LINUX NEW MEDIA
The Pulse of Open Source

55 Junho 2009

LINUX MAGAZINE

A REVISTA DO PROFISSIONAL DE TI

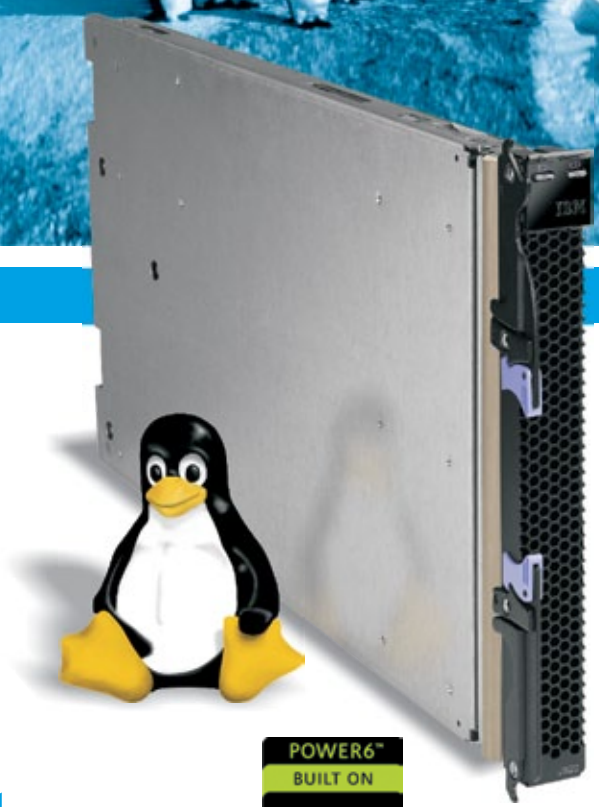
o melhor DATA CENTER

VOCÊ SABE QUAL DATA CENTER ESCOLHER PARA ABRIGAR SEU SERVIDOR? PESQUISAMOS AS OFERTAS NACIONAIS EM VÁRIAS CATEGORIAS DE PREÇOS E SERVIÇOS. p.27

VEJA TAMBÉM NESTA EDIÇÃO:

WWW.LINUXMAGAZINE.COM.BR

Turbine suas aplicações **Linux** com todo o poder dos **processadores Power6**



Processadores IBM Power6:

- ☑ Melhores Benchmark em performance para aplicações Linux e Web;
- ☑ Inclui o SW de virtualização mais poderoso do mercado, PowerVM, migre facilmente aplicações Linux com o LX86;
- ☑ Utilizado para aplicações de missão crítica nas maiores empresas do mundo;
- ☑ Indicado para consolidação de aplicações com potencial redução de custo em até 60%.

IBM Power Systems

Soluções para um planeta mais inteligente!

POWER6™ BUILT ON Power™

Venha conhecer o Servidor Risc líder de mercado!

IBM Business Partner

INGRAM MICRO®

0800.14 48 49 | www.ingrammicro.com.br | reservaopplow@ingrammicro.com.br

Av. Francisco Matarazzo, 1500 - Torre New York - Cj. 31 - 1° 2° 3° andar - CEP 05001-100 - Água Branca - São Paulo - SP

Expediente editorial

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

Editor
Pablo Hess
phess@linuxmagazine.com.br

Revisora
Aileen Otomi Nakamura
anakamura@linuxmagazine.com.br

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

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

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

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

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

Amy Phalen (Estados Unidos)
aphalen@linuxmagazine.com

Hubert Wiest (Outros países)
hwiest@linuxnewmedia.de

Gerente de Circulação
Claudio Bazzoli
cbazzoli@linuxmagazine.com.br

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

Linux Magazine é publicada mensalmente por:

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

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

Atendimento Assinante

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

ISSN 1806-9428 **Impresso no Brasil**

INSTITUTO VERIFICADOR DE CIRCULAÇÃO

EDITORIAL

Decisões de migração

Prezados leitores,

Estamos vendo atualmente o deslocamento de uma parte significativa da infraestrutura de TI das empresas para os data centers. Terceirizar a infraestrutura de TI é uma boa ideia: ao operar grandes números de máquinas de forma centralizada, os data centers são capazes de oferecer poder de processamento e espaço de armazenamento a preços menores do que as empresas jamais conseguiriam. Porém, essa nova tendência traz, como de costume, novos desafios.

O mais marcante é a conectividade, item ainda extremamente precário no Brasil. Conexões de rede de nível corporativo, com acordos de nível de serviço acima dos 99,95% e velocidades superiores a 10 megabits por segundo, ultrapassam facilmente a barreira das dezenas de milhares de reais. Porém, são absolutamente necessárias para conectar o escritório ao data center.

Os cuidados com a segurança também são importantes, já que entre o escritório e o data center os dados circulam visíveis para eventuais bisbilhoteiros. Da mesma forma, uma nova cultura é necessária para gerenciar os servidores, agora remotos, que não podem ser facilmente desligados pelo administrador. Vale a pena considerar formas de acesso *out-of-band* para gerenciar o hardware remotamente.

Decidir quais serviços migrar para o data center não é fácil, nem há fórmulas já estabelecidas para pautar essa escolha, que envolve usuários, administradores e gestores do negócio.

Esta edição foi escrita justamente para ajudá-los nesse processo. Boa leitura e boas escolhas. ■

Pablo Hess
Editor

ÍNDICE

CAPA

COLUNAS

NOTÍCIAS

CORPORATE

ANÁLISE

TUTORIAL

REDES

SEGURANÇA

PROGRAMAÇÃO

SERVIÇOS

Emails para o editor

Permissão de Escrita

Se você tem dúvidas sobre o mundo Linux, críticas ou sugestões que possam ajudar a melhorar a nossa revista, escreva para o seguinte endereço: ***cartas@linuxmagazine.com.br****. Devido ao 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.*

Scripts

Em primeiro lugar parabéns pela ótima revista. Me ajuda muito em minha atualização e formação como profissional de TI.

Eu sou técnico de suporte júnior em uma conhecida empresa de contact center do Brasil. Presto suporte para usuários de um provedor de acesso à Internet e fiquei indignado quando soube em meu treinamento que nós não prestamos suporte para clientes que possuem o sistema Linux. O argumento inicialmente é até válido: "Devido às diversas versões e à possibilidade de alterar o sistema, existem inúmeras dificuldades na hora de prestar o suporte para esse tipo de sistema operacional".

Apesar de ser iniciante nos estudos sobre Linux, sei da possibilidade da criação de scripts para automatizar algumas tarefas. Acredito que este seja o drama de muitos usuários Linux. Seria esta uma possível matéria para a revista que é referência no mundo Open Source? Fica aí minha dica.

Marcio Leite

Resposta

Muito obrigado pelos elogios, Marcio. De fato, prestar suporte a uma variedade muito grande de sistemas operacionais é complicado. Porém, muitos usuários do sistema do pinguim já enfrentaram a experiência de pedir uma informação técnica a respeito do provedor e receber instruções específicas do sistema Windows. Questionamentos sobre o endereço IP de um servidor DNS, por exemplo, podem facilmente resultar na sugestão de reinício do computador por parte do suporte técnico.

Os scripts podem, sim, facilitar tarefas de configuração, conexão etc. No entanto, o que os usuários Linux esperam é que o suporte técnico do provedor abranja justamente os aspectos técnicos do serviço provido. Quando uma pergunta sobre conectividade leva a considerações sobre determinado Service Pack, fica claro que o suporte está indo além de seu domínio de ação.

Ademais, creio que a melhor recomendação aos provedores de acesso seja concentrar-se em uma única distribuição Linux, justamente para evitar as dificuldades provenientes da variedade de sistemas. Com a solução funcionando em uma única distribuição, fica muito mais fácil a própria comunidade obter dessa distribuição os dados necessários para fazer com que o serviço funcione em outros sistemas Linux. ■

COLUNA

Coluna do Klaus

Pergunte ao Klaus!

O professor Klaus responde as mais diversas dúvidas dos leitores.

Atalhos no Eee PC

Como faço para ligar e desligar, no meu Eee PC, o leitor de cartões de memória, a rede sem fio e a webcam? As combinações do teclado parecem não funcionar.

Resposta

Os kernels 2.6.28 e posteriores possuem suporte ao hardware específico do Eee PC e de outros sistemas por meio do diretório virtual `/sys/`. Escrevendo nos arquivos `/sys/devices/platform/eeepc/camera`, `/sys/devices/platform/eeepc/cardr` e `/sys/class/rfkill/rfkill0/state` é possível controlar partes do computador. Para obter a configuração atual, use o comando `cat`:

```
$ cat /sys/devices/platform/eeepc/camera
1
```

Neste exemplo, o valor 1 retornado indica que a webcam está ligada e portanto disponível para os programas (contanto que o driver *uvcvideo* esteja instalado), então é possível usar o comando `mplayer tv://` para exibir o vídeo capturado pela webcam.

Para alterar o estado de um dispositivo, use o comando `echo` (mas note que é preciso fazer isso como usuário root devido às permissões de escrita no diretório `/sys/`):

```
echo 1 > /sys/class/rfkill/rfkill0/state
```

Esse comando ativa a placa de rede sem fio embutida e também ativa o LED azul. O *daemon* do *udev*, com isso, deve carregar automaticamente o driver Wi-Fi (*ath5k*), e o *Network Manager* começará a procurar redes disponíveis. Essa técnica não é específica para o Eee PC; ela pode funcionar em outros notebooks com novos chipsets Wi-Fi da Atheros.

O motivo para algumas combinações de teclado não funcionarem com algumas distribuições é sua configuração padrão em `/etc/acpi/`, que às vezes é muito conservadora. Então, pode ser necessário adicionar essas combinações observando os eventos ACPI durante o pressionamento de uma tecla ou botão e inserindo em `/etc/acpi/` alguns scripts que empreguem esses eventos para acionar os itens de hardware.

MTU

Recentemente um cliente meu enfrentou um problema de conectividade. Ele conseguia acessar o Google e fazer buscas, mas ao clicar em qualquer link, todos os navegadores testados exibiam "Esperando...". Esse problema já aconteceu quando instalei outras distribuições nessa mesma máquina. E o mais chato era que a rede funcionava perfeitamente com o Windows no mesmo computador.

Hoje li que a configuração do MTU pode causar problemas de longas esperas como essas que meu cliente está experimentando. Segundo li, alguns provedores usam valores de MTU diferentes do padrão (1500), e então somente alguns sites funcionam.

Resposta

O provedor não deveria fornecer uma configuração automática caso ele use um MTU diferente? Usar um MTU menor (`ifconfig ethX mtu 1100`, por exemplo) pode ajudar em alguns ambientes, caso o outro lado da conexão fique confuso com o MTU padrão. Já vi serviços ISDN, por exemplo, usarem um valor de 1450. De qualquer forma, você está correto: em certas situações, alterar o MTU pode corrigir o comportamento inexplicavelmente lento da rede. ■

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

WatchGuard™

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

SODIC
SINCE 1944

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

COLUNA

Coluna do Charly

Blog fácil

Às vezes, Charly tem que sair do escritório e levar sua vida normal. Nessas horas, é bom ter em mãos as melhores ferramentas.

Eventualmente, até mesmo o Scotty de Jornada nas Estrelas [1] é incapaz de evitar as tarefas que não são sua especialidade, independentemente de suas reclamações, "Eu sou um mecânico, não um médico". As soluções que ele usa para salvar a Enterprise do que parecem centenas de episódios de perda de controle em dobra espacial são pouco ortodoxas.

Com relação às ferramentas, Scotty tem uma opinião clara: "Use sempre a ferramenta adequada. Se ela não estiver disponível, use um martelo".

Dobra 2

Quando me pedem para criar sites, eu sinto empatia por Scotty. Sou administrador de sistemas, não webdesigner!

O fato de usar o *Vi* para criar meu código HTML dá ao resultado uma aparência ascética e minimalista. O código faz o que se espera, mas o visual é feio. Scotty me amaria por isso.

Às vezes, dobra 1 simplesmente não é suficiente. Recentemente, precisei de uma página semelhante a um blog, que oferecesse aos usuários a opção de comentar parte do conteúdo. O mecanismo de blog *Serendipity* [2] é suficientemente flexível para servir como CMS e garante resultados rápidos.

O *S9y*, como a comunidade do Serendipity costuma abreviá-lo, requer pacotes PHP relativamente recentes e uma conexão com um banco de dados. Após terminar de descompactar o código-fonte, copie-o para um diretório no servidor web, entre nesse diretório e faça a instalação, que é realizada com perfeição num navegador.

Depois de instalado, o S9y parece com o que esperaríamos do visual de um blog; porém a interface de administração oferece vários plugins para os mais variados fins.

Com uns poucos plugins, é fácil inserir código HTML ou PHP externo na estrutura da página. Preciso dessa função com frequência, para integrar gráficos do RRD ou resultados do Nagios. Acrescentei um tempero sob a forma de fóruns de discussão, galerias, conectores para incontáveis mensageiros instantâneos e outras dezenas de utilidades – todas obtidas diretamente do diretório de plugins.

Isso não significa que eu tenha negligenciado a questão da segurança, no entanto. A equipe do desenvolvedor Garvin Hicking adora código limpo, tanto que marca os plugins com alertas inconfundíveis de que o plugin parece mais indicado para atirar no seu pé.

Amigo do advogado

O sistema de comentários, importante na minha aplicação, precisava de um recurso de dupla adesão em sua função `subscribe` desde o Serendipity 1.4. Infelizmente, sabe-se que advogados sagazes processam nesses casos, pois, em sua opinião, emails de comentários que você esteja acompanhando são o equivalente legal de uma *newsletter*, e newsletters precisam de dupla adesão. Scotty diria apenas: "Eu sou um mecânico, não um advogado". ■

Mais informações

[1] Montgomery Scott, Star Trek: http://pt.wikipedia.org/wiki/Montgomery_Scott

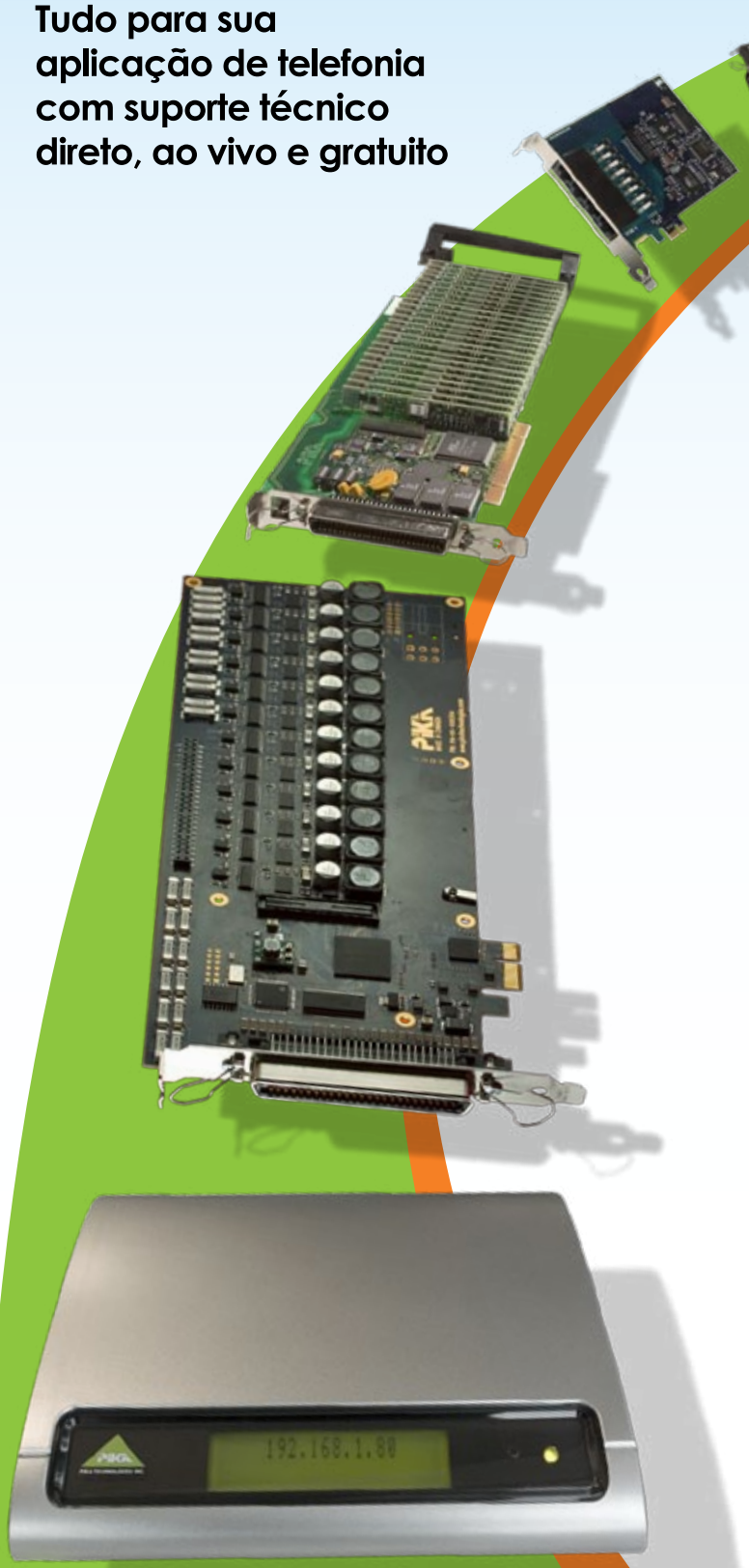
[2] Serendipity: http://www.s9y.org

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

PIKA

Tudo para sua aplicação de telefonia com suporte técnico direto, ao vivo e gratuito

PIKA TECHNOLOGIES INC.



WARP appliance para Linux / Asterisk

- Processador embarcado
- Ambiente de desenvolvimento aberto
- Com suporte a Asterisk, Freeswitch e outras plataformas de Código Aberto
- Módulo GSM disponível em 2010 – basta instalar seu SIM card!

Placas CTI (HMP e DSP)

- Analógicas (FXO ou FXS) e Digitais E1 (ISDN, R2/MFC) e T1 (ISDN)
- Licenças atualizáveis em campo via sofware, reduzindo as taxas de importação.

Aplicações de Voz

- Cancelamento de eco
- VoIP
- Geração/detecção de tons
- Conferência
- Suporte nativo a FAX - T.30 e v.34 (alta velocidade)

Kit de Desenvolvimento

- API de baixo nível - para controle total - e de alto nível - para desenvolvimento rápido
- Sem custo na compra de qualquer hardware
- Suporte a Windows ou Linux (mesmo código fonte)

vendas@pikatech.com

www.pikatechnologies.com

COLUNA

Coluna do Zack

Crônicas do kernel

Mais uma aula sobre o desenvolvimento do kernel, por Greg Kroah-Hartman.

O que é a árvore staging?

Greg Kroah-Hartman ofereceu recentemente esclarecimentos sobre a natureza da árvore *staging* (que significa "ensaio"), pois seu papel mudou; além disso, aparentemente havia certa confusão sobre o assunto.

A árvore staging, segundo ele, era o diretório `drivers/staging/` do kernel oficial. Códigos submetidos para esse diretório no repositório git *linux-next* seriam enviados diretamente para Linus durante a janela de inclusão e seriam incluídos na próxima versão oficial do kernel com pouca ou nenhuma objeção dele.

> ***As restrições impostas pela árvore staging aos projetos servem para assegurar que todo código preserve a estabilidade do kernel.***

Os projetos adequados à árvore staging são drivers e sistemas de arquivos que não requerem alterações de código em qualquer outro local da árvore (ou seja, são *patches* independentes). As únicas exceções a isso são: o firmware pode (e deve) residir no diretório `firmware/`, símbolos podem ser exportados do código principal do kernel caso o mantenedor do subsistema relevante aprovar, e a documentação pode residir no diretório `Documentation/`, embora isso não seja considerável.

A vantagem de colocar o código na staging é que ele existe na árvore principal do kernel; portanto, tem à disposição todo o universo de usuários do kernel para testá-lo enquanto apresenta apenas um risco mínimo à estabilidade do kernel. Ela atende uma necessidade que foi resolvida de várias formas ao longo dos anos: como os desenvolvedores poderiam ter seu código testado por usuários suficientes para torná-lo aceitável na árvore principal antes de finalmente ser aceito nela?

As restrições impostas pela árvore staging aos projetos servem para assegurar que todo código preserve a estabilidade do kernel e esteja rumando diretamente para fora dessa árvore e para dentro da árvore principal. Portanto, qualquer projeto que entre na staging precisa ser bem mantido, seja pela pessoa que o submeteu, seja por um voluntário disposto a cuidar dele. A staging não é o local para "despejar código e fugir", como Greg disse. Qualquer código que resida na staging "contamina" os logs ao ser executado (isto é, exibe uma mensagem informando que executou código da staging).

Relatórios de erros de um kernel contaminado têm menor probabilidade de encontrar alguém que queira depurá-lo. Se você estiver trabalhando com código da staging, a maior parte do ônus da depuração fica para você mesmo, e se você pensa que o erro não foi causado pelo seu código, é preciso reproduzi-lo num kernel não contaminado e submeter o relatório. Então, haverá vários hackers dispostos a ajudá-lo.

Tudo isso tem o propósito de isolar o desenvolvimento da staging daquele do restante do kernel. Como desenvolvedor de código da staging, você tem o benefício de um público potencial de milhões de usuários, mas a responsabilidade de lidar com relatórios desses usuários, assim como o comportamento do seu próprio código, cabe a você.

Para mim, parece uma solução muito elegante para um problema que assola os desenvolvedores do kernel há anos; sem dúvida ela vai melhorar ao longo do tempo. ■

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.

RIMATRIX5®
DRIVING IT-PERFORMANCE

A solução de alta perfomance - Eficiente, flexível e segura

Para pequenos negócios ou grandes empresas, **RimatriX5** atende as suas necessidades com soluções flexíveis e seguras.

Racks: para servidores e rede com maior espaço interno, design diferenciado, flexibilidade e segurança.

Energia: soluções seguras e eficientes (até 95%) para distribuição de energia e fornecimento contínuo.

Climatização: soluções tradicionais e para alta densidade de elevada eficiência.

Segurança: Soluções inovadoras com tecnologia wireless e de captura de vídeo.

Monitoramento & Gerenciamento remoto: monitorar, medir e controlar para máxima disponibilidade e eficiência energética.

Rittal. Rumo à perfeição.

FRIEDHELM LOH GROUP

Rittal Sistemas Eletromecânicos Ltda.
Av. Cândido Portinari, 1174 | Vila Jaguara | São Paulo . SP | Brasil | CEP: 05114.001
www.rittal.com.br | info@rittal.com.br | Fone: +55 11 3622.2377 | Fax: +55 11 3622.2399

RITTAL®

COLUNA

Coluna do Augusto

Sobre softwares livres e pica-paus

Todo software tem problemas, mas talvez os consumidores mereçam garantias.

A conhecida Segunda Lei de Weinberg já nos adverte há décadas: se os empreiteiros construíssem prédios do jeito que os desenvolvedores de software criam seus programas, o primeiro pica-pau que aparecesse destruiria a civilização.

E embora seja uma frase humorística, ela expressa uma verdade muitas vezes demonstrada: as garantias oferecidas ao consumidor junto às licenças de programas de computador que estes adquirem não encontram paralelo no mercado.

Ninguém aceitaria que um forno de microondas recém-comprado e em perfeitas condições costumeiramente travasse e tivesse que ser reinicializado, nem que um carro pudesse subitamente parar de responder a comandos do motorista, voltando ao normal 30 segundos depois.

> ***Ninguém aceitaria que um forno de microondas recém-comprado e em perfeitas condições costumeiramente travasse e tivesse que ser reinicializado.***

Mas praticamente todo usuário de computador está sujeito a este tipo de acontecimento, diariamente, e quem lhe forneceu o software (seja ele livre ou proprietário) oferece pouca ou nenhuma garantia sobre as consequências, como poderão atestar todos que já perderam um documento importante (ou um disco inteiro) por uma falha de programação em aplicativos ou mesmo no sistema operacional.

Essa situação varia pouco em todo o mundo, e os consumidores já estão acostumados com uma realidade em que – diferentemente do que ocorre com carros, edificações e serviços em geral – pode-se contar como certo que a maioria dos softwares adquiridos terá algum número de falhas, que a solução dessas falhas muitas vezes depende de procedimentos cuja iniciativa e execução dependem do usuário, e que o desenvolvedor eventualmente poderá optar por simplesmente não corrigir determinados problemas – algo que pode ser menos grave no caso do código aberto, mas continua sendo um problema potencialmente sério.

Mas algo pode mudar neste cenário. No início de maio foi anunciado que a União Européia está estudando medidas que levariam aos consumidores de software às mesmas garantias obrigatórias que consideramos naturais em tantos outros produtos, e que nos levariam a poder ter razoável expectativa quanto ao funcionamento dos softwares cujas licenças adquirimos, pois seus fornecedores passariam a ter responsabilidade pelas consequências do seu eventual mau funcionamento.

Para o Software Livre, esta medida traz novos desafios – especialmente aos distribuidores, que hoje não têm maiores preocupações em agregar uma série de programas em variados graus de estabilidade e oferecê-los a um mercado ávido por consumi-los. Eles passarão a ter de enfrentar o dilema de obter garantias dos desenvolvedores de cada pacote (que podem não estar interessados) ou arcar eles próprios com o ônus de oferecê-las a seus consumidores, o que acrescentaria custos bastante consideráveis aos produtos baseados em softwares livres.

Para o consumidor em geral, entretanto, trata-se de uma melhoria (que terá seu preço), e possivelmente constitui uma tendência inevitável a longo prazo. Se você desenvolve ou distribui comercialmente softwares livres, vale a pena manter-se informado a respeito e se preparar! ■

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.

COLUNA

Coluna do Kurt

OSSEC

Veja como monitorar e bloquear ataques sem levantar um dedo.

Uma das coisas que eu aprendi sobre a segurança de computadores é o log. Se você não tem logs, tentar reconstruir o que aconteceu quando algo quebrar, ou quando alguma máquina for invadida, é quase impossível. A segunda coisa que aprendi foi que é preciso centralizar os logs; essa é a única forma de obter um panorama completo da situação e garantir que um agressor não consiga simplesmente apagar os logs de uma máquina comprometida, deixando o administrador sem material para analisar. Mas nenhum desses aprendizados chamará a atenção do administrador para um agressor ou, mais importante ainda, impedirá que um agressor entre. Eles simplesmente oferecerão algo para observar quando o administrador descobrir que foi invadido. Para isso, é necessário um ser humano no processo, certo? Bem, é preciso ou um ser humano ou algum software inteligente.

Não seria ótimo se pudéssemos monitorar os arquivos de log críticos (como de email e web) e realmente ter um programa para reagir a ataques, notificar o administrador e até bloquear futuros acessos do agressor? Bem, você não é o único. O brasileiro Daniel B. Cid é o líder do desenvolvimento do projeto OSSEC, um esforço para criar um sistema de código aberto para detecção de intrusos com base nas máquinas [2]. O OSSEC usa uma técnica tradicional de servidor e agente: o administrador instala o software agente em cada sistema a ser monitorado e um servidor central coleta todos os dados e envia alertas. Além disso, o projeto OSSEC lançou uma interface web; porém, ela só é capaz de exibir relatórios, e não pode ser usada para configurar o sistema.

Instalação

Na instalação do OSSEC há três opções. A opção *server* (servidor) permite usar o OSSEC para monitorar a si mesmo e coletar alertas de outros sistemas. A opção *agent* (agente) simplesmente monitora eventos locais e informa ao servidor qualquer acontecimento interessante. A opção *local* realiza o monitoramento localmente e pode enviar alertas por email, mas não escuta agentes remotos (então é a opção certa caso você só tenha um servidor ou queira testar o OSSEC). Simplesmente baixe o pacote do OSSEDC e descompacte-o num diretório:

```
# wget http://www.ossec.net/files/ossec-hids-2.0.tar.gz
# tar -zxf ossec-hids-2.0.tar.gz
# cd ossec-hids-2.0
# ./install.sh
```

Agora, basta escolher o idioma, o tipo de servidor e informar se você deseja executar o *daemon* de verificação de integridade, o mecanismo de detecção de rootkits, ativar a resposta ativa e ativar o firewall para bloquear ataques. Se você estiver configurando o sistema como agente, também é preciso apontá-lo para o servidor e colar nele a chave do agente. Ela é uma longa cadeia de caracteres usada para garantir a segurança nas comunicações entre cada agente e o servidor, evitando a injeção de mensagens falsas e assim por diante. Por que é importante evitar que esse tipo de mensagem forjada seja enviada ao servidor?

Cuidado

Se um agressor conseguir realizar ataques forjados ou falsos e um sistema bloquear IPs ou usuários por conta disso, o agressor conseguirá facilmente bloquear sistemas legítimos e "trancar usuários do lado de fora". Na pior das hipóteses, pode ser preciso invadir seu próprio sistema caso as contas estejam bloqueadas, e é por isso que a maioria dos HIDS e NIDS suportam listas brancas. Os administradores simplesmente criam uma lista de máquinas e redes críticas.

APRESENTAMOS O NOVO LIMITE DOS PLANOS DE HOSPEDAGEM UOL HOST.

100.000 CLIENTES JÁ UTILIZAM!

A PARTIR DE
R$ 7,90* MÊS
HOSPEDAGEM ILIMITADA

HOSPEDAGEM ILIMITADA UOL HOST.

O UOL HOST acaba de lançar seus novos planos, sem limites de transferência de dados e sem limite de domínios, com preços a partir de R$ 7,90*. Além disso, suporte técnico, construtor de sites, e-mails e o mais moderno Painel de Controle para administração da sua hospedagem. Agora o céu é o limite para a audiência de seu site.

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

UOL HOST
QUALIDADE EM SERVIÇOS WEB

*Nos primeiros 3 meses, depois R$14,90. Promoção válida até 30/06/2009.

Obviamente, determinar quais máquinas são críticas depende da configuração exata (servidores DNS, de email e web, de autenticação, roteadores etc. são um bom começo). No OSSEC, a lista branca fica no arquivo `ossec.conf` (por padrão, em `/var/ossec/etc/`), e é possível especificar máquinas ou redes individuais:

```
<global>
   <white_list>127.0.0.1</white_list>
   <white_list>1.2.3.4</white_list>
   <white_list>10.0.0.0/8</white_list>
   <white_list>192.168.0.0/16</white_list>
</global>
```

Rodando...

O OSSEC traz seu próprio programa de controle, chamado `ossec-control`. Além disso, quando instalado num sistema Red Hat Enterprise Linux ou CentOS, são criados scripts de inicialização em `rc.d/`, que permitem que os serviços do OSSEC sejam controlados pelo utilitário padrão `chkconfig`. Quando o OSSEC estiver em execução, deve ser possível ver diversos programas em execução.

Os processos de monitoramento geralmente precisam ser executados pelo usuário root:

```
USER   PID   COMMAND
ossecm 17381 .../ossec-maild
root   17385 .../ossec-execd
ossec  17389 .../ossec-analysisd
root   17393 .../ossec-logcollector
root   17405 .../ossec-syscheckd
ossec  17409 .../ossec-monitord
```

Agente

Com o servidor em execução, é hora de encaminhar para ele o restante dos logs. Simplesmente instale o OSSEC em todas as máquinas que precisarem ser monitoradas e escolha a opção de instalação de agente, naturalmente.

Durante a instalação, serão perguntados o IP do servidor e algumas opções padrão relativas ao monitoramento. Ao término desse processo, será preciso criar e importar a chave do agente, o que é feito pelo programa `manage_agents`. No servidor, basta adicionar o agente.

Depois de terminar isso, extraia a chave de um agente particular, copie-a e cole-a (prefira logins remotos via SSH). Use o comando `manage_agents` no agente para importar a chave. O processo é semelhante no Windows, mas foi criada uma interface gráfica para facilitar a vida do administrador (felizmente, as versões em linha de comando ainda estão disponíveis e permitem o gerenciamento remoto via scripts na linha de comando).

Por padrão, o OSSEC monitora todos os arquivos em `/etc/`, `/bin/`, `/sbin/`, `/usr/bin/` e `/usr/sbin/` (essencialmente, as vísceras de quase qualquer sistema) e vários arquivos de log de daemons de rede (`named`, `smbd`, `myusql`, `telnetd` etc.).

Para modificar os diretórios a ser monitorados ou para acrescentar novas regras aos serviços de monitoramento, basta editar o arquivo `ossec.conf`, que usa um formato no estilo XML bem autoexplicativo.

Interface web

Agora que o OSSEC já está configurado e em ação, protegendo sua rede, o que você deve fazer? Um recurso que eu adoro no OSSEC são os relatórios. Por exemplo, é possível gerar relatórios em texto relativos à maior atividade por IP, nomes usados em tentativas de login e assim por diante.

Claro que um relatório em texto não deve impressionar seu chefe, mas felizmente existe uma solução. A interface web do OSSEC permite consultas posteriores, mas infelizmente não suporta a configuração do servidor ou dos agentes (para isso ainda é preciso ater-se à linha de comando). Além disso, a interface web do OSSEC permite visualizar de uma única vez o estado do servidor e dos agentes.

