LINUX NEW MEDIA
The Pulse of Open Source

FISL p.24
Mais uma edição, mais novidades

ENTREVISTA: CAIXA p.22
Um dos maiores cases de Linux corporativo no mundo

EDGAR SILVA p.28
A era dos Jetsons já começou

#43 Junho 2008
LINUX MAGAZINE

LINUX MAGAZINE

A REVISTA DO PROFISSIONAL DE TI

#43 06/08
R$ 13,90
€ 7,50
9 771806 942009 00043

ALTA DISPONIBILIDADE

A REDE NÃO PODE PARAR, OS SEUS SERVIDORES DEVEM ESTAR SEMPRE DE PÉ. O CÓDIGO ABERTO OFERECE VÁRIAS FERRAMENTAS PARA QUE VOCÊ ESTEJA SEMPRE PREVENIDO. p.30

» Storage sempre alerta: Com AoE, tudo fica mais rápido p.32

» Xen altamente disponível: Servidores virtuais migram para cobrir a falha dos outros p.37

» Gestão da disponibilidade: Por que monitorar é fundamental? p.43

SEGURANÇA: NEM ADIANTA INSISTIR p.65

O DenyHosts bloqueia agressores antes que eles consigam sequer desferir o ataque

REDES: ACESSO ADMINISTRATIVO COM IPMI p.62

Gerenciamento completo pela rede, sem porta serial, mesmo que a máquina esteja desligada

VEJA TAMBÉM NESTA EDIÇÃO:

» LPI nível 2: na décima primeira aula, implemente um servidor Web completo p.49

» Kwiki, o wiki repleto de recursos corporativos p.56

» Google Android, a plataforma do futuro para celulares p.73

» Firewall fácil e organizado com o Shorewall p.68

» ADempiere ERP e CRM, em português, a partir do Eclipse p.46

Concurso do

TRT

Edital em breve

Técnico Judiciário

Remuneração:

R$ 3.383,40

Nível Médio

PRF

Policial Rodoviário

Remuneração:

R$ 6.100,00

CONFIRMADO:
Nível Médio e
3.000 vagas

Conquiste seu emprego estável na Carreira Pública com a Central de Concursos.

- ☒ Sem experiência anterior
- ☒ Sem limite de idade
- ☒ Ambos os sexos

Prepare-se com a equipe que mais aprova no Brasil.

Seja FISCAL DA RECEITA FEDERAL

Concurso em breve • 1.800 vagas

Nível Superior em qualquer área **R$ 10.200,00 inicial**

Exame OAB - São Paulo

Direito: Penal, Civil, Trabalho e Tributário
Teoria + Exercícios práticos com correção de peças (CESPE/UnB)

Exame 135º - 2ª Fase

Coordenador Pedagógico:
Desembargador Antônio Carlos Malheiros

Delegado da Polícia Civil

Curso Avançado de Teoria
2ª Fase + Questões
Comentários da Banca e de provas anteriores

Aprovamos 202 candidatos para 2ª fase do concurso Delegado-SP/06

Coordenador e Professor:
Dr. Caetano Paulo Filho, Delegado de Polícia

TURMAS COM INÍCIO IMEDIATO: manhã, tarde, noite ou finais de semana
Apostilas auto-explicativas à venda com envio rápido para todo o Brasil.

Palestras informativas GRÁTIS, com profissionais da carreira pública
Informe-se sobre datas e horários

HÁ NECESSIDADE DE RESERVA. GARANTA A SUA VAGA!

www.centraldeconcursos.com.br

CENTRAL DE CONCURSOS

CENTRO: Rua Barão de Itapetininga, 163 - 6º andar (Metrô República) - Tel: 3017-8800
SANTO ANDRÉ: Av. José Caballero, 257 (Em frente ao Paço Municipal) - Tel: 4437-8800
SANTO AMARO: Av. Santo Amaro, 5.860 (Em frente ao Borba Gato) - Tel: 5189-8800
ALPHAVILLE: Calçada das Rosas, 74 - Centro Comercial - Tel: 4197-5000

Expediente editorial

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

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

Editor
Pablo Hess
phess@linuxmagazine.com.br

Redator
Rodrigo Amorim
ramorim@linuxmagazine.com.br

Revisão
Aileen Otomi Nakamura
anakamura@linuxmagazine.com.br

Editor de Arte
Lucas Oliveira
oliveira@linuxmagazine.com.br

Assistente de Arte
Igor Daurício
silva@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: mhilzinger@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)
anzeigen@linuxnewmedia.de

Hubert Wiest (Outros países)
hwiest@linuxnewmedia.de

Assinaturas:
www.linuxnewmedia.com.br
assinaturas@linuxmagazine.com.br

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

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

Linux Magazine é publicada mensalmente por:

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

Distribuição: Distmag
Impressão e Acabamento: Parma

Atendimento Assinantes
São Paulo: +55 (0)11 3512 9460
Rio de Janeiro: +55 (0)21 3512 0888
Belo Horizonte: +55 (0)31 3516 1280

ISSN 1806-9428 **Impresso no Brasil**

INSTITUTO VERIFICADOR DE CIRCULAÇÃO

Para quem pode

Prezados leitores da Linux Magazine,

A edição deste mês é um prazer para qualquer entusiasta do Software Livre e de Código Aberto (SL/CA), em especial, o Linux. Comparativamente, nenhum outro sistema operacional é tão flexível, sendo usado em praticamente qualquer cenário, desde grandes clusters para computação de alto desempenho até sistemas embarcados em dispositivos móveis.

Nos equipamentos mais modestos – telefones celulares e companhia –, as múltiplas iniciativas de uso do Linux já lhe rendem o posto de sistema que mais cresce na atualidade. LiMo Foundation e Google já começam a disputar espaço no mercado, ambas usando um kernel Linux com poucas modificações em comparação com o que vinha ocorrendo até o momento. Novamente, a liberdade de se ter múltiplas "distribuições" – como acabam sendo as duas opções – de sistema operacional mostra seus benefícios, oferecendo ao consumidor uma ampla gama de possibilidades para todos os gostos e necessidades.

Já no terreno dos clusters – seja para computação de alto desmpenho ou em alta disponibilidade –, o sistema aberto é soberano há tempos. Encabeça há tempos a lista dos 500 computadores mais poderosos do planeta, sendo também responsável pela maioria dos serviços que simplesmente não podem parar, como comprovam a Nasa, inúmeros bancos e operadoras de telefonia.

O único risco numa edição como esta é soarmos arrogantes. Porém, ainda que sejamos julgados dessa forma, garantimos, sem titubear, um fator importante: nós podemos. ■

Pablo Hess
Editor

ÍNDICE

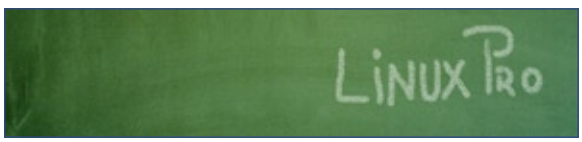
CAPA

COLUNAS

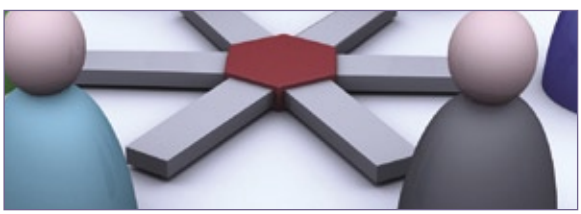
NOTÍCIAS

CORPORATE

TUTORIAL

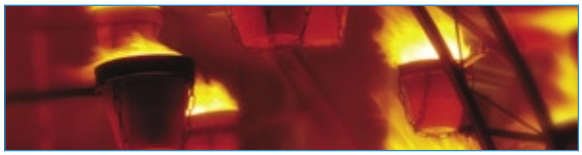


ANÁLISE

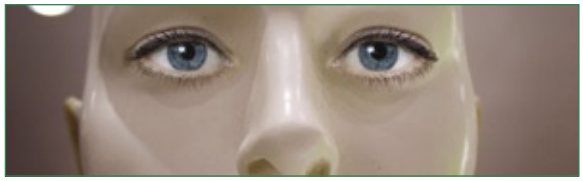


REDES

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.*

Market share do Linux

Acompanho a revista desde a primeira edição em Agosto de 2004 e tenho uma pequena coleção desta, mas tenho algumas perguntas:

- Qual é a real participação do Linux no *market share* mundial?
- Nos segmentos de desktops, em uma comparação direta entre Linux, Mac OS X e Windows, quanto o sistema do pingüim abocanha dessa pizza?
- E com relação ao sistemas Linux em dispositivos embarcados? Qual sua participação em relação à concorrência?

Quais são as fontes realmente seguras e confiáveis concernentes a esses números, sem "puxarem a sardinha" para um dos lados? Pergunto porque muitos links que me apresentam mostram o Linux com um índice de participação com os mesmos números de sete ou oito anos atrás. Será que não mudou nada? Existe mesmo crescimento?

Jeferson L.O. Mendes

Resposta

Prezado Jeferson, contabilizar o número de computadores rodando sistemas proprietários como Windows e Mac OS X é relativamente simples, já que eles devem ser, obrigatoriamente, comercializados. Já com sistemas livres, que não requerem a aquisição de licenças, é muito mais difícil obter os números verdadeiros.

Entretanto, o mercado de desktops parece ter o market share mais fácil de se medir de formas indiretas, como fazem os links que você citou. Como uma das atividades mais comuns em desktops é o acesso à Internet, a proporção de sistemas operacionais que acessam os principais sites de interesse geral pode ser considerada um bom indicativo da proporção real de sistemas operacionais instalados em desktops.

Portanto, em relação ao market share de desktops, acredito que o Linux de fato exiba números semelhantes aos mostrados nos links citados.

Já em relação a servidores, a questão pode ser mais complicada, pois é de se imaginar que poucos servidores acessem os mesmos sites de interesse geral, e não conheço qualquer outra forma indireta de se contabilizar a proporção de sistemas operacionais nessas máquinas.

No Brasil, a pesquisa mais recente de que temos notícia nesse sentido é a que foi realizada pelo Instituto Sem Fronteiras, ao longo de 2007, que constatou o crescimento real do uso de Linux em ambientes corporativos, tanto em desktops quanto em servidores. ■

Errata

No artigo de análise do Librix 3 ("Para conquistar o público"), publicado na página 64 da Linux Magazine 42, o autor afirma que não há uma ferramenta gráfica para a configuração de conexões PPPoE (ADSL). No entanto, trata-se de um engano, pois o Librix 3 traz o PyADSL, que realiza exatamente essa tarefa.

LINUXPARK 2008

O ECOSSISTEMA DE NEGÓCIOS EM SOFTWARE LIVRE NO BRASIL

O Linux Park 2008 é o evento que vai definir o futuro do mercado de tecnologias abertas no Brasil. Compareça e compartilhe suas experiências com os principais decisores e influenciadores do mercado.

Para mais informações, visite o site:
www.linuxpark.com.br

- Modelos de negócios com Software Livre em vários segmentos
- Cases de sucesso
- Keynotes
- Conteúdo específico para o segmento de revendas de Software Livre
- Provas de certificação

Patrocínio Diamond: Itautec, SERPRO

Patrocínio Gold: LxPN Distributions GmbH, QualityWare, Kenos Sistemas de Gestão Integrada

Organização e realização: Linux New Media

Promoção: Linux Magazine

COLUNA

Filme já visto: sucesso em estratégia Open Source

Augusto Campos

Novas empresas resolvem adotar modelos abertos com freqüência. Porém, há formas certas e erradas de iniciar um projeto desse tipo, sob o risco de fracasso sonoro.

por Augusto Campos

Hoje eu revi um filme que já passou outras vezes: organização de grande porte subitamente anuncia sua entrada na "onda do Código Aberto". Em vez de buscar interesses em iniciativas existentes, lança diversos projetos em paralelo e espera que desenvolvedores embarquem com entusiasmo. No lugar de escolher plataformas populares nesse meio, opta por outras de seu interesse específico.

> ***Há algumas outras características em comum entre projetos colaborativos e abertos largamente bem-sucedidos.***

Em vez de começar oferecendo código e documentação, faz já uma reunião para definir diretorias. E em vez de participar ativamente nas comunidades, envia *releases* preparados por assessorias de imprensa, que não trazem as informações essenciais ao seu alvo, como URLs com detalhamento dos projetos, como regras de participação, objetivos, links para download etc.

Você também já viu esse filme? Eu vi muitas vezes, e ele termina com o projeto sendo abandonado e os gestores convencidos de que a culpa é do modelo aberto, que não funciona.

Projetos de código aberto bem-sucedidos costumam começar com um desenvolvedor motivado a resolver um problema seu. Há uma coceira e ele precisa coçar, afirma Eric Raymond no seu livro sobre o processo de desenvolvimento aberto, "A Catedral e o Bazar".

O projeto aberto prospera quando existe demanda de usuários interessados, e assim mais desenvolvedores acabam gravitando ao redor dele, afligidos por suas próprias coceiras, agregando mais recursos ao projeto, num processo circular.

Mas há algumas outras características em comum entre projetos colaborativos e abertos largamente bem sucedidos. Vamos ver alguns casos.

O Linux começou com um estudante com um 386 na mão – e muitas idéias na cabeça – e avançou aos poucos, criando sua estrutura formal ao longo do processo. O *Apache* começou quando o *NCSA httpd* parou e uma série de usuários resolveu se coordenar informalmente no esforço de dar continuidade a ele.

O *Firefox* começou quando dois funcionários descontentes da Netscape resolveram criar um navegador mais magro que o Mozilla, e então deram início a seu projeto pessoal – que mais tarde acabou sendo adotado como carro-chefe da própria organização. O *Wordpress* nasceu como um projeto pessoal e deu origem a uma bem sucedida empresa, que há poucos meses recebeu um investimento de US$ 29,5 milhões de gigantes da mídia como o New York Times e a CNET. O *MySQL* nasceu dentro de uma empresa, para resolver uma demanda, e acabou virando o seu carro-chefe, agregando usuários e desenvolvedores externos ao longo do caminho.

O que esses projetos de sucesso têm em comum? Nasceram por interesse dos desenvolvedores (individuais, grupos ou corporativos), mantiveram licenças livres desde o princípio, participaram ativamente das comunidades de usuários. Todos foram desenvolvidos em linguagens populares e tornaram-se multiplataforma de maneira natural. Todos alcançaram velocidade de cruzeiro devido ao próprio impulso da demanda que supriam junto aos desenvolvedores e usuários. Inclusive, são bons modelos para copiar quando se pensa em estratégia Open Source numa organização de TI. ■

Sobre o autor

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

A revolução do software livre chegou ao mundo corporativo: Sistema Librix Itautec. Testado e homologado pela Itautec, é a melhor, mais segura e estável distribuição Linux do mercado. Sua capacidade de comunicação e convivência com diversas possibilidades de hardware e com o sistema operacional mais usado no mercado minimiza eventuais barreiras restritivas à sua implementação. Do ponto de vista do usuário, é bastante intuitivo e de fácil assimilação, com assistentes amigáveis e as mais diversas funcionalidades. Além disso, a Itautec oferece diversas opções de garantia e suporte, que vão do básico à missão crítica, de acordo com a necessidade de sua empresa. Até o suporte ao Librix é mais livre. Pode ser feito por telefone, internet, visita técnica ou em mais de 2.700 localidades em todo o Brasil.

Sistema Librix 2.0. Sua empresa com muito mais TI: Tecnologia Itautec.

A ITAUTEC ESTÁ PRESENTE EM MAIS DE 2.700 CIDADES.

www.itautecshop.com.br

COMPRE DIRETAMENTE DO FABRICANTE

0800 121 444

De 2ª a 6ª, das 8h às 20h. Sábado, das 9h às 18h.

Itautec

COLUNA

RSyslog

Charly Kühnast

Os montes de informações gerados pelos bons serviços de log sobrecarregam o armazenamento e o grep. Será que acoplar o Syslog a um banco de dados ajuda?

por Charly Kühnast

Quem disse que tamanho não é documento? Meus filtros de spam cuspiram, só hoje, um logfile de 3 GB, o que não seria um problema se eu simplesmente quisesse me livrar do lixo eletrônico. Porém, preciso obter várias estatísticas sobre ameaças de spam e vírus a partir desse arquivo, e o `grep` leva muito tempo, além de ocupar a I/O em demasia.

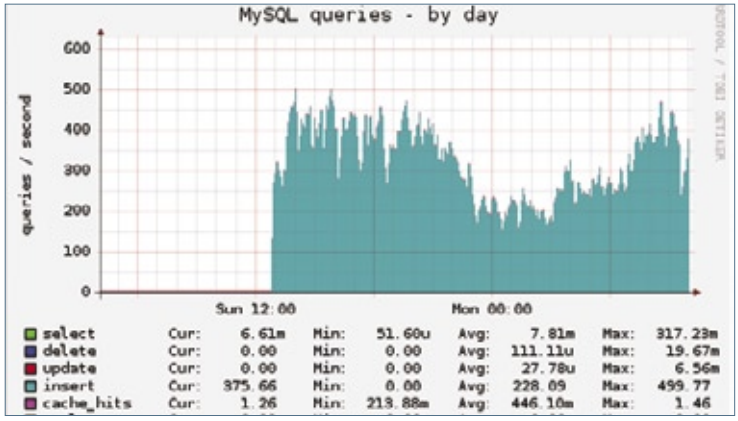


Figura 1 O monitor exibe as consultas SQL feitas pelo *RSyslog*.

O *RSyslog*[1] se aproxima muito da solução para esse problema – ele insere os logs diretamente num banco de dados *MySQL* ou *PostgreSQL*, o que significa que é possível substituir os comandos do `grep` por rápidos comandos *SQL*. O RSyslog está disponível em várias distribuições e é o syslog padrão no *Fedora* 8, por exemplo. Por padrão, meu ambiente de laboratório com *Ubuntu* utiliza o *Sysklogd*, o que facilita a migração para o RSyslog. Inicialmente, é possível até mesmo manter o arquivo `syslog.conf`. Em sua maioria, o arquivo de configuração do RSyslog tem o mesmo formato que o sistema legado, embora suporte algumas opções a mais para conexão a bancos de dados.

Primeiro, é necessário configurar um banco de dados. Para isso, pode-se executar o script `createDB.sql`, que é fornecido junto com o pacote do RSyslog:

```
mysql -u root -pSenha <./createDB.sql
```

Essa linha de comando cria automaticamente um banco de dados chamado *Syslog*, assim como as tabelas necessárias.

Em seguida, no prompt do MySQL, deve-se criar um usuário e atribuir-lhe os privilégios:

```
> grant ALL ON Syslog.* to rsyslog@localhost
➥ identified by 'secret';
> flush privileges;
```

Depois, é muito fácil ordenar o RSyslog para que use o banco de dados – bastam duas linhas no arquivo `/etc/rsyslog.d/mysql.conf`:

```
$ModLoad MySQL
mail.* >localhost,Syslog,rsyslog,secret
```

A primeira linha carrega o módulo necessário para que o RSyslog acesse o banco de dados. A segunda define o recurso de log que contém as entradas que o RSyslog deve inserir no banco de dados. No meu caso, preciso apenas dos dados do recurso de email para criar estatísticas do filtro de spam, seguidos pelos parâmetros de acesso ao banco de dados: nome da máquina, do banco de dados, do usuário do MySQL e senha.

Após iniciar o RSyslog, conferi sua atividade, inserindo dados no banco (**figura 1**).

É claro que isso não melhora as estatísticas do filtro anti-spam, mas acelera e facilita muito o trabalho de obtê-las. ■

Mais informações

[1] RSyslog: http://www.rsyslog.com

Sobre o autor

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

IBM Development Conference

***A Linux New Media** apoia a maior conferência técnica da IBM no Brasil.*

Entenda, através de palestras e mini-cursos com hands on, como a IBM pode trabalhar de forma eficaz em procedimentos de desenvolvimento ágil para aplicativos de melhor performance e alta qualidade.

Veja como a Super Liga de Desenvolvimento IBM pode combater os terríveis bugs que atrapalham o seu dia-a-dia. Junte-se a nós e saiba como suportar a criação do Software Fantástico.

Passe Simples

R$ 400,00**

03 Testes de certificação*
Palestras
Laboratórios
Material de apoio
Tradução simultânea
Almoço no local

Palestras abordando temas como:

- Arquitetura Orientada a Serviços (SOA)
- Segurança no ambiente de desenvolvimento
- Open Computing
- Web 2.0
- Gestão de Qualidade em ambiente de desenvolvimento

e muito mais!

Certificações

Certified for IBM Information Management software
Certified for IBM Rational. software
Certified for IBM Tivoli. software
Certified for IBM WebSphere. software

Acesse:
ibm.com/br/navcode
código IBMDC2008

18 e 19/06

WTC Hotel - São Paulo

Apoio

LINUX Magazine | easyLINUX! | LINUX NEW MEDIA The Pulse of Open Source

Patrocínio

AUDARE Engenharia de Software | IBM developerWorks Live! | Optimize

*Não inclui certificação em Lotus **Preços validos para pacotes comprados ate 18/05/2008

COLUNA

Pergunte ao Klaus!

Klaus Knopper

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

por Pablo Hess

Múltiplas placas de som

Tenho duas placas de som M-Audio Delta 1010LT e quero que elas funcionem juntas, como se fossem uma única placa, pois meu interesse é ter 16 entradas de áudio na máquina. Já consultei várias documentações a esse respeito e algumas sugestões são muito difíceis – exigindo a reinstalação do *ALSA* e aplicação de *patches* no kernel, por exemplo. Também já li que o antigo subsistema de áudio OSS permite isso, mas acho que remover o ALSA e instalar o OSS seria mais problemático que prático.

> ***Simplesmente ajustar o desempenho do sistema e as prioridades dos processos não é suficiente. Provavelmente, será necessária a extensão de tempo real do kernel.***

Estou usando um processador AMD de 2.6 GHz e a distribuição AGNULA, que resulta em menos *xruns* que qualquer outra distribuição multimídia que eu já tenha testado. Ainda não encontrei uma configuração que diminua os xruns e não entendo por que o AGNULA é tão melhor a esse respeito.

É possível conseguir o que eu quero com alguma versão mais recente do ALSA, sem uma recompilação e reinstalação completa? Sei que a segunda placa precisará ser escrava da primeira e conectada a esta através das conexões SMPTE ou *Word Clock*. Preciso descobrir como fazer as duas placas funcionarem como uma única, pois tenho um estúdio de gravação e necessito das entradas extras. Alguma sugestão?

Resposta

Em resumo, a sua questão está respondida (em inglês) em [1]. Com essa configuração, basicamente, informa-se à biblioteca ALSA quais entradas de hardware e placas usar para cada entrada (virtual) de áudio nos aplicativos, e reunir mixers para que as duas placas se comportem como uma única. Como isso é feito por software, é uma tarefa que depende totalmente do compartilhamento de tempo, o que explica porque é provável sofrer *overruns* e *underruns* quando o sistema não está preparado especialmente para esse fim. Simplesmente ajustar o desempenho do sistema e as prioridades dos processos não é suficiente. Provavelmente será necessária a extensão de tempo real do kernel [2].

O motivo para o melhor desempenho no AGNULA pode estar relacionado com o fato de que ele também utiliza um kernel modificado para aplicações de tempo real. A maioria das distribuições mais usadas (ainda) não incluem esse recurso do kernel, pois ele não faz parte do kernel oficial (também chamado de *vanilla*) e cria um certo *overhead*, além de modificar muitos aspectos internos do kernel, tais como o tratamento de interrupções para dispositivos. Para processamento de som e sintetizadores de áudio de tempo real é essencial utilizar essa extensão do kernel, independente da velocidade do seu computador. ■

Mais informações

[1] Tutorial de uso de múltiplas placas de som: http://www.sound-man.co.uk/linuxaudio/ice1712multi.html

[2] Extensões de tempo real para o kernel: http://rt.wiki.kernel.org/

Sobre o autor

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

Pablo Hess

É impossível não se impressionar com o volume de melhorias no kernel. Veja os motivos para adotar a versão mais recente.

por Pablo Hess

O kernel 2.6.25, lançado oficialmente no dia 17 de abril (83 dias após a versão 2.4.24 ser liberada), dá prosseguimento a seu processo incrivelmente veloz de desenvolvimento. Seus 12.243 *commits* incluem inovações tecnológicas, técnicas – para aumentar a velocidade e eficiência do sistema –, recursos de segurança e ferramentas de virtualização.

Inovações

Após a integração de sete novos drivers Wi-fi ao kernel 2.6.24, finalmente foi incluído o driver *Ath5k* para chips de rede sem fio Atheros, acompanhado do driver para chipsets Realtek RTL8180 e 8185. No campo dos sistemas de arquivos, o *Ext4* se aproxima da fase estável, com novos recursos importantes, como um alocador multi-blocos, por exemplo.

O gerenciamento de memória também ganhou possibilidades com o uso de grupos de tarefas (*cgroups*) pelo novo controlador de recursos de memória. Quanto aos processos, foi introduzido um terceiro estado para processos dormentes – *killable* –, que deve oferecer um maior controle sobre sua execução.

Acelerando

O escalonador de tarefas CFS, introduzido no Linux 2.6.23, recebeu sua segunda leva de atualizações. Embora a maioria não afete desktops, a latência foi um dos focos das alterações a seu código, que agora suporta o programa *LatencyTop* para medição de latência e oferece melhor tratamento a tarefas que exijam tempo real através do recurso *Preempt RCU*. O agrupamento de tarefas para escalonamento também tende a melhorar o desempenho do sistema como um todo.

O acesso aos recursos do sistema também passou a ser mais igualitário com a inclusão do novo mecanismo de bloqueio de recursos com filas tipo *FIFO*.

Segurança

O mecanismo de controle obrigatório de acesso *SELinux* é possivelmente a ferramenta de segurança mais eficaz disponível para o sistema do pingüim. No entanto, não foi incluído no kernel. Em vez disso, o novo SMACK (*Simplified Mandatory Access Control Kernel*) tem agora sua estréia, com menos recursos que o maduro SELinux – voluntariamente, pois isso o torna mais fácil de administrar. O sistema de segurança concorrente, *AppArmor*, ainda recebe duras críticas de diversos desenvolvedores do kernel e não se sabe se algum dia será incluído.

Virtualização

Na área da virtualização, o *KVM* começa a se estabilizar e as mudanças sofridas melhoram tanto seu desempenho quanto sua compatibilidade. Além disso, finalmente outras arquiteturas entraram nos planos dessa infra-estrutura de virtualização nativa do kernel – antes restrita a sistemas *x86*.

Outras estruturas de virtualização, como *Virtio* e *Paravirt_ops*, também evoluíram, com o segundo recebendo suporte a *x86-64*.

Drivers

Como de costume, toneladas de novos equipamentos ganham suporte com a nova versão do kernel. Esse é o caso, além dos adaptadores Wi-fi, de chips de áudio, vídeo (DRM), controladores SATA, adaptadores de rede UMTS (conhecidos popularmente como 3G) e também de alguns subsistemas, como DVB, V4L e I2C.

Futuro

A árvore *Linux-next* promete facilitar o trabalho dos desenvolvedores, reunindo todas as mudanças a serem propostas em um único local, de forma a permitir a rápida correção de interferências entre as alterações propostas por cada desenvolvedor. ■

Mais informações

[1] Linux 2.6.25: http://kernelnewbies.org/Linux_2_6_25

COLUNA

Crônicas do kernel

Zack Brown

Questionamento sobre a manutenção do kernel 2.2 e o git ganha facilidade.

por Zack Brown

Kernel 2.2

Em agosto de 2007, Xose Vazquez Perez perguntou sobre o status da árvore do kernel 2.2 e notou que a versão 2.2.26 havia sido lançada há muito tempo, em 2004. Por outro lado, o *rc* mais recente do 2.2.27 datava de janeiro de 2005. Willy Tarreau respondeu que qualquer nova versão do kernel 2.2 levaria os usuários a acreditarem que ele seria utilizável. Entretanto, apontou que várias falhas de segurança ainda existem nessa árvore, que está simplesmente desatualizada demais para continuar a ser mantida.

> ***Várias falhas de segurança ainda existem nessa árvore, que está simplesmente desatualizada demais para continuar a ser mantida.***

Xose aceitou a explicação na época, mas recentemente tornou a manifestar-se, dessa vez, sugerindo a remoção do kernel 2.2 da página inicial do *kernel.org*. Se essa versão está tão desatualizada que ninguém deveria usá-la ou aplicar-lhe *patches*, afirmou, não deveria ser mostrada no kernel.org. Apesar do argumento de Xose fazer sentido, o kernel 2.2 continua listado na página do kernel.

Não ao Cogito

Quando Linus Torvalds criou o *git*, tinha em mente um equivalente a uma camada de chamadas de sistema para o controle de revisões. Seu aplicativo fornecia os recursos de baixo nível para manipulação de alterações em diretórios que o *BitKeeper* oferecia, eliminando aqueles que não eram usados e acrescentando outros, como uma semântica de *tags* com sentido.

No início, o programa *git* era difícil de entender, pois não oferecia os recursos e serviços completos esperados de um sistema de controle de revisões. Em vez de permitir aos usuários a digitação de um único comando para sincronizarem seus repositórios com o *upstream*, por exemplo, era obrigatório obter as alterações nesse repositório e depois incorporá-las ao repositório local com outro comando.

Esse comportamento era intencional, pois Linus não tinha o objetivo de fornecer uma interface para repositórios, esperando, em vez disso, que cada um criasse seus scripts pessoais para usarem as "chamadas de sistema" do git.

O *Cogito* foi a primeira e mais popular dessas interfaces de script e chegou-se a acreditar que ele seria a principal ferramenta usada por usuários comuns em conjunto com o git. Porém, agora vemos o fim do desenvolvimento do Cogito e o próprio git passará a oferecer também a camada superior para os usuários comuns.

A interface amigável do git está em desenvolvimento há algum tempo e costuma ser chamada de camada de "porcelana". Ela oferece um conjunto de comandos familiar para a maioria dos usuários de sistemas de controle de versão e utiliza os comandos de nível mais baixo em sua implementação.

Com isso, qualquer um que esteja usando o Cogito deve mudar para o git imediatamente, segundo conselho de Torvalds. ■

Sobre o autor

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

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

info
MELHOR RELAÇÃO CUSTO/BENEFÍCIO

Hospedagem de Sites

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

R$ 14,90 /mês

Registro de domínios

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

R$ 15,00 /ano

Domínio Nacional (".br")

R$ 30,00 /ano

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

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

Servidores dedicados

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

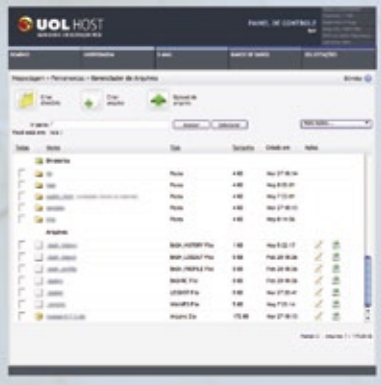
R$ 490,00 /mês

Programa de Parcerias UOL HOST

Entre em contato e saiba as vantagens

Painel de Controle UOL HOST

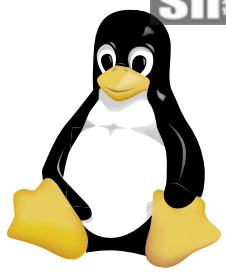
O painel mais moderno do mercado. Gerenciamento completo para as necessidades administrativas do dia-a-dia do seu website.



UOL HOST
QUALIDADE EM SERVIÇOS WEB

ASSINE 0800 723 6000

WWW.UOLHOST.COM.BR



Linux é o sistema operacional embarcado mais utilizado

De acordo com um estudo da empresa americana de pesquisas de mercado Venture Development Corporation (VDC), o Linux é o sistema operacional mais utilizado em sistemas embarcados na indústria. Segundo a pesquisa, 18% dos engenheiros na área de dispositivos embarcados que tomaram parte da pesquisa utilizam um firmware Linux em seus equipamentos. Enquanto isso, 5% lançam mão de outros sistemas embarcados de código aberto, tais como o sistema operacional com resposta em tempo real FreeRTOS, o TinyOS ou o eCOS.

Como principais motivos para a utilização do Linux como sistema embarcado, foram citados, entre outros, a disponibilidade de ferramentas de desenvolvimento gratuitas e de qualidade, desnecessidade de pagamento de licenças ou *royalties* por equipamento produzido, flexibilidade do sistema operacional, advinda especialmente do fato de que seu código-fonte está disponível, e familiaridade dos desenvolvedores com o sistema, pois já o utilizam para desenvolvimento em servidores e desktops.

Ainda de acordo com o estudo, as constantes melhoras no suporte a hardware, proveniente especialmente da popularização do Linux em sistemas de uso geral — notadamente, os desktops, laptops e, mais recentemente, subnotebooks — teriam contribuído fortemente para uma disseminação mais indiscriminada do sistema do pingüim, que já chegou há algum tempo aos dispositivos embarcados. Entretanto, a popularidade do sistema ainda não chegou aos casos em que os dispositivos são muito pequenos, bem como àqueles com especificações muito rígidas de resposta em tempo real ou em áreas que necessitem de um alto grau de segurança.

Fornecedores de ferramentas de desenvolvimento comerciais, como é o caso da Montavista e da Wind River, teriam que se esforçar mais no futuro para oferecer um diferencial competitivo e se destacar entre as ferramentas de código aberto, que já atingiram um excelente grau de sofisticação. Além disso, há grande demanda por sistemas modulares e integrados de desenvolvimento, consistindo em hardware, software e ferramenta de desenvolvimento. Essa seria uma área em que fornecedores de sistemas de desenvolvimento comercias poderiam se diferenciar da concorrência "livre". ■

Asterisk é o PBX mais usado no mundo

O Asterisk, plataforma de telefonia IP mais utilizada em todo o mundo, alcançou a marca de 3 milhões de downloads em seu site apenas no ano de 2007. O sistema é totalmente desenvolvido em código aberto e está atualmente nas versões 1.4.19.2 (estável) e 1.6.0-beta-9 (desenvolvimento).

Mark Spencer, criador do Asterisk, participou recentemente do VoIP Summit Brasil, evento realizado em São Paulo e organizado pela Commlogik Corporation. Segundo Spencer, o sucesso do Asterisk está baseado em sua segurança, escalabilidade e interoperabilidade. De acordo com Alexandre Hebra, presidente da Commlogik, a plataforma Asterisk pode reduzir o custo de uma solução de telefonia em até 80% do valor. ■

XP no XO

Agora é definitivo. O XO, do projeto OLPC (*One Laptop Per Child*) virá embarcado com o Windows XP como opção ao sistema operacional Linux. A participação da Microsoft nesse projeto foi marcada por muitos mistérios e considerável desinformação, mas, no dia 15 de maio, a empresa de Redmond finalmente deu sua bênção ao projeto.

De acordo com James Utzschneider, gerente da unidade de desenvolvimento de marketing da Microsoft, os testes foram bem sucedidos. Em seu blog, Utzschneider afirma que "a Microsoft e a OLPC anunciaram suporte do Windows XP para o computador OLPC XO". As duas organizações trabalharão juntas, a partir do próximo mês, em diversos programas-piloto e em mercados-chave, e os primeiros computadores serão lançados em agosto ou setembro. Inicialmente, ele estará disponível apenas em países emergentes onde o governo esteja subsidiando a compra de um grande número de PCs para estudantes. ■

OpenSUSE adere ao Google Summer of Code

O projeto OpenSUSE anunciou que tem dez projetos sendo financiados pelo Google Summer of Code este ano, por meio do qual trabalhará com estudantes de todo o mundo para desenvolver novos códigos e aperfeiçoar os projetos existentes. O programa do Google oferece aos estudantes desenvolvedores um pagamento em dinheiro como forma de incentivá-los a escrever códigos para vários projetos em plataforma aberta, além de inspirar jovens desenvolvedores a participar do desenvolvimento em código aberto e ajudar projetos a identificar novos desenvolvedores.

"Estou muito satisfeito pelo oferecimento de dez vagas no programa Summer of Code por parte do Google", afirma Joe "Zonker" Brockmeier, o administrador da comunidade openSUSE. "É um ótimo programa, que permite que a comunidade desenvolva novas aplicações ou funcionalidades e, o mais importante, oferece oportunidade para novos colaboradores aprenderem a trabalhar com projetos em código aberto. Nós não apenas conseguimos códigos de valor, mas também estamos aptos a trabalhar mais próximos da nova geração de colaboradores".

De acordo com Brockmeier, o interesse foi tão alto que o openSUSE recebeu mais de cinqüenta aplicações para suas dez vagas, o que lhe gerou a confiança de que, a longo prazo, o trabalho com os estudantes renderá contribuições valiosas.

