, vai servir para mostrar um programa do Cfengine 3 em execução. Primeiramente, execute o comando *cf-key* sem argumentos. Esse comando cria alguns arquivos ocultos no diretório *home* e gera um par de chaves (que nós não vamos precisar usar no momento, mas que serão necessárias para fazer cópias remotas).

Nosso programa “Olá mundo!” será escrito para o *cf-agent*, que é o programa que faz o “grosso” do trabalho de configuração no Cfengine. O *cf-agent* monitora o estado do sistema e aplica ações corretivas sempre que necessário. Da mesma forma que *perl* e *sh* são os interpretadores para Perl e para Bourne Shell, respectivamente, pode-se encarar o *cf-agent* como um interpretador de comandos na linguagem do Cfengine. Por padrão, como usuário sem nenhum privilégio, o *cf-agent* lê e executa código armazenado em *~/cfagent/input/promises.cf*. Assim, utilizando seu editor de textos (sem formatação) preferido, crie esse arquivo, incluindo nele o seguinte:

```
body common control {
  bundlesequence => {"hello"};
}
```

```
bundle agent hello {
  reports:
  linux::
    # Isto é um comentário
    "Olá mundo!";
}
```

Espaços em branco não são considerados na linguagem do Cfengine, assim, pode-se indentar o código “a gosto”. Sem nenhum argumento no terminal, basta executar agora o *cf-agent*. Não importa em qual das máquinas vamos executá-lo, uma vez que o software está instalado em ambas.

Como se pode ver, as duas entidades principais presentes no código são um *body* de nome *control* e um *bundle* chamado *hello*. A entidade do tipo *bundle* (inglês para “pacote”) é a principal diretiva de agregação do Cfengine (da mesma forma que uma função é a principal estrutura de dados em C, muito embora *bundles* não sejam funções do ponto de vista da matemática). Uma entidade do tipo *body* é basicamente um agrupamento de parâmetros. Ambas, *body* e *bundle*, especificam por qual componente do Cfengine eles serão “consumidos”. No caso do *body* do tipo *control*, o consumidor é *common*, uma palavra-chave especial que significa a plataforma Cfengine como um todo, e no caso do *bundle hello*, o consumidor é *agent*, que se refere ao executável do Cfengine de nome *cf-agent*.

Exemplo 1: cf-serverd.cf

```
01 body server control {
02   trustkeysfrom => { "192.168.1.62", "192.168.1.61" };
03   allowconnects => { "192.168.1.62", "192.168.1.61" };
04   maxconnections => "10";
05   logallconnections => "true";
06 }
07 bundle server access_rules {
08   access:
09     "/srv/cf-serverd"
10     admit => { "192\..168\..*" };
11 }
```

Exemplo 2: update.cf

```

01 body copy_from remote(server, path) {
02   servers => {
03     "${server}" };
04   encrypt => "true";
04   trustkey => "true";
05   source => "${path}";
06   compare => "digest";
07   preserve => "true"; # Preservar permissões
08   verify => "true";
09   purge => "true";
10 }
11 body depth_search recurse {
12   depth => "inf";
13 }
14 bundle agent update {
15   vars:
16     any::
17     "cfserverd" string => "192.168.1.61";
18     "policyfiles" string => "/srv/cf-serverd";
19     "server_inputs" string => "${policyfiles}/inputs";
20     "client_inputs" string => "${sys.workdir}/inputs";
21   files:
22     any::
23     "${client_inputs}"
24     copy_from => remote("${cfserverd}", "${server_inputs}");
25     depth_search => recurse;
26 }

```

A entidade tipo *bundle* de nome *hello* é referenciada em *bundlesequence*, que é uma diretiva especial que diz ao *cf-agent* qual código deverá ser executado e em que ordem. O identificador especial *reports* é um tipo de “compromisso” – um dos muitos tipos de instruções que podem ser feitas sobre como se deseja que o sistema funcione.

Assim, entidades do tipo *bundle* são formadas por “compromissos”. Neste caso, como o leitor provavelmente já pode imaginar, *reports* são um meio de gerar conteúdo de saída (*output*). O próximo identificador, *linux*, seguido por dois pontos, é uma classe. Mais adiante vamos explicar classes mais detalhadamente. Por enquanto, basta saber que códigos

Exemplo 3: promises.cf

```

01 body common control {
02   bundlesequence => {
03     "update" };
03   inputs => { "update.cf", "cf-serverd.cf" };
04 }
05 # Algumas ações arbitrárias e
05   inócuas que vão gerar alguma saída
06 bundle agent hello {
07   commands:
08     any::
09     "/bin/date";
10     reports:
11     linux::
12     "Olá mundo!";
13 }

```

pertencentes a esta classe só serão executados em máquinas equipadas com Linux.

Arquivos de configuração

Agora que o *cf-agent* está ativo e em execução, o próximo passo é configurar o serviço *cf-serverd* no *PolicyServer*, de modo que o cliente possa obter daí uma política atualizada. O *cf-serverd* funciona como um servidor de arquivos seguro que fornece acesso externo ao *cf-agent* funcionando em uma máquina específica.

No *PolicyServer*, indique um diretório como repositório canônico de políticas. Pode-se utilizar, por exemplo, */srv/cf-serverd* ou qualquer outro local que melhor se adeque ao seu ambiente operacional. Não é indicado utilizar */var/cfengine*. O *PolicyServer* também será provavelmente um cliente, isto é, o servidor vai atualizar sua política e avaliá-la usando o programa *cf-agent*.

Em seu repositório central, crie um diretório de nome *inputs*. Vamos espelhar o conteúdo do diretório de trabalho */var/cfengine*, mas esse será o único diretório com que devemos nos preocupar no momento. No diretório */srv/cf-serverd* é necessário criar quatro arquivos. O primeiro passo é criar o arquivo *cf-serverd.cf* (**exemplo 1**). Esse arquivo controla quais máquinas podem conectar-se ao servidor e a quais arquivos elas terão acesso. Além disso, esse arquivo também contém algumas variáveis de configuração específicas do programa *cf-serverd*.

Vamos criar agora o arquivo *update.cf*, que vai conter o código que o cliente executa para sincronizar a sua política local com a política central no repositório (**exemplo 2**).

O **exemplo 2** introduz algumas variáveis específicas do Cfengine. Diferentemente de versões anteriores, todas as variáveis agora têm

tipos dinâmicos (antes eram todas simples cadeias de caracteres, ou *strings*). Outros tipos de variável incluem *slit* (uma lista de *strings*), *real* (um número com ponto decimal flutuante) e *int* (um número inteiro). Variáveis são – da mesma forma que no shell – substituídas por `#{nome-da-variável}`.

O **exemplo 3** mostra o arquivo `promises.cf`. A último arquivo de configuração é o `failsafe.cf`, que contém simplesmente o seguinte:

```
body common control {
  bundlesequence => { "update" };
  inputs => { "update.cf" };
}
```

Os arquivos especiais `promises.cf` e `failsafe.cf` trabalham basicamente como “despachantes” que especificam qual outro código o programa `cf-agent` deve executar. Os nomes dos arquivos `cf-serverd.cf` e `update.cf` são totalmente arbitrários, de modo que se pode batizá-los “a gosto”, embora seja inteligente utilizar nomes que tenham a ver com as suas respectivas funções.

O ponto inicial programado no `cf-agent` é o arquivo `promises.cf`. Todo código que se queira executar tem que estar ou nesse arquivo ou referenciado por ele. O arquivo `failsafe.cf` não é realmente necessário, mas se houver um problema com o arquivo `promises.cf`, o `cf-agent` irá buscar alternativamente `failsafe.cf`, de modo que é uma boa ideia se certificar de que esteja disponível um bom `failsafe.cf` simples e bem conhecido.

O arquivo `failsafe.cf` simplesmente tenta atualizar os arquivos de política a partir do servidor. Como no nosso caso criamos o `failsafe.cf` apenas para buscar a política mais recente, ele funciona também como instrução de inicialização para o cliente Cfengine. Assim, para configurar o cliente

inicialmente, basta copiar `failsafe.cf` (e os arquivos referenciados nele) para o cliente.

Obtendo as chaves

Antes de testar o sistema, é necessário gerar pares de chaves públicas para criptografia. Como *root*, execute o programa `cf-key` tanto no *PolicyServer* quanto no *Client*. Esse comando cria identidades no diretório `/var/cfengine/ppkeys`. Devido à maneira como o `cf-serverd` está configurado em `cf-serverd.cf`:

```
trustkeysfrom => { "192.168.1.62",
  ↪ "192.168.1.61" };
```

e como o `cf-agent` está configurado em `update.cf`:

```
trustkey => "true";
```

o comportamento das máquinas será aceitar a chave de uma máquina remota em confiança na primeira vez, mas daí por diante vai aceitar clientes provenientes do mesmo IP em confiança se eles puderem provar que possuem a mesma chave. Essa postura é bem permissiva, mas, com o devido esforço e cuidado, pode-se ser mais rigoroso em sistemas de produção. Para tanto, será

Exemplo 4: cf-execd.cf

```
01 body executor control {
02   splaytime => "1";
03   mailto => "root@example.com";
04   smtpserver => "192.168.1.61";
05   mailmaxlines => "1000";
06   schedule => { "Min00_05", "Min30_35" };
07   executorfacility => "LOG_DAEMON";
08 }
09 bundle agent executor {
10   processes:
11     any::
12       "cf-execd"
13       restart_class => "start_cfexecd";
14   commands:
15     start_cfexecd::
16       "/usr/local/sbin/cf-execd";
17 }
```

necessário lidar com a distribuição de chaves através de um canal externo. Um modo comum de melhorar isso é distribuir a chave pública do servidor usando o sistema de instalação do sistema operacional, mas permitir que o servidor aceite novos clientes em confiança. O nível de segurança adequado para cada caso é sempre uma decisão complicada e de responsabilidade do administrador de sistemas, que deve saber avaliar o grau de vulnerabilidade da sua rede e o nível de hostilidade do ambiente em que ela está inserida.

Começando

Para começar, copie manualmente os arquivos de configuração do `cf-serverd` para o diretório correto:

```
cd /srv/cf-serverd/inputs
cp promises.cf update.cf cf-
  ↪serverd.cf /var/cfengine/inputs
```

Exemplo 5: O bundle comum

```
01 bundle common httpd {
02   vars:
03     any::
04       "version" string => "httpd-2.2.10";
05       "prefix" string => "/opt/httpd/${version}";
06       "server" string => "${prefix}/bin/httpd";
07       "apachectl" string => "${prefix}/bin/apachectl";
08       "conf" string => "${prefix}/conf/httpd.conf";
09 }
```

Exemplo 6: Configurando o Apache

```

01 bundle agent install_web_server {
02   vars:
03     any::
04       "source" string =>
05         "${sys.workdir}/inputs/support_files/${httpd.version}.
↳tar.gz";
06
07       # Will get automatically cleaned up by the update purge
08       "compiledir" string => "${sys.workdir}/inputs/${
↳httpd.version}";
09     classes:
10       "web_server_installed" expression => fileexists("${
↳httpd.server}");
11     commands:
12       !web_server_installed::
13         "/bin/tar xzf ${source} -C ${sys.workdir}/inputs";
14         "/bin/sh configure --prefix=${httpd.prefix}
↳--enable-modules=all"
15         contain => cd("${compiledir}");
16         "/usr/bin/make"
17         contain => cd("${compiledir}");
18         "/usr/bin/make install"
19         contain => cd("${compiledir}");
20 }

```

Perceba que o servidor está recebendo cópias de `update.cf` e de todos os outros arquivos. Durante a operação do sistema em produção, qualquer modificação realizada no arquivo `cf-serverd.cf` no repositório central será automaticamente distribuída para todos os sistemas.

Com todos os arquivos de configuração no lugar, é hora de iniciar o serviço `cf-serverd`. O comando a seguir inicia o `cf-serverd` em modo "verboso" e em plano de fundo. Caso essas opções não sejam ativadas, o `cf-serverd` vai iniciar em modo silencioso em plano de fundo.

```
cf-serverd --verbose --no-fork
```

Agora inicie o cliente copiando os arquivos `failsafe.cf` e `update.cf` manualmente para `/var/cfengine/inputs` no cliente (lembre-se de que, em um sistema de produção, esse tipo de tarefa poderia ser realizada automaticamente), e então execute `cf-agent`, que vai executar o código disponível no arquivo `failsafe.cf` que está no diretório que contém esse arquivo:

```
cf-agent --bootstrap
```

Se voltarmos ao console do servidor, veremos muitas mensagens sobre o que está acontecendo do lado do servidor. Se o controle de acesso não for configurado corretamente, haverá mensagens de registro diagnosticando por que a conexão ou a cópia foi negada. Uma vez que se verifique que a cópia via rede foi bem sucedida, pode-se encerrar o serviço `cf-serverd` sendo executado em primeiro plano com **[Ctrl]+[C]** e inicializá-lo para rodar como serviço em plano de fundo sem argumentos.

Quadro 1: Princípios de projeto

O Cfengine foi desenvolvido em torno de alguns conceitos de projeto. Genericamente, sua linguagem é descritiva em vez de iterativa. Sempre que possível, estamos tentando descrever o que e não como o sistema deve se comportar. Na prática, essa abordagem geralmente significa que as ações do Cfengine são *idempotentes*, ou seja, que a aplicação da mesma função duas vezes gera o mesmo resultado. Essa característica é importante porque o Cfengine monitora continuamente o estado das máquinas em seu ambiente e, dependendo de como a política de monitoramento e configuração dessas máquinas for definida, o Cfengine corrige quaisquer divergências.

Outro princípio que rege o funcionamento do Cfengine é a sua aderência a uma arquitetura baseada em interrupções, na qual os clientes requisitam novos códigos de política de um servidor. Esse comportamento difere

de um sistema mandatório (*push*), que requer que uma entidade central se conecte periodicamente a todos os clientes para configurá-las "goela abaixo". O uso de uma arquitetura dirigida por interrupções que vem dos clientes permite que uma máquina que estiver desligada, ou que até mesmo nem estiver disponível, seja configurada, uma vez que as modificações realizadas no servidor serão requisitadas por essa máquina automaticamente assim que elas forem conectadas à rede. O Cfengine também dispõe de recursos para configurar as máquinas de cima para baixo, mas mesmo esses recursos são feitos usando um mecanismo de interrupção. Esse princípio também tem implicações importantes na autonomia das máquinas clientes: se o servidor no qual o Cfengine está instalado parar de funcionar por alguma razão, o cliente pode continuar a usar a política armazenada localmente e seguir funcionando, até a próxima vez em que ele puder se conectar ao servidor novamente.

Agendador

O último componente da infraestrutura do Cfengine é o agendador periódico. O `cf-execd` é um serviço de agendamento similar ao `cron`. Pode-se questionar a razão pela qual o Cfengine não usa simplesmente o `cron`, e muitos administradores realmente o executam usando também o `cron`, no intuito de aumentar a confiabilidade do sistema, configurando o `cf-agent` para reiniciar o `cron` ou o `cf-execd` sempre que necessário. O uso do `cf-execd` traz vários benefícios adicionais, incluindo o controle do agendamento em uma política central do Cfengine, bem como a possibilidade de formatar e enviar relatórios via e-mail a respeito de qualquer ação que ocorrer no sistema. Caso se decida também pela execução do `cf-agent` em conjunto com o `cron`, é recomendável que o `cron` execute o `cf-agent` usando a versão do `cf-execd` em plano de fundo. Desta forma, teremos as mesmas configurações de email em ambos os sistemas e o `cf-execd` vai registrar qualquer atividade em `/var/cfengine/outputs`. Neste caso, entretanto, vamos assumir que o `cf-agent` será executado pelo `cf-execd` e não pelo `cron` diretamente.

Primeiramente, vamos criar um novo arquivo que controle os recursos do `cf-execd` (`cf-execd.cf`) e incluí-lo na lista de entradas (**exemplo 4**).

O **exemplo 4** indica que o `cf-execd` vai ser executado duas vezes a cada hora (que é a linha de agendamento – de número 06, indicada pela palavra-chave `schedule` – e os dois membros da lista são chamados classes de temporização do Cfengine) e enviará mensagens de correio eletrônico para o endereço `root@example.com`, com a máquina de endereço IP `192.168.1.61` atuando com relay. Se houver um endereço de email utilizável e um servidor de relay disponível, é recomendável

Exemplo 7: library.cf

```
01 bundle edit_line DeleteLinesContaining(pattern) {
02   delete_lines:
03     ".*${pattern}.*";
04 }
05 body replace_with ReplaceValue(value) {
06   replace_value => "${value}";
07   occurrences => "all";
08 }
09 bundle edit_line ReplaceAll(from,to) {
10   replace_patterns:
11     "${from}"
12   replace_with => ReplaceValue(${to});
13 }
```

usá-los para desenvolver uma primeira impressão de como o sistema se comunica com o administrador de sistemas.

O item que mais carece de informações é o `splaytime`. Se um determinado `splaytime` for fornecido, o `cf-execd` efetivamente aguarda um número (pseudo) aleatório de minutos antes de tentar se conectar ao servidor, com o `splaytime` sendo o limite máximo a esperar. Assim, no exemplo 4, o `cf-execd` aguarda até um minuto. A estratégia por trás do conceito é evitar contenção de recursos.

No nosso caso, podemos ajustar o valor do `splaytime` para um valor baixo, como 1, por exemplo, de modo que o usuário não precise esperar muito para ver o `cf-execd` em atividade. Em um ambiente de produção, entretanto, seria melhor ajustar esse valor para algo entre 15 e 20 minutos, semelhante ao valor de `schedule` mostrado no **exemplo 4**.

É importante lembrar também de adicionar o `bundle` do tipo `executor` que acabamos de criar a uma `bundlesequence` no arquivo `promises.cf`. Feito isso, podemos retornar ao cliente e executar `cf-agent` novamen-

Exemplo 8: httpd.conf

```
01 bundle agent configure_web_server {
02   classes:
03     "web_server_installed" expression => fileexists("${
04     ↳{httpd.server}");
04   vars:
05     "info" string => "Include conf/extra/httpd-info.conf";
06   files:
07     web_server_installed::
08       # Descomentar linha contendo httpd-info.conf
09       "/tmp/httpd.conf"
10       edit_line => ReplaceAll("^#${info}.*", "${info}"),
11       classes => DefineIfChanged("restart_httpd");
12       # Remover controle de acesso de httpd-info.conf
13       "/tmp/httpd-info.conf"
14       edit_line => DeleteLinesContaining("(Allow|Order
15     ↳|Deny)"),
15     classes => DefineIfChanged("restart_httpd");
16   commands:
17     restart_httpd::
18       "${httpd.apachectl} graceful";
19 }
```

te. Isso deverá atualizar a política a partir do servidor e colocá-la em funcionamento.

Em seguida, verificando uma listagem de processos, deveremos ser capazes de conferir que o serviço *cf-execd* foi iniciado. De ponto de vista do cliente, o processo passou a ser totalmente automatizado: qualquer modificação realizada no repositório central de políticas de funcionamento será baixada e executada automaticamente pelo cliente. Uma vez que o tempo de agendamento seja atingido, o *cf-execd* será ativado, executará o *cf-agent* e depositará qualquer saída em */var/cfengine/outputs*.

Manutenção de um serviço

Suponhamos que queiramos usar o Cfengine para instalar e configurar o servidor *httpd* Apache. Na verdade, podemos até compilar o sistema a partir de seu código-fonte, de modo que nossa solução será portátil, rodando em muitas distribuições Linux e plataformas. Em um ambiente de produção, entretanto, é questionável deixar os servidores compilarem o seu próprio software, por questões de segurança. Se for realmente necessário compilar um programa a

partir do código-fonte, é preferível montar um pacote customizado e distribuí-lo. Contudo, o uso do *cf-agent* para compilar um programa diretamente do código-fonte é uma alternativa (multiplataforma) que ilustra bem o nível dos recursos e a flexibilidade oferecidos pelo Cfengine.

Vamos, primeiramente, baixar o código-fonte do Apache e copiá-lo no repositório do Cfengine [3]. Em vez de configurar o cliente para baixar o código-fonte diretamente da Internet, é melhor armazená-lo localmente, de modo a não ficar dependente de repositórios externos. Simplesmente deixaremos o arquivo compactado contendo todo o código-fonte no diretório */srv/cf-serverd/inputs* do *PolicyServer* – de preferência em um subdiretório, por questões de boa organização –, e o *bundle* do tipo *update* vai cuidar de distribuí-lo.

Vamos criar um novo arquivo para armazenar todo o código relativo ao serviço *httpd*, por exemplo, com o nome *web_server.cf*. Esse arquivo precisa ser adicionado à diretiva *inputs* do arquivo *promises.cf*, bem como todas as instruções do tipo *bundle* contidas nele à diretiva *bundlesequence*. O primeiro passo é criar um *bundle* com algumas variáveis que podem ser reutiliza-

das por outras diretivas tipo *bundle*. Um *bundle* do tipo *common* pode ser consumido por qualquer componente do Cfengine e não precisa ser listado em *bundlesequence*. Cada *bundle* tem seu próprio escopo, e variáveis de um *bundle* externo podem ser acessadas por meio do esquema de interpolação *\${nome-do-bundle.variável}*. Assim, o código mostrado no exemplo 5 permite que outros tipos de *bundle* utilizem, por exemplo, *\${httpd.conf}*, que vão avaliar o caminho inteiro.

Diretivas do tipo “compromisso” (i.e., *promises*), tais como comandos, arquivos ou relatórios (*reports*), têm com frequência parâmetros que determinam a natureza do compromisso. O par variável/valor apropriado vem na sequência do compromisso. Por exemplo, vamos considerar a seguinte diretiva do tipo compromisso:

```
processes:
  any::
    "cf-execd"
    restart_class => "start_
    cfexecd";
```

A diretiva tem um parâmetro chamado *restart_class*, que recebe uma cadeia de caracteres como valor (do seu lado direito). Neste caso, essa cadeia de caracteres se torna uma definição de classe se nenhum processo *cf-execd* estiver sendo executado. Alguns parâmetros usam conteúdo do tipo *body* (corpo) externo como valor. O uso de um corpo externo permite múltiplos pares variável/valor, bem como mais parametrização, o que possibilita reutilização. Para tornar esse conceito mais concreto, vamos considerar o exemplo que usaremos em breve para compilar o Apache. O seguinte corpo, que usa um argumento, nos permite executar comandos em um diretório específico sem a necessidade de dispor de um terminal:

Exemplo 9: Cão de guarda (Watchdog)

```
01 bundle agent monitor_web_server {
02   classes:
03     "web_server_installed" expression => fileexists("${
04     {httpd.server}");
05   processes:
06     web_server_installed::
07       # Define uma classe se o serviço httpd não
08       estiver rodando,
09       # de modo que possamos inicializá-lo
10       "httpd"
11       restart_class => "start_httpd";
12   commands:
13     start_httpd::
14       "${httpd.apachectl} start";
15 }
```

```
body contain cd(dir) {
  useshell => "false";
  chdir => "${dir}";
}
```

Tais corpos podem ser armazenados em qualquer arquivo de entrada do Cfengine, mas como eles são frequentemente genéricos e podem ser reutilizados por muitas diretivas do tipo compromisso, faz mais sentido que eles sejam armazenados em arquivos separados, que chamaremos aqui pelo nome `library.cf`. Caso o leitor ainda não tenha feito isso, vamos colocar esse corpo `cd` em um arquivo `library.cf` e incluir esse arquivo no `bundlesequence` do arquivo `promises.cf`. É importante lembrar que, se modificarmos esse corpo mais tarde, isso pode afetar diversos compromissos que estiverem ativos, de modo que é preciso ter cuidado

ao manipular esse tipo de recurso, já que ele pode ser compartilhado por outras diretivas.

No Cfengine, uma classe é uma condição booleana com o objetivo de representar algum aspecto do estado do sistema, seja esse estado um sistema operacional ou a hora do dia. Muitas classes são definidas automaticamente pelo `cf-agent`, mas o administrador de sistemas pode definir outras baseados nos valores retornados pelos programas ou mesmo por outros meios. Qualquer compromisso seguindo uma expressão de classe (cadeias de caracteres terminando com `::`) só entra em vigor quando a classe retornar o valor “verdade” (`true`). Por exemplo, podemos entender a seguinte expressão:

```
bundle agent a { reports: linux:
  ↳ “asdf”; }
```

como “imprima `asdf` se a classe `linux` estiver definida”. Como era de se esperar, o `cf-agent` define automaticamente a classe `linux` em máquinas rodando Linux em um ambiente Cfengine.