Conclusão

Um dos maiores problemas da segurança é a quantidade de esforço de configuração e manutenção contínuos que o problema exige. O OSSEC oferece um grau de segurança e proteção ativa com custo mínimo de configuração e baixa manutenção. Faltam nele alguns recursos que eu adoraria ver (como me informar o que mudou num arquivo em vez de apenas me dizer que o arquivo foi alterado) e também alguns recursos de usabilidade (como gerenciamento de alterações e configuração em massa), mas, com essa enorme simplicidade de configuração e gerenciamento, acho que ainda vale a pena. ■

Mais informações

[1] OSSEC: http://www.ossec.net/

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.

Coluna do Alexandre

Solaris x OpenSolaris

Solaris e OpenSolaris são sistemas diferentes. Entenda por que e em quais aspectos.

Nos últimos meses, o OpenSolaris tem ganhado destaque na comunidade do Código Aberto, pois é um produto derivado do Solaris 10 e tem todo o seu código e desenvolvimento conduzidos por pessoas brilhantes, dispostas a contribuir com uma proposta em que todos acreditam. A Sun, de alguns anos para cá, tem disponibilizado todos os seus produtos na forma binária, para que os interessados possam baixar e fazer testes, junto com a documentação.

Antes de lançar o Solaris 10 de forma oficial, a Sun abriu o código do *Dtrace*, ferramenta de análise de desempenho e resolução de problemas. Com os dois, os desenvolvedores poderiam fazer suas contribuições, nascendo, assim, o *Solaris Express Community Edition* – um embrião da distribuição OpenSolaris. Esta versão não é totalmente aberta e possui trechos proprietários de código. Depois, em 2007, a Sun criou o OpenSolaris como uma distribuição totalmente de código aberto que hoje atua de forma independente e tem um caminho de duas vias com o Solaris: novidades implementadas em um sistema operacional são exportadas para o outro.

Neste aspecto, recebo diariamente perguntas como "Posso compilar o código do OpenSolaris como fazemos no Linux?". Claro. Para isso existe o site www.opensolaris.org, onde todos podem baixar o código e também a descrição dos passos para a compilação do seu próprio sistema.

Uma outra pergunta frequente que merece atenção especial é: "Se o OpenSolaris é um sistema operacional derivado do Solaris 10 e os dois trocam código entre si, então eles serão idênticos no fim das contas?".

Definitivamente, o OpenSolaris não é igual ao Solaris. É mais que conveniente expor aqui os detalhes dos motivos pelos quais devemos estar atentos:

- o OpenSolaris tem seu código aberto (licenciamento CDDL), enquanto que o Solaris não, pois este possui drivers proprietários da Sun e de outros fabricantes;
- as implementações feitas no OpenSolaris são independentes do Solaris, ou seja, o que for implementado no Solaris pode vir a ser importado para o OpenSolaris e vice-versa; contudo, isso não é regra;
- o OpenSolaris tem muito mais ferramentas do que o Solaris 10, pois existe uma enorme contribuição do mundo do Código Aberto. Além disto, existem diversas melhorias e softwares da própria Sun que ainda não chegaram no Solaris, mas que já estão presentes no OpenSolaris, como o xVM Hypervisor, IPS (software de gerenciamento de pacotes), entre outros;
- o Solaris foi exaustivamente testado, otimizado e homologado para trabalhar com os principais softwares do mercado, como banco de dados Oracle, SAP etc., assim como com toda a linha de hardware Sun de alto desempenho;
- o OpenSolaris tem muito mais drivers do que o Solaris, o que facilita a vida de um desenvolvedor, pois é bem comum encontrar na distribuição drivers para placas wireless ou ainda para dispositivos relacionados com biometria que estão sendo introduzidos agora;
- o processo de instalação do OpenSolaris é muito mais simples e tem menos possibilidades de configuração do que o Solaris, em virtude do foco do projeto.

Espero que com estes poucos pontos o leitor possa entender as diferenças entre estes dois projetos e apreciar ambos da mesma forma. E fique atento: o projeto OpenSolaris está crescendo em um ritmo alucinante, do qual você também pode fazer parte! ■

Alexandre Borges é Especialista Sênior em Solaris, OpenSolaris e Linux. Trabalha com desenvolvimento, segurança, administração e performance desses sistemas operacionais, atuando como instrutor e consultor. É pesquisador de novas tecnologias e assuntos relacionados ao kernel.

AVG para Linux

A AVG Technologies lançou uma nova versão de seu antivírus para Linux, de número 8.5. Os principais recursos são a proteção contra *malware*, um filtro antivírus aprimorado e um antivírus que atua em cada acesso ao arquivo, com base no sistema de arquivos *RedirFS*.

O *Redirect filesystem* é uma nova camada entre o alternador virtual de sistema de arquivos (VFS) e os drivers dos sistemas de arquivos. Quando o Linux abre um arquivo, o RedirFS registra o fato e notifica o novo filtro antivírus *afvlt* no módulo externo ao kernel, que por sua vez testa o arquivo. Esse mecanismo supostamente aumenta o desempenho da varredura de vírus. O RedirFS desenvolvido pela AVG Technologies substitui o *DazukoFS*, solução anterior para a filtragem de vírus em cada acesso.

Outros avanços do AVG 8.5 para Linux incluem uma heurística melhorada para detecção de malwares novos e ainda desconhecidos. Nessa versão, o antivírus também faz melhor uso dos recursos do sistema e usa menos processamento. Graças ao suporte a CPUs de 64 bits e multicore, o AVG tem escalabilidade consideravelmente melhor. Sua arquitetura totalmente modular também deve reduzir o número de reinícios necessários. □

Nagios sofre fork

O projeto de código aberto *Nagios* ganhou recentemente um *fork*: o projeto *Icinga*. A empresa Netways, especializada em serviços de gerenciamento de TI de código aberto – e particularmente no Nagios – será responsável pelo fork.

De acordo com relatos, diversos desenvolvedores dos plugins atuais já se encontram na diretoria. O CEO da Netways, Julian Hein, enxerga o desenvolvimento de *add-ons* primariamente como um projeto comunitário, enquanto o desenvolvimento do núcleo do Nagios fica unicamente a cargo do desenvolvedor-chefe Ethan Galstad, o que leva a gargalos nesse processo. A tentativa da comunidade de eliminar esse gargalo do desenvolvimento do núcleo da ferramenta havia encontrado um obstáculo, o que levou a Netways a liderar o movimento de realizar o fork do Nagios para um projeto separado. "Após muitos anos em que inúmeras tentativas de melhorias não deram em nada, não vemos outra forma de promover o avanço do Nagios", disse Hein numa entrevista à Linux Magazine alemã.

Hein garante que o Icinga manterá a compatibilidade com o Nagios em vários aspectos. Ele assegura que o Icinga usará os mesmos plugins de monitoramento e os add-ons funcionarão nos dois projetos. O portal do Nagios utilizará uma estratégia de compatibilidade semelhante para o fork. ■

Xen 3.4 traz nova estratégia

A comunidade Xen.org anunciou no dia 18 de maio o lançamento da versão 3.4 do hypervisor de código aberto Xen. A principal novidade do Xen 3.4 é uma alteração na estratégia do projeto, destinada a reposicioná-lo no mercado após os importantes acontecimentos recentes relacionados ao software: a aquisição da XenSource pela Citrix e o crescimento do apoio ao concorrente KVM – também de código aberto – são os mais significativos.

A alteração de estratégia na versão 3.4 passa pela XCI (*Xen Client Initiative*), uma iniciativa que visa a tornar o Xen mais compatível com extensões. Um exemplo de uso dessa tecnologia seria uma máquina virtual com um antivírus ser capaz de varrer outras máquinas virtuais.

Além disso, o Xen avançou na área em que já se destaca, a alta disponibilidade, com um controle mais granular sobre os componentes do sistema que podem ou não ser utilizados pelas máquinas virtuais. O gerenciamento de energia também ganhou avanços, com novos algoritmos de escalonamento que permitem economizar mais energia do que antes.

Outras novidades incluem a possibilidade de máquinas que utilizam virtualização completa acessarem o barramento PCI diretamente (*PCI passthrough*, antes restrito às máquinas paravirtualizadas) e o suporte à tecnologia Viridian, que, em sistemas virtualizados sobre o hypervisor da Microsoft (*Hyper-V*), acelera operações de I/O da máquina virtual. Contudo, infelizmente a integração do Xen ao kernel Linux não avançou significamente, continuando restrita ao funcionamento do Linux como *domU*. ■

Hotéis Plaza em Porto Alegre

Excelência em serviços







PLAZA SÃO RAFAEL HOTEL E CENTRO DE EVENTOS
Av. Alberto Bins, 514 - Centro Histórico - Porto Alegre - RS - CEP 90030-140
Tel. (51) 3220.7000 - Fax (51) 3220.7001 - res-saorafael@plazahoteis.com.br







PLAZA PORTO ALEGRE HOTEL
R. Senhor dos Passos, 154 - Centro Histórico - Porto Alegre - RS - CEP 90020-180
Tel. (51) 3220.8000 - Fax (51) 3220.8001 - res-portoalegre@plazahoteis.com.br

Consulte seu agente de viagens.

Plaza HOTEIS RESORTS SPAS BRASIL

Reservas: 0800 70 75292 PLAZA

www.plazahoteis.com.br

Oracle adquire Virtual Iron

Pouco depois da aquisição da Sun Microsystems, a Oracle anunciou em maio a compra da Virtual Iron, empresa especialista em virtualização, por um valor não revelado. A Virtual Iron produz softwares de gerenciamento de virtualização e servidores virtuais. "Com a adição da Virtual Iron, a Oracle espera permitir que seus clientes gerenciem de forma mais dinâmica seus servidores e otimizem seu consumo energético", afirmou Wim Coekaerts, vice-presidente de Linux e engenharia de virtualização da Oracle. "A aquisição é consistente com a estratégia da Oracle de propiciar o amplo gerenciamento de softwares corporativos, e facilitará o gerenciamento mais eficiente dos níveis de serviço das aplicações", completou.

A aquisição será efetivada ao longo do verão no hemisfério norte, e até lá as duas empresas continuarão operando de forma independente.

A Oracle já possuía sua própria solução de virtualização de servidores, o Oracle VM. No entanto, essa solução é voltada ao mercado de alto desempenho, enquanto a oferta da Virtual Iron se destina ao mercado de pequenas e médias empresas. Ainda assim, somados às soluções de virtualização da Sun, que respondem sob o nome de *xVM*, esses produtos oferecem redundância de ofertas por parte da gigante dos bancos de dados. □

Aliança busca salvar MySQL

O fundador do MySQL Monty Widenius, juntamente com a empresa finlandesa de serviços e suporte Percona, juntaram forças para criar a Open Database Alliance. A intenção do novo consórcio é proteger o status de Código Aberto dos componentes essenciais do MySQL.

A insatisfação com as políticas de gestão e lançamentos fizeram Widenius deixar a Sun no início do ano e criar sua própria empresa, Monty Program AB, para continuar o desenvolvimento de seu próprio mecanismo de armazenamento (*Maria*). O desenvolvimento do MariaDB e o trabalho no MySQL também são os objetivos da nova aliança. "Nosso objetivo com a Open Database Alliance é fornecer uma entidade central para o desenvolvimento do MySQL, encorajar um ambiente de desenvolvimento verdadeiramente aberto com participação da comunidade e garantir que o código do MySQL permaneça com qualidade extremamente alta", disse Widenius.

A aquisição da Sun pela Oracle incomodou a comunidade, creem os novos parceiros. A Open Database Alliance fornecerá um ponto de encontro central para desenvolvedores e empresas, oferecendo diversos serviços de código aberto, e esperamos que atraia vários membros novos. O suporte já está sendo oferecido. A Open Query, empresa criada pelos desenvolvedores do MySQL Arjen Lentz, Peter Lieverdink e Zak Greant, deu boas vindas à ação. Lentz afirmou em seu blog: "Essa aliança é um excelente passo que mostra a maturidade, amplitude e profundidade de conhecimentos para serviços relacionados ao MySQL!". ■

Cisco e a GPL

Em dezembro de 2008, a Free Software Foundation (FSF) entrou com uma ação contra a gigante das redes Cisco, alegando que sua subsidiária Linksys havia cometido múltiplas violações da licença pública geral GNU, conhecida como GPL. As envolvidas finalmente chegaram a um acordo.

Como parte deste, a Cisco criará na Linksys o cargo de Diretor de Software Livre. Esse funcionário será responsável pela adequação da empresa às licenças de Software Livre, principalmente a GPL. O diretor também deverá reportar-se periodicamente à FSF com relação a seus esforços de adequação.

A Cisco também concordou em publicar uma nota de licenciamento no site da Linksys e numa publicação separada, notificar os clientes da Linksys a respeito de seus direitos de licenciamento sob as diretrizes da FSF, e fornecer downloads gratuitos do código-fonte das partes dos produtos Linksys afetados pelas licenças. A Cisco também contribuirá monetariamente com a FSF para promover os esforços desta. ■

UE dá multa bilionária à Intel

A gigante dos microchips Intel recebeu uma multa recorde de € 1,06 bilhões (pouco mais de R$ 3 bilhões) da Comissão Europeia por abusar de sua posição de liderança no mercado de CPUs.

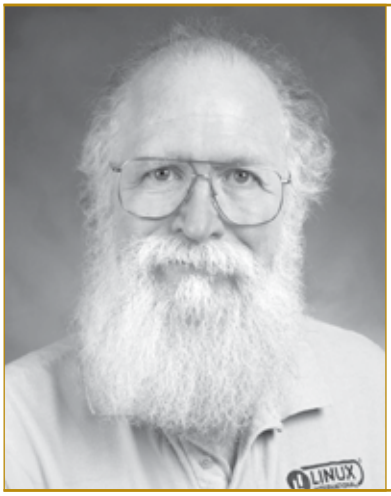
"A decisão está errada e ignora a realidade do mercado altamente competitivo de microprocessadores", comentou o presidente da empresa, Paul Otellini. Ele acrescentou que "a Intel jamais vende produtos abaixo do custo. Porém, investimos consistentemente em inovação, na manufatura e no desenvolvimento de liderança tecnológica. O resultado é que conseguimos reduzir o custo de nossos produtos para competir num mercado altamente competitivo".

Contudo, o relatório da UE é bem diferente. A comissão acusa a empresa de abusar de sua posição de mercado entre 2002 e 2007, alegando que a Intel fez generosos pagamentos a fabricantes e vendedores de PCs para estes boicotarem os chips da concorrente AMD. Dell, Acer, HP, Lenovo e NEC estavam entre as empresas ligadas às más práticas da Intel.

De acordo com o comissário europeu para concorrência, Neelie Kroes, "a Intel prejudicou milhões de consumidores europeus ao agir deliberadamente para manter concorrentes fora do mercado de chips de computadores durante muitos anos. Uma violação tão séria e duradoura das regras antitruste da UE não pode ser tolerada". Como se pode esperar, a AMD está feliz com a decisão, mesmo com o valor recorde da multa sendo inferior à quantia que a UE poderia ter pedido. A Intel vai apelar da decisão. ■

Acionistas da Sun resistem à venda

A aquisição da Sun Microsystems pela Oracle está enfrentando resistência por parte dos acionistas da tradicional fabricante de Unix. Já no mês de abril, foram três as ações coletivas contra a aquisição, alegando que os termos da operação são "injustos e inadequados" e que o grupo está ignorando importantes aspectos financeiros e tributários referentes à transação, provavelmente por meio de corrupção em subsidiárias da Sun fora dos EUA. As alegações estão sob investigação do departamento de justiça norte-americano. ■



Coluna do maddog

Em busca de programadores

Se você está começando do zero, vai precisar de vários usuários para atrair uma forte comunidade de desenvolvimento.

Tenho um amigo que está trabalhando num projeto de código aberto há três anos. Ultimamente, ele ficou um pouco decepcionado porque poucas pessoas parecem estar ajudando no projeto, então discutimos algumas questões.

Primeiramente, a maioria dos seus usuários não é programador. Alguns usuários até fornecem retorno, testam alterações e verificam correções de falhas, mas poucos contribuem com sequer uma linha de código.

Sua base de usuários também é relativamente pequena. Embora o número potencial de usuários pudesse chegar às centenas de milhares, ele limitou intencionalmente esse número até que o código alcance um estado mais maduro.

Eu disse que quando conheci Linus Torvalds, em maio de 1994, o kernel Linux tinha acabado de chegar ao estágio 1.0. Naquele ponto, alguém calculou que havia mais de 124 mil pessoas usando e contribuindo com o Linux.

A cara do meu amigo ficou um pouco pálida. Depois, eu contei a ele minha fórmula para o sucesso num software livre e de código aberto:

"Se um milhão de pessoas usam seu código, pelo menos metade delas achará que há algo errado com ele. Um quarto desse meio milhão talvez tenha tempo para alterar o código, caso possua o conhecimento necessário. Um décimo desses 125 mil não apenas terá tempo e conhecimento, mas também a inclinação para as programação. Uma pequena percentagem dessas 12,5 mil pessoas não terá filhos, então conseguirá concentrar-se o suficiente para completar a tarefa. Por último, três *patches* serão enviados por três pessoas diferentes, e você rejeitará dois deles porque não gosta da solução ou do estilo do código".

Agora, digo isso com a língua na minha bochecha, mas essa fórmula ainda ressalta um ponto importante: para alcançar um pequeno número de contribuidores potenciais, pode ser necessária uma base de usuários relativamente grande. Por esse motivo, é absolutamente necessário que as pessoas do Software Livre se disponham a sair e divulgar o Software Livre para quem quer que deseje escutar.

Algumas outras considerações para criar uma forte comunidade de desenvolvimento são:

- *Facilidade de imersão* – Um novo programador que esteja sobrecarregado para visitar muitas páginas diferentes, ler anos de listas de email e aprender a se enquadrar numa cultura específica do projeto talvez jamais se sinta confortável o suficiente para contribuir. Considere acrescentar uma seção para "novos desenvolvedores" ao site do projeto para fornecer informações essencias a programadores potenciais.
- *Inclusão* – Com frequência, a falta de inclusão é um motivo para programadores potenciais não permanecerem. Interagir com outros é uma parte importante das habilidades de qualquer líder de projeto. Certifique-se de "compartilhar a glória" por meio da divulgação de contribuições e do reconhecimento do trabalho. Na Digital, certa vez elogiei um programador sênior por fazer um bom trabalho, e essa pessoa realmente acabou-se em lágrimas. Mesmo após vários bons aumentos e bônus, meu colega jamais havia sido elogiado por ter feito um bom trabalho num trecho específico de código.

Se você possui um bom projeto, não tenha medo de "vender sua ideia". Seja direto a respeito de onde o projeto se encontra e em que direção vai seguir. Venda a visão e faça todo o possível para criar uma forte equipe de contribuidores. Com isso, você deve conseguir atrair uma comunidade suficiente para tornar seu projeto auto-sustentável. ■

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.

Ubuntu Certified Professional

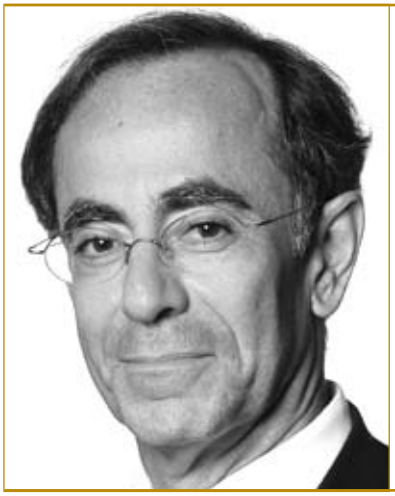
A plataforma Linux mais usada no mundo agora certifica você aqui no Brasil!

- **Desktop Ubuntu**
- **Ubuntu Professional, UCP**

Seja nosso Parceiro

Participe do programa de qualificação de parceiros para treinamento Ubuntu no Brasil.
Fuctura Tecnologia 81.3223.8348 / Linux New Media 11.4082.1300 / www.fuctura.com.br

Fuctura tecnologia · ubuntu training partner · LINUX MAGAZINE · easyLINUX! · Faculdade Maurício de Nassau · FSA



Coluna do Taurion

Open Source e SaaS

Com a crescente popularização do modelo SaaS, como fica o Open Source?

O modelo de software como serviço – SaaS – já está saindo do "se" para o "como", impulsionado até pela crise de crédito, quando as empresas procuram trocar *capex* (*capital expenses*) por *opex* (*operating expenses*).

Na prática, SaaS e Open Source compartilham o mesmo modelo econômico, de baixo custo de capital e custos operacionais variáveis. Isto gera sinergia entre os dois modelos e um impulsiona o outro. Os mesmos argumentos que atraem os usuários para o Open Source são usados pelos provedores de softwares como serviços. Que argumentos são esses? Simplesmente não haver necessidade de aquisição prévia de licenças de uso antes de usar o software. No SaaS você paga pelo que consumiu de recursos. No Open Source, o software também é visto como serviço e as receitas das empresas envolvidas neste setor são obtidas por serviços prestados, como empacotamento e distribuição de um conjunto de softwares sob a forma de uma distribuição Linux, por exemplo.

A computação em nuvem também será um acelerador do Open Source. A combinação de uma infraestrutura "pay-per-use" associada ao uso de softwares abertos vai reduzir significativamente as necessidades de capital e os custos de desenvolvimento de aplicações e acelerar o *time to market*. É um cenário que vai permitir às pequenas e médias empresas entrar mais rapidamente no mundo da Tecnologia da Informação. Portanto, na minha opinião, Open Source, SaaS e Cloud Computing vão criar um inter-relacionamento e gerar sinergias, cada um impulsionando os demais. O resultado final será um outro modelo computacional que vai mudar em muito o atual cenário da indústria de TI.

O livro "A Cauda Longa" de Chris Anderson propõe que determinados negócios podem obter uma parcela significativa de sua receita pela venda cumulativa de grande número de itens, cada um dos quais vendidos em pequenas quantidades. Isto é possível porque a Internet abre oportunidades de acesso que antes não existiam. É um modelo diferente do mercado de massa, em que poucos artigos são vendidos em quantidades muito grandes. Por exemplo, a Amazon reporta que uma parcela significativa de sua receita já vem de produtos da Cauda Longa não disponíveis (e jamais estariam) nas livrarias tradicionais, limitadas pelos caros espaços físicos das lojas.

E como Open Source, SaaS e Cloud Computing vão afetar a indústria de software? Nestes modelos, o custo de capital é substituído por custos operacionais.

Softwares que têm seu projeto de desenvolvimento cercado pelo pequeno tamanho do seu mercado potencial (seu custo de produção não gerava retorno financeiro suficiente) podem agora, se desenvolvidos em Open Source e operados em nuvens computacionais, entrar no mercado. Os custos de comercialização destes softwares também tendem a zero, pois não é necessário termos equipes de vendedores, mas simples downloads e marketing viral (blogs e outros meios de disseminação de informação). A receita dos desenvolvedores dos softwares Open Source será obtida pelo seu uso (*pay-as-you-use*), típico do modelo SaaS. A imensa maioria das empresas não vai investir tempo e dinheiro modificando código, a não ser quando absolutamente necessário – aliás, situação raríssima.

Então, isto tudo significa que o mercado de software tradicional, baseado em licenças, vai morrer? Na minha opinião, não! Pelo menos no horizonte visível. Acredito que conviveremos em um contexto em que os modelos de vendas de licença e software como serviços vão compartilhar os palcos por algum tempo ainda. ■

Cezar Taurion (ctaurion@br.ibm.com) é diretor de novas tecnologias aplicadas da IBM Brasil e editor do primeiro blog da América Latina do Portal de Tecnologia da IBM developerWorks, em www-03.ibm.com/developerworks/blogs/page/ctaurion.

O data center é sua garagem

Desenvolver na Web é o novo padrão. Garanta o máximo de desempenho e confiabilidade com o menor custo possível.

por Pablo Hess

No princípio da computação, muitas das empresas de TI que hoje são verdadeiros gigantes surgiram nas garagens de estudantes universitários, em especial aqueles que residiam na região do Vale do Silício nos Estados Unidos. Bastavam alguns computadores e um ou mais programadores com habilidades suficientes e ambição de sobra, e rapidamente tinha-se uma empresa produtora de software.

Ao longo das últimas três décadas, no entanto, esse fenômeno se tornou menos frequente. Qualquer programa com qualidade ou recursos acima da média fatalmente seria adquirido por uma das muitas gigantes do software – ou possivelmente até pelas gigantes do hardware.

Internet e a nuvem

Com a popularização da Internet, não apenas o número de clientes potenciais de qualquer software foi multiplicado, como tornou-se possível atender mercados de software que antes seriam incapazes de manter um negócio dedicado. Na nuvem da Internet, qualquer programador pode contratar um serviço de hospedagem, desenvolver sua aplicação web e oferecê-la instantaneamente como um serviço para qualquer cliente que a desejar.

Nesse cenário, o data center ocupa o papel antes pertencente à garagem, mas com vantagens significativas – escalabilidade sem precedentes, ciclo reduzidíssimo de desenvolvimento do software e baixo gasto de produção, entre elas.

A **Linux Magazine** deste mês mostra como utilizar as "novas garagens" com proveito máximo para seu investimento. Começamos analisando as principais ofertas de hospedagem em data centers nacionais de forma que você possa escolher o mais adequado à sua necessidade. Em seguida, no artigo "Nuvens escaláveis", apresentamos alguns conceitos de programação para você usar na computação em nuvem, radicalmente diferentes daqueles empregados no paradigma tradicional da computação local. O terceiro artigo desta seção, "Aceleração virtual", introduz métricas e medidas que devem ser usadas para garantir um melhor desempenho no uso de servidores virtuais.

Boa leitura! ■

Índice das matérias de capa

Comparativo

O melhor data center

Comparamos os melhores data centers do Brasil em quatro categorias de ofertas. Leia e descubra qual é o mais adequado para a sua necessidade.

por Pablo Hess

A nuvem está disponível para todos. Oferecer softwares sob a forma de serviços através da grande rede é, possivelmente, a forma mais prática de começar um novo negócio. Com isso, ganhar dinheiro na Web voltou a ser um sonho muito comum.

São poucos os riscos envolvidos: quando os negócios crescerem em volume ou demanda de hardware, podemos simplesmente "jogar" mais poder computacional no problema e manter a aplicação funcionando com a mesma velocidade de sempre. Portanto, gasta-se aproximadamente uma parcela fixa do que se pode ganhar.

Então, com ótimas possibilidades de ganhar dinheiro com risco reduzido, você decide iniciar seu negócio pela Web. Depois de desenvolver um plano de negócios altamente eficiente, basta encontrar um local conectado para desenvolver sua aplicação na Web e já começar a ameaçar clientes – e receita, espera-se.

No entanto, a primeira etapa dessa última fase – encontrar um data center – pode ser mais difícil do que parece. Por exemplo, como ter certeza da sua necessidade de um servidor físico dedicado para sua aplicação? Se for realmente necessário, vale mais a pena contratar um servidor dedicado num data center ou apenas hospedar seu próprio servidor em regime de *colocation*? E se a escalabilidade for fundamental, vale mais a pena contratar vários servidores virtuais ou apenas algumas máquinas físicas?

São diversos os fatores que afetam essa decisão. A única certeza é a necessidade de interagir com um data center. Pensando nisso, a **Linux Magazine** foi à luta para pesquisar os melhores preços de data centers para facilitar a sua busca.

Pesquisa

Entramos em contato com os principais data centers do Brasil com atuação no varejo. Perguntamos

quais as suas melhores ofertas tanto na área de servidores virtuais quanto no grupo dos servidores dedicados. Nas **tabelas 1 a 4**, você confere as respostas que obtivemos, e o **quadro 1** explica os critérios de pontuação de cada item.

Mais em conta

A **tabela 1** lista as ofertas "de entrada" de servidores virtuais: tratam-se das opções de menor custo de cada data center, contanto que ofereçam acesso de administrador via SSH. Nessa categoria, é interessante observar a variedade de soluções de virtualização, com Xen, Hyper-V e VMware figurando, cada um, três vezes. As quantidades e velocidades dos componentes das ofertas também variam consideravelmente, desde os limites de tráfego de rede até o espaço de becape.

Nesta categoria, a escolha da **Linux Magazine** vai para a Locaweb, que oferece flexibilidade desejável na configuração de rede, SLA entre os mais altos e armazenamento de grande confiabilidade "na nuvem", além de ter o custo mais baixo entre as pesquisadas.

O espaço de becape parece compor boa parte do custo das ofertas, pois as duas ofertas que incluem esse recurso ultrapassam os R$ 200,00 mensais.

Virtual, mas poderoso

A **tabela 2**, referente às ofertas com maiores recursos em cada data center, traz uma maior homogeneidade, embora ainda haja certa variação. São marcantes as capacidades de processamento (todas as ofertas contam com mais de um núcleo com *clock* de pelo menos 2 GHz) e o espaço de memória disponível (no mínimo 2 GB). Quem associa servidor virtual a espaço em disco reduzido certamente vai se surpreender com os "latifúndios" oferecidos no mercado nacional.

Na **tabela 2**, os preços já são mais semelhantes do que na **tabela 1**. Com a Tehospedo aparentemente voltada a um mercado diferente daquele das demais (e com custo bem mais baixo, naturalmente), a escolha da **Linux Magazine** vai para a oferta da King Host. O número de CPUs e a quantidade de memória são semelhantes às demais ofertas, mas a banda de rede, o limite de tráfego e o suporte a

Quadro 1: Critérios de pontuação

Toda pesquisa que envolve uma pontuação depende de quem avalia. Portanto, o melhor a fazer é esclarecer os critérios para cada pontuação.

O item *Sistemas operacionais* tem peso 1,0 e é julgado conforme a variedade de distribuições oferecidas: menos distribuições significam uma nota mais baixa do que uma grande variedade de distribuições. A oferta com maior número de distribuições Linux recebe nota 10, enquanto que a oferta de uma única distribuição recebe nota 5,0 (pelo menos temos algum Linux, certo?).

Os *Sistemas de virtualização* não têm grande importância para o administrador de cada máquina virtual individual, portanto tem peso 0,5. A oferta de um sistema de virtualização compatível com Linux (como anfitrião) dá pontuação 10.

A *Rede* é muito importante em qualquer servidor, portanto tem peso 3,0. A banda de rede compõe metade da pontuação, e o limite de tráfego compõe a outra metade. Larguras de banda de 10 Mbps conferem nota 3,0; tráfego ilimitado significa nota 5,0, e as notas dos demais valores seguem sua distribuição normalizada pelo maior valor, num máximo de 4,0.

O suporte a IPv6, embora seja importante para o futuro, não é decisivo agora, portanto tem peso 0,2.

Em *Processador/Memória* (peso 2,5), aplica-se a regra: muito nunca é o bastante. No caso dos servidores virtuais existe a dúvida quanto à parcela do processador físico que é dedicada a cada máquina virtual. Em todas as categorias, a quantidade de memória compõe metade da nota, variando desde 0,0 para nenhuma memória até 5,0 para a maior quantidade de memória dentreas ofertas.

Os *Discos rígidos* (peso 1,0) têm importância variada de acordo com a categoria: em servidores dedicados, discos SCSI (incluindo SAS) representam grande ganho de confiabilidade e velocidade, enquanto discos SATA sem RAID sequer deveriam fazer parte das ofertas. O espaço em disco compõe 80% da nota, e os 20% restantes dependem do tipo de discos.

Espaço para becape tem peso 1,0. A impossibilidade de contratá-lo confere nota zero, enquanto o espaço garantido varia do maior disponível (nota 10,0) até a mera possibilidade de contratação (nota 5,0), passando pelo menor (nota 6,0).

O valor de *SLA*, de grande importância (peso 3,0), tem notas de acordo com os valores da tabela normalizados e começando em 99,0%.

O *Preço*, como todos sabemos, também tem importância fundamental, e por isso a **Linux Magazine** confere peso 3,0 a esse item.

A nota final de cada oferta é a média ponderada pelos pesos acima e transformada em um valor arredondado entre zero e cinco.