O Google Summer of Code financiou mais de 1500 estudantes e 2000 tutores de 90 países nos últimos três anos. Este ano o programa está financiando 1125 estudantes com 175 projetos em código aberto, incluindo o openSUSE. Para mais informações sobre as atividades do openSUSE no Google Summer of Code, visite http://code.google.com/soc/2008/suse/about.html. ■

US$ 12 milhões para projeto livre

O *Openbravo*, projeto de sistema ERP e ponto de venda (PoS – *Point of Sale*) de código aberto, recebeu em maio US$ 12 milhões em fundos. Esse investimento reforça o crescente interesse em sistemas abertos como alternativas customizadas às gigantes do meio, como Oracle e SAP.

Baseado na Espanha, o Openbravo se especializou em ERP e PoS e vem empurrando o mercado norte-americano. De acordo com a empresa, parte do financiamento será direcionado para consolidar a posição de liderança no setor de ERP e PoS. O Openbravo tem crescido em todas as direções desde a publicação de seu código em abril de 2006, quando alcançou mais de 1500 downloads diários de seu ERP. Até hoje ele já foi baixado mais de 500 mil vezes – o triplo do número de vezes dos outros projetos ERP de código aberto – e conta com 40 projetos de localização e 80 parceiros, com presença em 40 países.

O *Openbravo POS*, adquirido no ano passado, já é lider destacado no mercado de aplicativos POS de código aberto. Diariamente, o sistema foi baixado mais de 250 vezes, e tem tido um retorno favorável de sua comunidade, parceiros e clientes.

Do ponto de vista dos negócios, a empresa está construindo o mercado à volta de seu produto. Suas ações nesse quesito são descritas como sigilosas, em função da estratégia adotada pela companhia. Atualmente, a empresa tem sido procurada por fabricantes de hardware interessados em explorar o mercado para o Openbravo POS.

Adicionalmente, a companhia tem estabelecido parcerias-chave em tecnologia com o intuito de aumentar o número de instalações do sistema. O tipo de companhia que instala e utiliza o Openbravo é de médio e grande portes. Algumas de suas características são inovadoras e não possuem equivalentes em seus concorrentes proprietários. ■

Outsourcing na América Latina

A North-by-South, empresa de serviços de terceirização de desenvolvimento de softwares de código aberto em âmbito internacional para a América Latina, anunciou no último mês ter fechado um investimento com a Launch Capital LCC. Essa injeção de capital provém do sucesso recente da North-by-South em consolidar as suas operações.

De acordo com Ryan Bagueros, fundador da North-by-South, a empresa "tem conseguido produzir uma rede significativa de desenvolvedores de programas de código aberto na América Latina por meio de nossos centros em São Fransisco (EUA) e São Paulo, e esse capital adicional nos dá a oportunidade de realmente acelerar esse processo". Bagueros também informa que "o investimento da Launch Capital nos ajudará a fazer com que mais companhias percebam que há um fenômeno incrível acontecendo com o desenvolvimento de sistemas de código aberto nas Américas".

A North-by-South é a única empresa de terceirização internacional de serviços especializada no desenvolvimento de soluções de código aberto, incluindo Linux, PHP, MySQL, Ruby on Rails e outras tecnologias consideradas de ponta. "Já é fato comprovado que o Software Livre é mais eficiente nos quesitos custo e segurança, oferecendo uma plataforma escalável para o desenvolvimento de aplicações Web 2.0 e em rede", colocou Bagueros.

De acordo com o executivo, devido ao suporte dos governos de países da América Latina, uma onda de entusiasmo em torno do Código Aberto teria se espalhado por todo o hemisfério sul. Uma geração inteira de programadores latino-americanos altamente qualificados tecnicamente estaria disponível e de posse das qualidades ideais em desenvolvedores de código aberto: paixão pelo desenvolvimento de software, atenção meticulosa a detalhes e um profundo entendimento do funcionamento dos sistemas operacionais, bancos de dados e plataformas web.

Esse nível de excelência em tecnologia, combinado às vantagens do trabalho em equipes disponíveis a uma diferença de fusos horários de apenas quatro horas, posicionaria a América Latina como a nova escolha para a redução de custos com melhoria tecnológica e desenvolvimento terceirizado. ■

Nova estratégia da RH em 2008

Em mais uma visita ao Brasil, Alex Pinchev, vice-presidente e presidente global de vendas, serviços e marketing da Red Hat, anunciou as mudanças planejadas pela empresa norte-americana para o ano fiscal que se inicia dentro de um mês. Segundo Pinchev, o novo CEO da empresa, Jim Whitehurst, já está imprimindo um novo ritmo a ela: atribuiu novas responsabilidades a executivos e mexeu nos relacionamentos entre áreas dentro da companhia.

Segundo o vice-presidente, as mudanças na Red Hat se devem a diversos fatores, como a crescente sofisticação dos softwares de código aberto e a globalização da própria empresa. O propósito da empresa também muda: "o mercado de código aberto ficou mais orientado ao cliente", afirmou Pinchev, "que não quer ser só um cliente, mas parte da inovação". Com isso, o executivo definiu a nova estratégia impressa pelo novo CEO: "Para a Red Hat, tudo gira em torno do cliente".

Especificamente com relação ao mercado brasileiro, Alex afirmou que esse é um dos mercados que mais crescem no mundo, e o apoio do Governo Federal é fundamental. Além disso, outros diferenciais do Brasil são a compreensão da dinâmica e dos valores do Código Aberto pelas grandes empresas – "muito maior que na maioria dos outros países", colocou o executivo –, que enxergam como vantagem dessa tecnologia a velocidade de desenvolvimento e implementação, além, é claro, do menor custo.

Alex Pinchev anunciou também o reforço e esclarecimento da política de parceiros comerciais da Red Hat: "parceiros são cruciais para nosso sucesso; 60% dos negócios da Red Hat vêm de parceiros", contabilizou. Segundo ele, "os parceiros sabem o que é o Código Aberto, e sabem vender Software Livre"; por isso, são tratados "como parte da Red Hat". Existe até um departamento de marketing exclusivo para os parceiros.

"A Red Hat começou no Brasil há dois anos, com aproximadamente 20 funcionários. Hoje, temos 60", colocou Julián Somodi, Gerente Geral da Red Hat para a América do Sul, também presente no evento. Ele acrescentou ainda que há planos de criação de novos escritórios da companhia em outras cidades do Brasil, mas não revelou quais, informando apenas que já existem equipes da empresa trabalhando em Brasília, Curitiba, Porto Alegre, Rio de Janeiro e Belo Horizonte.

Os negócios em torno do servidor de aplicações JBoss foram os que mais cresceram no último ano, segundo Gabriel. A expectativa para o próximo ano, portanto, é de 100% de crescimento. Por isso, o mercado de JBoss é estratégico para a Red Hat, assim como os de infra-estrutura (com a virtualização ocupando um papel fundamental) e o de gerenciamento (*RHQ*). ■

Silverlight para Linux

No mês de maio foi lançada a primeira versão estável do *Moonlight*, uma implementação de código aberto da tecnologia *Silverlight*, da Microsoft. O programa foi desenvolvido para uso em sistemas baseados no Unix, o que inclui o Linux.

Todos sabem que ainda resta um longo caminho para o Silverlight alcançar a popularidade do *Flash*, da Adobe. Essa dificuldade força a Microsoft a se aproximar cada vez mais do Código Aberto para acelerar o desenvolvimento de seu produto.

O Moonlight não é um projeto da Microsoft, mas a empresa tem trabalhado junto à equipe do Mono em seu desenvolvimento. ■

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

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

Flexibilidade e Confiabilidade

Solução de gestão integrada ADempiere:

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

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

Kenos
Sistemas de Gestão Integrada

Entrevista com Jair Silva, gerente de software da área de arquitetura tecnológica da Caixa.

Vem pro Linux você também

A Caixa Econômica Federal é grande usuária de SL/CA e responsável por um dos maiores cases de sucesso dessa tecnologia em todo o mundo. Veja por quê.

por Pablo Hess

Linux Magazine» ***Como e por que começou o envolvimento da Caixa com Linux e Software Livre e de Código Aberto?***

Jair Silva» O envolvimento da Caixa com Linux e SL/CA se dá basicamente devido a dois pontos: operacional e estratégico. Do ponto de vista operacional, precisávamos utilizar soluções com baixo grau de complexidade e aderentes às nossas especifidades. Ou seja, soluções cuja curva de aprendizagem pelas equipes técnicas não fossem tão longas e cujo processo de implementação não nos onerasse com a aquisição de novos hardwares e redimensionamento de nossa rede de telecomunicações. Em resumo, as soluções com SL/CA se adaptam ao nosso ambiente, ao contrário do que ocorre com algumas soluções proprietárias que exigem a adaptação do ambiente.

Do ponto de vista estratégico, tínhamos que internalizar o processo de inteligência das soluções em TI e adquirir independência de alguns fornecedores, pois nosso poder de negociação junto a alguns fornecedores era inversamente proporcional à nossa dependência. Outro ponto para a adoção de SL/CA é a alta competitividade imposta pelo segmento bancário. Por causa dela, tínhamos que reduzir o custo de TI para que nossos produtos fossem mais competitivos.

Jair Silva, gerente de software da área de arquitetura tecnológica da Caixa.

LM» ***Por onde começou a adoção do SL/CA na empresa?***

JS» O projeto das loterias foi nosso primeiro grande desafio em SL/CA. Há aproximadamente quatro anos, a Caixa iniciou o processo de internalização do canal lotérico, que era gerida por uma empresa terceira. Para se ter idéia do tamanho do canal lotérico, ele é constituído por aproximadamente 9,6 mil casas lotéricas, com 25 mil terminais financeiros lotéricos (TFL) que realizam 1.200 transações por segundo, num total de 28 bilhões de transações por dia.

Nesse processo de internalização, as áreas de TI da Caixa trabalharam na especificação e contratação dos circuitos de redes de telecomunicações para os 9,6 mil pontos, no desenvolvimento da aplicação em *Java*, na especificação e contratação dos TFLs e na especificação e implementação de todos os softwares de infra-estrutura, sistema operacional, DNS, distribuição, sincronismo de horário etc.

Tínhamos um prazo curto para definir e implementar a arquitetura da solução das loterias. Havia duas soluções candidatas a atender esse projeto, uma proprietária e outra de código aberto. Após apresentarmos ao canal de negócios da Caixa o custo de cada solução, não foi difícil justificar o porquê de adotarmos SL/CA.

LM» ***Em que consiste a solução nas lotéricas?***

JS» Inicialmente, os TFLs entraram em produção com uma distribuição da UFMG denominada de *Libertas*, derivada do *Debian*. Hoje, a customização do sistema operacional é realizada pela equipe de TI Caixa. O Código Aberto nos permitiu otimizar o sistema operacional ao extremo. A CETEC (Central de Tecnologia Caixa) alterou a distribuição ao extremo, chegando ao *Zebrix*, cuja inicialização leva apenas dez segundos e cujo tamanho é três vezes menor que o da primeira versão.

Além do sistema operacional, desenvolvemos uma aplicação em SL/CA responsável pela distribuição e atualização de arquivos aos 22 mil TFLs. Em um único dia, conseguimos distribuir e atualizar versões de aplicativos ou softwares de infra-estrutura para todos os terminais, sem impactar o negócio.

Quando o projeto foi implementado na totalidade, em 2005, as loterias da Caixa eram a maior rede Linux corporativa do continente americano.

LM» ***Além das lotéricas, em que áreas e aplicações a Caixa usa SL/CA no momento? Há planos de expansão para outras áreas no futuro?***

JS» Sim, há vários projetos em andamento e muitos outros planejados. Ou seja, estamos apenas no início.

A Caixa já implementou vários aplicativos em SL/CA, alguns utilizados por clientes ou empresas e orgãos públicos conveniados, a exemplo do simulador habitacional e da Universidade Corporativa Caixa – que disponibiliza ao público interno e externo diversos cursos para aprendizagem à distância. Para esses sistemas, utilizamos *Zope*, *Plone*, *Apache*, *Squid*, *PostgreSQL*, *Tomcat* etc.

Também desenvolvemos um gerenciador de impressão – o *Curupira* – baseado no *Cups*, o que nos possibilitou uma redução na ordem de 30% em impressões. Estamos implementando agora uma solução corporativa de fax que utiliza o *Hylafax* e *Asterisk*.

A mensagem de espera telefônica com mensagem institucional implantada nas unidades a Caixa também é uma solução baseada em SL/CA. Algumas centrais telefônicas têm o Asterisk em fase piloto. A tendência é expandir para o maior número possível de unidades. Nossos escritórios internacionais no Japão e Estados Unidos já utilizam o Asterisk como central telefônica.

O sistema de mensageria financeira está implantado 100% em SL/CA. Esse sistema envia um SMS ao correntista todas as vezes que há uma movimentação financeira de débito em sua conta. Todos os aproximadamente 3 milhões de clientes de conta corrente e poupança da Caixa têm esse serviço a sua disposição.

A partir de julho de 2008, começaremos a substituir também o sistema operacional e a aplicação de todos os terminais de auto-atendimento. Aproximadamente 20 mil terminais receberão um aplicativo Java sobre Debian. Já iniciamos os trabalhos de migração de toda a automação bancária da Caixa para plataformas livres, com Debian, *PostgreSQL* e *JBoss*. São cerca de 16 mil estações financeiras, cuja previsão de término é para o final de 2009.

Internamente, estamos adequando nossos normativos e nossa metodologia de desenvolvimento para atender aos padrões W3C e ODF.

Outro projeto que estamos finalizando é o Estação Livre, um desktop para escritórios com todos os componentes em SL/CA, incluindo aplicativos de produtividade, antivírus, mensagens instantâneas, inventário, distribuição e atualização de arquivos. Esse projeto inclui também o serviço de diretório para autenticação dos usuários.

LM» ***Qual a importância, para a Caixa, de usar sistemas e aplicativos de Código Aberto?***

JS» Com o SL/CA, além de sabermos exatamente o que está contido no código, podemos modificá-lo para nossas necessidades, a exemplo do Zebrix e do Curupira. Ter acesso ao código-fonte é muito importante para a Caixa, principalmente no segmento bancário, onde a segurança está acima de tudo. A implementação de sistemas e aplicativos com SL/CA tem-se mostrado mais rápida que com software proprietário, e seu processo de manutenção é mais simples e tem menor custo.

LM» ***Que vantagens a Caixa percebeu ao adotar Software Livre em suas operações?***

JS» Como o negócio da Caixa é banco, e não TI, uma das vantagens que percebemos foi a economia que o SL/CA proporciona, tanto na implementação quanto na manutenção. Isso é facilmente perceptível quando analisamos os 25 mil terminais lotéricos em produção. Outra vantagem é que, com o SL/CA, deixamos de ser apenas usuários, passando a ser também detentores da tecnologia.

Jair Silva, rodeado por sua equipe.

LM» ***E quais foram as dificuldades? O ecossistema em torno dessa tecnologia foi um problema?***

JS» O SL é uma tecnologia inovadora, que resulta, obviamente, em mudança. E é do ser humano resistir a mudanças. Essa resistência tem sido uns dos maiores dificultadores para nossa área na Caixa. Enquanto algumas pessoas aceitam com facilidade as mudanças e tornam-se grandes propulsoras do SL/CA, outras se recusam a deixar a zona de conforto. Mudar isso é uma questão de tempo e persistência.

A carência de mão de obra especializada no mercado brasileiro tem-se mostrado também como um dificultador. O mercado está carente de especialistas em Java, JBoss e PostgreSQL, bem como em grandes ferramentais como *R*, *Pentaho* e outras. A barreira imposta por alguns fabricantes de hardware, por acharem que SL/CA está restrito a apenas duas distribuições Linux, torna-se outro dificultador. Porém, aos poucos, estamos conseguindo mudar essa situação, até porque esses players estão sentido o quanto o SL/CA está crescendo.

Nosso grande problema em expandir soluções em SL/CA com maior velocidade não é nosso ecossistema, mas a falta de padrão de algumas soluções proprietárias. Por conseqüência, alguns sistemas foram implementados com essa característica. Esses sistemas vão perdurar até sua inanição. Porém, estamos trabalhando para conviver com ambos os mundos por um bom período. ■

Fórum Internacional Software Livre 9.0

Potência da comunidade

O FISL 9.0 demonstrou todo o vigor da comunidade brasileira de usuários e desenvolvedores de código aberto.

por Pablo Hess

A cidade de Porto Alegre, no Rio Grande do Sul, tem integrado uma interessante rota migratória nos últimos anos. Todos os anos, em meados de abril, milhares de entusiastas do Software Livre e de Código Aberto (SL/CA) chegam à capital gaúcha para participarem de um evento de troca de informações, contatos profissionais e aquisição de material relacionado ao tema. O Fórum Internacional Software Livre – FISL – estreou no ano 2000 e, desde então, tem tido um público cada vez mais volumoso, internacional e com diferentes motivações.

Na edição 9.0, que ocorreu de 17 a 19 de abril, no Centro de Convenções da Pontifícia Universidade Católica, mantiveram-se os princípios da edição anterior[1], com forte interação entre empresas, desenvolvedores, usuários e governo. O setor público, representado em estandes da Casa Civil, Banco do Brasil, Caixa Econômica Federal, Serpro, Dataprev, Prefeitura Municipal de Porto Alegre e Correios, entre outros, também marcou presença do

Figura 1 Knut Yrvin exibe o *QTopia Greenphone*.

Quadro 1: Entrevista com Knut Yrvin, gerente de comunidades da Trolltech

Linux Magazine» ***A Nokia utiliza a biblioteca GTK na maioria de seus projetos embarcados. Como deve ocorrer a harmonização das duas bibliotecas gráficas?***

Knut Yrvin» Os desenvolvedores das duas bibliotecas já sabem que precisam trabalhar em conjunto. Na conferência GUADEC, na Espanha, por exemplo, os desenvolvedores do KDE e do GNOME perceberam que, isolados, não atrairiam um público suficiente para uma conferência sobre apenas o seu ambiente. Resolveram, então, unir suas conferências em uma única, na qual compartilham idéias e código, beneficiando ambos os públicos.

LM» ***Qual o valor que a Nokia enxerga na Trolltech?***

KY» A Nokia tem uma estratégia multiplataforma, não apenas para telefones, mas também destinada a desktops. A estratégia de negócios da Trolltech é totalmente diferente, com 5 mil clientes pagantes e 15 mil usuários comerciais. O que a Trolltech pode levar para a Nokia

é essa percepção de que é possível praticar os dois modelos de negócios: o do Software Livre e o comercial. Parece-me que a Nokia gosta dessa possibilidade.

LM» ***Durante a última Bossa Conference, várias palestras exibiram as bibliotecas do Enlightenment rodando com ótimo desempenho nos sistemas embarcados. Essas bibliotecas seriam, então, a concorrência para a Qt?***

KY» O peso de um aplicativo depende do número de bibliotecas que ele carrega na memória. O ambiente Qtopia pode consumir, hoje em dia, míseros 16 MB de RAM. Além disso, ele usa o *framebuffer* diretamente, o que elimina a necessidade de uma camada intermediária no vídeo.

Para a Nokia, é muito importante o foco em economia de recursos de hardware, pois eles reduzem o preço final do dispositivo, e a Nokia vem crescendo mais justamente nos mercados em que o custo é um fator importante, como o Brasil, por exemplo. E o que a Qt oferece é um ambiente que se encarrega do "encanamento" e oferece maior produtividade sem aumentar o consumo de memória.

LM» ***Que pontos podem melhorar para o Linux no mercado embarcado?***

KY» O principal segmento em que ele precisa melhorar para conquistar definitivamente esse mercado é o gerenciamento de energia. O telefone precisa ficar praticamente desligado quando o usuário não estiver fazendo algo. E sistemas que usam apenas um chip gastam bem menos do que aqueles que rodam, por exemplo, o kernel num chip, o processamento gráfico em outro e o restante do sistema num terceiro. Além disso, é necessário que o hardware e o kernel – os componentes de baixo nível – façam uma maior parte do trabalho de "encanamento", para que os softwares possam ser reduzidos e gastar menos recursos.

Confira a entrevista na íntegra no site da Linux Magazine[3].

Quadro 2: Entrevista com Fabio Tagnin, gerente de marketing de soluções da Intel do Brasil

Linux Magazine» ***Como está a evolução do ClassmatePC?***

Fabio Tagnin» Esse modelo em exposição aqui foi lançado há duas semanas em Xangai, na China. Ele está com ótima aceitação. Todos estão bem impressionados com o novo design e as novas opções que ele traz. Além da possibilidade de tela maior (8,9 polegadas), agora existe também uma versão com disco rígido, além da opção de um disco Flash maior que o anterior. A câmera embutida é outra adição à máquina, que agora passa a atender, além do mercado educacional, o segmento dos subnotebooks.

Inicialmente, a nova versão do Classmate será vendida no varejo somente na América do Norte, Europa e Austrália, sendo indicado para aplicações empresariais e para o que mais for de interesse do consumidor, é claro.

LM» ***Então o Classmate deixou de ser um projeto voltado à educação?***

FT» Ele deixou de ser voltado exclusivamente à área educacional. Na verdade, o segmento de netbooks não é voltado unicamente à educação. Embora a segunda geração do Classmate ainda seja recente, já estamos trabalhando na terceira.

LM» ***O avanço para outros mercados representa uma falha do segmento de educação?***

FT» Muito pelo contrário. Nosso movimento é motivado justamente pelo sucesso que tivemos na área educacional, antes intocada por um produto como o Classmate. Ficamos impressionados com a demanda por essa máquina no varejo e em outros mercados.

LM» ***Quais as suas previsões para o futuro do Classmate?***

FT» No início de 2009, teremos o lançamento de uma terceira versão da máquina. A segunda versão, recém-lançada, não será descontinuada – diferentemente da primeira geração, que será substituída por essa segunda. A terceira versão será uma máquina diferente, que não vai competir com a segunda, mas complementá-la.

LM» ***Quanto ao software, será mantida a parceria com a Metasys para prover o conteúdo educacional?***

FT» No mundo todo, temos trabalhado com diversas distribuições, e vamos manter a parceria com a Metasys no Brasil. Aqui mesmo no FISL, você pode encontrar o Classmate equipado com o Ubuntu e com o Mandriva. Na América Latina, há outras três ou quatro distribuições com quem estamos trabalhando (inclusive vendendo para governos e escolas privadas). Na Ásia e na Índia também estamos trabalhando com outras distribuições.

No Brasil, a Metasys foi a primeira a ser habilitada no computador, mas, com a demanda de outras distribuições e outros governos, isso mudou. E a Intel acredita nessa liberdade de cada um escolher a plataforma que deseja usar.

Confira a entrevista na íntegra no site da Linux Magazine[4].

Quadro 3: Entrevista com Sulamita Garcia, gerente de estratégia Linux para a América Latina da Intel

Linux Magazine» ***O que é o Moblin?***
Sulamita Garcia» A maneira mais simples de apresentarmos o Moblin é como se fosse uma distribuição Linux da Intel, bastante simplificada, destinada à nova geração de dispositivos para Internet (MIDs – *Mobile Internet Devices*). Ele é uma plataforma aberta e engloba vários outros projetos, além de ser todo de código aberto.

Há também uma interface muito simples – um emulador – para geração de uma imagem do sistema embarcado, facilitando a criação de aplicativos com todo um ambiente já pronto.

LM» ***O que exatamente é o concurso para desenvolvimento no Moblin?***
SG» O concurso é chamado de *Your Move*, levando à pergunta: "Qual seria o seu próximo movimento?". Ele tem como público-alvo os desenvolvedores de software, para darem idéias sobre o que gostariam de ver no Moblin, o que está faltando ou quais recursos ou aplicativos seriam muito interessantes de ter no aparelho. As idéias podem ser enviadas a partir de 12 de junho até 13 de julho e devem incluir, inicialmente, um rascunho da interface e das funcionalidades dos aplicativos.

No dia 17 de julho, as idéias mais interessantes serão escolhidas pelo público por meio de uma votação. As idéias mais votadas ganharão um MID com processador Atom e um prêmio equivalente a mil dólares.

Depois dessa etapa, os vencedores terão três meses para desenvolverem e implementarem essas idéias de fato. Ao final desse período, as idéias serão julgadas por uma equipe de especialistas. A melhor idéia ganhará uma passagem com acompanhante e estadia de uma semana para qualquer conferência Open Source no mundo, à escolha do ganhador.

O mais interessante é o fato de o Brasil estar no mapa de um concurso como esse, acompanhado apenas de China, Índia e EUA. Isso é um reconhecimento para a comunidade brasileira de desenvolvedores.

LM» ***Apesar disso, a Intel não tem desenvolvedores no Brasil. Isso não é contraditório?***
SG» Isso sempre depende do mercado local. A China, com mais de um bilhão de habitantes, gera negócios de bilhões de dólares. O Brasil está caminhando para se tornar o terceiro maior mercado mundial de computadores. No entanto, ainda não surgiu a necessidade de termos um grupo de engenheiros aqui.

Por exemplo, a equipe da Intel que trabalha no kernel é de 300 pessoas. Porém, quantos profissionais trabalham profissionalmente no kernel no Brasil? Aqui, temos uma comunidade de usuários muito grande, mas faltam desenvolvedores. Os eventos deveriam ter uma preocupação maior em formar mais profissionais para termos quem contratar.

LM» ***E a Intel tem iniciativas nesse sentido?***
SG» Sim. Na Argentina, por exemplo, uma equipe da Intel ofereceu um curso de reciclagem para professores universitários da área de computação, com o objetivo de atualizá-los na programação multi-core. No Brasil também há programas específicos de capacitação de professores de computação para ensinar a seus alunos programação paralela para processadores de múltiplos núcleos.

LM» ***Como você avalia a relação da Intel com a comunidade brasileira de usuários Linux?***
SG» Acho interessante a Intel trazer para a comunidade o pensamento de que o objetivo, ao participar de um evento como o FISL, não é apenas participar, mas agregar valor. Ou seja, a empresa não comparece simplesmente com patrocínio, mas também com código, documentação e treinamento. Acho que é uma relação que beneficia ambos os lados.

Confira a entrevista na íntegra no site da Linux Magazine[5].

lado de dentro das salas. No evento, ocorreu o terceiro encontro da comunidade CACIC, a exemplo das últimas edições. O Portal do Software Público[2], que abriga o CACIC e outros 11 softwares de Código Aberto, recebeu dois novos integrantes durante o FISL 9.0: o *Sagui* (Sistema de Apoio à Gerência Unificada de Informações), desenvolvido pelo Serpro, e o sistema bilhetador de impressão *Curupira*, criado pela Caixa Econômica Federal.

Como de costume, a parte do pavilhão dedicada aos grupos de usuários foi freqüentada por diversos desenvolvedores, usuários e entusiastas. Seu público constantemente em movimento justifica a denominação de Fórum ao evento, e a área é palco de alguns avanços em distribuições e softwares específicos.

Evento internacional

As empresas internacionais, embora não muito numerosas, foram responsáveis por alguns importantes anúncios durante essa edição do FISL. A norueguesa Trolltech, desenvolvedora da biblioteca gráfica

de Código Aberto *Qt* – parte fundamental do projeto KDE –, demonstrava seu aparelho celular verde, o Green Phone. Completamente de código aberto, o Green Phone utiliza a interface gráfica *Qtopia*, desenvolvida pela Trolltech para sistemas embarcados. O celular não é comercializado no Brasil, mas, em conversa com a Linux Magazine, o gerente de comunidades da empresa Knut Yrvin afirmou que isso talvez aconteça. Além disso, Knut falou sobre a aquisição da Trolltech pela finlandesa Nokia no início de 2008 (**quadro 1**).

A Intel, com um dos mais sofisticados estandes do pavilhão, demonstrou a nova geração do ClassmatePC, que deixa de ser voltado unicamente à educação e se lança no mercado geral de subnotebooks (**quadro 2**). Além disso, a empresa demonstrou em várias palestras seu envolvimento com a comunidade do Código Aberto, muito maior que no passado e incluindo grandes quantidades de código (**quadro 3**).

Figura 2 Como nas edições passadas, um grande número de usuários e desenvolvedores compareceu ao FISL.

Encontro de empresas

Anúncios de parcerias não faltaram em Porto Alegre. A própria Intel divulgou sua parceria com a Dataprev para suporte do CACIC, o software público de maior fama no portal brasileiro, à tecnologia *vPro* de gerenciamento de hardware e software. A sul-africana Canonical também anunciou uma parceria com a Intel para melhor suporte entre o sistema operacional da primeira – o Ubuntu – e o hardware da segunda.

Fora os anúncios públicos, o FISL foi palco de inúmeras reuniões de negócios, detectadas pelas eventuais concentrações de pessoas no interior dos estandes, a portas fechadas.

Figura 3 O estande da Intel, com um exemplar do novo Classemate PC, atraiu um grande público, contando também com sorteio de brindes.

FISL 10

A próxima edição do FISL, de número dez, terá a ousada meta de contar com dez mil participantes. A campanha para aumentar ainda mais o número de pessoas no evento será lançada, provavelmente, apenas alguns meses antes do início do evento. Se seguir a tendência das últimas edições, podemos esperar para 2009 um evento recordista em participação. ■

Mais informações

[1] Pablo Hess, "FISL 8.0": http://www.linuxnewmedia.com.br/article/fisl_80

[2] Portal do Software Público: http://www.softwarepublico.gov.br/

[3] Entrevista com Knut Yrvin: http://www.linuxmagazine.com.br/noticia/1887

[4] Entrevista com Fabio Tagnin: http://www.linuxmagazine.com.br/noticia/1888

[5] Entrevista com Sulamita Garcia: http://www.linuxmagazine.com.br/noticia/1889

Integrações simplificadas por meio do REST

Edgar Silva

A era dos Jetsons já começou – e o REST tem um importante papel nisso.

por Edgar Silva

O modelo de *Web Services* é vitorioso frente a outros do passado. O fato de utilizar o formato XML como a definição dos serviços é uma escolha muito boa. Hoje, porém, é possível termos modelos extremamente elaborados quando falamos de serviços web, que variam em forma de processamento (síncrono ou assíncrono), suporte a anexos e várias aberturas para definições complexas, que permitem o intercâmbio entre tecnologias como *Java* e *.Net*, por exemplo.

Porém, quando precisamos de algo mais simples, ainda assim somos obrigados a usar todo o modelo de Web Services. Eis, então, que o padrão REST (*Representational State Transfer*) chega ao mercado. O REST é, em resumo, uma forma de expor serviços por meio do protocolo HTTP – o mesmo usado em Web Services – com uma forma diferente de definição de serviços. Enquanto no modelo mais antigo as operações permanecem em seu endereço (URI), no REST suas operações são oferecidas por meio do WSDL (*Web Services Definition Language*).

No exemplo `http://site/rest/solicitaorcamento/XXXX`, temos um serviço chamado *solicitaorcamento* que funciona como um verbo. Sendo assim, solicita-se o orçamento com base na última informação do endereço. Ou seja, essa URI diz "solicite o orçamento do produto XXXX".

O interessante é que, ao digitar isso num navegador, é você quem escolhe qual o retorno. Por padrão, ao digitar o endereço no navegador, faz-se uma conexão pelo método *GET* no protocolo HTTP. Se a operação for feita por um navegador, o retorno mais natural pode ser um arquivo HTML, ou os dados podem ser retornados no formato JSON e renderizados por técnicas do Ajax, proporcionando uma experiência rica para o usuário.

Entretanto, se a necessidade for outra, o resultado pode ser um arquivo XML com validação de *schemas* para permitir o intercâmbio com qualquer tecnologia que suporte XML. Ou, se for preferível, pode-se até mesmo retornar um arquivo de texto puro. Afinal, cabe a quem oferece o serviço definir seu protocolo.

Ao utilizar o REST, é muito comum esperar que os serviços respondam por meio de um simples servidor web. Portanto, construir serviços em *PHP*, *Python*, *Ruby* e expor tudo por meio de um simples servidor web Apache pode ser trivial. E já que o HTTP pode ser conectado como um socket TCP/IP, criar um cliente em Java ou até em *Delphi* seria também algo fácil.

Alguns candidatos para serviços REST são aplicativos móveis que precisam de simplicidade nos dados de retorno, serviços sem a necessidade de manter estado de comunicação (*stateless*) e serviços que podem ter caráter público, como os voltados a consumidores que criam pequenas aplicações (widgets) para usuários.

O REST é uma forma não tão nova de integrar sistemas. Por intermédio de um barramento de serviços (ESB), por exemplo, pode-se expor serviços por esse formato e aproveitar sua capacidade de transformação de dados.

SOA e Web 2.0 muitas vezes podem estar juntos, a exemplo de vários provedores de serviços, como del.icio.us, Flickr, Ning, Facebook etc., que já expõem alguns de seus serviços em REST, objetivando trazer maior imersão comercial em serviços que anteriormente pareciam um simples "fotolog".

Entretanto, por meio dessas possibilidades, uma gráfica pode oferecer serviços de impressão e entrega de fotos, bastando que você informe seu álbum num quiosque ou no balcão da gráfica. De fato, já vivemos a era dos Jetsons. ■

Sobre o autor

Edgar Silva (`edgar.silva@redhat.com`) é Arquiteto de Soluções JBoss na Red Hat Brasil. Com experiência em objetos distribuídos (Corba, COM+ e Java) desde 1998, nos últimos anos Edgar vem pesquisando, aplicando e ministrando palestras e treinamentos no Brasil e no exterior sobre assuntos de alta tecnologia, incluindo JavaEE e SOA.

A consolidação do movimento Open Source

Cezar Taurion

Estudos revelam a forte participação de grandes empresas no crescimento do Linux e do Código Aberto.

por Cezar Taurion

Em abril tivemos o FISL 9.0, um importante evento no qual tive uma boa idéia da evolução da avançada maturidade do movimento Open Source e do Linux. Esses termos não são mais novidades estranhas às corporações e estão rapidamente se inserindo no *mainstream* corporativo.

Um recente relatório publicado pela IDC, intitulado "The Role of Linux Servers and Commercial Workloads", mostra alguns números bem interessantes, como o que demonstra a solidez do ecossistema de negócios em torno do Linux (hardware, software e serviços). Este totalizou US$ 21 bilhões em 2007 e deve crescer até 49 bilhões para 2011, principalmente pelo crescimento do Linux em servidores rodando aplicações comerciais como ERP, CRM, banco de dados e outras aplicações de negócio. O Linux não é mais apenas um nicho de workloads técnicos de infra-estrutura, como servidores de arquivos ou email, mas já faz parte do cerne das aplicações que movem os negócios das empresas.

O relatório da IDC aponta como principais oportunidades de serviços para esse ecossistema as atividades de migração, integração e implantação. Educação e treinamento são vistos como menor oportunidade, mas geralmente são os pontos de entrada para os serviços de maior valor agregado, como consultoria e integração. A IDC estima que esses serviços para Linux e Código Aberto deverão crescer acima da média do próprio mercado de serviços, e chama atenção para o fato de que as receitas de software em torno das plataformas Linux já somam 10 bilhões de dólares, cerca de 4% do total dessa indústria de US$ 242 bilhões. Estima-se que até 2011 essa porcentagem deva crescer para acima de 9%, representando US$ 31 bilhões de um mercado de 330 bilhões.

A Linux Foundation também publicou um relatório muito interessante, com números sobre o desenvolvimento do kernel, chamado "How Fast it is Going, Who is Doing It, What They are Doing, and Who is Sponsoring It". Analisando a atividade em torno do kernel, chegamos a uma impressionante estatística de que, a cada dia, 3621 novas linhas de código são adicionadas, 1150 são removidas e 1425 são modificadas.

Quem faz esse trabalho? Das versões 2.6.11 à 2.6.24 foram 3678 desenvolvedores autonômos ou contratados por uma dentre 271 companhias. Os dez contribuidores mais ativos ajudaram com quase 15% e os trinta mais, com cerca de 30%. Vemos também que, entre as empresas contribuidoras, a Red Hat aparece em primeiro lugar no número de contribuições, seguida por Novell e IBM. Entre as demais, vemos Intel, Oracle, Google e HP. O maior volume de contribuições ao kernel, quase 70%, vieram de desenvolvedores empregados por empresas, enquanto 26,8% vieram de colaborações individuais, sem patrocínio de empresas ou cujo empregador não pode ser identificado.

E já vemos também colaborações de empresas que antes não imaginávamos que pudessem contribuir, como a Volkswagen, que contribuiu para o kernel 2.6.25 com a implementação do protocolo *PF_CAN* para comunicações em ambientes que sofrem fortes interferências, como automóveis.