Já usamos a classe `any` diversas vezes no curso deste artigo. Essa classe retorna sempre o valor booleano `true`, e é usada com frequência, mesmo quando não é estritamente necessário, para manter uma indentação correta nos blocos de diretivas. Se executarmos o comando `cf-agent -pv` – o que é sempre seguro, uma vez que, assim, códigos de política não são executados –, poderemos ver todas as classes definidas automaticamente. Em uma das máquinas de teste que utilizamos na confecção deste artigo, algumas das classes automaticamente definidas são: `64_bit`, `Friday`, `debian_4` e `xen`.

Certificação Linux Número 1 no Mundo



LPIC-1: reconhecida no mundo todo como A certificação inicial para profissionais de Linux



LPIC-2: uma certificação avançada em Linux, largamente reconhecida como uma "HOT CERT" do mercado, que proporciona os mais altos salários entre os profissionais de Linux



LPIC-3: a primeira certificação profissional enterprise-level em Linux, disponível a partir de janeiro de 2007



OSPREY: um programa único de progresso na carreira para TODOS os profissionais de Open Source



Saiba mais,
faça-nos uma visita
www.lpi.org/americ Latina

O exemplo do Apache

O **exemplo 6** ilustra um *bundle* que descompacta, compila e instala o Apache. Na maioria dos sistemas, a variável especial pré-definida `sys.workdir` vai indicar como diretório de trabalho `/var/cfengine`, o que essencialmente significa: “Testar se o software está instalado, verificando um determinado arquivo (heurísticas mais precisas poderiam também ser definidas); se não estiver, compile o programa executando a seguinte sequência de comandos padrão `untar`, `configure`, `make`, `make install`.”

Muitos aplicativos para servidores vêm com arquivos de configuração que precisam estar disponíveis em diretórios padrão antes que o serviço possa ser disponibilizado inteiramente. Neste caso, vamos configurar o Apache para permitir solicitações do tipo `server-info` e `server-status`. Isso requer a edição de dois arquivos de configuração diferentes. O Cfengine 3 dispõe de quatro tipos diferentes de *promises* que residem em *bundles* externos especiais do tipo `edit_lines – delete_lines`, `replace_patterns`, `field_edits` e `insert_lines` – e oferecem suporte a parâmetros adicionais.

Com esses compromissos, pode-se modificar a configuração de variáveis, desativar comentários de linhas de arquivos de configuração, ativando determinados recursos, o que acaba por permitir o gerenciamento desses arquivos de configuração. Antes de utilizar `edit_lines` em um compromisso do tipo *files*, vamos precisar criar alguns *bundles* do tipo `edit_lines`. Via de regra, eles são genéricos o suficiente para serem reutilizados em muitos componentes. Vamos usar dois deles em nosso exemplo: `DeleteLinesContaining` e `ReplaceAll`. Se o leitor estiver acompanhando a organização de arquivos utilizada no decorrer deste artigo até agora,

perceberá que o melhor local para incluir esses dois *bundles* é o arquivo `library.cf`, juntamente com outros *bundles* compartilhados (**exemplo 7**). Como se pode ver, eles têm praticamente a mesma estrutura e podem ser parametrizados também.

Adicionalmente, vamos precisar de uma maneira de definir uma classe que, caso editemos qualquer arquivo, nos permita disparar uma reinicialização do serviço relacionado àquele arquivo:

```
body classes
↳ DefineIfChanged(class) {
    promise_repaired => { "${class}"
↳ };
}
```

Uma vez que todos esses componentes estejam prontos, podemos dizer ao `cf-agent` para usá-los para editar arquivos de configuração. No nosso exemplo, precisamos desativar o comentário da linha `httpd-info` do arquivo `httpd.conf` e remover o controle de acesso do arquivo `httpd-info.conf` (**exemplo 8**).

Cão de guarda

Se precisarmos monitorar o processo do servidor de Internet – para reiniciá-lo caso ele pare de funcionar –, basta criar um outro *bundle* ou simplesmente incluir um outro compromisso no **exemplo 9**.

O código no **exemplo 9** envolve a detecção de processos usando uma classe, de modo a assegurar que o servidor web esteja sempre operante em máquinas que tenham um servidor desse tipo instalado.

Para aumentar ainda mais a confiabilidade, podemos criar alguns testes funcionais, ou seja, testes que realizem solicitações aos serviços em operação. No nosso exemplo, isso implicaria realizar o download de alguns dados através da porta 80, além da verificação do conteúdo dos dados propriamente

ditos, que devem ser aquilo que se esperava obter.

Conclusão

Como o ambiente Cfengine está configurado, aqui vão algumas sugestões de melhorias interessantes:

- ▶ Centralizar periodicamente as tarefas executadas;
- ▶ Integrar o monitoramento e a implantação de sistemas usando o `cf-agent` para configurar os monitores automaticamente;
- ▶ Integrar sistemas de backup aos sistemas de implantação;
- ▶ Certificar-se de que todas as máquinas estejam configuradas para enviar logs a um sistema de monitoramento central.

Quanto mais recursos estiverem disponíveis no ambiente Cfengine, mais fácil será a disponibilização de serviços online e a resolução de problemas, tais como falha de hardware ou brechas de segurança. Como é possível codificar todas as regras de criação de uma máquina de um determinado tipo em uma linguagem executável por máquinas, tudo o que precisamos é de uma instalação de sistema operacional básica e ter o Cfengine instalado, que poderá refazer a instalação do sistema automaticamente sempre que necessário. ■

Mais informações

[1] Cfengine: <http://www.cfengine.org/>

[2] Código-fonte do Cfengine: <http://www.cfengine.org/downloads/>

[3] Código-fonte do Apache: <http://httpd.apache.org/download.cgi/>



Segurança e Proteção de Rede



- ✓ Firewall
- ✓ Intrusion Prevention
- ✓ URL Filtering
- ✓ Antispam
- ✓ Anti-Vírus
- ✓ Anti-Spyware
- ✓ Branch Office VPN
- ✓ Mobile User VPN
- ✓ Zero Day Protection
- ✓ LiveSecurity® Service

Linha de Appliances			
Edge	Core	Peak	XTM 10
Até 50 usuários	Até 750 usuários	Até 2500 usuários	Até 5000 usuários

Facilidades

- Múltiplos Links de Internet (até 16)
- Load Balancing
- Drag-N-Drop VPN
- VPN Failover
- Traffic Shaping
- Qos
- VLANs
- Proxy Server
- 100% Interface Gráfica
- Server Load Balancing
- Suporte e Segurança à Voip
- Relatórios
- Servidores de Log
- Servidor de Quarentena
- Monitoramento "real time"
- Alta Disponibilidade
- Gerenciamento Centralizado
- Outras



Consulte os canais certificados
(Professional & Expert Partners)
+55 11 3393-3344
www.sodic.com.br/canais

Consulte políticas especiais:

- Trade-In to Trade-Up
- Alta Disponibilidade
- Licenças para 2 e 3 anos

Compre e Ganhe 12 meses de assinatura Linux Magazine

Gerenciamento de configurações e alterações com o Bcfg2

O gerente

O poderoso Bcfg2 oferece um ambiente sofisticado para gerenciamento de configuração centralizado.

por Marko Jung e Nils Magnus



Os especialistas no departamento de matemática e ciência da computação do Argonne National Laboratory [1] estavam tão descontentes por ter que configurar seus inúmeros computadores manualmente que começaram um projeto interno de pesquisa, chamado *Bcfg2* [2], que depois liberaram sob a licença BSD.

O Bcfg2 oferece um sistema sofisticado para descrever e instalar configurações clientes completas. Essa flexível ferramenta utiliza um formato XML abrangente para descrever as configurações e RPC para se comunicar com os clientes.

Os experientes acharão o Bcfg2 fácil de estender, mas a curva de aprendizado é íngreme – o programa utiliza uma abordagem poderosa e abstrata.

Plataformas

O Bcfg2 suporta várias plataformas, incluindo *openSUSE*, *Fedora*, *Gentoo* e *Debian*, assim como diversos derivados. A ferramenta também é compatível com FreeBSD, AIX, Solaris e Mac OS X com uso dos pacotes *Encap* independentes de distribuição [3] por cima dos pacotes de cliente e servidor prontos para o uso. Como alternativa, pode-se conferir o *openSUSE Build Service* [4], que oferece o pacote para várias outras plataformas.

Arquitetura

Para gerenciar especificações, o Bcfg2 usa um servidor que se comunica com uma contraparte bastante simples no cliente. Para instalar ambos os softwares, que englobam apenas algumas linhas de código em *Python*, é possível usar o gerenciador de pacotes da sua distribuição.

Para permitir que o cliente peça atualizações do servidor em intervalos regulares, é preciso criar uma entrada no Crontab. Outra possibilidade é executar o Bcfg2 como processo em segundo plano. Nesse caso, o servidor pode contactar o agente ativamente.

As configurações dos sistemas gerenciados são configuradas no servidor Bcfg2. Para cada cliente, o servidor armazena uma descrição que ele gera a partir de uma especificação central.

No nível mais alto, o Bcfg2 se baseia em perfis que descrevem classes de computadores idênticos, como sistemas desktop ou servidores web, por exemplo. Cada máquina gerenciada possui exatamente um perfil.

Áreas lógicas específicas do sistema dentro de um perfil são organizadas em grupos, tais como softwares para escritório ou configurações de rede. Os grupos, que podem ser aninhados recursivamente, permitem que os administradores organizem as

especificações de configuração de forma a conferir-lhes algum sentido.

Cada grupo, por sua vez, é composto por um número arbitrário de partes (chamados de *bundles*) com escopo que geralmente se estendem a um único produto de software, como Postfix, OpenOffice.org ou o mecanismo de *nameswitch*.

Perfis, grupos e bundles são definidos no arquivo `metadata/groups.xml` (veja o **exemplo 1**).

Criação de pacotes

Bundles podem ser subdivididos: o Bcfg2 agrupa os arquivos de configuração e pacotes de software que pertençam a um serviço específico do sistema num arquivo dentro do diretório `Bundler`. Por exemplo, `Bundler/motd.xml` define o bundle de configuração para a mensagem de boas vindas `/etc/motd`:

```
<Bundle name='motd' version='2.0'>
  <Package name='login' />
  <ConfigFile name='/etc/motd' />
</Bundle>
```

Alguns exemplos muito bem comentados de bundles estão disponíveis no wiki do projeto [5]. Os bundles contêm vários itens de configuração, denominados *entradas* (*entries*) pelo Bcfg2.

O sistema define seis tipos diferentes de entradas (veja a [tabela 1](#)): o tipo *ConfigFile* gerencia um arquivo e seu conteúdo; os tipos *Directory*, *Permission* e *SymLink* permitem que o administrador gerencie ou monitore objetos. Os tipos de entrada *Package* e *Service* são mais servidos no campo da inteligência artificial.

O Bcfg2 abstrai os métodos específicos de cada distribuição para, por exemplo, instalar um pacote num cliente; isto é, ele chamará o comando *aptitude* num sistema Debian e *rpm* ou *yum* num Fedora. O mesmo princípio se aplica a serviços de sistema que costumam estar listados em */etc/init.d*.

Instalação: servidor

A estrutura abstrata que descreve o cliente é gerenciada inteiramente no lado do servidor. Digitar *bcfg2-admin init* inicia a nova configuração.

Primeiramente, são pedidos os detalhes do caminho do repositório, um certificado SSL para comunicação segura com os clientes, e uma senha de acesso. O script de administração do Bcfg2 então procede à criação de vários arquivos e diretórios e popula o arquivo de configuração */etc/bcfg2.conf* com padrões que fazem sentido. Pode ser preciso modificar a entrada na seção *[components]* para que coincida com o nome da máquina,

Exemplo 1: Definições de bundle e subgrupo

```
01 <Groups>
02   <Group name='desktop' profile='true'>
03     <Bundle name='motd' />
04     <Bundle name='networking' />
05     <Group name='office-workstation' />
06     <Group name='debian-stable' />
07   </Group>
08
09   <Group name='webserver' profile='true'>
10     <Group name='apache' />
11     <Bundle name='networking' />
12     <!-- ... --!>
13   </Group>
14
15   <Group name='office-workstation'>
16     <Group name='gnome-desktop' />
17     <!-- ... --!>
18   </Group>
19
20   <Group name='debian-stable' toolset='debian' />
21 </Groups>
```

quina, o qual seus clientes podem resolver por DNS.

Esse nome também é a escolha perfeita para o *Common Name* (nome comum) quando for gerado o certificado. O *bcfg2-admin* talvez crie o arquivo com permissão de leitura por todos os usuários, mas é bom alterar isso por conter a senha de acesso ao cliente.

Além disso, a ferramenta configura um repositório de configuração vazio em */var/lib/bcfg2*. O comando */etc/init.d/bcfg2-server start* inicia o servidor.

Configuração do cliente

O único componente que é preciso instalar no cliente é o pacote cliente *bcfg2*. Além disso, é necessário salvar o arquivo de configuração em */etc/bcfg2.conf*.

O próximo passo é adicionar cada cliente Bcfg2 ao arquivo *Metadata/clients.xml* do servidor ([exemplo 2](#)). Todas as especificações usam o formato XML. O administrador depois pode atribuir perfis a máquinas por meio desse arquivo.

Tabela 1: Tipos de entradas de configuração

Nome	Descrição	Exemplo
Package	Nome do pacote de software	<code><Package name='bcfg2' /></code>
ConfigFile	Caminho absoluto do arquivo de configuração	<code><ConfigFile name='/etc/bcfg2.conf' /></code>
Service	Nome do script de inicialização (não do daemon respectivo)	<code><Service name='ntpd' /></code>
Directory	Caminho absoluto do diretório no sistema de arquivos	<code><Directory name='/var/tmp' /></code>
SymLink	Caminho absoluto do link simbólico	<code><SymLink name='/dev/MAKEDEV' /></code>
Permissions	Permissões do caminho absoluto	<code><Permissions name='/etc/passwords' /></code>

O Bcfg2 identifica os clientes por seus nomes DNS, o que torna importante a existência de um sistema DNS funcional. O exemplo atribui o perfil *desktop* às máquinas *alpha* e *beta.exemplo.com* e *webserver* a *gamma.exemplo.com*. O Bcfg2 já está pronto para a ação.

Vários estágios

O processo de atualização é composto por múltiplas etapas (veja a [figura 1](#)): primeiro o cliente obtém sua configuração em XML a partir do servidor, cria um inventário e compara os estados atual e desejado. Após completar todas as alterações associadas à atualização, o cliente novamente verifica os vetores e informa ao servidor o resultado. O servidor gera relatórios e estatísticas com base nas informações. Para verificar os relatórios, o administrador do sistema pode acionar uma atualização de teste. Para acionar uma atualização no lado cliente, digite:

```
bcfg2 -q -v -n
```

Esse comando inicia o processo de atualização de um modo não invasivo e sem necessidade de operador (opção *-n*). A opção *-q*, que significa *quick* (rápido), omite algumas verificações. A opção *-v* oferece mais informações. O [exemplo 3](#) exibe os resultados desse tipo de consulta.

Até agora, a especificação ainda está vazia. O Bcfg2 não exibe as entradas corretas ([linha 5](#)) nem incorretas ([linha 6](#)) porque o servidor não possui uma única entrada de configuração em seu repositório central ([linha 7](#)). O número de entradas não gerenciadas (*unmanaged entries*) na [linha 8](#) é mais interessante: o cliente Bcfg2 encontrou 242 objetos de configuração que o administrador não configurou explicitamente. O servidor tentará registrar e gerenciar esses objetos no futuro. Essas entradas são principalmente itens dos tipos *Service* e *Package* adicionados no lado cliente pela distribuição Linux. A [linha 2](#) dá mais informações sobre eles.

O Bcfg2 identificou automaticamente a distribuição como usuária do serviço *Chkconfig* para configurar

serviços de inicialização e do RPM para gerenciamento de pacotes. Um sistema Debian usaria o *update-rc.d* e o formato de pacotes *DEB*.

Como o comando *bcfg2* acabou de pedir uma atualização sem alterações, os detalhes nas [linhas 10 a 14](#) coincidem com os valores das linhas acima. Agora, fica a cargo do administrador do sistema visualizar as entradas não gerenciadas uma por uma e adicionar qualquer definição apropriada. A opção *-e* faz o sistema detalhar as entradas. Uma das principais forças do Bcfg2 é sua capacidade de completar gradativamente uma configuração incompleta.

O processo de atualização é o elemento central de qualquer sistema de gerenciamento de configurações, e é importante examinar esse processo mais detalhadamente. Ele compreende três fases.

Sondagem

Na fase inicial, o cliente se conecta ao servidor e realiza vários testes, conhecidos como sondas. Essas sondas têm a forma de curtos scripts de shell

Exemplo 2: Registro de clientes

```
01 <Clients>
02   <Client profile="desktop" name="alpha.exemplo.com" pingable="N"/>
03   <Client profile="desktop" name="beta.exemplo.com" pingable="Y"/>
04   <Client profile="webserver" name="gamma.exemplo.com" pingable="N"/>
05   <!-- .. --!>
06 </Clients>
```

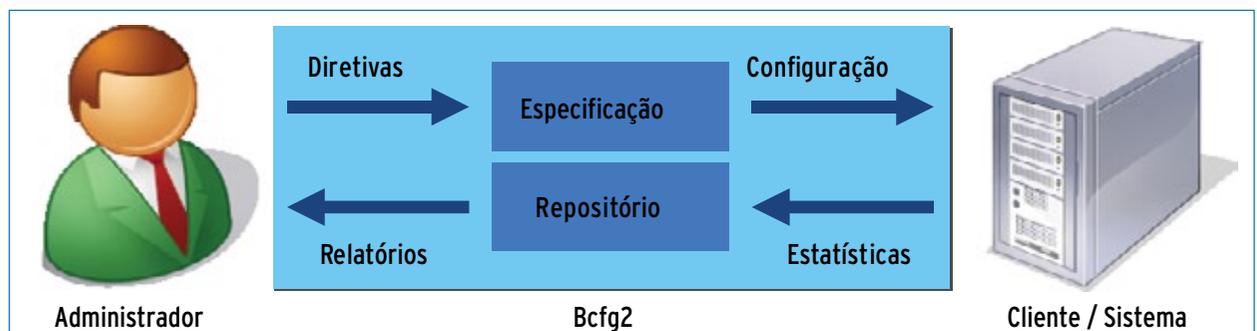


Figura 1 O administrador usa o Bcfg2 para criar uma especificação que define a configuração necessária do cliente. O Bcfg2 tenta efetuar as alterações e documenta o resultado.

que são executados no lado cliente. Dependendo do resultado, o servidor pode acrescentar grupos ou bundles à especificação do cliente. Um teste retornará simplesmente um resultado de `grupo:nome_do_grupo`.

O servidor atribui automaticamente o cliente a mais grupos. Isso significa que ele adicionará automaticamente, por exemplo, um bundle de modem caso descubra o `lspci` no cliente. Para mais exemplos e um Howto abrangente, confira o site do Bcfg2 [6].

Configuração

Na segunda fase, o cliente recebe do servidor a descrição da configuração. Essa descrição contém várias entradas de configuração dos seis tipos básicos. O cliente faz um inventário local para criar uma estrutura comparável e depois procede à comparação do inventário local com a descrição vinda do servidor. Em caso de discordâncias, o cliente realiza mudanças dependendo dos tipos de elementos de configuração correspondentes: o cliente Bcfg2 resolve as diferenças entre arquivos de configuração usando a versão definida no servidor.

Se não houver um serviço em execução, o cliente o iniciará. As dependências entre elementos de configuração são resolvidas automaticamente.

O cliente repete esse processo até que não seja mais possível realizar qualquer progresso – isto é, até o próximo processo de atualização não conseguir fazer alterações.

Relatórios

Na terceira e última fase, o cliente gera um relatório com o estado do sistema e outros detalhes, incluindo o número de entradas de configuração corretas e incorretas e o número de objetos do sistema não gerenciados.

O cliente envia essa mensagem ao servidor, que depois processa para criar páginas web, feeds RSS e emails.

O núcleo de qualquer sistema Bcfg2 é a especificação da configuração. Os administradores a utilizam para descrever as configurações desejadas dos sistemas gerenciados por eles. Esse processo é feito em dois estágios: o Bcfg2 se refere à estrutura verificada antes, assim como aos perfis, grupos e bundles que ela contém como metadados. Os metadados definem os elementos de que o Bcfg2 precisa configurar no cliente.

Quando um cliente envia uma requisição para um servidor, o servidor gera a configuração abstrata a partir dos metadados correspondentes (veja a figura 2). Esse modelo contém todas as entradas de configuração necessárias para o sistema de destino, mas sem qualquer conteúdo. Por exemplo, um elemento `ConfigFile` contém o nome do arquivo, mas não o conteúdo do arquivo.

Geradores

Depois que o servidor cria a plataforma de configuração, ele usa geradores para atribuir informações tangíveis a cada entrada. O Bcfg2 usa diversos geradores escritos em Python.

Exemplo 3: Servidor não configurado

```
01 Loaded tool drivers:
02 Chkconfig POSIX PostInstall
  ↳RPM
03
04 Phase: initial
05 Correct entries: 0
06 Incorrect entries: 0
07 Total managed entries: 0
08 Unmanaged entries: 242
09
10 Phase: final
11 Correct entries: 0
12 Incorrect entries: 0
13 Total managed entries: 0
14 Unmanaged entries: 242
```

O administrador precisa ativar os geradores no arquivo `/etc/bcfg2.conf`. Uma instalação típica usaria pelo menos:

```
generators = Cfg, Pkgmgr, Rules,
  ↳Tcheetah
```

Cada gerador registrado é capaz de instanciar vários elementos de configuração.

Nos casos simples, o gerador `Cfg` retorna um arquivo estático, e nos

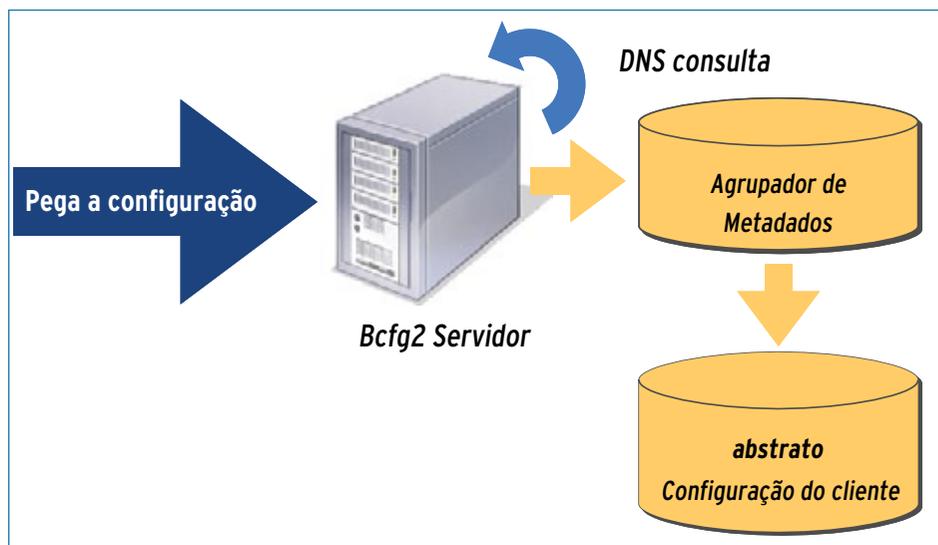


Figura 2 Durante a primeira etapa, o servidor Bcfg2 gera a configuração abstrata do cliente a partir dos metadados.