Tabela 1: Planos de hospedagem virtual (baixo custo)

Servidor virtual mais barato					
Empresa	**Rede Host**	**Locaweb**	**King Host**	**Tehospedo**	**Tecla**
Sistemas operacionais	Suse Linux Enterprise 10 (32/64 bits), Windows Server 2008/2003 Data Center (32/64 bits)	Ubuntu	Gentoo e CentOS	CentOS, Debian Sarge/ Etch, Ubuntu Server, Fedora, Slackware, trixbox CE, Red Hat	CentOS 5.1
Sistemas de virtualização	Xen e Hyper-V	VMware	VMware	Xen	Hyper-V
Rede (banda/limite de tráfego)	Ilimitada/100 GB	2 Mbps/ilimitado ou ilimitado / 300 GB	100 Mbps / 1.500 GB	2 Mbps/10 GB	n/a / 150 GB
Ipv6	Sim	Não	Sim	Não	Não
Processador / Memória	1 Xeon 886Mhz / 512 MB	2 x 300 MHz / 300 MB	1 Xeon 2,0 Ghz / 2 GB	2 x 2,66 Ghz / 256 MB	Dual Xeon E5410, 2.33 / 256 MB
Discos rígidos (espaço / tipo)	30 GB SAS	20 GB / nuvem	200 GB / SATA II	10 GB / SAS em RAID 10	30 GB / n/a
Becape	À parte	À parte	50 GB	À parte	20 GB
SLA	99,90%	99,90%	99,50%	99,50%	99,95%
Preço mensal para contratação anual	R$ 99,00	R$ 59,00	R$ 379,05	R$ 79,00	R$ 250,00
Nota					

Tabela 2: Planos de hospedagem virtual (maiores recursos)

Servidor virtual mais caro				
Empresa	**Rede Host**	**Locaweb**	**King Host**	**Tehospedo**
Sistemas operacionais	Suse Linux Enterprise 10 (32/64 bits), Windows Server 2008/2003 Data Center (32/64 bits)	CentOS 5, Ubuntu 8.04 ou Windows 2003 Data Center	Gentoo e CentOS	CentOS, Debian Sarge/ Etch, Ubuntu Server, Fedora, Slackware, trixbox CE, Red Hat
Sistemas de virtualização	Xen e Hyper-V	VMware	VMware	Xen
Rede (banda/ limite de tráfego)	Ilimitada/1 TB	12 Mbps/ilimitado ou ilimitada/1,8 TB	1 Gbps/3 TB	4 Mbps/40 GB
Ipv6	Sim	Não	Sim	Não
Processador/Memória	4 Xeon 2,66 Ghz / 8 GB	4 x 2 Ghz / 6 GB	4 Xeon 2 Ghz / 8 GB	6 x 2,66 Ghz / 2 GB
Discos rígidos (espaço/tipo)	990 GB/SAS	400 GB / nuvem	200 GB / SATA II	80 GB / SAS em RAID 10
Becape	À parte	À parte	200 GB	À parte
SLA	99,9% para hardware e conectividade	99,90%	99,50%	99,50%
Preço mensal para contratação anual	R$ 1.774,00	R$ 999,00	R$ 949,05	R$ 329,00
Nota				

IPv6 conquistaram o coração da equipe de redação. Sua única desvantagem – que de fato pode ser importante em alguns casos – são seus 200 GB de espaço em disco, significativamente menor que os dos concorrentes.

Dedicação em conta

Na área de servidores dedicados (**tabela 3**), a lista de concorrentes aumenta com a participação do UOL Host. Os preços parecem dividir-se em duas categorias: Rede Host e Locaweb, próximos aos R$ 1.400,00 mensais, e King Host, Tehospedo e UOL Host com preços entre R$ 427,50 e R$ 650,00. Como fator comum às ofertas de custo mais elevado, apenas os discos SAS se destacam.

A difícil escolha da **Linux Magazine** nesta categoria cabe à King Host.

A empresa ganha pontos pela quantidade de núcleos de processamento (quatro), memória (4 GB), banda (100 Mbps) e espaço de becape incluído, além de ter o menor custo entre todas as ofertas da tabela. Esses fatores compensam, embora por uma margem não muito dilatada, a falta de redundância de discos – absolutamente essencial quando se usa discos SATA – e o limite de tráfego, dispensado por três dos demais data centers.

Maior poder

A **tabela 4** expõe as ofertas para quem demanda mais do servidor, e mostra as ofertas com maiores recursos dentre os participantes desta pesquisa. Os preços evidentemente acompanham essa exigência, variando desde R$ 1.595,00 até R$ 5.699,05.

Os data centers parecem destinar-se a diferentes públicos nessa categoria. Enquanto a King Host oferece oito núcleos de processamento e 32 GB de memória com 2 TB de espaço em disco, há configurações com apenas dois núcleos de processamento, 2 GB de memória ou 250 GB de disco.

O melhor compromisso entre processamento, espaço em disco, rede e preço – e portanto a escolha da **Linux Magazine** nesta categoria – é a Rede Host. Por R$ 2.890,00 mensais o cliente tem um grande poder de processamento acompanhado por 16 GB de memória, excelente espaço

Tabela 3: Planos de servidores dedicados (menor custo)

Servidor dedicado mais barato					
Empresa	**Rede Host**	**Locaweb**	**King Host**	**Tehospedo**	**UOL Host**
Sistemas operacionais	Suse Linux Enterprise 10 (32/64 bits), Windows Server 2008/2003 Data Center (32/64 bits)	Red Hat Enterprise Linux 5.x, CentOS 5 e Windows Server 2003/2008	Gentoo e CentOS	CentOS, Debian Sarge/Etch, Ubuntu Server, Fedora, Slackware, trixbox CE, Red Hat, Windows Server 2003/2008	Linux CentOS, Red Hat Enterprise Linux, Windows 2003/2008 Enterprise
Sistemas de virtualização	Xen e Hyper-V	n/a	n/a	Xen	n/a
Rede (banda/ limite de tráfego)	4 Mbps/ilimitado	12 Mbps/ ilimitado ou ilimitada/1,8 TB	100 Mbps/1 TB	4 Mbps/40 GB	4 Mbps/ilimitado
Ipv6	Sim	Não	Sim	Não	Sim
Processador/ Memória	2 Xeon quad core 2,66 Ghz / 8 GB	1x Xeon quad core 2,5 Ghz / 4 GB	1 quad core 2,83 Ghz / 4 GB	2 x 2,33 Ghz / 1 GB ECC	Xeon dual core 2,33 Ghz / 2 GB
Discos rígidos (espaço/tipo)	73 GB (2 SAS em RAID 1)	73 GB (2 SAS em RAID 1)	250 GB 1 SATA	250 GB 1 SATA	250 2 SATA em RAID 1
Becape	À parte	À parte	50 GB	À parte	À parte
SLA	99,5% para hardware e conectividade	1	1	1	99,8% para software, 99,5% para hardware
Preço mensal para contratação anual	R$ 1.390,00	R$ 1.470,00 por mês + R$ 800 (instalação)	R$ 427,50	R$ 449,00	R$ 650,00
Nota	5	4	5	1	4

Tabela 4: Planos de servidores dedicados (maiores recursos)

Servidor dedicado mais caro						
Empresa	**Rede Host**	**Locaweb**	**King Host**	**Tehospedo**	**UOL Host**	**Tecla**
Sistemas operacionais	Suse Linux Enterprise 10 (32/64 bits), Windows Server 2008/2003 Data Center (32/64 bits)	Red Hat Enterprise Linux 5.x, CentOS 5 e Windows Server 2003/2008	Gentoo e CentOS	CentOS, Debian Sarge/ Etch, Ubuntu Server, Fedora, Slackware, trixbox CE, Red Hat, Windows Server 2003/2008	Linux CentOS, Red Hat Enterprise Linux, Windows 2003/2008 Enterprise	CentOS 5.1
Sistemas de virtualização	Xen e Hyper-V	--	--	Xen	--	--
Rede (banda/ limite de tráfego)	10 Mbps/ilimitado	14 Mbps/ ilimitado ou ilimitada/2,1 TB	1 Gbps/10 TB	6 Mbps/ilimitado	10 Mbps/ ilimitado	n/a / 200 GB
Ipv6	Sim	Não	Sim	Não	Sim	Não
Processador/ Memória	2 Xeon Quad 2,66 GHz / 16 GB	1x Xeon Quad 2,5 Ghz / 8 GB	2 Xeon Quad 2,26 Ghz / 32 GB	2 x 2,33 Ghz / 6 GB ECC	2x Xeon Quad 2,33 Ghz / 2 GB	Intel Dual Core 2 Ghz / 2 GB
Discos rígidos (espaço/tipo)	1.500 GB (6 SAS em RAID 5)	500 GB (4 SATA em RAID 10)	2 TB (2 SATA em RAID 1)	250 GB / 2 SATA em RAID 1	900 GB / 6 SAS em RAID 1	250 GB / 2 discos SATA em RAID 1
Becape	À parte	À parte	50 GB	À parte	À parte	320 GB
SLA	99,5% para hardware e conectividade	1	1	1	99,8% para software, 99,5% para hardware	1
Preço mensal para contratação anual	R$ 2.890,00	R$ 2.040,00 por mês + R$ 800,00 (instalação)	R$ 5.699,05	R$ 1.595,00	R$ 3.285,00	Sob consulta
Nota	5	4,5	4	4,5	4	1

em disco, conectividade decente (veja a seguir as considerações sobre conectividade), suporte a IPv6 e ainda a possibilidade de utilizar seus próprios sistemas virtuais com Xen ou Hyper-V.

Análise geral

Os resultados desta pesquisa apontam alguns dados interessantes sobre o mercado nacional de data centers.

Em primeiro lugar, cabe um destaque negativo relacionado à banda de rede, um dos recursos ainda escassos no Brasil. Embora diversos países contem com conexões de rede domésticas bem superiores a 10 Mbps, com 100 Mbps sendo o padrão nos data centers, não foram muitas as ofertas com conexões de rede realmente velozes. O limite de tráfego, outro verdadeiro empecilho ao progresso da rede, também figura entre os maiores inimigos do consumidor desse tipo de serviço.

No caso dos servidores virtuais, também é marcante o baixo valor de SLA. Embora um valor como 99,5% pareça alto e aceitável, ele significa 2.628 minutos – quase dois dias inteiros – fora do ar a cada ano, ou 3h36min fora do ar a cada mês. Um dos maiores benefícios da virtualização é justamente o aumento de disponibilidade que ela proporciona, já que os melhores sistemas de virtualização permitem a migração de máquinas virtuais para outros servidores físicos sem necessidade de tirá-las do ar.

Felizmente também ocorreram surpresas positivas. A ampla adoção de processadores de múltiplos núcleos significa maior eficiência energética de cada computador, e o suporte ao IPv6, embora ainda não difundido, mostra que os data centers de fato têm os olhos voltados para o futuro. ■

Compacto
Design inovador
Alta performance

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

BULLET
UBIQUITI NETWORKS

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

NanoStation loco

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

PicoStation

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

md brasil telecomunicações

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

WDC Networks

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

UBIQUITI NETWORKS

Programação na nuvem Amazon EC2

Nuvens escaláveis

Conheça algumas técnicas para usufruir dos benefícios da computação em nuvem.

por Dan Frost

Todos estão falando da promessa da computação em nuvem, mas na hora de implementar, alguns dos primeiros aventureiros simplesmente implantaram serviços de nuvem replicando os métodos antigos aplicados em ambientes convencionais. Na verdade, a nuvem pode fazer muito mais por você. Hospedar sites na EC2 é fácil, mas realmente utilizar a escalabilidade e a flexibilidade da computação em nuvem requer uma nova abordagem (**figura 1**). Este artigo descreve algumas técnicas para aproveitar os benefícios da computação em nuvem na sua infraestrutura. Apesar de usar exemplos baseados na linguagem *Ruby* e no ambiente EC2 da Amazon, esses conceitos também se aplicam a outras linguagens e fornecedores de nuvem.

Conteúdo estático

Na nuvem, não é necessário que tudo passe pelo *seu* servidor (mesmo que ele seja virtual). Não é preciso um servidor virtual para servir arquivos, gerenciar filas e armazenar dados compartilhados. Serviços dedicados podem realizar essas tarefas, e utilizá-los ajuda a melhorar o funcionamento das suas aplicações na nuvem.

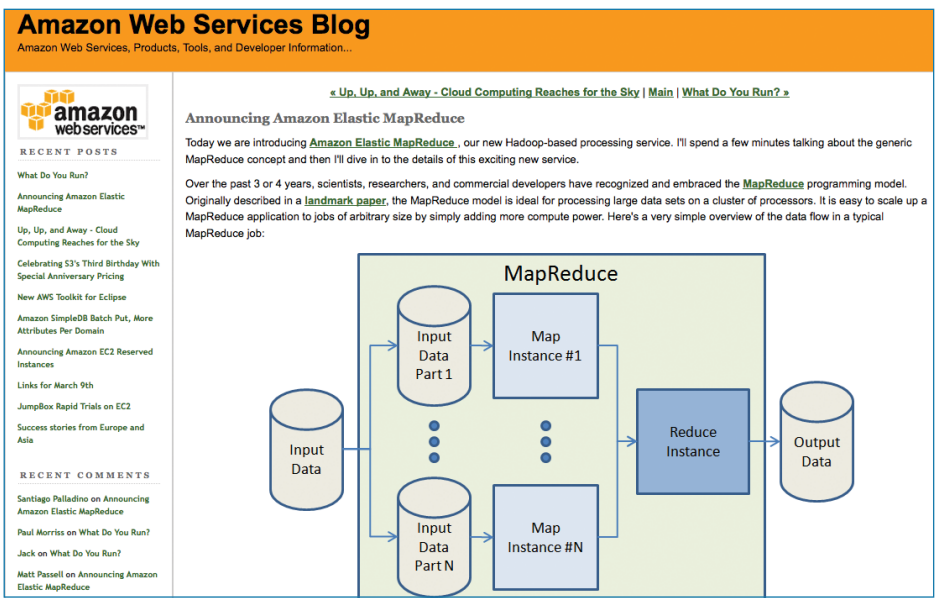


Figura 1 A Amazon incluiu recentemente o *MapReduce* em sua lista de serviços. Como se cache, computação e filas não fossem suficientes, agora é possível criar tarefas gigantescas e distribuídas.

Armazenamento

Neste primeiro exemplo, usamos um serviço de armazenamento online para abrigar nossos arquivos estáticos. Por retirar um peso desnecessário dos servidores web, o armazenamento online é uma boa prática para qualquer site que opere no paradigma da nuvem. No caso do ambiente da Amazon, o serviço S3 (*Simple Storage Service*) funciona como abrigo para os arquivos estáticos.

Suponhamos a presença de uma aplicação Ruby simples como um blog ou wiki. Quando os usuários sobem um arquivo, ele geralmente é gravado no sistema de arquivos; em vez disso, poderíamos repassar o arquivo diretamente para o S3.

Para fazer isso em Ruby, comece instalando a biblioteca:

```
sudo gem install aws-s3
```

Em seguida, crie um script simples como o da **listagem 1**. Para enviar o arquivo para o S3 e torná-lo público, basta uma única linha:

```
AWS::S3::S3Object.store(
    'exemplo.jpg',
re  open('exemplo.jpg'),
    'meu-local-publico',
    :access => :public_read
```

Claro que a URL será diferente, então precisamos alterar o link no

post do blog. O exemplo a seguir cria a URL:

```
http://s3.amazonaws.com/meu-local-
➥publico/exemplo.jpg
```

É relativamente fácil enviar todos os arquivos estáticos para o S3 – podemos pensar no S3 como um enorme servidor de arquivos estáticos. Ainda mais interessante é o SQS, que realmente nos leva a solucionar problemas de forma escalável.

SQS

O SQS é um servidor de fila que abriga uma fila de dados a qual as aplicações podem adicionar e remover dados. Essa tarefa aparentemente trivial facilita o ato de escalar grandes tarefas. Em vez de precisar executar todas as tarefas num único lugar e manter tudo coordenado, é possível enviar uma lista de tarefas para a fila, iniciar uma dúzia de servidores e vê-los processar a fila.

Por exemplo, imagine que você precise preparar um grande número de recomendações personalizadas para clientes. Num ambiente LAMP normal, seria preciso atravessar uma lista de registros de usuários, criar um conjunto de recomendações e armazenar as informações em uma segunda tabela do banco de dados. Com o SQS, podemos dividir o processo. Em outras palavras, é possível "desmontar" o processo enviando as informações para a fila no primeiro script e depois processando os dados da fila no segundo script.

Com o *Rails*, é possível instalar os *bindings* do SQS para Ruby e enviar um modelo para a fila usando o método `to_xml`:

```
q = SQS.get_queue "faz-as-
➥recomendacoes"
q.send_message meuobjeto.to_xml
```

Esse código significa que uma entrada XML na fila *faz-as-recomendacoes* será semelhante a:

```
<meuobjeto>
    <usuario>Sr. Silva</usuario>
    <produtos_favoritos>
      <produto>2412</produto>
      <produto>9374</produto>
      <produto>1029</produto>
    </produtos_favoritos>
</meuobjeto>
```

Em seguida, é necessário retirar da fila essa entrada XML e fazer algo com ela:

```
f = SQS.get_queue "faz-as-
➥recomendacoes"
item_da_fila = f.receive_message
trabalho = MeuObjeto.new()
trabalho.from_xml item_da_fila.
➥body
```

O objeto `trabalho` é o mesmo que `meuobjeto` nos trechos de código anteriores, mas com uma diferença importante: não é necessário conectar-se ao banco de dados original, então há problemas com o número de conexões ou com a velocidade do servidor de banco de dados.

Você fica livre para usar o XML para criar uma mensagem, que pode ser enviada em seguida ao S3 para ser usada por qualquer outra parte da aplicação (**listagem 2**). Note que essa mensagem não é pública. Como vamos usá-las apenas internamente, não é preciso expor esses trechos.

Ao criar suas páginas web, é possível economizar alguns ciclos de CPU puxando a mensagem de boas vindas do S3 em vez de conectar-se a algum outro servidor:

```
trecho_cacheado =
➥AWS::S3::S3Object.find 'Welcome-
➥dan@exemplo.com', 'welcome-
➥messages'
```

A única coisa que esse código faz é o cache. Usar o SQS e o S3 oferece uma forma de cache completamente escalável que não afeta de forma alguma o desempenho do site.

SimpleDB – escalável

Um último serviço a considerar é o *SimpleDB* – um banco de dados extremamente escalável. A Amazon oferece uma faixa de preços gratuita, o que significa que podemos escalar até dois milhões de consultas antes

Listagem 1: Uso do S3

```
01 require 'rubygems'
02 require 'aws/s3'
03 AWS::S3::Base.establish_connection!(
04   :access_key_id => 'Sua ID',
05   :secret_access_key => 'Sua chave'
06 )
```

Listagem 2: Criação de uma mensagem

```
01 welcome_message = "Bem vindo(a), " + work_object.username + " -
Aqui está uma mensagem especial criada para você."
02 welcome_id = "Welcome-" + work_object.username
03 AWS::S3::S3Object.store(
04   welcome_id,
05   welcome_message,
06   'weclome-messages'
07 )
```

de o serviço ser cobrado. É verdade que você pode atingir esse número de consultas assim que a sua aplicação ganhar muitos clientes, mas esses dois milhões devem ser suficientes para dar um fôlego inicial. Há um *gem* Ruby que oferece uma solução para a integração do SimpleDB à sua aplicação web. Também há *bindings* para várias outras linguagens. No Ruby, comece instalando o gem:

```
gem install aws-sdb
```

Para instalar esse gem na sua aplicação em Rails, confira a documentação completa [1].

Com o modelo criado, o que pode ser feito em uma única linha,

```
class Post < ActiveResource::Base
    self.site = "http://
➥localhost:8888"
    self.prefix = "/usuarios_do_
➥site/"
end
```

o interessante dos bindings do Rails é que mal percebemos que estamos usando o SimpleDB.

O primeiro parâmetro, `site`, é o proxy que deve ser atravessado para o Rails acessar o SimpleDB, enquanto `prefix` é o domínio do SimpleDB onde os dados são armazenados. Se você decidir abrigar um modelo de usuário no SimpleDB, ele ainda será parecido com qualquer outro modelo:

```
user = User.create(
    :username => 'dan@exemplo.com',
    :produtos_favoritos => {2341,
➥4251, 2567})
user.save
```

Então, podemos rapidamente mover nossas tabelas de usuários para o SimpleDB mantendo o banco de dados de produtos num banco relacional e depois criar nossas páginas usando a técnica de *preemptive caching*. Essa solução oferece todos os serviços realmente úteis na frente do seu site: instâncias ilimitadas no EC2, S3 para arquivos estáticos e cache, e o SimpleDB para tabelas gigantes.

Suponhamos que a maioria do site seja constituída por fragmentos pré-cacheados e precisemos recuperar fragmentos com base no usuário que está logado. Se ainda tivéssemos os bancos de dados nas instâncias do EC2 (por exemplo, um cluster MySQL), ainda teríamos que gerenciar como esse banco de dados escala.

Usando o SimpleDB, podemos simplesmente jogar os dados nele e obter de volta o registro do usuário:

```
user = User.find(9876)
cached_snippet =
➥AWS::S3::S3Object.find 'Welcome-'
➥+ user.username, 'welcome-
➥messages'
```

Para efetuar a validação, usamos a API do Rails como de costume:

```
user = User.find(:first, :params
➥=> { :username => 'dan@exemplo.
➥com', :password => 'secrets' })
```

O SimpleDB é o local para guardar todas essas tabelas terrivelmente grandes, em vez de gastar dias otimizando estruturas relacionais e criando caches inteligentes.

Este exemplo ilustra o verdadeiro benefício dos serviços na computação em nuvem – o trabalho pesado pode ficar para os outros. SimpleDB, S3 e EC2, além dos vários outros serviços, oferecem uma forma eficiente para realizarmos uma tarefa importante.

Maior, menor

Após criar a aplicação que usará os serviços em nuvem para escalar de forma elegante, como escalar de fato?

Parte do "ecossistema" que está crescendo em torno do AWS (assim como vários outros serviços de rede) são ferramentas como RightScale e Scalr que se encarregam de iniciar e parar servidores conforme sejam necessários (**figura 2**). Nos dois sistemas, o que fazemos é projetar os tipos de servidores necessários e em seguida definir algumas regras para escalar com base no uso da CPU, número máximo de máquinas e quaisquer outras considerações relevantes. Esses serviços conversam diretamente com o AWS em nosso nome, então não precisamos iniciar

Figura 2 A Amazon diz que seus serviços fazem o "trabalho pesado" para você não precisar fazê-lo. Aplicações como o *RightScale* e o *Scalr* ajudam a gerenciar os detalhes para você se concentrar na aplicação.

e parar de usar a API do EC2 no AWS diretamente.

É possível assinar qualquer um dos dois serviços e implantar sua aplicação em quantos servidores você desejar. Se você realmente gostar de "investigar sob o capô", sempre pode criar seu próprio sistema de escalabilidade que converse diretamente com o Ec2, S3 e outros serviços. A API é baseada em SOAP, com bindings para as linguagens mais comuns.

Apesar de cada sistema funcionar de uma forma particular, os princípios são semelhantes. Por exemplo, o exemplo anterior de um sistema para gerar recomendações para clientes requer ao menos um servidor em atividade ininterrupta, mas se o número de clientes crescer, talvez seja preciso aumentar automaticamente o número de servidores.

Aplicação de recomendação

Podemos criar uma "aplicação de recomendação" que obtenha itens da fila e gere recomendações. Juntamente com ela, podemos implementar um conjunto de regras para criar uma nova instância do servidor caso o uso da CPU ultrapasse um determinado nível (por exemplo, 70%).

Também poderíamos incluir regras para iniciar um novo servidor com base no número de itens na fila (por exemplo, se o número de itens ultrapassar 1.000, iniciar um novo servidor). Essas regras mantêm a fila rápida por meio da adição de mais poder de processamento quando ela fica grande demais. Nossa aplicação é verdadeira e dinamicamente escalável.

Gargalos

Criar softwares para computação em nuvem consiste principalmente em otimizar a aplicação com as novas ferramentas disponíveis.

Quadro 1: Interoperabilidade

Os provedores de serviços de computação em nuvem – Amazon [2], GoGrid [3], Rackspace [4] e Google [5] – atualmente oferecem pacotes de serviços levemente diferentes. A interoperabilidade é uma grande questão para quem está no ecossistema da nuvem, pois atrelar sua aplicação a um único provedor pode ser prejudicial a longo prazo; se sua aplicação escalável funcionar somente no EC2, como você migra se (ou quando) um dos outros provedores oferecer um custo menor?

Quando precisamos escalar, nossa primeira pergunta é: Como? Temos muitos usuários? Ou apenas muitas visitas? Os usuários podem compartilhar dados ou suas informações são únicas? O que **precisa** acontecer quando os usuários entram no site e o que pode ser servido pelo cache?

Se compararmos como as pessoas solucionaram os problemas de escalabilidade de aplicações comuns como o *WordPress* e online como o *Twitter*, veremos que há problemas bem diferentes a resolver.

Escalar nas nuvens envolve grandes desmontagens – fazer um componente funcionar de forma completamente independente dos outros para que cada processo não seja atrasado por um outro. Às vezes, isso requer a reescrita da aplicação, mas se tivermos sorte suficiente de estar escrevendo o programa do zero, é importante não nos basearmos apenas no hábito para a escolha dos métodos.

Para escalar uma aplicação já existente ou criar uma do zero, é necessário otimizar. A otimização é uma das tarefas sem fim – o Google adora divulgar como elimina cada milissegundo possível do tempo de carregamento da página, e quem já precisou otimizar algo entende o valor disso.

Certifique-se de ter as ferramentas para realizar a otimização e saber usá-las – cada linguagem possui uma gama de ferramentas de *benchmark* e *profiling* de código. A otimização é importante quando se pensa em escalabilidade, pois se o código contiver um gargalo, o problema de desempenho será multiplicado conforme sua aplicação ganhe usuários. Além disso, os gargalos são bons candidatos para divisão da aplicação.

Criação nas nuvens

Assim que entendemos a forma mais rápida de servir uma página web a partir dos seus servidores no rack, veio a computação em nuvem com milhares de servidores e uma abordagem totalmente nova. Incluir esses serviços da nuvem no seu conjunto de ferramentas economiza boa parte do que a Amazon chama de "trabalho pesado". ■

Mais informações

[1] SimpleDB com Rails: http://developer.amazonwebservices.com/connect/entry.jspa?externalID=1242

[2] Amazon Elastic Compute Cloud (EC2): http://aws.amazon.com/ec2/

[3] GoGrid: http://www.gogrid.com/

[4] Rackspace: www.rackspace.com/solutions/cloud_hosting/index.php

[5] Google Apps Engine: http://code.google.com/appengine/

Dicas de otimização de desempenho de ambientes virtuais

Desempenho virtual

A otimização de desempenho é bem semelhante em ambientes virtualizados e comuns – mas essa semelhança é mera coincidência.

por Federico Lucifredi

Desde o aparecimento da virtualização de baixo custo em 1999 com o lançamento da primeira versão do *VMware Workstation*, o público já foi devidamente instruído sobre os benefícios dessa tecnologia. Contudo, certamente os usuários de virtualização se perguntam com frequência como é possível reverter as perdas de desempenho oriundas do uso da tecnologia.

O nível de performance da virtualização evoluiu com o amadurecimento da tecnologia. À época em que processadores de 400 MHz foram lançados no mercado, os fatores que limitavam o uso indiscriminado da virtualização eram a frequência da CPU e a quantidade de memória RAM. Essa situação experimentou uma melhora contínua conforme a lei de Moore avançou em sua marcha inexorável, fornecendo tanto a capacidade de processamento quanto a quantidade de memória suficientes para executar múltiplas máquinas virtuais simultaneamente no mesmo hardware, pavimentando o caminho para o florescimento do mercado de virtualização.

Um segundo desafio de desempenho provém da habilidade da virtualização de permitir acesso simultâneo de escrita aos dispositivos físicos. A alocação de mais processadores virtuais do que a máquina real dispõe a um grupo de máquinas virtuais é até uma escolha aceitável sob uma baixa necessidade de processamento, mas a partir do momento em que um ou mais dos sistemas hospedados comecem a apresentar picos de uso de processador, um esquema de balanceamento dinâmico de recursos de processamento passa a ser necessário. O uso de recursos avançados como migração de máquinas virtuais, desligamento de máquinas que executem serviços de baixa prioridade etc., precisam ser "orquestrados" por um sistema de vigilância que garanta o nível de serviços necessário, mesmo em ocasiões em que os mecanismos que assegurem o desempenho de

máquinas reais tenham sido desabilitados de alguma forma.

Um terceiro desafio de performance advém da necessidade de lidar com a quantidade de processamento para realizar a medição do desempenho em um ambiente virtualizado. A adição da camada de virtualização à complexidade dos esquemas de integração de sistemas disponíveis atualmente aumenta o número de fatores com os quais o administrador precisa lidar para poder realizar uma implantação eficiente e bem sucedida.

Este artigo elenca algumas dicas – independentes da tecnologia de virtualização utilizada – para melhorar o desempenho de ambientes virtualizados.

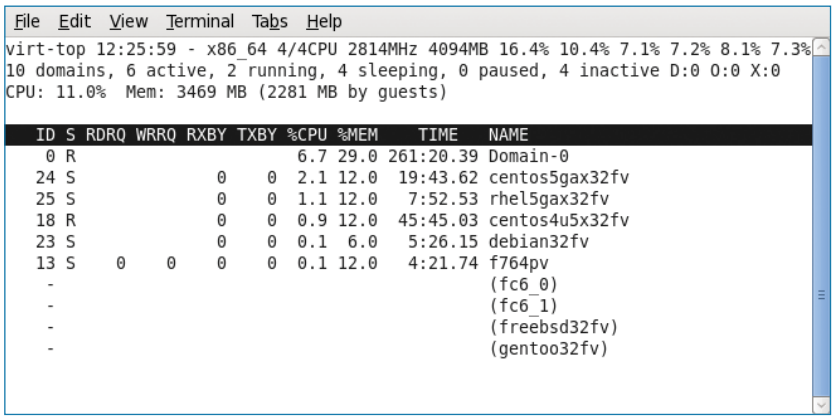


Figura 1 O *virt-top* se baseia no clássico *top* do Unix, mas trata da virtualização.

Testes de desempenho

As equipes de desenvolvimento do Xen [1] e do VMware [2], além de diversos integradores que trabalham com Xen, produziram um contingente excelente de material para descrever os benefícios de performance dos seus respectivos *hypervisors*. Sem entrar muito em detalhes, vale como regra geral o conceito de que podemos esperar que um sistema executado em um ambiente virtualizado bem dimensionado, numa configuração na qual a máquina virtual esteja rodando sozinha em uma combinação adequada de hypervisor e hardware, entregue pelo menos 85% do desempenho do sistema, caso ele fosse executado nativamente no hardware.

É necessário ter em mente que, ao adotar qualquer tecnologia de virtualização, estamos cedendo um pouco de capacidade de processamento em troca de uma ou mais vantagens oferecidas pela virtualização, tais como consolidação de servidores, independência de hardware, migração de carga de processamento, instantâneos/recuperação de estado etc. Desse ponto de vista, pode-se reduzir a configuração do sistema para as necessidades espe-

Quadro 1: Antes da implantação

Antes de implantar sua estrutura de virtualização no hardware físico, é preciso levar em consideração vários aspectos de desempenho. A primeira pergunta é "Qual carga deve ser virtualizada?". Apesar de ser tecnicamente possível virtualizar praticamente qualquer serviço, os profissionais de planejamento precisam ter em mente o desempenho: obviamente, um serviço que esteja exaurindo os recursos de um sistema específico (I/O de rede, de disco e CPU) é péssimo candidato à virtualização. Uma das muitas formas de pensar sobre virtualização é como um equilíbrio entre capacidade disponível e flexibilidade operacional. Se não houver capacidade disponível, a virtualização não vai ajudar a resolver o problema.

Mesmo com as soluções atuais de virtualização oferecendo desempenho quase igual ao do hardware físico, cenários que agregam múltiplas cargas de trabalho virtuais na mesma máquina física exigem cuidado para que nenhuma das métricas fundamentais de desempenho do ativo físico seja excedida pelo uso **combinado** das máquinas virtuais. Se você preferir permitir esse excesso, é preciso considerar os requisitos de vazão dos picos de carga de trabalho no hardware em questão, pois essas cargas **compartilham** aqueles 90% do desempenho físico que o fornecedor promete.

A migração de máquinas virtuais e um recurso de orquestração inteligente para gerenciá-la podem solucionar as colisões no pico da carga de forma eficaz, além de poder simplificar uma parte do processo de planejamento em detrimento de outro – a saber, a implementação do próprio sistema de gerenciamento de recursos. Mesmo quando a migração faz parte do processo de implantação, a constante meta de desempenho no âmbito operacional é garantir que os requisitos combinados de uma única máquina física não excedam a capacidade nos eixos de disco, rede e CPU.

Seu entusiasmo com a virtualização não deve prejudicar os fatos evidentes: a consolidação de cargas de trabalho permite um melhor uso dos recursos de hardware existentes, mas nenhum novo recurso pode ser "criado" magicamente pela solução de virtualização.

cíficas de processamento, mantendo sempre em mente que está se trocando CPU por conveniência.

Pode melhorar

Uma das decisões mais importantes a se tomar na busca dos 90% de desempenho é se é necessário incluir na solução de virtualização um kernel que tenha sido paravirtualizado com tecnologias tais como a *Vitual Machine Interface* (VMI), da VMware, ou o adaptador *Hypercall* [3], da Microsoft.

Essas tecnologias fornecem mecanismos específicos para cada hypervisor acelerar determinados aspectos da operação do kernel virtualizado. As solicitações de chamadas ao sistema e as vias de retorno de respostas, em particular, são aceleradas de maneira significativa, e a ineficiência de gerenciamento de memória devida à virtualização é reduzida de um modo significativo para alguns tipos de carga de processamento [6]. Drivers de dispositivos paravirtualizados possibilitam uma integração de hypervisor conceitualmente similar a kernels de sistemas operacionais que não tenham sido otimizados de outro modo para funcionar em um ambiente virtualizado.