A conclusão disso tudo é que o Linux é, sem sombra de dúvida, um excelente sistema operacional e um dos mais bem sucedidos exemplos de projetos Open Source. Sua comunidade é vibrante e demonstra de forma inequívoca que colaboradores individuais e empresas podem criar uma comunidade com ampla sinergia. Desenvolvimento colaborativo por excelência. Definitivamente, Linux não é obra de hobistas, mas de desenvolvedores competentes. ■

Sobre o autor

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: www-03.ibm.com/developerworks/blogs/page/ctaurion

O máximo da disponibilidade

Sempre alerta

Para obter alta disponibilidade, é necessário investir tempo de planejamento e dinheiro. Por isso, é bom saber como fazer.

por Fernando Ike

Alta disponibilidade aparentemente é um assunto que não desperta grandes discussões, pois, até o momento, existe um consenso em relação à necessidade de implementação desse recurso em diversas áreas. Consenso que, para muitos entusiastas do Software Livre, resume-se ao *Heartbeat*; porém, na realidade, engloba muitos outros aspectos.

A alta disponibilidade é um sistema tolerante a qualquer tipo de falha, seja ela de equipamento, energia elétrica, software etc. Esse tipo de sistema busca diminuir ou eliminar os pontos únicos de falhas, podendo utilizar redundância de nós de ativos de rede (switches, roteadores etc.), servidores de aplicação, servidores de banco de dados, geradores de energia e outros. Para manter a maior disponibilidade possível, costuma-se escolher áreas geográficas de baixa incidência de desastres naturais, como terremotos, furacões e inundações, por exemplo, além de se ter dois ou mais datacenters.

Pensar em alta disponibilidade é tão importante que pode significar a falência ou a permanência de uma empresa. No atentado de 2001 ao World Trade Center aconteceram, em Nova York , dois casos notórios da importância do planejamento em alta disponibilidade:

- uma corretora de seguros tinha seu datacenter em uma das torres e sua réplica na outra torre. Não imaginaram que a segunda torre cairia, mas infelizmente foi o que aconteceu;
- uma instituição bancária também tinha seu datacenter em uma das torres, mas sua réplica estava a alguns quilômetros dali. Nesse banco, houve apenas uma leve indisponibilidade do sistema corporativo, até que o segundo datacenter estivesse em plena operação.

Para medir a disponibilidade, basicamente usa-se uma fórmula: disponibilidade = tempo médio entre falhas / (tempo médio entre falhas + tempo médio de recuperação). Na maioria dos casos, os valores das variáveis são projetados por meio de estimativas, mas a validação do valor da disponibilidade somente é feita quando acontece algum incidente, provando a disponibilidade do sistema.

Geralmente, quando uma empresa pede a uma equipe de TI o desenvolvimento de um projeto de manutenção do sistema corporativo, a primeira informação que a equipe deve perseguir é o nível de disponibilidade. Nesse momento, é apresentada

uma pequena tabela com os famosos noves. A projeção de custo é: quanto mais disponível for um sistema, mais cara será a solução. Em qualquer cálculo de disponibilidade, não são contabilizadas as paradas programadas para manutenção, instalação ou atualização de um sistema ou parte dele. Entretanto, é importante calcular o valor absoluto da indisponibilidade, pois, embora 99% pareça um bom número, uma disponibilidade com esse valor significa que o sistema ficará indisponível durante 87,5 horas por ano – inaceitável para muitos negócios. Alguns valores de disponibilidade:

- 99%: 87,5 horas por ano;
- 99,9%: 8,76 horas/ano;
- 99,99%: 52,6 minutos/ano;
- 99,999%: 5,26 minutos/ano.

Apesar de cinco noves (99,999%) de disponibilidade serem um bom valor, em algumas empresas o custo de uma solução assim pode se tornar inviável. Ainda assim, é possível propor soluções pensando numa disponibilidade menor ou em partes importantes de um sistema, como um servidor de aplicação ou banco de dados.

Existem muitas soluções para garantir a continuidade de partes dos componentes de um sistema, como equipamentos de rede, armazenamento, energia elétrica e os próprios servidores. Ao olharmos para a parte da aplicação, dependendo de como a aplicação é construída, também existe uma grande variadade de opções.

Planejamento

Ao pensar em disponibilidade, o planejamento é um tanto complexo e freqüentemente menosprezado. Para se ter uma idéia, na área de bancos de dados, as etapas do planejamento são:

- análise do tipo de aplicação e modelagem do banco de dados;
- política de becape e restauração: becape completo, por logs binários ou cópia física;
- tempo de recuperação de um desastre;
- sincronicidade da replicação dos dados;
- volume de dados replicados (megabytes, gigabytes, terabytes...);
- tipo de interconexão de rede entre as bases de dados: fibra ótica, *frame relay*, ATM, ADSL, conexão serial;
- arquitetura da aplicação (suporte a múltiplos bancos de dados);

A virtualização também tem sido muito usada em soluções de alta disponibilidade. Nesta edição, o especialista Marco Sinhoreli explica o uso do *Xen* sobre hospedeiros espelhados como solução de alta disponibilidade, explicando também como criar a infra-estrutura de rede adequada a esse uso. Além disso, a gestão da disponibilidade é abordada por um profissional experiente na área. ■

Índice das matérias de capa

Armazenamento com alta disponibilidade

Os dados não param

Planeje seu servidor de armazenamento e sua infra-estrutura de redes para oferecer alta disponibilidade com alto desempenho.

por Marco Sinhoreli

Os sistemas atuais são sedentos por dados. Servidores de email corporativos precisam cada vez mais de espaço para armazenar mensagens em HTML com figuras, enquanto servidores Web acessam bancos de dados que gerenciam terabytes de informação, e a prática do *data mining* vê cada vez mais uso em aplicações de negócios.

Com toda essa dependência, qualquer parada no acesso aos dados é potencialmente muito prejudicial. Então, como impedimos a falha no acesso aos dados? Em primeiro lugar, há de se fazer um mapeamento dos pontos de falha no servidor de armazenamento.

A **tabela 1** indica os possíveis pontos de falha em um servidor e o que deveria ser considerado em nosso planejamento para nos anteciparmos a um futuro desastre.

Especialista ou genérico?

Alguns dos itens citados na **tabela 1** podem ser resolvidos com a compra de servidores especializados. Pensando em reduzir custos, caso a aquisição da solução de armazenamento externo (NAS[1], SAN[2] ou FC[3]) seja demasiadamente cara para o projeto em questão, uma solução intermediária e igualmente competente seria a aquisição de um servidor com uma controladora SAS com discos de 15.000 RPM ou SATA II (7.200 RPM) com suporte a *RAID 10* e *hot swap* para fazer o papel do NAS.

Outra solução de baixíssimo custo seria o emprego de RAID via software, associado ao uso de *DRBD* sobre discos SCSI ou SATA; em contrapartida, isso comprometeria o desempenho, dadas as diversas camadas existentes para o acesso aos dados no disco.

Rede unida

Para prover acesso constante aos dados pela rede, é importante garantir que a própria conexão de rede não seja parada. Nesse intuito, a **tabela 1** sugere o uso de múltiplas interfaces de rede no servidor.

O módulo do Linux para a união de canais Ethernet se chama *bonding*. Esse módulo disponibiliza um método para agregação de múltiplas interfaces de rede em uma única interface lógica (chamada de *bond*). O comportamento de interfaces bond depende do modo como são configuradas.

Modos

Existem sete modos disponíveis no módulo para Linux, numerados de 0 a 6. Como se pode imaginar, cada um dos modos possui um propósito diferente dos demais, com as interfaces de rede envolvidas (chamadas de *escravas* ou *portas*) comportando-se de forma diferente, o que oferece uma ampla gama de possibilidades para seu uso.

O modo de operação escolhido deve ser passado para o módulo do kernel no momento de seu carregamento. Por exemplo, se desejássemos utilizar um hipotético modo 9, deveríamos carregar o módulo com o seguinte comando:

```
modprobe bonding mode=9
```

No modo 0 (*balance-rr* ou *round-robin*), o sistema transmite pacotes em ordem seqüencial do primeiro dispositivo escravo disponível até o último. Esse modo disponibiliza

Tabela 1: Problemas e soluções de hardware

Falha de hardware possível	Solução
Fonte de alimentação	Uso de servidor com fonte redundante.
Disco	Uso de RAID 10 ou 1 via software ou hardware, ou aquisição de um SAN.
Rede	Uso de bonding com mais de uma interface de rede para cada bridge.
Falha completa do servidor (memória, processador, mobo)	Redundância do servidor.

balanceamento de carga e tolerância a falhas.

No modo 1 (*active-backup*), somente um escravo do bond fica ativo. Outros dispositivos escravos somente serão ativados (e apenas um deles) se o escravo ativo falhar. O endereço MAC do bond é visível, externamente, por meio de apenas uma porta, para evitar confundir o switch, ligado à outra ponta do cabo de rede. Esse modo oferece tolerância a falhas e é afetado pela opção *primary* (descrita adiante).

No modo 2 (*balance-xor*), a transmissão é baseada na política de *hash* selecionada e no operador booleano XOR[4]. A política padrão é simples:

(origem XOR destino) % número_de_slaves

Esse modo seleciona a mesma interface escrava para cada endereço MAC de destino e oferece balanceamento de carga e tolerância a falhas.

O modo 3 (*broadcast*) transmite todo o tráfego sobre todas as interfaces escravas, oferecendo, assim, tolerância a falhas.

O modo 4 (*802.3ad*, ou *dynamic link aggregation*) cria (agrega) grupos de interfaces que compartilham as configurações de velocidade e duplex. Ele utiliza todas as interfaces escravas no agregador ativo, de acordo com a especificação 802.3ad, e tem os seguintes pré-requisitos:

- suporte ao *Ethertool* nos drivers dos dispositivos para obter a velocidade e a função duplex em cada interface escrava;
- um switch com suporte a IEEE 802.3ad. A maioria dos switches precisam ser configurados especificamente para ativar o suporte ao modo 802.3ad.

O modo 5 (*balance-tlb*, ou *adaptive transmit load balancing*), estabelece um canal de bonding que não requer qualquer suporte especial por parte do switch. O tráfego de saída é distribuído de acordo com a carga sobre a interface escrava atual. O de entrada é recebido pela interface escrava atual. Se a interface escrava receptora falhar, outra interface escrava adquire o endereço MAC daquela defeituosa. Assim como o modo 4, este também tem como pré-requisito o suporte ao Ethertool, porém, somente para obter a velocidade de cada interface escrava.

O modo 6 (*balance-alb*, ou *adaptive load balancing*) inclui o balanceamento de carga de transmissão (*transmit load balancing*, ou *tlb*) com balanceamento também na recepção (*receive load balancing*, ou *rlb*) para tráfego IPv4, e não requer qualquer suporte especial por parte do switch. O rlb é realizado por meio da negociação ARP. O driver *bonding* intercepta a resposta ARP enviada pelo sistema local em sua saída e reescreve o endereço do hardware de origem com um único endereço de hardware de uma das interfaces escravas do bond para que pares diferentes usem endereços físicos distintos para o servidor.

Acesso aos dados

O site Linuxdevices[5] comparou as opções de protocolos que implementam uma SAN sobre Linux (*AoE*[6] e *iSCSI*[7]), e o novato AoE se mostrou bastante capaz. O AoE é uma alternativa rápida e barata para SANs iSCSI e *Fiber Channel*. O iSCSI utiliza o TCP/IP como transporte para disponibilizar dispositivos remotos de armazenamento.

O AoE, por sua vez, não é um protocolo roteável, pois funciona na camada Ethernet (camada 2). Ele não inclui as complexidades do protocolo TCP/IP para roteamento, como faz o iSCSI. O protocolo AoE é muito mais simples do que o iSCSI, como mostra o diagrama da **figura 1**, e é nativamente suportado pelo Linux desde a versão 2.6.11.

Mãos à obra

Vamos agora construir um servidor dedicado ao armazenamento NAS (cujo hostname é *nas*). Em seguida, configuraremos o acesso a esses dados via AoE em duas máquinas clientes.

Nosso servidor terá quatro interfaces de rede (`eth0` a `eth3`) agregadas sob o modo 4 (802.3ad) do módulo *bonding* em uma única interface lógica, `bond0`. Além delas, outras duas (`eth4` e `eth5`) serão usadas numa segunda interface lógica, `bond1`, que será destinada à administração e ao acesso aos serviços pela LAN.

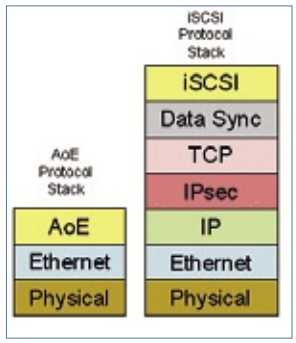


Figura 1 O protocolo AoE é significativamente mais simples que o iSCSI.

Além da transmissão de dados pelo servidor, precisamos considerar a possibilidade de falhas no meio do caminho de transmissão, ou

seja, no switch. Para resolver essa questão de *failover*, a aquisição de switches com *stacking* e suporte a 802.3ad deverá ser considerada. A sugestão, neste artigo, é de dois switches com suporte a 802.3ad, evidentemente, e conectados, cada um, a duas interfaces de rede do servidor. Ou seja, as interfaces `eth0` e `eth1` se conectam ao switch 1, enquanto `eth2` e `eth3` são ligadas ao switch 2. Ambos os switches permanecerão ativos e conectados por stacking. O stacking, por sua vez, também deverá ter suporte a 802.3ad, o qual deverá estar ativo.

É interessante também separar seis portas de cada switch para uma VLAN dedicada ao tráfego do SAN. Uma segunda VLAN também deve ser criada para se comunicar com a LAN, reservando três portas em cada switch para a `bond1` do servidor composta pelas interfaces `eth4` e `eth5`, com a `eth4` de cada servidor sendo ligada ao switch 1 e a `eth5` ao switch 2.

Especificações do NAS

A opção pelo AoE se mostra melhor do que pelo iSCSI. Por ser menos complexa, ter uma carga de processamento muito inferior e oferecer o mesmo *throughput*, além de possibilitar o isolamento na camada Ethernet (lembre-se de que o AoE não é roteável), e também pelo fato de que o AoE passa por qualquer tipo de switch, a opção por ele é a mais desejável. Com isso, não será necessário um hardware com grande poder de processamento.

Um dado de que necessitamos é o volume de tráfego de entrada e saída de dados entre o armazenamento e os hospedeiros. Essa variável depende da demanda dos sistemas clientes e do servidor. Neste artigo, consideramos um throughput alto de entrada e saída de dados, acompanhado do uso de múltiplas interfaces Gigabit Ethernet. Por isso, vamos precisar também de discos velozes com RAID via hardware para maior garantia contra falhas. Discos hot swap também são aconselhados, assim como fontes de alimentação redundantes.

Com vista nesses aspectos, um servidor básico que atenda as necessidades projetadas neste artigo teria, atualmente, os seguintes componentes físicos:

- processador Intel Core 2 Duo ou superior;
- 1 GB de memória;
- controladora SATA com suporte a RAID 10;
- seis interfaces Gigabit ethernet (quatro para `bond0` – *802.3ad* – e duas para `bond1` – *active-backup*);
- dez discos SATA de 500 GB, fornecendo 2,5 TB em RAID 10, hot swap.

Essa configuração visa a ser apenas uma base para nosso sistema de armazenamento. Em projetos reais, evidentemente, a quantidade de discos necessários vai variar. Para melhor desempenho, vale a pena trocar os discos e sua controladora pela tecnologia SAS. Discos hot swap se justificam, em nosso modelo, para que não ocorram paradas em caso de falha de um dos discos, já que, em nosso caso, todos os clientes utilizarão esse servidor de armazenamento.

Configuração do NAS

Montado o servidor, já podemos configurá-lo. Como primeira providência, é necessário ativar o RAID 10 para todos os discos, o que deve ser descrito no manual da máquina. No caso de se optar por uma solução sem RAID via hardware, a configuração do RAID (nível 1 caso o nível 10 não esteja disponível) deve ser feita na instalação do sistema operacional. O nível 0 (zero) não deve ser usado, pois multiplica a probabilidade de falhas e não oferece qualquer redundância. Geralmente é suficiente alocar cerca de 20 GB para o sistema operacional e 1 GB para swap, enquanto o restante pode ser exportado para os clientes via AoE.

Como nosso objetivo é agregar o link das interfaces de rede no modo 4, é necessário que o driver das placas de rede ofereça suporte a Ethertool. Além disso, precisaremos habilitar no switch o suporte ao modo *802.3ad*.

Um detalhe importante, com relação ao switch, é a separação do tráfego dos dados entre a `bond0` e a `bond1`, para segurança do storage. A interface `bond1` servirá somente para administração do servidor a partir da LAN e deverá estar em uma VLAN ou em switches separados das interfaces que compõem a `bond0`, como explicado anteriormente.

Software

Com todos esses itens contemplados, basta instalar o pacote *ifenslave* (*ifenslave-2.6*, no Debian), que contém a ferramenta para agrupar e desagrupar interfaces de rede na interface bond lógica. Para carregar o módulo *bonding* na inicialização do sistema, deve-se inserir algumas linhas no arquivo `/etc/modprobe.d/arch-aliases`, conforme o **exemplo 1**. Em seguida,

Exemplo 1: Arquivo /etc/modprobe.d/arch-aliases

```
01 alias bond0 bonding
02 options bond0 mode=4 miimon=100 downdelay=200 updelay=200
03 alias bond1 bonding
04 options bond1 mode=4 miimon=100 downdelay=200 updelay=200
05 options bonding max_bonds=2
```

o comando `update-modules` efetiva as configurações. Por último, basta carregar o módulo *bonding* (`modprobe bonding`) para prosseguir com a configuração.

Os parâmetros que podem ser usados para o módulo bonding são:

- `max_bonds`: número máximo de dispositivos bond;
- `use_carrier`: usar o `netif_carrier_ok` (em vez dos *ioctls MII*) no *miimon*. `0` para desativar e `1` para ativar (padrão);
- `primary=ethX`: interface primária para uso;
- `lacp_rate=[slow/fast]`: taxa de transmissão LACPDU para requisição 802.3ad;
- `xmit_hash_policy`: método de hashing XOR. `0` para camada 2 (padrão), `1` para camadas 3+4;
- `arp_interval`: intervalo ARP em milissegundos;
- `arp_ip_target=n.n.n.n`: alvo ARP (origem);
- `arp_validate=[none (padrão), active, backup ou all]`: validar origem ou destino do ARP.

Agregando

Para que os links das interfaces `eth0`, `eth1`, `eth2` e `eth3` sejam agregados em um único dispositivo — no nosso caso, a interface lógica `bond0` — e os links da `eth4` e da `eth5` sejam unidos na interface lógica `bond1`, é preciso alterar o arquivo `/etc/network/interfaces` de acordo com o **exemplo 2**, além de configurar os endereços das interfaces do servidor NAS de acordo com a **tabela 2**. Feitas as alterações, precisamos apenas reiniciar o serviço de rede:

```
# invoke-rc.d networking restart
```

AoE

O *aoe* é um módulo do kernel Linux que disponibiliza a comunicação pelo protocolo AoE (ATA sobre Ethernet). Para o servidor utilizar o protocolo, é necessário carregar o módulo com o comando `modprobe aoe`. Para carregar o módulo automaticamente na inicialização, basta acrescentá-lo ao arquivo `/etc/modules`.

Exemplo 2: Arquivo /etc/network/interfaces

```
01 auto lo
02 iface lo inet loopback
03
04 auto bond0
05 iface bond0 inet static
06   pre-up modprobe bond0
07   address 192.168.1.4
08   netmask 255.255.255.0
09   network 192.168.1.0
10   broadcast 192.168.1.255
11   slaves eth0 eth1 eth2 eth3
12
13 auto bond1
14 iface bond1 inet static
15   pre-up modprobe bond1
16   address 192.168.0.101
17   netmask 255.255.255.0
18   network 192.168.0.0
19   broadcast 192.168.0.255
20   gateway 192.168.0.1
21   dns-nameservers 192.168.0.254
22   dns-search domain.net
23   slaves eth4 eth5
```

Vblade

O pacote *vblade* é utilizado para criar e gerenciar os dispositivos AoE exportados. Neste artigo, consideramos o uso de LVM no dispositivo `/dev/sda4`, com o volume físico LVM tendo sido criado durante a instalação. Precisaremos, então, ativar o LVM e criar um grupo de volumes (VG). Em seguida, para cada cliente, precisaremos de um volume lógico para a raiz do sistema e outro para swap. Os comandos `pvcreate` e `vgcreate` criam o volume físico (PV) e o grupo de volumes (VG), respectivamente:

```
# pvcreate /dev/sda4
# vgcreate /dev/sda4 storagevg
```

Considerando um conjunto hipotético de três clientes, cada um com sua necessidade de disco e de memória, precisaremos criar os volumes lógicos para a raiz e a swap de cada um desses clientes. Para o swap, podemos considerar um volume lógico (LV) do mesmo tamanho que a quantidade de memória do cliente.

Portanto, se desejarmos exportar 500 GB de disco e 2 GB de swap para cada cliente, os comandos serão:

```
# for cl in cl1 cl2 cl3; do
> lvcreate -L 500G -n ${cl}.dsk
➥ storagevg
> lvcreate -L 2G -n ${cl}.swp
➥ storagevg
```

Em seguida, é interessante automatizar a exportação dos volumes lógicos por AoE a cada inicialização. Para isso, vamos preparar um script no arquivo `/etc/rc.local` de acordo com o **exemplo 3**.

Tabela 2: Configuração dos dispositivos de rede

Interface bond	bond0	bond1
Pool de interfaces	eth[0,1,2,3]	eth[4,5]
Endereço IP	192.168.100.1	192.168.0.101
Tipo de bonding	*Dynamic link aggregation*	*Active-backup*
Rede	NAS	LAN

Exemplo 3: Script para exportação via AoE

```
01 #! /bin/bash
02 VG="storagevg"
03 LVS=(cliente1.dsk cliente1.swp cliente2.dsk cliente2.swp cliente3.dsk
   ➥ cliente3.swp)
04 IFACE=bond0
05 part=0
06 numvm=1
07 for ((count=0;count<${#LVS[@]};count++)); do
08   let part++
09   if [ $part -ge 3 ]; then
10     part=1
11     let numvm++
12   fi
13   vbladed $numvm $part $IFACE /dev/$VG/{LVS[$count]}
14 done
```

E os clientes?

O pacote *aoetools* é um conjunto de ferramentas para clientes AoE, feito para auxiliar na configuração de dispositivos AoE exportados na camada Ethernet. Esse pacote é projetado para funcionar sobre o driver *aoe* do kernel. As ferramentas que compõem o pacote são:

- *aoe-discover*: inicia a descoberta de dispositivos AoE na camada Ethernet;
- *aoe-interfaces*: restringe buscas de AoE somente à interface indicada;
- *aoe-mkdevs*: cria dispositivos de caractere e de bloco;
- *aoe-mkshelf*: cria arquivos de dispositivo de bloco para uma lista de endereços;
- *aoe-stat*: exibe informações de status de dispositivos AoE;
- *aoeping*: aplicativo de comunicação com dispositivos AoE;
- *aoe-revalidate*: revalida o tamanho do *doscp* de um dispositivo AoE.

Executando nos clientes o comando `aoe-discover`, todos os volumes lógicos exportados pelo servidor já se tornarão visíveis. Como resultado, cada um dos volumes exportados será automaticamente representado por um dispositivo sob o diretório `/dev/etherd/`. Por fim, basta que cada cliente defina o dispositivo de blocos adequado como sua raiz e partição swap, de acordo com a **tabela 3**.

Conclusão

A criação de um servidor de armazenamento para fornecer dados via rede com alto desempenho e alta disponibilidade não é complicada. O uso do protocolo AoE garante a velocidade, dentre outras vantagens sobre o "concorrente" iSCSI.

A infra-estrutura de rede, do servidor e dos clientes proposta neste artigo garante a alta disponibilidade dos dados. No entanto, receber os dados da partição raiz via rede é um procedimento mais adequado a máquinas virtuais, cujo dispositivo de armazenamento, mesmo que seja externo, estará disponível antes mesmo do carregamento do kernel.

Acompanhe, no artigo **Substituto Virtual**, na página 37 desta edição, o uso dessa estrutura na configuração de um sistema de servidores virtuais. ■

Tabela 3: Dispositivos de bloco nos clientes

Cliente	Dispositivo de blocos raiz	Dispositivo de blocos swap
Cliente1	/dev/etherd/e1.1	/dev/etherd/e1.2
Cliente2	/dev/etherd/e2.1	/dev/etherd/e2.2
Cliente3	/dev/etherd/e3.1	/dev/etherd/e3.2

Mais informações

[1] Network Attached Storage: http://en.wikipedia.org/wiki/Network_Attached_Storage

[2] Storage Area Network: http://en.wikipedia.org/wiki/Storage_Area_Network

[3] Fiber Channel: http://en.wikipedia.org/wiki/Fibre_Channel

[4] XOR: http://pt.wikipedia.org/wiki/XOR

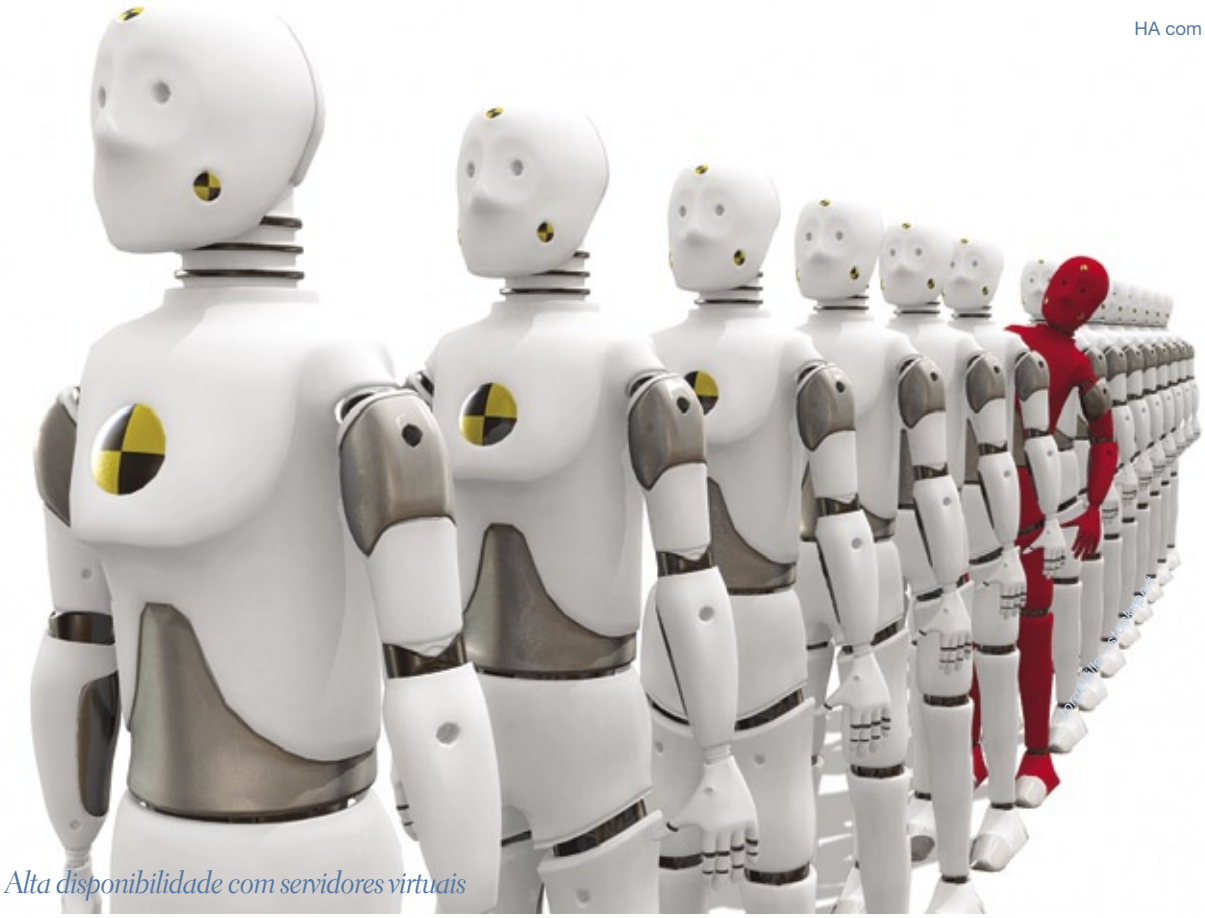
[5] Artigo no LinuxDevices: http://www.linuxdevices.com/news/NS3189760067.html

[6] ATA sobre Ethernet: http://www.coraid.com/support/linux/EtherDrive-2.6-HOWTO.html

[7] iSCSI: http://www.open-iscsi.org/index.html

Sobre o autor

Marco Sinhoreli (msinhore@gmail.com) trabalha com Xen há três anos. É co-mantenedor do pacote *ibvirt* no Debian, fundador do grupo de usuários Xen-BR e trabalha no provedor de Internet Orolix, onde gerencia cerca de 180 máquinas virtuais Xen. Inclusive, jamais teria conseguido escrever este artigo sem as valiosas dicas de Luiz Ricardo Malheiros e Liberie da Cunha Neto.



Alta disponibilidade com servidores virtuais

Substituto virtual

Associado a uma infra-estrutura de rede e armazenamento de alta disponibilidade, o Xen permite a criação de servidores com alto desempenho.

por Marco Sinhoreli

A tecnologia da virtualização é mais do que uma moda recente, pois não é moda, nem recente. Na busca da alta disponibilidade, sistemas virtuais podem ser de grande ajuda na aplicação de balanceamento de carga ou *failover*, pois podem ser migrados de um hospedeiro para outro com facilidade.

Este artigo abordará mecanismos para prevenir desastres em ambientes de máquinas virtuais, antecipando-se às falhas de hardware e de software. No entanto, mesmo em ambientes sem uso de virtualização (*standalone*), alguns dos exercícios aqui descritos também serão muito úteis.

Prevendo o desastre

Ambientes virtuais provavelmente são os mais sensíveis a desastres. Uma falha em um disco ou em uma interface de rede compartilhada entre diversas máquinas virtuais pode ser crítica, pois não indisponibiliza somente um serviço isolado, mas, em alguns casos, todos os serviços alocados nas máquinas virtuais do hospedeiro falho. Como prevenir é melhor que remediar, em ambientes virtuais, seu planejamento será a pedra fundamental para o sucesso do projeto. O bom planejamento para evitar desastres é uma boa prática na área de administração de sistemas.

Os mesmos problemas que causariam desastres em ambientes standalone são também os culpados em ambientes de máquinas virtuais, porém em escala muito maior. Quando optamos por virtualização, temos como foco a consolidação de nossa infra-estrutura computacional e, por conseqüência, a economia de recursos. No entanto, a consolidação de servidores em um único hospedeiro físico acaba por potencializar o tamanho dos problemas em caso de falhas de hardware. Porém, a proteção contra esse tipo de problemas está além do escopo deste artigo, sendo melhor coberta no artigo **Os dados não param**, na página 32 desta edição.

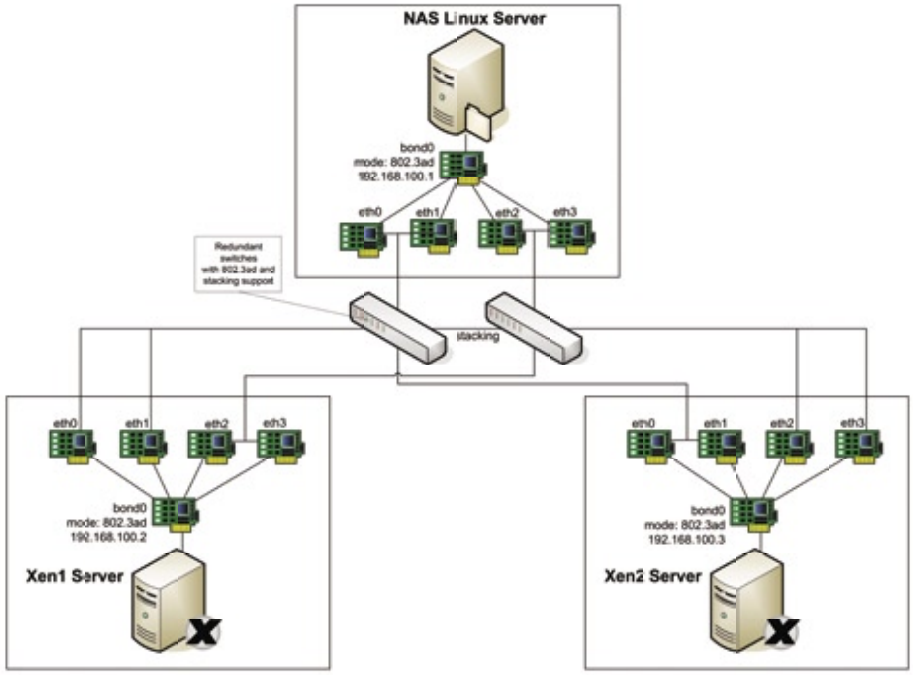


Figura 1 Estrutura da rede de exemplo, com o storage *nas* e os hospedeiros *xen1* e *xen2*.

Neste artigo, consideraremos que há um servidor dedicado ao armazenamento NAS com *hostname* NAS, configurado de acordo com o artigo "Os dados não param". Além disso, mostraremos como configurar dois hospedeiros de máquinas virtuais Xen, com hostnames Xen1 e Xen2.

Hardware

Vamos considerar cerca de seis máquinas virtuais rodando em nossos dois hospedeiros. Para isso, a configuração proposta para cada hospedeiro seria:

- processador Xeon Quad-Core;
- 8 GB de memória;
- fonte redundante;
- dois discos SATA de 250 GB;
- seis interfaces Gigabit Ethernet.

Como forma de aumentar a disponibilidade dos servidores virtuais, é interessante abrigar os discos dos hóspedes no NAS, acessando-os pelo protocolo ATA sobre Ethernet, conforme o artigo supracitado. Os 2,5 TB de armazenamento no NAS garantem espaço de sobra para futuros crescimentos na capacidade de armazenamento dos hospedeiros. Com relação à memória dessas máquinas, é preciso considerar que serão necessários 7 GB para os hóspedes (domU) e 1 GB para o hospedeiro (dom0). Apesar de dividirmos os hóspedes entre os dois servidores, é fundamental a capacidade de se adiantar a uma parada programada de um dos hospedeiros ou mesmo a sua falha total. Portanto, é justificável conferir 8 GB de memória RAM para cada servidor para que eles suportem toda a infra-estutura de hóspedes em caso de desastre com um deles.

Os dois discos rígidos têm como objetivo uma configuração em RAID 1 via software, já que serão usados somente pelo dom0 – portanto, não são necessárias configurações mais sofisticadas, como RAID via hardware, por exemplo.

As seis interfaces de rede Gigabit Ethernet em cada servidor se justificam pela necessidade de agregação de link dinâmico (*bon-*

Tabela 1: Endereços IP dos hospedeiros

Servidor NAS	Interface bond	Pool de interfaces	Endereço IP	Tipo de bonding	Rede
Servidor Xen1	bond0	eth[0,1,2,3]	192.168.100.1	Dynamic link aggregation	NAS
Servidor Xen2	bond1	eth[4,5]	192.168.0.101	Active-backup	LAN
	bond0	eth[0,1,2,3]	192.168.100.2	Dynamic link aggregation	NAS
	bond1	eth[4,5]	192.168.0.101	Active-backup	LAN
	bond0	eth[0,1,2,3]	192.168.100.3	Dynamic link aggregation	NAS
	bond1	eth[4,5]	192.168.0.102	Active-backup	LAN

ding) em quatro delas, ligadas ao switch do NAS, com as duas remanescentes conectadas à LAN, novamente para garantir a alta disponibilidade (**figura 1**).

Instalação

Na instalação do Linux no hospedeiro, recomenda-se reservar ao menos 20 GB para a partição raiz e 1 GB para swap. Nesse ponto, é interessante instalar somente o sistema básico nessas máquinas, pois apenas o Xen será executado nelas.

A configuração do bonding pode ser feita da mesma forma que o NAS, coberto no artigo "Os dados não param", alterando-se os arquivos `/etc/modprobe.d/arch-aliases`, executando-se `update-modules` e carregando-se o módulo com `modprobe bonding`. Assim como no artigo supracitado, contaremos aqui com duas interfaces lógicas agregadas: `bond0` e `bond1`. Isso requer a alteração do arquivo `/etc/network/interfaces` e a configuração de IPs de acordo com as VLANs criadas no NAS. A única diferença entre os dois hospedeiros, evidentemente, reside em seu endereço IP.

Após as alterações, basta executar o comando

```
# invoke-rc.d networking
➥restart
```

para reiniciar a rede com as novas configurações.