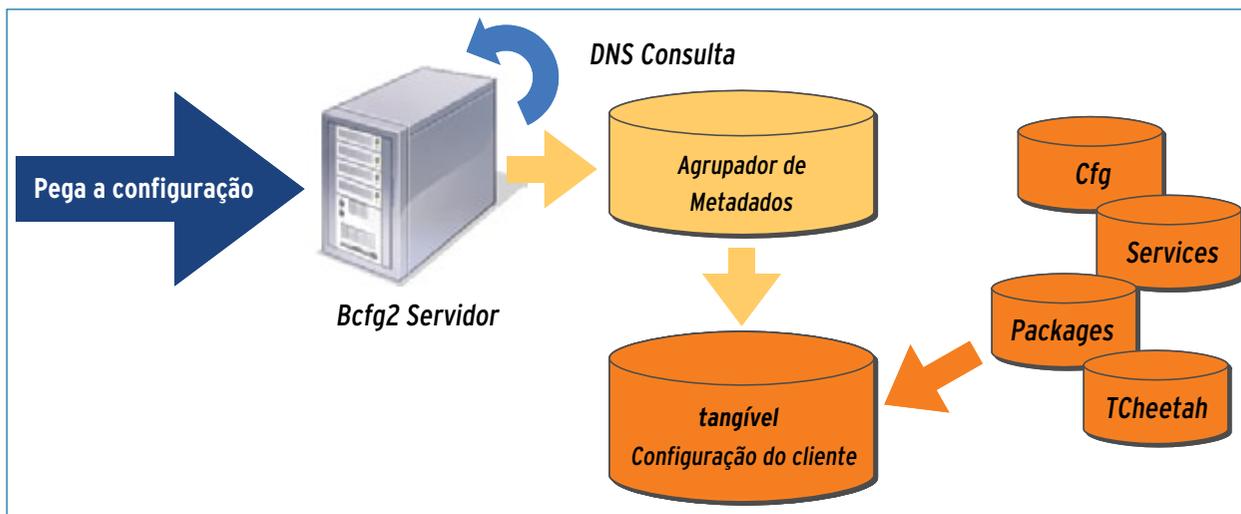


Figura 3 O Bcfg2 usa múltiplos geradores para preencher com conteúdo entradas de especificação abstrata. Esse processo cria informações completas a partir de bundles e metadados.

mais complexos, um gerador *TCheetah* usa um modelo e uma linguagem de script para obter o conteúdo do arquivo a partir de uma entrada do banco de dados. Outros geradores lidam com elementos de configuração como serviços e pacotes. Conseqüentemente, o Bcfg2 é capaz de usar quase qualquer fonte de dados para compilar uma configuração tangível (**figura 3**).

Cfg

O plugin *Cfg* tem como principal função gerar conteúdo para as entradas do tipo *ConfigFile*. Para configurar um elemento, o administrador cria um subdiretório sob *Cfg/* no repositório, com o mesmo nome que o bundle correspondente. Depois, ele cria um arquivo estático no diretório

e deixa o Bcfg2 distribuir o arquivo para todos os seus clientes.

Para definir os clientes de destino, é possível adicionar sufixos aos nomes dos arquivos. O sufixo *H_Hostname* distribui o arquivo apenas para as máquinas especificadas; *GPrio_Group* envia o arquivo para todos os sistemas que possuem o perfil de grupo especificado. Se uma máquina pertencer a múltiplos grupos, o Bcfg2 aplica o arquivo com a maior prioridade.

Um arquivo *:info* no mesmo diretório define as permissões, com entradas como:

```
owner: root
group: admin
perms: 0644
```

Para gerenciar grandes redes, os desenvolvedores do Bcfg2 criaram o gerador *TCheetah*, com base no modelo na linguagem *Cheetah* [7]. *Cheetah* suporta instruções que vão desde simples operações sobre textos, passando por controle de fluxo, até código Python embutido diretamente em arquivos de configuração.

O *TCheetah* adota a estrutura do diretório do gerador *Cfg*, com diretórios sob */var/lib/bcfg2/TCheetah* representando os elementos de configuração. Cada diretório contém um arquivo *info* com o mesmo conteúdo que o gerador *Cfg*, juntamente com uma configuração de *template* (modelo). O código em *Cheetah*, que pode conter algumas extensões específicas do Bcfg2, é adicionado em seguida. Ao colocar um arquivo com o conteúdo do **exemplo 4** em */var/lib/bcfg2/TCheetah/etc/motd/template*, é criada uma *message of the day* dinâmica. O gerador *TCheetah* substitui *\$self.metadata.hostname* pelos valores reais e depois executa o loop que começa com *#for*.

Conexões

Um banco de dados permite que se obtenha informações de configuração a partir de ainda mais fontes de dados. Por exemplo, podemos gerar

Exemplo 4: Script para motd automático

```
01 Bem-vindo a $self.metadata.hostname!
02
03 Este sistema é gerenciado pelo Bcfg2.
04 Ele é
05 membro dos seguintes grupos:
06 #for $group in $self.metadata.groups:
07 * $group
08 #end for
```

Além disso, é possível especificar valores como codificação do arquivo e comportamento para alterações locais. A funcionalidade oferecida pelo gerador *Cfg* ajuda a gerenciar a maior parte do sistema; entretanto, nem sempre oferece a flexibilidade necessária para gerenciar sistemas de grande escala.

Exemplo 5: Arquivo network/interfaces configurado com TCheetah

```
01 #from Bcfg2.Server.dbconnection import DBPgConnection
02 #silent result = DBPgConnection().execute(
03     "SELECT ip, netmask, broadcast, gateway \
04     FROM hosts \
05     WHERE hostname = '%s'" % $self.metadata.hostname)
06
07 auto eth0
08 iface eth0 inet static
09     address $result[0]
10     netmask $result[1]
11     broadcast $result[2]
12     gateway $result[3]
```

automaticamente os dados de configuração de DHCP, DNS e NIS a partir de uma origem como um serviço de diretórios. O **exemplo 5** mostra como o TCheetah no Debian configura as interfaces de rede em `/etc/network/interfaces` com base nos dados de um banco de dados PostgreSQL.

Serviços

As configurações não se aplicam apenas a entradas de arquivos. Nomes de serviços precisam ser configurados de forma a refletir os *runlevels*. O gerador Service lê as informações administrativas contidas em `Svcmgms/services.xml` para descobrir como configurar, digamos, o serviço NTP.

Para isso, o servidor faz referências ao serviço citado como `<service name='ntpd' />` no bundle correspondente.

Em seguida, `services.xml` é usado para especificar se o cliente deve ou não iniciar o serviço:

```
<Services priority='0'>
  <Service name='ntpd'
  ▶status='on' />
</Services>
```

O gerador converte esses detalhes para configurações tangíveis e envia-as para o cliente, que em

seguida aplica métodos específicos para cada distribuição para ativar ou desativar o serviço.

Pacotes

O Bcfg2 não substitui o gerenciador de pacotes, mas pode contribuir para mover o trabalho do gerenciador de pacotes para o administrador do sistema, que pode usar o Bcfg2 a fim de especificar qual versão de quais pacotes individuais a ferramenta instala. Arquivos XML gerenciam informações sobre os pacotes disponíveis e sincronizam os detalhes com a seleção de pacotes do servidor de instalação. Múltiplos servidores de instalação permitem que os administradores atribuam prioridades diferentes – por exemplo, para atualizações de segurança.

O cliente do Bcfg2 compara as versões local e global do pacote e atualiza ou “atrasa” os pacotes de acordo. Os administradores podem “congelar” versões específicas atribuindo-lhes a maior prioridade possível.

Outros geradores configuram diretórios, links simbólicos e diversos outros tipos de elementos. Alguns administradores mais experientes apreciarão a possibilidade de usar plugins para vincular funções em Python aos geradores fornecidos pela distribuição do Bcfg2.

Documentação iminente

A comunidade muito ativa de desenvolvedores que circunda o Bcfg2 integra novos designs ao sistema quase toda semana. Recentemente foi criada uma nova equipe com foco em melhorar a documentação [8]. A documentação é absolutamente vital, pois o Bcfg2 exige que se saiba tantos detalhes do sistema.

Os administradores também apreciarão o suporte da ferramenta à migração gradativa, que elimina a necessidade de mudanças drásticas e permite a especificação da configuração passo a passo. Com tudo isso, o uso do Bcfg2 para configurar e validar clientes é uma ferramenta muito poderosa para qualquer pessoa que consiga lidar com seu alto nível de abstração. ■

Mais informações

- [1] Argonne National Laboratory: <http://www-new.mcs.anl.gov/new>
- [2] Bcfg2: <http://www.bcfg2.org>
- [3] Pacotes Encap do Bcfg2: <http://trac.mcs.anl.gov/projects/bcfg2/wiki/EncapPackages>
- [4] Pacotes do Bcfg2 no openSUSE Build Service: <http://download.opensuse.org/repositories/home:/markojung:/bcfg2>
- [5] Exemplos anotados do Bcfg2: <http://www.bcfg2.org/wiki/AnnotatedExamples>
- [6] Sondas do Bcfg2: <http://trac.mcs.anl.gov/projects/bcfg2/wiki/Probes>
- [7] Mecanismo de modelos de Cheetah: <http://www.cheetahtemplate.org>
- [8] Lista do Bcfg2: bcfg-dev@mcs.anl.gov

Monitoramento de rede com o Zenoss

O observador

Veja como essa ferramenta boa, bonita, livre e gratuita pode ajudar no monitoramento de rede.
por David Nalley



Com uma interface web conveniente e um design flexível, a ferramenta de monitoramento Zenoss está ganhando adeptos em todo o mundo. O Zenoss possui uma lista impressionante de recursos que parece crescer a cada mês. Ele também se sai bem como monitor de status e até oferece suporte a plugins do todo-poderoso Nagios. O sistema

Zenoss também é competente para monitoramento de desempenho e geração de gráficos (figura 1). A ferramenta traz uma grande variedade de configurações para vários tipos de dispositivos, como computadores Linux, switches, roteadores e até máquinas Windows. E também é fácil instalar novos recursos. Na grande tradição dos ambientes *nix, o Zenoss

foi projetado com uma arquitetura modular. Para adicionar novas funcionalidades, basta plugar um novo módulo (um *ZenPack*, no linguajar dos mestres do Zenoss).



Figura 1 Os gráficos de desempenho do Zenoss ajudam a analisar tendências e a projetar necessidades futuras.

Servidor syslog

Uma função especialmente útil do Zenoss é seu servidor *syslog*. O Zenoss recebe a saída padrão do *syslog* e, além de agir como um servidor comum (isto é, verificar o estado da máquina e monitorar seu desempenho), ele ainda exibe informações, que geralmente é a melhor forma de detectar causas e efeitos. As máquinas Windows não ficam de fora dos logs, pois o Zenoss trata eventos desse sistema via WMI (*Windows Management Instrumentation*).

Protocolos

O Zenoss suporta tecnologias de monitoramento e gerenciamento como SNMP, WMI, ping, varreduras de portas e monitoramento baseado em SSH.

device	eventClass	summary	firstTime	lastTime	count
marc-irlandezs-cor	/Status/Ping	marc-irlandezs-computer.local ip 192.168.1.103 is down	2007/05/15 17:47:24.000	2007/05/16 15:53:05.000	1319
ConfPrinter	/Status/Ping	ConfPrinter ip 192.168.1.102 is down	2007/05/16 13:13:16.000	2007/05/16 15:53:02.000	154
centos-5-test3	/Status/Ping	centos-5-test3 ip 192.168.1.75 is down	2007/05/15 14:24:06.000	2007/05/16 15:46:38.000	1447
centos-5-test1	/Status/Ping	centos-5-test1 ip 192.168.1.73 is down	2007/05/15 14:24:06.000	2007/05/16 15:46:35.000	1447
train2	/Status/Ping	train2 ip 192.168.1.68 is down	2007/05/15 14:24:06.000	2007/05/16 15:46:32.000	1447
esx-cent44.zenoss	/Status/Ping	esx-cent44.zenoss.loc ip 192.168.1.66 is down	2007/05/11 17:42:14.000	2007/05/16 15:46:29.000	1726
WIN2K-TEST3	/Status/Ping	WIN2K-TEST3 ip 192.168.1.79 is down	2007/05/15 14:24:03.000	2007/05/16 15:46:26.000	1447
WIN2K-TEST2	/Status/Ping	WIN2K-TEST2 ip 192.168.1.78 is down	2007/05/15 14:24:03.000	2007/05/16 15:46:23.000	1447
WIN2K-TEST1	/Status/Ping	WIN2K-TEST1 ip 192.168.1.77 is down	2007/05/15 14:24:00.000	2007/05/16 15:46:20.000	1447
ubuntu610.zenoss	/Status/Ping	ubuntu610.zenoss.loc ip 192.168.1.203 is down	2007/05/11 14:50:27.000	2007/05/16 15:46:17.000	1737
rpath10x.zenoss.k	/Status/Ping	rpath10x.zenoss.loc ip 192.168.1.25 is down	2007/05/11 14:50:27.000	2007/05/16 15:46:14.000	1737
rhel43.zenoss.loc	/Status/Ping	rhel43.zenoss.loc ip 192.168.1.201 is down	2007/05/11 14:50:27.000	2007/05/16 15:46:11.000	1737

Figura 2 O console de Eventos oferece uma visão dos eventos de monitoramento.

O SNMP é o padrão para obtenção de informações de rede, e virtualmente todos os dispositivos de computação e de rede o suportam.

Com dispositivos que não o utilizam e não oferecem suporte a WMI, ou que estejam além do acesso de ferramentas convencionais de monitoramento, é possível realizar testes de rede limitados com o monitoramento baseado em ping ou varreduras de porta.

O monitoramento por SSH permite que o Zenoss se conecte a uma máquina e execute comandos para determinar o estado desta.

Interfaces

O Zenoss oferece várias avenidas para as informações de rede. A primeira opção é a interface de rede. A visão mais útil do que está ocorrendo na rede é o *Event Console* (console de eventos, [figura 2](#)), que oferece uma interface para visualizar e configurar eventos de monitoramento.

Entretanto, a maioria dos administradores provavelmente não ficará de olho no console o tempo todo. Felizmente, o Zenoss é capaz de enviar alertas por SMS e email. O que é realmente fabuloso é a granularidade que pode ser aplicada aos alertas. Por exemplo, um administrador de email precisa saber de problemas do servidor de email a qualquer momento, mas outros problemas da rede só devem chegar a seu conhecimento nos dias úteis. O Zenoss facilita e agiliza a configuração de vários tipos de alertas para uma grande variedade de eventos diferentes.

Outra ferramenta do Zenoss para visualizar dados de rede é um *applet* para o desktop chamado *Zapplet*, que fornece informações sobre status e eventos na bandeja do sistema. O Zapplet precisa apenas da *Gtk2*.

Instalação

Para configurar o Zenoss, use um instalador ou pacotes para a sua distribuição. O programa também está

disponível sob a forma de appliance virtual para VMware.

O instalador inclui dependências como o *MySQL* e apresenta uma agradável interface gráfica que pede as informações necessárias; porém, o instalador não oferece alguns dos importantes benefícios de um sistema de gerenciamento de pacotes.

A maioria das instalações do Zenoss ocorrem em sistemas *Red Hat Enterprise Linux 5* ou *CentOS 5*. Portanto, a forma ideal de instalação é por meio dos pacotes RPM.

O site do Zenoss [\[1\]](#) contém a versão mais recente para download. Após baixar e instalar o RPM e suas dependências, basta adicionar o serviço do *MySQL* à inicialização do sistema e em seguida iniciá-lo:

```
/etc/init.d/mysql start
```

Como o Zenoss precisa comunicar-se com outros servidores, serão necessárias as seguintes portas:

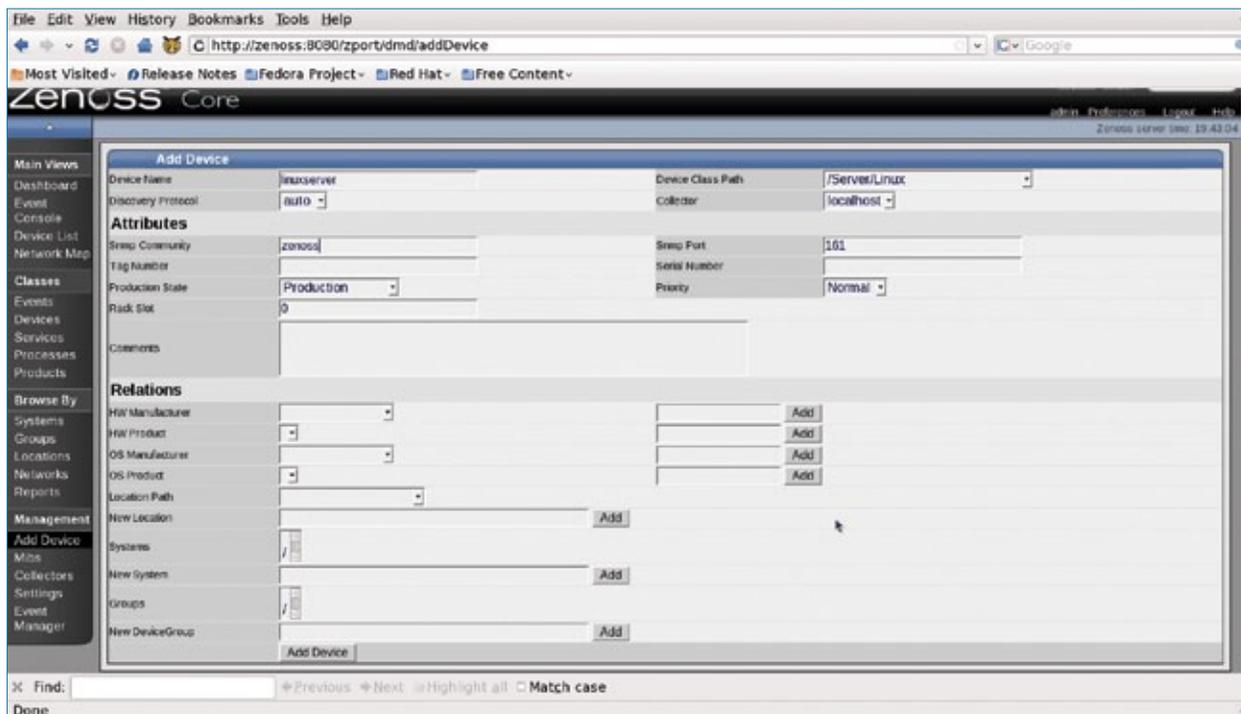


Figura 3 Use a página *Add Device* para informar o Zenoss sobre um dispositivo.

- ◆ 8080 TCP – interface web
- ◆ 162 UDP – trap SNMP
- ◆ 514 UDP – Syslog

Execução

Executar o Zenoss inicializa o banco de dados. Mas atenção: o programa presume que a senha do usuário root do MySQL seja vazia e que o banco de dados esteja rodando na mesma máquina. Se não for o caso, é preciso editar o arquivo `/opt/zenoss/bin/zenoss_init_pre`.

Ter o banco de dados na mesma máquina que o sistema de monitoramento é um pouco controverso. Especialistas geralmente recomendam ter o banco de dados numa máquina dedicada. Porém, com um sistema de monitoramento que armazena eventos no banco de dados, colocar o banco num sistema separado introduz mais um ponto de falha.

Para inicializar o banco e executar o Zenoss, basta iniciar seu serviço:

```
/etc/init.d/zenoss start
```

Para se conectar à interface web, aponte o navegador para `http://<ip_do_servidor>:8080`. O usuário padrão é `adin` e a senha é `zenoss`.

Monitoramento

Antes de começar o monitoramento com o Zenoss, é preciso garantir que o `snmpd` esteja instalado no sistema:

```
# yum -y install net-snmp
```

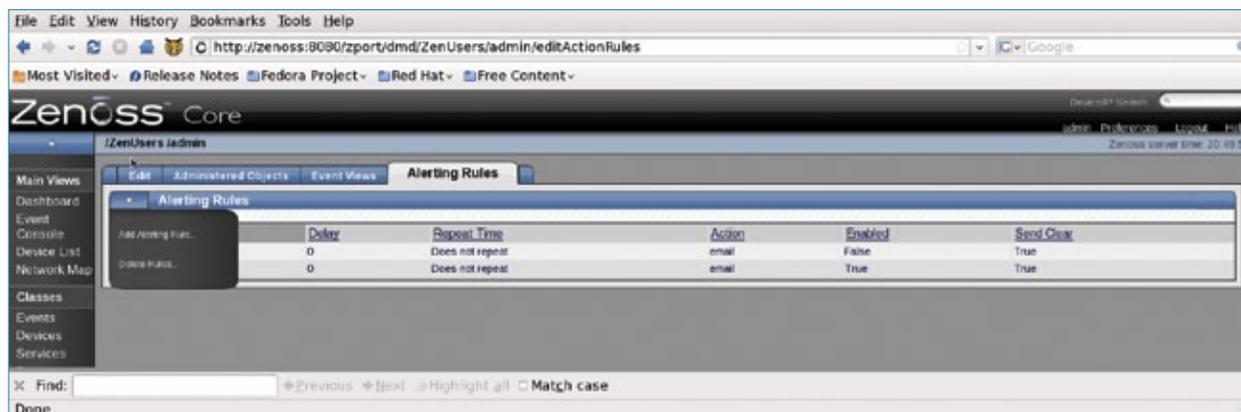


Figura 4 Aba de regras de alerta.

Quadro 1: Monitoramento de clientes Windows

Monitorar uma máquina Windows também exige certas providências do lado cliente. Para começar, é preciso instalar o serviço SNMP selecionando *Iniciar | Painel de Controle | Adicionar/Remover Programas | Componentes do Windows | SNMP*.

Infelizmente, o SNMP do Windows é muito limitado. A Zenoss recomenda usar o gratuito *SNMP Informant* em vez dele.

Além disso, é preciso configurar o daemon SNMP. Para tanto, clique com o botão direito em *Meu Computador* e selecione *Gerenciar*. Depois, selecione *Serviços, Serviço SNMP* e, com um clique direito, selecione *Propriedades* e a aba *Segurança*. Adicione o nome de comunidade escolhido e defina-o como somente-leitura.

Para configurar qual serviço aceita pacotes SNMP de máquinas específicas, adicione uma entrada para o servidor Zenoss. Agora inicie o serviço e faça-o iniciar automaticamente com o sistema. Além disso, é preciso abrir

a porta UDP 161 para que o Zenoss consiga conectar-se ao daemon.

Dentro da interface web, clique em *Add Device* (Adicionar Dispositivo), digite o IP ou nome da máquina, escolha a classe */Server/Windows* e especifique o nome adequado da comunidade. A coleta de dados começa ao se clicar em *Add Device*.

Como o Zenoss também é capaz de monitorar via WMI, deve-se fornecer credenciais do Windows para permitir a coleta: clique em *Devices/Servers/Windows*, escolha a aba *zProperties* e digite os dados nos campos *zUsername* e *zWinpassword*. Lembre-se de inserir no início desses dados o nome do domínio, caso esteja informando credenciais de domínio. Digitar o domínio no nível do servidor Windows significa que todas as máquinas Windows usarão essas credenciais. Se for necessária uma configuração única para uma máquina, é possível clicar na aba *zProperties* desse dispositivo e alterar apenas a sua configuração.

Para criar um arquivo de configuração mínimo, digite o comando:

```
# echo 'rocommunity zenoss
-><endereço_IP>' > /etc/snmp/snmpd
```

Essa linha permite que o IP do Zenoss se conecte ao *daemon* SNMP do servidor Linux, usando o nome de comunidade somente-leitura *zenoss*.

Em seguida, é preciso abrir a porta 161 UDP na máquina que se deseja monitorar. Por último, precisamos iniciar o daemon SNMP e ativar sua execução na inicialização:

```
# /etc/init.d/snmpd start
# chkconfig snmpd on
```

Na interface web do Zenoss, clique em *Add device* no canto inferior esquerdo (**figura 3**) e digite pelo menos o seguinte:

- ▶ o endereço IP ou nome da máquina que deve ser monitorada;
- ▶ a classe da máquina que deve ser monitorada (*/Server/Linux*, no caso);
- ▶ o nome da comunidade SNMP (*zenoss*, no caso).

Clique no botão *Add Device* para começar a coletar dados. Embora o SNMP seja o protocolo de monitoramento preferido para o Zenoss, é possível alterá-lo na página *Add Devices*. Note que definir a classe de dispositivo é crucial. O Zenoss define o que será monitorado com base na classe do dispositivo.