Uma dica primordial quando se trata de otimização de desempenho de ambientes virtualizados é que as lições tradicionais relativas à performance de hardware real ainda são aplicáveis – se soubermos considerá-las corretamente, claro. O processo de "sintonia fina" do desempenho propriamente dito permaneceu inalterado: quando confrontados com um problema, devemos lançar mão de ferramentas que sejam capazes de realizar medições reais e tangíveis da situação, que devem então ser comparadas com uma referência operacional, determinada durante o dimensionamento da necessidade de processamento do sistema. Depois, é necessário localizar os gargalos indicados pelos dados medidos e eliminá-los, bem como a qualquer disputa por recursos que estiver ocorrendo entre os sistemas virtualizados. A diferença consiste apenas no fato de que, em sistemas tradicionais, a otimização se restringe a uma única máquina (a física). Agora, é preciso considerar a carga de processamento do sistema virtualizado, o sistema sobre o qual a máquina virtual está rodando e o hypervisor utilizado, bem como a interação com outras máquinas virtuais que possam estar em execução no mesmo hardware real. Para que isso possa acontecer, é necessário um conjunto novo de ferramentas que permitam desenvolver uma noção geral por meio do estudo do desempenho, mas olhando "através" dos vários sistemas virtuais, bem como para o sistema real que os hospeda e para uma máquina virtual isoladamente. A virtualização adiciona uma outra camada à "arte" (alguns chamariam provavelmente de "feitiçaria") da otimização de desempenho, mas não invalida a ciência anterior, contanto que o aprendiz esteja ciente de que agora há novos "controles" introduzidos pela virtualização nessa camada de abstração adicional.

Ferramentas

Nosso baú de ferramentas deverá ser preenchido conforme a tecnologia de virtualização escolhida, mas os utilitários deverão ser suplementados variações capazes de lidar com ambientes virtualizados. Por exemplo, o tradicional `top` será substituído pelo `virt-top` (**figura 1**) ou o `esxtop`. Uma característica que simplifica a vida das ferramentas de virtualização de código aberto é o fato de que elas são implementadas em sua maioria utilizando a *Libvirt*, podendo desta forma operar automaticamente com o Xen, KVM ou potencialmente qualquer meta-solução de virtualização sem necessidade de modificação. O resultado disso é que o virt-top –

Quadro 2: Virtualização por contêineres

Na escolha da plataforma de virtualização, não elimine os contêineres de sistema operacional. Apesar de os sistemas de virtualização por contêineres como o OpenVZ (de código aberto) receberem bem menos atenção do que as soluções de virtualização completa, as arquiteturas de contêineres estão disponíveis para quase todas as plataformas *nix.

Da forma mais geral, os contêineres oferecem um grau menor de isolamento do que os *hypervisors*, pois elevam a abstração de processos do sistema operacional e podem estar limitados a uma única versão de kernel (ou uma que tenha sido modificada para esse fim). Mesmo assim, as ofertas modernas de contêineres são soluções perfeitamente palatáveis em que as necessidades operacionais estão de acordo com o design.

Estudos de fornecedores mostram que contêineres são um pouco mais rápidos que a virtualização completa [4], mas recomenda-se dedicar algum tempo para avaliar se de fato é possível obter um resultado melhor para a sua carga de trabalho e para seus requisitos operacionais específicos. Se essa diferença for significativa, vá em frente; se não, é melhor usar o padrão da virtualização completa, que costuma ser mais flexível.

que fornece a medição da taxa de transferência de dados em disco, do tráfego de rede e de uso de CPU –, bem como ferramenta semelhantes, como `virt-df`, trabalham em várias plataformas de virtualização.

É necessário ter cuidado com os aplicativos que medem o uso dos recursos mas não oferecem suporte a ambientes virtuais: como esse tipo de ferramenta normalmente mede os ciclos e o desempenho do processador real como um todo (em vez da fatia do processador "virtual" alocada a uma determinada máquina virtual), os resultados numéricos apresentados podem estar totalmente errados. Na maioria dos casos, os valores relativos indicados entre as diferentes situações estão corretos, mas os valores absolutos – por exemplo, os números especificamente – não refletiram valores reais.

Um outro problema que ocorre é a temporização: além dos célebres problemas de desvio de clock em ambientes virtualizados, não há um jeito simples para o comando `time` dizer se a porção compartilhada da CPU alocada a uma máquina virtual foi alterada de maneira significativa no nível do hypervisor. Quando um nova máquina virtual é iniciada, uma máquina que já esteja operando no mesmo sistema mostra internamente que 90% do processador em espaço de usuário está sendo utilizado com a carga de processamento. Entretanto, uma medida real do desempenho nesse momento mostra que a taxa de processamento é apenas metade da original, levando assim o dobro do tempo para ser finalizada. Independentemente disso, medidas realizadas do lado do sistema virtualizado ainda indicam a mesma quantidade de CPU virtual disponível de antes: do ponto de vista do sistema virtualizado, seria como se (literalmente) o processador tivesse sido trocado por um outro menos poderoso em tempo de execução. Como essa não é uma condição prevista pela maioria dos programadores, as ferramentas tradicionais podem falhar em produzir resultados corretos quando confrontadas com essa situação em uma máquina virtual.

Melhores práticas

Como mencionado anteriormente, a virtualização é a arte de trocar um recurso (a CPU) por um conjunto de recursos que não estariam disponíveis de outra forma. Se a carga de processamento saturar a CPU, é necessário pensar duas vezes antes

de virtualizá-la. Como adendo a esse critério vital há também algumas outras sugestões que ajudam a tirar o máximo de desempenho do processador.

CPUs virtuais

A primeira coisa a fazer é analisar a possibilidade de atribuir uma máquina virtual específica a uma única CPU, de maneira a efetivamente criar um mapeamento entre a CPU virtual e a física. Isso reduz drasticamente a "poluição" do cache, e como os especialistas em performance sabem, o desempenho dos processadores modernos está intimamente atrelado à quantidade de acessos ao cache – mais do que a qualquer outro fator. Se esse arranjo não for possível, geralmente é bom ao menos alocar o mesmo número de CPUs a todas as máquinas virtuais hospedadas em um determinado hardware – mesmo que elas disputem o acesso aos mesmos dispositivos. Essa estratégia vem do fato de que a atividade do escalonador das *threads* do hypervisor será mais simples se a distribuição das CPUs entre as diversas máquinas virtuais estiver balanceada. De maneira análoga, é prudente evitar a alocação de mais processadores virtuais do que o estritamente necessário. Se a carga de processamento não faz uso efetivo de núcleos múltiplos, deve-se também evitar configurações que utilizem SMP (multiprocessamento simétrico, na sigla em inglês), já que as CPUs virtuais adicionais ainda requerem interrupções, criando um excesso – e com isso um desperdício – de processamento só por estarem presentes.

Claro que se a máquina virtual estiver configurada para trabalhar com SMP, deve-se considerar ajustar a "afinidade" do sistema virtualizado propriamente dito, no intuito de evitar que a migração de muitos processadores tenha impacto negativo sobre a performance. Devemos nos certificar de usar sempre o tipo correto de kernel: SMP, para o caso de núcleos múltiplos, e uniprocessado, para o caso de uma única CPU virtual. O kernel para sistemas uniprocessados não utiliza outras CPUs virtuais, e o kernel SMP é exagerado no uso de recursos do sistema de virtualização, o que é simplesmente desperdício quando apenas um processador for utilizado pela máquina virtual. Uma outra sugestão é lembrar que a afinidade da CPU – que determina quando e qual processo (ou thread) será enviado pelo agendador para execução, por qual unidade de processamento – pode ser alocada para solicitações de interrupção (IRQ) assim como as threads o são pelo kernel Linux: nessa analogia, pode-se comparar a alocação de uma capacidade de processamento para uma determinada carga à interrupção entregando essa carga a um processador dedicado ou distribuindo-a uniformemente onde haja dispositivos presentes no sistema que demandem uma grande quantidade de interrupções (tais como múltiplas placas de rede, por exemplo).

Memória

Se múltiplas máquinas virtuais estiverem sendo executadas no mesmo sistema hospedeiro, pode-se ganhar

Quadro 3: Teste de hardware com VMmark

Os números fornecidos pelo seu confiável fornecedor são bons, mas nem os mais respeitados benchmarks estão totalmente de acordo com o seu hardware específico. No fim das contas, será preciso consultar seu ambiente real de implantação. Atualmente, o *VMmark* [5], da VMware, é uma escolha popular para benchmark de desempenho virtual. Lançado pela primeira vez em 2006 e agora na versão 1.1, o VMmark é diferente de benchmarks de uma máquina só, pois cria uma única medida do ambiente de virtualização com base numa gama de cargas de trabalho consolidadas num anfitrião físico e executadas concomitantemente em máquinas virtuais separadas. O VMmark chama essa unidade de medida de trabalho de "tile" (tijolo, ladrilho).

Quem tiver disposição para estudar os próprios sistemas virtuais com o VMmark deve começar baixando os componentes apropriados do site da VMware, incluindo o toolkit do VMmark e uma ou mais cargas de trabalho, algumas das quais já estão pré-empacotadas como *appliances* virtuais. Executar o VMware nas suas máquinas não é tão simples quanto instalar outros produtos da VMware, então é preciso consultar o diretório `/docs/` do pacote do VMmark e ler o *Benchmarking Guide*. Esse guia contém listas de itens detalhadas que ajudam a navegar pelo labirinto de etapas obrigatórias e opcionais à realização do benchmark.

Assim que o hypervisor a ser testado estiver em execução no hardware, é preciso selecionar as cargas de trabalho para teste. Apesar de algumas já virem "prontas para o uso" em suas próprias appliances virtuais, outras exigem configurações mais atenciosas por causa de limites de licenciamento de componentes não livres. Realizar um benchmark completo de virtualização não é trivial e aloca o hardware de forma considerável conforme mais clientes sejam necessários para operar cada "tijolo".

uma vantagem nada trivial ao se escolher implementar a mesma imagem de sistema operacional para todas as máquinas virtuais, independentemente de qualquer tipo de diferença da carga de processamento que serão alocadas a elas. Usando a mesma imagem para todas as máquinas virtuais em uma arquitetura na qual as páginas de memória compartilhada são bem implementadas, obtém-se inevitavelmente uma redução significativa de alocação de memória RAM real, pois as cópias múltiplas das páginas desses sistemas operacionais idênticos são carregadas na memória uma única vez.

É uma boa ideia dedicar algum tempo otimizando a alocação de memória virtual de acordo com as necessidades da carga de processamento. Também é muito importante fornecer aos sistemas virtuais uma quantidade confortável de RAM, que serve para minimizar – e possivelmente eliminar – a necessidade do uso de uma área de troca (*swap*). Falhas de paginação em ambientes virtuais afetam o desempenho de maneira mais contundente que em sistemas reais, e esse tipo de problema deve ser evitado ao máximo.

Um suporte a um maior espaço de paginação também pode melhorar a performance de cargas de processamento que se beneficiariam desse tipo de configuração em ambientes não virtuais; para decidir isso, é importante testar a carga e determinar se uma mudança no espaço de paginação é benéfica ou prejudicial em cada caso. E, para finalizar, um número significativo de máquinas virtuais Linux são equipadas com 896 MB de RAM. Páginas de memória até esse limite são mapeadas diretamente no espaço do kernel, enquanto que páginas acima desse limite requerem um esquema de endereçamento mais complicado e desperdiçam processamento.

Armazenamento

O armazenamento de dados no disco também deve ser sempre o mais simples possível. Usar LVM na máquina hóspede e ao mesmo tempo na anfitriã, por exemplo, degrada significativamente o desempenho.

Para garantir performance ótima, também é aconselhável empregar discos SCSI, pois não se limitam a uma única transação por vez – diferentemente até dos mais modernos discos EIDE e SATA.

Rede

Algumas armadilhas de rede comuns incluem o uso de um driver virtual que esteja sub-otimizado (um exemplo típico é o uso do `vlance` pelo VMware, em vez do `vmxnet`, este mais otimizado) ou a falha despercebida da auto-negociação duplex. As possibilidades de ajuste fino do desempenho de rede em virtualização estão avançando rapidamente com as tecnologias de assistência por hardware, como *Virtual Machine Device Queues* (VMDQs).

Como muita atenção é direcionada aos detalhes de baixo nível, as decisões de alto nível, como o protocolo de rede utilizado para armazenamento de dados, também carecem de atenção significativa. Resultados recentes mostram que implementações do iSCSI tanto em hardware quanto em software são comparáveis ao NFS [9], e soluções com *Fibre Channel*, significativamente mais caras, ainda não provaram ser capazes de fornecer desempenho significativamente melhor.

Conclusões

É importante escolher cuidadosamente uma carga de processamento, simplificar a configuração da máquina virtual e medir seu desempenho, bem como realizar seu ajuste fino. Esses passos simples, no entanto, são apenas o começo. Muitos detalhes específicos são inerentes à solução de virtualização escolhida e terão que ser otimizados conforme se testa e mede os resultados de performance. ■

Mais informações

[1] Xen e a arte da virtualização: http://www.cl.cam.ac.uk/research/srg/netos/papers/2003-xenosp.pdf

[2] Comparação de desempenho de hypervisors: http://www.vmware.com/pdf/hypervisor_performance.pdf

[3] Especificação funcional de hypervisors: http://tinyurl.com/pvohsr

[4] Virtualização por contêineres: http://www.cs.princeton.edu/~mef/research/vserver/paper.pdf

[5] VMmark: Um benchmark escalável para sistemas virtualizados: http://www.vmware.com/pdf/vmmark_intro.pdf

[6] Desempenho do VMI do VMware: http://www.vmware.com/pdf/VMware_VMI_performance.pdf

[7] Comparação de desempenho de protocolos de armazenamento: http://www.vmware.com/files/pdf/storage_protocol_perf.pdf

[8] Técnicas de virtualização por software e hardware em x86: http://www.vmware.com/pdf/asplos235_adams.pdf

[9] VProbes: http://www.vmware.com/pdf/ws65_vprobes_reference.pdf

Rede equilibrada

Quem possui múltiplos links de Internet frequentemente deseja balancear a carga entre eles. A série Balance de roteadores PePLink torna essa tarefa mais fácil e flexível.

por Pablo Hess

O Linux é um ótimo sistema para montagem de roteadores. A PePLink, empresa sediada em Hong Kong e representada no Brasil pela Thin Networks, aposta nisso para produzir seus *appliances* de conectividade de redes. Baseados no sistema de código aberto, os aparelhos da linha Balance são roteadores focados no balanceamento de carga e que empregam mecanismos altamente eficientes para isso.

A **Linux Magazine** pôs as mãos num Balance 300 e revela neste artigo os resultados do teste.

Exterior

O PePLink Balance 300 oferece ampla conectividade com suas três portas WAN e quatro conexões LAN (**figura 1**). No entanto, como um dos recursos mais interessantes do aparelho é o balanceamento de carga de entrada, seria interessante a existência de mais portas para a LAN.

Figura 1 Visão do painel traseiro do PePLink Balance 300.

Figura 2 O painel frontal informa a conectividade e a velocidade de operação dos links.

As portas de rede localizam-se na parte traseira do Balance 300, enquanto o painel frontal exibe dois leds para cada conexão (**figura 2**): um para indicar a atividade na porta e outro para informar a velocidade de conexão.

O tamanho reduzido do aparelho (24,4 x 15,7 x 3,2 cm) é um atrativo para quem não precisa organizar sua infraestrutura de rede num rack. Além de poder ser apoiado sobre outras máquinas, ele também possui furos para instalação em superfícies verticais.

Interface

A administração do aparelho é bastante prática e pode ser feita inteiramente via Web. Por padrão (e por motivos de segurança), ele somente aceita conexões à interface HTTP vindas das portas LAN, mas isso pode ser alterado na própria interface.

Ao conectar um computador à porta LAN e pedir um IP ao PePLink por DHCP, o cliente recebe, no primeiro acesso, um endereço na rede 192.168.1.0/24 e é brindado com um pedido de autenticação. Nesse primeiro acesso, o valor para o nome de usuário e a senha é o mesmo: *admin*. Após a autenticação, é exibida a página inicial (**figura 3**).

Segurança primeiro

A primeira providência a tomar no PePLink é ajustar as opções de segurança. Clicando no item *System* do menu superior da interface, o administrador deve alterar a senha de login. Uma opção pouco valorizada é a obrigatoriedade do uso do HTTPS para acesso à interface, que também deve ser ativada (campo *Security*). Mudar a porta de acesso (443 por padrão, evidentemente) fica a cargo do administrador, pois pode acabar sendo uma inconveniência. Por último, recomenda-se manter o acesso à interface de administração limitado às portas LAN (opção *Web Admin Access*).

Finalizados os ajustes, é preciso salvá-los clicando no botão *Save* na parte inferior da janela e, em seguida, efetivá-los em *Apply Changes* (canto superior direito) como manda a caixa de texto exibida após o clique em *Save*. A interface retorna à página inicial (*Main*) e exibe uma animação que informa estar processando as alterações. Porém, caso tenha sido selecionado o acesso unicamente por HTTPS, não adianta esperar, pois é preciso acessar novamente a interface, dessa vez pelo novo endereço começando por `https`.

Assistente de configuração

Finalmente vamos começar a configuração. O assistente (*Setup Wizard*) começa pedindo a configuração das interfaces WAN, incluindo a defi-

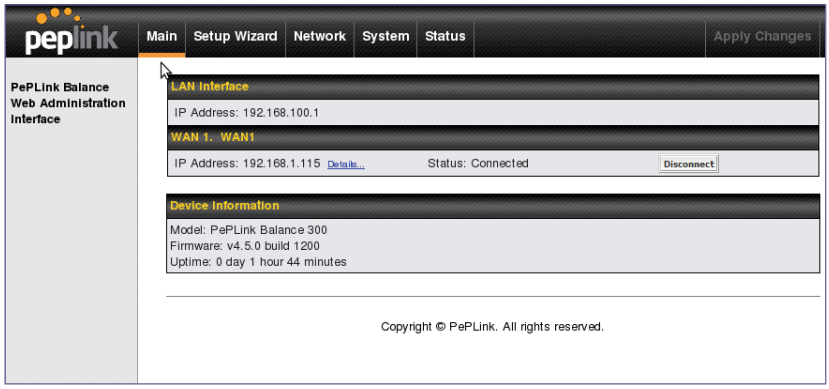


Figura 3 A página inicial da interface web do aparelho informa o status das conexões.

nição de seu tipo de acesso como DHCP, PPPoE ou IP estático. Depois da WAN... o assistente é finalizado. Como há muitas formas de configuração da LAN, o PePLink opta por não interferir nesse ponto e permitir total flexibilidade ao administrador.

Para efetivar a nova configuração das WANs, basta clicar novamente em *Apply Changes*. Como já se pode perceber, o último clique nesse botão é uma constante na configuração do aparelho, o que representa uma segurança a mais contra erros de digitação e administradores incautos.

LAN

É no link *Network* (**figura 4**) que se passa a verdadeira diversão do administrador. Nele, há diversas caixas separadas por utilidade.

Clicando em *LAN* no canto esquerdo da janela, a caixa *IP Settings* permite definir o IP e a máscara da rede interna, além da velocidade de conexão.

A caixa *Drop-In Mode Settings* ativa o modo "Drop-In" – uma espécie de bridge – entre a WAN e a LAN. A limitação, nesse caso, permite somente à interface WAN1 atuar no bridge. O resultado da ativação do modo Drop-In é a transparência entre os dois lados da comunicação. Esse modo é especialmente útil quando já existem um firewall e um roteador em uso na rede ligados um ao outro e se deseja inserir o PePLink no meio dessa conexão. Usando o modo Drop-In no novo aparelho, os outros dois dispositivos não requerem qualquer alteração na configuração.

É possível especificar múltiplas máquinas no segmento WAN, caso essa porta esteja conectada a um switch.

A terceira caixa da configuração da LAN, *DHCP Server Settings*, é onde são definidas as opções do servidor DHCP interno do PePLink, incluindo IPs e nomes de máquina reservados a MAC addresses específicos.

Logo abaixo, as caixas *Static Route Settings* e *DNS Proxy Settings* englobam, respectivamente, a definição rotas estáticas e as configurações do DNS local, que inclui capacidade de caching.

Terminadas as alterações, basta seguir o ritual de clicar em *Save* e *Apply Changes* para ativá-las.

Saída

Ainda na seção *Network*, a diversão continua nos demais tópicos. Em *Outbound Policy* é possível definir as políticas das conexões de saída. A política *High Application Compatibility* fixa uma única interface WAN para a saída de todos os pacotes vindos de um mesmo host na LAN. Como diz o nome da política, o objetivo disso é evitar problemas com aplicações que requeiram um mesmo IP em todas as comunicações. A política *Normal Application Compatibility* é semelhante, mas não usa como único critério a máquina da LAN: toda comunicação entre uma dada máquina na LAN e outra fora dela é feita por uma mesma interface WAN. Por último, também é possível selecionar *Managed by Custom Rules* para criar regras específicas de persistência por protocolo e portas de entrada e saída (**figura 5**). Vale a pena notar que cada regra pode ter uma política diferente de persistência, desde a mais simples (fixar uma interface) até aquelas mais complexas, como um balanceamento com pesos ou a interface menos usada.

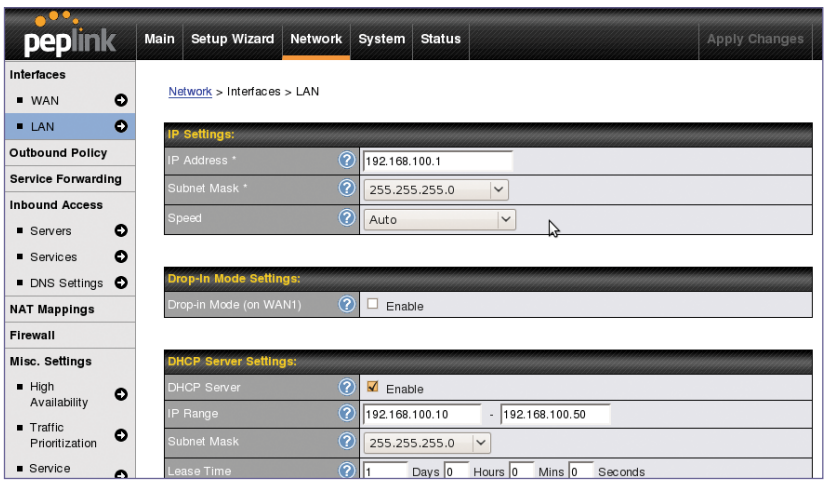


Figura 4 A configuração das interfaces LAN é feita no menu da seção *Networks*.

Interceptação

O PePLink leva a sério o balanceamento de carga, e o item *Service Forwarding* no menu da seção *Network* permite malabarismos interessantes, como o redirecionamento de conexões SMTP e HTTP de saída para um servidor SMTP ou HTTP específico (ou um para cada interface WAN). Outro recurso é a interceptação de requisições DNS de saída para o fornecimento de respostas pelo cache DNS interno do aparelho, aliada ao balanceamento de requisições DNS de saída pelas interfaces WAN.

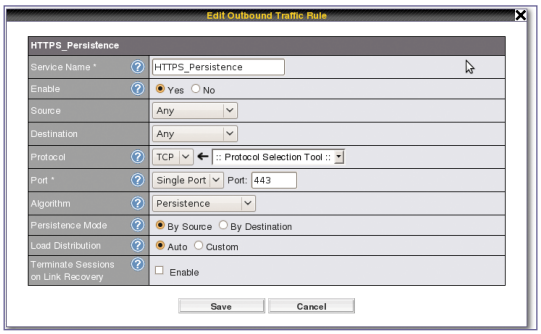


Figura 5 O Balance 300 oferece grande flexibilidade na definição de políticas de saída.

Serviços internos

Para permitir o acesso externo a serviços oferecidos dentro da LAN (o *port forwarding*), são necessários pelo menos dois passos. No primeiro, são definidos todos os servidores presentes na LAN, e para isso usa-se o item *Servers* no menu da seção *Network*. A segunda etapa está no acesso ao item *Services*, no qual se define cada serviço disponibilizado por cada um desses servidores (**figura 6**).

O terceiro item dentro do menu *Inbound Access* trata exclusivamente do DNS. Nele são configurados todos os aspectos do servidor DNS embutido no Balance 300 (**figura 7**), como os domínios pelos quais ele responde e os clientes com permissão para efetuar transferência de zona. Como característica obrigatória no dispositivo, o balanceamento de carga também permite especificar prioridades diferentes para cada porta WAN, fazendo com que uma delas só responda caso as outras estejam fora do ar, por exemplo.

Firewall e NAT

Os itens de menu *NAT Mappings* e *Firewall* funcionam exatamente como se espera, sempre permitindo a definição de diferentes prioridades para cada porta WAN. No item *Firewall*, uma surpresa agradável: pode-se ativar o recurso *Intrusion Detection and DoS Prevention* (detecção de intrusão e prevenção de DoS) que, segundo o texto de ajuda do recurso, protege o Balance 300 e sua rede contra varreduras de porta (*port scan*) e diversos ataques comuns.

Vários PePLinks

Quem se apaixonar pelo Balance 300 e quiser adquirir vários aparelhos (ou quem o fizer por necessidade) pode contar com um mecanismo de alta disponibilidade. Localizado também no menu da seção *Networks*, o item *High Availability* permite a união de múltiplos roteadores em um *pool* de alta disponibilidade.

Eu primeiro!

A priorização de tráfego é um dos principais aspectos negativos do Balance 300. Embora seja um recurso presente no dispositivo, a flexibilidade da sua configuração contrasta com o restante dos recursos, pois conta com apenas alguns tipos de tráfego genéricos (**figura 8**).

Nessa seção há ainda a misteriosa opção *DSL Optimization*, que, segundo seu texto de ajuda da interface, reduz o efeito da saturação da taxa de upload sobre a velocidade de download. Dada a explicação, um nome melhor para essa opção seria "ADSL Optimization", justamente por se aplicar somente a links assíncronos.

Sistema

Como mostra a **figura 9**, o menu da seção *System* permite a definição dos parâmetros mais importantes do sistema do roteador. Além de permitir a detecção, o download e a atualização do firmware do aparelho, é possível definir a hora do sistema e especificar um endereço de email para receber avisos do PePLink. Os logs também podem ser enviados a um servidor *syslog* remoto, e o Balance 300 pode ser continuamente monitorado por SNMP (versões 1 a 3). O

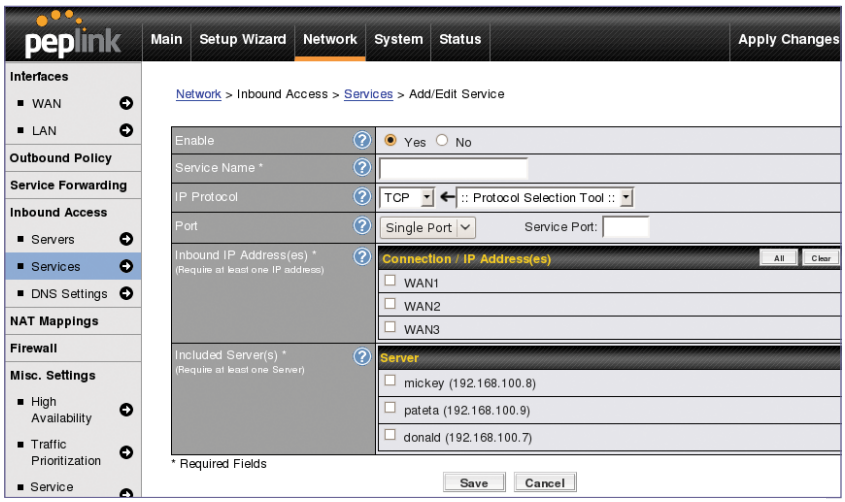


Figura 6 Especificação dos serviços oferecidos por cada um dos servidores já definidos.

fabricante do aparelho disponibiliza ainda um servidor mundial para receber relatórios de todos aparelhos comercializados. Se for ativado (no item *Reporting Server* do menu da seção *System*), esse recurso permite ao administrador conferir os relatórios recebidos pelo servidor, bastando se registrar no site (a própria interface de administração do PePLink fornece os links).

Após finalizar todas as configurações do Balance 300, é possível exportá-las para um arquivo binário para fazer upload em caso de "barbeiragens" futuras. Outra alternativa é especificar um parceiro de alta disponibilidade do qual o aparelho deve receber o arquivo com as configurações corretas.

Diagnóstico

As únicas ferramentas internas de diagnóstico do Balance 300 são *ping* e *traceroute*, disponíveis também no menu da seção *System*. O restante do diagnóstico, em caso de problemas, deve ser feito via syslog ou SNMP, ou até mesmo por meio dos relatórios enviados ao servidor da PePLink.

Conclusões

O PePLink Balance 300 é um bom roteador. Com seu foco em balanceamento de carga, qualquer pequena empresa que possua mais de um link de acesso à Internet pode se beneficiar das capacidades desse aparelho. A limitação a pequenas empresas decorre principalmente do *throughput* máximo de 25 Mbps

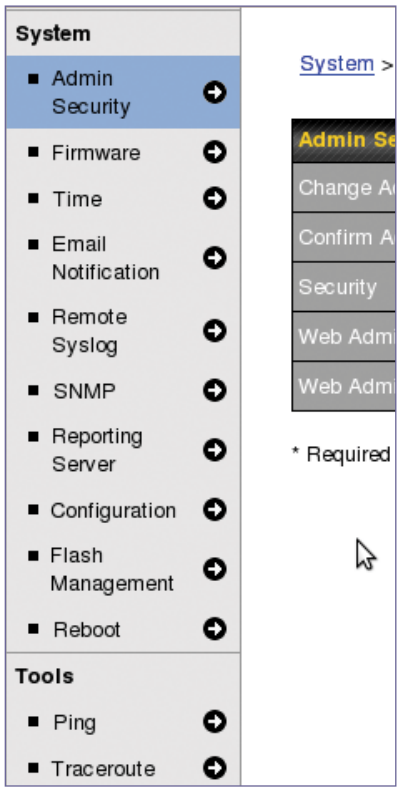


Figura 9 Na seção *System*, o menu é bastante auto-explicativo.

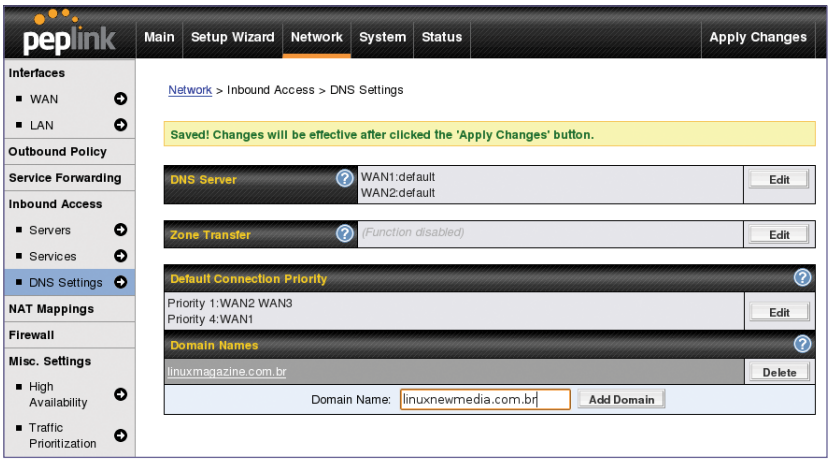


Figura 7 Configuração do servidor DNS embutido no PePLink Balance 300.

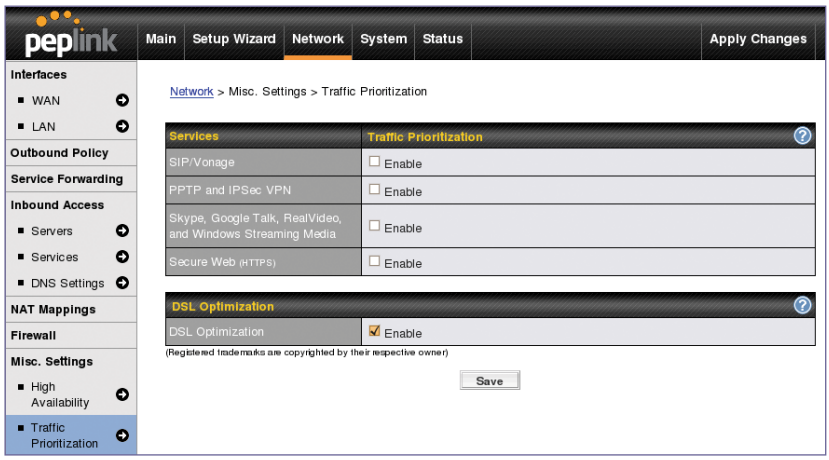


Figura 8 A escassez de opções de configuração para priorização de tráfego decepciona.

informado no manual do dispositivo. Porém, caso seja necessária uma taxa maior, sempre é possível acrescentar outros PePLinks ao pool e aumentar a capacidade do conjunto.

Em pleno funcionamento em nosso ambiente de testes, o PePLink demonstrou que faria bom uso de um processador mais poderoso – ou de uma CPU exclusiva para sua interface de gerenciamento –, pois o uso da interface web foi um pouco prejudicado pela carga de trabalho do aparelho. O outro fator negativo é a inflexibilidade das configurações de priorização de tráfego.

No entanto, esses aspectos não são suficientes para manchar a boa impressão deixada pelo Balance 300. ■

Mais informações

[1] PePLink Balance 300: http://preview.tinyurl.com/peplink

TUTORIAL

Aprenda a usar e administrar o sistema operacional aberto da Sun

OpenSolaris 2008.11, parte 2

Continuando a série sobre o OpenSolaris, conheça alguns detalhes sobre a administração de servidores.

por Alexandre Borges

Na edição 54 da **Linux Magazine**, que trouxe encartados um *live CD* do OpenSolaris 2008.11 e um DVD com softwares diversos da Sun Microsystems, apresentamos esse sistema operacional e seu processo de instalação [1].