Instalação do hypervisor Xen

No *Debian Lenny*, está disponível o pacote do Xen 3.2.0. Um *backport* dos pacotes para o *Etch* está disponível no site do grupo de usuários Xen-BR. O pacote do kernel já preparado com os *patches* do Xen só estará disponível nos repositórios Debian quando a arquitetura do hospedeiro estiver disponível no kernel oficial, o que ainda não ocorreu. No entanto, é possível obter o kernel com suporte ao Xen compilando a partir dos fontes mantidos por sua equipe de desenvolvimento, ou, alternativamente, utilizando um pacote binário mantido pelo grupo de usuários Xen-BR.

Para optar pelo pacote do kernel compilado e os backports dos pacotes do Xen, basta acrescentar a seguinte linha ao arquivo `/etc/apt/sources.list`:

```
deb http://mirror.xen-br.org/
➥xen/ ./
```

Depois de atualizar os dados do sistema *apt* nos hospedeiros *Xen1* e *Xen2*, é fácil instalar os pacotes com o comando:

```
# apt-get install xen-hypervisor
➥-3.2-1-amd64 xen-utils-3.2-1
➥libxenstore3.0 libxen-dev xen-
➥utils-common xenstore-utils
➥linux-image-2.6.18.8-xen-1-
➥amd64
```

Segundo a **figura 1**, a LAN está conectada à VLAN2. Por isso, é necessário que as interfaces das máquinas virtuais estejam conectadas à interface lógica `bond1` para que os serviços sejam disponibilizados para a LAN. Então, vamos criar uma *bridge* (vlanbr0) na interface lógica `bond1`, para então criar as interfaces virtuais das máquinas virtuais, agregado-as à bridge. Esse procedimento aparentemente complexo fica mais simples quando se observa o **exemplo 1**, que mostra como deve ser alterado o arquivo `/etc/network/interfaces` dos hospedeiros. A **tabela 1** mostra os endereços IP planejados para cada componente da configuração.

Exemplo 1: Arquivo /etc/network/interfaces nos hospedeiros

```
01 # Troque o 'X' no campo 'address'
   ➥pelo IP do hospedeiro
02 auto lo
03 iface lo inet loopback
04
05 auto bond0
06 iface bond0 inet static
07    pre-up modprobe bond0
08    address 192.168.100.X
09    netmask 255.255.255.0
10    network 192.168.1.0
11    broadcast 192.168.1.255
12    slaves eth0 eth1 eth2 eth3
13
14 auto bond1
15 iface bond1 inet manual
16    pre-up modprobe bond1
17    pre-up ifconfig bond1 up
18    slaves eth4 eth5
19
20 auto vlanbr0
21 iface vlanbr0 inet static
22    pre-up ifup bond1
23    address 192.168.0.X
24    netmask 255.255.255.0
25    network 192.168.0.0
26    broadcast 192.168.0.255
27    gateway 192.168.0.1
28    dns-nameservers 192.168.0.254
29    dns-search domain.net
30    bridge_ports bond1
```

Discos virtuais remotos

As seis máquinas virtuais terão seus discos virtuais armazenados no NAS. Então, antes de instalarmos o sistema operacional nelas, é necessário formatar seus discos. Seguindo as indicações do artigo "Os dados não param", os dispositivos de bloco recebidos via AoE ficam no diretório `/dev/etherd/` e se chamam `eX.Y`, com X variando de 1 a 6 e Y valendo 1 ou 2. Essa configuração é resultado das instruções contidas no artigo supracitado.

Exemplo 2: Arquivo /mnt/etc/fstab

```
01 proc    /proc   proc    defaults   0 0
02 /dev/xvda1  /   ext3    errors=remount-ro  0 1
03 /dev/xvda2  none   swap    sw              0 0
```

Com o objetivo de realizar um balanceamento de carga entre os dois hospedeiros, vamos separar as máquinas virtuais entre os dois, ficando as máquinas *XenVm1* e a *XenVm3* no servidor *Xen1*, e as três restantes no servidor *Xen2*.

Após criar uma partição (*Ext3* é o sistema de arquivos recomendado) nos dispositivos adequados, não se esqueça de criar também um sistema swap (segundo as orientações, seus dispositivos são os que terminam em `.2`). Em seguida, usando o comando `debootstrap`, crie o primeiro modelo do Debian no disco da *XenVm1*, copiando para elas os módulos do kernel em seguida:

```
# mkdir /mnt/XenVm{1,2,3,4,5,6}
# mount /dev/etherd/e1.1 /mnt/
➥XenVm1
# debootstrap --arch amd64 etch
➥/mnt/XenVm1 http://ftp.br.
➥debian.org/debian
# cp -a /lib/modules/$(uname -r)
➥/mnt/lib/modules
```

A instalação e configuração das seis máquinas virtuais pode ser feita a partir de um mesmo hospedeiro, mesmo que elas depois venham a ser executadas no outro hospedeiro.

Os arquivos `/mnt/etc/fstab` e `/mnt/etc/network/interfaces` das máquinas virtuais ainda devem ser editados de acordo com os **exemplos 2** e **3**, respectivamente. Depois, deve-se montar o restante dos dispositivos AoE e copiar para cada um deles todo o conteúdo da partição-modelo, isto é, a que criamos para *XenVm1*. Para isso, em cada partição raiz de máquina virtual deve-se executar:

```
cp -a /mnt/XenVm1/* /mnt/XenVmY
```

no qual Y representa o número da máquina virtual.

Tabela 2: Componentes dos servidores virtuais

Hóspede	Serviço	Memória	Disco	IP
XenVm1	Mysql	2 GB	500 GB	192.168.100.11
XenVm2	Apache/intranet	1 GB	80 GB	192.168.100.12
XenVm3	Samba	1 GB	1 TB	192.168.100.13
XenVm4	Apache/Site	1 GB	100 GB	192.168.100.14
XenVm5	Mail server	1 GB	100 GB	192.168.100.15
XenVm6	POP/IMAP	1 GB	100 GB	192.168.100.16
	TOTAL	7 GB	1.88 TB	

Não tão iguais

Nesse momento, todas as máquinas virtuais já possuem um sistema operacional instalado, mas estão idênticas, o que não é nosso desejo. Cada uma deve ter seu próprio IP e arquivo de configuração que os hospedeiros precisam ter.

Para atribuir os IPs diferenciados, basta configurar o campo `address` do arquivo `/etc/network/interfaces` de cada máquina virtual de acordo com a **tabela 2**. Após alterar os arquivos de cada uma, desmonte os dispositivos AoE das máquinas virtuais com `umount /mnt/*`.

Precisamos agora criar os arquivos de configuração das máquinas virtuais nos hospedeiros. Para isso, crie no diretório `/etc/xen/` de cada hospedeiro um arquivo de acordo com o **exemplo 4** para cada máquina virtual. Ambos os hospedeiros precisam possuir os mesmos arquivos, que devem ter o nome da máquina virtual a que se referem: `XenVm1.cfg`, `XenVm2.cfg`, e assim por diante.

Exemplo 3: Arquivo /mnt/etc/network/interfaces

```
01 auto lo
02 iface lo inet loopback
03
04 auto eth0
05 iface eth0 inet static
06    address 192.168.100.X
07    network 192.168.100.0
08    netmask 255.255.255.0
09    gateway 192.168.100.1
```

Bate, coração

O *Heartbeat*[1] é um componente do núcleo do projeto Linux-HA[2] e é responsável por verificar perio-

Exemplo 4: Configuração da máquina virtual XenVm1

```
01 name ='XenVm1'
02 kernel = '/boot/vmlinuz-2.6.18.8-xen'
03 ramdisk = '/boot/initrd.img-2.6.18.8-xen'
04 disk = ['phy:/dev/etherd/XenVm1.dsk,xvda1,w',
   ➥'phy:/dev/etherd/XenVm1.swp,xvda2,w']
05 root = '/dev/xvda1 ro'
06 extra = 'xencons=xvc console=xvc0 video=tty'
07 memory = 512
08 vif = [ 'bridge=vlanbr0' ]
09 on_poweroff = 'destroy'
10 on_reboot = 'restart'
11 on_crash = 'restart'
12 vcpus = 2
```

dicamente a integridade dos nós de um cluster. Em caso de falhas no servidor remoto, o heartbeat ativa os serviços locais. Quando o servidor remoto for recuperado, seu próprio heartbeat anuncia sua disponibilidade para os demais componentes do cluster, retornando o serviço a seu servidor original. Em nossa configuração de recuperação de desastres em máquinas virtuais, o heartbeat é, sem dúvida, uma excelente opção.

Temos dois eventos que podem requerer a ação do heartbeat: (i) parada programada do hospedeiro para manutenção e (ii) desastre total de um hospedeiro por falha de hardware ou software. No primeiro caso, o próprio Xen pode se encarregar da solução, migrando (por live-migration) as máquinas virtuais para o outro hospedeiro. Já no caso de desastre do hospedeiro, o heartbeat é a ferramenta mais adequada.

Exemplo 5: Arquivo /etc/ha.d/ha.cf

```
01 debugfile /var/log/ha-debug
02 logfile /var/log/ha-log
03 logfacility     local7
04 keepalive 2
05 deadtime 10
06 warntime 10
07 initdead 120
08 udpport 694
09 bcast  bond0
10 # Troque o 'X' por '2' se for Xen1 e por'3' se for Xen2
11 ucast bond0 192.168.100.X
12 auto_failback on
13 node    xen1
14 node    xen2
15 respawn hacluster /usr/lib/heartbeat/ipfail
```

Exemplo 6: Arquivo /etc/ha.d/haresources

```
01 xen1 xen::/etc/xen/XenVm1.cfg::XenVm1 xen::/etc/xen/XenVm2.
   ➥cfg::XenVm2  xen::/etc/xen/XenVm3.cfg::XenVm3
02 xen2 xen::/etc/xen/XenVm4.cfg::XenVm4 xen::/etc/xen/XenVm5.
   ➥cfg::XenVm5 xen::/etc/xen/XenVm6.cfg::XenVm6
05 auto bond0
06 iface bond0 inet static
07    pre-up modprobe bond0
08    address 192.168.100.X
09    netmask 255.255.255.0
10    network 192.168.1.0
11    broadcast 192.168.1.255
12    slaves eth0 eth1 eth2 eth3
13
14 auto bond1
15 iface bond1 inet manual
16    pre-up modprobe bond1
17    pre-up ifconfig bond1 up
18    slaves eth4 eth5
19
20 auto vlanbr0
21 iface vlanbr0 inet static
22    pre-up ifup bond1
23    address 192.168.0.X
24    netmask 255.255.255.0
25    network 192.168.0.0
26    broadcast 192.168.0.255
27    gateway 192.168.0.1
28    dns-nameservers 192.168.0.254
29    dns-search domain.net
30    bridge_ports bond1
```

Próxima parada...

Para que o Xen esteja habilitado a efetuar a migração entre hospedeiros com tempo mínimo de parada das máquinas virtuais, é necessário ajustar, no arquivo de configuração do Xen (`/etc/xen/xend-config.sxp`), as variáveis `xend-relocation-server`, `xend-relocation-port`, `xend-relocation-hosts-allow` e `xend-relocation-address`. No arquivo citado acima, descomente, em ambos os hospedeiros, as seguintes linhas:

```
(xend-relocation-server 'yes')
(xend-relocation-port 8002)
(xend-relocation-address 'ip.ou.
➥hostname.do.hospedeiro.remoto')
(xend-relocation-hosts-allow
➥'ip.ou.hostname.do.hospedeiro.
➥remoto')
```

Com isso, parte do primeiro problema está resolvida. A outra parte se refere à inicialização do hospedeiro após a parada programada. Essa função será exercida pelo heartbeat e será uma rotina genérica a ser usada também após a recuperação nos casos de falha completa do hospedeiro.

Ajuste fino

Depois de instalar o heartbeat (`apt-get install heartbeat`) nos hospedeiros, é necessário fazer a configuração específica das duas máquinas no arquivo `/etc/ha.d/ha.cf` de acordo com o **exemplo 5**.

O arquivo `/etc/ha.d/authkeys` contém informações para o heartbeat autenticar membros do cluster.

Três métodos de autenticação são suportados (*SHA1*, *MD5* e *CRC*). Para usar o mais seguro (SHA1), primeiro crie o *hash* da chave:

```
# echo 'minha_chave' | sha1sum
➥011f9bcd00198d739a28af472b4f75a
➥1fadb0af2  -
```

Em seguida, copie esse hash para o arquivo `/etc/ha.d/authkeys` da seguinte forma:

```
auth 1
1 sha1 011f9bcd00198d739a28af472
➥b4
```

É interessante garantir que somente o usuário root possa acessar o arquivo `authkeys` (permissões `600`), já que ele contém informações confidenciais.

No arquivo `/etc/ha.d/haresources`, precisamos depois definir os recursos de cada hospedeiro, inserindo as linhas do **exemplo 6**. O campo `script` define o script a ser usado. O heartbeat tenta localizar esse script inicialmente no diretório `/etc/ha.d/resource.d/` e depois em `/etc/init.d/`. Então, sugere-se o uso da primeira alternativa, pois na segunda geralmente há apenas arquivos do sistema. Nosso script personalizado `xen` é descrito no **exemplo 7**.

Para acelerar a comunicação, é imprescindível o ajuste do arquivo `/etc/hosts` em cada um dos servidores (*nas*, *xen1* e *xen2*) com o hostname de todos.

Ao final, deve-se desligar os dois hospedeiros. Após o fim da inicialização do primeiro hospedeiro (*xen1*), verifique se todas as máquinas virtuais estão ativas com o comando `xm list`. Se sim, pode-se ligar o hospedeiro *xen2*. Após seu carregamento completo, parte das máquinas virtuais alocadas no hospedeiro Xen1 serão migradas para o hospedeiro Xen2.

Exemplo 7: Arquivo /etc/ha.d/resource.d/xen

```
01 # Xen heartbeat module em Xen1
02 FILE="$1"
03 VM="$2"
04 ACT="$3"
05 XM=/usr/sbin/xm
06 case "${ACT}" in
07   start)
08     xm list $VM >/dev/null 2>(e)1
09     if [ $? -eq 1 ]; then
10       $XM create $FILE
11     fi
12   ;;
13   stop)
14     # Ajuste para xen1 se o arquivo for do heartbeat do xen2
15     xm migrate -live ${VM} xen2
16   ;;
17 esac
```

Exemplo 8: Arquivo haresources em xen1

```
xen1 xen::/etc/xen/XenVm1.cfg::XenVm1 xen::/etc/xen/XenVm2.
➥cfg::XenVm2 xen::/etc/xen/XenVm3.cfg::XenVm3
```

Vai funcionar?

Alguns testes são aconselháveis para verificar se tudo está funcionando de acordo com o planejado. Quando se executa o comando `/etc/init.d/heartbeat stop`, o arquivo de configuração `/etc/ha.d/haresources` é lido. No primeiro hospedeiro, esse arquivo contém as informações mostradas no **exemplo 8**.

Portanto, a parada do servidor *xen1* executará o script `/etc/ha.d/resource.d/xen` (**exemplo 7**), passando como argumentos o arquivo de configuração (`/etc/xen/XenVm1.cfg`, por exemplo) e o nome de máquina virtual (`XenVm1`, por exemplo).

A migração das máquinas é feita na **linha 15** do **exemplo 7**, chamando o comando `xm migrate -live ${VM} xen2`. Ela informa ao Xen para migrar a máquina virtual imediatamente para o hospedeiro *xen2*. Outros testes a realizar são a retirada de cabos de rede aleatórios e o desligamento de um switch de rede. ■

Mais informações

[1] Heartbeat: http://www.linux-ha.org/Heartbeat

[2] Linux-HA: http://www.linux-ha.org

[3] Configuração de rede no Xen com bonding e VLAN: http://www.certifried.com/files/Xen_networking.pdf

[4] Bridge com Xen e bonding: http://etbe.coker.com.au/2007/08/14/ethernet-bonding-and-a-xen-bridge/

Sobre o autor

Marco Sinhoreli (msinhore@gmail.com) trabalha com Xen há três anos. É co-mantenedor do pacote *ibvirt* no Debian, fundador do grupo de usuários Xen-BR e trabalha no provedor de Internet Orolix, onde gerencia cerca de 180 máquinas virtuais Xen. Inclusive, jamais teria conseguido escrever este artigo sem as valiosas dicas de Luiz Ricardo Malheiros e Liberie da Cunha Neto.

De olho no serviço

Na busca da alta disponibilidade, é fundamental monitorar os serviços envolvidos.

por Durval Clemente

Há muito tempo o termo "alta disponibilidade" é conhecido no mundo da tecnologia. Normalmente, é associado a outro termo também muito conhecido: "pré-requisito". Ter os sistemas disponíveis é o mínimo que os usuários esperam do departamento de TI. Qualquer manutenção nos recursos tecnológicos é exaustivamente negociada com os usuários, e normalmente existe até um calendário pré-estabelecido com as paradas previstas para as manutenções preventivas e corretivas.

Quando se fala de disponibilidade, fala-se do tempo em que a aplicação ou o sistema estará disponível. Alta disponibilidade é um pré-requisito para sistemas críticos, cuja parada ou indisponibilidade, por mais curta que seja, não é aceita ou suportada pelos usuários ou pelo negócio – esses são os chamados de sistemas de missão crítica. Para esse tipo de necessidade, a disponibilidade total do ambiente, bem como os mecanismos para proteção e detecção de falhas, devem ser cuidadosamente avaliados e testados.

Normalmente, quando um fornecedor aborda a alta disponibilidade com um cliente, é importante rever os conceitos de *downtime*, SLA (*Service Level Agreement*) e a influência do encadeamento dos elementos de TI sobre a disponibilidade percebida pelo usuário final.

Porém, um sistema com 99% de disponibilidade pode ficar fora do ar por quase quatro dias ao ano. Mesmo assim, note que 99% é considerada uma disponibilidade elevada em muitas situações.

Multiplicação

A disponibilidade de um sistema completo geralmente não é calculada a partir de um único número. Em vez disso, quando o sistema possui múltiplos componentes –, a situação mais comum nas empresas – o cálculo é mais complexo.

A **figura 1** ilustra um exemplo fácil de ser encontrado nas empresas de médio e grande porte. Nela, a aplicação de missão crítica da empresa fica hospedada em um datacenter de alta disponibilidade, com redundância nos elementos de TI, inclusive com servidor clusterizado para a aplicação crítica. Já o local de trabalho não conta com redundância nos elementos e, portanto, é incapaz de oferecer alta disponibilidade.

Nesse ambiente, a disponibilidade final será o resultado do encadeamento dos elementos do *Posto de Trabalho*. Podemos calcular isso como a multiplicação do SLA de cada elemento:

$$0{,}95 \times 0{,}98 \times 0{,}98 \times 0{,}98 = 89{,}41\%$$

O cálculo da disponibilidade do datacenter é bem diferente, pois todos os elementos da infra-estrutura são redundantes, inclusive o servidor responsável pelo processamento do sistema de missão crítica. No datacenter, a disponibilidade total resultante do encadeamento dos elementos será de:

$$0{,}999 \times 0{,}999 \times 0{,}999 = 99{,}70\%$$

Calculando a disponibilidade total, de ponta a ponta, desde o acesso do usuário até o sistema de missão critica, a operação é:

$$0{,}95 \times 0{,}98 \times 0{,}98 \times 0{,}98 \times 0{,}999 \times 0{,}999 \times 0{,}999 = 89{,}15\%$$

O cálculo da disponibilidade do datacenter é bem diferente. Todos os elementos da infra-estrutura são redundantes, inclusive o servidor responsável pelo processamento do sistema de missão crítica.

A disponibilidade real que o usuário terá, em nosso exemplo para ilustrar o conceito, será de 89,15%. Por isso, é muito importante ter atenção aos contratos fechados com base em disponibilidade e SLA, pois sempre se deve levar em consideração a dispo-

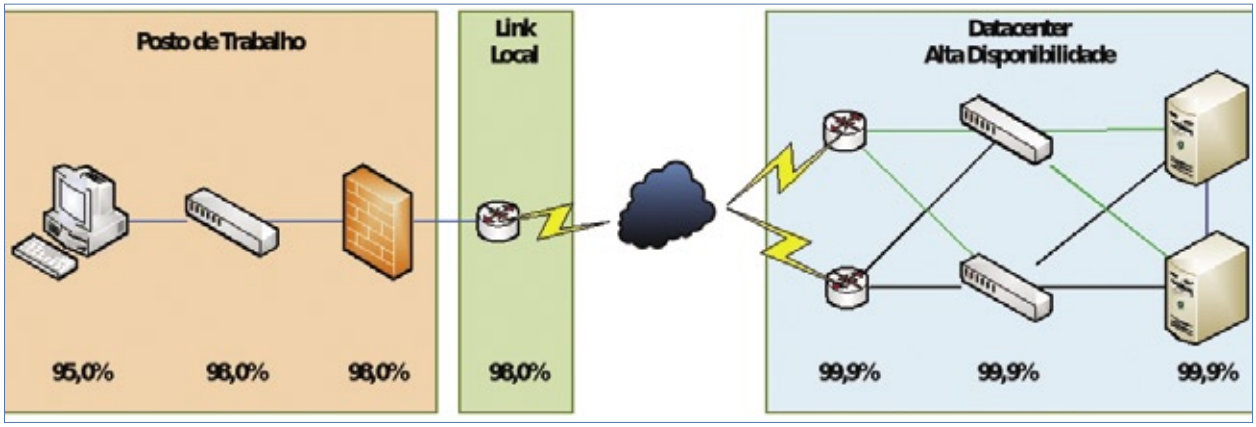


Figura 1 Com alta disponibilidade em apenas um dos "lados" do sistema, o todo não desfruta dessa vantagem.

nibilidade percebida pelo usuário, e não apenas a parte do datacenter.

Gestão

Controles são extremamente necessários em qualquer atividade empresarial ou pessoal. Definindo e acompanhando parâmetros, é possível avaliar continuamente o desempenho do negócio e corrigir desvios do plano original para atingir os objetivos planejados.

Cada vez mais as empresas estão contratando serviços baseados em níveis de serviços, ou SLAs. Para administrar esses contratos, é necessário que tanto as prestadoras de serviços como as empresas contratantes façam o gerenciamento dos parâmetros contratados. Um gerenciamento eficiente não significa ser sofisticado, com uma infinidade de parâmetros a serem acompanhados. Deve-se evitar que o próprio gerenciamento seja transformado no fim, e não no meio, para atender aos requisitos do negócio que o serviço se propõe. A simplicidade e o conhecimento pleno dos parâmetros contratados são fundamentais para a boa gestão do contrato, evitando conflitos pessoais e contratuais entre empresas e provedores de serviços.

O ITIL (*IT Infrastructure Library*) é um dos modelos de gestão para serviços de TI mais adotados pelas organizações. Ele é um modelo que define as melhores práticas para o gerenciamento dos serviços de TI. Cada módulo de gestão do ITIL define uma biblioteca de práticas para melhorar a eficiência de TI, reduzindo os riscos e aumentando a qualidade dos serviços e o gerenciamento da infra-estrutura.

Porém, como fazer esses controles no complexo mundo de TI? Como conciliar vários tipos de tecnologias de hardware e diferentes sistemas? Como otimizar os esforços com a solução de problemas? Como integrar isso a processos de melhores práticas?

Problemas comuns

Primeiramente, é necessário evitar os problemas comuns que impedem uma gestão eficiente de TI:

- sobrecarga de informações;
- escassez de tempo;
- excesso de decisões;
- déficit de atenção.

Qualquer um desses problemas, sozinho, configura uma ameaça à gestão. A manifestação de mais de um deles, portanto, é um risco muito sério.

Ferramentas

Com o crescimento diário de informações geradas por diversos sistemas e equipamentos, a tarefa de encontrar a solução para a equação das necessidades de controle com o orçamento cada vez mais disputado entre "áreas fins" e TI tem como uma boa alternativa o Software Livre.

Existem no mercado várias opções profissionais de sistemas para monitoração em tempo real dos elementos de TI, inclusive alternativas gratuitas. É importante procurar uma solução simples, flexível, funcional, de fácil implementação e manutenção – e existem alternativas gratuitas com essas características.

Tais características são fundamentais para atender às constantes necessidades de mudança nos ambientes de TI, necessárias para se adequar às exigências de disponibilidade dos recursos e ao cada vez menor orçamento da área de TI.

Necessidade

Não é errado o administrador se perguntar por que precisa de um sistema de monitoramento do ambiente de TI. A resposta, na realidade, é múltipla:

- aumentar a disponibilidade dos elementos de TI;
- identificar problemas rapidamente;
- identificar o impacto da indisponibilidade nos negócios;
- priorizar problemas, alocando equipes e focando esforços nos incidentes de maior impacto no negócio;
- implantar ou automatizar os processos do ITIL;
- informar aos responsáveis imediatamente, agilizando medidas de contingência;

- prover relatórios de negócio e técnicos em tempo real;
- alertar preventivamente falhas em serviços críticos, antes de causar impacto no negócio;
- otimizar investimentos em sua área de informática;
- demonstrar à empresa o valor da operação de TI;
- entender e tratar a complexidade do ambiente de informática a partir de uma única ferramenta.

O grande objetivo de uma ferramenta de monitoração é registrar, filtrar e organizar os eventos gerados pelo universo de TI. Para essas tarefas, a análise de volumes enormes de dados é desnecessária, pois, com um sistema eficiente de monitoração, os dados são transformados em informação, e assim o administrador dos recursos de TI recebe apenas o que é pertinente.

Monitoração eficiente

As regras básicas para uma monitoração eficiente são:

- gerenciar por objetivos: defina os indicadores-chave de desempenho e estabeleça os elementos a serem monitorados por metas de SLA e de desempenho;
- gerenciar por exceções: calcule o valor dos indicadores-chave de desempenho e compare com o que foi planejado ou adquirido;
- gerencie por fatos: analise as exceções com base no registro de informações reais, sem manipulação de informações;
- gerencie as ações: tome ações imediatas e assertivas de correção do desempenho e notifique os tomadores de decisão sobre as exceções.

Conclusão

O sucesso da operação de TI nos negócios depende da disponibilidade, que, por sua vez, deve ser continuamente monitorada por ferramentas eficazes. Portanto, sempre que for importante manter ou aumentar a disponibilidade, é importante contar com uma boa ferramenta de monitoração de TI. ■

Sobre o autor

Durval Clemente é economista e tem MBA em Gestão Empresarial. Com 28 anos de experiência em TI, atua na gestão de equipes em diversos segmentos de empresas.

TUTORIAL

Adicionando o projeto ADempiereLBR ao Eclipse

Em português, por favor

Finalizamos agora a série de tutoriais de instalação e configuração do ADempiere. Veja como iniciar o ERP e CRM a partir do Eclipse com o projeto de localização para o Brasil já instalado.

por Eduardo Montenegro

Esta é a quarta e última parte de nosso tutorial sobre o ADempiere ERP e CRM[1]. Na edição anterior[2], fizemos a instalação do ambiente de desenvolvimento *Java Eclipse*, do plugin SVN *Subclipse* e importamos o projeto do ADempiere. Agora, vamos importar o código-fonte do *AdempiereLBR*[3] para o Eclipse[4], o que permitirá o desenvolvimento e a execução do ADempiere com os recursos da localização para o Brasil.

Mais uma vez, é importante lembrar que o objetivo desta série de artigos é apresentar algumas das principais características do ADempiere, sendo impossível esgotar esse assunto ou nos aprofundarmos muito em determinados tópicos. Existem diversas fontes de informação disponíveis na Internet que podem ajudar a ampliar os conhecimentos sobre o sistema e que, inclusive, estão listados ao final deste artigo.

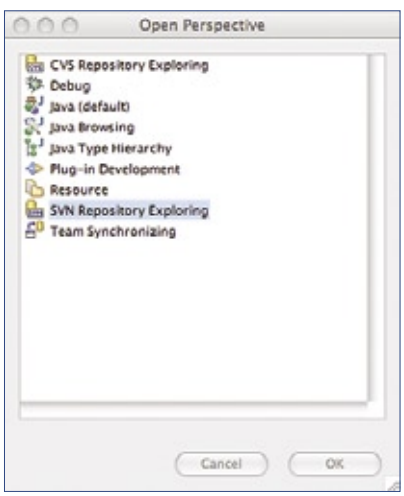


Figura 1 Janela de perspectivas.

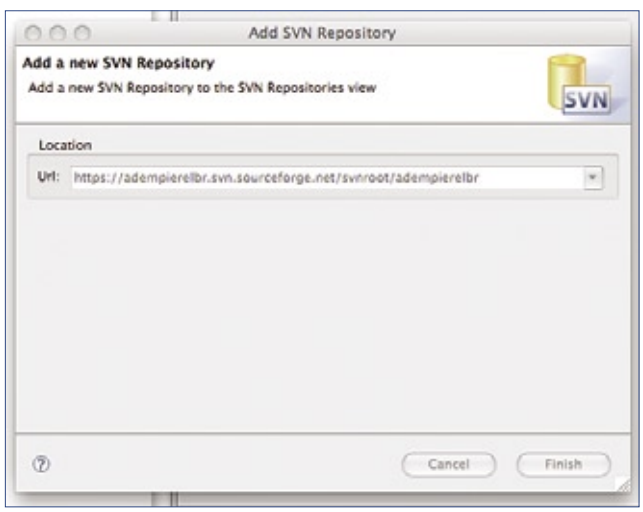


Figura 2 Acrescentando um novo repositório *SVN*.

Local: Brasil

Como vimos na edição anterior, o ambiente de desenvolvimento padrão utilizado pelos desenvolvedores do projeto ADempiere é o Eclipse. Por isso, vamos

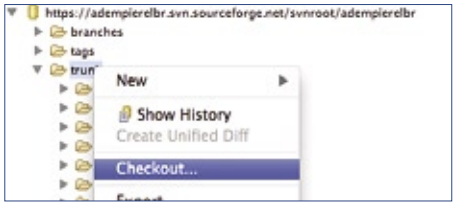


Figura 3 Download do código-fonte do projeto *AdempiereLBR*.

Figura 4 Importação do projeto *AdempiereLBR*.

Figura 5 Reabertura do projeto *AdempiereLBR* sob uma nova perspectiva.

seguir essa tendência e acompanhar os passos necessários para incluirmos o projeto AdempiereLBR a esse ambiente de desenvolvimento.

Para começar, inicie o Eclipse e, no menu *Window*, selecione *Open Perspective* e *Other*. Na janela que se abre (**figura 1**), selecione a opção *SVN Repository Exploring*. Na parte esquerda da janela, na aba *SVN Repository*, clique com o botão direito do mouse e adicione o repositório do ADempiere, conforme demonstra a **figura 2**.

O endereço do repositório do AdempiereLBR no Sourceforge, que deve ser adicionado ao campo *Url*, é `https://adempierelbr.svn.sourceforge.net/svnroot/adempierelbr`. Já com as informações do repositório no Eclipse, navegaremos até a pasta `Trunk/` e, em seguida, com o botão direito do mouse sobre a pasta, selecionaremos a opção *Checkout*, como mostra a **figura 3**.

Na próxima janela (**figura 4**), basta confirmar a operação selecionando os botões *Next* e, em seguida, *Finish*. Esse passo pode demorar um pouco, pois será feita uma cópia local de todos os arquivos do projeto do ADempiere.

Executando

Vamos agora executar o ADempiere a partir do Eclipse. Selecionando novamente no menu as opções *Window*, *Open Perspective* e *Other*, vamos retornar para a perspectiva *Java (default)*, conforme mostrado na **figura 5**.

Ao final desse procedimento, o projeto do AdempiereLBR estará disponível no Eclipse, permitindo a navegação pelos diversos pacotes e arquivos do projeto na aba do lado esquerdo, como mostra a **figura 6**.

O próximo passo é verificarmos se a dependência entre os projetos AdempiereLBR e ADempiere está definida corretamente. Para isso, devemos selecionar o projeto AdempiereLBR com o botão direito do mouse e, em seguida, selecionar a opção *Properties*, conforme demonstrado na **figura 7**. Na janela de propriedades do projeto, exibida na **figura 8**, na opção *Java Build Path* e na aba *Projects*, devemos adicionar o projeto *adempiere_trunk* que criamos no terceiro artigo desta série de tutoriais[2]. O projeto *adempiere_trunk* deve ser o único selecionado nesta janela.

Agora, para executarmos o projeto a partir do Eclipse, resta apenas definirmos um perfil de execução, que pode ser criado por meio dos seguintes passos:

- selecionar o menu *Run* e, em seguida, *Open Run Dialog*, conforme a **figura 9**;
- na janela mostrada em seguida (**figura 10**), selecione a opção *Java Application* no painel do lado esquerdo e selecione o botão *Novo*;

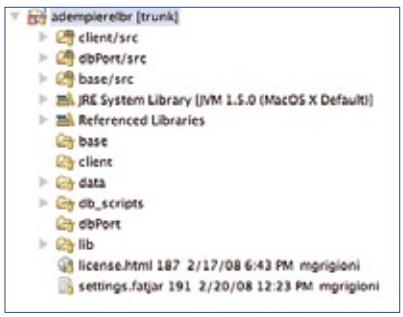


Figura 6 Navegação pelo código do projeto importado.

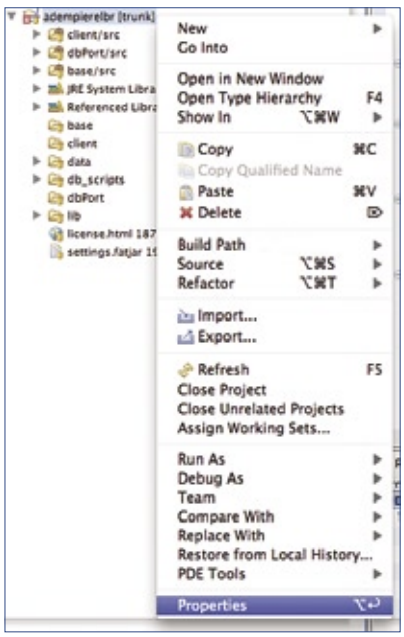


Figura 7 Verificação das dependências entre os dois projetos.

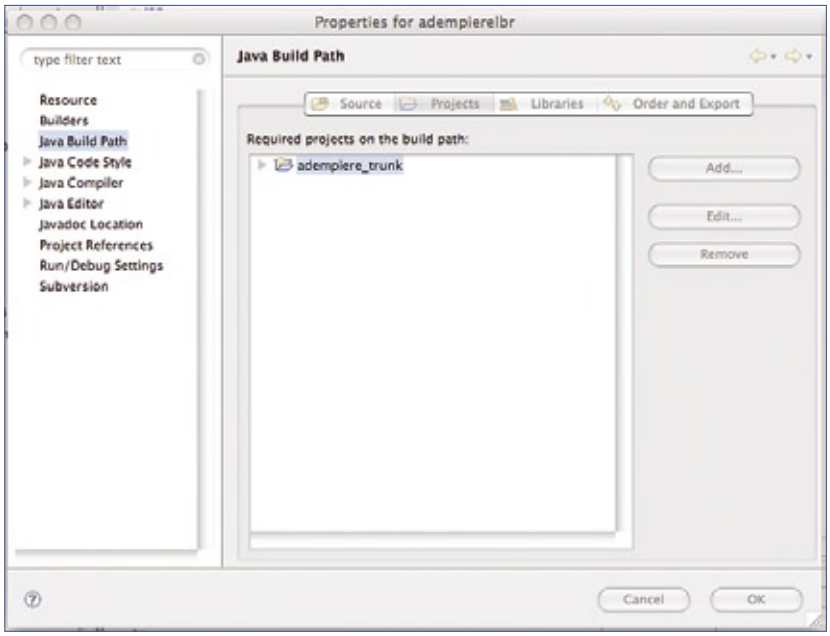


Figura 8 Criação do vínculo entre os projetos *ADempiere* e *AdempiereLBR*.

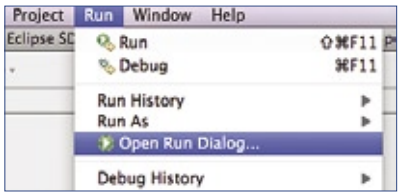


Figura 9 Se preparando para executar o projeto sob o *Eclipse*.

- no campo *Name*, entre com o nome *AdempiereLBR*;
- no campo *Project*, utilizando o botão *Browse*, selecione o projeto recém-criado;
- finalmente, no campo *Main Class*, digite: `org.compiere.Adempiere`.

Ao final, basta pressionar o botão *Apply* seguido de *Run* para que o AdempiereLBR seja executado a partir do Eclipse.