Alguns eventos de monitoramento talvez já estejam definidos no *Event Console* (console de eventos) – por exemplo, para alertar o administrador sobre configurações erradas. Para visualizar a lista de eventos, clique no link *Event Console* no canto superior esquerdo. Para adicionar alertas para outros eventos, clique no link *Settings* em *Management* no menu esquerdo, depois escolha a aba *Users*. Selecione um usuário e clique na aba *Alerting Rules* (regras de alertas, **figura 4**). No menu de *Alerting Rules*, escolha *Add Rule* (adicionar regra) e forneça um nome para a regra. Depois de clicar em OK, clique na regra que especifica como e para onde as mensagens serão enviadas, se haverá alguma espera para isso e quais critérios serão usados para determinar quais

mensagens enviar. Uma única regra pode tratar um grande número de alertas, enquanto alertas mais granulares talvez precisem de múltiplas regras.

Core e Enterprise

Muitas empresas de Código Aberto oferecem versões comerciais que oferecem funcionalidades substancialmente diferentes. No caso do Zenoss, no entanto, a principal diferença entre as versões Enterprise e Zenoss Core (a comunitária) é que a Enterprise traz algumas configurações já feitas. Por exemplo, um dos ZenPacks incluídos na Enterprise é um pacote de monitoramento do Exchange. A Zenoss sabe claramente que verdadeiros clientes corporativos pagam por suporte, então fornecer uma configuração mais rápida na versão Enterprise minimiza seu uso de recursos internos. ■

Mais informações

[1] Download do Zenoss:
<http://zenoss.com/download>

Implantando sistemas Debian com o FAI

Turbilhão!

O FAI auxilia na automatização do processo de instalar e configurar novos sistemas Debian.

por Steffen Bornemann e Christoph Karg

A plataforma FAI (acrônimo do inglês para *Fully Automatic Installation*, simplesmente “instalação totalmente automática” em português), desenvolvida na Universidade de Colônia, na Alemanha, é um analgésico para a dor de cabeça que advém da necessidade de instalar sistemas Debian em massa. A ferramenta oferece vários recursos de customização e permite a configuração de sistemas virtuais. A nova versão 3.2.9 [1] tem suporte para o Debian Lenny e inclui uma nova ferramenta de particionamento.

Como funciona

O FAI gerencia o processo de instalação automatizando os passos executados pelo instalador padrão do Debian. Como mostra a **figura 1**, um servidor FAI executa o serviço e hospeda os serviços necessários à instalação via rede, incluindo NFS, TFTP e DHCP. No cenário mais simples, um cliente dotado de uma placa de rede capaz de realizar um *boot* remoto via PXE (acrônimo do inglês *Preboot eXecution Environment*, ou “ambiente de execução pré-ini-

cialização) é inicializado, obtém um endereço IP do servidor DHCP e os arquivos necessários via TFTP para iniciar a instalação remota.

O FAI também trabalha com computadores mais antigos, sem suporte a PXE. Neste caso, é necessário iniciar a instalação manualmente a partir de uma imagem de inicialização armazenada em um disquete, CD-ROM ou pendrive USB. Independentemente de o sistema utilizado estar usando PXE ou não, a rotina de inicialização irá carregar um kernel inicializável. A máquina cliente vai entrar em contato com o servidor FAI e usar NFS para montar seus diretórios raiz e de configuração. Esses diretórios contêm toda a informação necessária para instalar o sistema na máquina cliente.

O FAI permite a definição de classes de computadores com a mesma localização e função. A definição de classes associa scripts, configurações e um conjunto customizado de pacotes aplicativos ao cliente. Como veremos mais adiante neste artigo, uma máquina cliente pode pertencer a mais de uma classe.

Um script de inicialização começa a instalação local. Esse script investiga o nome da máquina e os dados de configuração montados, para decidir a que classe de instalação um determinado cliente pertence. O processo de instalação formata o disco rígido da máquina cliente e baixa os pacotes necessários de um repositório espelhado do projeto Debian, antes de realizar a instalação propriamente dita dos pacotes usando o *Apt*. Por fim, o cliente é customizado de acordo com as especificações fornecidas via FAI.

Instalação do servidor

O servidor FAI dispõe de vários componentes. A **figura 2** ilustra os passos da instalação. O primeiro deles consiste na configuração do serviço responsável por distribuir a configuração. Para que isso funcione, vamos precisar de uma máquina Debian equipada com NFS, TFTP e DHCP. Além disso, recomendamos a instalação dos pacotes do FAI: *fai-server*, *fai-doc*, *fai-quickstart* e *fai-nfsroot*. Esses pacotes estão disponíveis nos repositórios padrão do Debian.

O pacote `fai-server` é o ponto inicial para a instalação do servidor. A lista de dependências desse pacote inclui os pacotes dos servidores NFS, DHCP e TFTP. Não devemos esquecer também do comando `fai-setup` para realizar a configuração do servidor central.

O comando `make-fai-bootfloppy` cria uma mídia de inicialização, tal como CD-ROMs ou disquetes para hardware sem suporte a PXE. O comando `fai-client` fornece os programas executados pela máquina cliente durante a instalação.

O aplicativo `fai-quickstart` instala todas as ferramentas necessárias a uma instalação do FAI e copia os arquivos de configuração padrão nos diretórios corretos. Ele instala todos os pacotes necessários e cria modelos de configuração no diretório `/etc/fai`. A menos que o NFS esteja sendo usado para montar um repositório Debian, não será necessário modificar os parâmetros do arquivo `fai.conf`, responsável pela definição das configurações centrais do servidor FAI.

O arquivo `make-fai-nfs-root.conf` instrui o FAI sobre como configurar o diretório raiz do NFS. Se o servidor FAI não tiver um nome alocado em um servidor DNS, será necessário ativar a linha `NFSROOT_ETC_HOSTS`, retirando o caractere de comentário dessa linha. Esse arquivo já tem endereços IP e nomes padrão, que podem ser alterados para fins de compatibilidade com os dados de outros ambientes de rede. Também é necessário especificar o servidor espelho do projeto Debian, a partir do qual os pacotes serão obtidos para criar o diretório raiz do NFS.

Usando padrões Debian

O FAI usa o sistema `Apt` padrão do Debian, que lista seus repositórios em `/etc/apt/sources.list`. O FAI inclui os servidores espelho padrão

Exemplo 1: Configuração do DHCP

```
01 group {
02   allow booting;
03   next-server 192.168.0.100;
04   filename "pxelinux.0";
05   option root-path "/srv/fai/nfsroot";
06   host demohost {
07     hardware ethernet 00:e0:81:5c:aa:82;
08     fixed-address 192.168.1.25;
09   }
10 }
```

da distribuição e o servidor espelho da Universidade de Colônia nessa lista. Se quisermos utilizar um outro conjunto de servidores espelho, é necessário modificar esse arquivo de configuração. Para evitar complicações desnecessárias, vamos deixar o FAI criar o diretório raiz do NFS com a mesma versão do Debian que será utilizada para as máquinas cliente. Após configurar corretamente todos esses parâmetros, o próximo passo é criar o diretório NFS raiz propriamente dito. Para fazê-lo, vamos executar o comando `fai-setup -v`. Após baixar cerca de 330 MB de dados de pacotes, o diretório `/srv/fai/nfsroot/live/fi-`

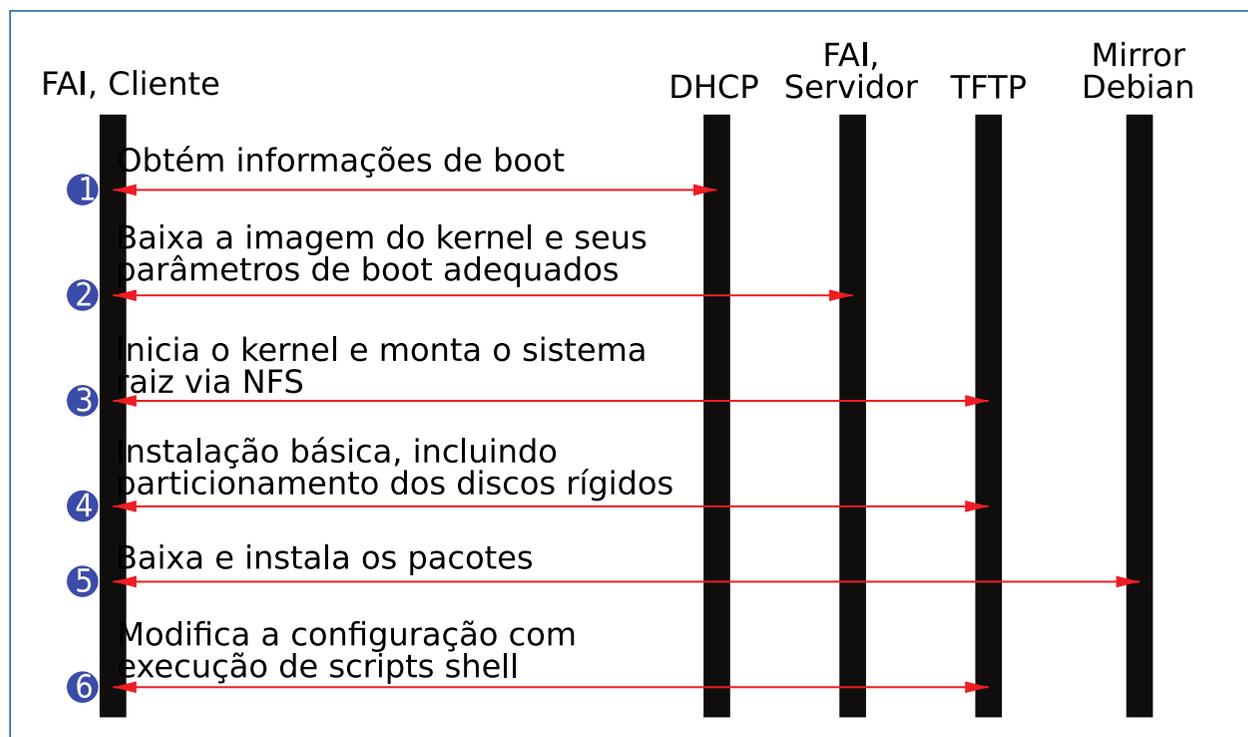


Figura 1 O FAI passa por diversas fases para instalar um sistema Debian.

`lesystem.dir` vai conter o diretório raiz do NFS. Esse script também exporta os diretórios necessários para a instalação dos clientes no NFS e copia uma imagem de kernel inicializável para o diretório `/srv/tftp`.

Testes iniciais

Para testar o servidor, vamos experimentar fazer a instalação em apenas uma máquina cliente. Pode-se utilizar a classe de pacote pré-definida

`DEMOHOST` para essa finalidade. Ela contém um sistema minimalista com requisitos de hardware fáceis de encontrar: um PC padrão com no mínimo 500 MB de espaço em disco e uma placa de rede com suporte a PXE.

Todos os serviços de rede necessários, tais como o servidor DNS e NFS, devem estar instalados no servidor FAI a essa altura. Para ajudar os clientes a serem inicializados, vamos configurar o arquivo `/etc/dhcp3/dhcpd.conf` do servidor DHCP de maneira similar à mostrada no **exemplo 1**. Em seguida, vamos designar um endereço IP e um nome de domínio ao endereço MAC da placa de rede e especificar a imagem TFTP de inicialização da máquina cliente.

O endereço IP do cliente precisa estar em notação hexadecimal: `CoA80119` para o endereço `192.168.1.25`, no nosso exemplo. Vamos criar então o arquivo `/srv/tftp/fai/pxelinux.cfg/COA80119` com o conteúdo indicado no **exemplo 2**. A configuração padrão vai controlar o comportamento da inicialização da máquina cliente. É melhor começar escolhendo `fai-generated`. Também é uma boa ideia usar o comando `fai-chboot -IFv demohost` para criar o arquivo. Isso vai incluir automaticamente os valores correntes. Após iniciar a máquina

cliente, o FAI assume o comando e instala um sistema Debian básico sem interface gráfica. Após a instalação ser finalizada, pode-se modificar o comportamento do `boot` de `fai-generated` para `uf-localboot` e reiniciar a máquina cliente, que está pronta para funcionar.

Além dos servidores espelho oficiais do projeto Debian, o FAI também trabalha como servidores espelho locais. Se houver um grande número de máquinas cliente locais que precisam ser instaladas com regularidade, é mais prático ter um servidor espelho próprio, já que isso evita o download de pacotes todas as vezes usando a conexão à Internet. Ademais, uma instalação local via Ethernet ou Gigabit Ethernet consome muito menos tempo.

Um outro benefício é a possibilidade de congelar o conteúdo do servidor espelho local, o que torna uma instalação local independente do estado corrente do repositório, além de garantir que todos os clientes tenham sempre versões idênticas dos aplicativos, independentemente de quando eles forem instalados. Adicionalmente, é possível incluir no servidor espelho local um repositório para pacotes customizados, que atendam à necessidade do seu ambiente operacional ou departamento de TI.

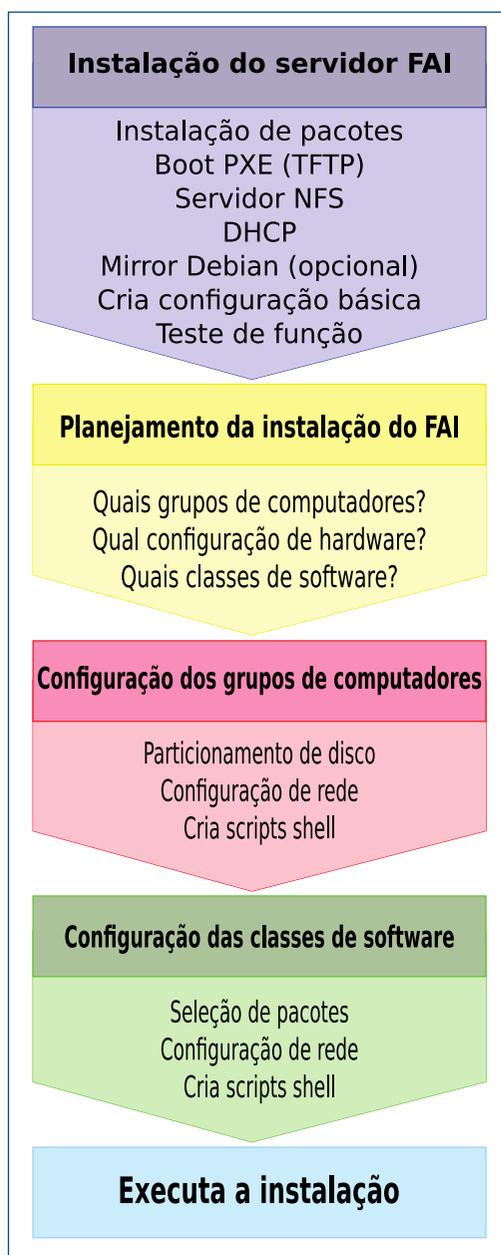


Figura 2 Uma instalação através do FAI requer planejamento cuidadoso.

Exemplo 2: Configuração do TFTP

```
01 # Seleciona comportamento de inicialização
02 # (favor retirar caractere de comentário de uma das duas
    ↳linhas abaixo)
03 default fai-generated
04 # default localboot
05
06 # Inicialização pela rede e do FAI
07 label fai-generated
08 kernel vmlinuz-2.6.25-2-486
09 append initrd=initrd.img-2.6.25-2-486 ip=dhcp \
10     root=/dev/nfs nfsroot=/srv/fai/nfsroot boot=live \
11     FAI_FLAGS=verbose,sshd,createvt
12 ACTION=install
13
14 # Inicialização a partir do disco-rígido
15 label localboot
16 localboot 0
```

Após instalar o cliente de testes *demohost* para testar os recursos do FAI, podemos começar a planejar a instalação em mais máquinas cliente. É importante seguir a divisa do FAI: “Planeje a instalação e o FAI instalará os seus planos”.

Trabalhando com classes

As classes do FAI fornecem um meio versátil de designar pacotes e configurações para sistemas cliente. Por exemplo, no departamento de Ciência da Computação da Universidade de Aalen, na Alemanha, os computadores são organizados em grupos e laboratórios, com máquinas idênticas disponíveis em diversas salas. Alguns laboratórios possuem computadores com arquiteturas diferentes, de modo que um kernel separado com drivers específicos para cada hardware são necessários para cada tipo de computador.

A configuração é baseada em uma classe comum para cada sala e uma classe para cada tipo de computador. Como o FAI também é utilizado para instalar máquina VMware, é necessária uma classe separada para máquinas virtuais. Em algumas salas com uma grande variedade de arquiteturas de computador, os administradores de sistemas usam uma combinação das classes de salas e computadores.

Conjuntos comuns de aplicativos podem definir categorias diferentes de classes de software – por exemplo uma classe básica (BC), uma classe de serviços (SC) e uma classe de programas (PC). A classe básica inclui o sistema Debian básico, além de programas, arquivos de configuração e scripts que são válidos para todos os grupos de máquinas e laboratórios. As classes básicas para a interface gráfica dos clientes são *BC_X11*, *BC_KDE* e *BC_GNOME*. Uma classe de serviço contém a informação necessária para preparar um cliente para um

Exemplo 3: Estrutura do 50-host-classes

```
01 #!/bin/bash
02 # Designa hosts de classes
03 case $HOSTNAME in
04     # LO.24 - CC_SUN (Classe de computador _ sun)
05     L024-*)
06         echo "BC_LINUX CC_SUN BC_X11 BC_KDE BC_BASE RC_L024
07     SC_LDAP" ;;
08     # Classe GNU/Linux Debian VMware: CC_VMWARE
09     vmware-1|vmware-2)
10         echo "BC_LINUX CC_VMWARE SC_LDAP" ;;
11     # Classe padrão
12     *)
13         echo "BC_LINUX" ;;
14 esac
15 (ifclass I386 || ifclass AMD64) && echo GRUB
16 exit 0
```

serviço específico. Por exemplo, a classe *SC_LDAP* contém todos os pacotes e dados de configuração necessários ao acesso ao serviço de diretório LDAP da própria faculdade.

Muitos projetos de estudantes requerem a instalação de programas em um grupo de computadores. Uma abordagem para lidar com isso

é definir uma classe separada de programas para cada um dos projetos.

Classes podem definir também a configuração de sistemas comuns. Por exemplo, pode-se desabilitar o mecanismo de travamento da tela do KDE em todos os computadores de um grupo. Essas configurações são tipicamente suportadas por uma li-

Exemplo 4: Parâmetros do BC_LINUX.var

```
01 # Permite repositórios não assinados
02 FAI_ALLOW_UNSIGNED=1
03
04 # Mapa de teclado brasileiro
05 FAI_KEYMAP=br-abnt2
06
07 # UTC=sim, caso o relógio do sistema esteja configurado para UTC
08 UTC=yes
09 # TIMEZONE=America/Sao Paulo
10 time_zone=America/Sao Paulo
11
12 # Chamar "openssl passwd -1" para criar a senha de root
13 # para o sistema novo; formatos suportados são md5 e crypt:
14 rootpw='$1$865YxXk$zRxd/ WUBLPU4gZfVmi1ax1'
15 servicepw='$1$arm/ uRPR$5w0Q7Z3i2cRSq1t0q/zyK/'
```

Exemplo 5: Configuração de pacotes em BC_LINUX

```
01 # Pacotes para todos os sistemas
02 PACKAGES aptitude
03 alsa-base
04 alsa-utils
05 discover
06 ...
07
08 PACKAGES aptitude BC_KDE
09 mozilla-firefox-locale-pt-br
10 thunderbird-locale-pt-br
```

Quadro 1: Outras ferramentas de instalação

Os programas `setup_harddisks` e `setup-storage` particionam o disco rígido. Esses pacotes incluem também os comandos `fcopy` e `ftar`, que copiam arquivos para o cliente independentemente de sua classe. O pacote `fai-doc` inclui a documentação sobre o FAI e alguns modelos de configurações. Após instalar o pacote, os arquivos podem ser encontrados no diretório `/usr/share/doc/fai-doc`.

O pacote `fai-nfsroot` não foi desenvolvido para ser instalado em computadores comuns. Em vez disso, o procedimento de configuração do FAI baixa esse pacote do servidor espelho durante a configuração do servidor, colocando o seu conteúdo dentro do diretório `/srv/fai/nfsroot/`. A partir daí, o cliente usa o NFS para montar o esse diretório como seu diretório raiz.

na em um arquivo de configuração existente ou por um script que altera essa linha. Caso configurações desse tipo sejam necessárias, é possível adicionar uma outra classe às máquinas.

A designação de programas a classes próprias facilita o trabalho de habilitá-los ou desativá-los. Dito isso, é melhor não definir muitas classes de programas, sob risco de se perder a visibilidade sobre elas. A **tabela 1** mostra uma visão geral das classes definidas, fornecendo exemplos.

O diretório de configuração `/srv/fai/config` e seus subdiretórios contêm a informação que o FAI necessita para instalar um cliente. Cada subdiretório tem uma tarefa diferen-

te. O subdiretório `class/` contém os arquivos e scripts que definem as classes e variáveis individualmente, tais como `50-host-classes`, na qual o administrador armazena as classes designadas a cada grupo de clientes.

O **exemplo 3** é um exemplo do grupo `50-host-classes`. O arquivo é um script shell que mostra o nome da classe dependendo da variável `$HOSTNAME`. Se o nome do cliente começar, por exemplo, com `L024-`, se trata de um computador do laboratório `L0.24`. Nesse tipo de cliente, o FAI vai instalar as classes básicas `BC_LINUX`, `BC_X11`, `BC_KDE` e `BC_BASE`, a classe de computador `CC_SUN`, a classe de sala `RC_L024` e a classe de serviço

`SC_LDAP`. Caso o FAI identifique esse cliente como uma máquina do tipo `vmware-1` ou `vmware-2`, trata-se de uma máquina virtual. Neste caso, o FAI vai instalar as classes `BC_LINUX`, `CC_VMWARE` e `SC_LDAP`.

Ambiente local

Para cada classe, pode-se definir padrões para a disposição do teclado, a zona de horários, senhas de usuários ou configurações similares. Os valores são armazenados no arquivo `classname.var`. O **exemplo 4** é um modelo para a classe `BC_LINUX`. O FAI percorre a lista de classes definida em `50-host-classes` da esquerda para a direita. Se múltiplas classes definem a mesma variável, o valor mais à direita da lista prevalece. Administradores espertos podem substituir valores padrão por valores específicos usando esse recurso.

Se diferentes senhas devem ser designadas aos computadores do laboratório `L0.24` por meio da configuração da classe `BC_LINUX`, é possível criar um novo arquivo `RC_L024.var` com as linhas de 12 a 15 do **exemplo 4** contemplando uma nova senha. Como o arquivo `50-host-classes` lista a classe `RC_L024` depois

Tabela 1: O conceito de classe

Classe	Abreviação	Exemplo	Explicação
Classe de sala	RC	RC_L024	Classe da sala do laboratório 0.24
		RC_P130	Classe da sala do grupo 1.30
		RC_O227	Classe da sala do escritório 2.27
Classe de computador	CC	CC_SUN	Classe de computadores Sun
		CC_HPCOMPAQ	Classe de computadores HP-Compaq
		CC_VMWARE	Classe de computadores VMware
Classe básica	BC	BC_LINUX	Classe básica para todos os cliente FAI
		BC_KDE	Classe básica para KDE
		BC_BASE	Classe básica para máquinas de grupos e laboratórios
Classe de serviço	SC	SC_LDAP	Classe de serviço para autenticação baseada em LDAP
Classe de programa	PC	PC_KIOSKTOOL	Classe de programa para ferramenta de modo quiosque
		PC_BOINC	Classe de programa para o serviço Boinc

Quadro 2: Particionamento avançado

Versões mais antigas do FAI usavam o script `setup_harddisks` para particionar o disco-rígido das máquinas cliente. Essa ferramenta funciona muito bem com discos-rígidos comuns, mas não dispõe de suporte para sistemas RAID ou para o gerenciador de volumes lógicos (LVM2 – *Logical Volume Manager*). Na sua versão 3.2.8, o FAI fornece a ferramenta `setup-storage` como alternativa ao programa `setup_harddisks`.