Este artigo retoma a explicação sobre os recursos do sistema de código aberto da Sun e sua administração. Portanto, partimos do ponto em que o artigo anterior terminou, isto é, um sistema OpenSolaris já instalado, seja numa máquina virtual, seja no sistema físico.

Dicas

No OpenSolaris, certos assuntos precisam ser levantados, principalmente se o usuário estiver mais acostumado a trabalhar no Linux.

O primeiro trata dos diretórios importantes no sistema da Sun (**tabela 1**). Além disso, no OpenSolaris o *terminal* serve para o usuário trabalhar, o que é totalmente diferente do *console*, que, além de poder ser utilizado como meio de trabalho, é principalmente usado pelo kernel para envio de mensagens importantes do sistema; ou seja, é aconselhável deixar um console aberto enquanto se trabalha, apenas para acompanhar tais mensagens. Para abri-lo, use o comando:

```
# /usr/X11/bin/xterm -C &
```

Além de poder verificar o console para mensagens de sistema, o leitor pode conferir os dois principais arquivos de log da máquina:

```
# more /var/adm/messages
# more /var/log/syslog
```

Muitas vezes é necessário verificar quanta memória o sistema operacional pode utilizar. Para isso, basta o comando:

```
# prtconf | grep -i memory
```

Também é possível saber mais sobre o hardware (barramento, processador, memória, I/O):

```
# prtdiag -v | more
```

Outra forma de obter informações do processador utilizado é o comando `psrinfo`:

```
# psrinfo -pv
```

O OpenSolaris é distribuído com um novo *build* a cada seis meses. Para que o leitor possa saber qual deles está usando, basta consultar o conteúdo do arquivo `/etc/release`.

Uma forma muito rápida de configurar manualmente a rede no OpenSolaris é pelo menu *System* | *Administration* | *Network* (**figura 1**). Isso não costuma ser necessário, já que o OpenSolaris cuida disso automaticamente por meio de um serviço chamado NWAM (*Network AutoMagic*) e faz a devida seleção de dispositivos de rede, além de cuidar da configuração da placa de rede via DHCP.

Mas é preciso ter cuidado: ao entrar neste utilitário de configuração manual, o OpenSolaris **desabilita** o serviço NWAM. Para reativá-lo, use o comando `svcadm`:

```
# svcadm disable network/
➥physical:default
# svcadm enable network/
➥physical:nwam
```

Uma maneira bem conhecida para verificar a configuração de rede do OpenSolaris é usando o tradicional comando `ifconfig -a`.

Para conexões remotas, sabe-se que o SSH é preferido sobre o vulnerável e venerável telnet. No OpenSolaris, o único serviço de conexão remota que vem habilitado por padrão é o SSH.

Os *runlevels* no OpenSolaris são diferentes dos usados pelo Linux. Para desligar o sistema, basta invocar o runlevel 5 com um dos seguintes comandos:

```
# init 5
# shutdown -i 5
```

SEMINÁRIO de Gestão de Processos

BPM

23 de junho de 2009 - São Paulo
Hotel Tryp Paulista
Haddock Lobo, 294 - Cerqueira Cesar - São Paulo

Programação Temária

Tutoriais

BPM e metodologias de gerenciamento de projetos
Qualidade e Produtividade com BPM

Palestras

Do Feudo ao Escritório de Processos
Escritório de Processos - Uma abordagem pragmática e viável através da automação e da perseverança
Mobilização de Processos

Caso de Sucesso

Automação do processo de acreditação de organismos de certificação

Faça agora a sua inscrição!
www.ideti.com.br/bpm/inscricao

Aproveite a oportunidade de conhecer o que há de melhor no cenário BPM.
02 Tutoriais, 03 Palestras Técnicas, 01 Caso de Sucesso (em um único dia!!)

Informações: 11 5531-3899 ramal 213
bpm@ideti.com.br
www.ideti.com.br/bpm

Organização e Realização
IDETI
eventos em tecnologia da informação

O runlevel 6, no entanto, é equivalente ao do Linux, e reinicia o sistema.

Muito cuidado: quando o Grub invoca o OpenSolaris, ele carrega na memória uma imagem com alguns módulos do kernel muito importantes. Essa imagem é nomeada pelo OpenSolaris com a inicialização *archive*. Se o sistema não for corretamente desligado, o chamado *boot-archive* poderá ser corrompido. Nesse caso, o sistema entrará em modo de manutenção e o administrador precisará atualizar o boot-archive da seguinte forma:

```
# svcadm clear system/
➥boot-archive/etc/default/init
# bootadm update-archive
# init 6
```

Idiomas

Muitas pessoas querem trabalhar com o OpenSolaris em diversos documentos e, não obstante, acabam inadvertidamente escolhendo o locale errado na hora da instalação. O locale altera não apenas o idioma que será usado, mas também moeda, formato decimal, data e hora, e ainda outros itens mais esotéricos.

É possível alterar o idioma antes de fazer login. Na tela de login, basta acionar *Select Language* e selecionar ≠o idioma desejado. Após o login, o sistema pergunta ao usuário se deve tornar aquele idioma o padrão. O único inconveniente nisso é que essa alteração vale somente para aquele usuário e para o ambiente gráfico

Tabela 1: Diretórios importantes do OpenSolaris

`/dev/`	Diretório com o nome lógico de todos os dispositivos do sistema, que são links simbólicos para o diretório `/devices/` (que possui a representação física dos dispositivos).
`/dev/fd/`	Descritores de arquivos (*file descriptors*), ou seja, objetos que representam arquivos abertos no sistema.
`/dev/rmt/`	Dispositivos de fita.
`/dev/term/`	Representações de dispositivos seriais.
`/etc/`	Como no Linux, é o local em que a imensa maioria dos arquivos de configuração se localizam.
`/kernel/`	Diretório com os módulos do kernel e o próprio kernel (`/kernel/genunix` em 32 bits, ou `/kernel/amd64/genunix` em 64 bits), que são independentes da plataforma, ou seja, independentes da arquitetura e da categoria do sistema.
`/lib/`	Bibliotecas compartilhadas do sistema. Assim como no Solaris 10, os aplicativos do OpenSolaris são linkados dinamicamente.
`/opt/`	Diretório padrão para instalação de pacotes de aplicativos.
`/platform/`	Diretório com os módulos do kernel e o próprio kernel (`/platform/i86pc/kernel/unix` em 32 bits e `/platform/i86pc/kernel/amd64/unix` para 64 bits) que são dependentes da plataforma, ou seja, dependentes da arquitetura e da categoria do sistema.
`/proc/`	Como no Linux, diretório que armazena informações sobre processos.
`/rpool/boot/grub/`	Menu do Grub.
`/tmp/`	Arquivos temporários. Cuidado, pois, no OpenSolaris o conteúdo deste diretório fica na memória, ou seja, seu conteúdo é perdido a cada desligamento.
`/usr/bin/`	Diretório padrão para comandos.
`/usr/gnu/bin/`	Versões GNU de comandos que são encontrados no `/usr/bin`.
`/usr/sbin/`	Ferramentas de sistema usadas na administração do OpenSolaris.
`/usr/sfw/bin/`	Ferramentas provenientes do repositório *Sunfreeware* que são, na maioria dos casos, GNU.
`/usr/bsd/`	Utilitários que seguem o padrão BSD.
`/usr/X11/bin/`	Comandos do X11.
`/sbin/`	Ferramentas de sistema e alguns scripts.
`/var/`	Diretório com arquivos temporários, arquivos de log e arquivo de status.
`/var/run/`	Arquivos de lock e de referências para processos.
`/var/spool/`	Emails, fila de impressão etc.

Gnome. Conexões remotas com a máquina utilizarão o idioma padrão do sistema.

Para alterar o locale padrão do sistema, é necessário editar o arquivo e alterar o valor da variável `LANG`. Os valores disponíveis para fazer essa troca estão em `/usr/lib/locale/`. Depois disso, é necessário reiniciar o sistema operacional.

Para verificar o locale atual, basta usar o comando `locale` sem argumentos.

Tela remota

Uma das capacidades mais simples e úteis do OpenSolaris é sua capacidade (embutida no X Windows) de exportar a tela da área de trabalho para um sistema remoto usando o conhecido protocolo VNC. As configurações são feitas em *System | Preferences | Desktop Sharing*. O administrador pode configurar se o compartilhamento é total ou apenas para visualização, e também pode inserir uma senha para controlar o acesso, entre outras possibilidades.

Para visualizar a área de trabalho remotamente, o administrador pode baixar o cliente VNC (*vncviewer*) que já está incluso no OpenSolaris e nas distribuições Linux, assim como pode baixar a versão para Windows [2]. Para se conectar ao computador remoto (com IP 192.168.1.103, por exemplo):

```
# vncviewer 192.168.1.103
```

Muitas vezes o administrador sequer terá ambiente gráfico na máquina, quando tratar-se de um servidor. Mesmo assim, ainda é possível usar o servidor VNC para fornecer uma sessão gráfica para um cliente externo que esteja, por exemplo, em um laptop. Para isso, são necessários alguns passos.

Primeiramente, adicionar as seguintes linhas ao arquivo `/etc/X11/gdm/custom.conf`:

```
[xdmcp]
Enable = true
[security]
DisallowTCP=false
```

Em seguida, ativar o início automático do serviço *xvnc-inetd* e reiniciar o *gdm*:

```
# svcadm enable
➥xvnc-inetd
# svcadm restart gdm
```

Feito isso, já podemos nos conectar a esse servidor OpenSolaris com um cliente VNC.

Figura 1 Se for preciso configurar a rede manualmente, é fácil fazê-lo pelo utilitário gráfico.

Por fim, é desejo de muitos administradores impedir totalmente o carregamento do ambiente gráfico, seja localmente ou via VNC, a fim de economizar memória e reduzir as brechas de segurança. Para fazer isso, basta desativar o serviço *gdm*:

```
# svcadm disable gdm
```

Porém, se o ambiente gráfico tiver sido desativado por falha de configuração, basta reconfigurá-lo com:

```
# /usr/X11/bin/Xorg -configure
```

e em seguida reiniciar a sessão do X:

```
# svcadm enable gdm
```

Conclusão

O OpenSolaris veio para estabelecer de fato sua posição no mundo do Código Aberto. Ele possui todas as qualidades do Solaris e agrega muitas outras, tendo agora uma vertente de desenvolvimento independente e servindo de inspiração para outros projetos ainda mais interessantes.

Nos próximos artigos desta série sobre o sistema operacional de código aberto da Sun, exploraremos os muitos recursos do OpenSolaris com o objetivo de oferecer a oportunidade ao leitor de aprender as características fantásticas desse novo sistema. ■

Mais informações

[1] Alexandre Borges, "OpenSolaris 2008.11": http://lnm.com.br/article/2753

[2] Real VNC para Windows: http://realvnc.com/products/free/4.1/winvncviewer.html

Sobre o autor

Alexandre Borges é Especialista Sênior em Solaris, OpenSolaris e Linux. Trabalha com desenvolvimento, segurança, administração e performance desses sistemas operacionais, atuando como instrutor e consultor. É pesquisador de novas tecnologias e assuntos relacionados ao kernel.

Explore o multicast IP no Linux

Múltiplos ouvintes

Conheça o lado prático do multicast, incluindo uma configuração de exemplo que usa o pacote de roteamento XORP.

por Tomasz Bartczak, Maciej Piechowiak, Tomasz Szewczyk e Piotr Zwierzykowski

As ubíquas redes IP já suportam transmissões multicast há quase 20 anos, mas só recentemente essa tecnologia ganhou mais atenção. Como o nome sugere, *multicast* é uma técnica para transmitir dados de uma única origem para um conjunto pré-definido de destinos. Esse conceito impõe alguns desafios especiais ausentes nas técnicas mais convencionais de transmissão, como *broadcast*, na qual a mensagem é enviada para **todos** os computadores de um segmento de rede, e *unicast*, em que uma mensagem passa de uma única origem para um único destino.

O uso eficaz do multicast pode reduzir significativamente o tráfego, principalmente em redes que suportam transmissões multimídia tipo *streaming*. As aplicações e tecnologias com multicast receberam cada vez mais atenção com o crescimento das tecnologias audiovisuais; entretanto, o multicast permanece um mistério para muitos desenvolvedores de software, administradores de sistema e usuários finais que poderiam beneficiar-se de um uso mais difundido dessa promissora técnica. Este artigo oferece uma visão dos aspectos práticos do multicast, incluindo uma configuração de exemplo que utiliza o pacote livre de protocolo de roteamento XORP.

O que é?

As **figura 1** e **2** mostram a ideia por trás da transmissão multicast. A origem *A* gera uma sequência de dados com taxa de 1 Mbps, e essa sequência é recebida por três destinatários. A transmissão resulta em três correntes de dados independentes, porém idênticas, o que significa que é consumida uma banda de 3 Mbps no link entre a origem e as redes de distribuição. Por outro lado, um cenário com multicast (veja a **figura 2**) requer apenas uma sequência de dados a partir da origem, então a carga sobre o link é constante e independente do número de destinatários.

Camada de enlace

A transmissão na camada de enlace é realizada com uso do endereço MAC, que identifica uma interface de rede no enlace. Endereços MAC são mapeados para seus respectivos IPs com ajuda do *address resolution protocol* (ARP, protocolo de resolução de endereços) e do seu parceiro RARP (*reverse ARP*). Por exemplo, se o roteador *B* quiser enviar dados para o roteador *D*, primeiro ele envia uma requisição ARP para o IP de *D*. Em resposta,

D envia uma resposta ARP que contém seu endereço MAC. Assim que o processo termina, B e D já podem comunicar-se pelo meio Ethernet. No caso do multicast, a questão é como obter o endereçamento na camada de enlace sem incorrer no trabalho adicional de resolver um endereço IP para uma rede complexa de endereços MAC de destino.

Esse problema específico é resolvido mapeando-se um endereço IP multicast para um único endereço MAC que então é usado por todos os destinatários. Um endereço MAC consiste em 48 bits. Endereços Ethernet que começam com a sequência de bits *01.00.5E* são atribuídas ao IANA (*Internet Assigned Number Authority*, a organização responsável por gerenciar faixas de IP). O IANA decidiu alocar metade da faixa de endereços Ethernet ao propósito da transmissão multicast. Como resultado, 23 bits do endereço MAC estão disponíveis para as comunicações em grupo.

No entanto, um endereço IP possui 32 bits, o que significa que 32 bits do IP devem ser mapeados para 23 bits do endereço MAC. Todos os IPs classe D são reservados para transmissão multicast. Os IPs classe D começam com o padrão de bits *110*. Como esse padrão é constante para todos os endereços multicast, ele não precisa fazer parte do mapeamento. Consequentemente, somente 28 bits do endereço IP são mapeados para os 23 bits do endereço MAC. A **figura 3** mostra como funciona o procedimento de mapeamento.

Como se pode ver na **figura 3**, após descartar os primeiros 4 bits, os 5 seguintes também são ignorados. Em seguida, os 23 restantes são diretamente mapeados para o endereço MAC. Note que esse mapeamento de IP para MAC multicast tem ambiguidades: a relação entre IPs e MACs não é um-para-um. Consequentemente,

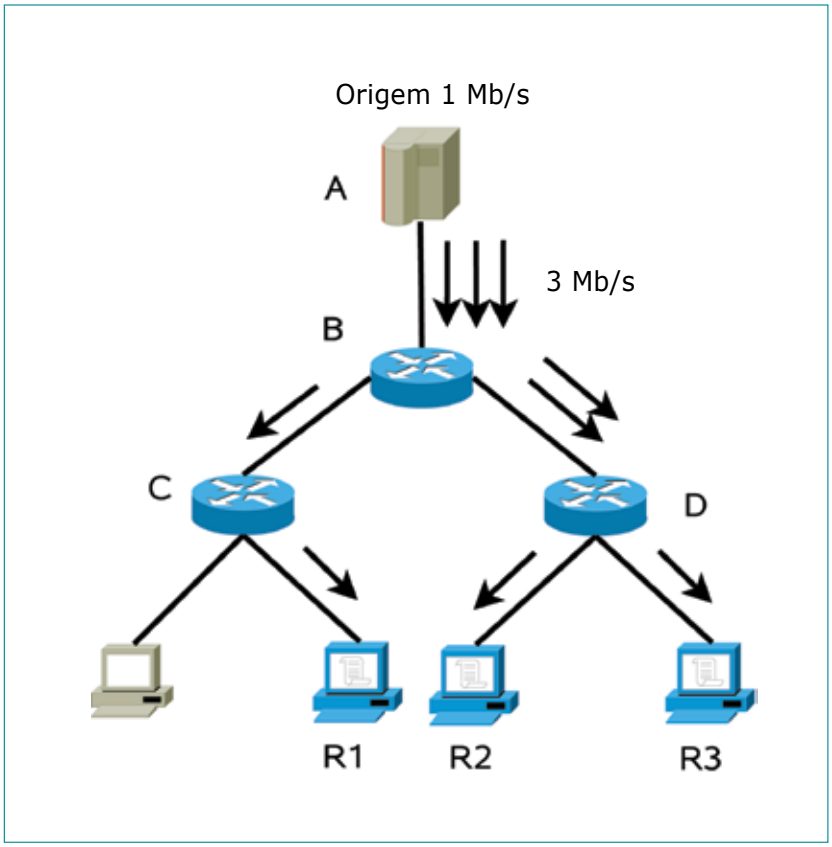


Figura 1 Transmissão unicast tradicional.

2^5 endereços IP grupais possuem os mesmos endereços MAC.

Um exemplo simples ilustra esse processo. Considere o endereço multicast 239.16.16.46, que possui a seguinte representação binária: *111 01111.00010000.00010000.00101110*.

Descartando os 4 bits mais significativos (o padrão da classe D), temos a sequência *1111.00010000.0 0010000.00101110*.

Se omitirmos os próximos 5 bits, teremos *0010000.0010000.00101110*, que, combinados com a sequência atribuída pelo IANA para transmissões multicast, chegam ao endereço MAC 01.00.5E.10.10.2E correspondente ao IP 239.16.16.46.

Como funciona

Quando um aplicativo requisita a recepção de uma transmissão multicast, o subsistema de rede do kernel computa o endereço MAC correspondente. Esse endereço em seguida é adicionado à lista de endereços multicast recebidos; por último, o kernel chama `set_multicast_list` a partir da estrutura `net_device`. A função `set_multicast_list` efetua algumas ações específicas do hardware no nível do driver, para que a placa de rede consiga receber os pacotes enviados para esse endereço MAC específico.

A **figura 4** mostra um exemplo de transmissão multicast realizada entre dois sistemas conectados ao mesmo segmento de rede Ethernet. O aplicativo do computador *A* transmite dados para o endereço multicast 239.16.16.46 (etapa *1a* da **figura 4**). O aplicativo passa os dados, juntamente com o endereço de destino, para o kernel. Em seguida, o kernel computa um endereço MAC correspondente a esse IP.

Na outra ponta, o aplicativo no computador *B* informa ao kernel Linux que está interessado em re-

ceber uma transmissão multicast enviada para o IP 239.16.16.46 (etapa *1b* da **figura 4**). O kernel computa o endereço MAC correspondente a ese IP (*2b*) e informa qual placa de rede deve receber os pacotes enviados a esse MAC (*3b*). Após receber o pacote de dados (*4b*), a placa de rede instalada no computador *B* gera uma interrupção e chama o método responsável por lidar com a interrupção (*5b*). Esse método entrega ao kernel os dados recebidos (*6b*), que ao final repassa os dados para o aplicativo (*7b*).

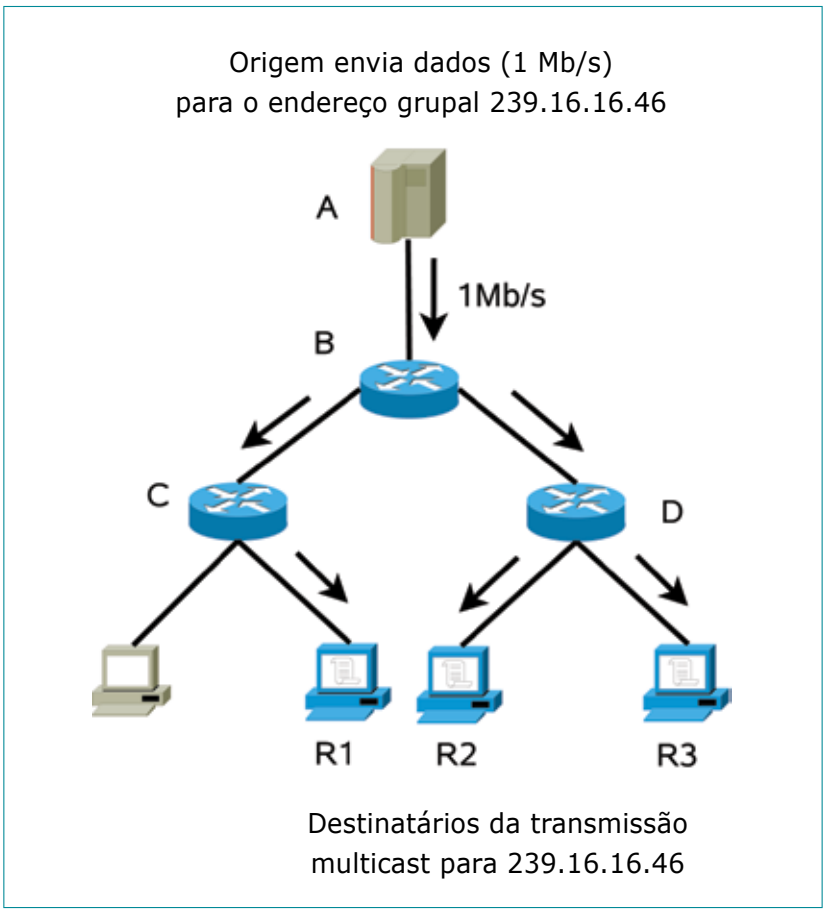


Figura 2 Transmissão multicast.

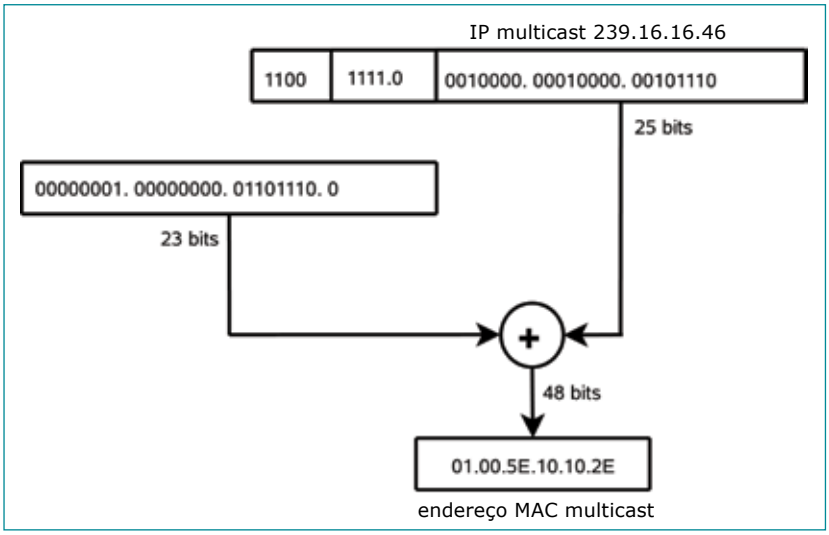


Figura 3 Mapeamento de um IP multicast para um endereço MAC.

Protocolos de roteamento

O multicast é tão eficiente que talvez você imagine por que não estamos todos usando-o. O problema é a necessidade de incluir mais funcionalidades na rede de transmissão para garantir o serviço adequado e a replicação da sequência única de dados por uma grande rede roteada. Passar os dados de forma eficiente através de uma corrente de roteadores requer uma nova classe de protocolos de roteamento multicast especiais. Infelizmente, eles são um tanto complexos, e portanto raramente implementados pelos provedores de acesso.

Um protocolo de roteamento multicast precisa suportar a possibilidade de encaminhar um único pacote para múltiplas interfaces. Atualmente, o protocolo de roteamento multicast mais popular é o PIM-SM (*Protocol-Independent Multicast-Sparse Mode*). A principal tarefa do protocolo PIM-SM é criar uma árvore de distribuição multicast que entregue pacotes multicast da origem para os destinatários. Em transmissões multicast, o PIM-SM mantém uma tabela de roteamento separada, chamada *Multicast Forwarding Cache* (MFC).

O PIM-SM também usa uma tabela de roteamento unicast para fornecer uma ambiente de encaminhamento livre de loops para entregas multicast. Portanto, para garantir o funcionamento apropriado do protocolo PIM-SM, também é necessário configurar as tabelas de roteamento unicast nos computadores que estão envolvidos na transmissão multicast.

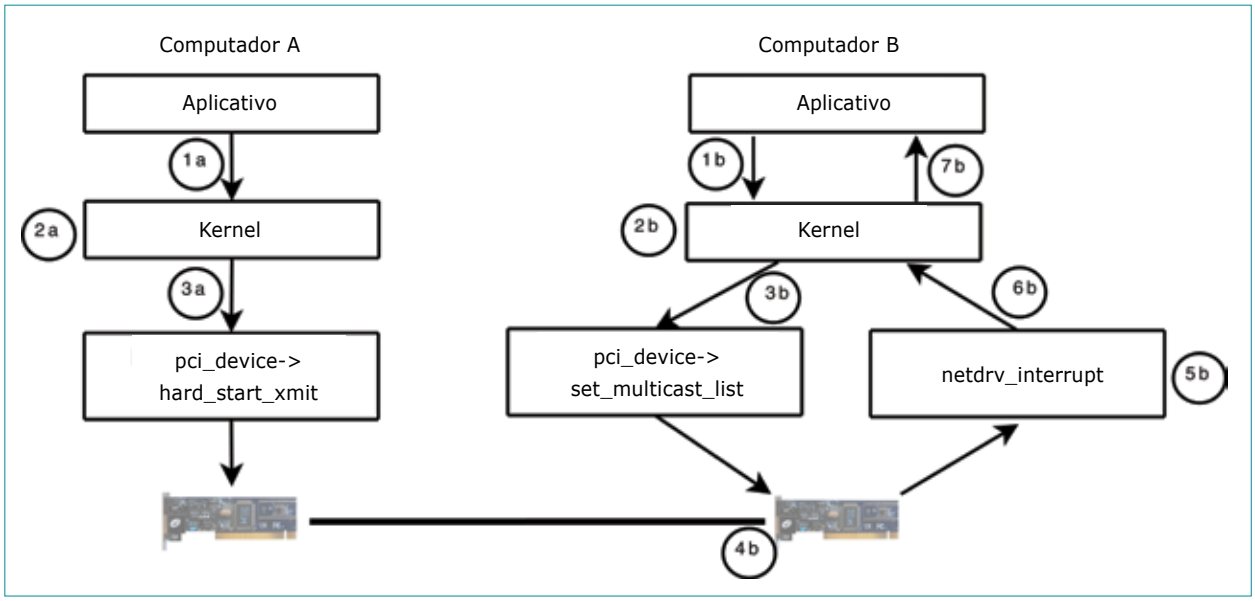


Figura 4 Esquema de transmissão multicast.

O protocolo PIM-SM utiliza o conceito de um *ponto de encontro* para gerenciar a comunicação multicast. O ponto de encontro é um roteador que recebe as requisições de transmissão feitas pelos destinatários. As origens de transmissão enviam seus dados para o ponto de encontro. O PIM-SM pode definir o ponto de encontro de forma dinâmica, ou o usuário pode atribuir o papel diretamente em sua configuração.

Configuração do roteamento

O XORP é um pacote de roteamento livre que inclui uma implementação excepcionalmente boa do protocolo PIM-SM [1]. Uma rápida inspeção do roteamento multicast com o XORP já deve oferecer uma boa noção de como começar seus experimentos com o multicast.

Primeiramente, baixe o código-fonte no site do projeto [2] (este artigo usa a versão 1.5, de julho de 2008) e instale-o com:

```
./configure
make
make check
make install
```

Este artigo supõe que os módulos responsáveis pelas placas de rede já estejam carregados (ou embutidos no kernel) e que a rede não tenha sido configurada de forma alguma (antes de começar a configuração ferramentas de rede como o *NetworkManager* devem ser desativadas).

O primeiro passo é executar o programa que configura o aplicativo XORP com o comando `xorpsh` (os arquivos executáveis do aplicativo XORP localizam-se em `/usr/local/xorp/bin/`). Como o XORP afeta significativamente o funcionamento do sistema, ele possui dois modos de operação: básico e avançado. No

Listagem 1: Configuração das interfaces de rede

```
01 >configure
02 # set interfaces interface eth0 vif eth0 address 192.168.2.1
➥prefix-length 24
03 # set interfaces interface eth1 vif eth1 address 192.168.3.2
➥prefix-lenght 24
04 # set interfaces interface eth0 vif eth0 disable false
05 # set interfaces interface eth1 vif eth1 disable false
06 # commit
```

Listagem 2: Configuração do OSPF

```
01 # set protocols ospf4 router-id 192.168.2.1
02 # set protocols ospf4 area 192.168.0.0 interface eth0 vif eth0 address 192.168.2.1
03 # set protocols ospf4 area 192.168.0.0 interface eth0 vif eth0 disable false
04 # set protocols ospf4 area 192.168.0.0 interface eth1 vif eth1 address 192.168.3.2
05 # set protocols ospf4 area 192.168.0.0 interface eth1 vif eth1 disable false
06 # commit
```

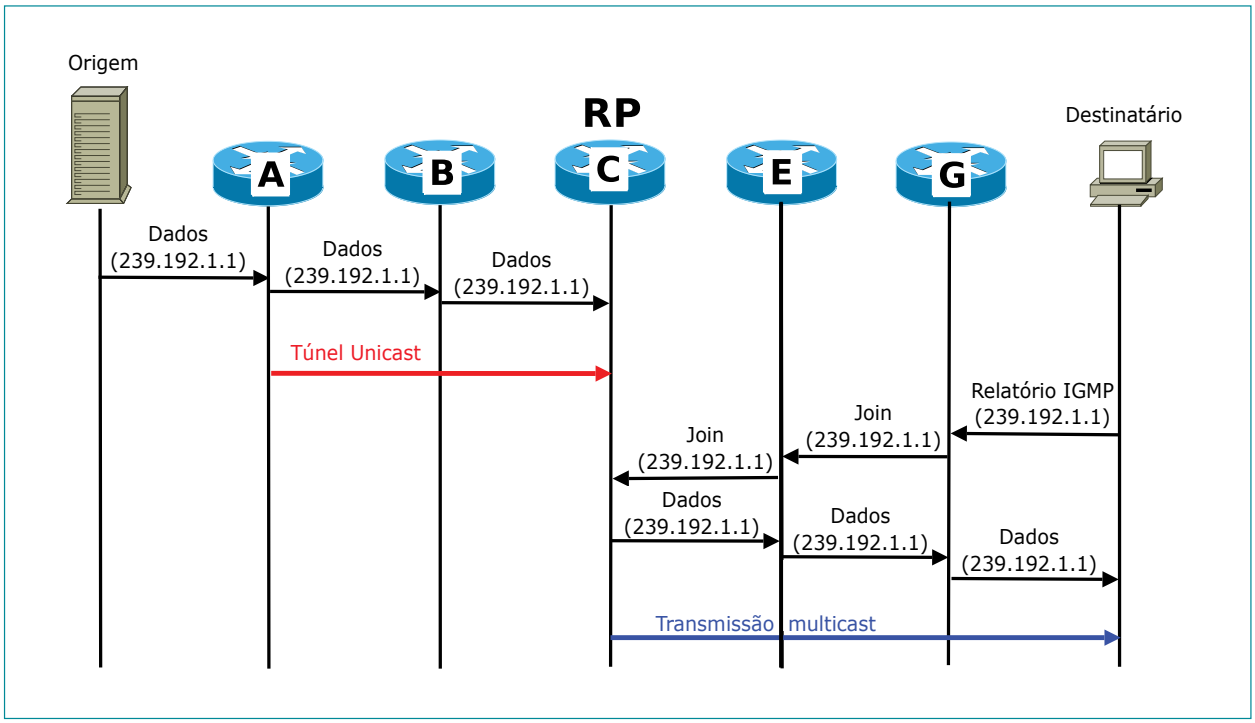


Figura 5 Início de uma transmissão multicast.

modo avançado, é necessário que o usuário pertença ao grupo *xorp* para conseguir iniciar o programa.

Configurar a rede e o protocolo PIM-SM requer os seguintes passos:

- ativar as interfaces de rede e atribuir-lhes IPs;
- configurar o roteamento unicast,
- ativar o encaminhamento de pacotes multicast;
- ativar o protocolo PIM-SM;
- ativar o IGMP para roteadores em proximidade direta dos destinatários da transmissão em grupo.

A interface de gerenciamento do XORP é semelhante à dos dispositivos Juniper. A **listagem 1** mostra a configuração das interfaces de rede.