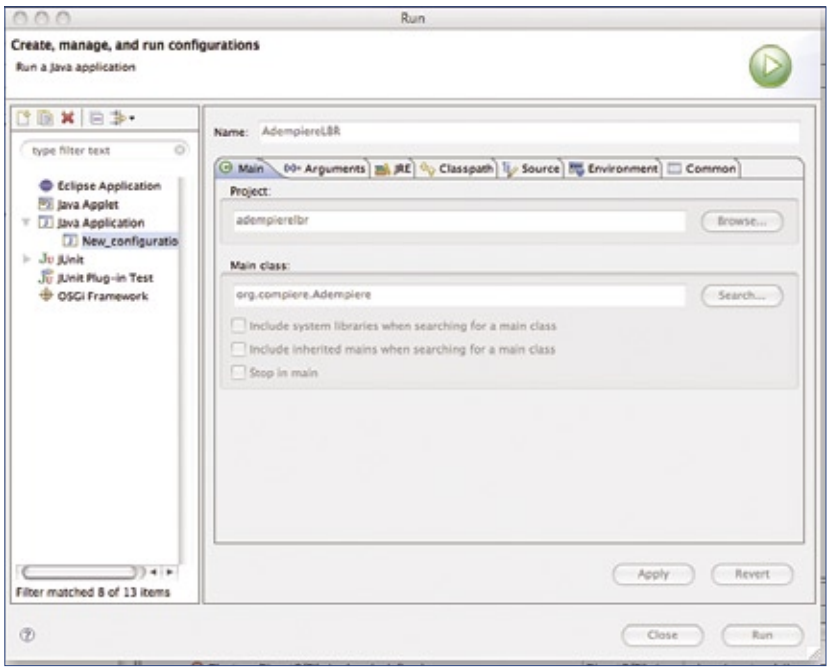


Figura 10 Basta aplicar as alterações e rodar o projeto.

Conclusão

Agora o ambiente completo de desenvolvimento já está configurado com ambos os projetos, ADempiere e AdempiereLBR.

Um sistema ERP e CRM é bastante extenso, o que acaba criando uma certa complexidade. Nos quatro artigos publicados nesta série, o objetivo foi ultrapassar a dificuldade inicial da instalação do sistema. A partir desse ponto, já é possível iniciar a explorar os recursos do sistema.

Conforme novas dúvidas forem surgindo, há ótimas fontes de informação e ajuda disponíveis na Internet [1][5][6][7][8], com grande participação de brasileiros. ■

Mais informações

[1] Site do ADempiere: http://www.adempiere.com

[2] Eduardo Montenegro, "Produto importado": http://www.linuxmagazine.com.br/article/1765

[3] AdempiereLBR: http://sf.net/projects/adempierelbr

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

[5] Wiki do ADempiere: http://www.adempiere.com/wiki

[6] ADempiere no Sourceforge: http://sf.net/projects/adempiere

[7] AdempiereLBR no Sourceforge: http://sf.net/projects/adempierelbr

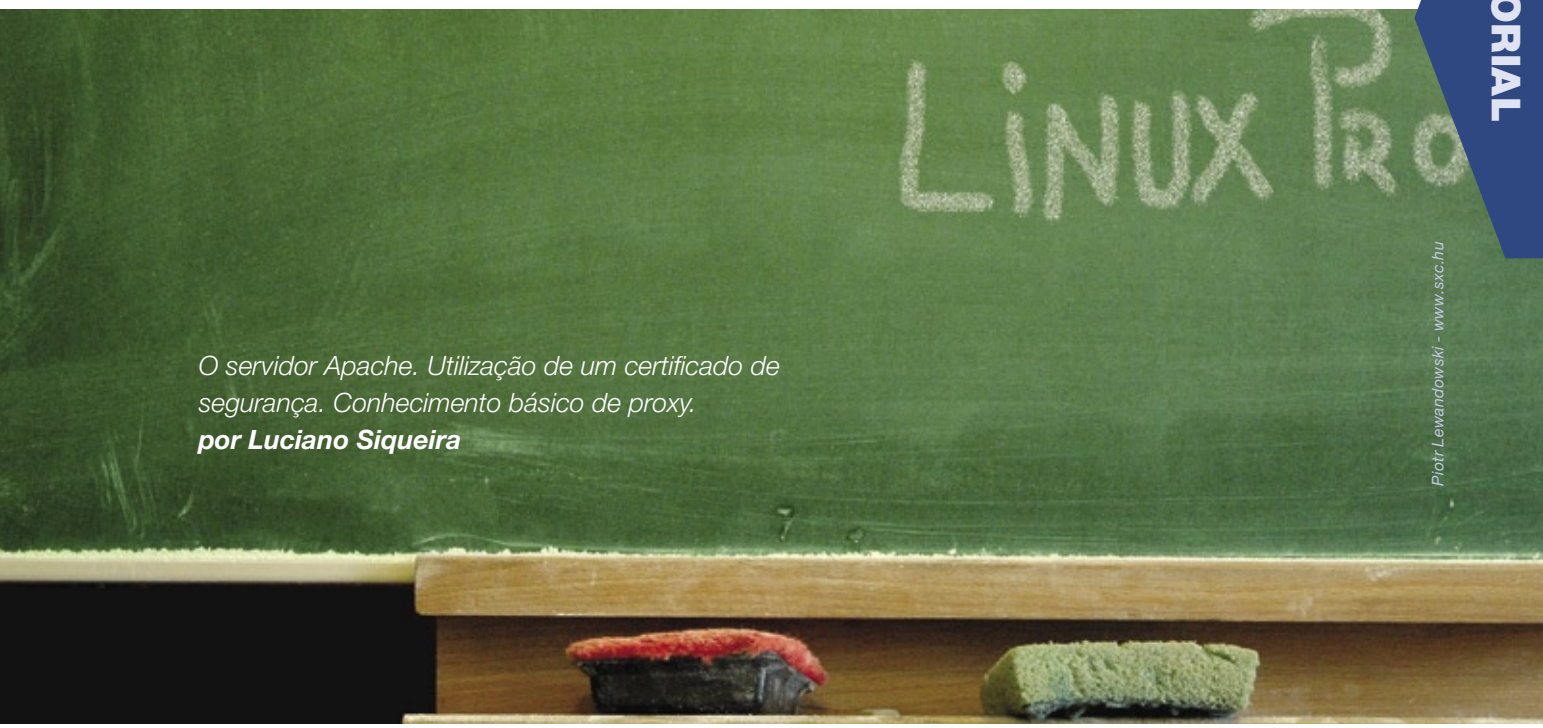
[8] Fórum sobre ADempiere em português: http://forum.kenos.com.br

Décima segunda aula da preparação LPIC-2

LPI nível 2: Aula 12

The Linux Professional Institute

TUTORIAL



Piotr Lewandowski - www.sxc.hu

O servidor Apache. Utilização de um certificado de segurança. Conhecimento básico de proxy.

por Luciano Siqueira

Tópico 208: Web Services

2.208.1 Implementando um servidor Web

O Apache é o servidor HTTP mais utilizado no mundo e acompanha todas as distribuições voltadas para servidores. A instalação a partir do código fonte é rara, sendo necessária somente se uma capacidade muito exótica for exigida do servidor. O daemon responsável pelo apache é o `httpd`. Apesar de já estar na versão 2.0, a versão 1.3 ainda é largamente utilizada e algumas diferenças entre elas devem ser levadas em consideração. Do lado do cliente, a versão do servidor Apache, via de regra, não pode ser notada. Já no lado do servidor, existem peculiaridades na configuração e manutenção de cada uma das versões.

Apache 1.3

O Apache 1.3 no Unix funciona como um servidor Web baseado em processos. O programa servidor replica várias cópias de si mesmo quando iniciado. Isso significa que o programa servidor iniciado, chamado processo "pai", cria várias cópias de si mesmo, chamadas processos "filhos", cada um dos atuando como um servidor independente. Dessa forma, se um dos processos se tornar instável, poderá ser terminado sem prejudicar os demais, e o servidor continuará operando. No entanto, a estratégia de utilizar vários processos filhos como servidores afeta a performance do serviço. Processos independentes não podem compartilhar funções e dados diretamente, o que aumenta o consumo de recursos do sistema.

Apache 2.x

Na versão 2.x do Apache, a arquitetura de processamento das requisições foi abstraída para módulos servidores especiais, chamados *Multi Processing Modules* (MPMs). Isso significa que o Apache pode ser configurado para operar como servidor baseado em processos, com chamadas internas (*threads*) ou uma mistura dos dois. Chamadas internas acontecem dentro de um único processo e ocorrem simultaneamente. Diferente de processos isolados, podem compartilhar funções e dados. Por isso, todo o processo consome menos recur-

sos, tornando-se mais ágil. Porém, se uma chamada interna provocar uma falha, todo o serviço pode ficar comprometido.

Configuração

A localização padrão para os arquivos de configuração pode ser `/etc/apache`, `/etc/httpd` ou `/etc/apache2`. O arquivo de configuração principal no Apache 1.3 é `httpd.conf`, que agrega praticamente todas as configurações do serviço. No Apache 2.x, o principal arquivo é `apache.conf` ou `apache2.conf`. Outros arquivos, embora em desuso, ainda podem ser utilizados na versão 1.3 do Apache, como o `/etc/apache/access.conf` e `/etc/apache/srm.conf`.

Algumas configurações fundamentais feitas em `/etc/apache/httpd.conf`:

- `ServerType valor`: Define se o `httpd` deve rodar separado ou se por meio de do daemon `inetd`. O valor pode ser `standalone` ou `inetd`;
- `ServerRoot caminho`: Define o topo do caminho de diretório em que estão os arquivos do Apache;
- `PidFile caminho`: Define o arquivo que armazenará o valor do PID para o processo `httpd` pai. O padrão é `/var/run/httpd.pid`;
- `ServerAdmin email`: Endereço de email do administrador do servidor, para onde deverão ser encaminhadas informações de erro;
- `DocumentRoot caminho`: Caminho do diretório que armazena os documentos disponibilizados no site. Geralmente `/var/www` ou `/var/www/htdoc;`
- `Servername www.nome.com`: Nome do site, o domínio registrado;
- `LoadModule nome caminho`: Carrega um módulo DSO (Dynamic Shared Object). Módulos adicionam novas funcionalidades ao Apache, como suporte a CGI, autenticação, scripts etc. O caminho é escrito a partir daquele definido em `ServerRoot`;
- `AddModule modulo.c`: Ativação dos módulos estáticos e externos. Utilizado para definir a ordem correta de carregamento dos módulos;
- `Port porta`: Define a porta onde o servidor escutará. Dificilmente será diferente de 80;
- `User usuário`: Usuário dono do processo servidor;
- `Group grupo`: Grupo dono do processo servidor.

Essas são as opções básicas de um arquivo de configuração do Apache. Um arquivo de configuração simples pode ser visto no **exemplo 1**.

Nele são utilizadas algumas opções que influenciam a performance do servidor e ajudam a

Exemplo 1: Arquivo de configuração simples

```
ServerType standalone
ServerRoot "/usr"
PidFile /var/run/httpd.pid
ScoreBoardFile /var/run/httpd.scoreboard
Timeout 300
KeepAlive On
MaxKeepAliveRequests 100
KeepAliveTimeout 15
MinSpareServers 5
MaxSpareServers 10
StartServers 5
MaxClients 150
MaxRequestsPerChild 0
LoadModule vhost_alias_module libexec/apache/mod_vhost_alias.so
LoadModule env_module         libexec/apache/mod_env.so
LoadModule define_module      libexec/apache/mod_define.so
(...)
ClearModuleList
AddModule mod_vhost_alias.c
AddModule mod_env.c
AddModule mod_define.c
AddModule mod_log_config.c
AddModule mod_mime_magic.c
AddModule mod_mime.c
AddModule mod_negotiation.c
AddModule mod_status.c
Port 80
User nobody
Group nobody
ServerAdmin lsiqueira@linuxnewmedia.com.br
Servername zyon
DocumentRoot "/var/www/htdocs"
<Directory />
    Options FollowSymLinks
    AllowOverride None
</Directory>
<Directory "/var/www/htdocs">
    Options Indexes FollowSymLinks MultiViews
    AllowOverride All
    Order allow,deny
    Allow from all
</Directory>
AccessFileName .htaccess
<Files ~ "^\.ht">
    Order allow,deny
    Deny from all
    Satisfy All
</Files>
```

manter a acessibilidade do site ali hospedado.

- `Timeout 300`: Tempo limite de espera para receber uma requisição GET, dados via POST ou PUT e intervalo entre ACKs em transmissões de pacotes TCP em respostas;
- `KeepAlive On`: Permite que mais de uma requisição seja realizada em uma única conexão;
- `MaxKeepAliveRequests 100`: Número máximo de requisições numa mesma conexão. `0`, não estabelece limite;
- `KeepAliveTimeout 15`: Intervalo, em segundos, da última requisição até o fechamento da conexão. Um valor alto manterá o processo servidor ocupado e poderá causar pouca responsividade num servidor muito acessado;
- `MinSpareServers 5`: Número mínimo de processos servidores inativos, aguardando conexão;
- `MaxSpareServers 10`: Número máximo de processos servidores inativos. Se esse número for ultrapassado, processos inativos excedentes serão finalizados;
- `StartServers 5`: Número de processos filhos disparados inicialmente mais o servidor principal;
- `MaxClients 256`: Total máximo de processos servidores. O valor máximo é igual ao valor padrão (`256`). Um valor maior só poderá ser utilizado se for alterado o valor de `HARD_SERVER_LIMIT` no arquivo `httpd.h` e o Apache for recompilado;
- `MaxRequestsPerChild 0`: Número máximo de requisições que um processo servidor filho poderá receber. Se o número for atingido, o processo filho será finalizado. Se o valor for `0`, não haverá limite máximo.

Todos os valores mostrados correspondem aos valores padrão das opções no Apache 1.3.

Restrição de acesso

O Apache pode criar restrições de acesso aos arquivos que podem ser vistos pelos clientes. Uma configuração típica é:

```
<Directory />
    Options FollowSymLinks
    AllowOverride None
</Directory>
```

O diretório em questão é especificado na abertura da seção. No exemplo, trata-se do diretório raiz (`<Directory />`). A opção `FollowSymLinks` orienta o Apache a obedecer os links simbólicos no diretório. `AllowOverride` especifica se pode ser utilizado um arquivo `.htaccess` no diretório (bloqueado no exemplo).

Criado na base do diretório em questão, o arquivo `.htaccess` define quais serão as restrições de acesso ao diretório em questão. Para utilizá-lo, deverá haver uma entrada liberando esse recurso no arquivo de configuração do Apache:

```
<Directory "/var/www/htdocs">
   Options Indexes FollowSymLinks
➥ MultiViews
   AllowOverride All
   Order allow,deny
   Allow from all
</Directory>
```

A opção `AllowOverride All` permite a utilização do arquivo `.htaccess`. As opções vinculadas à entrada `Directory` no arquivo de configuração agora podem ser definidas para um diretório a partir do arquivo `.htacces` nele contido. Por exemplo: é possível exigir uma senha para que o usuário acesse o conteúdo de determinado diretório por meio da autenticação simples oferecida pelo módulo `mod_auth`.

Semelhante à criação de uma conta de usuário no sistema, é utilizado o comando `htpasswd` para criar contas de acesso ao diretório restrito:

```
htpasswd -s -c /var/www/htdocs/
➥restrito/.htpasswd lsiqueira
```

A opção `-s` determina a utilização do algoritmo SHA1 no armazenamento da senha. A opção `-c` indica a localização do arquivo que armazenará as senhas. Se o arquivo existir, a conta será incluída. Por fim, é indicado o nome do usuário. A senha pode ser indicada em seguida ou inserida interativamente, exatamente como no comando `passwd`. Por ser um arquivo de senha, precauções quanto às permissões de acesso devem ser tomadas.

Em seguida, é criado o arquivo `.htaccess` no diretório a ser protegido. Exemplo de conteúdo básico desse arquivo:

```
AuthType Basic
AuthName "Restricted Area"
AuthUserFile "/var/www/htdocs/
➥restrito/.htpasswd"
Require valid-user
```

As definições mostradas são suficientes para fazer a autenticação. Como o arquivo contendo as contas pode estar em qualquer lugar no sistema, é importante fornecer seu caminho completo. A opção `AuthName` define o texto que aparecerá como título da área restrita na janela de autenticação mostrada para o usuário.

Arquivos de log

Os arquivos de log registram todas as transações realizadas pelo Apache e possíveis falhas. O log de erros é definido pelo parâmetro `ErrorLog`. Além de um arquivo, poderá ser especificado um comando para receber os dados sobre o erro, ou ser utilizado o daemon *Syslog*.

Para definir um comando, um sinal *pipe* ("|") é utilizado:

```
ErrorLog "| /usr/bin/mail -s Erro
➥ webmaster@finlandia.org"
```

Para utilizar o Syslog, utiliza-se o termo `syslog` seguido da facilidade. A facilidade padrão é `local7`. Por exemplo: para utilizar o Syslog e a facilidade `user`:

```
ErrorLog syslog:user
```

Todas as transações (inclusive imagens em páginas HTML, por exemplo) também podem ser registradas num arquivo de log. Primeiro deve ser criado o formato e definido um termo de referência, chamado *nickname*, por meio da opção `LogFormat`:

```
LogFormat "%h %l %u %t \"%r\" %>s
➥ %b" common
```

Cada caractere precedido de % especifica um campo da transação:

- `%h`: Host remoto;
- `%l`: Log remoto, se houver;
- `%u`: Usuário remoto, se disponível pelo auth;
- `%t`: Data e hora, no formato padrão americano;
- `%r`: Primeira linha da requisição;
- `%s`: Status da requisição;
- `%b`: Bytes enviandos, excluídos os cabeçalhos.

Definido o formato personalizado, a opção `CustomLog` define o arquivo e o nickname pré-definido:

```
CustomLog /var/log/apache/access_
➥log common
```

Existem muitas possibilidades de criação de logs personalizados. Pode ser criado um log apenas para registrar quais navegadores acessaram o site:

```
LogFormat "%{User-agent}i" agent
CustomLog /var/log/apache/agent_
➥log agent
```

Todas as alterações feitas nas configurações só terão efeito quando o Apache for reiniciado. Na versão 1.3, o servidor pode ser iniciado, terminado ou reiniciado por meio do comando `apachectl`, usando as seguintes opções:

- `apachectl start`: Inicia o servidor;
- `apachectl stop`: Termina o servidor;
- `apachectl restart`: Reinicia ou inicia o servidor se houver alterações de configuração;
- `apachectl graceful`: Inicia ou reinicia o servidor se houver alterações de configuração, mas antes espera as conexões ativas terminarem;
- `apachectl configtest`: Verifica se há erros de sintaxe nas configurações.

No caso do Apache 2.x, o comando chama-se `apache2ctl` e aceita as mesmas opções do comando `apache ctl`.

2.208.2 Manutenção do servidor Web

Hosts virtuais

Dada a grande capacidade dos servidores modernos, é comum que o mesmo servidor abrigue mais de um site. O site solicitado pode ser identificado tanto pelo IP quanto pelo nome do mesmo. Portanto, o host virtual pode ser baseado em IP ou em nome. Um host virtual baseado em IP extrai esse número da conexão e envia o site adequado. Um outro baseado em consulta de nomes verifica o nome solicitado a partir dos cabeçalhos HTTP e envia o site adequado. Por meio dos hosts baseados em nome, vários sites diferentes podem utilizar o mesmo endereço IP.

A principal diretiva para definir um host virtual no arquivo de configuração é `<VirtualHost>`. Para utilizar hosts virtuais baseados em nome, é necessário informar ao Apache que o servidor deve trabalhar com hosts virtuais baseados em nome, por meio da opção `NameVirtualHost`:

```
NameVirtualHost *
```

Usando o `*`, hosts virtuais baseados em nome poderão ser utilizados neste servidor a partir de qualquer interface nele configurada. Pode também ser especificada uma porta específica, dispensável se o servidor não escutar numa porta diferente de 80. Em seguida, poderão ser configurados os hosts virtuais, como mostra o **exemplo 2**.

Também em `<VirtualHost>` podem ser especificados o IP e a porta. Na maioria dos casos, apenas o `*` será suficiente. Os únicos parâmetros necessários para cada host virtual baseado em nome são `ServerName` e `DocumentRoot`, respectivamente o nome do site e o diretório com conteúdo fornecido. Outras opções poderão ser incluídas na diretiva `<VirtualHost>`, como `ServerAlias`,

Exemplo 2: Configurando os hosts virtuais

```
<VirtualHost *>
        ServerName www.guglio.com
        DocumentRoot /var/www/guglio
</VirtualHost>

<VirtualHost *>
        ServerName www.iarru.com
        DocumentRoot /var/www/iarru
</VirtualHost>
```

que indica outros nomes por meio dos quais o site será acessível:

```
<VirtualHost *>
        ServerName www.iarru.com
        ServerAlias iarru.com
➥*.iarru.com
        DocumentRoot /var/www/
➥iarru
</VirtualHost>
```

Dessa forma, requisições para qualquer host do domínio `iarru.com` serão servidas pelo host virtual `www.iarru.com`. Como visto no exemplo, são aceitos caracteres curinga nos nomes, como `*` e `?`.

Hosts virtuais baseados em IP são semelhantes. Basta indicar em `<VirtualHost>` o nome ou, preferencialmente, o IP do site:

```
<VirtualHost 192.168.02>
        DocumentRoot /var/www/
➥orcute
        ServerName www.orcute.com
</VirtualHost>
```

É recomendável definir também outros parâmetros para cada host virtual. Itens como `ServerAdmin`, `ErrorLog` e `TransferLog`. A maioria das definições feitas para um site único pode também ser feita para um host virtual.

Conexões seguras (SSL)

O servidor Web Apache é capaz de trabalhar com conexões seguras SSL (*Secure Socket Layers*). Nas versões do Apache anteriores à 2.0, era necessário obter o suporte a SSL (`mod_ssl`) separadamente. A versão 2.x do Apache inclui o `mod_ssl`, eliminando a necessidade de instalá-lo separadamente.

Quando um navegador solicita uma conexão segura – via protocolo HTTPS, que determina utilização da porta 443 –, o navegador envia de volta um certificado. Para garantir a autenticidade do servidor, o navegador verifica este certificado junto a uma terceira instância, chamada *Certificate Authority* (Autoridade Certificadora, ou simplesmente CA). Algumas das Autoridades Certificadoras populares são VeriSign (Thawte), GeoTrust e GoDaddy. Se o certificado fornecido pelo site for comprovado pela Autoridade Certificadora, o navegador aceitará a conexão criptografada como confiável.

O primeiro passo é gerar uma chave privada, que será mantida no servidor Web. O comando utilizado para gerar a chave é o `openssl`:

```
# openssl genrsa -des3 -out www.
➥guglio.com.br.key 1024
```

Esse comando gerará uma chave usando criptografia *Triple DES* e a gravará no arquivo `www.guglio.com.key`. Assim será solicitada uma frase de acesso para criar a chave, sendo importante manter uma cópia de segurança dessa chave.

Em seguida, é necessário criar um *Certificate Signing Request* (Pedido de Assinatura de Certifi-

Exemplo 3: Criando o CSR

```
# openssl req -new -key www.guglio.com.br.key -out www.guglio.com.br.csr
Enter pass phrase for www.guglio.com.br.key:
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:BR
State or Province Name (full name) [Some-State]:São Paulo
Locality Name (eg, city) []:São Paulo
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Linux New Media do Brasil
Organizational Unit Name (eg, section) []:.
Common Name (eg, YOUR name) []:www.linuxnewmedia.com.br
Email Address []:.


Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
```

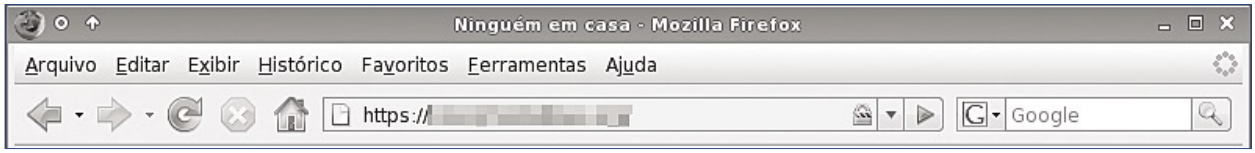


Figura 1 O protocolo https e o cadeado demonstram tratar-se de um site seguro.

cado). O CSR também é criado por meio do comando `openssl`, conforme o **exemplo 3**.

Alguns dados serão requisitados. Preencha-os cuidadosamente para não gerar alertas de segurança. Em `Common Name`, forneça o nome desejado para apareceer como a origem do certificado. Se for o endereço do site, não escreva o `http://`. A chave gerada dentro do conteúdo do arquivo CSR, `www.guglio.com.br.csr` será utilizada para requisitar o certificado junto à autoridade certificadora.

Os certificados são pagos, portanto só será possível prosseguir na criação do certificado depois de efetuado o pagamento. Um certificado de teste é fornecido gratuitamente pela CA Thawte e pode ser utilizado por 21 dias. O CSR deve ser enviado para a CA, que criará a chave de certificado. O arquivo CRT – `www.guglio.com.br.crt` – deve ser criado, contendo a chave gerada pela autoridade certificadora.

Criados os três arquivos, o Apache já pode ser configurado para utilizar conexões seguras. Copie os arquivos para seu local definitivo, por exemplo, `/usr/local/ssl/`. Os itens fundamentais no arquivo de configuração do Apache para lidar com conexões seguras são:

- `Listen 443`: O servidor deverá escutar na porta 443 (HTTPS);
- `SSLEngine on` ou `SSLEnable`: Ativa o suporte a conexões seguras;
- `SSLCertificateKeyFile` caminho: Indica o arquivo de chave privada (`.key`);
- `SSLCertificateFile caminho`: O arquivo do certificado, cujo conteúdo foi gerado pela autoridade certificadora.

Assim que o Apache for iniciado, será necessário fornecer a frase de acesso, como informada na cria-

ção do arquivo de chave privada. Os sites configurados poderão ser acessados via HTTPS. Um site com conexão segura pode ser identificado pela designação https:// e pelo ícone do cadeado (**figura 1**).

Checando as propriedades da página (**figura 2**), podemos obter mais informações sobre o certificado.

2.208.3 Implementando um servidor Proxy

Um servidor proxy atua como um filtro para Web. Instalado no servidor gateway, pode agir como um cache de conteúdo, bloqueador de conteúdo e autenticador de acesso.

Várias distribuições Linux possuem um pacote Squid, facilitando a instalação. Mesmo a instalação a partir do código fonte é corriqueira.

Cache proxy

A configuração do proxy de cache é muito simples. Basta editar o arquivo `squid.conf` e alterar poucas opções. Opções importantes no `squid.conf` para um proxy de cache:

- `http_port`: Define a(s) porta(s) utilizada pelo Squid. A porta normalmente utilizada é a 3182;
- `cache_mgr`: O email do administrador do proxy;
- `cache_effective_user`: O usuário sob o qual o daemon `squid` será executado;
- `cache_effective_group`: O grupo sob o qual o daemon `squid` será executado.

O Squid não pode rodar sob usuário root. É aconselhável criar um usuário e um grupo de sistema exclusivamente para esse serviço.

ACL

Uma ACL (*Access Control List*) é a definição de uma regra de acesso. No caso do proxy Squid, determina permissões e limites aos usuários do proxy.

Figura 2 Verificando informações de segurança para o domínio.

As ACLs também são definidas no arquivo `squid.conf`. Um exemplo de ACL simples:

```
acl lan src 192.168.1.0/24
```

Essa linha define uma ACL de nome *lan*, que se refere a todas as requisições para a rede 192.168.1.0/24.

Para liberar o acesso a esse grupo, também deve ser incluída a linha abaixo:

```
http_access allow lan
```

Considerações sobre o tópico

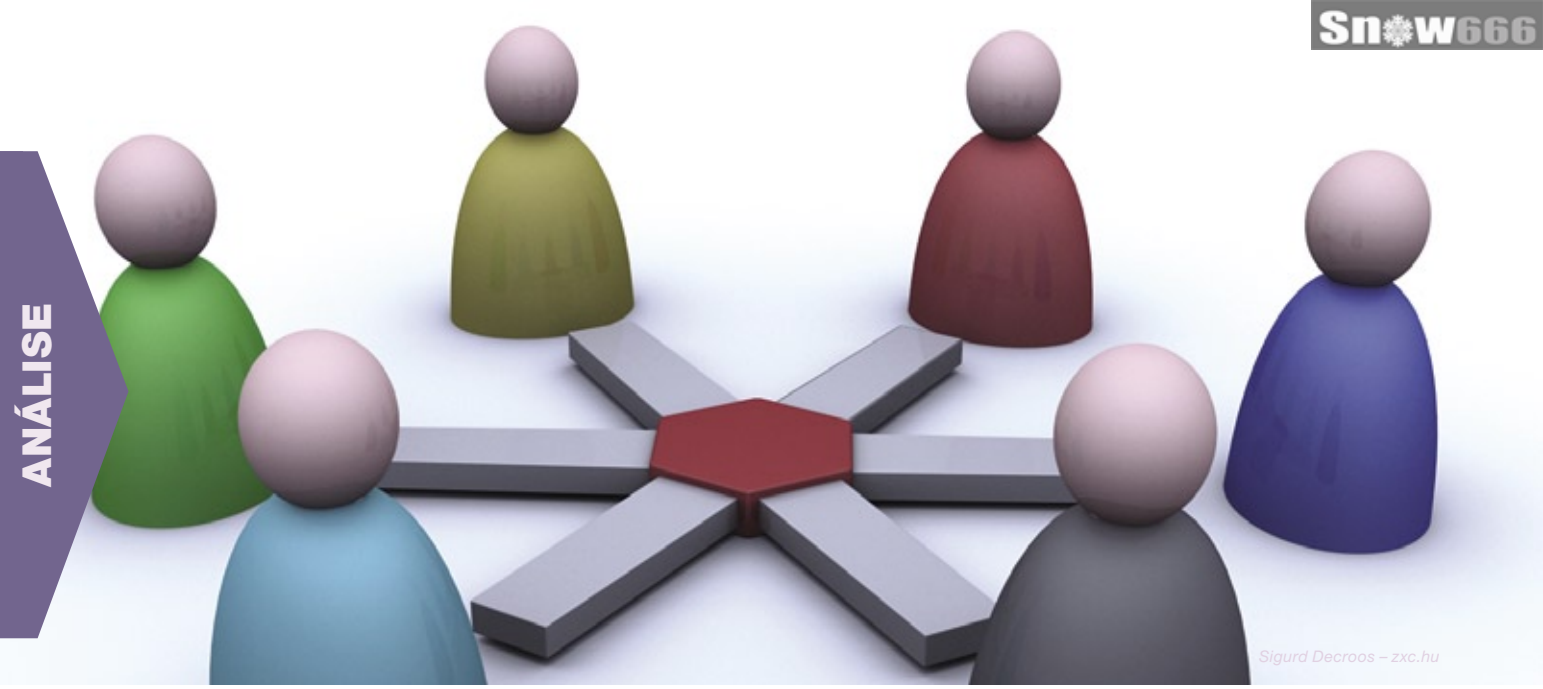
Nessa parte da prova você será questionado a respeito de algumas configurações do Apache, como ajustes de performace e utilização de domínios virtuais. Pelo menos uma questão a respeito do Squid e ACLs será feita.

O exame de certificação LPI exige essencialmente conhecimentos sobre diagnóstico e resolução de problemas.

Portanto, é necessário ser capaz de identificar configurações incorretas, sobretudo pela análise de arquivos de log. ■

Sobre o autor

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



Xwiki, um wiki de segunda geração

Wiki 2.0

Sistemas wiki já são usados em grandes empresas, mas vale a pena conhecer o Xwiki e seus diferenciais corporativos.

por Miguel Koren O'Brien de Lacy

Os wikis iniciaram sua trajetória devido à necessidade de gerar e modificar páginas da Web de forma simples e rápida por qualquer pessoa, sem a necessidade de acesso ao servidor, e usando apenas a própria Web. O primeiro wiki, o *WikiWikiWeb*, foi utilizado pela primeira vez em 1995, no site da empresa de seu criador [1], o que mostra a longa trajetória e o longo tempo que essa tecnologia levou para ser melhor conhecida e mais utilizada. Por sua vez, o WikiWikiWeb utilizou idéias que foram implementadas no sistema *Hypercard*[2], criado por Bill Atkinson para o Apple Macintosh em 1987. Entre alguns aportes interessantes do Hypercard à tecnologia da Internet utilizados até hoje podem ser mencionados o cursor de hyperlink – uma mão com o indicador estendido – e até um navegador web, o *ViolaWWW*, de 1992. O objetivo do WikiWikiWeb foi facilitar a colaboração entre os programadores da empresa. Hoje, o exemplo mais conhecido da tecnologia wiki é, sem dúvida, a Wikipédia, que utiliza o sistema *Media Wiki*[3].

Segunda geração

O grupo de desenvolvimento do *Xwiki*[4] o rotula como um "wiki de segunda geração". Segundo seus desenvolvedores, os wikis de primeira geração atendem a necessidade de colaborar na geração de conteúdo na Web, enquanto os de segunda geração atendem a necessidade de desenvolver aplicativos colaborativos na Web. Em termos de aplicativos colaborativos, o "mercado" visado pelo Xwiki é toda a classe de aplicativos simples, os quais são necessários e precisam ser desenvolvidos rapidamente ecom baixo custo. Além disso, consumiriam tempo ou recursos em demasia se fossem desenvolvidos dentro de uma metodologia formal da área de TI. A **figura 1** mostra graficamente o campo de aplicabilidade de aplicativos que podem ser implementados pelo Xwiki.

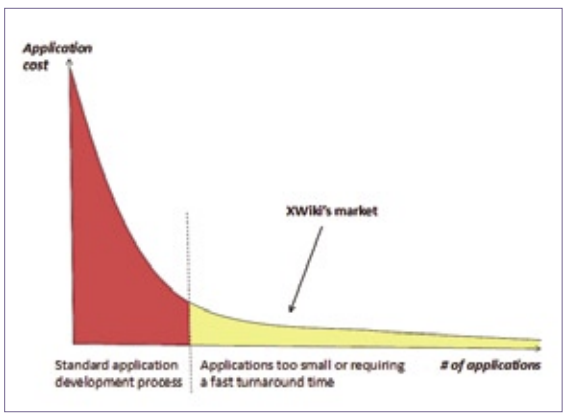


Figura 1 O mercado atendido pelo *Xwiki* consiste na cauda longa do mercado de aplicativos.

Um dos objetivos dos wikis é permitir a criação e a edição de páginas de uma forma simples. Entretanto, apesar de o HTML já ser, a princípio, uma linguagem simples, para a maioria das pessoas, é bastante difícil se lembrar de todas as *tags* HTML e da sintaxe exata. Assim, nasceram diversas linguagens de marcação para formatar as páginas. Lamentavelmente, ao mesmo tempo em que são consideravelmente mais simples de usar e que têm o HTML como referência, a multiplicidade de linguagens como *structured text*, *MoinMoin*, *reStructured text* e outras gera confusão e faz com que os wikis deixem de ser portáveis entre sistemas.

Devido a suas origens, os sistemas wiki são colaborativos por natureza e atendem muito bem as necessidades iniciais da Web que estão hoje em evolução. Respondem ao desejo de participação em equipe na criação de páginas e também às necessidades corporativas. No ambiente de comunidades e equipes de projeto, é útil permitir que todos os membros participem por igual na criação do conteúdo. No ambiente corporativo, as necessidades são opostas e, de certa forma, contrárias ao objetivo original dos wikis, pois existe a necessidade de controlar quem pode fazer modificações. Sendo assim, os wikis modernos têm fortes mecanismos de segurança de acesso.

Os sistemas wiki são, na realidade, sistemas de gestão de conteúdo (CMS) desenvolvidos colaborativamente, utilizando diretamente o próprio navegador web. Assim, seu foco está na criação do conteúdo e não nos demais aspectos do gerenciamento de sites tais como blogs, álbuns de fotos e outros, que por sua vez são o forte de sistemas como *Plone*[5], *Joomla* [6], *OpenCMS* [7], *Drupal*[8] e muitos outros.

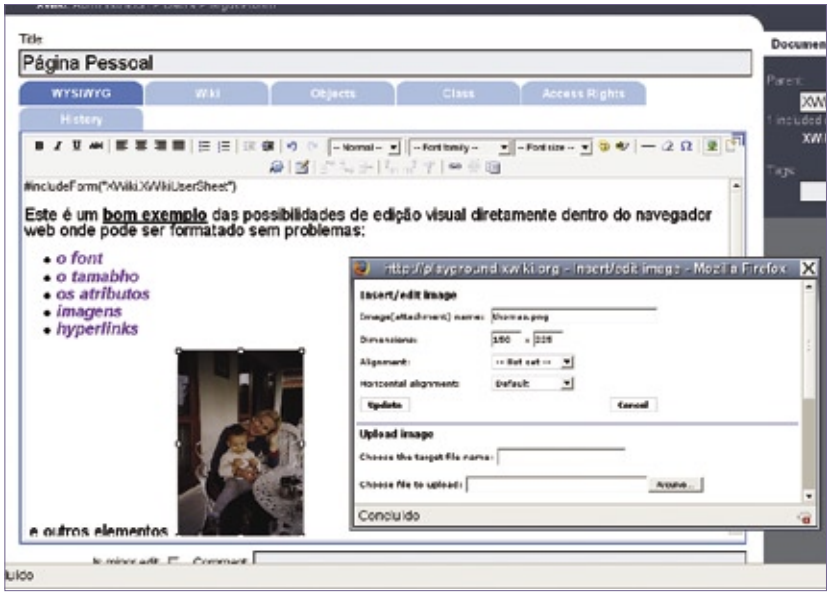


Figura 2 Edição visual de um documento (página) do Xwiki, no qual foi inserida uma imagem.