Se o FAI encontrar uma linha `USE_SETUP_STORAGE=1` na configuração de uma classe, ele usa o `setup-storage` para particionar os discos-rígidos em vez do `setup_harddisks`. Infelizmente, a ferramenta não dispõe de compatibilidade reversa, e a sintaxe do seu arquivo de configuração mudou.

O **exemplo 6**, que é um modelo de configuração para o `setup-storage`, mostra como particionar o primeiro disco-rígido de um sistema *dual-boot*, reservando a primeira partição para o Windows® XP™. Cada linha do script contém um comando com opções para essa finalidade. O comando `disk_config` define as configurações globais para o disco inteiro. A opção `disk 1` seleciona o primeiro disco-rígido. Se ele for um disco IDE, o `setup-storage` usa o identificador interno da partição, `hda`. Para discos SATA ou SCSI, esse identificador é `sda`.

A opção `preserve_always:1` diz à ferramenta de particionamento para não modificar a primeira partição primária, deixando a instalação do Windows® no lugar. O `setup-storage` vai apagar todas as outras partições. A opção `bootable:2` habilita a segunda partição como partição de boot. Os comandos `primary` e `logical` ordenam ao `setup-storage` a criação de uma partição primária e lógica,

respectivamente. O número de partições depende da ordem em que elas são listadas no arquivo.

A **linha 2** do **exemplo 6** usa a opção `primary` para dizer ao `setup-storage` para criar uma partição `sda2` de 200 MB. A partição contém um sistema de arquivos *Ext2* e `usa/boot` como ponto de montagem. O primeiro comando `logical` na linha 3 cria um sistema de arquivos de troca (*swap*) de 4 GB na primeira partição lógica (`sda5`). As partições lógicas `sda6` e `sda7` para `/tmp` e `/var` vêm em seguida. O último comando cria a partição `sda8`. O parâmetro `3000-` diz ao programa para usar o espaço remanescente do disco, mas com pelo menos 3 GB para a partição. No caso de o espaço em disco ser insuficiente, a instalação será encerrada com uma mensagem de erro. O FAI identifica os nomes das partições de maneira autônoma. O administrador só precisa saber dizer onde estão as partições primárias e lógicas.

O **exemplo 7** é um exemplo de particionamento em RAID 1 com dois discos SCSI. Primeiro, o `setup-storage` particiona os discos `sda` e `sdb` de maneira idêntica, mas não designa a eles sistemas de arquivos ou pontos de montagem. Comandos no bloco `disk_config raid` dizem ao `setup-storage` para configurar um sistema RAID com três partições e formata essas partições conforme especificado.

A ferramenta `setup-storage` é um utilitário muito poderoso com muito mais recursos que o `setup_harddisks`. A sintaxe de configuração de comandos é especificada por regras EBNF. Essas regras e maiores informações sobre o uso do `setup-storage` estão disponíveis na página do manual do utilitário e no wiki do FAI [2].

da classe `BC_LINUX`, os detalhes do novo arquivo prevalecem.

O diretório `debconf/` é usado para a configuração independente de classes dos parâmetros do sistema `Debconf`. O Debian usa o diretório `debconf/` para armazenar configurações globais, tais como o editor de textos ou o navegador de Internet padrão. A mídia de armazenamento é definida no diretório `disk_config` (veja o **quadro 1**).

O diretório `package_config/` define os pacotes necessários ao sistema alvo para cada uma das classes, geralmente usando o comando `PACKAGES aptitude package name...`. Também há suporte para a remoção de programas, por meio do comando `PACKAGES remove package name...`. O **exemplo 5** mostra como definir dependências entre as

classes. O comando `PACKAGES aptitude BC_KDE` instala os pacotes indicados apenas se eles fizerem parte do classe `BC_KDE`, o que permite aos administradores projetar e implantar estruturas altamente granulares.

Do seu jeito

O diretório `files/` contém todos os arquivos que o FAI vai copiar para o sistema alvo, armazenados por classe.

A hierarquia abaixo do diretório `files/` é baseada na árvore de diretórios do Debian. Para ilustrar esse ponto, se selecionarmos a classe `CC_HPCOMPAQ`, seria de se esperar que encontrássemos o arquivo `menu.lst` no diretório `/boot/grub` na máquina cliente após a instalação. Para que isso ocorra, é necessário que o conteúdo do arquivo `menu.lst` esteja copiado no diretório `files/boot/grup/menu.lst/CC_HPCOMPAQ/`. O FAI não

Exemplo 6: Particionamento de disco rígido

```
01 disk_config disk1 preserve_always:1 bootable:2
02 primary      /boot 200      ext2      rw
03 logical      swap 4000     swap      rw
04 logical      /tmp 10000    ext2      defaults
05 logical      /var 5000     ext3      defaults
06 logical      / 3000-    ext3      defaults,errors=remount-ro
```

```

-----
Fully Automatic Installation - FAI
FAI 3.2.9, 12 Aug 2000 Copyright (c) 1999-2000
Thomas Langa <langa@informatik.uni-koeln.de>
-----
      7876168   2845696   4678976   31% /var/lib/fai/config
/dev/sda7      5812488   728448   4829412   16% /target
/dev/sda1      132296    1918    123478    2% /target/boot
/dev/sda6      2871384   3896    1963854   1% /target/tmp
aufs          258348    2728    255628    2% /target/dev
Wed Aug 27 12:58:37 UTC 2000
The install took 436 seconds.
Calling task_chboot
SERVER not defined. Can't change network boot configuration
Exit code task_chboot: 2
Calling task_test
Will be implemented soon
Source hook: saveolog.LAST.source
ERRORS found in log files. See /tmp/fai/error.log.
saveolog.LAST.source OK.
Calling task_saveolog
Calling task_faiend
Press <RETURN> to reboot.
-----

```

Figura 3 No final da instalação, o FAI mostra um sumário contendo informações sobre a instalação. Pressionar **[ENTER]** reinicia o novo sistema Debian.

copiar automaticamente arquivos definidos por usuários abaixo de `files/` para o sistema alvo. Isso só acontece se o script de configuração contiver um comando `fcopy`.

O comando:

```
fcopy -iM /boot/grub/menu.lst
```

copiar o arquivo de configuração do gerenciador de inicialização `GRUB - menu.lst` – para o cliente. Ele é parte da classe `BC_LINUX`.

O diretório `hooks/` contém programas ou scripts para customização do processo de instalação. Por fim, o diretório `scripts/` contém os scripts que o FAI executa durante a

instalação. É fácil usar o `fcopy` para copiar arquivos com base na classe de cliente ou como um comando local com `/${ROOTCMD}`.

Como é comum em programas para o UNIX, o FAI oferece também diversas possibilidades de automação via scripts. Além do uso de scripts shell, o FAI também é capaz de executar scripts em Perl ou Cfengine. O Cfengine (veja artigo “Super máquina” à página 32) é uma boa escolha para realizar as modificações nos arquivos de configuração.

Diagnósticos

Após planejar, verificar e configurar arquivos de instalação e scripts, estamos finalmente prontos para usar

o FAI para automatizar o processo de instalação de um grande número de computadores. O último passo é estender as configurações de DHCP e TFTP de um modo que permita que os novos clientes iniciem pela rede e automaticamente carreguem a instalação via FAI. Para tornar isso possível, só precisamos aplicar as configurações para a primeira rodada de teste. Uma vez que o cliente FAI esteja completamente instalado, ele vai mostrar um sumário na tela e esperar que alguém pressione a tecla **[ENTER]** para disparar um processo de reboot (ver **figura 3**).

A plataforma de implantação do FAI armazena todos os processos de instalação em arquivos de registro no servidor. Caso seja necessário, é possível analisar os arquivos no diretório `/var/log/fai/` à caça de erros.

Controle remoto

O FAI é uma ferramenta versátil para automatizar a instalação de distribuições GNU/Linux baseadas em Debian. Além de arquiteturas x86, o instalador automático também dispõe de suporte para arquiteturas Sparc e PowerPC. A solução de instalação oferecida pelo FAI é ideal para muitas situações, de clusters a infraestruturas de TI heterogêneas em empresas. Uma vez que a curva de aprendizado tenha sido superada, o FAI torna-se uma plataforma poderosa nas mãos do administrador de sistemas, sendo capaz de automatizar quase todo tipo de instalação de sistemas baseada no Debian. ■

Exemplo 7: Particionamento para um sistema RAID 1

```

01 disk_config sda
02 primary      -      256      -      -
03 primary      swap    1024     swap    sw
04 primary      -      0-       -      -
05
06 disk_config sdb
07 primary      -      256      -      -
08 primary      -      1024     -      -
09 primary      -      0-       -      -
10
11 disk_config raid bootable:1
12 raid1/boot    sda1,sdb1    ext2     rw,errors=remount-ro
13 raid2swap     sda2,sdb2    swap     rw
14 raid3/        sda3,sdb3    ext3     rw

```

Mais informações

[1] Fully Automatic Installation (FAI): <http://www.informatik.uni-koeln.de/fai/>

[2] Setup-storage na wiki do FAI: <http://faiwiki.informatik.uni-koeln.de/index.php/Setup-storage/>

O appliance VoIP PIKA Warp

Appliance para toda obra

O PIKA Warp é, além de um appliance VoIP completo baseado em Linux, uma plataforma para desenvolvimento de soluções customizadas.

por Pablo Hess

ANÁLISE

Appliances são equipamentos indubitavelmente úteis. Encerrando uma única função, que realizam de forma especializada, eles são capazes de facilitar o gerenciamento, reduzir o consumo energético e, por consequência, reduzir significativamente o nível de estresse do administrador de sistemas moderno.

No entanto, a maior qualidade dos appliances – seu formato compacto e “desenvolvido para seu fim específico” – às vezes pode ser também seu ponto fraco. No caso de appliances VoIP, isso é ainda mais verdadeiro, pois o servidor de código aberto Asterisk se destaca por sua flexibilidade, inevitavelmente “castrada” pelas interfaces gráficas amigáveis, por melhores que estas sejam.

Imagine então um appliance realmente compacto, do tamanho de um típico telefone IP, que traz não apenas o Asterisk e uma interface web para seu gerenciamento, como também um verdadeiro kit de desenvolvimento para aquelas tarefas que exigem customização do software embarcado no dispositivo ou até instalação de novos programas.

Assim é o Warp, da canadense PIKA Technologies. Uma máquina compacta voltada tanto para o administrador com necessidades simples – supridas por praticamente qualquer outro appliance VoIP – quanto para

ambientes mais exigentes, como pequenos call centers, por exemplo.

Hardware

O PIKA Warp utiliza um processador PowerPC AMCC 440EP de 533 MHz e vem com 256 MB de memória RAM. Para armazenamento, há 256 MB de memória NAND (que abrigam o sistema operacional e aplicativos) e 4 MB de memória NOR para o sistema de inicialização. Além disso, há um leitor de cartões SD, que já vem carregado com um cartão de 1 GB.

A conectividade é o forte do equipamento: além de uma porta Ether-

net 10/100, um conector USB (infelizmente 1.1) e uma porta FXS, há dois encaixes para módulos internos que podem conter, cada um, quatro portas FXO ou quatro portas FXS – ou ainda duas portas (quatro canais) BRI ou duas portas GSM. Com isso, contando apenas os usos mais comuns de portas FXS e FXO, é possível usar o Warp com:

- ◆ 1 FXS + 8 FXO (até oito linhas e somente telefones IP, com um ramal legado);
- ◆ 5 FXS + 4 FXO (até quatro linhas e até cinco ramais legados); ou
- ◆ 9 FXS (somente linhas VoIP e até nove ramais legados).



Figura 1 Diversos conectores na visão traseira do PIKA Warp, enquanto a frente do aparelho exibe um display muito útil.

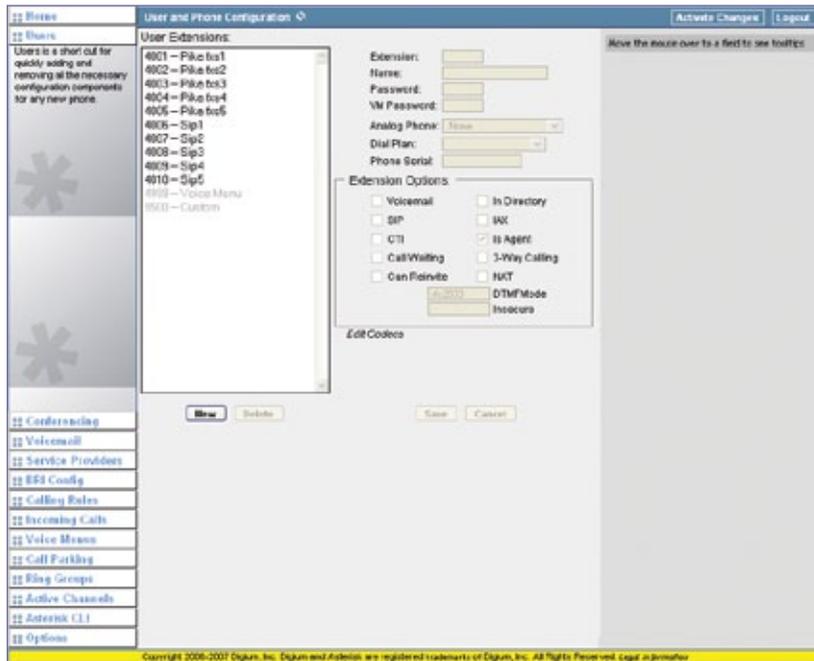


Figura 2 A interface web de administração do Asterisk, por si só, já oferece grande flexibilidade de configuração.

Para a função de música em espera, há também um conector de entrada de áudio e outro de saída, o que permite a ligação de um reproduzidor de MP3 ou um rádio ao Warp.

Exterior

Além da profusão de conectores na parte traseira do equipamento (figura 1), o Warp possui também um display frontal (figura 1) que

exibe o status de cada uma das conexões telefônicas. A superfície do aparelho é propositalmente deixada livre para que outras empresas apliquem suas marcas ao revender ou utilizar o Warp como base para seus produtos.

Para a instalação, é possível pendurar a máquina na parede ou simplesmente apoiá-la sobre outros equipamentos.

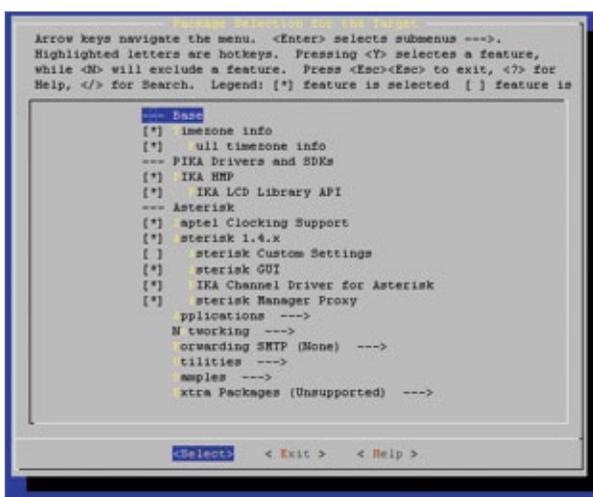


Figura 3 Lista de pacotes exibida pelo comando `make menuconfig`.

tantemente atualizada) com sua interface de administração (figura 3), o shell Busybox, um servidor web com `sqlite3` e suporte a PHP 5. Há ainda NTP, um cliente DHCP, servidor e cliente TFTP e um servidor DNS.

Desenvolvimento

Como o uso e a configuração pela interface web do Asterisk embarcada no PIKA Warp são bastante intuitivos, e devido ao fato de o dispositivo ser um convite ao desenvolvimento de soluções customizadas de VoIP, vale a pena concentrar esta análise nos aspectos de desenvolvimento do aparelho.

Há duas formas de fazer login no appliance: por SSH ou via porta serial. Por SSH, com o aparelho conectado a um outro computador na rede `192.168.1.0/24` (o cliente DHCP vem desativado, e o IP padrão é `192.168.1.80`), basta entrar por SSH com usuário `root` e senha `pikapika`. Recomenda-se alterar imediatamente essa senha com `passwd root`. A configuração de rede pode ser alterada (por exemplo, para ativar o cliente DHCP) editando-se o arquivo `/etc/networking.conf`, que é auto-explicativo.

O conector serial se encontra na placa do aparelho, portanto, para acessá-lo, é preciso desaparafusar sua tampa e localizar o conector serial. Uma vez conectados o aparelho e o outro computador via cabo serial, use a velocidade de `115200`, sem paridade, 8 bits com um bit de parada e nenhum controle de fluxo (por hardware ou software) para acessar o Warp.

PADS

Para desenvolver qualquer aplicativo para o Warp, é necessário empregar o PADS (*PIKA Application Development Suite*), um ambiente completo de desenvolvimento. Ele é estritamente necessário, pois, como

Software

O hardware não teria muito valor se não fosse pelo software que roda no PIKA Warp. O sistema Linux (kernel 2.6) que equipa o dispositivo é ajustado pela empresa à sua aplicação como servidor VoIP. Sobre o Linux, encontramos o todo-poderoso Asterisk (série 1.4, cons-

sistema embarcado, o Warp não é adequado ao desenvolvimento.

O PADS se baseia na plataforma *Buildroot*, um conjunto de *Makefiles* e *patches* que empregam a biblioteca *µClibc* e permitem a compilação cruzada e a geração de um sistema de arquivos raiz. Ele também inclui um gerenciador de pacotes que baixa e instala o código-fonte de vários projetos de código aberto.

O manual do PADS [1] lista os pacotes necessários para sua instalação numa estação Linux comum [2]. Com eles satisfeitos, baixe o PADS em [3], descompacte-o, entre no diretório criado e digite o comando `make menuconfig`. Ele exibirá uma lista de pacotes (figura 3). Após marcar os pacotes desejados, saia do menu e digite `make` para compilar e instalar os pacotes marcados. O ambiente compilado ficará em:

```
/diretorio/do/PADS/build_warp/root
```

NFS

Durante o processo de desenvolvimento, recomenda-se configurar o Warp para montar seu sistema de arquivos raiz via NFS a partir da estação de desenvolvimento. Como isso exige alterações no carregador de inicialização (U-Boot) [4], é obrigatório o acesso ao aparelho via porta serial.

Primeiro teste

Com o ambiente de teste instalado na estação e carregado no appliance, podemos fazer um teste conectando um telefone comum à porta FXS embutida no aparelho e chamando a extensão 600 (teste de gravação do Asterisk).

Arquitetura

A figura 4 mostra a arquitetura do sistema padrão do Warp. A API *GrandPrix*, ou apenas GP, abstrai todas as tarefas de acesso ao hardware PIKA incluído no Warp. Ela

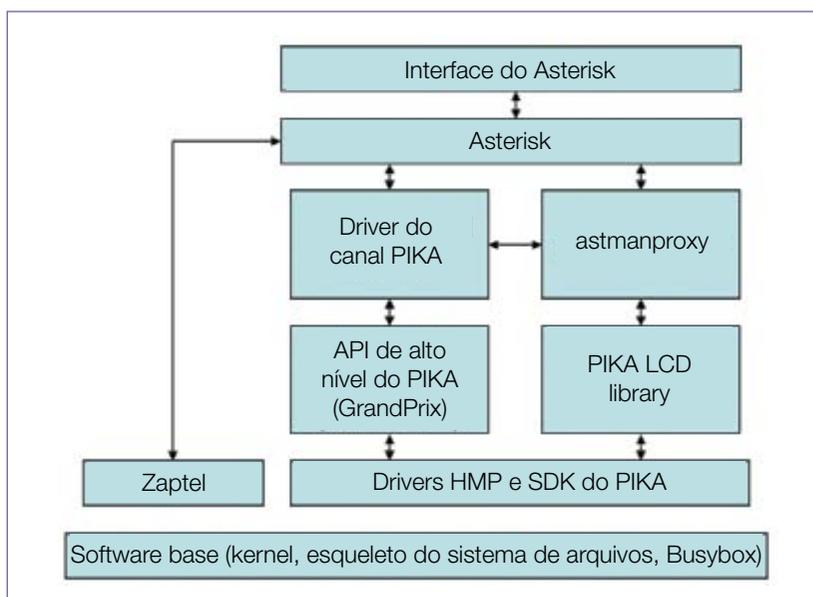


Figura 4 A arquitetura básica de software do Warp utiliza uma API de alto nível e uma biblioteca para acesso ao display. Ambas podem ser usadas para desenvolvimento de outros aplicativos.

facilita o estabelecimento de chamadas, a reprodução e gravação de áudio, detecção de tons e progresso e análise de chamadas.

A GP se baseia na API de baixo nível *HMP*, que permite o acesso às portas FXO, FXS e BRI, de áudio e também ao display.

Por último, a biblioteca do display (*LCD Library*) é usada pelo Asterisk para exibir informações sobre as chamadas, e também pode ser empregada por qualquer outro software.

Flexibilidade

O PIKA Warp reúne as características de appliance e computador. Como appliance, ele oferece um servidor Asterisk com nove conexões FXO/FXS capaz de sustentar até 32 chamadas telefônicas simultâneas, e portanto é mais adequado para pequenas e médias empresas.

Seu kit de desenvolvimento PADS é projetado para o uso por empresas que desejem criar produtos sobre o Warp, e oferece as melhores ferramentas de código aberto para permitir grande flexibilidade na escolha das aplicações e também o desenvolvimento de novas soluções.

Na intenção de agradar a todos os públicos, geralmente as empresas falham e oferecem um produto subótimo em todos os aspectos. Porém, com seu Warp, a PIKA Technologies acertou a mão e por isso merece a recomendação da Linux Magazine.

A extensa documentação disponibilizada em [5] oferece até mesmo informações sobre metodologias de desenvolvimento de sistemas embarcados, e auxilia bastante o uso do aparelho para qualquer propósito. ■

Mais informações

- [1] Manual do PADS: <http://tinyurl.com/warp-manual>
- [2] Dependências do PADS: <http://tinyurl.com/pika-01>
- [3] Download do PADS: <http://tinyurl.com/pika-02>
- [4] Configuração do U-Boot para inicialização por NFS: <http://tinyurl.com/pika-03>
- [5] Documentação do Warp: <http://tinyurl.com/warp-doc>

Liberdade ou abertura de software?

Flancos abertos por definição

O conceito do Software Livre é simples, mas ainda assim há quem se interesse em deturpá-lo para aproveitar suas vantagens sem se comprometer com a liberdade.

por Alexandre Oliva



Há mais de 25 anos, o movimento Software Livre vem defendendo e promovendo liberdade na vida digital, e também desenvolvendo software que atende a critérios de respeito a liberdades essenciais. Há pouco mais de uma década, uma dissidência (*Open Source*) tornou-se popular promovendo o software em vez da liberdade e adotando critérios bastante mais fracos, e não nos pontos que muita gente imagina.

Software é Livre quando usuários têm as liberdades, sem restrições substanciais, de (o) executá-lo para qualquer propósito, (1) estudar seu código-fonte e adaptá-lo para que se comporte como desejado, (2) copiá-lo e distribuí-lo da forma que foi recebido e (3) melhorá-lo e distribuir as modificações.

Diferente do que muitos acreditam, Software Livre não precisa ser *copyleft*, nem GPL, nem parte do projeto GNU, nem aprovado pela

FSF: basta poder gozar das quatro liberdades essenciais. A diferença é que, embora haja inúmeros mecanismos técnicos e jurídicos para respeitar as liberdades, a dissidência limitou-se a dois deles.

O mais óbvio, técnico, é a negação de acesso ao código-fonte. Sem ele, não há como estudá-lo, adaptá-lo ou melhorá-lo. É tão essencial que, quando a dissidência procurou um nome para sua iniciativa, escolheu um que fazia referência explícita a código-fonte. Eis que abriu dois flancos de ataque às liberdades: pela distorção do termo (basta acesso aos fontes?), e para criação de outros termos similares, aludindo à distorção e a um compartilhamento restrito. E tome confusão!