O primeiro comando da **listagem 1** entra no modo avançado, no qual é possível alterar a configuração do dispositivo. Os dois comandos `set interfaces` seguintes são responsáveis pela configuração das interfaces de rede. Como se pode ver, a sintaxe do comando é bem simples e não requer explicações. Nos próximos passos as interfaces são ativadas. O último comando é o `commit`, que permite a execução dos comandos anteriores.

Listagem 3: Ativação da transmissão multicast

```
01 # set plumbing mfea4 disable false
02 # set plumbing mfea4 interface eth0 vif eth0 disable fasle
03 # set plumbing mfea4 interface eth1 vif eth1 disable fasle
04 # set plumbing mfea4 interface register_vif vif register_vif
➥disable fasle
05 # commit
```

Listagem 4: Configuração do PIM-SM

```
01 # set protocols pimsm4 interface eth0 vif eth0 disable false
02 # set protocols pimsm4 interface eth1 vif eth1 disable false
03 # set protocols pimsm4 interface register_vif vif register_vif
➥disable false
04 # set protocols pimsm4 static-rps rp 192.168.3.1 group-prefix
➥224.0.0.0/4
05 # commit
```

Ativar unicast

Como dito anteriormente, o protocolo PIM-SM usa uma tabela de roteamento unicast para descobrir para onde enviar as mensagens de *Join*. Tabelas de roteamento de roteadores individuais podem ser configuradas manualmente com os comandos `route` e `ip`. Essa técnica, no entanto, é problemática e sujeita a erros, pois requer intervenção do operador toda vez que a configuração for alterada.

Os protocolos de roteamento dinâmico permitem a determinação automática das tabelas de roteamento. Um protocolo dinâmico

comum suportado pelo XORP é o OSPF (*Open Shortest Path First*). Uma discussão completa dos protocolos de roteamento unicast vai além do escopo deste artigo; entretanto, as etapas de configuração na **listagem 2** mostram como configurar o roteamento unicast com o OSPF.

Além disso, é preciso ativar o encaminhamento de dados por unicast com:

```
# set fea unicast-forwarding4
# commit
```

Ativar multicast

A **listagem 3** exibe os passos para ativar transmissões multicast. Como se pode ver, o multicast é ativado em interfaces individuais e na interface unicast.

A última etapa de configuração é a ativação do protocolo PIM-SM. Para isso, primeiro inicie o *daemon* do protocolo PIM:

```
# set protocols pimsm4 disable
➥false
# commit
```

O comando `commit` será executado com um pequeno atraso, devido ao início do processo responsável pelo serviço do protocolo de roteamento multicast. Os comandos posteriores, apresentados na **listagem 4**, configuram o protocolo PIM-SM.

Os comandos da **listagem 4** ativam o serviço do protocolo PIM-SM em interfaces individuais, assim como na interface virtual `register_vif`, que é usada para transmitir dados através de um túnel unicast desde a origem até o ponto de encontro. Além disso, é alocado o endereço do ponto de encontro – 192.168.3.1, neste caso. A configuração de *group-prefix* denota a faixa de endereços multicast servidos por um dado ponto de encontro.

Ativar IGMP

A configuração apresentada até aqui possibilita a transmissão de dados da origem para destinatários individuais. Estes, no entanto, precisam ser capazes de informar aos roteadores que estão interessados em receber transmissões multicast. Conforme descrito anteriormente, essa informação passa por meio da rede via IGMP, então é preciso configurar o IGMP nos roteadores que possuem destinatários locais.

Nesse ponto, talvez não esteja claro por que é necessário configurar o IGMP por meio do XORP quando o kernel já tem suporte ao IGMP.

O problema é que a implementação do IGMP incluída no kernel não oferece o lado servidor do protocolo, o que significa que essa implementação não é capaz de encaminhar informações em mensagens IGMP para o protocolo de roteamento multicast.

Como no caso do PIM-SM ou OSPF, a configuração do IGMP requer a ativação de um daemon responsável pelo serviço do protocolo:

```
# set protocols igmp disable false
# commit
```

Além disso, é preciso indicar as interfaces servidas pelo IGMP:

```
# set protocols igmp interface
➥eth2 vif eth2 disable false
# commit
```

Junta tudo

A **figura 5** mostra a transação inteira de uma vez. Como se pode ver, o computador à esquerda começa enviando uma sequência de vídeo para o IP *239.192.1.1*. O roteador *A*, conectado diretamente à origem, começa enviando dados para o ponto de encontro através de um túnel unicast. O aplicativo na extremidade receptora gera uma mensagem de relatório IGMP. Essa mensagem é processada pelo roteador e é seguida por uma mensagem *Join* do protocolo PIM-SM, enviada para o roteador *C*, que está agindo como ponto de encontro (RP, *Rendezvous Point*). Ao receber a mensagem, o roteador *C* envia a transmissão multicast na direção de seu destinatário, juntamente com todos os demais destinatários pertencentes ao grupo de destino dos dados multicast.

Conclusão

O multicast é uma questão complexa, e este artigo apresentou os conceitos básicos. Essa breve introdução deve ser suficiente para oferecer uma noção para determinar a melhor forma de implementar o multicast no seu ambiente de trabalho. ■

Mais informações

[1] XORP: http://www.xorp.org/

[2] Download do XORP: http://www.xorp.org/downloads.html

Sobre o autor

Ao longo dos últimos anos, os autores **Tomasz Bartczak**, **Maciej Piechowiak**, **Tomasz Szewczyk** e **Piotr Zwierzykowski** trabalharam com tecnologias de rede e sistemas operacionais Linux/Unix. Além disso, têm interesse em atividades de pesquisa com foco em algoritmos de multicast e otimização de protocolos.

Infraestrutura de chaves públicas com o Dogtag

Mestre das chaves

Se você deseja ter mais controle da sua infraestrutura de chaves públicas, experimente o sistema de certificados Dogtag.

por Thorsten Scherf

A criptografia assimétrica oferece uma forma poderosa e conveniente para criptografar comunicações via Internet. Nesse cenário, cada entidade envolvida no sistema de criptografia possui um par de chaves: uma pública e outra privada.

Se Alice quiser enviar uma mensagem criptografada para Bob, ela precisa obter a chave pública de Bob para colocá-la em seu chaveiro. O software de criptografia do computador de Alice em seguida usa a chave pública de Bob para criptografar a mensagem, e o computador de Bob utiliza a chave privada dele para decifrá-la.

Esse sistema funciona somente se conseguirmos ter certeza de que as chaves usadas são genuínas – isto é, se pudermos verificar que as chaves realmente pertencem à pessoa a que se referem. É nessa situação que aparece uma Infraestrutura de Chaves Públicas (ICP, ou PKI em inglês). A ICP é uma autoridade central que verifica a autenticidade de chaves públicas (para mais informações sobre o funcionamento de uma ICP, veja o **quadro 1**). Assim que a autenticidade da chave é verificada, a autoridade certificadora assina a chave para confirmar sua validade. O resultado é chamado de certificado digital.

Diversas autoridades certificadoras comerciais emitem e validam certificados mediante uma taxa. Autoridades gratuitas e comunitárias, como o CAcert.org [1], também oferecem serviços de certificação. Porém, em alguns casos pode ser preferível manter a sua própria autoridade certificadora dentro da empresa simplesmente como forma de economizar dinheiro. Em outros casos, o alcance global de uma autoridade baseada na Internet talvez seja desnecessário para um sistema que esteja operando numa rede local, ou um servidor local de certificados pode fazer parte de uma infraestrutura maior.

Muitos administradores preocupados com segurança preferem manter seus próprios sistemas de Autoridade Certificadora (AC) simplesmente porque não confiam em organizações externas para lidar com uma tarefa crítica. A recente controvérsia a respeito dos certificados baseados em *MD5* fornecidos por várias ACs comerciais [2] oferece novos argumentos para os administradores que optam por manter um rígido controle.

Em março de 2008, a Red Hat liberou o código-fonte do *Red Hat Certificate System*. Esse código finalmente encontrou um lar no sistema de certificados *Dogtag* [3], patrocinado pelo projeto Fedora. O Dogtag é uma ferramenta poderosa para usuários que desejem implementar uma ICP completa.

Dogtag

O Dogtag está disponível na versão 8 (e mais recentes) do Fedora como uma implementação de ICP em código aberto. Para instalar os pacotes, basta copiar o arquivo de configuração do repositório `pki.repo` para o diretório de repositórios do *Yum*, `/etc/yum.repos.d/`. Para armazenar os certificados, o Dogtag precisa do *Fedora Directory Server* (FDS), que pode ser instalado a partir do repositório do Yum. Há um tutorial de instalação no site do projeto [4]. O agente de registro precisa de um banco de dados *SQLite*, que está disponível nos repositórios padrão do Fedora.

A ferramenta de administração *pkiconsole* oferece uma interface gráfica. Ela requer a máquina vir-

Quadro 1: Dentro de um PKI

Um PKI abrange vários componentes, alguns opcionais. Esses componentes incluem:

- Autoridade Certificadora (AC ou CA, em inglês);
- Autoridade de Registro (RA);
- Lista de Revogação de Certificados (CRL);
- Serviço de diretório – Servidor LDAP;
- Serviço de validação – *Online Certificate Status Protocol* (OCSP);
- Agente de Recuperação de Dados (DRA);
- Certificados – X.509.

A AC é a entidade que emite os certificados; ela pode validar chaves públicas anexando sua assinatura. Em muitos casos, há toda uma hierarquia de autoridades certificadoras na qual a mais alta, conhecida como AC raiz, somente emite certificados de assinatura para ACs subordinadas. As autoridades hierarquicamente mais baixas autenticam usuários e chaves de servidores. Num cenário assim, a AC raiz geralmente não é acessível online. A RA aceita requisições de autenticação para chaves e as encaminha para a AC.

A CRL contém um panorama dos certificados inválidos e oferece um meio de verificar a validade de um certificado. Um serviço de diretório como o LDAP serve certificados e CRLs. Quando ocorre uma alteração numa CRL ou quando é emitido um novo certificado, essa informação é imediatamente armazenada no diretório e pode ser consultada por esse mesmo diretório. O OCSP suporta a validação de certificados em tempo real. Se o protocolo estiver ativo num navegador, a validade do certificado é confirmada em tempo real. Essa confirmação ocorre de forma transparente e automática em segundo plano. A DRA também pode armazenar uma cópia de qualquer chave que seja gerada, fornecendo assim a capacidade de recuperar chaves em caso de emergência. Os certificados propriamente ditos usam o formato X.509, que é um padrão de certificado da International Telecommunication Union Telecommunication Standardization Sector (ITU-T).

tual Java (JRE), que também pode ser instalada a partir dos repositórios padrão. Feitos os preparativos, é hora de instalar os subsistemas individuais:

```
yum install pki-ca pki-console
```

Este artigo concentra-se na instalação e configuração do PKI-CA. O projeto Dogtag oferece guias de instalação para os outros subsistemas do Dogtag, incluindo *pki-dra*, *pki-ocsp* e *pki-dra*.

Supondo que o pacote *pki-ca* seja instalado com sucesso, o serviço *pki-ca* será iniciado imediatamente e exibirá uma URL para a próxima etapa da configuração. Um clique na URL chama o navegador web e abre uma interface web que pode ser usada para todas as demais tarefas de configuração (**figura 1**).

A URL contém um PIN para configurar a AC. Se for preferível adiar um pouco a configuração, é possível buscar no arquivo de log, `/var/log/pki-ca-install.log`, a URL e o PIN.

Pela interface web é possível digitar as informações a respeito da AC que está sendo instalada, assim como o servidor de diretório que será usado como *back-end*, informações sobre o nível da sua AC (raiz ou subordinada) e a conta de administração a ser criada.

Também é possível usar uma ferramenta de linha de comando, *pki-create*, para todas essas configurações.

Após responder a todas as perguntas do assistente de configuração, acesse o site da AC no navegador, em `https://servidor:9443`.

Se você precisar acessar a AC como usuário comum para gerar um certificado para você mesmo ou para um serviço de rede, siga o link *SSL End Users Services*, que leva a uma página com vários perfis de certificados.

Os perfis permitem a criação de certificados com parâmetros e pro-

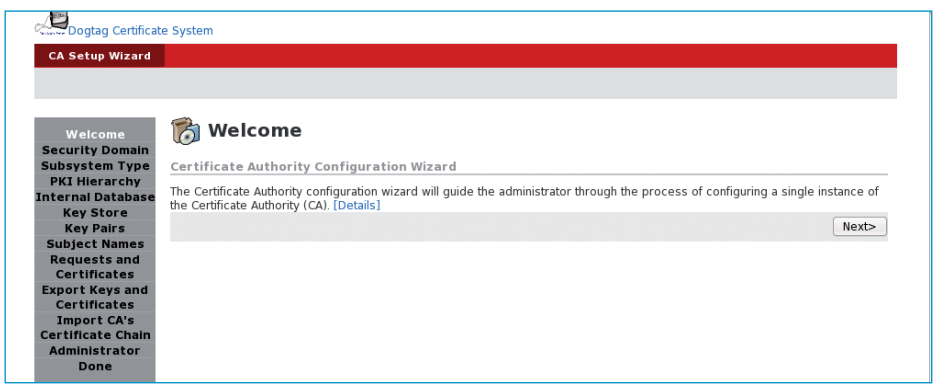


Figura 1 O Dogtag oferece uma conveniente interface web.

Listagem 1: certutil na linha de comando

```
01 certutil -L -d ~/.mozilla/firefox/i1nfei2a.default/ | grep -i tux
02
03 Certificate Authority - Tuxgeek Domain CT,C,C
04 CA Administrator of Instance pki-ca's Tuxgeek Domain ID u,u,u
05 foo1 bar's Tuxgeek Domain ID u,u,u
06 foo2 bar's Tuxgeek Domain ID u,u,u
07 Thorsten Scherf's Tuxgeek Domain ID u,u,u
```

priedades específicos. Por exemplo, o link *Manual User Dual-Use Certificate Enrollment* cria requisições de certificado de usuários.

A chave privada do certificado é gerada diretamente quando a requisição é feita e armazenada na memória de certificados do navegador. Depois, ela será mapeada para o certificado X.509 importado. Se for preciso gerar um certificado para um serviço – um servidor web, por exemplo –, selecione o perfil *Manual Server Certificate Enrollment* na lista de perfis disponíveis para emitir uma requisição de assinatura de certificado (CSR, na sigla em inglês) para o servidor. É relativamente fácil formular uma requisição de certificado de servidor no formato PKCS#10 [5] com o OpenSSL:

```
$ openssl genrsa -des3 -out \
    webserver.key 1024
$ openssl req -new -key \
    webserver.key -out webserver.csr
```

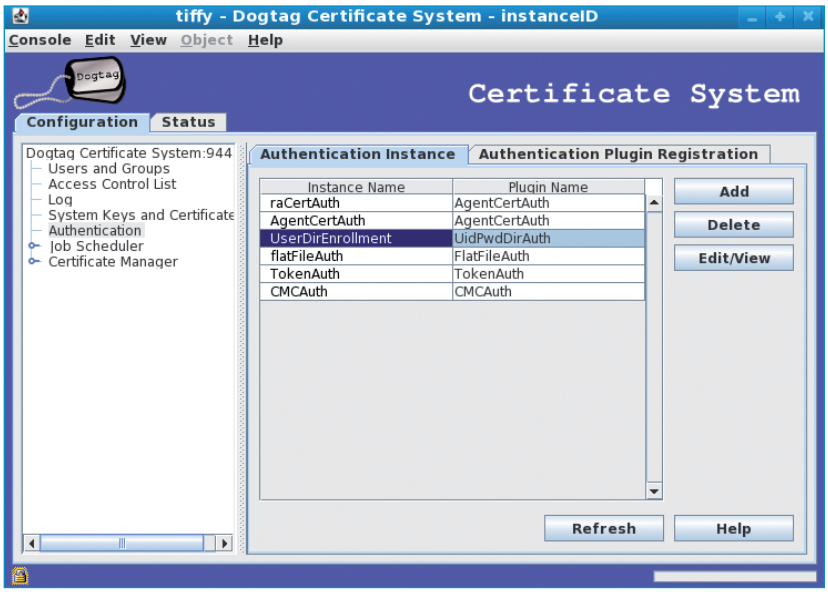


Figura 2 A ferramenta gráfica de administração *pkiconsole* permite a configuração de várias propriedades do Dogtag, tais como autenticação de usuários, a partir do console do Dogtag.

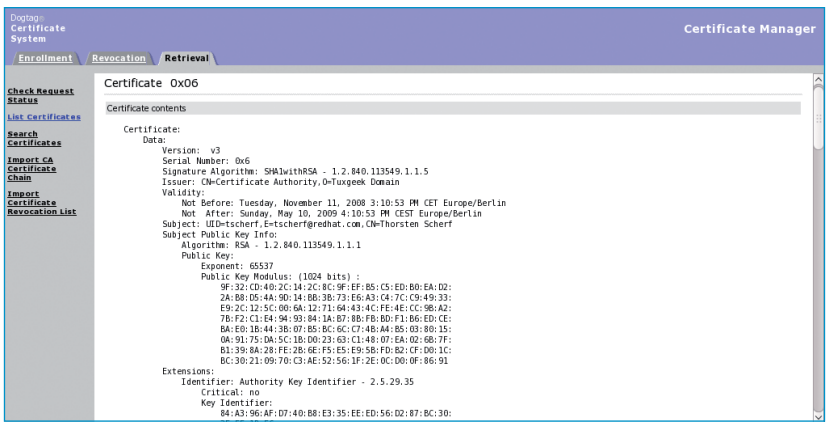


Figura 3 Os usuários podem baixar os certificados gerados pelo Dogtag por meio da página *SSL End Users Services*.

Após enviar a requisição, ela deve ser verificada e confirmada por um administrador da AC ou por um agente da AC com direitos adequados. Para isso, faça login na página inicial da AC e siga o link *Agent Services* para a página de gerenciamento de certificados da AC. Nesse login, é preciso autenticar-se com um certificado. O certificado necessário é gerado quando configuramos o Dogtag e o armazenamos no navegador. Evidentemente, é possível conferir privilégios de gerenciamento da AC a outros usuários a qualquer momento.

Após o login, o item *List Request* oferece uma lista de requisições de assinatura pendentes, que pode ser validada e confirmada. O item *List Certificates* lista todos os certificados autenticados no formato PKCS#7. Se um usuário desejar obter um certificado, basta clicar em *SSL End Users Services* na página principal da AC. A aba *Retrieval* permite listar todos os certificados autenticados ou buscar sua própria requisição por meio da ID da requisição que o Dogtag gera e exibe quando é submetida uma requisição.

Após localizar seu próprio certificado, importe-o para o navegador. Assim como o Dogtag, o Firefox utiliza a biblioteca *Network Security Services* (NSS). Vários arquivos de banco de dados BerkeleyDB são usados como *back-end* de banco de dados para o NSS, cada um dos

Listagem 2: ldapsearch

```
01 ldapsearch -x -b dc=tuxgeek,dc=de -h tiffy.tuxgeek.de uid=tscherf -LLL
02
03 dn: UID=tscherf,ou=people,DC=tuxgeek,DC=de
04 cn: Thorsten
05 sn: Scherf
06 objectClass: top
07 objectClass: person
08 objectClass: organizationalPerson
09 objectClass: inetOrgPerson
10 uid: tscherf
11 userCertificate;binary:: MIIDDzCCAfegAwIBAgIBCTANBgkqhkiG9w0BAQUFADA5MRcwFQYDV
12 QQKEw5UdYhnZWVrIERvbWFpbjEeMBwGA1UEAxMVQ2VydGlmaWNhdGUgQXV0aG9yaXR5MB4XDTA4MT
13 ExMTE3MzkwM1oXDTA5MDUxMDE3MzkwM1owSTERMA8GA1UEAxMIZm9vMiBiYXIxHjAcBgkqhkiG9w0
14 BCQEWD2ZvbzJAdHV4Z2Vlay5kZTEUMBIGCgmSJomT8ixkAQETBGZvbzIwgZ8wDQYJKoZIhvcNAQEB
15 BQADgY0AMIGJAoGBAO22zHGO/tIuKect+DMiWl4l5OtA4oQKp8DbQrBhVl8R4O7MroY6+g6EeDwpJ
16 6NFPFkbrxK4F+e5Pil1Sthr9LVjUb+E1CJGtdsWli3lrEnmdy2NjLRXY1obTwLn2PSd4Q4WGKcYGp
17 BlZT4QmoVhlJ3pByalIIJvRPhrSuZn4VThAgMBAAGjgZUwgZIwHwYDVR0jBBgwFoAUhKOWr9dAuOM
18 17u1WOoe8MD7vG/YwQAYIKwYBBQUHAQEENDAyMDAGCCsGAQUFBzABhiRodHRwOi8vdGlmZnkudHV4
19 Z2Vlay5kZTo5MDgwL2NhL29jc3AwDgYDVR0PAQH/BAQDAgXgMB0GA1UdJQQWMBQGCCsGAQUFBwMCB
20 ggrBgEFBQcDBDANBgkqhkiG9w0BAQUFAAOCAQEApSA7qHWm4dvjf6WcPm9rChDDOOMfbSL8HzCYCd
21 /b5RfrCAB7EOa5wdJNb8ldEi4Zj9OD3r4yxq7QJlOSlKUxd+vmrRLLCeDZZMsFUE5owdOMP7QCSzs
22 T+FMOQZaAVGrKFNbvO6ceuaKssbOHrD6gSAmFpqGP3wEhKHIGt76hHbmsYgl3gMawFpWmzuqEDzlx
23 KMeoOjdQF++icxnh3zpkJSyLwueGM33kQ2zmU6buZfSt/ROJ8qo4Te58Wy/G1lO1eI6NAMdMzKIOr
24 5nQLyEprj6j3ZU99+taxW+tHM9sjBXvEt1PCDTSiSrTv33064+qrEs4EGiaLWfPLikYafmxng==
```

quais guardado num diretório de perfil do Firefox. As listas públicas de revogação de certificados (CRLs, na sigla em inglês) geralmente são armazenadas no arquivo `cert8.db`, e as chaves privadas em `key3.db`. O item *Propriedades* do navegador lista todos os certificados importados.

Para importar os certificados para outro aplicativo como um cliente de email, por exemplo, escolha o formato PKCS#12, que exporta tanto o certificado quanto a chave privada. Se preferir a linha de comando, use a ferramenta `certutil`. O comando exibido na **listagem 1** mostra como obter detalhes do seu próprio armazém de certificados. Obviamente também é possível usar o `certutil` para adicionar novos certificados e apagar os que já existem [6].

O Dogtag pode emitir certificados diretamente, sem necessidade de um agente autenticá-los manualmente. Existem várias técnicas para lidar com isso, sendo o LDAP e a autenticação baseada em PIN as mais comuns. Nos dois casos, os usuários precisam autenticar-se contra um serviço de diretórios com seu nome de usuário e senha antes de emitir a requisição de certificado. No caso da autenticação baseada em PIN, o usuário também precisa fornecer um PIN, que é armazenado como atributo extra no objeto do usuário. Os dois métodos de autenticação podem ser configurados com uso do `pkiconsole`, a ferramenta gráfica de administração executada ao se

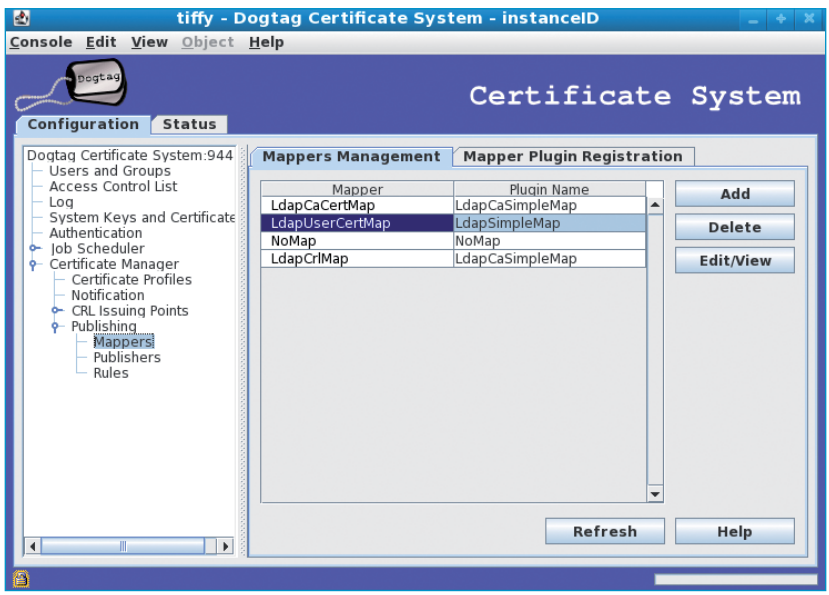


Figura 4 Use o *pkiconsole* para publicar certificados no LDAP.

digitar `pkiconsole https://servidor:9943/ca` (**figura 2**).

Em *Authentication* é possível definir vários plugins para a autenticação de usuários contra o servidor Dogtag. Primeiramente, é preciso selecionar e configurar o plugin *UidPwdDirAuth* na autenticação por LDAP, que se baseia no nome de usuário e senha. Para também exigir um PIN, escolha o plugin *UidPwdPinDirAuth*. Claro que cada objeto de usuário precisará de um atributo PIN. Para configurar isso, use a ferramenta `setpin` do Dogtag. Após configurar a autenticação dos usuários, eles não precisam esperar que um agente autorize suas requisições de certificado manualmente; em vez disso, os certificados gerados automaticamente estão disponíveis na aba *Retrieval* da seção *SSL End Users Services* (**figura 3**).

Em ambientes de grande escala, principalmente, é interessante publicar automaticamente todos os certificados X.509 emitidos num serviço de diretório. Apesar de ser preferível um servidor separado para uso em produção, também é possível usar o servidor de diretório que lida com a configuração do Dogtag. Em ambientes Windows, pode-se usar o servidor Active Directory para publicar os certificados, pois ele é, na verdade, um servidor LDAP. O administrador simplesmente vincula o certificado ao objeto do usuário como mais um atributo binário.

O item de menu *Certificate Manager | Publishing* na aba *Configuration* permite criar um mapeador para certificados de usuários (*LdapUserCertMap*; **figura 4**). O mapeador associa o nome do usuário ao certificado com seu *Distinguished Name* (DN), permitindo assim que se mapeie o certificado para um objeto tangível de usuário. O mapeamento *dnPattern* poderia ser assim:

```
UID=$subj.
➥UID,OU=people,dc=tuxgeek,dc=de
```

Para também guardar as CRLs e o certificado AC no LDAP, acrescente os mapeadores *LdapCaCertMap* e *LDAPCrlMap*. Para finalizar, é preciso adicionar à seção *Publishing* a data de conexão com o serviço de diretório. Feito isso, quando o usuário enviar uma requisição de certificado para o servidor Dogtag, o certificado emitido será imediatamente publicado no servidor LDAP. Uma requisição manual ao servidor de diretório confirma isso (**listagem 2**).

Note que é preciso um objeto para o usuário sob a *Organizational Unit* (OU); caso contrário, o sistema será incapaz de publicar o certificado. Além disso, só ficam disponíveis no LDAP os certificados gerados em resposta a novas requisições; aqueles emitidos antes de definirmos a configuração de publicação não serão automaticamente transferidos para o serviço de diretório, embora seja possível acrescentá-los manualmente depois com o `ldapmodify`.

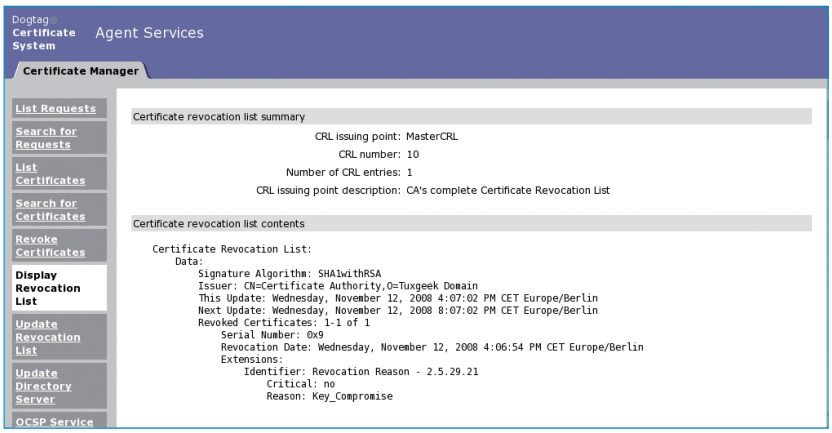


Figura 5 Adição de um certificado de usuário à CRL.

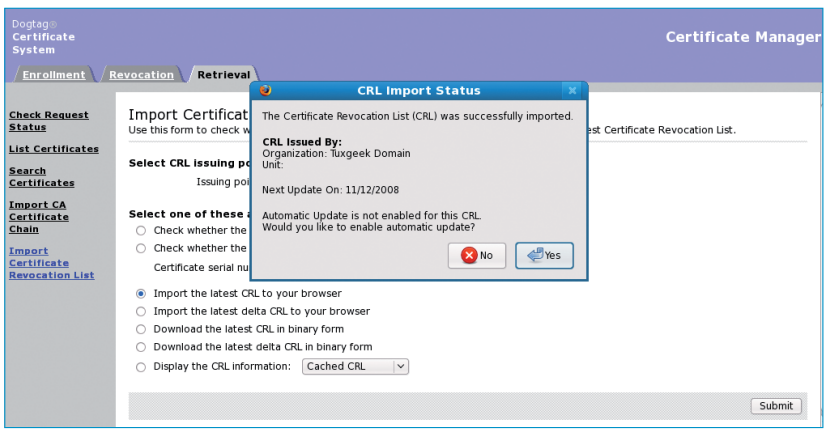


Figura 6 Importação da CRL num aplicativo cliente.

Certificados inválidos

Certificados tornam-se inválidos se, por exemplo, a chave privada for perdida. Para notificar isso a outros aplicativos, é possível criar listas de revogação de certificados (CRLs). Uma CRL é uma lista publicamente acessível que o navegador pode consultar ou importar periodicamente para identificar certificados inválidos.

Tanto o administrador da AC quanto o dono do certificado podem decidir quais certificados incluir na

Listagem 3: Consulta de CRL com ldapsearch

```
01 ldapsearch -LLL -x -b dc=tuxgeek,dc=de -h tiffy.tuxgeek.de -D
02
03 cn="Directory Manager" -w password objectClass=certificationAuthority
04 certificateRevocationList
05 dn: UID=Certificate Authority,OU=people,DC=tuxgeek,DC=de
06 certificateRevocationList;binary:: MIIBtjCBnwIBATANBgkqhkiG9w0BAQUFADA5MRcwFQY
07 DVQQKEw5UdXhnZWVrIERvbWFpbjEeMBwGA1UEAxMVQ2VydGlmaWNhdGUgQXV0aG9yaXR5Fw0wODEx
08 MTMxMjQ2MjZaFw0wODExMTMxNjQ2MjZaMCIwIAIBCRcNMDgxMTEyMTUwNjU0WjAMMAoGA1UdFQQDC
09 gEBoA4wDDAKBgNVHRQEAwIBDDANBgkqhkiG9w0BAQUFAAOCAQEAHpdSIx/tm3uOALqhbKJwdDVUsx
10 V/TaARtJ9Xthw5/EblPTrngNLmN1iVpdBRO2NrOvFfLdqGwDTpli35jUmK4mOyD5viVv1dv9TmEwG
11 aCU2q3SQceRcHAliAJv/2ol28Rr1/Dk+5LtgpppWxia2Smbt8II/ZZPsq1kwy2EmOWR9V8z4OWode
12 Eb3HUQzpZefKje8otH1xSX3eG7roblcVhFP/CnlHGfUDEB1sCGvv9VQkLQQqjQoGKvz2HMs6LiOv1
13 VmRfjXzlblrHBzHSmesliuGaCmZCaHg91WeEic1q7xJfOnw1v+VgpfidEV4gm+Ty5IYICcvEBlN7k
14 wjLbXO6A==
```

lista. Os administradores podem acessar *Agent Services*, selecionar o menu *Search for Certificates* para listar todos os certificados emitidos e depois pressionar *Revoke* para incluir um certificado na lista de revogação. Também é possível buscar um certificado específico. Em seguida, precisamos atualizar a CRL pressionando *Update Revocation List* e *Display Revocation List* para exibir na tela a versão modificada (**figura 5**).

Os usuários finais podem ir até *SSL End Users Services* para importar uma versão atualizada da CRL em um aplicativo. Para iniciar a importação, basta selecionar o botão de rádio *Import the latest CRL to your browser* no item de menu *Retrieval | Import Certificate Revocation List* (**figura 6**). Os usuários podem modificar suas propriedades do navegador para especificar o intervalo de atualização da CRL (**figura 6**, janela *CRL Import Status*), que evitaria a necessidade de baixar periodicamente a nova versão da lista. Para visualizar seu conteúdo no navegador, use as *Propriedades*. O comando usado na **listagem 3** lê o conteúdo diretamente no Dogtag.

Para uma versão mais legível da CRL, envie o conteúdo do atributo da CRL para a ferramenta *PrettyPrintCrl*.