Categorias

Os wikis podem ser classificados em três grandes grupos: os pessoais e comunitários, os wikis de aplicativos e os corporativos. Vejamos algumas características de cada um.

Os wikis pessoais e comunitários têm como objetivo a administração de informações de natureza fundamentalmente de texto, sem necessidades de acesso a bancos de dados ou outros aplicativos. Eles podem oferecer acesso colaborativo na mesma página ou simplesmente acesso exclusivo para a organização de informação individual, e por isso são muito simples de instalar e operar.

Os wikis de aplicativos têm uma estruturação que permite a criação de aplicativos. Geralmente vão além de administrar apenas páginas HTML e oferecem a possibilidade de incluir chamadas a programas externos a partir das páginas, além de permitirem o uso de scripts internos para incrementar a funcionalidade da edição com a linguagem de criação. Esses aplicativos também são conhecidos como aplicativos *situacionais*, pois são desenvolvidos por seus próprios usuários de forma não estruturada e sem uma metodologia definida. Tratam-se, normalmente, de aplicativos simples, como listas de tarefas, controles simples de materiais etc.

Por último, os wikis corporativos possuem recursos adequados, naturalmente, ao uso em ambientes corporativos. Normalmente são usados para formar sistemas de base de conhecimento e são disseminados internamente nas empresas. Entre suas principais características, encontram-se:

- sistema de permissões de acesso;
- facilidade de interação com sistemas externos;
- facilidade de classificação das informações de forma estruturada;
- acesso simplificado a bancos de dados SQL.

O site Wikimatrix[9] se dedica a comparar sistemas wiki e gera uma longa lista de comparação de recursos entre quaisquer sistemas que o usuário selecionar.

Xwiki

O Xwiki é um dos projetos membros do consórcio OW2[10], que tem por missão fornecer soluções de middleware (no sentido amplo

Figura 3 Exemplo de site público feito com o *Xwiki* e um skin personalizado.

do termo) de alta qualidade com as quais uma empresa possa atender suas necessidades em aplicativos de base. Sendo um membro OW2, o Xwiki é também um aplicativo em *Java* que pode rodar dentro de contêineres tais como *Tomcat* ou servidores *Java Enterprise* como *JBoss* ou *Jonas*. Essa característica do Xwiki aumenta seu apelo dentro da empresa, pois oferece integração ao restante da estrutura computacional. Porém, o Xwiki não é apenas um membro do consórcio OW2, mas também é usado em diversas páginas do próprio site do consórcio e de outros projetos. Vejamos alguns de seus recursos mais relevantes.

Recursos

A edição WYSIWYG (*what you see is what you get*) elimina o problema de aprender alguma sintaxe de editoração para formatar o conteúdo do documento. Isso é de grande utilidade para se usar o sistema sem qualquer treinamento. Porém, o Xwiki também permite a edição do conteúdo com a notação wiki. A **figura 2** mostra o poder de edição visual comparado à edição wiki de outros sistemas.

O controle de versões do conteúdo é mais um recurso importante, pois armazena todas as versões das páginas para possibilitar a auditoria do conteúdo. Ele permite desfazer as alterações para voltar qualquer página a uma versão anterior.

O gerenciamento de permissões permite a definição por usuário e por documento, indicando quem pode acessar ou modificar cada documento, área ou wikis completos.

Além disso, o gerenciamento de usuários e grupos fornece um bom controle sobre a definição de grupos e atribuição de usuários para aplicar as diretivas de segurança de forma flexível.

O Xwiki pode fazer um uso muito interessante do mecanismo de RSS. O RSS permite emitir e receber notificações de modificações, e normalmente é usado para acompanhamento de notícias. Porém o Xwiki possibilita a emissão de notificações ao serem alteradas as páginas, ou a inclusão de notificações de outras fontes no conteúdo do Xwiki.

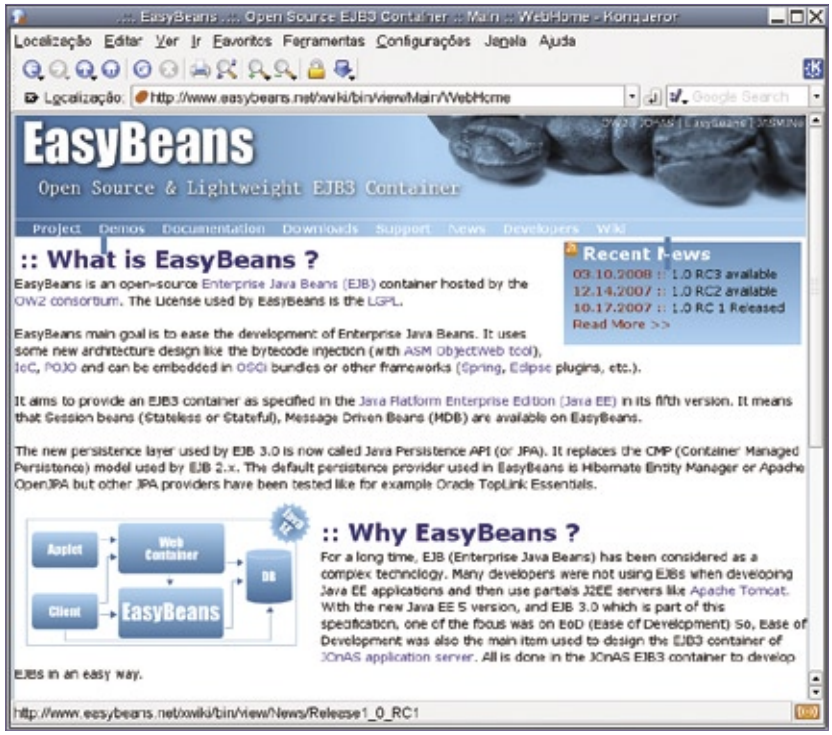


Figura 4 Com um skin diferente, o *Xwiki* pode ganhar um novo visual.

A arquitetura de plugins desse wiki de segunda geração prepara-o para o desenvolvimento modular de extensões. O site do projeto lista diversos plugins que podem ser instalados para incrementar a funcionalidade do sistema.

O visual do Xwiki pode ser alterado por temas, ou *skins*, como são oficialmente chamados na documentação. Esse é, sem dúvida, um recurso de grande utilidade para manter a imagem corporativa de uma área wiki. O uso de skins permite modificar o visual sem necessidade de modificação do conteúdo, separando a informação da apresentação. Os skins são desenhados com CSS (*Cascading Style Sheets*), um padrão Web. As **figuras 3** e **4** dão uma idéia da variedade de visuais oferecida pelos skins.

Além disso, podem ser definidos modelos para as páginas e modelos para formulários, auxiliando no desenvolvimento de novas páginas no mesmo padrão visual. Tanto as páginas quanto os modelos do Xwiki podem ser feitos nas linguagens *Groovy*[11] ou *Velocity*[12]. Em particular, o Groovy é atualmente bastante popular entre os desenvolvedores web. Já o Velocity faz parte do projeto *Apache*, e foi criado como uma linguagem a ser usada para modelos.

No gerenciamento, o sistema inclui o conceito de wikis individuais sendo gerenciados centralmente pelo Enterprise Manager.

Um dos maiores apelos de um wiki corporativo é a possibilidade de construir e utilizar aplicativos web. O Xwiki é distribuído com vários aplicativos de utilidade geral e também pode incorporar outros aplicativos. A programação destes é feita com a inclusão de programas dentro das páginas e com o agrupamento de páginas para formar um aplicativo. Um aplicativo pode ser exportado como arquivo XAR (*Xwiki Archive*) para ser importado em outro Xwiki. Entre os aplicativos distribuídos junto com o pacote básico, destacam-se os de blogs, álbum de fotos, calendário de eventos, busca, mapas mentais e listas de tarefas. Isso mostra que o Xwiki já "vem de fábrica" com aplicativos de utilidade para seu uso imediato no ambiente corporativo.

Pelo fato de incorporar uma API específica para a integração com outros sistemas, o Xwiki é considerado mais simples que os demais wikis neste quesito. Isso facilita bastante a escalabilidade das áreas wiki construídas na empresa e que, posteriormente, tenham que ser integradas a outros sistemas corporativos sem a necessidade de modificar a própria área wiki.

Além disso, o Xwiki atende às normas JSR 168 e, portanto, pode ser rodado como *portlet* dentro de portais corporativos como *JBoss Portal*[13], *Liferay*[14], *Exo Platform*[15] etc. Essa possibilidade ajuda a integração do sistema dentro da estrutura computacional da empresa.

O conteúdo gerenciado pelo Xwiki é guardado em bancos de dados relacionais SQL. Pode ser usado o banco de dados da preferência do cliente, pois o acesso é feito pelo *Hibernate*[16], que suporta diversos bancos. O Hibernate possibilita até a troca de banco de dados sem perder suas informações, algo que poderia eventualmente ser importante se um determinado wiki mudar de plataforma devido a fusões ou aquisições de empresas. Esse é outro destaque de apelo corporativo do Xwiki, pois, em grandes empresas, é recomendável manter as informações em bancos de dados por motivos de facilidade de administração e segurança de acesso. Além de usar o banco de dados para guardar o conteúdo, o Xwiki pode usá-lo para realizar a autenticação dos usuários no login. Outra forma de autenticação é a integração com LDAP.

Acompanhar as estatísticas de uso do sistema é uma tarefa importante,

seja para otimizar seu desempenho, seja para detectar problemas, e o Xwiki oferece tais estatísticas.

Módulos

A modularidade do sistema lhe permite ser estendido conforme as necessidades da empresa. O módulo básico é o próprio sistema Xwiki Enterprise (XE) com os recursos listados anteriormente. Ele é próprio para ser utilizado em intranets e na Internet para gestão de conhecimento, colaboração em projetos, sistemas *mashup*, gestão de conteúdo simples, dentre outros.

Para as situações em que devem ser administrados e gerenciados diversos wikis em conjunto, está disponível o *Xwiki Enterprise Manager* (XEM), que oferece a possibilidade de gerar novos wikis sob demanda e gerenciar o acesso de usuários e grupos a esses wikis.

O módulo *Xwiki Watch* tem como objetivo aceitar e filtrar diversas fontes de noticias por RSS e apresentá-las de forma personalizada para os usuários, incluindo anotações feitas por outros usuários. Ele é projetado para o uso em situações nas quais são indicadas ferramentas de inteligência competitiva. Um bom exemplo pode ser a agregação de notícias imobiliárias de diversas fontes, filtradas por palavras-chaves e apresentadas individualmente a corretores, os quais filtram os assuntos que sejam de interesse para seu trabalho imobiliário.

O *Xwiki Workspaces* atende a equipes de projeto e facilita a colaboração entre elas. Nesse módulo, cada usuário possui uma área pessoal, onde pode incluir documentos e anexos, além de poder convidar outros usuários a participarem em sua área.

O *Xwiki Platform* é o motor do sistema, utilizado para integrar serviços wiki dentro de outros aplicativos. O próprio Xwiki Enterprise e Manager é composto por aplicativos desenvolvidos usando essa plataforma como seu núcleo. Outro exemplo de uso do Xwiki Platform é a integração de um wiki dentro do sistema CRM *OpenCRX*[17]. A **figura 5** mostra a arquitetura do Platform e seu relacionamento com outros componentes.

Para facilitar a portabilidade, cada página do Xwiki pode ser exportada em diversos formatos, como PDF, HTML, RTF e XAR (formato de portabilidade do Xwiki). A possibilidade de obter um PDF do conteúdo sem complicação é uma característica de grande utilidade, pois permite que qualquer usuário possa procurar o material de que precisa e obtenha rapidamente uma versão formatada para impressão ou apresentação.

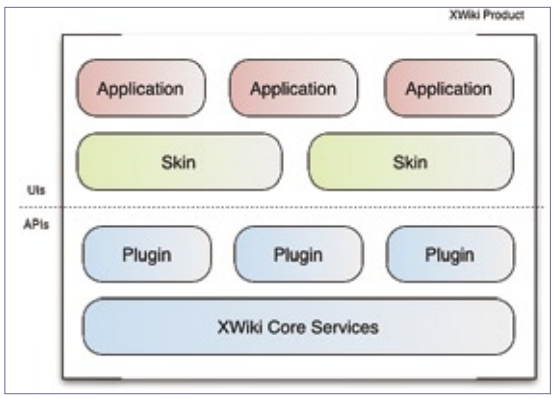


Figura 5 Arquitetura do *Xwiki Platform* e aplicativos.

Instalação e Operação

Existem diferentes pacotes de instalação, dependendo das necessidades do usuário. A forma mais simples para começar a usar o sistema é instalando o pacote completo, que inclui o contêiner Java *Jetty* [18] e o banco de dados *Hsqldb* [19]. Há também um instalador nativo para Windows, além de um pacote ZIP com os mesmo componentes que deve simplesmente ser descomprimido no diretório de escolha do usuário. Para um maior controle sobre a instalação, ou caso seja preciso integrar o Xwiki dentro de uma infra-estrutura existente, existem os pacotes WAR. Sua instalação não apresenta dificuldades ou dependências difíceis de solucionar, mas quem tiver problemas pode seguir as instruções na documentação. Depois da instalação do sistema, por exemplo, do Xwiki Enterprise, podem ser instalados os aplicativos padrão que são disponibilizados em formato XAR nativo do Xwiki. É recomendável instalar esses aplicativos, pois eles disponibilizam funcionalidades que provavelmente serão de utilidade.

Diversos plugins, aplicativos e skins podem ser baixados da mesma área de download. Para os desenvolvedores, existe um plugin para a plataforma *Eclipse*.

Usando o instalador genérico em Java, pode ser seguida a seguinte seqüência de passos: para iniciar esse instalador, primeiro é necessário ter o Java instalado no sistema. Para executar o instalador, usa-se o comando:

```
java -jar xwiki-pacote-a-instalar.
➥jar
```

Talvez seja necessário adicionar o parâmetro `-Xmx512m` ou algo semelhante para atender a necessidades de memória durante a instalação.

Os idiomas do aplicativo são apenas inglês e francês, mas o método de instalação segue o básico *Next-Next-Finish*.

Logo depois da instalação, o sistema deve ser iniciado, o que significa banco de dados e contêiner Java para Web operacionais. O instalador genérico mostra um ícone diretamente na área de trabalho, por meio do qual deve-se acionar o sistema. Depois de alguns minutos, já é possível apontar

o navegador Web para o endereço http://localhost:8080/xwiki/bin/view/Main/WebHome para visualizar o sistema padrão (**figura 6**).

A partir desse momento, já se pode modificar o conteúdo do Wiki e usá-lo para qualquer propósito que o usuário deseje. Para parar o sistema, pode-se acionar o ícone na área de trabalho específico para essa tarefa.

Um dado importante para o início é habilitar e conhecer o login padrão do usuário administrador. Por padrão, a instalação desabilita o login do superadministrador por motivos de segurança. O arquivo `xwiki.cfg` no diretório `WEB-INF/` do contêiner Java contém uma linha `xwiki.superadminpassword=system`, a qual deve ser descomentada e receber a senha desejada. Note que é possível utilizar o sistema sem habilitação de login do super administrador. Após essas alterações, o sistema deve ser reiniciado.

Conclusão

O Xwiki atende muito bem a seu mercado-alvo declarado. Assim, ele é uma boa alternativa para criar áreas colaborativas e aplicativos web simples em pouco tempo e com esforço reduzido. Podem ser gerados aplicativos complexos, mas esse uso extrapola os objetivos de projeto do sistema. Porém, chamamos atenção aos exemplos de sites públicos feitos com o Xwiki. Suas características corporativas, tais como integração LDAP, uso de bancos de dados SQL, gestão de permissões e controle de versões do conteúdo aumentam o apelo para o uso corporativo. A plataforma Java e o uso do mecanismo Hibernate para persistir os dados em bancos de dados aumentam a portabilidade do Xwiki para vários sistemas operacionais e bancos de dados. Para as empresas que usam a tecnologia Java, esse sistema apresenta ainda a vantagem de aderir aos padrões, além de facilitar a manutenção pela área de TI com experiência em Java. ■

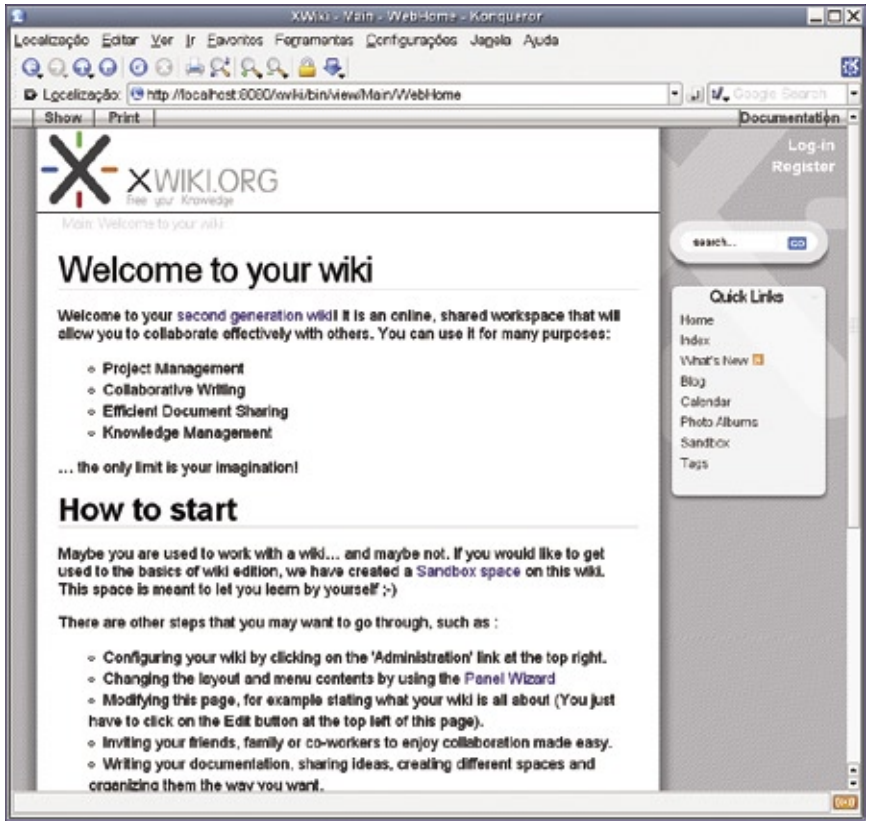


Figura 6 Página inicial do *Xwiki* após a instalação do pacote completo.

Mais informações

[1] História do primeiro wiki: http://c2.com/cgi/wiki

[2] Hypercard: http://en.wikipedia.org/wiki/HyperCard

[3] MediaWiki: http://www.mediawiki.org

[4] Xwiki: http://www.xwiki.org

[5] Plone: http://www.plone.org

[6] Joomla: http://www.joomla.org

[7] OpenCMS: http://www.opencms.org

[8] Drupal: http://drupal.org

[9] Wikimatrix: http://www.wikimatrix.org

[10] Consórcio OW2: http://www.ow2.org

[11] Groovy: http://groovy.codehaus.org/

[12] Velocity: http://velocity.apache.org/

[13] JBoss Portal: http://www.jboss.org/jbossportal/

[14] Liferay: http//www.liferay.com

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

[16] Hibernate: http://www.hibernate.org

[17] OpenCRX: http://www.linuxmagazine.com.br/article/forte_nao_gordo

[18] Jetty: http://jetty.mortbay.org

[19] Hsqldb: http://hsqldb.org/

Monitoramento de servidores remotos com IPMI

Observador de máquinas

O IPMI, Intelligent Platform Management Interface, permite o monitoramento do estado de servidores remotos, mesmo quando desligados.

por Justin Penney

O ambiente Linux oferece diversas técnicas para monitorar e gerenciar sistemas remotos, mas a administração remota convencional utiliza conexões com o sistema operacional da máquina remota. O que acontece quando a máquina a ser monitorada está desligada ou comprometida de alguma forma?

A *Intelligent Platform Management Interface* (IPMI)[1] é uma interface para monitorar e controlar o hardware de computadores independentemente do sistema operacional. Quando o sistema está inativo, é possível usar o IPMI para ligar ou desligar o computador. O IPMI também oferece acesso a várias outras informações e configurações de hardware que podem não ser acessíveis a ferramentas-padrão de gerenciamento. A interface IPMI controla a energia, lê sensores ambientais e até redireciona o console do sistema através da rede. Essa tecnologia requer o suporte por parte do fabricante da placa-mãe ou do computador.

A configuração inicial do IPMI costuma ser complexa e frustrante, mas o esforço é compensado na primeira vez em que o IPMI evita uma viagem do administrador ao datacenter.

A especificação IPMI atual está na versão 2.0. As interfaces da versão 1.5 ainda são comuns, assim como controladores com uma mistura de recursos de ambas versões. Essas versões mistas, comumente chamadas de *IPMI v1.5/2.0*, geralmente fornecem mecanismos criptografados de autenticação mais robustos, assim como o suporte a *Serial Over LAN* (SOL).

BMC

O sistema IPMI é baseado num componente de hardware conhecido como *Baseboard Management Controller* (BMC). O BMC recebe informações a partir de outros controladores periféricos, localizados no chassi, e serve como ponto de contato para a comunicação remota. Alguns computadores montados – ou os *barebones* – possuem essa funcionalidade IPMI embutida. Placas-mãe disponíveis no varejo normalmente têm um BMC IPMI por meio de um slot SO-DIMM, PCI ou cabo chato.

O uso da interface LAN varia entre fabricantes. Alguns produtos oferecem uma porta LAN conectada diretamente ao BMC; outros usam uma porta LAN da placa-mãe. Um terceiro tipo utiliza uma porta da placa-mãe, mas intercepta a comunicação IPMI enquanto lida com o restante do tráfego de rede com o driver da LAN. Essa técnica, chamada de *pass-through*, exige a cooperação do driver da LAN, o que pode ou não ser uma dificuldade no Linux.

Configuração inicial

A configuração inicial de uma interface IPMI varia bastante entre fabricantes. Algumas são bem polidas, demandando pouco mais que especificar um IP, enquanto outras possuem vários componentes de *firmware* que precisam ser modificados (por *flash*) e configurados em múltiplos locais.

O projeto *OpenIPMI*[2] oferece um driver IPMI para Linux que funciona com alguns BMCs.

IPMItool

O utilitário de linha de comando do Linux *IPMItool* permite a configuração e comunicação com sistemas equipados com IPMI. Várias das principais distribuições Linux incluem pacotes com esse utilitário e seu código-fonte está disponível no site do projeto[3]. A ferramenta fornece vários comandos para comunicação com a infra-estrutura IPMI (**tabela 1**).

Após um BMC ser configurado localmente, pode-se usar o IPMItool para configurar a interface LAN (**exemplo 1**).

O verdadeiro poder do IPMI está na interface LAN. Depois que ela for configurada, o BMC responderá a requisições remotas enquanto o sistema estiver recebendo energia (*standby*

Exemplo 1: Informações da interface LAN

```
01 ipmitool -I open lan set  <canal> ipaddr <IP>
02 ipmitool -I open lan set  <canal> netmask <máscara>
03 ipmitool -I open lan set  <canal> defgw <gateway padrão>
```

Tabela 1: Alguns comandos do IPMItool

Comando	Efeito
`sol activate`	Inicia uma sessão SOL.
`lan print`	Exibe informações da LAN.
`chassis status`	Exibe o estado da energia e do chassi.
`power`	Controle de energia (`on`, `off`, `cycle`, `reset`, `diag`).
`sensor`	Exibe informações do sensor ambiental.
`sensor get <nome do sensor>`	Obtém os valores do sensor informado.
`sel list`	Exibe o log de eventos do sistema.
`sel clear`	Limpa o log de eventos do sistema.
`mc info`	Exibe informações sobre o BMC.
`mc reset` <warm ou cold>	Reinicia o BMC.

incluído). O BMC fornece o controle remoto de energia, dá acesso a configurações de BIOS, monitora sensores ambientais, acessa o console e, em alguns casos, suporta até KVM (teclado, vídeo e mouse) sobre IP.

Alguns fabricantes suportam *mídias virtuais* que permitem a emulação de disquetes USB e leitores de CD; isso geralmente requer um utilitário – fornecido pelo fabricante – na máquina cliente, que pode ou não ser suportado no ambiente Linux.

A interface LAN da versão 2.0 do IPMI é chamada de *lanplus* pelo *ipmitool*, enquanto a interface da versão 1.5 é referida apenas como *lan*. A maioria dos controladores de gerenciamento atuais suporta a especificação 2.0 e usa a interface *lanplus*. No caso de máquinas com BMCs mistos 1.5/2.0, caso a interface *lanplus* não retorne resposta, deve-se tentar a interface *lan*.

Conexões com o BMC começam com a especificação da interface – *lanplus*, no caso –, o IP e o nome de usuário. Em nosso exemplo, a opção `-a` faz o *ipmitool* pedir a senha:

```
ipmitool -I lanplus -U
➥<usuário> -a -H <IP>
```

Um teste simples para a interface é retornar o estado de energia da máquina:

```
ipmitool -I lanplus -U
➥admin -a -H
➥192.168.2.1 chassis
➥power status
Password:
Chassis Power is off
```

A máquina está desligada. Para ligá-la, basta o comando:

```
ipmitool -I lanplus -U admin -a -H
➥192.168.2.1 chassis power on
```

A **tabela 1** e a documentação do IPMItool detalham outros comandos.

Serial pela LAN

O protocolo SOL oferece aos administradores o mesmo acesso a um computador que teriam por meio de um teclado e um monitor diretamente conectados à máquina. O SOL requer que a BIOS, o carregador de inicialização e o sistema operacional estejam configurados adequadamente.

A configuração da BIOS deve conter uma seção intitulada *remote console*, *serial console* ou algo nessa linha e o manual do BMC especificará as configurações necessárias. Uma vez configurado, será possível ver todas as mensagens do *POST*; também é possível entrar na configuração da BIOS através do console SOL.

É importante atentar à saída na tela, durante o POST, pois algumas teclas – principalmente [**Del**] e [**F9**] a [**F12**] – são atribuídas diferentemente. Se [**Del**] costuma ser usado para entrar na configuração da BIOS, talvez seja necessário pressionar [**F4**]. Esse tipo de mapeamento é informado, geralmente, nas linhas que contêm *on remote keyboard* (**figura 1**).

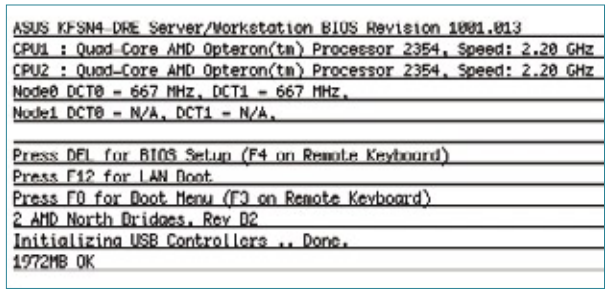


Figura 1 Saída do *POST* da BIOS.

O *Grub* precisa ser configurado para exibir a interface do SOL. A **figura 2** mostra o arquivo `/boot/grub/grub.conf` configurado para um console serial através da *COM2*.

O acesso ao Grub pelo console-padrão será permitido se for pressionada uma tecla, no intervalo de

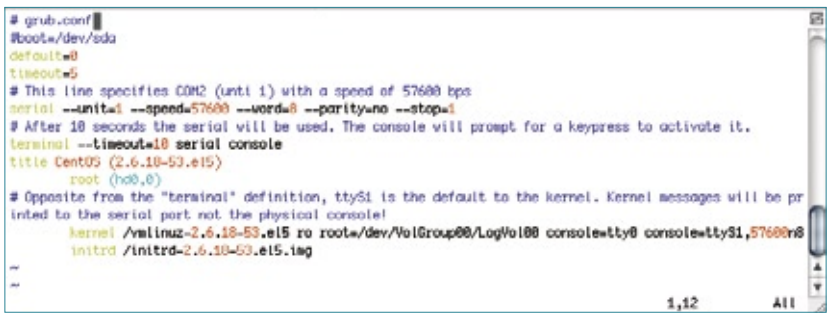


Figura 2 A *ttyS1* é especificada para o console do sistema.

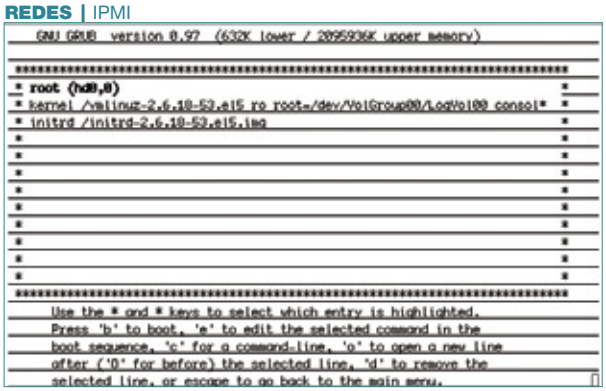


Figura 3 *Grub* sobre SOL.

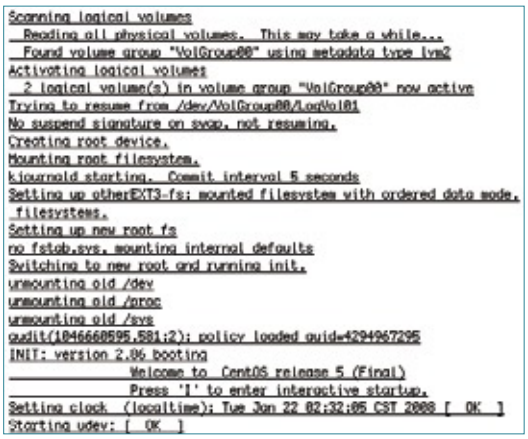


Figura 4 As mensagens do kernel e do *init* são exibidas por SOL.

dez segundos, em um teclado ligado diretamente à máquina. Com um monitor conectado diretamente à máquina, a mensagem "Press any key to continue" é exibida uma vez a cada segundo durante o período de espera. A **figura 3** mostra um exemplo do Grub sobre a interface SOL.

Quase toda a saída durante o processo de inicialização será exibida no console-serial (**figura 4**) em vez de no console padrão. Quando um monitor estiver conectado, serão mostradas apenas algumas mensagens e depois o console não responderá até que os programas *getty* iniciem os dispositivos normais de console, o que pode causar confusão e frustração ao tentar diagnosticar um computador mal comportado.

Para evitar o redirecionamento do console, basta retirar da linha do kernel no Grub o termo `console`. Após a edição da linha do kernel, pode-se iniciá-lo.

Última etapa

O último passo é configurar um getty para exibir um prompt de login pelo console serial. A maioria das distribuições Linux trazem o *agetty*, que é o mais comumente usado em consoles seriais. Iniciar um novo getty é simples; basta adicionar uma linha ao arquivo `/etc/inittab`:

```
s0:2345:/sbin/agetty ttyS1
➥ 57600 vt100
```

Para impedir o agetty de tentar detectar a linha no console serial, pode ser necessário acrescentar o argumento `-L`.

Adicionar `ttyS1` ao arquivo `/etc/securetty` permite que o usuário root faça o login pelo console serial. Esse arquivo especifica quais dispositivos terminais devem ser considerados seguros o suficiente para login pelo root.

Executar `init -q` como root força o *init* a recarregar sua configuração e iniciar um novo processo do agetty. Nesse ponto, já deve ser possível iniciar uma sessão SOL e acessar a máquina a qualquer momento:

```
ipmitool -I lanplus -U admin -a -H
➥ 192.168.2.1 sol activate
```

Alternativa

Se o sistema em questão não suportar o IPMI, ainda é possível obter algumas das mesmas funcionalidades por meio de outras ferramentas. Por exemplo, o controle de energia e o suporte ao console serial são possíveis com uso de hardware externo. Unidades de energia controladas por rede, como o PDU (unidade distribuidora de energia) Switched Rack da APC ou o Sentry, da Server Technologies, permitem que seja ligado, desligado ou reiniciado qualquer dispositivo conectado a eles.

Servidores de console serial, tais como os da Avocent e Open Gear, permitem o acesso ao console pela porta serial da placa-mãe. Sua configuração é semelhante àquela para o suporte a porta serial com IPMI. Algumas placas-mãe permitem também o redirecionamento da BIOS. Diferentemente do IPMI, as interfaces para esses dispositivos não seguem o padrão, impossibilitando o uso de instruções genéricas.

Conclusões

Como os processos de cada fabricante são diferentes, é preciso seguir suas instruções.

Fazer a configuração inicial de uma implementação de IPMI pode ser um desafio; porém, esse trabalho, junto com o planejamento, pode economizar um tempo considerável em caso de falha.

A possibilidade de visualizar os erros do POST ou dos estágios iniciais de carregamento do kernel pode ser fundamental na tarefa de diagnóstico de um servidor problemático. ■

Mais informações

[1] Especificação da IPMI: http://download.intel.com/design/servers/ipmi/IPMIv2_0rev1_0.pdf

[2] OpenIPMI: http://openipmi.sourceforge.net/

[3] IPMItool: htpp://ipmitool.sourceforge.net/

Sobre o autor

Justin Penney começou a usar Linux por hobby em 1997 e agora projeta clusters computacionais de alta performance.

David Ritter - www.sxc.hu

O simples e eficaz DenyHosts

Nem adianta insistir

O script DenyHosts verifica os logs do servidor em busca de ataques. Quando encontra uma máquina agressora, bloqueia e denuncia o agressor para toda uma rede internacional.

por Frederico Madeira

Todo administrador de redes Linux precisa ter acesso remoto aos servidores, de alguma forma, para realizar tarefas administrativas ou de suporte. O SSH geralmente requer que o servidor fique exposto a toda a Internet. Com o acesso por senha, o servidor SSH fica vulnerável a ataques de dicionário (força bruta), nos quais o agressor tenta, exaustivamente, inúmeras combinações de usuário e senha até que encontre o par correto e ganhe acesso à shell do servidor.

Uma forma de proteção do serviço SSH contra ataques desse tipo é a utilização de ferramentas como o *DenyHosts*. Trata-se de um script que pode ser executado pelo administrador para monitorar o arquivo de log `/var/log/secure` (no *Red Hat* ou no *Fedora*) ou ainda o `/var/log/auth.log` (no *Mandriva*) em busca das mensagens de tentativa de acesso negadas. O DenyHosts se integra aos *tcpwrappers*, adicionando entradas em `/etc/hosts.deny` toda vez que detecta que um determinado host teve uma certa quantidade de autenticações negadas durante um período de tempo definido pelo administrador.

Instalação

A instalação do DenyHosts é bastante simples. Primeiramente, é necessário baixar em [1] o pacote do programa. Caso se opte pelo pacote `.tar.gz`, é necessário fazer a instalação manualmente, como mostra o **exemplo 1**. Nesse caso, o programa estará acessível pelo diretório `/usr/share/denyhosts/`, devendo-se entrar nessa pasta para editar o arquivo de configuração `denyhosts.cfg`, conforme o **exemplo 2**. Felizmente, o programa já traz um arquivo `denyhosts.cfg-dist` repleto de comentários explicativos. Isso permite uma configuração ainda mais precisa do que a apresentada no **exemplo 2**.