No campo jurídico, figura em destaque o direito autoral, um poder de exclusão temporário concedido pela sociedade aos autores de obras como software. Salvo limitadas ex-

ceções, um autor de software tem poder de proibir terceiros de copiar, modificar, distribuir, publicar e, no Brasil, até executar o software. Como o autor pode transferir esse poder a terceiros, chamo o detentor desse poder de “autoridade”. Chama-se licença de direito autoral a promessa da “autoridade” de não se valer (de parte) desse poder de exclusão contra um licenciado.

Nos critérios estabelecidos pela dissidência, além da exigência de código-fonte, há inúmeras condições que a licença deve atender, de modo que o poder de exclusão da “autoridade” não seja usado para desrespeitar as liberdades essenciais dos licenciados.

Mas lembre que há muitos outros mecanismos de exclusão e cerceamento, que são incompatíveis não só com a filosofia que fundamenta o movimento Software Livre, mas também com os objetivos da própria iniciativa dissidente.

Contratos são um desses mecanismos. A promessa da “autoridade” a você (a licença de direito autoral) não o exime de outros compromissos que você tenha firmado ou venha a firmar com terceiros. Um distribuidor de software, ainda que não sua “autoridade”, pode exigir a adesão do futuro usuário a um contrato como condição para lhe conceder sequer acesso ao software.

O contrato, no caso, pode ser o próprio acordo de venda, ou um acordo de confidencialidade (NDA), um contrato de pacote (*shrink-wrap*), de download ou de instalação (*click-through*) etc. Em se tratando de software, muitos são chamados EULAs, ou Acordos de Licenciamento com Usuário Final, ainda que sejam paupérrimos em licenças (permissões) e abundantes em restrições contratuais.

Caso desrespeitem suas liberdades, tornam o Software não-Livre para você. No entanto, a definição adotada pela dissidência do movimento Software Livre, ao limitar-se à exigência de código-fonte e de permissões na licença, abriu brechas para restrições contratuais e muitas mais.

O titular de uma patente válida implementada por um Software Livre pode obter uma ordem judicial que proíba você de distribuir ou mesmo executar o software. Aí o Software deixa de ser Livre para você, pois lhe faltam as liberdades essenciais, mas não há qualquer violação dos fracos critérios da dissidência: mais uma brecha aberta.

Exemplos

É parecido o caso da “Microvellação”, um mecanismo jurídico lançado conjuntamente pela Microsoft e pela Novell, em que duas empresas conspiram para desrespeitar as liberdades de seus clientes: enquanto uma delas estabelece com o cliente um contrato restritivo de licenciamento de patentes supos-

tamente praticadas pelo software, a outra o distribui sob licença de Software Livre. Embora esse arranjo atenda aos critérios da dissidência, o Software deixa de ser Livre para os clientes dessas empresas, pois o contrato de licenciamento de patentes veda a distribuição.

“Tivoização” [1] é ainda outro caso de restrição adicional que escapa da definição dissidente, mas que torna o Software não-Livre, neste caso por mecanismos técnicos: TiVo, um fabricante de vídeo-cassetes digitais, introduziu neles artifícios de criptografia que verificam se o software tivoizado, antes Livre, está autorizado pelo fabricante para execução no dispositivo, impedindo que o usuário adapte o software para que se comporte, no dispositivo, conforme desejado.

As diferenças não terminam aí: há leis contra a desabilitação de mecanismos de restrição a cópia sendo usadas para proibir modificações; já houve codecs multimídia Livres redistribuídos com fontes, mas junto a licenças de patentes que permitiam somente a execução dos binários fornecidos; há especificações cobertas por patentes com exigências restritivas em suas licenças; há licenças aprovadas pela dissidência que transformam em obrigação a liberdade de distribuir (ou não) modificações. Todos esses casos podem tornar Software não-Livre para usuários, sem que deixe de atender à definição dissidente. Percebe o perigo?

Há empresas e empresários criativos em busca de ainda outros meios para aumentar a confusão e a divisão dentro e fora de nossas comunidades, ou para se valer da popularidade e da boa vontade que o termo dissidente gera sem respeitar as liberdades dos usuários promovidas pelo movimento Software Livre, nem gerar as consequências das liberdades propagandeadas pela iniciativa dissidente.

Flancos abertos

Esses tipos de ataque se fazem possíveis mediante a exploração de flancos abertos pelos critérios mais fracos. Em vez de focar nas liberdades dos usuários, limitam-se ao código-fonte e ao que licenças permitem, abrindo brechas para inúmeros mecanismos de restrição às liberdades essenciais e as suas consequências.

Para evitar essas distorções e ataques, que tal evitar o termo que remete a essa definição vulnerável? Que tal ajudar a desfazer a concepção errônea de que o direito autoral é um ponto chave? Que tal se preocupar com a liberdade, em vez de focar numa só permissão que pode se provar insuficiente? Que tal realçar a importância da liberdade, para cada usuário e para toda a sociedade, até para trazer as consequências benéficas que a dissidência promove? Que tal não abrir os flancos para aqueles que querem beber da nossa fonte sem ajudar a mantê-la limpa? É bem fácil: Software Livre! ■

Mais informações

[1] Tivoização: <http://en.wikipedia.org/wiki/Tivoization>

Nota de licenciamento

Copyright 2009 Alexandre Oliva

Cópia literal, distribuição e publicação da íntegra deste artigo são permitidas em qualquer meio, em todo o mundo, desde que sejam preservadas a nota de copyright, a URL oficial do documento e esta nota de permissão.

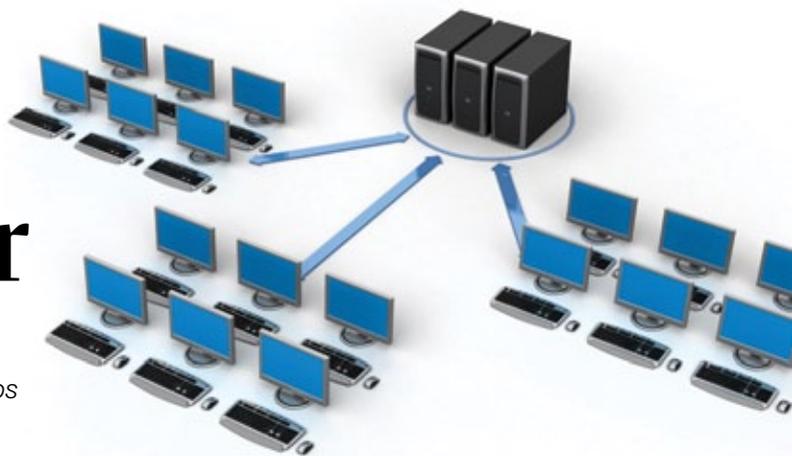
<http://www.fsf.org/svnwiki/blogs/lxo/pub/flancos-abertos>

Computação baseada no servidor com o X2Go

Deixa com o servidor

Em sua versão 3, já quase pronta, o projeto livre X2Go traz funções como novos clientes e janelas sem decoração.

por Heinz-M. Gräsing e Markus Feilner



O X2Go [1] é um servidor de terminais livre, rápido e flexível para qualquer cliente que suporte tecnologias modernas de autenticação, como leitores de cartão, tokens USB, gerenciamento de usuário centralizado via LDAP e ferramentas de autenticação integradas ao sistema de gerenciamento do KDE.

O projeto X2Go foi inspirado pela linha de produtos Sun Ray [2], que tem impressionado os adeptos de *thin clients* desde 2006. O segundo lançamento da Sun Ray incluía pequenos dispositivos que permitiam aos usuários fazer login usando um smartcard para trabalhar num servidor de terminais centralizado [3].

Além dos recursos multimídia e funções de segurança integradas nos produtos Sun Ray, o sistema de gerenciamento de sessão chamado pela Sun de *Hot Desktop Mobility* ou *Hot Desking* é a funcionalidade que mais chama a atenção.

Quando o usuário A retira seu cartão do leitor interno, o software automaticamente interrompe a sessão, liberando o thin client para o próximo usuário. Se o usuário A inserir seu smartcard no leitor de cartão em qualquer outra máquina, o servidor imediatamente lhe oferece a sessão interrompida.

Logicamente, os usuários Linux ficaram muito interessados num sistema versátil similar que, diferentemente do Sun Ray, não dependesse de hardware específico. Então, foi apenas uma questão de tempo até a comunidade do Código Aberto desenvolver tal produto. Oleksandr Shneyder e Heinz Gräsing, administradores de sistemas na cidade de Treuchtlingen, Alemanha, gastaram boa parte de seu tempo livre desenvolvendo um servidor de terminais livre que suportasse laptops e outros clientes, diferentemente do modelo da Sun. Graças a uma combinação inteligente de softwares GPL e seus próprios desenvolvimentos, a equipe chegou a uma resposta convincente: o X2Go.

Ferramentas integradas

Os desenvolvedores integraram ferramentas como inicialização por PXE e *Debootstrap* [4], as bibliotecas livres do NoMachine NX [5][6], ferramentas como *FUSE* [7] e *SSHFS* [8] a programas para desktop e extensões para GNOME e KDE. As bibliotecas PAM adicionam ainda o suporte à autenticação por smartcards e pendrives ao X2Go (figura 1).

Graças à capacidade do servidor NX para suspender e reiniciar sessões, a versão 2 foi a primeira a suportar a forma de login dos produtos Sun Ray.

Viajante mundial

Hoje, o X2Go está implantado em clientes e servidores desenvolvidos pelo Linux4Afrika [9] na Tanzânia e Moçambique e o Linux4Paraguay no Paraguai, além de estar presente em escolas alemãs (veja o quadro 1).

Versão 3

A versão 3 provavelmente estará disponível para uso em produção assim que esta edição chegar às bancas. O projeto é guiado pelo Debian, então os desenvolvedores do X2Go estavam esperando apenas o lançamento da versão 5 do sistema, o que ocorreu no último dia 14 de fevereiro.

Quatro novos recursos da lista ofuscam a enorme quantidade de falhas resolvidas e pequenas melhorias: além de versões para Linux, Windows e Mac, agora há uma versão para dispositivos baseados na plataforma aberta Maemo [10] da Nokia (incluindo alguns celulares) e o tão esperado cliente GTK, que inclui integração com o ambiente GNOME. O quarto acréscimo é a possibilidade de os usuários rodarem aplicações individuais sem depender de um desktop, como na solução da Citrix.

Embora o cliente Qt suporte todas essas novas funções, os desenvolvedores continuam a aparar as arestas. Por exemplo, a autenticação via USB, recentemente implementada, ainda

não está totalmente terminada. Quem precisa dela talvez deva esperar os desenvolvedores terminarem funções de segurança como *timestamps*, ID's dos clientes e a mudança dos tokens antes de fazer a atualização.

O próximo item na lista de tarefas a serem feitas é um serviço web para cada módulo X2Go que permitirá aos usuários acessar arquivos, músicas, aplicativos ou o desktop completo de uma máquina Linux pela Internet.

Conforme os desenvolvedores do X2Go revelaram no Ubuconf, eles imaginaram um tipo de computação em nuvem privada, chamada de *Pecloud*, em algum momento no futuro; a nuvem utilizaria informações de perfil para sincronizar a sessão com o ambiente individual, incluindo as aplicações e informações de dispositivos de armazenamento online.

Um pendrive do X2Go também está sendo planejado como aplicação portátil para Windows.

O X2Go procura criar um sistema aberto – porém completo – para servidor de terminais, o que explica as várias adições de softwares à distribuição. Elas incluem mecanismos para distribuir o sistema de arquivos do cliente via boot PXE, um gerenciador de login, plugins administrativos para o centro de controle do KDE e outras ferramentas. Os métodos de compressão do NX permitem sessões sobre links de banda-estreita.

Totalmente aberto

O X2Go não é compatível com as tecnologias LTSP (*Linux Terminal Server Project*) e NX, mas caminha com as próprias pernas. O projeto quer evitar a necessidade de integrar aplicações para compartilhamento de arquivos nos servidores ou clientes; porém, dependa de soluções como FUSE e SSHFS, ambas mantidas por outros grupos. Todos os componentes têm o código-fonte aberto e estão disponíveis para download no site do projeto.

Quadro 1: Linux4Afrika e X2Go

Na primavera de 2008 no hemisfério norte, o projeto Linux4Afrika [9], da ONG alemã FreiOSS.net, trocou o Edubuntu pelo X2Go. Hans-Peter Merkel, um dos líderes do projeto, explica a troca:

“A nova versão do X2Go para servidores do Linux4Afrika colocou a associação numa posição de dar suporte a redes maiores do que soluções típicas para salas de aula. A integração com a tecnologia LDAP é uma solução muito boa para estender nosso projeto de escolas para universidades. Outras tarefas de autenticação surgem aqui no uso cotidiano. Clientes Linux físicos agora podem fazer login no servidor LDAP do Linux4Afrika; pacotes do repositório padrão permitem isso com apenas algumas mudanças na configuração. Logicamente, a implantação desse tipo de ambiente exige operações num panorama heterogêneo de sistemas operacionais. Por esse motivo, os desenvolvedores atualmente estão bem dedicados à integração com os clientes Windows.

Com a maioria dos nossos usuários preferindo o desktop Gnome, a equipe de Heinz Gräsing respondeu rapidamente aos pedidos e implementaram modificações para dispositivos locais no Gnome.

A mais recente derivação do projeto Linux4Afrika na América do Sul, o Linux4Paraguay, será a primeira a se beneficiar da tecnologia do X2Go. No fim de 2008, Moçambique e Etiópia serão os primeiros a receber a nova solução.”

Os três clientes do X2Go pouco diferem em termos de funcionalidade, embora dependam de bibliotecas diferentes. O cliente Qt 4 na figura 2 roda sobre Linux, Windows, Mac OS X e Maemo, e – assim como o seu novo companheiro em Gtk (figura 3)

– funciona tanto como gerenciador de login em tela cheia no estilo do XDM quanto como aplicativo independente. Em ambos os casos, os administradores podem permitir configurações individuais ou dizer ao X2Go para usar um servidor LDAP central.



Figura 1 Os usuários do X2Go podem fazer login com um smartcard, pendrive ou senha. Os desenvolvedores criaram cartões com imagens semelhantes às do gerenciador de usuários do KDE para a versão demo.

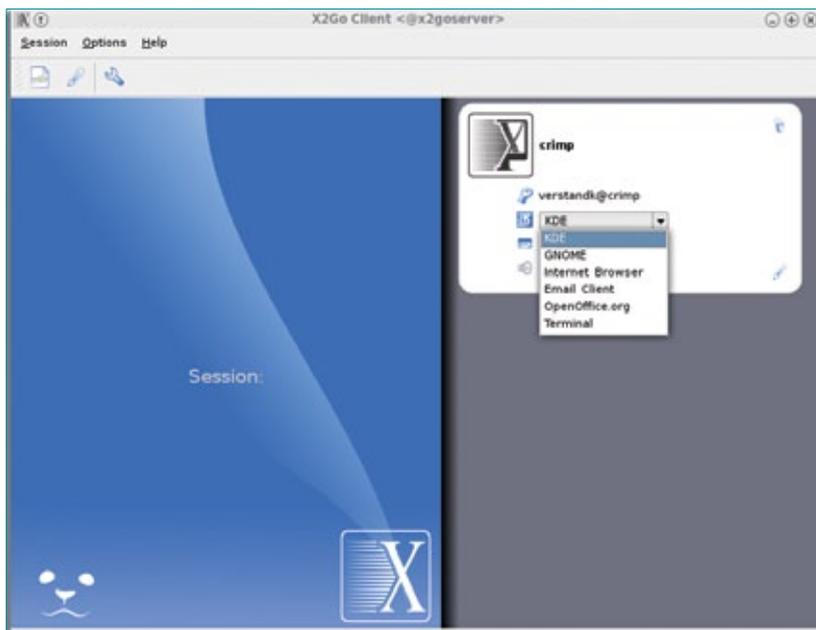


Figura 2 No login com o cliente X2Go, o usuário pode escolher se deseja executar um desktop Linux, como KDE ou Gnome, ou executar apenas aplicativos do ambiente local.

Todos os clientes gráficos seguem o mesmo conceito de usabilidade (ver **figuras 2 a 4**). O conjunto de *widgets* usado é chamado de *card-view* e utiliza uma abordagem no estilo de cartões de visita.

Sessões, usuários e configurações são configuráveis via listas *drop-down* e *pop-up* nessa tela, sem necessidade de alternar para uma ferramenta administrativa. Entretanto, o uso de LDAP para gerenciar informações de usuários e configurações dispensa a configuração por parte do usuário; a ferramenta simplesmente mostra uma lista de usuários que têm permissão de login a partir do sistema atual.

Janelas e comandos

O cliente X2Go pode ser configurado por um simples programa para desktop semelhante a um cliente físico de servidor de terminais. O acesso a um diretório LDAP central ainda é possível, e os usuários também podem acessar outros servidores e redimensionar ou minimizar a janela durante o uso. A terceira opção é um cliente flexível para linha

de comando, o *xzgoclient-cli*, mais apropriado para execução a partir de outros programas.

Por outro lado, o novo cliente Gtk está sendo projetado para usuários Gnome e Linux que desejem evitar programas baseados em Qt e KDE. Ele foi implementado nativamente e não depende do Qt. Oficialmente, esse cliente ainda estava sob desenvolvimento quando este artigo foi escrito, apesar de não haver falhas conhecidas até o momento.

Acesso remoto

Os programas clientes não são restritos à conexão à tela gráfica do servidor X2Go, mas também podem conectar os sistemas de arquivos locais ao servidor e redirecionar

a saída de som do servidor para a máquina cliente.

Para acessar o servidor, basta a porta SSH 22 e o túnel X2Go. Porém, ao contrário do NoMachine, o projeto utiliza o SSHFS para a transferência de arquivos e, portanto, depende dos pacotes mantidos pela distribuição.

O X2Go usa o *Udev* para oferecer suporte a dispositivos de armazenamento locais, como leitores de CD, e os conecta automaticamente ao servidor. Para computadores sem a tecla para ejeção do disco, a área de trabalho exibe um ícone que envia comandos ao cliente; essa função é importante para clientes Mac, por exemplo.

Enquanto uma sessão está sendo executada, os usuários podem compartilhar outros diretórios (**figura 5**). O X2Go os adiciona automaticamente à área de trabalho como compartilhamentos estáticos e adiciona ao menu drop-down as entradas para desmontagem.

Além do login simples baseado em nome de usuário e senha, o X2Go também oferece suporte a sessões flexíveis no estilo do produto da Sun, incluindo autenticação baseada em smartcards e pendrives. Entretanto,



Figura 3 O cliente Gtk recém-lançado parece muito semelhante à versão Qt, mas rodará no Gnome.

não há alternativa a um sistema de arquivos criptografado no pendrive; senão, os usuários que têm acesso a um pendrive perdido simplesmente poderiam ler o número ID.

Administradores em ambientes profissionais provavelmente desejarão optar pela segurança de um smartcard, dada a vantagem de o smartcard calcular o ID em lugar de armazená-lo.

Teclados Cherry com leitor de cartão integrado são uma boa escolha de hardware, já que a Towitoko colocou preços bem atraentes em seus dispositivos, ou outro leitor de cartões Classe 1 (ou superior) que suporte cartões *OpenPGP* [11].

Servidor X2Go

Existe uma gama de variantes dos componentes do servidor X2Go; a versão básica leva menos de dez minutos para instalar e está perfeitamente normal para testes e para a maioria dos desktops particulares. Ele inclui acesso remoto seguro, compartilhamentos e saída de áudio, e não depende do LDAP [12].

Os administradores preparados para investir mais tempo instalando o X2Go serão recompensados com capacidades multisservidor e um gerenciamento central de configurações, usuários e grupos via LDAP usando o *Luma* [13], por exemplo.

Se você necessita de suporte a thin clients que utilizam PXE para iniciar imagens individuais, não há alternativa a um serviço de diretório. O X2Go não necessita de esquemas individuais, mas se integra a configurações existentes. O gerenciamento centralizado das sessões ativas é suportado por um banco de dados *PostgreSQL*; basta uma instância central para múltiplos servidores X2Go numa rede.

O `sudo` ajuda administradores a especificar quais grupos de usuários têm permissão de login nos serviços X2Go. Como a configuração com

o comando `visudo` é difícil para os inexperientes, a nova versão do cliente agora verifica se o usuário é um membro do grupo certo e, em caso negativo, mostra uma mensagem de erro (figura 5).

Administração

Além do servidor e do cliente, o X2Go oferece ferramentas administrativas com interface gráfica que se integram ao centro de controle do KDE. Existem módulos para uso cotidiano dedicados ao gerenciamento de usuários, grupos e dispositivos, além do controle de sessões e os módulos de configuração do próprio X2Go.

Ligado diretamente a isso está um sistema separado de email (*x2go-mail*) com suporte a *rich text*, uma interface para administração do Samba e uma para gerenciar o compartilhamento da área de trabalho. O uso simultâneo de uma sessão única permite que múltiplos usuários trabalhem colaborativamente com um único aplicativo. Os administradores também apreciarão a possibilidade de monitorar as atividades dos usuários em caso de suporte (figura 6).

Para facilitar ainda mais, os módulos do centro de controle do

KDE também podem ser usados para gerenciar um servidor LDAP. Como os recursos de gerenciamento de usuários e grupos suportam buscas em tempo real e têm função de auto-completar, as ferramentas são úteis para grandes números de usuários. Os administradores podem procurar sessões em todos os servidores X2Go com uma visão clara em árvores mostrando atribuições individuais do servidor.

Requisitos e problemas

Os atuais requisitos de sistema do X2Go incluem uma tela de 640x480 ou maior e um cliente com processador de 800MHz.

Dito isso, o renderizador XVG da biblioteca Qt leva cinco segundos para apresentar a tela de login nessas condições. O X2Go é desenvolvido exclusivamente no Debian, e por isso é necessário um sistema Debian para instalar o X2Go com todos os seus recursos, embora também existam pacotes para Mandriva, ArchLinux e Alt Linux.

Os desenvolvedores ainda se referem ao X2Go como um hobby, mesmo com este tendo um escopo impressionante de ferramentas e



Figura 4 O X2Go lançou recentemente um cliente de terminal para a plataforma Maemo usada pelos tablets Nokia N770, N800 e N810.



Figura 5 Se o usuário não for membro do grupo X2Go, o cliente mostrará uma mensagem avisando sobre a configuração (incorreta) do sistema *sudo*.

referências. Os recursos são limitados; a equipe se concentra na programação, o que explica as poucas informações no website. Felizmente, os membros do projeto Linux4Afrika começaram a publicar tutoriais de instalação e guias online para resolução de problemas.

Atualmente, o processo de instalação do cliente para Windows do X2Go versão 3 não é compatível com o Vista; é preciso copiar alguns arquivos manualmente. A variante para Mac tem um problema com a versão do X11 incluída no OS X, e a autenticação por USB não está terminada. Acrescente os problemas conhecidos nas bibliotecas NX do FreeNX e OpenNX e seus componentes no código do X.org, que impedem a integração aos repositórios do Debian.

Luz no fim do túnel

Os administradores possuem complementos mais interessantes, como o *xzgospyglass*, útil para professores: ele mostra miniaturas das áreas de trabalho dos alunos, organizadas por sala de aula, grupo Posix ou individualmente.

O X2Go é um dos projetos de software de código aberto para acesso remoto mais substanciais disponíveis. Ele impressiona com sua seleção de clientes, administração extremamente flexível, seleção abrangente de ferramentas e métodos de autenticação que parecem obras de arte.

O X2Go também já converteu outros projetos e muitas escolas; o **quadro 1** explica por que o projeto de ajuda ao desenvolvimento mudou do Edubuntu para o X2Go. Além disso, o X2Go é interessante para qualquer um que queira dar acesso a um único sistema para múltiplos usuários, se a largura de banda é insuficiente para o VNC, ou se for preciso compartilhar arquivos e redirecionar áudio.

A R-zwo-R, em Rohrdorf, Alemanha [14], oferece acordos de níveis de serviço para qualquer um que esteja interessado em utilizar o X2Go num ambiente empresarial: a maior parte

da receita gerada a partir do suporte vai diretamente para o X2Go. Os desenvolvedores evitaram deliberadamente uma licença dupla.