As CRLs têm uma grande desvantagem: precisam ser gerenciadas manualmente. Por exemplo, alcançar um grande número de servidores distintos a partir dos quais é preciso requisitar uma CRL em intervalos regulares envolveria um trabalho considerável e desperdiçaria espaço em disco, porque as CRLs são armazenadas no disco local. Todo o processo é mais fácil se o cliente suportar o *Online Certificate Status Protocol* (OCSP).

O OCSP permite consultar em tempo real os certificados de diferentes autoridades certificadoras. A única condição é que a autoridade emissora use um serviço OCSP para responder às requisições dos clientes com relação à validade do certificado. Se a AC não tiver esse serviço, todos os certificados emitidos por ela terão uma extensão *Authority Information Access* com a URL do serviço de resposta.

Conclusões

O Dogtag finalmente traz uma infraestrutura de chaves públicas ao mundo do Código Aberto. Graças à interface web e ao console gráfico, os administradores não devem ter problemas para se nortear nas operações cotidianas e no seu gerenciamento. Com os vários modelos disponíveis em `/var/lib/pki-ca/webapps/`, é possível modificar o comportamento e o visual do aplicativo conforme desejado. ■

Mais informações

[1] CAcert.org: http://www.cacert.org/

[2] Kurt Seifried, "Corrente quebrada": http://lnm.com.br/article/2624

[3] Projeto Dogtag: http://pki.fedoraproject.org/

[4] Armazenamento do Dogtag: http://pki.fedoraproject.org/wiki/PKI_Data_Storage_Requirements

[5] Especificação do PKCS: http://en.wikipedia.org/wiki/PKCS

[6] Certutil: http://www.mozilla.org/projects/security/pki/nss/tools/certutil.html

Firewall de alto nível com o Portsmith

Firewall mais prático

Falta ao iptables uma função para abrir portas dinamicamente para usuários autenticados. O Portsmith resolve justamente isso.

por Christian Ney

Administradores de equipamentos Check Point e Cisco estão familiarizados com firewalls que abrem portas após um usuário fazer seu login. Infelizmente, essa técnica, às vezes chamada de *Client Authentication* (autenticação do cliente) ou *Cut-Through Proxy*, costuma estar sujeita a restrições. Em virtude dos problemas associados a firewalls que fazem autenticação, o iptables não inclui essa funcionalidade. Obviamente, é possível empregar suas próprias funções de autenticação com alguns scripts, mas poucos administradores se dão a esse trabalho.

O *Portsmith* [1] oferece uma opção livre e fácil para autenticação no firewall, e essa ferramenta inovadora permite até que usuários autenticados abram portas de seus próprios navegadores web. Para evitar ameaças potenciais de segurança, o administrador ainda mantém controle das permissões. Cada usuário recebe um conjunto de links de comunicação exigidos e só pode acessar os recursos atribuídos a esses links. Essa técnica impede que os usuários simplesmente abram buracos no firewall sempre que precisarem.

Uma aplicação potencial para um firewall com Portsmith é em substituição a uma VPN. O tráfego é impedido no firewall até que um usuário se autentique, e após o login, somente o tráfego vindo do IP desse usuário é admitido. Ao garantir que um serviço específico só esteja disponível para o usuário autenticado, o administrador consegue evitar a necessidade de um servidor VPN dedicado. Na outra ponta, o cliente também não precisa de softwares ou configurações especiais para iniciar a conexão. Segundo o site do Portsmith, "...é possível controlar o computador de trabalho a partir da sua casa, da casa de um amigo, de uma rede Wi-fi ou de qualquer outro local com acesso à Internet. Como não há exigências de software, após sair do local, não haverá vestígios de que você esteve lá, e nada é instalado no computador que estava em uso". Outra vantagem do Portsmith é uma solução de becape integrada baseada no navegador. Simplesmente dê um clique para gravar um conjunto de regras, arquivos críticos e banco de dados num CD.

O Portsmith prefere o Ubuntu 8.04 Server LTS [2]. Claro que é possível usar outras distribuições, embora seja necessário modificar os caminhos e o tratamento de componentes de acordo com as exigências do Portsmith. O Portsmith é projetado para funcionar com o servidor web Apache [3], com o módulo do PHP5 [4] e com o módulo para bancos de dados PostgreSQL [5]. Boa sorte se preferir outro sistema de banco de dados, pois nenhum outro é suportado.

O servidor web atua como interface com o administrador e os usuários. As contas são armazenadas no banco de dados. O conjunto dinâmico de regras também é guardado no banco de dados e obtido do banco sempre que necessário. Há scripts em execução em segundo plano para gerar regularmente os comandos iptables correspondentes a partir de trechos do banco de dados e em seguida adicioná-los ao conjunto de regras.

Para usar o Portsmith, primeiro instale o Ubuntu 8.04 Server. Recomenda-se usar uma partição separada para o diretório `/var/`, onde tanto os arquivos de log quanto o banco de dados residirão.

13 a 16 de outubro, 2009 • Transamerica Expo Center • São Paulo

4.800 Congressistas
Mais de 300 Palestrantes e Painelistas
7 Auditórios Simultâneos
14.300 Participantes de 42 Países
Presença de Dirigentes e Profissionais do Setor
25.000m^2 de Exposição

Futurecom, o mais qualificado Evento de Telecomunicações e Tecnologia da Informação da América Latina.

Um Empreendimento que reúne as Forças de Mercado e proporciona às Empresas, aos Profissionais e Dirigentes que dele participam um ambiente estimulante para novos Conhecimentos, Negócios e Relacionamento.

Provisuale

andre.veiga@provisuale.com.br
nalzira.muniz@provisuale.com.br
(41) 3314-3200

saiba mais www.futurecom.com.br

A documentação do Portsmith sugere a instalação do metapacote *ubuntu-desktop*, que oferece uma interface de usuário completa baseada no Gnome. Entretanto, não será realmente necessário um desktop Gnome. Por outro lado, a documentação nada informa a respeito de tarefas mais significativas, tais como melhorar a segurança do sistema operacional. Como o Portsmith tem conexão direta com a Internet, ele requer muito mais atenção à segurança do que um sistema comum.

O próximo passo é configurar as interfaces de rede e em seguida instalar os pacotes restantes. Os usuários favoráveis a um desktop gráfico podem usar as ferramentas gráficas para isso; todos os demais devem apenas usar o editor de texto para alterar o arquivo `/etc/network/interfaces`. O comando

```
aptitude install -y openssh-server
➥apache2 libapache2-mod-php5
➥libapache2-mod-auth-pgsql
➥postgresql-8.3 php5-pgsql
```

instala no sistema os pacotes necessários. Se for usada a solução de becape interna, será preciso instalar também os pacotes *mkisofs* e *cdrecord*.

A configuração do servidor web requer mais algumas etapas. Na configuração de DNS do firewall, defina os parâmetro `ServerName` e depois ative o módulo SSL com o comando `a2enmod ssl`.

Para evitar transmitir logins de usuários sem proteção, use conexões criptografadas por SSL.

Portsmith

O download do Portsmith ocupa 17 MB [6], e pode ser gravado num CD ou montado via dispositivo de *loop*:

```
mount -o loop /tmp/Portsmith_4.iso
➥/media/cdrom
```

O pacote do Portsmith inclui vários tarballs com scripts de shell e PHP, a estrutura da tabela do banco de dados e uma configuração de exemplo que ajuda a configurar a máquina com Portsmith como servidor DNS ou DHCP. Além disso, há um pequeno guia de instalação, além de dois binários para Windows (um para o Internet Explorer e outro para o Firefox) que suportam o uso de RDP através de firewalls do Portsmith. Para instalar o Portsmith, desempacote o tarball:

```
tar xvf /media/cdrom/server/ports.
➥tar -C /
```

Os shell scripts, que são copiados para `/usr/local/bin/`, contêm variáveis que refletem a estrutura da rede; o administrador do Portsmith precisará modificar os scripts de acordo. Eles se localizam nos arquivos `fw_policy` e `fw_lookup`. Entre outras tarefas, será preciso especificar a rede externa e o IP oficial do firewall. É mais fácil ter um IP estático; porém, usuários com IP dinâmico podem usar o *DynDNS* [7] ou scripts para publicar o endereço atual.

Segundo a documentação, o Portsmith deve ser iniciado diretamente pelo arquivo `/etc/rc.local`. Se seu firewall tiver um link de Internet direto, isso significa que o firewall e as redes escondidas atrás dele não seriam protegidas pelo filtro de pacotes durante um período curto após o início da máquina, pois o firewall seria o último item processado durante a inicialização. Ao ativar as interfaces de rede, pode ser preferível executar um script de inicialização ou chamar o Portsmith.

O banco de dados também precisa de algumas providências. Infelizmente, a documentação sugere que os usuários cortem e colem,

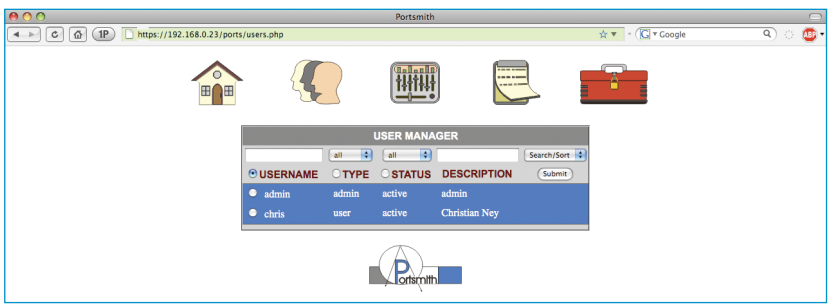


Figura 1 As contas dos usuários são facilmente modificadas acrescentando-se regras.

Figura 2 Alteração das regras: o exemplo encaminha a porta 80 do firewall para um servidor web interno.

um processo muito sujeito a erros; `psql < /media/cdrom/server/TABLES.txt` é uma forma mais fácil. Como o trabalho mais complexo em segundo plano é gerenciado por alguns shell scripts que precisam ser executados periodicamente, é necessário criar entradas para os scripts no Cron.

Reinicie o servidor com o comando `/etc/init.d/apache2 restart`. Assim, o Portsmith já deve ser iniciado.

Administração

Os administradores podem usar seu navegador para todas as atividades de gerenciamento do sistema: `http://firewall/ports/` leva o usuário à janela de login. O usuário padrão para administração é *admin*, com a mesma senha. Embora a documentação sugira que isso deva ser alterado, pode ser tarde demais se o firewall já estiver conectado à Internet – esses padrões são muito fáceis de adivinhar.

Após o login, usuários administrativos podem configurar o sistema, gerenciar usuários e ativar alguns recursos para si mesmos. As duas áreas principais do gerenciamento do sistema são a administração de usuários e o conjunto de regras. A lista de usuários é bastante simples e oferece aos administradores uma grande seleção de entradas e funções de busca (**figura 1**). A lista *drop-down* no canto superior direito permite ordenar, adicionar, modificar e apagar contas. Ao adicionar ou modificar, é preciso especificar um usuário e uma senha. O usuário então recebe um papel como usuário padrão ou administrador; administradores têm acesso completo ao sistema.

Em vez de apagar contas não mais necessárias, é possível simplesmente apagá-las. Porém, o Portsmith não possui uma função controlada pelo tempo para bloquear contas temporárias; novamente é necessária atenção manual por parte do administrador. Ele também pode definir uma regra padrão, revogar regras ou acrescentar novas regras. O gerenciamento de conjuntos de regras é semelhante ao de usuários (**figura 2**). Mais uma vez, o administrador do Portsmith pode procurar, modificar, adicionar e apagar regras.

Ao adicionar ou modificar, é possível especificar o protocolo a usar (TCP, UDP, ICMP), a ação a realizar (permitir ou encaminhar) e a porta de destino. Além disso, é possível referir-se a uma máquina por meio de seu IP ou (supondo que a resolução DNS esteja funcionando) seu nome. A interface de administração também oferece acesso a algumas ferramentas úteis: o *Log Manager* (gerenciador de log, **figura 3**) diz exatamente quais regras foram ativadas, por quais usuários e em qual IP. Uma útil função de busca ajuda a manter o controle de um número maior de entradas do log.

O botão de ferramentas leva o administrador a quatro outros assistentes que valem a pena. O *Login Analyzer* (analisador de login, **figura 4**) não apenas oferece ao administrador um panorama útli de quem fez login a que horas, como também relata o número e a hora das tentativas de login inválidas recentes.

Para evitar ataques de força bruta, o IP de origem do cliente é bloqueado após 3 logins, até o administrador reativá-lo. A função de bloqueio não depende de um filtro de pacotes; em vez disso, o atacante potencial recebe a mensagem *You are up to no good – you are now going to be blocked* (Você não tem boas intenções – agora será bloqueado), e os campos de nome de usuário e senha desaparecem para impedir tentativas de login com uma conta de usuário alternativa. Se ocorrer o pior, o administrador nem sequer conseguirá usar uma conta administrativa para desbloquear a conta. Nesse caso, a única alternativa é modificar o banco de dados manualmente.

Sob circunstâncias normais, também é possível liberar um computador bloqueado por excesso de tentativas de login por meio do Login Analyzer. Infelizmente, essa função está bem escondida: é preciso ativar a caixa à esquerda da entrada e em seguida clicar em *Enviar*.

O mostrador de status lista o conjunto de regras atual do firewall, embora seja apenas a saída do co-

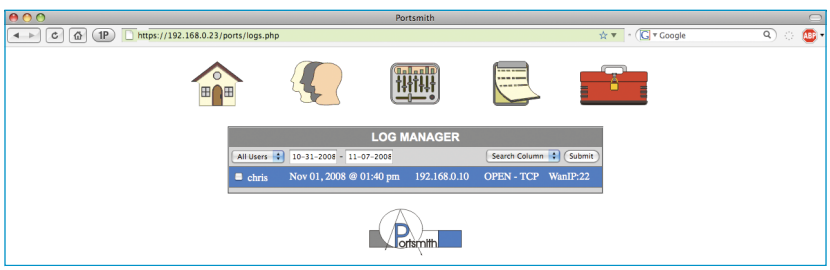


Figura 3 O *Log Manager* informa quem ativou qual regra.

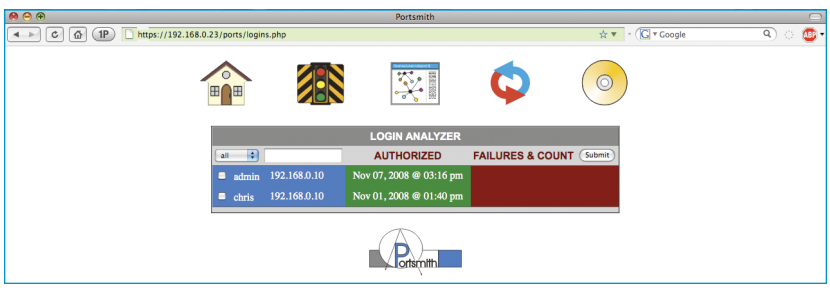


Figura 4 O *Login Analyzer*.

Figura 5 Alterar os serviços ativos não é tão fácil para usuários não técnicos.

mando `iptables -L -v`. Qualquer um que não tenha familiaridade com o iptables provavelmente ficará mais confuso após ler a lista; um relatório mais legível seria melhor para novos usuários.

O botão de reinício restaura o status original das regras que foram definidas pelos administradores e usuários. Essa etapa mantém todas as conexões já existentes.

Visão do usuário

O Portsmith é muito fácil do ponto de vista do usuário. Assim como o acesso pelo administrador, o acesso pelo usuário é feito via navegador, e os usuários precisam fornecer suas credenciais. Após fazer o login, os usuários recebem uma lista de regras de firewall disponíveis. O usuário pode selecionar uma regra e em seguida clicar nela para ativá-la.

Como se pode ver na **figura 5**, a lista de funções ativadas é bastante técnica. A maioria dos usuários finais dificilmente entenderá o significado das portas, e portanto precisarão de uma descrição por extenso. É preciso usar certa criatividade por parte do administrador, já que o banco de dados restringe o comprimento da descrição a 25 caracteres. Claro que é possível alterar o tamanho da coluna do banco de dados.

Diferentemente de uma VPN, o Portsmith não envia conexões diretamente para a máquina de destino; em vez disso, ele encaminha os pacotes recebidos, através do firewall, após o usuário se autenticar. Usuários finais talvez precisem tomar algumas ações. Por exemplo, se você quiser acessar remotamente uma impressora interna, será preciso configurar uma impressora no lado cliente para o usuário selecionar.

É uma boa ideia começar com uma definição clara das tarefas que se deseja realizar com o Portsmith

Quadro 1: Regras

A qualidade de um firewall é determinada pelas regras implementadas por seu filtro de pacotes. No caso do *Portsmith*, a política padrão é semelhante à **listagem 1**.

A rede interna, 192.168.2.0/24, que fica sob a interface `eth1`, consegue acessar a grande e assustadora Internet sem restrições à tradução de portas. Essa técnica pode ser adequada para uma rede comercial pequena ou até para redes domésticas, mas também as expõe a muitos perigos.

A página do Portsmith afirma que "... todas as portas externas ficam bloqueadas até ser liberadas após o login", mas na realidade a coisa é um pouco mais complicada. Não apenas as portas 80 e 443 ficam abertas para acesso a sites, como também a porta 25 fica aberta ao tráfego de emails. Por outro lado, todo o tráfego ICMP que alcança a interface externa é bloqueado, embora isso sacrifique informações importantes para a solução de problemas.

O Portsmith utiliza os estados *RELATED* e *ESTABLISHED* ("relacionado" e "estabelecido", respectivamente) para permitir automaticamente conexões TCP e DNS a partir da rede interna. O *Source NAT*, que é ativado para um IP genérico (192.168.1.250), impõe ainda mais questões (**listagem 2**).

Isso parece ser resquício de algum redirecionamento da porta LPD para um servidor de impressão interno. Apesar de a porta TCP 9100 estar bloqueada por padrão, isso pode causar problemas difíceis de encontrar numa configuração semelhante.

Felizmente, é possível modificar a política básica de acordo com as suas próprias necessidades. Simplesmente apague os padrões de `/usr/local/bin/fw_policy` ou edite-os para criar regras tão complexas quanto se queira.

Após fazer o login como usuário e ativar uma conexão SSH para o usuário em questão, a cadeia `INPUT` é ampliada como na **listagem 3**.

Como se pode ver, regras dinâmicas vêm primeiro. Isso evita conflitos potenciais com regras pré-existentes mais genéricas. O destino (0.0.0.0) da nova regra é um pouco perturbador, pois a própria política do Portsmith afirma que ele deveria ser restrito a um IP externo.

Listagem 1: Filtro do Portsmith

```
Chain INPUT (policy DROP 22 packets, 3590 bytes)
   pkts bytes target    prot opt in    out  source          destination
      7   476 ACCEPT    all  --  eth1  *    192.168.2.0/24  0.0.0.0/0
    200 17460 ACCEPT    all  --  lo    *    127.0.0.1       0.0.0.0/0
      0     0 ACCEPT    tcp  --  eth0  *    0.0.0.0/0       0.0.0.0/0  limit: avg 5/sec burst 5 tcp
➥dpt:80
      0     0 ACCEPT    tcp  --  eth0  *    0.0.0.0/0       0.0.0.0/0  limit: avg 5/sec burst 5 tcp
➥dpt:25
      0     0 ACCEPT    tcp  --  eth0  *    0.0.0.0/0       0.0.0.0/0  limit: avg 5/sec burst 5 tcp
➥dpt:443
      0     0 ACCEPT    tcp  --  *     *    0.0.0.0/0       0.0.0.0/0  state RELATED,ESTABLISHED
      1    62 ACCEPT    udp  --  *     *    0.0.0.0/0       0.0.0.0/0  limit: avg 15/sec burst 5 udp
➥spt:53 state RELATED,ESTABLISHED
      0     0 ACCEPT    icmp --  *     *    192.168.2.0/24  0.0.0.0/0  limit: avg 5/sec burst 5
Chain FORWARD (policy DROP 0 packets, 0 bytes)
   pkts bytes target   prot  opt in    out  source          destination
      0     0 ACCEPT    all  --  *     *    192.168.2.0/24  0.0.0.0/0
      0     0 ACCEPT    all  --  *     *    127.0.0.1       0.0.0.0/0
      0     0 ACCEPT    all  --  *     *    0.0.0.0/0       0.0.0.0/0  state RELATED,ESTABLISHED
Chain OUTPUT (policy ACCEPT 233 packets, 21730 bytes)
   pkts bytes target   prot  opt in    out  source          destination
```

(o exemplo anterior com a impressora seria fácil de implementar, mas é preciso questionar a segurança de transmitir a saída da impressora de forma descriptografada pela Internet).

Segurança

O aspecto mais crítico da segurança do Portsmith é que o servidor web é permanentemente acessível, mais particularmente por usar PHP. Se um agressor conseguir comprometer o processo de autenticação por meio de uma vulnerabilidade na lógica ou na própria linguagem PHP, toda a rede fica vulnerável.

O link do banco de dados é outro alvo potencial. Por exemplo, imagine um invasor iniciando um ataque de injeção SQL para "alterar" as regras, praticamente inutilizando a segurança que o firewall deveria proporcionar.

Embora uma pesquisa sobre o PHP do Portsmith não tenha revelado qualquer vulnerabilidade, não se pode eliminar completamente a possibilidade de um ataque. Desnecessário lembrar que é preciso atualizar com frequência. Para mais proteção, talvez seja interessante instalar também o *Suhosin* [8] ou o *ModSecurity* [9] para oferecer defesas contra *zero-day exploits*.

O sistema é baseado na permissão de conexão por um IP cliente autenticado. O IP de origem que chega na porta 443 do servidor web é consultado para se ter certeza do endereço. Esse comportamento é mais um risco potencial: no caso mais simples, o cliente talvez não esteja ciente de que se encontra atrás de um proxy que cria uma conexão com o firewall Portsmith para o navegador web. Isso causaria a ativação do endereço do proxy em vez daquele do cliente. Por sua vez, esse cenário significa que qualquer usuário no proxy receberia os mesmos privilégios que o usuário no cliente que, portanto, poderia acessar os recursos do usuário cliente.

Seria ainda pior uma situação em que um agressor utilizasse um servidor proxy comprometido. Considerando o comprimento do período de acesso permitido, isso novamente abriria um buraco para ataques.

Listagem 2: Source NAT

```
01 Chain PREROUTING (policy ACCEPT 1603 packets, 117K bytes)
02 pkts bytes target  prot opt in    out  source      destination
03    0    0  DNAT    tcp  --  eth0  *    0.0.0.0/0   0.0.0.0/0    tcp dpt:9100 to:192.168.1.250:9100
```

Listagem 3: Regras modificadas

```
01 Chain INPUT (policy DROP 122 packets, 14737 bytes)
02 pkts bytes target  prot opt in    out  source         destination
03   85  7589 ACCEPT  tcp  --  eth0  *    192.168.0.10   0.0.0.0/0  tcp dpt:22
04   14   961 ACCEPT  all  --  eth1  *    192.168.2.0/24 0.0.0.0/0
05 2497  640K ACCEPT  all  --  lo    *    127.0.0.1      0.0.0.0/0
06   23  3652 ACCEPT  tcp  --  eth0  *    0.0.0.0/0      0.0.0.0/0  limit: avg 5/sec burst 5 tcp dpt:80
07    0     0 ACCEPT  tcp  --  eth0  *    0.0.0.0/0      0.0.0.0/0  limit: avg 5/sec burst 5 tcp dpt:25
08  262 37622 ACCEPT  tcp  --  eth0  *    0.0.0.0/0      0.0.0.0/0  limit: avg 5/sec burst 5 tcp dpt:443
09  114 22241 ACCEPT  tcp  --  *     *    0.0.0.0/0      0.0.0.0/0  state RELATED,ESTABLISHED
10    3   204 ACCEPT  udp  --  *     *    0.0.0.0/0      0.0.0.0/0  limit: avg 15/sec burst 5 udp spt:53
➥state RELATED,ESTABLISHED
11    0     0 ACCEPT  icmp --  *     *    192.168.2.0/24 0.0.0.0/0  limit: avg 5/sec burst 5
```

Suplemento prático

O Portsmith é um suplemento prático para um firewall convencional. A solução acrescenta a permissão dinâmica e pré-definida às regras tradicionalmente estáticas, permitindo que os usuários realizem as alterações. Um uso potencial seria o reforço da segurança de um servidor de emails interno da empresa ou outros serviços, como o Sun Secure Global Desktop [10]. Com conexões criptografadas, o Portsmith poderia servir como substituto de uma VPN. Se for preferível uma solução VPN *de verdade*, é fácil integrar softwares para IPSec, como o *strongSwan* [11] ou o *OpenVPN* [12].

Simplesmente usar o Portsmith para fornecer acesso SSH pelo firewall a um grupo restrito de usuários é uma sub-utilização da solução. A técnica de *port knocking* [13], por exemplo, é uma alternativa mais simples e mais segura. Usuários com IP dinâmico precisam basear-se em técnicas manuais ou numa ferramenta externa como o serviço DynDNS para atualizar a configuração com um IP oficial ativo.

O conjunto de regras padrão impõe algumas questões, e certamente poderia melhorar em alguns pontos. Felizmente, é fácil realizar alterações, embora exijam edição manual dos arquivos de configuração do Portsmith. A edição manual pode causar complicações no momento da atualização do software.

Com relação à autenticação, o Portsmith felizmente baseia-se em sua própria técnica orientada a banco de dados. Seria preferível usar um sistema de tokens RSN ou outra forma de *single sign-on*. Elas significariam não apenas mais conveniência para o usuário, mas (principalmente no caso do RSA) uma camada extra de segurança.

Também seria útil introduzir controles baseados na hora para bloquear automaticamente contas temporárias, por exemplo, ou para restringir o login de alguns usuários ao horário comercial. É de se esperar que o sistema seja flexível o suficiente para suportar extensões dessa espécie.

Conclusão

Dito isso, e supondo uma configuração básica (mas que funcione), além de uma boa dose de reforços de segurança, o Portsmith é uma extensão útil a qualquer firewall baseado em iptables, e pode facilitar bastante a vida dos administradores, bem como a dos usuários. ■

Mais informações

[1] Portsmith: http://ddbolt.net/portsmith.php

[2] Download do Ubuntu Server: http://www.ubuntu.com/getubuntu/download

[3] Apache: http://httpd.apache.org

[4] PHP: http://www.php.net

[5] PostgreSQL: http://www.postgresql.org

[6] Download do Portsmith: http://www.ddbolt.net/downloads/Install_CD

[7] DynDNS: http://www.dyndns.org

[8] Suhosin: http://www.hardened-php.net/suhosin.127.html

[9] ModSecurity: http://www.modsecurity.org

[10] Sun Secure Global Desktop: http://www.sun.com/software/products/sgd/index.jsp

[11] strongSwan: http://www.strongswan.org

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

[13] Flávio do Carmo Júnior, "Quem bate?": http://lnm.com.br/article/772

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:

04/07/2009 – São Paulo/SP
18/07/2009 – Vitória/ES
01/08/2009 – Fortaleza/CE
03/10/2009 – São Paulo/SP

Inscrições e mais informações:

www.linuxmagazine.com.br/lpi
Tel (11) 4082-1300

Linux Professional Institute

LINUX MAGAZINE

LINUX NEW MEDIA
The Pulse of Open Source

Como usar o SQLReactor para persistência de objetos PHP num banco de dados

Objetos PHP no banco

A persistência de objetos PHP em bancos de dados não requer operações complicadas. Basta um mapeador competente como o SQLReactor.

por Rafael Marques Martins

Uma ferramenta de ORM (*Object-Relational Mapping*, ou Mapeamento Objeto-Relacional) consiste em uma interface que implementa todos os métodos de acesso ao banco de dados, busca e alteração de registros, traduzindo-os para o conceito de objetos.

Listagem 1: Estrutura do código com o SQLReactor

```
01 <?php
02 include "SQLReactor/SQLReactor.php";
03
04 $connection = new SQLReactorConnection( "postgres://
➥sqlreactor:sqlreactor@localhost/exemplo_reactor" );
05 SQLReactor::setDefaultConnection( $connection );
06
07 //Aqui vai o mapeamento
08 //Aqui vão as operações em banco
09
10 $connection->close();
11 ?>
```

Utilizamos, portanto o conceito de objetos persistentes. Esses objetos serão armazenados em um banco de dados relacional, porém o conceito de banco de dados só existe no momento do mapeamento das classes em tabelas. Na prática, não mais se utiliza código SQL para inserir, alterar, excluir ou buscar registros no banco. Utilizamos o os métodos que a ferramenta de ORM disponibiliza para executar essas operações.

Portanto, utilizar uma ferramenta de ORM consiste basicamente em mapear e criar as estruturas do banco de dados e utilizar os métodos de busca e manipulação dos objetos. A ferramenta é res-

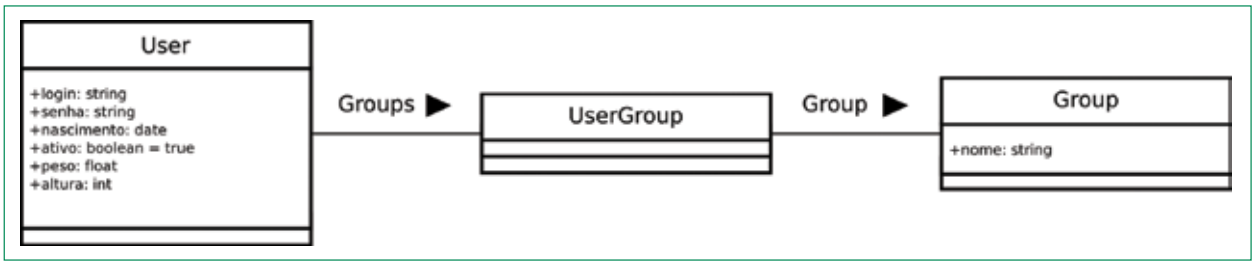


Figura 1 Diagrama de classes simples para exemplo.

ponsável por construir os comandos necessários para o sistema de banco de dados escolhido. Dessa forma, além de maior organização – pois o sistema fica completamente orientado a objetos –, obtém-se também maior liberdade quanto ao banco de dados a ser escolhido e uma maior facilidade para criar sistemas multibanco.

O SQLReactor

O SQLReactor é uma ferramenta de ORM de código aberto com suporte a MySQL, PostgreSQL, SQLite e Oracle. Funciona no PHP 5.0 ou superior e provê muitas opções de busca de dados e tradução automática de tipos de dados do PHP para o banco de dados e vice-versa.

Iniciando

Para iniciar o uso do SQLReactor, faça seu download em [1], descompacte os arquivos na estrutura do seu site e use a diretiva `include` para embutir o conteúdo do arquivo principal.

Depois disso, utilize a classe `SQLReactorConnection` para criar uma conexão com o banco de dados, defina-a como a conexão padrão, faça o mapeamento das classes e operações em banco e, no final, feche a conexão. A **listagem 1** mostra como fica a estrutura do código.

Nos exemplos deste artigo, todas as operações e mapeamentos são realizados em um único arquivo, para facilitar a leitura. Porém, a estrutura pode ser dividida pelo programador para uma maior organização do código.

Na **listagem 1**, utilizamos um banco de dados PostgreSQL. Para

Listagem 2: Exemplo de mapeamento

```
01 class User extends SQLReactor{
02   function __map(){
03     $this->login        = SQLReactor::StringCol( array( 'length' => 100, 'notNull' => true ) );
04     $this->password     = SQLReactor::StringCol( array( 'length' => 100, 'notNull' => true ) );
05     $this->birthday      = SQLReactor::DateCol();
06     $this->ativo      = SQLReactor::BoolCol( array( 'default' => true ) );
07     $this->weight        = SQLReactor::FloatCol();
08     $this->height        = SQLReactor::IntCol();
09
10     $this->unique( 'login' );
11
12     $this->groups       = SQLReactor::Backref( array( 'target' => array( 'UserGroup', 'user' ) ) );
13   }
14
15   function __setPassword( $value ){
16     return sha1( $value );
17   }
18 }
19
20 class Group extends SQLReactor{
21   function __map(){
22     $this->login        = SQLReactor::StringCol( array( 'length' => 100, 'notNull' => true ) );
23     $this->users         = SQLReactor::Backref( array( 'target' => array( 'UserGroup',
➥'group' ) ) );
24   }
25 }
26
27 class UserGroup extends SQLReactor{
28   function __map(){
29     $this->user          = SQLReactor::ForeignKey( array( 'target' => 'User' ) );
30     $this->group         = SQLReactor::ForeignKey( array( 'target' => 'Group' ) );
31
32     $this->primaryKey( 'userId', 'groupId' );
33   }
34 }
```

Listagem 3: Exemplo de criação das tabelas

```
01 <?php
02 include “open_connection.php”;
03 include “mapping.php”;
04
05 SQLReactor::createTable( ‘User’ );
06 SQLReactor::createTable( ‘Group’ );
07 SQLReactor::createTable( ‘UserGroup’ );
08
09 include “close_connection.php”;
10 ?>
```

Listagem 4: Inserindo dados de exemplo

```
01 $user = new User();
02 $user->setLogin( ‘user1’ );
03 $user->setPassword( ‘123456’ );
04 $user->setBirthday( mktime( 0, 0, 0, 3, 29, 1986 ) );
05 $user->save();
06 echo $user->id; //retorna o id do objeto inserido
07
08 $user = new User();
09 $user->login = ‘user2’;
10 $user->password = ‘123456’;
11 $user->birthday = mktime( 0, 0, 0, 3, 29, 1989 );
12 $user->save();
13
14 $group = new Group();
15 $group->name = ‘Group 1’;
16 $group->save();
17
18 $group = new Group();
29 $group->name = ‘Group 2’;
20 $group->save();
21
22 $ug = new UserGroup();
23 $ug->userId = 1;
24 $ug->groupId = 1;
25 $ug->save();
26
27 $ug = new UserGroup();
28 $ug->userId = 1;
29 $ug->groupId = 2;
30 $ug->save();
31
32 $ug = new UserGroup();
33 $ug->userId = 2;
34 $ug->groupId = 2;
35 $ug->save();
```

usar outro banco de dados, será necessário mudar a URI passada para a classe `SQLReactorConnection`. Os formatos de URIs para outros bancos de dados encontram-se na **tabela 1**.