Exemplo 1: Instalação manual do DenyHosts

```
# cd /usr/local/src
# tar xvfz DenyHosts-2.6.tar.gz
# ln -s /usr/local/src/DenyHosts-2.6 /usr/share/denyhosts
# ln -s /usr/local/src/DenyHosts-2.6/denyhosts.py /usr/bin
```

Tabela 1: Unidades de tempo

Valor a ser utilizado	Descrição
s	segundos
m	minutos
h	horas
d	dias
w	semanas
y	anos

Exemplo 2: Arquivo de configuração

```
# Arquivo de LOG a ser verificado
SECURE_LOG = /var/log/secure
# Arquivo com os hosts a bloquear
HOSTS_DENY = /etc/hosts.deny
# Limpar esse arquivo a cada 2 dias
PURGE_DENY = 2d
# Qual serviço deve ser bloqueado?
BLOCK_SERVICE  = sshd
# Quantos logins inválidos DE USUÁRIOS INEXISTENTES caracterizam um ataque?
DENY_THRESHOLD_INVALID = 5
# Quantos logins inválidos DE USUÁRIOS EXISTENTES caracterizam um ataque?
DENY_THRESHOLD_VALID = 10
DENY_THRESHOLD_ROOT = 1
# Denunciar logins inválidos vindos de máquinas válidas?
SUSPICIOUS_LOGIN_REPORT_ALLOWED_HOSTS=YES

############ PARÂMETROS OPCIONAIS ############
# Informações de email para os alertas.
ADMIN_EMAIL = admin@dominio.com.br
SMTP_HOST = mail.dominio.com.br
SMTP_PORT = 25
SMTP_FROM = DenyHosts
SMTP_SUBJECT = Informativo do DenyHosts

######### PARÂMETROS DO MODO DAEMON ##########
# Arquivo de log para o modo daemon
DAEMON_LOG = /var/log/denyhosts
# Intervalo de tempo para verificar o arquivo de log.
DAEMON_SLEEP = 30s
# Intervalo para limpeza da lista de bloqueados.
DAEMON_PURGE = 1h
```

Os campos que recebem valores de tempo merecem uma explicação mais detalhada. Neles, é possível definir as unidades de tempo, de acordo com a **tabela 1**. Se o período for deixado em branco, o valor assumido será o de segundos.

Existem duas formas de se executar o DenyHosts [2]. Na forma independente, ou *Standalone*, a ferramenta só será executada quando for solicitado pelo administrador. Já na forma *Daemon*, o programa é executado continuamente, porém, em segundo plano, verificando o arquivo de log.

Independente

Para executar o DenyHosts em modo Standalone, é necessário chamar o comando `denyhosts.py` com a opção `-c /diretório/do/denyhosts/denyhosts.cfg`. Com isso, o programa analisará o arquivo de log definido na variável `SECURE_LOG`, exibirá alguma saída na tela, criará a pasta `/usr/share/denyhosts/data/` e, dentro dela, criará seus arquivos de controle. Após a análise do arquivo, o DenyHosts adicionará as máquinas bloqueadas ao arquivo `/etc/hosts.deny`. Se o acesso ao serviço SSH for bloqueado para os IPs 123.123.123.1 e 234.234.234.2, o arquivo `deny.hosts` deverá receber as linhas:

```
sshd: 123.123.123.1
sshd: 234.234.234.2
```

É indicado que o DenyHosts seja executado periodicamente, de forma que possa atualizar as entradas em `/etc/deny.hosts` com os IPs dos novos aspirantes a invasores. Para isso, uma boa estratégia é usar o *Crontab* para disparar o programa em intervalos de tempo definidos.

Daemon

O uso do modo daemon requer que sejam observadas as configurações, no arquivo `denyhosts.cfg`, das opções `DAEMON_LOG`, `DAEMON_SLEEP` e `DAEMON_PURGE`. Além disso, é interessante que o daemon do DenyHosts seja iniciado junto com o sistema.

Para isso, primeiramente vamos criar um link simbólico em `/etc/init.d/` para o script de inicialização, afim de que ele seja encontrado dentro da pasta de scripts de inicialização de serviços do sistema:

```
# ln -s /usr/share/
➥denyhosts/daemon-
➥control-dist /etc/init.
➥d/DenyHosts
```

Em seguida, vamos configurá-lo para ser carregado nos runlevels 2, 3, 4 e 5:

```
# /sbin/chkconfig --level 2345
➥DenyHosts on
```

O próximo passo é configurar o script de inicialização (`/etc/init.d/DenyHosts`). Para tanto, basta editá-lo e configurar algumas variáveis com os caminhos referentes ao sistema, como mostra o **exemplo 3**.

Feito isso, o DenyHosts já estará pronto para ser iniciado, o que pode ser feito com o comando `/etc/init.d/DenyHosts start`.

Testes

Para testar o correto funcionamento do DenyHosts, serão necessárias duas estações que tenham permissão para se conectarem ao servidor

testado. A primeira terá o acesso bloqueado, enquanto a segunda poderá desbloquear a primeira estação.

De acordo com as configurações da máquina protegida, um usuário válido será bloqueado após errar a senha por dez vezes. Dessa forma, vamos tentar realizar o login no servidor (digitando a senha incorreta, claro) até a primeira máquina ser bloqueada.

Logo em seguida, o arquivo `/var/log/denyhosts` deve listar o que fez quanto à profusão de senhas erradas:

```
INFO new denied hosts:
➥['192.168.0.100']
```

Como esperado, o daemon bloqueou a máquina que tentou fazer os acessos indevidos.

Defesa mundial

O DenyHosts ainda possui a interessante capacidade de delatar para todo o mundo os hosts bloqueados com ele. Assim, é possível formar uma rede mundial de defesa contra invasores. Com isso, um servidor nem precisa esperar que um agressor erre a senha. O sistema mundial de linha de defesa funciona com o DenyHosts enviando periodicamente a base de hosts bloqueados por ele para um servidor central, e baixando a lista atualizada colaborativamente por outros servidores ao redor do planeta. Para ativar esse recurso, basta descomentar as seguintes linhas no arquivo de configuração:

```
SYNC_SERVER = http://xmlrpc.
➥denyhosts.net:9911
SYNC_DOWNLOAD = yes
SYNC_UPLOAD = yes
```

Embora a colaboração global de defesa seja interessante, é possível que ela transmita informações pouco confiáveis. Uma máquina que tenha sido bloqueada por um único daemon do DenyHosts mal configurado vai acabar sendo bloqueada por todos os colaboradores da rede. Para evitar isso, é interessante filtrar as informações recebidas do servidor central. Para somente considerar nocivas as máquinas que tenham sido bloqueadas por cinco serviores mundo afora, basta definir o parâmetro `SYNC_DOWNLOAD_THRESHOLD` da seguinte forma:

```
SYNC_DOWNLOAD_THRESHOLD = 5
```

Outro recurso importante para a filtragem de hosts bloqueados é `SYNC_DOWNLOAD_RESILIENCY`. Esse parâmetro define quanto tempo um host agressor da rede de defesa precisa ficar ativo para ser bloqueado também localmente. Ou seja, se seu valor for `2d`, isso significa que, após o DenyHosts local baixar do servidor central a lista de agressores, ele só vai bloquear aqueles hosts que estiverem realizando ataques há mais de dois dias. Nesse campo, as unidades de tempo também seguem o padrão descrito na **tabela 1**.

Conclusões

O daemon do DenyHosts apresenta bom desempenho sem utilizar muitos recursos da máquina ou afetar outros sistemas que estejam rodando nela. Por isso, ele se apresenta como uma ferramenta rápida e versátil para compor as medidas de segurança de qualquer servidor SSH.

Outra forma interessante de usar a ferramenta é em *honeypots*, espalhados em grandes redes. Dessa forma, é possível traçar estatísticas e padrões de ataques desferidos. As estatísticas do servidor central do Denyhosts pode ser visualizada em [3], sendo possível até mesmo montar um mapa com os principais pontos de ataque. Esse mapa é criado por meio da integração das detecções com projetos como o IP2location[4] e o MaxMind[5]. ■

Exemplo 3: Variáveis do script de inicialização

```
DENYHOSTS_BIN   = "/usr/bin/denyhosts.py"
DENYHOSTS_LOCK  = "/var/lock/subsys/denyhosts"
DENYHOSTS_CFG   = "/usr/share/denyhosts/denyhosts.cfg"
```

Mais informações

[1] Download do DenyHosts: http://sourceforge.net/project/showfiles.php?group_id=131204

[2] DenyHosts FAQ: http://denyhosts.sourceforge.net/faq.html

[3] Página de estatísticas das detecções submetidas ao servidor central: http://stats.denyhosts.net/stats.html

[4] Projeto IP2location: http://www.ip2location.com/

[5] Projeto MaxMind: http://www.maxmind.com/app/ip-location

Sobre o autor

Frederico Madeira (fred@madeira.eng.br) é formado em Engenharia Eletrônica e pós-graduado em Segurança de Redes em Computadores. É professor universitário, tem certificações CCNA e LPIC-1 e participa ativamente do projeto Fedora.

Firewall fácil com o Shorewall

Domando o fogo, parte 2

Na segunda parte de nosso tutorial de uso do poderoso Shorewall, aprenda a criar um firewall mais complexo e a proteger sua rede com muita praticidade.

por Tarcísio C. Espínola

Ramon Gonzalez - www.sxc.hu

O primeiro artigo desta série[1] apresentou o *Shorewall*, uma solução de Código Aberto para criação e gerenciamento de firewalls em diversos sistemas operacionais, incluindo, é claro, o Linux. Neste segundo artigo, vamos explicar algumas configurações mais avançadas dessa poderosa ferramenta.

Mascaramento

Para que o servidor firewall (veja na **figura 1**) funcione como um roteador e permita a passagem de pacotes entre as zonas *LOC* (rede local) e *NET* (a Internet), é necessário ativar o encaminhamento (*forward*) e o mascaramento (*postrouting*) entre as suas respectivas interfaces. No Shorewall, essa configuração deve ser feita no arquivo `/etc/shorewall/masq`, como no **exemplo 1**.

Com essa configuração, ativamos o encaminhamento das requisições vindas da interface da rede local (`eth1`) para a interface da Internet (`eth0`), assim como seu mascaramento. Não é necessário ativar o roteamento entre as zonas *DMZ* e *NET*; para isso, usaremos outra técnica: *Proxyarp*. Neste artigo, vamos abrir apenas os aspectos mais relevantes no contexto local O manual do arquivo de configuração (`man shorewall-masq`) contém todos os detalhes.

Proxyarp

O Shorewall não exige qualquer configuração do tipo *DNAT*, em que as requisições ao servidor firewall são desviadas para máquinas internas para montar uma DMZ. Por meio da função Proxyarp, cada servidor da DMZ será configurado com o seu próprio IP fixo e válido, pertencente à mesma rede do IP válido do servidor firewall. Isso significa que é como se cada servidor da DMZ estivesse conectado diretamente ao roteador, exatamente como fizemos com a interface `eth0` do servidor firewall[1].

Assim, poderemos adicionar facilmente mais servidores à DMZ sempre que necessário, bastando, para isso, configurá-los com os IPs fornecidos pela operadora e conectá-los no mesmo switch dos demais membros da DMZ. O limite, como se vê, é o número de endereços disponibilizados pela operadora. Vale lembrar que a interface `eth2` do servidor firewall também deverá estar conectada a esse switch.

Para configurar o Proxyarp, é preciso definir no arquivo `/etc/shorewall/proxyarp` os IPs de cada servidor da DMZ. Os servidores *mail.meu_site.com.br* e `www.meu_site.com.br`, em nosso exemplo

Exemplo 1: Mascaramento

```
#INTERFACE  SOURCE  ADDRESS  PROTO  PORT(S) IPSEC  MARK
eth0        eth1
# Não apagar esta última linha.
```

Exemplo 2: Configuração do Proxyarp

```
#ADDRESS      INTERFACE  EXTERNAL  HAVEROUTE  PERSISTENT

# servidor mail.meu_site.com.br:
200.166.161.194  eth2       eth0      no
# servidor www.meu_site.com.br:
200.166.161.195  eth2       eth0      no
# Não apagar esta última linha.
```

(**figura 1**) deveriam ser configurados conforme o **exemplo 2**.

Note que a opção `INTERFACE` precisa representar a interface do servidor firewall que foi vinculada à zona DMZ, enquanto a opção `EXTERNAL` sinaliza a interface do servidor firewall ligada à zona NET. A opção `HAVEROUTE` deve ser definida como `no` para que o próprio Shorewall se encarregue de criar as rotas para os servidores da DMZ na tabela de roteamento do servidor firewall.

Arquivo de configuração

Com a DMZ definida com facilidade, vamos agora definir algumas configurações específicas do Shorewall que devem ser realizadas em seu arquivo de configuração `/etc/shorewall/shorewall.conf`. Nele, são definidos alguns parâmetros utilizados na inicialização do firewall e, para o nosso exemplo, será necessário alterar as seguintes opções:

- `STARTUP_ENABLED=Yes`: Permite que o Shorewall seja iniciado;
- `SHOREWALL_COMPILER=perl`: Define o interpretador que será utilizado pelo Shorewall na compilação de suas regras (uma novidade na versão 4). A opção `perl` é a mais recente e também muito rápida. No entanto, ainda existem algumas restrições ao seu uso. A opção `shell` é mais antiga e lenta, e será descontinuada no futuro. Em nosso exemplo, usaremos `perl`;
- `DISABLE_IPV6=No`: Por padrão, o suporte ao protocolo IPv6 vem desativado no Shorewall, o que gera uma mensagem de alerta durante a compilação em distribuições como *RHEL*, *Fedora* e *CentOS*. Já no *Debian* e no *Ubuntu*, não existe esse problema.

Como em todos os outros arquivos de configuração citados, a página de manual do `shorewall.conf` (`man shorewall.conf`) lista todas as suas funcionalidades.

Regras

As regras do firewall são a parte que pode mudar com freqüência, diferentemente de todas as configurações até agora realizadas.

O firewall construído até aqui já pode ser iniciado, mas suas regras de política impedirão a passagem de qualquer tráfego entre zonas diferentes. É no arquivo de regras, `rules`, que são definidos os serviços que cada zona poderá acessar nas demais, da liberação de endereços e portas. Isso exige um estudo minucioso de cada regra, o que pode ser inconveniente a princípio, mas é muito importante.

A sintaxe de cada linha do arquivo de configuração é simples e consiste em informar a ação a ser tomada, origem e destino do pacote, seu protocolo e sua porta de destino. Vejamos como definir cada um desses campos (a página de manual *shorewall-rules* oferece todos os detalhes).

A **ação** determina o que a regra vai fazer com as conexões que coincidirem com o restante dos campos. As ações mais comuns são *ACCEPT* (aceitar o acesso), *REJECT* (rejeitar o acesso e informar ao solicitante) e *DROP* (simplesmente rejeitar o acesso).

A **origem** representa a zona e, opcionalmente, a máquina que acessará o serviço. Caso a máquina seja omitida, a regra será válida para todas as máquinas daquela zona. É permitido o uso do curinga *all* para representar todas as zonas.

O **destino** define a zona à qual pertence o serviço. Assim como no campo *origem*, pode-se especificar também a máquina nesse campo. Da mesma forma, o curinga *all* também

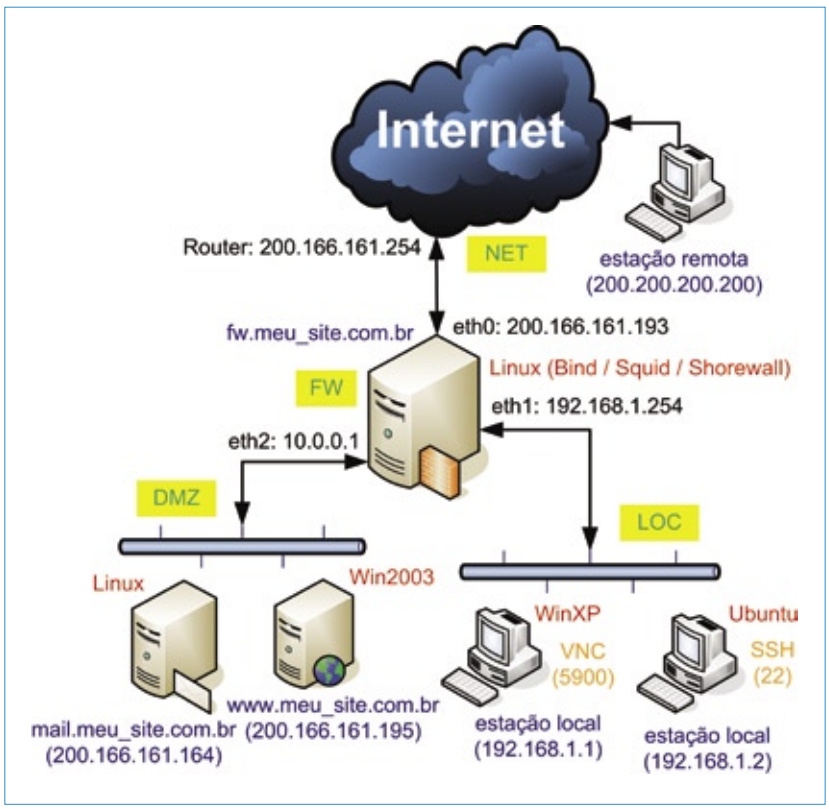


Figura 1 A rede padrão numa pequena empresa usada neste artigo possui dois servidores numa DMZ e duas estações na rede interna, ambas conectadas ao firewall, que as liga à Internet.

pode ser usado para representar todas as zonas.

No campo **protocolo**, auto-explicativo, as possibilidades são *tcp*, *udp* e *icmp*.

O campo **porta de destino** informa a(s) porta(s) afetada(s) pela regra. É permitido usar uma porta ou uma faixa de portas separadas por dois pontos, como `1024:1050`, por exemplo. Caso seja omitida a primeira ou a última porta na faixa, a porta 0 será usada como primeira ou a 65535 será considerada a última. Com `0:`, representamos todas as portas.

É importante ter em mente que um host pode representar tanto uma estação quanto um servidor, e que podemos utilizar tanto IPs quanto nomes totalmente qualificados em nossas regras.

Zona LOC

Vamos começar pelas regras referentes à zona LOC, definindo quais serviços suas estações devem conseguir acessar em cada uma das outras zonas.

O **exemplo 3** exibe o trecho inicial do arquivo `rules`, incluindo as definições de regras da zona LOC. Nos destinos da zona DMZ (**linhas 9 a 19**), está permitido o acesso aos serviços SSH (porta 22), SMTP (25), POP (110) e IMAP (445) no servidor *mail.meu_site.com.br*, e somente aos serviços web (portas 80 e 443) no servidor `www.meu_site.com.br`. Por último, fica permitido o uso do ping e mensagens de erro ICMP a partir de qualquer máquina da zona LOC para qualquer servidor da zona DMZ.

Note que nessas regras foi usada uma macro do Shorewall para facilitar ainda mais a escrita de regras. Com elas, podemos digitar, na **linha 16**:

```
Web/ACCEPT   loc   dmz:www.meu_
➥site.com.br
```

em vez de:

```
ACCEPT   loc   dmz:www.meu_site.
➥com.br   tcp   80
ACCEPT   loc   dmz:www.meu_site.
➥com.br   tcp   443
```

Existem macros para a maioria dos serviços mais comuns, o que realmente ajuda muito o administrador a usar melhor seu tempo. Elas estão disponíveis no diretório `/usr/share/shorewall/`.

Exemplo 3: Arquivo de regras, rede local

```
001 #ACTION  SOURCE  DEST  PROTO  DEST  SOURCE  ORIGINAL  RATE  USER/  MARK
002 #                            PORT  PORT(S) DEST      LIMIT GROUP
003 #SECTION ESTABLISHED
004 #SECTION RELATED
005 SECTION NEW
006
007 ###### Acessos da Zona LOC (Rede local)
008
009 ## Regras: LOC -> DMZ ##
010 # de todas as estações locais -> para mail.meu_site.com.br
011 SSH/ACCEPT      loc     dmz:mail.meu_site.com.br
012 SMTP/ACCEPT     loc     dmz:mail.meu_site.com.br
013 POP/ACCEPT      loc     dmz:mail.meu_site.com.br
014 IMAP/ACCEPT     loc     dmz:mail.meu_site.com.br
015 # de todos os hosts da LOC -> para www.meu_site.com.br
016 Web/ACCEPT      loc     dmz:www.meu_site.com.br
017 # de todos os hosts da LOC -> para: todos os hosts da DMZ
018 Ping/ACCEPT     loc     dmz
019 AllowICMPs      loc     dmz
020
021 ## Regras: LOC -> NET ##
022 # acesso total do host Ubuntu (tcp/udp) -> para: todos os hosts da NET.
023 ACCEPT        loc:192.198.1.2   net   tcp   0:  # todos os serviços tcp
024 ACCEPT        loc:192.198.1.2   net   udp   0:  # todos os serviços udp
025 # de: todos os hosts da LOC -> para: Redes da CEF.
026 Web/ACCEPT      loc     net:200.201.166.0/24
027 Web/ACCEPT      loc     net:200.201.173.0/24
028 Web/ACCEPT      loc     net:200.201.174.0/24
029 # de: todos os hosts da LOC -> para: todos os hosts da NET.
030 SSH/ACCEPT      loc     net
031 ACCEPT          loc     net     tcp     3456   # ReceitaNet
032 Ping/ACCEPT     loc     net
033 AllowICMPs      loc     net
034
035 ## Regras: LOC -> FW ##
036
037 # de: todos os hosts da LOC -> para: FW.
038 DNS/ACCEPT      loc     fw
039 SSH/ACCEPT      loc     fw
040 ACCEPT          loc     fw      udp     67     # DHCP Server
041 Ping/ACCEPT     loc     fw
042 AllowICMPs      loc     fw
```

As **linhas 21 a 33** do **exemplo 3** mostram que a estação com IP terminando em `.2` pode acessar qualquer serviço na zona NET, enquanto as demais estações têm permissão para acessar apenas os serviços web dos servidores da Caixa Econômica Federal, que se encontram nas sub-redes 200.201.166.0/24, 200.201.173.0/24 e 200.201.174.0/24. Além disso, todas as estações de LOC podem acessar os serviços SSH, *ReceitaNet* e ICMP.

Os acessos da zona LOC à zona FW são definidos nas **linhas 35 a 42** e permitem o tráfego dos serviços DNS, SSH, DHCP e ICMP.

Zona DMZ

Os servidores da DMZ somente terão acesso a serviços estritamente necessários: web na Internet, para o download de atualizações, e DNS no servidor firewall, além de ICMP nas duas zonas, como mostra o **exemplo 4**.

Note a facilidade para bloquear o acesso da zona DMZ à zona LOC: basta não permitir nada (**linha 60**), pois nossa política padrão já está definida para barrar esse tipo de acesso. O motivo dessa proibição de acesso é que, caso um servidor da DMZ seja invadido, este não terá acesso algum às estações da rede local.

Acesso remoto

É raro oferecer algum serviço nas estações da rede local. Uma possível exceção, no entanto, é o acesso remoto à área de trabalho, muito útil quando se está viajando, por exemplo. O **exemplo 5** mostra como permitir que uma estação remota na Internet (com IP 200.200.200.200) tenha acesso ao serviço *VNC* que será executado na estação *WinXP* e ao serviço *SSH* da estação Ubuntu, ambos na zona LOC.

Nas **linhas 67 e 70**, usamos o DNAT para permitir que as requisições feitas ao servidor nas portas 5900 e 2222 sejam redirecionadas, respectivamente, para as estações WinXP e Ubuntu, nas portas 5900 e 22. Além disso, o início das duas regras informa que tudo será registrado nos logs (`info`).

A sintaxe das regras do tipo DNAT é diferente da sintaxe padrão de regras de simples filtragem. Uma regra de DNAT exige os campos **ação**, **zona:máquina**, **destino:máquina:porta**, **protocolo** e portas de **origem** e **destino**.

É importante ressaltar que acessos do tipo DNAT às estações locais devem ser utilizados com bastante cautela, pois pode expor uma zona inteira ao acesso de invasores.

No acesso à DMZ, por outro lado, é necessário permitir o tráfego dos serviços oferecidos publicamente pelos servidores (**linhas 72 a 81**). Note, no entanto, que não permitimos o serviço SSH externamente, por medida de segurança.

Exemplo 4: Arquivo de regras, servidores

```
044 ###### Acessos da Zona DMZ
045
046 ## Regras: DMZ -> NET ##
047 # de: todos os hosts da DMZ
    -> para: todos os hosts da NET.
048 Web/ACCEPT      dmz     net
049 Ping/ACCEPT     dmz     net
050 AllowICMPs      dmz     net
051
052 ## Regras: DMZ -> FW ##
053 # de: todos os hosts da DMZ
    -> para: FW.
054 DNS/ACCEPT      dmz     fw
055 Ping/ACCEPT     dmz     fw
056 AllowICMPs      dmz     fw
057
058 ## Regras: DMZ -> LOC ##
059 # Acesso não permitido.
060
```

Exemplo 5: Arquivo de regras, acesso remoto

```
061 ###### Acessos da Zona NET (Internet).
062
063 ## Regras: NET -> LOC ##
064 # Atenção: Use estas regras com cautela!
065 # redirecionamento,
066 # de: fw.meu_site.com.br:5900 -> para: 192.168.1.1:5900 (WinXP)
067 DNAT:info net:200.200.200.200 loc:192.168.1.1:5900 tcp 5900 - fw.meu_site.com.br -  -
068 # redirecionamento,
069 # de: fw.meu_site.com.br:2222 -> para: 192.168.1.2:22 (Ubuntu)
070 DNAT:info net:200.200.200.200 loc:192.168.1.2:22   tcp 2222 - fw.meu_site.com.br -  -
071
072 ## Regras: NET -> DMZ ##
073 # de: todos os hosts da NET -> para: mail.meu_site.com.br
074 SMTP/ACCEPT     net     dmz:mail.meu_site.com.br
075 POP/ACCEPT      net     dmz:mail.meu_site.com.br
076 IMAP/ACCEPT     net     dmz:mail.meu_site.com.br
077 # de: todos os hosts da NET -> para: www.meu_site.com.br
078 Web/ACCEPT      net     dmz:www.meu_site.com.br
079 # de: todos os hosts da NET -> para: todos os hosts da DMZ.
080 Ping/ACCEPT     net     dmz
081 AllowICMPs      net     dmz
082
083 ## Regras: NET -> FW ##
084 # de: todos os hosts da NET -> para: FW.
085 DNS/ACCEPT      net     fw
086 Ping/ACCEPT     net     fw
087 AllowICMPs      net     fw
```

Exemplo 6: Arquivo de regras, proxy

```
089 ## Redirecionamento (Proxy Transparente) ##
090 ####
091 # Parâmetros para o Squid 2.5 ou anterior:
092 #   http_port 3128
093 #   httpd_accel_host virtual
094 #   httpd_accel_port 80
095 #   httpd_accel_with_proxy  on
096 #   httpd_accel_uses_host_header on
097 #
098 ###
099 # Parâmetros para o Squid 2.6 ou posterior:
100 #   http_port 3128 transparent
101 #
102 ###
103 #
104 REDIRECT  loc  3128 tcp 80 - !200.201.166.0/24,200.201.173.0/24,
➥200.201.174.0/24
105 # Não apagar esta última linha.
```

Para que o site e os emails sejam acessíveis de fora, é necessário também permitir o tráfego do serviço DNS da zona NET para o firewall (**linhas 83 a 87**).

Acesso do firewall

Não precisamos definir regras para a zona FW, pois essa zona foi definida com a *tag* `ACCEPT` no arquivo de políticas para todas as zonas (*all*)[1]. Isso significa que o firewall poderá acessar quaisquer serviços em quaisquer zonas, sem restrições, o que é bastante lógico.

Simples demais

O arquivo de regras parece demasiadamente simples, e de fato é. Tarefas mais complexas, como o controle do estado das conexões, por exemplo, são realizadas automaticamente pelo Shorewall. Além disso, o uso das macros também simplifica a definição de regras para serviços que utilizam múltiplas portas e protocolos.

As regras do tipo DNAT (prerouting) também desfrutam de grande facilidade, pois seu uso dispensa a criação de regras de encaminhamento (*forward*) entre as zonas envolvidas. No *Iptables*, por exemplo, essas regras devem ser criadas manualmente, mas o Shorewall cuida de tudo automaticamente.

Regras de proxy

Um último serviço que ainda não ativamos é o proxy transparente, a ser alojado no servidor firewall[1]. Para ser ativado, precisamos fazer com que o Shorewall redirecione as conexões vindas da rede LOC na 80 para a porta 3128 do servidor firewall (**exemplo 6**, **linha 104**), pois o servidor proxy (*Squid*) está escutando nessa porta no firewall. Porém, precisamos excluir as três faixas de IP da Caixa Econômica, pois elas não passarão pelo proxy, já que foram tratadas de forma específica em um ponto anterior do arquivo de regras (**exemplo 3**).

Iniciando

A última etapa para a ativação do firewall é iniciá-lo. Para isso, basta executar o comando `shorewall start`. Caso toda a configuração esteja em ordem, a palavra "Compiling" será a primeira a aparecer, indicando que o programa está compilando as regras passadas a ele. Por último, a palavra "done" (ou "Shorewall Restarted", caso se use o compilador shell) informa que o firewall já está ativo.

Estendendo

Com a rede funcionando de acordo com a **figura 1**, talvez surja a necessidade de se executar o serviço *Samba* no servidor firewall, por exemplo. Nesse caso, após configurar o Samba no servidor, será necessário dar permissão às estações da rede local para acessarem esses serviços. Para isso, basta adicionar a seguinte regra às configurações de acesso da zona LOC à zona FW no arquivo `rules`:

```
ACTION    SOURCE   DEST
SMB/ACCEPT  loc      fw
```

Feito isso, basta reiniciar o Shorewall com o comando `shorewall restart` para que os usuários da rede local possam acessar os compartilhamentos no servidor.

Conclusão

O Shorewall é uma ótima ferramenta para a criação e a administração de firewalls, não apenas em máquinas dedicadas como também em estações individuais, com uma única interface.

O site do desenvolvedor[2] contém várias informações e dicas sobre a configuração e utilização do Shorewall, além de mostrar o potencial dessa grande ferramenta. ■

Mais informações

[1] Tarcísio C. Espínola, "Domando o fogo". http://www.linuxmagazine.com.br/article/1716

[2] Shorewall: http://www.shorewall.net/

Sobre o autor

Tarcísio Carvalho Espínola é coordenador de TI do Instituto Centec e vem trabalhando na implementação de soluções livres nos servidores da empresa. Em seu tempo livre, mantém o site Opção Linux (http://www.opcaolinux.com.br).

Seu primeiro aplicativo para Android

Programe seu andróide

A plataforma Android, do Google, vai equipar com tecnologia de ponta diversos aparelhos celulares. Veja como é fácil começar a programar aplicativos nela.

por Alessandro de Oliveira Faria

Jean Scheijen – www.sxc.hu

O *Android* é uma plataforma de código aberto para dispositivos portáteis criado pelo Google em parceria com a Open Handset Alliance (OHA). Trata-se de uma aliança para o telefone celular aberto, composta por mais de 30 empresas do mercado de TI que apóiam soluções de código-fonte aberto, como Samsung, Intel, Motorola, Qualcomm e Telefónica. A OHA pretende repetir a estratégia da IBM com a fabricação do PC, composto por partes facilmente adquiridas no mercado.

Essa plataforma funciona como um sistema operacional como os já existentes *Symbian* e *Windows® Mobile*, com a diferença de ser baseado em Código Aberto. Com isso, qualquer desenvolvedor pode criar aplicativos para a plataforma Android. O kit de desenvolvimento do Android provê ferramentas e chamadas via APIs para o desenvolvimento de aplicativos baseados na linguagem Java.

Em outras palavras, trata-se de um pacote com programas para celulares, já com um sistema operacional, *middleware*, aplica-

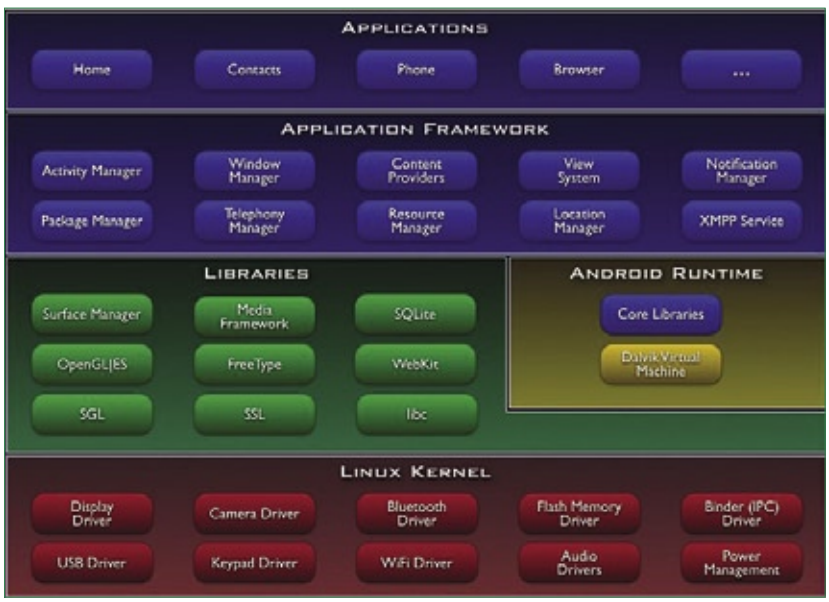


Figura 1 Camadas da plataforma Android.

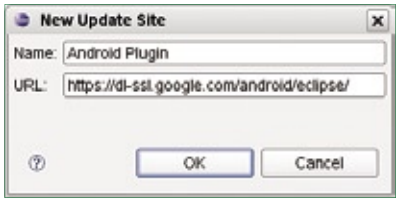


Figura 2 Especificação do site para o plugin

tivos e interface de usuário. Tais recursos permitirão que o Google e outras empresas ofereçam recursos mais ricos aos usuários que se encontram distantes de um computador de mesa.

Os principais recursos dessa plataforma móvel são a máquina virtual otimizada, o navegador integrado, a biblioteca 2D e 3D, o banco *SQLite* e o plugin para o *Eclipse*, chamado *ADT*.

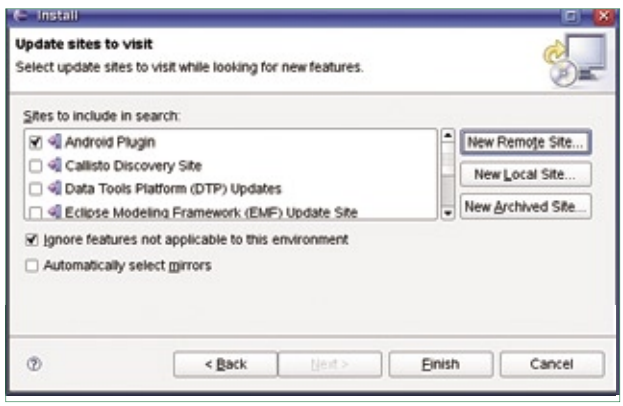


Figura 3 Seleção do novo site.

Arquitetura

A arquitetura do Android é dividida em cinco camadas, organizadas como mostra a **figura 1**: kernel Linux, bibliotecas, ambiente de execução, *framework* e aplicativo.

A camada do **kernel Linux** é composta pelo kernel 2.6 e se responsabiliza pelos serviços, segurança, gerenciamento de memória e processos, rede e drivers. Essa camada também é responsável pela abstração do hardware do dispositivo.

A segunda camada, a de **bibliotecas**, carrega consigo um conjunto de bibliotecas C/C++ utilizadas pelo sistema. Estão incluídas nesse conjunto a biblioteca C padrão (*Libc*) e também aquelas das áreas de multimídia, visualização de camadas 2D e 3D, funções para navegadores web, funções para gráficos, funções de aceleração de hardware, renderização 3D, fontes bitmap e vetorizadas e funções de acesso ao banco SQLite. Todos esses recursos estão disponíveis no framework para o desenvolvimento de aplicativos.

A pequena camada do **ambiente de execução** (*Android Runtime*, na **figura 1**) é uma instância da máquina virtual *Dalvik* criada para cada aplicação executada no Android. A Dalvik é uma máquina virtual com melhor desempenho, maior integração com a nova geração de hardware e projetada para executar várias máquinas virtuais paralelamente. Além disso, é otimizada para consumo mínimo de memória, bateria e CPU.

Sobre essas camadas, localiza-se a camada do **framework** (*Application Framework*, na **figura 1**). Nela, encontramos todas as APIs e os recursos utilizados pelos aplicativos, com classes visuais como botões e *views*, provedor de conteúdo (troca de recursos entre aplicativos) e gerenciadores de recursos, de notificação e de pacotes.

Acima de todas as outras camadas está a de **aplicativos**, na qual se encontram todos os aplicativos (escritos em Java) do Android, como cliente de email, navegador web, contatos e outros. Isso significa que, para desenvolver programas para a plataforma Android, vamos criar os aplicativos em Java na máquina virtual Dalvik.