Há uma imagem ISO do Live CD disponível em [15]. ■

Mais informações

- [1] X2Go: <http://www.x2go.org>
- [2] Sun Ray server 4: <http://www.sun.com/software/sunray/index.jsp>
- [3] Infraestrutura de desktop virtual da Sun: <http://www.sun.com/software/vdi/index.jsp>
- [4] Debootstrap: <http://www.debian-administration.org/articles/426>
- [5] NoMachine: <http://www.nomachine.com>
- [6] FreeNX: <http://freenx.berlios.de>
- [7] FUSE: <http://fuse.sourceforge.net>
- [8] SSHFS: <http://fuse.sourceforge.net/sshfs.html>
- [9] Linux4Afrika: <http://www.linux4afrika.de/index.php?id=2&L=0>
- [10] Maemo: <http://maemo.org>
- [11] Cartão OpenPGP: <http://www.g10code.com/p-card.html>
- [12] Guia de instalação do Linux4Afrika: <http://www.linux4afrika.de/x2go>
- [13] Luma: <http://luma.sourceforge.net>
- [14] R-zwo-R (em alemão): <http://www.rzwo.de>
- [15] Live CD: http://developer.berlios.de/project/showfiles.php?group_id=8454

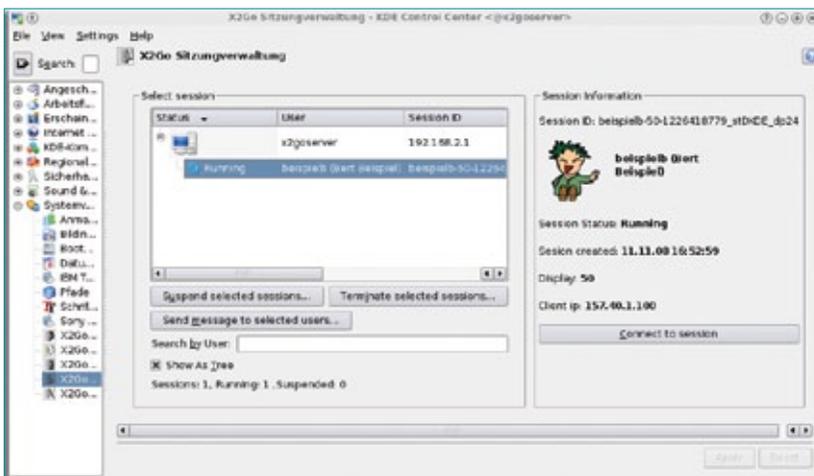


Figura 6 Vários itens das ferramentas do X2Go no centro de controle. Os administradores podem utilizar a ferramenta *System Administration | X2Go Session Management* para gerenciar as sessões ativas.



fisl10

10º Fórum Internacional Software Livre

A tecnologia que liberta

Edição Especial

24 a 27 de Junho de 2009 - Centro de Eventos PUCRS
Porto Alegre/RS - Brasil

Inscrições abertas para a submissão de propostas de palestras e artigos para o Workshop Software Livre 2009, caravanas e grupos de usuários. Faça já a sua inscrição de participante para o fisl10!

www.fisl.org.br



Promoção

Organização

Realização

Transmissão



PROJETO SOFTWARE LIVRE - RS



Servidores DNS e DHCP simples com Dnsmasq

DNS e muito mais

O Dnsmasq é uma alternativa prática para DNS em pequenas redes.

por **Martin Steigerwald e Pablo Hess**

Servidores DNS fornecem uma forma de associar nomes de domínio a endereços IP. Um sistema de servidores DNS operando na Internet fornece o mapeamento claro que permite a navegação na Web com nomes em vez de números. Porém, como fica a situação se você estiver numa pequena rede atrás de um firewall com NAT? Uma rede local simples não precisa de todas as funcionalidades de uma implementação completa do DNS. Geralmente, é suficiente responder requisições DNS vindas de máquinas na rede local e repassar tudo que for preciso para o servidor DNS do provedor.

O Dnsmasq é uma implementação simples e leve de servidores DNS, DHCP e TFTP para pequenas redes locais. Essa ferramenta prática

serve endereços para a rede local e encaminha requisições de máquinas externas para qualquer servidor DNS. Como o Dnsmasq integra DNS e DHCP, ele se lembra dos nomes de máquinas que receberam endereços por DHCP. Essa técnica reduz significativamente o tempo de configuração. Basta configurar todos os clientes para usar DHCP, e eliminar assim a necessidade dos mapeamentos no arquivo `/etc/hosts`. O programa é frugal no uso de recursos e, portanto, adequado à instalação em sistemas roteadores baseados em Linux.

Várias distribuições populares já possuem o Dnsmasq em seus repositórios, e as dedicadas a dispositivos roteadores, como *OpenWrt*, *DD-WRT* e *FreeWRT* incluem-no em suas ima-

gens [1][2]. Em nosso laboratório, o Dnsmasq foi executado no Debian a partir de um pendrive conectado a um roteador DSL Asus WL-500g Premium [3].

Configuração

O arquivo de configuração do Dnsmasq é `/etc/dnsmasq.conf`. Porém, há uma opção mais conveniente do que editá-lo e refazer todas as alterações sempre que o programa for atualizado: com `conf-dir=/etc/dnsmasq.d`, é possível carregar os arquivos de configuração a partir do diretório `/etc/dnsmasq.d/`. Outra possibilidade é usar a opção `conf-file` para carregar um único arquivo de configuração. A página de manual do programa contém mais informações sobre outras opções. Depois de alterar o que

Exemplo 1: Configuração do DNS no Dnsmasq

```
# Seja amigável com os servidores DNS superiores
domain-needed
bogus-priv

# Filtre algumas requisições DNS do Windows
filterwin2k

# Escute somente na LAN
interface=eth0.1
bind-interfaces

# Domínio local
domain=residencia.home
```

for preciso, basta reiniciar o serviço com `/etc/init.d/dnsmasq restart`.

O servidor DNS é muito fácil de configurar. Basta criar um arquivo de configuração bem pequeno chamado, digamos, `/etc/dnsmasq.d/dns` (**exemplo 1**). Com a linha `domain-needed`, o Dnsmasq faz a requisição ao servidor superior somente se for informado um nome de domínio. A linha `bogus-priv` evita que a ferramenta repasse requisições para endereços IP (ou seja, resolução reversa) para o servidor DNS superior caso elas se originem nas faixas de IP privadas.

As instruções `interface` e `bind-interfaces` fazem o servidor DNS escutar somente na rede local. Por último, `domain` especifica o domínio local, que é livremente configurável. Não é uma boa ideia usar domínios que já existam na Internet. O domínio `.home` é sempre uma boa escolha, e é preciso acrescentá-lo à diretiva `search` do arquivo `/etc/resolv.conf` dos clientes. Se for especificado um nome sem domínio, o software DNS tentará resolver o nome incluindo o domínio local; isso economiza digitação.

Essa configuração de exemplo ignora uma consideração importante: Como o Dnsmasq sabe qual servidor DNS está disponível para requisições

na Internet? Ele obtém essa configuração a partir do arquivo `/etc/resolv.conf` da mesma máquina onde ele está rodando. No Debian, o pacote `resolvconf` usa uma técnica ainda mais elegante: a lista de servidores DNS do Dnsmasq fica guardada em `/var/run/dnsmasq/resolv.conf`, e o `/etc/resolv.conf` aponta apenas para `127.0.0.1` como servidor de nomes [4].

Questão de ordem

Nas demais distribuições, o Dnsmasq utiliza os servidores conforme listados em `/etc/resolv.conf`.

Porém, o software tem certa inteligência: quando é apontado de um servidor, o Dnsmasq mantém uma lista dos servidores que respondem mais rápido e envia as requisições preferencialmente para eles. Há casos, no entanto, em que a ordem de busca dos servidores listados em `resolv.conf` deve ser observada, e para isso basta acrescentar o comando `strict-order` ao arquivo de configuração do Dnsmasq.

A instrução `resolv-fine` faz o Dnsmasq carregar seus servidores DNS a partir de um arquivo diferente, e `server` permite acrescentar servidores DNS diretamente no arquivos de configuração. Por exemplo, a diretiva `a seguir` usa um dos servidores DNS do OpenDNS [5] (altamente recomendado por causa da segurança superior desse serviço):

```
server=208.67.222.222
server=208.67.220.220
```

Outra possibilidade é integrar um servidor DNS já existente na rede ou em outro domínio. Além disso, o Dnsmasq adiciona as definições de `/etc/hosts` a seu DNS, que também é onde acrescentamos

Quadro 1: Dnsmasq contra os anúncios

Um uso muito interessante para o arquivo `/etc/hosts` local é a filtragem de anúncios diretamente pelo IP do site que os serve. Por exemplo, se o domínio `anunciaequi.br` for um servidor de anúncios mal comportados, daqueles que volta e meia entram na frente do texto principal dos sites que você visita, basta acrescentar a seguinte linha ao final do seu arquivo `/etc/hosts`:

```
127.0.0.1 anunciaequi.br
```

Com isso, consultas a esse site não retornarão as imagens, animações ou códigos JavaScript, livrando o visitante dos anúncios provenientes desse domínio. Existem vários arquivos `hosts` disponíveis pela Internet com o propósito de bloquear anúncios. Um deles, em [6], é citado na Wikipédia como exemplo de uso desse recurso.

Usando um arquivo `hosts` como esse, o Dnsmasq consegue livrar uma rede inteira (isto é, todos os clientes atendidos por ele) de diversas fontes de anúncios indesejados.

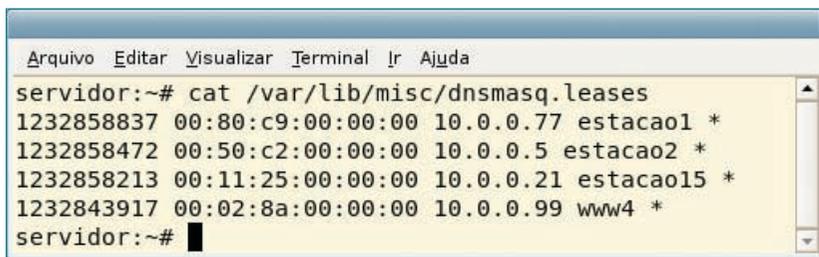


Figura 1 Arquivo com os clientes DHCP do Dnsmasq.

o nome da máquina que abriga o Dnsmasq.

Para as máquinas da rede local, o domínio precisa coincidir com aquele definido no Dnsmasq; a resolução de nomes não funcionará em casos diferentes.

DHCP em uma linha

A ativação do DHCP também é rápida. O programa usa a opção:

```
dhcp-range=10.0.1.9,10.0.1.99,12h
```

num arquivo como `/etc/dnsmasq.d/dhcp` para os IPs dinâmicos entre `10.0.1.9` e `10.0.1.99`, válidos por 12 horas.

Também é possível usar o `dhcp-host` para atribuir endereços estáticos a máquinas específicas. O Dnsmasq identifica as máquinas por seus endereços MAC, seus nomes ou seus IDs de cliente DHCP.

IPs constantes

Administrar os IPs de forma centralizada costuma ser bem mais produtivo, mesmo em redes pequenas. Para mapear endereços MAC a IPs, basta usar a seguinte linha (uma para cada endereço MAC):

```
dhcp-host=11:22:33:44:55:66,  
192.168.10.11
```

Para mais controle, pode-se inclusive fixar um nome (`www4`, por exemplo) para essa máquina específica, e até um tempo de validade do IP (42 minutos, no caso):

```
dhcp-host=11:22:33:44:55:66,www4,  
192.168.10.11,42m
```

E a flexibilidade do Dnsmasq não termina aí. Se quisermos fixar o IP `10.0.2.3` ao cliente chamado `estacao2`, basta usarmos a seguinte linha:

```
dhcp-host=estacao2,10.0.2.3
```

Centralizando

“Com grande flexibilidade vêm grandes dores de cabeça de administração”, já diziam os antigos. Um arquivo de configuração que atribui nomes a IPs e a endereços MAC pode facilmente entrar em conflito com os mapeamentos de `/etc/hosts`. Então, o mais sensato para manter o mapeamento IP-nome centralizado no arquivo tradicional (`/etc/hosts`) é ordenar que o Dnsmasq lhe obedeça:

```
dhcp-host=estacao2
```

No arquivo de configuração do `dhclient` dos clientes (`/etc/dhcp3/dhclient.conf`), é preciso usar uma opção como `send host-name "estacao5"` para enviar o nome da máquina ao servidor DHCP. Outra possibilidade é usar a opção `send dhcp-client-identifier` do `dhclient` para enviar a ID de cliente DHCP para o servidor. O `dhcpcd`, outro cliente DHCP, envia o nome da máquina por padrão.

Tudo funcionando?

Agora que já temos o DNS e o DHCP funcionando, é hora de levar o Dnsmasq para um passeio. Para evitar dores de cabeça, é importante garantir que não mais que um servidor

DHCP esteja em atividade em cada segmento da rede; lembre-se do servidor que reside no ponto de acesso, se for o caso.

Depois de reiniciar os clientes DHCP da rede para que o Dnsmasq lhes sirva, é possível acompanhar as requisições e atribuições de IP pelo arquivo `/var/lib/misc/dnsmasq.leases` no servidor (**figura 1**).

Um uso muito interessante do Dnsmasq, e altamente positivo para os clientes, é a aplicação de um arquivo `/etc/hosts` dedicado (**quadro 1**) a barrar anúncios mal comportados e propiciar uma navegação mais sã. ■

Mais informações

- [1] Dnsmasq no OpenWrt: <http://wiki.openwrt.org/OpenWrtDocs/dnsmasq>
- [2] Dnsmasq como servidor DHCP: http://www.dd-wrt.com/wiki/index.php/DNSMasq_as_DHCP_server
- [3] Debian no Asus WL-500g Deluxe: http://wpkg.org/Running_Debian_on_ASUS_WL-500G_deluxe
- [4] Dnsmasq no Debian: </usr/share/doc/dnsmasq/README.Debian>
- [5] OpenDNS: <http://www.opendns.com/>
- [6] Arquivo hosts contra anúncios: <http://www.mvps.org/winhelpt2002/hosts.zip>

Sobre o autor

Martin Steigerwald trabalha como instrutor, consultor e administrador de sistemas na team(ix) GmbH em Nuremberg, Alemanha. Seu trabalho se concentra principalmente em treinamentos em Linux, mas também em projetos, instalações e manutenção de infraestruturas robustas de TI baseadas em Debian.



ubuntu
linux for human beings

**Curso Ubuntu
Professional**

- Recife: 09/05
- São Paulo: 23/05

Ubuntu Certified Professional

A plataforma Linux mais usada no mundo agora certifica você aqui no Brasil!

- Desktop Ubuntu
- Ubuntu Professional 199

Seja nosso Parceiro

Participe do programa de qualificação de parceiros para treinamento Ubuntu no Brasil.
Fectura Tecnologia 81.3223.8348 / Linux New Media 11.4082.1300 / www.fectura.com.br



O Ratproxy procura vulnerabilidades em aplicações web

Tem rato na rede

O Ratproxy do Google é uma ferramenta gratuita que busca problemas de segurança em aplicações web.

por **Tim Schürmann**



Krisz Szkuriatowski – www.sxc.hu

Várias ferramentas de teste ajudam a procurar vulnerabilidades em aplicações baseadas na web [1][2], mas muitas dessas aplicações são caras ou difíceis de usar. Não seria ótimo apertar um botão e descobrir as vulnerabilidades do seu próprio software – junto com uma referência de linhas para ajudar a encontrar os problemas no código-fonte?

O Ratproxy [1] é uma ferramenta pequena, mas poderosa, com uma técnica simples para buscar problemas em aplicações web. Ele se originou nos laboratórios de desenvolvimento do Google, onde foi criado para testar as próprias aplicações web do gigante das buscas. Em julho de 2008, a empresa decidiu lançar a versão atual para o público geral sob a licença Apache 2.0.

O Google descreve o Ratproxy como uma “ferramenta majoritariamente passiva para auditoria de segurança em aplicações web”. Escondida sob essa descrição crítica existe uma ferramenta com um propósito simples: capturar as comunicações entre o navegador e a aplicação, registrar os dados enviados e verificar os registros atrás de problemas, riscos e vulnerabilidades conhecidos. Os desenvolvedores podem simples-

mente iniciar o Ratproxy e observar a saída. O Ratproxy alcança lugares que produtos concorrentes têm dificuldade em acessar. Por exemplo, outras ferramentas podem achar difícil chegar a áreas protegidas por senha, ou podem esbarrar em cenários de encaminhamento. Da mesma forma, o Ratproxy inteligentemente transpõe problemas de JavaScript. As ferramentas de teste legadas empregam chutes para descobrir qual função será usada em seguida. Esse problema ocorre particularmente em testes de interface gráfica, nos quais os usuários geralmente possuem uma escolha de vários botões e menus. O Ratproxy, por outro lado, simplesmente espera para conferir o que o usuário faz em seguida no navegador.

Como o Ratproxy não causa um aumento perceptível no tráfego de rede, ele permite até que se verifique as aplicações em uso em ambientes de produção (outros buscadores iniciam ataques de negação de serviço ou XSS que podem derrubar sistemas de produção).

Ratoeira

Instalar o Ratproxy é simples: basta baixar o código-fonte da página do programa e executar `make` para

compilar os poucos arquivos com código-fonte. A ferramenta não requer um script `configure` nem tem dependências importantes. Ela precisa apenas das bibliotecas `Libcrypto` e `Libssl` (normalmente fornecida como parte da distribuição `OpenSSL`) e seus cabeçalhos correspondentes.

Executar a ferramenta de teste é um pouco mais complicado: nada menos que 22 parâmetros (tabela 1) regulam a natureza e o escopo dos testes feitos pelo Ratproxy. Os parâmetros também são responsáveis por definir o nível de detalhamento a ser exibido. Para evitar o soterramento sob uma avalanche de mensagens ao se executar o programa, inicie com as configurações padrão:

```
$. /ratproxy -v /tmp -w ratproxy.  
log -d dominio.com -lfscm
```

Esse comando aponta o Ratproxy para a aplicação web no domínio `dominio.com`. O Ratproxy ignora qualquer URL que não esteja nesse servidor (essa técnica é uma forma de garantir que o Ratproxy não teste acidentalmente sites de anúncios externos). O tráfego HTTP capturado pelo Ratproxy é despejado num grande número de pequenos arquivos

Tabela 1: Parâmetros do Ratproxy

-l	Por padrão, o Ratproxy usa <i>checksums</i> para comparar sites. O parâmetro <code>-l</code> ativa um método menos estrito.
-f	O Ratproxy também inspeciona aplicações Flash; com o parâmetro <code>-v</code> , ele as descompila para uma análise mais detalhada.
-s	Todas as requisições <code>POST</code> são armazenadas no arquivo de log.
-c	Relembra páginas que definem cookies, independentemente de representarem ou não riscos à segurança.
-m	O Ratproxy guarda todo o conteúdo fora do domínio de teste. Sem esse parâmetro, somente folhas de estilo e scripts vinculados remotamente são registrados. Isto supõe que o parâmetro <code>-d</code> esteja sendo usado.
-e	Inspecciona o cache em mais detalhes.
-x	Registra todas as URLs que podem ser úteis para futuros testes manuais de XSS.
-t	Por padrão, o Ratproxy registra todas as vulnerabilidades do tipo <i>directory traversal</i> . Esse parâmetro permite candidatos menos prováveis, que então podem ser usados para análises manuais.
-i	Registra todos os arquivos PNG retornados; esses arquivos já foram usados no passado para ataques XSS (versões antigas do Internet Explorer estão particularmente sujeitas a isso).
-g	Estende os testes XSRF para incluir requisições <code>GET</code> .
-j	Ativa a detecção de construções arriscadas em <i>JavaScript</i> , como chamadas a <code>eval()</code> .
-X	O Ratproxy alterna para o modo ativo e testa aplicações web em busca de vulnerabilidades a ataques XSS e XSRF.
-C	O Ratproxy repete algumas requisições com parâmetros modificados.

Há uma lista completa e abrangente de parâmetros na documentação [1].

no diretório temporário (`-v /tmp`), enquanto a análise dos resultados – isto é, as informações que nos interessam – são armazenadas em `ratproxy.log`. O **quadro 1** explica a caixa de Pandora de opções de linha de comando.

Se for preferível um passeio completo, pode-se alterar os parâmetros da seguinte forma:

```
$ ./ratproxy -v /tmp -w ratproxy.  
➔ log -d dominio.com -ltextifscgjm
```

O dueto opcional `-XC` libera o Ratproxy de seu modo passivo. Uma vez livre, o Ratproxy verifica quanto sua aplicação web resiste a ataques XSS e XSRF (`-X`), e repete requisições com diferentes parâmetros (`-C`).

Se a aplicação web retornar objetos *Flash*, o Ratproxy pode decompô-los e analisá-los. Para isso, ele se utiliza do descompilador *ActionScript Flare*; infelizmente, o Flare só está disponível como aplicativo de código fechado pré-compilado. Por padrão,

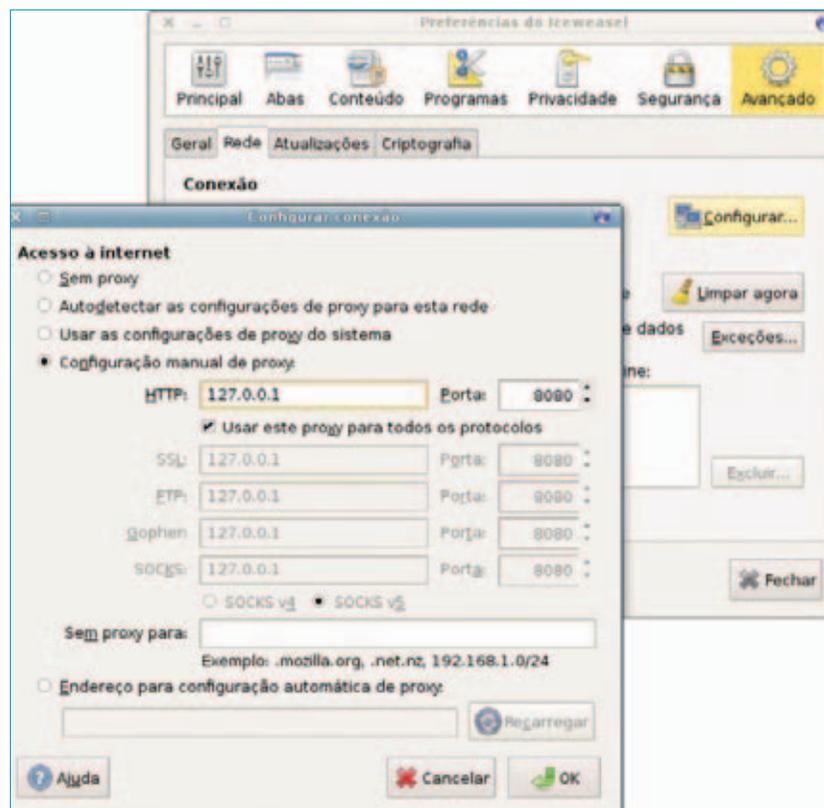


Figura 1 Para apontar o Firefox para o Ratproxy, é preciso defini-lo como proxy para todos os acessos do navegador e limpar seu cache.

preciso aceitar o novo certificado. A documentação do Ratproxy [1] recomenda não guardar o certificado permanentemente no navegador. Afinal, qualquer pessoa que baixa o Ratproxy conhece o certificado. Como o proxy da ferramenta força um certificado, surge outro problema: o Ratproxy negocia todos os passos seguintes com a aplicação web, então é impossível ter 100% de certeza de que se está “conversando” com o seu próprio servidor. Portanto, deve-se evitar o uso de contas críticas (administrativas) ao se digitar dados sensíveis enquanto ocorre o monitoramento pela ferramenta.

Além disso, é recomendável resistir à tentação de usar o *wget* para passar o site para o Ratproxy. A maioria dos testes do Ratproxy se baseia na interação com o usuário, e por isso eles seriam impossíveis no caso do *wget* por este não ser interativo.