Mapeando

Este artigo mostra como fazer o mapeamento do diagrama de classes da **figura 1**, pois, apesar de simples, esse processo envolve grande parte dos conceitos necessários para o uso da ferramenta.

Para fazer o mapeamento no SQLReactor, é preciso definir as classes desejadas estendendo a classe `SQLReactor`. Todos os atributos devem ser mapeados dentro do método mágico `__map`. A classe também permite *setters* e *getters* mágicos usando o nome do atributo com os prefixos `__set` e `__get`, respectivamente (`__setPassword`, por exemplo).

Todas as classes automaticamente recebem um atributo `id` do tipo inteiro, que será a chave primária da tabela. A chave primária pode ser sobrescrita usando o método `$this->primaryKey` (veja a **listagem 2**).

O mapeamento completo do diagrama da **figura 1** encontra-se na **listagem 2**. Os possíveis tipos de atributos (isto é, colunas) do mapeamento estão descritos na **tabela 2**.

Na **listagem 2**, foi criado o setter mágico `__setPassword` para fazer com que a senha seja “criptografada” automaticamente quando o atributo `senha` for alterado.

Tabelas e objetos

Após fazer o mapeamento, basta utilizar os métodos do SQLReactor para criar as tabelas e manipular os objetos persistentes. A **listagem 3** contém um exemplo de código para a criação das tabelas.

Depois de criar as tabelas, já podemos começar a manipular objetos persistentes. Para criar um novo objeto, basta criar uma nova

instância da classe desejada e chamar o método `save` para persistir às alterações no banco. Após chamar o método `save` em um novo objeto, o SQLReactor automaticamente atualiza seu atributo `id` para coincidir com o id salvo no banco. A **listagem 4** contém um trecho de código para inserir dados de exemplo nas tabelas. O resultado dessas operações no banco de dados pode ser visto na **listagem 5**.

A partir deste ponto, basta utilizar os métodos de busca e manipulação de objetos providos pelo SQLReactor.

Os métodos disponíveis para busca de objetos incluem busca por id, busca usando filtro e listagem. Por exemplo, para buscar o objeto da classe `User` que contém id 1:

```
$user = new User( 1 );
```

A **listagem 6** realiza uma busca pelo objeto `User` de login igual a `user1` e com o atributo `ativo` marcado como `true`. O método `get` deve ser usado para retornar um único registro (ou uma instância vazia da classe passada, caso nada seja encontrado). Se mais de um objeto for encontrado com os parâmetros passados, é lançada uma exceção.

Também é possível utilizar o método `getList` para obter uma lista de objetos. Em todos os tipos de filtros, é possível navegar para os objetos ligados via `ForeignKey` ou `Backref` para filtrar o retorno. A **listagem 7** ilustra um exemplo disso, filtrando o resultado por `ativo`, pela data de nascimento maior ou igual a 01/01/1986 e pelo grupo. Neste trecho de código só serão retornados usuários que pertençam ao grupo cujo id seja igual a 2.

Em todos esses casos, o sistema recupera apenas os objetos do tipo `User`; mesmo que o filtro use outros objetos relacionados, eles não são trazidos do banco. Caso um atribu-

Listagem 5: Resultado da listagem 4 no banco de dados

```
exemplo_reactor=# select * from "user";
id         | 1
login      | user1
password   | 7c4a8d09ca3762af61e59520943dc26494f8941b
birthday   | 1986-03-29
is_active  | t
weight     |
height     |
----+---------------
id         | 2
login      | user2
password   | 7c4a8d09ca3762af61e59520943dc26494f8941b
birthday   | 1989-03-29
is_active  | t
weight     |
height     |


exemplo_reactor=# select * from "group";
id   | 1
name | Group 1
---+----
id   | 2
name | Group 2


exemplo_reactor=# select * from "user_group";
user_id  | 1
group_id | 1
---+--
user_id  | 1
group_id | 2
---+--
user_id  | 2
group_id | 2
```

Tabela 1: Formatos de URIs para diferentes bancos de dados

Banco de dados	URI
PostgreSQL	`postgres://sqlreactor:sqlreactor@localhost/exemplo_reactor`
MySQL	`mysql://root:minhasenha@localhost/exemplo_reactor`
SQLite	`sqlite:///caminho/pro/arquivo.db`
Oracle	`oracle://sqlreactor:minhasenha@meuTNS`

Listagem 6: Busca de um objeto com filtros

```
01 $user = SQLReactor::get( 'User', array(
02   'filter' => array(
03     array( 'login', 'user1' ),
04     array( 'ativo', true ),
05   )
06 ) );
```

Listagem 7: Busca de uma lista de objetos

```
01 $list = SQLReactor::getList( 'User', array(
02     'filter' => array(
03         array( 'ativo', true ),
04         array( 'birthday', '>=', mktime( 0, 0, 0, 1, 1,
➥ 1986 ) ),
05         array( 'groups->group->id', 2 )
06     )
07 ) );
```

Listagem 8: Buscando objetos relacionados usando o eagerload

```
01 $list = SQLReactor::getList( 'User', array(
02     'filter' => array(
03         array( 'ativo', true ),
04         array( 'groups->group->id', 2 )
05     ),
06     'eagerload' => array( 'groups->group' )
07 ) );
```

Listagem 9: Exemplo completo de listagem

```
01 $list = SQLReactor::getList( 'User', array(
02   'filter' => array(
03     array( 'ativo', true ),
04     array( 'groups->group->id', 2 )
05   ),
06   'eagerload' => array( 'groups->group' ),
07   'limit' => 50,
08   'offset' => 0,
09   'orderBy' => 'birthday',
10   'direction' => 'asc'
11 ) );
```

Listagem 10: Obtendo o número de objetos no banco

```
01 $count = SQLReactor::count( 'User', array(
02     'filter' => array(
03         array( 'ativo', true ),
04         array( 'groups->group->id', 2 )
05     ) ) );
```

to do tipo `ForeignKey` ou `Backref` seja acessado, o sistema buscará os objetos relacionados automaticamente, porém fará uma nova consulta ao banco para isso.

Ao acessar `$user->groups` por exemplo, a ferramenta de ORM executará automaticamente uma consulta para buscar os objetos do tipo `UserGroup` que estão ligados ao usuário atual. Caso seja interesse do programador trazer os objetos `UserGroup` e `Group` (para exibir o nome dos grupos, por exemplo), usa-se uma técnica chamada *eager load*. Caso o parâmetro `eagerload` seja passado para uma busca, o SQLReactor automaticamente inclui os atributos ligados e traz os objetos no retorno. A **listagem 8** mostra como trazer as informações do grupo já na lista, utilizando apenas uma consulta ao banco de dados com o parâmetro `eagerload`.

Também é possível, nas listagens e contagens, passar o número máximo do registro a retornar e o índice do primeiro registro a ser retornado (conhecidos como `LIMIT` e `OFFSET` na maioria dos bancos de dados). As listagens também aceitam parâmetros de ordenação por um atributo e o método a ser usado na ordenação (ascendente ou descendente), definido no SQLReactor como `direction`.

A **listagem 9** mostra o uso desses parâmetros. Nela, utilizamos o mesmo filtro e `eagerload` definidos anteriormente, porém passando um número máximo de 50 objetos do tipo `User` (independentemente do número de grupos), iniciando no índice 0. Também solicita-se a ordenação dos objetos por data de nascimento em ordem crescente.

Também é possível utilizar um método de contagem de registros que não retorna os dados, apenas conta o número de objetos de um determinado tipo no banco, usando o mesmo método de filtragem dos métodos de busca. O código da **lis-**

Tabela 2: Tipos de atributos

Tipo	Descrição
`SQLReactor::IntCol`	Armazena números inteiros.
`SQLReactor::FloatCol`	Armazena números de ponto flutuante.
`SQLReactor::StringCol`	Armazena cadeias de caracteres. Se este campo receber o parâmtro `length`, o tipo de colunas do banco será `varchar(length)`; caso contrário será uma coluna de texto longo (normalmente Text ou CLOB, dependendo do banco de dados).
`SQLReactor::DateCol`	Armazena data.
`SQLReactor::DateTime`	Armazena data e hora.
`SQLReactor::TimeCol`	Armazena hora.
`SQLReactor::ForeignKey`	Define um relacionamento com outra classe. Recebe o parâmetro target no seguinte formato: `array( 'target' => 'NomeDaClasseAlvo' )` Este tipo cria automaticamente um atributo de mesmo nome, com o sufixo `Id` que contém o valor da chave estrangeira, enquanto o atributo original contém o objeto de `id` igual ao da chave estrangeira.
`SQLReactor::Backref`	Cria um atributo para navegar no sentido oposto ao da `ForeignKey`. Este relacionamento não vai para o banco de dados. É usado apenas para permitir a navegação entre os objetos. Recebe o parâmetro `target` no seguinte formato: `array( 'target' => array( 'ClasseQueContemAForeignKey', 'nomeDoAtributoForeignKey' ) )`

tagem 10 mostra como contar todos os usuários ativos que pertençam ao grupo de `id` igual a 2.

Cada execução do método `save` em um objeto já existente no banco de dados fará com que este objeto seja atualizado (caso algo nele tenha sido alterado). A **listagem 11** mostra como buscar um objeto por seu `id`, alterar o atributo ativo para `false` e persistir essa alteração no banco de dados.

Finalmente, objetos podem ser excluídos do banco de dados utilizando o método `delete` (**linha 6**).

Observações finais

Este artigo mostrou todos os passos para a utilização do SQLReactor em projetos ou sites orientados a objeto. Todas as operações foram descritas na forma de exemplo para facilitar a leitura, porém podem ser divididas em muitos arquivos, classes ou funções para maior organização.

As colunas to tipo `DateCol`, `DateTimeCol` e `TimeCol` aceitam entradas de data no formato de *unix timestamp* (padrão PHP) e cadeias de caracteres nos formatos `%y-%m-%d`, `%y-%m-%d %H:%M:%S` e `%H:%M:%S`, mas sempre retornam timestamps.

A utilização de uma ferramenta de ORM facilita muito o trabalho do programador – principalmente em sistemas orientados a objeto – e melhora significativamente a qualidade do código. Porém, o processo é mais pesado do que simplesmente obter os dados diretamente no banco (funções `mysql_fetch_array`, `pg_fetch_array` etc.).

Para maiores informações, pode-se consultar a página do projeto em [1] ou contactar o desenvolvedor da ferramenta (que é brasileiro) usando o endereço de email que consta nos cabeçalhos dos arquivos fonte. ■

Listagem 11: Persistindo alterações nos objetos

```
01 //Alterando objetos:
02 $user = new User( 1 );
03 $user->ativo = false;
04 $user->save();
05 //Apagando
06 $user->delete();
```

Mais informações

[1] Página do projeto SQLReactor: http://sourceforge.net/projects/sqlreactor

Sobre o autor

Rafael Marques Martins é analista programador graduado em Tecnologia de Sistemas de Informação pela Universidade Federal Fluminense.

Linux.local

O maior diretório de empresas que oferecem produtos, soluções e serviços em Linux e Software Livre, organizado por Estado. Sentiu falta do nome de sua empresa aqui? Entre em contato com a gente: **11 4082-1300** ou **anuncios@linuxmagazine.com.br**

Fornecedor de Hardware = 1
Redes e Telefonia / PBX = 2
Integrador de Soluções = 3
Literatura / Editora = 4
Fornecedor de Software = 5
Consultoria / Treinamento = 6

Empresa	Cidade	Endereço	Telefone	Web	1	2	3	4	5	6
Bahia										
IMTECH	Salvador	Av. Antonio Carlos Magalhaes, 846 – Edifício MaxCenter – Sala 337 – CEP 41825-000	71 4062-8688	www.imtech.com.br		✔	✔		✔	✔
Ceará										
F13 Tecnologia	Fortaleza	Rua Padre Valdevino, 526 – Centro	85 3252-3836	www.f13.com.br		✔	✔		✔	✔
Espírito Santo										
Linux Shopp	Vila Velha	Rua São Simão (Correspondência), 18 – CEP: 29113-120	27 3082-0932	www.linuxshopp.com.br	✔	✔		✔	✔	
Megawork Consultoria e Sistemas	Vitória	Rua Chapot Presvot, 389 – Praia do Canto – CEP: 29055-410 sl 201, 202	27 3315-2370	www.megawork.com.br			✔		✔	✔
Spirit Linux	Vitória	Rua Marins Alvarino, 150 – CEP: 29047-660	27 3227-5543	www.spiritlinux.com.br			✔		✔	✔
Minas Gerais										
Instituto Online	Belo Horizonte	Av. Bias Fortes, 932, Sala 204 – CEP: 30170-011	31 3224-7920	www.institutoonline.com.br				✔		✔
Linux Place	Belo Horizonte	Rua do Ouro, 136, Sala 301 – Serra – CEP: 30220-000	31 3284-0575	corporate.linuxplace.com.br		✔	✔		✔	✔
Microhard	Belo Horizonte	Rua República da Argentina, 520 – Sion – CEP: 30315-490	31 3281-5522	www.microhard.com.br	✔	✔	✔		✔	✔
TurboSite	Belo Horizonte	Rua Paraíba, 966, Sala 303 – Savassi – CEP: 30130-141	0800 702-9004	www.turbosite.com.br	✔				✔	✔
Paraná										
iSolve	Curitiba	Av. Cândido de Abreu, 526, Cj. 1206B – CEP: 80530-000	41 252-2977	www.isolve.com.br		✔	✔			✔
Mandriva Conectiva	Curitiba	Rua Tocantins, 89 – Cristo Rei – CEP: 80050-430	41 3360-2600	www.mandriva.com.br			✔	✔	✔	✔
Telway Tecnologia	Curitiba	Rua Francisco Rocha 1830/71	41 3203-0375	www.telway.com.br					✔	✔
Pernambuco										
Fuctura Tecnologia	Recife	Rua Nicarágua, 159 – Espinheiro – CEP: 52020-190	81 3223-8348	www.fuctura.com.br			✔			✔
Rio de Janeiro										
Múltipla Tecnologia da Informação	Rio de Janeiro	Av. Rio Branco, 37, 14° andar – CEP: 20090-003	21 2203-2622	www.multipla-ti.com.br	✔		✔		✔	✔
NSI Training	Rio de Janeiro	Rua Araújo Porto Alegre, 71, 4º andar Centro – CEP: 20030-012	21 2220-7055	www.nsi.com.br				✔		✔
Open IT	Rio de Janeiro	Rua do Mercado, 34, Sl, 402 – Centro – CEP: 20010-120	21 2508-9103	www.openit.com.br				✔		✔
Unipi Tecnologias	Campos dos Goytacazes	Av. Alberto Torres, 303, 1ºandar – Centro – CEP: 28035-581	22 2725-1041	www.unipi.com.br			✔	✔	✔	✔
Rio Grande do Sul										
4up Soluções Corporativas	Novo Hamburgo	Pso. Calçadão Osvaldo Cruz, 54 sl. 301 CEP: 93510-015	51 3581-4383	www.4up.com.br		✔	✔		✔	✔
Definitiva Informática	Novo Hamburgo	Rua General Osório, 402 - Hamburgo Velho	51 3594 3140	www.definitiva.com.br	✔		✔		✔	✔
Solis	Lajeado	Av. 7 de Setembro, 184, sala 401 – Bairro Moinhos CEP: 95900-000	51 3714-6653	www.solis.coop.br		✔	✔	✔	✔	✔
DualCon	Novo Hamburgo	Rua Joaquim Pedro Soares, 1099, Sl. 305 – Centro	51 3593-5437	www.dualcon.com.br	✔		✔		✔	✔
Datarecover	Porto Alegre	Av. Carlos Gomes, 403, Sala 908, Centro Comercial Atrium Center – Bela Vista – CEP: 90480-003	51 3018-1200	www.datarecover.com.br	✔		✔			
LM2 Consulting	Porto Alegre	Rua Germano Petersen Junior, 101-Sl 202 – Higienópolis – CEP: 90540-140	51 3018-1007	www.lm2.com.br			✔		✔	✔
Lnx-IT Informação e Tecnologia	Porto Alegre	Av. Venâncio Aires, 1137 – Rio Branco – CEP: 90.040.193	51 3331-1446	www.lnx-it.inf.br	✔		✔		✔	✔
Plugin	Porto Alegre	Av. Júlio de Castilhos, 132, 11º andar Centro – CEP: 90030-130	51 4003-1001	www.plugin.com.br	✔		✔		✔	
TeHospedo	Porto Alegre	Rua dos Andradas, 1234/610 – Centro – CEP: 90020-008	51 3286-3799	www.tehospedo.com.br	✔	✔				
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. Andrades Neves, 1579 – Castelo – CEP: 13070-001	19 3213-2100	www.insignesoftware.com			✔		✔	✔
Microcamp	Campinas	Av. Thomaz Alves, 20 – Centro – CEP: 13010-160	19 3236-1915	www.microcamp.com.br				✔		✔
PC2 Consultoria em Software Livre	Carapicuiba	Rua Edeia, 500 - CEP: 06350-080	11 3213-6388	www.pc2consultoria.com	✔					✔
Savant Tecnologia	Diadema	Av. Senador Vitorino Freire, 465 – CEP: 09910-550	11 5034-4199	www.savant.com.br	✔	✔	✔			✔
Epopéia Informática	Marília	Rua Goiás, 392 – Bairro Cascata – CEP: 17509-140	14 3413-1137	www.epopeia.com.br						✔
Redentor	Osasco	Rua Costante Piovan, 150 – Jd. Três Montanhas – CEP: 06263-270	11 2106-9392	www.redentor.ind.br	✔					
Go-Global	Santana de Parnaíba	Av. Yojiro Takaoca, 4384, Ed. Shopping Service, Cj. 1013 – CEP: 06541-038	11 2173-4211	www.go-global.com.br			✔		✔	✔

Empresa	Cidade	Endereço	Telefone	Web	1	2	3	4	5	6
São Paulo (continuação)										
AW2NET	Santo André	Rua Edson Soares, 59 – CEP: 09760-350	11 4990-0065	www.aw2net.com.br			✔		✔	✔
Async Open Source	São Carlos	Rua Orlando Damiano, 2212 – CEP 13560-450	16 3376-0125	www.async.com.br	✔				✔	✔
Delix Internet	São José do Rio Preto	Rua Voluntário de São Paulo, 3066 9º – Centro – CEP: 15015-909	11 4062-9889	www.delixhosting.com.br	✔		✔		✔	
4Linux	São Paulo	Rua Teixeira da Silva, 660, 6º andar – CEP: 04002-031	11 2125-4747	www.4linux.com.br					✔	✔
A Casa do Linux	São Paulo	Al. Jaú, 490 – Jd. Paulista – CEP: 01420-000	11 3549-5151	www.acasadolinux.com.br			✔		✔	✔
Accenture do Brasil Ltda.	São Paulo	Rua Alexandre Dumas, 2051 – Chácara Santo Antônio – CEP: 04717-004	11 5188-3000	www.accenture.com.br			✔		✔	✔
ACR Informática	São Paulo	Rua Lincoln de Albuquerque, 65 – Perdizes – CEP: 05004-010	11 3873-1515	www.acrinformatica.com.br	✔					✔
Agit Informática	São Paulo	Rua Major Quedinho, 111, 5º andar, Cj. 508 – Centro – CEP: 01050-030	11 3255-4945	www.agit.com.br	✔	✔				✔
Altbit - Informática Comércio e Serviços LTDA.	São Paulo	Av. Francisco Matarazzo, 229, Cj. 57 – Água Branca – CEP 05001-000	11 3879-9390	www.altbit.com.br	✔		✔		✔	✔
AS2M -WPC Consultoria	São Paulo	Rua Três Rios, 131, Cj. 61A – Bom Retiro – CEP: 01123-001	11 3228-3709	www.wpc.com.br			✔		✔	✔
Big Host	São Paulo	Rua Dr. Miguel Couto, 58 – Centro – CEP: 01008-010	11 3033-4000	www.bighost.com.br	✔				✔	✔
Blanes	São Paulo	Rua André Ampére, 153 – 9º andar – Conj. 91 CEP: 04562-907 (próx. Av. L. C. Berrini)	11 5506-9677	www.blanes.com.br	✔	✔	✔		✔	✔
Commlogik do Brasil Ltda.	São Paulo	Av. das Nações Unidas, 13.797, Bloco II, 6º andar – Morumbi – CEP: 04794-000	11 5503-1011	www.commlogik.com.br	✔	✔	✔		✔	✔
Computer Consulting Projeto e Consultoria Ltda.	São Paulo	Rua 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 Carnaubeiras, 98 – Metrô Conceição – CEP: 04343-080	11 5017-0040	www.dominiotecnologia.com.br	✔					✔
EDS do Brasil	São Paulo	Av. Pres. Juscelino Kubistcheck, 1830 Torre 4 - 5º andar	11 3707-4100	www.eds.com		✔	✔			✔
Ética Tecnologia	São Paulo	Rua Nova York, 945 – Brooklin – CEP:04560-002	11 5093-3025	www.etica.net	✔		✔		✔	✔
Getronics ICT Solutions and Services	São Paulo	Rua Verbo Divino, 1207 – CEP: 04719-002	11 5187-2700	www.getronics.com/br			✔		✔	✔
Hewlett-Packard Brasil Ltda.	São Paulo	Av. das Nações Unidas, 12.901, 25º andar – CEP: 04578-000	11 5502-5000	www.hp.com.br	✔		✔	✔	✔	✔
IBM Brasil Ltda.	São Paulo	Rua Tutóia, 1157 – CEP: 04007-900	0800-7074 837	www.br.ibm.com	✔		✔		✔	✔
iFractal	São Paulo	Rua Fiação da Saúde, 145, Conj. 66 – Saúde – CEP: 04144-020	11 5078-6618	www.ifractal.com.br			✔		✔	✔
Integral	São Paulo	Rua Dr. Gentil Leite Martins, 295, 2º andar Jd. Prudência – CEP: 04648-001	11 5545-2600	www.integral.com.br	✔				✔	
Itautec S.A.	São Paulo	Av. Paulista, 2028 – CEP: 01310-200	11 3543-5543	www.itautec.com.br	✔	✔	✔		✔	✔
Kenos Consultoria	São Paulo	Av: Fagundes Filho, 134, Conj 53 – CEP: 04304-000	11 40821305	www.kenos.com.br					✔	✔
Konsultex Informatica	São Paulo	Av. Dr. Guilherme Dumont Villares, 1410 6 andar, CEP: 05640-003	11 3773-9009	www.konsultex.com.br			✔		✔	✔
Linux Komputer Informática	São Paulo	Av. Dr. Lino de Moraes Leme, 185 – CEP: 04360-001	11 5034-4191	www.komputer.com.br	✔		✔		✔	✔
Linux Mall	São Paulo	Rua Machado Bittencourt, 190, Cj. 2087 – CEP: 04044-001	11 5087-9441	www.linuxmall.com.br	✔			✔	✔	
Livraria Tempo Real	São Paulo	Al. Santos, 1202 – Cerqueira César – CEP: 01418-100	11 3266-2988	www.temporeal.com.br				✔	✔	✔
Locasite Internet Service	São Paulo	Av. Brigadeiro Luiz Antonio, 2482, 3º andar – Centro – CEP: 01402-000	11 2121-4555	www.locasite.com.br	✔				✔	✔
Microsiga	São Paulo	Av. Braz Leme, 1631 – CEP: 02511-000	11 3981-7200	www.microsiga.com.br			✔		✔	✔
Novatec Editora Ltda.	São Paulo	Rua Luis Antonio dos Santos, 110 – Santana – CEP: 02460-000	11 6979-0071	www.novateceditora.com.br				✔		
Novell América Latina	São Paulo	Rua Funchal, 418 – Vila Olímpia	11 3345-3900	www.novell.com/brasil			✔		✔	✔
Oracle do Brasil Sistemas Ltda.	São Paulo	Av. Alfredo Egídio de Souza Aranha, 100 – Bloco B – 5º andar – CEP: 04726-170	11 5189-3000	www.oracle.com.br					✔	✔
Proelbra Tecnologia Eletrônica Ltda.	São Paulo	Av. Rouxinol, 1.041, Cj. 204, 2º andar Moema – CEP: 04516-001	11 5052- 8044	www.proelbra.com.br	✔		✔			✔
Provider	São Paulo	Av. Cardoso de Melo, 1450, 6º andar – Vila Olímpia – CEP: 04548-005	11 2165-6500	www.e-provider.com.br			✔		✔	✔
Red Hat Brasil	São Paulo	Av. Brigadeiro Faria Lima, 3900, Cj 81 8º andar Itaim Bibi – CEP: 04538-132	11 3529-6000	www.redhat.com.br			✔		✔	✔
Samurai Projetos Especiais	São Paulo	Rua Barão do Triunfo, 550, 6º andar – CEP: 04602-002	11 5097-3014	www.samurai.com.br			✔		✔	✔
SAP Brasil	São Paulo	Av. das Nações Unidas, 11.541, 16º andar – CEP: 04578-000	11 5503-2400	www.sap.com.br			✔		✔	✔
Simples Consultoria	São Paulo	Rua Mourato Coelho, 299, Cj. 02 Pinheiros – CEP: 05417-010	11 3898-2121	www.simplesconsultoria.com.br			✔		✔	✔
Smart Solutions	São Paulo	Av. Jabaquara, 2940 cj 56 e 57	11 5052-5958	www.smart-tec.com.br		✔	✔		✔	✔
Snap IT	São Paulo	Rua João Gomes Junior, 131 – Jd. Bonfiglioli – CEP: 05299-000	11 3731-8008	www.snapit.com.br			✔		✔	✔
Stefanini IT Solutions	São Paulo	Av. Brig. Faria Lima, 1355, 19º – Pinheiros – CEP: 01452-919	11 3039-2000	www.stefanini.com.br			✔		✔	✔
Sun Microsystems	São Paulo	Rua Alexandre Dumas, 2016 – CEP: 04717-004	11 5187-2100	www.sun.com.br	✔		✔		✔	✔
Sybase Brasil	São Paulo	Av. Juscelino Kubitschek, 510, 9º andar Itaim Bibi – CEP: 04543-000	11 3046-7388	www.sybase.com.br					✔	✔
The Source	São Paulo	Rua Marquês de Abrantes, 203 – Chácara Tatuapé – CEP: 03060-020	11 6698-5090	www.thesource.com.br			✔		✔	✔
Unisys Brasil Ltda.	São Paulo	R. Alexandre Dumas 1658 – 6º, 7º e 8º andares – Chácara Santo Antônio – CEP: 04717-004	11 3305-7000	www.unisys.com.br	✔		✔		✔	✔
Utah	São Paulo	Av. Paulista, 925, 13º andar – Cerqueira César – CEP: 01311-916	11 3145-5888	www.utah.com.br			✔		✔	✔
Visuelles	São Paulo	Rua Eng. Domicio Diele Pacheco e Silva, 585 – Interlagos – CEP: 04455-310	11 5614-1010	www.visuelles.com.br			✔		✔	✔
Webnow	São Paulo	Av. Nações Unidas, 12.995, 10º andar, Ed. Plaza Centenário – Chácara Itaim – CEP: 04578-000	11 5503-6510	www.webnow.com.br	✔		✔		✔	
WRL Informática Ltda.	São Paulo	Rua Santa Ifigênia, 211/213, Box 02– Centro – CEP: 01207-001	11 3362-1334	www.wrl.com.br	✔		✔		✔	
Systech	Taquaritinga	Rua São José, 1126 – Centro – Caixa Postal 71 – CEP: 15.900-000	16 3252-7308	www.systech-ltd.com.br	✔	✔			✔	
2MI Tecnologia e Informação	Embu	Rua José Bonifácio, 55 – Jd. Independência – CEP: 06826-080	11 4203-3937	www.2mi.com.br		✔	✔		✔	✔

Calendário de eventos

Evento	Data	Local	Informações
III ENSOL	19 a 21 de junho	João Pessoa, PB	www.ensol.com.br
Java Mobile	20 de junho	Goiânia, GO	www.m3ddla.com.br/
FISL 10	24 a 27 de junho	Porto Alegre, RS	www.fisl.softwarelivre.org
Google Developer Day	29 de junho	São Paulo, SP	tinyurl.com/rcagfm
Intensivo LPI+ provas	18 de julho	Vitória, ES	lpi@infomania.com.br
Intensivo LPI+ provas	1º de agosto	Fortaleza, CE	erlon@f13.com.br
Futurecom 2009	13 a 16 de outubro	São Paulo, SP	www.futurecom2009.com.br
Latinoware	22 a 24 de outubro	Foz de Iguaçu, PR	www.latinoware.org
PGCON Brasil 2009	24 e 25 de outubro	Campinas, SP	www.postgresql.org.br/eventos/pgconbr

Índice de anunciantes

Nerdson – Os quadrinhos mensais da Linux Magazine

fisl10

10° 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

Informações e inscrições pelo site:

www.fisl.org.br

Inscreva-se!

Patrocínio Ouro:

MARISTA · SERPRO Serviço Federal de Processamento de Dados · CAIXA BRASIL UM PAÍS DE TODOS GOVERNO FEDERAL · globo.com · egi.br Comitê Gestor da Internet no Brasil · nic.br Núcleo de Informação e Coordenação do Ponto BR · PREVIDÊNCIA SOCIAL DATAPREV · UOL HOST QUALIDADE EM SERVIÇOS WEB · pagseguro UOL

CELEPAR INFORMÁTICA do PARANÁ · BANCO DO BRASIL · redhat · Sun microsystems · Ministério do Planejamento Orçamento e Gestão · Ministério da Ciência e Tecnologia · BRASIL UM PAÍS DE TODOS GOVERNO FEDERAL

Promoção: software livre Brasil

Organização: Associação Software Livre.Org · PROJETO SOFTWARE LIVRE - RS · PSL-RN

Realização: Associação Software Livre.Org

Transmissão: TV software LIVRE

PREVIEW

Na Linux Magazine #56

DESTAQUE

Gerenciamento simplificado

Você conhece todos os equipamentos presentes na sua rede? Os departamentos de TI gerenciam infindáveis trechos de informação, contratos, tíquetes de suporte e detalhes de suporte dos fornecedores. No ritmo frenético da rede padrão, essas informações geralmente são mantidas de forma ineficiente e, muitas vezes, até perdidas.

Gerenciar as informações das máquinas e dos equipamentos de rede é uma tarefa fundamental do departamento de TI, mas frequentemente os administradores descuidam desse ponto.

A **Linux Magazine 56** vai abordar o gerenciamento facilitado de TI. Vamos apresentar o poderoso GLPI, que cuida do inventário de equipamentos, tíquetes de suporte e muito mais. Além disso, vamos mostrar scripts amigáveis para manter sincronizadas as bases de usuários do *Active Directory* e das estações Linux, e apresentaremos o excelente NagVis para visualizar sua rede com base no onipresente Nagios. O objetivo é sempre facilitar o trabalho do departamento de TI. ■

REDE

Controle de banda

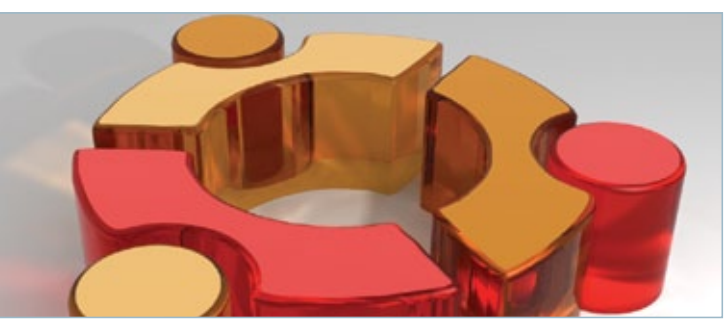
A maioria dos computadores são configurados para usar toda a banda de que precisam, até o limite do hardware. Porém, as técnicas padrão para compartilhamento de banda entre múltiplos sistemas numa rede local costumam ser inadequadas quando o volume de tráfego cresce. Muitos administradores descobrem que é possível obter melhor desempenho de rede por meio da imposição de limites de banda individual, em vez de usar as funcionalidades de *Quality of Service* (QoS, como é mais conhecido) do kernel Linux, que sofrem problemas de usabilidade.

A **Linux Magazine 56** vai apresentar o *WebHTB*, uma interface web para gerenciar e monitorar as *HTB-tools*, desenvolvida em PHP com amplo uso de AJAX. Com esse conjunto de softwares, é possível até gerenciar o uso de banda em redes atrás de SNAT. ■

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

BULL
Architect of an Open World™