Exemplo 1: Código do projeto HelloAndroid

```
01 package com.android.hello;
02
03 import android.app.Activity;
04 import android.os.Bundle;
05 import android.widget.TextView;
06
07 public class HelloAndroid extends Activity {
08   /** Called when the activity is first created. */
09   @Override
10   public void onCreate(Bundle icicle) {
11     super.onCreate(icicle);
12     TextView tv = new TextView(this);
13     tv.setText("Ola Mundo - Linux Magazine!");
14     setContentView(tv);
15     }
16 }
```

Instalação e configuração

Para instalarmos o Android, primeiramente devemos efetuar o download do ambiente de desenvolvimento (*Android SDK*) em [1]. Antes de baixar o arquivo, é necessário clicar em "*I agree to the terms of the SDK License*" para aceitar os termos da licença do SDK. Logo em seguida, deve-se selecionar o pacote correspondente ao sistema

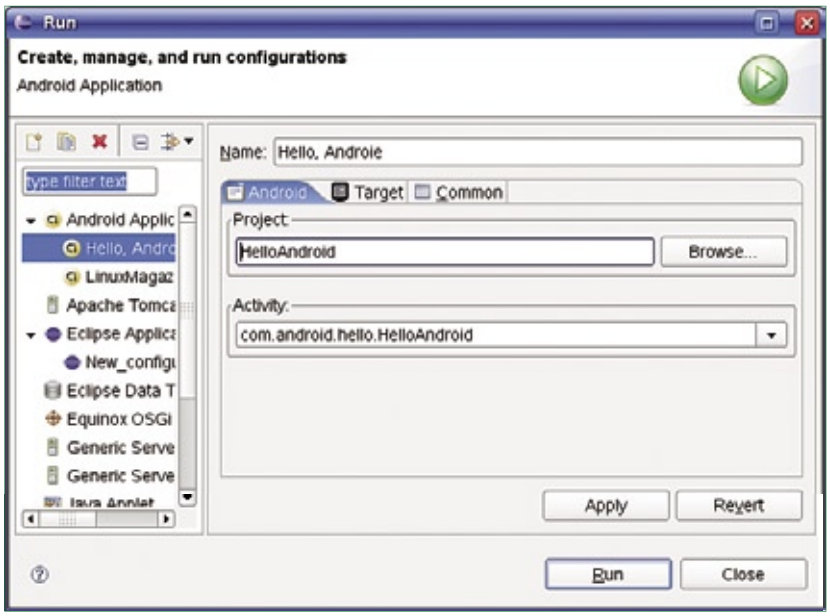


Figura 4 Preparação para execução do novo programa.

operacional (Windows, Mac OS X ou Linux).

Após descompactar o arquivo baixado (formato *ZIP*), é recomendável acrescentar a pasta `tools/` criada no processo à variável `$PATH`, acrescentando ao arquivo `~/.bashrc` a linha:

```
export PATH=${PATH}:/pasta/de/
➥instalação/tools
```

Plugin ADT

O plugin Eclipse para desenvolvimento de aplicativos para o Android no IDE Eclipse se chama *Android Development Tools*, ou *ADT*. Na página do Android é mencionada a compatibilidade com as versões 3.2 e 3.3 do IDE. Para iniciar a instalação do ADT, inicie o Eclipse e selecione o item *Help | Software Updates | Find and Install...* no menu principal.

Na janela de diálogo *Install/Update*, selecione o item *Search for new features to install* e pressione o botão *Next*. Na janela de diálogo *Install*, clique no botão *New Remote Site...* e, na janela que se abre (**figura 2**), digite o endereço `https://dl-ssl.google.com/android/eclipse/` para instalação do plugin e digite o nome que desejar (*Android Plugin*, *na* **figura 2**), confirmando , em seguida, com o botão *OK*.

Por último, basta selecionar o novo site (**figura 3**) e clicar em *Finish*, confirmando a instalação do plugin (que não é assinado – não precisa entrar em pânico) com *Install All*. Ao concluir a instalação, reinicie o Eclipse.

Após a reinicialização do Eclipse, atualize ou configure a localização do Android SDK no plugin ADT do Eclipse. Selecione o item "Windows" no menu principal e, ao abrir a janela de preferências, selecione a opção *Android* no painel da esquerda, informando a localização do Android SDK com o botão *Browse* no campo *SDK Location*. Para finalizar, pressione o botão *Apply* e, depois, *OK*.

Se tudo aconteceu como mostrado até esse ponto, o plugin do ADT já estará instalado e configurado corretamente no Eclipse.

Olá, mundo

Vamos agora criar nosso primeiro aplicativo para o Android usando o Eclipse. Para isso, selecione a opção *File* no menu principal, depois a opção *New* e, logo após clique em *Project*. Em seguida, selecione o item *Android Project* e clique no botão *Next*.

Na janela de diálogo do projeto, digite os nomes do projeto, do pacote, da classe e da aplicação. Selecione as opções *Create new project in workspace* e *Use default location*, clicando no botão *Finish*, ao final. Se tudo estiver funcionando corretamente, um código semelhante ao do **exemplo 1** será criado no projeto *HelloAndroid*, exceto pelas **linhas 5**, **12**, **13** e **14**, que devem ser acrescentadas ou editadas para que o resultado seja semelhante a ele.

Para executar o programa no emulador do Android, basta selecionar o item *Run | Run...* do menu principal. Na janela de diálogo (**figura 4**), selecione o projeto para execução e clique nos botões *Apply* e *Run*. Assim, o emulador

Figura 5 Resultado da execução do programa de teste.

Figura 6 Layout do programa de conversão de câmbio.

será iniciado, nos permitindo ver esse primeiro programa em ação no Android (**figura 5**).

Sem Eclipse?

Também é possível escrever aplicativos para o Android sem usar o Eclipse, recorrendo apenas à linha de comando. Para isso, o Android SDK traz um script escrito em *Python* chamado `activityCreator.py`. O comando adequado, nesse caso, seria:

```
activityCreator.py --out
➥HelloAndroid com.android.hello.
➥HelloAndroid
```

Em seguida, acesse a pasta `HelloAndroid/` (criada pelo script), onde se encontra-se o arquivo `build.xml`. Partindo do princípio de que o *Apache Ant* esteja instalado corretamente, basta executar o comando `ant` para compilar o programa `HelloAndroid`.

Exemplo 2: Aplicativo de câmbio

```
package com.android.lm;

import android.app.Activity;
import android.os.Bundle;
import android.view.View;
import android.view.View.OnClickListener;
import android.widget.Button;
import android.widget.RadioButton;
import android.widget.TextView;

public class HelloLM extends Activity {
     TextView dolar;
     TextView real;
     RadioButton dtor;
     RadioButton rtod;
     Button convert;

     /** Called when the activity is first created. */
     @Override
     public void onCreate(Bundle icicle) {
        super.onCreate(icicle);
        setContentView(R.layout.main);
        dolar = (TextView)this.findViewById(R.id.dolar);
        real = (TextView)this.findViewById(R.id.real);
        dtor = (RadioButton)this.findViewById(R.id.dtor);
        dtor.setChecked(true);
        rtod = (RadioButton)this.findViewById(R.id.rtod);

        convert = (Button)this.findViewById(R.id.convert);
        convert.setOnClickListener(new Button.OnClickListener() {
        public void onClick(View v) {
           if (dtor.isChecked()) {
              convertDolarToReal();
           }
           if (rtod.isChecked()) {
              convertRealToDolar();
           }
        }});
     }
        protected void convertDolarToReal() {
           double val = Double.parseDouble(dolar.getText().toString());
           real.setText(Double.toString(val*1.8));
        }
        protected void convertRealToDolar() {
           double val = Double.parseDouble(real.getText().toString());
           dolar.setText(Double.toString(val/1.8));
        }
```

Layout

No mundo dos aplicativos embarcados, a aparência tem uma importância ainda maior sobre a usabilidade. O *DroidDraw* é um editor de layout escrito em Java que possibilita a montagem de interfaces gráficas e sua gravação em um arquivo XML para posterior utilização no aplicativo. Essa ferramenta é muito útil para acelerar o desenvolvimento de aplicativos na plataforma Android.

O DroidDraw pode ser usado online[2] ou baixado a partir do site [3]. Para instalá-lo, basta descompactar o arquivo baixado, entrar no diretório criado por ele e executar o script `droiddraw.sh`.

Câmbio

Para explorar o DroidDraw, vamos criar um aplicativo para conversão de valores em reais para dólares.

Após iniciar o programa, o primeiro passo é selecionar a aba *Layouts* e, em seguida, o componente *LinearLayout*. Na aba *Properties*, altere a dimensão para 200 pixels de largura e 130 de altura, pressionando o botão *Apply* logo em seguida. Depois, na aba *Widgets*, arraste dois objetos *TextView*, dois *EditText*, dois *RadioButton* e um *Button* para a área da interface e crie um layout como na **figura 6**.

Novamente na aba *Properties*, altere o campo *id*

do primeiro objeto *EditText* para `@+id/dolar`", o do segundo *EditText* para `@+id/real`, o do primeiro *RadioButton* para `@+id/dor`, o do segundo *RadioButton* para `@+id/rtod` e o do *Button* para `@+id/convert`. Depois disso, basta clicar sobre o botão *Generate* para criar o arquivo do layout na janela *Output*.

Com o layout gerado, crie uma nova aplicação (com o Eclipse ou pelo script) e substitua o conteúdo do arquivo `res/layout/main.xml` pela estrutura XML gerada pelo DroidDraw. Depois, na pasta `src`, localize o arquivo `nome-da-classe.java` e insira o código do **exemplo 2** no arquivo fonte. Para visualizar o aplicativo em funcionamento, basta executar o programa com a opção *Run*, como mencionado anteriormente.

Emulador

O Android SDK traz ainda um prático emulador. Com ele, o desenvolvedor tem à disposição um aparelho celular emulado, capaz de executar todos os aplicativos desenvolvidos para a plataforma. Isso é ótimo para realizar testes sem um dispositivo físico. Todas as funções de um celular estão disponíveis, exceto aquelas relacionadas a chamadas telefônicas.

Para executar o emulador do Android, basta executar o comando `emulator`, que se encontra na pasta `tools/` do SDK. Por padrão, ele traz quatro "temas", chamados de *skins*. O que muda entre os skins é apenas a resolução da tela. Há as opções QVGA (320x240) e HVGA (480x320), nas orientações paisagem (sufixo *L*) e retrato (sufixo *P*). Para usar a resolução HVGA em formato paisagem, basta iniciar o emulador com o parâmetro `-skin HVGA-L`.

Exemplo 3: Shell do Android

```
$ adb shell
# ls  -l
drw-rw-rw- root     root          2008-04-14 06:29 cache
drwxr-xr-x root     root          2008-04-14 06:29 d
-rwxr-xr-x root     root     91952 1970-01-01 00:00 init
drwxr-xr-x root     root          1970-01-01 00:00 etc
drwxr-xr-x root     root          1970-01-01 00:00 var
drwxrwx--x system   system        2007-11-11 20:59 data
drwxr-xr-x root     root          2008-02-29 01:19 system
drwxr-xr-x root     root          1970-01-01 00:00 sys
drwxrwxrwt root     root          2008-04-14 06:49 tmp
dr-xr-xr-x root     root          1970-01-01 00:00 proc
drwxr-xr-x root     root          1970-01-01 00:00 sbin
drwx-- root     root          1970-01-01 00:00 root
drwxr-xr-x root     root          2008-04-14 06:29 dev
```

Depuração

O ADB, ou *Android Debug Bridge*, é um gerenciador de depuração poderoso. Este artigo ficaria muito extenso caso fossem mencionadas todas as opções e recursos disponíveis na ferramenta; por isso, serão abordadas apenas suas funções principais.

Para listar os emuladores disponíveis, usa-se o comando `adb devices`. A instalação de aplicativos também é possível e usa-se o comando `adb install /caminho/do/aplicativo.apk`. A desinstalação é igualmente fácil, pois requer apenas o comando `adb shell rm data/app/aplicativo.apk`. Como esse último comando leva a crer, é possível acessar uma shell do Android com o comando `adb shell` (**exemplo 3**).

O Android tem, embutido, um banco de dados *SQLite*, que se pode acessar, a partir da shell, com o comando:

```
# sqlite3 /data/data/com.
➥example.
 google.rss.rssexample/databases/
➥ rssitems.db
Ao vivo
```

Quem desejar poupar esforços de instalação do Android SDK pode recorrer ao *VD_Android*[4], uma distribuição Linux em *Live CD* que já traz o SDK instalado, assim como o IDE Eclipse e o aplicativo DroidDraw. A distribuição oferece ainda a opção de instalação no disco rígido ou em um *pendrive*. O VD_Android é baseado no *Debian Lenny* e utiliza como ambiente desktop padrão o *Xfce4*.

Conclusão

Para quem deseja ter contato com o Android, este artigo é um bom ponto de partida. A plataforma Android é poderosa e, como se vê, fácil de usar. Esperamos que ele ajude a iniciar uma longa caminhada de aprendizado. ■

Mais informações

[1] Download da SDK do Android: http://code.google.com/intl/pt-BR/android/download.html

[2] DroidDraw online: http://www.droiddraw.org/

[3] Download do DroidDraw: http://droiddraw.googlecode.com/files/droiddraw-r1b8.tgz

[4] VD_Android: http://tinyurl.com/6z2c3v

Linux.local

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

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

Empresa	Cidade	Endereço	Telefone	Web	1	2	3	4	5	6
Ceará										
F13 Tecnologia	Fortaleza	Rua Coronel Solon, 480 – Bairro de Fátima Fortaleza - CE - CEP: 60040-270	85 3252-3836	www.f13.com.br		✔	✔		✔	✔
Espírito Santo										
Linux Shopp	Vila Velha	Rua São Simão (Correspondência), 18 – CEP: 29113-120	27 3082-0932	www.linuxshopp.com.br	✔	✔		✔	✔	
Megawork Consultoria e Sistemas	Vitória	Rua Chapot Presvot, 389 – Praia do Canto – CEP: 29055-410 sl 201, 202	27 3315-2370	www.megawork.com.br			✔		✔	✔
Spirit Linux	Vitória	Rua Marins Alvarino, 150 – CEP: 29047-660	27 3227-5543	www.spiritlinux.com.br			✔		✔	✔
Minas Gerais										
Instituto Online	Belo Horizonte	Av. Bias Fortes, 932, Sala 204 – CEP: 30170-011	31 3224-7920	www.institutoonline.com.br				✔		✔
Linux Place	Belo Horizonte	Rua do Ouro, 136, Sala 301 – Serra – CEP: 30220-000	31 3284-0575	corporate.linuxplace.com.br		✔	✔		✔	✔
Microhard	Belo Horizonte	Rua República da Argentina, 520 – Sion – CEP: 30315-490	31 3281-5522	www.microhard.com.br	✔	✔	✔		✔	✔
TurboSite	Belo Horizonte	Rua Paraíba, 966, Sala 303 – Savassi – CEP: 30130-141	0800 702-9004	www.turbosite.com.br	✔				✔	✔
Paraná										
iSolve	Curitiba	Av. Cândido de Abreu, 526, Cj. 1206B – CEP: 80530-000	41 252-2977	www.isolve.com.br		✔	✔			✔
Mandriva Conectiva	Curitiba	Rua Tocantins, 89 – Cristo Rei – CEP: 80050-430	41 3360-2600	www.mandriva.com.br			✔	✔	✔	✔
Telway Tecnologia	Curitiba	Rua Francisco Rocha 1830/71	41 3203-0375	www.telway.com.br					✔	✔
Rio de Janeiro										
NSI Training	Rio de Janeiro	Rua Araújo Porto Alegre, 71, 4ºandar Centro – CEP: 20030-012	21 2220-7055	www.nsi.com.br				✔		✔
Open IT	Rio de Janeiro	Rua do Mercado, 34, Sl, 402 – Centro – CEP: 20010-120	21 2508-9103	www.openit.com.br				✔		✔
Unipi Tecnologias	Campos dos Goytacazes	Av. Alberto Torres, 303, 1ºandar - Centro – CEP: 28035-581	22 2725-1041	www.unipi.com.br			✔	✔	✔	✔
Rio Grande do Sul										
4up Soluções Corporativas	Novo Hamburgo	Pso. Calçadão Osvaldo Cruz, 54 sl. 301 CEP: 93510-015	51 3581-4383	www.4up.com.br		✔	✔		✔	✔
Definitiva Informática	Novo Hamburgo	Rua General Osório, 402 - Hamburgo Velho	51 3594 3140	www.definitiva.com.br	✔		✔		✔	✔
Solis	Lajeado	Rua Comandante Wagner, 12 – São Cristóvão – CEP: 95900-000	51 3714-6653	www.solis.coop.br		✔	✔	✔	✔	✔
DualCon	Novo Hamburgo	Rua Joaquim Pedro Soares, 1099, Sl. 305 – Centro	51 3593-5437	www.dualcon.com.br	✔		✔		✔	✔
Datarecover	Porto Alegre	Av. Carlos Gomes, 403, Sala 908, Centro Comercial Atrium Center – Bela Vista – CEP: 90480-003	51 3018-1200	www.datarecover.com.br	✔		✔			
LM2 Consulting	Porto Alegre	Rua Germano Petersen Junior, 101-Sl 202 – Higienópolis – CEP: 90540-140	51 3018-1007	www.lm2.com.br			✔		✔	✔
Lnx-IT Informação e Tecnologia	Porto Alegre	Av. Venâncio Aires, 1137 – Rio Branco – CEP: 90.040.193	51 3331-1446	www.lnx-it.inf.br	✔		✔		✔	✔
Plugin	Porto Alegre	Av. Júlio de Castilhos, 132, 11º andar Centro – CEP: 90030-130	51 4003-1001	www.plugin.com.br	✔		✔		✔	
TeHospedo	Porto Alegre	Rua dos Andradas, 1234/610 – Centro – CEP: 90020-008	51 3286-3799	www.tehospedo.com.br	✔	✔				
São Paulo										
Ws Host	Arthur Nogueira	Rua Jerere, 36 – Vista Alegre – CEP: 13280-000	19 3846-1137	www.wshost.com.br	✔		✔		✔	
DigiVoice	Barueri	Al. Juruá, 159, Térreo – Alphaville – CEP: 06455-010	11 4195-2557	www.digivoice.com.br	✔	✔	✔		✔	✔
Dextra Sistemas	Campinas	Rua Antônio Paioli, 320 – Pq. das Universidades – CEP: 13086-045	19 3256-6722	www.dextra.com.br			✔		✔	✔
Insigne Free Software do Brasil	Campinas	Av. Andrades Neves, 1579 – Castelo – CEP: 13070-001	19 3213-2100	www.insignesoftware.com			✔		✔	✔
Microcamp	Campinas	Av. Thomaz Alves, 20 – Centro – CEP: 13010-160	19 3236-1915	www.microcamp.com.br				✔		✔
PC2 Consultoria em Software Livre	Carapicuiba	Rua Edeia, 500 - CEP: 06350-080	11 3213-6388	www.pc2consultoria.com	✔					✔
Savant Tecnologia	Diadema	Av. Senador Vitorino Freire, 465 – CEP: 09910-550	11 5034-4199	www.savant.com.br	✔	✔	✔			✔
Epopéia Informática	Marília	Rua Goiás, 392 – Bairro Cascata – CEP: 17509-140	14 3413-1137	www.epopeia.com.br						✔
Redentor	Osasco	Rua Costante Piovan, 150 – Jd. Três Montanhas – CEP: 06263-270	11 2106-9392	www.redentor.ind.br	✔					
Go-Global	Santana de Parnaíba	Av. Yojiro Takaoca, 4384, Ed. Shopping Service, Cj. 1013 – CEP: 06541-038	11 2173-4211	www.go-global.com.br			✔		✔	✔
AW2NET	Santo André	Rua Edson Soares, 59 – CEP: 09760-350	11 4990-0065	www.aw2net.com.br			✔		✔	✔
Async Open Source	São Carlos	Rua Orlando Damiano, 2212 – CEP 13560-450	16 3376-0125	www.async.com.br	✔				✔	✔
Delix Internet	São José do Rio Preto	Rua Voluntário de São Paulo, 3066 9º – Centro – CEP: 15015-909	11 4062-9889	www.delixhosting.com.br	✔		✔		✔	

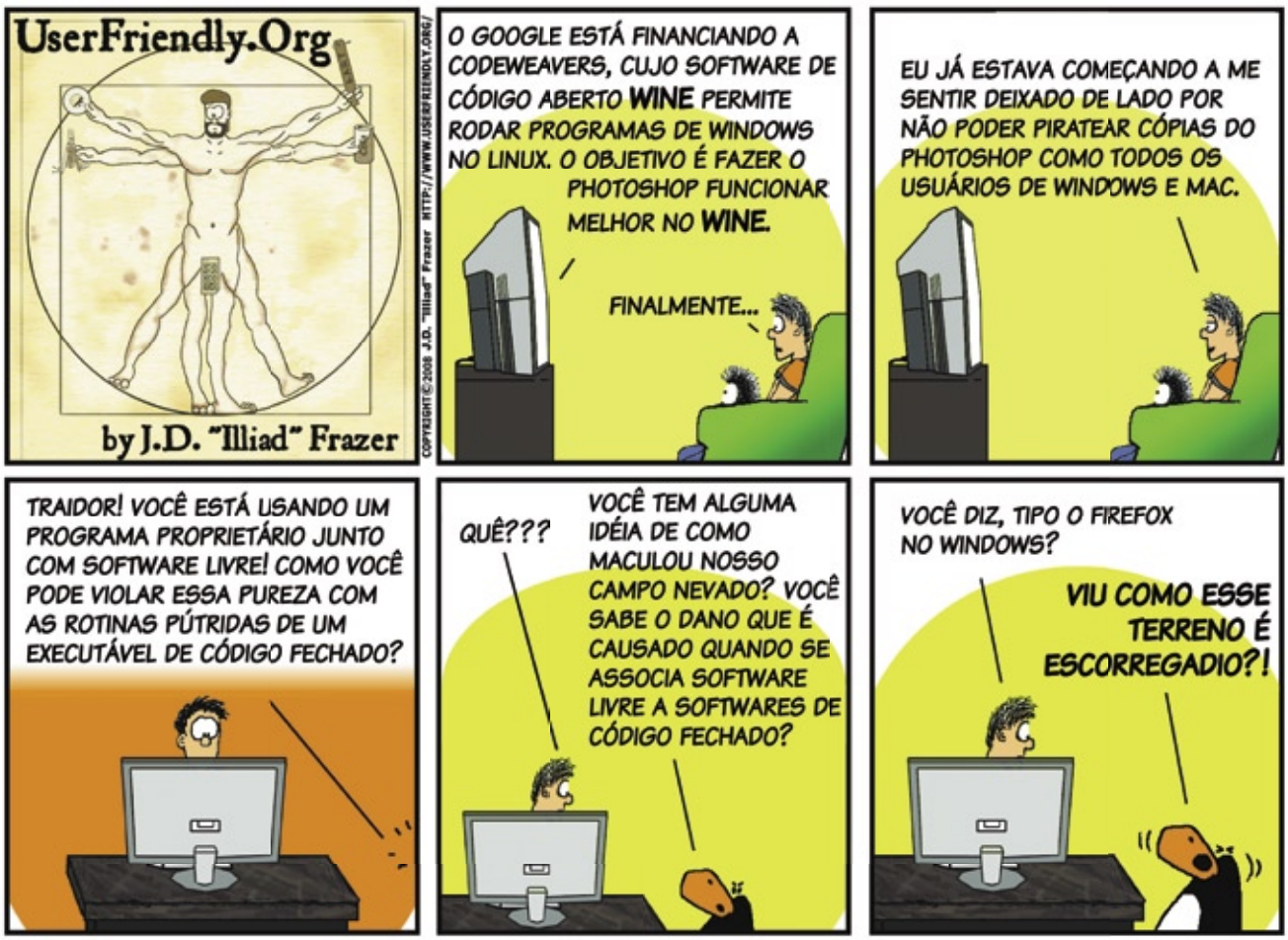
Empresa	Cidade	Endereço	Telefone	Web	1	2	3	4	5	6
São Paulo (continuação)										
4Linux	São Paulo	Rua Teixeira da Silva, 660, 6º andar – CEP: 04002-031	11 2125-4747	www.4linux.com.br					✔	✔
A Casa do Linux	São Paulo	Al. Jaú, 490 – Jd. Paulista – CEP: 01420-000	11 3549-5151	www.acasadolinux.com.br			✔		✔	✔
Accenture do Brasil Ltda.	São Paulo	Rua Alexandre Dumas, 2051 – Chácara Santo Antônio – CEP: 04717-004	11 5188-3000	www.accenture.com.br			✔		✔	✔
ACR Informática	São Paulo	Rua Lincoln de Albuquerque, 65 –Perdizes – CEP: 05004-010	11 3873-1515	www.acrinformatica.com.br	✔					✔
Agit Informática	São Paulo	Rua Major Quedinho, 111, 5º andar, Cj. 508 – Centro – CEP: 01050-030	11 3255-4945	www.agit.com.br	✔	✔				✔
Altbit - Informática Comércio e Serviços LTDA.	São Paulo	Av. Francisco Matarazzo, 229, Cj. 57 – Água Branca – CEP 05001-000	11 3879-9390	www.altbit.com.br	✔		✔		✔	✔
AS2M -WPC Consultoria	São Paulo	Rua Três Rios, 131, Cj. 61A – Bom Retiro – CEP: 01123-001	11 3228-3709	www.wpc.com.br			✔		✔	✔
Big Host	São Paulo	Rua Dr. Miguel Couto, 58 – Centro – CEP: 01008-010	11 3033-4000	www.bighost.com.br	✔				✔	✔
Blanes	São Paulo	Rua André Ampére, 153 – 9º andar – Conj. 91 CEP: 04562-907 (próx. Av. L. C. Berrini)	11 5506-9677	www.blanes.com.br	✔	✔	✔		✔	✔
Commlogik do Brasil Ltda.	São Paulo	Av. das Nações Unidas, 13.797, Bloco II, 6º andar – Morumbi – CEP: 04794-000	11 5503-1011	www.commlogik.com.br	✔	✔	✔		✔	✔
Computer Consulting Projeto e Consultoria Ltda.	São Paulo	Rua Vergueiro, 6455, Cj. 06 – Alto do Ipiranga – CEP: 04273-100	11 5062-3927	www.computerconsulting.com.br	✔		✔		✔	✔
Consist Consultoria, Sistemas e Representações Ltda.	São Paulo	Av. das Nações Unidas, 20.727 – CEP: 04795-100	11 5693-7210	www.consist.com.br			✔	✔	✔	✔
Domínio Tecnologia	São Paulo	Rua das Carnaubeiras, 98 – Metrô Conceição – CEP: 04343-080	11 5017-0040	www.dominiotecnologia.com.br	✔					✔
EDS do Brasil	São Paulo	Av. Pres. Juscelino Kubistcheck, 1830 Torre 4 - 5º andar	11 3707-4100	www.eds.com		✔	✔			✔
Ética Tecnologia	São Paulo	Rua Nova York, 945 – Brooklin – CEP:04560-002	11 5093-3025	www.etica.net	✔		✔		✔	✔
Getronics ICT Solutions and Services	São Paulo	Rua Verbo Divino, 1207 – CEP: 04719-002	11 5187-2700	www.getronics.com/br			✔		✔	✔
Hewlett-Packard Brasil Ltda.	São Paulo	Av. das Nações Unidas, 12.901, 25º andar – CEP: 04578-000	11 5502-5000	www.hp.com.br	✔		✔	✔	✔	✔
IBM Brasil Ltda.	São Paulo	Rua Tutóia, 1157 – CEP: 04007-900	0800-7074 837	www.br.ibm.com	✔		✔		✔	✔
iFractal	São Paulo	Rua Fiação da Saúde, 145, Conj. 66 – Saúde – CEP: 04144-020	11 5078-6618	www.ifractal.com.br			✔		✔	✔
Integral	São Paulo	Rua Dr. Gentil Leite Martins, 295, 2º andar Jd. Prudência – CEP: 04648-001	11 5545-2600	www.integral.com.br	✔				✔	
Itautec S.A.	São Paulo	Rua Santa Catarina, 1 – Tatuapé – CEP: 03086-025	11 6097-3000	www.itautec.com.br	✔	✔	✔		✔	✔
Kenos Consultoria	São Paulo	Av: Fagundes Filho, 13, Conj -53 – CEP: 04304-000	11 40821305	www.kenos.com.br					✔	✔
Konsultex Informatica	São Paulo	Av. Dr. Guilherme Dumont Villares, 1410 6 andar, CEP: 05640-003	11 3773-9009	www.konsultex.com.br			✔		✔	✔
Linux Komputer Informática	São Paulo	Av. Dr. Lino de Moraes Leme, 185 – CEP: 04360-001	11 5034-4191	www.komputer.com.br	✔		✔		✔	✔
Linux Mall	São Paulo	Rua Machado Bittencourt, 190, Cj. 2087 – CEP: 04044-001	11 5087-9441	www.linuxmall.com.br	✔			✔	✔	
Livraria Tempo Real	São Paulo	Al. Santos, 1202 – Cerqueira César – CEP: 01418-100	11 3266-2988	www.temporeal.com.br				✔	✔	✔
Locasite Internet Service	São Paulo	Av. Brigadeiro Luiz Antonio, 2482, 3º andar – Centro – CEP: 01402-000	11 2121-4555	www.locasite.com.br	✔				✔	✔
Microsiga	São Paulo	Av. Braz Leme, 1631 – CEP: 02511-000	11 3981-7200	www.microsiga.com.br			✔		✔	✔
Novatec Editora Ltda.	São Paulo	Rua Luis Antonio dos Santos, 110 – Santana – CEP: 02460-000	11 6979-0071	www.novateceditora.com.br				✔		
Novell América Latina	São Paulo	Rua Funchal, 418 – Vila Olímpia	11 3345-3900	www.novell.com/brasil			✔		✔	✔
Oracle do Brasil Sistemas Ltda.	São Paulo	Av. Alfredo Egídio de Souza Aranha, 100 – Bloco B – 5º andar – CEP: 04726-170	11 5189-3000	www.oracle.com.br					✔	✔
Proelbra Tecnologia Eletrônica Ltda.	São Paulo	Av. Rouxinol, 1.041, Cj. 204, 2º andar Moema – CEP: 04516-001	11 5052- 8044	www.proelbra.com.br	✔		✔			✔
Provider	São Paulo	Av. Cardoso de Melo, 1450, 6º andar – Vila Olímpia – CEP: 04548-005	11 2165-6500	www.e-provider.com.br			✔		✔	✔
Red Hat Brasil	São Paulo	Av. Brigadeiro Faria Lima, 3900, Cj 81 8º andar Itaim Bibi – CEP: 04538-132	11 3529-6000	www.redhat.com.br			✔		✔	✔
Samurai Projetos Especiais	São Paulo	Rua Barão do Triunfo, 550, 6º andar – CEP: 04602-002	11 5097-3014	www.samurai.com.br			✔		✔	✔
SAP Brasil	São Paulo	Av. das Nações Unidas, 11.541, 16º andar – CEP: 04578-000	11 5503-2400	www.sap.com.br			✔		✔	✔
Simples Consultoria	São Paulo	Rua Mourato Coelho, 299, Cj. 02 Pinheiros – CEP: 05417-010	11 3898-2121	www.simplesconsultoria.com.br			✔		✔	✔
Smart Solutions	São Paulo	Av. Jabaquara, 2940 cj 56 e 57	11 5052-5958	www.smart-tec.com.br		✔	✔		✔	✔
Snap IT	São Paulo	Rua João Gomes Junior, 131 – Jd. Bonfiglioli – CEP: 05299-000	11 3731-8008	www.snapit.com.br			✔		✔	✔
Stefanini IT Solutions	São Paulo	Av. Brig. Faria Lima, 1355, 19º – Pinheiros – CEP: 01452-919	11 3039-2000	www.stefanini.com.br			✔		✔	✔
Sun Microsystems	São Paulo	Rua Alexandre Dumas, 2016 – CEP: 04717-004	11 5187-2100	www.sun.com.br	✔		✔		✔	✔
Sybase Brasil	São Paulo	Av. Juscelino Kubitschek, 510, 9º andar Itaim Bibi – CEP: 04543-000	11 3046-7388	www.sybase.com.br					✔	✔
The Source	São Paulo	Rua Marquês de Abrantes, 203 – Chácara Tatuapé – CEP: 03060-020	11 6698-5090	www.thesource.com.br			✔		✔	✔
Unisys Brasil Ltda.	São Paulo	R. Alexandre Dumas 1658 – 6º, 7º e 8º andares – Chácara Santo Antônio – CEP: 04717-004	11 3305-7000	www.unisys.com.br	✔		✔		✔	✔
Utah	São Paulo	Av. Paulista, 925, 13º andar – Cerqueira César – CEP: 01311-916	11 3145-5888	www.utah.com.br			✔		✔	✔
Visuelles	São Paulo	Rua Eng. Domicio Diele Pacheco e Silva, 585 – Interlagos – CEP: 04455-310	11 5614-1010	www.visuelles.com.br			✔		✔	✔
Webnow	São Paulo	Av. Nações Unidas, 12.995, 10º andar, Ed. Plaza Centenário – Chácara Itaim – CEP: 04578-000	11 5503-6510	www.webnow.com.br	✔		✔		✔	
WRL Informática Ltda.	São Paulo	Rua Santa Ifigênia, 211/213, Box 02– Centro – CEP: 01207-001	11 3362-1334	www.wrl.com.br	✔		✔		✔	
Systech	Taquaritinga	Rua São José, 1126 – Centro - Caixa Postal 71 – CEP: 15.900-000	16 3252-7308	www.systech-ltd.com.br	✔	✔			✔	

Calendário de eventos

Evento	Data	Local	Website
DebConf8	10 a 16 de agosto	Mar del Plata, Argentina	www.debconf8.debconf.org
Linux Park	14 de agosto	Brasília, DF	www.linuxpark.com.br
Linux Park	28 de agosto	Curitiba, PR	www.linuxpark.com.brvv
Linux Park	30 de setembro	Ribeirão Preto, SP	www.linuxpark.com.br
Linux Park	9 de outubro	Recife, PE	www.linuxpark.com.br
Linux Park	21 de outubro	São Paulo, SP	www.linuxpark.com.br

Índice de anunciantes

User Friendly – Os quadrinhos mensais da Linux Magazine



Você está preparado para a TI virtualizada?

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

mais informações: www.linuxnewmedia.com.br

Coleção Linux Technical Review

LINUX NEW MEDIA
The Pulse of Open Source

PREVIEW

Na Linux Magazine #44

DESTAQUE

ITIL

Quem almeja vagas mais importantes na hierarquia de TI corporativa depende de alguns fatores, como tempo de experiência, habilidades de liderança e profundo conhecimento de todas as funções envolvidas num departamento de TI de uma grande empresa.

No entanto, apenas esses conhecimentos não bastam; as decisões sobre algumas práticas podem tender demais ao subjetivismo do gestor de TI, levando toda a equipe a resultados diferentes (com freqüência, piores) do que o esperado.

Para isso, existem as boas práticas, um conjunto de orientações bem fundadas e baseadas na experiência de muitos anos de administração. A *Information Technology Infrastructure Library* – ITIL – é um conjunto de orientações conceituais e práticas destinado a direcionar a gestão de TI, incluindo infra-estrutura, desenvolvimento e operações.

Na Linux Magazine 44, apresentaremos o ITIL, sua abrangência, suas certificações e as novidades da última versão da *biblioteca*. ■

Segurança

DNSSEC

Os administradores de sistemas e consultores de segurança utilizam estratégias sofisticadas para proteger redes, mas ainda existe uma parte muito básica da infra-estrutura da Internet que permanece surpreendentemente vulnerável: o sistema de resolução de nomes. Existem técnicas elaboradas para forjar respostas DNS e, da mesma forma, maneiras também engenhosas de se contornar esses ataques. De todas elas, o DNSSEC desponta como uma das mais eficazes para proteger redes por meio de criptografia e autenticação.

Conheça essa tecnologia e mantenha seu sistema de resolução de nomes protegido. ■

Na EasyLinux #13

DESTAQUE

Portáteis!

Os laptops e notebooks sempre deram aos seus possuidores um certo glamour, status de pessoas antenadas e, claro, fama de gente que tinha "grana" – afinal, um bom portátil, até dois anos atrás, não custava nada barato. Com o passar do tempo, no entanto, fabricantes foram criando uma nova geração de notebooks: menores, sem partes mecânicas quebráveis em boa parte de suas versões e mais baratos. Esses aparelhinhos, chamados de sub-notebooks, vêm ganhando espaço, tanto entre os clientes "tradicionais" dos laptops quanto entre pessoas que jamais imaginaram ter um portátil. ■

Oficina

Com jeito de cinema

A qualidade de aúdio e vídeo da TV digital, recentemente iniciada no Brasil, é um atrativo para quem deseja assistir programas em alta resolução e até gravar alguns de seus preferidos. Se os receptores de TV ainda estão muito caros, receptores USB para computador oferecem a imagem de cinema e qualidade de som de DVD. E, o que é melhor, usando Linux. ■

Guia de TI

Soluções em Tecnologias Abertas

LINUX NEW MEDIA
The Pulse of Open Source

Garanta já sua vaga para o Guia de TI 2009!

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

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

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

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

NovaForge™

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

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

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

BULL

Architect of an Open World™

www.bull.com