Demonstração

Com **[Ctrl]+[C]**, o teste do Ratproxy é terminado. Os resultados da análise são armazenados no arquivo levemente críptico *ratproxy.log*, que é feito para facilitar a leitura pelo computador e cooperar com o *grep* (figura 3). Até surgirem novas ferramentas, é possível usar o script *ratproxy-report.sh* para gerar um relatório mais intuitivo em HTML:

```
$ ./ratproxy-report.sh ratproxy.
↳ log > report.html
```

O relatório é semelhante àquele da figura 4: a lista apresenta os problemas identificados pelo Ratproxy, ordenados por tipo e importância. Riscos críticos de segurança são realçados com um *HIGH* em vermelho chamativo. *Toggle* exhibe ou oculta as mensagens de uma seção específica, e *view trace* abre o *trace* (isto é, a comunicação capturada) a partir do diretório *tmp*.

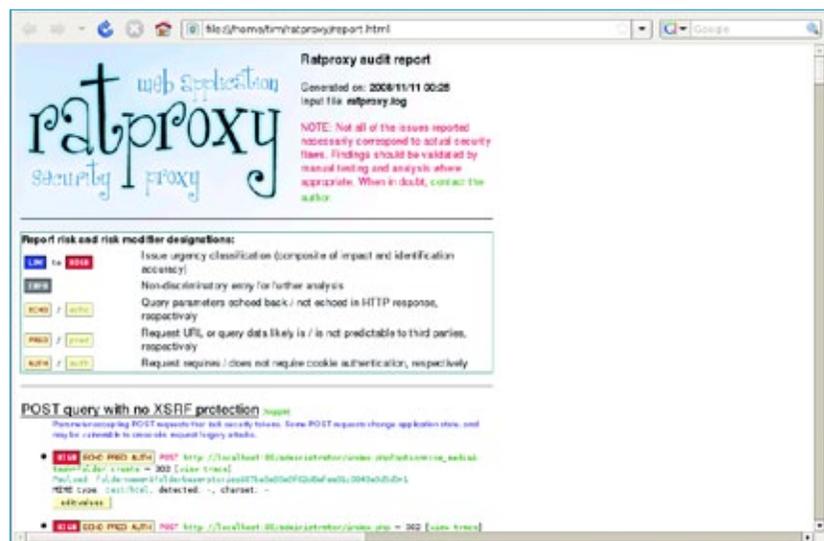


Figura 4 O Ratproxy fornece um relatório com resultados dos testes.

Nesse ponto, o usuário precisa interpretar os resultados. Para isso, é preciso dominar tanto a segurança de computadores e os detalhes da aplicação sendo testada. Afinal, não faz sentido o Ratproxy alertá-lo a respeito de um risco potencial de *cross-site scripting* se você não for capaz de solucioná-lo. Em outros casos, a ferramenta lista problemas genéricos que não necessariamente representam risco à segurança.

Conclusões

Como o Ratproxy funciona de forma inteiramente autônoma, é impossível injetar seus próprios dados de teste na aplicação web para confirmar suas suspeitas. Ele só consegue relatar vulnerabilidades detectadas nas partes da aplicação web que ele realmente investiga (veja o quadro 1). Os desenvolvedores estão cientes de que seu produto não é perfeito, portanto pedem sugestões, melhorias e detalhes de quaisquer problemas de segurança que o Ratproxy não consiga identificar.

Lembre-se de que o Ratproxy ainda está em fase beta. Não se surpreenda ao receber falsos positivos e não se baseie apenas no Ratproxy em detrimento de todas as outras ferramentas. Se você quiser solucionar problemas,

a ferramenta do Google ainda é uma novidade útil em seu kit de ferramentas para teste de segurança.

O Ratproxy ainda está longe de ser uma panaceia. Ele não fornece uma lista completa de vulnerabilidades sem solução, nem ajuda a resolver os problemas encontrados. Interpretar os resultados exige conhecimentos especializados em segurança na Web.

O que o Ratproxy faz é apontar de forma confiável os problemas potenciais, vulnerabilidades e códigos mal implementados. Se o Google continuar refinando sua ferramenta e conseguir atrair outras empresas para se comunicar com as interfaces abertas do Ratproxy, esse software pode se desenvolver até tornar-se uma joia para testar aplicações web. ■

Mais informações

[1] Ratproxy: <http://code.google.com/p/ratproxy>

[2] Chorizo: <https://chorizo-scanner.com>

[3] Descompilador Flash Flare: <http://www.nowrap.de/flare.html>

[4] Burp Suite: <http://portswigger.net/suite>

Linux.local

O maior diretório de empresas que oferecem produtos, soluções e serviços em Linux e Software Livre, organizado por Estado. Senti 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**

SERVIÇOS

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.turbsite.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						✓
Pernambuco										
Fectura Tecnologia	Recife	Rua Nicarágua, 159 – Espinheiro – CEP: 52020-190	81 3223-8348	www.fectura.com.br			✓			✓
Rio de Janeiro										
Múltipla Tecnologia da Informação	Rio de Janeiro	Av. Rio Branco, 37, 14º andar – CEP: 20090-003	21 2203-2622	www.multipa-ti.com.br	✓		✓		✓	✓
NSI Training	Rio de Janeiro	Rua Araújo Porto Alegre, 71, 4º andar Centro – CEP: 20030-012	21 2220-7055	www.nsi.com.br				✓		✓
Open IT	Rio de Janeiro	Rua do Mercado, 34, Sl, 402 – Centro – CEP: 20010-120	21 2508-9103	www.openit.com.br				✓		✓
Unipi Tecnologias	Campos dos Goytacazes	Av. Alberto Torres, 303, 1º andar – Centro – CEP: 28035-581	22 2725-1041	www.unipi.com.br			✓	✓	✓	✓
Rio Grande do Sul										
4up Soluções Corporativas	Novo Hamburgo	Pso. Calçadão Osvaldo Cruz, 54 sl. 301 CEP: 93510-015	51 3581-4383	www.4up.com.br		✓	✓		✓	✓
Definitiva Informática	Novo Hamburgo	Rua General Osório, 402 - Hamburgo Velho	51 3594 3140	www.definitiva.com.br	✓		✓		✓	✓
Solis	Lajeado	Av. 7 de Setembro, 184, sala 401 – Bairro Moinhos CEP: 95900-000	51 3714-6653	www.solis.coop.br		✓	✓	✓	✓	✓
DualCon	Novo Hamburgo	Rua Joaquim Pedro Soares, 1099, Sl. 305 – Centro	51 3593-5437	www.dualcon.com.br	✓		✓		✓	✓
Datarecover	Porto Alegre	Av. Carlos Gomes, 403, Sala 908, Centro Comercial Atrium Center – Bela Vista – CEP: 90480-003	51 3018-1200	www.datarecover.com.br	✓		✓			
LM2 Consulting	Porto Alegre	Rua Germano Petersen Junior, 101-Sl 202 – Higienópolis – CEP: 90540-140	51 3018-1007	www.lm2.com.br			✓		✓	✓
LnX-IT Informação e Tecnologia	Porto Alegre	Av. Venâncio Aires, 1137 – Rio Branco – CEP: 90.040.193	51 3331-1446	www.lnx-it.inf.br	✓		✓		✓	✓
Plugin	Porto Alegre	Av. Júlio de Castilhos, 132, 11º andar Centro – CEP: 90030-130	51 4003-1001	www.plugin.com.br	✓		✓		✓	✓
TeHospedo	Porto Alegre	Rua dos Andradas, 1234/610 – Centro – CEP: 90020-008	51 3286-3799	www.tehospedo.com.br	✓	✓				
Propus Informática	Porto Alegre	Rua Santa Rita, 282 – CEP 90220-220	51 3024-3568	www.propus.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. Andradas Neves, 1579 – Castelo – CEP: 13070-001	19 3213-2100	www.insignesoftware.com			✓		✓	✓
Microcamp	Campinas	Av. Thomaz Alves, 20 – Centro – CEP: 13010-160	19 3236-1915	www.microcamp.com.br				✓		✓
PC2 Consultoria em Software Livre	Carapicuíba	Rua Edéia, 500 - CEP: 06350-080	11 3213-6388	www.pc2consultoria.com	✓					✓
Savant Tecnologia	Diadema	Av. Senador Vitorino Freire, 465 – CEP: 09910-550	11 5034-4199	www.savant.com.br	✓	✓	✓			✓
Epopéia Informática	Marília	Rua Goiás, 392 – Bairro Cascata – CEP: 17509-140	14 3413-1137	www.epopeia.com.br						✓
Redentor	Osasco	Rua Costante Piovan, 150 – Jd. Três Montanhas – CEP: 06263-270	11 2106-9392	www.redentor.ind.br	✓					
Go-Global	Santana de Parnaíba	Av. Yojiro Takaoca, 4384, Ed. Shopping Service, Cj. 1013 – CEP: 06541-038	11 2173-4211	www.go-global.com.br			✓		✓	✓
AW2NET	Santo André	Rua Edson Soares, 59 – CEP: 09760-350	11 4990-0065	www.aw2net.com.br			✓		✓	✓
Async Open Source	São Carlos	Rua Orlando Damiano, 2212 – CEP 13560-450	16 3376-0125	www.async.com.br	✓					✓

Empresa	Cidade	Endereço	Telefone	Web	1	2	3	4	5	6
São Paulo (continuação)										
Delix Internet	São José do Rio Preto	Rua Voluntário de São Paulo, 3066 9º – Centro – CEP: 15015-909	11 4062-9889	www.delixhosting.com.br	✓		✓		✓	
4Linux	São Paulo	Rua Teixeira da Silva, 660, 6º andar – CEP: 04002-031	11 2125-4747	www.4linux.com.br						✓
A Casa do Linux	São Paulo	Al. Jaú, 490 – Jd. Paulista – CEP: 01420-000	11 3549-5151	www.acasadolinux.com.br				✓	✓	✓
Accenture do Brasil Ltda.	São Paulo	Rua Alexandre Dumas, 2051 – Chácara Santo Antônio – CEP: 04717-004	11 5188-3000	www.accenture.com.br				✓	✓	✓
ACR Informática	São Paulo	Rua Lincoln de Albuquerque, 65 – Perdizes – CEP: 05004-010	11 3873-1515	www.acrinformatica.com.br	✓					✓
Agit Informática	São Paulo	Rua Major Quedinho, 111, 5º andar, Cj. 508 – Centro – CEP: 01050-030	11 3255-4945	www.agit.com.br		✓	✓			✓
Altbit - Informática Comércio e Serviços LTDA.	São Paulo	Av. Francisco Matarazzo, 229, Cj. 57 – Água Branca – CEP 05001-000	11 3879-9390	www.altbit.com.br		✓	✓			✓
AS2M - WPC Consultoria	São Paulo	Rua Três Rios, 131, Cj. 61A – Bom Retiro – CEP: 01123-001	11 3228-3709	www.wpc.com.br				✓		✓
Big Host	São Paulo	Rua Dr. Miguel Couto, 58 – Centro – CEP: 01008-010	11 3033-4000	www.bighost.com.br		✓				✓
Blanes	São Paulo	Rua André Ampère, 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 Caramuru, 417, Cj. 23 – Saúde – CEP: 04138-001	11 5071-7988	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 Carubeiras, 98 – Metrô Conceição – CEP: 04343-080	11 5017-0040	www.dominiotecnologia.com.br	✓					✓
EDS do Brasil	São Paulo	Av. Pres. Juscelino Kubitschek, 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		✓				✓
Itaotec S.A.	São Paulo	Av. Paulista, 2028 – CEP: 01310-200	11 3543-5543	www.itaotec.com.br		✓	✓	✓		✓
Kenos Consultoria	São Paulo	Av. Fagundes Filho, 13, Conj 53 – CEP: 04304-000	11 40821305	www.kenos.com.br						✓
Konsultex Informatica	São Paulo	Av. Dr. Guilherme Dumont Villares, 1410 6 andar, CEP: 05640-003	11 3773-9009	www.konsultex.com.br				✓		✓
Linux Komputer Informática	São Paulo	Av. Dr. Lino de Moraes Leme, 185 – CEP: 04360-001	11 5034-4191	www.komputer.com.br				✓		✓
Linux Mall	São Paulo	Rua Machado Bittencourt, 190, Cj. 2087 – CEP: 04044-001	11 5087-9441	www.linuxmall.com.br				✓		✓
Livraria Tempo Real	São Paulo	Al. Santos, 1202 – Cerqueira César – CEP: 01418-100	11 3266-2988	www.tempreal.com.br					✓	✓
Locasite Internet Service	São Paulo	Av. Brigadeiro Luiz Antonio, 2482, 3º andar – Centro – CEP: 01402-000	11 2121-4555	www.locasite.com.br		✓				✓
Microsiga	São Paulo	Av. Braz Leme, 1631 – CEP: 02511-000	11 3981-7200	www.microsiga.com.br				✓		✓
Novatec Editora Ltda.	São Paulo	Rua Luis Antonio dos Santos, 110 – Santana – CEP: 02460-000	11 6979-0071	www.novateceditora.com.br						✓
Novell América Latina	São Paulo	Rua Funchal, 418 – Vila Olímpia	11 3345-3900	www.novell.com/brasil				✓		✓
Oracle do Brasil Sistemas Ltda.	São Paulo	Av. Alfredo Egídio de Souza Aranha, 100 – Bloco B – 5º andar – CEP: 04726-170	11 5189-3000	www.oracle.com.br						✓
Proelbra Tecnologia Eletrônica Ltda.	São Paulo	Av. Rouxinol, 1.041, Cj. 204, 2º andar Moema – CEP: 04516-001	11 5052- 8044	www.proelbra.com.br		✓		✓		✓
Provider	São Paulo	Av. Cardoso de Melo, 1450, 6º andar – Vila Olímpia – CEP: 04548-005	11 2165-6500	www.e-provider.com.br				✓		✓
Red Hat Brasil	São Paulo	Av. Brigadeiro Faria Lima, 3900, Cj 81 8º andar Itaim Bibi – CEP: 04538-132	11 3529-6000	www.redhat.com.br					✓	✓
Samurai Projetos Especiais	São Paulo	Rua Barão do Triunfo, 550, 6º andar – CEP: 04602-002	11 5097-3014	www.samurai.com.br				✓		✓
SAP Brasil	São Paulo	Av. das Nações Unidas, 11.541, 16º andar – CEP: 04578-000	11 5503-2400	www.sap.com.br				✓		✓
Simples Consultoria	São Paulo	Rua Mourato Coelho, 299, Cj. 02 Pinheiros – CEP: 05417-010	11 3898-2121	www.simplesconsultoria.com.br				✓		✓
Smart Solutions	São Paulo	Av. Jabaquara, 2940 cj 56 e 57	11 5052-5958	www.smart-tec.com.br				✓		✓
Snap IT	São Paulo	Rua João Gomes Junior, 131 – Jd. Bonfiglioli – CEP: 05299-000	11 3731-8008	www.snapit.com.br				✓		✓
Stefanini IT Solutions	São Paulo	Av. Brig. Faria Lima, 1355, 19º – Pinheiros – CEP: 01452-919	11 3039-2000	www.stefanini.com.br				✓		✓
Sun Microsystems	São Paulo	Rua Alexandre Dumas, 2016 – CEP: 04717-004	11 5187-2100	www.sun.com.br		✓				✓
Sybase Brasil	São Paulo	Av. Juscelino Kubitschek, 510, 9º andar Itaim Bibi – CEP: 04543-000	11 3046-7388	www.sybase.com.br						✓
The Source	São Paulo	Rua Marquês de Abrantes, 203 – Chácara Tatuapé – CEP: 03060-020	11 6698-5090	www.thesource.com.br				✓		✓
Unisys Brasil Ltda.	São Paulo	R. Alexandre Dumas 1658 – 6º, 7º e 8º andares – Chácara Santo Antônio – CEP: 04717-004	11 3305-7000	www.unisys.com.br		✓		✓		✓
Utah	São Paulo	Av. Paulista, 925, 13º andar – Cerqueira César – CEP: 01311-916	11 3145-5888	www.utah.com.br				✓		✓
Visuelles	São Paulo	Rua Eng. Domicio Diele Pacheco e Silva, 585 – Interlagos – CEP: 04455-310	11 5614-1010	www.visuelles.com.br				✓		✓
Webnow	São Paulo	Av. Nações Unidas, 12.995, 10º andar, Ed. Plaza Centenário – Chácara Itaim – CEP: 04578-000	11 5503-6510	www.webnow.com.br		✓		✓		✓
WRL Informática Ltda.	São Paulo	Rua Santa Ifigênia, 211/213, Box 02– Centro – CEP: 01207-001	11 3362-1334	www.wrl.com.br		✓				✓
Systech	Taquaritinga	Rua São José, 1126 – Centro – Caixa Postal 71 – CEP: 15.900-000	16 3252-7308	www.systech-td.com.br		✓	✓			✓
2MI Tecnologia e Informação	Embu	Rua José Bonifácio, 55 – Jd. Independência – CEP: 06826-080	11 4203-3937	www.2mi.com.br				✓	✓	✓

Calendário de eventos

Índice de anunciantes

SERVIÇOS

Evento	Data	Local	Website
Riowir eless	15d eab ril	Riod eJan eiro, RJ	www.networkeventos.com.br/evento
CONSOLIP	15a17d eab ril	Araras,SP	www.consolip.com.br
CNASI	18e19d emaio	Braslia,DF	www.cnasi.com.br
FreeS oftwareBa hia	28e29d emaio	Salvador,B A	www.networkeventos.com.br
FISL	24a27d eju nho	PortoA legre, RS	www.fisl.softwarelivre.org
Futurecom2009	13a16d eou tubro	SoP aulo,S P	www.futurecom2009.com.br

Empresa	P g.
Locaweb	2, 84
HP	7
Sun Microsystem	9
Caixa Econômica Federal	11
Plus server	13
UOL	15
IDETI	21
Linux Pocket Pro	23
CNASI	27
Senac	29
LPI	39
Watchguard	41
FISL	69
Fectura	73
Bull	83

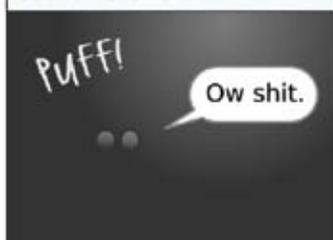
Nerdson – Os quadrinhos mensais da Linux Magazine

NERDSON
NÃO VAI À ESCOLA

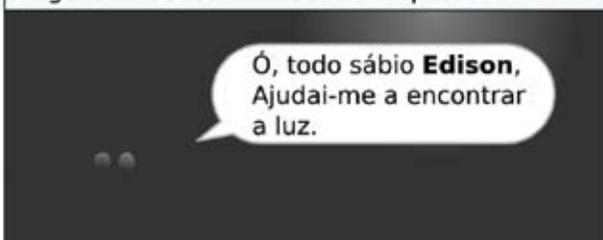
Breu bits

<http://nerdson.com>

Quando falta energia, os nerds perdem a razão de sua existência...



No breu total, assim como os homens normais, os nerds voltam ao passado, revisitam suas origins e reencarnam seus antepassados...



...e adotam suas mais primitivas técnicas...



Linux Magazine
A REVISTA DO PROFISSIONAL DE TI

Ligue já e garanta sua assinatura da Linux Magazine !!!

Informações:
11 4082-1300
info@linuxnewmedia.com.br



DECISÕES CERTAS PODEM MUDAR O RUMO DE SUA CARREIRA

Inclua em seu currículo a principal
certificação Linux no mundo – LPI.

Em tempos de crise, soluções de código aberto – como o Linux – se destacam na adoção por empresas de todos os tamanhos, como solução ideal para aumentar eficiência nos negócios e reduzir custos. Atualmente há no mercado uma carência por profissionais certificados para atender a essa demanda crescente. Aproveite essa oportunidade e inclua em seu currículo a principal certificação Linux no mundo.

As datas de realização das provas são:

18/04/2009 São Paulo

04/07/2009 São Paulo

03/10/2009 São Paulo



Inscrições e mais informações:

www.linuxmagazine.com.br/lpi

Tel (11) 4082-1300

Na Linux Magazine #54

DESTAQUE

Servidores de arquivos

Um dos maiores ativos de toda empresa é sua coleção de arquivos. Sejam projetos, documentos, músicas, livros, planilhas, filmes, softwares ou código-fonte, toda empresa precisa de um local para armazenar com segurança e velocidade seus dados. Fazer uso das melhores técnicas e ferramentas para garantir a qualidade do serviço de arquivos – incluindo segurança e velocidade, claro – é responsabilidade do administrador do servidor, mas todos sabemos que não há muito o que aprender na área de servidores de arquivos...

Ledo engano. Na Linux Magazine 54, vamos apresentar técnicas e ferramentas para você manter seus servidores de arquivos sempre em funcionamento e com toda a confiabilidade que o hardware oferece. Vamos apresentar os fundamentos de uma boa configuração de sistemas de arquivos, mostraremos como configurar o Samba em clusters de alta disponibilidade e vamos ainda comparar o desempenho de diferentes soluções de armazenamento por Fiber-Channel, além de analisar a confiabilidade dos vários níveis de RAID e avaliar nove ferramentas de backup profissionais. ■

SEGURANÇA

Laptop perdido e achado

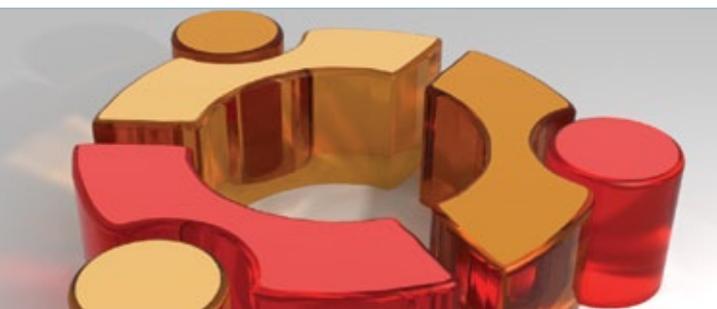
Laptops costumam conter informações estratégicas das empresas. O roubo dessas informações é uma ameaça constante a todos que utilizam essa conveniente forma de computação móvel. Conheça um projeto que rastreia o seu laptop em qualquer local do planeta e aumente significativamente a probabilidade de recuperar máquinas roubadas antes de sofrer o prejuízo. ■



Na EasyLinux #15

Ubuntu novo!

A próxima edição da Easy Linux vai explorar o Ubuntu 9.04. Vamos mostrar o que há de novo nessa primeira versão de 2009, quais as melhorias, o que a Canonical aprontou e como anda a comunidade em torno da distribuição Linux mais amigável da atualidade. ■



Monitores gigantes

Os monitores LCD de 19 polegadas e maiores já têm preços bem melhores que há um ano. Será que já chegou o momento de você comprar aquele monitor cinematográfico? Quais são as vantagens e desvantagens do LCD em relação

aos antigos monitores de tubo? Até que ponto 21 polegadas valem mais que 19? Na Easy Linux 15, vamos explicar a tecnologia por trás da parte mais visível – literalmente – do computador. ■



Primeiro Super-Computador Híbrido da Europa



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

O primeiro da Europa

Potência total acumulada de 295 Teraflops

Produção

8544 Núcleos (CPU's) Intel®

103 Teraflops

Pesquisa

46 080 Núcleos (CPU's) NVIDIA

192 Teraflops



Architect of an Open World™

O AMBIENTE OPEN SOURCE IDEAL PARA SEUS PROJETOS NA INTERNET.



```
class Payment < ActiveRecord::Base
  belongs_to :order
  after_save :check_payments
  after_destroy :check_payments
  private
  def check_payments
    return unless order.checkout_complete
    order.pay! if order.payment_total >=
order.total
  end
end
```



ESTA PARTE DO ANÚNCIO É EXCLUSIVA PARA QUEM É EXPERT.

A maior empresa de serviços de internet da América Latina oferece planos de hospedagem com programação Ruby on Rails™, Python/Django, PHP4/PHP5 e JVM Dedicado. Além disso, tem Instalador de Aplicativos, Construtor de Sites, Comércio Eletrônico, e-mail com antivírus e antispam, SSL dedicado e cupons no Google AdWords e BuscaPé a partir de **R\$ 20/mês**.

➤ E para você que quer mais performance e autonomia, conheça também o Cloud Mini, com todas as vantagens do Cloud Computing por um preço realmente "mini".

Exercite seu poder de decisão: acesse www.locaweb.com.br.

LOCAWEB

